



Лабораторные работы по курсу «Основы сетевой безопасности»

Часть 2: Технологии туннелирования

Расширенный курс D-Link

Москва, 2014

Оглавление

ЛАБОРАТОРНЫЙ ПРАКТИКУМ.....	3
Технологии туннелирования.....	3
Лабораторная работа 1. Соединение двух локальных сетей GRE-туннелем	3
Лабораторная работа 2. Соединение двух локальных сетей протоколом IPSec в туннельном режиме, аутентификация с использованием общего секрета	15
Лабораторная работа 3. Использование аутентификации по стандарту XAuth в протоколе IPSec	27
Лабораторная работа 4. Соединение двух межсетевых экранов протоколом IPSec в транспортном режиме, аутентификация с использованием общего секрета	35
Лабораторная работа 5. Использование преобразования NAT в протоколе IPSec.....	39
Лабораторная работа 6. Использование протокола DPD в протоколе IPSec	42
Лабораторная работа 7. Соединение двух локальных сетей протоколом L2TP, аутентификация с использованием общего секрета	45
Лабораторная работа 8. Соединение двух локальных сетей протоколом GRE/IPSec в транспортном режиме	56
Лабораторная работа 9. Соединение двух локальных сетей протоколом L2TP/IPSec в транспортном режиме	63
Лабораторная работа 10. Соединение двух локальных сетей протоколом L2TP/IPSec в транспортном режиме, для одной из локальных сетей используется NAT	77
Аутентификация и хранение учетных записей	82
Лабораторная работа 11. Использование локальной БД для хранения учетных записей.....	82
Лабораторная работа 12. Использование сервера RADIUS для хранения учетных записей..	85
Лабораторная работа 13. Использование сервера LDAP/MS AD для хранения учетных записей	94
Лабораторная работа 14. Аутентификация доступа к ресурсам с использованием браузера	103

Лабораторный практикум

Технологии туннелирования

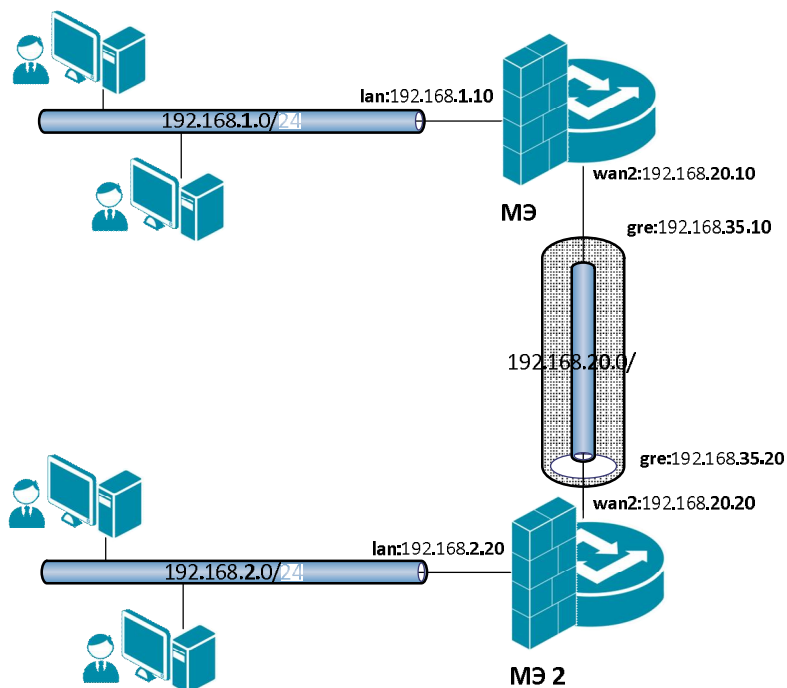
Лабораторная работа 1. Соединение двух локальных сетей GRE-туннелем

Цель

Соединить две локальные сети, каждая из которых расположена за своим межсетевым экраном, туннелем с использованием GRE-протокола.

1. Обе локальные сети знают IP-адреса друг друга.
2. Одна из локальных сетей находится за NAT.

Топология сети



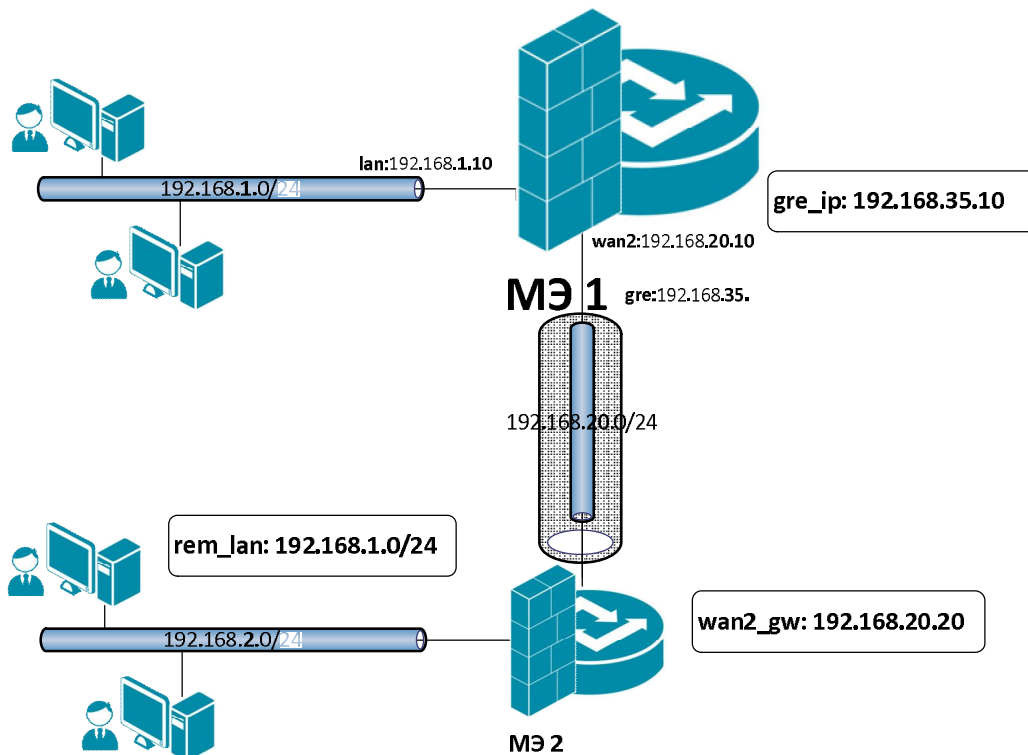
Между интерфейсами `wan2` на МЭ 1 и МЭ 2 требуется поднять GRE-туннель.

Описание практической работы

Создать статическую маршрутизацию и политики доступа, которые разрешают доступ между удаленными локальными сетями. При этом трафик между МЭ 1 и МЭ 2 проходит по GRE-туннелю.

Обе локальные сети знают IP-адреса друг друга

Межсетевой Экран 1



Объекты Адресной Книги

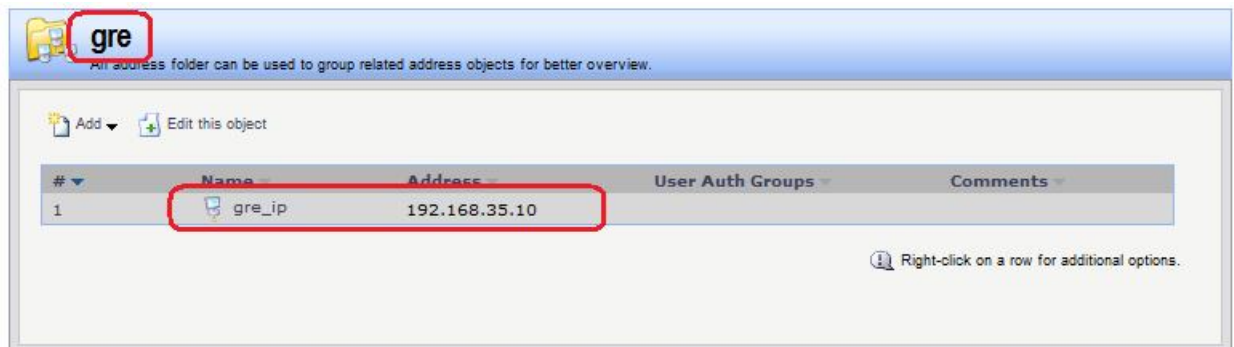
Создать объект, описывающий IP-адрес локальной стороны GRE-туннеля.

Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: gre

Object → Address Book → gre → Add



Командная строка:

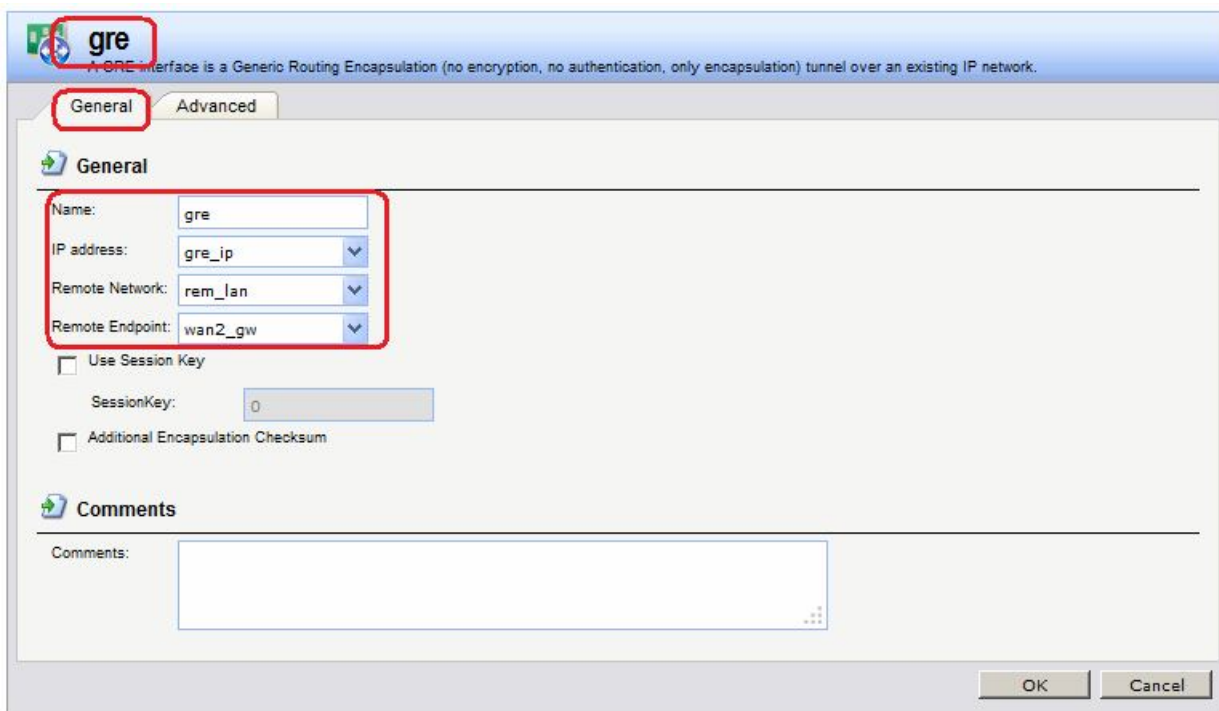
```
add Address AddressFolder gre
cc Address AddressFolder gre
add IP4Address gre_ip Address=192.168.35.10
```

GRE-Интерфейс

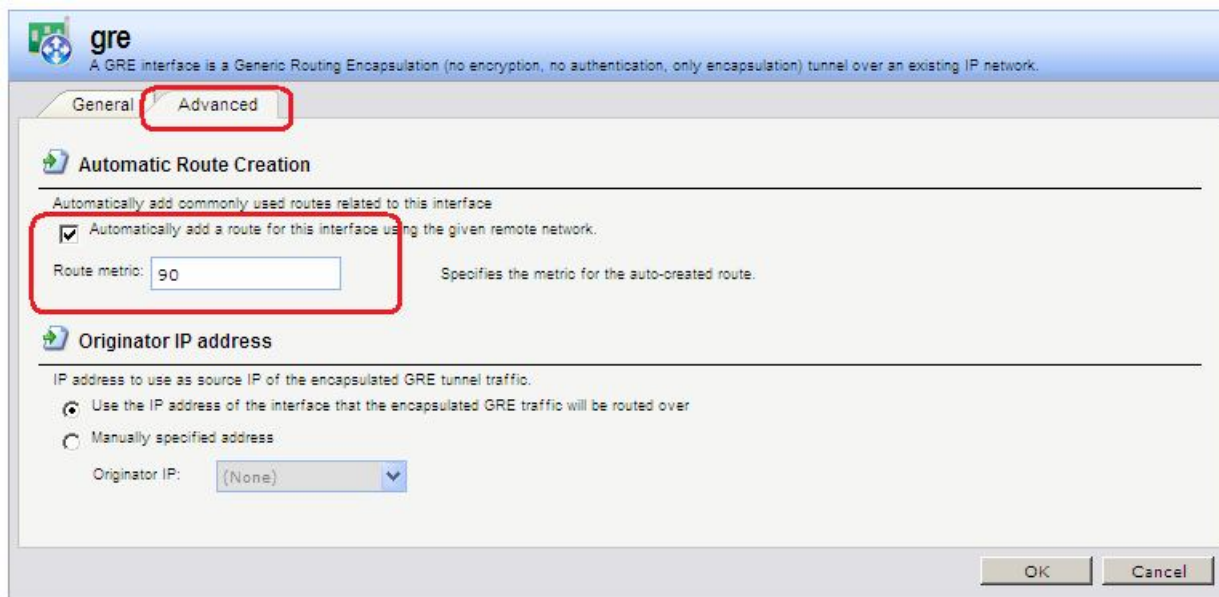
Веб-интерфейс:

Interfaces → GRE → Add → GRE Tunnel

На вкладке **General** указать IP-адрес локальной точки туннеля, удаленную сеть и IP-адрес удаленной точки.



Если на вкладке **Advanced** оставить флаг **Automatically add a route for this interface** ..., то в таблицу маршрутизации **main** добавится маршрут к данной сети с указанной метрикой.



Возможность редактировать параметры автоматически созданного маршрута отсутствует. Если необходимо отредактировать какие-либо параметры маршрута, то на вкладке **Advanced** интерфейса следует снять флаг автоматического добавления маршрута и добавить маршрут вручную с необходимыми параметрами.

Командная строка:

```
add Interface GREtunnel gre Network=remote/rem_lan IP=gre/gre_ip
RemoteEndpoint=wan2/wan2_gw
```

Статическая маршрутизация

В таблице маршрутизации должны быть маршруты с интерфейсов **wan2** и **gre** к соответствующим сетям.

Routing Table Contents

Routing Table Contents

Routing Table: <main>

Show all routes: (Including routes to interface addresses and Layer 3 Cache entries)

Do not show single host routes:

Max routes to display: 100

IPv4 Routing table contents (max 100 entries)

Flags	Network	Interface	Gateway	Local IP	Metric
	10.6.10.0/28	wan1			100
	192.168.2.0/24	gre			90
	192.168.1.0/24	lan			100
	172.17.100.0/24	dmz			100
	192.168.20.0/24	wan2			100
	0.0.0.0/0	wan1	10.6.10.3		100

IPv6 Routing table contents (max 100 entries)

Flags	Network	Interface	Gateway	Local IP	Metric
-------	---------	-----------	---------	----------	--------

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.)

Правила фильтрации

Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: gre

Rules → IP Rules → gre → Add

gre

All IP Rule Folder can be used to group IP Rules into logical groups for better overview and simplified management.

#	Name	Action	Source interface	Source network	Destination interface	Destination network	Service
1	gre_out	Allow	lan	lan_net	gre	rem_lan	all_services
2	gre_in	Allow	gre	rem_lan	lan	lan_net	all_services
3	gre_in_core	Allow	gre	rem_lan	core	lan_net	all_services

Right-click on a row for additional options.

Командная строка:

```
add IPRuleFolder Name=gre
```

```
cc IPRuleFolder <N folder>
```

```
add IPRule Action=Allow SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=gre DestinationNetwork=remote/rem_lan Service=
all_services Name=gre_out
```

```

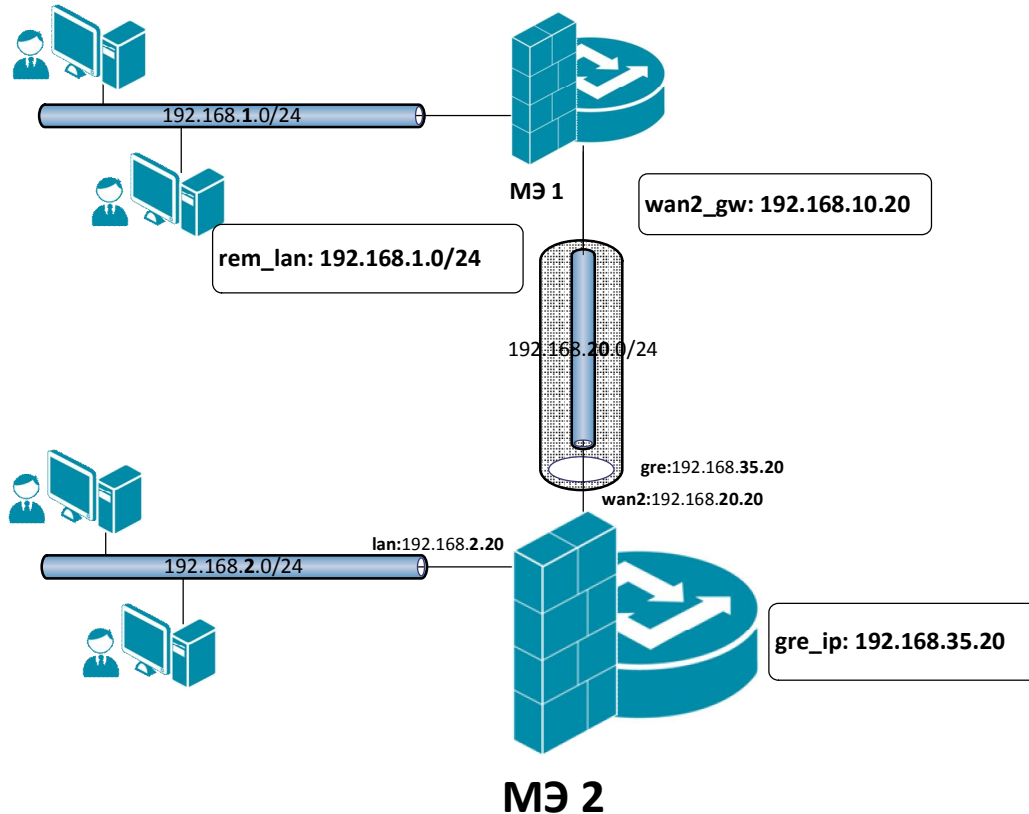
add IPRule Action=Allow SourceInterface=gre SourceNetwork=remote/rem_lan
DestinationInterface=lan DestinationNetwork=lan/lan_net Service=all_services
Name=gre_in

add IPRule Action=Allow SourceInterface=gre SourceNetwork=remote/rem_lan
DestinationInterface=core DestinationNetwork=lan/lan_net Service=all_services
Name=gre_in_core

```

Последнее правило разрешает доступ к lan-интерфейсу самого межсетевого экрана.

Межсетевой Экран 2



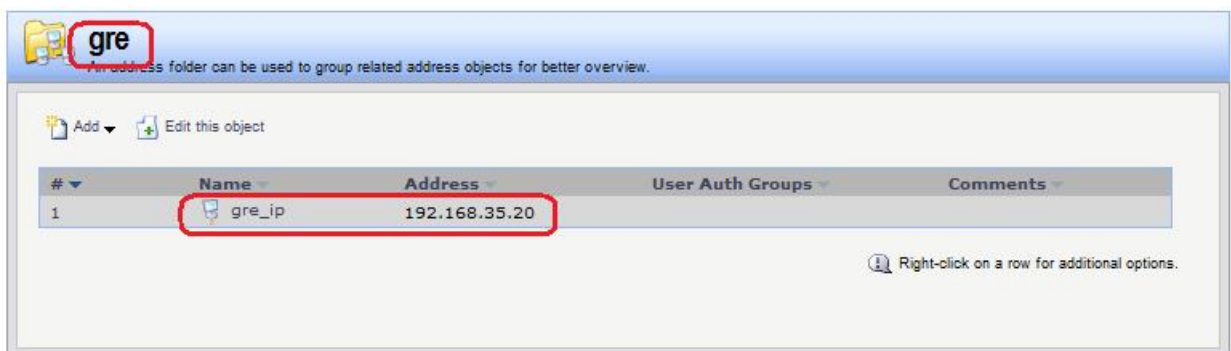
Объекты Адресной Книги

Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: gre

Object → Address Book → gre → Add



Командная строка:

```

add Address AddressFolder gre
cc Address AddressFolder gre

```

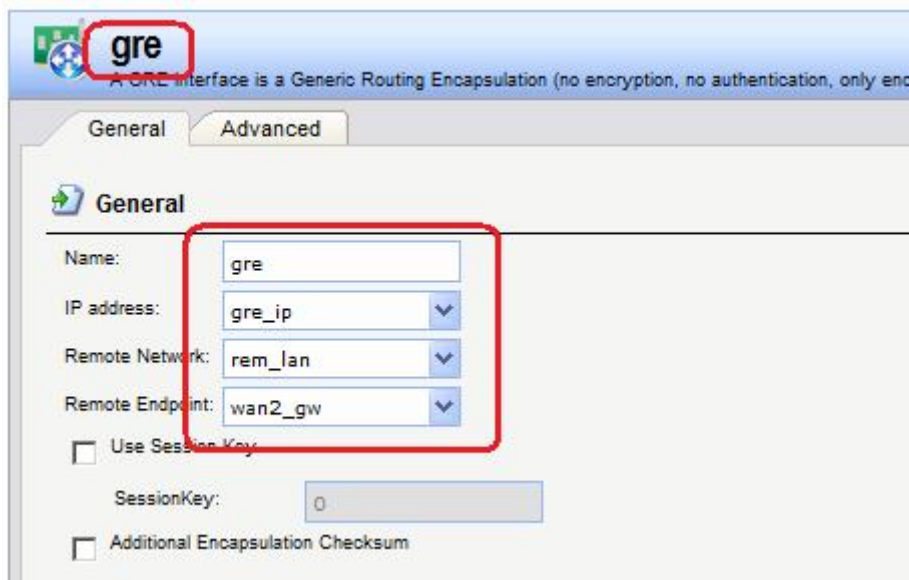
```
add IP4Address gre_ip Address=192.168.35.20
```

GRE-Интерфейс

Веб-интерфейс:

Interfaces → GRE → Add → GRE Tunnel

На вкладке **General** указать IP-адрес локальной точки туннеля, удаленную сеть и IP-адрес удаленной точки.



Командная строка:

```
add Interface GREtunnel gre1 Network=remote/rem_lan IP=gre/gre_ip  
RemoteEndpoint=wan2/wan2_gw
```

Статическая маршрутизация

В таблице маршрутизации должны быть маршруты с интерфейсов **wan2** и **gre** к соответствующим сетям.

Routing Table Contents

Routing Table Contents

Routing Table: <main>

Show all routes: (Including routes to interface addresses and Layer 3 Cache entries)

Do not show single host routes:

Max routes to display: 100

IPv4 Routing table contents (max 100 entries)

Flags	Network	Interface	Gateway	Local IP	Metric
	192.168.1.0/24	gre			90
	10.0.4.0/24	wan1			100
	192.168.20.0/24	wan2			100
	172.17.200.0/24	dmz			100
	192.168.2.0/24	lan			100
	0.0.0.0/0	wan1	10.0.4.1		100

IPv6 Routing table contents (max 100 entries)

Flags	Network	Interface	Gateway	Local IP	Metric
-------	---------	-----------	---------	----------	--------

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.)

Правила фильтрации

Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: gre

Rules → IP Rules → gre → Add

gre
An IP Rule Folder can be used to group IP Rules into logical groups for better overview and simplified management.

Add ▾ Edit this object

#	Name	Action	Source interface	Source network	Destination interface	Destination network	Service
1	gre_out	Allow	lan	lan_net	gre	rem_lan	all_services
2	gre_in	Allow	gre	rem_lan	lan	lan_net	all_services
3	gre_in_core	Allow	gre	rem_lan	core	lan_net	all_services

Right-click on a row for additional options.

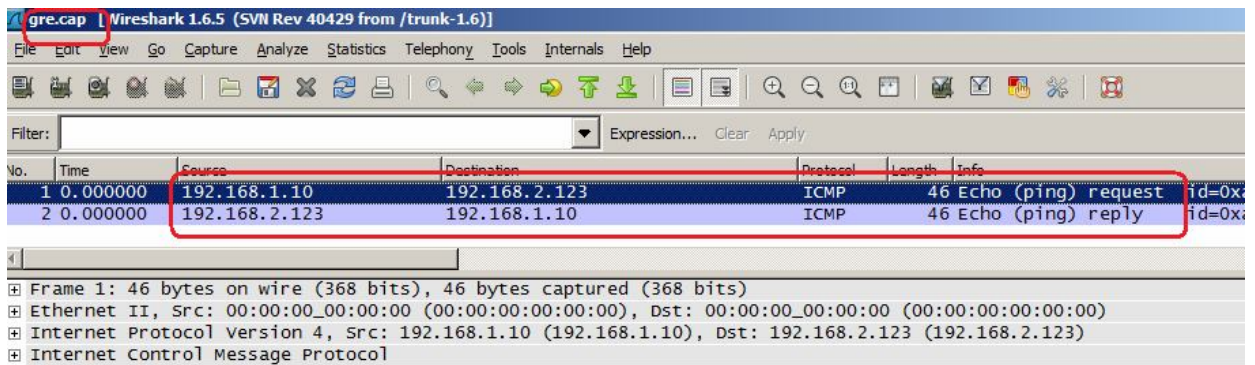
Командная строка:

```
add IPRuleFolder Name=gre
```

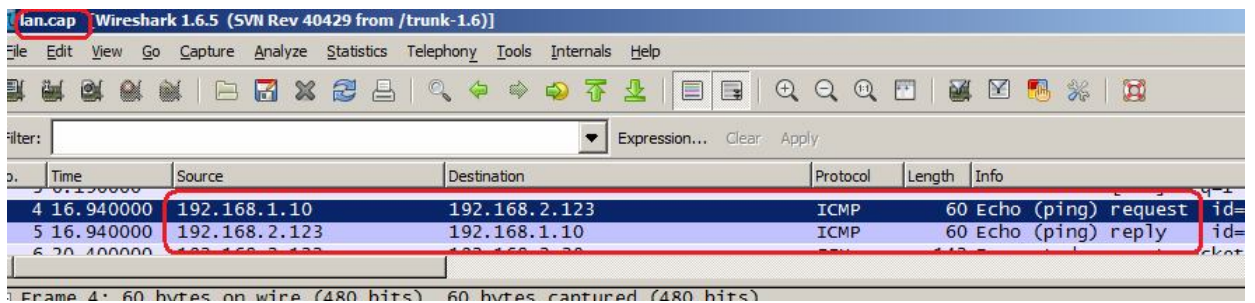
```
cc IPRuleFolder <N folder>
```

```
add IPRule Action=Allow SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=gre DestinationNetwork=remote/rem_lan
Service=all_services Name=gre_out
```

```
add IPRule Action=Allow SourceInterface=gre SourceNetwork=remote/rem_lan
DestinationInterface=gre DestinationNetwork=lan/lan_net Service=all_services
Name=gre_in
```

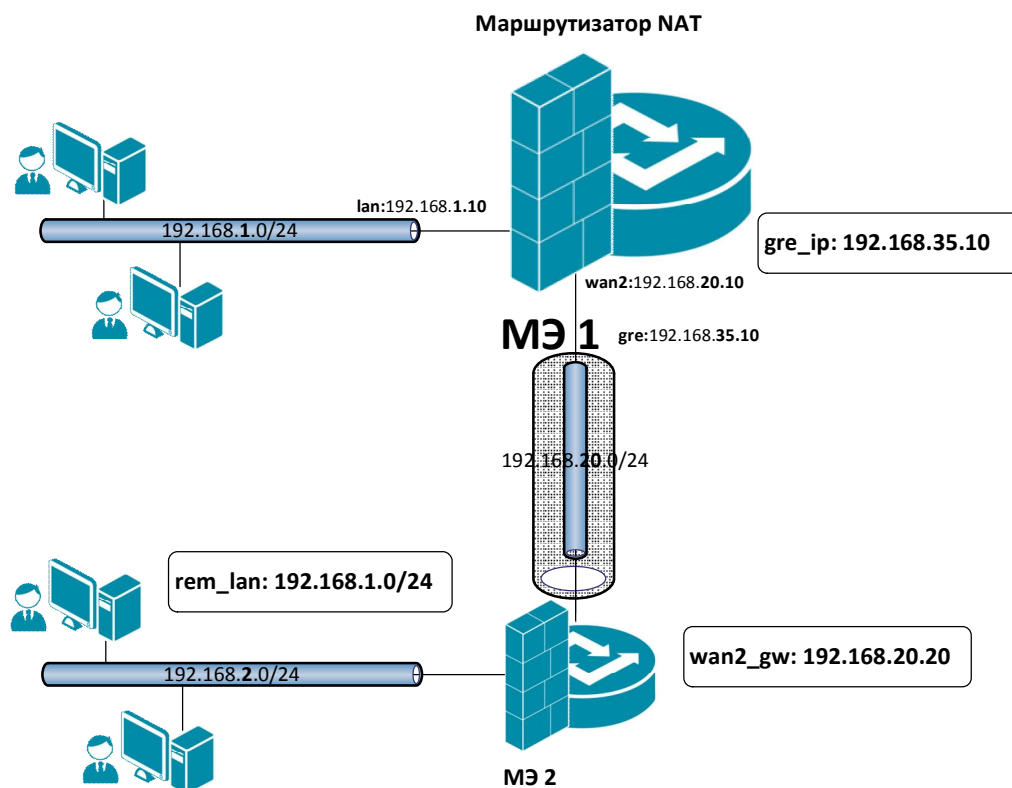
На интерфейсе `lan` видим также только ICMP-трафик с адресами из локальных сетей.



В данной топологии IP-адреса gre-интерфейсов используются исключительно для конфигурирования, в трафике они отсутствуют.

Одна из локальных сетей находится за NAT

Межсетевой Экран 1



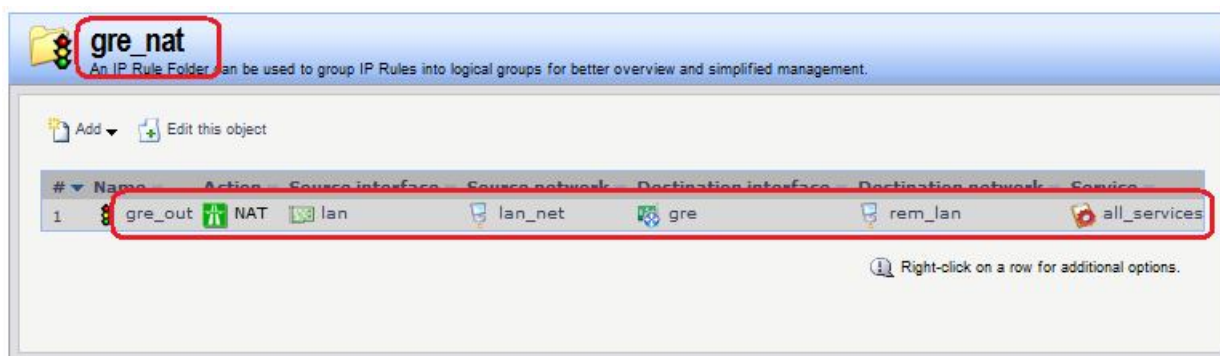
Правила фильтрации

Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: gre_nat

Rules → IP Rules → gre_nat → Add



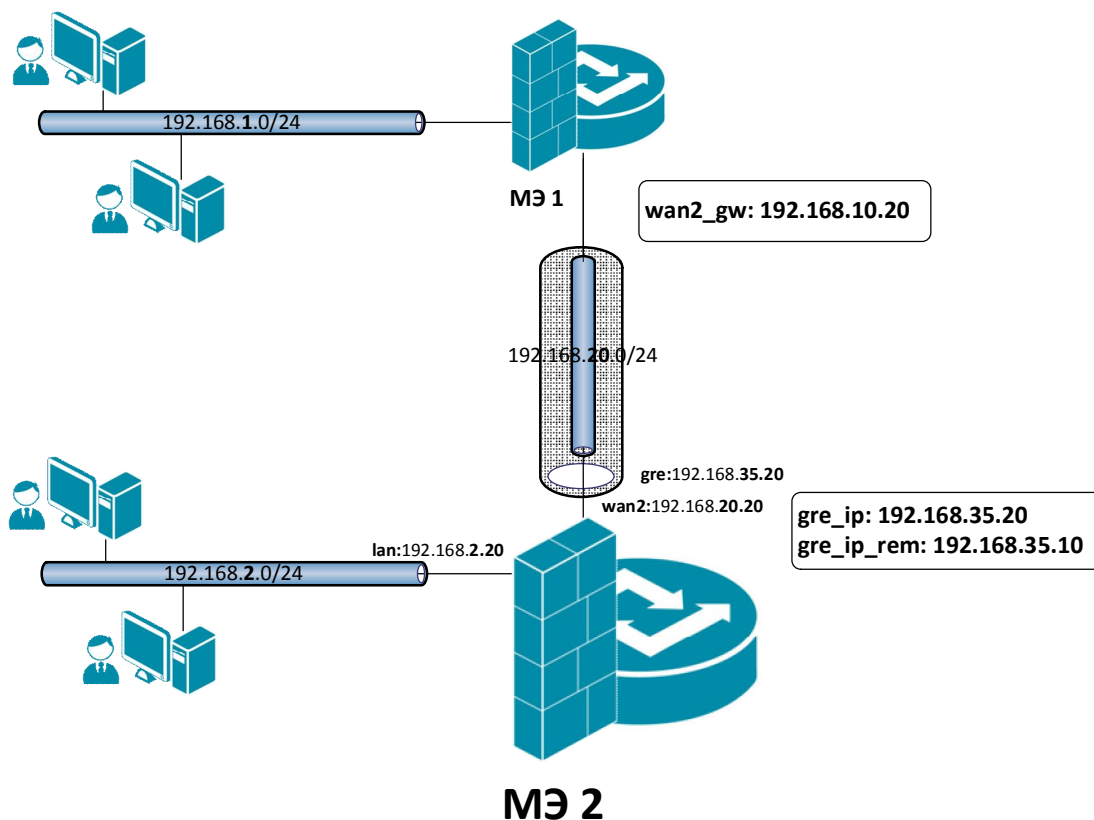
Командная строка:

```
add IPRuleFolder Name=gre_nat
```

```
cc IPRuleFolder <N folder>
```

```
add IPRule Action=Allow SourceInterface=lan SourceNetwork=lan/lan_net  
DestinationInterface=gre DestinationNetwork=remote/rem_lan  
Service=all_services Name=gre_out
```

Межсетевой Экран 2



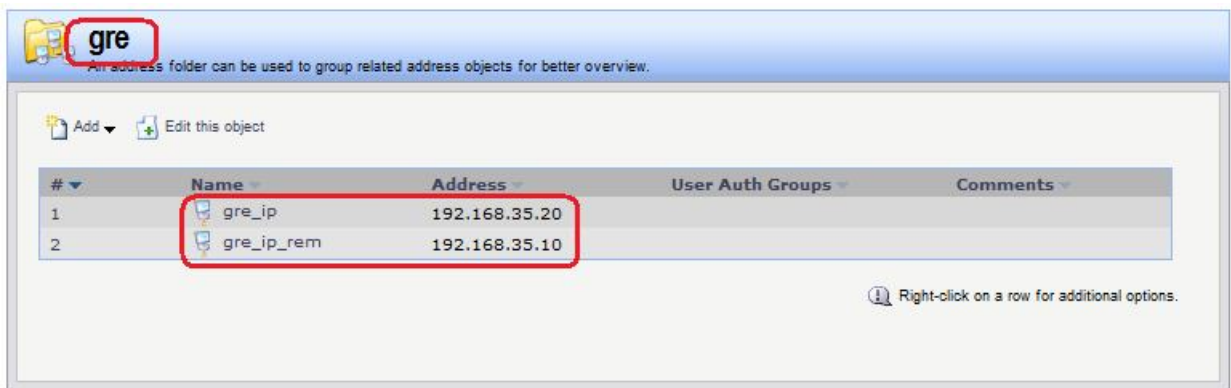
Объекты Адресной Книги

Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: gre

Object → Address Book → gre → Add



Командная строка:

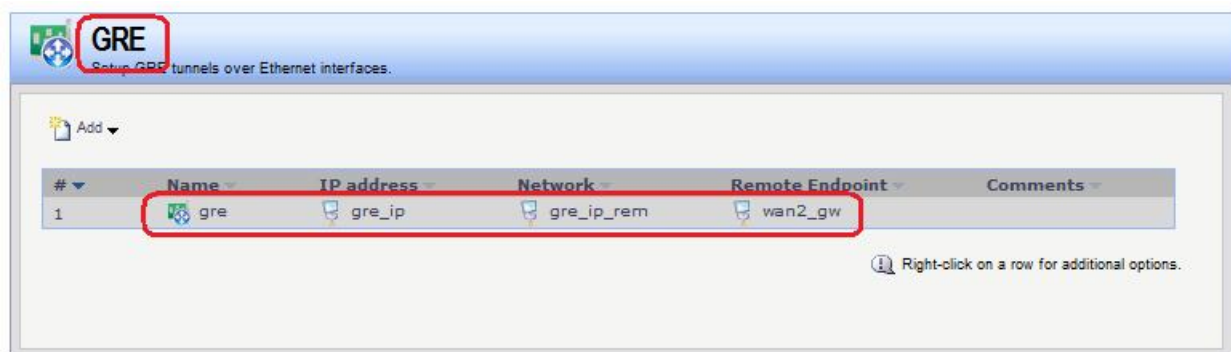
```
add Address AddressFolder gre
cc Address AddressFolder gre
add IP4Address gre_ip Address=192.168.35.20
add IP4Address gre_ip_rem Address=192.168.35.10
```

GRE-Интерфейс

Веб-интерфейс:

Interfaces → GRE → Add → GRE Tunnel

На вкладке **General** указать IP-адрес локальной точки туннеля, IP-адрес удаленной точки gre-туннеля, на котором выполняется преобразование NAT, и IP-адрес удаленного интерфейса.



Командная строка:

```
add Interface GREtunnel gre1 Network=gre/gre_ip_rem IP=gre/gre_ip
RemoteEndpoint=wan2/wan2_gw
```

Статическая маршрутизация

В таблице маршрутизации должны быть маршруты с интерфейсов **wan2** и **gre** к соответствующим сетям.

Routing Table Contents

Routing Table Contents

Routing Table: <main>

Show all routes: (Including routes to interface addresses and Layer 3 Cache entries)

Do not show single host routes:

Max routes to display: 100

IPv4 Routing table contents (max 100 entries)

Flags	Network	Interface	Gateway	Local IP	Metric
	192.168.35.10	gre			90
	10.0.4.0/24	wan1			100
	192.168.20.0/24	wan2			100
	172.17.200.0/24	dmz			100
	192.168.2.0/24	lan			100
	0.0.0.0/0	wan1	10.0.4.1		100

IPv6 Routing table contents (max 100 entries)

Flags	Network	Interface	Gateway	Local IP	Metric
-------	---------	-----------	---------	----------	--------

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.)

Правила фильтрации

Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: gre_nat

Rules → IP Rules → gre_nat → Add

gre_nat

An IP Rule Folder can be used to group IP Rules into logical groups for better overview and simplified management.

Add Edit this object

#	Name	Action	Source interface	Source network	Destination interface	Destination network	Service
1	gre_in	Allow	gre	gre_ip_rem	lan	lan_net	all_services
2	gre_in_core	Allow	gre	gre_ip_rem	core	lan_net	all_services

Right-click on a row for additional options.

Командная строка:

```
add IPRuleFolder Name=gre_nat
```

```
cc IPRuleFolder <N folder>
```

```
add IPRule Action=Allow SourceInterface=gre SourceNetwork=gre/gre_ip_rem
DestinationInterface=gre DestinationNetwork=lan/lan_net Service=all_services
Name=gre_in
```

```
add IPRule Action=Allow SourceInterface=gre SourceNetwork=gre/gre_ip_rem
DestinationInterface=core DestinationNetwork=lan/lan_net Service=all_services
Name=gre_in_core
```

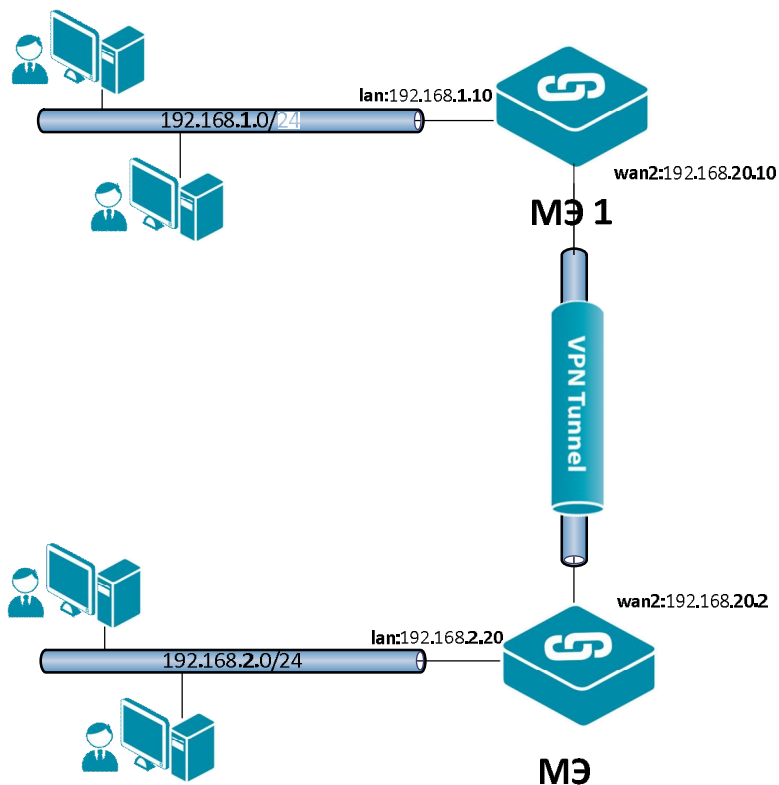
Последнее правило разрешает доступ к lan-интерфейсу самого межсетевого экрана.

Лабораторная работа 2. Соединение двух локальных сетей протоколом IPSec в туннельном режиме, аутентификация с использованием общего секрета

Цель

Соединить две сети, расположенные за межсетевыми экранами, VPN с использованием семейства протоколов IPSec. В этом случае необходимо использовать туннельный режим.

Топология сети



Между интерфейсами **wan2** на МЭ 1 и МЭ 2 требуется поднять VPN/IPSec.

Описание практической работы

Создать статическую маршрутизацию и политики доступа, которые разрешают доступ между удаленными локальными сетями. При этом трафик между МЭ 1 и МЭ 2 проходит по VPN/IPSec.

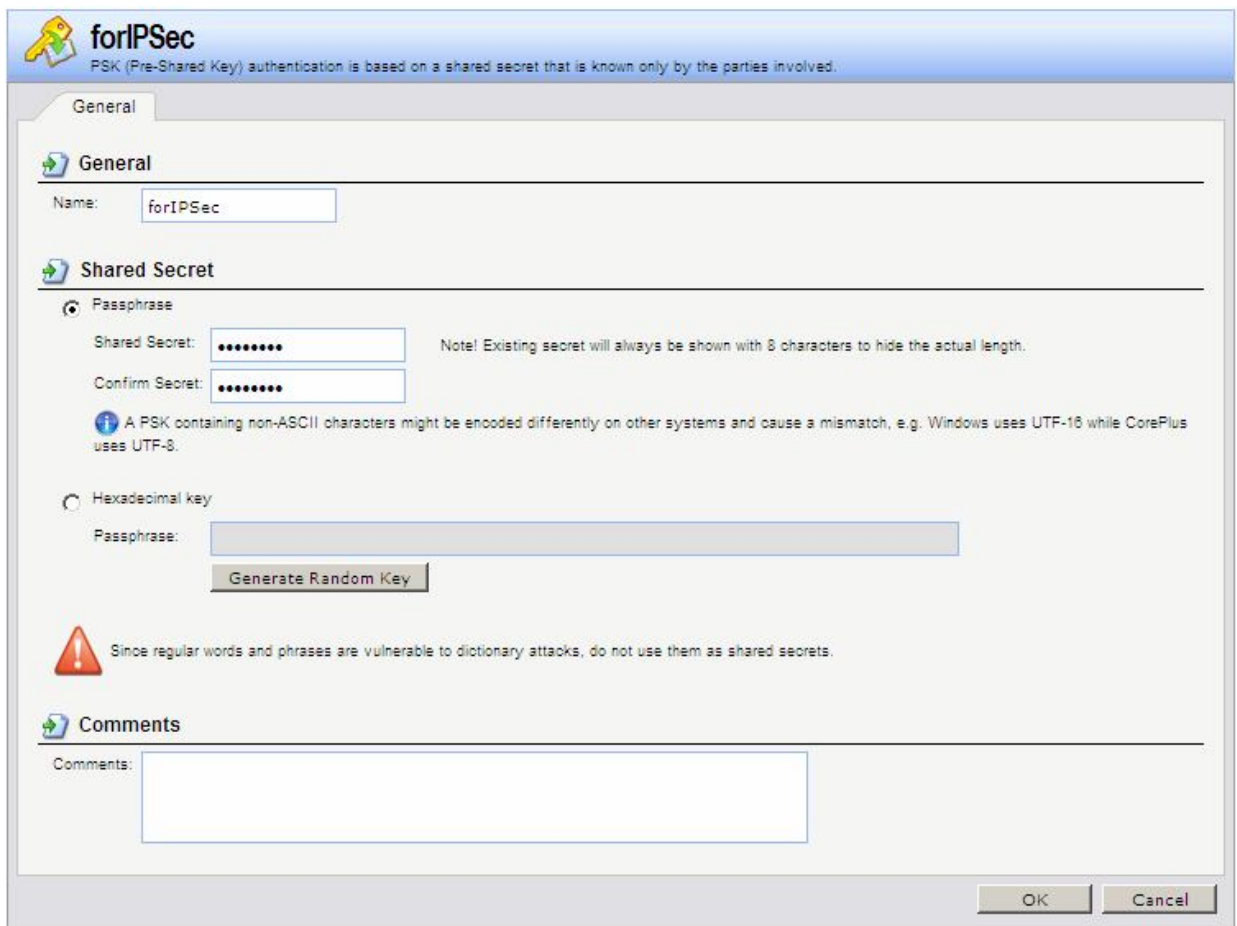
Межсетевой Экран 1

Аутентификационный Объект

Необходимо создать аутентификационный объект **Pre-Shared Key**.

Веб-интерфейс:

Object → Authentication Objects → Add → Pre-Shared Key



Командная строка:

```
add PSK forIPSec Type=ASCII PSKAscii=qwerty
```


IPSec-Интерфейс

Создать IPSec-интерфейс. Так как создается VPN-туннель между двумя локальными сетями, то необходим туннельный режим.

Веб-интерфейс:

Interfaces → **IPsec** → **Add** → **IPsec Tunnel**

На вкладке **General** указать сети перед и за туннелем, а также режим выполнения IPSec и используемые наборы алгоритмов для IPSec и IKE.

 **ipsec_tunnel**
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: ipsec_tunnel

Local Network: lan_net

Remote Network: rem_lan

Remote Endpoint: wan2_gw

Encapsulation mode: Tunnel

IKE Config Mode Pool: (None)

Algorithms

IKE Algorithms: Medium

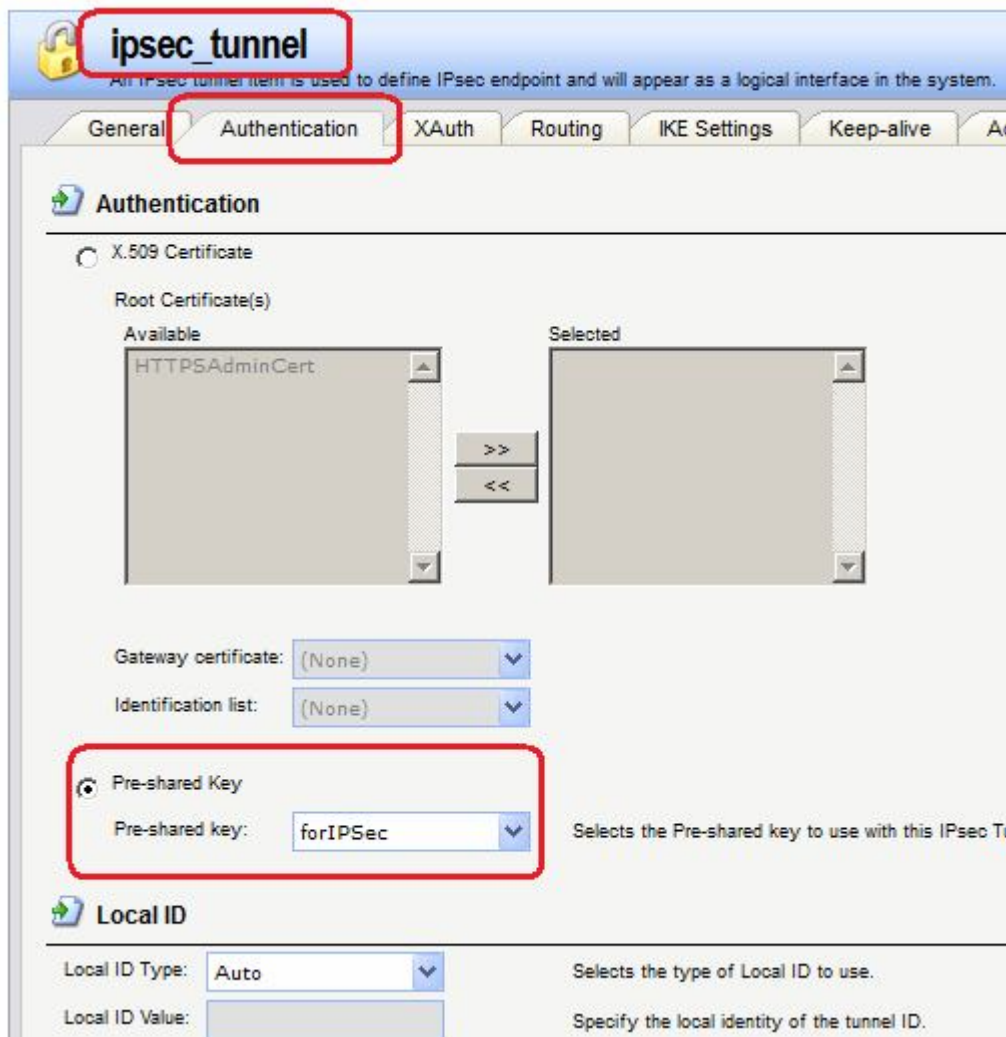
IKE Lifetime: 28800 seconds

IPsec Algorithms: Medium

IPsec Lifetime: 3600 seconds

IPsec Lifetime: 0 kilobytes

На вкладке **Authentication** указать созданный аутентификационный объект.



В данном случае, как и в большинстве случаев при создании туннелей с использованием различных протоколов, маршрут может создаваться либо статически, либо динамически на время создания туннеля.

1. Статически создаваемый маршрут.

Если все остальные параметры оставить по умолчанию, то в таблице маршрутизации будет создан маршрут.

Веб-интерфейс:

Routing Table Contents

Routing Table Contents

Routing Table:

Show all routes: (Including routes to interface addresses and Layer 3 Cache entries)

Do not show single host routes:

Max routes to display:

IPv4 Routing table contents (max 100 entries)

Flags	Network	Interface	Gateway	Local IP	Metric
	192.168.1.0/24	ipsec_tunnel			90
	10.0.4.0/24	wan1			100
	192.168.20.0/24	wan2			100
	172.17.200.0/24	dmz			100
	192.168.2.0/24	lan			100
	0.0.0.0/0	wan1	10.0.4.1		100

IPv6 Routing table contents (max 100 entries)

Flags	Network	Interface	Gateway	Local IP	Metric
-------	---------	-----------	---------	----------	--------

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.)

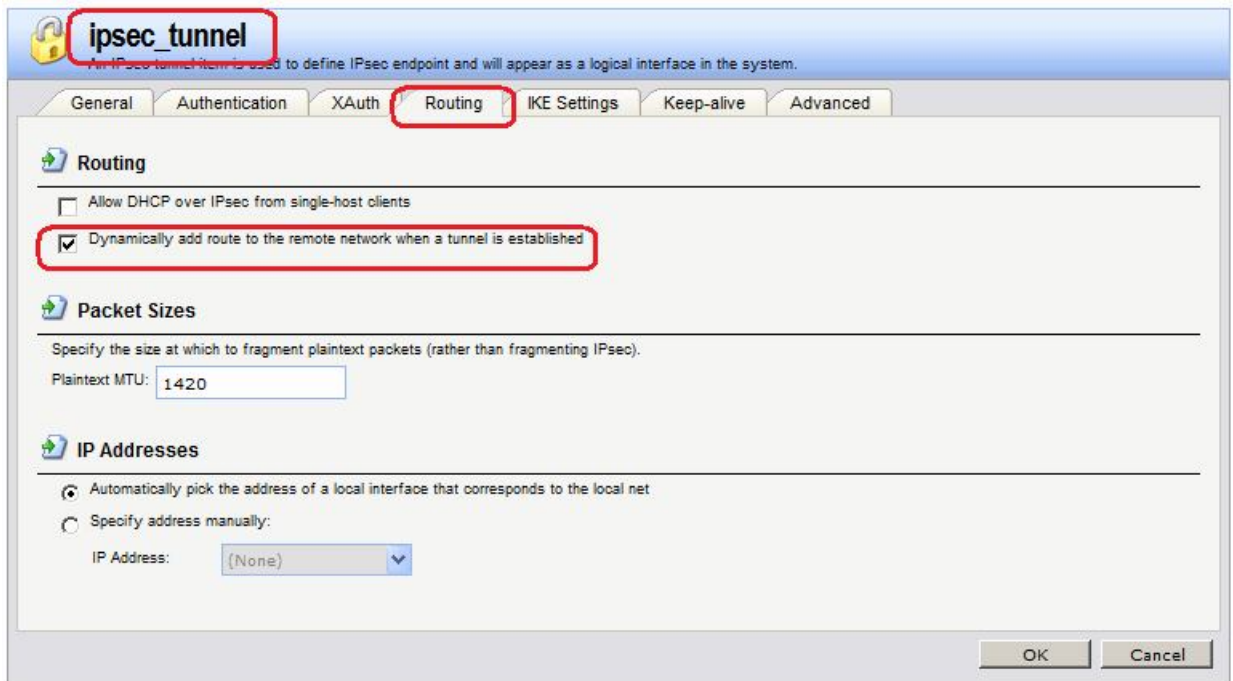
Командная строка:

```
add Interface IPsecTunnel ipsec_tunnel LocalNetwork=lan/lan_net
RemoteNetwork=remote/rem_lan AuthMethod=PSK PSK=forIPSec IKEAlgorithms=Medium
IPsecAlgorithms=Medium EncapsulationMode=Tunnel RemoteEndpoint=wan2/wan2_gw
```

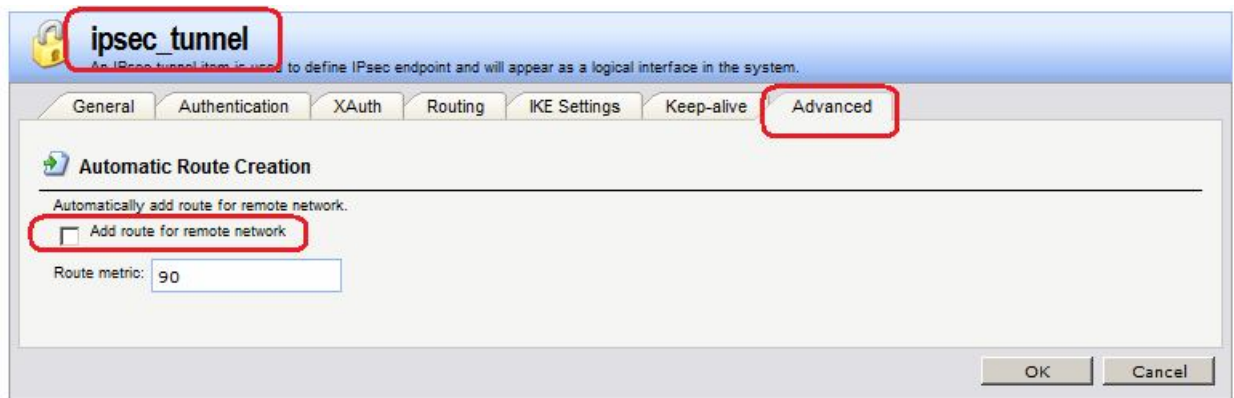
2. Динамически создаваемый маршрут.

Веб-интерфейс:

Если инициатором начального установления туннеля всегда будет являться противоположная сторона, возможно динамически создавать маршрут. Для этого на вкладке **Routing** следует поставить флаг динамического добавления маршрута.



А на вкладке **Advanced** снять флаг добавления маршрута, чтобы в таблице маршрутизации при наличии IPSec-трафика не было двух одинаковых маршрутов.



Командная строка:

```
set Interface IPsecTunnel ipsec_tunnel AddRouteToRemoteNet=Yes  
AutoInterfaceNetworkRoute=No
```

В этом случае в таблице маршрутизации будет динамически создаваться маршрут.

Routing Table Contents

Routing Table Contents

Routing Table: <main>

Show all routes: (Including routes to interface addresses and Layer 3 Cache entries)

Do not show single host routes:

Max routes to display: 100

IPv4 Routing table contents (max 100 entries)

Flags	Network	Interface	Gateway	Local IP	Metric
D	192.168.1.0/24	ipsec_tunnel			0
	10.0.4.0/24	wan1			100
	192.168.20.0/24	wan2			100
	172.17.200.0/24	dmz			100
	192.168.2.0/24	lan			100
	0.0.0.0/0	wan1	10.0.4.1		100

IPv6 Routing table contents (max 100 entries)

Flags	Network	Interface	Gateway	Local IP	Metric
-------	---------	-----------	---------	----------	--------

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.)

Правила фильтрации

Определим правило, разрешающее исходящий трафик с локальной сети, расположенной за МЭ 1, на локальную сеть, расположенную за МЭ 2.

Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: ipsec_tunnel

Rules → IP Rules → ipsec_tunnel → Add

ipsec_tunnel

An IP Rule Folder can be used to group IP Rules into logical groups for better overview and simplified management.

#	Name	Action	Source interface	Source network	Destination interface	Destination network	Service
1	ipsec_out	Allow	lan	lan_net	ipsec_tunnel	rem_lan	all_services

Right-click on a row for additional options.

Командная строка:

```
add IPRuleFolder Name=ipsec_tunnel
```

```
cc IPRuleFolder <N folder>
```

```
add IPRule Action=Allow SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=ipsec_tunnel DestinationNetwork=remote/rem_lan
Service=all_services Name=ipsec_out
```

Межсетевой Экран 2

Аутентификационный Объект

Необходимо создать аутентификационный объект **Pre-Shared Key** с тем же значением **Shared Secret**, что и на межсетевом экране 1.

Веб-интерфейс:

Object → **Authentication Objects** → **Add** → **Pre-Shared Key**

The screenshot shows the 'forIPSec' web interface for creating a Pre-Shared Key authentication object. The interface is titled 'forIPSec' and includes a subtitle: 'PSK (Pre-Shared Key) authentication is based on a shared secret that is known only by the parties involved.' The main content area is divided into sections: 'General', 'Shared Secret', and 'Comments'. In the 'General' section, the 'Name' field is set to 'forIPSec'. The 'Shared Secret' section has two radio buttons: 'Passphrase' (selected) and 'Hexadecimal key'. Under 'Passphrase', there are two input fields for 'Shared Secret' and 'Confirm Secret', both containing eight dots. A note states: 'Note! Existing secret will always be shown with 8 characters to hide the actual length.' Below this, a warning icon and text state: '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.' Under 'Hexadecimal key', there is a 'Passphrase' input field and a 'Generate Random Key' button. At the bottom of the 'Shared Secret' section, another warning icon and text state: 'Since regular words and phrases are vulnerable to dictionary attacks, do not use them as shared secrets.' The 'Comments' section has an empty text area. At the bottom right, there are 'OK' and 'Cancel' buttons.

Командная строка:

```
add PSK forIPSec Type=ASCII PSKAscii=qwerty
```

IPSec-Интерфейс

Необходимо создать IPSec-интерфейс.

Веб-интерфейс:

Interfaces → **IPsec** → **Add** → **IPsec Tunnel**

На вкладке **General** указать сети перед и за туннелем, а также режим выполнения IPSec и используемые наборы алгоритмов для IPSec и IKE.

ipsec_tunnel
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: ipsec_tunnel

Local Network: lan_net

Remote Network: rem_lan

Remote Endpoint: wan2_gw

Encapsulation mode: Tunnel

IKE Config Mode Pool: (None)

Algorithms

IKE Algorithms: Medium

IKE Lifetime: 28800 seconds

IPsec Algorithms: Medium

IPsec Lifetime: 3600 seconds

IPsec Lifetime: 0 kilobytes

На вкладке **Authentication** указать созданный аутентификационный объект.

ipsec_tunnel
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

Authentication

X.509 Certificate

Root Certificate(s)

Available: HTTPSAAdminCert

Selected:

Gateway certificate: (None)

Identification list: (None)

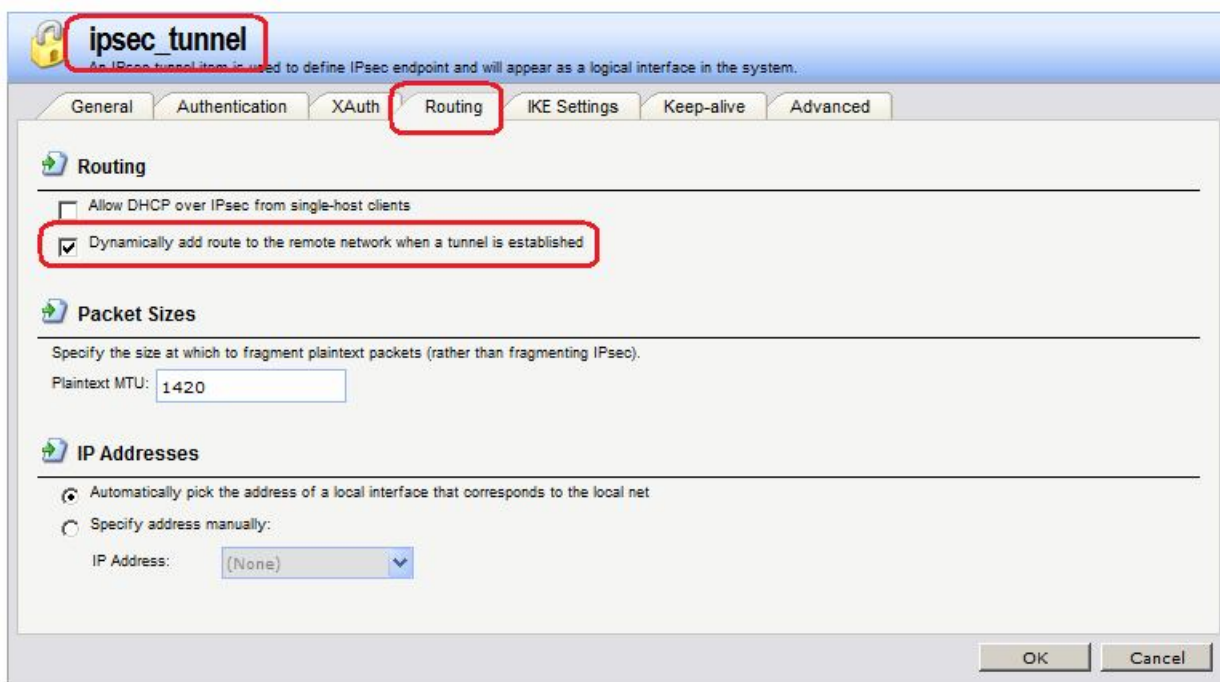
Pre-shared Key

Pre-shared key: forIPSec Selects the Pre-shared key to use with this IPsec Tunnel.

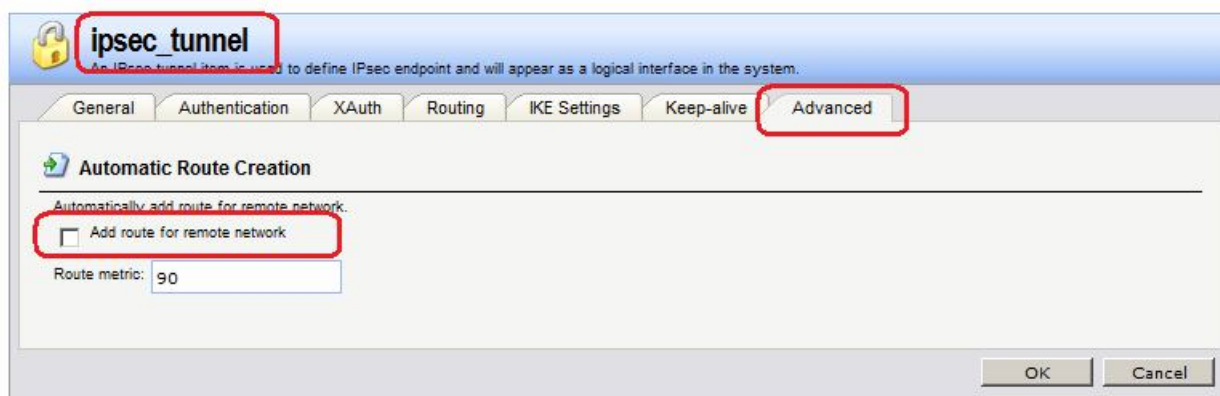
Local ID

Local ID Type: Auto Selects the type of Local ID to use.

Если все остальные параметры оставить по умолчанию, то в таблице маршрутизации маршрут будет создаваться статически. Если необходимо динамически создавать маршрут, то на вкладке **Routing** поставить флаг динамического добавления маршрута.



А на вкладке **Advanced** снять флаг добавления маршрута (иначе в таблице маршрутизации при наличии IPSec-трафика будет два одинаковых маршрута, что не является ошибкой, но смысла не имеет).



Командная строка:

```
add Interface IPsecTunnel ipsec_tunnel LocalNetwork=lan/lan_net
RemoteNetwork=remote/rem_lan AuthMethod=PSK PSK=forIPSec IKEAlgorithms=Medium
IPsecAlgorithms=Medium EncapsulationMode=Tunnel RemoteEndpoint=wan2/wan2_gw
```

Правила фильтрации

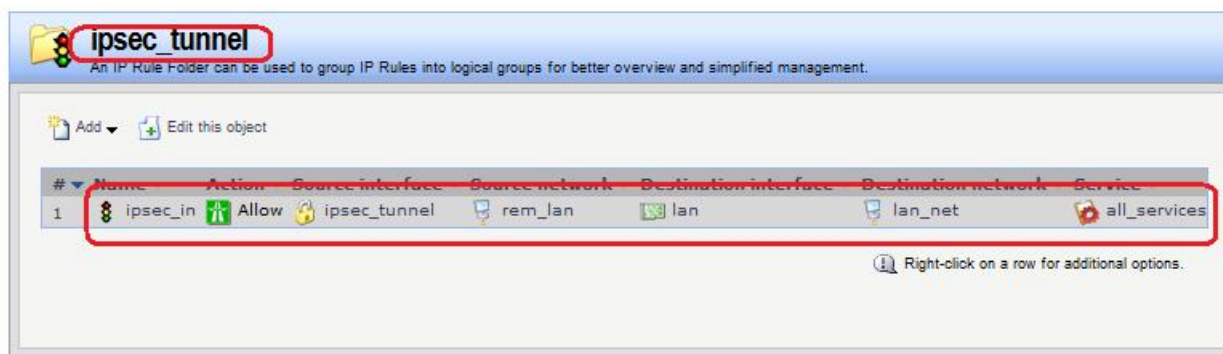
Создаем правила фильтрации, разрешающие входящий трафик с удаленной локальной сети, приходящий на ipsec-туннель, к локальной сети, расположенной за МЭ 2.

Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: ipsec_tunnel

Rules → IP Rules → ipsec_tunnel → Add



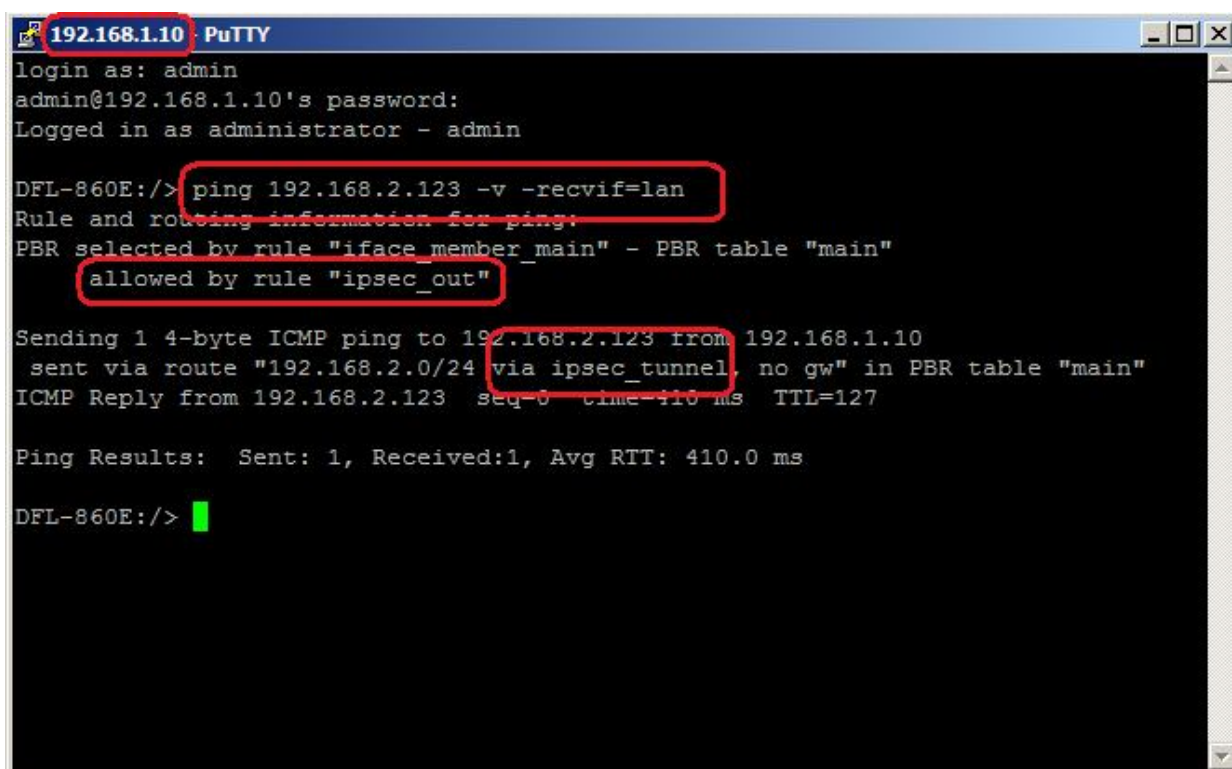
Командная строка:

```
add IPRuleFolder Name=ipsec_tunnel
cc IPRuleFolder <N folder>

add IPRule Action=Allow SourceInterface=ipsec_tunnel
SourceNetwork=remote/rem_lan DestinationInterface=lan
DestinationNetwork=lan/lan_net Service=all_services Name=ipsec_in
```

Проверка конфигурации

1. На МЭ1 выполняем команду `ping` рабочей станции, расположенной в удаленной локальной сети. В качестве интерфейса, с которого пакет будет отправлен, указываете `lan`.



2. На МЭ 1 проверяем наличие IKE SA и IPSec SA.

IPsec IKE Status

IPsec IKE Status List VPN Interfaces.

Gateway	Created	Expires	Encryption Algorithm	Remove IKE SA
192.168.20.20	2014-05-13 11:12:18	2014-05-13 19:12:18	3des-cbc	

24 hrs ago now

IPsec SAs

Remote Gateway	Local Net	Remote net	Protocol
192.168.20.20	192.168.1.0/24	192.168.2.0/24	3des-cbc

3. На МЭ 2 также проверяем наличие IKE SA и IPsec SA.

4. Можно также проверить наличие ISAKMP SA и ESP SA, сделав дамп трафика.

wan1_10.cap [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.20.10	192.168.20.20	ESP	134	ESP (SPI=0xe190ffeb)
2	0.000000	192.168.20.20	192.168.20.10	ESP	134	ESP (SPI=0x536a7e79)
3	1.000000	192.168.20.10	192.168.20.20	ESP	134	ESP (SPI=0xe190ffeb)
4	1.000000	192.168.20.20	192.168.20.10	ESP	134	ESP (SPI=0x536a7e79)
5	2.000000	192.168.20.10	192.168.20.20	ESP	134	ESP (SPI=0xe190ffeb)
6	2.000000	192.168.20.20	192.168.20.10	ESP	134	ESP (SPI=0x536a7e79)
7	3.000000	192.168.20.10	192.168.20.20	ESP	134	ESP (SPI=0xe190ffeb)
8	3.000000	192.168.20.20	192.168.20.10	ESP	134	ESP (SPI=0x536a7e79)
9	23.560000	192.168.20.20	192.168.20.10	ISAKMP	134	Informational
10	23.570000	192.168.20.10	192.168.20.20	ISAKMP	134	Informational

Frame 10: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits)

Ethernet II, Src: D-Link_49:dc:ff (5c:d9:98:49:dc:ff), Dst: D-Link_49:dd:03 (5c:d9:98:49:dd:03)

Internet Protocol Version 4, Src: 192.168.20.10 (192.168.20.10), Dst: 192.168.20.20 (192.168.20.20)

User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)

Internet Security Association and Key Management Protocol

Initiator cookie: fib429694a756b6e
 Responder cookie: e27ca92e62b397b8
 Next payload: Hash (8)
 Version: 1.0
 Exchange type: Informational (5)

Flags: 0x01
 Message ID: 0xd458537c
 Length: 92
 Encrypted Data (64 bytes)

```

0000  5c d9 98 49 dd 03 5c d9 98 49 dc ff 08 00 45 00  \.I..\.I...E.
0010  00 78 f0 19 00 00 ff 11 21 ec c0 a8 14 0a c0 a8  .X.....!.....
0020  14 14 01 f4 01 f4 00 64 01 d7 f1 b4 29 69 4a 75  .....d....)iU
0030  6b 6e e2 7c a9 2e 62 b3 97 b8 08 10 05 01 d4 58  kn.|.b.....X
0040  53 7c 00 00 00 5c 47 15 53 ca c6 8a b7 62 bc 58  S|...G.S...b.X
0050  f7 11 3f 40 5f 40 f6 2f 13 f7 00 3b 56 50 dd 0b  7T.  .VA
  
```

File: "C:\Downloads\SSH Client\wan1_10.cap" 1... Packets: 10 Displayed: 10 Marked: 0 Load time: 0:00:000 Profile: Default

Лабораторная работа 3. Посмотреть статистику IPsec-туннелей можно из командной строки:

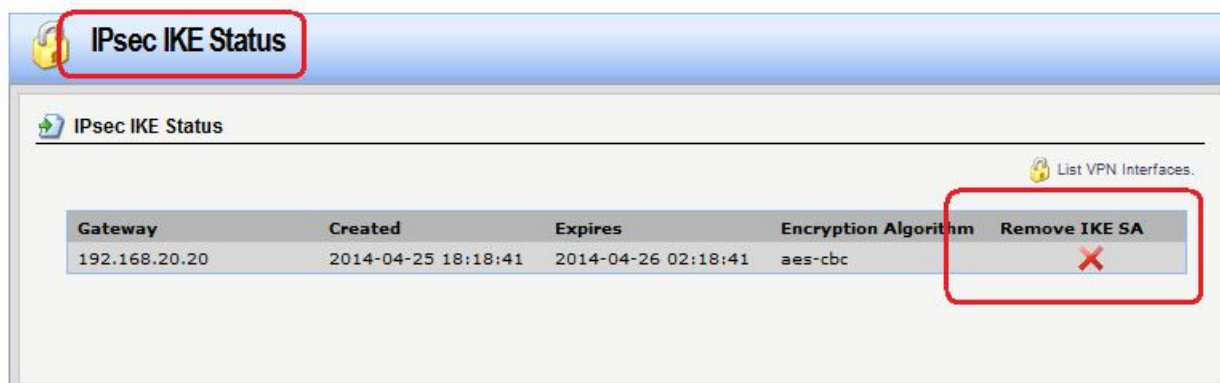
`ipsectunnels`

`ipsecstats`

ipsecglobalstats

Лабораторная работа 4. Удалить IKE SA можно из веб-интерфейса:

Status → IPsec → List all active IKE SAs



Лабораторная работа 5. Удалить ESP SA можно из командной строки:

```
killsa <IP-адрес>
```

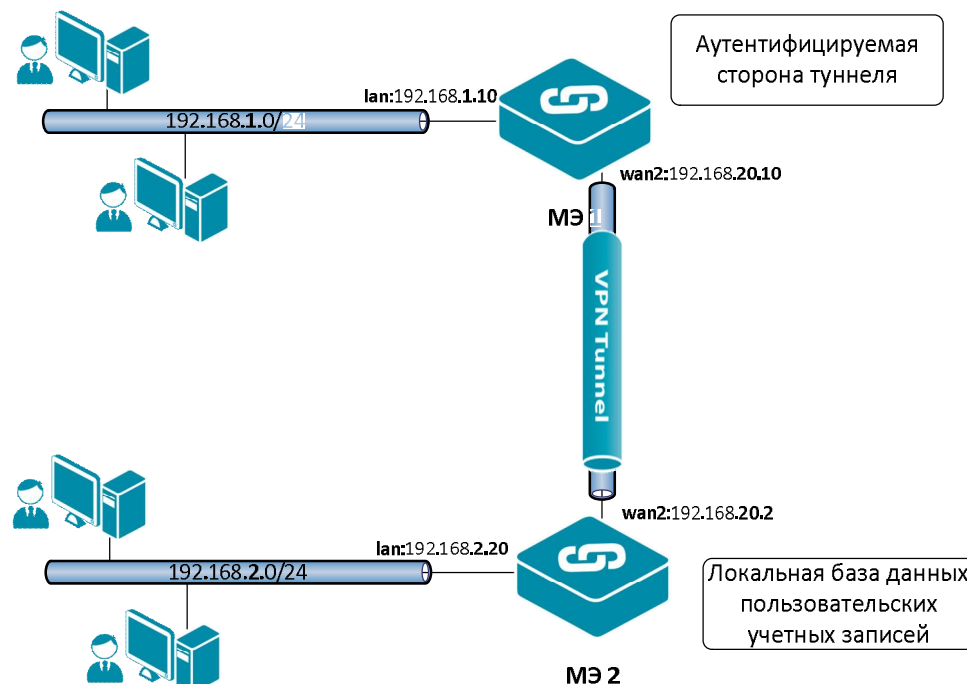
```
killsa -all
```

Лабораторная работа 3. Использование аутентификации по стандарту XAuth в протоколе IPsec

Цель

Соединить две сети, расположенные за межсетевыми экранами, VPN с использованием семейства протоколов IPsec, используя туннельный режим. Дополнительно выполнить аутентификацию на уровне пользователя по стандарту XAuth в Фазе II IKE (Quick Mode). БД пользовательских учетных записей хранится локально на МЭ 2. На МЭ 1 указывается имя пользователя и пароль.

Топология сети



Описание практической работы

Межсетевой Экран 1

IPSec-Интерфейс

В созданный ранее ipsec-интерфейс на вкладке **XAuth** добавить имя пользователя и пароль.

Веб-интерфейс:

Interfaces → IPsec → ipsec

The screenshot shows the Mikrotik WinBox configuration page for an IPsec tunnel named 'ipsec_tunnel'. The 'XAuth' tab is selected. Under the 'IKE XAuth' section, the option 'Pass username and password to peer via IKE XAuth, if the remote gateway requires it' is selected. The 'Username' field contains 'olga', and the 'Password' and 'Confirm Password' fields are masked with dots. A note states: 'Note! Existing passwords will always be shown with 8 characters to hide the actual length.' The 'OK' and 'Cancel' buttons are visible at the bottom right.

Командная строка:

```
set Interface IPsecTunnel ipsec_tunnel XAuth=PassToPeerGateway  
XAuthUsername=olga XAuthPassword=qwerty
```

Межсетевой Экран 2

IPSec-Интерфейс

В созданный ранее ipsec-интерфейс на вкладке **XAuth** добавить требование аутентификации пользователя.

Веб-интерфейс:

Interfaces → IPsec → IPsec_tunnel

The screenshot shows the Mikrotik WinBox configuration page for an IPsec tunnel named 'ipsec_tunnel'. The 'XAuth' tab is selected. Under the 'IKE XAuth' section, the option 'Require IKE XAuth user authentication for inbound IPsec tunnels' is selected. The 'Username', 'Password', and 'Confirm Password' fields are empty. A note states: 'Note! Existing passwords will always be shown with 8 characters to hide the actual length.' The 'OK' and 'Cancel' buttons are visible at the bottom right.

Командная строка:

```
set Interface IPsecTunnel ipsec_tunnel XAuth=RequiredForInbound
```

Аутентификация на уровне пользователя

Создать локальную БД пользователей и пользователя с тем же именем и паролем, которые были указаны на вкладке **XAuth** Межсетевого Экрана 1.

Веб-интерфейс:

User Authentication → Local User Databases → Add → Local User Database

The screenshot shows the configuration window for a local user database named 'ipsec_users'. The 'General' tab is selected. The 'Name' field is filled with 'ipsec_users'. The 'Comments' field is empty. The window has 'OK' and 'Cancel' buttons at the bottom right.

The screenshot shows the configuration window for a user named 'olga'. The 'General' tab is selected. The 'Name' field is filled with 'olga'. The 'Password' and 'Confirm Password' fields are filled with eight dots. A note states: 'Note! Existing passwords will always be shown with 8 characters to hide the actual length.' Below the password fields, there is a 'Groups' field and two buttons: 'Add administrators' and 'Add auditors'. The 'Per-user IP Configuration (for PPTP, L2TP and SSL VPN)' section has three dropdown menus: 'Static Client IP Address' (None), 'Networks behind user' (None), and 'Metric for networks'. The 'Comments' field is empty. The window has 'OK' and 'Cancel' buttons at the bottom right.

Командная строка:

```
add LocalUserDatabase ipsec_users
```

```
add User olga Password=qwerty
```

Создать правило аутентификации пользователей.

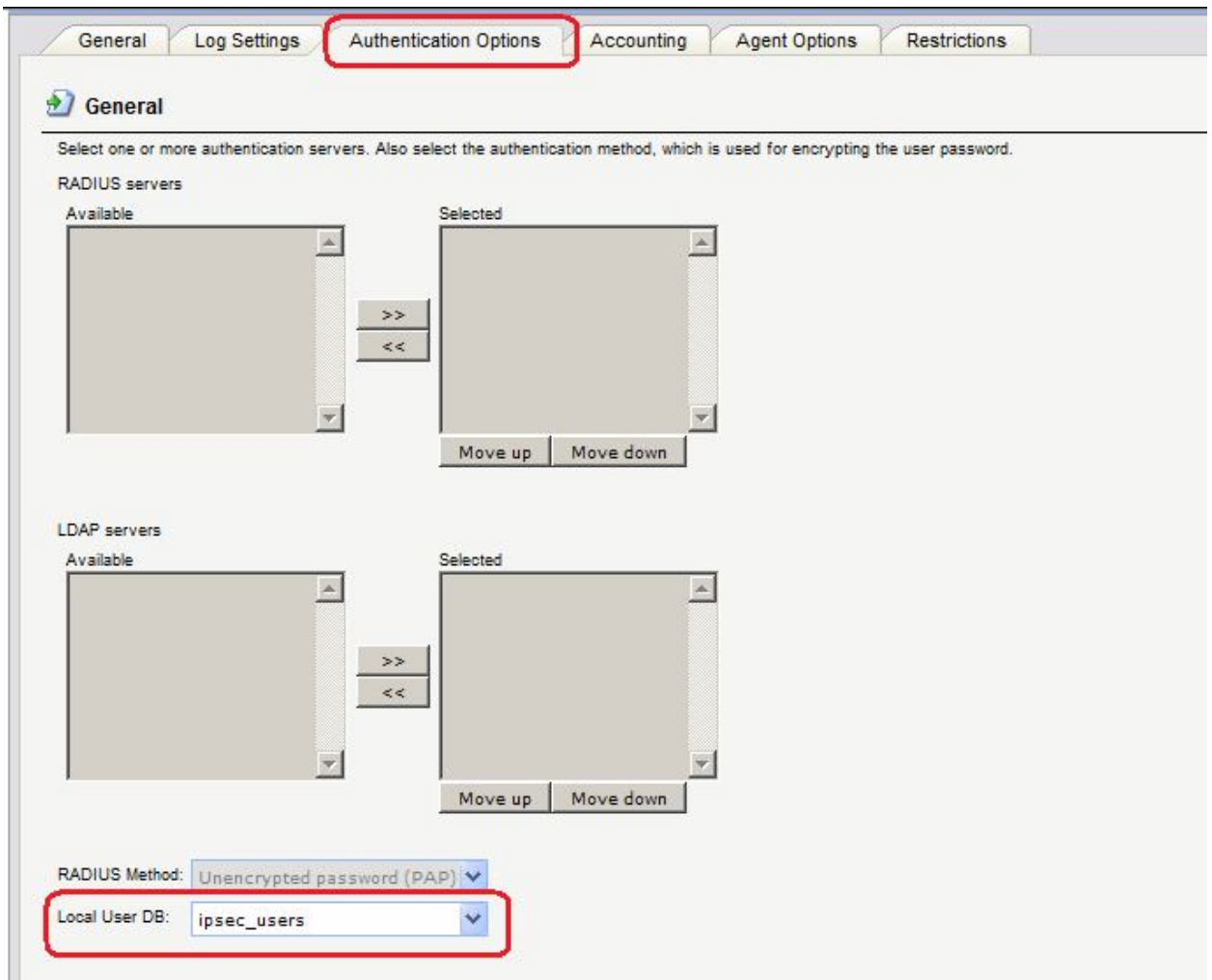
Веб-интерфейс:

User Authentication → User Authentication Rules → Add → User Authentication Rule

На вкладке **General** указать тип используемой базы данных, для какого протокола используется аутентификация и IP-адрес удаленного физического интерфейса.

The screenshot shows the configuration window for 'ipsec_rules'. The 'General' tab is selected. The 'Name' field contains 'ipsec_rules'. The 'Authentication agent' dropdown menu is set to 'XAuth'. The 'Authentication Source' dropdown menu is set to 'Local'. The 'Interface' dropdown menu is set to '(None)'. The 'Originator IP' dropdown menu is set to 'wan2_gw'. The 'Terminator IP' dropdown menu is set to '(None)'. A tooltip for 'Originator IP' states: 'For XAuth and PPP, this is the tunnel originator IP.' There is a 'Comments' section with an empty text area. 'OK' and 'Cancel' buttons are at the bottom right.

На вкладке **Authentication Options** указать локальную базу данных.



Командная строка:

```
add UserAuthRule AuthSource=Local OriginatorIP=wan2/wan2_gw  
LocalUserDB=ipsec_users Agent=XAuth Name=ipsec_rules
```

Проверка конфигурации

На МЭ 1 выполнить команду `ikesnoop`, которая позволяет отслеживать состояние IKE SA.


```
2014-04-22 13:59:34: IkeSnoop: Received IKE packet from 192.168.20.10:500
Exchange type : Identity Protection (main mode) 1 >
Payloads:
SA (Security Association)
VID (Vendor ID)
VID (Vendor ID)

2014-04-22 13:59:34: IkeSnoop: Sending IKE packet to 192.168.20.10:500
Exchange type : Identity Protection (main mode) < 1
Payloads:
SA (Security Association)
VID (Vendor ID)
VID (Vendor ID)

2014-04-22 13:59:34: IkeSnoop: Received IKE packet from 192.168.20.10:500
Exchange type : Identity Protection (main mode) 2 >
Payloads:
KE (Key Exchange)
NONCE (Nonce)

2014-04-22 13:59:34: IkeSnoop: Sending IKE packet to 192.168.20.10:500
Exchange type : Identity Protection (main mode) < 2
Payloads:
KE (Key Exchange)
NONCE (Nonce)

2014-04-22 13:59:35: IkeSnoop: Received IKE packet from 192.168.20.10:500
Exchange type : Identity Protection (main mode) 3 >
Payloads:
ID (Identification)
HASH (Hash)
N (Notification)

2014-04-22 13:59:35: IkeSnoop: Sending IKE packet to 192.168.20.10:500
Exchange type : Identity Protection (main mode) 3 <
Payloads:
ID (Identification)
HASH (Hash)
```

```

2014-04-22 13:59:35: IkeSnoop: Received IKE packet from 192.168.20.10:500
Exchange type : CFG mode 4 >
Payloads:
HASH (Hash)
CfgMode Attribute

2014-04-22 13:59:35: IkeSnoop: Sending IKE packet to 192.168.20.10:500
Exchange type : CFG mode < 4
Payloads:
HASH (Hash)
CfgMode Attribute

2014-04-22 13:59:35: IkeSnoop: Received IKE packet from 192.168.20.10:500
Exchange type : CFG mode 5 >
Payloads:
HASH (Hash)
CfgMode Attribute

2014-04-22 13:59:35: IkeSnoop: Received IKE packet from 192.168.20.10:500
Exchange type : Quick mode < 5
Payloads:
HASH (Hash)
SA (Security Association)
NONCE (Nonce)
ID (Identification)
ID (Identification)

2014-04-22 13:59:35: IkeSnoop: Sending IKE packet to 192.168.20.10:500
Exchange type : Quick mode 6 >
Payloads:
HASH (Hash)
SA (Security Association)
NONCE (Nonce)
ID (Identification)
ID (Identification)

2014-04-22 13:59:35: IkeSnoop: Received IKE packet from 192.168.20.10:500
Exchange type : Quick mode < 6

```

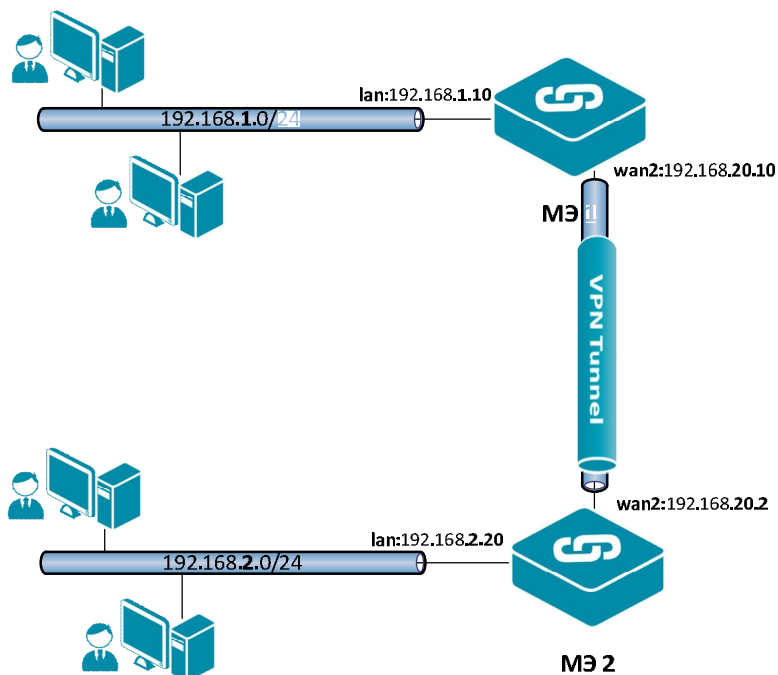
При использовании аутентификации по стандарту XAuth инициатором создания соединения всегда должна быть аутентифицируемая сторона (в нашем случае МЭ 1). В этом случае Инициатор до выполнения **Quick mode** использует **CFG mode** для передачи имени пользователя и пароля (транзакции 4 и 5), и только после этого выполняется **Quick mode** (транзакции 6). Если инициатором установления соединения является аутентифицирующая сторона (в нашем случае МЭ 2), то после **Main/Aggressive mode** сразу начинает выполняться **Quick mode**, и аутентификации на уровне пользователя не происходит. В дальнейшем установленные таким образом SA могут использоваться аутентифицируемой стороной без выполнения IKE с **CFG mode** и, соответственно, без аутентификации пользователя. Для предотвращения этого на аутентифицирующей стороне не следует использовать правила фильтрации, разрешающие установление соединения с аутентифицирующей стороны

Лабораторная работа 4. Соединение двух межсетевых экранов протоколом IPSec в транспортном режиме, аутентификация с использованием общего секрета

Цель

Обеспечить безопасность трафика только между двумя межсетевыми экранами. В этом случае следует поднять VPN с использованием семейства протоколов IPSec в транспортном режиме.

Топология сети



Топология аналогична топологии в предыдущей лабораторной работе. Между интерфейсами `wan1` на МЭ 1 и МЭ 2 требуется поднять VPN/IPSec в транспортном режиме.

Описание практической работы

Создать IPSec-туннель и политики доступа, которые разрешают доступ между межсетевыми экранами 1 и 2 по этому туннелю.

Межсетевой Экран 1

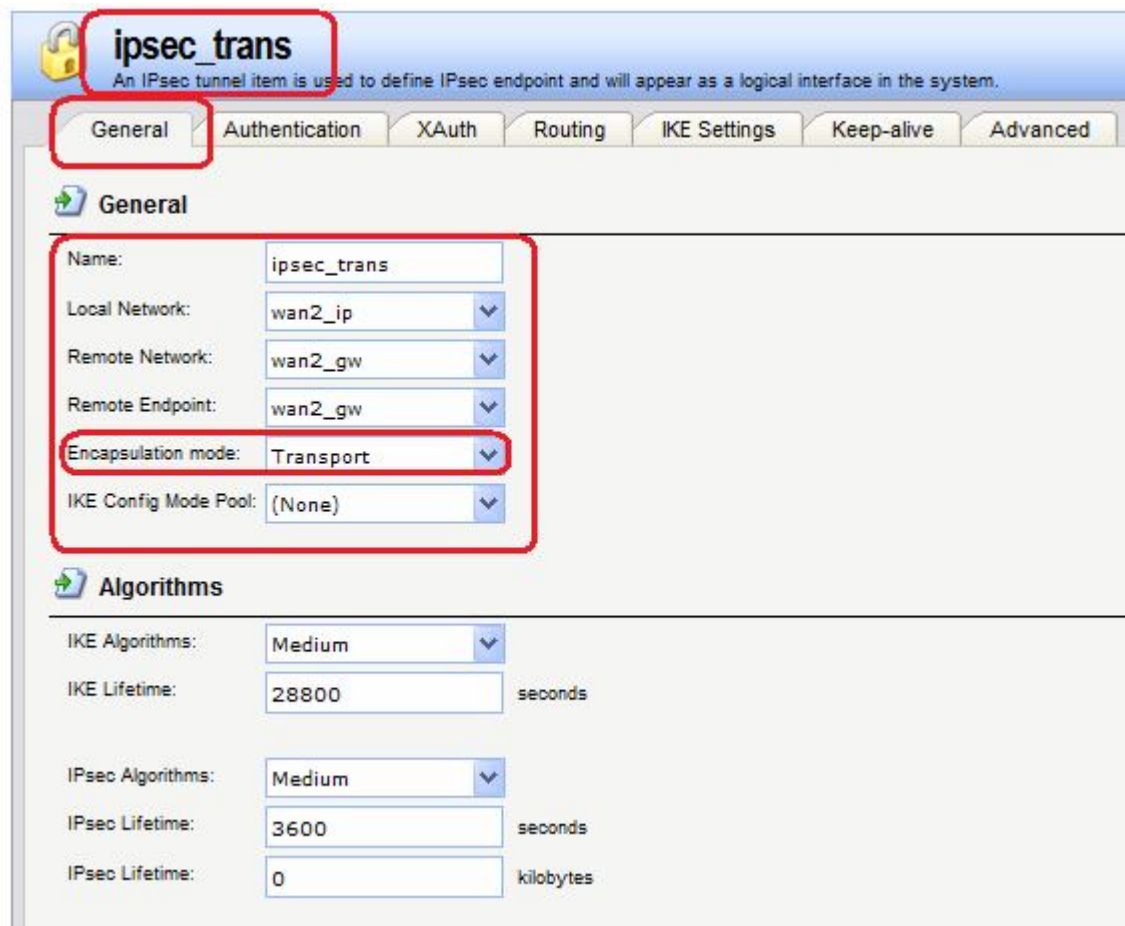
IPSec-Интерфейс

Создать IPSec-интерфейс в транспортном режиме.

Веб-интерфейс:

`Interfaces` → `IPsec` → `Add` → `IPsec Tunnel`

На вкладке **General** указать конечные точки туннеля, а также режим выполнения IPSec и используемые наборы алгоритмов для IPSec и IKE.



На вкладке **Authentication** указать созданный в предыдущей лабораторной работе аутентификационный объект.

Командная строка:

```
add Interface IPsecTunnel ipsec LocalNetwork=wan2/wan2_ip
RemoteNetwork=wan2/wan2_gw AuthMethod=PSK PSK=forIPSec IKEAlgorithms=Medium
IPsecAlgorithms=Medium EncapsulationMode=Transport
RemoteEndpoint=wan2/wan2_gw
```

Правила фильтрации

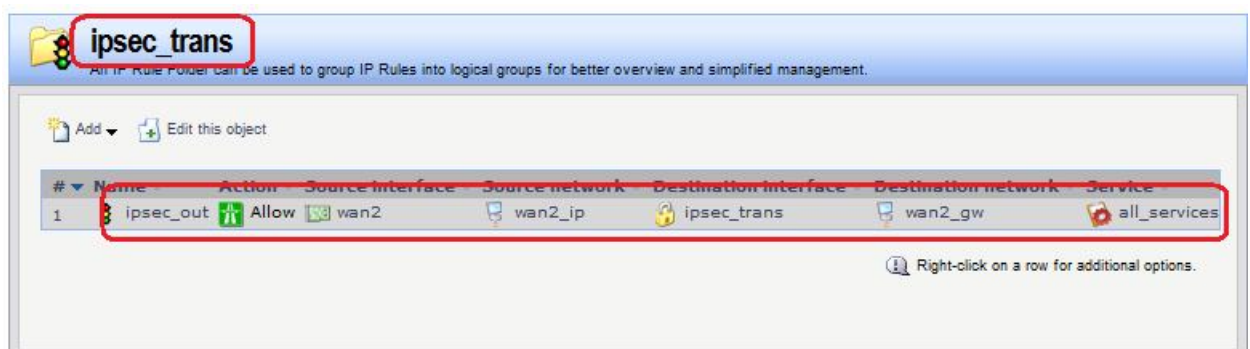
Определим правило, разрешающее исходящий трафик с МЭ 1 на МЭ 2.

Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: ipsec_trans

Rules → IP Rules → ipsec_trans



Командная строка:

```
add IPRuleFolder Name=ipsec_trans
cc IPRuleFolder <N folder>

add IPRule Action=Allow SourceInterface=wan2 SourceNetwork=wan2/wan2_ip
DestinationInterface=ipsec_trans DestinationNetwork=wan2/wan2_gw
Service=all_services Name=ipsec_out
```

Межсетевой Экран 2

IPSec-Интерфейс

Создать IPSec-интерфейс в транспортном режиме.

Веб-интерфейс:

Interfaces → IPsec → Add → IPsec Tunnel

На вкладке **General** указать конечные точки туннеля, а также режим выполнения IPSec и используемые наборы алгоритмов для IPSec и IKE.

The screenshot shows the Mikrotik WinBox web interface for configuring an IPsec tunnel. The page title is "ipsec_trans" and it includes a sub-header: "An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system." The interface has several tabs: "General", "Authentication", "XAuth", "Routing", "IKE Settings", "Keep-alive", and "Advanced". The "General" tab is selected and highlighted with a red box. Below the tabs, the "General" section contains several fields: "Name" (ipsec_trans), "Local Network" (wan2_ip), "Remote Network" (wan2_gw), "Remote Endpoint" (wan2_gw), "Encapsulation mode" (Transport), and "IKE Config Mode Pool" (None). The "Encapsulation mode" dropdown is highlighted with a red box. Below the "General" section is the "Algorithms" section, which includes: "IKE Algorithms" (Medium), "IKE Lifetime" (28800 seconds), "IPsec Algorithms" (Medium), "IPsec Lifetime" (3600 seconds), and "IPsec Lifetime" (0 kilobytes).

На вкладке **Authentication** указать созданный в предыдущей лабораторной работе аутентификационный объект.

Командная строка:

```
add Interface IPsecTunnel IPsec_trans LocalNetwork=wan2/wan2_ip
RemoteNetwork=wan2/wan2_gw AuthMethod=PSK PSK=forIPsec IKEAlgorithms=Medium
IPsecAlgorithms=Medium RemoteEndpoint=wan2/wan2_gw
```

Правила фильтрации

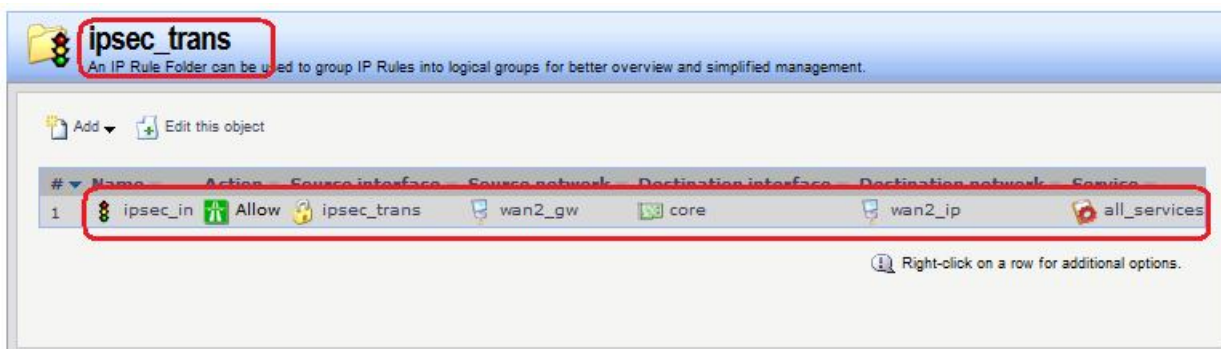
Определим правило, разрешающее входящий трафик с МЭ 1 на МЭ 2.

Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: ipsec_trans

Rules → IP Rules → ipsec_trans



Командная строка:

```
add IPRuleFolder Name=ipsec_trans
```

```
cc IPRuleFolder <N folder>
```

```
add IPRule Action=Allow SourceInterface=ipsec_trans  
SourceNetwork=wan2/wan2_gw DestinationInterface=core  
DestinationNetwork=wan2/wan2_ip Service=all_services Name=ipsec_in
```

Проверка конфигурации

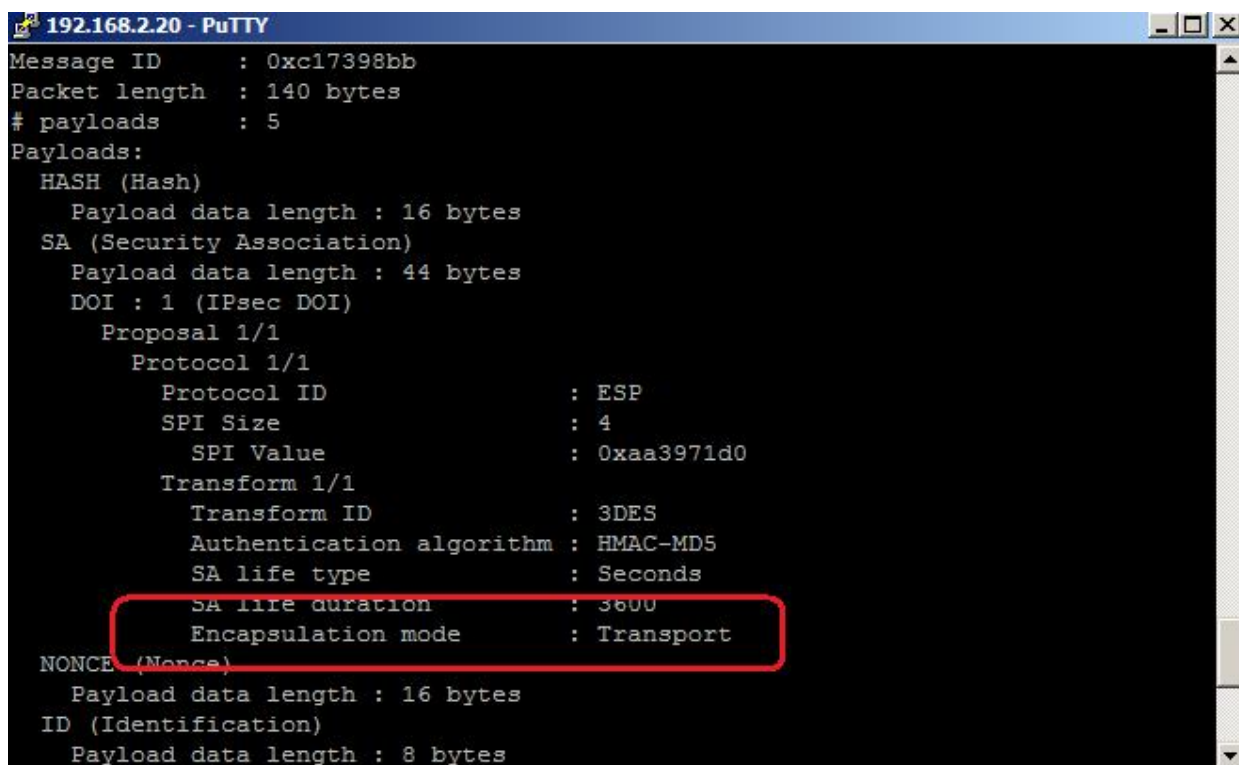
Выполнить команду

```
ikesnoop -on -verbose
```

на МЭ 1.

Выполнить команду ping на МЭ 2.

Команда `ikesnoop` должна показать, что выполняется IPsec в транспортном режиме.

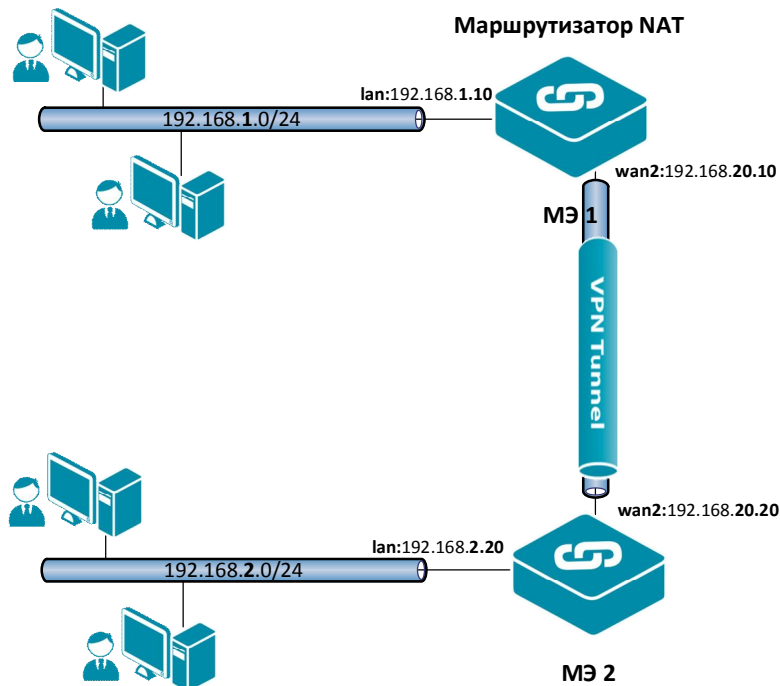


Лабораторная работа 5. Использование преобразования NAT в протоколе IPSec

Цель

Соединить две сети, расположенные за межсетевыми экранами, VPN с использованием семейства протоколов IPSec (Лабораторная работа 10). В этом случае необходимо использовать туннельный режим. На МЭ 1 должен выполняться NAT.

Топология сети



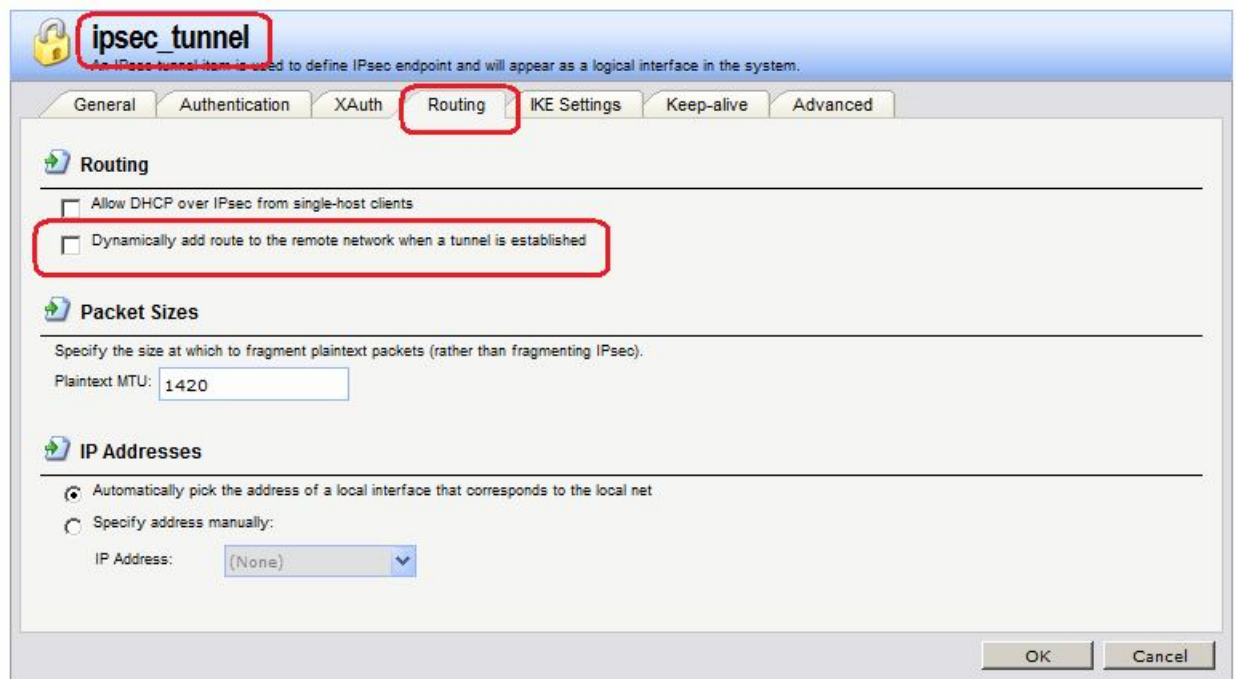
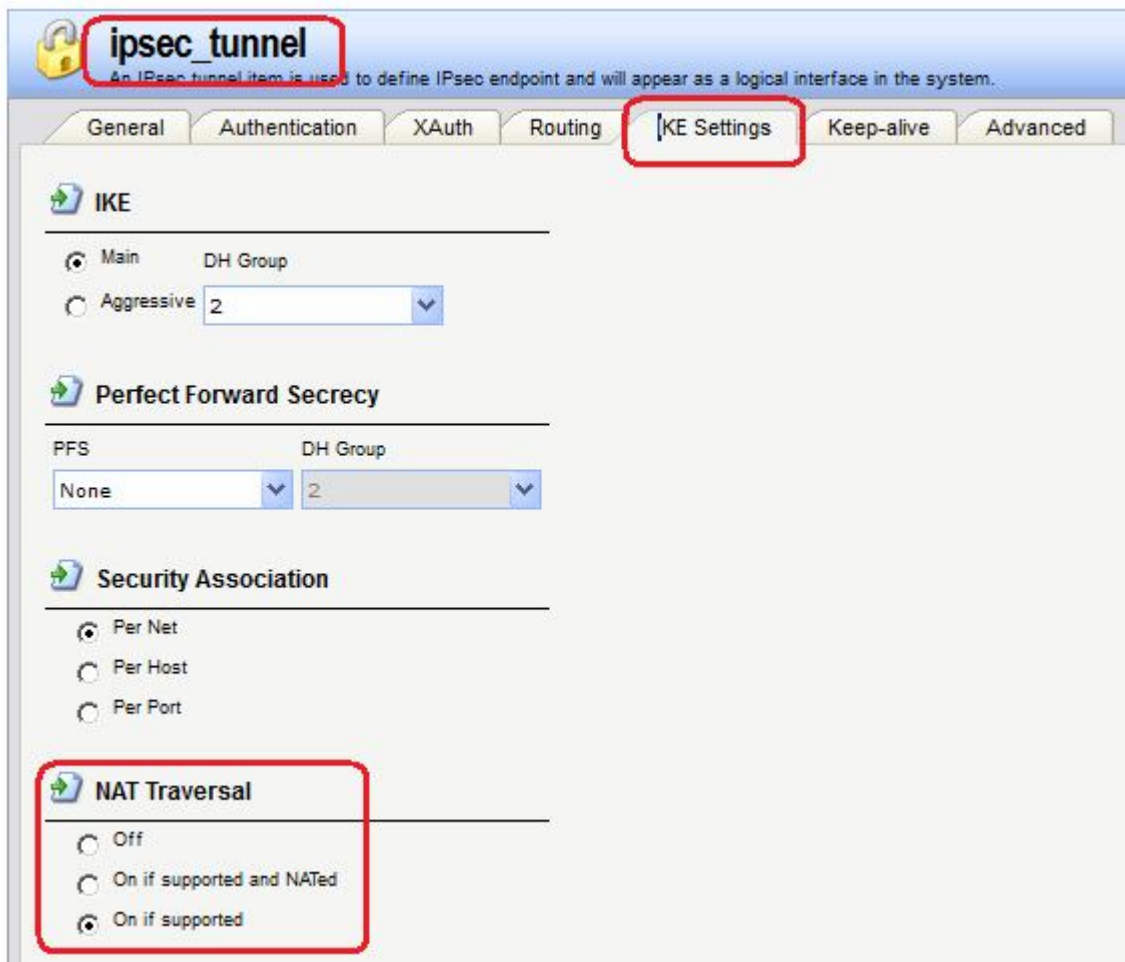
Описание практической работы

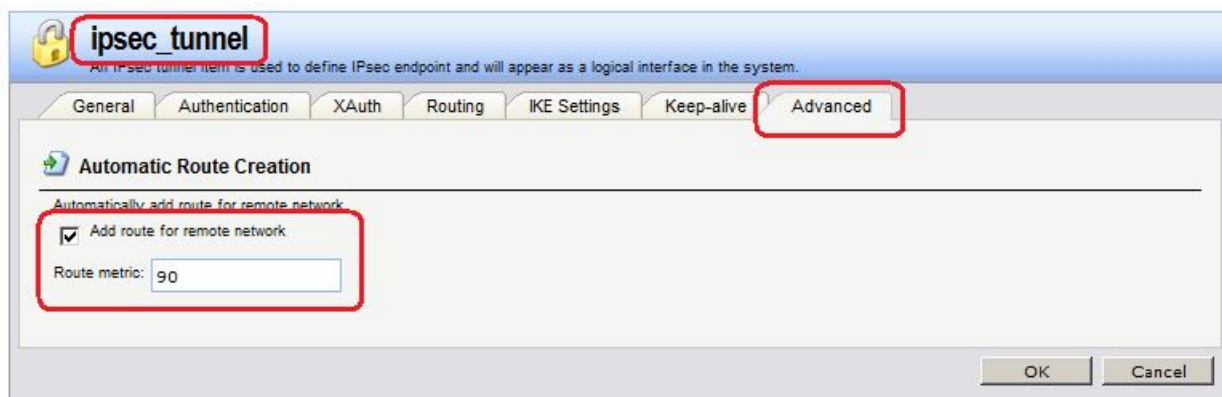
Межсетевой Экран 1

IPSec-Интерфейс

На IPSec-интерфейсе должна быть указана поддержка NAT. В этом случае инициатором установления туннеля всегда является хост, расположенный за NAT, поэтому для IPSec-интерфейса следует указать статическое добавление маршрута.

Веб-интерфейс:



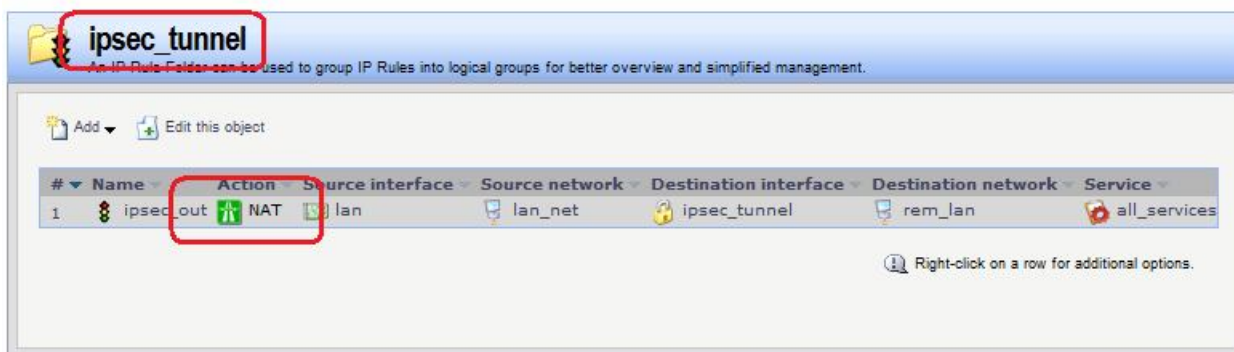


Командная строка:

```
set Interface IPsecTunnel ipsec_tunnel NATTraversal= AlwaysOn
AddRouteToRemoteNet=No AutoInterfaceNetworkRoute=Yes
```

Правила фильтрации

Вместо Правила **allow** следует указать правило **NAT**.



Межсетевой Экран 2

IPSec-Интерфейс

На IPSec-интерфейсе должна быть указана поддержка NAT. В этом случае инициатором установления туннеля всегда является хост, расположенный за NAT, поэтому для IPSec-интерфейса имеет смысл указать динамическое добавление маршрута.

Проверка конфигурации

Выполнить команду **ping** и проанализировать передаваемый трафик.

```

C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>ping 192.168.2.123

Pinging 192.168.2.123 with 32 bytes of data:
Reply from 192.168.2.123: bytes=32 time=2ms TTL=126
Reply from 192.168.2.123: bytes=32 time=1ms TTL=126
Reply from 192.168.2.123: bytes=32 time=1ms TTL=126
Reply from 192.168.2.123: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.123:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\Laponina>

```

Запишем дамп трафика в файлы и посмотрим его с помощью программы Wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.20.20	192.168.20.10	ESP	126	ESP (SPI=0x51ac7c46)
2	0.000000	192.168.20.10	192.168.20.20	ESP	126	ESP (SPI=0xf051d236)
3	0.070000	192.168.20.10	192.168.20.20	ISAKMP	122	Informational
4	10.010000	192.168.20.20	192.168.20.10	ISAKMP	202	Quick Mode
5	10.020000	192.168.20.10	192.168.20.20	ISAKMP	202	Quick Mode
6	10.020000	192.168.20.20	192.168.20.10	ISAKMP	106	Quick Mode
7	10.270000	192.168.20.20	192.168.20.10	ESP	126	ESP (SPI=0x702f0f3e)
8	10.270000	192.168.20.10	192.168.20.20	ESP	126	ESP (SPI=0xaf1edf49)
9	10.640000	192.168.20.20	192.168.20.10	ISAKMP	122	Informational
10	19.150000	192.168.20.10	192.168.20.20	ISAKMP	202	Quick Mode


```

# Frame 4: 202 bytes on wire (1616 bits), 202 bytes captured (1616 bits)
# Ethernet II, Src: D-Link_49:dd:03 (5c:d9:98:49:dd:03), Dst: D-Link_49:dc:ff (5c:d9:98:49:dc:ff)
# Internet Protocol Version 4, Src: 192.168.20.20 (192.168.20.20), Dst: 192.168.20.10 (192.168.20.10)
# User Datagram Protocol, Src Port: ipsec-nat-t (4500), Dst Port: ipsec-nat-t (4500)
# UDP Encapsulation of IPsec Packets
  Non-ESP Marker
# Internet Security Association and Key Management Protocol
  Initiator cookie: 7903e87930e63d13
  Responder cookie: 50a2ac2fab007f21
  Next payload: Hash (8)
  Version: 1.0
  Exchange type: quick Mode (32)
  Flags: 0x01
  Message ID: 0x90c12833
  Length: 156
  Encrypted Data (128 bytes)

```

На lan-интерфейсе трафик с измененным IP-адресом:

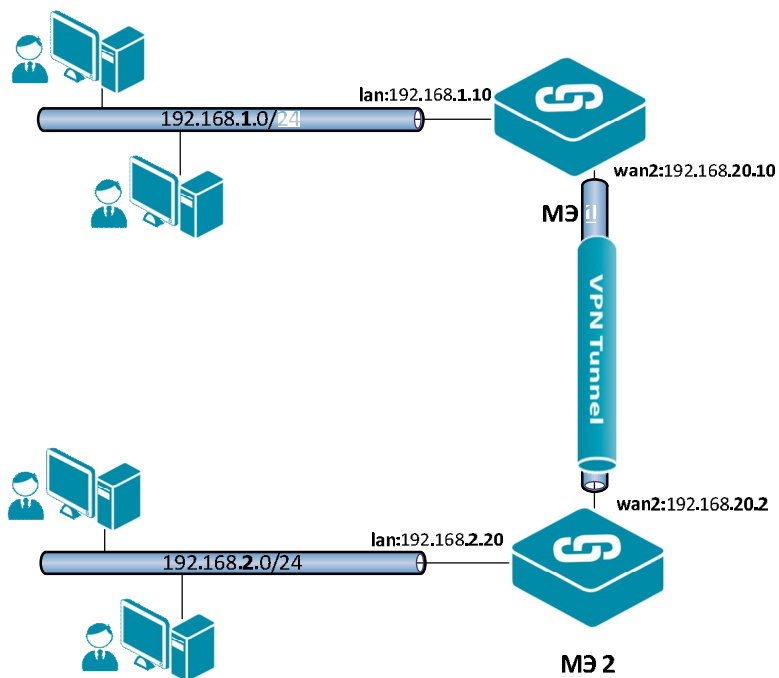
Time	Source	Destination	Protocol	Length	Info
1 0.000000	192.168.1.10	192.168.2.123	ICMP	74	Echo (ping) request id=0x8
2 0.000000	192.168.2.123	192.168.1.10	ICMP	74	Echo (ping) reply id=0x8
3 0.520000	192.168.1.10	192.168.2.123	ICMP	74	Echo (ping) request id=0x8

Лабораторная работа 6. Использование протокола DPD в протоколе IPSec

Цель

Соединить две сети, расположенные за межсетевыми экранами, VPN с использованием семейства протоколов IPSec в туннельном режиме. Дополнительно МЭ1 и МЭ2 используют протокол DPD для проверки жизнеспособности друг друга.

Топология сети



Топология аналогична топологии в предыдущей лабораторной работе. Между интерфейсами **wan2** на МЭ 1 и МЭ 2 требуется поднять VPN/IPSec. Жизнеспособность противоположной стороны необходимо проверять по протоколу DPD.

Описание практической работы

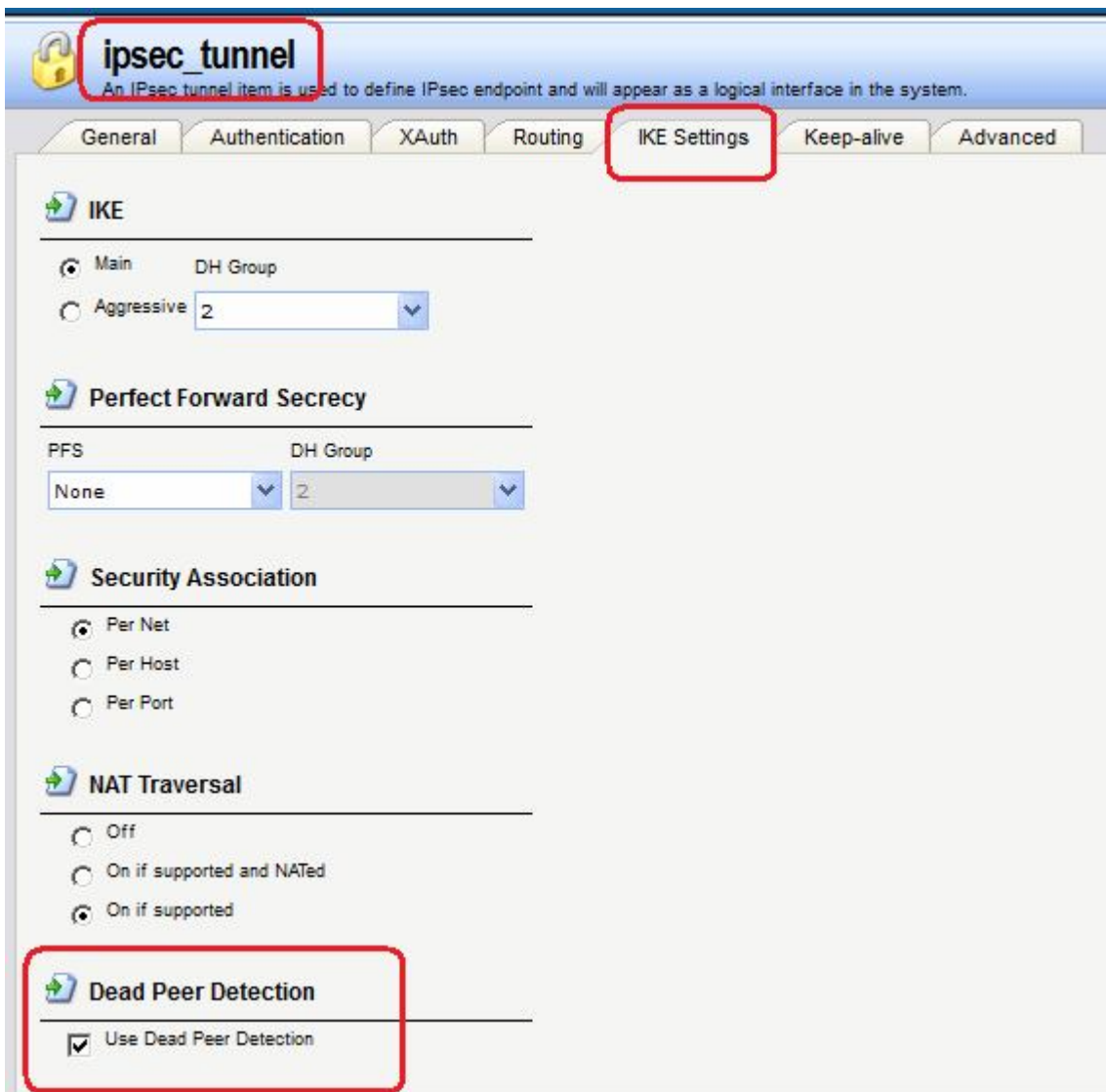
Межсетевой Экран 1

IPSec-Интерфейс

Установить использование протокола DPD.

Веб-интерфейс:

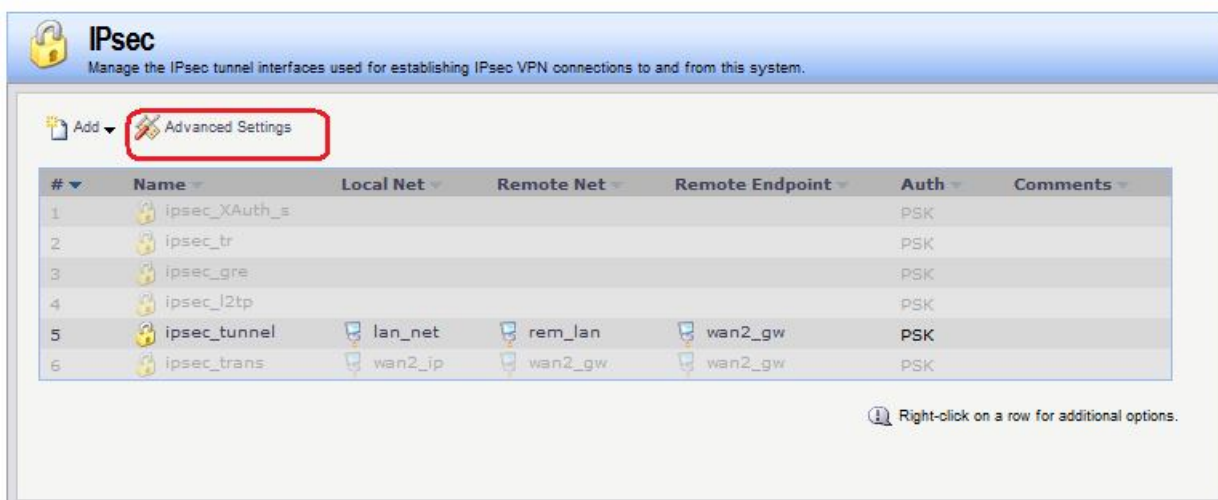
Interfaces → IPsec → ipsec



Командная строка:

```
set Interface IPsecTunnel ipsec_tunnel DeadPeerDetection=Yes
```

Настройки протокола DPD указываются в дополнительных установках (**Advanced Settings**).



Dead Peer Detection	
DPD Metric:	<input type="text" value="3"/> Metric 10s of seconds with no traffic or other evidence of life in tunnel before SA is removed.
Flow Metric:	<input type="text" value="15"/> Minimum number of seconds without data traffic in a flow to activate IKE DPD liveness checks from the corresponding IKE SA.
DPD no wait:	<input type="checkbox"/> Do not wait for 10 times the value of DPD Metric after the value of Flow Metric has expired without aliveness sign before activating IKE DPD.
DPD Keep Time:	<input type="text" value="2"/> Number 10s of seconds a SA will remain in dead cache after a delete. DPD will not trigger if peer already is cached as dead.
DPD Expire Time:	<input type="text" value="15"/> Number of seconds that DPD-R-U-THERE messages will be sent.

Межсетевой Экран 2

IPSec-Интерфейс

Если на МЭ 2 также необходима проверка жизнеспособности противоположной стороны, то необходимо сделать аналогичные изменения в настройках IPSec-интерфейса.

Проверка конфигурации

Запишем дамп трафика в файлы и посмотрим его с помощью программы Wireshark.

20	9.220000	192.168.20.10	192.168.20.20	ISAKMP	166 Identity Protection (Main Mode)
21	9.220000	192.168.20.20	192.168.20.10	ISAKMP	166 Identity Protection (Main Mode)
22	9.240000	192.168.20.10	192.168.20.20	ISAKMP	222 Identity Protection (Main Mode)
23	9.300000	192.168.20.20	192.168.20.10	ISAKMP	222 Identity Protection (Main Mode)
24	9.320000	192.168.20.10	192.168.20.20	ISAKMP	118 Identity Protection (Main Mode)
25	9.320000	192.168.20.20	192.168.20.10	ISAKMP	118 Identity Protection (Main Mode)
26	9.330000	192.168.20.10	192.168.20.20	ISAKMP	198 Quick Mode
27	9.330000	192.168.20.20	192.168.20.10	ISAKMP	198 Quick Mode
28	9.330000	192.168.20.10	192.168.20.20	ISAKMP	102 Quick Mode
29	9.500000	192.168.20.10	192.168.20.20	ESP	134 ESP (SPI=0x31c67c63)

```

Frame 20: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits) on interface 0
Ethernet II, Src: D-Link_49:dc:ff (5c:d9:98:49:dc:ff), Dst: D-Link_49:dd:03 (5c:d9:98:49:dd:03)
Internet Protocol Version 4, Src: 192.168.20.10 (192.168.20.10), Dst: 192.168.20.20 (192.168.20.20)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: f53a00b94733dae5
  Responder cookie: 0000000000000000
  Next payload: Security Association (1)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 124
  Type Payload: Security Association (1)
  Type Payload: Vendor ID (13) : Unknown Vendor ID
  Type Payload: Vendor ID (13) : RFC 3706 DPD (Dead Peer Detection)
  
```

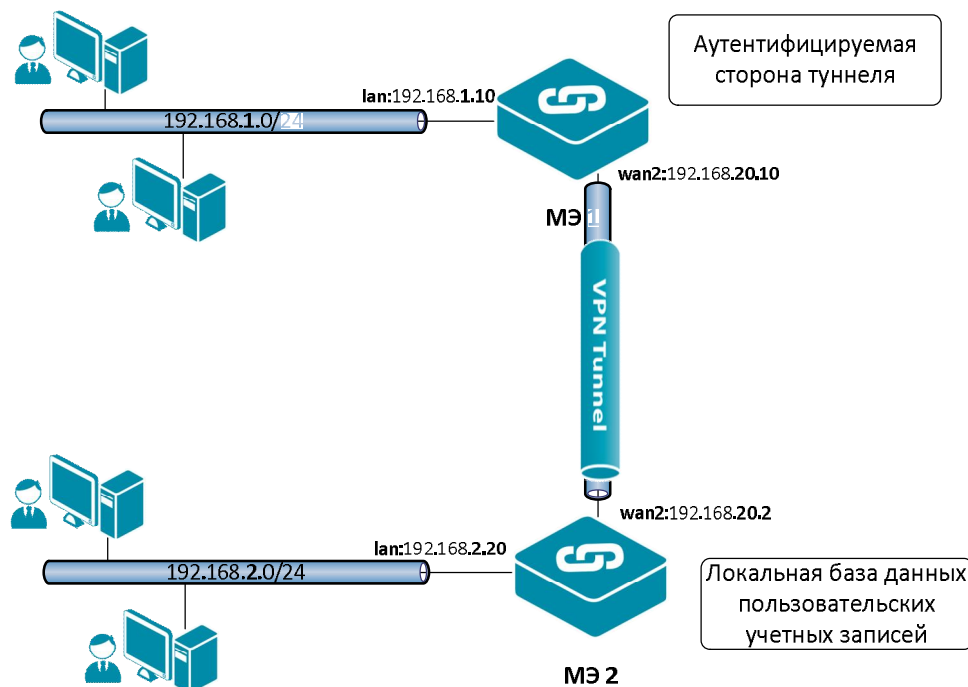
Лабораторная работа 7. Соединение двух локальных сетей протоколом L2TP, аутентификация с использованием общего секрета

Цель

Соединить два межсетевых экрана VPN с использованием протокола L2TP.

Топология сети аналогична топологии VPN/IPSec.

Топология сети



Между интерфейсами **wan1** на МЭ 1 и МЭ 2 требуется поднять VPN/L2TP.

Описание практической работы

Создать статическую маршрутизацию и политики доступа, которые разрешают доступ между локальными сетями, расположенными за межсетевыми экранами. При этом трафик между МЭ 1 и МЭ 2 проходит по VPN/L2TP.

Межсетевой Экран 1

Межсетевой Экран 1 является клиентом, т.е. в его конфигурации следует указать имя пользователя и пароль.

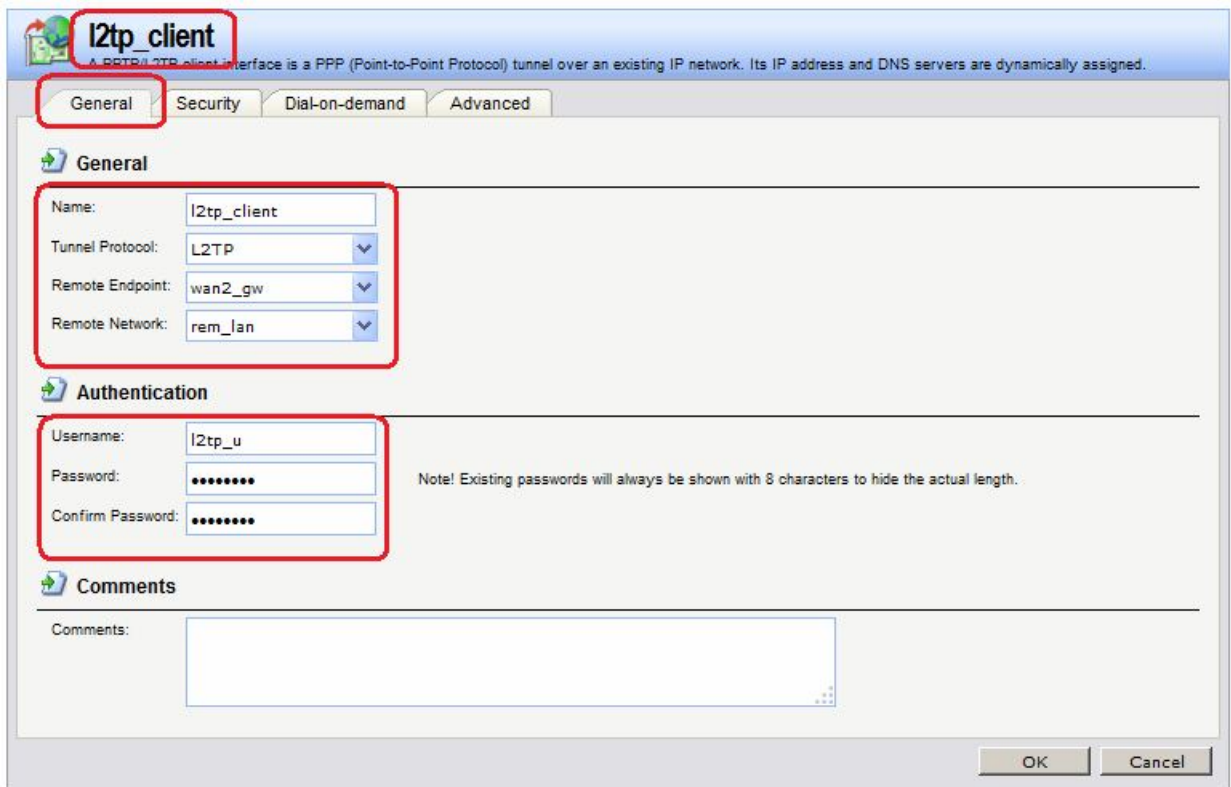
L2TP-Интерфейс

Веб-интерфейс:

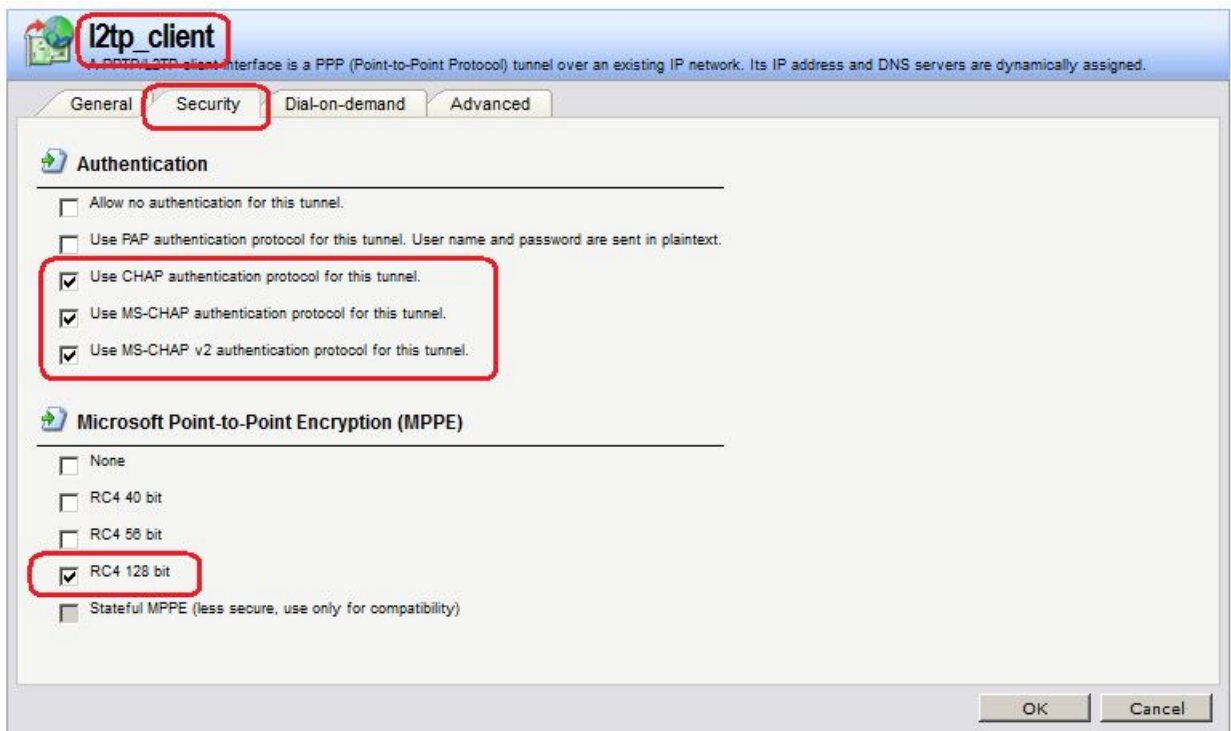
Interfaces → **PPTP/L2TP Clients** → **Add** → **PPTP/L2TP Client**

На вкладке **General** указать туннелирующий протокол L2TP, адрес конечной точки и сеть, расположенную за туннелем.

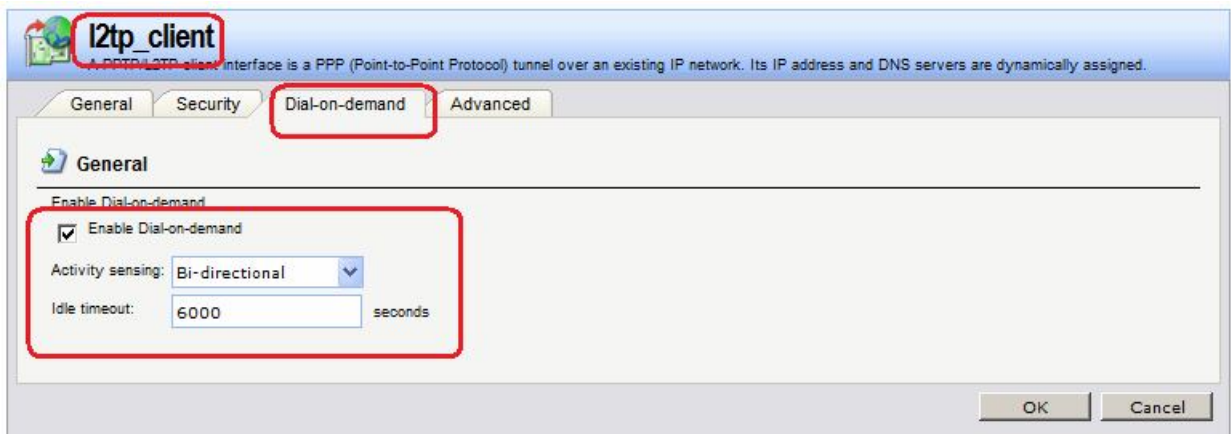
Также указать имя пользователя и пароль, созданные в базе данных на противоположной стороне туннеля.



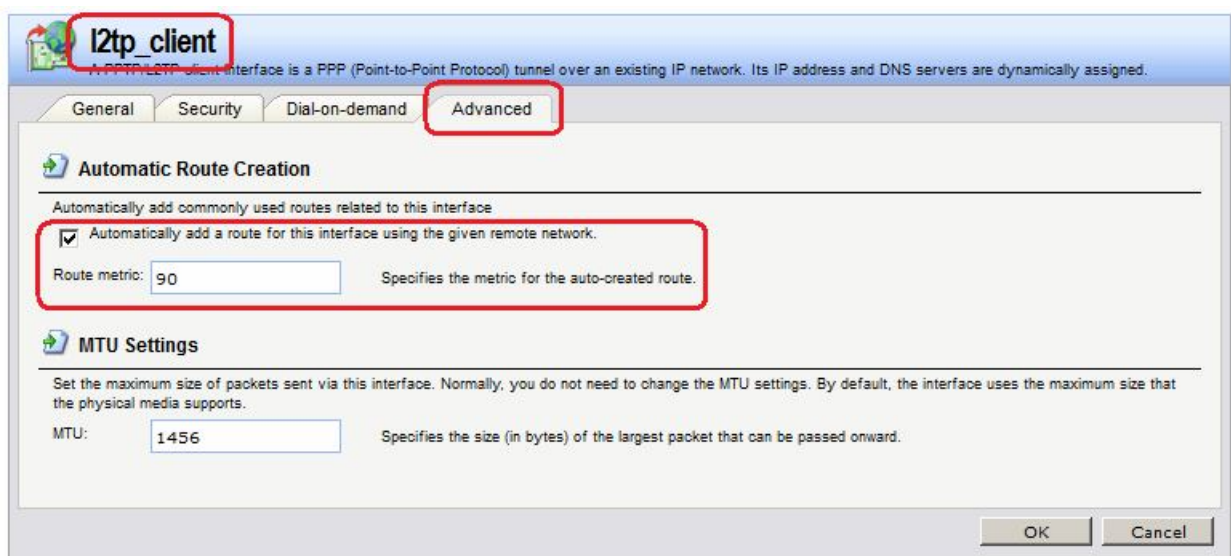
На вкладке **Security** указать параметры PPP-аутентификации и PPP-шифрования.



Если на вкладке **Dial-on-demand** установлен флаг **Enable Dial-on-demand**, то туннель будет установлен при появлении активности на стороне клиента и будет удален, если в течение указанного в параметре **Idle timeout** не было активности либо с обеих сторон, либо с одной из сторон, в зависимости от выбранной опции **Activity sensing**. Если флаг **Enable Dial-on-demand** не установлен, то туннель будет поднят всегда.



Если на вкладке **Advanced** установлен флаг **Automatically add a route for this interface using the given remote network**, то в таблицу маршрутизации **main** автоматически будет добавлен маршрут с указанной метрикой.



Командная строка:

```
add Interface L2TPClient l2tp_client Network=remote/rem_lan
RemoteEndpoint=wan2/wan2_gw Username=l2tp_u Password=qwerty
TunnelProtocol=L2TP
```

Правила фильтрации

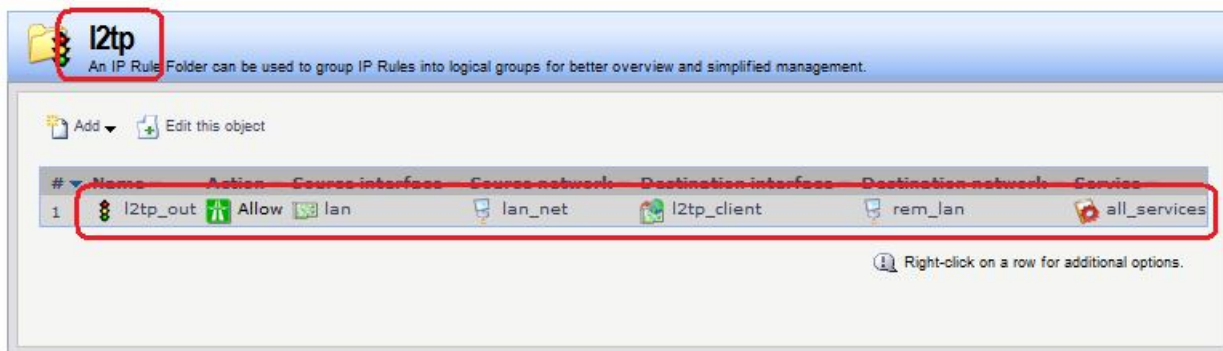
Разрешим трафик от сети, расположенной за межсетевым экраном, выполняющим роль L2TP-клиента, к сети, расположенной за межсетевым экраном, выполняющим роль L2TP-сервера.

Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: l2tp

Rules → IP Rules → l2tp → Add



Командная строка:

```
add IPRuleFolder Name=l2tp
cc IPRuleFolder <N folder>
add IPRule Action=Allow SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=l2tp_int DestinationNetwork=remote/rem_lan
Service=all_services Name=l2tp_out
```

Если требуется, чтобы у удаленного пользователя IP-адрес назначался L2TP-Сервером, то на стороне L2TP-Клиента в Правилах фильтрации указывается правило **NAT**.

На стороне клиента следует задать тот же пул IP-адресов, который задан на стороне сервера для L2TP-клиента.

Межсетевой Экран 2

Межсетевой Экран 2 является сервером, т.е. на нем надо создать не только интерфейс L2TP, но и БД учетных записей пользователей.

Объекты Адресной Книги

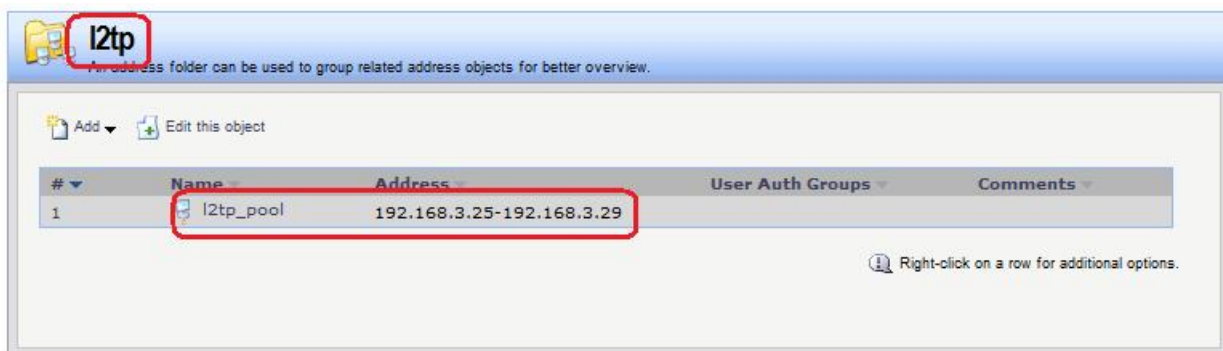
Создать пул IP-адресов.

Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: l2tp

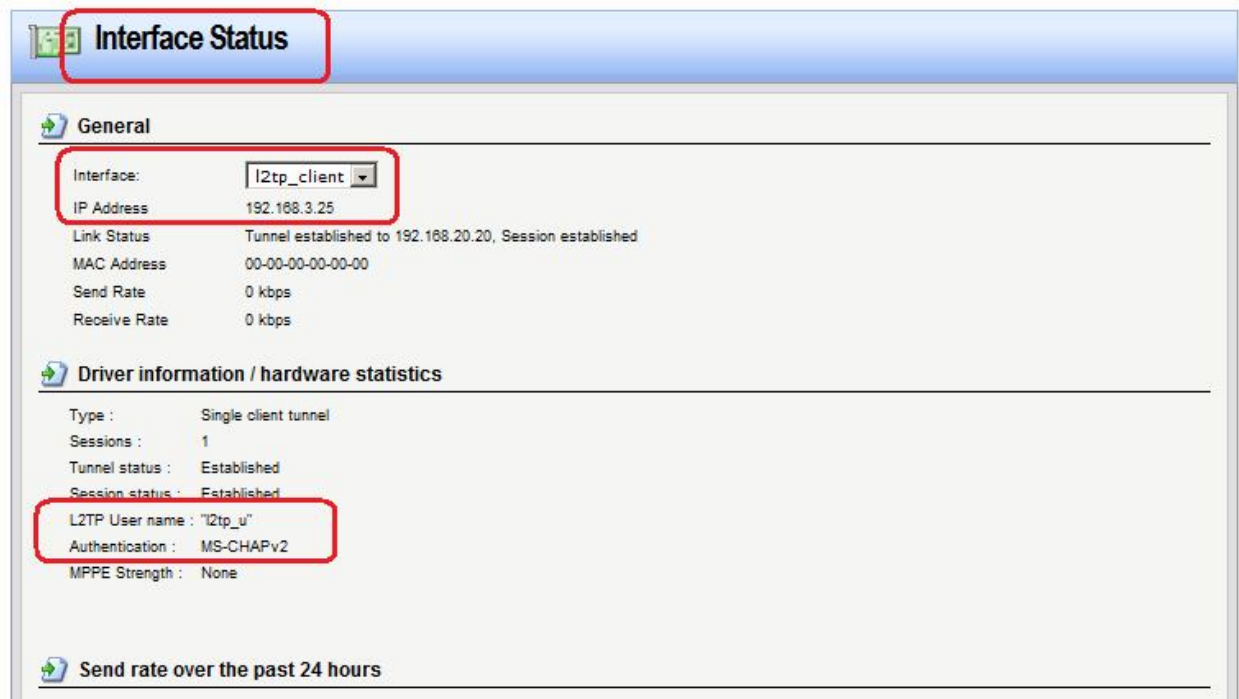
Object → Address Book → l2tp → Add



Командная строка:

```
add Address AddressFolder l2tp
cc Address AddressFolder l2tp
add IP4Address l2tp_pool Address=192.168.3.25-192.168.3.29
```

IP-адреса из этого пула будут выдаваться L2TP-клиенту, т.е. L2TP-интерфейсу на МЭ 1:

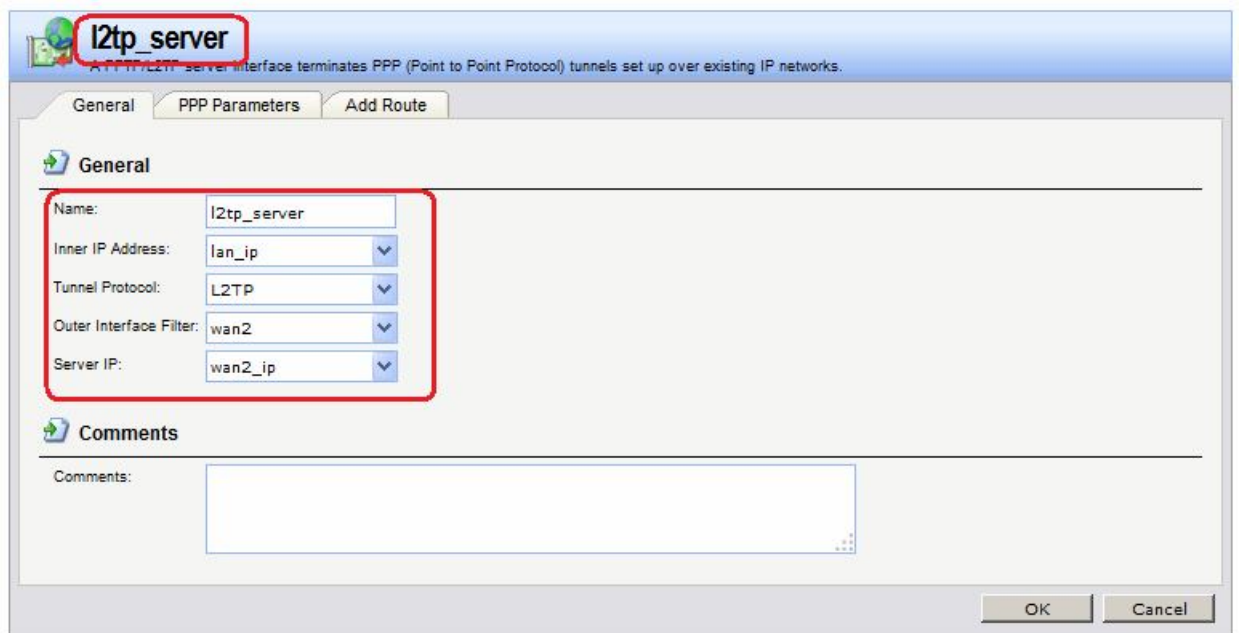


L2TP-Интерфейс

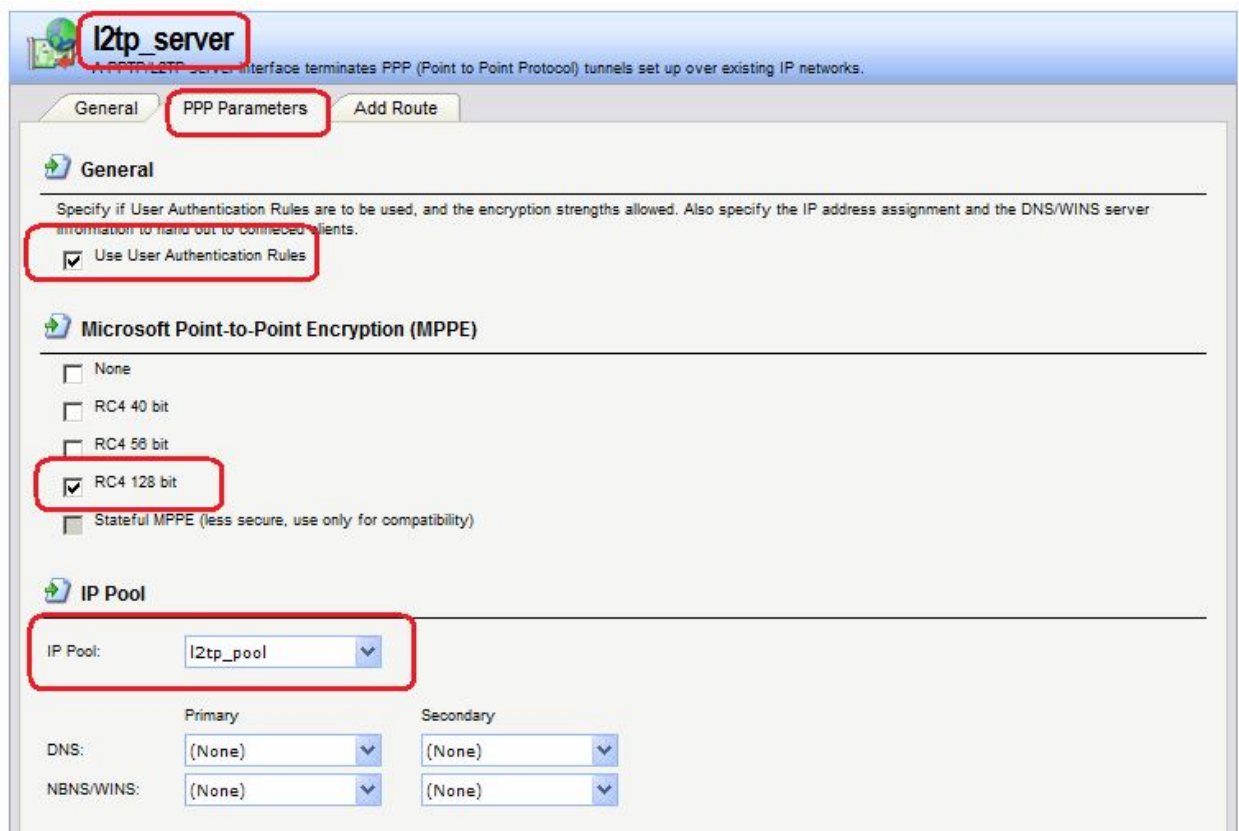
Веб-интерфейс:

Interfaces → PPTP/L2TP Servers → Add → PPTP/L2TP server

На вкладке **General** указываются параметры туннеля.



На вкладке **PPP Parameters** указываются параметры PPP-шифрования и пул IP-адресов, из которого будут выдаваться IP-адреса клиенту.



Командная строка:

```
add Interface L2TPServer l2tp_server Interface=wan2 IP=lan/lan_ip
ServerIP=wan2/wan2_ip IPPool=l2tp/l2tp_pool TunnelProtocol=L2TP
```

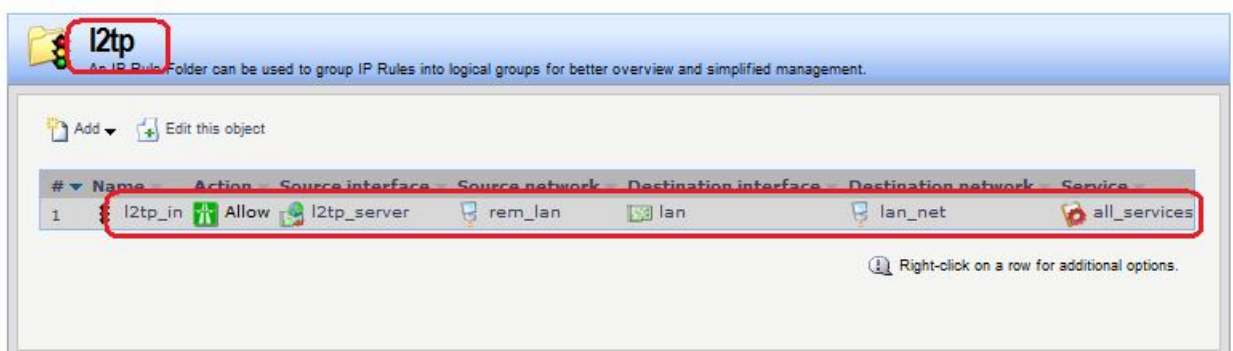
Правила фильтрации

Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: l2tp

Rules → IP Rules → l2tp → Add



Командная строка:

```
add IPRuleFolder Name=l2tp
```

```
cc IPRuleFolder <N folder>
```

```
add IPRule Action=Allow SourceInterface=l2tp_server
SourceNetwork=remote/rem_lan DestinationInterface=lan
DestinationNetwork=lan/lan_net Service=all_services Name=l2tp_in
```

Если у удаленного пользователя IP-адрес назначался L2TP-Сервером, то в Правилах фильтрации следует указать вместо удаленной сети пул выделяемых IP-адресов.

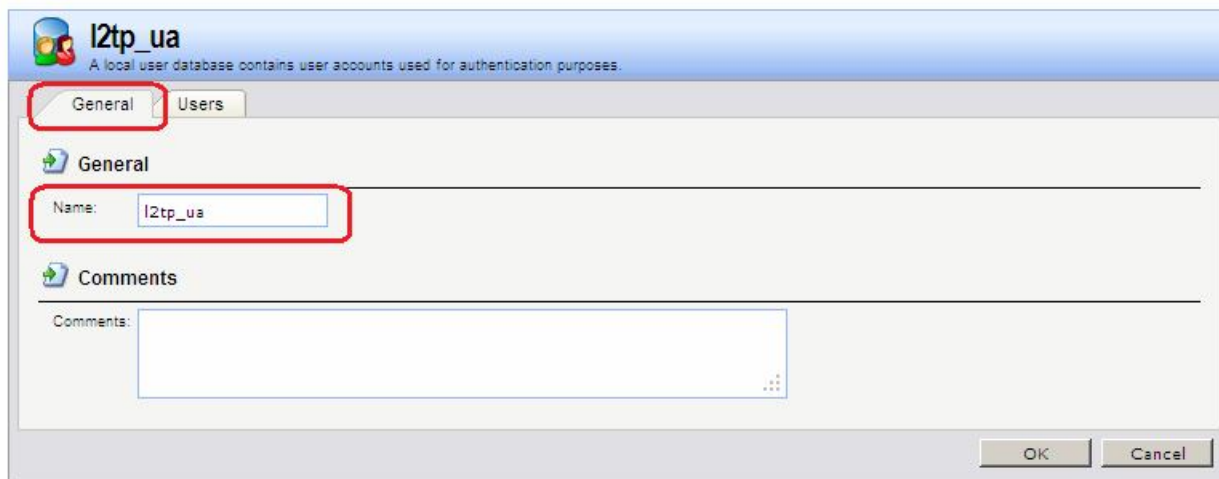
Аутентификация на уровне пользователя

Создать локальную базу данных пользователей.

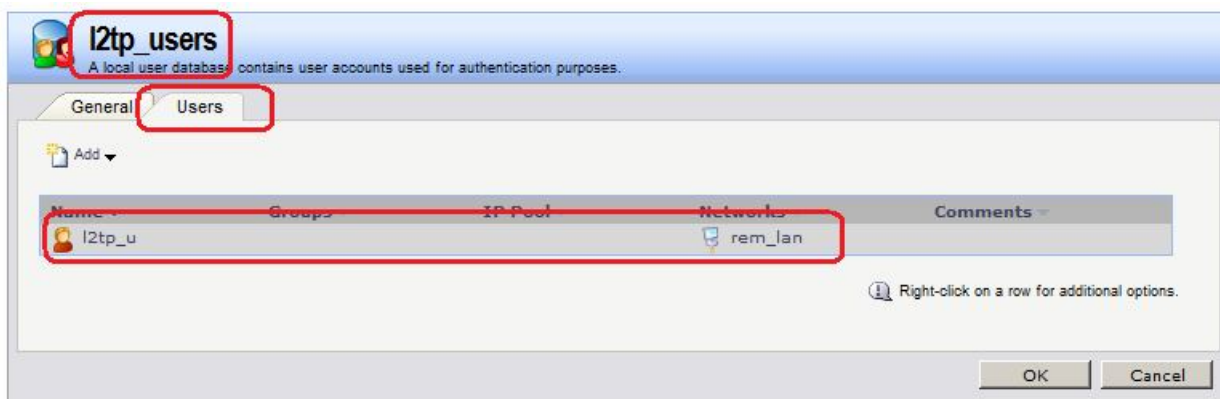
Веб-интерфейс:

User Authentication → Local User Databases → Add → Local User Database

На вкладке **General** указать имя базы данных.



На вкладке **Users** добавить учетные записи пользователей.



Командная строка:

```
add LocalUserDatabase I2tp_ua
```

```
add User olga Password=qwerty AutoAddRouteNet=remote/rem_lan
```

Создать правило аутентификации пользователей.

Веб-интерфейс:

User Authentication → User Authentication Rules → Add

Name: I2tp_rules

На вкладке **General** указать аутентификационный источник **Local** и необходимые для туннелирующего протокола опции. В нашем случае туннелирующим протоколом является L2TP.

l2tp_rules
The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

General Log Settings Authentication Options Accounting Agent Options Restrictions

General

Name: l2tp_rules

Authentication agent: L2TP/PPTP/SSL VP

Authentication Source: Local

Interface: l2tp_server

Originator IP: wan2_gw

Terminator IP: wan2_ip

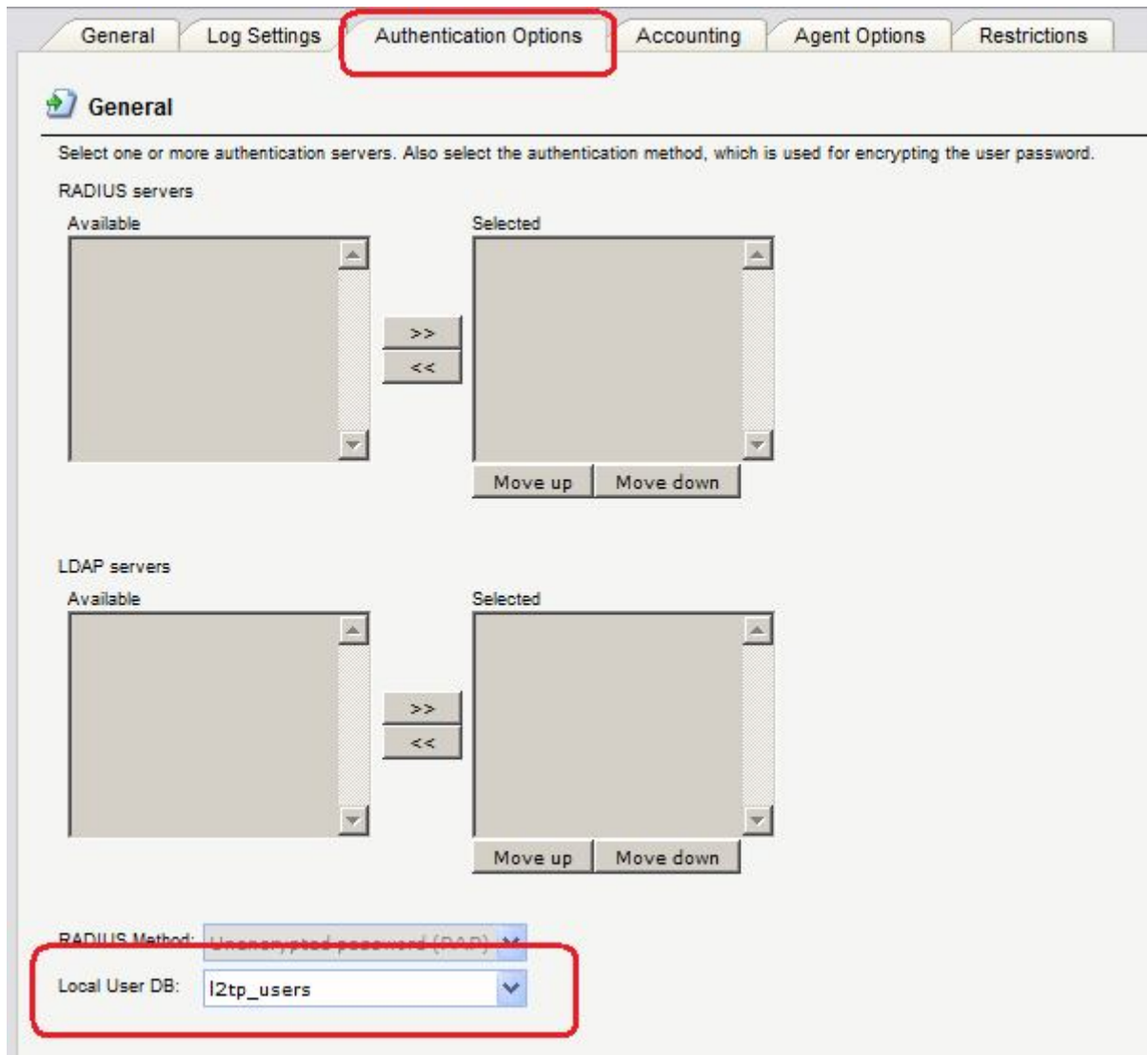
For XAuth and PPP, this is the tunnel originator IP.

Comments

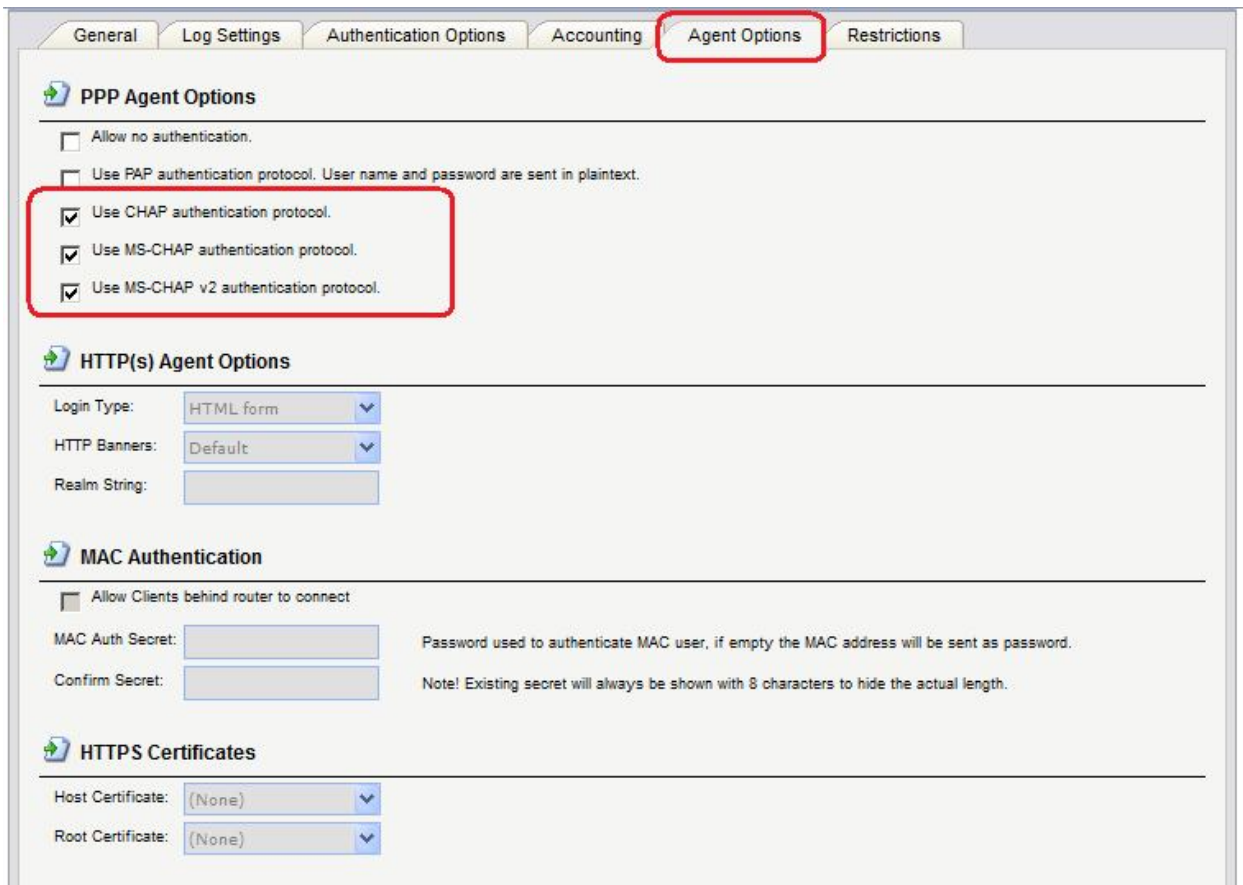
Comments:

OK

На вкладке **Authentication Options** указать имя локальной базы данных пользователей.



На вкладке **Agent Options** указать параметры PPP-аутентификации.

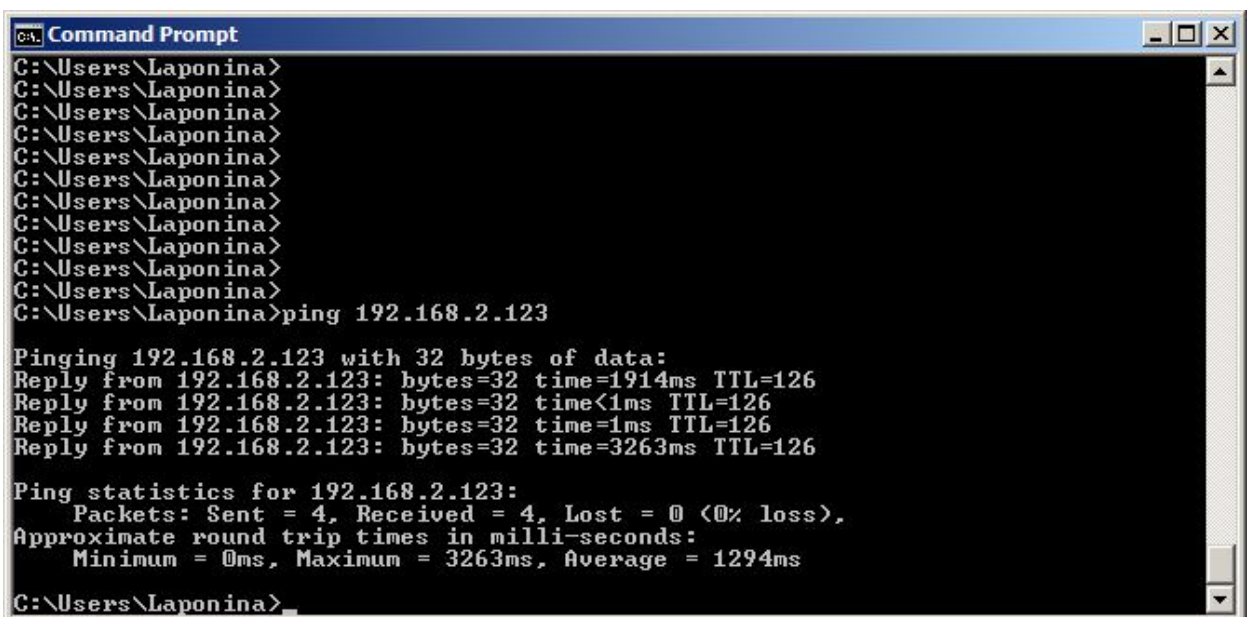


Командная строка:

```
add UserAuthRule AuthSource=Local Interface=l2tp_server LocalUserDB=l2tp_u
OriginatorIP=wan2/wan2_gw Agent=PPP TerminatorIP=wan2/wan2_ip Name=l2tp_rules
```

Проверка конфигурации

Выполнить команду ping.



На МЭ 2 в Статусах аутентификации пользователей должна появиться запись с именем пользователя, указанного в параметрах L2TP-клиента на противоположной стороне туннеля.

Username	IP Address	Interface	Session Timeout	Idle Timeout	Logged in as	Forcibly Log Out
l2tp_u	192.168.2.27	l2tp_server		29m		X

Дамп сетевого трафика на интерфейсе wan1 должен содержать команды протокола L2TP.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.20.10	192.168.20.20	PPP Comp	118	Compressed data
2	0.000000	192.168.20.20	192.168.20.10	PPP Comp	118	Compressed data
3	0.990000	192.168.20.10	192.168.20.20	PPP Comp	118	Compressed data
4	0.990000	192.168.20.20	192.168.20.10	PPP Comp	118	Compressed data
5	1.000000	192.168.20.10	192.168.20.20	L2TP	62	Control Message - Hello
6	1.000000	192.168.20.20	192.168.20.10	L2TP	60	Control Message - ZLB
7	1.990000	192.168.20.10	192.168.20.20	PPP Comp	118	Compressed data
8	1.990000	192.168.20.20	192.168.20.10	PPP Comp	118	Compressed data
9	2.990000	192.168.20.10	192.168.20.20	PPP Comp	118	Compressed data
10	2.990000	192.168.20.20	192.168.20.10	PPP Comp	118	Compressed data

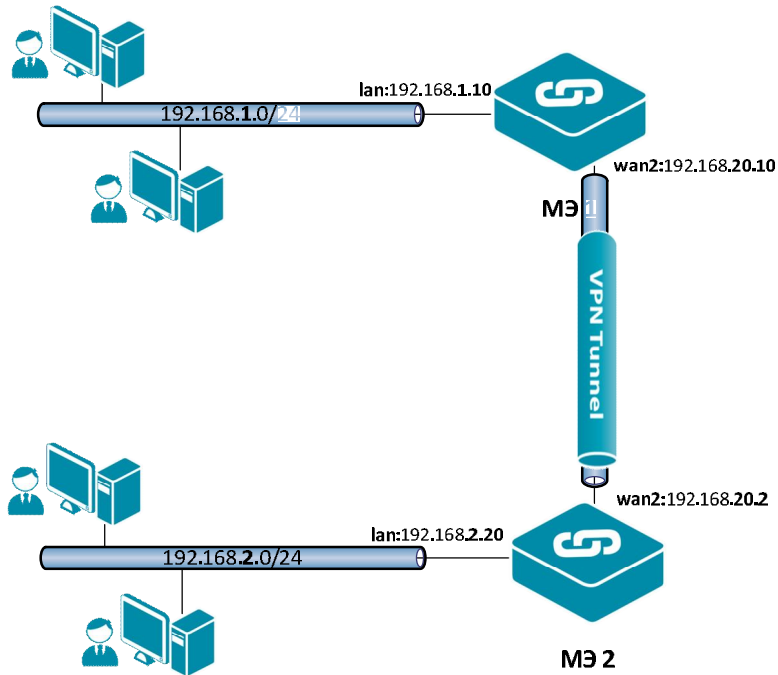
Лабораторная работа 8. Соединение двух локальных сетей протоколом GRE/IPSec в транспортном режиме

Цель

Соединить две сети, расположенные за межсетевыми экранами, VPN с использованием семейства протоколов IPSec. VPN с использованием IPSec будем создавать в транспортном режиме. Для туннеля между двумя локальными сетями будет использовать протокол GRE.

Топология сети аналогична топологии VPN/IPSec.

Топология сети



Описание практической работы

Межсетевой Экран 1

Аутентификационный Объект

Используем аутентификационный объект **Pre-Shared Key**, созданный в Лабораторной работе 9.

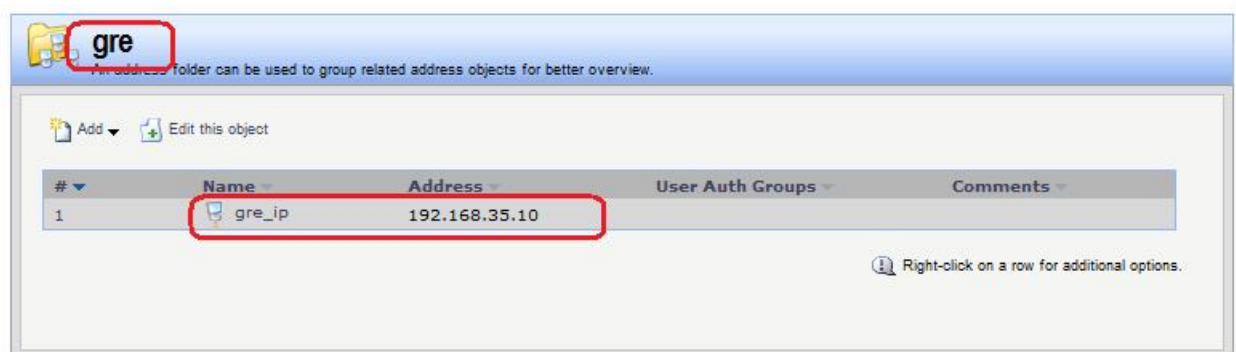
Объекты Адресной Книги

Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: gre

Object → Address Book → gre → Add



Командная строка:

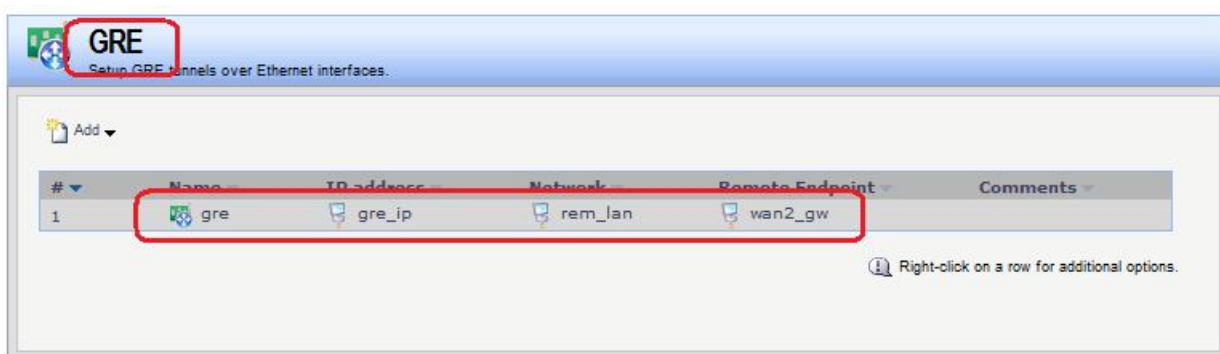
```
add Address AddressFolder gre
cc Address AddressFolder gre
add IP4Address gre_ip Address=192.168.35.10
```

GRE- и IPSec-Интерфейсы

Создать GRE-Интерфейс.

Веб-интерфейс:

Interfaces → GRE → Add → GRE Tunnel



Командная строка:

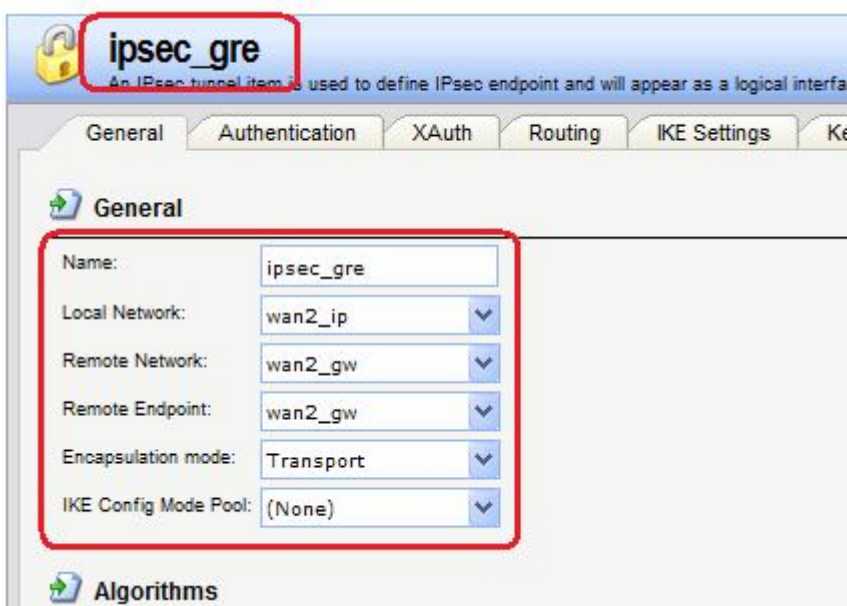
```
add Interface GREtunnel gre Network=remote/rem_lan IP=gre/gre_ip  
RemoteEndpoint=wan2/wan2_gw
```

Создать IPSec-интерфейс. Так как туннель между двумя локальными сетями создается с помощью протокола GRE, то для протокола IPSec следует использовать транспортный режим.

Веб-интерфейс:

Interfaces → IPsec → Add → IPsec Tunnel

На вкладке **General** указать сети перед и за туннелем, а также режим выполнения IPSec и используемые наборы алгоритмов для IPSec и IKE.



На вкладке **Authentication** указать созданный аутентификационный объект.

Командная строка:

```
add Interface IPsecTunnel ipsec_gre LocalNetwork=wan2/wan2_ip  
RemoteNetwork=wan2/wan2_gw AuthMethod=PSK PSK=forIPSec IKEAlgorithms=Medium  
IPsecAlgorithms=Medium EncapsulationMode=Transport  
RemoteEndpoint=wan2/wan2_gw
```

Статическая маршрутизация

В таблице маршрутизации должны быть маршруты к сетям через интерфейсы **wan1**, **gre** и **ipsec**.

Flags	Network	Interface	Gateway	Local IP	Metric
	192.168.20.20	ipsec_gre			90
	10.6.10.0/28	wan1			100
	192.168.2.0/24	gre			90
	192.168.1.0/24	lan			100
	172.17.100.0/24	dmz			100
	192.168.20.0/24	wan2			100
	0.0.0.0/0	wan1	10.6.10.3		100

Правила фильтрации

Правила фильтрации достаточно задать для GRE-интерфейса.

Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: gre_ipsec

Rules → IP Rules → gre → Add

#	Name	Action	Source interface	Source network	Destination interface	Destination network	Service
1	gre_out	Allow	lan	lan_net	gre	rem_lan	all_services

Командная строка:

```
add IPRuleFolder Name=gre_ipsec
```

```
cc IPRuleFolder <N folder>
```

```
add IPRule Action=Allow SourceInterface=lan SourceNetwork=lan/lan_net  
DestinationInterface=gre DestinationNetwork=remote/rem_lan  
Service=all_services Name=gre_out
```

Межсетевой Экран 2

Аутентификационный Объект

Используем аутентификационный объект **Pre-Shared Key**, созданный в Лабораторной работе 9.

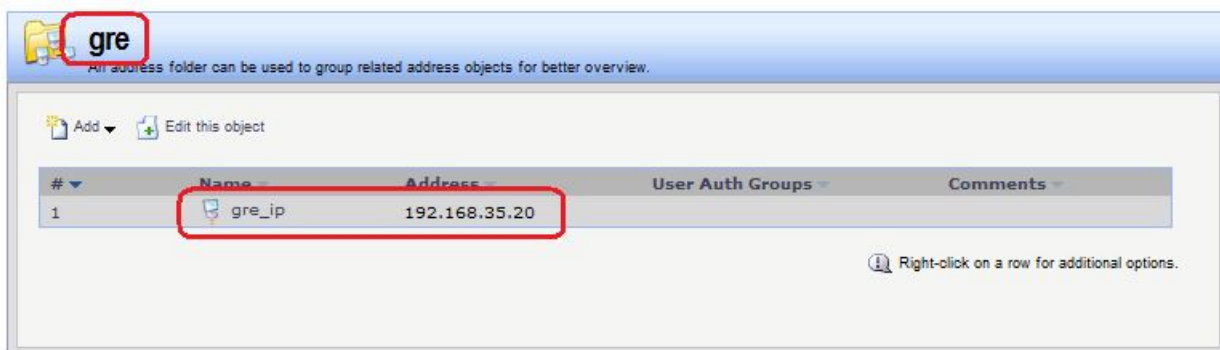
Объекты Адресной Книжки

Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: gre

Object → Address Book → gre → Add



Командная строка:

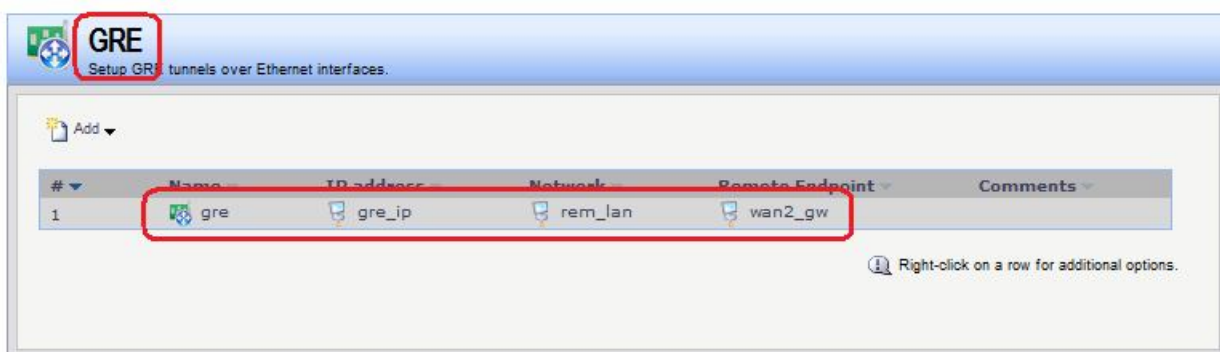
```
add Address AddressFolder gre
cc Address AddressFolder gre
add IP4Address gre_ip Address=192.168.35.20
```

GRE- и IPSec-Интерфейсы

Создать GRE-Интерфейс.

Веб-интерфейс:

Interfaces → GRE → Add → GRE Tunnel



Командная строка:

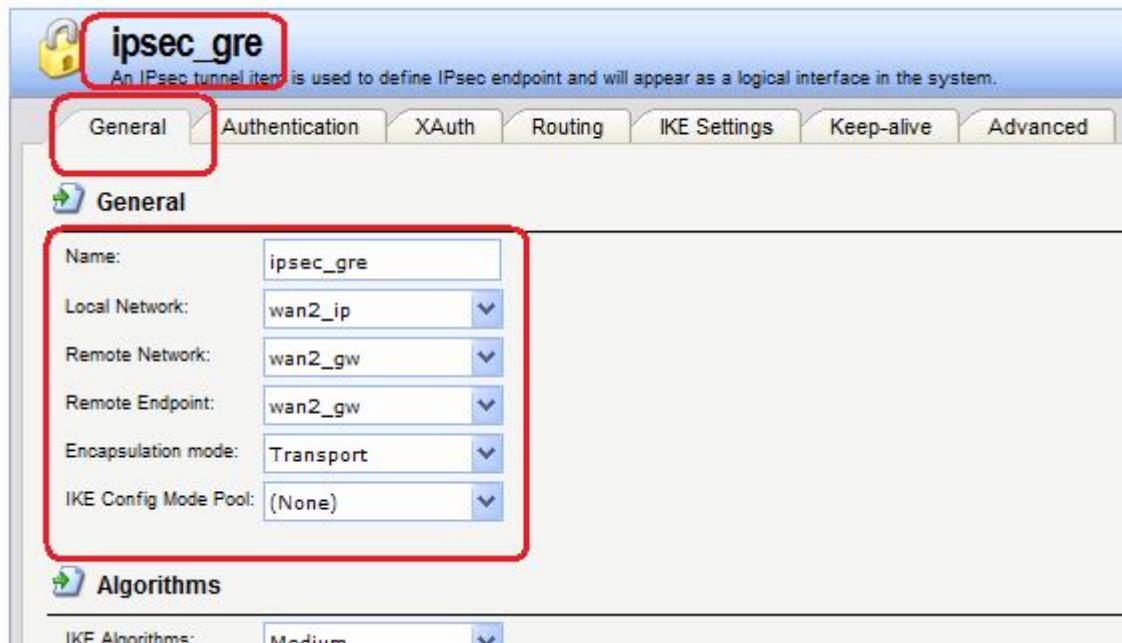
```
add Interface GREtunnel gre Network=remote/rem_lan IP=gre/gre_ip
RemoteEndpoint=wan2/wan2_gw
```

Создать IPSec-интерфейс. Так как создается туннель между двумя локальными сетями создается с помощью протокола GRE, то для протокола IPSec следует использовать транспортный режим.

Веб-интерфейс:

Interfaces → IPsec → Add → IPsec Tunnel

На вкладке **General** указать сети перед и за туннелем, а также режим выполнения IPsec и используемые наборы алгоритмов для IPsec и IKE.



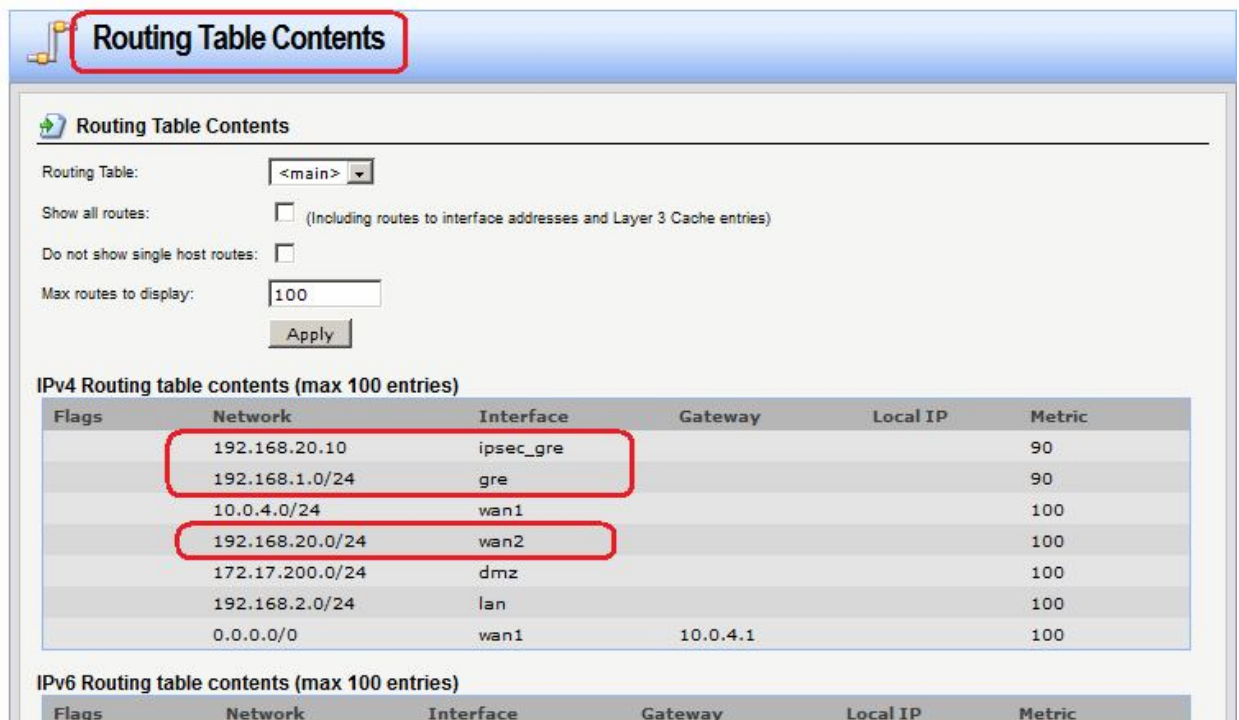
На вкладке **Authentication** указать созданный аутентификационный объект.

Командная строка:

```
add Interface IPsecTunnel ipsec_gre LocalNetwork=wan2/wan2_ip  
RemoteNetwork=wan2/wan2_gw AuthMethod=PSK PSK=forIPSec IKEAlgorithms=Medium  
IPsecAlgorithms=Medium EncapsulationMode=Transport  
RemoteEndpoint=wan2/wan2_gw
```

Статическая маршрутизация

В таблице маршрутизации должны быть маршруты к сетям через интерфейсы **wan1**, **gre** и **ipsec**.



Правила фильтрации

Правила фильтрации достаточно задать для GRE-интерфейса.

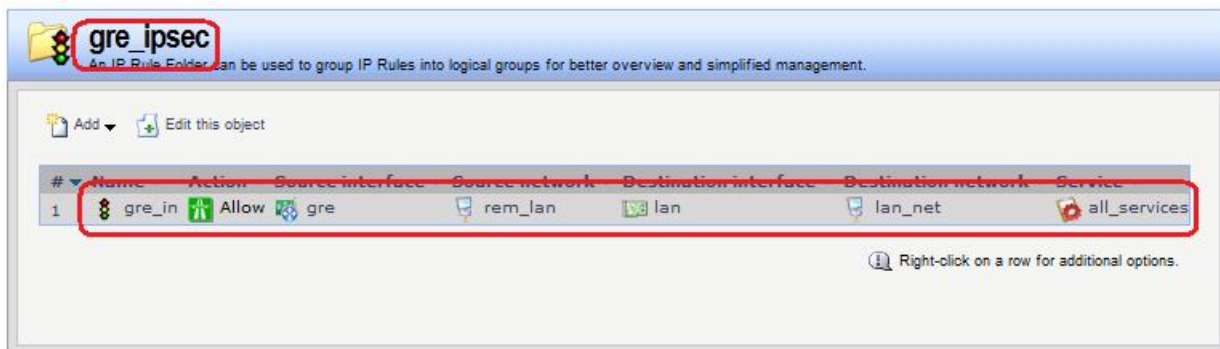
Веб-интерфейс:

Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: gre_ipsec

Rules → IP Rules → gre_ipsec → Add



Командная строка:

```
add IPRuleFolder Name=gre_ipsec
```

```
cc IPRuleFolder <N folder>
```

```
add IPRule Action=Allow SourceInterface=gre SourceNetwork=remote/rem_lan  
DestinationInterface=lan DestinationNetwork=lan/lan_net Service=all_services  
Name=gre_in
```

Проверка конфигурации

На Сервере 1 выполним команду ping.

```
Command Prompt
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>
C:\Users\Laponina>ping 192.168.2.123

Pinging 192.168.2.123 with 32 bytes of data:
Reply from 192.168.2.123: bytes=32 time=2ms TTL=126
Reply from 192.168.2.123: bytes=32 time=1ms TTL=126
Reply from 192.168.2.123: bytes=32 time=1ms TTL=126
Reply from 192.168.2.123: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.123:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\Laponina>
```

Получим дамп трафика аналогично тому, как это делалось в предыдущих лабораторных работах.

На интерфейсе wan1 видим следующий трафик:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.20.10	192.168.20.20	ISAKMP	146	Identity Protection (Main Mode)
2	0.000000	192.168.20.20	192.168.20.10	ISAKMP	306	Identity Protection (Main Mode)
3	0.030000	192.168.20.10	192.168.20.20	ISAKMP	222	Identity Protection (Main Mode)
4	0.080000	192.168.20.20	192.168.20.10	ISAKMP	222	Identity Protection (Main Mode)
5	0.110000	192.168.20.10	192.168.20.20	ISAKMP	118	Identity Protection (Main Mode)
6	0.110000	192.168.20.20	192.168.20.10	ISAKMP	118	Identity Protection (Main Mode)
7	0.120000	192.168.20.10	192.168.20.20	ISAKMP	198	Quick Mode
8	0.120000	192.168.20.20	192.168.20.10	ISAKMP	198	Quick Mode
9	0.130000	192.168.20.10	192.168.20.20	ISAKMP	102	Quick Mode
10	0.380000	192.168.20.10	192.168.20.20	ESP	150	ESP (SPI=0x7f7b4343)
11	0.380000	192.168.20.20	192.168.20.10	ESP	150	ESP (SPI=0x5d5121b5)
12	1.220000	192.168.20.10	192.168.20.20	ESP	150	ESP (SPI=0x7f7b4343)
13	1.220000	192.168.20.20	192.168.20.10	ESP	150	ESP (SPI=0x5d5121b5)
14	2.410000	192.168.20.10	192.168.20.20	ESP	150	ESP (SPI=0x7f7b4343)
15	2.410000	192.168.20.20	192.168.20.10	ESP	150	ESP (SPI=0x5d5121b5)
16	3.420000	192.168.20.10	192.168.20.20	ESP	150	ESP (SPI=0x7f7b4343)
17	3.420000	192.168.20.20	192.168.20.10	ESP	150	ESP (SPI=0x5d5121b5)

Frame 1: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits)
 Ethernet II, Src: D-Link_49:dc:ff (5c:d9:98:49:dc:ff), Dst: D-Link_49:dd:03 (5c:d9:98:49:dd:03)
 Internet Protocol Version 4, Src: 192.168.20.10 (192.168.20.10), Dst: 192.168.20.20 (192.168.20.20)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol

После обмена IKE-содержимыми трафик зашифрован, на интерфейсе **wan1** он не виден.

На интерфейсе **ipsec** видим следующий трафик:

ipsec.cap [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.30	192.168.2.123	ICMP	98	Echo (ping) request id=0
2	0.000000	192.168.2.123	192.168.1.30	ICMP	98	Echo (ping) reply id=0
3	0.990000	192.168.1.30	192.168.2.123	ICMP	98	Echo (ping) request id=0
4	0.990000	192.168.2.123	192.168.1.30	ICMP	98	Echo (ping) reply id=0
5	1.990000	192.168.1.30	192.168.2.123	ICMP	98	Echo (ping) request id=0

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
 Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
 Internet Protocol Version 4, Src: 192.168.20.10 (192.168.20.10), Dst: 192.168.20.20 (192.168.20.20)
Generic Routing Encapsulation (IP)
 Internet Protocol Version 4, Src: 192.168.1.30 (192.168.1.30), Dst: 192.168.2.123 (192.168.2.123)
 Internet Control Message Protocol

Между интерфейсами **ipsec** поднят GRE-туннель.

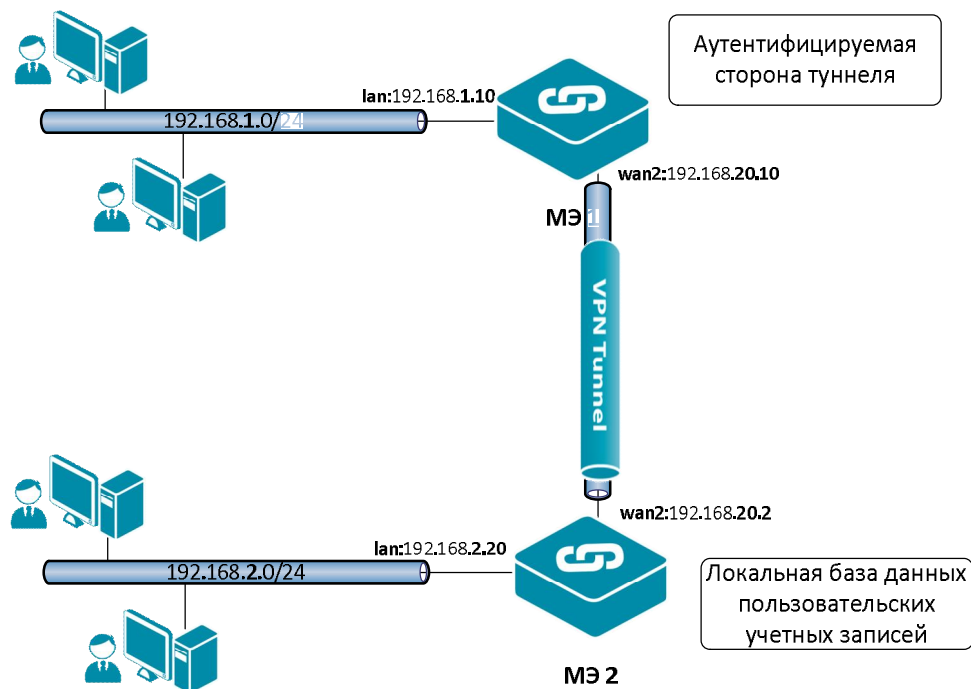
Лабораторная работа 9. Соединение двух локальных сетей протоколом L2TP/IPSec в транспортном режиме

Цель

Соединить две сети, расположенные за межсетевыми экранами, VPN с использованием семейства протоколов IPSec. VPN с использованием IPSec будем создавать в транспортном режиме. Для туннеля между двумя локальными сетями будет использовать протокол L2TP.

Топология сети аналогична топологии VPN/IPSec.

Топология



Описание практической работы

Межсетевой Экран 1

Аутентификационный Объект

Используем аутентификационный объект **Pre-Shared Key**, созданный в Лабораторной работе 9.

L2TP- и IPSec-Интерфейсы

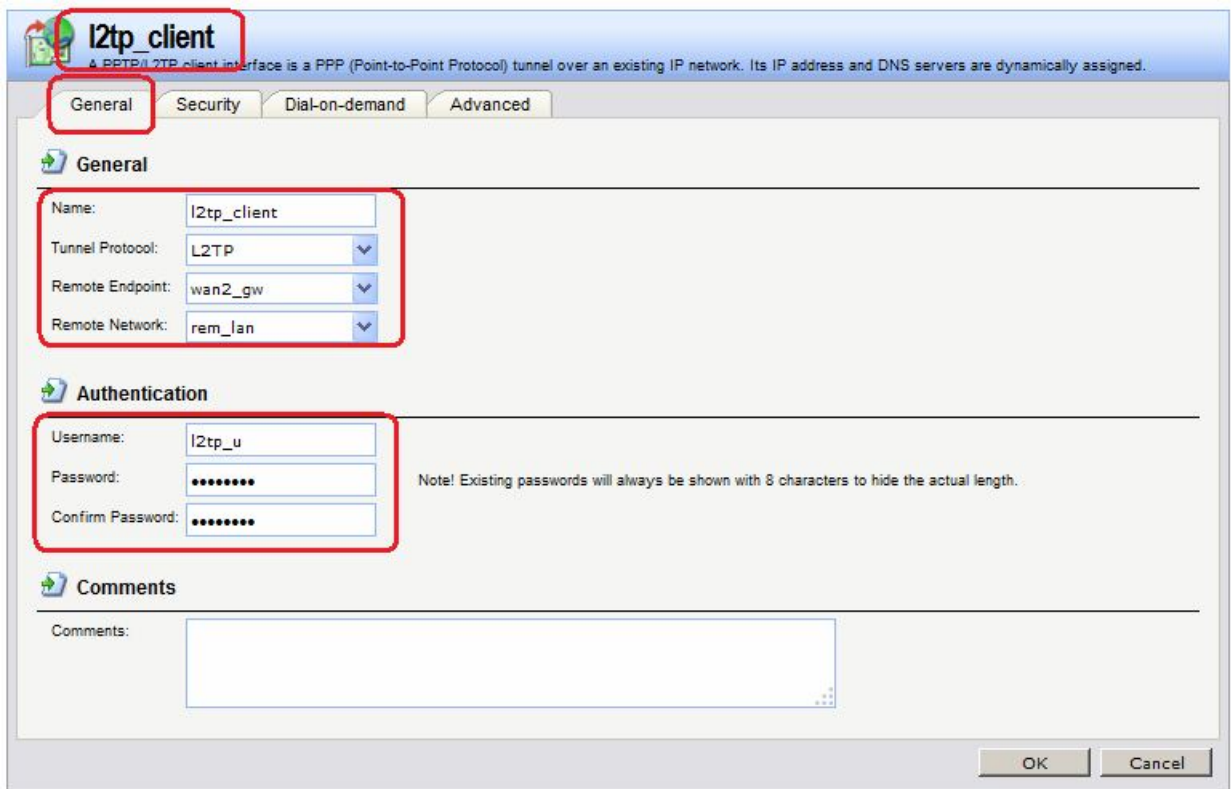
Создать L2TP-интерфейс аутентифицируемой стороны туннеля.

Веб-интерфейс:

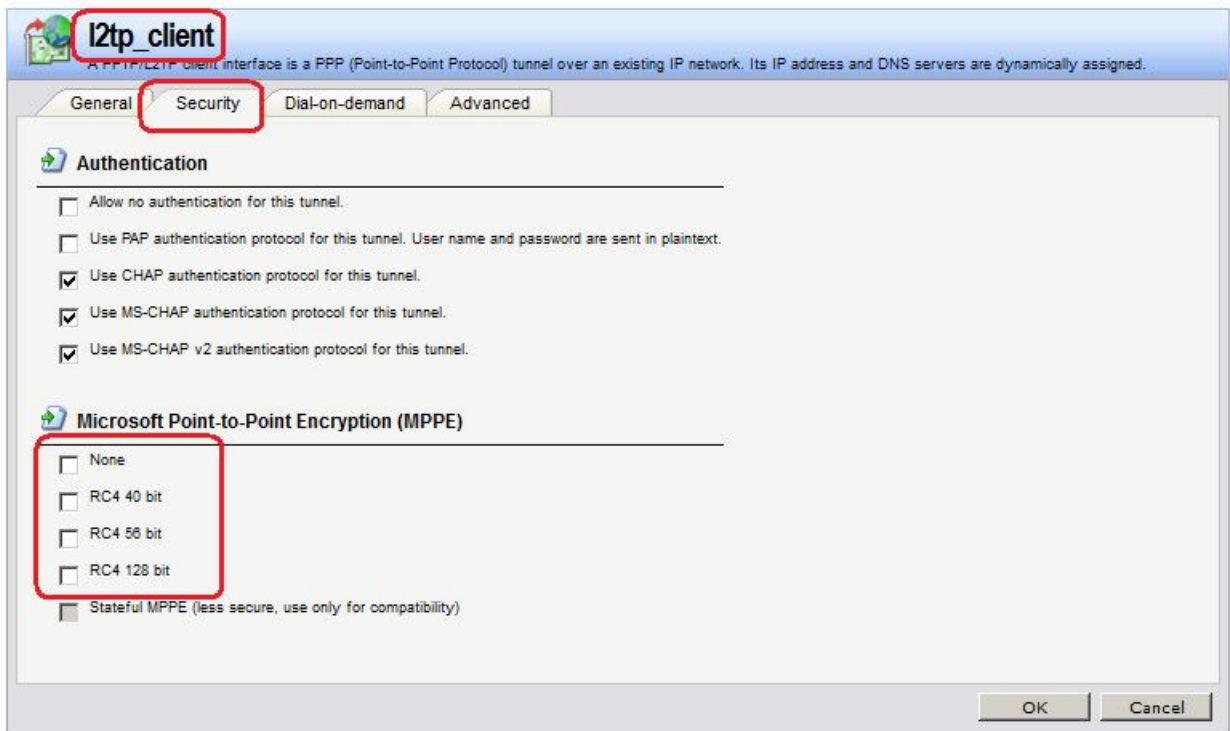
Interfaces → **PPTP/L2TP Clients** → **Add** → **PPTP/L2TP Client**

На вкладке **General** указать туннелирующий протокол, адрес конечной точки и сеть, расположенную за туннелем.

Также указать имя пользователя и пароль, созданные в базе данных на противоположной стороне туннеля.



На вкладке **Security** следует отключить всё шифрование, так как шифрование трафика будет выполнять протокол IPSec.



Командная строка:

```
add Interface L2TPClient l2tp_client Network=remote/rem_lan
RemoteEndpoint=wan2/wan2_gw Username=l2tp_u Password=qwerty
TunnelProtocol=L2TP MPPENone=No MPPERC4128=No MPPERC440=No MPPERC456=No
```

Создать IPSec-интерфейс.

Веб-интерфейс:

Interfaces → IPsec → Add → IPsec Tunnel

На вкладке **General** указать конечные точки туннеля, а также режим выполнения IPsec и используемые наборы алгоритмов для IPsec и IKE.

The screenshot shows the configuration page for an IPsec Tunnel named 'ipsec_l2tp'. The 'General' tab is selected. The configuration fields are as follows:

Field	Value
Name	ipsec_l2tp
Local Network	wan2_ip
Remote Network	wan2_gw
Remote Endpoint	wan2_gw
Encapsulation mode	Transport
IKE Config Mode Pool	(None)

Below the General tab, the Algorithms section is visible:

Algorithm Type	Algorithm	Lifetime	Unit
IKE Algorithms	Medium	28800	seconds
IPsec Algorithms	Medium	3600	seconds
IPsec Lifetime	0		kilobytes

На вкладке **Authentication** указать созданный аутентификационный объект.

Командная строка:

```
add Interface IPsecTunnel IPsec_l2tp LocalNetwork=wan2/wan2_ip  
RemoteNetwork=wan2/wan2_gw AuthMethod=PSK PSK=ipsec_psk IKEAlgorithms=Medium  
IPsecAlgorithms=Medium EncapsulationMode=Transport  
RemoteEndpoint=wan2/wan2_gw
```

Статическая маршрутизация

В таблице маршрутизации должны быть маршруты к соответствующим сетям через интерфейсы **wan1**, **l2tp_client** и **IPsec_l2tp**.

Routing Table Contents

Routing Table: <main>

Show all routes: (Including routes to interface addresses and Layer 3 Cache entries)

Do not show single host routes:

Max routes to display: 100

Apply

IPv4 Routing table contents (max 100 entries)

Flags	Network	Interface	Gateway	Local IP	Metric
	192.168.20.20	ipsec_l2tp			90
	10.6.10.0/28	wan1			100
	192.168.2.0/24	l2tp_client			90
	192.168.1.0/24	lan			100
	172.17.100.0/24	dmz			100
	192.168.20.0/24	wan2			100
	0.0.0.0/0	wan1	10.6.10.3		100

IPv6 Routing table contents (max 100 entries)

Flags	Network	Interface	Gateway	Local IP	Metric
-------	---------	-----------	---------	----------	--------

Правила фильтрации

Правила фильтрации достаточно задать для L2TP-интерфейса. Правило должно разрешать исходящий трафик с lan-интерфейса на созданный L2TP-интерфейс.

Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: ipsec_l2tp

Rules → IP Rules → ipsec_l2tp → Add

ipsec_l2tp

An IP Rule Folder can be used to group IP Rules into logical groups for better overview and simplified management.

Add Edit this object

#	Name	Action	Source interface	Source network	Destination interface	Destination network	Service
1	ipsec_l2tp_out	Allow	lan	lan_net	l2tp_client	rem_lan	all_services

Right-click on a row for additional options.

Командная строка:

```
add IPRuleFolder Name=ipsec_l2tp
```

```
cc IPRuleFolder <N folder>
```

```
add IPRule Action=Allow SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=l2tp_client DestinationNetwork=remote/rem_lan
Service=all_services Name=ipsec_l2tp_in
```

Межсетевой Экран 2

Аутентификационный Объект

Используем аутентификационный объект **Pre-Shared Key**, созданный в Лабораторной работе 9.

Объекты Адресной Книги

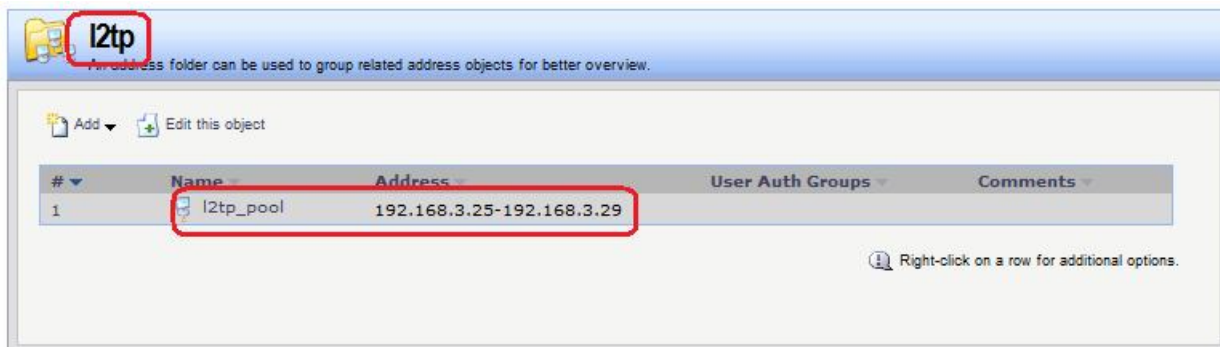
Создать пул IP-адресов.

Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: l2tp

Object → Address Book → l2tp → Add



Командная строка:

```
add Address AddressFolder l2tp
```

```
cc Address AddressFolder l2tp
```

```
add IP4Address l2tp_pool Address=192.168.3.25-192.168.3.29
```

IP-адреса из этого пула будут выдаваться l2tp-клиенту.

L2TP- и IPSec-Интерфейсы

Создать IPSec-интерфейс.

Веб-интерфейс:

Interfaces → IPsec → Add → IPsec Tunnel

На вкладке **General** указать конечные точки туннеля, а также режим выполнения IPSec и используемые наборы алгоритмов для IPSec и IKE.

ipsec_l2tp
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: ipsec_l2tp

Local Network: wan2_ip

Remote Network: wan2_gw

Remote Endpoint: wan2_gw

Encapsulation mode: Transport

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

На вкладке **Authentication** указать созданный аутентификационный объект.

Командная строка:

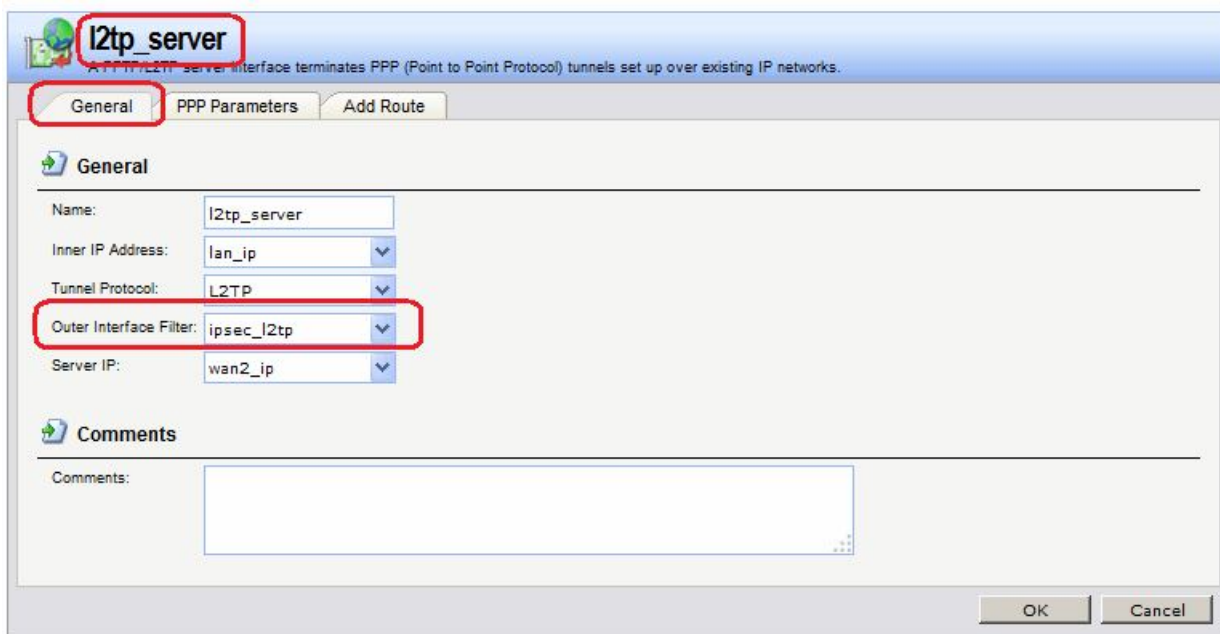
```
add Interface IPsecTunnel IPsec_l2tp LocalNetwork=wan2/wan2_ip
RemoteNetwork=wan2/wan2_gw AuthMethod=PSK PSK=ipsec_psk IKEAlgorithms=Medium
IPsecAlgorithms=Medium EncapsulationMode=Transport
RemoteEndpoint=wan2/wan2_gw
```

Создать L2TP-интерфейс, который будет аутентифицировать противоположную сторону туннеля.

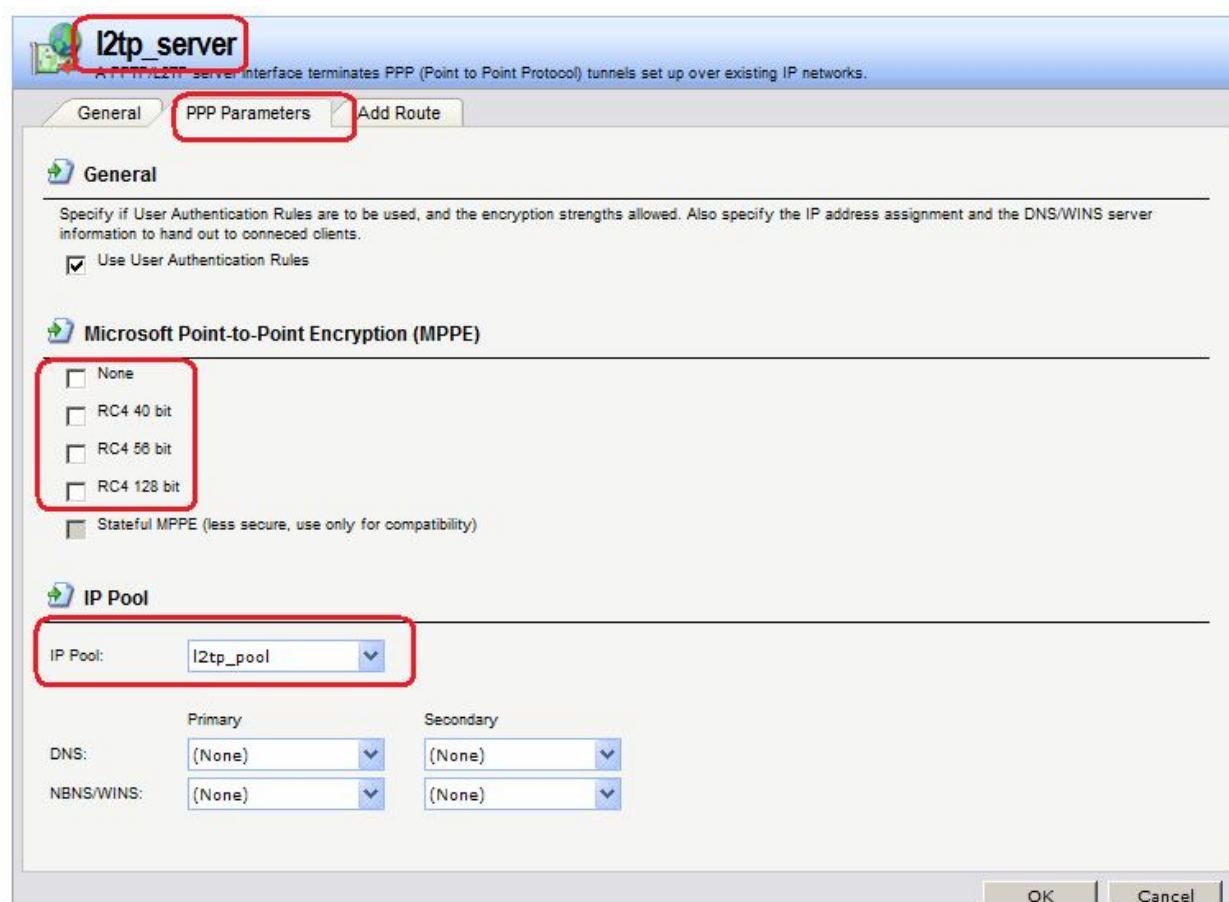
Веб-интерфейс:

Interfaces → **PPTP/L2TP Servers** → **Add** → **PPTP/L2TP server**

На вкладке **General** указываются параметры туннеля. В качестве интерфейса указывается **ipsec**.



На вкладке **PPP Parameters** снять параметры PPP-шифрования и указать пул IP-адресов, из которого будут выдаваться IP-адреса клиенту.

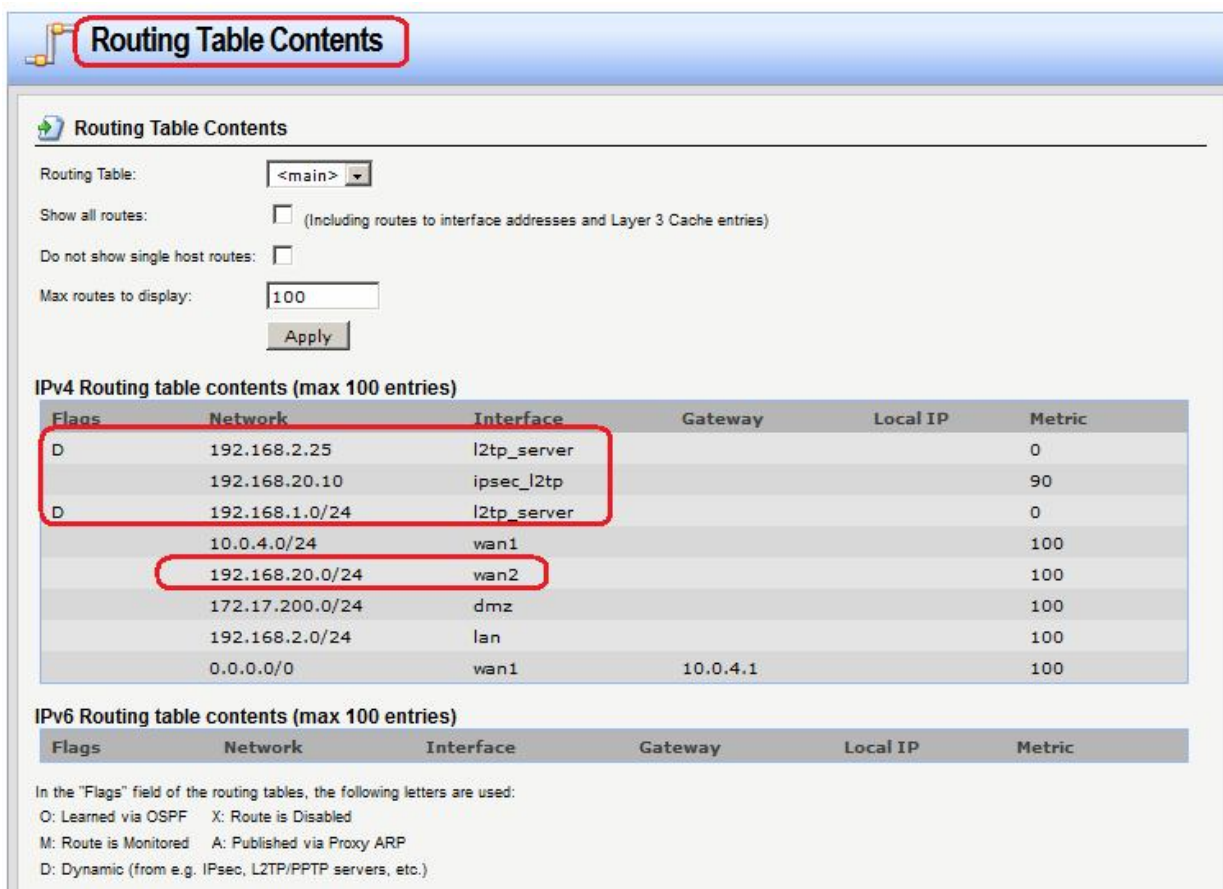


Командная строка:

```
add Interface L2TPServer l2tp_server Interface=ipsec_l2tp IP=lan/lan_ip
ServerIP=wan2/wan2_ip IPPool=l2tp/l2tp_pool TunnelProtocol=L2TP MPPENone=No
MPPERC4128=No MPPERC440=No MPPERC456=No
```

Статическая маршрутизация

В таблице маршрутизации должны быть маршруты к сетям через интерфейсы **wan1** и **ipsec**. Маршрут через интерфейс **l2tp** будет добавлен динамически.



Routing Table Contents

Routing Table: **<main>**

Show all routes: (Including routes to interface addresses and Layer 3 Cache entries)

Do not show single host routes:

Max routes to display: **100**

Apply

IPv4 Routing table contents (max 100 entries)

Flags	Network	Interface	Gateway	Local IP	Metric
D	192.168.2.25	l2tp_server			0
	192.168.20.10	ipsec_l2tp			90
D	192.168.1.0/24	l2tp_server			0
	10.0.4.0/24	wan1			100
	192.168.20.0/24	wan2			100
	172.17.200.0/24	dmz			100
	192.168.2.0/24	lan			100
	0.0.0.0/0	wan1	10.0.4.1		100

IPv6 Routing table contents (max 100 entries)

Flags	Network	Interface	Gateway	Local IP	Metric
-------	---------	-----------	---------	----------	--------

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.)

Правила фильтрации

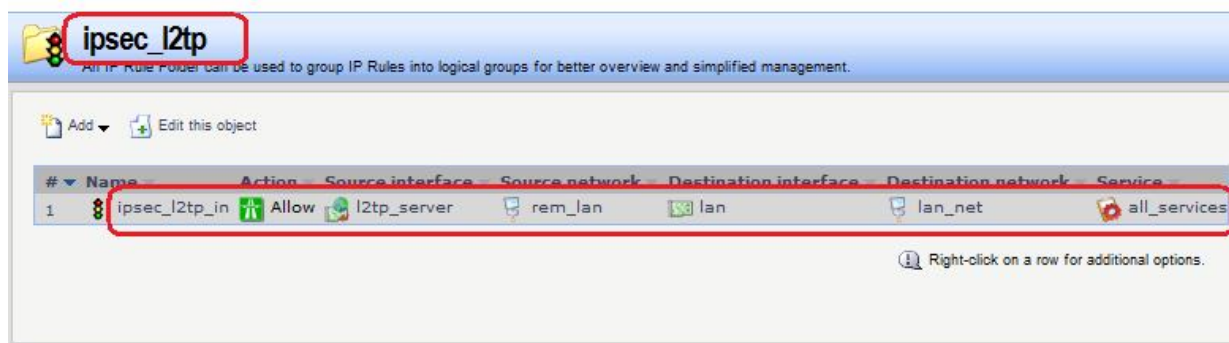
Правила фильтрации достаточно задать для L2TP-интерфейса.

Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: l2tp

Rules → IP Rules → l2tp → Add



ipsec_l2tp

All IP Rule Folders can be used to group IP Rules into logical groups for better overview and simplified management.

Add Edit this object

#	Name	Action	Source interface	Source network	Destination interface	Destination network	Service
1	ipsec_l2tp_in	Allow	l2tp_server	rem_lan	lan	lan_net	all_services

Right-click on a row for additional options.

Командная строка:

```
add IPRuleFolder Name=ipsec_l2tp
```

```
cc IPRuleFolder <N folder>
```

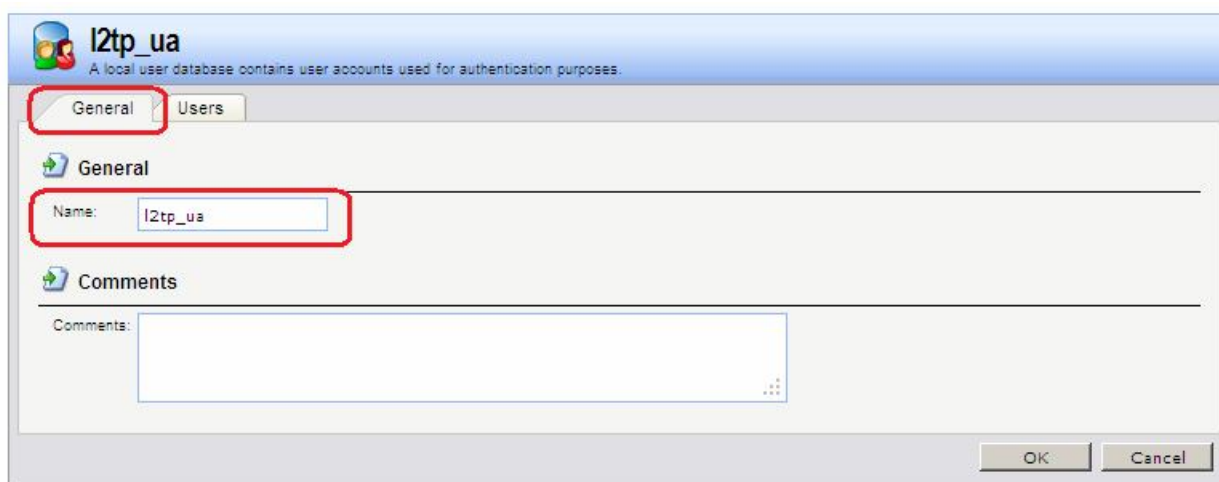
```
add IPRule Action=Allow SourceInterface=l2tp_server
SourceNetwork=remote/rem_lan DestinationInterface=lan
DestinationNetwork=lan/lan_net Service=all_services Name=ipsec_l2tp_in
```

Аутентификация на уровне пользователя
Создать локальную базу данных пользователей.

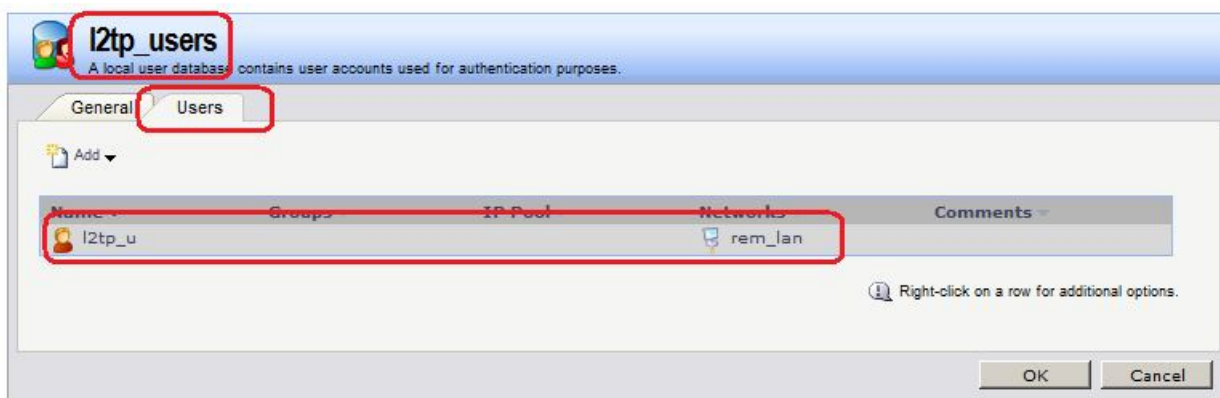
Веб-интерфейс:

User Authentication → Local User Databases → Add → Local User Database

На вкладке **General** указать имя базы данных.



На вкладке **Users** добавить учетные записи пользователей.



Командная строка:

```
add LocalUserDatabase l2tp_ua
add User olga Password=qwerty AutoAddRouteNet=remote/rem_lan
```

Создать правило аутентификации пользователей.

Веб-интерфейс:

User Authentication → User Authentication Rules → Add

Name: l2tp_rules

На вкладке **General** указать аутентификационный источник **Local** и необходимые для туннелирующего протокола опции. В нашем случае туннелирующим протоколом является L2TP.

l2tp_rules
The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

General Log Settings Authentication Options Accounting Agent Options Restrictions

General

Name: l2tp_rules

Authentication agent: L2TP/PPTP/SSL VP

Authentication Source: Local

Interface: l2tp_server

Originator IP: wan2_gw

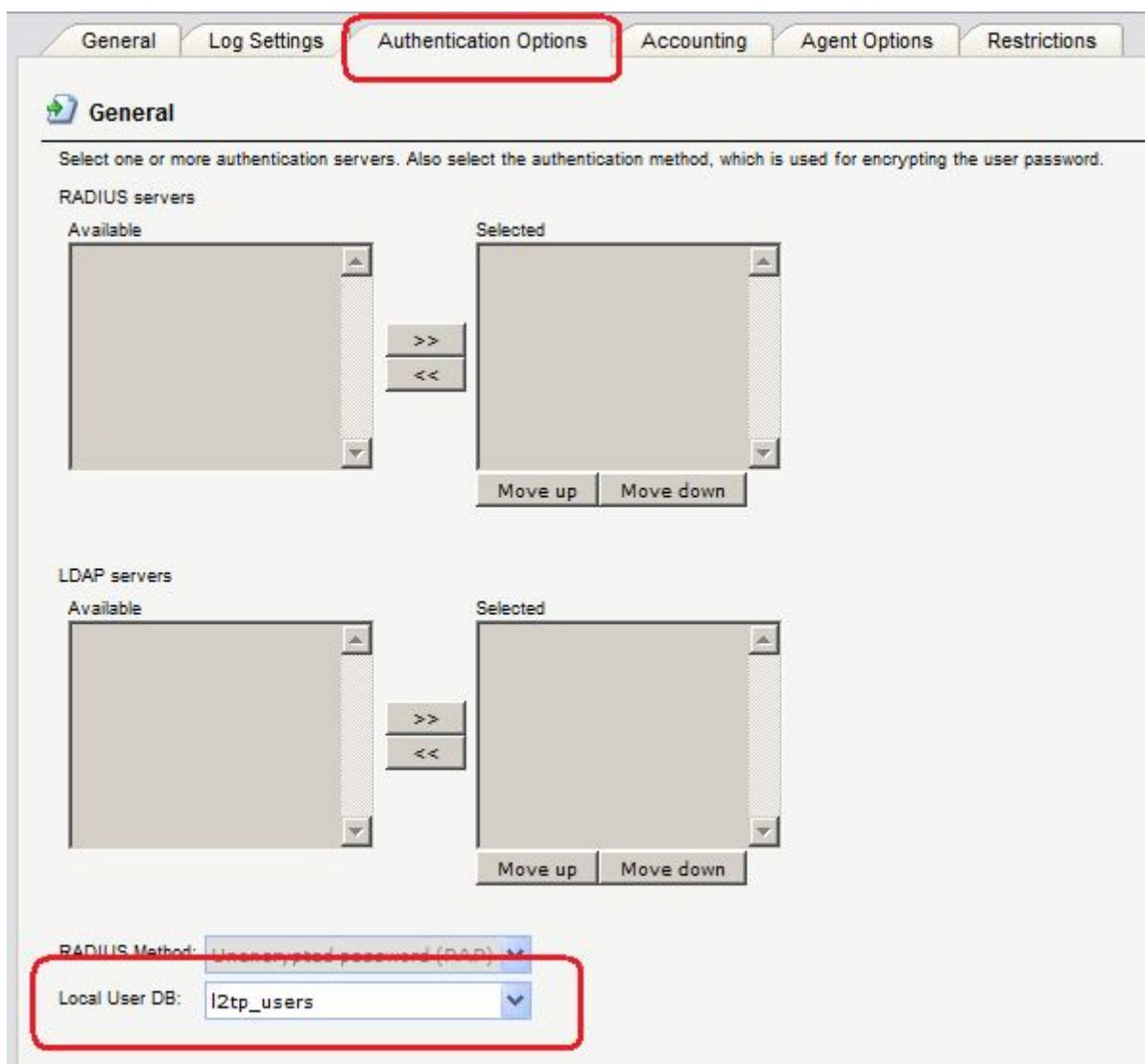
Terminator IP: wan2_ip

Comments

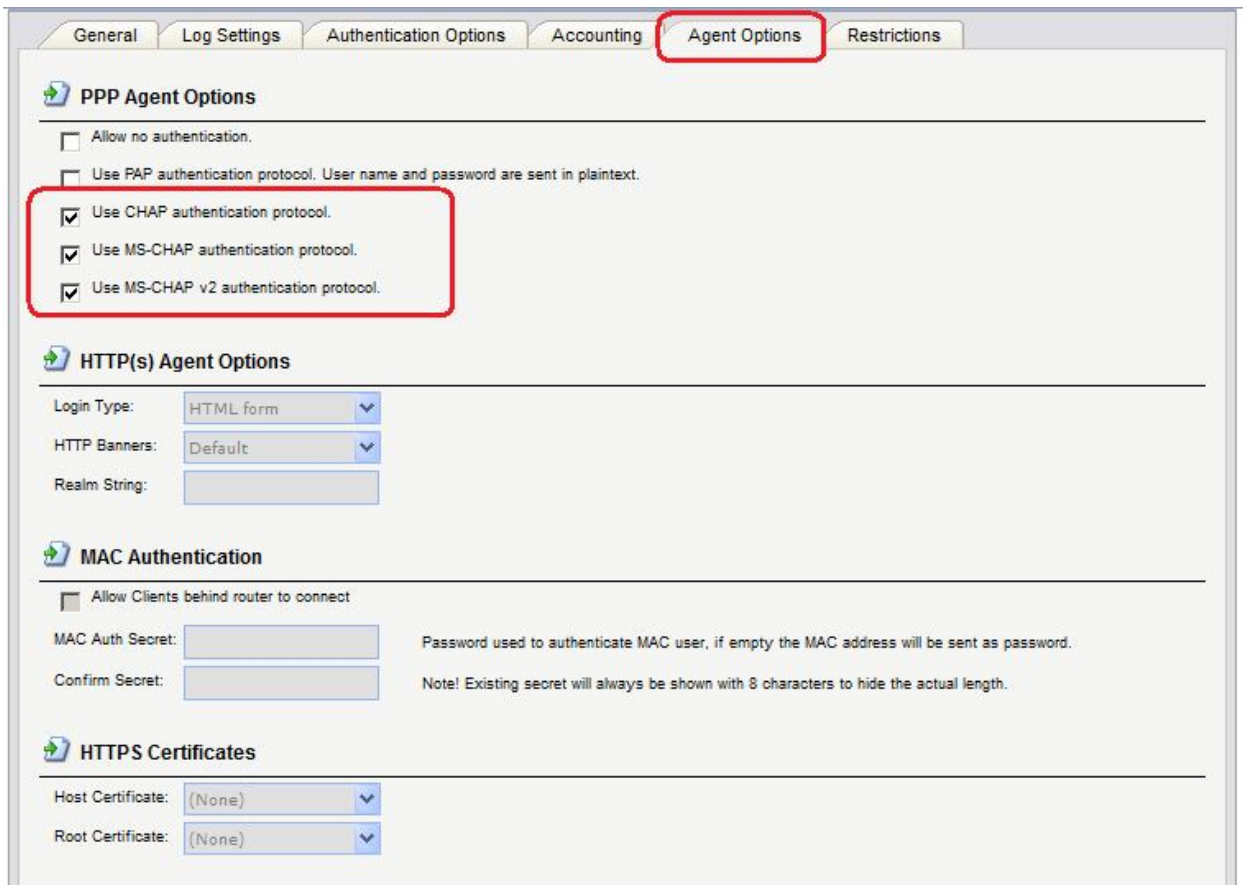
Comments:

OK

На вкладке **Authentication Options** указать имя локальной базы данных пользователей.



На вкладке **Agent Options** указать параметры PPP-аутентификации.

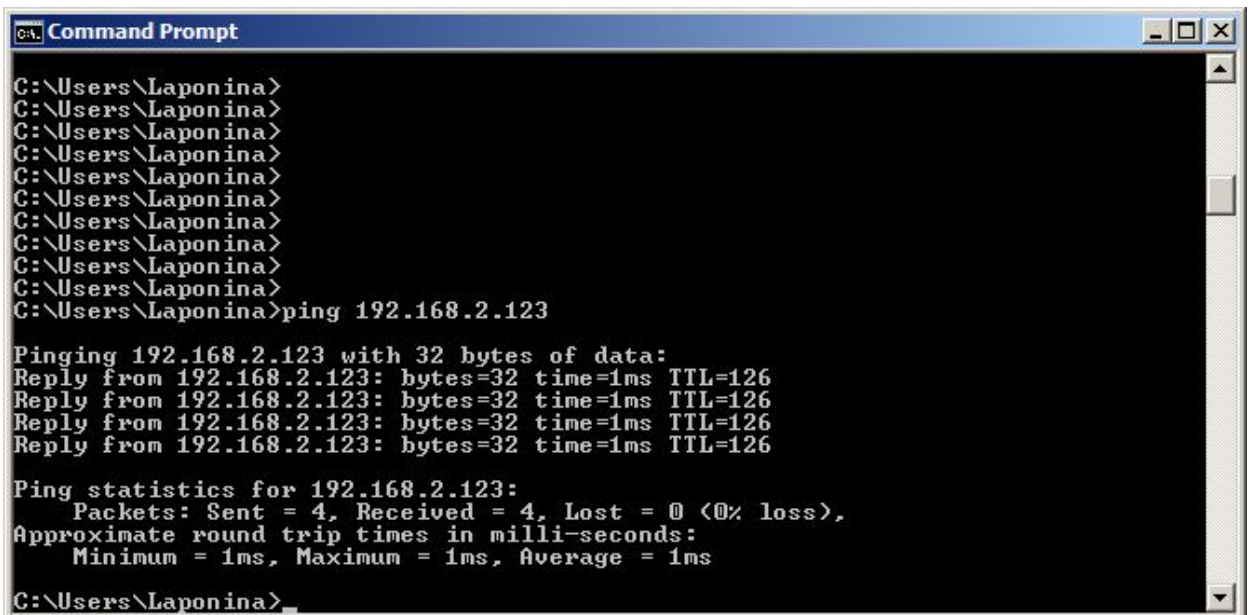


Командная строка:

```
add UserAuthRule AuthSource=Local Interface=l2tp_server LocalUserDB=l2tp_ua
OriginatorIP=wan2/wan2_gw Agent=PPP TerminatorIP=wan2/wan2_ip Name=l2tp_rules
```

Проверка конфигурации

На рабочей станции, расположенной в локальной сети за межсетевым экраном 1, выполним команду ping.



Получим дамп трафика аналогично тому, как это делалось в предыдущих лабораторных работах.

На интерфейсе wan2 видим IPSec-трафик.

23	21.960000	192.168.20.20	192.168.20.10	ISAKMP	118	Informational
24	21.970000	192.168.20.20	192.168.20.10	ISAKMP	118	Informational
25	24.710000	192.168.20.10	192.168.20.20	ISAKMP	478	Identity Protection (Main Mode)
26	24.710000	192.168.20.20	192.168.20.10	ISAKMP	306	Identity Protection (Main Mode)
27	24.740000	192.168.20.10	192.168.20.20	ISAKMP	262	Identity Protection (Main Mode)
28	24.790000	192.168.20.20	192.168.20.10	ISAKMP	262	Identity Protection (Main Mode)
29	24.820000	192.168.20.10	192.168.20.20	ISAKMP	118	Identity Protection (Main Mode)
30	24.820000	192.168.20.20	192.168.20.10	ISAKMP	102	Identity Protection (Main Mode)
31	24.830000	192.168.20.10	192.168.20.20	ISAKMP	326	Quick Mode
32	24.830000	192.168.20.20	192.168.20.10	ISAKMP	198	Quick Mode
33	24.840000	192.168.20.10	192.168.20.20	ISAKMP	102	Quick Mode
34	25.090000	192.168.20.10	192.168.20.20	ESP	166	ESP (SPI=0x285faaea)
35	25.090000	192.168.20.20	192.168.20.10	ESP	166	ESP (SPI=0x8e7ecf82)
36	25.090000	192.168.20.20	41.76.206.243	ICMP	60	Echo (ping) request id=0x0000, s
37	25.090000	192.168.20.20	199.119.106.162	ICMP	60	Echo (ping) request id=0x0001, s
38	25.090000	192.168.20.20	69.46.69.149	ICMP	60	Echo (ping) request id=0x0002, s
39	25.090000	192.168.20.20	85.11.194.39	ICMP	60	Echo (ping) request id=0x0003, s

Frame 25: 478 bytes on wire (3824 bits), 478 bytes captured (3824 bits)
 Ethernet II, Src: D-Link_49:dc:ff (5c:d9:98:49:dc:ff), Dst: D-Link_49:dd:03 (5c:d9:98:49:dd:03)
 Internet Protocol Version 4, Src: 192.168.20.10 (192.168.20.10), Dst: 192.168.20.20 (192.168.20.20)
 User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
 Internet Security Association and Key Management Protocol
 Initiator cookie: d6cfc9bd467a4b3d
 Responder cookie: 0000000000000000
 Next payload: Security Association (1)
 version: 1.0
 Exchange type: Identity Protection (Main Mode) (2)
 Flags: 0x00

На интерфейсе ipsec_12tp видим L2TP-трафик.

1	0.000000	192.168.20.10	192.168.20.20	L2TP	62	Control Message - Hello (tunnel id=19477,
2	0.000000	192.168.20.20	192.168.20.10	L2TP	54	Control Message - ZLB (tunnel id=9919,
3	1.990000	192.168.20.20	192.168.20.10	PPP LCP	62	Echo Request
4	1.990000	192.168.20.10	192.168.20.20	PPP LCP	62	Echo Reply
5	14.090000	192.168.20.10	192.168.20.20	PPP Comp	118	Compressed data
6	14.090000	192.168.20.20	192.168.20.10	PPP Comp	118	Compressed data
7	14.710000	192.168.20.10	192.168.20.20	PPP Comp	118	Compressed data
8	14.710000	192.168.20.20	192.168.20.10	PPP Comp	118	Compressed data
9	15.710000	192.168.20.10	192.168.20.20	PPP Comp	118	Compressed data
10	15.710000	192.168.20.20	192.168.20.10	PPP Comp	118	Compressed data
11	16.710000	192.168.20.10	192.168.20.20	PPP Comp	118	Compressed data
12	16.710000	192.168.20.20	192.168.20.10	PPP Comp	118	Compressed data
13	19.010000	192.168.20.20	192.168.20.10	L2TP	62	Control Message - Hello (tunnel id=9919,
14	19.010000	192.168.20.10	192.168.20.20	L2TP	54	Control Message - ZLB (tunnel id=19477,
15	29.990000	192.168.20.10	192.168.20.20	L2TP	62	Control Message - Hello (tunnel id=19477,
16	29.990000	192.168.20.20	192.168.20.10	L2TP	54	Control Message - ZLB (tunnel id=9919,
17	37.990000	192.168.20.20	192.168.20.10	PPP LCP	62	Echo Request
18	37.990000	192.168.20.10	192.168.20.20	PPP LCP	62	Echo Reply

Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
 Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
 Internet Protocol Version 4, Src: 192.168.20.10 (192.168.20.10), Dst: 192.168.20.20 (192.168.20.20)
 User Datagram Protocol, Src Port: 12f (1701), Dst Port: 12f (1701)
 Layer 2 Tunneling Protocol
 Packet Type: Control Message Tunnel Id=19477 Session Id=0
 Length: 20
 Tunnel ID: 19477
 Session ID: 0
 NS: 6
 NR: 4

На интерфейсе 12tp_server видим ICMP-трафик.

Time	Source	Destination	Protocol	Length	Info
0.000000	192.168.1.30	192.168.2.123	ICMP	74	Echo (ping) request id=0x
0.000000	192.168.2.123	192.168.1.30	ICMP	74	Echo (ping) reply id=0x
0.990000	192.168.1.30	192.168.2.123	ICMP	74	Echo (ping) request id=0x
1.000000	192.168.2.123	192.168.1.30	ICMP	74	Echo (ping) reply id=0x
1.990000	192.168.1.30	192.168.2.123	ICMP	74	Echo (ping) request id=0x

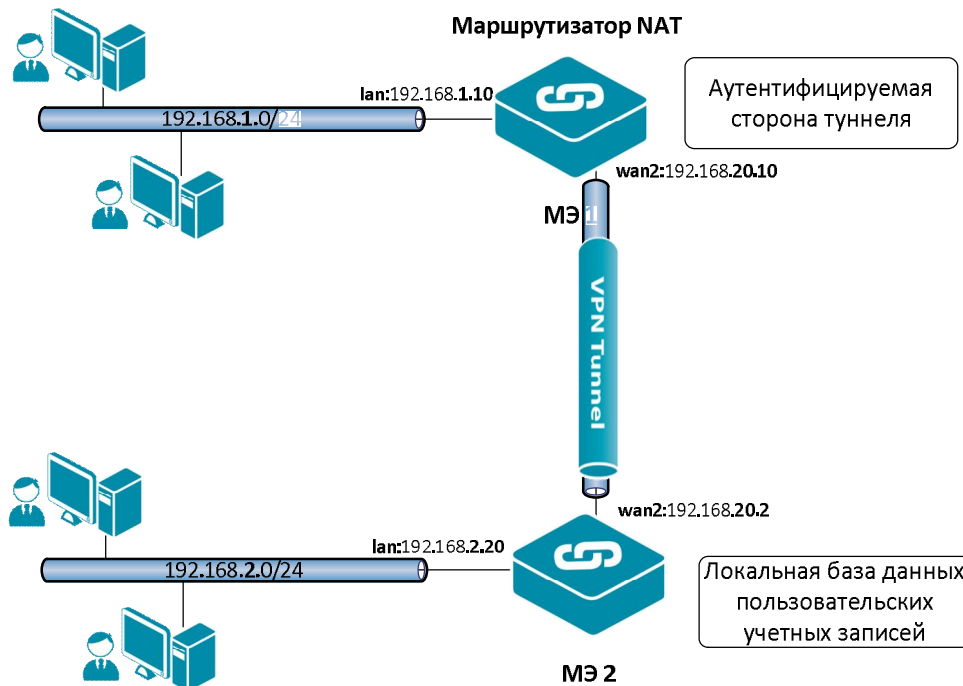
Лабораторная работа 10. Соединение двух локальных сетей протоколом L2TP/IPSec в транспортном режиме, для одной из локальных сетей используется NAT

Цель

Соединить две сети, расположенные за межсетевыми экранами, VPN с использованием семейства протоколов IPSec. VPN с использованием IPSec будем создавать в транспортном режиме. Для туннеля между двумя локальными сетями будет использоваться протокол L2TP. Локальная сеть, расположенная за L2TP-клиентом, используется NAT.

Топология сети аналогична топологии VPN/IPSec.

Топология



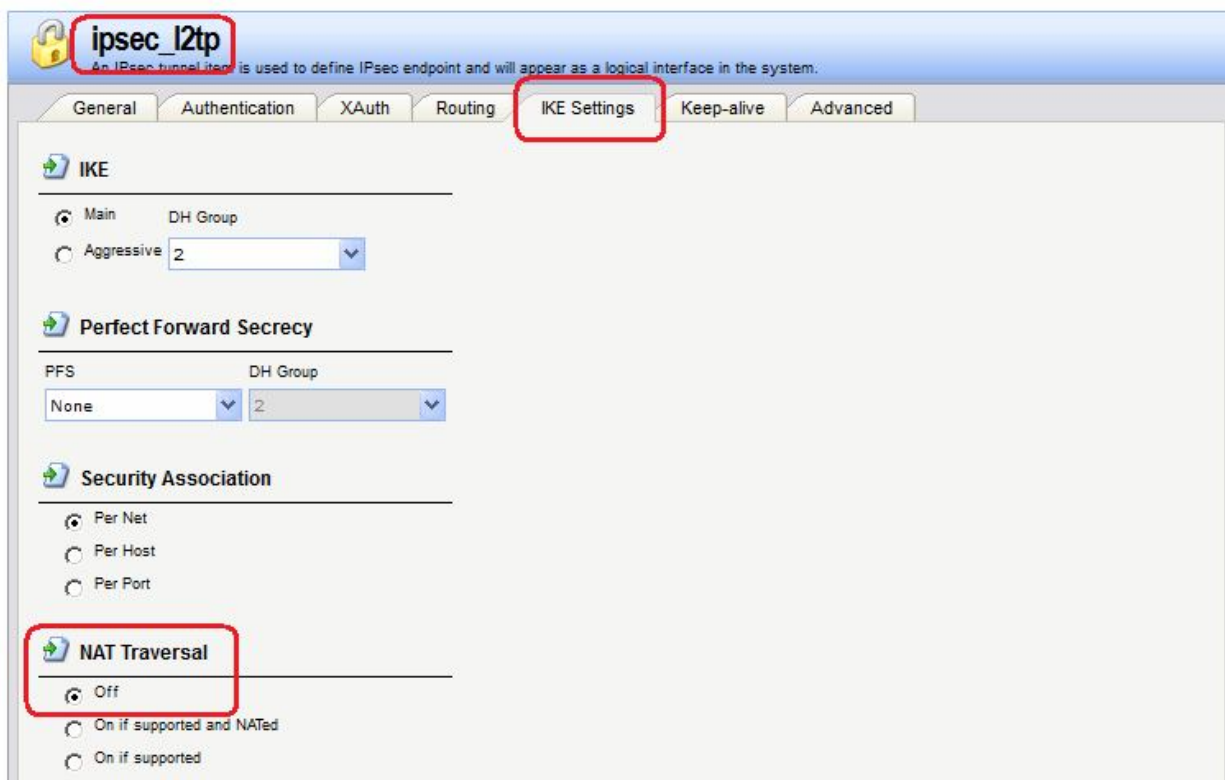
Описание практической работы

Межсетевой Экран 1

Все установки аналогичны установкам предыдущей лабораторной работы. Опишем только установки, которые отличаются от установок предыдущей лабораторной работы.

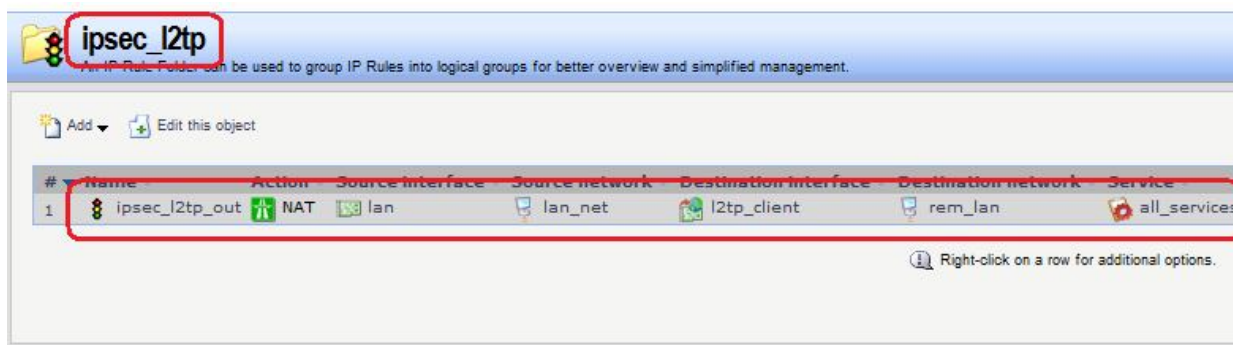
L2TP- и IPSec-Интерфейсы

NAT выполняется для L2TP-адресов. Поддержка NAT для IPSec не требуется.



Правила фильтрации

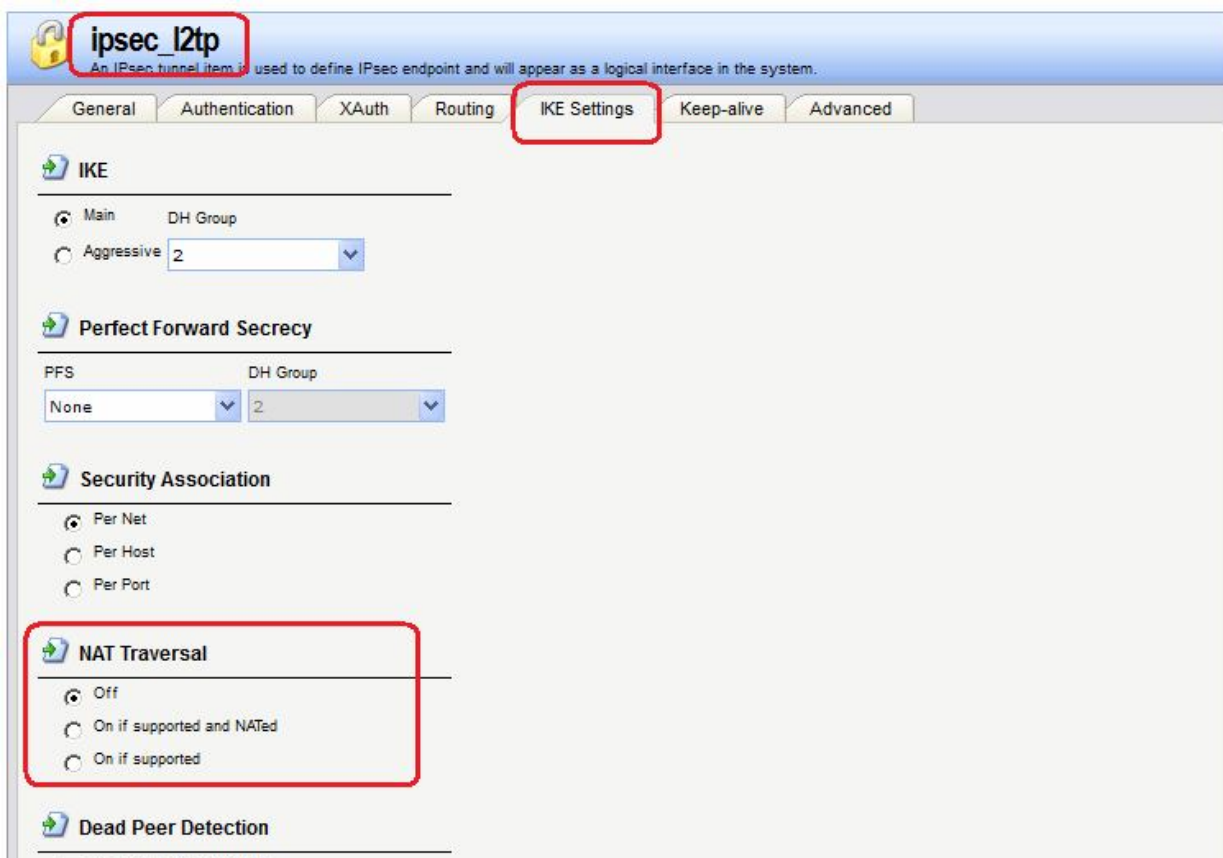
В Правилах фильтрации вместо действия **allow** следует указать действие **NAT**.



Межсетевой Экран 2

L2TP- и IPSec-Интерфейсы

NAT выполняется для L2TP-адресов. Поддержка NAT для IPSec не требуется.

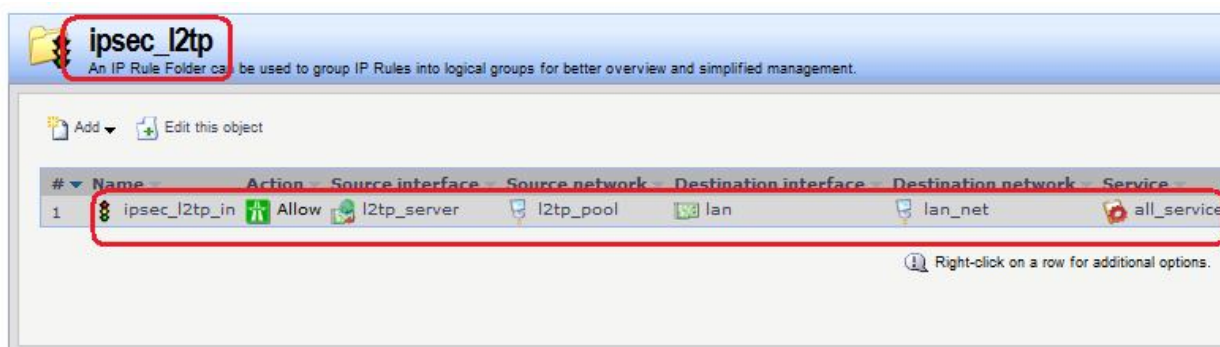


Правила фильтрации

В Правилах фильтрации вместо сети **remote_lan** следует указать пул IP-адресов, из которого выделяется IP-адрес противоположной стороне L2TP-туннеля.

Веб-интерфейс:

Rules → IP Rules → l2tp

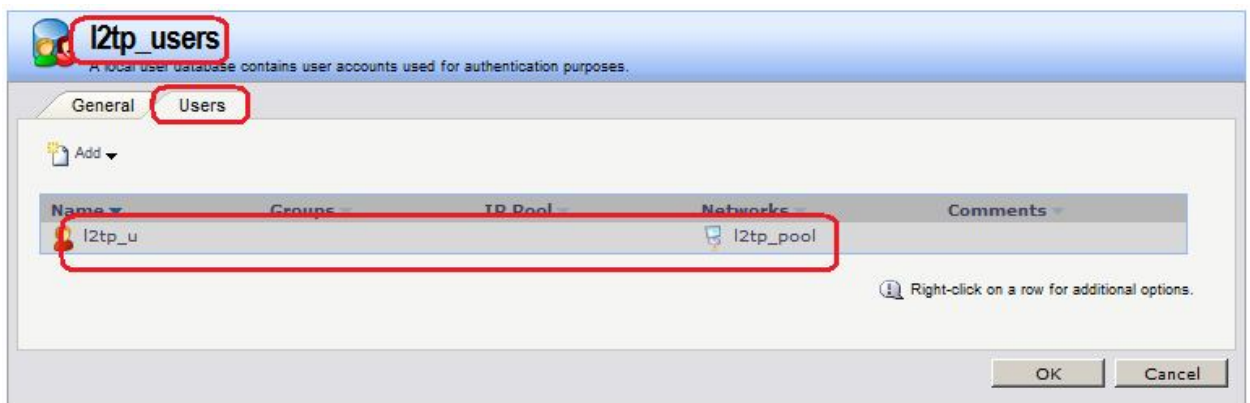


Командная строка:

```
set IPRule 1 DestinationNetwork=l2tp/l2tp_pool
```

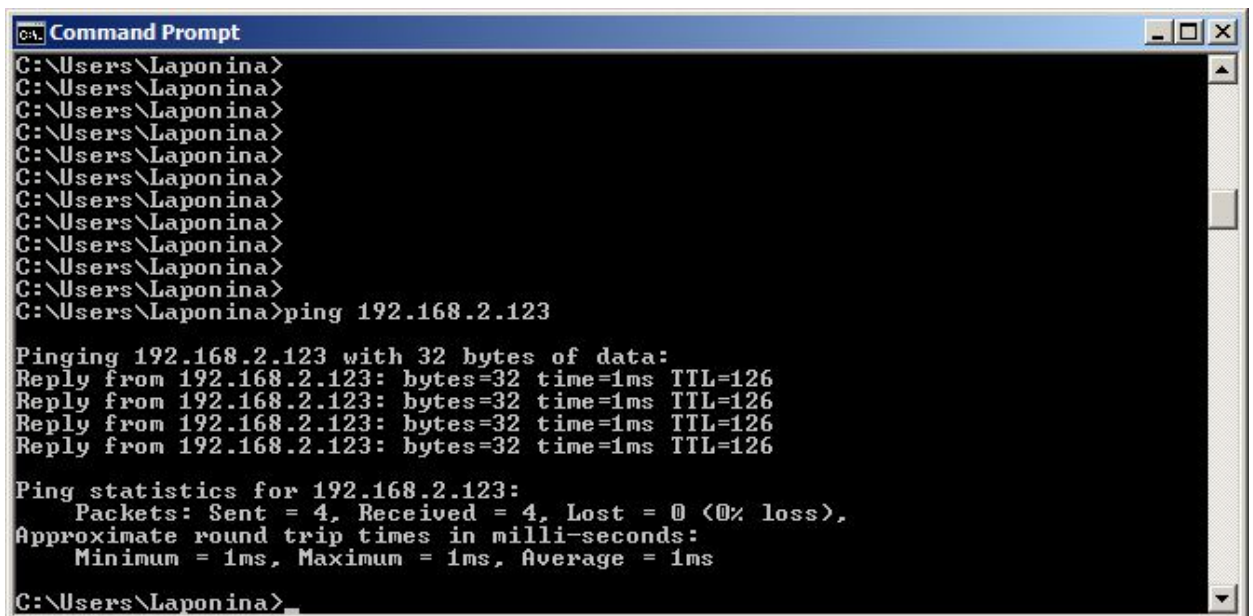
Аутентификация на уровне пользователя

В описании параметров пользователя вместо сети **remote_lan** следует указать пул IP-адресов, из которого выделяется IP-адрес противоположной стороне L2TP-туннеля.



Проверка конфигурации

На рабочей станции, расположенной за межсетевым экраном 1, выполним команду ping.



Получим дамп трафика аналогично тому, как это делалось в предыдущих лабораторных работах.

На интерфейсе wan2 видим IPSec-трафик.

Time	Source	Destination	Protocol	Length	Info
1 0.000000	192.168.20.20	192.168.20.10	ESP	94	ESP (SPI=0x6b1464a3)
2 0.000000	192.168.20.10	192.168.20.20	ESP	86	ESP (SPI=0x2fdb55a)
3 5.900000	192.168.20.10	192.168.20.20	ESP	150	ESP (SPI=0x2fdb55a)
4 5.900000	192.168.20.20	192.168.20.10	ESP	150	ESP (SPI=0x6b1464a3)
5 6.000000	192.168.20.10	192.168.20.20	ESP	150	ESP (SPI=0x2fdb55a)

Frame 1: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface wan2
 Ethernet II, Src: D-Link_49:de:3c (5c:d9:98:49:de:3c), Dst: D-Link_49:de:44 (5c:d9:98:49:de:44)
 Internet Protocol Version 4, Src: 192.168.20.20 (192.168.20.20), Dst: 192.168.20.10 (192.168.20.10)
 Encapsulating Security Payload

На интерфейсе ipsec_12tp видим L2TP-трафик.

Time	Source	Destination	Protocol	Length	Info
1 0.000000	192.168.20.20	192.168.20.10	L2TP	62	Control Message - Hello
2 0.000000	192.168.20.10	192.168.20.20	L2TP	54	Control Message - ZLB

Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
 Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
 Internet Protocol Version 4, Src: 192.168.20.20 (192.168.20.20), Dst: 192.168.20.10 (192.168.20.10)
 User Datagram Protocol, Src Port: 12f (1701), Dst Port: 12f (1701)
 Layer 2 Tunneling Protocol
 Packet Type: Control Message Tunnel Id=36461 Session Id=0
 Length: 20
 Tunnel ID: 36461
 Session ID: 0
 Message 11

На интерфейсе `l2tp_server` видим ICMP-трафик.

IP-адрес источника в ICMP-запросе принадлежит пулу IP-адресов, указанному для L2TP-клиента.

Time	Source	Destination	Protocol	Length	Info
1 0.000000	192.168.3.25	192.168.2.123	ICMP	74	Echo (ping) request
2 0.000000	192.168.2.123	192.168.3.25	ICMP	74	Echo (ping) reply

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
 Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
 Internet Protocol Version 4, Src: 192.168.3.25 (192.168.3.25), Dst: 192.168.2.123 (192.168.2.123)
 Internet Control Message Protocol

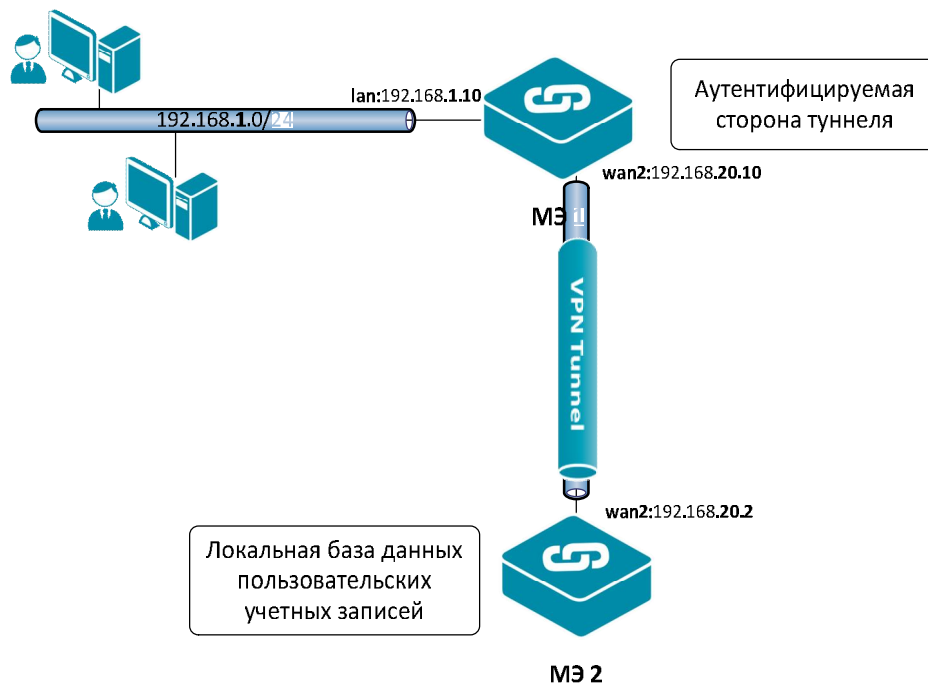
Аутентификация и хранение учетных записей

Лабораторная работа 11. Использование локальной БД для хранения учетных записей

Цель

Учетные записи пользователей хранятся в локальной базе данных.

Топология сети



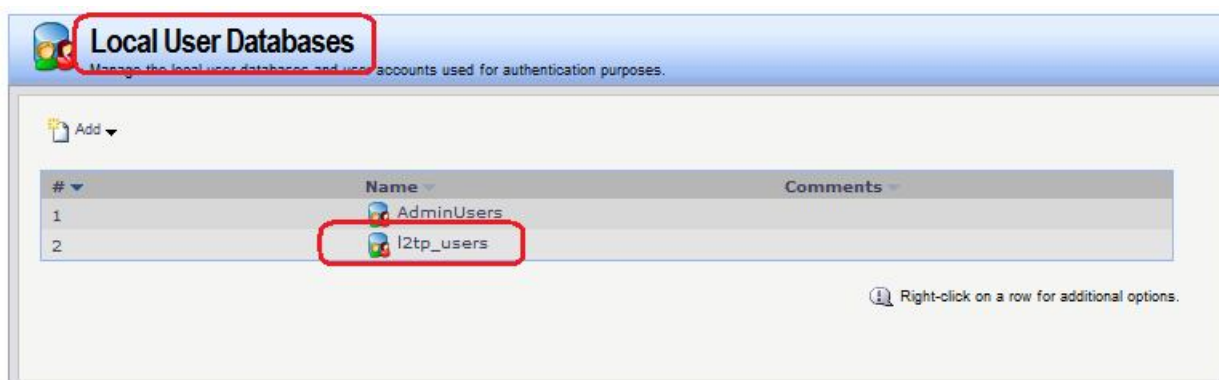
Описание практической работы

1. Создаем локальную базу данных.

Веб-интерфейс:

User Authentication → Local User Databases → Add

Name: l2tp_users



Командная строка:

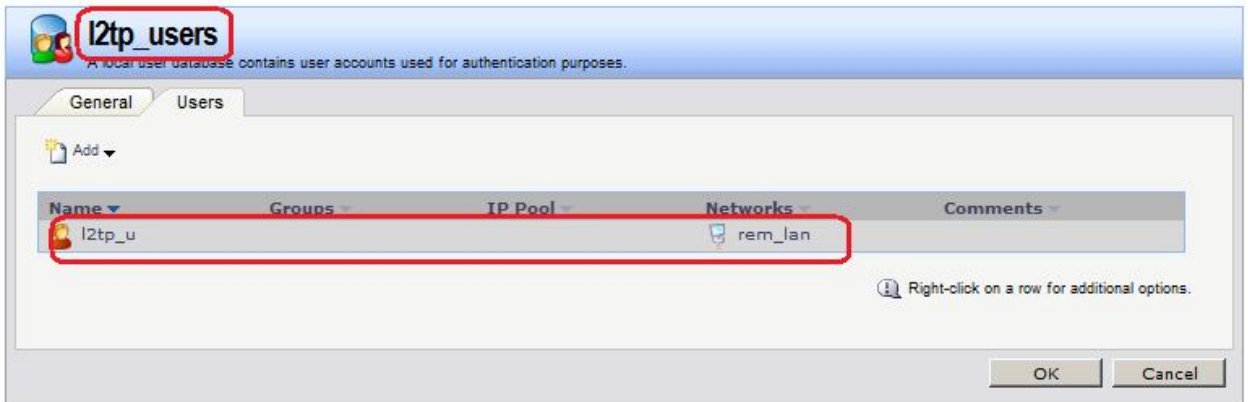
```
add LocalUserDatabase l2tp_users
```

2. Создаем учетные записи пользователей.

Веб-интерфейс:

User Authentication → Local User Databases → l2tp_users

Вкладка Users → Add



Командная строка:

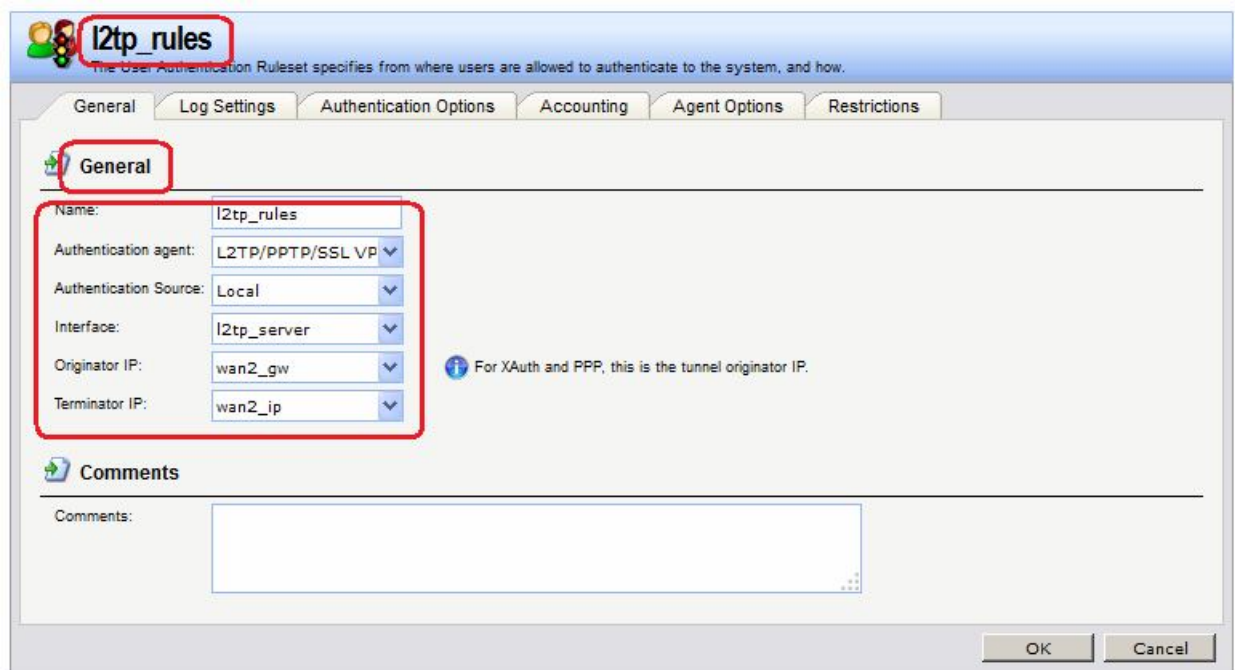
```
add User l2tp_u Password=qwerty AutoAddRouteNet=remote/rem_lan
```

3. Создаем правило аутентификации пользователей.

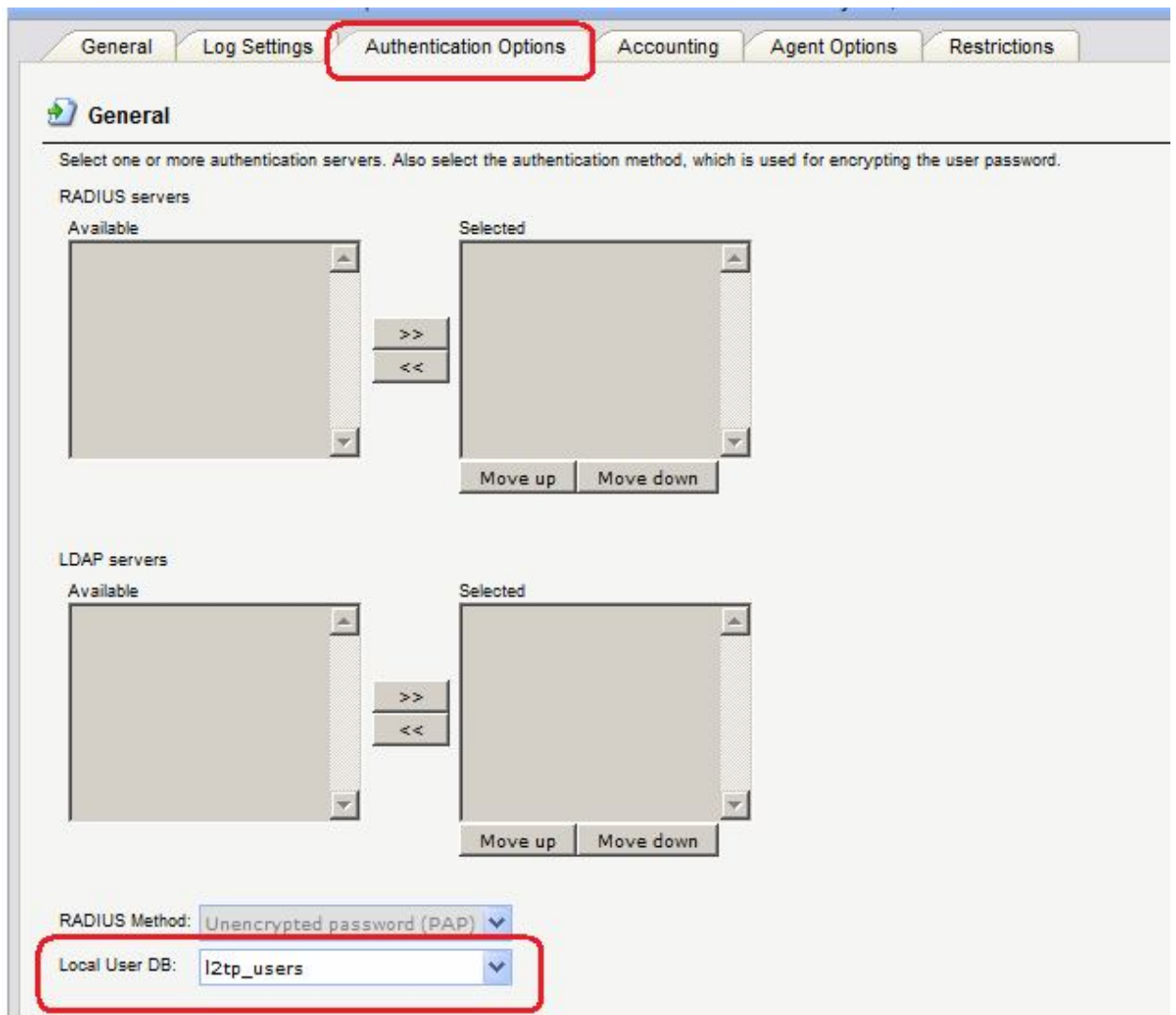
Веб-интерфейс:

User Authentication → User Authentication Rules → Add

На вкладке **General** указать аутентификационный источник **Local** и необходимые для туннелирующего протокола опции. В нашем случае туннелирующим протоколом является L2TP.



На вкладке **Authentication Options** указать имя локальной базы данных пользователей.



На вкладке **Agent Options** указать параметры PPP-аутентификации.

l2tp_ua
The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

General Log Settings Authentication Options Accounting **Agent Options** Restrictions

PPP Agent Options

- Allow no authentication.
- Use PAP authentication protocol. User name and password are sent in plaintext.
- Use CHAP authentication protocol.
- Use MS-CHAP authentication protocol.
- Use MS-CHAP v2 authentication protocol.

HTTP(s) Agent Options

Login Type:

HTTP Banners:

Realm String:

MAC Authentication

Allow Clients behind router to connect

MAC Auth Secret: Password used to authenticate MAC user, if empty the MAC address will be sent as password.

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

HTTPS Certificates

Host Certificate:

Root Certificate:

Командная строка:

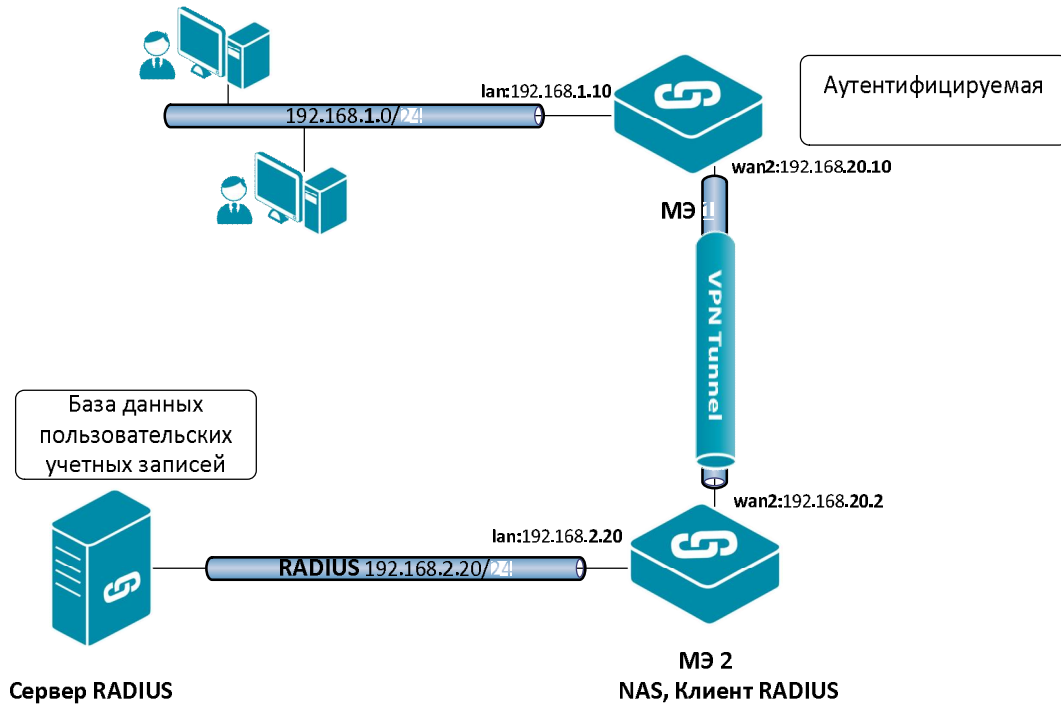
```
add UserAuthRule AuthSource=Local Interface=l2tp_server
LocalUserDB=l2tp_users OriginatorIP=wan2/wan2_gw Agent=PPP
TerminatorIP=wan2/wan2_ip Name=l2tp_rules
```

Лабораторная работа 12. Использование сервера RADIUS для хранения учетных записей

Цель

Учетные записи пользователей хранятся на отдельном сервере, доступ к которому выполняется по протоколу RADIUS.

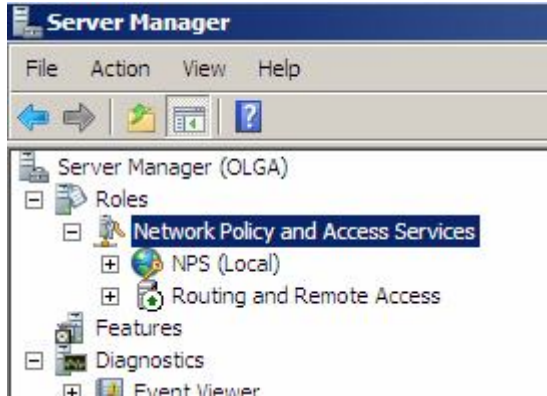
Топология сети



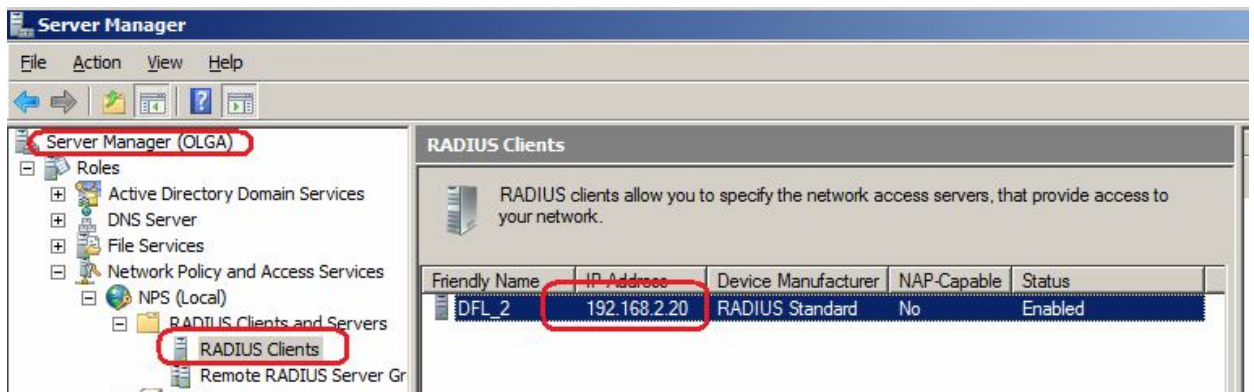
Описание практической работы

Сервер RADIUS

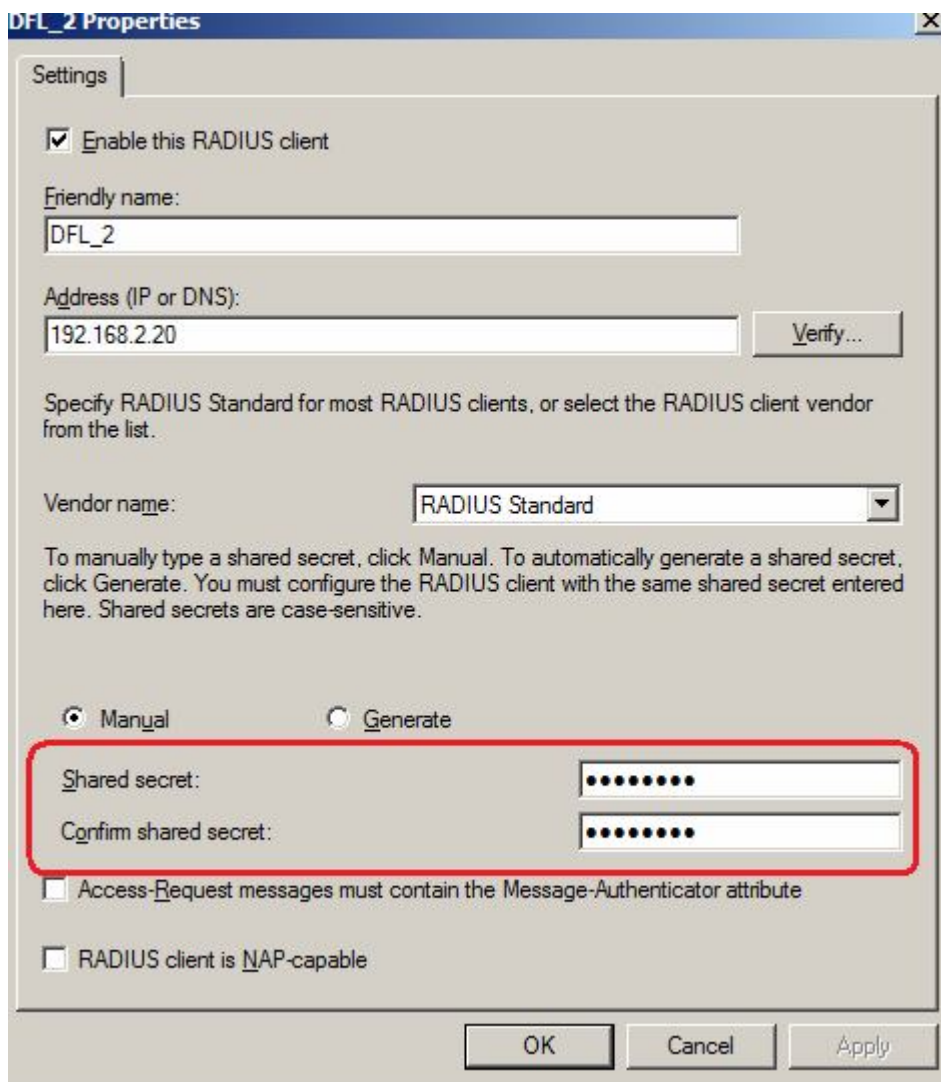
На Windows Server 2008 добавить роль **Network Policy and Access Services**.



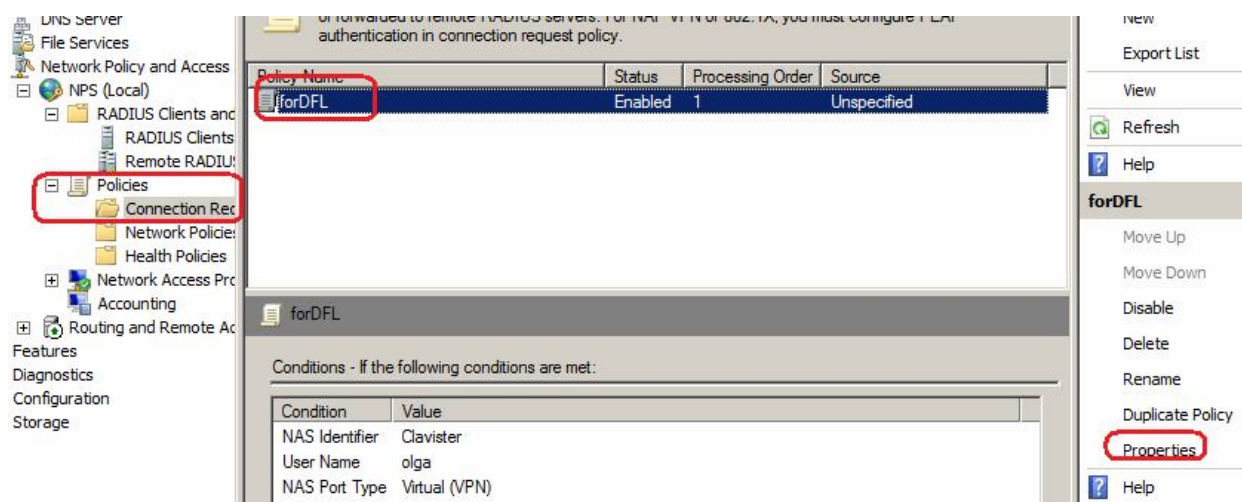
В качестве RADIUS-клиента указать IP-адрес MЭ 2.



В свойствах указать тот же самый разделяемый секрет, что на NAS.



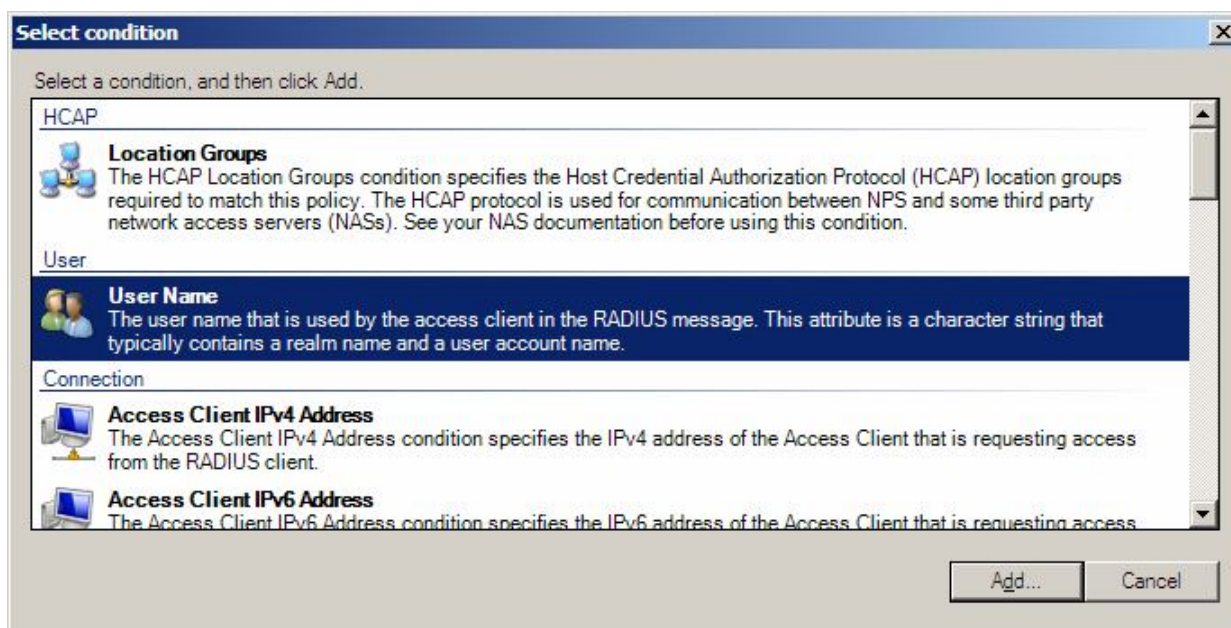
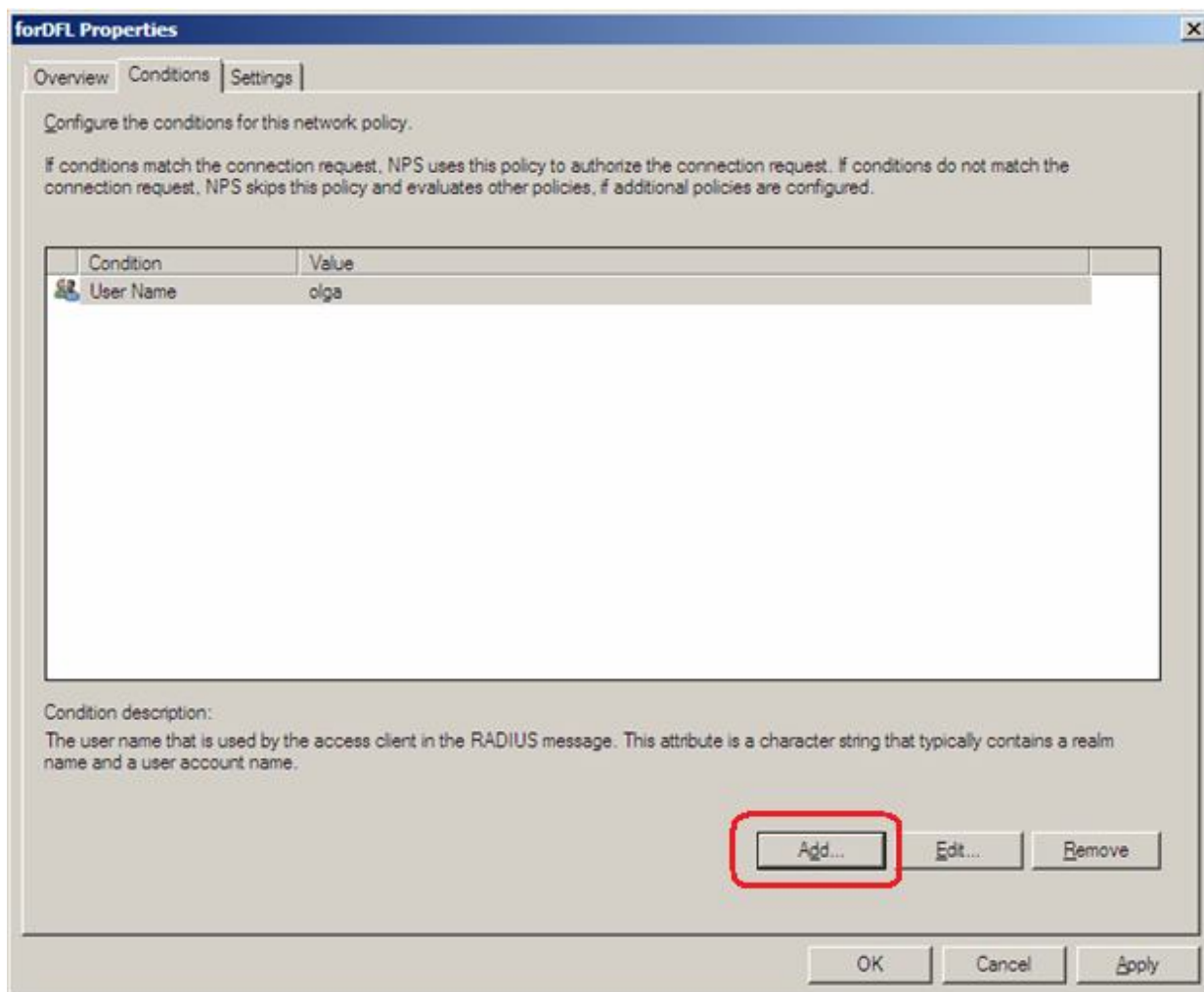
Создать политику запроса соединения (Connection Request Policies), в которой указать атрибуты RADIUS, присылаемые NAS.



Могут быть добавлены различные условия аутентификации NAS. Эта информация должна присылаться NAS при запросе доступа.

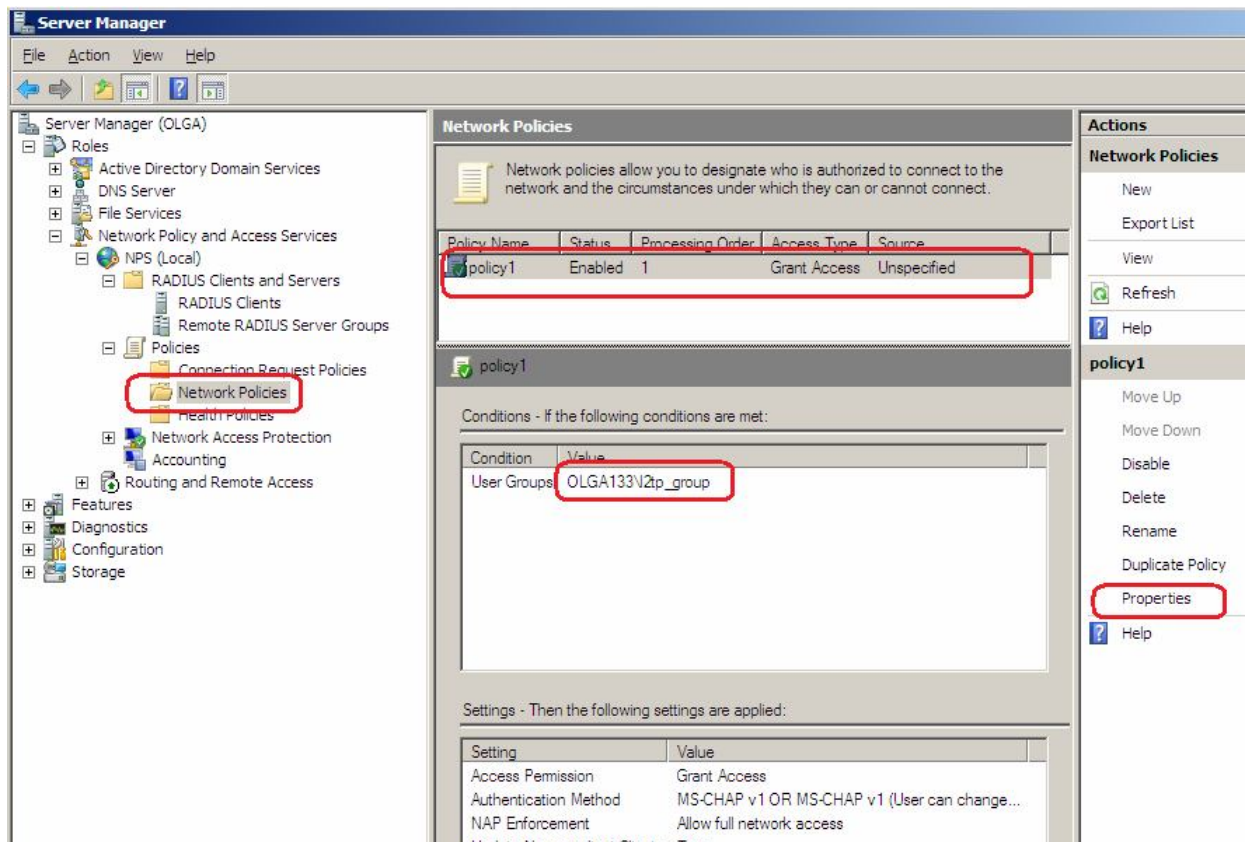
Имена пользователей, которым разрешен доступ и, следовательно, они могут быть указаны на аутентифицируемой стороне туннеля, задаются следующими способами.

1. В политиках запроса соединения (Connection Request Policies) можно указать имя пользователя, задаваемое на аутентифицируемой стороне туннеля.



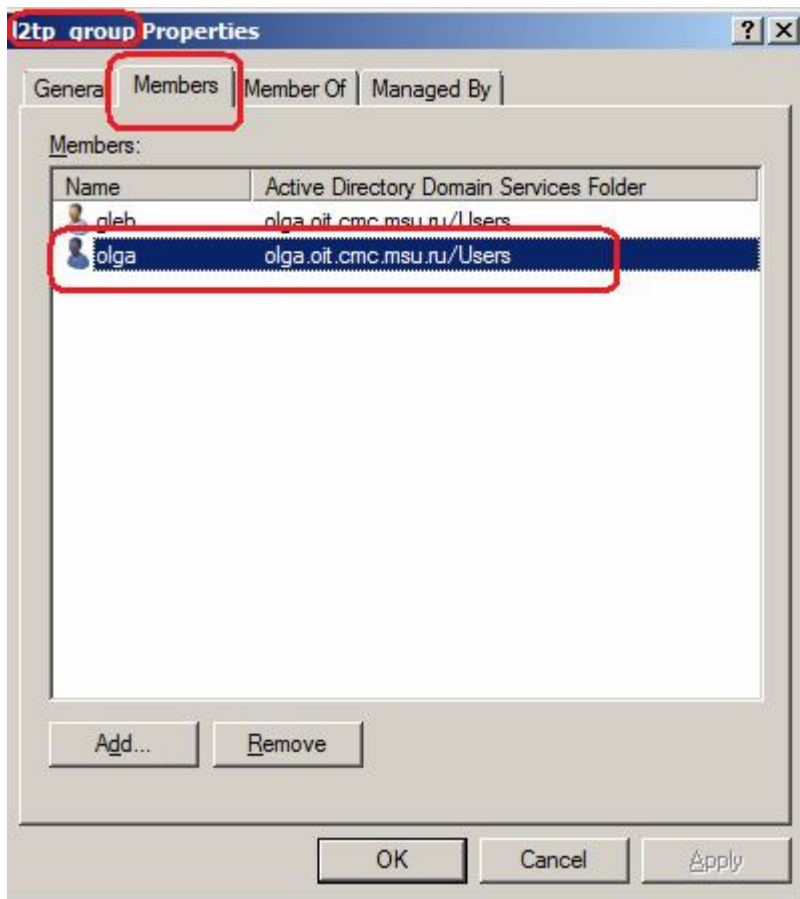
2. В политиках сети (Network Policies) перечислить группы, членам которых разрешен доступ.

На сервере RADIUS:



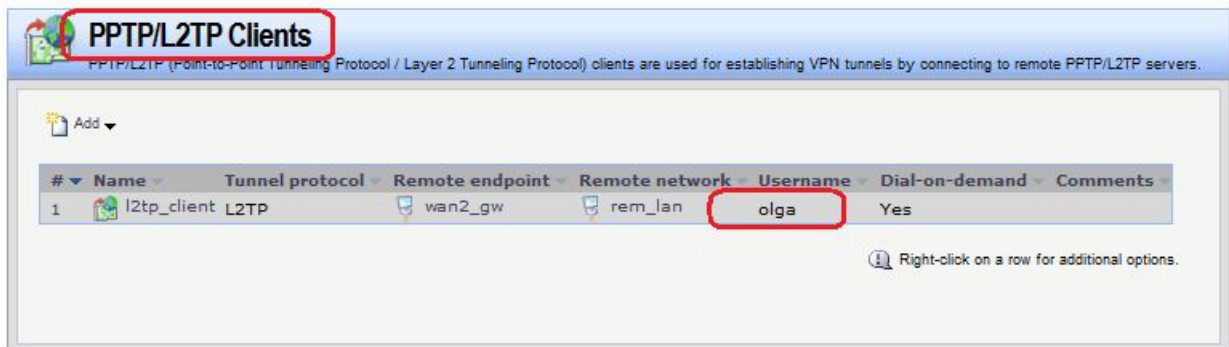
В данном примере члены группы **12tp_group** могут быть указаны на аутентифицируемой стороне туннеля.

Roles → Active Directory Users and Computers → Users → 12tp_group



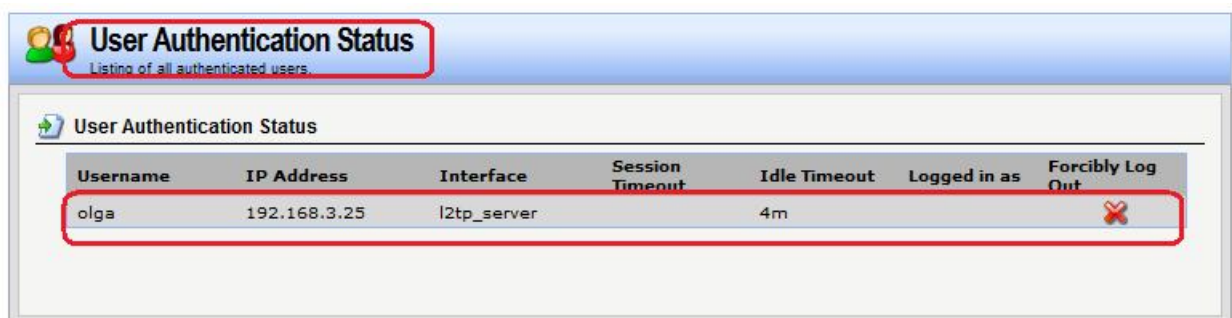
На аутентифицируемой стороне туннеля указывается имя пользователя:

Interfaces → **PPTP/L2TP Clients**



На стороне NAS проверяется, что аутентификация выполнена:

Status → **User Authentication**



NAS

Объекты Адресной Книги

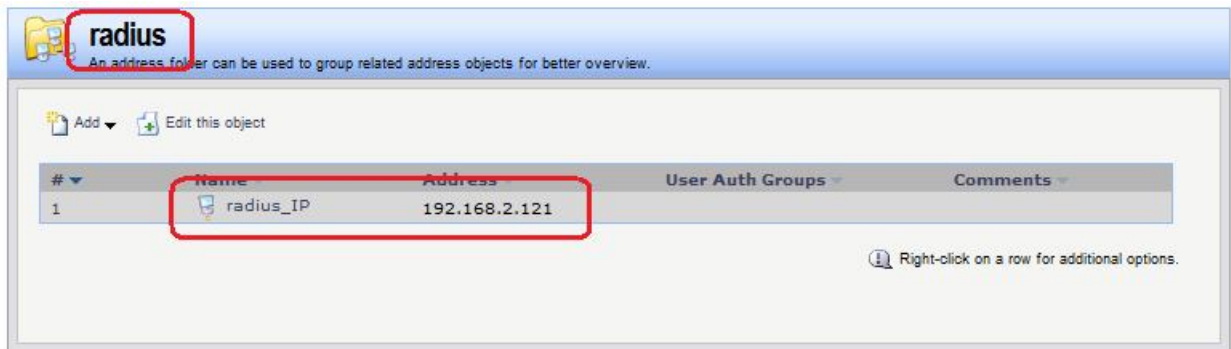
Создать объекты, описывающие IP-адреса RADIUS-серверов аутентификации и авторизации.

Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: radius

Object → Address Book → radius → Add



Командная строка:

```
add Address AddressFolder radius
```

```
cc Address AddressFolder radius
```

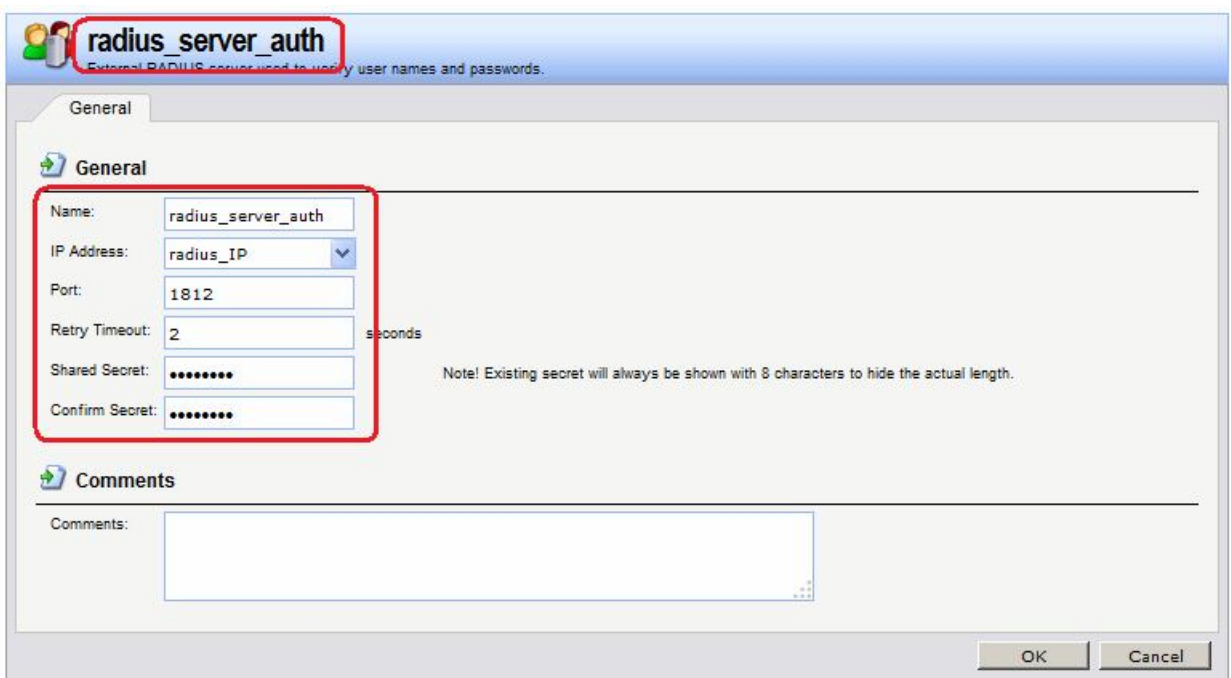
```
add IP4Address radius_ip Address=192.168.2.121
```

Ссылка на RADIUS-сервера

Создать ссылку на внешнюю базу данных пользователей, в которой указывается тот же пароль, что и на сервере RADIUS.

Веб-интерфейс:

User Authentication → External User Databases → Add → RADIUS Server



Командная строка:

```
add RadiusServer radius_server_auth IPAddress=radius/radius_IP  
SharedSecret=qwerty
```

Создать ссылку на сервер хранения учетных записей RADIUS, в которой указывается тот же пароль, что и на сервере RADIUS.

Веб-интерфейс:

User Authentication → Accounting Servers → Add → RADIUS Server

radius_server_ac
External RADIUS server used to collect user statistics.

General

Name: radius_server_ac

IP Address: radius_IP

Port: 1813

Retry Timeout: 2 seconds

Shared Secret:

Confirm Secret:

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

Comments:

OK Cancel

Командная строка:

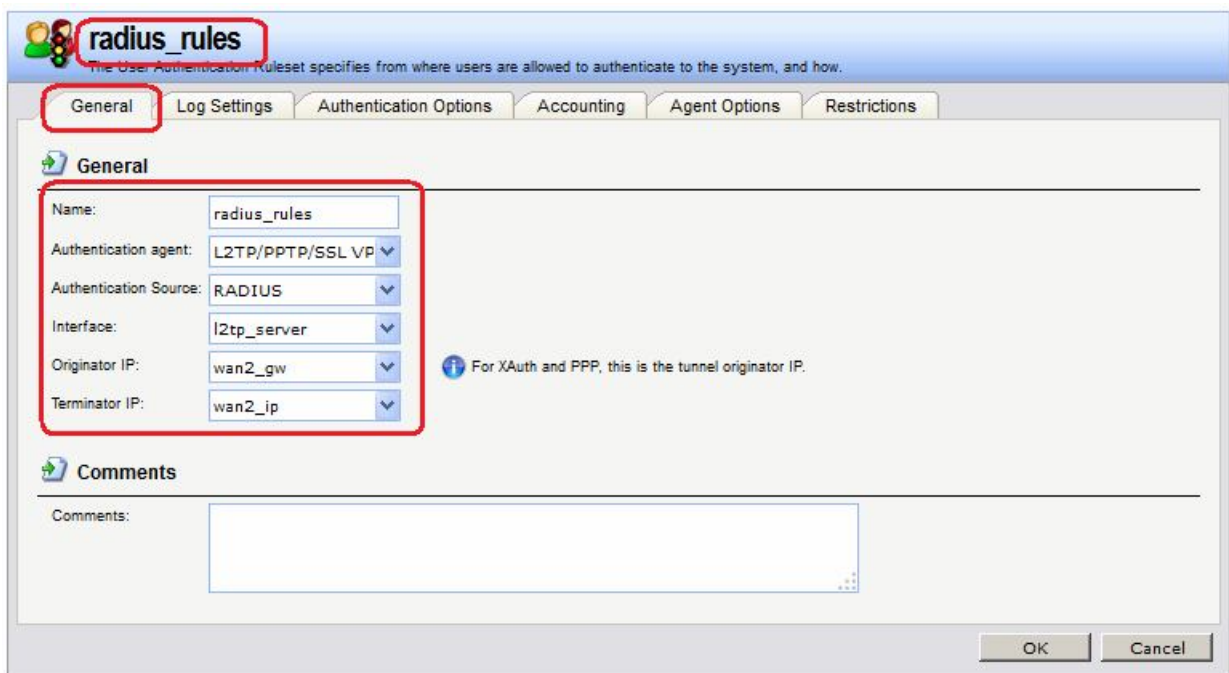
```
add RadiusAccounting radius_server_ac IPAddress=radius/radius_IP  
SharedSecret=qwerty
```

Правила аутентификации

Указать правила аутентификации.

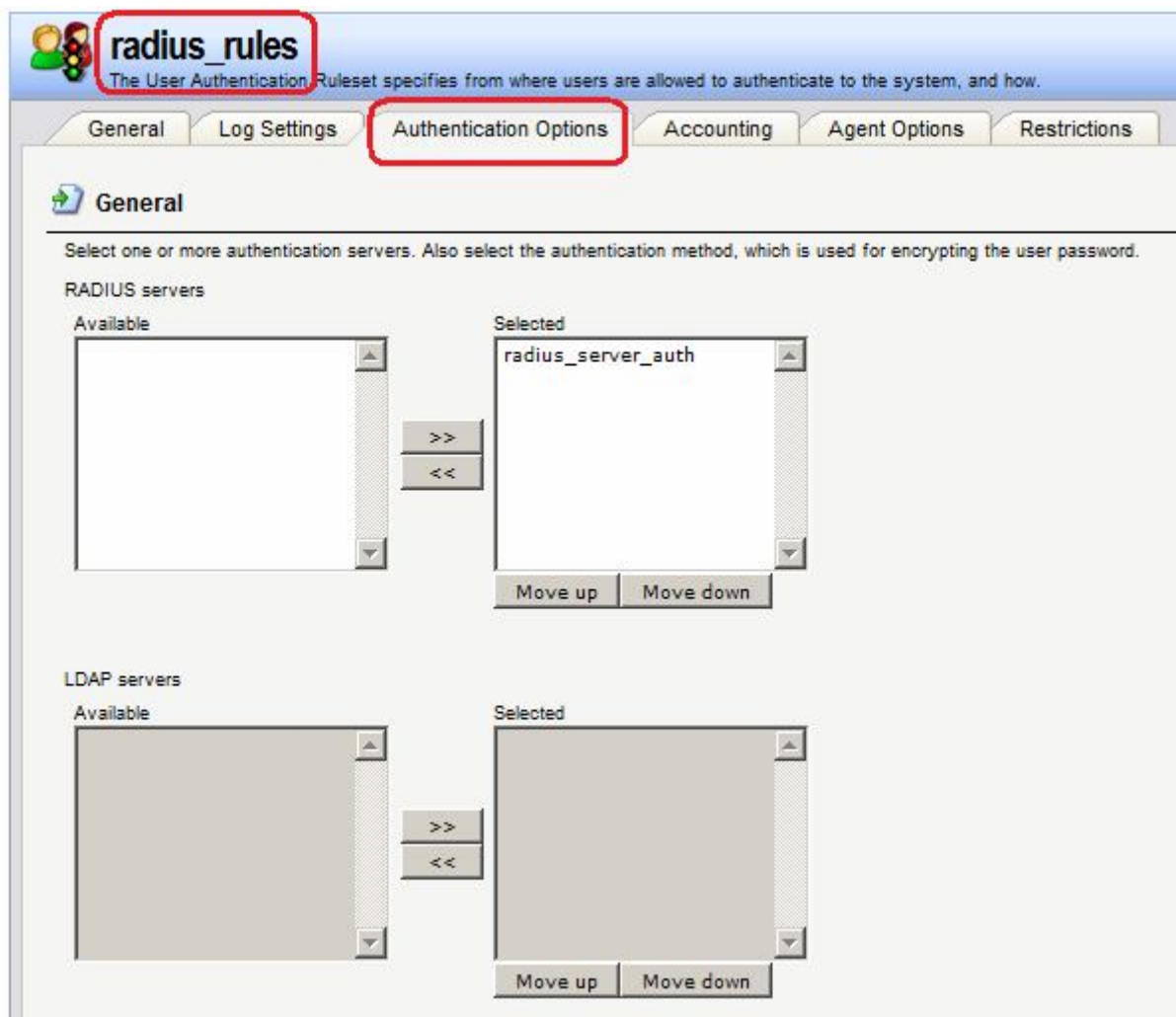
Веб-интерфейс:

User Authentication Rules → Add User Authentication Rule

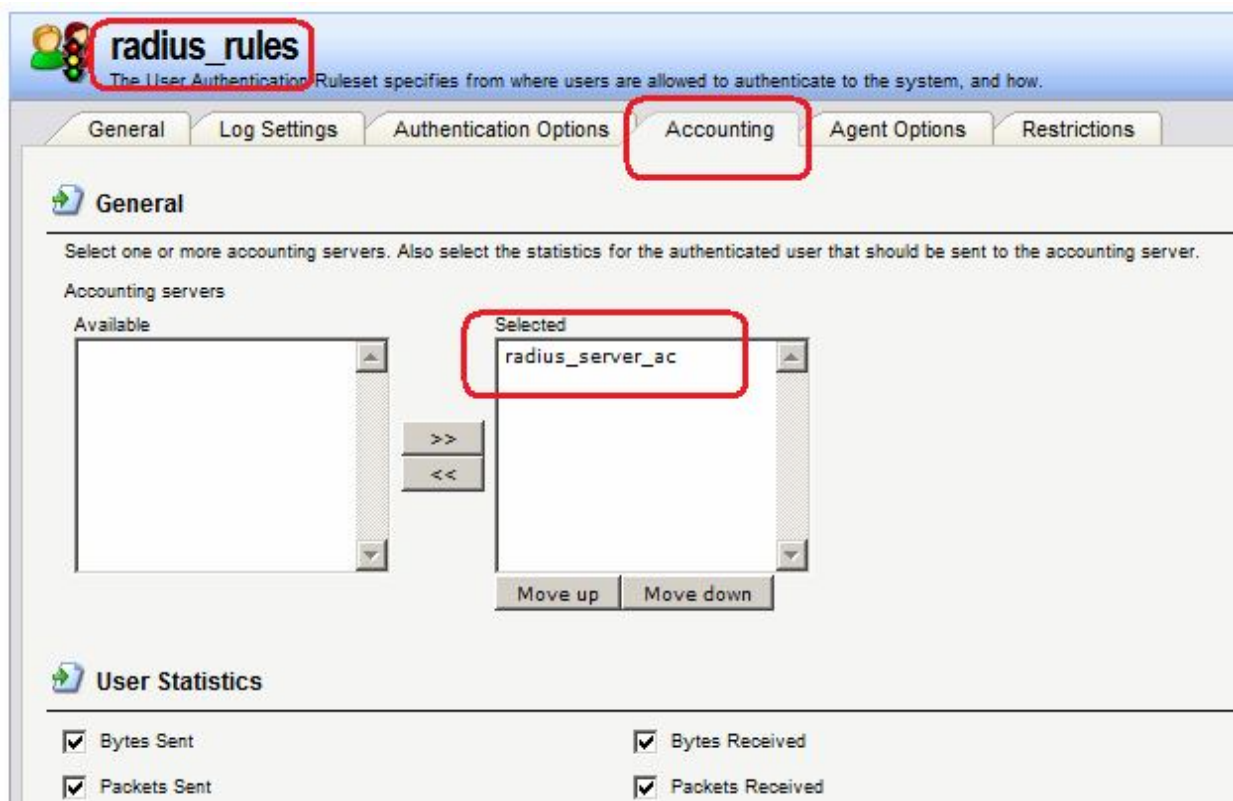


В качестве интерфейса указать интерфейс `l2tp_server`. В качестве исходного IP-адреса указать IP-адрес противоположной точки туннеля. В качестве IP-адреса завершения (**Terminator IP**) указать IP-адрес на локальной стороне.

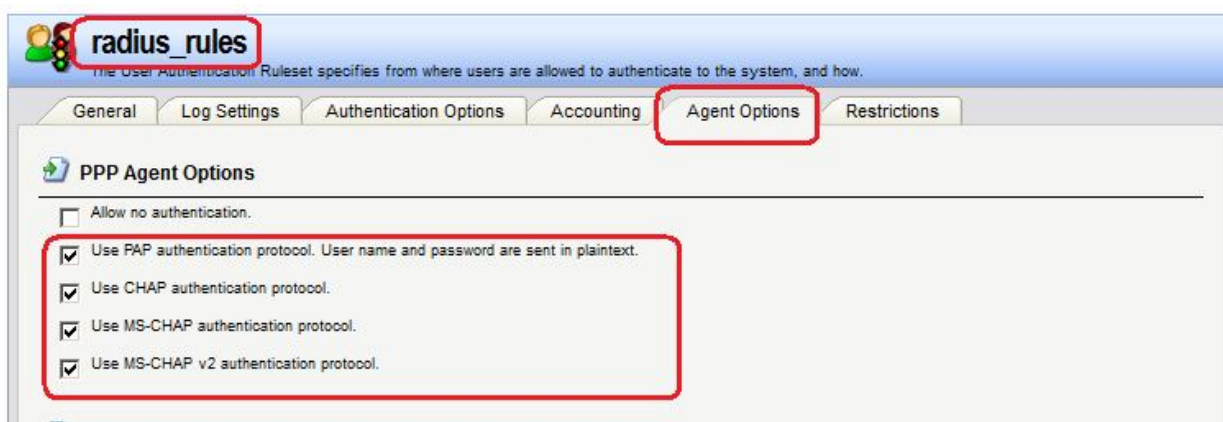
На вкладке **Authentication Options** выбрать созданный RADIUS-Сервер.



На вкладке **Accounting** выбрать созданный RADIUS-Сервер.



На вкладке **Agent Options** указать параметры PPP-шифрования.



Командная строка:

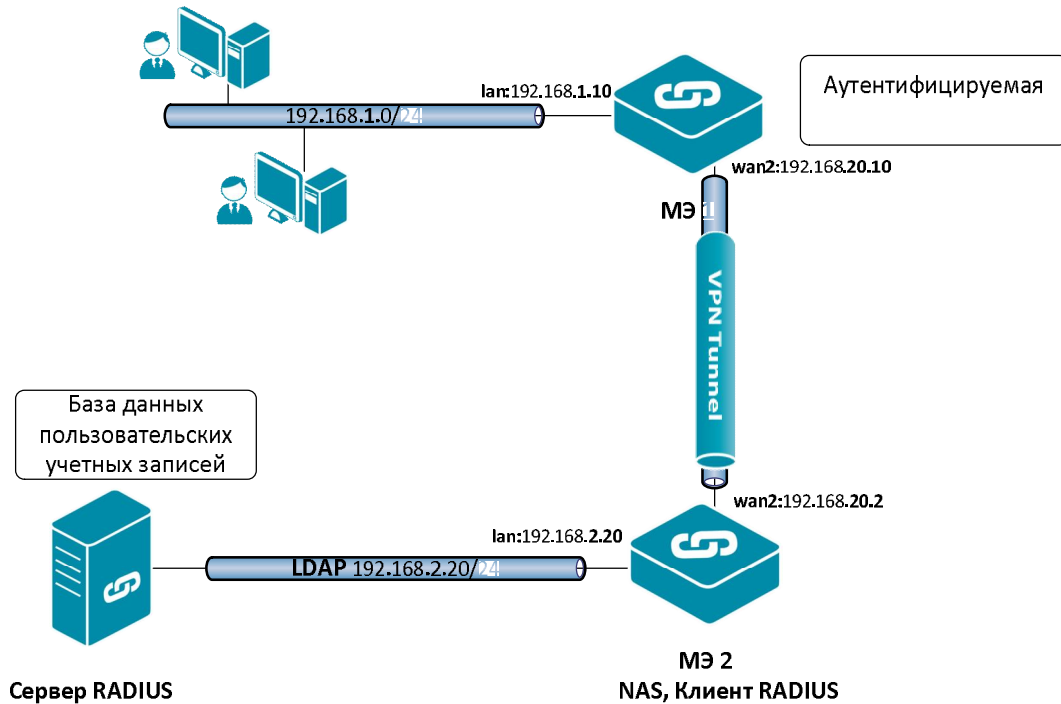
```
add UserAuthRule AuthSource=RADIUS Interface=l2tp  
OriginatorIP=wan1/wan1_gwFW2 RadiusServers=W2K8_radius Agent=PPP  
TerminatorIP=wan1/wan1_ipFW2 AccountingServers=W2K8_radius Name=l2tp_radius
```

Лабораторная работа 13. Использование сервера LDAP/MS AD для хранения учетных записей

Цель

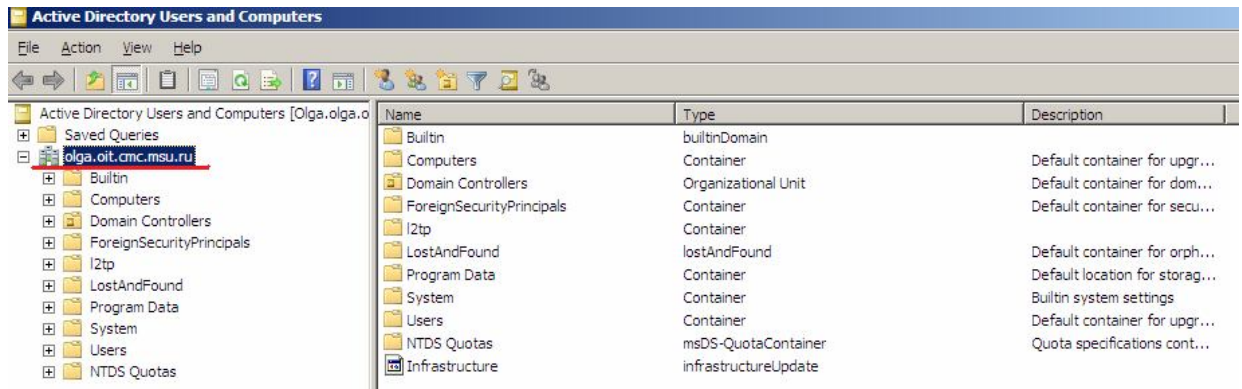
Учетные записи пользователей хранятся в MS AD сервере.

Топология сети



Описание практической работы

1. Создать AD с DNS-именем olga.oit.cmc.msu.ru



2. На межсетевом экране создать внешнюю базу данных пользователей. DNS-имя MS Active Directory указывается при создании этой базы данных.

Веб-интерфейс:

User Authentication → External User Databases → Add → LDAP Server

W2K8_AD
External LDAP server used to verify user names and passwords.

General

General

Name:

IP Address:

Port:

Timeout: seconds

Name Attribute:

Retrieve Group Membership

Membership Attribute:

Use Domain Name:

Database Settings

Base Object:

Administrator Account:

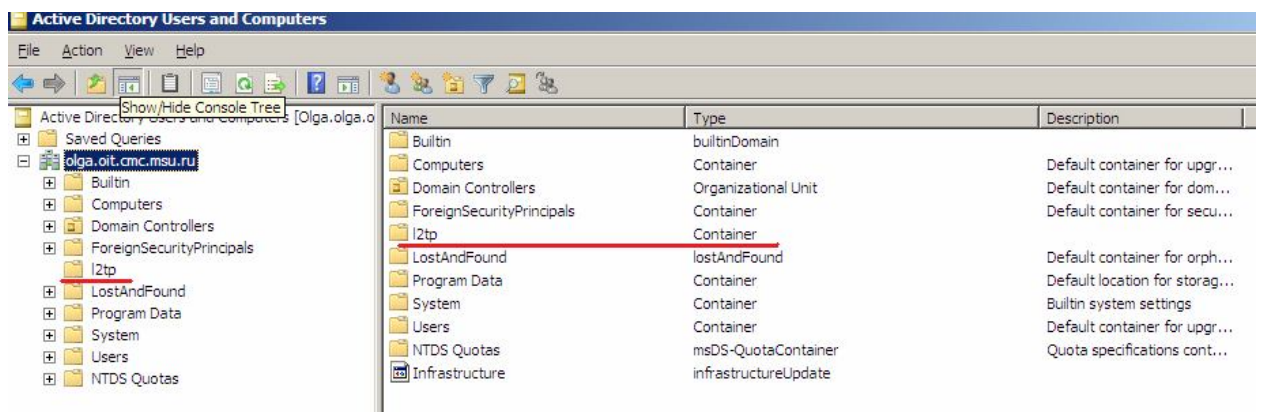
Password: Note! Existing passwords will always be shown with 8 c

Confirm Password:

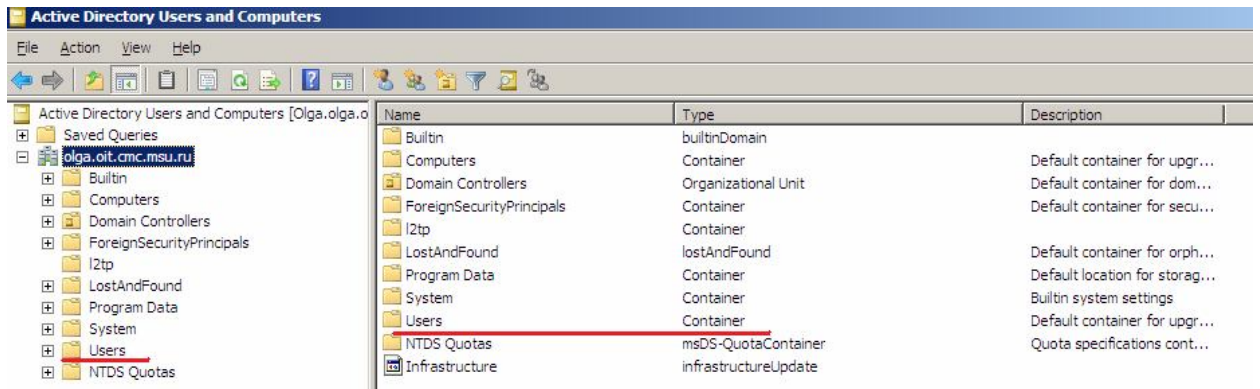
Domain Name:

В поле **Base Object** DNS-имя указано в формате DN, в поле **Domain Name** в формате DNS.

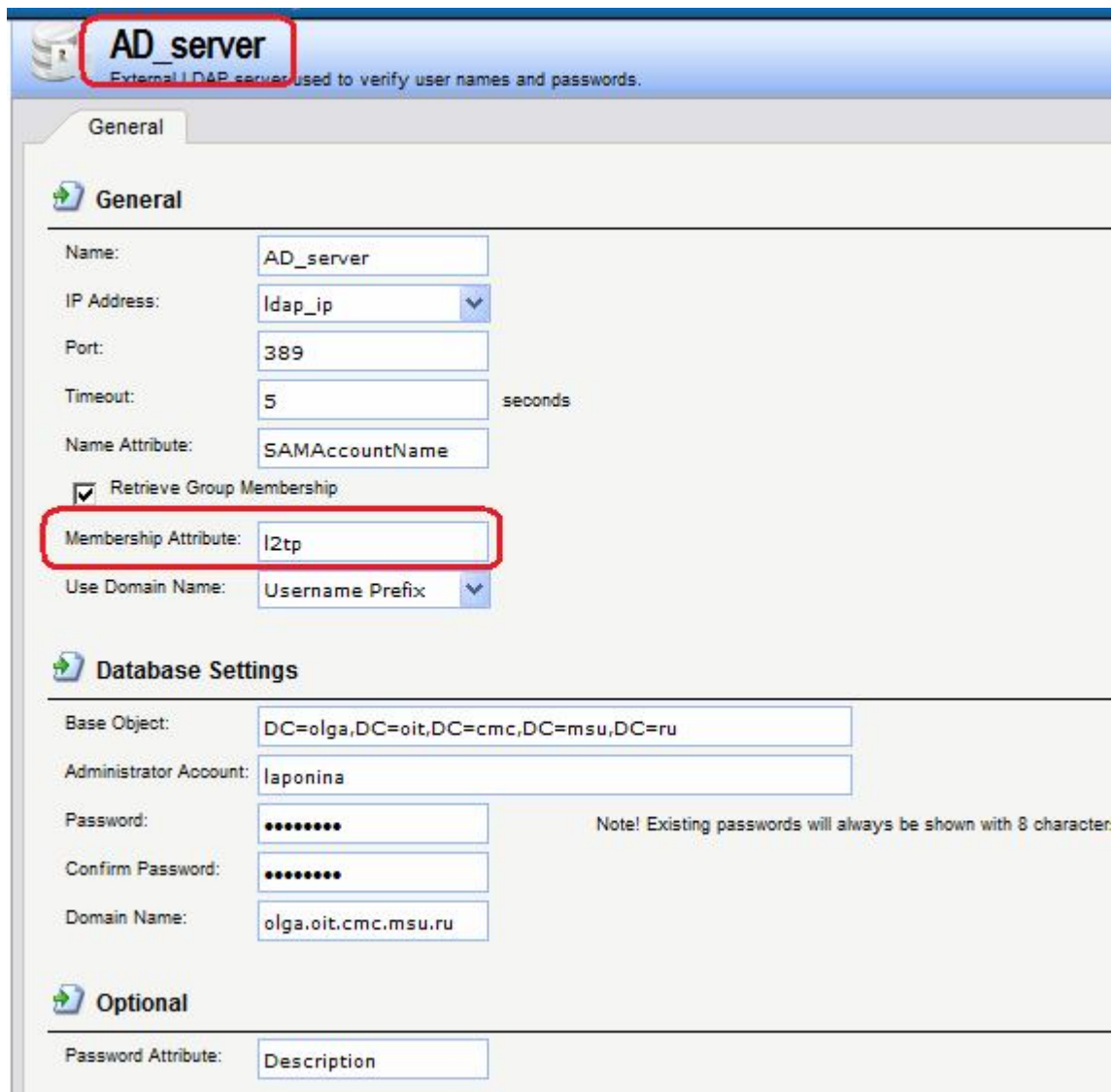
3. В AD создать контейнер хранения учетных записей удаленных пользователей.



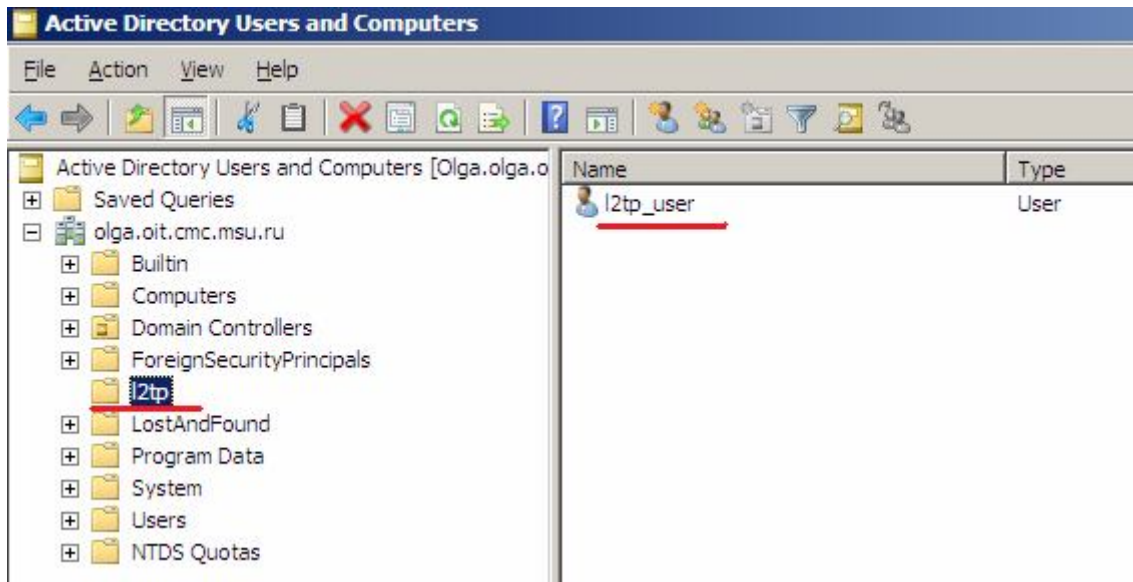
Или использовать существующий контейнер, например, **Users**:



Имя этого контейнера указывается в параметрах создания внешней базы данных пользователей на межсетевом экране, который выполняет функции NAS и является клиентом RADIUS.



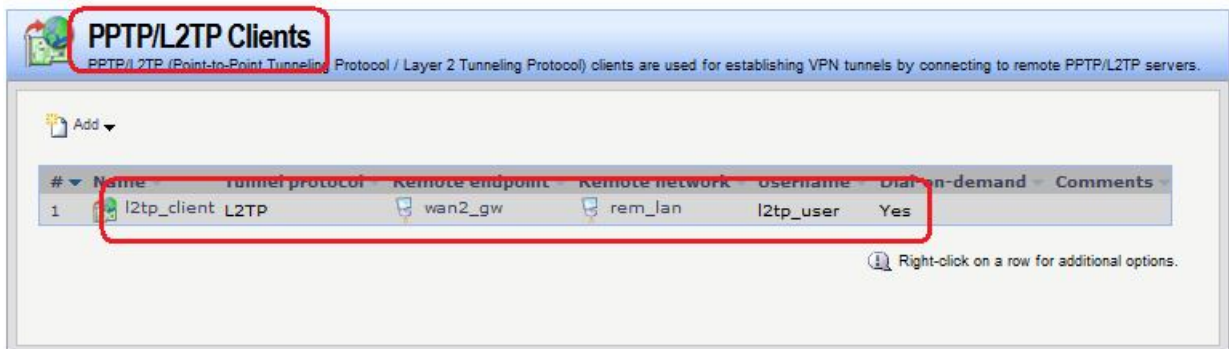
- В выбранном контейнере создать пользователя, в нашем случае создается пользователь **l2tp_user** в контейнере **l2tp**.



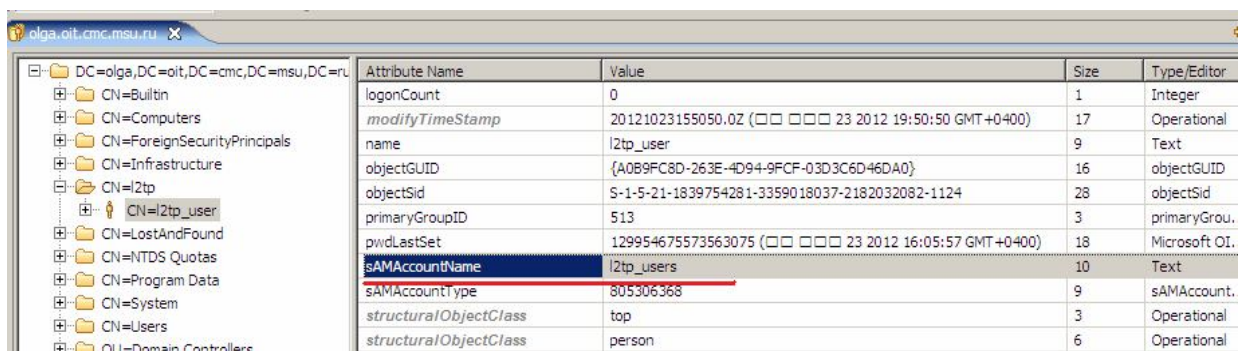
- Имя этого пользователя указывается на противоположной стороне туннеля (в нашем случае на стороне L2TP-клиента).

Веб-интерфейс:

Interfaces → PPTP/L2TP Clients → Add → PPTP/L2TP Client



- Имя пользователя в AD является значением атрибута **sAMAccountName**.



- Имя этого атрибута указывается в поле **Name Attribute** в параметрах создания внешней базы данных пользователей на межсетевом экране.

AD_server
External LDAP server used to verify user names and passwords.

General

General

Name: AD_server

IP Address: ldap_ip

Port: 389

Timeout: 5 seconds

Name Attribute: SAMAccountName

Retrieve Group Membership

Membership Attribute: l2tp

Use Domain Name: Username Prefix

Database Settings

Base Object: DC=olga,DC=oit,DC=cmc,DC=msu,DC=ru

Administrator Account: laponina

Password: Note! Existing passwords will always be shown with 8 characters to hide the a

Confirm Password:

Domain Name: olga.oit.cmc.msu.ru

Optional

Password Attribute: Description

8. Аутентификация противоположной стороны туннеля (в нашем случае L2TP-клиента) выполняется по значению поля, имя которого указано в поле **Password Attribute** в параметрах создания внешней базы данных пользователей на межсетевом экране.

AD_server
External LDAP server used to verify user names and passwords.

General

General

Name:

IP Address:

Port:

Timeout: seconds

Name Attribute:

Retrieve Group Membership

Membership Attribute:

Use Domain Name:

Database Settings

Base Object:

Administrator Account:

Password: Note! Existing passwords will always be shown with 8 characters

Confirm Password:

Domain Name:

Optional

Password Attribute:

9. Тип этого поля должен быть **Text**.

olga.oit.cmc.msu.ru

Attribute Name	Value	Size	Type/Editor
objectCategory	CN=Person,CN=Schema,CN=Configuration,DC=olga,DC=oit,DC=...	71	DN
nTSecurityDescriptor		0	Text
accountExpires	9223372036854775807 (□□□□ 14 30828 06:48:05 GMT+0400)	19	Microsoft OI...
badPasswordTime	0	1	Microsoft OI...
badPwdCount	0	1	Integer
codePage	0	1	Integer
countryCode	0	1	Integer
createTimeStamp	20121023120557.0Z (□□□□ 23 2012 16:05:57 GMT+0400)	17	Operational
<u>description</u>	qwerty	6	<u>Text</u>
displayName	l2tp_user	9	Text
distinguishedName	CN=l2tp_user,CN=l2tp,DC=olga,DC=oit,DC=cmc,DC=msu,DC=ru	55	DN
dSCorePreparationData	1601101000000.07 (□□□□ 01 1601 04:00:00 GMT+0400)	17	Generalized

10. Значение поля указывается в AD.

The image shows a Windows dialog box titled "l2tp_user Properties". The "General" tab is active. The "Description" field is highlighted with a red rectangle and contains the text "qwerty". Other fields include "First name: l2tp_user", "Display name: l2tp_user", and "Office:". Buttons for "OK", "Cancel", "Apply", and "Help" are at the bottom.

Published Certificates	Member Of	Password Replication	Dial-in	Object	
Security	Environment	Sessions	Remote control		
Terminal Services Profile	COM+	Attribute Editor			
General	Address	Account	Profile	Telephones	Organization

l2tp_user

First name: Initials:

Last name:

Display name:

Description:

Office:

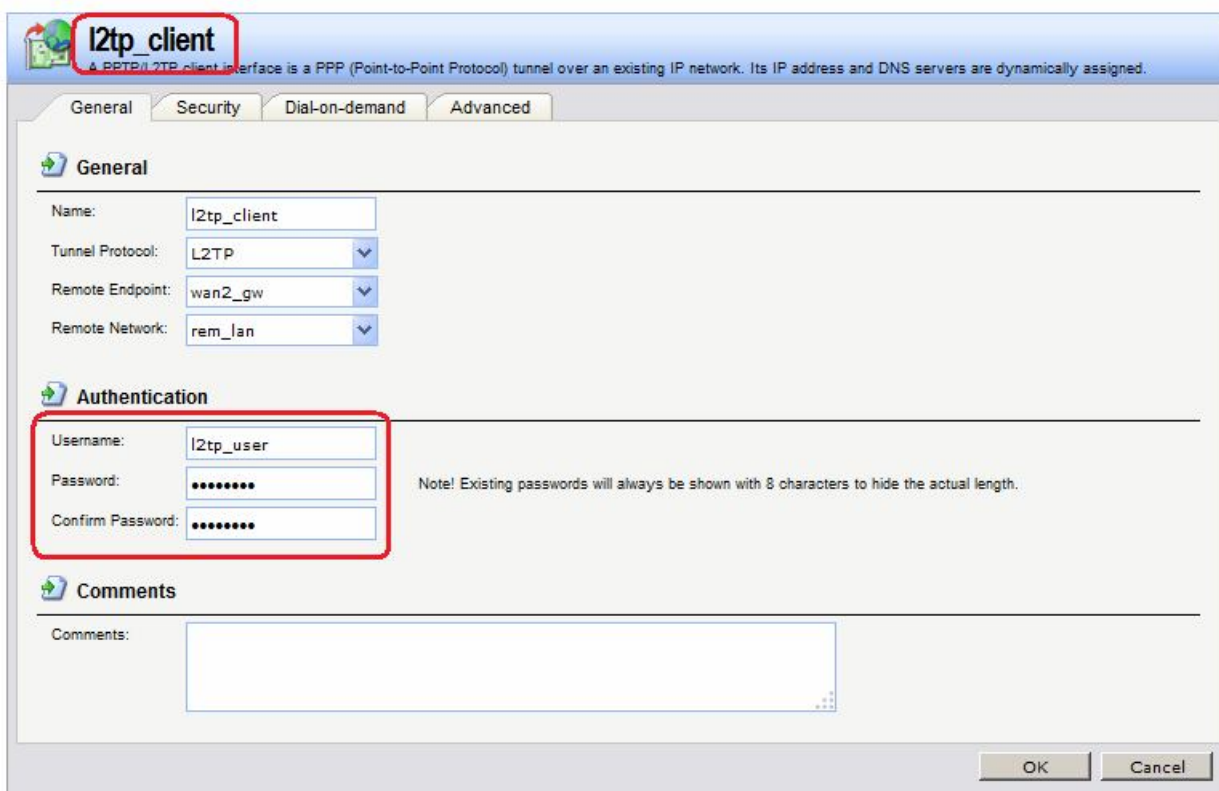
Telephone number: Other...

E-mail:

Web page: Other...

OK Cancel Apply Help

11. И на противоположной стороне туннеля (в нашем случае L2TP-клиента) в качестве значения пароля.



К AD посылается следующий запрос:

```

6334 7169.97368 192.168.14.20 192.168.14.70 LDAP 179 searchRequest(51) "DC=olga,DC=oit,DC=cmc,DC=msu,DC=ru"
6335 7169.97407 192.168.14.70 192.168.14.20 LDAP 505 searchResEntry(51) "CN=I2tp

[Frame 6334: 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits) on interface 0]
[Ethernet II, Src: D-Link_49:dd:01 (5c:d9:98:49:dd:01), Dst: Compex_25:1e:59 (00:80:48:25:1e:59)]
[Internet Protocol Version 4, Src: 192.168.14.20 (192.168.14.20), Dst: 192.168.14.70 (192.168.14.70)]
[Transmission Control Protocol, Src Port: 16006 (16006), Dst Port: ldap (389), Seq: 5850, Ack: 215, Win: 0, Len: 179]
[Lightweight Directory Access Protocol]
  LDAPMessage searchRequest(51) "DC=olga,DC=oit,DC=cmc,DC=msu,DC=ru" wholeSubtree
    messageID: 51
    protocolOp: searchRequest (3)
    searchRequest
      baseObject: DC=olga,DC=oit,DC=cmc,DC=msu,DC=ru
      scope: wholeSubtree (2)
      derefAliases: derefAlways (3)
      sizeLimit: 1
      timeLimit: 60
      typesOnly: False
    Filter: (SAMAccountName=I2tp_users)
    filter: equalityMatch (3)
      equalityMatch
        attributeDesc: SAMAccountName
        assertionValue: I2tp_users
    attributes: 2 items
      AttributeDescription: Description
      AttributeDescription: I2tp
[Response In: 6335]

```

Ответ от AD следующий:

```

.14.20 192.168.14.70 LDAP 178 searchRequest(19) "DC=olga,DC=oit,DC=cmc,
.14.70 192.168.14.20 LDAP 504 searchResEntry(19) "CN=l2tp_user,CN=l2tp,
.14.20 192.168.14.70 TCP 60 15167 > ldap [ACK] Seq=2150 Ack=5897 win=
[Response 10: 2775]
[Time: 0.020327000 seconds]
Lightweight Directory Access Protocol
Lightweight Directory Access Protocol
Lightweight Directory Access Protocol
Lightweight Directory Access Protocol

```

Значение поля **description**, которое является паролем пользователя, передается в открытом виде. Следовательно, канал между межсетевым экраном и AD должен быть защищен.

Лабораторная работа 14. Аутентификация доступа к ресурсам с использованием браузера

Цель

Выполнить аутентификацию локальных пользователей при доступе к ресурсам, расположенным в DMZ. Для доступа к этим ресурсам используется браузер. Межсетевой экран выполняет аутентификацию, используя либо Basic-аутентификацию протокола HTTP, либо аутентификацию с помощью HTML-формы, которая задана в настройках самого межсетевого экрана.

Оба эти способа аутентификации не обеспечивают конфиденциальность, поэтому их следует использовать только тогда, когда политика безопасности допускает возможность пассивных атак, либо когда используется туннелирование на более низком уровне стека протоколов.

Можно отредактировать существующую HTML-форму или создать собственную.

Веб-интерфейс:

Object → HTTP Banner Files → Add

Name: userAuth

HTTP Banner Files
 HTTP banner files specifies the look and feel of HTTP authentication pages and HTTP ALG restrictions pages

Add ▾

# ▾	Name ▾	Type ▾	Comments ▾
1	Default		Standard HTTP ALG HTML banner files.
2	Default		Standard User Authentication HTML banner files.
3	userAuth		

Right-click on a row for additional options.

userAuth
 HTTP banner files specifies the look and feel of HTML authentication web pages.

General Edit & Preview

General
 Customize your HTML authentication pages.

Edit
 Page: FormLogin ▾

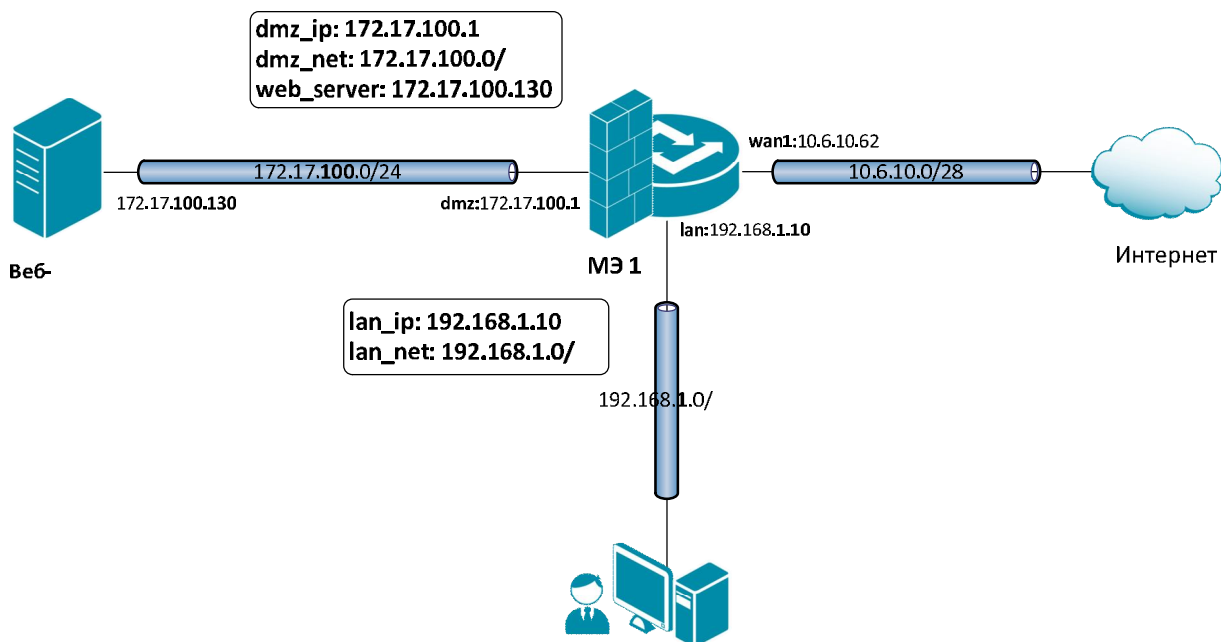
```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>Authentication required</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<style type="text/css">
body, table { font-family: verdana; font-size: 8pt; line-height: 11pt;}
.heading1 {font-family: verdana; font-size: 14pt; line-height: 16pt; font-weight: bold;}
.heading2 {font-family: verdana; font-size: 12pt; line-height: 20pt; font-weight: bold; text-align: left; color: red;}
.xstop, .xbottom {display: block; background: transparent; font-size: 1px;}
.xb1, .xb2, .xb3, .xb4 {display: block; overflow: hidden;}
.xb1, .xb2, .xb3 {height: 1px;}
.xb2, .xb3, .xb4 {background: #ffff; border-left: 1px solid #D8E0EB; border-right: 1px solid #D8E0EB;}
.xb1 {margin: 0 5px; background: #D8E0EB;}
.xb2 {margin: 0 3px; border-width: 0 2px;}
.xb3 {margin: 0 2px;}

```

Командная строка:

1. Переписать файл **FormLogin** из каталога **HTTPAuthBanners/userAuth/**.
pscp.exe admin@<IP-адрес>:HTTPAuthBanners/userAuth/FormLogin FormLogin
2. Отредактировать его редактором.
3. Переписать отредактированный файл в тот же каталог.

Топология сети



Описание практической работы

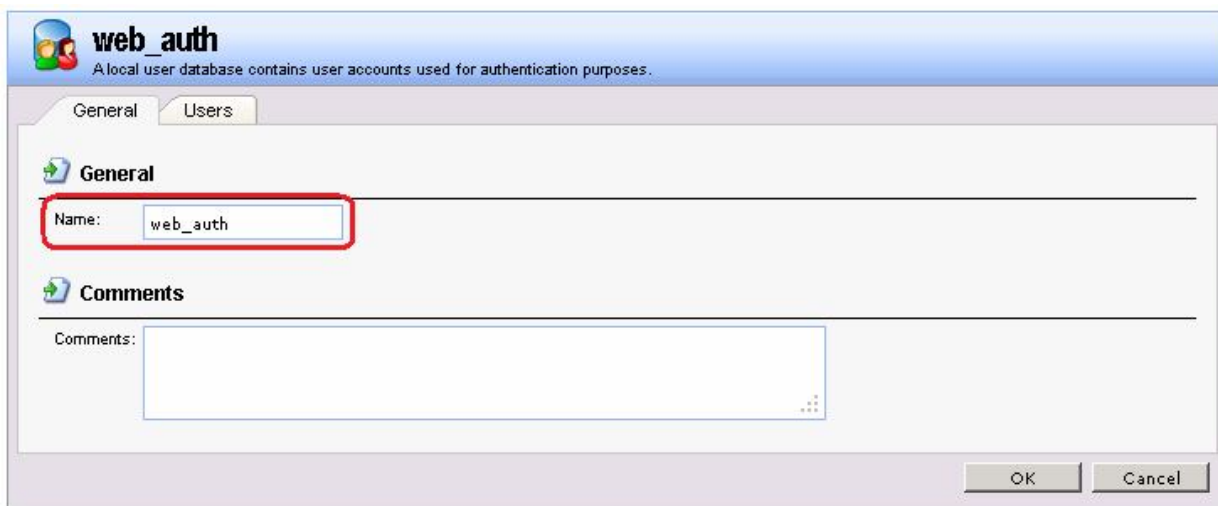
Правила аутентификации пользователей

1. Создание локальной базы данных пользователей.

Веб-интерфейс:

User Authentication → Local User Databases → Add

Name: web_auth



User Authentication → Local User Databases → web_auth

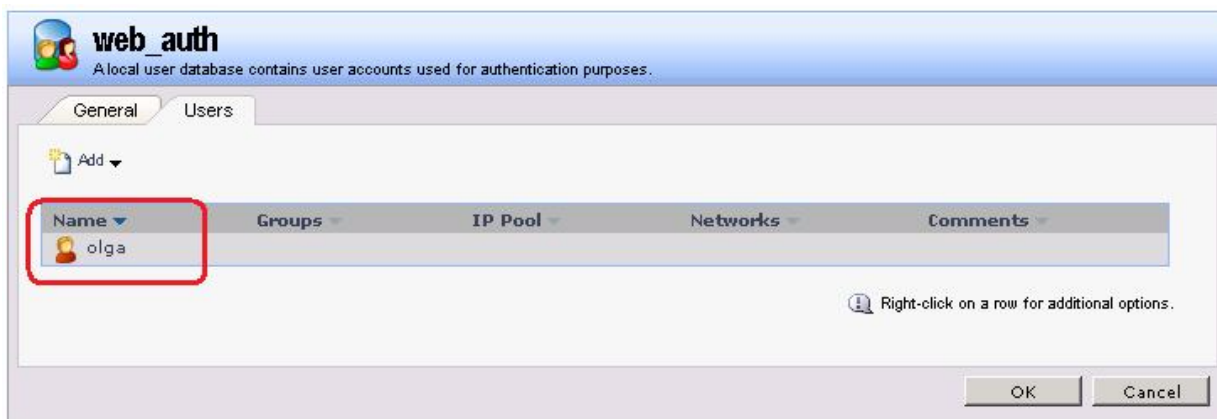
Вкладка Users → Add

Командная строка:

```
add LocalUserDatabase web_auth
```

```
cc LocalUserDatabase web_auth
```

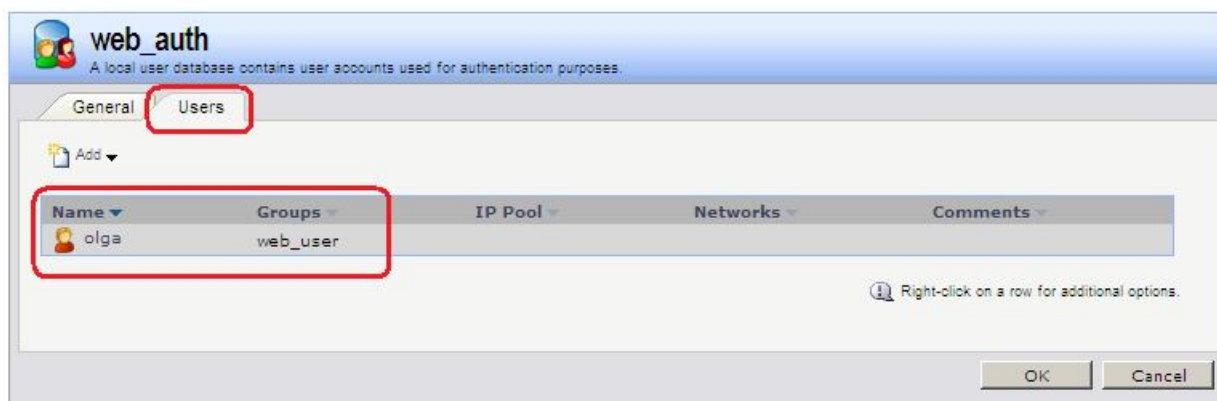
При использовании идентификатора пользователя:



Командная строка:

```
add User olga Password=qwerty
```

При использовании в правилах аутентификации идентификатора группы вместо идентификатора пользователя следует указать группу, в которую входит данный пользователь:



Командная строка:

```
add User olga Password=qwerty Groups=web_user
```

2. Создание правила аутентификации пользователей.

Веб-интерфейс:

User Authentication → User Authentication Rules → Add

Name: web_auth

web_auth
The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

General | Log Settings | Authentication Options | Accounting | Agent Options | Restrictions

General

Name: web_auth

Authentication agent: HTTP

Authentication Source: Local

Interface: lan

Originator IP: lan_net

Terminator IP: (None)

For XAuth and PPP, this is the tunnel originator IP.

Comments:

OK Cancel

web_auth
The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

General | Log Settings | Authentication Options | Accounting | Agent Options | Restrictions

General

Select one or more authentication servers. Also select the authentication method, which is used for encrypting the user password.

RADIUS servers

Available Selected

LDAP servers

Available Selected

RADIUS Method: Unencrypted password (PAP)

Local User DB: web_auth

web_auth
The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

General | Log Settings | Authentication Options | Accounting | **Agent Options** | Restrictions

PPP Agent Options

- Allow no authentication.
- Use PAP authentication protocol. User name and password are sent in plaintext.
- Use CHAP authentication protocol.
- Use MS-CHAP authentication protocol.
- Use MS-CHAP v2 authentication protocol.

HTTP(s) Agent Options

Login Type: ▼

HTTP Banners: ▼

Realm String:

MAC Authentication

- Allow Clients behind router to connect
- MAC Auth Secret: Password used to authenticate MAC user, if empty the MAC address will be sent as password.
- Confirm Secret: Note! Existing secret will always be shown with 8 characters to hide the actual length.

Командная строка:

```
add UserAuthRule Interface=lan AuthSource=Local LocalUserDB=web_auth
OriginatorIP=lan/lan_net LoginType=HTMLForm HTTPBanners=userAuth
Name=web_auth Agent=HTTP
```

3. Создание объекта в Адресной Книге с адресами локальной сети и требованием аутентификации пользователей.

Веб-интерфейс:

Object → Address Book → web_auth → Add

Name: lan_auth

lan_auth
Use an IP4 Address item to define a name for a specific IP4 host, network or range.

General | **User Authentication**

General

Name:

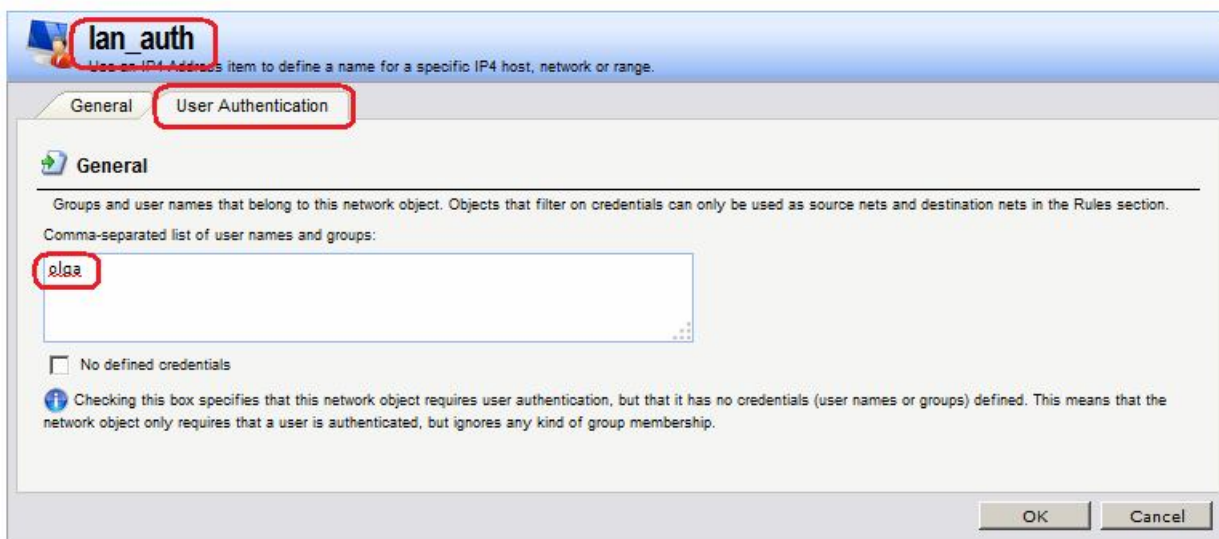
Address: IP address, e.g. "172.16.50.8", "192.168.7.0/24" or "172.16.25.10-172.16.25.50".

Comments

Comments:

OK Cancel

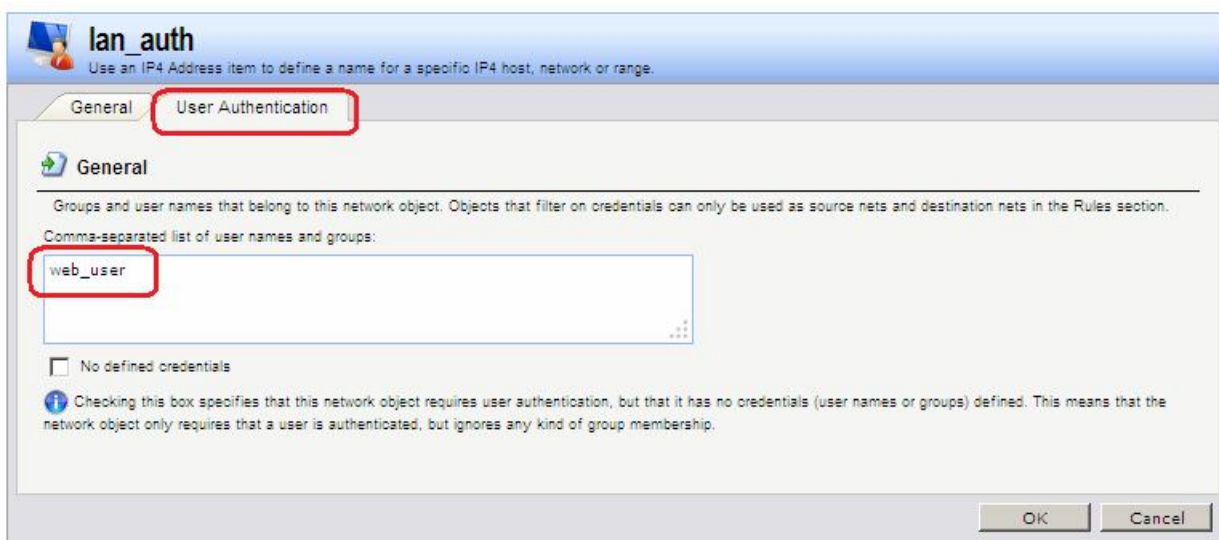
На вкладке **User Authentication** указать идентификатор пользователя:



Командная строка:

```
cc Address AddressFolder web_auth
add IP4Address lan_auth Address=192.168.1.0/24 UserAuthGroups=olga
```

Использование идентификатора группы:



Командная строка:

```
cc Address AddressFolder local_lan
add IP4Address lan_auth Address=192.168.12.0/24 UserAuthGroups=web_user
```

Правила фильтрации

- a) Правило, разрешающее доступ к веб-серверу аутентифицированным пользователям.

Веб-интерфейс:

Rules → IP Rules → web_auth → Add

Name: http_auth

Rules → IP Rules → web_auth → http_auth

The screenshot shows the configuration window for an IP rule named 'http_auth'. The 'General' tab is active. The 'Name' field is 'http_auth'. The 'Action' is set to 'Allow'. The 'Service' is set to 'http'. The 'Schedule' is '(None)'. In the 'Address Filter' section, the 'Source' interface is 'lan' and the 'Destination' is 'dmz'. The 'Network' dropdowns are set to 'lan_auth' for the source and 'web_server' for the destination. A note indicates that NAT, SAT, SLB SAT, and Multiplex SAT are not usable with an IPv6 rule. The 'Comments' field is empty. 'OK' and 'Cancel' buttons are at the bottom right.

Командная строка:

```
cc IPRuleFolder <N Folder>
```

```
add IPRule Action=Allow SourceInterface=lan SourceNetwork=lan/lan_auth
DestinationInterface=dmz DestinationNetwork=dmz/web_server Service=http
Name=http_auth
```

- b) Правило, перенаправляющее неаутентифицированных пользователей на межсетевой экран для прохождения аутентификации.

Веб-интерфейс:

```
Rules → IP Rules → web_auth → Add
```

```
Name: http_sat
```

```
Rules → IP Rules → web_auth → http_sat
```

http_sat
An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General | Log Settings | NAT | SAT | Multiplex SAT | SLB SAT | SLB Monitors

General

Name: http_sat

Action: SAT NAT, SAT, SLB SAT and Multiplex SAT is not usable with an IPv6 rule

Service: http

Schedule: (None)

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

Source: Interface: lan Network: lan_net

Destination: dmz web_server

Comments:

OK Cancel

http_sat
An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General | Log Settings | NAT | SAT | Multiplex SAT | SLB SAT | SLB Monitors

General

Translate the

Source IP

Destination IP

to:

New IP Address: lan_ip

New Port: This value may only be applied on TCP/UDP services with port set to either a single port number or a port range without gaps

All-to-One Mapping: rewrite all destination IPs to a single IP

OK Cancel

Командная строка:

```
cc IPRuleFolder <N Folder>
```

```
add IPRule Action=SAT SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=dmz DestinationNetwork=dmz/web_server Service=http
SATTranslateToIP=lan/lan_ip SATAllToOne=Yes Name=http_sat
```

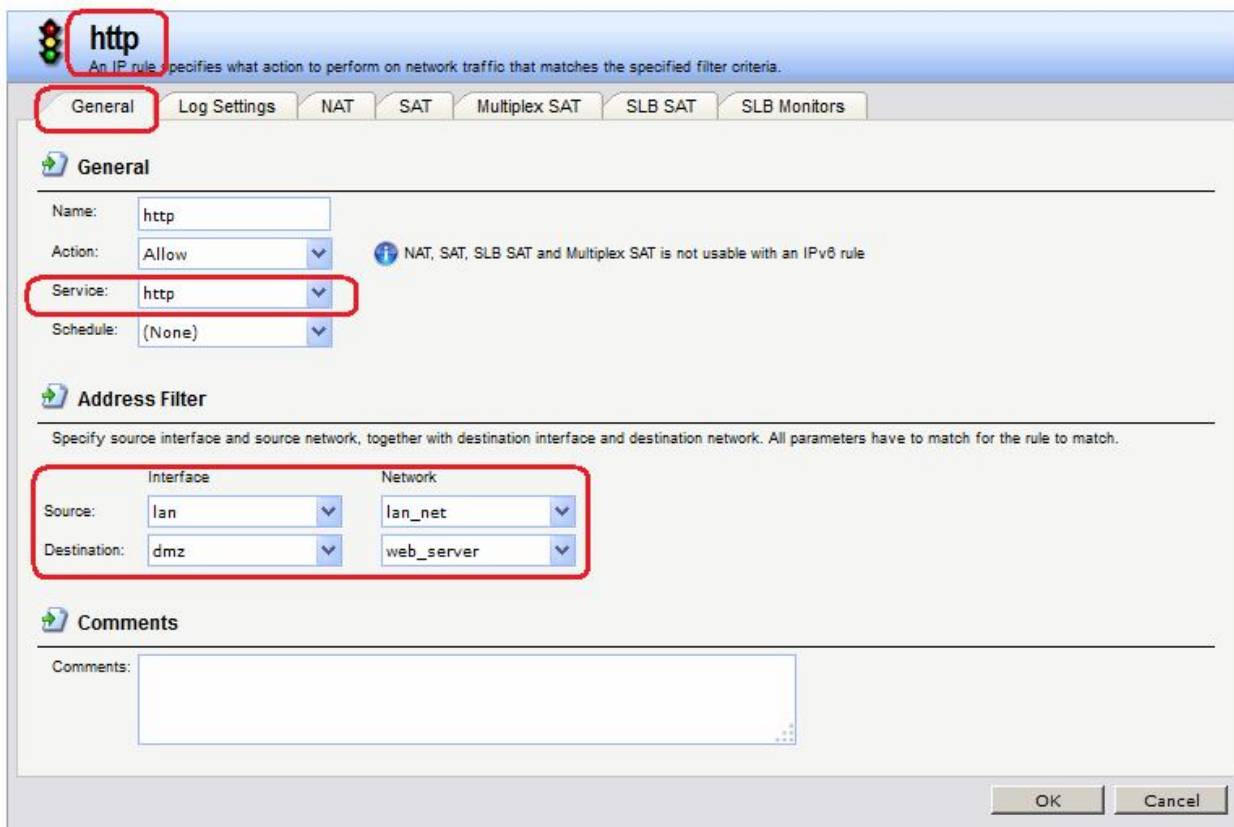
- с) Правило, разрешающее трафик для выполнения аутентификации пользователей.

Веб-интерфейс:

Rules → IP Rules → local_nets → Add

Name: http_auth

Rules → IP Rules → local_nets → http_auth



Командная строка:

```
cc IPRuleFolder <N Folder>
```

```
add IPRule Action=Allow SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=dmz DestinationNetwork=dmz/web_server Service=http
Name=http
```

- d) Правило, разрешающее трафик к интерфейсу **core** для доступа к форме аутентификации пользователей.

Веб-интерфейс:

```
Rules → IP Rules → local_nets → Add
```

```
Name: http_core
```

```
Rules → IP Rules → local_nets → http_core
```


Командная строка:

```
cc IPRuleFolder <N Folder>
```


```
add IPRule Action=Allow SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=core DestinationNetwork=dmz/web_server Service=http
Name=http_core
```


Проверка конфигурации

Используем браузер, в качестве адреса указываем IP-адрес веб-сервера, после чего попадаем на созданную html-страницу.



Проверяем статус аутентифицированных пользователей.

 **User Authentication Status**
Listing of all authenticated users

 **User Authentication Status**

Username	IP Address	Interface	Session Timeout	Idle Timeout	Loaded in as	Forcibly Log Out
olga	192.168.1.30	lan		19m	olga	