Построение кластера на базе протокола VRRP с балансировкой нагрузки (Active-Active) с настройкой при помощи CLI

Настоящий документ содержит описание способа совместного использования Продуктов компании ООО «С-Терра СиЭсПи» и Продуктов третьих производителей.
ООО «С-Терра СиЭсПи» осуществляет сопровождение настоящего сценария в части настроек Продуктов Компании. Упоминание наименований, продуктов, торговых марок третьих организаций исключительно неформально и не является поддержкой, рекомендацией либо рекламой. ООО «С-Терра СиЭсПи» не несет какой-либо ответственности в отношении работоспособности и использования этих Продуктов. Документ имеет статус вспомогательного материала, который может быть использован технологическими партнерами, компаниями-интеграторами, при разработке собственных решений.
Решения, разработанные на базе данного сценария, могут применяться в действующих сетях/системах только после тестовой и/или опытной эксплуатации.

Введение

Данная инструкция описывает настройку VRRP кластера из криптошлюзов «С-Терра Шлюз» с балансировкой нагрузки (Active-Active).

Схема взаимодействия

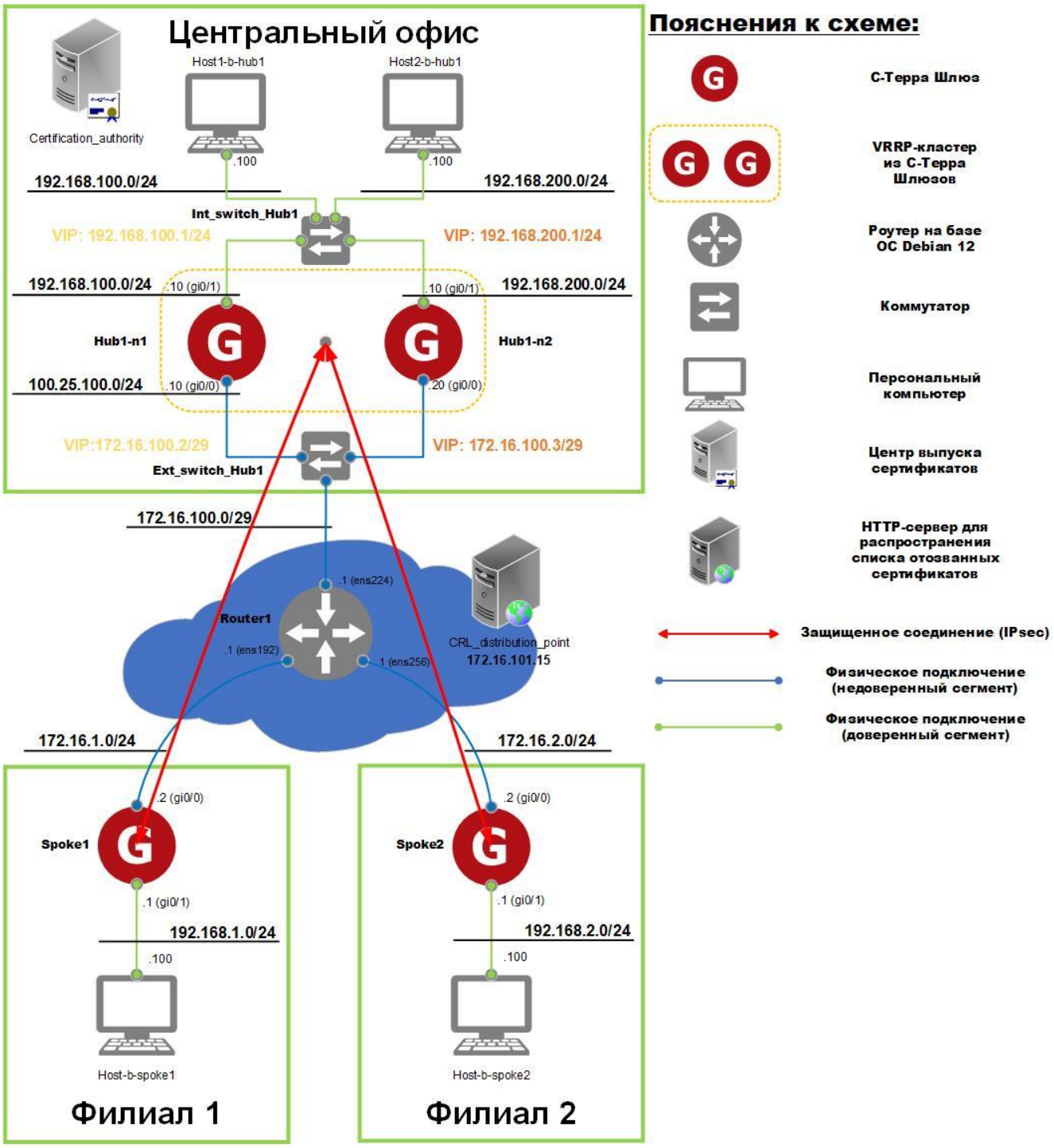


Рисунок 1. Схема взаимодействия

Общая логика работы

1. Размещение устройств.

   1.1. В центральном офисе размещаются: центр выпуска сертификатов (Certification_authority), криптошлюзы «С-Терра Шлюз» (Hub1-n1 и Hub1-n2) версии 5.0 и персональные компьютеры (Host1-b-hub1, Host2-b-hub1).

   1.2. В филиале № 1 размещаются: криптошлюз «С-Терра Шлюз» (Spoke1) версии 5.0 и персональный компьютер (Host-b-spoke1).

   1.3. В филиале № 2 размещаются: криптошлюз «С-Терра Шлюз» (Spoke2) версии 5.0 и персональный компьютер (Host-b-spoke2).

   1.4. В неконтролируемом сегменте (синее облако на схеме) размещаются: HTTP сервер для распространения списка отозванных сертификатов (CRL_distribution_point), маршрутизатор (Router1).

2. Отказоустойчивость и балансировка.

   Криптошлюзы Hub1-n1 и Hub1-n2 объединяются в отказоустойчивый кластер, работающий на базе протокола VRRP в режиме балансировки нагрузки Active-Active. За реализацию протокола VRRP отвечает ПО «keepalived». Криптошлюзы Hub1-n1 и Hub1-n2 являются нодами кластера.

   Конфигурация между нодами кластера не синхронизируется. При изменении настроек на одной ноде, нужно выполнить аналогичные настройки на другой. Ноды должны отличаться настройками отслеживаемых интерфейсов, приоритетом и маршрутом по умолчанию, используемым нодой при переходе в режим Backup/False.

   В режиме балансировки нагрузки Active-Active каждая нода (Hub1-n1 и Hub1-n2) одновременно находится в состоянии Master и владеет кластерными IP адресами в доверенном и недоверенном сегментах (см. Рисунок 1. Схема взаимодействия). Каждая нода обрабатывает трафик, направленный на её кластерные адреса, что позволяет более эффективно распределять нагрузку и оптимально использовать вычислительные ресурсы нод. В случае сбоя одной из нод, другая нода берет на себя обработку трафика, предназначенного для кластерных IP адресов вышедшей из строя ноды, используя механизм VRRP.

   VRRP интерфейсы синхронизированы в две VRRP группы на каждой ноде. Соответственно VRRP интерфейсы, синхронизированные в одной VRRP группе, одновременно меняют свое состояние (данное поведение отличается от Cisco IOS, где по умолчанию VRRP интерфейсы не синхронизированы). Каждая VRRP группа имеет разный приоритет и управляет парой VRRP интерфейсов с кластерными IP адресами в доверенном и недоверенном сегментах.

   Для предсказуемого восстановления работы кластера используется VRRP механизм `preempt`. Он позволяет VRRP группе с более высоким приоритетом на одной из нод автоматически вернуть себе роль Master после восстановления, если она была утрачена из-за сбоя или временной недоступности. Это предотвращает удержание роли Master у VRRP группы с более низким приоритетом, обеспечивая стабильную работу кластера в режиме Active-Active.

   Обнаружение отказа происходит благодаря служебным пакетам протокола VRRP (VRRP Advertisement messages). Каждая VRRP группа, находящаяся в состоянии Master, отправляет эти пакеты. Если одна из VRRP групп в состоянии Backup на одной ноде перестает получать VRRP Advertisement сообщения от Master группы другой ноды на всех синхронизированных VRRP интерфейсах, она захватывает роль Master для своей VRRP группы. Это состояние сохраняется до тех пор, пока VRRP группа с более высоким приоритетом не вернет себе статус Master.

   На нодах настроен маршрут по умолчанию через адрес доверенного сегмента другой ноды для обеспечения доступа ноды в сеть Интернет в случае временной недоступности WAN интерфейса. Метрика данного маршрута должна быть больше, чем метрика маршрута, добавляемая при переходе VRRP группы в состояние Master.

   Кластер с балансировкой нагрузки (Active-Active) обрабатывает следующие типы отказов:

   - отключение питания;

- выход из строя аппаратной платформы;
- отказ сетевого порта на аппаратной платформе;
- отказ сетевого порта на коммутационном оборудовании;
- отказ сервиса vpngate, обеспечивающего построение IPsec туннелей.

3. Подключение к сети Интернет.

   В данном сценарии для эмуляции сети Интернет используются маршрутизатор Router1.

   Подключение к сети Интернет на устройствах «С-Терра Шлюз» будет считаться успешным, если по протоколу ICMP (или «ping») будет доступен HTTP сервер для распространения списка отозванных сертификатов (устройство CRL_distribution_point на схеме).

   3.1. Криптошлюз Hub1 подключается к сети Интернет с помощью статической маршрутизации (маршрут по умолчанию через маршрутизатор Router1).

   3.2. Криптошлюз Spoke1 подключается к сети Интернет с помощью статической маршрутизации (маршрут по умолчанию через маршрутизатор Router1).

   3.3. Криптошлюз Spoke2 подключается к сети Интернет с помощью статической маршрутизации (маршрут по умолчанию через маршрутизатор Router1).

4. Параметры шифрования IPsec.

   Весь IPv4 трафик между подсетями центрального офиса (192.168.100.0/24, 192.168.200.0/24) и филиалов (192.168.1.0/24, 192.168.2.0/24) защищается с использованием алгоритмов ГОСТ и протокола IPsec в туннельном IPv4 режиме.

   Инициировать защищенное соединение между криптошлюзами Hub1 и Spoke1 может трафик из подсети филиала (192.168.1.0/24) в подсеть центра (192.168.100.0/24) и наоборот из центра в филиал.

   Инициировать защищенное соединение между криптошлюзами Hub1 и Spoke2 может трафик из подсети филиала (192.168.2.0/24) в подсеть центра (192.168.200.0/24) и наоборот из центра в филиал.

   4.1. Параметры протокола IKE

      4.1.1. Параметры протокола IKE для версии 5.0:

- Аутентификация при помощи цифровых сертификатов, алгоритм подписи – ГОСТ Р 34.10-2012 (ключ 256 бит);
- Алгоритм шифрования – ГОСТ Р 34.12-2015 Магма (ключ 256 бит);
- Алгоритм вычисления хеш-функции – ГОСТ Р 34.11-2012 ТК26 Стрибог (ключ 256 бит);
- Алгоритм выработки общего ключа (аналог алгоритма Диффи-Хеллмана) – VKO_GOSTR3410_2012_256 (ключ 256 бит).

   4.2. Параметры протокола ESP

- Комбинированный алгоритм шифрования и имитозащиты (контроль целостности) – ГОСТ Р 34.12-2015 Магма в режиме MGM (ключ 256 бит).

5. Параметры межсетевого экранирования.

   Для пакетов, которые не защищаются IPsec применяются следующие правила фильтрации:

   5.1. На LAN интерфейсах IPv4 трафик не контролируется.

   5.2. На LAN интерфейсах IPv6 трафик заблокирован.

   5.3. На WAN интерфейсах разрешен входящий IPv4 трафик:

      5.3.1. Протокол UDP порты 500 и 4500 – для IKE и NAT-Traversal (ESP in UDP).

      5.3.2. Протокол ICMP – для проверки доступности криптошлюза и работы механизма PathMTUd.

      5.3.3. Протокол ESP (номер 50) – для работы IPsec.

      5.3.4. Весь TCP и UDP трафик, для которого есть исходящее соединение (это динамические правила, которые создаются при помощи stateful фильтрации).

      5.3.5. VRRP трафик – для работы VRRP.

5.4. На WAN интерфейсах IPv6 трафик заблокирован.

5.5. На WAN интерфейсах инспектируются все исходящие локальные и транзитные IPv4 соединения для протоколов TCP и UDP. На основе результатов инспектирования осуществляется фильтрация входящего трафика с учетом состояния сессии (stateful).

Настройка стенда

Настройка криптошлюза Hub1-n1

В Приложении представлены тексты конфигураций для криптошлюза Hub1-n1:

- текст консоли cisco-like;
- текст LSP;
- правила iptables;
- текст `keepalived.conf`.

Настройка криптошлюза Hub1-n2

В Приложении представлены тексты конфигураций для криптошлюза Hub1-n2:

- текст консоли cisco-like;
- текст LSP
- правила iptables;
- текст `keepalived.conf`.

Настройка криптошлюза Spoke1

В Приложении представлены тексты конфигураций для криптошлюза Spoke1:

- текст консоли cisco-like;
- текст LSP.

Настройка криптошлюза Spoke2

В Приложении представлены тексты конфигураций для криптошлюза Spoke2:

- текст консоли cisco-like;
- текст LSP.

Приложение

Конфигурации криптошлюза Hub1-n1

1. Консоль cisco-like:

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto ipsec security-association lifetime kilobytes unlimited
crypto isakmp keepalive 3
crypto isakmp keepalive retry-count 5
username cscons privilege 15 secret 5 $6$RiWz4IVm$qMp6sbpYnTfSUxuaJPZ9UCq4yy8/x
heIEbSmbTfMzmbQqepMD6R1b18vHTdFQt949xNXzpRXWA9dZ/gCK70z./
aaa new-model
```

```
!
!
fhrp version vrrp v3
hostname Hub1-n1
enable secret 5 HGJcyG+CRmCjINGFkW48VQ==
!
!
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile NEW_ALGS
 match identity dn
 set identity mapping
 set policy 1
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
object-group network SELF
 remark WAN IP
 host 172.16.100.2
 host 172.16.100.3
 host 100.25.100.10
!
ip access-list extended IPSEC_ACL_HUB1_LAN1_AND_SPOKE1
 permit ip 192.168.100.0 0.0.0.255 192.168.1.0 0.0.0.255
!
ip access-list extended IPSEC_ACL_HUB1_LAN2_AND_SPOKE1
 permit ip 192.168.200.0 0.0.0.255 192.168.2.0 0.0.0.255
!
ip access-list extended FW_INPUT_WAN
 permit udp any object-group SELF eq isakmp
 permit udp any object-group SELF eq non500-isakmp
 permit icmp any object-group SELF
 permit esp any object-group SELF
 permit vrrp any host 224.0.0.18
!
ipv6 default filtering deny
!
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ip inspect name INSPECT tcp
ip inspect name INSPECT udp
!
crypto map VPN 1 ipsec-isakmp
 match address IPSEC_ACL_HUB1_LAN1_AND_SPOKE1
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set security-association mss-fix out
 set local-address 172.16.100.2
 set peer 172.16.1.2
 set pre-fragmentation
 set dead-connection history off
crypto map VPN 2 ipsec-isakmp
```

```
 match address IPSEC_ACL_HUB1_LAN2_AND_SPOKE1
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set security-association mss-fix out
 set local-address 172.16.100.3
 set peer 172.16.2.2
 set pre-fragmentation
 set dead-connection history off
!
interface GigabitEthernet0/0
 ip address 100.25.100.10 255.255.255.0
 ip access-group FW_INPUT_WAN in
 crypto map VPN
 ip inspect INSPECT out
 vrrp 1 address-family ipv4
  timers advertise 3
  timers garp 5
  priority 150
  sync-group 1
  address 172.16.100.2 255.255.255.248
  exit-vrrp
 vrrp 3 address-family ipv4
  timers advertise 3
  timers garp 5
  priority 50
  sync-group 2
  address 172.16.100.3 255.255.255.248
  exit-vrrp
!
interface GigabitEthernet0/1
 ip address 192.168.100.10 255.255.255.0
 ip address 192.168.200.20 255.255.255.0 secondary
 vrrp 2 address-family ipv4
  timers advertise 3
  timers garp 5
  priority 150
  sync-group 1
  address 192.168.100.1 255.255.255.0
  exit-vrrp
 vrrp 4 address-family ipv4
  timers advertise 3
  timers garp 5
  priority 50
  sync-group 2
  address 192.168.200.1 255.255.255.0
  exit-vrrp
!
interface GigabitEthernet0/2
 no ip address
 shutdown
!
!
ip route 0.0.0.0 0.0.0.0 192.168.200.10 100
!
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
 crl download group ROOTCA http://172.16.101.15/certcrl.crl
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 58E026BFD6D625BE4582C16C6189C183
30820227308201D4A003020102021058E026BFD6D625BE4582C16C6189C18330
```

```
...
AD4F8901771632E0A0AF83

quit
!
vrrp ip route 0.0.0.0 0.0.0.0 172.16.100.1 vrid 1
end
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Thu Mar  6 09:37:58 2025

GlobalParameters(
    Title                      = "This LSP was automatically generated by CSP Converter
at Thu Mar  6 09:37:58 2025 (user: cscons)"
    Version                      = LSP_5_0
    CRLHandlingMode              = ENABLE
    PreserveIPsecSA              = FALSE
)

RoutingTable(
    Routes =
        Route(
            Destination = 0.0.0.0/0
            Gateway = 192.168.200.10
            Metric = 100
        )

)

FirewallParameters(
    TCPSynSentTimeout = 30
    TCPFinTimeout = 5
    TCPClosedTimeout = 30
    TCPSynRcvdTimeout = 30
    TCPEstablishedTimeout = 3600
    TCPHalfOpenLow = 400
    TCPHalfOpenMax = 500
    TCPSessionRateLow = 400
    TCPSessionRateMax = 500
    TCPSessionsMax = 256000
    TCPStrictnessLevel = 3
    UDPNotEstablishedTimeout = 30
    UDPEstablishedTimeout = 120
    UDPSessionsMax = 65536
)

IKETransform crypto:isakmp:policy:1
(
    CipherAlg   = "GR341215M-K256-CFB-65526"
    HashAlg     = "GR341112_256TC26-65128"
    GroupID     = VKO2_1B
    RestrictAuthenticationTo = GOST_SIGN
    LifetimeSeconds = 86400
)

ESPProposal MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP
(
    Transform* = ESPTransform
    (
        CipherAlg*          = "GR341215M-K288-MGM-33"
```

```
        LifetimeSeconds     = 3600
    )
)

FilterChain FilterChain:FW_INPUT_WAN (
    Filters = Filter (
        DestinationIP = 172.16.100.2
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.3
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 100.25.100.10
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.2
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.3
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 100.25.100.10
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.2
        ProtocolID = 1
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.3
        ProtocolID = 1
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 100.25.100.10
        ProtocolID = 1
```

```
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.2
        ProtocolID = 50
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.3
        ProtocolID = 50
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 100.25.100.10
        ProtocolID = 50
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 224.0.0.18
        ProtocolID = 112
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        Action = DROP
    )
    IPv6Filters = Filter (
        DestinationIP = ::/0
        Action = DROP
    ))

FilterChain InspectChain:INSPECT (
    Filters = Filter (
        DestinationIP = 0.0.0.0/0
        ProtocolID = 6
        Action = PASS
        ExtendedAction = inspect_tcp<>
        LogEventID = "Inspect:INSPECT:tcp"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        ProtocolID = 17
        Action = PASS
        ExtendedAction = inspect_udp<>
        LogEventID = "Inspect:INSPECT:udp"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        Action = PASS
    )
    IPv6Filters = Filter (
        DestinationIP = ::/0
        Action = DROP
    ))

IdentityEntry Remote:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
```

```
)

IdentityEntry Local:Cert:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

FilterChain IPv6Default (
    Filters = Filter (
        DestinationIP = 0.0.0.0/0
        Action = PASS
    )
    IPv6Filters = Filter (
        DestinationIP = ::/0
        Action = DROP
    ))

IKEParameters(
    FragmentSize = 576
    SALifetimeDelta = 50
    InitiatorSessionsMax = 100
    ResponderSessionsMax = 100
)

AuthMethodGOSTSign GOST:Sign:NEW_ALGS
(
    RemoteID             = Remote:NEW_ALGS
    LocalID              = Local:Cert:NEW_ALGS
    SendRequestMode      = ALWAYS
    SendCertMode         = ALWAYS
)

IKERule IKERule:VPN:1
(
    IKEPeerIPFilter = 172.16.1.2
    IKELocalIPFilter = 172.16.100.2
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:NEW_ALGS
    MainModeAuthMethod  = GOST:Sign:NEW_ALGS
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 10
)

IKERule IKERule:VPN:2
(
    IKEPeerIPFilter = 172.16.2.2
    IKELocalIPFilter = 172.16.100.3
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:NEW_ALGS
    MainModeAuthMethod  = GOST:Sign:NEW_ALGS
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 20
)

IPsecAction IPsecAction:VPN:1
(
    TunnelingParameters = TunnelEntry(
        LocalIPAddress = 172.16.100.2
        PeerAddress = 172.16.1.2
```

```
        Prefragmentation = ENABLE
    )
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    MSSFixOutgoing = TRUE
    DFHandling = COPY
    IKERule = IKERule:VPN:1
)

IPsecAction IPsecAction:VPN:2
(
    TunnelingParameters = TunnelEntry(
        LocalIPAddress = 172.16.100.3
        PeerAddress = 172.16.2.2
        Prefragmentation = ENABLE
    )
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    MSSFixOutgoing = TRUE
    DFHandling = COPY
    IKERule = IKERule:VPN:2
)

FilterChain IPsecPolicy:VPN (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 192.168.100.0/24
        DestinationIP = 192.168.1.0/24
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN:1 >
        LogEventID = "IPsec:Protect:VPN:1:IPSEC_ACL_HUB1_LAN1_AND_SPOKE1"
    ),
    Filter (
        Label = "VPN:2:IPSEC_ACL_HUB1_LAN2_AND_SPOKE1"
        SourceIP = 192.168.200.0/24
        DestinationIP = 192.168.2.0/24
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN:2 >
        LogEventID = "IPsec:Protect:VPN:2:IPSEC_ACL_HUB1_LAN2_AND_SPOKE1"
    )
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/0"
    InputFilter = FilterChain:FW_INPUT_WAN
    OutputFilter = InspectChain:INSPECT
    IPsecPolicy = IPsecPolicy:VPN
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/1"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/2"
```

```
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)
```

3. Правила `iptables`:

```
iptables -N NO_SOURCE_NAT -t nat
iptables -N SOURCE_NAT -t nat

iptables -I POSTROUTING -t nat -j NO_SOURCE_NAT -m comment --comment 'pass traffic to
chain to bypass source NAT'
iptables -A POSTROUTING -t nat -j SOURCE_NAT -m comment --comment 'pass traffic to
chain to do source NAT'

iptables -t nat -A NO_SOURCE_NAT -m mark --mark 0x8000000/0x8000000 -j ACCEPT -m comment
--comment 'local IKE packets'
iptables -t nat -A NO_SOURCE_NAT -m mark --mark 0x40000000/0x40000000 -j ACCEPT -m
comment --comment 'local ESP/NAT-T packets'
iptables -t nat -A NO_SOURCE_NAT -p 112 -j ACCEPT -m comment --comment 'local VRRP
packets'
iptables -t nat -A NO_SOURCE_NAT -s 192.168.100.0/24 -d 192.168.1.0/24 -j ACCEPT -m
comment --comment 'traffic which must be protected by IPsec'
iptables -t nat -A NO_SOURCE_NAT -s 192.168.200.0/24 -d 192.168.2.0/24 -j ACCEPT -m
comment --comment 'traffic which must be protected by IPsec'

iptables -t nat -A SOURCE_NAT -p udp --sport 500 -o eth0 -j SNAT --to-source
172.16.100.2:40500-40540 -m comment --comment 'transit IKE packets'
iptables -t nat -A SOURCE_NAT -p udp --sport 4500 -o eth0 -j SNAT --to-source
172.16.100.2:44500-44540 -m comment --comment 'transit ESP/NAT-T packets'
iptables -t nat -A SOURCE_NAT -s 192.168.100.0/24 -o eth0 -j SNAT --to-source
172.16.100.2
iptables -t nat -A SOURCE_NAT -s 192.168.200.0/24 -o eth0 -j SNAT --to-source
172.16.100.3
```

4. Конфигурационный файл `keepalived.conf`:

```
cat root@Hub1-n1:~# cat /etc/keepalived/keepalived.conf
global_defs {
  enable_dbus
}
vrrp_sync_group 1 {
  group {
    eth0_1
    eth1_2
  }
}
vrrp_sync_group 2 {
  group {
    eth0_3
    eth1_4
  }
}
vrrp_instance eth0_1 {
  version 3
  interface eth0
  virtual_routes {
    0.0.0.0/0 via 172.16.100.1 dev eth0
  }
  virtual_ipaddress {
    172.16.100.2/29 label eth0:900
  }
  priority 150
  advert_int 3
```

```
  garp_master_refresh 5
  virtual_router_id 1
}
vrrp_instance eth0_3 {
  version 3
  interface eth0
  virtual_ipaddress {
    172.16.100.3/29 label eth0:900
  }
  priority 50
  advert_int 3
  garp_master_refresh 5
  virtual_router_id 3
}
vrrp_instance eth1_2 {
  version 3
  interface eth1
  virtual_ipaddress {
    192.168.100.1/24 label eth1:900
  }
  priority 150
  advert_int 3
  garp_master_refresh 5
  virtual_router_id 2
}
vrrp_instance eth1_4 {
  version 3
  interface eth1
  virtual_ipaddress {
    192.168.200.1/24 label eth1:900
  }
  priority 50
  advert_int 3
  garp_master_refresh 5
  virtual_router_id 4
}
```

Конфигурации криптошлюза Hub1-n2

1. Консоль cisco-like:

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto ipsec security-association lifetime kilobytes unlimited
crypto isakmp keepalive 3
crypto isakmp keepalive retry-count 5
username cscons privilege 15 secret 5 $6$RiWz4IVm$qMp6sbpYnTfSUxuaJPZ9UCq4yy8/x
heIEbSmbTfMzmbQqepMD6R1b18vHTdFQt949xNXzpRXWA9dZ/gCK70z./
aaa new-model
!
!
fhrp version vrrp v3
hostname Hub1-n2
enable secret 5 HGJcyG+CRmCjINGFkW48VQ==
```

```
!
!
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile NEW_ALGS
 match identity dn
 set identity mapping
 set policy 1
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
object-group network SELF
 remark WAN IP
 host 172.16.100.2
 host 172.16.100.3
 host 100.25.100.20
!
ip access-list extended IPSEC_ACL_HUB1_LAN1_AND_SPOKE1
 permit ip 192.168.100.0 0.0.0.255 192.168.1.0 0.0.0.255
!
ip access-list extended IPSEC_ACL_HUB1_LAN2_AND_SPOKE1
 permit ip 192.168.200.0 0.0.0.255 192.168.2.0 0.0.0.255
!
ip access-list extended FW_INPUT_WAN
 permit udp any object-group SELF eq isakmp
 permit udp any object-group SELF eq non500-isakmp
 permit icmp any object-group SELF
 permit esp any object-group SELF
 permit vrrp any host 224.0.0.18
!
ipv6 default filtering deny
!
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ip inspect name INSPECT tcp
ip inspect name INSPECT udp
!
crypto map VPN 1 ipsec-isakmp
 match address IPSEC_ACL_HUB1_LAN2_AND_SPOKE1
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set security-association mss-fix out
 set local-address 172.16.100.3
 set peer 172.16.2.2
 set pre-fragmentation
 set dead-connection history off
crypto map VPN 2 ipsec-isakmp
 match address IPSEC_ACL_HUB1_LAN1_AND_SPOKE1
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set security-association mss-fix out
 set local-address 172.16.100.2
```

```
 set peer 172.16.1.2
 set pre-fragmentation
 set dead-connection history off
!
interface GigabitEthernet0/0
 ip address 100.25.100.20 255.255.255.0
 ip access-group FW_INPUT_WAN in
 crypto map VPN
 ip inspect INSPECT out
 vrrp 1 address-family ipv4
  timers advertise 3
  timers garp 5
  priority 50
  sync-group 2
  address 172.16.100.2 255.255.255.248
  exit-vrrp
 vrrp 3 address-family ipv4
  timers advertise 3
  timers garp 5
  priority 150
  sync-group 1
  address 172.16.100.3 255.255.255.248
  exit-vrrp
!
interface GigabitEthernet0/1
 ip address 192.168.200.10 255.255.255.0
 ip address 192.168.100.20 255.255.255.0 secondary
 vrrp 2 address-family ipv4
  timers advertise 3
  timers garp 5
  priority 50
  sync-group 2
  address 192.168.100.1 255.255.255.0
  exit-vrrp
 vrrp 4 address-family ipv4
  timers advertise 3
  timers garp 5
  priority 150
  sync-group 1
  address 192.168.200.1 255.255.255.0
  exit-vrrp
!
interface GigabitEthernet0/2
 no ip address
 shutdown
!
!
ip route 0.0.0.0 0.0.0.0 192.168.100.10 100
!
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
 crl download group ROOTCA http://172.16.101.15/certcrl.crl
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 58E026BFD6D625BE4582C16C6189C183
30820227308201D4A003020102021058E026BFD6D625BE4582C16C6189C18330
...
AD4F8901771632E0A0AF83

quit
!
```

```
vrrp ip route 0.0.0.0 0.0.0.0 172.16.100.1 vrid 3
end
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Thu Mar  6 09:38:55 2025

GlobalParameters(
    Title                      = "This LSP was automatically generated by CSP Converter
at Thu Mar  6 09:38:55 2025 (user: cscons)"
    Version                      = LSP_5_0
    CRLHandlingMode              = ENABLE
    PreserveIPsecSA              = FALSE
)

RoutingTable(
    Routes =
        Route(
            Destination = 0.0.0.0/0
            Gateway = 192.168.100.10
            Metric = 100
        )

)

FirewallParameters(
    TCPSynSentTimeout = 30
    TCPFinTimeout = 5
    TCPClosedTimeout = 30
    TCPSynRcvdTimeout = 30
    TCPEstablishedTimeout = 3600
    TCPHalfOpenLow = 400
    TCPHalfOpenMax = 500
    TCPSessionRateLow = 400
    TCPSessionRateMax = 500
    TCPSessionsMax = 256000
    TCPStrictnessLevel = 3
    UDPNotEstablishedTimeout = 30
    UDPEstablishedTimeout = 120
    UDPSessionsMax = 65536
)

IKETransform crypto:isakmp:policy:1
(
    CipherAlg   = "GR341215M-K256-CFB-65526"
    HashAlg     = "GR341112_256TC26-65128"
    GroupID     = VKO2_1B
    RestrictAuthenticationTo = GOST_SIGN
    LifetimeSeconds = 86400
)

ESPProposal MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP
(
    Transform* = ESPTransform
    (
        CipherAlg*          = "GR341215M-K288-MGM-33"
        LifetimeSeconds     = 3600
    )
)

FilterChain FilterChain:FW_INPUT_WAN (
```

```
    Filters = Filter (
        DestinationIP = 172.16.100.2
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.3
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 100.25.100.20
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.2
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.3
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 100.25.100.20
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.2
        ProtocolID = 1
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.3
        ProtocolID = 1
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 100.25.100.20
        ProtocolID = 1
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.2
```

```
        ProtocolID = 50
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.3
        ProtocolID = 50
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 100.25.100.20
        ProtocolID = 50
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 224.0.0.18
        ProtocolID = 112
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        Action = DROP
    )
    IPv6Filters = Filter (
        DestinationIP = ::/0
        Action = DROP
    ))

FilterChain InspectChain:INSPECT (
    Filters = Filter (
        DestinationIP = 0.0.0.0/0
        ProtocolID = 6
        Action = PASS
        ExtendedAction = inspect_tcp<>
        LogEventID = "Inspect:INSPECT:tcp"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        ProtocolID = 17
        Action = PASS
        ExtendedAction = inspect_udp<>
        LogEventID = "Inspect:INSPECT:udp"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        Action = PASS
    )
    IPv6Filters = Filter (
        DestinationIP = ::/0
        Action = DROP
    ))

IdentityEntry Remote:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

IdentityEntry Local:Cert:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)
```

```
FilterChain IPv6Default (
    Filters = Filter (
        DestinationIP = 0.0.0.0/0
        Action = PASS
    )
    IPv6Filters = Filter (
        DestinationIP = ::/0
        Action = DROP
    ))

IKEParameters(
    FragmentSize = 576
    SALifetimeDelta = 50
    InitiatorSessionsMax = 100
    ResponderSessionsMax = 100
)

AuthMethodGOSTSign GOST:Sign:NEW_ALGS
(
    RemoteID             = Remote:NEW_ALGS
    LocalID              = Local:Cert:NEW_ALGS
    SendRequestMode      = ALWAYS
    SendCertMode         = ALWAYS
)

IKERule IKERule:VPN:1
(
    IKEPeerIPFilter = 172.16.2.2
    IKELocalIPFilter = 172.16.100.3
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:NEW_ALGS
    MainModeAuthMethod  = GOST:Sign:NEW_ALGS
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 10
)

IKERule IKERule:VPN:2
(
    IKEPeerIPFilter = 172.16.1.2
    IKELocalIPFilter = 172.16.100.2
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:NEW_ALGS
    MainModeAuthMethod  = GOST:Sign:NEW_ALGS
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 20
)

IPsecAction IPsecAction:VPN:1
(
    TunnelingParameters = TunnelEntry(
        LocalIPAddress = 172.16.100.3
        PeerAddress = 172.16.2.2
        Prefragmentation = ENABLE
    )
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    MSSFixOutgoing = TRUE
```

```
    DFHandling = COPY
    IKERule = IKERule:VPN:1
)

IPsecAction IPsecAction:VPN:2
(
    TunnelingParameters = TunnelEntry(
        LocalIPAddress = 172.16.100.2
        PeerAddress = 172.16.1.2
        Prefragmentation = ENABLE
    )
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    MSSFixOutgoing = TRUE
    DFHandling = COPY
    IKERule = IKERule:VPN:2
)

FilterChain IPsecPolicy:VPN (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 192.168.200.0/24
        DestinationIP = 192.168.2.0/24
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN:1 >
        LogEventID = "IPsec:Protect:VPN:1:IPSEC_ACL_HUB1_LAN2_AND_SPOKE1"
    ),
    Filter (
        Label = "VPN:2:IPSEC_ACL_HUB1_LAN1_AND_SPOKE1"
        SourceIP = 192.168.100.0/24
        DestinationIP = 192.168.1.0/24
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN:2 >
        LogEventID = "IPsec:Protect:VPN:2:IPSEC_ACL_HUB1_LAN1_AND_SPOKE1"
    )
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/0"
    InputFilter = FilterChain:FW_INPUT_WAN
    OutputFilter = InspectChain:INSPECT
    IPsecPolicy = IPsecPolicy:VPN
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/1"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/2"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)
```

3. Правила `iptables`:

```
iptables -N NO_SOURCE_NAT -t nat
iptables -N SOURCE_NAT -t nat

iptables -I POSTROUTING -t nat -j NO_SOURCE_NAT -m comment --comment 'pass traffic to
chain to bypass source NAT'
iptables -A POSTROUTING -t nat -j SOURCE_NAT -m comment --comment 'pass traffic to
chain to do source NAT'

iptables -t nat -A NO_SOURCE_NAT -m mark --mark 0x8000000/0x8000000 -j ACCEPT -m comment
--comment 'local IKE packets'
iptables -t nat -A NO_SOURCE_NAT -m mark --mark 0x40000000/0x40000000 -j ACCEPT -m
comment --comment 'local ESP/NAT-T packets'
iptables -t nat -A NO_SOURCE_NAT -p 112 -j ACCEPT -m comment --comment 'local VRRP
packets'
iptables -t nat -A NO_SOURCE_NAT -s 192.168.100.0/24 -d 192.168.1.0/24 -j ACCEPT -m
comment --comment 'traffic which must be protected by IPsec'
iptables -t nat -A NO_SOURCE_NAT -s 192.168.200.0/24 -d 192.168.2.0/24 -j ACCEPT -m
comment --comment 'traffic which must be protected by IPsec'

iptables -t nat -A SOURCE_NAT -p udp --sport 500 -o eth0 -j SNAT --to-source
172.16.100.3:40500-40540 -m comment --comment 'transit IKE packets'
iptables -t nat -A SOURCE_NAT -p udp --sport 4500 -o eth0 -j SNAT --to-source
172.16.100.3:44500-44540 -m comment --comment 'transit ESP/NAT-T packets'
iptables -t nat -A SOURCE_NAT -s 192.168.100.0/24 -o eth0 -j SNAT --to-source
172.16.100.2
iptables -t nat -A SOURCE_NAT -s 192.168.200.0/24 -o eth0 -j SNAT --to-source
172.16.100.3
```

4. Конфигурационный файл `keepalived.conf`:

```
global_defs {
  enable_dbus
}
vrrp_sync_group 1 {
  group {
    eth0_3
    eth1_4
  }
}
vrrp_sync_group 2 {
  group {
    eth0_1
    eth1_2
  }
}
vrrp_instance eth0_1 {
  version 3
  interface eth0
  virtual_ipaddress {
    172.16.100.2/29 label eth0:900
  }
  priority 50
  advert_int 3
  garp_master_refresh 5
  virtual_router_id 1
}
vrrp_instance eth0_3 {
  version 3
  interface eth0
  virtual_routes {
    0.0.0.0/0 via 172.16.100.1 dev eth0
  }
  virtual_ipaddress {
```

```
    172.16.100.3/29 label eth0:900
  }
  priority 150
  advert_int 3
  garp_master_refresh 5
  virtual_router_id 3
}
vrrp_instance eth1_2 {
  version 3
  interface eth1
  virtual_ipaddress {
    192.168.100.1/24 label eth1:900
  }
  priority 50
  advert_int 3
  garp_master_refresh 5
  virtual_router_id 2
}
vrrp_instance eth1_4 {
  version 3
  interface eth1
  virtual_ipaddress {
    192.168.200.1/24 label eth1:900
  }
  priority 150
  advert_int 3
  garp_master_refresh 5
  virtual_router_id 4
}
```

Конфигурации криптошлюза Spoke1

1. Консоль cisco-like:

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto ipsec security-association lifetime kilobytes unlimited
crypto isakmp keepalive 3
crypto isakmp keepalive retry-count 5
username cscons privilege 15 secret 5 $6$RiWz4IVm$qMp6sbpYnTfSUxuaJPZ9UCq4yy8/x
heIEbSmbTfMzmbQqepMD6R1b18vHTdFQt949xNXzpRXWA9dZ/gCK70z./
aaa new-model
!
!
hostname Spoke1
enable secret 5 HGJcyG+CRmCjINGFkW48VQ==
!
!
!
!
!
!
!
crypto isakmp policy 1
```

```
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile NEW_ALGS
 match identity dn
 set identity mapping
 set policy 1
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
object-group network SELF
 remark WAN IP
 host 172.16.1.2
!
ip access-list extended IPSEC_ACL_HUB1_AND_SPOKE1
 permit ip 192.168.1.0 0.0.0.255 192.168.100.0 0.0.0.255
!
ip access-list extended FW_INPUT_WAN
 permit udp any object-group SELF eq isakmp
 permit udp any object-group SELF eq non500-isakmp
 permit icmp any object-group SELF
 permit esp any object-group SELF
!
ipv6 default filtering deny
!
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ip inspect name INSPECT tcp
ip inspect name INSPECT udp
!
crypto map VPN 1 ipsec-isakmp
 match address IPSEC_ACL_HUB1_AND_SPOKE1
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set security-association mss-fix out
 set peer 172.16.100.2
 set pre-fragmentation
 set dead-connection history off
!
interface GigabitEthernet0/0
 ip address 172.16.1.2 255.255.255.0
 ip access-group FW_INPUT_WAN in
 crypto map VPN
 ip inspect INSPECT out
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/2
 no ip address
 shutdown
!
!
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
 crl download group ROOTCA http://172.16.101.15/certcrl.crl
```

```
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 58E026BFD6D625BE4582C16C6189C183
30820227308201D4A003020102021058E026BFD6D625BE4582C16C6189C18330
...
AD4F8901771632E0A0AF83

quit
!
end
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Thu Mar  6 09:39:46 2025

GlobalParameters(
    Title                      = "This LSP was automatically generated by CSP Converter
at Thu Mar  6 09:39:46 2025 (user: cscons)"
    Version                       = LSP_5_0
    CRLHandlingMode               = ENABLE
    PreserveIPsecSA               = FALSE
)

RoutingTable(
    Routes =
        Route(
            Destination = 0.0.0.0/0
            Gateway = 172.16.1.1
        )

)

FirewallParameters(
    TCPSynSentTimeout = 30
    TCPFinTimeout = 5
    TCPClosedTimeout = 30
    TCPSynRcvdTimeout = 30
    TCPEstablishedTimeout = 3600
    TCPHalfOpenLow = 400
    TCPHalfOpenMax = 500
    TCPSessionRateLow = 400
    TCPSessionRateMax = 500
    TCPSessionsMax = 256000
    TCPStrictnessLevel = 3
    UDPNotEstablishedTimeout = 30
    UDPEstablishedTimeout = 120
    UDPSessionsMax = 65536
)

IKETransform crypto:isakmp:policy:1
(
    CipherAlg   = "GR341215M-K256-CFB-65526"
    HashAlg     = "GR341112_256TC26-65128"
    GroupID     = VKO2_1B
    RestrictAuthenticationTo = GOST_SIGN
    LifetimeSeconds = 86400
)

ESPProposal MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP
(
    Transform* = ESPTransform
```

```
    (
        CipherAlg*          = "GR341215M-K288-MGM-33"
        LifetimeSeconds     = 3600
    )
)

FilterChain FilterChain:FW_INPUT_WAN (
    Filters = Filter (
        DestinationIP = 172.16.1.2
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.1.2
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.1.2
        ProtocolID = 1
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.1.2
        ProtocolID = 50
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        Action = DROP
    )
    IPv6Filters = Filter (
        DestinationIP = ::/0
        Action = DROP
    ))

FilterChain InspectChain:INSPECT (
    Filters = Filter (
        DestinationIP = 0.0.0.0/0
        ProtocolID = 6
        Action = PASS
        ExtendedAction = inspect_tcp<>
        LogEventID = "Inspect:INSPECT:tcp"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        ProtocolID = 17
        Action = PASS
        ExtendedAction = inspect_udp<>
        LogEventID = "Inspect:INSPECT:udp"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        Action = PASS
    )
    IPv6Filters = Filter (
```

```
        DestinationIP = ::/0
        Action = DROP
    ))

IdentityEntry Remote:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

IdentityEntry Local:Cert:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

FilterChain IPv6Default (
    Filters = Filter (
        DestinationIP = 0.0.0.0/0
        Action = PASS
    )
    IPv6Filters = Filter (
        DestinationIP = ::/0
        Action = DROP
    ))

IKEParameters(
    FragmentSize = 576
    SALifetimeDelta = 50
    InitiatorSessionsMax = 100
    ResponderSessionsMax = 100
)

AuthMethodGOSTSign GOST:Sign:NEW_ALGS
(
    RemoteID             = Remote:NEW_ALGS
    LocalID              = Local:Cert:NEW_ALGS
    SendRequestMode      = ALWAYS
    SendCertMode         = ALWAYS
)

IKERule IKERule:VPN:1
(
    IKEPeerIPFilter = 172.16.100.2
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:NEW_ALGS
    MainModeAuthMethod  = GOST:Sign:NEW_ALGS
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 10
)

IPsecAction IPsecAction:VPN:1
(
    TunnelingParameters = TunnelEntry(
        PeerAddress = 172.16.100.2
        Prefragmentation = ENABLE
    )
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    MSSFixOutgoing = TRUE
    DFHandling = COPY
    IKERule = IKERule:VPN:1
)
```

```
FilterChain IPsecPolicy:VPN (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 192.168.1.0/24
        DestinationIP = 192.168.100.0/24
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN:1 >
        LogEventID = "IPsec:Protect:VPN:1:IPSEC_ACL_HUB1_AND_SPOKE1"
    )
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/0"
    InputFilter = FilterChain:FW_INPUT_WAN
    OutputFilter = InspectChain:INSPECT
    IPsecPolicy = IPsecPolicy:VPN
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/1"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/2"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)
```

Конфигурации криптошлюза Spoke2

1. Консоль cisco-like:

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto ipsec security-association lifetime kilobytes unlimited
crypto isakmp keepalive 3
crypto isakmp keepalive retry-count 5
username cscons privilege 15 secret 5 $6$RiWz4IVm$qMp6sbpYnTfSUxuaJPZ9UCq4yy8/x
heIEbSmbTfMzmbQqepMD6R1b18vHTdFQt949xNXzpRXWA9dZ/gCK70z./
aaa new-model
!
!
hostname Spoke2
enable secret 5 HGJcyG+CRmCjINGFkW48VQ==
!
!
!
```

```
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile NEW_ALGS
 match identity dn
 set identity mapping
 set policy 1
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
object-group network SELF
 remark WAN IP
 host 172.16.2.2
!
ip access-list extended IPSEC_ACL_HUB1_AND_SPOKE2
 permit ip 192.168.2.0 0.0.0.255 192.168.200.0 0.0.0.255
!
ip access-list extended FW_INPUT_WAN
 permit udp any object-group SELF eq isakmp
 permit udp any object-group SELF eq non500-isakmp
 permit icmp any object-group SELF
 permit esp any object-group SELF
!
ipv6 default filtering deny
!
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ip inspect name INSPECT tcp
ip inspect name INSPECT udp
!
crypto map VPN 1 ipsec-isakmp
 match address IPSEC_ACL_HUB1_AND_SPOKE2
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set security-association mss-fix out
 set peer 172.16.100.3
 set pre-fragmentation
 set dead-connection history off
!
interface GigabitEthernet0/0
 ip address 172.16.2.2 255.255.255.0
 ip access-group FW_INPUT_WAN in
 crypto map VPN
 ip inspect INSPECT out
!
interface GigabitEthernet0/1
 ip address 192.168.2.1 255.255.255.0
!
interface GigabitEthernet0/2
 no ip address
 shutdown
!
!
ip route 0.0.0.0 0.0.0.0 172.16.2.1
```

```
!
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
 crl download group ROOTCA http://172.16.101.15/certcrl.crl
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 58E026BFD6D625BE4582C16C6189C183
30820227308201D4A003020102021058E026BFD6D625BE4582C16C6189C18330
...
AD4F8901771632E0A0AF83

quit
!
end
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Thu Mar  6 09:40:29 2025

GlobalParameters(
    Title                      = "This LSP was automatically generated by CSP Converter
at Thu Mar  6 09:40:29 2025 (user: cscons)"
    Version                      = LSP_5_0
    CRLHandlingMode              = ENABLE
    PreserveIPsecSA              = FALSE
)

RoutingTable(
    Routes =
        Route(
            Destination = 0.0.0.0/0
            Gateway = 172.16.2.1
        )

)

FirewallParameters(
    TCPSynSentTimeout = 30
    TCPFinTimeout = 5
    TCPClosedTimeout = 30
    TCPSynRcvdTimeout = 30
    TCPEstablishedTimeout = 3600
    TCPHalfOpenLow = 400
    TCPHalfOpenMax = 500
    TCPSessionRateLow = 400
    TCPSessionRateMax = 500
    TCPSessionsMax = 256000
    TCPStrictnessLevel = 3
    UDPNotEstablishedTimeout = 30
    UDPEstablishedTimeout = 120
    UDPSessionsMax = 65536
)

IKETransform crypto:isakmp:policy:1
(
    CipherAlg   = "GR341215M-K256-CFB-65526"
    HashAlg     = "GR341112_256TC26-65128"
    GroupID     = VKO2_1B
    RestrictAuthenticationTo = GOST_SIGN
    LifetimeSeconds = 86400
```

```
)

ESPProposal MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP
(
    Transform* = ESPTransform
    (
        CipherAlg*          = "GR341215M-K288-MGM-33"
        LifetimeSeconds     = 3600
    )
)

FilterChain FilterChain:FW_INPUT_WAN (
    Filters = Filter (
        DestinationIP = 172.16.2.2
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.2.2
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.2.2
        ProtocolID = 1
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.2.2
        ProtocolID = 50
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        Action = DROP
    )
    IPv6Filters = Filter (
        DestinationIP = ::/0
        Action = DROP
    ))

FilterChain InspectChain:INSPECT (
    Filters = Filter (
        DestinationIP = 0.0.0.0/0
        ProtocolID = 6
        Action = PASS
        ExtendedAction = inspect_tcp<>
        LogEventID = "Inspect:INSPECT:tcp"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        ProtocolID = 17
        Action = PASS
        ExtendedAction = inspect_udp<>
        LogEventID = "Inspect:INSPECT:udp"
    ),
```

```
    Filter (
        DestinationIP = 0.0.0.0/0
        Action = PASS
    )
    IPv6Filters = Filter (
        DestinationIP = ::/0
        Action = DROP
    ))

IdentityEntry Remote:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

IdentityEntry Local:Cert:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

FilterChain IPv6Default (
    Filters = Filter (
        DestinationIP = 0.0.0.0/0
        Action = PASS
    )
    IPv6Filters = Filter (
        DestinationIP = ::/0
        Action = DROP
    ))

IKEParameters(
    FragmentSize = 576
    SALifetimeDelta = 50
    InitiatorSessionsMax = 100
    ResponderSessionsMax = 100
)

AuthMethodGOSTSign GOST:Sign:NEW_ALGS
(
    RemoteID             = Remote:NEW_ALGS
    LocalID              = Local:Cert:NEW_ALGS
    SendRequestMode      = ALWAYS
    SendCertMode         = ALWAYS
)

IKERule IKERule:VPN:1
(
    IKEPeerIPFilter = 172.16.100.3
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:NEW_ALGS
    MainModeAuthMethod  = GOST:Sign:NEW_ALGS
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 10
)

IPsecAction IPsecAction:VPN:1
(
    TunnelingParameters = TunnelEntry(
        PeerAddress = 172.16.100.3
        Prefragmentation = ENABLE
    )
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
```

```
    MSSFixOutgoing = TRUE
    DFHandling = COPY
    IKERule = IKERule:VPN:1
)

FilterChain IPsecPolicy:VPN (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 192.168.2.0/24
        DestinationIP = 192.168.200.0/24
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN:1 >
        LogEventID = "IPsec:Protect:VPN:1:IPSEC_ACL_HUB1_AND_SPOKE2"
    )
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/0"
    InputFilter = FilterChain:FW_INPUT_WAN
    OutputFilter = InspectChain:INSPECT
    IPsecPolicy = IPsecPolicy:VPN
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/1"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/2"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)
```