

OSPF, NAT 및 Cisco IOS 방화벽에서 GRE Over IPsec을 사용하여 동적 멀티포인트 VPN 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[구성](#)

[네트워크 다이어그램](#)

[구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[문제 해결 명령](#)

[관련 정보](#)

소개

이 문서에서는 OSPF(Open Shortest Path First), NAT(Network Address Translation) 및 Cisco IOS® Firewall이 있는 IPsec을 통한 GRE(Generic Routing Encapsulation) 사용 DMVPN(Dynamic Multipoint VPN)의 샘플 컨피그레이션을 제공합니다.

사전 요구 사항

요구 사항

mGRE(Multipoint GRE) 및 IPsec 터널을 설정하려면 먼저 `crypto isakmp policy` 명령을 사용하여 IKE(Internet Key Exchange) 정책을 정의해야 합니다.

참고: [명령 조회 도구](#)([등록된](#) 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 허브 라우터의 Cisco IOS® Software Release 12.2(15)T1 및 스포크 라우터의 Cisco IOS Software Release 12.3(1.6)
 - 허브 라우터로 Cisco 3620, Cisco 1720 라우터 2개 및 스포크 라우터로 Cisco 3620 라우터 1개
- 이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 규칙](#)을 참조하십시오.

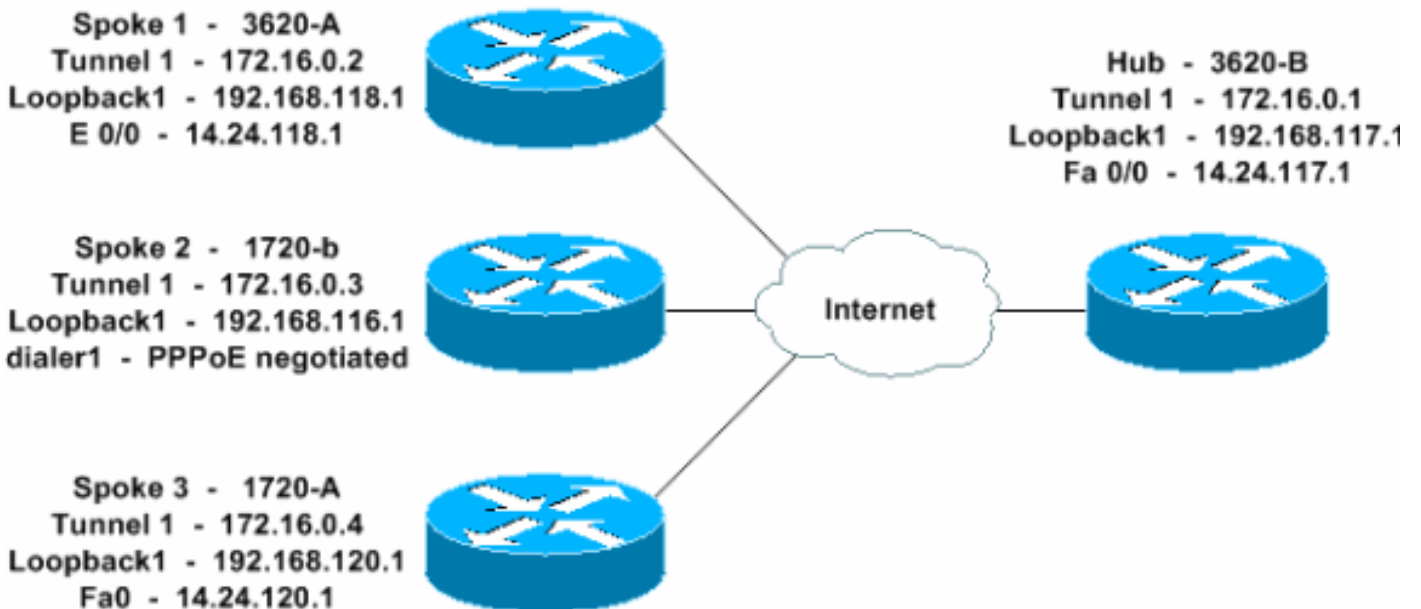
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: [명령 조회 도구](#) (등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.



구성

이 문서에서는 이러한 구성을 사용합니다.

- [허브 - 3620-B](#)
- [스포크 1 - 3620-A](#)
- [스포크 2 - 1720-b](#)
- [스포크 3 - 1720-A](#)

허브 - 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
Tunnell1 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#

```

스포크 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 Tunnel1 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#

```

스포크 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 premit 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#
```

스포크 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 Tunnell1 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#
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output [Interpreter 도구](#) (등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show crypto isakmp sa** - ISAKMP SA(Security Association)의 상태를 표시합니다.
- **show crypto engine connections active**(암호화 엔진 연결 활성 표시) - SA당 총 암호화/해독 횟수를 표시합니다.
- **show crypto ipsec sa** - 활성 터널의 통계를 표시합니다.
- **show ip route** - 라우팅 테이블을 표시합니다.
- **show ip ospf neighbor** - 인터페이스별로 OSPF 네이버 정보를 표시합니다.
- **show ip nhrp** - 특정 인터페이스에 대한 동적 또는 정적 캐시 엔트리로 선택적으로 제한된 IP NHRP(Next Hop Resolution Protocol) 캐시를 표시합니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 명령

참고: 디버그 명령을 [실행하기](#) 전에 [디버그 명령](#)에 대한 중요 정보를 참조하십시오.

- **debug crypto ipsec** - IPsec 이벤트를 표시합니다.
- **debug crypto isakmp** - IKE 이벤트에 대한 메시지를 표시합니다.
- **debug crypto engine** - 암호화 엔진의 정보를 표시합니다.

IPsec 문제 해결에 대한 자세한 내용은 [IP Security Troubleshooting - Understanding and Using debug 명령을 참조하십시오.](#)

관련 정보

- [Cisco IOS 방화벽 구성 트러블슈팅](#)
- [DMVPN 및 Cisco IOS 개요](#)
- [IPsec 협상/IKE 프로토콜](#)
- [기술 지원 및 문서 - Cisco Systems](#)