

Настройка Динамического Многоточечного VPN используя GRE по IPSec с EIGRP, NAT и СВАС

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Настройка](#)

[Схема сети](#)

[Конфигурации](#)

[Проверка](#)

[Устранение неполадок](#)

[Команды для устранения неполадок](#)

[Дополнительные сведения](#)

Введение

Этот документ предоставляет эталонную конфигурацию для динамической многоточечной сети VPN (DMVPN) в топологии «звезда» с использованием общей инкапсуляции маршрутов (GRE) через IPSec с усовершенствованным внутренним протоколом маршрутизации сетевых интерфейсов (EIGRP), преобразованием сетевых адресов (NAT) и контекстно-ориентированным управлением доступом (СВАС).

Предварительные условия

Требования

Перед установлением многоточечного туннеля с помощью протоколов GRE (mGRE) и IPSec следует определить политику IKE (Internet Key Exchange, обмен ключами в Интернете), используя команду `crypto isakmp policy`.

Примечание: [Поиск дополнительной информации о командах в данном документе можно выполнить с помощью средства "Command Lookup" \(Поиск команд\) \(только для зарегистрированных клиентов\).](#)

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- ПО Cisco IOS® выпуск 12.2(15)T1 на центральном маршрутизаторе и выпуск 12.3(1.6) на оконечных маршрутизаторах
- Cisco 3620 в качестве маршрутизатора концентратора, два маршрутизатора Cisco 1720 и один маршрутизатор Cisco 3620 в качестве маршрутизаторов оконечного устройства

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

Условные обозначения

[Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.](#)

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: [Поиск дополнительной информации о командах в данном документе можно выполнить с помощью средства "Command Lookup" \(Поиск команд\) \(только для зарегистрированных клиентов\).](#)

Схема сети

В данном документе используется сетевая установка, показанная на следующей схеме.

Конфигурации

В данном документе используются следующие конфигурации.

- [Центр – 3620-B](#)
- [1-е оконечное устройство – 3620-A](#)
- [2-е оконечное устройство – 1720-b](#)
- [Spoke 3 - 1720-A](#)

Центр – 3620-B

```
3620-B#write terminal Building configuration... Current
configuration : 2607 bytes ! version 12.2 service
timestamps debug datetime msec service timestamps log
datetime msec no service password-encryption ! hostname
3620-B ! logging queue-limit 100 ! memory-size iomem 10
ip subnet-zero ! ! ip cef no ip domain lookup ! !---
This is the CBAC configuration and what to inspect. !---
This will be applied outbound on the external interface.
ip inspect name in2out rcmd ip inspect name in2out ftp
ip inspect name in2out tftp ip inspect name in2out tcp
timeout 43200 ip inspect name in2out http ip inspect
name in2out udp ip audit po max-events 100 ! ! ! !---
```

```

Create an Internet Security Association and Key
Management !--- Protocol (ISAKMP) policy for Phase 1
negotiations. ! crypto isakmp policy 5 authentication
pre-share group 2 !--- Add dynamic pre-shared key. !---
Here "dmvpn" is the word that is used as the key. crypto
isakmp key dmvpnkey address 0.0.0.0 0.0.0.0 crypto
isakmp nat keepalive 20 ! ! !--- Create the Phase 2
policy for actual data encryption. crypto ipsec
transform-set dmvpnset esp-3des esp-sha-hmac ! !---
Create an IPSec profile to be applied dynamically !---
to the GRE over IPSec tunnels. crypto ipsec profile
dmvpnprof set transform-set dmvpnset ! ! no voice hpi
capture buffer no voice hpi capture destination ! ! mta
receive maximum-recipients 0 ! ! !--- This is the inside
interface. interface Loopback1 ip address 192.168.117.1
255.255.255.0 ip nat inside ! !--- This is the mGRE
interface for dynamic GRE tunnels. interface Tunnel1
description MULTI-POINT GRE TUNNEL for BRANCHES
bandwidth 1000 ip address 172.16.0.1 255.255.255.0 no ip
redirects ip mtu 1400 ip nhrp authentication dmvpn ip
nhrp map multicast dynamic ip nhrp network-id 99 ip nhrp
holdtime 300 no ip split-horizon eigrp 1 no ip mroute-
cache delay 1000 tunnel source FastEthernet0/0 tunnel
mode gre multipoint tunnel key 100000 tunnel protection
ipsec profile dmvpnprof ! !--- This is the outside
interface. interface FastEthernet0/0 ip address
14.24.117.1 255.255.0.0 ip nat outside ip access-group
100 in ip inspect in2out out no ip mroute-cache duplex
auto speed auto ! interface Serial0/0 no ip address
shutdown clockrate 2000000 no fair-queue ! interface
FastEthernet0/1 no ip address no ip mroute-cache duplex
auto speed auto ! !--- Enable a routing protocol to
send/receive dynamic !--- updates about the private
networks over the tunnels. router eigrp 1 network
172.16.0.0 0.0.0.255 network 192.168.117.0 no auto-
summary ! !--- Perform NAT on local traffic !--- going
directly out FastEthernet0/0. ip nat inside source list
110 interface FastEthernet0/0 overload ip http server no
ip http secure-server ip classless ip route 0.0.0.0
0.0.0.0 14.24.1.1 ip route 2.0.0.0 255.0.0.0 14.24.121.1
! ! ! !--- Allow ISAKMP, ESP, and GRE traffic inbound.
!--- CBAC will open other inbound access as needed.
access-list 100 permit udp any host 14.24.117.1 eq 500
access-list 100 permit esp any host 14.24.117.1 access-
list 100 permit gre any host 14.24.117.1 access-list 100
deny ip any any access-list 110 permit ip 192.168.117.0
0.0.0.255 any ! ! call rsvp-sync ! ! mgcp profile
default ! dial-peer cor custom ! ! line con 0 exec-
timeout 0 0 line aux 0 line vty 0 4 login ! ! end 3620-
B#

```

1-е оконечное устройство – 3620-A

```

3620-A#write terminal Building configuration... Current
configuration : 2559 bytes ! version 12.2 service
timestamps debug uptime service timestamps log uptime no
service password-encryption ! hostname 3620-A ! boot
system flash slot0:c3620-ik9o3s7-mz.122-15.T1.bin
logging queue-limit 100 ! memory-size iomem 15 ip
subnet-zero ! ! ip cef no ip domain lookup ! !--- This
is the CBAC configuration and what to inspect. !--- This
will be applied outbound on the external interface. ip
inspect name in2out rcmd ip inspect name in2out tftp ip
inspect name in2out udp ip inspect name in2out tcp
timeout 43200 ip inspect name in2out realaudio ip

```

```

inspect name in2out vdolive ip inspect name in2out
netshow ip audit po max-events 100 ! ! ! !--- Create an
ISAKMP policy for !--- Phase 1 negotiations. crypto
isakmp policy 5 authentication pre-share group 2 !---
Add dynamic pre-shared key. crypto isakmp key dmvpnkey
address 0.0.0.0 0.0.0.0 ! ! !--- Create the Phase 2
policy for actual data encryption. crypto ipsec
transform-set dmvpnset esp-3des esp-sha-hmac ! !---
Create an IPSec profile to be applied dynamically !---
to the GRE over IPSec tunnels. crypto ipsec profile
dmvpnprof set transform-set dmvpnset ! ! no voice hpi
capture buffer no voice hpi capture destination ! ! mta
receive maximum-recipients 0 ! ! !--- This is the inside
interface. interface Loopback1 ip address 192.168.118.1
255.255.255.0 ip nat inside ! !--- This is the mGRE
interface for dynamic GRE tunnels. interface Tunnel1
description HOST DYNAMIC TUNNEL bandwidth 1000 ip
address 172.16.0.2 255.255.255.0 no ip redirects ip mtu
1400 ip nhrp authentication dmvpn ip nhrp map 172.16.0.1
14.24.117.1 ip nhrp map multicast 14.24.117.1 ip nhrp
network-id 99 ip nhrp holdtime 300 ip nhrp nhs
172.16.0.1 no ip mroute-cache delay 1000 tunnel source
Ethernet0/0 tunnel mode gre multipoint tunnel key 100000
tunnel protection ipsec profile dmvpnprof ! !--- This is
the outside interface. interface Ethernet0/0 ip address
14.24.118.1 255.255.0.0 ip nat outside ip inspect in2out
out ip access-group 100 in no ip mroute-cache half-
duplex ! interface Ethernet0/1 no ip address half-duplex
! interface Ethernet0/2 no ip address shutdown half-
duplex ! interface Ethernet0/3 no ip address shutdown
half-duplex ! !--- Enable a routing protocol to
send/receive dynamic !--- updates about the private
networks over the tunnel. router eigrp 1 network
172.16.0.0 0.0.0.255 network 192.168.118.0 no auto-
summary ! !--- Perform NAT on local traffic !--- going
directly out Ethernet0/0. ip nat inside source list 110
interface Ethernet0/0 overload ip http server no ip http
secure-server ip classless ip route 0.0.0.0 0.0.0.0
14.24.1.1 ! ! !--- Allow ISAKMP, ESP, and GRE traffic
inbound. !--- CBAC will open inbound access as needed.
access-list 100 permit udp any host 14.24.118.1 eq 500
access-list 100 permit esp any host 14.24.118.1 access-
list 100 permit gre any host 14.24.118.1 access-list 100
deny ip any any access-list 110 permit ip 192.168.118.0
0.0.0.255 any ! ! call rsvp-sync ! ! mgcp profile
default ! dial-peer cor custom ! ! line con 0 exec-
timeout 0 0 line aux 0 line vty 0 4 login ! ! end 3620-
A#

```

2-е оконечное устройство – 1720-b

```

1720-b#write terminal Building configuration... Current
configuration : 2543 bytes ! version 12.2 service
timestamps debug uptime service timestamps log uptime no
service password-encryption ! hostname 1720-b ! boot
system flash flash:c1700-ny-mz.122-8.YJ logging queue-
limit 100 enable password cisco ! username 7206-B
password 0 cisco ip subnet-zero ! ! no ip domain lookup
! ip cef !--- This is the CBAC configuration and what to
inspect. !--- This will be applied outbound on the
external interface. ip inspect name in2out rcmd ip
inspect name in2out tftp ip inspect name in2out udp ip
inspect name in2out tcp timeout 43200 ip inspect name
in2out realaudio ip inspect name in2out vdolive ip
inspect name in2out netshow ip audit po max-events 100 !

```

```

! vpdn-group 1 request-dialin protocol pppoe ! ! !---
Create an ISAKMP policy for !--- Phase 1 negotiations.
crypto isakmp policy 5 authentication pre-share group 2
!--- Add dynamic pre-shared key. crypto isakmp key
dmvpnkey address 0.0.0.0 0.0.0.0 ! ! !--- Create the
Phase 2 policy for actual data encryption. crypto ipsec
transform-set dmvpnset esp-3des esp-sha-hmac ! !---
Create an IPsec profile to be applied dynamically !---
to the GRE over IPsec tunnels. crypto ipsec profile
dmvpnprof set transform-set dmvpnset ! ! !--- This is
the inside interface. interface Loopback1 ip address
192.168.116.1 255.255.255.0 ip nat inside ! !--- This is
the mGRE interface for dynamic GRE tunnels. interface
Tunnel1 description HOST DYNAMIC TUNNEL bandwidth 1000
ip address 172.16.0.3 255.255.255.0 no ip redirects ip
mtu 1400 ip nhrp authentication dmvpn ip nhrp map
172.16.0.1 14.24.117.1 ip nhrp map multicast 14.24.117.1
ip nhrp network-id 99 ip nhrp holdtime 300 ip nhrp nhs
172.16.0.1 no ip mroute-cache delay 1000 tunnel source
Dialer1 tunnel mode gre multipoint tunnel key 100000
tunnel protection ipsec profile dmvpnprof ! interface
Ethernet0 no ip address half-duplex ! interface
FastEthernet0 no ip address no ip mroute-cache speed
auto pppoe enable pppoe-client dial-pool-number 1 ! !---
This is the outside interface. interface Dialer1 ip
address 2.2.2.10 255.255.255.0 ip inspect in2out out ip
access-group 100 in encapsulation ppp dialer pool 1
dialer-group 1 ppp authentication pap chap callin ! !---
Enable a routing protocol to send/receive dynamic !---
updates about the private networks. router eigrp 1
network 172.16.0.0 0.0.0.255 network 192.168.116.0 no
auto-summary ! !--- Perform NAT on local traffic !---
going directly out Dialer1. ip nat inside source list
110 interface Dialer1 overload ip classless ip route
0.0.0.0 0.0.0.0 Dialer1 no ip http server no ip http
secure-server ! ! ! !--- Allow ISAKMP, ESP, and GRE
traffic inbound. !--- CBAC will open inbound access as
needed. access-list 100 permit udp any host 14.24.116.1
eq 500 access-list 100 permit esp any host 14.24.116.1
access-list 100 permit gre any host 14.24.116.1 access-
list 100 deny ip any any access-list 110 permit ip
192.168.116.0 0.0.0.255 any dialer-list 1 protocol ip
permit ! ! ! line con 0 exec-timeout 0 0 line aux 0 line
vty 0 4 login ! no scheduler allocate end 1720-b#

```

Spoke 3 - 1720-A

```

1720-A#write terminal Building configuration... Current
configuration : 1770 bytes ! version 12.2 service
timestamps debug datetime msec service timestamps log
datetime msec no service password-encryption ! hostname
1720-A ! logging queue-limit 100 ! memory-size iomem 25
ip subnet-zero ! ! ! ip cef !--- This is the CBAC
configuration and what to inspect. !--- This will be
applied outbound on the external interface. ip inspect
name in2out rcmd ip inspect name in2out tftp ip inspect
name in2out udp ip inspect name in2out tcp timeout 43200
ip inspect name in2out realaudio ip inspect name in2out
vdolive ip inspect name in2out netshow ip audit po max-
events 100 ! ! !--- Create an ISAKMP policy for !---
Phase 1 negotiations. crypto isakmp policy 5
authentication pre-share group 2 !--- Add dynamic pre-
shared key. crypto isakmp key dmvpnkey address 0.0.0.0
0.0.0.0 ! ! !--- Create the Phase 2 policy for actual
data encryption. crypto ipsec transform-set dmvpnset

```

```

esp-3des esp-sha-hmac ! !--- Create an IPSec profile to
be applied dynamically !--- to the GRE over IPSec
tunnels. crypto ipsec profile dmvpnprof set transform-
set dmvpnset ! !--- This is the inside interface.
interface Loopback1 ip address 192.168.120.1
255.255.255.0 ip nat inside ! !--- This is the mGRE
interface for dynamic GRE tunnels. interface Tunnel1
description HOST DYNAMIC TUNNEL bandwidth 1000 ip
address 172.16.0.4 255.255.255.0 no ip redirects ip mtu
1400 ip nhrp authentication dmvpn ip nhrp map 172.16.0.1
14.24.117.1 ip nhrp map multicast 14.24.117.1 ip nhrp
network-id 99 ip nhrp holdtime 300 ip nhrp nhs
172.16.0.1 no ip mroute-cache delay 1000 tunnel source
FastEthernet0 tunnel mode gre multipoint tunnel key
100000 tunnel protection ipsec profile dmvpnprof !
interface Ethernet0 no ip address no ip mroute-cache
half-duplex ! !--- This is the outside interface.
interface FastEthernet0 ip address 14.24.120.1
255.255.0.0 ip nat outside ip inspect in2out out ip
access-group 100 in no ip mroute-cache speed auto ! !---
Enable a routing protocol to send/receive dynamic !---
updates about the private networks. router eigrp 1
network 172.16.0.0 0.0.0.255 network 192.168.120.0 no
auto-summary ! !--- Perform NAT on local traffic !---
going directly out FastEthernet0. ip nat inside source
list 110 interface FastEthernet0 overload ip classless
ip route 0.0.0.0 0.0.0.0 14.24.1.1 no ip http server no
ip http secure-server ! ! ! !--- Allow ISAKMP, ESP, and
GRE traffic inbound. !--- CBAC will open inbound access
as needed. access-list 100 permit udp any host
14.24.116.1 eq 500 access-list 100 permit esp any host
14.24.116.1 access-list 100 permit gre any host
14.24.116.1 access-list 100 deny ip any any access-list
110 permit ip 192.168.120.0 0.0.0.255 any ! ! ! line con
0 exec-timeout 0 0 line aux 0 line vty 0 4 login ! no
scheduler allocate end 1720-A#

```

Проверка

В этом разделе содержатся сведения, которые помогают убедиться в надлежащей работе конфигурации.

Некоторые команды `show` поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды `show`.

- `show crypto isakmp sa` — выводит состояние контекста безопасности (SA) по протоколу ISAKMP.
- `show crypto engine connections active` – выводит количество шифровок или дешифровок на контекст безопасности.
- `show crypto ipsec sa` – выводит статистику по активным туннелям.
- `show ip route` – выводит таблицу маршрутизации.
- `show ip eigrp neighbor`– показывает соседние узлы EIGRP.
- `show ip nhrp` — показывает кэш протокола разрешения следующего перехода IP (NHRP) с возможностью ограничения динамическими или статическими записями кэша для определенного интерфейса.
- `show crypto socket`– показывает таблицу сокетов шифрования между NHRP и IPSec.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

Примечание: Прежде чем применять команды отладки, ознакомьтесь с разделом "Важные сведения о командах отладки".

- `debug crypto ipsec`– показывает события IPSec.
- `debug crypto isakmp` – отображает сообщения о событиях IKE.
- `debug crypto engine`– выводит информацию о криптографическом модуле.
- `debug crypto socket`– показывает сведения о таблице сокетов между NHRP и IPSec.
- `debug nhrp`– показывает сведения о событиях NHRP.
- `debug nhrp packet`– показывает сведения о пакетах NHRP.
- `debug tunnel protection`– показывает сведения о динамических туннелях GRE.

[Дополнительные сведения об устранении проблем IPSec см. в документе Основные сведения об устранении проблем в IP-безопасности и об использовании команд отладки.](#)

Дополнительные сведения

- [Обзор DMVPN и Cisco IOS](#)
- [Страница поддержки IPSec](#)
- [Cisco Systems – техническая поддержка и документация](#)