Построение VPN туннеля между двумя подсетями, защищаемыми шлюзами безопасности «С-Терра Шлюз», при наличии динамического NAT

Описание стенда

Сценарий иллюстрирует построение защищенного соединения между двумя подсетями SN1 и SN2, которые защищаются шлюзами безопасности «С-Терра Шлюз». 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. Шлюз GW1 находится за динамическим NAT-ом. Инициатором при таком соединении сможет выступать только шлюз, находящийся за динамическим NAT-ом – GW1.

В рамках данного сценария для аутентификации партнеры будут использовать сертификаты. В качестве криптопровайдера будет использован «КриптоПро CSP» версии 3.9. Шлюзы безопасности «С-Терра Шлюз 4.1».

Параметры защищенного соединения:

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

Схема стенда (Рисунок 1):

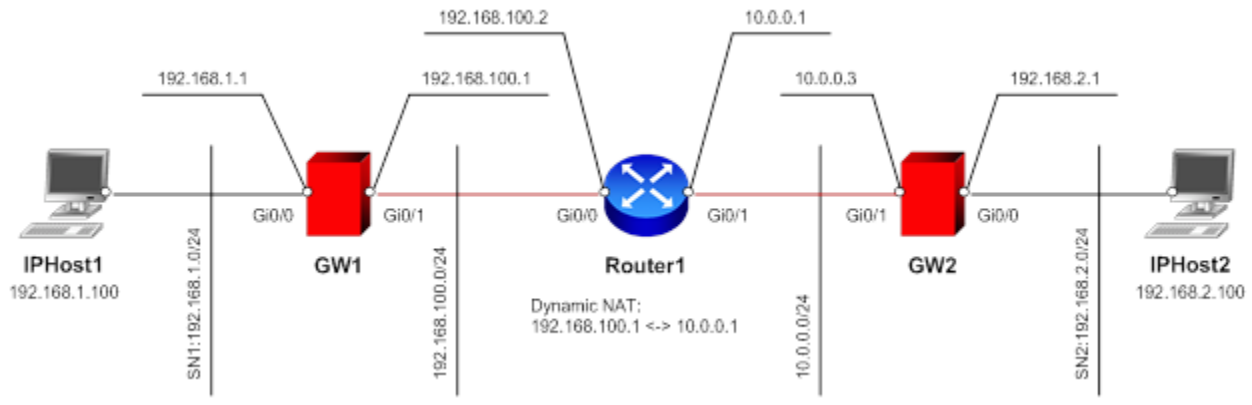

Рисунок 1

Настройка стенда

Настройка шлюза безопасности GW1

Настройку начните со шлюза безопасности GW1. Все настройки производятся через локальную консоль или удаленно (SSH с правами суперпользователя) по доверенному каналу связи.

Инициализация шлюза описывается в документации на ПК «С-Терра Шлюз 4.1» («Инициализация S-Terra Gate на вычислительных системах архитектуры Intel x86/x86-64», раздел «Инициализация S-Terra Gate при первом старте»).

В данном сценарии для аутентификации используются сертификаты. Для корректной работы необходимо зарегистрировать сертификат CA (УЦ) и локальный сертификат.

В данном сценарии список отозванных сертификатов (CRL) не используется и будет отключен. Информацию об использовании CRL можно найти в документации на ПК «С-Терра Шлюз 4.1» («Cisco-like команды», раздел «Команды для работы с сертификатами»).

Настройка интерфейсов

IP-адреса для интерфейсов рекомендуется настроить через cisco-like консоль.

1. Для входа в консоль запустите cs_console:

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

   Пароль по умолчанию: csp.
2. Перейдите в режим настройки:

```
sterragate#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

3. В настройках интерфейсов задайте IP-адреса:

```
sterragate(config)#interface GigabitEthernet 0/0
sterragate(config-if)#ip address 192.168.1.1 255.255.255.0
sterragate(config-if)#no shutdown
sterragate(config-if)#exit
sterragate(config)#interface GigabitEthernet 0/1
sterragate(config-if)#ip address 192.168.100.1 255.255.255.0
sterragate(config-if)#no shutdown
sterragate(config-if)#exit
```

4. Задайте адрес шлюза по умолчанию:

```
sterragate(config)#ip route 0.0.0.0 0.0.0.0 192.168.100.2
```

5. Выйдите из cisco-like интерфейса:

```
sterragate(config)#end
sterragate#exit
```

Регистрация CA сертификата (сертификата УЦ)

Для регистрации CA сертификата (сертификата УЦ) необходимо выполнить следующие действия:

1. Установите правильное системное время.

   Например:

```
root@sterragate:~# date 041013152013
Wed Apr 10 13:15:00 UTC 2013
```

Данная запись соответствует 10 апреля 2013 года 13:15.

2. Создайте папку /certs:

```
root@sterragate:~# mkdir /certs
```

3. Доставьте файл CA сертификата на шлюз безопасности в предварительно созданный на нем каталог /certs. Для доставки можно воспользоваться утилитой pscp.exe из пакета Putty, применив команду:

```
pscp <CA file path>/<CA file name> root@<gate address>:/<path>
```

Например:

```
pscp D:\ca.cer root@192.168.1.1:/certs
```

```
…
Store key in cache? (y/n)
root@192.168.1.1's password:
```

Важно: Среда передачи в этом случае должна быть доверенной.
Описание создания доверенной среды через недоверенные каналы связи смотрите в документации на ПК «С-Терра Шлюз 4.1» («Построение VPN туннеля между шлюзом S-Terra Gate 4.1 и рабочим местом администратора для удаленной настройки шлюза»).

4. С помощью утилиты cert_mgr зарегистрируйте сертификат в базе продукта:

```
root@sterragate:~# cert_mgr import -f /certs/ca.cer -t
```

```
1 OK C=RU,L=Moscow,O=S-Terra CSP,OU=Research,CN=CA-W2008SP1-X64-CA
```

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

Регистрация локального сертификата

Для регистрации локального сертификата в базе продукта выполните следующие действия:

1. Сформируйте запрос на сертификат при помощи утилиты cert_mgr:

```
root@sterragate:~# cert_mgr create -subj "C=RU,OU=Research,CN=GW1" -GOST_R3410EL
```

```
Press keys...
[.....................................]
-----BEGIN CERTIFICATE REQUEST-----
MIIBCjCBuAIBADAuMQswCQYDVQQGEwJSVTERMA8GA1UECxMIUmVzZWFyY2gx
DDAKBgNVBAMTA0dXMTBjMBwGBiqFAwICEzASBgcqhQMCAiMBBgcqhQMCAh4B
A0MABECTQeB5UoPsTbSs8obnrQ6KMJwpc/BFrUgfI6AjQl95ccE4D5jEAq8m
HB3ZvXfxMsQ/1NAy73OPgaz32W/scOkgoB4wHAYJKoZIhvcNAQkOMQ8wDTAL
BgNVHQ8EBAMCB4AwCgYGKoUDAgIDBQADQQBAuCzk8bASJqbP5pYHAG5A3LKx
OPFjiF1m+2/WkxGkWJWEm5gjNNyWquslmxLq9nX2rff4X3E5xF40iudzHoZz
-----END CERTIFICATE REQUEST-----
```

2. Передайте полученный запрос сертификата на УЦ. Процедура выдачи сертификата на УЦ по запросу описана в документации на ПК «С-Терра Шлюз 4.1» («Приложение», раздел «Создание локального сертификата с использованием СКЗИ «КриптоПро CSP»»).
3. Перенесите полученный файл на шлюз безопасности (параметры pscp описаны выше).
4. Зарегистрируйте локальный сертификат в базе продукта, применив утилиту cert_mgr:

```
root@sterragate:~# cert_mgr import -f /certs/gw1.cer
```

```
1 OK C=RU,OU=Research,CN=GW1
```

5. Убедитесь, что сертификаты импортированы успешно:

```
root@sterragate:~# cert_mgr show
```

```
Found 2 certificates. No CRLs found.
1 Status: trusted C=RU,L=Moscow,O=S-Terra CSP,OU=Research,CN=CA-W2008SP1-X64-CA
```

```
2 Status: local   C=RU,OU=Research,CN=GW1
```

Создание политики безопасности

После регистрации сертификатов необходимо создать политику безопасности для GW1. Создавать политику рекомендуется в интерфейсе командной строки. Для входа в консоль запустите cs_console:

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

Пароль по умолчанию: csp.

Важно: пароль по умолчанию необходимо сменить.

1. Перейдите в режим настройки:

```
sterragate#conf t
```

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

2. Смените пароль по умолчанию:

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

3. Смените название шлюза:

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

4. Задайте тип идентификации:

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

5. Задайте параметры для IKE:

```
GW1(config)#crypto isakmp policy 1
GW1(config-isakmp)#hash gost
GW1(config-isakmp)#encryption gost
GW1(config-isakmp)#authentication gost-sig
GW1(config-isakmp)#group vko
GW1(config-isakmp)#exit
```

6. Создайте набор преобразований для IPsec:

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

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

```
GW1(config)#ip access-list extended LIST
GW1(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
GW1(config-ext-nacl)#exit
```

8. Создайте крипто-карту:

```
GW1(config)#crypto map CMAP 1 ipsec-isakmp
```

```
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
```

```
GW1(config-crypto-map)#match address LIST
GW1(config-crypto-map)#set transform-set TSET
GW1(config-crypto-map)#set pfs vko
GW1(config-crypto-map)#set peer 10.0.0.3
GW1(config-crypto-map)#exit
```

9. Привяжите крипто-карту к интерфейсу, на котором будет туннель:

```
GW1(config)#interface GigabitEthernet 0/1
```

```
GW1(config-if)#crypto map CMAP
GW1(config-if)#exit
```

10. Отключите обработку списка отозванных сертификатов (CRL):

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

11. 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 и текст LSP конфигурации для шлюза GW1.

Настройка шлюза GW2

Настройка шлюза безопасности GW2 происходит аналогично настройке устройства GW1, за исключением отмеченных ниже особенностей, связанных с тем, что при наличии динамического NAT-а, адрес партнера не может быть заранее известен.

Список доступа, описывающий трафик, подлежащий шифрованию:

```
GW2(config)#ip access-list extended LIST
GW2(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255 any
GW2(config-ext-nacl)#exit
```

Т.к. адрес партнера неизвестен заранее, следует использовать динамическую крипто-карту:

```
GW2(config)#crypto dynamic-map DMAP 1
GW2(config-crypto-map)#match address LIST
GW2(config-crypto-map)#set transform-set TSET
GW2(config-crypto-map)#set pfs vko
GW2(config-crypto-map)#exit
```

Динамическую крипто-карту следует привязать к статической:

```
GW2(config)#crypto map CMAP 1 ipsec-isakmp dynamic DMAP
```

В **Приложении** представлен текст cisco-like конфигурации и текст LSP конфигурации для шлюза GW2.

Настройка устройства IPHost1

На устройстве IPHost1 задайте IP-адрес, а в качестве шлюза по умолчанию укажите адрес внутреннего интерфейса шлюза безопасности GW1 – 192.168.1.1.

Настройка устройства IPHost2

На устройстве IPHost2 задайте IP-адрес, а в качестве шлюза по умолчанию укажите адрес внутреннего интерфейса шлюза безопасности GW2 – 192.168.2.1.

Настройка устройства Router1

На устройстве Router1 необходимо настроить динамический NAT, который будет преобразовывать адреса из подсети 192.168.100.0/24 во внешний адрес (10.0.0.1) и наоборот.

Проверка работоспособности стенда

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

На устройстве IPHost1 выполните команду ping:

```
ping 192.168.2.100
```

```
PING 192.168.2.100 (192.168.2.100) 56(84) bytes of data.
64 bytes from 192.168.2.100: icmp_req=1 ttl=62 time=1177 ms
64 bytes from 192.168.2.100: icmp_req=2 ttl=62 time=177 ms
64 bytes from 192.168.2.100: icmp_req=3 ttl=62 time=5.37 ms
64 bytes from 192.168.2.100: icmp_req=4 ttl=62 time=4.32 ms
64 bytes from 192.168.2.100: icmp_req=5 ttl=62 time=8.60 ms
^C
--- 192.168.2.100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4010ms
rtt min/avg/max/mdev = 4.326/274.593/1177.297/456.201 ms, pipe 2
```

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 3 (192.168.100.1,4500)-(10.0.0.3,4500) active 1976 1904

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 2 (192.168.1.0-192.168.1.255,*)-(192.168.2.0-192.168.2.255,*) * ESP nat-t-tunn 440
440
```

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
username cscons privilege 15 password 0 csp
aaa new-model
!
!
hostname GW1
enable password csp
!
!
!
logging trap debugging
!
!
crypto isakmp policy 1
 encr gost
 hash gost
 authentication gost-sig
 group vko
!
crypto ipsec transform-set TSET esp-gost28147-4m-imit
!
ip access-list extended LIST
 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
!
!
crypto map CMAP 1 ipsec-isakmp
 match address LIST
 set transform-set TSET
 set pfs vko
 set peer 10.0.0.3
!
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 ip address 192.168.100.1 255.255.255.0
 crypto map CMAP
!
interface GigabitEthernet0/2
 no ip address
 shutdown
!
interface GigabitEthernet0/3
 no ip address
 shutdown
!
!
ip route 0.0.0.0 0.0.0.0 192.168.100.2
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check none
```

```
crypto pki certificate chain s-terra_technological_trustpoint
certificate 4E4B0B11EFDB389E4E86244CDAA1B275
30820216308201C5A00302010202104E4B0B11EFDB389E4E86244CDAA1B27530
0806062A85030202033064310B300906035504061302525310F300D06035504
…
009B097DD81A81CFC792664AAC9E6908587195AE17A5D526DE196CB0D5B7E713
E9D07F4DC61F04CDBC87579FC44CE66D524CF742F2784805733F

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
username cscons privilege 15 password 0 csp
aaa new-model
!
!
hostname GW2
enable password csp
!
!
!
logging trap debugging
!
!
crypto isakmp policy 1
 encr gost
 hash gost
 authentication gost-sig
 group vko
!
crypto ipsec transform-set TSET esp-gost28147-4m-imit
!
ip access-list extended LIST
 permit ip 192.168.2.0 0.0.0.255 any
!
!
crypto dynamic-map DMAP 1
 match address LIST
 set transform-set TSET
 set pfs vko
!
crypto map CMAP 1 ipsec-isakmp dynamic DMAP
!
interface GigabitEthernet0/0
 ip address 192.168.2.1 255.255.255.0
!
interface GigabitEthernet0/1
 ip address 10.0.0.3 255.255.255.0
 crypto map CMAP
!
interface GigabitEthernet0/2
 no ip address
 shutdown
```

```
!
interface GigabitEthernet0/3
 no ip address
 shutdown
!
!
ip route 0.0.0.0 0.0.0.0 10.0.0.1
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check none
crypto pki certificate chain s-terra_technological_trustpoint
certificate 4E4B0B11EFDB389E4E86244CDAA1B275
30820216308201C5A003020102021O4E4B0B11EFDB389E4E86244CDAA1B27530
…
009B097DD81A81CFC792664AAC9E6908587195AE17A5D526DE196CB0D5B7E713
E9D07F4DC61F04CDBC87579FC44CE66D524CF742F2784805733F

quit
!
end
```

Текст LSP конфигурации для шлюза GW1

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Tue Apr 16 15:47:40 2013

GlobalParameters(
    Title                      = "This LSP was automatically generated by CSP Converter
at Tue Apr 16 15:47:40 2013"
    Version                      = LSP_4_1
    CRLHandlingMode              = OPTIONAL
    PreserveIPsecSA              = FALSE
)

IKEParameters(
    FragmentSize = 0
)

RoutingTable(
    Routes =
        Route(
            Destination = 0.0.0.0/0
            Gateway = 192.168.100.2
        )
)

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     = "GR341194CPRO1-65534"
    GroupID     = VKO_1B
    RestrictAuthenticationTo = GOST_SIGN
    LifetimeSeconds = 86400
)

ESPProposal TSET:ESP
(
    Transform* = ESPTransform
    (
        CipherAlg*          = "G2814789CPRO1-K288-CNTMAC-253"
        LifetimeSeconds     = 3600
        LifetimeKilobytes   = 4608000
    )
)

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

IKERule IKERule:CMAP:1
(
    IKEPeerIPFilter = 10.0.0.3
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign
    MainModeAuthMethod  = GOST:Sign
    DoNotUseDPD         = TRUE
    Priority            = 10
)

IPsecAction IPsecAction:CMAP:1
(
    TunnelingParameters = TunnelEntry(
        PeerIPAddress = 10.0.0.3
        DFHandling=COPY
        Assemble=TRUE
    )
    ContainedProposals = ( TSET:ESP )
    GroupID = VKO_1B
    IKERule = IKERule:CMAP:1
)

FilterChain IPsecPolicy:CMAP (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 192.168.1.0/24
        DestinationIP = 192.168.2.0/24
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)
```

```
NetworkInterface (
    LogicalName = "GigabitEthernet0/1"
    IPsecPolicy = IPsecPolicy:CMAP
)
```

Текст LSP конфигурации для шлюза GW2

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Tue Apr 16 15:55:34 2013

GlobalParameters(
    Title                       = "This LSP was automatically generated by CSP Converter
at Tue Apr 16 15:55:34 2013"
    Version                       = LSP_4_1
    CRLHandlingMode               = OPTIONAL
    PreserveIPsecSA               = FALSE
)

IKEParameters(
    FragmentSize = 0
)

RoutingTable(
    Routes =
        Route(
            Destination = 0.0.0.0/0
            Gateway = 10.0.0.1
        )
)

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     = "GR341194CPRO1-65534"
    GroupID     = VKO_1B
    RestrictAuthenticationTo = GOST_SIGN
    LifetimeSeconds = 86400
)

ESPProposal TSET:ESP
(
    Transform* = ESPTransform
    (
        CipherAlg*          = "G2814789CPRO1-K288-CNTMAC-253"
        LifetimeSeconds     = 3600
        LifetimeKilobytes   = 4608000
    )
```

```
)

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

IKERule IKERule:CMAP:1:DMAP:1
(
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign
    MainModeAuthMethod  = GOST:Sign
    DoNotUseDPD         = TRUE
    Priority            = 100
)

IPsecAction IPsecAction:CMAP:1:DMAP:1
(
    TunnelingParameters = TunnelEntry(
        DFHandling=COPY
        Assemble=TRUE
    )
    ContainedProposals = ( TSET:ESP )
    GroupID = VKO_1B
    IKERule = IKERule:CMAP:1:DMAP:1
)

FilterChain IPsecPolicy:CMAP (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 192.168.2.0/24
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1:DMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:DMAP:1:LIST"
    )
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/1"
    IPsecPolicy = IPsecPolicy:CMAP
)
```