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

Описание стенда

Сценарий иллюстрирует построение VPN туннелей между тремя подсетями, которые защищаются шлюзами безопасности Bel VPN Gate. VPN туннели, которые будут построены между устройствами GW1, GW2 и GW3, изображены на Рисунке 1. Шлюз GW3 является центральным. Между шлюзами GW1 и GW2 строится защищенное соединение только через центральный шлюз. Устройства Host1, Host2 и Host3 могут общаться между собой по VPN туннелю. Внутри подсетей LAN1, LAN2 и LAN3 трафик является “открытым”.

Настройка политики безопасности на шлюзах производится с учетом положений инструкции администратора категорированной сети (см. «Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 3.0.1.» Инструкция администратора категорированной сети»).

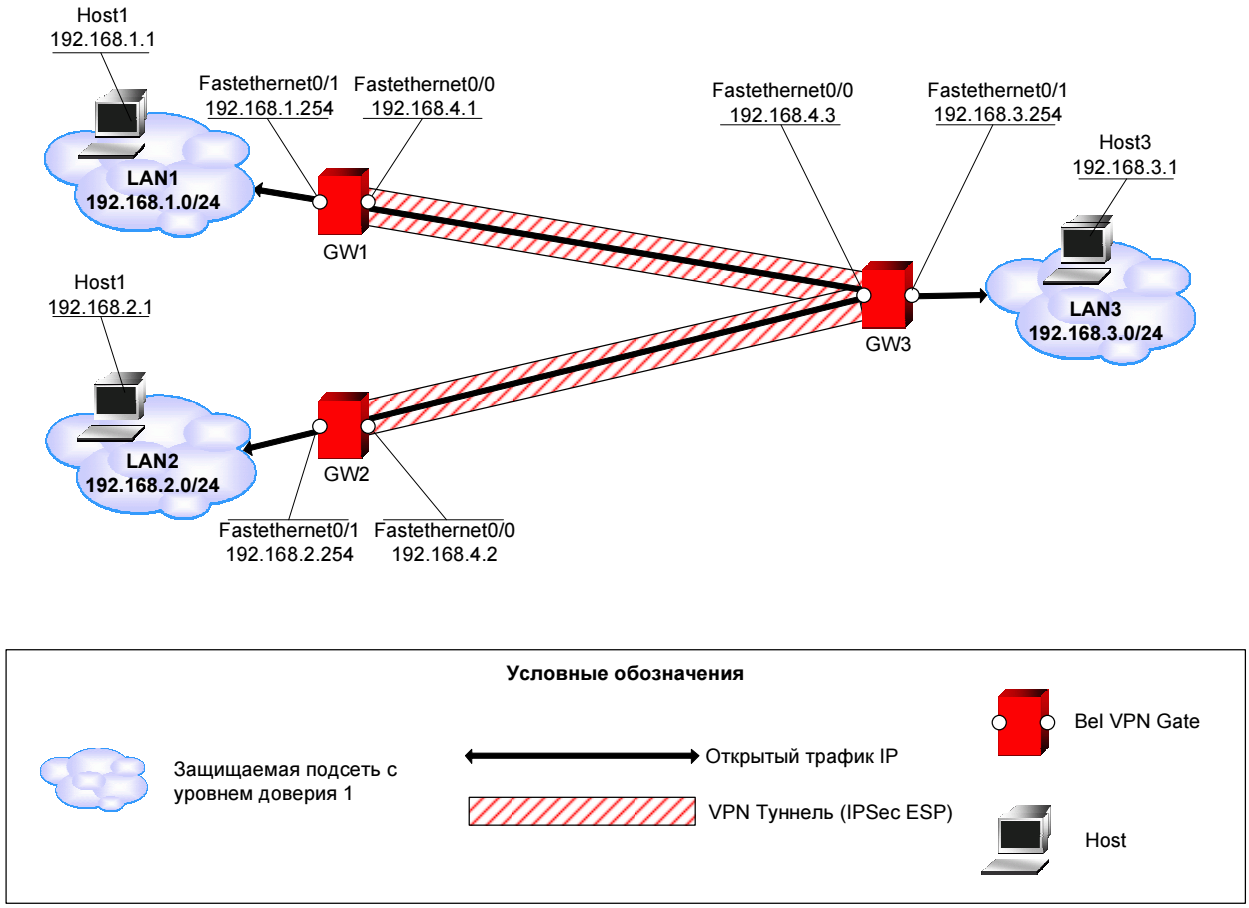

Рисунок 1

Параметры защищенного соединения:

- Аутентификация на Preshared Key.
- IKE parameters:

- Encryption algorithm – ГОСТ 28147-89
- Hash algorithm – СТБ 1176.1-99
- DH-group – group5 (1536)

- IPSec parameters:
  - ESP encryption algorithm – ГОСТ 28147-89
  - ESP integrity algorithm – ГОСТ 28147-89
  - PFS – group5 (1536)

Предварительные настройки

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

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

   на Host1 в качестве шлюза по умолчанию назначим адрес 192.168.1.254

   на Host2 назначим адрес 192.168.2.254

   на Host3 - адрес 192.168.3.254

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

   ```
   ip route 192.168.2.0 255.255.255.0 192.168.4.3 1
   ip route 192.168.3.0 255.255.255.0 192.168.4.3 1
   ```

3. На шлюзе GW2 выполним аналогичные действия:

   ```
   ip route 192.168.1.0 255.255.255.0 192.168.4.3 1
   ip route 192.168.3.0 255.255.255.0 192.168.4.3 1
   ```

4. На шлюзе GW3 выполним такие же действия:

   ```
   ip route 192.168.1.0 255.255.255.0 192.168.4.1 1
   ip route 192.168.2.0 255.255.255.0 192.168.4.1 1
   ```

5. После выполнения настроек убедимся, что пакеты маршрутизируются верно. Для этого на устройстве Host2 выполним команду traceroute 192.168.1.1:

   ```
   traceroute 192.168.1.1
   ```

   ```
   traceroute to 192.168.1.1 (192.168.1.1), 30 hops max, 40 byte packets
    1  192.168.2.254 (192.168.2.254)  0.980 ms  0.850 ms  0.691 ms
    2  192.168.4.3 (192.168.4.3)  0.731 ms  0.873 ms  0.711 ms
    3  192.168.4.1 (192.168.4.1)  0.797 ms  0.844 ms  0.690 ms
    4  192.168.1.1 (192.168.1.1)  0.838 ms  0.925 ms  0.791 ms
   ```

   Убедимся, что устройства в подсетях LAN1 и LAN2 доступны из подсети LAN3. Для этого на устройстве Host3 выполним:

   ```
   ping 192.168.1.1
   ```

   ```
   PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
   64 bytes from 192.168.2.1: icmp_seq=1 ttl=253 time=1.17 ms
   64 bytes from 192.168.2.1: icmp_seq=2 ttl=253 time=0.984 ms
   64 bytes from 192.168.2.1: icmp_seq=3 ttl=253 time=0.642 ms
   64 bytes from 192.168.2.1: icmp_seq=4 ttl=253 time=0.637 ms
   ```

```
ping 192.168.2.1

PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.3.1: icmp_seq=1 ttl=253 time=1.17 ms
64 bytes from 192.168.3.1: icmp_seq=2 ttl=253 time=0.984 ms
64 bytes from 192.168.3.1: icmp_seq=3 ttl=253 time=0.642 ms
64 bytes from 192.168.3.1: icmp_seq=4 ttl=253 time=0.637 ms
```

Настройка шлюза безопасности GW3

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

зададим параметры для IKE:

```
gw3(config)#crypto isakmp policy 1
gw3(config-isakmp)#hash md5
gw3(config-isakmp)#encryption des
gw3(config-isakmp)#authentication pre-share
gw3(config-isakmp)#group 5
gw3(config-isakmp)#exit
```

создадим предопределенные ключи для шлюзов GW1 и GW2:

```
gw3(config)#crypto isakmp key 12345 address 192.168.4.1
gw3(config)#crypto isakmp key 123456 address 192.168.4.2
```

создадим набор преобразований для IPsec:

```
gw3(config)#crypto ipsec transform-set TS1 esp-des esp-md5-hmac
gw3(cfg-crypto-trans)#mode tunnel
gw3(cfg-crypto-trans)#exit
```

опишем трафик, который планируется защищать:

```
gw3(config)#ip access-list extended LAN3toLAN2
gw3(config-ext-nacl)#permit  ip  192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
gw3(config-ext-nacl)#exit

gw3(config)#ip access-list extended LAN3toLAN1
gw3(config-ext-nacl)#permit  ip  192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
gw3(config-ext-nacl)#exit

gw3(config)#ip access-list extended LAN1toLAN2
gw3(config-ext-nacl)#permit  ip  192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
gw3(config-ext-nacl)#exit

gw3(config)#ip access-list extended LAN2toLAN1
gw3(config-ext-nacl)#permit  ip  192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
gw3(config-ext-nacl)#exit
```

создадим криптокарту:

```
gw3(config)#crypto map CMAP 1 ipsec-isakmp
gw3(config-crypto-map)#match address LAN3toLAN2
gw3(config-crypto-map)#set transform-set TS1
gw3(config-crypto-map)#set peer 192.168.4.2
gw3(config-crypto-map)#set pfs group5

gw3(config)#crypto map CMAP 2 ipsec-isakmp
gw3(config-crypto-map)#match address LAN3toLAN1
```

```
gw3(config-crypto-map)#set transform-set TS1
gw3(config-crypto-map)#set peer 192.168.4.1
gw3(config-crypto-map)#set pfs group5

gw3(config)#crypto map CMAP 3 ipsec-isakmp
gw3(config-crypto-map)#match address LAN1toLAN2
gw3(config-crypto-map)#set transform-set TS1
gw3(config-crypto-map)#set peer 192.168.4.2
gw3(config-crypto-map)#set pfs group5

gw3(config)#crypto map CMAP 4 ipsec-isakmp
gw3(config-crypto-map)#match address LAN2toLAN1
gw3(config-crypto-map)#set transform-set TS1
gw3(config-crypto-map)#set peer 192.168.4.1
gw3(config-crypto-map)#set pfs group5
```

привяжем криптокарту к интерфейсу, на котором будут терминироваться туннели:

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

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

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

Настройка шлюза безопасности GW1

Настройку шлюза безопасности GW1 будем производить аналогично устройству GW3.

Создадим политику безопасности, приведенную в Приложении.

Настройка шлюза безопасности GW2

Конфигурация для этого устройства приведена в Приложении.

Проверка работоспособности стенда

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

1. выполним команду ping 192.168.3.1 на устройстве Host1:

```
ping 192.168.3.1
```

```
PING 192.168.3.1 (192.168.3.1) from 192.168.2.1 : 56(84) bytes of data.
64 bytes from 192.168.3.1: icmp_seq=0 ttl=253 time=548.495 msec
64 bytes from 192.168.3.1: icmp_seq=1 ttl=253 time=1.318 msec
64 bytes from 192.168.3.1: icmp_seq=2 ttl=253 time=930 usec

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

2. также выполним команду ping 192.168.3.1 на устройстве Host 2:

```
ping 192.168.3.1

 PING 192.168.3.1 (192.168.3.1) 56(84) bytes of data.
 64 bytes from 192.168.3.1: icmp_seq=1 ttl=253 time=139 ms
 64 bytes from 192.168.3.1: icmp_seq=2 ttl=253 time=0.625 ms
 64 bytes from 192.168.3.1: icmp_seq=3 ttl=253 time=0.621 ms
 64 bytes from 192.168.3.1: icmp_seq=4 ttl=253 time=0.652 ms

 --- 192.168.3.1 ping statistics ---
 4 packets transmitted, 4 received, 0% packet loss, time 2998ms
 rtt min/avg/max/mdev = 0.621/35.275/139.202/60.002 ms
```

3. выполним команду ping 192.168.1.1 на устройстве Host2:

```
 ping 192.168.1.1

 PING 192.168.1.1 (192.168.1.1) from 192.168.2.1 : 56(84) bytes of data.
 64 bytes from 192.168.1.1: icmp_seq=0 ttl=59 time=711.478 msec
 64 bytes from 192.168.1.1: icmp_seq=1 ttl=59 time=1.982 msec
 64 bytes from 192.168.1.1: icmp_seq=2 ttl=59 time=5.508 msec
 64 bytes from 192.168.1.1: icmp_seq=3 ttl=59 time=1.716 msec

 --- 192.168.1.1 ping statistics ---
 4 packets transmitted, 4 packets received, 0% packet loss
 round-trip min/avg/max/mdev = 1.716/180.171/711.478/306.753 ms
```

В результате, между устройствами GW1, GW2 и GW3 должны установиться 4 VPN туннеля: из LAN1 в LAN3, из LAN2 в LAN3 и два туннеля для защиты трафика между подсетями LAN1 - LAN2. Убедиться в этом можно при помощи утилиты sa_show.

На устройстве GW3 выполним команду:

```
/opt/VPNagent/bin/sa_show

 IKE sessions: 0 initiated, 0 responded

 ISAKMP SA Num (Remote Addr,Port)-(Local Addr,Port) State Sent Rec
 ISAKMP SA 1 (192.168.4.1,500)-(192.168.4.3,500) ready 1588 1096
 ISAKMP SA 2 (192.168.4.2,500)-(192.168.4.3,500) ready 1604 1476

 IPSec SA Num (Remote Addr,Port)-(Local Addr,Port) Protocol Action Type Sent
 Rec
 IPSec SA 1 5 (192.168.1.0-192.168.1.255,*)-(192.168.3.0-192.168.3.255,*) * ESP
 tunn 9912 15104
 IPSec SA 2 6 (192.168.2.0-192.168.2.255,*)-(192.168.3.0-192.168.3.255,*) * ESP
 tunn 8904 13568
 IPSec SA 3 7 (192.168.2.0-192.168.2.255,*)-(192.168.1.0-192.168.1.255,*) * ESP
 tunn 924 1408
 IPSec SA 4 8 (192.168.1.0-192.168.1.255,*)-(192.168.2.0-192.168.2.255,*) * ESP
 tunn 924 1408
```

Данные настройки обеспечивают защищенный обмен между подсетями LAN1, LAN2 и LAN3. Остальной трафик разрешен, но защищаться не будет.

Приложение

Текст cisco-like конфигурации для GW1

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity address
username cscons privilege 15 password 0 csp
hostname GW1
enable password csp
!
!
!
logging trap debugging
!
!
crypto isakmp policy 1
 hash md5
 encr des
 authentication pre-share
 group 5
!
crypto isakmp key 12345 address 192.168.4.3
!
crypto ipsec transform-set TS1 esp-des esp-md5-hmac
!
ip access-list extended LAN1toLAN3
 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
!
ip access-list extended LAN1toLAN2
 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 LAN1toLAN3
 set transform-set TS1
 set pfs group5
 set peer 192.168.4.3
!
crypto map CMAP 2 ipsec-isakmp
 match address LAN1toLAN2
 set transform-set TS1
 set pfs group5
 set peer 192.168.4.3
!
!
!
interface FastEthernet0/0
 ip address 192.168.4.1 255.255.255.0
 crypto map CMAP
!
interface FastEthernet0/1
 ip address 192.168.1.254 255.255.255.0
!
!
ip route 192.168.2.0 255.255.255.0 192.168.4.3
ip route 192.168.3.0 255.255.255.0 192.168.4.3
!
end
```

Текст LSP для GW1

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Sun Apr 13 03:18:15 2014

GlobalParameters(
```

```
    Title                       = "This LSP was automatically generated by CSP
Converter at Sun Apr 13 03:18:15 2014"
    Version                     = "2.1"
    LDAPLogMessageLevel         = DEBUG
    SystemLogMessageLevel       = DEBUG
    PolicyLogMessageLevel       = DEBUG
    CertificatesLogMessageLevel = DEBUG
)

SyslogSettings(
    Server = 127.0.0.1
    Facility = LOG_LOCAL7
)

RoutingTable(
    Routes *=
        Route(
            Destination = 192.168.2.0/24
            Gateway = 192.168.4.3
            Metric = 1
        ),
        Route(
            Destination = 192.168.3.0/24
            Gateway = 192.168.4.3
            Metric = 1
        )
)
IKETransform IKETransform_1
(
    CipherAlg   *= "G2814789CPRO1-K256-CBC-65530"
    HashAlg     *= "STB1176199-65530"
    GroupID     *= MODP_1536
    LifetimeSeconds = 86400
)

ESPProposal ESP_TS1
(
    Transform* = ESPTransform
    (
        IntegrityAlg*       = "G2814789AV1-K256-MAC-65531"
        CipherAlg*          = "G2814789CPRO1-K256-CBC-250"
        LifetimeSeconds    = 3600
        LifetimeKilobytes   = 4608000
    )
)

ESPProposal ESP_TS1_1
(
    Transform* = ESPTransform
    (
        IntegrityAlg*       = "G2814789AV1-K256-MAC-65531"
        CipherAlg*          = "G2814789CPRO1-K256-CBC-250"
        LifetimeSeconds    = 3600
        LifetimeKilobytes   = 4608000
    )
)

AuthMethodPreshared IKE_auth_cs_key_192_168_4_3
(
    RemoteID = IdentityEntry(
        IPv4Address *= 192.168.4.3
    )
    SharedIKESecret = "cs_key_192_168_4_3"
)

IKERule IKE_CMAP_1
(
    Transform* = IKETransform_1
    AggrModeAuthMethod  *= IKE_auth_cs_key_192_168_4_3
    MainModeAuthMethod  *= IKE_auth_cs_key_192_168_4_3
    DoAutopass          = TRUE
```

```
    DoNotUseDPD         = TRUE
)

IPsecAction CMAP_1
(
    TunnelingParameters *= TunnelEntry(
        PeerIPAddress = 192.168.4.3

        DFHandling=COPY
    )
    ContainedProposals *= ( ESP_TS1 )
    GroupID *= MODP_1536
    IKERule = IKE_CMAP_1
)

AuthMethodPreshared IKE_auth_cs_key_192_168_4_3_1
(
    RemoteID = IdentityEntry(
        IPv4Address *= 192.168.4.3
    )
    SharedIKESecret = "cs_key_192_168_4_3"
)

IKERule IKE_CMAP_2
(
    Transform* = IKETransform_1
    AggrModeAuthMethod  *= IKE_auth_cs_key_192_168_4_3_1
    MainModeAuthMethod  *= IKE_auth_cs_key_192_168_4_3_1
    DoAutopass          = TRUE
    DoNotUseDPD         = TRUE
)

IPsecAction CMAP_2
(
    TunnelingParameters *= TunnelEntry(
        PeerIPAddress = 192.168.4.3

        DFHandling=COPY
    )
    ContainedProposals *= ( ESP_TS1_1 )
    GroupID *= MODP_1536
    IKERule = IKE_CMAP_2
)

FilteringRule Filter_nil_acl_CMAP_1
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.1.0/24 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.3.0/24 )
    NetworkInterfaces *= "eth0"
    Action *= ( CMAP_1 )
)

FilteringRule Filter_nil_acl_CMAP_2
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.1.0/24 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.2.0/24 )
    NetworkInterfaces *= "eth0"
    Action *= ( CMAP_2 )
)

FilteringRule Filter_nil_acl
(
    LocalIPFilter *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    NetworkInterfaces *= "eth0"
    Action *= ( PASS )
)

FilteringRule Filter_nil_acl_1
(
    LocalIPFilter *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
```

```
    PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    NetworkInterfaces *= "eth1"
    Action *= ( PASS )
)
```

Текст cisco-like конфигурации для GW2

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity address
username cscons privilege 15 password 0 csp
hostname GW2
enable password csp
!
!
!
logging trap debugging
!
!
crypto isakmp policy 1
 hash md5
 encr des
 authentication pre-share
 group 5
!
crypto isakmp key 123456 address 192.168.4.3
!
crypto ipsec transform-set TS1 esp-des esp-md5-hmac
!
ip access-list extended LAN2toLAN3
 permit ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
!
ip access-list extended LAN2toLAN1
 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
!
!
crypto map CMAP 1 ipsec-isakmp
 match address LAN2toLAN3
 set transform-set TS1
 set pfs group5
 set peer 192.168.4.3
!
crypto map CMAP 2 ipsec-isakmp
 match address LAN2toLAN1
 set transform-set TS1
 set pfs group5
 set peer 192.168.4.3
!
!
!
interface FastEthernet0/0
 ip address 192.168.4.2 255.255.255.0
 crypto map CMAP
!
interface FastEthernet0/1
 ip address 192.168.2.254 255.255.255.0
!
!
ip route 192.168.1.0 255.255.255.0 192.168.4.3
ip route 192.168.3.0 255.255.255.0 192.168.4.3
!
end
```

Текст LSP для GW2

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Sun Apr 13 03:30:18 2014

GlobalParameters(
    Title                       = "This LSP was automatically generated by CSP
Converter at Sun Apr 13 03:30:18 2014"
    Version                     = "2.1"
    LDAPLogMessageLevel         = DEBUG
    SystemLogMessageLevel       = DEBUG
    PolicyLogMessageLevel       = DEBUG
    CertificatesLogMessageLevel = DEBUG
)

SyslogSettings(
    Server = 127.0.0.1
    Facility = LOG_LOCAL7
)

RoutingTable(
    Routes *=
        Route(
            Destination = 192.168.1.0/24
            Gateway = 192.168.4.3
            Metric = 1
        ),
        Route(
            Destination = 192.168.3.0/24
            Gateway = 192.168.4.3
            Metric = 1
        )
)
IKETransform IKETransform_1
(
    CipherAlg   *= "G2814789CPRO1-K256-CBC-65530"
    HashAlg     *= "STB1176199-65530"
    GroupID     *= MODP_1536
    LifetimeSeconds = 86400
)

ESPProposal ESP_TS1
(
    Transform* = ESPTransform
    (
        IntegrityAlg*       = "G2814789AV1-K256-MAC-65531"
        CipherAlg*          = "G2814789CPRO1-K256-CBC-250"
        LifetimeSeconds    = 3600
        LifetimeKilobytes   = 4608000
    )
)

ESPProposal ESP_TS1_1
(
    Transform* = ESPTransform
    (
        IntegrityAlg*       = "G2814789AV1-K256-MAC-65531"
        CipherAlg*          = "G2814789CPRO1-K256-CBC-250"
        LifetimeSeconds    = 3600
        LifetimeKilobytes   = 4608000
    )
)

AuthMethodPreshared IKE_auth_cs_key_192_168_4_3
(
    RemoteID = IdentityEntry(
        IPv4Address *= 192.168.4.3
    )
    SharedIKESecret = "cs_key_192_168_4_3"
)

IKERule IKE_CMAP_1
```

```
(
    Transform* = IKETransform_1
    AggrModeAuthMethod  *= IKE_auth_cs_key_192_168_4_3
    MainModeAuthMethod  *= IKE_auth_cs_key_192_168_4_3
    DoAutopass          = TRUE
    DoNotUseDPD         = TRUE
)

IPsecAction CMAP_1
(
    TunnelingParameters *= TunnelEntry(
        PeerIPAddress = 192.168.4.3

        DFHandling=COPY
    )
    ContainedProposals *= ( ESP_TS1 )
    GroupID *= MODP_1536
    IKERule = IKE_CMAP_1
)

AuthMethodPreshared IKE_auth_cs_key_192_168_4_3_1
(
    RemoteID = IdentityEntry(
        IPv4Address *= 192.168.4.3
    )
    SharedIKESecret = "cs_key_192_168_4_3"
)

IKERule IKE_CMAP_2
(
    Transform* = IKETransform_1
    AggrModeAuthMethod  *= IKE_auth_cs_key_192_168_4_3_1
    MainModeAuthMethod  *= IKE_auth_cs_key_192_168_4_3_1
    DoAutopass          = TRUE
    DoNotUseDPD         = TRUE
)

IPsecAction CMAP_2
(
    TunnelingParameters *= TunnelEntry(
        PeerIPAddress = 192.168.4.3

        DFHandling=COPY
    )
    ContainedProposals *= ( ESP_TS1_1 )
    GroupID *= MODP_1536
    IKERule = IKE_CMAP_2
)

FilteringRule Filter_nil_acl_CMAP_1
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.2.0/24 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.3.0/24 )
    NetworkInterfaces *= "eth0"
    Action *= ( CMAP_1 )
)

FilteringRule Filter_nil_acl_CMAP_2
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.2.0/24 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.1.0/24 )
    NetworkInterfaces *= "eth0"
    Action *= ( CMAP_2 )
)

FilteringRule Filter_nil_acl
(
    LocalIPFilter *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    NetworkInterfaces *= "eth0"
    Action *= ( PASS )
```

```
)

FilteringRule Filter_nil_acl_1
(
    LocalIPFilter *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    NetworkInterfaces *= "eth1"
    Action *= ( PASS )
)
```

Текст cisco-like конфигурации для GW3

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity address
username cscons privilege 15 password 0 csp
hostname GW3
enable password csp
!
!
!
logging trap debugging
!
!
crypto isakmp policy 1
 hash md5
 encr des
 authentication pre-share
 group 5
!
crypto isakmp key 12345 address 192.168.4.1
!
crypto isakmp key 123456 address 192.168.4.2
!
crypto ipsec transform-set TS1 esp-des esp-md5-hmac
!
ip access-list extended LAN3toLAN2
 permit ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
!
ip access-list extended LAN3toLAN1
 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
!
ip access-list extended LAN1toLAN2
 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
!
ip access-list extended LAN2toLAN1
 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
!
!
crypto map CMAP 1 ipsec-isakmp
 match address LAN3toLAN2
 set transform-set TS1
 set pfs group5
 set peer 192.168.4.2
!
crypto map CMAP 2 ipsec-isakmp
 match address LAN3toLAN1
 set transform-set TS1
 set pfs group5
 set peer 192.168.4.1
!
crypto map CMAP 3 ipsec-isakmp
 match address LAN1toLAN2
 set transform-set TS1
 set pfs group5
 set peer 192.168.4.2
```

```
!
crypto map CMAP 4 ipsec-isakmp
 match address LAN2toLAN1
 set transform-set TS1
 set pfs group5
 set peer 192.168.4.1
!
!
!
interface FastEthernet0/0
 ip address 192.168.4.3 255.255.255.0
 crypto map CMAP
!
interface FastEthernet0/1
 ip address 192.168.3.254 255.255.255.0
!
!
ip route 192.168.1.0 255.255.255.0 192.168.4.1
ip route 192.168.2.0 255.255.255.0 192.168.4.2
!
end


.255.0 10.0.177.3 1
```

Текст LSP для GW3

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Wed Apr 16 03:51:11 2014

GlobalParameters(
    Title                       = "This LSP was automatically generated by CSP
Converter at Wed Apr 16 03:51:11 2014"
    Version                     = "2.1"
    LDAPLogMessageLevel         = DEBUG
    SystemLogMessageLevel       = DEBUG
    PolicyLogMessageLevel       = DEBUG
    CertificatesLogMessageLevel = DEBUG
)

SyslogSettings(
    Server = 127.0.0.1
    Facility = LOG_LOCAL7
)

RoutingTable(
    Routes *=
        Route(
            Destination = 192.168.1.0/24
            Gateway = 192.168.4.1
            Metric = 1
        ),
        Route(
            Destination = 192.168.2.0/24
            Gateway = 192.168.4.2
            Metric = 1
        )
)
IKETransform IKETransform_1
(
    CipherAlg   *= "G2814789CPRO1-K256-CBC-65530"
    HashAlg     *= "STB1176199-65530"
    GroupID     *= MODP_1536
    LifetimeSeconds = 86400
)

ESPProposal ESP_TS1
```

```
(
    Transform* = ESPTransform
    (
        IntegrityAlg*       = "G2814789AV1-K256-MAC-65531"
        CipherAlg*          = "G2814789CPRO1-K256-CBC-250"
        LifetimeSeconds    = 3600
        LifetimeKilobytes   = 4608000
    )
)

ESPProposal ESP_TS1_1
(
    Transform* = ESPTransform
    (
        IntegrityAlg*       = "G2814789AV1-K256-MAC-65531"
        CipherAlg*          = "G2814789CPRO1-K256-CBC-250"
        LifetimeSeconds    = 3600
        LifetimeKilobytes   = 4608000
    )
)

ESPProposal ESP_TS1_2
(
    Transform* = ESPTransform
    (
        IntegrityAlg*       = "G2814789AV1-K256-MAC-65531"
        CipherAlg*          = "G2814789CPRO1-K256-CBC-250"
        LifetimeSeconds    = 3600
        LifetimeKilobytes   = 4608000
    )
)

ESPProposal ESP_TS1_3
(
    Transform* = ESPTransform
    (
        IntegrityAlg*       = "G2814789AV1-K256-MAC-65531"
        CipherAlg*          = "G2814789CPRO1-K256-CBC-250"
        LifetimeSeconds    = 3600
        LifetimeKilobytes   = 4608000
    )
)

AuthMethodPreshared IKE_auth_cs_key_192_168_4_2
(
    RemoteID = IdentityEntry(
        IPv4Address *= 192.168.4.2
    )
    SharedIKESecret = "cs_key_192_168_4_2"
)

IKERule IKE_CMAP_1
(
    Transform* = IKETransform_1
    AggrModeAuthMethod  *= IKE_auth_cs_key_192_168_4_2
    MainModeAuthMethod  *= IKE_auth_cs_key_192_168_4_2
    DoAutopass          = TRUE
    DoNotUseDPD         = TRUE
)

IPsecAction CMAP_1
(
    TunnelingParameters *= TunnelEntry(
        PeerIPAddress = 192.168.4.2

        DFHandling=COPY
    )
    ContainedProposals *= ( ESP_TS1 )
    GroupID *= MODP_1536
    IKERule = IKE_CMAP_1
)
```

```
AuthMethodPreshared IKE_auth_cs_key_192_168_4_1
(
    RemoteID = IdentityEntry(
        IPv4Address *= 192.168.4.1
    )
    SharedIKESecret = "cs_key_192_168_4_1"
)

IKERule IKE_CMAP_2
(
    Transform* = IKETransform_1
    AggrModeAuthMethod  *= IKE_auth_cs_key_192_168_4_1
    MainModeAuthMethod  *= IKE_auth_cs_key_192_168_4_1
    DoAutopass          = TRUE
    DoNotUseDPD         = TRUE
)

IPsecAction CMAP_2
(
    TunnelingParameters *= TunnelEntry(
        PeerIPAddress = 192.168.4.1

        DFHandling=COPY
    )
    ContainedProposals *= ( ESP_TS1_1 )
    GroupID *= MODP_1536
    IKERule = IKE_CMAP_2
)

AuthMethodPreshared IKE_auth_cs_key_192_168_4_2_1
(
    RemoteID = IdentityEntry(
        IPv4Address *= 192.168.4.2
    )
    SharedIKESecret = "cs_key_192_168_4_2"
)

IKERule IKE_CMAP_3
(
    Transform* = IKETransform_1
    AggrModeAuthMethod  *= IKE_auth_cs_key_192_168_4_2_1
    MainModeAuthMethod  *= IKE_auth_cs_key_192_168_4_2_1
    DoAutopass          = TRUE
    DoNotUseDPD         = TRUE
)

IPsecAction CMAP_3
(
    TunnelingParameters *= TunnelEntry(
        PeerIPAddress = 192.168.4.2

        DFHandling=COPY
    )
    ContainedProposals *= ( ESP_TS1_2 )
    GroupID *= MODP_1536
    IKERule = IKE_CMAP_3
)

AuthMethodPreshared IKE_auth_cs_key_192_168_4_1_1
(
    RemoteID = IdentityEntry(
        IPv4Address *= 192.168.4.1
    )
    SharedIKESecret = "cs_key_192_168_4_1"
)

IKERule IKE_CMAP_4
(
    Transform* = IKETransform_1
    AggrModeAuthMethod  *= IKE_auth_cs_key_192_168_4_1_1
```

```
    MainModeAuthMethod  *= IKE_auth_cs_key_192_168_4_1_1
    DoAutopass          = TRUE
    DoNotUseDPD         = TRUE
)

IPsecAction CMAP_4
(
    TunnelingParameters *= TunnelEntry(
        PeerIPAddress = 192.168.4.1

        DFHandling=COPY
    )
    ContainedProposals *= ( ESP_TS1_3 )
    GroupID *= MODP_1536
    IKERule = IKE_CMAP_4
)

FilteringRule Filter_nil_acl_CMAP_1
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.3.0/24 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.2.0/24 )
    NetworkInterfaces *= "eth0"
    Action *= ( CMAP_1 )
)

FilteringRule Filter_nil_acl_CMAP_2
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.3.0/24 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.1.0/24 )
    NetworkInterfaces *= "eth0"
    Action *= ( CMAP_2 )
)

FilteringRule Filter_nil_acl_CMAP_3
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.1.0/24 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.2.0/24 )
    NetworkInterfaces *= "eth0"
    Action *= ( CMAP_3 )
)

FilteringRule Filter_nil_acl_CMAP_4
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.2.0/24 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.1.0/24 )
    NetworkInterfaces *= "eth0"
    Action *= ( CMAP_4 )
)

FilteringRule Filter_nil_acl
(
    LocalIPFilter *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    NetworkInterfaces *= "eth0"
    Action *= ( PASS )
)

FilteringRule Filter_nil_acl_1
(
    LocalIPFilter *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    NetworkInterfaces *= "eth1"
    Action *= ( PASS )
)
```