通过 EIGRP、NAT 和 CBAC 使用 GRE Over IPSec 配置动态多点 VPN

Contents

Introduction

本文为星型网动态多点VPN (DMVPN)提供一配置示例使用在IPSec的通用路由封装(GRE)以增强的内部网关路由选择协议(EIGRP)、网络地址转换(NAT)和基于上下文的访问控制(CBAC)。

Prerequisites

Requirements

在一多点GRE (mGRE)通过使用**crypto isakmp policy命令，**和IPSec隧道前可以设立，您必须定义Internet Key Exchange (IKE)策略。

Note: 要查找本文档所用命令的其他信息，请使用命令查找工具（仅限注册用户）。

Components Used

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创建的。All of the devices used in this document started with a cleared (default) configuration.如果您是在真实网络上操作，请确保您在使用任何命

令前已经了解其潜在影响。

Conventions

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

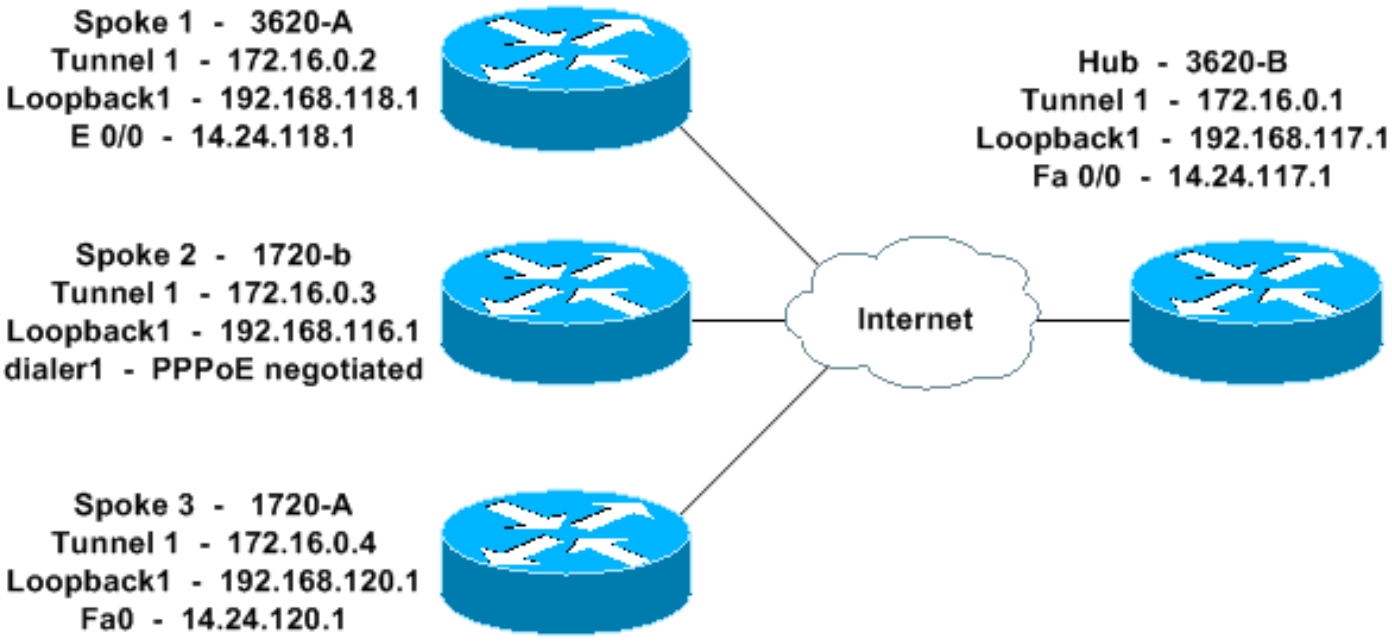
Configure

本部分提供有关如何配置本文档所述功能的信息。

Note: 要查找本文档所用命令的其他信息，请使用命令查找工具（仅限注册用户）。

Network Diagram

本文档使用下图所示的网络设置。



配置

本文档使用如下所示的配置。

- 中心 - 3620-B
- 分支 1 - 3620-A
- 分支 2 - 1720-b
- 分支 3 - 1720-A

中心 - 3620-B

```
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#
```

分支 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#
```

分支 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#
```

分支 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#
```

Verify

本部分所提供的信息可用于确认您的配置是否正常工作。

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 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 eigrp neighbor** - 显示 EIGRP 邻居。
- **show ip nhrp** —显示IP下一跳解析协议(NHRP)高速缓冲存储器，可选地有限对一个特定接口的

动态或静态缓存条目。
- **show crypto socket** - 显示 NHRP 和 IPSec 之间的加密套接字表。

Troubleshoot

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

Note: 在发出 **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。
- **debug crypto socket** 显示有关 NHRP 和 IPSec 之间的套接字表的信息。
- **debug nhrp** - 显示有关 NHRP 事件的信息。
- **debug nhrp packet** - 显示有关 NHRP 数据包的信息。
- **debug tunnel protection** - 显示有关动态 GRE 隧道的信息。

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。

Related Information

- DMVPN 和 Cisco IOS 概述
- IPSec 支持页面
- Technical Support & Documentation - Cisco Systems