Построение VPN туннеля между двумя сегментами одной сети, защищаемыми шлюзами «С-Терра Шлюз 10G»

Описание стенда

Сценарий иллюстрирует построение защищенного соединения между двумя сегментами одной сети SN1, разрыв между которыми защищается шлюзами безопасности «С-Терра Шлюз 10G». Для защиты будет построен VPN туннель между устройствами GW1 и GW2. Устройства IPHost1 и IPHost2 смогут общаться между собой по защищенному каналу (VPN). Все остальные соединения разрешены, но защищаться не будут.

В рамках данного сценария для аутентификации партнеры будут использовать сертификаты. В качестве криптопровайдера будет использована криптографическая библиотека, разработанная компанией «С-Терра СиЭсПи». Шлюзы безопасности «С-Терра Шлюз 10G» версии 4.2.

Параметры защищенного соединения:

Параметры протокола IKE:

- Аутентификация при помощи цифровых сертификатов, алгоритм подписи – ГОСТ Р 34.10-2012;
- Алгоритм шифрования – ГОСТ 28147-89 (ключ 256 бит);
- Алгоритм вычисления хеш-функции – ГОСТ Р 34.11-2012 ТК26 (ключ 256 бит);
- Алгоритм выработки общего ключа (аналог алгоритма Диффи-Хеллмана) – VKO_GOSTR3410_2012_256 (ключ 256 бит).

Параметры протокола ESP:

- Комбинированный алгоритм шифрования и имитозащиты (контроль целостности) – ESP_GOST-4M-IMIT (ключ 256 бит).

Схема стенда (Рисунок 1):

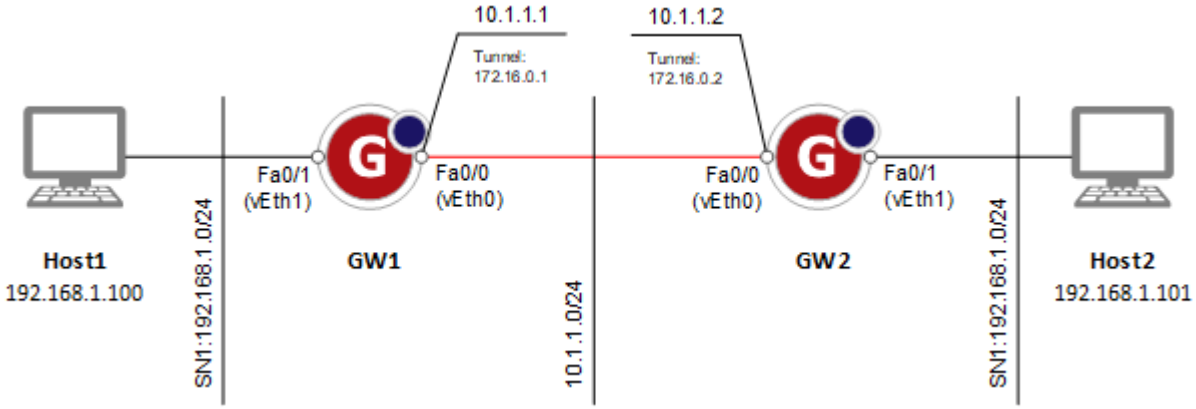

Рисунок 1

Логика работы

Рассмотрим логику работу на примере трафика, идущего от IPHost1 к IPHost2. Фреймы канального уровня, приходящие на внутренний интерфейс (`FastEthernet0/1`) шлюза GW1, захватываются и инкапсулируются в пакеты сетевого уровня (source IP-адрес – `172.16.0.1`, destination IP-адрес – `172.16.0.2`). Далее пакеты попадают под правила шифрования и передаются по IPsec туннелю между GW1 и GW2. На GW2 происходит обратный процесс.

Необходимо отметить, что между шлюзами безопасности GW1 и GW2 могут находиться устройства 3 уровня (маршрутизаторы, межсетевые экраны и др.), то есть они не обязаны быть связаны на канальном уровне.

Важно! В случае, если в реализации есть существенные отклонения от описанного сценария, требуется учесть следующие моменты:

- Успешное построение туннеля между шлюзами безопасности «С-Терра Шлюз 10G» версии 4.2 возможно только в топологии точка-точка;
- Связность между защищаемыми сегментами сети обеспечивается на уровне L2 (сегменты должны находиться в одной подсети);
- Существует несовместимость по протоколу обработки данных со шлюзами безопасности «С-Терра Шлюз».

Настройка стенда

Настройка шлюза безопасности GW1

Инициализация шлюза

Настройку начните со шлюза безопасности GW1.

После полной загрузки шлюза пользователь попадает в S-Terra administrative console.

```
S-Terra administrative console

login as:
```

1. Пройдите процедуру аутентификации (пользователь по умолчанию – `administrator`), пароль по умолчанию – `s-terra`).

```
login as: administrator
administrator's password:
```

```
############################################################
System is not initialized. Please run "initialize" command to start initialization
procedure.
############################################################

administrator@sterragate]
```

2. Смените пароль на S-Terra administrative console (команда `change user password`):

```
administrator@sterragate] change user password
Old user password:
New user password:
Re-type new password:
```

3. Пройдите процедуру инициализации (команда `initialize`). При этом запустится интерактивный ДСЧ.

```
administrator@sterragate] initialize
```

```
Initializing RNG: (press requested keys or Ctrl+C to interrupt)
[****************]
Successfully initialized RNG
```

3.1. Введите лицензию (`product code – GATEDP`):

```
You have to enter license for S-Terra Gate DP
Available product code:
 GATE
 GATEESR
 GATEDP
 MVPN
```

```
Enter product code: GATEDP
Enter customer code: CUSTOMER
Enter license number: 1234567890
Enter license code: 42000-123AB-123AB-123AB-123AB
```

```
...
```

```
Is this above data correct? yes
```

3.2. Далее следуют настройки, которые изменят конфигурационный файл `ipsm_dpdk.cfg`:

```
"This script will stop ipsmapp daemon and create new ipsm_dpdk.cfg. All ipsmapp settings
will be reset. Do you want to continue?" "Yes" yes
```

```
Restoring interfaces settings
```

3.3. Введите количество тредов. Максимальное количество тредов равно количеству процессорных ядер в системе минус шесть. В данном сценарии используется 38 тредов, как значение по умолчанию для артикула `10G-4.2-1757-8-4-RED`.

```
threads (1-38) [38] : 38
```

3.4. Введите PCI ID WAN интерфейса (Рисунок 2):

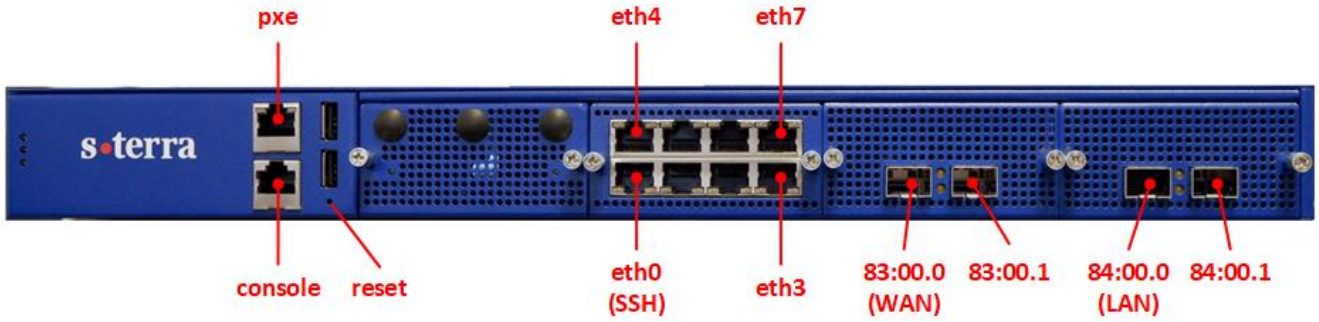

Рисунок 2

```
Port#   pci_id          Configured
-       83:00.0
-       83:00.1
-       84:00.0
-       84:00.1
```

```
Enter pci_id for WAN interface : 83:00.0
```

3.5. Введите исходящий IP-адрес (`l3_ip`). Данный адрес будет задан интерфейсу `FastEthernet0/0` (`FastEthernet0/0` – в cisco-like консоли или `vEth0` – в Linux).

```
Enter IP-address for WAN interface (l3_ip): 10.1.1.1
```

3.6. Введите маску подсети для данного IP-адреса (`l3_mask`), значение по умолчанию – `24`:

```
Enter netmask for WAN interface (l3_mask) (0-32) [24]: 24
```

3.7. Введите IP-адрес шлюза по умолчанию. Данный IP-адрес необходим для маршрутизации шифрованного трафика. Для маршрутизации трафика ОС используются маршруты из cisco-like конфигурации:

```
Enter default gateway IP-address (gw_ip): 10.1.1.2
```

3.8. Есть возможность указать MAC-адрес следующего хопа (`next_hop_mac`), значение по умолчанию – нет:

```
Do you want to enter and enable next_hop_mac? [No] No
```

3.9. Введите PCI ID LAN интерфейса, который будет использоваться в паре с настроенным ранее:

```
Port#   pci_id          Configured
PORT0   83:00.0         *
-       83:00.1
-       84:00.0
-       84:00.1
```

```
Enter pci_id to pair with 83:00.0 : 84:00.0
```

3.10. Введите исходящий IP-адрес для L2 туннеля (`l2_src_ip`):

```
Enter source IP-address for l2-tunnel (l2_src_ip) : 172.16.0.1
```

3.11. Введите IP-адрес назначения для L2 туннеля (`l2_dst_ip`):

```
Enter destination IP-address for l2-tunnel (l2_dst_ip): 172.16.0.2
```

3.12. Введите MTU для WAN интерфейса, значение по умолчанию – `9710`:

```
Enter MTU for WAN interface (68-9710) [9710] : 9710
```

3.13. Введите MTU для LAN интерфейса, значение по умолчанию – `9610`:

```
Enter MTU for LAN interface (68-9610) [9610] : 9610
```

```
SUCCESS:  Operation was successful:
```

```
Port#   pci_id          Configured
PORT0   83:00.0         *
-       83:00.1
PORT1   84:00.0         *
-       84:00.1
OK

Starting IPSM daemon……done
Starting VPN log daemon……done
Starting IPsec daemon……done

Initialization completed
Some settings will take effect after OS reboot only.

Network traffic is blocked.
To unblock network traffic, please setup the network security policy or use “run csconf_mgr activate” command to activate the predefined permissive network security policy now.
```

3.14. Инициализация окончена. Конфигурация сохранена в файл `/opt/VPNagent/etc/ipsm_dpdk.cfg`.

3.15. Для тестового использования политики драйвера по умолчанию безопасности необходимо выполнить команду `run csconf_mgr activate`.

Скрипт настройки `ipsm_dpdk.cfg` находится по следующему пути – `/opt/VPNagent/bin/configure_dp.sh`. Запустите данный скрипт при необходимости изменить конфигурацию, настроенную выше (начиная с п.3.2).

Более подробно консоль разграничения доступа S-Terra administrative console описана в документации.

Настройка SSH

На шлюзе 10G в качестве интерфейсов управления выступают 1G порты (обычно встроенные в материнскую плату сервера).

Данные порты не контролируются драйвером `vpngate`, настройки безопасности на них не распространяются, поэтому в cisco-like интерфейсе данные порты отсутствуют.

Важно! Данные порты разрешается подключать только в доверенные сети.

При необходимости настройки шлюза через SSH можно задать интерфейсу управления IP-адрес.

1. Просмотрите доступные для настройки интерфейсы:

```
administrator@sterragate] run ifconfig -a | grep eth
```

```
eth0      Link encap:Ethernet  HWaddr 00:90:0b:68:51:1d
eth1      Link encap:Ethernet  HWaddr 00:90:0b:68:51:1e
eth2      Link encap:Ethernet  HWaddr 00:90:0b:68:51:1f
eth3      Link encap:Ethernet  HWaddr 00:90:0b:68:51:20
eth4      Link encap:Ethernet  HWaddr 00:90:0b:68:51:21
eth5      Link encap:Ethernet  HWaddr 00:90:0b:68:51:22
eth6      Link encap:Ethernet  HWaddr 00:90:0b:68:51:23
eth7      Link encap:Ethernet  HWaddr 00:90:0b:68:51:24
```

2. Добавьте следующие настройки (после строк `###netifcfg-end###`) в файл `/etc/network/interfaces`:

```
administrator@sterragate] run vim.tiny /etc/network/interfaces
```

```
auto eth0
iface eth0 inet static
address 192.168.1.1
netmask 255.255.255.0
```

Где `eth0` – настраиваемый интерфейс.

2.1. После внесенных изменений файл будет выглядеть следующим образом:

```
administrator@sterragate] run cat /etc/network/interfaces

############################################################
# CAUTION: lines under special marker: ###netifcfg-*###
# contains autogenerated information. You can add/modify
# lines outside of those markers
############################################################

# loopback configuration
auto lo
iface lo inet loopback

###netifcfg-begin###
###netifcfg-end###
auto eth0
iface eth0 inet static
address 192.168.1.1
netmask 255.255.255.0
```

3. Установите пароль на пользователя `root` (команда `run passwd`).

```
administrator@sterragate] run passwd
Enter new UNIX password:
Retype new UNIX password:

passwd: password updated successfully
```

4. Включите настроенный интерфейс:

```
administrator@sterragate] run ifup eth0
```

5. Дальнейшую настройку можно выполнять, подключившись к шлюзу через SSH. При этом пользователь попадает в консоль Linux. Для перехода в консоль настройки шлюза (cisco-like интерфейс) выполните следующие команды:

```
root@sterragate:~# cs_console
sterragate>enable
Password:
```

По умолчанию пароль – `csp`.

Регистрация сертификатов

В данном сценарии для аутентификации используются сертификаты. Для корректной работы необходимо зарегистрировать доверенный сертификат УЦ и локальный сертификат, выданный данным УЦ.

1. Установите правильное системное время.

Например:

```
administrator@sterragate] run date -s "01/31/2017 15:00"

Tue Jan 31 15:00:00 MSK 2017
```

Данная запись соответствует 31 января 2017 года 15:00.

В данном случае формат даты указывается в виде месяц/день/год (ММ/ДД/ГГГГ).

Для автоматической настройки правильного времени рекомендуется настроить NTP-клиент по соответствующей инструкции.

2. Подключите к шлюзу USB-носитель. Он будет автоматически примонтирован в системе.

3. Узнайте под каким именем USB-носитель был примонтирован. В данном случае - 041F-4C1B.

```
administrator@sterragate] dir media
    1  drwx         8192  Thu Jan  1 03:00:00 1970  041F-4C1B
```

4. Сформируйте запрос на сертификат при помощи утилиты `cert_mgr`:

```
administrator@sterragate]    run    cert_mgr    create    -subj    "C=RU,O=S-Terra
CSP,OU=Research,CN=GW1" -GOST_R341012_256 -fb64 media:041F-4C1B/gw1.req
```

- Ключ `-subj <DN>` задает поля сертификата.

- Ключ `-GOST_R341012_256` предполагает использование ГОСТ 2012. На УЦ для его поддержки должно быть установлено СКЗИ «КриптоПро CSP» версии 4.0 или новее. При необходимости, можно воспользоваться более старым ключом `-GOST_R3410EL`.
- Ключ `-fb64 <путь до файла>` позволяет сохранить запрос в файл по указанному пути.

5. Передайте полученный запрос сертификата на УЦ. Процедура выдачи сертификата на УЦ по запросу описана в документации.
6. Перенесите полученный локальный сертификат и сертификат УЦ на шлюз безопасности. В данном сценарии сертификаты будут на USB-носителе.
7. С помощью утилиты `cert_mgr` зарегистрируйте сертификат УЦ в базе продукта:

```
administrator@sterragate] run cert_mgr import -f media:041F-4C1B/ca.cer -t
```

```
1 OK C=RU,L=Moscow,O=S-Terra CSP,OU=Research,CN=Research Root CA
```

Ключ `-t` в данной команде указывает на то, что импортируемый сертификат – корневой (сертификат УЦ).

8. Зарегистрируйте локальный сертификат в базе продукта:

```
administrator@sterragate] run cert_mgr import -f media:041F-4C1B/gw1.cer
```

```
1 OK C=RU,O=S-Terra CSP,OU=Research,CN=GW1
```

9. Убедитесь, что сертификаты импортированы успешно:

```
administrator@sterragate] run cert_mgr show
```

```
Found 2 certificates. No CRLs found.
1 Status: trusted C=RU,L=Moscow,O=S-Terra CSP,OU=Research,CN=Research Root CA
2 Status: local   C=RU,O=S-Terra CSP,OU=Research,CN=GW1
```

Создание политики безопасности

После регистрации сертификатов необходимо создать политику безопасности для шлюза GW1

1. Перейдите из консоли разграничения доступа (S-Terra Administrative console) в консоль настройки шлюза (cisco-like интерфейс) (команда `configure`). По умолчанию имя пользователя – `cscons`, пароль – `csp`.

```
administrator@sterragate] configure
sterragate login: cscons
Password:
```

```
...
sterragate#
```

Важно! Пароль по умолчанию необходимо сменить.

2. Перейдите в режим настройки:

```
sterragate#configure terminal
```

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

3. Смените пароль по умолчанию:

```
sterragate(config)#username cscons password <пароль>
```

4. Смените название шлюза:

```
sterragate(config)#hostname GW1
```

5. Задайте тип идентификации:

```
GW1(config)#crypto isakmp identity dn
```

В данном сценарии для идентификации будет использоваться поле DN сертификата.

6. Задайте параметры DPD (dead peer detection)

```
GW1(config)#crypto isakmp keepalive 10 2
GW1(config)#crypto isakmp keepalive retry-count 5
```

Если в течение 10 секунд отсутствует входящий трафик в IPsec туннеле, то с интервалом в 2 секунды посылается 5 keepalive-пакетов в IKE туннеле, чтобы удостовериться в работоспособности туннеля. Если партнер не отвечает на keepalive-пакеты, то существующий IKE туннель переходит в состояние disabled, а связанные с ним IPsec туннели удаляются. В случае наличия исходящего трафика происходит попытка создать новый IKE туннель.

7. Задайте параметры для IKE:

```
GW1(config)#crypto isakmp policy 1
GW1(config-isakmp)#authentication gost-sig
GW1(config-isakmp)#encr gost
GW1(config-isakmp)#hash gost341112-256-tc26
GW1(config-isakmp)#group vko2
GW1(config-isakmp)#exit
```

8. Задайте параметры для IPsec:

```
GW1(config)#crypto ipsec transform-set TSET esp-gost28147-4m-imit
GW1(cfg-crypto-trans)#mode tunnel
GW1(cfg-crypto-trans)#exit
```

9. Опишите трафик, который планируется защищать. Для этого создайте расширенный список доступа:

```
GW1(config)#ip access-list extended LIST
GW1(config-ext-nacl)#permit ip host 172.16.0.1 host 172.16.0.2
GW1(config-ext-nacl)#exit
```

10. Создайте крипто-карту:

```
GW1(config)#crypto map CMAP 1 ipsec-isakmp
GW1(config-crypto-map)#match address LIST
GW1(config-crypto-map)#set transform-set TSET
GW1(config-crypto-map)#set peer 10.1.1.2
GW1(config-crypto-map)#set security-association lifetime kilobytes 4294967295
GW1(config-crypto-map)#exit
```

11. Настройка IP-адреса для исходящего интерфейса (vEth0) была произведена в процессе инициализации.

12. Задайте адрес шлюза по умолчанию:

```
GW1(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.2
```

13. Привяжите крипто-карту ко всем интерфейсам DP:

```
GW1(config)#interface DP0
GW1(config-if)#crypto map CMAP
GW1(config-if)#exit
GW1(config)#interface DP1
GW1(config-if)#crypto map CMAP
GW1(config-if)#exit
…
GW1(config)#interface DP37
GW1(config-if)#crypto map CMAP
GW1(config-if)#exit
```

14. Настройте получение списка отозванных сертификатов (CRL) по HTTP:

```
GW1(config)#crypto pki trustpoint s-terra_technological_trustpoint
GW1(ca-trustpoint)#crl download group GROUP http://10.0.221.179/certsrv/certcrl.crl
GW1(ca-trustpoint)#exit
```

Предполагается, что CRL выкладывается на общедоступное место (доступ к которому обеспечен без использования IPsec) для всех шлюзов. При указании имени домена, вместо IP-адреса, необходимо настроить адрес DNS-сервера в системном файле `/etc/resolv.conf`.

Также необходимо учитывать, что у CRL есть срок действия и нужно обеспечивать своевременное их обновление в данном общедоступном месте.

По умолчанию CRL будет запрашиваться раз в сутки (раз в 1440 минут), для изменения интервала запросов можно воспользоваться командой `crl download time <интервал в минутах>`.

При необходимости отключения CRL (не рекомендуется отключать CRL) воспользуйтесь командой `revocation-check none`.

15. Настройка устройства GW1 в cisco-like консоли завершена. При выходе из конфигурационного режима происходит загрузка конфигурации:

```
GW1(config)#end
GW1#exit
```

В приложении представлен текст cisco-like конфигурации, текст LSP конфигурации и текст файла ipsm_dpdk.cfg для шлюза GW1.

Настройка шлюза безопасности GW2

Настройка шлюза безопасности GW2 происходит аналогично настройке шлюза GW1, с заменой IP-адресов в соответствующих разделах конфигурации.

В приложении представлен текст cisco-like конфигурации, текст LSP конфигурации и текст файла ipsm_dpdk.cfg для шлюза GW2.

Настройка устройства Host1

На устройстве Host1 задайте IP-адрес.

Настройка устройства Host2

На устройстве Host2 задайте IP-адрес.

Проверка работоспособности стенда

После того, как настройка всех устройств завершена, инициируйте создание защищенного соединения.

На устройстве Host1 выполните команду ping:

```
root@Host1:~# ping -c 5 192.168.1.101
```

```
PING 192.168.1.101 (192.168.1.101) 56(84) bytes of data.
64 bytes from 192.168.1.101: icmp_req=1 ttl=64 time=0.831 ms
64 bytes from 192.168.1.101: icmp_req=2 ttl=64 time=0.358 ms
64 bytes from 192.168.1.101: icmp_req=3 ttl=64 time=0.270 ms
64 bytes from 192.168.1.101: icmp_req=4 ttl=64 time=0.304 ms
64 bytes from 192.168.1.101: icmp_req=5 ttl=64 time=0.359 ms

--- 192.168.1.101 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.270/0.424/0.831/0.206 ms
```

В результате выполнения этой команды между устройствами GW1 и GW2 будет установлен VPN туннель.

Убедиться в этом можно, выполнив на устройстве GW1 команду:

```
root@GW1:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 1 (10.1.1.1,500)-(10.1.1.2,500) active 2420 2296

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 1 (172.16.0.1,*)-(172.16.0.2,*) * ESP tunn 1856 1592
2 2 (172.16.0.1,*)-(172.16.0.2,*) * ESP tunn 560 472
…
38 38 (172.16.0.1,*)-(172.16.0.2,*) * ESP tunn 560 472
```

Согласно созданной политике безопасности весь трафик между сетями SN1 и SN2 будет зашифрован. Прохождение остального трафика будет разрешено, но не будет защищаться шифрованием.

Приложение

Текст cisco-like конфигурации для шлюза GW1

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp keepalive 10
crypto isakmp keepalive retry-count 5
username cscons privilege 15 password 0 csp
aaa new-model
!
!
hostname GW1
enable password csp
!
!
!
!
!
crypto isakmp policy 1
 encr gost
 hash gost341112-256-tc26
 authentication gost-sig
 group vko2
!
crypto ipsec transform-set TSET esp-gost28147-4m-imit
!
ip access-list extended LIST
 permit ip host 172.16.0.1 host 172.16.0.2
!
!
crypto map CMAP 1 ipsec-isakmp
 match address LIST
 set transform-set TSET
 set security-association lifetime kilobytes 4294967295
 set peer 10.1.1.2
!
interface DP0
! Warning: no physical interface found (pattern "10G_000")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1000
 shutdown
!
interface DP1
! Warning: no physical interface found (pattern "10G_001")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1001
 shutdown
!
interface DP2
! Warning: no physical interface found (pattern "10G_002")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1002
 shutdown
!
interface DP3
! Warning: no physical interface found (pattern "10G_003")
 no ip address
```

```
 crypto map CMAP
 crypto ipsec stream-id 1003
 shutdown
!
interface DP4
! Warning: no physical interface found (pattern "10G_004")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1004
 shutdown
!
interface DP5
! Warning: no physical interface found (pattern "10G_005")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1005
 shutdown
!
interface DP6
! Warning: no physical interface found (pattern "10G_006")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1006
 shutdown
!
interface DP7
! Warning: no physical interface found (pattern "10G_007")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1007
 shutdown
!
interface DP8
! Warning: no physical interface found (pattern "10G_008")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1008
 shutdown
!
interface DP9
! Warning: no physical interface found (pattern "10G_009")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1009
 shutdown
!
interface DP10
! Warning: no physical interface found (pattern "10G_010")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1010
 shutdown
!
interface DP11
! Warning: no physical interface found (pattern "10G_011")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1011
 shutdown
!
interface DP12
! Warning: no physical interface found (pattern "10G_012")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1012
 shutdown
```

```
!
interface DP13
! Warning: no physical interface found (pattern "10G_013")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1013
 shutdown
!
interface DP14
! Warning: no physical interface found (pattern "10G_014")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1014
 shutdown
!
interface DP15
! Warning: no physical interface found (pattern "10G_015")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1015
 shutdown
!
interface DP16
! Warning: no physical interface found (pattern "10G_016")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1016
 shutdown
!
interface DP17
! Warning: no physical interface found (pattern "10G_017")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1017
 shutdown
!
interface DP18
! Warning: no physical interface found (pattern "10G_018")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1018
 shutdown
!
interface DP19
! Warning: no physical interface found (pattern "10G_019")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1019
 shutdown
!
interface DP20
! Warning: no physical interface found (pattern "10G_020")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1020
 shutdown
!
interface DP21
! Warning: no physical interface found (pattern "10G_021")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1021
 shutdown
!
interface DP22
! Warning: no physical interface found (pattern "10G_022")
```

```
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1022
 shutdown
!
interface DP23
! Warning: no physical interface found (pattern "10G_023")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1023
 shutdown
!
interface DP24
! Warning: no physical interface found (pattern "10G_024")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1024
 shutdown
!
interface DP25
! Warning: no physical interface found (pattern "10G_025")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1025
 shutdown
!
interface DP26
! Warning: no physical interface found (pattern "10G_026")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1026
 shutdown
!
interface DP27
! Warning: no physical interface found (pattern "10G_027")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1027
 shutdown
!
interface DP28
! Warning: no physical interface found (pattern "10G_028")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1028
 shutdown
!
interface DP29
! Warning: no physical interface found (pattern "10G_029")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1029
 shutdown
!
interface DP30
! Warning: no physical interface found (pattern "10G_030")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1030
 shutdown
!
interface DP31
! Warning: no physical interface found (pattern "10G_031")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1031
```

```
 shutdown
!
interface DP32
! Warning: no physical interface found (pattern "10G_032")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1032
 shutdown
!
interface DP33
! Warning: no physical interface found (pattern "10G_033")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1033
 shutdown
!
interface DP34
! Warning: no physical interface found (pattern "10G_034")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1034
 shutdown
!
interface DP35
! Warning: no physical interface found (pattern "10G_035")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1035
 shutdown
!
interface DP36
! Warning: no physical interface found (pattern "10G_036")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1036
 shutdown
!
interface DP37
! Warning: no physical interface found (pattern "10G_037")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1037
 shutdown
!
interface FastEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 mtu 9710
!
interface FastEthernet0/1
 no ip address
 shutdown
 mtu 9610
!
!
ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
 crl download group GROUP http://10.0.221.179/certsrv/certcrl.crl
crypto pki certificate chain s-terra_technological_trustpoint
certificate 1F76A0063C0401B94DA17E11D2B4AC8A
3082023B308201A7A00302010202101F76A0063C0401B94DA17E11D2B4AC8A30
0A06082A850307010103033030310B300906035504061302525531103 00E0603
55040A1307532D5465727261310F300D06035504031306526F6F744341301E17
0D313930313238303834323235A170D323430313238303835323138 5A303031
0B300906035504061302525531103 00E060355040A1307532D5465727261310F
```

```
300D06035504031306526F6F7443413081AA302106082A850307010101023015
06092A85030701020102010608 2A850307010102030381840004818079 89CA30
6C7FAC17952BFC327F48ADC1853D077497940F63BBCE26B668A2A44A494362D5
29058F5B2C78703A51650F82545F96A6ABAA0FA513C10B3E49B06C54F46D1745
7F357829721E4BB09003AFF511020E31B276E12C0335877BD758AFD00AFE0540
DBDA22BC79A41912FA92D2EEF12DAED35C453AD15B7B58B82BA2064EA351304F
300B0603551D0F040403020186300F0603551D130101FF040530030101FF301D
0603551D0E041604149174BF9BB185172A7DFB3A73689CD749EEF0C941301006
092B0601040182371501040302010030 0A06082A850307010103030381810076
640885EFA693A8B42EDAB6D74685F1EC9F061B4AC24074AAD3FD5B9A38AF22DB
34E4B4F552A4053F9CEC637E483BBA713BDBC49D59E80E0152D29C8613D0E967
7D6BE3AAEE568B51498BB4143B0873AEDFD1A71BF97C3067C538E3821D97D0C8
6278713A76B6046B582F722FDB3854A1F603212EC0FA537A1D2E36C453EFC6

quit
!
end
```

Текст cisco-like конфигурации для шлюза GW2

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp keepalive 10
username cscons privilege 15 password 0 csp
aaa new-model
!
!
hostname GW2
enable password csp
!
!
!
!
!
crypto isakmp policy 1
 encr gost
 hash gost341112-256-tc26
 authentication gost-sig
 group vko2
!
crypto ipsec transform-set TSET esp-gost28147-4m-imit
!
ip access-list extended LIST
 permit ip host 172.16.0.2 host 172.16.0.1
!
!
crypto map CMAP 1 ipsec-isakmp
 match address LIST
 set transform-set TSET
 set security-association lifetime kilobytes 4294967295
 set peer 10.1.1.1
!
interface DP0
! Warning: no physical interface found (pattern "10G_000")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1000
 shutdown
!
interface DP1
! Warning: no physical interface found (pattern "10G_001")
 no ip address
```

```
 crypto map CMAP
 crypto ipsec stream-id 1001
 shutdown
!
interface DP2
! Warning: no physical interface found (pattern "10G_002")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1002
 shutdown
!
interface DP3
! Warning: no physical interface found (pattern "10G_003")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1003
 shutdown
!
interface DP4
! Warning: no physical interface found (pattern "10G_004")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1004
 shutdown
!
interface DP5
! Warning: no physical interface found (pattern "10G_005")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1005
 shutdown
!
interface DP6
! Warning: no physical interface found (pattern "10G_006")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1006
 shutdown
!
interface DP7
! Warning: no physical interface found (pattern "10G_007")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1007
 shutdown
!
interface DP8
! Warning: no physical interface found (pattern "10G_008")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1008
 shutdown
!
interface DP9
! Warning: no physical interface found (pattern "10G_009")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1009
 shutdown
!
interface DP10
! Warning: no physical interface found (pattern "10G_010")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1010
 shutdown
```

```
!
interface DP11
! Warning: no physical interface found (pattern "10G_011")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1011
 shutdown
!
interface DP12
! Warning: no physical interface found (pattern "10G_012")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1012
 shutdown
!
interface DP13
! Warning: no physical interface found (pattern "10G_013")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1013
 shutdown
!
interface DP14
! Warning: no physical interface found (pattern "10G_014")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1014
 shutdown
!
interface DP15
! Warning: no physical interface found (pattern "10G_015")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1015
 shutdown
!
interface DP16
! Warning: no physical interface found (pattern "10G_016")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1016
 shutdown
!
interface DP17
! Warning: no physical interface found (pattern "10G_017")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1017
 shutdown
!
interface DP18
! Warning: no physical interface found (pattern "10G_018")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1018
 shutdown
!
interface DP19
! Warning: no physical interface found (pattern "10G_019")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1019
 shutdown
!
interface DP20
! Warning: no physical interface found (pattern "10G_020")
```

```
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1020
 shutdown
!
interface DP21
! Warning: no physical interface found (pattern "10G_021")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1021
 shutdown
!
interface DP22
! Warning: no physical interface found (pattern "10G_022")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1022
 shutdown
!
interface DP23
! Warning: no physical interface found (pattern "10G_023")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1023
 shutdown
!
interface DP24
! Warning: no physical interface found (pattern "10G_024")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1024
 shutdown
!
interface DP25
! Warning: no physical interface found (pattern "10G_025")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1025
 shutdown
!
interface DP26
! Warning: no physical interface found (pattern "10G_026")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1026
 shutdown
!
interface DP27
! Warning: no physical interface found (pattern "10G_027")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1027
 shutdown
!
interface DP28
! Warning: no physical interface found (pattern "10G_028")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1028
 shutdown
!
interface DP29
! Warning: no physical interface found (pattern "10G_029")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1029
```

```
 shutdown
!
interface DP30
! Warning: no physical interface found (pattern "10G_030")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1030
 shutdown
!
interface DP31
! Warning: no physical interface found (pattern "10G_031")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1031
 shutdown
!
interface DP32
! Warning: no physical interface found (pattern "10G_032")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1032
 shutdown
!
interface DP33
! Warning: no physical interface found (pattern "10G_033")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1033
 shutdown
!
interface DP34
! Warning: no physical interface found (pattern "10G_034")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1034
 shutdown
!
interface DP35
! Warning: no physical interface found (pattern "10G_035")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1035
 shutdown
!
interface DP36
! Warning: no physical interface found (pattern "10G_036")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1036
 shutdown
!
interface DP37
! Warning: no physical interface found (pattern "10G_037")
 no ip address
 crypto map CMAP
 crypto ipsec stream-id 1037
 shutdown
!
interface FastEthernet0/0
 ip address 10.1.1.2 255.255.255.0
 mtu 9710
!
interface FastEthernet0/1
 no ip address
 shutdown
 mtu 9610
```

```
!
!
ip route 0.0.0.0 0.0.0.0 10.1.1.1
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
 crl download group GROUP http://10.0.221.179/certsrv/certcrl.crl
crypto pki certificate chain s-terra_technological_trustpoint
certificate 1F76A0063C0401B94DA17E11D2B4AC8A
3082023B308201A7A00302010202101F76A0063C0401B94DA17E11D2B4AC8A30
0A06082A850307010103033030310B300906035504061302525531103 00E0603
55040A1307532D5465727261310F300D06035504031306526F6F744341301E17
0D3139303132383038343232335A170D3234303132383038353231385A303031
0B300906035504061302525531103 00E060355040A1307532D5465727261310F
300D06035504031306526F6F7443413081AA302106082A850307010101023015
06092A850307010201020106082A85030701010203038184000481807989CA30
6C7FAC17952BFC327F48ADC1853D077497940F63BBCE26B668A2A44A494362D5
29058F5B2C78703A51650F82545F96A6ABAA0FA513C10B3E49B06C54F46D1745
7F357829721E4BB09003AFF511020E31B276E12C0335877BD758AFD00AFE0540
DBDA22BC79A41912FA92D2EEF12DAED35C453AD15B7B58B82BA2064EA351304F
300B0603551D0F040403020186300F0603551D130101FF040530030101FF301D
0603551D0E041604149174BF9BB185172A7DFB3A73689CD749EEF0C941301006
092B06010401823715010403020100300A06082A850307010103030381810076
640885EFA693A8B42EDAB6D74685F1EC9F061B4AC24074AAD3FD5B9A38AF22DB
34E4B4F552A4053F9CEC637E483BBA713BDBC49D59E80E0152D29C8613D0E967
7D6BE3AAEE568B51498BB4143B0873AEDFD1A71BF97C3067C538E3821D97D0C8
6278713A76B6046B582F722FDB3854A1F603212EC0FA537A1D2E36C453EFC6

quit
!
end
```

Текст LSP конфигурации для шлюза GW1

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Tue Feb 12 10:13:03 2019

GlobalParameters(
    Title                       = "This LSP was automatically generated by CSP Converter
at Tue Feb 12 10:13:03 2019"
    Version                       = LSP_4_2
    CRLHandlingMode               = ENABLE
    PreserveIPsecSA               = FALSE
)

IKEParameters(
    FragmentSize = 0
)

RoutingTable(
    Routes =
        Route(
            Destination = 0.0.0.0/0
            Gateway = 10.1.1.2
        )
)

FirewallParameters(
    TCPSynSentTimeout = 30
    TCPFinTimeout = 5
    TCPClosedTimeout = 30
    TCPSynRcvdTimeout = 30
    TCPEstablishedTimeout = 3600
    TCPHalfOpenLow = 400
    TCPHalfOpenMax = 500
```

```
    TCPSessionRateLow = 400
    TCPSessionRateMax = 500
)

IKETransform crypto:isakmp:policy:1
(
    CipherAlg   = "G2814789CPRO1-K256-CBC-65534"
    HashAlg     = "GR341112_256TC26-65128"
    GroupID     = VKO2_1B
    RestrictAuthenticationTo = GOST_SIGN
    LifetimeSeconds = 86400
)

ESPProposal TSET:ESP
(
    Transform* = ESPTransform
    (
        CipherAlg*          = "G2814789CPRO2-K288-CNTMAC-253"
        LifetimeSeconds     = 3600
        LifetimeKilobytes   = 4294967295
    )
)

AuthMethodGOSTSign GOST:Sign
(
    LocalID        =  IdentityEntry( DistinguishedName* = USER_SPECIFIC_DATA )
    SendRequestMode    =  ALWAYS
    SendCertMode       =  ALWAYS
)

IKERule IKERule:CMAP:1
(
    IKEPeerIPFilter = 10.1.1.2
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign
    MainModeAuthMethod  = GOST:Sign
    DPDIdleDuration     = 10
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 10
)

IPsecAction IPsecAction:CMAP:1
(
    TunnelingParameters = TunnelEntry(
        PeerAddress = 10.1.1.2
        DFHandling=COPY
        Assemble=TRUE
    )
    ContainedProposals = ( TSET:ESP )
    IKERule = IKERule:CMAP:1
)

FilterChain IPsecPolicy:CMAP:1000 (
    StreamID = 1000
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
```

```
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1001 (
    StreamID = 1001
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1002 (
    StreamID = 1002
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1003 (
    StreamID = 1003
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1004 (
    StreamID = 1004
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
```

```
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1005 (
    StreamID = 1005
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1006 (
    StreamID = 1006
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1007 (
    StreamID = 1007
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1008 (
    StreamID = 1008
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
```

```
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1009 (
    StreamID = 1009
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1010 (
    StreamID = 1010
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1011 (
    StreamID = 1011
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1012 (
    StreamID = 1012
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
```

```
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1013 (
    StreamID = 1013
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1014 (
    StreamID = 1014
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1015 (
    StreamID = 1015
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1016 (
    StreamID = 1016
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
```

```
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1017 (
    StreamID = 1017
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1018 (
    StreamID = 1018
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1019 (
    StreamID = 1019
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1020 (
    StreamID = 1020
    Filters = Filter (
```

```
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1021 (
    StreamID = 1021
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1022 (
    StreamID = 1022
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1023 (
    StreamID = 1023
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1024 (
```

```
    StreamID = 1024
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1025 (
    StreamID = 1025
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1026 (
    StreamID = 1026
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1027 (
    StreamID = 1027
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)
```

```
FilterChain IPsecPolicy:CMAP:1028 (
    StreamID = 1028
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1029 (
    StreamID = 1029
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1030 (
    StreamID = 1030
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1031 (
    StreamID = 1031
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
```

```
    )
)

FilterChain IPsecPolicy:CMAP:1032 (
    StreamID = 1032
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1033 (
    StreamID = 1033
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1034 (
    StreamID = 1034
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1035 (
    StreamID = 1035
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
```

```
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1036 (
    StreamID = 1036
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1037 (
    StreamID = 1037
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.1
        DestinationIP = 172.16.0.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

NetworkInterface (
    LogicalName = "DP0"
    IPsecPolicy = IPsecPolicy:CMAP:1000
)

NetworkInterface (
    LogicalName = "DP1"
    IPsecPolicy = IPsecPolicy:CMAP:1001
)

NetworkInterface (
    LogicalName = "DP2"
    IPsecPolicy = IPsecPolicy:CMAP:1002
)

NetworkInterface (
    LogicalName = "DP3"
    IPsecPolicy = IPsecPolicy:CMAP:1003
)

NetworkInterface (
    LogicalName = "DP4"
    IPsecPolicy = IPsecPolicy:CMAP:1004
)

NetworkInterface (
    LogicalName = "DP5"
```

```
    IPsecPolicy = IPsecPolicy:CMAP:1005
)

NetworkInterface (
    LogicalName = "DP6"
    IPsecPolicy = IPsecPolicy:CMAP:1006
)

NetworkInterface (
    LogicalName = "DP7"
    IPsecPolicy = IPsecPolicy:CMAP:1007
)

NetworkInterface (
    LogicalName = "DP8"
    IPsecPolicy = IPsecPolicy:CMAP:1008
)

NetworkInterface (
    LogicalName = "DP9"
    IPsecPolicy = IPsecPolicy:CMAP:1009
)

NetworkInterface (
    LogicalName = "DP10"
    IPsecPolicy = IPsecPolicy:CMAP:1010
)

NetworkInterface (
    LogicalName = "DP11"
    IPsecPolicy = IPsecPolicy:CMAP:1011
)

NetworkInterface (
    LogicalName = "DP12"
    IPsecPolicy = IPsecPolicy:CMAP:1012
)

NetworkInterface (
    LogicalName = "DP13"
    IPsecPolicy = IPsecPolicy:CMAP:1013
)

NetworkInterface (
    LogicalName = "DP14"
    IPsecPolicy = IPsecPolicy:CMAP:1014
)

NetworkInterface (
    LogicalName = "DP15"
    IPsecPolicy = IPsecPolicy:CMAP:1015
)

NetworkInterface (
    LogicalName = "DP16"
    IPsecPolicy = IPsecPolicy:CMAP:1016
)

NetworkInterface (
    LogicalName = "DP17"
    IPsecPolicy = IPsecPolicy:CMAP:1017
)

NetworkInterface (
    LogicalName = "DP18"
    IPsecPolicy = IPsecPolicy:CMAP:1018
```

```
)

NetworkInterface (
    LogicalName = "DP19"
    IPsecPolicy = IPsecPolicy:CMAP:1019
)

NetworkInterface (
    LogicalName = "DP20"
    IPsecPolicy = IPsecPolicy:CMAP:1020
)

NetworkInterface (
    LogicalName = "DP21"
    IPsecPolicy = IPsecPolicy:CMAP:1021
)

NetworkInterface (
    LogicalName = "DP22"
    IPsecPolicy = IPsecPolicy:CMAP:1022
)

NetworkInterface (
    LogicalName = "DP23"
    IPsecPolicy = IPsecPolicy:CMAP:1023
)

NetworkInterface (
    LogicalName = "DP24"
    IPsecPolicy = IPsecPolicy:CMAP:1024
)

NetworkInterface (
    LogicalName = "DP25"
    IPsecPolicy = IPsecPolicy:CMAP:1025
)

NetworkInterface (
    LogicalName = "DP26"
    IPsecPolicy = IPsecPolicy:CMAP:1026
)

NetworkInterface (
    LogicalName = "DP27"
    IPsecPolicy = IPsecPolicy:CMAP:1027
)

NetworkInterface (
    LogicalName = "DP28"
    IPsecPolicy = IPsecPolicy:CMAP:1028
)

NetworkInterface (
    LogicalName = "DP29"
    IPsecPolicy = IPsecPolicy:CMAP:1029
)

NetworkInterface (
    LogicalName = "DP30"
    IPsecPolicy = IPsecPolicy:CMAP:1030
)

NetworkInterface (
    LogicalName = "DP31"
    IPsecPolicy = IPsecPolicy:CMAP:1031
)
```

```
NetworkInterface (
    LogicalName = "DP32"
    IPsecPolicy = IPsecPolicy:CMAP:1032
)

NetworkInterface (
    LogicalName = "DP33"
    IPsecPolicy = IPsecPolicy:CMAP:1033
)

NetworkInterface (
    LogicalName = "DP34"
    IPsecPolicy = IPsecPolicy:CMAP:1034
)

NetworkInterface (
    LogicalName = "DP35"
    IPsecPolicy = IPsecPolicy:CMAP:1035
)

NetworkInterface (
    LogicalName = "DP36"
    IPsecPolicy = IPsecPolicy:CMAP:1036
)

NetworkInterface (
    LogicalName = "DP37"
    IPsecPolicy = IPsecPolicy:CMAP:1037
)
```

Текст LSP конфигурации для шлюза GW2

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Mon Feb 11 17:53:25 2019

GlobalParameters(
    Title                       = "This LSP was automatically generated by CSP Converter
at Mon Feb 11 17:53:25 2019"
    Version                       = LSP_4_2
    CRLHandlingMode               = ENABLE
    PreserveIPsecSA               = FALSE
)

IKEParameters(
    FragmentSize = 0
)

RoutingTable(
    Routes =
        Route(
            Destination = 0.0.0.0/0
            Gateway = 10.1.1.1
        )
)

FirewallParameters(
    TCPSynSentTimeout = 30
    TCPFinTimeout = 5
    TCPClosedTimeout = 30
    TCPSynRcvdTimeout = 30
    TCPEstablishedTimeout = 3600
    TCPHalfOpenLow = 400
    TCPHalfOpenMax = 500
```

```
    TCPSessionRateLow = 400
    TCPSessionRateMax = 500
)

IKETransform crypto:isakmp:policy:1
(
    CipherAlg   = "G2814789CPRO1-K256-CBC-65534"
    HashAlg     = "GR341112_256TC26-65128"
    GroupID     = VKO2_1B
    RestrictAuthenticationTo = GOST_SIGN
    LifetimeSeconds = 86400
)

ESPProposal TSET:ESP
(
    Transform* = ESPTransform
    (
        CipherAlg*          = "G2814789CPRO2-K288-CNTMAC-253"
        LifetimeSeconds     = 3600
        LifetimeKilobytes   = 4294967295
    )
)

AuthMethodGOSTSign GOST:Sign
(
    LocalID        =  IdentityEntry( DistinguishedName* = USER_SPECIFIC_DATA )
    SendRequestMode    =  ALWAYS
    SendCertMode       =  ALWAYS
)

IKERule IKERule:CMAP:1
(
    IKEPeerIPFilter = 10.1.1.1
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign
    MainModeAuthMethod  = GOST:Sign
    DPDIdleDuration     = 10
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 10
)

IPsecAction IPsecAction:CMAP:1
(
    TunnelingParameters = TunnelEntry(
        PeerAddress = 10.1.1.1
        DFHandling=COPY
        Assemble=TRUE
    )
    ContainedProposals = ( TSET:ESP )
    IKERule = IKERule:CMAP:1
)

FilterChain IPsecPolicy:CMAP:1000 (
    StreamID = 1000
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
```

```
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1001 (
    StreamID = 1001
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1002 (
    StreamID = 1002
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1003 (
    StreamID = 1003
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1004 (
    StreamID = 1004
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
```

```
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1005 (
    StreamID = 1005
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1006 (
    StreamID = 1006
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1007 (
    StreamID = 1007
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1008 (
    StreamID = 1008
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
```

```
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1009 (
    StreamID = 1009
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1010 (
    StreamID = 1010
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1011 (
    StreamID = 1011
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1012 (
    StreamID = 1012
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
```

```
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1013 (
    StreamID = 1013
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1014 (
    StreamID = 1014
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1015 (
    StreamID = 1015
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1016 (
    StreamID = 1016
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
```

```
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1017 (
    StreamID = 1017
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1018 (
    StreamID = 1018
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1019 (
    StreamID = 1019
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1020 (
    StreamID = 1020
    Filters = Filter (
```

```
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1021 (
    StreamID = 1021
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1022 (
    StreamID = 1022
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1023 (
    StreamID = 1023
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1024 (
```

```
    StreamID = 1024
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1025 (
    StreamID = 1025
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1026 (
    StreamID = 1026
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1027 (
    StreamID = 1027
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)
```

```
FilterChain IPsecPolicy:CMAP:1028 (
    StreamID = 1028
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1029 (
    StreamID = 1029
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1030 (
    StreamID = 1030
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1031 (
    StreamID = 1031
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
```

```
    )
)

FilterChain IPsecPolicy:CMAP:1032 (
    StreamID = 1032
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1033 (
    StreamID = 1033
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1034 (
    StreamID = 1034
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1035 (
    StreamID = 1035
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
```

```
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1036 (
    StreamID = 1036
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

FilterChain IPsecPolicy:CMAP:1037 (
    StreamID = 1037
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.0.2
        DestinationIP = 172.16.0.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

NetworkInterface (
    LogicalName = "DP0"
    IPsecPolicy = IPsecPolicy:CMAP:1000
)

NetworkInterface (
    LogicalName = "DP1"
    IPsecPolicy = IPsecPolicy:CMAP:1001
)

NetworkInterface (
    LogicalName = "DP2"
    IPsecPolicy = IPsecPolicy:CMAP:1002
)

NetworkInterface (
    LogicalName = "DP3"
    IPsecPolicy = IPsecPolicy:CMAP:1003
)

NetworkInterface (
    LogicalName = "DP4"
    IPsecPolicy = IPsecPolicy:CMAP:1004
)

NetworkInterface (
    LogicalName = "DP5"
```

```
    IPsecPolicy = IPsecPolicy:CMAP:1005
)

NetworkInterface (
    LogicalName = "DP6"
    IPsecPolicy = IPsecPolicy:CMAP:1006
)

NetworkInterface (
    LogicalName = "DP7"
    IPsecPolicy = IPsecPolicy:CMAP:1007
)

NetworkInterface (
    LogicalName = "DP8"
    IPsecPolicy = IPsecPolicy:CMAP:1008
)

NetworkInterface (
    LogicalName = "DP9"
    IPsecPolicy = IPsecPolicy:CMAP:1009
)

NetworkInterface (
    LogicalName = "DP10"
    IPsecPolicy = IPsecPolicy:CMAP:1010
)

NetworkInterface (
    LogicalName = "DP11"
    IPsecPolicy = IPsecPolicy:CMAP:1011
)

NetworkInterface (
    LogicalName = "DP12"
    IPsecPolicy = IPsecPolicy:CMAP:1012
)

NetworkInterface (
    LogicalName = "DP13"
    IPsecPolicy = IPsecPolicy:CMAP:1013
)

NetworkInterface (
    LogicalName = "DP14"
    IPsecPolicy = IPsecPolicy:CMAP:1014
)

NetworkInterface (
    LogicalName = "DP15"
    IPsecPolicy = IPsecPolicy:CMAP:1015
)

NetworkInterface (
    LogicalName = "DP16"
    IPsecPolicy = IPsecPolicy:CMAP:1016
)

NetworkInterface (
    LogicalName = "DP17"
    IPsecPolicy = IPsecPolicy:CMAP:1017
)

NetworkInterface (
    LogicalName = "DP18"
    IPsecPolicy = IPsecPolicy:CMAP:1018
```

```
)

NetworkInterface (
    LogicalName = "DP19"
    IPsecPolicy = IPsecPolicy:CMAP:1019
)

NetworkInterface (
    LogicalName = "DP20"
    IPsecPolicy = IPsecPolicy:CMAP:1020
)

NetworkInterface (
    LogicalName = "DP21"
    IPsecPolicy = IPsecPolicy:CMAP:1021
)

NetworkInterface (
    LogicalName = "DP22"
    IPsecPolicy = IPsecPolicy:CMAP:1022
)

NetworkInterface (
    LogicalName = "DP23"
    IPsecPolicy = IPsecPolicy:CMAP:1023
)

NetworkInterface (
    LogicalName = "DP24"
    IPsecPolicy = IPsecPolicy:CMAP:1024
)

NetworkInterface (
    LogicalName = "DP25"
    IPsecPolicy = IPsecPolicy:CMAP:1025
)

NetworkInterface (
    LogicalName = "DP26"
    IPsecPolicy = IPsecPolicy:CMAP:1026
)

NetworkInterface (
    LogicalName = "DP27"
    IPsecPolicy = IPsecPolicy:CMAP:1027
)

NetworkInterface (
    LogicalName = "DP28"
    IPsecPolicy = IPsecPolicy:CMAP:1028
)

NetworkInterface (
    LogicalName = "DP29"
    IPsecPolicy = IPsecPolicy:CMAP:1029
)

NetworkInterface (
    LogicalName = "DP30"
    IPsecPolicy = IPsecPolicy:CMAP:1030
)

NetworkInterface (
    LogicalName = "DP31"
    IPsecPolicy = IPsecPolicy:CMAP:1031
)
```

```
NetworkInterface (
    LogicalName = "DP32"
    IPsecPolicy = IPsecPolicy:CMAP:1032
)

NetworkInterface (
    LogicalName = "DP33"
    IPsecPolicy = IPsecPolicy:CMAP:1033
)

NetworkInterface (
    LogicalName = "DP34"
    IPsecPolicy = IPsecPolicy:CMAP:1034
)

NetworkInterface (
    LogicalName = "DP35"
    IPsecPolicy = IPsecPolicy:CMAP:1035
)

NetworkInterface (
    LogicalName = "DP36"
    IPsecPolicy = IPsecPolicy:CMAP:1036
)

NetworkInterface (
    LogicalName = "DP37"
    IPsecPolicy = IPsecPolicy:CMAP:1037
)
```

Текст конфигурации ipsm_dpdk.cfg для шлюза GW1

```
[PERFORMANCE]
threads = 38                        ;maximum: (cpu core num (maximum:254, including
HyperThreading) - 2 - 2 * ports_num) -- processing (encrypt/decrypt/filter) threads
number
;sendqueue_size = 64000     ;min: 1000 max: 100000 default: 64000 -- size of re-order
fixing queue
;disable_sendqueue = no     ;yes/no, default: no -- disable re-order fixing queue
;tx_retries = 10           ;min: 0 max: 1000 default: 10 -- retries count for outgoing
packets before drop
;tx_delay = 20                ;min: 0 max: 200 default: 20 -- delay in microseconds
before another retry of sending packet burst
;rx_desc = 2048           ;min: 32 max: 4096 default: 2048 -- number of rx descriptors
in network adapter configuration
;tx_desc = 2048           ;min: 32 max: 4096 default: 2048 -- number of tx descriptors
in network adapter configuration
;no_max_freq = no             ;yes/no, default: no -- disable setting max possible
frequency for our processor cores
;sendq_burst_threshold = 0   ;min: 100 max: 100000 default: 0 (disabled) -- make a
delay, if sending N packets from sendqueue in a row
;sendq_burst_delay = 10     ;min: 1 max: 200 default: 10 -- delay in microseconds when
sendq_burst_threshold activated
;pcap_mpool_size = 262143    ;min: 131071: max 4194303: default: 262143 -- number of
buffers in memory pool, num = 2^q - 1
;rx_queue_len = 16           ;min: 1 max: 32 default: 16 -- size of thread queue (in
bursts)
;rx_sleep = 5               ;min: 0 max: 10000 default: 5 -- pause in microseconds on
rx thread if there are no packets incoming
;tx_sleep = 5               ;min: 0 max: 10000 default: 5 -- pause in microseconds on
tx thread if there are no packets to send
;wrk_sleep = 5              ;min: 0 max: 10000 default: 5 -- pause in microseconds on
wrk thread if there are no packets incoming
```

```
;cb_wait = 5                 ;min: 0 max: 10000 default: 5 -- wait in microseconds on
wrk thread if corresponding tx thread is busy
;single_local_thr = yes      ;yes/no, default: yes -- process all incoming local (dst
is gate itself) IPv4 (not etherip) traffic in single thread (DP0)
;rx_cache_size = 64000      ;min: 2000: max 200000: default: 64000 -- size of rx thread
packet cache
;cache_burst_size = 8       ;min: 1: max 32: default: 8 -- max size of single transfer
from rx thread cache to wrk thread (in bursts). Must be less then rx_queue_len

[EAL]
coremask = 0xfffffffffff                ;mask should cover all cpu cores, including
HyperThreading
;channels = 1               ;min: 1 max: 4 default: 1    -- memory channels number
;cpuset    =    (0-2,4)@(0-1)                    ;map    threads    to    cpu    cores:
<threads[@cpus]>[<,threads[@cpus]>...]
;eal_log_level = 4          ;min: 1 max: 8 default: 4    -- log level of dpdk messages
;rx_pthresh = 8               ;min: 0 max: 255 default: 8  -- rx prefetch threshold
register value
;rx_hthresh = 8             ;min: 0 max: 255 default: 8  -- rx host threshold register
value
;rx_wthresh = 4              ;min: 0 max: 255 default: 4  -- rx write-back threshold
register value
;tx_pthresh = 36             ;min: 0 max: 255 default: 36 -- tx prefetch threshold
register value
;tx_hthresh = 0             ;min: 0 max: 255 default: 0  -- tx host threshold register
value
;tx_wthresh = 0              ;min: 0 max: 255 default: 0  -- tx write-back threshold
register value

[MISC]
;print_stats = no           ;yes/no, default: no -- print send/receive/drop statistics
;stats_period = 1              ;min: 1: max: 86400 default: 1 -- at this period (in
seconds) statistics is collected
;stats_file = /tmp/pkt_stats.txt    ;name of file for print_stats
;stats_file_size = 10       ;min: 1 max: 100 default: 10 -- max size of statistics file
in megabytes. After rotate, previous instance saves as ".old"
;print_frames = no          ;yes/no, default: no -- print incoming/outgoing packets in
hex
;frames_file = /tmp/frames.txt      ;name of file for print_frames
;frames_file_size = 50      ;min: 1 max: 200 default: 50 -- max size of packet hexdump
file in megabytes. After roteate, previous instance saves as ".old"
;frames_time = no             ;yes/no, default: no -- print time for each packet in
print_frames
;pf_max_bytes = 42          ;min: 14 max: 1400 default: 42 -- print only N firs bytes
in print_frames
;natt_port = 4500           ;min: 1 max: 65535: default: 4500
;mssfix = 8000              ;min: 536 max: 9670 default: disabled  -- change MSS field
in forwarded tcp syn packets if it greater than N
;mssfix_force = no         ;yes/no, default: no -- always change MSS field in forwarded
tcp syn packets, even if it's lesser than mssfix value

[PORT0]
pci_id = 83:00.0                   ;pci address of network interface
outer = yes                        ;yes/no, default: no -- consider port as looking to
outer network; outer port cant be in l2-mode
l3_ip = 10.1.1.1                   ;ip address of corresponding vEthN
l3_mask = 24                       ;mask of corresponding vEthN
gw_ip = 10.1.1.2                   ;default gateway ip-address
;next_hop_mac = 00:00:00:00:00:00  ;default destination mac-address for outgoing frames
pair_port = 1                      ;index of port for sending packets received on this
one; also packets, received on pair_port, will be sent from this one
mtu = 9710                         ;min: 68 max: 9710 default: 9710
;next_hop_mac_force = no           ;yes/no, default no -- always set next_hop_mac as
destination mac address for outgoing L3-frames
;vlan_identifier = 0            ;min: 0 max: 4094 default: 0 -- 802.1Q VLAN identifier
(VID)
```

```
;vlan_priority_code_point = 0       ;min: 0 max: 7 default: 0 -- Priority code point
(PCP) which is referts to the 802.1p class of service
;allowed_ethertypes = none        ; ethertypes in hex (32 max, "," as divider) -- pass
this ethertypes to/from corresponding vEth. IPv4(0x0800) and ARP(0x0806) always passed,
others dropped by default
;no_fc = no                         ;yes/no, default no  -- disable flow control on
this port
;no_promisc = yes                   ;yes/no, default: yes (for l2-port port - no) --
disable promiscuous mode on this port
;multicast_enable = yes            ;yes/no, default: yes (for l2-port - no) -- enable
receiving all multicast ip packets mode on this port
;hw_ip_checksum = no                ;yes/no, default: no -- enable additional stats
about l3/l4 checksum errors and oversized packets
;hw_vlan_extend = no               ;yes/no, default: no -- enable double-vlan
;pmtud = 8000                      ;min: 68 max: 65535 default: disabled -- send "ICMP
Destination Unreachable -- Fragmentation Needed" for ip packets with DF bit, greater
than N bytes

[PORT1]
pci_id = 84:00.0                   ;pci address of network interface
l2_src_ip = 172.16.0.1                ;source ip address of new ip packet for l2-
encalpsulation
l2_dst_ip = 172.16.0.2             ;destination ip address of new ip packet for l2-
encalpsulation
pair_port = 0                      ;index of port for sending packets received on this
one; also packets, received on pair_port, will be sent from this one
mtu = 9610                         ;min: 68 max: 9710 default: 9710
;no_fc = no                          ;yes/no, default no  -- disable flow control on
this port
;no_promisc = no                     ;yes/no, default: no (for outer port - yes) --
disable promiscuous mode on this port
;multicast_enable = no              ;yes/no, default: no (for outer port - yes) --
enable receiving all multicast ip packets mode on this port
;copy_tos = no                     ;yes/no, default: no -- copy ToS-field from orig ip
header to l2-encalpsulation ip header
;df_handling = copy                ;copy/set/clear, default copy -- DF bit: copy from
orig ip header to l2-encapsulation ip header
;hw_ip_checksum = no                ;yes/no, default: no -- enable additional stats
about l3/l4 checksum errors and oversized packets
;hw_vlan_extend = no               ;yes/no, default: no -- enable double-vlan
;pmtud = 8000                      ;min: 68 max: 65535 default: disabled -- send "ICMP
Destination Unreachable -- Fragmentation Needed" for ip packets with DF bit, greater
than N bytes
```

Текст конфигурации ipsm_dpdk.cfg для шлюза GW2

```
[PERFORMANCE]
threads = 38                       ;maximum: (cpu core num (maximum:254, including
HyperThreading) - 2 - 2 * ports_num) -- processing (encrypt/decrypt/filter) threads
number
;sendqueue_size = 64000     ;min: 1000 max: 100000 default: 64000 -- size of re-order
fixing queue
;disable_sendqueue = no     ;yes/no, default: no -- disable re-order fixing queue
;tx_retries = 10           ;min: 0 max: 1000 default: 10 -- retries count for outgoing
packets before drop
;tx_delay = 20                ;min: 0 max: 200 default: 20 -- delay in microseconds
before another retry of sending packet burst
;rx_desc = 2048           ;min: 32 max: 4096 default: 2048 -- number of rx descriptors
in network adapter configuration
;tx_desc = 2048           ;min: 32 max: 4096 default: 2048 -- number of tx descriptors
in network adapter configuration
;no_max_freq = no             ;yes/no, default: no -- disable setting max possible
frequency for our processor cores
;sendq_burst_threshold = 0   ;min: 100 max: 100000 default: 0 (disabled) -- make a
delay, if sending N packets from sendqueue in a row
```

```
;sendq_burst_delay = 10     ;min: 1 max: 200 default: 10 -- delay in microseconds when
sendq_burst_threshold activated
;pcap_mpool_size = 262143    ;min: 131071: max 4194303: default: 262143 -- number of
buffers in memory pool, num = 2^q - 1
;rx_queue_len = 16           ;min: 1 max: 32 default: 16 -- size of thread queue (in
bursts)
;rx_sleep = 5               ;min: 0 max: 10000 default: 5 -- pause in microseconds on
rx thread if there are no packets incoming
;tx_sleep = 5               ;min: 0 max: 10000 default: 5 -- pause in microseconds on
tx thread if there are no packets to send
;wrk_sleep = 5              ;min: 0 max: 10000 default: 5 -- pause in microseconds on
wrk thread if there are no packets incoming
;cb_wait = 5                ;min: 0 max: 10000 default: 5 -- wait in microseconds on
wrk thread if corresponding tx thread is busy
;single_local_thr = yes     ;yes/no, default: yes -- process all incoming local (dst
is gate itself) IPv4 (not etherip) traffic in single thread (DP0)
;rx_cache_size = 64000      ;min: 2000: max 200000: default: 64000 -- size of rx thread
packet cache
;cache_burst_size = 8       ;min: 1: max 32: default: 8 -- max size of single transfer
from rx thread cache to wrk thread (in bursts). Must be less then rx_queue_len

[EAL]
coremask = 0xfffffffffff                ;mask should cover all cpu cores, including
HyperThreading
;channels = 1               ;min: 1 max: 4 default: 1    -- memory channels number
;cpuset    =    (0-2,4)@(0-1)                  ;map    threads    to    cpu    cores:
<threads[@cpus]>[<,threads[@cpus]>...]
;eal_log_level = 4          ;min: 1 max: 8 default: 4    -- log level of dpdk messages
;rx_pthresh = 8               ;min: 0 max: 255 default: 8   -- rx prefetch threshold
register value
;rx_hthresh = 8             ;min: 0 max: 255 default: 8  -- rx host threshold register
value
;rx_wthresh = 4              ;min: 0 max: 255 default: 4  -- rx write-back threshold
register value
;tx_pthresh = 36             ;min: 0 max: 255 default: 36 -- tx prefetch threshold
register value
;tx_hthresh = 0             ;min: 0 max: 255 default: 0  -- tx host threshold register
value
;tx_wthresh = 0              ;min: 0 max: 255 default: 0  -- tx write-back threshold
register value

[MISC]
;print_stats = no           ;yes/no, default: no -- print send/receive/drop statistics
;stats_period = 1              ;min: 1: max: 86400 default: 1 -- at this period (in
seconds) statistics is collected
;stats_file = /tmp/pkt_stats.txt    ;name of file for print_stats
;stats_file_size = 10       ;min: 1 max: 100 default: 10 -- max size of statistics file
in megabytes. After rotate, previous instance saves as ".old"
;print_frames = no          ;yes/no, default: no -- print incoming/outgoing packets in
hex
;frames_file = /tmp/frames.txt      ;name of file for print_frames
;frames_file_size = 50      ;min: 1 max: 200 default: 50 -- max size of packet hexdump
file in megabytes. After roteate, previous instance saves as ".old"
;frames_time = no             ;yes/no, default: no -- print time for each packet in
print_frames
;pf_max_bytes = 42          ;min: 14 max: 1400 default: 42 -- print only N firs bytes
in print_frames
;natt_port = 4500           ;min: 1 max: 65535: default: 4500
;mssfix = 8000              ;min: 536 max: 9670 default: disabled  -- change MSS field
in forwarded tcp syn packets if it greater than N
;mssfix_force = no         ;yes/no, default: no -- always change MSS field in forwarded
tcp syn packets, even if it's lesser than mssfix value

[PORT0]
pci_id = 83:00.0                   ;pci address of network interface
```

```
outer = yes                          ;yes/no, default: no -- consider port as looking to
outer network; outer port cant be in l2-mode
l3_ip = 10.1.1.2                     ;ip address of corresponding vEthN
l3_mask = 24                         ;mask of corresponding vEthN
gw_ip = 10.1.1.1                     ;default gateway ip-address
;next_hop_mac = 00:00:00:00:00:00  ;default destination mac-address for outgoing frames
pair_port = 1                        ;index of port for sending packets received on this
one; also packets, received on pair_port, will be sent from this one
mtu = 9710                           ;min: 68 max: 9710 default: 9710
;next_hop_mac_force = no             ;yes/no, default no -- always set next_hop_mac as
destination mac address for outgoing L3-frames
;vlan_identifier = 0             ;min: 0 max: 4094 default: 0 -- 802.1Q VLAN identifier
(VID)
;vlan_priority_code_point = 0       ;min: 0 max: 7 default: 0 -- Priority code point
(PCP) which is referts to the 802.1p class of service
;allowed_ethertypes = none        ; ethertypes in hex (32 max, "," as divider) -- pass
this ethertypes to/from corresponding vEth. IPv4(0x0800) and ARP(0x0806) always passed,
others dropped by default
;no_fc = no                           ;yes/no, default no  -- disable flow control on
this port
;no_promisc = yes                    ;yes/no, default: yes (for l2-port port - no) --
disable promiscuous mode on this port
;multicast_enable = yes              ;yes/no, default: yes (for l2-port - no) -- enable
receiving all multicast ip packets mode on this port
;hw_ip_checksum = no                 ;yes/no, default: no -- enable additional stats
about l3/l4 checksum errors and oversized packets
;hw_vlan_extend = no                 ;yes/no, default: no -- enable double-vlan
;pmtud = 8000                        ;min: 68 max: 65535 default: disabled -- send "ICMP
Destination Unreachable -- Fragmentation Needed" for ip packets with DF bit, greater
than N bytes

[PORT1]
pci_id = 84:00.0                     ;pci address of network interface
l2_src_ip = 172.16.0.2               ;source ip address of new ip packet for l2-
encalpsulation
l2_dst_ip = 172.16.0.1               ;destination ip address of new ip packet for l2-
encalpsulation
pair_port = 0                        ;index of port for sending packets received on this
one; also packets, received on pair_port, will be sent from this one
mtu = 9610                           ;min: 68 max: 9710 default: 9710
;no_fc = no                          ;yes/no, default no  -- disable flow control on
this port
;no_promisc = no                     ;yes/no, default: no (for outer port - yes) --
disable promiscuous mode on this port
;multicast_enable = no               ;yes/no, default: no (for outer port - yes) --
enable receiving all multicast ip packets mode on this port
;copy_tos = no                       ;yes/no, default: no -- copy ToS-field from orig ip
header to l2-encalpsulation ip header
;df_handling = copy                  ;copy/set/clear, default copy -- DF bit: copy from
orig ip header to l2-encapsulation ip header
;hw_ip_checksum = no                 ;yes/no, default: no -- enable additional stats
about l3/l4 checksum errors and oversized packets
;hw_vlan_extend = no                 ;yes/no, default: no -- enable double-vlan
;pmtud = 8000                        ;min: 68 max: 65535 default: disabled -- send "ICMP
Destination Unreachable -- Fragmentation Needed" for ip packets with DF bit, greater
than                                 N                                    bytes
```

Текст файла /etc/ifaliases.cf для шлюзов GW1 и GW2

```
interface (name="DP0" pattern="10G_000")
interface (name="DP1" pattern="10G_001")
interface (name="DP2" pattern="10G_002")
interface (name="DP3" pattern="10G_003")
interface (name="DP4" pattern="10G_004")
interface (name="DP5" pattern="10G_005")
```

```
interface (name="DP6" pattern="10G_006")
interface (name="DP7" pattern="10G_007")
interface (name="DP8" pattern="10G_008")
interface (name="DP9" pattern="10G_009")
interface (name="DP10" pattern="10G_010")
interface (name="DP11" pattern="10G_011")
interface (name="DP12" pattern="10G_012")
interface (name="DP13" pattern="10G_013")
interface (name="DP14" pattern="10G_014")
interface (name="DP15" pattern="10G_015")
interface (name="DP16" pattern="10G_016")
interface (name="DP17" pattern="10G_017")
interface (name="DP18" pattern="10G_018")
interface (name="DP19" pattern="10G_019")
interface (name="DP20" pattern="10G_020")
interface (name="DP21" pattern="10G_021")
interface (name="DP22" pattern="10G_022")
interface (name="DP23" pattern="10G_023")
interface (name="DP24" pattern="10G_024")
interface (name="DP25" pattern="10G_025")
interface (name="DP26" pattern="10G_026")
interface (name="DP27" pattern="10G_027")
interface (name="DP28" pattern="10G_028")
interface (name="DP29" pattern="10G_029")
interface (name="DP30" pattern="10G_030")
interface (name="DP31" pattern="10G_031")
interface (name="DP32" pattern="10G_032")
interface (name="DP33" pattern="10G_033")
interface (name="DP34" pattern="10G_034")
interface (name="DP35" pattern="10G_035")
interface (name="DP36" pattern="10G_036")
interface (name="DP37" pattern="10G_037")
interface (name="FastEthernet0/0" pattern="vEth0")
interface (name="FastEthernet0/1" pattern="vEth1")
```