

Пример настройки межсетевого экрана D-Link DFL-860E

В данном документе описаны основные шаги и принципы, которые нужно учитывать при работе с межсетевым экраном **D-Link DFL-860E**. Роутер является достаточно продвинутым для использования в сложных конфигурациях и обладает широкими возможностями. На данном примере хорошо видно как эти возможности можно использовать при одновременном подключении двух провайдеров, один из которых – Beeline (бывшая Корбина), отличающийся нетривиальностью подключения

Последовательность действий:

- 1) Создание адресной книги
- 2) Конфигурирование интерфейсов
- 3) Настройка маршрутизации
- 4) Настройка правил безопасности
- 5) Конфигурирование VPN сервера
- 6) Настройка маршрутизации VPN
- 7) Настройка правил безопасности

1 Устройство сети

Сеть состоит из внутренней сети LAN, Сети DMZ

Снаружи подключено два провайдера. Один провайдер - Corbina (Корбина) или Beeline (Билайн) подключен к интернет через соединение l2tp с получением динамического IP адреса. Второй провайдер ПТН, подключен через ADSL модем с прямым статическим IP адресом.

Необходимо обеспечить выход офисной сети в интернет через канал Корбины, и обеспечить работу внутренних сервисов через второго провайдера ПТН.

Вся сложность в том, что интернет-соединение от Корбины имеет динамические параметры.

Последовательность шагов настройки роутера D-Link DFL-860E

2 Создание адресной книги D-Link DFL-860E

В таблицу адресов вносятся адреса объектов которые взаимодействуют с роутером

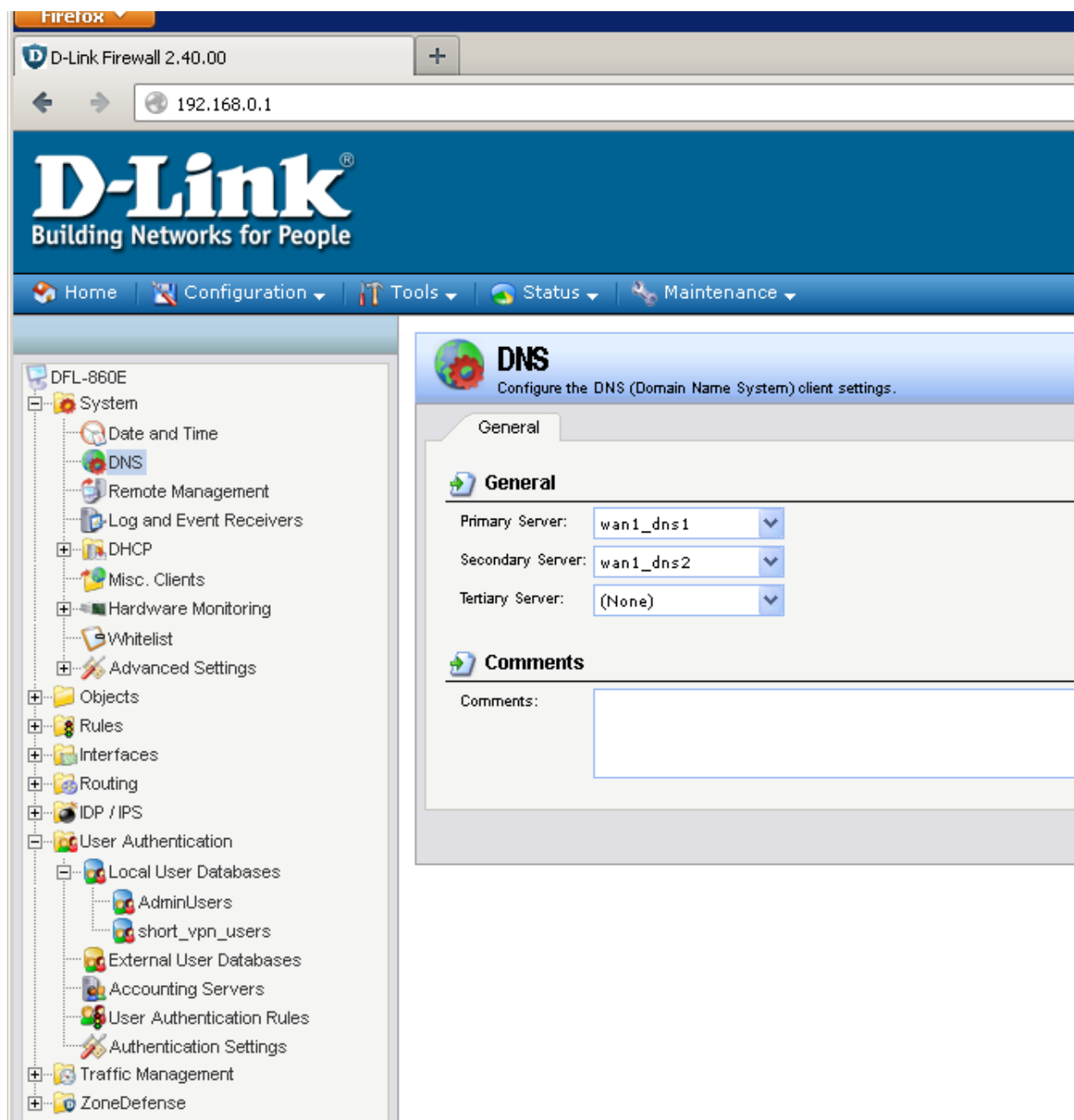
The screenshot shows the D-Link Firewall 2.40.00 web interface. The left sidebar contains a tree view with categories like System, Objects, Rules, Interfaces, Routing, IDP / IPS, User Authentication, Traffic Management, and ZoneDefense. The 'InterfaceAddresses' folder is selected under the 'Objects' category. The main content area displays a table titled 'InterfaceAddresses' with the following data:

#	Name	Address	User Auth Groups	Comments
1	wan1_ip	0.0.0.0		IPAddress of interface wan1
2	wan1net	0.0.0.0/0		The network on interface wan1
3	wan1_gw	0.0.0.0		Default gateway for interface wan1.
4	wan1_dns1	0.0.0.0		Primary DNS server for interface wan1.
5	wan1_dns2	0.0.0.0		Secondary DNS server for interface wan1.
6	wan1_br	0.0.0.0		Broadcast address for interface wan1.
7	lan_ip	192.168.0.1		IPAddress of interface lan
8	lannet	192.168.0.0/24		The network on interface lan
9	dmz_ip	10.1.1.11		IPAddress of interface dmz
10	dmznet	10.1.1.0/24		The network on interface dmz
11	wan2_ip	91.122.137.173		IPAddress of interface wan2
12	wan2net	91.122.0.0/16		The network on interface wan2
13	wan2_gw	91.122.138.1		
14	L2TP_Corb_ip	0.0.0.0		IP address received from L2TP/PPTP client L2TP_Cor...
15	L2TP_Corb_dns1	0.0.0.0		Primary DNS server received from L2TP/PPTP client ...
16	L2TP_Corb_dns2	0.0.0.0		Secondary DNS server received from L2TP/PPTP clien...
17	dmz_mail	10.1.1.10		
18	lan_qnap	192.168.0.8		
19	short_l2tp_server2	10.6.0.1		
20	short_l2tp_pool2	10.6.0.10-10.6.0.100		
21	short_l2tp_server1	10.5.0.1		
22	short_l2tp_pool1	10.5.0.10-10.5.0.100		
23	bobcat	192.168.0.163		
24	short_xman	192.168.0.100		

3 Конфигурирование интерфейсов D-Link DFL-860E

Настройка соединения с интернет-провайдерами

В DNS ничего не меняем. Все адреса будут присвоены провайдером автоматически. Или если во внутренней сети уже существует DNS сервер



Настраиваем интерфейсы. Заходим во вкладку Interfaces-Ethernet

D-Link Firewall 2.40.00

192.168.0.1

D-Link®

Building Networks for People

Home Configuration Tools Status Maintenance

DFL-860E

- System
- Objects
- Rules
- Interfaces
 - Ethernet**
 - VLAN
 - IPsec
 - GRE
 - PPPoE
 - PPTP/L2TP Servers
 - PPTP/L2TP Clients
 - SSL VPN Interface
 - Switch Management
 - Interface Groups
 - ARP/Neighbor Discovery
- Routing

Ethernet

Configure the settings for the Ethernet adapters in the system.

#	Name	IPv4 Address	IPv6 Address	Network	Default Gateway	Enable
1	wan1	wan1_ip		wan1net	wan1_gw	Yes
2	wan2	wan2_ip		wan2net	wan2_gw	No
3	dmz	dmz_ip		dmznet		No
4	lan	lan_ip		lanet		No

Wan1 подключен к Корбине. Адрес получает автоматически.

192.168.0.1

D-Link®

Building Networks for People

Logged in as administrator
admin - 192.168.0.50

Home Configuration Tools Status Maintenance Logout Help

DFL-860E

- System
- Objects
- Rules
- Interfaces
 - Ethernet**
 - VLAN
 - IPsec
 - GRE
 - PPPoE
 - PPTP/L2TP Servers
 - PPTP/L2TP Clients
 - SSL VPN Interface
 - Switch Management
 - Interface Groups
 - ARP/Neighbor Discovery
- Routing
- IDP / IPS
- User Authentication
- Traffic Management
- ZoneDefense

wan1

An Ethernet interface represents a logical endpoint for Ethernet traffic.

General Hardware Settings Advanced

General

Name: wan1

IP address: wan1_ip

Network: wan1net

Default Gateway: wan1_gw

Receive Multicast Traffic: Auto

☒ Enable DHCP Client

Enabling the DHCP Client will create and use the objects <interface name>.dns1 and <interface name>.dns2 as the DNS objects. Objects that are needed by the DHCP client and don't exist in the Address Book will be created, all objects used by the DHCP client will be set to '0.0.0.0' and dynamically updated.

DHCP Host Name: Optional DHCP Host Name. Leave blank to use default name.

☐ Enable transparent mode

IPv6

☐ Enable IPv6

IP address: (None)

Network: (None)

Default Gateway: (None)

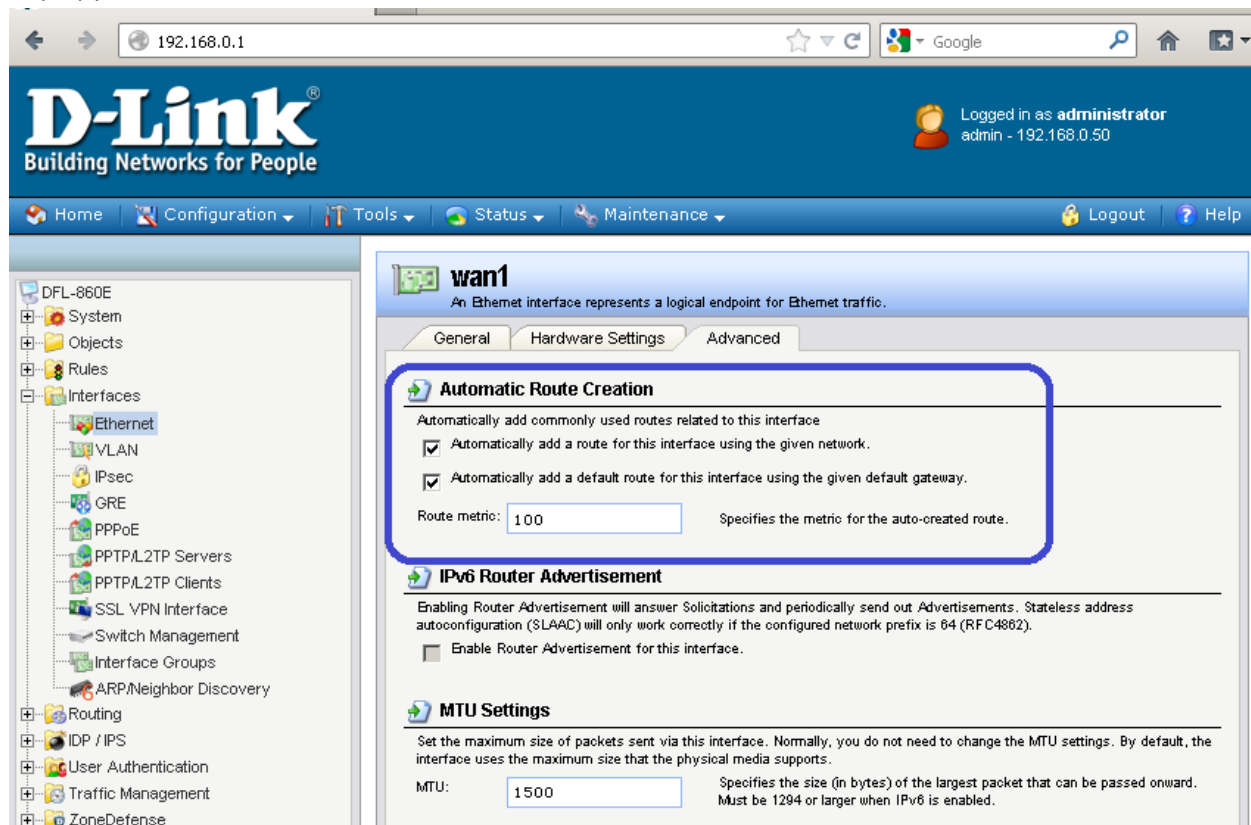
Comments

Comments:

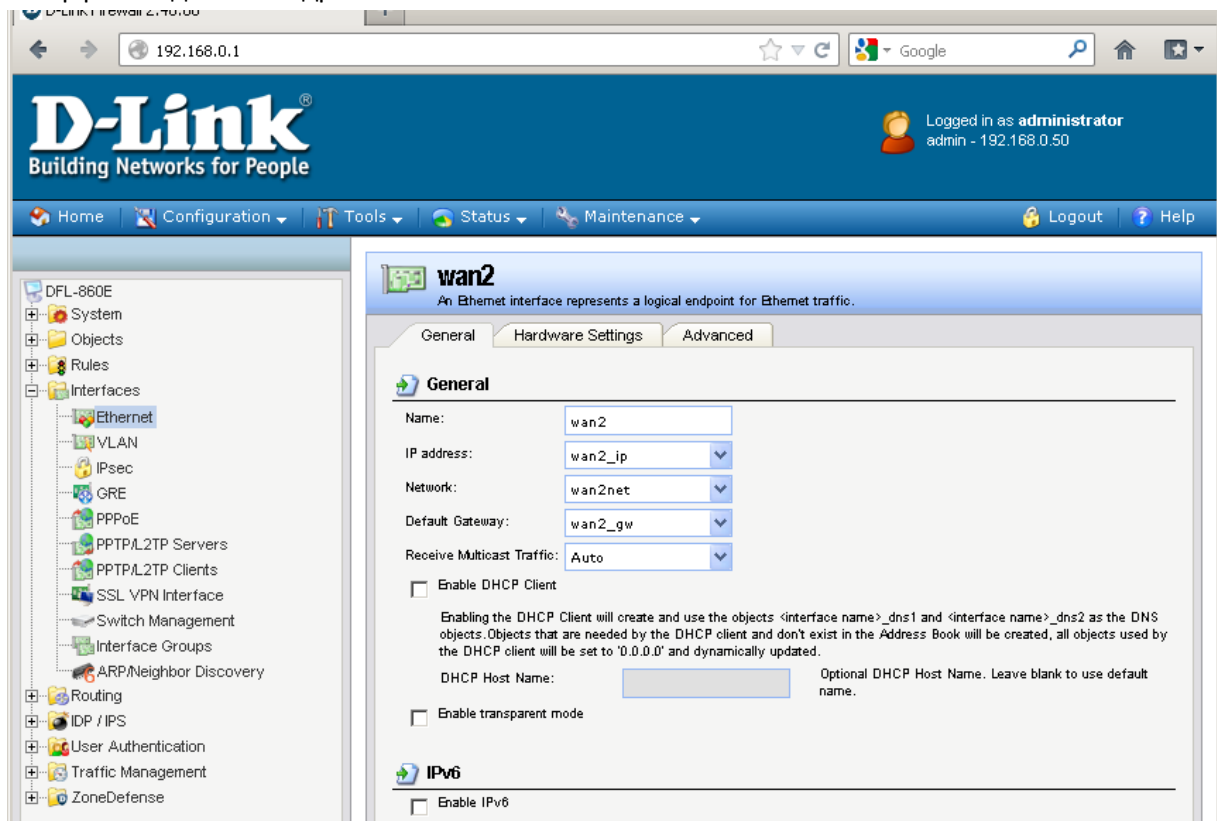
OK Cancel

Вкладка Hardware по умолчанию

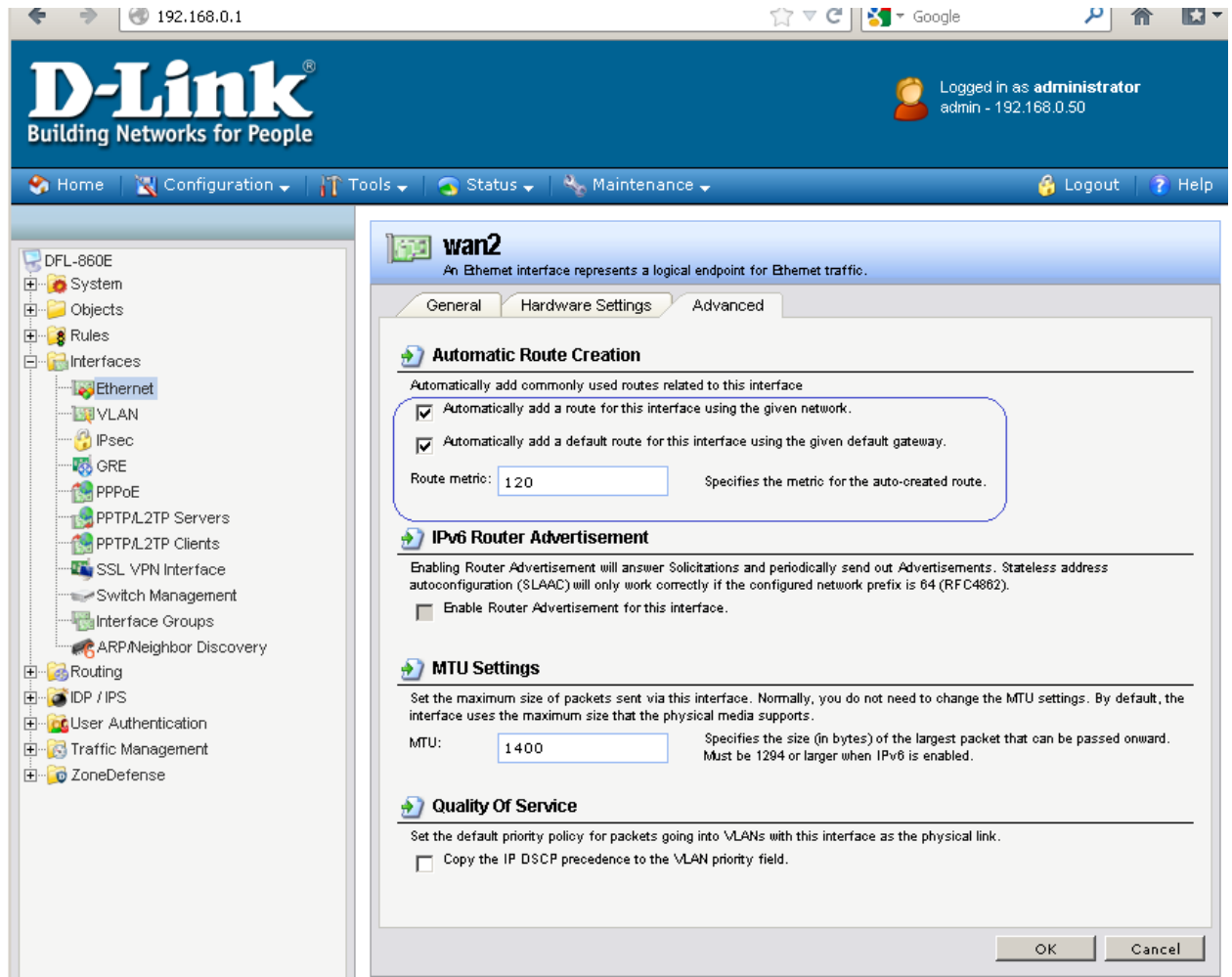
Во вкладке Advanced проверяем назначение метрики, и автоматическое добавление маршрутов



WAN2 подключен к ПТН, через ADSL модем, который работает в режиме моста. Адреса на этот интерфейс задаются в адресной книге



Если этот интерфейс у нас является вспомогательным, то весь трафик по умолчанию идет через Корбину, то на него необходимо прописать метрику больше чем для интерфейса Wan1. Надо отметить, что в сложном маршрутизаторе маршрут по умолчанию всегда должен быть один. У основного маршрута всегда метрика должна быть меньше чем у других. Одинаковые метрики для маршрута по умолчанию ведут к раздвоению пакетов и неработоспособности многих сервисов.



Корбина известна своим геморройным подключением через сервис L2TP в PPTP. Для этого идем в PPTP/L2TP Clients и настраиваем соединение. Для того что бы интерфейс получил правильные адреса и таблицу маршрутизации необходимо правильно прописать удаленный хост. Дело в том, что у Корбины адрес хоста определяется автоматически. Прописываем туда следующую запись: DNS:internet.beeline.ru. Достоинство данного роутера в том, что он может разрешать адрес удаленного хоста. К сожалению, не все роутеры, даже продвинутые имеют такую настройку.

D-Link®
Building Networks for People

Logged in as **administrator**
admin - 192.168.0.50

Home Configuration Tools Status Maintenance Logout Help

L2TP_Corb
A PPTP/L2TP client interface is a PPP (Point-to-Point Protocol) tunnel over an existing IP network. Its IP address and DNS servers are dynamically assigned.

General Security Dial-on-demand Advanced

General

Name: L2TP_Corb

Tunnel Protocol: L2TP

Remote Endpoint: dns:tp.internet.beel

Remote Network: all-nets

Authentication

Username: [REDACTED]

Password: [REDACTED]

Confirm Password: [REDACTED]

Note! Existing passwords will always be shown with 8 characters to hide the actual length.

Comments

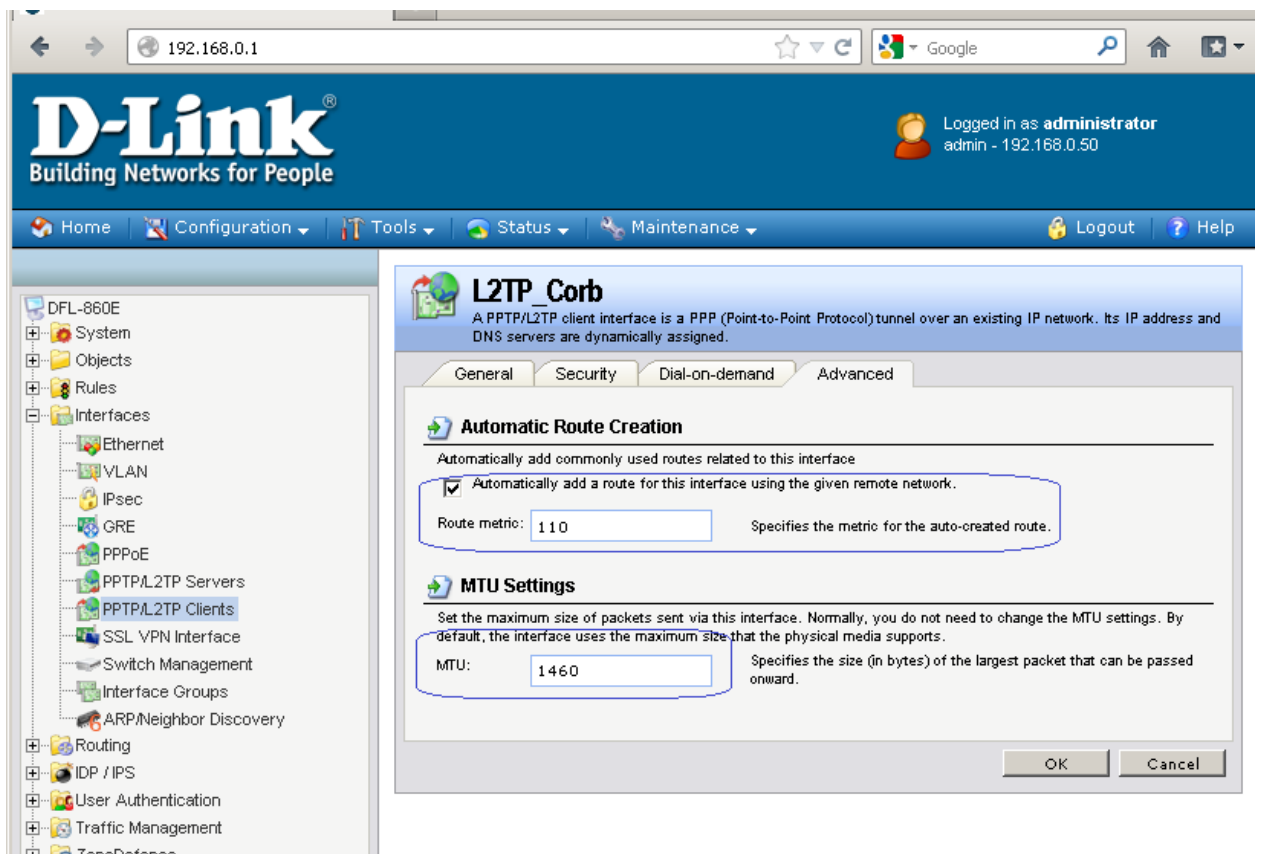
Comments: [REDACTED]

OK Cancel

Во вкладке Security почти ничего не меняем, а во вкладку Advanced прописываем метрику и MTU

С метрикой надо поподробнее:

Из текущих настроек наименьшую метрику имеет интерфейс WAN1 значение - 100. А L2tp-client имеет значение 120. Т.е весь трафик по прежнему будет идти во внутреннюю сеть Корбины. А нам нужно, чтобы весь трафик из внутренней сети шел уже через новое L2TP-соединение. Установить метрику L2TP-Клиента меньше чем на WAN1 мы не можем, потому, что тогда интерфейс от Корбины не получит настройки и таблицу маршрутизации и L2TP-соединение не установится. Поэтому метрика изначально ставится больше. Когда интерфейс L2TP получит все адреса и туннель будет установлен, тогда таблицу маршрутизации можно будет менять динамически. Для этого и будут использоваться динамические правила маршрутизации.

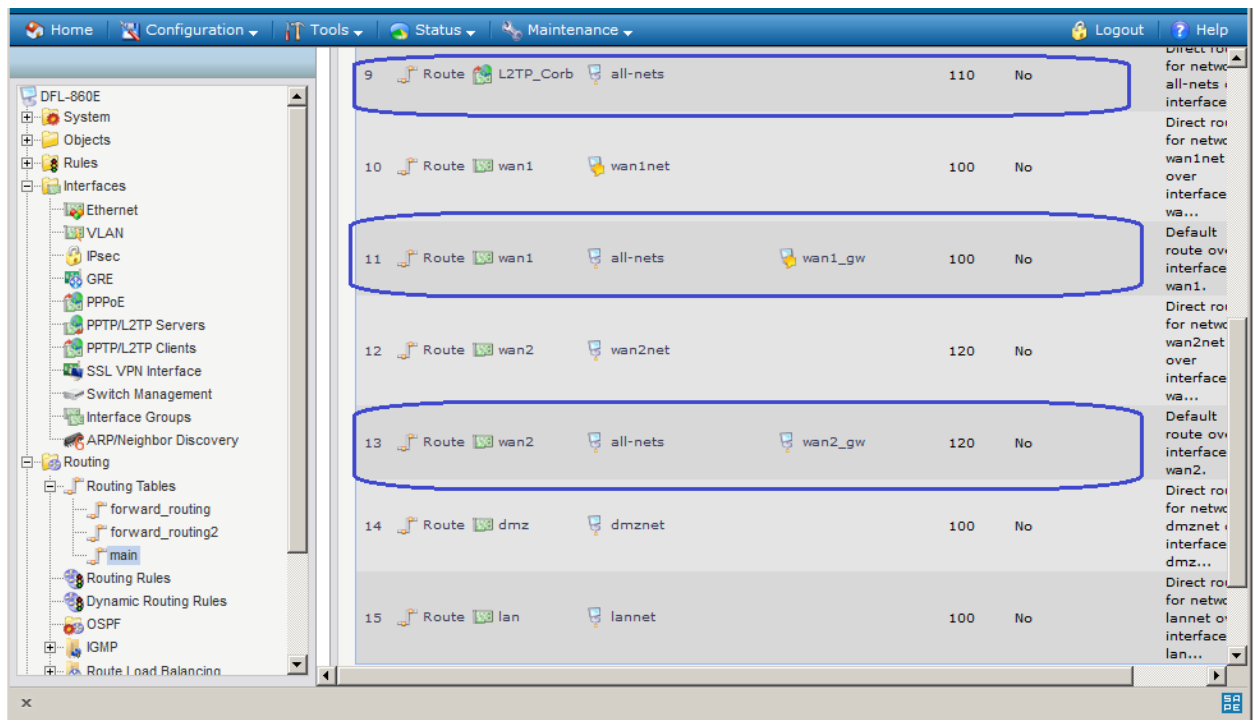


Обратим внимание, на метрику на интерфейсе L2tp -110, которая больше метрики на wan1 -100

Весь трафик идет через wan1, во внутреннюю сеть Корбины. Следующий пункт делает возможным направление интернет трафика из внутренней сети в установившееся l2tp соединение

4 Настройка таблиц динамической маршрутизации для правильного направления трафика D-Link DFL-860E

Смотрим основную таблицу:



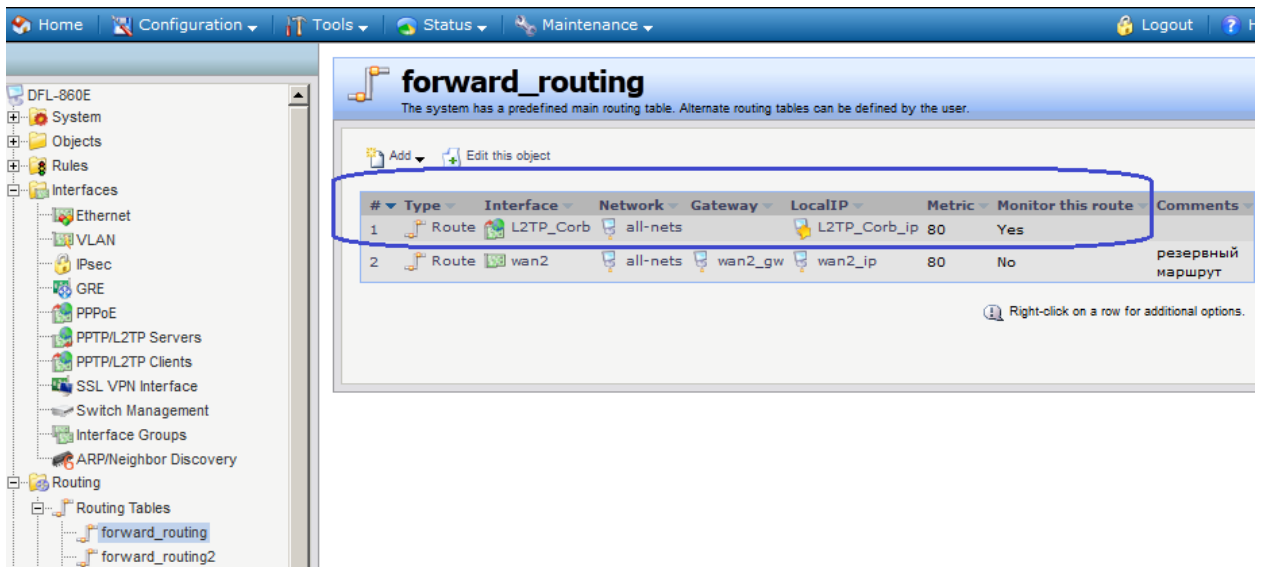
Как видим есть 3 маршрута с разными метриками. Основной маршрут с метрикой 100

Маршрут в интернет соединение Корбины L2TP с метрикой 110

Запасной маршрут в ПТН с метрикой 120

Задача трафик из внутренней сети Lan пустить через l2tp канал Корбины

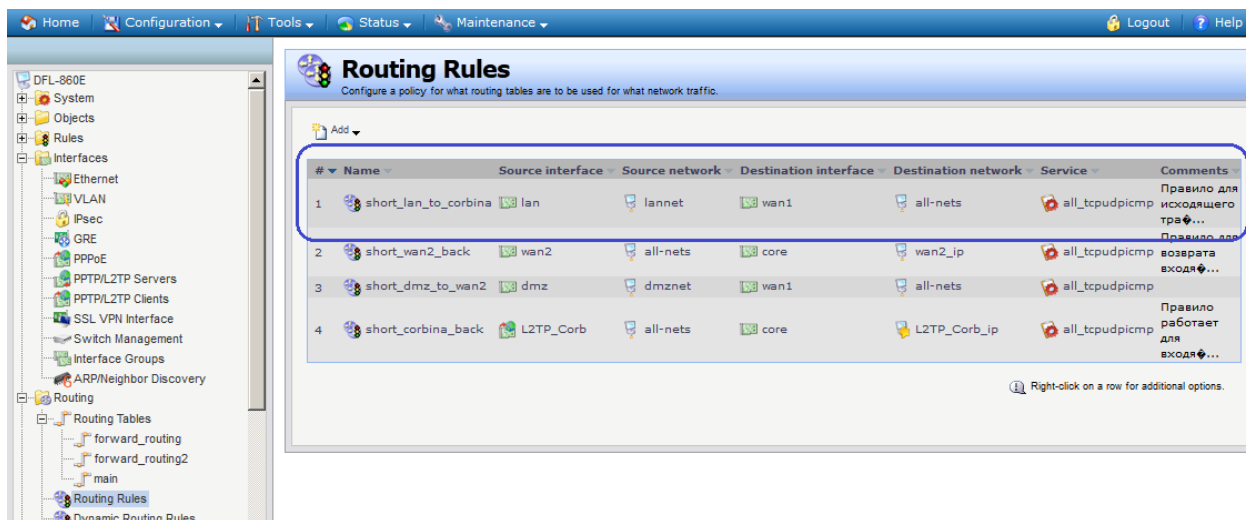
Создаем для этого еще одну таблицу маршрутизации forward_routing



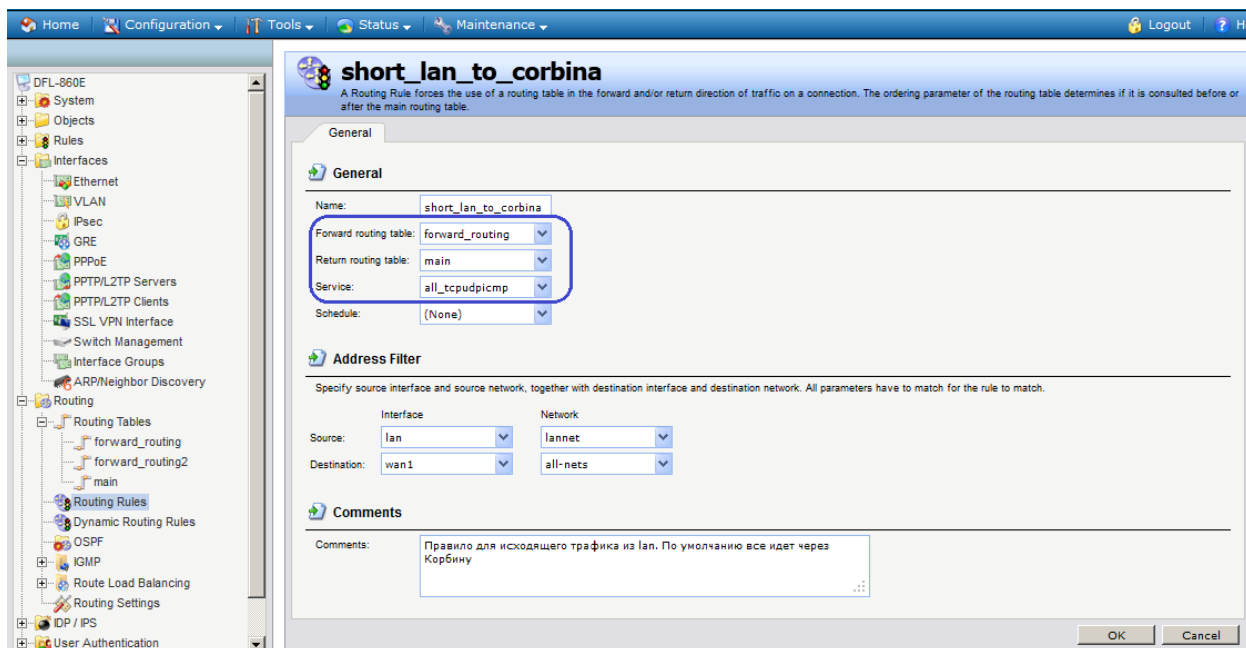
В этой таблице запись 1 - маршрут всего трафика через интерфейс L2TP с метрикой 80. Включаем мониторинг маршрута. Когда этот маршрут становится не доступен, то начинает работать запись 2, которая пускает весь трафик в интерфейс wan2 через запасной канал ПТН

А теперь самое интересное

Идем в раздел Routing Rules и создаем правила для таблиц маршрутизации

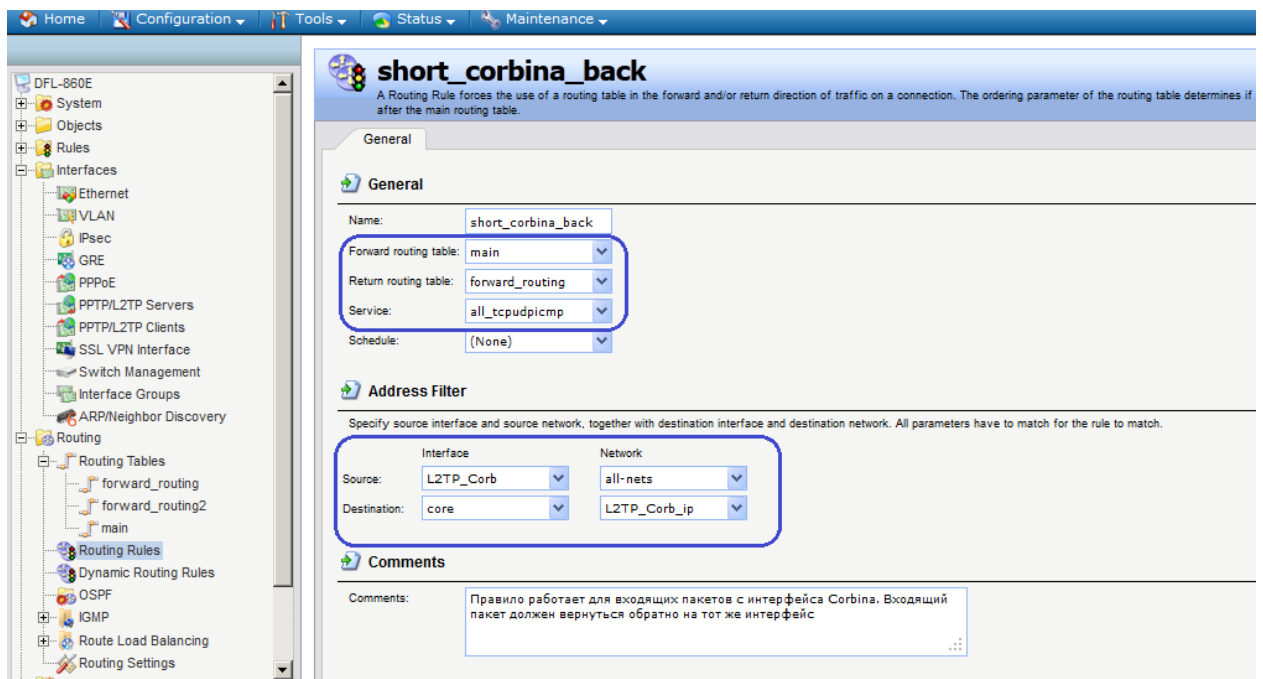


Правило 1- short_lan_to_corbina дает возможность динамического применения таблицы маршрутизации

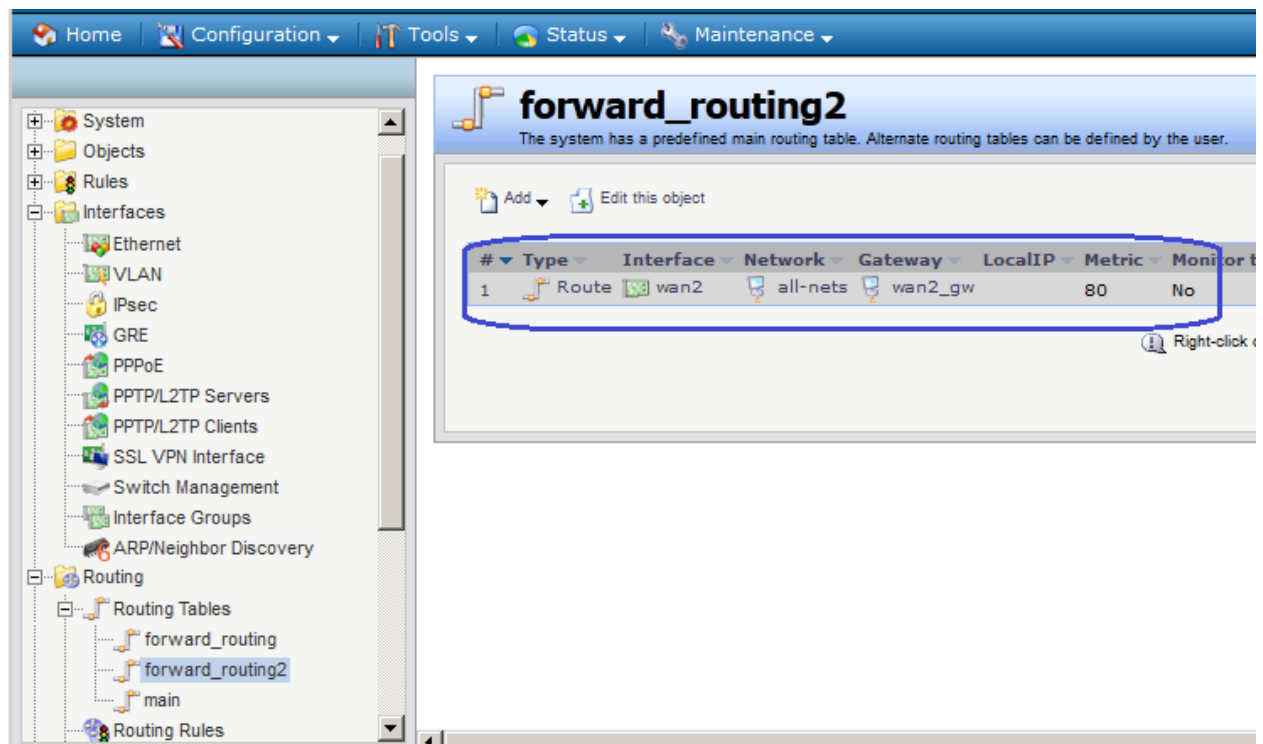


В случае если источник находится в сети Lan и направляется согласно метрике в основной таблице в Wan1, к нему применяются таблицы маршрутизации forward_routing, которая направляет его в интерфейс L2TP. Для приходящих обратно пакетов работает таблица main

Для того чтобы наружу могли работать внутренние сервисы, необходимо создать еще одно правило: short_corbina_back, согласно которому, входящие пакеты приходящие на интерфейс L2tp_corb должны направляться согласно основной таблице main, а возвращаться согласно той же таблицы forward_routing

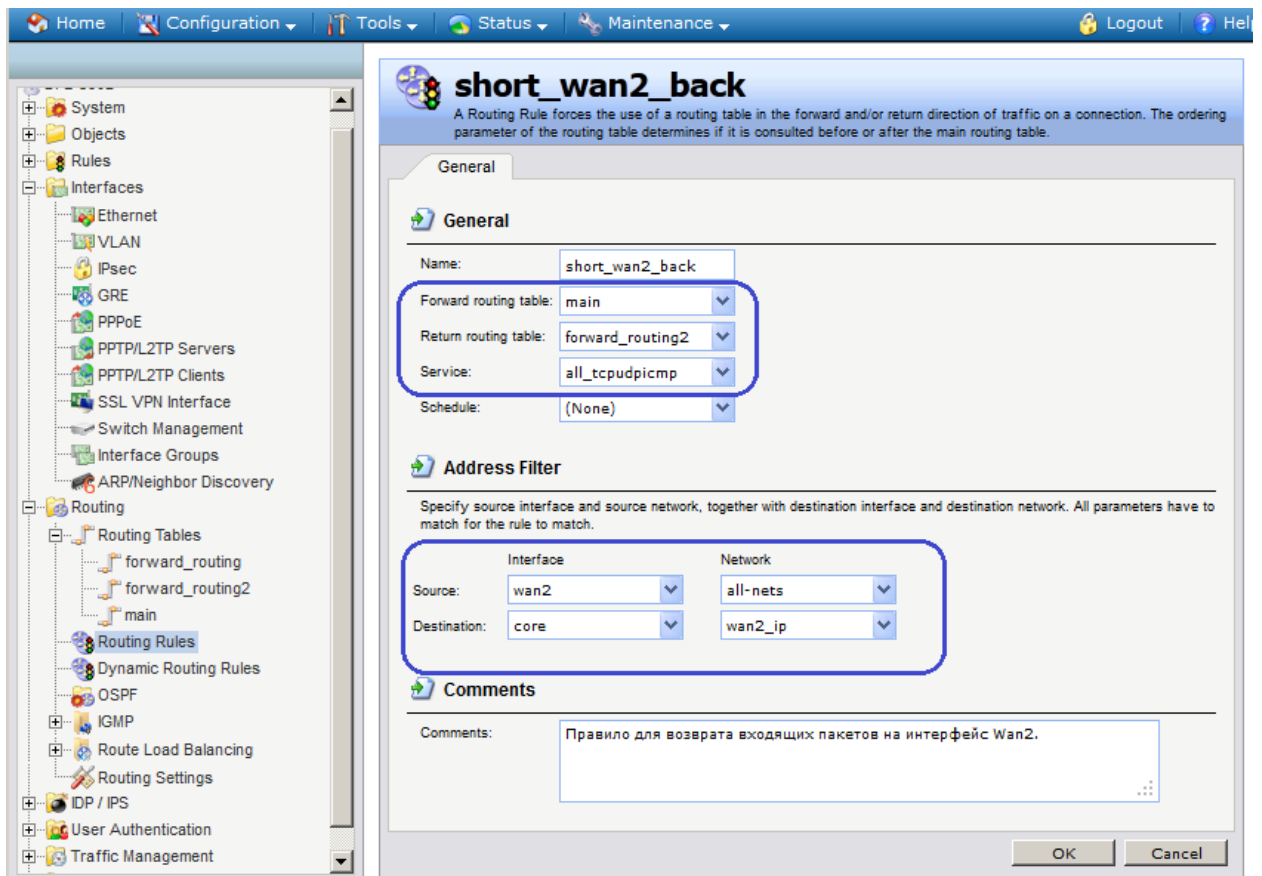


Для того что бы через интерфейс wan2 можно было раздавать сервисы из внутренней сети в интернет необходимо создать динамическое правило для входящих пакетов. Сначала создается дополнительная таблица маршрутизации forward_routing2



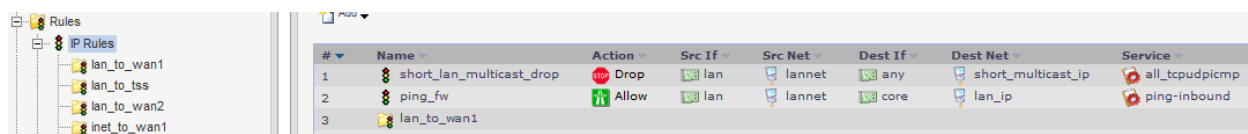
В ней создается маршрут по умолчанию с метрикой 80 для интерфейса wan2

Для того чтобы входящие пакеты с интерфейса wan2 могли попасть во внутреннюю сеть и выйти обратно через тот же интерфейс wan2 необходимо создать еще одно правило: short_wan2_back

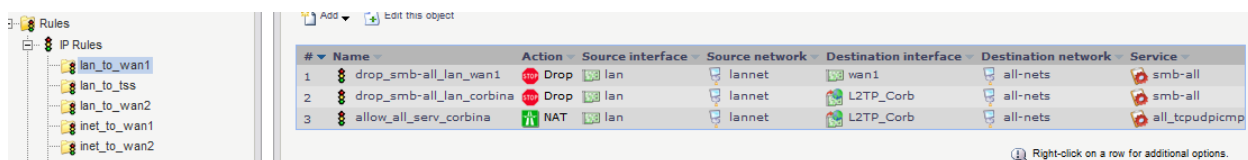


Согласно этому правилу, входящий пакет с интерфейса wan2 разгуживается согласно основной таблицы маршрутизации main, а обратный пакет направляется согласно таблицы forward_routing2. Таким образом можно заставить правильно работать, например, web-сайт, который находится во внутренней сети через запасной канал wan2. Пакеты будут правильно приходить и уходить через один и тот же интерфейс.

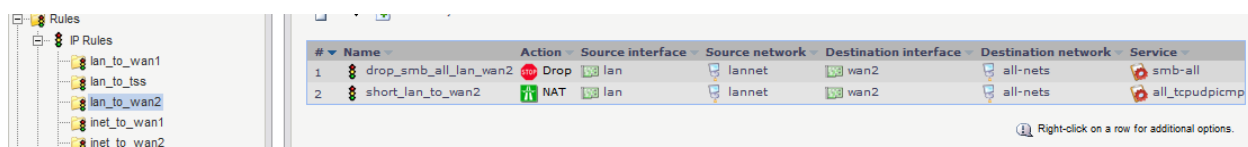
5 Настройка правил безопасности D-Link DFL-860E



Правило 2 разрешает пинг маршрутизатора из локальной сети



Правило 3 в данной папке включает NAT от интерфейса L2TP Корбины во внутреннюю сеть



Правило 2 в данной папке включает NAT через интерфейс второго провайдера во внутреннюю сеть

#	Name	Action	Source interface	Source network	Destination interface	Destination network	Service
1	short_allow_ping_corbina	Allow	L2TP_Corb	all-nets	core	L2TP_Corb_ip	all_icmp
2	short_wan1_ftp_sat	SAT	L2TP_Corb	all-nets	core	L2TP_Corb_ip	short_ftp
3	short_wan1_ftp_allow	Allow	any	all-nets	core	L2TP_Corb_ip	short_ftp
4	short_wan1_ftp_sat_1	SAT	L2TP_Corb	all-nets	core	L2TP_Corb_ip	short_ftp_qnap_passive
5	short_wan1_ftp_allow_1	Allow	any	all-nets	core	L2TP_Corb_ip	short_ftp_qnap_passive
6	short_corbina_nat	NAT	L2TP_Corb	all-nets	core	L2TP_Corb_ip	all_tcpudpicmp

(1) Right-click on a row for additional options.

Правило 1 в данной папке позволяет пинговать внешний IP адрес L2TP интерфейса

Правило 2-5 проброс сервиса ftp из внутренней сети через интерфейс L2TP Корбины в интернет

Правило 6 включает преобразование адресов NAT на интерфейсе L2TP Корбины

#	Name	Action	Source interface	Source network	Destination interface	Destination network	Service
1	short_allow_ping_wan2	Allow	any	all-nets	core	wan2_ip	all_icmp
2	short_http_sat_to_dmz	SAT	wan2	all-nets	core	wan2_ip	http
3	short_allow_http_to_wan2	Allow	any	all-nets	core	wan2_ip	http-all
4	short_smtp_sat_dmz	SAT	wan2	all-nets	core	wan2_ip	smtp
5	short_allow_smtp_to_wan2	Allow	any	all-nets	core	wan2_ip	smtp
6	short_pop3_sat_dmz	SAT	wan2	all-nets	core	wan2_ip	pop3
7	short_allow_pop3_to_wan2	Allow	any	all-nets	core	wan2_ip	pop3
8	short_jabber_sat_dmz	SAT	wan2	all-nets	core	wan2_ip	short_xmpp-client
9	short_allow_jabber_to_wan2	Allow	any	all-nets	core	wan2_ip	short_xmpp-client
10	short_jabber1_sat_dmz	SAT	wan2	all-nets	core	wan2_ip	short_openfire
11	short_allow_jabber1_to_wan2	Allow	any	all-nets	core	wan2_ip	short_openfire
12	short_jabber3_sat_dmz	SAT	wan2	all-nets	core	wan2_ip	short_xmpp-client1
13	short_allow_jabber3_to_wan2	Allow	any	all-nets	core	wan2_ip	short_xmpp-client1
14	short_all_nat_wan2	NAT	wan2	all-nets	core	wan2_ip	all_tcpudpicmp

Правило 1-13 проброс внутренних сервисов через интерфейс WAN2 второго провайдера в интернет

Правило 14 включает преобразование адресов NAT на интерфейсе WAN2 второго провайдера

6 Конфигурирование VPN сервера D-Link DFL-860E

Данный маршрутизатор можно использовать как L2TP –Сервер для подключения удаленных пользователей через защищенное соединение по протоколу IPSEC.

Заходим в Authentication Objects

Создаем новый Preshared key

General

General

Name:

Shared Secret

☒ Passphrase

Shared Secret: Note! Existing secret will always be shown with 8 characters to hide the actual length.

Confirm Secret:

A PSK containing non-ASCII characters might be encoded differently on other systems and cause a mismatch, e.g. Windows uses UTF-16 while CorePlus uses UTF-8.

☐ Hexadecimal key

Passphrase:

Generate Random Key

Since regular words and phrases are vulnerable to dictionary attacks, do not use them as shared secrets.

Comments

Comments:

OK

Cancel

Заходим в interfaces/IPSec и создаем новый интерфейс

D-Link Firewall 2.40.00 - Mozilla Firefox

Файл Правка Вид Журнал Закладки Инструменты Справка

Aqua Computer ... YCH++ Онлайн... бизнес форум ... Бизнес форум ... Кто автор выск... Контакты Реестр ПТО Входящие - sle... GLPI - Компьют... D-Link Firewa... x

10.6.0.1

SEO ссылки

Поиск

D-Link®
Building Networks for People

Logged in as administrator
admin - 10.6.0.22

Home Configuration Tools Status Maintenance Logout Help

IPsec
Manage the IPsec tunnel interfaces used for establishing IPsec VPN connections to and from this system.

Add Advanced Settings

#	Name	Local Net	Remote Net	Remote Endpoint	Auth	Comments
1	TSS_tunnel	lanet	TSS_net	TSS_vpn_endpoint	PSK	
2	short_ipsec_wan2_transport	wan2_ip	all-nets		PSK	
3	short_ipsec_wan1_transport	L2TP_Corb_ip	all-nets		PSK	

Right-click on a row for additional options.

DFL-860E

- System
 - Date and Time
 - DNS
 - Remote Management
 - Log and Event Receivers
 - DHCP
 - DHCP Servers
 - DHCP Relays
 - Misc. Clients
 - Hardware Monitoring
 - Whitelist
- Advanced Settings
- Objects
 - Address Book
 - ALG with AV/WCF
 - Services
 - IP Pools
 - NAT Pools
 - Schedules
 - Authentication Objects
 - VPN Objects
 - HTTP Banner Files
- Rules
- Interfaces
 - Ethernet
 - VLAN
 - IPsec
 - GRE
 - PPPoE
 - PPTP/L2TP Servers
 - PPTP/L2TP Clients
 - SSL VPN Interface
 - Switch Management
 - Interface Groups
 - ARP/Neighbor Discovery
- Routing
- IDP / IPS
- User Authentication
- Traffic Management
- ZoneDefense

Вкладка General

short_ipsec_wan2_transport
An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

General Authentication XAuth Routing IKE Settings Keep-alive Advanced

General

Name: short_ipsec_wan2_tra
 Local Network: wan2_ip
 Remote Network: all-nets
 Remote Endpoint: (None)
 Encapsulation mode: Both
 IKE Config Mode Pool: (None)

Algorithms

IKE Algorithms: Medium
 IKE Lifetime: 28800 seconds
 IPsec Algorithms: Medium
 IPsec Lifetime: 3600 seconds
 IPsec Lifetime: 0 kilobytes

Comments

Comments:

OK Cancel

Вкладка Authentication. Выбираем Preshared key который мы создали ранее

General Authentication XAuth Routing IKE Settings Keep-alive Advanced

Authentication

X.509 Certificate

Root Certificate(s)

Available: HTTPSAdminCert
 Selected:

Gateway certificate: (None)
 Identification list: (None)

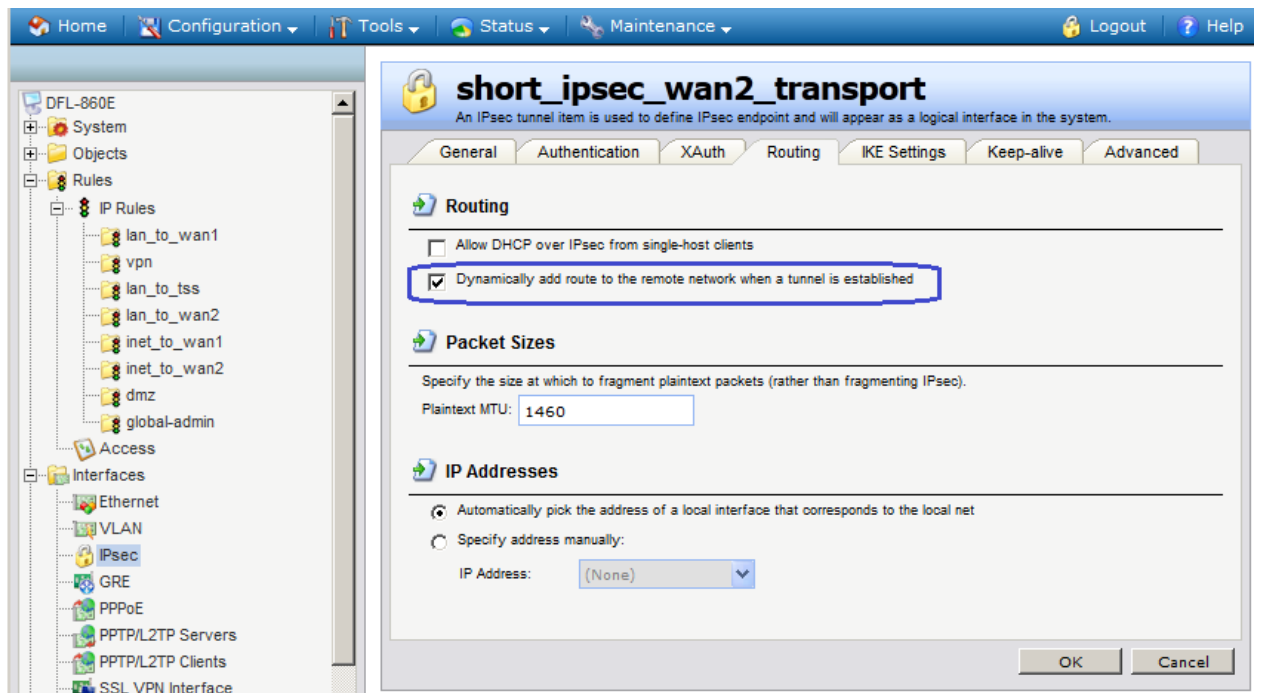
☒ Pre-shared Key
 Pre-shared key: short_wan2_prekey Selects the Pre-shared key to use with this IPsec Tunnel.

Local ID

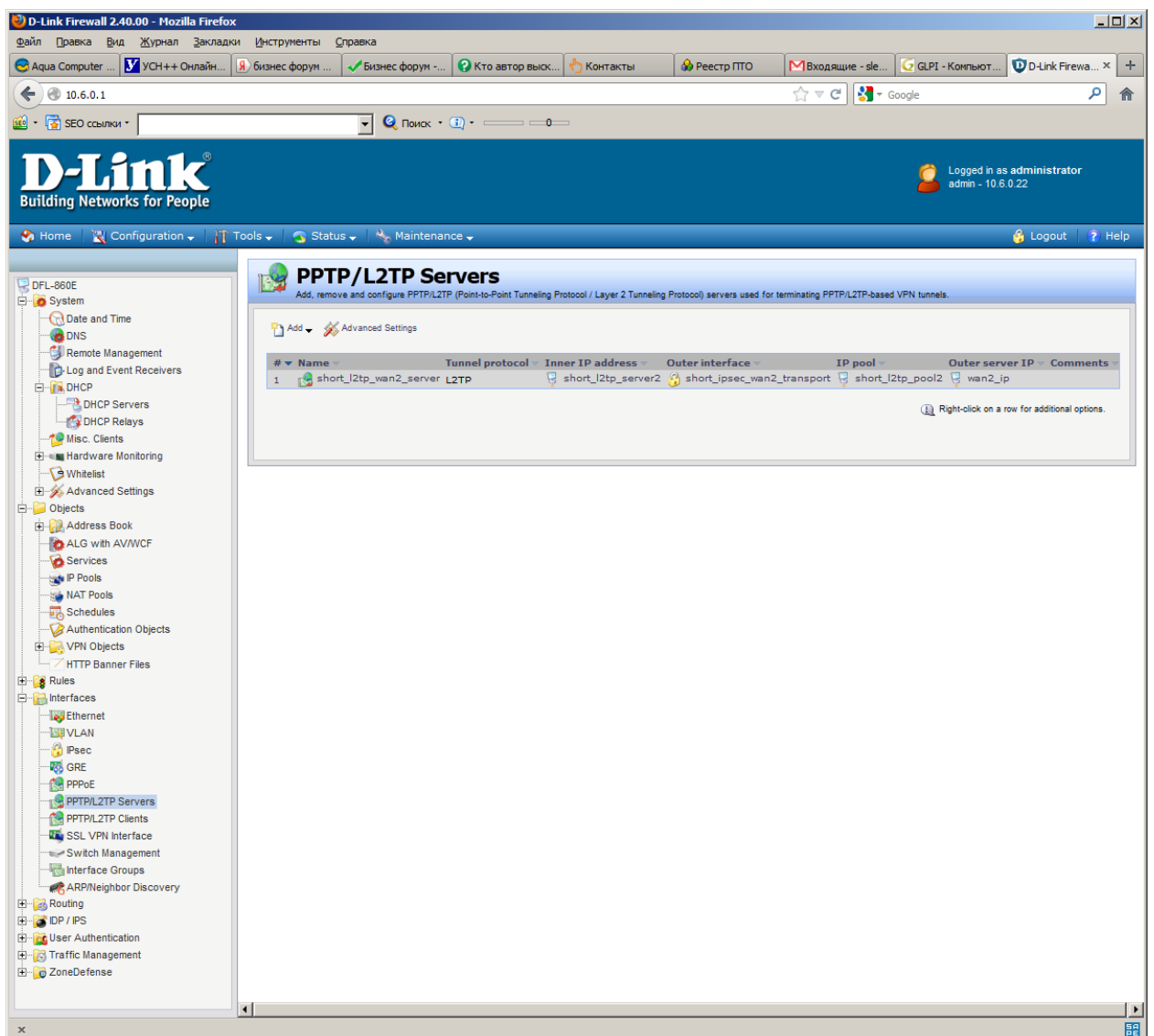
Local ID Type: Auto
 Local ID Value:

OK Cancel

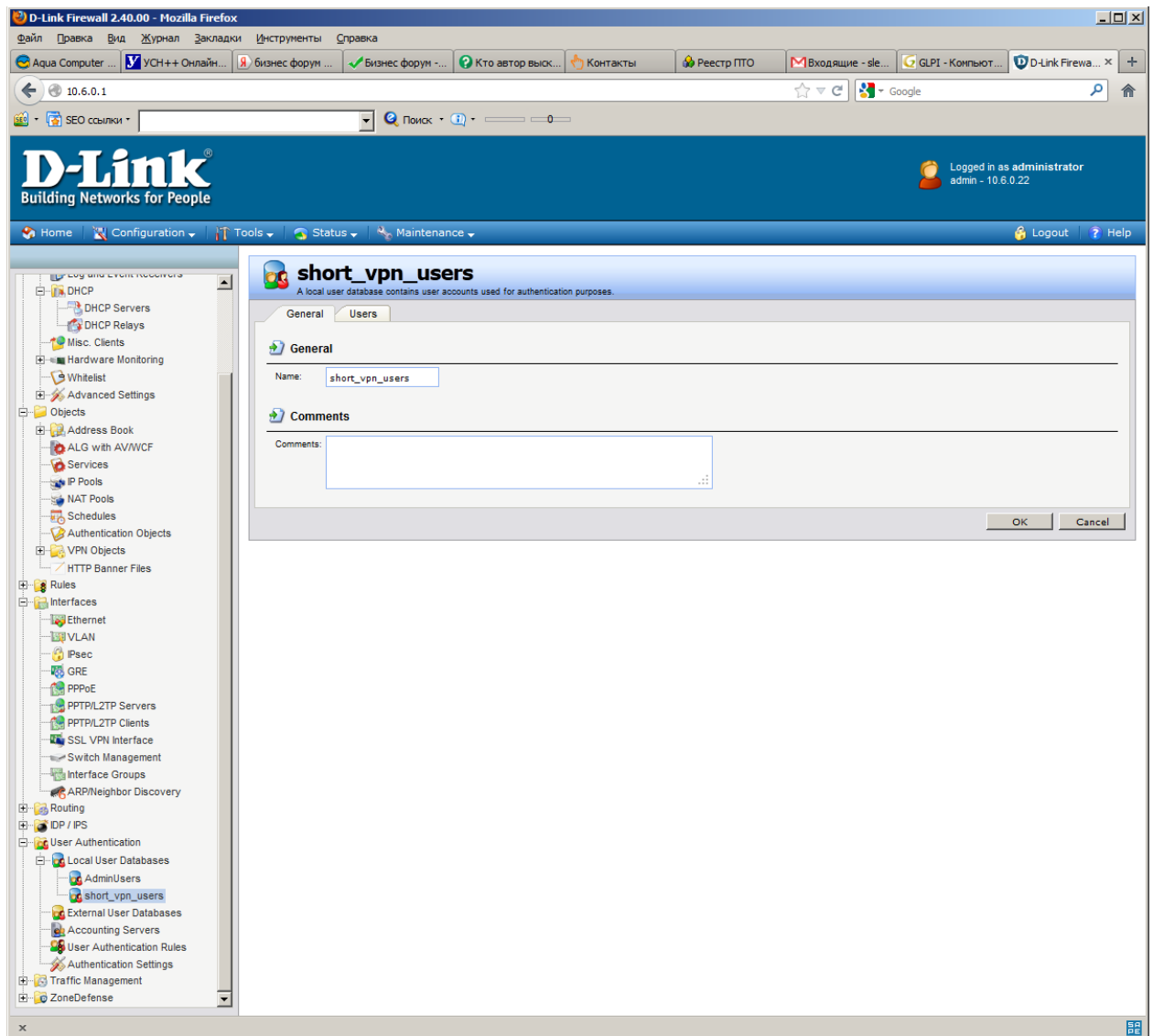
Во вкладке Routing отмечаем автоматическое добавление маршрута



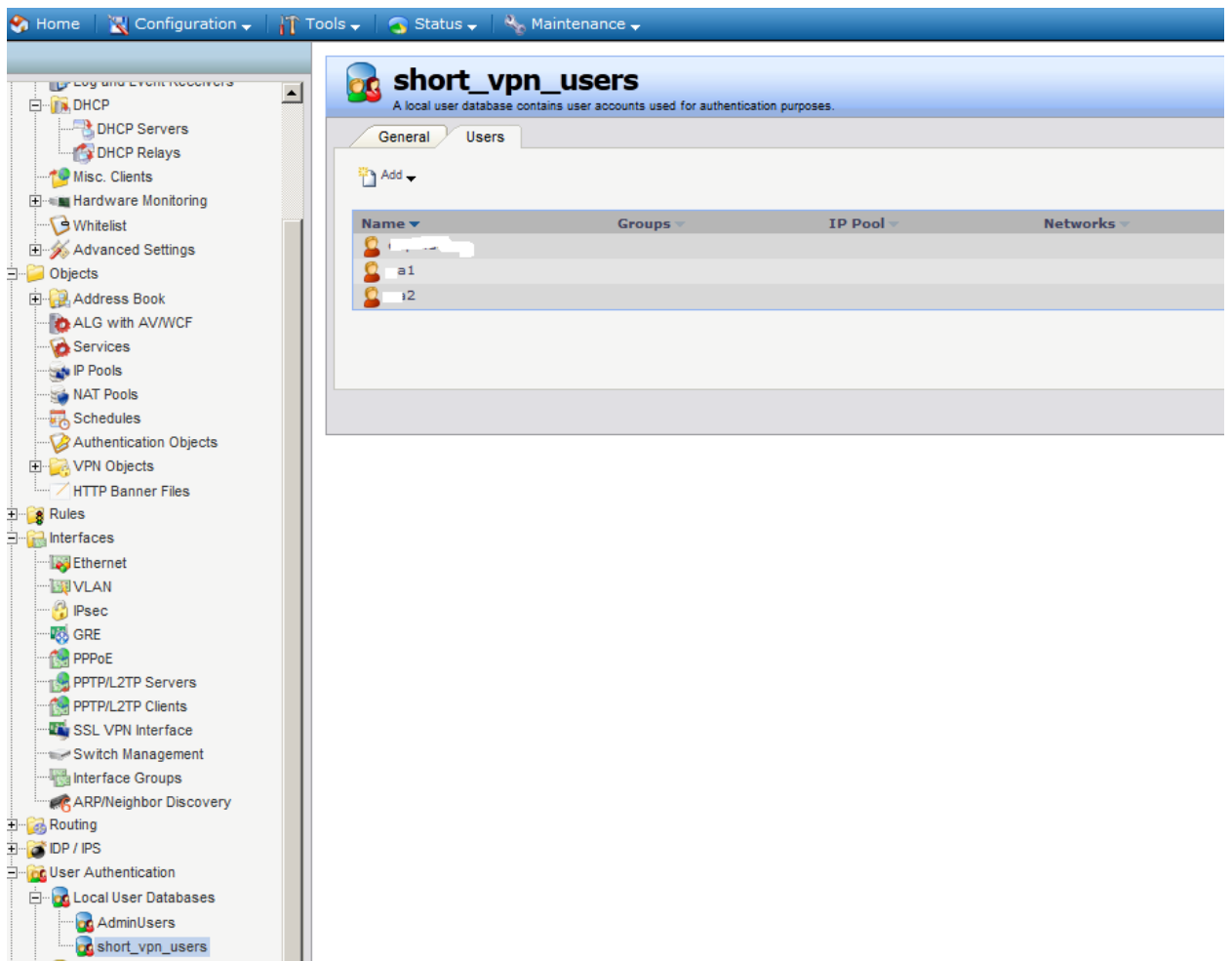
Заходим в меню PPTP/L2TP Servers и добавляем новый сервер



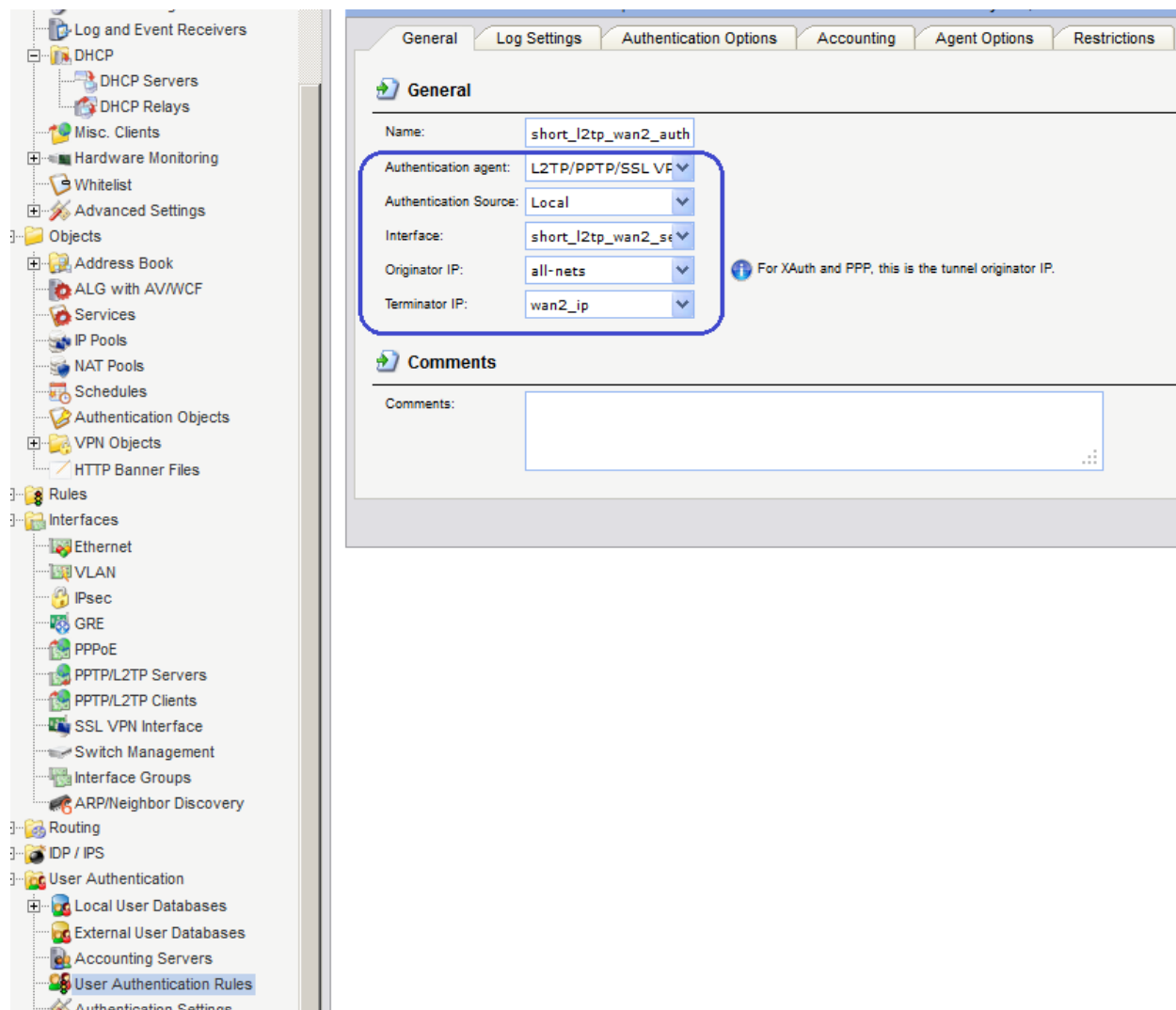
Заходим в User Authentication/ Local User Databases и создаем базу для удаленных пользователей



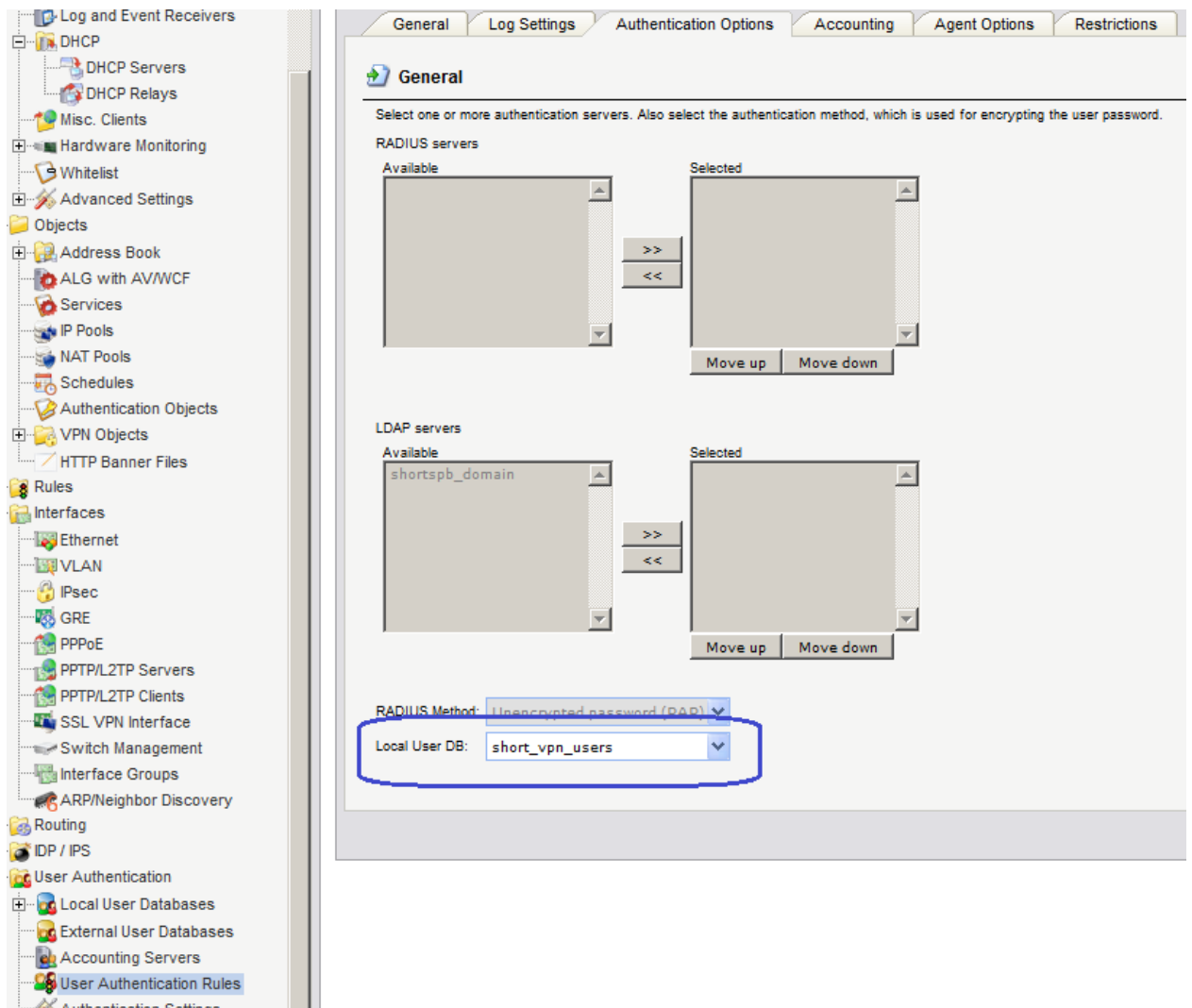
После чего создам самих удаленных пользователей



Идем в User Authentication /User Authentication Rules и создаем правило аутентификации.
Привязываемся там ко всем объектам, которые мы создали ранее



Во вкладке Authentication Options выбираем базу данных для удаленных пользователей.



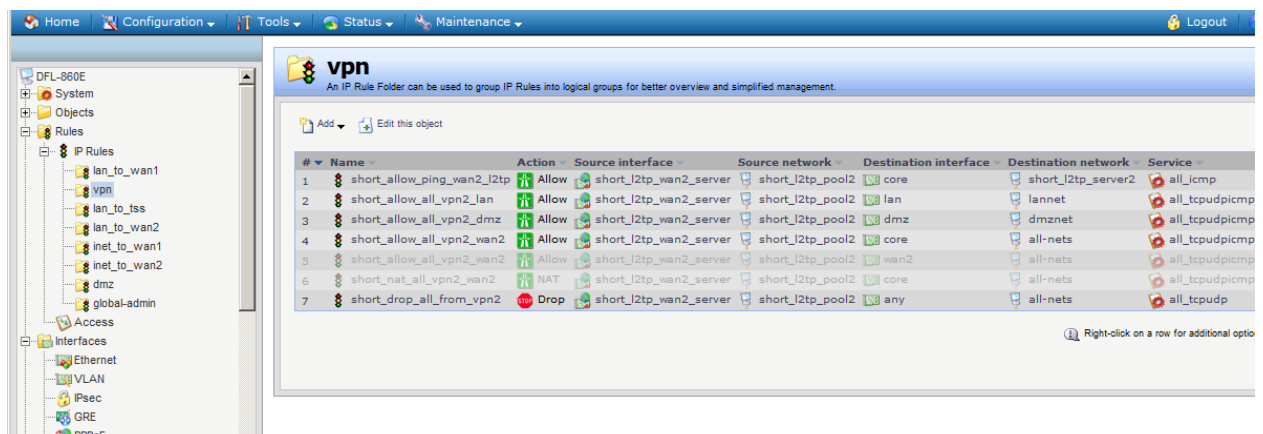
7 Настройка маршрутизации для VPN . D-Link DFL-860E

При установке канала в основную таблицу маршрутизации автоматически добавляются интерфейсы VPN подсети. Основная задача – это разрешить трафик туда, куда нужно

8 Настройка правил безопасности D-Link DFL-860E

Разрешаем хождение трафика во внутреннюю сеть и в сеть DMZ

При желании можно правила ужесточить и назначить только специфические сервисы



Все пожелания по данному документу прошу направлять Егорову Ярославу – инженеру Компании «Глобал-Админ»

Контакты на сайте www.globaladmin.ru

Любое использование материалов данной статьи разрешаются с указанием автора и ссылкой на источник www.globaladmin.ru