Лабораторные работы по курсу «Основы сетевой безопасности»

Часть 2: Технологии туннелирования

Расширенный курс D-Link

Москва,2014

Оглавление

Лабораторный практикум

Технологии туннелирования

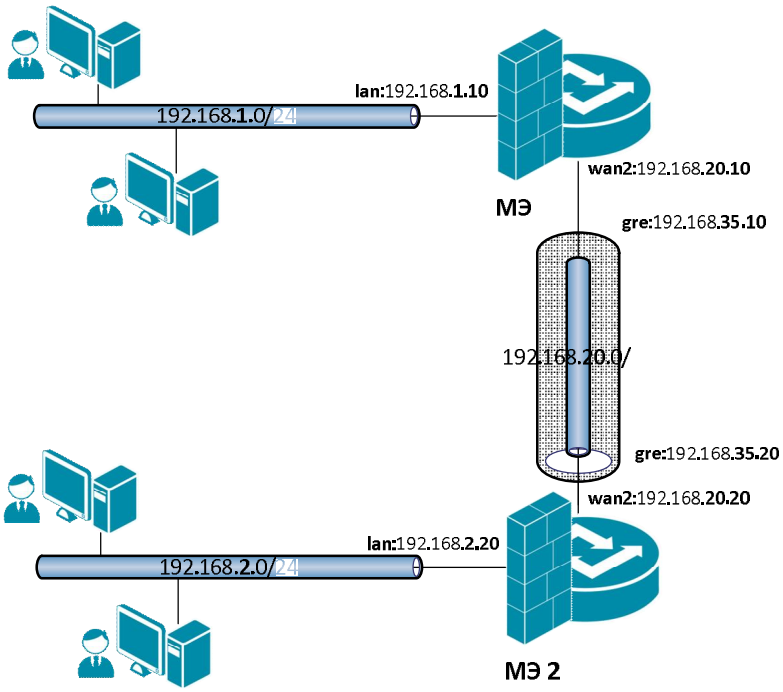
Лабораторная работа 1. Соединение двух локальных сетей GRE-туннелем

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



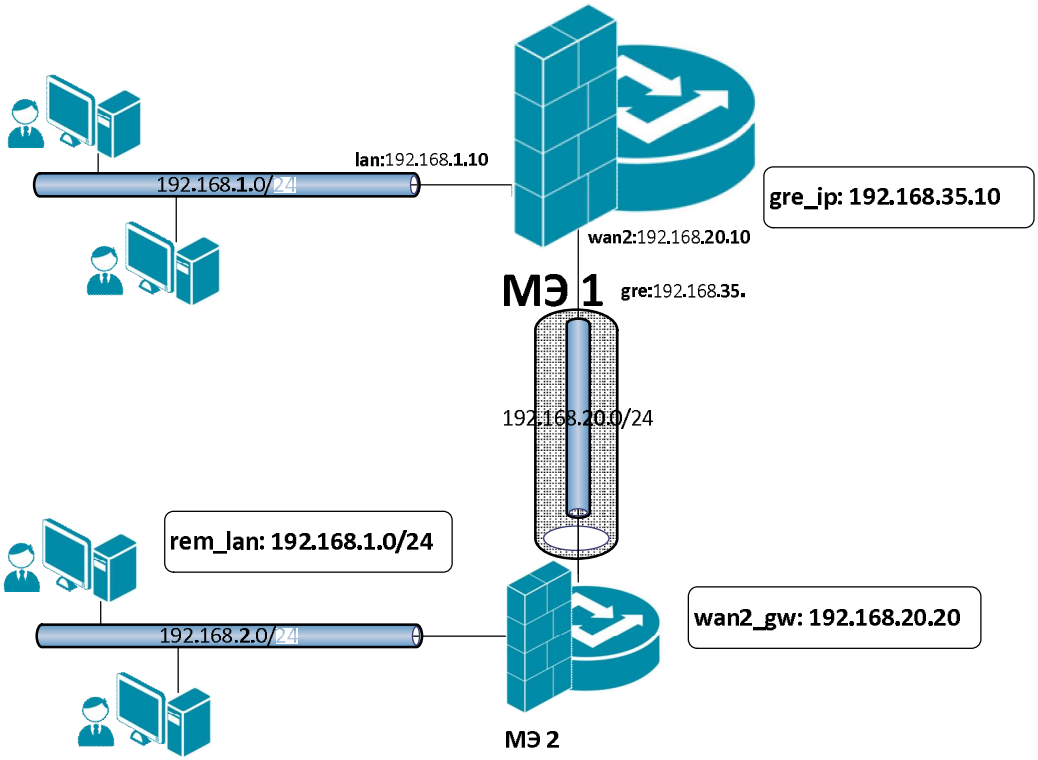
Между интерфейсами **`wan2`** на МЭ 1и МЭ 2 требуется поднять GRE-туннель.

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

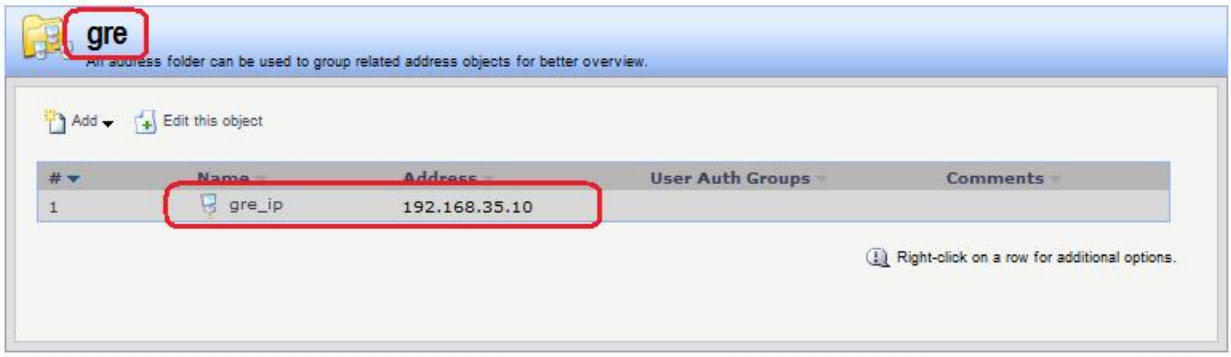
Создать объект, описывающий IP-адрес локальной стороны GRE-туннеля.

Веб-интерфейс:

`Object → Address Book → Add → Address Folder`

`Name: gre`

`Object → Address Book → gre → Add`



Командная строка:

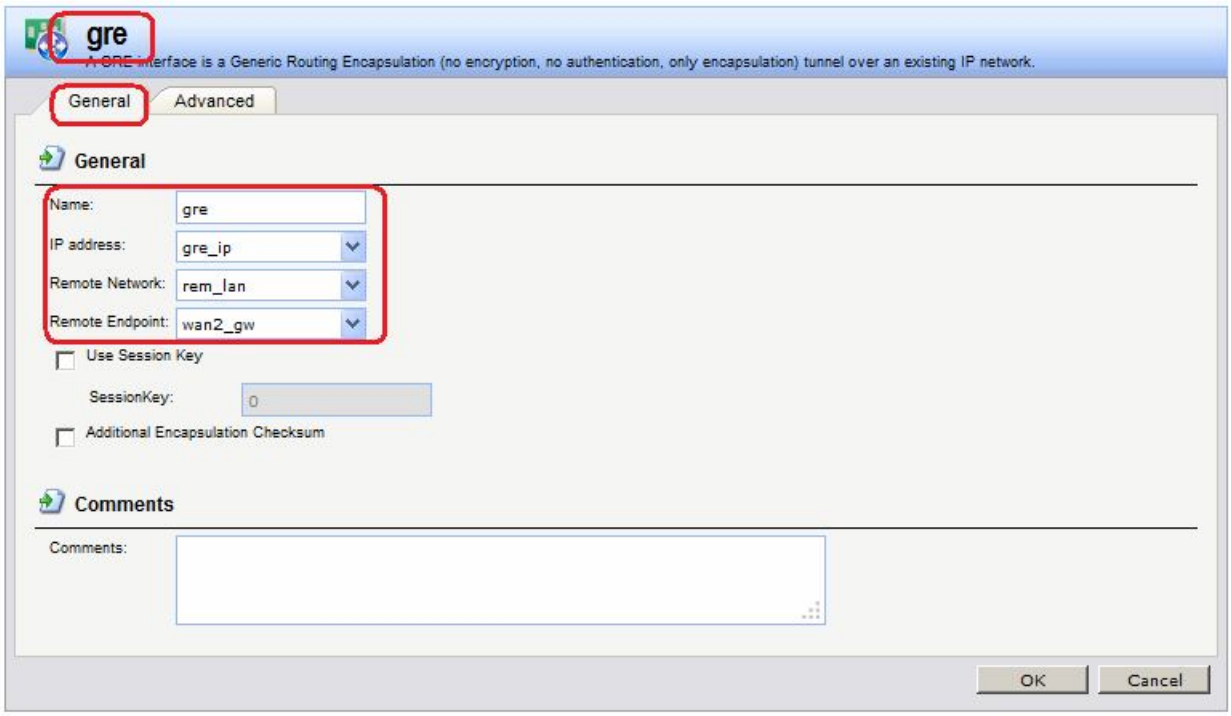
```
add Address AddressFolder gre
cc Address AddressFolder gre
add IP4Address gre_ip Address=192.168.35.10
```

GRE-Интерфейс

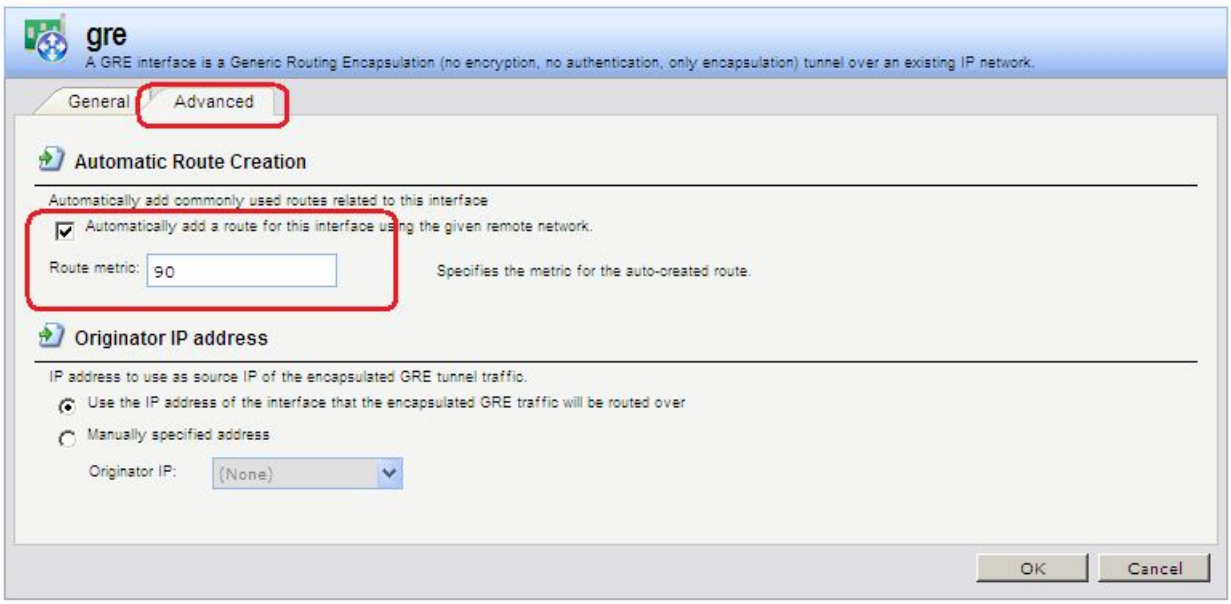
Веб-интерфейс:

`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.



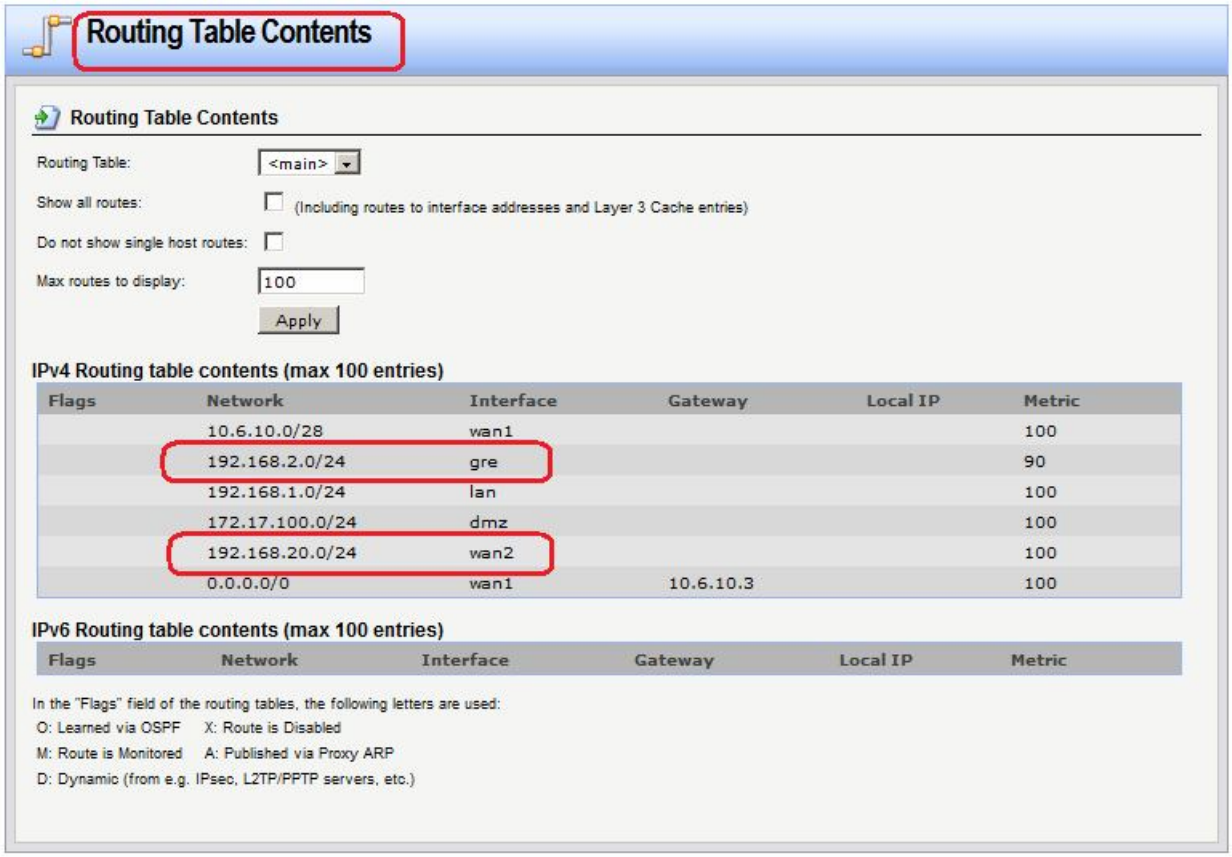
Возможность редактировать параметры автоматически созданного маршрута отсутствует. Если необходимо отредактировать какие-либо параметры маршрута, то на вкладке **Advanced** интерфейса следует снять флаг автоматического добавления маршрута и добавить маршрут вручную с необходимыми параметрами.

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.



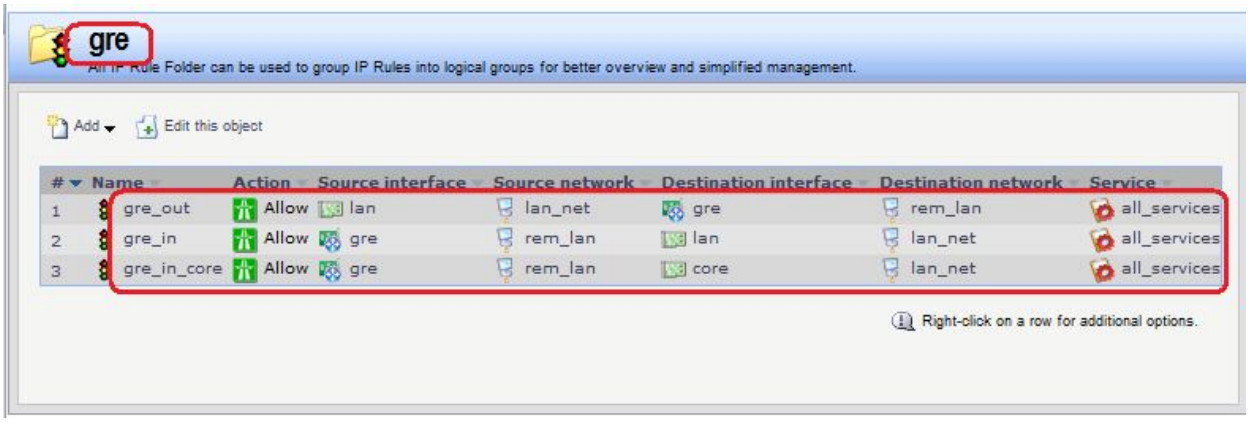
Правила фильтрования

Веб-интерфейс:

`Rules → IP Rules → Add → IP Rule Folder`

`Name: gre`

`Rules → IP Rules → gre → Add`



Командная строка:

```
add IPRuleFolder Name=gre
```

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

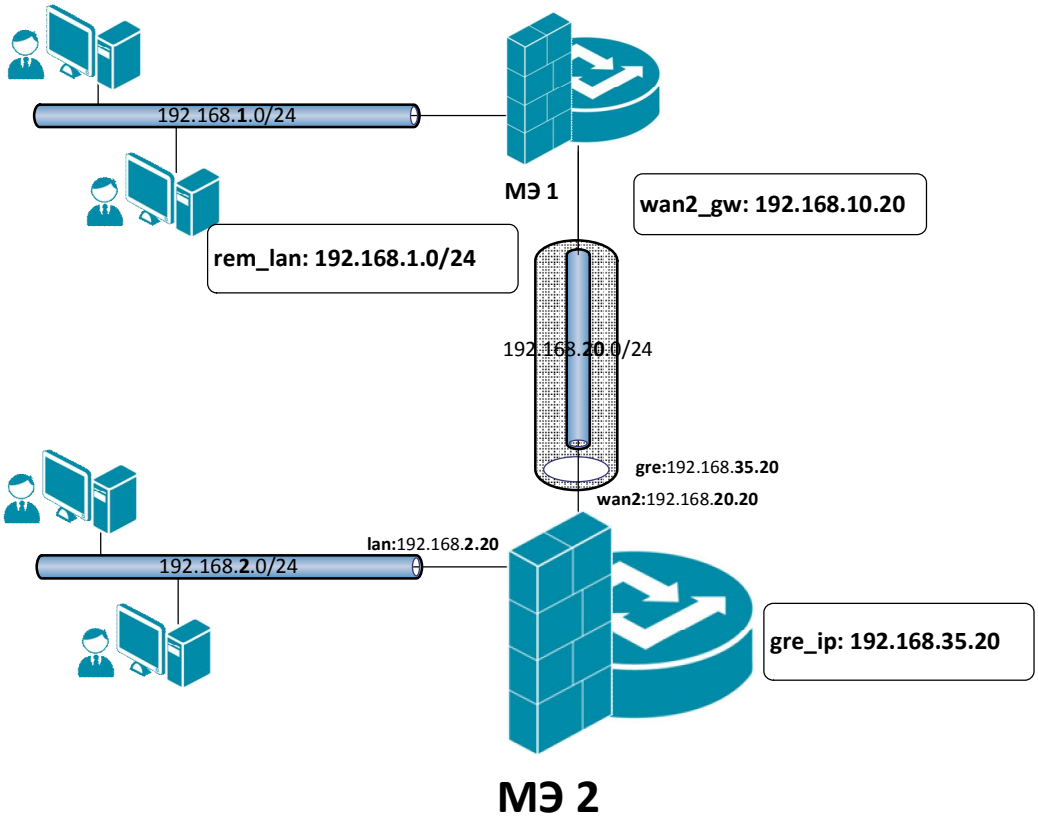
```
add IPRule Action=Allow SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=gre DestinationNetwork=remote/rem_lan Service=
all_services Name=gre_out
```

```
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.

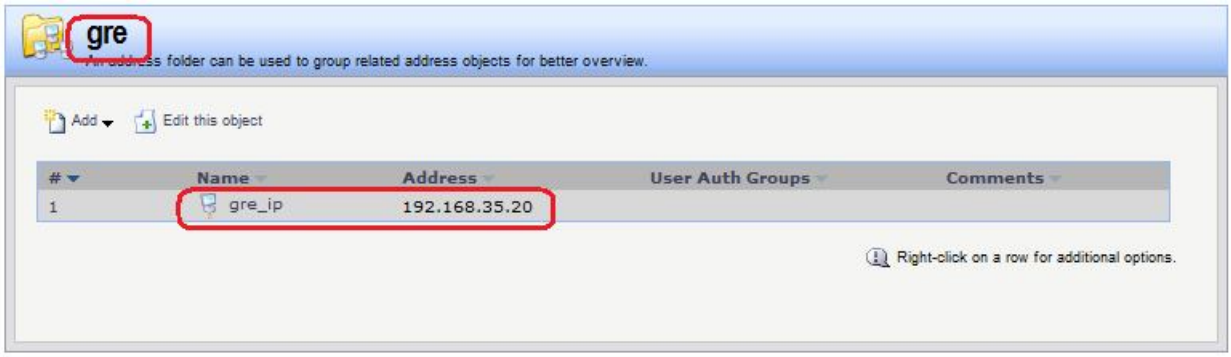
Межсетевой Экран 2



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
```

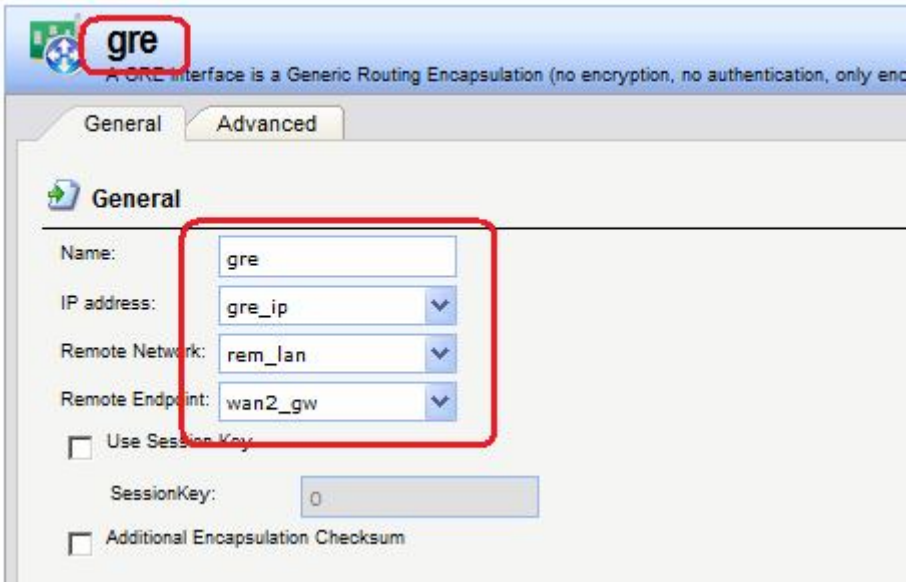
```
add IP4Address gre_ip Address=192.168.35.20
```

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.

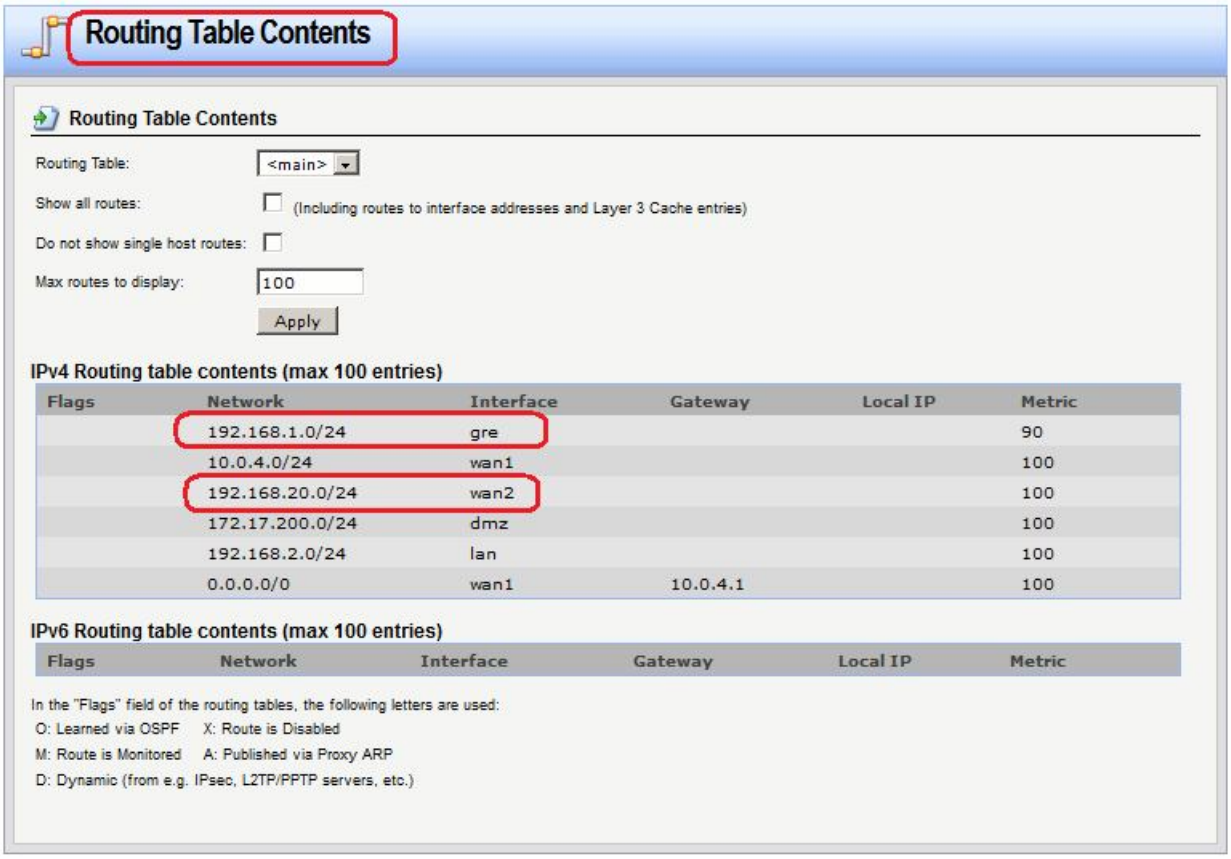


Командная строка:

```
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.



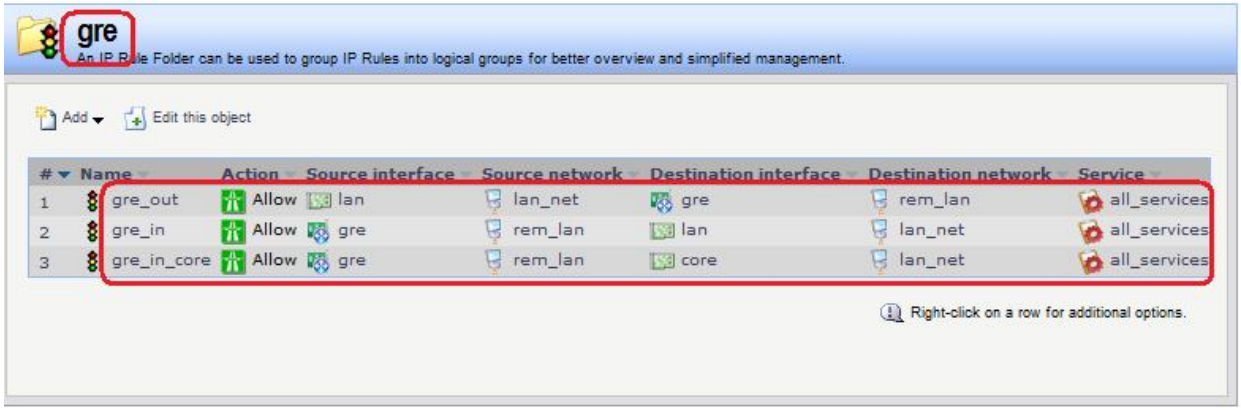
Правила фильтрования

Веб-интерфейс:

`Rules → IP Rules → Add → IP Rule Folder`

`Name: gre`

`Rules → IP Rules → gre → Add`



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_lann
Service=all_services Name=gre_out
```

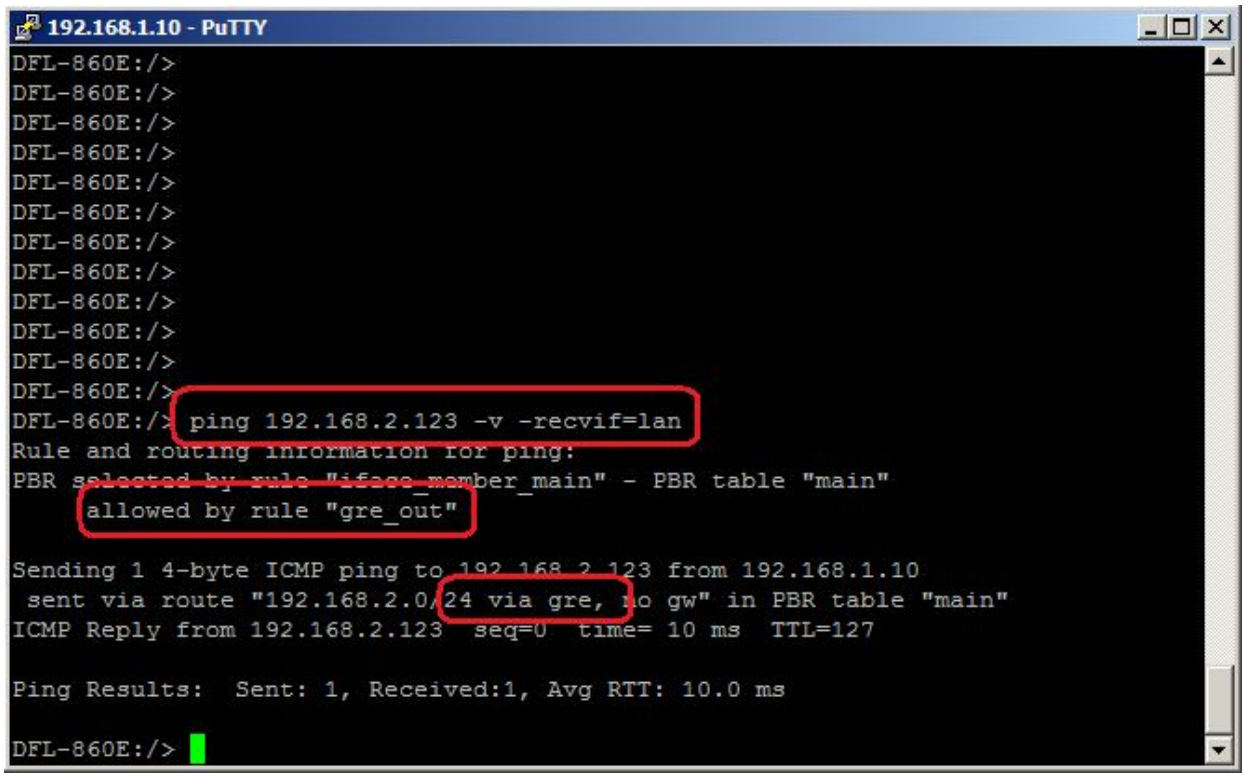
```
add IPRule Action=Allow SourceInterface=gre SourceNetwork=remote/rem_lan
DestinationInterface=gre DestinationNetwork=lan/lan_net Service=all_services
Name=gre_in
```

```
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.

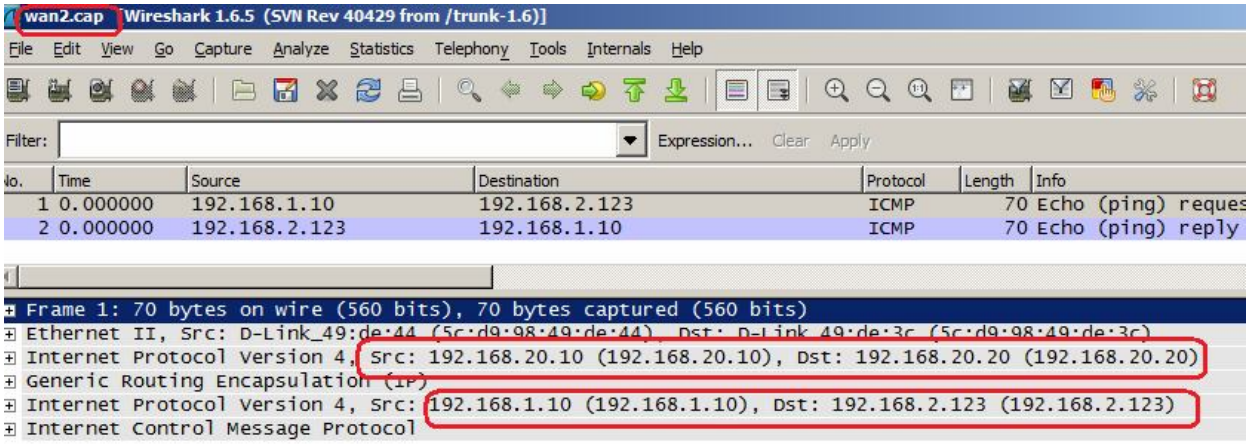
Анализ трафика

На Межсетевом Экране 1 выполним команду **ping** хоста в удаленной локальной сети:

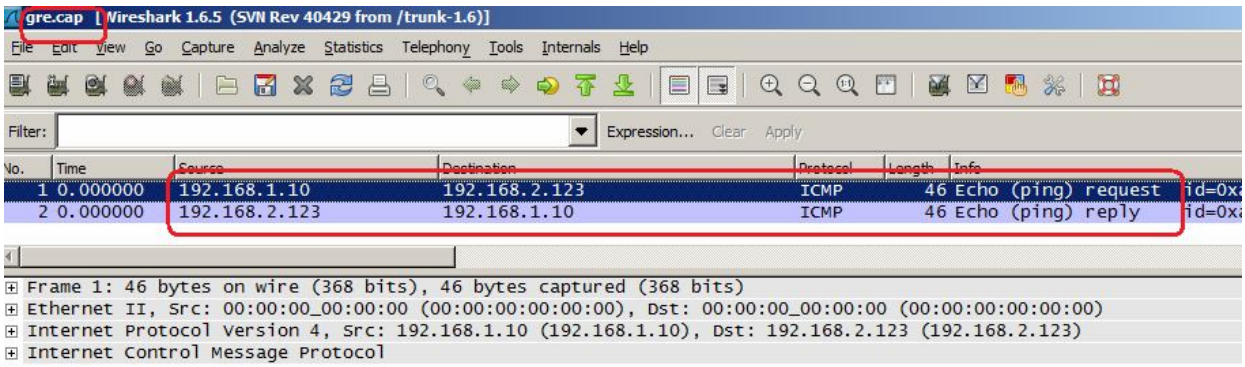


Смотрим трафик на интерфейсах **wan2**, **gre** и **lan** Межсетевого Экрана 2.

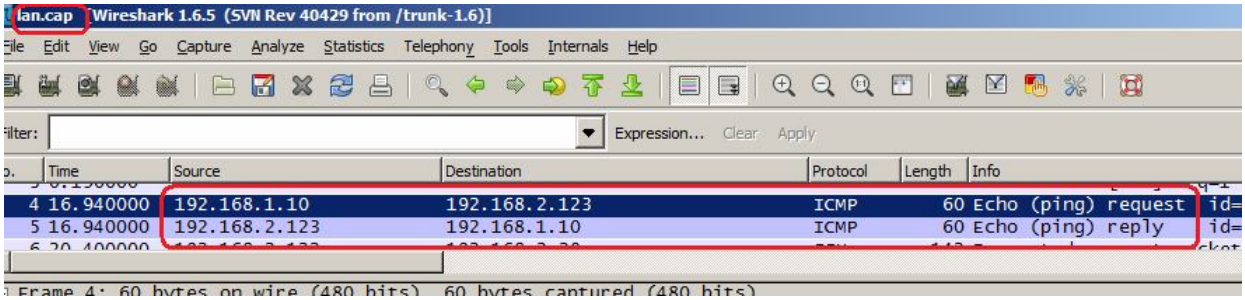
На интерфейсе **wan2** внешними IP-адресами является IP-адреса интерфейсов **wan2** межсетевых экранов.



На интерфейсе **gre** видим только ICMP-трафик с адресами из локальных сетей.



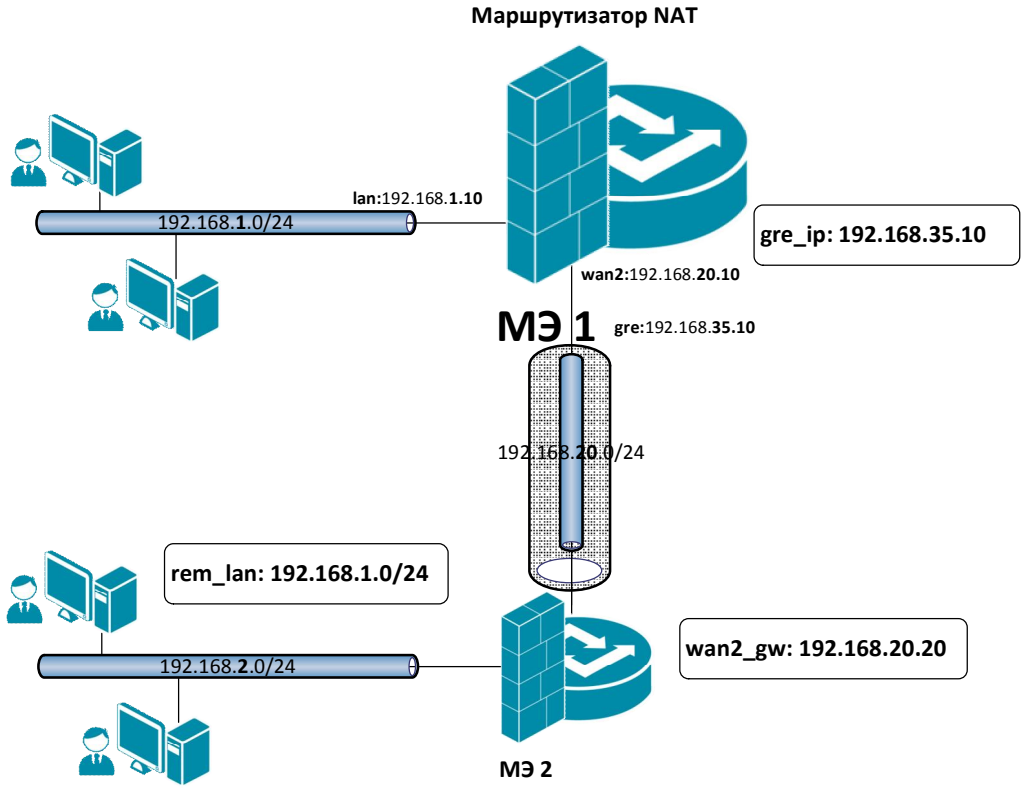
На интерфейсе **`lan`** видим также только ICMP-трафик с адресами из локальных сетей.



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



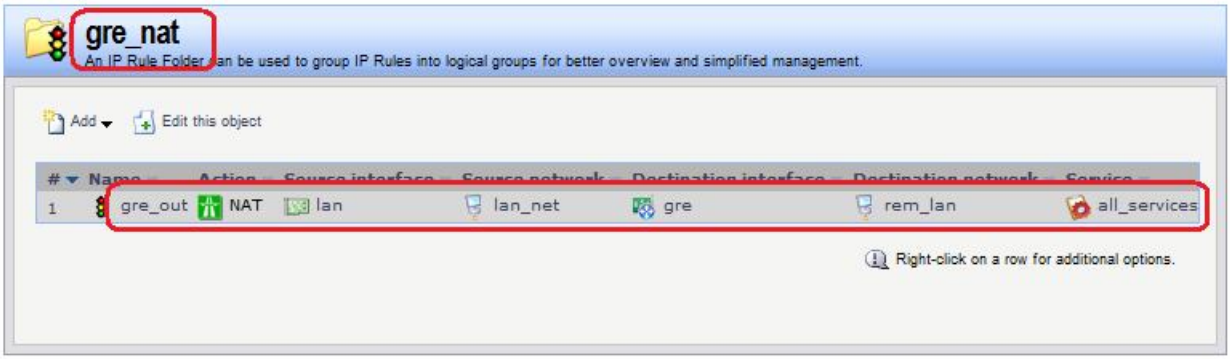
Правила фильтрования

Веб-интерфейс:

`Rules → IP Rules → Add → IP Rule Folder`

Name: gre_nat

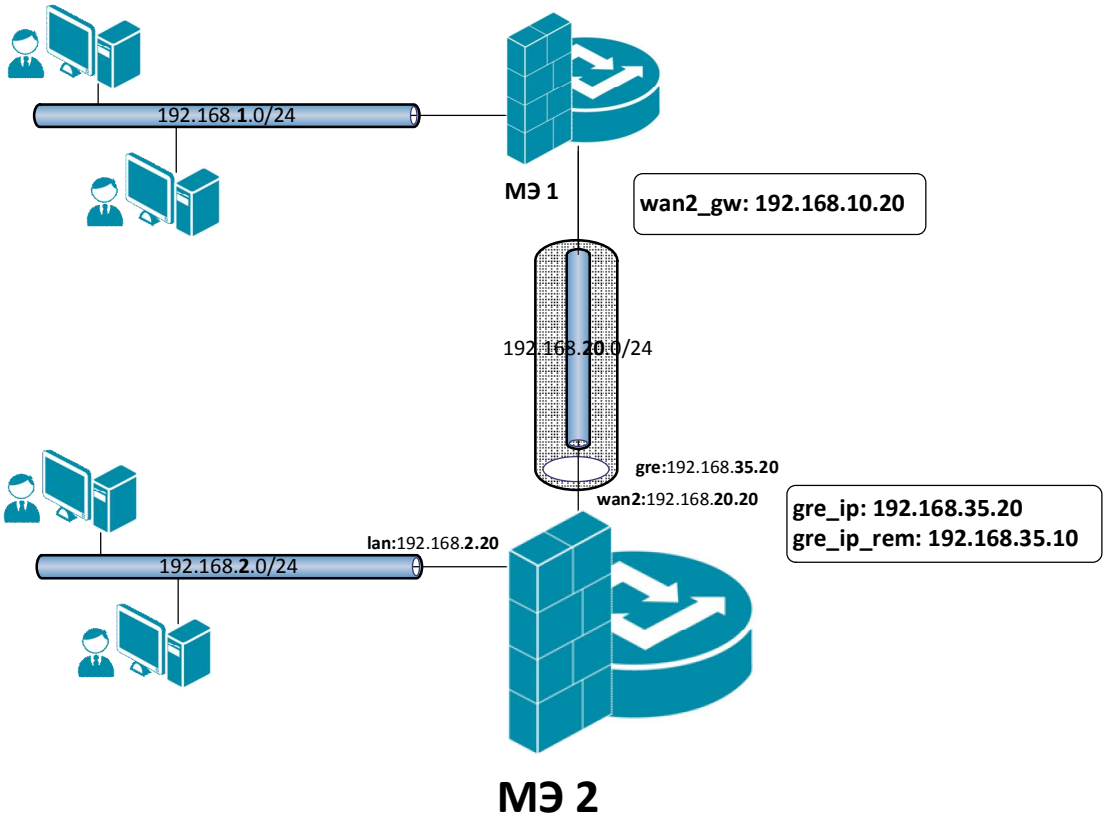
Rules → IP Rules → gre_nat → Add



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_lann
Service=all_services Name=gre_out
```

Межсетевой Экран 2



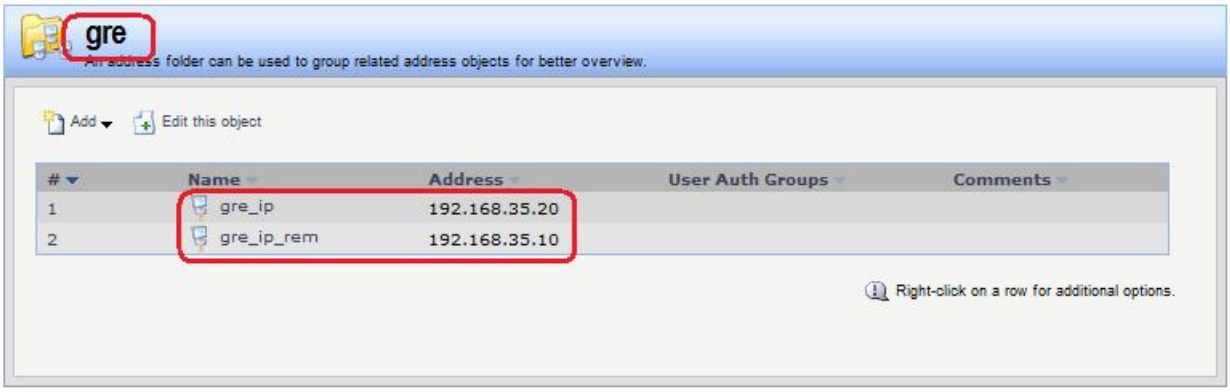
Объекты Адресной Книги

Веб-интерфейс:

Object → Address Book → Add → Address Folder

Name: gre

Object → Address Book → gre → Add



Командная строка:

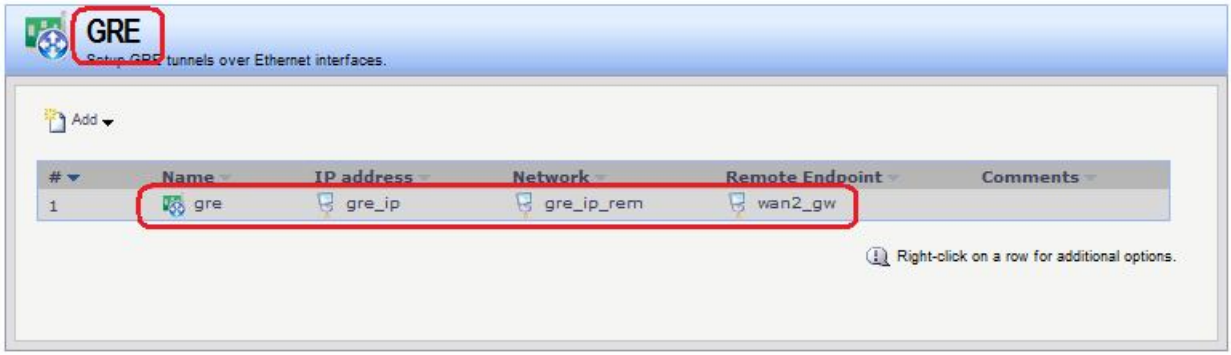
```
add Address AddressFolder gre
cc Address AddressFolder gre
add IP4Address gre_ip Address=192.168.35.20
add IP4Address gre_ip_rem Address=192.168.35.10
```

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.

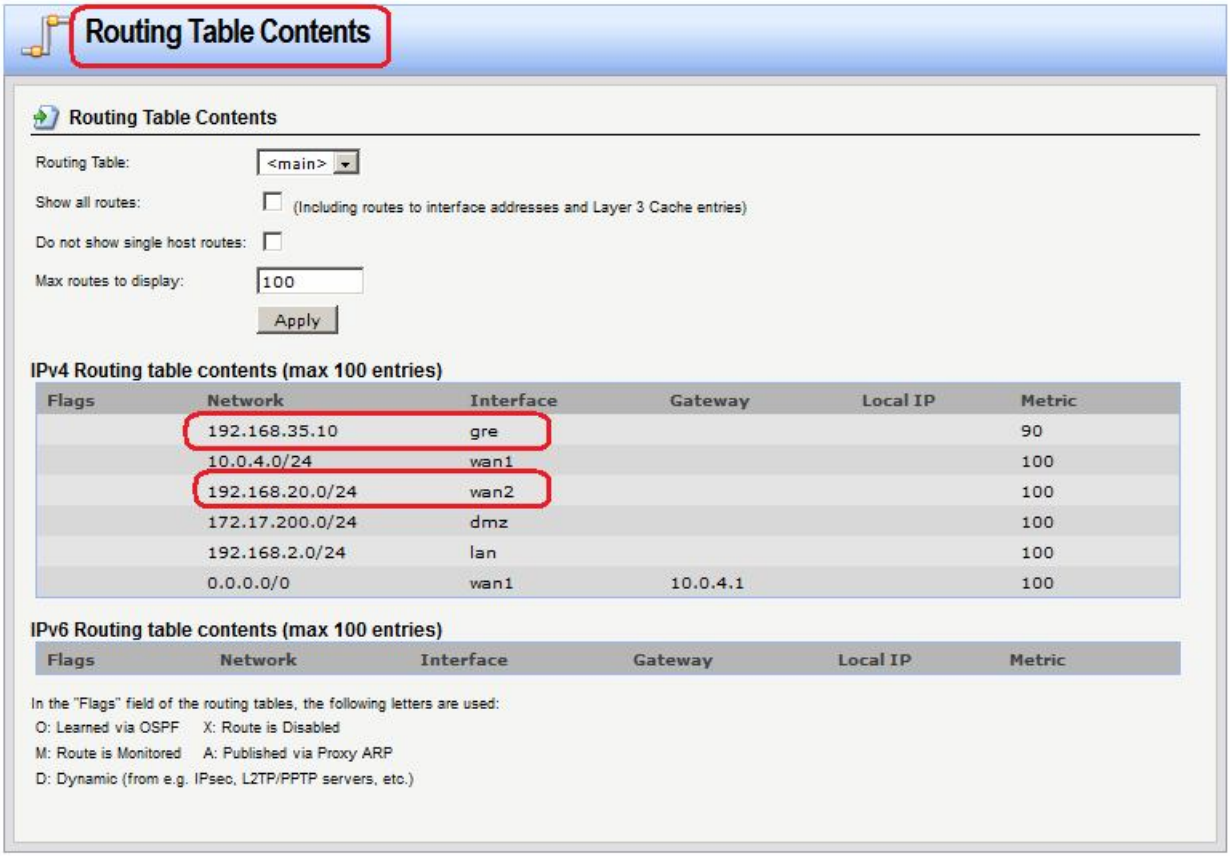


Командная строка:

```
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.



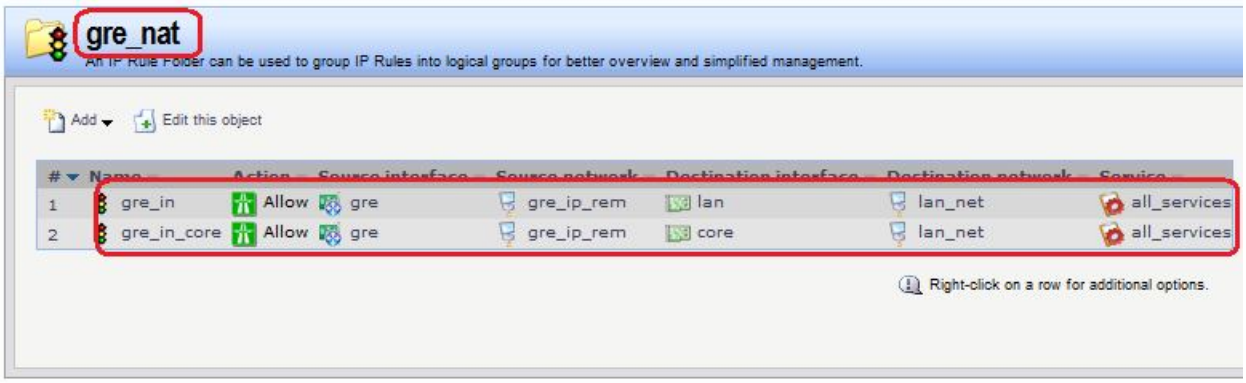
Правила фильтрования

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=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`

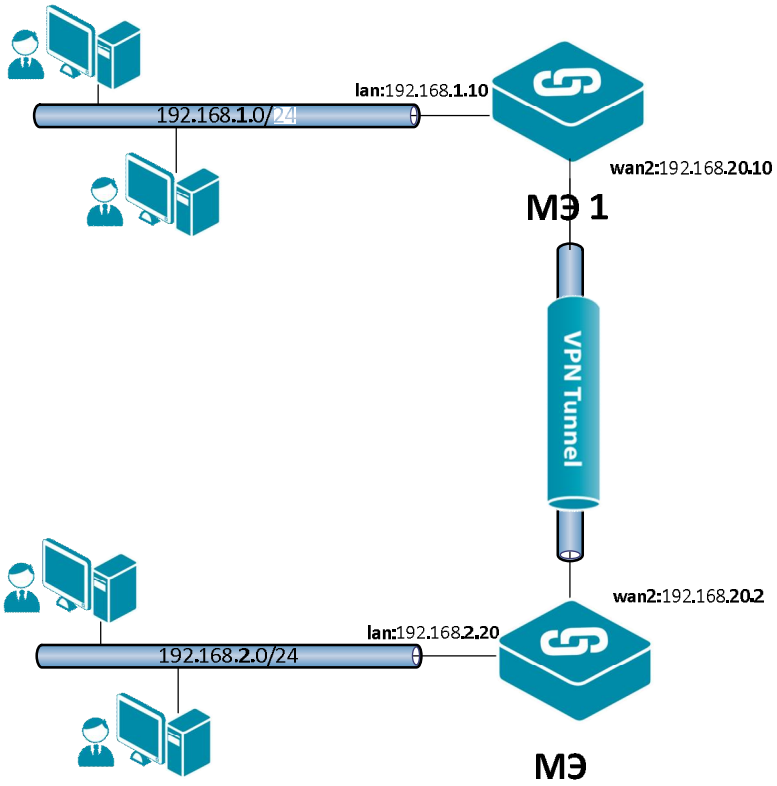
Последнее правило разрешает доступ к lan-интерфейсу самого межсетевого экрана.

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 1и МЭ 2 требуется поднять VPN/IPSec.

Описание практической работы

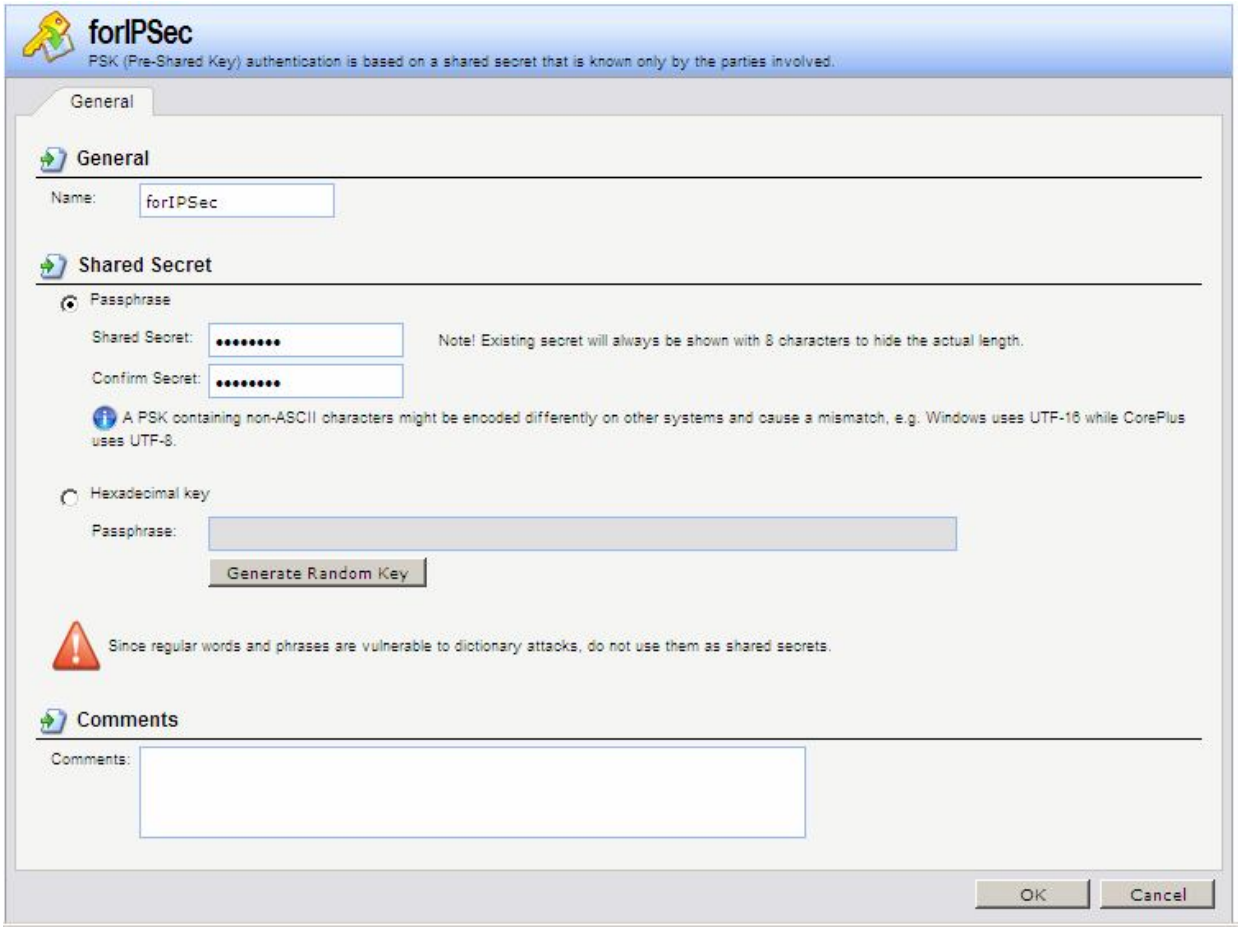
Создать статическую маршрутизацию и политики доступа, которые разрешают доступ между удаленными локальными сетями. При этом трафик между МЭ 1 и МЭ 2 проходит по VPN/IPSec.

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
```

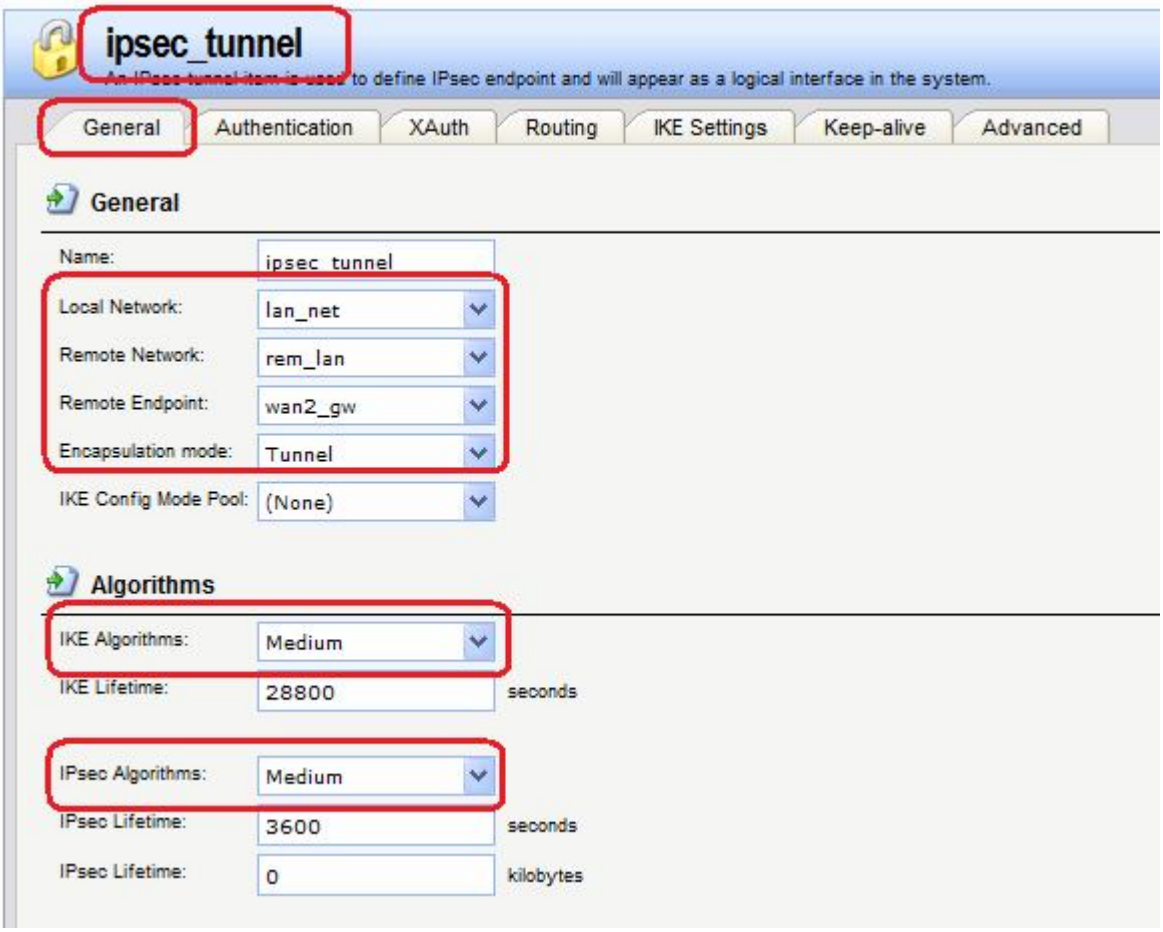
IPSec-Интерфейс

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

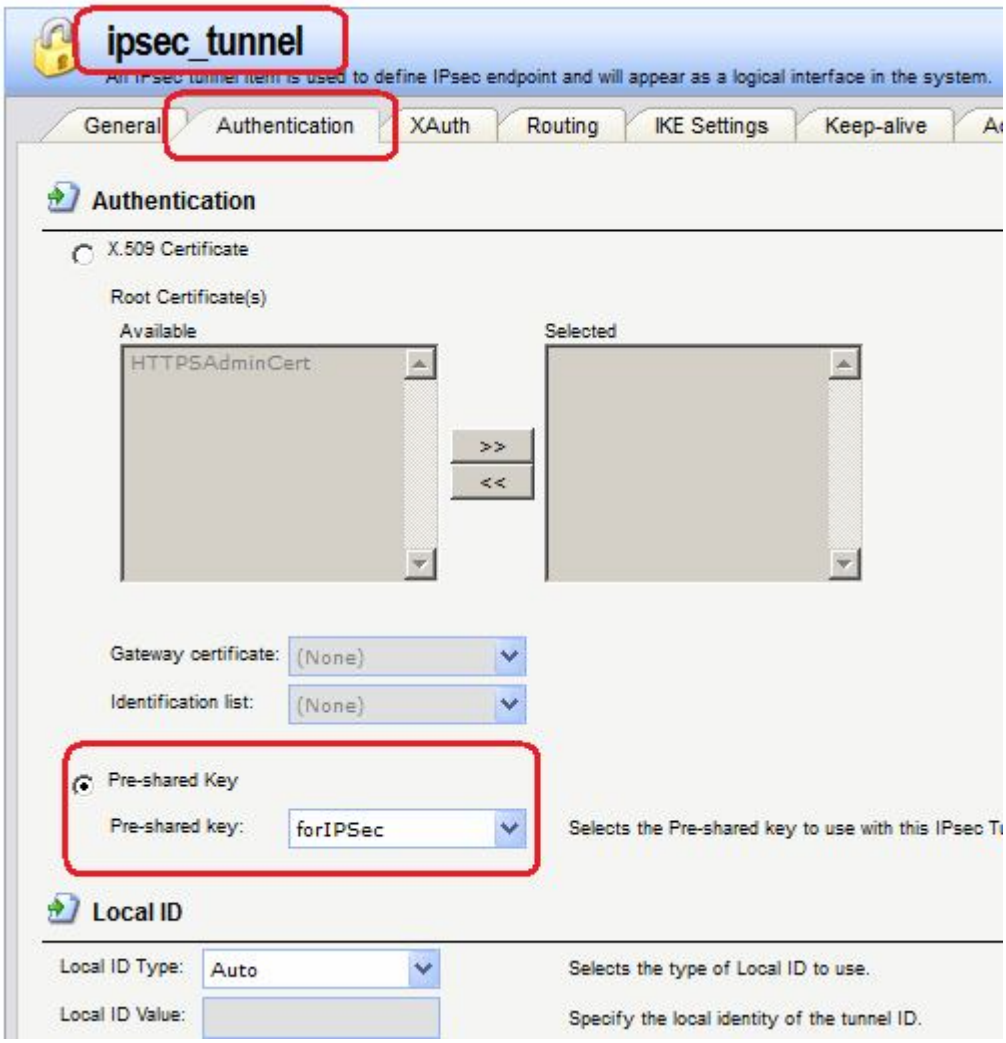
Веб-интерфейс:

`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.



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

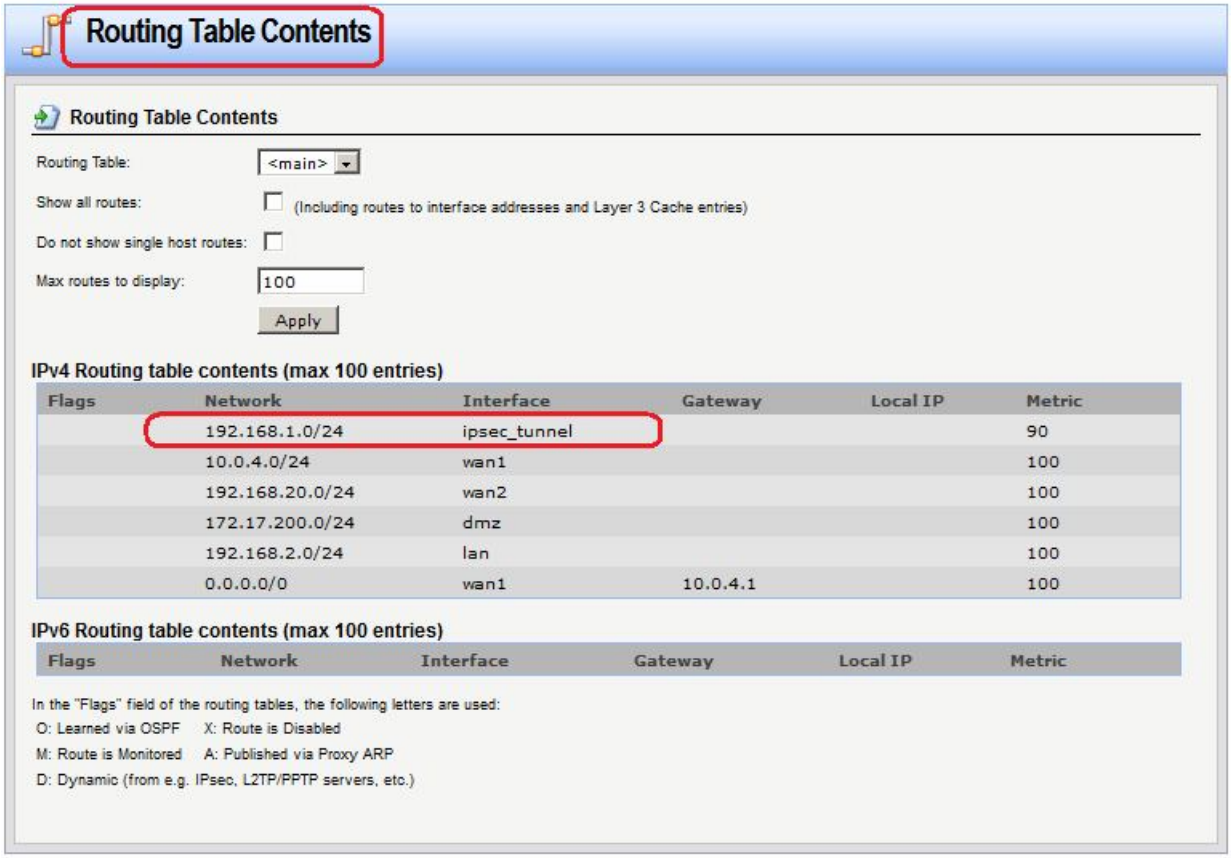


В данном случае, как и в большинстве случаев при создании туннелей с использованием различных протоколов, маршрут может создаваться либо статически, либо динамически на время создания туннеля.

1. Статически создаваемый маршрут.

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

Веб-интерфейс:



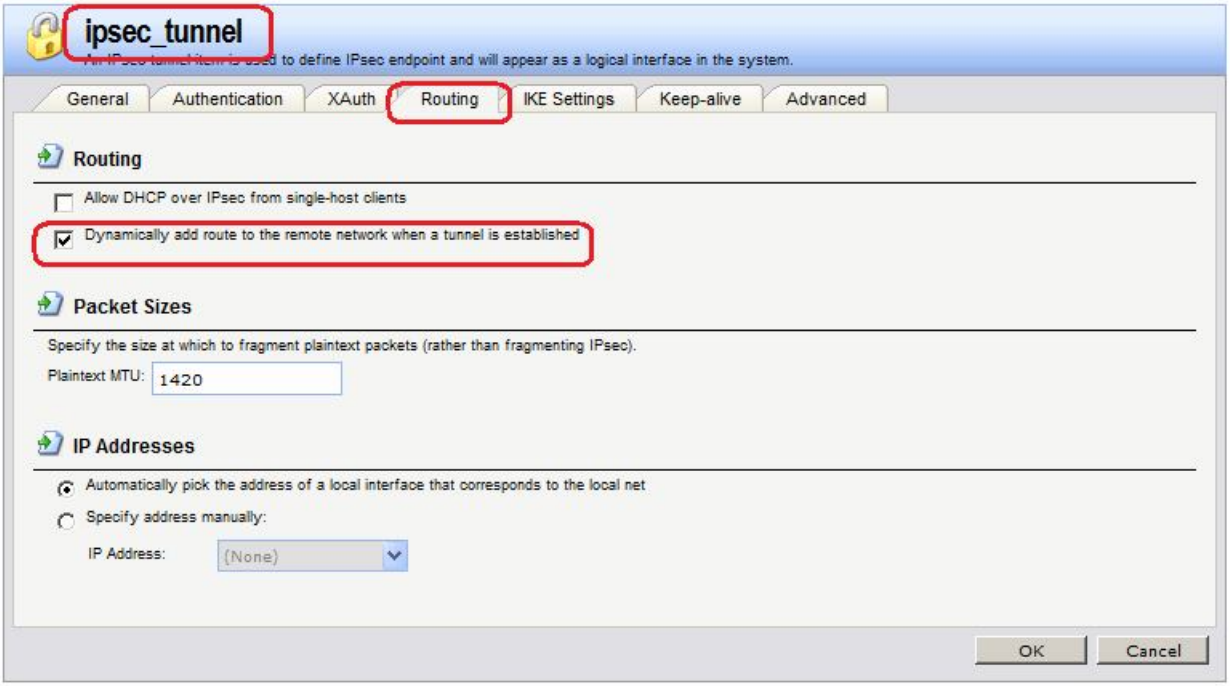
Командная строка:

```
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
```

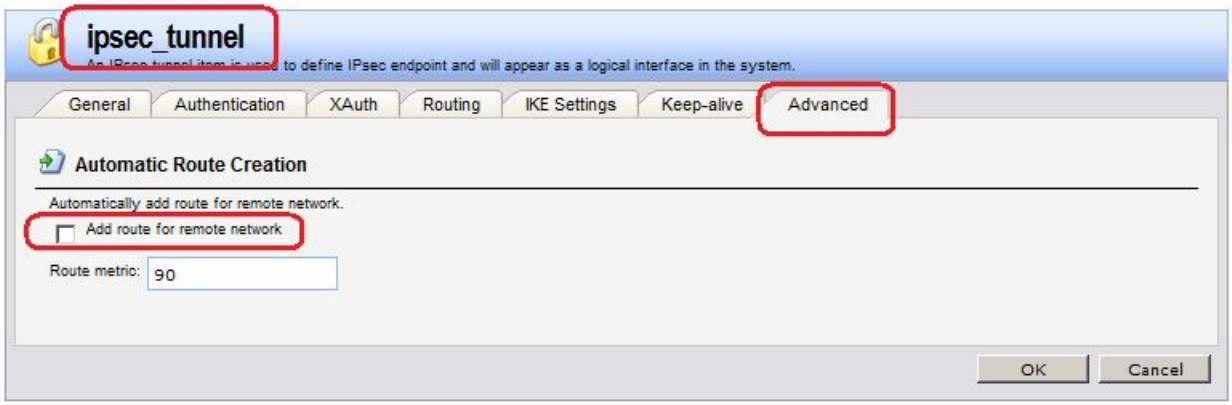
2. Динамически создаваемый маршрут.

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.



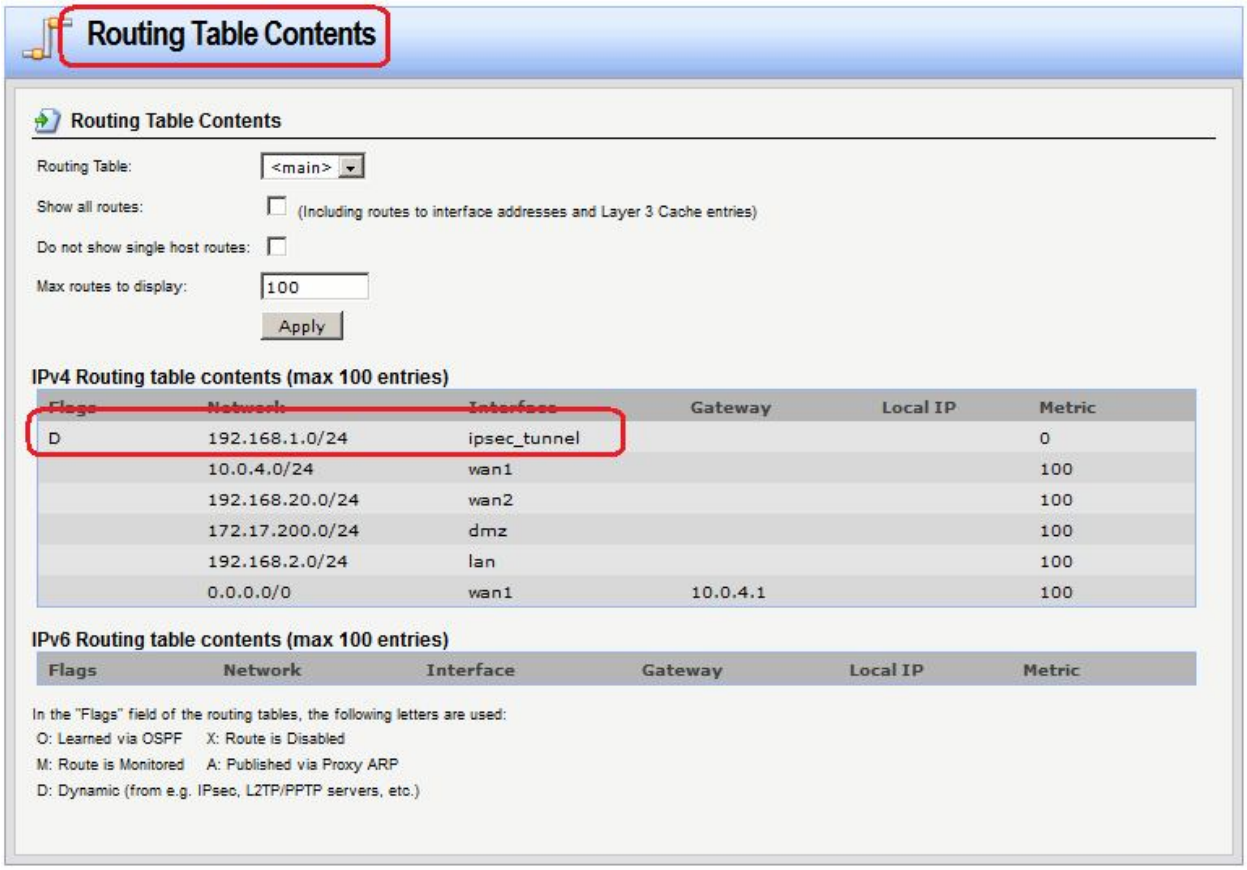
А на вкладке **Advanced** снять флаг добавления маршрута, чтобы в таблице маршрутизации при наличии IPSec-трафика не было двух одинаковых маршрутов.



Командная строка:

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

В этом случае в таблице маршрутизации будет динамически создаваться маршрут.



Правила фильтрования

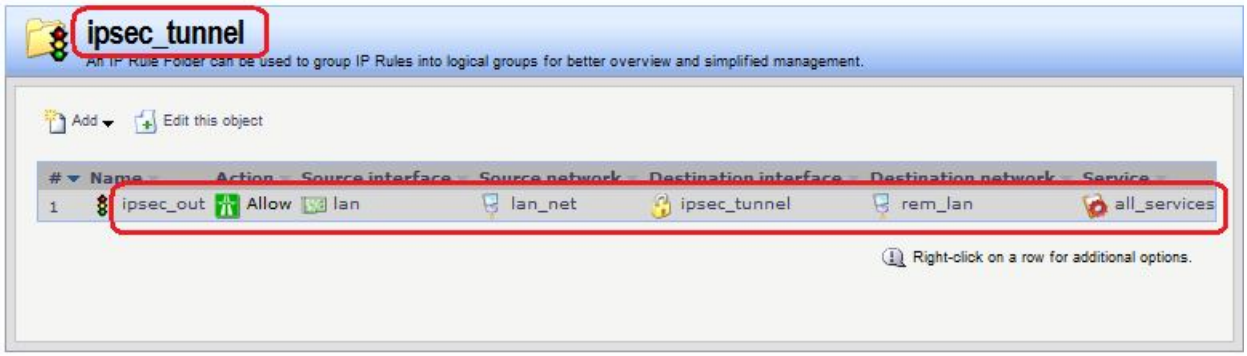
Определим правило, разрешающее исходящий трафик с локальной сети, расположенной за МЭ 1, на локальную сеть, расположенную за МЭ 2.

Веб-интерфейс:

`Rules → IP Rules → Add → IP Rule Folder`

`Name: ipsec_tunnel`

`Rules → IP Rules → ipsec_tunnel → Add`



Командная строка:

```
add IPRuleFolder Name=ipsec_tunnel
```

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

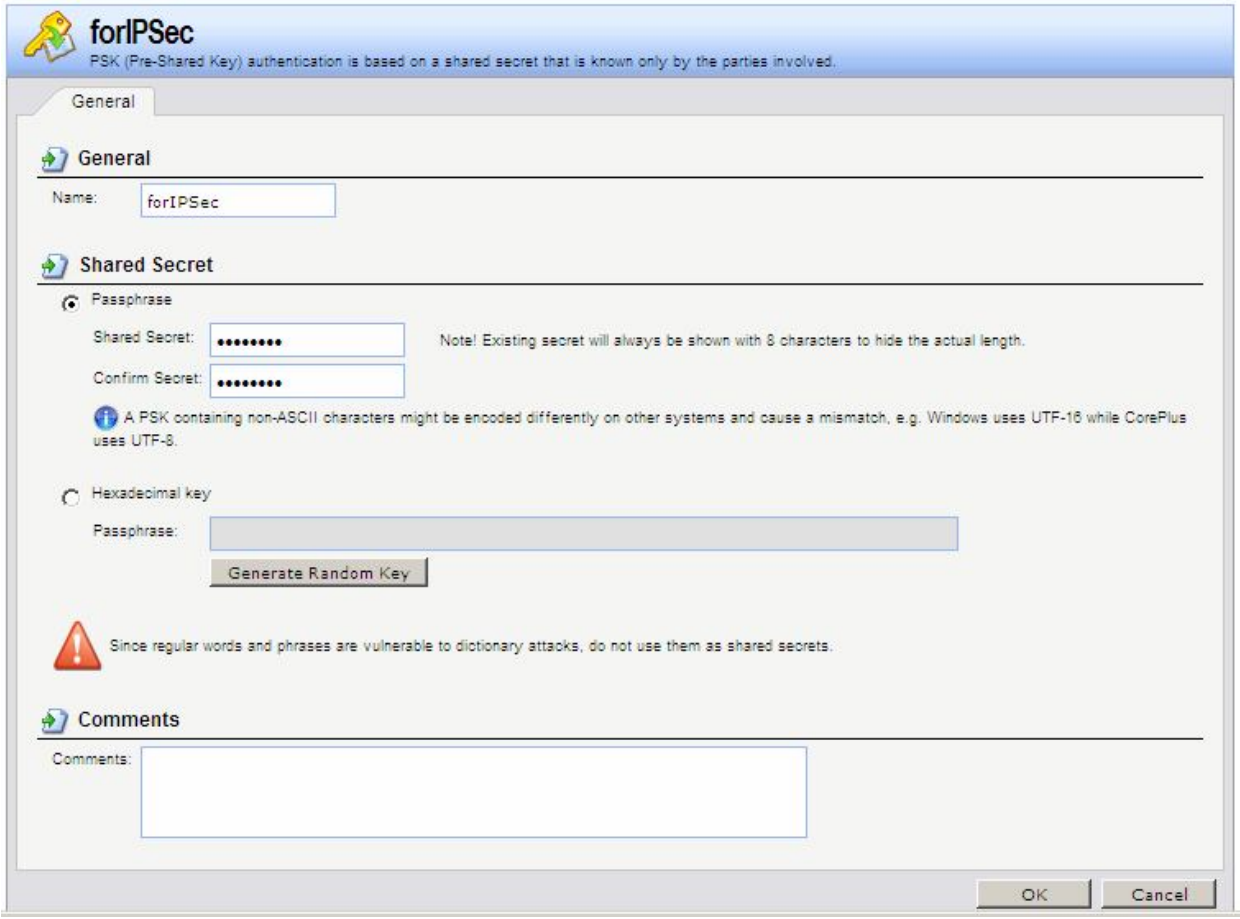
```
add IPRule Action=Allow SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=ipsec_tunnel DestinationNetwork=remote/rem_lan
Service=all_services Name=ipsec_out
```

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`



Командная строка:

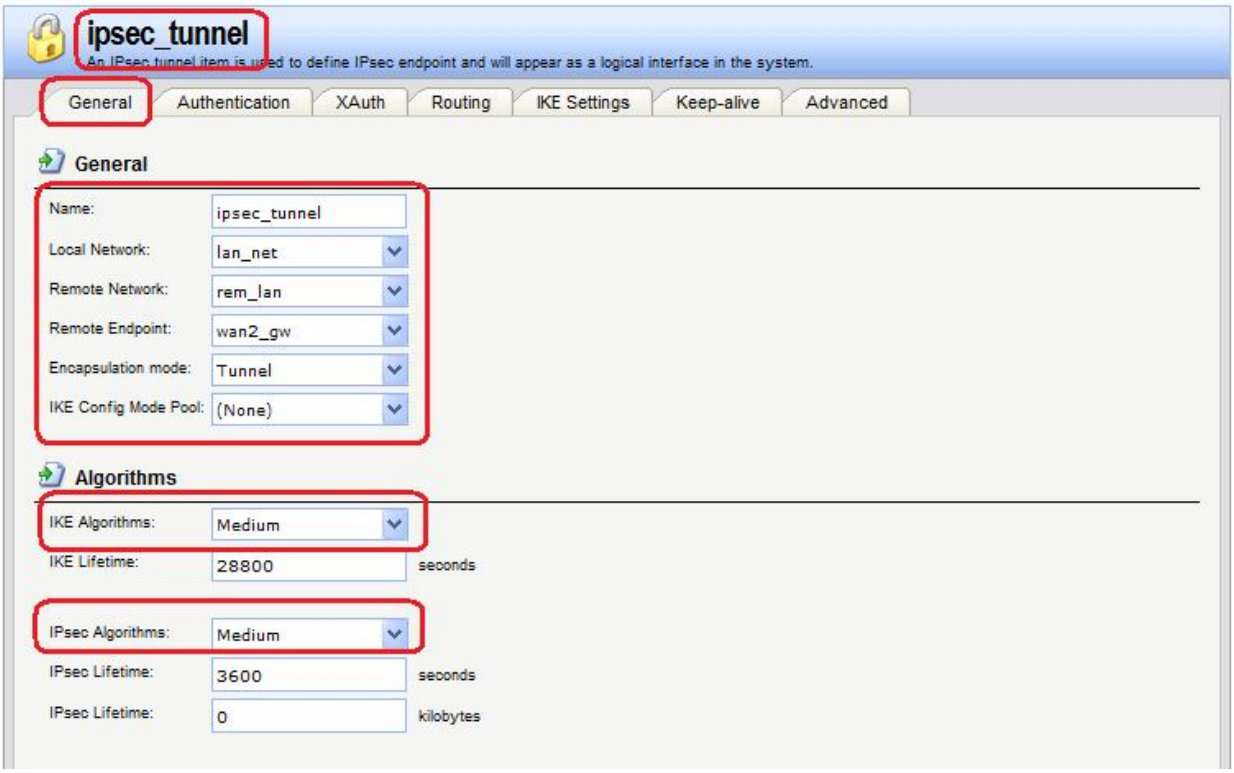
```
add PSK forIPSec Type=ASCII PSKAscii=qwerty
```

IPSec-Интерфейс
Необходимо создать IPSec-интерфейс.

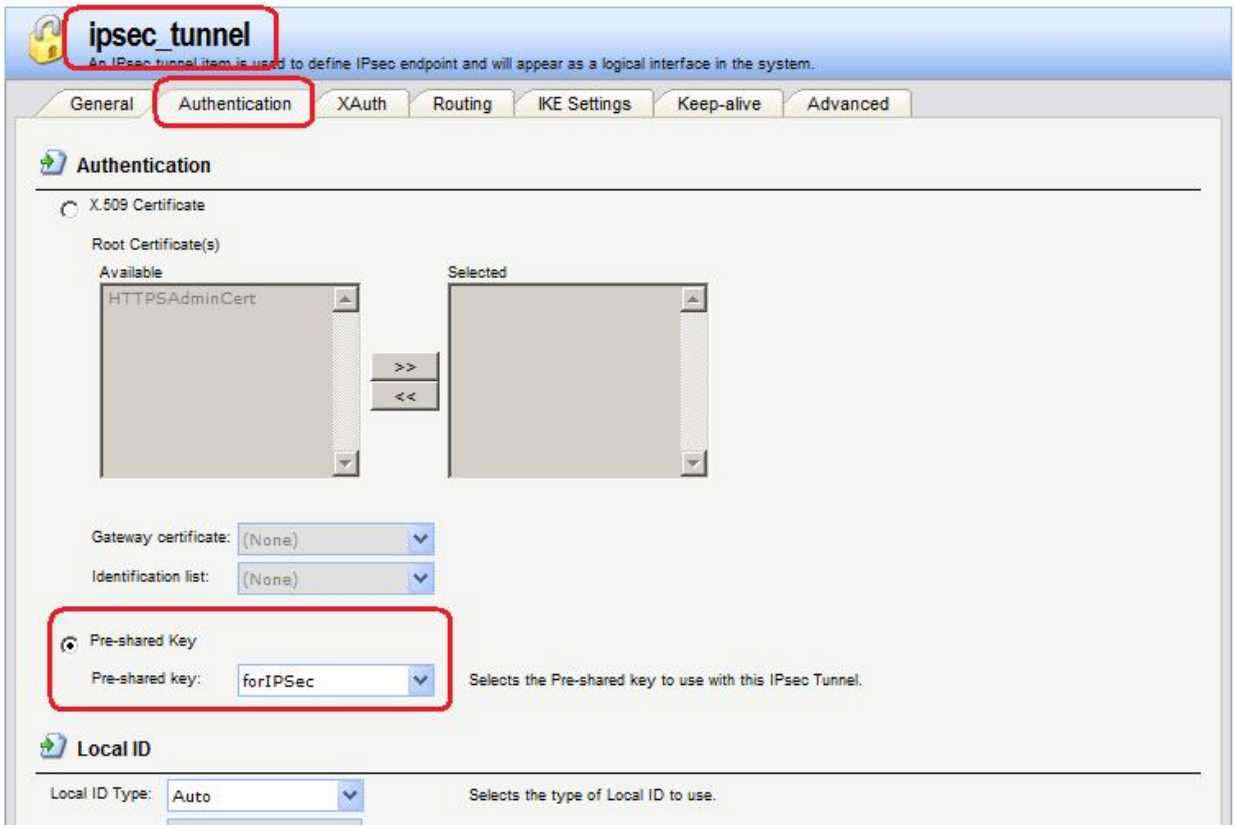
Веб-интерфейс:

`Interfaces → IPsec → Add → IPsec Tunnel`

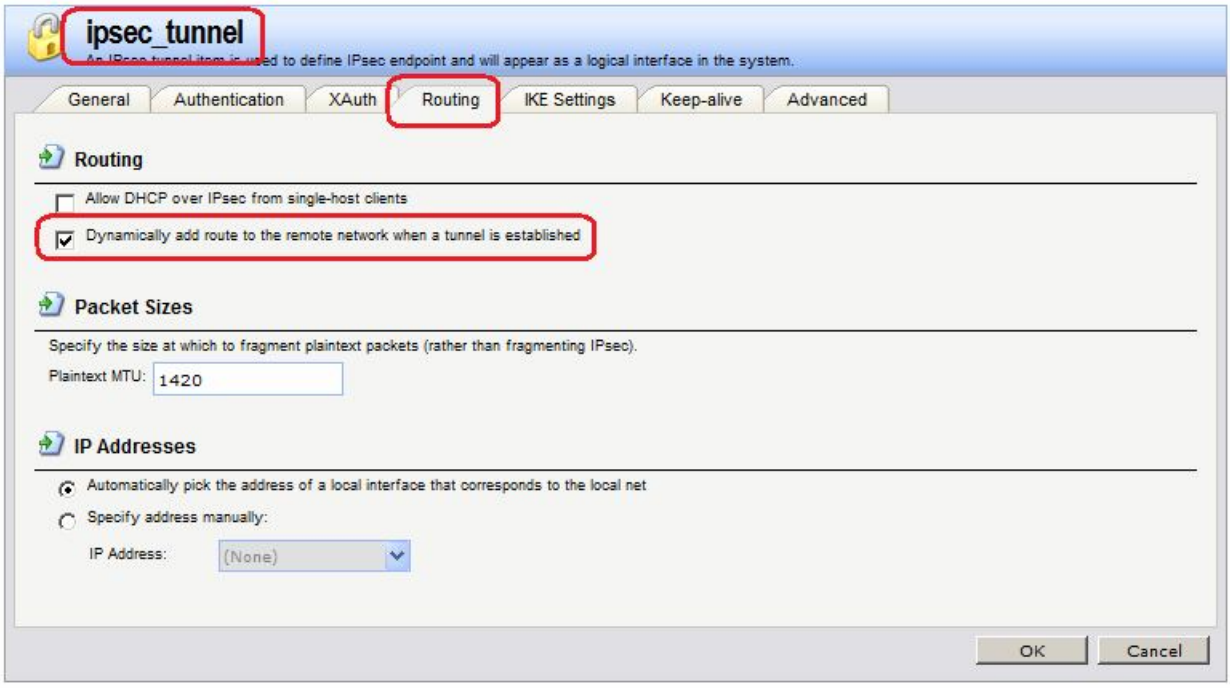
На вкладке **`General`** указать сети перед и за туннелем, а также режим выполнения IPSec и используемые наборы алгоритмов для IPSec и IKE.



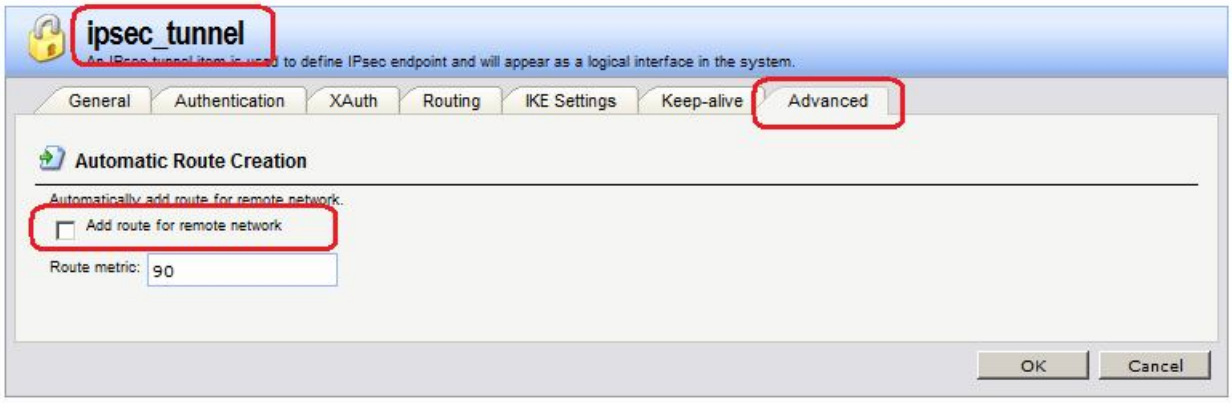
На вкладке **`Authentication`** указать созданный аутентификационный объект.



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 фильтрования

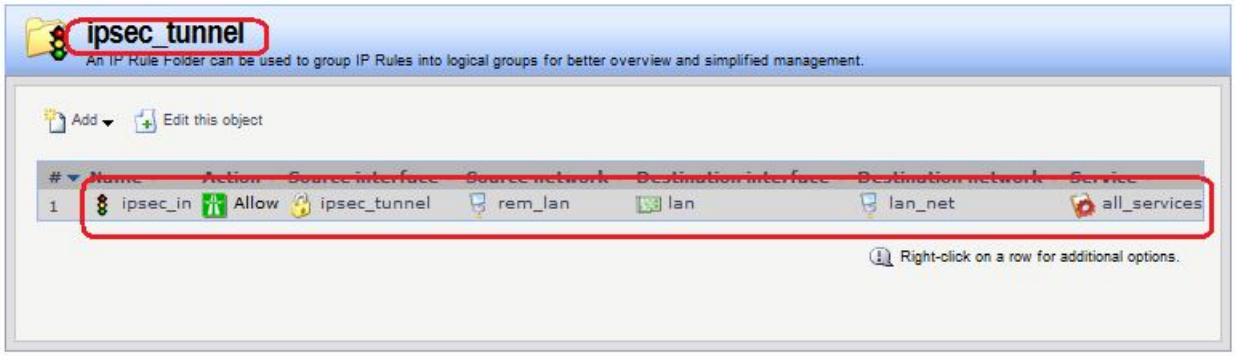
Создаем правила фильтрования, разрешающие входящий трафик с удаленной локальной сети, приходящий на ipsec-туннель, к локальной сети, расположенной за МЭ 2.

Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: ipsec_tunnel

Rules → IP Rules → ipsec_tunnel → Add

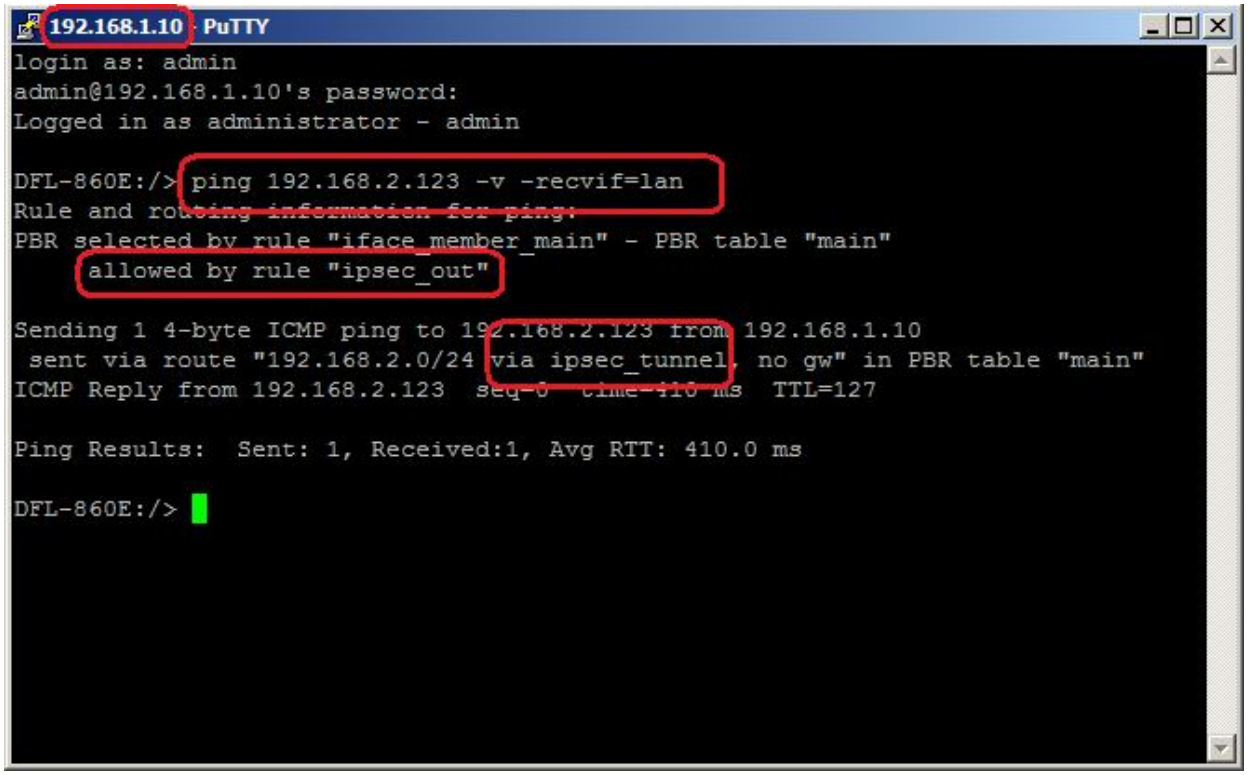


Командная строка:

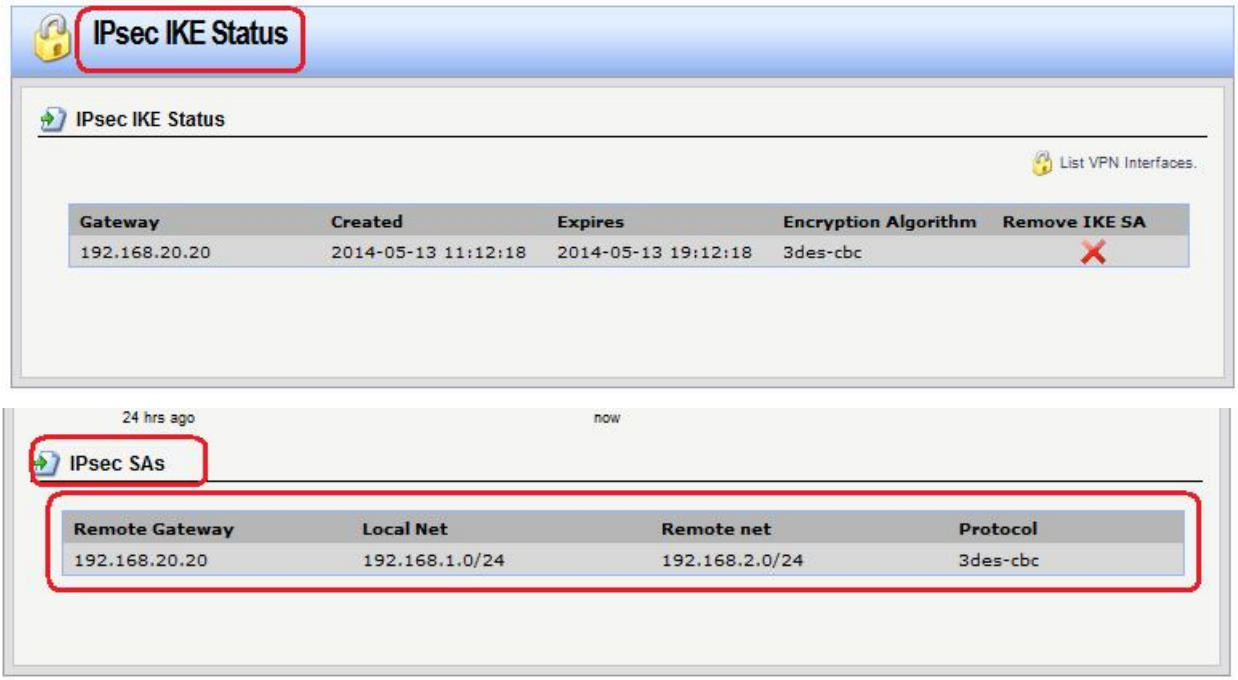
```
add IPRuleFolder Name=ipsec_tunnel
cc IPRuleFolder <N folder>
add IPRule Action=Allow SourceInterface=ipsec_tunnel
SourceNetwork=remote/rem_lan DestinationInterface=lan
DestinationNetwork=lan/lan_net Service=all_services Name=ipsec_in
```

Проверка конфигурации

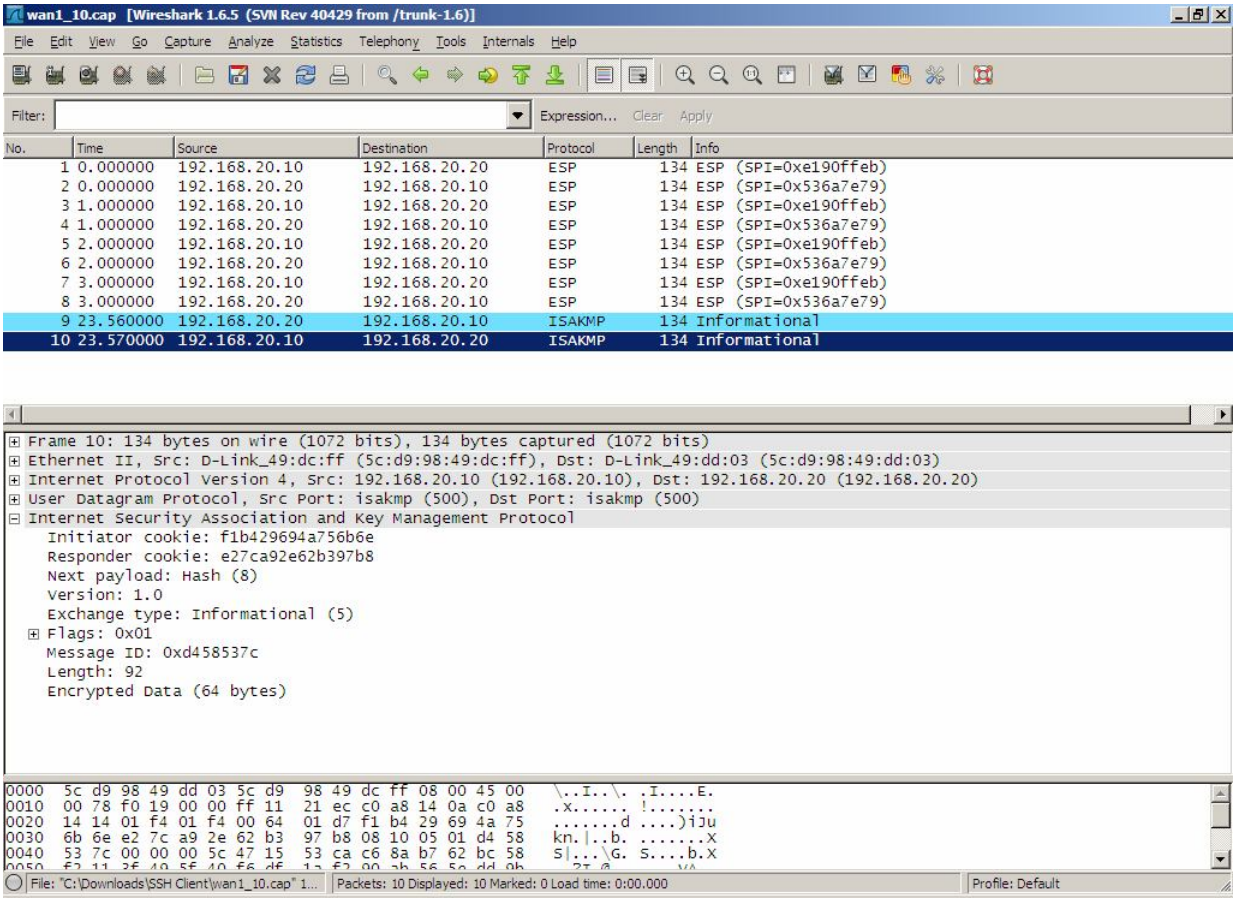
1. На МЭ1 выполняем команду **ping** рабочей станции, расположенной в удаленной локальной сети. В качестве интерфейса, с которого пакет будет отправлен, указывает **lan**.



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



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.



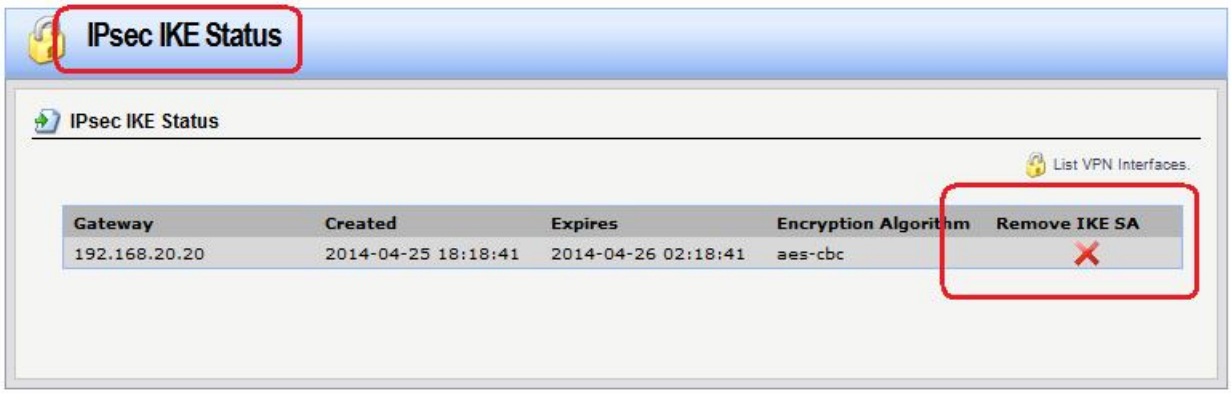
Лабораторная работа 3. Посмотреть статистику IPSec-туннелей можно из командной строки:

```
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:

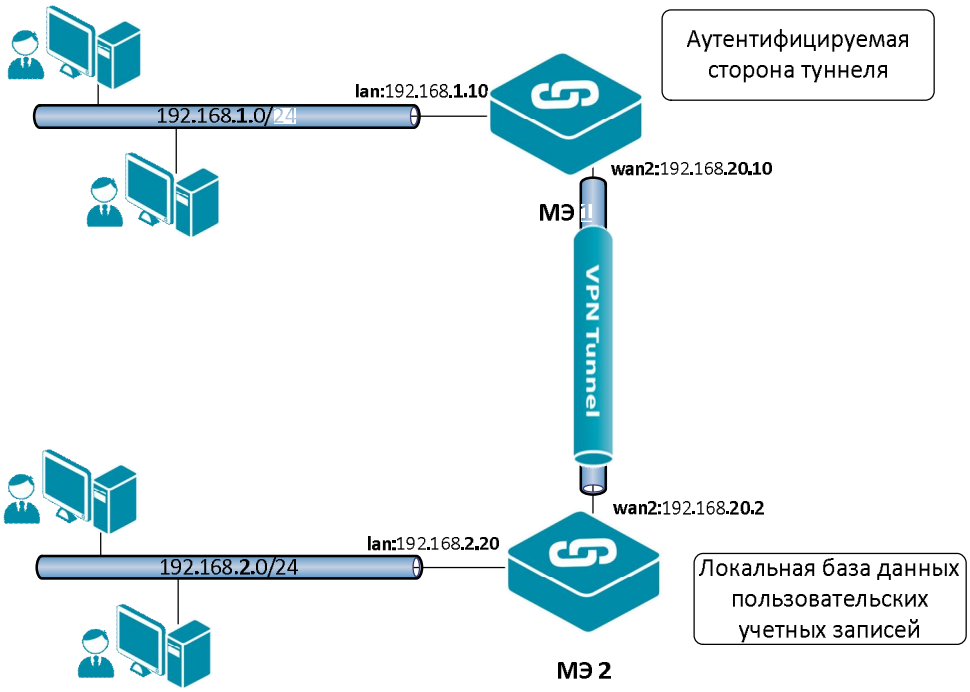
```
killsa <IP-адрес>
killsa -all
```

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



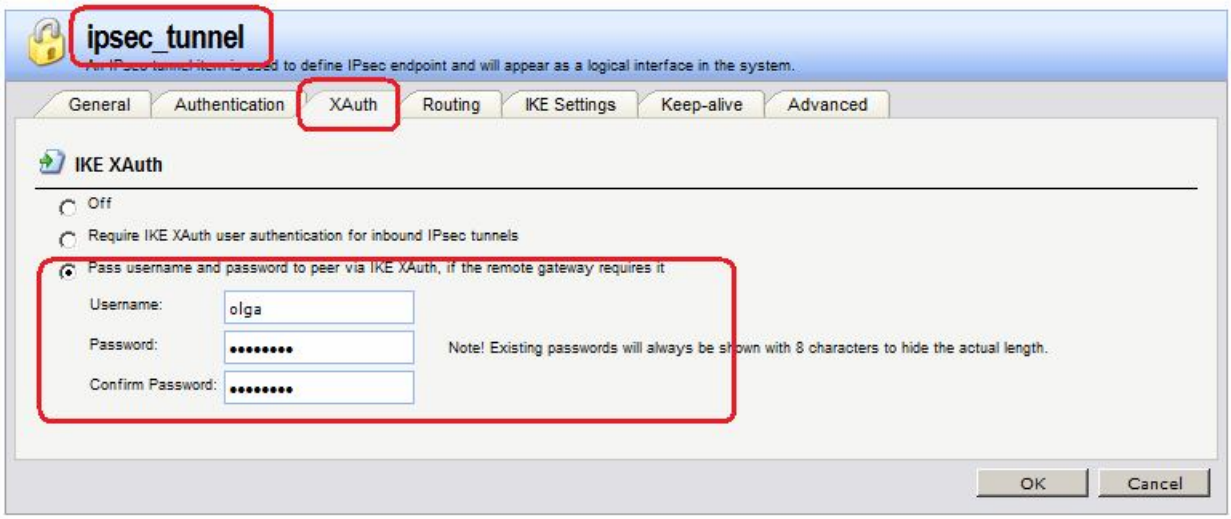
Описание практической работы

Межсетевой Экран 1

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

Веб-интерфейс:

`Interfaces → IPsec → ipsec`



Командная строка:

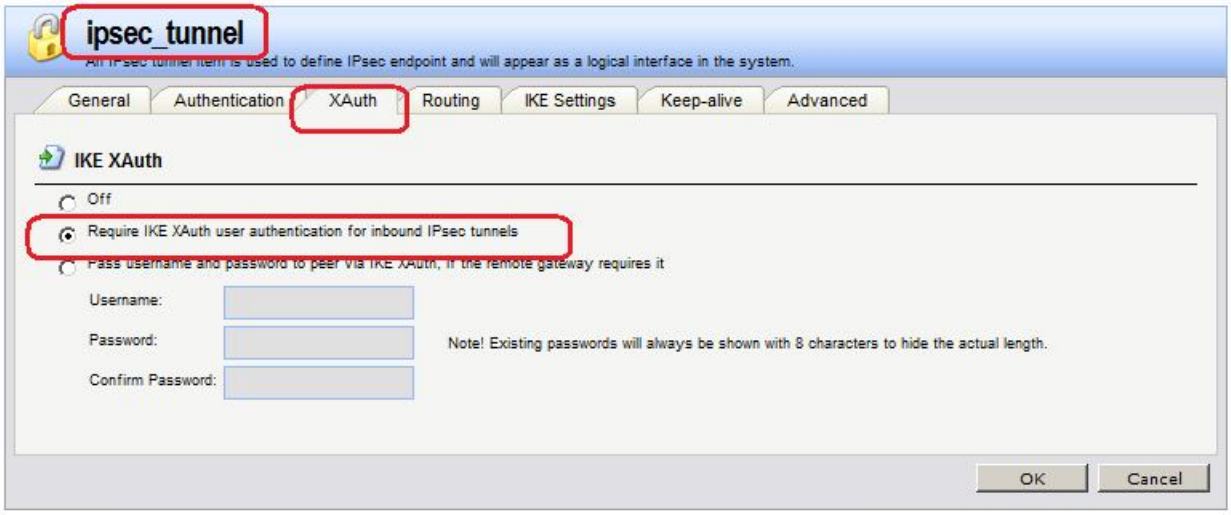
```
set Interface IPsecTunnel ipsec_tunnel XAuth=PassToPeerGateway
XAuthUsername=olga XAuthPassword=qwerty
```

Межсетевой Экран 2

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

Веб-интерфейс:

`Interfaces → IPsec → IPSec_tunnel`



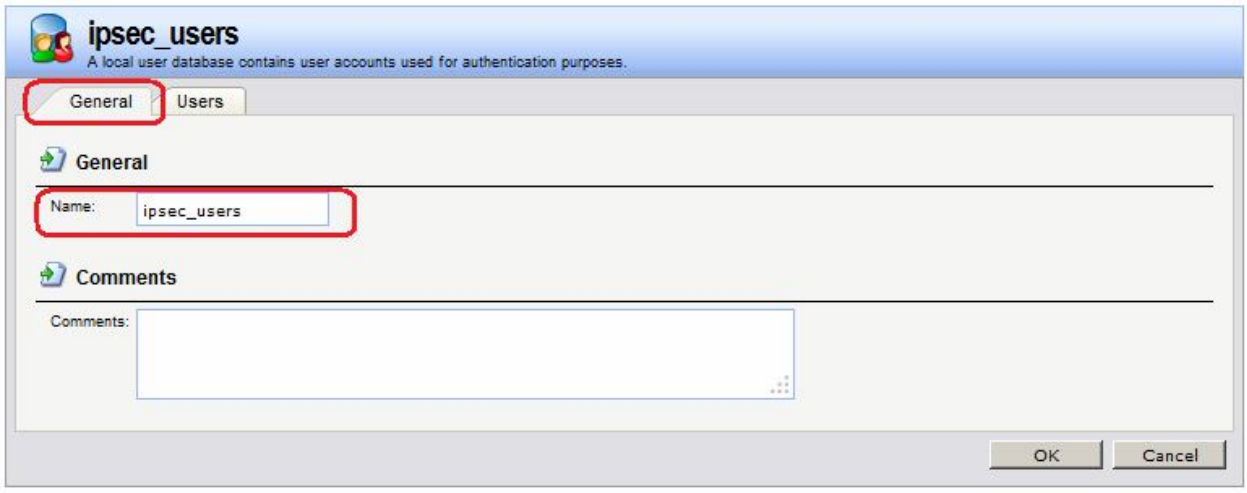
Командная строка:

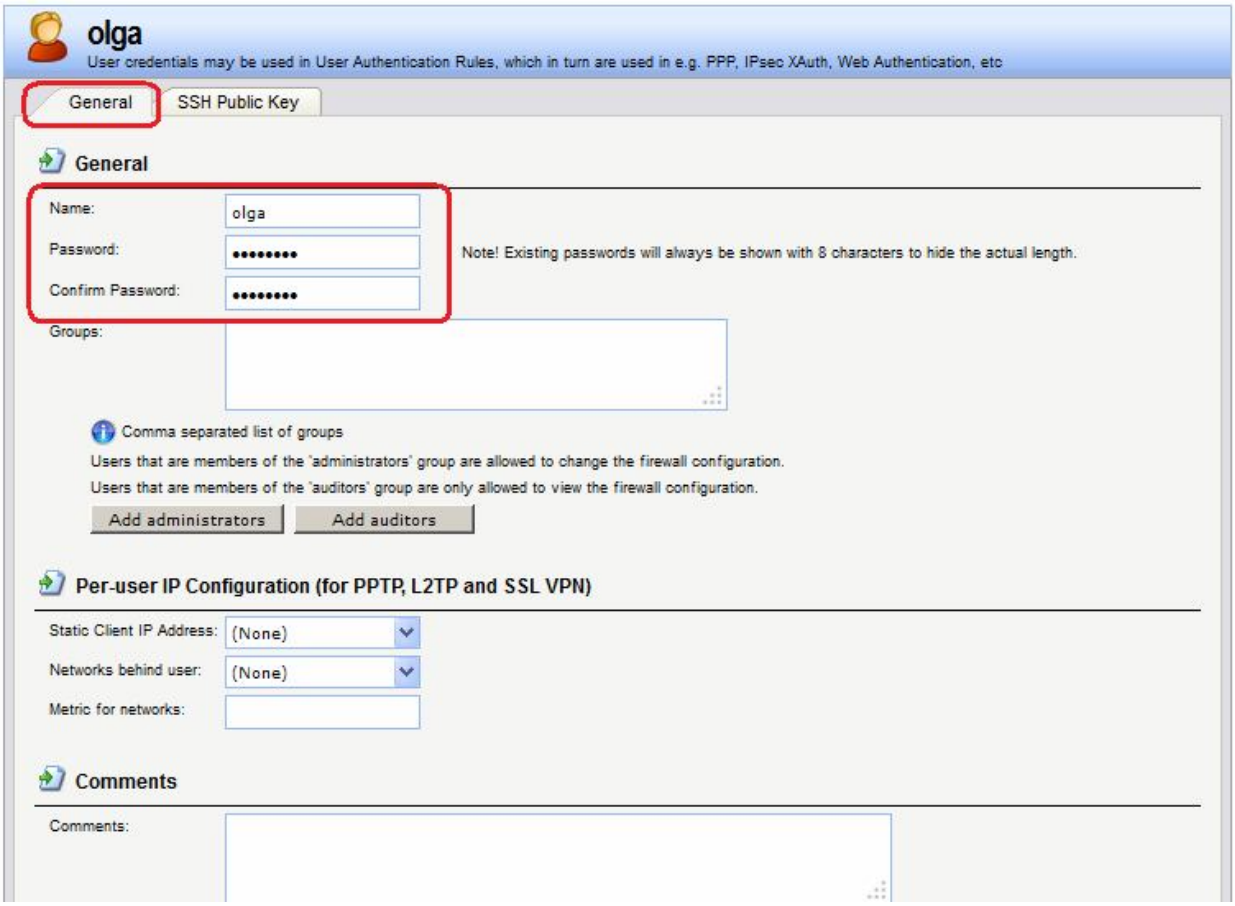
```
set Interface IPsecTunnel ipsec_tunnel XAuth=RequiredForInbound
```

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`





Командная строка:

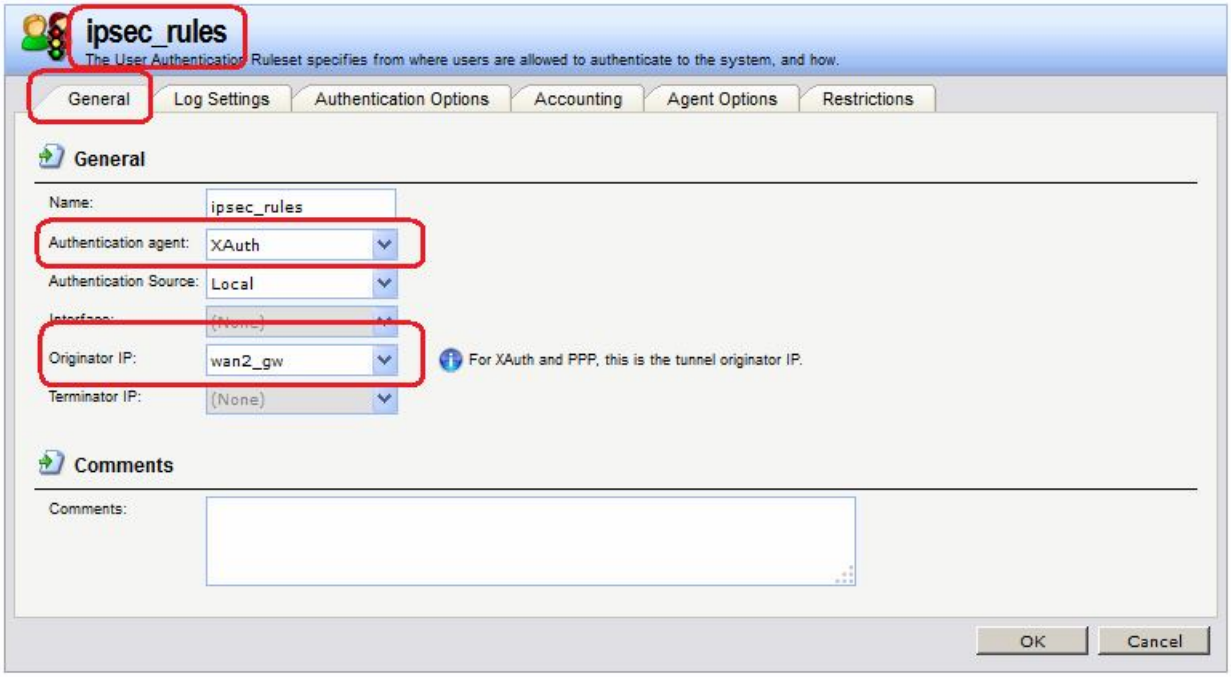
```
add LocalUserDatabase ipsec_users
add User olga Password=qwerty
```

Создать правило аутентификации пользователей.

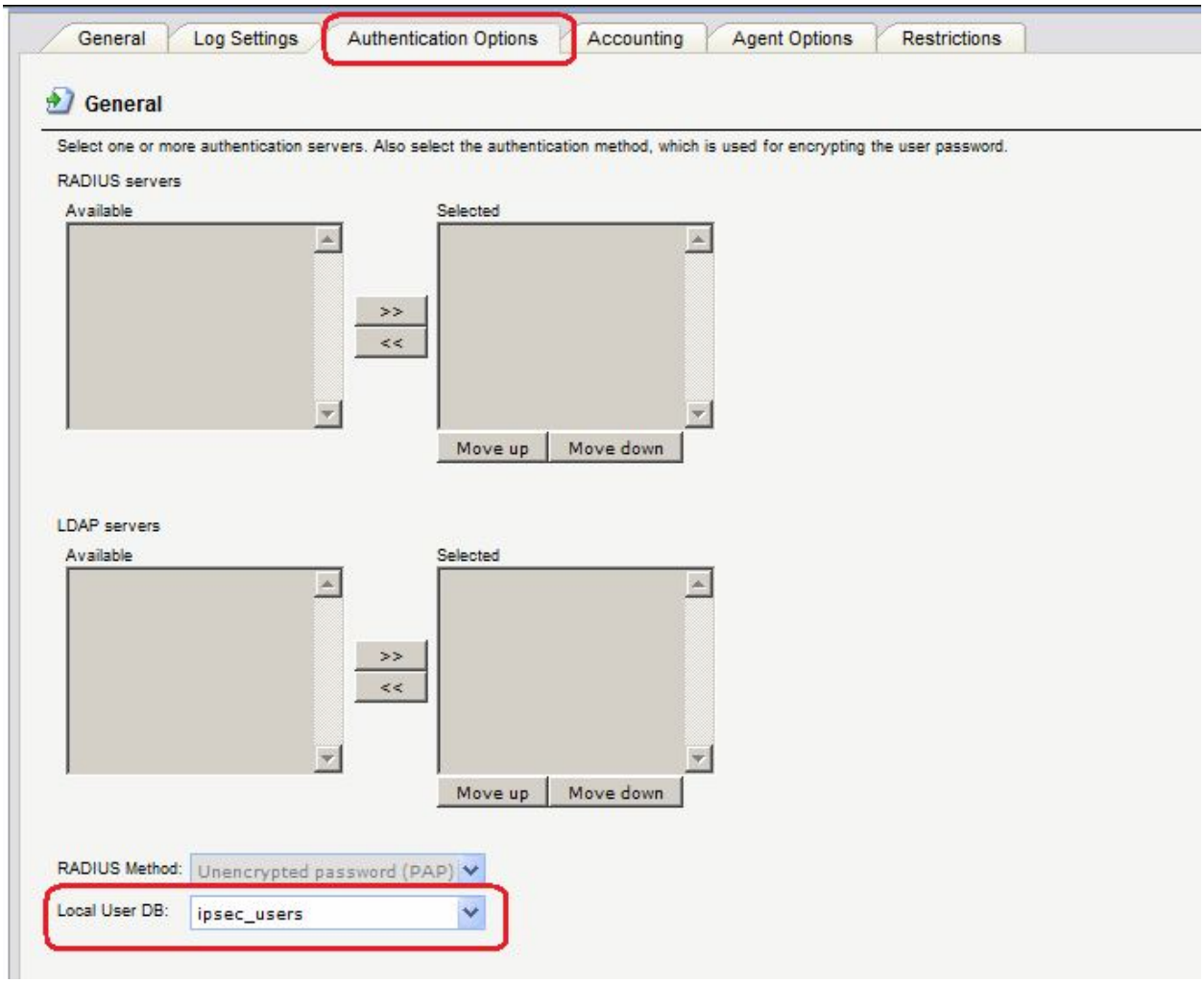
Веб-интерфейс:

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.



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

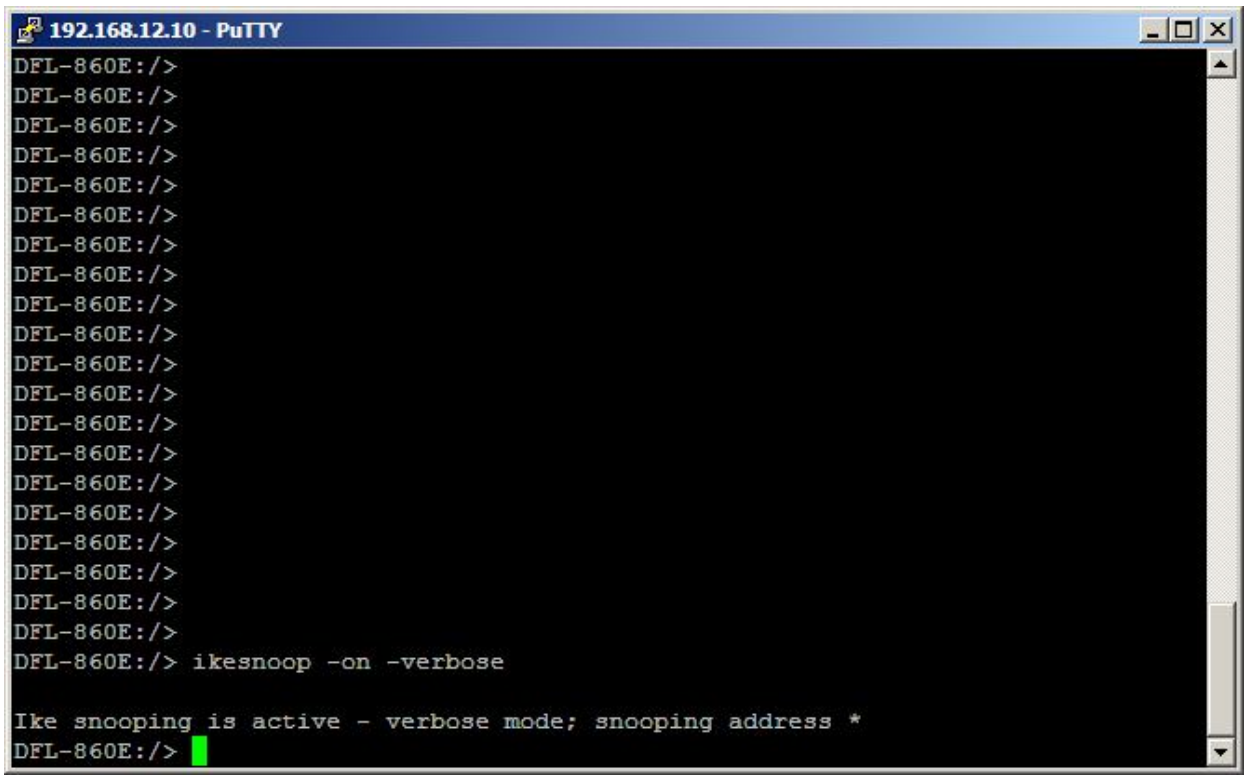


Командная строка:

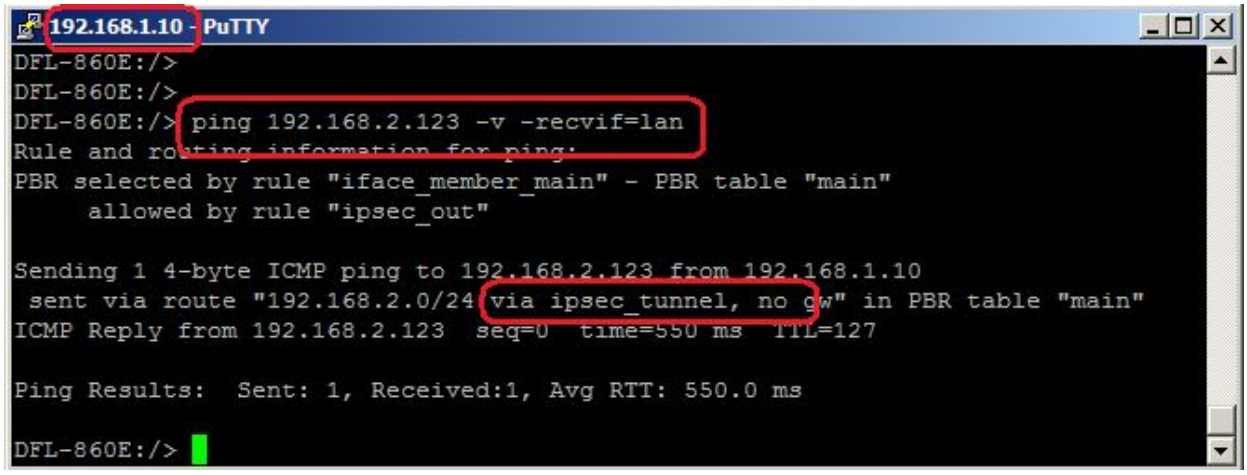
```
add UserAuthRule AuthSource=Local OriginatorIP=wan2/wan2_gw
LocalUserDB=ipsec_users Agent=XAuth Name=ipsec_rules
```

Проверка конфигурации

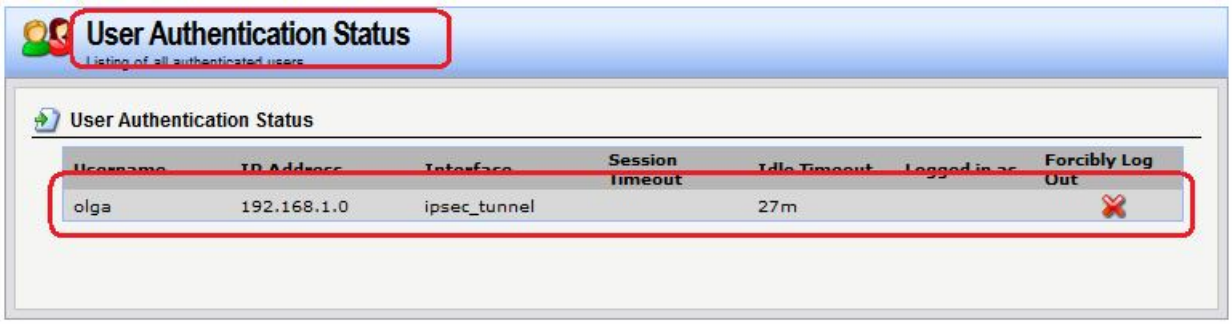
На МЭ 1 выполнить команду **`ikesnoop`**, которая позволяет отслеживать состояние IKE SA.



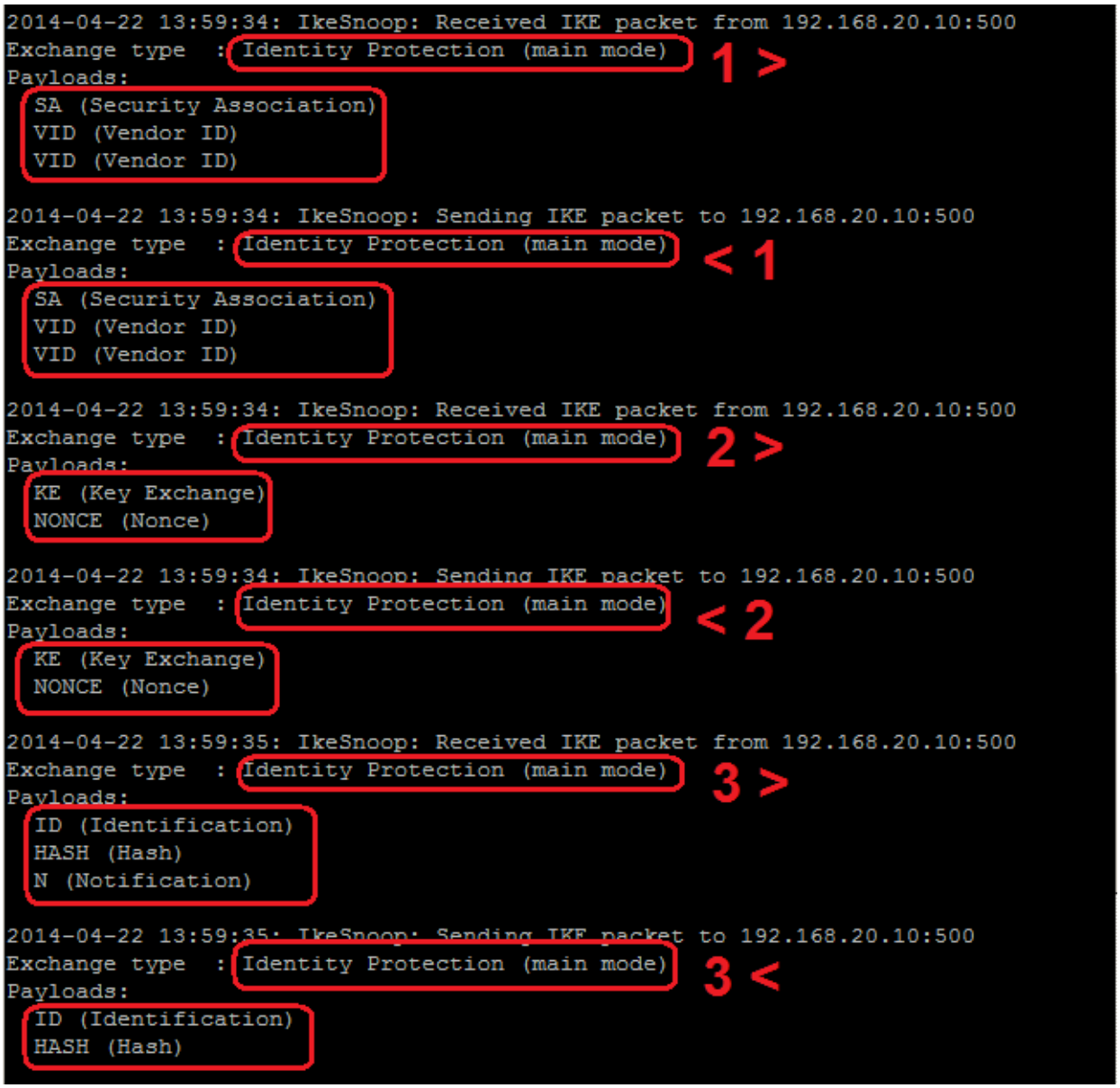
Выполнить команду **ping** на хосте, расположенный в удаленной локальной сети.

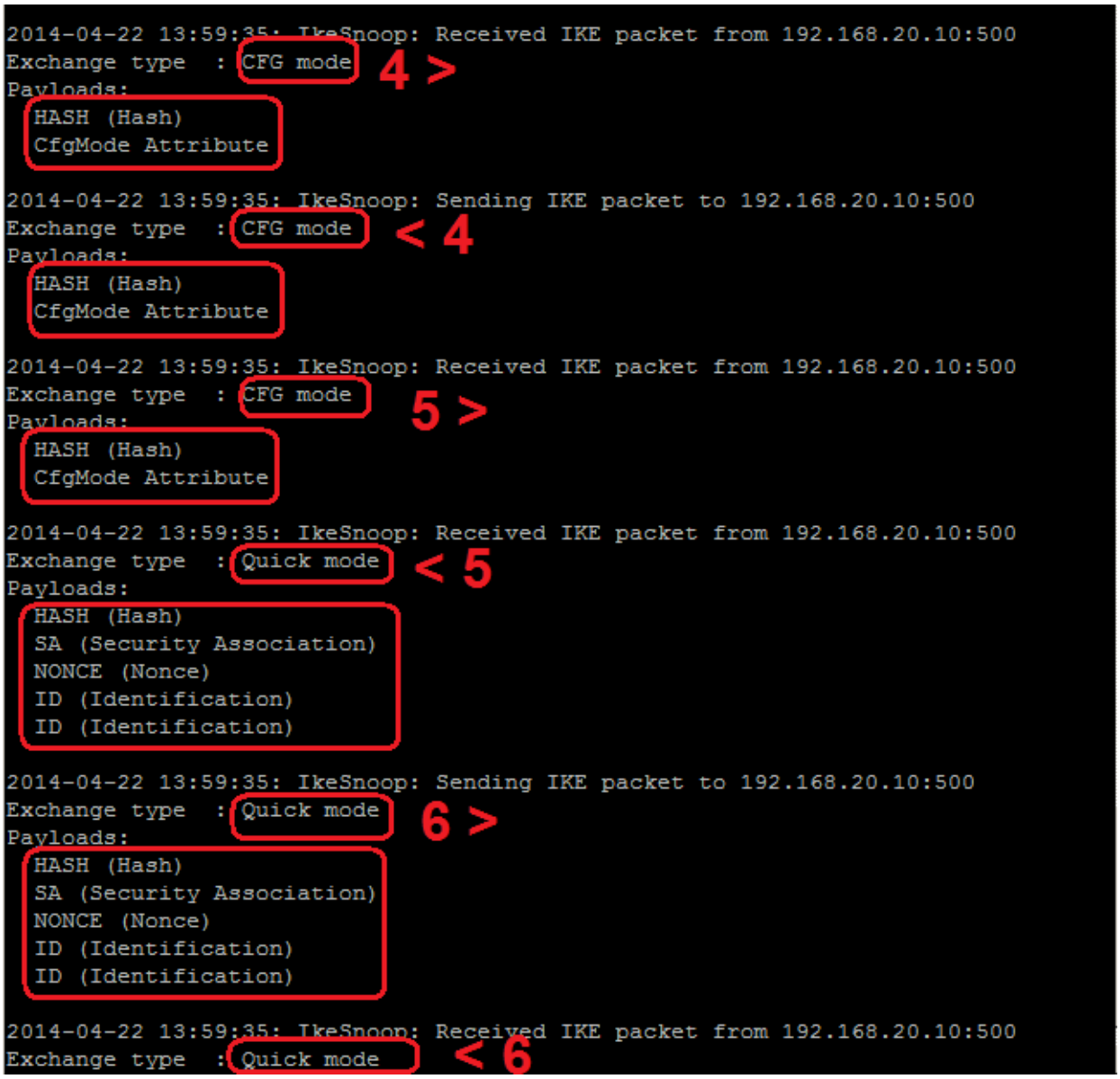


В этом случае на аутентифицирующей стороне туннеля будет не только установлены SA IPSec и SA IKE, но и будет показан статус аутентифицированного пользователя.



Проверить, что **ikesnoop** показывает наличие **mode CFG** и атрибутов **XAuth**.


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)



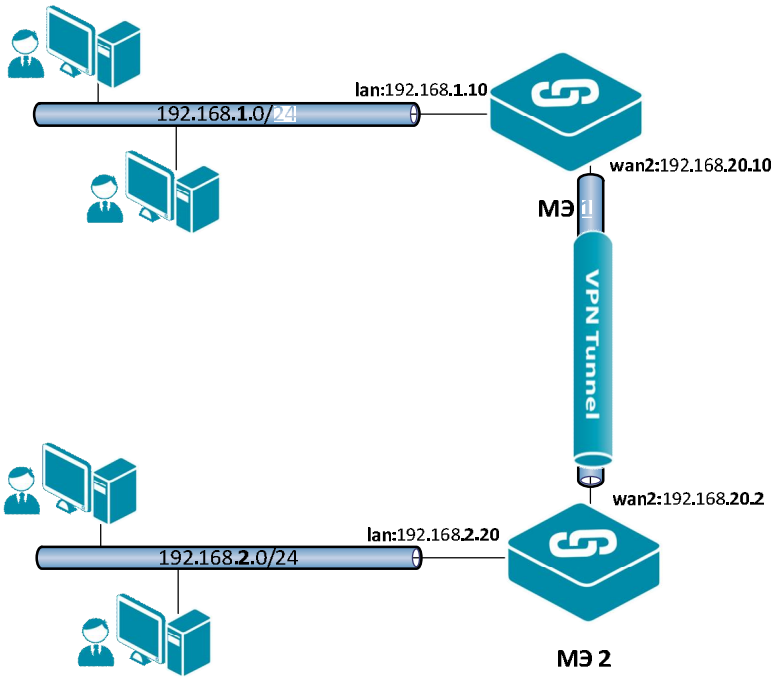
При использовании аутентификации по стандарту XAuth инициатором создания соединения всегда должна быть аутентифицируемая сторона (в нашем случае МЭ 1). В этом случае Инициатор до выполнения **Quick mode** использует **CFG mode** для передачи имени пользователя и пароля (транзакции 4 и 5), и только после 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 фильтрования, 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 1и 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.

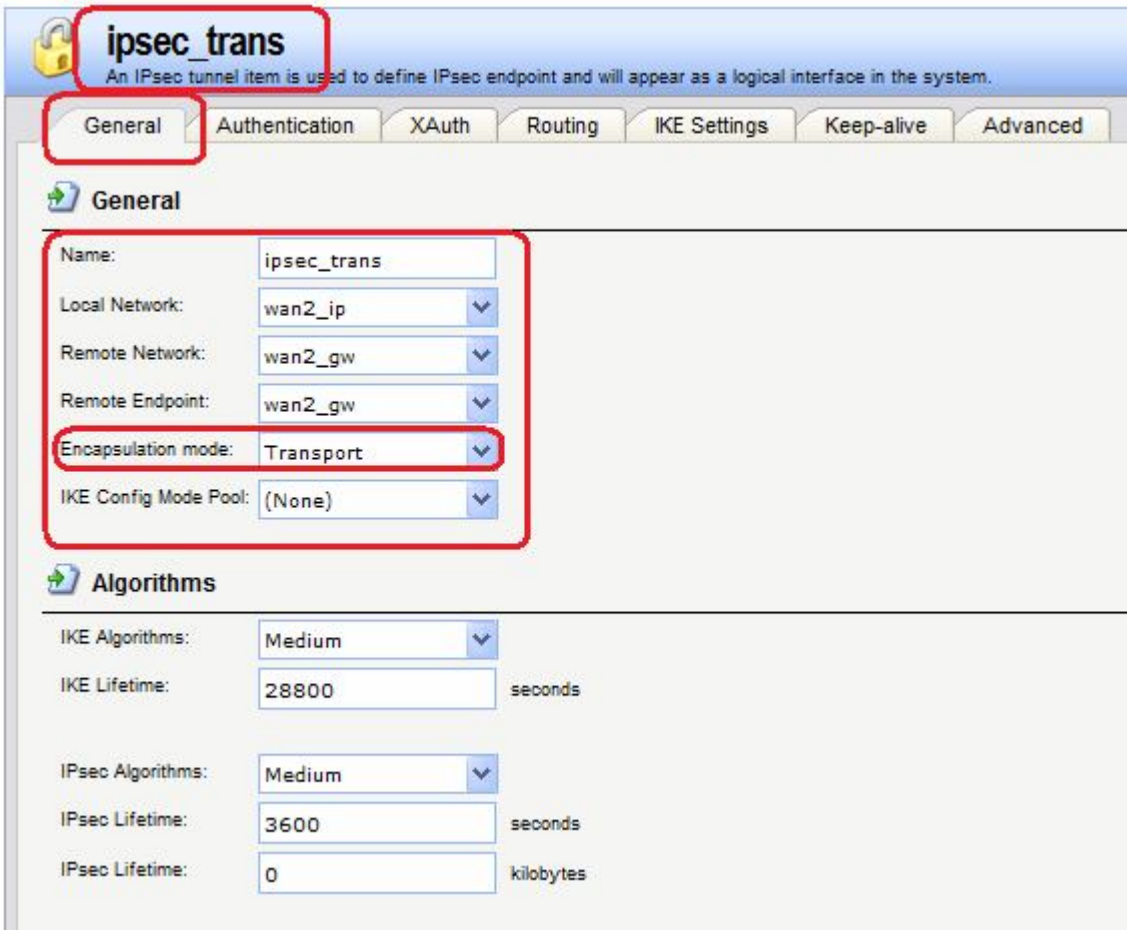
Межсетевой Экран 1

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 фильтрования

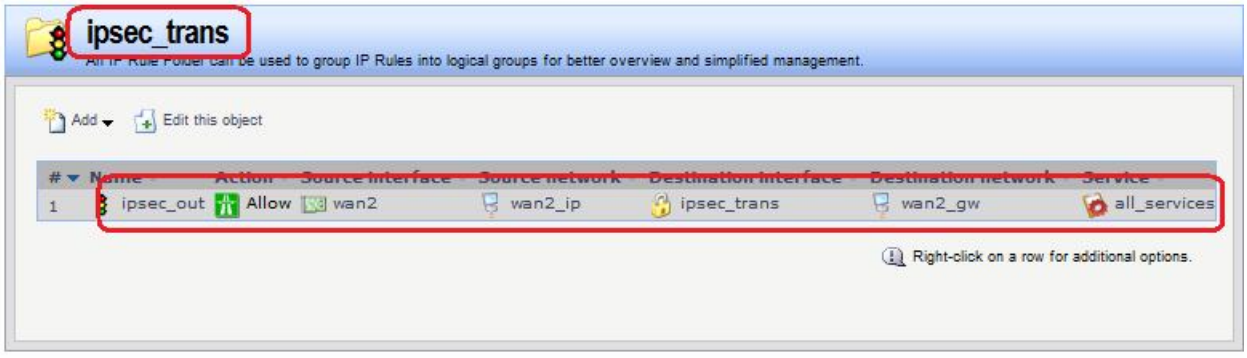
Определим правило, разрешающее исходящий трафик с МЭ 1 на МЭ 2.

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
```

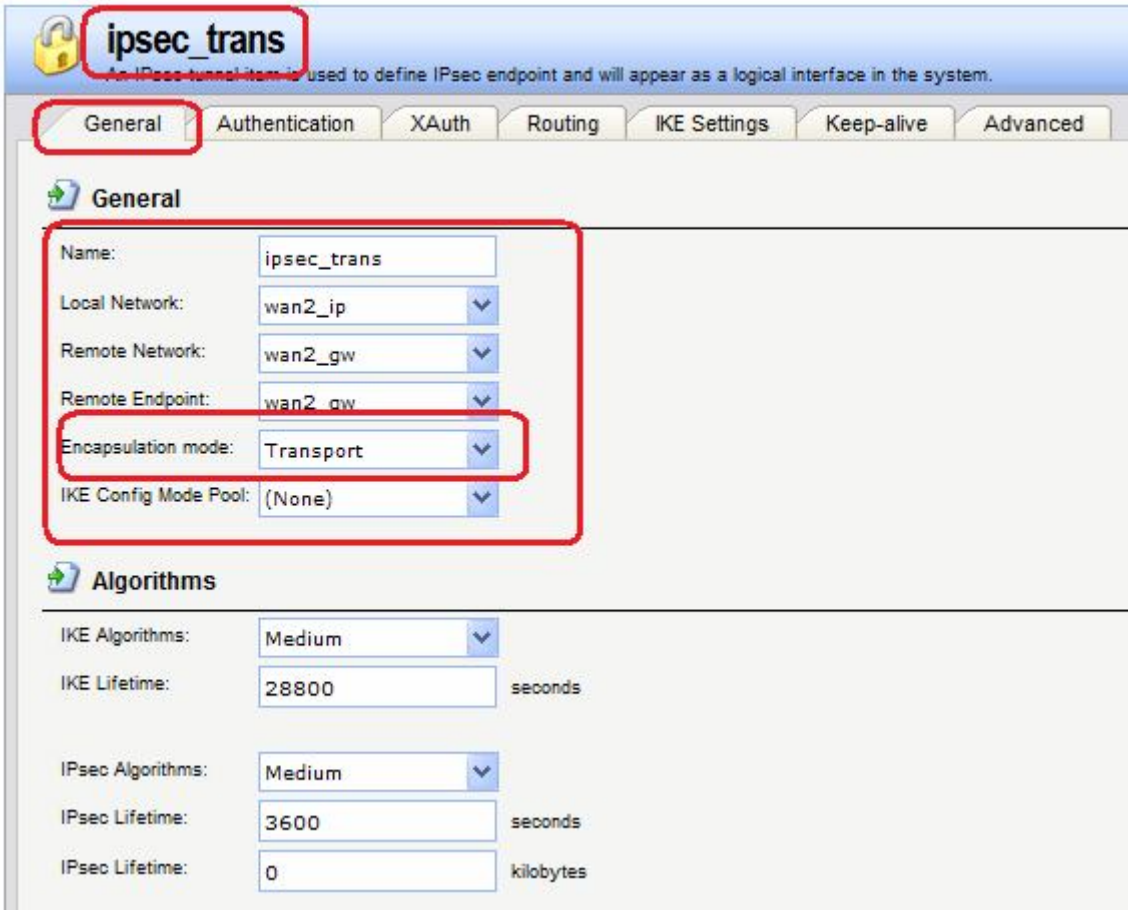
Межсетевой Экран 2

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.



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
```

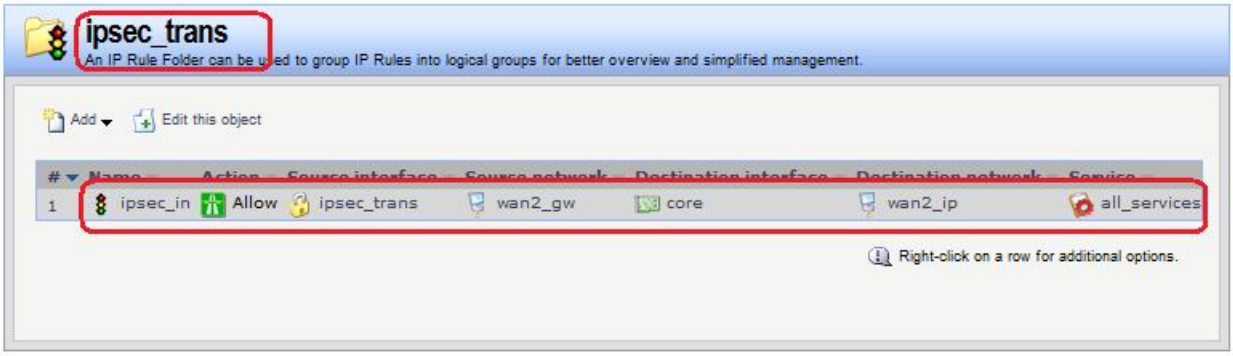
Правила фильтрования
Определим правило, разрешающее входящий трафик с МЭ 1 на МЭ 2.

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

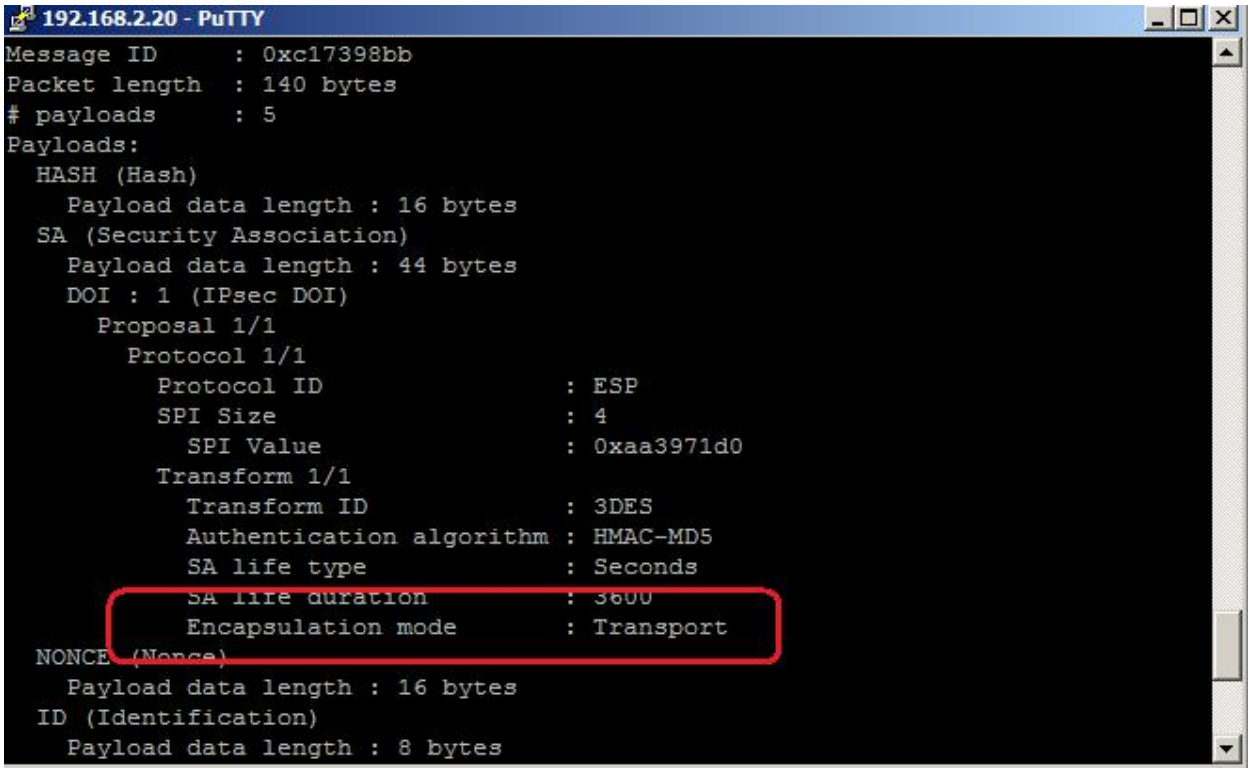
Выполнить команду

```
ikesnoop -on –verbose
```

на МЭ 1.

Выполнить команду **ping** на МЭ 2.

Команда **ikesnoop** должна показать, что выполняется IPSec в транспортном режиме.

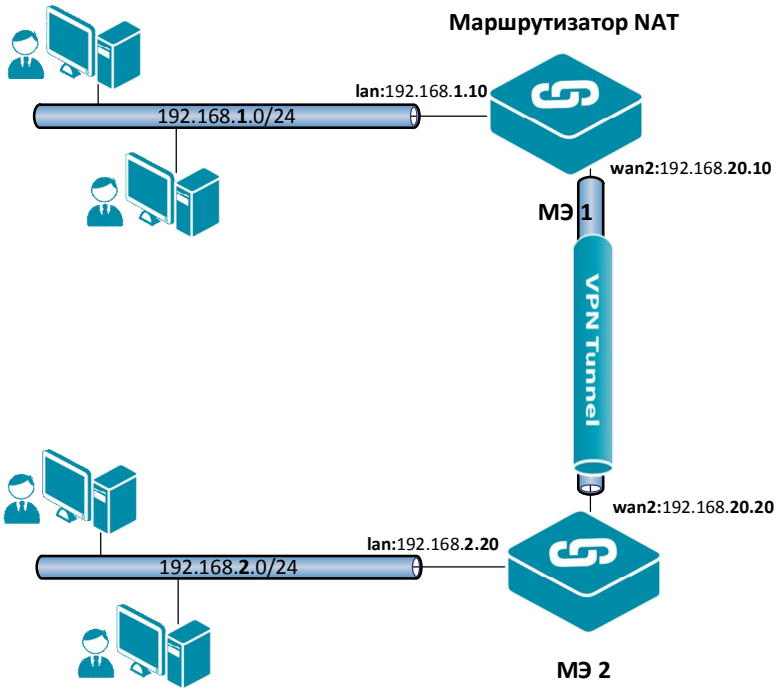


Лабораторная работа 5. Использование преобразования NAT в протоколе IPSec

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



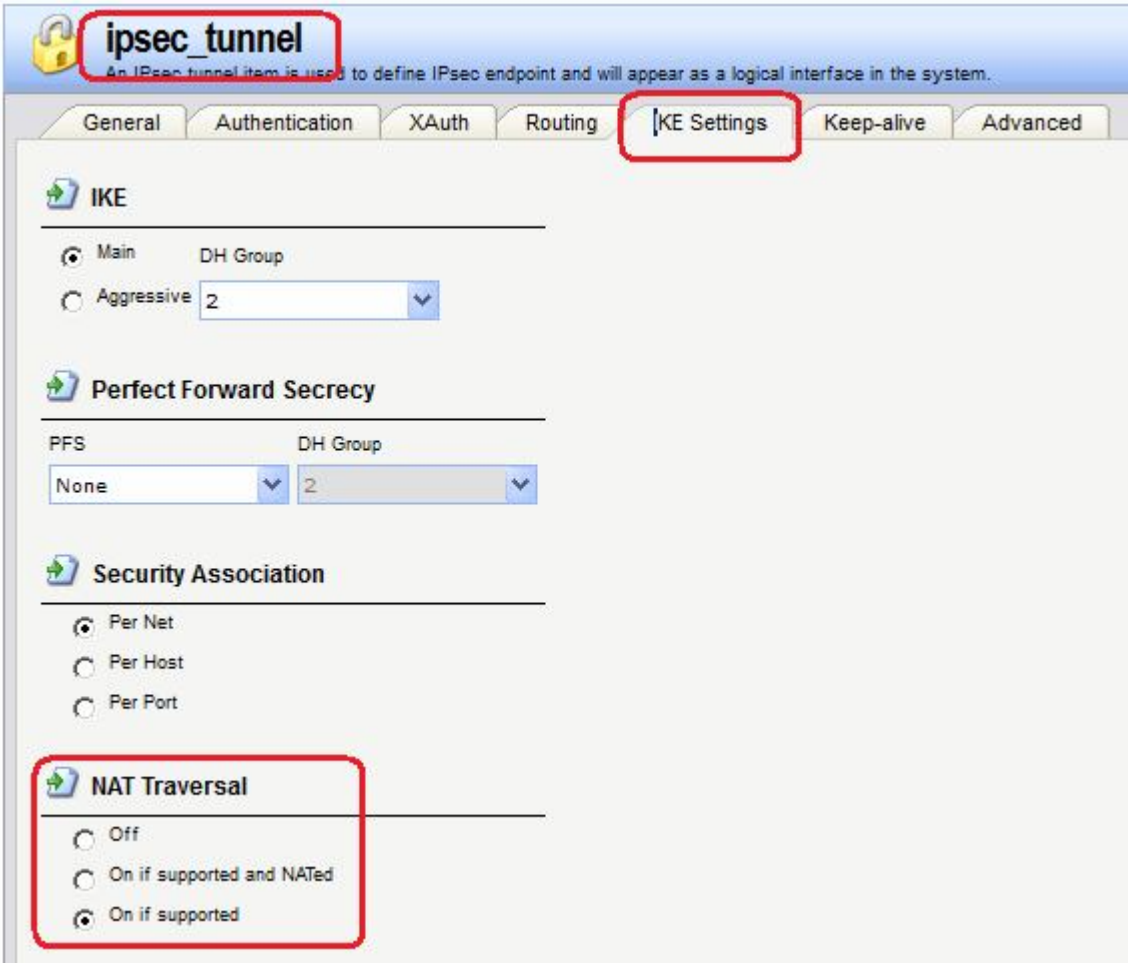
Описание практической работы

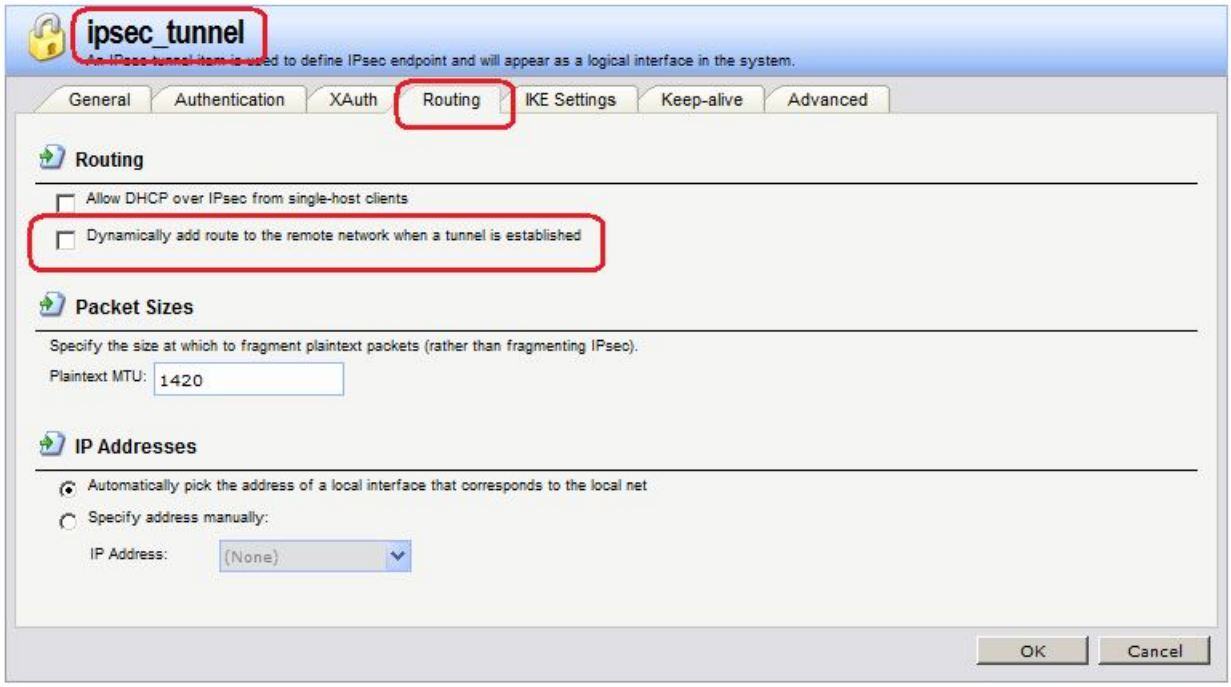
Межсетевой Экран 1

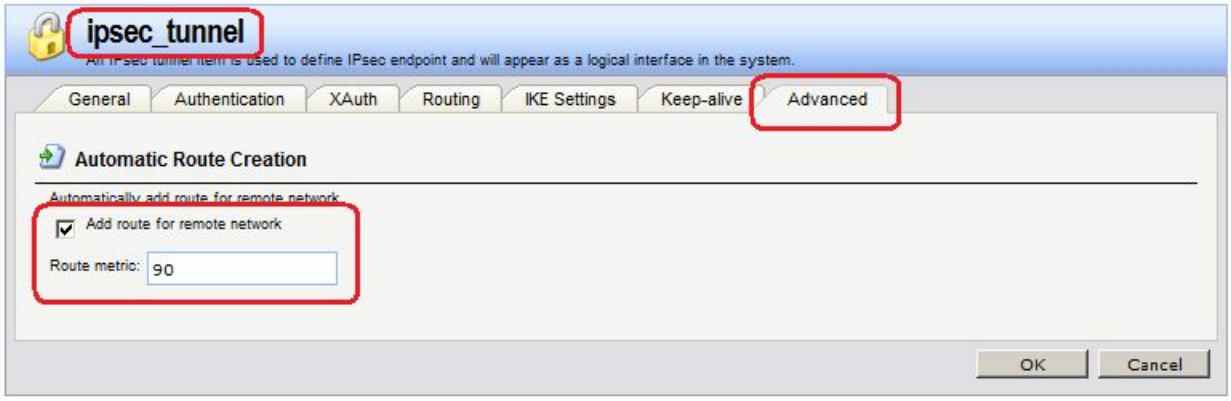
IPSec-Интерфейс

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:


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
IKE
Main
Aggressive
DH Group
2
Perfect Forward Secrecy
PFS
None
DH Group
2
Security Association
Per Net
Per Host
Per Port
NAT Traversal
Off
On if supported and NATed
On if supported


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
Routing
Allow DHCP over IPsec from single-host clients
Dynamically add route to the remote network when a tunnel is established
Packet Sizes
Specify the size at which to fragment plaintext packets (rather than fragmenting IPsec).
Plaintext MTU:
1420
IP Addresses
Automatically pick the address of a local interface that corresponds to the local net
Specify address manually:
IP Address:
(None)
OK
Cancel

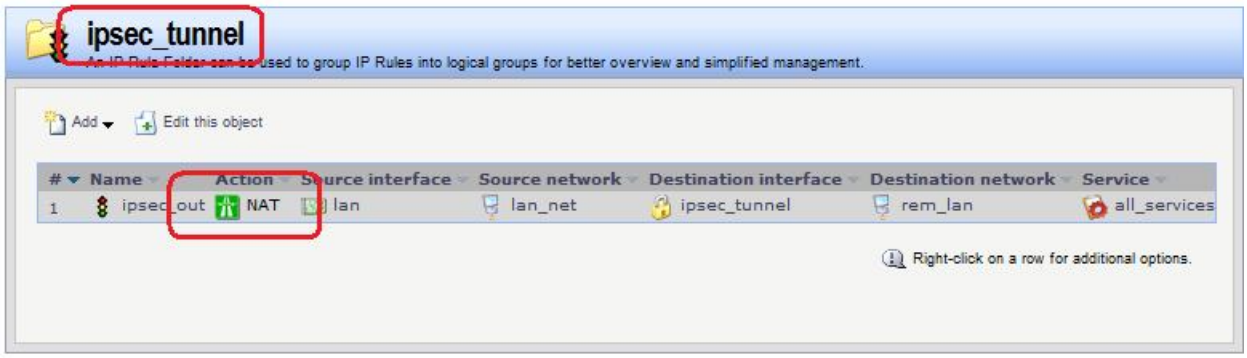


Командная строка:

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

Правила фильтрования

Вместо Правила **`Allow`** следует указать правило **`NAT`**.



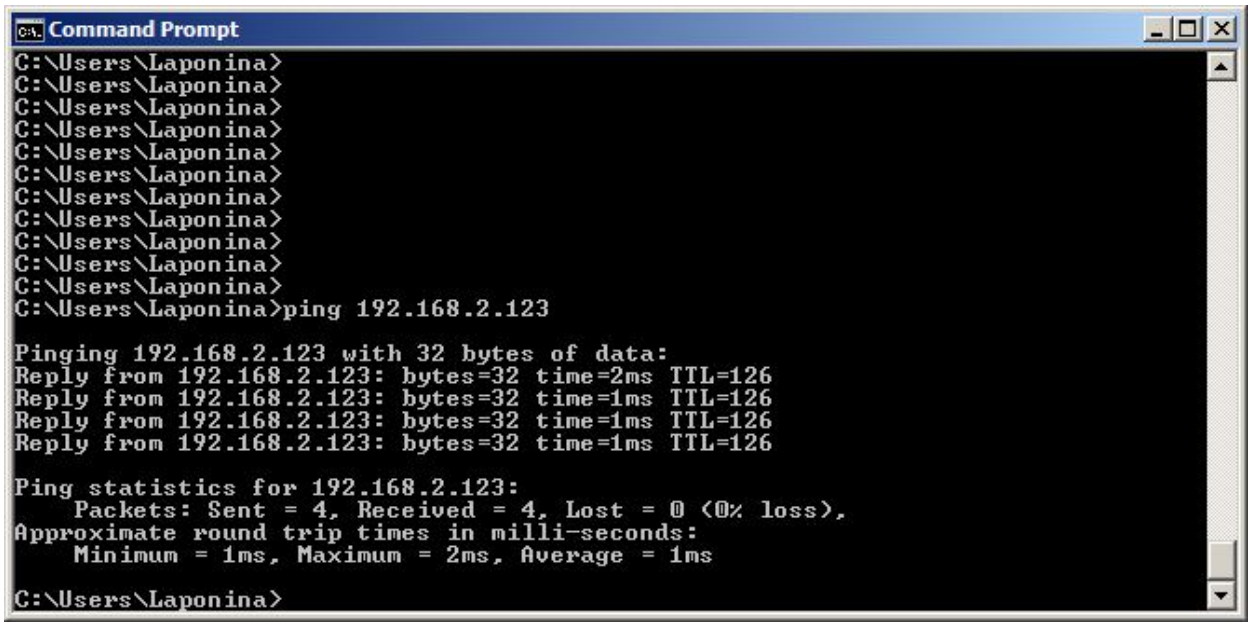
Межсетевой Экран 2

IPSec-Интерфейс

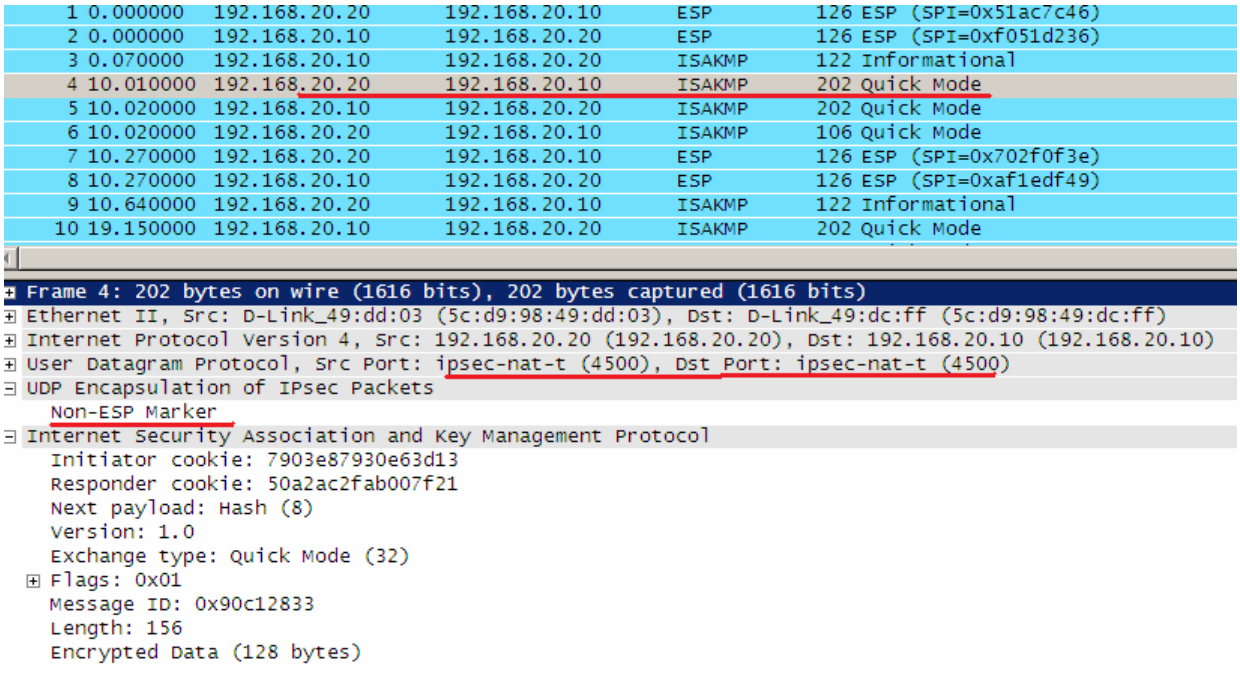
На IPSec-интерфейсе должна быть указана поддержка NAT. В этом случае инициатором установления туннеля всегда является хост, расположенный за NAT, поэтому для IPSec-интерфейса имеет смысл указать динамическое добавление маршрута.

Проверка конфигурации

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



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



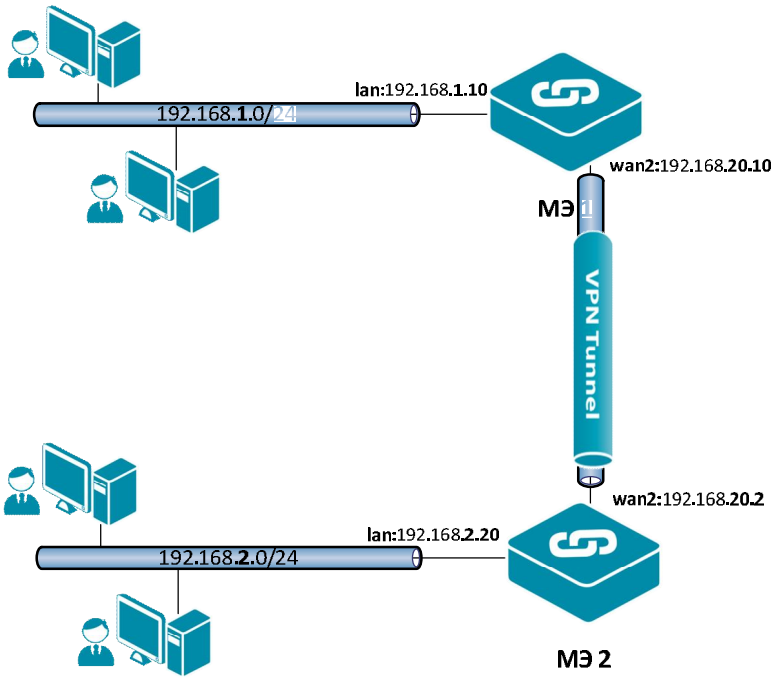
На lan-интерфейсе трафик с измененным IP-адресом:

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 1и МЭ 2 требуется поднять VPN/IPSec. Жизнеспособность противоположной стороны необходимо проверять по протоколу DPD.

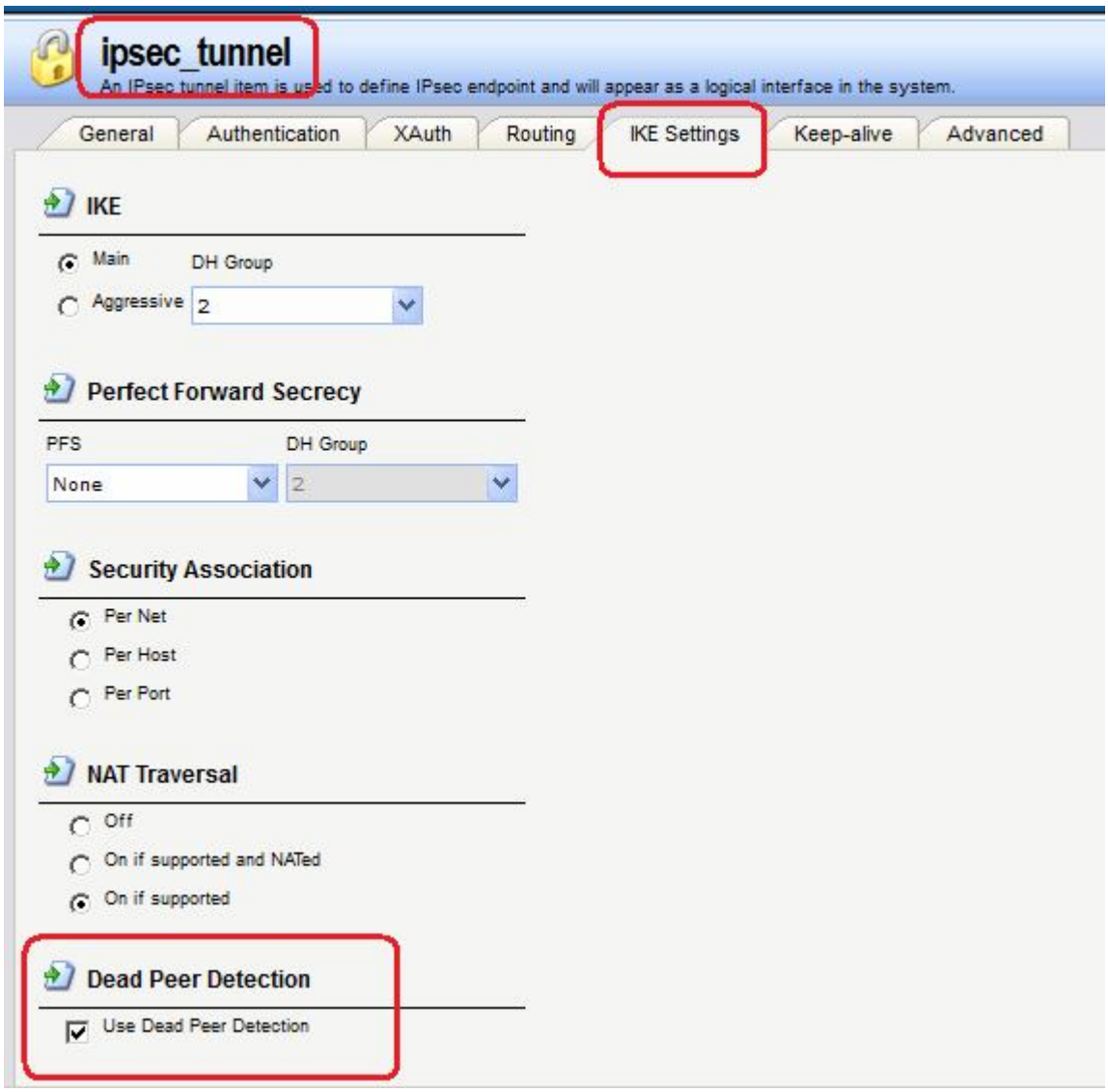
Описание практической работы

Межсетевой Экран 1

IPSec-Интерфейс
Установить использование протокола DPD.

Веб-интерфейс:

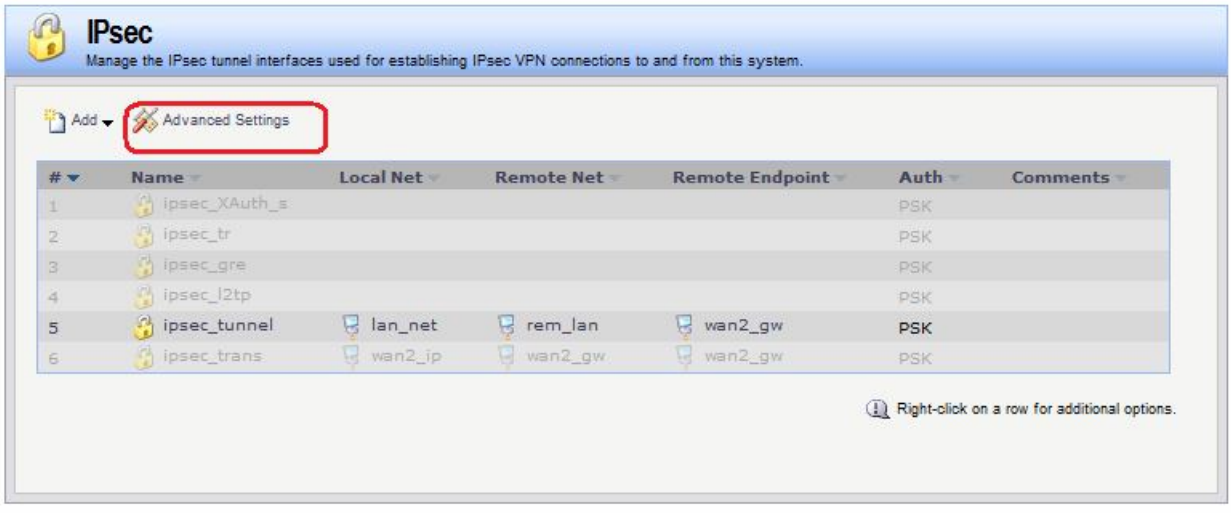
`Interfaces → IPsec → ipsec`

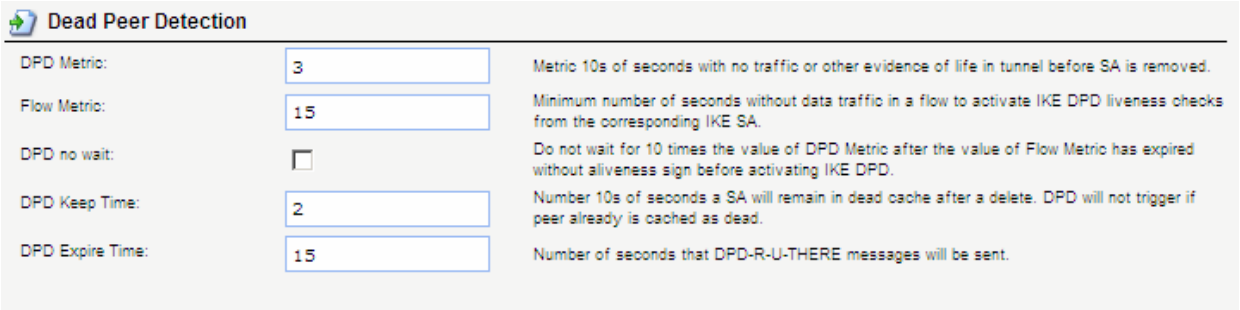


Командная строка:

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

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





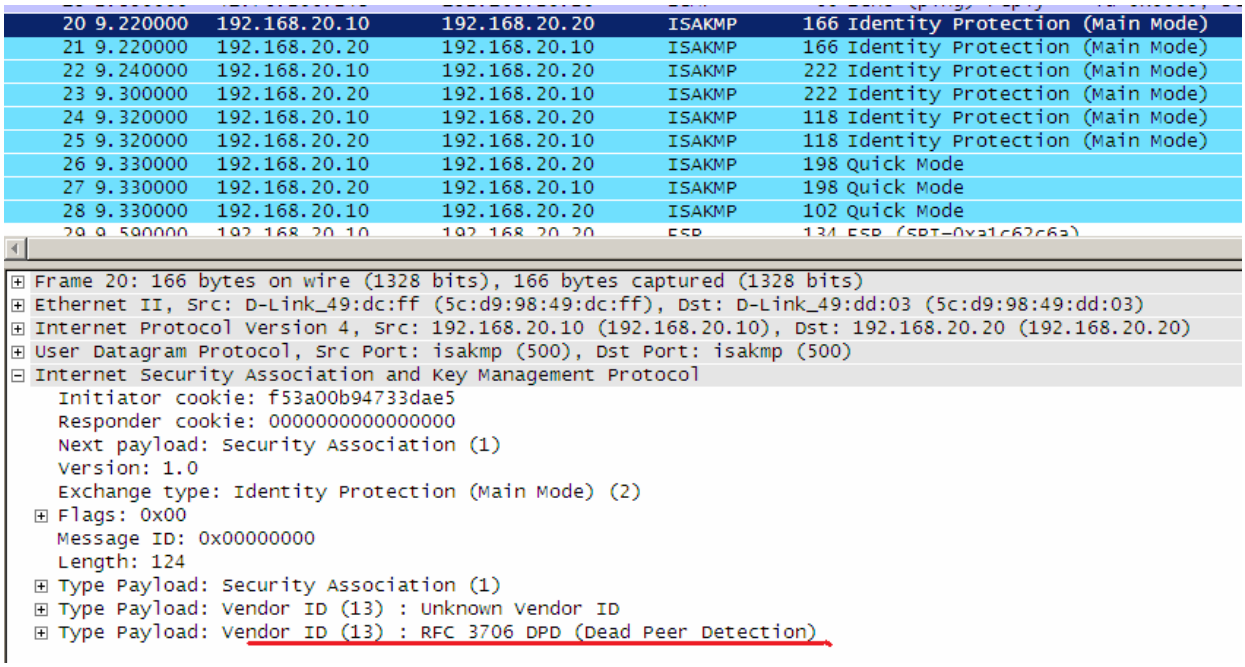
Межсетевой Экран 2

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.



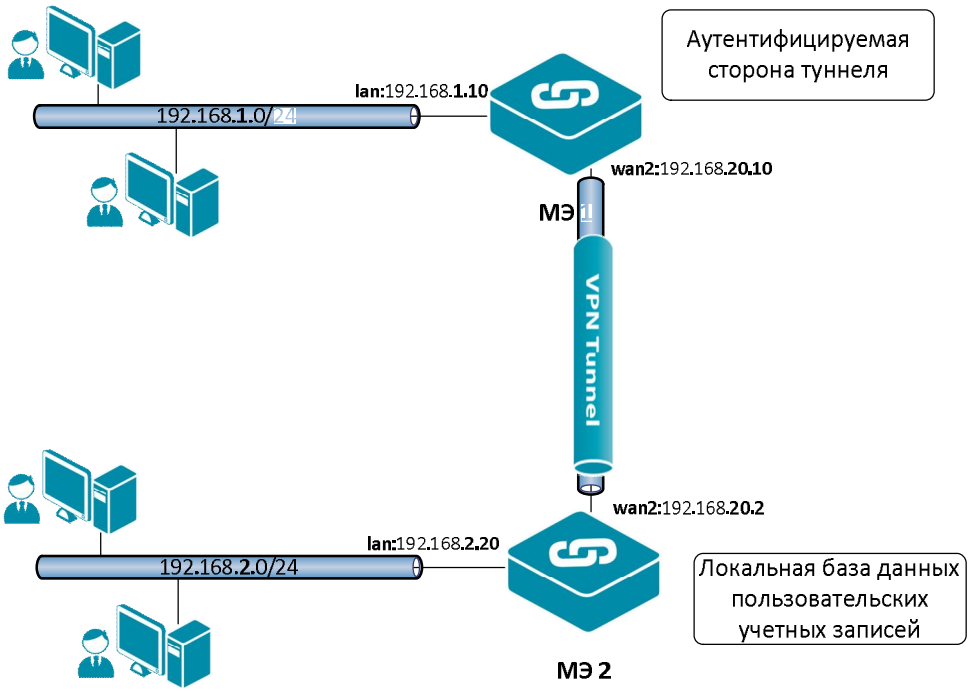
Лабораторная работа 7. Соединение двух локальных сетей протоколом L2TP, аутентификация с использованием общего секрета

Цель

Соединить два межсетевых экрана VPN с использованием протокола L2TP.

Топология сети аналогична топологии VPN/IPSec.

Топология сети



Между интерфейсами **`wan1`** на МЭ 1и 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

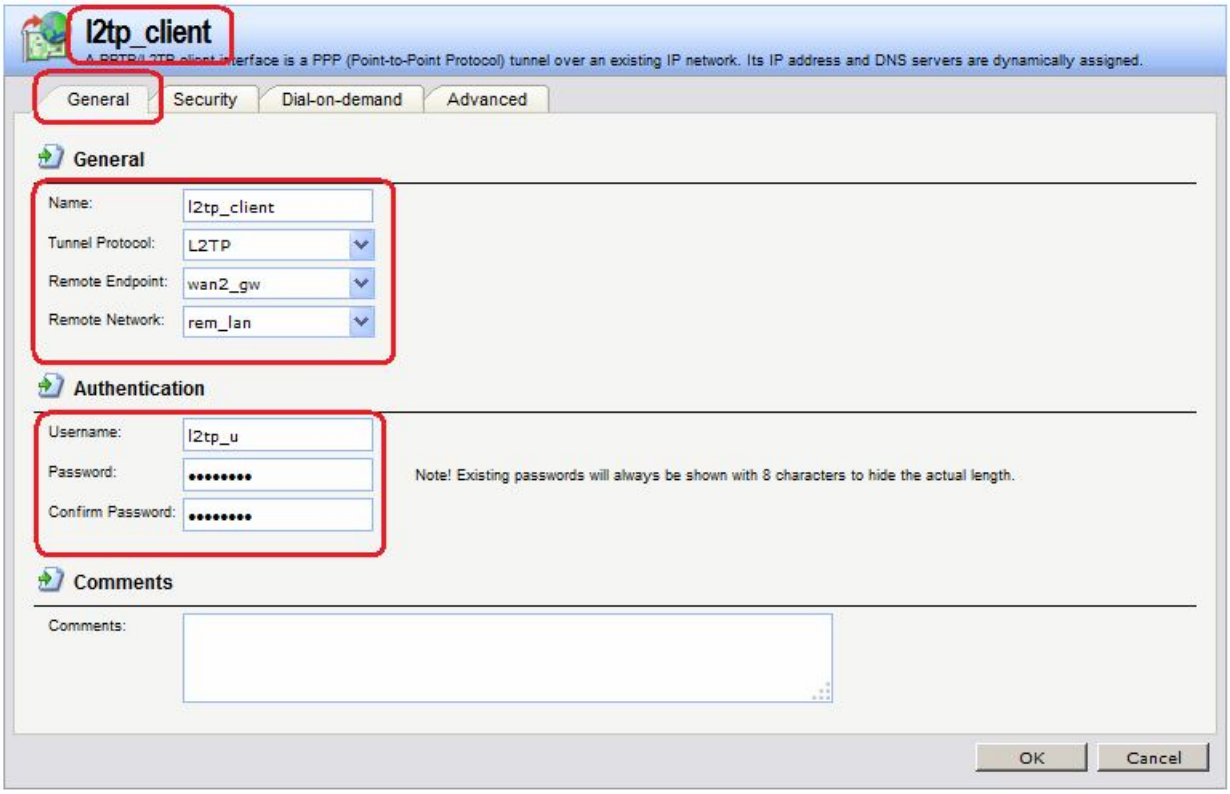
Межсетевой Экран 1 является клиентом, т.е. в его конфигурации следует указать имя пользователя и пароль.

L2TP-Интерфейс
Веб-интерфейс:

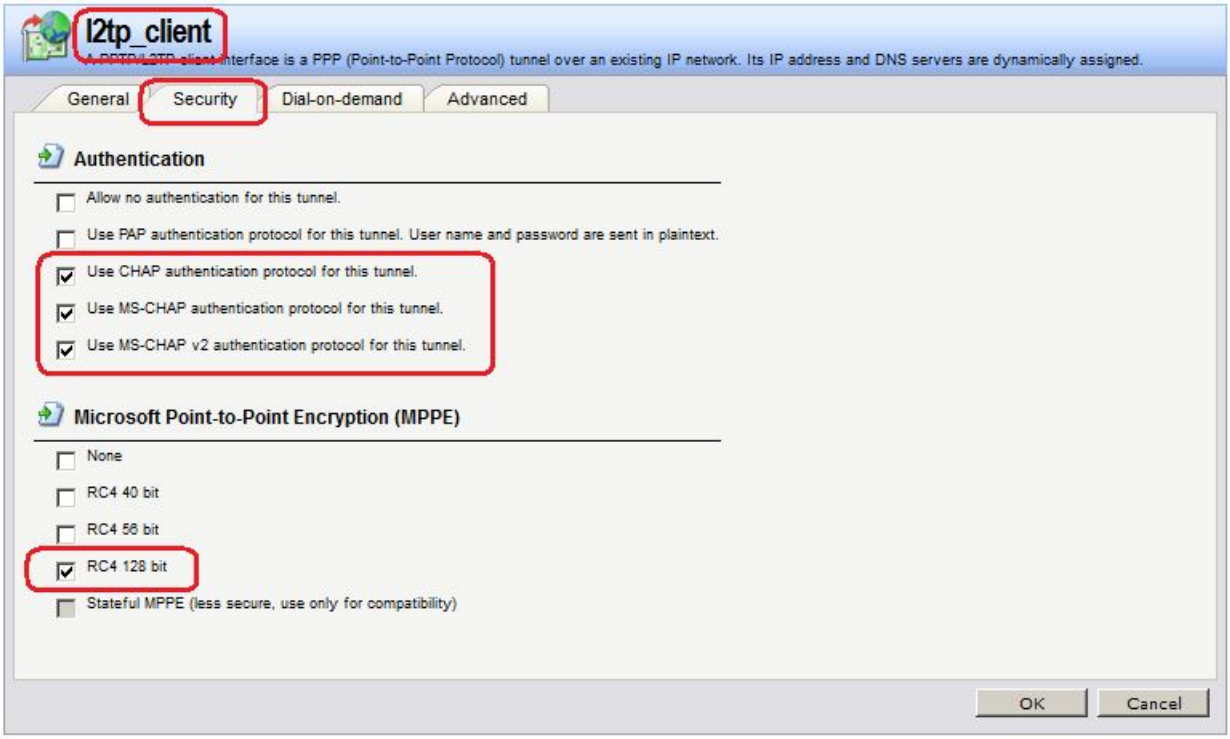
`Interfaces → PPTP/L2TP Clients → Add → PPTP/L2TP Client`

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

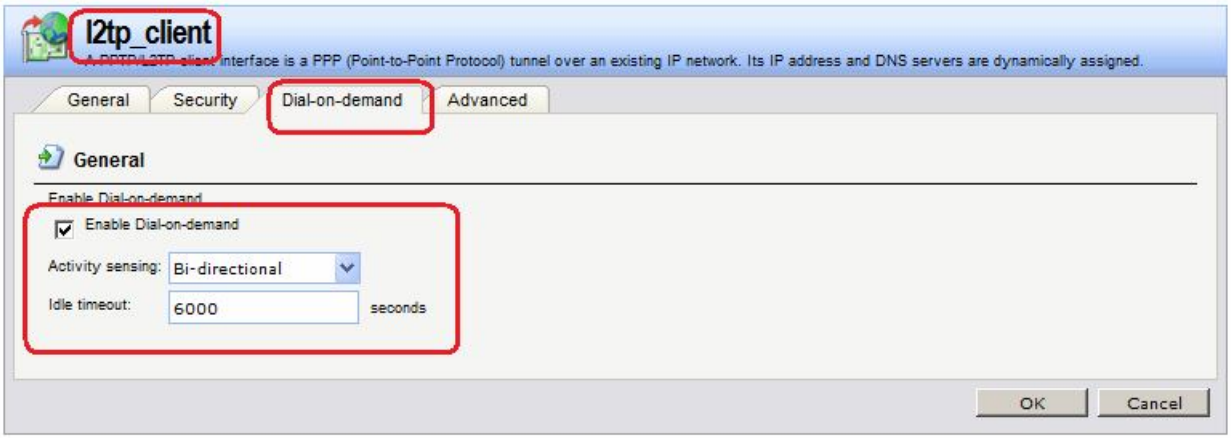
Также указать имя пользователя и пароль, созданные в базе данных на противоположной стороне туннеля.



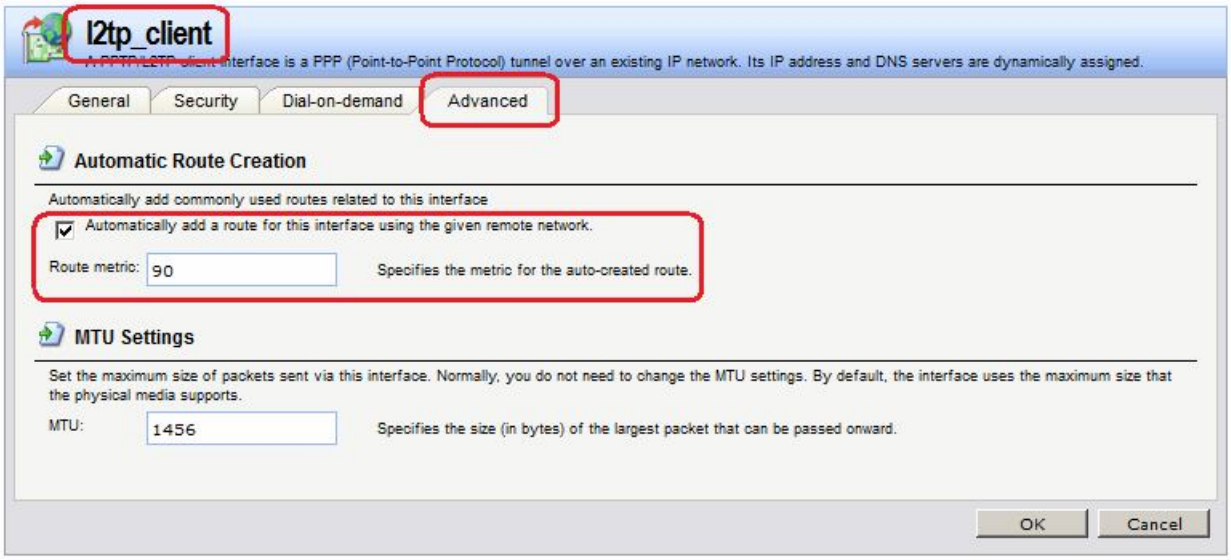
На вкладке **`Security`** указать параметры PPP-аутентификации и PPP-шифрования.



Если на вкладке **`Dial-on-demand`** установлен флаг **`Enable Dial-on-demand`**, то туннель будет устанавлен 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 фильтрования

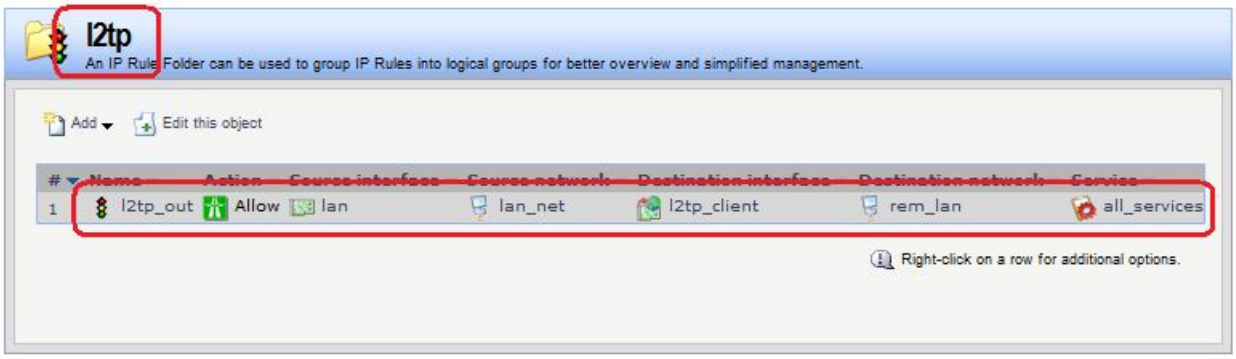
Разрешим трафик от сети, расположенной за межсетевым экраном, выполняющим роль L2TP-клиента, к сети, расположенной за межсетевым экраном, выполняющим роль L2TP-сервера.

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 фильтрования указывается правило **NAT**.

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

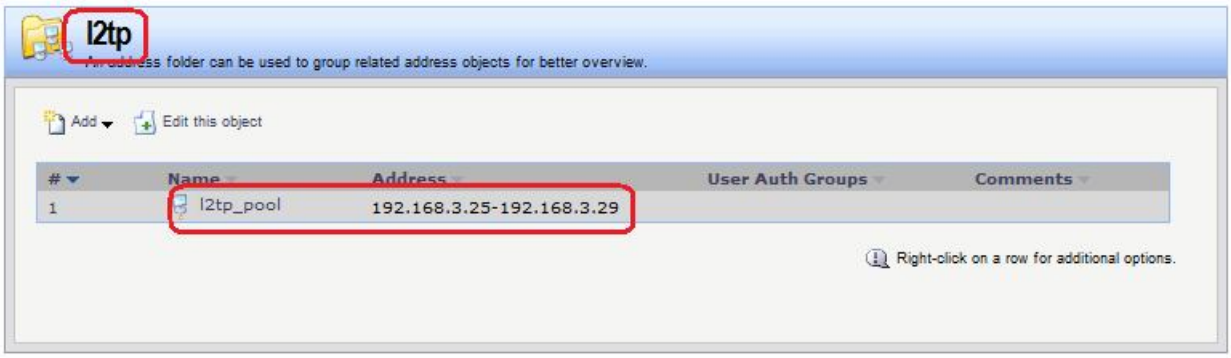
Межсетевой Экран 2

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
```



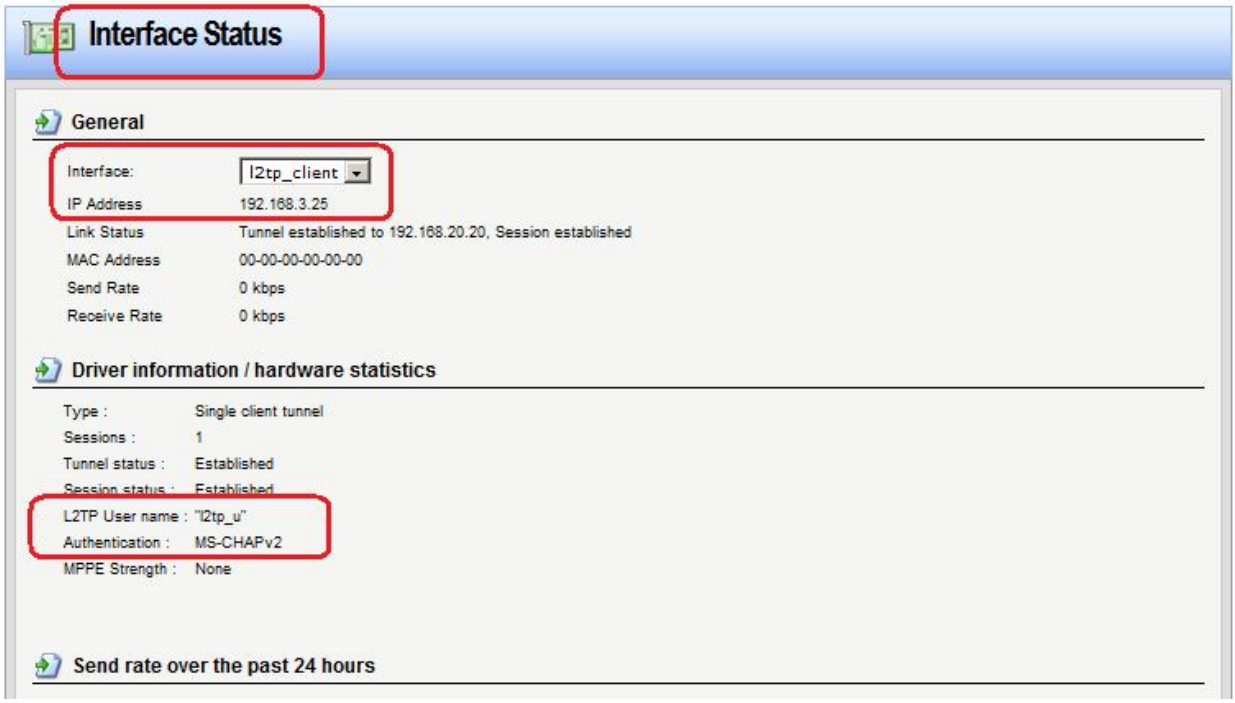
Командная строка:

```
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:

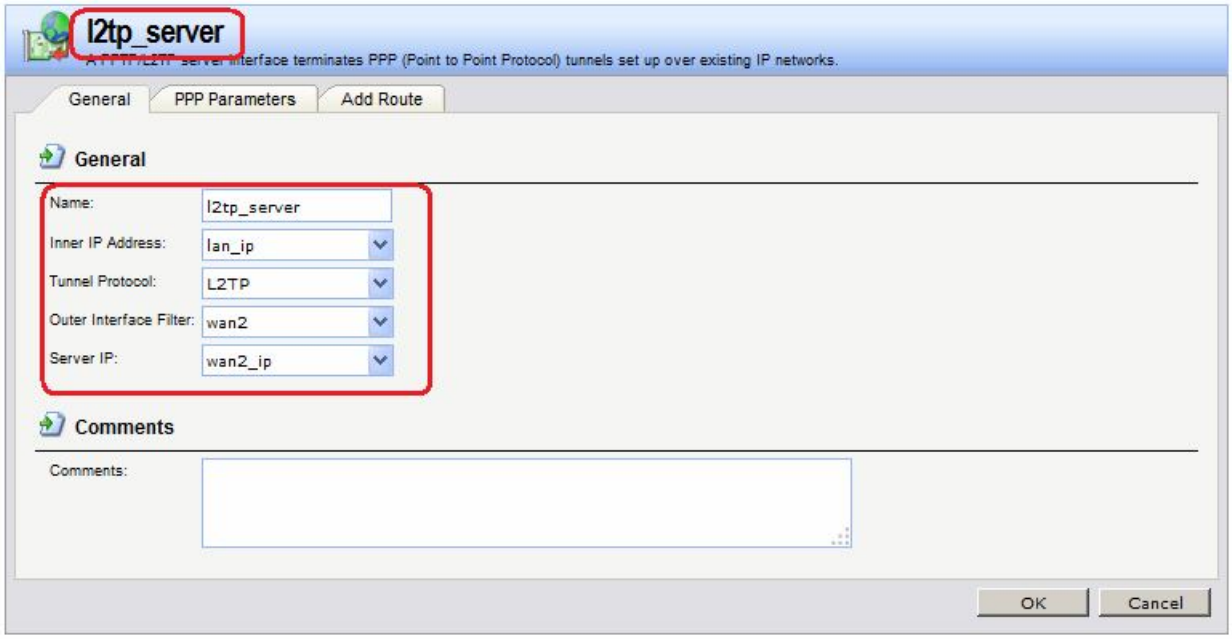


L2TP-Интерфейс

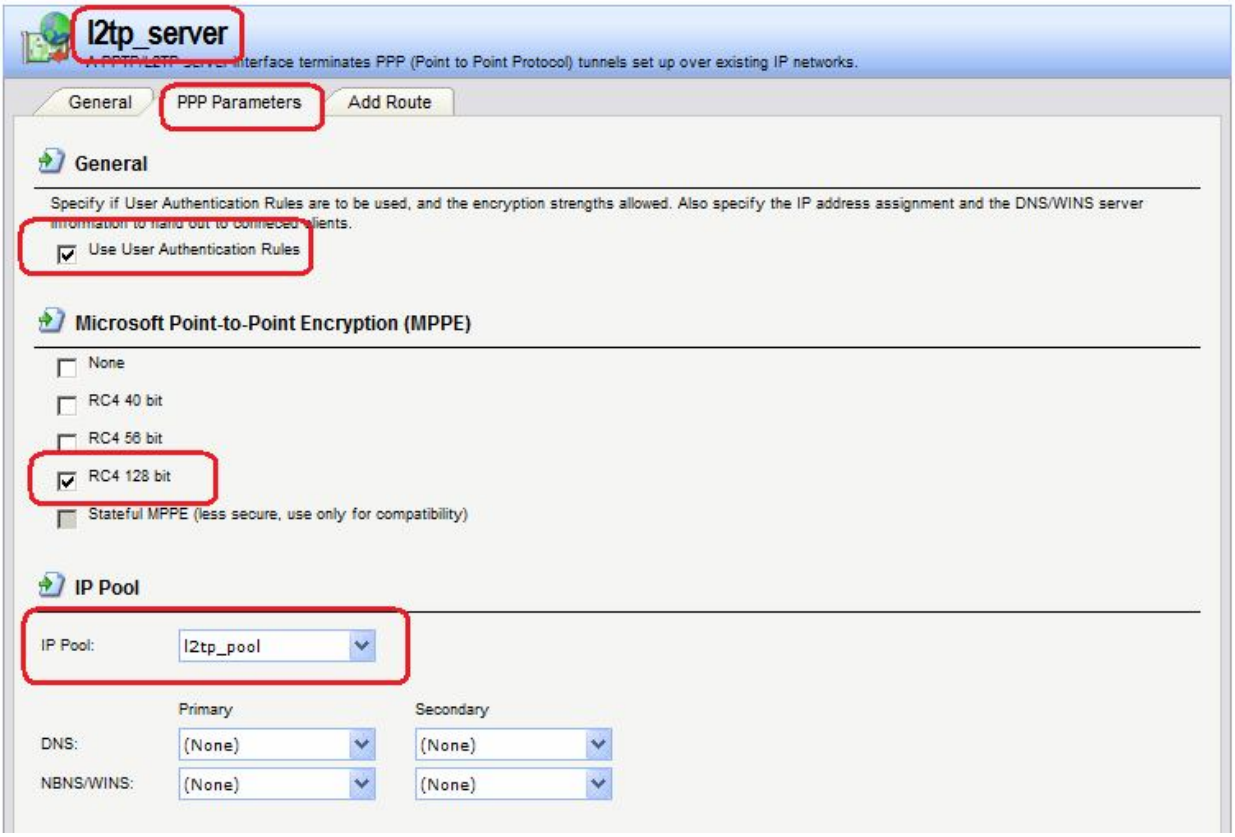
Веб-интерфейс:

`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
```

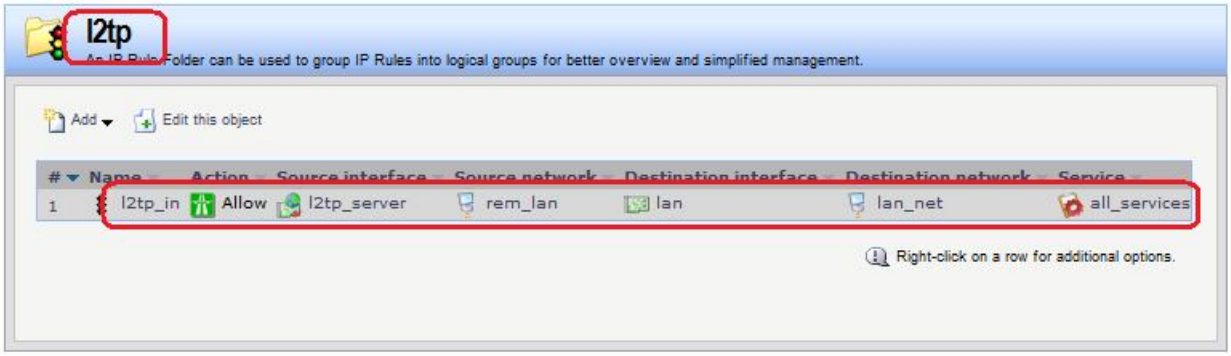
Правила фильтрования

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
```

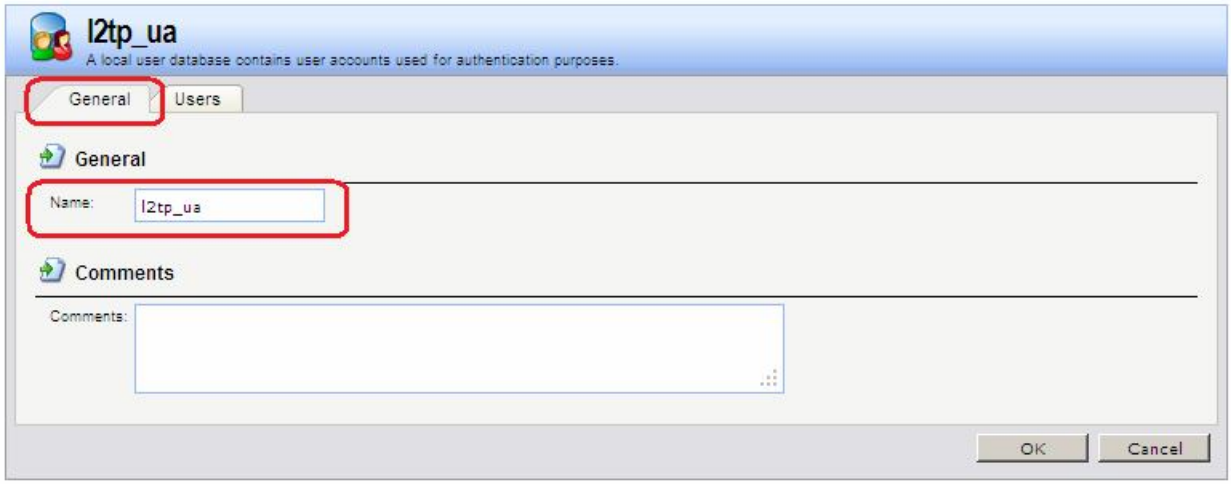
Если у удаленного пользователя IP-адрес назначался L2TP-Сервером, то в Правилах фильтрования следует указать вместо удаленной сети пул выделяемых IP-адресов.

Аутентификация на уровне пользователя
Создать локальную базу данных пользователей.

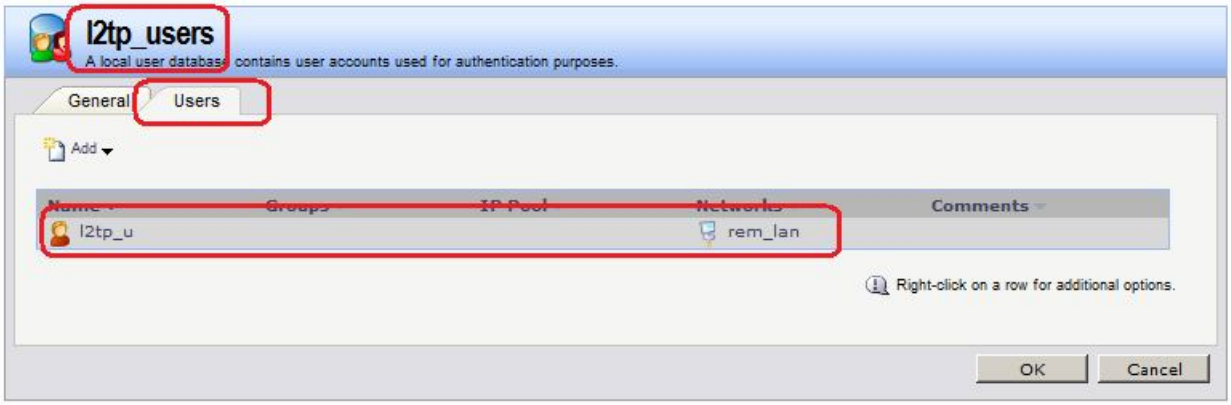
Веб-интерфейс:

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

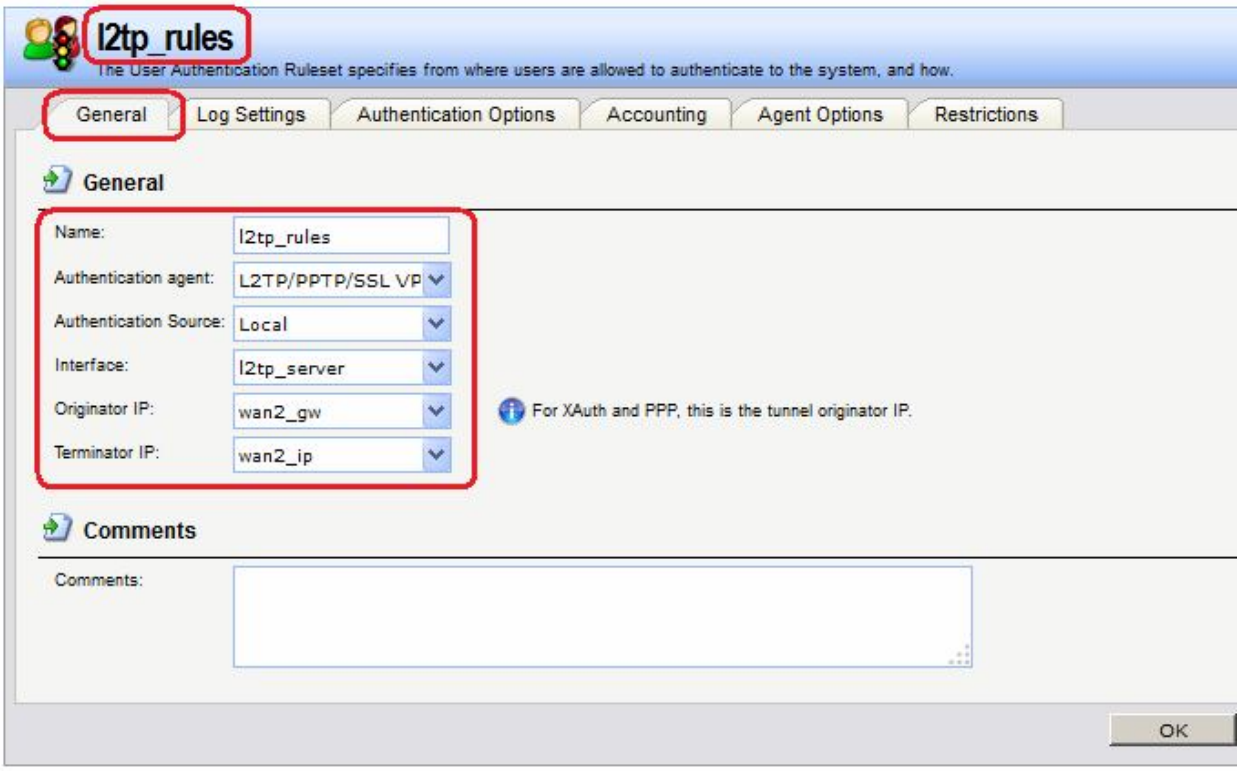
Создать правило аутентификации пользователей.

Веб-интерфейс:

`User Authentication → User Authentication Rules → Add`

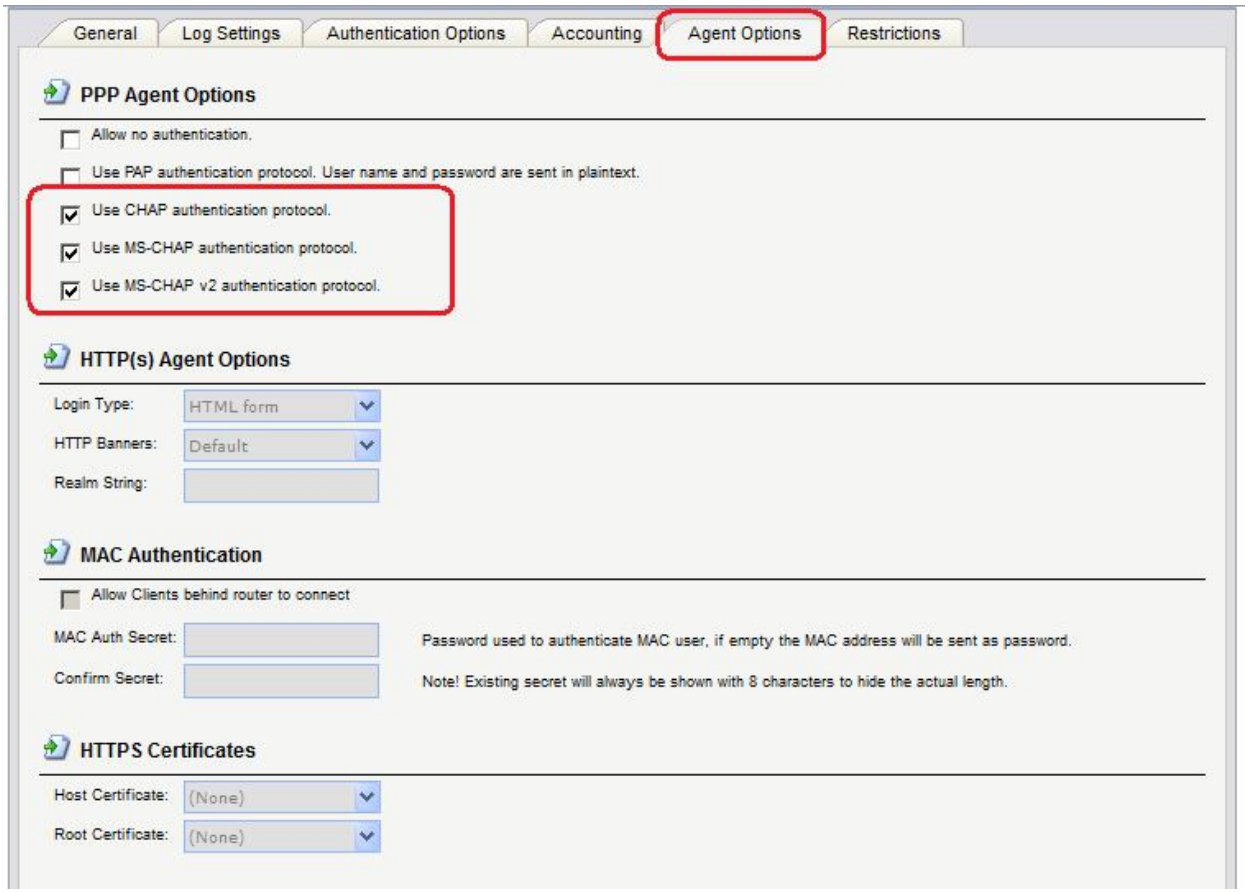
`Name: l2tp_rules`

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



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

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

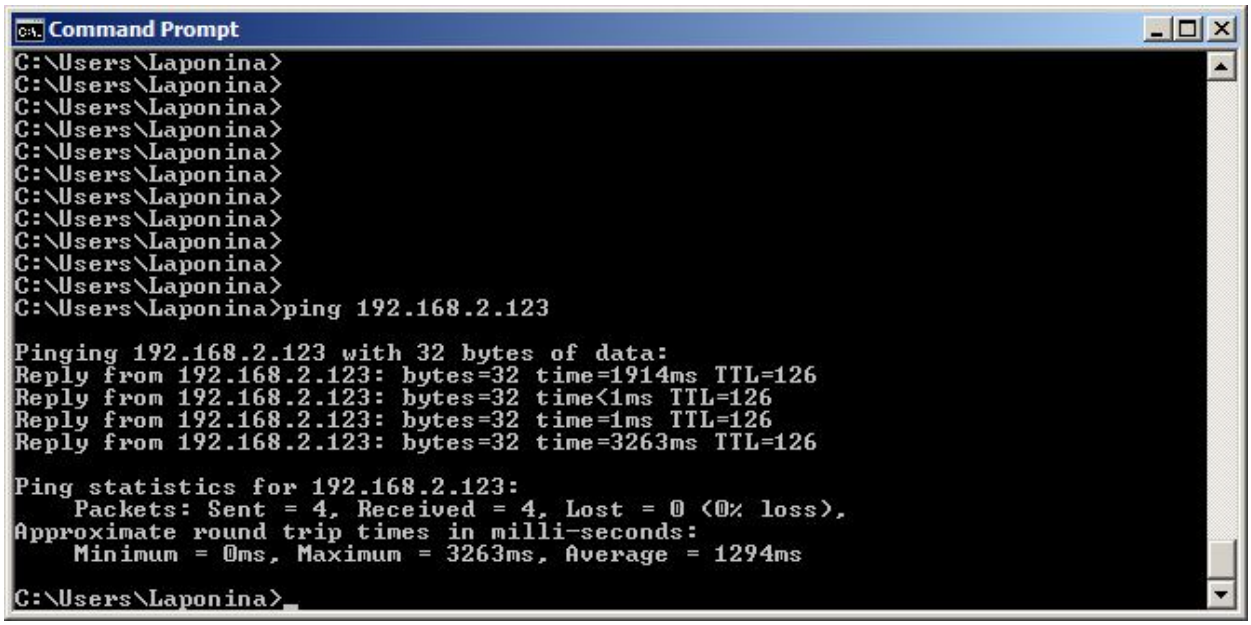


Командная строка:

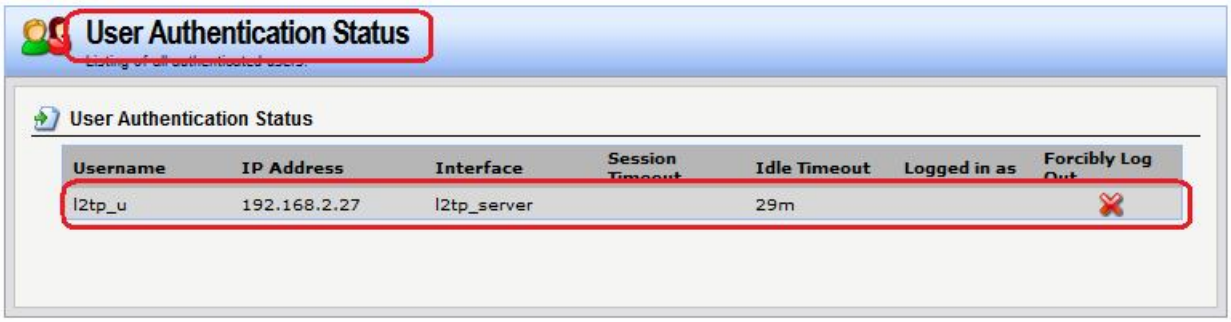
```
add UserAuthRule AuthSource=Local Interface=l2tp_server LocalUserDB=l2tp_ua
OriginatorIP=wan2/wan2_gw Agent=PPP TerminatorIP=wan2/wan2_ip Name=l2tp_rules
```

Проверка конфигурации

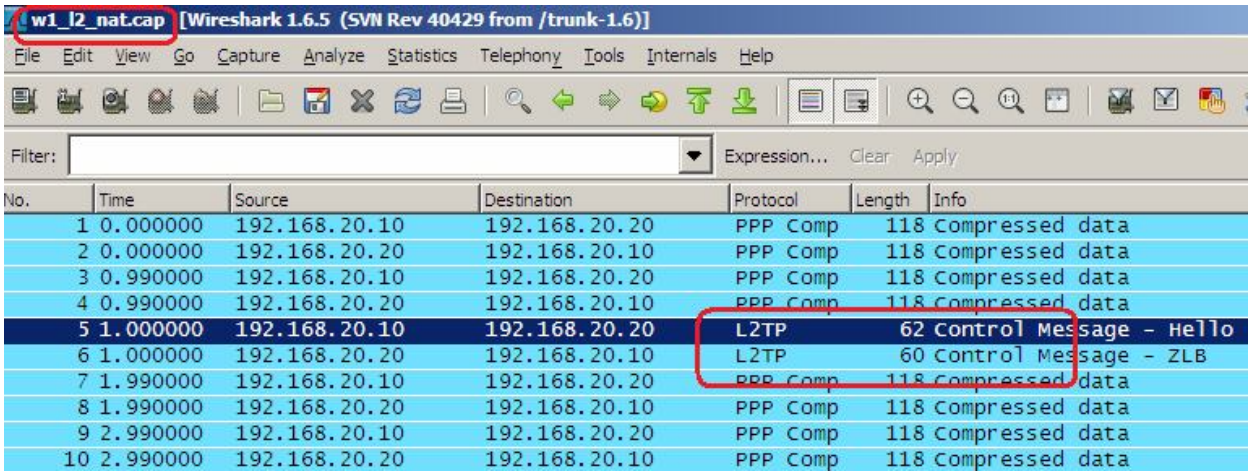
Выполнить команду **ping**.



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



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



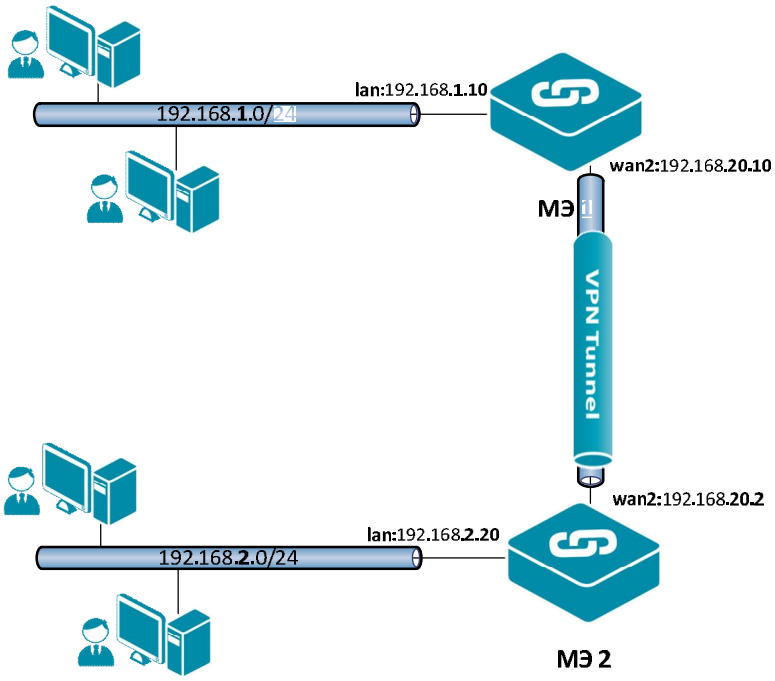
Лабораторная работа 8. Соединение двух локальных сетей протоколом GRE/IPSec в транспортном режиме

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

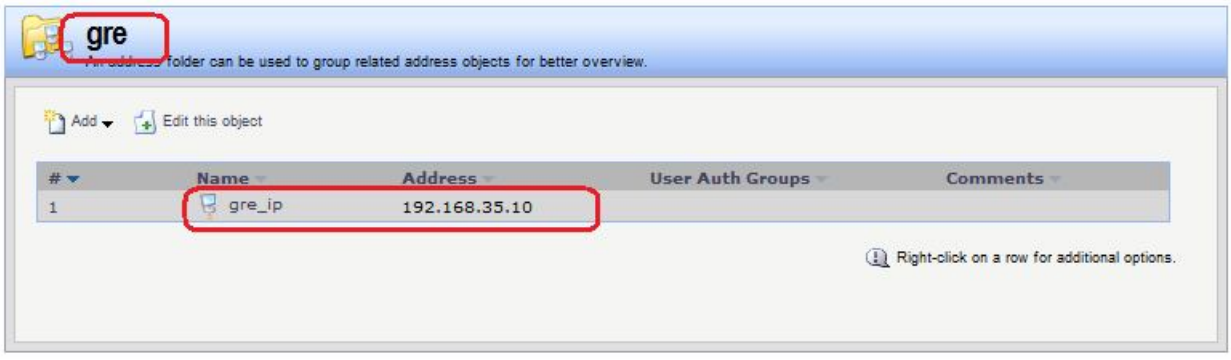
Аутентификационный Объект
Используем аутентификационный объект **`Pre-Shared Key`**, созданный в Лабораторной работе 9.

Объекты Адресной Книги
Веб-интерфейс:

`Object → Address Book → Add → Address Folder`

`Name: gre`

`Object → Address Book → gre → Add`



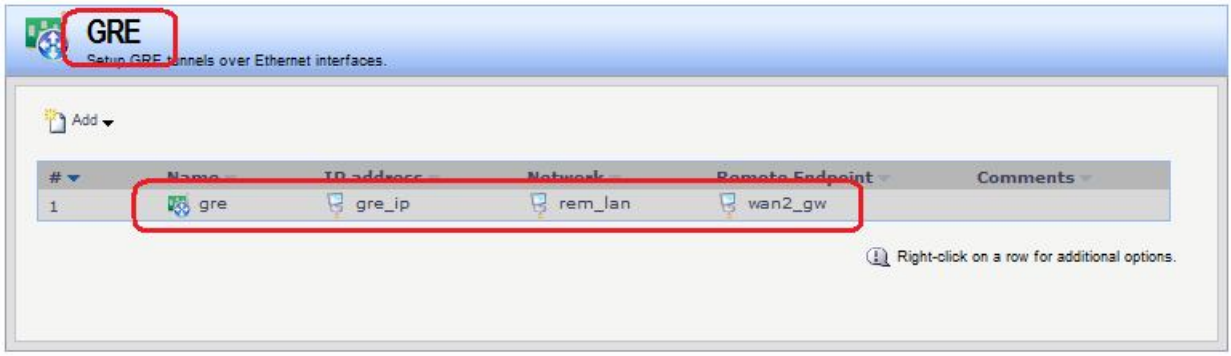
Командная строка:

```
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.

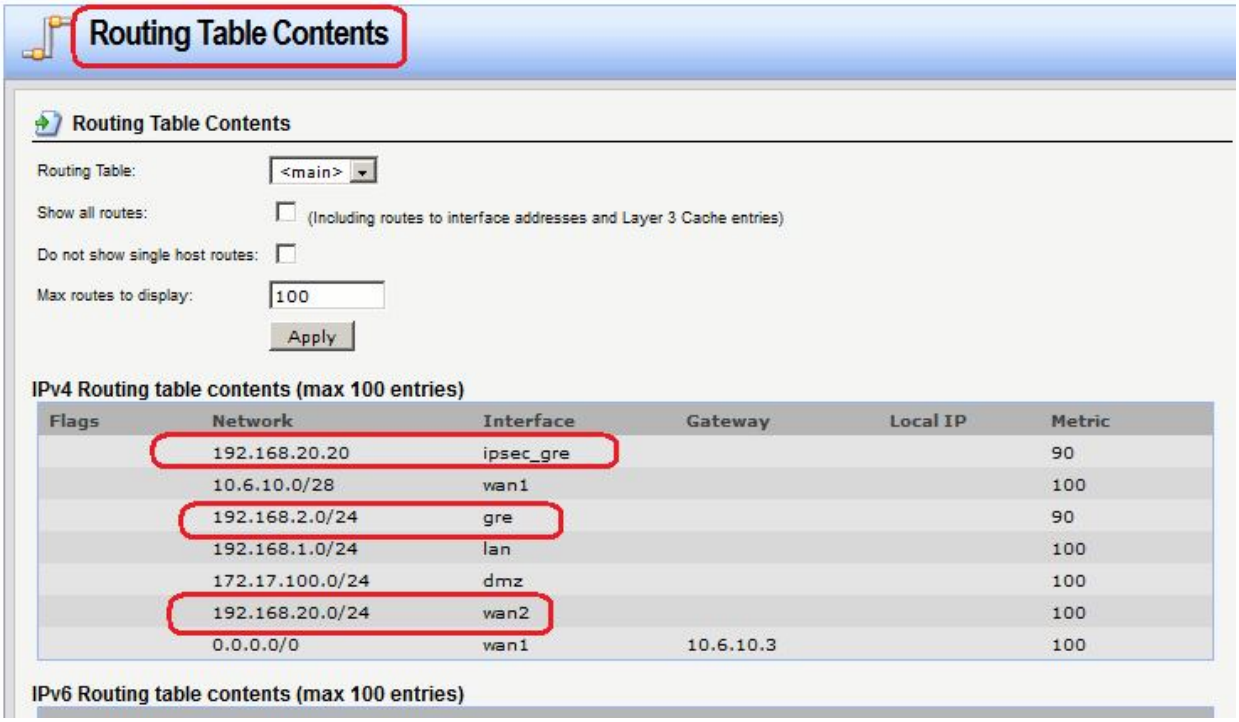
На вкладке **`Authentication`** указать созданный аутентификационный объект.

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**.



Правила фильтрования

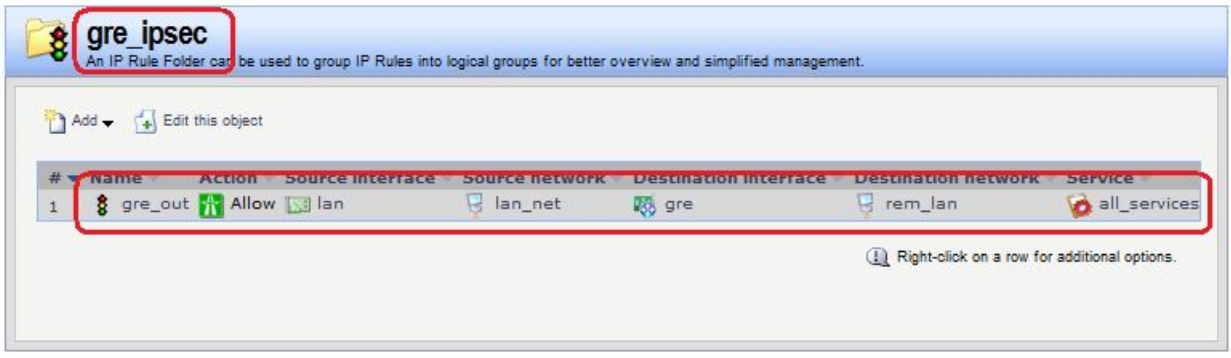
Правила фильтрования достаточно задать для GRE-интерфейса.

Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: gre_ipsec

Rules → IP Rules → gre → Add



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

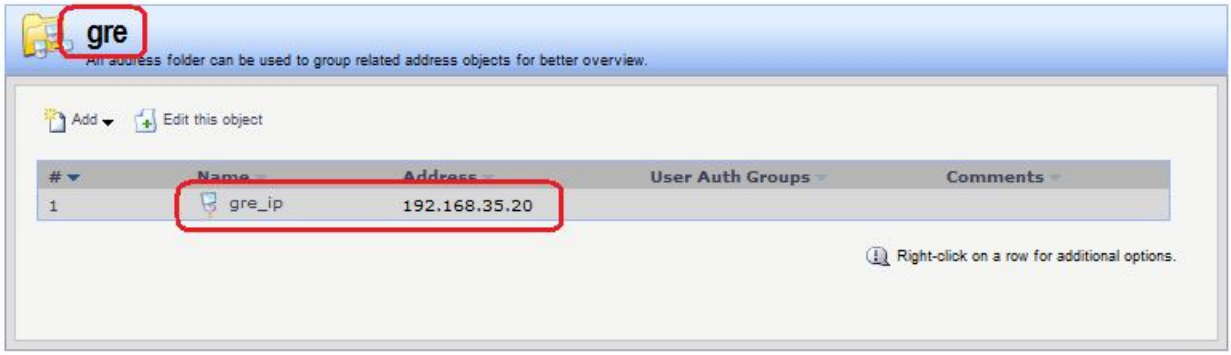
Аутентификационный Объект
Используем аутентификационный объект **`Pre-Shared Key`**, созданный в Лабораторной работе 9.

Объекты Адресной Книги
Веб-интерфейс:

`Object → Address Book → Add → Address Folder`

`Name: gre`

`Object → Address Book → gre → Add`



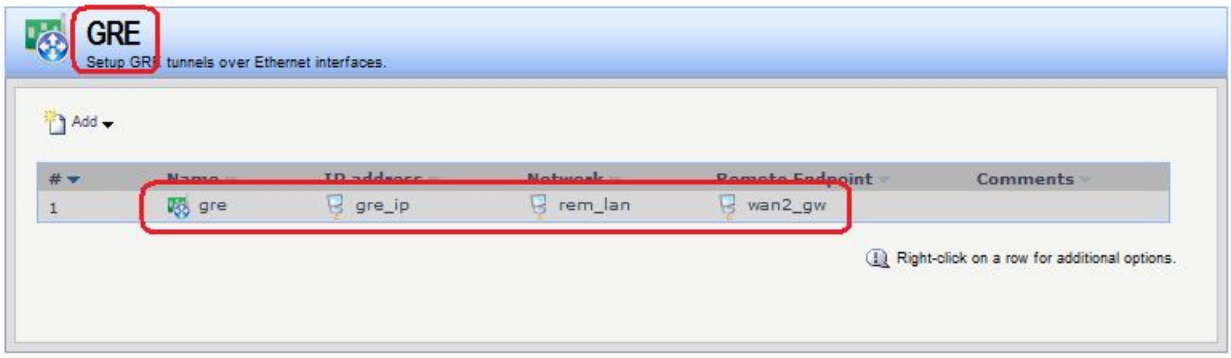
Командная строка:

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

GRE- 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.

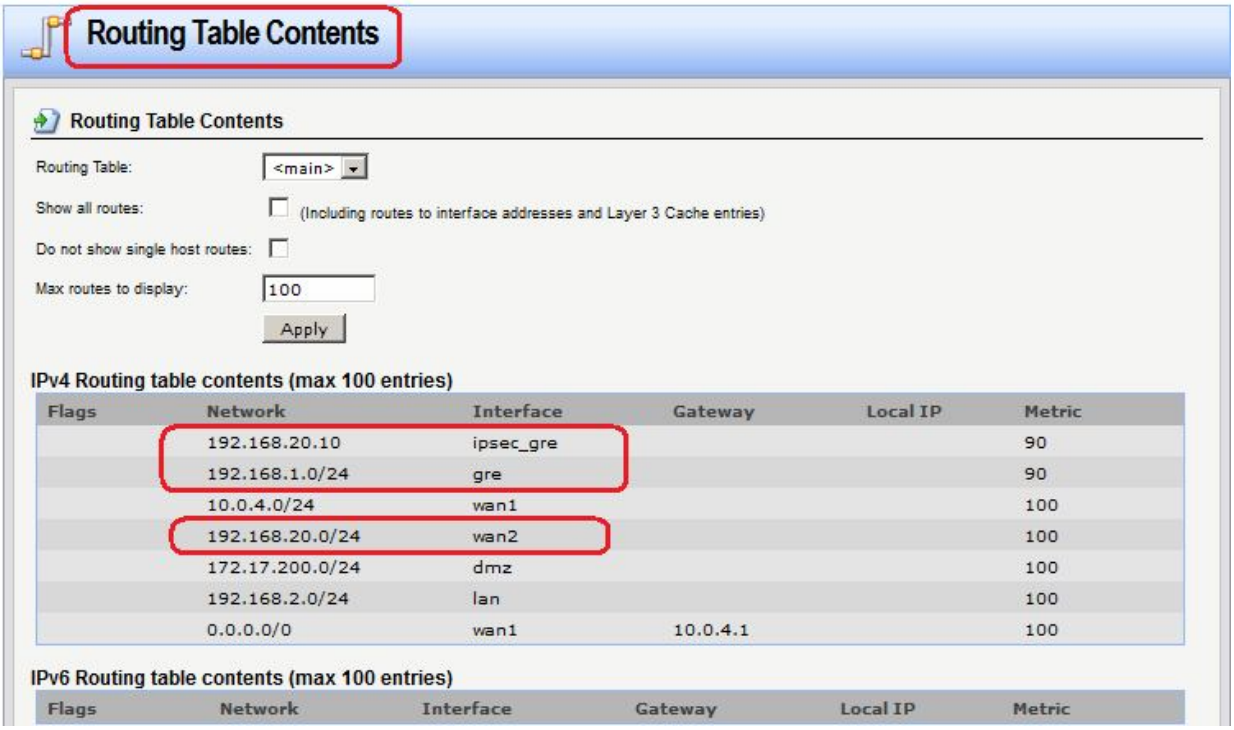
На вкладке **Authentication** указать созданный аутентификационный объект.

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 фильтрования
Правила фильтрования достаточно задать для GRE-интерфейса.

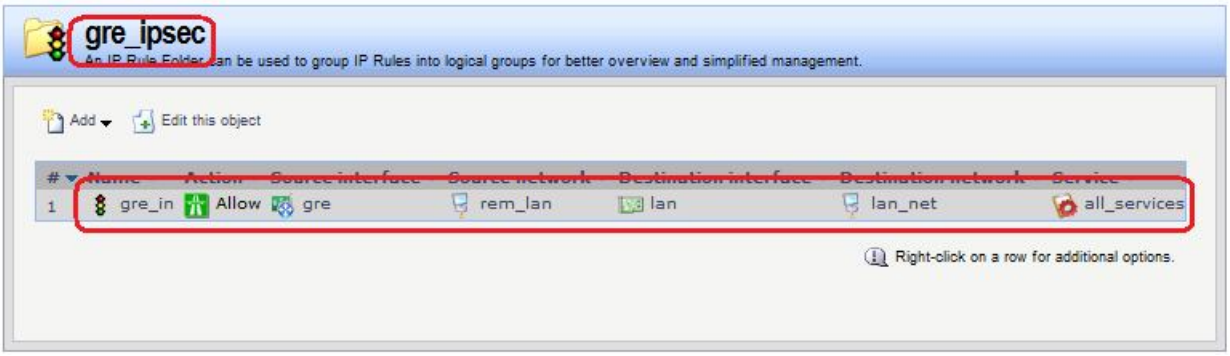
Веб-интерфейс:

Веб-интерфейс:

`Rules → IP Rules → Add → IP Rule Folder`

`Name: gre_ipsec`

`Rules → IP Rules → gre_ipsec → Add`



Командная строка:

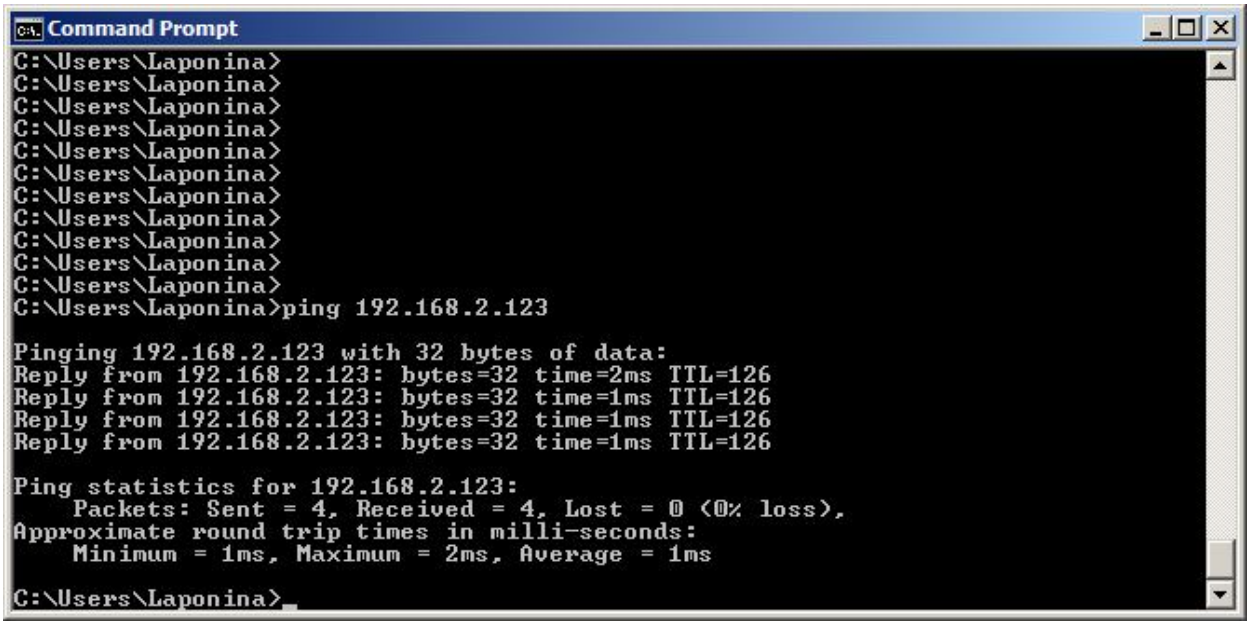
```
add IPRuleFolder Name=gre_ipsec
```

```
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
```

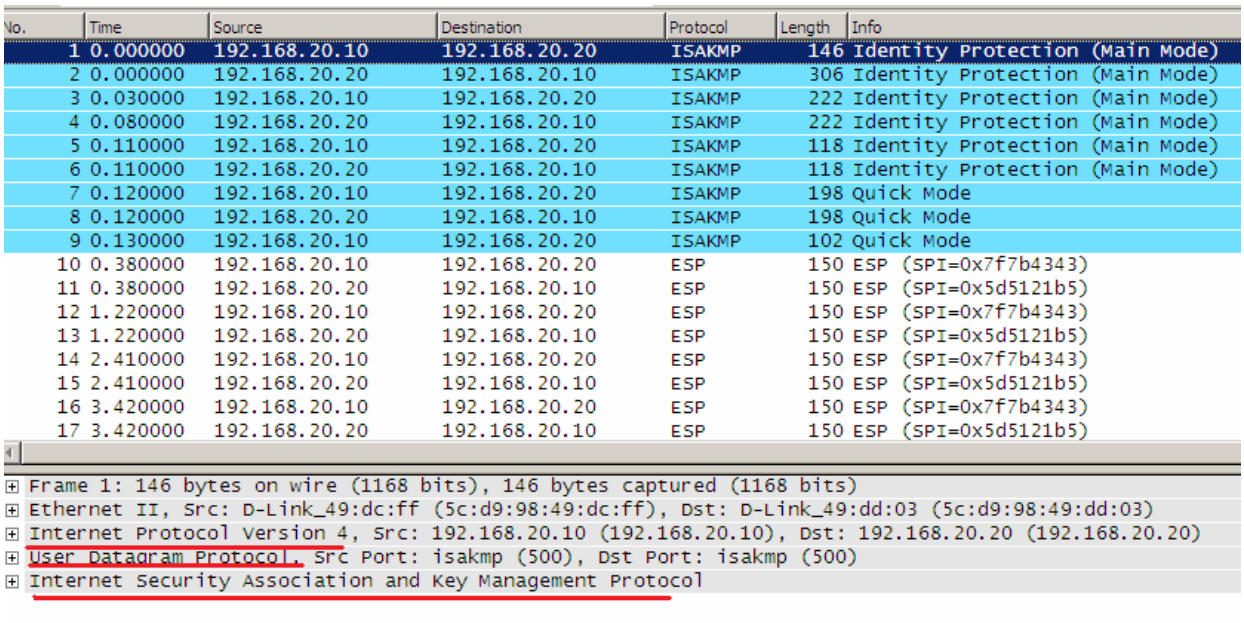
Проверка конфигурации

На Сервере 1 выполним команду **`ping`**.



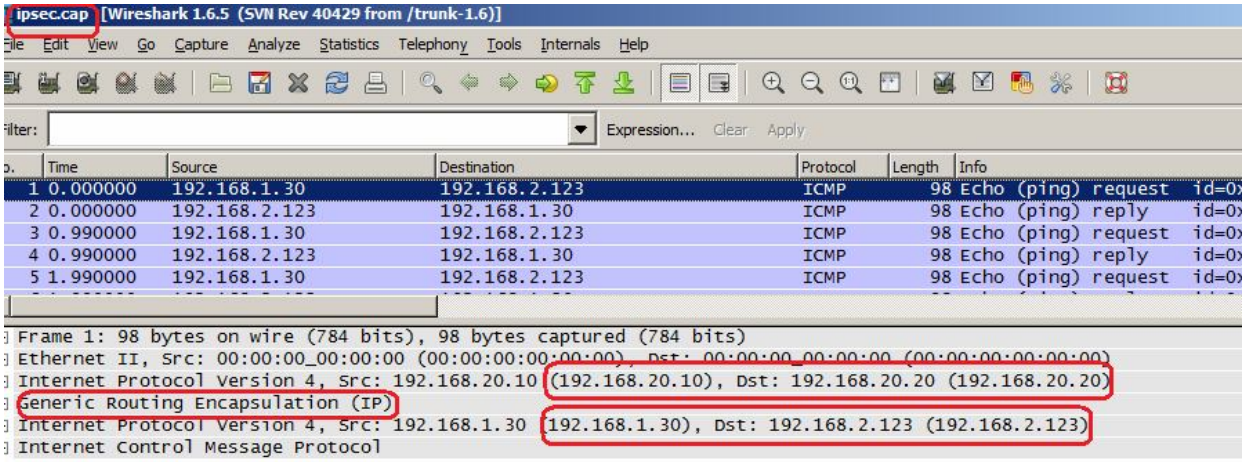
Получим дамп трафика аналогично тому, как это делалось в предыдущих лабораторных работах.

На интерфейсе **`wan1`** видим следующий трафик:



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

На интерфейсе **`ipsec`** видим следующий трафик:



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

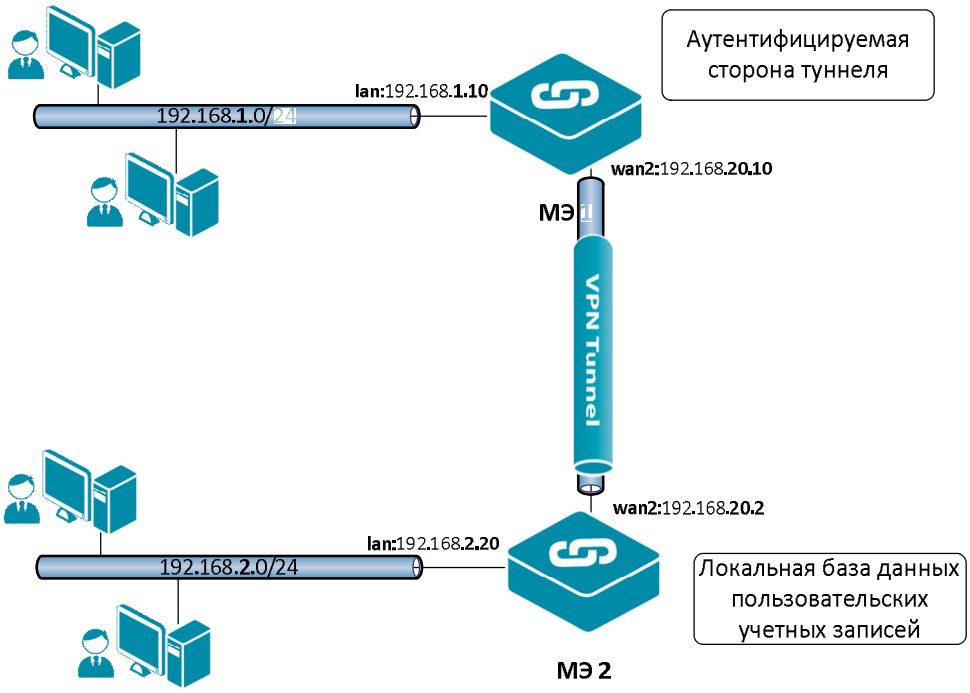
Лабораторная работа 9. Соединение двух локальных сетей протоколом L2TP/IPSec в транспортном режиме

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.

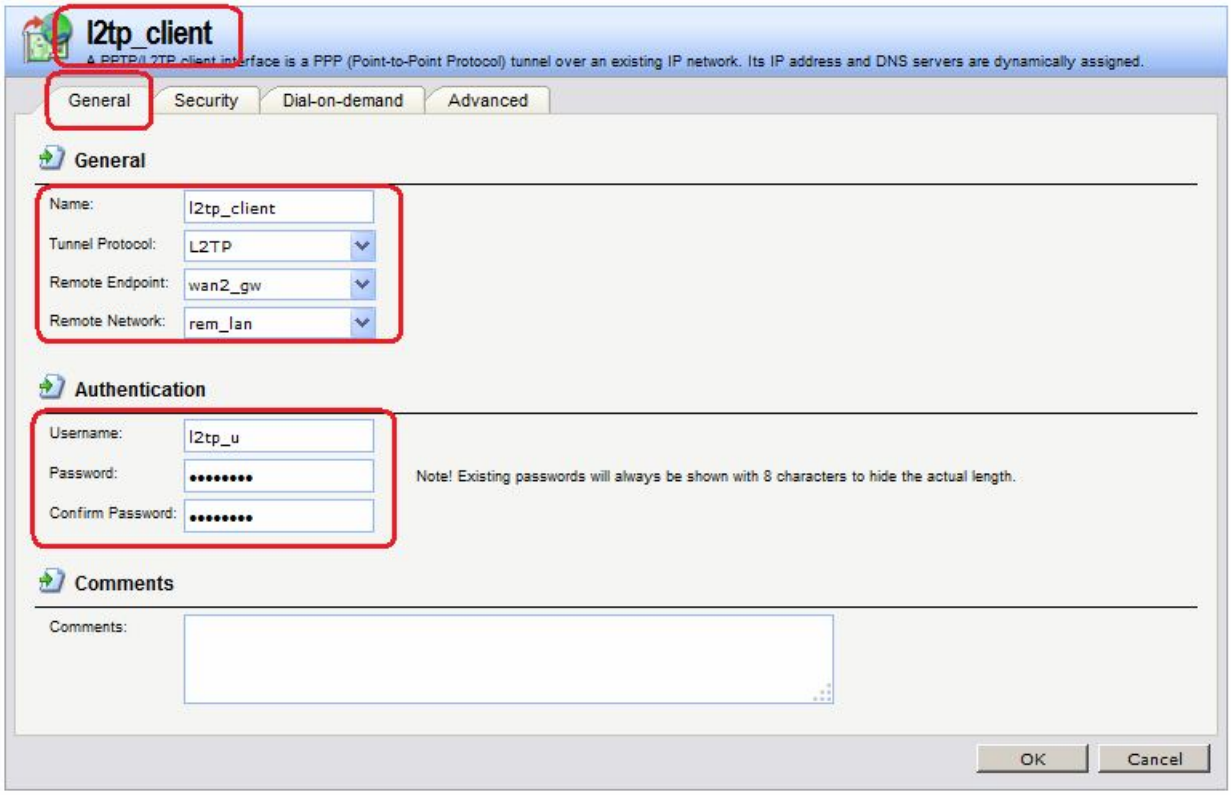
L2TP- и IPSec-Интерфейсы
Создать L2TP-интерфейс аутентифицируемой стороны туннеля.

Веб-интерфейс:

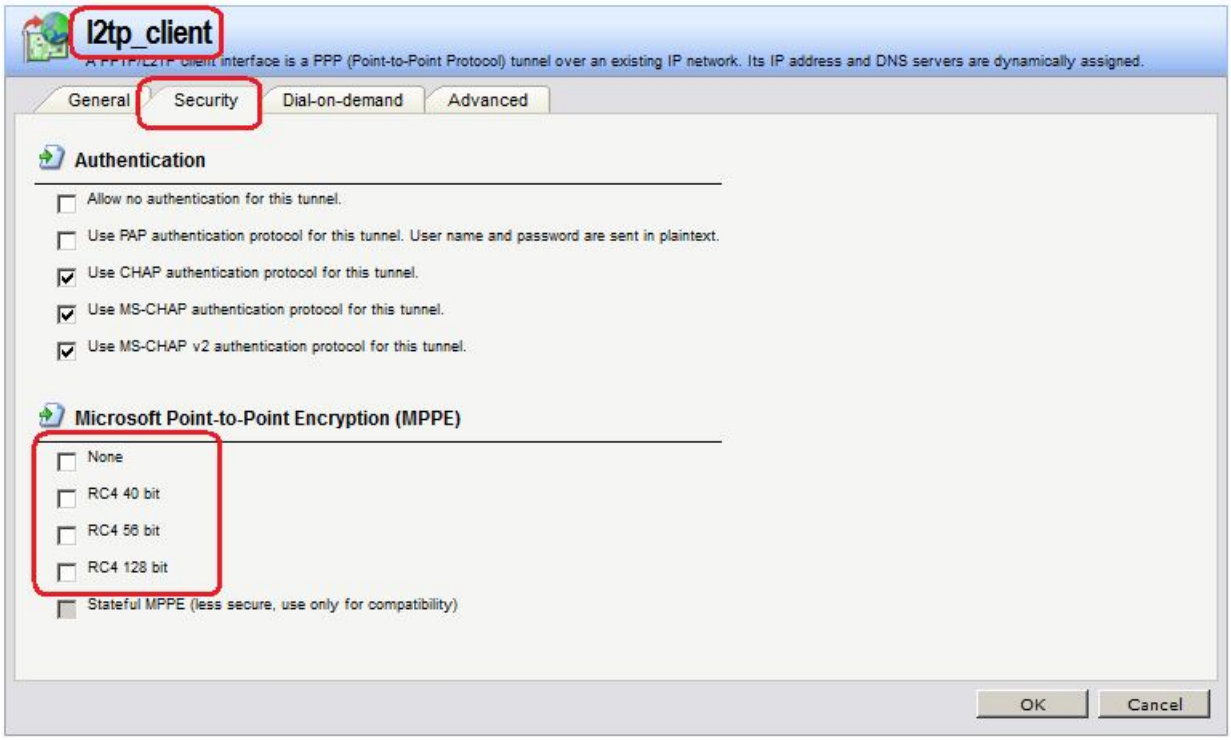
`Interfaces → PPTP/L2TP Clients → Add → PPTP/L2TP Client`

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:

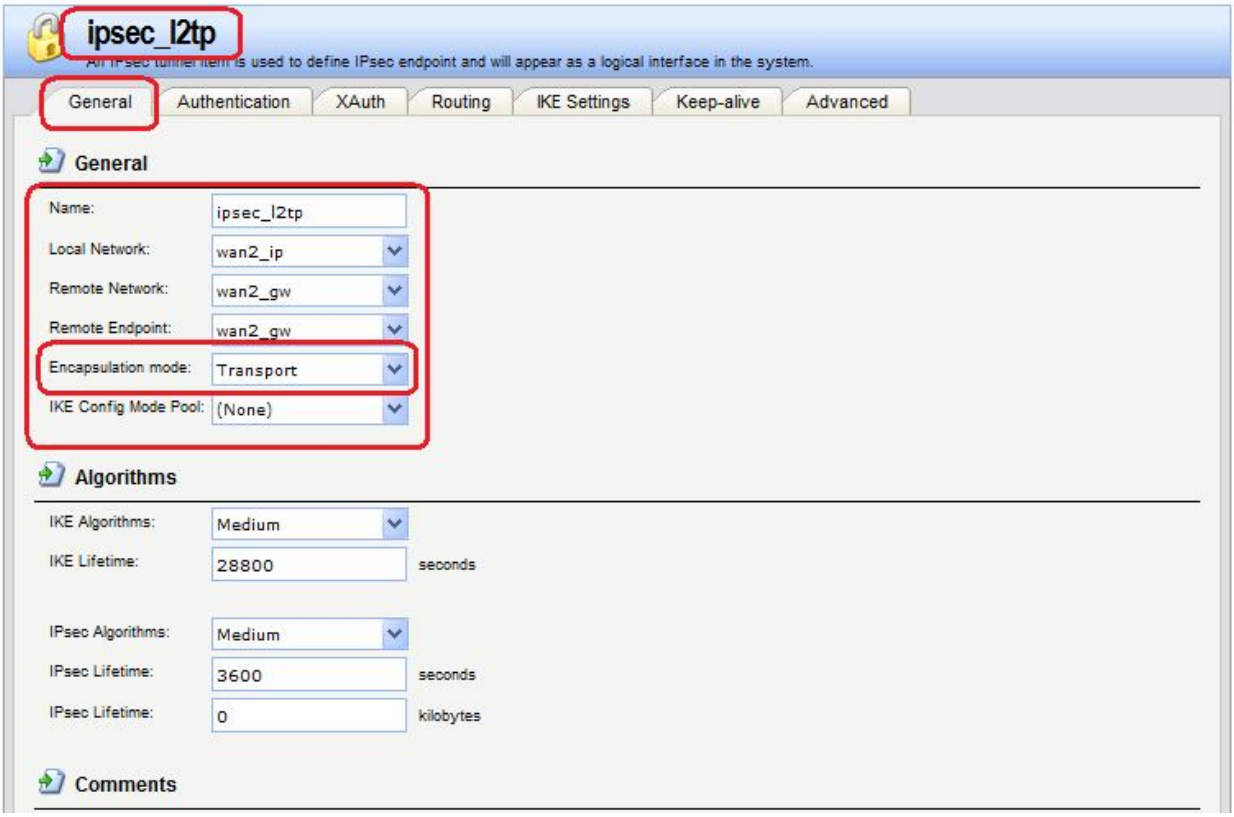
```
add Interface L2TPClient l2tp_client Network=remote/rem_lan
RemoteEndpoint=wan2/wan2_gw Username=l2tp_u Password=qwerty
TunnelProtocol=L2TP MPPENone=No MPPERC4128=No MPPERC440=No MPPERC456=No
```

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.



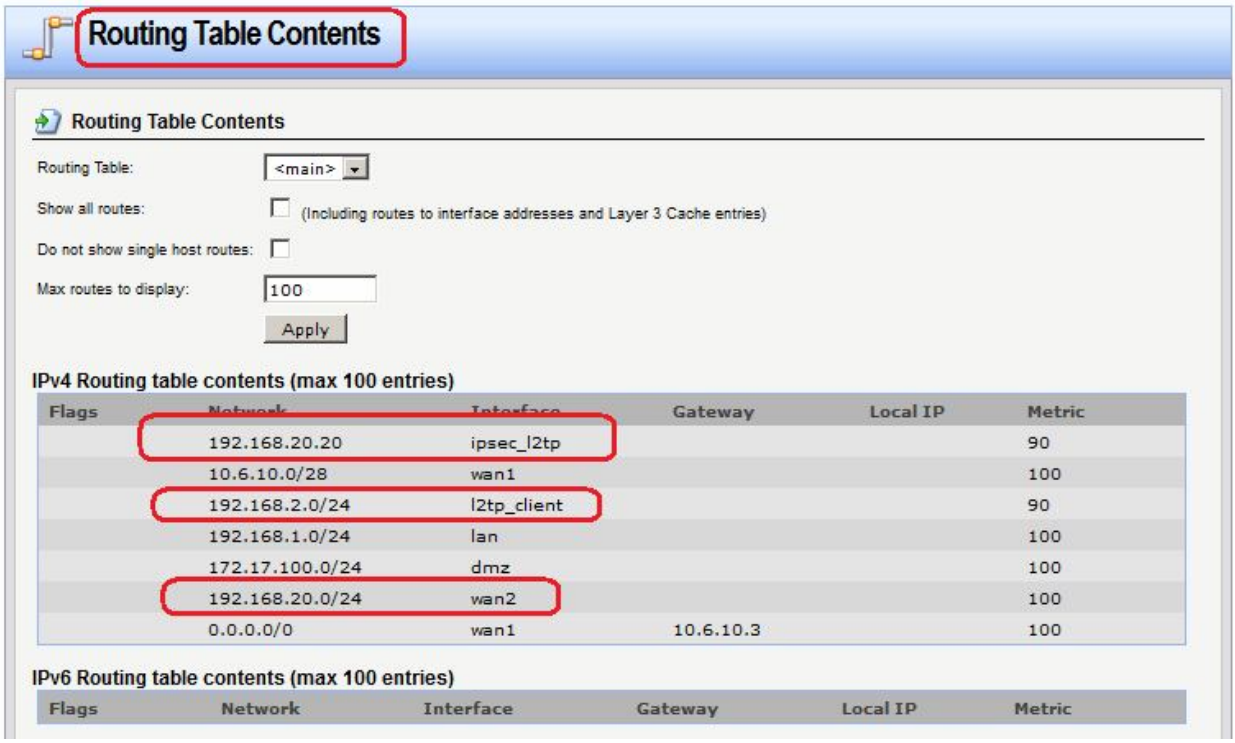
На вкладке **Authentication** указать созданный аутентификационный объект.

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**.



Правила фильтрования

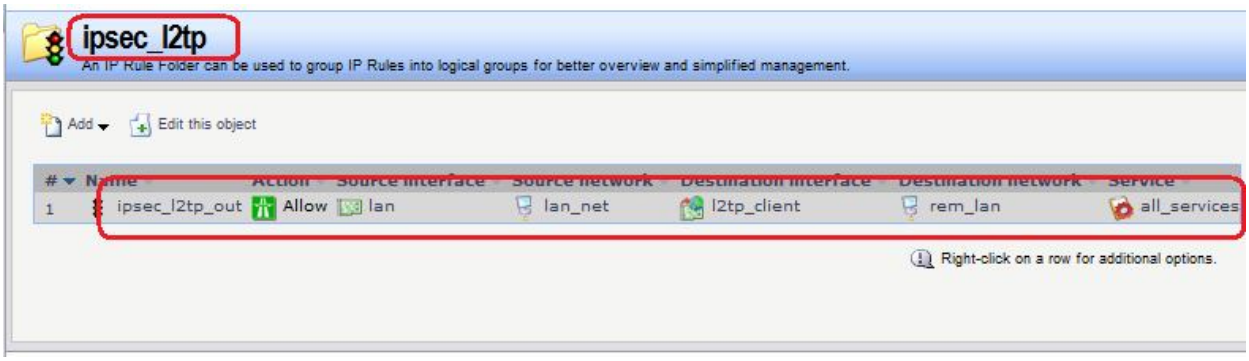
Правила фильтрования достаточно задать для L2TP-интерфейса. Правило должно разрешать исходящий трафик с lan-интерфейса на созданный L2TP-интерфейс.

Веб-интерфейс:

`Rules → IP Rules → Add → IP Rule Folder`

`Name: ipsec_l2tp`

`Rules → IP Rules → ipsec_l2tp → Add`



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.

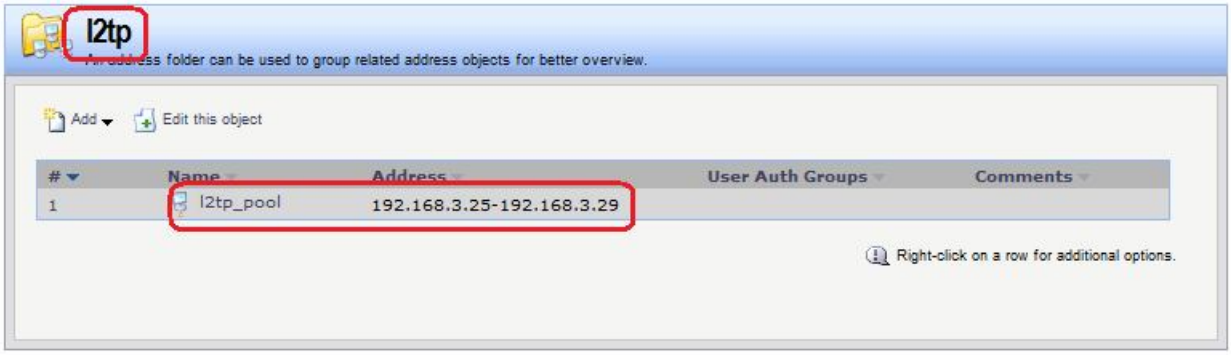
Объекты Адресной Книги
Создать пул IP-адресов.

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
```

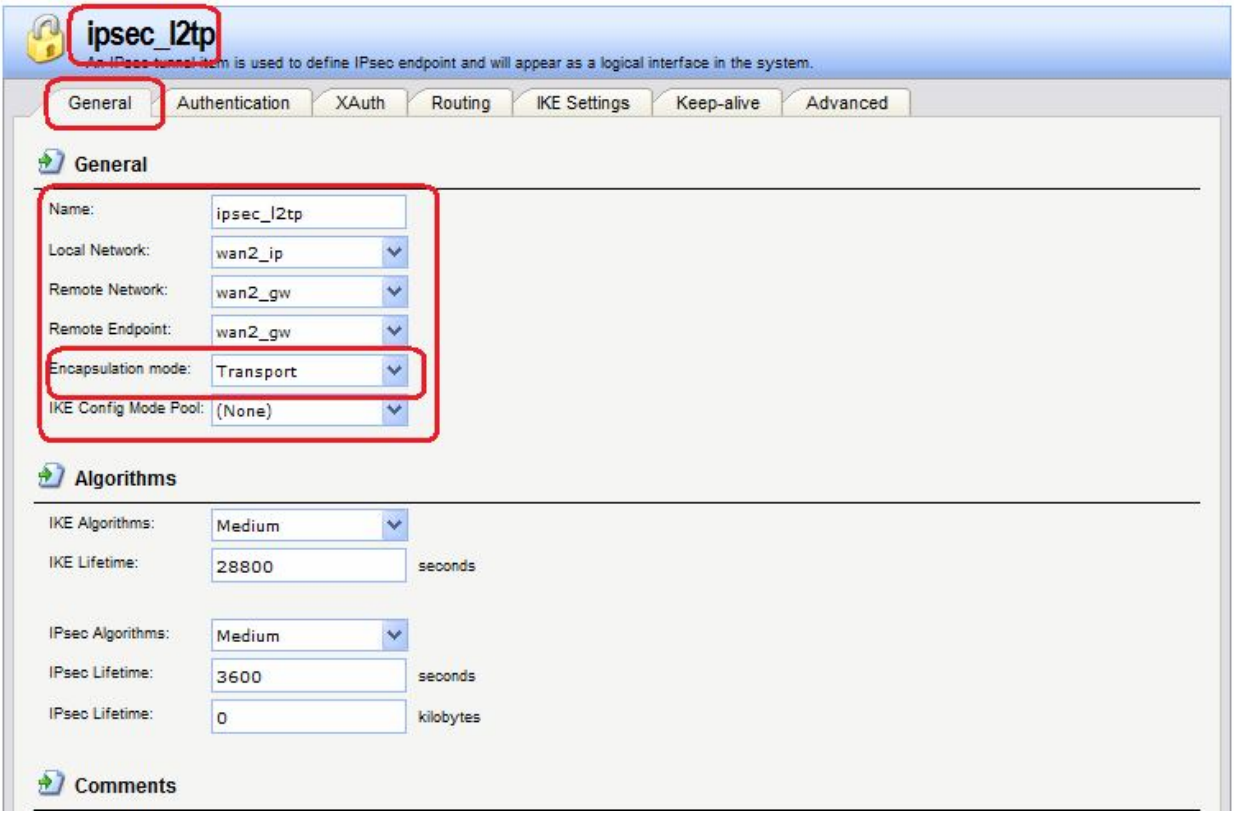
IP-адреса из этого пула будут выдаваться l2tp-клиенту.

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.



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

Командная строка:

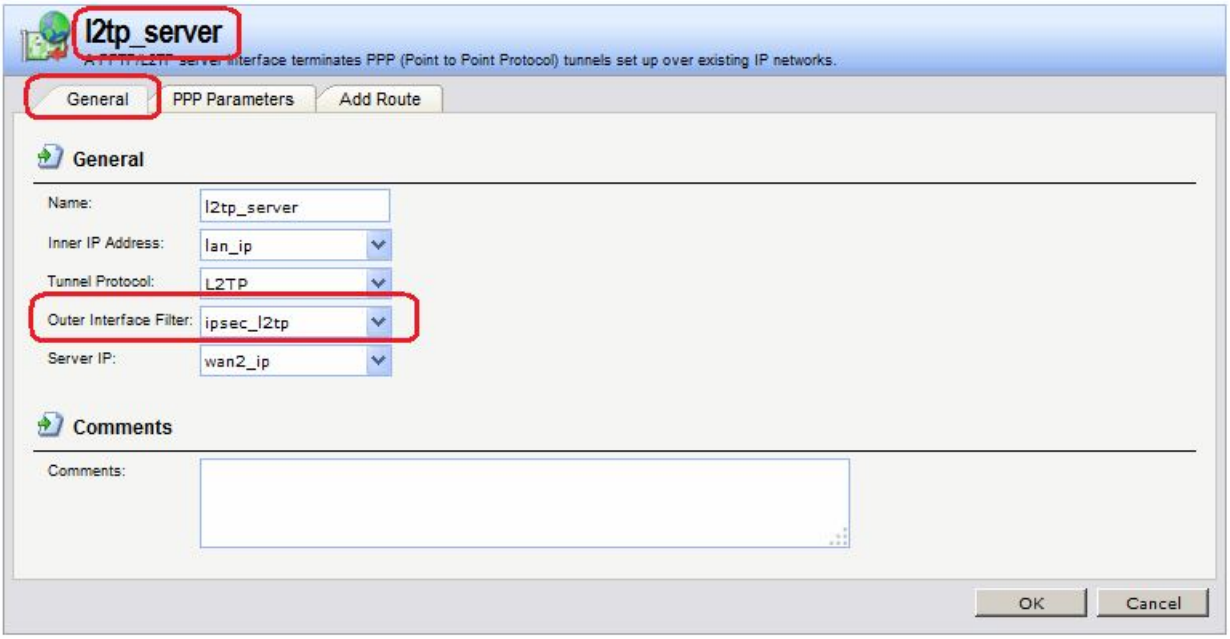
```
add Interface IPsecTunnel IPSec_l2tp LocalNetwork=wan2/wan2_ip
RemoteNetwork=wan2/wan2_gw AuthMethod=PSK PSK=ipsec_psk IKEAlgorithms=Medium
IPsecAlgorithms=Medium EncapsulationMode=Transport
RemoteEndpoint=wan2/wan2_gw
```

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

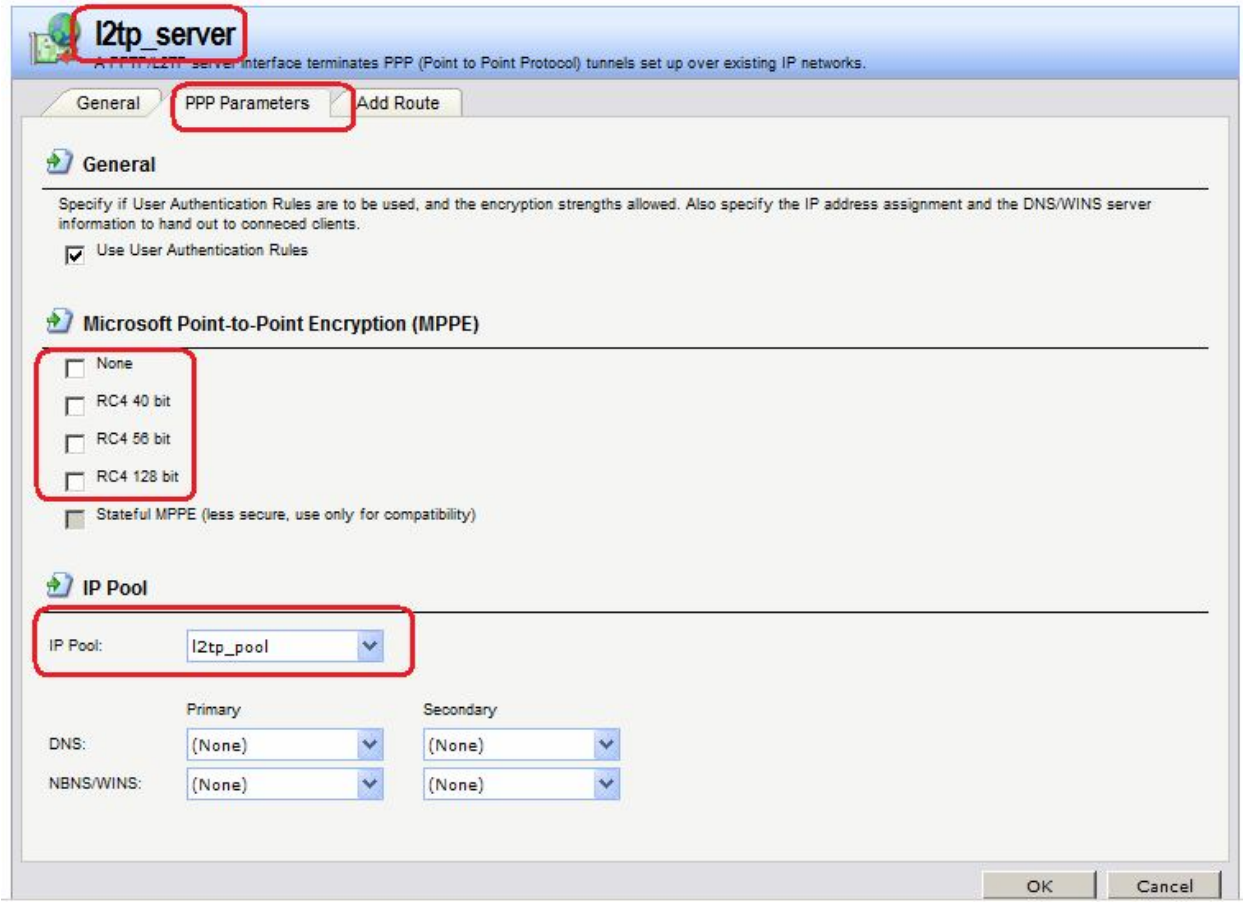
Веб-интерфейс:

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.

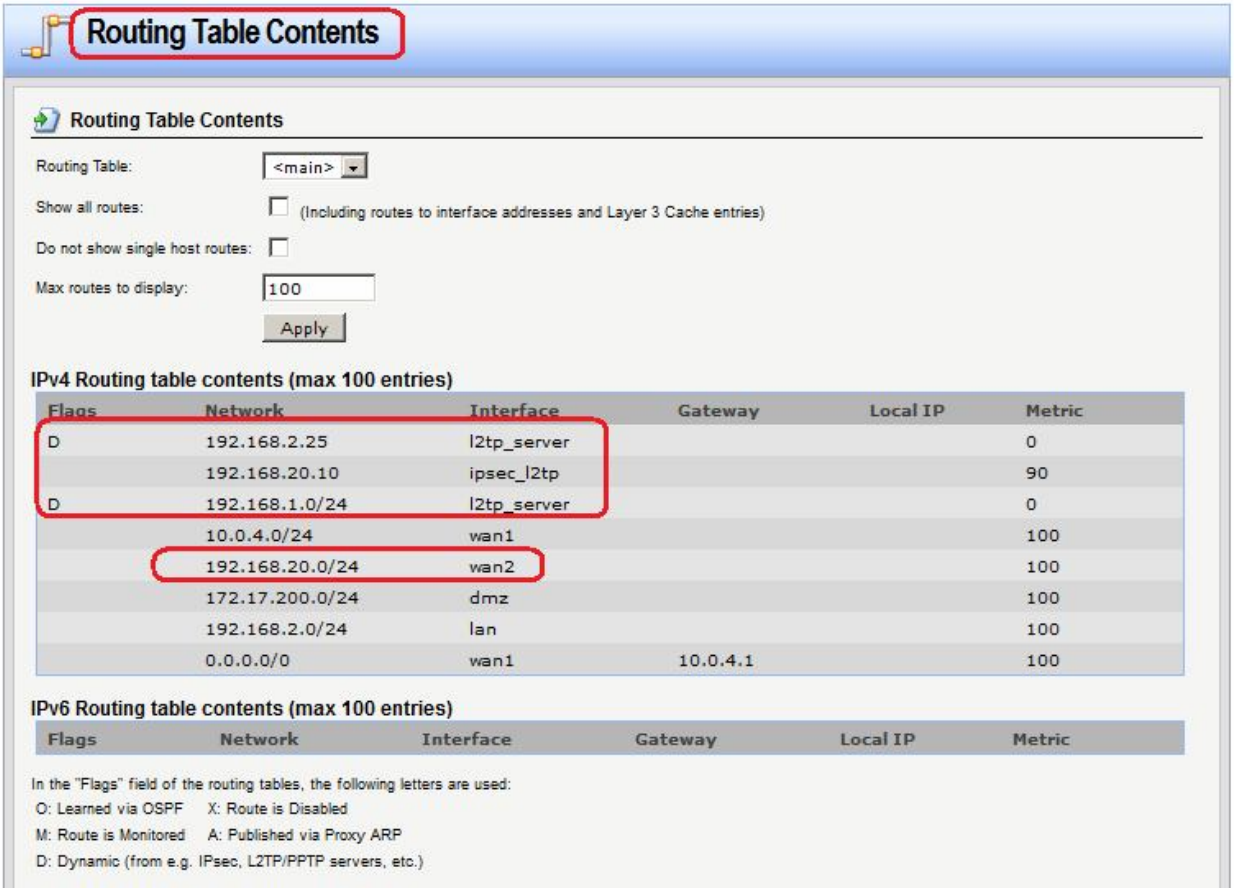


Командная строка:

```
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.



Правила фильтрования

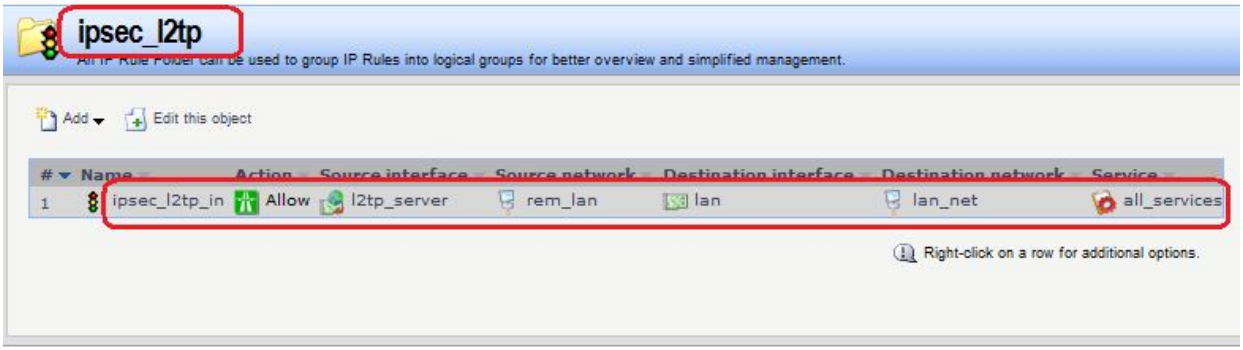
Правила фильтрования достаточно задать для L2TP-интерфейса.

Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: l2tp

Rules → IP Rules → l2tp → Add



Командная строка:

add IPRuleFolder Name=ipsec_l2tp

cc IPRuleFolder <N folder>

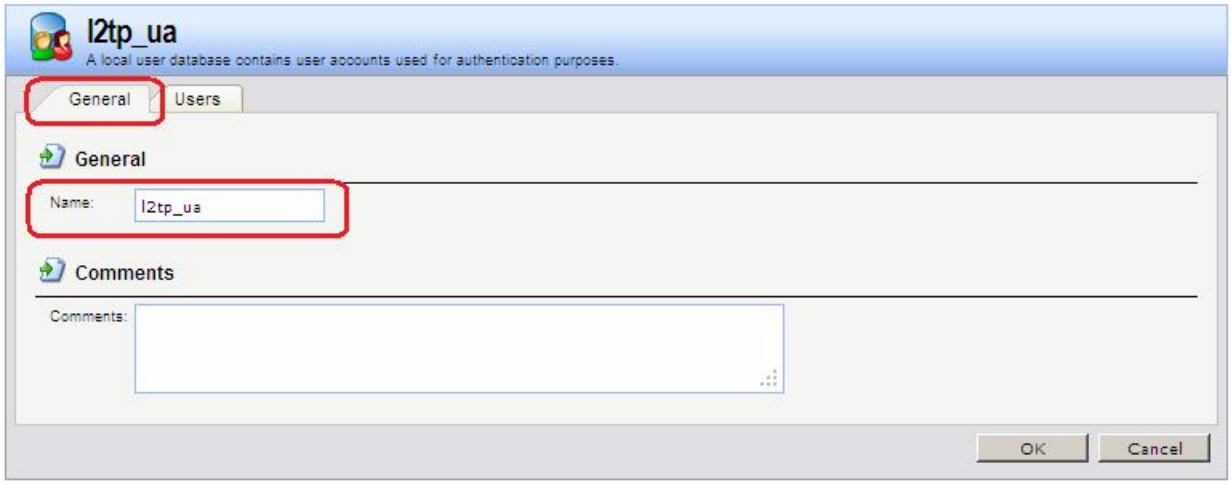
```
add IPRule Action=Allow SourceInterface=l2tp_server
SourceNetwork=remote/rem_lan DestinationInterface=lan
DestinationNetwork=lan/lan_net Service=all_services Name=ipsec_l2tp_in
```

Аутентификация на уровне пользователя
Создать локальную базу данных пользователей.

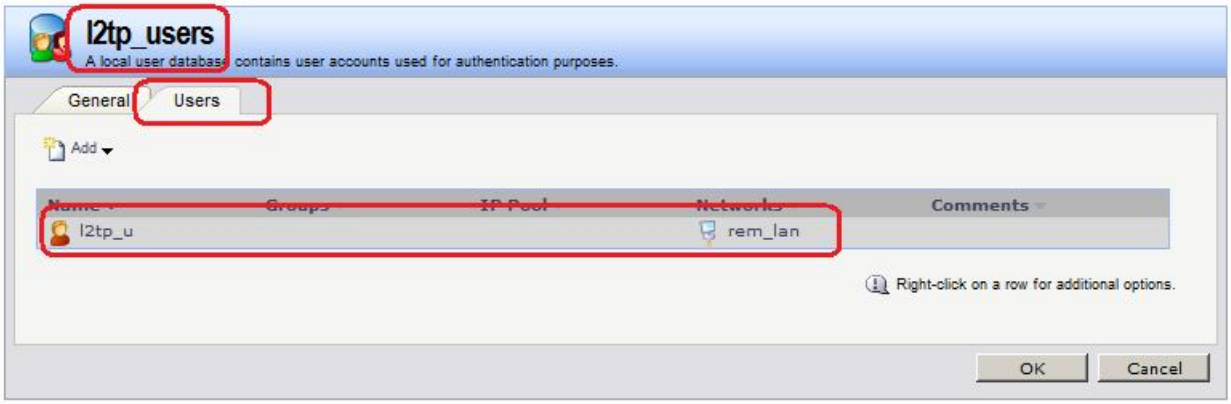
Веб-интерфейс:

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
```

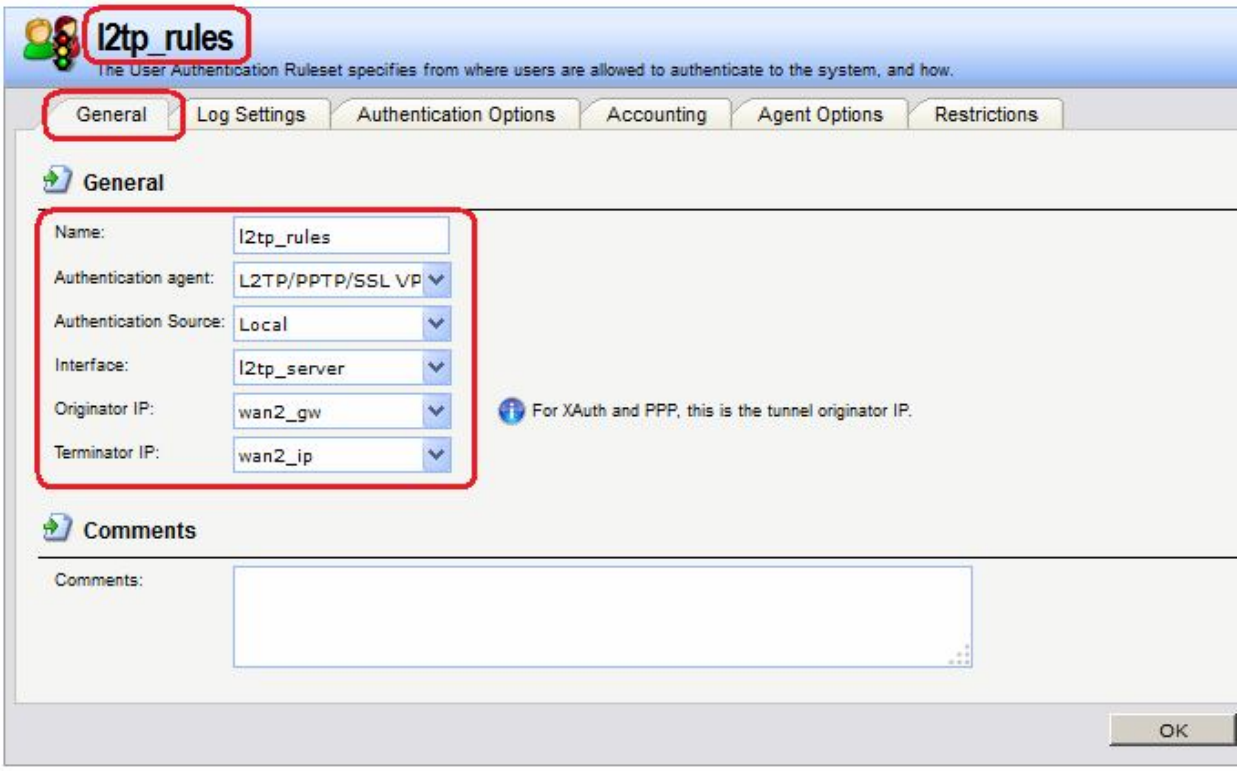
Создать правило аутентификации пользователей.

Веб-интерфейс:

User Authentication → User Authentication Rules → Add

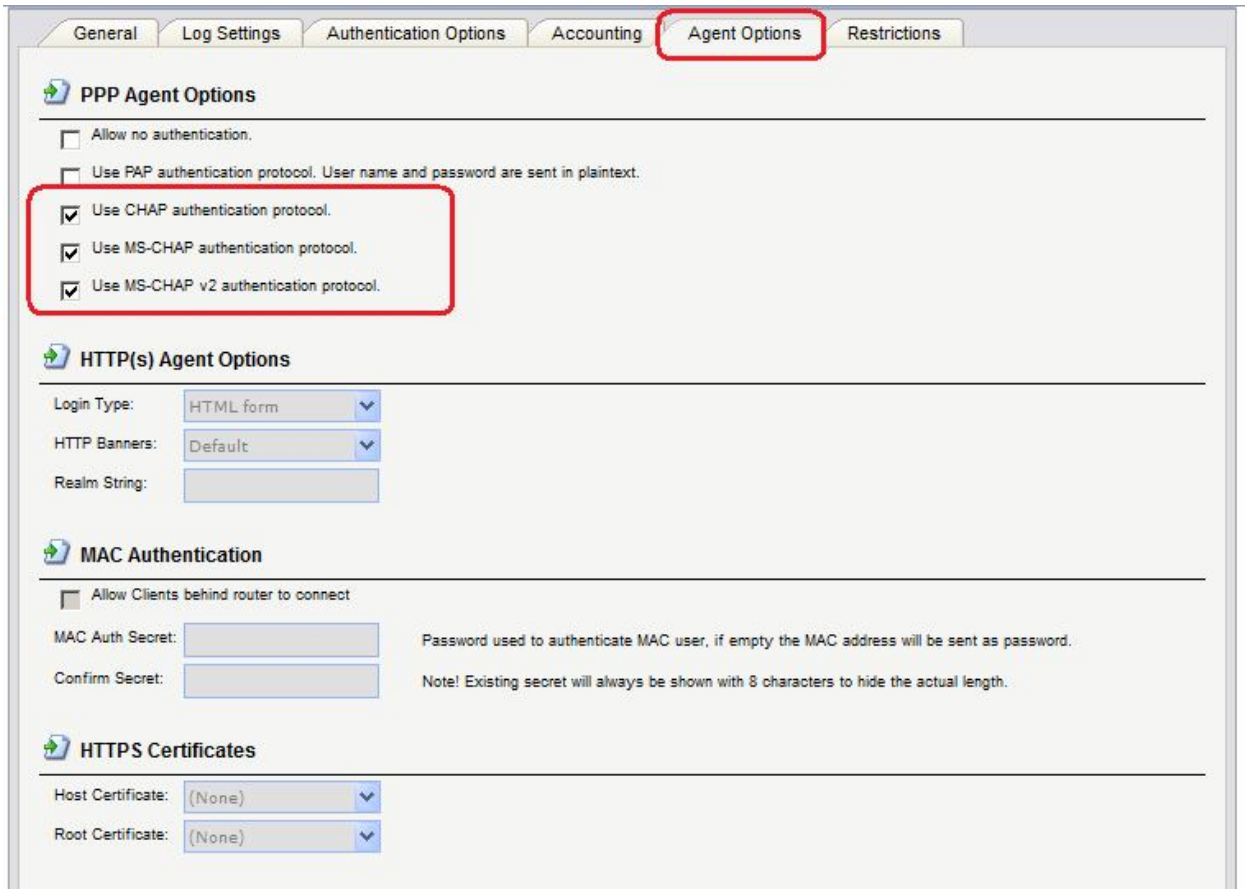
Name: l2tp_rules

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



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

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

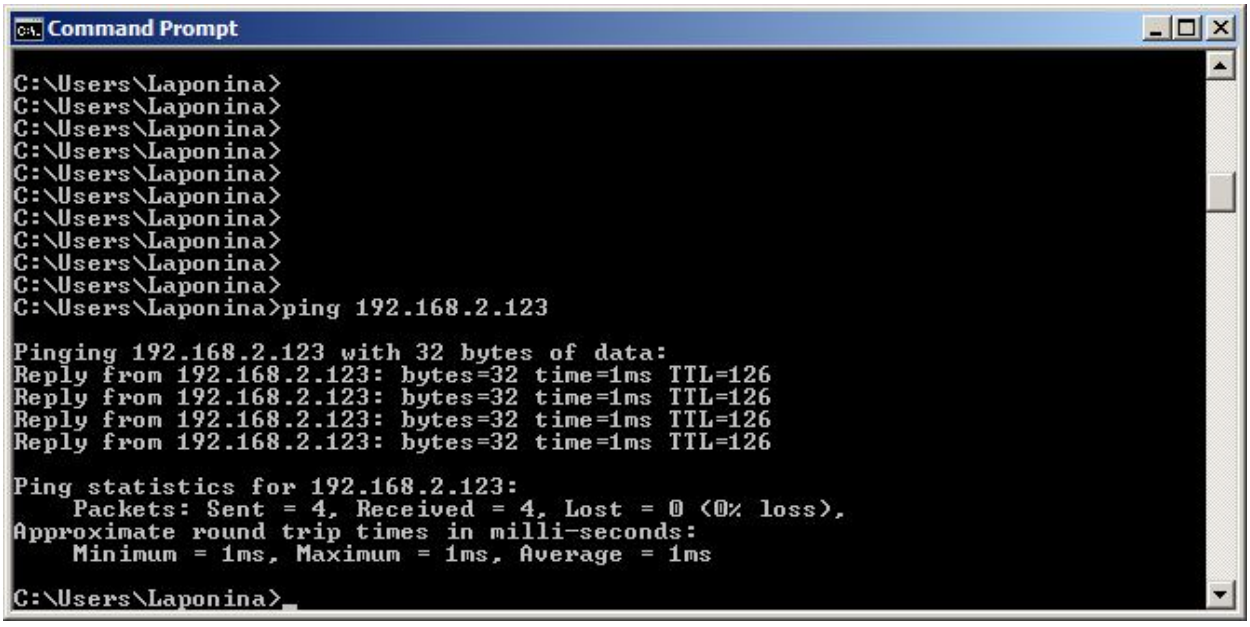


Командная строка:

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

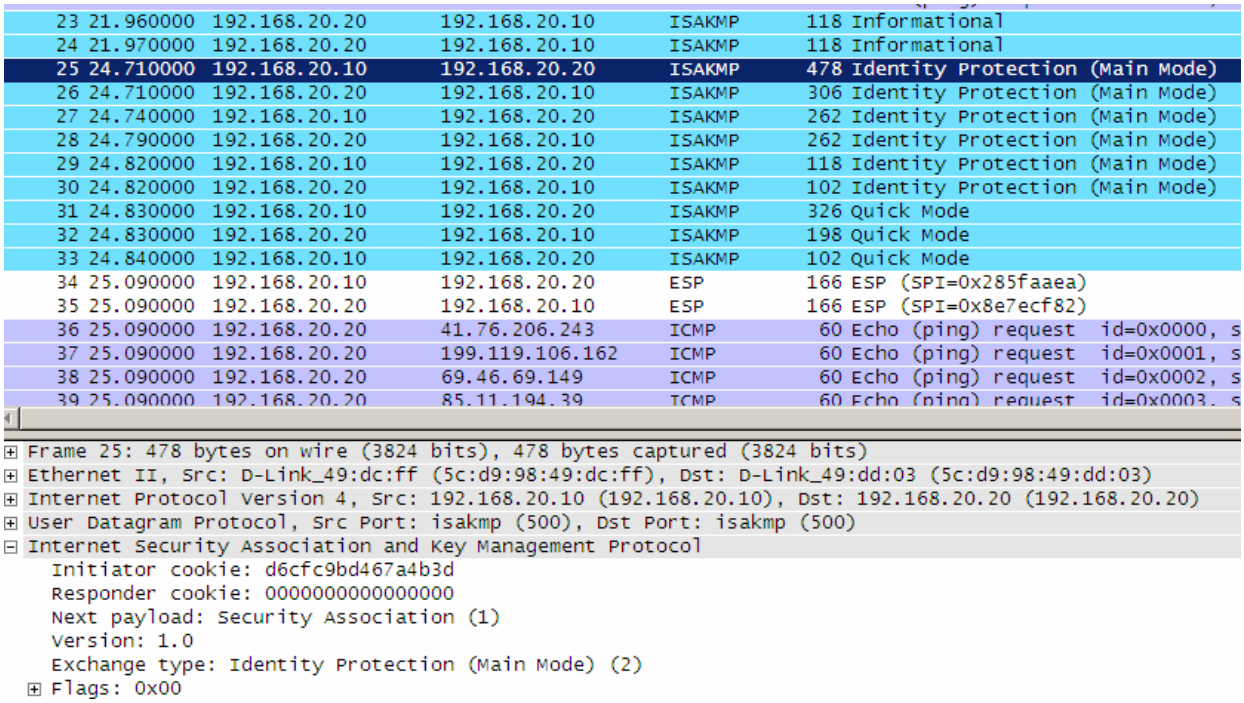
Проверка конфигурации

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

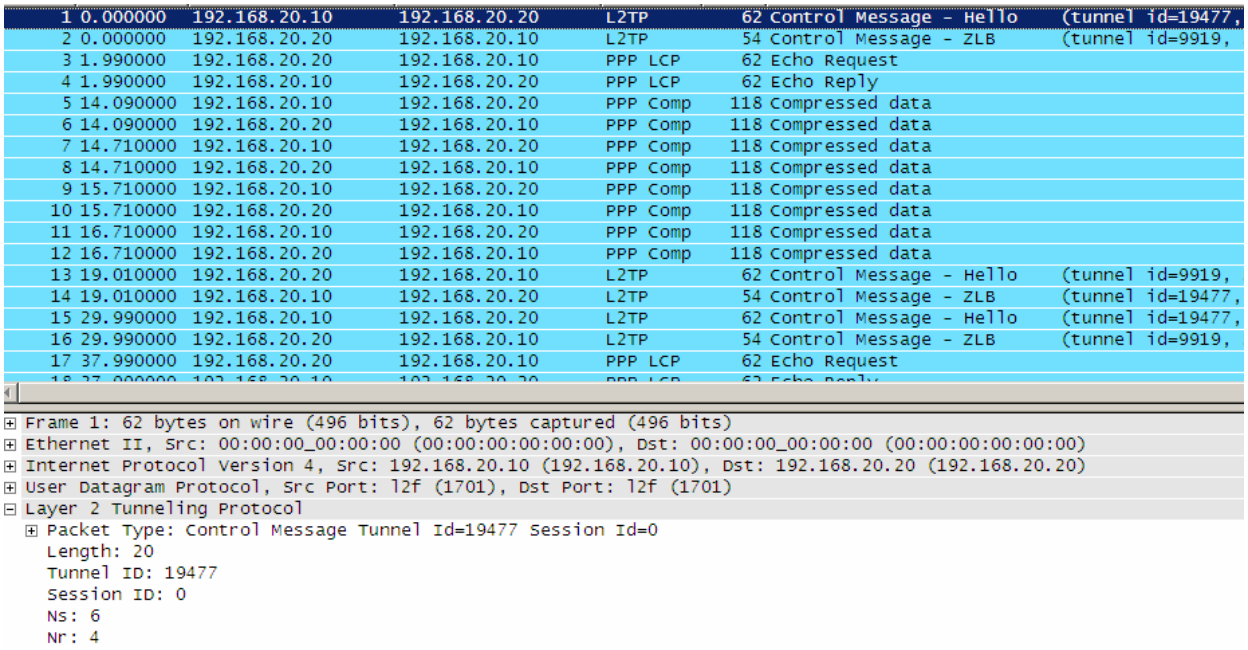


Получим дамп трафика аналогично тому, как это делалось в предыдущих лабораторных работах.

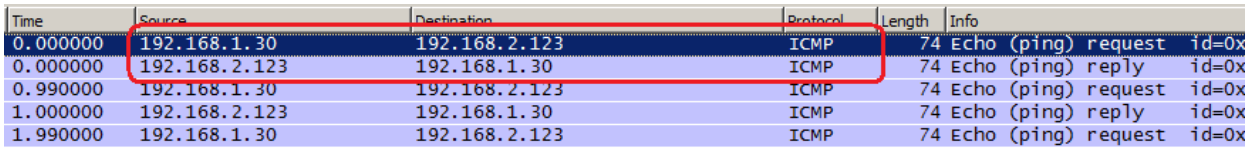
На интерфейсе **`wan2`** видим IPSec-трафик.



На интерфейсе **`IPSec_l2tp`** видим L2TP-трафик.



На интерфейсе **`l2tp_server`** видим ICMP-трафик.



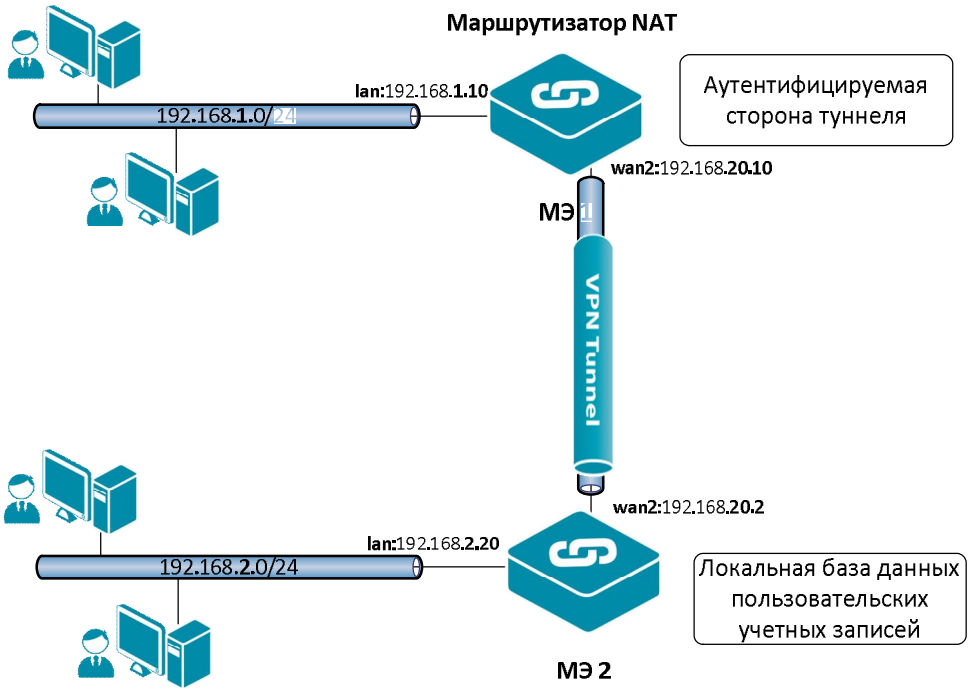
Лабораторная работа 10. Соединение двух локальных сетей протоколом L2TP/IPSec в транспортном режиме, для одной из локальных сетей используется NAT

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 использовать протокол L2TP. Локальная сеть, расположенная за L2TP-клиентом, используется NAT.

Топология сети аналогична топологии VPN/IPSec.

Топология

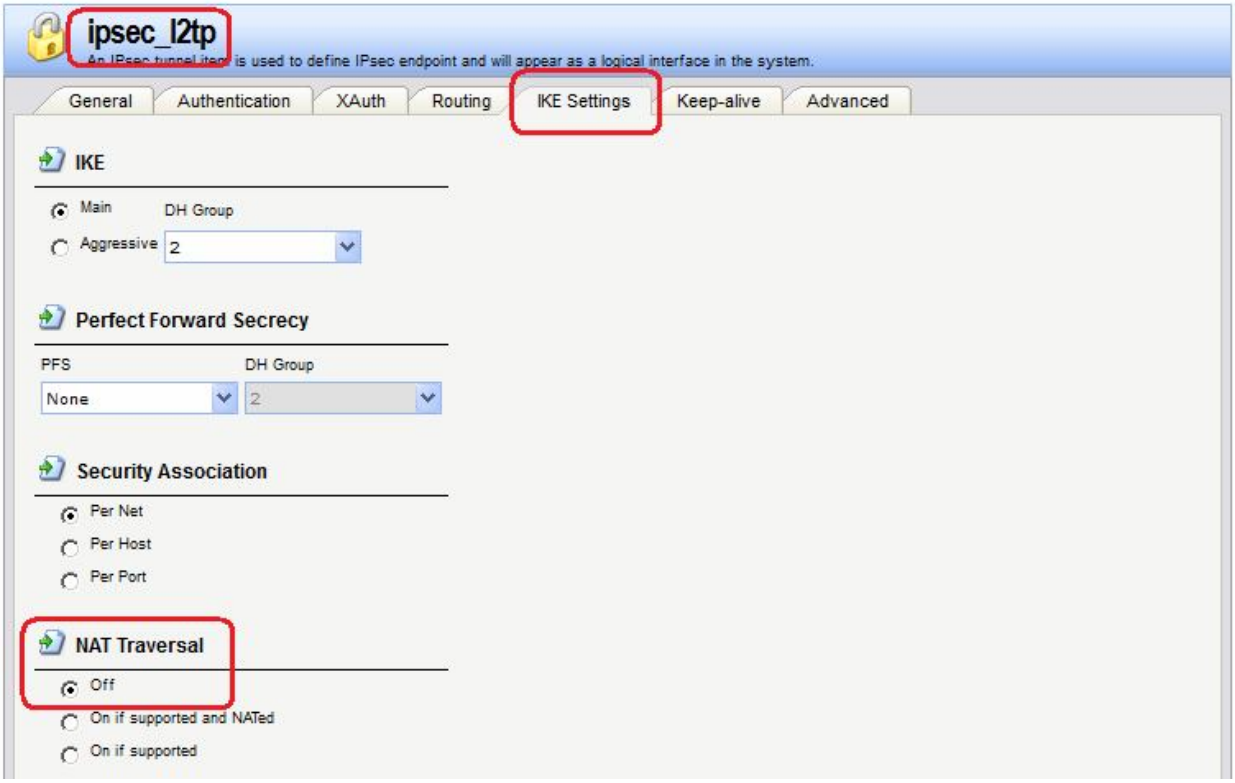


Описание практической работы

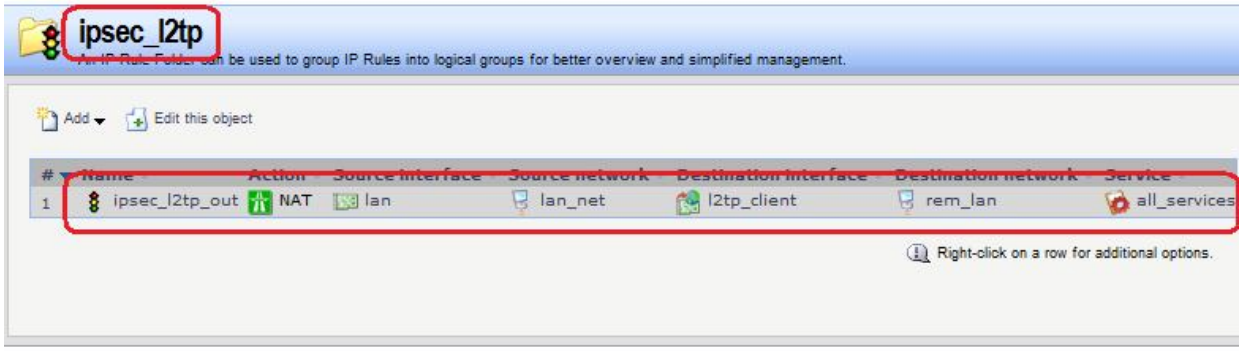
Межсетевой Экран 1

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.

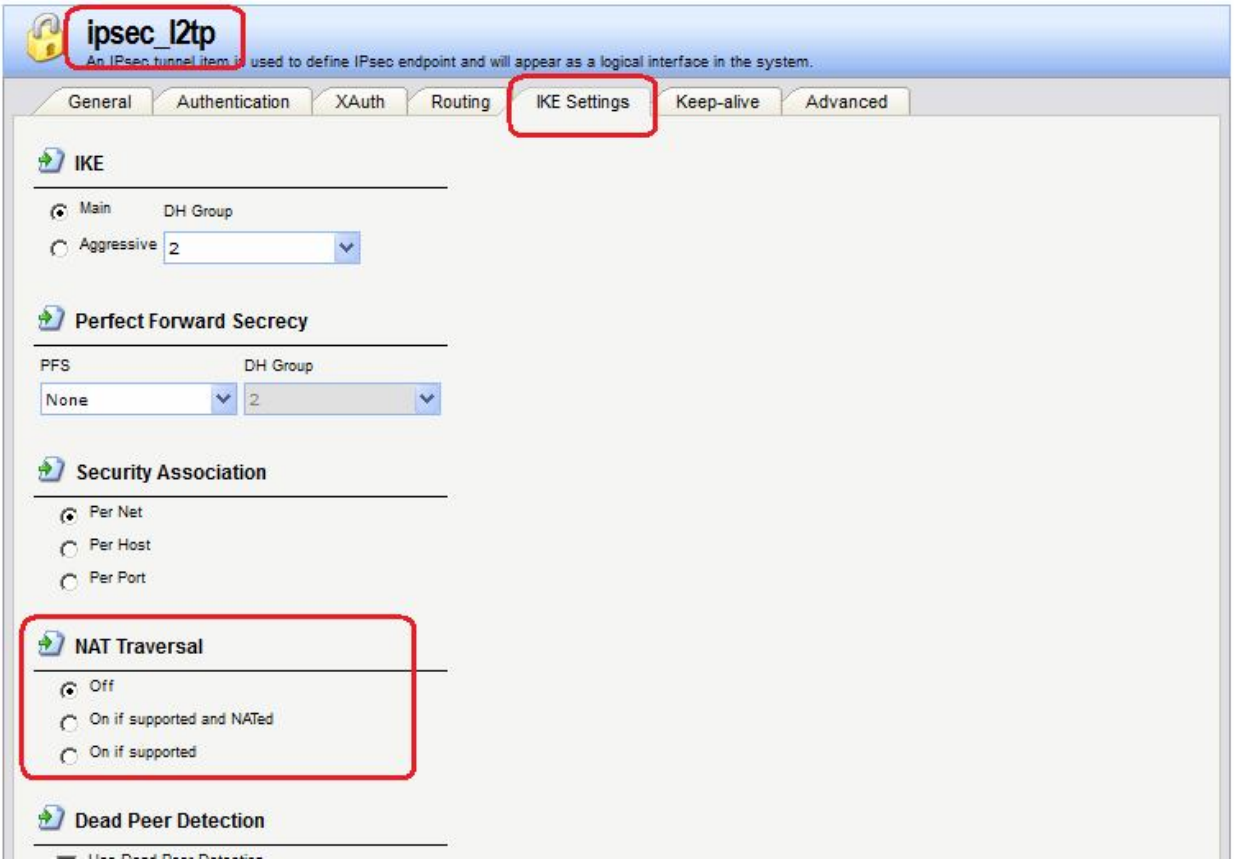


Правила фильтрования
В Правилах фильтрования вместо действия **`Allow`** следует указать действие **`NAT`**.



Межсетевой Экран 2

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

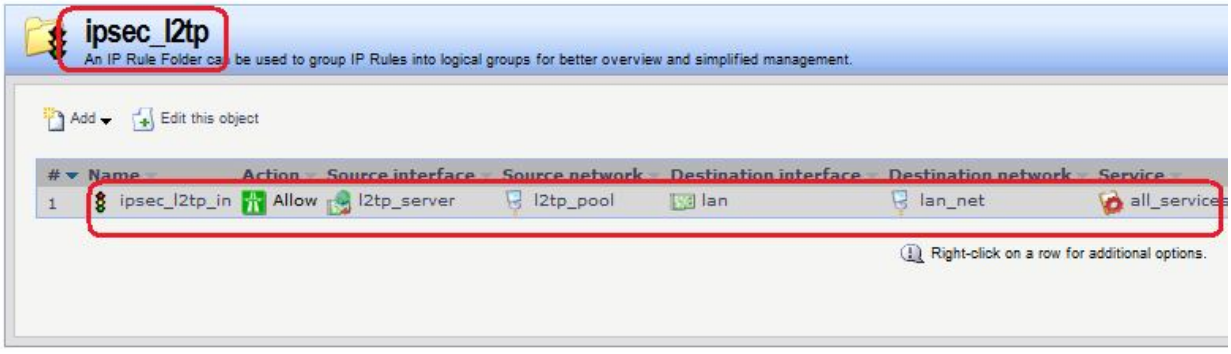


Правила фильтрования

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

Веб-интерфейс:

`Rules → IP Rules → l2tp`

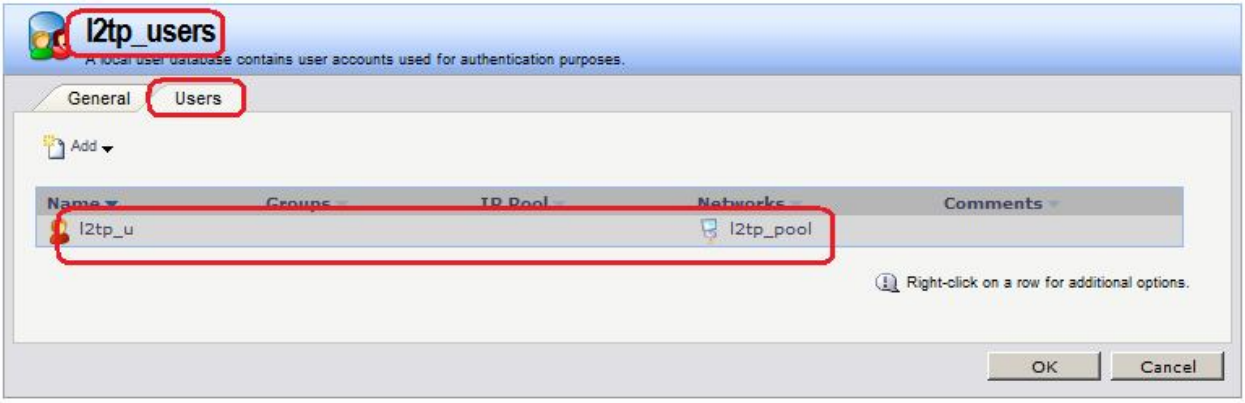


Командная строка:

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

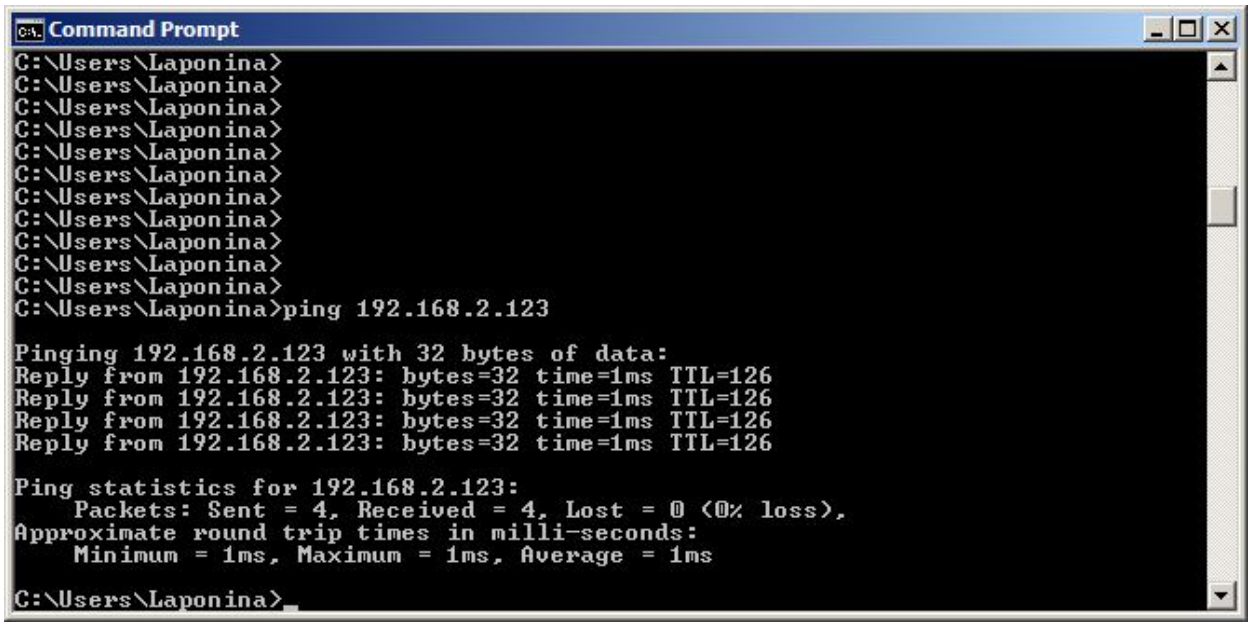
Аутентификация на уровне пользователя

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



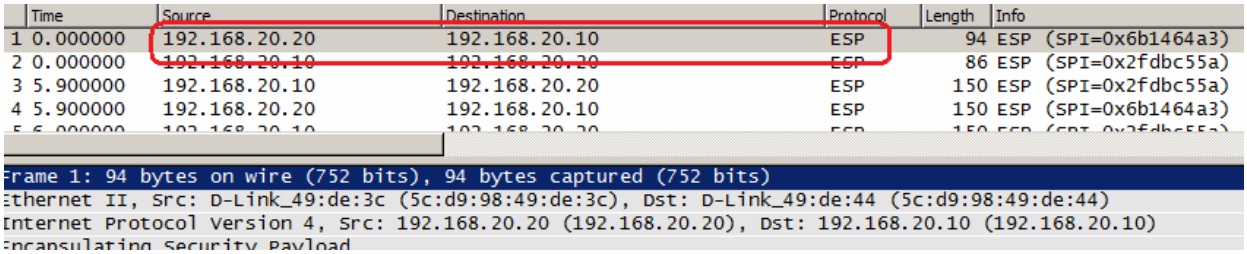
Проверка конфигурации

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

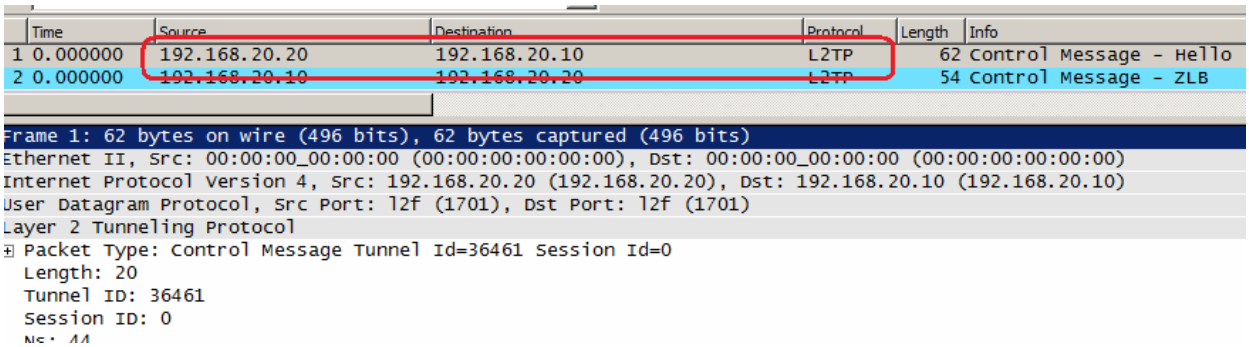


Получим дамп трафика аналогично тому, как это делалось в предыдущих лабораторных работах.

На интерфейсе **`wan2`** видим IPSec-трафик.

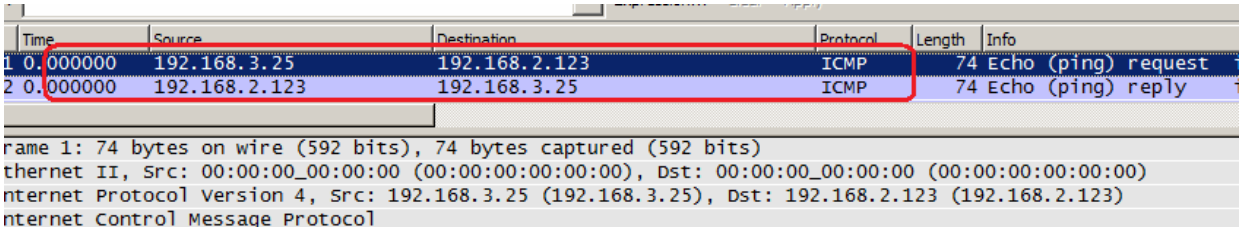


На интерфейсе **`IPSec_l2tp`** видим L2TP-трафик.



На интерфейсе **`l2tp_server`** видим ICMP-трафик.

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



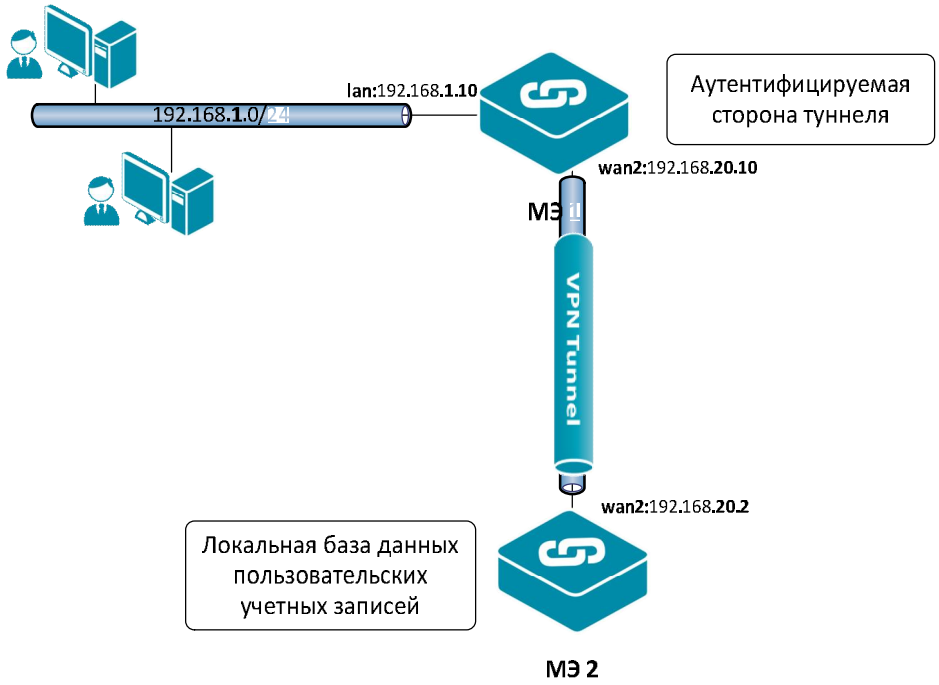
Аутентификация и хранение учетных записей

Лабораторная работа 11. Использование локальной БД для хранения учетных записей

Цель

Учетные записи пользователей хранятся в локальной базе данных.

Топология сети



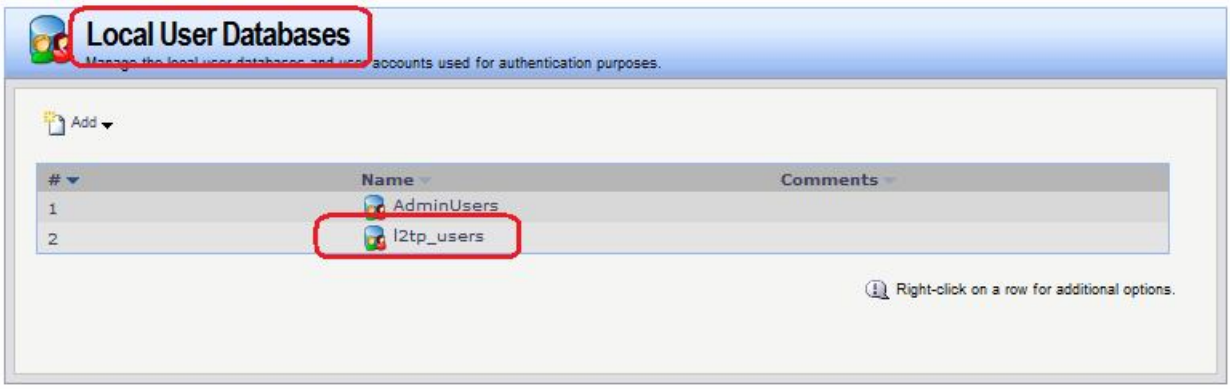
Описание практической работы

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:

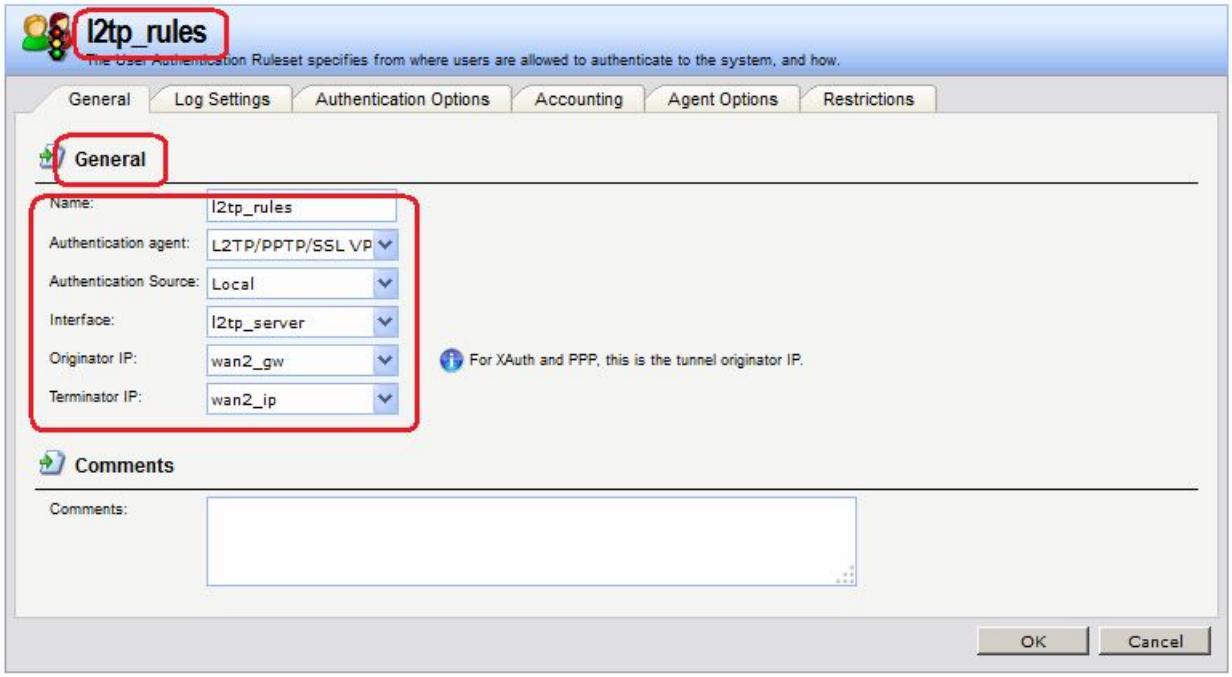
```
add User l2tp_u Password=qwerty AutoAddRouteNet=remote/rem_lan
```

3. Создаем правило аутентификации пользователей.

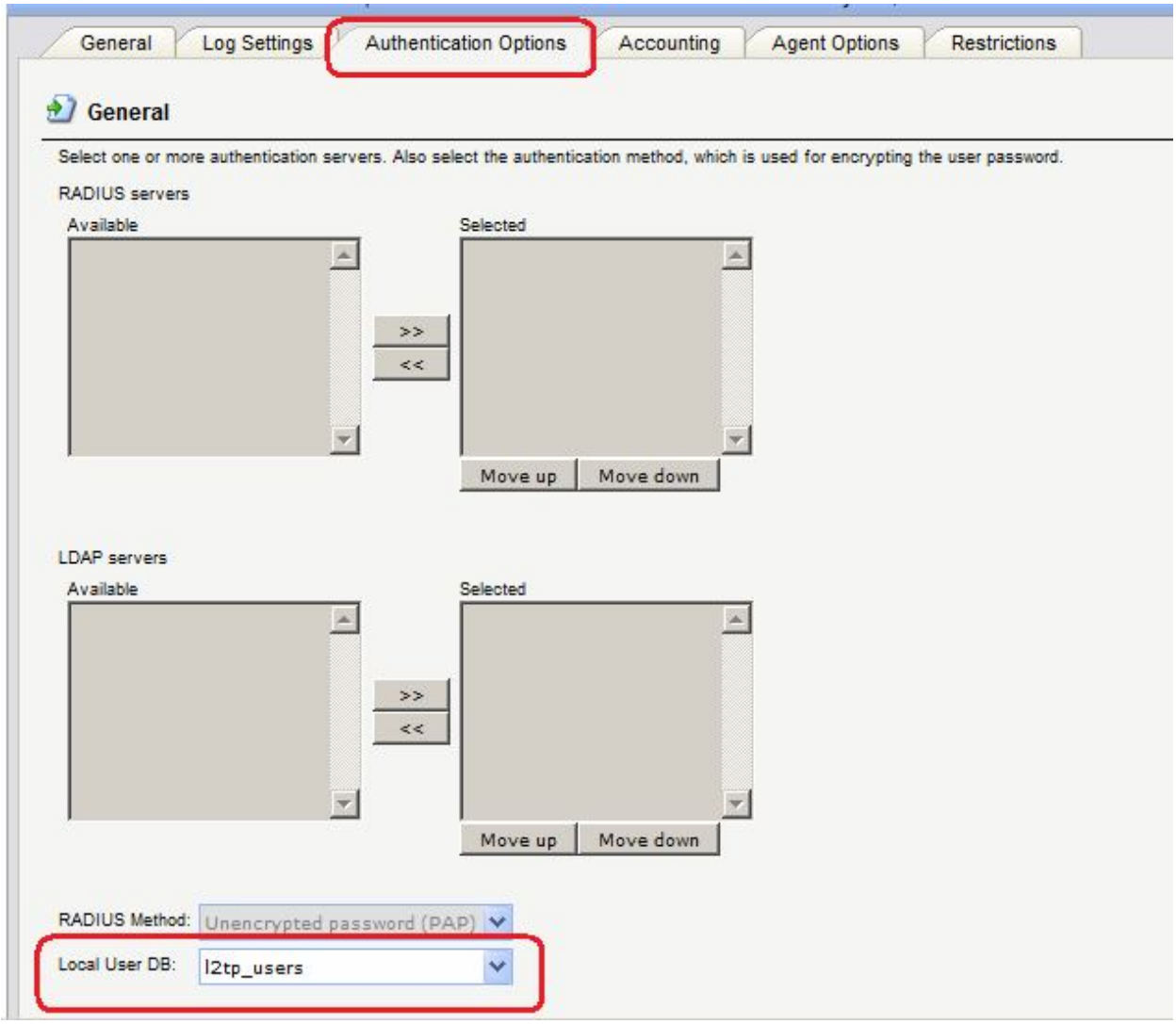
Веб-интерфейс:

`User Authentication → User Authentication Rules → Add`

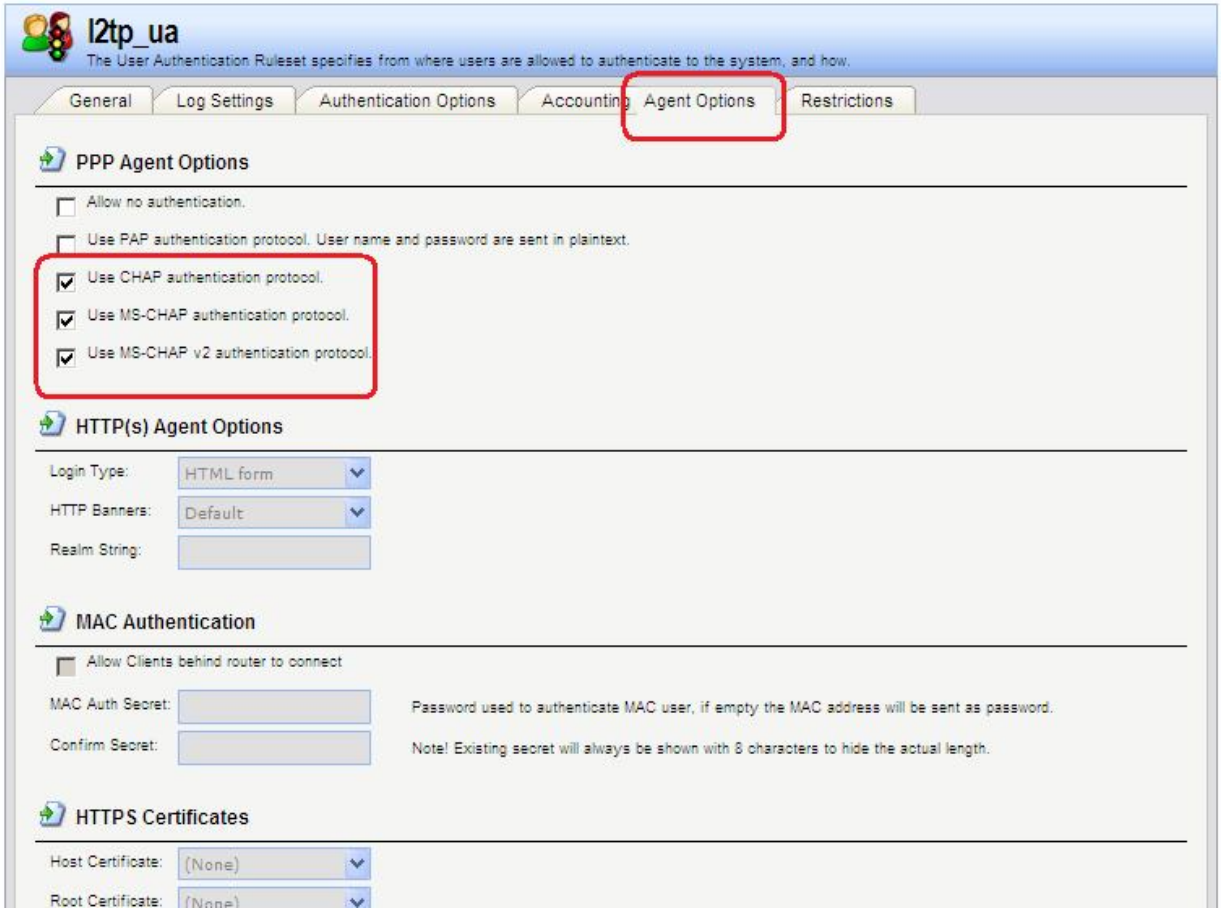
На вкладке **`General`** указать аутентификационный источник **`Local`** и необходимые для туннелирующего протокола опции. В нашем случае туннелирующим протоколом является L2TP.



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



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



Командная строка:

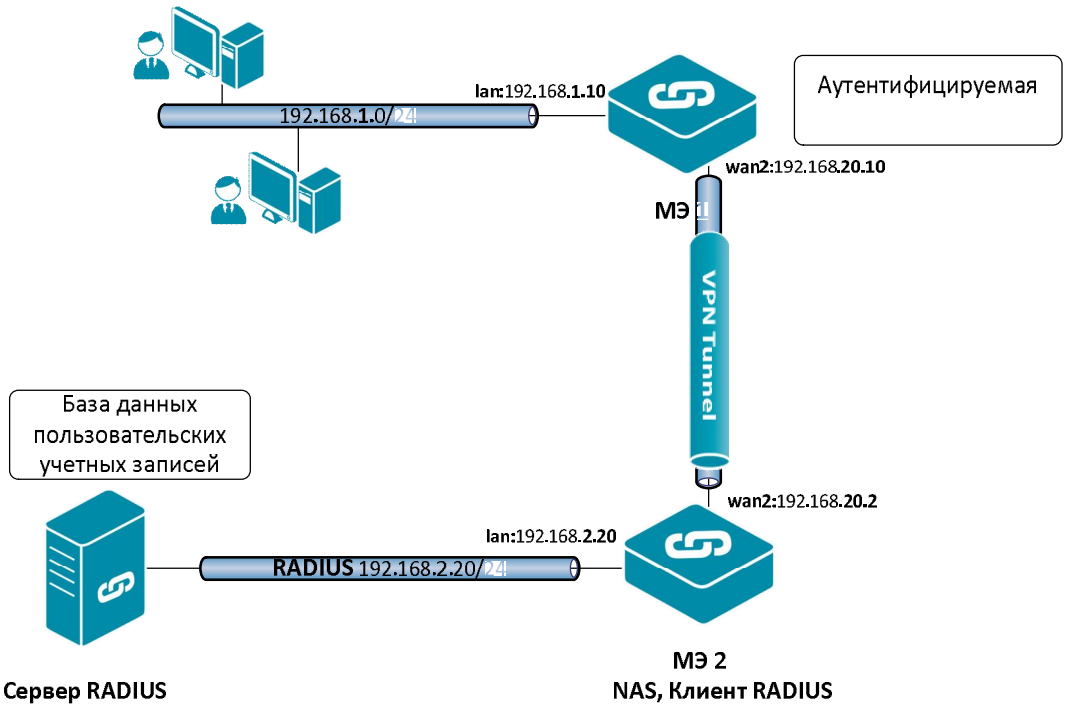
```
add UserAuthRule AuthSource=Local Interface=l2tp_server
LocalUserDB=l2tp_users OriginatorIP=wan2/wan2_gw Agent=PPP
TerminatorIP=wan2/wan2_ip Name=l2tp_rules
```

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.

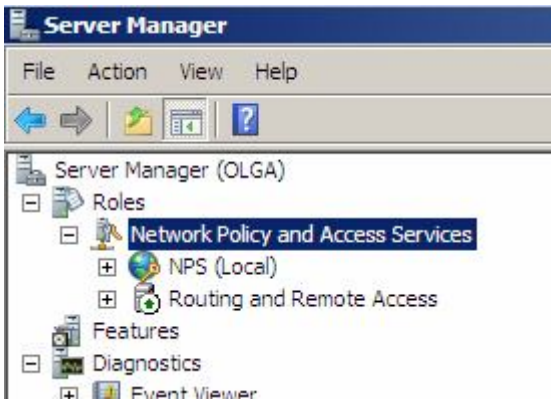
Топология сети



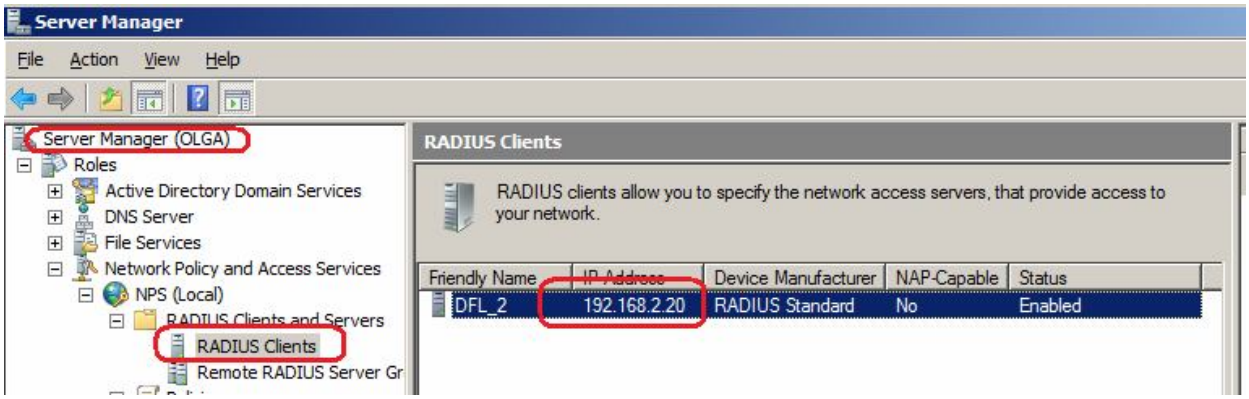
Описание практической работы

Сервер RADIUS

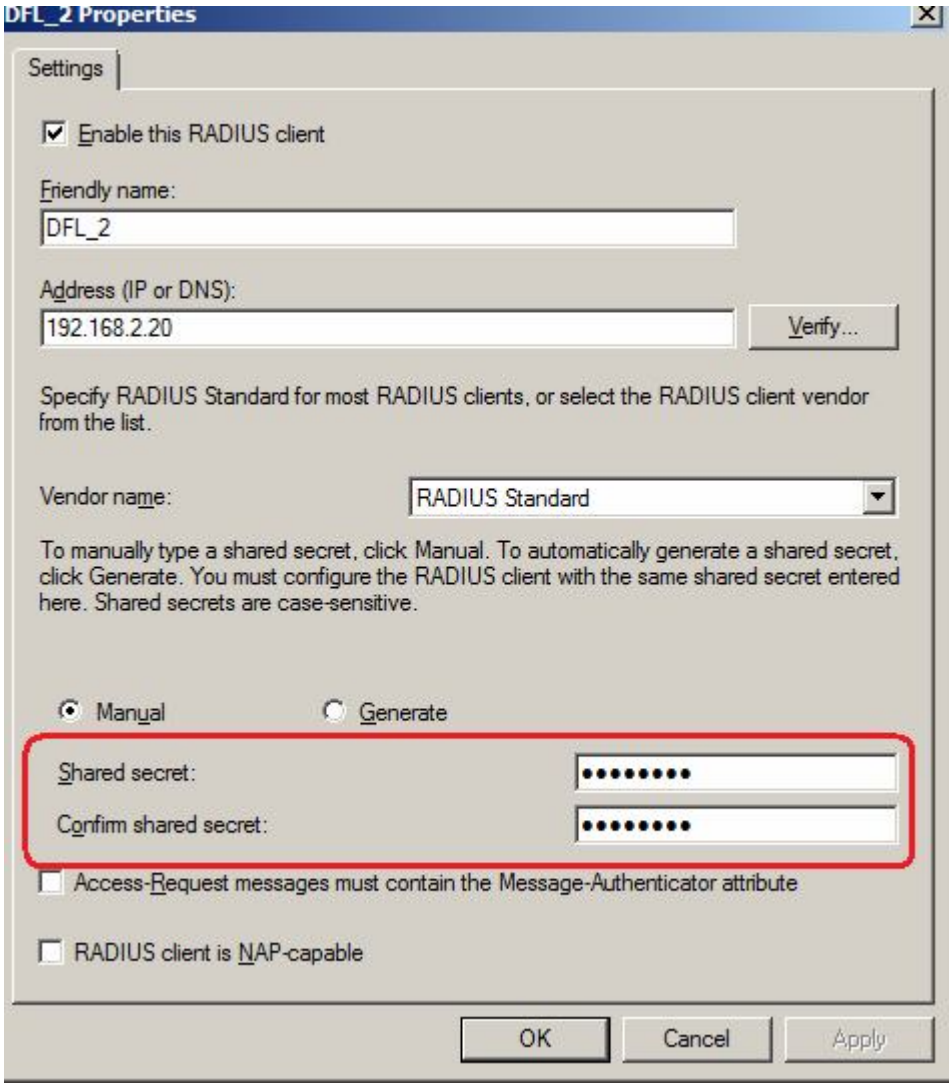
На Windows Server 2008 добавить роль **`Network Policy and Access Services`**.



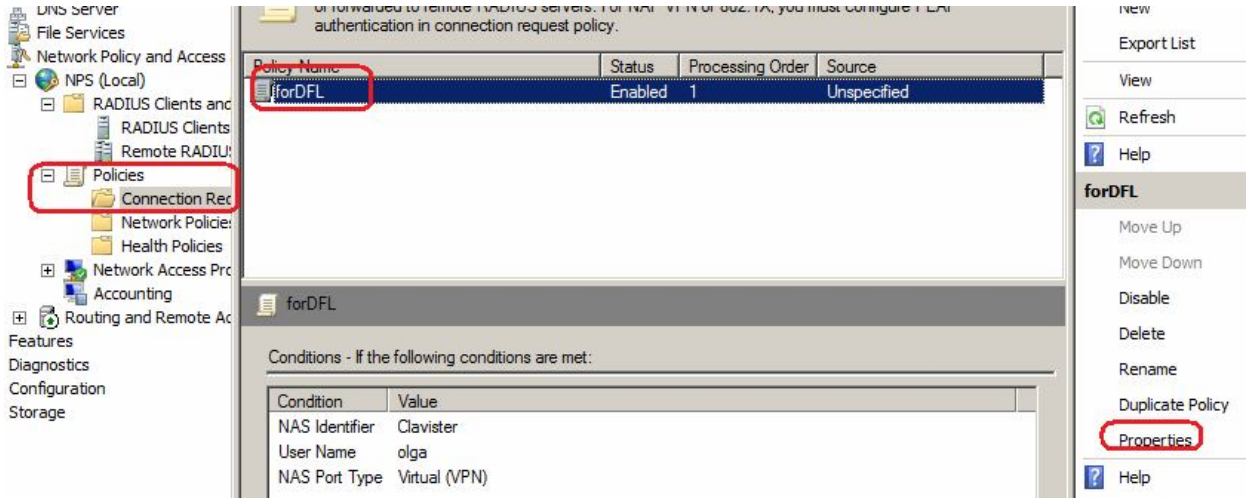
В качестве RADIUS-клиента указать IP-адрес МЭ 2.



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.

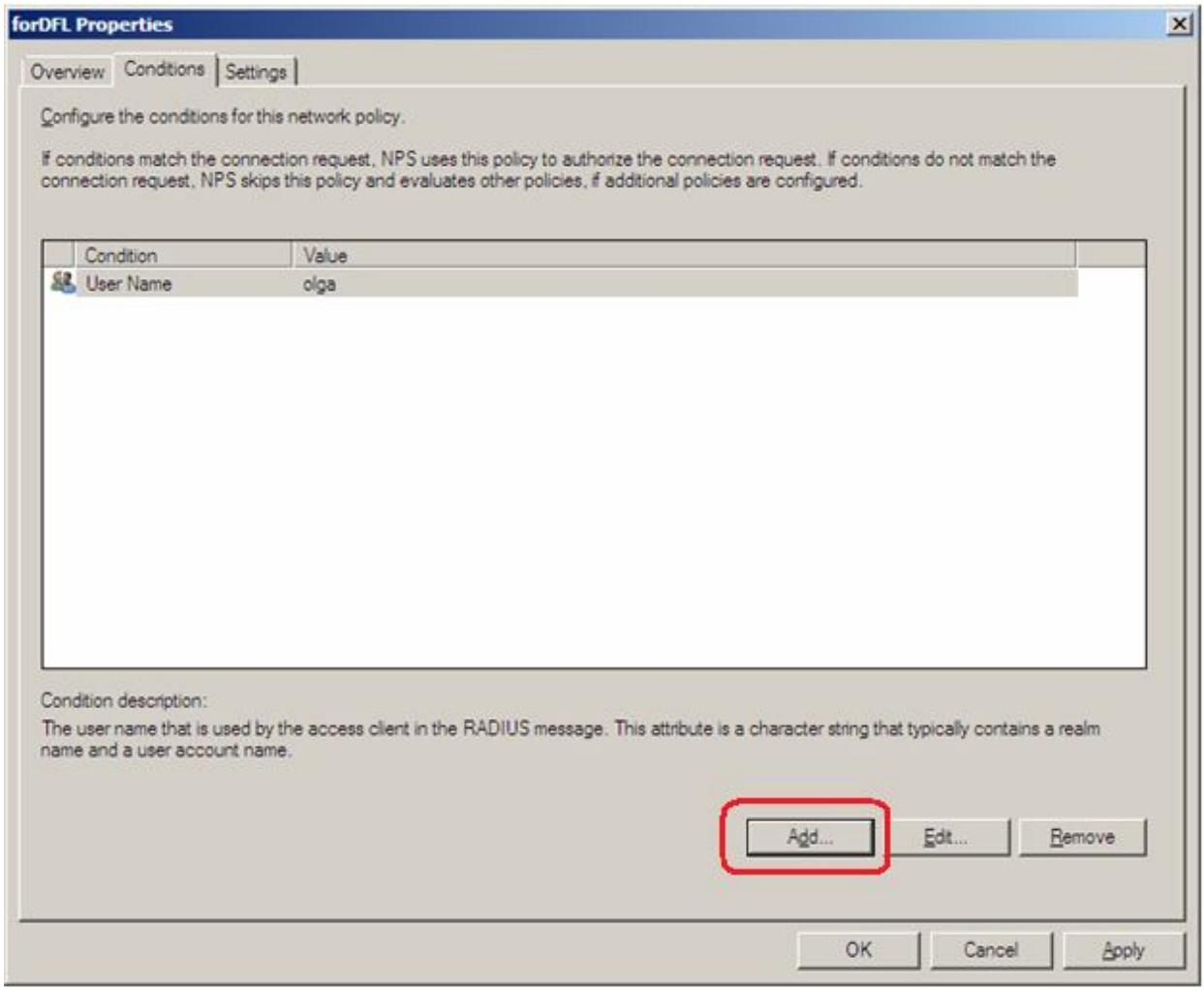


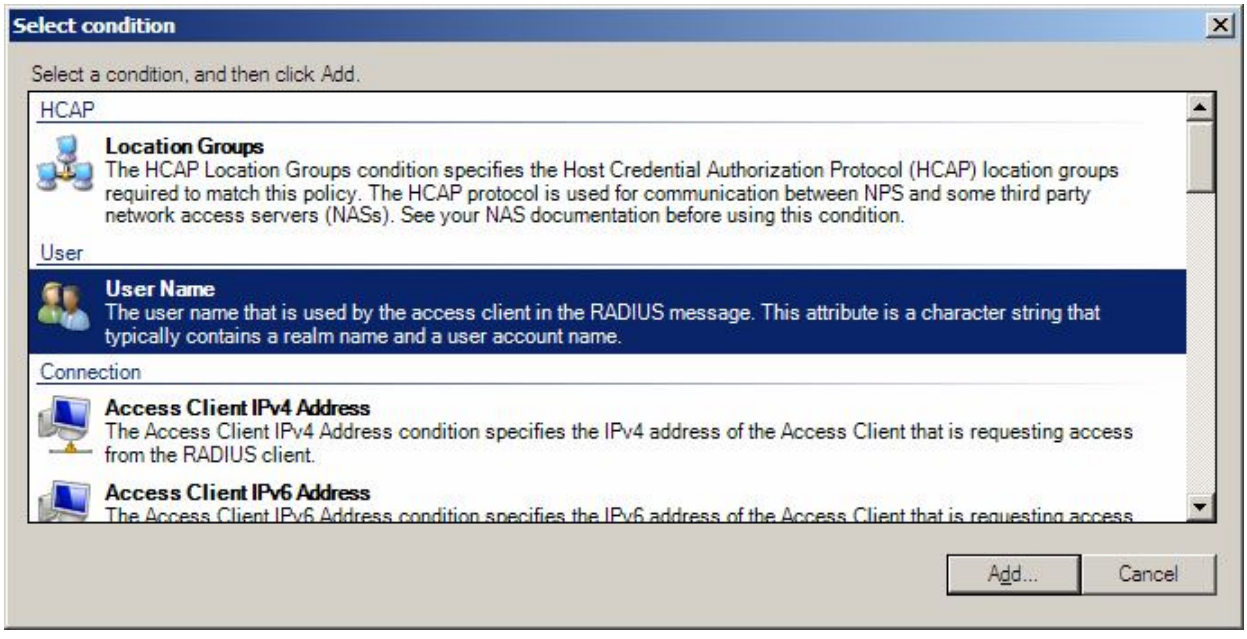
Могут быть добавлены различные условия аутентификации NAS.

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.

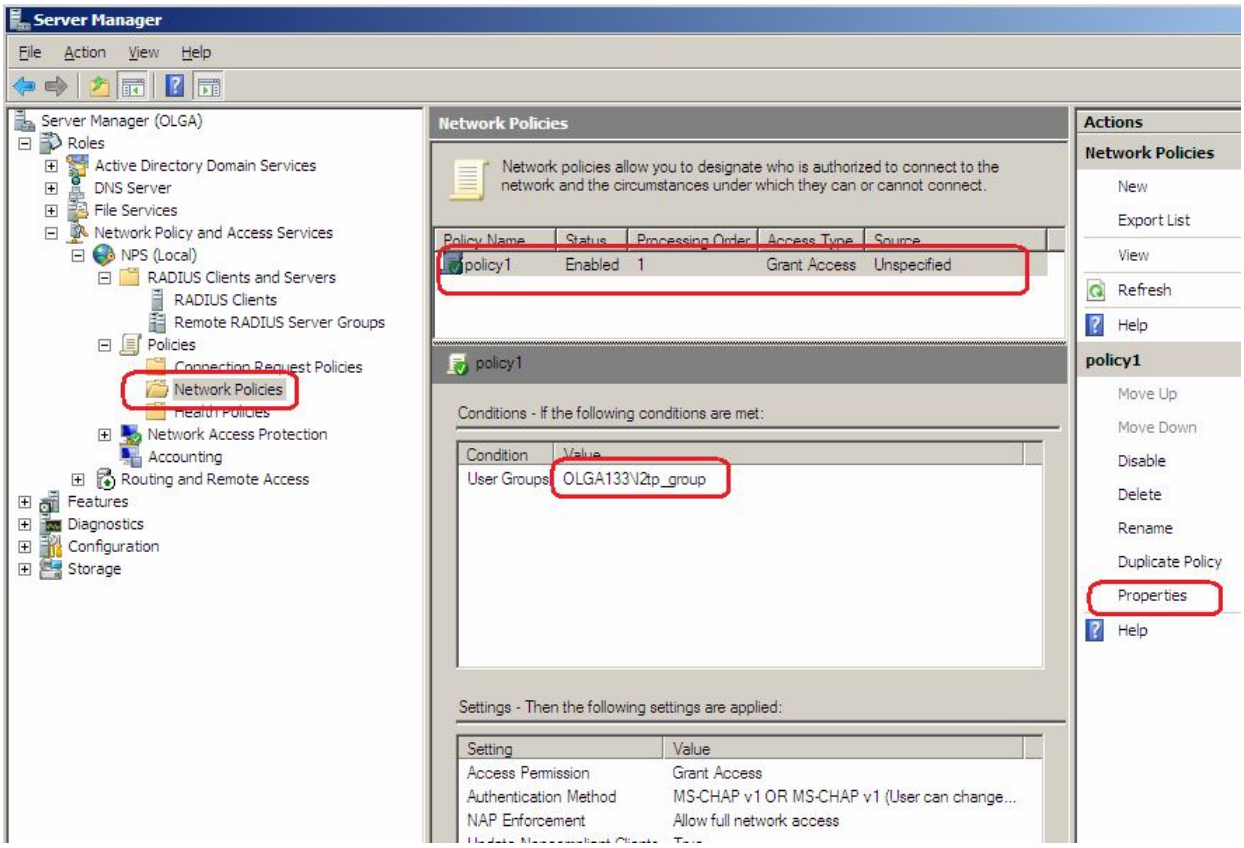
1. В политиках запроса соединения (Connection Request Policies) можно указать имя пользователя, задаваемое на аутентифицируемой стороне туннеля.





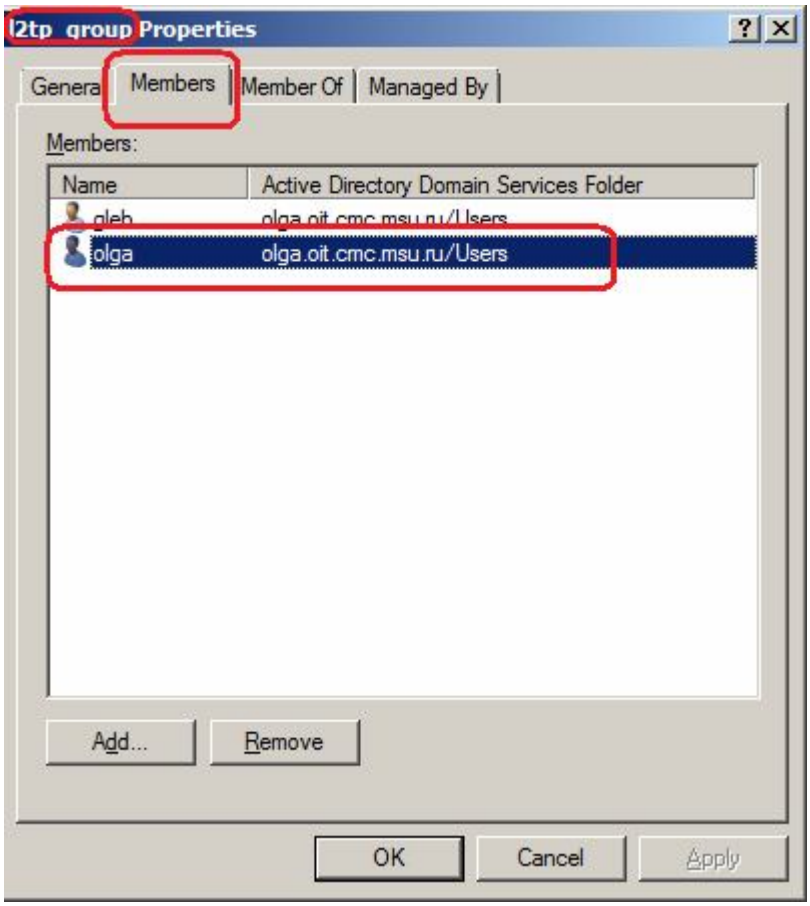
2. В политиках сети (Network Policies) перечислить группы, членам которых разрешен доступ.

На сервере RADIUS:



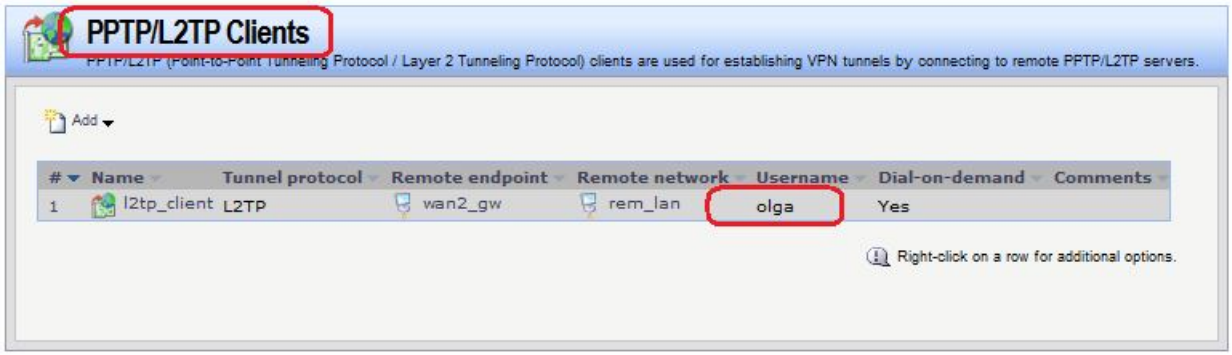
В данном примере члены группы **`l2tp_group`** могут быть указаны на аутентифицируемой стороне туннеля.

`Roles → Active Directory Users and Computers → Users → l2tp_group`



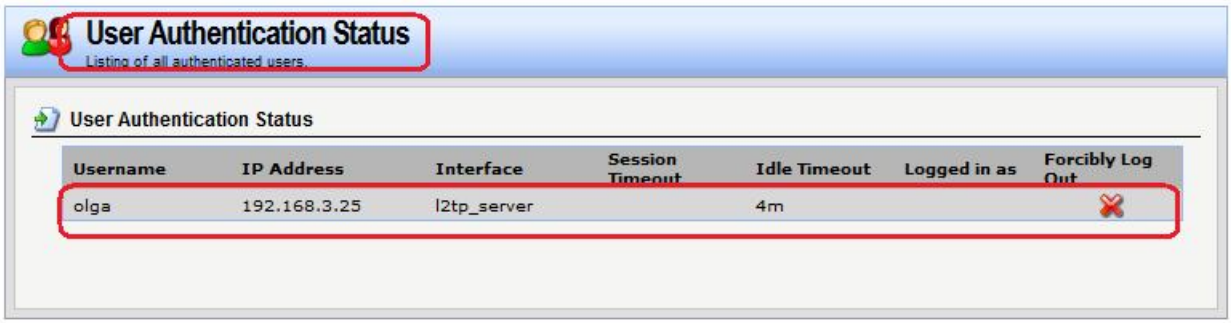
На аутентифицируемой стороне туннеля указывается имя пользователя:

`Interfaces → PPTP/L2TP Clients`



На стороне NAS проверяется, что аутентификация выполнена:

`Status → User Authentication`



NAS

Объекты Адресной Книги

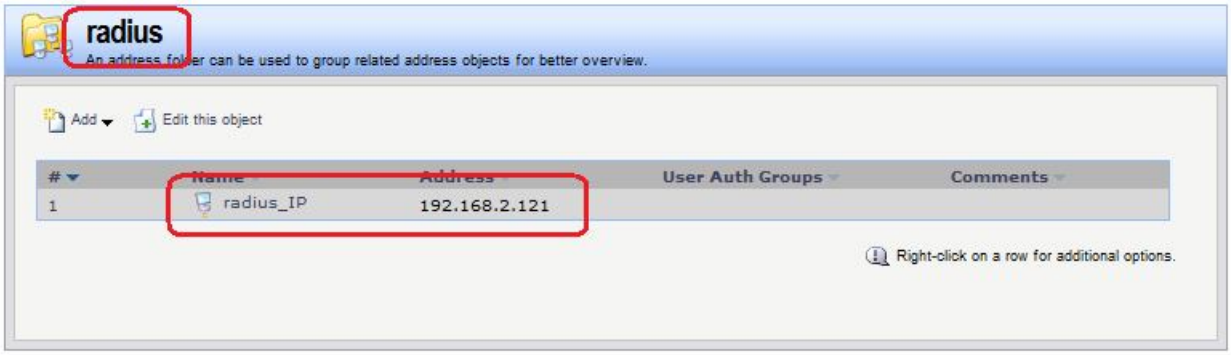
Создать объекты, описывающие IP-адреса RADIUS-серверов аутентификации и авторизации.

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`

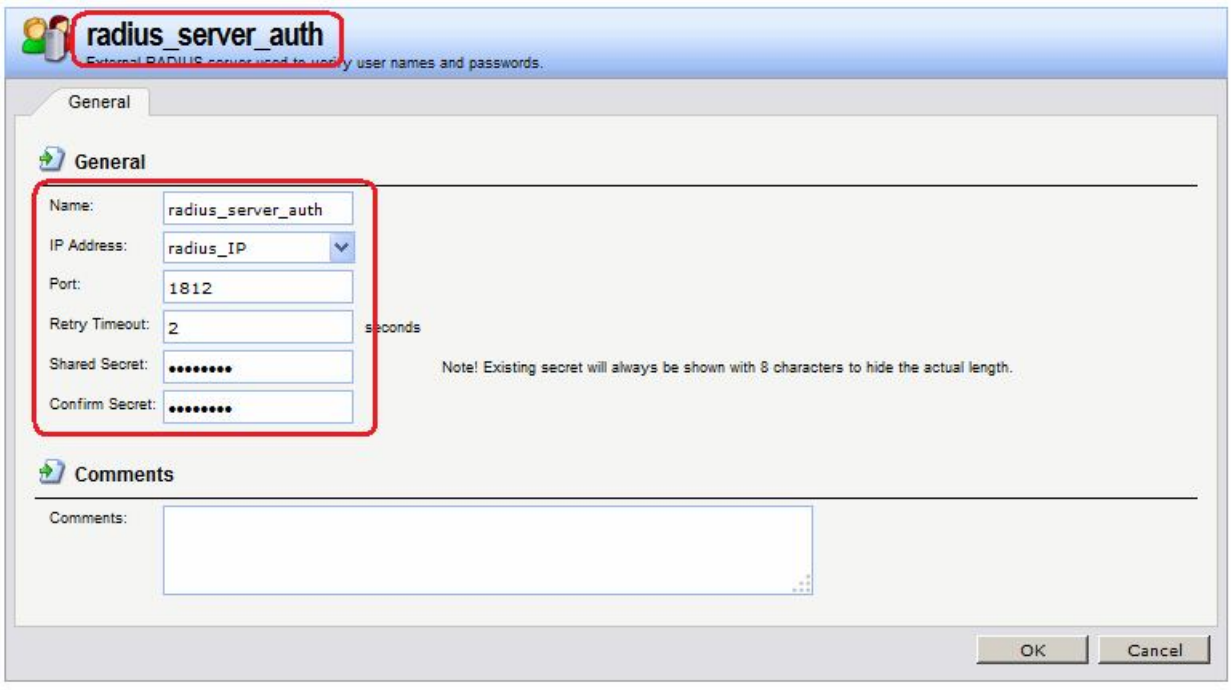
`add IP4Address radius_ip Address=192.168.2.121`

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`



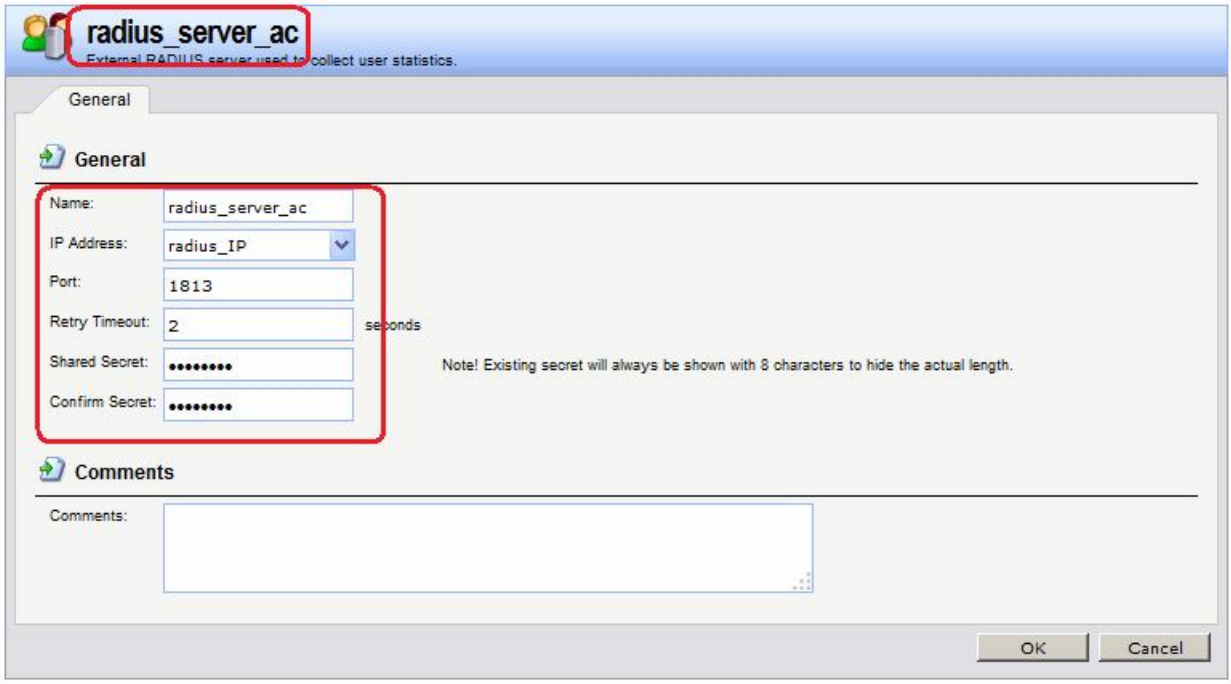
Командная строка:

```
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



Командная строка:

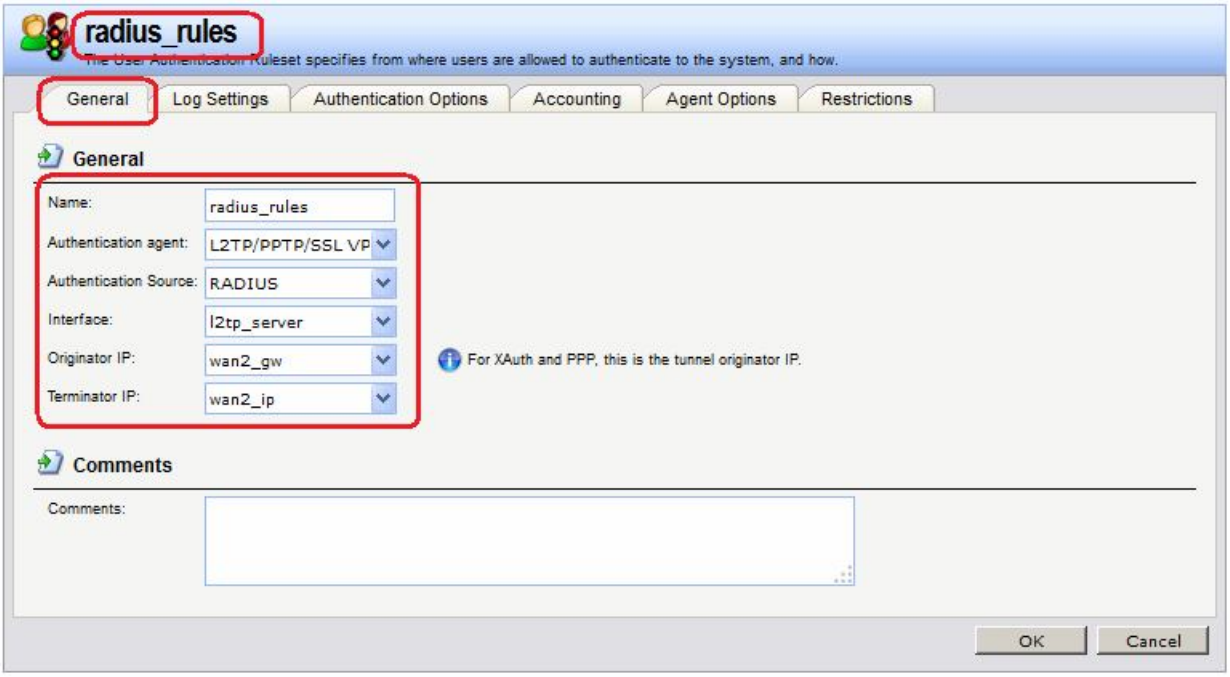
```
add RadiusAccounting radius_server_ac IPAddress=radius/radius_IP
SharedSecret=qwerty
```

Правила аутентификации

Указать правила аутентификации.

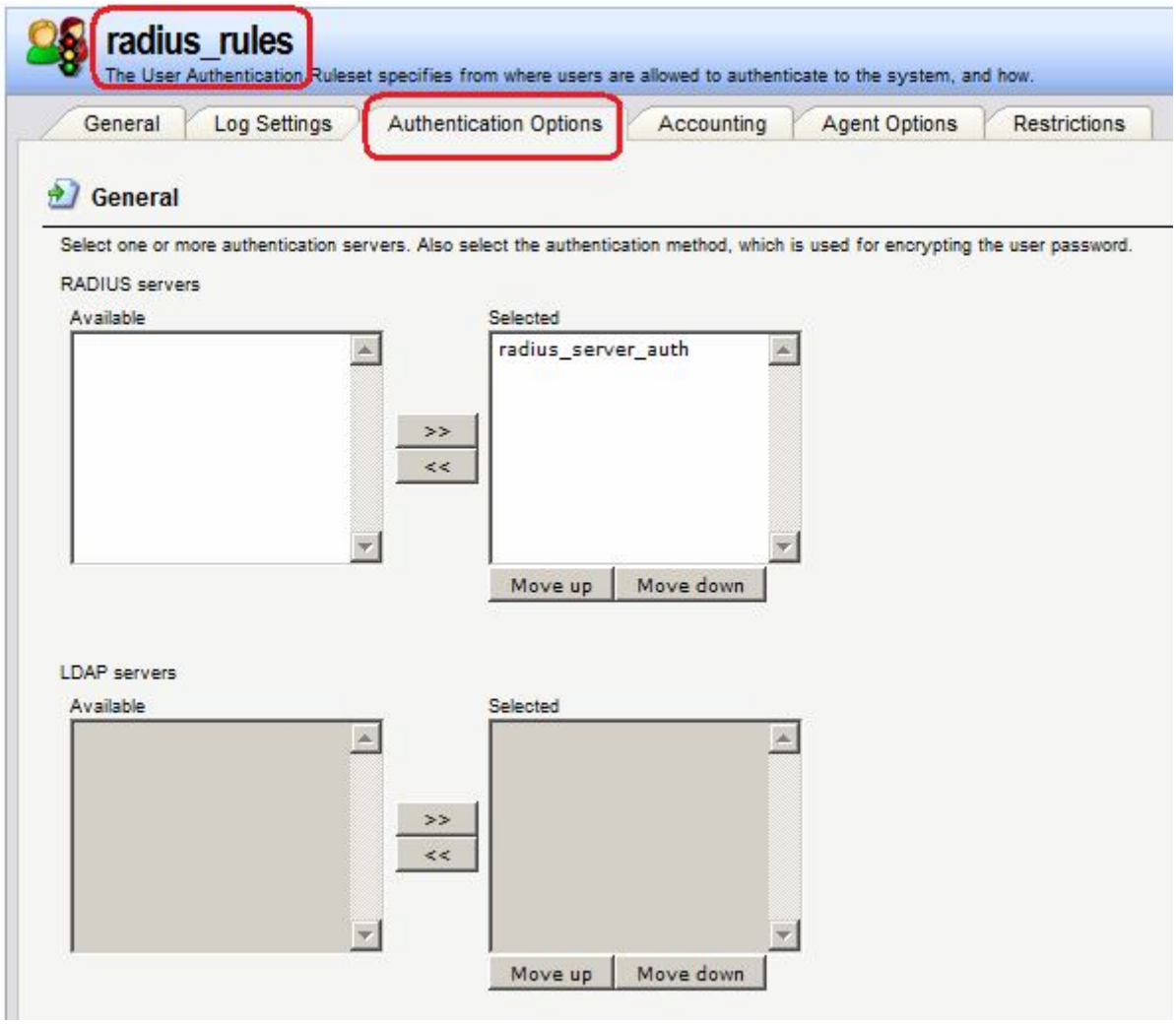
Веб-интерфейс:

User Authentication Rules → Add User Authentication Rule

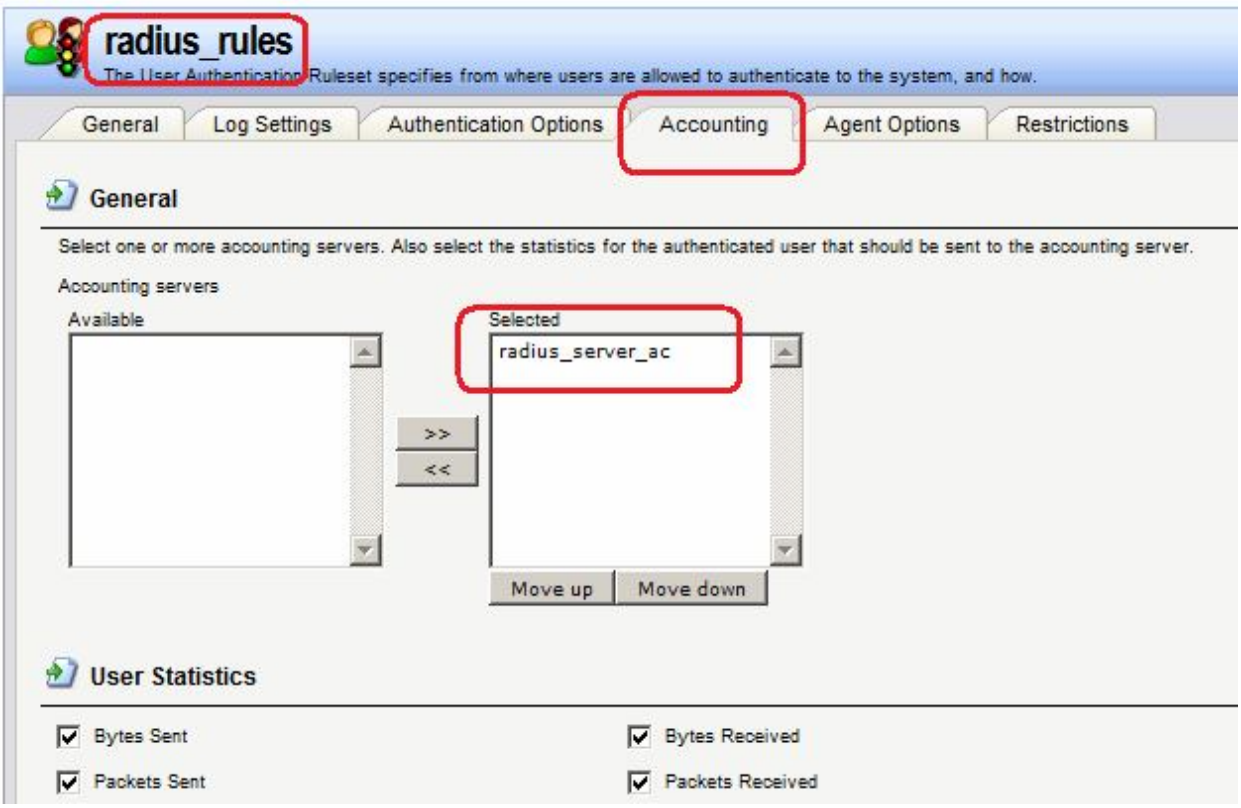


В качестве интерфейса указать интерфейс **`l2tp_server`**. В качестве исходного IP-адреса указать IP-адрес противоположной точки туннеля. В качестве IP-адреса завершения (**`Terminator IP`**) указать IP-адрес на локальной стороне.

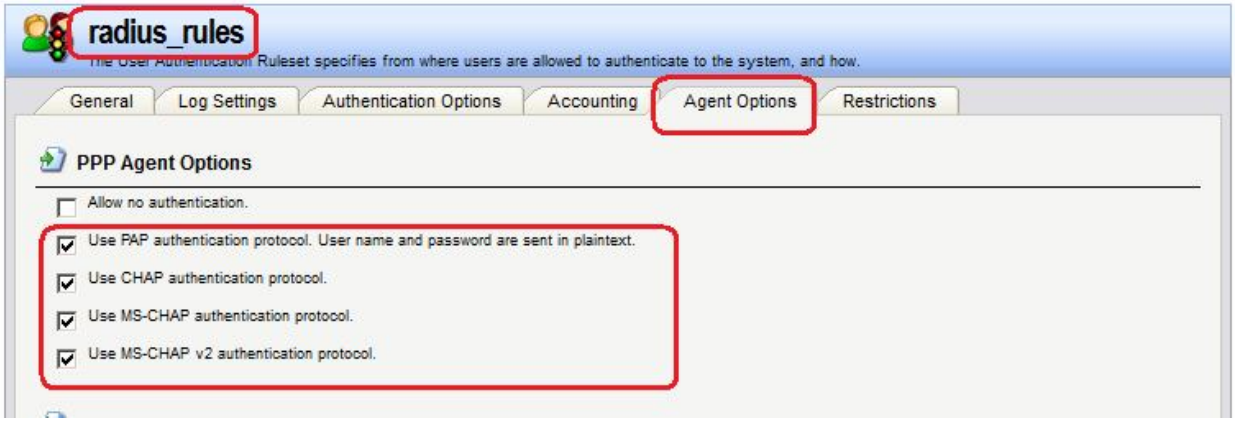
На вкладке **`Authentication Options`** выбрать созданный RADIUS-Сервер.



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



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



Командная строка:

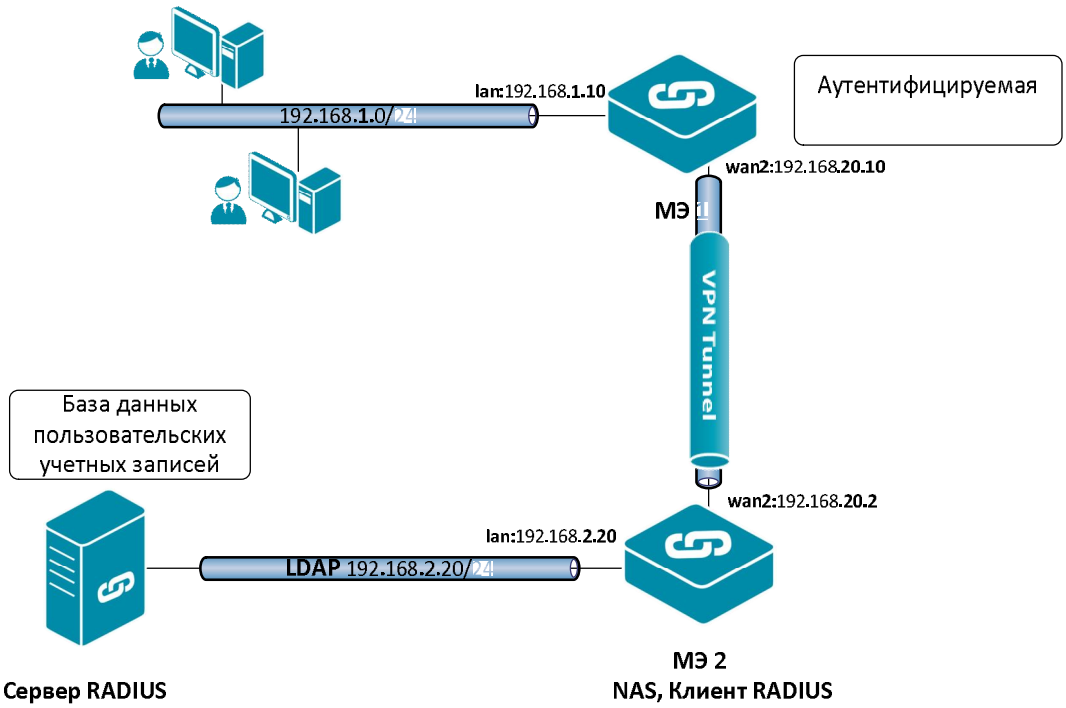
```
add UserAuthRule AuthSource=RADIUS Interface=l2tp
OriginatorIP=wan1/wan1_gwFW2 RadiusServers=W2K8_radius Agent=PPP
TerminatorIP=wan1/wan1_ipFW2 AccountingServers=W2K8_radius Name=l2tp_radius
```

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

Цель

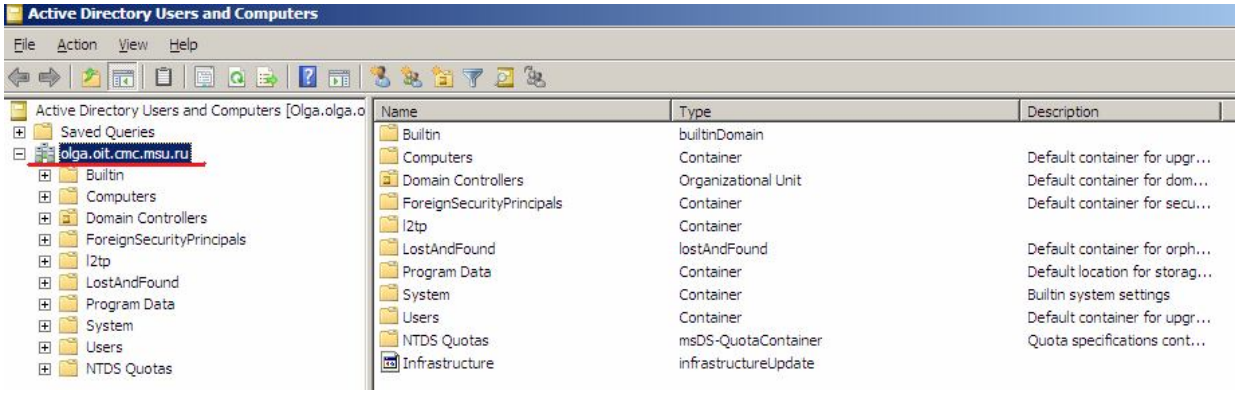
Учетные записи пользователей хранятся в MS AD сервере.

Топология сети



Описание практической работы

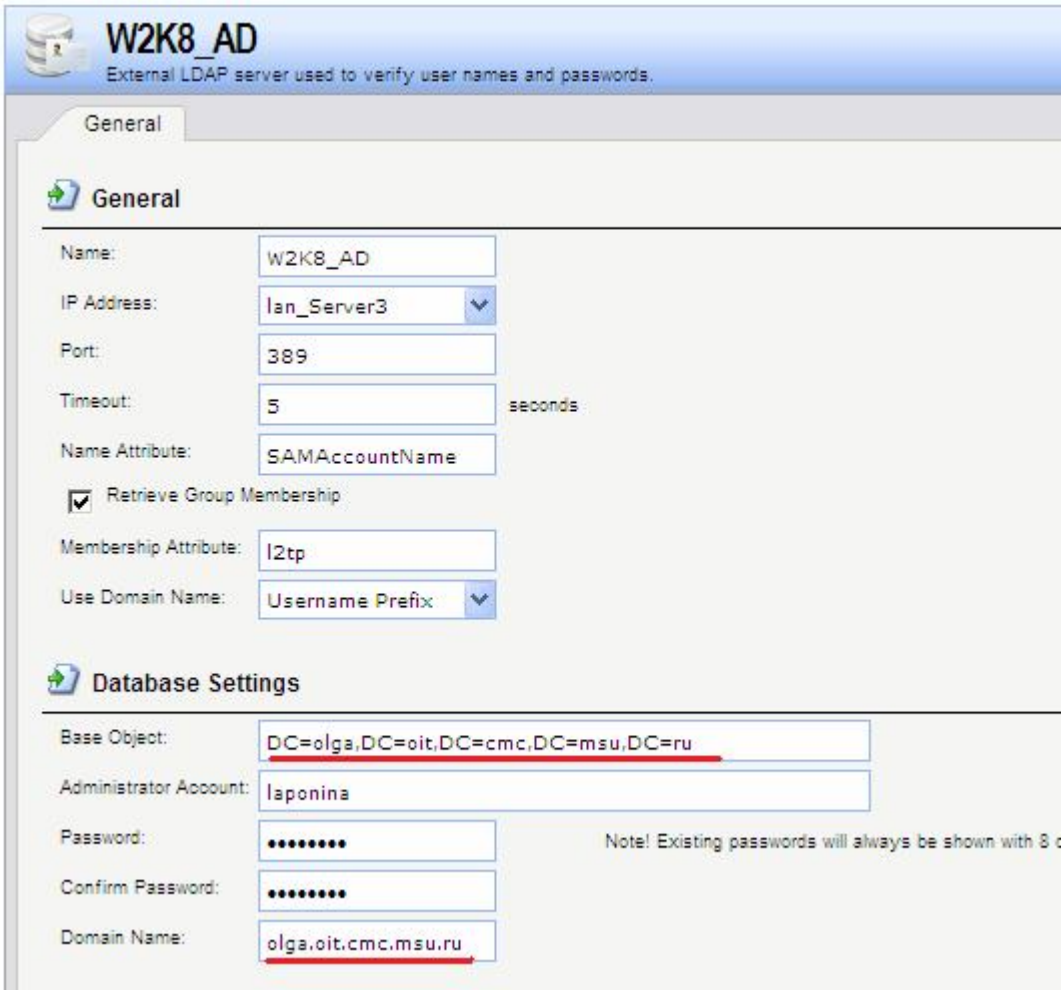
1. Создать AD с DNS-именем olga.oit.cmc.msu.ru



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

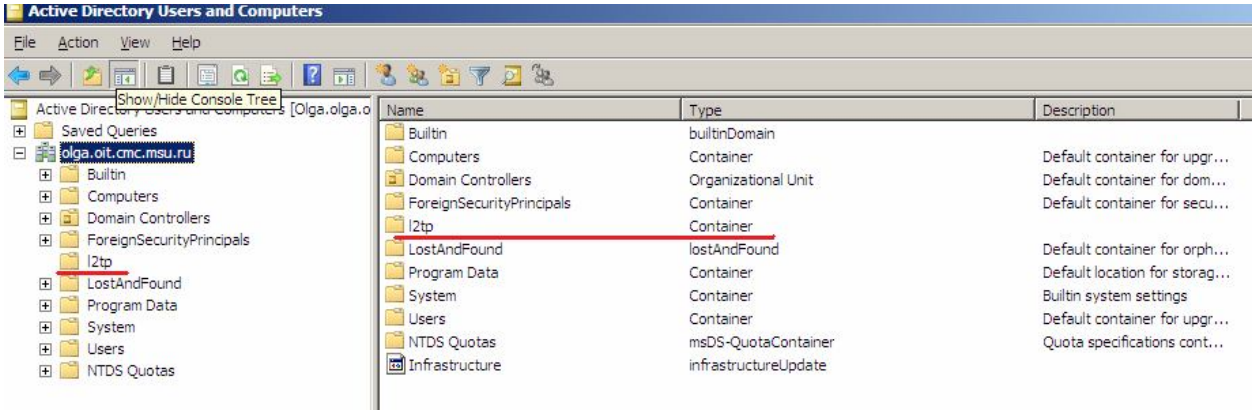
Веб-интерфейс:

`User Authentication → External User Databases → Add → LDAP Server`

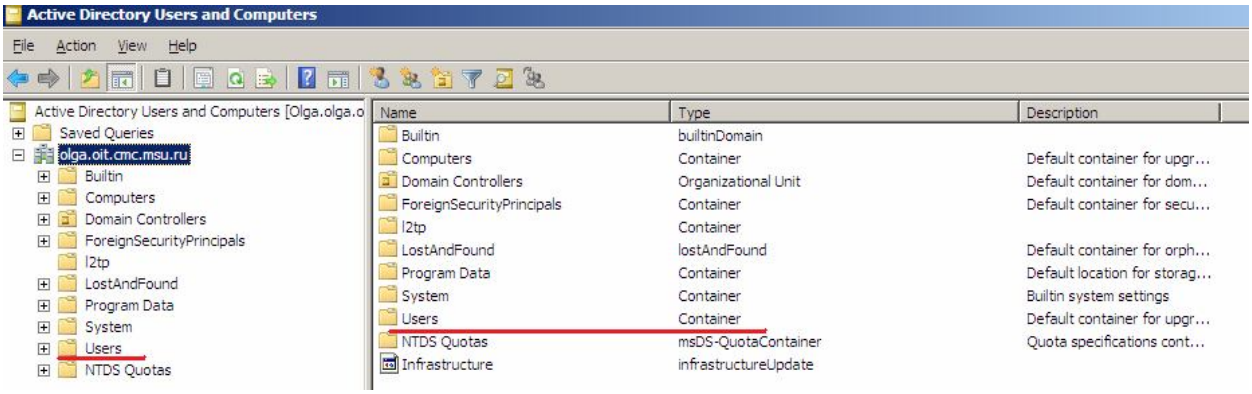


В поле **`Base Object`** DNS-имя указано в формате DN, в поле **`Domain Name`** в формате DNS.

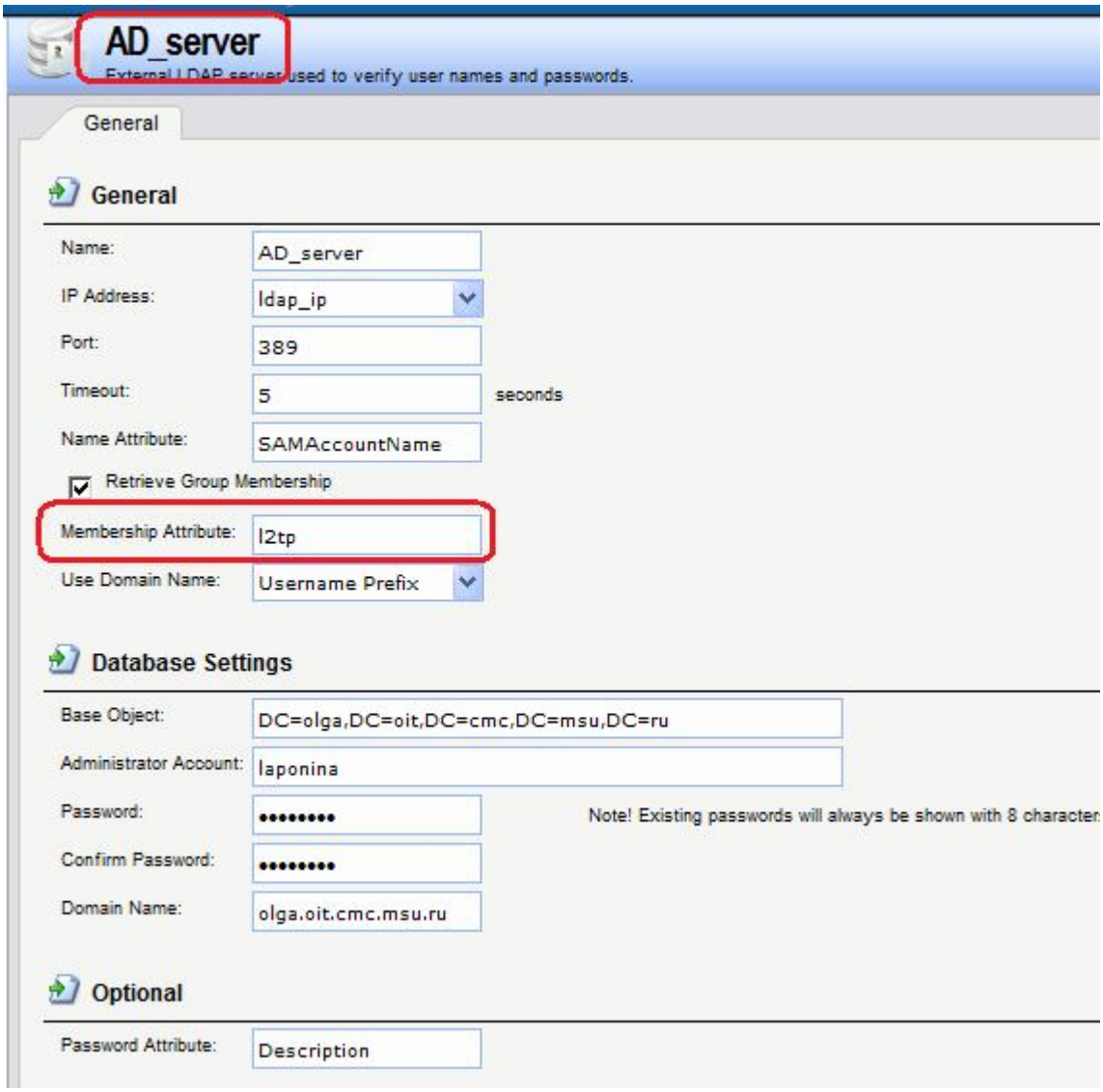
3. В AD создать контейнер хранения учетных записей удаленных пользователей.



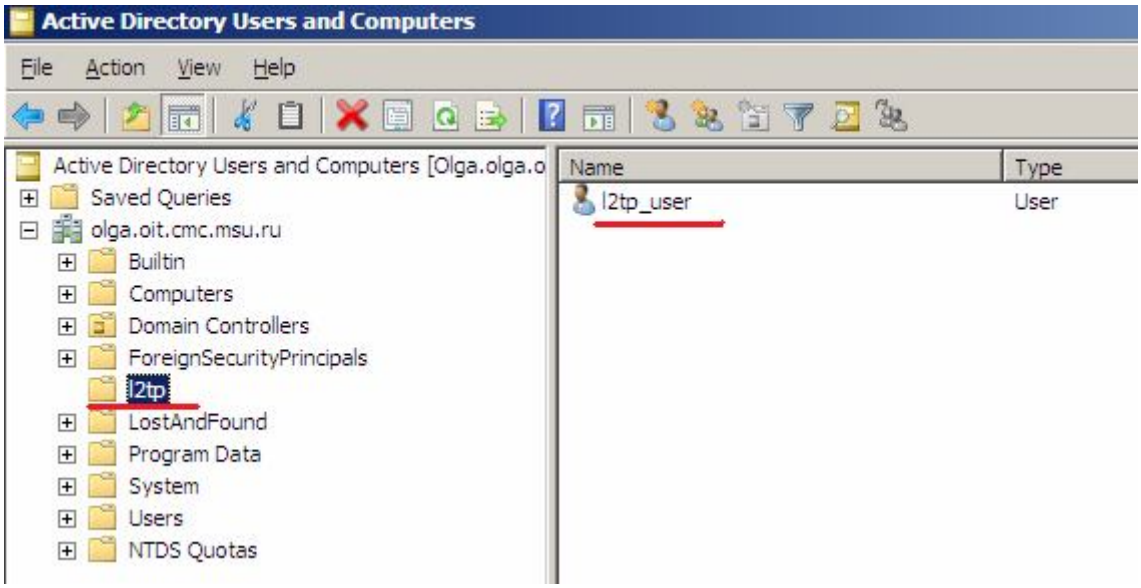
Или использовать существующий контейнер, например, **`Users`**:



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



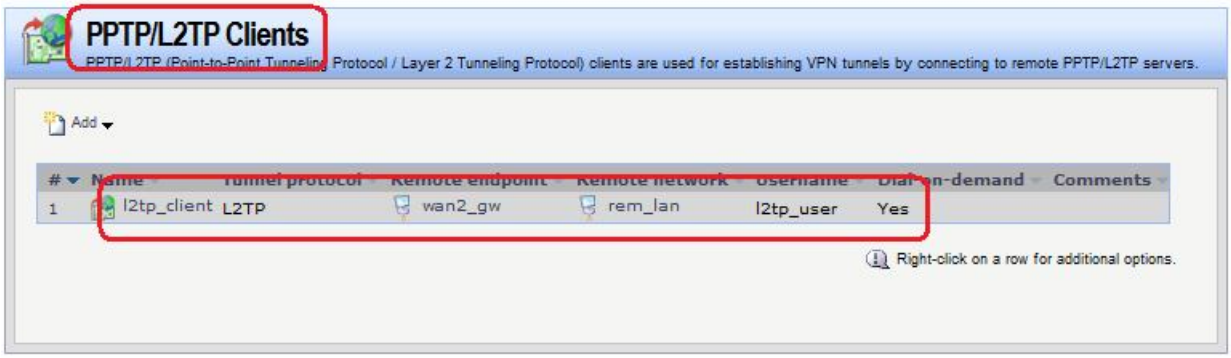
4. В выбранном контейнере создать пользователя, в нашем случае создается пользователь **`l2tp_user`** в контейнере **`l2tp`**.



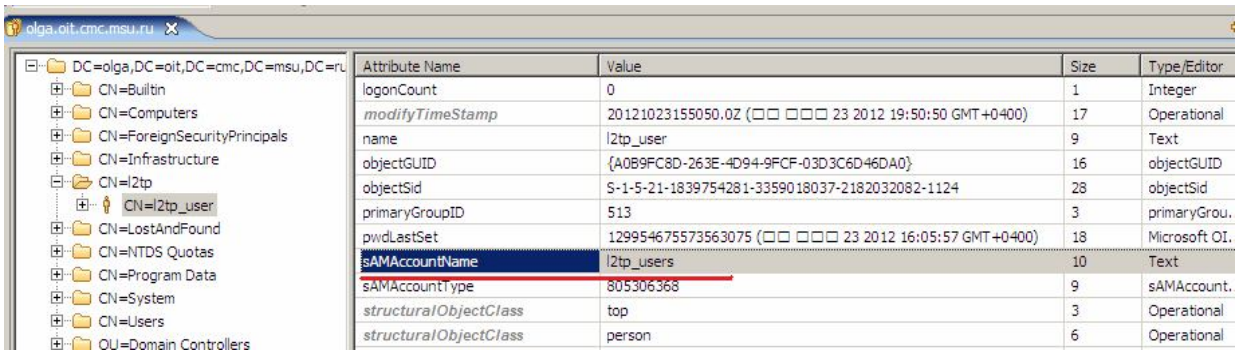
5. Имя этого пользователя указывается на противоположной стороне туннеля (в нашем случае на стороне L2TP-клиента).

Веб-интерфейс:

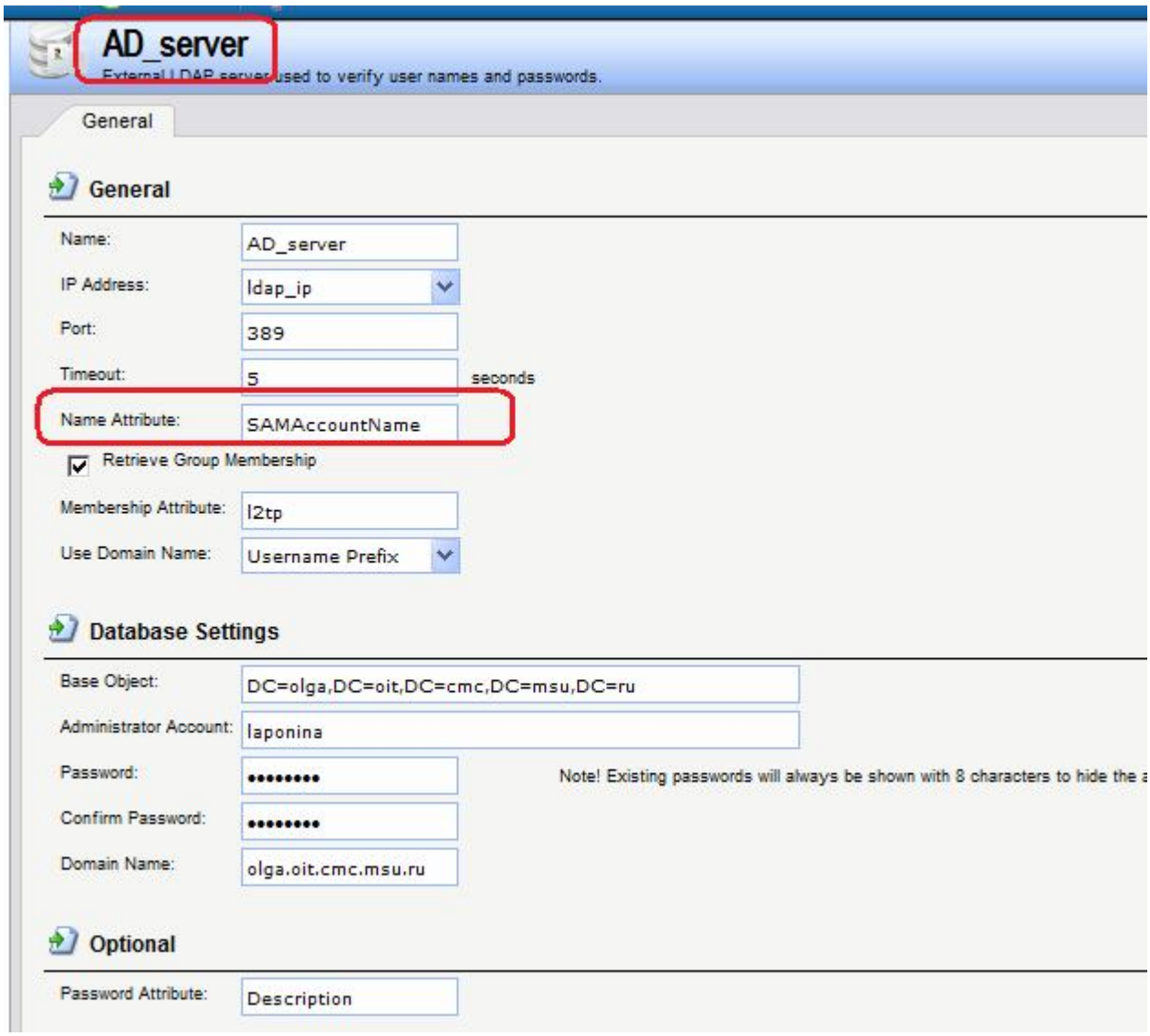
`Interfaces → PPTP/L2TP Clients → Add → PPTP/L2TP Client`



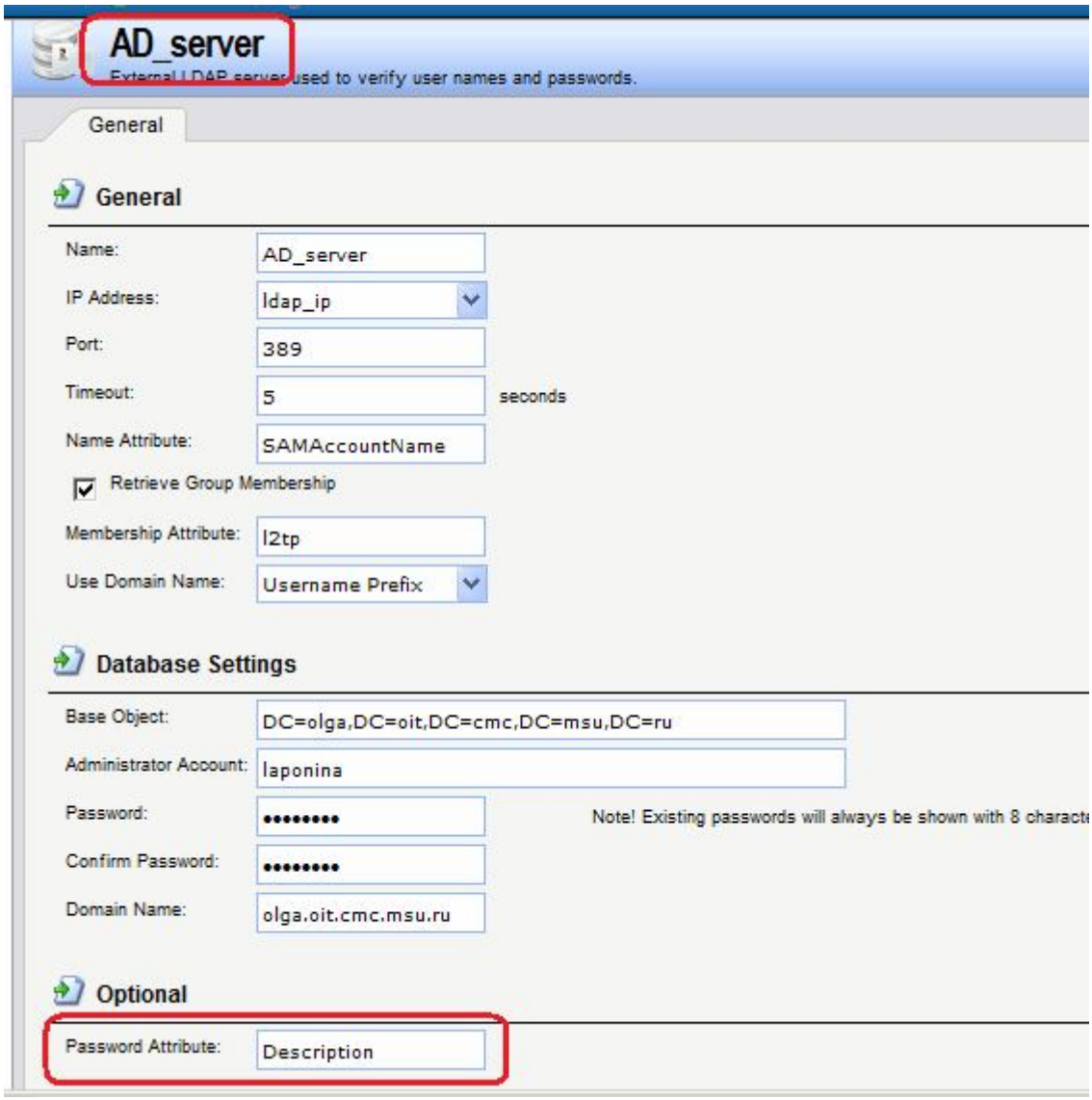
6. Имя пользователя в AD является значением атрибута **`sAMAccountName`**.



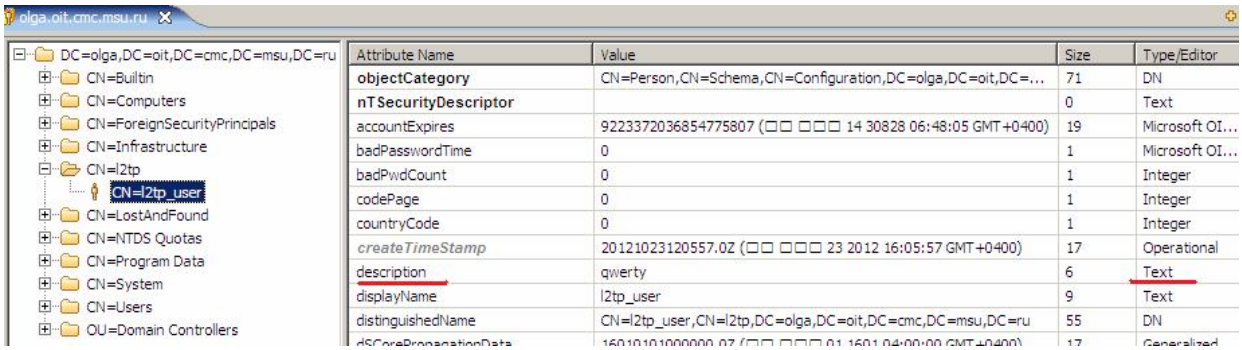
7. Имя этого атрибута указывается в поле **`Name Attribute`** в параметрах создания внешней базы данных пользователей на межсетевом экране.



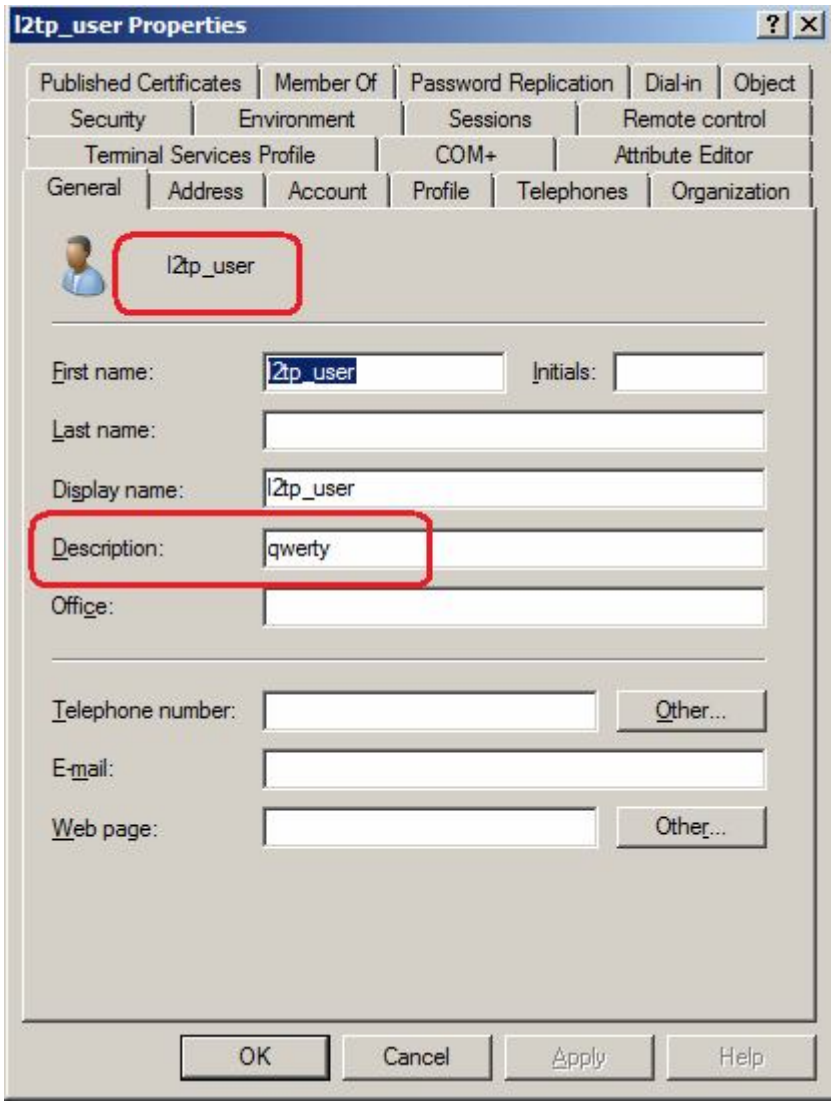
8. Аутентификация противоположной стороны туннеля (в нашем случае L2TP-клиента) выполняется по значению поля, имя которого указано в поле **`Password Attribute`** в параметрах создания внешней базы данных пользователей на межсетевом экране.



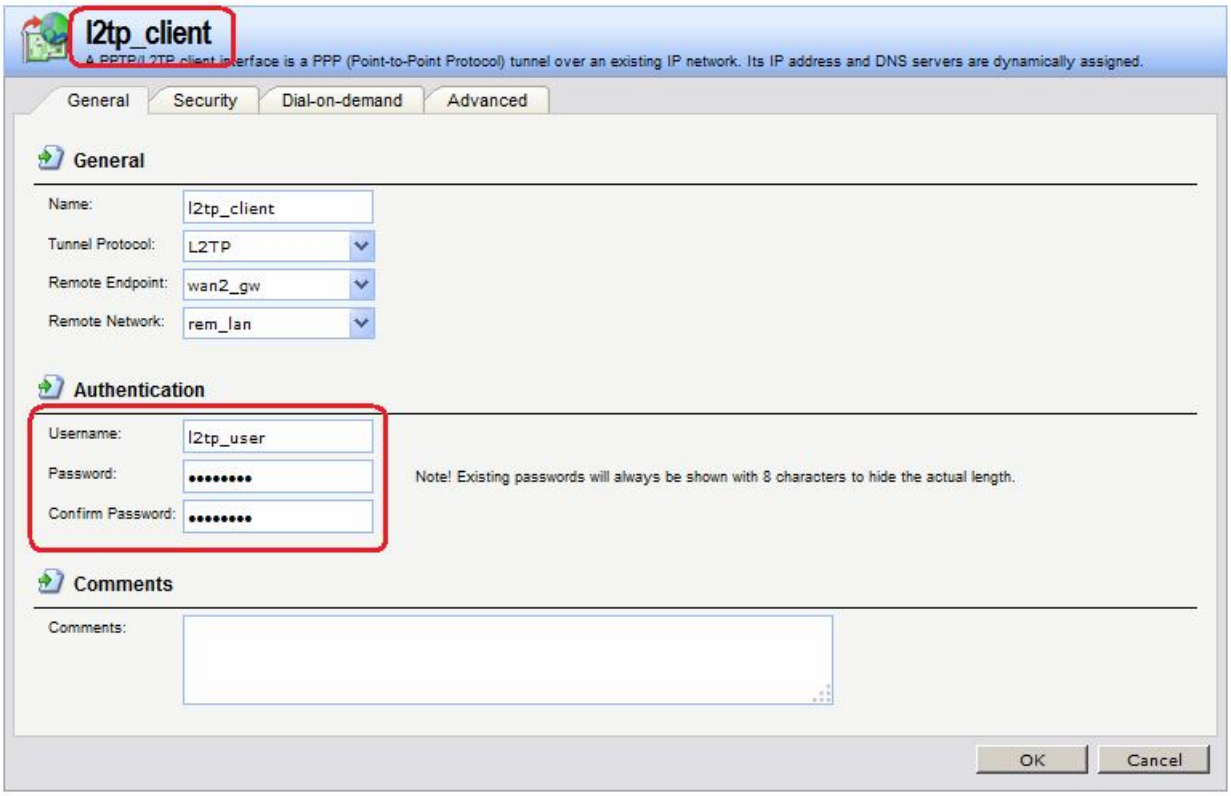
9. Тип этого поля должен быть **`Text`**.



10. Значение поля указывается в AD.



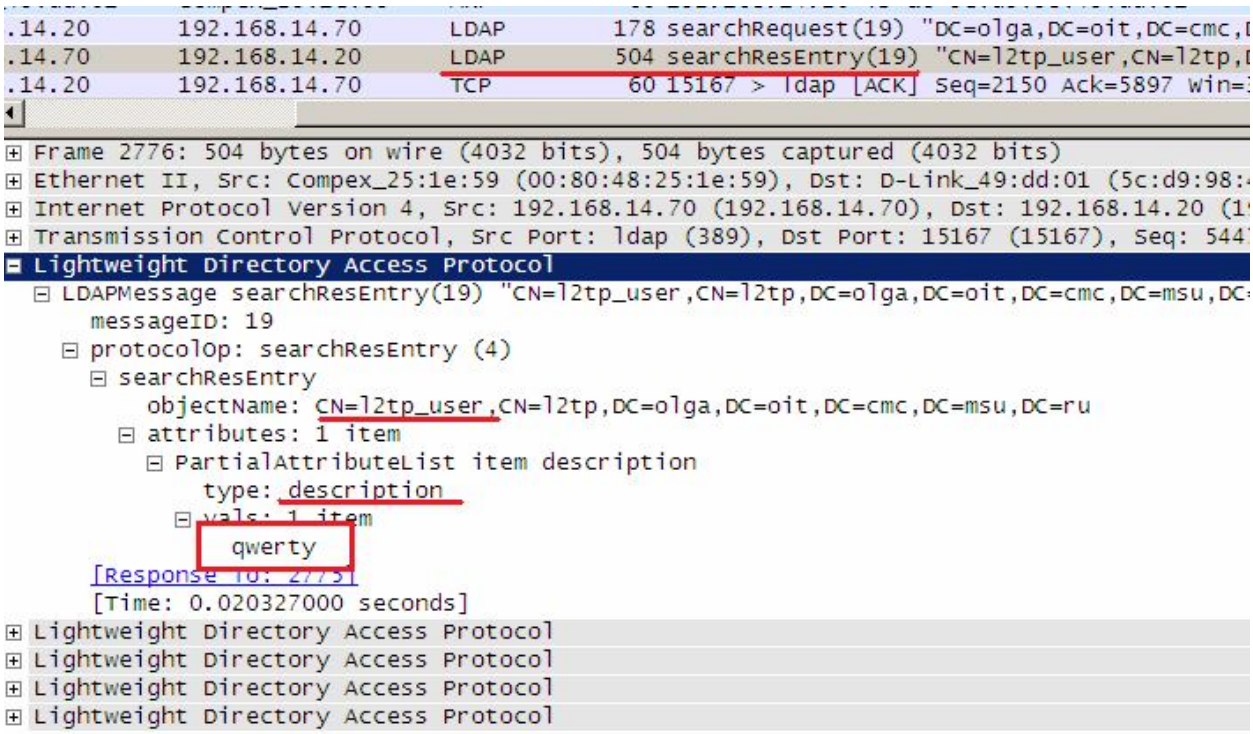
11. И на противоположной стороне туннеля (в нашем случае L2TP-клиента) в качестве значения пароля.



К AD посылается следующий запрос:

```
6334 7169.97368 192.168.14.20   192.168.14.70   LDAP   179 searchRequest(51) "DC=olga,D
6335 7169.97407 192.168.14.70   192.168.14.20   LDAP   505 searchResEntry(51) "CN=l2tp
⊞ Frame 6334: 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits)
⊞ 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 (192.168.14.7
⊞ Transmission Control Protocol, Src Port: 16006 (16006), Dst Port: ldap (389), Seq: 5850, Ack: 215
⊟ 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=l2tp_users)
          ⊟ filter: equalityMatch (3)
            ⊟ equalityMatch
                attributeDesc: SAMAccountName
                assertionValue: l2tp_users
        ⊟ attributes: 2 items
            AttributeDescription: Description
            AttributeDescription: l2tp
      [Response In: 6335]
```

Ответ от AD следующий:



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.

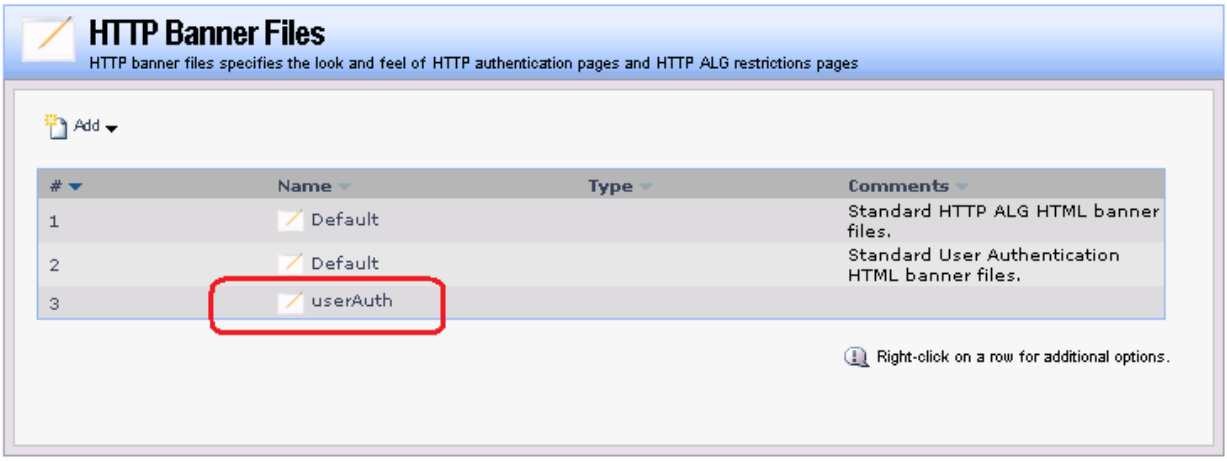
Оба эти способа аутентификации не обеспечивают конфиденциальность, поэтому их следует использовать только тогда, когда политика безопасности допускает возможность пассивных атак, либо когда используется туннелирование на более низком уровне стека протоколов.

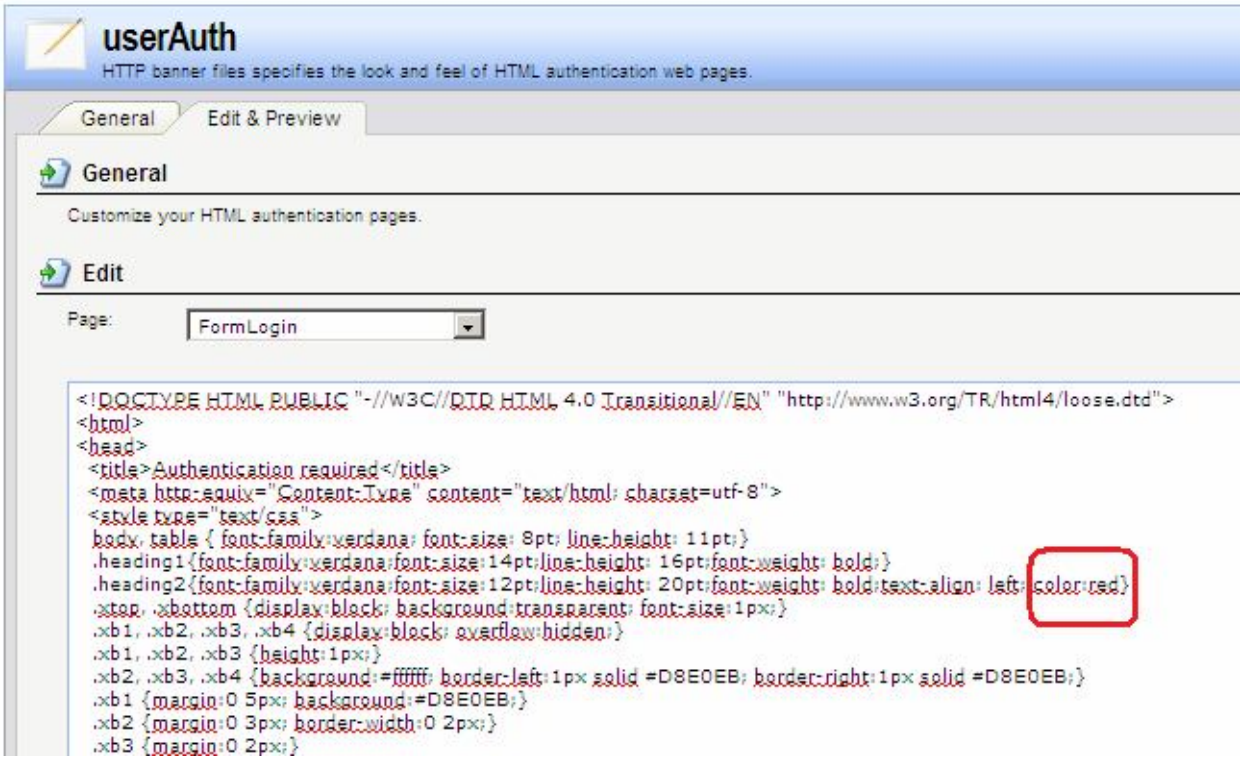
Можно отредактировать существующую HTML-форму или создать собственную.

Веб-интерфейс:

Object → HTTP Banner Files → Add

Name: userAuth





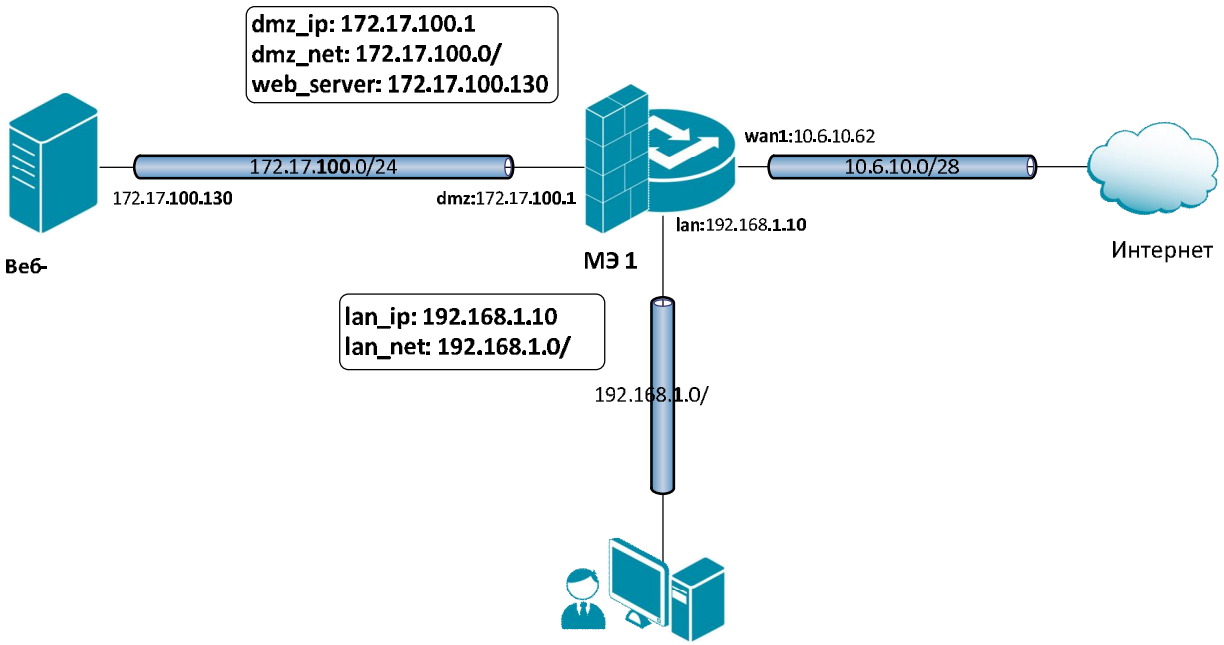
Командная строка:

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

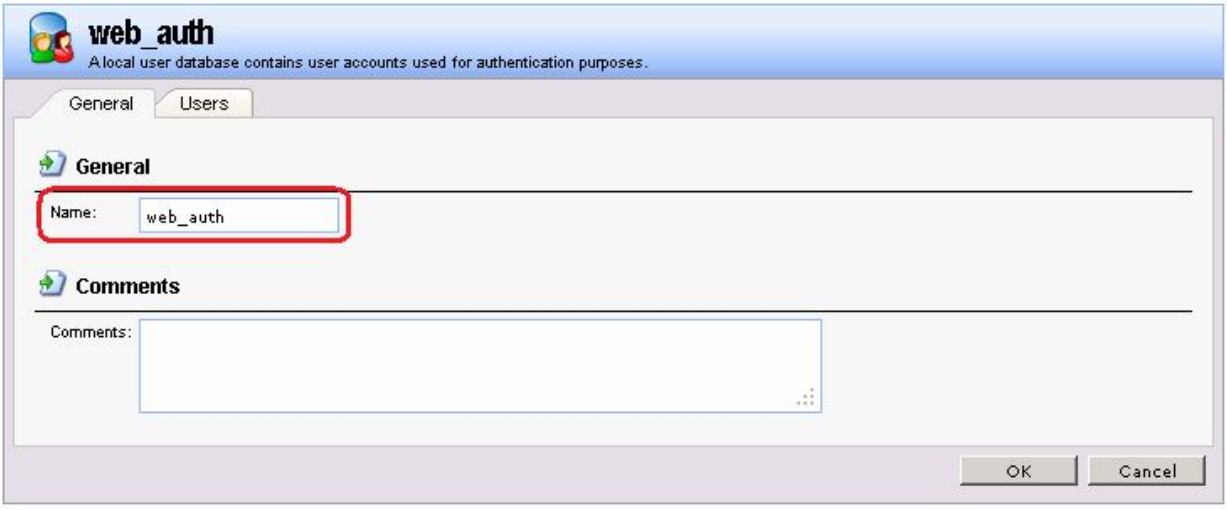
Правила аутентификации пользователей

1. Создание локальной базы данных пользователей.

Веб-интерфейс:

`User Authentication → Local User Databases → Add`

`Name: web_auth`



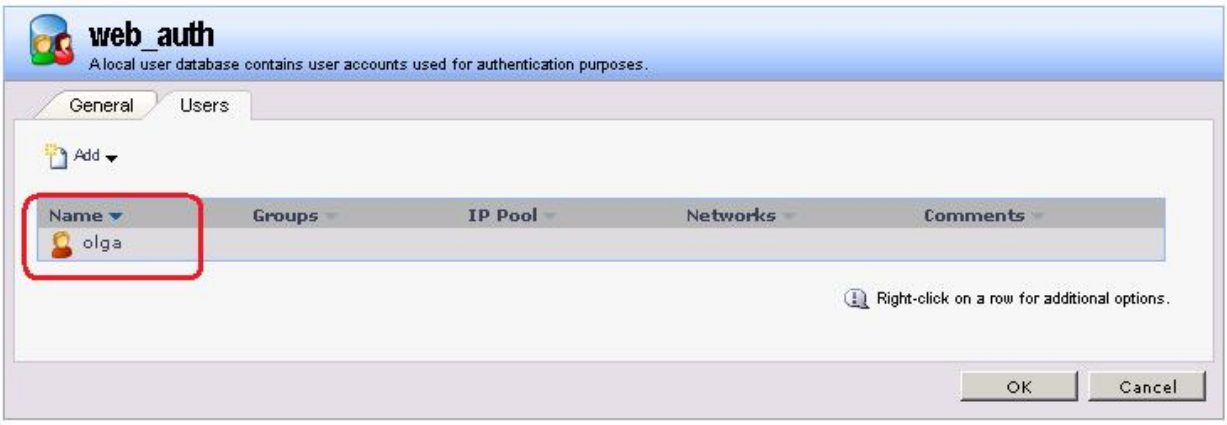
`User Authentication → Local User Databases → web_auth`

Вкладка **`Users → Add`**

Командная строка:

```
add LocalUserDatabase web_auth
cc LocalUserDatabase web_auth
```

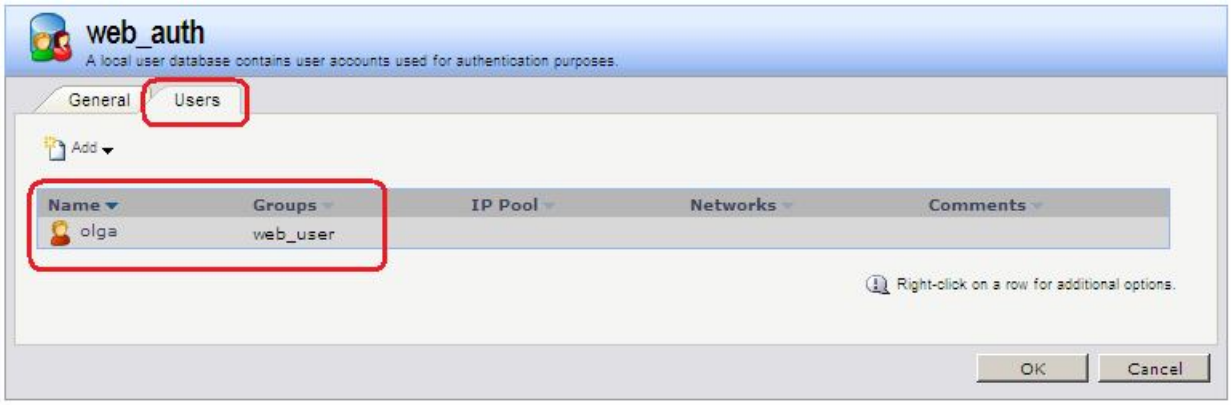
При использовании идентификатора пользователя:



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:

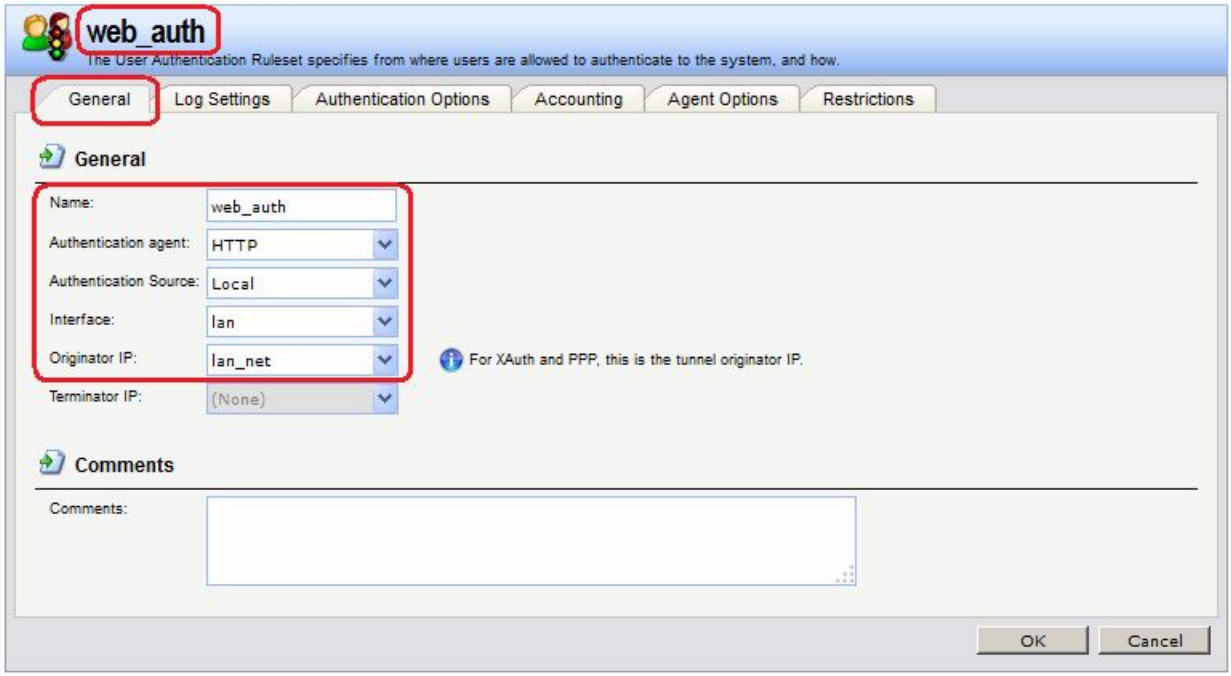
```
add User olga Password=qwerty Groups=web_user
```

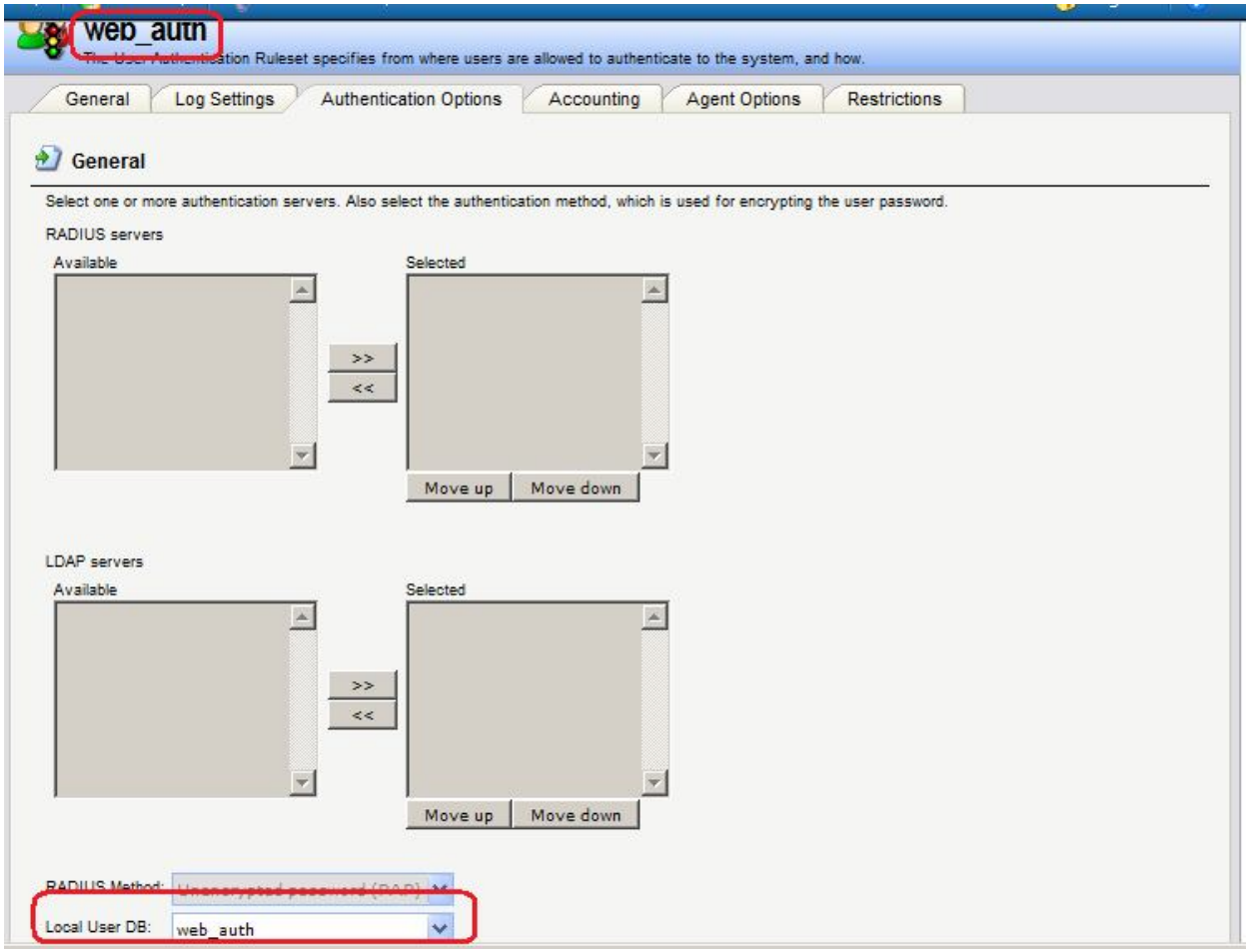
2. Создание правила аутентификации пользователей.

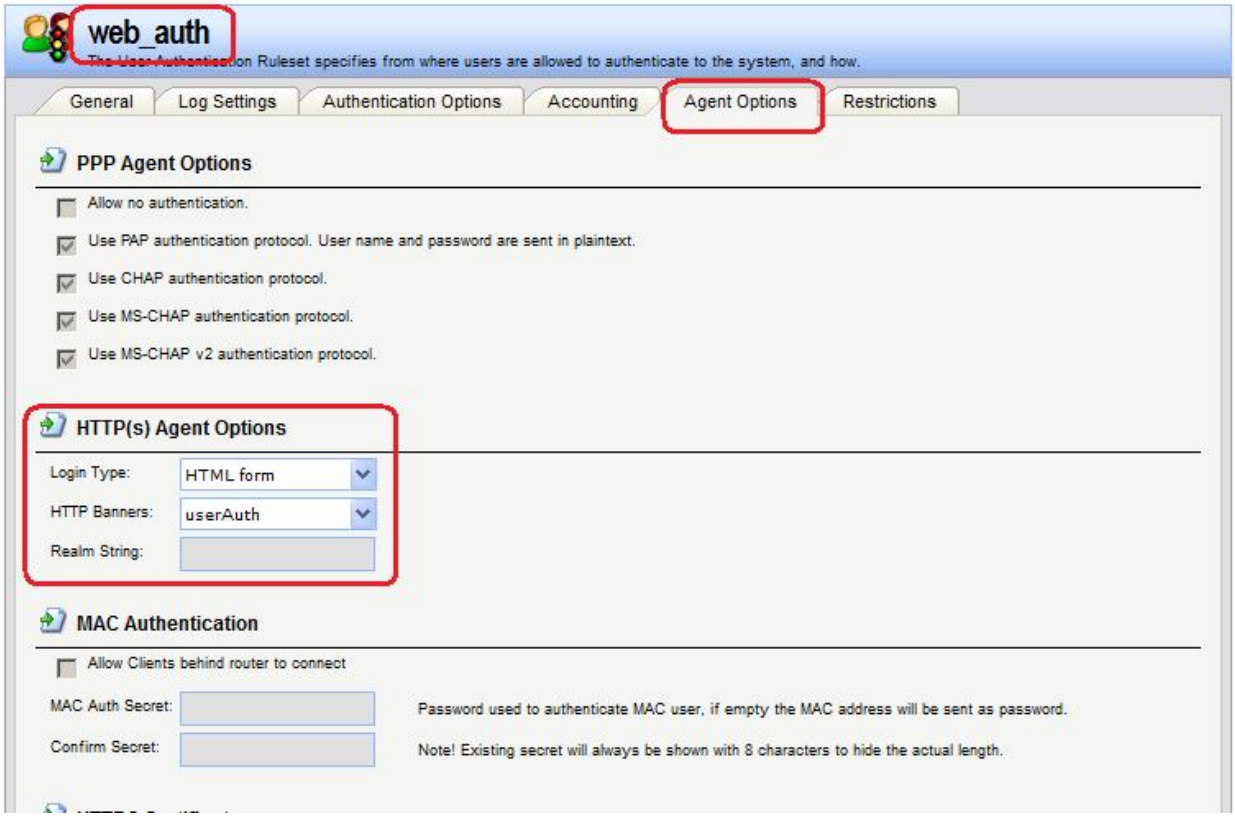
Веб-интерфейс:

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
For XAuth and PPP, this is the tunnel originator IP.
Terminator IP:
(None)
Comments
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
>>
<<
Move up
Move down
LDAP servers
Available
Selected
>>
<<
Move up
Move down
RADIUS Method:
Local User DB:
web_auth



Командная строка:

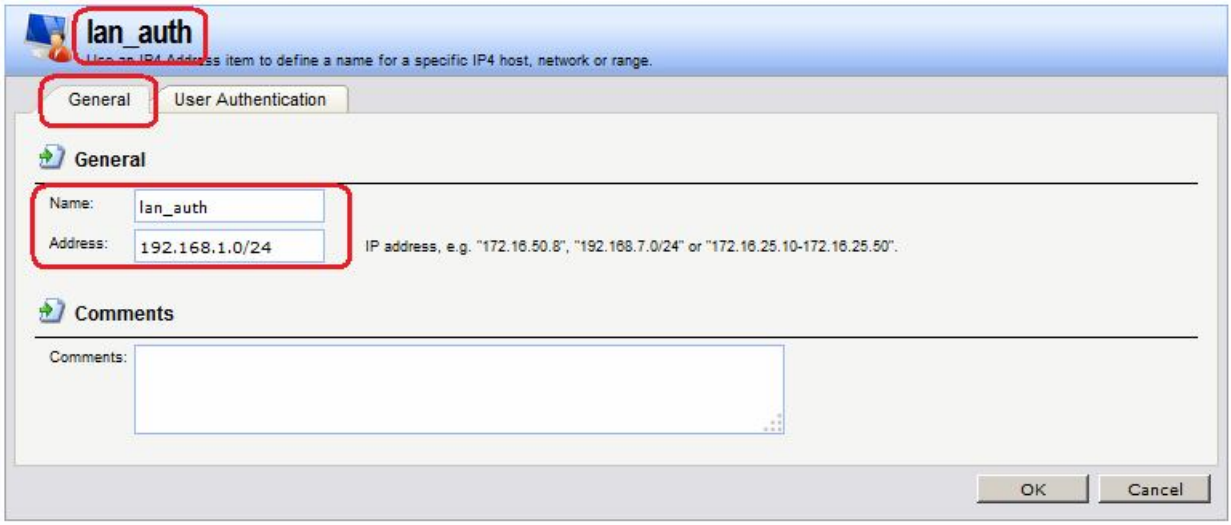
```
add UserAuthRule Interface=lan AuthSource=Local LocalUserDB=web_auth
OriginatorIP=lan/lan_net LoginType=HTMLForm HTTPBanners=userAuth
Name=web_auth Agent=HTTP
```

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

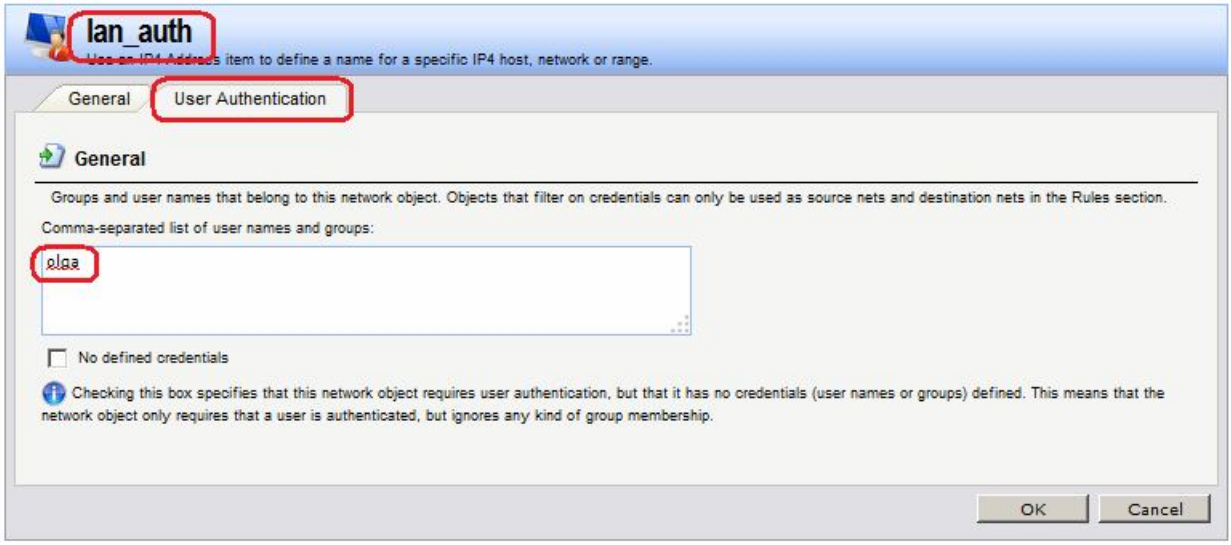
Веб-интерфейс:

`Object → Address Book → web_auth → Add`

`Name: lan_auth`



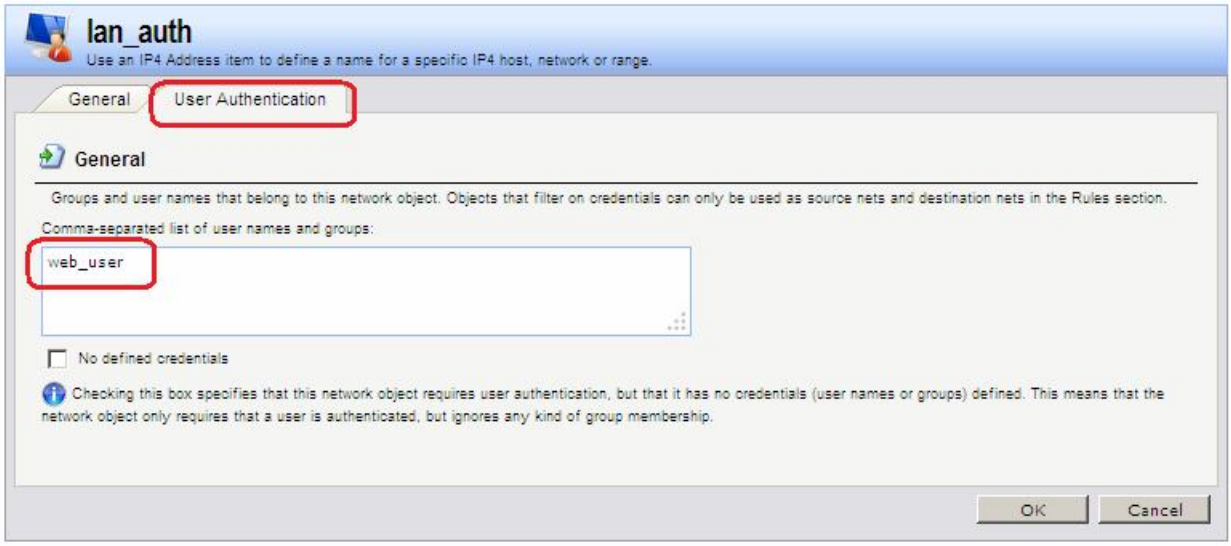
На вкладке **`User Authentication`** указать идентификатор пользователя:



Командная строка:

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

Использование идентификатора группы:



Командная строка:

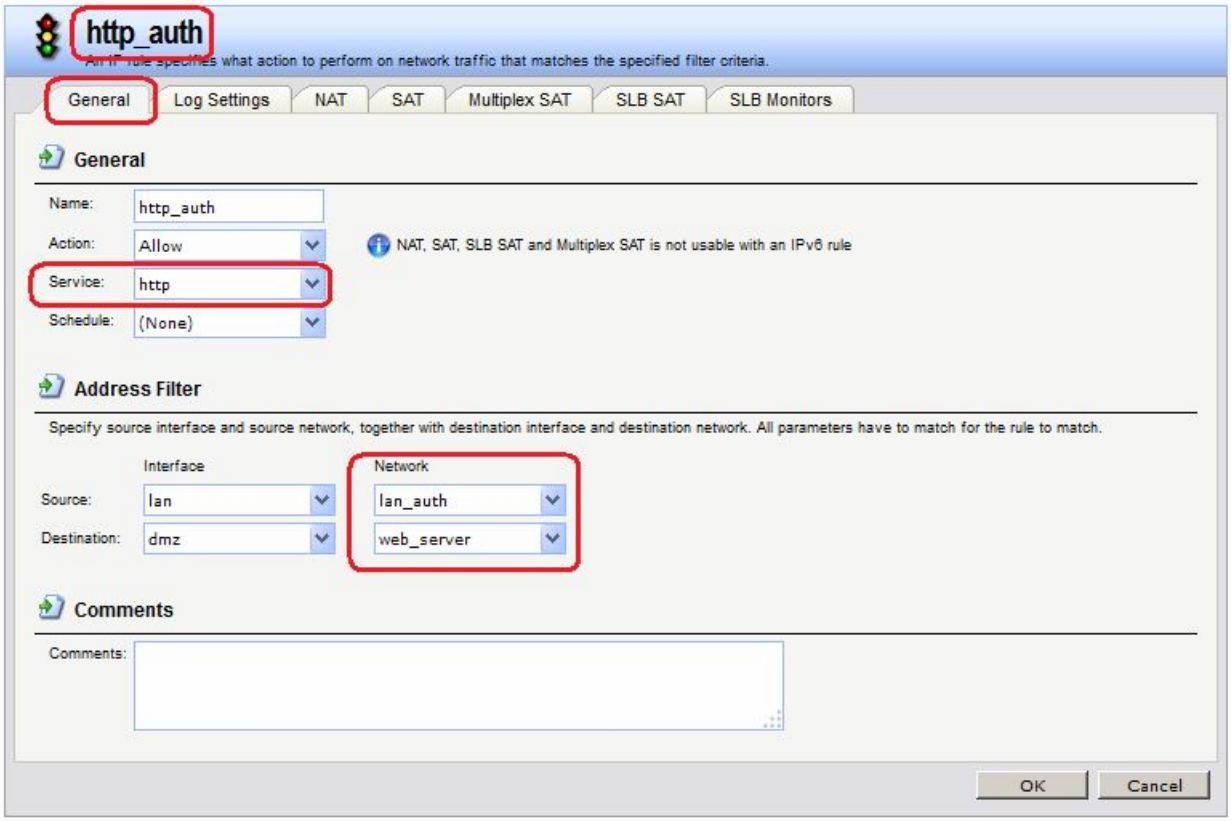
```
cc Address AddressFolder local_lan
add IP4Address lan_auth Address=192.168.12.0/24 UserAuthGroups=web_user
```

Правила фильтрования

а) 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
```



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
```

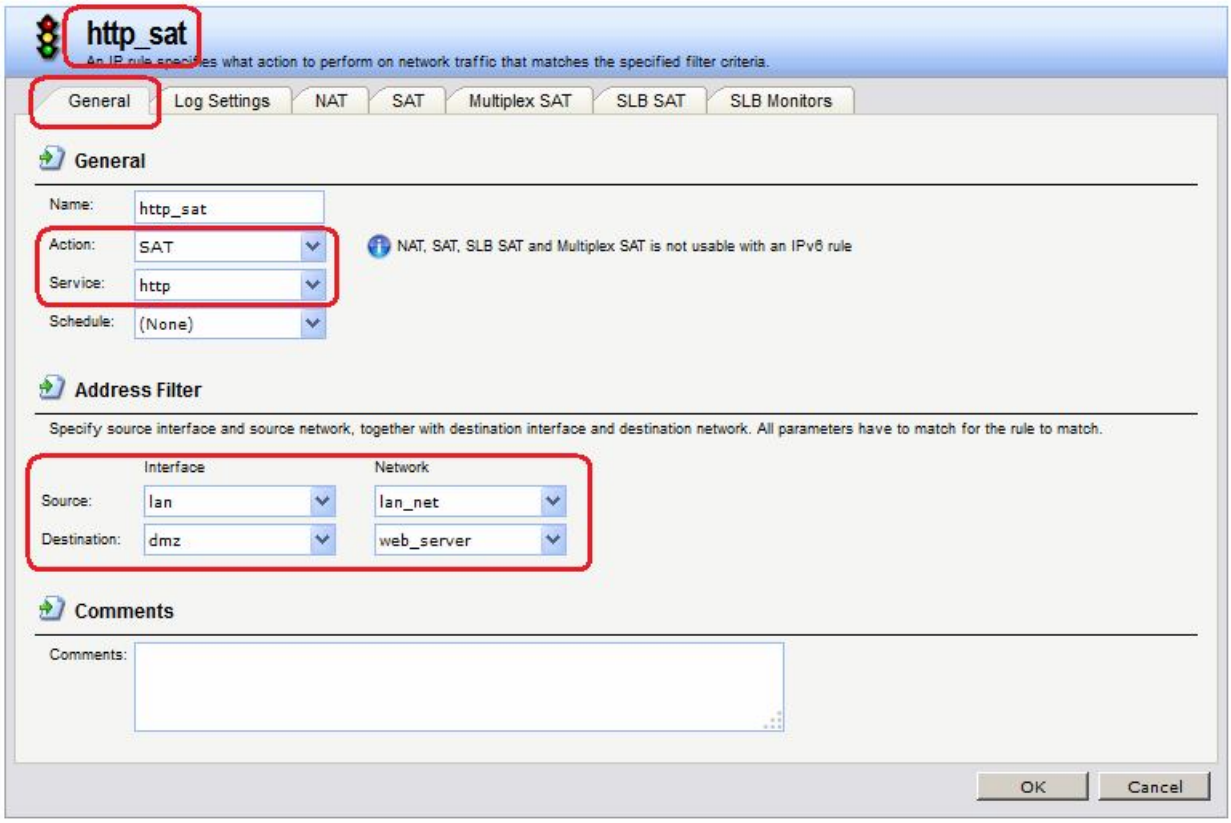
b) Правило, перенаправляющее неаутентифицированных пользователей на межсетевой экран для прохождения аутентификации.

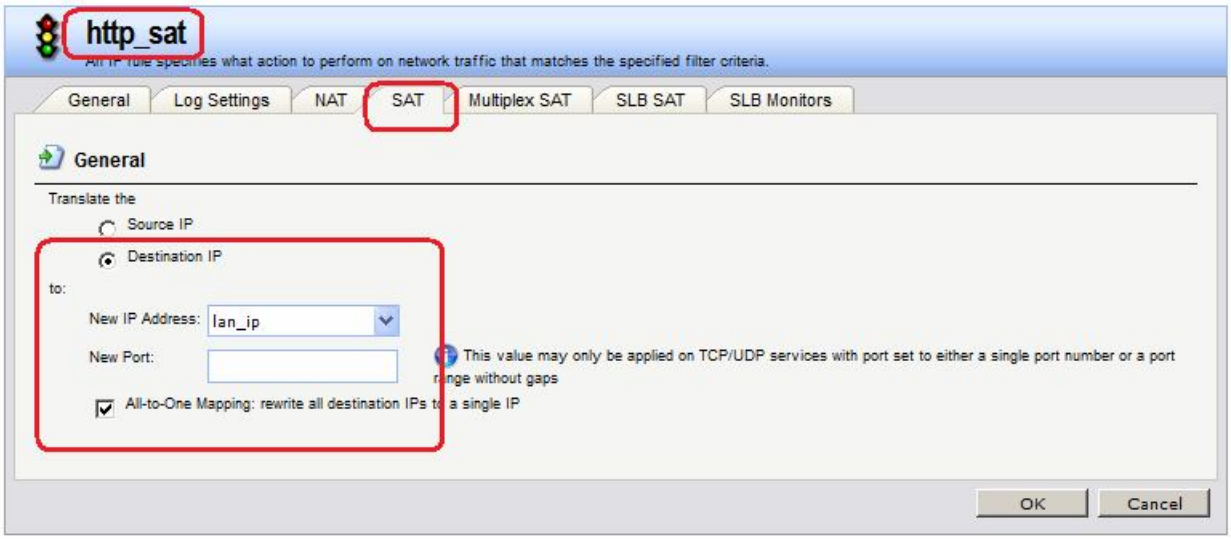
Веб-интерфейс:

Rules → IP Rules → web_auth → Add

Name: http_sat

Rules → IP Rules → web_auth → http_sat





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
```

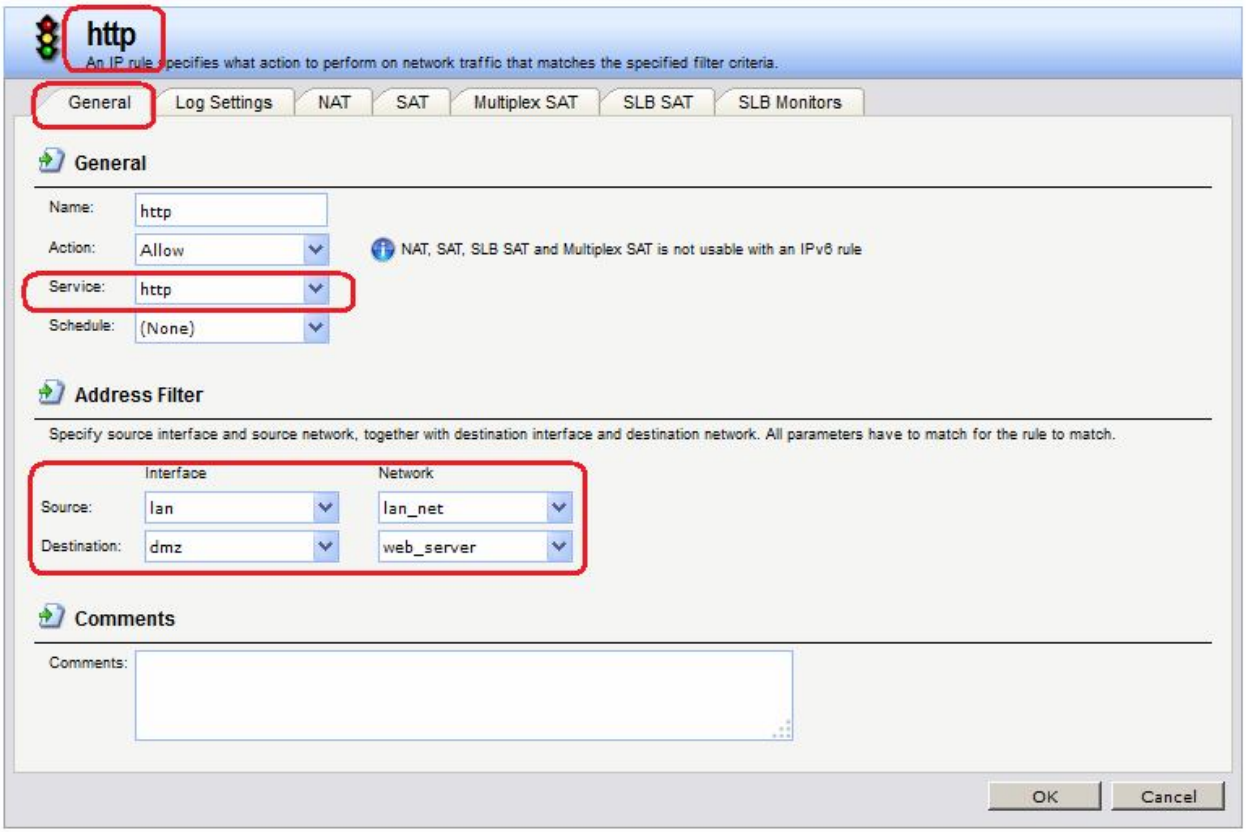
c) Правило, разрешающее трафик для выполнения аутентификации пользователей.

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
```

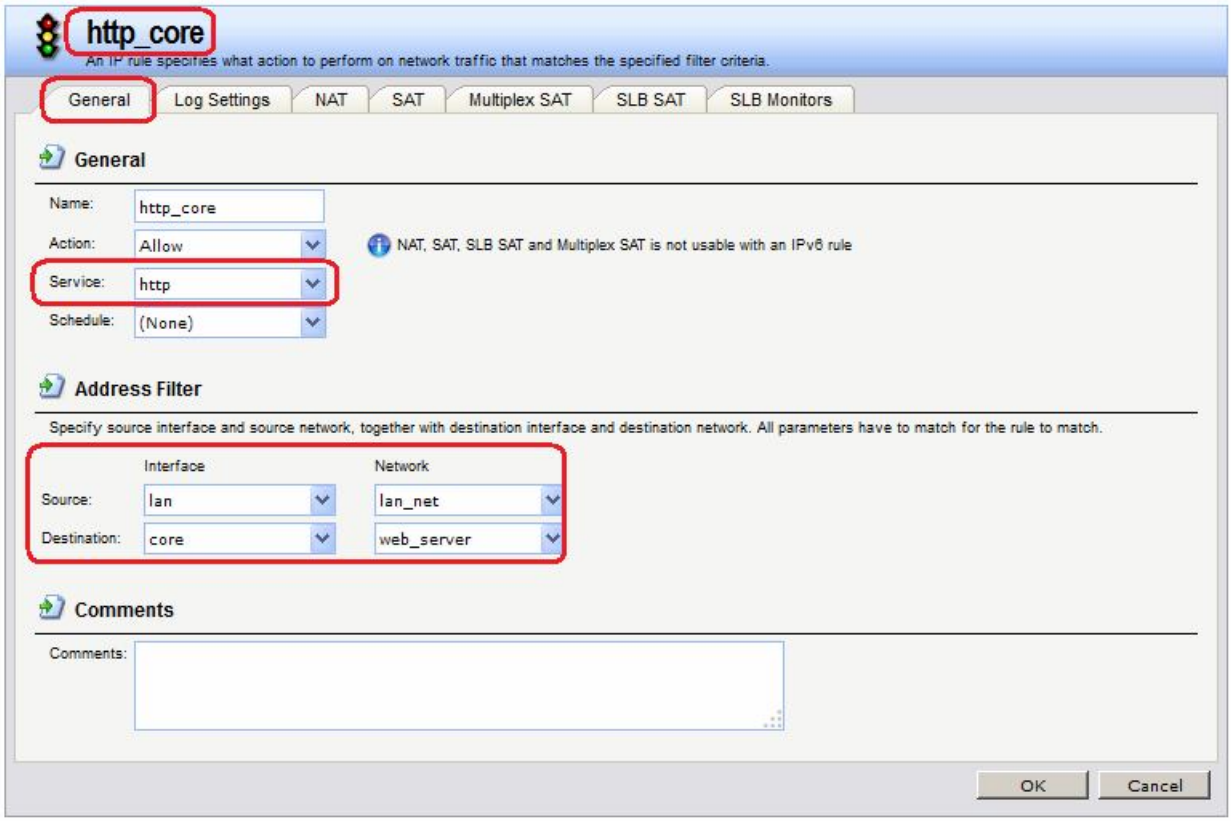
d) Правило, разрешающее трафик к интерфейсу **core** для доступа к форме аутентификации пользователей.

Веб-интерфейс:

Rules → IP Rules → local_nets → Add

Name: http_core

Rules → IP Rules → local_nets → http_core



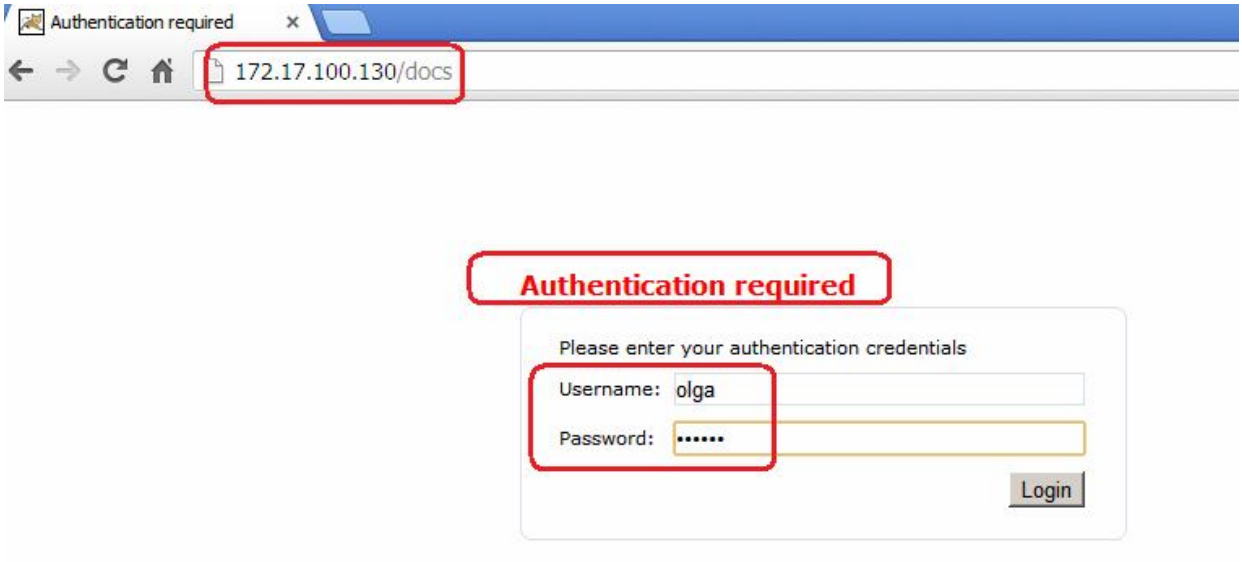
Командная строка:

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

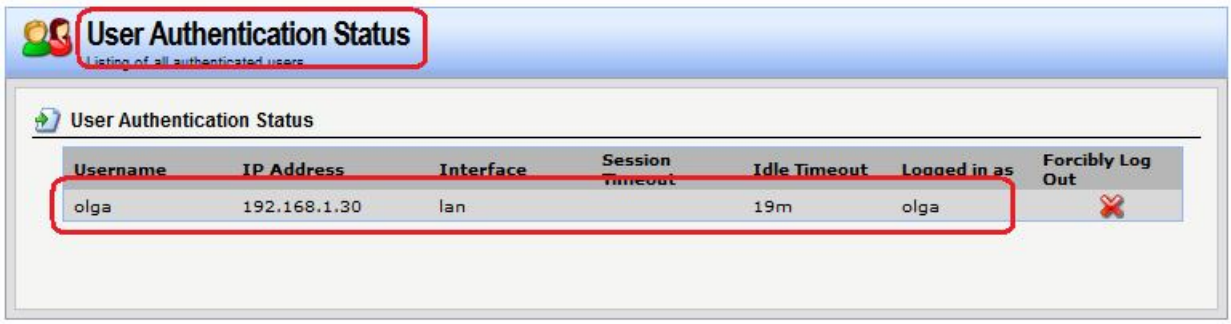
```
add IPRule Action=Allow SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=core DestinationNetwork=dmz/web_server Service=http
Name=http_core
```

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
Logged in as
Forcibly Log Out
olga
192.168.1.30
lan
19m
olga