

Высокопроизводительное решение с использованием «С-Терра L2» и балансировки на базе Catalyst 3560-X

Описание стенда

Сценарий иллюстрирует построение защищенного соединения между двумя сегментами одной сети SN1. Для защиты соединения будут построены VPN-туннели между шлюзами GW101-105 и GW201-205. Устройства IPHost1 и IPHost2 смогут общаться между собой по защищенному каналу (VPN). Трафик уровня L2 приходит на коммутатор, балансируется на один из шлюзов, инкапсулируется в L3, шифруется и передается другой стороне. На другой стороне пришедший трафик дешифруется, декапсулируется в L2 и передается далее.

Порты Gi0/1-4 коммутаторов Switch11 и Switch21 объединены в EtherChannel. Балансировка осуществляется с помощью протокола PAgP. Балансировка происходит по IP-адресу получателя, но этот параметр может быть изменен. Настройка шлюзов будет осуществляться преимущественно через «С-Терра КП».

Важно! При необходимости использования протокола LACP, обратитесь в Службу Технической Поддержки – <https://support.s-terra.com/>.

В рамках данного сценария для аутентификации партнеры будут использовать сертификаты. В качестве криптопровайдера будет использован «КриптоПро CSP» версии 3.6 (R4). Шлюзы безопасности «С-Терра Шлюз 4.1» с программным модулем «С-Терра L2 4.1». Система управления «С-Терра КП 4.1».

Параметры защищенного соединения:

- IKE параметры:
 - Аутентификация на сертификатах – GOST R 34.10-2001 Signature;
 - Алгоритм шифрования – GOST 28147-89 Encryption;
 - Алгоритм вычисления хеш-функции – GOST R 34.11-94 Hash;
 - Группа Диффи-Хеллмана – VKO GOST R 34.10-2001;
- IPsec параметры:
 - ESP алгоритм шифрования – ESP_GOST-4M-IMIT cipher.

Схема стенда (Рисунок 1):

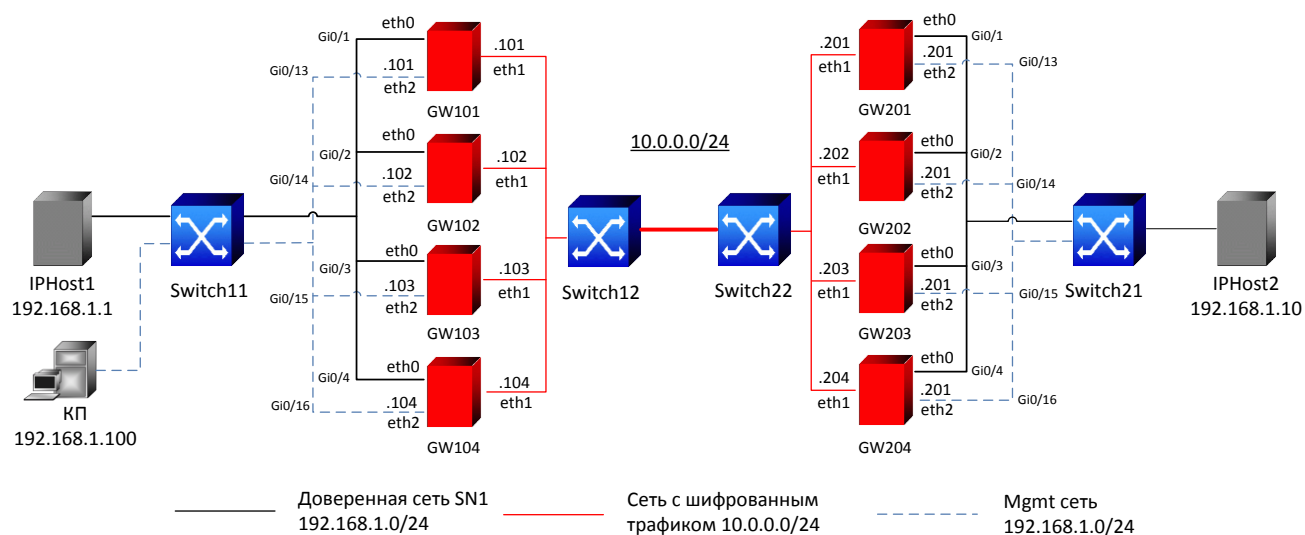


Рисунок 1

Настройка стенда

Подготовка к настройке

Предполагается, что:

- Шлюзы не настроены и процесс инициализации не пройден.
- Генерация контейнеров с закрытыми ключами происходит не на шлюзах.
- УЦ настроен.
- Продукт «С-Терра КП» установлен на устройстве Server и произведена начальная настройка.
- Локальные сертификаты сгенерированы, контейнеры с ключами созданы на отдельных ключевых носителях.

Этапы настройки:

- [Создание установочных пакетов для каждого шлюза при помощи «С-Терра КП»;](#)
- [Создание файлов конфигураций и лицензий «С-Терра L2»;](#)
- [Настройка шлюзов;](#)
- [Настройка EtherChannel на Switch11 и Switch21;](#)
- [Настройка остальных устройств;](#)

Процессы генерации сертификата УЦ и локальных сертификатов в данном сценарии не рассматриваются. На выходе мы должны получить файлы формата .cer (локальные сертификаты для каждого шлюза и доверенный сертификат УЦ) на устройстве Server. Контейнеры сохраняются на отдельные ключевые носители.

В данном сценарии будет использоваться уже установленный и настроенный продукт «С-Терра КП» на устройстве Server. Процесс установки и настройки описан в документации «[Программный продукт С-Терра КП. Версия 4.1. Руководство администратора](#)».

Создание установочных пакетов при помощи «С-Терра КП»

Добавление шлюза GW101 в КП

1. В меню “Clients” выберите пункт “Create” (Рисунок 2).

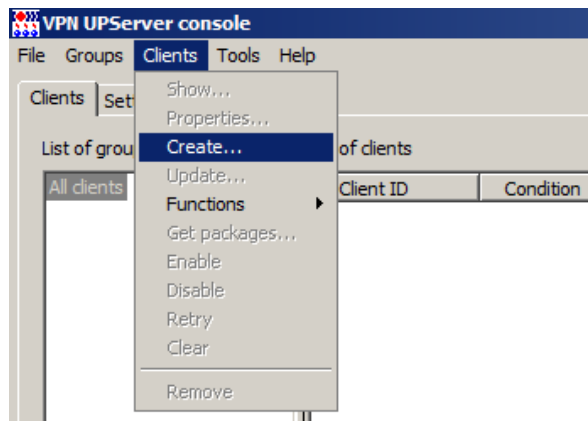


Рисунок 2

2. В появившемся окне “Create new client” (Рисунок 3) введите имя в поле “Client ID” и нажмите кнопку “Е”:

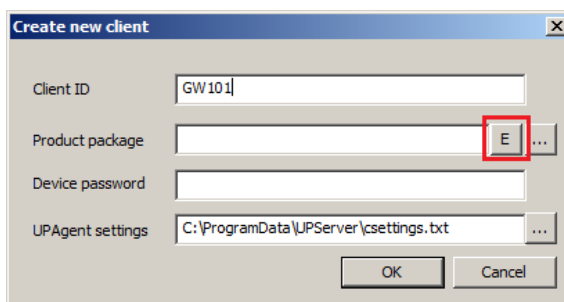


Рисунок 3

3. В окне “VPN data maker” в поле “VPN product” выберите “S-Terra Gate 4.1” (Рисунок 4) и нажмите кнопку “Run Wizard” для запуска мастера настройки.

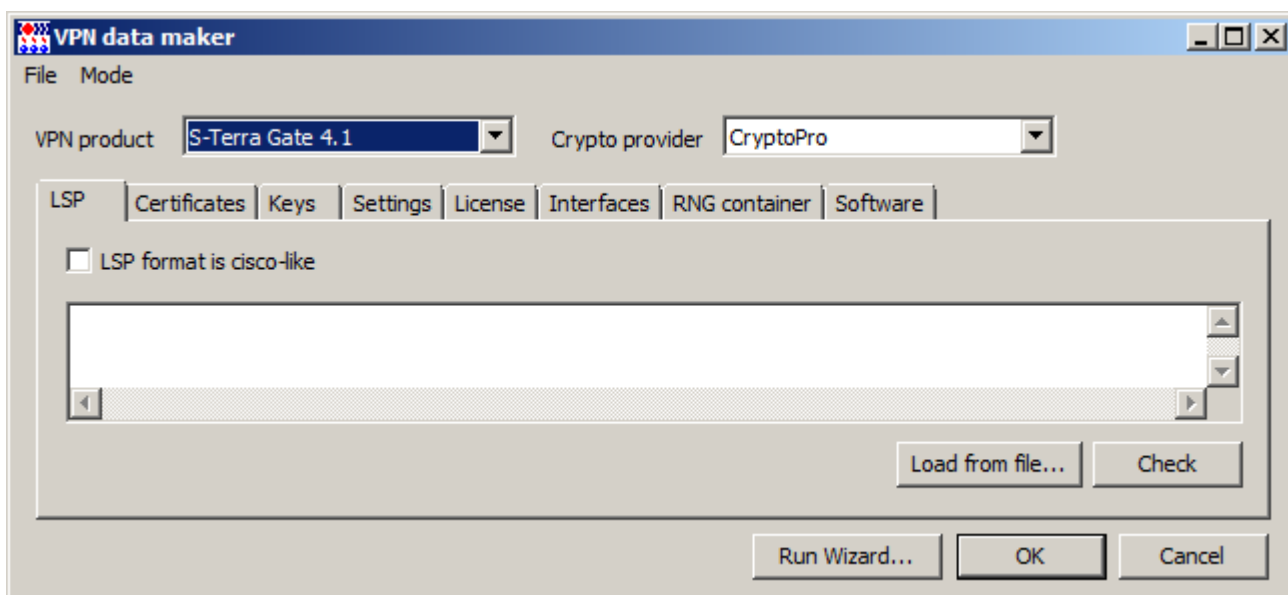


Рисунок 4

4. В окне мастера настройки добавьте сертификат УЦ и локальный сертификат (Рисунок 5).

При добавлении локального сертификата введите имя контейнера в поле “Key container name” и пароль (пароль соответствует паролю на контейнер конечного устройства, он может отличаться от пароля заданного при изначальной генерации контейнера) в поле “Key container password” (Рисунок 6).

Важно: обратите внимание на имя контейнера – \\.\HDIMAGE\HDIMAGE\vpngate101
Необходимо указать имя контейнера на конечном устройстве.

После добавления сертификатов нажмите кнопку “Next >”

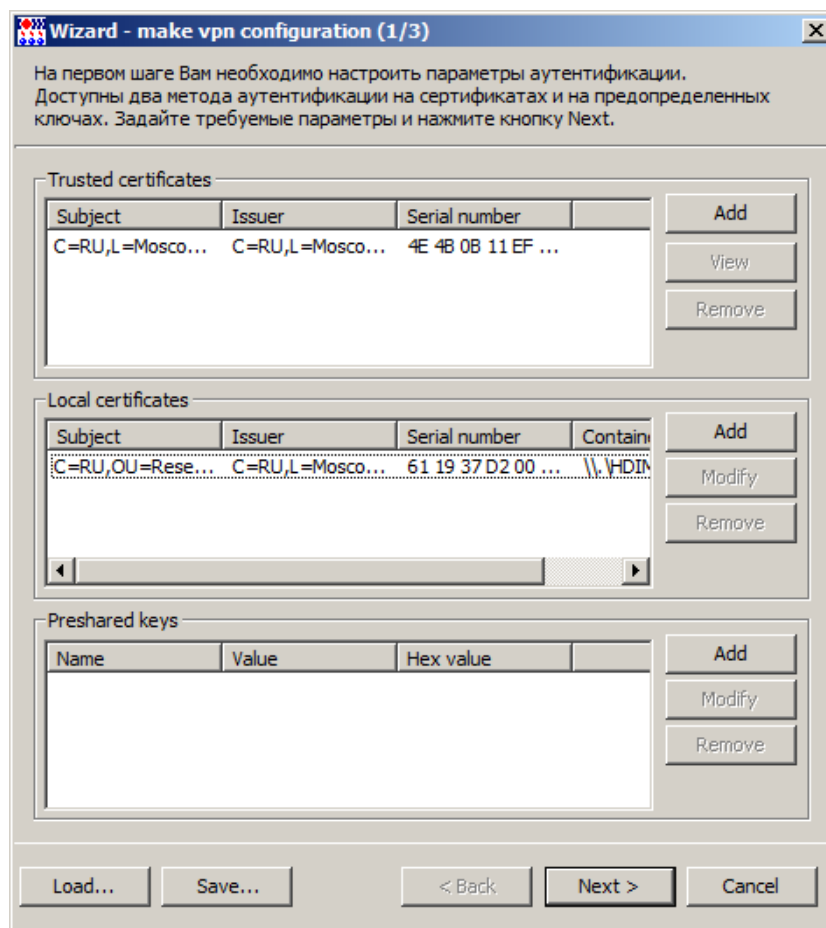


Рисунок 5

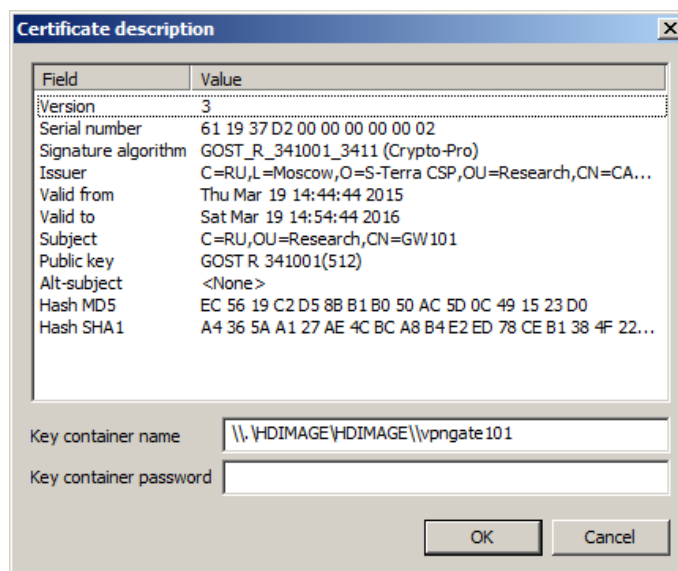


Рисунок 6

5. В следующем окне мастера добавьте правила обработки сетевого трафика, нажав кнопку “Add...”.

5.1. В появившемся окне “Add Rule” настройте защищенное соединение между SN1 и SN2:

- укажите алиас для шифрующего интерфейса в поле “Network interface alias” (алиас GigabitEthernet0/1 обычно соответствует интерфейсу eth1; соответствие алиас – физический интерфейс можно поменять в п. 8.3 данного раздела);
- в поле “Local IP Addresses” настройте адрес интерфейса Gi0/1 шлюза GW101 (10.0.0.101/32);

- в поле “Partner IP Addresses” настройте адрес интерфейса Gi0/1 шлюза GW201 (10.0.0.201/32);
- в поле “Action” выберите пункт “Protect using IPsec” и добавьте адрес интерфейса Gi0/1 шлюза GW2 (10.0.0.201), нажав клавишу “Add...”;
- после проведения всех настроек нажмите кнопку “OK” (Рисунок 7).

Рисунок 7

5.2. Созданное правило поднимите в приоритете (Рисунок 8). Нажмите кнопку “Next >”.

Рисунок 8

6. В следующем окне введите данные о продукте «С-Терра Шлюз» и номер лицензии на «КриптоПро CSP». После этого нажмите кнопку “Finish”.
7. Все введенные настройки будут отражены в конфигурации (Рисунок 9).

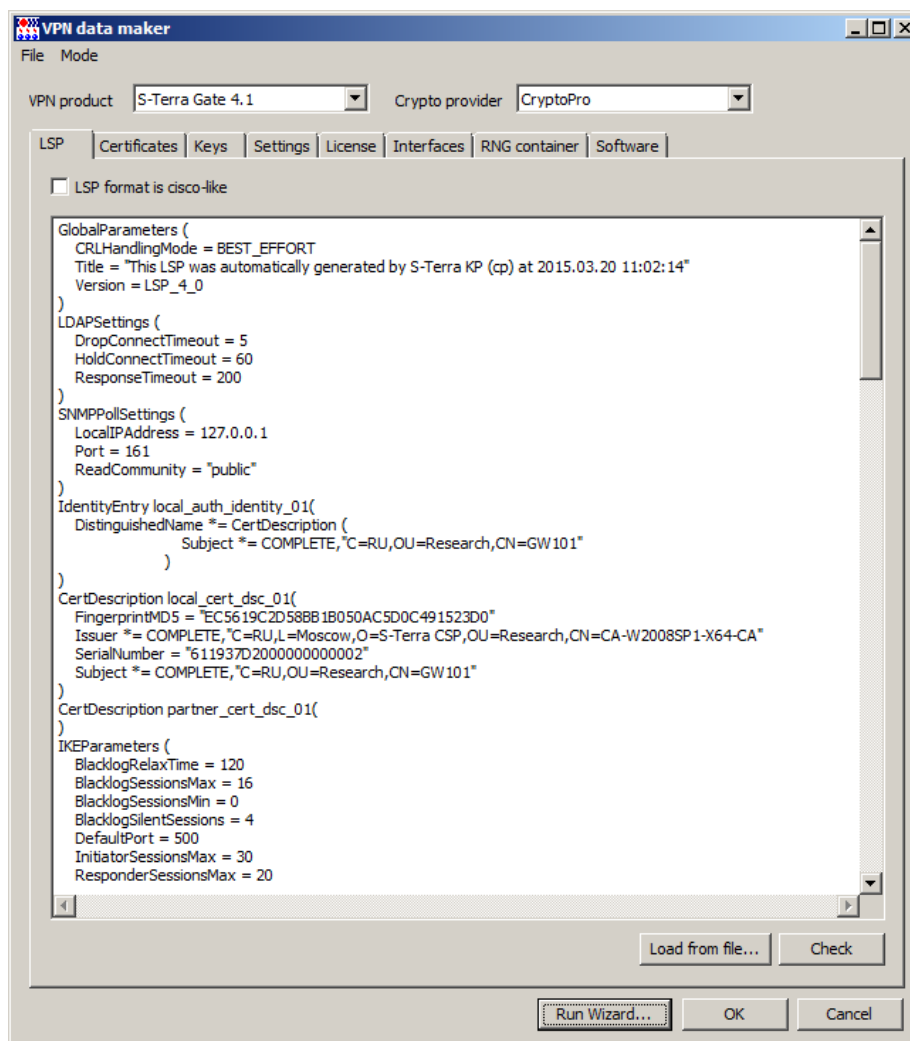


Рисунок 9

8. Откройте вкладку “Interfaces”.
- 8.1. Отметьте пункт “Network interface descriptions”.
- 8.1.1 Настройте IP-адреса для интерфейсов: 10.0.0.101/24 для eth1 и 192.168.1.101/24 для eth2.
- 8.2. Добавьте маршрут по умолчанию в разделе “Extended routing” – 0.0.0.0/0 через 10.0.0.201.
- 8.3. **Необязательный пункт.** По умолчанию карта интерфейсов с соответствием “Logical interface name” – “Physical interface name” на шлюзе настроена (файл /etc/aliases.cf), если есть необходимость в ее замене отметьте пункт “Network interface aliases”.
- 8.3.1 Добавьте соответствие логических и физических названий интерфейсов: GigabitEthernet0/0 (logical name) для eth0 (physical name), GigabitEthernet0/1 для eth1, GigabitEthernet0/2 для eth2, GigabitEthernet0/3 для eth3 (для разных моделей шлюзов и их компоновки количество интерфейсов может быть различным).
- 8.4. После внесения изменений вкладка “Interfaces” будет выглядеть следующим образом (Рисунок 10):

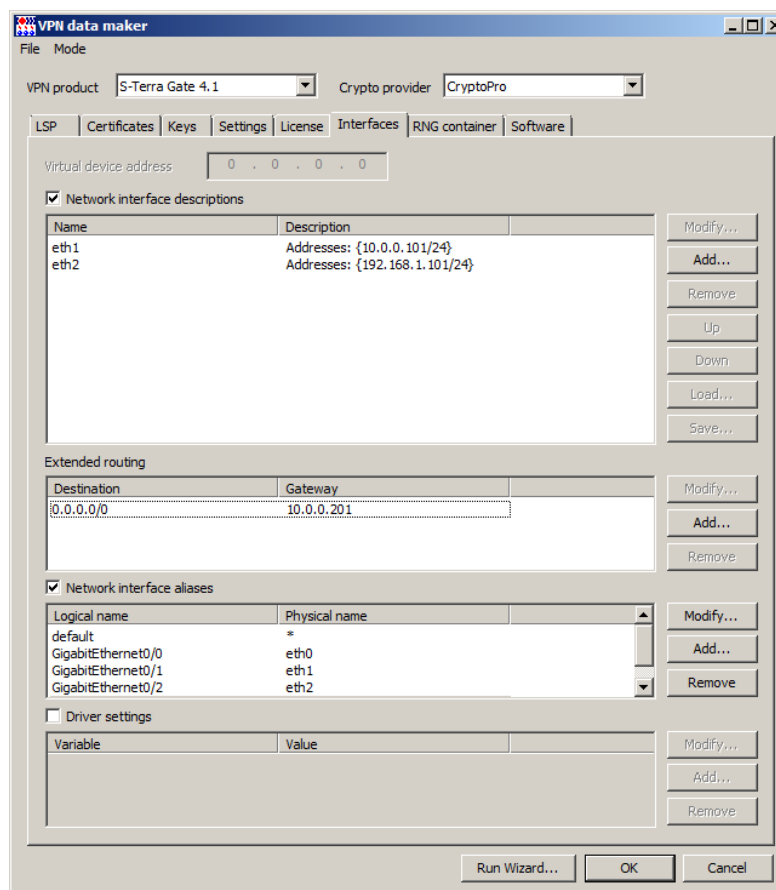


Рисунок 10

9. Настройка завершена. Чтобы в дальнейшем настраивать остальные шлюзы из шаблона, необходимо сохранить настройки в файл *.vpd. Для этого в окне “VPN data maker” выберите меню “File”, пункт “Save as...” и сохраните файл.
10. Для сохранения настроек шлюза GW101 в окне “VPN data maker” нажмите кнопку “OK”.
11. В окне “Create new client” (Рисунок 11) нажмите кнопку “OK”.

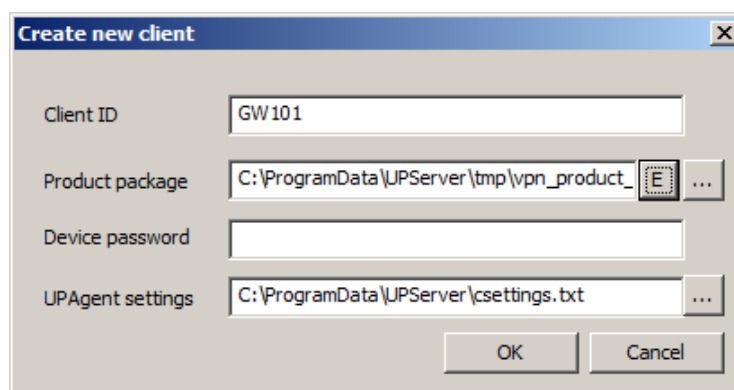


Рисунок 11

12. В окне КП отобразится шлюз GW101. Переведите его в активное состояние, выбрав в контекстном меню пункт “Enable” (Рисунок 12). “Administrative state” изменится с “disabled” на “enabled”.

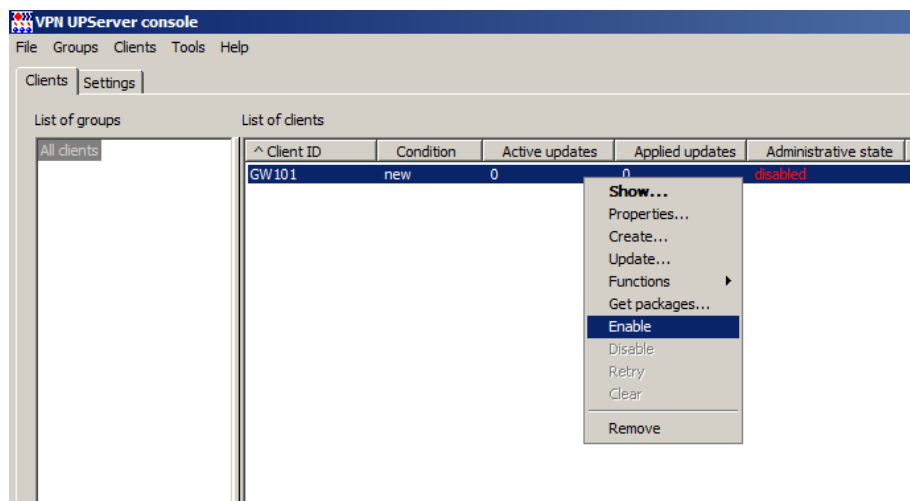


Рисунок 12

13. В контекстном меню шлюза GW101 выберите пункт “Get packages” (Рисунок 13). Укажите каталог для сохранения установочных пакетов. В указанный каталог будут сохранены два файла:

- setup_upagent.sh – файл, содержащий данные для КП;
- setup_product.sh – файл, содержащий настройки для «С-Терра Шлюз».

Данные файлы, вместе с ключами необходимо будет перенести на шлюз и там установить.

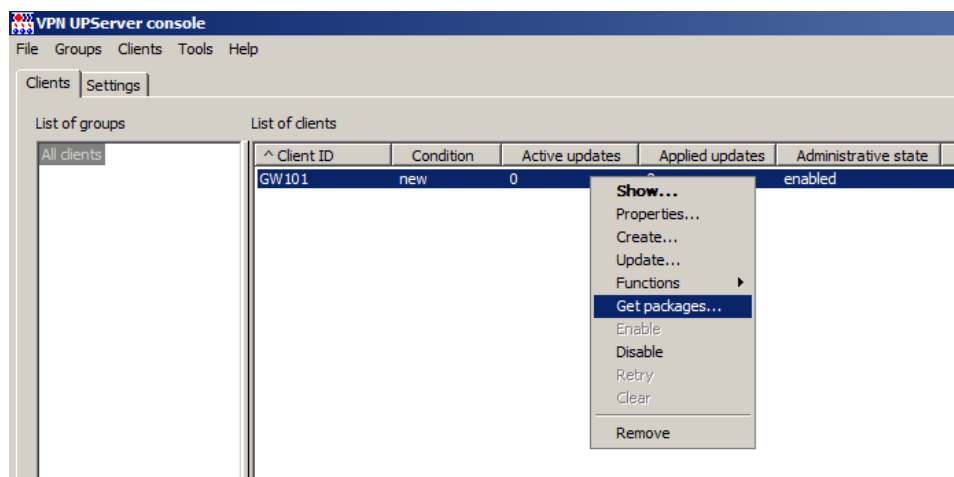


Рисунок 13

Добавление шлюза GW201 в КП

1. В меню “Clients” выберите пункт “Create”.
2. В окне “Create new client” введите название шлюза GW201 в поле “Client ID” и нажмите кнопку “E”.
3. В окне “VPN data maker” откройте меню “File” и выберите пункт “Load...”.
4. Откройте созданный ранее (п. 9 раздела “Добавление шлюза GW101 в КП”) файл *.vpd с настройками шлюза GW101.
5. Загрузится конфигурация шлюза GW101, в которой необходимо изменить IP-адреса, сертификат, имя контейнера, лицензию, настройки интерфейсов.
6. Запустите мастер настройки, нажав кнопку “Run Wizard...”
 - 6.1. В первом окне мастера замените локальный сертификат (раздел “Local certificates”) на сертификат для шлюза GW201.

- 6.1.1 Удалите старый сертификат, добавьте новый для шлюза GW201.
- 6.1.2 В поле “Key container name” укажите имя контейнера – \\.\HDIMAGE\HDIMAGE\vpngate201.
- 6.1.3 В поле “Key container password” введите пароль для контейнера шлюза GW201 (пароль соответствует паролю на контейнер конечного устройства, он может отличаться от пароля заданного при изначальной генерации контейнера).
- 6.1.4 В окне “Certificate description” нажмите кнопку “OK” для сохранения внесенных изменений локального сертификата.
- 6.2. Перейдите к следующему окну мастера, нажав кнопку “Next >”.
- 6.3. В следующем окне измените правило для интерфейса “GigabitEthernet0/1”, нажав кнопку “Edit”.
 - 6.3.1 В разделе “Local IP Addresses” необходимо сменить IP-адрес на 10.0.0.201 с маской 255.255.255.255.
 - 6.3.2 В разделе “Partner IP Addresses” необходимо сменить IP-адрес на 10.0.0.101 с маской 255.255.255.255.
 - 6.3.3 В разделе “Action” необходимо сменить IP-адрес с которым будет строиться туннель на 10.0.0.101.
 - 6.3.4 В разделе “Action” измените привязанный к правилу сертификат. Нажмите на кнопку “...” рядом с полем “Auth object”. В открывшемся окне “Local ID” в поле “Auth object list” выберите сертификат для шлюза GW201 и нажмите “OK” (Рисунок 14).

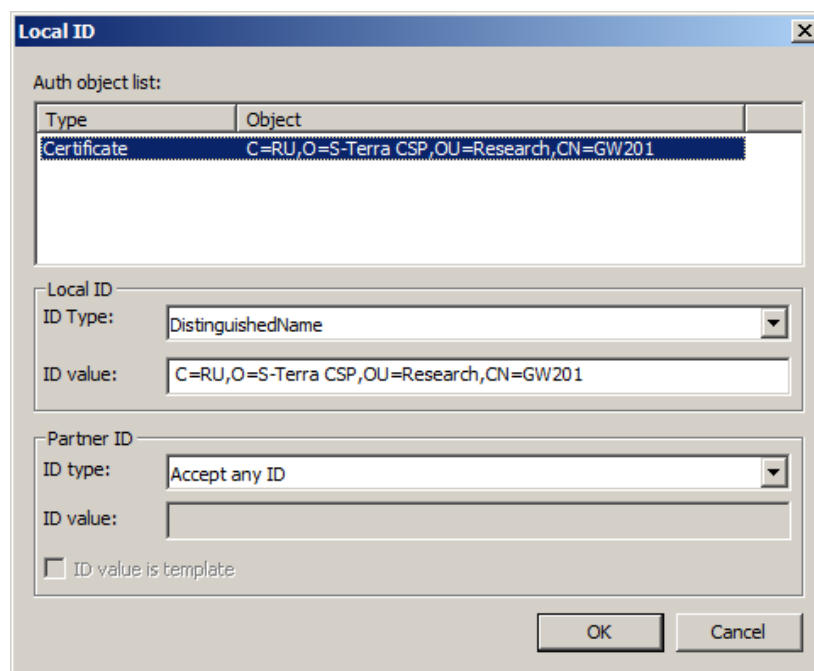


Рисунок 14

- 6.3.5 После изменения настроек окно “Edit rule” будет выглядеть следующим образом (Рисунок 15):

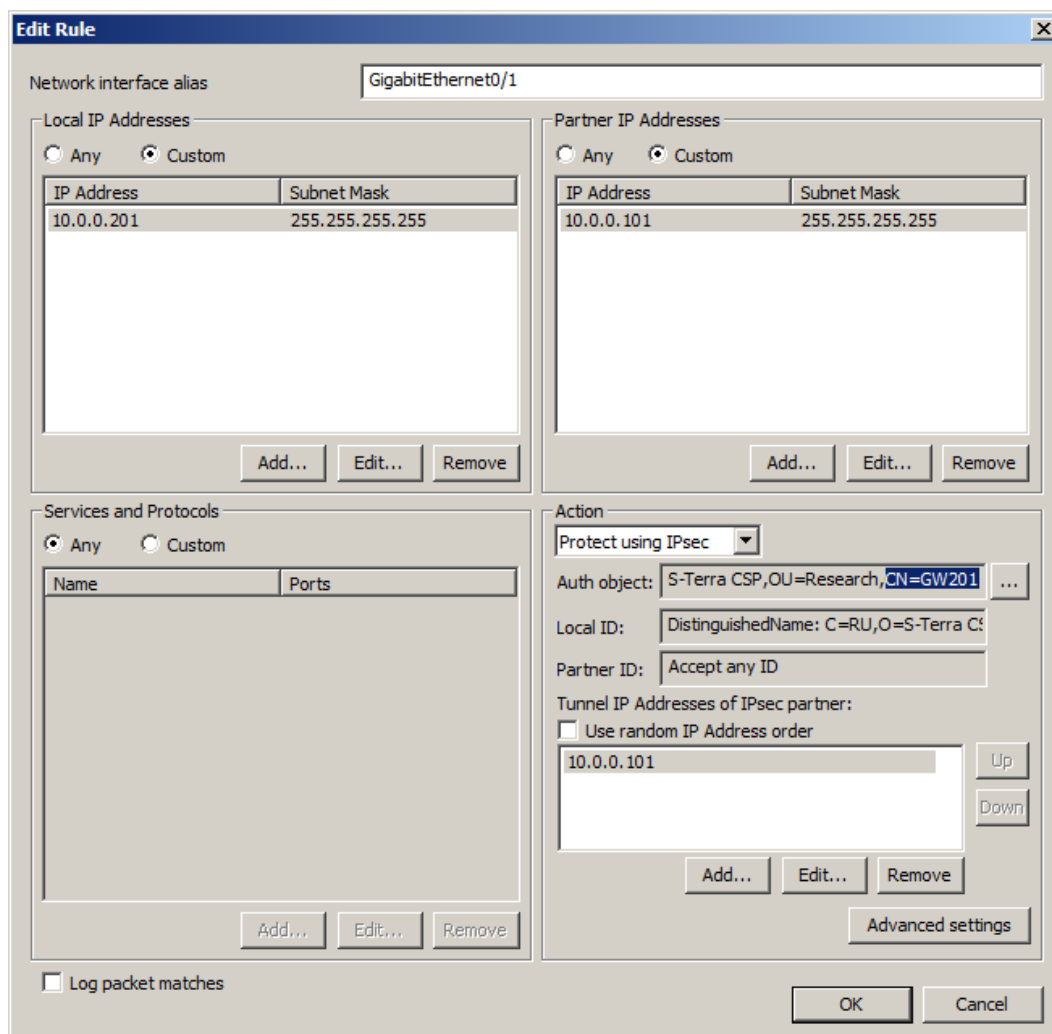


Рисунок 15

- 6.3.6 После внесения изменений нажмите кнопку “OK”.
- 6.4. В окне мастера настройки перейдите на следующее окно, нажав кнопку “Next >”.
- 6.5. В следующем окне измените номер лицензии на продукты «С-Терра Шлюз» и «КриптоПро CSP». После этого нажмите кнопку “Finish”.
7. На вкладке “Interfaces” измените IP-адреса, маршрутизацию и соответствие интерфейсов.
- 7.1. Для eth1 IP-адрес будет 10.0.0.201/24, для eth2 – 192.168.1.201/24.
- 7.2. Маршрут по умолчанию – 0.0.0.0/0 через 10.0.0.101.
- 7.3. Соответствие интерфейсов на однотипных шлюзах с одинаковой комплектацией можно не менять.
- 7.4. После внесенных изменений вкладка “Interfaces” будет выглядеть следующим образом (Рисунок 16):

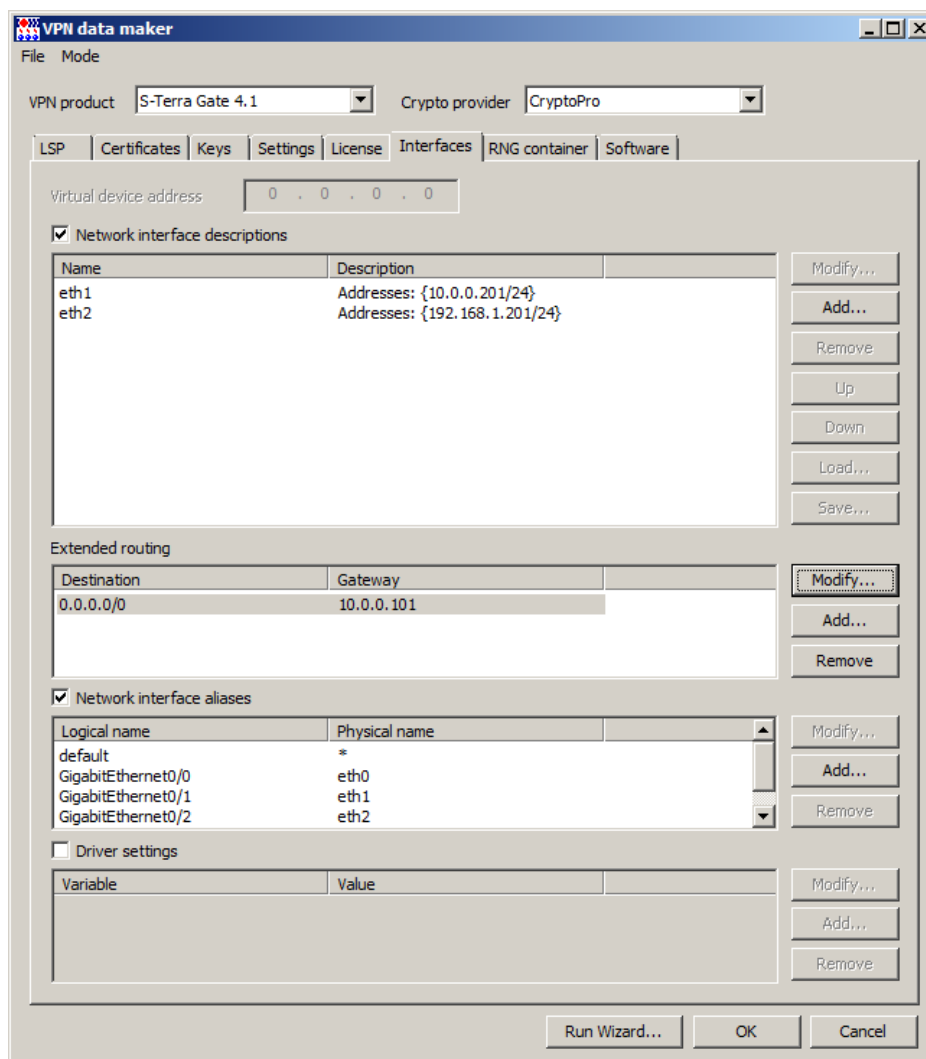


Рисунок 16

8. Настройки шлюза GW201 стоит сохранить в файл *.vpd.
9. После этого в окне “VPN data maker” нажмите кнопку “OK”.
10. В окне “Create new client” (Рисунок 15) нажмите кнопку “OK”.
11. В окне КП появится шлюз GW201, который нужно активировать, выбрав в контекстном меню пункт “Enable”. После этого создайте установочные пакеты, выбрав в контекстном меню пункт “Get packages”. Сохраните пакеты в отдельную папку (папки для каждого шлюза должны быть различными, так как названия пакетов – одинаковые).

Добавление остальных шлюзов в КП

Добавление остальных шлюзов происходит аналогично, с заменой необходимых IP-адресов, маршрутизации, локального сертификата, пути до контейнера, пароля на контейнер и лицензий.

После завершения всех операций у нас будут установочные пакеты для всех шлюзов.

В **Приложении** представлены тексты LSP-конфигураций для шлюзов [GW101](#) и [GW201](#).

Создание файлов конфигураций и лицензий «С-Терра L2»

Рекомендуется заранее создать файлы конфигураций «С-Терра L2» и файлы лицензий на «С-Терра L2», а на конечных устройствах копировать их с носителя.

1. Файл лицензии l2.lic должен находиться в директории /opt/l2svc/etc/. Файл l2.lic должен быть представлен в следующем виде:

```
[license]
CustomerCode=test
ProductCode=L2VPN
LicenseNumber=12345
LicenseCode=1234567890ABCDEF
```

2. Файл конфигурации config.conf должен находиться в директории /opt/l2svc/etc/. Пример конфигурации для шлюза GW1:

```
vif tap0
bridge br0
capture eth0
remote 10.0.0.201
mssfix 1400
passtos
```

Где:

- **vif <name>** – название виртуального интерфейса (TAP). Обязательный параметр. Рекомендуется **tapN**, где **N** – цифра.
- **bridge <name>** – название виртуального интерфейса моста. Обязательный параметр. Рекомендуется **brN**, где **N** – цифра.
- **capture <name>** – имя сетевого интерфейса, с которого будет осуществляться захват Ethernet-фреймов. Обязательный параметр.
- **remote <host> [port]** – IP-адрес или имя и порт удаленного хоста. Обязательный параметр (адрес, номер порта опционально).
- **fragment <n>** – Все пакеты большие **n** байт, будут фрагментироваться самим продуктом на примерно равные части. Опциональный параметр
- **mssfix <n>** – при включении данной опции поле MSS всех проходящих через туннель TCP-пакетов будет выставлено в **n**. При этом TCP/IP стек отправителя и получателя сам уменьшит максимальный размер пакета, не прибегая к использованию ICMP. Это позволит избежать фрагментации. Если параметр **n** отсутствует, будет взято значение параметра **fragment**, если оно задано. Работает только для TCP-трафика. Опциональный параметр. Значение по умолчанию – 1450.
- **passtos** – параметр, позволяющий сохранять поле TOS у передаваемых пакетов. Опциональный параметр. По умолчанию - отключен.
- **tun_mtu <n>** - MTU туннельного интерфейса. При загрузке конфигурации с параметром **tun_mtu <n>**, значения MTU интерфейсов, указанных в опциях **capture <name>**, **vif <name>**, **bridge <name>**, устанавливаются в **n**. Значение по умолчанию – 1500. При использовании VLAN-интерфейсов, смотрите [соответствующий сценарий](#).

3. Необязательный пункт.

На конечных устройствах будут так же выполняться команды для запуска l2svc и для добавления в автозагрузку:

```
/etc/init.d/l2svc start
update-rc.d l2svc enable
```

Копирование файлов и прописывание необходимых команд на конечном устройстве можно автоматизировать с помощью скрипта.

4. Создайте необходимые файлы для всех шлюзов.

В Приложении представлены тексты конфигурации /opt/l2svc/etc/config.conf для [GW101](#) и [GW201](#).

Настройка шлюзов

Настройка шлюза GW101

Копирование контейнера

1. Установите правильное системное время. Например:

```
date 032014082015
```

Что соответствует 20 марта 2015 года 14:08.

2. Подключите носитель с ключевой информацией и установочными пакетами КП к шлюзу. В dmesg отобразится подключенный носитель:

```
...
[13575.003633] scsi 3:0:0:0: Direct-Access      General  USB Flash Disk   1.0  PQ:
0 ANSI: 2[13575.020071] sd 3:0:0:0: [sdb] 3915776 512-byte logical blocks: (2.00
GB/1.86 G
iB)[13575.028257] sd 3:0:0:0: [sdb] Write Protect is off
[13575.028267] sd 3:0:0:0: [sdb] Mode Sense: 03 00 00 00
[13575.028271] sd 3:0:0:0: [sdb] Assuming drive cache: write through
[13575.069176] sd 3:0:0:0: [sdb] Assuming drive cache: write through
[13575.069528]  sdb: sdb1
[13575.110967] sd 3:0:0:0: [sdb] Assuming drive cache: write through
[13575.112492] sd 3:0:0:0: [sdb] Attached SCSI removable disk
```

3. Подмонтируйте раздел:

```
root@sterragate:~# mkdir /flash
root@sterragate:~# mount /dev/sdb1 /flash
```

4. Для просмотра контейнеров на подключенном носителе можно воспользоваться утилитой csptest.

- Для x64 ОС:

```
/opt/cproccsp/bin/amd64/csptest -keyset -machinekeyset -verifycontext -enum_containers
-fqcn -unique
```

```
CSP (Type:75) v3.9.8000 KC1 Release Ver:3.9.8212 OS:Linux CPU:AMD64 FastCode:READ
Y:AVX.AcquireContext: OK. HCRYPTPROV: 14470883
\\.\FLASH\GW101 |\\.\FLASH\FLASH\GW101.000\2BA0
OK.
Total:
[ErrorCode: 0x00000000]
```

- Для x32 ОС:

```
/opt/cproccsp/bin/ia32/csptest -keyset -machinekeyset -verifycontext -enum_containers
-fqcn -unique
```

5. Скопируйте контейнер на жесткий диск устройства; при этом будут запрошены пароли на существующий и создаваемый контейнеры.

Важно: путь до создаваемого контейнера и пароль должен совпадать с настроенным в «С-Терра КП» (п. 4 раздела «Добавление шлюза GW101 в КП»).

- Для x64 ОС:

```
/opt/cproccsp/bin/amd64/csptest -keycopy -machinekeyset -src
'\\.\FLASH\FLASH\GW101.000' -dest '\\.\HDIMAGE\HDIMAGE\vpngate101'
```

```
CSP (Type:75) v3.9.8000 KC1 Release Ver:3.9.8212 OS:Linux CPU:AMD64
FastCode:READY:AVX.
CryptAcquireContext succeeded.HCRYPTPROV: 11026147
```

```
CryptAcquireContext succeeded.HCRYPTPROV: 11193683
CryptoPro CSP: Set password on produced container "HDIMAGE\\vpngate101".
Password:
Retype password:
Total:
[ErrorCode: 0x00000000]
```

- Для x32 ОС:

```
/opt/cproscsp/bin/ia32/csptest -keycopy -machinekeyset -src
'\\.\FLASH\FLASH\GW101.000' -dest '\\.\HDIMAGE\HDIMAGE\vpngate101'
```

Разворачивание установочных файлов

1. Пропишите права на выполнение скриптов:

```
root@sterragate:~# chmod +x /flash/exe/GW101/setup_*.sh
```

2. Запустите файлы:

```
root@sterragate:~# /flash/exe/GW101/setup_product.sh
```

```
VPN data are set successfully
```

```
root@sterragate:~# /flash/exe/GW101/setup_upagent.sh
```

```
File decompression...
```

```
cacert.cer
reg.txt
settings.txt
```

```
...Done
```

```
Starting VPN UPAgent watchdog daemon..done.
```

```
Initialization is successful
```

Настройка «С-Терра L2»

1. Скопируйте файл лицензии l2.lic в директорию /opt/l2svc/etc/.
2. Скопируйте файл конфигурации config.conf в директорию /opt/l2svc/etc/.
3. Запустите «С-Терра L2»:

```
root@GW1:~# /etc/init.d/l2svc start
```

```
Starting l2svc:
```

```
Configuration successfully loaded from config.conf
```

4. Чтобы при перезагрузке демон стартовал автоматически, выполните команду:

```
root@GW1:~# update-rc.d l2svc enable
```

Настройка остальных шлюзов

Настройка шлюзов GW102-104 и GW201-204 производится аналогично настройке шлюза GW101.

Стоит отметить, что соединение шлюзов GW201-204 с КП происходит только при работающем продукте «С-Терра L2». Т.е. при разворачивании скриптов КП, подключение не будет окончательно завершено до корректной настройки «С-Терра L2».

В результате настройка шлюза сведется к следующим действиям:

1. Копирование контейнера с закрытыми ключами с переносного носителя на жесткий диск конечного устройства.
2. Прописывание прав на скрипты, созданные на «С-Терра КП» и установка их.

3. Копирование конфигурации и лицензии «С-Терра L2» с переносного носителя на жесткий диск конечного устройства, запуск и прописывание l2svc в автозагрузку.

Настройка EtherChannel

На устройствах Switch11 и Switch21 настройте EtherChannel по протоколу PAgP (Port Aggregation Protocol) с правилом балансировки dst-ip.

Настройка Switch11

1. Настройте EtherChannel по протоколу PAgP на интерфейсах GigabitEthernet 0/1-4:

```
Switch11>en
Switch11#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Switch11(config)#int range Gi0/1-4
Switch11(config-if-range)#channel-protocol pagp
Switch11(config-if-range)#channel-group 1 mode desirable
Switch11(config-if-range)#no sh
Switch11(config-if-range)#exit
```

2. Настройте правило балансировки по IP-адресу назначения (destination ip):

```
Switch11(config)#port-channel load-balance dst-ip
Switch11(config)#end
```

3. Сохраните конфигурацию устройства:

```
Switch11#wr
```

```
Building configuration...
[OK]
```

Настройка Switch21

1. Настройте EtherChannel по протоколу PAgP на интерфейсах GigabitEthernet 0/1-4:

```
Switch21>en
Switch21#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Switch21(config)#int range Gi0/1-4
Switch11(config-if-range)#channel-protocol pagp
Switch11(config-if-range)#channel-group 1 mode auto
Switch21(config-if-range)#exit
```

2. Настройте правило балансировки по IP-адресу назначения (destination ip):

```
Switch21(config)#port-channel load-balance dst-ip
Switch21(config)#end
```

3. Сохраните конфигурацию устройства:

```
Switch21#wr
```

```
Building configuration...
[OK]
```

В Приложении представлены тексты конфигураций для устройств [Switch11](#) и [Switch21](#).

Настройка устройств IPHost1 и IPHost2

На устройствах Host1 и Host2 необходимо задать IP-адреса согласно схеме (Рисунок 1).

Проверка работоспособности стенда

После того, как настройка завершена, все устройства будут отображены в КП:

На устройстве Switch11 проверьте, что EtherChannel нормально функционирует:

```
Switch11#show etherchannel summary
```

```
Flags:  D - down          P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
```

```
Number of channel-groups in use: 1
Number of aggregators:          1
```

Group	Port-channel	Protocol	Ports
1	Po1 (SU)	PAgP	Gi0/1(P) Gi0/2(P) Gi0/3(P) Gi0/4(P)

У всех интерфейсов состояние P – in port-channel, т.е. EtherChannel работает корректно, служебные пакеты между Switch11 и Switch21 проходят нормально.

На IPHost1 выполните команду:

```
ping 192.168.1.10
```

```
PING 192.168.1.10 (192.168.1.10): 56 data bytes
64 bytes from 192.168.1.10: icmp_seq=0 ttl=61 time=1.3 ms
64 bytes from 192.168.1.10: icmp_seq=1 ttl=61 time=2.8 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=61 time=1.3 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=61 time=1.6 ms
```

В зависимости от настройки балансировки на устройствах Switch11 и Switch21 трафик между хостами будет по-разному балансироваться между интерфейсами свитчей.

В данном сценарии описывается настройка правила балансировки – dst-ip.

Проверить правило балансировки можно, выполнив команду:

```
Switch11#show etherchannel load-balance
```

```
EtherChannel Load-Balancing Operational State (dst-ip):
Non-IP: Destination MAC address
IPv4: Destination IP address
IPv6: Destination IP address
```

Проверить через какие интерфейсы шел трафик от Host1 к Host2 можно выполнив команду:

```
Switch11#test etherchannel load-balance interface Port-channel 1 ip 192.168.1.1
192.168.1.10
```

```
Would select Gi0/2 of Po1
```

Обратный трафик может балансироваться по другим интерфейсам:

```
Switch11#test etherchannel load-balance interface Port-channel 1 ip 192.168.1.10
192.168.1.1
```

```
Would select Gi0/1 of Po1
```

При работе EtherChannel между коммутаторами Switch11 и Switch21 будут ходить служебные пакеты. Поэтому при правильной настройке между шлюзами всегда будут VPN-туннели.

Просмотреть созданный туннель можно, выполнив на шлюзе команду:

```
[root@gw101 ~]# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded
```

```
ISAKMP connections:
```

```
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd  
1 20 (10.0.0.101,500)-(10.0.0.201,500) active 3192 3632
```

```
IPsec connections:
```

```
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd  
1 1 (10.0.0.101,*)-(10.0.0.201,*) * ESP tunn 134992 172616
```

Приложение

Текст LSP конфигурации для устройства GW101

```
GlobalParameters (
    CRLHandlingMode = BEST_EFFORT
    Title = "This LSP was automatically generated by S-Terra KP (cp) at 2015.05.06
12:34:02"
    Version = LSP_4_0
)
LDAPSettings (
    DropConnectTimeout = 5
    HoldConnectTimeout = 60
    ResponseTimeout = 200
)
SNMPPollSettings (
    LocalIPAddress = 127.0.0.1
    Port = 161
    ReadCommunity = "public"
)
IdentityEntry local_auth_identity_01(
    DistinguishedName *= CertDescription (
        Subject *= COMPLETE,"C=RU,O=S-Terra
CSP,OU=Research,CN=GW101"
    )
)
CertDescription local_cert_dsc_01(
    FingerprintMD5 = "406A5176D988F4FEA00B568FA8E719D8"
    Issuer *= COMPLETE,"C=RU,L=Moscow,O=S-Terra CSP,OU=Research,CN=CA-W2008SP1-X64-
CA"
    SerialNumber = "6107669E0000000000002"
    Subject *= COMPLETE,"C=RU,O=S-Terra CSP,OU=Research,CN=GW101"
)
CertDescription partner_cert_dsc_01(
)
IKEParameters (
    BlacklogRelaxTime = 120
    BlacklogSessionsMax = 16
    BlacklogSessionsMin = 0
    BlacklogSilentSessions = 4
    DefaultPort = 500
    InitiatorSessionsMax = 30
    ResponderSessionsMax = 20
    RetryTimeBase = 1
    RetryTimeMax = 30
    SendRetries = 5
    SessionTimeMax = 60
)
AuthMethodGOSTSign auth_method_01(
    LocalCredential = local_cert_dsc_01
    LocalID = local_auth_identity_01
    RemoteCredential *= partner_cert_dsc_01
    SendCertMode = AUTO
    SendRequestMode = AUTO
)
IKETransform ike_trf_01(
    CipherAlg *= "G2814789CPR01-K256-CBC-65534"
    GroupID *= VKO_1B
    HashAlg *= "GR341194CPR01-65534"
    LifetimeSeconds = 28800
)
```

```
NoSmoothRekeying = FALSE
)
IKETransform ike_trf_02(
    CipherAlg *= "G2814789CPRO1-K256-CBC-65534"
    GroupID *= MODP_1536
    HashAlg *= "GR341194CPRO1-65534"
    LifetimeSeconds = 28800
    NoSmoothRekeying = FALSE
)
IKETransform ike_trf_03(
    CipherAlg *= "G2814789CPRO1-K256-CBC-65534"
    GroupID *= MODP_1024
    HashAlg *= "GR341194CPRO1-65534"
    LifetimeSeconds = 28800
    NoSmoothRekeying = FALSE
)
IKETransform ike_trf_04(
    CipherAlg *= "G2814789CPRO1-K256-CBC-65534"
    GroupID *= MODP_768
    HashAlg *= "GR341194CPRO1-65534"
    LifetimeSeconds = 28800
    NoSmoothRekeying = FALSE
)
ESPTransform esp_trf_01(
    CipherAlg *= "G2814789CPRO1-K288-CNTMAC-253"
    LifetimeKilobytes = 4608000
    LifetimeSeconds = 3600
)
ESPProposal esp_proposal_01(
    Transform = esp_trf_01
)
ESPTransform esp_trf_02(
    CipherAlg *= "G2814789CPRO1-K256-CBC-254"
    IntegrityAlg *= "GR341194CPRO1-H96-HMAC-65534"
    LifetimeKilobytes = 4608000
    LifetimeSeconds = 3600
)
ESPProposal esp_proposal_02(
    Transform = esp_trf_02
)
ESPTransform esp_trf_03(
    CipherAlg *= "G2814789CPRO1-K256-CBC-254"
    IntegrityAlg *= "G2814789CPRO1-K256-MAC-65535"
    LifetimeKilobytes = 4608000
    LifetimeSeconds = 3600
)
ESPProposal esp_proposal_03(
    Transform = esp_trf_03
)
ESPTransform esp_trf_04(
    CipherAlg *= "G2814789CPRO1-K256-CBC-254"
    LifetimeKilobytes = 4608000
    LifetimeSeconds = 3600
)
ESPProposal esp_proposal_04(
    Transform = esp_trf_04
)
IKERule ike_rule_01(
    DPDIIdleDuration = 60
    DPDResponseDuration = 5
    DPDRetries = 3
)
```

```

    DoNotUseDPD = FALSE
    IKECFGBindToPeerAddress = FALSE
    MainModeAuthMethod *= auth_method_01
    Transform *= ike_trf_01,ike_trf_02,ike_trf_03,ike_trf_04
    XAuthServerEnabled = FALSE
)
IPsecAction ipsec_action_01(
    ContainedProposals
(esp_proposal_01),(esp_proposal_02),(esp_proposal_03),(esp_proposal_04)
    GroupID *= VKO_1B
    IKERule = ike_rule_01
    TunnelingParameters *= TunnelEntry (
        Assemble = FALSE
        DFHandling = COPY
        PeerIPAddress = 10.0.0.201
        ReRoute = FALSE
    )
)
FilterChain filter_chain_ipsec_01(
    Filters *= Filter (
        Action = PASS
        LogEventID = "ike_autopass_action_01"
        ProtocolID *= 17
        SourcePort *= 500, 4500
    ),Filter (
        Action = PASS
        LogEventID = "pass_action_02"
    )
)
NetworkInterface (
    IPsecPolicy = filter_chain_ipsec_01
)
FilterChain filter_chain_ipsec_02(
    Filters *= Filter (
        Action = PASS
        LogEventID = "ike_autopass_action_02"
        ProtocolID *= 17
        SourcePort *= 500, 4500
    ),Filter (
        Action = PASS
        SourceIP *= 10.0.0.101
        DestinationIP *= 10.0.0.201
        ExtendedAction = ipsec<sa=ipsec_action_01>
        LogEventID = "ipsec_action_01"
    )
)
NetworkInterface (
    IPsecPolicy = filter_chain_ipsec_02
    LogicalName = "GigabitEthernet0/1"
)

```

Текст LSP конфигурации для устройства GW201

```

GlobalParameters (
    CRLHandlingMode = BEST_EFFORT
    Title = "This LSP was automatically generated by S-Terra KP (cp) at 2015.05.06
12:59:11"
    Version = LSP_4_0
)
LDAPSettings (
    DropConnectTimeout = 5
)

```

```
    HoldConnectTimeout = 60
    ResponseTimeout = 200
)
SNMPPollSettings (
    LocalIPAddress = 127.0.0.1
    Port = 161
    ReadCommunity = "public"
)
IdentityEntry local_auth_identity_01(
    DistinguishedName *= CertDescription (
        Subject *= COMPLETE, "C=RU, O=S-Terra
CSP, OU=Research, CN=GW201"
    )
)
CertDescription local_cert_dsc_01(
    FingerprintMD5 = "611BF60AB890F7E26DC6CA047D671553"
    Issuer *= COMPLETE, "C=RU, L=Moscow, O=S-Terra CSP, OU=Research, CN=CA-W2008SP1-X64-
CA"
    SerialNumber = "61080A6B00000000000003"
    Subject *= COMPLETE, "C=RU, O=S-Terra CSP, OU=Research, CN=GW201"
)
CertDescription partner_cert_dsc_01(
)
IKEParameters (
    BlacklogRelaxTime = 120
    BlacklogSessionsMax = 16
    BlacklogSessionsMin = 0
    BlacklogSilentSessions = 4
    DefaultPort = 500
    InitiatorSessionsMax = 30
    ResponderSessionsMax = 20
    RetryTimeBase = 1
    RetryTimeMax = 30
    SendRetries = 5
    SessionTimeMax = 60
)
AuthMethodGOSTSign auth_method_01(
    LocalCredential = local_cert_dsc_01
    LocalID = local_auth_identity_01
    RemoteCredential *= partner_cert_dsc_01
    SendCertMode = AUTO
    SendRequestMode = AUTO
)
IKETransform ike_trf_01(
    CipherAlg *= "G2814789CPR01-K256-CBC-65534"
    GroupID *= VKO_1B
    HashAlg *= "GR341194CPR01-65534"
    LifetimeSeconds = 28800
    NoSmoothRekeying = FALSE
)
IKETransform ike_trf_02(
    CipherAlg *= "G2814789CPR01-K256-CBC-65534"
    GroupID *= MODP_1536
    HashAlg *= "GR341194CPR01-65534"
    LifetimeSeconds = 28800
    NoSmoothRekeying = FALSE
)
IKETransform ike_trf_03(
    CipherAlg *= "G2814789CPR01-K256-CBC-65534"
    GroupID *= MODP_1024
    HashAlg *= "GR341194CPR01-65534"
```

```

    LifetimeSeconds = 28800
    NoSmoothRekeying = FALSE
)
IKETransform ike_trf_04(
    CipherAlg *= "G2814789CPRO1-K256-CBC-65534"
    GroupID *= MODP_768
    HashAlg *= "GR341194CPRO1-65534"
    LifetimeSeconds = 28800
    NoSmoothRekeying = FALSE
)
ESPTransform esp_trf_01(
    CipherAlg *= "G2814789CPRO1-K288-CNTMAC-253"
    LifetimeKilobytes = 4608000
    LifetimeSeconds = 3600
)
ESPProposal esp_proposal_01(
    Transform = esp_trf_01
)
ESPTransform esp_trf_02(
    CipherAlg *= "G2814789CPRO1-K256-CBC-254"
    IntegrityAlg *= "GR341194CPRO1-H96-HMAC-65534"
    LifetimeKilobytes = 4608000
    LifetimeSeconds = 3600
)
ESPProposal esp_proposal_02(
    Transform = esp_trf_02
)
ESPTransform esp_trf_03(
    CipherAlg *= "G2814789CPRO1-K256-CBC-254"
    IntegrityAlg *= "G2814789CPRO1-K256-MAC-65535"
    LifetimeKilobytes = 4608000
    LifetimeSeconds = 3600
)
ESPProposal esp_proposal_03(
    Transform = esp_trf_03
)
ESPTransform esp_trf_04(
    CipherAlg *= "G2814789CPRO1-K256-CBC-254"
    LifetimeKilobytes = 4608000
    LifetimeSeconds = 3600
)
ESPProposal esp_proposal_04(
    Transform = esp_trf_04
)
IKERule ike_rule_01(
    DPDIIdleDuration = 60
    DPDResponseDuration = 5
    DPDRetries = 3
    DoNotUseDPD = FALSE
    IKECFGBindToPeerAddress = FALSE
    MainModeAuthMethod *= auth_method_01
    Transform *= ike_trf_01,ike_trf_02,ike_trf_03,ike_trf_04
    XAuthServerEnabled = FALSE
)
IPsecAction ipsec_action_01(
    ContainedProposals
    (esp_proposal_01),(esp_proposal_02),(esp_proposal_03),(esp_proposal_04)
    GroupID *= VKO_1B
    IKERule = ike_rule_01
    TunnelingParameters *= TunnelEntry (
        Assemble = FALSE

```

* =

```
        DFHandling = COPY
        PeerIPAddress = 10.0.0.101
        ReRoute = FALSE
    )
)
FilterChain filter_chain_ipsec_01(
    Filters *= Filter (
        Action = PASS
        LogEventID = "ike_autopass_action_01"
        ProtocolID *= 17
        SourcePort *= 500, 4500
    ), Filter (
        Action = PASS
        LogEventID = "pass_action_02"
    )
)
NetworkInterface (
    IPsecPolicy = filter_chain_ipsec_01
)
FilterChain filter_chain_ipsec_02(
    Filters *= Filter (
        Action = PASS
        LogEventID = "ike_autopass_action_02"
        ProtocolID *= 17
        SourcePort *= 500, 4500
    ), Filter (
        Action = PASS
        SourceIP *= 10.0.0.201
        DestinationIP *= 10.0.0.101
        ExtendedAction = ipsec<sa=ipsec_action_01>
        LogEventID = "ipsec_action_01"
    )
)
NetworkInterface (
    IPsecPolicy = filter_chain_ipsec_02
    LogicalName = "GigabitEthernet0/1"
)
```

Текст /opt/l2svc/etc/config.conf для GW101

```
vif tap0
bridge br0
capture eth0
remote 10.0.0.201
mssfix 1400
passtos
```

Текст /opt/l2svc/etc/config.conf для GW201

```
vif tap0
bridge br0
capture eth0
remote 10.0.0.101
mssfix 1400
passtos
```

Текст конфигурации Switch11

```
Current configuration : 1954 bytes
!
```

```
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Switch11
!
boot-start-marker
boot-end-marker
!
no aaa new-model
system mtu routing 1500
authentication mac-move permit
ip subnet-zero
!
!
spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
!
port-channel load-balance dst-ip
!
vlan internal allocation policy ascending
!
interface Port-channel1
!
interface FastEthernet0
  no ip address
  shutdown
!
interface GigabitEthernet0/1
  channel-protocol pagp
  channel-group 1 mode desirable
!
interface GigabitEthernet0/2
  channel-protocol pagp
  channel-group 1 mode desirable
!
interface GigabitEthernet0/3
  channel-protocol pagp
  channel-group 1 mode desirable
!
interface GigabitEthernet0/4
  channel-protocol pagp
  channel-group 1 mode desirable
!
interface GigabitEthernet0/5
!
interface GigabitEthernet0/6
!
interface GigabitEthernet0/7
!
interface GigabitEthernet0/8
!
interface GigabitEthernet0/9
!
interface GigabitEthernet0/10
!
interface GigabitEthernet0/11
!
```

```
interface GigabitEthernet0/12
!
interface GigabitEthernet0/13
!
interface GigabitEthernet0/14
!
interface GigabitEthernet0/15
!
interface GigabitEthernet0/16
!
interface GigabitEthernet0/17
!
interface GigabitEthernet0/18
!
interface GigabitEthernet0/19
!
interface GigabitEthernet0/20
!
interface GigabitEthernet0/21
!
interface GigabitEthernet0/22
!
interface GigabitEthernet0/23
!
interface GigabitEthernet0/24
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4
!
interface TenGigabitEthernet1/1
!
interface TenGigabitEthernet1/2
!
interface Vlan1
  no ip address
  shutdown
!
ip classless
ip http server
ip http secure-server
!
ip sla enable reaction-alerts
!
!
line con 0
line vty 5 15
!
end
```

Текст конфигурации Switch21

```
Current configuration : 1954 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
no service password-encryption
!
hostname Switch21
!
boot-start-marker
boot-end-marker
!
no aaa new-model
system mtu routing 1500
authentication mac-move permit
ip subnet-zero
!
!
spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
!
port-channel load-balance dst-ip
!
vlan internal allocation policy ascending
!
interface Port-channel1
!
interface FastEthernet0
  no ip address
  shutdown
!
interface GigabitEthernet0/1
  channel-protocol pagp
  channel-group 1 mode auto
!
interface GigabitEthernet0/2
  channel-protocol pagp
  channel-group 1 mode auto
!
interface GigabitEthernet0/3
  channel-protocol pagp
  channel-group 1 mode auto
!
interface GigabitEthernet0/4
  channel-protocol pagp
  channel-group 1 mode auto
!
interface GigabitEthernet0/5
!
interface GigabitEthernet0/6
!
interface GigabitEthernet0/7
!
interface GigabitEthernet0/8
!
interface GigabitEthernet0/9
!
interface GigabitEthernet0/10
!
interface GigabitEthernet0/11
!
interface GigabitEthernet0/12
!
interface GigabitEthernet0/13
```

```
!  
interface GigabitEthernet0/14  
!  
interface GigabitEthernet0/15  
!  
interface GigabitEthernet0/16  
!  
interface GigabitEthernet0/17  
!  
interface GigabitEthernet0/18  
!  
interface GigabitEthernet0/19  
!  
interface GigabitEthernet0/20  
!  
interface GigabitEthernet0/21  
!  
interface GigabitEthernet0/22  
!  
interface GigabitEthernet0/23  
!  
interface GigabitEthernet0/24  
!  
interface GigabitEthernet1/1  
!  
interface GigabitEthernet1/2  
!  
interface GigabitEthernet1/3  
!  
interface GigabitEthernet1/4  
!  
interface TenGigabitEthernet1/1  
!  
interface TenGigabitEthernet1/2  
!  
interface Vlan1  
  no ip address  
  shutdown  
!  
ip classless  
ip http server  
ip http secure-server  
!  
ip sla enable reaction-alerts  
!  
!  
line con 0  
line vty 5 15  
!  
end
```