

OSPF、NAT、および Cisco IOS Firewall を使用する GRE Over IPsec によるダイナミックマルチポイント VPN の設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[関連情報](#)

概要

このドキュメントでは、Open Shortest Path First (OSPF)、ネットワーク アドレス変換 (NAT)、および Cisco IOS® ファイアウォールによる総称ルーティング カプセル化 (GRE) over IPsec を使用した Dynamic Multipoint VPN (DMVPN) の設定例について説明します。

前提条件

要件

マルチポイント GRE (mGRE) および IPsec トンネルを確立するためには、`crypto isakmp policy` コマンドを使用して、インターネット キー エクスチェンジ (IKE) ポリシーを定義しておく必要があります。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool (登録ユーザ専用) を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ハブルータではCisco IOS®ソフトウェアリリース12.2(15)T1、スポークルータではCisco IOSソフトウェアリリース12.3(1.6)
- ハブルータとして Cisco 3620、スポークルータとして 2 台の Cisco 1720 ルータと 1 台の Cisco 3620 ルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『[シスコテクニカルティップスの表記法](#)』を参照してください。

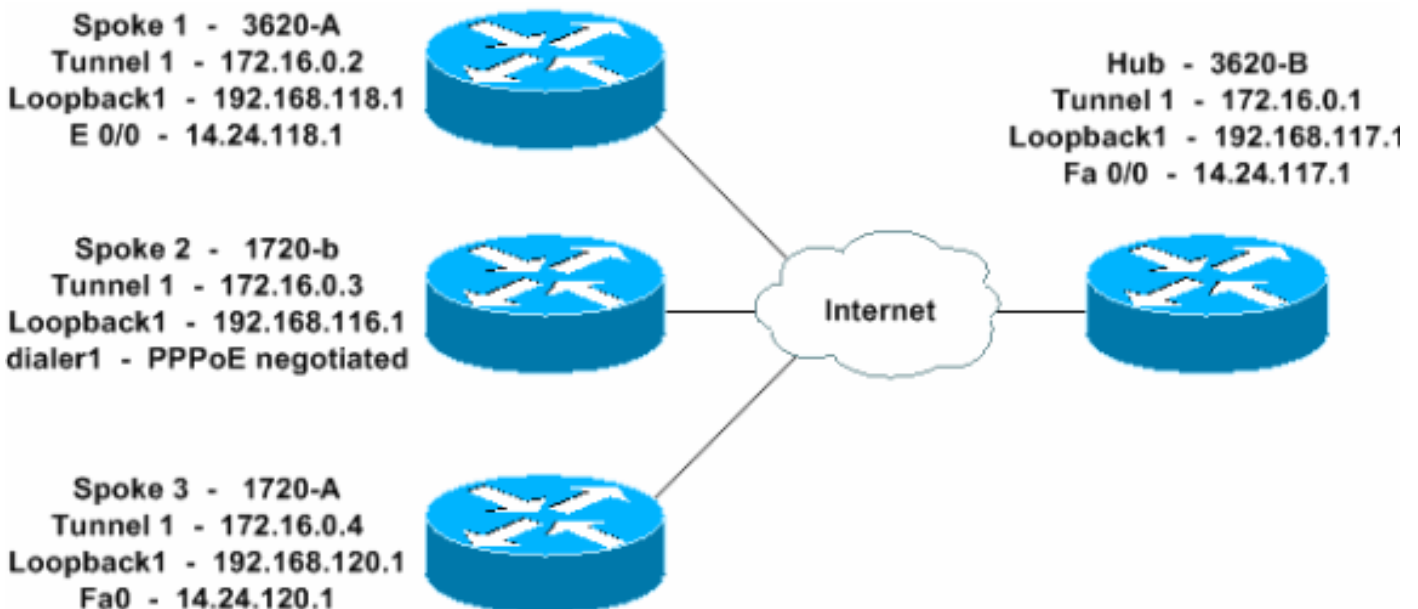
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

ネットワーク図

このドキュメントでは、次のネットワーク設定を使用します。



設定

このドキュメントでは次の設定を使用します。

- [ハブ : 3620-B](#)
- [スポーク 1 : 3620-A](#)

- [スポーク 2 : 1720-b](#)
- [スポーク 3 : 1720-A](#)

ハブ : 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#

```

スプーク 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#

```

スプーク 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#

```

スプーク 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#
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

[アウトプット インタープリタ ツール \(登録ユーザ専用 \) \(OIT \)](#) は、特定の show コマンドをサ
ポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- show crypto isakmp sa : ISAKMP セキュリティ アソシエーション (SA) の状態を表示しま
す。
- show crypto engine connections active : SA ごとの暗号化と復号化の総計を表示します。
- show crypto ipsec sa : アクティブなトンネルの統計情報を表示します。
- show ip route : ルーティング テーブルを表示します。
- show ip ospf neighbor:OSPFネイバー情報をインターフェイスごとに表示します。
- show ip nhrp : IP Next Hop Resolution Protocol (NHRP) キャッシュを表示します。オプシ
ョンで、特定のインターフェイスの動的または静的なキャッシュに表示を限定できます。

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

トラブルシューティングのためのコマンド

注：debugコマンドを発行する前に、『[debugコマンドの重要な情報](#)』を参照してください。

- debug crypto ipsec：IPsec イベントを表示します。
- debug crypto isakmp：IKE イベントに関するメッセージを表示します。
- debug crypto engine：暗号エンジンからの情報を表示します。

IPSec のトラブルシューティングに関する詳細については、[IP セキュリティのトラブルシューティング：デバッグ コマンドの詳細と使用法](#)を参照してください。

関連情報

- [Cisco IOS ファイアウォール設定のトラブルシューティング](#)
- [DMVPN と Cisco IOS の概要](#)
- [IPSec ネゴシエーション/IKE プロトコル](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)