

Построение защищенной сети передачи данных в топологии «звезда» с резервированием шлюзов безопасности, с использованием технологии DMVPN

Описание стенда

Сценарий описывает построение защищенной сети передачи данных в топологии звезда с резервированием шлюзов безопасности. Использование технологии DMVPN (Dynamic Multipoint VPN) позволяет динамически подключать новые сети (филиалы) без перенастройки оборудования центрального офиса.

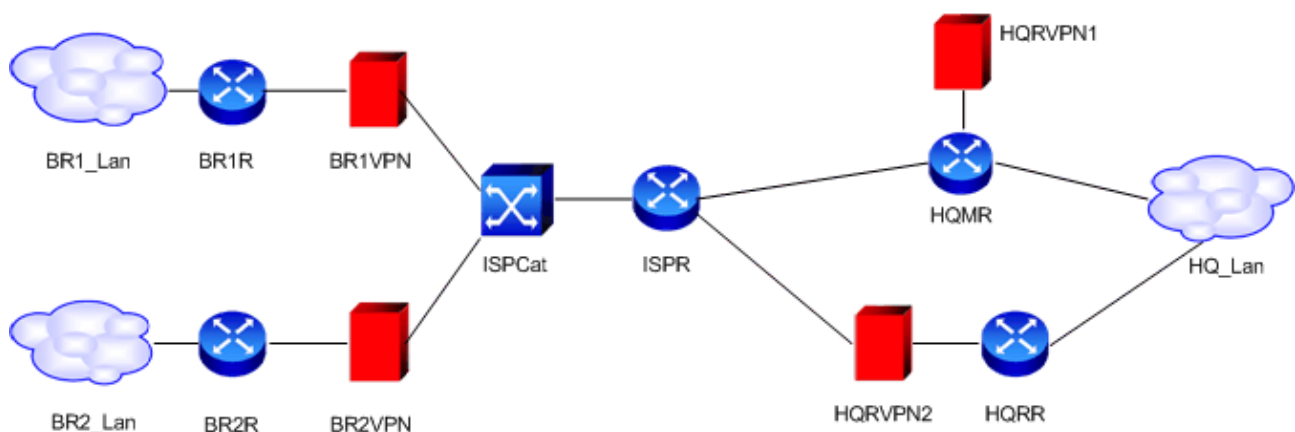


Рисунок 1

Адресация

BR1

Object	Address
BR1_Lan	192.168.1.0/24
BR1R_FA1/0	192.168.1.1/24
BR1R_FA1/1	192.168.11.1/30
BR1VPN_FA0/0	192.168.11.2/30
BR1VPN_FA0/1	10.0.0.2/29

ISP

Object	Address
ISPR_FA1/0.x	10.0.0.1/29
ISPR_FA1/0.y	10.0.1.1/30
ISPR_FA1/0.z	10.0.2.1/30

Loopbacks

Object	Address
BR1R_Lo0	192.168.250.1/32
BR2R_Lo0	192.168.250.2/32
HQMR_Lo0	192.168.250.3/32
HQRR_Lo0	192.168.250.4/32

BR2

Object	Address
BR2_Lan	192.168.2.0/24
BR2R_FA1/0	192.168.2.1/24
BR2R_FA1/1	192.168.22.1/30
BR2VPN_FA0/0	192.168.22.2/30
BR2VPN_FA0/1	10.0.0.3/29

HQ

Object	Address
HQ_Lan	192.168.0.0/24
HQMR_FA0/0	192.168.0.1/24
HQMR_FA0/1	10.0.1.2/30
HQMR_SPE1/0	192.168.33.1/30
HQRVPN1_FA0/0	192.168.33.2/30
HQRR_FA0/0	192.168.0.2/24
HQRR_SPE1/0	192.168.44.1/30
HQRVPN2_FA0/0	192.168.44.2/30
HQRVPN2_FA0/1	10.0.2.2/30

NAT: HQMR_FA0/1 UDP 500 & 4500 -> HQRVPN1 UDP 500 & 4500

mGRE Scenario1

Object	Address
HQMR_Tun0	11.0.0.1/29
HQRR_Tun0	11.0.0.2/29
BR1R_Tun0	11.0.0.3/29
BR2R_Tun0	11.0.0.4/29

mGRE Scenario2

Object	Address
HQMR_Tun0	11.0.0.1/29
HQRR_Tun0	11.0.0.9/29
BR1R_Tun0	11.0.0.2/29
BR1R_Tun1	11.0.0.10/29
BR2R_Tun0	11.0.0.3/29
BR2R_Tun1	11.0.0.11/29

В стенде представлены два варианта размещения шлюзов безопасности S-Terra VPN Gate:

- inline – BR1VPN, BR2VPN, HQRVPN2
- on-stick – HQRVPN1.

На маршрутизаторах Cisco: BR1R, BR2R, HQMR, HQRR настроен DMVPN в режиме без защиты туннелей (without tunnel protection). Сетевые взаимодействия сетей филиалов BR1_Lan, BR2_Lan и сети головного офиса HQ_Lan происходят внутри туннелей, поднятых в рамках DMVPN. Шифрование туннелированного трафика осуществляется на шлюзах безопасности семейства CSP VPN Gate с использованием криптоалгоритмов ГОСТ. Взаимная аутентификация шлюзов безопасности осуществляется на predetermined ключах (preshared-key).

В предложенной схеме используется NAT (на устройстве HQMR). Использование NAT не является необходимым для построения данного сценария и введено с целью демонстрации возможности работы данного решения в сетях, где используется NAT-преобразование трафика.

Резервирование шлюзов безопасности (каналов связи) в центральном офисе организовано за счет использования двух маршрутизаторов – основного (HQMR – HQ Main Router) и резервного (HQRR – HQ Reserve Router). По умолчанию весь трафик из удаленных офисов проходит через HQMR. В случае выхода из строя HQMR, трафик автоматически перенаправляется через HQRR.

Рассмотрим два варианта сценария, в обоих случаях будет использоваться топология «звезда»:

1. Обмен данными возможен только между центральным офисом и филиалами. Защита сетевого трафика между филиалами не предусматривается, сетевые взаимодействия между филиалами должны быть запрещены политиками безопасности.
2. Обмен данными возможен как между головным офисом и филиалом, так и между филиалами с перешифрацией трафика в головном офисе. В каждом из филиалов настроено по две DMVPN сети – одна с HQMR и одна с HQRR.

Сценарий 1

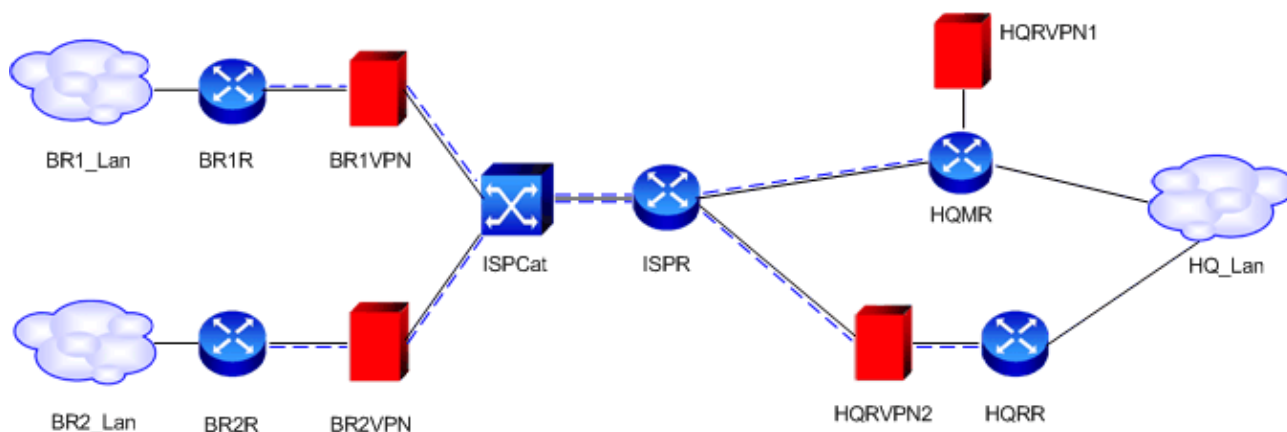


Рисунок 2

Синей пунктирной линией показана DMVPN сеть.

Маршрутизация между центральным и удаленными офисами осуществляется с помощью протокола OSPF.

Настройка DMVPN туннеля на маршрутизаторе HQMR

Создадим туннельный интерфейс: interface Tunnel0.

Для того, чтобы HQMR был более предпочтителен для протоколов динамической маршрутизации, выставим следующее значение для bandwidth:

```
bandwidth 1000
```

Зададим IP адрес туннельному интерфейсу:

```
ip address 11.0.0.1 255.255.255.248
```

Для предотвращения фрагментации на VPN шлюзах, зададим максимальное значение MTU на туннельном интерфейсе:

```
ip mtu 1400
```

Для того, чтобы HUB автоматически добавлял адреса Spoke маршрутизаторов для рассылки multicast-пакетов:

```
ip nhrp map multicast dynamic
```

Зададим nhrp network-id:

```
ip nhrp network-id 1000
```

Зададим параметр holdtime для nhrp. Параметр показывает, как часто Spoke маршрутизатор будет регистрироваться на HUB маршрутизаторе:

```
ip nhrp holdtime 60
```

Для работы OSPF через туннельный интерфейс зададим network type – broadcast:

```
ip ospf network broadcast
```

Для того, чтобы HQMR был DR зададим ospf priority:

```
ip ospf priority 20
```

В качестве адреса туннельного интерфейса будем использовать loopback интерфейс:

```
tunnel source Loopback0
```

Сделаем данный интерфейс mGRE интерфейсом:

```
tunnel mode gre multipoint
```

Для работы VPN шлюза через NAT, настроим статическую трансляцию udp портов 500 и 4500 с внешнего адреса устройства HQMR на адрес HQRVPN1:

```
ip nat inside source static udp 192.168.33.2 500 10.0.1.2 500 extendable
```

```
ip nat inside source static udp 192.168.33.2 4500 10.0.1.2 4500 extendable
```

Зададим статический маршрут, показывающий, что адреса туннельных интерфейсов партнерских шлюзов доступны через адрес RVPN модуля:

```
ip route 192.168.250.0 255.255.255.0 192.168.33.2
```

Настройка шлюза HQRVPN1

Так как адреса партнерских шлюзов заранее неизвестны, то для шифруемого трафика в access-list в destination указываем any:

```
ip access-list extended GRE_HQMR_TO_ANY
  permit gre host 192.168.250.3 any
```

Создаем динамическую криптокарту, так как адреса партнеров также заранее неизвестны:

```
!
crypto dynamic-map FA00_DMAP 10
  match address GRE_HQMR_TO_ANY
  set transform-set ESP_GOST_CI
  set pfs group5
!
crypto map FA00_CMAP 10 ipsec-isakmp dynamic FA00_DMAP
```

Полные тексты конфигурации устройств HQMR и HQRVPN1 доступны в конце описания данного сценария.

Настройка устройства HQRR

Так как данный маршрутизатор является резервным, то он является HUB для всех Spoke маршрутизаторов, а так же Spoke для маршрутизатора HQMR.

```
interface Tunnel0
  description ### HQ RESERVE DMVPN HUB ###

  bandwidth 900

  ip address 11.0.0.2 255.255.255.248
  no ip redirects
  ip mtu 1400
  ip nhrp map multicast dynamic
```

Так как данный маршрутизатор является Spoke для HQMR, то зададим маппирование туннельного адреса маршрутизатора HQMR к его физическому:

```
ip nhrp map 11.0.0.1 192.168.250.3
```

Для того, чтобы multicast-пакеты явно отсылались на физический адрес маршрутизатора HQMR:

```
ip nhrp map multicast 192.168.250.3
```

```
ip nhrp network-id 1000
ip nhrp holdtime 60
```

Зададим адрес next hop resolution protocol server – туннельный адрес маршрутизатора HQMR:

```
ip nhrp nhs 11.0.0.1
```

```
ip ospf network broadcast
```

Для того, чтобы маршрутизатор HQRR был BDR – зададим его priority:

```
ip ospf priority 10
```

```
tunnel source Loopback0
tunnel mode gre multipoint
!
```

Настройка шлюза HQRVPN2

Так как мы знаем адрес маршрутизатора HQMR, то access-list описывающий трафик, который необходимо шифровать между HQRR и HQMR, будет выглядеть следующим образом:

```
!
ip access-list extended GRE_HQRR_TO_HQMR
 permit gre host 192.168.250.4 host 192.168.250.3
!
```

В отличие от адреса маршрутизатора HQMR, адреса Spoke шлюзов заранее неизвестны – поэтому destination – any:

```
ip access-list extended GRE_HQRR_TO_ANY
 permit gre host 192.168.250.4 any
!
```

Так как адреса Spoke роутеров неизвестны заранее – для шифрования трафика будет использоваться динамическая криптокарта:

```
crypto dynamic-map FA01_DMAP 10
 match address GRE_HQRR_TO_ANY
 set transform-set ESP_GOST_CI
 set pfs group5
!
```

Для шифрования трафика между HQRR и HQMR используется статическая криптокарта:

```
crypto map FA01_CMAP 10 ipsec-isakmp
 match address GRE_HQRR_TO_HQMR
 set transform-set ESP_GOST_CI
 set pfs group5
```

```
set peer 10.0.1.2
!  
crypto map FA01_CMAP 20 ipsec-isakmp dynamic FA01_DMAP
```

Полные тексты конфигурации устройств HQRR и HQVPN2 доступны в конце описания данного сценария.

Настройка устройства BR1R

Данный маршрутизатор является Spoke как для маршрутизатора HQMR, так и для маршрутизатора HQRR. Поэтому настройки туннельного интерфейса аналогичны настройкам, относящимся к Spoke части устройства HQRR за исключением того, что:

- у данного шлюза два HUB маршрутизатора
- данный шлюз никогда не должен быть DR или BDR – поэтому ospf priority выставлена в 0.

```
interface Tunnel0  
description ### BRANCH1 DMVPN INTF ###  
ip address 11.0.0.3 255.255.255.248  
no ip redirects  
ip mtu 1400  
ip nhrp map 11.0.0.1 192.168.250.3  
ip nhrp map 11.0.0.2 192.168.250.4  
ip nhrp map multicast 192.168.250.3  
ip nhrp map multicast 192.168.250.4  
ip nhrp network-id 1000  
ip nhrp holdtime 60  
ip nhrp nhs 11.0.0.1  
ip nhrp nhs 11.0.0.2  
ip ospf network broadcast  
ip ospf priority 0  
tunnel source Loopback0  
tunnel mode gre multipoint  
!
```

Настройка устройства BR1VPN

Так как адреса HUB маршрутизаторов известны заранее, то в access list они явно указываются и используются статические криптокарты:

```

ip access-list extended GRE_BR1R_TO_HQRR
  permit gre host 192.168.250.1 host 192.168.250.4
!
ip access-list extended GRE_BR1R_TO_HQMR
  permit gre host 192.168.250.1 host 192.168.250.3
!
!
crypto map FA01_CMAP 10 ipsec-isakmp
  match address GRE_BR1R_TO_HQMR
  set transform-set ESP_GOST_CI
  set pfs group5
  set peer 10.0.1.2
!
crypto map FA01_CMAP 20 ipsec-isakmp
  match address GRE_BR1R_TO_HQRR
  set transform-set ESP_GOST_CI
  set pfs group5
  set peer 10.0.2.2
!

```

Важно: в случае, если один из Spoke маршрутизаторов (например, BR1VPN) попытается послать что-либо в сеть, защищаемую другим Spoke маршрутизатором, то пакет, придя на устройство BR1VPN и (так как адресом назначения для данного GRE пакета будет физический адрес другого Spoke) не попадая под какое-либо правило шифрования, уйдет с устройства BR1VPN в открытом виде. Избежать этого можно, например, повесив access-list на интерфейсе устройства BR1R, разрешающий прохождение GRE пакетов только на адреса устройств HQMR и HQRR.

Полные тексты конфигурации устройств BR1R и BR1VPN доступны в конце описания данного сценария.

Устройства BR2R и BR2VPN настраиваются аналогично устройствам BR1R и BR1VPN. Текст их конфигурации так же доступен в конце описания данного сценария.

Проверка отказоустойчивости (на примере BR1)

Для проверки отказоустойчивости данного решения проведем следующие действия.

В штатном случае весь трафик от BR1_Lan в HQ_Lan проходит через устройство HQMR:

```

BR1R#show ip route 192.168.0.0 255.255.255.0
Routing entry for 192.168.0.0/24
  Known via "ospf 10", distance 110, metric 1001, type inter area
  Last update from 11.0.0.1 on Tunnel0, 00:29:18 ago
Routing Descriptor Blocks:

```

```
* 11.0.0.1, from 192.168.250.3, 00:29:18 ago, via Tunnel0
  Route metric is 1001, traffic share count is 1
```

Отключим внешний интерфейс (интерфейс fa0/1) на данном устройстве и проверим за какое время маршрут на устройстве BR1R в сеть HQ_Lan переключится на устройство HQRR (вывод команды show clock сделан практически одновременно с командой shut на интерфейсе fa0/1 устройства HQMR). Проверять время переключения будем по timestampам вывода debug ip route. (время должно быть около 40сек – значение по умолчанию dead timerа ospf).

```
BR1R#show clock
13:41:19.807 UTC Thu Jul 2 2009
BR1R#
Jul  2 13:41:22.507: RT: NET-RED 0.0.0.0/0
BR1R#
Jul  2 13:41:56.191: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.250.3 on
Tunnel0 from FULL to DOWN, Neighbor Down: Dead timer expired
BR1R#
Jul  2 13:42:01.699: RT: del 192.168.0.0/24 via 11.0.0.1, ospf metric
[110/1001]
Jul  2 13:42:01.699: RT: add 192.168.0.0/24 via 11.0.0.2, ospf metric
[110/1010]
Jul  2 13:42:01.699: RT: NET-RED 192.168.0.0/24
```

Как видно, маршрут успешно переключился на устройство HQRR:

```
BR1R#show ip route 192.168.0.0 255.255.255.0
Routing entry for 192.168.0.0/24
  Known via "ospf 10", distance 110, metric 1010, type inter area
  Last update from 11.0.0.2 on Tunnel0, 00:00:11 ago
  Routing Descriptor Blocks:
    * 11.0.0.2, from 192.168.250.4, 00:00:11 ago, via Tunnel0
      Route metric is 1010, traffic share count is 1

BR1R#ping 192.168.0.
Jul  2 13:42:22.507: RT: NET-RED 0.0.0.0/0
BR1R#ping 192.168.0.1 source 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/10/16 ms
```

```
BR1R#
```

Теперь вновь включим интерфейс fa0/1 на устройстве HQMR – маршрут вновь должен переключиться на него:

```
Jul  2 13:44:22.511: RT: NET-RED 0.0.0.0/0
Jul  2 13:44:22.803: RT: del 192.168.0.0/24 via 11.0.0.2, ospf metric
[110/1010]
Jul  2 13:44:22.803: RT: add 192.168.0.0/24 via 11.0.0.1, ospf metric
[110/1001]
Jul  2 13:44:22.803: RT: NET-RED 192.168.0.0/24
BR1R#show ip route 192.168.0.0 255.255.255.0
Routing entry for 192.168.0.0/24
  Known via "ospf 10", distance 110, metric 1001, type inter area
  Last update from 11.0.0.1 on Tunnel0, 00:00:06 ago
  Routing Descriptor Blocks:
  * 11.0.0.1, from 192.168.250.3, 00:00:06 ago, via Tunnel0
    Route metric is 1001, traffic share count is 1
```

Вывод таблицы маршрутизации с устройства ISP:

```
ISP#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.0.2.0/30 is directly connected, FastEthernet1/0.45
C       10.0.0.0/29 is directly connected, FastEthernet1/0.43
C       10.0.1.0/30 is directly connected, FastEthernet1/0.44
ISP#
```

Вывод таблицы маршрутизации, DMVPN-related информации, а также статистики IPsec соединения с устройств в головном и удаленных офисах

HQMR и HQRVPN1

```
HQMR#show dmvpn
```

```
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding
        UpDn Time --> Up or Down Time for a Tunnel
```

```
=====
```

```
Interface: Tunnel0, IPv4 NHRP Details
```

```
Type:Hub, NHRP Peers:3,
```

# Ent	Peer NBMA Addr	Peer Tunnel Add	State	UpDn Tm	Attrb
1	192.168.250.4	11.0.0.2	UP	00:19:12	D
1	192.168.250.1	11.0.0.3	UP	00:11:24	D
1	192.168.250.2	11.0.0.4	UP	00:18:01	D

```
HQMR#show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static
route
        o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is 10.0.1.1 to network 0.0.0.0
```

```
192.168.250.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.250.3/32 is directly connected, Loopback0
S    192.168.250.0/24 [1/0] via 192.168.33.2
10.0.0.0/30 is subnetted, 1 subnets
C    10.0.1.0 is directly connected, FastEthernet0/1
```

```
11.0.0.0/29 is subnetted, 1 subnets
C    11.0.0.0 is directly connected, Tunnel0
C    192.168.0.0/24 is directly connected, FastEthernet0/0
O    192.168.1.0/24 [110/101] via 11.0.0.3, 00:11:22, Tunnel0
O    192.168.2.0/24 [110/101] via 11.0.0.4, 00:17:58, Tunnel0
    192.168.33.0/30 is subnetted, 1 subnets
C    192.168.33.0 is directly connected, Special-Services-Engine1/0
S*   0.0.0.0/0 [1/0] via 10.0.1.1
HQMR#show ip nhrp
11.0.0.2/32 via 11.0.0.2
    Tunnel0 created 00:22:11, expire 00:00:59
    Type: dynamic, Flags: unique registered used
    NBMA address: 192.168.250.4
11.0.0.3/32 via 11.0.0.3
    Tunnel0 created 00:12:03, expire 00:00:47
    Type: dynamic, Flags: unique registered
    NBMA address: 192.168.250.1
11.0.0.4/32 via 11.0.0.4
    Tunnel0 created 00:19:02, expire 00:00:50
    Type: dynamic, Flags: unique registered used
    NBMA address: 192.168.250.2
HQMR#

HQRVPN1:~# sa_show -e
IKE sessions: 0 initiated, 0 responded

ISAKMP SA Num (Remote Addr,Port)-(Local Addr,Port) State Sent Rec
ISAKMP SA 1 (10.0.0.3,4500)-(192.168.33.2,4500) ready 1160 1084
ISAKMP SA 2 (10.0.0.2,4500)-(192.168.33.2,4500) ready 1160 1084
ISAKMP SA 3 (10.0.2.2,4500)-(192.168.33.2,4500) ready 1128 1116

IPSec SA Num (Remote Addr,Port)-(Local Addr,Port) Protocol Action Type
Sent Rec
IPSec SA 1 30 (192.168.250.2,*)-(192.168.250.3,*) 47 ESP tunn 6096 8696
IPSec SA 2 31 (192.168.250.1,*)-(192.168.250.3,*) 47 ESP tunn 6256 9048
IPSec SA 3 32 (192.168.250.4,*)-(192.168.250.3,*) 47 ESP tunn 5264 7744
HQRVPN1:~#
```

HQRR u HQRVPN2

```

HQRVPN2:~# sa_show -e
IKE sessions: 0 initiated, 0 responded

ISAKMP SA Num (Remote Addr,Port)-(Local Addr,Port) State Sent Rec
ISAKMP SA 1 (10.0.0.2,500)-(10.0.2.2,500) ready 1160 1084
ISAKMP SA 2 (10.0.1.2,4500)-(10.0.2.2,4500) ready 1184 672
ISAKMP SA 3 (10.0.0.3,500)-(10.0.2.2,500) ready 1160 1084

IPSec SA Num (Remote Addr,Port)-(Local Addr,Port) Protocol Action Type
Sent Rec
IPSec SA 1 31 (192.168.250.3,*)-(192.168.250.4,*) 47 ESP tunn 8608 13952
IPSec SA 2 32 (192.168.250.1,*)-(192.168.250.4,*) 47 ESP tunn 9224 12520
IPSec SA 3 33 (192.168.250.2,*)-(192.168.250.4,*) 47 ESP tunn 9224 12520
HQRVPN2:~#

HQRR#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.44.2 to network 0.0.0.0

    192.168.44.0/30 is subnetted, 1 subnets
C      192.168.44.0 is directly connected, Special-Services-Engine1/0
    192.168.250.0/32 is subnetted, 1 subnets
C      192.168.250.4 is directly connected, Loopback0
    11.0.0.0/29 is subnetted, 1 subnets
C      11.0.0.0 is directly connected, Tunnel0
C      192.168.0.0/24 is directly connected, FastEthernet0/0
O      192.168.1.0/24 [110/112] via 11.0.0.3, 00:16:27, Tunnel0
O      192.168.2.0/24 [110/112] via 11.0.0.4, 00:23:01, Tunnel0
S*    0.0.0.0/0 [1/0] via 192.168.44.2
HQRR#

```

BR1R u BR1VPN

```

BR1VPN:~# sa_show -e
IKE sessions: 0 initiated, 0 responded

ISAKMP SA Num (Remote Addr,Port)-(Local Addr,Port) State Sent Rec
ISAKMP SA 1 (10.0.1.2,4500)-(10.0.0.2,4500) ready 1152 672
ISAKMP SA 2 (10.0.2.2,500)-(10.0.0.2,500) ready 1152 672

IPSec SA Num (Remote Addr,Port)-(Local Addr,Port) Protocol Action Type
Sent Rec
IPSec SA 1 8 (192.168.250.3,*)-(192.168.250.1,*) 47 ESP tunn 15264 25368
IPSec SA 2 9 (192.168.250.4,*)-(192.168.250.1,*) 47 ESP tunn 14484 22848
BR1VPN:~#

BR1R#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.11.2 to network 0.0.0.0

    192.168.11.0/30 is subnetted, 1 subnets
C      192.168.11.0 is directly connected, FastEthernet1/1
    192.168.250.0/32 is subnetted, 1 subnets
C      192.168.250.1 is directly connected, Loopback0
    11.0.0.0/29 is subnetted, 1 subnets
C      11.0.0.0 is directly connected, Tunnel0
O IA 192.168.0.0/24 [110/1001] via 11.0.0.1, 00:22:20, Tunnel0
C    192.168.1.0/24 is directly connected, FastEthernet1/0
O    192.168.2.0/24 [110/1001] via 11.0.0.4, 00:22:20, Tunnel0
S*   0.0.0.0/0 [1/0] via 192.168.11.2
BR1R#show dmvpn

```

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
 N - NATed, L - Local, X - No Socket
 # Ent --> Number of NHRP entries with same NBMA peer
 NHS Status: E --> Expecting Replies, R --> Responding
 UpDn Time --> Up or Down Time for a Tunnel

Interface: Tunnel0, IPv4 NHRP Details

Type:Spoke, NHRP Peers:2,

```

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
-----
      1   192.168.250.3      11.0.0.1   UP 00:22:32   S
      1   192.168.250.4      11.0.0.2   UP 00:22:33   S

```

BR1R#show ip nhrp

```

11.0.0.1/32 via 11.0.0.1
  Tunnel0 created 00:22:36, never expire
  Type: static, Flags: used
  NBMA address: 192.168.250.3
11.0.0.2/32 via 11.0.0.2
  Tunnel0 created 00:22:36, never expire
  Type: static, Flags: used
  NBMA address: 192.168.250.4

```

BR1R#

BR2R u BR2VPN

BR2VPN:~# sa_show -e

IKE sessions: 0 initiated, 0 responded

```

ISAKMP SA Num (Remote Addr,Port)-(Local Addr,Port) State Sent Rec
ISAKMP SA 1 (10.0.1.2,4500)-(10.0.0.3,4500) ready 1152 672
ISAKMP SA 2 (10.0.2.2,500)-(10.0.0.3,500) ready 1152 672

```

```

IPSec SA Num (Remote Addr,Port)-(Local Addr,Port) Protocol Action Type
Sent Rec
IPSec SA 1 9 (192.168.250.3,*)-(192.168.250.2,*) 47 ESP tunn 20452 33768
IPSec SA 2 10 (192.168.250.4,*)-(192.168.250.2,*) 47 ESP tunn 19680 31240

```

```
BR2VPN:~#
```

```
BR2R#show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is 192.168.22.2 to network 0.0.0.0
```

```

192.168.250.0/32 is subnetted, 1 subnets
C      192.168.250.2 is directly connected, Loopback0
11.0.0.0/29 is subnetted, 1 subnets
C      11.0.0.0 is directly connected, Tunnel0
192.168.22.0/30 is subnetted, 1 subnets
C      192.168.22.0 is directly connected, FastEthernet1/1
O IA 192.168.0.0/24 [110/1001] via 11.0.0.1, 00:33:50, Tunnel0
O    192.168.1.0/24 [110/1001] via 11.0.0.3, 00:27:05, Tunnel0
C    192.168.2.0/24 is directly connected, FastEthernet1/0
S*   0.0.0.0/0 [1/0] via 192.168.22.2
```

```
BR2R#show dmvpn
```

```
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
         N - NATed, L - Local, X - No Socket
         # Ent --> Number of NHRP entries with same NBMA peer
         NHS Status: E --> Expecting Replies, R --> Responding
         UpDn Time --> Up or Down Time for a Tunnel
```

```
Interface: Tunnel0, IPv4 NHRP Details
```

```
Type:Spoke, NHRP Peers:2,
```

```
=====
```

#	Ent	Peer NBMA Addr	Peer Tunnel Add	State	UpDn Tm	Attrb
1		192.168.250.3	11.0.0.1	UP	01:07:46	S
1		192.168.250.4	11.0.0.2	UP	01:07:24	S

```
BR2R#show ip nhrp
11.0.0.1/32 via 11.0.0.1
    Tunnel0 created 01:08:16, never expire
    Type: static, Flags: used
    NBMA address: 192.168.250.3
11.0.0.2/32 via 11.0.0.2
    Tunnel0 created 01:08:13, never expire
    Type: static, Flags: used
    NBMA address: 192.168.250.4
BR2R#
```

```
BR1R#
```

Конфигурации маршрутизаторов и S-Terra VPN шлюзов (cisco-like и native lsp)

HQMR и HQRVPN1

```
HQMR#sh run
Building configuration...

Current configuration : 3327 bytes
!
! Last configuration change at 13:15:38 MSD Thu Jul 2 2009 by root
! NVRAM config last updated at 11:43:36 MSD Thu Jul 2 2009 by root
!+
version 12.4
configuration mode exclusive manual
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime localtime
no service password-encryption
!
hostname HQMR
!
```

```
boot-start-marker
boot-end-marker
!
security authentication failure rate 3 log
logging message-counter syslog
logging buffered 51200 warnings
enable secret 5 $1$8LcD$fdBOc7n3wYChIkiDy4Zto0
enable password csp
!
aaa new-model
!
!
aaa authentication login default local
aaa authentication enable default enable
aaa authorization exec default local
!
!
aaa session-id common
clock timezone MSD 3
clock summer-time MSD recurring
!
dot11 syslog
ip source-route
!
!
ip cef
!
!
no ip domain lookup
ip domain name s-terra.com
login block-for 120 attempts 3 within 30
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
```

```
voice-card 0
!
!
!
username root privilege 15 secret 5 $1$AmFY$nvOYpWE2qF1Kx3Q91fCsB1
archive
  log config
  hidekeys
!
!
!
ip ssh version 2
!
!
!
interface Loopback0
  description ### HQMR MANAGEMENT INTERFACE ###
  ip address 192.168.250.3 255.255.255.255
!
interface Tunnel0
  description ### HQ MAIN DMVPN HUB ###
  bandwidth 1000
  ip address 11.0.0.1 255.255.255.248
  no ip redirects
  ip mtu 1400
  ip nhrp map multicast dynamic
  ip nhrp network-id 1000
  ip nhrp holdtime 60
  ip ospf network broadcast
  ip ospf priority 20
  tunnel source Loopback0
  tunnel mode gre multipoint
!
interface FastEthernet0/0
  description ### TO HQ LAN ###
  ip address 192.168.0.1 255.255.255.0
  no ip proxy-arp
  duplex auto
  speed auto
  no keepalive
```

```
no mop enabled
!
interface FastEthernet0/1
description ### TO ISP ###
ip address 10.0.1.2 255.255.255.252
no ip unreachable
no ip proxy-arp
ip nat outside
ip virtual-reassembly
duplex auto
speed auto
no keepalive
no mop enabled
!
interface Special-Services-Engine1/0
description ### TO HQRVPN1 ###
ip address 192.168.33.1 255.255.255.252
no ip proxy-arp
ip nat inside
ip virtual-reassembly
no keepalive
no mop enabled
!
router ospf 10
log-adjacency-changes
area 1 nssa
network 11.0.0.0 0.0.0.7 area 1
network 192.168.0.0 0.0.0.255 area 0
!
no ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.0.1.1
ip route 192.168.250.0 255.255.255.0 192.168.33.2
no ip http server
ip http authentication aaa
no ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
!
ip nat inside source static udp 192.168.33.2 500 10.0.1.2 500 extendable
ip nat inside source static udp 192.168.33.2 4500 10.0.1.2 4500 extendable
```

```
!  
ip access-list standard LOCAL_TO_RVPN  
  permit 192.168.33.1  
  deny any  
!  
!  
!  
!  
control-plane  
!  
!  
!  
no ccm-manager fax protocol cisco  
!  
mgcp fax t38 ecm  
!  
!  
!  
line con 0  
  exec-timeout 0 0  
  privilege level 15  
  logging synchronous  
line aux 0  
  access-class 3 in  
  privilege level 15  
  transport input telnet  
line 66  
  access-class LOCAL_TO_RVPN in  
  no activation-character  
  no exec  
  transport preferred none  
  transport input all  
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh  
line vty 0 4  
  exec-timeout 0 0  
  privilege level 15  
  transport input all  
!  
scheduler allocate 20000 1000  
end
```

HQMR#

```
HQRVPN1#show running-config
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit clear
crypto isakmp identity hostname
crypto isakmp keepalive 10 3
ip host HQRVPN2 10.0.2.2
ip host BR1VPN 10.0.0.2
ip host BR2VPN 10.0.0.3
username cscons privilege 15 password 0 newsecretpw
hostname HQRVPN1
enable password csp
!
!
!
crypto isakmp policy 10
  hash md5
  encr des
  authentication pre-share
  group 5
!
crypto isakmp key key333 hostname HQRVPN2
!
crypto isakmp key key111 hostname BR1VPN
!
crypto isakmp key key222 hostname BR2VPN
!
crypto ipsec transform-set ESP_GOST_CI esp-des esp-md5-hmac
!
ip access-list extended GRE_HQMR_TO_ANY
  permit gre host 192.168.250.3 any
!
!
```

```
crypto dynamic-map FA00_DMAP 10
  match address GRE_HQMR_TO_ANY
  set transform-set ESP_GOST_CI
  set pfs group5
!
crypto map FA00_CMAP 10 ipsec-isakmp dynamic FA00_DMAP
!
!
!
interface FastEthernet0/0
  ip address 192.168.33.2 255.255.255.252
  crypto map FA00_CMAP
!
interface FastEthernet0/1
  shutdown
!
!
ip route 0.0.0.0 0.0.0.0 192.168.33.1
end
HQRVPN1#
```

```
HQRVPN1:~# lsp_mgr show
```

```
# This is automatically generated LSP
#
# Conversion Date/Time: Thu Jul 2 09:20:37 2009
```

```
GlobalParameters(
```

```
  Title = "This LSP was automatically generated by
CSP Converter at Thu Jul 2 09:20:37 2009"
  Version = "2.1"
  LDAPLogMessageLevel = INFO
  SystemLogMessageLevel = INFO
  PolicyLogMessageLevel = INFO
  CertificatesLogMessageLevel = INFO
)
```

```
SyslogSettings(
```

```
  Server = 127.0.0.1
  Facility = LOG_LOCAL7
```

```
)

RoutingTable(
    Routes *=
        Route(
            Destination = 0.0.0.0/0
            Gateway = 192.168.33.1
            Metric = 1
        )
    )
)

IKETransform IKETransform_10
(
    CipherAlg    *= "G2814789CPRO1-K256-CBC-65534"
    HashAlg      *= "GR341194CPRO1-65534"
    GroupID      *= MODP_1536
    LifetimeSeconds = 86400
)

ESPProposal ESP_ESP_GOST_CI
(
    Transform* = ESPTransform
    (
        IntegrityAlg*      = "GR341194CPRO1-H96-HMAC-65534"
        CipherAlg*          = "G2814789CPRO1-K256-CBC-254"
        LifetimeSeconds     = 3600
        LifetimeKilobytes   = 4608000
    )
)

AuthMethodPreshared IKE_auth_cs_key_HQRVPN2
(
    LocalID = IdentityEntry( KeyID *= "48515256504e31" )
    RemoteID = IdentityEntry(
        IPv4Address *= 10.0.2.2
        KeyID *= "48515256504e32"
    )
    SharedIKESecret = "cs_key_HQRVPN2"
)

IKERule IKE_FA00_DMAP_10
```

```
(
    IKEPeerIPFilter* = FilterEntry( IPAddress *= 10.0.2.2 )
    Transform* = IKETransform_10
    AggrModeAuthMethod *= IKE_auth_cs_key_HQRVPN2
    MainModeAuthMethod *= IKE_auth_cs_key_HQRVPN2
    DoAutopass          = TRUE
    DPDIdleDuration     = 10
    DPDResponseDuration = 3
    DPDRetries          = 5
)
```

```
IPsecAction FA00_DMAP_10
```

```
(
    TunnelingParameters *= TunnelEntry(
        DFHandling=CLEAR
    )
    ContainedProposals *= ( ESP_ESP_GOST_CI )
    GroupID *= MODP_1536
    IKERule = IKE_FA00_DMAP_10
)
```

```
AuthMethodPreshared IKE_auth_cs_key_BR1VPN
```

```
(
    LocalID = IdentityEntry( KeyID *= "48515256504e31" )
    RemoteID = IdentityEntry(
        IPv4Address *= 10.0.0.2
        KeyID *= "42523156504e"
    )
    SharedIKESecret = "cs_key_BR1VPN"
)
```

```
IKERule IKE_FA00_DMAP_10_1
```

```
(
    IKEPeerIPFilter* = FilterEntry( IPAddress *= 10.0.0.2 )
    Transform* = IKETransform_10
    AggrModeAuthMethod *= IKE_auth_cs_key_BR1VPN
    MainModeAuthMethod *= IKE_auth_cs_key_BR1VPN
    DoAutopass          = TRUE
    DPDIdleDuration     = 10
)
```

```
DPDResponseDuration = 3
DPDRetries           = 5
)

IPsecAction FA00_DMAP_10_1
(
    TunnelingParameters *= TunnelEntry(

        DFHandling=CLEAR
    )
    ContainedProposals *= ( ESP_ESP_GOST_CI )
    GroupID *= MODP_1536
    IKERule = IKE_FA00_DMAP_10_1
)

AuthMethodPreshared IKE_auth_cs_key_BR2VPN
(
    LocalID = IdentityEntry( KeyID *= "48515256504e31" )
    RemoteID = IdentityEntry(
        IPv4Address *= 10.0.0.3
        KeyID *= "42523256504e"
    )
    SharedIKESecret = "cs_key_BR2VPN"
)

IKERule IKE_FA00_DMAP_10_2
(
    IKEPeerIPFilter* = FilterEntry( IPAddress *= 10.0.0.3 )
    Transform* = IKETransform_10
    AggrModeAuthMethod *= IKE_auth_cs_key_BR2VPN
    MainModeAuthMethod *= IKE_auth_cs_key_BR2VPN
    DoAutopass          = TRUE
    DPDIIdleDuration    = 10
    DPDResponseDuration = 3
    DPDRetries          = 5
)

IPsecAction FA00_DMAP_10_2
(
    TunnelingParameters *= TunnelEntry(
```

```
        DFHandling=CLEAR
    )
    ContainedProposals *= ( ESP_ESP_GOST_CI )
    GroupID *= MODP_1536
    IKERule = IKE_FA00_DMAP_10_2
)

FilteringRule Filter_nil_acl_FA00_DMAP_10
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.250.3 ProtocolID *=
47 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255
ProtocolID *= 47 )
    NetworkInterfaces *= "eth0"
    Action *= ( FA00_DMAP_10 ), ( FA00_DMAP_10_1 ), ( FA00_DMAP_10_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 )
)

HQRVPN1:~#
```

HQRR и HQRVPN2

```
HQRR:
HQRR#sh running-config
Building configuration...

Current configuration : 2850 bytes
!
version 12.4
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQRR
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 3 log
logging message-counter syslog
enable secret 5 $1$emDN$rVoGtT4YVYh3yHd.CTVFG1
!
aaa new-model
!
!
aaa authentication login default local
aaa authentication enable default enable
aaa authorization exec default local
!
!
aaa session-id common
clock timezone MSK 3
clock summer-time MSK recurring
!
dot11 syslog
ip source-route
!
!
```

```
ip cef
!
!
no ip domain lookup
ip domain name s-terra.com
login block-for 120 attempts 3 within 30
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
voice-card 0
!
!
!
!
!
username root privilege 15 secret 5 $1$uXHA$q7HSM0NzBuAMUk3W8VjXh0
archive
  log config
  hidekeys
!
!
!
ip ssh version 2
!
!
!
interface Loopback0
  description ### HQRR MANAGEMENT INTERFACE ###
  ip address 192.168.250.4 255.255.255.255
!
interface Tunnel0
  description ### HQ RESERVE DMVPN HUB ###
  bandwidth 900
  ip address 11.0.0.2 255.255.255.248
```

```
no ip redirects
ip mtu 1400
ip nhrp map multicast dynamic
ip nhrp map 11.0.0.1 192.168.250.3
ip nhrp map multicast 192.168.250.3
ip nhrp network-id 1000
ip nhrp holdtime 60
ip nhrp nhs 11.0.0.1
ip ospf network broadcast
ip ospf priority 10
tunnel source Loopback0
tunnel mode gre multipoint
!
interface FastEthernet0/0
description ### TO HQ LAN ###
bandwidth 10000
ip address 192.168.0.2 255.255.255.0
no ip proxy-arp
duplex auto
speed auto
no keepalive
no mop enabled
!
interface FastEthernet0/1
no ip address
no ip proxy-arp
shutdown
duplex auto
speed auto
!
interface Special-Services-Engine1/0
description ### TO HQVPN2 ###
ip address 192.168.44.1 255.255.255.252
no ip unreachable
no ip proxy-arp
no keepalive
no mop enabled
!
router ospf 10
log-adjacency-changes
```

```
area 1 nssa
network 11.0.0.0 0.0.0.7 area 1
network 192.168.0.0 0.0.0.255 area 0
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.44.2
no ip http server
ip http authentication local
no ip http secure-server
!
!
!
ip access-list standard LOCAL_TO_RVPN
remark ### PERMIT ONLY LOCAL ACCESS TO RVPNS CONSOLE ###
permit 192.168.44.1
deny any
!
!
!
control-plane
!
!
!
ccm-manager fax protocol cisco
!
mgcp fax t38 ecm
!
!
dial-peer cor custom
!
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
transport input telnet
speed 115200
line 66
```

```
access-class LOCAL_TO_RVPN in
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
privilege level 15
transport input all
!
scheduler allocate 20000 1000
end
```

HQRR#

```
HQRVPN2#sh run
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit clear
crypto isakmp identity hostname
crypto isakmp keepalive 10 3
ip host HQRVPN1 10.0.1.2
ip host BR1VPN 10.0.0.2
ip host BR2VPN 10.0.0.3
username cscons privilege 15 password 0 newsecretpw
hostname HQRVPN2
enable password csp
!
!
!
crypto isakmp policy 10
hash md5
encr des
authentication pre-share
group 5
!
crypto isakmp key key333 hostname HQRVPN1
```

```
!  
crypto isakmp key key444 hostname BR1VPN  
!  
crypto isakmp key key555 hostname BR2VPN  
!  
crypto ipsec transform-set ESP_GOST_CI esp-des esp-md5-hmac  
!  
ip access-list extended GRE_HQRR_TO_HQMR  
  permit gre host 192.168.250.4 host 192.168.250.3  
!  
ip access-list extended GRE_HQRR_TO_ANY  
  permit gre host 192.168.250.4 any  
!  
!  
crypto dynamic-map FA01_DMAP 10  
  match address GRE_HQRR_TO_ANY  
  set transform-set ESP_GOST_CI  
  set pfs group5  
!  
crypto map FA01_CMAP 10 ipsec-isakmp  
  match address GRE_HQRR_TO_HQMR  
  set transform-set ESP_GOST_CI  
  set pfs group5  
  set peer 10.0.1.2  
!  
crypto map FA01_CMAP 20 ipsec-isakmp dynamic FA01_DMAP  
!  
!  
!  
interface FastEthernet0/0  
  ip address 192.168.44.2 255.255.255.252  
!  
interface FastEthernet0/1  
  ip address 10.0.2.2 255.255.255.252  
  crypto map FA01_CMAP  
!  
!  
ip route 0.0.0.0 0.0.0.0 10.0.2.1  
ip route 192.168.250.4 255.255.255.255 192.168.44.1  
end
```

HQRVPN2#

HQRVPN2:~# lsp_mgr show

This is automatically generated LSP

#

Conversion Date/Time: Thu Jul 2 12:22:10 2009

GlobalParameters(

Title = "This LSP was automatically generated by
CSP Converter at Thu Jul 2 12:22:10 2009"

Version = "2.1"

LDAPLogMessageLevel = INFO

SystemLogMessageLevel = INFO

PolicyLogMessageLevel = INFO

CertificatesLogMessageLevel = INFO

)

SyslogSettings(

Server = 127.0.0.1

Facility = LOG_LOCAL7

)

RoutingTable(

Routes *=

Route(

Destination = 0.0.0.0/0

Gateway = 10.0.2.1

Metric = 1

),

Route(

Destination = 192.168.250.4

Gateway = 192.168.44.1

Metric = 1

)

)

IKETransform IKETransform_10

(

CipherAlg *= "G2814789CPR01-K256-CBC-65534"

HashAlg *= "GR341194CPR01-65534"

GroupID *= MODP_1536

```
LifetimeSeconds = 86400
)

ESPProposal ESP_ESP_GOST_CI
(
    Transform* = ESPTransform
    (
        IntegrityAlg*      = "GR341194CPRO1-H96-HMAC-65534"
        CipherAlg*         = "G2814789CPRO1-K256-CBC-254"
        LifetimeSeconds    = 3600
        LifetimeKilobytes  = 4608000
    )
)

ESPProposal ESP_ESP_GOST_CI_1
(
    Transform* = ESPTransform
    (
        IntegrityAlg*      = "GR341194CPRO1-H96-HMAC-65534"
        CipherAlg*         = "G2814789CPRO1-K256-CBC-254"
        LifetimeSeconds    = 3600
        LifetimeKilobytes  = 4608000
    )
)

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

AuthMethodPreshared IKE_auth_cs_key_HQRVPN1
(
    LocalID = IdentityEntry( KeyID *= "48515256504e32" )
    RemoteID = IdentityEntry(
        IPv4Address *= 10.0.1.2
        KeyID *= "48515256504e31"
    )
)
```

```
    SharedIKESecret = "cs_key_HQRVPN1"
)

IKERule IKE_FA01_CMAP_10
(
    Transform* = IKETransform_10
    AggrModeAuthMethod *= IKE_auth_cs_key_HQRVPN1
    MainModeAuthMethod *= IKE_auth_cs_key_HQRVPN1
    DoAutopass          = TRUE
    DPDIdleDuration     = 10
    DPDResponseDuration = 3
    DPDRetries          = 5
)

IPsecAction FA01_CMAP_10
(
    TunnelingParameters *= TunnelEntry(
        PeerIPAddress = 10.0.1.2

        DFHandling=CLEAR
    )
    ContainedProposals *= ( ESP_ESP_GOST_CI )
    GroupID *= MODP_1536
    IKERule = IKE_FA01_CMAP_10
)

AuthMethodPreshared IKE_auth_cs_key_HQRVPN1_1
(
    LocalID = IdentityEntry( KeyID *= "48515256504e32" )
    RemoteID = IdentityEntry(
        IPv4Address *= 10.0.1.2
        KeyID *= "48515256504e31"
    )
    SharedIKESecret = "cs_key_HQRVPN1"
)

IKERule IKE_FA01_DMAP_10
(
    IKEPeerIPFilter* = FilterEntry( IPAddress *= 10.0.1.2 )
    Transform* = IKETransform_10
)
```

```
AggrModeAuthMethod *= IKE_auth_cs_key_HQRVPN1_1
MainModeAuthMethod *= IKE_auth_cs_key_HQRVPN1_1
DoAutopass          = TRUE
DPDIdleDuration     = 10
DPDResponseDuration = 3
DPDRetries          = 5
)

IPsecAction FA01_DMAP_10
(
    TunnelingParameters *= TunnelEntry(

        DFHandling=CLEAR
    )
    ContainedProposals *= ( ESP_ESP_GOST_CI_1 )
    GroupID *= MODP_1536
    IKERule = IKE_FA01_DMAP_10
)

AuthMethodPreshared IKE_auth_cs_key_BR1VPN
(
    LocalID = IdentityEntry( KeyID *= "48515256504e32" )
    RemoteID = IdentityEntry(
        IPv4Address *= 10.0.0.2
        KeyID *= "42523156504e"
    )
    SharedIKESecret = "cs_key_BR1VPN"
)

IKERule IKE_FA01_DMAP_10_1
(
    IKEPeerIPFilter* = FilterEntry( IPAddress *= 10.0.0.2 )
    Transform* = IKETransform_10
    AggrModeAuthMethod *= IKE_auth_cs_key_BR1VPN
    MainModeAuthMethod *= IKE_auth_cs_key_BR1VPN
    DoAutopass          = TRUE
    DPDIdleDuration     = 10
    DPDResponseDuration = 3
    DPDRetries          = 5
)
```

```
IPsecAction FA01_DMAP_10_1
(
    TunnelingParameters *= TunnelEntry(

        DFHandling=CLEAR
    )
    ContainedProposals *= ( ESP_ESP_GOST_CI_1 )
    GroupID *= MODP_1536
    IKERule = IKE_FA01_DMAP_10_1
)

AuthMethodPreshared IKE_auth_cs_key_BR2VPN
(
    LocalID = IdentityEntry( KeyID *= "48515256504e32" )
    RemoteID = IdentityEntry(
        IPv4Address *= 10.0.0.3
        KeyID *= "42523256504e"
    )
    SharedIKESecret = "cs_key_BR2VPN"
)

IKERule IKE_FA01_DMAP_10_2
(
    IKEPeerIPFilter* = FilterEntry( IPAddress *= 10.0.0.3 )
    Transform* = IKETransform_10
    AggrModeAuthMethod *= IKE_auth_cs_key_BR2VPN
    MainModeAuthMethod *= IKE_auth_cs_key_BR2VPN
    DoAutopass          = TRUE
    DPDIdleDuration     = 10
    DPDResponseDuration = 3
    DPDRetries          = 5
)

IPsecAction FA01_DMAP_10_2
(
    TunnelingParameters *= TunnelEntry(

        DFHandling=CLEAR
    )
)
```

```
    ContainedProposals *= ( ESP_ESP_GOST_CI_1 )
    GroupID *= MODP_1536
    IKERule = IKE_FA01_DMAP_10_2
)

FilteringRule Filter_nil_acl_FA01_CMAP_10
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.250.4 ProtocolID *=
47 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.250.3 ProtocolID *=
47 )
    NetworkInterfaces *= "eth1"
    Action *= ( FA01_CMAP_10 )
)

FilteringRule Filter_nil_acl_FA01_DMAP_10
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.250.4 ProtocolID *=
47 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255
ProtocolID *= 47 )
    NetworkInterfaces *= "eth1"
    Action *= ( FA01_DMAP_10 ), ( FA01_DMAP_10_1 ), ( FA01_DMAP_10_2 )
)

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

ISPR

```
show running-config
Building configuration...
```

```
Current configuration : 1750 bytes
```

```
!  
upgrade fpd auto  
version 12.4  
service tcp-keepalives-in  
service tcp-keepalives-out  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname ISP  
!  
boot-start-marker  
boot-end-marker  
!  
logging message-counter syslog  
enable secret 5 $1$bG4U$aN6pOq7GkjUUSkhrMJFJg0  
!  
aaa new-model  
!  
!  
aaa authentication login default local  
aaa authentication enable default enable  
aaa authorization exec default local  
!  
!  
aaa session-id common  
ip source-route  
ip cef  
!  
!  
!  
!  
no ipv6 cef  
!  
multilink bundle-name authenticated  
!  
!  
voice dsp waitstate 0  
!  
!
```

```
!  
!  
!  
!  
!  
memory-size iomem 0  
username root privilege 15 secret 5 $1$gkW0$ulRSKlmUHkbMH66YN16QN.  
archive  
  log config  
  hidekeys  
!  
!  
!  
interface FastEthernet0/0  
  no ip address  
  shutdown  
  duplex half  
!  
interface FastEthernet1/0  
  no ip address  
  duplex auto  
  speed auto  
  no keepalive  
!  
interface FastEthernet1/0.43  
  description ### TO BRANCHES ###  
  encapsulation dot1Q 43  
  ip address 10.0.0.1 255.255.255.248  
  no ip unreachable  
  no ip proxy-arp  
!  
interface FastEthernet1/0.44  
  description ### TO HQMR ###  
  encapsulation dot1Q 44  
  ip address 10.0.1.1 255.255.255.252  
  no ip unreachable  
  no ip proxy-arp  
!  
interface FastEthernet1/0.45  
  description ### TO HQRR ###
```

```
encapsulation dot1Q 45
ip address 10.0.2.1 255.255.255.252
no ip unreachable
no ip proxy-arp
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
logging alarm informational
!
!
!
!
!
!
!
!
control-plane
!
!
!
mgcp fax t38 ecm
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
```

```
logging synchronous
stopbits 1
line aux 0
  stopbits 1
line vty 0 4
!
end

ISP#
```

BR1R и BR1VPN

```
BR1R#show running-config
Building configuration...

Current configuration : 2318 bytes
!
upgrade fpd auto
version 12.4
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname BR1R
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 3 log
logging message-counter syslog
enable secret 5 $1$YU52$/3RzR8PirNSp4IFlod00d/
!
aaa new-model
!
!
aaa authentication login default local
```



```
!  
interface Loopback0  
  description ### BR1R MANAGEMENT INTERFACE ###  
  ip address 192.168.250.1 255.255.255.255  
!  
interface Tunnel0  
  description ### BRANCH1 DMVPN INTF ###  
  ip address 11.0.0.3 255.255.255.248  
  no ip redirects  
  ip mtu 1400  
  ip nhrp map 11.0.0.1 192.168.250.3  
  ip nhrp map 11.0.0.2 192.168.250.4  
  ip nhrp map multicast 192.168.250.3  
  ip nhrp map multicast 192.168.250.4  
  ip nhrp network-id 1000  
  ip nhrp holdtime 60  
  ip nhrp nhs 11.0.0.1  
  ip nhrp nhs 11.0.0.2  
  ip ospf network broadcast  
  ip ospf priority 0  
  tunnel source Loopback0  
  tunnel mode gre multipoint  
!  
interface FastEthernet0/0  
  no ip address  
  shutdown  
  duplex half  
!  
interface FastEthernet1/0  
  description ### TO BR1 LAN ###  
  ip address 192.168.1.1 255.255.255.0  
  no ip proxy-arp  
  duplex auto  
  speed auto  
  no keepalive  
  no mop enabled  
!  
interface FastEthernet1/1  
  description ### TO BR1VPN ###  
  ip address 192.168.11.1 255.255.255.252
```

```
no ip unreachable
no ip proxy-arp
duplex auto
speed auto
no keepalive
no mop enabled
!
router ospf 10
  log-adjacency-changes
  area 1 nssa
  network 11.0.0.0 0.0.0.7 area 1
  network 192.168.1.0 0.0.0.255 area 1
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.11.2
no ip http server
no ip http secure-server
!
!
!
!
logging alarm informational
!
!
!
control-plane
!
!
!
mgcp fax t38 ecm
!
!
!
!
gatekeeper
  shutdown
!
!
line con 0
  exec-timeout 0 0
```

```
logging synchronous
stopbits 1
line aux 0
  stopbits 1
line vty 0 4
!
end

BR1R#

BR1VPN#show running-config
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit clear
crypto isakmp identity hostname
crypto isakmp keepalive 10 3
ip host HQRVPN1 10.0.1.2
ip host HQRVPN2 10.0.2.2
username cscons privilege 15 password 0 newsecretpw
hostname BR1VPN
enable password csp
!
!
!
crypto isakmp policy 10
  hash md5
  encr des
  authentication pre-share
  group 5
!
crypto isakmp key key111 hostname HQRVPN1
!
crypto isakmp key key444 hostname HQRVPN2
!
crypto ipsec transform-set ESP_GOST_CI esp-des esp-md5-hmac
!
ip access-list extended GRE_BR1R_TO_HQRR
  permit gre host 192.168.250.1 host 192.168.250.4
```

```
!  
ip access-list extended GRE_BR1R_TO_HQMR  
  permit gre host 192.168.250.1 host 192.168.250.3  
!  
!  
crypto map FA01_CMAP 10 ipsec-isakmp  
  match address GRE_BR1R_TO_HQMR  
  set transform-set ESP_GOST_CI  
  set pfs group5  
  set peer 10.0.1.2  
!  
crypto map FA01_CMAP 20 ipsec-isakmp  
  match address GRE_BR1R_TO_HQRR  
  set transform-set ESP_GOST_CI  
  set pfs group5  
  set peer 10.0.2.2  
!  
!  
!  
interface FastEthernet0/0  
  ip address 192.168.11.2 255.255.255.252  
!  
interface FastEthernet0/1  
  ip address 10.0.0.2 255.255.255.248  
  crypto map FA01_CMAP  
!  
!  
ip route 0.0.0.0 0.0.0.0 10.0.0.1  
ip route 192.168.250.1 255.255.255.255 192.168.11.1  
end  
BR1VPN#  
  
BR1VPN:~# lsp_mgr show  
#   This is automatically generated LSP  
#  
#   Conversion Date/Time:   Thu Jul  2 13:17:50 2009  
  
GlobalParameters(  
  Title                               = "This LSP was automatically generated by  
CSP Converter at Thu Jul  2 13:17:50 2009"  
  Version                             = "2.1"
```

```
LDAPLogMessageLevel      = INFO
SystemLogMessageLevel    = INFO
PolicyLogMessageLevel    = INFO
CertificatesLogMessageLevel = INFO
)

SyslogSettings(
    Server = 127.0.0.1
    Facility = LOG_LOCAL7
)

RoutingTable(
    Routes *=
        Route(
            Destination = 0.0.0.0/0
            Gateway = 10.0.0.1
            Metric = 1
        ),
        Route(
            Destination = 192.168.250.1
            Gateway = 192.168.11.1
            Metric = 1
        )
    )
)

IKETransform IKETransform_10
(
    CipherAlg      *= "G2814789CPR01-K256-CBC-65534"
    HashAlg        *= "GR341194CPR01-65534"
    GroupID        *= MODP_1536
    LifetimeSeconds = 86400
)

ESPProposal ESP_ESP_GOST_CI
(
    Transform* = ESPTransform
    (
        IntegrityAlg*      = "GR341194CPR01-H96-HMAC-65534"
        CipherAlg*         = "G2814789CPR01-K256-CBC-254"
        LifetimeSeconds    = 3600
        LifetimeKilobytes  = 4608000
    )
)
```

```
)
)

ESPProposal ESP_ESP_GOST_CI_1
(
    Transform* = ESPTransform
    (
        IntegrityAlg*      = "GR341194CPR01-H96-HMAC-65534"
        CipherAlg*         = "G2814789CPR01-K256-CBC-254"
        LifetimeSeconds    = 3600
        LifetimeKilobytes  = 4608000
    )
)

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

AuthMethodPreshared IKE_auth_cs_key_HQRVPN1
(
    LocalID = IdentityEntry( KeyID *= "42523156504e" )
    RemoteID = IdentityEntry(
        IPv4Address *= 10.0.1.2
        KeyID *= "48515256504e31"
    )
    SharedIKESecret = "cs_key_HQRVPN1"
)

IKERule IKE_FA01_CMAP_10
(
    Transform* = IKETransform_10
    AggrModeAuthMethod *= IKE_auth_cs_key_HQRVPN1
    MainModeAuthMethod *= IKE_auth_cs_key_HQRVPN1
    DoAutopass          = TRUE
    DPDIIdleDuration    = 10
    DPDResponseDuration = 3
)
```

```
        DPDRetries          = 5
    )

IPsecAction FA01_CMAP_10
(
    TunnelingParameters *= TunnelEntry(
        PeerIPAddress = 10.0.1.2

        DFHandling=CLEAR
    )
    ContainedProposals *= ( ESP_ESP_GOST_CI )
    GroupID *= MODP_1536
    IKERule = IKE_FA01_CMAP_10
)

AuthMethodPreshared IKE_auth_cs_key_HQRVPN2
(
    LocalID = IdentityEntry( KeyID *= "42523156504e" )
    RemoteID = IdentityEntry(
        IPv4Address *= 10.0.2.2
        KeyID *= "48515256504e32"
    )
    SharedIKESecret = "cs_key_HQRVPN2"
)

IKERule IKE_FA01_CMAP_20
(
    Transform* = IKETransform_10
    AggrModeAuthMethod *= IKE_auth_cs_key_HQRVPN2
    MainModeAuthMethod *= IKE_auth_cs_key_HQRVPN2
    DoAutopass          = TRUE
    DPDIIdleDuration    = 10
    DPDResponseDuration = 3
    DPDRetries          = 5
)

IPsecAction FA01_CMAP_20
(
    TunnelingParameters *= TunnelEntry(
        PeerIPAddress = 10.0.2.2
```

```
        DFHandling=CLEAR
    )
    ContainedProposals *= ( ESP_ESP_GOST_CI_1 )
    GroupID *= MODP_1536
    IKERule = IKE_FA01_CMAP_20
)

FilteringRule Filter_nil_acl_FA01_CMAP_10
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.250.1 ProtocolID *=
47 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.250.3 ProtocolID *=
47 )
    NetworkInterfaces *= "eth1"
    Action *= ( FA01_CMAP_10 )
)

FilteringRule Filter_nil_acl_FA01_CMAP_20
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.250.1 ProtocolID *=
47 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.250.4 ProtocolID *=
47 )
    NetworkInterfaces *= "eth1"
    Action *= ( FA01_CMAP_20 )
)

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 )
)

BR1VPN:~#
```

BR2R и BR2VPN

```
BR2R#show running-config
Building configuration...

Current configuration : 2232 bytes
!
upgrade fpd auto
version 12.4
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname BR2R
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5 $1$yn3M$nBVGR3O1lgEG2LsqEOVDS.
!
aaa new-model
!
!
aaa authentication login default local
aaa authentication enable default enable
aaa authorization exec default local
!
!
aaa session-id common
ip source-route
ip cef
!
!
no ip domain lookup
no ipv6 cef
!
```

```
multilink bundle-name authenticated
!
!
voice dsp waitstate 0
!
!
!
!
!
!
!
!
memory-size iomem 0
username root privilege 15 secret 5 $1$q0yB$7dfoQlqWRvbpnimMONBy2.
archive
  log config
  hidekeys
!
!
!
interface Loopback0
  description ### BR2R MANAGEMENT INTERFACE ###
  ip address 192.168.250.2 255.255.255.255
!
interface Tunnel0
  description ### BRANCH2 DMVPN INTF ###
  ip address 11.0.0.4 255.255.255.248
  no ip redirects
  ip mtu 1400
  ip nhrp map 11.0.0.1 192.168.250.3
  ip nhrp map 11.0.0.2 192.168.250.4
  ip nhrp map multicast 192.168.250.3
  ip nhrp map multicast 192.168.250.4
  ip nhrp network-id 1000
  ip nhrp holdtime 60
  ip nhrp nhs 11.0.0.1
  ip nhrp nhs 11.0.0.2
  ip ospf network broadcast
  ip ospf priority 0
  tunnel source Loopback0
  tunnel mode gre multipoint
```

```
!  
interface FastEthernet0/0  
  no ip address  
  shutdown  
  duplex half  
!  
interface FastEthernet1/0  
  description ### TO BR2 LAN ###  
  ip address 192.168.2.1 255.255.255.0  
  no ip proxy-arp  
  duplex auto  
  speed auto  
  no keepalive  
  no mop enabled  
!  
interface FastEthernet1/1  
  description ### TO BR2VPN ###  
  ip address 192.168.22.1 255.255.255.252  
  no ip unreachable  
  no ip proxy-arp  
  duplex auto  
  speed auto  
  no keepalive  
  no mop enabled  
!  
router ospf 10  
  log-adjacency-changes  
  area 1 nssa  
  network 11.0.0.0 0.0.0.7 area 1  
  network 192.168.2.0 0.0.0.255 area 1  
!  
ip forward-protocol nd  
ip route 0.0.0.0 0.0.0.0 192.168.22.2  
no ip http server  
no ip http secure-server  
!  
!  
!  
logging alarm informational  
!
```

```
!  
!  
control-plane  
!  
!  
!  
mgcp fax t38 ecm  
!  
!  
!  
!  
gatekeeper  
  shutdown  
!  
!  
line con 0  
  exec-timeout 0 0  
  logging synchronous  
  stopbits 1  
line aux 0  
  stopbits 1  
line vty 0 4  
!  
end
```

BR2R#

BR2VPN#sh run

```
!  
version 12.4  
no service password-encryption  
!  
crypto ipsec df-bit clear  
crypto isakmp identity hostname  
crypto isakmp keepalive 10 3  
ip host HQRVPN1 10.0.1.2  
ip host HQRVPN2 10.0.2.2  
username cscons privilege 15 password 0 newsecretpw  
hostname BR2VPN
```

```
enable password csp
!
!
!
crypto isakmp policy 10
  hash md5
  encr des
  authentication pre-share
  group 5
!
crypto isakmp key key222 hostname HQRVPN1
!
crypto isakmp key key555 hostname HQRVPN2
!
crypto ipsec transform-set ESP_GOST_CI esp-des esp-md5-hmac
!
ip access-list extended GRE_BR2R_TO_HQMR
  permit gre host 192.168.250.2 host 192.168.250.3
!
ip access-list extended GRE_BR2R_TO_HQRR
  permit gre host 192.168.250.2 host 192.168.250.4
!
!
crypto map FA01_CMAP 10 ipsec-isakmp
  match address GRE_BR2R_TO_HQMR
  set transform-set ESP_GOST_CI
  set pfs group5
  set peer 10.0.1.2
!
crypto map FA01_CMAP 20 ipsec-isakmp
  match address GRE_BR2R_TO_HQRR
  set transform-set ESP_GOST_CI
  set pfs group5
  set peer 10.0.2.2
!
!
!
interface FastEthernet0/0
  ip address 192.168.22.2 255.255.255.252
!
```

```
interface FastEthernet0/1
  ip address 10.0.0.3 255.255.255.248
  crypto map FA01_CMAP
!
!
ip route 0.0.0.0 0.0.0.0 10.0.0.1
ip route 192.168.250.2 255.255.255.255 192.168.22.1
end
BR2VPN#

BR2VPN:~# lsp_mgr show
# This is automatically generated LSP
#
# Conversion Date/Time: Thu Jul 2 13:17:23 2009

GlobalParameters(
  Title = "This LSP was automatically generated by
CSP Converter at Thu Jul 2 13:17:23 2009"
  Version = "2.1"
  LDAPLogMessageLevel = INFO
  SystemLogMessageLevel = INFO
  PolicyLogMessageLevel = INFO
  CertificatesLogMessageLevel = INFO
)

SyslogSettings(
  Server = 127.0.0.1
  Facility = LOG_LOCAL7
)

RoutingTable(
  Routes *=
    Route(
      Destination = 0.0.0.0/0
      Gateway = 10.0.0.1
      Metric = 1
    ),
    Route(
      Destination = 192.168.250.2
      Gateway = 192.168.22.1
      Metric = 1
```

```
    )
)
IKETransform IKETransform_10
(
    CipherAlg    *= "G2814789CPR01-K256-CBC-65534"
    HashAlg      *= "GR341194CPR01-65534"
    GroupID     *= MODP_1536
    LifetimeSeconds = 86400
)

ESPProposal ESP_ESP_GOST_CI
(
    Transform* = ESPTransform
    (
        IntegrityAlg*      = "GR341194CPR01-H96-HMAC-65534"
        CipherAlg*         = "G2814789CPR01-K256-CBC-254"
        LifetimeSeconds    = 3600
        LifetimeKilobytes  = 4608000
    )
)

ESPProposal ESP_ESP_GOST_CI_1
(
    Transform* = ESPTransform
    (
        IntegrityAlg*      = "GR341194CPR01-H96-HMAC-65534"
        CipherAlg*         = "G2814789CPR01-K256-CBC-254"
        LifetimeSeconds    = 3600
        LifetimeKilobytes  = 4608000
    )
)

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

```
AuthMethodPreshared IKE_auth_cs_key_HQRVPN1
(
  LocalID = IdentityEntry( KeyID *= "42523256504e" )
  RemoteID = IdentityEntry(
    IPv4Address *= 10.0.1.2
    KeyID *= "48515256504e31"
  )
  SharedIKESecret = "cs_key_HQRVPN1"
)
```

```
IKERule IKE_FA01_CMAP_10
(
  Transform* = IKETransform_10
  AggrModeAuthMethod *= IKE_auth_cs_key_HQRVPN1
  MainModeAuthMethod *= IKE_auth_cs_key_HQRVPN1
  DoAutopass = TRUE
  DPDIdleDuration = 10
  DPDResponseDuration = 3
  DPDRetries = 5
)
```

```
IPsecAction FA01_CMAP_10
(
  TunnelingParameters *= TunnelEntry(
    PeerIPAddress = 10.0.1.2

    DFHandling=CLEAR
  )
  ContainedProposals *= ( ESP_ESP_GOST_CI )
  GroupID *= MODP_1536
  IKERule = IKE_FA01_CMAP_10
)
```

```
AuthMethodPreshared IKE_auth_cs_key_HQRVPN2
(
  LocalID = IdentityEntry( KeyID *= "42523256504e" )
  RemoteID = IdentityEntry(
    IPv4Address *= 10.0.2.2
    KeyID *= "48515256504e32"
  )
)
```

```
    SharedIKESecret = "cs_key_HQRVPN2"
)

IKERule IKE_FA01_CMAP_20
(
    Transform* = IKETransform_10
    AggrModeAuthMethod *= IKE_auth_cs_key_HQRVPN2
    MainModeAuthMethod *= IKE_auth_cs_key_HQRVPN2
    DoAutopass          = TRUE
    DPDIdleDuration     = 10
    DPDResponseDuration = 3
    DPDRetries          = 5
)

IPsecAction FA01_CMAP_20
(
    TunnelingParameters *= TunnelEntry(
        PeerIPAddress = 10.0.2.2

        DFHandling=CLEAR
    )
    ContainedProposals *= ( ESP_ESP_GOST_CI_1 )
    GroupID *= MODP_1536
    IKERule = IKE_FA01_CMAP_20
)

FilteringRule Filter_nil_acl_FA01_CMAP_10
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.250.2 ProtocolID *=
47 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.250.3 ProtocolID *=
47 )
    NetworkInterfaces *= "eth1"
    Action *= ( FA01_CMAP_10 )
)

FilteringRule Filter_nil_acl_FA01_CMAP_20
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.250.2 ProtocolID *=
47 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 192.168.250.4 ProtocolID *=
47 )
```

```

NetworkInterfaces *= "eth1"
Action *= ( FA01_CMAP_20 )
)

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 )
)

```

```
BR2VPN:~#
```

Сценарий 2

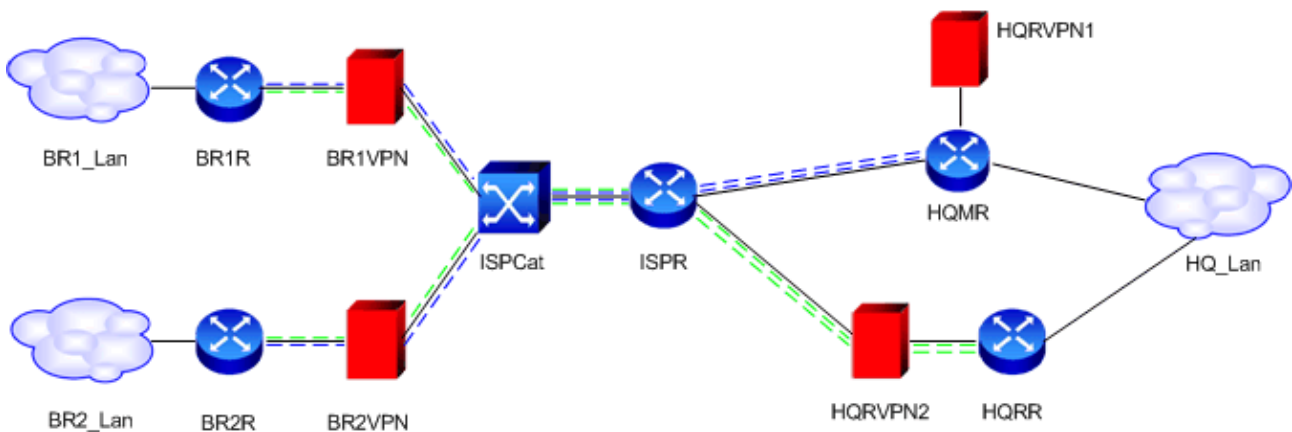


Рисунок 3

Синей и зеленой пунктирной линией показаны две DMVPN сети (у первой HUB – HQMR, у второй – HQRR).

Отличие настроек данного сценария от сценария №1:

- Теперь две DMVPN сети – у первой HUB HQMR, у второй HQRR. Так как HUB больше не связаны между собой, то нет необходимости HQRR настраивать как Spoke для HQMR. Настройка HQVRM осталась без изменений. Настройка HQRR:

```

interface Tunnel0
  description ### HQ RESERVE DMVPN HUB ###
  bandwidth 900
  ip address 11.0.0.9 255.255.255.248
  no ip redirects

```

```

ip mtu 1400
ip nhrp map multicast dynamic
ip nhrp network-id 2000
ip nhrp holdtime 60
ip ospf network broadcast
ip ospf priority 10
tunnel source Loopback0
tunnel mode gre multipoint
!
```

- Так же на устройстве HQVPN2 пропала необходимость в настройке статической криптокарты для связи HQRR с HQMR.
- На каждом из Spoke (BR1R и BR2R) маршрутизаторов теперь поднимаются на один, а два туннельных интерфейса. Причем их тип не mGRE, а p2p GRE (tunnel mode gre ip).

Настройки устройств BR1VPN и BR2VPN не изменились.

BR1R

```

BR1R(config)#do sh run | beg Tun
interface Tunnel0
  description ### BRANCH1 DMVPN INTF ###
  bandwidth 1000
  ip address 11.0.0.3 255.255.255.248
  ip mtu 1400
  ip nhrp map 11.0.0.1 192.168.250.3
  ip nhrp map multicast 192.168.250.3
  ip nhrp network-id 1000
  ip nhrp holdtime 60
  ip nhrp nhs 11.0.0.1
  ip ospf network broadcast
  ip ospf priority 0
  tunnel source Loopback0
  tunnel destination 192.168.250.3
!
interface Tunnel1
  description ### BRANCH1 DMVPN BACKUP INTF ###
  ip address 11.0.0.10 255.255.255.248
  ip mtu 1400
  ip nhrp map 11.0.0.9 192.168.250.4
```

```
ip nhrp map multicast 192.168.250.4
ip nhrp network-id 2000
ip nhrp holdtime 60
ip nhrp nhs 11.0.0.9
ip ospf network broadcast
ip ospf priority 0
tunnel source Loopback0
tunnel destination 192.168.250.4
!
```

BR2R

```
BR2R#show running-config | beg Tun
```

```
*Jul  2 14:06:04.154: %SYS-5-CONFIG_I: Configured from console by
consoleinterface Tunnel0
description ### BRANCH2 DMVPN INTF ###
bandwidth 1000
ip address 11.0.0.4 255.255.255.248
ip mtu 1400
ip nhrp map 11.0.0.1 192.168.250.3
ip nhrp map multicast 192.168.250.3
ip nhrp network-id 1000
ip nhrp holdtime 60
ip nhrp nhs 11.0.0.1
ip ospf network broadcast
ip ospf priority 0
tunnel source Loopback0
tunnel destination 192.168.250.3
!
interface Tunnel1
description ### BRANCH2 DMVPN BACKUP INTF ###
ip address 11.0.0.11 255.255.255.248
ip mtu 1400
ip nhrp map 11.0.0.9 192.168.250.4
ip nhrp map multicast 192.168.250.4
ip nhrp network-id 2000
ip nhrp holdtime 60
```

```

ip nhrp nhs 11.0.0.9
ip ospf network broadcast
ip ospf priority 0
tunnel source Loopback0
tunnel destination 192.168.250.4
!
```

Проверка работоспособности отказоустойчивого решения

Для проверки будем с адреса из BR1_Lan пинговать адрес из BR2_Lan пакетами размером 1000 байт. В штатном случае, трафик из BR1_Lan в BR2_Lan будет проходить через HQMR:

```

BR1R#show ip route 192.168.2.1
Routing entry for 192.168.2.0/24
  Known via "ospf 10", distance 110, metric 101, type intra area
  Last update from 11.0.0.4 on Tunnel0, 00:04:11 ago
R2outing Descriptor Blocks:
  * 11.0.0.4, from 192.168.250.2, 00:04:11 ago, via Tunnel0
    Route metric is 101, traffic share count is 1
```

До того, как мы запустим ping-пакеты, проверим счетчики зашифрованных и расшифрованных пакетов на устройстве BR1VPN:

```

BR1VPN:~# sa_show -e
IKE sessions: 0 initiated, 0 responded

ISAKMP SA Num (Remote Addr,Port)-(Local Addr,Port) State Sent Rec
ISAKMP SA 1 (10.0.2.2,500)-(10.0.0.2,500) ready 1552 1072
ISAKMP SA 2 (10.0.1.2,4500)-(10.0.0.2,4500) ready 1184 672

IPSec SA Num (Remote Addr,Port)-(Local Addr,Port) Protocol Action Type
Sent Rec
IPSec SA 1 9 (192.168.250.4,*)-(192.168.250.1,*) 47 ESP tunn 65728 89872
IPSec SA 2 10 (192.168.250.3,*)-(192.168.250.1,*) 47 ESP tunn 30220 50752
```

Запустим ping:

```
BR1R#ping 192.168.2.1 source 192.168.1.1 size 1000 repeat 100
```

```
Type escape sequence to abort.
Sending 100, 1000-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 12/22/40
ms
BR1R#
```

Убедимся, что трафик между BR1R и HQMR увеличился:

```
BR1VPN:~# sa_show -e
IKE sessions: 0 initiated, 0 responded

ISAKMP SA Num (Remote Addr,Port)-(Local Addr,Port) State Sent Rec
ISAKMP SA 1 (10.0.2.2,500)-(10.0.0.2,500) ready 1552 1072
ISAKMP SA 2 (10.0.1.2,4500)-(10.0.0.2,4500) ready 1184 672

IPSec SA Num (Remote Addr,Port)-(Local Addr,Port) Protocol Action Type
Sent Rec
IPSec SA 1 9 (192.168.250.4,*)-(192.168.250.1,*) 47 ESP tunn 66052 90384
IPSec SA 2 10 (192.168.250.3,*)-(192.168.250.1,*) 47 ESP tunn 132944
160256
BR1VPN:~#
```

Теперь отключим интерфейс fa0/1 на устройстве HQMR и убедимся, что маршрут переключился на HQRR:

```
BR1R#
Jul  2 14:10:27.063: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.250.3 on
Tunnel0 from FULL to DOWN, Neighbor Down: Dead timer expired
BR1R#show ip route 192.168.2.1
Routing entry for 192.168.2.0/24
  Known via "ospf 10", distance 110, metric 1001, type intra area
  Last update from 11.0.0.11 on Tunnel1, 00:00:37 ago
  Routing Descriptor Blocks:
    * 11.0.0.11, from 192.168.250.2, 00:00:37 ago, via Tunnel1
      Route metric is 1001, traffic share count is 1
```

Запустим ping и проверим счетчик пакетов (на этот раз трафик должен увеличиваться между BR1VPN и HQRR)

```
BR1R#ping 192.168.2.1 source 192.168.1.1 size 1000 repeat 100
```

```
Type escape sequence to abort.
```

```
Sending 100, 1000-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
```

```
Packet sent with a source address of 192.168.1.1
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
Success rate is 100 percent (100/100), round-trip min/avg/max = 12/23/44 ms
```

```
BR1VPN:~# sa_show -e
```

```
IKE sessions: 0 initiated, 0 responded
```

```
ISAKMP SA Num (Remote Addr,Port)-(Local Addr,Port) State Sent Rec
```

```
ISAKMP SA 1 (10.0.2.2,500)-(10.0.0.2,500) ready 1552 1072
```

```
IPSec SA Num (Remote Addr,Port)-(Local Addr,Port) Protocol Action Type  
Sent Rec
```

```
IPSec SA 1 9 (192.168.250.4,*)-(192.168.250.1,*) 47 ESP tunn 170720 201824
```

```
BR1VPN:~#
```

Вновь включим интерфейс fa0/1 на HQMR и убедимся, что маршрут переключился обратно:

```
BR1R#
```

```
Jul 2 14:12:47.515: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.250.3 on  
Tunnel0 from LOADING to FULL, Loading Done
```

```
BR1R#show ip route 192.168.2.1
```

```
Routing entry for 192.168.2.0/24
```

```
Known via "ospf 10", distance 110, metric 101, type intra area
```

```
Last update from 11.0.0.4 on Tunnel0, 00:00:00 ago
```

```
Routing Descriptor Blocks:
```

```
* 11.0.0.4, from 192.168.250.2, 00:00:00 ago, via Tunnel0
```

```
Route metric is 101, traffic share count is 1
```

```
BR1R#
```

Вывод таблиц маршрутизации информации о DMVPN с устройств

BR1R

```
BR1R#show dmvpn
```

```
Jul  2 14:07:07.151: %SYS-5-CONFIG_I: Configured from console by console
```

```
BR1R#show dmvpn
```

```
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
```

```
  N - NATed, L - Local, X - No Socket
```

```
  # Ent --> Number of NHRP entries with same NBMA peer
```

```
  NHS Status: E --> Expecting Replies, R --> Responding
```

```
  UpDn Time --> Up or Down Time for a Tunnel
```

```
=====
```

```
Interface: Tunnel0, IPv4 NHRP Details
```

```
Type:Spoke, NHRP Peers:1,
```

# Ent	Peer NBMA Addr	Peer Tunnel Add	State	UpDn Tm	Attrb
1	192.168.250.3	11.0.0.1	UP	00:17:26	S

```
Interface: Tunnell1, IPv4 NHRP Details
```

```
Type:Spoke, NHRP Peers:1,
```

# Ent	Peer NBMA Addr	Peer Tunnel Add	State	UpDn Tm	Attrb
1	192.168.250.4	11.0.0.9	UP	00:15:00	S

```
BR1R#show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
  D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
  N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
  E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
  i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
  ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```
  o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is 192.168.11.2 to network 0.0.0.0
```

```

192.168.11.0/30 is subnetted, 1 subnets
C    192.168.11.0 is directly connected, FastEthernet1/1
192.168.250.0/32 is subnetted, 1 subnets
C    192.168.250.1 is directly connected, Loopback0
11.0.0.0/29 is subnetted, 2 subnets
C    11.0.0.8 is directly connected, Tunnel1
C    11.0.0.0 is directly connected, Tunnel0
O IA 192.168.0.0/24 [110/101] via 11.0.0.1, 00:02:34, Tunnel0
C    192.168.1.0/24 is directly connected, FastEthernet1/0
O    192.168.2.0/24 [110/101] via 11.0.0.4, 00:02:34, Tunnel0
S*   0.0.0.0/0 [1/0] via 192.168.11.2
BR1R#

```

BR2R

```
BR2R#show dmvpn
```

```

Legend: Attrib --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding
        UpDn Time --> Up or Down Time for a Tunnel
=====

```

```
Interface: Tunnel0, IPv4 NHRP Details
```

```
Type:Spoke, NHRP Peers:1,
```

# Ent	Peer NBMA Addr	Peer Tunnel Add	State	UpDn Tm	Attrib
1	192.168.250.3	11.0.0.1	UP	00:07:24	S

```
Interface: Tunnel1, IPv4 NHRP Details
```

```
Type:Spoke, NHRP Peers:1,
```

# Ent	Peer NBMA Addr	Peer Tunnel Add	State	UpDn Tm	Attrib
1	192.168.250.4	11.0.0.9	UP	00:04:30	S

```
BR2R#sho
```

```
BR2R#show ip rout
```

```
BR2R#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.22.2 to network 0.0.0.0

    192.168.250.0/32 is subnetted, 1 subnets
C      192.168.250.2 is directly connected, Loopback0
    11.0.0.0/29 is subnetted, 2 subnets
C      11.0.0.8 is directly connected, Tunnel1
C      11.0.0.0 is directly connected, Tunnel0
    192.168.22.0/30 is subnetted, 1 subnets
C      192.168.22.0 is directly connected, FastEthernet1/1
O IA 192.168.0.0/24 [110/101] via 11.0.0.1, 00:03:37, Tunnel0
O    192.168.1.0/24 [110/101] via 11.0.0.3, 00:03:37, Tunnel0
C    192.168.2.0/24 is directly connected, FastEthernet1/0
S*   0.0.0.0/0 [1/0] via 192.168.22.2
BR2R#
```