

# 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 для 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](#)

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: [Используйте инструмент Command Lookup \(только для зарегистрированных](#)

[пользователей\) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.](#)

## Используемые компоненты

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

- Cisco IOS® версии 12.2(15)T1 на маршрутизаторе концентратора и Cisco IOS версии 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, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

## Условные обозначения

[Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.](#)

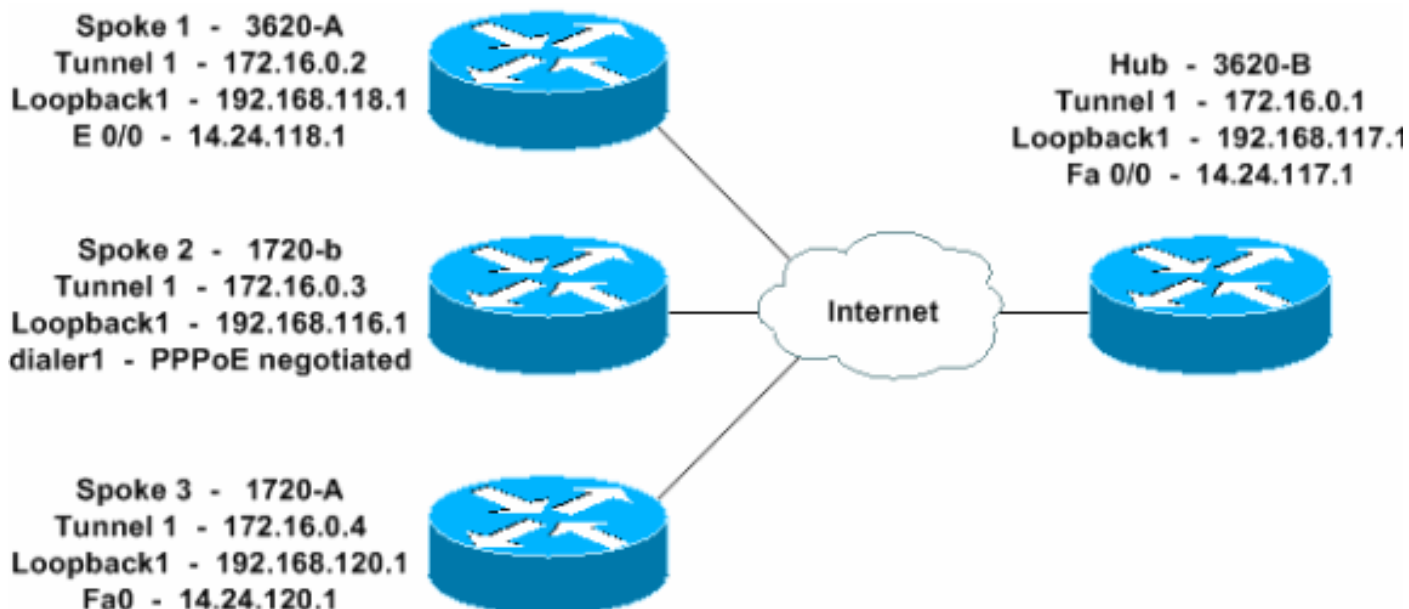
## Настройка

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

**Примечание:** [Используйте инструмент Command Lookup \(только для зарегистрированных пользователей\) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.](#)

## Схема сети

В настоящем документе используется следующая схема сети.



## Конфигурации

Эти конфигурации используются в данном документе.

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

### **Центр – 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 ! !--- This is the Cisco IOS
Firewall configuration and what to inspect. !--- This is
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. 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
inbound interface. interface Loopback1 ip address
192.168.117.1 255.255.255.0 ip nat inside ! !--- Create
a GRE tunnel template to be applied !--- to all the
dynamically created 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 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 ! !---
This is the outbound 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. 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 ! !--- Except the private
network traffic from the NAT process. 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 ! ! ! !--- Allow ISAKMP,
ESP, and GRE traffic inbound. !--- Cisco IOS Firewall
opens other inbound access as needed. access-list 100
permit udp any host 14.24.117.1 eq 500 access-list 100
premit 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
!--- Except the private network traffic from the NAT
process. 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 ! !--- Except the private network traffic
from the NAT process. 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 !
!--- This is the Cisco IOS Firewall configuration and
what to inspect. !--- This is 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 inbound interface. interface
Loopback1 ip address 192.168.118.1 255.255.255.0 ip nat
inside ! !--- Create a GRE tunnel template to be applied
to !--- all the dynamically created GRE tunnels.
interface Tunnell1 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 ! !--- This is the
outbound interface. 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 ! !--- Enable a routing protocol to
send/receive dynamic !--- updates about the private
networks. 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 ! !--- Except
the private network traffic from the NAT process. 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 ! ! ! !--- Allow ISAKMP,
ESP, and GRE traffic inbound. !--- Cisco IOS Firewall
opens 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 !---
Except the private network traffic from the NAT process.
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 ! !--- Except the private network traffic
from the NAT process. 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-е 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 !--- This is the Cisco IOS Firewall
configuration and what to inspect. !--- This is 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 inbound interface. interface
Loopback1 ip address 192.168.116.1 255.255.255.0 ip nat
inside ! !--- Create a GRE tunnel template to be applied
to !--- all the dynamically created GRE tunnels.
interface Tunnell 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 ! !--- This is the
outbound 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 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
! !--- Except the private network traffic from the NAT
process. 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 ! ! ! !--- Allow ISAKMP,
ESP, and GRE traffic inbound. !--- Cisco IOS Firewall
opens 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 !---
Except the private network traffic from the NAT process.
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 ! !---
Except the private network traffic from the NAT process.
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#

```

### Spoke 3 - 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 !--- This is the Cisco IOS
Firewall configuration and what to inspect. !--- This is
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 notify
log 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 inbound interface. interface Loopback1 ip address
192.168.120.1 255.255.255.0 ip nat inside ! !--- Create
a GRE tunnel template to be applied to !--- all the

```



```
dynamically created GRE tunnels. interface Tunnell
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 ! !--- This is the outbound 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 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 ! !--- Except the private network
traffic from the NAT process. 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 ! ! ! !--- Allow ISAKMP, ESP, and GRE
traffic inbound. !--- Cisco IOS Firewall opens 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 ! !--- Except
the private network traffic from the NAT process.
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 ! !--- Except the private network traffic
from the NAT process. 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

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. Посредством OIT можно анализировать выходные данные команд 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 ospf neighbor** – выводит информацию протокола OSPF о соседних узлах для каждого интерфейса.

- `show ip nhrp` — показывает кэш протокола разрешения следующего перехода IP (NHRP) с возможностью ограничения динамическими или статическими записями кэша для определенного интерфейса.

## Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

### Команды для устранения неполадок

**Примечание:** [Обратитесь к документу Важная информация о командах отладки, прежде чем использовать команды debug.](#)

- `debug crypto ipsec`– показывает события IPSec.
- `debug crypto isakmp` – отображает сообщения о событиях IKE.
- `debug crypto engine`– выводит информацию о криптографическом модуле.

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

## Дополнительные сведения

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