

Настройка динамических многоточечных виртуальных частных сетей с использованием протокола GRE через протокол IPsec с помощью протоколов OSPF, NAT и межсетевого экрана Cisco IOS

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Настройка](#)

[Схема сети](#)

[Конфигурации](#)

[Проверка](#)

[Устранение неполадок](#)

[Команды устранения неполадок](#)

[Дополнительные сведения](#)

[Введение](#)

В этом документе приводится пример конфигурации для динамических многоточечных виртуальных частных сетей (Dynamic Multipoint Virtual Private Network, DMVPN) с использованием протокола GRE (generic routing encapsulation, протокол туннелирования сетевых пакетов) через IPsec (IP Security, межсетевой протокол безопасности) с помощью протоколов OSPF (Open Shortest Path First, протокол предпочтения кратчайшего пути), NAT (Network Address Translation, преобразование сетевых адресов) и межсетевого экрана Cisco IOS®.

[Предварительные условия](#)

[Требования](#)

Прежде чем устанавливать многоточечный туннель с помощью протоколов GRE (mGRE, multipoint GRE) и IPsec, следует определить политику IKE (Internet Key Exchange, обмен ключами в Интернете), используя команду `crypto isakmp policy`.

Примечание. См. дополнительные сведения о командах, используемых в данном документе, в [Средстве поиска команд](#) (только для [зарегистрированных](#) пользователей).

[Используемые компоненты](#)

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

- Cisco IOS® версии 12.2(15)T1 на маршрутизаторе концентратора и Cisco IOS версии 12.3(1.6) на конечных маршрутизаторах;
- Cisco 3620 в качестве маршрутизатора концентратора, два маршрутизатора Cisco 1720 и один маршрутизатор Cisco 3620 в качестве конечных маршрутизаторов.

Данные для этого документа были получены при тестировании указанных устройств в специально созданных лабораторных условиях. Все устройства, используемые в этом документе, запускались с чистой (заданной по умолчанию) конфигурацией. Если сеть работает в реальных условиях, при использовании каждой команды следует адекватно оценивать ее потенциальное воздействие.

Условные обозначения

Дополнительные сведения о применяемых в документе обозначениях см. в статье [Условные обозначения, используемые в технической документации Cisco](#).

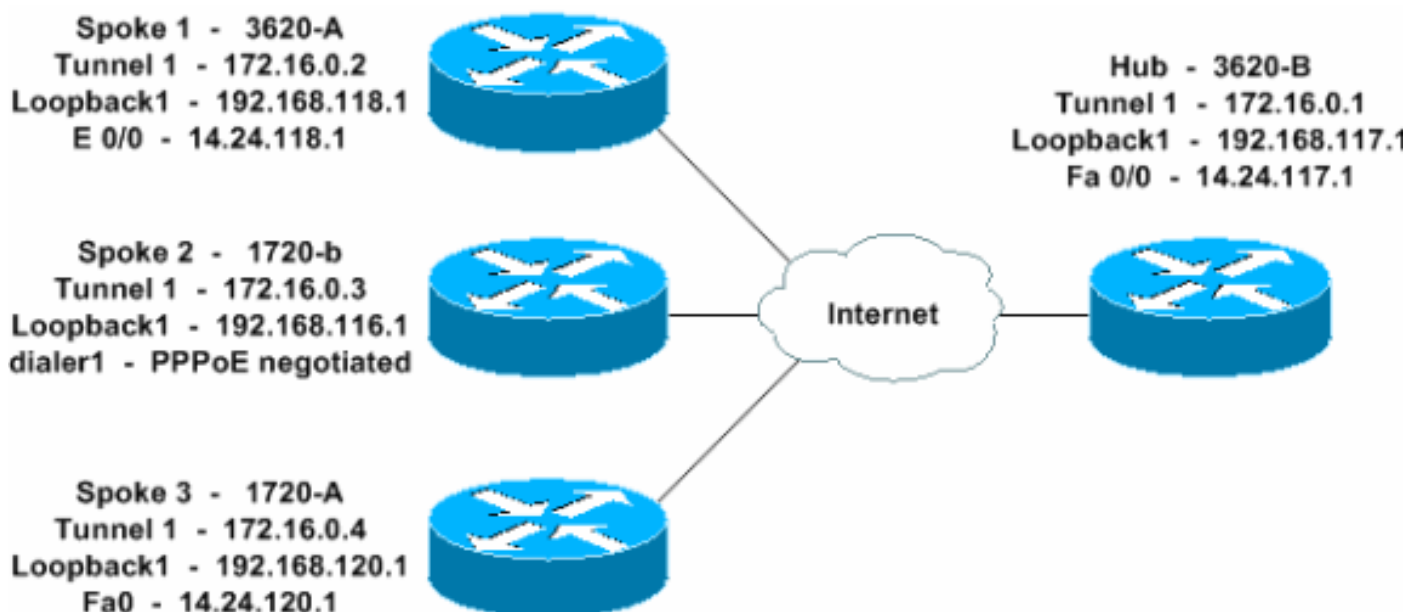
Настройка

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

Примечание. См. дополнительные сведения о командах, используемых в данном документе, в [Средстве поиска команд](#) (только для [зарегистрированных](#) пользователей).

Схема сети

В этом документе использованы параметры данной сети.



Конфигурации

В данном документе используются следующие конфигурации:

- [концентратор – 3620-B;](#)
- [1-ое оконечное устройство – 3620-A;](#)
- [2-ое оконечное устройство – 1720-b;](#)
- [3-е оконечное устройство –1720-A.](#)

Концентратор – 3620-B

```

W2N-6.16-3620-B#write terminal
Building configuration...

Current configuration : 2613 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname W2N-6.16-3620-B
!
logging queue-limit 100
!
memory-size iomem 10
ip subnet-zero
!
!
ip cef
no ip domain lookup
!
!--- Cisco IOS , . !--- . 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 ! ! ! !--- ISAKMP !--- 1- .
crypto isakmp policy 5 authentication pre-share group 2
!--- . crypto isakmp key dmvpnkey address 0.0.0.0
0.0.0.0 crypto isakmp nat keepalive 20 ! ! !--- 2-
. crypto ipsec transform-set dmvpnset esp-3des esp-sha-
hmac ! !--- IPsec, !--- GRE IPsec. crypto ipsec
profile dmvpnprof set transform-set dmvpnset ! ! ! ! !
! ! ! ! ! no voice hpi capture buffer no voice hpi
capture destination ! ! mta receive maximum-recipients 0
! ! ! !--- . interface Loopback1 ip address
192.168.117.1 255.255.255.0 ip nat inside ! !--- GRE,
!--- GRE. 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 1416 ip
nhrp authentication dmvpn ip nhrp map multicast dynamic
ip nhrp network-id 99 ip nhrp holdtime 300 no ip route-
cache ip ospf network broadcast no ip mroute-cache delay
1000 tunnel source FastEthernet0/0 tunnel mode gre
multipoint tunnel key 100000 tunnel protection ipsec
profile dmvpnprof ! !--- . 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 ! !--- !--- .
router ospf 1 log-adjacency-changes network 172.16.0.0
0.0.0.255 area 0 network 192.168.117.0 0.0.0.255 area 0
! !--- NAT. ip nat inside source route-map nonat
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 ! ! !
!--- ISAKMP, ESP GRE. !--- Cisco IOS .
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 !--- NAT. access-list 110 deny ip
192.168.117.0 0.0.0.255 192.168.118.0 0.0.0.255 access-
list 110 deny ip 192.168.117.0 0.0.0.255 192.168.116.0
0.0.0.255 access-list 110 deny ip 192.168.117.0
0.0.0.255 192.168.120.0 0.0.0.255 access-list 110 permit
ip 192.168.117.0 0.0.0.255 any ! !--- NAT. route-
map nonat permit 10 match ip address 110 ! 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 W2N-6.16-3620-B#

```

1-е оконечное устройство –3620-A

```

W2N-6.16-3620-A#write terminal
Building configuration...

Current configuration : 2678 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname W2N-6.16-3620-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
!
!--- Cisco IOS , . !--- . 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 ! ! ! !--- ISAKMP !--- 1- . crypto isakmp
policy 5 authentication pre-share group 2 !--- .
crypto isakmp key dmvpnkey address 0.0.0.0 0.0.0.0 ! !
!--- 2- . crypto ipsec transform-set dmvpnset esp-
3des esp-sha-hmac ! !--- IPsec, !--- GRE IPsec.
crypto ipsec profile dmvpnprof set transform-set
dmvpnset ! ! ! ! ! ! ! ! ! ! no voice hpi capture
buffer no voice hpi capture destination ! ! mta receive
maximum-recipients 0 ! ! ! !--- . interface Loopback1
ip address 192.168.118.1 255.255.255.0 ip nat inside !
!--- GRE, !--- GRE. interface Tunnell
description HOST DYNAMIC TUNNEL bandwidth 1000 ip
address 172.16.0.2 255.255.255.0 no ip redirects ip mtu
1416 ip nhrp authentication dmvpn ip nhrp map multicast
dynamic 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 route-cache ip
ospf network broadcast no ip mroute-cache delay 1000
tunnel source Ethernet0/0 tunnel mode gre multipoint

```

```

tunnel key 100000 tunnel protection ipsec profile
dmvpnprof ! !--- . interface Ethernet0/0 ip address
14.24.118.1 255.255.0.0 ip nat outside ip access-group
100 in ip inspect in2out out 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 ! !--- !--- . router ospf 1 log-
adjacency-changes redistribute connected network
172.16.0.0 0.0.0.255 area 0 network 192.168.118.0
0.0.0.255 area 0 ! !--- NAT. ip nat inside source
route-map nonat 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 ip route 2.0.0.0 255.0.0.0
14.24.121.1 ! ! ! !--- ISAKMP, ESP GRE. !--- Cisco
IOS . access-list 100 permit udp any host
14.24.118.1 eq 500 access-list 100 premit 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 !---
NAT. access-list 110 deny ip 192.168.118.0 0.0.0.255
192.168.117.0 0.0.0.255 access-list 110 deny ip
192.168.118.0 0.0.0.255 192.168.116.0 0.0.0.255 access-
list 110 deny ip 192.168.118.0 0.0.0.255 192.168.120.0
0.0.0.255 access-list 110 permit ip 192.168.118.0
0.0.0.255 any ! !--- NAT. route-map nonat permit
10 match ip address 110 ! 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 W2N-6.16-3620-A#

```

2-ое оконечное устройство – 1720-b

```

1720-b#write terminal
Building configuration...

Current configuration : 2623 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 1720-b
!
logging queue-limit 100
enable password cisco
!
username 7206-B password 0 cisco
ip subnet-zero
!
!
no ip domain lookup
!
ip cef
!--- Cisco IOS , . !--- . 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 !
! ! ! ! !--- ISAKMP !--- 1- . crypto isakmp policy 5
authentication pre-share group 2 !--- . crypto
isakmp key dmvpnkey address 0.0.0.0 0.0.0.0 ! ! !---
2- . crypto ipsec transform-set dmvpnset esp-3des
esp-sha-hmac ! !--- IPsec, !--- GRE IPsec.

```

```

crypto ipsec profile dmvpnprof set transform-set
dmvpnset ! ! ! ! ! !--- . interface Loopback1 ip
address 192.168.116.1 255.255.255.0 ip nat inside ! !---
GRE, !--- GRE. interface Tunnel1 description
HOST DYNAMIC TUNNEL bandwidth 1000 ip address 172.16.0.3
255.255.255.0 no ip redirects ip mtu 1416 ip nhrp
authentication dmvpn ip nhrp map multicast dynamic 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 route-cache ip ospf network
broadcast 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 ! !---
. 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 ! !--- !--- .
router ospf 1 log-adjacency-changes redistribute
connected network 172.16.0.0 0.0.0.255 area 0 network
192.168.116.0 0.0.0.255 area 0 ! !--- NAT. ip nat
inside source route-map nonat interface Dialer1 overload
ip classless ip route 0.0.0.0 0.0.0.0 14.24.1.1 ip route
0.0.0.0 0.0.0.0 Dialer1 no ip http server no ip http
secure-server ! ! ! !--- ISAKMP, ESP GRE. !---
Cisco IOS . 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 !---
NAT. access-list 110 deny ip 192.168.116.0 0.0.0.255
192.168.117.0 0.0.0.255 access-list 110 deny ip
192.168.116.0 0.0.0.255 192.168.118.0 0.0.0.255 access-
list 110 deny ip 192.168.116.0 0.0.0.255 192.168.120.0
0.0.0.255 access-list 110 permit ip 192.168.116.0
0.0.0.255 any dialer-list 1 protocol ip permit ! !---
NAT. route-map nonat permit 10 match ip address 110 !
! line con 0 exec-timeout 0 0 line aux 0 line vty 0 4
login ! no scheduler allocate end 1720-b#

```

3-е оконечное устройство –1720-A

```

W2N-6.16-1720-A#write terminal
Building configuration...

Current configuration : 2303 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname W2N-6.16-1720-A
!
logging queue-limit 100
!
memory-size iomem 25
ip subnet-zero
!
!
no ip domain lookup
!
ip cef
!--- Cisco IOS , . !--- . 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 notify
log ip audit po max-events 100 ! ! ! ! !--- ISAKMP !-
-- 1- . crypto isakmp policy 5 authentication pre-share
group 2 !--- . crypto isakmp key dmvpnkey address
0.0.0.0 0.0.0.0 ! ! !--- 2- . crypto ipsec
transform-set dmvpnset esp-3des esp-sha-hmac ! !---
IPsec, !--- GRE IPsec. crypto ipsec profile
dmvpnprof set transform-set dmvpnset ! ! ! ! !--- .
interface Loopback1 ip address 192.168.120.1
255.255.255.0 ip nat inside ! !--- GRE, !---
GRE. interface Tunnel1 description HOST DYNAMIC TUNNEL
bandwidth 1000 ip address 172.16.0.4 255.255.255.0 no ip
redirects ip mtu 1416 ip nhrp authentication dmvpn ip
nhrp map multicast dynamic 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 ip ospf network broadcast 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 ! !--- . 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 ! !--- !--- .
router ospf 1 log-adjacency-changes redistribute
connected network 172.16.0.0 0.0.0.255 area 0 network
192.168.120.0 0.0.0.255 area 0 ! !--- NAT. ip nat
inside source route-map nonat interface FastEthernet0
overload 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 no ip http server
no ip http secure-server ! ! ! !--- ISAKMP, ESP GRE.
!--- Cisco IOS . 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 !---
NAT. access-list 110 deny ip 192.168.120.0 0.0.0.255
192.168.116.0 0.0.0.255 access-list 110 deny ip
192.168.120.0 0.0.0.255 192.168.117.0 0.0.0.255 access-
list 110 deny ip 192.168.120.0 0.0.0.255 192.168.118.0
0.0.0.255 access-list 110 permit ip 192.168.120.0
0.0.0.255 any ! !--- NAT. route-map nonat permit
10 match ip address 110 ! ! line con 0 exec-timeout 0 0
line aux 0 line vty 0 4 login ! end W2N-6.16-1720-A#

```

Проверка

В этом разделе приводятся способы проверки работы конфигурации.

Приложение [Интерпретатор выходных данных](#) (только для [зарегистрированных](#) пользователей) поддерживает некоторые команды **show**. Используйте этот интерпретатор для просмотра результатов анализа выходных данных команды **show**.

- **show crypto isakmp sa** – выводит состояние контекста безопасности (security association, SA) по протоколу ISAKMP (Internet Security Association and Key Management Protocol, протокол контекстов безопасности и управления ключами в Интернете).

- **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 ospf neighbor** – выводит информацию протокола OSPF о соседних узлах для каждого интерфейса.
- **show ip nhrp** – выводит кэш IP-протокола NHRP (Next Hop Resolution Protocol, протокол разрешения следующего перехода), при необходимости ограничиваемый динамическими или статическими записями кэша для определенного интерфейса.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды устранения неполадок

Примечание. Дополнительные сведения о командах **debug** см. в документе [Важные сведения о командах debug](#).

- **debug crypto ipsec** – отображает события протокола IPSec.
- **debug crypto isakmp** – отображает сообщения о событиях протокола IKE.
- **debug crypto engine** – отображает информацию от криптографического модуля.

Дополнительные сведения об устранении неисправностей протокола IPSec см. в документе [Основные сведения об устранении неполадок протокола IP Security и использовании команд отладки debug](#).

Дополнительные сведения

- [Устранение неполадок конфигураций межсетевого экрана Cisco IOS](#)
- [Обзор DMVPN и Cisco IOS](#)
- [Протоколы согласования IPsec/IKE](#)
- [Cisco Systems – Техническая поддержка и документация](#)