

**Программные комплексы
"Шлюз безопасности
CSP VPN Gate. Версия 3.0"
и
"Шлюз безопасности
CSP RVPN. Версия 3.0"**

**Руководство
администратора**

Примеры конфигураций в различных сценариях

СЦЕНАРИЙ 1	3
СЦЕНАРИЙ 2	12

Здесь приведены два типовых сценария применения шлюза безопасности, роль которого может выполнять программный комплекс «Шлюз безопасности CSP VPN Gate» или программный комплекс «Шлюз безопасности CSP RVPN».

Остальные Сценарии опубликованы на сайте компании по адресу: <http://www.s-terra.com/CSP/RU/support/scn.htm>.

Сценарий 1

Построение VPN туннеля между двумя подсетями при наличии NAT. Аутентификация на сертификатах

Сценарий описывает методику построения защищенного соединения при наличии устройств, транслирующих сетевые адреса шлюзов безопасности.

Описание стенда

На Рисунке 1 изображена схема стенда. Две подсети SN1 (192.168.103.0) и SN2 (192.168.101.0) защищаются шлюзами безопасности GW1 и GW2, и общаются между собой только по защищенному VPN туннелю. На устройствах Router1 и Router2 будет осуществляться трансляция сетевых адресов шлюзов безопасности GW1 и GW2.

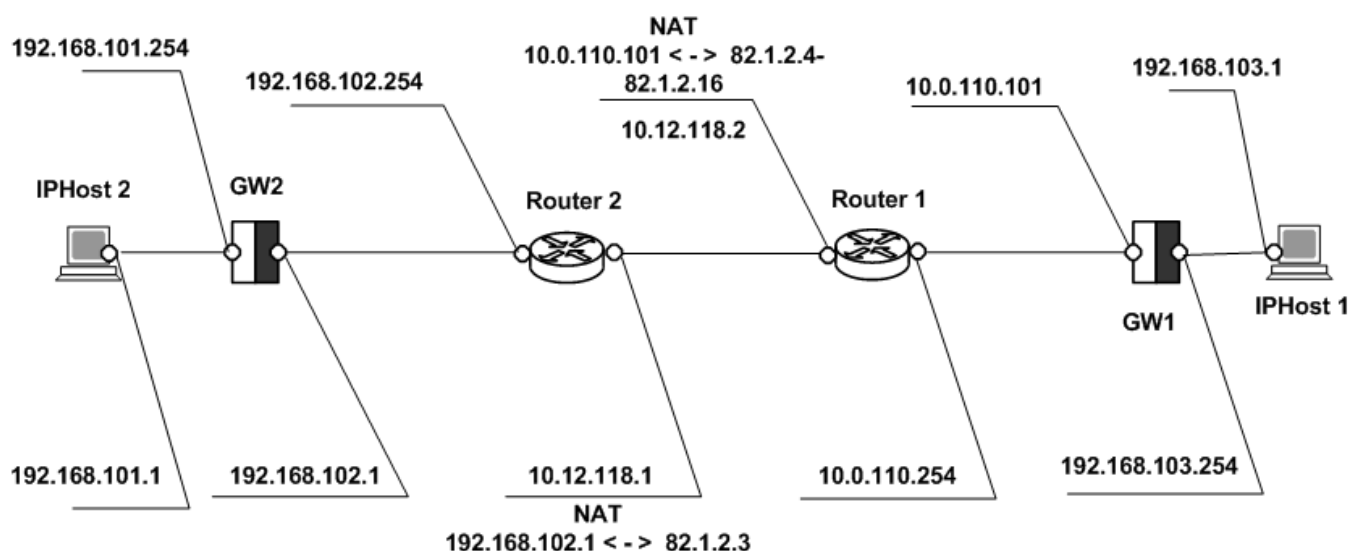


Рисунок 1

Параметры защищенного соединения

Параметры защищенного соединения между шлюзами безопасности GW1 и GW2:

- Аутентификация на сертификатах
- IKE parameters:
 - Encryption algorithm – GOST
 - Hash algorithm – GOST
 - DH-group – group2 (1024)
- IPSec parameters:
 - ESP encryption algorithm – GOST

Настройте два шлюза безопасности GW1, GW2 и настройте остальные устройства стенда.

Настройка шлюза безопасности GW1

Перед созданием конфигурации зарегистрируйте CA сертификат и локальный сертификат в базе Продукта. Создание сертификатов описано в документе [«Шлюзы безопасности CSP VPN Gate и CSP RVPN. Приложение»](#).

Регистрация CA сертификата

Для регистрации CA сертификата на шлюзе безопасности выполните следующие действия:

- На отдельном компьютере с ОС Windows преобразуйте CA сертификат в формат DER encoded binary X.509 (.CER). Для этого воспользуйтесь стандартным приложением для просмотра сертификатов и нажмите кнопку Copy to File, выбрав нужный формат.
- доставьте любым способом файл с CA сертификатом на шлюз безопасности в файловую систему. Например, можно воспользоваться утилитой pscp.exe из пакета Putty для доставки CA сертификата gateca.cer в каталог /certif:

```
pscp -r gateca.cer root@10.0.110.101:/certif
```

- зарегистрируйте CA сертификат в базе Продукта с помощью утилиты cert_mgr import, входящей в состав продукта:

```
/opt/VPNagent/bin# ./cert_mgr import -f /certif/gateca.cer -t
```

Регистрация локального сертификата

Для регистрации локального сертификата в базе Продукта выполните следующие действия:

- доставьте на шлюз безопасности в файловую систему любым способом локальный сертификат, скопированный в формате DER encoded binary X.509 (.CER) в файл. Например, можно доставить на дискете, по протоколам FTP, TFTP или воспользоваться утилитой pscp.exe, описанной для регистрации CA сертификата.

```
pscp -r gate1.cer root@10.0.110.101:/certif
```

- доставьте контейнер с секретным ключом для локального сертификата на шлюз безопасности. Например, для доставки контейнера gate1, представляющего собой каталог при использовании криптографии "Сигнал-КОМ", можно воспользоваться той же утилитой:

```
pscp -r gate1 root@10.0.110.101:/certif
```

- зарегистрируйте локальный сертификат в базе продукта, используя утилиту cert_mgr import из состава продукта. Например, для локального сертификата и контейнера, созданных при использовании криптопровайдера "Signal-COM", команда имеет следующий вид:

```
/opt/VPNagent/bin# ./cert_mgr import -f /certif/gate1.cer -kc  
/certif/gate1
```

- а при использовании криптопровайдера "КриптоПро CSP" регистрация локального сертификата в продукте, контейнер которого размещен на дискете, производится командой примерно следующего вида:

```
/opt/VPNagent/bin/# ./cert_mgr import -f /certif/gate1.cer -  
kc 'FAT12\\gate1.000'
```

Проверим, что регистрация сертификатов в базе Продукта прошла успешно:

```
/opt/VPNagent/bin# ./cert_mgr show
Found 2 certificates. No CRLs found.
1 Status: trusted C=RU,O=GINS,OU=QA,CN=MSCA
2 Status: local 1.2.840.113549.1.9.1=gatel@s-
terra.com,C=RU,ST=Moskow,L=Zelenograd,O=S-Terra,OU=mgmt,CN=gatel
```

Создание политики безопасности

После регистрации сертификатов перейдите к созданию политики безопасности для шлюза GW1. Настройка шлюза безопасности произведите в интерфейсе командной строки. Для входа в консоль, которая имитирует интерфейс командной строки Cisco IOS, перейдите в директорию /opt/VPNagent/bin/ и запустите cs_console:

```
GW1:/opt/VPNagent/bin# ./cs_console
GW1>enable
Password:
```

Перейдите в конфигурационный режим:

```
GW1#configure terminal
Enter configuration commands, one per line.
GW1(config)#
```

Установите тип идентификатора партнера для IKE:

```
crypto isakmp identity dn
```

Задайте параметры IKE:

```
GW1(config)#crypto isakmp policy 1
GW1(config-isakmp)# hash md5
GW1(config-isakmp)# encryption des
GW1(config-isakmp)# authentication rsa-sig
GW1(config-isakmp)# group 2
GW1(config-isakmp)#exit
GW1(config)#
```

Создайте набор преобразований для IPsec:

```
GW1(config)#crypto ipsec transform-set GOST esp-des
GW1(cfg-crypto-trans)# mode tunnel
GW1(cfg-crypto-trans)#exit
GW1(config)#
```

Общие настройки на этом закончены. Далее надо описать параметры защищенного соединения GW1 – GW2:

опишите трафик, который планируется шифровать, для этого создайте расширенный access list:

```
GW1(config)#ip access-list extended Subnet-Subnet
GW1(config-ext-nacl)# permit ip 192.168.103.0 0.0.0.255
192.168.101.0 0.0.0.255
GW1(config-ext-nacl)#exit
GW1(config)#
```

создайте криптографическую карту для связывания всех параметров соединения:

```
GW1(config)#crypto map CMAP 1 ipsec-isakmp
GW1(config-crypto-map)# match address Subnet-Subnet
GW1(config-crypto-map)# set transform-set GOST
GW1(config-crypto-map)# set pfs group2
GW1(config-crypto-map)# set peer 82.1.2.3
GW1(config-crypto-map)#exit
GW1(config)#
```

отключите обработку списка отозванных сертификатов (CRL):

```
GW1(config)#crypto pki trustpoint s-
terra_technological_trustpoint
GW1(ca-trustpoint)# revocation-check none
GW1(ca-trustpoint)#exit
GW1(config)#
```

привяжите криптокарту к интерфейсу:

```
GW1(config)#interface FastEthernet0/0
GW1(config-if)# crypto map CMAP
GW1(config-if)# ip address 10.0.110.101 255.255.0.0
GW1(config-if)#exit
GW1(config)#exit

GW1(config)#interface FastEthernet0/1
GW1(config-if)# ip address 192.168.103.254 255.255.255.0
GW1(config-if)#exit
GW1(config)#exit
```

Настройка устройства GW1 завершена. При выходе из конфигурационного режима происходит загрузка конфигурации на шлюз безопасности GW1.

Получить политику безопасности (LSP) в текстовом формате, можно, используя утилиту `lsp_mgr show` из каталога продукта `/opt/VPNagent/bin/`.

Настройка маршрутизации

После создания конфигурации и выхода из консоли настройте маршрутизацию шлюза GW1.

В качестве шлюза по умолчанию выберите адрес устройства Router1 – 10.0.110.254.

В Приложении представлена [таблица маршрутизации](#) для шлюза безопасности GW1.

На этом настройка шлюза безопасности GW1 закончено.

Настройка шлюза безопасности GW2

Регистрация СА и локального сертификатов

Зарегистрируйте в продукте CSP VPN Gate на шлюзе безопасности GW2 СА и локальный сертификаты, как было описано для шлюза безопасности GW1.

Создание политики безопасности

Создание политики безопасности для шлюза безопасности GW2 также выполните в интерфейсе командной строки.

Конфигурация для шлюза GW2 приведена в [Приложении](#).

Настройка маршрутизации

В качестве шлюза по умолчанию выберите адрес устройства Router2 - 192.168.102.254.

В Приложении представлена [таблица маршрутизации](#) для шлюза безопасности GW2.

На этом настройка шлюза безопасности GW2 закончено.

Настройка устройства Router1

На устройстве Router1 в качестве шлюза по умолчанию нужно указать адрес Router2 - 10.12.118.1.

Также на этом устройстве необходимо настроить NAT таким образом, чтобы адрес 10.0.110.101 динамически транслировался в диапазон адресов 82.1.2.4 – 82.1.2.16.

Настройка устройства Router2

На устройстве Router2 в качестве шлюза по умолчанию нужно установить адрес Router1 - 10.12.118.2.

Также на этом устройстве необходимо настроить NAT таким образом, чтобы адрес 192.168.102.1 статически транслировался в адрес 82.1.2.3.

Настройка устройства IPHost1

На устройстве IPHost1 в качестве шлюза по умолчанию нужно указать адрес внутреннего интерфейса шлюза безопасности GW1 - 192.168.103.254.

Настройка устройства IPHost2

На этом устройстве в качестве шлюза по умолчанию нужно указать адрес внутреннего интерфейса шлюза безопасности GW2 - 192.168.101.254.

Приложение к Сценарию 1

Таблица маршрутов устройства GW1

Routing Table: IPv4

Destination	Gateway	Flags	Ref	Use	Interface
-----	-----	-----	-----	-----	-----
192.168.103.0	192.168.103.254	U	1	5	rtls1
10.0.0.0	10.0.110.101	U	1	73	rtls0

224.0.0.0	10.0.110.101	U	1	0	rtls0
default	10.0.110.254	UG	1	101	
127.0.0.1	127.0.0.1	UH	2	787	lo0

Таблица маршрутов устройства GW2

Routing Table: IPv4

Destination	Gateway	Flags	Ref	Use	Interface
-----	-----	-----	-----	-----	-----
192.168.101.0	192.168.101.254	U	1	4	rtls0
192.168.102.0	192.168.102.1	U	1	65	iprb0
224.0.0.0	192.168.102.1	U	1	0	iprb0
default	192.168.102.254	UG	1	162	
127.0.0.1	127.0.0.1	UH	31993825		lo0

Вывод команды ifconfig –а устройства GW1

```
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232
index 1

    inet 127.0.0.1 netmask ff000000

rtls0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu
1500 index 2

    inet 10.0.110.101 netmask ffff0000 broadcast
10.0.255.255

    ether 0:50:fc:90:7f:1c

rtls1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu
1500 index 3

    inet 192.168.103.254 netmask fffffff0 broadcast
192.168.103.255

    ether 4c:0:10:71:5c:b6
```

Вывод команды ifconfig –а устройства GW2

```
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232
index 1

    inet 127.0.0.1 netmask ff000000

iprb0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu
1500 index 2

    inet 192.168.102.1 netmask fffffff0 broadcast
192.168.102.255

    ether 0:a0:c9:85:6f:17

iprb1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu
1500 index 3

    inet 192.168.101.254 netmask fffffff0 broadcast
192.168.101.255

    ether 0:e:a6:78:83:2d
```

Текст конфигурации GW1

Ниже приведена конфигурация для шлюза GW1:

```
GW1#show run
version 12.4
no service password-encryption
crypto ipsec df-bit clear
crypto isakmp identity dn
username cscons password csp
hostname cspgate
enable password csp
logging trap debugging
crypto isakmp policy 1
  hash md5
  encr des
  group 2
crypto ipsec transform-set GOST esp-des
ip access-list extended CryptoAcl
  permit ip 192.168.103.0 0.0.0.255 192.168.101.0 0.0.0.255
crypto map CMAP 1 ipsec-isakmp
  match address CryptoAcl
  set transform-set GOST
  set pfs group2
  set peer 82.1.2.3

interface FastEthernet0/1
  ip address 192.168.103.254 255.255.255.0
interface FastEthernet0/0
  ip address 10.0.110.101 255.255.0.0
  crypto map CMAP

(*следующие команды появляются в конфигурации после регистрации
CA сертификата*)
crypto pki trustpoint s-terra_technological_trustpoint
  revocation-check none
crypto pki certificate chain s-terra_technological_trustpoint
certificate 33AE6C6B85536F834A8D8E5358333F4F
30820337308202E4A003020102021033AE6C6B85536F834A8D8E5358333F4F30
0A06062A850302020405003038310B3009060355040613025255310D300B0603
55040A130447494E53310B3009060355040B13025141310D300B060355040313
044D534341301E170D3033303831353132313432365A170D3133303831353132
323331315A3038310B3009060355040613025255310D300B060355040A130447
494E53310B3009060355040B13025141310D300B060355040313044D53434130
81A5301C06062A8503020214301206072A85030202200206072A850302021E01
038184000481807856C3E39A3871868AB1A95406857899963E5FB1368EFDD4EE
00B9ABC63CF37FF0694358C90137E9FE22E333EBE6F5C67BA2ED497C4951CA72
4101BCB552C99CF357C22E3962E772BFCE681E324B318E25CA222F7AD15E3DEB
```

```
182BB8CD5C1499F9B7AEE9630982B6F20217CE73B9FADAD25DF85E41F72C3CC9
EAD30A1761233FA38201813082017D301306092B060104018237140204061E04
00430041300B0603551D0F040403020146300F0603551D130101FF0405300301
01FF301D0603551D0E04160414AF466A089157E764B3560AC6DAAA99D655E145
52308201150603551D1F0482010C308201083081C3A081C0A081BD8681BA6C64
61703A2F2F2F434E3D4D5343412C434E3D76772D77326B6164762C434E3D4344
502C434E3D5075626C69632532304B657925323053657276696365732C434E3D
53657276696365732C434E3D436F6E66696775726174696F6E2C44433D71616D
7363612C44433D67696E736F6674776172652C44433D72753F63657274696669
636174655265766F636174696F6E4C6973743F626173653F6F626A656374636C
6173733D63524C446973747269627574696F6E506F696E743040A03EA03C863A
687474703A2F2F76772D77326B6164762E71616D7363612E67696E736F667477
6172652E72752F43657274456E726F6C6C2F4D5343412E63726C301006092B06
010401823715010403020100300A06062A850302020405000341003F58DCDD86
C752B99C4BF09FE1CA9E5B567B19904B0B2BC6BE654A29E05550033B7F94B498
C5E6BBF6440FCB9624390F48E3A97835867E8C4346EA84952361F3
```

Quit

exit

Текст конфигурации GW2

```
GW2#show run
version 12.4
no service password-encryption
crypto ipsec df-bit clear
crypto isakmp identity dn
crypto ipsec security-association lifetime kilobytes 4608011
crypto isakmp keepalive 10 3
username cscons password csp
hostname stndgate
enable password csp
logging trap debugging
crypto isakmp policy 1
  hash md5
  encr des
  group 2
crypto ipsec transform-set GOST esp-des
ip access-list extended CryptoAcl
  permit ip 192.168.101.0 0.0.0.255 192.168.103.0 0.0.0.255
!
crypto dynamic-map Dmap 1
  match address CryptoAcl
  set transform-set GOST
  set pfs group2
!
crypto map CMAP 1 ipsec-isakmp dynamic Dmap
interface FastEthernet0/0
  ip address 192.168.102.1 255.255.255.0
```

```

crypto map CMAP
interface FastEthernet0/1
 ip address 192.168.101.254 255.255.255.0
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check none
crypto pki certificate chain s-terra_technological_trustpoint
certificate 33AE6C6B85536F834A8D8E5358333F4F
30820337308202E4A003020102021033AE6C6B85536F834A8D8E5358333F4F30
0A06062A850302020405003038310B3009060355040613025255310D300B0603
55040A130447494E53310B3009060355040B13025141310D300B060355040313
044D534341301E170D3033303831353132313432365A170D3133303831353132
323331315A3038310B3009060355040613025255310D300B060355040A130447
494E53310B3009060355040B13025141310D300B060355040313044D53434130
81A5301C06062A8503020214301206072A85030202200206072A850302021E01
038184000481807856C3E39A3871868AB1A95406857899963E5FB1368EFDD4EE
00B9ABC63CF37FF0694358C90137E9FE22E333EBE6F5C67BA2ED497C4951CA72
4101BCB552C99CF357C22E3962E772BFCE681E324B318E25CA222F7AD15E3DEB
182BB8CD5C1499F9B7AEE9630982B6F20217CE73B9FADAD25DF85E41F72C3CC9
EAD30A1761233FA38201813082017D301306092B060104018237140204061E04
00430041300B0603551D0F040403020146300F0603551D130101FF0405300301
01FF301D0603551D0E04160414AF466A089157E764B3560AC6DAAA99D655E145
52308201150603551D1F0482010C308201083081C3A081C0A081BD8681BA6C64
61703A2F2F2F434E3D4D5343412C434E3D76772D77326B6164762C434E3D4344
502C434E3D5075626C69632532304B657925323053657276696365732C434E3D
53657276696365732C434E3D436F6E66696775726174696F6E2C44433D71616D
7363612C44433D67696E736F6674776172652C44433D72753F63657274696669
636174655265766F636174696F6E4C6973743F626173653F6F626A656374636C
6173733D63524C446973747269627574696F6E506F696E743040A03EA03C863A
687474703A2F2F76772D77326B6164762E71616D7363612E67696E736F667477
6172652E72752F43657274456E726F6C6C2F4D5343412E63726C301006092B06
010401823715010403020100300A06062A850302020405000341003F58DCDD86
C752B99C4BF09FE1CA9E5B567B19904B0B2BC6BE654A29E05550033B7F94B498
C5E6BBF6440FCB9624390F48E3A97835867E8C4346EA84952361F3
quit
exit
end

```

Сценарий 2

Построение VPN туннеля между подсетями через центральный шлюз с перешифрованием трафика в топологии «звезда». Аутентификация на preshared key

Описание стенда

Сценарий иллюстрирует построение VPN туннелей между тремя подсетями, которые защищаются шлюзами безопасности CSP VPN Gate. VPN туннели, которые будут построены между устройствами GW1, GW2 и GW3, изображены на Рисунке 1. Шлюз GW3 является центральным. Между шлюзами GW1 и GW2 строится защищенное соединение только через центральный шлюз. Устройства Host1, Host2 и Host3 могут общаться между собой по VPN туннелю. Внутри подсетей SN1, SN2 и SN3 трафик является “открытым”.

Параметры защищенного соединения:

- Метод аутентификации – Preshared Key.
- IKE parameters:
 - Encryption algorithm – GOST
 - Hash algorithm – GOST
 - DH-group – group2 (1024)
- IPSec parameters:
 - ESP encryption algorithm – GOST

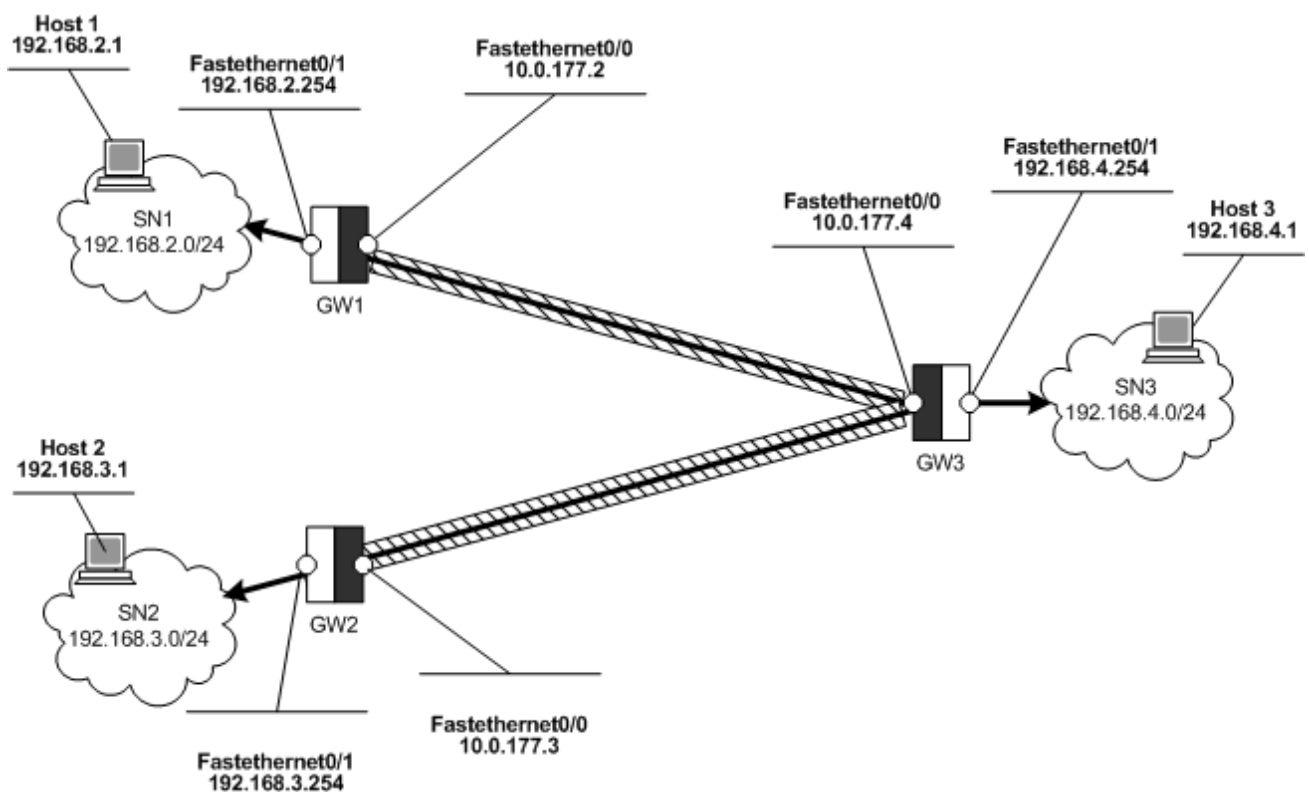


Рисунок 2



Предварительные настройки

Перед созданием защищенного соединения необходимо настроить маршрутизацию и убедиться в том, что на устройствах стенда сделаны корректные настройки. Для этого:

На устройствах Host1, Host2 и Host3 зададим адреса маршрутизаторов по умолчанию (default gateway):

на Host1 в качестве шлюза по умолчанию назначим адрес 192.168.2.254
 на Host2 назначим адрес 192.168.3.254
 на Host3 - адрес 192.168.4.254

На шлюзе GW1 укажем маршруты в подсети, которые защищаются шлюзами-партнерами. Для этого в глобальном конфигурационном режиме cs_console зададим команды:

```
ip route 192.168.3.0 255.255.255.0 10.0.177.4 1
ip route 192.168.4.0 255.255.255.0 10.0.177.4 1
```

На шлюзе GW2 выполним аналогичные действия:

```
ip route 192.168.2.0 255.255.255.0 10.0.177.4 1
ip route 192.168.4.0 255.255.255.0 10.0.177.4 1
```

На шлюзе GW3 выполним такие же действия:

```
ip route 192.168.2.0 255.255.255.0 10.0.177.2 1
ip route 192.168.3.0 255.255.255.0 10.0.177.3 1
```

После выполнения настроек убедимся, что пакеты маршрутизируются верно. Для этого на устройстве Host2 выполним команду traceroute 192.168.2.1:

```
traceroute 192.168.2.1

traceroute to 192.168.2.1 (192.168.2.1), 30 hops max, 40 byte
packets
 1  192.168.3.254 (192.168.3.254)  0.980 ms  0.850 ms  0.691
ms
 2  10.0.177.4 (10.0.177.4)  0.731 ms  0.873 ms  0.711 ms
 3  10.0.177.2 (10.0.177.2)  0.797 ms  0.844 ms  0.690 ms
 4  192.168.2.1 (192.168.2.1)  0.838 ms  0.925 ms  0.791 ms
```

Убедимся, что устройства в подсетях SN1 и SN2 доступны из подсети SN3. Для этого на устройстве Host3 выполним:

```
ping 192.168.2.1

PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=253 time=1.17 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=253 time=0.984 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=253 time=0.642 ms
64 bytes from 192.168.2.1: icmp_seq=4 ttl=253 time=0.637 ms

ping 192.168.3.1
```

```
PING 192.168.3.1 (192.168.3.1) 56(84) bytes of data.  
64 bytes from 192.168.3.1: icmp_seq=1 ttl=253 time=1.17 ms  
64 bytes from 192.168.3.1: icmp_seq=2 ttl=253 time=0.984 ms  
64 bytes from 192.168.3.1: icmp_seq=3 ttl=253 time=0.642 ms  
64 bytes from 192.168.3.1: icmp_seq=4 ttl=253 time=0.637 ms
```

Настройка шлюза безопасности GW3

Настройку шлюза безопасности GW3 будем производить в интерфейсе командной строки. Для входа в консоль перейдем в директорию /opt/VPNagent/bin/ и запустим cs_console. В глобальном конфигурационном режиме выполним следующее:

зададим параметры для IKE:

```
gw3(config)#crypto isakmp policy 1  
gw3(config-isakmp)#hash md5  
gw3(config-isakmp)#encryption des  
gw3(config-isakmp)#authentication pre-share  
gw3(config-isakmp)#group 2  
gw3(config-isakmp)#exit
```

создадим предопределенные ключи для шлюзов GW1 и GW2:

```
gw3(config)#crypto isakmp key 1258 address 10.0.177.2  
gw3(config)#crypto isakmp key 1258 address 10.0.177.3
```

создадим набор преобразований для IPsec:

```
gw3(config)#crypto ipsec transform-set Gost esp-des  
gw3(cfg-crypto-trans)#mode tunnel  
gw3(cfg-crypto-trans)#exit
```

опишем трафик, который планируется защищать:

```
gw3(config)#ip access-list extended SN3toSN2  
gw3(config-ext-nacl)#permit ip 192.168.4.0 0.0.0.255  
192.168.3.0 0.0.0.255  
gw3(config-ext-nacl)#exit
```

```
gw3(config)#ip access-list extended SN3toSN1  
gw3(config-ext-nacl)#permit ip 192.168.4.0 0.0.0.255  
192.168.2.0 0.0.0.255  
gw3(config-ext-nacl)#exit
```

```
gw3(config)#ip access-list extended SN1toSN2  
gw3(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255  
192.168.3.0 0.0.0.255  
gw3(config-ext-nacl)#exit
```

```
gw3(config)#ip access-list extended SN2toSN1  
gw3(config-ext-nacl)#permit ip 192.168.3.0 0.0.0.255  
192.168.2.0 0.0.0.255  
gw3(config-ext-nacl)#exit
```

создадим криптокарту:

```
gw3(config)#crypto map CMAP 1 ipsec-isakmp  
gw3(config-crypto-map)#match address SN3toSN2  
gw3(config-crypto-map)#set transform-set Gost  
gw3(config-crypto-map)#set peer 10.0.177.3
```

```
gw3(config)#crypto map CMAP 2 ipsec-isakmp  
gw3(config-crypto-map)#match address SN3toSN1  
gw3(config-crypto-map)#set transform-set Gost
```

```
gw3(config-crypto-map)#set peer 10.0.177.2

gw3(config)#crypto map CMAP 3 ipsec-isakmp
gw3(config-crypto-map)#match address SN1toSN2
gw3(config-crypto-map)#set transform-set Gost
gw3(config-crypto-map)#set peer 10.0.177.3

gw3(config)#crypto map CMAP 4 ipsec-isakmp
gw3(config-crypto-map)#match address SN2toSN1
gw3(config-crypto-map)#set transform-set Gost
gw3(config-crypto-map)#set peer 10.0.177.2
```

привяжем криптокарту к интерфейсу, на котором будут terminating туннели:

```
gw3(config)#interface FastEthernet0/0
gw3(config-if)# crypto map CMAP
gw3(config-if)#exit
```

Настройка устройства GW3 завершена. При выходе из конфигурационного режима произойдет загрузка конфигурации. Устройство готово к работе.

В Приложении приведена [текстовая конфигурация](#), текст которой можно просмотреть при помощи утилиты `lsp_mgr` с опцией `show`. Утилита входит в состав CSP VPN Gate и находится в каталоге `/opt/VPNagent/bin/`.

Настройка шлюза безопасности GW1

Настройку шлюза безопасности GW1 будем производить аналогично устройству GW1. Создадим политику безопасности, приведенную в [Приложении](#).

Настройка шлюза безопасности GW2

Конфигурация для этого устройства приведена в [Приложении](#).

Проверка работоспособности стенда

После загрузки конфигурации на GW1, GW2 и GW3 иницируем создание VPN туннелей. Для этого:

выполним команду `ping 192.168.4.1` на устройстве Host1:

```
ping 192.168.4.1

PING 192.168.4.1 (192.168.4.1) from 192.168.2.1 : 56(84)
bytes of data.
64 bytes from 192.168.4.1: icmp_seq=0 ttl=253 time=548.495
msec
64 bytes from 192.168.4.1: icmp_seq=1 ttl=253 time=1.318 msec
64 bytes from 192.168.4.1: icmp_seq=2 ttl=253 time=930 usec

--- 192.168.4.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.930/183.581/548.495/258.033
ms
```

также выполним команду `ping 192.168.4.1` на устройстве Host 2:

```
ping 192.168.4.1
```

```
PING 192.168.4.1 (192.168.4.1) 56(84) bytes of data.  
64 bytes from 192.168.4.1: icmp_seq=1 ttl=253 time=139 ms  
64 bytes from 192.168.4.1: icmp_seq=2 ttl=253 time=0.625 ms  
64 bytes from 192.168.4.1: icmp_seq=3 ttl=253 time=0.621 ms  
64 bytes from 192.168.4.1: icmp_seq=4 ttl=253 time=0.652 ms  
  
--- 192.168.4.1 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time  
2998ms  
rtt min/avg/max/mdev = 0.621/35.275/139.202/60.002 ms
```

выполним команду ping и на устройстве Host2:

```
ping 192.168.3.1  
  
PING 192.168.3.1 (192.168.3.1) from 192.168.2.1 : 56(84)  
bytes of data.  
64 bytes from 192.168.3.1: icmp_seq=0 ttl=59 time=711.478  
msec  
64 bytes from 192.168.3.1: icmp_seq=1 ttl=59 time=1.982 msec  
64 bytes from 192.168.3.1: icmp_seq=2 ttl=59 time=5.508 msec  
64 bytes from 192.168.3.1: icmp_seq=3 ttl=59 time=1.716 msec  
  
--- 192.168.3.1 ping statistics ---  
4 packets transmitted, 4 packets received, 0% packet loss  
round-trip min/avg/max/mdev = 1.716/180.171/711.478/306.753  
ms
```

В результате, между устройствами GW1, GW2 и GW3 должны установиться 4 VPN туннеля: из SN1 в SN3, из SN2 в SN3 и два туннеля для защиты трафика между подсетями SN1 - SN2. Убедиться в этом можно при помощи утилиты sa_show.

На устройстве GW3 выполним команду:

```
/opt/VPNagent/bin/sa_show  
  
IPSec SA Num (Remote Addr,Port)-(Local Addr,Port) Protocol  
Action Type Sent Rec  
IPSec SA 1 (192.168.2.0-192.168.2.255,*)-(192.168.4.0-  
192.168.4.255,*) * ESP tunn 252 1364  
IPSec SA 2 (192.168.2.0-192.168.2.255,*)-(192.168.3.0-  
192.168.3.255,*) * ESP tunn 336 496  
IPSec SA 3 (192.168.3.0-192.168.3.255,*)-(192.168.2.0-  
192.168.2.255,*) * ESP tunn 336 496  
IPSec SA 4 (192.168.3.0-192.168.3.255,*)-(192.168.4.0-  
192.168.4.255,*) * ESP tunn 336 496
```

Данные настройки обеспечивают защищенный обмен между подсетями SN1, SN2 и SN3. Остальной трафик разрешен, но защищаться не будет.

Приложение к Сценарию 2

Текст cisco-like конфигурации для GW1

```
version 12.4
no service password-encryption

crypto ipsec df-bit copy
crypto isakmp identity address
crypto isakmp keepalive 10 3
username cscons password csp
hostname suppgate
enable password csp

logging trap debugging

crypto isakmp policy 1
  hash md5
  encr des
  authentication pre-share
  group 2

crypto isakmp key 1258 address 10.0.177.4
crypto ipsec transform-set Gost esp-des

ip access-list extended SN1toSN3
  permit ip 192.168.2.0 0.0.0.255 192.168.4.0 0.0.0.255

ip access-list extended SN1toSN2
  permit ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255

crypto map CMAP 1 ipsec-isakmp
  match address SN1toSN3
  set transform-set Gost
  set peer 10.0.177.4

crypto map CMAP 2 ipsec-isakmp
  match address SN1toSN2
  set transform-set Gost
  set peer 10.0.177.4
interface FastEthernet0/1
```

```
ip address 192.168.2.254 255.255.255.0
interface FastEthernet0/0
ip address 10.0.177.2 255.255.255.0
crypto map CMAP

ip route 192.168.3.0 255.255.255.0 10.0.177.4 1
ip route 192.168.4.0 255.255.255.0 10.0.177.4 1
```

Текст LSP для GW1

```
# This is automatically generated LSP
#
# Conversion Date/Time: Thu Nov 29 12:01:27 2007

GlobalParameters(
    Title = "This LSP was automatically
generated by CSP Converter at Thu Nov 29 12:01:27 2007"
    Version = "3.0"
    LDAPLogMessageLevel = DEBUG
    SystemLogMessageLevel = DEBUG
    PolicyLogMessageLevel = DEBUG
    CertificatesLogMessageLevel = DEBUG
)

SyslogSettings(
    Server = 127.0.0.1
    Facility = LOG_LOCAL7
)

RoutingTable(
    Routes *=
        Route(
            Destination = 192.168.3.0/24
            Gateway = 10.0.177.4
            Metric = 1
        ),
        Route(
            Destination = 192.168.4.0/24
            Gateway = 10.0.177.4
            Metric = 1
        )
    )
)
```

```

IKETransform IKETransform_1
(
    CipherAlg      *= "G2814789CPRO1-K256-CBC-65534"
    HashAlg        *= "GR341194CPRO1-65534"
    GroupID        *= MODP_1024
    LifetimeSeconds = 86400
)

ESPProposal ESP_Gost
(
    Transform* = ESPTransform
    (
        CipherAlg*      = "G2814789CPRO1-K256-CBC-254"
        LifetimeSeconds  = 3600
        LifetimeKilobytes = 4608000
    )
)

ESPProposal ESP_Gost_1
(
    Transform* = ESPTransform
    (
        CipherAlg*      = "G2814789CPRO1-K256-CBC-254"
        LifetimeSeconds  = 3600
        LifetimeKilobytes = 4608000
    )
)

FilteringRule Filter_nil_acl
(
    LocalIPFilter *= FilterEntry( IPAddress *=
0.0.0.0..255.255.255.255 )
    PeerIPFilter  *= FilterEntry( IPAddress *=
0.0.0.0..255.255.255.255 )
    NetworkInterfaces *= "rtls1"
    Action *= ( PASS )
)

AuthMethodPreshared IKE_auth_cs_key_10_0_177_4
(

```

```
RemoteID = IdentityEntry(
    IPv4Address *= 10.0.177.4
)
SharedIKESecret = "cs_key_10_0_177_4"
)

IKERule IKE_CMAP_1
(
    Transform* = IKETransform_1
    AggrModeAuthMethod *= IKE_auth_cs_key_10_0_177_4
    MainModeAuthMethod *= IKE_auth_cs_key_10_0_177_4
    DoAutopass          = TRUE
    DPDIdleDuration     = 10
    DPDResponseDuration = 3
    DPDRetries          = 5
)

IPsecAction CMAP_1
(
    TunnelingParameters *= TunnelEntry(
        PeerIPAddress = 10.0.177.4

        DFHandling=COPY
    )
    ContainedProposals *= ( ESP_Gost )
    IKERule = IKE_CMAP_1
)

AuthMethodPreshared IKE_auth_cs_key_10_0_177_4_1
(
    RemoteID = IdentityEntry(
        IPv4Address *= 10.0.177.4
    )
    SharedIKESecret = "cs_key_10_0_177_4"
)

IKERule IKE_CMAP_2
(
    Transform* = IKETransform_1
    AggrModeAuthMethod *= IKE_auth_cs_key_10_0_177_4_1
    MainModeAuthMethod *= IKE_auth_cs_key_10_0_177_4_1
    DoAutopass          = TRUE
```

```
DPDIdleDuration      = 10
DPDResponseDuration  = 3
DPDRetries           = 5
)

IPsecAction CMAP_2
(
    TunnelingParameters *= TunnelEntry(
        PeerIPAddress = 10.0.177.4

        DFHandling=COPY
    )
    ContainedProposals *= ( ESP_Gost_1 )
    IKERule = IKE_CMAP_2
)

FilteringRule Filter_nil_acl_CMAP_1
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.2.0/24 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.4.0/24 )
    NetworkInterfaces *= "rtls0"
    Action *= ( CMAP_1 )
)

FilteringRule Filter_nil_acl_CMAP_2
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.2.0/24 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.3.0/24 )
    NetworkInterfaces *= "rtls0"
    Action *= ( CMAP_2 )
)

FilteringRule Filter_nil_acl_1
(
    LocalIPFilter *= FilterEntry( IPAddress *=
0.0.0.0..255.255.255.255 )
    PeerIPFilter  *= FilterEntry( IPAddress *=
0.0.0.0..255.255.255.255 )
    NetworkInterfaces *= "rtls0"
    Action *= ( PASS )
)
```

Текст cisco-like конфигурации для GW2

```
version 12.4
no service password-encryption
crypto ipsec df-bit copy
crypto isakmp identity address
crypto isakmp keepalive 120 10
username cscons password csp
hostname suppgw
enable password csp

logging trap debugging

crypto isakmp policy 1
  hash md5
  encr des
  authentication pre-share
  group 2

crypto isakmp key 1258 address 10.0.177.4

crypto ipsec transform-set Gost esp-des

ip access-list extended SN2toSN3
  permit ip 192.168.3.0 0.0.0.255 192.168.4.0 0.0.0.255

ip access-list extended SN2toSN1
  permit ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255

crypto map CMAP 1 ipsec-isakmp
  match address SN2toSN3
  set transform-set Gost
  set peer 10.0.177.4

crypto map CMAP 2 ipsec-isakmp
  match address SN2toSN1
  set transform-set Gost
  set peer 10.0.177.4

interface FastEthernet0/1
  ip address 192.168.3.254 255.255.255.0
interface FastEthernet0/0
```

```
ip address 10.0.177.3 255.255.0.0
crypto map CMAP

ip route 192.168.2.0 255.255.255.0 10.0.177.4 1
ip route 192.168.4.0 255.255.255.0 10.0.177.4 1
```

Текст LSP для GW2

```
# This is automatically generated LSP
#
# Conversion Date/Time: Thu Nov 29 12:01:18 2007

GlobalParameters(
    Title = "This LSP was automatically
generated by CSP Converter at Thu Nov 29 12:01:18 2007"
    Version = "3.0"
    LDAPLogMessageLevel = DEBUG
    SystemLogMessageLevel = DEBUG
    PolicyLogMessageLevel = DEBUG
    CertificatesLogMessageLevel = DEBUG
)

SyslogSettings(
    Server = 127.0.0.1
    Facility = LOG_LOCAL7
)

RoutingTable(
    Routes *=
        Route(
            Destination = 192.168.2.0/24
            Gateway = 10.0.177.4
            Metric = 1
        ),
        Route(
            Destination = 192.168.4.0/24
            Gateway = 10.0.177.4
            Metric = 1
        )
)

IKETransform IKETransform_1
```

```
(
    CipherAlg      *= "G2814789CPRO1-K256-CBC-65534"
    HashAlg        *= "GR341194CPRO1-65534"
    GroupID        *= MODP_1024
    LifetimeSeconds = 86400
)

ESPProposal ESP_Gost
(
    Transform* = ESPTransform
    (
        CipherAlg*      = "G2814789CPRO1-K256-CBC-254"
        LifetimeSeconds  = 3600
        LifetimeKilobytes = 4608000
    )
)

ESPProposal ESP_Gost_1
(
    Transform* = ESPTransform
    (
        CipherAlg*      = "G2814789CPRO1-K256-CBC-254"
        LifetimeSeconds  = 3600
        LifetimeKilobytes = 4608000
    )
)

FilteringRule Filter_nil_acl
(
    LocalIPFilter *= FilterEntry( IPAddress *=
0.0.0.0..255.255.255.255 )
    PeerIPFilter  *= FilterEntry( IPAddress *=
0.0.0.0..255.255.255.255 )
    NetworkInterfaces *= "rtls1"
    Action *= ( PASS )
)

AuthMethodPreshared IKE_auth_cs_key_10_0_177_4
(
    RemoteID = IdentityEntry(
```

```
        IPv4Address *= 10.0.177.4
    )
    SharedIKESecret = "cs_key_10_0_177_4"
)

IKERule IKE_CMAP_1
(
    Transform* = IKETransform_1
    AggrModeAuthMethod *= IKE_auth_cs_key_10_0_177_4
    MainModeAuthMethod *= IKE_auth_cs_key_10_0_177_4
    DoAutopass          = TRUE
    DPDIdleDuration     = 120
    DPDResponseDuration = 10
    DPDRetries          = 5
)

IPsecAction CMAP_1
(
    TunnelingParameters *= TunnelEntry(
        PeerIPAddress = 10.0.177.4

        DFHandling=COPY
    )
    ContainedProposals *= ( ESP_Gost )
    IKERule = IKE_CMAP_1
)

AuthMethodPreshared IKE_auth_cs_key_10_0_177_4_1
(
    RemoteID = IdentityEntry(
        IPv4Address *= 10.0.177.4
    )
    SharedIKESecret = "cs_key_10_0_177_4"
)

IKERule IKE_CMAP_2
(
    Transform* = IKETransform_1
    AggrModeAuthMethod *= IKE_auth_cs_key_10_0_177_4_1
    MainModeAuthMethod *= IKE_auth_cs_key_10_0_177_4_1
    DoAutopass          = TRUE
    DPDIdleDuration     = 120
```

```

        DPDResponseDuration = 10
        DPDRetries           = 5
    )

IPsecAction CMAP_2
(
    TunnelingParameters *= TunnelEntry(
        PeerIPAddress = 10.0.177.4

        DFHandling=COPY
    )
    ContainedProposals *= ( ESP_Gost_1 )
    IKERule = IKE_CMAP_2
)

FilteringRule Filter_nil_acl_CMAP_1
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.3.0/24 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.4.0/24 )
    NetworkInterfaces *= "rtls0"
    Action *= ( CMAP_1 )
)

FilteringRule Filter_nil_acl_CMAP_2
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.3.0/24 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.2.0/24 )
    NetworkInterfaces *= "rtls0"
    Action *= ( CMAP_2 )
)

FilteringRule Filter_nil_acl_1
(
    LocalIPFilter *= FilterEntry( IPAddress *=
0.0.0.0..255.255.255.255 )
    PeerIPFilter  *= FilterEntry( IPAddress *=
0.0.0.0..255.255.255.255 )
    NetworkInterfaces *= "rtls0"
    Action *= ( PASS )
)

```

Текст cisco-like конфигурации для GW3

```
version 12.4
no service password-encryption
crypto ipsec df-bit copy
crypto isakmp identity address
username cscons password csp
hostname cspgate
enable password csp

logging trap debugging

crypto isakmp policy 1
  hash md5
  encr des
  authentication pre-share
  group 2

crypto isakmp key 1258 address 10.0.177.2

crypto isakmp key 1258 address 10.0.177.3

crypto ipsec transform-set Gost esp-des

ip access-list extended SN3toSN2
  permit ip 192.168.4.0 0.0.0.255 192.168.3.0 0.0.0.255

ip access-list extended SN3toSN1
  permit ip 192.168.4.0 0.0.0.255 192.168.2.0 0.0.0.255

ip access-list extended SN1toSN2
  permit ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255

ip access-list extended SN2toSN1
  permit ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255

crypto map CMAP 1 ipsec-isakmp
  match address SN3toSN2
  set transform-set Gost
  set peer 10.0.177.3

crypto map CMAP 2 ipsec-isakmp
```

```
match address SN3toSN1
set transform-set Gost
set peer 10.0.177.2

crypto map CMAP 3 ipsec-isakmp
match address SN1toSN2
set transform-set Gost
set peer 10.0.177.3

crypto map CMAP 4 ipsec-isakmp
match address SN2toSN1
set transform-set Gost
set peer 10.0.177.2

interface FastEthernet0/0
ip address 10.0.177.4 255.255.0.0
crypto map CMAP

ip route 192.168.2.0 255.255.255.0 10.0.177.2 1
ip route 192.168.3.0 255.255.255.0 10.0.177.3 1
```

Текст LSP для GW3

```
# This is automatically generated LSP
#
# Conversion Date/Time: Thu Nov 29 11:48:26 2007

GlobalParameters(
    Title = "This LSP was automatically
generated by CSP Converter at Thu Nov 29 11:48:26 2007"
    Version = "3.0"
    LDAPLogMessageLevel = DEBUG
    SystemLogMessageLevel = DEBUG
    PolicyLogMessageLevel = DEBUG
    CertificatesLogMessageLevel = DEBUG
)

SyslogSettings(
    Server = 127.0.0.1
    Facility = LOG_LOCAL7
)
```

```
RoutingTable (
    Routes *=
        Route (
            Destination = 192.168.2.0/24
            Gateway = 10.0.177.2
            Metric = 1
        ),
        Route (
            Destination = 192.168.3.0/24
            Gateway = 10.0.177.3
            Metric = 1
        )
    )
IKETransform IKETransform_1
(
    CipherAlg    *= "G2814789CPRO1-K256-CBC-65534"
    HashAlg      *= "GR341194CPRO1-65534"
    GroupID      *= MODP_1024
    LifetimeSeconds = 86400
)

ESPProposal ESP_Gost
(
    Transform* = ESPTransform
    (
        CipherAlg*          = "G2814789CPRO1-K256-CBC-254"
        LifetimeSeconds      = 3600
        LifetimeKilobytes    = 4608000
    )
)

ESPProposal ESP_Gost_1
(
    Transform* = ESPTransform
    (
        CipherAlg*          = "G2814789CPRO1-K256-CBC-254"
        LifetimeSeconds      = 3600
        LifetimeKilobytes    = 4608000
    )
)
```

```

)

ESPProposal ESP_Gost_2
(
    Transform* = ESPTransform
    (
        CipherAlg*          = "G2814789CPRO1-K256-CBC-254"
        LifetimeSeconds      = 3600
        LifetimeKilobytes    = 4608000
    )
)

ESPProposal ESP_Gost_3
(
    Transform* = ESPTransform
    (
        CipherAlg*          = "G2814789CPRO1-K256-CBC-254"
        LifetimeSeconds      = 3600
        LifetimeKilobytes    = 4608000
    )
)

AuthMethodPreshared IKE_auth_cs_key_10_0_177_3
(
    RemoteID = IdentityEntry(
        IPv4Address *= 10.0.177.3
    )
    SharedIKESecret = "cs_key_10_0_177_3"
)

IKERule IKE_CMAP_1
(
    Transform* = IKETransform_1
    AggrModeAuthMethod *= IKE_auth_cs_key_10_0_177_3
    MainModeAuthMethod *= IKE_auth_cs_key_10_0_177_3
    DoAutopass          = TRUE
    DoNotUseDPD          = TRUE
)

IPsecAction CMAP_1

```

```
(
    TunnelingParameters *= TunnelEntry(
        PeerIPAddress = 10.0.177.3

        DFHandling=COPY
    )
    ContainedProposals *= ( ESP_Gost )
    IKERule = IKE_CMAP_1
)

AuthMethodPreshared IKE_auth_cs_key_10_0_177_2
(
    RemoteID = IdentityEntry(
        IPv4Address *= 10.0.177.2
    )
    SharedIKESecret = "cs_key_10_0_177_2"
)

IKERule IKE_CMAP_2
(
    Transform* = IKETransform_1
    AggrModeAuthMethod *= IKE_auth_cs_key_10_0_177_2
    MainModeAuthMethod *= IKE_auth_cs_key_10_0_177_2
    DoAutopass          = TRUE
    DoNotUseDPD          = TRUE
)

IPsecAction CMAP_2
(
    TunnelingParameters *= TunnelEntry(
        PeerIPAddress = 10.0.177.2

        DFHandling=COPY
    )
    ContainedProposals *= ( ESP_Gost_1 )
    IKERule = IKE_CMAP_2
)

AuthMethodPreshared IKE_auth_cs_key_10_0_177_3_1
(
    RemoteID = IdentityEntry(
        IPv4Address *= 10.0.177.3
```

```

    )
    SharedIKESecret = "cs_key_10_0_177_3"
)

IKERule IKE_CMAP_3
(
    Transform* = IKETransform_1
    AggrModeAuthMethod *= IKE_auth_cs_key_10_0_177_3_1
    MainModeAuthMethod *= IKE_auth_cs_key_10_0_177_3_1
    DoAutopass          = TRUE
    DoNotUseDPD          = TRUE
)

IPsecAction CMAP_3
(
    TunnelingParameters *= TunnelEntry(
        PeerIPAddress = 10.0.177.3

        DFHandling=COPY
    )
    ContainedProposals *= ( ESP_Gost_2 )
    IKERule = IKE_CMAP_3
)

AuthMethodPreshared IKE_auth_cs_key_10_0_177_2_1
(
    RemoteID = IdentityEntry(
        IPv4Address *= 10.0.177.2
    )
    SharedIKESecret = "cs_key_10_0_177_2"
)

IKERule IKE_CMAP_4
(
    Transform* = IKETransform_1
    AggrModeAuthMethod *= IKE_auth_cs_key_10_0_177_2_1
    MainModeAuthMethod *= IKE_auth_cs_key_10_0_177_2_1
    DoAutopass          = TRUE
    DoNotUseDPD          = TRUE
)

IPsecAction CMAP_4

```

```
(
    TunnelingParameters *= TunnelEntry(
        PeerIPAddress = 10.0.177.2

        DFHandling=COPY
    )
    ContainedProposals *= ( ESP_Gost_3 )
    IKERule = IKE_CMAP_4
)

FilteringRule Filter_nil_acl_CMAP_1
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.4.0/24 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.3.0/24 )
    NetworkInterfaces *= "rtls0"
    Action *= ( CMAP_1 )
)

FilteringRule Filter_nil_acl_CMAP_2
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.4.0/24 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.2.0/24 )
    NetworkInterfaces *= "rtls0"
    Action *= ( CMAP_2 )
)

FilteringRule Filter_nil_acl_CMAP_3
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.2.0/24 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.3.0/24 )
    NetworkInterfaces *= "rtls0"
    Action *= ( CMAP_3 )
)

FilteringRule Filter_nil_acl_CMAP_4
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.3.0/24 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.2.0/24 )
    NetworkInterfaces *= "rtls0"
    Action *= ( CMAP_4 )
)
```

```
FilteringRule Filter_nil_acl
(
    LocalIPFilter *= FilterEntry( IPAddress *=
0.0.0.0..255.255.255.255 )
    PeerIPFilter  *= FilterEntry( IPAddress *=
0.0.0.0..255.255.255.255 )
    NetworkInterfaces *= "rtls0"
    Action *= ( PASS )
)
```