

# 使用IPSec的GRE通过OSPF、NAT和Cisco IOS防火墙配置动态多点VPN

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

[故障排除命令](#)

[相关信息](#)

## 简介

本文档通过开放最短路径优先 (OSPF)、网络地址转换 (NAT) 和 Cisco IOS® 防火墙使用基于 IPSec 的通用路由封装 (GRE) 提供了动态多点 VPN (DMVPN) 的示例配置。

## 先决条件

### 要求

必须先使用 `crypto isakmp policy` 命令定义 Internet 密钥交换 (IKE) 策略，然后才能创建多点 GRE (mGRE) 和 IPsec 隧道。

**注意：** 使用 [命令查找工具](#) ( [仅限注册用户](#) ) 可获取有关本部分所使用命令的详细信息。

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 中心路由器上的 Cisco IOS® 软件版本 12.2(15)T1 和分支路由器上的 Cisco IOS 软件版本 12.3(1.6)
- Cisco 3620 作为中心路由器，两个 Cisco 1720 路由器和一个 Cisco 3620 路由器作为分支路由器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始 (默认) 配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

## 配置

本部分提供有关如何配置本文档所述功能的信息。

**注意：** 使用 [命令查找工具](#) ( [仅限注册用户](#) ) 可获取有关本部分所使用命令的详细信息。

## 网络图

本文档使用此网络设置。

## 配置

本文档使用以下配置。

- [中心 - 3620-B](#)
- [分支 1 - 3620-A](#)
- [分支 2 - 1720-b](#)
- [分支 3 - 1720-A](#)

### 中心 - 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 Tunnell
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#

```

## 分支 1 - 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 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 ! !--- 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#

```

## 分支 2 - 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 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 ! !--- 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#

```

### 分支 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 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 ! !--- 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#

```

**验证**

使用本部分可确认配置能否正常运行。

[命令输出解释程序 \( 仅限注册用户 \)](#) (OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show crypto isakmp sa** - 显示 ISAKMP 安全关联 (SA) 的状态。
- **show crypto engine connections active** - 按 SA 显示总加密/解密。
- **show crypto ipsec sa** - 显示有关活动隧道的统计数据。
- **show ip route** - 显示路由表。
- **show ip ospf neighbor** - 按接口显示 OSPF 邻接设备信息。
- **show ip nhrp** - 显示 IP 下一跳解析协议 (NHRP) 缓存，可选择限制为特定接口的动态或静态缓存条目。

## [故障排除](#)

本部分提供的信息可用于对配置进行故障排除。

### [故障排除命令](#)

**注意：** 发出 **debug** 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

- **debug crypto ipsec** — 显示 IPsec 事件。
- **debug crypto isakmp** — 显示关于 IKE 事件的消息。
- **debug crypto engine** - 显示来自加密引擎的信息。

有关 IPsec 故障排除的其他信息，请参阅 [IP 安全故障排除 - 了解和使用 debug 命令](#)。

## [相关信息](#)

- [对 Cisco IOS 防火墙配置进行故障排除](#)
- [DMVPN 和 Cisco IOS 概述](#)
- [IPsec 协商/IKE 协议](#)
- [技术支持和文档 - Cisco Systems](#)