ЗАНЯТИЕ №1. Подключение и основные настройки межсетевого экрана, управление через консоль, Web-интерфейс, SSH. Сброс межсетевого экрана к заводским настройкам по умолчанию. Обновление прошивки, сохранение конфигурации. Режимы admin, audit.

Межсетевыми экранами D-Link, можно управлять через консольный порт (в DFL-210/260/800/860/1600/1660/2500/2560 – это RS-232; в DFL-260E/860E – это порт RJ-45 через кабель RJ45-to-DB9), Web-интерфейс, с использованием протокола SSH или SNMP (централизованная система управления). Интерфейс командной строки (CLI) может быть использован для настройки и управления межсетевым экраном через консоль и с помощью протокола SSH.

На протяжении всех лабораторных работ мы сосредоточимся в основном на использовании Web-интерфейса для настройки различных возможностей межсетевых экранов.

Цель	Эта лабораторная работа предназначена для ознакомления пользователей с основными командами для настройки, контроля и устранения неполадок межсетевых экранов D-Link	
Оборудование	DFL-860E	1
	Рабочая станция	1
	Кабель Ethernet (патч-корд)	2
	Консольный кабель	1

Настройка DFL-860E

Индикаторы и порты устройства

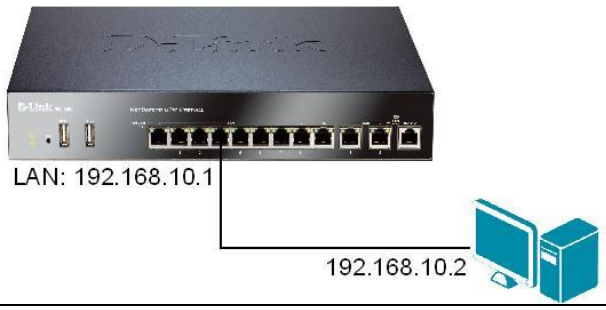
На передней панели устройства D-Link DFL-860E расположены следующие индикаторы:
- Power
- System
- индикаторы портов (левый и правый)
Порты передней панели:
- 2 порта WAN,
- 1 порт DMZ,
- 8 портов LAN,
- консольный порт RJ-45.
Описание индикации:

Индикатор	*Статус*	*Цвет*	*Описание*
Power	*Горит*	*Зеленый*	*Питание устройства включено*
	Не горит		*Питание устройства выключено*
System	*Горит*	*Зеленый*	*Система работает надлежащим образом*
	Не горит		*Устройство не работает*
Индикатор порта (левый)	*Горит*	*Зеленый*	*Канал организован (скорость 100 Мбит/с)*
	Мигает		*Передача и прием данных на порту*
	Не горит		*Канал отсутвует*
Индикатор порта (правый)	*Горит*	*Желтый*	*Канал организован (скорость 1000 Мбит/с)*
	Мигает		*Передача и прием данных на порту*
	Не горит		*Канал отсутвует*

Настройки интерфейсов по умолчанию:

	Интерфейс	*Имя интерфейса по умолчанию*	*Тип интерфейса по умолчанию*	*IP-адрес интерфейса по умолчанию*	*Статус DHCP по умолчанию*
	WAN1	*wan1*	*DHCP-клиент*	*0.0.0.0/0*	*Включен*
	WAN2	*wan2*	*Статический IP*	*192.168.120.254/24*	*Выключен*
	DMZ	*dmz*	*Статический IP*	*172.17.100.254/24*	*Выключен*
	Ports: 1~8	*lan*	*Статический IP*	*192.168.10.1/24*	*Выключен*

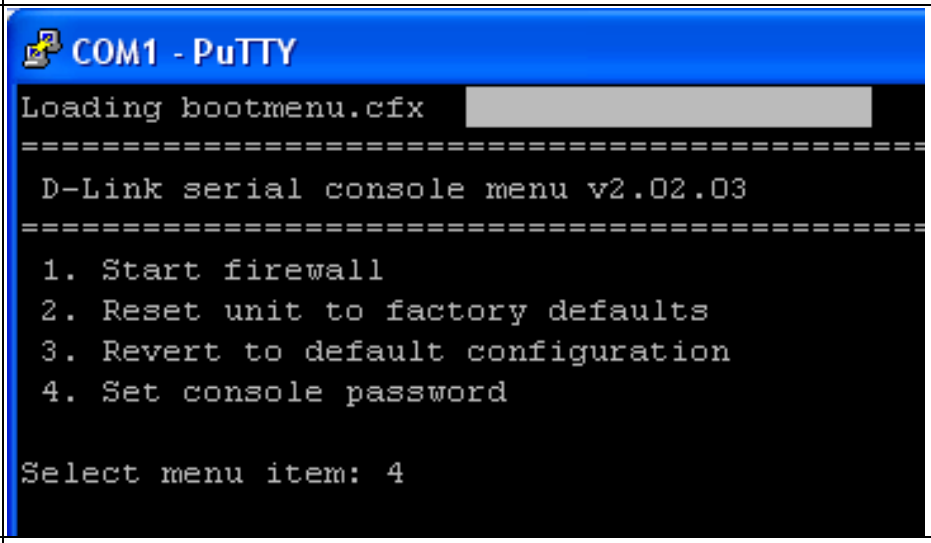
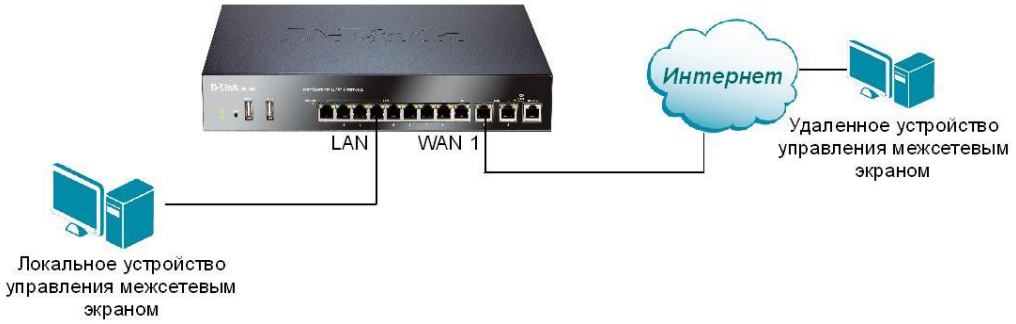
Примечание:
1. Интерфейсы* wan1 *и* wan2 *не поддерживают автоматическое определение полярности кабеля MDI/MDI-X (тип кабеля Straight-through или Crossover).
2. В целях безопасности по умолчанию Web-управление включено только на интерфейсе* lan *(192.168.10.1), через который может быть осуществлен доступ к Web-интерфейсу посредством Web-браузера с использованием протокола HTTPS. Эти настройки могут быть изменены после входа в Web-интерфейс.
3. Настройки для других моделей межсетевых экранов серии DFL аналогичны, за исключением именования интерфейсов и их IP-адресов. Интерфейсы различаются количеством, настройками подсети по умолчанию (например, для интерфейсов* lan *в DFL-210/260/800/860/1600/2500: 192.168.1.1; в DFL-1660/2560: lan1 192.168.10.1, lan2 192.168.20.1, lan3 192.168.30.1).

Подключение устройства	*Подключите устройство к розетке питания. Для первоначальной настройки подсоедините кабелем Ethernet один из портов* **lan** *к локальной сети, в которой находиться используемый для управления межсетевым экраном компьютер (либо напрямую к компьютеру).*
Схема 1	

Настройка рабочей станции

Зададим сетевые настройки:
Для ОС Microsoft Windows XP: *Пуск → Настройка → Сетевые подключения → Подключение по локальной сети → Свойства → Протокол Интернета TCP/IP → Свойства → Использовать следующий IP-адрес*
Для ОС Microsoft Windows Vista/ Windows 7: *Пуск → Панель управления → Центр управления сетями и общим доступом → Изменение параметров адаптера → Подключение по локальной сети → Свойства → Протокол Интернета TCP/IPv4 → Свойства → Использовать следующий IP-адрес*
Введите параметры:

IP-адрес	192.168.10.2
Маска подсети	255.255.255.0
Основной шлюз	192.168.10.1
Авторизация в системе (Web-интерфейс)	*После подключения через Web-интерфейс необходимо авторизоваться в системе. По умолчанию имя пользователя (Username) – admin, пароль (Password) – admin.*

Схема 2	
Авторизация в системе (консольный порт)	*По умолчанию авторизация в системе с использованием командной строки CLI отключена. Очень важно задать пароль на консоли в процессе первоначальной настройки устройства, иначе при наличии физического доступа к консольному порту любой человек сможет зайти на межсетевой экран без авторизации.* *Следует отметить, что пароль, назначенный на консольном интерфейсе, не вляет на авторизацию через Web-интерфейс.*
Установка пароля на консольный интерфейс с помощью командрой строки	Для установки пароля на консоль зайдите в меню консоли, нажав клавишу при загрузке устройства, выберите пункт *4. Set console password.*
Меню консоли	
Установка даты и времени через Web-интерфейс	Задайте время и дату в папке *System*→кнопка *Set Date and Time*. Выберите соответствующий часовой пояс – *для Москвы GMT+3:00*. Выключите переход на летнее/зимнее время, убрав галочку *Enable daylight saving time.*
Настройка удаленного управления с помощью HTTP и HTTPS протоколов.	
Схема 3	

Web-интерфейс	
Зайдите в меню *System→Remote Management→Add→HTTP/HTTPS Management*, введите следующие параметры:	
Name	My_http_manage
HTTP	поставьте галочку (включено)
HTTPS	поставьте галочку (включено)
UserDatabase	AdminUsers
AccessLevel	Admin
Interface	wan1 (интерфейс, для которого настраивается управление)
Network	all-nets
Примечание: Существуют два уровня доступа для межсетевого экрана – Admin или Audit. В режиме аудита настройки устройства можно будет просматривать, но невозможно будет изменить.	
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> add RemoteManagement RemoteMgmtHTTP My_http_manage Network=all-nets Interface=wan1 LocalUserDatabase=AdminUsers HTTPS=Yes HTTP=Yes gw-world:/> activate (*подождать 3-5 секунд*) gw-world:/>commit	
Настройка удаленного управления по SSH (также доступ по SSH можно осуществить через LAN)**.**	
Разрешение управления по SSH	*Для удаленного управления по SSH необходимо создать SSH Management.*
Web-интерфейс	
Зайдите в меню *System→Remote Management→Add→SSH Management*, введите следующие параметры:	
Name	My_ssh_manage
Listening Port	22
Max Concurrent Clients	5
Session idle timeout	1800
Login grace timeout	30
Greeting Message	Hello!
Maximum Authentication Retries	5
Password	Поставьте галочку
Public key	Поставьте галочку
Host Key Algorithms	Выберите все доступные
Key Exchange Algorithms	Выберите все доступные
Integrity Algorithms	Выберите все доступные
UserDatabase	AdminUsers
AccessLevel	Admin
Interface	wan1 (интерфейс, для которого настраивается управление)
Network	all-nets
Командная строка (CLI)	

gw-world:/> add RemoteManagement RemoteMgmtSSH My_ssh_manage Network=all-nets Interface=wan1 LocalUserDatabase=AdminUsers gw-world:/> activate gw-world:/>commit	
Авторизация в системе	*После подключения через ssh необходимо зарегистрироваться в системе. По умолчанию имя пользователя (Username) – admin, пароль (Password) – admin.*
Использование сценариев (скриптов) CLI.	
Описание	*Для хранения и выполнения команд CLI администратором, NetDefendOS поддерживает функцию CLI scripting. CLI script – это предварительно определенная последовательность команд CLI, которые можно выполнить после их сохранения в файл и последующей загрузки файла на межсетевой экран NetDefend.* *Для создания CLI script нужно выполнить следующие шаги:* *1. Создайте текстовый файл в текстовом редакторе, содержащим последовательный список команд, по одной на строку.* *Для этих файлов D-Link рекомендует использовать расширение .sgs (Security Gateway Script). Имя файла, включая расширение, не должно содержать более 16 символов.* *2. Загрузите файл на межсетевой экран NetDefend, используя Secure Copy (SCP). Файлы-сценарии должны храниться в папке script. Загрузка SCP подробно описана ниже.* *3. Используйте команду CLI* ***script -execute*** *для запуска файла.* *ВНИМАНИЕ: В файлах скриптов используются только четыре команды:* ***add*** ***set*** ***delete*** ***cc*** *С помощью команды script -execute запускается именованный файл сценария (скрипта), предварительно загруженный на межсетевой экран. Например, для выполнения файла сценария my_script.sgs, который был предварительно загружен, используется следующая команда CLI:* *gw-world:/> script -execute -name=my_script.sgs* *Переменные скриптов. Файлы скриптов могут содержать любое количество переменных сценария, которые выглядят следующим образом:* *$1, $2, $3, $4…. $n* *Значения, используемые как имена переменных, определены в списке в конце командной строки script –execute. Числа 1…n в имени переменной указывают на положение значения переменной в списке. Первым идет значение $1, затем $2 и т.д. Переменная $0 является зарезервированной и перед выполнением всегда заменяется именем файла скрипта.* *Например, выполняется скрипт my_script.sgs с IP-адресом 126.12.11.1 и комментарием If1 Address , везде заменяя имеющуюся в скрипте переменную $1 на 126.12.11.1, и, соответственно, переменную $2 на строку If1 address.* *Файл my_script.sgs содержит одну командную строку CLI:*

	add IP4Address If1_ip Address=$1 Comments=$2
Описание сценария	*Необходимо использовать скрипт общей конфигурации для импорта конфигурации. Решение должно поддерживать следующие условия:* *- статическое подключение к Интернет-провайдеру;* *- DHCP-подключение компьютеров пользователей ко внутренней сети. Параметры настроек необходимо задать переменными.*
В любом текстовом редакторе (например, Блокноте) создайте текстовый файл с расширением .sgs , в котором прописываем команды, которые будут выполняться в соответствии с заданными шагами, сохраните файл как conf_b.sgs, введите следующие параметры:	
cc Address AddressFolder InterfaceAddresses add IP4Address ISP1_ip Address=$1 add IP4Address ISP1net Address=$2 add IP4Address ISP1_gw Address=$3 add IP4Address ISP1_dns1 Address=$4 add IP4Address ISP1_dns2 Address=$5 cc .. set Interface Ethernet 1 Name=ISP1 IP=InterfaceAddresses/ISP_ip Network=InterfaceAddresses/ISP1net DefaultGateway=InterfaceAddresses/ISP1_gw DHCPEnable=No add DHCPServer Lan_DHCPServer Interface=$6 IPAddressPool=InterfaceAddresses/lannet Netmask=255.255.255.0 DNS1=InterfaceAddresses/ISP1_dns1 DNS2=InterfaceAddresses/ISP1_dns2	
Примечание:1. Ethernet 1 – это интерфейс WAN/WAN1 (в зависимости от модели DFL) по умолчанию. ***2. Файл скрипта должен находиться в той же папке, что и файл pscp.exe.***	
Загрузите созданный скрипт, введя пароль администратора межсетевого экрана на запрос pscp:	
PSCP-клиент	C:\Users\User\pscp –scp conf_b.sgs admin@192.168.10.1:script/
Уточните успешность загрузки скрипта на межсетевой экран:	
Командная строка (консоль)	gw-world:/>script
Запустите скрипт, задав необходимые значения переменных:	
Командная строка (консоль)	gw-world:/>script –execute –name=conf_b.sgs 5.5.5.2 5.5.5.0/24 5.5.5.1 8.8.8.8 8.8.4.4 lan
Упражнение	Проверьте результаты работы скрипта.
Использование Dynamic DNS.	
Описание	*DNS-характеристики системы NetDefendOS позволяют информировать DNS-серверы при изменении IP-адреса межсетевого экрана NetDefend. Данные характеристики ссылаются на Dynamic DNS и используются при изменении внешних IP-адресов межсетевых экранов NetDefend.* *Dynamic DNS может применяться в VPN-сценариях, где обе конечные точки используют динамические IP-адреса. Также с помощью DynamicDNS можно управлять устройством, зная только его DNS-имя, при этом IP-адрес может меняться.* *HTTP Poster-клиент – сгенерированный динамический DNS-клиент, который позволяет определить 3 различных URL и значение поля Delay in seconds until all URLs are refetched (по умолчанию 604800 секунд или 7 дней).*

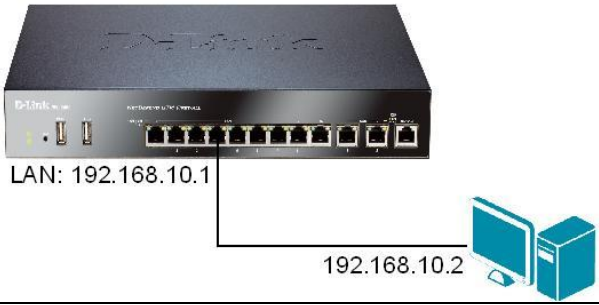
	По окончании каждого временного интервала HTTP Poster будет отправлять HTTP GET- запрос для определения URL. Запросы не посылаются автоматически при изменении настроек системы NetDefendOS, но есть одно исключение – изменение настроек из-за получения нового локального IP-адреса интерфейса, который соединяется с DNS-сервером.
Web-интерфейс	
Зайдите в меню *System→Misc. Clients→Add→D-Link DynDNS*, введите следующие параметры:	
DNS Prefix	mstu (имя хоста в dlinkddns.com)
Username	ksuser1
Password	Пароль к аккаунту
Confirm password	Пароль к аккаунту
Командная строка (CLI)	
gw-world:/> add Client DynDnsClientDLink DNSName=mstu Username=ksuser1 Password=P@ssw0rd gw-world:/> activate (*подождать 3-5 секунд*) gw-world:/>commit	
Упражнение	Зайдите из сети Интернет на устройство по wan1-интерфейсу, имеющему «белый» IP-адрес в D-Link DynDNS.
Примечание:1. Управление по wan1 должно быть разрешено для IP-адреса компьютера, с которого будет осуществлен вход на устройство. 2. DynDNS каждого типа может быть создан только один.	
Internet Explorer MS Windows	https://mstu.dlinkddns.com
Обновление прошивки межсетевого экрана.	
Зайдите в меню *Maintenance→Upgrade*, введите следующие параметры:	
Upgrade unit's firmware	Укажите путь к новой прошивке.
Нажмите *Upload firmware image*для загрузки новой прошивки в устройство.	
Сохранение конфигурации межсетевого экрана.	
Описание	*Настройки объектов и правил межсетевого экрана можно сохранить путем сохранения конфигурации устройства.*
Зайдите в меню *Maintenance→Backup*, введите следующие параметры:	
Backup configuration	Укажите путь для сохранения конфигурации.
По умолчанию файл конфигурации будет называться config-YYYYMMDD-v00N.bak, где YYYYMMDD – год, месяц, день, N – номер версии сохраненной конфигурации.	
Сброс межсетевого экрана к заводским настройкам по умолчанию.	
Описание	*В случаи необходимости межсетевой экран можно сбросить к заводским настройкам по умолчанию, используя один из следующих методов: - нажатие на кнопку Reset, - с помощью командной строки, - с помощью Web-интерфейса.*
Сброс нажатием на кнопку Reset	*Полный сброс – и конфигурации, и ПО устройства к заводским настройкам по умолчанию: 1. Убедитесь, что питание устройства отключено. 2. Нажмите и удерживайте кнопку Reset, расположенную на*

	задней панели межсетевого экрана. Удерживая в нажатом положении кнопку reset, включите питание межсетевого экрана. *3. Продолжайте удерживать кнопку reset в нажатом состоянии в течении 30 секунд после включения устройства* *4. Отпустите кнопку reset, и межсетевой экран будет сброшен к заводским настройкам по умолчанию.* *Частичный сброс – только конфигурации к настройкам по умолчанию:* *При поданном питании нажмите на кнопку Reset и удерживайте ее в нажатом состоянии в течении 30 секунд.*
Примечание: Межсетевой экран готов к настройке только, когда загорится светодиодный индикатор System.	
Сброс через консоль при загрузке	*1. Подключите консольный кабель на консольный порт DFL-860E ,и запустите программу putty.exe.* *2. В открывшемся окне выберите порт COM1, скорость 9600 и тип подключения Serial. Нажмите Open.* *3. Отключите на 5 секунд питание межсетевого экрана, а затем снова включите.* *4. В окне программы Putty выберите опцию по номером 1 для запуска межсетевого экрана D-Link.* *5. Быстро нажмите на Enter дважды, чтобы загрузить меню* *6. Выберите опцию 2.* *7. Введите Y (Да) на клавиатуре для сброса межсетевого экрана к заводским настройкам по умолчанию.*
Сброс с помощью Web-интерфейса	*1. Зайдите на устройство по Web-интерфейсу. По умолчанию установлен IP-адрес 192.168.10.1, имя пользователя admin, пароль admin.* *2. Зайдите в меню Maintenance→Reset.* *3. Выберите Restore the configuration to factory default и нажмите Reset to Factory Defaults.* *4. Нажмите Ok в появившемся окне. Это запустит процесс сброса межсетевого экрана к заводским настройкам по умолчанию.*
Сброс с помощью командной строки	*1. Зайдите на устройство через ssh-подключение. IP-адрес 192.168.10.1, имя пользователя admin, пароль admin.* *2. Введите следующую команду:* gw-word:/> reset -configuration
Примечание: При первом включении ненастроенного устройства запускается мастер установки (Setup Wizard), позволяющий задать все необходимые настройки – установить имя пользователя и пароль для учетной записи уровня администратора, установить дату и время, часовой пояс, NTP-сервер, настроить wan-интерфейсы (сетевые настройки, PPPoE, PPTP, BigPond, установить встроенный DHCP-сервер, настроить helper-сервер, Syslog-сервер для lan-интерфейса.	

ЗАНЯТИЕ №2. Логические объекты – адресная книга (Address Book), сервисы (Services), интерфейсы (Interfaces). Правила (Rules). Шлюз уровня приложений (Application Layer Gateway).

Для удобства использования и управления правилами безопасности в межсетевых экранах серии DFL используются логические объекты, позволяющие понятно для пользователя именовать различные базовые сетевые элементы устройства (интерфейсы, правила, сервисы, учетные записи пользователей и т.д.). Сервисы представляют собой программы, использующие сетевые протоколы для обеспечения различных приложений пользователей сети. Интерфейсы в межсетевых экранах DFL представлены как физические, так и некоторые логические (VLAN, PPPoE, ARP). Правила определяют основные функции фильтрации межсетевого экрана. Списки ALG позволяют организовать фильтрацию на самом верхнем уровне модели OSI (уровень приложения).

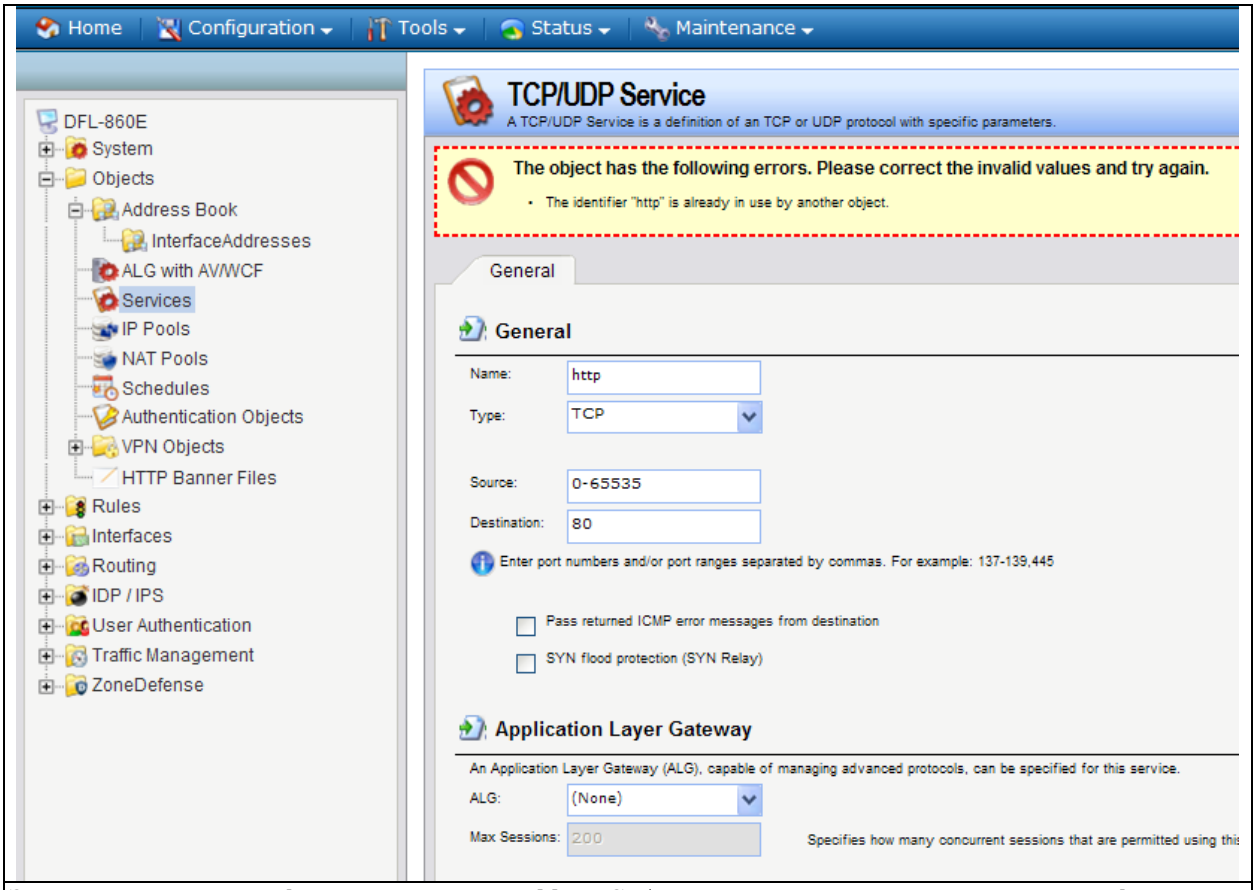
Цель	Эта лабораторная работа предназначена для изучения логических объектов, сервисов, интерфейсов, правил, списков ALG межсетевого экрана.	
Оборудование	DFL-860E	1
	Рабочая станция	1
	Кабель Ethernet (патч-корд)	2

Настройка DFL-860E	
Логические объекты (Objects)	
Определение	*Логические объекты – это базовые сетевые элементы, определённые в межсетевом экране. Фактически представляют собой защищаемые сети, недоверенные ресурсы и приложения, подлежащие проверке политиками безопасности.*
Address Book	*Address Book – совокупность символьных имен различных видов объектов межсетевого экрана (IP-адресов, групп IP-адресов, и др.).*
IP address	*Address Book межсетевых экранов D-Link позволяет именовать IP-адреса отдельных хостов, сетей, пары мастер/слейв или группы компьютеров и интерфейсов. Например, адрес «0.0.0.0/0» именуется «**all-nets**» и означает все возможные сети.*
Схема 4	
Создадим объект «IP-адрес». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Во вкладке *General* введите следующие параметры:	
Name	my_ip
IP Address	192.168.0.1

Создадим подсеть IPv4. Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Во вкладке *General* введите следующие параметры:	
Name	my_net
IP Address	192.168.0.0/24
Разрешим аутентификацию для IP-объекта. Зайдите в меню *User Authentication→Local User Databases→Add→Local User Database.*Создайте группу пользователей users для адреса локальной сети lannet, введите следующие параметры:	
Name	users
Создадим объект аутентификации net_users. Зайдите в *Objects→Address Book→Add→IP4 Group.* На вкладке *General* введите следующие параметры*:*	
Name	net_users
Group members	Выберите my_net из списка Available, переместите в список Selected.
Comments	Аутентификация “users” в my_net
На вкладке *User Authentication,* введите следующие параметры*:*	
Comma-separated list of user names and groups	users
Ethernet address	*Существует возможность задать MAC-адрес сетевого адаптера (физический адрес).*
Создадим объект «MAC-адрес». Зайдите в меню *Objects→Address Book→ InterfaceAddresses→Add→Ethernet Address.* На вкладке *General* введите следующие параметры:	
Name	MAC_ws
MAC Address	00-14-85-8E-E9-C6
Сервисы	*Services (сервисы, службы) – специальные программы, использующие определенные протоколы для предоставления различных приложений сетевым пользователям. Большинство приложений зависят от протоколов 7-го уровня модели OSI (Application Layer), передачу данных обеспечивает связка типа протокол/порт. Например, сервис HTTP использует протокол TCP и порт 80. Межсетевой экран позволяет создавать свои нестандартные сервисы.* *При этом сервис не проводит никакого действия над проходящим трафиком, для этого служат правила IP Rules.*
Типы сервисов	*На межсетевом экране сервисы могут быть сконфигурированы с помощью трех опций TCP/UDP Service, ICMP Service и IP Protocol Service. Сервис определяется именем, типом протокола и параметрами протокола. Различные сервисы могут быть объединены в группу (Service Group) для упрощения конфигурации политик, таким образом администратору нет необходимости конфигурировать каждый сервис отдельно.*
Сервисы на основе TCP и UDP	*Большинство приложений работает с протоколами TCP и UDP, связанными с одним определенным номером порта. В межсетевом экране такие сервисы определяются типом протокола, используемым приложением, и привязываются к определенному порту или диапазону портов. Для большинства сервисов достаточен только порт назначения, при этом порты источника могут быть любыми (в диапазоне 0-65535). Примеры: HTTP – TCP:80, Telnet – TCP:23, SMTP – TCP:25.* *Допускается диапазон портов назначения и диапазон портов источника одновременно. Пример: сервис имеет порты источника 1024-65535, порты назначения 80-82, 90-92, 95.*
Создадим TCP-сервис HTTP. Зайдите в меню *Objects→Services→Add→TCP/UDP Service.* Во	

вкладке *General* введите следующие параметры*:*	
Name	my_http
Type	TCP
Source	0-65535
Destination	80
Сервисы на основе ICMP	*ICMP – протокол, интегрированный с протоколом IP для сообщения об ошибках и передачи контрольной информации. Например, команда PING использует протокол ICMP для проверки сети. Сообщение ICMP доставляется IP-пакетами, каждое сообщение представляет собой отдельный протокол, имеющий свой собственный формат. Их изменения содержания зависят от Message Type&Code.* *Типы ICMP-сообщений в межсетевом экране с различными кодами:* *- Echo Request – посылает PING узлу назначения для проверки его доступности,* *- Destination Unreachable – источник сообщает о проблеме при доставке пакета:* *Code 0. Net Unreachable. Заданная сеть не доступна.* *Code 1. Host Unreachable. Заданный узел не доступен.* *Code 2. Protocol Unreachable. Протокол не доступен.* *Code 3. Port Unreachable. Порт не доступен.* *Code 4. Cannot Fragment. Не поддерживаются данный размер фрагмента.* *Code 5. Source Route Failed. Ошибка маршрутизации источника.* *- Redirect – сообщение от хоста о наличии более лучшего маршрута для конкретного пакета:* *Code 0. Rredirect datagrams for the network. Перенаправление датаграм для сети.* *Code 1. Redirect datagrams for the host. Перенаправление датаграм для хоста.* *Code 2. Redirect datagrams for the Type of Service and the network. Перенаправление датаграм для типа сервиса и сети.* *Code 3. Redirect datagrams for the Type of Service and the host. Перенаправление датаграм для типа сервиса и хоста.* *- Parameter Problem – определяет некорректный параметр датаграмы.* *- Echo Reply – ответ узла назначения, отправленный в качестве EchoRequest.* *- Source Quenching – источник посылает данные слишком быстро для приемника, буфер переполнен.* *- Time Exceeded – пакет отброшен, т.к. превышен интервал ожидания для запроса.*
Создадим ICMP-сервис. Зайдите в меню *Objects→Services→Add→ICMP Service.* Во вкладке *General* введите следующие параметры*:*	
Name	my_ICMP_service
Во вкладке *ICMP Parameters* введите следующие параметры*:*	
ICMP Type	Redirect
Code	Code 1
Примечание: Если выбрать опцию All ICMP Message Types, то создаваемый сервис будет соответствовать всем 256 возможным типам ICMP-сообщений.	

Сервисы IP-протоколов, определенных пользователем	*Сервисы IP-протокола, функционирующие на уровне приложений и транспортном уровне, можно определить по номеру IP-протокола. IP-протокол может переносить данные различных протоколов, эти протоколы определяются уникальным номером IP-протокола, который указывается в соответствующем поле заголовка IP-пакета. Например, ICMP – 1, IGMP – 2, EGP – 8. Текущее соответствие номеров IP-протоколов публикуется организацией Internet Assigned Numbers Authority (IANA). В межсетевом экране сервису можно поставить в соответствие диапазон номеров IP-протоколов.*
Создадим сервис протокола GRE. Зайдите в меню *Objects→Services→Add→IP Protocol Service*. Во вкладке *General* введите следующие параметры*:*	
Name	GRE
IP Protocol	47
Pass returned ICMP error message from destination	Поставьте галочку для разрешения доставки сообщений ICMP об ошибках.
Группы сервисов	*Service Group (группы сервисов) – позволяют облегчить конфигурацию политик безопасности. Например, для Web-сервера удобно использовать одну группу для протоколов HTTP и HTTPS.*
Создадим Web-группу сервисов. Зайдите в меню *Objects→Services→Add→TCP/UDP Service.* Во вкладке *General* введите следующие параметры:	
Name	http
Type	TCP
Source	0-65535
Destination	80
Примечание: Если сервис с таким именем уже существует, то будет выдано сообщение об ошибке одинаковых имен (см. рисунок 7.1).	
Рисунок 7.1: Ошибка при попытке создания объектов межсетевого экрана с одинаковыми именами.	



Зайдите в меню *Objects→Services→Add→TCP/UDP Service*. Во вкладке *General* введите следующие параметры:

Name	https
Destination	443

Примечание: Если служба с таким именем уже существует, то будет выдано сообщение об ошибке одинаковых имен.

Зайдите в меню *Objects→Services→Add→Service Group*. Во вкладке *General* введите следующие параметры:

Name	Web
Selected	Переместите HTTP и HTTPS из списка Available.
Pass returned ICMP error messages from destination (см рисунок 7.1)	*Сообщения об ошибках ICMP позволяют диагностировать проблемы в сети, они генерируются узлом назначения. По умолчанию межсетевым экраном такие сообщения считаются новым соединением и отбрасываются, если нет соответствующего разрешающего правила. С точки зрения безопасности подобный механизм полезен – он позволяет избежать опасности многих сетевых атак и скрыть защищаемую сеть извне. Однако, для целей диагностики проблем в сети данная особенность работы устройства неудобна. Выходом из подобной ситуации является возможность конфигурации межсетевого экрана пропускать ICMP error message только при существующем соединении конкретной службы.*
SYN flood protection (SYN Relay) (см рисунок 7.1)	*SYN Relay позволяет защитить адреса назначения службы от атаки типа SYN-flooding. Атака SYN-flood запускается путем отправки запросов на TCP-соединение быстрее, чем узел назначения может их обработать. Злоумышленник шлет SYN-*

	запрос серверу с подмененым (spoofed) адресом источника, который никогда не ответит серверу запросом SYN/ACK. Каждый SYN-запрос добавляет новое TCP-соединение в серверную таблицу соединений; когда все соединения в таблице ожидают ответа и таблица заполнена, то сервер не ответит на любое новое соединение. Таким образом, запросы легитимных пользователей потом будут игнорироваться. *Механизм SYN Relay скрывает атакуемый сервер от хакера. Межсетевой экран получает SYN-запрос и от своего имени устанавливает соединение с удаленным инициатором TCP соединения, затем межсетевым экраном ожидается ответ источника SYN/ACK. Если после определенного времени ответ ACK не получен межсетевым экраном, то соединение разъединяется.*
Сертификат X.509	*Межсетевой экран поддерживает сертификаты международного стандарта ITU-TX.509. Данная технология задействована в процессах распределения ключей и идентификации объектов. Сертификат состоит из двух частей – public key и digital signature – публичный ключ и цифровая подпись. Публичный ключ определяет пользователя (имя, ID пользователя и т.д.), цифровая подпись показывает, что информация сертификата заверена центром сертификации (Certificate Authority). Вместе эта пара образует сертификат безопасности.* *Доверенный центр сертификации (CA) выпускает сертификаты для других пользователей. Валидная цифровая подпись сертификата гарантирует, что владельцу сертификата тоже можно доверять.* *CA может выпускать сертификаты для других CA, образуя таким образом деревоподобную иерархию сертификатов. Наивысший сертификат называется корневым (root certificate). В этой иерархии каждый сертификат подписан родительским, кроме корневого. Корневой сертификат подписывается самим собой.* *При проверке валидности сертификатов используется полный путь от сертификата пользователя до корневого сертификата.* *Если CA сертификат скомпрометирован, то все подписанные им сертификаты также становятся недоверенными.* *Сертификат имеет определенное время действия (validity time), по истечении которого он перестает действовать и необходим его перевыпуск.* *Для сертификатов, которые более не действуют, издаются специальные Certificate Revocation List (CRL). Это списки отозванных до окончания срока действия сертификатов. Причиной досрочного окончания срока действия является компрометация, лишение прав пользователю использовать этот сертификат (например, увольнение сотрудника), и др. CRL регулярно публикуются на сервере, к которому имеют доступ сертифицированные пользователи. Список можно скачать с помощью протоколов LDAP или HTTP.* *Обычно сертификат содержит поле CRL Distribution Point (CDP), которое определяет локацию, где можно скачать CRL. Если CDP нет в сертификате, то локацию можно определить вручную.*

	Интервал обновления информации в CRL зависит от настроек центра сертификации. Обычно этот интервал составляет от часа до нескольких дней. *Проверка сертификата состоит из следующих этапов:* *- восстановление пути к корневому сертификату,* *- проверка сигнатур всех сертификатов в сертификационном пути,* *- проверка отсутствия каждого из пути сертификатов в CRL.* *Сертификаты в межсетевом экране поддерживают функцию Identification Lists (ID-списки), которые определяют сертификаты для использования в IPSec.* *В межсетевой экран можно загрузить сертификаты двух типов – самоподписанные сертификаты и удаленные сертификаты, принадлежащие удаленному Peer- или CA-серверу.*
Добавим сертификат X.509. Зайдите в меню *Objects→Authentication Objects→Add→Certificate.* Введите следующие параметры*:*	
Name	my_cert
Options	Выберите одну из опций: - Upload self-signed X.509 Certificate - Upload a remote certificate.
Примечание: Сертификат должен быть создан с помощью программы генерации сертификатов (пример создания CA-сертификатов описан в приложении G) или сертификат загружается с удаленного сервера центра сертификации.	
Интерфейсы	*Interfaces (интерфейсы) – физические средства осуществления соединений. Они непосредственно обеспечивают прохождение трафика в/из сетей. Для контроля трафика во всех направлениях и защиты локальной сети применяют правила безопасности на всех интерфейсах.*
Ethernet	*Ethernet – одна из архитектур LAN, определяемая стандартом IEEE 802.3. Это на сегодня наиболее широко используемый стандарт. Фактически Ethernet-интерфейс представляет собой физический адаптер, используемый в межсетевом экране. Настройка Ethernet-интерфейса заключается в задании IP-адреса и других параметров, необходимых для настройки доступности интерфейса для сетевого уровня.* *При настройке межсетевого экрана все поддерживаемые Ethernet-адаптеры будут пронумерованы и сконфугурированы в процессе установки локальной консоли. Каждый физический Ethernet-адаптер станет Ethernet-интерфейсом и ему будет присвоено имя в конфигурации межсетевого экрана. Администраторы могут изменять описательное имя и IP-адреса интерфейса после первоначальной установки.* *Обычно настройка Ethernet-интерфейса заключается в присвоении ему имени и задания IP-адреса. IP-адрес интерфейса может быть использован для пингования межсетевого экрана, удаленного управления и задания адреса источника для динамически преобразуемых соединений (dynamically translated connections). Кроме того, IP-адрес может быть опубликован на интерфейсе с помощью ARP для симуляции эффекта интерфейса, имеющего более одного IP-адреса. IP-адрес может быть получен динамически при разрешении DHCP на интерфейсе. На основных интерфейсах межсетевого экрана может быть применена технология High Availability (HA). Эта технология позволяет выделить для двух интерфейсов один*

	общий IP-адрес при объединении нескольких межсетевых экранов в кластер. При этом каждый интерфейс имеет приватный IP-адрес, определяемый HA IP4 Address Pair в объекте Address Book. *При задействовании интерфейса в прозрачном режиме (transparent mode) межсетевой экран будет работать как коммутатор второго уровня и регистрировать трафик через интерфейс без модифицирования адресов назначения и отправления. Обе стороны коммутируемых хостов не будут ощущать присутствие межсетевого экрана.* *В межсетевом экране существует два специальных логических интерфейса* core *и* any. *Интерфейс* core *обозначает «сердце» межсетевого экрана, весь трафик с физических интерфейсов на интерфейс* core *будет контролироваться политиками безопасности. Интерфейс* any *представляет собой любой возможный интерфейс, в том числе и* core.
Настроим **lan-**интерфейс.Создайте сначала необходимые логические объекты.	
Создадим объект «IP-адрес». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Во вкладке *General* введите следующие параметры:	
Name	lan_ip
Address	192.168.0.1
Примечание: Если объект с таким именем уже существует, то будет выдано сообщение об ошибке одинаковых имен.	
ВНИМАНИЕ: При изменении IP-адреса LAN необходимо зайти на интерфейс DFL по новому IP-адресу в течение 30 секунд (период времени задан по умолчанию, его можно изменить в папке **System → Remote Management → Advanced Settings → Validation Timeout**). Иначе настройки LAN останутся прежними.	
Создадим объект «основной шлюз». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Во вкладке *General* введите следующие параметры:	
Name	lan_gate
Address	192.168.0.254
Создадим IP4 подсеть. Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Во вкладке *General* введите следующие параметры:	
Name	lannet
Address	192.168.0.0/24
Примечание: Если объект с таким именем уже существует, то будет выдано сообщение об ошибке одинаковых имен.	
Зайдите в меню *Objects→Interfaces→Ethernet.* Выберите **lan-**интерфейс. Во вкладке *General* введите следующие параметры:	
Name	lan (или измените на свое имя)
IP Address	Выберите lan_ip из списка.
Network	Выберите lannet из списка.
Default Gateway	Выберите lan_gate из списка.
Во вкладке *General* можно также выбрать опции разрешающие DHCP Client и Transparent Mode.	
Во вкладке *Hardware Settings* можно задать скорость сетевого адаптера. Media задает автовыбор скорости или статическую настройку скорости. Duplex задает автовыбор дуплексного режима или полный/полудуплекс (full и half duplex). Также можно указать MAC-адрес.	
Во вкладке *Advanced* можно задать свойства автоматического создания маршрута. Route Metric задает значение метрики, интерфейс при этом будет добавлен к главной таблице маршрутизации (Main Routing Table) в качестве информации о маршруте назначения. По умолчанию метрика равна 100.	

IP Rule	*Политики безопасности системы NetDefendOS настраиваются администратором для регулирования правил, в соответствии с которыми трафик может проходить через межсетевой экран NetDefend. Такие политики описываются содержанием различных наборов правил системы NetDefendOS. Набор правил связан с сервисами, определяющими тип трафика, к которым они будут применяться. Трафик, не соответствующий ни одному правилу в наборе IP-правил, отклоняется системой NetDefendOS по умолчанию.* *Правило состоит из двух частей: параметров фильтрации и действий, которые следует предпринимать после фильтрации. Как описано выше, к параметрам любого правила NetDefendOS, в том числе IP-правила, относятся:* *- Интерфейс источника (Source Interface)* *- Сеть источника (Source Network)* *- Интерфейс назначения (Destination Interface)* *- Сеть назначения (Destination Network)* *- Сервис (Service).* *Когда IP-правило активировано, может произойти одно из следующих действий (Action):* ***Allow.** Пакеты пропускаются дальше. Применяется к только что открытому соединению, в таблицу состояний производится запись о том, что соединение открыто. Остальные пакеты данного соединения будут подвергаться проверке «Stateful engine» системы NetDefendOS.* ***NAT** Подобно действию Allow, но с использованием динамической трансляции адресов.* ***Forward fast**. Пусть, например, пакет проходит через межсетевой экран NetDefend без записи его состояния в таблицу состояний. Это означает, что процесс stateful inspection не осуществляется, что менее безопасно, чем действия Allow или NAT.* ***SAT.** Уведомляет NetDefendOS о выполнении статического преобразования адреса. Действие SAT всегда требует получения разрешения о прохождении трафика от действий Allow, NAT или Forward fast.* ***Drop.** Уведомляет NetDefendOS о том, что пакет необходимо отклонить. Это более строгая версия действия Reject, так как при этом отправителю не посылается ответ. Очень часто данное действие предпочтительнее, так как потенциальные злоумышленники не знают о том, что случилось с их пакетом.* ***Reject.** Данное действие работает примерно так же, как и Drop, но при этом возвращается сообщение TCP RST или ICMP Unreachable, информирующее компьютер отправителя о том, что его пакет был отклонен. Данное действие является более «мягкой» формой действия Drop.* *Действие Reject полезно применять в приложениях, где исходящий трафик отклоняется только после наступления тайм-аута, если пришло уведомление об отказе, то трафик отклоняется, не дожидаясь тайм-аута.*
Создайте IP Rule для DNS-запросов. Во вкладке *General* введите:	
Name	DNS_from_LAN
Action	NAT

Service	dns-all
Source Interface	lan
Source Network	lannet
Destination Interface	any
Destination Network	all-nets
Создайте IP Rule для запрета протокола SMB (Server Messege Block) при выходе за межсетевой экран. Во вкладке *General* введите:	
Name	drop_smb-all
Action	drop
Service	smb-all
Source Interface	lan
Source Network	lannet
Destination Interface	wan1 (Интернет)
Destination Network	all-nets
Создайте IP Rule для запрета протокола ICMP для wan1_ip. Во вкладке *General* введите:	
Name	reject_icmp
Action	reject
Service	all-icmp
Source Interface	any
Source Network	all-nets
Destination Interface	wan1 (Интернет)
Destination Network	wan1_ip
Virtual LAN	*Технология VLAN позволяет управлять логической топологией сети поверх реальных физических соединений. Виртуальные подсети можно объединять в логические группы. Межсетевой экран полностью поддерживает спецификацию IEEE 802.1Q для VLAN, позволяя определять виртуальные интерфейсы поверх физических Ethernet-интерфейсов.* *Сети VLAN разделяют единый домен широковещательного трафика сети LAN на несколько виртуальных сетей, тем самым уменьшая обычно излишний трафик в сети и повышая защищенность сети.* *Технология VLAN по спецификации 802.1Q построена на использовании теггирования Ethernet-фреймов по принадлежности к определенной VLAN. Четырех битный тег содержит индикатор типа фрейма VLAN (VLAN frame type indicator - 0x8100), индикатор VLAN (VLAN identifier - VID), 3 бита приоритета и контрольную информацию. 12 бит VID позволяют задать 4096 VLAN-подсетей на основе физической сети. При этом VID со всеми нулями и всеми единицами не используются.* *Межсетевой экран обеспечивает 802.1Q посредством задания одного или более VLAN-интерфейсов с уникальным VID для каждого VLAN. При поступлении Ethernet-фреймов на межсетевой экран определяется соответствие VID и применяется соответствующее правило доставки пакетов. Технология VLAN может быть использована в межсетевых экранах для разделения трафика разных отделов организации или при необходимости увеличения количества логических*

	интерфейсов.
Создадим VLAN-интерфейс. Зайдите в меню *Interfaces→VLAN→Add→VLAN.* На вкладке *General* введите следующие параметры*:*	
Name	vlan01
Interface	Выберите интерфейс Ethernet.
VLAN ID	Выберите корректный VID (например, 1).
Примечание: Две VLAN-сети не могут иметь одинаковый VID, если они определенны на одном и том же Ethernet-интерфейсе.	
В разделе *Address Settings* введите следующие параметры*:*	
IP Address	Выберите IP-адрес, который должен быть использован VLAN-интерфейсом. Если значение не введено, то будет использован IP-адрес сетевого адаптера.
Network	Выберите сеть для VLAN-интерфейса.
Default Gateway	Выберите основной шлюз для VLAN-интерфейса.
DHCP	*Протокол DHCP является протоколом третьего поколения для стека TCP/IP, базируется непосредственно на BOOTP-протоколе. Позволяет автоматически присваивать сетевые настройки хостам в сети. Межсетевой экран поддерживает функции DHCP-клиента, DHCP-сервера и DHCP Relay. На интерфейсах межсетевого экрана можно включить эти функции.*
PPPoE	*Протокол PPPoE представляет собой объединение протоколов PPP и Ethernet. Позволяет авторизовать пользователей в сети Ethernet, которые выходят в Интернет через общий последовательный интерфейс (DSL-линия, кабельный модем или выделенная линия).* *На сегодня многие крупные провайдеры используют эту технологию для работы с пользователями.* *PPPoE при этом позволяет обеспечить безопасность и аутентификацию (привязать IP-адрес к конкретному пользователю), а также раздавать сетевые настройки пользователям автоматически (аналогично DHCP). IP-адресация может быть создана для групп пользователей.* *Протокол PPP – двухточечный протокол канального уровня (Data Link) сетевой модели OSI. Обычно используется для установления прямой связи между двумя узлами сети, причем он может обеспечить аутентификацию соединения, шифрование и сжатие данных. Используется на многих типах физических сетей: нуль-модемный кабель, телефонная линия, сотовая связь и т.д.* *PPP представляет собой целое семейство протоколов: протокол управления линией связи (LCP), протокол управления сетью (NCP), протоколы аутентификации (PAP, CHAP), многоканальный протокол PPP (MLPPP).* *На канальном уровне протокол определяет механизм инкапсуляции для поддержки мультипротокольных пакетов в IP-сети. LCP устанавливает, настраивает и проверяет соединение, затем используется NCP-протокол для передачи трафика, при этом разнородные по принципу построения передачи протоколы могут работать на одном установленном PPP-линке (например, IP и IPX).* *PPP поддерживает на сегодня следующие протоколы*

	аутентификации: *- PAP,* *- CHAP,* *- Microsoft CHAP version 1,* *- Microsoft CHAP version 2.* *При использовании аутентификации в протоколе одна из участвующих в передачи сторон обязательно должна быть идентифицирована перед тем, как будет использоваться NCP-протокол.* *Так как PPPoE работает на Ethernet-интерфейсе, то межсетевой экран должен использовать один из обычных Ethernet-интерфейсов для создания PPPoE-туннеля. Каждый PPPoE-туннель межсетевым экраном интерпретируется как логический интерфейс, имеющий такие же функции фильтрации, управления трафиком и возможности настройки, как у обычного аппаратного интерфейса. Сетевой трафик, приходящий из PPPoE-туннеля, будет отправляться для обработки набором правил межсетевого экрана.* *PPPoE использует автоматическое выделение IP-адресов, похожее на DHCP. Получая информацию об IP-адресе от ISP-провайдера, межсетевой экран сохраняет ее в сетевом объекте с символьным именем хоста/сети для установления PPP-соединения.* *Если ISP требует аутентификацию по логину и паролю, то в межсетевом экране можно задать логин и пароль для аутентификации на PPPoE-сервере.* *Опция Dial-on-demand позволяет отключать PPPoE-туннель при отсутвии активности за определенное время.*
Создадим PPPoE-клиента на **wan-**интерфейсе с маршрутизацией всего трафика через PPPoE-туннель. Зайдите в меню *Interfaces→PPPoE->Add->PPPoE Tunnel*. Введите следующие параметры:	
Name	PPPoE_Client
Physical Interface	wan1
Remote Network	0.0.0.0/0 (all-nets, т.к. выбираем маршрутизацию всего трафика)
Service Name	Введите данные ISP.
Username	Введите данные ISP.
Password	Введите данные ISP.
Confirm Password	Повторите пароль.
Во вкладке *Authentication* можно выбрать конкретные протоколы для аутентификации PPPoE-клиента.	
Во вкладке *Dial-on-demand* можно разрешить опцию Dial-on-demand.	
Во вкладке *Advanced* добавляются новые маршруты для этого интерфейса.	
Группа интерфейсов	*Интерфейсы различных типов можно объединить в группу для настройки общей политики.*
Создадим группуинтерфейсов. Зайдите в меню *Interfaces→Interface Groups →Add →Interface Group*. Введите следующие параметры*:*	
Name	testifgroup
Security/Transport Equivalent	disable
Interfaces	Введите lan, VLAN, Ethernet
Примечание: опция Security/TransportEquivalent позволяет задать группу интерфейсов в качестве интерфейса назначения в правилах, где соединения между интерфейсами могут	

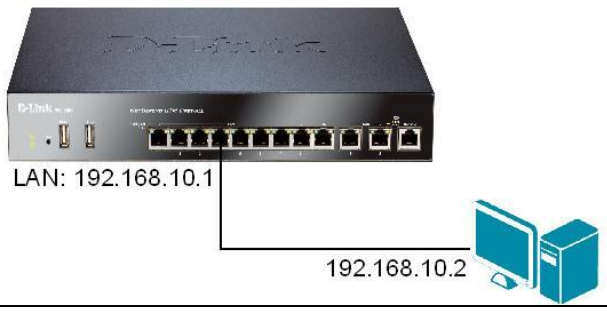
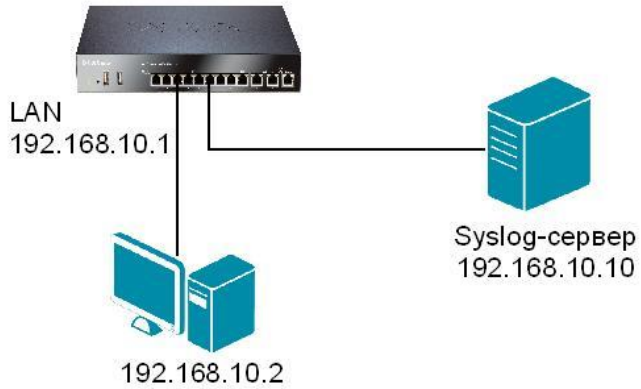
быть удаленными. Например, это необходимо при настройке Route Fail-Over и OSPF.	
ARP	*Протокол ARP ставит в соответствие адреса протоколов сетевого уровня (network layer) с аппаратными адресами уровня данных (data link layer). Например, ARP используется для разрешения IP-адреса в соответствующий MAC-адрес. Протокол работает на втором уровне модели OSI и инкапсулируется в Ethernet-заголовки для передачи.* *ARP используется для получения Ethernet-адреса хоста по его IP-адресу. Когда есть необходимость разрешить IP-адрес в Ethernet-адрес, выдается широковещательный ARP-запрос. Этот запрос содержит IP-адрес источника, MAC-адрес источника и IP-адрес назначения. Каждый хост в локальной сети получает это сообщение, хост с указанным IP-адресом назначения отправляет ARP ответное сообщение вызывающему хосту, содержащие свой MAC-адрес.* *Для задания статического сопоставления IP-адресов и аппаратных адресов (MAC-адресов) используется ARP-таблица.* *В межсетевом экране публикация IP-адреса с использованием ARP служит двум целям: помочь сетевому оборудованию отвечать на ARP-запросы в корректной форме и создать видимость наличия у интерфейса межсетевого экрана более одного IP-адреса.*
ARP-прокси	*Технология ARP Proxy позволяет «опубликовать» MAC-адрес на интерфейсе, чтобы при ARP-запросах он ставился в соответствии с указанным IP-адресом. Таким образом можно задать дополнительный IP-адрес на интерфейсе или, например, разделить сеть на две подсети, проходящие через межсетевой экран с помощью маршрутизации.*
Создадим ARP-таблицу. Зайдите в меню *Interfaces→ARP→Add→ARP*. Введите следующие параметры:	
Mode	Publish
Interface	Выберите интерфейс, который должен иметь дополнительный IP-адрес
IP Address	Введите дополнительный IP-адрес для выбранного интерфейса
MAC	00-00-00-00-00-00 (используется MAC-адрес интерфейса)

ЗАНЯТИЕ №3. Настройка Syslog-сервера. SNMP Trap.

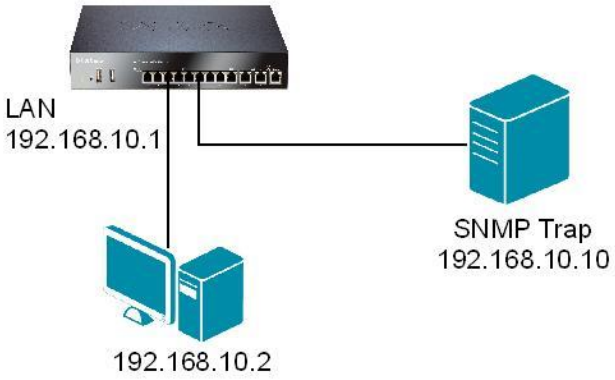
Возможность логировать и анализировать все системные события – очень важная функция межсетевого экрана. Логирование позволяет не только мониторить статус системы, но также проводить аудит использования сети и помогать в решении проблем.

Цель	Эта лабораторная работа предназначена для изучения настройки внешних и внутренних получателей (ресиверов) лог-сообщений межсетевого экрана.	
Оборудование	DFL-860E	1
	Рабочая станция	1
	Ethernet-кабель (патч-корд)	2
	Внешний Syslog-сервер	1
	SNMP trap ресивер	1

События и логирование	
Определение	*В межсетевых экранах определено большое количество различных лог-сообщений о событиях (log event messages), генерируемых в результате соответвующих системных событий. Например, установление или разрыв соединений, получение определенных пакетов, отбрасывание трафика в результате фильтрации политик межсетевого экрана.* *Каждое создаваемое сообщение может быть отфильтровано и передано на все сконфигурированные получатели (ресиверы) сообщений о событиях (Event Receivers). Каждый получатель может быть настроен на определенный фильтр событий.*
Типы лог-сообщений	*В операционной системе межсетевого экрана определено несколько сот событий, по которым могут быть сгенерированы лог-сообщения.* *Все сообщения имеют общий формат с атрибутами, включающими категорию, важность (severity) и рекомендуемые действия. Атрибуты позволяют легко отфильтровать все сообщения перед отправкой получателю сообщений (внешнему или внутреннему).* *Параметр SeverityFilter.* *Возможные значения параметра:* *- Emergency,* *- Alert,* *- Criticle,* *- Error,* *- Warning,* *- Notice,* *- Info,* *- Debug.* *По умолчанию ОС межсетевого экрана отсылает все сообщения уровня Info и выше на указанный лог-сервер. Категория Debug может быть включена в случае необходимости отладки.*
Создание лог-получателя (ресивера)	*Для распределения и логирования сообщений о событиях, генерируемых межсетевым экраном, необходимо определить один или более получателей и задать параметры: какое событие отслеживать и куда отсылать сообщения.*

	<u>Memory Log Receiver.</u> *Межсетевой экран имеет один встроенный механизм логгирования – MemLog. Он сохраняет все лог-сообщения в памяти и позволяет просматривать текущие сообщения через Web-интерфейс.* *MemLog можно запретить. Запись в MemLog ограничена доступной памятью в операционной системе межсетевого экрана, когда свободная память заканчивается новые сообщения будут записываться на место ранее записанных.* *<u>Syslog Receiver.</u>* *Syslog – стандарт логирования событий сетевых устройств. Хотя формат сообщений может зависить от настроек внешнего лог-сервера, обычно все сообщения имеют похожую структуру.* *Пример лог-сообщений:* *Feb 5 2010 10:45:12 firewall.mipk.ru EFW: DROP:* *Для автоматизации процесса обработки всех сообщений межсетевой экран записывает все лог-данные в одну текстовую строку. Формат записей: name=value. Поле Prio соответствует информации в Severity устройств D-Link.*
Схема 5	
<u>Упражнение</u>	Просмотрите лог-сообщения встроенного лог-ресивера межсетевого экрана.
<u>Web-интерфейс</u>	Зайдите в меню *Status→Logging*. Просмотрите сообщения.
Настройка внешнего лог-сервера.	
Схема 6	
<u>Настройка DFL-860E</u>	
<u>Web-интерфейс</u>	
Создадим объект «IP-адрес syslog-сервера». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. *Во* вкладке *General* введите следующие параметры:	

Name	ip-syslog
IPAddress	192.168.10.10
Настроим на межсетевом экране внешний лог-сервер. Зайдите в меню *System→Log and Event Receivers→Add→Syslog Receiver*. Введите следующие параметры:	
Name	my_syslog
IP Address	ip-syslog
Facility	Выберите необходимые события для логирования.
Примечание: лог-сервер должен быть настроен на получение сообщений от межсетевого экрана. Например, можно использовать условно-бесплатный лог-сервер Kiwi Syslog Server.	
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add Address IP4Address ip-syslog Address=192.168.10.10 gw-world:/labs> cc gw-world:/> add LogReceiver LogReceiverSyslog my_syslog IPAddress=labs/ip-syslog gw-world:/> activate (*подождать 3-5 секунд*) gw-world:/>commit	
Упражнение	Проверьте работоспособность syslog-сервера, откройте лог на syslog-сервере (IP-адрес – 192.168.10.10), посмотрите лог-записи.
Устранение возможных проблем	Если лог-сообщения не поступают на внешний syslog-сервер, решите возникшую проблему с помощью описанных ниже диагностических средств.
Проверьте корректность физических подключений устройства, работоспособность патч-кордов, индикацию на устройстве. Проверьте корректность настроек syslog-сервера.	
Зайдите в меню *Status→Logging* и просмотрите лог-сообщения встроенного syslog-сервера.	
Зайдите в меню *Tools→Ping*, проверьте доступность адреса ip-syslog.	
SNMP Traps	
Определение	*Протокол SNMP обеспечивает связь между системой управления сети Network Management system (NMS) и управляемым устройством. Протоколом SNMP определены три типа сообщений: команда Readom NMS для проверки управляемого устройства, команда Write для изменения состояния управляемого устройства и Trap, используемая управляемыми устройствами для отправки сообщений NMS об изменении состояния.* *В межсетевом экране концепция SNMP Trap исполняется в виде возможности отправки любого сообщения о событии в виде SNMP Trap. Таким образом администратор может задать отправку сообщений SNMP Trap, которые считаются важными при функционировании сети. Поддерживается стандарт SNMPv.2c, определенный в RFC1901, RFC1905, RFC1906.* *Для описания SNMP Trap определен файл DFLNNN-TRAP.MIB (NNN – номер модели межсетевого экрана, например DFL-860E), в нем задается SNMP-объект и типы данных. Для каждой модели межсетевого экрана используется свой файл, существует один общий trap-объект – DLNNNosGenericTrap (NNN–номер модели межсетевого экрана), который включает следующие параметры:* *- System. Система, создавшая trap.* *- Severity. Важность сообщения.* *- Category. Подсистема операционной системы межсетевого*

	экрана, сообщающая о проблеме. *- ID. Уникальный идентификатор в пределах категории.* *- Description. Короткое текстовое пояснение.* *- Action. Действие, предпринятое ОС межсетевого экрана.* *Администратором могут быть заданы дополнительные опции логирования:* *Send Limit.* *Этот параметр ограничивает число отправляемых лог-пакетов в секунду. Значение по умолчанию – 3600.* *Alarm Repetition Interval.* *Задержка в секундах между предупреждениями. Минимум – 0, максимум – 10000, значение по умолчанию – 60.*
Схема 7	

Настройка DFL-860E

Web-интерфейс

Создадим объект «IP-адрес snmp-trap». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Во вкладке *General* введите следующие параметры:

Name	ip-snmp
IPAddress	192.168.10.10

Настроим отправку сообщений SNMP Trap на получатель SNMP Trap. Зайдите в меню *System→Log and Event Receivers→Add→SNMP2c Event Receiver*. Во вкладке *General* введите следующие параметры:

Name	my_snmp
IPAddress	ip-snmp
SNMP Community String	Введите строку, если этого требует получатель trap-сообщений.

Зайдите в меню *Configuration* и выберите *Save and Activate*.

Командная строка (CLI)

```
gw-world:/> add Address AddressFolder labs
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add Address IP4Address ip-snmp Address=192.168.10.10
gw-world:/labs> cc
gw-world:/>add LogReceiver EventReceiverSNMP2c my_snmp IPAddress=labs/ip-snmp Community=private
gw-world:/> activate (подождать 3-5 секунд)
gw-world:/>commit
```

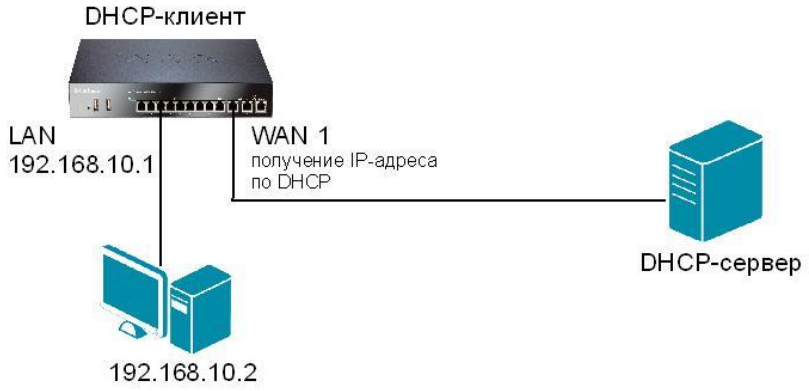
Упражнение	Проверьте работоспособность SNMP Trap, откройте его на компьютере-получателе (IP-адрес – 192.168.10.10), посмотрите записи о межсетевом экране.

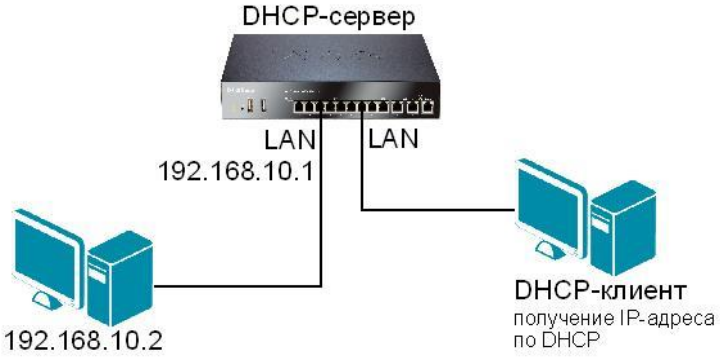
Устранение возможных проблем	Если лог-сообщения не поступают на SNMP Trap, решите возникшую проблему с помощью описанных ниже диагностических средств.
Проверьте корректность физических подключений устройства, работоспособность патч-кордов, индикацию на устройстве. Проверьте корректность настроек SNMP Trap.	
Зайдите в меню *Status→Logging* и просмотрите лог-сообщения встроенного syslog-сервера.	
Зайдите в меню *Tools→Ping*, проверьте доступность адреса ip-snmp.	

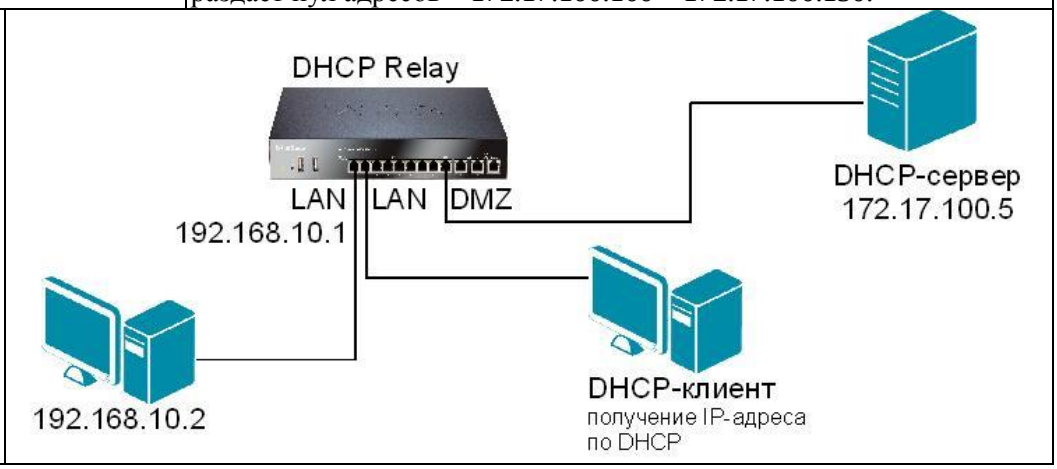
ЗАНЯТИЕ №4. DHCP-клиент, DHCP-сервер, DHCP Relay, IP Pool.

Межсетевой экран поддерживает различные функции протокола DHCP. На интерфейсах можно настроить функции DHCP-клиент, DHCP-сервер и DHCP Relay.

Цель	Эта лабораторная работа предназначена для изучения настройки функций DHCP на межсетевом экране.	
Оборудование	DFL-860E	1
	Рабочая станция	2
	DHCP-сервер	1
	Ethernet-кабель (патч-корд)	3

DHCP-клиент	
Определение	*DHCP-клиент рассылает широковещательные сообщения для нахождения DHCP-сервера (или DHCP-серверов) и получает для своего физического интерфейса IP-адрес динамически от DHCP-сервера. DHCP-клиент может получить предложения от нескольких DHCP-серверов и обычно применяет настройки от первого полученного предложения. DHCP-клиент может обновить или освободить IP-адрес в течении срока аренды.*
Схема 8	
Настройка DFL-860E	
Web-интерфейс	
Настроим межсетевой экран в качестве DHCP-клиента. Зайдите в меню *Interfaces→Ethernet*. Выберите интерфейс, на котором задается DHCP-клиент (wan1). Во вкладке *General* введите следующие параметры:	
Name	wan1
Enable DHCP Client	Поставьте галочку
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/>set Interface Ethernet wan1 DHCPEnabled=Yes gw-world:/> activate (*подождать 3-5 секунд*) gw-world:/>commit	
Упражнение	Проверьте сетевые настройки **wan1**-интерфейса. Зайдите в меню *Status→Interfaces→wan1*.

DHCP-сервер	
Определение	*DHCP-сервер межсетевого экрана позволяет раздавать настройки хостам автоматически из заданного пула адресов. Получая запрос от DHCP-клиента, DHCP-сервер высылает ответ с параметрами конфигурации (IP-адрес, маску подсети, IP-адрес шлюза, DNS-адреса, срок аренды IP-адреса). Хост может обновить (renew) или освободить (release) арендованный IP-адрес.*
Схема 9	
Настройка DFL-860E	
Web-интерфейс	
Создадим объект «пул IP-адресов». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Во вкладке *General* введите следующие параметры:	
Name	ip-pool
IPAddress	192.168.10.11-192.168.10.20
Настроим межсетевой экран в качестве DHCP-сервера для внутреннего интерфейса **lan**. Зайдите в меню *System→DHCP→DHCP Servers→Add→DHCP Server*. Во вкладке *General* введите следующие параметры*:*	
Name	dhcp_server_lan
Interface Filter	lan
Relay Filter	0.0.0.0/0
IPAddress Pool	ip-pool
Netmask	255.255.255.0
Во вкладке *Options* введите следующие параметры*:*	
Default GW	Выбрать из списка lan_ip
Domain	- (оставить поле пустым)
Lease Time	86400
DNS	- (оставить поле пустым)
NBNS/WINS	- (оставить поле пустым)
Next Server	- (следующий сервер в загрузочном процессе, обычно TFTP-сервер)
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address ip-pool Address=192.168.10.11-192.168.10.20 gw-world:/labs> cc gw-world:/> add DHCPServer dhcpserver_lan Interface=lan	

IPAddressPool=ip-pool Netmask=255.255.255.0 gw-world:/> activate (*подождать 3-5 секунд*) gw-world:/>commit	
Упражнение	Получите сетевые настройки автоматически на компьютере, подключенном к **lan**-интерфейсу межсетевого экрана. Проверьте сетевые настройки с помощью командной строки CMD на компьютере из **lan**-сети. Проверьте статус DHCP-сервера на устройстве.
Командная строка CMD ОС Windows	C:\>ipconfig /all
SSH CLI (Console CLI)	gw-world:/> dhcpserver gw-world:/> dhcpserver -show gw-world:/> dhcpserver -show -mappings
Устранение возможных проблем	Если клиенты **lan**-сети не получают сетевые настройки от DHCP-сервера межсетевого экрана, решите возникшую проблему с помощью описанных ниже диагностических средств.
Проверьте корректность физических подключений устройства, работоспособность патч-кордов, индикацию на устройстве. Проверьте корректность настроек клиента.	
Зайдите в меню *Status→Logging* и просмотрите лог-сообщения встроенного syslog-сервера.	
DHCP Relay	
Определение	*Исполнение протокола DHCP предполагает, что DHCP-клиент и DHCP-сервер находятся физически в одной локальной сети, т.к. клиенты посылают широковещательные запросы. В крупных распределенных сетях это приводит к необходимости иметь несколько DHCP-серверов в каждой подсети, что не всегда эффективно. Желательно иметь централизованную серверную конфигурацию. Для решения этой проблемы используется технология DHCP Relay. Устройство для DHCP Relay служит средством связи между удаленным DHCP-сервером во внешней сети и DHCP-клиентами. DHCP Relayer перехватывает запросы от клиентов и перенаправляет их к DHCP-серверу, который отвечает устройству, выступающему в качестве DHCP Relay, и который в свою очередь перенаправляет ответ клиенту. DHCP Relay обычно называют BOOTP relay agent, т.к. он выполняет его функциональность и поддерживает формат протокола BOOTP.*
Описание сценария	Настроим DHCP Relay для клиентов **lan**-сети, чтобы они могли получать IP-адреса от DHCP-сервера, подключенному к **dmz**-интерфейсу. IP-адрес DHCP-сервера в **dmz** – 172.17.100.5, сервер раздает пул адресов – 172.17.100.100 – 172.17.100.150.
Схема 10	

Настройка DFL-860E	
Web-интерфейс	
Создадим объект «IP-адрес DHCP-сервера». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Во вкладке *General* введите следующие параметры:	
Name	ip-dhcp
Address	172.17.100.5
Создадим DHCP Relay. Зайдите в меню *System→DHCP→DHCP Relays→Add→DHCP Relay*. Во вкладке *General* введите следующие параметры:	
Name	my_dhcp_relay
Action	Relay
Source Interface	lan
DHCP Server to relay to:	ip-dhcp
Allowed IP offers from server	all-nets
Во вкладке *Options* введите следующие параметры:	
The relayer uses the ip of the interface which it uses to send the request to the server.	Выберите эту опцию.
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address ip-dhcp Address=172.17.100.5 gw-world:/labs> cc gw-world:/> add DHCPRelay my_dhcp_relay Action=Relay TargetDHCPServer=labs/ip-dhcp SourceInterface=lan AddRoute=Yes ProxyARPInterfaces=lan gw-world:/> activate (*подождать 3-5 секунд*) gw-world:/>commit	
Упражнение	Получите сетевые настройки автоматически на компьютере, подключенном к **lan-**интерфейсу межсетевого экрана. Проверьте сетевые настройки с помощью CMD на компьютере из **lan-**сети. Просмотрите полученные IP-адреса с помощью CLI.
CMD OC Windows	C:\>ipconfig /all
Устранение возможных проблем	Если клиенты **lan-**сети не получают сетевые настройки от DHCP-сервера, решите возникшую проблему с помощью описанных ниже диагностических средств.
Проверьте корректность физических подключений устройства, работоспособность патч-кордов, индикацию на устройстве. Проверьте корректность настроек клиента.	
Зайдите в меню *Status→Logging* и просмотрите лог-сообщения встроенного syslog-сервера.	
IP Pool	
Описание IP Pool	Настройки IP Pool используются для разрешения другим подсистемам доступа к списку IP-адресов DHCP-сервера. Межсетевой экран получает этот диапазон IP-адресов в аренду, затем он может самостоятельно от своего имени раздавать IP-адреса для клиентов, в том числе для IP Pool в режиме шифрования

	IKE Config Mode. Возможно задать множественный IP Pool для группы DHCP-серверов.
Описание сценария	Настроим IP Pool для DHCP-сервера, подключенного к **dmz**-интерфейсу для получения 10 IP-адресов от DHCP-сервера.
Настройка DFL-860E	
Web-интерфейс	
Создадим объект «IP-адрес DHCP-сервера». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Во вкладке *General* введите следующие параметры:	
Name	ippool_dhcp
Address	172.17.100.10
Создадим IP Pool. Зайдите в меню *Objects→IP Pools→Add→IP Pool*. Во вкладке *General* введите следующие параметры:	
Name	my_ip_pool
Specify DHCP Server Address	Переместите из списка *Available* в список *Selected* ippool_dhcp
Server Filter	all-nets
Client IP Filter	all-nets
Во вкладке *Advanced* введите следующие параметры:	
Routing Table	main
Receive Interface	dmz
Prefetch Leases	10
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address ippool_dhcp Address=172.17.100.10 gw-world:/labs> cc gw-world:/> add IPPool my_ip_pool DHCPServerType=ServerIP ServerIP=labs/ippool_dhcp PrefetchLeases=10 gw-world:/> activate (*подождать 3-5 секунд*) gw-world:/>commit	
Упражнение	Просмотрите полученные IP-адреса с помощью командной строки (CLI).
SSH CLI (Console CLI)	gw-world:/>ippool –show
Устранение возможных проблем	Если IP-адреса не раздаются в IP Pool от DHCP-сервера, решите возникшую проблему с помощью описанных ниже диагностических средств.
Проверьте корректность физических подключений устройства, работоспособность патч-кордов, индикацию на устройстве. Проверьте корректность настроек DHCP-сервера.	
Зайдите в меню *Status→Logging* и просмотрите лог-сообщения встроенного syslog-сервера.	
Зайдите в меню *Tools→Ping*, проверьте доступность DHCP-сервера.	
Зайдите в меню *Status→Routes*, проверьте наличие корректного маршрута к DHCP-серверу.	

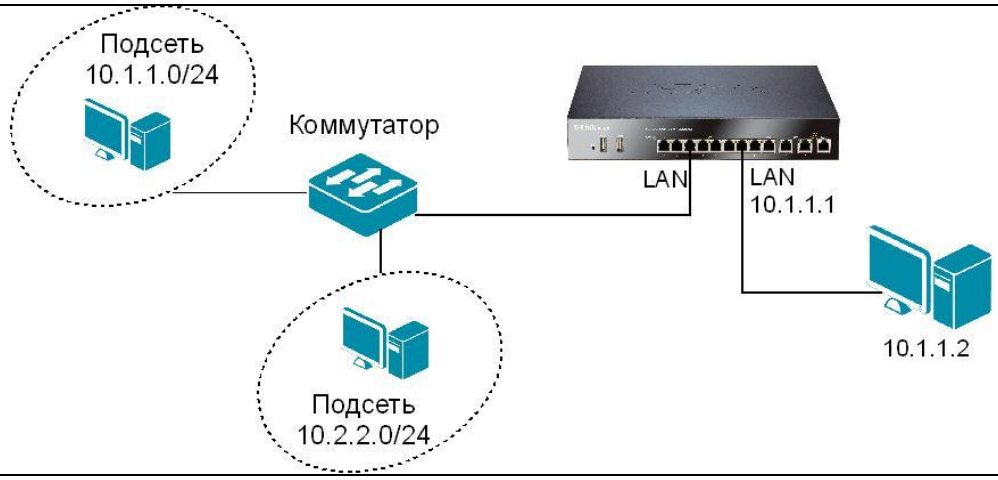
ЗАНЯТИЕ №5. Настройка доступа в Интернет и маршрутизации. Способы подключения к Интернет-провайдеру с использованием межсетевого экрана.

Межсетевой экран является маршрутизатором третьего уровня, позволяя маршрутизировать трафик между своими интерфейсами (как физическими так и логическими). Для настройки доступа в Интернет пользователей, находящихся за межсетевым экраном, необходимо настроить маршрутизацию и разрешающие трафик IP Rule. На интерфейсах **wan** можно настроить различные виды Интернет-подключения (статические адреса, DHCP-клиент, PPPoE, PPTP, L2TP).

Цель	Эта лабораторная работа предназначена для изучения настройки Интернет-соединения и основ маршрутизации на межсетевом экране.	
Оборудование	DFL-860E	1
	Рабочая станция	2
	Ethernet-кабель (патч-корд)	2
	Коммутатор	1
	Маршрутизатор	1

Настройка DFL-860E	
Настройка Интернет-соединения на межсетевом экране.	
Настройки по умолчанию	*Для наличия доступа в Интернет-сеть пользователей, находящихся за межсетевым экраном (т.е. во внутренней сети), необходима настройка двух обязательных параметров – маршрута к провайдеру Интернета и правил IP Rule, разрешающих соответствующий тип трафика пользователей в сторону Интернета и обратно. По умолчанию для пользователей в сети **lan (lan1**, **lan2**, **lan3** в DFL-1660/2560) доступ в Интернет предоставлен через интерфейс wan1 с помощью технологии NAT. Авторизация осуществляется только в соответствии с правилами IP Rule, разрешающими доступ в Интернет компьютеров, подключенных к внутренней сети и имеюших IP-адреса в пределах **lannet**-подсетей.* *Таким образом есть предопределенные маршруты и правила IP Rule, рассмотренные далее.*
Маршрут в Интернет по умолчанию.	
Interface	wan1
Network	all-nets
Правила IP Rule по умолчанию для доступа пользователей из lan (lan1, lan2, lan3) в Интернет.	
Name	allow_standart
Action	NAT
Service	all_tcpudp
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets

Основные понятия маршрутизации на межсетевом экране.	
Основы маршрутизации на межсетевом экране	*На межсетевых экранах D-Link серии DFL существует возможность создать статические и динамические маршруты. Статические маршруты добавляются в главную таблицу маршрутизации (main routing table) вручную администратором или автоматически при добавлении логических объектов-интерфейсов, со включенным параметром автоматического добавления маршрута.* *Динамические маршруты могут быть добавлены в таблицу маршрутизации протоколом динамической маршрутизации OSPF.*
Статические маршруты	*Статический маршрут состоит из следующих компонентов:* *- Интерфейс (Interface).* *Интерфейс, на который должны перенаправляться пакеты для того, чтобы достичь сеть назначения. Фактически этот интерфейс напрямую или через маршрутизатор подключен к данной сети назначения.* *- Сеть (Network).* *Это сеть (или подсеть) назначения – диапазон IP-адресов. В таблице маршрутизации поиск маршрута осуществляется по данному параметру. При наличии одинаковых маршрутов, но с разными подсетями выбирается маршрут с более меньшей метрикой в таблице маршрутизации* *- Шлюз (Gateway).* *Это IP-адрес шлюза, являющимся следующим маршрутизатором по пути к сети назначения. Если сеть назначения подключена напрямую к интерфейсу межсетевого экрана, то данный параметр не нужно задавать.* *- Локальный IP-адрес (Local IP address).* *Обычно данный параметр указывать не нужно. Если он задан, то межсетевой экран будет отвечать на ARP-запросы к этому IP-адресу.* *- Метрика (Metric).* *Значение метрики для маршрута – это вес маршрута при сравнении между альтернативными маршрутами. При наличии одинаковых маршрутов будет выбран маршрут с меньшей метрикой.* *Метрика также используется для настройки Route Failover и Route Load Balancing.*
Маршрут к all-nets	*Межсетевой экран имеет встроенный объект all-nets (0.0.0.0/0), означающий все возможные сети.*
Использование параметра Local IP address.	
Описание сценария	*Подсеть 10.1.1.0/24 подключена к физическому интерфейсу **lan** межсетевого экрана, имеющему IP-адрес 10.1.1.1. Подсеть 10.2.2.0/24 подключена к межсетевому экрану через коммутатор (схема 11). Необходимо обеспечить маршрутизацию к сети 10.2.2.0/24. При обращении в другую подсеть запросы проходят через межсетевой экран.*

Схема 11	

Настройка DFL-860E

Web-интерфейс

Создание необходимых объектов
Подразумевается, что управляющий компьютер также находится в подсети 10.1.1.0/24

Создадим IPv4-подсеть 10.1.1.0/24. Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Во вкладке *General* введите следующие параметры:

Name	net1
Address	10.1.1.0/24

Создадим IPv4-подсеть 10.2.2.0/24. Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Во вкладке *General* введите следующие параметры:

Name	net2
Address	10.2.2.0/24

Создадим IPv4-адрес 10.2.2.1. Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Во вкладке *General* введите следующие параметры*:*

Name	local_ip_addr
Address	10.2.2.1

Создадим маршрут к сети 10.1.1.0/24. Зайдите в меню *Routing→Routing Tables→main→Add→ Route.* Добавьте маршрут:

Interface	lan
Network	net1

Создадим маршрут к сети 10.2.2.0/24. Зайдите в меню *Routing→Routing Tables→main→Add→ Route.* Добавьте маршрут:

Interface	lan
Network	net2
Local IP address	local_ip_addr

Зайдите в меню *Configuration* и выберите *Save and Activate.*

Командная строка (CLI)

```
gw-world:/> add Address AddressFolder labs
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address net1 Address=10.1.1.0/24
gw-world:/labs> add IP4Address net2 Address=10.2.2.0/24
gw-world:/labs> add IP4Address local_ip_addr Address=10.2.2.1
gw-world:/labs> cc
gw-world:/> cc RoutingTable main
```

gw-world:/main>add Route Interface=lan Network=labs/net1
gw-world:/main>add Route Interface=lan Network=labs/net2 LocalIP=labs/local_ip_addr
gw-world:/main> cc
gw-world:/> activate (*подождать 3-5 секунд*)
gw-world:/>commit

Настройка сетевого подключения Windows XP/Vista/7 для хостов в сети 10.2.2.0/24

1) Зайдите в свойства подключения по локальной сети.
2) Откройте Протокол интернета (TCP/IP).
3) Убедитесь, что в качестве основного шлюза стоит IP-адрес 10.2.2.1.

Упражнение	Проверьте правильность маршрутизации к сети 10.2.2.0/24. Запустите трассировку с компьютера, находящегося в этой подсети.
CMD ОС Windows	C:\>tracert 10.1.1.1
Устранение возможных проблем	Если маршрутизация не работает должным образом, решите возникшую проблему с помощью описанных ниже диагностических средств.

Проверьте корректность физических подключений устройства, работоспособность патч-кордов, индикацию на устройстве. Проверьте корректность сетевых настроек компьютера, с которого проводится проверка схемы.

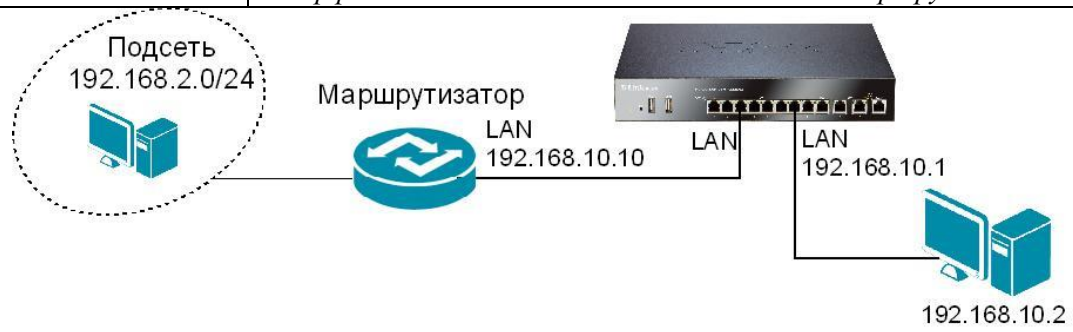
Зайдите в меню *Status→Logging* и просмотрите лог-сообщения встроенного syslog-сервера.

Зайдите в *Status→Routes*, проверьте наличие созданного маршрута.

Настройка статической маршрутизации (Static Routing)

Описание сценария	*В этом сценарии подсеть 192.168.2.0/24 задана как маршрутизируемая через маршрутизатор 192.168.10.10 локальной сети. Для связи межсетевого экрана через* ***lan****-интерфейс должен быть создан статический маршрут.*

Схема 12



Настройка DFL-860E

Web-интерфейс

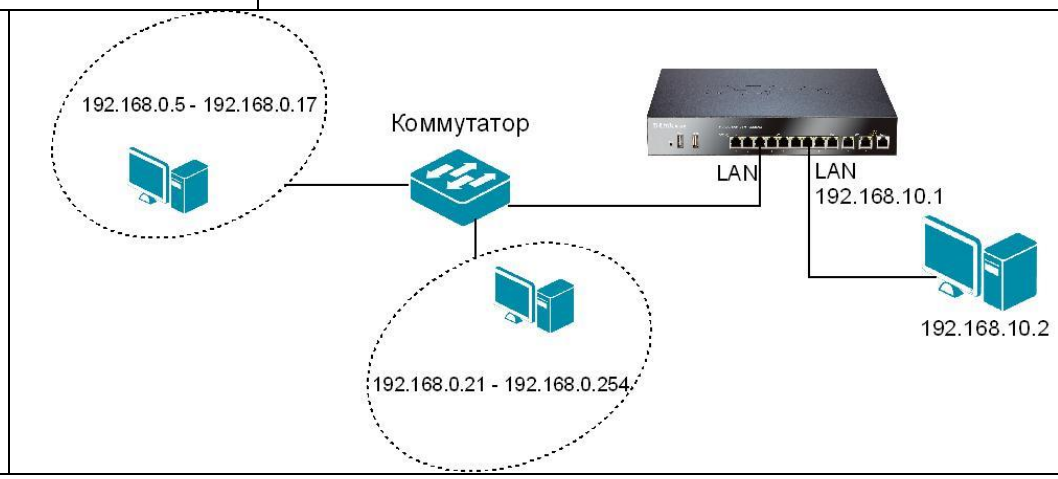
Создадим объект «подсеть 192.168.2.0/24». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:

Name	our_net
Address	192.168.2.0/24

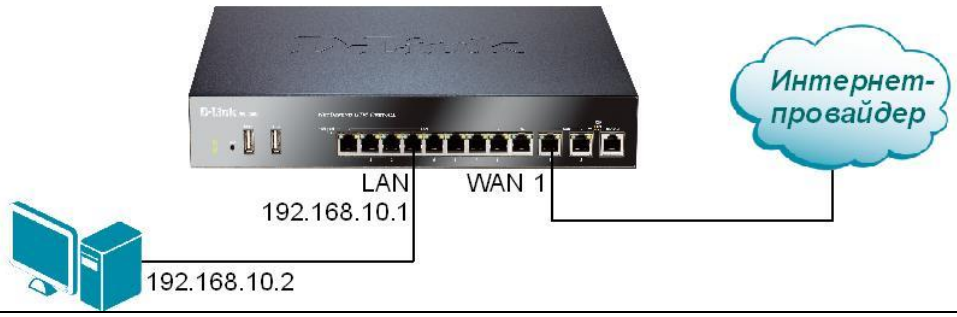
Создадим объект «IP-адрес маршрутизатора». Зайдите в меню *Objects→Address Book→Add→ IP4 Address*. Введите следующие параметры:

Name	router_ip
Address	192.168.10.10

Добавим статический маршрут для маршрутизации трафика из подсети 192.168.2.0/24 через маршрутизатор 192.168.10.10. Зайдите в меню *Routing→ Routing Tables→ main→Add→Route.* Во

вкладке *General* введите:	
Interface	lan
Network	our_net
Gateway	router_ip
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Примечание: После вышеуказанной настройки межсетевого экрана обратный трафик от маршрутизатора будет маршрутизироваться непосредственно через локальную сеть со стандартным набором правил Allow. При этом IP Rule должны быть заданы как «NAT» для трафика данной подсети или Forward fast (обработка без оценки состояния соединения).	
Командная строка (CLI)	
gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address our_net Address=192.168.2.0/24 gw-world:/labs> add IP4Address router_ipAddress=192.168.10.10 gw-world:/labs> cc gw-world:/> cc RoutingTable main gw-world:/main> add Route Interface=lan Network=labs/our_net Gateway=labs/router_ip gw-world:/main> cc gw-world:/> activate (*подождать 3-5 секунд*) gw-world:/>commit	
Упражнение	Проверьте правильность маршрутизации.
CMD OC Windows	C:\>tracert 192.168.2.10 (компьютер с таким IP-адресом должен быть в подсети 192.168.2.0/24)
Устранение возможных проблем	Если маршрутизация не работает должным образом, решите возникшую проблему с помощью описанных ниже диагностических средств.
Проверьте корректность физических подключений устройства, работоспособность патч-кордов, индикацию на устройстве. Проверьте корректность сетевых настроек компьютера, с которого проводится проверка схемы.	
Зайдите в меню *Status→Logging* и просмотрите лог-сообщения встроенного syslog-сервера.	
Зайдите в меню *Status→Routes*, проверьте наличие созданного маршрута.	
Настройка маршрутизации сложных сетей	
Описание сценария	*В этом сценарии необходимо настроить отдельные маршруты для диапазона IP-адресов 192.168.0.5-192.168.0.17 и другой маршрут для диапазона 192.168.0.21-192.168.0.254.*
Схема 13	
Настройка DFL-860E	

Web-интерфейс	
Создадим пул адресов. Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Во вкладке *General* введите следующие параметры:	
Name	ip_pool1
IP Address	192.168.0.5-192.168.0.17
Создадим второй пул адресов. Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Во вкладке *General* введите следующие параметры:	
Name	ip_pool2
IP Address	192.168.0.21-192.168.0.254
Добавим статический маршрут. Зайдите в меню *Routing→ Routing Tables→main→ Add→Route.* Во вкладке *General* введите:	
Interface	lan
Network	Выберите ip_pool1
Gateway	-
Добавим статический маршрут. Зайдите в меню *Routing→Routing Tables→main→Add→Route.* Во вкладке *General* введите:	
Interface	lan
Network	Выберите ip_pool2
Gateway	-
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address ip_pool1Address=192.168.0.5-192.168.0.17 gw-world:/labs> add IP4Address ip_pool2Address=192.168.0.21-192.168.0.254 gw-world:/labs> cc gw-world:/> cc RoutingTable main gw-world:/main> add Route Interface=lan Network=labs/ip_pool1 gw-world:/main> add Route Interface=lan Network=labs/ip_pool2 gw-world:/main> cc gw-world:/> activate (*подождать 3-5 секунд*) gw-world:/>commit	
Упражнение	Проверьте маршрутизацию.
CM DOC Windows	C:\>tracert 192.168.0.6 C:\>tracert 192.168.0.100
Устранение возможных проблем	Если маршрутизация не работает должным образом, решите возникшую проблему с помощью описанных ниже диагностических средств.
Проверьте корректность физических подключений устройства, работоспособность патч-кордов, индикацию на устройстве. Проверьте корректность сетевых настроек компьютера, с которого проводится проверка схемы.	
Зайдите в меню *Status→Logging* и просмотрите лог-сообщения встроенного syslog-сервера.	
Зайдите в меню *Status→Routes*, проверьте наличие созданных маршрутов.	
Способы подключения к Интернет-провайдеру (ISP) с использованием межсетевого экрана.	
Настройки wan-интерфейса	*Установка Интернет-соединения на межсетевом экране заключается в настройке сетевых параметров интерфейсов* ***wan***.

	Необходимые настройки предоставляет Интернет-провайдер. Возможные варианты настроек: статические адреса, DHCP-клиент, L2TP/PPTP-клиент, PPoE-клиент.
Схема 14	
Настройка DFL-860EG	
Статические настройки *wan*-интерфейса.	
Web-интерфейс	
Зайдите в меню *Interfaces→Ethernet→wan1*. Выберите следующие параметры:	
Enable DHCP Client	Снять галочку
IP address	wan1_ip
Network	wan1net
Default Gateway	wan1_gw
Зайдите в меню *Objects→Address Book→InterfaceAddresses→wan1_ip*. Введите следующие параметры:	
Address	10.95.5.100
Зайдите в меню *Objects→Address Book→InterfaceAddresses→wan1_net*. Введите следующие параметры:	
Network	10.95.5.0/24
Зайдите в меню *Objects→Address Book→InterfaceAddresses→wan1_gw*. Введите следующие параметры:	
Default Gateway	10.95.5.254
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/>set Interface Ethernet wan1 DHCPEnabled=No gw-world:/>set IP4Address InterfaceAddresses/wan1_ip Address=10.95.5.100 gw-world:/>set IP4Address InterfaceAddresses/wan1net Address=10.95.5.0/24 gw-world:/>set IP4Address InterfaceAddresses/wan1_gw Address=10.95.5.254 gw-world:/> activate (*подождать 3-5 секунд*) gw-world:/>commit	
Динамические настройки wan-интерфейса.	
Web-интерфейс	
Зайдите в *Interfaces→Ethernet→wan1*. Введите следующие параметры*:*	
Enable DHCP Client	Поставьте галочку
Зайдите в *Configuration* и выберите *Save and Activate*.	
Кломандная строка (CLI)	

gw-world:/> set Interface Ethernet wan1 DHCPEnabled=Yes
gw-world:/> activate (*подождать 3-5 секунд*)
gw-world:/>commit

L2TP/PPTP-клиент в настройках wan-интерфейса (на примере провайдера Билайн).

Настройка DFL-860E

Web-интерфейс

Создание необходимых объектов

Создадим IPv4-подсеть. Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Во вкладке *General* введите следующие параметры:

Name	l2tp_network
Address	85.21.0.0/24

Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Во вкладке *General* введите следующие параметры:

Name	tp_beeline_ru
Address	85.21.0.251

Зайдите в меню *Interfaces→Ethernet→wan1*. Введите следующие параметры:

Enable DHCP Client	Поставьте галочку

Зайдите в *Interfaces→PPTP/L2TP Clients→Add→PPTP/L2TP Client.* Во вкладке *General* введите следующие параметры:

Name	Internet
Tunnel Protocol	L2TP
Remote Endpoint	dns:tp.internet.beeline.ru
Remote Network	all-nets
Username	Mstu (введите логин, предоставленный провайдером)
Password	P@ssw0rd (введите пароль, предоставленный провайдером)
Confirm Password	P@ssw0rd (подтвердите пароль)

Изменение IP Rule

Зайдите в меню *Rules→IP Rules→lan_to_wan1*. Измените *Destination Interface* для всех правил в этой папке с *wan1*на ранее созданный *Internet*.

Маршрут для L2TP-соединения

Зайдите в меню *Routing→Routing Tables→main→Add→Route*. Введите следующие параметры:

Interface	wan1
Network	l2tp_network
Gateway	wan_gw
Local IP Address	(None)
Metric	100

Маршрутизация для провайдера Билайн.

Зайдите в меню *Objects→Address Book→Add→IP4 Address. Bo* вкладке *General* введите следующие параметры:

Name	Net1
IP Address	85.21.72.83

Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Во вкладке *General* введите

следующие параметры:	
Name	Net2
Address	10.0.0.0/8
Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Во вкладке *General* введите следующие параметры:	
Name	Net3
Address	195.14.50.26
Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Во вкладке *General* введите следующие параметры:	
Name	Net4
Address	195.14.50.93
Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Во вкладке *General* введите следующие параметры:	
Name	Net5
Address	195.14.50.16
Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Во вкладке *General* введите следующие параметры:	
Name	Net6
Address	85.21.79.0/24
Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Во вкладке *General* введите следующие параметры:	
Name	Net7
Address	85.21.90.0/24
Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Во вкладке *General* введите следующие параметры:	
Name	Net8
Address	83.102.231.32/28
Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Во вкладке *General* введите следующие параметры:	
Name	Net9
Address	85.21.108.16/28
Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Во вкладке *General* введите следующие параметры:	
Name	Net10
Address	195.14.40.141
Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Во вкладке *General* введите следующие параметры:	
Name	Net11
IP Address	85.21.37.16/28
Объединим сети в группу. Зайдите в меню *Objects→Address Book→Add→IP4 Group*. Во вкладке *General* введите следующие параметры:	
Name	ISP_nets
Переместите элементы Net1, Net2, Net3, Net4, Net5, Net6, Net7, Net8, Net9, Net10, Net11 из списка *Available* в список *Selected*.	
Зайдите в меню *Routing→Routing Tables→main→Add→Route*. Введите следующие параметры:	
Interface	wan1
Network	ISP_Nets

Gateway	wan_gw
Local IP Address	(None)
Metric	100
Создание правил IP Rule	
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Введите следующие параметры:	
Name	all_services
Action	NAT
Service	all_services
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	ISP_Nets
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Введите следующие параметры:	
Name	ping-outbound
Action	NAT
Service	ping-outbound
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	ISP_Nets
Примечание: Для выхода в Интернет через L2TP/PPTP-туннель необходимо изменить соответствующие правила доступа, где в качестве параметра **Source Interface нужно** ***использовать созданный интерфейс L2TP/PPTP.***	
Командная строка (CLI)	
gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address l2tp_network Address=85.21.0.0/24 gw-world:/labs> add IP4Address tp_beeline_ru Address=85.21.0.251 gw-world:/labs> cc gw-world:/> set Interface Ethernet wan1 DHCPEnabled=Yes gw-world:/>add Interface L2TPClient Internet RemoteEndpoint=dns:tp.internet.beeline.ru Username=mstu Password=P@ssw0rd gw-world:/> cc IPRuleFolder lan_to_wan1 gw-world:/3(lan_to_wan1)> set IPRule 4(allow_standard)DestinationInterface=Internet gw-world:/3(lan_to_wan1)> cc gw-world:/> cc RoutingTable main gw-world:/main>add Route Interface=wan1 Network=labs/pptp_network Gateway=InterfaceAddresses/wan_gw Metric=100 gw-world:/main> cc gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address Net1 Address=85.21.72.83 gw-world:/labs> add IP4Address Net2 Address=10.0.0.0/8 gw-world:/labs> add IP4Address Net3 Address=195.14.50.26 gw-world:/labs> add IP4Address Net4 Address=195.14.50.93 gw-world:/labs> add IP4Address Net5 Address=195.14.50.16 gw-world:/labs> add IP4Address Net6 Address=85.21.79.0/24 gw-world:/labs> add IP4Address Net7 Address=85.21.90.0/24 gw-world:/labs> add IP4Address Net8 Address=85.102.231.32/28	

gw-world:/labs> add IP4Address Net9 Address=85.21.108.16/28
gw-world:/labs> add IP4Address Net10 Address=195.14.40.141
gw-world:/labs> add IP4Address Net11 Address=85.21.37.16/28
gw-world:/labs>add IP4Group ISP_Nets Members=labs/Net1, labs/Net2, labs/Net3, labs/Net4, labs/Net5, labs/Net6, labs/Net7, labs/Net8, labs/Net9, labs/Net10, labs/Net11
gw-world:/labs> cc
gw-world:/> cc RoutingTable main
gw-world:/main> add Route Interface=wan1 Network=labs/ISP_Nets Gateway=InterfaceAddresses/wan_gw
gw-world:/main> cc
gw-world:/>cc IPRuleFolder labs
gw-world:/1(labs)>add IPRule Action=NAT DestinationInterface=wan1 DestinationNetwork=labs/ISP_Nets Service=all_services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Name=all_services
gw-world:/1(labs)>add IPRule Action=NAT DestinationInterface=wan1 DestinationNetwork=labs/ISP_Nets Service=ping-outbound SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Name=ping-outbound
gw-world:/1(labs)> cc
gw-world:/> activate (*подождать 3-5 секунд*)
gw-world:/>commit

Настройка PPPoE-подключения на *wan1*-интерфейсе.

Настройка DFL-860E

Web-интерфейс

Зайдите в меню *Interfaces→PPPoE→Add→PPPoE Tunnel.* Введите следующие параметры:

Name	PPPoE_inet
Physical Interface	wan1
Remote Network	all-nets
Username	mstu
Pasword	1234
Confirm Pasword	1234

На вкладке *Authentication* отметьте необходимые протоколы шифрования в соответсвии с настройками провайдера Интернета.

Примечание: Для выхода в Интернет через PPPoE-туннель необходимо изменить соответствующие правила доступа IP Rules, где в качестве параметра wan1* нужно *использовать созданный интерфейс PPPoE (PPPoE_inet).

Зайдите в меню *Configuration* и выберите *Save and Activate*.

Командная строка (CLI)

gw-world:/>add Interface PPPoETunnel PPPoE_inet EthernetInterface=wan1 Network=all-nets Password=1234 Username=mstu
gw-world:/> activate (*подождать 3-5 секунд*)
gw-world:/>commit

Упражнение	Проверьте наличие Интернета для пользователей **lan**-сети в соответствии с правилами фильтрации сетевых адресов.
CMD ОС Windows	C:\>ping 8.8.8.8
Устранение возможных проблем	Если маршрутизация к ISP не работает должным образом, решите возникшую проблему с помощью описанных ниже диагностических средств.

Проверьте корректность физических подключений устройства, работоспособность патч-кордов, индикацию на устройстве. Проверьте корректность сетевых настроек компьютера, с которого проводится проверка схемы.
Зайдите в меню *Status→Logging* и просмотрите лог-сообщения встроенного syslog-сервера.
Зайдите в меню *Status→Routes*, проверьте наличие созданных маршрутов.

ЗАНЯТИЕ №6. Ограничение размера пакетов транспортных и диагностических протоколов, запрет и разрешение ICMP. Поддержка IPv6.

На межсетевых экранах D-Link можно настроить большое количество параметров сетевых протоколов. С точки зрения системного администратора для диагностики сети удобно применять команды ping, telnet и tracert. По умолчанию на межсетевых экранах D-Link эти средства диагностики запрещены между интерфейсами устройства.

Цель	Эта лабораторная работа позволяет пользователем изучить основные настройки параметров протоколов IPv4, IPv6, TCP, UDP, ICMPv4, ICMPv6 на межсетевом экране и разрешение выполнения команд ping, telnet и tracert.	
Оборудование	DFL-860E	1
	Рабочая станция	2
	Ethernet-кабель (патч-корд)	2

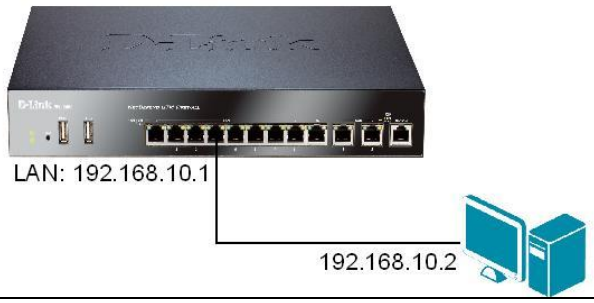
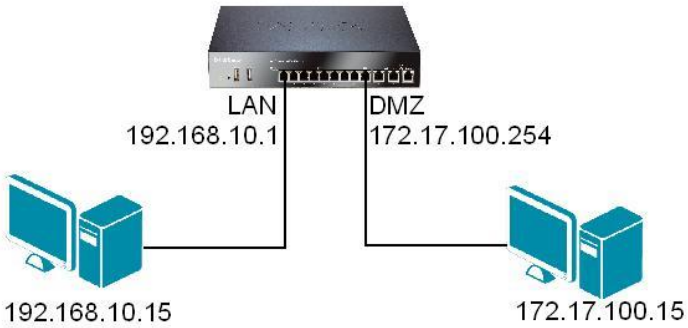
Ограничение размера пакетов ICMP-протокола	
Описание сценария	*Ограничим размер ICMP-сообщений 1024 байтами для всего трафика, проходящего через межсетевой экран.*
Схема 15	
Настройка DFL-860E	
Web-интерфейс	
Зайдите в меню *System→Advanced Settings→Length Limit Setting.* Введите следующие параметры:	
Max ICMP Length	1024
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/>set Settings LengthLimSettings MaxICMPLen=1024 gw-world:/> activate (*подождать 3-5 секунд*) gw-world:/>commit	
Упражнение	Пропингуйте lan_ip межсетевого экрана с компьютера, подключенного к **lan-**интерфейсу устройства. Установите размер пакетов больше и меньше 1024 байта.
CMD ОС Windows	C:\>ping 192.168.10.1 –l 1400 C:\>ping 192.168.10.1 –l 900
Ограничение размера пакетов TCP	
Описание сценария	*Ограничим размер TCP-пакетов 1024 байтами для всего трафика, проходящего через межсетевой экран.*

Схема 16	

Настройка DFL-860E

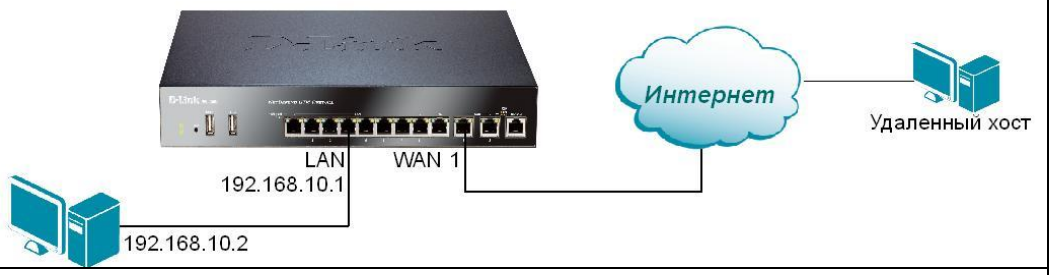
Web-интерфейс

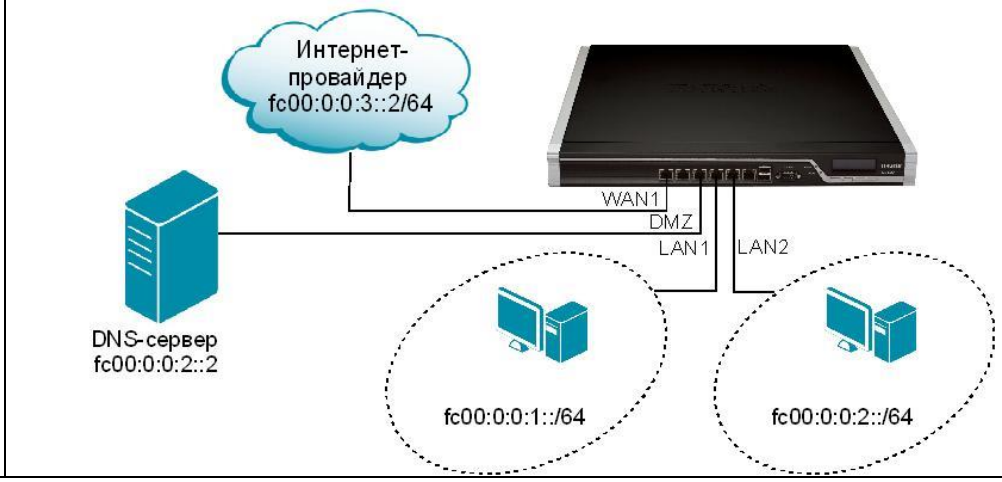
Зайдите в меню *System→Advanced Settings→Length Limit Setting.* Введите следующие параметры:	
Max TCP Length	1024
Зайдите в меню *Objects→Services*, добавьте *TCP/UDP Service* со следующими параметрами:	
Name	iperf
Type	TCP/UDP (выберите из списка)
Source	0-65535
Destination	5001
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	pc1
IPAddress	192.168.10.15
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	pc2
IPAddress	172.17.100.15
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	Allow_tcp
Action	Allow
Service	iperf
Source Interface	lan
Source Network	pc1
Destination Interface	dmz
Destination Network	pc2
Зайдите в меню *Configuration* и выберите *Save and Activate*.	

Командная строка (CLI)

```
gw-world:/>set Settings LengthLimSettings MaxTCPLen=1024
gw-world:/> add Service ServiceTCPUDP iperf SourcePorts=0-65535 DestinationPorts=5001 Type=TCPUDP
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address pc1Address=192.168.10.15
gw-world:/labs> add IP4Address pc2 Address=172.17.100.15
gw-world:/labs> cc
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow Service=iperf SourceInterface=lan SourceNetwork=labs/pc1 DestinationInterface=dmz DestinationNetwork=labs/pc2 Name=Allow_tcp
```

gw-world:/1(labs)> cc gw-world:/> activate (*подождать 3-5 секунд*) gw-world:/>commit	
Упражнение	Установите TCP-соединение с компьютера, подключенного к **lan**-интерфейсу устройства, на компьютер, подключенный к **dmz**-интерфейсу, выбрав размер пакетов больше и меньше 1024 байта.
CMD OC Windows (pc2)	C:\>iperf –s –t –p 5001
CMD OC Windows (pc1)	C:\>iperf –c 172.17.100.15 –t –p 5001
Разрешение трассировки DFL	
Описание сценария	*По умолчанию нет возможности осуществлять трассировку DFL от рабочей станции внутренней сети, подключенной к **lan**-интерфейсу, до удаленного хоста с помощью команды tracert. В случае необходимости данного действия выполните следующие настройки.*
Настройка DFL-860E	
Web-интерфейс	
Зайдите в меню *System→Advanced Settings→IP Settings*. Введите следующие параметры:	
TTL on Low	Log (выберите из списка)
Примечание: после этих операций в журнал будет выводится сообщение «значение TTL слишком мало». Описанные далее действия позволяют избежать этого.	
Зайдите в меню *System→Advanced Settings→IP Settings*. Введите следующие параметры:	
TTL Min	1
Создание правила для ICMP	
Зайдите в *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	tracert_to_DMZ
Action	Allow
Service	all_icmp
Source Interface	lan
Source Network	lannet
Destination Interface	core
Destination Network	dmz_ip
Зайдите в *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/>set Settings IPSettings TTLOnLow=Log TTLMin=1 gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=core DestinationNetwork=InterfaceAddresses/dmz_ip Service=all_icmp SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Name=tracert_to_DMZ gw-world:/1(labs)> cc gw-world:/> activate (*подождать 3-5 секунд*) gw-world:/>commit	
Упражнение	Выполните трассировку dmz_ip межсетевого экрана с компьютера, подключенного к **lan**-интерфейсу устройства.
CMD OC Windows	C:\>tracert 172.17.100.254

Разрешение команды ping на внешние адреса (ICMP - Ping)	
Описание сценария	*По умолчанию нет возможности осуществить ping внешних адресов от рабочей станции во внутренней сети, подключенной к* ***lan****-интерфейсу, до удаленного хоста с помощью команды ping.*
Схема 17	
Настройка DFL-860E	
Web-интерфейс	
Создание необходимых объектов	
Создадим объект «IP-адрес хоста», который будет разрешен для выполнения команды ping. Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Во вкладке *General* введите следующие параметры:	
Name	ip_ext
Address	8.8.8.8
Создадим ICMP-сервис. Зайдите в меню *Objects→Services*. Создайте новый сервис ICMP Service, введите следующие параметры:	
Name	ping-outbound
Во вкладке *ICMP Parameters*:	
ICMP Message Types	Echo Request (Codes 0-255)
Примечание: Если сервис с таким именем уже существует, то будет выдано сообщение об ошибке одинаковых имен.	
Создание правила для ICMP	
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	Ping_to_Ext
Action	NAT
Service	ping-outbound
Source Interface	lan
Source Network	lannet
Destination Interface	wan1 (Интернет)
Destination Network	ip_ext
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address ip_ext Address=8.8.8.8 gw-world:/labs> cc gw-world:/>add Service ServiceICMP ping-outbound MessageTypes=Specific EchoRequest=Yes gw-world:/> cc IPRuleFolder labs	

gw-world:/1(labs)> add IPRule Action=NAT DestinationInterface=wan1 DestinationNetwork=labs/ip_ext Service=ping-outbound SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Name=Ping_to_Ext gw-world:/1(labs)> cc gw-world:/> activate (*подождать 3-5 секунд*) gw-world:/>commit	
Упражнение	Пропингуйте IP-адрес ip_ext с компьютера, подключенного к **lan**-интерфейсу устройства.
CMD OC Windows	C:\>ping 8.8.8.8
Поддержка IPv6 (на примере настройки DFL-1660/2560)	
Описание сценария	*Необходимо настроить фильтрацию трафика IPv6 и разрешить доступ к DNS-серверу, расположенному в **lan2**-сети с адресацией IPv6. Пользователи **lan1**-сети используют подсеть fc00:0:0:1::/64 (используется автоконфигурирование с EUI-64), подсеть в **lan2** – fc00:0:0:2::/64. Доступ в Интернет осуществляется через провайдера, поддерживающего IPv6. Сетевые настройки для **wan1**, предоставленные провайдером: IP-адрес fc00:0:0:3::2/64, основной шлюз – fc00:0:0:3::1.*
Схема 18	
Настройка DFL-1660 (для прошивок старше 2.40.00)	
Web-интерфейс	
Разрешим глобально обработку данных IPv6 межсетевым экраном. Зайдите в меню *System→Advanced Settings→IP Setting.* Введите следующие параметры:	
Enable IPv6	Поставьте галочку
Создадим IPv6-подсеть на lan1. Зайдите в меню *Objects→Address Book→Add→IP6 Address.* Введите следующие параметры:	
Name	lan1net6
IPAddress	fc00:0:0:1::/64
Создадим IPv6-адрес на lan1. Зайдите в меню *Objects→Address Book→Add→IP6 Address.* Введите следующие параметры:	
Name	lan1_ip6
Address	fc00:0:0:1::1
Создадим IPv6-подсеть на lan2. Зайдите в меню *Objects→Address Book→Add→IP6 Address.* Введите следующие параметры:	
Name	lan2net6

Address	fc00:0:0:2::/64
Создадим IPv6-адрес на lan2. Зайдите в меню *Objects→Address Book→Add→IP6 Address*. Введите следующие параметры:	
Name	lan2_ip6
Address	fc00:0:0:2::1
Создадим IPv6-адрес DNS-сервера. Зайдите в *Objects→Address Book→Add→IP6 Address*. Введите следующие параметры:	
Name	dns_ip6
Address	fc00:0:0:2::2
Создадим IPv6-подсеть на wan1. Зайдите в меню *Objects→Address Book→Add→IP6 Address*. Введите следующие параметры:	
Name	wan1net6
Address	fc00:0:0:3::/64
Создадим IPv6-адрес на wan1. Зайдите в меню *Objects→Address Book→Add→IP6 Address*. Введите следующие параметры:	
Name	wan1_ip6
Address	fc00:0:0:3::2
Создадим IPv6-адрес основного шлюза на wan1. Зайдите в меню *Objects→Address Book→Add→IP6 Address*. Введите следующие параметры:	
Name	wan1_gw6
Address	fc00:0:0:3::1
Настроим IPv6 на интерфейсе lan1. Зайдите в меню *Interfaces→Ethernet→lan1*. Введите следующие параметры:	
Enable IPv6	Поставьте галочку
IPAddress	lan1_ip6
Network	lan1net6
Во вкладке *Advanced* введите следующие параметры:	
Enable Router Advertisement for this interface.	Поставьте галочку
Настроим IPv6 на интерфейсе lan2. Зайдите в меню *Interfaces→Ethernet→lan2*. Введите следующие параметры:	
Enable IPv6	Поставьте галочку
IPAddress	lan2_ip6
Network	lan2net6
Настроим IPv6 на интерфейсе wan1. Зайдите в меню *Interfaces→Ethernet→wan1*. Введите следующие параметры:	
Enable IPv6	Поставьте галочку
IPAddress	wan1_ip6
Network	wan1net6
Default Gateway	wan1_gw6
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	Allow_inet_ipv6
Action	Allow
Service	http
Source Interface	lan1
Source Network	lan1net6

Destination Interface	wan1
Destination Network	all-nets6 (::/0)
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	Allow_lan1_lan2
Action	Allow
Service	dns-all
Source Interface	lan1
Source Network	lan1net6
Destination Interface	lan2
Destination Network	dns_ip6
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	Allow_icmp
Action	Allow
Service	all_icmpv6
Source Interface	lan1
Source Network	lan1net6
Destination Interface	lan2
Destination Network	dns_ip6
Зайдите в меню *Routing→Routing Tables→main→Add→Route6*. Во вкладке *General* введите:	
Interface	wan1
Network	wan1net6
Gateway	-
Local IP address	-
Metric	100
Зайдите в меню *Routing→Routing Tables→main→Add→Route6*. Во вкладке *General* введите:	
Interface	wan1
Network	all-nets6
Gateway	wan1_gw6
Local IP address	-
Metric	100
Зайдите в меню *Routing→Routing Tables→main→Add→Route6*. Во вкладке *General* введите:	
Interface	lan1
Network	lan1net6
Gateway	-
Local IP address	-
Metric	100
Зайдите в меню *Routing→Routing Tables→main→Add→Route6*. Во вкладке *Genera l*введите:	
Interface	lan2
Network	lan2net6
Gateway	-
Local IP address	-
Metric	100
Зайдите в меню *Configuration* и выберите *Save and Activate*.	

Примечание: 1. Для IPv6 пока поддерживаются только правила с действиями Allow, Forward fast, Drop, Reject. Также IPv6 нельзя использовать с VPN, ALG, IDP. Нельзя комбинировать объекты IPv4 и IPv6.
2. DNS-сервер, находящийся в lan2-сети должен поддерживать IPv6 и иметь IP6-адрес fc00:0:0:2::2/64, основной шлюз fc00:0:0:2::1. На нем также должно быть настроена пересылка DNS запросов на уполномоченный DNS-сервер провайдера.

Командная строка (CLI)

```
gw-world:/> set Settings IPSettings EnableIPv6=Yes
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP6Address lan1net6Address=fc00:0:0:1::/64
gw-world:/labs> add IP6Address lan1_ip6Address=fc00:0:0:1::1
gw-world:/labs> add IP6Address lan2net6 Address=fc00:0:0:2::/64
gw-world:/labs> add IP6Address lan2_ip6 Address=fc00:0:0:2::1
gw-world:/labs> add IP6Address dns_ip6 Address=fc00:0:0:2::2
gw-world:/labs> add IP6Address wan1net6 Address=fc00:0:0:3::/64
gw-world:/labs> add IP6Address wan1_ip6 Address=fc00:0:0:3::2
gw-world:/labs> add IP6Address wan1_gw6 Address=fc00:0:0:3::1
gw-world:/labs> cc
gw-world:/> set Interface Ethernet lan1 EnableIPv6=Yes IPv6IP=labs/lan1_ip6
IPv6Network=labs/lan1net6
gw-world:/>set Interface Ethernet lan1 EnableRouterAdvertisement=Yes
gw-world:/> set Interface Ethernet lan2 EnableIPv6=Yes IPv6IP=labs/lan2_ip6
IPv6Network=labs/lan2net6
gw-world:/> set Interface Ethernet wan1 EnableIPv6=Yes IPv6IP=labs/wan1_ip6
IPv6Network=labs/wan1net6IPv6DefaultGateway=labs/wan1_gw6
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=wan1 DestinationNetwork=all-nets6
Service=http SourceInterface=lan1 SourceNetwork=labs/lan1net6Name=Allow_inet_ipv6
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=lan2
DestinationNetwork=labs/dns_ip6 Service=dns-all SourceInterface=lan1 SourceNetwork=labs/lan1net6
Name=Allow_lan1_lan2
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=lan2
DestinationNetwork=labs/dns_ip6 Service=all_icmpv6 SourceInterface=lan1
SourceNetwork=labs/lan1net6 Name=Allow_icmp
gw-world:/1(labs)> cc
gw-world:/> cc RoutingTable main
gw-world:/main> add Route6 Interface=wan1 Network= labs/wan1net6 Metric=100 Index=1
gw-world:/main>add Route6 Interface=wan1 Network=all-nets6 Metric=100 Gateway=labs/wan1_gw6
Index=2
gw-world:/main> add Route6 Interface=lan1 Network=labs/lan1net6 Metric=100 Index=3
gw-world:/main> add Route6 Interface=lan2 Network=labs/lan2net6 Metric=100 Index=4
gw-world:/main> cc
gw-world:/> activate (подождать 3-5 секунд)
gw-world:/>commit
```

Настройка IPv6 в Microsoft Windows Vista/7/Server 2008

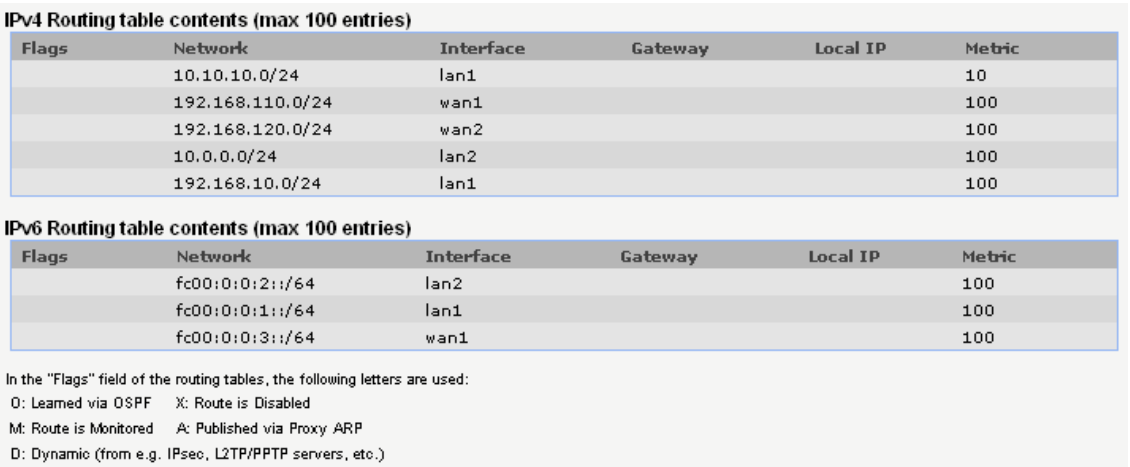
Зайдите в *Центр управления сетями и общим доступом*, откройте свойства подключения по локальной сети. Поставьте галочку напротив *Протокол Интернета версии 6 (TCP/IPv6)*, откройте его свойства. Выберите *Получить IPv6-адрес автоматически*, Использовать следующие адреса DNS-серверов: *Предпочитаемый DNS-сервер* fc00:0:0:2::2.

Упражнение	Проверьте доступность сети Интернет по протоколу IPv6, зайдите на ресурсы Интернета с компьютера **lan1**-сети, имеющего настройки адресации IPv6. Проверьте доступность DNS-сервера

	пингованием по ICMPv6.
Internet Explorer ОС Windows	http://yandex.ru
CMD ОС Windows	C:\>ping fc00:0:0:2::2

На рисунке 7.2 показаны таблицы маршрутизации IPv4 и IPv6.

Рисунок 7.2



IPv4 Routing table contents (max 100 entries)

Flags	Network	Interface	Gateway	Local IP	Metric
	10.10.10.0/24	lan1			10
	192.168.110.0/24	wan1			100
	192.168.120.0/24	wan2			100
	10.0.0.0/24	lan2			100
	192.168.10.0/24	lan1			100

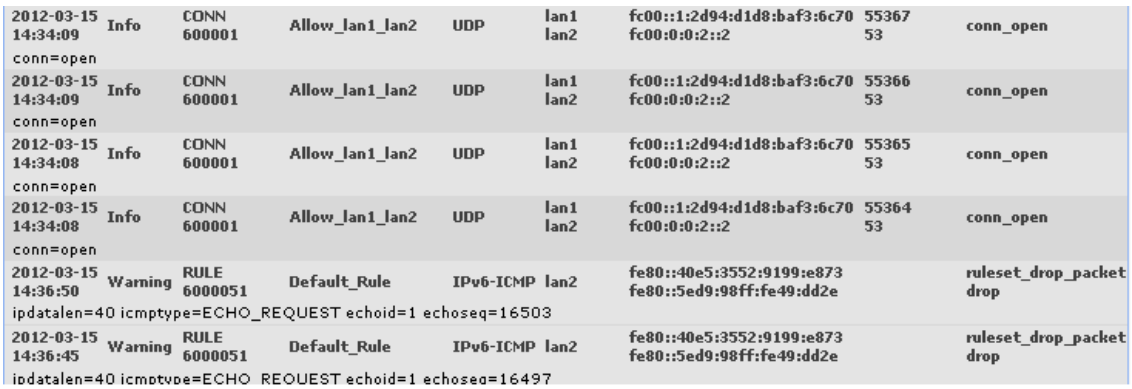
IPv6 Routing table contents (max 100 entries)

Flags	Network	Interface	Gateway	Local IP	Metric
	fc00:0:0:2::/64	lan2			100
	fc00:0:0:1::/64	lan1			100
	fc00:0:0:3::/64	wan1			100

In the "Flags" field of the routing tables, the following letters are used:
O: Learned via OSPF X: Route is Disabled
M: Route is Monitored A: Published via Proxy ARP
D: Dynamic (from e.g. IPsec, L2TP/PPTP servers, etc.)

На рисунке 7.3 показаны лог-сообщения для адресации IPv6.

Рисунок 7.3

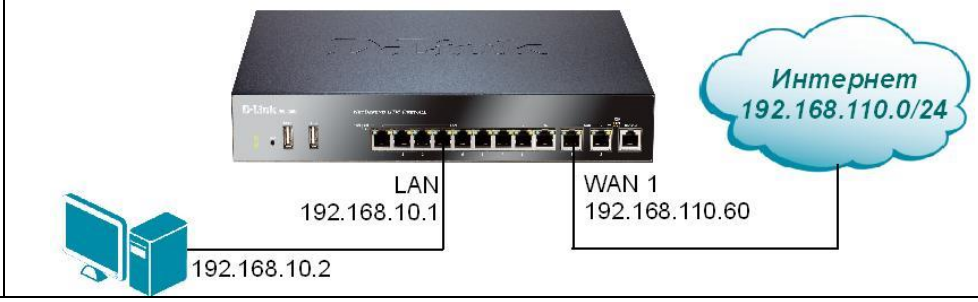


2012-03-15 14:34:09	Info	CONN 600001	Allow_lan1_lan2	UDP	lan1 lan2	fc00::1:2d94:d1d8:baf3:6c70 fc00:0:0:2::2	55367 53	conn_open
conn=open								
2012-03-15 14:34:09	Info	CONN 600001	Allow_lan1_lan2	UDP	lan1 lan2	fc00::1:2d94:d1d8:baf3:6c70 fc00:0:0:2::2	55366 53	conn_open
conn=open								
2012-03-15 14:34:08	Info	CONN 600001	Allow_lan1_lan2	UDP	lan1 lan2	fc00::1:2d94:d1d8:baf3:6c70 fc00:0:0:2::2	55365 53	conn_open
conn=open								
2012-03-15 14:34:08	Info	CONN 600001	Allow_lan1_lan2	UDP	lan1 lan2	fc00::1:2d94:d1d8:baf3:6c70 fc00:0:0:2::2	55364 53	conn_open
conn=open								
2012-03-15 14:36:50	Warning	RULE 6000051	Default_Rule	IPv6-ICMP	lan2	fe80::40e5:3552:9199:e873 fe80::5ed9:98ff:fe49:dd2e		ruleset_drop_packet drop
ipdatalen=40 icmptype=ECHO_REQUEST echoid=1 echoseq=16503								
2012-03-15 14:36:45	Warning	RULE 6000051	Default_Rule	IPv6-ICMP	lan2	fe80::40e5:3552:9199:e873 fe80::5ed9:98ff:fe49:dd2e		ruleset_drop_packet drop
ipdatalen=40 icmptype=ECHO_REQUEST echoid=1 echoseq=16497								

ЗАНЯТИЕ №7. Настройка NAT, NAT Pool, SAT, PAT, DNS Relay, перенаправление портов. Фильтрация по MAC-адресу. Создание нескольких подсетей на интерфейсе

Межсетевые экраны позволяют обеспечить безопасные соединения для защищаемой сети с помощью протоколов NAT и PAT. Межсетевые экраны серии DFL не имеют встроенного DNS-сервера, но существует возможность настроить перенаправление DNS-запросов от хостов во внутренней сети к внешним DNS-серверам. Возможность настройки параметров ARP позволяет осуществлять фильтрацию по MAC-адресам и создавать дополнительные подсети.

Цель	Эта лабораторная работа предназначена для изучения технологии NAT, PAT, SAT, механизма DNSRelay на межсетевом экране.Также рассмотрен механизм фильтрации по MAC-адресу и создание нескольких подсетей на **lan-**интерфейсе.	
Оборудование	DFL-860E	1
	Рабочая станция	2
	Ethernet-кабель (патч-корд)	3
	DNS-сервер	1

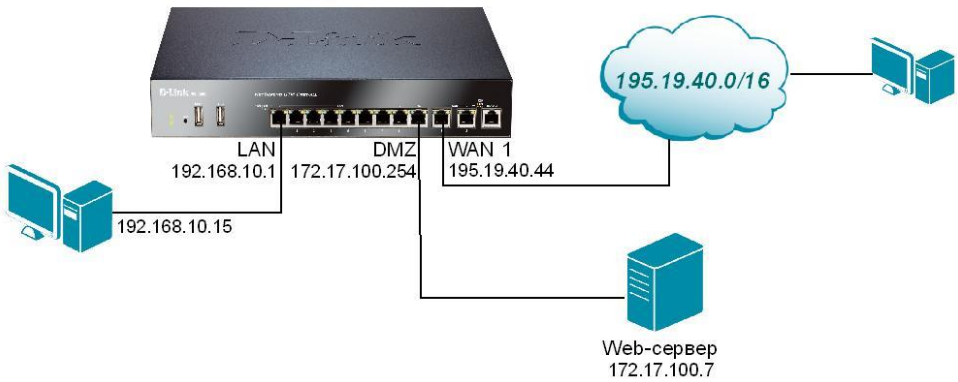
NAT	
Описание сценария	*Технология NAT (Network Address Translation) позволяет компьютерам, имеющим внутренние адреса (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16), выходить в Интернет через внешние адреса. При этом большему количеству внутренних сетевых адресов можно проставить в соответствие меньшее количество внешних адресов. Различают динамический NAT – адреса преобразуются динамически, и статический NAT (SAT) – адреса преобразуются в соответствии со статическими настройками.* *Создадим правила NAT для доступа в Интернет.*
Схема 19	
Настройка DFL-860E	
Web-интерфейс	
Создание необходимых объектов	
Зайдите в меню *Interfaces→Ethernet→wan1*. Снимите выделение *Enable DHCP Client.*	
Зайдите в меню *Objects→Address Book→InterfaceAddresses→wan1_ip*. Введите следующие	

параметры:	
Name	wan1_ip
Address	Введите настройки, полученные от провайдера (например, 192.168.110.60)
Зайдите в меню *Objects→Address Book→InterfaceAddresses→wan1net.* Введите следующие параметры:	
Name	wan1net
Address	Введите настройки, полученные от провайдера (например, 192.168.110.0/24)
Зайдите в меню *Objects→Address Book→InterfaceAddresses→wan1_gw.* Введите следующие параметры:	
Name	wan1_gw
Address	Введите настройки, полученные от провайдера (например, 192.168.110.1)
Зайдите в меню *Objects→Address Book→InterfaceAddresses→wan1_dns1.* Введите следующие параметры:	
Name	wan1_dns1
Address	Введите настройки, полученные от провайдера (например, 8.8.8.8)
Зайдите в меню *Objects→Services→Add→TCP/UDP Service.* Введите следующие параметры:	
Name	httptest
Type	TCP
Source	0-65535
Destination	80
Зайдите в меню *Objects→Services→Add→TCP/UDP Service.* Введите следующие параметры:	
Name	dns-alltest
Type	TCP/UDP
Source	0-65535
Destination	53
Настройка IP-правила межсетевого экрана	
Зайдите в меню *Rules→IP Rules.* Создайте новое IP Rule с действием NAT. Во вкладке *General* введите:	
Name	HTTP_from_LAN
Action	NAT
Service	httptest
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets
Создайте новое IP Rule для DNS. Во вкладке *General* введите:	
Name	DNS_from_LAN
Action	NAT
Service	dns-alltest
Source Interface	lan
Source Network	lannet

Destination Interface	wan1
Destination Network	all-nets
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/>set Interface Ethernet wan1 DHCPEnabled=No gw-world:/>set IP4Address InterfaceAddresses/wan1_ip Address=192.168.110.60 gw-world:/>set IP4Address InterfaceAddresses/wan1net Address=192.168.110.0/24 gw-world:/>set IP4Address InterfaceAddresses/wan1_gw Address=192.168.110.1 gw-world:/>set IP4Address InterfaceAddresses/wan1_dns1 Address=8.8.8.8 gw-world:/>add Service ServiceTCPUDP httptest DestinationPorts=80 SourcePorts=0-65535 gw-world:/> add Service ServiceTCPUDP dns-alltest DestinationPorts=53 SourcePorts=0-65535 gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=NAT DestinationInterface=wan1 DestinationNetwork=all-nets Service=httptest SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Name=HTTP_from_LAN gw-world:/1(labs)> add IPRule Action=NAT DestinationInterface=wan1 DestinationNetwork=all-nets Service=dns-alltest SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Name=DNS_from_LAN gw-world:/1(labs)> cc gw-world:/> activate (*подождать 3-5 секунд*) gw-world:/>commit	
Упражнение	Проверьте динамическое преобразование адресов для межсетевого экрана и компьютера, подключенного к **lan-**интерфейсу устройства.
CMD OC Windows	C:\>netstat –a
Web-интерфейс	Зайдите в меню *Status→Connections*, просмотрите преобразование сетевых адресов.
CMD OC Windows (компьютер в подсети wan1net) с IP-адресом 192.168.110.100.	C:\>iperf –s –t –p 5001
CMD OC Windows (компьютер в подсети lannet)	C:\>iperf – c192.168.110.100 –t –p 5001
NAT Pool	
Описание сценария	*Количество одновременных NAT-соединений не может превышать 64 500. При этом каждое соединение «состоит» из уникальной пары IP-адресов. Здесь под «парой IP-адресов» подразумевается соединение, установленное между IP-адресом на каком-либо интерфейсе системы NetDefendOS и IP-адресом некоторого внешнего хоста. Но если два разных IP-адреса внешнего хоста подключены с использованием одного и того же NAT-адреса межсетевого экрана, то они составляют две разные уникальные IP-пары. Поэтому количество в 64 500 одновременных соединений не является верхним пределом для всего межсетевого экрана NetDefend.* *Ограничения количества соединений можно избежать, используя NAT-пулы. NAT-пулы обычно применяются, если требуется создать много уникальных подключений, используя один порт. Менеджер портов в системе NetDefendOS может поддерживать до 65 000 соединений с уникальной комбинацией*

	из IP-адреса источника и IP-адреса назначения. Большое количество портов может потребоваться, если многие внутренние клиенты используют, например, программные средства по совместному использованию файлов. Аналогичные требования могут возникнуть в ситуации, когда множество клиентов одновременно имеет доступ в Интернет через прокси-сервер. Проблема с ограниченным количеством портов решается с помощью выделения дополнительных внешних IP-адресов для выхода в Интернет и использования NAT-пулов для распределения новых подключений через эти IP-адреса. Для использования NAT-пула необходимо наличие нескольких публичных IP-адресов. *Существует три типа NAT-пулов, каждый из которых производит распределение новых подключений разными способами: Stateful (проверка состояния соединения), Stateless (без проверки состояния соединения), Fixed (Фиксированный). При назначении внешних IP-адресов в NAT-пул не обязательно прописывать их вручную. Можно выбрать объект «IP-пул» системы NetDefendOS.* *В сценарии необходимо настроить доступ в Интернет через NAT с использованием NAT-пула (схема 19).*
Настройка DFL-860E	
Web-интерфейс	
Создание необходимых объектов	
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Во вкладке *General* введите:	
Name	wan1_ip2
Address	192.168.110.253
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Во вкладке *General* введите:	
Name	NAT_pool_IPs
Address	192.168.110.253-192.168.110.254
Создание NAT-пула	
Зайдите в меню *Objects→NAT Pools→Add→NAT Pool.* Во вкладке *General* введите:	
Name	My_NAT_pool
Pool Type	stateful
IP Range	NAT_pool_IPs
Во вкладке *Proxy ARP* введите:	
wan1	Переместите в Selected
Публикация второго IP-адреса на wan1	
Зайдите в меню *Interfaces→ARP→Add→ARP.* Во вкладке *General* введите:	
Mode	Publish
Interface	wan1
IP Address	wan1_ip2 (192.168.110.253)
MAC	00:00:00:00:00:00 (используется MAC-адрес физического интерфейса)
Настройка IP-правила межсетевого экрана	

Зайдите в меню *Rules→IP Rules.* Создайте новое IP Rule с действием NAT. Во вкладке *General* введите:	
Name	HTTP_from_LAN
Action	NAT
Service	http
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets
Во вкладке *NAT* введите:	
Use NAT Pool	Выберите опцию
NAT Pool	My_NAT_pool
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/>set IP4Address InterfaceAddresses/wan1_ip2 Address=192.168.110.253 gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address NAT_pool_IPs Address=192.168.110.253-192.168.110.254 gw-world:/labs> cc gw-world:/> add NATPool My_NAT_pool IPRange=labs/NAT_pool_IPs Type=stateful ProxyARPInterfaces=wan1 gw-world:/> add ARP IP=labs/wan1_ip2 Interface=wan1 Mode=Publish gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=NAT DestinationInterface=wan1 DestinationNetwork= all-nets Service=http SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Name=HTTP_from_LAN gw-world:/1(labs)> cc gw-world:/> activate (*подождать 3-5 секунд*) gw-world:/>commit	
Упражнение	Проверьте динамическое преобразование адресов для межсетевого экрана и компьютера, подключенного к **lan-**интерфейсу и компьютера, подключенного **wan1-**интерфейсу.
CMD ОС Windows	C:\>netstat -n
Web-интерфейс	Зайдите в меню *Status→Connections*, просмотрите преобразование сетевых адресов для двух публичных адресов – wan1_ip и wan1_ip2.
CMD ОСWindows (компьютер в подсети wan1net) с IP-адресом 192.168.110.100.	C:\>iperf –s –t –p 80
CMD ОСWindows (компьютер в подсети lannet)	C:\>iperf – c192.168.110.100 –t –p 80
Настройка SAT для Web-сервера, подключенного к DMZ-интерфейсу	

Схема20	

Настройка DFL-860E

Web-интерфейс

Зайдите в меню *Objects→Services→Add→TCP/UDP Service.* Введите следующие параметры:

Name	http
Type	TCP
Source	0-65535
Destination	80

Примечание: Если сервис с таким именем уже существует, то будет выдано сообщение об ошибке одинаковых имен.

Создадим IPv4-адрес – внешний IP-адрес Web-сервера в DMZ. Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Во вкладке *General* введите следующие параметры:

Name	ip_ext
Address	195.19.40.44 («белый»IP-адрес)

Создадим IPv4-адрес – внутренний IP-адрес Web-сервера в DMZ. Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Во вкладке *General* введите следующие параметры:

Name	ip_webserver
Address	172.17.100.7

Настройка IP-правила межсетевого экрана

Зайдите в меню *Rules→IP Rules.* Создайте новое IP Rule с действием SAT. Во вкладке *General* введите:

Name	SAT_to_WebServer
Action	SAT
Service	http
Source Interface	wan1
Source Network	all-nets
Destination Interface	core
Destination Network	ip_ext

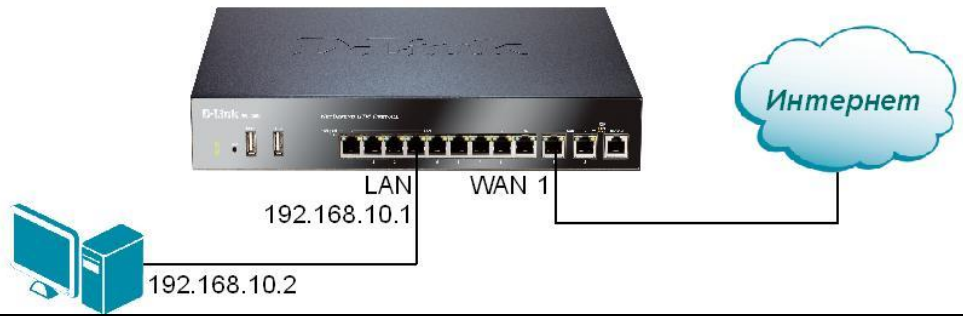
Во вкладке *SAT* введите:

Translate the	Destination IP Address
to New IP Address	ip-webserver

Создайте новое IP Rule с действием NAT для HTTP. Во вкладке *General* введите:

Name	SATNAT_to_WebServer
Action	NAT

Service	http
Source Interface	wan1
Source Network	all-nets
Destination Interface	core
Destination Network	ip_ext
Создайте новое IP Rule с действием NAT для обеспечения безопасного доступа к серверу в DMZ из внутренней сети (lannet). Во вкладке *General* введите:	
Name	HTTP_from_LAN
Action	NAT
Service	http
Source Interface	lan
Source Network	lannet
Destination Interface	dmz
Destination Network	ip-webserver
Примечание: правило SAT требует создания второго правила, следующего за первым, для пропуска трафика. Второе правило может быть – Allow, Forward Fast, NAT, и данное второе правило должно быть размещено ниже исходного SAT правила. ***Исходное правило в реальности ничего не делает, прошедшие проверку соответствия правилам пакеты будут пропускаться, пока не будет достигнуто второе правило.*** ***Заданный набор правил делает видимым внешние адреса хостам в DMZ. Если внутренние хосты подключаются к внешнему интерфейсу* ip_ext*, то они будут способны проходить без NAT с помощью правила SAT. С точки зрения безопасности подобная схема не обеспечивает «невидимость» хостов извне в DMZ.***	
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> add Service ServiceTCPUDP http DestinationPorts=80 SourcePorts=0-65535 gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address ip_ext Address=195.19.40.44 gw-world:/labs> add IP4Address ip_webserver Address=172.17.100.7 gw-world:/labs> cc gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)>add IPRule Action=SAT Service=http SourceInterface=wan1 SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=labs/ip_ext SATTranslateToIP=labs/ip-webserver SATTranslate DestinationIP Name=SAT_to_WebServer gw-world:/1(labs)> add IPRule Action=NAT DestinationInterface=core DestinationNetwork=labs/ip_ext Service=http SourceInterface=wan1 SourceNetwork=all-nets Name=SATNAT_to_WebServer gw-world:/1(labs)> add IPRule Action=NAT DestinationInterface=dmz DestinationNetwork=labs/ip_ext Service=http SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Name=HTTP_from_LAN gw-world:/1(labs)> cc gw-world:/> activate (*подождать 3-5 секунд*) gw-world:/>commit	
Упражнение	Проверьте статическое преобразование адресов для сервера в **dmz**, подключитесь к серверу из Интернета. Предполагается, что на нем настроен HTTP-сервер.
Internet Explorer ОС Windows	http://195.19.40.44 (ip_ext)
CMD ОС Windows (компьютер в подсети dmznet)	C:\>iperf –s –t –p 80

CMD OC Windows (компьютер в подсети wan1net)	C:\>iperf –c 195.19.40.44 –t –p 80
Настройка DNS Relay	
Описание сценария	*Все межсетевые экраны серий DFL) поддерживают функцию DNS Relay, начиная с прошивок v2.04 и далее. Функция DNS Relay обеспечивает только передачу/пересылку DNS-пакетов, т.к. межсетевые экраны D-Link DFL не имеют встроенного в ядро операционной системы DNS-сервера. Таким образом они не могут заменить реальный DNS-сервер для обеспечения преобразования доменных имен в IP-адреса.*
Схема 21	
Настройка DFL-860E	
Web-интерфейс	
Создание необходимых объектов	
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	dns_server
Address	195.19.40.8
Настройка IP-правила межсетевого экрана	
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	SAT_DNS_Relay
Action	SAT
Service	dns_all
Source Interface	lan
Source Network	lannet
Destination Interface	core
Destination Network	lan_ip
Во вкладке *SAT* введите:	
Translate the	Выберите Destination IP Address.
to New IP Address	dns_server
Зайдите в меню *Rules→IP Rules.* Создайте новое IP Rule с действием NAT. Во вкладке *General* введите:	
Name	Allow_DNS_Relay
Action	NAT
Service	dns_all
Source Interface	lan

Source Network	lannet
Destination Interface	core
Destination Network	lan_ip

Убедитесь, что два созданных правила находятся перед другими правилами (перед allow_standart правилами).

Зайдите в меню *Configuration* и выберите *Save and Activate*.

Командная строка (CLI)

```
gw-world:/> add Address AddressFolder labs
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address dns_server Address=195.19.40.8
gw-world:/labs> cc
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)>add IPRule Action=SAT Service=dns_all SourceInterface=lan
SourceNetwork=InterfaceAddresses/lannet DestinationInterface=core
DestinationNetwork=InterfaceAddresses/lan_ip SATTranslateToIP=labs/dns_server SATTranslate
DestinationIP Name=SAT_DNS_Relay Index=1
gw-world:/1(labs)> add IPRule Action=NAT DestinationInterface=core
DestinationNetwork=InterfaceAddresses/lan_ip Service=dns_all SourceInterface=lan
SourceNetwork=InterfaceAddresses/lannet Name=Allow_DNS_Relay Index=2
gw-world:/1(labs)> cc
gw-world:/> activate (подождать 3-5 секунд)
gw-world:/>commit
```

Настройка сетевого подключения Windows XP/Vista/7

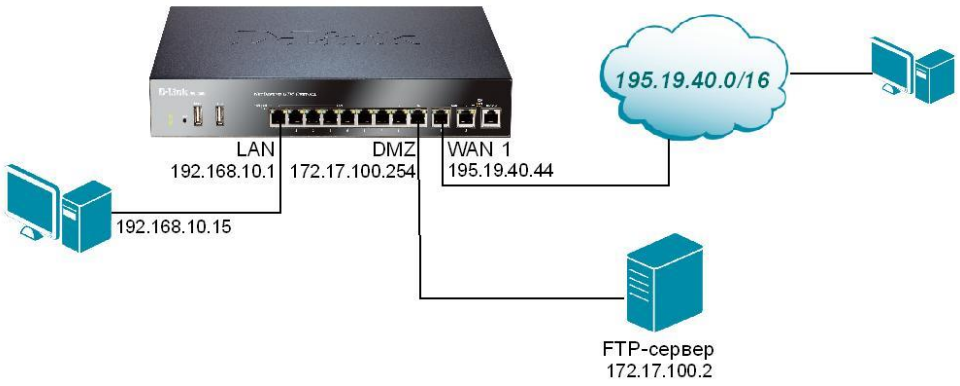
1) Зайдите в свойства подключения по локальной сети.
2) Откройте Протокол Интернета TCP/IP (Windows XP) / Протокол Интернета версии 4 TCP/IPv4 (MS Windows Vista/7).
3) Убедитесь, что в качестве основного шлюза и DNS сервера стоит адрес lan_ip межсетевого экрана (192.168.10.1).

Упражнение	Проверьте разрешение DNS-запросов на компьютере, подключем к **lan**-сети.
CMD OC Windows	C:\>nslookup yandex.ru

PAT

Описание сценария	*Скроем стандартный порт FTP-сервера за случайным динамическим портом 34512 для клиентов, заходящих на сервер через **wan1**-интерфейс.*

Схема 22



Настройка DFL-860E

Web-интерфейс	
Создание необходимых объектов	
Зайдите в меню *Objects→Services→Add→TCP/UDP Service.* Введите следующие параметры:	
Name	secret_service
Type	TCP/UDP
Source	0-65535
Destination	34512
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	private_ip
Address	172.17.100.2
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	public_ip
Address	195.19.40.44
Создание записи ARP	
Зайдите в меню *Interfaces→ARP.* Создайте новую запись ARP:	
Mode	Publish
Interface	wan1
IP Address	public_ip
MAC	00:00:00:00:00:00
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	PAT_rule
Action	SAT
Service	secret_service
Source Interface	wan1
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip
Во вкладке *SAT* введите:	
Translate the	Выберите Destination IP Address.
to New IP Address	private_ip
New Port	21
Создайте новое IP Rule для DNS. Во вкладке *General* введите:	
Name	Allow_PAT
Action	NAT
Service	secret_service
Source Interface	wan1
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip
Зайдите в меню *Configuration* и выберите *Save and Activate.*	
Командная строка (CLI)	

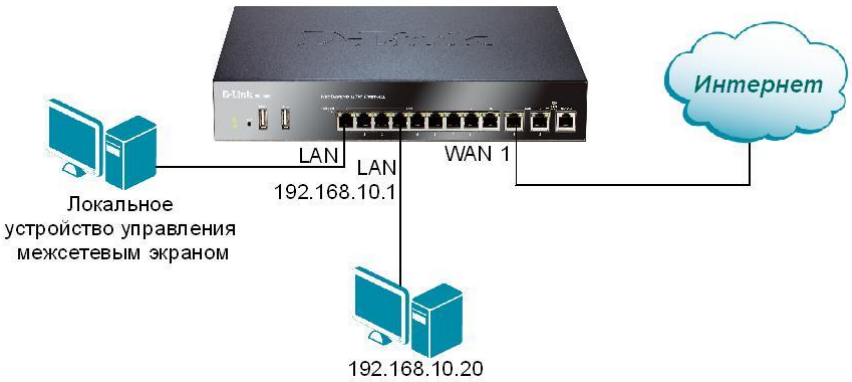
gw-world:/> add Service ServiceTCPUDP secret_service DestinationPorts=34512 SourcePorts=0-65535
gw-world:/> add Address AddressFolder labs
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address private_ip Address=172.17.100.2
gw-world:/labs> add IP4Address public_ip Address=195.19.40.44
gw-world:/labs> cc
gw-world:/> add ARP IP=labs/public_ip Interface=wan1 Mode=Publish
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=SAT Service=secret_service SourceInterface=wan1 SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip SATTranslateToIP=labs/private_ip SATTranslateToPort=21 SATTranslate DestinationIP Name=PAT_rule
gw-world:/1(labs)> add IPRule Action=NAT DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip Service=secret_service SourceInterface=wan1 SourceNetwork=all-nets Name=Allow_PAT
gw-world:/1(labs)> cc
gw-world:/> activate (*подождать 3-5 секунд*)
gw-world:/>commit

Упражнение	Проверьте преобразование портов на компьютере, подключенном к **wan**-интерфейсу.
Internet Explorer ОС Windows	ftp://<ip_ext>:34512
CMD ОС Windows	C:\>netstat -n
CMD ОС Windows (компьютер в подсети dmznet)	C:\>iperf –s –t –p 21
CMD ОС Windows (компьютер в подсети wan1net)	C:\>iperf –c <ip_ext> –t –p 21

Перенаправление портов

Описание сценария	*Зададим перенаправление второго публичного IP-адреса на **wan1**-интерфейсе на компьютер, подключенный к **lan**-сети межсетевого экрана и имеющий IP-адрес 192.168.10.20*

Схема 23



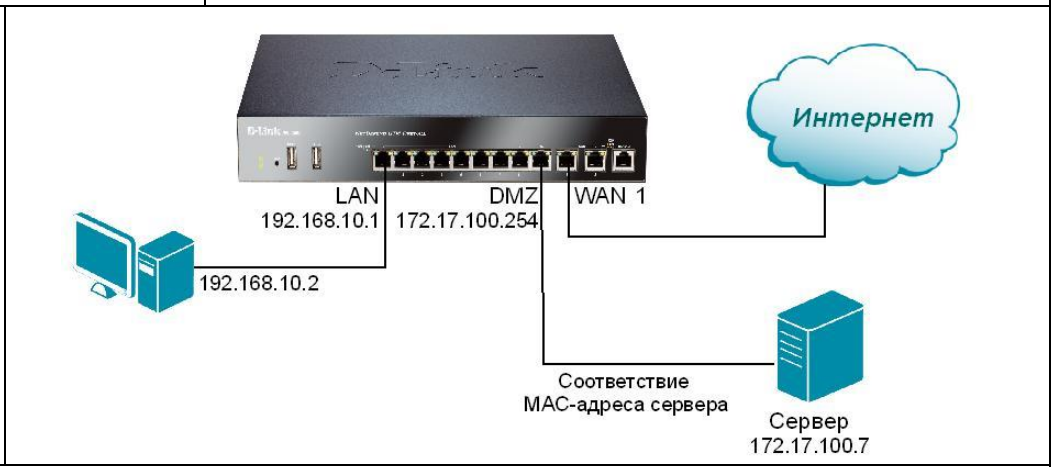
Настройка DFL-860E

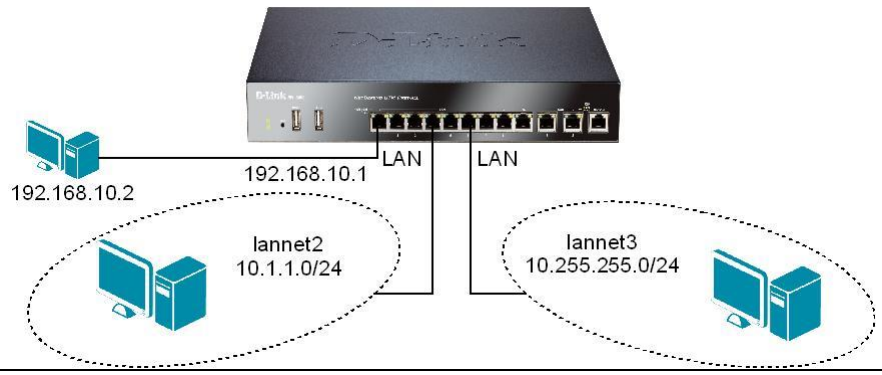
Web-интерфейс

Создание необходимых объектов

Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры (если объекты еще не созданы ранее):

Name	private_ip
Address	192.168.10.20
Настройка IP Rule	
Зайдите в меню *Rules→IP Rules.* Создайте новую папку IP Rule Folder:	
Name	port_mapping_rule
Зайдите в меню *Rules→IP Rules.* Создайте новое IP Rule с действием SAT. Во вкладке *General* введите:	
Name	allow_sat
Action	SAT
Service	rdp (Remote Desktop Protocol)
Source Interface	any
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip
Во вкладке *SAT* введите:	
Translate the	Выберите Destination IP Address.
to New IP Address	private_ip
Создайте новое IP Rule. Во вкладке *General* введите:	
Name	allow_rdp
Action	Allow
Service	rdp
Source Interface	any
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address private_ip Address=192.168.10.20 gw-world:/labs> cc gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=SAT Service=rdp SourceInterface=any SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=wan1_ip SATTranslateToIP=private_ip SATTranslate DestinationIP Name=allow_sat gw-world:/1(labs)> add IPRule Action=NAT SourceInterface=any SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=wan1_ip Service=rdp Name=allow_rdp gw-world:/1(labs)> cc gw-world:/> activate (*подождать 3-5 секунд*) gw-world:/>commit	
Настройка сетевого подключения Windows XP/Vista/7	
1) Зайдите в свойства подключения по локальной сети. 2) Откройте Протокол Интернета TCP/IP (Windows XP) / Протокол Интернета версии 4 TCP/IPv4 (MS Windows Vista/7). 3) Убедитесь, что в качестве IP-адреса используется адрес из подсети 192.168.10.0/24.	

4) В качестве основного шлюза нужно использовать значение lan_ip межсетевого экрана – 192.168.10.1 (значение по умолчанию). Теперь эта рабочая станция ассоциирована с публичным адресом wan1_ip.	
Упражнение	Зайдите из Интернета на wan1_ip, тем самым – на рабочую станцию, подключенную к **lan-**сети.
ОС Windows	Меню→ Пуск→ Все программы→ Стандартные→ Связь→ Подключение к удаленному рабочему столу. Компьютер: wan1_ip
Фильтрация по MAC-адресу	
Описание сценария	*Необходимо обеспечить защиту сервера, подключенному к* ***dmz****-интерфейсу, с помощью фильтрации по MAC-адресу. Трафик к IP-адресу сервера с другим MAC-адресом будет отброшен.*
Схема 24	
Настройка DFL-860E	
Web-интерфейс	
Создание необходимых объектов	
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	ip-server
Address	172.17.100.7
Зайдите в меню *Interfaces→ARP→Add→ARP.* Во вкладке *General* введите:	
Mode	Static
Interface	dmz
IP Address	ip-server (IP-адрес сервера)
MAC	Введите MAC-адрес сервера (например, 48-5B-39-BE-CA-52)
Создание IP Rule	
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Создайте новое правило, введите следующие параметры:	
Name	icmp_to_server
Action	Allow
Service	all_icmp
Source Interface	lan
Source Network	lannet

Destination Interface	dmz
Destination Network	ip-server
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address ip-server Address=172.17.100.7 gw-world:/labs> cc gw-world:/> add ARP IP=labs/ip-server Interface=dmz Mode=Static MACAddress=48-5B-39-BE-CA-52 gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=dmz DestinationNetwork=labs/ip-server Name=icmp_to_server gw-world:/1(labs)> cc gw-world:/> activate (*подождать 3-5 секунд*) gw-world:/>commit	
Упражнение	Проверьте доступность легального сервера, подключенного к **lan**-интерфейсу. Разместите в **dmz** подложный сервер, имеющий другой MAC-адрес. Убедитесь, что он не пингуется. Посмотрите лог-сообщения межсетевого экрана.
CMD OC Windows	C:\>ping 172.17.100.7
Создание нескольких подсетей на lan-интерфейсе	
Описание сценария	*Необходимо создать несколько подсетей на интерфейсе* ***lan****, для этого можно использовать публикацию ARP-записей в режиме Publish.*
Схема 25	
Настройка DFL-860E	
Web-интерфейс	
Создание необходимых объектов	
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	lan_ip2
Address	10.1.1.1
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	lannet2
Address	10.1.1.0/24

Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	lan_ip3
Address	10.255.255.1
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	Lannet3
Address	10.255.255.0/24
Зайдите в меню *Interfaces→ARP→Add→ARP.* Во вкладке *General* введите:	
Mode	Publish
Interface	lan
IP Address	lan_ip2
MAC	00:00:00:00:00:00 (используется MAC-адрес физического интерфейса)
Зайдите в меню *Interfaces→ARP→Add→ARP.* Во вкладке *General* введите:	
Mode	Publish
Interface	lan
IP Address	lan_ip3
MAC	00:00:00:00:00:00 (используется MAC-адрес физического интерфейса)
Создадим маршрут к сети 10.1.1.0/24. Зайдите в меню *Routing→Routing Tables→main→Add→Route.* Добавьте маршрут:	
Interface	lan
Network	lannet2
Metric	100
Создадим маршрут к сети 10.255.255.0/24. Зайдите в меню *Routing→Routing Tables→main→ Add→Route*. Добавьте маршрут:	
Interface	lan
Network	lannet3
Metric	100
Создание IP Rule	
Зайдите в меню *Rules→IP Rules*. Создайте новое правило, введите следующие параметры:	
Name	icmp_from_lannet2
Action	Allow
Service	all_icmp
Source Interface	lan
Source Network	lannet2
Destination Interface	core
Destination Network	lan_ip
Зайдите в меню *Rules→IP Rules*. Создайте новое правило, введите следующие параметры:	
Name	icmp_from_lannet3
Action	Allow
Service	all_icmp
Source Interface	lan
Source Network	lannet3
Destination Interface	core

Destination Network	lan_ip
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
<u>Командная строка (CLI)</u>	
gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address lan_ip2 Address=10.1.1.1 gw-world:/labs> add IP4Address lannet2 Address=10.1.1.0/24 gw-world:/labs> add IP4Address lan_ip3 Address=10.255.255.1 gw-world:/labs> add IP4Address lannet3 Address=10.255.255.0/24 gw-world:/labs> cc gw-world:/> add ARP IP=labs/lan_ip2 Interface=lan Mode=Publish gw-world:/> add ARP IP=labs/lan_ip3 Interface=lan Mode=Publish gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet2 DestinationInterface=core DestinationNetwork=InterfaceAddresses/lan_ip Name=icmp_from_lannet2 gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet3 DestinationInterface=core DestinationNetwork=InterfaceAddresses/lan_ip Name=icmp_from_lannet3 gw-world:/1(labs)> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Упражнение	Пропингуйте адрес lan_ip с настроенных соответственно компьютеров из сетей lannet2 и lannet3.
CMD ОС Windows (подсеть lannet2)	C:\>ping 192.168.10.1
CMD ОС Windows (подсеть lannet3)	C:\>ping 192.168.10.1

ЗАНЯТИЕ №8. Аутентификация пользователей. Встроенная база данных, внешние базы данных – RADIUS, LDAP, Active Directory. Ограничение доступа по времени с использованием расписаний (Schedules).

Межсетевые экраны позволяют задать авторизацию доступа пользователей в защищаемой сети и доступа к серверам в защищаемых интерфейсах межсетевого экрана. Авторизация может быть организована с учетом привязки к текущему времени. Источники аутентификации пользователей могут быть как внутренние, так и внешние.

Цель	Эта лабораторная работа позволяет пользователям научиться настраивать авторизацию пользователей на межсетевых экранах.	
Оборудование	DFL-860E	1
	Рабочая станция	2
	Ethernet-кабель (патч-корд)	3
	RADIUS-сервер	1
	LDAP-сервер	1
	Домен Microsoft Windows Server 2003/2008	1

Аутентификация пользователей	
Определение	*Аутентификация пользователей в межсетевом экране может быть выполнена на основе следующих аутентификационных источников (authentication source):* *- Локальная внутренняя база пользователей (local internal user database),* *- RADIUS-сервер,* *- LDAP-сервер.* *Аутентификационные источники содержат записи о пользователях, с полями* «имя пользователя\пароль»*.* *Настройка аутентификации пользователей может быть выполнена в несколько этапов, описанных ниже:* *- Создание и заполнение аутентификационного источника.* *- Задание аутентификационных правил (Authentication Rule), описывающих какой проходящий через межсетевой экран трафик должен быть аутентифицирован и какой аутентификационный источник будет для этого использован.* *- При необходимости задание IP-объекта для IP-адресов аутентифицируемых клиентов. Такая привязка может быть сделана напрямую для правила аутентификации в качестве IP-адреса инициатора соединения или может быть ассоциирована с группой аутентификации (Authentication Group).* *- Настройка IP Rule для разрешения аутентификации и разрешения клиентам, входящим в заданный в предыдущем пункте IP-объект, доступа к ресурсам.*
Локальная база пользователей	*Локальная база пользователей встроена в операционную систему межсетевого экрана, содержит профили авторизованных пользователей и групп пользователей. Имена пользователей и пароли могут быть введены в эту базу через Web-интерфейс или командную строку.* *Каждый пользователь в локальной базе пользователей может быть членом одной или более групп аутентификации. Эти группы не являются предопределенными, задаются текстовой строкой, чувствительной к регистру. Группы аутентификации не*

	используются с правилами аутентификации, но зато ассоциируются с IP-объектами, которые далее используются в наборе IP-правил (IP rule set). *Использование групп с IP-правилами заключается в следующем. При задании сети источника в IP Rule может быть создан определенный пользователем IP-объект и группа аутентификации может быть связанна с этим IP-объектом. Это будет означать, что правила IP Rule применяются только к пользователям, прошедшим аутентификацию, и принадлежащим связанной с ними группе сети источника. Цель использования этого механизма – ограничить доступ к определенным сетям отдельным группам по правилам, применяемым только к членам этих групп. Для предоставления доступа необходимо создать разрешающее правила IP Rule и пользователь должен принадлежать к той же группе, что и группа правил для сети источника.* *Существуют две административные группы по умолчанию: administrators, auditors. Члены группы administrators могут подключаться к межсетевому экрану через Web-интерфейс или командную строку и изменять конфигурацию устройства. Члены группы auditors могут только просматривать конфигурацию межсетевого экрана, но не могут изменять её.*
PPTP/L2TP конфигурация.	*При подключении клиента через PPTP/L2TP-соединение для локальной базы пользователей могут быть заданы следующие опции:* *- Статический IP-адрес клиента (Static Client IP Address). Данным IP-адресом клиент должен обладать, чтобы иметь возможность пройти аутентификацию.* *- Сеть за пользователем (Network behind user). Если данная опция задана, то маршрут при аутентификации этого пользователя будет автоматически добавляться к основной таблице маршрутизации межсетевого экрана. Существование такого добавленного маршрута означает, что любой направляющийся в данную подсеть трафик будет корректно смаршрутизирован через PPTP/L2TP-туннель клиента. По завершении соединения клиента маршрут автоматически будет удален из межсетевого экрана.* *- Метрика сетей (Metric for Networks). Если задан параметр Network behind user, то параметр Metric for Networks будет использован в качестве метрики для автоматически добавляемого маршрута. Этот параметр позволяет сделать выбор между несколькими маршрутами для определенной сети.*
Примечание: 1. Опцию Network behind user нужно использовать осторожно. Например, если задать значение all-nets, то станет возможно направить весь Инернет-трафик пользователю через туннель.	
Задание публичного ключа SSH.	*Для PPTP/L2TP-клиентов использование публичного ключа SSH (SSH Public Key) часто является альтернативой задания имени пользователя и пароля. Приватный (частный) ключ может быть указан для локальной базы пользователей путем выбора предварительно загруженного объекта SSH Client Key операционной системы межсетевого экрана. При подключении пользователей происходит автоматическая проверка ключей клиентов для аутентификации. Достаточно один раз пройти аутентификацию, потом уже нет необходимости вводить имя пользователя и пароль. Для использования этой опции объект SSH*

	Client Key или объекты должны быть раздельно заданны в ОС межсетевого экрана. В Web-интерфейсе клиентские ключи относятся к объектам Authentication Objects. Требуется загрузка файла публичного ключа для пары ключей, используемых клиентом.
Внешний RADIUS-сервер	*В большой сети желательно применять централизованную базу аутентификации на выделенном сервере. Если в сети более одного межсетевого экрана и тысячи пользователей, то использование раздельных баз данных на каждом устройстве становится проблематичным. Использование внешнего сервера аутентификации для проверки комбинации* «имя пользователя/пароль» *в ответ на запросы межсетевого экрана является удачным решением. ОС межсетевого экрана поддерживает протокол Remote Authentication Dial-In User Server (RADIUS).* *Межсетевой экран может выступать в качестве RADIUS-клиента, посылая RADIUS-сообщения с аутентификационными данными пользователя и информацией о параметрах соединения. RADIUS-сервер отвечает сообщением с подтверждением аутентификации или отказом в доступе. Можно задать несколько внешних аутентификационных серверов.* *Безопасность RADIUS-протокола обеспечивается наличием у RADIUS-клиента и RADIUS-сервера общего секрета (Shared Secret). Этот секрет обеспечивает дальнейшее шифрование сообщений между клиентом и сервером RADIUS. Общий секрет – это относительно длинная строка чувствительных к регистру символов (до 100 символов).* *Протокол RADIUS использует протокол PPP для передачи запросов* имени пользователя/пароля *между клиентами и сервером RADIUS, а также схемы аутентификации PPP – PAP и CHAP. Сообщения RADIUS пересылаются через UDP, порт 1812.* *Аутентификация RADIUS поддерживает спецификацию групп пользователя (группы administrators, auditors).*
Внешние LDAP-сервер	*На межсетевом экране можно настроить работу с LDAP-серверами (Lightweight Directory Access Protocol). ОС межсетевого экрана будет выступать в качестве клиента одного или нескольких LDAP-серверов. Для обеспечения безотказности может быть настроена работа с несколькими серверами, если какой либо сервер станет недоступен.* *Для настройки LDAP-аутентификации необходимо выполнить два этапа:* *- Определить один или более объектов аутентификационных LDAP-серверов в межсетевом экране.* *- В правилах аутентификации пользователей указать один (или список) данных объектов.* *Список LDAP-серверов может быть упорядочен по очередности аутентификации на сервере. Первый LDAP-сервер имеет наивысший приоритет и будет использован первым, при неудаче аутетификации будет использован следующий и т.д.* *Применение LDAP-аутетификации может быть затруднено из-за различных версий LDAP. Проблемы заключаются в следующем:* *- LDAP-сервера различаются в реализации, некоторые опции конфигурирования могут отличаться в зависимости от версии программного обеспечения.* *- Аутентификация PPTP- и L2TP-клиентов может потребовать*

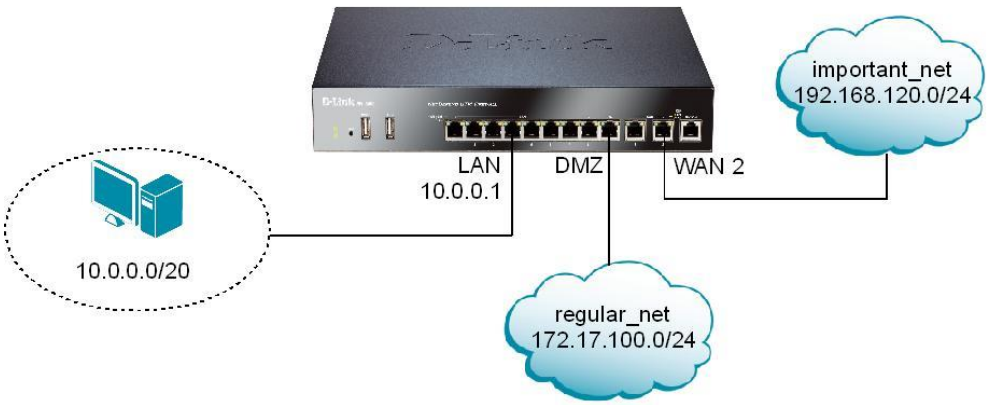
	некоторых административных изменений в LDAP-сервере.
Аутентификация пользователей с помощью Microsoft Active Directory	*Microsoft Active Directory может быть настроен на межсетевом экране в качестве LDAP-сервера. Опция LDAP-сервера Name Attribute определяет наличие Microsoft Active Directory в межсетевом экране. Его значение должно быть равно* SAM Account Name.
Описание технологии LDAP-сервера	*В связи с различием версий LDAP, есть возможность модифицировать схему организации LDAP-аутентификации (LDAP schema), и таким образом переименовать LDAP-атрибуты (LDAP attribute).* *Атрибуты LDAP: Name, Membership, Password – состоят из пары, имя атрибута (attribute name) и значение атрибута (attribute value). Например, для имени пользователя – имя атрибута username, значение Ivanov. Атрибуты могут использоваться по-разному в LDAPсервере, их определение задается схемой.* *Общие настройки (меню User Authentication→External User Databases→Add→LDAP Server).* *- Name. Имя, данное объекту сервера межсетевого экрана, в качестве ссылки. Не имеет ничего общего с Name Attribute, является внутренним только для межсетевого экрана, ничего не значит для LDAP-сервера.* *- IPAddress. IP-адрес LDAP-сервера.* *- Port. Номер порта LDAP-сервера, на который поступают запросы клиентов через TCP/IP. Значение по умолчанию – 389* *- Timeout. Таймаут попытки аутентификации пользователя LDAP-сервером. Если за указанный временной интервал LDAP-сервер не ответит, то но будет считаться недоступным. Значение по умолчанию – 5 сек.* *- Name Attribute. Идентификатор поля данных LDAP-сервера, содержащий имя пользователя. Значение по умолчанию – uid (UNIX-системы). При использовании Microsoft Active Directory данный параметр должен быть установлен в SAM Account Name (не чувствительно к регистру). При поиске подробностей пользователя в Active Directory значение имени пользователя для авторизации (UserLogonName) опрделеяется в поле SAM Account Name на вкладке Account. LDAP-сервер выбирает правильное значение согласно схеме.* *- Retrieve Group Membership. Опция указывает, что группа пользователя должна находиться на LDAP-сервере. Имя группы часто используется при проверки доступа пользователя к службе после успешной аутентификации.* *- Membership Attribute. Если опция Retrieve Group Membership выбрана, то атрибут Membership Attribute определяет для пользователя к какой группе он принадлежит. Название параметра определяется схемой LDAP-сервера, значение по умолчанию - MemberOf. В Microsoft Active Directory группы, к которым принадлежит пользователь, могут быть найдены в свойствах пользователя на закладке «MemberOf».* *- Use Domain Name. Для некоторых LDAP-серверов для успешной аутентификации требуется указывать имя домена (domain name) в комбинации с именем пользователя. Доменное имя – это имя хоста LDAP-сервера. Возможны следующие варианты этой опции:*

	1) None – имя пользователя не модифицируется. *2) Username Prefix – при аутентификации перед именем пользователя будет добавлено «domainname\».* *3) Username Postfix – при аутентификации после имени пользователя будет добавлено «@domainname».* *Если выбрана любая опция, кроме None, то должен быть задан параметр Domain Name. Различные версии LDAPсерверов обрабатывают доменного имени по разному. Большинство версий WindowsActiveDirectoryтребуют опцию Postfix.* *- RoutingTable. Указывает таблицу маршрутизации, где будет разрешаться маршрут к IP-адресу LDAPсервера. По умолчанию используется основная таблица маршрутизации.* *Настройки базы данных (Database Settings).* *- Base Object. Определяет, где в дереве LDAP-сервера будет начинаться поиск учетных записей пользователей. Задание данного параметра влияет на скорость поиска в базе данных LDAP-сервера. Очень важно задать этот параметр верно, иначе пользователь может быть не найден вообще. Изначально рекомендуется выставлять эту опцию в качестве маршрута всей схемы.* *Формат задания опции – разделенный запятыми набор компонентов домена (domain Component). Например для полного доменного имени ldapserver.local.mstu.ru BaseObject записывается в виде:* *DC=ldapserver, DC=local, DC=mstu, DC=ru.* *Таким образом поиск будет начинаться в корне дерева ldapserver.* *- Administrator Account. LDAP-сервер требует наличия административных привилегий у пользователя, устанавливающего соединение для выполнения поиска. Опция Administrator Account задает имя пользователя администратора. Это имя также может быть запрошено с указанием домена, к которому принадлежит этот пользователь.* *- Password/Confirm Password. Пароль к учетной записи администратора.* *- Domain Name. Опция используется для формата имен пользователей. Это первая часть полного доменного имени. Например для полного доменного имени ldapserver.local.mstu.ru эта опция равна ldapserver. Опция Domain Name доступа, если значение Server Type не установлено в Other. Возможно оставить эту опцию незаполненной, но она обязательна, если LDAP-сервер требует доменного имени при выполнении запросов.* *Дополнительные настройки.* *- Password Attribute. Определяет контейнер на LDAP-сервере, содержащий пароль пользователя. Значение по умолчанию – userPassword. Опция может быть незаполнена при использовании LDAP-сервером соединения PPP с CHAP, MS-CHAPv1, MS-CHAPv2. Фактически, если опция задана, то она указывает идентификатор поля данных базы LDAP-сервера, содержащий пароль в виде простого текста.* *Аутентификация BindRequest.* *Аутентификация LDAP-сервера автоматически сконфигурирована на использование LDAP BindRequest Authentication. Это означает следование аутентификации за успешним соединением с LDAP-сервером. Отдельные клиенты не могут распознавать друг друга. При неуспешном соединении с*

	LDAP-сервером, он будет считаться не доступным. *<u>Ответы LDAPсервера.</u>* *При запросе аутентификации на LDAP-сервер межсетевой экран может получить следующие возможные ответы:* *- сервер пришлет ответ об успешной аутентификации пользователя. При этом пользователи, использующие PPP с CHAP, MS-CHAPv1, MS-CHAPv2 фактически аутентифицируются операционной системой межсетевого экрана;* *- сервер пришлет ответ об успешной аутентификации пользователя;* *- сервер не ответит в течении указанного для сервера таймаута Timeout. Если используется один сервер, то аутентификация будет считаться неуспешной. Если же применяются несколько серверов, то будут использованы альтернативные в соответствии с порядком их использования.* *<u>LDAP-аутентификация и PPP.</u>* *При использовании PPP-клиентов для PPTP- или L2TP-доступа при аутентификации используются специальные соглашения для LDAP-аутентификации с CHAP, MS-CHAPv1, MS-CHAPv2. Возможны два варианта.* *1) Нормальная LDAP-аутентификация.* *Для аутентификаций Webauth, XAuth, PPP с безопасностью PAP используется следующий алгоритм. Запрос аутентификации bindrequest с именем пользователя и паролем посылается LDAP-серверу, который проводит аутентификацию и отсылает обратно ответ с результатом bindresponse. Процесс отличается при задействовании группового членства, соответственно в запросе и ответе указывается это членство группы.* *2) PPP-аутентификация с CHAP, MS-CHAPv1, MS-CHAPv2.* *В этом варианте клиент высылает операционной системе межсетевого экрана указатель digest на пароль пользователя. Данный указатель межсетевой экран не сможет переправить напрямую LDAP-серверу, т.к. он будет ему не понятен. Решение – межсетевой экран получает пароль в текстовом виде с LDAP-сервера, создает указатель и сравнивает его с указателем, полученным от клиента. Если указатели идентичны, то аутентификация прошла успешно, но решение об этом принимает межсетевой экран, а не LDAP-сервер.* *Для получения пароля от LDAP-сервера необходимо сделать две вещи:* *- Задать в межсетевом экране параметр Password Attribute, который будет являться идентификатором поля LDAP-сервера, содержащего отсылаемый пароль. Данный идентификатор обязательно должен отличаться от атрибута пароля по умолчанию (обычно userPassword). Рекомендуется использовать поле description в базе данных LDAP.* *- Чтобы сервер вернул пароль из поля базы данных в соответствии с идентификатором, администратор LDAP должен удостовериться в обнаружении там пароля в простом текстовом виде. LDAP-сервера хранят пароли в виде зашифрованных форм указателей и не предоставляют автоматических механизмов для осуществления преобразования. Данное действие должно быть выполнено администратором заранее, когда добавляется новый пользователь и изменяются пароли пользователей. Однако хранение паролей в простой текстовой форме снижает уровень*

	безопасности LDAP-сервера. Поэтому LDAP не всегда применяют в качестве решения аутентификации для CHAP, MS-CHAPv1, MS-CHAPv2 протокола PPP. *После получения межсетевым экраном указателя пароля от пользователя инициируется запрос Search Request к LDAP-серверу. Сервер высылает ответ Search Response, содержащий пароль пользователя и любое групповое членство.* *После получения межсетевым экраном указателя пароля от пользователя инициируется запрос Search Request к LDAP-серверу. Сервер высылает ответ Search Response, содержащий пароль пользователя и любое групповое членство*
Примечание:Очень важно защитить связь с LDAP-сервером. Если связь не локальная, то нужно применять VPN-туннель. Также необходимо ограничить доступ к LDAP-серверу.	
Правила аутентификации	*Правила аутентификации Authentication Rules должны быть определенны для пользователя, прошедшего проверку имени пользователяпароля и установившего соединение через межсетевой экран. Правила аутентификации аналогичны другим политикам безопасности межсетевого экрана, указывается какой трафик будет проверятся правилами. Отличие заключается в отсутствии проверки сети или интерфейса назначения.*
Параметры правил аутентификации	*Можно выделить следующие параметры правил аутентификации (меню User Authentication→ User Authentication Rules→Add→ User Authentication Rule):* *- агент аутентификации (Authentication Agent).Это тип трафика для аутентификации. Возможен один из следующих типов:* *1. HTTP – Web-подключение должно быть аутентифицировано через пользовательскую страницу по протоколу HTTP.* *2. HTTPS – Web-подключение должно быть аутентифицировано через пользовательскую страницу по протоколу HTTPS.* *3. XAuth – метод IKE-аутентификации, используется как часть реализации VPN-туннеля с IPSec. XAuth является расширением нормального IKE-обмена и предоставляет дополнение к обычной IPSec-безопасности, означающее необходимость предоставления имени пользователя и пароля при доступе по VPN-туннелю.* *При этом параметр interface не вводится при правилах XAuth-аутентификации, т.к. единственное правило с агентом XAuth будет использовано для всех IPSec-туннелей (для всех туннелей используется единственный источник аутентификации).* *4. PPP – используется специально для L2TP или PPTP-аутентификации.* *- источник аутентификации (Authentication Source).* *Задает один из следующих источников:* *1. LDAP – поиск пользователей будет происходить во внешней базе LDAP-сервера.* *2. RADIUS – используется внешний RADIUS-сервер.* *3. Disallow – эта опция явно запрещает все соединения, вызвавшие исполнение этого правила. Подобные соединения никогда не будут аутентифицированы. Правила Disallow лучше всего размещать в конце набора правил аутентификации.* *4. Local – используется локальная база пользователей межсетевого экрана.* *5. Allow – опция разрешает все соединения, вызвавшие исполнение этого правила. Поиск в базе аутентификации не проводится.*

	- интерфейс (Interface). *Обязательный для указания параметр – интерфейс источника, на котором будут аутентифицироваться подключения.* *- адрес инициатора (Originator IP).* *IP-адрес источника или сети с которой создаются новые подключения. Для XAuth PPP – это Tunnel Originator IP.* *- адрес оконечного устройства (Terminator IP).* *Конечный адрес с которым создаются новые подключения. Задается только если Authentication Agent задан параметром PPP.*
Таймауты соединений	*Правила аутентификации могут задавать следующие таймауты для сессий пользователей (вкладка Restrictions):* *- Idle Timeout.* *Задает таймаут бездействия подключения до автоматического завершения, значение по умолчанию – 1800 сек.* *- Session Timeout.* *Максимальное время длительности существования подключения.* *Если используется сервер аутентификации, то можно использовать опцию* Use timeouts received from the authentication server *для получения значений таймаутов от сервера.*
Процесс аутентификации	*Процесс аутентификации операционной системой межсетевого экрана состоит из следующих этапов:* *1. Пользователь создает новое подключение к межсетевому экрану.* *2. Межсетевой экран обнаруживает новое подключение на интерфейсе и проверяет набор правил аутентификации на наличие правила для трафика на данном интерфейсе, пришедшего из определенной сети и одного из этих типов:* *- HTTP трафик,* *- HTTPS трафик,* *- трафик IPSec-туннеля,* *- трафик L2TP-туннеля,* *- трафик PPTP-туннеля.* *3. Если правило не найдено, соединение разрешается на основе набора обычных IP Rule.* *4. Основываясь на настройках первого найденного правила аутентификации межсетевой экран делает запрос пользователю для аутентификации.* *5. Пользователь отвечает вводом идентификационной информации (обычно имя пользователя и пароль).* *6. Межсетевой экран проверяет информацию с учетом источника аутентификации, указанного в правиле аутентификации (это локальная база пользователей межсетевой экран, внешний LDAP- или RADIUS-сервер).* *7. Межсетевой экран разрешает трафик данного подключения в соответствии с успешной аутентификацией,запросом сервиса и разрешением службы набором IP Rule. Этот объект правил сети источника имеет либо разрешенную опцию* No Defined Credentials *(нет предопределенных настроек), либо альтернативно связан с группой и конкретным пользователем данной группы.* *8. При заданном ограничении по таймауту прошедший аутентификацию пользователь будет автоматически отключен после окончания этого таймаута.* *Любой пакет с IP-адреса, не прошедший аутентификацию, будет*

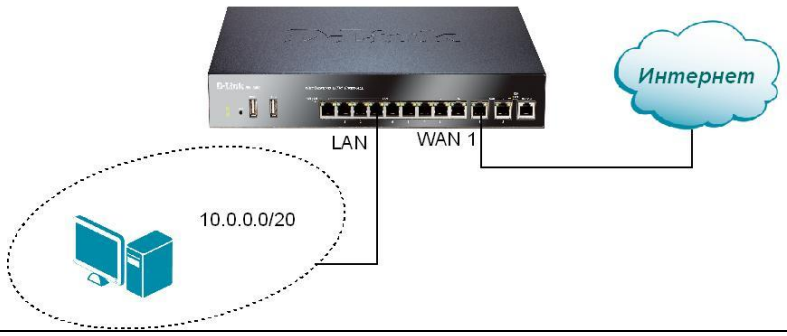
	отброшен.
Настройка использования группы.	
Описание сценария	*Некоторое количество пользователей подключено к сети 10.0.0.0/20* ***lan****-интерфейса. Необходимо ограничить доступ к сети important_net на* ***wan2****-интерфейсе одной группе пользователей (untrusted), другой группе нужно предоставить доступ к сети regular_net на* ***dmz****-интерфейсе и к сети important_net. Группа untrusted должна иметь только доступ к regular_net.*
Схема 26	
Настройка DFL-860E	
Web-интерфейс	
Создадим группы пользователей. Зайдите в меню *User Authentication→Local User Databases→Add→Local User Database*. Во вкладке *General* введите следующие параметры:	
Name	trusted
Зайдите в меню *User Authentication→Local User Databases→Add→Local User Database*. Во вкладке *General* введите следующие параметры:	
Name	untrusted
Создадим необходимые логические объекты, связанные с группами. Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	untrusted_net
Address	10.0.0.0/20
Во вкладке *User Authentication* введите следующие параметры:	
Comma-separated list of user names and groups:	untrusted
Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	trusted_net
Address	10.0.0.0/20
Во вкладке *User Authentication* введите следующие параметры:	
Comma-separated list of user names and groups:	trusted
Перейдите в меню *User Authentication→Local User Databases→trusted→вкладка Users→Add→User*. Во вкладке *General* введите:	
Username	user1
Password	P@ssw0rd

Confirm Password	P@ssw0rd
Groups	trusted
Перейдите в меню *User Authentication→Local User Databases→untrusted→ вкладка Users→Add→User*. Во вкладке *General* введите:	
Username	user2
Password	P@ssw0rd
Confirm Password	P@ssw0rd
Groups	untrusted
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	important_net
Address	192.168.120.0/24
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	regular_net
IP Address	172.17.100.0/24
Настроим порт Web-интерфейс. Перейдите в меню *System→Remote Management→вкладка Advanced Settings*. Измените следующий параметр:	
WebUI HTTP Port	81
Создание IP Rule	
Перейдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	Allow_trusted_to_wan
Action	Allow
Service	all_icmp
Source Interface	lan
Source Network	trusted_net
Destination Interface	wan2
Destination Network	important_net
Перейдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	Allow_untrusted_to_dmz
Action	Allow
Service	all_icmp
Source Interface	lan
Source Network	untrusted_net
Destination Interface	dmz
Destination Network	regular_net
Создадим правила для доступа группы trusted к сети regular_net. Перейдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	Allow_trusted_to_dmz
Action	Allow
Service	all_icmp
Source Interface	lan
Source Network	trusted_net
Destination Interface	dmz
Destination Network	regular_net
Создадим правило для прохождения аутентификации пользователей – доступ к lan_ip. Перейдите в	

меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	Allow_auth
Action	Allow
Service	all_services
SourceInterface	lan
SourceNetwork	lannet
DestinationInterface	core
Destination Network	lan_ip
Создадим правило аутентификации для trusted. Перейдите в меню *User Authentication→User Authentication Rules→Add→User Authentication Rule*. Во вкладке *General* введите:	
Name	Trusted_login
Agent	HTTP
Authentication Source	Local
Interface	lan
Originator IP	lannet
Во вкладке *Authentication Options* введите:	
Local User DB	Выберите *trusted* из списка.
Во вкладке *Agent Options* введите:	
Login Type	Выберите *HTML form* из списка.
Создадим правило аутентификации для группы untrusted. Перейдите в меню *User Authentication→User Authentication Rules→Add→User Authentication Rule*. Во вкладке *General* введите:	
Name	Untrusted_login
Agent	HTTP
Authentication Source	Local
Interface	lan
Originator IP	lannet
Во вкладке *Authentication Options* введите:	
Local User DB	Выберите *untrusted* из списка.
Во вкладке *Agent Options* введите:	
Login Type	Выберите *HTML form* из списка.
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> add Address AddressFolder labs gw-world:/>add LocalUserDatabase trusted gw-world:/> cc LocalUserDatabase trusted gw-world:/trusted>add User user1Password=P@ssw0rd Groups=trusted gw-world:/trusted> cc gw-world:/>add LocalUserDatabase untrusted gw-world:/> cc LocalUserDatabase untrusted gw-world:/untrusted> add User user2 Password=P@ssw0rd Groups=untrusted gw-world:/untrusted > cc gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address trusted_net Address=10.0.0.0/24 UserAuthGroups=trusted gw-world:/labs> add IP4Address untrusted_net Address=10.0.0.0/24 UserAuthGroups=untrusted gw-world:/labs> add IP4Address important_net Address=192.168.120.0/24	

gw-world:/labs> add IP4Address regular_net Address=172.17.100.0/24
gw-world:/labs> cc
gw-world:/>set Settings RemoteMgmtSettings WWWSrv_HTTPPort=81
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=lan SourceNetwork=labs/trusted_net DestinationInterface=wan2 DestinationNetwork=labs/important_net Name=Allow_trusted_to_wan
gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=lan SourceNetwork=labs/untrusted_net DestinationInterface=dmz DestinationNetwork=labs/regular_net Name=Allow_untrusted_to_dmz
gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=lan SourceNetwork=labs/trusted_net DestinationInterface=dmz DestinationNetwork=labs/regular_net Name=Allow_trusted_to_dmz
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=core DestinationNetwork=lan_ip Name=Allow_auth
gw-world:/1(labs)> cc
gw-world:/> add UserAuthRule AuthSource=Local Interface=lan LocalUserDB=trusted OriginatorIP=InterfaceAddresses/lannet Agent=HTTP Name=Trusted_login
gw-world:/> add UserAuthRule AuthSource=Local Interface=lan LocalUserDB=untrusted OriginatorIP=InterfaceAddresses/lannet Agent=HTTP Name=Untrusted_login
gw-world:/> activate (*подождать 3-5 секунд*)
gw-world:/>commit

<u>Упражнение</u>	Проверьте доступ пользователей из разных групп к сетям regular_net и important_net из сетей trusted_net, untrusted_net.
Пользователь user1 (trusted)	Необходимо авторизовать IP-адрес на межсетевом экране.
Internet ExplorerOC Windows	http://<lan_ip> Введите имя пользователя, пароль.
CMD OC Windows	C:\>ping 192.168.110.7 –t (рабочая станция в сети important_net) C:\>ping 172.17.100.7 –t (рабочая станция в сети regular_net)
Пользователь user2 (untrusted)	Необходимо авторизовать IP-адрес на межсетевом экране.
Internet ExplorerOC Windows	http://<lan_ip> Введите имя пользователя, пароль.
CMDOC Windows	C:\>ping 192.168.110.7 –t (рабочая станция в сети important_net) C:\>ping 172.17.100.7–t (рабочая станция в сети regular_net)
HTTP-аутентификация	
WebAuth	*Аутентификация пользователей при доступе через Web-браузер по HTTP-протоколу может быть создана на основе HTML-страниц. Обычно HTTP-аутентификация использует TCP порт 80 для Web-интерфейса удаленного управления. Перед конфигурированием аутентификации нужно изменить номер порта HTTP-протокола. Для HTTP- и HTTPS-аутентификации существует набор опций в правилах аутентификации (меню User Authentication Rules→Add→ User Authentication Rule), называемый Agent Options. Это следующие опции:* *- Login Type.* *Может быть одно из следующих значений:* *1. HTML form – пользователь представлен HTML-страницей для аутентификации, которая заполнена, данные посылаются назад межсетевому экрану через POST-запрос.* *2. Basic authentication – с этой опцией браузеру отправляется назад сообщение «401 – Authentication Required», что ведет к*

	вызову собственного диалогового окна браузера для запроса имени пользователя/пароля. Строка Realm String может быть указана, она появится в диалоговом окне браузера. *- Host Certificate, Root Certificate.* *Эти настройки необходимо ввести, если параметр Agent установлен как HTTPS. Сертификаты выбираются из уже загруженных в межсетевой экран.*
Описание сценария	*Нескольким пользователям локальной сети lannet необходимо обеспечить доступ к публично сети Интернет через* ***wan1****-интерфейс.*
Схема 27	
Настройка DFL-860E	
Web-интерфейс	
Настроим порт Web-интерфейса. Перейдите в меню *System→Remote Management→вкладка Advanced Settings*. Измените следующий параметр:	
WebUI HTTP Port	81
Создадим группы пользователей. Зайдите в меню *User Authentication→Local User Databases→Add→Local User Database*. На вкладке *General* введите следующие параметры:	
Name	inet_users
Перейдите в меню *User Authentication→Local User Databases→inet_users→вкладка Users→Add→User*. Во вкладке *General* введите:	
Username	user
Password	P@ssw0rd
Confirm Password	P@ssw0rd
Groups	inet_users
Создадим IP-объект с опцией аутентификации. Перейдите в меню *Objects→Address Book→Add→ IP4 Address*. Введите следующие параметры:	
Name	lan_auth
Address	10.0.0.0/20
Во вкладке *User Authentication* введите:	
No defined credentials	Разрешите, если не выбрана групповая аутентификация.
Создадим правило, разрешающее процесс аутентификации для доступа пользователей из локальной сети. Перейдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	Allow_auth
Action	Allow
Service	http-all
Source Interface	lan
Source Network	lannet

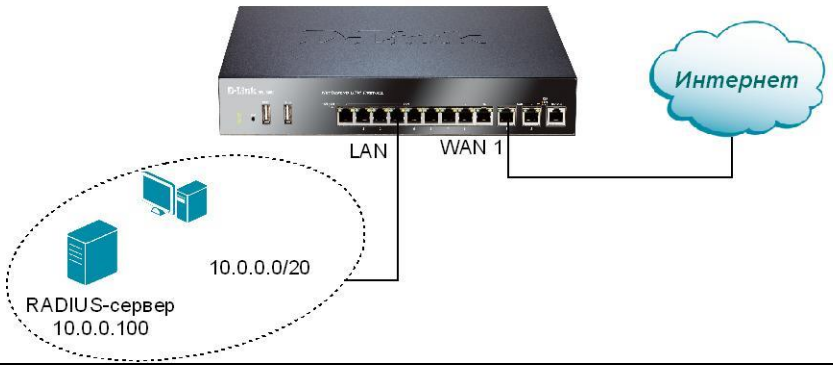
Destination Interface	core
Destination Network	lan_ip
Создадим правило, разрешающее только доверенным пользователем доступ из локальной сети. Перейдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	Allow_internet_access
Action	NAT
Service	http-all
Source Interface	lan
Source Network	lan_auth
Destination Interface	wan1
Destination Network	all-nets
Создадим правило, разрешающее DNS-запросы для URL. Перейдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	Allow_dns
Action	NAT
Service	dns-all
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets
Создадим правило аутентификации для inet_users. Перейдите в меню *User Authentication→User Authentication Rules→Add→User Authentication Rule*. Во вкладке *General* введите:	
Name	inet_user_login
Agent	HTTP
Authentication Source	Local
Interface	lan
Originator IP	lannet
Во вкладке *Authentication Options* введите:	
Local User DB	Выберите *inet_users* из списка.
Во вкладке *Agent Options* выберите:	
Login Type	*HTML form*
Командная строка (CLI)	
gw-world:/> add Address AddressFolder labs gw-world:/>set Settings RemoteMgmtSettings WWWSrv_HTTPPort=81 gw-world:/>add LocalUserDatabase inet_users gw-world:/> cc LocalUserDatabase inet_users gw-world:/inet_users> add User user Password=P@ssw0rd Groups=inet_users gw-world:/inet_users> cc gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address trusted_net Address=10.0.0.0/24 NoDefinedCredentials=Yes gw-world:/labs> cc gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=http-all SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=core DestinationNetwork=InterfaceAddresses/lan_ip Name=Allow_auth gw-world:/1(labs)> add IPRule Action=Allow Service=http-all SourceInterface=lan SourceNetwork=labs/lan_auth DestinationInterface=wan1 DestinationNetwork=all-nets Name=	

Allow_internet_access gw-world:/1(labs)> add IPRule Action=Allow Service=dns-all SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=wan1 DestinationNetwork=all-nets Name=Allow_dns gw-world:/1(labs)> cc gw-world:/> add UserAuthRule AuthSource=Local Interface=lan LocalUserDB=inet_users OriginatorIP=InterfaceAddresses/lannet Agent=HTTP Name=inet_user_login gw-world:/> activate (*подождать 3-5 секунд*) gw-world:/>commit	
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Упражнение	Проверьте доступ пользователей в Интернет через страницу авторизации межсетевого экрана. 
Internet Explorer ОС Windows	http://google.com
Настройка автоматического перехода для HTTP-аутентификации	
Описание сценария	*Необходимо настроить автоматический переход для пользователя на страницу авторизации. Таким образом, при неудачной аутентификации по IP-адресации, соединение не будет сброшено.*
Настройка DFL-860E	
Web-интерфейс	
Настроим порт Web-интерфейса. Перейдите в меню *System→Remote Management→вкладка Advanced Settings*. Измените следующий параметр:	
WebUI HTTP Port	81
Создадим группы пользователей. Зайдите в меню *User Authentication→Local User Databases→Add→Local User Database*. Во вкладке *General* введите следующие параметры:	
Name	inet_users
Перейдите в меню *User Authentication→Local User Databases→inet_users→вкладка Users→Add→User*. Во вкладке *General* введите:	
Username	user
Password	P@ssw0rd
Confirm Password	P@ssw0rd
Groups	inet_users
Создадим IP-объект с опцией аутентификации. Перейдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	lan_auth
Address	10.0.0.0/20
Во вкладке *User Authentication* введите следующие параметры:	
Comma-separated list of user names and groups:	inet_users
Создадим правило, разрешающее процесс аутентификации длядоступа пользователей из локальной сети. Перейдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	

Name	Allow_auth
Action	Allow
Service	http-all
Source Interface	lan
Source Network	lannet
Destination Interface	core
Destination Network	lan_ip
Создадим правило, разрешающее только доверенным пользователем доступ из локальной сети. Перейдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	Allow_trusted
Action	NAT
Service	http-all
Source Interface	lan
Source Network	lan_auth
Destination Interface	wan1
Destination Network	all-nets
Создадим правило, разрешающее DNS-запросы для URL. Перейдите в меню *Rules→IP Rules→ Add→IP Rule*. Во вкладке *General* введите:	
Name	Allow_dns
Action	NAT
Service	dns-all
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets
Создадим правило с действием SAT, чтобы пользователи всегда отправлялись к странице аутентификации. Перейдите в *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	SAT_auth
Action	SAT
Service	http-all
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets
Во вкладке *SAT* введите:	
Translate the	Выберите Destination IP Address
New IP Address	lan_ip
All-to-One Mapping: rewrite all destination IPs to a single IP	Поставьте галочку
Перейдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	Allow_SAT_auth
Action	Allow
Service	http-all
Source Interface	lan
Source Network	lannet

Destination Interface	wan1
Destination Network	all-nets
Создадим правило аутентификации для inet_users. Перейдите в *User Authentication→User Authentication Rules→Add→User Authentication Rule*. Во вкладке *General* введите:	
Name	inet_user_login
Agent	HTTP
Authentication Source	Local
Interface	lan
Originator IP	lannet
Во вкладке *Authentication* Options введите:	
Local User DB	Выберите *inet_users* из списка.
Во вкладке *Agent Options* выберите:	
Login Type	*HTML form*
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Примечание: Правило SAT перехватывает все неавторизованные запросы и должно быть задано в соответствии с опцией All-in-One Mapping, перенаправляя запросы на адрес 127.0.0.1, означающее ядро core (операционная система межсетевого экрана).	
Командная строка (CLI)	
gw-world:/> add Address AddressFolder labs gw-world:/> set Settings RemoteMgmtSettings WWWSrv_HTTPPort=81 gw-world:/> add LocalUserDatabase inet_users gw-world:/> cc LocalUserDatabase inet_users gw-world:/inet_users> add User user Password=P@ssw0rd Groups=inet_users gw-world:/inet_users> cc gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address lan_auth Address=10.0.0.0/24 UserAuthGroups=inet_users gw-world:/labs> cc gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=http-all SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=core DestinationNetwork=InterfaceAddresses/lan_ip Name=Allow_auth gw-world:/1(labs)> add IPRule Action=Allow Service=http-all SourceInterface=lan SourceNetwork=labs/lan_auth DestinationInterface=wan1 DestinationNetwork=all-nets Name= Allow_trusted gw-world:/1(labs)> add IPRule Action=Allow Service=dns-all SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=wan1 DestinationNetwork=all-nets Name=Allow_dns gw-world:/1(labs)> add IPRule Action=SAT Service=http-all SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=wan1 DestinationNetwork=all-nets SATTranslateToIP=InterfaceAddresses/lan_ip SATTranslate DestinationIP SATAlltoOne=YesName=SAT_auth gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=wan1 DestinationNetwork=all-nets Service=http-all SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Name=Allow_SAT_auth gw-world:/1(labs)> cc gw-world:/> add UserAuthRule AuthSource=Local Interface=lan LocalUserDB=inet_users OriginatorIP=InterfaceAddresses/lannet Agent=HTTP Name=inet_user_login gw-world:/> activate (*подождать 3-5 секунд*) gw-world:/>commit	
Упражнение	Проверьте доступ пользователей в Интернет через страницу авторизации межсетевого экрана.

Internet Explorer OC Windows	http://yandex.ru
Настройка ограничения доступа по времени с использованием расписания (Schedules)	
Расписание	*Расписание (Schedule) позволяет пользователям задавать определенный временной период в формате год-дата-время, который активирует правила только в определенное время. Любые события вне Schedule не затронут связанные правила. Если это разрешающие правила, то вне заданного интервала времени разрешения действовать не будут. Расписание может быть сконфигурировано на начальное и конечное время или различные периоды времени в течении дня.*
Описание сценария	*Настроим межсетевой экран для разрешения аутентификации пользователей только в рабочее время*
Настройка DFL-860E	
Web-интерфейс	
Создадим расписание для доступа в Интернет в рабочее время. Зайдите в меню *Objects→Schedule Profiles→Add→Schedule Profile*. Во вкладке *General* введите следующие параметры:	
Name	Office-hours
Start Date	Введите начальное время периода в формату гггг-мм-дд чч:мм:сс или на календаре установите день-время: Понедельник, 9-00.
End Date	Введите конечное время периода в формату гггг-мм-дд чч:мм:сс или на календаре выберите день-время: Пятница 18-00.
Добавьте созданное расписание (Schedule) в правила IP Rule, разрешающее пользователям доступ в Интернет.	
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Упражнение	Проверьте доступ пользователей в Интернет в рабочее и нерабочее время из сети lannet.
Internet Explorer OC Windows	http://yandex.ru
Аутентификация с помощью RADIUS-сервера	
Обзор	*При наличии в сети большого количества пользователей для их авторизации эффективнее установить один или несколько (кластер) серверов аутентификации. Remote Authentication Dial-In User Service (RADIUS) представляет собой протокол аутентификации, авторизации и учета (AAA – Authentication, Authorizationand, Accounting), используется операционной системой межсетевого экрана.*
Архитектура RADIUS	*Протокол RADIUS основывается на архитектуре клиент-сервер. ОС межсетевого экрана действует в качестве клиента RADIUS-сервера, создавая и отсылая запросы выделенному серверу. В терминах протокола RADUIS межсетевой экран выступает в качестве Network Access Server (NAS).* *Для аутентификации RADUIS-сервер получает запросы, проверяет пользователя в своей базе и возвращает ответ «accept» (разрешить) или «reject» (запретить).* *Статистика количества отправленных и полученных байтов и количества пакетов обновляется и сохраняется в течении RADUIS-сессии. Вся статистика по аутентифицированному пользователю обновляется, даже если соответствующее соединение этого пользователя закрыто.*

Сообщения об учетных записях по протоколу RADIUS	*При установке соединения новой сессии через межсетевой экран, последний посылает сообщение START (Accounting Request) соответствующему RADUIS-серверу для записи начала новой сессии с информацией об учетной записи пользователя, в ответ сервер отправляет сообщение (Accounting Respone) межсетевому экрану, подтверждающее получение первого сообщения.* *После того как пользовательская сессия завершена, (например, после истечения таймаута сессии) межсетевой экран высылает сообщение STOP (Accounting Request), содержащие статистику сессии.*
Описание сценария	*Необходимо настроить аутентификацию для доступа пользователей в Интернет на RADIUS-сервере, расположенном в **lan**-сети.*
Схема 28	

Создание необходимых объектов

Настройка RADIUS-сервера

Настройте RADIUS-сервер с IP-адресом 10.0.0.100, подключите его к **lan**-интерфейсу межсетевого экрана, сетевые настройки должны соответствовать подсети 10.0.0.0/20. Создайте тестовую учетную запись пользователя.

Настройка DFL-860E

Web-интерфейс

Создадим IP-объект с опцией аутентификации. Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:

Name	lan_auth
Address	10.0.0.0/20

Во вкладке *User Authentication* введите следующие параметры:

No Defined Credentials	Поставьте галочку

Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:

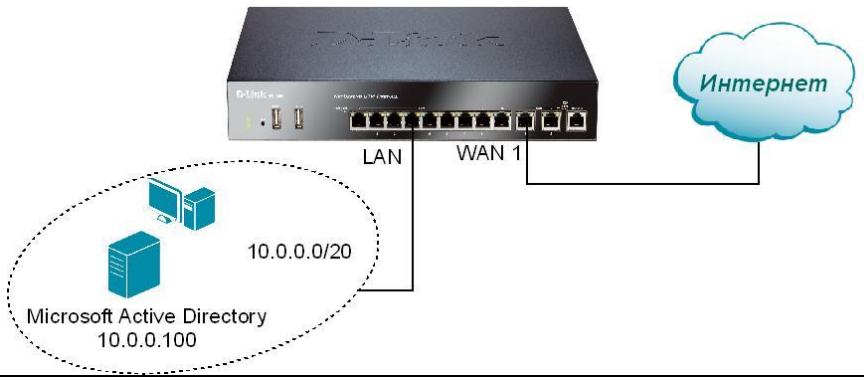
Name	radius_srv_ip
Address	10.0.0.100

Создадим объект «RADIUS-сервер». Зайдите в меню *User Authentication→External User Databases→Add→RADIUS Server*. Введите следующие параметры:

Name	radius_srv
IP Address	radius_srv_ip
Port	1812
Retry Timeout	2
Shared Secret	Введите общий ключ RADIUS-сервера

Confirm Secret	Введите общий ключ RADIUS-сервера.
Создадим правило, разрешающее процесс аутентификации для доступа пользователей из локальной сети. Перейдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	Allow_auth
Action	Allow
Service	http-all
Source Interface	lan
Source Network	lannet
Destination Interface	core
Destination Network	lan_ip
Создадим правило, разрешающее доступ из локальной сети только доверенным пользователем. Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	Allow_trusted
Action	NAT
Service	http-all
Source Interface	lan
Source Network	lan_auth
Destination Interface	wan1
Destination Network	all-nets
Создадим правило, разрешающее DNS-запросы для URL. Зайдите в *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	Allow_dns
Action	NAT
Service	dns-all
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets
Создадим правило с действием SAT, чтобы пользователи всегда отправлялись к странице аутентификации. Перейдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	SAT_auth
Action	SAT
Service	http-all
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets
Во вкладке *SAT* введите:	
Translate the	Выберите Destination IP Address
New IP Address	lan_ip
All-to-One Mapping: rewrite all destination IPs to a single IP	Поставьте галочку
Перейдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	Allow_SAT_auth
Action	Allow

Service	http-all
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets
Создадим правило аутентификации для inet_users. Перейдите в меню *User Authentication→User Authentication Rules→Add→User Authentication Rule*. Во вкладке *General* введите:	
Name	inet_user_login
Agent	HTTP
Authentication Source	RADIUS
Interface	lan
Originator IP	lannet
Во вкладке *Authentication Options* введите:	
RADIUS servers	Переместите *radius_srv* в *Selected*.
RADIUS Method	Выберите метод аутентификации PAP или CHAP.
Во вкладке *Agent Options* выберите:	
Login Type	*HTML form*
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Примечание: Правило SAT перехватывает все неавторизованные запросы и должно быть задано в соответствии с опцией All-in-One Mapping, перенаправляя запросы на адрес 127.0.0.1, означающее ядро core (операционная система межсетевого экрана).	
Командная строка (CLI)	
gw-world:/> add Address AddressFolder labs gw-world:/> set Settings RemoteMgmtSettings WWWSrv_HTTPPort=81 gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address lan_auth Address=10.0.0.0/24 NoDefinedCredentials=Yes gw-world:/labs> add IP4Address radius_srv_ip Address=10.0.0.100 gw-world:/labs> cc gw-world:/> add RadiusServer radius_srv IPAddress=labs/radius_srv_ip SharedSecret=private gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=http-all SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=core DestinationNetwork=InterfaceAddresses/lan_ip Name=Allow_auth gw-world:/1(labs)> add IPRule Action=Allow Service=http-all SourceInterface=lan SourceNetwork=labs/lan_auth DestinationInterface=wan1 DestinationNetwork=all-nets Name=Allow_trusted gw-world:/1(labs)> add IPRule Action=Allow Service=dns-all SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=wan1 DestinationNetwork=all-nets Name=Allow_dns gw-world:/1(labs)> add IPRule Action=SAT Service=http-all SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=wan1 DestinationNetwork=all-nets SATTranslateToIP=InterfaceAddresses/lan_ip SATTranslate DestinationIP SATAlltoOne=Yes Name=SAT_auth gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=wan1 DestinationNetwork=all-nets Service=http-all SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Name=Allow_SAT_auth gw-world:/1(labs)> cc gw-world:/> add UserAuthRule AuthSource=RADIUS Interface=lan OriginatorIP=InterfaceAddresses/lannet Agent=HTTP RadiusServers=radius_srv Name=inet_user_login gw-world:/> activate (*подождать 3-5 секунд*)	

gw-world:/>commit	
Упражнение	Проверьте доступ пользователей в Интернет через страницу авторизации межсетевого экрана.
Internet Explorer ОС Windows	http://yandex.ru
Аутентификация с помощью Microsoft Active Directory.	
Описание сценария	*Необходимо настроить аутентификацию для доступа пользователей в Интернет на базе Microsoft Active Directory в домене Microsoft Windows Server 2003/2008, расположенном в* ***lan****-сети.*
Схема 29	
Создание необходимых объектов	
Настройка домена Microsoft Windows Server 2003/2008	
Настройте контроллер домена Microsoft Windows Server 2003/2008 с IP-адресом 10.0.0.100, подключите его к **lan-**интерфейсу межсетевого экрана, сетевые настройки должны соответствовать подсети 10.0.0.0/20. Создайте тестовый учетную запись пользователя в домене существующей сети (например, ks.mstu.ru). Учетная запись администратора домена – admin, пароль P@ssw0rd.	
Настройка DFL-860E	
Web-интерфейс	
Создадим IP-объект с опцией аутентификации. Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	lan_auth
Address	10.0.0.0/20
Во вкладке *User Authentication* введите следующие параметры:	
No Defined Credentials	Поставьте галочку
Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	dc_ip
Address	10.0.0.100
Создадим объект «LDAP-сервер». Зайдите в меню *User Authentication→External User Databases→Add→LDAP Server*. Введите следующие параметры:	
Name	ad_srv
IP Address	dc_ip
Port	389
Retry Timeout	5
Name Attribute	SAMAccountName

Retrieve Group Membership	Поставьте галочку
Membership Attribute	MemberOf
Use Domain Name	UserNamePrefix (выберите из списка)
Base Object	DC=ks,DC=mstu,DC=ru
Administrator Account	admin
Password	Введите пароль администратора домена
Confirm Password	Введите пароль администратора домена
Domain Name	ks
Password Attribute	userPassword
Создадим правило, разрешающее процесс аутентификации для доступа пользователей из локальной сети. Перейдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	Allow_auth
Action	Allow
Service	http-all
Source Interface	lan
Source Network	lannet
Destination Interface	core
Destination Network	lan_ip
Создадим правило, разрешающее доступ из локальной сети только доверенным пользователем. Перейдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	Allow_trusted
Action	NAT
Service	http-all
Source Interface	lan
Source Network	lan_auth
Destination Interface	wan1
Destination Network	all-nets
Создадим правило, разрешающее DNS-запросы для URL. Перейдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	Allow_dns
Action	NAT
Service	dns-all
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets
Создадим правило с действием SAT, чтобы пользователи всегда отправлялись к странице аутентификации. Перейдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	SAT_auth
Action	SAT
Service	http-all
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets

Во вкладке *SAT* введите:	
Translate the	Выберите Destination IP Address
New IP Address	lan_ip
All-to-One Mapping: rewrite all destination IPs to a single IP	Поставьте галочку
Перейдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	Allow_SAT_auth
Action	Allow
Service	http-all
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets
Создадим правило аутентификации для inet_users. Перейдите в *User Authentication→User Authentication Rules→Add→User Authentication Rule*. Во вкладке *General* введите:	
Name	inet_user_login
Agent	HTTP
Authentication Source	LDAP
Interface	lan
Originator IP	lannet
Во вкладке *Authentication Options* введите:	
LDAP servers	Переместите *ad_srv* в *Selected*.
Во вкладке *Agent Options* выберите:	
Login Type	*HTML form*
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Примечание: Правило SAT перехватывает все неавторизованные запросы и должно быть задано в соответствии с опцией All-in-One Mapping, перенаправляя запросы на адрес 127.0.0.1, означающее ядро core (операционная система межсетевого экрана).	
Командная строка (CLI)	
gw-world:/> add Address AddressFolder labs gw-world:/> set Settings RemoteMgmtSettings WWWSrv_HTTPPort=81 gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address lan_auth Address=10.0.0.0/20 NoDefinedCredentials=Yes gw-world:/labs> add IP4Address dc_ip Address=10.0.0.100 gw-world:/labs> cc gw-world:/> add LDAPDatabase ad_srv IP=labs/dc_ip Port=389 Timeout=5 BaseObject=DC=ks,DC=mstu,DC=ru PassAttr=userPassword GroupsAttr=memberOf NameAttr=SAMAccountName GetGroups=Yes UserName=admin Password=P@ssw0rd gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=http-all SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=core DestinationNetwork=InterfaceAddresses/lan_ip Name=Allow_auth gw-world:/1(labs)> add IPRule Action=Allow Service=http-all SourceInterface=lan SourceNetwork=labs/lan_auth DestinationInterface=wan1 DestinationNetwork=all-nets Name=Allow_trusted gw-world:/1(labs)> add IPRule Action=Allow Service=dns-all SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=wan1 DestinationNetwork=all-nets Name=Allow_dns	

gw-world:/1(labs)> add IPRule Action=SAT Service=http-all SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=wan1 DestinationNetwork=all-nets SATTranslateToIP=InterfaceAddresses/lan_ip SATTranslate DestinationIP SATAlltoOne=Yes Name=SAT_auth gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=wan1 DestinationNetwork=all-nets Service=http-all SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Name=Allow_SAT_auth gw-world:/1(labs)> cc gw-world:/> add UserAuthRule AuthSource=LDAP Interface=lan OriginatorIP=InterfaceAddresses/lannet Agent=HTTP LDAPServers=ad_srv Name=inet_user_login gw-world:/> activate (*подождать 3-5 секунд*) gw-world:/>commit	
Упражнение	Проверьте доступ пользователей в Интернет через страницу авторизации межсетевого экрана.
Internet Explorer ОС Windows	http://yandex.ru

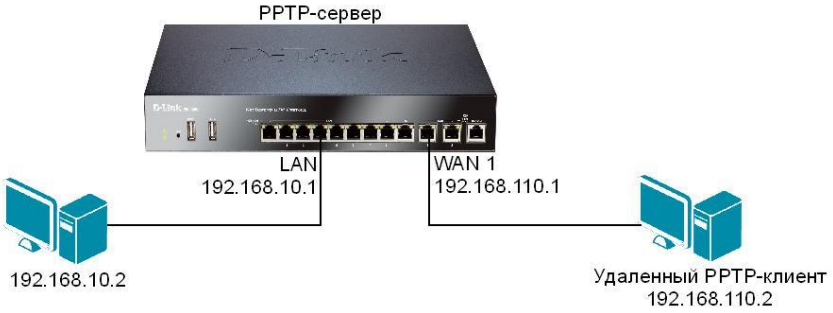
ЗАНЯТИЕ №9. Виртуальные частные сети IPSec\PPTP\L2TP\SSL VPN.

ЗАНЯТИЕ №9.1. Настройка PPTP-сервера для доступа удаленных пользователей. IPSec-туннель LAN to LAN с заранее установленным ключем совместного использования (pre-shared key). IPSec-туннель LAN to LAN с сертификатами, подписанными центром сертификации CA. IPSec-туннель LAN to LAN с самоподписанными сертификатами (self-signed certificates).

Обеспечение безопасной связи удаленных офисов и удаленных клиентов одной организации на сегодня очень актуальная задача. При прохождении трафика через сети, которым нет доверия (например, Интернет), необходимо гарантировать шифрование, проверку целостности данных, аутентификацию и отсутствие подмены сообщений. Технология VPN позволяет решить указанные задачи, архитектура IKE при максимальном шифровании делает перехват и дешифровку данных злоумышленником практически бесполезным.

Цель	Эта лабораторная работа предназначена для изучения технологии VPN.	
Оборудование	DFL-860E	3
	Рабочая станция	3
	Ethernet-кабель (патч-корд)	7
	Центр сертификации на базе Microsoft Windows Server 2003/2008 (или на базе другой программной платформы).	1
	RADIUS-сервер	1
	Домен Microsoft Windows 2003/2008	1

Описание технологии VPN	*Группа стандартов VPN (Virtual Private Network) была создана для организации защищенных соединений между разными типами устройств через незащищенные сети, а также защиты каналов связи с удаленными клиентами. Технология включает в себя ряд стандартов – IPSec, PPTP, L2TP, рекомендации по организации центров сертификации.* *VPN позволяет установить между устройствами так называемый туннель, в котором обеспечивается шифрование данных, аутентификация пользователей с помощью других протоколов (PPP, PPTP, L2TP).* *Различают два вида VPN-сценариев: соединение LAN to LAN (локальная сеть – локальная сеть) и соединение Client to LAN (клиент – локальная сеть).* *Защита VPN определяет гарантию конфиденциальности, аутентификацию и целостность данных, невозможность отказа от факта передачи данных.* *Устройства, организовывающие туннель, называют конечными точками туннеля.* *Ключи шифрования в VPN могут быть использованы как общий ключ (парольная фраза, заранее установленный ключ совместного использования) или сертификат (X.509).*
Примечание: В ходе работы преимущественно будут использованы приватные (частные) IP-адреса VPN-шлюзов, конечных точек туннелей. При создании VPN-туннелей принципиально неважна адресация в сети, через которую пробрасывается туннель. Все примеры можно сделать для случая туннелей через Интернет, для этого необходимо будет использовать	

«белые» IP-адреса в настройках удаленных VPN-шлюзов и конечных точек туннелей.	
Настройка PPTP-сервера для доступа удаленных пользователей.	
Описание сценария	*Необходимо настроить доступ удаленным пользователем к межсетевому экрану, выступающему в роли PPTP-сервера.*
Схема 30	
Настройка DFL-860E	
Web-интерфейс	
Настройте wan1-интерфейс в соответствии со схемой подключения.	
Создание необходимых объектов	
Зайдите в меню *Objects→Address Book*. Создайте новую папку *Address Folder*:	
Name	ip_pools
Создайте папке ip_pools новый *IP4 Address*. При организации туннеля один из адресов данного пула будет назначен удаленному клиенту.	
Name	pptp_ippool
IP Address	10.0.0.100-10.0.0.150
Зайдите в меню *User Authentication→Local User Databases→Add→Local User Database*:	
Name	RemoteUsers
Зайдите в меню *User Authentication→Local User Databases→RemoteUsers*. Во вкладке *Users* создайте нового пользователя *User*:	
Name	test
Password	P@ssw0rd
Confirm Password	P@ssw0rd
Настройка PPTP-сервера	
Зайдите в меню *Interfaces→PPTP/L2TP Servers→Add→PPTP/L2TP Server*. Во вкладке *General* введите следующие параметры:	
Name	pptp_server
Inner IP Address	lan_ip
Tunnel Protocol	PPTP
Outer Interface Filter	wan1
Server IP	wan1_ip
Примечание: Если внешняя сеть (WAN) настроена для DSL или DHCP, установите «any» в поле Outer Interface Filter и «wan1_ip» - в поле Server IP. ***Если же внешняя сеть настроена как Static, установите «wan» в поле Outer Interface Filter и «wan1_ip» - в поле Server IP.***	
Вкладка *PPP Parameters*:	
IP Pool	pptp_ippool (выберите из списка)

Во вкладке *Add Route* установите галочку в поле *Always select ALL interfaces, including new ones.*	
Настройка правил аутентификации пользователей	
Зайдите в меню *User Authentication→User Authentication Rules→Add→ User Authentication Rule*. Во вкладке *General* введите следующие параметры:	
Name	pptp_rule
Agent	PPP
Authentication Source	Local
Interface	pptp_server (выберите из списка созданный сервер)
Originator IP	all-nets
Terminator IP	wan1_ip
Примечание: Если внешняя сеть (WAN) настроена для DSL или DHCP, установите «wan_ip» в поле Terminator IP. Если же внешняя сеть настроена как Static, установите «wan_ip» в поле Terminator IP.	
Вкладка *Authentication Options*	
Local User DB	RemoteUsers (выберите созданную ранее базу данных).
Настройка IP-правила межсетевого экрана	
Перейдите в меню *Rules→IP Rules*. СоздайтеIP Rule Folder, во вкладке *General* введите:	
Name	remote_site
Создайте IP-правило от клиентов PPTP-сервера. Во вкладке *General* введите:	
Name	fromPPtPclients
Action	Allow
Service	all_services
Schedule	None
Source Interface	pptp_server
Source Network	pptp_ippool
Destination Interface	lan
Destination Network	lannet
Создайте IP-правило клиентам PPTP-сервера. Во вкладке *General* введите:	
Name	toPPtPclients
Action	Allow
Service	all_services
Schedule	None
Source Interface	lan
Source Network	lannet
Destination Interface	pptp_server
Destination Network	pptp_ippool
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address pptp_ippool Address=10.0.0.100-10.0.0.150 gw-world:/labs> cc gw-world:/> add LocalUserDatabase RemoteUsers gw-world:/> cc LocalUserDatabase RemoteUsers	

gw-world:/RemoteUsers> add User test Password=P@ssw0rd
gw-world:/RemoteUsers> cc
gw-world:/>add Interface L2TPServer pptp_server Interface=wan1 IPPool=labs/pptp_ippool IP=InterfaceAddresses/lan_ip ServerIP=InterfaceAddresses/wan1_ip TunnelProtocol=PPTP ProxyARPAllInterfaces=Yes
gw-world:/> add UserAuthRule Interface=pptp_server AuthSource=Local LocalUserDB=RemoteUsers OriginatorIP=all-nets Agent=PPP TerminatorIP=InterfaceAddresses/wan1_ip
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=pptp_server SourceNetwork=labs/pptp_ippool DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=fromPPtPclients
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=pptp_server DestinationNetwork=labs/pptp_ippool Name=toPPtPclients
gw-world:/1(labs)> cc
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

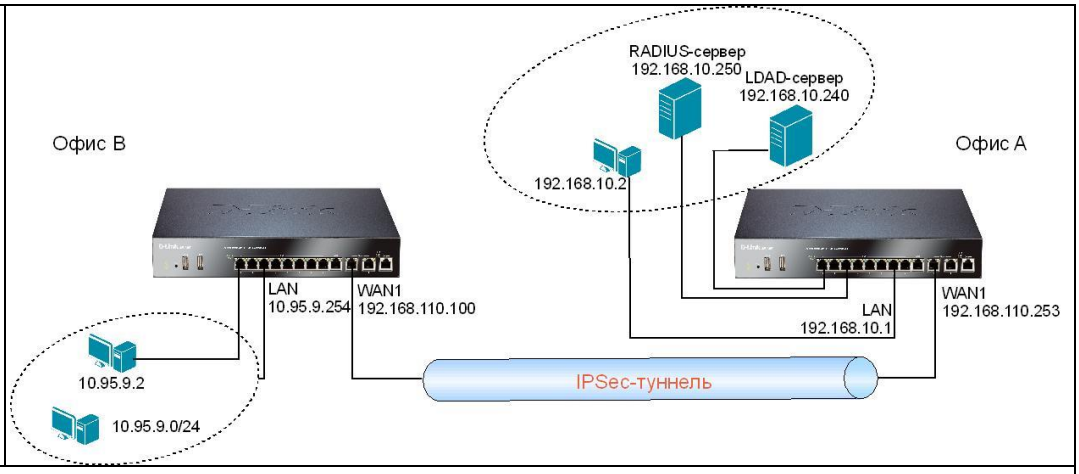
Настройка VPN-клиента в ОС Windows XP/Vista/7

1)Зайдите в сетевые подключения, выберите Создание нового подключения.
2) Выберите *Подключиться к сети на рабочем месте* (Connect to the network at my workplace).
3) Далее выберите *Подключение к виртуальной частной сети* (Virtual Private Network connection).
4) Введите имя компании (например, MSTU).
5) Введите IP-адрес устройства, к которому будет производиться подключение (в нашем примере 192.168.110.1).
6) В окне, запрашивающем имя пользователя и пароль. введите PPTPusername–test, password – P@ssw0rd.

Упражнение	Выполните подключение VPN на компьютере пользователя, находящийся в одной подсети с wan1net. Проверьте работу туннеля через сеть wan1net.
Сетевые подключения	Запустите WAN (PPTP) MSTU
CMD ОС Windows (компьютер за межсетевым экраном, подсеть lannet)	C:\>iperf –s –u –p 5001
CMD ОС Windows (компьютер пользователя, подсеть wan1net+VPN PPTP), IP-адрес 192.168.110.2	C:\>iperf – c 192.168.10.2 –u –p 5001

IPSec-туннель LAN to LAN с заранее установленным ключом совместного использования (pre-shared key). Аутентификация XAuth, локальная база данных пользователей, аутентификация Microsoft Active Directory, аутентификация RADIUS.

Описание сценария	*В первой части сценария между офисом A и офисом B необходимо настроить IPSec-туннель для безопасного соединения по VPN, аутентификация – общий ключ. Во второй части сценария дополнительно используется XAuth-аутентификация. Устройство A – XAuth-сервер, устройство B – XAuth-клиент. Базы данных пользователей используются различные – локальная, LDAP-сервер (Microsoft Active Directory), RADIUS-сервер. RADIUS-сервер и LDAP-сервер подключены к **lan**-интерфейсу устройства офиса A. Полное доменное имя – ks.mstu.ru. Администратор домена – admin.*

Схема 31	
<u>Часть 1</u>	
<u>Настройка DFL-860E</u>	
<u>Устройство офиса A</u>	
<u>Web-интерфейс</u>	
Создание необходимых объектов	
Создадим объект «Pre-shared Key». Зайдите в меню *Objects→Authentication Objects→Add→Pre-Shared Key*. Введите следующие параметры:	
Name	pre-shared_key
Выберите *Shared Secret*. Введите следующие параметры:	
Shared Secret	123456qw
Confirm Secret	123456qw
Создадим объект IP-адрес удаленного VPN-шлюза. Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	remote_gw_pool
Address	192.168.110.100-192.168.110.252
Создадим объект «удаленную подсеть за VPN-шлюзом». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	remote_net
Address	10.95.9.0/24
Создадим IPSec-туннель. Зайдите в меню *Interfaces→IPSec→Add→IPSecTunnel*. Введите следующие параметры:	
Name	ipsec_tunnel
Local Network	lannet (192.168.10.0/24)
Remote Network	remote_net
Remote Endpoint	remote_gw_pool
Encapsulation mode	Tunnel
Выберите алгоритмы IKE и IPSec:	
IKE Algorithms	Standard (выберите из списка)
IPSec Algorithms	Standard (выберите из списка)
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите pre-shared_key из списка.

Во вкладке *XAuth* введите следующие параметры:	
IKE XAuth	Off
Во вкладке *Keep-alive* введите следующие параметры:	
Keep-alive	Выберите Auto из списка
Во вкладке *Advanced* введите следующие параметры:	
Add route for remote network	Уберите галочку
Создание правил IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	outbound_rule
Action	Allow
Service	all-services
Source Interface	lan
Source Network	lannet
Destination Interface	ipsec_tunnel
Destination Network	remote_net
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	inbound_rule
Action	Allow
Service	all-services
Source Interface	ipsec_tunnel
Source Network	remote_net
Destination Interface	lan
Destination Network	lannet
Создадим правило IP Rule, разрешающее выполнение команды ping в туннеле. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	icmp_allow
Action	Allow
Service	all-icmp
Source Interface	ipsec_tunnel
Source Network	all-nets
Destination Interface	core
Destination Network	all-nets
Создание маршрута для туннеля	
Зайдите в меню *Routing→Routing Tables→main→Add→Route.* Во вкладке *General* введите:	
Interface	ipsec_tunnel
Network	remote_net
Gateway	-
Local IP address	-
Metric	10
Зайдите в *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/>add PSK pre-shared_key Type=ASCII PSKAscii=123456qw gw-world:/> add Address AddressFolder labs	

gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address remote_gw_pool Address=192.168.110.100-192.168.110.252
gw-world:/labs> add IP4Address remote_net Address=10.95.9.0/24
gw-world:/labs> cc
gw-world:/>add Interface IPsecTunnel ipsec_tunnel AuthMethod=PSK IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet PSK=pre-shared_key RemoteNetwork=labs/remote_net RemoteEndpoint=labs/remote_gw_pool KeepAlive=Auto AddRouteToRemoteNet=No EncapsulationMode=Tunnel
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=ipsec_tunnel DestinationNetwork=labs/remote_net Name=outbound_rule
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=ipsec_tunnel SourceNetwork=labs/remote_net DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule
gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnel SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=all-nets Name=icmp_allow
gw-world:/1(labs)> cc
gw-world:/>cc RoutingTable main
gw-world:/main>add Route Interface=ipsec_tunnel Network=labs/remote_net Metric=10
gw-world:/main> cc
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Настройка DFL-860E

Устройство офиса B

Web-интерфейс

Создание необходимых объектов

Создадим объект «Pre-shared Key». Зайдите в меню *Objects→Authentication Objects→Add→Pre-Shared Key*. Введите следующие параметры:

Name	pre-shared_key

Выберите *Shared Secret*.Введите следующие параметры:

Shared Secret	123456qw
Confirm Secret	123456qw

Создадим объект «IPадрес удаленного VPN-шлюза». Зайдите в *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:

Name	remote_gw
IPAddress	192.168.110.253

Создадим объект «удаленную подсеть за VPN-шлюзом». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:

Name	remote_net
IPAddress	192.168.10.0/24

Изменим подсеть lannet. Зайдите в меню *Objects→Address Book→InterfaceAddresses→lannet*. Введите следующие параметры:

Name	lannet
IPAddress	10.95.9.0/24

Изменим lan_ip. Зайдите в меню *Objects→Address Book→InterfaceAddresses→lan_ip*. Введите следующие параметры:

Name	lan_ip

IPAddress	10.95.9.254
Примечание: При изменении IP-адреса LAN необходимо зайти на интерфейс DFL по новому IP-адресу в течение 30 секунд (период времени задан по умолчанию, его можно изменить в меню System→Remote Management→Advanced Settings→Validation Timeout). Иначе настройки LAN останутся прежними.	
Создадим IPSec-туннель. Зайдите в меню *Interfaces→IPSec→Add→IPSec Tunnel*. Введите следующие параметры:	
Name	ipsec_tunnel
Local Network	lannet
Remote Network	remote_net
Remote Endpoint	remote_gw
Encapsulation mode	Tunnel
Выберите алгоритмы IKE и IPSec:	
IKE Algorithms	Standard (выберите из списка)
IPSec Algorithms	Standard (выберите из списка)
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите pre-shared_key из списка.
Во вкладке *XAuth* введите следующие параметры:	
IKE XAuth	Off
Во вкладке *Keep-alive* введите следующие параметры:	
Keep-alive	Выберите Auto из списка
Во вкладке *Advanced* введите следующие параметры:	
Add route for remote network	Уберите галочку
Создание правил IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	outbound_rule
Action	Allow
Service	all-services
Source Interface	lan
Source Network	lannet
Destination Interface	ipsec_tunnel
Destination Network	remote_net
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	inbound_rule
Action	Allow
Service	all-services
Source Interface	ipsec_tunnel
Source Network	remote_net
Destination Interface	lan
Destination Network	lannet
Создадим IP Rule, разрешающее выполнение команды ping в туннеле. Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	icmp_allow
Action	Allow

Service	all-icmp
Source Interface	ipsec_tunnel
Source Network	all-nets
Destination Interface	core
Destination Network	all-nets

Создание маршрута для туннеля

Зайдите в меню *Routing→Routing Tables→main→Add→Route.* Во вкладке *General* введите:

Interface	ipsec_tunnel
Network	remote_net
Gateway	-
Local IP address	-
Metric	10

Зайдите в *Configuration* и выберите *Save and Activate*.

Примечание: Общий ключ и настройки алгоритмов IKE и IPSec должны быть одинаковыми на устройствах.

Командная строка (CLI)

```
gw-world:/>add PSK pre-shared_key Type=ASCII PSKAscii=123456qw
gw-world:/> add Address AddressFolder labs
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address remote_gw Address=192.168.110.253
gw-world:/labs> add IP4Address remote_net Address=remote_net
gw-world:/labs> cc
gw-world:/> set Address IP4Address InterfaceAddresses/lannet Address=10.95.9.0/24
gw-world:/> set Address IP4Address InterfaceAddresses/lan_ip Address=10.95.9.254
gw-world:/>add Interface IPsecTunnel ipsec_tunnel AuthMethod=PSK IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet PSK=pre-shared_key RemoteNetwork=labs/remote_net RemoteEndpoint=labs/remote_gw_pool KeepAlive=Auto AddRouteToRemoteNet=No EncapsulationMode=Tunnel
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=ipsec_tunnel DestinationNetwork=labs/remote_net Name=outbound_rule
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=ipsec_tunnel SourceNetwork=labs/remote_net DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule
gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnel SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=all-nets Name=icmp_allow
gw-world:/1(labs)> cc
gw-world:/>cc RoutingTable main
gw-world:/main>add Route Interface=ipsec_tunnel Network=labs/remote_net Metric=10
gw-world:/main> cc
gw-world:/> activate (подождать 3-5 секунд)
gw-world:/>commit
```

Упражнение	Проверьте работоспособность туннеля.

Зайдите в меню *Status→IPSec→ipsec_tunnel.* Уточните статус соединения IPSec SAs.

Запустите команду ping (бесконечно) с хостов, подключенных к **lan-**интерфейсам межсетевых экранов A и B. Зайдите в меню *Status→IPSec→ipsec_tunnel.* Уточните скорость трафика в туннеле.

CMD Windows (устройство A)	C:\>ping 10.95.9.254 –t –l 1400
CMD Windows (устройство B)	C:\>ping 192.168.10.1 –t –l 1400
Устранение возможных проблем	Если туннель не был создан устройствами, решите возникшую проблему с помощью описанных ниже диагностических средств.
Проверьте корректность физических подключений устройств, работоспособность патч-кордов, индикацию на устройствах. Включите режим отладки:	
SSH CLI (Console CLI) Устройство A	gw-world:/>ikesnoop –on<IP-адрес удаленного VPN-шлюза>
SSH CLI (Console CLI) Устройство B	gw-world:/>ikesnoop –on<IP-адрес удаленного VPN-шлюза>
На устройствах зайдите в меню *Status→IPSec→ipsec_tunnel.* Проверьте корректность настроек туннелей, уточните статус SA для фазы 1 и фазы 2.	
На устройствах зайдите в меню *Status→Logging* или просмотрите лог-сообщения на syslog-сервере, настроенном для работы с межсетевыми экранами.	
Выполните настройку туннелей с простейшими параметрами аутентификации – общим секретом, используйте стандартные (заданные по умолчанию) настройки для алгоритмов IKE и IPSec, режимов IKE, работы с NAT-T, и не используйте пользовательские настройки для XAuth, IKE Config Mode Pool, PFS, ID, Local ID Type. После того, как туннель с этими упрощенными стандартными настройками будет установлен устройствами, измените его параметры в соответствии с особенностями задания в данном сценарии.	
Часть 2 Настройка XAuth	
Настройка DFL-860E	
Устройство офиса A	
Web-интерфейс	
Создание необходимых объектов	
Создадим объект «IP-адрес RADIUS-сервера». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	radius_srv_ip
Address	192.168.10.250
Создадим объект IP-адрес LDAP-сервера. Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	ldap_srv_ip
Address	192.168.10.240
Создадим объект «RADIUS-сервер». Зайдите в *User Authentication→External User Databases→Add→RADIUS Server.* Введите следующие параметры:	
Name	radius_srv
IP Address	radius_srv_ip
Port	1812
Retry Timeout	2
Shared Secret	Введите общий секрет RADIUS-сервера.
Confirm Secret	Введите общий секрет RADIUS-сервера.
Создадим объект «LDAP-сервер». Зайдите в *User Authentication→External User Databases→Add→LDAP Server.* Введите следующие параметры:	
Name	ldap_srv
IP Address	ldap_srv_ip

Port	389
Retry Timeout	5
Name Attribute	SAMAccountName
Retrieve Group Membership	Поставьте галочку
Membership Attribute	MemberOf
Use Domain Name	Username Prefix (выберите из списка)
Base Object	DC=ks,DC=mstu,DC=ru
Administrator Account	admin
Password	Введите пароль администратора домена.
Confirm Password	Введите пароль администратора домена.
Domain Name	ks
Password Attribute	userPassword
Отредактируйте IPSec-туннель. Зайдите в меню *Interfaces→IPSec→ipsec_tunnel.*	
Во вкладке *XAuth* введите следующие параметры:	
IKE XAuth	Require IKE XAuth user authentication for inbound IPsec tunnels
Вариант 1. Аутентификация XAuth, локальная база данных пользователей.	
Создадим локальную базу пользователей. Перейдите в меню *User Authentication→Local User Databases→Add→Local User Database*. Во вкладке *General* введите:	
Name	RemoteUsers
Перейдите в меню *User Authentication→Local User Databases→RemoteUsers→вкладка Users→Add→User*. Во вкладке *General* введите:	
Username	user1
Password	P@ssw0rd
Confirm Password	P@ssw0rd
Groups	RemoteUsers
Перейдите в меню *User Authentication→Local User Databases→RemoteUsers→ вкладка Users→Add→User*. Во вкладке *General* введите:	
Username	user2
Password	P@ssw0rd
Confirm Password	P@ssw0rd
Groups	RemoteUsers
Создайте правило аутентификации пользователя. Перейдите в меню *User Authentication→User Authentication Rules→Add→User Authentication Rule*. Во вкладке *General* введите:	
Name	remote_users_rule
Agent	XAUTH
Authentication Source	Local
Originator IP	all-nets
Во вкладке *Authentication Options* введите:	
Local User DB	Выберите из списка RemoteUsers.
Вариант 2. Аутентификация XAuth, аутентификация на внешнем RADIUS-сервере.	
Создайте правило аутентификации пользователя. Перейдите в меню *User Authentication→User Authentication Rules→Add→User Authentication Rule*. Во вкладке *General* введите:	
Name	remote_users_rule
Agent	XAUTH

Authentication Source	RADIUS
Originator IP	all-nets
Во вкладке *Authentication Options* введите:	
RADIUS servers	Переместите radius_srv из списка Available в список Selected.
Вариант 3. Аутентификация XAuth, аутентификация на внешнем LDAP-сервере.	
Создайте правило аутентификации пользователя. Перейдите в меню *User Authentication→User Authentication Rules→Add→User Authentication Rule*. Во вкладке *General* введите:	
Name	remote_users_rule
Agent	XAUTH
Authentication Source	LDAP
Originator IP	all-nets
Во вкладке *Authentication Options* введите:	
LDAP servers	Переместите ldap_srv из списка Available в список Selected.
Примечание: 1. На устройстве, выступающем в качестве сервера XAuth-аутентификации, может быть выбран какой-нибудь один источник аутентификации, правило аутентификации с агентом XAUTH будет действовать на все туннели, в которых используется XAuth-аутентификация. ***2. В остальных сценариях IPSec-туннелей также можно использовать дополнительную XAuth-аутентификацию совместно с аутентификацией по общему ключу и сертификатам.*** ***3. XAuth-аутентификация работает на входящих к серверу XAuth-туннелях, поэтому конечную точку туннеля на устройстве А явно указывать не надо, она задается диапазоном адресов.***	
Командная строка (CLI)	
gw-world:/>add PSK pre-shared_key Type=ASCII PSKAscii=123456qw gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address remote_gw_pool Address=192.168.110.100-192.168.110.254 gw-world:/labs> add IP4Address remote_net Address=10.95.9.0/24 gw-world:/labs> add IP4Address radius_srv_ip Address=192.168.10.250 gw-world:/labs> add IP4Address ldap_srv_ip Address=192.168.10.240 gw-world:/labs> cc gw-world:/> add RadiusServer radius_srv IPAddress=labs/radius_srv_ip SharedSecret=private gw-world:/> add LDAPDatabase ldap_srv IP=labs/ldap_srv_ip Port=389 Timeout=5 BaseObject=DC=ks,DC=mstu,DC=ru PassAttr=userPassword GroupsAttr=memberOf NameAttr=SAMAccountName GetGroups=Yes UserName=admin Password=P@ssw0rd gw-world:/>add Interface IPsecTunnel ipsec_tunnel AuthMethod=PSK IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet PSK=pre-shared_key RemoteNetwork=labs/remote_net RemoteEndpoint=labs/remote_gw_pool KeepAlive=Auto AddRouteToRemoteNet=No XAuth=RequiredForInboundEncapsulationMode=Tunnel gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=ipsec_tunnel DestinationNetwork=labs/remote_net Name=outbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=ipsec_tunnel SourceNetwork=labs/remote_net DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnel SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=all-nets Name=icmp_allow gw-world:/1(labs)> cc gw-world:/>cc RoutingTable main	

gw-world:/main>add Route Interface=ipsec_tunnel Network=labs/remote_net Metric=10
gw-world:/main> cc

Вариант 1
gw-world:/> add LocalUserDatabase RemoteUsers
gw-world:/> cc LocalUserDatabase RemoteUsers
gw-world:/RemoteUsers> add User user1 Password=P@ssw0rd
gw-world:/RemoteUsers> add User user2 Password=P@ssw0rd
gw-world:/RemoteUsers> cc
gw-world:/> add UserAuthRule AuthSource=Local LocalUserDB=RemoteUsers OriginatorIP=all-nets Agent=XAUTHName=remote_users_rule

Вариант 2
gw-world:/> add UserAuthRule AuthSource=RADIUS OriginatorIP=all-nets Agent=XAUTHRadiusServers=radius_srv Name=remote_users_rule

Вариант 3
gw-world:/> add UserAuthRule AuthSource=LDAP OriginatorIP=all-nets Agent=XAUTHLDAPServers=ldap_srv Name=remote_users_rule

gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Настройка DFL-860E

Устройство офиса B

Web-интерфейс

Создание необходимых объектов

Отредактируйте IPSec-туннель. Зайдите в меню *Interfaces→IPSec→ipsec_tunnel.*

Во вкладке *XAuth* введите следующие параметры:

Pass username and password to peer via IKE XAuth, if the remote gateway requires it	Введите имя пользователя и пароль для XAuth-аутентификации.

Командная строка (CLI)

gw-world:/>add PSK pre-shared_key Type=ASCII PSKAscii=123456qw
gw-world:/> add Address AddressFolder labs
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address remote_gw Address=192.168.110.253
gw-world:/labs> add IP4Address remote_net Address=remote_net
gw-world:/labs> cc
gw-world:/> set Address IP4Address InterfaceAddresses/lannet Address=10.95.9.0/24
gw-world:/> set Address IP4Address InterfaceAddresses/lan_ip Address=10.95.9.254
gw-world:/>add Interface IPsecTunnel ipsec_tunnel AuthMethod=PSK IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet PSK=pre-shared_key RemoteNetwork=labs/remote_net RemoteEndpoint=labs/remote_gw_pool KeepAlive=Auto AddRouteToRemoteNet=No XAuth=PassToPeerGateway XAuthUsername=user XAuthPassword=P@ssw0rd EncapsulationMode=Tunnel
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=ipsec_tunnel DestinationNetwork=labs/remote_net Name=outbound_rule

gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=ipsec_tunnel SourceNetwork=labs/remote_net DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule
gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnel SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=all-nets Name=icmp_allow
gw-world:/1(labs)> cc
gw-world:/>cc RoutingTable main
gw-world:/main>add Route Interface=ipsec_tunnel Network=labs/remote_net Metric=10
gw-world:/main> cc
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Упражнение	Проверьте работоспособность туннеля.

Зайдите в меню *Status→IPSec→ipsec_tunnel*. Уточните статус соединения IPSec SAs.

Запустите команду ping (бесконечно) с хостов, подключенных к **lan-**интерфейсам межсетевых экранов A и B. Зайдите в меню *Status→IPSec→ipsec_tunnel*. Уточните скорость трафика в туннеле.

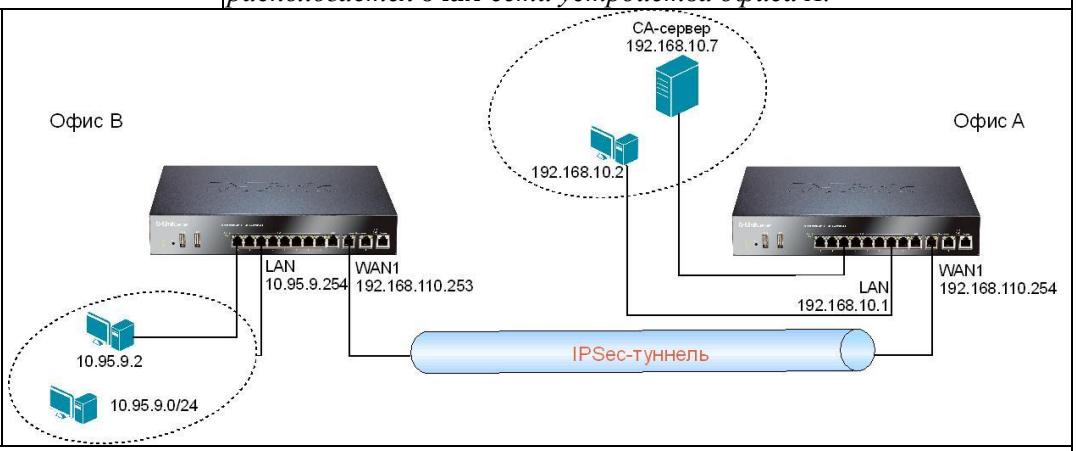
CMD Windows (устройство A)	C:\>ping 10.95.9.254 –t –l 1400
CMD Windows (устройство B)	C:\>ping 192.168.10.1 –t –l 1400

Проверьте работу механизма XAuth для входящих туннелей к устройству A (центральный офис). Укажите на устройстве B неверные параметры аутентификации XAuth-клиента. Удалите созданную SA, проверьте состояние туннеля.

IPSec-туннель LAN to LAN с сертификатами, подписанными центром сертификации CA.

Описание сценария	*Между офисом A и офисом B необходимо настроить IPSec-туннель для безопасного соединения по VPN, аутентификация – центр сертификации CA. Сервер CA (например, внутренний сервер компании dc1.ks.ru) имеет IP-адрес 192.168.10.7, располагается в* ***lan****-сети устройства офиса A.*

Схема 32



Создание необходимых объектов

Microsoft Windows Server 2003/2008

Создайте два набора подписанных CA-сертификатов с помощью CA центра сертификации Microsoft Windows Server 2003/2008.
Зайдите на сервер (в нашем примере: http://dc1.ks.ru/certsrv), выберите опцию *Загрузить CA сертификат*. Сохраните сертификат под именем CA_cert.cer.
Создайте запрос к CA-серверу для генерации клиентских сертификатов.

Зайдите http://dc1.ks.ru/certsrv, выберите опцию *Расширенный запрос сертификата*, введите следующие параметры:	
Name	Ivan Inanov
E-Mail	ivanov@company.com
Company	MSTU
Department	IT
City	Moscow
Type of certificate needed	IPSec (Offline request)
Key Option	Выберите Create new key set
CSP	Microsoft Edvanced Cryptographic Provider v1.0
Key Usage	Both
Key Size	1024
Automatic Key Container Name	Выберите из списка
Mark keys as exportable	Поставьте галочку
Создайте сертификат шлюза. Зайдите http://dc1.ks.ru/certsrv, выберите опцию *Расширенный запрос сертификата*, введите следующие параметры:	
Name	gw_cert
Company	MSTU
Department	HQ
City	Moscow
Typeofcertificateneeded	IPSec (Offline request)
Key Option	Выберите Create new key set
CSP	Microsoft Edvanced Cryptographic Provider v1.0
Key Usage	Both
Key Size	1024
Automatic Key Container Name	Выберите из списка
Mark keys as exportable	Поставьте галочку
Сохраните файлы сертификатов через опцию экспорт сертификатов в формате **.pfx**. Конвертируйте тип сертификатов в форматы **.cer** и **.key**. Можно воспользоваться программой OpenSSL 0.9.8k или аналогичной программой работы с сертификатами X.509.	
Настройка DFL-860E	
Устройство офиса А	
Web-интерфейс	
Создание необходимых объектов	
Импортируйте наборы созданных сертификатов (корневой сертификат CA, сертификат шлюза – CA_cert.cer, gw_cert.cer, gw_cert.key). Зайдите в меню *Objects→Authentication Objects→Add→Certificate.* Введите следующие параметры:	
Name	CA_cert
Upload a remove certificate.	Выберите эту опцию и укажите путь к файлам сертификатов.
Зайдите в *Objects→Authentication Objects→Add→Certificate.* Введите следующие параметры:	
Name	gw_cert
Upload X.509 Certificate.	Выберите эту опцию и укажите путь к файлам сертификатов
Создадим объект «IP-адрес удаленного VPN-шлюза». Зайдите в *Objects→Address*	

Book→Add→IP4 Address. Введите следующие параметры:	
Name	remote_gw
Address	192.168.110.253
Создадим объект «удаленную подсеть за VPN-шлюзом». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote_net
Address	10.95.9.0/24
Создадим IPSec-туннель. Зайдите в меню *Interfaces→IPSec→Add→IPSec Tunnel.* Введите следующие параметры:	
Name	ipsec_tunnel
Local Network	lannet
Remote Network	remote_net
Remote Endpoint	remote_gw
Encapsulation mode	Tunnel
Выберите алгоритмы IKE и IPSec:	
IKE Algorithms	Standard (выберите из списка)
IPSec Algorithms	Standard (выберите из списка)
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите X.509 Certificate из списка
Root Certificate (s)	Переместите CA_cert из списка Available в список Selected.
Gateway Certificate	Переместите gw_cert из списка Available в список Selected.
Во вкладке *Keep-alive* введите следующие параметры:	
Keep-alive	Выберите Auto из списка
Во вкладке *Advanced* введите следующие параметры:	
Add route for remote network	Уберите галочку
Пример создания объекта стороннего CA-сервера на межсетевом экране.	
Зайдите в *Objects→VPN Objects→LDAP→Add→LDAP Server.* Во вкладке *General* введите:	
IP Address	CA_server_ip
Username	Admin (авторизация доступа на CA-сервер, если есть)
Password	P@ssw0rd (пароль доступа на CA-сервер, если есть)
Confirm Password	P@ssw0rd (пароль доступа на CA-сервер, если есть)
Port	389
Создание правил IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	outbound_rule
Action	Allow
Service	all-services
Source Interface	lan
Source Network	lannet
Destination Interface	ipsec_tunnel
Destination Network	remote_net
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	inbound_rule

Action	Allow
Service	all-services
Source Interface	ipsec_tunnel
Source Network	remote_net
Destination Interface	lan
Destination Network	lannet
Создадим IP Rule, разрешающее выполнение команды ping в туннеле. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	icmp_allow
Action	Allow
Service	all-icmp
Source Interface	ipsec_tunnel
Source Network	all-nets
Destination Interface	core
Destination Network	all-nets
Создание маршрута для туннеля	
Зайдите в меню *Routing→Routing Tables→Add→Routing Table.* Во вкладке *General* введите:	
Name	labs
Ordering	First (выберите из списка).
Нажмите правой кнопкой мыши по созданной таблице маршрутизации *labs*, выберите *Move to top*.	
Зайдите в меню *Routing→Routing Tables→labs→Add→Route*. Во вкладке *General* введите:	
Interface	ipsec_tunnel
Network	remote_net
Gateway	-
Local IP address	-
Metric	10
Настройка интервалов проверки CRL	
Зайдите в меню *Interfaces→IPSec→Advanced Settings.* Настройте следующие параметры:	
IKE Send CRLs	Поставьте галочку
IKE CRL Validity Time	60
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Примечание: 1. Объект «сторонний CA-сервер» (Objects→VPN Objects→LDAP→Add→LDAP Server) необходимо использовать в случае наличия внешнего CA, для которого CRL-списки не включены в сертификаты шлюза устройства. ***2. Для успешной загрузки устройством CRL-списков DNS-клиент межсетевого экрана должен корректно разрешить DNS-имя сервера CA.***	
Командная строка (CLI)	
gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address remote_gw Address=192.168.110.253 gw-world:/labs> add IP4Address remote_net Address=10.95.9.0/24 gw-world:/labs> cc gw-world:/>add Interface IPsecTunnel ipsec_tunnel AuthMethod=Certificate GatewayCertificate=gw_cert RootCertificates=CA_cert IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet RemoteNetwork=labs/remote_net	

RemoteEndpoint=labs/remote_gw KeepAlive=Auto AddRouteToRemoteNet=No EncapsulationMode=Tunnel
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=ipsec_tunnel DestinationNetwork=labs/remote_net Name=outbound_rule
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=ipsec_tunnel SourceNetwork=labs/remote_net DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule
gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnel SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=all-nets Name=icmp_allow
gw-world:/1(labs)> cc
gw-world:/>add RoutingTable labs Ordering=First
gw-world:/>cc RoutingTable labs
gw-world:/labs>add Route Interface=ipsec_tunnel Network=labs/remote_net Metric=10
gw-world:/labs> cc
gw-world:/>set Settings IPsecTunnelSettings IKESendCRLs=Yes IKECRLValidityTime=60
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Настройка DFL-860E

Устройство офиса B

Web-интерфейс

Создание необходимых объектов

Импортируйте наборы созданных сертификатов (корневой сертификат, сертификат шлюза – CA_cert.cer, gw_cert.cer, gw_cert.key). Зайдите в меню *Objects→Authentication Objects→Add→Certificate.* Введите следующие параметры:

Name	CA_cert
Upload a remove certificate.	Выберите эту опцию и укажите путь к файлам сертификатов.

Зайдите в меню *Objects→Authentication Objects→Add→Certificate.* Введите следующие параметры:

Name	gw_cert
Upload X.509 certificate.	Выберите эту опцию и укажите путь к файлам сертификатов.

Создадим объект «IP-адрес удаленного VPN-шлюза». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:

Name	remote_gw
Address	192.168.110.254

Создадим объект «удаленную подсеть за VPN-шлюзом). Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:

Name	remote_net
Address	192.168.10.0/24

Создадим IPSec-туннель. Зайдите в меню *Interfaces→IPSec→Add→IPSec Tunnel.* Введите следующие параметры:

Name	ipsec_tunnel
Local Network	lannet
Remote Network	remote_net
Remote Endpoint	remote_gw
Encapsulation mode	Tunnel

Выберите алгоритмы IKE и IPSec:	
IKE Algorithms	Standard (выберите из списка)
IPSec Algorithms	Standard (выберите из списка)
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите X.509 Certificate из списка.
Root Certificate (s)	Переместите CA_cert из списка Available в список Selected.
Gateway Certificate	Переместите gw_cert из списка Available в список Selected.
Во вкладке *Keep-alive* введите следующие параметры:	
Keep-alive	Выберите Auto из списка
Во вкладке *Advanced* введите следующие параметры:	
Add route for remote network	Уберите галочку
Создание правил IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	outbound_rule
Action	Allow
Service	all-services
Source Interface	lan
Source Network	lannet
Destination Interface	ipsec_tunnel
Destination Network	remote_net
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	inbound_rule
Action	Allow
Service	all-services
Source Interface	ipsec_tunnel
Source Network	remote_net
Destination Interface	lan
Destination Network	lannet
Создадим IP Rule, разрешающее выполнение команды ping втуннеле. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	icmp_allow
Action	Allow
Service	all-icmp
Source Interface	ipsec_tunnel
Source Network	all-nets
Destination Interface	core
Destination Network	all-nets
Создание маршрута для туннеля	
Зайдите в меню *Routing→Routing Tables→Add→Routing Table.* Во вкладке *General* введите:	
Name	labs
Ordering	First (выберите из списка).
Нажмите правой кнопкой мыши по созданной таблице маршрутизации *labs*, выберите *Move to top*.	
Зайдите в меню *Routing→Routing Tables→labs→Add→Route*. Во вкладке *General* введите:	

Interface	ipsec_tunnel
Network	remote_net
Gateway	-
Local IP address	-
Metric	10

Зайдите в меню *Configuration* и выберите *Save and Activate*.

Командная строка (CLI)

```
gw-world:/> add Address AddressFolder labs
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address remote_gw Address=192.168.110.254
gw-world:/labs> add IP4Address remote_net Address=192.168.10.0/24
gw-world:/labs> cc
gw-world:/>add Interface IPsecTunnel ipsec_tunnel AuthMethod=Certificate
GatewayCertificate=gw_cert RootCertificates=CA_cert IKEAlgorithms=Standard
IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet RemoteNetwork=labs/remote_net
RemoteEndpoint=labs/remote_gw KeepAlive=Auto AddRouteToRemoteNet=No
EncapsulationMode=Tunnel
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan
SourceNetwork=InterfaceAddresses/lannet DestinationInterface=ipsec_tunnel
DestinationNetwork=labs/remote_net Name=outbound_rule
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=ipsec_tunnel
SourceNetwork=labs/remote_net DestinationInterface=lan
DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule
gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnel
SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=all-nets Name=icmp_allow
gw-world:/1(labs)> cc
gw-world:/>add RoutingTable labs Ordering=First
gw-world:/>cc RoutingTable labs
gw-world:/labs>add Route Interface=ipsec_tunnel Network=labs/remote_net Metric=10
gw-world:/labs> cc
gw-world:/> activate (подождать 3-5 секунд)
gw-world:/>commit
```

Примечание: 1. Настройки алгоритмов IKE и IPSec должны быть одинаковыми на устройствах.
2. Системное время и даты должны быть корректны, т.к. сертификаты имеют срок действия.

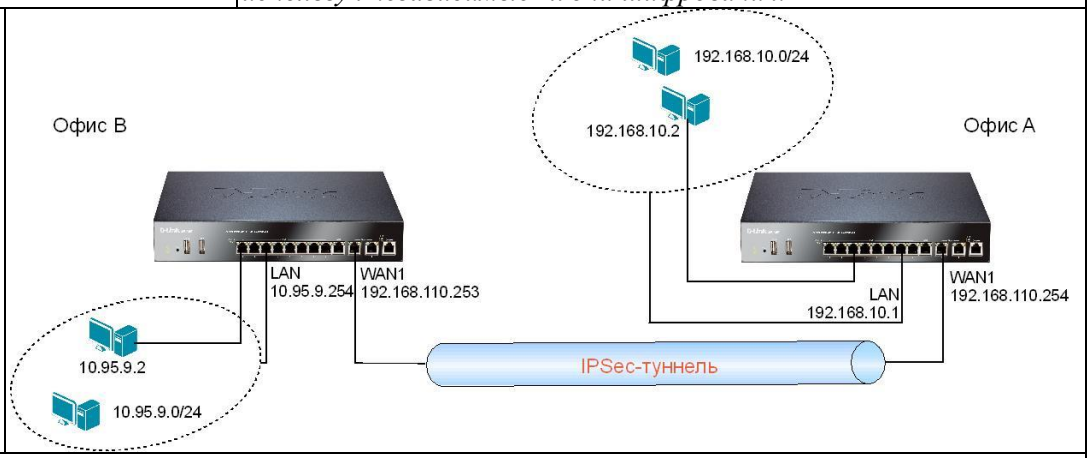
Упражнение	Проверьте работоспособность туннеля.

Зайдите в меню *Status→IPSec→ipsec_tunnel*. Уточните статус соединения IPSec SAs..

Запустите команду ping (с ключом -t) с хостов, подключенных к **lan-**интерфейсам межсетевых экранов A и B. Зайдите в меню *Status→IPSec→ipsec_tunnel*. Уточните скорость трафика в туннеле.

CMD Windows (устройство A)	C:\>ping 10.95.9.254 –t –l 1400
CMD Windows (устройство B)	C:\>ping 192.168.10.1 –t –l 1400

Отзовите сертификат шлюза на CA-сервере, проверьте корректность изменений в списках CRL:
http://dc1.ks.ru/CertEnroll/CA.crl
ldap:///CN=CA,CN=dc1,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=ks,DC=ru?certificateRevocationList?base?objectClass=cRLDistributionPoint.
Перегрузите устройства по питанию, проверьте наличие туннеля. Зайдите в меню

Status→IPSec→ipsec_tunnel.	
Просмотрите заблокированные и доверенные сертификаты на межсетевом экране.	
SSH CLI (Console CLI)	gw-world:/> certcache
Устранение возможных проблем	Если туннель не был создан устройствами, решите возникшую проблему с помощью описанных ниже диагностических средств.
Проверьте корректность физических подключений устройств, работоспособность патч-кордов, индикацию на устройствах. Включите режим отладки:	
SSH CLI (Console CLI) Устройство A	gw-world:/>ikesnoop –on<IP-адрес удаленного VPN-шлюза>
SSH CLI (Console CLI) Устройство B	gw-world:/>ikesnoop –on<IP-адрес удаленногоVPN-шлюза>
На устройствах зайдите в меню *Status→IPSec→ipsec_tunnel.* Проверьте корректность настроек туннелей, уточните статус SA для фазы 1 и фазы 2.	
На устройствах зайдите в меню *Status→Logging* или просмотрите лог-сообщения на syslog-сервере, настроенном для работы с межсетевыми экранами.	
Выполните настройку туннелей с простейшими параметрами аутентификации – общим ключом, используйте стандартные (заданные по умолчанию) настройки для алгоритмов IKE и IPSec, режимов IKE, работы с NAT-T, и не используйте пользовательские настройки для XAuth, IKE Config Mode Pool, PFS, ID, Local ID Type. После того, как туннель с этими упрощенными стандартными настройками будет установлен устройствами, измените его параметры в соответствии с особенностями задания в данном сценарии.	
IPSec-туннель LAN to LAN с самоподписанными сертификатами (self-signed certificates). Настройка PFS.	
Описание сценария	*Между офисом A и офисом B необходимо настроить IPSec-туннель для безопасного соединения по VPN, аутентификация – набор самоподписанных сертификатов. Кроме того, необходимо обеспечить защиту от взлома ключей шифрования в IKE, используя независимые ключи шифрования.*
Схема 33	
Рабочая станция с Microsoft Windows XP/Vista/7	
Создайте два самоподписанных сертификата с помощью специальной программы. Сохраните файлы сертификатов через экспорт сертификатов. Конвертируйте тип сертификатов в **.cer** и **.key** форматы. Можно воспользоваться программой OpenSSL 0.9.8k или аналогичной программой работы с сертификатами X.509.	
Настройка DFL-860E	
Устройство офиса A	
Web-интерфейс	

Создание необходимых объектов	
Импортируйте наборы созданных сертификатов (корневой сертификат, сертификат шлюза – root_cert.cer, root_cert.key, gw_cert.cer, gw_cert.key), при этом root_cert подписывает gw_cert. Зайдите в меню *Objects→Authentication Objects→Add→Certificate.* Введите следующие параметры:	
Name	root_cert
Upload X.509 certificate.	Выберите эту опцию и укажите путь к файлам сертификатов.
Зайдите в меню *Objects→Authentication Objects→Add→Certificate.* Введите следующие параметры:	
Name	gw_cert
Upload X.509 certificate.	Выберите эту опцию и укажите путь к файлам сертификатов.
Создадим объект «IPадрес удаленного VPN-шлюза». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote_gw
Address	192.168.110.253
Создадим объект «удаленную подсеть за VPN-шлюзом». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote_net
Address	10.95.9.0/24
Создадим IPSec-туннель. Зайдите в меню *Interfaces→IPSec→Add→IPSecTunnel.* Введите следующие параметры:	
Name	ipsec_tunnel
Local Network	lannet
Remote Network	remote_net
Remote Endpoint	remote_gw
Encapsulation mode	Tunnel
Выберите алгоритмы IKE и IPSec:	
IKE Algorithms	Standard (выберите из списка)
IPSec Algorithms	Standard (выберите из списка)
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите X.509 Certificate из списка.
Root Certificate (s)	Переместите root_cert из списка Available в список Selected.
Gateway Certificate	Переместите gw_cert из списка Available в список Selected.
Во вкладке *IKESettings* введите следующие параметры:	
IKE	Main, DHGroup 2 (выберите из списка)
Perfect Forward Secrecy	PFS, DHGroup 2 (выберите из списка)
Во вкладке *Keep-alive* введите следующие параметры:	
Keep-alive	Выберите Auto из списка.
Создание правил IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	outbound_rule
Action	Allow
Service	all-services
Source Interface	lan
Source Network	lannet

Destination Interface	ipsec_tunnel
Destination Network	remote_net
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	inbound_rule
Action	Allow
Service	all-services
Source Interface	ipsec_tunnel
Source Network	remote_net
Destination Interface	lan
Destination Network	lannet
Создадим IP Rule, разрешающее выполнение команды ping в туннеле. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	icmp_allow
Action	Allow
Service	all-icmp
Source Interface	ipsec_tunnel
Source Network	all-nets
Destination Interface	core
Destination Network	all-nets
Создание маршрута для туннеля	
Зайдите в меню *Routing→Routing Tables→Add→Routing Table.* Во вкладке *General* введите:	
Name	labs
Ordering	First (выберите из списка).
Нажмите правой кнопкой мыши по созданной таблице маршрутизации *labs*, выберите *Move to top*.	
Зайдите в меню *Routing→Routing Tables→labs→Add→Route*. Во вкладке *General* введите:	
Interface	ipsec_tunnel
Network	remote_net
Gateway	-
Local IP address	-
Metric	10
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address remote_gw Address=192.168.110.253 gw-world:/labs> add IP4Address remote_net Address=10.95.9.0/24 gw-world:/labs> cc gw-world:/>add Interface IPsecTunnel ipsec_tunnel AuthMethod=Certificate GatewayCertificate=gw_cert RootCertificates=root_cert IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet RemoteNetwork=labs/remote_net RemoteEndpoint=labs/remote_gw IKEMode=Main DHGroup=2 PFS=PFS PFSDHGroup=2KeepAlive=Auto AddRouteToRemoteNet=No EncapsulationMode=Tunnel gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=ipsec_tunnel	

DestinationNetwork=labs/remote_net Name=outbound_rule
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=ipsec_tunnel SourceNetwork=labs/remote_net DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule
gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnel SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=all-nets Name=icmp_allow
gw-world:/1(labs)> cc
gw-world:/>add RoutingTable labs Ordering=First
gw-world:/>cc RoutingTable labs
gw-world:/labs>add Route Interface=ipsec_tunnel Network=labs/remote_net Metric=10
gw-world:/labs> cc
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Настройка DFL-860E

Устройство офиса B

Web-интерфейс

Создание необходимых объектов

Импортируйте наборы созданных сертификатов (корневой сертификат, сертификат шлюза – root_cert.cer, root_cert.key, gw_cert.cer, gw_cert.key), при этом root_cert подписывает gw_cert. Зайдите в меню *Objects→Authentication Objects→Add→Certificate.* Введите следующие параметры:

Name	root_cert
Upload X.509 certificate.	Выберите эту опцию и укажите путь к файлам сертификатов.

Зайдите в меню *Objects→Authentication Objects→Add→Certificate.* Введите следующие параметры:

Name	gw_cert
Upload X.509 certificate.	Выберите эту опцию и укажите путь к файлам сертификатов.

Создадим объект «IPадрес удаленного VPN-шлюза». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:

Name	remote_gw
Address	192.168.110.254

Создадим объект «удаленную подсеть за VPN-шлюзом». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:

Name	remote_net
Address	192.168.10.0/24

Создадим IPSec-туннель. Зайдите в меню *Interfaces→IPSec→Add→IPSec Tunnel.* Введите следующие параметры:

Name	ipsec_tunnel
Local Network	lannet
Remote Network	remote_net
Remote Endpoint	remote_gw
Encapsulation mode	Tunnel

Выберите алгоритмы IKE и IPSec:

IKE Algorithms	Standard (выберите из списка)
IPSec Algorithms	Standard (выберите из списка)

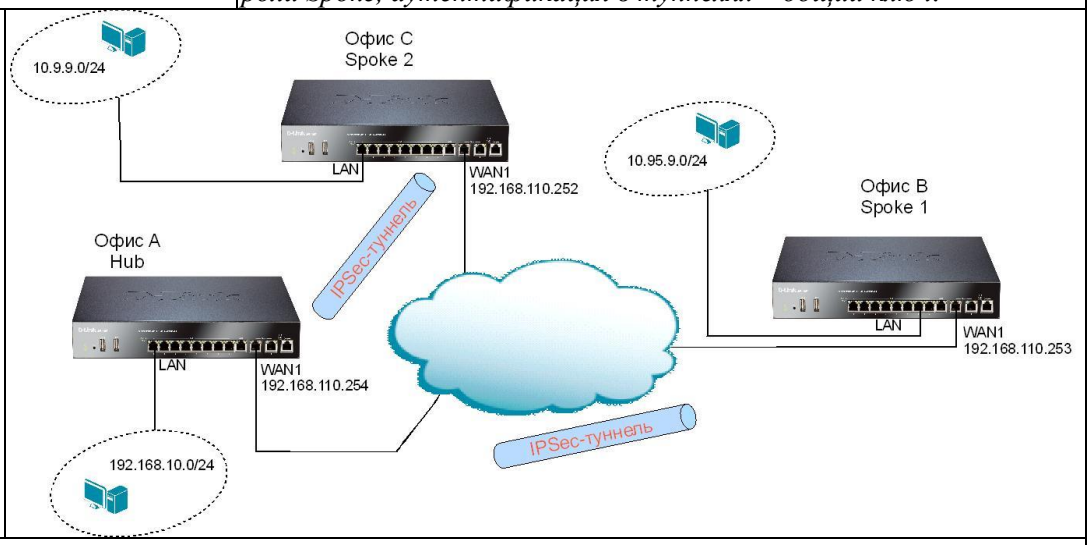
Во вкладке *Authentication* введите следующие параметры:

Authentication	Выберите X.509 Certificate из списка.
Root Certificate (s)	Переместите root_cert из списка Available в список Selected.
Gateway Certificate	Переместите gw_cert из списка Available в список Selected.
Во вкладке *IKE Settings* введите следующие параметры:	
IKE	Main, DHGroup 2 (выберите из списка)
Perfect Forward Secrecy	PFS, DHGroup 2 (выберите из списка)
Во вкладке *Keep-alive* введите следующие параметры:	
Keep-alive	Выберите Auto из списка.
Создание правил IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	outbound_rule
Action	Allow
Service	all-services
Source Interface	lan
Source Network	lannet
Destination Interface	ipsec_tunnel
Destination Network	remote_net
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	inbound_rule
Action	Allow
Service	all-services
Source Interface	ipsec_tunnel
Source Network	remote_net
Destination Interface	lan
Destination Network	lannet
Создадим IP Rule, разрешающее выполнение команды ping в туннеле. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	icmp_allow
Action	Allow
Service	all-icmp
Source Interface	ipsec_tunnel
Source Network	all-nets
Destination Interface	core
Destination Network	all-nets
Создание маршрута для туннеля	
Зайдите в меню *Routing→Routing Tables→Add→Routing Table.* Во вкладке *General* введите:	
Name	labs
Ordering	First (выберите из списка).
Нажмите правой кнопкой мыши по созданной таблице маршрутизации *labs*, выберите *Move to top*.	
Зайдите в меню *Routing→Routing Tables→labs→Add→Route*. Во вкладке *General* введите:	
Interface	ipsec_tunnel
Network	remote_net
Gateway	-

Local IP address	-
Metric	10
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address remote_gw Address=192.168.110.254 gw-world:/labs> add IP4Address remote_net Address=192.168.10.0/24 gw-world:/labs> cc gw-world:/>add Interface IPsecTunnel ipsec_tunnel AuthMethod=Certificate GatewayCertificate=gw_cert RootCertificates=root_cert IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet RemoteNetwork=labs/remote_net RemoteEndpoint=labs/remote_gw IKEMode=Main DHGroup=2 PFS=PFS PFSDHGroup=2KeepAlive=Auto AddRouteToRemoteNet=No EncapsulationMode=Tunnel gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=ipsec_tunnel DestinationNetwork=labs/remote_net Name=outbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=ipsec_tunnel SourceNetwork=labs/remote_net DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnel SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=all-nets Name=icmp_allow gw-world:/1(labs)> cc gw-world:/>add RoutingTable labs Ordering=First gw-world:/>cc RoutingTable labs gw-world:/labs>add Route Interface=ipsec_tunnel Network=labs/remote_net Metric=10 gw-world:/labs> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Примечание: 1. Настройки алгоритмов IKE и IPSec должны быть одинаковыми на устройствах. ***2. Системное время и даты должны быть корректны, т.к. сертификаты имеют срок действия.*** ***3. Если используется PFS (Perfect Forwarding Secrecy), для каждого согласования фазы 2 выполняется новый обмен Диффи-Хеллмана. PFS гарантирует, что никакие ключи не будут зависеть от любых ранее использованных ключей; никакие ключи не будут извлекаться из начального ключа. Это сделано для того, чтобы в случае рассекречивания некоторых ключей, не создавались зависимые ключи.*** ***4. При использовании режима Aggressive, некоторые параметры настройки, такие как группы Диффи-Хеллман и PFS, не могут быть согласованы, что подчеркивает важность наличия «совместимых» настроек в обеих точках.***	
Упражнение	Проверьте работоспособность туннеля.
Зайдите в меню *Status→IPSec→ipsec_tunnel*. Уточните статус соединения IPSec SAs.	
Запустите команду ping (с ключом -t) с хостов, подключенных к **lan-**интерфейсам межсетевых экранов A и B. Зайдите в меню *Status→IPSec→ipsec_tunnel*. Уточните скорость трафика в туннеле.	
CMD Windows (устройство A)	C:\>ping 10.95.9.254 –t –l 1400
CMD Windows (устройство B)	C:\>ping 192.168.10.1 –t –l 1400

<u>Устранение возможных проблем</u>	Если туннель не был создан устройствами, решите возникшую проблему с помощью описанных ниже диагностических средств.
Проверьте корректность физических подключений устройств, работоспособность патч-кордов, индикацию на устройствах. Включите режим отладки:	
SSH CLI (Console CLI) Устройство A	gw-world:/>ikesnoop –on<IP-адрес удаленного VPN-шлюза>
SSH CLI (Console CLI) Устройство B	gw-world:/>ikesnoop –on<IP-адрес удаленногоVPN-шлюза>
На устройствах зайдите в меню *Status→IPSec→ipsec_tunnel.* Проверьте корректность настроек туннелей, уточните статус SA для фазы 1 и фазы 2.	
На устройствах зайдите в меню *Status→Logging* или просмотрите лог-сообщения на syslog-сервере, настроенном для работы с межсетевыми экранами.	
Выполните настройку туннелей с простейшими параметрами аутентификации – общим ключом, используйте стандартные (заданные по умолчанию) настройки для алгоритмов IKE и IPSec, режимов IKE, работы с NAT-T, и не используйте пользовательские настройки для XAuth, IKE Config Mode Pool, PFS, ID, Local ID Type. После того, как туннель с этими упрощенными стандартными настройками будет установлен устройствами, измените его параметры в соответствии с особенностями задания в данном сценарии.	

ЗАНЯТИЕ №9.2. Технология Hub-and-Spoke. «Динамический» IPSec-туннель с заранее неизвестным адресом удаленного VPN-шлюза. Использование DynDNS для указания адреса удаленногоVPN-шлюза, настройка параметра IPSec Lifetime. Установка PPTP-туннеля.
Удаленные IPSec-клиенты с общим ключом (Pre-shared Keys). Удаленные IPSec-клиенты с сертификатами.

Технология Hub-and-Spoke на примере IPSec туннелей с заранее установленным ключом совместного использования (pre-shared key).	
Описание сценария	*Офис А является головным офисом, необходимо связать туннелями каждый с каждым офисы А, В и С. Вместо создания шести туннелей необходимо настроить три туннеля с использование механизма Hub-and-Spoke. Межсетевой экран офиса А будет выступать в роли Hub, межсетевые экраны В, С в роли Spoke, аутентификация в туннелях – общий ключ.*
Схема 34	
Настройка DFL-860E	
Устройство офиса А (Hub)	
Web-интерфейс	
Создание необходимых объектов	
Убедитесь в правильных настройках параметров интерфейсов:	
Name	lannet
IPAddress	192.168.10.0/24
Name	wan1_ip
IPAddress	192.168.110.254
Создадим объект «Pre-shared Key». Зайдите в меню *Objects→Authentication Objects→Add→Pre-Shared Key*. Введите следующие параметры:	
Name	pre-shared_key
Выберите *Shared Secret*. Введите следующие параметры:	
Shared Secret	123456qw
Confirm Secret	123456qw
Создадим объект «IP-адрес удаленного VPN-шлюза офиса В». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	

Name	remote_gwB
Address	192.168.110.253
Создадим объект «удаленную подсеть за VPN-шлюзом офиса B». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	netB
Address	10.95.9.0/24
Создадим объект «IP-адрес удаленного VPN-шлюза офиса C». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote_gwC
Address	192.168.110.252
Создадим объект «удаленную подсеть за VPN-шлюзом офиса C». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	netC
Address	10.9.9.0/24
Зайдите в меню *Objects→Address Book→Add→IP4 Group.* Введите следующие параметры:	
Name	netAB
Group members	lannet, netB переместите из *Available* в *Selected*
Зайдите в меню *Objects→Address Book→Add→IP4 Group.* Введите следующие параметры:	
Name	netAC
Group members	lannet, netC переместите из *Available* в *Selected*
Создадим IPSec-туннель в офис B. Зайдите в меню *Interfaces→IPSec→Add→IPSec Tunnel.* Введите следующие параметры:	
Name	ipsec_tunnelAB
Local Network	netAC
Remote Network	netB
Remote Endpoint	remote_gwB
Encapsulation mode	Tunnel
Выберите алгоритмы IKE и IPSec:	
IKE Algorithms	Standard (выберите из списка)
IPSec Algorithms	Standard (выберите из списка)
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите pre-shared_key из списка
Во вкладке *Keep-alive* введите следующие параметры:	
Keep-alive	Выберите Auto из списка
Во вкладке *Advanced* введите следующие параметры:	
Add route for remote network	Уберите галочку
Создадим IPSec туннель в офис C. Зайдите в меню *Interfaces→IPSec→Add→IPSec Tunnel.* Введите следующие параметры:	
Name	ipsec_tunnelAC
Local Network	netAB
Remote Network	netC
Remote Endpoint	remote_gwC
Encapsulation mode	Tunnel
Выберите алгоритмы IKE и IPSec:	
IKE Algorithms	Standard (выберите из списка)

IPSec Algorithms	Standard (выберите из списка)
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите pre-shared_key из списка
Во вкладке *Keep-alive* введите следующие параметры:	
Keep-alive	Выберите Auto из списка
Во вкладке *Advanced* введите следующие параметры:	
Add route for remote network	Уберите галочку
Примечание: Большинство функций NAT Traversal полностью автоматические, для инициации межсетевого экрана не требуется специальная настройка. Тем не менее, для отвечающих межсетевых экранов необходимо отметить два пункта: ***1. На отвечающих межсетевых экранах поле Remote Endpoint (Удаленная конечная точка) используется в качестве фильтра для IP-адреса источника полученных IKE-пакетов. Необходимо разрешить преобразование IP-адреса инициатора с помощью технологии NAT.*** ***2. При использовании общих ключей с несколькими туннелями, подключенными к одному удаленному межсетевому экрану, которые были преобразованы с помощью NAT в один и тот же адрес, важно убедиться в том, что Local ID является уникальным для каждого туннеля. Local ID может быть одним из:*** ***- Auto – в качестве локального идентификатора используется IP-адрес интерфейса исходящего трафика. Это рекомендуемая настройка, за исключением случаев, когда у двух межсетевых экранов один и тот же внешний IP-адрес.*** ***- IP – IP-адрес можно ввести вручную*** ***- DNS – DNS-адрес можно ввести вручную*** ***- Email – Email можно ввести вручную.***	
Настройка NAT Traversal	
Зайдите в меню *Interfaces→IPSec→ipsec_tunnelAB.* Введите следующие параметры во вкладке *Authentication*:	
Local ID Type	DNS
Local ID Value	OfficeAB
Зайдите в меню *Interfaces→IPSec→ipsec_tunnelAC.* Введите следующие параметры во вкладке *Authentication*:	
Local ID Type	DNS
Local ID Value	OfficeAC
Создание IP Rule для туннелей	
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	outbound_rule1
Action	Allow
Service	all-services
Source Interface	lan
Source Network	netAC
Destination Interface	ipsec_tunnelAB
Destination Network	netB
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	outbound_rule2
Action	Allow
Service	all-services
Source Interface	lan

Source Network	netAB
Destination Interface	ipsec_tunnelAC
Destination Network	netC
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	inbound_rule1
Action	Allow
Service	all-services
Source Interface	ipsec_tunnelAB
Source Network	netB
Destination Interface	lan
Destination Network	netAC
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	inbound_rule2
Action	Allow
Service	all-services
Source Interface	ipsec_tunnelAC
Source Network	netC
Destination Interface	lan
Destination Network	netAB
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	bypass_rule1
Action	Allow
Service	all-services
Source Interface	ipsec_tunnelAB
Source Network	netB
Destination Interface	ipsec_tunnelAC
Destination Network	netC
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	bypass_rule2
Action	Allow
Service	all-services
Source Interface	ipsec_tunnelAC
Source Network	netC
Destination Interface	ipsec_tunnelAB
Destination Network	netB
Создадим IP Rule, разрешающее выполнение команды ping в туннелях. Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	icmp_allow1
Action	Allow
Service	all-icmp
Source Interface	ipsec_tunnelAB
Source Network	all-nets
Destination Interface	core
Destination Network	all-nets

Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	icmp_allow2
Action	Allow
Service	all-icmp
Source Interface	ipsec_tunnelAC
Source Network	all-nets
Destination Interface	core
Destination Network	all-nets
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	icmp_bypass1
Action	Allow
Service	all-icmp
Source Interface	ipsec_tunnelAB
Source Network	all-nets
Destination Interface	ipsec_tunnelAC
Destination Network	all-nets
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	icmp_bypass2
Action	Allow
Service	all-icmp
Source Interface	ipsec_tunnelAC
Source Network	all-nets
Destination Interface	ipsec_tunnelAB
Destination Network	all-nets
Создание маршрутов для туннелей	
Зайдите в меню *Routing→Routing Tables→Add→Routing Table*. Во вкладке *General* введите:	
Name	labs
Ordering	First (выберите из списка).
Нажмите правой кнопкой мыши по созданной таблице маршрутизации *labs*, выберите *Move to top*.	
Зайдите в меню *Routing→Routing Tables→labs→Add→Route*. Во вкладке *General* введите:	
Interface	ipsec_tunnelAB
Network	netB
Gateway	-
Local IP address	-
Metric	10
Зайдите в меню *Routing→Routing Tables→labs→Add→Route*. Во вкладке *General* введите:	
Interface	ipsec_tunnelAC
Network	netC
Gateway	-
Local IP address	-
Metric	10
Зайдите в меню *Configuration* и выберите *Save and Activate*.	

Командная строка (CLI)

```
gw-world:/>add PSK pre-shared_key Type=ASCII PSKAscii=123456qw
gw-world:/> add Address AddressFolder labs
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address remote_gwBAddress=192.168.110.253
gw-world:/labs> add IP4Address remote_gwCAddress=192.168.110.252
gw-world:/labs> add IP4Address netB Address=10.95.9.0/24
gw-world:/labs> add IP4Address netC Address=10.9.9.0/24
gw-world:/labs> add IP4Group netAB Members=InterfaceAddresses/lannet,labs/netB
gw-world:/labs> add IP4Group netAC Members=InterfaceAddresses/lannet,labs/netC
gw-world:/labs> cc
gw-world:/>add Interface IPsecTunnel ipsec_tunnelAB AuthMethod=PSK IKEAlgorithms=Standard
IPsecAlgorithms=Standard LocalNetwork=labs/netAC PSK=pre-shared_key RemoteNetwork=labs/netB
RemoteEndpoint=labs/remote_gwB KeepAlive=Auto AddRouteToRemoteNet=No LocalIDType=DNS
LocalIDValue=OfficeABEncapsulationMode=Tunnel
gw-world:/>add Interface IPsecTunnel ipsec_tunnelAC AuthMethod=PSK IKEAlgorithms=Standard
IPsecAlgorithms=Standard LocalNetwork=labs/netABPSK=pre-shared_key RemoteNetwork=labs/netC
RemoteEndpoint=labs/remote_gwC KeepAlive=Auto AddRouteToRemoteNet=No LocalIDType=DNS
LocalIDValue=OfficeACEncapsulationMode=Tunnel
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan
SourceNetwork=labs/netC DestinationInterface=ipsec_tunnelAB DestinationNetwork=labs/netB
Name=outbound_rule1
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=ipsec_tunnelAB
SourceNetwork=labs/netB DestinationInterface=lan DestinationNetwork=labs/netAC
Name=inbound_rule1
gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnelAB
SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=all-nets Name=icmp_allow1
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan
SourceNetwork=labs/netBDestinationInterface=ipsec_tunnelAC DestinationNetwork=labs/netC
Name=outbound_rule2
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=ipsec_tunnelAC
SourceNetwork=labs/netC DestinationInterface=lan
DestinationNetwork=labs/netBName=inbound_rule2
gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnelAC
SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=all-nets Name=icmp_allow2
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=ipsec_tunnelAB
SourceNetwork=labs/netB DestinationInterface=ipsec_tunnelACDestinationNetwork=labs/netC
Name=bypass_rule1
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=ipsec_tunnelAC
SourceNetwork=labs/netC DestinationInterface=ipsec_tunnelAB DestinationNetwork=labs/netB
Name=bypass_rule2
gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnelAB
SourceNetwork=all-nets DestinationInterface=ipsec_tunnelAC DestinationNetwork=all-nets
Name=icmp_bypass1
gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnelAC
SourceNetwork=all-nets DestinationInterface=ipsec_tunnelAB DestinationNetwork=all-nets
Name=icmp_bypass2
gw-world:/1(labs)> cc
gw-world:/>add RoutingTable labs Ordering=First
gw-world:/>cc RoutingTable labs
gw-world:/labs>add Route Interface=ipsec_tunnelAB Network=labs/netB Metric=10
gw-world:/labs> add Route Interface=ipsec_tunnelAC Network=labs/netC Metric=10
```

gw-world:/labs> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Настройка DFL-860E	
Устройство офиса B (Spoke 1)	
Web-интерфейс	
Создание необходимых объектов	
Убедитесь в правильных настройках параметров интерфейсов:	
Name	lannet
Address	10.95.9.0/24
Name	wan1_ip
Address	192.168.110.253
Создадим объект «Pre-shared Key». Зайдите в меню *Objects→Authentication Objects→Add→Pre-Shared Key*. Введите следующие параметры:	
Name	pre-shared_key
Выберите *Shared Secret*. Введите следующие параметры:	
Shared Secret	123456qw
Confirm Secret	123456qw
Создадим объект «IP-адрес удаленного VPN-шлюза офиса A». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	remote_gwA
Address	192.168.110.254
Создадим объект «удаленную подсеть за VPN-шлюзом офиса A». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	netA
Address	192.168.10.0/24
Создадим объект «удаленную подсеть за VPN-шлюзом офиса C». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	netC
Address	10.9.9.0/24
Зайдите в меню *Objects→Address Book→Add→IP4 Group*. Введите следующие параметры:	
Name	netAC
Group members	netA, netC переместите из *Available* в *Selected*
Создадим IPSec-туннель. Зайдите в *Interfaces→IPSec→Add→IPSecTunnel*. Введите следующие параметры:	
Name	ipsec_tunnelBA
Local Network	lannet
Remote Network	netAC
Remote Endpoint	remote_gwA
Encapsulation mode	Tunnel
Выберите алгоритмы IKE и IPSec:	
IKE Algorithms	Standard (выберите из списка)
IPSec Algorithms	Standard (выберите из списка)

Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите pre-shared_key из списка
Local ID Type	DNS
Local ID Value	OfficeB
Во вкладке *Keep-alive* введите следующие параметры:	
Keep-alive	Выберите Auto из списка
Во вкладке *Advanced* введите следующие параметры:	
Add route for remote network	Уберите галочку
Создание IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	outbound_rule
Action	Allow
Service	all-services
Source Interface	lan
Source Network	lannet
Destination Interface	ipsec_tunnelBA
Destination Network	netAC
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	inbound_rule
Action	Allow
Service	all-services
Source Interface	ipsec_tunnelBA
Source Network	netAC
Destination Interface	lan
Destination Network	lannet
Создадим IP Rule, разрешающее выполнение команды ping в туннеле. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	icmp_allow
Action	Allow
Service	all-icmp
Source Interface	ipsec_tunnelBA
Source Network	all-nets
Destination Interface	core
Destination Network	all-nets
Создание маршрута для туннеля	
Зайдите в меню *Routing→Routing Tables→Add→Routing Table.* Во вкладке *General* введите:	
Name	labs
Ordering	First (выберите из списка).
Нажмите правой кнопкой мыши по созданной таблице маршрутизации *labs*, выберите *Move to top*.	
Зайдите в меню *Routing→Routing Tables→Add→Route.* Во вкладке *General* введите:	
Interface	ipsec_tunnelBA
Network	netAC
Gateway	-

Local IP address	-
Metric	10
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=192.168.110.253 gw-world:/> set IP4Address InterfaceAddresses/lannet Address=10.95.9.0/24 gw-world:/>add PSK pre-shared_key Type=ASCII PSKAscii=123456qw gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address remote_gwAAddress=192.168.110.254 gw-world:/labs> add IP4Address netA Address=192.168.10.0/24 gw-world:/labs> add IP4Address netC Address=10.9.9.0/24 gw-world:/labs> add IP4Group netAC Members=labs/netA,labs/netC gw-world:/labs> cc gw-world:/>add Interface IPsecTunnel ipsec_tunnelBA AuthMethod=PSK IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet PSK=pre-shared_key RemoteNetwork=labs/netAC RemoteEndpoint=labs/remote_gwA KeepAlive=Auto AddRouteToRemoteNet=No LocalIDType=DNS LocalIDValue=OfficeBEncapsulationMode=Tunnel gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=ipsec_tunnelBA DestinationNetwork=labs/netAC Name=outbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=ipsec_tunnelBA SourceNetwork=labs/netAC DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnelBA SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=all-nets Name=icmp_allow gw-world:/1(labs)> cc gw-world:/>add RoutingTable labs Ordering=First gw-world:/>cc RoutingTable labs gw-world:/labs>add Route Interface=ipsec_tunnelBA Network=labs/netAC Metric=10 gw-world:/labs> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Настройка DFL-860E	
Устройство офиса C (Spoke 2)	
Web-интерфейс	
Создание необходимых объектов	
Убедитесь в правильных настройках параметров интерфейсов:	
Name	lannet
Address	10.9.9.0/24
Name	wan1_ip
Address	192.168.110.252
Создадим объект «Pre-shared Key». Зайдите в меню *Objects→Authentication Objects→Add→Pre-Shared Key*. Введите следующие параметры:	
Name	pre-shared_key
Выберите *Shared Secret*. Введите следующие параметры:	

Shared Secret	123456qw
Confirm Secret	123456qw
Создадим объект «IP-адрес удаленного VPN-шлюза офиса A». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote_gwA
Address	192.168.110.254
Создадим объект «удаленную подсеть за VPN-шлюзом офиса A». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	netA
Address	192.168.10.0/24
Создадим объект «удаленную подсеть за VPN-шлюзом офиса B». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	netB
Address	10.95.9.0/24
Зайдите в меню *Objects→Address Book→Add→IP4 Group.* Введите следующие параметры:	
Name	netAB
Group members	netA, netB переместите из *Available* в *Selected*
Создадим IPSec-туннель. Зайдите в *Interfaces→IPSec→Add→IPSec Tunnel.* Введите следующие параметры:	
Name	ipsec_tunnelCA
Local Network	lannet
Remote Network	netAB
Remote Endpoint	remote_gwA
Encapsulation mode	Tunnel
Выберите алгоритмы IKE и IPSec:	
IKE Algorithms	Standard (выберите из списка)
IPSec Algorithms	Standard (выберите из списка)
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите pre-shared_key из списка.
Local ID Type	DNS
Local ID Value	OfficeC
Во вкладке *Keep-alive* введите следующие параметры:	
Keep-alive	Выберите Auto из списка
На вкладке *Advanced*введите следующие параметры:	
Add route for remote network	Уберите галочку
Создание IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	outbound_rule
Action	Allow
Service	all-services
Source Interface	lan
Source Network	lannet
Destination Interface	ipsec_tunnelCA
Destination Network	netAB

Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	inbound_rule
Action	Allow
Service	all-services
Source Interface	ipsec_tunnelCA
Source Network	netAB
Destination Interface	lan
Destination Network	lannet
Создадим IP Rule, разрешающее выполнение команды ping в туннеле. Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	icmp_allow
Action	Allow
Service	all-icmp
Source Interface	ipsec_tunnelCA
Source Network	all-nets
Destination Interface	core
Destination Network	all-nets
Создание маршрута для туннеля	
Зайдите в *Routing→Routing Tables→Add→Routing Table*. Во вкладке *General* введите:	
Name	labs
Ordering	First (выберите из списка).
Нажмите правой кнопкой мыши по созданной таблице маршрутизации *labs*, выберите *Move to top*.	
Зайдите в меню *Routing→Routing Tables→labs→Add→Route*. Во вкладке *General* введите:	
Interface	ipsec_tunnelCA
Network	netAB
Gateway	-
Local IP address	-
Metric	10
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=192.168.110.252 gw-world:/> IP4Address InterfaceAddresses/lannet Address=10.9.9.0/24 gw-world:/>add PSK pre-shared_key Type=ASCII PSKAscii=123456qw gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address remote_gwAAddress=192.168.110.254 gw-world:/labs> add IP4Address netA Address=192.168.10.0/24 gw-world:/labs> add IP4Address netB Address=10.95.9.0/24 gw-world:/labs> add IP4Group netABMembers=labs/netA,labs/netB gw-world:/labs> cc gw-world:/>add Interface IPsecTunnel ipsec_tunnelCA AuthMethod=PSK IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet PSK=pre-shared_key RemoteNetwork=labs/netAB RemoteEndpoint=labs/remote_gwA KeepAlive=Auto AddRouteToRemoteNet=No LocalIDType=DNS LocalIDValue=OfficeCEncapsulationMode=Tunnel gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan	

SourceNetwork=InterfaceAddresses/lannet DestinationInterface=ipsec_tunnelCA DestinationNetwork=labs/netAB Name=outbound_rule
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=ipsec_tunnelCA SourceNetwork=labs/netAB DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule
gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnelCA SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=all-nets Name=icmp_allow
gw-world:/1(labs)> cc
gw-world:/>add RoutingTable labs Ordering=First
gw-world:/>cc RoutingTable labs
gw-world:/labs>add Route Interface=ipsec_tunnelCA Network=labs/netAB Metric=10
gw-world:/labs> cc
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Примечание: Общий ключ и настройки алгоритмов IKE и IPSec должны быть одинаковыми на устройствах.

Упражнение	Проверьте работоспособность туннелей. Проверьте работу Hub and Spoke – зайдите с устройства B на устройство C через A.

Зайдите в меню *Status→IPSec→ipsec_tunnel.* Уточните статус соединения IPSec SA.

Запустите команду ping (с ключом -t) с хостов, подключенных к **lan-**интерфейсам межсетевых экранов A и B. Зайдите в меню *Status→IPSec→ipsec_tunnel*. Уточните скорость трафика в туннелях.

CMD Windows (устройство B)	C:\>ping 10.9.9.254 –t –l 1400
CMD Windows (устройство C)	C:\>ping 10.95.9.254 –t –l 1400
Устранение возможных проблем	Если туннель не был создан устройствами, решите возникшую проблему с помощью описанных ниже диагностических средств.

Проверьте корректность физических подключений устройств, работоспособность патч-кордов, индикацию на устройствах. Включите режим отладки:

SSH CLI (Console CLI) Устройство A	gw-world:/>ikesnoop –on<IP-адрес удаленного VPN-шлюза>
SSH CLI (Console CLI) Устройство B	gw-world:/>ikesnoop –on<IP-адресудаленногоVPN-шлюза>
SSH CLI (Console CLI) Устройство C	gw-world:/>ikesnoop –on<IP-адресудаленногоVPN-шлюза>

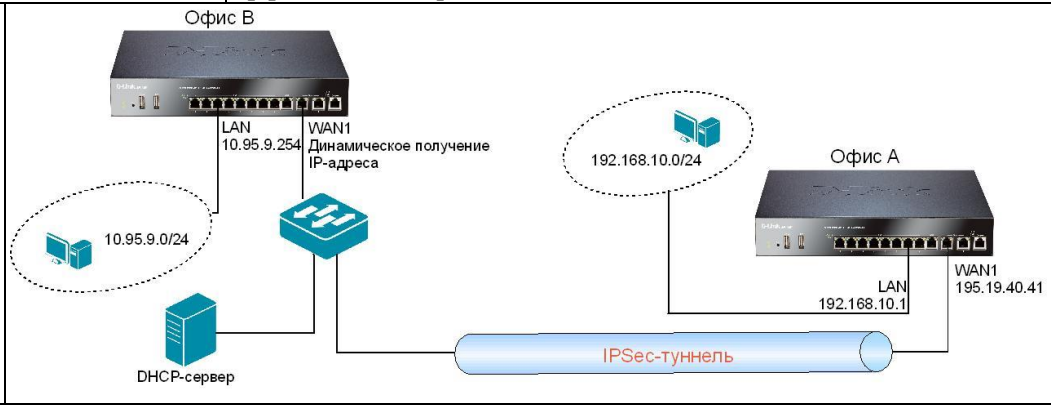
На всех устройствах зайдите в меню *Status→IPSec→ipsec_tunnel.* Проверьте корректность настроек туннелей, уточните статус SA для фазы 1 и фазы 2.

На всех устройствах зайдите в меню *Status→Logging* или просмотрите лог-сообщения на syslog-сервере, настроенном для работы с межсетевыми экранами.

Выполните настройку туннелей с простейшими параметрами аутентификации – общим ключом, используйте стандартные (заданные по умолчанию) настройки для алгоритмов IKE и IPSec, режимов IKE, работы с NAT-T, и не используйте пользовательские настройки для XAuth, IKE Config Mode Pool, PFS, ID, Local ID Type. После того, как туннель с этими упрощенными стандартными настройками будет установлен устройствами, измените его параметры в соответствии с особенностями задания в данном сценарии.

IPSec туннель LAN to LAN с заранее установленным ключом совместного использования (pre-shared key) и заранее неизвестным адресом удаленного VPN-шлюза в офисе B. Настройка режима IKE Aggressive Mode.

Описание сценария	*Между офисом A и офисом B необходимо настроить IPSec-туннель для безопасного соединения по VPN, аутентификация – общий ключ. Довольно часто возникает ситуация, при которой*

	Интернет-провайдер не может выделить статический IP-адрес для устройства в удаленном дополнительном офисе организации. Необходимо настроить туннель с заранее неизвестным адресом удаленного шлюза в офисе B. Устройство B будет инициатором установления туннеля. Необходимо настроить режим IKE Aggressive Mode для более быстрой установки соединения и эффективной передачи.
Схема 35	
Настройка DFL-860E	
Устройство офиса A	
Web-интерфейс	
Создание необходимых объектов	
Зайдите в меню *Interfaces→Ethernet→wan1*. Выберите следующие параметры:	
Enable DHCP Client	Снять галочку
Зайдите в меню *Objects→Address Book→InterfaceAddresses→wan1_ip*. Введите следующие параметры:	
Address	195.19.40.41
Зайдите в меню *Objects→Address Book→InterfaceAddresses→wan1_net*. Введите следующие параметры:	
Network	195.19.40.0/24
Зайдите в меню *Objects→Address Book→InterfaceAddresses→wan1_gw*. Введите следующие параметры:	
Default Gateway	0.0.0.0/0
Создадим объект «Pre-shared Key». Зайдите в меню *Objects→Authentication Objects→Add→Pre-Shared Key*. Введите следующие параметры:	
Name	pre-shared_key
Выберите *Shared Secret*. Введите следующие параметры:	
Shared Secret	123456qw
Confirm Secret	123456qw
Создадим объект «удаленную подсеть за VPN-шлюзом». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	remote_net
Address	10.95.9.0/24
Создадим IPSec-туннель. Зайдите в меню *Interfaces→IPSec→Add→IPSec Tunnel*. Введите следующие параметры:	
Name	ipsec_tunnel

Local Network	lannet (192.168.10.0/24)
Remote Network	remote_net
Remote Endpoint	all-nets (можно указать более узкий диапазон IP-адресов)
Encapsulation mode	Tunnel
Выберите алгоритмы IKE и IPSec:	
IKE Algorithms	Standard (выберите из списка)
IPSec Algorithms	Standard (выберите из списка)
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите pre-shared_key из списка.
Во вкладке *IKE Settings* введите следующие параметры:	
IKE	Aggressive, DHGroup 2 (выберите из списка)
Perfect Forward Secrecy	None (выберите из списка)
Во вкладке *Keep-alive* введите следующие параметры:	
Keep-alive	Выберите Auto из списка
Во вкладке *Advanced* введите следующие параметры:	
Add route for remote network	Уберите галочку
Создание IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	outbound_rule
Action	Allow
Service	all-services
Source Interface	lan
Source Network	lannet
Destination Interface	ipsec_tunnel
Destination Network	remote_net
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	inbound_rule
Action	Allow
Service	all-services
Source Interface	ipsec_tunnel
Source Network	remote_net
Destination Interface	lan
Destination Network	lannet
Создадим IP Rule, разрешающее выполнение команды ping в туннеле. Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	icmp_allow
Action	Allow
Service	all-icmp
Source Interface	ipsec_tunnel
Source Network	all-nets
Destination Interface	Core
Destination Network	all-nets
Создание маршрута для туннеля	

Зайдите в меню *Routing→Routing Tables→Add→Routing Table.* Во вкладке *General* введите:	
Name	labs
Ordering	First (выберите из списка).
Нажмите правой кнопкой мыши по созданной таблице маршрутизации *labs*, выберите *Move to top*.	
Зайдите в меню *Routing→Routing Tables→Add→Route.* Во вкладке *General* введите:	
Interface	ipsec_tunnel
Network	remote_net
Gateway	-
Local IP address	-
Metric	10
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.19.40.41 gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.19.40.0/24 gw-world:/>add PSK pre-shared_key Type=ASCII PSKAscii=123456qw gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address remote_net Address=10.95.9.0/24 gw-world:/labs> cc gw-world:/>add Interface IPsecTunnel ipsec_tunnel AuthMethod=PSK IKEAlgorithms=Standard IpsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet PSK=pre-shared_key RemoteNetwork=labs/remote_net RemoteEndpoint=all-nets KeepAlive=Auto AddRouteToRemoteNet=No IKEMode=Aggressive PFS=None DHGroup=2 EncapsulationMode=Tunnel gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=ipsec_tunnel DestinationNetwork=labs/remote_net Name=outbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=ipsec_tunnel SourceNetwork=labs/remote_net DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnel SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=all-nets Name=icmp_allow gw-world:/1(labs)> cc gw-world:/>add RoutingTable labs Ordering=First gw-world:/>cc RoutingTable labs gw-world:/labs>add Route Interface=ipsec_tunnel Network=labs/remote_net Metric=10 gw-world:/labs> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Настройка DFL-860E	
Устройство офиса B	
Web-интерфейс	
Создание необходимых объектов	
Зайдите в меню *Interfaces→Ethernet→wan1*. Отметьте Enable DHCP Client.	
Создадим объект «Pre-shared Key». Зайдите в меню *Objects→Authentication Objects→Add→Pre-*	

Shared Key. Введите следующие параметры:	
Name	pre-shared_key
Выберите *Shared Secret*. Введите следующие параметры:	
Shared Secret	123456qw
Confirm Secret	123456qw
Создадим объект «IP-адрес удаленного VPN-шлюза. Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	remote_gw
Address	195.19.40.41
Создадим объект «удаленную подсеть за VPN-шлюзом». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	remote_net
Address	192.168.10.0/24
Изменим подсеть lannet. Зайдите в меню *Objects→Address Book→lannet.* Введите следующие параметры:	
Name	lannet
Address	10.95.9.0/24
Изменим lan_ip. Зайдите в меню *Objects→Address Book→lan_ip*. Введите следующие параметры:	
Name	lan_ip
Address	10.95.9.254
Создадим IPSec-туннель. Зайдите в меню *Interfaces→IPSec→Add→IPSec Tunnel*. Введите следующие параметры:	
Name	ipsec_tunnel
Local Network	lannet
Remote Network	remote_net
Remote Endpoint	remote_gw
Encapsulation mode	Tunnel
Выберите алгоритмы IKE и IPSec:	
IKE Algorithms	Standard (выберите из списка)
IPSec Algorithms	Standard (выберите из списка)
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите pre-shared_key из списка.
Во вкладке *IKE Settings* введите следующие параметры:	
IKE	Aggressive, DHGroup 2 (выберите из списка)
Perfect Forward Secrecy	None (выберите из списка)
Во вкладке *Keep-alive* введите следующие параметры:	
Keep-alive	Выберите Auto из списка
Во вкладке *Advanced* введите следующие параметры:	
Add route for remote network	Уберите галочку
Создание IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	outbound_rule
Action	Allow
Service	all-services

Source Interface	lan
Source Network	lannet
Destination Interface	ipsec_tunnel
Destination Network	remote_net
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	inbound_rule
Action	Allow
Service	all-services
Source Interface	ipsec_tunnel
Source Network	remote_net
Destination Interface	lan
Destination Network	lannet
Создадим IP Rule, разрешающее выполнение команды ping в туннеле. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	icmp_allow
Action	Allow
Service	all-icmp
Source Interface	ipsec_tunnel
Source Network	all-nets
Destination Interface	core
Destination Network	all-nets
Создание маршрута для туннеля	
Зайдите в меню *Routing→Routing Tables→Add→R outing Table.* Во вкладке *General* введите:	
Name	labs
Ordering	First (выберите из списка).
Нажмите правой кнопкой мыши по созданной таблице маршрутизации *labs*, выберите *Move to top*.	
Зайдите в меню *Routing→Routing Tables→labs→Add→Route*. Во вкладке *General* введите:	
Interface	ipsec_tunnel
Network	remote_net
Gateway	-
Local IP address	-
Metric	10
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/>set Interface Ethernet wan1 DHCPEnabled=No gw-world:/> set IP4Address InterfaceAddresses/lan_ip Address=10.95.9.254 gw-world:/> set IP4Address InterfaceAddresses/lannet Address=10.95.9.0/24 gw-world:/>add PSK pre-shared_key Type=ASCII PSKAscii=123456qw gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address remote_net Address=192.168.10.0/24 gw-world:/labs> add IP4Address remote_gw Address=195.19.40.41 gw-world:/labs> cc gw-world:/>add Interface IPsecTunnel ipsec_tunnel AuthMethod=PSK IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet PSK=pre-shared_key	

RemoteNetwork=labs/remote_net RemoteEndpoint=labs/remote_gwKeepAlive=Auto AddRouteToRemoteNet=No IKEMode=Aggressive PFS=None DHGroup=2 EncapsulationMode=Tunnel
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=ipsec_tunnel DestinationNetwork=labs/remote_net Name=outbound_rule
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=ipsec_tunnel SourceNetwork=labs/remote_net DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule
gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnel SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=all-nets Name=icmp_allow
gw-world:/1(labs)> cc
gw-world:/>add RoutingTable labs Ordering=First
gw-world:/>cc RoutingTable labs
gw-world:/labs>add Route Interface=ipsec_tunnel Network=labs/remote_net Metric=10
gw-world:/labs> cc
gw-world:/> activate *(подождать 3-5 секнуд)*
gw-world:/>commit

Упражнение	Проверьте работоспособность туннеля.

Зайдите в меню *Status→IPSec→ipsec_tunnel.* Уточните статус соединения IPSec SA.

Запустите команду ping (с ключом -t) с хостов, подключенных к **lan-**интерфейсам межсетевых экранов A и B. Зайдите в меню *Status→IPSec→ipsec_tunnel.* Уточните скорость трафика в туннеле.

CMD Windows (устройство A)	C:\>ping 10.95.9.254 –t –l 1400
CMD Windows (устройство B)	C:\>ping 192.168.1.1 –t –l 1400
Устранение возможных проблем	Если туннель не был создан устройствами, решите возникшую проблему с помощью описанных ниже диагностических средств.

Проверьте корректность физических подключений устройств, работоспособность патч-кордов, индикацию на устройствах. Включите режим отладки:

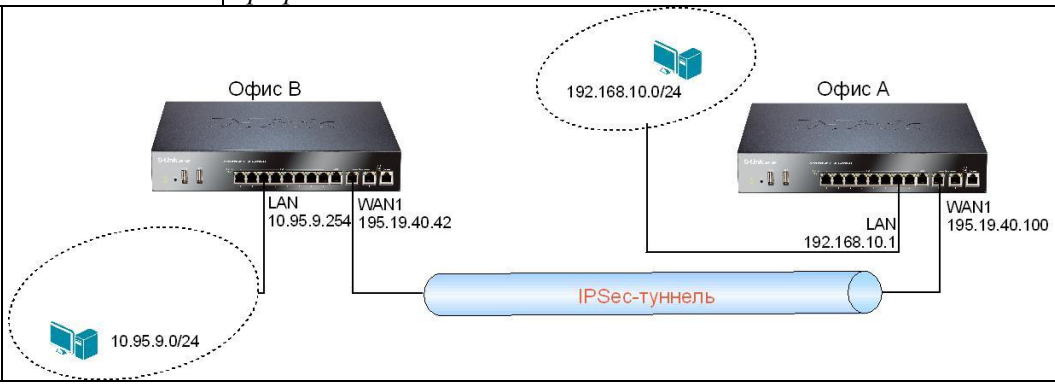
SSH CLI (Console CLI) Устройство A	gw-world:/>ikesnoop –on<IP-адрес удаленного VPN-шлюза>
SSH CLI (Console CLI) Устройство B	gw-world:/>ikesnoop –on<IP-адрес удаленногоVPN-шлюза>

На устройствах зайдите в меню *Status→IPSec→ipsec_tunnel.* Проверьте корректность настроек туннелей, уточните статус SA для фазы 1 и фазы 2.

На устройствах зайдите в меню *Status→Logging* или просмотрите лог-сообщения на syslog-сервере, настроенном для работы с межсетевыми экранами.

Выполните настройку туннелей с простейшими параметрами аутентификации – общим ключом, используйте стандартные (заданные по умолчанию) настройки для алгоритмов IKE и IPSec, режимов IKE, работы с NAT-T, и не используйте пользовательские настройки для XAuth, IKE Config Mode Pool, PFS, ID, Local ID Type. После того, как туннель с этими упрощенными стандартными настройками будет установлен устройствами, измените его параметры в соответствии с особенностями задания в данном сценарии.

IPSec-туннель LAN to LAN с заранее установленным ключом совместного использования (pre-shared key) и заранее неизвестным адресом удаленного VPN-шлюза в офисе B, заданным с помощью DynDNS. Настройка нестандартного IPSec Lifetime.

Описание сценария	*Между офисом A и офисом B необходимо настроить IPSec-туннель для безопасного соединения по VPN, аутентификация – общий ключ. При этом адрес удаленного VPN-шлюза офиса B заранее не известен, задан DNS-именем. На устройстве в офисе B IP-адрес wan1-интерфейса зарегистрирован в службе DynDNS (меню System→Misc.Clients). Необходимо установить смену IPSec-ключей через каждые 10 Мб переданного в туннеле трафика.*
Схема 36	

Настройка DynDNS

«Белый» IP-адрес устройства офиса B задан динамическим DNS-именем: ksuser1.dlinkddns.com.

Настройка DFL-860E

Устройство офиса A

Web-интерфейс

Создание необходимых объектов

Создадим объект «Pre-shared Key». Зайдите в меню *Objects→Authentication Objects→Add→Pre-Shared Key*. Введите следующие параметры:

Name	pre-shared_key

Выберите *Shared Secret*. Введите следующие параметры:

Shared Secret	123456qw
Confirm Secret	123456qw

Создадим объект «удаленную подсеть за VPN-шлюзом». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:

Name	remote_net
Address	10.95.9.0/24

Создадим IPSec-туннель. Зайдите в меню *Interfaces→IPSec→Add→IPSec Tunnel*. Введите следующие параметры:

Name	ipsec_tunnel
Local Network	lannet (192.168.10.0/24)
Remote Network	remote_net
Remote Endpoint	dns:ksuser1.dlinkddns.com
Encapsulation mode	Tunnel

Выберите алгоритмы IKE и IPSec:

IKE Algorithms	Standard (выберите из списка)
IPSec Algorithms	Standard (выберите из списка)
IPsec Lifetime	0 seconds

IPsec Lifetime	10240 kilobytes
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите pre-shared_key из списка
Во вкладке *Keep-alive* введите следующие параметры:	
Keep-alive	Выберите Auto из списка
Во вкладке *Advanced* введите следующие параметры:	
Add route for remote network	Уберите галочку
Создание IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	outbound_rule
Action	Allow
Service	all-services
Source Interface	lan
Source Network	lannet
Destination Interface	ipsec_tunnel
Destination Network	remote_net
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	inbound_rule
Action	Allow
Service	all-services
Source Interface	ipsec_tunnel
Source Network	remote_net
Destination Interface	lan
Destination Network	lannet
Создадим IP Rule, разрешающее выполнение команды ping в туннеле. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	icmp_allow
Action	Allow
Service	all-icmp
Source Interface	ipsec_tunnel
Source Network	all-nets
Destination Interface	core
Destination Network	all-nets
Создание маршрута для туннеля	
Зайдите в меню *Routing→Routing Tables→Add→Routing Table.* Во вкладке *General* введите:	
Name	labs
Ordering	First (выберите из списка).
Нажмите правой кнопкой мыши по созданной таблице маршрутизации *labs*, выберите *Move to top*.	
Зайдите в меню *Routing→Routing Tables→labs→Add→Route*. Во вкладке *General* введите:	
Interface	ipsec_tunnel
Network	remote_net
Gateway	-
Local IP address	-

Metric	10
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.19.40.100 gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.19.40.0/24 gw-world:/>add PSK pre-shared_key Type=ASCII PSKAscii=123456qw gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address remote_net Address=10.95.9.0/24 gw-world:/labs> cc gw-world:/>add Interface IPsecTunnel ipsec_tunnel AuthMethod=PSK IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet PSK=pre-shared_key RemoteNetwork=labs/remote_net RemoteEndpoint=dns:ksuser1.dlinkddns.com KeepAlive=Auto AddRouteToRemoteNet=No IPsecLifeTimeKilobytes=10240 IPsecLifeTimeSeconds=0 EncapsulationMode=Tunnel gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=ipsec_tunnel DestinationNetwork=labs/remote_net Name=outbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=ipsec_tunnel SourceNetwork=labs/remote_net DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnel SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=all-nets Name=icmp_allow gw-world:/1(labs)> cc gw-world:/>add RoutingTable labs Ordering=First gw-world:/>cc RoutingTable labs gw-world:/labs>add Route Interface=ipsec_tunnel Network=labs/remote_net Metric=10 gw-world:/labs> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Настройка DFL-860E	
Устройство офиса B	
Создание необходимых объектов	
Настройка DynDNS	
«Белый» IP-адрес устройства должен быть связан с записью ksuser1.dlinkddns.com.	
Web-интерфейс	
Создадим объект «DynDNS». Зайдите в меню *System→Misc. Clients→Add→D-Link DynDNS*. Введите следующие параметры:	
DNS Prefix	ksuser1 (имя хоста в dlinkddns.com)
Username	ksuser1
Password	Пароль к аккаунту
Confirm password	Пароль к аккаунту
Создадим объект «Pre-shared Key». Зайдите в меню *Objects→Authentication Objects→Add→Pre-Shared Key*. Введите следующие параметры:	
Name	pre-shared_key
Выберите *Shared Secret*. Введите следующие параметры:	

Shared Secret	123456qw
Confirm Secret	123456qw
Создадим объект «IP-адрес удаленного VPN-шлюза». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote_gw
Address	195.19.40.100
Создадим объект «удаленную подсеть за VPN-шлюзом». Зайдите в меню *Objects→Address Book→→Add→IP4 Address.* Введите следующие параметры:	
Name	remote_net
Address	192.168.10.0/24
Изменим подсеть lannet. Зайдите в меню *Objects→Address Book→lannet.* Введите следующие параметры:	
Name	lannet
Address	10.95.9.0/24
Изменим lan_ip. Зайдите в меню *Objects→Address Book→lan_ip.* Введите следующие параметры:	
Name	lan_ip
Address	10.95.9.254
Создадим IPSec-туннель. Зайдите в меню *Interfaces→IPSec→Add→IPSec Tunnel.* Введите следующие параметры:	
Name	ipsec_tunnel
Local Network	lannet
Remote Network	remote_net
Remote Endpoint	remote_gw
Encapsulation mode	Tunnel
Выберите алгоритмы IKE и IPSec:	
IKE Algorithms	Standard (выберите из списка)
IPSec Algorithms	Standard (выберите из списка)
IPsec Lifetime	0 seconds
IPsec Lifetime	10240 kilobytes
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите pre-shared_key из списка
Во вкладке *Keep-alive* введите следующие параметры:	
Keep-alive	Выберите Auto из списка
Во вкладке *Advanced* введите следующие параметры:	
Add route for remote network	Уберите галочку
Создание IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	outbound_rule
Action	Allow
Service	all-services
Source Interface	lan
Source Network	lannet
Destination Interface	ipsec_tunnel
Destination Network	remote_net

Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	inbound_rule
Action	Allow
Service	all-services
Source Interface	ipsec_tunnel
Source Network	remote_net
Destination Interface	lan
Destination Network	lannet
Создадим IP Rule, разрешающее выполнение команды ping в туннеле. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	icmp_allow
Action	Allow
Service	all-icmp
Source Interface	ipsec_tunnel
Source Network	all-nets
Destination Interface	core
Destination Network	all-nets
Создание маршрута для туннеля	
Зайдите в меню *Routing→Routing Tables→Add→Routing Table.* Во вкладке *General* введите:	
Name	labs
Ordering	First (выберите из списка).
Нажмите правой кнопкой мыши по созданной таблице маршрутизации *labs*, выберите *Move to top*.	
Зайдите в меню *Routing→Routing Tables→labs→Add→Route*. Во вкладке *General* введите:	
Interface	ipsec_tunnel
Network	remote_net
Gateway	-
Local IP address	-
Metric	10
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/>add Client DynDnsClientDLink DNSName=ksuser1 Username=ksuser1 Password=P@ssw0rd gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.19.40.42 gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.19.40.0/24 gw-world:/> set IP4Address InterfaceAddresses/lan_ip Address=10.95.9.254 gw-world:/> set IP4Address InterfaceAddresses/lannet Address=10.95.9.0/24 gw-world:/>add PSK pre-shared_key Type=ASCII PSKAscii=123456qw gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address remote_net Address=192.168.10.0/24 gw-world:/labs> add IP4Address remote_gw Address=195.19.40.100 gw-world:/labs> cc gw-world:/>add Interface IPsecTunnel ipsec_tunnel AuthMethod=PSK IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet PSK=pre-shared_key RemoteNetwork=labs/remote_net RemoteEndpoint=labs/remote_gwKeepAlive=Auto AddRouteToRemoteNet=No IPsecLifeTimeKilobytes=10240 IPsecLifeTimeSeconds=0	

EncapsulationMode=Tunnel
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=ipsec_tunnel DestinationNetwork=labs/remote_net Name=outbound_rule
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=ipsec_tunnel SourceNetwork=labs/remote_net DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule
gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnel SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=all-nets Name=icmp_allow
gw-world:/1(labs)> cc
gw-world:/>add RoutingTable labs Ordering=First
gw-world:/>cc RoutingTable labs
gw-world:/labs>add Route Interface=ipsec_tunnel Network=labs/remote_net Metric=10
gw-world:/labs> cc
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Упражнение	Проверьте работоспособность туннеля.

Зайдите в меню *Status→IPSec→ipsec_tunnel.* Уточните статус соединения IPSec SA.

Запустите команду ping (с ключом -t) с хостов, подключенных к **lan-**интерфейсам межсетевых экранов A и B. Зайдите в меню *Status→IPSec→ipsec_tunnel.* Уточните скорость трафика в туннеле.

CMD Windows (устройство A)	C:\>ping 10.95.9.254 –t –l 1400
CMD Windows (устройство B)	C:\>ping 192.168.10.1 –t –l 1400
Устранение возможных проблем	Если туннель не был создан устройствами, решите возникшую проблему с помощью описанных ниже диагностических средств.

Проверьте корректность физических подключений устройств, работоспособность патч-кордов, индикацию на устройствах. Включите режим отладки:

SSH CLI (Console CLI) Устройство A	gw-world:/>ikesnoop –on<IP-адрес удаленного VPN-шлюза>
SSH CLI (Console CLI) Устройство B	gw-world:/>ikesnoop –on<IP-адресудаленногоVPN-шлюза>

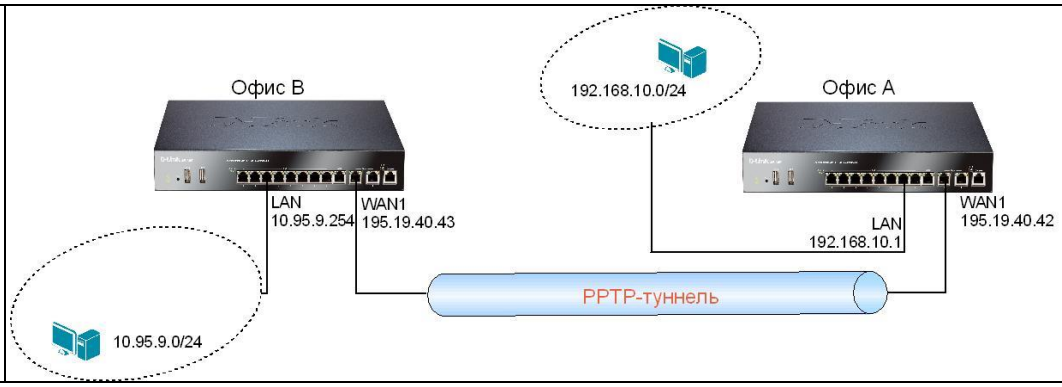
На устройствах зайдите в меню *Status→IPSec→ipsec_tunnel.* Проверьте корректность настроек туннелей, уточните статус SA для фазы 1 и фазы 2.

На устройствах зайдите в меню *Status→Logging* или просмотрите лог-сообщения на syslog-сервере, настроенном для работы с межсетевыми экранами.

Выполните настройку туннелей с простейшими параметрами аутентификации – общим ключом, используйте стандартные (заданные по умолчанию) настройки для алгоритмов IKE и IPSec, режимов IKE, работы с NAT-T, и не используйте пользовательские настройки для XAuth, IKE Config Mode Pool, PFS, ID, Local ID Type. После того, как туннель с этими упрощенными стандартными настройками будет установлен устройствами, измените его параметры в соответствии с особенностями задания в данном сценарии.

Настройка доступа определенным клиентам офиса B к ресурсам сети офиса A через PPTP-туннель

Описание сценария	*Между офисом A и офисом B необходимо настроить PPTP-туннель для безопасного соединения по VPN, аутентификация – PPP.*

Схема 37	

Настройка DFL-860E

Устройство офиса A

Web-интерфейс

Создание необходимых объектов

Создадим объект «IP-адрес PPTP-сервера». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:

Name	pptp_srv_ip
Address	10.254.0.1

Создадим объект «удаленную подсеть за VPN-шлюзом (и удаленным VPN-клиентом)». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:

Name	remote_net
Address	10.95.9.0/24

Создадим объект «пул IP-адресов PPTP-клиентов». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:

Name	pptp_client_pool
Address	10.254.0.150-10.254.0.200

Создадим PPTP-сервер. Зайдите в меню *Interfaces→PPTP/L2TP Servers→Add→PPTP/L2TP Server*. Во вкладке *General* введите следующие параметры:

Name	pptp_pns
Inner IP Address	pptp_srv_ip
Tunnel Protocol	PPTP
Outer Interface Filter	wan1
Server IP	wan1_ip

Во вкладке *PPP Parameters* введите следующие параметры:

Use User Authentication Rules	Поставьте галочку
Microsoft Point-to-Point Encryption	Поставьте галочки – None, RC4 40 bit, RC4 56 bit,
IP Pool	pptp_client_pool

Во вкладке *Add Route* введите следующие параметры:

Allowed Networks	all-nets

Создадим локальную базу пользователей. Перейдите в меню *User Authentication→Local User Databases→Add→Local User Database*. Во вкладке *General* введите:

Name	RemoteUsers

Перейдите в меню *User Authentication→Local User Databases→RemoteUsers→Add→User*. Во вкладке *General* введите:

Username	Remote_user
Password	P@ssw0rd
Confirm Password	P@ssw0rd
Static Client IP Address	pptp_srv_ip
Networks behind user	remote_net
Создайте правило аутентификации пользователя. Перейдите в меню *User Authentication→User Authentication Rules→Add→User Authentication Rule*. Во вкладке *General* введите:	
Name	trusted_users_rule
Agent	PPP
Authentication Source	Local
Interface	pptp_pns
Originator IP	all-nets
Terminator IP	wan1_ip
Во вкладке *Authentication Options* введите:	
Local User DB	Выберите из списка RemoteUsers.
Во вкладке *Agent Options* введите:	
Use MS-CHAP v2 authentication protocol	Поставьте галочку
Создание правил IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	outbound_rule
Action	Allow
Service	all-services
Source Interface	lan
Source Network	lannet
Destination Interface	pptp_pns
Destination Network	remote_net
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	inbound_rule
Action	Allow
Service	all-services
Source Interface	pptp_pns
Source Network	remote_net
Destination Interface	lan
Destination Network	lannet
Создадим IP Rule, разрешающее выполнение команды ping в туннеле. Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	inbound_icmp_allow
Action	Allow
Service	all-icmp
Source Interface	pptp_pns
Source Network	remote_net
Destination Interface	lan
Destination Network	lannet

Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	outbound_icmp_allow
Action	Allow
Service	all-icmp
Source Interface	lan
Source Network	lannet
Destination Interface	pptp_pns
Destination Network	remote_net
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.19.40.42 gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.19.40.0/24 gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address remote_net Address=10.95.9.0/24 gw-world:/labs> add IP4Address pptp_srv_ip Address=10.254.0.1 gw-world:/labs> add IP4Address pptp_client_pool Address=10.254.0.150-10.254.0.200 gw-world:/labs> cc gw-world:/> add Interface L2TPServer pptp_pns Interface=wan1 IPPool=labs/pptp_ippool IP=labs/pptp_srv_ip ServerIP=InterfaceAddresses/wan1_ip TunnelProtocol=PPTP ProxyARPAllInterfaces=Yes gw-world:/> add LocalUserDatabase RemoteUsers gw-world:/> cc LocalUserDatabase RemoteUsers gw-world:/RemoteUsers> add User Remote_user Password=P@ssw0rd IPPool=labs/pptp_srv_ip AutoAddRouteNet=labs/remote_net gw-world:/RemoteUsers> cc gw-world:/> add UserAuthRule Interface=pptp_pns AuthSource=Local LocalUserDB= RemoteUsers OriginatorIP=all-nets Agent=PPP TerminatorIP=InterfaceAddresses/wan1_ip gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=pptp_pns DestinationNetwork=labs/remote_net Name=outbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=pptp_pns SourceNetwork=labs/remote_net DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=pptp_pns SourceNetwork=labs/remote_net DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_icmp_allow gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=pptp_pns DestinationNetwork=labs/remote_net Name=outbound_icmp_allow gw-world:/1(labs)> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Настройка удаленного PPTP клиента (удаленный офис) на базе Microsoft Windows XP/Vista/7	
Создайте новое VPN подключение.	
Укажите URL или IP-адрес межсетевого экрана в качестве конечной точки туннеля.	
Укажите VPN-пользователя:	
Имя	Remote_user

Пароль	P@ssw0rd
Выберите тип VPN-подключения – туннельный протокол точка-точка (PPTP).	
Настройте общий доступ для этого подключения для других хостов в сети 10.95.9.0/24. На хостах в качестве основного шлюза нужно использовать компьютер (или маршрутизатор), на котором настроен PPTP VPN.	
Настройка удаленного PPTP клиента (удаленный офис) на базе другого межсетевого экрана, выступающего в роли PPTP-клиента	
Настройка DFL-860E	
Устройство офиса B	
Web-интерфейс	
Создание необходимых объектов	
Создадим объект «IP-адрес PPTP-сервера». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote_pptp_srv
Address	195.19.40.42 (wan1_ip межсетевого экрана офиса A)
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote_net
Address	10.254.0.0/24
Создадим PPTP-клиента. Зайдите в меню *Interfaces→PPTP/L2TP Clients→Add→PPTP/L2TP Client.* Во вкладке *General* введите следующие параметры:	
Name	pptp_cln
Tunnel Protocol	PPTP
Remote Endpoint	remote_pptp_srv
Remote Network	remote_net
Username	Remote_user
Password	P@ssw0rd
Confirm Password	P@ssw0rd
Во вкладке *Security* введите следующие параметры:	
Authentication	Поставьте галочки: Use PAP, Use CHAP, Use MS-CHAP, Use MS-CHAP v2
Microsoft Point-to-Point Encryption	Поставьте галочки – None, RC4 40 bit, RC4 56 bit
Во вкладке *Advanced* введите следующие параметры:	
Automatically add a route for this interface using the given remote network	Поставьте галочку
Создание правил IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	outbound_rule
Action	Allow
Service	all-services
Source Interface	lan
Source Network	lannet

Destination Interface	pptp_cln
Destination Network	remote_net
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	inbound_rule
Action	Allow
Service	all-services
Source Interface	pptp_cln
Source Network	remote_net
Destination Interface	lan
Destination Network	lannet
Создадим IP Rule, разрешающее выполнение команды ping в туннеле. Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	inbound_icmp_allow
Action	Allow
Service	all-icmp
Source Interface	pptp_cln
Source Network	remote_net
Destination Interface	lan
Destination Network	lannet
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	outbound_icmp_allow
Action	Allow
Service	all-icmp
Source Interface	lan
Source Network	lannet
Destination Interface	pptp_cln
Destination Network	remote_net
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.19.40.43 gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.19.40.0/24 gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address remote_net Address=10.254.0.0/24 gw-world:/labs> add IP4Address remote_pptp_srv Address=10.254.0.1 gw-world:/labs> cc gw-world:/> add Interface L2TPServer pptp_pns Interface=wan1 IPPool=labs/pptp_ippool IP=labs/pptp_srv_ip ServerIP=InterfaceAddresses/wan1_ip TunnelProtocol=PPTP ProxyARPAllInterfaces=Yes gw-world:/> add Interface L2TPClient pptp_cln Username=Remote_user Password=P@ssw0rd Network=labs/remote_net RemoteEndpoint=labs/remote_pptp_srv TunnelProtocol=PPTP PPPAuthMSCHAPv2=Yes PPPAuthMSCHAP=Yes PPPAuthCHAP=Yes PPPAuthPAP=Yes MPPENone=Yes MPPERC440=Yes MPPERC456=Yes gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=pptp_cln	

DestinationNetwork=labs/remote_net Name=outbound_rule
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=pptp_cln SourceNetwork=labs/remote_net DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule
gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=pptp_cln SourceNetwork=labs/remote_net DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_icmp_allow
gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=pptp_clnDestinationNetwork=labs/remote_net Name=outbound_icmp_allow
gw-world:/1(labs)> cc
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Упражнение	Проверьте работоспособность туннеля.

Запустите команду ping (с ключом -t) межсетевого экрана с удаленного VPN-клиента. На межсетевом экране зайдите в меню *Status→Interfaces→pptp_pns.* Уточните скорость трафика в туннеле.

CMD Windows	C:\>ping 10.254.0.1–t –l 1400

На межсетевом экране A зайдите в меню *Status→Routes.* Найдите созданный маршрут к удаленной сети с флагом D.

На межсетевом экране B зайдите в меню *Status→Routes.* Найдите созданный маршрут к удаленной сети.

На межсетевом экране A зайдите в меню *Status→User Authentication.* Найдите аутентификацию пользователя Remote_user.

Устранение возможных проблем	Если туннель не был создан, решите возникшую проблему с помощью описанных ниже диагностических средств.

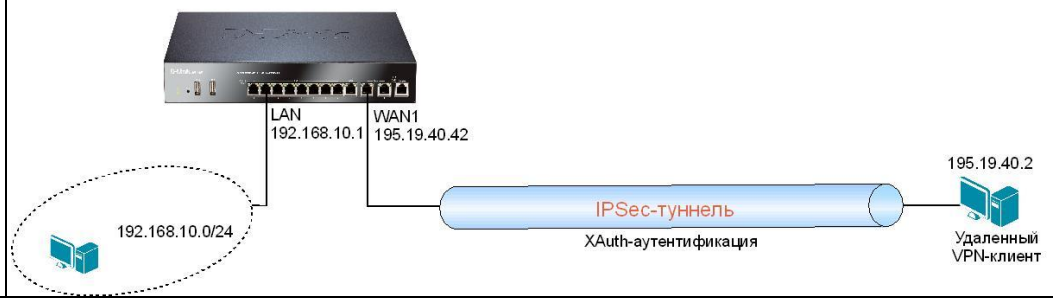
Проверьте корректность физических подключений устройств, работоспособность патч-кордов, индикацию на устройствах.

Зайдите в меню *Status→Interfaces→pptp_pns.* Проверьте статус туннеля.

Зайдите в меню *Status→Logging* или просмотрите лог-сообщения на syslog-сервере, настроенном для работы с межсетевыми экранами.

Удаленные IPSec-клиенты с общим ключом (Pre-shared Key).

Описание сценария	*Между центральным офисом и удаленными пользователями необходимо настроить подключение по VPN, аутентификация – общий ключ.*

Схема 38	

Настройка VPN-клиентов при известном IP-адресе и локальной базе аутентификации пользователей (Local User DB). Аутентификация XAuth. Настройка удаленного управления через IPSec-туннель.

Настройка DFL-860E

Web-интерфейс

Создание необходимых объектов	
Создадим объект «IP-адрес удаленного VPN-клиента». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	remote_gw
Address	195.19.40.2
Создадим объект «Pre-shared Key». Зайдите в меню *Objects→Authentication Objects→Add→Pre-Shared Key*. Введите следующие параметры:	
Name	pre-shared_key
Выберите *Shared Secret*. Введите следующие параметры:	
Shared Secret	123456qw
Confirm Secret	123456qw
Создадим локальную базу пользователей. Перейдите в *User Authentication→Local User Databases→Add→Local User Database*. Во вкладке *General* введите:	
Name	TrustedUsers
Перейдите в *User Authentication→Local User Databases→TrustedUsers→Add→User*. Во вкладке *General* введите:	
Username	user1
Password	P@ssw0rd
Confirm Password	P@ssw0rd
Groups	TrustedUsers
Перейдите в *User Authentication→Local User Databases→TrustedUsers→Add→User*. Во вкладке *General* введите:	
Username	user2
Password	P@ssw0rd
Confirm Password	P@ssw0rd
Groups	TrustedUsers
Создайте правило аутентификации пользователя. Перейдите в *User Authentication→User Authentication Rules→Add→User Authentication Rule*. Во вкладке *General* введите:	
Name	trusted_users_rule
Agent	XAUTH
Authentication Source	Local
Originator IP	lan_ip
Во вкладке *Authentication Options* введите:	
Local User DB	Выберите из списка TrustedUsers.
Создадим IPSec-туннель. Зайдите в *Interfaces→IPSec→Add→IPSec Tunnel*. Введите следующие параметры:	
Name	ipsec_tunnel
Local Network	lannet
Remote Network	all-nets (можно указать более узкий диапазон IP-адресов)
Remote Endpoint	remote_gw
Encapsulation mode	Tunnel
Выберите алгоритмы IKE и IPSec:	
IKE Algorithms	Standard (выберите из списка)
IPSec Algorithms	Standard (выберите из списка)
Во вкладке *Authentication* введите следующие параметры:	

Authentication	Выберите pre-shared_key из списка.
Local ID Type	DNS
Local ID Value	Office1
Во вкладке *XAuth* введите следующие параметры:	
Require IKE XAuth user authentication for inbound IPsec tunnels.	Выберите из списка
Во вкладке *Routing* введите следующие параметры:	
Dynamically add route to the remote network when a tunnel is established	Поставьте галочку
Во вкладке *Advanced* введите следующие параметры:	
Add route for remote network	Уберите галочку
Создание IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	vpn_user_rule
Action	Allow
Service	all-icmp
Source Interface	ipsec_tunnel
Source Network	all-nets
Destination Interface	lan
Destination Network	lannet
Зайдите в *Configuration* и выберите *Save and Activate*.	
Примечание: 1. Требуется одно IP-правило, разрешающее трафик для всех сетей (all-nets) в одну сторону, что автоматически разрешает трафик в другую сторону. ***2. Вместо all-nets в качестве сети источника можно указать более узкий диапазон IP-адресов, с которых будет разрешен доступ.*** ***3. Параметр Local ID для IPSec-туннеля может дополнительно идентифицировать устройство или пользователя. Таким образом, можно разрешить удаленный доступ не всем пользователям, а только знающим значение конкретного Local ID. Кроме того, параметр Local ID может применяться к обоим сторонам туннеля, в этом случае будет использоваться пара Local ID и Remote ID.***	
Настройка удаленного управления межсетевым экраном через IPSec-туннель	
Зайдите в меню *System→Remote Management→Add→HTTP/HTTPS Management.* Введите следующие параметры:	
Name	My_http_manage
HHTPS	поставьте галочку (включено)
UserDatabase	AdminUsers
AccessLevel	Admin
Interface	ipsec_tunnel
Network	all-nets (можно указать более узкий диапазон IP-адресов)
Командная строка (CLI)	
gw-world:/>add PSK pre-shared_key Type=ASCII PSKAscii=123456qw gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address remote_gw Address=195.19.40.2	

gw-world:/labs> cc
gw-world:/> add LocalUserDatabase RemoteUsers
gw-world:/> cc LocalUserDatabase RemoteUsers
gw-world:/RemoteUsers> add User user1 Password=P@ssw0rd
gw-world:/RemoteUsers> add User user2 Password=P@ssw0rd
gw-world:/RemoteUsers> cc
gw-world:/> add UserAuthRule AuthSource=Local LocalUserDB=RemoteUsers OriginatorIP=InterfaceAddresses/lan_ip Agent=XAUTH Name=trusted_users_rule
gw-world:/>add Interface IPsecTunnel ipsec_tunnel AuthMethod=PSK IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet PSK=pre-shared_key RemoteNetwork=all-nets RemoteEndpoint=labs/remote_gw KeepAlive=Auto AddRouteToRemoteNet=Yes XAuth=RequiredForInboundLocalIDType=DNS LocalIDValue=Office1 EncapsulationMode=Tunnel
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnel SourceNetwork=labs/remote_net DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=vpn_user_rule
gw-world:/1(labs)> cc
gw-world:/>add RemoteManagement RemoteMgmtHTTP My_http_manage Interface=ipsec_tunnel LocalUserDatabase=AdminUsers Network=all-nets AccessLevel=Admin HTTPS=Yes
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Настройка IPSec-клиентов

Укажите URL или IP-адрес межсетевого экрана в качестве конечной точки туннеля.

Создадим объект «Pre-shared Key». Зайдите в *Objects→Authentication Objects→Add→Pre-Shared Key*. Введите следующие параметры:

Name	pre-shared_key

Выберите *Shared Secret*. Введите следующие параметры:

Shared Secret	123456qw
Confirm Secret	123456qw

Выберите алгоритмы IKE и IPSec:

IKE Standard на межсетевом экране соответствует использованию следующих опций:

IKE Algorithms	DES, MD5, SHA1

IPSec Standard на межсетевом экране соответсвует использованию следующих опций:

IPSec Algorithms	DES, MD5, SHA1

Выберите ID:

Local ID Type	DNS
Local ID Value	Client1
Remote ID Type	DNS
Remote ID Value	Office1

Настройте XAuth:

Username	user1
Password	P@ssw0rd

Упражнение	Подключите нескольких VPN-клиентов. Например, можно использовать программу The Green Bow VPN Client 5. Проверьте работоспособность туннеля.

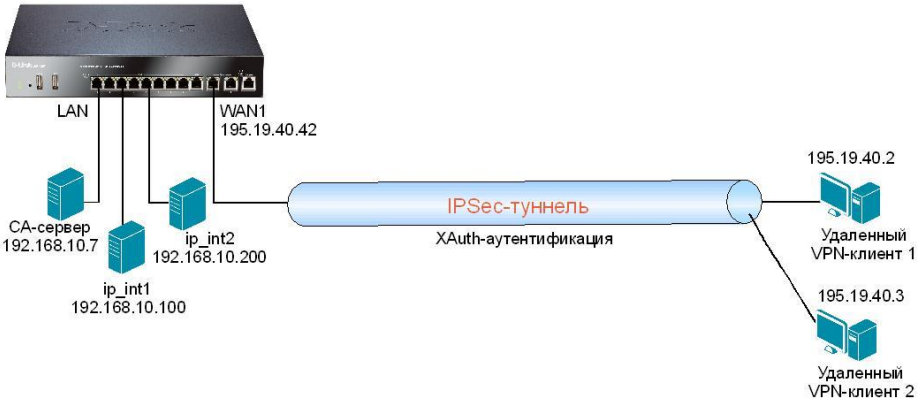
Запустите команду ping (с ключом -t) межсетевого экрана с удаленного VPN-клиента. На межсетевом экране зайдите в меню *Status→IPSec→ipsec_tunnel*. Уточните скорость трафика в туннеле.

CMD Windows	C:\>ping 192.168.10.1 –t –l 1400
После установления IPSec-туннеля зайдите на межсетевой экран для управления с удаленного VPN-клиента.	
MS Internet Explorer	https://<lan_ip>
Устранение возможных проблем	Если туннель не был создан, решите возникшую проблему с помощью описанных ниже диагностических средств.
Проверьте корректность физических подключений устройств, работоспособность патч-кордов, индикацию на устройствах. Включите режим отладки:	
SSH CLI (Console CLI)	gw-world:/>ikesnoop –on<IP-адрес удаленного VPN-шлюза>
Зайдите в меню *Status→IPSec→ipsec_tunnel*. Проверьте корректность настроек туннелей, уточните статус SA для фазы 1 и фазы 2.	
Зайдите в меню *Status→Logging* или просмотрите лог-сообщения на syslog-сервере, настроенном для работы с межсетевыми экранами.	
Выполните настройку туннелей с простейшими параметрами аутентификации – общим ключом, используйте стандартные (заданные по умолчанию) настройки для алгоритмов IKE и IPSec, режимов IKE, работы с NAT-T, и не используйте пользовательские настройки для XAuth, IKE Config Mode Pool, PFS, ID, Local ID Type. После того, как туннель с этими упрощенными стандартными настройками будет установлен устройствами, измените его параметры в соответствии с особенностями задания в данном сценарии.	
Настройка VPN-клиентов при заранее неизвестных IP-адресах клиентов и локальной базе аутентификации пользователей (Local User DB). Аутентификация XAuth.	
Настройка DFL-860E	
Web-интерфейс	
Создание необходимых объектов	
Создадим объект «Pre-shared Key». Зайдите в *Objects→Authentication Objects→Add→Pre-Shared Key*. Введите следующие параметры:	
Name	pre-shared_key
Выберите *Shared Secret*. Введите следующие параметры:	
Shared Secret	123456qw
Confirm Secret	123456qw
Создадим локальную базу пользователей. Перейдите в *User Authentication→Local User Databases→Add→Local User Database*. Во вкладке *General* введите:	
Name	TrustedUsers
Перейдите в *User Authentication→Local User Databases→TrustedUsers→Add→User*. Во вкладке *General* введите:	
Username	user1
Password	P@ssw0rd
Confirm Password	P@ssw0rd
Groups	TrustedUsers
Перейдите в *User Authentication→Local User Databases→TrustedUsers→Add→User*. Во вкладке *General* введите:	
Username	user2
Password	P@ssw0rd
Confirm Password	P@ssw0rd
Groups	TrustedUsers

Создайте правило аутентификации пользователя. Перейдите в *User Authentication→Local User Databases→ TrustedUsers→Add→User*. Во вкладке *General* введите:	
Name	trusted_users_rule
Agent	XAUTH
Authentication Source	Local
Originator IP	all-nets
Во вкладке *Authentication Options* введите:	
Local User DB	Выберите из списка TrustedUsers.
Если известен диапазон IP-адресов, то необходимо использовать объект IKE Config Mode Pool. Перейдите в *Objects→VPN Objects→IKE Config Mode Pool→Add→IKE Config Mode Pool*. Во вкладке *General* введите:	
Use a pre-defined IPPool Object	Выберите известный диапазон адресов.
Создадим объект «IP-адрес DHCP-сервера». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	dhcp-ip
Address	192.168.10.250
Если применяется DHCP-сервер, то необходимо использовать объект IP Pool, в котором указывается данный DHCP-сервер. Перейдите в *Objects→IP Pools→Add→IP Pool*. Во вкладке *General* введите:	
Name	ippool
Specify DHCP Server Address	Переместите из списка *Available* в список *Selected* объект dhcp-ip
Server Filter	all-nets
Client IP Filter	all-nets
Во вкладке *Advanced* введите следующие параметры:	
Routing Table	main
Receive Interface	lan
Prefetch Leases	10
Примечание: Использование IKE Config Mode Pool и IP Pool позволяет передать удаленным VPN-клиентам дополнительные параметры внутренней сети (например, адрес DNS-сервера, DHCP-сервера, и т.п.) и выдать IP-адрес динамически (от DHCP-сервера организации). Применение IKE Config Mode Pool и IP Pool необязательно при создании VPN-туннелей.	
Создадим IPSec-туннель. Зайдите в *Interfaces→IPSec→Add→IPSec Tunnel*. Введите следующие параметры:	
Name	ipsec_tunnel
Local Network	lannet
Remote Network	all-nets
Remote Endpoint	all-nets
Encapsulation mode	Tunnel
IKE Config Mode Pool	Выберите созданный ранее дипазон IP Pool (***pre-defined*** или ***Static***).
Выберите алгоритмы IKE и IPSec:	
IKE Algorithms	Standard (выберите из списка)
IPSec Algorithms	Standard (выберите из списка)
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите pre-shared_key из списка.
Local ID Type	DNS

Local ID Value	Office1
Во вкладке *XAuth* введите следующие параметры:	
Require IKE XAuth user authentication for inbound IPsec tunnels.	Выберите из списка
Во вкладке *Routing* введите следующие параметры:	
Dynamically add route to the remote network when a tunnel is established	Поставьте галочку
Во вкладке *Advanced* введите следующие параметры:	
Add route for remote network	Уберите галочку
Создание правил IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	vpn_user_rule
Action	Allow
Service	all-services
Source Interface	ipsec_tunnel
Source Network	all-nets
Destination Interface	lan
Destination Network	lannet
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Примечание: 1. Требуется одно IP-правило, разрешающее трафик для всех сетей (all-nets) в одну сторону, что автоматически разрешает трафик в другую сторону. ***2. Вместо all-nets в качестве сети источника можно указать более узкий диапазон IP-адресов, с которых будет разрешен доступ.*** ***3. Разрешение удаленного управления для этого сценария опасно, т.к. диапазон адресов клиентов неограничен.***	
Командная строка (CLI)	
gw-world:/>add PSK pre-shared_key Type=ASCII PSKAscii=123456qw gw-world:/>add IPPool ippool Interface=dmz PrefetchLeases=10 ServerFilter=all-nets RoutingTable=main ReceiveInterface=lan DHCPServerType=Interface IPFilter=all-nets gw-world:/> set ConfigModePool IPPoolType=PreDefined IPPool=ippool gw-world:/> add LocalUserDatabase RemoteUsers gw-world:/> cc LocalUserDatabase RemoteUsers gw-world:/RemoteUsers> add User user1 Password=P@ssw0rd gw-world:/RemoteUsers> add User user2 Password=P@ssw0rd gw-world:/RemoteUsers> cc gw-world:/> add UserAuthRule AuthSource=Local LocalUserDB=RemoteUsers OriginatorIP=InterfaceAddresses/lan_ip Agent=XAUTH Name=trusted_users_rule gw-world:/>add Interface IPsecTunnel ipsec_tunnel AuthMethod=PSK IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet PSK=pre-shared_key RemoteNetwork=all-nets RemoteEndpoint=all-nets KeepAlive=Auto AddRouteToRemoteNet=Yes XAuth=RequiredForInboundIKEConfigModePool=ConfigModePool LocalIDType=DNS LocalIDValue=Office1 EncapsulationMode=Tunnel gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnel SourceNetwork=labs/remote_net DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=vpn_user_rule gw-world:/1(labs)> cc	

gw-world:/> activate *(подождать 3-5 секунд* gw-world:/>commit	
Настройка IPSec-клиентов	
Укажите URL или IP-адрес межсетевого экрана в качестве конечной точки туннеля.	
Создадим объект «Pre-shared Key».	
Выберите *Shared Secret*. Введите следующие параметры:	
Shared Secret	123456qw
Confirm Secret	123456qw
Выберите алгоритмы IKE и IPSec:	
IKE Standard на межсетевом экране соответсвует использованию следующих опций:	
IKE Algorithms	DES, MD5, SHA1
IPSec Standard на межсетевом экране соответсвует использованию следующих опций:	
IPSec Algorithms	DES, MD5, SHA1
Укажите config mode, если он используется на межсетевом экране.	
Выберите ID:	
Local ID Type	DNS
Local ID Value	Client1
Remote ID Type	DNS
Remote ID Value	Office1
Настройте XAuth:	
Username	user1
Password	P@ssw0rd
Упражнение	Подключите нескольких VPN-клиентов. Например, можно использовать программу The Green Bow VPN Client 5. Проверьте работоспособность туннеля.
Запустите команду ping (с ключом -t) межсетевого экрана с удаленного VPN-клиента. На межсетевом экране зайдите в меню *Status→IPSec→ipsec_tunnel*. Уточните скорость трафика в туннеле.	
CMD Windows	C:\>ping 192.168.10.1 –t –l 1400
Устранение возможных проблем	Если туннель не был создан, решите возникшую проблему с помощью описанных ниже диагностических средств.
Проверьте корректность физических подключений устройств, работоспособность патч-кордов, индикацию на устройствах. Включите режим отладки:	
SSH CLI (Console CLI)	gw-world:/>ikesnoop –on<IP-адрес удаленного VPN-шлюза>
Зайдите в меню *Status→IPSec→ipsec_tunnel*. Проверьте корректность настроек туннелей, уточните статус SA для фазы 1 и фазы 2.	
Зайдите в меню *Status→Logging* или просмотрите лог-сообщения на syslog-сервере, настроенном для работы с межсетевыми экранами.	
Выполните настройку туннелей с простейшими параметрами аутентификации – общим ключом, используйте стандартные (заданные по умолчанию) настройки для алгоритмов IKE и IPSec, режимов IKE, работы с NAT-T, и не используйте пользовательские настройки для XAuth, IKE Config Mode Pool, PFS, ID, Local ID Type. После того, как туннель с этими упрощенными стандартными настройками будет установлен устройствами, измените его параметры в соответствии с особенностями задания в данном сценарии.	
Настройка VPN-клиентов с сертификатами и локальной базой аутентификации пользователей (Local User DB). Аутентификация XAuth.	

Описание сценария	*Между центральным офисом и удаленными пользователями необходимо настроить подключение по VPN, аутентификация – CA-сервер и XAuth. CA-сервер (например, dc1.ks.ru (192.168.10.7)) поодключен к **lan**-интерфейсу межсетевого экрана А. Доступ пользователей user1 и user2 к ресурсам внутренней сети различный: user1 – разрешен доступ к ip_int1, user2 – разрешен доступ к ip_int2.*
Схема 39	

Создание необходимых объектов

Microsoft Windows Server 2003/2008

Создайте два набора подписанных CA-сертификатов с помощью CA центра сертификации Microsoft Windows Server 2003/2008.
Зайдите http://dc1.ks.ru/certsrv, выберите опцию *Загрузить CA сертификат*. Сохраните сертификат под именем CA_cert.
Создайте запрос к CA-серверу для генерации клиентских сертификатов.
Зайдите http://dc1.ks.ru/certsrv, выберите опцию *Расширенный запрос сертификата*,
введите следующие параметры:

Name	user1
E-Mail	user1@company.com
Company	MSTU
Department	IT
City	Moscow
Type of certificate needed	IPSec Certificate
Key Option	Выберите Create new key set
CSP	Microsoft Edvanced Cryptographic Provider v1.0
Key Usage	Both
Key Size	1024
Automatic Key Container Name	Выберите из списка
Mark keys as exportable	Поставьте галочку

Создайте сертификат второго пользователя. Зайдите http://dc1.ks.ru/certsrv, выберите опцию *Расширенный запрос сертификата*, введите следующие параметры:

Name	user2
E-Mail	user2@company.com
Company	MSTU
Department	IT
City	Moscow
Type of certificate needed	IPSec Certificate

Key Option	Выберите Create new key set
CSP	Microsoft Edvanced Cryptographic Provider v1.0
Key Usage	Both
Key Size	1024
Automatic Key Container Name	Выберите из списка
Mark keys as exportable	Поставьте галочку
Создайте сертификат шлюза. Зайдите http://dc1.ks.ru/certsrv, выберите опцию Расширенный запрос сертификата, введите следующие параметры:	
Name	gw_cert
E-Mail	gateway@company.com
Company	MSTU
Department	HQ
City	Moscow
Typeofcertificateneeded	IPSecCertificate
Key Option	Выберите Create new key set
CSP	Microsoft Edvanced Cryptographic Provider v1.0
Key Usage	Both
Key Size	1024
Automatic Key Container Name	Выберите из списка
Mark keys as exportable	Поставьте галочку
Сохраните файлы сертификатов через экспорт сертификатов. Конвертируйте тип сертификатов в форматы **.cer** и **.key**. Можно воспользоваться программой OpenSSL 0.9.8k или аналогичной программой работы с сертификатами X.509.	
Настройка DFL-860E	
Web-интерфейс	
Создание необходимых объектов	
Создадим объект «IP-адрес, которые будет использован удаленными клиентами». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	ip_int1
Address	192.168.10.100
Создадим объект «IP-адрес, которые будет использован удаленными клиентами». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	ip_int2
Address	192.168.10.200
Импортируйте наборы созданных сертификатов (корневой сертификат, сертификат шлюза – CA_cert.cer, gw_cert.cer, gw_cert.key). Зайдите в меню *Objects→Authentication Objects→Add→Certificate*. Введите следующие параметры:	
Name	CA_cert
Upload remove certificate.	Выберите эту опцию и укажите путь к файлу сертификата CA_cert.cer.
Зайдите в меню *Objects→Authentication Objects→Add→Certificate.* Введите следующие параметры:	
Name	gw_cert
Upload X.509 certificate.	Выберите эту опцию и укажите путь к файлам сертификатов **.cer** и **.key**.

Создадим локальную базу пользователей. Перейдите в меню *User Authentication→Local User Databases→Add→Local User Database*. Во вкладке *General* введите:	
Name	TrustedUsers
Перейдите в меню *User Authentication→Local User Databases→TrustedUsers→Add→User*. Во вкладке *General* введите:	
Username	user1
Password	P@ssw0rd
Confirm Password	P@ssw0rd
Groups	TrustedUsers
Перейдите в *User Authentication→Local User Databases→TrustedUsers→Add→User*. Во вкладке *General* введите:	
Username	user2
Password	P@ssw0rd
Confirm Password	P@ssw0rd
Groups	TrustedUsers
Создайте правило аутентификации пользователя. Перейдите в *User Authentication→User Authentication Rules→Add→User Authentication Rule*. Во вкладке *General* введите:	
Name	trusted_users_rule
Agent	XAUTH
Authentication Source	Local
Originator IP	all-nets
Во вкладке *Authentication Options* введите:	
Local User DB	Выберите из списка TrustedUsers.
Примечание: Так как IP-адреса VPN-клиентов выездных сотрудников не известны заранее, входящие VPN-соединения от клиентов не могут дифференцироваться. Это означает, что межсетевой экран не способен контролировать доступ к различным частям внутренних сетей. В этом сценарии это ip_int1 и ip_int2. ***Использование списков идентификаторов представляет собой решение этой проблемы. Список идентификаторов содержит один или более идентификаторов (ID), где каждый идентификатор соответствует предметному полю в сертификате. Списки идентификаторов могут таким образом использоваться для регулирования того, какие сертификаты с доступом использовать и с какими IPsec-туннелями.***	
Создадим объект «список идентификаторов ID». Зайдите в меню *Objects→VPN Objects→IKE ID Lists→Add→ID List.* Введите следующие параметры:	
Name	ID_list_user1
Зайдите в меню *Objects→VPN Objects→IKE ID Lists→ID_List_user1→Ids→Add→ID.* Введите следующие параметры:	
Name	user1
Type	Distinguished name
Common Name	user1
Organization Name	MSTU
Organizational Unit	IT
Country	Russia
Email Address	user1@company.com
Зайдите в меню *Objects→VPN Objects→IKE ID Lists→Add→ID List.* Введите следующие параметры:	
Name	ID_list_user2
Зайдите в меню *Objects→VPN Objects→IKE ID Lists→ID_List_user2→Ids→Add→ID.* Введите	

следующие параметры:	
Name	user2
Type	Distinguished name
Common Name	user2
Organization Name	MSTU
Organizational Unit	IT
Country	Russia
Email Address	user2@company.com
Если известен диапазон IP-адресов, то необходимо использовать объект IKE Config Mode Pool. Перейдите в меню *Objects→VPN Objects→IKE Config Mode Pool→Add→IKE Config Mode Pool*. Во вкладке *General* введите:	
Use a pre-defined IPPool Object	Выберите известный диапазон адресов.
Создадим объект «IP-адрес DHCP-сервера». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	dhcp-ip
Address	192.168.10.250
Если применяется DHCP-сервер, то необходимо использовать объект IP Pool, в котором указывается данный DHCP-сервер. Перейдите в меню *Objects→IP Pools→Add→IP Pool*. Во вкладке *General* введите:	
Name	ippool
Specify DHCP Server Address	Переместите из списка *Available* в список *Selected* объект dhcp-ip.
Server Filter	all-nets
Client IP Filter	all-nets
Во вкладке *Advanced* введите следующие параметры:	
Routing Table	main
Receive Interface	lan
Prefetch Leases	10
Примечание: Использование IKE Config Mode Pool и IP Pool позволяет передать удаленным VPN-клиентам дополнительные параметры внутренней сети (например, адрес DNS-сервера, DHCP-сервера, и т.п.) и выдать IP-адрес динамически (от DHCP-сервера организации). Применение IKE Config Mode Pool и IP Pool необязательно при создании VPN-туннелей.	
Создадим IPSec-туннель для пользователей типа user1. Зайдите в меню *Interfaces→IPSec→Add→IPSec Tunnel.* Введите следующие параметры:	
Name	ipsec_tunnel1
Local Network	lannet
Remote Network	all-nets
Remote Endpoint	all-nets
Encapsulation mode	Tunnel
IKE Config ModePool	Выберите созданный ранее дипазон IP Pool (***pre-defined*** или ***Static***).
Выберите алгоритмы IKE и IPSec:	
IKE Algorithms	Standard (выберите из списка)
IPSec Algorithms	Standard (выберите из списка)
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите X.509 Certificate из списка.
Root Certificate (s)	Переместите CA_cert из списка Available в список Selected.

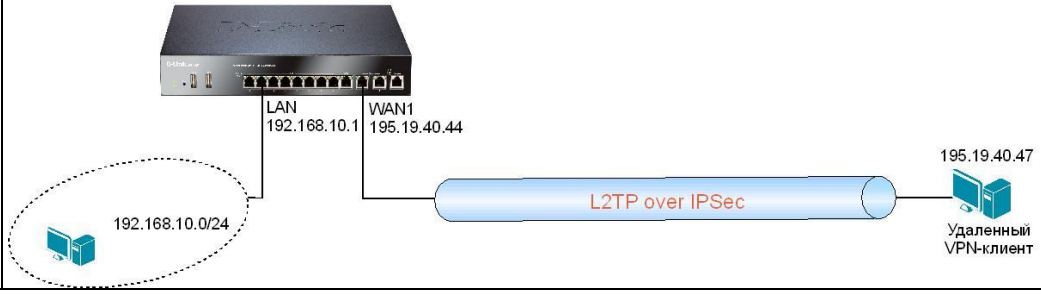
Gateway certificate	Переместите gw_cert из списка Available в список Selected.
Identification list	Выберите My_ID_list1.
Во вкладке *XAuth* введите следующие параметры:	
Require IKE XAuth user authentication for inbound IPsec tunnels.	Выберите из списка
Во вкладке *Routing* введите следующие параметры:	
Dynamically add route to the remote network when a tunnel is established	Поставьте галочку
Во вкладке *Advanced* введите следующие параметры:	
Add route for remote network	Уберите галочку
Создадим IPSec-туннель для пользователей типа user2. Зайдите в меню *Interfaces→IPSec→Add→IPSec Tunnel*. Введите следующие параметры:	
Name	ipsec_tunnel2
Local Network	lannet
Remote Network	all-nets
Remote Endpoint	all-nets
Encapsulation mode	Tunnel
IKE Config ModePool	Выберите созданный ранее диапазон IP Pool (***pre-defined*** или ***Static***)
Выберите алгоритмы IKE и IPSec:	
IKE Algorithms	Standard (выберите из списка)
IPSec Algorithms	Standard (выберите из списка)
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите X.509 Certificate из списка.
Roo tCertificate (s)	Переместите CA_cert из списка Available в список Selected.
Gateway Certificate	Переместите gw_cert из списка Available в список Selected.
Identification list	Выберите My_ID_list2.
Во вкладке *XAuth* введите следующие параметры:	
Require IKE XAuth user authentication for inbound IPsec tunnels.	Выберите из списка.
Во вкладке *Routing* введите следующие параметры:	
Dynamically add route to the remote network when a tunnel is established	Поставьте галочку
Во вкладке *Advanced* введите следующие параметры:	
Add route for remote network	Уберите галочку
Создание правил IP Rule для туннелей	
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	vpn_user_rule1
Action	Allow
Service	all-icmp
Source Interface	ipsec_tunnel1
Source Network	all-nets

Destination Interface	lan
Destination Network	ip_int1
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	vpn_user_rule2
Action	Allow
Service	all-icmp
Source Interface	ipsec_tunnel2
Source Network	all-nets
Destination Interface	lan
Destination Network	ip_int2
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Примечание: 1. Требуется всего одно IP-правило, разрешающее трафик ICMP для всех сетей (all-nets) как в одну сторону, так и в другую. ***2. Вместо all-nets в качестве сети источника можно указать более узкий диапазон IP-адресов, с которых будет разрешен доступ.***	
Командная строка (CLI)	
gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address ip_int1 Address=192.168.10.100 gw-world:/labs> add IP4Address ip_int2 Address=192.168.10.200 gw-world:/labs> cc gw-world:/> add LocalUserDatabase TrustedUsers gw-world:/> cc LocalUserDatabase TrustedUsers gw-world:/TrustedUsers > add User user1 Password=P@ssw0rd gw-world:/TrustedUsers > add User user2 Password=P@ssw0rd gw-world:/TrustedUsers > cc gw-world:/> add UserAuthRule AuthSource=Local LocalUserDB=TrustedUsers OriginatorIP= InterfaceAddresses/lan_ip Agent=XAUTH Name=trusted_users_rule gw-world:/> add IDList ID_list_user1 gw-world:/> cc IDList ID_list_user1 gw-world:/ID_list_user1> add ID user1 Type=DistinguishedName Country=Russia OrganizationalUnit=IT CommonName=user1 OrganizationName=MSTU EMailAddress=user1@company.com gw-world:/ID_list_user1> cc gw-world:/> add IDList ID_list_user2 gw-world:/> cc IDList ID_list_user2 gw-world:/ID_list_user2> add ID user2 Type=DistinguishedName Country=Russia OrganizationalUnit=IT CommonName=user2 OrganizationName=MSTU EMailAddress=user2@company.com gw-world:/ID_list_user2> cc gw-world:/>add IPPool ippool Interface=dmz PrefetchLeases=10 ServerFilter=all-nets RoutingTable=main ReceiveInterface=lan DHCPServerType=Interface IPFilter=all-nets gw-world:/> set ConfigModePool IPPoolType=PreDefined IPPool=ippool gw-world:/> add Interface IPsecTunnel ipsec_tunnel1 AuthMethod=Certificate GatewayCertificate=gw_cert RootCertificates=CA_cert IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet RemoteNetwork=all-nets RemoteEndpoint=all-netsXAuth=RequiredForInbound IDList=ID_list_user1IKEConfigModePool=ConfigModePool KeepAlive=Auto AddRouteToRemoteNet=Yes EncapsulationMode=Tunnel gw-world:/> add Interface IPsecTunnel ipsec_tunnel2 AuthMethod=Certificate	

GatewayCertificate=gw_cert RootCertificates=CA_cert IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet RemoteNetwork=all-nets RemoteEndpoint=all-nets XAuth=RequiredForInbound IDList=ID_list_user2 IKEConfigModePool=ConfigModePool KeepAlive=Auto AddRouteToRemoteNet=Yes EncapsulationMode=Tunnel gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmpSourceInterface=ipsec_tunnel1 SourceNetwork=all-nets DestinationInterface=lan DestinationNetwork=labs/ip_int1Name=vpn_user_rule1 gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnel2 SourceNetwork=all-nets DestinationInterface=lan DestinationNetwork=labs/ip_int2 Name=vpn_user_rule2 gw-world:/1(labs)> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Настройка IPSec-клиентов	
Укажите URL или IP-адрес межсетевого экрана в качестве конечной точки туннеля.	
Импортируйте наборы созданных сертификатов (корневой сертификат, сертификат пользователя – CA_cert, user1 или user2).	
Выберите алгоритмы IKE и IPSec:	
IKE Standard на межсетевом экране соответствует использованию следующих опций:	
IKE Algorithms	DES, MD5, SHA1
IPSec Standard на межсетевом экране соответсвует использованию следующих опций:	
IPSec Algorithms	DES, MD5, SHA1
Настройте XAuth-аутентификацию для пользователя user1:	
XAuth user name	user1
XAuth password	P@ssw0rd
Настройте XAuth-аутентификацию для пользователя user2:	
XAuth user name	user2
XAuth password	P@ssw0rd
Укажите config mode, если он используется на межсетевом экране.	
Упражнение	Проверьте работоспособность туннеля.
Запустите команду ping (с ключом -t) межсетевого экрана с удаленного VPN-клиента 1 и 2. На межсетевом экране зайдите в меню *Status→IPSec→ipsec_tunnel1* и *Status→IPSec→ipsec_tunnel2*. Уточните скорость трафика в туннелях.	
CMD Windows (VPN клиент 1)	C:\>ping 192.168.10.100 –t –l 1400
CMD Windows (VPN клиент 2)	C:\>ping 192.168.10.200 –t –l 1400
Устранение возможных проблем	Если туннель не был создан, решите возникшую проблему с помощью описанных ниже диагностических средств.
Проверьте корректность физических подключений устройств, работоспособность патч-кордов, индикацию на устройствах. Включите режим отладки:	
SSH CLI (Console CLI)	gw-world:/>ikesnoop –on<IP-адрес удаленного VPN-шлюза>
Зайдите в меню *Status→IPSec→ipsec_tunnel*. Проверьте корректность настроек туннелей, уточните статус SA для фазы 1 и фазы 2.	
Зайдите в меню *Status→Logging* или просмотрите лог-сообщения на syslog-сервере, настроенном для работы с межсетевыми экранами.	

Выполните настройку туннелей с простейшими параметрами аутентификации – общим ключом, используйте стандартные (заданные по умолчанию) настройки для алгоритмов IKE и IPSec, режимов IKE, работы с NAT-T, и не используйте пользовательские настройки для XAuth, IKE Config Mode Pool, PFS, ID, Local ID Type. После того, как туннель с этими упрощенными стандартными настройками будет установлен устройствами, измените его параметры в соответствии с особенностями задания в данном сценарии.

ЗАНЯТИЕ №9.3. Настройка удаленных L2TP-клиентов с общим ключом (L2TP over IPSec с общим ключом). Настройка удаленных L2TP-клиентов с сертификатами (L2TP over IPSec с сертификатами). Настройка SSL VPN. GRE-туннель. PPTP ALG для PPTP-туннелей с NAT.

Настройка удаленных L2TP-клиентов с общим ключом (L2TP over IPSec с общим ключом).	
Описание сценария	*Между центральным офисом и удаленными пользователями необходимо настроить подключение по протоколу L2TP over IPSec, аутентификация – общий ключ.*
Схема 40	
Настройка DFL-860E	
Web-интерфейс	
Создание необходимых объектов	
Создадим объект «диапазон IP-адресов, которые могут быть использованы удаленными клиентами». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	l2tp_pool
IPAddress	192.168.10.10-192.168.10.20
Создадим объект «внешний IP-адрес, через который могут подключаться клиенты». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	ip_ext (wan1_ip)
Address	195.19.40.44
Создадим объект «внутренний IP-адрес, через который могут подключаться клиенты». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	ip_int
Address	192.168.10.1
Создадим объект «Pre-shared Key». Зайдите в меню *Objects→Authentication Objects→Add→Pre-Shared Key*. Введите следующие параметры:	
Name	pre-shared_key
Выберите *Shared Secret*. Введите следующие параметры:	
Shared Secret	123456qw
Confirm Secret	123456qw
Создадим локальную базу пользователей. Перейдите в *User Authentication→Local User Databases→Add→Local User Database*. Во вкладке *General* введите:	
Name	TrustedUsers
Перейдите в меню *User Authentication→Local User Databases→TrustedUsers→Add→User*. Во вкладке *General* введите:	
Username	user1

Password	P@ssw0rd
Confirm Password	P@ssw0rd
Groups	TrustedUsers
Перейдите в *User Authentication→Local User Databases→TrustedUsers→Add→User*. Во вкладке *General* введите:	
Username	user2
Password	P@ssw0rd
Confirm Password	P@ssw0rd
Groups	TrustedUsers
Если известен диапазон IP-адресов, то необходимо использовать объект IKE Config Mode Pool. Перейдите в меню *Objects→VPN Objects→IKE Config Mode Pool→Add→IKE Config Mode Pool*. Во вкладке *General* введите:	
Use a pre-defined IPPool Object	Выберите известный диапазон адресов.
Если применяется DHCP-сервер, то необходимо использовать объект IP Pool, в котором указывается данный DHCP-сервер. Создадим объект «IP-адрес DHCP-сервера». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Во вкладке *General* введите следующие параметры:	
Name	ippool_dhcp
Address	172.17.100.10
Создадим IP Pool. Перейдите в меню *Objects→IP Pools→Add→IPPool*. Во вкладке *General* введите:	
Name	ippool
Specify DHCP Server Address	Переместите из списка *Available* в список *Selected* объект ippool_dhcp
Server Filter	all-nets
Client IP Filter	all-nets
Во вкладке *Advanced* введите следующие параметры:	
Routing Table	main
Receive Interface	dmz
Prefetch Leases	10
Создадим IPSec-туннель. Зайдите в *Interfaces→IPSec→Add→IPSecTunnel*. Введите следующие параметры:	
Name	ipsec_tunnel
Local Network	ip_ext (укажите all-nets, если межсетевой экран за NAT).
Remote Network	all-nets
Remote Endpoint	none
Encapsulation mode	Transport
IKE Config ModePool	Выберите созданный ранее дипазон IP Pool (***pre-defined*** или ***Static***).
Выберите алгоритмы IKE и IPSec:	
IKE Algorithms	Standard (выберите из списка)
IPSec Algorithms	Standard (выберите из списка)
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите pre-shared_key из списка.
Во вкладке *Routing* введите следующие параметры:	
Dynamically add route to the remote network when a tunnel	Поставьте галочку

is established	
Во вкладке *Advanced* введите следующие параметры:	
Add route for remote network	Уберите галочку
Добавьте PPTP/L2TP. Зайдите в *Interfaces→PPTP/L2TP Servers→Add→PPTP/L2TP Server*. Введите следующие параметры во вкладке *General*:	
Name	l2tp_srv
Inner IP Address	ip_int
Tunnel Protocol	L2TP
Outer Interface Filter	ipsec_tunnel
Server IP	ip_ext
Во вкладке *PPP Parameters* введите:	
Use User Authentication Rules	Поставьте галочку
Microsoft Point-to-Point Encryption	Разрешите – поставьте галочки.
IP Pool	l2tp_pool
Во вкладке *Add Route* введите:	
Proxy ARP	Разрешите на интерфейсе, к которому подключена внутренняя сеть.
Allowed Networks	all-nets
Создайте правило аутентификации пользователя. Перейдите в *User Authentication→User Authentication Rules→Add→User Authentication Rule*. Во вкладке *General* введите:	
Name	trusted_users_rule
Agent	PPP
Authentication Source	Local
Interface	l2tp_srv
Originator IP	all-nets
Terminator IP	ip_ext
Во вкладке *Authentication Options* введите:	
Local User DB	Выберите из списка TrustedUsers.
Во вкладке *Agent Options* введите:	
Use MS-CHAP authentication protocol	Поставьте галочку (для клиентов MS Windows XP).
Use MS-CHAP v2 authentication protocol	Поставьте галочку (для клиентов MS Windows Vista/7).
Создание правил IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	inbound_rule
Action	Allow
Service	all-services
Source Interface	l2tp_srv
Source Network	l2tp_pool
Destination Interface	lan
Destination Network	lannet
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	outbound_rule

Action	Allow
Service	all-services
Source Interface	lan
Source Network	lannet
Destination Interface	l2tp_srv
Destination Network	l2tp_pool
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	icmp_rule
Action	Allow
Service	all-icmp
Source Interface	l2tp_srv
Source Network	l2tp_pool
Destination Interface	core
Destination Network	lan_ip
Зайдите в *Configuration* и выберите *Save and Activate*.	

Примечание: 1. Если уже настроены статические туннели или в будущем предполагается их использовать, необходимо расположить их выше так называемого динамического туннеля с параметром Remote Network и/или Remote Gateway, имеющем значение all-nets. Все туннели в списке туннелей Interfaces→IPSec, находящиеся ниже динамического туннеля, окажуться неработоспособны.

2. Динамический туннель может быть только один для данных параметров аутентификации, для разделения удаленных клиентов на подключение к разным динамическим туннелям нужно использовать параметры Local ID и Identification list (для сертификатов).

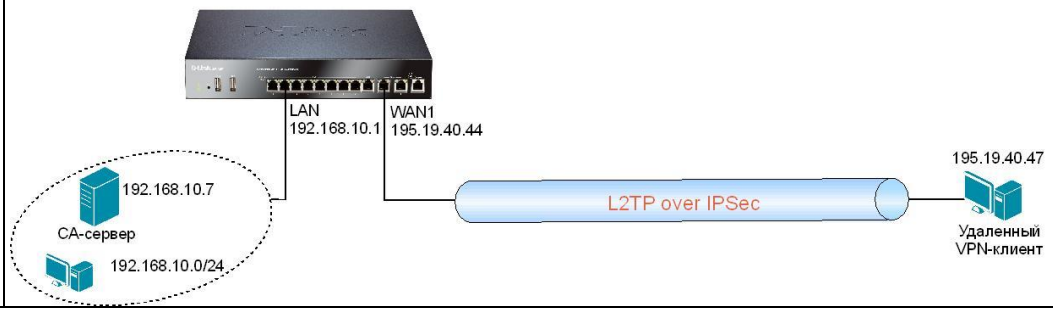
Командная строка (CLI)

```
gw-world:/> add Address AddressFolder labs
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address l2tp_pool Address=192.168.10.10-192.168.10.20
gw-world:/labs> add IP4Address ip_ext Address=195.19.40.44
gw-world:/labs> add IP4Address ip_intAddress=192.168.10.1
gw-world:/labs> cc
gw-world:/> add PSK pre-shared_key Type=ASCII PSKAscii=123456qw
gw-world:/> add LocalUserDatabase TrustedUsers
gw-world:/> cc LocalUserDatabase TrustedUsers
gw-world:/TrustedUsers > add User user1 Password=P@ssw0rd
gw-world:/TrustedUsers > add User user2 Password=P@ssw0rd
gw-world:/TrustedUsers > cc
gw-world:/>add IPPool ippool Interface=dmz PrefetchLeases=10 ServerFilter=all-nets
RoutingTable=main ReceiveInterface=dmz DHCPServerType=Interface IPFilter=all-nets
gw-world:/> set ConfigModePool IPPoolType=PreDefined IPPool=ippool
gw-world:/> add Interface IPsecTunnel ipsec_tunnel AuthMethod=PSK IKEAlgorithms=Standard
IPsecAlgorithms=Standard LocalNetwork=labs/ip_ext PSK=pre-shared_key RemoteNetwork=all-nets
AddRouteToRemoteNet=Yes IKEConfigModePool=ConfigModePool EncapsulationMode=Transport
gw-world:/> add Interface L2TPServer l2tp_srv Interface=ipsec_tunnel IPPool=labs/l2tp_pool
IP=labs/ip_int ServerIP=labs/ip_ext TunnelProtocol=L2TP ProxyARPInterfaces=lanUseUserAuth=Yes
gw-world:/> add UserAuthRule Interface=l2tp_srv AuthSource=Local LocalUserDB=TrustedUsers
OriginatorIP=all-nets Agent=PPP TerminatorIP=labs/ip_ext Name=trusted_users_rule
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=l2tp_srv
```

SourceNetwork=labs/l2tp_pool DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=l2tp_srv DestinationNetwork=labs/l2tp_pool Name=outbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=l2tp_srv SourceNetwork=labs/l2tp_pool DestinationInterface=core DestinationNetwork=InterfaceAddresses/lan_ipName=icmp_rule gw-world:/1(labs)> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Настройка IPSec IKE в Microsoft Windows XP/Vista/7	
Сетевые настройки компьютера должны соответствовать подсети 195.19.40.0/24. IP-адрес компьютера – 195.19.40.47.	
Зайдите Пуск→Выполнить→mmc	
В консоле MMC добавьте оснастку Политики IP-безопасности для локального компьютера.	
Примечание: Для домена Microsoft Windows можно добавить оснастку для групповой политики и далее ее применить на граничном шлюзе в данном сегменте сети.	
В оснастке Политики IP-безопасности задайте новую политику IP-безопасности со следующими параметрами:	
Имя	L2tp_ipsec_policy
Зайдите в свойства созданной политики. Во вкладке *Общие→Параметры* введите:	
Основной ключ безопасной пересылки (PFS)	Уберите галочку
Проверять подлинность и создавать новый ключ каждые	480 мин
Проверять подлинность и создавать новый ключ через каждые	0 сеансов
Зайдите во вкладку *Общие→Параметры→Методы→Добавить.* Введите следующие параметры:	
Алгоритм проверки целостности	SHA1
Алгоритм шифрования	DES
Группа Диффи-Хельмана	средняя (2)
Зайдите *Свойства→Управление списками IP-фильтра и действиями фильтра→Управление списками IP-фильтров→Добавить*, введите следующие параметры (нажимайте *Далее* после заполнения необходимых параметров в каждом окне):	
Имя	Inbound
Зайдите *Список IP-фильтров→Добавить*, введите следующие параметры:	
Описание IP-фильтра и свойство «Отраженный»	Уберите галочку *Отраженный*
Источник IP-трафика	Выберите из списка *Определенный IP-адрес или подсеть*, введите 195.19.40.44
Назначение IP-трафика	Выберите из списка *Определенный IP-адрес или подсеть*, введите 195.19.40.47
Тип протокола IP	Выберите из списка *Любой (*можно указать конкретные протоколы в соответствии со схемой сетевой безопасности в организации).
Зайдите *Свойства→Управление списками IP-фильтра и действиями фильтра→Управление списками IP-фильтров→Добавить*, введите следующие параметры (нажимайте *Далее* после	

заполнения необходимых параметров в каждом окне):	
Имя	Outbound
Зайдите *Список IP-фильтров→Добавить*, введите следующие параметры:	
Описание IP-фильтра и свойство «Отраженный»	Уберите галочку *Отраженный*
Источник IP-трафика	Выберите из списка *Определенный IP-адрес или подсеть*, введите 195.19.40.47
Назначение IP-трафика	Выберите из списка *Определенный IP-адрес или подсеть*, введите 195.19.40.44
Тип протокола IP	Выберите из списка *Любой (*можно указать конкретные протоколы в соответствии со схемой сетевой безопасности в организации).
Зайдите *Свойства→Управление списками IP-фильтра и действиями фильтра→Управление действиями фильтра→Добавить*, введите следующие параметры (нажимайте *Далее* после заполнения необходимых параметров в каждом окне):	
Имя	IKE1
Общие параметры действия фильтра	Согласовать безопасность
Соединение с компьютерами, не поддерживающими IPsec	Запретить небезопасное соединение.
Безопасность IP-трафика	Другой
Нажмите кнопку *Параметры*,введите следующие параметры:	
Целостность данных и адресов без шифрования (AH)	Уберите галочку
Целостность данных с шифрованием (ESP)	Поставьте галочку
Алгоритм проверки целостности	SHA1
Алгоритм шифрования	DES
Смена ключа каждые	Поставьте галочку, введите – 3600 сек.
Зайдите *Свойства→Управление списками IP-фильтра и действиями фильтра→Управление действиями фильтра→IKE1→Изменить*, введите следующие параметры:	
Принимать небезопасную связь, но отвечать с помощью IPsec	Поставьте галочку
Зайдите *Правила→Добавить*, введите следующие параметры (нажимайте *Далее* после заполнения необходимых параметров в каждом окне):	
Конечная точка туннеля	Это правило не определяет туннель
Тип сети	Все сетевые подключения
Список IP-фильтров	Inbound
Действие фильтра	IKE1
Метод проверки подлинности	Использовать данную строку для защиты обмена ключами – введите 123456qw
Зайдите *Правила→Добавить*, введите следующие параметры (нажимайте *Далее* после заполнения необходимых параметров в каждом окне):	
Конечная точка туннеля	Это правило не определяет туннель
Тип сети	Все сетевые подключения
Список IP-фильтров	Outbound
Действие фильтра	IKE1

Метод проверки подлинности	Использовать данную строку для защиты обмена ключами – введите 123456qw
Нажмите правой кнопкой мыщи по созданной политике IP-безопасности, выберите *Назначить*.	
Настройка L2TP-клиента в Microsoft Windows XP	
Создайте VPN-подключение: Пуск→Сетевые подключения→Мастер новых подключений→Подключить к сети на рабочем месте (VPN)→Подключение к виртуальной частной сети→Укажите имя подключения: IPSec VPN→Выберите «Не набирать номер для подключения». Укажите удаленную точку туннеля 195.19.40.44→Введите: Пользователь – user и пароль – P@ssw0rd. В свойствах созданного подключения во вкладке Безопасность→Дополнительно→Параметры выберите Шифрование данных: необязательное (подключаться даже без шифрования), разрешите протокол проверки пароля Microsoft MS-CHAP. Во вкладке Сеть выберите Тип VPN L2TP IPSec VPN. Параметры IPSec – введите ключ 123456qw.	
Настройка L2TP-клиента в Microsoft Windows Vista/7	
Создайте VPN-подключение: Центр управления сетями и общим доступом→Установка подключения или сети→Подключение к рабочему месту (VPN)→Создать новое подключение→использовать мое подключение к Интернету (VPN)→Укажите имя подключения: IPSec VPN→Укажите удаленную точку туннеля 195.19.40.44→Введите: Пользователь – user и пароль – P@ssw0rd. В свойствах созданного подключения во вкладке Безопасность→Дополнительно→Параметры выберите Шифрование данных: необязательное (подключаться даже без шифрования), разрешите протокол проверки пароля Microsoft MS-CHAPv2. Во вкладке Сеть выберите Тип VPN L2TP IPSec VPN. Дополнительные параметры→L2TP – введите ключ 123456qw.	
Упражнение	Проверьте работоспособность туннеля.
Запустите команду ping (с ключом -t) межсетевого экрана с удаленного VPN-клиента, назначьте политику IPSec, запустите созданное подключение L2TP IPsec VPN. На межсетевом экране зайдите в меню *Status→IPSec→ipsec_tunnel.* Уточните скорость трафика в туннеле. Далее зайдите в меню *Status→User Authentication*, уточните выданный IP-адрес удаленным клиентам на интерфейсе L2TP Server. Отключите туннель на MS Windows, уточните состояние запущенной команды ping на lan_ip межсетевого экрана.	
CMD Windows	C:\>ping192.168.10.1 –t –l 1400
Устранение возможных проблем	Если туннель не был создан, решите возникшую проблему с помощью описанных ниже диагностических средств.
Проверьте корректность физических подключений устройств, работоспособность патч-кордов, индикацию на устройствах. Включите режим отладки:	
SSH CLI (Console CLI)	gw-world:/>ikesnoop –on<IP-адрес удаленного VPN-шлюза>
Зайдите в меню*Status→IPSec→ipsec_tunnel.* Проверьте корректность настроек туннелей, уточните статус SA для фазы 1 и фазы 2.	
Зайдите в меню *Status→Logging* или просмотрите лог-сообщения на syslog-сервере, настроенном для работы с межсетевыми экранами.	
Выполните настройку туннелей с простейшими параметрами аутентификации – общим ключом, используйте стандартные (заданные по умолчанию) настройки для алгоритмов IKE и IPSec, режимов IKE, работы с NAT-T, и не используйте пользовательские настройки для XAuth, IKE Config Mode Pool, PFS, ID, Local ID Type. После того, как туннель с этими упрощенными стандартными настройками будет установлен устройствами, измените его параметры в соответствии с особенностями задания в данном сценарии.	
Настройка удаленных L2TP-клиентов с сертификатами (L2TP over IPSec с сертификатами).	

Описание сценария	*Между центральным офисом и удаленными пользователями необходимо настроить подключение по L2TP over IPSec, аутентификация – центр сертификации CA. Сервер CA dc1.ks.ru имеет IP-адрес 192.168.10.7, располагается в* ***lan****-сети межсетевого экрана.*
Схема 41	

Создание необходимых объектов

Microsoft Windows Server 2003/2008

Создайте два набора подписанных CA-сертификатов с помощью CA центра сертификации Microsoft Windows Server 2003/2008.
Зайдите http://dc1.ks.ru/certsrv, выберите опцию *Загрузить CA сертификат*. Сохраните сертификат под именем CA_cert.
Создайте запрос к CA-серверу для генерации клиентских сертификатов.
Зайдите http://dc1.ks.ru/certsrv, выберите опцию *Расширенный запрос сертификата*, введите следующие параметры:

Name	user1
E-Mail	user1@company.com
Company	MSTU
Department	IT
City	Moscow
Type of certificate needed	IPSec Certificate
Key Option	Выберите Create new key set
CSP	Microsoft Edvanced Cryptographic Provider v1.0
Key Usage	Both
Key Size	1024
Automatic Key Container Name	Выберите из списка.
Mark keys as exportable	Поставьте галочку

Создайте сертификат шлюза. Зайдите http://dc1.ks.ru/certsrv, выберите опцию Расширенный запрос сертификата, введите следующие параметры:

Name	gw_cert
Company	MSTU
Department	HQ
City	Moscow
Type of certificate needed	IPSec Certificate
Key Option	ВыберитеCreate new key set
CSP	Microsoft Edvanced Cryptographic Provider v1.0
Key Usage	Both
Key Size	1024
Automatic Key Container Name	Выберите из списка.

Mark keys as exportable	Поставьте галочку
Сохраните файлы сертификатов через экспорт сертификатов. Конвертируйте тип сертификатов в форматы **.cer** и **.key**. Можно воспользоваться программой OpenSSL 0.9.8k или аналогичной программой работы с сертификатами X.509.	
Настройка DFL-860E	
Web-интерфейс	
Создание необходимых объектов	
Импортируйте наборы созданных сертификатов (корневой сертификат CA, сертификат шлюза – CA_cert.cer, gw_cert.cer, gw_cert.key). Зайдите в меню *Objects→Authentication Objects→Add→Certificate.* Введите следующие параметры:	
Name	CA_cert
Upload remove certificate.	Выберите эту опцию и укажите путь к файлам сертификатов.
Зайдите в меню *Objects→Authentication Objects→Add→Certificate.* Введите следующие параметры:	
Name	gw_cert
Upload X.509 certificate.	Выберите эту опцию и укажите путь к файлам сертификатов.
Создадим локальную базу пользователей. Перейдите в меню *User Authentication→Local User Databases→Add→Local User Database*. Во вкладке *General* введите:	
Name	TrustedUsers
Перейдите в меню *User Authentication→Local User Databases→TrustedUsers→Add→User*. Во вкладке *General* введите:	
Username	user1
Password	P@ssw0rd
Confirm Password	P@ssw0rd
Groups	TrustedUsers
Перейдите в *User Authentication→Local User Databases→TrustedUsers→Add→User*. Во вкладке *General* введите:	
Username	user2
Password	P@ssw0rd
Confirm Password	P@ssw0rd
Groups	TrustedUsers
Примечание: 1. Если уже настроены статические туннели или в будущем предполагается их использовать, необходимо расположить их выше так называемого динамического туннеля с параметром Remote Network и/или Remote Gateway, имеющем значение all-nets. Все туннели в списке туннелей Interfaces→IPSec, находящиеся ниже динамического туннеля, окажутся неработоспособны. ***2. Так как IP-адреса VPN-клиентов выездных сотрудников не известны заранее, входящие VPN-соединения от клиентов не могут дифференцироваться. Это означает, что межсетевой экран не способен контролировать доступ к различным частям внутренних сетей. Использование списков идентификаторов представляет собой решение этой проблемы. Список идентификаторов содержит один или более идентификаторов (ID), где каждый идентификатор соответствует предметному полю в сертификате. Списки идентификаторов могут таким образом использоваться для регулирования того, какие сертификаты с доступом использовать и с какими IPSec-туннелями.***	
Создадим объект «список идентификаторов ID». Зайдите в меню *Objects→VPN Objects→IKE ID Lists→Add→ID List.* Введите следующие параметры:	
Name	ID_list_user1

Зайдите в меню *Objects→VPN Objects→IKE ID Lists→ID_List_user1→Ids→Add→ID.* Введите следующие параметры:	
Name	user1
Type	Distinguished name
Common Name	user1
Organization Name	MSTU
Organizational Unit	IT
Country	Russia
Email Address	user1@company.com
Если известен диапазон IP-адресов, то необходимо использовать объект IKE Config Mode Pool. Перейдите в меню *Objects→VPN Objects→IKE Config Mode Pool→Add→IKE Config Mode Pool*. Во вкладке *General* введите:	
Use a pre-defined IPPool Object	Выберите известный диапазон адресов.
Если применяется DHCP-сервер, то необходимо использовать объект IP Pool, в котором указывается данный DHCP-сервер. Создадим объект «IP-адрес DHCP-сервера». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Во вкладке *General* введите следующие параметры:	
Name	ippool_dhcp
Address	172.17.100.10
Перейдите в меню *Objects→IP Pools→Add→IP Pool*. Во вкладке *General* введите:	
Name	ippool
Specify DHCP Server Address	Переместите из списка *Available* в список *Selected* объект ippool_dhcp
Server Filter	all-nets
Client IP Filter	all-nets
Во вкладке *Advanced* введите следующие параметры:	
Routing Table	main
Receive Interface	dmz
Prefetch Leases	10
Примечание: Режим настройки IKE Configuration Mode (Config Mode) – это расширение IKE, позволяющее системе NetDefendOS предоставлять удаленным клиентам информацию о настройках LAN. Используется для динамической настройки IPsec-клиентов с IP-адресами и соответствующими масками и для обмена другой информацией, связанной с DHCP. IP-адрес, назначенный клиенту, может быть в диапазоне предварительно указанных статических IP-адресов, определенных для режима настройки, а также может быть назначен DHCP-серверами, связанными с объектом IP Pool. ***Пул IP-адресов – это IP-адреса DHCP-сервера. Аренда этих адресов продлевается автоматически после истечения указанного срока. Пулы IP-адресов управляют дополнительной информацией, такой как DNS и WINS / NBNS, так же как и обычный DHCP-сервер.***	
Создадим объект «диапазон IP-адресов, которые могут быть использованы удаленными клиентами». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	l2tp_pool
Address	192.168.0.10-192.168.10.20
Создадим объект «внешний IP-адрес, через который могут подключаться клиенты». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	ip_ext
Address	195.19.40.44

Создадим объект «внутренний IP-адрес, через который могут подключаться клиенты». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	ip_int
Address	192.168.10.1
Создадим IPSec-туннель. Зайдите в меню *Interfaces→IPSec→Add→IPSec Tunnel*. Введите следующие параметры:	
Name	ipsec_tunnel
Local Network	ip_ext (укажите all-nets, если межсетевой экран за NAT).
Remote Network	all-nets
Remote Endpoint	none
Encapsulation mode	Transport
Выберите алгоритмы IKE и IPSec:	
IKE Algorithms	Standard (выберите из списка)
IPSec Algorithms	Standard (выберите из списка)
IKE Config ModePool	Выберите созданный ранее диапазон IP Pool (***pre-defined*** или ***Static***)
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите X.509 Certificate из списка.
Root Certificate (s)	Переместите CA_cert из списка Available в список Selected.
Gateway Certificate	Переместите gw_cert из списка Available в список Selected.
Identification list	Выберите ID_list_user1.
Во вкладке *Routing* введите следующие параметры:	
Dynamically add route to the remote network when a tunnel is established	Поставьте галочку
Во вкладке *Advanced* введите следующие параметры:	
Add route for remote network	Уберите галочку
Добавьте PPTP/L2TP. Зайдите в меню *Interfaces→PPTP/L2TP Servers→Add→PPTP/L2TP Server*. Во вкладке *General* введите следующие параметры:	
Name	l2tp_tunnel
Inner IP Address	ip_int
Tunnel Protocol	L2TP
Outer Interface Filter	ipsec_tunnel
Outer Server IP	ip_ext
Во вкладке *PPP Parameters* введите:	
Microsoft Point-to-Point Encryption	Разрешите – поставьте галочки.
IP Pool	l2tp_pool
Во вкладке *Add Route* введите:	
Proxy ARP	Разрешите на интерфейсе, к которому подключена внутренняя сеть.
Создайте правило аутентификации пользователя. Перейдите в *User Authentication→User Authentication Rules→Add→User Authentication Rule*. Во вкладке *General* введите:	
Name	trusted_users_rule
Agent	PPP
Authentication Source	Local

Source Network	all-nets
Interface	l2tp_tunnel
Client Source IP	all-nets
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите pre-shared_key из списка.
Allowed Networks	all-nets
Создайте правило аутентификации пользователя. Перейдите в *User Authentication→s→Add→User Authentication Rule*. Во вкладке *General* введите:	
Name	trusted_users_rule
Agent	PPP
Authentication Source	Local
Interface	l2tp_srv
Originator IP	all-nets
Terminator IP	ip_ext
Во вкладке *Authentication Options* введите:	
Local User DB	Выберите из списка TrustedUsers.
Во вкладке *Agent Options* введите:	
Use MS-CHAP authentication protocol	Поставьте галочку (для клиентов MS Windows XP).
Use MS-CHAP v2 authentication protocol	Поставьте галочку (для клиентов MS Windows Vista/7).
Создание правил IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	inbound_rule
Action	Allow
Service	all-services
Source Interface	l2tp_srv
Source Network	l2tp_pool
Destination Interface	lan
Destination Network	lannet
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	outbound_rule
Action	Allow
Service	all-services
Source Interface	lan
Source Network	lannet
Destination Interface	l2tp_srv
Destination Network	l2tp_pool
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	icmp_rule
Action	Allow
Service	all-icmp
Source Interface	l2tp_srv
Source Network	l2tp_pool

Destination Interface	core
Destination Network	lan_ip
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address l2tp_pool Address=192.168.10.10-192.168.10.20 gw-world:/labs> add IP4Address ip_ext Address=195.19.40.44 gw-world:/labs> add IP4Address ip_intAddress=192.168.10.1 gw-world:/labs> cc gw-world:/> add PSK pre-shared_key Type=ASCII PSKAscii=123456qw gw-world:/> add LocalUserDatabase TrustedUsers gw-world:/> cc LocalUserDatabase TrustedUsers gw-world:/TrustedUsers > add User user1 Password=P@ssw0rd gw-world:/TrustedUsers > add User user2 Password=P@ssw0rd gw-world:/TrustedUsers > cc gw-world:/>add IPPool ippool Interface=dmz PrefetchLeases=10 ServerFilter=all-nets RoutingTable=main ReceiveInterface=dmz DHCPServerType=Interface IPFilter=all-nets gw-world:/> set ConfigModePool IPPoolType=PreDefined IPPool=ippool gw-world:/> cc IDList ID_list_user1 gw-world:/ID_list_user1> add ID user1 Type=DistinguishedName Country=Russia OrganizationalUnit=IT CommonName=user1 OrganizationName=MSTU EMailAddress=user1@company.com gw-world:/ID_list_user1> cc gw-world:/> add Interface IPsecTunnel ipsec_tunnel AuthMethod=Certificate GatewayCertificate=gw_cert RootCertificates=CA_cert IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=labs/ip_ext RemoteNetwork=all-nets AddRouteToRemoteNet=Yes IDList=ID_list_user1 IKEConfigModePool=ConfigModePool EncapsulationMode=Transport gw-world:/> add Interface L2TPServer l2tp_srv Interface=ipsec_tunnel IPPool=labs/l2tp_pool IP=labs/ip_int ServerIP=labs/ip_ext TunnelProtocol=L2TP ProxyARPInterfaces=lanUseUserAuth=Yes gw-world:/> add UserAuthRule Interface=l2tp_srv AuthSource=Local LocalUserDB=TrustedUsers OriginatorIP=all-nets Agent=PPP TerminatorIP=labs/ip_ext Name=trusted_users_rule gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=l2tp_srv SourceNetwork=labs/l2tp_pool DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=l2tp_srv DestinationNetwork=labs/l2tp_pool Name=outbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=l2tp_srv SourceNetwork=labs/l2tp_pool DestinationInterface=core DestinationNetwork=InterfaceAddresses/lan_ipName=icmp_rule gw-world:/1(labs)> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Примечание: 1. Объект сторонний CA-сервер (Objects→VPN Objects→LDAP→Add→LDAP Server) необходимо использовать в случае использования внешнего CA, списки CRL для которого не включены в сертификаты шлюза устройства. ***2. Для успешной загрузки устройством CRL-списков клиент DNS должен корректно разрешать DNS-имя сервера CA.*** ***3. Системное время и даты должны быть корректны, т.к. сертификаты имеют срок действия.***	

Настройка IPSec IKE в Microsoft Windows XP/Vista/7	
Сетевые настройки компьютера должны соответствовать подсети 195.19.40.0/24. IP-адрес компьютера – 195.19.40.47.	
Зайдите Пуск→Выполнить→mmc	
В консоле MMC добавьте оснастку Политики IP-безопасности для локального компьютера.	
Примечание: Для домена MS Windows можно добавить оснастку для групповой политики и далее ее применить на граничном шлюзе в данном сегменте сети.	
В оснастке Политики IP-безопасности задайте новую политику IP-безопасности со следующими параметрами:	
Имя	L2tp_ipsec_policy
Зайдите в свойства созданной политики. Во вкладке *Общие→Параметры* введите:	
Основной ключ безопасной пересылки (PFS)	Уберите галочку
Проверять подлинность и создавать новый ключ каждые	480 мин
Проверять подлинность и создавать новый ключ через каждые	0 сеансов
Зайдите *Общие→Параметры→Методы→Добавить*, введите следующие параметры:	
Алгоритм проверки целостности	SHA1
Алгоритм шифрования	DES
Группа Диффи-Хельмана	средняя (2)
Зайдите *Свойства→Управление списками IP-фильтра и действиями фильтра→Управление списками IP-фильтров→Добавить*, введите следующие параметры (нажимайте *Далее* после заполнения необходимых параметров в каждом окне):	
Имя	Inbound
Зайдите *Список IP-фильтров→Добавить*, введите следующие параметры:	
Описание IP-фильтра и свойство «Отраженный»	Уберите галочку *Отраженный*
Источник IP-трафика	Выберите из списка *Определенный IP-адрес или подсеть*, введите 195.19.40.44
Назначение IP-трафика	Выберите из списка *Определенный IP-адрес или подсеть*, введите 195.19.40.47
Тип протокола IP	Выберите из списка *Любой (*можно указать конкретные протоколы в соответствии со схемой сетевой безопасности в организации).
Зайдите *Свойства→Управление списками IP-фильтра и действиями фильтра→Управление списками IP-фильтров→Добавить*, введите следующие параметры (нажимайте *Далее* после заполнения необходимых параметров в каждом окне):	
Имя	Outbound
Зайдите *Список IP-фильтров→Добавить*, введите следующие параметры:	
Описание IP-фильтра и свойство «Отраженный»	Уберите галочку *Отраженный*
Источник IP-трафика	Выберите из списка *Определенный IP-адрес или подсеть*, введите 195.19.40.47
Назначение IP-трафика	Выберите из списка *Определенный IP-адрес или подсеть*, введите 195.19.40.44
Тип протокола IP	Выберите из списка *Любой (*можно указать конкретные

	протоколы в соответствии со схемой сетевой безопасности в организации).
Зайдите *Свойства→Управление списками IP-фильтра и действиями фильтра→Управление действиями фильтра→Добавить*, введите следующие параметры (нажимайте *Далее* после заполнения необходимых параметров в каждом окне):	
Имя	IKE1
Общие параметры действия фильтра	Согласовать безопасность
Соединение с компьютерами, не поддерживающими IPsec	Запретить небезопасное соединение.
Безопасность IP-трафика	Другой
Нажмите кнопку *Параметры*,введите следующие параметры:	
Целостность данных и адресов без шифрования (AH)	Уберите галочку
Целостность данных с шифрованием (ESP)	Поставьте галочку
Алгоритм проверки целостности	SHA1
Алгоритм шифрования	DES
Смена ключа каждые	Поставьте галочку, введите – 3600 сек.
Зайдите *Свойства→Управление списками IP-фильтра и действиями фильтра→Управление действиями фильтра→IKE1→Изменить*, введите следующие параметры:	
Принимать небезопасную связь, но отвечать с помощью IPsec	Поставьте галочку
Зайдите *Правила→Добавить*, введите следующие параметры (нажимайте *Далее* после заполнения необходимых параметров в каждом окне):	
Конечная точка туннеля	Это правило не определяет туннель
Тип сети	Все сетевые подключения
Список IP-фильтров	Inbound
Действие фильтра	IKE1
Метод проверки подлинности	Использовать сертификат данного центра сертификации (ЦС) – DC=ru, DC=ks, CN=CA. Нажмите *Обзор*, выберите сертификат CA.
Зайдите *Правила→Добавить*, введите следующие параметры (нажимайте *Далее* после заполнения необходимых параметров в каждом окне):	
Конечная точка туннеля	Это правило не определяет туннель
Тип сети	Все сетевые подключения
Список IP-фильтров	Outbound
Действие фильтра	IKE1
Метод проверки подлинности	Использовать сертификат данного центра сертификации (ЦС) – DC=ru, DC=ks, CN=CA. Нажмите *Обзор*, выберите сертификат CA.
Примечание: Сертификат CA должен быть импортирован в хранилище доверенных корневых сертификации для учетной записи компьютера.	
Нажмите правой кнопкой мыщи по созданной политике IP-безопасности, выберите *Назначить*.	
Настройка L2TP-клиента в Microsoft Windows XP	
Создайте VPN-подключение: Пуск→Сетевые подключения→Мастер новых	

подключений→Подключить к сети на рабочем месте (VPN)→Подключение к виртуальной частной сети→Укажите имя подключения:IPSec VPN→Выберите: Не набирать номер для подключения→Укажите удаленную точку туннеля 195.19.40.44→Введите: Пользователь – user и пароль – P@ssw0rd. В свойствах созданного подключения во вкладке Безопасность→Дополнительно→Параметры выберите Шифрование данных: необязательное (подключаться даже без шифрования), разрешите протокол проверки пароля Microsoft MS-CHAP. Во вкладке Сеть выберите Тип VPN L2TP IPSec VPN.
Настройка L2TP-клиента в Microsoft Windows Vista/7
Создайте VPN-подключение: Центр управления сетями и общим доступом→Установка подключения или сети→Подключение к рабочему месту (VPN)→Создать новое подключение→использовать мое подключение к Интернету (VPN)→Укажите имя подключения: IPSec VPN→Укажите удаленную точку туннеля 195.19.40.44→Введите: Пользователь – user и пароль – P@ssw0rd. В свойствах созданного подключения во вкладке Безопасность→Дополнительно→Параметры выберите Шифрование данных: необязательное (подключаться даже без шифрования), разрешите протокол проверки пароля Microsoft MS-CHAPv2. Во вкладке Сеть выберите Тип VPN L2TP IPSec VPN.

Упражнение	Проверьте работоспособность туннеля.
Запустите команду ping (с ключом -t) межсетевого экрана с удаленного VPN-клиента, назначьте политику IPSec, запустите созданное подключение L2TP IPsec VPN. На межсетевом экране зайдите в меню *Status→IPSec→ipsec_tunnel.* Уточните скорость трафика в туннеле. Далее зайдите в *Status→User Authentication*, уточните выданный IP-адрес удаленным клиентам на интерфейсе L2TP Server. Отключите туннель на MS Windows, уточните состояние запущенной команды ping на lan_ip межсетевого экрана.	
CMD Windows	C:\>ping 192.168.1.1 –t –l 1400
Устранение возможных проблем	Если туннель не был создан, решите возникшую проблему с помощью описанных ниже диагностических средств.
Проверьте корректность физических подключений устройств, работоспособность патч-кордов, индикацию на устройствах. Включите режим отладки:	
SSH CLI (Console CLI)	gw-world:/>ikesnoop –on<IP-адрес удаленного VPN-шлюза>
Зайдите в меню *Status→IPSec→ipsec_tunnel.* Проверьте корректность настроек туннелей, уточните статус SA для фазы 1 и фазы 2.	
Зайдите в меню *Status→Logging* или просмотрите лог-сообщения на syslog-сервере, настроенном для работы с межсетевыми экранами.	
Выполните настройку туннелей с простейшими параметрами аутентификации – общим ключом, используйте стандартные (заданные по умолчанию) настройки для алгоритмов IKE и IPSec, режимов IKE, работы с NAT-T, и не используйте пользовательские настройки для XAuth, IKE Config Mode Pool, PFS, ID, Local ID Type. После того, как туннель с этими упрощенными стандартными настройками будет установлен устройствами, измените его параметры в соответствии с особенностями задания в данном сценарии.	
Настройка SSL VPN.	
Описание сценария	*Между центральным офисом и удаленными пользователями необходимо настроить подключение по SSL VPN.*
Схема42	

Настройка DFL-860E (для прошивок старше 2.30.00)	
Web-интерфейс	
Создание необходимых объектов	
Создадим объект «диапазон IP-адресов, которые могут быть использованы удаленными клиентами». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	ssl_pool
Address	192.168.10.10-192.168.10.20
Создадим объект «внешний IP-адрес, через который могут подключаться клиенты». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	ip_ext (wan1_ip)
Address	192.168.110.254
Создадим объект «внутренний IP-адрес, через который могут подключаться клиенты». Зайдите в *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	ip_int (lan_ip)
Address	192.168.10.1
Создадим локальную базу пользователей. Перейдите в меню *User Authentication→Local User Databases→Add→Local User Database*. Во вкладке *General* введите:	
Name	TrustedUsers
Перейдите в меню *User Authentication→Local User Databases→TrustedUsers→Add→User*. Во вкладке *General* введите:	
Username	user1
Password	P@ssw0rd
Confirm Password	P@ssw0rd
Groups	TrustedUsers
Перейдите в меню *User Authentication→Local User Databases→TrustedUsers→Add→User*. Во вкладке *General* введите:	
Username	user2
Password	P@ssw0rd
Confirm Password	P@ssw0rd
Groups	TrustedUsers
Создадим сервер SSL VPN. Зайдите в меню *Interfaces→SSL VPN Interface→Add→SSL VPN Interface.* Введите следующие параметры:	
Name	ssl_vpn
Inner IP	ip_int
Outer Interface	wan1
Server IP	ip_ext
Server Port	10443 (можно выбрать стандартный порт 443)
IP Address Pool	ssl_pool
Во вкладке *Add Route* введите следующие параметры:	
Selected	Выберите необходимые интерфейсы из списка (например, lan).
Создайте правило аутентификации пользователя. Перейдите в меню *User Authentication→User Authentication Rules→Add→User Authentication Rule*. Во вкладке *General* введите:	
Name	ssl_rule
Authentication agent	L2TP/PPTP/SSL VPN

Authentication Source	Local
Interface	ssl_vpn
Originator IP	all-nets (можно указать более узкий диапазон)
Terminator IP	ip_ext
Во вкладке *Authentication* Options введите:	
Local User DB	Выберите из списка TrustedUsers.
Во вкладке *Agent* Options введите:	
Use MS-CHAP authentication protocol	Поставьте галочку (для клиентов MS Windows XP).
Use MS-CHAP v2 authentication protocol	Поставьте галочку (для клиентов MS Windows Vista/7).
Создание правила IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	inbound_rule
Action	Allow
Service	all-services
Source Interface	ssl_vpn
Source Network	ssl_pool
Destination Interface	lan
Destination Network	lannet
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	outbound_rule
Action	Allow
Service	all-services
Source Interface	lan
Source Network	lannet
Destination Interface	ssl_vpn
Destination Network	ssl_pool
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	icmp_rule
Action	Allow
Service	all-icmp
Source Interface	ssl_vpn
Source Network	ssl_pool
Destination Interface	core
Destination Network	lan_ip
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address ssl_pool Address=192.168.10.10-192.168.10.20 gw-world:/labs> add IP4Address ip_ext Address=192.168.110.254 gw-world:/labs> add IP4Address ip_intAddress=192.168.10.1 gw-world:/labs> cc	

gw-world:/> add LocalUserDatabase TrustedUsers
gw-world:/> cc LocalUserDatabase TrustedUsers
gw-world:/TrustedUsers > add User user1 Password=P@ssw0rd
gw-world:/TrustedUsers > add User user2 Password=P@ssw0rd
gw-world:/TrustedUsers > cc
gw-world:/>add Interface SSLVPNInterface ssl_vpn InnerIP=labs/ip_int IPAddressPool=labs/ssl_pool OuterInterface=wan1 ServerIP=labs/ip_ext ServerPort=10443 ProxyARPInterfaces=lan
gw-world:/> add UserAuthRule Interface=ssl_vpn AuthSource=Local LocalUserDB=TrustedUsers OriginatorIP=labs/ip_int Agent=PPP TerminatorIP=labs/ip_ext PPPAuthMSCHAP=Yes PPPAuthMSCHAPv2=Yes PPPAuthNoAuth=No PPPAuthPAP=No Name=ssl_rule
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=ssl_vpn SourceNetwork=labs/ssl_pool DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=ssl_vpn DestinationNetwork=labs/ssl_pool Name=outbound_rule
gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ssl_vpn SourceNetwork=labs/ssl_pool DestinationInterface=core DestinationNetwork=InterfaceAddresses/lan_ipName=icmp_rule
gw-world:/1(labs)> cc
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Настройка SSL VPN клиента в Microsoft Windows XP/Vista/7

Установите программное обеспечение SSL VPN клиент или загрузите его с межсетевого экрана. Укажите следующие параметры:

Хост VPN-сервера	192.168.110.254 (или DNS-имя)
Порт VPN-сервера	10443
Имя пользователя	user1
Пароль	P@ssw0rd
Протокол	TCP (SSL/TLS)
Сжатие	Без сжатия

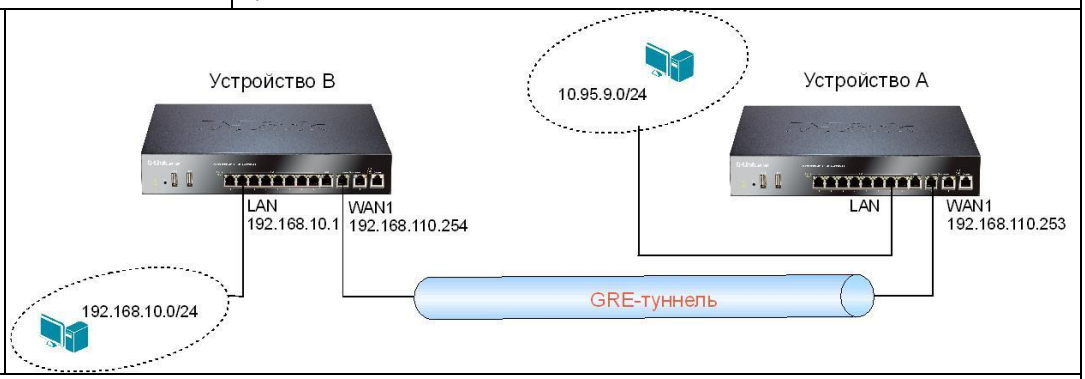
Примечание: 1. SSL VPN клиент может быть скачен с межсетевого экрана при соединении HTTPS или установлен из дистрибутива заранее на клиентском компьютере. Может использоваться D-Link SSL VPN клиент или любой другой совместимый условно-бесплатный SSL VPN клиент, например BirdsSoft VPN-X.
2. SSL VPN сервер может быть настроен для PPPoE, для этого необходимо указать в качестве исходящего интерфейса соответствующий PPPoE-интерфейс.

Упражнение	Проверьте работоспособность SSL VPN.

Откройте SSL-сессию с удаленного клиента. Запустите команду ping (с ключом -t) межсетевого экрана с удаленного SSL VPN клиента. На межсетевом экране зайдите в меню *Status→Interfaces→ssl_vpn.* Уточните скорость трафика в туннеле. Далее зайдите в *Status→User Authentication*, уточните выданный IP-адрес удаленным клиентам на интерфейсе SSL VPN Server. Отключите туннель на MS Windows, уточните состояние запущенной команды ping на lan_ip межсетевого экрана.

Internet ExplorerOC Windows	https://<wan1_ip> Введите имя пользователя, пароль.
CMD Windows	C:\>ping 192.168.10.1 –t –l 1400
Устранение возможных проблем	Если туннель не был создан, решите возникшую проблему с помощью описанных ниже диагностических средств.

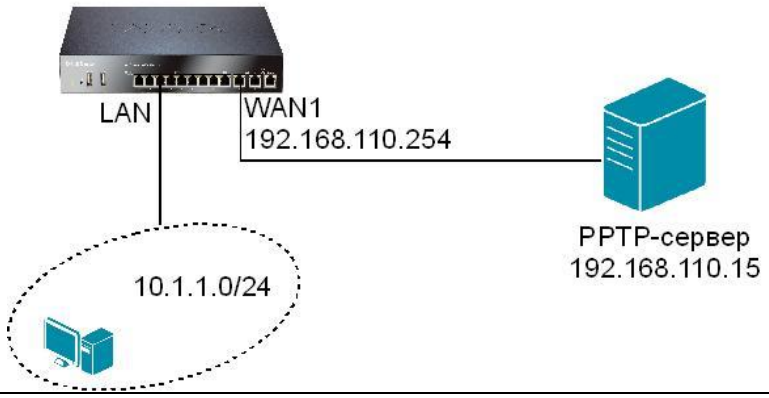
Проверьте корректность физических подключений устройств, работоспособность патч-кордов,

индикацию на устройствах. Включите режим отладки:	
Зайдите в меню *Status→Interfaces→ssl_vpn.* Проверьте корректность настроек туннелей.	
Зайдите в меню *Status→Logging* или просмотрите лог-сообщения на syslog-сервере, настроенном для работы с межсетевыми экранами.	
Выполните настройку туннелей с простейшими параметрами аутентификации, используйте стандартные (заданные по умолчанию) настройки для алгоритмов. После того как туннель с этими упрощенными стандартными настройками будет установлен между устройствами, измените его параметры в соответствии с особенностями задания в данном сценарии.	
GRE-туннель	
Описание сценария	*Между устройством A и B необходимо организовать GRE-туннель.*
Схема 43	
Настройка DFL-860E	
Устройство A	
Web-интерфейс	
Создание необходимых объектов	
Создадим объект «IP-адрес удаленной конечной точки туннеля. Зайдите в меню *Objects→Address book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote_ep
Address	192.168.110.254
Создадим объект «удаленную подсеть». Зайдите в *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote_net
Address	192.168.10.0/24
Создадим объект «IP-адрес начала туннеля. Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	gre_ip
Address	192.168.0.1
Изменим объект «IP-адрес wan1_ip». Зайдите в меню *Interfaces→Ethernet→wan1.* Снимите выделение *Enable DHCP Client*	
Зайдите в меню *Objects→Address Book→Interface Addresses→wan1_ip.* Введите следующие параметры:	
Name	wan1_ip
Address	192.168.110.253
Создадим GRE-туннель. Зайдите в меню *Interfaces→GRE→Add→GRE Tunnel.* Введите следующие параметры:	

Name	gre_tunnel
Address	gre_ip
Remote Network	remote_net
Remote Endpoint	remote_ep
Во вкладке *Advanced* введите следующие параметры:	
Automatically add a route for this interface using the given remote network.	Поставьте галочку
Создание правил IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	outbound_rule
Action	Allow
Service	all-services
Source Interface	lan
Source Network	lannet
Destination Interface	gre_tunnel
Destination Network	remote_net
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	inbound_rule
Action	Allow
Service	all-services
Source Interface	gre_tunnel
Source Network	remote_net
Destination Interface	lan
Destination Network	lannet
Зайдите в *Configuration* и выберите *Save and Activate*.	
Командняа строка (CLI)	
gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address remote_ep Address=192.168.110.254 gw-world:/labs> add IP4Address remote_net Address=192.168.10.0/24 gw-world:/labs> add IP4Address gre_ip Address=192.168.0.1 gw-world:/>set Interface Ethernet wan1 DHCPEnabled=No gw-world:/labs> set Address IP4Address InterfaceAddresses/wan1_ip Address=192.168.110.253 gw-world:/labs> add Interface GRETunnel gre_tunnel IP=labs/gre_ip Network=labs/remote_net RemoteEndpoint=labs/remote_ep AutoInterfaceNetworkRoute=Yes gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=all-services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=gre_tunnel DestinationNetwork=labs/remote_netName=outbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all-services SourceInterface=gre_tunnel SourceNetwork=labs/remote_net DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule gw-world:/1(labs)> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	

Настройка DFL-860E	
Устройство B	
Web-интерфейс	
Создание необходимых объектов	
Создадим объект «IP-адрес удаленной конечной точки туннеля». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote_ep
Address	192.168.110.253
Создадим объект «удаленную подсеть». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote_net
Address	10.95.9.0/24
Создадим объект «IP-адрес начала туннеля». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	gre_ip
Address	192.168.0.2
Создадим GRE-туннель. Зайдите в меню *Interfaces→GRE→Add→GRE Tunnel.* Введите следующие параметры:	
Name	gre_tunnel
IP Address	gre_ip
Remote Network	remote_net
Remote Endpoint	remote_ep
Во вкладке *Advanced* введите следующие параметры:	
Automatically add a route for this interface using the given remote network.	Поставьте галочку
Создание правил IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	outbound_rule
Action	Allow
Service	all-services
Source Interface	lan
Source Network	lannet
Destination Interface	gre_tunnel
Destination Network	remote_net
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	inbound_rule
Action	Allow
Service	all-services
Source Interface	gre_tunnel
Source Network	remote_net
Destination Interface	lan
Destination Network	lannet

Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address remote_ep Address=192.168.110.253 gw-world:/labs> add IP4Address remote_net Address=10.95.9.0/24 gw-world:/labs> add IP4Address gre_ip Address=192.168.0.2 gw-world:/labs> cc gw-world:/> set Address IP4Address InterfaceAddresses/wan1_ip Address=192.168.110.254 gw-world:/> add Interface GRETunnel gre_tunnel IP=labs/gre_ip Network=labs/remote_net RemoteEndpoint=labs/remote_ep AutoInterfaceNetworkRoute=Yes gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=all-services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=gre_tunnel DestinationNetwork=labs/remote_net Name=outbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all-services SourceInterface=gre_tunnel SourceNetwork=labs/remote_net DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule gw-world:/1(labs)> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Упражнение	Проверьте работоспособность туннеля.
Запустите команду ping (с ключом -t) межсетевого экрана с устройства A на устройство B через GRE-туннель. На межсетевом экране зайдите в меню *Status→Interfaces→gre_tunnel*. Уточните скорость трафика в туннеле.	
CMD Windows	C:\>ping 192.168.10.1 –t–l 1400
Устранение возможных проблем	Если туннель не был создан, решите возникшую проблему с помощью описанных ниже диагностических средств.
Проверьте корректность физических подключений устройств, работоспособность патч-кордов, индикацию на устройствах.	
На устройствах зайдите в меню *Status→Interfaces→gre_tunnel*. Проверьте корректность настроек туннелей.	
На устройствах зайдите в меню *Status→Logging* или просмотрите лог-сообщения на syslog-сервере, настроенном для работы с межсетевыми экранами.	
PPTP ALG для PPTP-туннелей с NAT	
Описание сценария	*Для решения проблем с доступом к PPTP-клиентов через NAT удаленному VPN-серверу необходимо настроить PPTP ALG для службы HTTP. Пользователи в **lan**-сети межсетевого экрана должны иметь доступ по протоколу PPTP к VPN-серверу, имеющему IP-адрес 195.168.110.15 (через интерфейс **wan1**).*

Схема 44	

Настройка DFL-860E

Web-интерфейс

Добавим новый PPTP ALG. Зайдите в *Objects→ALG→Add→PPTP ALG*. Во вкладке *General* введите следующие параметры:

Name	pptp_alg
Echo timeout	100
Idle timeout	100

Добавим новый сервис *pptp_srv*, в которой используется созданный PPTP ALG. Зайдите в меню *Objects→Servises→Add→TCP/UDP Service*. Во вкладке *General* введите следующие параметры:

Name	pptp_srv
Type	TCP
Source	0-65535
Destination	1723
ALG	pptp_alg (выберите из списка)
Max Sessions	200

Создание правил IP Rule

Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:

Name	pptp_rule
Action	NAT
Service	pptp_srv
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets

Зайдите в меню *Configuration* и выберите *Save and Activate*.

Командная строка (CLI)

```
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.168.110.254
gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.168.110.0/24
gw-world:/>add ALG ALG_PPTP pptp_alg EchoTimeout=100 IdleTimeout=100
gw-world:/>add Service ServiceTCPUDP pptp_srv DestinationPorts=1723 SourcePorts=0-65535
Type=TCP ALG=pptp_alg MaxSessions=200
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=NAT Service=pptp_srv SourceInterface=lan
SourceNetwork=InterfaceAddresses/lannet DestinationInterface=wan1DestinationNetwork=all-
netsName=pptp_rule
gw-world:/1(labs)> cc
```

gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Настройка VPN-сервера (PPTP-сервера) на базе службы маршрутизации и удаленного доступа (RRAS) в Microsoft Windows Server 2003/2008

Откройте консоль Маршрутизация и удаленный доступ, убедитесь, что служба запущена. Откройте *Свойства*, нажав правой кнопкой мыши по имени сервера, введите следующие параметры во вкладке *Общие*:

Использовать этот компьютер как IP4-маршрутизатор	Локальной сети и вызова по требованию
IP4-сервер удаленного доступа	Поставьте галочку

Откройте *Свойства*, нажав правой кнопкой мыши по имени сервера, введите следующие параметры на вкладке *PPP*:

Многоканальные подключения	Поставьте галочку
Расширения протокола LCP	Поставьте галочку

Откройте *Свойства*, нажав правой кнопкой мыши по опции *Порты*, выделите мышью WAN Miniport (PPTP), нажмите *Настроить*, введите следующие параметры:

Подключения удаленного доступа (только входящие)	Поставьте галочку
Подключения по требованию (входящие и исходящие)	Уберите галочку

Откройте консоль Маршрутизация и удаленный доступ, убедитесь, что служба запущена. Откройте *Свойства*, нажав правой кнопкой мыши по имени сервера, введите следующие параметры на вкладке *IPv4*:

Включить пересылку IPv4	Поставьте галочку
Назначение IPv4-адресов	Статический пул адресов

Нажмите *Добавить*, создайте пул адресов, входящий в диапазон адресов локальной сети, к которой организуется удаленный доступ:

Начальный IP-адрес	10.1.1.10
Конечный IP-адрес	10.1.1.50

Нажмите *Ok*, при необходимости перезапустите службу RRAS.

Настройка PPTP-клиента в Microsoft Windows XP

Создайте VPN-подключение: Пуск→Сетевые подключения→Мастер новых подключений→Подключить к сети на рабочем месте (VPN)→Подключение к виртуальной частной сети→Укажите имя подключения: PPTP_VPN→Выберите: Не набирать номер для подключения→Укажите удаленную точку туннеля 195.168.110.15→Введите: Пользователь – user1 и пароль – P@ssw0rd. В свойствах созданного подключения во вкладке Безопасность→Дополнительно→Параметры выберите Шифрование данных: необязательное (подключаться даже без шифрования), разрешите протокол проверки пароля Microsoft MS-CHAP. Во вкладке Сеть выберите Тип VPN PPTP VPN.

Настройка PPTP-клиента в Microsoft Windows Vista/7

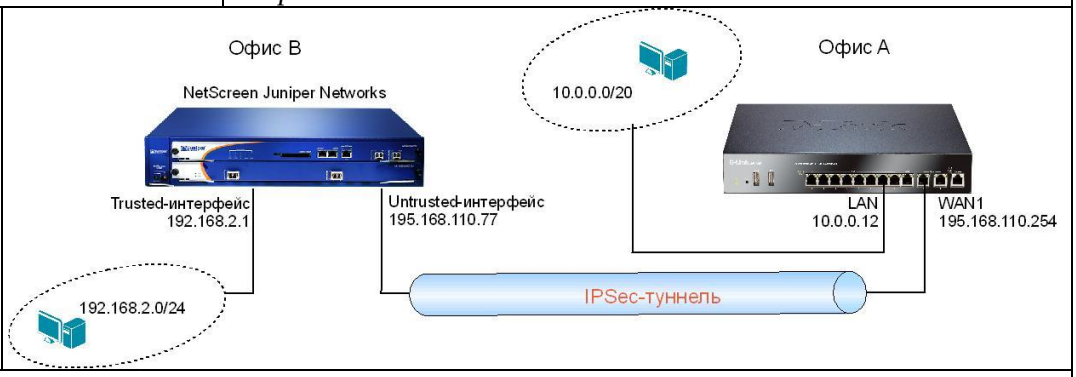
Создайте VPN-подключение: Центр управлнения сетями и общим доступом→Установка подключения или сети→Подключение к рабочему месту (VPN)→Создать новое подключение→использовать мое подключение к Интернету (VPN)→Укажите имя подключения: PPTP_VPN→Укажите удаленную точку туннеля 195.168.110.15→Введите: Пользователь – user1 и пароль – P@ssw0rd. В свойствах созданного подключения во вкладке Безопасность→Дополнительно→Параметры выберите Шифрование данных: необязательное (подключаться даже без шифрования), разрешите протокол проверки пароля Microsoft MS-

CHAPv2. Во вкладке Сеть выберите Тип VPN PPTPVPN.	
Упражнение	Проверьте возможность подключения к удаленному серверу через NAT сразу двух PPTP-клиентов user1 и user2.
WAN Miniport (PPTP)	Запустите созданное подключение с двух компьютеров в **lan-**сети.
Устранение возможных проблем	Если туннель не был создан, решите возникшую проблему с помощью описанных ниже диагностических средств.
Проверьте корректность физических подключений устройств, работоспособность патч-кордов, индикацию на устройствах.	
Зайдите в меню *Status→Logging* или просмотрите лог-сообщения на syslog-сервере, настроенном для работы с межсетевыми экранами.	

ЗАНЯТИЕ №9.4. Примеры настройки туннелей между межсетевым экраном D-Link и программными/аппаратными устройствами безопасности других производителей.

IPSec-туннель LAN to LAN с заранее установленным ключом совместного использования (pre-shared key) между межсетевым экраном D-Link и устройством безопасности NetScreen Juniper Networks (…и маршрутизатором Cisco VPN; …и межсетевым экраном Cisco PIX/ASA; …и Microsoft Forefront Threat Management Gateway 2010; …и FreeBSD Unix).

L2TP over IPSec туннель LAN to LAN с заранее установленным ключом совместного использования (pre-shared key) между межсетевым экраном D-Link и удаленным офисом с использованием службы маршрутизации и удаленного доступа Microsoft Windows Server 2008 R2.

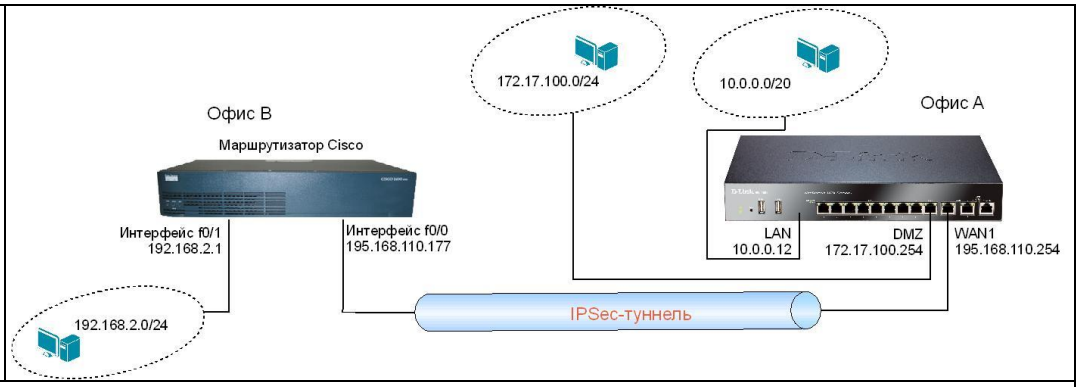
IPSec-туннель LAN to LAN с заранее установленным ключем совместного использования (pre-shared key) между межсетевым экраном D-Link и NetScreen Juniper Networks.	
Описание сценария	*Между офисом A и офисом B необходимо настроить IPSec туннель для безопасного соединения по VPN, аутентификация – общий секрет. Устройство безопасности офиса A – межсетевой экран D-Link, устройство безопасности офиса B – NetScreen Juniper Networks.*
Схема 45	
<u>Настройка DFL-860E</u>	
<u>Web-интерфейс</u>	
Убедитесь в правильных настройках параметров интерфейсов:	
Name	lannet
Address	10.0.0.0/20
Name	lan_ip
Address	10.0.0.12
Name	wan1_ip
Address	195.168.110.254
Создание необходимых объектов	
Создадим объект «Pre-shared Key». Зайдите в меню *Objects→Authentication Objects→Add→Pre-Shared Key*. Введите следующие параметры:	
Name	pre-shared_key
Выберите *Shared Secret*. Введите следующие параметры:	
Shared Secret	123456qw
Confirm Secret	123456qw
Создадим объект «удаленную подсеть за VPN-шлюзом». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	

Name	remote_net
Address	192.168.2.0/24
Создадим объект «IP-адрес удаленного VPN-шлюза». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote_gw
Address	195.168.110.77
Создадим IPSec-туннель. Зайдите в меню *Interfaces→IPSec→Add→IPSecTunnel.* Введите следующие параметры:	
Name	ipsec_tunnel
Local Network	lannet (10.0.0.0/20)
Remote Network	remote_net
Remote Endpoint	remote_gw
Encapsulation mode	Tunnel
Выберите алгоритмы IKE и IPSec:	
IKE Algorithms	Standard (выберите из списка)
IPSec Algorithms	Standard (выберите из списка)
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите pre-shared_key из списка.
Local ID	Auto (выберите из списка)
Во вкладке *IKE Settings* введите следующие параметры:	
IKE	Main, DHGroup 2 (выберите из списка)
Perfect Forward Secrecy	PFS, DHGroup 2 (выберите из списка)
Security Association	Per Net
NAT Traversal	On if supported and NATed
Use Dead Peer Detection	Поставьте галочку
Во вкладке *Keep-alive* введите следующие параметры:	
Keep-alive	Выберите Auto из списка
Во вкладке *Advanced* введите следующие параметры:	
Add route for remote network	Уберите галочку
Создание правил IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	outbound_rule
Action	Allow
Service	all-services
Source Interface	lan
Source Network	lannet
Destination Interface	ipsec_tunnel
Destination Network	remote_net
Зайдите в меню *Rules→IP Rule→Add→IP Rule.* Во вкладке *General* введите:	
Name	inbound_rule
Action	Allow
Service	all-services
Source Interface	ipsec_tunnel
Source Network	remote_net

Destination Interface	lan
Destination Network	lannet
Создадим IP Rule, разрешающее выполнение команды ping в туннеле. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	icmp_allow
Action	Allow
Service	all-icmp
Source Interface	ipsec_tunnel
Source Network	all-nets
Destination Interface	core
Destination Network	all-nets
Создание маршрута для туннеля	
Зайдите в меню *Routing→Routing Tables→Add→Routing Table.* Во вкладке *General* введите:	
Name	labs
Ordering	First (выберите из списка).
Нажмите правой кнопкой мыши по созданной таблице маршрутизации *labs*, выберите *Move to top*.	
Зайдите в меню *Routing→Routing Tables→labs→Add→Route*. Во вкладке *General* введите:	
Interface	ipsec_tunnel
Network	remote_net
Gateway	-
Local IP address	-
Metric	10
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.168.110.254 gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.168.110.0/24 gw-world:/> set IP4Address InterfaceAddresses/lan_ip Address=10.0.0.12 gw-world:/> set IP4Address InterfaceAddresses/lannet Address=10.0.0.0/20 gw-world:/>add PSK pre-shared_key Type=ASCII PSKAscii=123456qw gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address remote_net Address=192.168.2.0/24 gw-world:/labs> add IP4Address remote_gw Address=195.168.110.77 gw-world:/labs> cc gw-world:/>add Interface IPsecTunnel ipsec_tunnel AuthMethod=PSK IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet PSK=pre-shared_key RemoteNetwork=labs/remote_net RemoteEndpoint=labs/remote_gwKeepAlive=Auto AddRouteToRemoteNet=No PFS=PFS PFSDHGroup=2 SetupSAPer=Net DHGroup=2 NATTraversal=OnIfNeeded DeadPeerDetection=YesEncapsulationMode=Tunnel gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=ipsec_tunnel DestinationNetwork=labs/remote_net Name=outbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=ipsec_tunnel SourceNetwork=labs/remote_net DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnel	

SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=all-nets Name=icmp_allow gw-world:/1(labs)> cc gw-world:/>add RoutingTable labs Ordering=First gw-world:/>cc RoutingTable labs gw-world:/labs>add Route Interface=ipsec_tunnel Network=labs/remote_net Metric=10 gw-world:/labs> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Настройка Netscreen Juniper Networks	
Web-интерфейс	
Конфигурация интерфейсов	
Имя	trust (зона Trusted)
Зайдите в *Network→Interfaces→trust→Edit.* Введите следующие параметры:	
Static IP	192.168.2.1/24
Нажмите *Apply* и *Ok.*	
Имя	untrust (зона Untrusted)
Зайдите в *Network→Interfaces→untrust→Edit.* Введите следующие параметры:	
Static IP	195.168.110.77/24
Нажмите *Apply* и *Ok.*	
Конфигурация удаленного VPN-шлюза	
Зайдите в *VPNs→Auto Key Advanced→Gateway→New.* Введите следующие параметры:	
Gateway Name	DLink_gw
Remote Gateway Type	StaticIPAddress (выберите из списка)
IP Address/Hostname	195.168.110.254
Preshared Key	123456qw
Outgoing Interface	untrust
Зайдите в *VPNs→Auto Key Advanced→Gateway→DLink_gw→Advanced.* Введите следующие параметры:	
Security Level	User Defined (Custom)
Phase 1 Proposal	pre-g1-des-md5 pre-g1-des-sha pre-g2-des-md5 pre-g2-des-sha
Mode (Initiator)	Main (ID Protection)
Нажмите *Return* и *Ok.*	
Настройка туннеля	
Зайдите в *VPNs→Auto Key IKE→New.* Введите следующие параметры:	
VPN Name	DLink_tunnel
Security Level	Custom
Remote Gateway	Predefined - DLink_gw (выберите из списка)
Зайдите в *VPNs→Auto Key IKE→DLink_tunnel→Advanced.* Введите следующие параметры:	
Security Level	User Defined (Custom)
Phase 2 Proposal	g2-esp-des-md5 g2-esp-des-sha

	none none
Bind to	Tunnel Interface – tunnel.1 (выберите из списка)
Proxy-ID	Поставьте галочку
Local IP/Netmask	192.168.2.0/24
Remote IP/Netmask	10.0.0.0/20
Service	ANY
Нажмите *Return* и *Ok*.	
Проверка работоспособности туннеля	
Конфигурация сохраняется автоматически, после нажатия *Ok* или *Apply*. Правила, разрешающие трафик в туннеле, и маршрут к удаленной сети также должны добавиться автоматически. Зайдите в *VPNs→Monitor Status.* Уточните статус созданного соединения SA.	
Зайдите в *Network→Routing→Routing Entries.* Найдите автоматически созданный маршрут к удаленной сети.	
Зайдите в *Policies.* Найдите автоматически созданные правила.	
Упражнение	Проверьте работоспособность туннеля.
Зайдите в *Status→IPSec→ipsec_tunnel.* Уточните статус SA.	
Запустите команду ping (с ключом -t) с хостов, подключенных к **lan-**интерфейсам межсетевых экранов D-Link и Netscreen. Зайдите в меню *Status→IPSec→ipsec_tunnel.* Уточните скорость трафика в туннеле.	
CMD Windows (устройство D-Link)	C:\>ping 192.168.2.1
CMD Windows (устройство Netscreen)	C:\>ping 10.0.0.12
Устранение возможных проблем	Если туннель не был создан устройствами, решите возникшую проблему с помощью описанных ниже диагностических средств.
Проверьте корректность физических подключений устройств, работоспособность патч-кордов, индикацию на устройствах. Включите режим отладки:	
SSH CLI (Console CLI) Устройство D-Link	gw-world:/>ikesnoop –on<IP-адресудаленногоVPN-шлюза>
Зайдите в меню *Status→IPSec→ipsec_tunnel.* Проверьте корректность настроек туннелей, уточните статус SA для фазы 1 и фазы 2.	
Зайдите в меню *Status→Logging* или просмотрите лог-сообщения на syslog-сервере, настроенном для работы с межсетевыми экранами.	
Выполните настройку туннелей с простейшими параметрами аутентификации – общим ключом, используйте стандартные (заданные по умолчанию) настройки для алгоритмов IKE и IPSec, режимов IKE, работы с NAT-T, и не используйте пользовательские настройки для XAuth, IKE Config Mode Pool, PFS, ID, Local ID Type. После того как туннель с этими упрощенными стандартными настройками будет установлен устройствами, измените его параметры в соответствии с особенностями задания в данном сценарии.	
IPSec-туннель LAN to LAN с заранее установленным ключом совместного использования (pre-shared key) между межсетевым экраном D-Link и маршрутизатором Cisco VPN Site-to-Site.	
Описание сценария	*Между офисом A и офисом B необходимо настроить IPSec-туннель для безопасного соединения по VPN, аутентификация – общий ключ. Устройство безопасности офиса A – межсетевой экран D-Link, устройство безопасности офиса B – маршрутизатор Cisco.*

Схема 46	

Настройка DFL-860E

Web-интерфейс

Убедитесь в правильных настройках параметров интерфейсов:

Name	dmznet
Address	172.17.100.0/24
Name	dmz_ip
Address	172.17.100.254
Name	wan1_ip
Address	195.168.110.254

Создание необходимых объектов

Создадим объект «Pre-shared Key». Зайдите в меню *Objects→Authentication Objects→Add→Pre-Shared Key*. Введите следующие параметры:

Name	pre-shared_key

Выберите *Shared Secret*. Введите следующие параметры:

Shared Secret	123456qw
Confirm Secret	123456qw

Создадим объект «удаленную подсеть за VPN-шлюзом». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:

Name	remote_net
IPAddress	192.168.2.0/24

Создадим объект «IP-адрес удаленного VPN-шлюза. Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:

Name	remote_gw
IPAddress	195.168.110.177

Создадим IPSec-туннель. Зайдите в меню *Interfaces→IPSec→Add→IPSec Tunnel*. Введите следующие параметры:

Name	ipsec_tunnel
Local Network	dmznet
Remote Network	remote_net
Remote Endpoint	remote_gw
Encapsulation mode	Tunnel

Выберите алгоритмы IKE и IPSec:

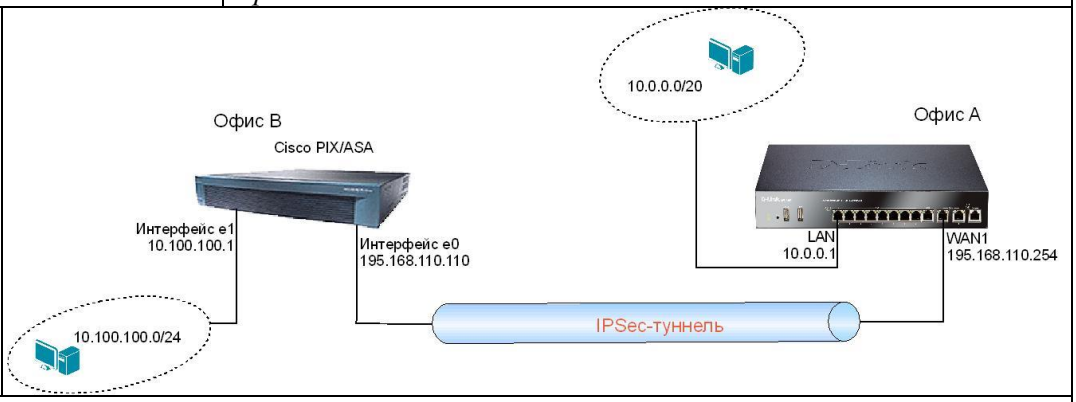
IKE Algorithms	Standard (выберите из списка)
IKE Lifetime	86400 seconds

IPSec Algorithms	Standard (выберите из списка)
IPsec Lifetime	3600 seconds
IPsec Lifetime	4608000 kilobytes
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите pre-shared_key из списка.
Local ID	Auto (выберите из списка)
Во вкладке *IKE Settings* введите следующие параметры:	
IKE	Main, DHGroup1 (выберите из списка)
Perfect Forward Secrecy	PFS, DHGroup1 (выберите из списка)
Security Association	Per Net
NAT Traversal	On if supported and NATed
Use Dead Peer Detection	Поставьте галочку
Во вкладке *Keep-alive* введите следующие параметры:	
Keep-alive	Выберите Auto из списка
Во вкладке *Advanced* введите следующие параметры:	
Add route for remote network	Уберите галочку
Создание правил IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	outbound_rule
Action	Allow
Service	all-services
Source Interface	dmz
Source Network	dmznet
Destination Interface	ipsec_tunnel
Destination Network	remote_net
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	inbound_rule
Action	Allow
Service	all-services
Source Interface	ipsec_tunnel
Source Network	remote_net
Destination Interface	dmz
Destination Network	dmznet
Создадим IP Rule, разрешающее выполнение команды ping в туннеле. Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	icmp_allow
Action	Allow
Service	all-icmp
Source Interface	ipsec_tunnel
Source Network	all-nets
Destination Interface	core
Destination Network	all-nets
Создание маршрута для туннеля	

Зайдите в *Routing→Routing Tables→Add→Routing Table*. Во вкладке *General* введите:	
Name	labs
Ordering	First (выберите из списка).
Нажмите правой кнопкой мыши по созданной таблице маршрутизации *labs*, выберите *Move to top*.	
Зайдите в меню *Routing→Routing Tables→labs→Add→Route*. Во вкладке *General* введите:	
Interface	ipsec_tunnel
Network	remote_net
Gateway	-
Local IP address	-
Metric	10
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.168.110.254 gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.168.110.0/24 gw-world:/> set IP4Address InterfaceAddresses/dmz_ip Address=172.17.100.254 gw-world:/> set IP4Address InterfaceAddresses/dmznet Address=172.17.100.0/24 gw-world:/>add PSK pre-shared_key Type=ASCII PSKAscii=123456qw gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address remote_net Address=192.168.2.0/24 gw-world:/labs> add IP4Address remote_gw Address=195.168.110.177 gw-world:/labs> cc gw-world:/>add Interface IPsecTunnel ipsec_tunnel AuthMethod=PSK IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet PSK=pre-shared_key RemoteNetwork=labs/remote_net RemoteEndpoint=labs/remote_gwKeepAlive=Auto AddRouteToRemoteNet=No IKELifeTimeSeconds=86400 IPsecLifeTimeKilobytes=4608000 IPsecLifeTimeSeconds=3600 PFS=PFS PFSDHGroup=1 SetupSAPer=Net DHGroup=1 NATTraversal=OnIfNeeded DeadPeerDetection=YesEncapsulationMode=Tunnel gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=dmz SourceNetwork=InterfaceAddresses/dmznet DestinationInterface=ipsec_tunnel DestinationNetwork=labs/remote_net Name=outbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=ipsec_tunnel SourceNetwork=labs/remote_net DestinationInterface=dmz DestinationNetwork=InterfaceAddresses/dmznet Name=inbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnel SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=all-nets Name=icmp_allow gw-world:/1(labs)> cc gw-world:/>add RoutingTable labs Ordering=First gw-world:/>cc RoutingTable labs gw-world:/labs>add Route Interface=ipsec_tunnel Network=labs/remote_net Metric=10 gw-world:/labs> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Настройка маршрутизатора Cisco (на примере модели Cisco 2691, IOS 12.4 (13b))	
Командная строка (CLI) – консоль	
cisco>enable cisco#configure terminal	

Enter configuration commands, one per line. End with CNTL/Z. cisco(config)#interface f0/0 cisco(config-if)#ip address 195.168.110.117 255.255.255.0 cisco(config-if)#no shutdown cisco(config-if)#exit cisco(config)#interface f0/1 cisco(config-if)#ip address 192.168.2.1 255.255.255.0 cisco(config-if)#no shutdown cisco(config-if)#exit cisco(config)#ip route 172.17.100.0 255.255.255.0 f0/0 cisco(config)#ip http server Cntr+Z	
Примечание: 1. Интерфейс Fast Ethernet 0/0 подключен к тому же коммутатору, что и межсетевой экран D-Link. ***2. Интерфейс Fast Ethernet 0/1 – внутренняя сеть для маршрутизатора Cisco.***	
Web-интерфейс SDM	
Конфигурирование параметров IKE и IPSec	
Зайдите в *VPN→VPN Components→Edit.* Введите следующие параметры во вкладке *IKE*:	
Enable IKE	Поставьте галочку
Identity (of this router)	ADDRESS (выберите из списка)
Enable Aggressive Mode	Уберите галочку
Enable Dead Peer Detection	Поставьте галочку
Keep-alive	15
Retry	20
DPD Type	On-Demand
Введите следующие параметры во вкладке *IPSec*:	
Authenticate and generate new key after every	1 час
Generate new key after the current key encrypts a volume of	4608000 килобайт
Нажмите *Ok*.	
Настройка туннеля	
Зайдите в *VPN→Site-to-Site VPN→Create Site to Site VPN.* Нажмите *Launch the selected task.*	
В окне мастера выберите *Step by step wizard*, нажмите *Next*.	
В следующем окне мастера выберите следующие параметры:	
Select the interface for this VPN connection	FastEthernet 0/0
Select the the IP address of the remote peer	195.168.110.254
Authentication	Pre-shared Keys
pre-shared key	123456qw
Re-enter Key	123456qw
Нажмите *Next.*	
В следующем окне мастера выберите *Add* для IKE Proposals, введите следующие параметры:	
Priority	2

Encryption	DES
Hash	SHA_1
Authentication	PRE_SHARE
D-H Group	group1
Lifetime	24 часа
Нажмите *Ok* и *Next.*	
В следующем окне мастера выберите *Add* для Transform Set, введите следующие параметры:	
Name	trs
Data integrity with encryption (ESP)	Поставьте галочку
Integrity Algorithm	ESP_MD5_HMAC
Encryption Algorithm	ESP_DES
Data and address integrity without encryption (AH)	Уберите галочку
Mode	Tunnel (Encrypt data and IP header)
Нажмите*Ok* и *Next.*	
В следующем окне мастера для *Traffic to protect* введите следующие параметры:	
Protect all traffic between the following subnets	Выберите из списка
Для *Local Network*:	
IP Address	192.168.2.0
Subnet Mask	255.255.255.0
Для *Remote Network*:	
IP Address	172.17.100.0
Subnet Mask	255.255.255.0
Нажмите*Next* и *Finish.*	
Проверка работоспособности туннеля на маршрутизаторе Cisco	
Для *Cisco Router and Security Device Manager* конфигурация сохраняется автоматически, после нажатия *Ok* или *Finish*. Правила, разрешающие трафик в туннеле, представляют собой ACL, маршрут к удаленной сети обязательно добавляется, маршрутизатор определяет с помощью *cryptomap* шифровать трафик к удаленной сети или нет на данном интерфейсе. Зайдите в *VPN→Site-to-Site VPN→TestTunnel.* Уточните работоспособность туннеля.	
Зайдите в *Routing→Static Routing.* Найдите созданный маршрут к удаленной сети.	
Зайдите в *Firewall and ACL→Edit Firewall Policy/ACL.* Найдите созданный ACL.	
Упражнение	Проверьте работоспособность туннеля.
Зайдите в *Status→IPSec→ipsec_tunnel.* Уточните статус SA.	
Запустите команду ping с хостов, подключенных к **lan-**интерфейсам межсетевого экрана D-Link и маршрутизатора Cisco. Зайдите в меню *Status→IPSec→ipsec_tunnel.* Уточните скорость трафика в туннеле.	
CMD Windows (устройство D-Link)	C:\>ping 192.168.2.1
CMD Windows (устройство Cisco)	C:\>ping 172.17.100.254
Устранение возможных проблем	Если туннель не был создан устройствами, решите возникшую проблему с помощью описанных ниже диагностических средств.
Проверьте корректность физических подключений устройств, работоспособность патч-кордов,	

индикацию на устройствах. Включите режим отладки:	
SSH CLI (Console CLI) УстройствоD-Link	gw-world:/>ikesnoop –on<IP-адресудаленногоVPN-шлюза>
Зайдите в меню *Status→IPSec→ipsec_tunnel*. Проверьте корректность настроек туннелей, уточните статус SA для фазы 1 и фазы 2.	
Зайдите в меню *Status→Logging* или просмотрите лог-сообщения на syslog-сервере, настроенном для работы с межсетевыми экранами.	
Выполните настройку туннелей с простейшими параметрами аутентификации – общим ключом, используйте стандартные (заданные по умолчанию) настройки для алгоритмов IKE и IPSec, режимов IKE, работы с NAT-T, и не используйте пользовательские настройки для XAuth, IKE Config Mode Pool, PFS, ID, Local ID Type. После того как туннель с этими упрощенными стандартными настройками будет установлен устройствами, измените его параметры в соответствии с особенностями задания в данном сценарии.	
IPSec-туннель LAN to LAN с заранее установленным ключом совместного использования (pre-shared key) между межсетевым экраном D-Link и межсетевым экраном Cisco PIX/ASA.	
Описание сценария	*Между офисом A и офисом B необходимо настроить IPSec-туннель для безопасного соединения по VPN, аутентификация – общий ключ. Устройство безопасности офиса A – межсетевой экран D-Link, устройство безопасности офиса B – межсетевой экран Cisco PIX/ASA.*
Схема 47	
Настройка DFL-860E	
Web-интерфейс	
Убедитесь в правильных настройках параметров интерфейсов:	
Name	lannet
Address	10.0.0.0/20
Name	lan_ip
Address	10.0.0.1
Name	wan1_ip
Address	195.168.110.254
Создание необходимых объектов	
Создадим объект «Pre-shared Key». Зайдите в меню *Objects→Authentication Objects→Add→Pre-Shared Key*. Введите следующие параметры:	
Name	pre-shared_key
Выберите *Shared Secret*. Введите следующие параметры:	
Shared Secret	123456qw

Confirm Secret	123456qw
Создадим объект «удаленную подсеть за VPN-шлюзом». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote_net
Address	10.100.100.0/24
Создадим объект «IP-адрес удаленного VPN-шлюза». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote_gw
Address	195.168.110.110
Создадим IPSec-туннель. Зайдите в меню *Interfaces→IPSec→Add→IPSec Tunnel.* Введите следующие параметры:	
Name	ipsec_tunnel
Local Network	lannet
Remote Network	remote_net
Remote Endpoint	remote_gw
Encapsulation mode	Tunnel
Выберите алгоритмы IKE и IPSec:	
IKE Algorithms	Standard (выберите из списка)
IKE Lifetime	28800 seconds
IPSec Algorithms	Standard (выберите из списка)
IPsec Lifetime	3600 seconds
IPsec Lifetime	4608000 kilobytes
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите pre-shared_key из списка.
Local ID	Auto (выберите из списка)
Во вкладке *IKE Settings* введите следующие параметры:	
IKE	Main, DHGroup1 (выберите из списка)
Perfect Forward Secrecy	None (выберите из списка)
Security Association	Per Net
NAT Traversal	On if supported and NATed
Use Dead Peer Detection	Поставьте галочку
На вкладке *Keep-alive*введите следующие параметры:	
Keep-alive	Выберите Auto из списка
На вкладке *Advanced*введите следующие параметры:	
Add route for remote network	Уберите галочку
Создание правил IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	outbound_rule
Action	Allow
Service	all-services
Source Interface	lan
Source Network	lannet
Destination Interface	ipsec_tunnel
Destination Network	remote_net

Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	inbound_rule
Action	Allow
Service	all-services
Source Interface	ipsec_tunnel
Source Network	remote_net
Destination Interface	lan
Destination Network	lannet
Создадим IP Rule, разрешающее выполнение команды ping в туннеле. Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	icmp_allow
Action	Allow
Service	all-icmp
Source Interface	ipsec_tunnel
Source Network	all-nets
Destination Interface	core
Destination Network	all-nets
Создание маршрута для туннеля	
Зайдите в меню *Routing→Routing Tables→Add→Routing Table*. Во вкладке *General* введите:	
Name	labs
Ordering	First (выберите из списка).
Нажмите правой кнопкой мыши по созданной таблице маршрутизации *labs*, выберите*Move to top*.	
Зайдите в *Routing→Routing Tables→labs→Add→Route*. Во вкладке *General* введите:	
Interface	ipsec_tunnel
Network	remote_net
Gateway	-
Local IP address	-
Metric	10
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.168.110.254 gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.168.110.0/24 gw-world:/> set IP4Address InterfaceAddresses/lan_ip Address=10.0.0.1 gw-world:/> set IP4Address InterfaceAddresses/lannet Address=10.0.0.0/20 gw-world:/>add PSK pre-shared_key Type=ASCII PSKAscii=123456qw gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address remote_net Address=10.100.100.0/24 gw-world:/labs> add IP4Address remote_gw Address=195.168.110.110 gw-world:/labs> cc gw-world:/>add Interface IPsecTunnel ipsec_tunnel AuthMethod=PSK IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet PSK=pre-shared_key RemoteNetwork=labs/remote_net RemoteEndpoint=labs/remote_gwKeepAlive=Auto AddRouteToRemoteNet=No IKELifeTimeSeconds=28800 IPsecLifeTimeKilobytes=4608000 IPsecLifeTimeSeconds=3600 SetupSAPer=Net DHGroup=1 NATTraversal=OnIfNeeded DeadPeerDetection=YesEncapsulationMode=Tunnel	

gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=ipsec_tunnel DestinationNetwork=labs/remote_net Name=outbound_rule
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=ipsec_tunnel SourceNetwork=labs/remote_net DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule
gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnel SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=all-nets Name=icmp_allow
gw-world:/1(labs)> cc
gw-world:/>add RoutingTable labs Ordering=First
gw-world:/>cc RoutingTable labs
gw-world:/labs>add Route Interface=ipsec_tunnel Network=labs/remote_net Metric=10
gw-world:/labs> cc
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Настройка Cisco PIX/ASA (на примере модели Cisco PIX-525, Cisco PIX Security Appliance Software Version 7.2(3))

Командная строка (CLI) – консоль

pixfirewall>enable
pixfirewall#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
pixfirewall(config)#interface e0
pixfirewall(config-if)#ip address 195.168.110.110 255.255.255.0
pixfirewall(config-if)#no shutdown
pixfirewall(config-if)#nameif outside
pixfirewall(config-if)#security-level 10
pixfirewall(config-if)#interface e1
pixfirewall(config-if)#ip address 10.100.100.0 255.255.255.0
pixfirewall(config-if)#no shutdown
pixfirewall(config-if)#nameif inside
pixfirewall(config-if)#security-level 100
pixfirewall(config-if)#exit
pixfirewall(config)#asdm image flash:/asdm.bin
pixfirewall(config)#http server enable
pixfirewall(config)#http 10.100.100.2 255.255.255.255 inside
Cntr+Z

Примечание: 1. Интерфейс Ethernet 0 Outside подключен к тому же коммутатору, что и межсетевой экран D-Link.
2. Интерфейс Ethernet 1 Inside – внутренняя сеть Cisco PIX.
3. Интерфейс Ethernet 0 Outside имеет уровень безопасности ниже, чем уровень безопасности Ethernet 1 Inside, таким образом он внешний для межсетевого экрана Cisco PIX.
4. Образ Cisco ASDM должен быть предварительно скопирован во флеш-память межсетевого экрана Cisco.

Web-интерфейс ASDM

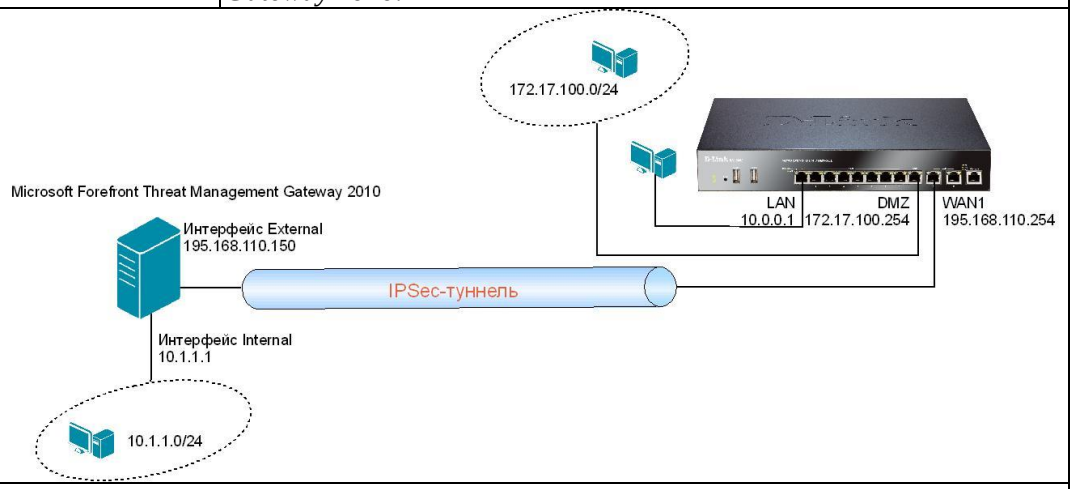
Настройка туннеля

Зайдите в *Configuration→VPN→VPN Wizard*. Нажмите *Launch VPN Wizard.*

В следующем окне мастера выберите следующие параметры:

VPN Tunnel Type	Site-to-Site
VPN Tunnel Interface	outside

Enable inbound IPSec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.	Поставьте галочку
Нажмите *Next.*	
В следующем окне мастера выберите следующие параметры:	
Peer IP Address	195.168.110.254
Pre-Shared key	123456qw
Нажмите *Next.*	
В следующем окне мастера выберите IKE Policy, введите следующие параметры:	
Encryption	DES
Authentication	SHA
DH Group	2
Нажмите *Next.*	
В следующем окне мастера выберите IPSec Encryprion and Authentication, введите следующие параметры:	
Encryption	DES
Authentication	SHA
Нажмите *Next.*	
В следующем окне мастера выберите Hostsand Networks, введите следующие параметры:	
Source IP Address	10.100.100.0
Netmask	255.255.255.0
Destination IP Address	10.0.0.0
Netmask	255.255.240.0
Нажмите *Next* и *Finish.*	
Зайдите в *Configuration→VPN→IPSec→IPSec Rules→static 1*. Нажмите *Edit*, измените следующие параметры:	
Enable Perfect Forwarding Secrecy	Уберите галочку
Нажмите *Ok* и *Apply*.	
Проверка работоспособности туннеля на Cisco PIX/ASA	
Для *Cisco Adaptive Security Device Manager* конфигурация сохраняется автоматически, после нажатия *Apply* и *Save*. Зайдите в *Monitoring→VPN→VPN Statistics.* Уточните работоспособность туннеля.	
Упражнение	Проверьте работоспособность туннеля.
Зайдите в *Status→IPSec→ipsec_tunnel.* Уточните статус SA.	
Запустите команду ping с хостов, подключенных к **lan-**интерфейсам межсетевого экрана D-Link и Cisco PIX/ASA. Зайдите в *Status→IPSec→ipsec_tunnel.* Уточните скорость трафика в туннеле.	
CMD Windows (устройство D-Link)	C:\>ping 10.100.100.1
CMD Windows (устройство Cisco)	C:\>ping 10.0.0.1
Устранение возможных проблем	Если туннель не был создан устройствами, решите возникшую проблему с помощью описанных ниже диагностических средств.
Проверьте корректность физических подключений устройств, работоспособность патч-кордов, индикацию на устройствах. Включите режим отладки:	

SSH CLI (Console CLI) Устройство D-Link	gw-world:/>ikesnoop –on<IP-адрес удаленного VPN-шлюза>
Зайдите в *Status→IPSec→ipsec_tunnel*. Проверьте корректность настроек туннелей, уточните статус SA для фазы 1 и фазы 2.	
Зайдите в *Status→Logging* или просмотрите лог-сообщения на syslog-сервере, настроенном для работы с межсетевыми экранами.	
Выполните настройку туннелей с простейшими параметрами аутентификации – общим ключом, используйте стандартные (заданные по умолчанию) настройки для алгоритмов IKE и IPSec, режимов IKE, работы с NAT-T, и не используйте пользовательские настройки для XAuth, IKE Config Mode Pool, PFS, ID, Local ID Type. После того, как туннель с этими упрощенными стандартными настройками будет установлен устройствами, измените его параметры в соответствии с особенностями задания в данном сценарии.	
IPSec-туннель LAN to LAN с заранее установленным ключом совместного использования (pre-shared key) между межсетевым экраном D-Link и Microsoft Forefront Threat Management Gateway 2010	
Описание сценария	*Между офисом A и офисом B необходимо настроить IPSec-туннель для безопасного соединения по VPN, аутентификация – общий ключ. Устройство безопасности офиса A – межсетевой экран D-Link, устройство безопасности офиса B – сервер на базе Microsoft Windows Server 2008 R2 с установленным на нем межсетевым экраном Microsoft Forefront Threat Management Gateway 2010.*
Схема 48	
Настройка DFL-860E	
Web-интерфейс	
Убедитесь в правильных настройках параметров интерфейсов:	
Name	dmznet
Address	172.17.100.0/24
Name	dmz_ip
Address	172.17.100.254
Name	wan1_ip
Address	195.168.110.254
Создание необходимых объектов	
Создадим объект «Pre-shared Key». Зайдите в меню *Objects→Authentication Objects→Add→Pre-Shared Key*. Введите следующие параметры:	

Name	pre-shared_key
Выберите *Shared Secret*. Введите следующие параметры:	
Shared Secret	123456qw
Confirm Secret	123456qw
Создадим объект «удаленную подсеть за VPN-шлюзом». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	remote_net
Address	10.1.1.0/24
Создадим объект «IP-адрес удаленного VPN-шлюза». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	remote_gw
Address	195.168.110.150
Создадим IPSec-туннель. Зайдите в меню *Interfaces→IPSec→Add→IPSec Tunnel*. Введите следующие параметры:	
Name	ipsec_tunnel
Local Network	dmz_ip
Remote Network	remote_net
Remote Endpoint	remote_gw
Encapsulation mode	Tunnel
Выберите алгоритмы IKE и IPSec:	
IKE Algorithms	Standard (выберите из списка)
IKE Lifetime	28800 seconds
IPSec Algorithms	Standard (выберите из списка)
IPsec Lifetime	3600 seconds
IPsec Lifetime	20480 kilobytes
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите pre-shared_key из списка.
Local ID	Auto (выберите из списка)
Во вкладке *IKE Settings* введите следующие параметры:	
IKE	Main, DHGroup2 (выберите из списка)
Perfect Forward Secrecy	None (выберите из списка)
Security Association	Per Net
NAT Traversal	On if supported and NATed
Use Dead Peer Detection	Поставьте галочку
Во вкладке *Keep-alive* введите следующие параметры:	
Keep-alive	Выберите Auto из списка
Во вкладке *Routing* введите следующие параметры:	
Dynamically add route to the remote network when a tunnel is established	Поставьте галочку
Во вкладке *Advanced* введите следующие параметры:	
Add route for remote network	Уберите галочку
Создание правил IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	

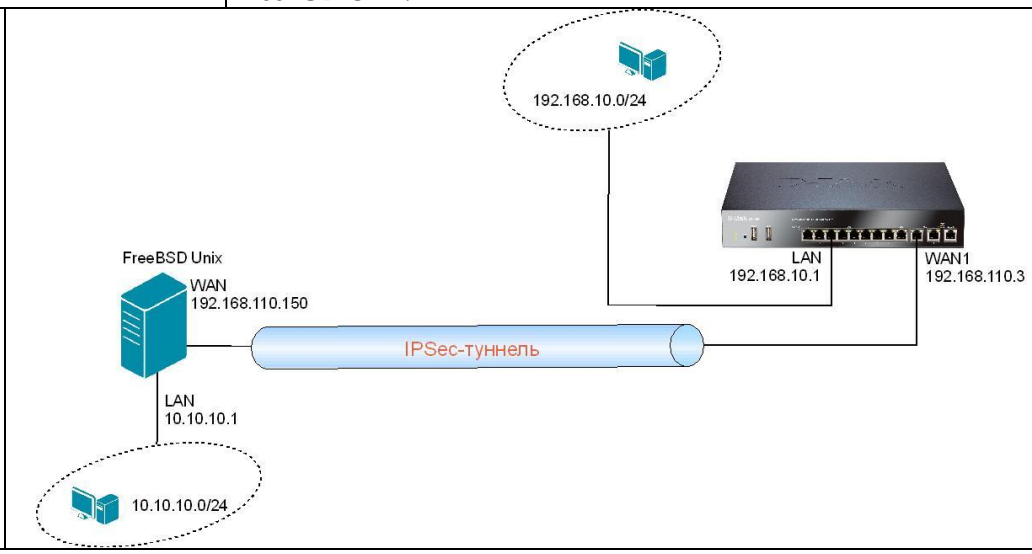
Name	outbound_rule
Action	Allow
Service	all-services
Source Interface	dmz
Source Network	dmz_ip
Destination Interface	ipsec_tunnel
Destination Network	remote_net
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	inbound_rule
Action	Allow
Service	all-services
Source Interface	ipsec_tunnel
Source Network	remote_net
Destination Interface	dmz
Destination Network	dmz_ip
Создадим IP Rule, разрешающее выполнение команды ping в туннеле. Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	icmp_allow
Action	Allow
Service	all-icmp
Source Interface	ipsec_tunnel
Source Network	all-nets
Destination Interface	core
Destination Network	all-nets
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.168.110.254 gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.168.110.0/24 gw-world:/> set IP4Address InterfaceAddresses/dmz_ip Address=172.17.100.254 gw-world:/> set IP4Address InterfaceAddresses/dmznet Address=172.17.100.0/24 gw-world:/>add PSK pre-shared_key Type=ASCII PSKAscii=123456qw gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address remote_net Address=10.1.1.0/24 gw-world:/labs> add IP4Address remote_gw Address=195.168.110.150 gw-world:/labs> cc gw-world:/>add Interface IPsecTunnel ipsec_tunnel AuthMethod=PSK IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/dmz_ip PSK=pre-shared_key RemoteNetwork=labs/remote_net RemoteEndpoint=labs/remote_gwKeepAlive=Auto AddRouteToRemoteNet=No IKELifeTimeSeconds=28800 IPsecLifeTimeKilobytes=20480 IPsecLifeTimeSeconds=3600 PFS=NoneSetupSAPer=Net DHGroup=2 NATTraversal=OnIfNeeded DeadPeerDetection=YesEncapsulationMode=Tunnel gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=dmz SourceNetwork=InterfaceAddresses/dmznet DestinationInterface=ipsec_tunnel DestinationNetwork=labs/remote_net Name=outbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=ipsec_tunnel	

SourceNetwork=labs/remote_net DestinationInterface=dmz DestinationNetwork=InterfaceAddresses/dmznet Name=inbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnel SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=all-nets Name=icmp_allow gw-world:/1(labs)> cc gw-world:/>add RoutingTable labs Ordering=First gw-world:/>cc RoutingTable labs gw-world:/labs>add Route Interface=ipsec_tunnel Network=labs/remote_net Metric=10 gw-world:/labs> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Настройка Microsoft Forefront Threat Management Gateway 2010	
Web-интерфейс	
Создание туннеля	
Откройте консоль Forefront TMG. Зайдите в *Forefront TMG (srv2008R2)→Remote Access Policy (VPN)→Remote Sites→Tasks→Create VPN Site-to-Site Connection.* Введите следующие параметры во вкладке *IKE*:	
Site-to-site network name	dlink
Нажмите *Next.*	
В следующем окне мастера введите следующие параметры:	
VPN Protocol	IP Security protocol (IPSec) tunnel mode (выберите из списка)
Нажмите *Next.*	
В следующем окне мастера введите следующие параметры:	
Remote VPN gateway IP address	195.168.110.254
Local VPN gateway IP address	195.168.110.150
Нажмите *Next.*	
В следующем окне мастера введите следующие параметры:	
Use pre-shared key for authentication	123456qw
Нажмите *Next.*	
В следующем окне мастера нажмите *Add Range*, введите следующие параметры:	
Start address	172.17.100.254
End address	172.17.100.254
Нажмите *Ok* и *Next.*	
В следующем окне мастера введите следующие параметры:	
Create a network rule specifying a route relationship	Выберите из списка
Network rule name	dlink to Internal Network
Route traffic between the new network and these destination	Internal
Нажмите *Next.*	
В следующем окне мастера нажмите *Add Range*, введите следующие параметры:	
Create an allow access rule. This rule will allow traffic between the Internal network and the new site-to-site network	Выберите из списка

for all users.	
Access rule name	Allow access between dlink and Internal (название по умолчанию)
Apply the rule to these protocols	All outbound traffic
Нажмите *Next* и *Finish.*	
Конфигурирование параметров IKE и IPSec	
Зайдите в *Forefront TMG (srv2008R2)→Remote Access Policy (VPN)→Remote Sites→dlink→Properties.* Введите следующие параметры во вкладке *Connection,* нажав кнопку *IPsec Settings*:	
Во вкладке *Phase I*:	
Encryption algorithm	DES
Integrity algorithm	MD5
Diffe-Hellman group	Group 2 (1024 bit)
Authenticate and generate a new key every	28800 seconds
Во вкладке *Phase II*:	
Encryption algorithm	DES
Integrity algorithm	SHA1
Generate a new key every	20480 Kbytes
Generate a new key every	3600 seconds
Use Perfect Forward Secrecy (PFS)	Уберите галочку
Нажмите *Apply* и сохраните сделанные изменения.	
Примечание: 1. Интерфейс External должен быть подключен к тому же коммутатору, что и межсетевой экран D-Link и иметь IP-адрес 195.168.110.150. ***2. Интерфейс Internal– внутренняя сеть 10.1.1.0/24.***	
Проверка работоспособности туннеля на MS Forefront TMG 2010	
Зайдите в *Forefront TMG (srv2008R2)→Remote Access Policy (VPN)→Remote Sites→dlink→Monitor Site Sessions.* Уточните работоспособность туннеля.	
<u>Упражнение</u>	Проверьте работоспособность туннеля.
Зайдите в *Status→IPSec→ipsec_tunnel.* Уточните статус SA.	
Запустите команду ping (с ключом -t) с хостов, подключенных к интерфейсу Internal межсетевого экрана MS Forefront TMG 2010. Зайдите в *Status→IPSec→ipsec_tunnel.* Уточните скорость трафика в туннеле.	
CMD Windows (MS Forefront TMG 2010)	C:\>ping 172.17.100.254 -t
<u>Устранение возможных проблем</u>	Если туннель не был создан, решите возникшую проблему с помощью описанных ниже диагностических средств.
Проверьте корректность физических подключений устройств, работоспособность патч-кордов, индикацию на устройствах. Включите режим отладки:	
SSH CLI (Console CLI) Устройство D-Link	gw-world:/>ikesnoop –on<IP-адрес удаленного VPN-шлюза>
Зайдите в *Status→IPSec→ipsec_tunnel.* Проверьте корректность настроек туннелей, уточните статус SA для фазы 1 и фазы 2.	
Зайдите в *Status→Logging* или просмотрите лог-сообщения на syslog-сервере, настроенном для работы с межсетевыми экранами.	
Выполните настройку туннелей с простейшими параметрами аутентификации – общим ключом,	

используйте стандартные (заданные по умолчанию) настройки для алгоритмов IKE и IPSec, режимов IKE, работы с NAT-T, и не используйте пользовательские настройки для XAuth, IKE Config Mode Pool, PFS, ID, Local ID Type. После того как туннель с этими упрощенными стандартными настройками будет установлен устройствами, измените его параметры в соответствии с особенностями задания в данном сценарии.

IPSec-туннель LAN to LAN с заранее установленным ключом совместного использования (pre-sharedkey) между межсетевым экраном D-Link и FreeBSD Unix

Описание сценария	*Между офисом A и офисом B необходимо настроить IPSec-туннель для безопасного соединения по VPN, аутентификация – общий ключ. Устройство безопасности офиса A – межсетевой экран D-Link, устройство безопасности офиса B – компьютер с FreeBSD Unix.*
Схема 49	

Настройка DFL-860E

Web-интерфейс

Убедитесь в правильных настройках параметров интерфейсов:

Name	lannet
IPAddress	192.168.10.0/24
Name	lan_ip
IPAddress	192.168.10.1
Name	wan1_ip
IPAddress	192.168.110.3

Создание необходимых объектов

Создадим объект «Pre-shared Key». Зайдите в меню *Objects→Authentication Objects→Add→Pre-Shared Key*. Введите следующие параметры:

Name	pre-shared_key

Выберите *Shared Secret*. Введите следующие параметры:

Shared Secret	123456qw
Confirm Secret	123456qw

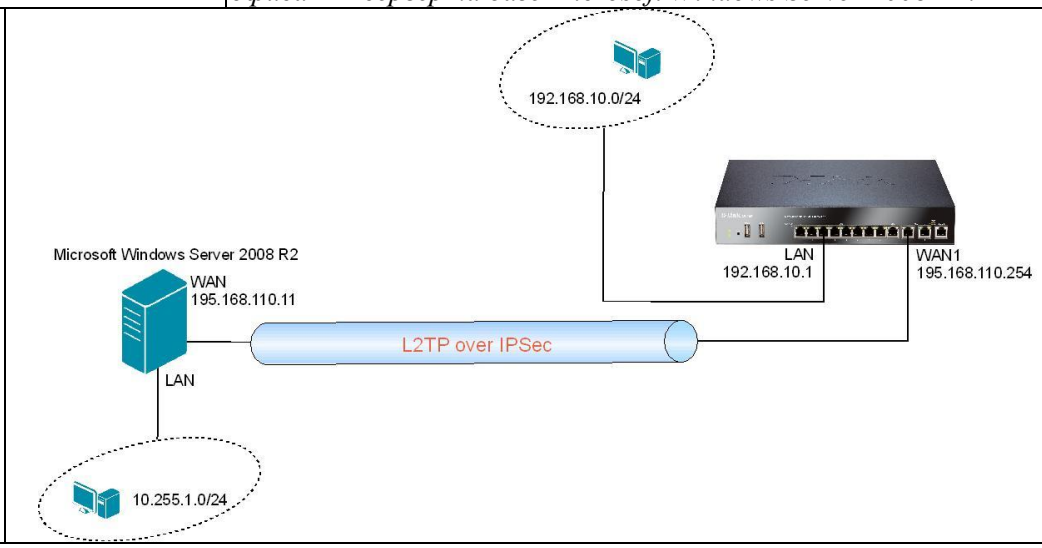
Создадим объект «удаленную подсеть за VPN-шлюзом». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:

Name	remote_net

Address	10.10.10.0/24
Создадим объект «IP-адрес удаленного VPN-шлюза». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote_gw
Address	192.168.110.150
Создадим IPSec-туннель. Зайдите в меню *Interfaces→IPSec→Add→IPSec Tunnel.* Введите следующие параметры:	
Name	ipsec_tunnel
Local Network	lannet
Remote Network	remote_net
Remote Endpoint	remote_gw
Encapsulation mode	Tunnel
Выберите алгоритмы IKE иI PSec:	
IKE Algorithms	Standard (выберите из списка)
IKE Lifetime	28800 seconds
IPSec Algorithms	Standard (выберите из списка)
IPsec Lifetime	3600 seconds
IPsec Lifetime	0 kilobytes
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите pre-shared_key из списка.
Local ID	Auto (выберите из списка)
Во вкладке *IKE Settings* введите следующие параметры:	
IKE	Main, DHGroup2 (выберите из списка)
Perfect Forward Secrecy	PFS, DHGroup 2 (выберите из списка)
Security Association	Per Net
NAT Traversal	On if supported and NATed
Use Dead Peer Detection	Поставьте галочку
Во вкладке *Keep-alive* введите следующие параметры:	
Keep-alive	Выберите Auto из списка.
Во вкладке *Routing* введите следующие параметры:	
Dynamically add route to the remote network when a tunnel is established	Поставьте галочку
Во вкладке *Advanced* введите следующие параметры:	
Add route for remote network	Уберите галочку
Создание правил IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	outbound_rule
Action	Allow
Service	all-services
Source Interface	lan
Source Network	lannet
Destination Interface	ipsec_tunnel
Destination Network	remote_net

Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	inbound_rule
Action	Allow
Service	all-services
Source Interface	ipsec_tunnel
Source Network	remote_net
Destination Interface	lan
Destination Network	lannet
Создадим IP Rule, разрешающее выполнение команды в туннеле. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	icmp_allow
Action	Allow
Service	all-icmp
Source Interface	ipsec_tunnel
Source Network	all-nets
Destination Interface	core
Destination Network	all-nets
Зайдите в *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=192.168.110.3 gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=192.168.110.0/24 gw-world:/> set IP4Address InterfaceAddresses/dmz_ip Address=192.168.10.1 gw-world:/> set IP4Address InterfaceAddresses/dmznet Address=192.168.10.0/24 gw-world:/>add PSK pre-shared_key Type=ASCII PSKAscii=123456qw gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address remote_net Address=10.10.10.0/24 gw-world:/labs> add IP4Address remote_gw Address=192.168.110.150 gw-world:/labs> cc gw-world:/>add Interface IPsecTunnel ipsec_tunnel AuthMethod=PSK IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet PSK=pre-shared_key RemoteNetwork=labs/remote_net RemoteEndpoint=labs/remote_gwKeepAlive=Auto AddRouteToRemoteNet=No IKELifeTimeSeconds=28800 IPsecLifeTimeSeconds=3600 PFS=PFS PFSDHGroup=2 SetupSAPer=Net DHGroup=2 NATTraversal=OnIfNeeded DeadPeerDetection=YesEncapsulationMode=Tunnel gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=ipsec_tunnel DestinationNetwork=labs/remote_net Name=outbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=ipsec_tunnel SourceNetwork=labs/remote_net DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=ipsec_tunnel SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=all-nets Name=icmp_allow gw-world:/1(labs)> cc gw-world:/>add RoutingTable labs Ordering=First gw-world:/>cc RoutingTable labs gw-world:/labs>add Route Interface=ipsec_tunnel Network=labs/remote_net Metric=10 gw-world:/labs> cc	

gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Настройка Sense FreeBSD Unix	
Web-интерфейс	
Параметры фазы 1	
Откройте инструмент Sense, введите следующие параметры в окне настроек Edit Phase 1:	
Name	dlink
Disabled	Уберите галочку
Interface	WAN (подключен к сети wan1net межсетевого экрана D-Link)
Remote gateway	192.168.110.3
Description	ipsec_dlink
Authentication method	Mutual PSK
Negotiation mode	main
My identifier	Выберите IP address, введите 192.168.110.150
Peer identifier	Peer IP address
Pre-Shared Key	123456qw
Policy Generation	Default
Proposal Checking	Default
Encryption algorithm	DES
Hash alhorithm	SHA1
DH key group	2
Lifetime	3600
NAT Traversal	Enable
Dead Peer Detection	Поставьте галочку
Параметры фазы 2	
Откройте инструмент Sense, введите следующие параметры в окне настроек Edit Phase 2:	
Disabled	Уберите галочку
Mode	Tunnel
Local Network	LAN subnet (10.10.10.0/24)
Remote Network	192.168.10.0/24
Description	office_dlink
Protocol	ESP
Encryption algorithm	DES
Hash algorithm	Выберите SHA1, MD5
PFS key group	2
Lifetime	3600
Нажмите *Save.*	
Примечание: 1. Интерфейс WAN компьютера Unix должен быть подключен к тому же коммутатору, что и межсетевой экран D-Link и иметь IP-адрес 192.168.110.150/24. 2. Интерфейс LAN компьютера Unix – внутренняя сеть 10.10.10.0/24.	
Упражнение	Проверьте работоспособность туннеля.
Зайдите в *Status→IPSec→ipsec_tunnel.* Уточните статус SA.	

Запустите команду ping (с ключом -t) с хостов, подключенных к LAN-интерфейсу FreeBSD Unix. На межсетевом экране D-Link зайдите в меню *Status→IPSec→ipsec_tunnel.* Уточните скорость трафика в туннеле.	
CMD Windows (FreeBSD Unix)	C:\>ping 192.168.10.1 -t
Устранение возможных проблем	Если туннель не был создан, решите возникшую проблему с помощью описанных ниже диагностических средств.
Проверьте корректность физических подключений устройств, работоспособность патч-кордов, индикацию на устройствах. Включите режим отладки:	
SSH CLI (Console CLI) Устройство D-Link	gw-world:/>ikesnoop –on<IP-адрес удаленного VPN-шлюза>
Зайдите в меню *Status→IPSec→ipsec_tunnel.* Проверьте корректность настроек туннелей, уточните статус SA для фазы 1 и фазы 2.	
Зайдите в *Status→Logging* или просмотрите лог-сообщения на syslog-сервере, настроенном для работы с межсетевыми экранами.	
Выполните настройку туннелей с простейшими параметрами аутентификации – общим ключом, используйте стандартные (заданные по умолчанию) настройки для алгоритмов IKE и IPSec, режимов IKE, работы с NAT-T, и не используйте пользовательские настройки для XAuth, IKE Config Mode Pool, PFS, ID, Local ID Type. После того как туннель с этими упрощенными стандартными настройками будет установлен устройствами, измените его параметры в соответствии с особенностями задания в данном сценарии.	
L2TP over IPSec туннель LAN to LAN с заранее установленным ключом совместного использования (pre-shared key) между межсетевым экраном D-Link и удаленным офисом с использованием службы маршрутизации и удаленного доступа Microsoft Windows Server 2008 R2	
Описание сценария	*Между офисом A и офисом B необходимо настроить L2TP over IPSec туннель для безопасного соединения по VPN, аутентификация – общий секрет. Устройство безопасности офиса A – межсетевой экран D-Link, устройство безопасности офиса B – сервер на базе Microsoft Windows Server 2008 R2.*
Схема 50	
Настройка DFL-860E	
Web-интерфейс	
Убедитесь в правильных настройках параметров интерфейсов:	
Name	lannet

Address	192.168.10.0/24
Name	lan_ip
Address	192.168.10.1
Name	wan1_ip
Address	195.168.110.254
Создание необходимых объектов	
Создадим объект Pre-shared Key. Зайдите в меню *Objects→Authentication Objects→Add→Pre-Shared Key*. Введите следующие параметры:	
Name	pre-shared_key
Выберите *Shared Secret*. Введите следующие параметры:	
Shared Secret	123456qw
Confirm Secret	123456qw
Создадим объект «диапазон IP-адресов, которые могут быть использованы удаленными клиентами». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	l2tp_pool
Address	10.1.1.10-10.1.1.50
Создадим объект «внутренний IP-адрес, через который могут подключаться клиенты». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	l2tp_ip
Address	10.1.1.1
Создадим локальную базу пользователей. Перейдите в меню *User Authentication→Local User Databases→Add→Local User Database*. Во вкладке *General* введите:	
Name	RemoteOffice
Перейдите в меню *User Authentication→Local User Databases→RemoteOffice→Add→User*. Во вкладке *General* введите:	
Username	office1
Password	P@ssw0rd
Confirm Password	P@ssw0rd
Создадим IPSec-туннель. Зайдите в меню *Interfaces→IPSec→Add→IPSec Tunnel*. Введите следующие параметры:	
Name	ipsec_tunnel
Local Network	wan1_ip
Remote Network	all-nets
Remote Endpoint	none
Encapsulation mode	Transport
Выберите алгоритмы IKE и IPSec:	
IKE Algorithms	Standard (выберите из списка)
IPSec Algorithms	Standard (выберите из списка)
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите pre-shared_key из списка
Во вкладке *Routing* введите следующие параметры:	
Dynamically add route to the remote network when a tunnel is established	Поставьте галочку
Во вкладке *Advanced* введите следующие параметры:	

Add route for remote network	Уберите галочку
Добавьте PPTP/L2TP. Зайдите в меню *Interfaces→PPTP/L2TP Servers→Add→PPTP/L2TP Server*. Введите следующие параметры во вкладке *General*:	
Name	l2tp_srv
Inner IP Address	l2tp_ip
Tunnel Protocol	L2TP
Outer Interface Filter	ipsec_tunnel
Server IP	wan1_ip
Во вкладке *PPP Parameters* введите:	
Use User Authentication Rules	Поставьте галочку
Microsoft Point-to-Point Encryption	Разрешите – поставьте галочки
IP Pool	l2tp_pool
Во вкладке *Add Route* введите:	
Proxy ARP	Разрешите на интерфейсе, к которому подключена внутренняя сеть.
Allowed Networks	all-nets
Создайте правило аутентификации пользователя. Перейдите в *User Authentication→User Authentication Rules→Add→ User Authentication Rule*. Во вкладке *General* введите:	
Name	auth_rule
Agent	PPP
Authentication Source	Local
Interface	l2tp_srv
Originator IP	all-nets
Terminator IP	wan1_ip
Во вкладке *Authentication Options* введите:	
Local User DB	Выберите из списка RemoteOffice
Во вкладке *Agent Options* введите:	
Use MS-CHAP v2 authentication protocol	Поставьте галочку
Создание правил IP Rule для туннеля	
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	inbound_rule
Action	Allow
Service	all-services
Source Interface	l2tp_srv
Source Network	l2tp_pool
Destination Interface	lan
Destination Network	lannet
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	outbound_rule
Action	Allow
Service	all-services
Source Interface	lan
Source Network	lannet

Destination Interface	l2tp_srv
Destination Network	l2tp_pool
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	icmp_rule
Action	Allow
Service	all-icmp
Source Interface	l2tp_srv
Source Network	l2tp_pool
Destination Interface	core
Destination Network	lan_ip
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.168.110.254 gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.168.110.0/24 gw-world:/> add Address AddressFolder labs gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address l2tp_pool Address=10.1.1.10-10.1.1.50 gw-world:/labs> add IP4Address l2tp_ip Address=10.1.1.1 gw-world:/labs>cc gw-world:/> add PSK pre-shared_key Type=ASCII PSKAscii=123456qw gw-world:/> add LocalUserDatabase RemoteOffice gw-world:/> cc LocalUserDatabase RemoteOffice gw-world:/RemoteOffice> add User office1 Password=P@ssw0rd gw-world:/RemoteOffice> cc gw-world:/> add Interface IPsecTunnel ipsec_tunnel AuthMethod=PSK IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/wan1_ipPSK=pre-shared_key RemoteNetwork=all-nets AddRouteToRemoteNet=Yes EncapsulationMode=Transport gw-world:/> add Interface L2TPServer l2tp_srv Interface=ipsec_tunnel IPPool=labs/l2tp_pool IP=labs/l2tp_ip ServerIP=InterfaceAddresses/wan1_ip TunnelProtocol=L2TP ProxyARPInterfaces=lanUseUserAuth=Yes gw-world:/> add UserAuthRule Interface=l2tp_srv AuthSource=Local LocalUserDB=RemoteOffice OriginatorIP=all-nets Agent=PPP TerminatorIP=InterfaceAddresses/wan1_ip Name=auth_rule gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=l2tp_srv SourceNetwork=labs/l2tp_pool DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Name=inbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=l2tp_srv DestinationNetwork=labs/l2tp_pool Name=outbound_rule gw-world:/1(labs)> add IPRule Action=Allow Service=all_icmp SourceInterface=l2tp_srv SourceNetwork=labs/l2tp_pool DestinationInterface=core DestinationNetwork=InterfaceAddresses/lan_ipName=icmp_rule gw-world:/1(labs)> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Настройка IPSec IKE в Microsoft Windows Server 2008 R2	
Сетевые настройки сервера должны соответствовать подсети 195.168.110.0/24. IP-адрес компьютера – 195.168.110.11.	
Зайдите в Пуск→Выполнить→mmc	

В консоли MMC добавьте оснастку Политики IP-безопасности для локального компьютера.	
Примечание: Для домена Microsoft Windows можно добавить оснастку для групповой политики и далее ее применить на граничном шлюзе в данном сегменте сети.	
В оснастке Политики IP-безопасности задайте новую политику IP-безопасности со следующими параметрами:	
Имя	L2tp_ipsec_policy
Зайдите в свойства созданной политики. Во вкладке *Общие→Параметры* введите:	
Основной ключ безопасной пересылки (PFS)	Уберите галочку
Проверять подлинность и создавать новый ключ каждые	480 мин
Проверять подлинность и создавать новый ключ через каждые	0 сеансов
Зайдите в *Общие→Параметры→Методы→Добавить*, введите следующие параметры:	
Алгоритм проверки целостности	SHA1
Алгоритм шифрования	DES
Группа Диффи-Хельмана	средняя (2)
Зайдите в *Свойства→Управление списками IP-фильтра и действиями фильтра→Управление списками IP-фильтров→Добавить*, введите следующие параметры (нажимайте *Далее* после заполнения необходимых параметров в каждом окне):	
Имя	Inbound
Зайдите в *Список IP-фильтров→Добавить*, введите следующие параметры:	
Описание IP-фильтра и свойство «Отраженный»	Уберите галочку *Отраженный*
Источник IP-трафика	Выберите из списка *Определенный IP-адрес или подсеть*, введите 195.168.110.254
Назначение IP-трафика	Выберите из списка *Определенный IP-адрес или подсеть*, введите 195.168.110.11
Тип протокола IP	Выберите из списка *Любой (*можно указать конкретные протоколы в соответствии со схемой сетевой безопасности в организации).
Зайдите в *Свойства→Управление списками IP-фильтра и действиями фильтра→Управление списками IP-фильтров→Добавить*,введите следующие параметры (нажимайте *Далее* после заполнения необходимых параметров в каждом окне):	
Имя	Outbound
Зайдите в *Список IP-фильтров→Добавить*, введите следующие параметры:	
Описание IP-фильтра и свойство «Отраженный»	Уберите галочку *Отраженный*
Источник IP-трафика	Выберите из списка *Определенный IP-адрес или подсеть*, введите 195.168.110.11
Назначение IP-трафика	Выберите из списка *Определенный IP-адрес или подсеть*, введите 195.168.110.254
Тип протокола IP	Выберите из списка *Любой (*можно указать конкретные протоколы в соответствии со схемой сетевой безопасности в организации).
Зайдите в *Свойства→Управление списками IP-фильтра и действиями фильтра→Управление действиями фильтра→Добавить*, введите следующие параметры (нажимайте *Далее* после заполнения необходимых параметров в каждом окне):	

Имя	IKE1
Общие параметры действия фильтра	Согласовать безопасность
Соединение с компьютерами, не поддерживающими IPsec	Запретить небезопасное соединение.
Безопасность IP-трафика	Другой
Нажмите кнопку *Параметры*, введите следующие параметры:	
Целостность данных и адресов без шифрования (AH)	Уберите галочку
Целостность данных с шифрованием (ESP)	Поставьте галочку
Алгоритм проверки целостности	SHA1
Алгоритм шифрования	DES
Смена ключа каждые	Поставьте галочку, введите – 3600 сек.
Зайдите в *Свойства→Управление списками IP-фильтра и действиями фильтра→Управление действиями фильтра→IKE1→Изменить*, введите следующие параметры:	
Принимать небезопасную связь, но отвечать с помощью IPsec	Поставьте галочку
Зайдите в *Правила→Добавить*, введите следующие параметры (нажимайте *Далее* после заполнения необходимых параметров в каждом окне):	
Конечная точка туннеля	Это правило не определяет туннель
Тип сети	Все сетевые подключения
Список IP-фильтров	Inbound
Действие фильтра	IKE1
Метод проверки подлинности	Использовать данную строку для защиты обмена ключами – введите 123456qw
Зайдите в *Правила→Добавить*, введите следующие параметры (нажимайте *Далее* после заполнения необходимых параметров в каждом окне):	
Конечная точка туннеля	Это правило не определяет туннель
Тип сети	Все сетевые подключения
Список IP-фильтров	Outbound
Действие фильтра	IKE1
Метод проверки подлинности	Использовать данную строку для защиты обмена ключами – введите 123456qw
Нажмите правой кнопкой мыши по созданной политике IP-безопасности, выберите *Назначить*.	
Настройка службы маршрутизации и удаленного доступа (RRAS) в Microsoft Windows Server 2008 R2	
Откройте консоль Маршрутизация и удаленный доступ, убедитесь, что служба запущена. Откройте *Свойства*, нажав правой кнопкой мыши по имени сервера, введите следующие параметры на вкладке *Общие*:	
Использовать этот компьютер как IP4-маршрутизатор	Локальной сети и вызова по требованию
IP4-сервер удаленного доступа	Поставьте галочку
Введите следующие параметры во вкладке *Безопасность*:	

Разрешить особые IPsec-политики для L2TP-подключения	Поставьте галочку, введите предварительный ключ – 123456qw
Откройте *Свойства*, нажав правой кнопкой мыши по опции *Порты*, выделите мышью WANMiniport (L2TP) нажмите *Настроить*, введите следующие параметры:	
Подключения удаленного доступа (только входящие)	Уберите галочку
Подключения по требованию (входящие и исходящие)	Поставьте галочку
Нажмите правой кнопкой мыши по опции *Интерфейсы сети*, выберите *Создать новый интерфейс вызова по требованию*. Введите следующие параметры (нажимайте Далее после заполнения необходимых параметров в каждом окне):	
Имя интерфейса	dlink
Тип подключения	Подключаться с использованием виртуальной частной сети (VPN)
Тип сети VPN	Туннельный протокол второго уровня (L2TP)
Адрес назначения	195.168.110.254
Протоколы и безопасность	Перенаправлять пакеты IP на этот интерфейс
Статические маршруты для удаленных сетей	Нажмите *Добавить*. Введите следующие параметры:
Поддержка удаленной сети с помощью IPv4	Выберите из списка
Назначение	192.168.10.0
Маска подсети	255.255.255.0
Метрика	1
Нажмите *Ок* и *Далее*. В следующем окне введите следующие параметры:	
Учетные данные исходящих вызовов	Имя пользователя – user, пароль – P@ssw0rd.
Зайдите в Интерфейсы сети, нажмите правой кнопкой мыши на dlink и выберите *Подключить*. При необходимости перезапустите службу RRAS.	
Упражнение	Проверьте работоспособность L2TP over IPSec туннеля.
Проверка работоспособности туннеляна MS Windows Server 2008 R2	
Зайдите в консоли RRAS в IPv4→Статические маршруты, убедитесь в наличии маршрута к удаленной сети за межсетевым экраном D-Link через созданный интерфейс dlink. Откройте консоль Монитор IP-безопасности, уточните статус примененной политики IPSec, статистику для *Быстрого режима* и наличие *Сопоставлений безопасности* (SA).	
Запустите команду ping с хостов, подключенных к другим интерфейсам маршрутизатора MS Windows Server. Проверьте состояние выполнения команды ping при отключении интерфейса вызова по требованию в RRAS, при откате IPSec политике на MS Windows Server 2008 R2.	
CMD Windows (устройство D-Link)	C:\>ping 192.168.10.1 -t
Проверка работоспособности туннеля на межстевом экране D-Link	
Зайдите в меню *Status→IPSec→ipsec_tunnel.* Уточните статус соединения SA.	
Запустите команду ping (с ключом -t) с хостов, подключенных к **lan-**интерфейсу межсетевого экрана D-Link и маршрутизатора MS Windows Server 2003/2008. Зайдите в меню *Status→IPSec→ipsec_tunnel.* Уточните скорость трафика в туннеле.	
Зайдите в меню *Status→User Authentication*, уточните выданный IP-адрес для маршрутизатора удаленного офиса на интерфейсе L2TP Server. Отключите туннель на MS Windows, уточните состояние запущенной команды ping на lan_ip межсетевого экрана.	
CMD Windows (устройство	C:\>ping10.255.1.1 –t (сеть за маршрутизатором MS Windows)

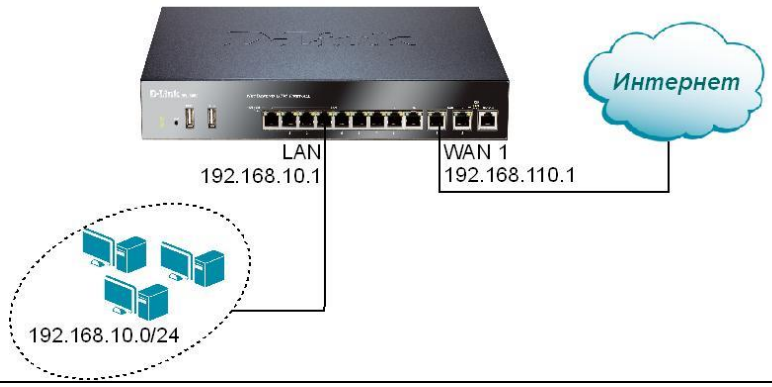
D-Link)	
<u>Устранение возможных проблем</u>	Если туннель не был создан, решите возникшую проблему с помощью описанных ниже диагностических средств.
Проверьте корректность физических подключений устройств, работоспособность патч-кордов, индикацию на устройствах. Включите режим отладки:	
SSH CLI (Console CLI) Устройство D-Link	gw-world:/>ikesnoop –on<IP-адрес удаленногоVPN-шлюза>
Зайдите в меню*Status→IPSec→ipsec_tunnel*. Проверьте корректность настроек туннелей, уточните статус SA для фазы 1 и фазы 2.	
Зайдите в меню *Status→Logging* или просмотрите лог-сообщения на syslog-сервере, настроенном для работы с межсетевыми экранами.	
Выполните настройку туннелей с простейшими параметрами аутентификации – общим ключом, используйте стандартные (заданные по умолчанию) настройки для алгоритмов IKE и IPSec, режимов IKE, работы с NAT-T, и не используйте пользовательские настройки для XAuth, IKE Config Mode Pool, PFS, ID, Local ID Type. После того, как туннель с этими упрощенными стандартными настройками будет установлен устройствами, измените его параметры в соответствии с особенностями задания в данном сценарии.	

ЗАНЯТИЕ №10. Балансировка нагрузки, управление трафиком для обеспечения гарантированного качества обслуживания. Server Load Balancing. Создание Threshold Rule. IDP Traffic Shaping.

Межсетевые экраны D-Link позволяют ограничивать полосу пропускания трафика как для передачи, так для приема данных. Данная функция используется в сетях Интернет-провайдеров (ISP), а также в инфраструктуре предприятий для выравнивания асимметричного трафика. Исходящий (восходящий) трафик называется Upstream (Tx), входящий (нисходящий) – Downstream (Rx). Также есть функции настройки гарантированного качества обслуживания (гарантированной полосы пропускания). Кроме того, управление трафиком возможно с помощью механизмов Server Load Balancing и IDP Traffic Shaping.

Цель	Эта лабораторная работа предназначена для более глубокого понимания назначения и использования настройки полосы пропускания	
Оборудование	DFL-860E	1
	Рабочая станция	1
	Ethernet-кабель (патч-корд)	3

Управление трафиком для обеспечения гарантированного качества обслуживания	*Этот сценарий позволяет гарантировать полосу пропускания для таких приложений, как E-mail, Web-приложения и передача файлов.*
Описание сценария	*1. Фиксированная скорость восходящего/нисходящего потока для Интернет-соединения 2000 Кбит\с / 2000 Кбит\с.* *2. Протокол SMTP двунаправленный: гарантированная полоса пропускания 800 Кбит\с, максимальная полоса пропускания 1600 Кбит\с.* *3. Протокол HTTP/HTTPS двунаправленный: гарантированная полоса пропускания 600 Кбит\с, максимальная полоса пропускания 1200 Кбит\с.* *4. Протокол FTP двунаправленный: гарантированная полоса пропускания 400 Кбит\с, максимальная полоса пропускания 800 Кбит\с.* *5. Другие двунаправленные протоколы: полоса пропускания не гарантируется и не ограничивается. Этот трафик будет использовать всю доступную полосу пропускания, если протоколы SMTP/HTTP/HTTPS/FTP не загружают полностью полосу пропускания.* *5. Приоритеты: наибольший SMTP – 7,* *второй приоритет HTTP/HTTPS – 5,* *третий приоритет FTP – 3.*

Схема 51	

Настройка DFL-860E

Web-интерфейс

Настройка адреса интерфейса и основного шлюза

Зайдите в меню *Interfaces→Ethernet→wan1*. Снимите выделение *Enable DHCP Client.*

Зайдите в меню *Objects→Address Book→InterfaceAddresses*. Введите следующие параметры:

lan_ip	192.168.10.1
lannet	192.168.10.0/24
wan1_ip	192.168.110.1
wan1net	192.168.110.0/24
wan1_gw	192.168.110.254 (если этот объект не существует, то создайте его)

Зайдите в меню *Interfaces→Ethernet→wan1*. В выпадающем меню *Default Gateway* выберите ***wan1_gw*** для интерфейса ***wan1***. Нажмите Ok.

IP-правила межсетевого экрана

Перейдите в меню *Rules→IP Rules*. Создайте IP-правило для протокола SMTP во вкладке *General*:

Name	SMTP_BW_Control
Action	NAT
Service	smtp
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets

Создайте IP-правило для протокола HTTP во вкладке *General*:

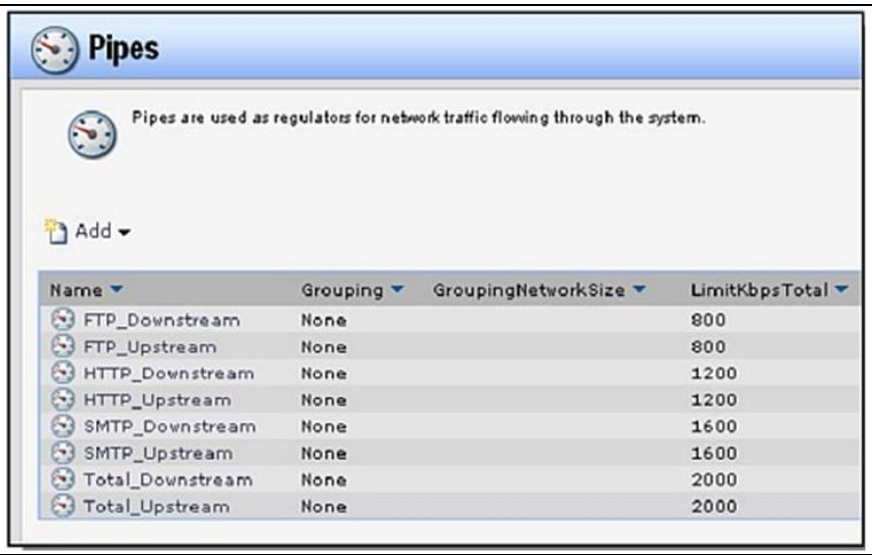
Name	HTTP_BW_Control
Action	NAT
Service	http-all
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets

Создайте IP-правило для протокола FTP во вкладке *General*:

Name	FTP_BW_Control
Action	NAT

Service	ftp-passthrough
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets
Создайте IP-правило для других протоколов (others) во вкладке *General*:	
Name	Others_BW_Control
Action	NAT
Service	all-services
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets
Создание Pipe-канала для каждого протокола	
Перейдите в меню *Traffic Management→Traffic Shaping→Pipes*. Добавьте новый Pipe-канал для нисходящего потока SMTP:	
Вкладка *General*:	
Name	SMTP_Downstream
Precedences	оставьте значения по умолчанию 0, 0, 7
Вкладка *Pipe Limits*:	
Precedence 0~7	оставьте поля незаполненными (по умолчанию)
Total kilobits per second	1600
Добавьте новый Pipe-канал для восходящего потока SMTP:	
Вкладка *General*:	
Name	SMTP_Upstream
Precedences	оставьте значения по умолчанию 0, 0, 7
Вкладка *Pipe Limits*:	
Precedence 0~7	оставьте поля незаполненными (по умолчанию)
Total kilobits per second	1600
Добавьте новый Pipe-канал для нисходящего потока HTTP:	
Вкладка *General*:	
Name	HTTP_Downstream
Precedences	оставьте значения по умолчанию 0, 0, 7
Вкладка *Pipe Limits*:	
Precedence 0~7	оставьте поля незаполненными (по умолчанию)
Total kilobits per second	1200
Добавьте новый Pipe-канал для восходящего потока HTTP:	
Вкладка *General*:	
Name	HTTP_Upstream
Precedences	оставьте значения по умолчанию 0, 0, 7
Вкладка *Pipe Limits*:	
Precedence 0~7	оставьте поля незаполненными (по умолчанию)
Total kilobits per second	1200

Добавьте новый Pipe-канал для нисходящего потока FTP:	
Вкладка *General*:	
Name	FTP_Downstream
Precedences	оставьте значения по умолчанию 0, 0, 7
Вкладка *Pipe Limits*:	
Precedence 0~7	оставьте поля незаполненными (по умолчанию)
Total kilobits per second	800
Добавьте новый Pipe-канал для восходящего потока FTP:	
Вкладка *General*:	
Name	FTP_Upstream
Precedences	оставьте значения по умолчанию 0, 0, 7
Вкладка *Pipe Limits*:	
Precedence 0~7	оставьте поля незаполненными (по умолчанию)
Total kilobits per second	800
Добавьте новый Pipe-канал дляTotal Downstream:	
Вкладка *General*:	
Name	Total_Downstream
Precedences	оставьте значения по умолчанию 0, 0, 7
Вкладка *Pipe Limits*:	
Precedence 7	800
Precedence 5	600
Precedence 3	400
Total kilobits per second	2000
Добавьте новый Pipe-канал для Total Upstream:	
Вкладка *General*:	
Name	Total_Upstream
Precedences	оставьте значения по умолчанию 0, 0, 7
Вкладка *Pipe Limits*:	
Precedence 7	800
Precedence 5	600
Precedence 3	400
Total kilobits per second	2000
Проверьте выполненные настройки pipe в общем списке Traffic Management→Traffic Shaping→Pipes (см. рисунок 7.4)	
Рисунок 7.4	



Создание Pipe-правил для каждого протокола

Перейдите в меню *Traffic Management→Traffic Shaping→Pipe Rules*. Добавьте новое правило Pipe Rule для нисходящего потока SMTP:

Вкладка *General*:

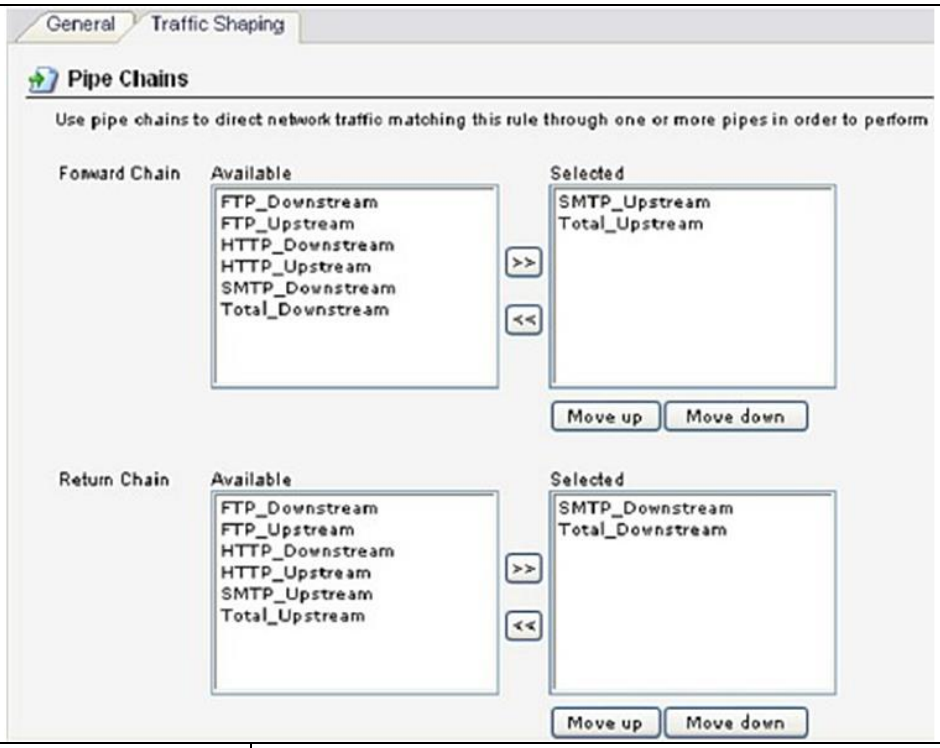
Name	SMTP_Shaping
Service	smtp
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets

Вкладка *Traffic Shaping*:

Selected Forward Chain	SMTP_Upstream, Total_Upstream
Selected Return Chain	SMTP_Downstream, Total_Downstream

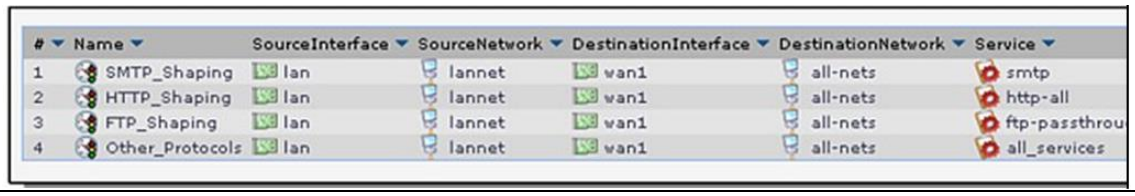
Примечание: SMTP Pipes (SMTP_Upstream или SMTP_Downstream) необходимо расположить перед Total band width (total_Upstream или Total_Downstream) (см. рисунок 7.5).

Рисунок 7.5



Precedence	Use Fixed Precedence: 7
Добавьте новое правило Pipe Rule для потока HTTP:	
Вкладка *General*:	
Name	HTTP_Shaping
Service	http-all
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets
Вкладка *Traffic Shaping*:	
Selected Forward Chain	HTTP_Upstream, Total_Upstream
Selected Return Chain	HTTP_Downstream, Total_Downstream
Примечание: HTTP Pipes (HTTP_Upstream или HTTP_Downstream) необходимо расположить перед Total band width (Total_Upstream или Total_Downstream).	
Precedence	Use Fixed Precedence: 5
Добавьте новое правило Pipe Rule для потока FTP:	
Вкладка *General*:	
Name	FTP_Shaping
Service	ftp-passthrough
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets
Вкладка *Traffic Shaping*:	
Selected Forward Chain	FTP_Upstream, Total_Upstream
Selected Return Chain	FTP_Downstream, Total_Downstream

Примечание: FTP Pipes (FTP_Upstream или FTP_Downstream) необходимо расположить перед Total band width (Total_Upstream или Total_Downstream).	
Precedence	Use Fixed Precedence: 3
Добавьте новое правило Pipe Rule для остальных (Other) протоколов:	
Вкладка *General*:	
Name	Other_Protocols
Service	all-services
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets
Вкладка *Traffic Shaping*:	
Selected Forward Chain	Total_Upstream
Selected Return Chain	Total_Downstream
Precedence	Use Fixed Precedence: 0
Примечание: HTTP Pipes (HTTP_Upstream или HTTP_Downstream) необходимо расположить перед Total band width (Total_Upstream или Total_Downstream.	
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Убедитесь, что настройки Pipe Rule имеют вид, как на рисунке 7.6.	
Рисунок 7.6	



Командная строка (CLI)

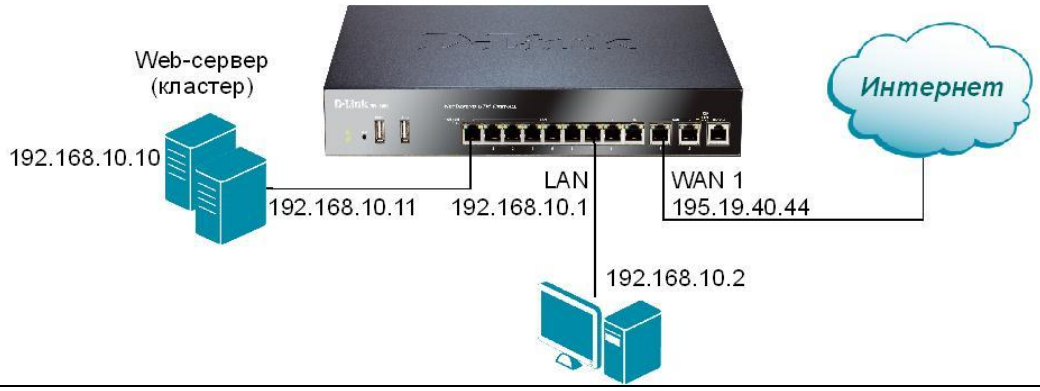
```
gw-world:/>set Interface Ethernet wan1 DHCPEnabled=No
gw-world:/> set IP4Address InterfaceAddresses/lan_ip Address=192.168.10.1
gw-world:/> set IP4Address InterfaceAddresses/lannet Address=192.168.10.0/24
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=192.168.110.1
gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=192.168.110.0/24
gw-world:/> set IP4Address InterfaceAddresses/wan1_gw Address=192.168.110.254
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=NAT Service=smtp SourceInterface=lan
SourceNetwork=InterfaceAddresses/lannet DestinationInterface=wan1 DestinationNetwork=all-nets
Name=SMTP_BW_Control
gw-world:/1(labs)> add IPRule Action=NAT Service=http-all SourceInterface=lan
SourceNetwork=InterfaceAddresses/lannet DestinationInterface=wan1 DestinationNetwork=all-nets
Name=HTTP_BW_Control
gw-world:/1(labs)> add IPRule Action=NAT Service=ftp-passthroughSourceInterface=lan
SourceNetwork=InterfaceAddresses/lannet DestinationInterface=wan1 DestinationNetwork=all-nets
Name=FTP_BW_Control
gw-world:/1(labs)> add IPRule Action=NAT Service=all-services SourceInterface=lan
SourceNetwork=InterfaceAddresses/lannet DestinationInterface=wan1 DestinationNetwork=all-nets
Name=Others_BW_Control
gw-world:/1(labs)> cc
gw-world:/>add Pipe SMTP_Downstream LimitKbpsTotal=1600 PrecedenceMin=0
PrecedenceDefault=0 PrecedenceMax=7
```

gw-world:/>add Pipe SMTP_Upstream LimitKbpsTotal=1600 PrecedenceMin=0 PrecedenceDefault=0 PrecedenceMax=7
gw-world:/> add Pipe HTTP_Downstream LimitKbpsTotal=1200 PrecedenceMin=0 PrecedenceDefault=0 PrecedenceMax=7
gw-world:/> add Pipe HTTP_Upstream LimitKbpsTotal=1200 PrecedenceMin=0 PrecedenceDefault=0 PrecedenceMax=7
gw-world:/> add Pipe FTP_Downstream LimitKbpsTotal=800 PrecedenceMin=0 PrecedenceDefault=0 PrecedenceMax=7
gw-world:/> add Pipe FTP_Upstream LimitKbpsTotal=800 PrecedenceMin=0 PrecedenceDefault=0 PrecedenceMax=7
gw-world:/> add Pipe Total_Downstream PrecedenceMin=0 PrecedenceDefault=0 PrecedenceMax=7LimitKbpsTotal=2000 LimitKbps3=400 LimitKbps5=600 LimitKbps7=800
gw-world:/> add Pipe Total_Upstream PrecedenceMin=0 PrecedenceDefault=0 PrecedenceMax=7LimitKbpsTotal=2000 LimitKbps3=400 LimitKbps5=600 LimitKbps7=800
gw-world:/>add PipeRule DestinationInterface=wan1 DestinationNetwork=all-nets SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Service=smtp Name=SMTP_Shaping ForwardChain=SMTP_Upstream,Total_Upstream ReturnChain=SMTP_Downstream,Total_DownstreamIndex=1
gw-world:/>add PipeRule DestinationInterface=wan1 DestinationNetwork=all-nets SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Service=http-all Name=HTTP_Shaping ForwardChain=HTTP_Upstream,Total_Upstream ReturnChain=HTTP_Downstream,Total_DownstreamIndex=2
gw-world:/>add PipeRule DestinationInterface=wan1 DestinationNetwork=all-nets SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Service=ftp-passthrough Name=FTP_Shaping ForwardChain=FTP_Upstream,Total_Upstream ReturnChain=FTP_Downstream,Total_DownstreamIndex=3
gw-world:/>add PipeRule DestinationInterface=wan1 DestinationNetwork=all-nets SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Service=all-servicesName=Other_Protocols ForwardChain=Total_Upstream ReturnChain=Total_DownstreamIndex=4 Precedence=Fixed FixedPrecedence=0
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Упражнение	Измерьте скорости входящего/исходящего потока для компьютерного класса без межсетевого экрана. Затем измерьте скорости входящего/исходящего потоков с компьютера, расположенного за межсетевым экраном. Сравните заданные параметры с полученными при измерении.
InternetExplorer ОС Windows	http://www.speedtest.net. Запустите тест скорости Интернета.

Настройка опции Server Load Balancing.

Описание	*Функция Server Load Balancing (SLB) позволяет создавать на межсетевом экране правило IP Rule с действием SLB_SAT для группы серверов с одним IP-адресом. Такие группы серверов называются обычно серверной фермой и представляют собой кластерное решение для повышения эффективности, доступности и надежности серверных систем.* *На межсетевых экранах D-Link используется два алгоритма распределения серверной нагрузки SLB–Round-robin и Connection-rate.* *- Round-robin* *Алгоритм распределяет подключения между серверами поочередно, все сервера считаются одинаковыми.* *- Connection-rate* *Алгоритм распределяет запросы к серверам в соответствии с*

	определенными временными периодами Window Time. Следующий запрос будет отправлен серверу, имеющему наименьшее количество подключений за указанное время Window Time. *SLB может учитывать необходимую привязку некоторых клиентов к определенным серверам. Эта опция называется stickiness. Различают следующие виды такой привязки:* *- Pre-state Distribution* *Этот режим не включает опцию stickiness. Каждое последующее соединение будет независимо от предыдущих.* *- IP Address Stickiness* *При этом режиме серия соединений от определенного клиента будет обработана определенным сервером. Обычно этот режим используется для TLS- и SSL-служб, таких как HTTPS.* *- Network Stickiness* *Этот режим использует привязку клиентов к определенной подсети. Для подсети указывается ее размер в качестве параметра.* *SLB использует функции мониторинга состояния серверов в серверной ферме – Server Health Monitoring. Мониторинг может осуществляется с помощью ICMP ping и TCP Connection.* *Правило с действием SLB требует наличия еще одного правила с действием Allow или NAT. При этом действие Forward fast во втором правиле не допустимо.*
Описание сценария	*Два Web-сервера в кластере серверов находятся за межсетевым экраном. Приватные IP-адреса серверов – 192.168.10.10 и 192.168.10.11. Необходимо настроить мониторинг серверов в ферме, опцию stickiness. NAT совместно с SLB_SAT используется для доступа к серверам внутренних пользователей, для внешних пользователей – правило SLB_SAT и правило с действием Allow.*
Схема 52	

<u>Настройка DFL-860E</u>

<u>Web-интерфейс</u>

Создадим объект «IP-адрес сервера 1». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:

Name	server1
Address	192.168.10.10

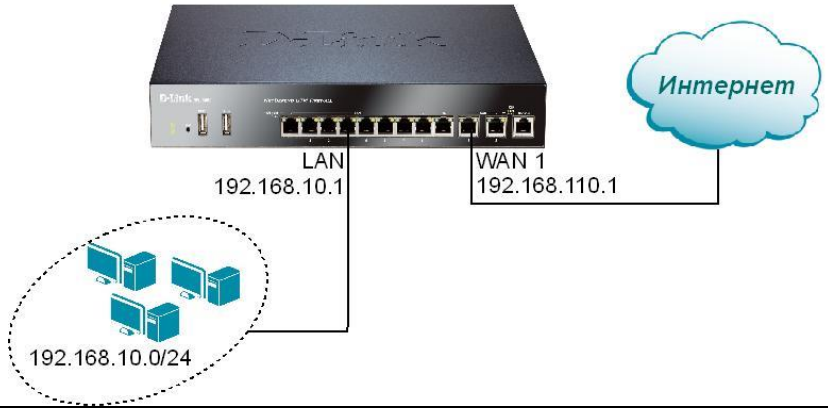
Создадим объект «IP-адрес сервера 2». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:

Name	server2
Address	192.168.10.11

Создадим объект «внешний IP-адрес сервера (ip_ext)». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	ip_ext
Address	195.19.40.44
Создадим IP4 Group. Зайдите в меню *Objects→Address Book Add→IP4 Group*. Введите следующие параметры:	
Name	server_group
Переместите server1 и server2 из списка Available в список Selected.	
Создание правил IP Rule	
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	Web_SLB
Action	SLB_SAT
Service	http
Source Interface	any
Source Network	all-nets
Destination Interface	core
Destination Network	ip_ext
Во вкладке *SLB SAT* для Server Addresses добавьте server_group в список Selected.	
Distribution	Выберите Connection-rate
Stickiness	IP Address Stickiness
Во вкладке *SLB Monitors* введите:	
Monitoring using ICMP Ping packets	Поставьте галочку
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	Web_SLB_NAT
Action	NAT
Service	http
Source Interface	any
Source Network	all-nets
Destination Interface	core
Destination Network	ip_ext
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	Web_SLB_ALW
Action	Allow
Service	http
Source Interface	any
Source Network	all-nets
Destination Interface	core
Destination Network	ip_ext
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.19.40.44 gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.19.40.0/24 gw-world:/> add Address AddressFolder labs	

gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address server1 Address=192.168.10.10
gw-world:/labs> add IP4Address server2 Address=192.168.10.11
gw-world:/labs> add IP4Address ip_ext Address=195.19.40.44
gw-world:/labs> add IP4Group server_group Members=labs/server1,labs/server2
gw-world:/labs> cc
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=SLB_SAT Service=http SourceInterface=anySourceNetwork=all-nets DestinationInterface=core DestinationNetwork=labs/ip_ext Name=Web_SLBSLBAddresses=labs/server_group SLBDistribution=ConnectionRate SLBStickiness=IP SLBMonitorPing=Yes
gw-world:/1(labs)> add IPRule Action=NAT Service=http SourceInterface=any SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=labs/ip_ext Name=Web_SLB_NAT
gw-world:/1(labs)> add IPRule Action=Allow Service=http SourceInterface=any SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=labs/ip_ext Name=Web_SLB_ALW
gw-world:/1(labs)> cc
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Упражнение	Проверьте доступность серверной фермы. Просмотрите статистику подключений на серверах. Зайдите в меню *Status→Server Load Balancing*, посмотрите состояние правила SLB.
Internet Explorer ОС Windows	http://<ip_ext>
Опция Threshold Rules.	
Описание	*Задача правила Threshold Rule состоит в обнаружении ненормальной активности создаваемых подключений. Например, зараженный вирусом хост пытается распространить вирус далее в сети, интенсивно создавая одинаковые подключения на другие адреса в сети.* *Параметры Threshold Rule:* *- Action* *Задает событие при превышении лимита. Могут быть выбраны опции Audit или Protect.* *- Group by* *Правило будет действовать на хост или подсеть (Host, Network).* *- Threshold* *Цифровое значение контролируемого предела в правиле.* *- Threshold Type* *Тип правила – предел по подключениям в секунду или предел общего количества подключений.*
Описание сценария	*Необходимо ограничить общее количество подключений для пользователей в **lan**-сети значением 10. Протокол – HTTP. В случае превышения предела хост необходимо заблокировать на минуту.*

Схема 53	

Настройка DFL-860E

Web-интерфейс

Создание Threshold Rule

Зайдите в меню *Traffic Management→Threshold Rules→Add→Threshold Rule.* Во вкладке *General* введите:

Name	http_rule
Service	http
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets

Во вкладке *Threshold Action* добавьте пороговое действие, введите для него:

Action	Protect
Group By	Host-based
Threshold	10 connections
Activate BlackList	Поставьте галочку
Time to block	60

Создание IP Rule

Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:

Name	NAT-http
Action	NAT
Service	http
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets

Зайдите в меню *Configuration* и выберите *Save and Activate.*

Командная строка (CLI)

```
gw-world:/> add ThresholdRule DestinationInterface=wan1 DestinationNetwork=all-nets SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Service=http Name=http_rule Index=1
gw-world:/> cc ThresholdRule 1(http_rule)
gw-world:/1(http_rule)> add ThresholdAction Threshold=10 Action=Protect GroupBy=SourceIP
```

Index=1 ThresholdUnit=Conns BlackList=Yes BlackListTimeToBlock=60 gw-world:/1(http_rule)> cc gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=NAT Service=http SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=wan1 DestinationNetwork=all-nets Name=NAT-http gw-world:/1(labs)> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Упражнение	Проверьте работоспособность пороговых правил. С компьютера в lan-сети откройте подключения, превышающие порог срабатывания. Зайдите в меню *Status→Black List*. Проверьте наличие блокирования хоста, превысившего лимит подключений.
Internet Explorer ОС Windows	http://<более десяти различных сайтов>
Опция IDP Traffic Shaping.	
Описание	*IDP Traffic Shaping – механизм управления трафиком на основе системы IDP. Для приложений P2P очень часто возникает проблема загрузки всей полосы пропускания, что влияет на гарантированное качество обслуживания. Используя комбинацию IDP и Traffic Shaping, можно выделить трафик от критических приложений и применить к нему правила управления трафиком.*
Описание сценария	*Необходимо организовать управление трафиком приложения P2P. Ограничение для приложений P2P – 100 Кбит/сек (схема 53)*
Настройка DFL-860E	
Web-интерфейс	
Создадим IDP Rule. Зайдите в меню *IDP/IPS→IDP Rules→Add→IDP Rule*. Задайте параметры:	
Name	IPS_P2P
Service	all_tcp
Schedule	None
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets
Создадим IDP Rule Action. Во вкладке *Rule Action* добавьте действие и задайте параметры:	
Action	Pipe
Signature (s)	Выберите POLICY_P2P_POLICY
Bandwidth	100
Network	all-nets
Во вкладке *LogSettings* задайте параметры:	
Enable Logging	Поставьте галочку
Log with severity	Выберите из списка Info
Создание IP Rule	
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:	
Name	NAT-tcp

Action	NAT
Service	all_tcp
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets

Зайдите в меню *Configuration* и выберите *Save and Activate*.

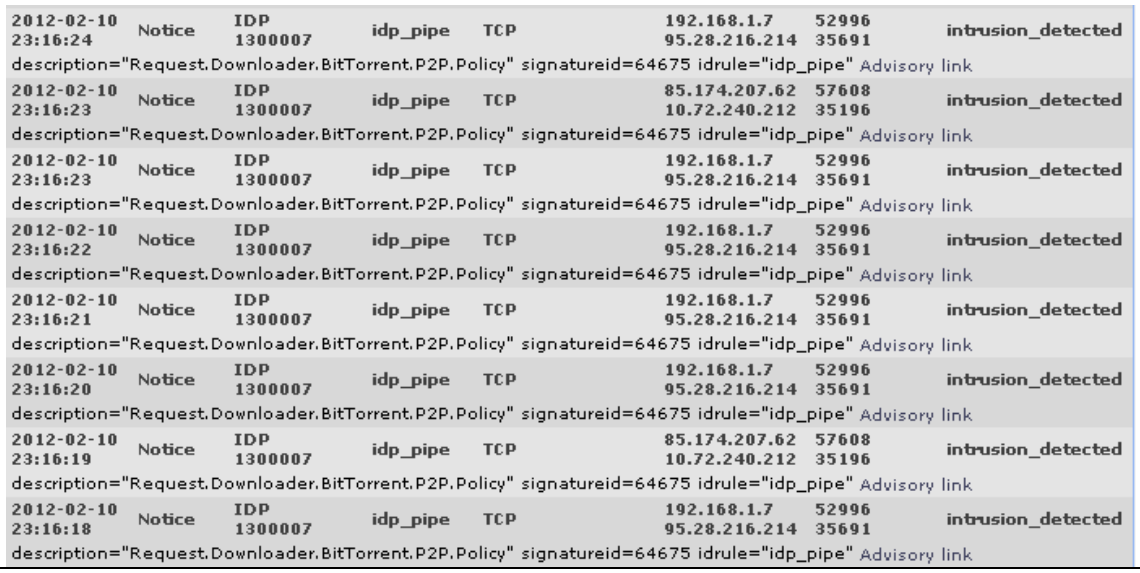
Командная строка (CLI)

```
gw-world:/> add IDPRule DestinationInterface=wan1 DestinationNetwork=all-nets SourceInterface=lan
SourceNetwork=InterfaceAddresses/lannet Service=all_tcp Index=1 Name=IPS_P2P
gw-world:/> cc IDPRule 1(IPS_P2P)
gw-world:/1(IPS_P2P)> add IDPRuleAction Action=Pipe PipeLimit=100 PipeNetwork=all-nets Index=1
Signatures=POLICY_P2P_POLICY
gw-world:/1(IPS_P2P)> cc
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=NAT Service=all_tcp SourceInterface=lan
SourceNetwork=InterfaceAddresses/lannet DestinationInterface=wan1 DestinationNetwork=all-nets
Name=NAT-tcp
gw-world:/1(labs)> cc
gw-world:/> activate (подождать 3-5 секунд)
gw-world:/>commit
```

Упражнение	Проверьте работоспособность IDP-правила. С компьютера **lan**-сети откройте подключение P2P. Зайдите в меню *Status→IDP/IPS*. Проверьте наличие срабатывания сигнатуры для управления трафиком приложения P2P.
P2P	Bit Torrent

Пример сообщений IDP/IPS с действием Pipe показан на рисунке 7.7.

Рисунок 7.7



ЗАНЯТИЕ №11. Функции отказоустойчивости. Настройка конфигурации Failover на примере двух ISP-подключений. Настройка IPSec VPN failover.

Надежность и отказоустойчивость – очень важное требование для современных сетей. Межсетевые экраны D-Link позволяют настроить переключение соединения с одного ISP-подключения на другое при отказе одного из них. Переключение между туннелями IPSec.

Цель	Эта лабораторная работа предназначена для ознакомления пользователей с настройкой функции переключения при отказе (Failover) на межсетевых экранах D-Link	
Оборудование	DFL-860E	2
	Рабочая станция	2
	Ethernet-кабель (патч-корд)	6

Настройка Failover на межсетевом экране	
Настройка IPSec VPN failover	*Этот сценарий показывает как на двух межсетевых экранах настроить переключение при отказе одного из соединений IPSec VPN, установленных между двумя каналами связи на wan-интерфейсах.*
Описание сценария	*При выходе из строя одного из каналов (основного), весь VPN-трафик необходимо перенаправить в реальном режиме времени на другой (резервный) канал. Когда основной канал вернется в рабочее состояние, сервисы продолжат работу на нем.* *Wan-каналы: основной канал (main circuit) и резервный канал (backup circuit). Весь трафик между межсетевыми экранами A и B передается по IPSec VPN-туннелю.*
Схема 54	
Настройка DFL-860E	
Устройство A	
Web-интерфейс	
Создание необходимых объектов	
Зайдите в меню *Interfaces→Ethernet→wan1*. Снимите выделение *Enable DHCP Client.*	
Зайдите в меню *Objects→Address Book→InterfaceAddresses*. Введите значения:	
lan_ip	192.168.10.1

lannet	192.168.10.0/24
wan1_ip	192.168.110.1
wan1net	192.168.110.0/24
wan2_ip	192.168.120.1
wan2net	192.168.120.0/24
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Создайте следующие объекты:	
Name	fwB-IPSec-remote-net
Address	192.168.2.0/24
Name	fwB-main-remote-gw
Address	192.168.110.253
Name	fwB-backup-remote-gw
Address	192.168.120.253
Создание Pre-shared Keys для IPSec-туннелей	
Зайдите в меню *Objects→Authentication Objects→Pre-Shared keys.* Добавьте ключи Pre-Shared Key для основного (main) и резервного (backup) туннелей (ключи могут быть как одинаковыми,так и разными):	
Name	fwB-main-psk
Shared secret	123456qw
Shared secret Confirm Secret	123456qw
Name	fwB-backup-psk
Shared secret	12345678
Shared secret Confirm Secret	12345678
Настройка основного IPSec-интерфейса	
Зайдите в меню *Interfaces→IPSec.* Добавьте новый туннель IPSec Tunnel для Main WAN link (основной каналWAN). Во вкладке *General* введите*:*	
Name	Main-IPSec-tunnel
Local Network	lannet
Remote Network	fwB-IPSec-remote-net
Remote Endpoint	fwB-main-remote-gw
Encapsulation Mode	Tunnel
В разделе *Algorithms* введите*:*	
IKE Algorithms	Standard
IKE Lifetime	28800
IPSec Algorithms	Standard
IPSec Lifetime	3600 (seconds)
IPSec Lifetime	0 (kilobytes)
Во вкладке *Authentication* введите*:*	
Pre-Shared Key	fwB-main-psk (выберите из списка)
Во вкладке *Keep-alive* (элемент поддержки установленного соединения) выберите Auto.	
Во вкладке *Advanced* введите*:*	
Add route for remote network	Уберите галочку, т.к. функции мониторинга нет.

Настройка резервного IPSec-интерфейса	
Зайдите в меню *Interfaces→IPSec*. Добавьте новый туннель IPSec Tunnel для Backup WAN link (резервный канал WAN). Во вкладке *General* введите*:*	
Name	Backup-IPSec-tunnel
Local Network	lannet
Remote Network	fwB-IPSec-remote-net
Remote Endpoint	fwB-backup-remote-gw
Encapsulation Mode	Tunnel
В разделе *Algorithms* введите*:*	
IKE Algorithms	Standard
IKE Lifetime	28800
IPSec Algorithms	Standard
IPSec Lifetime	3600 (seconds)
IPSec Lifetime	0 (kilobytes)
Во вкладке *Authentication* введите*:*	
Pre-Shared Key	fwB-backup-psk (выберите из списка)
Во вкладке *Keep-alive* (элемент поддержки установленного соединения) выберите Auto.	
Во вкладке *Advanced* введите*:*	
Add route for remote network	Уберите галочку, т.к. функции мониторинга нет.
Настройка интерфейсной группы	
Зайдите в меню *Interfaces→Interface Groups.* Добавьте новую группу Interface Group. Во вкладке *General* введите*:*	
Name	IPSec-Lan-Group
Interfaces	Выберите из списка: Backup-IPSec-tunnel, Main-IPSec-tunnel, lan.
Настройка IP Rule	
Перейдите в меню *Rules→IP Rules*. Создайте IP Rule. Во вкладке *General* введите:	
Name	allow_Lan_to_fwB-IPSec
Action	Allow
Service	all_services
Source Interface	IPSec-Lan-Group
Source Network	all-nets
Destination Interface	IPSec-Lan-Group
Destination Network	all-nets
Настройка маршрута для мониторинга интерфейса	
Перейдите в меню *Routing→Routing Tables*. Нажмите на таблицу маршрутизации ***main***. Добавьте новый маршрут Route для основного туннеля IPSec. Во вкладке *General* введите:	
Interface	Main-IPSec-tunnel
Network	fwB-IPSec-remote-net
Gateway	none
Local IP Address	none
Metric	60
Во вкладке *Monitor*	
Monitor This Route	Поставьте галочку

Monitor Interface Link Status	Поставьте галочку
Добавьте новый маршрут Route для резервного туннеля IPSec. Во вкладке *General* введите:	
Interface	Backup-IPSec-tunnel
Network	fwB-IPSec-remote-net
Gateway	none
Local IP Address	none
Metric	70
Во вкладке *Monitor*	
Monitor This Route	Поставьте галочку
Monitor Interface Link Status	Поставьте галочку
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	

```
gw-world:/>set Interface Ethernet wan1 DHCPEnabled=No
gw-world:/> set IP4Address InterfaceAddresses/lan_ip Address=192.168.10.1
gw-world:/> set IP4Address InterfaceAddresses/lannet Address=192.168.10.0/24
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=192.168.110.1
gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=192.168.110.0/24
gw-world:/> set IP4Address InterfaceAddresses/wan2_ip Address=192.168.120.1
gw-world:/> set IP4Address InterfaceAddresses/wan2net Address=192.168.120.0/24
gw-world:/> add Address AddressFolder labs
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address fwB-IPSec-remote-net Address=192.168.2.0/24
gw-world:/labs> add IP4Address fwB-main-remote-gw Address=192.168.110.253
gw-world:/labs> add IP4Address fwB-backup-remote-gw Address=192.168.120.253
gw-world:/labs> cc
gw-world:/> add PSK fwB-main-psk Type=ASCII PSKAscii=123456qw
gw-world:/> add PSK fwB-backup-psk Type=ASCII PSKAscii=12345678
gw-world:/> add Interface IPsecTunnel Main-IPSec-tunnel AuthMethod=PSK IKEAlgorithms=Standard
IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet PSK=fwB-main-psk
RemoteNetwork=labs/fwB-IPSec-remote-netRemoteEndpoint=labs/fwB-main-remote-gw
KeepAlive=Auto AddRouteToRemoteNet=No IKELifeTimeSeconds=28800
IPsecLifeTimeSeconds=3600 PFS=None SetupSAPer=Net DHGroup=2 NATTraversal=OnIfNeeded
DeadPeerDetection=Yes EncapsulationMode=Tunnel
gw-world:/> add Interface IPsecTunnel Backup-IPSec-tunnel AuthMethod=PSK
IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet
PSK=fwB-backup-psk RemoteNetwork=labs/fwB-IPSec-remote-net RemoteEndpoint=labs/fwB-
backup-remote-gw KeepAlive=Auto AddRouteToRemoteNet=No IKELifeTimeSeconds=28800
IPsecLifeTimeSeconds=3600 PFS=None SetupSAPer=Net DHGroup=2 NATTraversal=OnIfNeeded
DeadPeerDetection=Yes EncapsulationMode=Tunnel
gw-world:/> add Interface InterfaceGroup IPSec-Lan-Group Members=Main-IPSec-tunnel, Backup-
IPSec-tunnel,lan
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=IPSec-Lan-Group
SourceNetwork=all-nets DestinationInterface=IPSec-Lan-Group DestinationNetwork=all-nets
Name=allow_Lan_to_fwB-IPSec
gw-world:/1(labs)> cc
gw-world:/> cc RoutingTable main
gw-world:/main> add Route Interface=Main-IPSec-tunnel Network=labs/fwB-IPSec-remote-net
Metric=60 RouteMonitor=Yes MonitorLinkStatus=Yes
gw-world:/main> add Route Interface=Backup-IPSec-tunnel Network=labs/fwB-IPSec-remote-net
Metric=70 RouteMonitor=Yes MonitorLinkStatus=Yes MonitorGateway=Yes
```

gw-world:/main> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Настройка DFL-860E	
Устройство B	
Web-интерфейс	
Создание необходимых объектов	
Зайдите в меню *Interfaces→Ethernet→wan1*. Снимите выделение *Enable DHCP Client.*	
Зайдите в меню *Objects→Address Book→InterfaceAddresses*. Введите значения:	
lan_ip	192.168.2.1
lannet	192.168.2.0/24
wan1_ip	192.168.110.253
wan1net	192.168.110.0/24
wan2_ip	192.168.120.253
wan2net	192.168.120.0/24
Зайдите в меню *Objects→Address Book*. Добавьте новую папку *Address Folder* под именем *RemoteHost*, в ней создайте следующие объекты:	
Name	fwA-IPSec-remote-net
Address	192.168.10.0/24
Name	fwA-main-remote-gw
Address	192.168.110.1
Name	fwA-backup-remote-gw
Address	192.168.120.1
Создание Pre-shared Keys для IPSec-туннелей	
Зайдите в меню *Objects→Authentication Objects→Pre-Shared Key*. Добавьте ключи Pre-Shared Key для основного (main) и резервного (backup) туннелей (ключи могут быть как одинаковыми, так и разными):	
Name	fwA-main-psk
Shared secret	123456qw
Shared secret ***Confirm Secret***	123456qw
Name	fwA-backup-psk
Shared secret	12345678
Shared secret ***Confirm Secret***	12345678
Настройка главного IPSec-интерфейса	
Зайдите в меню *Interfaces→IPSec*. Добавьте новый туннель IPSec Tunnel для Main WAN link (основной канал WAN). Во вкладке *General* введите*:*	
Name	Main-IPSec-tunnel
Local Network	lannet
Remote Network	fwA-IPSec-remote-net
Remote Endpoint	fwA-main-remote-gw
Encapsulation Mode	Tunnel

В разделе *Algorithms* введите*:*	
IKE Algorithms	Standard
IKE Lifetime	28800
IPSec Algorithms	Standard
IPSec Lifetime	3600 (seconds)
IPSec Lifetime	0 (kilobytes)
Во вкладке *Authentication* введите*:*	
Pre-Shared Key	fwA-main-psk (выберите из списка)
Во вкладке *Keep-alive* (элемент поддержки установленного соединения) выберите Auto.	
Во вкладке *Advanced* введите*:*	
Add route for remote network	Уберите галочку, т.к. функции мониторинга нет.
Настройка резервного IPSec-интерфейса	
Зайдите в меню *Interfaces→IPSec*. Добавьте новый туннель IPSec Tunnel для Backup WAN link (резервный канал WAN). Во вкладке *General* введите*:*	
Name	Backup-IPSec-tunnel
Local Network	lannet
Remote Network	fwA-IPSec-remote-net
Remote Endpoint	fwA-backup-remote-gw
Encapsulation Mode	Tunnel
В разделе *Algorithms* введите*:*	
IKE Algorithms	Standard
IKE Lifetime	28800
IPSec Algorithms	Standard
IPSec Lifetime	3600 (seconds)
IPSec Lifetime	0 (kilobytes)
Во вкладке *Authentication* введите*:*	
Pre-Shared Key	fwA-backup-psk (выберите из списка)
Во вкладке *Keep-alive* (элемент поддержки установленного соединения) выберите Auto.	
Во вкладке *Advanced* введите*:*	
Add route for remote network	Уберите галочку, т.к. функции мониторинга нет.
Настройка интерфейсной группы	
Зайдите в меню *Interfaces→Interface Groups.* Добавьте новую группу Interface Group. Во вкладке *General* введите*:*	
Name	IPSec-Lan-Group
Interfaces	Выберите из списка: Backup-IPSec-tunnel, Main-IPSec-tunnel, lan.
Настройка правил	
Перейдите в меню *Rules→IP Rules*. Создайте IP Rule, во вкладке *General* введите:	
Name	allow_Lan_to_fwA-IPSec
Action	Allow
Service	all_services
Source Interface	IPSec-Lan-Group

Source Network	all-nets
Destination Interface	IPSec-Lan-Group
Destination Network	all-nets
Настройка маршрута для мониторинга интерфейса	
Перейдите в меню *Routing→Routing Tables*. Нажмите на таблицу маршрутизации ***main***. Добавьте новый маршрут Route для основного туннеля IPSec. Во вкладке *General* введите:	
Interface	Main-IPSec-tunnel
Network	fwA-IPSec-remote-net
Gateway	none
Local IP Address	none
Metric	60
Во вкладке *Monitor*	
Monitor This Route	Поставьте галочку
Monitor Interface Link Status	Поставьте галочку
Добавьте новый маршрут Route для резервного туннеля IPSec. Во вкладке *General* введите:	
Interface	Backup-IPSec-tunnel
Network	fwA-IPSec-remote-net
Gateway	none
Local IP Address	none
Metric	70
Во вкладке *Monitor*	
Monitor This Route	Поставьте галочку
Monitor Interface Link Status	Поставьте галочку
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	

```
gw-world:/>set Interface Ethernet wan1 DHCPEnabled=No
gw-world:/> set IP4Address InterfaceAddresses/lan_ip Address=192.168.2.1
gw-world:/> set IP4Address InterfaceAddresses/lannet Address=192.168.2.0/24
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=192.168.110.253
gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=192.168.110.0/24
gw-world:/> set IP4Address InterfaceAddresses/wan2_ip Address=192.168.120.253
gw-world:/> set IP4Address InterfaceAddresses/wan2net Address=192.168.120.0/24
gw-world:/> add Address AddressFolder labs
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address fwA-IPSec-remote-net Address=192.168.2.0/24
gw-world:/labs> add IP4Address fwA-main-remote-gw Address=192.168.110.1
gw-world:/labs> add IP4Address fwA-backup-remote-gw Address=192.168.120.1
gw-world:/labs> cc
gw-world:/> add PSK fwA-main-psk Type=ASCII PSKAscii=123456qw
gw-world:/> add PSK fwA-backup-psk Type=ASCII PSKAscii=12345678
gw-world:/> add Interface IPsecTunnel Main-IPSec-tunnel AuthMethod=PSK IKEAlgorithms=Standard
IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet PSK=fwA-main-psk
RemoteNetwork=labs/fwA-IPSec-remote-net RemoteEndpoint=labs/fwA-main-remote-gw
KeepAlive=Auto AddRouteToRemoteNet=No IKELifeTimeSeconds=28800
IPsecLifeTimeSeconds=3600 PFS=None SetupSAPer=Net DHGroup=2 NATTraversal=OnIfNeeded
DeadPeerDetection=Yes EncapsulationMode=Tunnel
gw-world:/> add Interface IPsecTunnel Backup-IPSec-tunnel AuthMethod=PSK
IKEAlgorithms=Standard IPsecAlgorithms=Standard LocalNetwork=InterfaceAddresses/lannet
```

PSK=fwA-backup-psk RemoteNetwork=labs/fwA-IPSec-remote-net RemoteEndpoint=labs/fwA-backup-remote-gw KeepAlive=Auto AddRouteToRemoteNet=No IKELifeTimeSeconds=28800 IPsecLifeTimeSeconds=3600 PFS=None SetupSAPer=Net DHGroup=2 NATTraversal=OnIfNeeded DeadPeerDetection=Yes EncapsulationMode=Tunnel
gw-world:/> add Interface InterfaceGroup IPSec-Lan-Group Members=Main-IPSec-tunnel, Backup-IPSec-tunnel,lan
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow Service=all_services SourceInterface=IPSec-Lan-Group SourceNetwork=all-nets DestinationInterface=IPSec-Lan-Group DestinationNetwork=all-nets Name=allow_Lan_to_fwB-IPSec
gw-world:/1(labs)> cc
gw-world:/> cc RoutingTable main
gw-world:/main> add Route Interface=Main-IPSec-tunnel Network=labs/fwA-IPSec-remote-net Metric=60 RouteMonitor=Yes MonitorLinkStatus=Yes
gw-world:/main> add Route Interface=Backup-IPSec-tunnel Network=labs/fwA-IPSec-remote-net Metric=70 RouteMonitor=Yes MonitorLinkStatus=Yes MonitorGateway=Yes
gw-world:/main> cc
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Упражнение	Проверьте работоспособность Failover. Физически отключите основной канал VPN-туннеля, проверьте наличие переключения на резервный канал. Зайдите в меню *Status→IPSec*. Проверьте переключение каналов.
CMD Windows (за межсетевым экраном A)	C:\>ping 192.168.2.1 –t –l 1400
CMD Windows(за межсетевым экраном B)	C:\>ping 192.168.10.1 –t –l 1400
Устранение возможных проблем	Если туннель не был создан, решите возникшую проблему с помощью описанных ниже диагностических средств.

Проверьте корректность физических подключений устройств, работоспособность патч-кордов, индикацию на устройствах. Включите режим отладки:

SSH CLI (Console CLI)	gw-world:/>ikesnoop –on<IP-адрес удаленного VPN-шлюза>

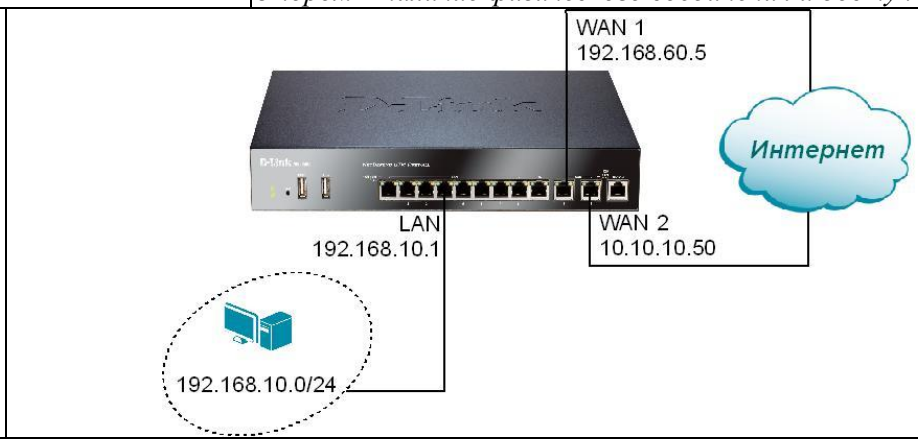
На устройствах зайдите в меню *Status→IPSec→ipsec_tunnel.* Проверьте корректность настроек туннелей, уточните статус SA для фазы 1 и фазы 2.

Зайдите в меню *Status→Logging* или просмотрите лог-сообщения на syslog-сервере, настроенном для работы с межсетевыми экранами.

Выполните настройку туннелей с простейшими параметрами аутентификации – общим ключом, используйте стандартные (заданные по умолчанию) настройки для алгоритмов IKE и IPSec, режимов IKE, работы с NAT-T, и не используйте пользовательские настройки для XAuth, IKE Config Mode Pool, PFS, ID, Local ID Type. После того, как туннель с этими упрощенными стандартными настройками будет установлен устройствами, измените его параметры в соответствии с особенностями задания в данном сценарии.

Настройка конфигурации Failover на примере двух ISP-подключений

Описание сценария	*Этот сценарий позволяет настроить конфигурацию межсетевого экрана для направления различных типов трафика через разные ISP-подключения (Internet Service Provider).* *1. Подключение к первому ISP основное, а ко второму – резервное.* *2. Для переключения с основного канала на резервный необходимо отслеживать статус подключения. Устройство имеет возможность отслеживать следующие параметры:* *- наличие физического подключения (*link*)* *- доступность шлюза (устройство запрашивает шлюз с*

	помощью ARP). *Если шлюз перестает быть доступным или пропадает физическое соединение, устройство отключает основной маршрут к all-nets (подключение wan1 для этого сценария), но при этом останется маршрут к all-nets на резервном подключении, через который и пойдет уже весь трафик.* *3. Параметры, предоставленные Интернет-провайдерами:* *Первый ISP* *Тип подключения: Статический IP* *IP: 192.168.60.5* *Маска: 255.255.255.248 (192.168.60.0/29)* *Шлюз: 192.168.60.1* *DNS: 192.168.100.1* *Второй ISP* *Тип подключения: Статический IP* *IP: 10.10.10.50* *Маска: 255.255.255.252 (10.10.10.48/30)* *Шлюз: 10.10.10.49* *DNS: 10.1.10.1* *Особенность конфигурации Failover: разделение маршрутов в all-nets, у основного подключения метрика имеет высший приоритет в отличии от резервного подключения (чем меньше параметр метрики, тем главнее маршрут). Из-за этой особенности не работает функция перенаправления портов с резервного подключения, но этого можно избежать. Для отслеживания статуса основного соединения, необходимо создать два «мониторящих» маршрута, первый – wan1-wan1net, второй – wan1-all-nets-wan1_gw и удалить существующие маршруты этого интерфейса. В первом маршруте будем отслеживать только наличие физического соединения (link), во втором – наличие физического соединения и доступность шлюза.*
Схема 55	
Настройка DFL-860E	
Web-интерфейс	
Настройка интерфейсов wan	
Зайдите в меню *Interfaces→Ethernet*. Снимите галочку с Enable DHCP Client на wan1.	
Зайдите в меню *Objects→Address Book→InterfaceAddresses*. Введите следующие данные:	
wan1_ip	192.168.60.5
wan1_gw	192.168.60.1

wan1net	192.168.60.0/29
wan1_dns1	192.168.100.1
wan2_ip	10.10.10.50
wan2net	10.10.10.48/30
wan2_gw	10.10.10.49
Зайдите в меню *Objects→Interfaces→Ethernet*. В выпадающем меню *Default Gateway* выберите ***wan2_gw*** дляинтерфейса ***wan2***. Нажмите Ok.	
Пример настройки функции перенаправления портов	
Зайдите в меню *Objects→Interfaces→Ethernet*. Во вкладке *Advanced* для интерфейса wan1 введите:	
Add route for interface network	Уберите галочку
Add default route if default gateway is specified	Уберите галочку
Примечание: описанное действие автоматически удаляет создающиеся маршруты на интерфейсе wan1. Зайдите в меню Routing→RoutingTables→main (read-only), здесь можно увидеть два перечеркнутых маршрута. Данные маршруты были созданы автоматически системой для интерфейса wan1 и будут удаленны после активации настроек.	
Создание маршрутов для wan1	
Зайдите в меню *Routing→Routing Tables*. Создайте маршрут, введите данные для него:	
Interface	wan1
Network	wan1net
Metric	90
Во вкладке *Monitor* введите:	
Monitor This Route	Поставьте галочку
Monitor Interface Link Status	Поставьте галочку
Примечание: Созданный маршрут указывает DFL-устройству, что по интерфейсу wan1 у него находится сеть 192.168.60.0/29 (устройство будет обращаться к IP-адресам с 192.168.60.1 по 192.168.60.6, минуя шлюз), и что активирована функция отслеживания статуса физического соединения.	
Создайте второй маршрут, введите данные для него:	
Interface	wan1
Network	all-nets
Gateway	wan1_gw
Metric	95
Во вкладке *Monitor*:	
Monitor This Route	Поставьте галочку
Monitor Interface Link Status	Поставьте галочку
Monitor gateway Using ARP Lookup	Поставьте галочку
Примечание: Созданный маршрут указывает DFL-устройству, что следует через wan1_gw маршрутизировать весь разрешенный трафик, который предназначен для сетей, не обозначенных на интерфейсах DFL, и что активирована функция отслеживания статуса физического соединения. Настроенная конфигурация Failover не может использоваться полноценно, т.к. нет разрешающих правил для резервного соединения, то есть при срабатывании Failover устройство просто не выпустит трафик через второго ISP..	
Настроим разрешение для второго ISP	
Создание маршрутов для wan2	

Зайдите в меню *Routing→Routing Tables*. Создайте маршрут, введите данные для него:	
Interface	wan2
Network	wan2net
Metric	90
Во вкладке *Monitor* введите:	
Monitor This Route	Поставьте галочку
Monitor Interface Link Status	Поставьте галочку
Создайте второй маршрут, введите данные для него:	
Interface	wan2
Network	all-nets
Gateway	wan2_gw
Metric	100
Во вкладке *Monitor*:	
Monitor This Route	Поставьте галочку
Monitor Interface Link Status	Поставьте галочку
Monitor gateway Using ARP Lookup	Поставьте галочку
Настройка правил для группы ISP	
Перейдите в меню *Interfaces→Interface Groups*. Создайте Interface Group для wan, во вкладке *General*:	
Name	wans
Selected	Добавьте с помощью >> wan1 и wan2
Security/Transport Equivalent	Поставьте галочку
IP-правила межсетевого экрана	
Перейдите в меню *Rules→IP Rules→lan_to_wan1*. Измените в каждом из четырех правил интерфейс назначения с wan1 на wans:	
Destination Interface	Wans
Зайдите в *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/>set Interface Ethernet wan1 DHCPEnabled=No gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=192.168.60.5 gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=192.168.60.0/29 gw-world:/> set IP4Address InterfaceAddresses/wan1_gw Address=192.168.60.1 gw-world:/> set IP4Address InterfaceAddresses/wan1_dns1 Address=192.168.100.1 gw-world:/> set IP4Address InterfaceAddresses/wan2_ip Address=10.10.10.50 gw-world:/> set IP4Address InterfaceAddresses/wan2net Address=10.10.10.48/30 gw-world:/> set IP4Address InterfaceAddresses/wan2_gw Address=10.10.10.49 gw-world:/>set Interface Ethernet wan2 DefaultGateway=InterfaceAddresses/wan2_gw gw-world:/>set Interface Ethernet wan1 AutoDefaultGatewayRoute=No AutoInterfaceNetworkRoute=No gw-world:/>cc RoutingTable main gw-world:/main>add Route Interface=wan1 Network=InterfaceAddresses/wan1netMetric=90 RouteMonitor=Yes MonitorLinkStatus=Yes gw-world:/main> add Route Interface=wan1 Network=all-nets Metric=95 RouteMonitor=Yes MonitorLinkStatus=YesMonitorGateway=Yes gw-world:/main> add Route Interface=wan2 Network=InterfaceAddresses/wan2netMetric=90 RouteMonitor=Yes MonitorLinkStatus=Yes	

gw-world:/main> add Route Interface=wan2 Network=all-nets Metric=100 RouteMonitor=Yes MonitorLinkStatus=YesMonitorGateway=Yes gw-world:/main> cc gw-world:/>add Interface InterfaceGroup wans Members=wan1,wan2 Equivalent=Yes gw-world:/>set IPRule 2/1(drop_smb-all) DestinationInterface=wans gw-world:/> set IPRule 2/2(allow_ping-outbound) DestinationInterface=wans gw-world:/>set IPRule 2/3(allow_ftp-passthrough_av) DestinationInterface=wans gw-world:/>set IPRule 2/4(allow_standard) DestinationInterface=wans gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Упражнение	Проверьте работоспособность Failover. Физически отключите основной канал **wan1**, проверьте наличие переключения на резервный канал. У пользователей **lan**-сети должен снова появиться Интернет.
Internet Explorer MS Windows	http://yandex.ru

ЗАНЯТИЕ №12. Маршрутизация на основе политик (PBR). Использование PBR для направления различных типов трафика через разные ISP-подключения. Балансировка нагрузки (Route Load Balancing).

Межсетевые экраны D-Link позволяют настроить маршрутизацию на основе политик, заданных администратором сети. Механизм, обеспечивающий указанные возможности, называется PBR.

Цель	Эта лабораторная работа предназначена для ознакомления пользователей с настройкой PBR и Route Load Balancing на межсетевых экранах D-Link	
Оборудовани	DFL-860E	1
	Рабочая станция	2
	Ethernet-кабель (патч-корд)	4

Маршрутизация на основе политик (Policy Based Routing)	
Описание маршрутизации на основе политик	*Policy Based Routing (PBR) – дополнение к обычной маршрутизации, позволяющее администраторам более эффективно выполнять маршрутизацию на основе собственных политик. В PBR пакеты могут маршрутизироваться иначе, чем алгоритмы маршрутизации. Возможно более четко контролировать трафик с учетом различных критериев, таких как адреса источников и типы сервисов.* *Более того, применение PBR позволяет не только просматривать пакеты один за одним, но также использовать информацию о состоянияи соединения, таким образом контролировать оба направления продвижения пакетов.* *PBR:* *- Маршрутизация, чувствительная к источнику. При использовании подключений нескольких Интернет-провайдеров применение PBR обеспечивает маршрутизацию трафика, проходящего через межсетевой экран.* *- Маршрутизация на основе сервисов. Применение PBR обеспечивает маршрутизацию трафика различных протоколов через разные «прозрачные» прокси, например, Web-кэши и антивирусные сканеры.* *- Создание сети организации, независимой от Интернет-провайдера. Все пользователи имеют доступ к общей активной основной зоне (backbone), но могут пользоваться услугами различных Интернет-провайдеров в зависимости от потоковых медиаканалов.* *В межсетевом экране реализация PBR состоит из* *- одной или нескольких именованных PBR-таблиц (named PBR table) в дополнение к обычной таблице маршрутизации.* *- отдельного набора правил PBR, которые определяют какую именованную PBR-таблицу маршрутизации следует использовать.*

Таблицы маршрутизации на основе политик (Policy-based Routing Table)	*Таблицы маршрутизации на основе политик являются альтернативными таблицами в дополнение к главной таблице маршрутизации. Эта таблица содержит такие же поля для описания маршрутов, что и главная таблица маршрутизации, кроме параметра Ordering для каждого маршрута. Параметр Ordering определяет: когда PBR-таблица будет задействована межсетевым экраном при расчете маршрута – ранее или позже главной таблицы маршрутизации.*
Политика маршрутизации на основе политик (Policy-based Routing Policy)	*Правила, определенные в PBR-политике, представляют собой селекторы различных таблиц маршрутизации. Каждое PBR-правило срабатывает на поля типа службы, интерфейсов отправления и назначения, сети отправления и назначения. В процессе определения маршрута межсетевым экраном исполняется первое подходящее правило, и маршруты могут быть выбраны и приоритизированы исходя из параметра порядка маршрута на основе состояния, в отличии от условий определения маршрута по порядку пакетов (packet-by-packet). Таким образом, PBR-правило может определять таблицу маршрутизации для использования прямого и обратного направлений перенаправления пакетов (forward и return direction).*
Исполнение PBR на межсетевом экране	*Порядок исполнения PBR в кооперации с главной таблицей маршрутизации и настройками правил межсетевого экрана:* *1. Проверка главной таблицы маршрутизации – поиск по интерфейсам адресов назначения пакетов.* *2. Анализ правил – поиск по списку правил межсетевого экрана для определения действия при обработке пакета.* *3. Анализ PBR-политики – если поиск в пункте 2 привел к разрешению пересылки пакетов, то межсетевой экран выполнит поиск маршрута в PBR-правилах. Первое подошедшее правило будет использовано в маршрутизации. В соответствии со спецификациями в правиле будет выбрана соответствующая таблица маршрутизации. Если не найдено подходящего правила, то PBR-таблицы не используются и не будет выполнено PBR-преобразования. Межсетевой экран перенаправляет пакеты только в соответствии с главной таблицей маршрутизации.* *4. Преобразование адресов – если SAT-правило упоминается в построении правил пункта № 2, то будет выполнено преобразование адресов.* *5. Финальное определение маршрута и перенаправление пакетов – межсетевой экран определяет финальный маршрут в соответствии с пунктом № 3 и перенаправляет пакет.* *Решение об использовании конкретной таблицы маршрутизации принимается до проведения преобразования адресов.*
Описание сценария	*В этом сценарии создается PBR-таблица маршрутизации «TestPBRTable».*
Настройка DFL-860E	
Web-интерфейс	
Добавим PBR-таблицу маршрутизации. Зайдите в меню *Routing→Policy-based Routing Tables→Add→Policy-based Routing Table*. Во вкладке *General* введите:	
Name	TestPBRTable
Во вкладке *Ordering* введите:	

First	Именованная таблица маршрутизации строится первой из всех. Если этот поиск окончиться неудачей, то поиск будет продолжен в главной таблице маршрутизации.
Default	Главная таблица маршрутизации будет использована первой. Если единственным соответствием является маршрут по умолчанию 0.0.0.0/0, то будет использована именованная таблица маршрутизации. Если поиск маршрута в именованной таблице маршрутизации потерпит неудачу, то весь процесс поиска маршрута потерпит неудачу.
Only	Используется только именованная таблица маршрутизации. Если поиск маршрута будет неуспешный, то поиск в главной таблице маршрутизации производиться не будет.
Описание сценария	*В этом сценарии создается PBRмаршрут.*
Настройка DFL-860E	
Добавим PBR-маршрут. Зайдите в меню *Routing→Policy-based Routing Tables→TestPBRTable→ Add→Route*. Во вкладке *General* введите:	
Interface	Выберите интерфейс для маршрутизации.
Network	Выберите подсеть для маршрутизации.
Gateway	Выберите шлюз, на который будут отсылаться смаршрутизированные пакеты.
Local IP Address	Этот IP-адрес будет автоматически опубликован на отвечающем интерфейсе, кроме того, он будет использоваться в качестве адреса отправителя в ARP-записях. Если не указан конкретный IP-адрес, то будет использован IP-адрес интерфейса межсетевого экрана.
Metric	Выберите метрику маршрута (в основном для сценария Failover).
Направление различных типов трафика через разные ISP-подключения.	
Сценарий 1	
Описание сценария	*Зададим направление всего FTP-трафика через подключение второго провайдера, а в случае его недоступности – через первого. Все перенаправления осуществляет PBR, который направляет указанный трафик на альтернативную таблицу маршрутизации, где в отличие от основной таблицы маршрутизации основным подключением служит второй провайдер, а резервным – первый (см. схему 55).*
Настройка DFL-860E	
Web-интерфейс	
Создание альтернативной таблицы маршрутизации	
Перейдите в меню *Routing→Routing Tables*. Добавьте новую таблицу маршрутизации, укажите для неё параметры:	
Name	Alt
Ordering	Only (выберите из списка)
Создание основного и резервного маршрутов	
Зайдите в меню *Routing→Routing Tables*. Создайте основной маршрут, введите данные для него:	
Interface	wan2

Network	all-nets
Gateway	wan2_gw
Metric	90
Во вкладке *Monitor*:	
Monitor This Route	поставьте галочку
Monitor Interface Link Status	поставьте галочку
Monitor Gateway Using ARP Lookup	поставьте галочку
Зайдите в меню *Routing→Routing Tables*. Создайте резервный маршрут, введите данные для него:	
Interface	wan1
Network	all-nets
Gateway	wan1_gw
Metric	100
Во вкладке *Monitor*:	
Monitor This Route	поставьте галочку
Monitor Interface Link Status	поставьте галочку
Monitor Gateway Using ARP Lookup	поставьте галочку
Перенаправление трафика в созданную таблицу с помощью PBR	
Примечание: Основной принцип при применении PBR состоит в использовании правил маршрутизации (Routing Rule), в параметры которых включены: Address Filter, Service, Forward Table и Return Table.	
Создайте соответствующее правило для FTP-трафика.	
Зайдите в меню *Routing→Routing Rules→Add→Routing Rule*. Введите данные для него:	
Name	ftp_outbound
Forward Table	Alt
Return Table	main
Service	ftp-passthrough
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Примечание: Весь FTP-трафик перенаправляется через второго провайдера. В случае отказа второго провайдера будет задействован второй маршрут в альтернативной таблице, и FTP-трафик пойдет через первого провайдера. При необходимости можно маршрутизировать трафик только от некоторых внутренних пользователей, для этого необходимо изменить Source Network lannet на диапазон внутренних IP-адресов пользователей. Возможно также маршрутизировать FTP-трафик через второго провайдера, когда трафик идет только на определенный сервер, здесь вместо all-nets необходимо указать IP-адрес FTP-сервера.	
Командная строка (CLI)	
gw-world:/> add RoutingTable Alt Ordering=Only gw-world:/> cc RoutingTable Alt gw-world:/Alt>add Route Interface=wan2 Network=all-netsGateway=InterfaceAddresses/wan2_gw Metric=90 RouteMonitor=Yes MonitorLinkStatus=Yes	

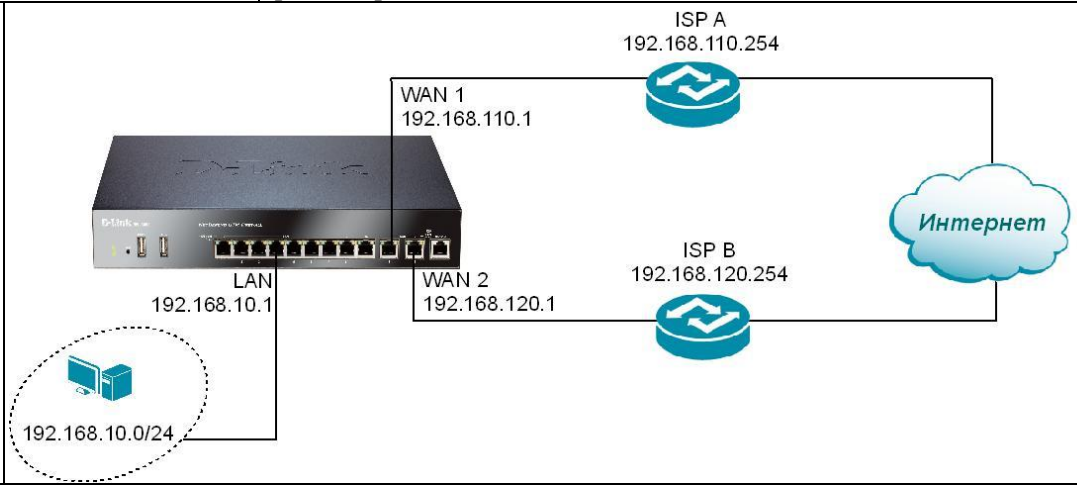
gw-world:/Alt> add Route Interface=wan1 Network=all-netsGateway=InterfaceAddresses/wan1_gw Metric=100 RouteMonitor=Yes MonitorLinkStatus=YesMonitorGateway=Yes
gw-world:/Alt> cc
gw-world:/>add RoutingRule ForwardRoutingTable=Alt ReturnRoutingTable=main Service=ftp-passthrough SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationNetwork=all-nets DestinationInterface=wan1 Name=ftp_outbound
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Упражнение	Проверьте работоспособность PBR. Физически отключите соединение первого Интернет-провайдера. Пользователям lan-сети все равно должен быть доступен ftp-трафик на внешние ресурсы через межсетевой экран.
Internet Explorer MS Windows	ftp://ftp.dlink.ru

Сценарий 2

Описание сценария	*В сценарии используются два провайдера Интернета ISP A и ISP B, подключенные соответственно к* ***wan1*** *и* ***wan2*** *интерфейсам межсетевого экрана. Необходимо сконфигурировать межсетевой экран для использования ISP A в качестве основного провайдера и ISP B в качестве резервного провайдера с соответствующей конфигурацией маршрутов.* *Необходимо настроить два маршрута – один маршрут по умолчанию 0.0.0.0/0 (default route) с метрикой 1, использующий шлюз по умолчанию провайдера ISP A, второй маршрут по умолчанию с метрикой 2, использующий шлюз по умолчанию провайдера ISP B.*

Схема 56



Настройка DFL-860E

Web-интерфейс

Создание необходимых объектов.
Создайте объекты в соответствии со схемой 56.

Убедимся в отсутствии автоматически добавленных маршрутов на интерфейсах wan1 и wan2. Зайдите в меню *Interfaces→Ethernet→wan1*. Во вкладке *Advanced* введите:

Add default route if default gateway is specified	Уберите галочку

Зайдите в меню *Interfaces→Ethernet→wan2*. Во вкладке *Advanced* введите:

Add default route if default gateway is specified	Уберите галочку

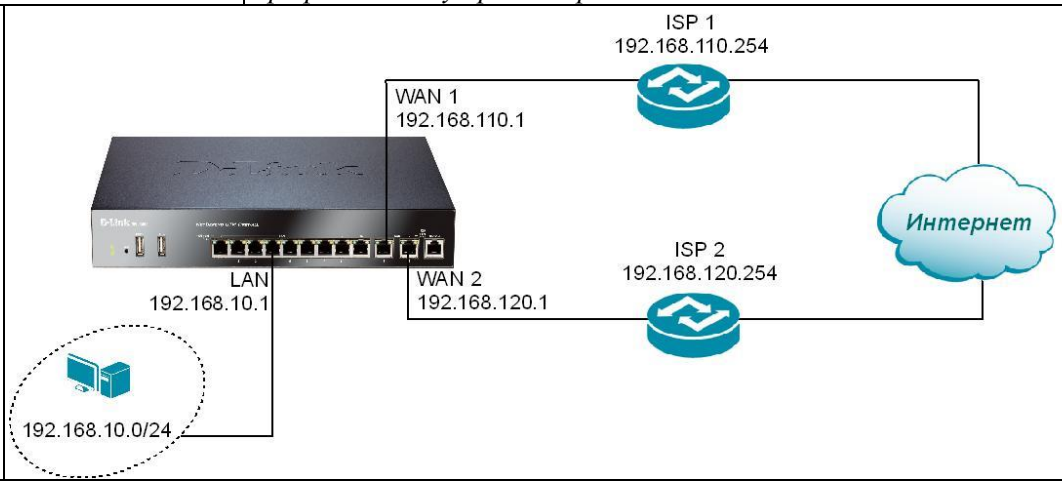
Добавим маршрут по умолчанию на интерфейс wan1. Зайдите в меню *Routers→ Routing*

Tables→main→Add→Route. Во вкладке *General* введите:	
Interface	wan1
Network	all-nets (0.0.0.0/0)
Gateway	Шлюз по умолчанию ISP A
Local IP Address	-
Metric	1
Во вкладке *Monitor* введите:	
Monitor This Route	Поставьте галочку
Monitor Interface Link Status	Поставьте галочку
Monitor Gateway Using ARP Lookup	Поставьте галочку
Примечание: Существует возможность вручную сконфигурировать интервал ARP-запросов, используемый при проверки отказа маршрута. Выбранное значение должно быть по крайней мере 100 мс. Если на одном интерфейсе мониторится несколько роутеров, может быть выбрано большее значение чтобы избежать «затопления» сети ARP-запросами.	
Добавим маршрут по умолчанию на интерфейс wan2. Зайдите в меню *Routers→ Routing Table →main→Add→Route.*Во вкладке *General* введите:	
Interface	wan2
Network	all-nets (0.0.0.0/0)
Gateway	Шлюз по умолчанию ISP B
Local IP Address	-
Metric	2
Создадим интерфейсную группу для возможности написать правила с интерфейсом назначения для любого маршрута. Интерфейсная группа позволит рассматривать интерфейсы эквивалентно в опциях Security/Transport Equivalent. Зайдите в меню *Interfaces→Interface Group→Add→Interface Group.* Во вкладке *General* введите:	
Name	route_inf_group
Security/Transport Equivalent	Поставьте галочку
Interfaces	Выберите wan1 и wan2.
Добавим IP Rule для группы интерфейсов. Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Введите параметры во вкладке *General*:	
Name	route_failover_wan1
Action	NAT
Service	http
Source Interface	lan
Source Network	lannet
Destination Interface	route_inf_group
Destination Network	all-nets
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Примечание: Маршрут по умолчанию для интерфейса wan2 не будет мониториться, т.к. нет резервного маршрута для интерфейса wan2.	
Командная строка (CLI)	
gw-world:/> set Interface Ethernet wan1 AutoDefaultGatewayRoute=No gw-world:/> set Interface Ethernet wan2 AutoDefaultGatewayRoute=No gw-world:/> cc RoutingTable main gw-world:/main> add Route Interface=wan1 Network=all-nets Metric=1 RouteMonitor=Yes MonitorLinkStatus=Yes MonitorGateway=Yes	

gw-world:/main> add Route Interface=wan2 Network=all-nets Metric=2 RouteMonitor=Yes MonitorLinkStatus=Yes MonitorGateway=Yes
gw-world:/main> cc
gw-world:/> add Interface InterfaceGroup route_inf_group Members=wan1,wan2 Equivalent=Yes
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=NAT Service=http SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=route_inf_group DestinationNetwork=all-nets Name=route_failover_wan1
gw-world:/1(labs)> cc
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Упражнение	Проверьте работоспособность PBR. Физически отключите соединение первого Интернет-провайдера. Пользователям lan-сети все равно должен быть доступен http-трафик на внешние ресурсы через межсетевой экран.
Internet Explorer MS Windows	http://yandex.ru

Route Load Balancing

Описание метода	*Механизм RLB (Route Load Balancing) позволяет осуществить балансировку нагрузки трафика между интерфейсами с привязкой к определенному Интернет-провайдеру по типу трафика, между множеством VPN-туннелей.* *Существует три алгоритма балансировки:* *- Round Robin* *Переключение между маршрутами происходит поочередно.* *- Destination* *Переключение между маршрутами происходит поочередно, но один и тот же IP-адрес назначения использует один и тот же маршрут.* *- Spillover* *Используется следующий маршрут при превышении лимита трафика за определенное время на текущем маршруте.*
Описание сценария	*Пользователи **lan**-сети имеют доступ в Интернет через межсетевой экран. Используются подключения двух Интернет-провайдеров. Необходимо осуществить балансировку нагрузки трафика между провайдерами.*
Схема 57	

Настройка DFL-860E

Web-интерфейс

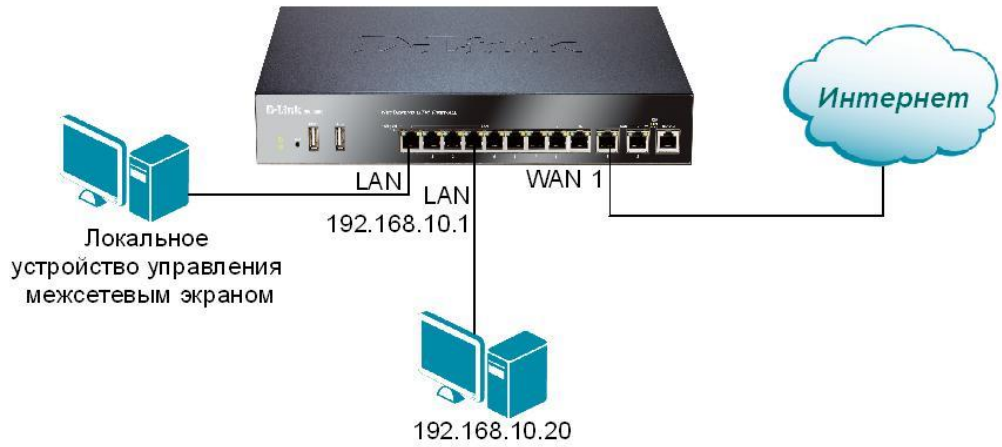
Создание необходимых объектов. Создайте объекты в соответствии со схемой 57.	
Добавим маршрут по умолчанию на интерфейс wan1. Зайдите в меню *Routers→ Routing Tables→ main→Add→Route.* Во вкладке *General* введите:	
Interface	wan1
Network	all-nets (0.0.0.0/0)
Gateway	Шлюз по умолчанию ISP 1
Local IP Address	-
Metric	100
Добавим маршрут по умолчанию на интерфейс wan2. Зайдите в меню *Routers→ Routing Tables→ main→Add→Route.* Во вкладке *General* введите:	
Interface	wan2
Network	all-nets (0.0.0.0/0)
Gateway	Шлюз по умолчанию ISP 2
Local IP Address	-
Metric	100
Добавим IP Rule для интерфейса wan1. Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Введите параметры во вкладке *General*:	
Name	rule_wan1
Action	NAT
Service	all-services
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets
Добавим IP Rule для интерфейса wan2. Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Введите параметры во вкладке *General*:	
Name	rule_wan2
Action	NAT
Service	all-services
Source Interface	lan
Source Network	lannet
Destination Interface	wan2
Destination Network	all-nets
Создадим RLB Instance. Зайдите в меню *Routing→Route Load Balancing→Add→Route Balancing Instance*. Введите параметры во вкладке *General*:	
Routing Table	Main
Algorithm	Destination
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> set Interface Ethernet wan1 AutoDefaultGatewayRoute=No gw-world:/> set Interface Ethernet wan2 AutoDefaultGatewayRoute=No gw-world:/> cc RoutingTable main gw-world:/main> add Route Interface=wan1 Network=all-nets Gateway=InterfaceAddresses/wan1_gwMetric=100 gw-world:/main> add Route Interface=wan2 Network=all-nets Gateway=InterfaceAddresses/wan2_gw	

Metric=100 gw-world:/main> cc gw-world:/>add RouteBalancingInstance main Algorithm=Destination gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=NAT Service=all-services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=wan1 DestinationNetwork=all-nets Name=rule_wan1 gw-world:/1(labs)> add IPRule Action=NAT Service=all-services SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=wan2 DestinationNetwork=all-nets Name=rule_wan2 gw-world:/1(labs)> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Упражнение	Проверьте работоспособность схемы. Запустите множество приложений для доступа в Интернет на компьютерах lan-сети. Проверьте работу RLB-трассировкой – при переключении маршрутов будут выдаваться разные результаты команды tracert.
CMD MS Windows	C:\>tracert yandex.ru

ЗАНЯТИЕ №13. Фильтрация URL. Установка HTTP ALG для Web URL фильтра. Запрет доступа на все сайты, кроме разрешенных. Фильтрация содержимого Web Content Filter.

Механизм HTTP ALG позволяет управлять доступом пользователей на различные сайты Интернета, блокировать определенные сайты, настраивать правила загрузки контента.

Цель	Эта лабораторная работа предназначена для понимания назначения HTTP ALG, настройки URL-фильтрации.	
Оборудование	DFL-860E	1
	Рабочая станция	2
	Ethernet-кабель (патч-корд)	3

Установка HTTP ALG для Web URL фильтра	*Этот сценарий показывает как межсетевой экран может управлять Internet Web-поиском для сетевых клиентов, а также запретить доступ на все сайты, кроме нескольких.*
Описание сценария	*1. Заблокируем Web-сайт http:/www.yandex.ru* *2. Разрешим посещение только http://news.yandex.ru* *3. Заблокируем все сайты, в URL которых встречается mail (т.е. все почтовые сервера с доступом по Web-интерфейсу)*
Схема 58	
Настройка DFL-860E	
Web-интерфейс	
Создание необходимых объектов. Создайте объекты в соответствии со схемой 58. Для wan1-интерфейса введите параметры, предоставленные Интернет-провайдером.	
Настройка ALG	
Зайдите в меню *Objects→ALG with AV/WCF*. Добавьте новый HTTP ALG, введите следующие параметры:	
Name	http_alg
Зайдите в *Objects→ALG→http_alg→URL Filter→Add→HTTP ALG URL*, введите следующие параметры:	
Action	Blacklist

URL	*.yandex.ru/*
Запретим посещение любых адресов, имеющих в URL слово mail (т.е. Интернет-почта). Добавьте в созданный HTTP ALG URL параметры:	
Action	Blacklist
URL	*mail*
Разрешим посещение http://news.yandex.ru. Добавьте в созданный HTTP ALG URL параметры:	
Action	Whitelist
URL	news.yandex.ru/*
Настройка TCP/UDP Service	
Добавим новый сервис *http-outbound* (если его нет в разделе Services), в котором используется созданный HTTP ALG. Зайдите в меню *Objects→Services→Add→TCP/UDP Service.* Во вкладке *General* введите следующие параметры:	
Name	http-outbound
Type	TCP
Source	0-65535
Destination	80
ALG	http_alg (выберите из списка)
Max Sessions	200
Настройка IP Rule	
Зайдите в меню *Rules→IP Rules*. Добавьте новое IP Rule, введите параметры во вкладке *General*:	
Name	http_ALG_rule
Action	NAT
Service	http-outbound
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets
Выставите приоритет правил: нажмите правой кнопкой мыши на http_ALG_rule и выберите *Move to top*.	
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Примечание: Приоритет белого листа выше, чем блок-листа. Это значит, сначала необходимо полностью заблокировать URL или Web-сайты, и только после этого разрешить некоторые разделы Web-сайта. В данном сценарии, если установлено действие Action: blockURL: news.yandex.ru/*, и Action: whitelistURL: *.yandex.ru/*, то межсетевой экран не сможет заблокировать news.yandex.ru/*, пока другое правило разрешает сначала весь Web-сайт *yandex.ru/*.	
<u>Командная строка (CLI)</u>	
gw-world:/>add ALG ALG_HTTP http_alg gw-world:/> add Service ServiceTCPUDP http-outbound DestinationPorts=80 SourcePorts=0-65535 Type=TCP ALG=http_alg MaxSessions=200 gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=NAT Service=http-outbound SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=wan1 DestinationNetwork=all-nets Name=http_ALG_rule gw-world:/1(labs)> cc gw-world:/> activate *(подождать 3-5 секунд)*	

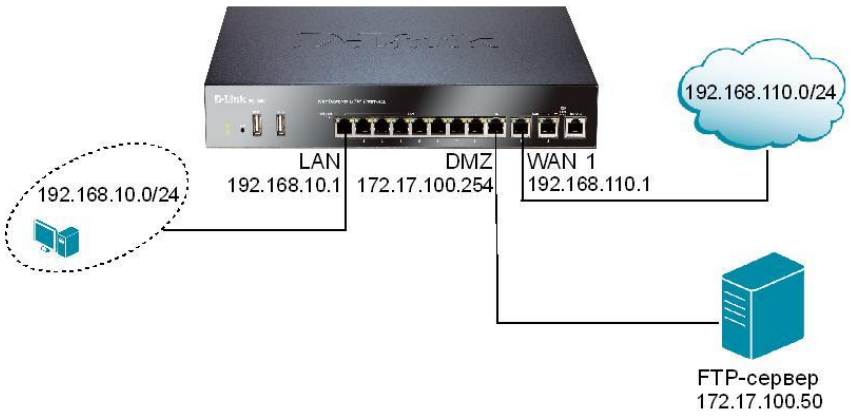
gw-world:/>commit	
Упражнение	Проверьте работоспособность HTTP ALG. С компьютера lan-сети попробуйте зайти на заблокированные сайты и на new.yandex.ru.
Internet ExplorerOC Windows	http://mail.ru http://yandex.ru http://new.yandex.ru
Web Content Filter	
Описание сценария	*Заблокируем пользователям **lan**-сети доступ к сайтам нежелательного содержания.*
Настройка DFL-860E	
Web-интерфейс	
Настройка ALG	
Зайдите в меню *Objects→ALG with AV/WCF*. Добавьте новый HTTP ALG, введите следующие параметры:	
Name	http_alg
Зайдите в меню *Objects→ALG→http_alg* , введите во вкладке *Web Content Filtering* следующие параметры:	
Mode	Enabled
Переместите *Adult content* из списка *Allowed* в список *Blocked*.	
Добавим новый сервис *http-outbound* (если его нет в *Services*), в котором используется созданный HTTP ALG. Зайдите в меню *Objects→Services→Add→TCP/UDP Service.* Во вкладке *General* введите следующие параметры:	
Name	http-outbound
Type	TCP
Source	0-65535
Destination	80
ALG	http_alg (выберите из списка)
Max Sessions	200
Настройка IP Rule	
Зайдите в меню *Rules→IP Rules*. Добавьте новое IP Rule, введите параметры во вкладке *General*:	
Name	http_ALG_rule
Action	NAT
Service	http-outbound
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> add ALG ALG_HTTP http_alg WebContentFilteringMode=Enabled FilteringCategories=ADULT_CONTENT gw-world:/> add Service ServiceTCPUDP http-outbound DestinationPorts=80 SourcePorts=0-65535 Type=TCP ALG=http_alg MaxSessions=200	

gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=NAT Service=http-outbound SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=wan1 DestinationNetwork=all-nets Name=http_ALG_rule gw-world:/1(labs)> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Упражнение	Проверьте работоспособность Web Content Filter. С компьютера **lan-**сети попробуйте зайти на заблокированные сайты.
Internet Explorer ОС Windows	http://porno.com

ЗАНЯТИЕ №14. FTP ALG. TFTP ALG. Защита FTP-сервера с помощью FTP ALG.

Механизм FTP ALG на межсетевых экранах D-Link позволяет настроить защиту FTP-серверов и FTP-клиентов.

Цель	Эта лабораторная работа предназначена для ознакомления пользователей с настройкой функций FTP ALG, TFTP ALG.	
Оборудование	DFL-860E	1
	Рабочая станция	2
	Ethernet-кабель (патч-корд)	3

Защита FTP-сервера с помощью FTP ALG	
Описание сценария	*1. Защитим FTP-сервер, подключенный к DMZ-интерфейсу межсетевого экрана с помощью FTP ALG.* *2. Защитим FTP-клиентов, выходящих через межсетевой экран на сервер FTP, расположенный в Интернете.* *3. В целях повышенной информационной безопасности запретим скачивание файлов **.exe** с FTP-сервера.*
Схема 59	
Настройка DFL-860E	
Web-интерфейс	
Создание необходимых объектов	
Создадим объект «IP-адрес FTP-сервера». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	ftp-internal
Address	172.17.100.50
Настройка ALG	
Зайдите в меню *Objects→ALG*. Добавьте новый FTP ALG.	
Name	ftp_alg
Allow client touse active mode	Поставьте галочку
Allow server to use passive mode	Уберите галочку
Во вкладке *File Integrity* введите:	

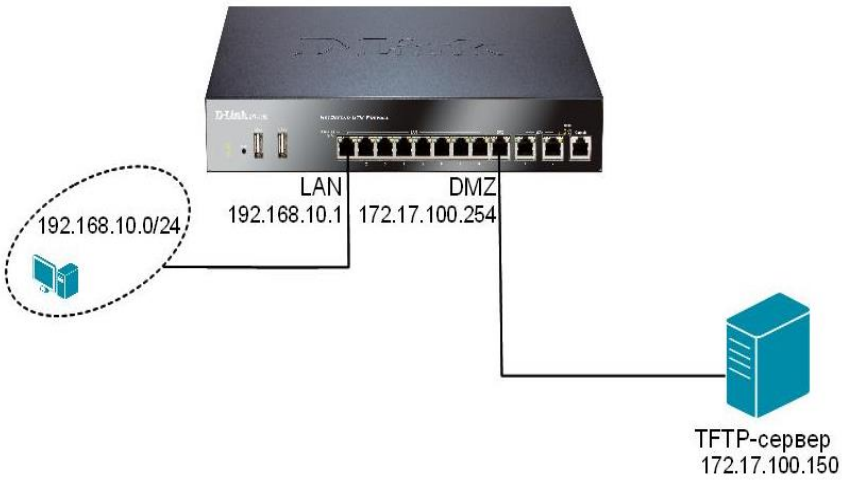
Verify MIME-type against file content.	Поставьте галочку
Block selected file types	Добавьте расширение **.exe** из списка
Создание FTP-сервиса	
Создадим сервис ftp-inbound (если его нет в *Services*). Зайдите в меню *Objects→Services*, добавьте TCP/UDP Service со следующими параметрами:	
Name	ftp-inbound
Type	TCP (выберите из списка)
Destination	21 (порт FTP-сервера)
ALG	ftp_alg (выберите из списка ранее созданный ALG)
Настройка IP Rule	
Зайдите в меню *Rules→IP Rules*. Добавьте новое IP Rule для SAT, введите параметры во вкладке *General*:	
Name	SAT-ftp-inbound
Action	SAT
Service	ftp-inbound
Source Interface	wan1
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip (настраиваем для внешнего интерфейса)
Введите параметры во вкладке *SAT*:	
Translate the	Destination IP Address
To New IP Address	ftp-internal (внутренний IP адрес FTP-сервера)
Зайдите в меню *Rules→IP Rules*. Добавьте новое IP Rule, введите параметры во вкладке *General*:	
Name	NAT-ftp
Action	NAT
Service	ftp-inbound
Source Interface	lan
Source Network	lannet
Destination Interface	dmz
Destination Network	ftp-internal
Вкладка *NAT*:	
Use Interface Address	поставьте галочку
Зайдите в меню *Rules→IP Rules*. Добавьте новое второе IP Rule для SAT, введите параметры во вкладке *General*:	
Name	Allow-ftp
Action	Allow
Service	ftp-inbound
Source Interface	wan1
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip
Зайдите в меню *Configuration* и выберите *Save and Activate*.	

Командная строка (CLI)

gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address ftp-internal Address=172.17.100.50
gw-world:/labs> cc
gw-world:/>add ALG ALG_FTP ftp_alg AllowClientActive=Yes AllowServerPassive=No VerifyContentMimetype=Yes File exe
gw-world:/> add Service ServiceTCPUDP ftp-inbound DestinationPorts=21 SourcePorts=0-65535 Type=TCP ALG=ftp_alg
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=SAT Service=ftp-inbound SourceInterface=wan1 SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip SATTranslateToIP=labs/ftp-internal SATTranslate DestinationIP Name=SAT-ftp-inbound
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip Service=ftp-inbound SourceInterface=wan1 SourceNetwork=all-nets Name=Allow-ftp
gw-world:/1(labs)> add IPRule Action=NAT DestinationInterface=dmz DestinationNetwork=labs/ftp-internal Service=ftp-inbound SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Name=NAT-ftp
gw-world:/1(labs)> cc
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Упражнение	Проверьте работоспособность FTP-сервера. Зайдите на сервер с компьютера, подключенного к **lan**-интерфейсу межсетевого экрана и с компьютера за **wan1**-интерфейсом межсетевого экрана.
Internet Explorer ОС Windows (компьютер в сети lannet)	ftp://<ftp-internal>
Internet Explorer ОС Windows (компьютер в сети wan1net)	ftp://<wan1_ip>

Защита TFTP-сервера с помощью TFTP ALG

Описание сценария	*Защитим TFTP-сервер, подключенный к DMZ-интерфейсу. Запретим пользователям запись данных на него и ограничим размер передаваемых файлов – 120 Кбайт.*
Схема 60	

Настройка DFL-860E

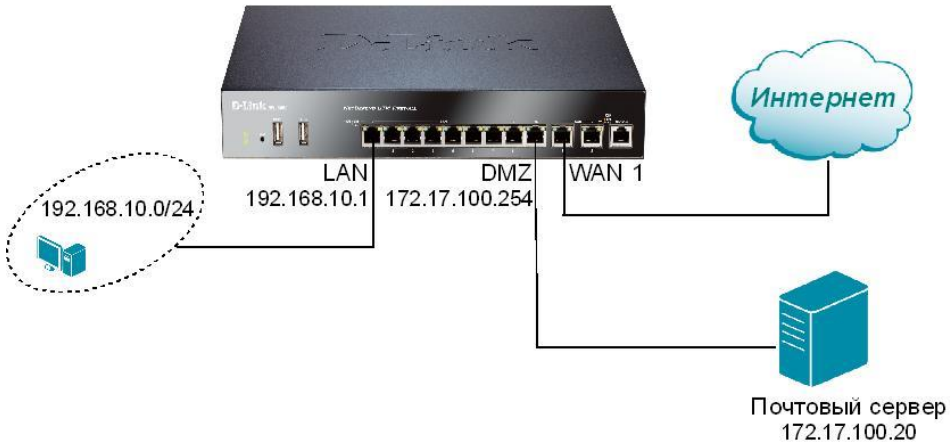
Web-интерфейс

Создание необходимых объектов	
Создадим объект «IP-адрес FTP-сервера». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	tftp-ip
Address	172.17.100.150
Настройка ALG	
Зайдите в меню *Objects→ALG→Add→TFTP ALG*. Введите следующие параметры:	
Name	tftp_alg
Allow only read	Выберите из списка.
Max file transfer size	120
Создание TFTP сервиса	
Зайдите в меню *Objects→Services*, добавьте TCP/UDP Service со следующими параметрами:	
Name	tftp-srv
Type	UDP (выберите из списка)
Destination	69
ALG	tftp_alg (выберите из списка ранее созданный ALG)
Настройка IP Rule	
Зайдите в меню *Rules→IP Rules*. Добавьте новое IP Rule, введите параметры во вкладке *General*:	
Name	NAT-tftp
Action	NAT
Service	tftp-srv
Source Interface	lan
Source Network	lannet
Destination Interface	dmz
Destination Network	tftp-ip
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address tftp-ip Address=172.17.100.150 gw-world:/labs> cc gw-world:/>add ALG ALG_TFTP tftp_alg AllowedCommands=ReadOnly MaxFileTransferSize=120 gw-world:/> add Service ServiceTCPUDP tftp-srv DestinationPorts=66 SourcePorts=0-65535 Type=UDP ALG=tftp_alg gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=NAT DestinationInterface=dmz DestinationNetwork=labs/tftp-ip Service=tftp-srv SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Name=NAT-tftp gw-world:/1(labs)> cc gw-world:/> activate gw-world:/>commit	
Упражнение	Проверьте работоспособность TFTP-сервера с заданными ALG-ограничениями. Зайдите на сервер с компьютера, подключенного к **lan-**сети межсетевого экрана.
TFTP client	tftp://<tftp-ip>

ЗАНЯТИЕ №15. Защита почтового сервера и почтовых клиентов с помощью SMTP ALG, POP3 ALG. Антиспам-фильтр.

Межсетевой экран позволяет защитить почтовые сервера и почтовых клиентов от спама и вредоносных действий, а также заблокировать отдельных почтовые домены.

Цель	Эта лабораторная работа предназначена для ознакомления пользователей с настройкой защиты почтовых серверов и почтовых клиентов с помощью межсетевых экранов.	
Оборудование	DFL-860E	1
	Рабочая станция	2
	Ethernet-кабель (патч-корд)	3

Защита почты с помощью SMTP ALG, черные/белые списки почтовых доменов.	
Описание сценария	*Необходимо заблокировать почтовые домены mail.ru, yandex.ru, google.ru для почтовых клиентов **lan**-сети. Отдельно необходимо заблокировать почтовый ящик baduser на любом почтовом домене .ru. Почтовый сервер располагается в **dmz**-зоне.*
Схема 61	
Настройка DFL-860E	
Web-интерфейс	
Создание необходимых объектов. Создайте объекты в соответствии со схемой 61. Для wan1-интерфейса введите параметры, предоставленные Интернет-провайдером.	
Создадим объект «IP-адрес почтового сервера в dmz-зоне». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	email_server
Address	172.17.100.20
Настройка ALG	
Создайте SMTP ALG. Зайдите в меню *Objects→ALG→Add→SMTP ALG*. Введите следующие параметры на вкладке *General*:	
Name	smtp_alg
Во вкладке *Whitelist/Black list* добавьте новый *Email Sender/Recipient*, введите следующие параметры:	

Sender/Recipient to classify	Sender
Classify the email address	Blacklist
Email	*@mail.ru
Во вкладке *Whitelist/Black list* добавьте новый *Email Sender/Recipient*, введите следующие параметры:	
Sender/Recipient to classify	Sender
Classify the email address	Blacklist
Email	*@yandex.ru
Во вкладке *Whitelist/Black list* добавьте новый *Email Sender/Recipient*, введите следующие параметры:	
Sender/Recipient to classify	Sender
Classify the email address	Blacklist
Email	*@google.ru
Во вкладке *Whitelist/Black list* добавьте новый *Email Sender/Recipient*, введите следующие параметры:	
Sender/Recipient to classify	Sender
Classify the email address	Blacklist
Email	baduser@*.ru
Создайте POP3 ALG. Зайдите в меню *Objects→ALG→Add→POP3 ALG*. Введите следующие параметры во вкладке *General*:	
Name	pop3_alg
Block clients from sending USER and PASS command	Поставьте галочку
Allow unknown commands	Уберите галочку
Создание SMTP-сервиса	
Создадим сервис smtp-inbound (если его нет в разделе *Service*). Зайдите в меню *Objects→Services*, добавьте TCP/UDP Service со следующими параметрами:	
Name	smtp-inbound
Type	TCP (выберите из списка)
Destination	25
ALG	smtp_alg (выберите из списка ранее созданный ALG)
Создание POP3-сервиса	
Зайдите в меню *Objects→Services*, добавьте TCP/UDP Service со следующими параметрами:	
Name	pop3
Type	TCP (выберите из списка)
Destination	110
ALG	pop3_alg (выберите из списка ранее созданный ALG)
Настройка IP Rule	
Зайдите в меню *Rules→IP Rules*. Добавьте новое IP Rule для SAT, введите параметры во вкладке *General*:	
Name	SAT-smtp
Action	SAT
Service	smtp-inbound
Source Interface	wan1
Source Network	all-nets

Destination Interface	core
Destination Network	wan1_ip (настраиваем для внешнего интерфейса)
Введите параметры во вкладке *SAT*:	
Translate the	Destination IP Address
To New IP Address	email_server (внутренний IP-адрес почтового сервера)
Зайдите в меню *Rules→IP Rules*. Добавьте новое второе IP Rule для SAT, введите параметры во вкладке *General*:	
Name	Allow-smtp
Action	Allow
Service	smtp-inbound
Source Interface	wan1
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip
Зайдите в меню *Rules→IP Rules*. Добавьте новое IP Rule, введите параметры во вкладке *General*:	
Name	NAT-pop3
Action	NAT
Service	pop3
Source Interface	lan
Source Network	lannet
Destination Interface	dmz
Destination Network	email_server
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address email_server Address=172.17.100.20 gw-world:/labs> cc gw-world:/>add ALG ALG_SMTP smtp_alg VerifySenderEmail=Yes VerifySenderEmailAction=Deny VerifySenderEmailDomainOnly=Yes gw-world:/>add ALG ALG_POP3 pop3_alg BlockUserPass=Yes AllowUnknownCommands=No gw-world:/> add Service ServiceTCPUDP smtp-inbound DestinationPorts=25 SourcePorts=0-65535 Type=TCP ALG=smtp_alg gw-world:/> add Service ServiceTCPUDP pop3 DestinationPorts=110 SourcePorts=0-65535 Type=TCP ALG=pop3_alg gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=SAT Service=smtp-inbound SourceInterface=wan1 SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip SATTranslateToIP=labs/email_server SATTranslate DestinationIP Name=SAT-smtp gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip Service=smtp-inbound SourceInterface=wan1 SourceNetwork=all-nets Name=Allow-smtp gw-world:/1(labs)> add IPRule Action=NAT DestinationInterface=dmz DestinationNetwork=labs/email_server Service=pop3 SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Name=NAT-pop3 gw-world:/1(labs)> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	

Упражнение	Отправьте почтовому клиенту, защищенному межсетевым экраном, письмо с заблокированных почтовых доменов и с незаблокированных почтовых доменов, а также от имени baduser.
Outlook Express	Отправить письмо с почтовых ящиков: baduser@ya.ru ksuser@mail.ru ksuser@yandex.ru ksuser@google.ru ksuser@jmail.com.
DNSBL SPAM фильтрация	
Описание сценария	*Нежелательная почта (SPAM) – на сегодняшний день серьёзная проблема организации почтовой инфраструктуры. Кроме большого объема писем с излишней информацией, многие сообщения могут содержать вирусы и вредоносные программы. Межсетевой экран позволяет настроить фильтрацию почтового трафика. Фильтр позволяет отбросить потенциальное SPAM-сообщение или пометить его как нежелательное (SPAM-флаг).*
Настройка DFL-860E	
Web-интерфейс	
Проверка входящих потовых сообщений на спам.	
Добавим новый SMTP ALG. Зайдите в меню *Objects→ALG→Add→SMTP ALG.* Во вкладке *General* введите следующие параметры:	
Name	SMTP-inbound
Email Rate	200
Email Size	5120
Fail Mode	Deny
Во вкладке *Anti-spam*:	
Check emails for mismatching SMTP command "From" address and email header "From" address.	Поставьте галочку и выберите *...and block them*.
DNSBL Anti-Spam Filter	Поставьте галочку напротив *Enable*.
Spam Threshold	3
Drop Threshold	5
Spam Tag	*** SPAM ***
Cache Size	0
Cache Timeout	600
Для *DNS Blacklists* введите спам-сервера и значения веса для них, после ввода нажимая *Add*:	
sbl.spamhaus.org	Weight Value 1
virbl.dnsbl.bit.nl	Weight Value 1
bl.spamcop.netorg	Weight Value 1
list.dsbl.org	Weight Value 1
zen.spamhaus.org	Weight Value 1
Примечание: Значение Weight Value сохраняется в памяти, после просчета всех «черных списков» значения суммируются. Если общее значение будет больше или равно Spam	

Threshold и DropThreshold, то письмо будет помечено как спам (SPAM***)или отброшено ALG.***

Пример расчета спама по значениям Weightvalue:

1) Если каждый сервер рассматривает отправителя спамером (1, 1, 1), результат будет 1*1+2*1+2*1=5. Таким образом, сообщение будет отброшено.

2) Допустим сервер SpamHaus считает сообщение спамом (0, 1, 0). Результат: 1*0+2*1+1*0=2. С сообщением ничего не будет сделано, т.к. пороговые значения не достигнуты.

3) Сервера SpamHaus и Sorbs считают сообщение спамом (0, 1, 1). Сумма будет следующая – 1*0+2*1+2*1=4. Сообщение будет помечено как спам-сообщение (квота письма изменена на квоту спам письма), но получатель его получит, т.к. порог drop threshold не достигнут.

Веса серверов могут быть назначены разные, в зависимости от степени доверия,

Более подробную информацию по DNSBL-серверам можно получить в Интернете: http://spamlinks.net/filter-dnsbl-lists.htm.

Настройка IP Rule

Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:

Name	email_spam
Action	SAT
Service	smtp-inbound (содержит SMTP ALG)
Source Interface	wan1
Destination Interface	core
Source Network	all-nets
Destination Network	wan1_ip

Введите параметры во вкладке *SAT*:

Translate the	Destination IP Address
To New IP Address	email_server

Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:

Name	email_spam2
Action	Allow
Service	smtp-inbound
Source Interface	wan1
Destination Interface	core
Source Network	all-nets
Destination Network	wan1_ip

Зайдите в меню *Configuration* и выберите *Save and Activate*.

Командная строка (CLI)

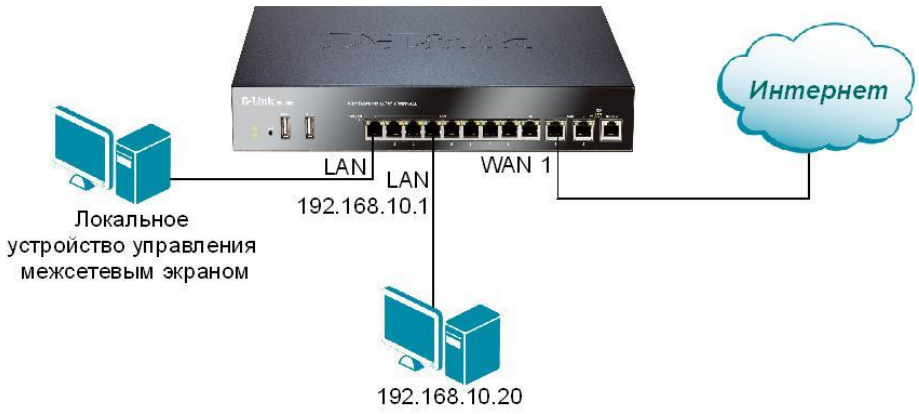
```
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address email_server Address=172.17.100.20
gw-world:/labs> cc
gw-world:/>add ALG ALG_SMTP smtp_alg DNSBL=Yes
gw-world:/> add Service ServiceTCPUDP smtp-inbound DestinationPorts=25 SourcePorts=0-65535 Type=TCP ALG=smtp_alg
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=SAT Service=smtp-inbound SourceInterface=wan1 SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip SATTranslateToIP=labs/email_server SATTranslate DestinationIP Name=email_spam
```

gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip Service=smtp-inbound SourceInterface=wan1 SourceNetwork=all-nets Name=email_spam2 gw-world:/1(labs)> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Упражнение	Проверьте работу фильтра антиспам. Спам-сообщения должны помечаться -SPAM- и занимать меньший объем.

ЗАНЯТИЕ №16. Антивирус. Обновление, использование.

Межсетевые экраны D-Link поддерживают антивирусное программное обеспечение на базе антивируса Касперского. Антивирус может быть использован при защите приложений с помощью ALG.

Цель	Эта лабораторная работа предназначена для ознакомления пользователей с настройкой антивируса на межсетевых экранах	
Оборудование	DFL-860E	1
	Рабочая станция	2
	Ethernet-кабель (патч-корд)	2

Активация антивирусной службы (AV) на межсетевом экране	
Схема 62	
Описание	*Существует пробная версия лицензии AV на 90 дней для тестирования на межсетевом экране. Для дальнейшего использования лицензию на антивирусную службу необходимо приобрести отдельно.* *Далее нужно активировать эту опцию на устройстве.*
Настройка DFL-860E	
Web-интерфейс	
Зайдите в меню *Maintenance→License*. Введите серийный номер Вашей антивирусной службы и нажмите *Activate*.	
Примечание: Устройство должно иметь доступ в Интернет для связи с сайтом D-Link **http://security.dlink.com.tw/.**	
Обновление антивирусной службы на межсетевом экране	
Настройка DFL-860E	
Web-интерфейс	
Зайдите в меню *Maintenance→Update Center*. Отметьте *Enable* для антивирусной службы. Во вкладке *Update Interval* выберите желаемое время обновления (обычно нерабочие часы предприятия), нажмите *Update.*	
Примечание: Устройство должно иметь доступ в Интернет для связи с сайтом D-Link **http://security.dlink.com.tw/.**	
Использование антивирусной службы на межсетевом экране	

Описание сценария	*Необходимо защитить HTTP-трафик, FTP-трафик и почтовый трафик от вирусов.*
Настройка DFL-860E	
Web-интерфейс	
Настройка HTTP ALG	
Зайдите в меню *Objects→ALG with AV/WCF*. Добавьте новый HTTP ALG.	
Во вкладке *General* введите следующие параметры:	
Name	http_alg
Во вкладке *Anti-Virus* введите следующие параметры:	
Mode	Protect
Block Range	lannet
Настройка FTP ALG	
Зайдите в меню *Objects→ALG with AV/WCF*. Добавьте новый FTP ALG.	
Во вкладке *General* введите следующие параметры:	
Name	ftp_alg
Во вкладке *Anti-Virus* введите следующие параметры:	
Mode	Protect
Block Range	lannet
Настройка POP3 ALG	
Зайдите в меню *Objects→ALG with AV/WCF*. Добавьте новый POP3 ALG.	
Во вкладке *General* введите следующие параметры:	
Name	pop3_alg
Во вкладке *Anti-Virus* введите следующие параметры:	
Mode	Protect
Block Range	lannet
Настройка SMTP ALG	
Зайдите в меню *Objects→ALG with AV/WCF*. Добавьте новый SMTP ALG.	
Во вкладке *General* введите следующие параметры:	
Name	smtp_alg
Во вкладке *Anti-Virus* введите следующие параметры:	
Mode	Protect
Block Range	lannet
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Примечание: 1. Опция Scan exclusion control позволяет исключить из сканирования антивирусом некоторые файлы. ***2. Все созданные ALG необходимо привязать к соответствующим службам.***	
Командная строка (CLI)	
gw-world:/>set UpdateCenter AVEnabled=Yes UpdateInterval=Daily UpdateHour=0 UpdateMinute=0 gw-world:/>updatecenter -update antivirus gw-world:/>add ALG ALG_HTTP http_alg Antivirus=Protect	

gw-world:/> add ALG ALG_FTP ftp_alg Antivirus=Protect gw-world:/> add ALG ALG_POP3 pop3_alg Antivirus=Protect gw-world:/> add ALG ALG_SMTP smtp_alg Antivirus=Protect gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Упражнение	Проверьте работоспособность антивируса. Зайдите в Интернет-сети на сайты с вирусами, попробуйте их скачать на компьютер **lan-**сети, затем – выложить файлы вирусов на FTP-сервер и передать вирусы по почте. Зайдите в меню *Status→Anti-Virus*, просмотрите лог-события антивирусной службы межсетевого экрана.

ЗАНЯТИЕ №17. Организация VoIP-телефонии на основе H.323 ALG и SIP ALG.

Механизмы H.323 ALG и SIP ALG позволяют организовать передачу VoIP-трафика (Voice over IP).

Цель	Эта лабораторная работа позволяет пользователям изучить способы организации VoIP-телефонии с помощью H.323 ALG и SIP ALG.	
Оборудование	DFL-860E	3
	Рабочая станция	3
	VoIP-телефон	4
	Ethetnet-кабель (патч-корд)	13

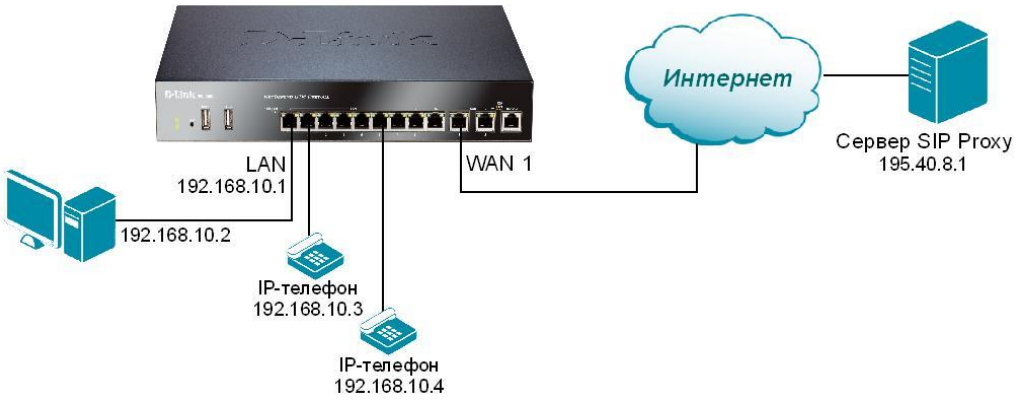
Передача трафика по протоколу SIP	
Описание сценария	*Обеспечим передачу VoIP-трафика, передаваемого между VoIP-терминалами и VoIP-прокси серверами.*
Настройка DFL-860E	
Web-интерфейс	
Настройка ALG	
Зайдите в меню *Objects→ALG*. Добавьте новый SIP ALG.	
Name	SIP-ALG
Max Sessions per ID	2 (только 2 одновременные сессии разрешено, по умолчанию – 5)
Max Registration Time	1200 (по умолчанию 3600 секунд)
SIP Signal Timeout	60 (по умолчанию 43200 секунд)
Data Channel Timeout	100 (по умолчанию 120 секунд)
Allow clients to exchange media directly when possible.	Уберите галочку
Примечание: Allow clients to exchange media directly when possible разрешает трафик по протоколу RTP/RTCP напрямую между клиентами без межсетевого экрана, клиенты должны быть на одном интерфейсе и в одной подсети. Разрешение этой опции позволяет сократить время на обработку данных и улучшить качество голосового сигнала, но означает отсутствие защиты трафика со стороны межсетевого экрана.	
Настройка TCP/UDP Service	
Зайдите в меню *Objects→Services*. Создайте новую службу TCP/UDP Service, введите следующие параметры:	
Name	SIP-service
Type	UDP (выберите из списка)
Source	0-65535
Destination	5060 (порт сигнализации SIP по умолчанию)
ALG	SIP-ALG (выберите из списка ранее созданный объект)
Командная строка (CLI)	
gw-world:/>add ALG ALG_SIP SIP-ALG MaxSessionsPerId=2 MaxRegistrationTime=1200 SipSignalTmout=60 DataChannelTmout=100 AllowMediaByPass=No gw-world:/> add Service ServiceTCPUDP SIP-service DestinationPorts=5060 SourcePorts=0-65535	

Type=UDP ALG=SIP-ALG
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Организация VoIP-сети, если клиенты находятся в локальной сети, а сервер SIP Proxy расположен в Интернет-сети

Описание сценария	*Обеспечим передачу VoIP-трафика, если Voip-сеть размещена за межсетевым экраном с NAT. Сервер SIP Proxy размещается в Интернет-сети.*

Схема 63



Настройка DFL-860E

Web-интерфейс

Предполагается, что IP-телефоны настроены в соответствии с параметрами, позволяющими выполнять внутренние и внешние звонки.
Настройте wan1-интерфейс в соответствии с параметрами, заданными Интернет-провайдером.

Создадим объект «IP-адрес сервера SIP Proxy». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:

Name	ip_proxy
Address	195.40.8.1

Настройка IP Rule

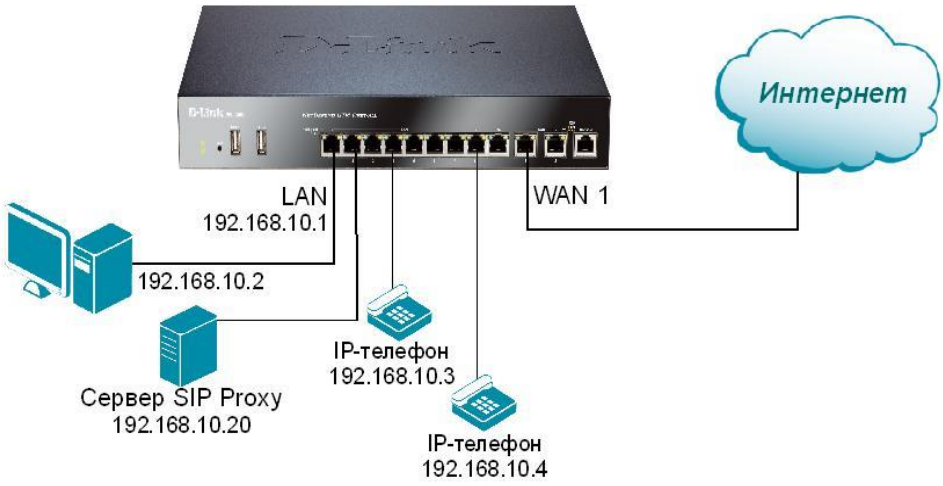
Зайдите в меню *Rules→IP Rules*. Добавьте новое правило IP Rule для SIP, введите параметры во вкладке *General*:

Name	SIP-outbound
Action	NAT
Service	SIP-service
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	ip_proxy

Зайдите в меню *Rules→IP Rules*. Добавьте новое правило IP Rule для SIP, введите параметры во вкладке *General*:

Name	SIP-inbound
Action	Allow
Service	SIP-service
Source Interface	wan1
Source Network	ip_proxy

Destination Interface	core
Destination Network	wan1_ip (настраиваем для внешнего IP-адреса межсетевого экрана)
Измените параметр UDP Life Time и отметьте UDP Bidirectional keep-alive. Зайдите в меню *System→Advanced Setting→ Conn. Timeout Settings,* во вкладке *General* введите:	
TCP SYN Idle Lifetime	60
TCP Idle Lifetime	262144
TCP FIN Idle Lifetime	80
UDP Idle Lifetime	3600
UDP Bidirectional keep-alive	Поставьте галочку
Ping Idle Lifetime	8
IGMP Idle Lifetime	12
Other Protcols Idle Lifetime	130
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Примечание: 1. NAT Traversal не настраивается на строне VoIP-терминалов и SIP Proxy, т.к. SIP ALG берет функцию преобразования адресов на себя. Также нет необходимости использовать технологию STUN. ***2. Правило SAT для трафика от прокси не требуется, т.к. межсетевой экран будет автоматически перенаправлять SIP-запросы конткретному внешнему пользователю.***	
Командная строка (CLI)	
gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address ip_proxy Address=195.40.8.1 gw-world:/labs> cc gw-world:/> add ALG ALG_SIP SIP-ALG MaxSessionsPerId=2 MaxRegistrationTime=1200 SipSignalTmout=60 DataChannelTmout=100 AllowMediaByPass=No gw-world:/> add Service ServiceTCPUDP SIP-service DestinationPorts=5060 SourcePorts=0-65535 Type=UDP ALG=SIP-ALG gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=NAT DestinationInterface=wan1 DestinationNetwork=labs/ip_proxy Service=SIP-service SourceInterface=lan SourceNetwork=InterfaceAddresses/lannetName=SIP-outbound gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ipService=SIP-service SourceInterface=wan1 SourceNetwork=labs/ip_proxy Name=SIP-inbound gw-world:/> set Settings ConnTimeoutSettings ConnLife_UDP=3600 gw-world:/> set Settings ConnTimeoutSettings AllowBothSidesToKeepConnAlive_UDP=yes gw-world:/1(labs)> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Упражнение	Проверьте работосопособность VoIP-сети, сделайте пробные звонки на внутренние телефоны и на внешние телефоны.
Организация VoIP-сети, если клиенты и сервер SIP Proxy расположены в локальной сети	
Описание сценария	*Обеспечим передачу VoIP-трафика, Voip-сеть размещена за межсетевым экраном с NAT. Сервер SIP Proxy размещается также в локальной сети* ***lan.***

Схема 64	

Настройка DFL-860E

Web-интерфейс

Создадим объект «IP-адрес сервера SIP Proxy». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:

Name	ip_proxy_lan
Address	192.168.10.20

Настройка IP Rule

Зайдите в меню *Rules→IP Rules*. Добавьте новое правило IP Rule для SIP, введите параметры во вкладке *General*:

Name	SIP-outbound
Action	NAT
Service	SIP-service
Source Interface	lan
Source Network	ip_proxy_lan
Destination Interface	wan1
Destination Network	all-nets

Зайдите в меню *Rules→IP Rules*. Добавьте новое правило IP Rule для SIP, введите параметры во вкладке *General*:

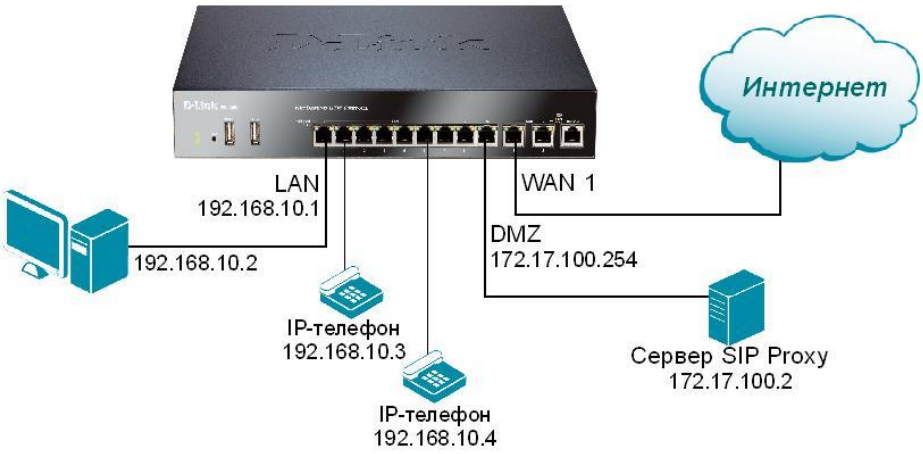
Name	SIP-inbound-SAT
Action	SAT
Service	SIP-service
Source Interface	wan1
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip

Во вкладке *SAT* введите параметры:

Translate the	Destination IP Address
To New IP Address	ip_proxy_lan

Зайдите в меню *Rules→IP Rules*. Добавьте новое правило IP Rule для SIP, введите параметры во вкладке *General*:

Name	SIP-inbound-allow

Action	Allow
Service	SIP-service
Source Interface	wan1
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address ip_proxy_lan Address=192.168.10.20 gw-world:/labs> cc gw-world:/> add ALG ALG_SIP SIP-ALG MaxSessionsPerId=2 MaxRegistrationTime=1200 SipSignalTmout=60 DataChannelTmout=100 AllowMediaByPass=No gw-world:/> add Service ServiceTCPUDP SIP-service DestinationPorts=5060 SourcePorts=0-65535 Type=UDP ALG=SIP-ALG gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=NAT DestinationInterface=wan1 DestinationNetwork=all-netsService=SIP-service SourceInterface=lan SourceNetwork=labs/ip_proxy_lan Name=SIP-outbound gw-world:/1(labs)> add IPRule Action=SAT Service=SIP-service SourceInterface=wan1 SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip SATTranslateToIP=labs/ip_proxy_lan SATTranslate DestinationIP Name=SIP-inbound-SAT gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ipService=SIP-service SourceInterface=wan1 SourceNetwork=all-netsName=SIP-inbound-allow gw-world:/1(labs)> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Упражнение	Проверьте работосопособность VoIP-сети, сделайте пробные звонки на внутренние телефоны и на внешние телефоны.
Организация VoIP-сети, если клиенты находятся в локальной сети, а сервер SIP Proxy подключен к dmz-интерфейсу	
Описание сценария	*Обеспечим передачу VoIP-трафика, VoIP-сеть размещена за межсетевым экраном с NAT. Сервер SIP Proxy размещается в* ***dmz***-зоне.
Схема 65	
Настройка DFL-860E	

Web-интерфейс	
Создадим объект «IP-адрес сервера SIP Proxy». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	ip_proxy_dmz
Address	172.17.100.2
Настройка IP Rule	
Зайдите в меню *Rules→IP Rules*. Добавьте новое правило IP Rule для SIP, введите параметры во вкладке *General*:	
Name	SIP-outbound
Action	NAT
Service	SIP-service
Source Interface	lan
Source Network	lannet
Destination Interface	dmz
Destination Network	ip_proxy_dmz
Зайдите в меню *Rules→IP Rules*. Добавьте новое правило IP Rule для SIP, введите параметры во вкладке *General*:	
Name	SIP-outbound-allow
Action	Allow
Service	SIP-service
Source Interface	dmz
Source Network	ip_proxy_dmz
Destination Interface	wan1
Destination Network	all-nets
Зайдите в меню *Rules→IP Rules*. Добавьте новое IP Rule для SIP, введите параметры во вкладке *General*:	
Name	SIP-inbound-from-proxy
Action	Allow
Service	SIP-service
Source Interface	dmz
Source Network	ip_proxy_dmz
Destination Interface	core
Destination Network	dmz_ip
Зайдите в меню *Rules→IP Rules*. Добавьте новое правило IP Rule для SIP, введите параметры во вкладке *General*:	
Name	SIP-inbound-to-proxy
Action	Allow
Service	SIP-service
Source Interface	wan1
Source Network	all-nets
Destination Interface	dmz
Destination Network	ip_proxy_dmz
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Примечание: При регистрации клиентов на прокси используется IP-адрес dmz-интерфейса	

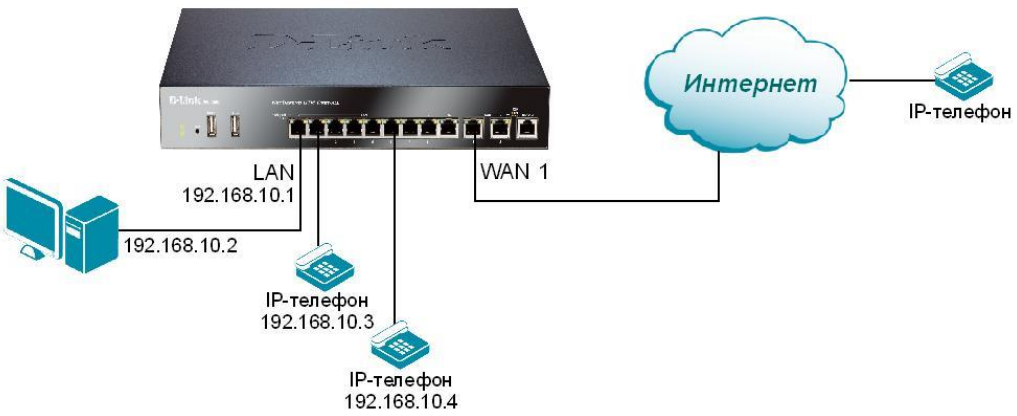
устройства.
<u>Командная строка (CLI)</u>
gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address ip_proxy_dmz Address=172.17.100.2 gw-world:/labs> cc gw-world:/> add ALG ALG_SIP SIP-ALG MaxSessionsPerId=2 MaxRegistrationTime=1200 SipSignalTmout=60 DataChannelTmout=100 AllowMediaByPass=No gw-world:/> add Service ServiceTCPUDP SIP-service DestinationPorts=5060 SourcePorts=0-65535 Type=UDP ALG=SIP-ALG gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=NAT DestinationInterface=dmz DestinationNetwork=labs/ip_proxy_dmz Service=SIP-service SourceInterface=lan SourceNetwork=InterfaceAddresses/lannetName=SIP-outbound gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=wan1 DestinationNetwork=all-nets Service=SIP-service SourceInterface=dmz SourceNetwork=labs/ip_proxy_dmz Name=SIP-outbound-allow gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=core DestinationNetwork=InterfaceAddresses/dmz_ip Service=SIP-service SourceInterface=dmz SourceNetwork=labs/ip_proxy_dmz Name=SIP-inbound-from-proxy gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=dmz DestinationNetwork=labs/ip_proxy_dmz Service=SIP-service SourceInterface=wan1 SourceNetwork=all-nets Name=SIP-inbound-to-proxy gw-world:/1(labs)> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit

<u>Упражнение</u>	Проверьте работосопособность VoIP-сети, сделайте пробные звонки на внутренние телефоны и на внешние телефоны.

H.323

Описание стандарта H.323	*Стандарт H.323 используется для передачи аудио-, видео-данных через сети с коммутацией пакетов (например, IP-сети). H.323 является основой для обеспечения работы VoIP-телефонов в VoIP-сети.* *Компоненты H.323:* *- Терминалы, устройства, оконечное оборудование, например, телефоны, устройства для организации конференций, программные телефоны и т.д.* *- Шлюзы, соединяющие две различные по природе сети и преобразующие трафик между ними, например, между H.323-сетями и телефонной сетью общего пользования (ТфОП). H.323-шлюзы не обязательны для организации связи между H.323-терминалами.* *- Привратники, устройство адресации, авторизации и аутентификации терминалов и шлюзов H.323-системы. Также может выполнять функции управления полосой пропускания, учетными записями пользователей и биллингом. Привратник может разрешать звонки непосредственно между двумя конечными точками или маршрутизировать звонки с функциями удержания, переадресации, дозвона и т.д. Привратник необходимо использовать при наличии более одного терминала за межсетевым экраном с одним публичным IP-адресом и настроенным NAT-преобразованием.* *- Управляющие устройства много-точка (MCU), поддерживают*

	конференцию трех или более H.323-терминалов. Все H.323-терминалы, участвующие в конференции, должны устанавливать соединение с MCU. MCU управляют звонками, ресурсами, видео- и аудио-кодеками, используемыми при звонках. *При организации сигнализации вызова (call signaling) используется протокол H.225. Для организации связи между оконечным оборудованием H.323 используется TCP-порт 1720, для связи с привратником используется UDP-порт 1719 (в сообщении H.225 RAS).* *Протокол H.245 предоставляет управление сессиями мультимедиа между двумя оконечными точками H.323. Основная задача протокола H.245 – открывать и закрывать логические каналы при передачи медиаданных в интересах протокола T.120.*
Описание H.323 ALG	*H.323 ALG позволяет организовать взаимодействие H.323-устройств и приложений через приватную сеть, организованную на межсетевом экране D-Link.* *Спецификация H.323 не поддерживает NAT-технологии, т.к. IP-адреса и порты отсылаются встроенными в H.323-сообщения. H.323 ALG модифицирует и преобразует H.323-сообщения для гарантированной доставки и маршрутизации узлу назначения через межсетевой экран.* *Особенности H.323 ALG: поддержка H.323 версия 5 (H.225 версия 5, H.245 версия 10), доступ приложений (T.120), поддержка привратника, поддержка NAT, SAT.*
Конфигурации H.323 ALG	*H.323 ALG могут быть настроены несколькими способами. Возможно настроить запрет или разрешение прохождения TCP-каналов данных (TCP data channel) через межсетевой экран (для протокола T.120). Максимальное количество TCP-каналов данных может быть ограниченно фиксированным значением.* *Время регистрации на привратнике может быть задано администратором межсетевого экрана некоторым временным интервалом.* *Устройства в соответствии с портами могут быть указанны следующим образом:* *- Gatekeeper: все UDP→1719;* *-H323: H.323 ALG, все TCP→1720;* *- H323-Gatekeeper: H.323 ALG, UDP→1719.*
Описание сценария	*Телефон с поддержкой H.323 подключается к **lan**-сети межсетевого экрана с приватным IP-адресом. Необходимо настроить межсетевой экран так, чтобы было возможно звонить с данного телефона через Интернет и звонить на него с других H.323-телефонов из Интернета.*

Схема 66	

Настройка DFL-860E

Web-интерфейс

Создадим объект «IP-адрес VoIP-телефона». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:

Name	ip-phone
Address	192.168.10.3

Настройка ALG

Зайдите в меню *Objects→ALG*. Добавьте новый H.323 ALG.

Name	H323-alg
Allow TCP data channels (T.120)	Поставьте галочку
Maximum number of TCP data channels per call	10
Max Gatekeeper Registration Lifetime	1800

Настройка TCP/UDP Service

Зайдите в меню *Objects→Services*. Создайте новую службу, введите следующие параметры:

Name	H323
Type	TCP (выберите из списка)
Destination	1720
ALG	H323-alg

Настройка IP Rule

Настроем правило для исходящего трафика. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:

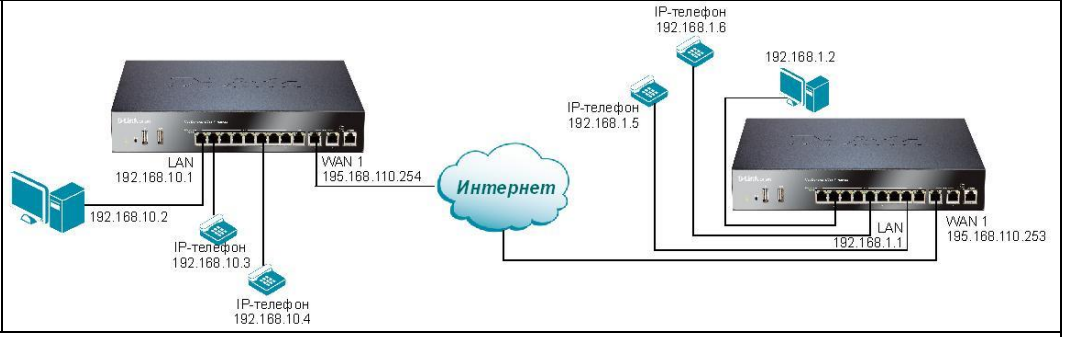
Name	H323AllowOut
Action	Allow
Service	h323
Source Interface	lan
Source Network	lannet
Destination Interface	any
Destination Network	all-nets

Настроем правило для входящего трафика. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:

Name	H323AllowIn
Action	Allow
Service	h323
Source Interface	any
Source Network	all-nets
Destination Interface	lan
Destination Network	lannet
Примечание: Описанные выше правила должны быть добавлены в список правил, убедитесь, что перед ними нет правил, разрешающих/запрещающих те же порты и тот же трафик.	
Настроем правило для исходящего трафика с учетом необходимости SAT-преобразования на приватный IP-адрес телефона. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:	
Name	H323Out
Action	NAT
Service	h323
Source Interface	lan
Source Network	lannet
Destination Interface	any
Destination Network	all-nets
Настроем правило для входящего трафика с учетом необходимости SAT-преобразования на приватный IP-адрес телефона (IP-адрес телефона – ip-phone). Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:	
Name	H323In
Action	SAT
Service	h323
Source Interface	any
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip (внешний IP-адрес межсетевого экрана)
Введите параметры во вкладке *SAT*:	
Translate the	Destination IP Address
To New IP Address	ip_phone
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:	
Name	H323In-allow
Action	Allow
Service	h323
Source Interface	any
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip (внешний IP-адрес межсетевого экрана)
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Примечание: если за межсетевым экраном размещается несколько H.323-телефонов, то для каждого должно быть создано SAT-правило. Чтобы избежать множественной внешней адресации, используется H.323-привратник – в этом случае понадобиться только один внешний адрес.	

Командная строка (CLI)

gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address ip_phoneAddress=192.168.10.3
gw-world:/labs> cc
gw-world:/>add ALG ALG_H323 H323-alg AllowTCPDataChannels=Yes MaxTCPDataChannels=10 MaxGKRegLifeTime=1800
gw-world:/> add Service ServiceTCPUDP H323 DestinationPorts=1720 SourcePorts=0-65535 Type=TCP ALG=H323-alg
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=any DestinationNetwork=all-nets Service=H323 SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Name=H323AllowOut
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Service=H323 SourceInterface=any SourceNetwork=all-nets Name=H323AllowIn
gw-world:/1(labs)> add IPRule Action=NAT DestinationInterface=any DestinationNetwork=all-nets Service=H323 SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Name=H323Out
gw-world:/1(labs)> add IPRule Action=SAT Service=H323 SourceInterface=any SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip SATTranslateToIP=labs/ip_phone SATTranslate DestinationIP Name=H323In
gw-world:/1(labs)> add IPRule Action=Allow Service=H323 SourceInterface=any SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip Name=H323In-allow
gw-world:/1(labs)> cc
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Упражнение	Проверьте работоспособность VoIP-сети, сделайте пробные звонки на внутренние телефоны и на внешние телефоны.
Описание сценария	*Два H.323-телефона подключаются к сети с публичным адресом. Необходимо настроить межсетевой экран так, чтобы было возможно звонить с этого H.323-телефона через Интернет на другой и наоборот.*
Схема 67	

Настройка DFL-860E

Устройство A

Web-интерфейс

Настройте параметры интерфейсов:

Name	wan1_ip
Address	195.168.110.254
Name	wan1net
Address	195.168.110.0/24

Name	lan_ip
Address	192.168.10.1
Name	lannet
Address	192.168.10.0/24
Создадим объект «IP-адрес VoIP-телефона». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	ip-phone
Address	192.168.10.4
Настройка IP Rule	
Настроем правило для исходящего трафика. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:	
Name	H323AllowOut
Action	Allow
Service	h323
Source Interface	lan
Source Network	lannet
Destination Interface	any
Destination Network	all-nets
Настроем правило для входящего трафика. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:	
Name	H323AllowIn
Action	Allow
Service	h323
Source Interface	any
Source Network	all-nets
Destination Interface	lan
Destination Network	lannet
Примечание: Описанные выше правила должны быть добавлены в список правил, убедитесь, что перед ними нет правил, разрешающих/запрещающих те же порты и тот же трафик.	
Настроем правило для исходящего трафика для возможности осуществления звонков через Интернет. Т.к. телефоны используют приватные IP-адреса, необходимо осуществлять SAT-преобразование на приватный IP-адрес телефона. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:	
Name	H323Out
Action	NAT
Service	h323
Source Interface	lan
Source Network	lannet
Destination Interface	any
Destination Network	all-nets
Настроем правило для входящего трафика для возможности осуществления звонков через Интернет. Т.к. телефоны используют приватные IP-адреса, необходимо осуществлять SAT-преобразование на приватный IP-адрес телефона. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:	
Name	H323In
Action	SAT

Service	h323
Source Interface	any
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip (внешний IP-адрес межсетевого экрана)
Введите параметры во вкладке *SAT*:	
Translate the	Destination IP Address
To New IP Address	ip_phone
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите следующие параметры:	
Name	H323In-allow
Action	Allow
Service	h323
Source Interface	any
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip (внешний IP-адрес межсетевого экрана)
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.168.110.254 gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.168.110.0/24 gw-world:/> set IP4Address InterfaceAddresses/lan_ip Address=192.168.10.1 gw-world:/> set IP4Address InterfaceAddresses/lannet Address=192.168.10.0/24 gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address ip_phoneAddress=192.168.10.4 gw-world:/labs> cc gw-world:/>add ALG ALG_H323 H323-alg AllowTCPDataChannels=Yes MaxTCPDataChannels=10 MaxGKRegLifeTime=1800 gw-world:/> add Service ServiceTCPUDP H323 DestinationPorts=1720 SourcePorts=0-65535 Type=TCP ALG=H323-alg gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=any DestinationNetwork=all-nets Service=H323 SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Name=H323AllowOut gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Service=H323 SourceInterface=any SourceNetwork=all-nets Name=H323AllowIn gw-world:/1(labs)> add IPRule Action=NAT DestinationInterface=any DestinationNetwork=all-nets Service=H323 SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Name=H323Out gw-world:/1(labs)> add IPRule Action=SAT Service=H323 SourceInterface=any SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip SATTranslateToIP=labs/ip_phone SATTranslate DestinationIP Name=H323In gw-world:/1(labs)> add IPRule Action=Allow Service=H323 SourceInterface=any SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip Name=H323In-allow gw-world:/1(labs)> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Настройка DFL-860E	

Устройство B	
Web-интерфейс	
Настройте параметры интерфейсов:	
Name	wan1_ip
Address	195.168.110.253
Name	wan1net
Address	195.168.110.0/24
Name	lan_ip
Address	192.168.1.1
Name	lannet
Address	192.168.1.0/24
Создадим объект «IP-адрес VoIP-телефона». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	ip-phone
Address	192.168.1.5
Настройка IP Rule	
Настроем правило для исходящего трафика. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:	
Name	H323AllowOut
Action	Allow
Service	h323
Source Interface	lan
Source Network	lannet
Destination Interface	any
Destination Network	all-nets (0.0.0.0/0)
Настроем правило для входящего трафика. Зайдите в папк у*Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:	
Name	H323AllowIn
Action	Allow
Service	h323
Source Interface	any
Source Network	all-nets
Destination Interface	lan
Destination Network	lannet
Примечание: Описанные выше правила должны быть добавлены в список правил, убедитесь, что перед ними нет правил, разрешающих/запрещающих те же порты и тот же трафик.	
Настроем правило для исходящего трафика для возможности осуществления звонков через Интернет. Т.к. телефоны используют приватные IP-адреса, необходимо осуществлять SAT-преобразование на приватный IP-адрес телефона. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:	
Name	H323Out
Action	NAT
Service	h323
Source Interface	lan

Source Network	lannet
Destination Interface	any
Destination Network	all-nets

Настроем правило для входящего трафика для возможности осуществления звонков через Интернет. Т.к. телефоны используют приватные IP-адреса, необходимо осуществлять SAT-преобразование на приватный IP-адрес телефона. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:

Name	H323In
Action	SAT
Service	h323
Source Interface	any
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip (внешний IP-адрес межсетевого экрана)

Введите параметры во вкладке *SAT*:

Translate the	Destination IP Address
To New IP Address	ip_phone

Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:

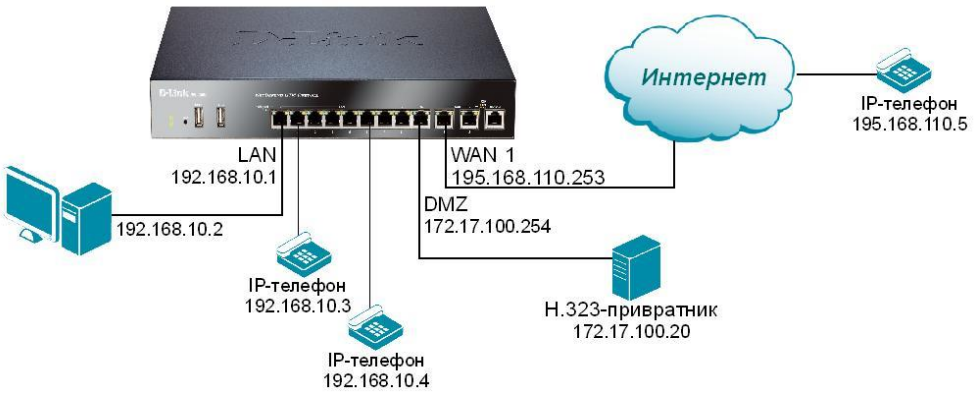
Name	H323In-allow
Action	Allow
Service	h323
Source Interface	any
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip (внешний IP-адрес межсетевого экрана)

Зайдите в меню *Configuration* и выберите *Save and Activate*.

Командая строка (CLI)

```
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.168.110.253
gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.168.110.0/24
gw-world:/> set IP4Address InterfaceAddresses/lan_ip Address=192.168.1.1
gw-world:/> set IP4Address InterfaceAddresses/lannet Address=192.168.1.0/24
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address ip_phoneAddress=192.168.1.5
gw-world:/labs> cc
gw-world:/>add ALG ALG_H323 H323-alg AllowTCPDataChannels=Yes MaxTCPDataChannels=10
MaxGKRegLifeTime=1800
gw-world:/> add Service ServiceTCPUDP H323 DestinationPorts=1720 SourcePorts=0-65535
Type=TCP ALG=H323-alg
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=any DestinationNetwork=all-nets
Service=H323 SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Name=H323AllowOut
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=lan
DestinationNetwork=InterfaceAddresses/lannet Service=H323 SourceInterface=any SourceNetwork=all-
nets Name=H323AllowIn
gw-world:/1(labs)> add IPRule Action=NAT DestinationInterface=any DestinationNetwork=all-nets
Service=H323 SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Name=H323Out
gw-world:/1(labs)> add IPRule Action=SAT Service=H323 SourceInterface=any SourceNetwork=all-
```

nets DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip SATTranslateToIP=labs/ip_phone SATTranslate DestinationIP Name=H323In
gw-world:/1(labs)> add IPRule Action=Allow Service=H323 SourceInterface=any SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip Name=H323In-allow
gw-world:/1(labs)> cc
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Упражнение	Проверьте работоспособность VoIP-телефонии, сделайте пробные звонки на внутренние телефоны и на внешние телефоны.
Описание сценария	*H.323-привратник размещается в **dmz**-зоне межсетевого экрана. Необходимо разрешить трафик между локальной сетью, где подключены H.323-телефоны, и привратником в **dmz**-зоне. Привратник имеет приватный IP-адрес.*
Схема 68	

Настройка DFL-860E

Web-интерфейс

Создадим объект «IP-адрес H.323-привратника». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:

Name	ip-gatekeeper
Address	172.17.100.20

Настройка ALG

Зайдите в меню *Objects→ALG*. Добавьте новый H.323 ALG.

Name	H323-alg
Allow TCP data channels (T.120)	Поставьте галочку
Maximum number of TCP data channels per call	10
Max Gatekeeper Registration Lifetime	1800

Настройка TCP/UDP Service

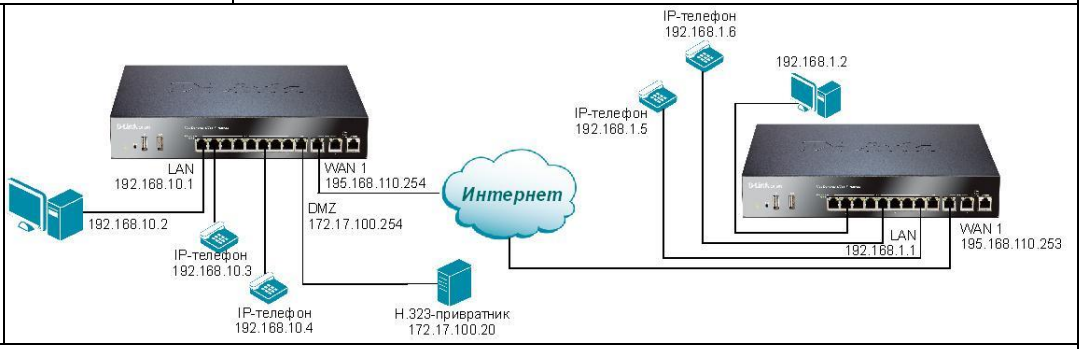
Зайдите в меню *Objects→Services*. Создайте новую службу, введите следующие параметры:

Name	H323-gatekeeper
Type	UDP (выберите из списка)
Destination	1719
ALG	H323-alg

Настройка IP Rule

Настроем правило для исходящего трафика. Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите следующие параметры:	
Name	H323In
Action	SAT
Service	h323-gatekeeper
Source Interface	any
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip (внешний IP-адрес межсетевого экрана)
Введите параметры во вкладке *SAT*:	
Translate the	Destination IP Address
To New IP Address	ip-gatekeeper (IP-адрес привратника)
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите следующие параметры:	
Name	H323In-allow
Action	Allow
Service	h323-gatekeeper
Source Interface	any
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip (внешний IP-адрес межсетевого экрана)
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите следующие параметры:	
Name	H323In-dmz
Action	Allow
Service	h323-gatekeeper
Source Interface	lan
Source Network	lannet
Destination Interface	dmz
Destination Network	ip-gatekeeper
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Примечание: 1. Нет необходимости определять правило для исходящих звонков. Межсетевой экран мониторит соединение между внешними телефонами и привратником, чтобы для внутренних телефонов было возможно звонить на внешние телефоны, зарегистрированные на привратнике. ***2. Описанные выше правила должны быть добавлены в список правил, убедитесь, что перед ними нет правил, разрешающих/запрещающих те же порты и тот же трафик.***	
Командная строка (CLI)	
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.168.110.253 gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.168.110.0/24 gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address ip-gatekeeper Address=172.17.100.20 gw-world:/labs> cc gw-world:/>add ALG ALG_H323 H323-alg AllowTCPDataChannels=Yes MaxTCPDataChannels=10 MaxGKRegLifeTime=1800 gw-world:/> add Service ServiceTCPUDP H323-gatekeeper DestinationPorts=1719 SourcePorts=0-65535 Type=UDP ALG=H323-alg	

gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=SAT Service=H323-gatekeeper SourceInterface=any SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip SATTranslateToIP=labs/ip-gatekeeper SATTranslate DestinationIP Name=H323In
gw-world:/1(labs)> add IPRule Action=Allow Service=H323-gatekeeper SourceInterface=any SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip Name=H323In-allow
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=dmz DestinationNetwork=labs/ip-gatekeeper Service=H323-gatekeeper SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Name=H323In-dmz
gw-world:/1(labs)> cc
gw-world:/> activate *(подождать 3-5секунд)*
gw-world:/>commit

Упражнение	Проверьте работоспособность VoIP-телефонии, сделайте пробные звонки на внутренние телефоны и на внешние телефоны.
Описание сценария	*H.323-привратник размещается в **dmz**-зоне межсетевого экрана A, в локальной сети межсетевого экрана B размещается H.323 телефон. Необходимо разрешить трафик между локальной сетью A, где подключены H.323-телефоны, и привратником **dmz**-зоны с H.323-телефоном, подключенным к межсетевому экрану B.*
Схема 69	

Настройка DFL-860E

Устройство A

Web-интерфейс

Создадим объект «IP-адрес H.323-привратника». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:

Name	ip-gatekeeper
Address	172.17.100.20

Настройка IP Rule

Настроем правило для исходящего трафика. Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите следующие параметры:

Name	H323In
Action	SAT
Service	h323-gatekeeper
Source Interface	any
Source Network	all-nets
Destination Interface	core

Destination Network	wan1_ip (внешний IP-адрес межсетевого экрана)
Введите параметры во вкладке *SAT*:	
Translate the	Destination IP Address
To New IP Address	ip-gatekeeper (IP-адрес привратника)
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите следующие параметры:	
Name	H323In-allow
Action	Allow
Service	h323-gatekeeper
Source Interface	any
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip (внешний IP-адрес межсетевого экрана)
Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите следующие параметры:	
Name	H323In-dmz
Action	Allow
Service	h323-gatekeeper
Source Interface	lan
Source Network	lannet
Destination Interface	dmz
Destination Network	ip-gatekeeper
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.168.110.254 gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.168.110.0/24 gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address ip-gatekeeper Address=172.17.100.20 gw-world:/labs> cc gw-world:/>add ALG ALG_H323 H323-alg AllowTCPDataChannels=Yes MaxTCPDataChannels=10 MaxGKRegLifeTime=1800 gw-world:/> add Service ServiceTCPUDP H323-gatekeeper DestinationPorts=1719 SourcePorts=0-65535 Type=UDP ALG=H323-alg gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=SAT Service=H323-gatekeeper SourceInterface=any SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip SATTranslateToIP=labs/ip-gatekeeper SATTranslate DestinationIP Name=H323In gw-world:/1(labs)> add IPRule Action=Allow Service=H323-gatekeeper SourceInterface=any SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip Name=H323In-allow gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=dmz DestinationNetwork=labs/ip-gatekeeper Service=H323-gatekeeper SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Name=H323In-dmz gw-world:/1(labs)> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Настройка DFL-860E	

Устройство B

Web-интерфейс

Настроем правила для исходящего трафика. Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите следующие параметры:

Name	H323Out
Action	NAT
Service	h323-Gatekeeper
Source Interface	lan
Source Network	lannet
Destination Interface	any
Destination Network	all-nets

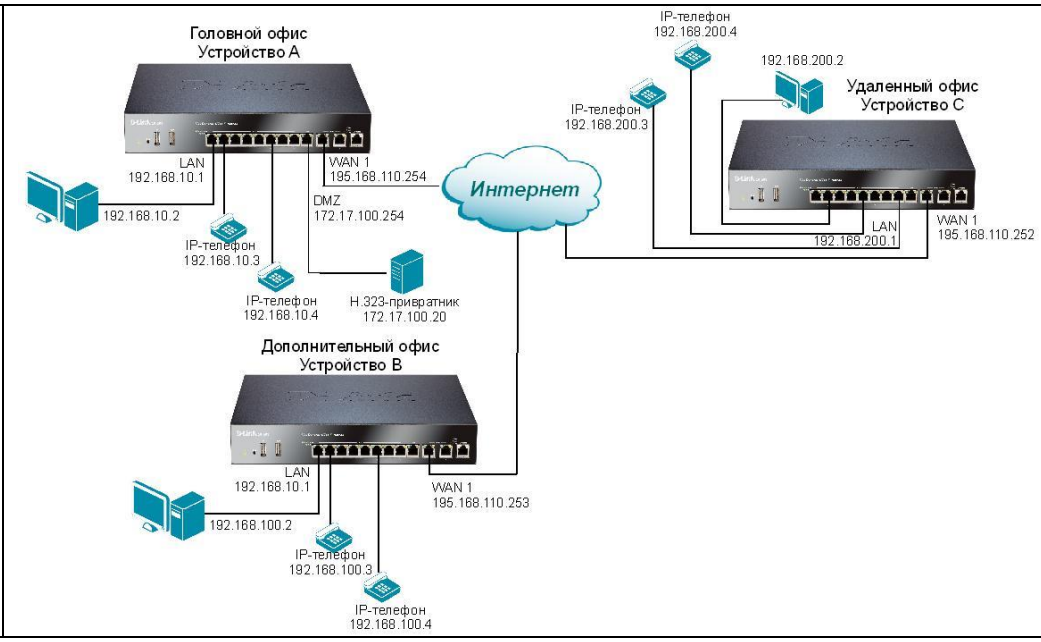
Зайдите вменю *Configuration* и выберите *Save and Activate*.

Примечание: 1. Нет необходимости определять правило для исходящих звонков. Межсетевой экран мониторит соединение между внешними телефонами и привратником, чтобы для внутренних телефонов было возможно звонить на внешние телефоны, зарегистрированные на привратнике.
2. Описанные выше правила должны быть добавлены в список правил, убедитесь, что перед ними нет правил, разрешающих/запрещающих те же порты и тот же трафик.

Командная строка (CLI)

```
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.168.110.253
gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.168.110.0/24
gw-world:/>add ALG ALG_H323 H323-alg AllowTCPDataChannels=Yes MaxTCPDataChannels=10
MaxGKRegLifeTime=1800
gw-world:/> add Service ServiceTCPUDP H323-gatekeeper DestinationPorts=1719 SourcePorts=0-
65535 Type=UDP ALG=H323-alg
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=NAT Service=H323-gatekeeper SourceInterface=lan
SourceNetwork=InterfaceAddresses/lannet DestinationInterface=any DestinationNetwork=all-nets
Name=H323Out
gw-world:/1(labs)> cc
gw-world:/> activate (подождать 3-5 секунд)
gw-world:/>commit
```

Упражнение	Проверьте работоспособность VoIP-телефонии, сделайте пробные звонки на внутренние телефоны и на внешние телефоны.
Описание сценария	*H.323-привратник размещается в крупной корпоративной сети. В **dmz**-зоне головного офиса размещается H.323-привратник, обрабатывающий звонки H.323-клиентов головного, дополнительного и удаленных офисов. Таким образом, организация использует сеть для передачи разных видов трафика. Предполагается, что на каналах подняты VPN-тунели. Все внешние звонки осуществляются через сети ТфОП.*

Схема 70	

Настройка DFL-860E

Устройство A (головной офис)

Web-интерфейс

Настройте параметры интерфейсов:

Name	wan1_ip
Address	195.168.110.254
Name	wan1net
Address	195.168.110.0/24
Name	lan_ip
Address	192.168.10.1
Name	lannet
Address	192.168.10.0/24
Name	dmz_ip
Address	172.17.100.254
Name	dmznet
Address	172.17.100.0/24

Создадим объект «IP-адрес H.323-привратника». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:

Name	ip-gatekeeper
Address	172.17.100.20

Создадим объект «IP-адрес H.323-шлюза». Зайдите в *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:

Name	ip-gateway
Address	172.17.100.30

Создадим объект «IP-адрес сети дополнительного офиса». Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:

Name	branch-net

Address	192.168.100.0/24
Создадим объект «IP-адрес сети удаленного офиса». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote-net
Address	192.168.200.0/24
Настройка ALG	
Зайдите в меню *Objects→ALG*. Добавьте новый H.323 ALG.	
Name	H323-alg
Allow TCP data channels (T.120)	Поставьте галочку
Maximum number of TCP data channels per call	10
Max Gatekeeper Registration Lifetime	1800
Настройка TCP/UDP Service	
Зайдите в меню *Objects→Services*. Создайте новую службу, введите следующие параметры:	
Name	H323-gatekeeper
Type	UDP (выберите из списка)
Destination	1719
ALG	H323-alg
Зайдите в меню *Objects→Services*. Создайте новую службу, введите следующие параметры:	
Name	H323
Type	TCP (выберите из списка)
Destination	1720
ALG	H323-alg
Настройка IP Rule	
Настроем IP Rule, разрешающие доступ H.323-устройств из локальной сети lannet к привратнику. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:	
Name	LanToGK
Action	Allow
Service	h323-gatekeeper
Source Interface	lan
Source Network	lannet
Destination Interface	dmz
Destination Network	ip-gatekeeper
Настроем IP Rule, разрешающие звонки телефонам в H.323-шлюзе DMZ-зоны. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:	
Name	LanToGW
Action	Allow
Service	h323
Source Interface	lan
Source Network	lannet
Destination Interface	dmz
Destination Network	ip-gateway

Настроем IP Rule, разрешающие доступ H.323-шлюза к H.323-телефонам во внешней сети. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:

Name	GWToLan
Action	Allow
Service	h323
Source Interface	dmz
Source Network	ip-gateway
Destination Interface	lan
Destination Network	lannet

Настроем IP Rule, разрешающие доступ H.323-привратника в DMZ-зоне к дополнительному офису (межсетевой экран B). Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:

Name	BranchToGW
Action	Allow
Service	h323-gatekeeper
Source Interface	vpn-branch (VPN канал в дополнительный офис)
Source Network	branch-net (сеть дополнительного офиса)
Destination Interface	dmz
Destination Network	ip-gatekeeper, ip-gateway

Настроем IP Rule, разрешающие доступ H.323-привратника в DMZ-зоне к удаленному офису (межсетевой экран C). Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:

Name	RemoteToGW
Action	Allow
Service	h323-gatekeeper
Source Interface	vpn-remote (VPN канал в удаленный офис)
Source Network	remote-net (сеть удаленного офиса)
Destination Interface	dmz
Destination Network	ip-gatekeeper

Зайдите в меню *Configuration* и выберите *Save and Activate*.

Командная строка (CLI)

```
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.168.110.254
gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.168.110.0/24
gw-world:/> set IP4Address InterfaceAddresses/lan_ip Address=192.168.10.1
gw-world:/> set IP4Address InterfaceAddresses/lannet Address=192.168.10.0/24
gw-world:/> set IP4Address InterfaceAddresses/dmz_ip Address=172.17.100.254
gw-world:/> set IP4Address InterfaceAddresses/dmznet Address=172.17.100.0/24
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address ip-gatekeeper Address=172.17.100.20
gw-world:/labs> add IP4Address ip-gateway Address=172.17.100.30
gw-world:/labs> add IP4Address branch-net Address=192.168.100.0/24
gw-world:/labs> add IP4Address remote-net Address=192.168.200.0/24
gw-world:/labs> cc
gw-world:/>add ALG ALG_H323 H323-alg AllowTCPDataChannels=Yes MaxTCPDataChannels=10
MaxGKRegLifeTime=1800
gw-world:/> add Service ServiceTCPUDP H323 DestinationPorts=1720 SourcePorts=0-65535
Type=TCP ALG=H323-alg
```

gw-world:/> add Service ServiceTCPUDP H323-gatekeeper DestinationPorts=1719 SourcePorts=0-65535 Type=UDP ALG=H323-alg
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=dmz DestinationNetwork=labs/ip-gatekeeper Service=H323-gatekeeper SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Name=LanToGK
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=dmz DestinationNetwork=labs/ip-gateway Service=H323 SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Name=LanToGW
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=lan DestinationNetwork=InterfaceAddresses/lannet Service=H323 SourceInterface=dmz SourceNetwork=labs/ip-gateway Name=GWToLan
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=dmz DestinationNetwork=labs/ip-gatekeeper,labs/ip-gateway Service=H323-gatekeeper SourceInterface=vpn-branch SourceNetwork=labs/branch-net Name=BranchToGW
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=dmz DestinationNetwork=labs/ip-gatekeeper Service=H323-gatekeeper SourceInterface=vpn-remote SourceNetwork=labs/remote-net Name=RemoteToGW
gw-world:/1(labs)> cc
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Настройка DFL-860E

Устройство B (дополнительный офис)

Web-интерфейс

Настройте параметры интерфейсов:

Name	wan1_ip
Address	195.168.110.253
Name	wan1net
Address	195.168.110.0/24
Name	lan_ip
Address	192.168.100.1
Name	lannet
Address	192.168.100.0/24

Создадим «объект IP-адрес сети головного офиса». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:

Name	hq-net
Address	192.168.10.0/24

Создадим объект «IP-адрес шлюза дополнительного офиса». Зайдите в *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:

Name	ip-branchgwlan-net
Address	172.17.100.50

Настроем IP Rule, разрешающие доступ H.323-телефонов к H.323-привратнику головного офиса (межсетевой экран A). Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:

Name	ToGK
Action	Allow
Service	h323-gatekeeper

Source Interface	lan
Source Network	lannet
Destination Interface	vpn-hq (VPN-канал в центральный офис)
Destination Network	hq-net (сеть в центральном офисе)

Настроем IP Rule, разрешающие доступ H.323-шлюза к H.323-привратнику головного офиса (межстевой экран A). Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:

Name	GWToGK
Action	Allow
Service	h323-gatekeeper
Source Interface	dmz
Source Network	ip-branchgwlan-net (IP-адрес шлюза дополнительного офиса)
Destination Interface	vpn-hq (VPN-канал в центральный офис)
Destination Network	hq-net (сеть в центральном офисе)

Зайдите в меню *Configuration* и выберите *Save and Activate*.

Примечание: Нет необходимости определять правило для исходящих звонков. Межсетевой экран мониторит соединение между внешними телефонами и привратником, чтобы для внутренних телефонов было возможно звонить на внешние телефоны, зарегистрированные на привратнике.

Командная строка (CLI)

```
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.168.110.253
gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.168.110.0/24
gw-world:/> set IP4Address InterfaceAddresses/lan_ip Address=192.168.100.1
gw-world:/> set IP4Address InterfaceAddresses/lannet Address=192.168.100.0/24
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address ip-branchgwlan-net Address=172.17.100.50
gw-world:/labs> add IP4Address hq-net Address=192.168.10.0/24
gw-world:/labs> cc
gw-world:/>add ALG ALG_H323 H323-alg AllowTCPDataChannels=Yes MaxTCPDataChannels=10
MaxGKRegLifeTime=1800
gw-world:/> add Service ServiceTCPUDP H323-gatekeeper DestinationPorts=1719 SourcePorts=0-
65535 Type=UDP ALG=H323-alg
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=vpn-hq
DestinationNetwork=labs/hq-net Service=H323-gatekeeper
SourceInterface=lanSourceNetwork=InterfaceAddresses/lannet Name=ToGK
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=vpn-hq
DestinationNetwork=labs/hq-net Service=H323-gatekeeper SourceInterface=dmz
SourceNetwork=labs/ip-branchgwlan-net Name=GWToGK
gw-world:/1(labs)> cc
gw-world:/> activate (подождать 3-5 секунд)
gw-world:/>commit
```

Настройка DFL-860E

Устройство C (удаленный офис)

Web-интерфейс

Настройте параметры интерфейсов:

Name	wan1_ip
Address	195.168.110.252
Name	wan1net
Address	195.168.110.0/24
Name	lan_ip
Address	192.168.200.1
Name	lannet
Address	192.168.200.0/24

Создадим объект «IP-адрес сети головного офиса». Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:

Name	hq-net
Address	192.168.10.0/24

Настроем IP Rule, разрешающие доступ H.323-телефонов к H.323-привратнику головного офиса (межсетевой экран A). Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:

Name	ToGK
Action	Allow
Service	h323-gatekeeper
Source Interface	lan
Source Network	lannet
Destination Interface	vpn-hq (VPN-канал в центральный офис)
Destination Network	hq-net (сеть в головном офисе)

Зайдите в меню *Configuration* и выберите *Save and Activate*.

<u>Командная строка (CLI)</u>

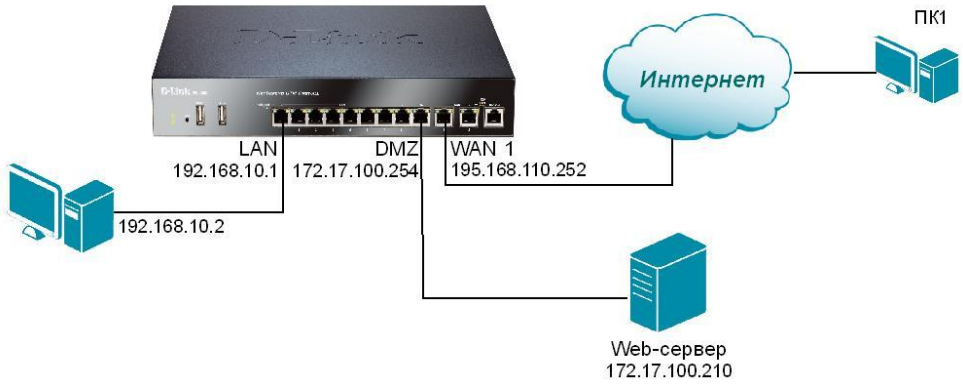
```
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.168.110.252
gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.168.110.0/24
gw-world:/> set IP4Address InterfaceAddresses/lan_ip Address=192.168.200.1
gw-world:/> set IP4Address InterfaceAddresses/lannet Address=192.168.200.0/24
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address hq-net Address=192.168.10.0/24
gw-world:/labs> cc
gw-world:/>add ALG ALG_H323 H323-alg AllowTCPDataChannels=Yes MaxTCPDataChannels=10
MaxGKRegLifeTime=1800
gw-world:/> add Service ServiceTCPUDP H323-gatekeeper DestinationPorts=1719 SourcePorts=0-
65535 Type=UDP ALG=H323-alg
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=vpn-hq
DestinationNetwork=labs/hq-net Service=H323-gatekeeper SourceInterface=lan
SourceNetwork=InterfaceAddresses/lannet Name=ToGK
gw-world:/1(labs)> cc
gw-world:/> activate (подождать 3-5 секунд)
gw-world:/>commit
```

<u>Упражнение</u>	Проверьте работосопособность VoIP-телефонии между офисами, сделайте пробные звонки на внутренние телефоны и на внешние телефоны.

ЗАНЯТИЕ №18. Использование TLS ALG

При применении защищенных соединений клиент-сервер типа SSL/TLS возникает необходимость использования промежуточного сервера SSL/TLS-аутентификации. Таким сервером может выступать межсетевой экран.

Цель	Эта лабораторная работа предназначена для ознакомления пользователей с использованием TLS ALG на межсетевом экране D-Link	
Оборудование	DFL-860E	1
	Рабочая станция	2
	Ethernet-кабель (патч-корд)	4

Настройка TLS ALG	
Описание сценария	*Необходимо настроить службу HTTPS для доступа пользователей **lan**-сети к сайту, аутентификация на котором происходит с помощью набора сертификатов. Вместо импорта сертификатов каждому пользователю в отдельности будет назначен механизм TLS ALG.*
Схема 71	
Рабочая станция с Microsoft Windows XP/Vista/7	
Создайте два самоподписанных сертификата с помощью специальной программы. Сохраните файлы сертификатов через экспорт сертификатов. Конвертируйте тип сертификатов в форматы **.cer** и **.key**. Можно воспользоваться программой OpenSSL 0.9.8k или аналогичной программой работы с сертификатами X.509.	
Настройка DFL-860E	
Web-интерфейс	
Настройте параметры интерфейсов:	
Name	wan1_ip
Address	195.168.110.252
Name	wan1net
Address	195.168.110.0/24
Импортируйте наборы созданных сертификатов (корневой сертификат, сертификат хоста – root_cert.cer, root_cert.key, host_cert.cer, host_cert.key), при этом root_cert подписывает host_cert. Зайдите в меню *Objects→Authentication Objects→Add→Certificate.* Введите следующие	

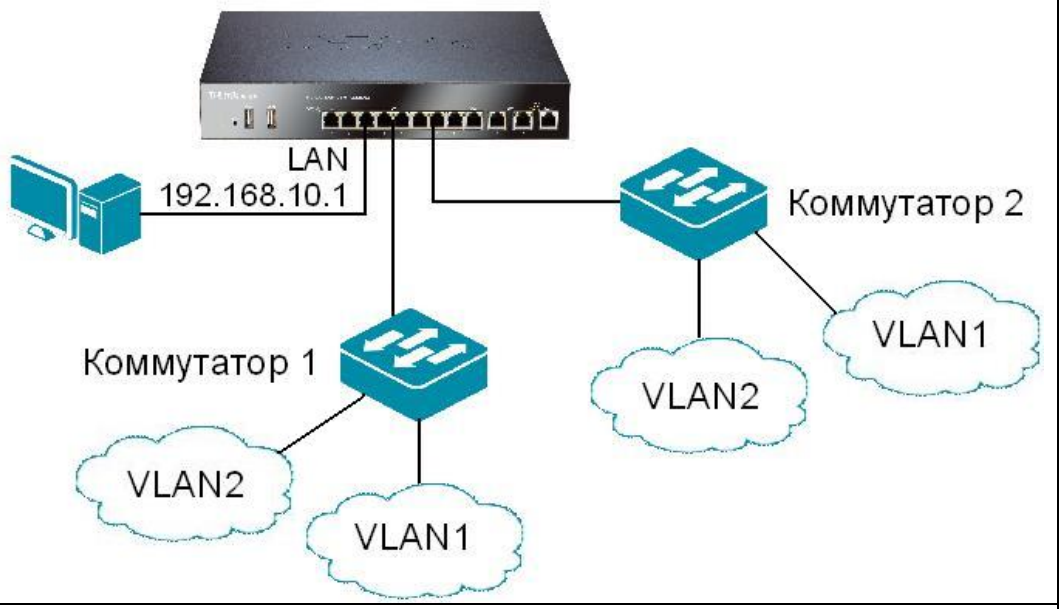
параметры:	
Name	root_cert
Upload X.509 certificate.	Выберите эту опцию и укажите путь к файлам сертификатов.
Зайдите в меню *Objects→Authentication Objects→Add→Certificate*. Введите следующие параметры:	
Name	host_cert
Upload X.509 certificate.	Выберите эту опцию и укажите путь к файлам сертификатов.
Создадим «объект IP-адрес Web-сервера dmz-зоны». Зайдите в *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	ip-webserver
Address	172.17.100.210
Настройка ALG	
Зайдите в меню *Objects→ALG→Add→TLS ALG*. Введите следующие параметры:	
Name	tls_alg
Host certificate	host_cert (выберите из списка)
Root certificate	root_cert (выберите из списка)
Примечание: Созданный ALG необходимо привязать к соответствующим службам.	
Настройка TCP/UDP Service	
Зайдите в меню *Objects→Services*. Создайте новую службу, введите следующие параметры:	
Name	https-tls
Type	TCP (выберите из списка)
Destination	443
ALG	tls_alg
Настройка IP Rule	
Настроем правило для исходящего трафика. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:	
Name	SAT-web-srv
Action	SAT
Service	https-tls
Source Interface	wan1
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip (внешний IP-адрес межсетевого экрана)
Введите параметры во вкладке *SAT*:	
Translate the	Destination IP Address
To New IP Address	ip-webserver
New Port	80
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:	
Name	Web-srv-allow
Action	Allow
Service	https-tls
Source Interface	wan1
Source Network	all-nets

Destination Interface	core
Destination Network	wan1_ip (внешний IP-адрес межсетевого экрана)
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.168.110.254 gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.168.110.0/24 gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address ip-webserverAddress=172.17.100.210 gw-world:/labs> cc gw-world:/>add ALG ALG_TLS tls_alg HostCert=host_cert _ad RootCert=root_cert gw-world:/> add Service ServiceTCPUDP https-tls DestinationPorts=443 SourcePorts=0-65535 Type=TCP ALG=tls_alg gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=SAT Service=https-tls SourceInterface=wan1 SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip SATTranslateToIP=labs/ip-webserver SATTranslate DestinationIP SATTranslateToPort=80 Name=SAT-web-srv gw-world:/1(labs)> add IPRule Action=Allow Service=https-tls SourceInterface=wan1 SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip Name=Web-srv-allow gw-world:/1(labs)> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Упражнение	Проверьте доступность HTTPS-сервера для пользователей, подключенных к **wan1**-интерфейсу межсетевого экрана. Зайдите с компьютера ПК1 через IP-адрес межсетевого экрана.
Internet Explorer ОС Windows (компьютер в сети wan1net)	https://<wan1_ip>

ЗАНЯТИЕ №19. Настройка VLAN.

Межсетевые экраны D-Link поддерживают технологию VLAN, позволяя администратору настраивать дополнительные механизмы обеспечения сетевой безопасности.

Цель	Эта лабораторная работа предназначена для изучения настройки VLAN на межсетевых экранах D-Link.	
Оборудование	DFL-860E	1
	Рабочая станция	3
	Ethernet-кабель (патч-корд)	7
	Коммутатор с поддержкой VLAN	2

Описание сценария	*Два коммутатора Коммутатор 1 и Коммутатор 2 подключены к физическим интерфейсам межсетевого экрана, на коммутаторах есть клиенты двух VLAN (vlan1, vlan2), типа port-based VLAN. Соединения между коммутаторами и межсетевым экраном – транкинговые (VLAN TRUNK). Необходимо настроить возможность функционирования VLAN.*
Схема 72	

Настройка DFL-860E

Web-интерфейс

Создание необходимых объектов

Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:

Name	vlannet1_ip
Address	192.168.100.1

Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:

Name	vlannet1
Address	192.168.100.0/24

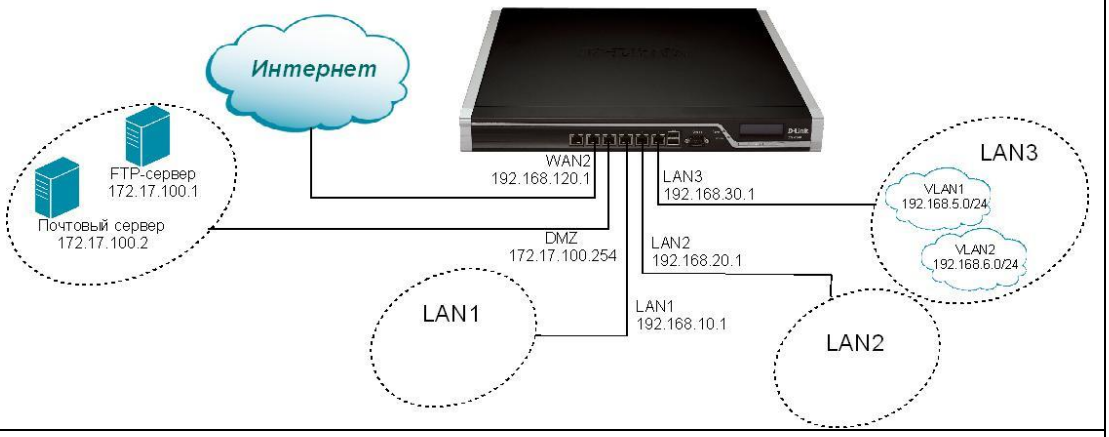
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:

Name	vlannet2_ip
Address	192.168.200.1
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	vlannet2
Address	192.168.200.0/24
Создадим VLAN-интерфейсы. Зайдите в меню *Interfaces→VLAN→Add→VLAN.* Во вкладке *General* введите следующие параметры*:*	
Name	vlan01
Interface	Укажите интерфейс lan
IP Address	vlannet1_ip
Network	vlannet1
VLAN ID	Укажите корректный VID - 5.
Зайдите в меню *Interfaces→VLAN→Add→VLAN.* Во вкладке *General* введите следующие параметры:	
Name	vlan02
Interface	Укажите интерфейс lan
IP Address	vlannet2_ip
Network	vlannet2
VLAN ID	Укажите корректный VID - 7.
Создание IP Rule	
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	vlan01_rule
Action	Allow
Service	all-services
Source Interface	vlan01
Source Network	vlannet1
Destination Interface	lan
Destination Network	lannet
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	vlan02_rule
Action	Allow
Service	all-services
Source Interface	vlan02
Source Network	vlannet2
Destination Interface	lan
Destination Network	lannet
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.168.110.254 gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.168.110.0/24 gw-world:/> set IP4Address InterfaceAddresses/lan_ip Address=192.168.10.1 gw-world:/> set IP4Address InterfaceAddresses/lannet Address=192.168.10.0/24 gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address vlannet1_ipAddress=192.168.100.1	

```
gw-world:/labs> add IP4Address vlannet1Address=192.168.100.0/24
gw-world:/labs> add IP4Address vlannet2_ipAddress=192.168.200.1
gw-world:/labs> add IP4Address vlannet2Address=192.168.200.0/24
gw-world:/labs> cc
gw-world:/>add Interface VLAN vlan01 Ethernet=lan IP=labs/vlannet1_ip Network=labs/vlannet1
VLANID=5
gw-world:/> add Interface VLAN vlan02 Ethernet=lan IP=labs/vlannet2_ip Network=labs/vlannet2
VLANID=7
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=lan
DestinationNetwork=InterfaceAddresses/lannet Service=all-services SourceInterface=vlan01
SourceNetwork=labs/vlannet1 Name=vlan01_rule
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=lan
DestinationNetwork=InterfaceAddresses/lannet Service=all-services SourceInterface=vlan02
SourceNetwork=labs/vlannet2 Name=vlan02_rule
gw-world:/1(labs)> cc
gw-world:/> activate (подождать 3-5 секунд)
gw-world:/>commit
```

Описание сценария	Данная работа выполняется на межсетевых экранах DFL-1660/2560. *Две VLAN-сети на основе меток созданы на **lan3**-интерфейсе, подключенному к порту коммутатора с VLAN tag. Из **lan1**-сети, **lan2**-сети, **lan3**-сети HTTP, HTTPS и DNS имеют выход в Интернет через **wan2**-интерфейс. Все внутренние сети также имеют доступ к почтовому серверу, расположенному в **dmz**-зоне. Только из VLAN2 есть доступ к FTP-серверу, расположенному в **dmz**-зоне.*

Схема 73



<u>Настройка DFL-1660</u>

<u>Web-интерфейс</u>

Создание необходимых объектов

Зайдите в меню *Objects→Address Book→InterfaceAddresses→lan1_ip.* Введите следующие параметры:

Name	lan1_ip
Address	192.168.10.1

Зайдите в меню *Objects→Address Book→InterfaceAddresses→lan1net.* Введите следующие параметры:

Name	lan1net

Address	192.168.10.0/24
Зайдите в меню *Objects→Address Book→InterfaceAddresses→lan2_ip*. Введите следующие параметры:	
Name	lan2_ip
Address	192.168.20.1
Зайдите в меню *Objects→Address Book→InterfaceAddresses→lan2net*. Введите следующие параметры:	
Name	lan2net
Address	192.168.20.0/24
Зайдите в меню *Objects→Address Book→InterfaceAddresses→lan3_ip*. Введите следующие параметры:	
Name	lan3_ip
Address	192.168.30.1
Зайдите в меню *Objects→Address Book→InterfaceAddresses→lan3net*. Введите следующие параметры:	
Name	lan3net
Address	192.168.30.0/24
Зайдите в меню *Objects→Address Book→InterfaceAddresses→dmz_ip*. Введите следующие параметры:	
Name	dmz_ip
Address	172.17.100.254
Зайдите в меню *Objects→Address Book→InterfaceAddresses→dmznet*. Введите следующие параметры:	
Name	dmznet
Address	172.17.100.0/24
Зайдите в меню *Objects→Address Book→InterfaceAddresses→wan1_ip*. Введите следующие параметры:	
Name	wan1_ip
Address	192.168.110.1
Зайдите в меню *Objects→Address Book→InterfaceAddresses→wan1net*. Введите следующие параметры:	
Name	wan1net
Address	192.168.110.0/24
Зайдите в меню *Objects→Address Book→InterfaceAddresses→wan1_gw*. Введите следующие параметры:	
Name	wan1_gw
Address	192.168.110.254
Зайдите в меню *Objects→Address Book→InterfaceAddresses→wan2_ip*. Введите следующие параметры:	
Name	wan2_ip
Address	192.168.120.1
Зайдите в меню *Objects→Address Book→InterfaceAddresses→wan2net*. Введите следующие параметры:	
Name	wan2net
Address	192.168.120.0/24
Зайдите в меню *Objects→Address Book→InterfaceAddresses→wan2_gw*. Введите следующие параметры:	
Name	wan2_gw

Address	192.168.120.254
Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	vlan1_ip
Address	192.168.5.254
Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	vlan1net
Address	192.168.5.0/24
Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	vlan2_ip
Address	192.168.6.254
Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	vlan2net
Address	192.168.6.0/24
Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	ftp-server
Address	172.17.100.1
Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	mail-server
Address	172.17.100.2
Зайдите в меню *Objects→Address Book→Add→IP4 Group*. Введите следующие параметры:	
Name	all-lannets
Selected	Выберите: lan1net, lan2net, vlan1net, vlan2net
Зайдите в *Interfaces→Ethernet→wan1*. Введите следующие параметры во вкладке *General*:	
IP Address	wan1_ip
Network	wan1net
Default Gateway	wan1_gw
Введите следующие параметры во вкладке *Advanced*:	
Add route for interface network	Уберите галочку
Add default route if default gateway is specified	Уберите галочку
Зайдите в меню *Interfaces→Ethernet→wan2*. Введите следующие параметры во вкладке *General*:	
IP Address	wan2_ip
Network	wan2net
Default Gateway	wan2_gw
Введите следующие параметры во вкладке *Advanced*:	
Add route for interface network	Уберите галочку
Add default route if default gateway is specified	Уберите галочку
Зайдите в меню *Routing→Routing Tables→main→Add→Route*. Введите следующие параметры:	
Interface	wan1
Network	all-nets
Gateway	wan1_gw
Local IP Address	None
Metric	90

Зайдите в меню *Routing→Routing Tables→main→Add→Route.* Введите следующие параметры:	
Interface	wan2
Network	all-nets
Gateway	wan2_gw
Local IP Address	None
Metric	80
Зайдите в меню *Interfaces→VLAN→Add→VLAN.* Введите следующие параметры во вкладке *General*:	
Name	vlan1
Interface	lan3
VLAN ID	1
IP Address	vlan1_ip
Network	vlan1net
Default Gateway	None
Зайдите в меню *Interfaces→VLAN→Add→VLAN.* Введите следующие параметры во вкладке *General*:	
Name	vlan2
Interface	lan3
VLAN ID	2
IP Address	vlan2_ip
Network	vlan2net
Default Gateway	None
Зайдите в меню *Interfaces→Interface Groups→Add→Interface Group.* Введите следующие параметры:	
Name	all-lan
Selected	Выберите: lan1, lan2, vlan1, vlan2
Зайдите в меню *Interfaces→Interface Groups→Add→Interface Group.* Введите следующие параметры:	
Name	all-wan
Selected	Выберите: wan1, wan2
Security/Transport Equivalent	Поставьте галочку
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	allow-http-all
Action	NAT
Service	http-all
Source Interface	all-lan
Source Network	all-lannets
Destination Interface	all-wan
Destination Network	all-nets
Зайдите в папк у*Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	allow-dns-all
Action	NAT
Service	dns-all
Source Interface	all-lan
Source Network	all-lannets

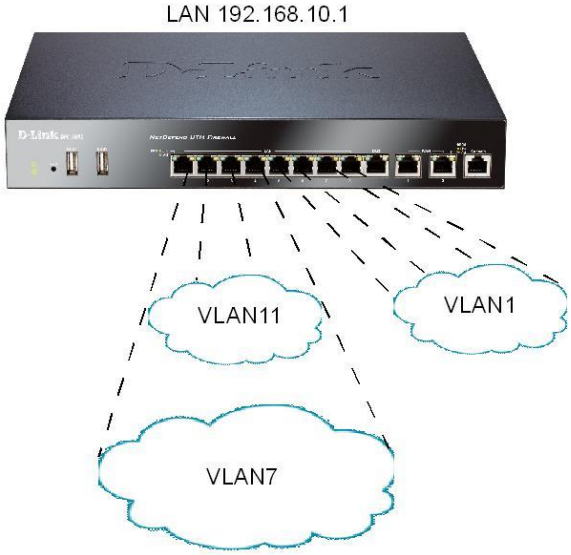
Destination Interface	all-wan
Destination Network	all-nets
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	allow-smtp-int
Action	Allow
Service	smtp
Source Interface	any
Source Network	all-nets
Destination Interface	dmz
Destination Network	mail-server
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	allow-ftp
Action	Allow
Service	ftp-passthrough
Source Interface	vlan2
Source Network	vlan2net
Destination Interface	dmz
Destination Network	dmznet
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	

```
gw-world:/> set IP4Address InterfaceAddresses/lan1_ip Address=192.168.10.1
gw-world:/> set IP4Address InterfaceAddresses/lan1net Address=192.168.10.0/24
gw-world:/> set IP4Address InterfaceAddresses/lan2_ip Address=192.168.20.1
gw-world:/> set IP4Address InterfaceAddresses/lan2net Address=192.168.20.0/24
gw-world:/> set IP4Address InterfaceAddresses/lan3_ip Address=192.168.30.1
gw-world:/> set IP4Address InterfaceAddresses/lan3net Address=192.168.30.0/24
gw-world:/> set IP4Address InterfaceAddresses/dmz_ip Address=172.17.100.254
gw-world:/> set IP4Address InterfaceAddresses/dmznet Address=172.17.100.0/24
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=192.168.110.1
gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=192.168.110.0/24
gw-world:/> set IP4Address InterfaceAddresses/wan1_gw Address=192.168.110.254
gw-world:/> set IP4Address InterfaceAddresses/wan2_ip Address=192.168.120.1
gw-world:/> set IP4Address InterfaceAddresses/wan2net Address=192.168.120.0/24
gw-world:/> set IP4Address InterfaceAddresses/wan2_gw Address=192.168.120.254
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address vlan1_ipAddress=192.168.5.254
gw-world:/labs> add IP4Address vlan1netAddress=192.168.5.0/24
gw-world:/labs> add IP4Address vlan2_ipAddress=192.168.6.254
gw-world:/labs> add IP4Address vlan2netAddress=192.168.6.0/24
gw-world:/labs> add IP4Address ftp-server Address=172.17.100.1
gw-world:/labs> add IP4Address mail-server Address=172.17.100.2
gw-world:/labs> cc
gw-world:/labs> add IP4Group all-lannets
Members=InterfaceAddresses/lan1net,InterfaceAddresses/lan2net,labs/vlan1net,labs/vlan2net
gw-world:/> set Interface Ethernet wan1 AutoDefaultGatewayRoute=No AutoInterfaceNetworkRoute=No
gw-world:/> set Interface Ethernet wan2 AutoDefaultGatewayRoute=No AutoInterfaceNetworkRoute=No
gw-world:/> cc RoutingTable main
gw-world:/main> add Route Interface=wan1 Network=all-nets Gateway=InterfaceAddresses/wan1_gw
Metric=90
```

gw-world:/main> add Route Interface=wan2 Network=all-netsGateway=InterfaceAddresses/wan2_gw Metric=80
gw-world:/main> cc
gw-world:/>add Interface VLAN vlan1Ethernet=lan3 IP=labs/vlan1_ip Network=labs/vlan1net VLANID=1
gw-world:/> add Interface VLAN vlan2 Ethernet=lan3 IP=labs/vlan2_ip Network=labs/vlan2net VLANID=2
gw-world:/> add Interface InterfaceGroup all-lan Members=lan1,lan2,vlan1,vlan2
gw-world:/> add Interface InterfaceGroup all-wan Members=wan1,wan2 Equivalent=Yes
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=NAT DestinationInterface=all-wan DestinationNetwork=all-nets Service=http-all SourceInterface=all-lan SourceNetwork=labs/vlannet1 Name=allow-http-all
gw-world:/1(labs)> add IPRule Action=NAT DestinationInterface=all-wan DestinationNetwork=all-nets Service=http-all SourceInterface=all-lan SourceNetwork=labs/vlannet1 Name=allow-dns-all
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=dmz DestinationNetwork=labs/mail-server Service=smtp SourceInterface=any SourceNetwork=all-nets Name=allow-smtp-int
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=dmz DestinationNetwork=InterfaceAddresses/dmznet Service=ftp-passthrough SourceInterface=vlan2 SourceNetwork=labs/vlan2net Name=allow-ftp
gw-world:/1(labs)> cc
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Упражнение	Проверьте доступность FTP-сервера, почтового сервера для пользователей сетей **lan1**, **lan2**, **lan3**.
Microsoft Outlook Express	Отправьте/получите электронную почту.
Internet Explorer ОС Windows	ftp://<ftp-server>

Настройка Switch Management (Port based VLAN)

Описание сценария	*Для встроенного коммутатора межсетевого экрана DFL-860E необходимо 1 и 4 порты отнести к VLAN7, а 2 и 3 – к VLAN11. Оставшиеся порты будут ассоциироваться с VLAN 1.*
Схема 74	

Настройка DFL-860E

Web-интерфейс

Создание необходимых объектов

Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:

Name	vlannet7_ip
Address	192.168.7.1
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	vlannet7
Address	192.168.7.0/24
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	vlannet11_ip
Address	192.168.11.1
Зайдите в меню *Objects Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	vlannet11
Address	192.168.11.0/24
Создадим VLAN-интерфейсы. Зайдите в меню *Interfaces→VLAN→Add→VLAN.* Во вкладке *General* введите следующие параметры*:*	
Name	vlan7
Interface	Укажите интерфейс lan
IP Address	vlannet7_ip
Network	vlannet7
VLAN ID	Укажите корректный VID - 7.
Зайдите в меню *Objects→Interfaces→Add→VLAN.* Во вкладке *General* введите следующие параметры:	
Name	vlan11
Interface	Укажите интерфейс lan
IP Address	vlannet11_ip
Network	vlannet11
VLAN ID	Укажите корректный VID - 11.
Настроим Port based VLAN. Зайдите в меню *Interfaces→Switch Management.* Во вкладке *General* введите следующие параметры*:*	
Enable Port based VLAN	Поставьте галочку
Port 1	vlan7
Port 2	vlan11
Port 3	vlan11
Port 4	vlan7
Port 5	(None)
Создание IP Rule	
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	vlan7_rule
Action	Allow
Service	all-services
Source Interface	vlan7
Source Network	vlannet7
Destination Interface	any
Destination Network	all-nets
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	vlan11_rule

Action	Allow
Service	all-services
Source Interface	vlan11
Source Network	vlannet2
Destination Interface	any
Destination Network	all-nets

Зайдите в меню *Configuration* и выберите *Save and Activate*.

Командная строка (CLI)

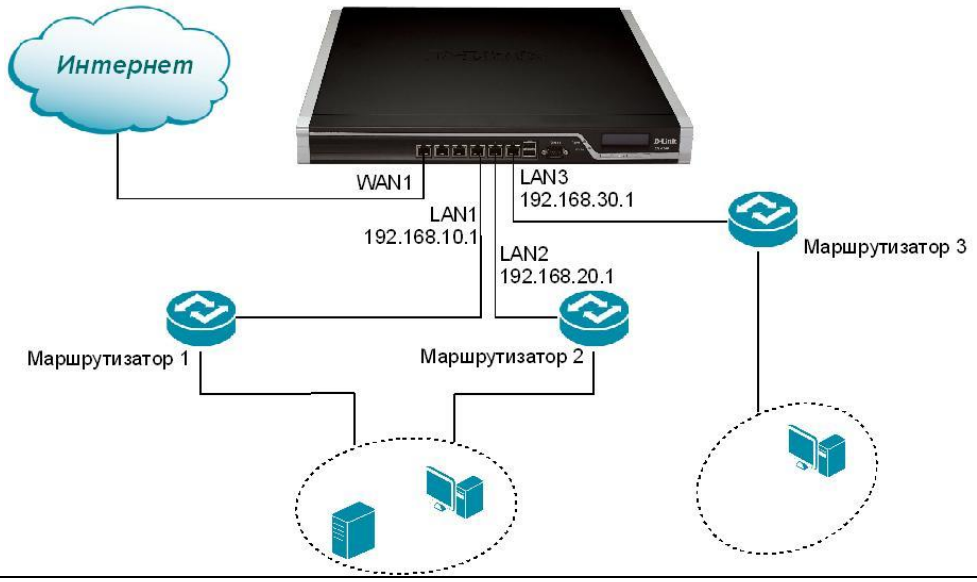
```
gw-world:/> set IP4Address InterfaceAddresses/lan_ip Address=192.168.10.1
gw-world:/> set IP4Address InterfaceAddresses/lannet Address=192.168.10.0/24
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address vlannet7_ipAddress=192.168.7.1
gw-world:/labs> add IP4Address vlannet7Address=192.168.7.0/24
gw-world:/labs> add IP4Address vlannet11_ipAddress=192.168.11.1
gw-world:/labs> add IP4Address vlannet11Address=192.168.11.0/24
gw-world:/labs> cc
gw-world:/>add Interface VLAN vlan7Ethernet=lan IP=labs/vlannet7_ip Network=labs/vlannet7 VLANID=7
gw-world:/> add Interface VLAN vlan11 Ethernet=lan IP=labs/vlannet11_ip Network=labs/vlannet11 VLANID=11
gw-world:/> set SwitchManagement EnableVLAN=Yes Port1=vlan7 Port2=vlan11 Port3=vlan11 Port4=vlan7
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=any DestinationNetwork=all-nets Service=all-services SourceInterface=vlan7 SourceNetwork=labs/vlannet7Name=vlan7_rule
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=any DestinationNetwork=all-nets Service=all-services SourceInterface=vlan11 SourceNetwork=labs/vlannet11 Name=vlan11_rule
gw-world:/1(labs)> cc
gw-world:/> activate (подождать 3-5 секунд)
gw-world:/>commit
```

ЗАНЯТИЕ №20. Управление маршрутизацией, протокол OSPF на межсетевом экране.

На межсетевом экране серии DFL может быть настроена динамическая маршрутизация на основе протокола OSPF. Таким образом, можно обеспечить автоматический выбор оптимального маршрута в крупных сетях или настроить межсетевой экран, как маршрутизатор OSPF в некоторой отдельной области сети.

Цель	Эта лабораторная работа предназначена для ознакомления пользователей с настройкой протокола OSPF на межсетевых экранах D-Link	
Оборудование	DFL-1660	1
	Рабочая станция	2
	Ethrenet-кабель (патч-корд)	5
	Маршрутизатор с поддержкой OSPF	3

Описание OSPF	*Протокол OSPF – наиболее широко используемый LS-алгоритм. Маршрутизатор, поддерживающий OSPF, определяет непосредственно подключенные к нему другие маршрутизаторы и подсети. Затем OSPF-маршрутизатор широковещательно рассылает информацию всем остальным маршрутизаторам, каждый из которых, используя получаемую информацию, строит таблицу маршрутизации (routing table). После построения таблицы маршрутизации каждый маршрутизатор может определить подсети и другие маршрутизаторы, ведущие к определенному узлу. OSPF-маршрутизаторы широковещательно рассылают только модифицированную информацию, а не всю таблицу маршрутизации целиком. Протокол OSPF поддерживает маршрутизацию исходя из метрик пути к удаленному хосту, полосы пропускания, загрузки канала, задержки и др.* *OSPF в межсетевых экранах D-Link реализован как алгоритм динамической маршрутизации.*
Описание сценария	*Настроим OSPF-процесс на межсетевом экране. К интерфейсу **lan3** межсетевого экрана подключено несколько локальных сетей, здесь устройство контролирует только путь в подсеть. К интерфейсам **lan1** и **lan2** подключены большие локальные сети. Некоторые сети будут доступны через оба интерфейса (lan1 и lan2), таким образом может быть получена некоторая избыточность при недоступности одного пути маршрутизации. Этого можно достичь путем помещения интерфейсов **lan1** и **lan2** в интерфейсную группу равноценной безопасности (security equivalent interface group).* *Используется один OSPF-процесс и одна OSPF-область – основная область 0.0.0.0. Три интерфейса (lan1, lan2, lan3)добавляются в область для того, чтобы межсетевой экран стал участником OSPF-процесса. При этом никакие известные маршруты не добавляются в таблицу маршрутизации и соседние маршрутизаторы не оповещаются о каких либо статических маршрутах (кроме маршрутов этих трех интерфейсов, участвующих в OSPF-процессе).*

Схема 75	

Настройка DFL-1660

Web-интерфейс

Убедитесь в правильных настройках параметров интерфейсов:

Name	lan1net
Address	192.168.10.0/24
Name	lan1_ip
Address	192.168.10.1
Name	lan2net
Address	192.168.20.0/24
Name	lan2_ip
Address	192.168.20.1
Name	lan3net
Address	192.168.30.0/24
Name	lan3_ip
Address	192.168.30.1

Настройка OSPF-процесса

Добавим OSPF-процесс. Зайдите в меню *Routing→OSFP→Add→OSPF Router Process*. Во вкладке *General* введите:

Name	ospf-proc1
Router ID	lan1_ip
Reference Bandwidth	1 Gbps (полоса пропускания на интерфейсе)

Во вкладке *Authentication* введите следующие параметры:

Passphrase	123456qw

Зайдите в меню *Routing→OSFP→ospf-proc1→Add→OSPF Area*, во вкладке *General* введите:

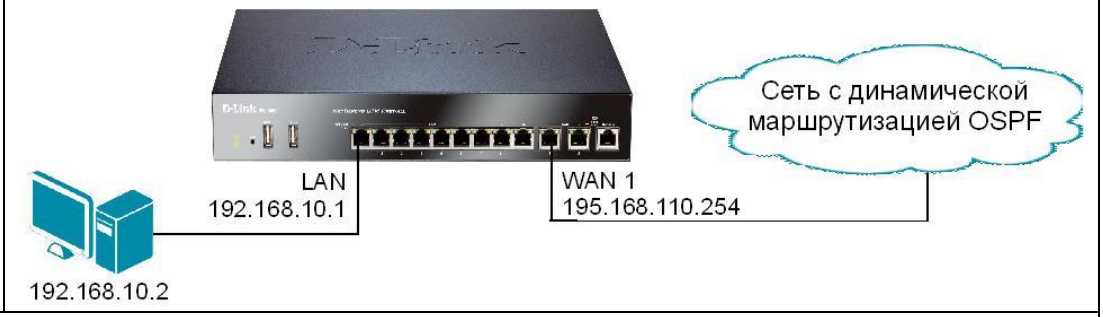
Name	area0
Area ID	0.0.0.0

Добавим интерфейсы, участвующие в OSPF-процессе. На странице конфигурации area0 зайдите в *OSPF Interfaces→Add→OSFP Interface*. Во вкладке *General* введите:

Interface	Выберите lan1 из списка интерфейсов (lan1 должен быть определен в Ethernet-интерфейсах).
Network	lan1net (или None)
Interface Type	Broadcast
Metric/Bandwidth	Поставьте метрику или выберите ширину канала – 1000 Мбит/с.
Добавим интерфейс lan2. На странице конфигурации area0 зайдите в *OSPF Interfaces→Add→OSFP Interface.* Во вкладке *General* введите:	
Interface	Выберите lan2 из списка интерфейсов (lan2 должен быть определен в Ethernet-интерфейсах).
Network	lan2net (или None)
Interface Type	Broadcast
Metric/Bandwidth	Поставьте метрику или выберите ширину канала – 1000 Мбит/с.
Добавим интерфейс lan3. На странице конфигурации area0 зайдите в *OSPF Interfaces→Add→OSFP Interface.* Во вкладке *General* введите:	
Interface	Выберите lan3 из списка интерфейсов (lan3 должен быть определен в Ethernet-интерфейсах).
Network	lan3net (или None)
Interface Type	Broadcast
Metric/Bandwidth	Поставьте метрику или выберите ширину канала – 1000 Мбит/с.
Добавим интерфейсную группу равноценной безопасности для интерфейсов lan1 и lan2. Зайдите в *Interfaces→Interface Groups→Add→Interface Group.* Во вкладке *General* введите:	
Name	ifgrp-ospf1
Security/Transport Equivalent	Поставьте галочку
В разделе *Interfaces* переместите интерфейсы lan1 и lan2 из списка Available в список Selected.	
Примечание: Необходимо убедиться в правильной настройке уже существующих IP Rule для этих интерфейсов. Созданная интерфейсная группа должна быть выбрана в качестве интерфейса источника (Source Interface).	
Настройка импорта маршрутов из OSPF в главную таблицу маршрутизации.	
Добавим все маршруты, полученные от ospf-proc1 в главную таблицу маршрутизации, если это не сделано автоматически межсетевым экраном. Зайдите в *Routing→Dynamic Routing Rules→Add→Dynamic Routing Policy Rule*. Во вкладке *General* введите:	
Name	importOSPFRoutes
From OSPF Process	Выберите ospf-proc1 из списка Available и переместите в список Selected.
Destination Network ***…Or is within***	all-nets
Добавим действие маршрутизации (Routing Actions). На странице import OSPF Routes зайдите в *Routing Actions→Add→DynamicRoutingRuleAddRoute*. Во вкладке *General* введите:	
Destination	Выберите главную таблицу маршрутизации main из списка Available и переместите в список Selected.
Примечание: В результате указанного выше конфигурирования межсетевого экрана вся информация о найденных маршрутах будет добавляться в главную таблицу маршрутизации так долго, пока она не покроет любые статические маршруты или ранее заданные маршруты по умолчанию.	
Настройка экспорта маршрута по умолчанию (default troute) в OSPF.	
Экспортируем только маршрут по умолчанию из главной таблицы маршрутизации в OSPF-процесс ospf-proc1. Зайдите в меню *Routing→Dynamic Routing Rules→Add→Dynamic Routing Policy Rule.* Во вкладке *General* введите:	
Name	exportDefRoute

From OSPF Process	Выберите главную таблицу маршрутизации из списка Available и переместите в список Selected.
В разделе *Destination Network* введите:	
Exactly Matches	all-nets
Добавим действие OSPF. На странице exportDefRoute зайдите в *OSPF Actions→Add→Export OSPF*. Во вкладке *General* введите:	
Export to process	Выберите ospf-proc1 из списка.
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> set IP4Address InterfaceAddresses/lan1_ip Address=192.168.10.1 gw-world:/> set IP4Address InterfaceAddresses/lan1net Address=192.168.10.0/24 gw-world:/> set IP4Address InterfaceAddresses/lan2_ip Address=192.168.20.1 gw-world:/> set IP4Address InterfaceAddresses/lan2net Address=192.168.20.0/24 gw-world:/> set IP4Address InterfaceAddresses/lan3_ip Address=192.168.30.1 gw-world:/> set IP4Address InterfaceAddresses/lan3net Address=192.168.30.0/24 gw-world:/>add OSPFProcess ospf-proc1RouterID=InterfaceAddresses/lan1_ip RefBandwidthUnit=Gbps RefBandwidthValue=1 AuthType=Passphrase AuthPassphrase=123456qw gw-world:/>cc OSPFProcess ospf-proc1 gw-world:/ospf-proc1> add OSPFArea area0 AreaID=0.0.0.0 gw-world:/ospf-proc1>cc OSPFArea area0 gw-world:/ospf-proc1/area0>add OSPFInterface lan1 Network=InterfaceAddresses/lan1net Type=Broadcast MetricType=Bandwidth BandwidthValue=1 UseDefaultAuth=Yes gw-world:/ospf-proc1/area0>add OSPFInterface lan2 Network=InterfaceAddresses/lan2net Type=Broadcast MetricType=Bandwidth BandwidthValue=1 UseDefaultAuth=Yes gw-world:/ospf-proc1/area0> add OSPFInterface lan3 Network=InterfaceAddresses/lan3net Type=Broadcast MetricType=Bandwidth BandwidthValue=1 UseDefaultAuth=Yes gw-world:/ospf-proc1/area0> cc gw-world:/>add Interface InterfaceGroup ifgrp-ospf1 Members=lan1,lan2 gw-world:/>add DynamicRoutingRule OSPFProcess=ospf-proc1 Name=importOSPFRoutes From=OSPF DestinationNetworkIn=all-nets Index=1 gw-world:/>cc DynamicRoutingRule 1(importOSFPRoutes) gw-world:/1(importOSFPRoutes)> add DynamicRoutingRuleAddRoute Destination=main gw-world:/1(importOSFPRoutes)> cc gw-world:/>add DynamicRoutingRule OSPFProcess=ospf-proc1 From=RTable RoutingTable=main DestinationNetworkExactly=all-nets Index=2 Name=exportDefRoute gw-world:/> cc DynamicRoutingRule 2(exportDefRoute) gw-world:/2(exportDefRoute)> add DynamicRoutingRuleExportOSPF ExportToProcess=ospf-proc1 gw-world:/2(exportDefRoute)> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Настройка службы маршрутизации и удаленного доступа (RRAS) в Microsoft Windows Server 2003 в качестве OSPF-маршрутизатора 1	
Зайдите в *Network connections*, переименуйте интерфейсы маршрутизатора в WAN1 и WAN2, задайте им IP-адреса 192.168.10.25/24 и 10.25.2.25/24 соответственно.	
Откройте консоль Маршрутизация и удаленный доступ, убедитесь, что служба запущена. Откройте *Свойства*, нажав правой кнопкой мыши по имени сервера, введите следующие параметры на вкладке *Общие*:	
Использовать этот компьютер как IP4-маршрутизатор	Локальной сети
Откройте *IP Routing→OSPF*, нажав правой кнопкой мыши, выберите *New Interface*, для	

интерфейса WAN1 ведите следующие параметры:	
Enable OSPF for this address	Поставьте галочку
Area ID	0.0.0.0
Router priority	0
Cost	2
Password	123456qw
Network type	Broadcast
Откройте *IP Routing→OSPF*, нажав правой кнопкой мыши, выберите *New Interface*, для интерфейса WAN2 ведите следующие параметры:	
Enable OSPF for this address	Поставьте галочку
Area ID	0.0.0.1
Router priority	2
Cost	2
Password	12345678
Network type	Broadcast
При необходимости перезапустите службу RRAS.	
Настройка службы маршрутизации и удаленного доступа (RRAS) в Microsoft Windows Server 2003 в качестве OSPF-маршрутизатора 2	
Зайдите в *Network connections*, переименуйте интерфейсы маршрутизатора в WAN1 и WAN2, задайте им IP-адреса 192.168.20.10/24 и 10.25.2.5/24 соответственно.	
Откройте консоль Маршрутизация и удаленный доступ, убедитесь, что служба запущена. Откройте *Свойства*, нажав правой кнопкой мыши по имени сервера, введите следующие параметры на вкладке *Общие*:	
Использовать этот компьютер как IP4-маршрутизатор	Локальной сети
Откройте *IP Routing→OSPF*, нажав правой кнопкой мыши, выберите *New Interface*, для интерфейса WAN1 ведите следующие параметры:	
Enable OSPF for this address	Поставьте галочку
Area ID	0.0.0.0
Router priority	4
Cost	2
Password	123456qw
Network type	Broadcast
Откройте *IP Routing→OSPF*, нажав правой кнопкой мыши, выберите *New Interface*, для интерфейса WAN2 ведите следующие параметры:	
Enable OSPF for this address	Поставьте галочку
Area ID	0.0.0.1
Router priority	7
Cost	3
Password	12345678
Network type	Broadcast
При необходимости перезапустите службу RRAS.	
Настройка службы маршрутизации и удаленного доступа (RRAS) в Microsoft Windows Server 2003 в качестве OSPF-маршрутизатора 3	

Зайдите в *Network connections*, переименуйте интерфейсы маршрутизатора в WAN1 и WAN2, задайте им IP-адреса 192.168.30.10/24 и 10.210.10.2/24 соответственно.	
Откройте консоль Маршрутизация и удаленный доступ, убедитесь, что служба запущена. Откройте *Свойства*, нажав правой кнопкой мыши по имени сервера, введите следующие параметры на вкладке *Общие*:	
Использовать этот компьютер как IP4-маршрутизатор	Локальной сети
Откройте *IP Routing→OSPF*, нажав правой кнопкой мыши, выберите *New Interface*, для интерфейса WAN1 ведите следующие параметры:	
Enable OSPF for this address	Поставьте галочку
Area ID	0.0.0.0
Router priority	9
Cost	2
Password	123456qw
Network type	Broadcast
Откройте *IP Routing→OSPF*, нажав правой кнопкой мыши, выберите *New Interface*, для интерфейса WAN2 ведите следующие параметры:	
Enable OSPF for this address	Поставьте галочку
Area ID	0.0.0.2
Router priority	10
Cost	2
Password	1234567890
Network type	Non-broadcast multiple access (NBMA)
При необходимости перезапустите службу RRAS.	
Упражнение	Проверьте работу протокола OSPF. Убедитесь в наличии динамических маршрутов на устройствах, зайдите *Status→Routes*.
Проверьте анонсирование маршрута по умолчанию для маршрутизаторов 1,2, 3. Зайдите в меню *IP Routing→OSPF→Show Link-state Database*.	
Настройка OSPF на интерфейсе wan1 межсетевого экрана	
Описание сценария	*В существующей крупной динамически маршрутизируемой сети необходимо настроить межсетевой экран в качестве участника OSPF-процесса в OSPF-области 0.0.0.0. Подключение к сети, маршрутизируемой с помощью OSPF, осуществляется через **wan1**-интерфейс устройства.*
Схема 76	
Настройка DFL-860E	
Web-интерфейс	

Настройка OSPF-процесса	
Добавим OSPF-процесс. Зайдите в меню *Routing→OSPF→Add→OSPF Router Process.* Во вкладке *General* введите:	
Name	ospf-proc1
Router ID	wan1_ip (межсетевой экран подключаем к динамически маршрутизируемой сети через интерфейс wan1)
Reference Bandwidth	1000 Mbps
Во вкладке *Authentication* введите следующие параметры:	
Passphrase	123456qw (введите аутентификацию в OSPF)
Зайдите в меню *Routing→OSPF→ospf-proc1→Add→OSPF Area*, во вкладке *General* введите:	
Name	area0
Area ID	0.0.0.0
Добавим интерфейсы, участвующие в OSPF-процессе. На странице конфигурации area0 зайдите в *OSPF Interfaces→Add→OSPF Interface.* Во вкладке *General* введите:	
Interface	wan2
Network	None
Interface Type	Auto
Bandwidth	1000 Mbps
Во вкладке *Advanced* введите:	
No OSPF routers connected to this interface ("Passive")	Поставьте галочку
На странице конфигурации area0 зайдите в *OSPF Interfaces→Add→OSPF Interface.* Во вкладке *General* введите:	
Interface	dmz
Network	None
Interface Type	Auto
Bandwidth	1000 Mbps
Во вкладке *Advanced* введите:	
No OSPF routers connected to this interface ("Passive")	Поставьте галочку
На странице конфигурации area0 зайдите в *OSPF Interfaces→Add→OSPF Interface.* Во вкладке *General* введите:	
Interface	lan
Network	None
Interface Type	Auto
Bandwidth	1000 Mbps
Во вкладке *Advanced* введите:	
No OSPF routers connected to this interface ("Passive")	Поставьте галочку
На странице конфигурации area0 зайдите в *OSPF Interfaces→Add→OSPF Interface.* Во вкладке *General* введите:	
Interface	wan1
Network	None
Interface Type	Point-to-point
Bandwidth	1000 Mbps
Во вкладке *Advanced* введите:	

No OSPF routers connected to this interface ("Passive")	Уберите галочку
Настройка импорта маршрутов из OSPF в главную таблицу маршрутизации.	
Добавим все маршруты, полученные от ospf-proc1 в главную таблицу маршрутизации, если это не сделано автоматически межсетевым экраном. Зайдите в *Routing→Dynamic Routing Rules→Add→Dynamic Routing Policy Rule*. Во вкладке *General* введите:	
Name	importOSPFRoutes
From OSPF Process	Выберите ospf-proc1 из списка Available и переместите в список Selected.
Destination Network ***…Or is within***	all-nets
Добавим действие маршрутизации (Routing Action). На странице importOSPFRoutes зайдите в *Routing Actions→Add→DynamicRoutingRuleAddRoute*. Во вкладке *General* введите:	
Destination	Выберите главную таблицу маршрутизации main из списка Available и переместите в список Selected.
Примечание: В результате указанного выше конфигурирования межсетевого экрана вся информация о найденных маршрутах будет добавляться в главную таблицу маршрутизации так долго, пока она не покроет любые статические маршруты или ранее заданные маршруты по умолчанию.	
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.168.110.254 gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.168.110.0/24 gw-world:/>add OSPFProcess ospf-proc1 RouterID=InterfaceAddresses/wan1_ip RefBandwidthUnit=Gbps RefBandwidthValue=1 AuthType=Passphrase AuthPassphrase=123456qw gw-world:/>cc OSPFProcess ospf-proc1 gw-world:/ospf-proc1> add OSPFArea area0 AreaID=0.0.0.0 gw-world:/ospf-proc1>cc OSPFArea area0 gw-world:/ospf-proc1/area0>add OSPFInterface lan Type=Auto MetricType=Bandwidth BandwidthValue=1 UseDefaultAuth=Yes Passive=Yes gw-world:/ospf-proc1/area0>add OSPFInterface wan2 Type=Auto MetricType=Bandwidth BandwidthValue=1 UseDefaultAuth=Yes Passive=Yes gw-world:/ospf-proc1/area0> add OSPFInterface dmz Type=Auto MetricType=Bandwidth BandwidthValue=1 UseDefaultAuth=YesPassive=Yes gw-world:/ospf-proc1/area0> add OSPFInterface wan1 Type=Point-to-pointMetricType=Bandwidth BandwidthValue=1 UseDefaultAuth=Yes gw-world:/ospf-proc1/area0> cc gw-world:/>add DynamicRoutingRule OSPFProcess=ospf-proc1 Name=importOSPFRoutes From=OSPF DestinationNetworkIn=all-nets Index=1 gw-world:/>cc DynamicRoutingRule 1(importOSFPRoutes) gw-world:/1(importOSFPRoutes)> add DynamicRoutingRuleAddRoute Destination=main gw-world:/1(importOSFPRoutes)> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Упражнение	Проверьте работу протокола OSPF. Убедитесь в наличии динамических маршрутов на устройстве, зайдите в меню *Status→Routes.*

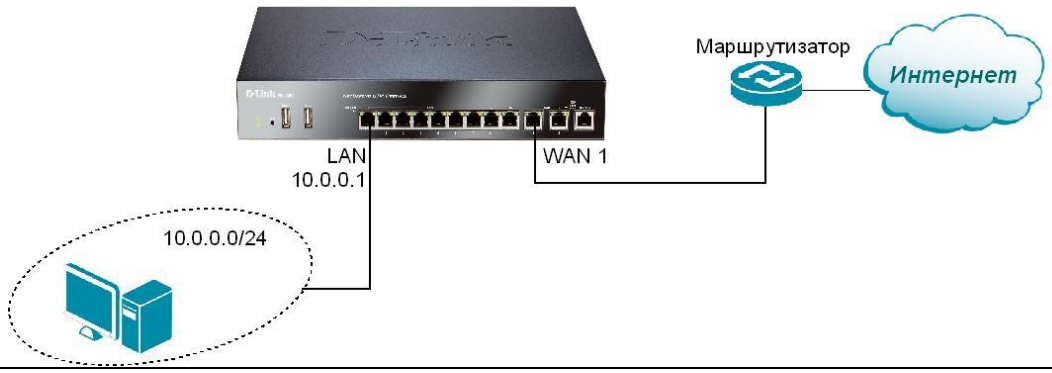
ЗАНЯТИЕ №21. Режим Transparent Mode. Настройка сетевой защиты с помощью системы IDP/IPS для прозрачного режима работы интерфейсов межсетевого экрана (функция сенсора уровня 2).

Межсетевой экран может работать в режиме коммутатора второго уровня без осуществления маршрутизации. Этот режим называется прозрачным режимом – Transparent Mode.

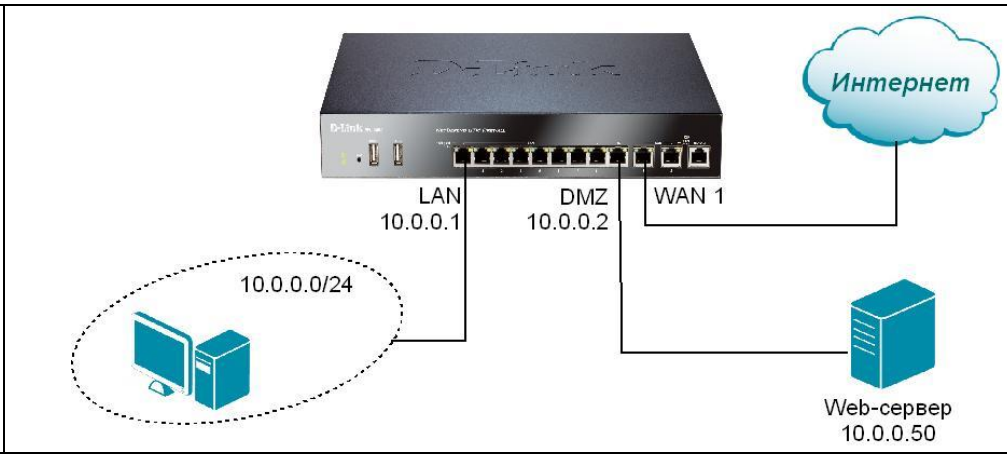
Цель	Эта лабораторная работа позволяет пользователям изучить настройку Transparent Mode на межсетевом экране	
Оборудование	DFL-860E	1
	Рабочая станция	2
	Ethernet-кабель (патч-корд)	4

Описание технологии	*Transparent Mode – технология межсетевых экранов D-Link, позволяющая упростить применение технологий безопасности межсетевого экрана для существующей топологии сети. Технология позволяет упростить работу администратора в смысле отсутствия необходимости переконфигурирования всех настроек узлов (nodes) в пределах текущей сети, когда межсетевой экран подключается к общему потоку коммуникаций.* *Прозрачность означает видимость хостов по обе стороны от межсетевого экрана. Для пользователей прозрачность означает «не обнаружение межсетевого экрана» в потоке пакетов.* *Можно выделить следующие преимущества режима прозрачности:* *- отсутствие необходимости переконфигурирования, клиенты могут оставаться с той же конфигурацией сети, что и до установки межсетевого экрана,* *- не добавляются сложности доступа к службам, использование межсетевого экрана невидимо для внешних пользователей,* *- дополнительная безопасность.* *Межсетевой экран может работать только в двух режимах: Routing Mode и Transparent Mode. В режиме Routing Mode межсетевой экран действует в качестве маршрутизатора 3-го уровня. Если межсетевой экран размещается в сети впервые, или происходят изменения любых узлов в сети, конфигурация маршрутизации должна быть заново перенастроена для построения новой таблицы маршрутизации. Переконфигурация IP-настроек затронет существующие маршрутизаторы и защищенные сервера. Режим Routing Mode используется для полного контроля над маршрутизацией, для максимальной возможной безопасности. Например, для случая защищенного сервера, который должен получать только необходимый контролируемый трафик.* *В режиме Transparent Mode межсетевой экран работает, как коммутатор 2 уровня. Он отслеживает прохождение IP-пакетов через устройство на соответствующий интерфейс, без модификации какой либо информации об источнике и назначении. Все «прозрачные» интерфейсы относят к одной и той же подсети, таким образом клиенты могут перемещаться между*

	различными интерфейсами, при этом службы будут также доступны без переконфигурации маршрутизации. В «прозрачном» режиме межсетевой экран разрешает ARP-транзакции и разучивает, исходя из ARP-трафика, соответствие между IP-адресом и физическим адресом источника и назначения. При транзакции ни одна из конечных сторон не замечает работу межсетевого экрана между ними. *Для настройки Transparent Mode необходимо настроить следующие параметры на межсетевом экране:* *- сгруппировать интерфейсы, которые будут использованы в режиме Transparent Mode,* *- создать Switch Route. В случае интерфейса – это интерфейс выбранной ранее интерфейсной группы. В случае подсети – это диапазон адресов, которые должны быть «прозрачны» между интерфейсами. Если весь межсетевой экран работает в режиме Transparent Mode, то это обычно подсеть 0.0.0.0/0.* *При инициализации коммуникаций хост определяет физический адрес другого хоста посредством выдачи широковещательного ARP-запроса. Межсетевой экран, перехватывая этот ARP-запрос, задает ARP Transaction State внутри межсетевого экрана и широковещательно передает ARP-запрос всем остальным подобным интерфейсам, кроме интерфейса, с которого первоначально и пришел ARP-запрос. Если межсетевой экран получает ARP-ответ от узла назначения в пределах трехсекундного таймаута, устройство перешлет ответ отправителю запроса, используя сохраненную в ARP Transaction State информацию.* *В процессе ARP-транзакции межсетевой экран узнает информацию об адресе источника с обеих сторон запроса и ответа. В межсетевом экране существуют две таблицы, хранящие эту информацию – Content-Addressable Memory (CAM) Table и Layer 3 Cache.* *CAM-таблица содержит информацию о MAC-адресах, доступных на данном физическом интерфейсе межсетевого экрана, таблица Layer 3 Cache содержит связи между IP-адресами, MAC-адресами и интерфейсом. Т.к. Layer 3 Cache используется только для IP-трафика, то записи сохраняются как данные для одного хоста в таблице маршрутизации.* *Для каждого IP-пакета, проходящего через межсетевой экран, будет производиться запрос маршрутизации до узла назначения (routelookup). При совпадении маршрута пакета с маршрутизацией коммутатора или записями Layer 3 Cache в таблице маршрутизации, то межсетевой экран должен его соответственно обработать в режиме «прозрачности». Если интерфейс назначения и MAC-адрес доступны в маршруте, межсетевой экран будет обладать необходимой информацией для направления пакета к узлу назначения. В случае отсутствия информации об узле назначения, межсетевой экран будет определять маршрут путем ARP-запросов, действуя в качестве инициатора отправления исходного IP-пакета. При получении ARP-ответа межсетевой экран обновит записи CAM-таблицы и Layer 3 Cache и перешлет пакет к узлу назначения. При переполнении CAM-таблицы или таблицы Layer 3 Cache будут автоматически очищены. Удаленные записи могут быть снова*

	восстановлены, используя механизм маршрутизации.
Описание сценария	*Межсетевой экран в существующей сети расположен между шлюзом доступа в Интернет и внутренней сетью, что не влечет необходимость переконфигурирования клиентов во внутренней сети. Маршрутизатор используется для подключения к Интернету, использующему один публичный IP-адрес. Внешняя сеть за NAT располагается в адресном пространстве 10.0.0.0/24. Клиенты внутренней сети должны иметь возможность выходить в Интернет по протоколу HTTP.* *Для повышения эффективности автоматического поиска хостов интерфейсы **wan1** и **lan** межсетевого экрана должны быть сконфигурированы дополнительно.*
Схема 77	
Настройка DFL-860E	
Web-интерфейс	
Отредактируем интерфейсы wan1 и lan. Зайдите в меню *Interfaces→Ethernet→wan1*. Во вкладке *General* введите следующие параметры:	
IP Address	wan_ip
Network	wannet
Enable transparent mode	Поставьте галочку
Зайдите в меню *Interfaces→Ethernet→lan*. Во вкладке *General* введите следующие параметры:	
IP Address	lan_ip
Network	lannet
Enable transparent mode	Поставьте галочку
Добавим интерфейсную группу равноценной безопасности для интерфейсов lan и wan1. Зайдите в меню *Interfaces→Interface Groups→Add→Interface Group*. Во вкладке *General* введите:	
Name	lanwan
Security/Transport Equivalent	Поставьте галочку
Interfaces	Добавьте lan и wan1 из Available в Selected
Создадим маршрут Switch Route в маршрутной таблице. Зайдите в меню *Routing→Routing table→main→Add→Switch Route*. Во вкладке General введите:	
Switch Interfaces	lanwan
Network	wan1net
Metric	0
Настроем IP Rules. Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Введите следующие параметры:	
Name	HTTPAllow

Action	Allow
Service	http
Source Interface	lanwan
Destination Interface	lanwan
Source Network	lannet
Destination Network	all-nets
Удалите любые маршруты на интерфейсах wan1 и lan, кроме маршрута Switch Route.	
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> set IP4Address InterfaceAddresses/lan_ip Address=10.0.0.1 gw-world:/> set IP4Address InterfaceAddresses/lannet Address=10.0.0.0/24 gw-world:/>set Interface Ethernet wan1 IP=InterfaceAddresses/lan_ip Network=InterfaceAddresses/lannet AutoSwitchRoute=Yes gw-world:/>set Interface Ethernet lanIP=InterfaceAddresses/lan_ip Network=InterfaceAddresses/lannetAutoSwitchRoute=Yes gw-world:/> add Interface InterfaceGroup lanwan Members=lan,wan1 gw-world:/>cc RoutingTable main gw-world:/main>add SwitchRoute Interface=lanwan Network=InterfaceAddresses/wan1net Index=1 Metric=0 gw-world:/main>cc gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=http SourceInterface=lanwan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=lanwan DestinationNetwork=all-nets Name=HTTPAllow gw-world:/1(labs)> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Упражнение	Проверьте наличие Интернета у пользователей **lan-**сети.
Internet Explorer ОС Windows	http://yandex.ru
Описание сценария	*Межсетевой экран в режиме Transparent Mode может быть использован для отделения серверных ресурсов от внешней сети путем подключения к разным интерфейсам. При этом нет необходимости создавать разное адресное пространство.* *Сервер обычно содержит ресурсы, к которым необходим доступ извне (из Интернета), поэтому сервера обычно помещают в отдельный интерфейс межсетевого экрана (**dmz**-интерфейс).* *В этом сценарии все хосты помещены в **lan**, **dmz** также использует одно общее адресное пространство 10.0.0.0/24. Т.к. используется Transparent Mode, то для сервера может быть использован любой IP-адрес, и для хостов внешней сети не важно, где ресурсы – в той же сети или в **dmz**. Таким образом, межсетевой экран становится прозрачным в коммуникациях между **dmz** и **lan**, несмотря на применяемые к трафику правила межсетевого экрана IP Rules.* *Разрешим хостам во внутренней сети взаимодействовать с Web-сервером, расположенным в **dmz**-зоне. Web-сервер настроем доступным из Интернета. Для разрешения дополнительного трафика должны быть созданы соответствующие правила.*

Схема 78	

Настройка DFL-860E

Web-интерфейс

Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	ip-webserver
Address	10.0.0.50
Настроем SwitchRoute на lan- и dmz-интерфейсах для адресного пространства 10.0.0.0/24. Wan-интерфейс должен быть сконфигурирован соответственно. Зайдите в меню *Interfaces→Ethernet→lan.* Введите следующие параметры:	
IP Address	10.0.0.1
Network	10.0.0.0/24 (lannet)
Enable transparent mode	Уберите галочку
Во вкладке *Advanced* введите следующие параметры:	
Automatically add a route for this interface using the given network.	Уберите галочку
Зайдите в меню *Interfaces→Ethernet→dmz.* Введите следующие параметры:	
IP Address	10.0.0.2
Network	10.0.0.0/24 (lannet)
Enable transparent mode	Уберите галочку
Во вкладке *Advanced* введите следующие параметры:	
Automatically add a route for this interface using the given network.	Уберите галочку
Создадим Interface Group. Зайдите в меню *Interfaces→Interface Groups→Add→Interface Group.* Введите следующие параметры:	
Name	Transparent_Group
Security/Transport Equivalent	Поставьте галочку
Во вкладке *Interfaces* переместите интерфейсы lan и dmz из списка Available в список Selected.	
Настроим Routing. Зайдите в меню *Routing→Routing Table→ main→Add→Switch Route.* Введите следующие параметры:	
Switched Interfaces	Transparent_Group
Network	10.0.0.0/24
Metric	0
Настроим IP Rules. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Введите следующие	

параметры:	
Name	HTTP-LAN-to-DMZ
Action	Allow
Service	http
Source Interface	lan
Destination Interface	dmz
Source Network	lannet
Destination Network	ip-webserver
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Введите следующие параметры:	
Name	HTTP-WAN-to-DMZ
Action	SAT
Service	http
Source Interface	wan1
Destination Interface	dmz
Source Network	lannet
Destination Network	wan1_ip
Введите параметры во вкладке *SAT*:	
Translate the	Destination IP Address
To New IP Address	ip-webserver
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Введите следующие параметры:	
Name	HTTP-WAN-to-DMZ-allow
Action	Allow
Service	http
Source Interface	wan1
Destination Interface	dmz
Source Network	lannet
Destination Network	wan1_ip
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> set IP4Address InterfaceAddresses/lan_ip Address=10.0.0.1 gw-world:/> set IP4Address InterfaceAddresses/lannet Address=10.0.0.0/24 gw-world:/>set Interface Ethernet lanIP=10.0.0.1 Network=InterfaceAddresses/lannetAutoSwitchRoute=Yes gw-world:/>set Interface Ethernet lanIP=10.0.0.2 Network=InterfaceAddresses/lannetAutoSwitchRoute=Yes gw-world:/> add Interface InterfaceGroup TransparentGroup Members=lan,dmz gw-world:/>cc RoutingTable main gw-world:/main>add SwitchRoute Interface=TransparentGroup Network=InterfaceAddresses/lannet Index=1 Metric=0 gw-world:/main>cc gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow Service=http SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=dmz DestinationNetwork=labs/ip-webserver Name=HTTP-LAN-to-DMZ gw-world:/1(labs)> add IPRule Action=SAT Service=http SourceInterface=wan1 SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip	

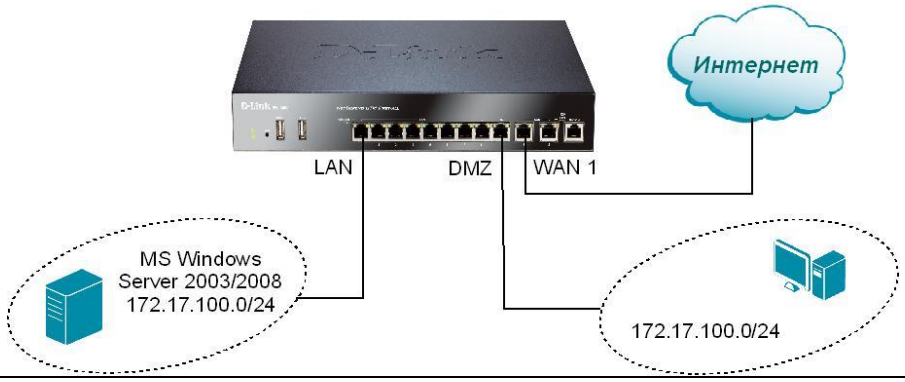
SATTranslateToIP=labs/ip-webserver SATTranslate DestinationIP Name=HTTP-WAN-to-DMZ
gw-world:/1(labs)> add IPRule Action=Allow Service=http SourceInterface=wan1 SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip Name=HTTP-WAN-to-DMZ-allow
gw-world:/1(labs)> cc
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Упражнение	Проверьте доступность Web-сервера, расположенного в dmz-зоне для пользователей **lan**-сети.
Internet Explorer ОС Windows	http://10.0.0.50

Настройка сетевой защиты с помощью системы IDP/IPS для прозрачного режима работы интерфейсов межсетевого экрана (функция сенсора уровня 2).

Описание сценария	*Необходимо обеспечить защиту сервера контроллера домена под управлением MS Windows Server 2003/2008 от атак на SMB (Server Messege Block), а также от использования злоумышленником других уязвимостей и эксплоитов проникновения. При этом сервер располагается в одной подсети с клиентскими компьютерами и другими серверами. Таким образом, порты служб Active Directory (AD) должны быть открыты для внутренней сети, и маршрутизация не осуществляется. Наложение сигнатур системы IDP/IPS на трафик служб AD поможет защитить сервер от атак из внутренней сети (атак «человек посередине»), порты AD (особенно SMB) закрыты для доступа из внешних сетей. Сервер контроллера домена размещается в **lan**-сети, клиенты AD и другие сервера – в **dmz**-сети (или других интерфейсах при необходимости в зависимости от модели межсетевого экрана).*

Схема 79



Настройка DFL-860E

Web-интерфейс

Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:

Name	ad-net
Address	172.17.100.0/24

Настроем Switch Route на lan- и dmz-интерфейсах для адресного пространства 172.17.100.0/24.

Создадим Interface Group. Зайдите в меню *Interfaces→Interface Groups→Add→Interface Group.* Введите следующие параметры:

Name	lan_dmz
Security/Transport Equivalent	Поставьте галочку

Во вкладке *Interfaces* переместите интерфейсы lan и dmz из списка Available в список Selected.

Настроим Routing. Зайдите в меню *Routing→ Routing Table→ main→Add→Switch Route.* Введите следующие параметры:	
Switched Interfaces	lan_dmz
Network	ad-net
Metric	0
Создание служб, необходимых для функционирования MS Active Directory	
Создадим службу LDAP. Зайдите в меню *Objects→Services*, добавьте TCP/UDP Service со следующими параметрами:	
Name	ldap
Type	TCP/UDP (выберите из списка)
Destination	389
SYN flood protection (SYN Relay)	Поставьте галочку
Создадим службы SMB. Зайдите в меню *Objects→Services*, добавьте TCP/UDP Service со следующими параметрами:	
Name	smb-all
Type	TCP/UDP (выберите из списка)
Destination	135-139,445
SYN flood protection (SYN Relay)	Поставьте галочку
Создадим службу аутентификации Kerberos. Зайдите в меню *Objects→Services*, добавьте TCP/UDP Service со следующими параметрами:	
Name	kerberos-auth
Type	UDP (выберите из списка)
Destination	88
Создадим службу смены паролей Kerberos. Зайдите в меню *Objects→Services*, добавьте TCP/UDP Service со следующими параметрами:	
Name	kerberos
Type	TCP/UDP (выберите из списка)
Destination	464
SYN flood protection (SYN Relay)	Поставьте галочку
Создадим службу DNS. Зайдите в меню *Objects→Services*, добавьте TCP/UDP Service со следующими параметрами:	
Name	dns-all
Type	TCP/UDP (выберите из списка)
Destination	53
SYN flood protection (SYN Relay)	Поставьте галочку
Создадим службу GC. Зайдите в меню *Objects→Services*, добавьте TCP/UDP Service со следующими параметрами:	
Name	gc
Type	TCP (выберите из списка)
Destination	3268,3269
SYN flood protection (SYN Relay)	Поставьте галочку
Создадим службу MSRPC. Зайдите в меню *Objects→Services*, добавьте TCP/UDP Service со следующими параметрами:	

Name	rpc
Type	TCP (выберите из списка)
Destination	1025
SYN flood protection (SYN Relay)	Поставьте галочку
Создадим Service Group из всех служб, необходимых для MS AD. Зайдите в меню *Objects→Services→Add→Service Group.* Во вкладке *General,* введите следующие параметры:	
Name	ad-all-srv
Selected	Переместите ldap, smb-all, kerberos-auth, kerberos, dns-all, gc, rpc из списка Available.
Настроим IP Rules. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Введите следующие параметры:	
Name	allow-srvDC
Action	Allow
Service	ad-all-srv
Source Interface	lan1_lan2
Source Network	ad-net
Destination Interface	lan1_lan2
Destination Network	ad-net
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Введите следующие параметры:	
Name	drop-outside
Action	Drop
Service	ad-all-srv
Source Interface	any
Source Network	all-nets
Destination Interface	any
Destination Network	all-nets
Создадим IDP Rule. Зайдите в меню *IDP/IPS→IDP Rules→Add→IDP Rule.* Задайте параметры:	
Name	IPS_srvDC
Service	ad-all-srv
Protect against insertion/evasion attacks	Поставьте галочку
Source Interface	lan_dmz
Source Network	ad-net
Destination Interface	lan_dmz
Destination Network	ad-net
Примечание: Созданое правило будет мониторить только трафик служб ad-all-srv, любой другой вид трафика не будет пропускаться этим правилом. Для других служб необходимо создать соответствующие правила, если есть необходимость их мониторить.	
Создадим IDP Rule Action. Зайдите в меню *IDP/IPS→IDP Rules→IPS_srvDC→вкладка Rule Actions→Add→IDP Rule Action.* Задайте параметры:	
Action	Protect
Signature (s)	Введите IPS_MALWARE*, IPS_AUTHENTICATION_KERBEROS, IPS_DNS*, IPS_REMOTEACCESS_GENERAL,

	IPS_OS-SPECIFIC_WINDOWS, IPS_WORM_GENERAL, IPS_SMB*, IPS_COMPONENT*, IPS_DCOM_GENERAL, IPS_RPC_GENERAL, IPS_SCANNER* IPS_TCP* IPS_UDP*
Во вкладке *LogSettings* задайте параметры:	
Enable Logging	Поставьте галочку
Log with severity	Выберите из списка Debug
Создадим IDP Rule Action. Зайдите в меню *IDP/IPS→IDP Rules→IPS_srvDC→вкладка Rule Actions→Add→IDP Rule Action.* Задайте параметры:	
Action	Audit
Signature (s)	Введите IDS*
Во вкладке *LogSettings* задайте параметры:	
Enable Logging	Поставьте галочку
Log with severity	Выберите из списка Debug
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Примечание: Для того, чтобы избежать ложных срабатываний правил, необходимо внимательнее подходить к обозначению действия правила сигнатур как Protect, Audit и Ignored. Описание сигнатур можно найти на сайте центра сетевой защиты D-Link http://security.dlink.com.tw. Например, при нормальной работе легальных клиентов и серверов AD возможны ложные срабатывания правил IDP на сигнатуры № 17353 и 61541.	
Командная строка (CLI)	
gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address ad-net Address=172.17.100.0/24 gw-world:/labs> cc gw-world:/> add Interface InterfaceGroup lan_dmz Members=lan,dmz Equivalent=Yes gw-world:/> cc RoutingTable main gw-world:/main> add SwitchRoute Interface=lan_dmz Network=labs/ad-net Index=1 Metric=0 gw-world:/main> cc gw-world:/> add Service ServiceTCPUDP ldap DestinationPorts=389 SourcePorts=0-65535 Type=TCPUDP SYNRelay=Yes gw-world:/> add Service ServiceTCPUDP smb-all DestinationPorts=135-139,445 SourcePorts=0-65535 Type=TCPUDP SYNRelay=Yes gw-world:/> add Service ServiceTCPUDP kerberos-auth DestinationPorts=88 SourcePorts=0-65535 Type=UDP gw-world:/> add Service ServiceTCPUDP kerberos DestinationPorts=464 SourcePorts=0-65535 Type=TCPUDP SYNRelay=Yes gw-world:/> add Service ServiceTCPUDP dns-all DestinationPorts=53 SourcePorts=0-65535 Type=TCPUDP SYNRelay=Yes gw-world:/> add Service ServiceTCPUDP gc DestinationPorts=3268,3269 SourcePorts=0-65535 Type=TCP SYNRelay=Yes gw-world:/> add Service ServiceTCPUDP rpc DestinationPorts=1025 SourcePorts=0-65535 Type=TCP SYNRelay=Yes gw-world:/>add Service ServiceGroup ad-all-srv Members=ldap,smb-all,kerberos-auth,kerberos,dns-all,gc,rpc gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=lan_dmz	

DestinationNetwork=labs/ad-net Service=ad-all-srv SourceInterface=lan_dmz SourceNetwork=labs/ad-net Index=1 Name=allow-srvDC
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=any DestinationNetwork=all-nets Service=ad-all-srv SourceInterface=any SourceNetwork=all-nets Index=2 Name=drop-outside
gw-world:/1(labs)> cc
gw-world:/> add IDPRule DestinationInterface=lan1_lan2 DestinationNetwork=labs/ad-net SourceInterface=lan_dmz SourceNetwork=labs/ad-net Service=ad-all-srv Index=1 InsertionEvasion=Yes Name=IPS_srvDC
gw-world:/> cc IDPRule 1(IPS_srvDC)
gw-world:/1(IPS_srvDC)> add IDPRuleAction Action=Protect Index=1 Signatures=IPS_MALWARE*,IPS_AUTHENTICATION_KERBEROS,IPS_DNS*,IPS_REMOTEACCESS_GENERAL,IPS_OS-SPECIFIC_WINDOWS,IPS_WORM_GENERAL,IPS_SMB*,IPS_COMPONENT*,IPS_DCOM_GENERAL,IPS_RPC_GENERAL,IPS_SCANNER*IPS_TCP*IPS_UDP* LogSeverity=Debug LogEnabled=Yes
gw-world:/1(IPS_srvDC)> add IDPRuleAction Action=AuditIndex=2 Signatures=IDS* LogSeverity=Debug LogEnabled=Yes
gw-world:/1(IPS_srvDC)> cc
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Упражнение	Для проверки срабатывания IDP/IPS-правил зайдите в меню *Status→IDP/IPS*. Проведите сканирование уязвимостей и эмуляцию сетевой атаки на сервер контроллера домена.

Пример сообщений IDP/IPS при аудите контроллера домена 172.17.100.220 с использованием сканера уязвимостей Rapid7 Nexpose показан на рисунке 7.8.

Рисунок 7.8

Date	Severity	Category/ID	Rule	Proto	Src/DstIf	Src/DstIP	Src/DstPort	Event/Action
2012-02-22 22:53:37	Notice	IDP 1300007	idp_core	TCP		172.17.100.7 172.17.100.220	8585 139	intrusion_detected
description="NetPathCanonicalize.SRVSVC.MicrosoftWindows.MS08-067.Buffer.Overflow.A" signatureid=61540 idrule="idp_core" Advisory link								
2012-02-22 22:53:37	Notice	IDP 1300007	idp_core	TCP		172.17.100.7 172.17.100.220	8563 139	intrusion_detected
description="NetPathCanonicalize.SRVSVC.MicrosoftWindows.MS08-067.Buffer.Overflow.A" signatureid=61540 idrule="idp_core" Advisory link								
2012-02-22 22:53:19	Notice	IDP 1300007	idp_core	TCP		172.17.100.7 172.17.100.220	8517 53	intrusion_detected
description="DNS.BIND.QUERY-VER.DISCOVER" signatureid=22501 idrule="idp_core" Advisory link								

Пример сообщений IDP/IPS при атаке на контроллер домена 172.17.100.220 с использованием механизма Exploiting ПО эмуляции проникновений и сетевых атак Rapid7 Metasploit показан на рисунке 7.9.

Рисунок 7.9

Date	Severity	Category/ID	Rule	Proto	Src/DstIf	Src/DstIP	Src/DstPort	Event/Action
2012-02-22 23:56:34	Warning	IDP 1300003	idp_core	TCP		172.17.100.212 172.17.100.220	3774 445	intrusion_detected close
description="NetPathCanonicalize.SRVSVC.MicrosoftWindows.MS08-067.Buffer.Overflow.B" signatureid=61541 idrule="idp_core" Advisory link								
2012-02-22 23:56:34	Debug	IDP 1300001	idp_core	TCP		172.17.100.212 172.17.100.220	3774 445	scan_detected close
description="FnstEnv.x86.GetPC.Shellcode" signatureid=58375 idrule="idp_core" Advisory link								
2012-02-22 23:56:33	Debug	IDP 1300001	idp_core	TCP		172.17.100.212 172.17.100.220	3773 135	scan_detected close
description="UUID.MicrosoftWindows.DCERPC.MS03-026.BIND.Attempt.A" signatureid=57303 idrule="idp_core" Advisory link								
2012-02-22 23:53:09	Debug	IDP 1300001	idp_core	TCP		172.17.100.212 172.17.100.220	3690 445	scan_detected close
description="FnstEnv.x86.GetPC.Shellcode" signatureid=58375 idrule="idp_core" Advisory link								
2012-02-22 23:53:06	Debug	IDP 1300001	idp_core	TCP		172.17.100.212 172.17.100.220	3689 135	scan_detected close
description="UUID.MicrosoftWindows.DCERPC.MS03-026.BIND.Attempt.A" signatureid=57303 idrule="idp_core" Advisory link								
2012-02-22 23:50:40	Debug	IDP 1300001	idp_core	TCP		172.17.100.212 172.17.100.220	3636 445	scan_detected close
description="FnstEnv.x86.GetPC.Shellcode" signatureid=58375 idrule="idp_core" Advisory link								
2012-02-22 23:50:38	Debug	IDP 1300001	idp_core	TCP		172.17.100.212 172.17.100.220	3634 135	scan_detected close
description="UUID.MicrosoftWindows.DCERPC.MS03-026.BIND.Attempt.A" signatureid=57303 idrule="idp_core" Advisory link								

Пример сообщений IDP/IPS при атаке на контроллер домена 172.17.100.220 с использованием Rapid7 Metasploit и Nexpose, действие IDP-правил – Protect, показан на рисунке 7.10.

Рисунок 7.10

Date	Severity	Category/ID	Rule	Proto	Src/DstIf	Src/DstIP	Src/DstPort	Event/Action
2012-02-23 20:16:41	Warning	IDP 1300003	idp_core	TCP		172.17.100.212 172.17.100.220	1262 445	intrusion_detected close
description="NetPathCanonicalize.SRVSVC.MicrosoftWindows.MS08-067.Buffer.Overflow.B" signatureid=61541 idrule="idp_core" Advisory link								
2012-02-23 20:16:41	Debug	IDP 1300001	idp_core	TCP		172.17.100.212 172.17.100.220	1262 445	scan_detected close
description="FnstEnv.x86.GetPC.Shellcode" signatureid=58375 idrule="idp_core" Advisory link								
2012-02-23 20:16:39	Debug	IDP 1300001	idp_core	TCP		172.17.100.212 172.17.100.220	1259 135	scan_detected close
description="UUID.MicrosoftWindows.DCERPC.MS03-026.BIND.Attempt.A" signatureid=57303 idrule="idp_core" Advisory link								
2012-02-23 20:07:32	Warning	IDP 1300003	idp_core	TCP		172.17.100.7 172.17.100.220	13361 445	intrusion_detected close
description="NetPathCanonicalize.SRVSVC.MicrosoftWindows.MS08-067.Buffer.Overflow.B" signatureid=61541 idrule="idp_core" Advisory link								
2012-02-23 20:07:30	Warning	IDP 1300003	idp_core	TCP		172.17.100.7 172.17.100.220	13354 139	intrusion_detected close
description="NetPathCanonicalize.SRVSVC.MicrosoftWindows.MS08-067.Buffer.Overflow.A" signatureid=61540 idrule="idp_core" Advisory link								
2012-02-23 20:07:30	Warning	IDP 1300003	idp_core	TCP		172.17.100.7 172.17.100.220	13338 445	intrusion_detected close
description="NetPathCanonicalize.SRVSVC.MicrosoftWindows.MS08-067.Buffer.Overflow.B" signatureid=61541 idrule="idp_core" Advisory link								
2012-02-23 20:07:29	Warning	IDP 1300003	idp_core	TCP		172.17.100.7 172.17.100.220	13343 139	intrusion_detected close
description="NetPathCanonicalize.SRVSVC.MicrosoftWindows.MS08-067.Buffer.Overflow.A" signatureid=61540 idrule="idp_core" Advisory link								
2012-02-23 20:07:29	Warning	IDP 1300003	idp_core	TCP		172.17.100.7 172.17.100.220	13342 445	intrusion_detected close
description="SMB.RAW.ASN1-MS04-007.OVERFLOW" signatureid=21971 idrule="idp_core" Advisory link								

Примечание: Для демонстрации работы IDP-системы в качестве цели атаки используется контороллер домена Microsoft Windows Server 2003 без установленных последних обновлений безопасности, операционные системы последних версий со всеми установленными обновлениями безопасности не имеют уязвимостей.

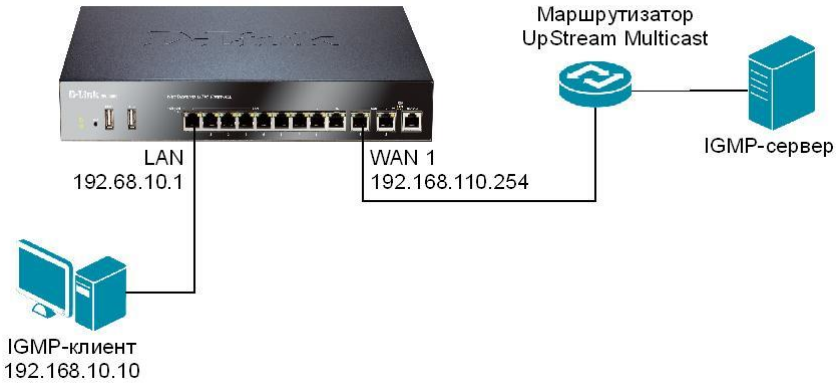
ЗАНЯТИЕ №22. Широковещательные рассылки. Multicast Routing. IGMP. Multicast GRE over IPSec.

Управление широковещательным трафиком в современных сетях – необходимая составляющая обеспечения информационной безопасности. Межсетевые экраны D-Link предоставляют механизмы управления широковещательным трафиком.

Цель	Эта лабораторная работа позволяет пользователям изучить процесс управления широковещательным трафиком.	
Оборудование	DFL-860E	2
	Рабочая станция	2
	Рабочая станция с ПО IGMP-клиент	2
	Ethernet-кабель (патч-корд)	6
	IGMP-сервер	1
	Маршрутизатор Upstream Multicast	1

Обзор	*Некоторые приложения сети Интернет (например, конференции и широковещательная рассылка видео) требуют рассылки одним клиентом или хостом одного и того же пакета множеству получателей. Это может быть достигнуто повторением рассылки пакета с различными IP-адресами назначения или широковещательной рассылкой пакета через Интернет. Маршрутизация для каждого пакета в отдельности в данном случае не удовлетворительна с точки зрения нагрузки на сеть и пропускной способности сети. Эффективным решением данной задачи является многоадресная маршрутизация (multicast routing), с помощью которой маршрутизация осуществляется целиком для всех членов группы пакетов широковещательного трафика.* *Стандарты IETF предусматривают следующие виды многоадресной рассылки:* *- подсеть класса D, зарезервированная для многоадресного трафика. Каждый многоадресный IP-адрес представляет определенную группу получателей трафика.* *- протокол IGMP позволяет получателям сообщить сети, что он является членом конкретной группы многоадресной рассылки.* *- группа протоколов Protocol Independent Multicast (PIM) служит для вычисления оптимального пути для многоадресных пакетов.* *Общий принцип функционирования многоадресной рассылки заключается в использовании протокола IGMP для присоединения к группе интересующей рассылки, маршрутизаторы PIM в дальнейшем могут множить и продвигать пакеты всем членам такой многоадресной группы, таким образом создавая дерево распределения (distribution tree) для потока пакетов. PIM может использовать информацию от других протоколов (например, OSPF) для оценки информации о маршрутизации в сети.* *Ключевой механизм в процессе многоадресной маршрутизации*

	– продвижение по обратному пути (Reverse Path Forwarding). Для трафика unicast маршрутизатор имеет дело только с адресом назначения пакета, для многоадресного трафика маршрутизатор также работает с источником пакетов, т.к. необходимо отправить пакеты на группу адресов, в которую не включается адрес отправителя. Таким образом можно избежать зацикливания в дереве распределения.
Реализация на межсетевом экране	*По умолчанию пакеты многоадресной рассылки приходят на интерфейс* core *операционной системы межсетевого экрана. Для совершения продвижения пакетов на правильный интерфейс используются правила с действием SAT Multiplex.* *Правило SAT Multiplex позволяет размножить и продвигать пакеты на несколько интерфейсов.* *У правила два режима:* *- Multicast traffic must have been requested using IGMP before it is forwarded – используется IGMP, режим по умолчанию – хост первоначально использует протокол IGMP для широковещательной рассылки.* *- All-to-One Mapping: rewrite all destination IPs to a single IP – протокол IGMP не используется.* *При этом правила NAT или Allow также должны быть созданы для трафика.*
Примечание: На Ethernet-интерфейсах должна быть включена функция поддержки многоадресного трафика (значение Multicast handling – On или Auto).	
Конфигурация IGMP	*Сигнализация IGMP между хостами и маршрутизаторами делится на две категории:* *- IGMP Report – сообщения отсылаются хостами маршрутизатору, когда хост желает подписаться на новую многоадресную рассылку (группу) или изменить текущие соглашения многоадресной рассылки.* *- IGMP Query – IGMP- сообщения от маршрутизатора к хосту для уточнения доступности потока, который необходимо получать.* *Если источник многоадресной рассылки расположен в локальной сети, непосредственно подключенной к маршрутизатору, то IGMP Query правил не нужно.* *Если соседний маршрутизатор сконфигурирован так, чтобы статически доставлять многоадресный поток межсетевому экрану, то IGMP Query также указывать не нужно.* *Межсетевой экран поддерживает два режима операций IGMP:* *- Snoop Mode – межсетевой экран прозрачен для соединения хоста и другого IGMP-маршрутизатора.* *- Proxy Mode – межсетевой экран выступает в качестве IGMP-маршрутизатора по отношению к клиентам. По отношению к другим IGMP-маршрутизаторам межсетевой экран выступает в качестве обычного хоста, в соответствии с группой его клиентов.*
Многоадресная рассылка без преобразования адреса	
Описание сценария	*Необходимо сконфигурировать многоадресную рассылку с IGMP. Отправитель многоадресного трафика – 192.168.110.10, многоадресный поток – 239.192.10.0:12345. Поток должен быть пропущен с интерфейса wan1 на интерфейсы* ***dmz***, ***lan*** *(lan1, lan2 в моделях DFL-1660/2560) только в том случае, если*

	отправитель использует протокол IGMP.
Схема 80	

Настройка DFL-860E

Web-интерфейс

Создание необходимых объектов

Зайдите в меню *Objects→Services*. Создайте SMTP Service. Введите во вкладке *General* следующие параметры:

Name	multicast_service1
Type	UDP
Destination Port	12345

Зайдите в меню *Objects→Address Book*. Добавьте новую папку *Address Folder* под именем *RemoteHost*, в ней создайте следующие объекты:

Name	MC_sender_ip
Address	192.168.110.10
Name	MC_destination_net
Address	239.192.10.0

Зайдите в меню *Interfaces→Interface Groups→Add→Interfaces Group*. Введите следующие параметры:

Name	ifGrpClients
Selected	dmz, lan

Настройка IP Rule

Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Во вкладке *General* введите:

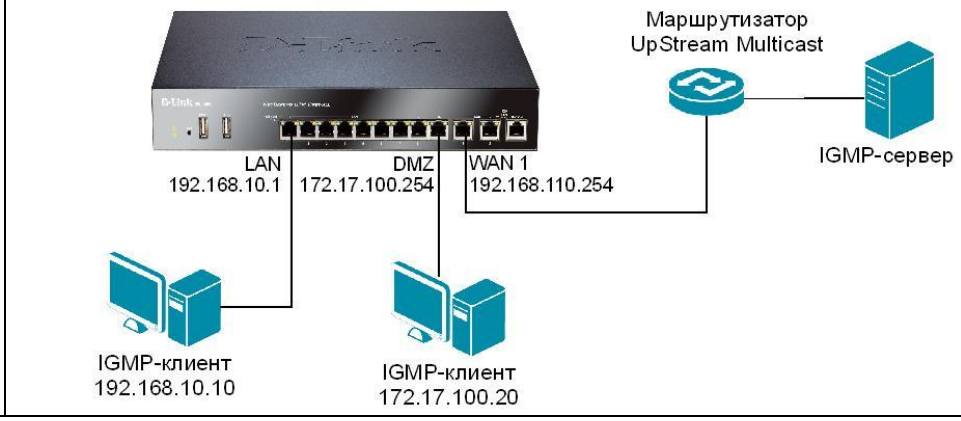
Name	Multicast_Multiplex
Action	Multiplex SAT
Service	multicast_service1
Source Interface	wan1
Source Network	MC_sender_ip
Destination Interface	core
Destination Network	MC_destination_net

Во вкладке *Multiplex SAT* выберите интерфейсы dmz, lan, для каждого оставьте поле IP Address пустым, т.к. преобразование адреса отправителя не производиться. Введите параметры:

Multicast traffic must have been requested using IGMP before it is forwarded	Поставьте галочку

Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	Multicast_Multiplex_allow
Action	Allow
Service	multicast_service1
Source Interface	wan1
Source Network	MC_sender_ip
Destination Interface	core
Destination Network	MC_destination_net
Настройка IGMP Rule	
Зайдите в меню *Routing→IGMP→IGMP Rules→Add→IGMP Rule.* Во вкладке *General* введите:	
Name	Reports
Type	Report
Action	Proxy
Relay interface	wan1
В поле *Address Filter* введите:	
Source Interface	ifGrpClients
Source Network	dmznet, lannet
Destination Interface	core
Destination Network	auto
Multicast Source	MC_sender_ip
Multicast Group	MC_destination_net
Зайдите в меню *Routing→IGMP→IGMP Rules→Add→IGMP Rule.* Во вкладке *General* введите:	
Name	Queries
Type	Query
Action	Proxy
Relay interface	ifGrpClients
В поле *Address Filter* введите:	
Source Interface	wan1
Source Network	MC_sender_ip
Destination Interface	core
Destination Network	auto
Multicast Source	MC_sender_ip
Multicast Group	MC_destination_net
Зайдите вменю *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> add Service ServiceTCPUDP multicast_service1 DestinationPorts=12345 SourcePorts=0-65535 Type=UDP gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address MC_sender_ip Address=192.168.110.10 gw-world:/labs> add IP4Address MC_destination_net Address=239.192.10.0 gw-world:/labs> cc gw-world:/> add Interface InterfaceGroup ifGrpClients Members=lan,dmz gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)>add IPRule Action=MultiplexSAT Service=multicast_service	

DestinationInterface=core DestinationNetwork=labs/MC_destination_net SourceInterface=wan1 SourceNetwork=labs/MC_sender_ip MultiplexArgument=lan,dmz RequireIGMP=Yes Index=1 Name=Multicast_Multiplex gw-world:/1(labs)>add IPRule Action=Allow Service=multicast_service1 DestinationInterface=core DestinationNetwork=labs/MC_destination_net SourceInterface=wan1 SourceNetwork=labs/MC_sender_ip Index=2 Name=Multicast_Multiplex_allow gw-world:/1(labs)> cc gw-world:/>add IGMPRule MulticastGroup=labs/MC_destination_net MulticastSource=labs/MC_sender_ip RelayInterface=wan1 SourceInterface=ifGrpClients SourceNetwork=InterfaceAddresses/lan1net,InterfaceAddresses/lan2net,InterfaceAddresses/dmznet DestinationInterface=core Index=1 Name=Reports Type=Report Action=Proxy Filter=Yes gw-world:/> add IGMPRule MulticastGroup=labs/MC_destination_net MulticastSource=labs/MC_sender_ip RelayInterface=ifGrpClients SourceInterface=wan1 SourceNetwork=labs/MC_sender_ip DestinationInterface=core Index=2 Name=Queries Type=Query Action=Proxy Filter=Yes gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Настройка IGMP-сервера на примере программы Медиа-проигрователь VLC 1.1.11	
Зайдите *Медиа→Потоковое вещание→Файл→Добавить*. Добавьте медиафайл, который будет широковещательно передаваться в сеть.	
Нажмите кнопку *Поток*, настройте вывод потока. В появившемся окошке нажмите *Следующий*. Введите следующие параметры для *Пути назначения*:	
Новый путь назначения	UDP (legacy)
Включить перекодирование	Уберите галочку
Нажмите кнопку *Добавить*, введите следующие параметры для *UDP*:	
Адрес	239.192.10.0
Порт	12345
Нажмите кнопку *Следующий*, введите следующие параметры:	
“Время жизни” (TTL)	30
Нажмите кнопку *Поток*.	
Убедитесь в корректности сетевых настроек компьютера, на котором запущен IGMP-сервер: 192.168.110.10/24.	
Настройка IGMP-клиента на примере программы Медиа-проигрователь VLC 1.1.11	
Зайдите *Медиа→Открыть файл с параметрами→Сеть*. Введите следующие параметры:	
Сетевой протокол (network URL)	udp://@239.192.10.1:12345
Нажмите кнопку *Воспроизвести*.	
Убедитесь в корректности сетевых настроек компьютера, на котором запущен IGMP-клиент: 192.168.10.10/24, основной шлюз – 192.168.10.1.	
Упражнение	Проверьте работоспособность схемы. Получите широковещательный трафик на стороне клиента.
Многоадресная рассылка с преобразованием адреса	
Описание сценария	*Необходимо сконфигурировать многоадресную рассылку с IGMP. Отправитель многоадресного трафика – 192.168.20.10, многоадресный поток – 239.192.10.0:12345. Поток должен быть пропущен с интерфейса **wan1** на интерфейсы **dmz**, **lan** только в том случае, если отправитель использует протокол IGMP. Необходимо выполнить преобразование адресов: 239.192.10.0 в 237.192.10.0, когда поток направляется через*

	интерфейс ***lan.***
Схема 81	

Настройка DFL-860E

Web-интерфейс

Создание необходимых объектов

Зайдите в меню *Objects→Services*. Создайте SMTP Service. Введите во вкладке *General* следующие параметры:

Name	multicast_service2
Type	UDP
Destination Port	12345

Зайдите в меню *Objects→Address Book*. Добавьте новую папку *Address Folder* под именем *RemoteHost*, в ней создайте следующие объекты:

Name	MC_sender_ip
Address	192.168.20.10
Name	UpstreamRouterIP
Address	192.168.110.10
Name	MC_destination_net
Address	239.192.10.0
Name	MC_destination_IP_NATed
Address	237.192.10.0

Настройка IP Rule

Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:

Name	Multicast_Multiplex
Action	Multiplex SAT
Service	multicast_service2
Source Interface	wan1
Source Network	MC_sender_ip
Destination Interface	core
Destination Network	MC_destination_net

Во вкладке *Multiplex SAT* выберите интерфейсы dmz, lan. Введите параметры:

Multicast traffic must have been requested using IGMP before it is forwarded	Поставьте галочку

Для интерфейса lan введите параметры:	
IP Address	MC_destination_IP_NATed
All-to-One Mapping: rewrite all destination IPs to a single IP	Поставьте галочку
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	Multicast_Multiplex_allow
Action	Allow
Service	multicast_service2
Source Interface	wan1
Source Network	MC_sender_ip
Destination Interface	core
Destination Network	MC_destination_net
Настройка IGMP Rule для интерфейса dmz.	
Зайдите в меню *Routing→IGMP→IGMP Rules→Add→IGMPRule.* Во вкладке *General* введите:	
Name	Reports_dmz
Type	Report
Action	Proxy
Relay interface	wan1
В поле *Address Filter* введите:	
Source Interface	dmz
Source Network	dmznet
Destination Interface	core
Destination Network	auto
Multicast Source	MC_sender_ip
Multicast Group	MC_destination_net
Зайдите в меню *Routing→IGMP→IGMP Rules→Add→IGMP Rule.* Во вкладке *General* введите:	
Name	Queries_dmz
Type	Query
Action	Proxy
Relay interface	dmz
В поле *Address Filter* введите:	
Source Interface	wan1
Source Network	UpstreamRouterIP
Destination Interface	core
Destination Network	auto
Multicast Source	MC_sender_ip
Multicast Group	MC_destination_net
Настройка IGMP Rule для интерфейса lan.	
Зайдите в меню *Routing→IGMP→IGMP Rules→Add→IGMP Rule.* Во вкладке *General* введите:	
Name	Reports_lan
Type	Report
Action	Proxy
Relay interface	wan1

В поле *Address Filter* введите:	
Source Interface	lan
Source Network	lannet
Destination Interface	core
Destination Network	auto
Multicast Source	MC_sender_ip
Multicast Destination	MC_destination_IP_NATed
Во вкладке *IGMP SAT* введите:	
Translate Group Address	Поставьте галочку
New Group IP	MC_destination_net
All-to-one mapping: Rewrite all addresses to a single IP	Поставьте галочку
Зайдите в меню *Routing→IGMP→IGMP Rules→Add→IGMP Rule.* Во вкладке *General* введите:	
Name	Queries_lan
Type	Query
Action	Proxy
Relay interface	lan
В поле *Address Filter* введите:	
Source Interface	wan1
Source Network	UpstreamRouterIP
Destination Interface	core
Destination Network	auto
Multicast Source	MC_sender_ip
Multicast Destination	MC_destination_net
Во вкладке *IGMP SAT* введите:	
Translate Group Address	Поставьте галочку
New Group IP	MC_destination_IP_NATed
All-to-one mapping: Rewrite all addresses to a single IP	Поставьте галочку
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> add Service ServiceTCPUDP multicast_service2 DestinationPorts=12345 SourcePorts=0-65535 Type=UDP gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address MC_sender_ip Address=192.168.20.10 gw-world:/labs> add IP4Address UpstreamRouterIP Address=192.168.110.10 gw-world:/labs> add IP4Address MC_destination_net Address=239.192.10.0 gw-world:/labs> add IP4Address MC_destination_IP_NATed Address=237.192.10.0 gw-world:/labs> cc gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)>add IPRule Action=MultiplexSAT Service=multicast_service2 DestinationInterface=core DestinationNetwork=labs/MC_destination_net SourceInterface=wan1 SourceNetwork=labs/MC_sender_ip MultiplexArgument=lan,dmz RequireIGMP=Yes Index=1 TranslateMGroup=Yes NewGrpIP=labs/MC_destination_IP_NATed GrpAllToOne=YesName=Multicast_Multiplex gw-world:/1(labs)>add IPRule Action=Allow Service=multicast_service2 DestinationInterface=core DestinationNetwork=labs/MC_destination_net SourceInterface=wan1	

SourceNetwork=labs/MC_sender_ip Index=2 Name=Multicast_Multiplex_allow
gw-world:/1(labs)> cc
gw-world:/> add IGMPRule MulticastGroup=labs/MC_destination_net MulticastSource=labs/MC_sender_ip RelayInterface=wan1 SourceInterface=dmzSourceNetwork=InterfaceAddresses/dmznet DestinationInterface=core Index=1 Name=Reports_dmzType=Report Action=Proxy Filter=Yes
gw-world:/> add IGMPRule MulticastGroup=labs/MC_destination_net MulticastSource=labs/MC_sender_ip RelayInterface=dmz SourceInterface=wan1 SourceNetwork=labs/UpstreamRouterIP DestinationInterface=core Index=2 Name=Queries_dmz Type=Query Action=Proxy Filter=Yes
gw-world:/> add IGMPRule MulticastGroup=labs/MC_destination_IP_NATed MulticastSource=labs/MC_sender_ip RelayInterface=wan1 SourceInterface=lanSourceNetwork=InterfaceAddresses/lannet DestinationInterface=core Index=3 Name=Reports_lanType=Report Action=Proxy Filter=YesTranslateMGroup=Yes NewGrpIP=labs/MC_destination_net GrpAllToOne=Yes
gw-world:/> add IGMPRule MulticastGroup=labs/MC_destination_net MulticastSource=labs/MC_sender_ip RelayInterface=lan SourceInterface=wan1 SourceNetwork=labs/UpstreamRouterIP DestinationInterface=core Index=4 Name=Queries_lan Type=Query Action=Proxy Filter=YesTranslateMGroup=Yes NewGrpIP=labs/MC_destination_IP_NATed GrpAllToOne=Yes
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Настройка IGMP-сервера на примере программы Медиа-проигрователь VLC 1.1.11

Зайдите *Медиа→Потоковое вещание→Файл→Добавить*. Добавьте медиафайл, который будет широковещательно передаваться в сеть.

Нажмите кнопку *Поток*, настройте вывод потока. В появившемся окошке нажмите *Следующий*. Введите следующие параметры для *Пути назначения*:

Новый путь назначения	UDP (legacy)
Включить перекодирование	Уберите галочку

Нажмите кнопку *Добавить*, введите следующие параметры для *UDP*:

Адрес	239.192.10.0
Порт	12345

Нажмите кнопку *Следующий*, введите следующие параметры:

“Время жизни” (TTL)	30

Нажмите кнопку *Поток*.

Убедитесь в корректности сетевых настроек компьютера, на котором запущен IGMP-сервер: 192.168.20.10/24.

Настройка IGMP-клиента в dmz-зоне на примере программы Медиа-проигрователь VLC 1.1.11

Зайдите *Медиа→Открыть файл с параметрами→Сеть*. Введите следующие параметры:

Сетевой протокол (network URL)	udp://@239.192.10.1:12345

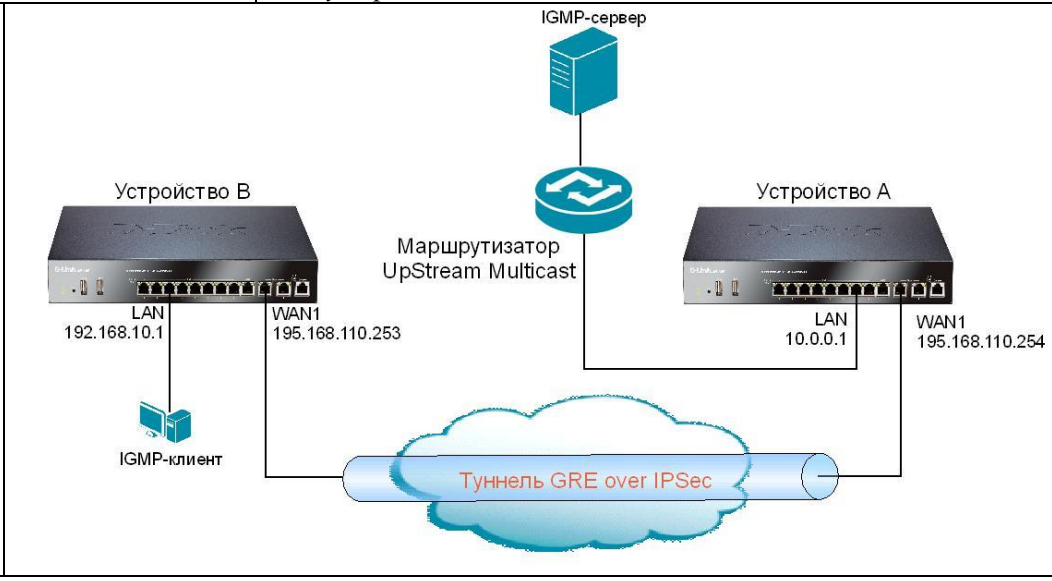
Нажмите кнопку *Воспроизвести*.

Убедитесь в корректности сетевых настроек компьютера, на котором запущен IGMP-клиент: 172.17.100.20/24, основной шлюз – 172.17.100.254.

Настройка IGMP-клиента в lan-сети на примере программы Медиа-проигрователь VLC 1.1.11

Зайдите *Медиа→Открыть файл с параметрами→Сеть*. Введите следующие параметры:

Сетевой протокол (network URL)	udp://@237.192.10.1:12345

Нажмите кнопку *Воспроизвести*.	
Убедитесь в корректности сетевых настроек компьютера, на котором запущен IGMP-клиент: 192.168.10.20/24, основной шлюз – 192.168.10.1.	
Упражнение	Проверьте работоспособность схемы. Получите широковещательный трафик на стороне клиента.
GRE over IPSec	
Описание сценария	*Между устройством A и B необходимо организовать GRE-туннель через защищенный IPSec-туннель. Через туннель GRE over IPSec необходимо разрешить прохождение мультикастового трафика из **lan**-сети устройства A в **lan**-сеть устройства B.*
Схема 82	
Настройка DFL-860E	
Устройство A	
Web-интерфейс	
Создание необходимых объектов	
Зайдите в меню *Objects→Address Book→InterfaceAddresses→Add→IP4 Address.* Введите следующие параметры:	
Name	lan_ip
Address	10.0.0.1
Зайдите в меню *Objects→Address Book→InterfaceAddresses→Add→IP4 Address.* Введите следующие параметры:	
Name	lannet
Address	10.0.0.0/20
Зайдите в меню *Objects→Address Book→InterfaceAddresses→Add→IP4 Address.* Введите следующие параметры:	
Name	wan1_ip
Address	195.168.110.254
Зайдите в меню *Objects→Address Book→InterfaceAddresses→Add→IP4 Address.* Введите следующие параметры:	
Name	wan1net

Address	195.168.110.0/24
Зайдите в меню *Objects→Address Book→InterfaceAddresses→Add→IP4 Address.* Введите следующие параметры:	
Name	wan1_gw
Address	195.168.110.1
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote-gre-id
Address	10.10.10.2
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote-gre-net
Address	192.168.10.0/24
Зайдите в меню *Objects→Address Book→Add→IP4 Group.* Введите следующие параметры:	
Name	remote-gre-all
Selected	remote-gre-id, remote-gre-net
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote_net
Address	195.168.110.0/24
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote_gw
Address	195.168.110.253
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	gre-ip
Address	10.10.10.1
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	multicast_net
Address	224.0.0.0
Создадим объект «Pre-shared Key». Зайдите в меню *Objects→Authentication Objects→Add→Pre-Shared Key*. Введите следующие параметры:	
Name	pre-shared_key
Выберите *Shared Secret*.Введите следующие параметры:	
Shared Secret	123456qw
Confirm Secret	123456qw
Зайдите в меню *Objects→VPN Objects→IKE Algorithms→Add→IKE Algorithms.* Введите следующие параметры:	
Name	ike-phase1
Encryption Algorithms	DES (только один из всех)
Encryption Algorithms	SHA1 (только один из всех)
Зайдите в меню *Objects→VPN Objects→IKE Algorithms→Add→Ipsec Algorithms.* Введите следующие параметры:	
Name	esp-phase2
Encryption Algorithms	DES (только один из всех)
Encryption Algorithms	SHA1 (только один из всех)
Создадим IPSec-туннель. Зайдите в *Interfaces→IPSec→Add→IPSec Tunnel*. Введите следующие параметры:	
Name	ipsec-if

Local Network	wan1_ip
Remote Network	remote_net
Remote Endpoint	remote_gw
Encapsulation mode	Transport
Выберите алгоритмы IKE и IPSec:	
IKE Algorithms	ike-phase1
IPSec Algorithms	esp-phase2
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите pre-shared_key из списка
Во вкладке *Advanced* введите следующие параметры:	
Add route for remote network	Поставьте галочку
Создадим GRE-туннель. Зайдите в меню *Interfaces→GRE→Add→GRE Tunnel.* Введите следующие параметры:	
Name	gre-if
IP Address	gre-ip
Remote Network	remote-gre-all
Remote Endpoint	remote_gw
Во вкладке *Advanced* введите следующие параметры:	
Automatically add a route for this interface using the given remote network.	Поставьте галочку
Зайдите в меню *Routing→IGMP→IGMP Rules→Add→IGMP Rule.* Во вкладке *General* введите:	
Name	IGMP-report-IF-lan
Type	Report
Action	Proxy
Relay interface	lan
В поле *Address Filter* введите:	
Source Interface	gre-if
Source Network	remote-gre-net
Destination Interface	core
Destination Network	auto
Multicast Source	remote-gre-all
Multicast Group	multicast_net
Зайдите в меню *Routing→IGMP→IGMP Rules→Add→IGMP Rule.* Во вкладке *General* введите:	
Name	IGMP-query-IF-GRE
Type	Query
Action	Proxy
Relay interface	gre-if
В поле *Address Filter* введите:	
Source Interface	lan
Source Network	lannet
Destination Interface	core
Destination Network	auto
Multicast Source	remote-gre-net

Multicast Group	multicast_net
Зайдите в меню *Interfaces→Interface Groups→Add→Interfaces Group.* Введите следующие параметры:	
Name	gre-lan
Selected	gre-if, lan
Создание IP Rule	
Зайдите в папк у*Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	allow-gre-lan-all
Action	Allow
Service	all-services
Source Interface	gre-lan
Source Network	all-nets
Destination Interface	gre-lan
Destination Network	all-nets
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	forwarding-MC-from-lan
Action	Multiplex SAT
Service	all_udp
Source Interface	lan
Source Network	lannet
Destination Interface	core
Destination Network	multicast_net
Во вкладке *Multiplex SAT* выберите gre-if, поле IP Address пустым, т.к. преобразование адреса отправителя не производиться. Введите параметры:	
Multicast traffic must have been requested using IGMP before it is forwarded	Поставьте галочку
All-to-One Mapping: rewrite all destination IPs to a single IP	Поставьте галочку
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	allow-forwarding-MC-from-GRE
Action	Allow
Service	all_udp
Source Interface	lan
Source Network	lannet
Destination Interface	core
Destination Network	multicast_net
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/> set IP4Address InterfaceAddresses/lan_ip Address=10.0.0.1 gw-world:/> set IP4Address InterfaceAddresses/lannet Address=10.0.0.0/24 gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.168.110.254 gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.168.110.0/24 gw-world:/> set IP4Address InterfaceAddresses/wan1_gw Address=195.168.110.1 gw-world:/> cc Address AddressFolder labs	

gw-world:/labs> add IP4Address remote-gre-id Address=10.10.10.2
gw-world:/labs> add IP4Address remote-gre-net Address=192.168.10.0/24
gw-world:/labs> add IP4Address remote_net Address=195.168.110.253
gw-world:/labs> add IP4Address remote_gw Address=195.168.110.253
gw-world:/labs> add IP4Address gre-ip Address=10.10.10.1
gw-world:/labs> add IP4Address multicast_net Address=224.0.0.0
gw-world:/labs> cc
gw-world:/>add Address IP4Group remote-gre-all Members=labs/remote-gre-id,labs/remote-gre-net
gw-world:/>add PSK pre-shared_key Type=ASCII PSKAscii=123456qw
gw-world:/>add IKEAlgorithms ike-phase1DESEnabled=Yes SHA1Enabled=Yes
gw-world:/>add IPsecAlgorithmsesp-phase2DESEnabled=Yes SHA1Enabled=Yes
gw-world:/> add Interface IPsecTunnel ipsec-if AuthMethod=PSK IKEAlgorithms=ike-phase1 IPsecAlgorithms=esp-phase2 LocalNetwork=InterfaceAddresses/wan1_ip PSK=pre-shared_key RemoteNetwork=labs/remote_netRemoteEndpoint=labs/remote_gw AddRouteToRemoteNet=Yes EncapsulationMode=Transport
gw-world:/> add Interface GRETunnel gre-if IP=labs/gre-ip Network=lans/remote-gre-all RemoteEndpoint=labs/remote_gw AutoInterfaceNetworkRoute=Yes
gw-world:/> add IGMPRule MulticastGroup=labs/multicast_net MulticastSource=labs/remote-gre-all RelayInterface=lan SourceInterface=gre-if SourceNetwork=labs/remote-gre-net DestinationInterface=core Index=1 Name=IGMP-report-IF-lan Type=Report Action=Proxy Filter=Yes
gw-world:/> add IGMPRule MulticastGroup=labs/multicast_net MulticastSource=labs/remote-gre-net RelayInterface=gre-if SourceInterface=lan SourceNetwork=InterfaceAddresses/lannetDestinationInterface=core Index=2 Name=IGMP-query-IF-GRE Type=Query Action=Proxy Filter=Yes
gw-world:/> add Interface InterfaceGroup gre-lan Members=lan,gre-if
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow Service=all-services SourceInterface=gre-lan SourceNetwork=all-nets DestinationInterface=gre-lan DestinationNetwork=all-nets Index=1 Name=allow-gre-lan-all
gw-world:/1(labs)> add IPRule Action=MultiplexSAT Service=all_udp DestinationInterface=core DestinationNetwork=labs/multicast_net SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet MultiplexArgument=gre-if RequireIGMP=Yes Index=2 GrpAllToOne=Yes Name=forwarding-MC-from-lan
gw-world:/1(labs)> add IPRule Action=Allow Service=all_udp DestinationInterface=core DestinationNetwork=labs/multicast_net SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Index=3 Name=allow-forwarding-MC-from-GRE
gw-world:/1(labs)> cc
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Настройка DFL-860E

Устройство B

Web-интерфейс

Создание необходимых объектов

Зайдите в меню *Objects→Address Book→InterfaceAddresses→Add→IP4 Address.* Введите следующие параметры:

Name	lan_ip
Address	192.168.10.1

Зайдите в меню *Objects→Address Book→InterfaceAddresses→Add→IP4 Address.* Введите следующие параметры:

Name	lannet

Address	192.168.10.0/24
Зайдите в меню *Objects→Address Book→InterfaceAddresses→Add→IP4 Address.* Введите следующие параметры:	
Name	wan1_ip
Address	195.168.110.253
Зайдите в меню *Objects→Address Book→InterfaceAddresses→Add→IP4 Address.* Введите следующие параметры:	
Name	wan1net
Address	195.168.110.0/24
Зайдите в меню *Objects→Address Book→InterfaceAddresses→Add→IP4 Address.* Введите следующие параметры:	
Name	wan1_gw
Address	195.168.110.1
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote-gre-id
Address	10.10.10.1
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote-gre-net
Address	10.0.0.0/20
Зайдите в меню *Objects→Address Book→Add→IP4 Group.* Введите следующие параметры:	
Name	remote-gre-all
Selected	remote-gre-id, remote-gre-net
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote_net
Address	195.168.110.0/24
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	remote_gw
Address	195.168.110.254
Зайдите в меню *Objects→Addressbook→Add→IP4 Address.* Введите следующие параметры:	
Name	gre-ip
Address	10.10.10.2
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	multicast_net
Address	224.0.0.0
Создадим объект «Pre-shared Key». Зайдите в меню *Objects→Authentication Objects→Add→Pre-Shared Key.* Введите следующие параметры:	
Name	pre-shared_key
Выберите *Shared Secret*.Введите следующие параметры:	
Shared Secret	123456qw
Confirm Secret	123456qw
Зайдите в меню *Objects→VPN Objects→IKE Algorithms→Add→IKE Algorithms.* Введите следующие параметры:	
Name	ike-phase1
Encryption Algorithms	DES (только один из всех)
Encryption Algorithms	SHA1 (только один из всех)

Зайдите в меню *Objects→VPN Objects→IKE Algorithms→Add→IPsec Algorithms.* Введите следующие параметры:	
Name	esp-phase2
Encryption Algorithms	DES (только один из всех)
Encryption Algorithms	SHA1 (только один из всех)
Создадим IPSec-туннель. Зайдите в *Interfaces→IPSec→Add→IPSec Tunnel.* Введите следующие параметры:	
Name	ipsec-if
Local Network	wan1_ip
Remote Network	remote_net
Remote Endpoint	remote_gw
Encapsulation mode	Transport
Выберите алгоритмы IKE и IPSec:	
IKE Algorithms	ike-phase1
IPSec Algorithms	esp-phase2
Во вкладке *Authentication* введите следующие параметры:	
Authentication	Выберите pre-shared_key из списка
Во вкладке *Advanced* введите следующие параметры:	
Add route for remote network	Поставьте галочку
Создадим GRE-туннель. Зайдите в меню *Interfaces→GRE→Add→GRE Tunnel.* Введите следующие параметры:	
Name	gre-if
IP Address	gre-ip
Remote Network	remote-gre-all
Remote Endpoint	remote_gw
Во вкладке *Advanced* введите следующие параметры:	
Automatically add a route for this interface using the given remote network.	Поставьте галочку
Зайдите в меню *Routing→IGMP→IGMP Rules→Add→IGMP Rule.* Во вкладке *General* введите:	
Name	IGMP-report-IF-lan
Type	Report
Action	Proxy
Relay interface	gre-if
В поле *Address Filter* введите:	
Source Interface	lan
Source Network	lannet
Destination Interface	core
Destination Network	auto
Multicast Source	remote-gre-net
Multicast Group	multicast_net
Зайдите в меню *Routing→IGMP→IGMP Rules→Add→IGMP Rule.* Во вкладке *General* введите:	
Name	IGMP-query-IF-GRE
Type	Query
Action	Proxy

Relay interface	lan
В поле *Address Filter* введите:	
Source Interface	gre-if
Source Network	remote-gre-all
Destination Interface	core
Destination Network	auto
Multicast Source	remote-gre-net
Multicast Group	multicast_net
Зайдите в меню *Interfaces→Interface Groups→Add→Interfaces Group.* Введите следующие параметры:	
Name	gre-lan
Selected	gre-if, lan
Создание IP Rule	
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	allow-gre-lan-all
Action	Allow
Service	all-services
Source Interface	gre-lan
Source Network	all-nets
Destination Interface	gre-lan
Destination Network	all-nets
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	forwarding-MC-from-lan
Action	Multiplex SAT
Service	all_udp
Source Interface	gre-if
Source Network	remote-gre-net
Destination Interface	core
Destination Network	multicast_net
Во вкладке *Multiplex SAT* выберите lan, поле IP Address пустым, т.к. преобразование адреса отправителя не производиться. Введите параметры:	
Multicast traffic must have been requested using IGMP before it is forwarded	Поставьте галочку
All-to-One Mapping: rewrite all destination IPs to a single IP	Поставьте галочку
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите:	
Name	allow-forwarding-MC-from-GRE
Action	Allow
Service	all_udp
Source Interface	gre-if
Source Network	remote-gre-net
Destination Interface	core
Destination Network	multicast_net
Зайдите в меню *Configuration* и выберите *Save and Activate*.	

Командная строка (CLI)

gw-world:/> set IP4Address InterfaceAddresses/lan_ip Address=192.168.10.1
gw-world:/> set IP4Address InterfaceAddresses/lannet Address=192.168.10.0/24
gw-world:/> set IP4Address InterfaceAddresses/wan1_ip Address=195.168.110.253
gw-world:/> set IP4Address InterfaceAddresses/wan1net Address=195.168.110.0/24
gw-world:/> set IP4Address InterfaceAddresses/wan1_gw Address=195.168.110.1
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address remote-gre-id Address=10.10.10.1
gw-world:/labs> add IP4Address remote-gre-net Address=10.0.0.0/20
gw-world:/labs> add IP4Address remote_net Address=195.168.110.254
gw-world:/labs> add IP4Address remote_gw Address=195.168.110.254
gw-world:/labs> add IP4Address gre-ip Address=10.10.10.2
gw-world:/labs> add IP4Address multicast_net Address=224.0.0.0
gw-world:/labs> cc
gw-world:/>add Address IP4Group remote-gre-all Members=labs/remote-gre-id,labs/remote-gre-net
gw-world:/>add PSK pre-shared_key Type=ASCII PSKAscii=123456qw
gw-world:/>add IKEAlgorithms ike-phase1DESEnabled=Yes SHA1Enabled=Yes
gw-world:/>add IPsecAlgorithmsesp-phase2DESEnabled=Yes SHA1Enabled=Yes
gw-world:/> add Interface IPsecTunnel ipsec-if AuthMethod=PSK IKEAlgorithms=ike-phase1 IPsecAlgorithms=esp-phase2 LocalNetwork=InterfaceAddresses/wan1_ip PSK=pre-shared_key RemoteNetwork=labs/remote_netRemoteEndpoint=labs/remote_gw AddRouteToRemoteNet=Yes EncapsulationMode=Transport
gw-world:/> add Interface GRETunnel gre-if IP=labs/gre-ip Network=lans/remote-gre-all RemoteEndpoint=labs/remote_gw AutoInterfaceNetworkRoute=Yes
gw-world:/> add IGMPRule MulticastGroup=labs/multicast_net MulticastSource=labs/remote-gre-all RelayInterface=gre-if
SourceInterface=lanSourceNetwork=InterfaceAddresses/lannetDestinationInterface=core Index=1 Name=IGMP-report-IF-lan Type=Report Action=Proxy Filter=Yes
gw-world:/> add IGMPRule MulticastGroup=labs/multicast_net MulticastSource=labs/remote-gre-net RelayInterface=lanSourceInterface=gre-if SourceNetwork=labs/remote-gre-net DestinationInterface=core Index=2 Name=IGMP-query-IF-GRE Type=Query Action=Proxy Filter=Yes
gw-world:/> add Interface InterfaceGroup gre-lan Members=lan,gre-if
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow Service=all-services SourceInterface=gre-lan SourceNetwork=all-nets DestinationInterface=gre-lan DestinationNetwork=all-nets Index=1 Name=allow-gre-lan-all
gw-world:/1(labs)> add IPRule Action=MultiplexSAT Service=all_udp DestinationInterface=core DestinationNetwork=labs/multicast_net SourceInterface=gre-if SourceNetwork=labs/remote-gre-net MultiplexArgument=lanRequireIGMP=Yes Index=2 GrpAllToOne=Yes Name=forwarding-MC-from-lan
gw-world:/1(labs)> add IPRule Action=Allow Service=all_udp DestinationInterface=core DestinationNetwork=labs/multicast_net SourceInterface=gre-if SourceNetwork=labs/remote-gre-net Index=3 Name=allow-forwarding-MC-from-GRE
gw-world:/1(labs)> cc
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Настройка IGMP-сервера на примере программы Медиа-проигрователь VLC 1.1.11

Зайдите *Медиа→Потоковое вещание→Файл→Добавить*. Добавьте медиафайл, который будет широковещательно передаваться в сеть.

Нажмите кнопку *Поток*, настройте вывод потока. В появившемся окошке нажмите *Следующий*. Введите следующие параметры для *Пути назначения*:

Новый путь назначения	UDP (legacy)
Включить перекодирование	Уберите галочку
Нажмите кнопку *Добавить*, введите следующие параметры для *UDP*:	
Адрес	224.0.0.0
Порт	12345
Нажмите кнопку *Следующий*, введите следующие параметры:	
“Время жизни” (TTL)	30
Нажмите кнопку *Поток*.	
Убедитесь в корректности сетевых настроек компьютера, на котором запущен IGMP-сервер: 195.168.110.10/24.	
Настройка IGMP-клиента на примере программы Медиа-проигрователь VLC 1.1.11	
Зайдите *Медиа→Открыть файл с параметрами→Сеть*. Введите следующие параметры:	
Сетевой протокол (network URL)	udp://@224.0.0.0:12345
Нажмите кнопку *Воспроизвести*.	
Убедитесь в корректности сетевых настроек компьютера, на котором запущен IGMP-клиент: 192.168.10.10/24, основной шлюз – 192.168.10.1.	
Упражнение	Проверьте работоспособность схемы. Получите широковещательный трафик на стороне клиента.

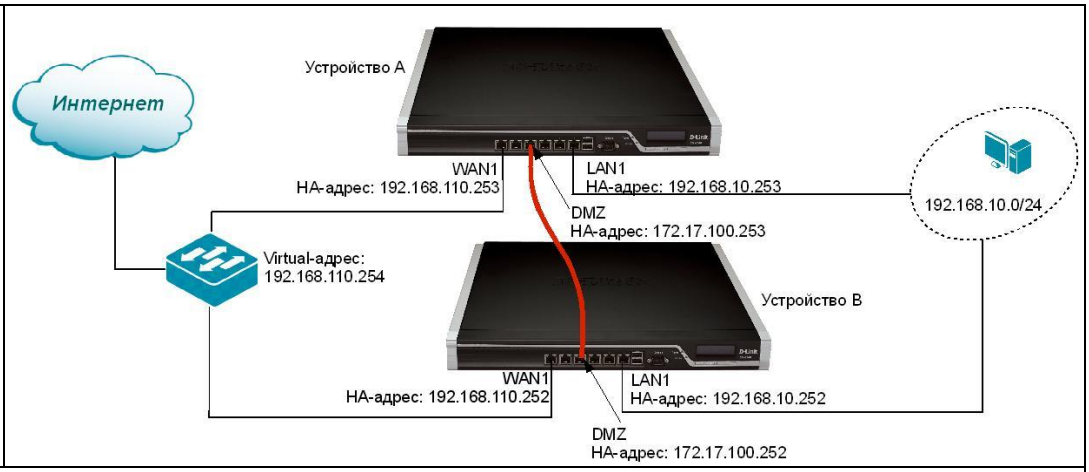
ЗАНЯТИЕ №23. Кластеры межсетевых экранов. Режим High Availability.

Межсетевые экраны D-Link могут быть объединены в кластеры для обеспечения повышенной надежности работы и доступности служб.

Создание кластеров и режим High Availability (HA) поддерживают только межсетевые экраны DFL-1600/1660/2500/2560 и объединяются по парам DFL-1660 / DFL-1660, DFL-2560 / DFL-2560 и т.д.

Цель	Эта лабораторная работа позволяет пользователям изучить режим High Availability.	
Оборудование	DFL-1660	2
	Рабочая станция	1
	Ethernet-кабель (патч-корд)	5
	Кросс патч-корд	1

Описание сценария	*Необходимо сконфигурировать межсетевые экраны в режиме High Availability для обеспечения кластерной функции безотказной работы устройств.* *Межсетевой экран A – основной межсетевой экран (Master).* *Межсетевой экран B – резервный межсетевой экран (Slave).* *Интерфейс синхронизации подключается через* ***dmz****-порт кабелем «кросс-овер».* *Все интерфейсы основного межсетевого экрана должны присутствовать на резервном межсетевом экране и подключаться к тем же подсетям.* *Каждый интерфейс кластера имеет три IP-адреса: два «реальных» IP-адреса (HA-адрес) (один для каждого устройства) и один «виртуальный» IP-адрес – общий для обоих устройств.* *В случае выхода из строя основного межсетевого экрана, резервный межсетевой экран будет задействован вместо Master-устройства, коммуникации тем самым не прервутся.* *Сетевые настройки:* *wan1_ip Устройство A- 192.168.110.253 Netmask 255.255.255.0;* *lan1_ip Устройство A - 192.168.10.253 Netmask 255.255.255.0;* *wan1_ip Устройство B - 192.168.110.252 Netmask 255.255.255.0;* *lan1_ip Устройство B - 192.168.10.252 Netmask 255.255.255.0;* *Устройство A 192.168.110.254 (Virtual IP HA cluster),* *Netmask 255.255.255.0,* *Gateway 192.168.110.250;* *Устройство B - 192.168.110.254 (Virtual IP HA cluster)* *Netmask 255.255.255.0,* *Gateway 192.168.110.250*

Схема 83	

Настройка DFL-1660

Устройство A

Web-интерфейс

Создание необходимых объектов

Зайдите в меню *Interfaces→Ethernet→wan1*. Выберите следующие параметры:

Enable DHCP Client	Снять галочку
IP address	wan1_ip
Network	wan1net
Default Gateway	wan1_gw

Зайдите в меню *Objects→Address Book→InterfaceAddresses*. Введите значения:

dmz_ip переименуйте в Virtual_dmz_ip	172.17.100.254
dmznet переименуйте в Virtual_dmznet	172.17.100.0/24
lan1_ip переименуйте в Virtual_lan1_ip	192.168.10.254
lan1net переименуйте в Virtual_lan1net	192.168.10.0/24
lan2_ip переименуйте в Virtual_lan2_ip	192.168.20.254
lan2net переименуйте в Virtual_lan2net	192.168.20.0/24
lan3_ip переименуйте в Virtual_lan3_ip	192.168.30.254
lan3net переименуйте в Virtual_lan3net	192.168.30.0/24
wan1_ip переименуйте в Virtual_wan1_ip	192.168.110.254
wan1net переименуйте в Virtual_wan1net	192.168.110.0/24
wan1_gw переименуйте в Virtual_wan1_gw	192.168.110.250

wan2_ip переименуйте в Virtual_wan2_ip	192.168.120.254
wan2net переименуйте в Virtual_wan2net	192.168.120.0/24
Зайдите в меню *Objects→Address Book→InterfaceAddresses.* Создайте объект «IP4 HA address» для двух «реальных» IP-адресов **dmz-**интерфейса:	
Name	HA-dmz
Master IP address	172.17.100.253
Slave IP address	172.17.100.252
Зайдите в меню *Objects→Address Book→InterfaceAddresses.* Создайте объект «IP4 HA address» для двух «реальных» IP-адресов **lan1**-интерфейса:	
Name	HA-lan1
Master IP address	192.168.10.253
Slave IP address	192.168.10.252
Зайдите в меню *Objects→Address Book→InterfaceAddresses.* Создайте объект «IP4 HA address» для двух «реальных» IP-адресов **lan2**-интерфейса:	
Name	HA-lan2
Master IP address	192.168.20.253
Slave IP address	192.168.20.252
Зайдите в меню *Objects→Address Book→InterfaceAddresses.* Создайте объект «IP4 HA address» для двух «реальных» IP-адресов **lan3**-интерфейса:	
Name	HA-lan3
Master IP address	192.168.30.253
Slave IP address	192.168.30.252
Зайдите в меню *Objects→Address Book→InterfaceAddresses.* Создайте объект «IP4 HA address» для двух «реальных» IP-адресов **wan1**-интерфейса:	
Name	HA-wan1
Master IP address	192.168.110.253
Slave IP address	192.168.110.252
Зайдите в меню *Objects→Address Book→InterfaceAddresses.* Создайте объект «IP4 HA address» для двух «реальных» IP-адресов **wan2**-интерфейса:	
Name	HA-wan2
Master IP address	192.168.120.253
Slave IP address	192.168.120.252
Настройка интерфейсов	
Зайдите в меню *Interfaces→Ethernet→dmz.*Во вкладке *General* введите следующие параметры:	
IP Address	Virtual_dmz_ip
Network	Virtual_dmznet
Default Gateway	Оставьте пустым - None
Во вкладке *Advanced* введите следующие параметры:	
Private IP Address	HA-dmz
Зайдите в *Interfaces→Ethernet→lan1.* Во вкладке *General* введите следующие параметры:	
IP Address	Virtual_lan1_ip
Network	Virtual_lan1net
Default Gateway	Оставьте пустым - None
Во вкладке *Advanced* введите следующие параметры:	

Private IP Address	HA-lan1
Зайдите в меню *Interfaces→Ethernet→lan2*. Во вкладке *General* введите следующие параметры:	
IP Address	Virtual_lan2_ip
Network	Virtual_lan2net
Default Gateway	Оставьте пустым - None
Во вкладке *Advanced* введите следующие параметры:	
Private IP Address	HA-lan2
Зайдите в меню *Interfaces→Ethernet→lan3*. Во вкладке *General* введите следующие параметры:	
IP Address	Virtual_lan3_ip
Network	Virtual_lan3net
Default Gateway	Оставьте пустым - None
Во вкладке *Advanced* введите следующие параметры:	
Private IP Address	HA-lan3
Зайдите в меню *Interfaces→Ethernet→wan1*. Во вкладке *General* введите следующие параметры:	
IP Address	Virtual_wan1_ip
Network	Virtual_wan1net
Default Gateway	Virtual_wan1_gw
Во вкладке *Advanced* введите следующие параметры:	
Private IP Address	HA-wan1
Зайдите в меню *Interfaces→Ethernet→wan2*. Во вкладке *General* введите следующие параметры:	
IP Address	Virtual_wan2_ip
Network	Virtual_wan2net
Default Gateway	Оставьте пустым - None
Во вкладке *Advanced* введите следующие параметры:	
Private IP Address	HA-wan2
Настройка High Availability	
Зайдите в меню *System→High Availability*. Во вкладке *General* введите следующие параметры:	
Enable High Availability	Поставьте галочку
Cluster ID	1
Sync Interface	dmz
Node Type	Master
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	
gw-world:/>set Interface Ethernet wan1 DHCPEnabled=No gw-world:/>set Address IP4Address InterfaceAddresses/dmz_ip Name=Virtual_dmz_ip Address=172.17.100.254 gw-world:/>set Address IP4Address InterfaceAddresses/dmznet Name=Virtual_dmznet Address=172.17.100.0/24 gw-world:/>set Address IP4Address InterfaceAddresses/lan1_ip Name=Virtual_lan1_ip Address=192.168.10.254 gw-world:/>set Address IP4Address InterfaceAddresses/lan1net Name=Virtual_lan1net Address=192.168.10.0/24 gw-world:/>set Address IP4Address InterfaceAddresses/lan2_ip Name=Virtual_lan2_ip Address=192.168.20.254 gw-world:/>set Address IP4Address InterfaceAddresses/lan2net Name=Virtual_lan2net	

Address=192.168.20.0/24
gw-world:/>set Address IP4Address InterfaceAddresses/lan3_ip Name=Virtual_lan3_ip Address=192.168.30.254
gw-world:/>set Address IP4Address InterfaceAddresses/lan3net Name=Virtual_lan3net Address=192.168.30.0/24
gw-world:/>set Address IP4Address InterfaceAddresses/wan1_ip Name=Virtual_wan1_ip Address=192.168.110.254
gw-world:/>set Address IP4Address InterfaceAddresses/wan1net Name=Virtual_wan1net Address=192.168.110.0/24
gw-world:/>set Address IP4Address InterfaceAddresses/wan1_gw Name=Virtual_wan1_gw Address=192.168.110.250
gw-world:/>set Address IP4Address InterfaceAddresses/wan2_ip Name=Virtual_wan2_ip Address=192.168.120.254
gw-world:/>set Address IP4Address InterfaceAddresses/wan2net Name=Virtual_wan2net Address=192.168.120.0/24
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4HAAddress HA-dmzMasterIP=172.17.100.253 SlaveIP=172.17.100.252
gw-world:/labs> add IP4HAAddress HA-lan1 MasterIP=192.168.10.253 SlaveIP=192.168.10.252
gw-world:/labs> add IP4HAAddress HA-lan2 MasterIP=192.168.20.253 SlaveIP=192.168.20.252
gw-world:/labs> add IP4HAAddress HA-lan3 MasterIP=192.168.30.253 SlaveIP=192.168.30.252
gw-world:/labs> add IP4HAAddress HA-wan1 MasterIP=192.168.110.253 SlaveIP=192.168.110.252
gw-world:/labs> add IP4HAAddress HA-wan2 MasterIP=192.168.120.253 SlaveIP=192.168.120.252
gw-world:/labs> cc
gw-world:/> set Interface Ethernet dmz IP=InterfaceAddresses/Virtual_dmz_ip Network=InterfaceAddresses/Virtual_dmznet PrivateIP=labs/HA-dmz
gw-world:/> set Interface Ethernet lan1 IP=InterfaceAddresses/Virtual_lan1_ip Network=InterfaceAddresses/Virtual_lan1netPrivateIP=labs/HA-lan1
gw-world:/> set Interface Ethernet lan2 IP=InterfaceAddresses/Virtual_lan2_ip Network=InterfaceAddresses/Virtual_lan2netPrivateIP=labs/HA-lan2
gw-world:/> set Interface Ethernet lan3 IP=InterfaceAddresses/Virtual_lan3_ip Network=InterfaceAddresses/Virtual_lan3net PrivateIP=labs/HA-lan3
gw-world:/> set Interface Ethernet wan1 IP=InterfaceAddresses/Virtual_wan1_ip Network=InterfaceAddresses/Virtual_wan1net PrivateIP=labs/HA-wan1
gw-world:/> set Interface Ethernet wan2 IP=InterfaceAddresses/Virtual_wan2_ip Network=InterfaceAddresses/Virtual_wan2net PrivateIP=labs/HA-wan2
gw-world:/>HighAvailabilityEnabled=Yes ClusterID=1 SyncIface=dmz NodeID=Master
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Настройка DFL-1660

Устройство B

Web-интерфейс

Создание необходимых объектов

Зайдите в меню *Interfaces→Ethernet→wan1*. Выберите следующие параметры:

Enable DHCP Client	Снять галочку
IP address	wan1_ip
Network	wan1net
Default Gateway	wan1_gw

Зайдите в меню *Objects→Address Book→InterfaceAddresses*. Введите значения:	
dmz_ip переименуйте в Virtual_dmz_ip	172.17.100.254
dmznet переименуйте в Virtual_dmznet	172.17.100.0/24
lan1_ip переименуйте в Virtual_lan1_ip	192.168.10.254
lan1net переименуйте в Virtual_lan1net	192.168.10.0/24
lan2_ip переименуйте в Virtual_lan2_ip	192.168.20.254
lan2net переименуйте в Virtual_lan2net	192.168.20.0/24
lan3_ip переименуйте в Virtual_lan3_ip	192.168.30.254
lan3net переименуйте в Virtual_lan3net	192.168.30.0/24
wan1_ip переименуйте в Virtual_wan1_ip	192.168.110.254
wan1net переименуйте в Virtual_wan1net	192.168.110.0/24
wan1_gw переименуйте в Virtual_wan1_gw	192.168.110.250
wan2_ip переименуйте в Virtual_wan2_ip	192.168.120.254
wan2net переименуйте в Virtual_wan2net	192.168.120.0/24
Зайдите в меню *Objects→Address Book→InterfaceAddresses*. Создайте объект «IP4 HA address» для двух «реальных» IP-адресов **dmz-**интерфейса:	
Name	HA-dmz
Master IP address	172.17.100.253
Slave IP address	172.17.100.252
Зайдите в меню *Objects→Address Book→InterfaceAddresses*. Создайте объект «IP4 HA address» для двух «реальных» IP-адресов **lan1-**интерфейса:	
Name	HA-lan1
Master IP address	192.168.10.253
Slave IP address	192.168.10.252
Зайдите в меню *Objects→Address Book→InterfaceAddresses*. Создайте объект «IP4 HA address» для двух «реальных» IP-адресов **lan2-**интерфейса:	
Name	HA-lan2
Master IP address	192.168.20.253
Slave IP address	192.168.20.252
Зайдите в меню *Objects→Address Book→InterfaceAddresses*. Создайте объект «IP4 HA address» для двух «реальных» IP-адресов **lan3-**интерфейса:	
Name	HA-lan3
Master IP address	192.168.30.253
Slave IP address	192.168.30.252
Зайдите в меню *Objects→Address Book→InterfaceAddresses*. Создайте объект «IP4 HA address» для двух «реальных» IP-адресов **wan1-**интерфейса:	
Name	HA-wan1

Master IP address	192.168.110.253
Slave IP address	192.168.110.252
Зайдите в меню *Objects→Address Book→InterfaceAddresses*. Создайте объект «IP4 HA address» для двух «реальных» IP-адресов **wan2**-интерфейса:	
Name	HA-wan2
Master IP address	192.168.120.253
Slave IP address	192.168.120.252
Настройка интерфейсов	
Зайдите в меню *Interfaces→Ethernet→dmz.*Во вкладке *General* введите следующие параметры:	
IP Address	Virtual_dmz_ip
Network	Virtual_dmznet
Default Gateway	Оставьте пустым - None
Во вкладке *Advanced* введите следующие параметры:	
Private IP Address	HA-dmz
Зайдите в меню *Interfaces→Ethernet→lan1*. Во вкладке *General* введите следующие параметры:	
IP Address	Virtual_lan1_ip
Network	Virtual_lan1net
Default Gateway	Оставьте пустым - None
Во вкладке *Advanced* введите следующие параметры:	
Private IP Address	HA-lan1
Зайдите в меню *Interfaces→Ethernet→lan2*. Во вкладке *General* введите следующие параметры:	
IP Address	Virtual_lan2_ip
Network	Virtual_lan2net
Default Gateway	Оставьте пустым - None
Во вкладке *Advanced* введите следующие параметры:	
Private IP Address	HA-lan2
Зайдите в меню *Interfaces→Ethernet→lan3*. Во вкладке *General* введите следующие параметры:	
IP Address	Virtual_lan3_ip
Network	Virtual_lan3net
Default Gateway	Оставьте пустым - None
Во вкладке *Advanced* введите следующие параметры:	
Private IP Address	HA-lan3
Зайдите в меню *Interfaces→Ethernet→wan1*. Во вкладке *General* введите следующие параметры:	
IP Address	Virtual_wan1_ip
Network	Virtual_wan1net
Default Gateway	Virtual_wan1_gw
Во вкладке *Advanced* введите следующие параметры:	
Private IP Address	HA-wan1
Зайдите в меню *Interfaces→Ethernet→wan2*. Во вкладке *General* введите следующие параметры:	
IP Address	Virtual_wan2_ip
Network	Virtual_wan2net
Default Gateway	Оставьте пустым – None
Во вкладке *Advanced* введите следующие параметры:	

Private IP Address	HA_wan2
Настройка High Availability	
Зайдите в меню *System→High Availability*. Во вкладке *General* введите следующие параметры:	
Enable High Availability	Поставьте галочку
Cluster ID	1
Sync Interface	dmz
Node Type	Slave
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Командная строка (CLI)	

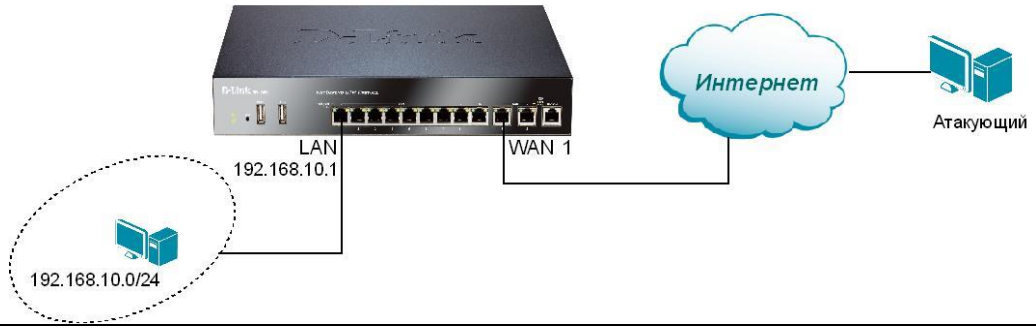
```
gw-world:/>set Interface Ethernet wan1 DHCPEnabled=No
gw-world:/>set Address IP4Address InterfaceAddresses/dmz_ip Name=Virtual_dmz_ip
Address=172.17.100.254
gw-world:/>set Address IP4Address InterfaceAddresses/dmznet Name=Virtual_dmznet
Address=172.17.100.0/24
gw-world:/>set Address IP4Address InterfaceAddresses/lan1_ip Name=Virtual_lan1_ip
Address=192.168.10.254
gw-world:/>set Address IP4Address InterfaceAddresses/lan1net Name=Virtual_lan1net
Address=192.168.10.0/24
gw-world:/>set Address IP4Address InterfaceAddresses/lan2_ip Name=Virtual_lan2_ip
Address=192.168.20.254
gw-world:/>set Address IP4Address InterfaceAddresses/lan2net Name=Virtual_lan2net
Address=192.168.20.0/24
gw-world:/>set Address IP4Address InterfaceAddresses/lan3_ip Name=Virtual_lan3_ip
Address=192.168.30.254
gw-world:/>set Address IP4Address InterfaceAddresses/lan3net Name=Virtual_lan3net
Address=192.168.30.0/24
gw-world:/>set Address IP4Address InterfaceAddresses/wan1_ip Name=Virtual_wan1_ip
Address=192.168.110.254
gw-world:/>set Address IP4Address InterfaceAddresses/wan1net Name=Virtual_wan1net
Address=192.168.110.0/24
gw-world:/>set Address IP4Address InterfaceAddresses/wan1_gw Name=Virtual_wan1_gw
Address=192.168.110.250
gw-world:/>set Address IP4Address InterfaceAddresses/wan2_ip Name=Virtual_wan2_ip
Address=192.168.120.254
gw-world:/>set Address IP4Address InterfaceAddresses/wan2net Name=Virtual_wan2net
Address=192.168.120.0/24
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4HAAddress HA-dmzMasterIP=172.17.100.253 SlaveIP=172.17.100.252
gw-world:/labs> add IP4HAAddress HA-lan1 MasterIP=192.168.10.253 SlaveIP=192.168.10.252
gw-world:/labs> add IP4HAAddress HA-lan2 MasterIP=192.168.20.253 SlaveIP=192.168.20.252
gw-world:/labs> add IP4HAAddress HA-lan3 MasterIP=192.168.30.253 SlaveIP=192.168.30.252
gw-world:/labs> add IP4HAAddress HA-wan1 MasterIP=192.168.110.253 SlaveIP=192.168.110.252
gw-world:/labs> add IP4HAAddress HA-wan2 MasterIP=192.168.120.253 SlaveIP=192.168.120.252
gw-world:/labs> cc
gw-world:/> set Interface Ethernet dmz IP=InterfaceAddresses/Virtual_dmz_ip
Network=InterfaceAddresses/Virtual_dmznet PrivateIP=labs/HA-dmz
gw-world:/> set Interface Ethernet lan1 IP=InterfaceAddresses/Virtual_lan1_ip
Network=InterfaceAddresses/Virtual_lan1netPrivateIP=labs/HA-lan1
gw-world:/> set Interface Ethernet lan2 IP=InterfaceAddresses/Virtual_lan2_ip
Network=InterfaceAddresses/Virtual_lan2netPrivateIP=labs/HA-lan2
gw-world:/> set Interface Ethernet lan3 IP=InterfaceAddresses/Virtual_lan3_ip
```

Network=InterfaceAddresses/Virtual_lan3net PrivateIP=labs/HA-lan3 gw-world:/> set Interface Ethernet wan1 IP=InterfaceAddresses/Virtual_wan1_ip Network=InterfaceAddresses/Virtual_wan1net PrivateIP=labs/HA-wan1 gw-world:/> set Interface Ethernet wan2 IP=InterfaceAddresses/Virtual_wan2_ip Network=InterfaceAddresses/Virtual_wan2net PrivateIP=labs/HA-wan2 gw-world:/>HighAvailabilityEnabled=Yes ClusterID=1 SyncIface=dmz NodeID=Slave gw-world:/> activate gw-world:/>commit	
Упражнение	Проверьте работоспособность кластерной схемы. Отключите физически сетевой кабель от устройства Master, убедитесь в доступности всех настроенных сервисов, уточните статус устройства Slave.

ЗАНЯТИЕ №24. Защита от сетевых атак. Защита от атак типа «отказ в обслуживании» DoS, встроенные механизмы защиты. «Черные» и «белые» списки хостов и сетей. Настройка SMTP Receiver. Активная сетевая защита Intrusion Detection Prevention (IDP). Настройка системы IDP/IPS: для защиты Web-сервера на базе службы IIS операционной системы Microsoft Windows Server, для защиты FTP-сервера, почтового сервера, MS SQL-сервера, NFS-сервера на базе Oracle Solaris. Защита от сетевых атак при помощи пороговых правил (Threshold Rules). Настройка IDP/IPS для защиты пользователей lan-сети, имеющих доступ в Интернет.

Основное назначение межсетевого экрана – защита сети от различных видов сетевых атак. В межсетевых экранах D-Link используется несколько видов обеспечения сетевой защиты.

Цель	Эта лабораторная работа позволяет пользователем изучить механизмы защиты от сетевых атак на межсетевых экранах D-Link.	
Оборудование	DFL-860E	1
	Рабочая станция	2
	Ethernet-кабель (патч-корд)	4

Функции защиты от атак DoS	*Этот сценарий описывает существующие встроенные механизмы защиты межсетевого экрана от атак типа DoS (Denial of Service).*
Описание сценария	*На сегодняшний день хакеры располагают всё более совершенными средствами осуществления атак. Инструментальные средства атак можно открыто скачать в Интернете, процесс атаки может быть легко автоматизирован. Большое количество новых методов атак используют распределенную природу Интернета для запуска атак типа «отказ в обслуживании» (DoS, на сервер отправляется неограниченное количество запросов) против организаций, в результате чего их сервера становятся не в состоянии отвечать на легитимные запросы.*
Схема 84	
Настройка DFL-860E	
АтакаPing of Death и Jolt Attacks	
Описание атаки	*Атака «ping of death» является одной из ранних атак 3 и 4 уровня. Jolt – программное обеспечение, позволяющее генерировать ping-пакеты с неверным размером пакетов. Данные действия приводят к переполнению 16-битной переменной и переходу к очень малому значению, что обусловлено реализацией IP-стека.*

Примечание: наличие атаки «ping of death» будет зарегистрировано в логах с пометкой «пакет отброшен – LogOversizedPackets». Наличие таких записей в лог-файлах означает попытку атаки этого типа через устройство.	
Атаки перекрытия фрагментации (Fragmentation overlap attacks)	
Описание атаки	*Атака «fragmentation overlap attacks» использует уязвимость стека IP при некорректном заголовке пакета с перекрытием фрагментов. Типы подобных атак – Teardrop, Bonk, Boink, Nestea. Обычно существует однотипное хакерское программное обеспечение для осуществления атаки.*
Примечание: наличие атаки «fragment overlap attack» будет зарегистрировано в логах с пометкой «пакет отброшен –IllegalFrags». Наличие таких записей в лог-файлах означает попытку атаки этого типа через устройство.	
Атаки Land и LaTierra	
Описание атаки	*Атаки типа Land и LaTierra посылают пакеты к цели атаки и заставляют ее отвечать самой себе, и далее в цикле, что приводит к выходу из строя цели атаки. Подобный эффект достигается посылкой IP-пакетов с одинаковыми IP-адресами цели атаки в поле источника и приёмника. Межсетевой экран обеспечивает защиту от подобной атаки, используя защиту от IP-спуфинга (IPspoofing) для всех пакетов. IP-спуфинг – подмена адреса отправителя в поле адреса IP-пакета. По умолчанию будет производится сравнение приходящих пакетов с таблицей маршрутизации. Если пакет отправляется на интерфейс, отличный от интерфейса, где система ожидала «видеть» источник, то пакет будет отброшен.*
Примечание: наличие атак Land и LaTierra будет зарегистрировано в логах с пометкой «пакет отброшен –AutoAccess».	
Атака WinNuke	
Описание атаки	*Атаки типа WinNuke осуществляются путём подключения к TCP-службе, не имеющей обработчиков «срочных»данных («out-of-band» – TCP-пакеты с пометкой срочной пересылки URG), но принимающие такие данные. Это приводит к зацикливанию службы на выполнение обработки этих данных, на что уходит практически всё CPU-время. Одна из подобных служб – NetBIOS через TCP/IP.* *Защита может быть обеспеченна аккуратной политикой правил безопасности внутренней сети, т.к. публичные службы лучше защищены, чем службы локальной сети.* *Второй способ – установка флага URG bit по умолчанию для всех TCP-сегментов.*
Зайдите в меню *System→Advanced Settings→TCP Settings*. Введите значения:	
TCP Urg	StripLog
Примечание: наличие атаки «WinNuke» для соединений, разрешенных в системе, будет зарегистрировано в логах с пометкой «пакет отброшен –TCPUrg». Наличие таких записей в лог-файлах означает попытку атаки этого типа через устройство. Выставление флагов для сегментов TCP осуществляется только после задания правил обработки пакетов межсетевого экрана.	
Атаки типа Amplification (Smurf, papasmurf, Fraggle)	

Описание атаки	*Атаки типа Amplification осуществляются путём «усиления» потока пакетов в плохо сконфигурированной сети и их посылки на выбранную цель атаки. Интенсивное увеличение полосы пропускания захватывает все возможности Интернет-подключений. Атакующий, даже имея меньшую полосу пропускания, может усилить поток пакетов для атаки цели с гораздо большей полосой пропускания канала Интернет-соединения.* *Атаки типа «Smurf» и «Papasmurf» посылают эхо-пакеты ICMP на широковещательный адрес (broadcast) сети с большим количеством машин, заставляя IP-адрес источника являться целью атаки. Все машины в открытой сети «отвечают» атакуемой машине.* *Атаки типа «Fraggle» используют ту же идею, но посылают эхо-пакеты UDP по 7-му порту. Этот тип атаки дает меньший фактор усиления, т.к. в Интернете меньше хостов, с разрешённой эхо-службой UDP.*
Примечание: атаки «Smurf» будут зарегистрированы в логах с пометкой «пакет отброшен –ICMPEchoReplypackets». Атаки «Smurf» будут зарегистрированы в логах как масса пакетов с пометкой «пакет отброшен», «пакет пропущен» – в зависимости от настроенных политик. Наличие таких записей в лог-файлах означает попытку атаки этого типа через устройство. IP-адреса источников будут соответствовать адресам сети «усиления».	
Зайдите в меню *System→Advanced Settings→IP Settings.* Здесь можно настроить отбрасывание широковещательных пакетов, отправляемых в напрямую подключенные сети:	
Directed Broadcasts	DropLog
Защита на стороне цели атаки	*«Smurf» и «Papasmurf» затопляющие сеть пакеты будут видны на стороне цели как ICMPEchoResponses. Этим пакетам никогда не будет позволено инициировать новое подключение в зависимости от разрешающих или запрещающих правил, только если не используется правило «Forward Fast».* *Пакеты атаки «Fraggle» могут достичь любого UDP-порта назначения, определенного хакером. Помочь в борьбе с этим типом атаки может ужесточение правил внутренней сети и функция Traffic Shaping.*
Атаки IP Spoofing	
Описание атаки	*Злоумышленник фальсифицирует IP-адрес пакетов, идущих с доверенного хоста, с целью обмана системы безопасности межсетевого экрана. Такая атака известна как Spoofing.* *IP spoofing – одна из наиболее распространенных атак spoofing. Злоумышленники используют IP-адреса доверенных хостов, чтобы «обойти» фильтрацию. В заголовке IP-пакета указывается адрес источника пакета, измененный злоумышленником и используемый как адрес локального хоста. Межсетевой экран воспринимает пакет как пришедший с доверенного источника. Хотя источник пакета не может отреагировать корректно, возникает потенциальная угроза перегрузки сети и создания условий для атак Denial of Service (DoS).*
Правила Access Rule	*Перед проверкой нового соединения на соответствие набору IP-правил, система NetDefendOS выполняет проверку источника соединения на соответствие Правилам доступа. Правила доступа могут использоваться для того, чтобы определить источник трафика на указанном интерфейсе, а также для*

	автоматической блокировки пакетов с определенных источников. Правила доступа обеспечивают эффективную и направленную фильтрацию новых попыток соединения. Если администратор не может четко указать какие-либо Правила доступа, используется Правило доступа по умолчанию. *Правило доступа по умолчанию не является действующим, но на его основе осуществляется проверка входящего трафика с выполнением обратного поиска (reverse lookup) в таблицах маршрутизации NetDefendOS. Данный поиск выполняется для подтверждения того, что входящий трафик идет от источника, который, как указано в таблицах маршрутизации, доступен через интерфейс, на который приходит трафик. В случае сбоя обратного поиска, произойдет потеря соединения и генерирование журнального сообщения об отбрасывании пакетов правилом Default Access Rule.* *Если при выполнении поиска и устранения неисправностей произошла потеря соединения, администратору необходимо просмотреть сообщения Default Access Rule в журналах. Решением проблемы является создание маршрута для интерфейса входящего соединения. Таким образом, сеть назначения маршрута та же, или в диапазон адресов сети входит IP-адрес входящего соединения.*
Создадим пользовательское правило доступа. Зайдите в меню *Rules→Access→Add→Access*. Введите значения:	
Name	My_access_rule
Action	Expect
Interface	wan1
Network	all-nets
Примечание: Действие Expect – при соответствии адреса отправителя пакета указанной сети интерфейс, на который приходит пакет, сравнивается с указанным интерфейсом. При соответствии интерфейсов, пакет принимается, далее задействуются IP Rules. Если интерфейсы не совпадают, пакет отбрасывается, наличие атаки IP-spoofing может быть зарегистрировано в логах с пометкой «пакет отброшен – DefaultAccessRule» или «пакет отброшен – My_access_rule».	
Атаки TCP SYN Flood	
Описание атаки	*Атаки типа TCP SYN Flood осуществляются путём отправки большого количества TCP SYN-пакетов на определённый порт и затем игнорирования ответного сообщения SYN ACKs. Эти действия приведут к уменьшению ресурсов локального TCP-стека атакуемой машины до тех пор, пока она станет неспособна отвечать на SYN-пакеты до истечения тайм-аута половины существующих соединений.* *Межсетевой экран будет защищать от атак TCP SYN Flood, если защита включена для объекта Service, соответствующего правилу в наборе IP-правил,и это правило – разрешающее. По умолчанию данный механизм применяется к предопределенным службам http-in, https-in, smtp-in, ssh-in. Для вновь созданной службы защита может быть включена или отключена по усмотрению администратора.* *Защита «SynRelay» работает посредством совершения 3-х соединений с клиентом перед осуществлением второго соединения со службой назначения. Операционная система межсетевого экрана, в отличие от обычной системы хостов,*

	может обработать тысячи или миллионы проблемных соединений (обычная ОС – не больше 5-ти «зависших» наполовину установленных соединений) до того, как возникнет проблема в работе устройства. При заполнении таблицы состояний старые ожидающие SYN-соединения будут среди первых по очереди на отбрасывание для уменьшения числа соединений.
По умолчанию опция SYN Flood Protection включена на всех ALG, дополнительная настройка не требуется. Для дополнительный защиты можно включить SYN Flood Protection для служб, разрешенных на межсетевом экране. Для этого в окне настроек конкретной службы необходимо поставить галочку *SYN flood protection*.	
Примечание: 1. Атаки «TCP SYN Flood» будут зарегистрированы в логах как огромное количество новых соединений (отброшенных, если атака идет на закрытый порт). IP-адрес отправителя обычно подменяется случайным образом. ***2. Если защита от Syn Flood включена для некоторого объекта Service и этот объект имеет ALG, связанный с данной службой, то ALG будет запрещен.***	
Атака Jolt2	
Описание атаки	*Атака Jolt2 осуществляются путём отправки большого потока однотипных фрагментов на атакуемую машину. Несколько сотен пакетов в секунду «затормаживают» работу атакуемого компьютера до окончания потока пакетов.* *Межсетевой экран полностью защищает от этой атаки. Первый фрагмент будет помещён в очередь, ожидая остальные фрагменты для отправки их в заданном порядке сразу все вместе. Но остальные пакеты никогда не поступят, таким образом, первый фрагмент не будет пропущен. С остальными одинаковыми фрагментами потока пакетов будут проведены те же действия.*
Защита заключается в настройке определенного предела размера пакетов для каждого протокола. Зайдите в меню *System→Advanced Setting→Length Limit Settings*, просмотрите текущие настройки. Если на устройство придет пакет с превышением лимита, он сразу будет отброшен.	
Примечание: 1. Если смещение фрагмента (fragment offset) атакующего потока выше, чем Length Lim, то фрагменты будут отброшены сразу. ***2. Атаки «Jolt2» могут быть зарегистрированы или не зарегистрированы в логах. Если смещение фрагмента слишком большое, то в логах будут помечены отброшенные фрагменты – LogOversizedPackets. Если смещение достаточно для применения правил, то в логах отмечаться не будет.*** ***3. IP-адрес отправителя может подменяться.***	
Атаки Distributed Denial of Service (DDoS)	
Описание атаки	*Атака типа DDoS представляют собой более сложную форму атак отказа в обслуживании, осуществляются с сотен или тысяч машин в Интернете, на которые хакером установлено специальное ПО. Атака координируется хакером, обычно приводит к превышению пропускной способности, перегрузки процессов вычисления маршрутов, переполнение стеков, нарушение соединений в целевой сети.* *Средства осуществления этого вида атак – Trin00, Tribe Flood Network (TFN), Stacheldraht.* *Защита от атак DDoS – более сложная задача, но могут быть использованы средства, описанные выше. При этом атака DDoS может включать в себя различные типы других атак. Средство «черных» и «белых» списков хостов и сетей позволяет уменьшить эффективность атак DDoS.*

Описание механизма защиты	*Intrusion Detection System (IDS) – система обнаружения вторжения, синоним – Intrusion Detection Prevention (IDP). IDS – технология, которая позволяет мониторить сетевой трафик с целью обнаружения возможных нарушений безопасности – вторжений в сеть. Вторжение – это попытка взломать или обойти защитные механизмы корпоративной сети предприятия. Существуют различные формы атак в Интернете, и часто процедура атаки может быть легко автоматизирована хакерами. Для работы системы IDS необходимо указать 3 группы параметров:* *- какой трафик анализировать,* *- какой тип атаки искать,* *- какое действие выполнять при обнаружении угрозы.* *Intrusion Detection Rules (IDR)* – правила обнаружения вторжения *– определяют тип трафика (service), который требует анализа. Поля фильтрации, включающие интерфейсы источника и назначения, порты, протоколы, также определяются IDR. Только трафик, удовлетворяющий правилам IDR, пропускается на следующий уровень анализа IDS.* *Signatures* – сигнатуры – *определяют «образец» определенной атаки, метод называется определение сигнатур.* *После обнаружения сигнатуры атаки, осуществляется определенное* действие *(action). В зависимости от опасности атаки трафик может быть отброшен, залогирован, отброшен и залогирован, или просто игнорирован (drooped, logged, both, ignored).* Цепь событий *(chain of events) определяет два сценария обработки трафика. В первом случае пакеты пропускаются правилами межсетевого экрана до попадания на IDS, во втором – пакеты пропускаются в IDS, даже если правила межсетевого экрана это запрещают (вариант для логирования пакетов).* *Группы сигнатур (signature groups) – объединенный набор сигнатур, обычно использующийся для одного протокола и двух групп для внутренней и внешней сети.* *Базы данных сигнатур требуют постоянного обновления. Период обновления можно настроить, обновление на межсетевых экранах D-Link происходит по протоколу HTTP с сайта D-Link.* *Для автоматического оповещения об обнаружении вторжения необходимо сконфигурировать SMTP Log Receiver для IDS Events. При возникновении IDS event межсетевой экран будет ждать в течении* Hold Time *секунд, перед посылкой уведомления по почте. Сообщение будет отправлено при возникновении определенного количества событий, равного или большего чем* Log Threshold. *После отправки сообщения межсетевой экран будет ждать* Minimum Repeat Time *секунд перед посылкой нового сообщения.*
Примеры лог-сообщений при аудите к DoS-атакам на межсетевой экран с использованием сканера уязвимостей Rapid7 Nexpose. На рисунке 7.11 показаны лог-сообщения при сканировании портов.	
Рисунок 7.11	

2012-02-22 14:31:27	Warning	RULE 6000051	Default_Rule	TCP	lan	192.168.10.7 192.168.10.1	29188 759	ruleset_drop_packet drop
ipdatalen=20 syn=1								
2012-02-22 14:31:27	Warning	RULE 6000051	Default_Rule	TCP	lan	192.168.10.7 192.168.10.1	29187 2002	ruleset_drop_packet drop
ipdatalen=20 syn=1								
2012-02-22 14:31:27	Warning	RULE 6000051	Default_Rule	TCP	lan	192.168.10.7 192.168.10.1	29187 2002	ruleset_drop_packet drop
ipdatalen=20 syn=1								
2012-02-22 14:31:27	Warning	RULE 6000051	Default_Rule	TCP	lan	192.168.10.7 192.168.10.1	29186 25	ruleset_drop_packet drop
ipdatalen=20 syn=1								
2012-02-22 14:31:27	Warning	RULE 6000051	Default_Rule	TCP	lan	192.168.10.7 192.168.10.1	29185 369	ruleset_drop_packet drop
ipdatalen=20 syn=1								
2012-02-22 14:31:27	Warning	RULE 6000051	Default_Rule	TCP	lan	192.168.10.7 192.168.10.1	29185 369	ruleset_drop_packet drop
ipdatalen=20 syn=1								
2012-02-22 14:31:27	Warning	RULE 6000051	Default_Rule	TCP	lan	192.168.10.7 192.168.10.1	29184 461	ruleset_drop_packet drop
ipdatalen=20 syn=1								
2012-02-22 14:31:27	Warning	RULE 6000051	Default_Rule	TCP	lan	192.168.10.7 192.168.10.1	29184 461	ruleset_drop_packet drop
ipdatalen=20 syn=1								
2012-02-22 14:31:27	Warning	RULE 6000051	Default_Rule	TCP	lan	192.168.10.7 192.168.10.1	29183 852	ruleset_drop_packet drop
ipdatalen=20 syn=1								
2012-02-22 14:31:27	Warning	RULE 6000051	Default_Rule	TCP	lan	192.168.10.7 192.168.10.1	29183 852	ruleset_drop_packet drop
ipdatalen=20 syn=1								
2012-02-22 14:31:27	Warning	RULE 6000051	Default_Rule	TCP	lan	192.168.10.7 192.168.10.1	29182 690	ruleset_drop_packet drop
ipdatalen=20 syn=1								
2012-02-22 14:31:27	Warning	RULE 6000051	Default_Rule	TCP	lan	192.168.10.7 192.168.10.1	29182 690	ruleset_drop_packet drop
ipdatalen=20 syn=1								
2012-02-22 14:31:27	Warning	RULE 6000051	Default_Rule	TCP	lan	192.168.10.7 192.168.10.1	29189 726	ruleset_drop_packet drop
ipdatalen=20 syn=1								
2012-02-22 14:31:27	Warning	RULE 6000051	Default_Rule	TCP	lan	192.168.10.7 192.168.10.1	29189 726	ruleset_drop_packet drop
ipdatalen=20 syn=1								

На рисунке 7.12 показаны лог-сообщения при подборе логина к встроенному Web-серверу межсетевого экрана и попытка вторжения через порт SNMP.

Рисунок 7.12

2012-02-22 14:44:04	Warning	SYSTEM 3203002						admin_login_failed disallow_admin_access
authsystem=HTTPS username= server_ip=192.168.10.1 server_port=443 client_ip=192.168.10.7 client_port=4046								
2012-02-22 14:44:02	Warning	SYSTEM 3203002						admin_login_failed disallow_admin_access
authsystem=HTTPS username= server_ip=192.168.10.1 server_port=443 client_ip=192.168.10.7 client_port=4004								
2012-02-22 14:44:02	Warning	IP_PROTO 7000014	TTLOnLowMulticast	UDP	lan	192.168.10.7 239.255.255.250	49172 1900	ttl_low drop
ttl=1 ttlmin=3 ipdatalen=125 udptotlen=125								
2012-02-22 14:44:01	Notice	RULE 6000060	LocalUndelivered	UDP	lan	192.168.10.7 192.168.10.1	49188 161	unhandled_local drop
ipdatalen=20 udptotlen=20								
2012-02-22 14:44:01	Notice	SNMP 3100001		UDP	lan core	192.168.10.7 192.168.10.1	49188 161	disallowed_sender drop
peer=192.168.10.7 origsent=0 termsent=0								
2012-02-22 14:44:01	Info	CONN 600001	SNMPBeforeRules	UDP	lan core	192.168.10.7 192.168.10.1	49188 161	conn_open
conn=open								
2012-02-22 14:44:00	Notice	RULE 6000060	LocalUndelivered	UDP	lan	192.168.10.7 192.168.10.1	49187 161	unhandled_local drop
ipdatalen=20 udptotlen=20								

На рисунке 7.13 показаны лог-сообщения при подборе логина для доступа на межсетевой экран через SSH.

Рисунок 7.13

2012-02-22 14:33:23	Warning	SYSTEM 3203002						admin_login_failed disallow_admin_access
authsystem=SSH username=root client_ip=192.168.10.7 client_port=3249								
2012-02-22 14:33:23	Warning	SYSTEM 3203002						admin_login_failed disallow_admin_access
authsystem=SSH username=root client_ip=192.168.10.7 client_port=3248								
2012-02-22 14:33:23	Warning	SYSTEM 3203002						admin_login_failed disallow_admin_access
authsystem=SSH username=guest client_ip=192.168.10.7 client_port=3247								
2012-02-22 14:33:23	Warning	SYSTEM 3203002						admin_login_failed disallow_admin_access
authsystem=SSH username=admin client_ip=192.168.10.7 client_port=3246								
2012-02-22 14:33:23	Warning	SYSTEM 3203002						admin_login_failed disallow_admin_access
authsystem=SSH username=pix client_ip=192.168.10.7 client_port=3245								
2012-02-22 14:33:22	Warning	SYSTEM 3203002						admin_login_failed disallow_admin_access
authsystem=SSH username=pix client_ip=192.168.10.7 client_port=3243								
2012-02-22 14:33:22	Warning	SYSTEM 3203002						admin_login_failed disallow_admin_access
authsystem=SSH username=pix client_ip=192.168.10.7 client_port=3242								
2012-02-22 14:33:22	Warning	SYSTEM 3203002						admin_login_failed disallow_admin_access
authsystem=SSH username=cisco client_ip=192.168.10.7 client_port=3239								

На рисунке 7.14 показаны лог-сообщения при атаке на PPTP-туннель. Туннель создан злоумышленником. В прошивке межсетевого экрана выявлена ошибка – неизвестное правило, помеченное вопросительными знаками.

Рисунок 7.14

2012-02-22 18:07:35	Info	CONN 600002	,��	TCP	wan1 core	10.72.246.212 10.72.246.213	2417 1723	conn_close close
conn=close origsent=776 termsent=320								
2012-02-22 18:07:35	Info	CONN 600002	,��	TCP	wan1 core	10.72.246.212 10.72.246.213	2411 1723	conn_close close
conn=close origsent=472 termsent=164								
2012-02-22 18:07:34	Notice	PPTP 2700019						pptp_tunnel_up
iface=pptp_server remotegw=10.72.246.212								
2012-02-22 18:07:34	Warning	PPTP 2700014						tunnel_idle_timeout close_tunnel
iface=pptp_server remotegw=10.72.246.212								
2012-02-22 18:07:25	Info	CONN 600002	,��	TCP	wan1 core	10.72.246.212 10.72.246.213	54019 1723	conn_close close
conn=close origsent=128 termsent=44								

На рисунке 7.15 показаны лог-сообщения: неверный формат ICMP-сообщений вызвал их запрет межсетевым экраном, хотя ping lan_ip (192.168.10.1) по умолчанию разрешен, далее идет попытка установить IPSec-туннель (легально настроенный на межсетевом экране), последнее лог-сообщение в списке – отброшен пакет якобы уже существующего (на самом деле несуществующего) TCP-соединения по SSH.

Рисунок 7.15

2012-02-22 13:26:05	Warning	RULE 6000051	Default_Rule	ICMP	lan	192.168.10.7 192.168.10.1		ruleset_drop_packet drop
ipdatalen=12 icmptype=ADDR_MASK icmpcode=0								
2012-02-22 13:26:05	Warning	RULE 6000051	Default_Rule	ICMP	lan	192.168.10.7 192.168.10.1		ruleset_drop_packet drop
ipdatalen=12 icmptype=ADDR_MASK icmpcode=0								
2012-02-22 13:26:05	Info	IPSEC 1802708						ike_sa_destroyed ike_sa_killed
ike_sa=" Initiator SPI ESP=0x3127fcb0, AH=0x38109e89, IPComp=0x3224498"								
2012-02-22 13:26:05	Warning	IPSEC 1802022						ike_sa_failed no_ike_sa
statusmsg="No proposal chosen" local_peer="192.168.10.1 ID No Id" remote_peer="192.168.10.7:52057 ID No Id" initiator_spi="ESP=0x3127fcb0, AH=0x38109e89, IPComp=0x3224498a"								
2012-02-22 13:26:05	Warning	IPSEC 1802715						event_on_ike_sa
side=Responder msg="failed" int_severity=6								
2012-02-22 13:26:05	Warning	IPSEC 1800107						ike_invalid_proposal
local_ip=192.168.10.1 remote_ip=192.168.10.7 cookies=3127fcb038109e893224498a0b0c8b41 reason="Could not find acceptable proposal"								
2012-02-22 13:26:05	Notice	IPSEC 1802300						rule_selection_failed
info="Peer IP address mismatch" int_severity=6								
2012-02-22 13:26:05	Info	IPSEC 1803001						failed_to_select_policy_rule
2012-02-22 13:26:05	Warning	IPSEC 1802715						event_on_ike_sa
side=Responder msg="failed" int_severity=6								
2012-02-22 13:26:05	Info	CONN 600001	IPsecBeforeRules	UDP	lan core	192.168.10.7 192.168.10.1	52057 500	conn_open
conn=open								
2012-02-22 13:26:05	Warning	CONN 600012	LogOpenFails	TCP	lan	192.168.10.7 192.168.10.1	34034 22	no_new_conn_for_this_packet reject
protocol=tcp ipdatalen=21 ack=1 psh=1								

На рисунке 7.16 показаны лог-сообщения: неверный формат TCP-сообщений и некорректная длина, указанная в опциях пакета TCP.

Рисунок 7.16

2012-02-22 13:18:12	Warning	IP_OPT 1700023	IPOPT_OTHER	TCP	lan	192.168.10.7 192.168.10.1	1024 666	ipopt_present_disallowed drop
ipopt=40 optname=UNKNOWN iphdrlen=60 ipdatalen=20 syn=1								
2012-02-22 13:18:12	Warning	IP_OPT 1700023	IPOPT_OTHER	TCP	lan	192.168.10.7 192.168.10.1	1024 666	ipopt_present_disallowed drop
ipopt=40 optname=UNKNOWN iphdrlen=60 ipdatalen=20 syn=1								
2012-02-22 13:18:12	Warning	IP_OPT 1700023	IPOPT_OTHER	TCP	lan	192.168.10.7 192.168.10.1	1024 666	ipopt_present_disallowed drop
ipopt=40 optname=UNKNOWN iphdrlen=60 ipdatalen=20 syn=1								
2012-02-22 13:18:12	Warning	TCP_OPT 3400011	TCPOptionsSizes	TCP	lan	192.168.10.7 192.168.10.1	1024 443	bad_tcpopt_length drop
tcpopt=4 len=253 avail=2 ipdatalen=28 tcphdrlen=28								
2012-02-22 13:18:12	Warning	TCP_OPT 3400011	TCPOptionsSizes	TCP	lan	192.168.10.7 192.168.10.1	1024 443	bad_tcpopt_length drop
tcpopt=4 len=253 avail=2 ipdatalen=28 tcphdrlen=28								
2012-02-22 13:18:12	Warning	TCP_OPT 3400011	TCPOptionsSizes	TCP	lan	192.168.10.7 192.168.10.1	1024 443	bad_tcpopt_length drop
tcpopt=4 len=253 avail=2 ipdatalen=28 tcphdrlen=28								
2012-02-22 13:18:12	Warning	TCP_OPT 3400011	TCPOptionsSizes	TCP	lan	192.168.10.7 192.168.10.1	1024 22	bad_tcpopt_length drop
tcpopt=4 len=253 avail=2 ipdatalen=28 tcphdrlen=28								
2012-02-22 13:18:12	Warning	TCP_OPT 3400011	TCPOptionsSizes	TCP	lan	192.168.10.7 192.168.10.1	1024 22	bad_tcpopt_length drop
tcpopt=4 len=253 avail=2 ipdatalen=28 tcphdrlen=28								
2012-02-22 13:18:12	Warning	TCP_OPT 3400011	TCPOptionsSizes	TCP	lan	192.168.10.7 192.168.10.1	1024 22	bad_tcpopt_length drop
tcpopt=4 len=253 avail=2 ipdatalen=28 tcphdrlen=28								

На рисунке 7.17 показаны лог-сообщения: отброшены TCP-пакеты с флагом URG (срочная пересылка).

Рисунок 7.17

2012-02-22 14:33:10	Warning	TCP_FLAG 3300008	TCPFinUrg	TCP	lan	192.168.10.7 192.168.10.1	29202 42325	tcp_flags_set drop
good_flag=FIN bad_flag=URG ipdatalen=40 tcphdrlen=40 psh=1 fin=1 urg=1								
2012-02-22 14:33:10	Warning	TCP_FLAG 3300008	TCPFinUrg	TCP	lan	192.168.10.7 192.168.10.1	29202 42325	tcp_flags_set drop
good_flag=FIN bad_flag=URG ipdatalen=40 tcphdrlen=40 psh=1 fin=1 urg=1								

На рисунке 7.18 показаны лог-сообщения: предотвращена попытка «затопления» SYN-пакетами для TCP.

Рисунок 7.18

2012-02-22 14:37:46	Warning	TCP_FLAG 3300008	TCPSynRst	TCP	lan	192.168.10.7 192.168.10.1	29255 445	tcp_flags_set drop
good_flag=SYN bad_flag=RST ipdatalen=20 syn=1 rst=1								
2012-02-22 14:37:46	Warning	TCP_FLAG 3300008	TCPSynRst	TCP	lan	192.168.10.7 192.168.10.1	29256 443	tcp_flags_set drop
good_flag=SYN bad_flag=RST ipdatalen=20 syn=1 rst=1								
2012-02-22 14:37:46	Warning	TCP_FLAG 3300008	TCPSynRst	TCP	lan	192.168.10.7 192.168.10.1	29255 445	tcp_flags_set drop
good_flag=SYN bad_flag=RST ipdatalen=20 syn=1 rst=1								
2012-02-22 14:37:46	Warning	RULE 6000051	Default_Rule	UDP	lan	192.168.10.7 192.168.10.1	49179 17185	ruleset_drop_packet drop
ipdatalen=72 udptotlen=72								
2012-02-22 14:37:46	Warning	TCP_FLAG 3300008	TCPSynRst	TCP	lan	192.168.10.7 192.168.10.1	29254 139	tcp_flags_set drop
good_flag=SYN bad_flag=RST ipdatalen=20 syn=1 rst=1								
2012-02-22 14:37:46	Warning	TCP_FLAG 3300008	TCPSynRst	TCP	lan	192.168.10.7 192.168.10.1	29242 8080	tcp_flags_set drop
good_flag=SYN bad_flag=RST ipdatalen=20 syn=1 rst=1								
2012-02-22 14:37:46	Warning	TCP_FLAG 3300008	TCPSynRst	TCP	lan	192.168.10.7 192.168.10.1	29242 8080	tcp_flags_set drop
good_flag=SYN bad_flag=RST ipdatalen=20 syn=1 rst=1								
2012-02-22 14:37:46	Warning	TCP_FLAG 3300008	TCPSynRst	TCP	lan	192.168.10.7 192.168.10.1	29253 25	tcp_flags_set drop
good_flag=SYN bad_flag=RST ipdatalen=20 syn=1 rst=1								
2012-02-22 14:37:46	Warning	TCP_FLAG 3300008	TCPSynRst	TCP	lan	192.168.10.7 192.168.10.1	29252 449	tcp_flags_set drop
good_flag=SYN bad_flag=RST ipdatalen=20 syn=1 rst=1								
2012-02-22 14:37:46	Warning	TCP_FLAG 3300008	TCPSynRst	TCP	lan	192.168.10.7 192.168.10.1	29252 449	tcp_flags_set drop
good_flag=SYN bad_flag=RST ipdatalen=20 syn=1 rst=1								
2012-02-22 14:37:46	Warning	IP_PROTO 7000014	TTLOnLowMulticast	UDP	lan	192.168.10.7 239.255.255.250	49172 1900	ttl_low drop
ttl=1 ttlmin=3 ipdatalen=125 udptotlen=125								
2012-02-22 14:37:46	Warning	TCP_FLAG 3300008	TCPSynRst	TCP	lan	192.168.10.7 192.168.10.1	29251 111	tcp_flags_set drop
good_flag=SYN bad_flag=RST ipdatalen=20 syn=1 rst=1								
2012-02-22 14:37:46	Warning	TCP_FLAG 3300008	TCPSynRst	TCP	lan	192.168.10.7 192.168.10.1	29251 111	tcp_flags_set drop
good_flag=SYN bad_flag=RST ipdatalen=20 syn=1 rst=1								

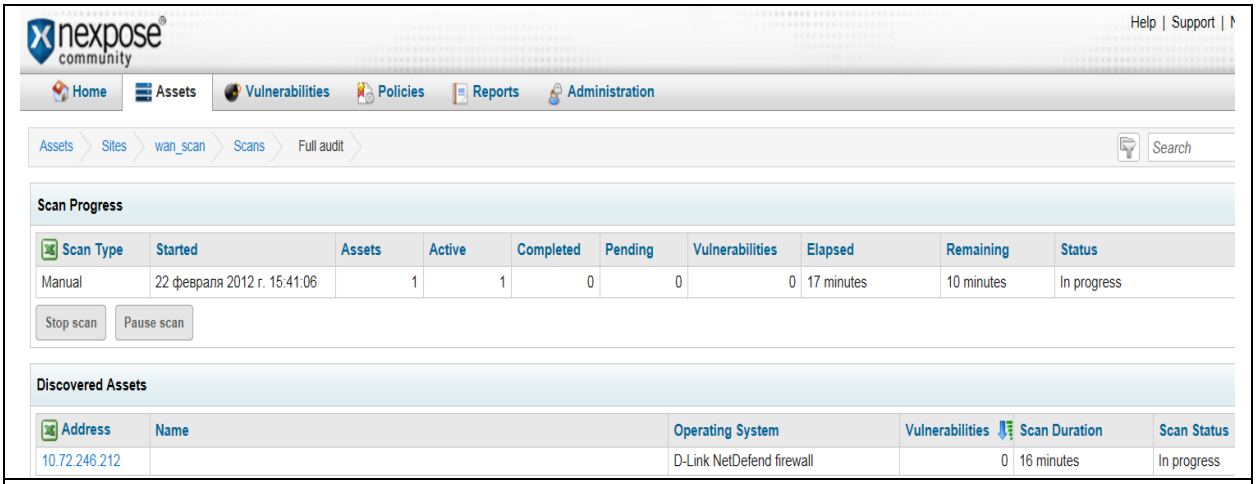
На рисунке 7.19 показаны лог-сообщения: отброшены некорректные TCP-пакеты различных типов.

Рисунок 7.19

2012-02-22 14:32:50	Warning	TCP_FLAG 3300008	TCPSynUrg	TCP	lan	192.168.10.7 192.168.10.1	29198 22	tcp_flags_set drop
good_flag=SYN bad_flag=URG ipdatalen=40 tcphdrlen=40 syn=1 psh=1 fin=1 urg=1								
2012-02-22 14:32:50	Warning	TCP_FLAG 3300008	TCPSynUrg	TCP	lan	192.168.10.7 192.168.10.1	29198 22	tcp_flags_set drop
good_flag=SYN bad_flag=URG ipdatalen=40 tcphdrlen=40 syn=1 psh=1 fin=1 urg=1								
2012-02-22 14:32:47	Warning	IP_PROTO 7000014	TTLOnLowMulticast	UDP	lan	192.168.10.7 239.255.255.250	49172 1900	ttl_low drop
ttl=1 ttlmin=3 ipdatalen=125 udptotlen=125								
2012-02-22 14:32:45	Warning	TCP_OPT 3400016	TCPNull	TCP	lan	192.168.10.7 192.168.10.1	29197 22	tcp_null_flags drop
ipdatalen=40 tcphdrlen=40								
2012-02-22 14:32:45	Warning	TCP_OPT 3400016	TCPNull	TCP	lan	192.168.10.7 192.168.10.1	29197 22	tcp_null_flags drop
ipdatalen=40 tcphdrlen=40								
2012-02-22 14:32:45	Notice	TCP_FLAG 3300004	TCPECN	TCP	lan	192.168.10.7 192.168.10.1	29196 22	tcp_flag_set strip_flag
bad_flag=ECN ipdatalen=32 tcphdrlen=32 syn=1 ece=1 cwr=1 ns=1								
2012-02-22 14:32:45	Notice	TCP_FLAG 3300004	TCPECN	TCP	lan	192.168.10.7 192.168.10.1	29196 22	tcp_flag_set strip_flag
bad_flag=ECN ipdatalen=32 tcphdrlen=32 syn=1 ece=1 cwr=1 ns=1								

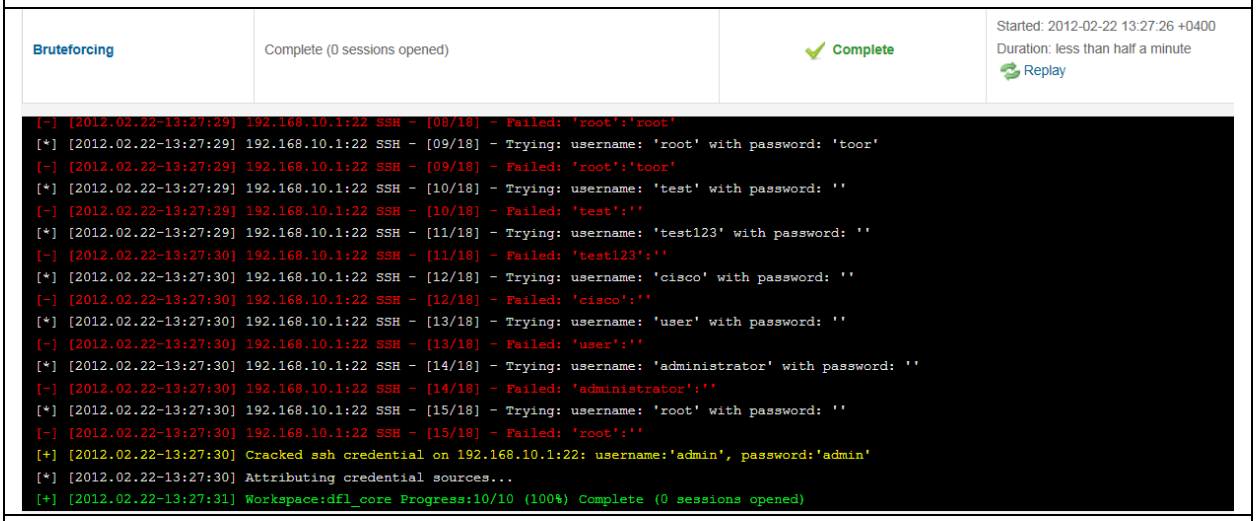
На рисунке 7.20 показан процесс сканирования межсетевого экрана сканером уязвимостей Rapid7 Nexpose, сканер верно определил тип устройства – D-Link NetDefend firewall.

Рисунок 7.20



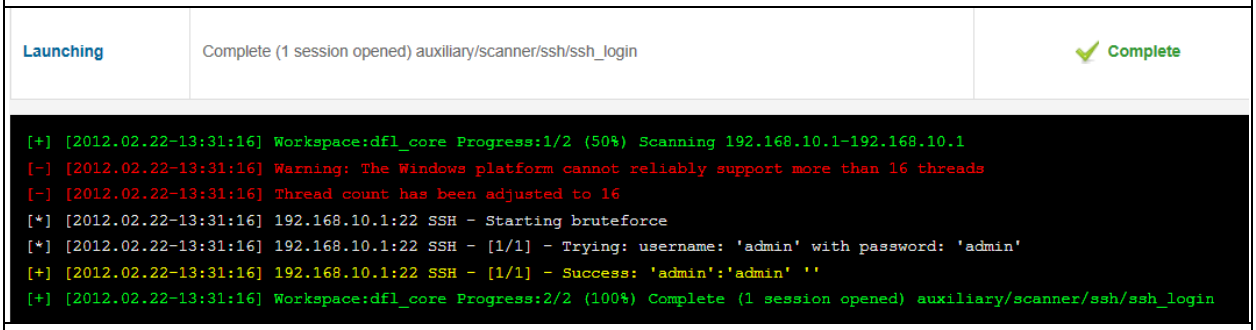
На рисунке 7.21 показан процесс успешного взлома простого логина по умолчанию для SSH-управления межсетевым экраном с использованием Rapid7 Metasploit. При практическом использовании межсетевых экранов все стандартные административные учетные записи должны быть изменены, недопустимо давать лишних разрешений, не нужных для нормального администрирования системы межсетевых экранов.

Рисунок 7.21



На рисунке 7.22 показана открытая сессия на SSH для межсетевого экрана с использованием Rapid7 Metasploit. Злоумышленник прошел аутентификацию, используя слабый логин по умолчанию (admin/admin), теперь он может настроить взломанный им межсетевой экран как пожелает.

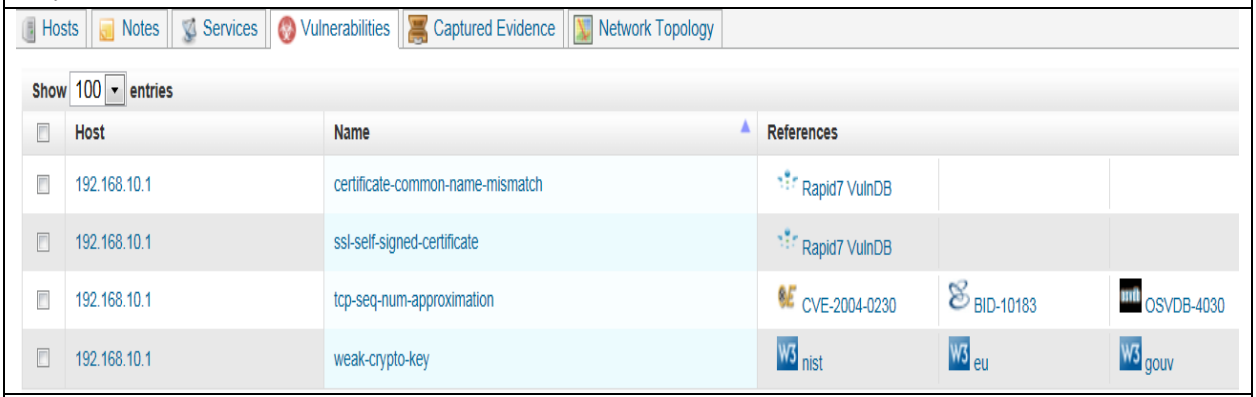
Рисунок 7.22



На рисунке 7.23 показаны найденные с использованием Rapid7 Metasploit уязвимости межсетевого экрана, которые можно использовать для дальнейших атак на устройство и защищаемую сеть. Присутствуют ссылки с описанием уязвимостей, есть возможность на некоторых ресурсах Интернета скачать исходные тексты программ, реализующих уязвимость. При практическом использовании межсетевых экранов все уязвимости,

найденные с помощью сканеров уязвимостей и других подобных программ должны быть устранены.

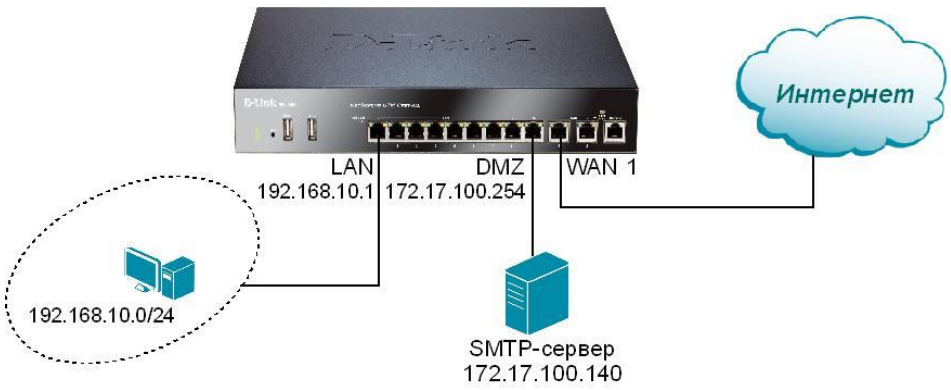
Рисунок 7.23



Настройка SMTP Event Receiver для IDP/IPS

Описание сценария	*Необходимо настроить автоматическое уведомление администратора информационной безопасности компании о событиях системы IDP/IPS. Сообщения должны приходить на почтовый ящик admin@company.com.*

Схема 85



Настройка DFL-860E

Web-интерфейс

Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:

Name	smtp_server_ip
Address	172.17.100.140

Зайдите в меню *System->Log and Event Receivers→Add→SMTP Event Receiver*. Введите во вкладке *General* следующиепараметры:

Name	smtp_idp
SMTP Server	smtp_server_ip
ServerPort	25
1:st Email Receive	admin.company.com
Sender	hostmaster
Subject	Enemy Attack!!!
Minimum Repeat Delay	600
Hold Time	120
Log Threshold	2

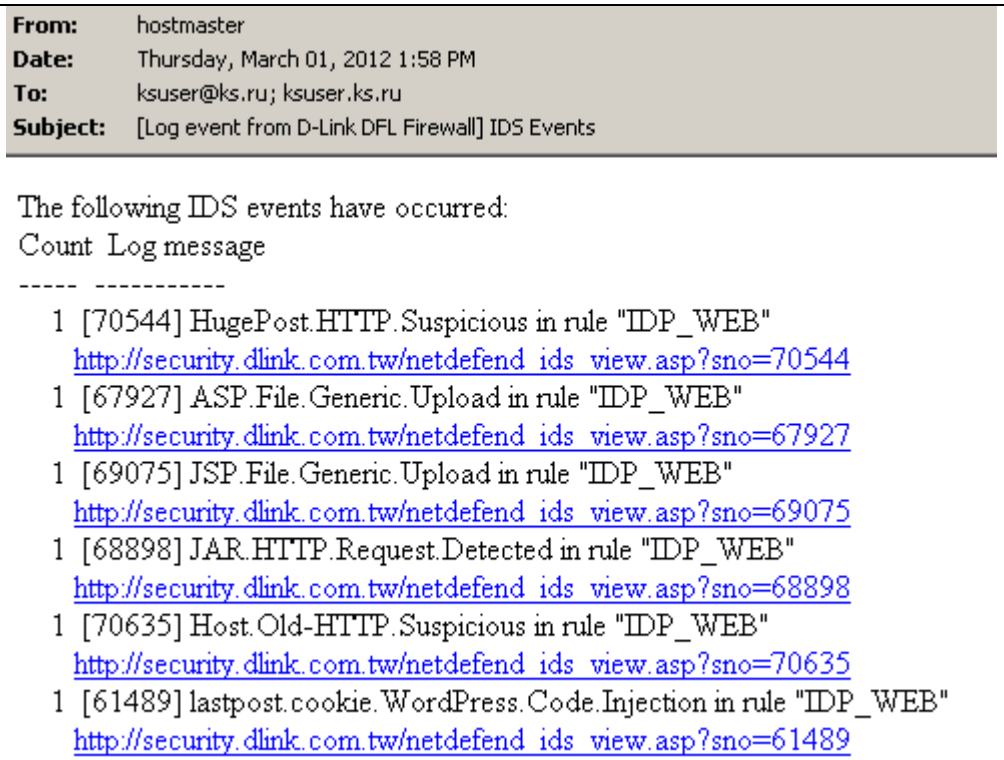
Командная строка (CLI)

gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address smtp_server_ip Address=172.17.100.140
gw-world:/labs> cc
gw-world:/> add LogReceiver LogReceiverSMTP smtp_idp IPAddress=labs/smtp_server_ip Receiver1=admin.company.com Port=25 Sender=hostmaster Subject=Enemy_Attack! MinRepeatDelay=600 HoldTime=120 LogThreshold=2
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Упражнение	Проверьте работу SMTP Event Receiver. Осуществите DoS-атаку на межсетевой экран. Проверьте наличие сообщений от SMTP Event Receiver.

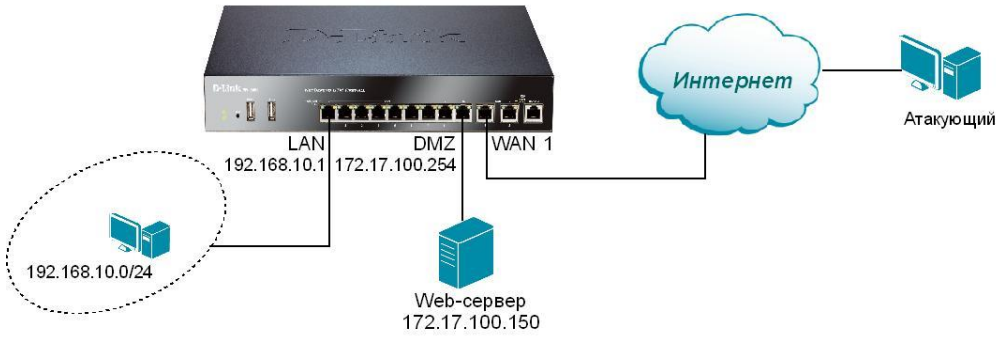
Примеры сообщений SMTP Event Receiver показан на рисунке 7.24.

Рисунок 7.24



Настройка системы IDP/IPS для защиты Web-сервера на базе службы IIS операционной системы Microsoft Windows Server

Описание сценария	*Необходимо защитить Web-сервер, расположенный в* ***dmz****-зоне межсетевого экрана, от атак из Интернета.*

Схема 86	

<u>Настройка DFL-860E</u>

<u>Web-интерфейс</u>

Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:

Name	ip-webserver
Address	172.17.100.150

Создание сервиса

Зайдите в меню *Objects→Services*, добавьте TCP/UDP Service со следующими параметрами:

Name	http-idp
Type	TCP (выберите из списка)
Source	0-65535
Destination	80
SYN flood protection (SYN Relay)	Поставьте галочку

Настроим IP Rules. Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Введите следующие параметры:

Name	allow-icmp
Action	Allow
Service	all_icmp
Source Interface	wan1
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip

Зайдите в меню *Rules→IP Rules→Add→IP Rule*. Введите следующие параметры:

Name	SAT-web-srv
Action	SAT
Service	http-idp
Source Interface	wan1
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip

Введите параметры во вкладке *SAT*:

Translate the	Destination IP Address
To New IP Address	ip-webserver

Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Введите следующие параметры:	
Name	allow-web-srv
Action	Allow
Service	http-idp
Source Interface	wan1
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip
Создадим IDP Rule. Зайдите в меню *IDP/IPS→IDP Rules→Add→IDP Rule*. Задайте параметры:	
Name	IPS_WEB
Service	http-idp
Protect against insertion/evasion attacks	Поставьте галочку
Invalid UTF8	DropLog
Invalid hex encoding	DropLog
Double encoding	DropLog
Source Interface	wan1
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip
Примечание: Созданное правило будет мониторить только трафик сервиса* http-idp*, любой другой вид трафика не будет пропускаться данным правилом. Для других сервисов необходимо создать соответствующие правила, если есть необходимость в их мониторинге.	
Создадим IDP Rule Action. Зайдите в меню *IDP/IPS→IDP Rules→IPS_WEB→вкладка Rule Actions→Add→IDP Rule Action.* Задайте параметры:	
Action	Protect
Signature (s)	Введите IPS_MALWARE*, IPS_HTTP_MICROSOFTIIS, IPS_WORM_GENERAL, IPS_SCANNER*, IPS_HTTP_CGI, IPS_HTTP_OVERFLOWS, IPS_HTTP_ASP.NET, IPS_HTTP_GENERAL, IPS_COMPONENT_SHELLCODE, IPS_COMPONENT_INFECTION, IPS_COMPONENT_ENCODER, IPS_WEB*, IPS_TCP*, IPS_TROJAN*
Во вкладке *Log Settings* задайте параметры:	
Enable Logging	Поставьте галочку
Log with severity	Выберите из списка Debug
Создадим IDP Rule Action. Зайдите в меню *IDP/IPS→IDP Rules→IPS_WEB→вкладка Rule Actions→Add→IDP Rule Action.* Задайте параметры:	
Action	Audit

Signature (s)	Введите IDS*
Во вкладке *LogSettings* задайте параметры:	
Enable Logging	Поставьте галочку
Log with severity	Выберите из списка Debug
Зайдите в меню *Configuration* и выберите *Save and Activate*.	

Примечание: 1. Для того чтобы избежать ложных срабатываний правил, необходимо внимательнее подходить к обозначению действия правила сигнатур как Protect, Audit и Ignored. Описание сигнатур можно найти на сайте центра сетевой защиты D-Link http://security.dlink.com.tw.
2. Можно указать группу сигнатур IPS_HTTP*, но тогда трафик будет оцениваться на наличие атак и сканирование элементов, явно отсутствующих в данной схеме – например, IPS_HTTP_CISCO, что приведет к дополнительной нежелательной нагрузке на процессор межсетевого экрана.
3. Если совместно с Web-сервером работает СУБД или другая дополнительная служба, то желательно добавить следующие группы сигнатур для анализа трафика на вторжение и сканирование: IPS_HTTP_ORACLE, IPS_HTTP_TOMCAT, IPS_HTTP_WEBDAV, IPS_HTTP_BADBLUE, IPS_WEB_XSS, IPS_WEB_SQL-INJECTION, IPS_WEB_SCANNER и др.
4. В действии правила IDP используется группа сигнатур IPS_WEB*, содержащая очень большое количество сигнатур (более 20000). Такая модель безопасности неэффективна при практическом применении схемы безопасности в реальной сети, т.к. также приведет к серьезной нагрузке на вычислительную систему межсетевого экрана. Рекомендуется использовать отдельные группы сигнатур в зависимости от используемых на Web-сервере дополнительных служб и компонентов: IPS_WEB_JAVASCRIPT, IPS_WEB_PHP-XML-RPC, IPS_WEB_JSP-FILE-INCLUSION, IPS_WEB_ACTIVEX и т.д.

Командная строка (CLI)

```
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address ip-webserver Address=172.17.100.150
gw-world:/labs> cc
gw-world:/> add Service ServiceTCPUDP http-idp DestinationPorts=80 SourcePorts=0-65535
Type=TCP SYNRelay=Yes
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=core
DestinationNetwork=InterfaceAddresses/wan1_ipService=all_icmp SourceInterface=wan1
SourceNetwork=all-nets Name=allow-icmp
gw-world:/1(labs)> add IPRule Action=SAT Service=http-idp SourceInterface=wan1
SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip
SATTranslateToIP=labs/ip-webserver SATTranslate DestinationIP Name=SAT-web-srv
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=core
DestinationNetwork=InterfaceAddresses/wan1_ip Service=http-idp SourceInterface=wan1
SourceNetwork=all-nets Name=allow-web-srv
gw-world:/1(labs)> cc
gw-world:/> add IDPRule DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip
SourceInterface=wan1 SourceNetwork=all-nets Service=http-idp Index=1 InsertionEvasion=Yes
URIIllegalUTF8=DropLog URIIllegalHex=DropLog URIDoubleEncode=DropLogName=IPS_WEB
gw-world:/> cc IDPRule 1(IPS_WEB)
gw-world:/1(IPS_WEB)> add IDPRuleAction Action=Protect Index=1
Signatures=IPS_MALWARE*,IPS_HTTP_MICROSOFTIIS,IPS_WORM_GENERAL,IPS_SCANNER
*,IPS_HTTP_CGI,IPS_HTTP_OVERFLOWS,IPS_HTTP_ASP.NET,IPS_HTTP_GENERAL,IPS_CO
MPONENT_SHELLCODE,IPS_COMPONENT_INFECTION,IPS_COMPONENT_ENCODER,IPS_W
EB*,IPS_TCP*,IPS_TROJAN*LogSeverity=Debug LogEnabled=Yes
gw-world:/1(IPS_WEB)> add IDPRuleAction Action=AuditIndex=2 Signatures=IDS*
```

LogSeverity=Debug LogEnabled=Yes
gw-world:/1(IPS_WEB)> cc
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Упражнение	Осуществите тестовую атаку на Web-сервер из сети wan1net. Для проверки срабатывания IDP-правил зайдите в меню *Status→IDP/IPS*. На указанную при настройке SMTP Event Receiver почту будут приходить уведомления о срабатывании IDP-правил.

Примеры сообщений при аудите к атакам на Web-сервер, защищенный межсетевым экраном. Для осуществления атак используется сканер уязвимостей Rapid7 Nexpose. На рисунке 7.25 показаны сообщения IDP/IPS об использовании некорректного URL, шелл-кодов и ряда известных уязвимостей HTTP.

Рисунок 7.25

Date	Severity	Category/ID	Rule	Proto	Src/DstIf	Src/DstIP	Src/DstPort	Event/Action
2012-02-25 20:18:17	Warning	IDP 1300010	IDP_WEB			192.168.110.212 192.168.110.254	1897 80	invalid_url_format ignore
idrule="IDP_WEB" url="/OvCgi/jovgraph.exe?sel=a&act=U&arg=%981%e1C%d8%d3%3d%bf%ed%92%f0%99%14-%dd %c1%11%ef%c3d%d6%ee%ac%9c%91%3f%cd%a8%06o%c3g%7eq%13%eb%d3%08%e9%a9%21%7b%5e%ea %2b%06n%28%b7%23%c8%d9%87%3asj%bb%bf%d4%2bL%d8%90q%04%21%88%dc%ab%fa%ac%b6%c5%9fgt%18 %fcf%e6H%94%d6"						
2012-02-25 20:18:17	Warning	IDP 1300010	IDP_WEB			192.168.110.212 192.168.110.254	1897 80	invalid_url_format ignore
idrule="IDP_WEB" url="/OvCgi/jovgraph.exe?sel=a&act=U&arg=%981%e1C%d8%d3%3d%bf%ed%92%f0%99%14-%dd %c1%11%ef%c3d%d6%ee%ac%9c%91%3f%cd%a8%06o%c3g%7eq%13%eb%d3%08%e9%a9%21%7b%5e%ea %2b%06n%28%b7%23%c8%d9%87%3asj%bb%bf%d4%2bL%d8%90q%04%21%88%dc%ab%fa%ac%b6%c5%9fgt%18 %fcf%e6H%94%d6"						
2012-02-25 20:18:10	Notice	IDP 1300007	IDP_WEB	TCP		192.168.110.212 192.168.110.254	1892 80	intrusion_detected
description="HugePost.HTTP.Suspicious" signatureid=70544 idrule="IDP_WEB" Advisory link								
2012-02-25 20:17:52	Notice	IDP 1300005	IDP_WEB	TCP		192.168.110.212 192.168.110.254	1880 80	scan_detected
description="Host.Old-HTTP.Suspicious" signatureid=70635 idrule="IDP_WEB" Advisory link								
2012-02-25 20:17:45	Notice	IDP 1300005	IDP_WEB	TCP		192.168.110.212 192.168.110.254	1876 80	scan_detected
description="FnstEnv.x86.GetPC.Shellcode" signatureid=58375 idrule="IDP_WEB" Advisory link								
2012-02-25 20:17:41	Notice	IDP 1300005	IDP_WEB	TCP		192.168.110.212 192.168.110.254	1872 80	scan_detected
description="FnstEnv.x86.GetPC.Shellcode" signatureid=58375 idrule="IDP_WEB" Advisory link								
2012-02-25 20:17:41	Notice	IDP 1300005	IDP_WEB	TCP		192.168.110.212 192.168.110.254	1872 80	scan_detected
description="Content-length.GET-Request.HTTP.Suspicious" signatureid=69025 idrule="IDP_WEB" Advisory link								

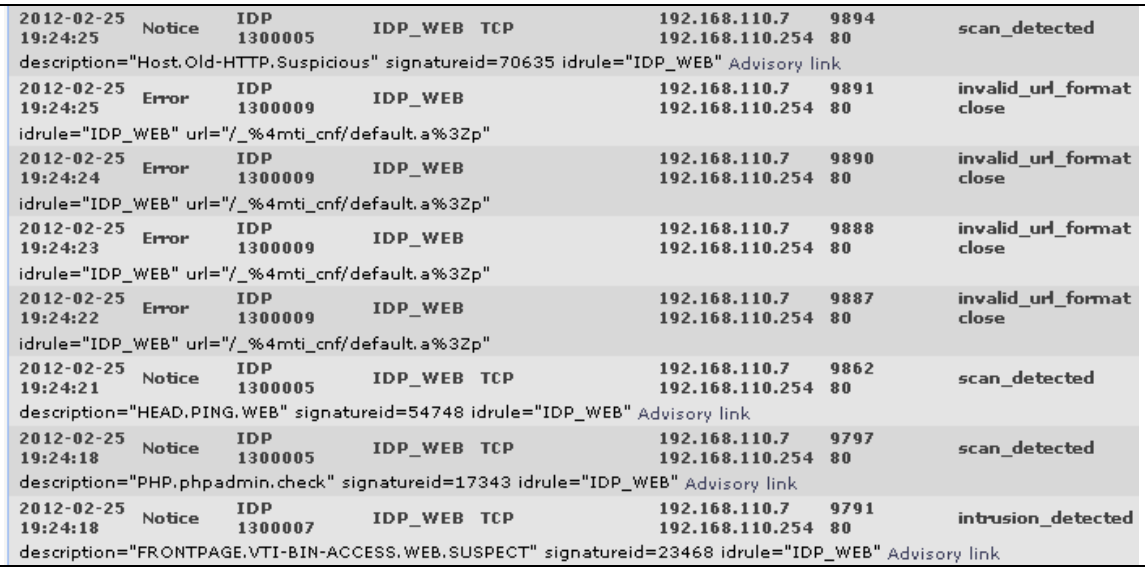
На рисунке 7.26 показаны лог-сообщения об использовании некорректного порядкового номера TCP-сегментов.

Рисунок 7.26

:012-02-25 :0:09:00	Warning	TCP_FLAG 3300019	TCPSequenceNumbers	TCP	wan1 dmz	192.168.110.212 172.17.100.150	1408 80	tcp_seqno_too_high drop
eqno=3686793801 accstart=3686793264 accend=3686793266 origsent=1662 termsent=40 ipdatalen=63 ack=1 psh=1								
:012-02-25 :0:09:00	Warning	TCP_FLAG 3300019	TCPSequenceNumbers	TCP	wan1 dmz	192.168.110.212 172.17.100.150	1408 80	tcp_seqno_too_high drop
eqno=3686793801 accstart=3686793264 accend=3686793266 origsent=1579 termsent=40 ipdatalen=63 ack=1 psh=1								

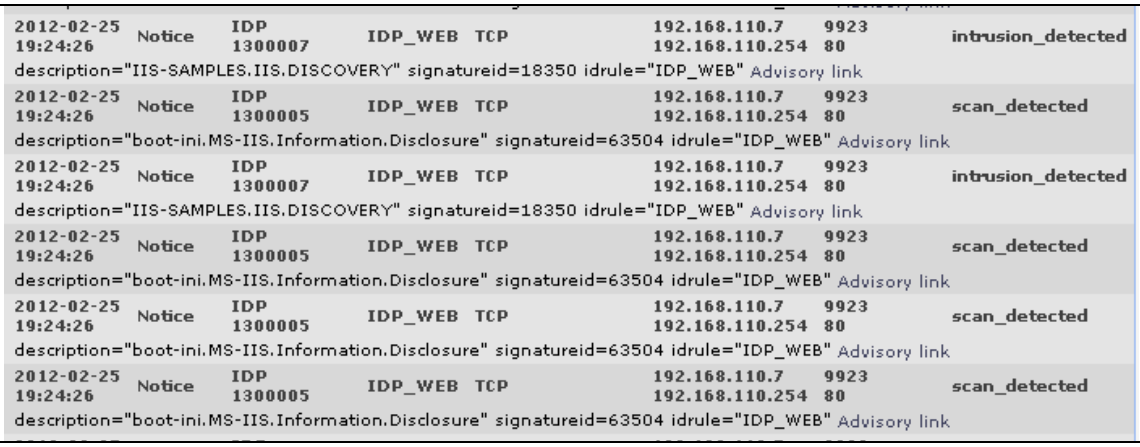
На рисунке 7.27 показаны сообщения IDP/IPS об использовании некорректного URL, уязвимостей PHP, Frontpage.

Рисунок 7.27



На рисунке 7.28 показаны сообщения IDP/IPS об использовании различных уязвимостей MS IIS.

Рисунок 7.28

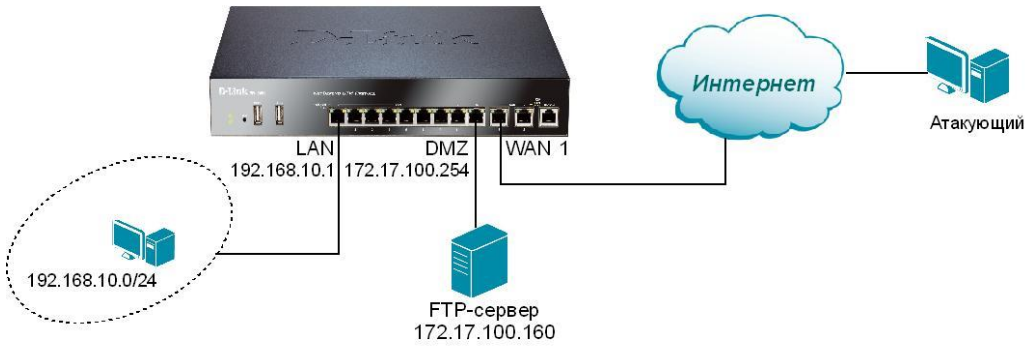


Защита от сетевых атак при помощи «чёрных» списков хостов и сетей (blacklist) в IDP

Описание метода	*Межсетевой экран поддерживает «черный» список (Blacklist) хостов или сетей, IP-адреса которых могут быть использованы для защиты от трафика с определенных ресурсов Интернета.*

Настройка системы IDP/IPS для защиты FTP-сервера.

Описание сценария	*Необходимо защитить FTP-сервер, расположенный в* ***dmz****-зоне межсетевого экрана, от атак из Интернета. При выявлении атаки необходимо использовать автоматическое блокирование хостов с помощью IDP/IPS.*

Схема 87	

Настройка DFL-860E

Web-интерфейс

Зайдите в меню *Objects→Address Book→IP4 Address.* Введите следующие параметры:	
Name	ip-ftp
Address	172.17.100.160
Добавим новый FTP ALG. Зайдите в меню *Objects→ALG→Add→FTP ALG.* Во вкладке *General* введите следующие параметры:	
Name	ftp-alg
Allow client to use active mode (unsafe for client)	Поставьте галочку
Во вкладке *Anti-Virus* введите следующие параметры:	
Mode	Protect
Создание сервиса	
Зайдите в меню *Objects→Services*, добавьте TCP/UDP Service со следующими параметрами:	
Name	ftp-idp
Type	TCP (выберите из списка)
Source	0-65535
Destination	21
ALG	ftp-alg
Настроим IP Rules. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Введите следующие параметры:	
Name	allow-icmp
Action	Allow
Service	all_icmp
Source Interface	wan1
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Введите следующие параметры:	
Name	SAT-ftp-srv
Action	SAT
Service	ftp-idp
Source Interface	wan1
Source Network	all-nets

Destination Interface	core
Destination Network	wan1_ip
Введите параметры во вкладке *SAT*:	
Translate the	Destination IP Address
To New IP Address	ip-ftp
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Введите следующие параметры:	
Name	allow-ftp-srv
Action	Allow
Service	ftp-idp
Source Interface	wan1
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip
Создадим IDP Rule. Зайдите в папу *IDP/IPS→IDP Rules→Add→IDP Rule*. Задайте параметры:	
Name	IPS_FTP
Service	ftp-idp
Protect against insertion/evasion attacks	Поставьте галочку
Source Interface	wan1
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip
Примечание: Созданое правило будет мониторить только трафик сервиса ftp-idp, любой другой вид трафика не будет пропускаться данным правилом. Для других сервисов необходимо создать соответствующие правила, если есть необходимость в их мониторинге.	
Создадим IDP Rule Action. Зайдите в меню *IDP/IPS→IDP Rules→IPS_FTP→вкладка Rule Actions→Add→IDP Rule Action.* Задайтепараметры:	
Action	Protect
Signature (s)	Введите IPS_MALWARE*, IPS_FTP*, IPS_WORM_GENERAL, IPS_SCANNER*, IPS_COMPONENT_SHELLCODE, IPS_COMPONENT_INFECTION, IPS_COMPONENT_ENCODER, IPS_TCP*, IPS_TROJAN*
Dynamic Black Listing	Поставьте галочку напротив Enable
Block duration	3600 seconds
Block service only	Уберите галочку
Ignore established	Поставьте галочку
Во вкладке *Log Settings* задайте параметры:	
Enable Logging	Поставьте галочку
Log with severity	Выберите из списка Debug
Создадим IDP Rule Action. Зайдите в меню *IDP/IPS→IDP Rules→IPS_FTP→вкладка Rule*	

Actions→Add→IDP Rule Action. Задайте параметры:	
Action	Audit
Signature (s)	Введите IDS*
Во вкладке *Log Settings* задайте параметры:	
Enable Logging	Поставьте галочку
Log with severity	Выберите из списка Debug
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Примечание: 1. Для того чтобы избежать ложных срабатываний правил, необходимо внимательнее подходить к обозначению действия правила сигнатур как Protect, Audit и Ignored. Описание сигнатур можно найти на сайте центра сетевой защиты D-Link http://security.dlink.com.tw. ***2. Если хост или сеть, находящаяся в «черном» списке, удалены из него по истечении времени блокирования, но снова попадают в него, то это время будет задано заново.*** ***3. По умолчанию все службы блокируются для хоста, попавшего в blacklist.*** ***4. Если установлена опция Ignore established, то существующие соединения того же источника, который попадает в blacklist, не будут отброшены.*** ***5. Перезагрузка межсетевого экрана не влияет на blacklist, их содержимое не пропадет***.	
Командная строка (CLI)	
gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address ip-ftp Address=172.17.100.160 gw-world:/labs> cc gw-world:/>add ALG ALG_FTP ftp-alg AllowClientActive=Yes Antivirus=Protect gw-world:/> add Service ServiceTCPUDP ftp-idp DestinationPorts=21 SourcePorts=0-65535 Type=TCP ALG=ftp-alg gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ipService=all_icmp SourceInterface=wan1 SourceNetwork=all-nets Name=allow-icmp gw-world:/1(labs)> add IPRule Action=SAT Service=ftp-idp SourceInterface=wan1 SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip SATTranslateToIP=labs/ip-ftp SATTranslate DestinationIP Name=SAT-ftp-srv gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip Service=ftp-idp SourceInterface=wan1 SourceNetwork=all-nets Name=allow-ftp-srv gw-world:/1(labs)> cc gw-world:/> add IDPRule DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip SourceInterface=wan1 SourceNetwork=all-nets Service=ftp-idp Index=1 InsertionEvasion=Yes URIIllegalUTF8=DropLog URIIllegalHex=DropLog URIDoubleEncode=DropLogName=IPS_FTP gw-world:/> cc IDPRule 1(IPS_FTP) gw-world:/1(IPS_FTP)> add IDPRuleAction Action=Protect Index=1 Signatures=IPS_MALWARE*,IPS_FTP*,IPS_WORM_GENERAL,IPS_SCANNER*,IPS_COMPONENT_SHELLCODE,IPS_COMPONENT_INFECTION,IPS_COMPONENT_ENCODER,IPS_TCP*,IPS_TROJAN*BlackList=Yes BlackListTimeToBlock=3600 BlackListIgnoreEstablished=Yes BlackListBlockOnlyService=NoLogSeverity=Debug LogEnabled=Yes gw-world:/1(IPS_FTP)> add IDPRuleAction Action=AuditIndex=2 Signatures=IDS* LogSeverity=Debug LogEnabled=Yes gw-world:/1(IPS_FTP)> cc gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Упражнение	Осуществите тестовую атаку на FTP-сервер из сети wan1net. Для проверки срабатывания IDP-правил зайдите в меню *Status→IDP/IPS*. На указанную при настройке SMTP Event

	Receiver почту будут приходить уведомления о срабатывании IDP-правил. Проверьте блокирование атакующих IP-адресов, зайдите в меню *Status→Blacklist*.

Примеры сообщений при аудите к атакам на FTP-сервер, защищенный межсетевым экраном. Для осуществления атак используется Rapid7 Metasploit. На рисунке 7.29 показаны сообщения IDP/IPS об использовании нескольких шелл-кодов и ряда известных уязвимостей FTP-серверов.

Рисунок 7.29

2012-02-29 20:55:12	Notice	IDP 1300007	IDP_FTP	TCP	192.168.110.212 192.168.110.254	1595 21	intrusion_detected
description="specifiers.BolinTech.DreamFTPServer.Format.String" signatureid=58036 idrule="IDP_FTP" Advisory link							
2012-02-29 20:55:12	Notice	IDP 1300007	IDP_FTP	TCP	192.168.110.212 192.168.110.254	1595 21	intrusion_detected
description="FSTENV.x86.TCP.Generic-Shellcode" signatureid=63052 idrule="IDP_FTP" Advisory link							
2012-02-29 20:55:09	Notice	IDP 1300007	IDP_FTP	TCP	192.168.110.212 192.168.110.254	1592 21	intrusion_detected
description="specifiers.BolinTech.DreamFTPServer.Format.String" signatureid=58036 idrule="IDP_FTP" Advisory link							
2012-02-29 20:55:09	Notice	IDP 1300007	IDP_FTP	TCP	192.168.110.212 192.168.110.254	1592 21	intrusion_detected
description="FSTENV.x86.TCP.Generic-Shellcode" signatureid=63052 idrule="IDP_FTP" Advisory link							
2012-02-29 20:55:06	Notice	IDP 1300007	IDP_FTP	TCP	192.168.110.212 192.168.110.254	1590 21	intrusion_detected
description="FSTENV.x86.TCP.Generic-Shellcode" signatureid=63052 idrule="IDP_FTP" Advisory link							
2012-02-29 20:54:25	Notice	IDP 1300007	IDP_FTP	TCP	192.168.110.212 192.168.110.254	1569 21	intrusion_detected
description="FSTENV.x86.TCP.Generic-Shellcode" signatureid=63052 idrule="IDP_FTP" Advisory link							
2012-02-29 20:54:25	Notice	IDP 1300007	IDP_FTP	TCP	192.168.110.212 192.168.110.254	1569 21	intrusion_detected
description="specifiers.BolinTech.DreamFTPServer.Format.String" signatureid=58036 idrule="IDP_FTP" Advisory link							
2012-02-29 20:54:21	Notice	IDP 1300007	IDP_FTP	TCP	192.168.110.212 192.168.110.254	1565 21	intrusion_detected
description="X86.popECX-call.Shellcode.Sequence" signatureid=17187 idrule="IDP_FTP" Advisory link							
2012-02-29 20:54:21	Notice	IDP 1300007	IDP_FTP	TCP	192.168.110.212 192.168.110.254	1565 21	intrusion_detected
description="specifiers.BolinTech.DreamFTPServer.Format.String" signatureid=58036 idrule="IDP_FTP" Advisory link							

На рисунке 7.30 показаны сообщения IDP/IPS об использовании нескольких шелл-кодов и ряда известных уязвимостей FTP-серверов при атаке с разных IP-адресов.

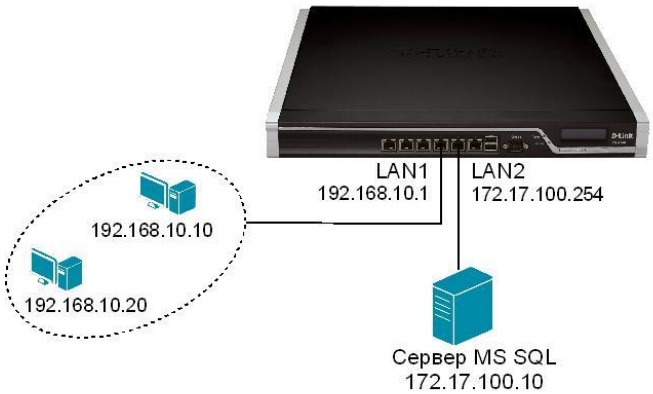
Рисунок 7.30

2012-02-29 21:01:45	Notice	IDP 1300007	IDP_FTP	TCP	192.168.110.7 192.168.110.254	7465 21	intrusion_detected
description="FTP.SERVU-DIR-TRANS.SUSPECT" signatureid=22599 idrule="IDP_FTP" Advisory link							
2012-02-29 20:55:12	Notice	IDP 1300007	IDP_FTP	TCP	192.168.110.212 192.168.110.254	1595 21	intrusion_detected
description="specifiers.BolinTech.DreamFTPServer.Format.String" signatureid=58036 idrule="IDP_FTP" Advisory link							
2012-02-29 20:55:12	Notice	IDP 1300007	IDP_FTP	TCP	192.168.110.212 192.168.110.254	1595 21	intrusion_detected
description="FSTENV.x86.TCP.Generic-Shellcode" signatureid=63052 idrule="IDP_FTP" Advisory link							
2012-02-29 20:55:09	Notice	IDP 1300007	IDP_FTP	TCP	192.168.110.212 192.168.110.254	1592 21	intrusion_detected
description="specifiers.BolinTech.DreamFTPServer.Format.String" signatureid=58036 idrule="IDP_FTP" Advisory link							
2012-02-29 20:55:09	Notice	IDP 1300007	IDP_FTP	TCP	192.168.110.212 192.168.110.254	1592 21	intrusion_detected
description="FSTENV.x86.TCP.Generic-Shellcode" signatureid=63052 idrule="IDP_FTP" Advisory link							
2012-02-29 20:55:06	Notice	IDP 1300007	IDP_FTP	TCP	192.168.110.212 192.168.110.254	1590 21	intrusion_detected
description="FSTENV.x86.TCP.Generic-Shellcode" signatureid=63052 idrule="IDP_FTP" Advisory link							
2012-02-29 20:54:25	Notice	IDP 1300007	IDP_FTP	TCP	192.168.110.212 192.168.110.254	1569 21	intrusion_detected
description="FSTENV.x86.TCP.Generic-Shellcode" signatureid=63052 idrule="IDP_FTP" Advisory link							
2012-02-29 20:54:25	Notice	IDP 1300007	IDP_FTP	TCP	192.168.110.212 192.168.110.254	1569 21	intrusion_detected
description="specifiers.BolinTech.DreamFTPServer.Format.String" signatureid=58036 idrule="IDP_FTP" Advisory link							
2012-02-29 20:54:21	Notice	IDP 1300007	IDP_FTP	TCP	192.168.110.212 192.168.110.254	1565 21	intrusion_detected
description="X86.popECX-call.Shellcode.Sequence" signatureid=17187 idrule="IDP_FTP" Advisory link							
2012-02-29 20:54:15	Notice	IDP 1300007	IDP_FTP	TCP	192.168.110.212 192.168.110.254	1563 21	intrusion_detected
description="USER.FTP.ANOMALY" signatureid=17603 idrule="IDP_FTP" Advisory link							
2012-02-29 20:54:15	Notice	IDP 1300007	IDP_FTP	TCP	192.168.110.212 192.168.110.254	1563 21	intrusion_detected
description="USER.WebSTAR.FTP.Buffer.Overflow" signatureid=57609 idrule="IDP_FTP" Advisory link							

Защита почтового сервера с помощью IDP/IPS	
Описание сценария	*Необходимо защитить почтовый сервер с помощью механизма IDP/IPS.*
Схема 88	
Настройка DFL-860E	
Web-интерфейс	
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	ip-mail
Address	172.17.100.170
Добавим новый SMTP ALG. Зайдите в меню *Objects→ALG→Add→SMTP ALG.* Во вкладке *General* введите следующие параметры:	
Name	smtp-alg
Fail Mode	Deny
Во вкладке *File Integrity* введите следующие параметры:	
Verify MIME-type against file content.	Поставьте галочку
Block selected file types	cmd, com, doc, exe, pif, ppt, scr, xls
Во вкладке *Anti-Virus* введите следующие параметры:	
Mode	Protect
Во вкладке *Anti-Spam* введите следующие параметры:	
Check emails for mismatching SMTP command "From" address and email header "From" address.	Поставьте галочку и выберите *...and block them.*
Создание сервиса	
Зайдите в меню *Objects→Services*, добавьте TCP/UDP Service со следующими параметрами:	
Name	smtp-idp
Type	TCP (выберите из списка)
Source	0-65535
Destination	25
ALG	smtp-alg
Настроим IP Rules. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Введите следующие параметры:	
Name	allow-icmp
Action	Allow

Service	all_icmp
Source Interface	wan1
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Введите следующие параметры:	
Name	SAT-smtp-srv
Action	SAT
Service	smtp-idp
Source Interface	wan1
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip
Введите параметры во вкладке *SAT*:	
Translate the	Destination IP Address
To New IP Address	ip-mail
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Введите следующие параметры:	
Name	allow-smtp-srv
Action	Allow
Service	smtp-idp
Source Interface	wan1
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip
Создадим IDP Rule. Зайдите в меню *IDP/IPS→IDP Rules→Add→IDP Rule*. Задайте параметры:	
Name	IPS_SMTP
Service	smtp-idp
Protect against insertion/evasion attacks	Поставьте галочку
Source Interface	wan1
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip
Примечание: Созданное правило будет мониторить только трафик сервиса smtp-idp, любой другой вид трафика не будет пропускаться данным правилом. Для других сервисов необходимо создать соответствующие правила, если есть необходимость в их мониторинге.	
Создадим IDP Rule Action. Зайдите в меню *IDP/IPS→IDP Rules→IPS_SMTP→вкладка Rule Actions→Add→IDP Rule Action.* Задайте параметры:	
Action	Protect
Signature (s)	Введите IPS_MALWARE*, IPS_SMTP*, IPS_WORM_GENERAL, IPS_SCANNER*, IPS_COMPONENT_SHELLCODE,

	IPS_COMPONENT_INFECTION, IPS_COMPONENT_ENCODER, IPS_TCP*, IPS_TROJAN*
Во вкладке *Log Settings* задайте параметры:	
Enable Logging	Поставьте галочку
Log with severity	Выберите из списка Debug
Создадим IDP Rule Action. Зайдите в меню *IDP/IPS→IDP Rules→IPS_SMTP→вкладка Rule Actions→Add→IDP Rule Action.* Задайте параметры:	
Action	Audit
Signature (s)	ВведитеIDS*
Во вкладке *LogSettings* задайте параметры:	
Enable Logging	Поставьте галочку
Log with severity	Выберите из списка Debug
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Примечание: Для того чтобы избежать ложных срабатываний правил, необходимо внимательнее подходить к обозначению действия правила сигнатур как Protect, Audit и Ignored. Описание сигнатур можно найти на сайте центра сетевой защиты D-Link http://security.dlink.com.tw.	
Командная строка (CLI)	
gw-world:/> cc Address AddressFolder labs gw-world:/labs> add IP4Address ip-mail Address=172.17.100.170 gw-world:/labs> cc gw-world:/>add ALG ALG_SMTP smtp-alg FailModeBehavior=Deny VerifyContentMimetype=Yes FileListType=Block File=cmd,com,doc,exe,pif,ppt,scr,xls Antivirus=Protect VerifySenderEmail=Yes VerifySenderEmailDomainOnly=Yes VerifySenderEmailAction=Deny gw-world:/> add Service ServiceTCPUDP smtp-idp DestinationPorts=25 SourcePorts=0-65535 Type=TCP ALG=smtp-alg gw-world:/> cc IPRuleFolder labs gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ipService=all_icmp SourceInterface=wan1 SourceNetwork=all-nets Name=allow-icmp gw-world:/1(labs)> add IPRule Action=SAT Service=smtp-idp SourceInterface=wan1 SourceNetwork=all-nets DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip SATTranslateToIP=labs/ip-mail SATTranslate DestinationIP Name=SAT-smtp-srv gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip Service=smtp-idp SourceInterface=wan1 SourceNetwork=all-nets Name=allow-smtp-srv gw-world:/1(labs)> cc gw-world:/> add IDPRule DestinationInterface=core DestinationNetwork=InterfaceAddresses/wan1_ip SourceInterface=wan1 SourceNetwork=all-nets Service=smtp-idp Index=1 InsertionEvasion=Yes Name=IPS_SMTP gw-world:/> cc IDPRule 1(IPS_SMTP) gw-world:/1(IPS_SMTP)> add IDPRuleAction Action=Protect Index=1 Signatures=IPS_MALWARE*,IPS_SMTP*,IPS_WORM_GENERAL,IPS_SCANNER*,IPS_COMPONENT_SHELLCODE,IPS_COMPONENT_INFECTION,IPS_COMPONENT_ENCODER,IPS_TCP*,IPS_TROJAN* LogSeverity=Debug LogEnabled=Yes gw-world:/1(IPS_SMTP)> add IDPRuleAction Action=AuditIndex=2 Signatures=IDS* LogSeverity=Debug LogEnabled=Yes gw-world:/1(IPS_SMTP)> cc	

gw-world:/> activate *(подождать 3-5 секунд)* gw-world:/>commit	
Упражнение	Осуществите тестовую атаку на почтовый сервер из сети wan1net. Для проверки срабатывания IDP-правил зайдите в меню *Status→IDP/IPS*. На указанную при настройке SMTP Event Receiver почту будут приходить уведомления о срабатывании IDP-правил.
«Белый» список в IDP/IPS	
Описание метода	*Доверенные важные IP-адреса обязательно должны быть добавлены в «белый» список.*
Зайдите в меню *System→Whitelist→Add→Whitelist Host*. Добавьте IP-адрес *lan_ip* в «белый» список – переместите *lan_ip* из списка *Available* в список *Selected*, выберите соответствующий сервис.	
Примечание: Даже если хост внесён в «белый» список, трафик от него может быть отброшен пороговыми правилами (Threshold Rules).	
Защита сервера MS SQL с помощью IDP/IPS	
Описание сценария	*Необходимо защитить сервер MS SQL, расположенный в* ***lan2****, с помощью механизма IDP/IPS. IP-адреса 192.168.10.10 и 192.168.10.20 необходимо оградить от возможных ложных IDP-срабатываний с помощью White list.* *Данная работа выполняется на межсетевом экране DFL-1660.*
Схема 89	
Настройка DFL-1660	
Web-интерфейс	
Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	ip_whitelist1
Address	192.168.10.10
Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	ip_whitelist2
Address	192.168.10.20
Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	
Name	ip-mssql
Address	172.17.100.10
Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:	

Name	lan1net
Address	192.168.10.0/24
Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:	
Name	lan2net
Address	172.17.100.0/24
Создание сервисов	
Зайдите в меню *Objects→Services*, добавьте TCP/UDP Service со следующими параметрами:	
Name	ms-sql-s
Type	TCP (выберите из списка)
Source	1025-5000,49132-65535
Destination	1433
SYN flood protection (SYN Relay)	Поставьте галочку
Зайдите в меню *Objects→Services*, добавьте TCP/UDP Service со следующими параметрами:	
Name	ms-sql-m
Type	TCP/UDP (выберите из списка)
Source	0-65535
Destination	1434
SYN flood protection (SYN Relay)	Поставьте галочку
Создадим Service Group из всех сервисов, необходимых для MS SQL. Зайдите в меню *Objects→Services→Add→Service Group.* Во вкладке *General*, введите следующие параметры:	
Name	ms-sql-all
Selected	Переместите ms-sql-s, ms-sql-m из списка Available.
Зайдите в меню *System→Whitelist→Add→Whitelist Host.* Добавьте IP-адрес *ip_whitelist1* в «белый» список – переместите *ip_whitelist1* из списка *Available* в список *Selected*, выберите службу:	
Service	ms-sql-all
Зайдите в меню *System→Whitelist→Add→Whitelist Host.* Добавьте IP-адрес *ip_whitelist2* в «белый» список – переместите *ip_whitelist2* из списка *Available* в список *Selected*, выберите службу:	
Service	ms-sql-all
Настроим IP Rules. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Введите следующие параметры:	
Name	allow-icmp
Action	Allow
Service	all_icmp
Source Interface	lan1
Source Network	lan1net (lannet)
Destination Interface	lan2
Destination Network	ip-mssql
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Введите следующие параметры:	
Name	allow-sql
Action	Allow
Service	ms-sql-all
Source Interface	lan1
Source Network	lan1net (lannet)

Destination Interface	lan2
Destination Network	ip-mssql
Создадим IDP Rule. Зайдите в меню *IDP/IPS→IDP Rules→Add→IDP Rule*. Задайте параметры:	
Name	IPS_SQL
Service	ms-sql-all
Protect against insertion/evasion attacks	Поставьте галочку
Source Interface	lan1
Source Network	lan1net (lannet)
Destination Interface	lan2
Destination Network	ip-mssql
Примечание: Созданное правило будет мониторить только трафик службы ms-sql-all, любой другой вид трафика не будет пропускаться данным правилом. Для других сервисов необходимо создать соответствующие правила, если есть необходимость в их мониторинге.	
Создадим IDP Rule Action. Зайдите в меню *IDP/IPS→IDP Rules→IPS_SQL→вкладка Rule Actions→Add→IDP Rule Action.* Задайте параметры:	
Action	Protect
Signature (s)	Введите IPS_MALWARE*, IPS_DB_GENERAL, IPS_DB_MSSQL, IPS_WORM_GENERAL, IPS_SCANNER*, IPS_COMPONENT_SHELLCODE, IPS_COMPONENT_INFECTION, IPS_COMPONENT_ENCODER, IPS_TCP*, IPS_UDP*, IPS_TROJAN*
Во вкладке *Log Settings* задайте параметры:	
Enable Logging	Поставьте галочку
Log with severity	Выберите из списка Debug
Создадим IDP Rule Action. Зайдите в меню *IDP/IPS→IDP Rules→IPS_SQL→вкладка Rule Actions→Add→IDP Rule Action.* Задайте параметры:	
Action	Audit
Signature (s)	Введите IDS*
Во вкладке *Log Settings* задайте параметры:	
Enable Logging	Поставьте галочку
Log with severity	Выберите из списка Debug
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Примечание: Для того чтобы избежать ложных срабатываний правил, необходимо внимательнее подходить к обозначению действия правила сигнатур как Protect, Audit и Ignored. Описание сигнатур можно найти на сайте центра сетевой защиты D-Link http://security.dlink.com.tw.	
Командная строка (CLI)	
gw-world:/> set IP4Address InterfaceAddresses/lan1net Address=192.168.10.0/24 gw-world:/> set IP4Address InterfaceAddresses/lan2net Address=172.17.100.0/24	

```
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address ip_whitelist1Address=192.168.10.10
gw-world:/labs> add IP4Address ip_whitelist2 Address=192.168.10.20
gw-world:/labs> add IP4Address ip-mssqlAddress=172.17.100.10
gw-world:/labs> cc
gw-world:/> add Service ServiceTCPUDP ms-sql-s DestinationPorts=1433 SourcePorts=1025-5000,49132-65535Type=TCP SYNRelay=Yes
gw-world:/> add Service ServiceTCPUDP ms-sql-m DestinationPorts=1434 SourcePorts=0-65535 Type=TCPUDP SYNRelay=Yes
gw-world:/> add Service ServiceGroup ms-sql-all Members=ms-sql-s,ms-sql-m
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=lan2 DestinationNetwork=labs/ip-mssql Service=all_icmp SourceInterface=lan1 SourceNetwork=InterfaceAddresses/lan1net Name=allow-icmp
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=lan2 DestinationNetwork=labs/ip-mssql Service=ms-sql-all SourceInterface=lan1 SourceNetwork=InterfaceAddresses/lan1net Name=allow-sql
gw-world:/1(labs)> cc
gw-world:/> add IDPRule DestinationInterface=lan2 DestinationNetwork=labs/ip-mssql SourceInterface=lan1 SourceNetwork=InterfaceAddresses/lan1net Service=ms-sql-all Index=1 InsertionEvasion=Yes Name=IPS_SQL
gw-world:/> cc IDPRule 1(IPS_SQL)
gw-world:/1(IPS_SQL)> add IDPRuleAction Action=Protect Index=1 Signatures=IPS_MALWARE*,IPS_DB_GENERAL,IPS_DB_MSSQL,IPS_WORM_GENERAL,IPS_SCANNER*,IPS_COMPONENT_SHELLCODE,IPS_COMPONENT_INFECTION,IPS_COMPONENT_ENCODER,IPS_TCP*,IPS_UDP*,IPS_TROJAN*LogSeverity=Debug LogEnabled=Yes
gw-world:/1(IPS_SQL)> add IDPRuleAction Action=AuditIndex=2 Signatures=IDS* LogSeverity=Debug LogEnabled=Yes
gw-world:/1(IPS_SQL)> cc
gw-world:/> activate (подождать 3-5 секунд)
gw-world:/>commit
```

Упражнение	Осуществите тестовую атаку на сервер MS SQL из сети lan1net. Для проверки срабатывания IDP-правил зайдите в статус *Status→IDP/IPS*. На указанную при настройке SMTP Event Receiver почту будут приходить уведомления о срабатывании IDP-правил. Используйте на атакующей машине IP-адреса 192.168.10.7 и 192.168.10.20 поочередно, проверте статус IDP/IPS для этих разных адресов атакующего компьютера.

Примеры сообщений при аудите к атакам на SQL-сервер, защищенный межсетевым экраном. Для осуществления атак используется Rapid7 Metasploit и Nexpose. На рисунке 7.31 показаны сообщения IDP/IPS о сканировании и атаке на SQL-сервер с разных IP-адресов lan1-сети.

Рисунок 7.31

Date	Severity	Category/ID	Rule	Proto	Src/DstIf	Src/DstIP	Src/DstPort	Event/Action
2012-03-04 16:47:20	Notice	IDP 1300007	IDP_SQL	TCP		192.168.10.7 172.17.100.10	16108 1433	intrusion_detected
description="MSSQL.PING.METASPLOIT" signatureid=17421 idrule="IDP_SQL" Advisory link								
2012-03-04 15:02:50	Notice	IDP 1300005	IDP_SQL	TCP		192.168.10.212 172.17.100.10	1221 1433	scan_detected
description="APPCHECK.RPC.DISCOVERY" signatureid=17431 idrule="IDP_SQL" Advisory link								

На рисунке 7.32 показаны найденные уязвимости сервера MS SQL

Рисунок 7.32

Vulnerability Listing

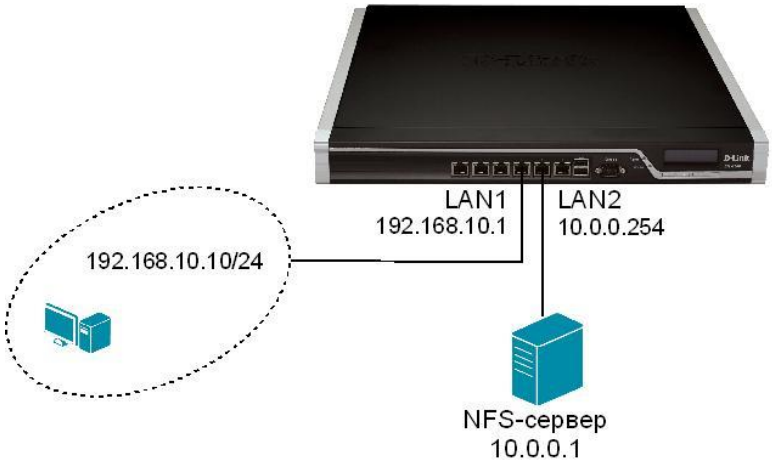
Exposures: Susceptible to malware attacks Metasploit-exploitable Exploit published

Title	CVSS	Risk	Published On	Severity	Instances
Microsoft SQL Server 2005 Service Pack 4 (KB2463332)	6.8	126	Sat Dec 18 2010	Severe	1
Microsoft SQL Server 2005 Service Pack 1 (KB 913090)	6.8	278	Tue Apr 18 2006	Severe	1
Microsoft SQL Server 2005 Service Pack 2 (KB 921896)	6.8	256	Tue Mar 6 2007	Severe	1
Microsoft SQL Server 2005 Service Pack 3 (KB955706)	6.8	201	Tue Feb 10 2009	Severe	1
Database Open Access	5	169	Fri Jan 1 2010	Moderate	2

Защита NFS-сервера на базе Oracle Solaris с помощью IDP/IPS

Описание сценария	*Необходимо защитить NFS-сервер, расположенный в* ***lan2****, с помощью механизма IDP/IPS.* *Данная работа выполняется на межсетевом экране DFL-1660.*

Схема 90



Настройка DFL-1660

Web-интерфейс

Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:

Name	ip-nfs
Address	10.0.0.1

Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:

Name	lan1net
Address	192.168.10.0/24

Зайдите в меню *Objects→Address Book→Add→IP4 Address*. Введите следующие параметры:

Name	lan2net
Address	10.0.0.0/24

Создание сервисов

Зайдите в меню *Objects→Services*, добавьте TCP/UDP Service со следующими параметрами:

Name	rpcbind
Type	TCP/UDP (выберите из списка)
Source	0-65535
Destination	111
SYN flood protection (SYN Relay)	Поставьте галочку

Зайдите в меню *Objects→Services*, добавьте TCP/UDP Service со следующими параметрами:	
Name	mountd
Type	TCP/UDP (выберите из списка)
Source	0-65535
Destination	32814, 33201
SYN flood protection (SYN Relay)	Поставьте галочку
Зайдите в меню *Objects→Services*, добавьте TCP/UDP Service со следующими параметрами:	
Name	nfs
Type	TCP/UDP (выберите из списка)
Source	0-65535
Destination	2049
SYN flood protection (SYN Relay)	Поставьте галочку
Зайдите в меню *Objects→Services*, добавьте TCP/UDP Service со следующими параметрами:	
Name	nlockmgr
Type	TCP/UDP (выберите из списка)
Source	0-65535
Destination	4045
SYN flood protection (SYN Relay)	Поставьте галочку
Зайдите в меню *Objects→Services*, добавьте TCP/UDP Service со следующими параметрами:	
Name	meta-and-other
Type	TCP/UDP(выберите из списка)
Source	0-65535
Destination	32772-32779
SYN flood protection (SYN Relay)	Поставьте галочку
Создадим Service Group из всех сервисов, необходимых для NFS. Зайдите в меню *Objects→Services→Add→Service Group*. Во вкладке *General*, введите следующие параметры:	
Name	nfs-all
Selected	Переместите rpcbind, mountd, nfs, nlockmgr, meta-and-other из списка Available.
Настроим IP Rules. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Введите следующие параметры:	
Name	allow-icmp
Action	Allow
Service	all_icmp
Source Interface	lan1
Source Network	lan1net (lannet)
Destination Interface	lan2
Destination Network	ip-nfs
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Введите следующие параметры:	
Name	allow-nfs
Action	Allow
Service	nfs-all

Source Interface	lan1
Source Network	lan1net (lannet)
Destination Interface	lan2
Destination Network	ip-nfs
Создадим IDP Rule. Зайдите в меню *IDP/IPS→IDP Rules→Add→IDP Rule*. Задайте параметры:	
Name	IPS_SOL
Service	nfs-all
Protect against insertion/evasion attacks	Поставьте галочку
Source Interface	lan1
Source Network	lan1net (lannet)
Destination Interface	lan2
Destination Network	ip-nfs
Примечание: Созданное правило будет мониторить только трафик службы nfs-all, любой другой вид трафика не будет пропускаться данным правилом. Для других служб необходимо создать соответствующие правила, если есть необходимость в их мониторинге.	
Создадим IDP Rule Action. Зайдите в меню *IDP/IPS→IDP Rules→IPS_SOL→вкладка Rule Actions→Add→IDP Rule Action.* Задайте параметры:	
Action	Protect
Signature (s)	Введите IPS_MALWARE*, IPS_OS-SPECIFIC_GENERAL, IPS_OS-SPECIFIC_SOLARIS, IPS_NFS*, IPS_WORM_GENERAL, IPS_SCANNER*, IPS_COMPONENT_SHELLCODE, IPS_COMPONENT_INFECTION, IPS_COMPONENT_ENCODER, IPS_TCP*, IPS_UDP*, IPS_TROJAN*
Во вкладке *Log Settings* задайте параметры:	
Enable Logging	Поставьте галочку
Log with severity	Выберите из списка Debug.
Создадим IDP Rule Action. Зайдите в меню *IDP/IPS→IDP Rules→IPS_SOL→вкладка Rule Actions→Add→IDP Rule Action.* Задайте параметры:	
Action	Audit
Signature (s)	Введите IDS*
Во вкладке *Log Settings* задайте параметры:	
Enable Logging	Поставьте галочку
Log with severity	Выберите из списка Debug
Зайдите в меню *Configuration* и выберите *Save and Activate*.	
Примечание: Для того чтобы избежать ложных срабатываний правил, необходимо внимательнее подходить к обозначению действия правила сигнатур как Protect, Audit и Ignored. Описание сигнатур можно найти на сайте центра сетевой защиты D-Link http://security.dlink.com.tw.	
Командная строка (CLI)	

```
gw-world:/> set IP4Address InterfaceAddresses/lan1net Address=192.168.10.0/24
gw-world:/> set IP4Address InterfaceAddresses/lan2net Address=10.0.0.0/24
gw-world:/> cc Address AddressFolder labs
gw-world:/labs> add IP4Address ip-nfsAddress=10.0.0.1
gw-world:/labs> cc
gw-world:/> add Service ServiceTCPUDP rpcbind DestinationPorts=111 SourcePorts=0-65535Type=TCPUDP SYNRelay=Yes
gw-world:/> add Service ServiceTCPUDP mountd DestinationPorts=32814,33201SourcePorts=0-65535 Type=TCPUDP SYNRelay=Yes
gw-world:/> add Service ServiceTCPUDP nfs DestinationPorts=2049SourcePorts=0-65535 Type=TCPUDP SYNRelay=Yes
gw-world:/> add Service ServiceTCPUDP nlockmgr DestinationPorts=4045SourcePorts=0-65535 Type=TCPUDP SYNRelay=Yes
gw-world:/> add Service ServiceTCPUDP meta-and-other DestinationPorts=32772-32779SourcePorts=0-65535 Type=TCPUDP SYNRelay=Yes
gw-world:/> add Service ServiceGroup nfs-all Members=pcbind,mountd,nfs,nlockmgr,meta-and-other
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=lan2 DestinationNetwork=labs/ip-nfsService=all_icmp SourceInterface=lan1 SourceNetwork=InterfaceAddresses/lan1net Name=allow-icmp
gw-world:/1(labs)> add IPRule Action=Allow DestinationInterface=lan2 DestinationNetwork=labs/ip-nfsService=nfs-all SourceInterface=lan1 SourceNetwork=InterfaceAddresses/lan1net Name=allow-nfs
gw-world:/1(labs)> cc
gw-world:/> add IDPRule DestinationInterface=lan2 DestinationNetwork=labs/ip-nfsSourceInterface=lan1 SourceNetwork=InterfaceAddresses/lan1net Service=nfs-all Index=1 InsertionEvasion=Yes Name=IPS_SOL
gw-world:/> cc IDPRule 1(IPS_SOL)
gw-world:/1(IPS_SOL)> add IDPRuleAction Action=Protect Index=1 Signatures=IPS_MALWARE*,IPS_OS-SPECIFIC_GENERAL,IPS_OS-SPECIFIC_SOLARIS,IPS_NFS*,IPS_WORM_GENERAL,IPS_SCANNER*,IPS_COMPONENT_SHELLCODE,IPS_COMPONENT_INFECTION,IPS_COMPONENT_ENCODER,IPS_TCP*,IPS_UDP*,IPS_TROJAN*LogSeverity=Debug LogEnabled=Yes
gw-world:/1(IPS_SOL)> add IDPRuleAction Action=AuditIndex=2 Signatures=IDS* LogSeverity=Debug LogEnabled=Yes
gw-world:/1(IPS_SOL)> cc
gw-world:/> activate (подождать 3-5 секунд)
gw-world:/>commit
```

Упражнение	Осуществите тестовую атаку на NFS-сервер из сети lan1net. Для проверки срабатывания IDP-правил зайдите в меню *Status→IDP/IPS*. На указанную при настройке SMTP Event Receiver почту будут приходить уведомления о срабатывании IDP-правил.

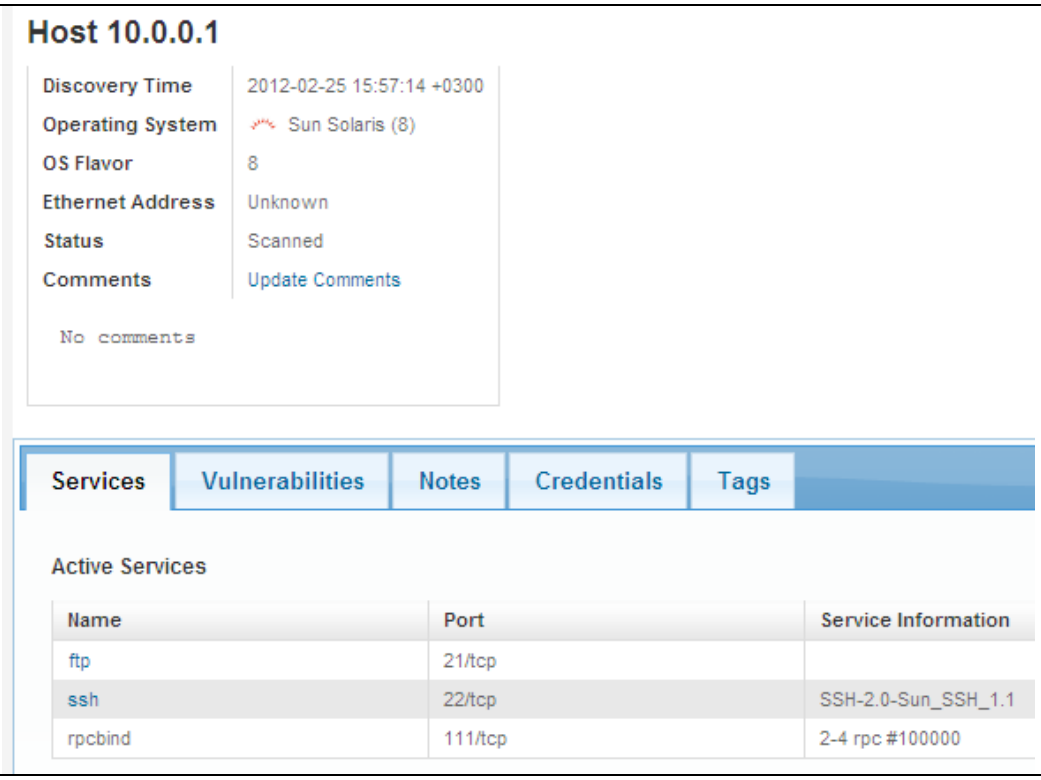
Примеры сообщений при аудите к атакам на NFS-сервер, защищенный межсетевым экраном. Для осуществления атак используется Rapid7 Metasploitu Nexpose. На рисунке 7.33 показаны сообщения IDP/IPS о сканировании и атаке на NFS-сервер.

Рисунок 7.33

2012-03-04 17:34:49	Notice	IDP 1300005	IDP_SOL	TCP	192.168.10.212 10.0.0.1	5937 111	scan_detected
description="APPCHECK.RPC.DISCOVERY" signatureid=17431 idrule="IDP_SOL" Advisory link							
2012-03-04 17:34:33	Notice	IDP 1300005	IDP_SOL	TCP	192.168.10.212 10.0.0.1	5927 111	scan_detected
description="APPCHECK.RPC.DISCOVERY" signatureid=17431 idrule="IDP_SOL" Advisory link							

На рисунке 7.34 показана часть результата сканирования NFS-сервера.

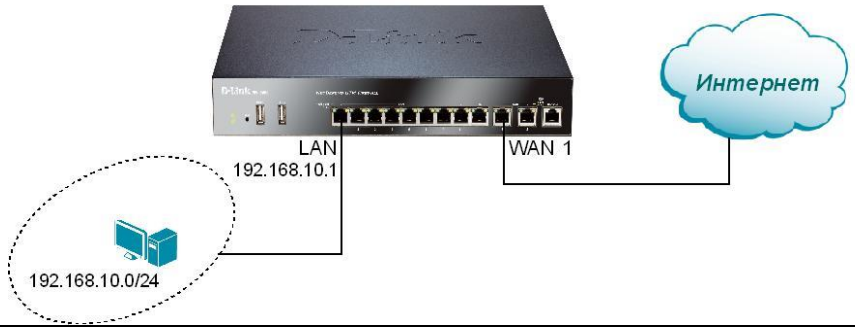
Рисунок 7.34



Защита от сетевых атак при помощи пороговых правил (Threshold Rules)

Описание метода	*Цель действия пороговых правил состоит в обнаружении необычной активности хостов и реагирования на неё. Пример подобной необычной активности – заражение компьютера в локальной сети вирусом, пытающегося повторить подключения к внешним адресам. Пороговые правила основываются на пороговых политиках, возможные действия Action – Audit или Protect.*

Настройка IDP/IPS для защиты пользователей lan-сети, имеющих доступ в Интернет.

Описание сценария	*Защитим локальную сеть от атак, вирусов, сканирования через протокол HTTP при использовании пользователями Web-браузера MS Internet Explorer. Также необходимо ограничить подозрительно активные компьютеры в сети lannet с помощью пороговых правил. Установим порог в 100 подключений/сек, но только для мониторинга (действие Audit).*
Схема 91	

<u>Настройка DFL-860E</u>

<u>Web-интерфейс</u>

Настройте wan1-интерфейс в соответствии с параметрами, заданными Интернет-провайдером.

Добавим новый HTTP ALG. Зайдите в меню *Objects→ALG→Add→HTTP ALG.* Во вкладке *General* введите следующие параметры:	
Name	http-alg
Fail Mode	Deny
Во вкладке *File Integrity* введите следующие параметры:	
Verify MIME-type against file content.	Поставьте галочку
Block selected file types	cmd, com, doc, exe, pif, ppt, scr, xls
Во вкладке *Anti-Virus* введите следующие параметры:	
Mode	Protect
Создание сервиса	
Зайдите в меню *Objects→Services*, добавьте TCP/UDP Service со следующими параметрами:	
Name	http-outbound1
Type	TCP (выберите из списка)
Source	0-65535
Destination	80
ALG	http-alg
Настроим IP Rules. Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Введите следующие параметры:	
Name	allow-http
Action	NAT
Service	http-outbound1
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets
Создадим пороговое правило. Зайдите в меню *Traffic Management→Threshold Rules→Add→Threshold Rule*.Задайте параметры правила:	
Name	threshold-rule
Service	all-services
Source Interface	lan
Source Network	lannet
Destination Interface	any
Destination Network	all-nets
Во вкладке *Threshold Action* добавьте новое действие правила, введите следующие параметры:	
Action	Audit
Group By	Host-based
Threshold	100 Connections/Second
Создадим IDP Rule. Зайдите в меню *IDP/IPS→IDP Rules→Add→IDP Rule*. Задайте параметры:	
Name	IPS_HTTP
Service	http-outbound1
Protect against insertion/evasion attacks	Поставьте галочку
Invalid UTF8	DropLog
Invalid hex encoding	DropLog

Double encoding	DropLog
Source Interface	lan
Source Network	lannet
Destination Interface	wan1
Destination Network	all-nets

Примечание: Созданное правило будет мониторить только трафик службы http-outbound1, любой другой вид трафика не будет пропускаться данным правилом. Для других сервисов необходимо создать соответствующие правила, если есть необходимость в их мониторинге.

Создадим IDP Rule Action. Зайдите в меню *IDP/IPS→IDP Rules→IPS_HTTP→вкладка Rule Actions→Add→IDP Rule Action.* Задайте параметры:

Action	Protect
Signature (s)	Введите IPS_HTTP*, IPS_BROWSER_GENERAL, IPS_BROWSER_JAVASCRIPT, IPS_BROWSER_IE, IPS_MALWARE*, IPS_WORM_GENERAL, IPS_SCANNER*, IPS_COMPONENT_SHELLCODE, IPS_TCP*, IPS_TROJAN*

Во вкладке *Log Settings* задайте параметры:

Enable Logging	Поставьте галочку
Log with severity	Выберите из списка Debug

Зайдите в меню *Configuration* и выберите *Save and Activate*.

Примечание: 1. IPS_HTTP* – включает группы сигнатур IPS_HTTP_CGI, IPS_HTTP_CISCO, IPS_HTTP_GENERAL, IPS_HTTP_MICROSOFT IIS и другие. Введенный параметр IPS* добавит все IPS-сигнатуры, параметр ** задействует все сигнатуры.
2. Для того чтобы избежать ложных срабатываний правил, необходимо внимательнее подходить к обозначению действия правила сигнатур как Protect, Audit и Ignored. Описание сигнатур можно найти на сайте центра сетевой защиты D-Link http://security.dlink.com.tw.
3. Если есть несколько правил с различными действиями для одной и той же комбинации Type и Grouping, то будет выполняться действие, соответствующее наибольшему пороговому значению.
4. Существует опция дополнительных настроек Before Rules, которые понижают пороговое значение при их разрешении.

Командная строка (CLI)

```
gw-world:/> add ALG ALG_HTTP http-alg FailModeBehavior=Deny VerifyContentMimetype=Yes FileListType=Block File=cmd,com,doc,exe,pif,ppt,scr,xls Antivirus=Protect
gw-world:/> add Service ServiceTCPUDP http-outbound1 DestinationPorts=80 SourcePorts=0-65535 Type=TCP ALG=http-alg
gw-world:/> cc IPRuleFolder labs
gw-world:/1(labs)> add IPRule Action=NAT DestinationInterface=wan1 DestinationNetwork=all-netsService=http-outbound1 SourceInterface=lan SourceNetwork=InterfaceAddresses/lannetName=allow-http
gw-world:/1(labs)> cc
gw-world:/>add ThresholdRule DestinationInterface=any Service=all_services DestinationNetwork=all-nets SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet Index=1 Name=threshold-rule
gw-world:/> cc ThresholdRule 1(threshold-rule)
```

gw-world:/1(threshold-rule)> add ThresholdAction Threshold=100 Index=1 ThresholdUnit=ConnsSec Action=Audit GroupBy=SourceIP
gw-world:/1(threshold-rule)> cc
gw-world:/> add IDPRule DestinationInterface=wan1 DestinationNetwork=all-netsSourceInterface=lan SourceNetwork=InterfaceAddresses/lannetService=http-outbound1 Index=1 InsertionEvasion=Yes URIIllegalUTF8=DropLog URIIllegalHex=DropLog URIDoubleEncode=DropLogName=IPS_HTTP
gw-world:/> cc IDPRule 1(IPS_HTTP)
gw-world:/1(IPS_HTTP)> add IDPRuleAction Action=Protect Index=1 Signatures=IPS_HTTP*,IPS_BROWSER_GENERAL,IPS_BROWSER_JAVASCRIPT,IPS_BROWSER_IE,IPS_MALWARE*,IPS_WORM_GENERAL,IPS_SCANNER*,IPS_COMPONENT_SHELLCODE,IPS_TCP*,IPS_TROJAN*
LogSeverity=Debug LogEnabled=Yes
gw-world:/1(IPS_HTTP)> add IDPRuleAction Action=AuditIndex=2 Signatures=IDS* LogSeverity=Debug LogEnabled=Yes
gw-world:/1(IPS_HTTP)> cc
gw-world:/> activate *(подождать 3-5 секунд)*
gw-world:/>commit

Упражнение	Откройте незаслуживающие доверия ресурсы Интернета с компьютеров **lan**-сети, используя Web-браузер MS Internet Explorer. Для проверки срабатывания IDP-правил зайдите в меню *Status→IDP/IPS*. На указанную при настройке SMTP Event Receiver почту будут приходить уведомления о срабатывании IDP-правил.

На рисунке 7.35 показаны примеры сообщений IDP/IPS об обнаружении сканирования с различных ресурсов (на wan1_ip межсетевого экрана).

Рисунок 7.35

Date	Severity	Category/ID	Rule	Proto	Src/DstIf	Src/DstIP	Src/DstPort	Event/Action
2012-02-10 23:04:55	Notice	IDP 1300001	IPS_HTTP	TCP		74.125.229.56 10.72.240.212	80 27705	scan_detected close
description="GIF.File.Microsoft.InternetExplorer.Double.Free.A" signatureid=55977 idrule="IPS_HTTP" Advisory link								
2012-02-10 23:04:42	Notice	IDP 1300001	IPS_HTTP	TCP		74.125.229.56 10.72.240.212	80 8275	scan_detected close
description="GIF.File.Microsoft.InternetExplorer.Double.Free.A" signatureid=55977 idrule="IPS_HTTP" Advisory link								
2012-02-10 23:04:26	Notice	IDP 1300001	IPS_HTTP	TCP		89.108.75.166 10.72.240.212	80 8158	scan_detected close
description="GIF.File.Microsoft.InternetExplorer.Double.Free.A" signatureid=55977 idrule="IPS_HTTP" Advisory link								
2012-02-10 23:04:24	Notice	IDP 1300001	IPS_HTTP	TCP		89.108.75.166 10.72.240.212	80 61624	scan_detected close
description="GIF.File.Microsoft.InternetExplorer.Double.Free.A" signatureid=55977 idrule="IPS_HTTP" Advisory link								
2012-02-10 23:04:24	Notice	IDP 1300001	IPS_HTTP	TCP		81.19.88.102 10.72.240.212	80 32630	scan_detected close
description="GIF.File.Microsoft.InternetExplorer.Double.Free.A" signatureid=55977 idrule="IPS_HTTP" Advisory link								
2012-02-10 23:04:24	Notice	IDP 1300001	IPS_HTTP	TCP		88.212.196.66 10.72.240.212	80 41279	scan_detected close
description="GIF.File.Microsoft.InternetExplorer.Double.Free.A" signatureid=55977 idrule="IPS_HTTP" Advisory link								
2012-02-10 23:04:24	Notice	IDP 1300001	IPS_HTTP	TCP		89.108.75.166 10.72.240.212	80 38955	scan_detected close
description="GIF.File.Microsoft.InternetExplorer.Double.Free.A" signatureid=55977 idrule="IPS_HTTP" Advisory link								
2012-02-10 23:02:07	Notice	IDP 1300001	IPS_HTTP	TCP		193.219.52.197 10.72.240.212	80 22764	scan_detected close
description="http.URI.Handler.MicrosoftWindows.Command.Execution" signatureid=56051 idrule="IPS_HTTP" Advisory link								
2012-02-10 23:02:00	Notice	IDP 1300001	IPS_HTTP	TCP		74.125.229.56 10.72.240.212	80 10407	scan_detected close
description="GIF.File.Microsoft.InternetExplorer.Double.Free.A" signatureid=55977 idrule="IPS_HTTP" Advisory link								

Приложение Е

Пример создания и работы с сертификатами

Создание сертификатов.
Для создания сертификатов можно использовать программу OpenSSL.

В примере используется программа **OpenSSL 0.9.8k** для **ОС LinuxDebianLenny.**

Откройте файл */etc/ssl/openssl.cnf*, найдите строку *default_days = 365* и укажите нужное вам количество дней, на которые выдается сертификат, например, *1095*, затем найдите строку *# subjectAltName=email:copy* и удалите символ #. Сохраните файл.

Создайте отдельную папку для сертификатов:

mkdircert&&cdcert/

Скопируйте скрипт, упрощающий создание CA сертификата.

test@svasiliev:~/cert$ cp /usr/lib/ssl/misc/CA.sh .

Проверьте наличие файла:

test@svasiliev:~/cert$ ls

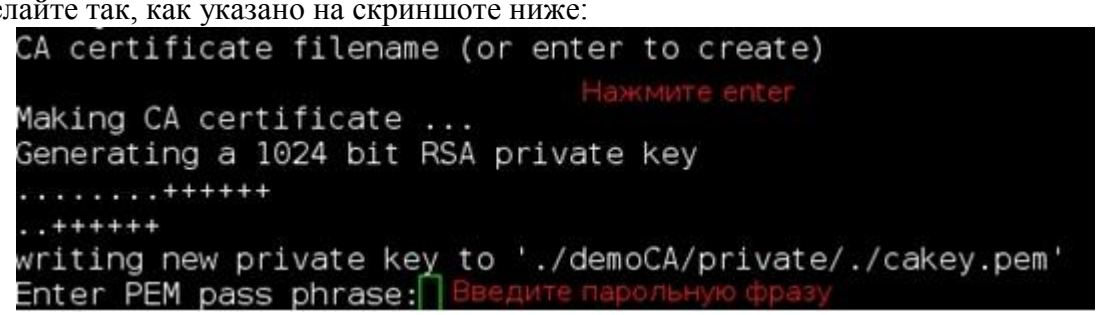
CA.sh

Измените в файле строку *DAYS="-days 365"*, указав нужное количество дней, в противном случае необходимо выдавать новые сертификаты каждый год. Не рекомендуется менять это значение для повышения безопасности.

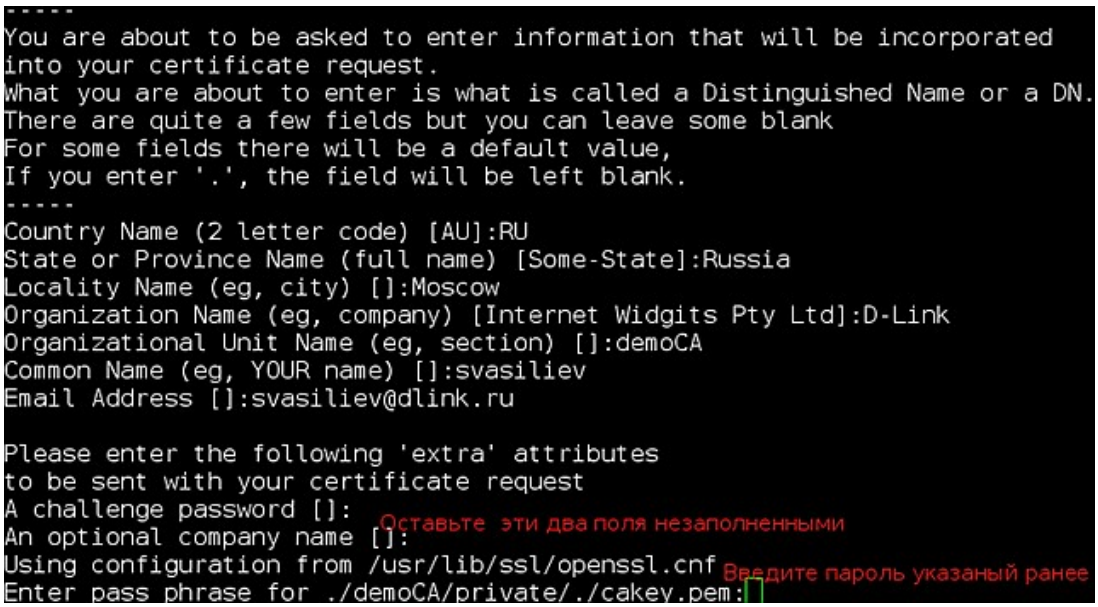
Создаем самоподписанный сертификат CA.

test@svasiliev:~/cert$ sh CA.sh -newca

Сделайте так, как указано на скриншоте ниже:



Теперь ответьте на максимум вопросов, пример показан ниже на скриншоте:



Создание самоподписанного сертификата CA demoCA/cacert.pem и секретного ключа demoCA/private/cakey.pem завершено. В дальнейшем сертификат и ключ понадобятся для подписи сертификатов, а CA сертификат будет импортирован в удаленные устройства или компьютеры без секретного ключа.

ВНИМАНИЕ: НЕ РАСПРОСТРАНЯЙТЕ СЕКРЕТНЫЙ КЛЮЧ ОТ CA СЕРТИФИКАТА! В СЛУЧАЕ КОМПРОМЕТАЦИИ КЛЮЧА НЕМЕДЛЕННО СОЗДАТЬ НОВЫЙ КЛЮЧ И СЕРТИФИКАТ CA. ЭТО ПРИВЕДЕТ К НЕОБХОДИМОСТИ ЗАМЕНЫ ВСЕХ ВЫДАННЫХ РАНЕЕ СЕРТИФИКАТОВ.

Теперь необходимо создать два подписанных сертификата с секретными ключами, один из сертификатов должен быть импортирован в DFL и установлен в тоннеле в качестве local certificate, другой сертификат должен быть импортирован в удаленное устройство или компьютер (в нашем примере – во второй DFL).

Создаем запрос на сертификат с секретным ключом для DFL:

test@svasiliev:~/cert$ openssl req -new -keyout dflkey.pem -out dflreq.pem

Как и при создании сертификата CA, введите парольную фразу и ответьте на вопросы.

Подпишите сертификат с помощью сертификата CA и секретного ключа сертификата CA (Примечание: т.к. для создания сертификата использовался скрипт CA.sh, все параметры уже заданны, и система знает, где искать сертификат CA и его приватный ключ, поэтому можно не указывать их явно для подписи):

test@svasiliev:~/cert$ openssl ca -policy policy_anything -out dflcert.pem -infiles dflreq.pem

Введите парольную фразу для секретного ключа CA (demoCA/private/cakey.pem).

Снимите шифрование с секретного ключа для DFL:

test@svasiliev:~/cert$ openssl rsa -in dflkey.pem -out dfl.pem

Создайте таким же способом подписанный сертификат с секретным ключем для удаленного хоста.

test@svasiliev:~/cert$ openssl req -new -keyout remotekey.pem -out remotereq.pem
test@svasiliev:~/cert$ openssl ca -policy policy_anything -out remotecert.pem -infiles remotereq.pem

test@svasiliev:~/cert$ openssl rsa -in remotekey.pem -out remote.pem

Таким же образом необходимо создать отдельные сертификаты на каждый удаленный хост.

ВНИМАНИЕ: Все сертификаты должны отличаться вводимыми данными!

Теперь созданные сертификаты должны быть импортированы в первый и второй DFL.

Сертификаты **cacert.pem, dflcert.pem**и секретный ключ**dfl.pem**должны быть импортированы в локальный DFL (первый DFL), а в удаленное устройство (второй DFL) должны быть импортированы сертификаты **cacert.pem, remotecert**и секретный ключ**remote.pem**.

УСТАНОВКА СЕРТИФИКАТОВ В ОС WINDOWS.

Преобразуйте сертификаты в формат, понятный Windows:

test@svasiliev:~/cert$ openssl pkcs12 -export -inkey remote.pem -certfile demoCA/cacert.pem -in remotecert.pem -out wincert.p12

Введите парольную фразу, которая понадобится для установки сертификата в Windows.

Скопируйте файлы **cacert.pem** и **wincert.p12** на компьютер под управлением ОС Windows. Переименуйте файл **cacert.pem** на **cacert.crt**

Нажмите дважды мышкой по файлу **cacert.crt**, нажмите Установить сертификат, затем **Далее**, выберите **Поместить все сертификаты в следующие хранилище**, нажмите кнопку **Обзор** и укажите **Доверенные корневые центры сертификации**, затем нажмите **ОК** и **Далее,** потом на кнопку **Готово.**

Нажмите дважды мышкой по файлу **wincert.p12**, запустится мастер импорта сертификатов. Дважды нажмите на кнопку **Далее,** в поле **Пароль** введите парольную фразу, используемую для конвертации сертификата в формат p12 и нажмите **Далее,** выберите **Поместить все сертификаты в следующие хранилище**, нажмите кнопку **Обзор**, выберите **Личные**, затем нажмите **ОК, Далее**, затем кнопку **Готово.**

ВНИМАНИЕ: При использовании Windows 2003 необходимо импортировать сертификаты в профиль пользователя и компьютера.

Приложение F

Группы сигнатур IDP

Имя группы	Тип вторжения
APP_AMANDA	Amanda, популярное ПО для резервного копирования
APP_ETHEREAL	Ethereal
APP_ITUNES	Медиаплеер Apple iTunes
APP_REALPLAYER	Медиаплеер RealNetworks
APP_REALSERVER	Медиаплеер RealServer RealNetworks
APP_WINAMP	WinAMP
APP_WMP	Медиаплеер MS Windows
AUTHENTICATION_GENERAL	Аутентификация
AUTHENTICATION_KERBEROS	Kerberos
AUTHENTICATION_XTACACS	XTACACS
BACKUP_ARKEIA	Решение для резервного копирования
BACKUP_BRIGHTSTOR	Решения для резервного копирования, созданные CA
BACKUP_GENERAL	Решения для резервного копирования
BACKUP_NETVAULT	Решение для резервного копирования
BACKUP_VERITAS	Решения для резервного копирования
BOT_GENERAL	Программы-роботы, включая боты, управляемые IRC-каналами
BROWSER_FIREFOX	Mozilla Firefox
BROWSER_GENERAL	Основные атаки на web-браузеры/клиенты
BROWSER_IE	Microsoft IE
BROWSER_MOZILLA	Браузер Mozilla
COMPONENT_ENCODER	Шифраторы как часть атаки
COMPONENT_INFECTION	Вирус как часть атаки
COMPONENT_SHELLCODE	Шелл-код как часть атак
DB_GENERAL	Системы базы данных
DB_MSSQL	Сервер MS SQL
DB_MYSQL	MySQL DBMS
DB_ORACLE	Oracle DBMS
DB_SYBASE	Сервер Sybase
DCOM_GENERAL	MS DCOM
DHCP_CLIENT	DHCP-клиент
DHCP_GENERAL	DHCP-протокол
DHCP_SERVER	DHCP-сервер
DNS_EXPLOIT	DNS-атаки
DNS_GENERAL	Система доменных имен
DNS_OVERFLOW	Атака на переполнение длины DNS запроса
DNS_QUERY	Атаки, связанные с запросом
ECHO_GENERAL	Принцип работы Echo протокола
ECHO_OVERFLOW	Переполнение буфера Echo
FINGER_BACKDOOR	Finger backdoor
FINGER_GENERAL	Принцип работы протокола Finger

FINGER_OVERFLOW	Переполнение буфера в реализации протокола Finger
FS_AFS	Файловаясистема AFS (Andrew File System)
FTP_DIRNAME	Атака Directory name attack
FTP_FORMATSTRING	Атака Format string attack
FTP_GENERAL	FTP-протокол и использование
FTP_LOGIN	Атака с целью определения логина
FTP_OVERFLOW	Переполнение буфера FTP
GAME_BOMBERCLONE	Игра Bomberclone
GAME_GENERAL	Generic game servers/clients
GAME_UNREAL	Игровой сервер UnReal
HTTP_APACHE	Apache httpd
HTTP_BADBLUE	Web-сервер Badblue
HTTP_CGI	HTTP CGI
HTTP_CISCO	Встроенный Web сервер Cisco
HTTP_GENERAL	Основные операции HTTP
HTTP_MICROSOFTIIS	HTTP атаки, специфичные для Web сервера MS IIS
HTTP_OVERFLOWS	Переполнение буфера для HTTP-серверов
HTTP_TOMCAT	Tomcat JSP
ICMP_GENERAL	Принцип работы ICMP-протокола
IGMP_GENERAL	IGMP
IMAP_GENERAL	Принцип работы IMAP-протокола
IM_AOL	AOL IM
IM_GENERAL	Реализация обмена мгновенными сообщениями
IM_MSN	MSN Messenger
IM_YAHOO	Yahoo Messenger
IP_GENERAL	Принцип работы IP-протокола
IP_OVERFLOW	Переполнение буфера в реализации протокола IP
IRC_GENERAL	Internet Relay Chat
LDAP_GENERAL	Основные LDAP клиенты/серверы
LDAP_OPENLDAP	Открыть LDAP
LICENSE_CA-LICENSE	Лицензия для программного обеспечения CA
LICENSE_GENERAL	Менеджер лицензии
MALWARE_GENERAL	Вредоносные атаки
METASPLOIT_FRAME	Атака с помощью metasploit frame
METASPLOIT_GENERAL	Атака Metasploit general attack
MISC_GENERAL	Основная атака
MSDTC_GENERAL	MS DTC
MSHELP_GENERAL	Справка Microsoft Windows
NETWARE_GENERAL	Основной протокол NetWare
NFS_FORMAT	Форматировать
NFS_GENERAL	Принцип работы NFS-протокола
NNTP_GENERAL	Принцип работы NNTP-протокола
OS_SPECIFIC-AIX	AIX specific
OS_SPECIFIC-GENERAL	OS general
OS_SPECIFIC-HPUX	HP-UX related

OS_SPECIFIC-LINUX	Linux specific
OS_SPECIFIC-SCO	SCO specific
OS_SPECIFIC-SOLARIS	Solaris specific
OS_SPECIFIC-WINDOWS	Windows specific
P2P_EMULE	Инструмент eMule P2P
P2P_GENERAL	Основные инструменты P2P
P2P_GNUTELLA	Инструмент Gnutella P2P
PACKINGTOOLS_GENERAL	Атака General packing tools
PBX_GENERAL	PBX
POP3_DOS	Denial of Service для POP
POP3_GENERAL	Post Office Protocol v3
POP3_LOGIN-ATTACKS	Атака с целью определения логина и пароля
POP3_OVERFLOW	Переполнение сервера POP3
POP3_REQUEST-ERRORS	Ошибка запроса
PORTMAPPER_GENERAL	PortMapper
PRINT_GENERAL	LP printing server: LPR LPD
PRINT_OVERFLOW	Переполнение буфера в реализации протокола IP или LPR/LPD
REMOTEACCESS_GOTOMYPC	Перейти в Мой компьютер
REMOTEACCESS_PCANYWHERE	PcAnywhere
REMOTEACCESS_RADMIN	Удаленный администратор
REMOTEACCESS_VNC-CLIENT	Атаки на VNC-клиентов
REMOTEACCESS_VNC-SERVER	Атаки на VNC-серверы
REMOTEACCESS_WIN-TERMINAL	Windows terminal/Удаленный рабочий стол
RLOGIN_GENERAL	RLogin протокол и использование
RLOGIN_LOGIN-ATTACK	Атаки с целью определения логина
ROUTER_CISCO	Атаки на маршрутизатор Cisco
ROUTER_GENERAL	Атаки на маршрутизатор
ROUTING_BGP	Протокол BGP
RPC_GENERAL	Принцип работы RPC-протокола
RPC_JAVA-RMI	Java RMI
RSYNC_GENERAL	Rsync
SCANNER_GENERAL	Сканеры
SCANNER_NESSUS	Сканер Nessus
SECURITY_GENERAL	Антивирусные решения
SECURITY_ISS	ПО для обеспечения безопасности
SECURITY_MCAFEE	McAfee
SECURITY_NAV	Решение Symantec AV
SMB_ERROR	Ошибка SMB
SMB_EXPLOIT	SMB Exploit
SMB_GENERAL	Атаки SMB
SMB_NETBIOS	Атаки NetBIOS
SMB_WORMS	Черви SMB
SMTP_COMMAND-ATTACK	SMTP command attack
SMTP_DOS	Denial of Service для SMTP
SMTP_GENERAL	Принцип работы SMTP-протокола
SMTP_OVERFLOW	Переполнение буфера SMTP
SMTP_SPAM	СПАМ

SNMP_ENCODING	SNMP шифрование
SNMP_GENERAL	Принцип работы SNMP-протокола
SOCKS_GENERAL	Принцип работы SOCKS-протокола
SSH_GENERAL	Принцип работы SSH-протокола
SSH_LOGIN-ATTACK	Атаки с целью определения логина и пароля
SSH_OPENSSH	Сервер OpenSSH
SSL_GENERAL	Принцип работы SSL-протокола
TCP_GENERAL	Принцип работы TCP-протокола
TCP_PPTP	Point-to-Point Tunneling Protocol
TELNET_GENERAL	Принцип работы Telnet протокола
TELNET_OVERFLOW	Telnet buffer overflow attack
TFTP_DIR_NAME	Directory Name attack
TFTP_GENERAL	Принцип работы TFTP-протокола
TFTP_OPERATION	Атака, нарушающая работоспособность
TFTP_OVERFLOW	Атака на переполнение буфера TFTP
TFTP_REPLY	TFTP Reply attack
TFTP_REQUEST	TFTP request attack
TROJAN_GENERAL	Троян
UDP_GENERAL	UDP
UDP_POPUP	Всплывающее окно для MS Windows
UPNP_GENERAL	UPNP
VERSION_CVS	CVS
VERSION_SVN	Свободная централизованная система управления версиями
VIRUS_GENERAL	Вирус
VOIP_GENERAL	Принцип работы VoIP-протокола
VOIP_SIP	Принцип работы SIP-протокола
WEB_CF-FILE-INCLUSION	Вложение файлов Coldfusion
WEB_FILE-INCLUSION	Вложение файлов
WEB_GENERAL	Web application attacks
WEB_JSP-FILE-INCLUSION	Вложение файлов JSP
WEB_PACKAGES	Пакеты популярных Web-приложений
WEB_PHP-XML-RPC	PHP XML RPC
WEB_SQL-INJECTION	Внедрение SQL-кода
WEB_XSS	Cross-Site-Scripting
WINS_GENERAL	Служба MS WINS
WORM_GENERAL	Черви
X_GENERAL	Generic X applications

Для каждой группы сигнатур существует три типа IDS, IPS и Policy.