EIGRP、NAT および CBAC による GRE Over IPSec を使ったダイナミック マルチポイント VPN の設定

目次

概要

この文書では、Enhanced Interior Gateway Routing Protocol（EIGRP）、Network Address Translation（NAT; ネットワーク アドレス変換）、および Context-Based Access Control（CBAC）による、Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）over IPSec を使ったハブ & スポーク Dynamic Multipoint VPN（DMVPN; ダイナミック マルチポイント VPN）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には、crypto isakmp policy コマンドを使用して Internet Key Exchange（IKE; インターネット鍵交換）ポリシーを定義しておく必要があります。

注: このドキュメント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）を使用してください。

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くものです。

- スポークルータのハブルータの Cisco IOS® ソフトウェア リリース 12.2(15)T1 および 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 ルータおよび 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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 対象のネットワークが実稼働中である場合には、どのような作業についても、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

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このドキュメント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）を使用してください。

ネットワーク図

このドキュメントでは次の図に示すネットワーク

設定

このドキュメントでは次に示す設定を使用しています。

- 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

```
3620-B#write terminal Building configuration... Current
configuration : 2607 bytes ! version 12.2 service
timestamps debug datetime msec service timestamps log
datetime msec no service password-encryption ! hostname
3620-B ! logging queue-limit 100 ! memory-size iomem 10
ip subnet-zero ! ! ip cef no ip domain lookup ! !---
This is the CBAC configuration and what to inspect. !---
This will be 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. !---
Here "dmvpn" is the word that is used as the 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 inside
interface. interface Loopback1 ip address 192.168.117.1
255.255.255.0 ip nat inside ! !--- This is the mGRE
interface for dynamic 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 1400 ip nhrp authentication dmvpn ip
nhrp map multicast dynamic ip nhrp network-id 99 ip nhrp
holdtime 300 no ip split-horizon eigrp 1 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 outside
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 over the tunnels. router eigrp 1 network
172.16.0.0 0.0.0.255 network 192.168.117.0 no auto-
summary ! !--- Perform NAT on local traffic !--- going
directly out FastEthernet0/0. ip nat inside source list
110 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.
!--- CBAC will open other inbound access as needed.
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 access-list 110 permit ip 192.168.117.0
0.0.0.255 any ! ! 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 3620-
B#
```

スポーク 1 - 3620-A

```
3620-A#write terminal Building configuration... Current
configuration : 2559 bytes ! version 12.2 service
timestamps debug uptime service timestamps log uptime no
service password-encryption ! hostname 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 CBAC configuration and what to inspect. !--- This
will be 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 inside
interface. interface Loopback1 ip address 192.168.118.1
255.255.255.0 ip nat inside ! !--- This is the mGRE
interface for dynamic 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
1400 ip nhrp authentication dmvpn 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 mroute-cache delay 1000 tunnel source
Ethernet0/0 tunnel mode gre multipoint tunnel key 100000
tunnel protection ipsec profile dmvpnprof ! !--- This is
the outside interface. interface Ethernet0/0 ip address
14.24.118.1 255.255.0.0 ip nat outside ip inspect in2out
out ip access-group 100 in 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 over the tunnel. router eigrp 1 network
172.16.0.0 0.0.0.255 network 192.168.118.0 no auto-
summary ! !--- Perform NAT on local traffic !--- going
directly out Ethernet0/0. ip nat inside source list 110
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 ! ! !--- Allow ISAKMP, ESP, and GRE traffic
inbound. !--- CBAC will open 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 access-list 110 permit ip 192.168.118.0
0.0.0.255 any ! ! 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 3620-
A#
```

スポーク 2 - 1720-b

```
1720-b#write terminal Building configuration... Current
configuration : 2543 bytes ! version 12.2 service
timestamps debug uptime service timestamps log uptime no
service password-encryption ! hostname 1720-b ! boot
system flash flash:c1700-ny-mz.122-8.YJ 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 CBAC configuration and what to
inspect. !--- This will be 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 inside interface. interface Loopback1 ip address 192.168.116.1 255.255.255.0 ip nat inside ! !--- This is the mGRE interface for dynamic 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 1400 ip nhrp authentication dmvpn 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 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 outside 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 eigrp 1 network 172.16.0.0 0.0.0.255 network 192.168.116.0 no auto-summary ! !--- Perform NAT on local traffic !--- going directly out Dialer1. ip nat inside source list 110 interface Dialer1 overload ip classless 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. !--- CBAC will open 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 192.168.116.0 0.0.0.255 any dialer-list 1 protocol ip permit ! ! ! line con 0 exec-timeout 0 0 line aux 0 line vty 0 4 login ! no scheduler allocate end 1720-b#
```

スポーク 3 - 1720-A

```
1720-A#write terminal Building configuration... Current configuration : 1770 bytes ! version 12.2 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname 1720-A ! logging queue-limit 100 ! memory-size iomem 25 ip subnet-zero ! ! ! ip cef !--- This is the CBAC configuration and what to inspect. !--- This will be 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 ! ! !--- This is the inside interface. interface Loopback1 ip address 192.168.120.1 255.255.255.0 ip nat inside ! !--- This is the mGRE
```

```
interface for dynamic 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
1400 ip nhrp authentication dmvpn 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 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 outside 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 eigrp 1
network 172.16.0.0 0.0.0.255 network 192.168.120.0 no
auto-summary ! !--- Perform NAT on local traffic !---
going directly out FastEthernet0. ip nat inside source
list 110 interface FastEthernet0 overload ip classless
ip route 0.0.0.0 0.0.0.0 14.24.1.1 no ip http server no
ip http secure-server ! ! ! !--- Allow ISAKMP, ESP, and
GRE traffic inbound. !--- CBAC will open 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 ! ! ! line con
0 exec-timeout 0 0 line aux 0 line vty 0 4 login ! no
scheduler allocate end 1720-A#
```

確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供しています。

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

- show crypto isakmp sa - ISAKMP Security Association（SA; セキュリティ アソシエーション）の状態を表示します。
- show crypto engine connections active：SA ごとの合計の暗号化/復号化を表示します。
- 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 eigrp neighbor - EIGRP 隣接ルータを表示します。
- 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に対する動的または静的なキャッシュ エントリに制限できます。
- show crypto socket - NHRP と IPSec 間の暗号化ソケット テーブルを表示します。

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役立つ情報について説明します。

トラブルシューティングのためのコマンド

注: debug コマンドを使用する前に、『debug コマンドに関する重要な情報』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**：暗号化エンジンからの情報を表示します。
- debug crypto socket - NHRP と IPSec 間のソケット テーブルに関する情報を表示します。
- debug nhrp - NHRP イベントの情報を表示します。
- debug nhrp packet - NHRP パケットの情報を表示します。
- debug tunnel protection - ダイナミック GRE トンネルの情報を表示します。

IPSec のトラブルシューティングの詳細については、「IP Security のトラブルシューティング - debug コマンドの理解と使用」を参照してください。

関連情報

- **DMVPN および Cisco IOS の概要**
- **IPSec に関するサポート ページ**
- **テクニカルサポートとドキュメント - Cisco Systems**