使用动态路由在 Cisco IOS 路由器与 VPN 5000 集中器之间配置 GRE Over IPSec

目录

简介

此示例配置描述了如何在 Cisco VPN 5000 集中器与运行 Cisco IOS® 软件的 Cisco 路由器之间配置基于 IPSec 的通用路由封装 (GRE)。GRE-over-IPSec 功能是在 VPN 5000 集中器 6.0(19) 软件版本中引入的。此示例中使用 Open Shortest Path First (OSPF) 动态路由协议，用于路由跨 VPN 隧道的流量。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS® 软件版本 12.2(3)
- VPN 5000 集中器软件版本 6.0(19)

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。

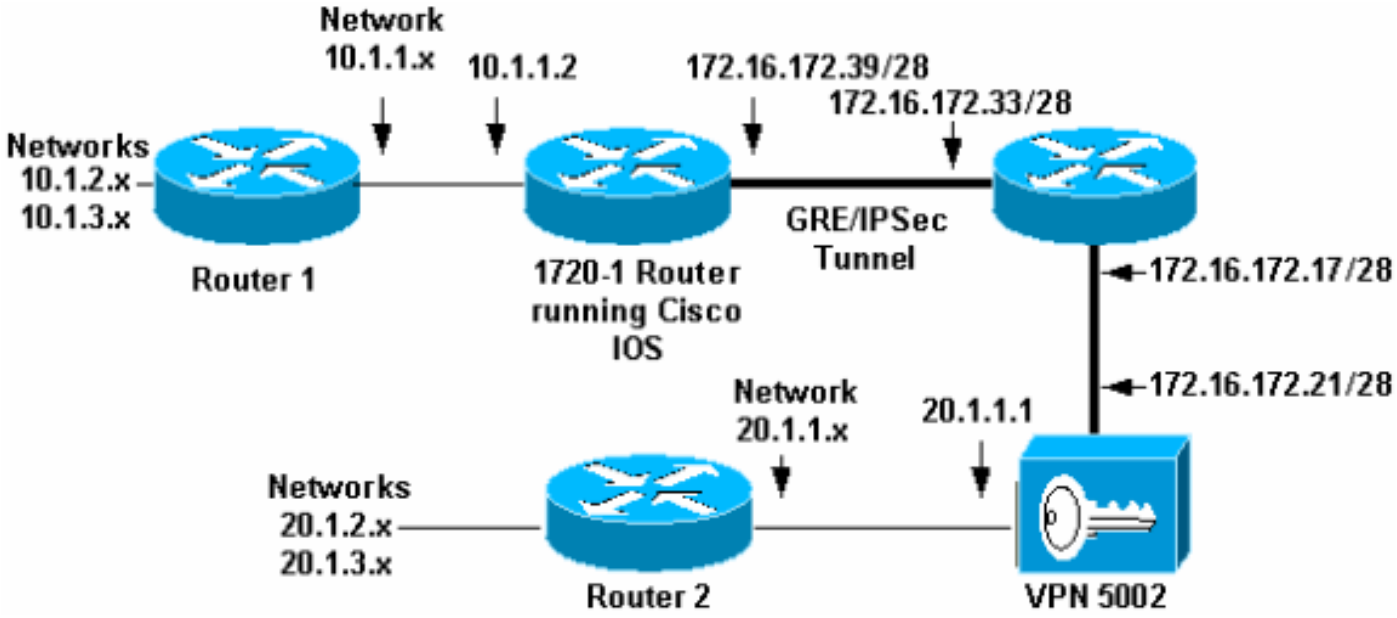
配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 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）。

网络图

本文档使用此图所示的网络设置。



GRE over IPSec 配置在 Cisco IOS 路由器 (1720-1) 与 VPN 5002 集中器之间。在这些设备后面，多个网络通过 OSPF 得到通告，而 OSPF 在 1720-1 与 VPN 5002 之间的 GRE 隧道内运行。

下面的网络位于 1720-1 路由器后面。

- 10.1.1.0/24
- 10.1.2.0/24
- 10.1.3.0/24

下面的网络位于 VPN 5002 集中器后面。

- 20.1.1.0/24
- 20.1.2.0/24
- 20.1.3.0/24

注意： 对于此拓扑，所有网段都放在 OSPF 区域 0 中。

配置

本文档使用以下配置。

- Cisco IOS 路由器
- VPN 5000 集中器

Cisco IOS 路由器

```
Building configuration...
Current configuration : 1351 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 1720-1
!
no logging buffered
no logging monitor
enable secret 5 $1$vIzI$RqD0LqlqbSFCCjVELFLfH/
!
memory-size iomem 15
ip subnet-zero
no ip domain-lookup
!
ip audit notify log
ip audit po max-events 100
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto isakmp policy 1 hash md5 authentication pre-share
crypto isakmp key cisco123 address 172.16.172.21 ! !
crypto ipsec transform-set myset esp-des esp-md5-hmac
mode transport ! crypto dynamic-map dyna 10 set
transform-set myset match address 102 ! ! crypto map vpn
10 ipsec-isakmp dynamic dyna ! cns event-service server
! ! ! interface Tunnel0 ip address 50.1.1.1
255.255.255.252 ip ospf mtu-ignore tunnel source
FastEthernet0 tunnel destination 172.16.172.21 crypto
map vpn ! interface FastEthernet0 ip address
172.16.172.39 255.255.255.240 speed auto crypto map vpn
! interface Serial0 ip address 10.1.1.2 255.255.255.0
encapsulation ppp ! router ospf 1 log-adjacency-changes
network 10.1.1.0 0.0.0.255 area 0 network 50.1.1.0
0.0.0.3 area 0 ! ip classless ip route 0.0.0.0 0.0.0.0
172.16.172.33 no ip http server ! access-list 102 permit
gre host 172.16.172.39 host 172.16.172.21 ! line con 0
line aux 0 line vty 0 4 password cisco login ! end
```

VPN 5000 集中器

```
VPN5002_8_323E9040: Main# show config Edited
Configuration not Present, using Running [ General ]
VPNGateway = 172.16.172.17 IPSecGateway = 198.91.10.1
EthernetAddress = 00:05:32:3e:90:40 DeviceType = VPN
5002/8 Concentrator ConfiguredOn = Timeserver not
configured ConfiguredFrom = Command Line, from Console [
IKE Policy ] Protection = MD5_DES_G1 [ IP Ethernet 1:0 ]
Mode = Routed IPBroadcast = 172.16.172.32 SubnetMask =
255.255.255.240 IPAddress = 172.16.172.21 [ Logging ]
Level = Debug LogToAuxPort = On Enabled = On [ Ethernet
Interface Ethernet 0:0 ] DUPLEX = half SPEED = 10meg [
IP Ethernet 0:0 ] OSPFenabled = On OSPFAreaID = 0 Mode =
Routed IPBroadcast = 20.1.1.255 SubnetMask =
```

```
255.255.255.0 IPAddress = 20.1.1.1 [ IP Static ] 0.0.0.0
0.0.0.0 150.1.1.1 [ Tunnel Partner VPN 1 ] Partner =
172.16.172.39 KeyManage = Reliable Mode = Main
Certificates = Off SharedKey = "cisco123" BindTo =
"Ethernet 1:0" Transform = ESP(MD5,DES)
InactivityTimeout = 120 TunnelType = GREinIPSec
KeepaliveInterval = 120 KeyLifeSecs = 3500 [ IP VPN 1 ]
Mode = Routed Numbered = On DirectedBroadcast = Off
IPAddress = 50.1.1.2 SubnetMask = 255.255.255.252
OSPFenabled = On OSPFAreaID = 0 HelloInterval = 10 [
OSPF Area "0" ] OSPFAuthtype = None StubArea = Off
Configuration size is 1781 out of 65500 bytes.
VPN5002_8_323E9040: Main#
```

IOS 设备与 VPN 5000 集中器配置为建立起相互之间的一个 GRE 隧道。IOS 路由器还具有为 VPN 5000 集中器的 IP 地址配置的动态加密映射。VPN 5000 的隧道配置反映出，它会启动通向 IOS 设备的 IPSec 传输模式 GRE 隧道。当 IOS 设备启动时，它没有通过该隧道到达目的地的路由。它不会以明文形式转发专用网络流量。当 VPN 集中器启动时，它会自动协商加密安全连接 (SA) 以保护两个对等体之间的 GRE 流量。此时，隧道将会建立并运行，两个对等体交换参与网络的路由。VPN 集中器基于“InactivityTimeout”和“KeepAliveInterval”关键字不断对连接执行密钥更新。如果 IOS 路由器强制更新密钥，则两个对等体要使用的 SA 将不一致，VPN 集中器将在非活动状态达到 *x* 秒后重新协商隧道（其中 *x* 表示在“InactivityTimeout”中指定的值）。

注意： 此隧道配置始终保持运行。没有无操作断连选项。不应该在昂贵的按用量计费的链路上使用此隧道，或者在远程 (IOS) 路由器预计在空闲时间之后断开的情况下使用此隧道。

验证

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。

Cisco IOS 路由器

- **show crypto isakmp sa** - 显示所有当前 Internet Security Association and Key Management Protocol (ISAKMP) SA。
- **show crypto ipsec sa** - 显示所有当前 IPSec SA。
- **show crypto engine connection active** - 显示每个 IPSec SA 的数据包加密/解密计数器。

VPN 5000 集中器

- **show system log buffer** - 显示基本 syslog 信息。
- **vpn trace dump** - 显示 VPN 进程的详细信息。

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

下面的命令可在 Cisco IOS 路由器上使用。

注意： 在发出 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

- **debug crypto isakmp** - 显示有关 Internet Key Exchange (IKE) 阶段 I（主模式）协商的详细信息。
- **debug crypto ipsec** - 显示有关 IKE 阶段 II（快速模式）协商的详细信息。
- **debug crypto engine** - 调试数据包加密/解密与 Diffie-Hellman (DH) 进程。

调试输出示例

本部分提供配置设备的示例调试输出。

- Cisco IOS 路由器
- VPN 5000 集中器

Cisco IOS 路由器

此输出是在 Cisco IOS 路由器上使用 **debug crypto isakmp** 和 **debug crypto ipsec** 命令生成的。这是 Cisco IOS 路由器和 VPN 5000 集中器上的正确调试。

```
1720-1#show debug Cryptographic Subsystem: Crypto ISAKMP debugging is on Crypto Engine debugging
is on Crypto IPSEC debugging is on 1720-1# 19:16:24: ISAKMP (0:0): received packet from
172.16.172.21 (N) NEW SA 19:16:24: ISAKMP: local port 500, remote port 500 19:16:24: ISAKMP
(0:2): processing SA payload. message ID = 0 19:16:24: ISAKMP (0:2): found peer pre-shared key
matching 172.16.172.21 19:16:24: ISAKMP (0:2): Checking ISAKMP transform 1 against priority 1
policy 19:16:24: ISAKMP: encryption DES-CBC 19:16:24: ISAKMP: hash MD5 19:16:24: ISAKMP: auth
pre-share 19:16:24: ISAKMP: default group 1 19:16:24: ISAKMP (0:2): atts are acceptable. Next
payload is 0 19:16:24: CryptoEngine0: generate alg parameter 19:16:24: CryptoEngine0:
CRYPTO_ISA_DH_CREATE(hw)(ipsec) 19:16:24: CRYPTO_ENGINE: Dh phase 1 status: 0 19:16:24: ISAKMP
(0:2): processing vendor id payload 19:16:24: ISAKMP (0:2): SA is doing pre-shared key
authentication using id type ID_IPV4_ADDR 19:16:24: ISAKMP (0:2): sending packet to
172.16.172.21 (R) MM_SA_SETUP 19:16:24: ISAKMP (0:2): received packet from 172.16.172.21 (R)
MM_SA_SETUP 19:16:24: ISAKMP (0:2): processing KE payload. message ID = 0 19:16:24:
CryptoEngine0: generate alg parameter 19:16:24: CryptoEngine0:
CRYPTO_ISA_DH_SHARE_SECRET(hw)(ipsec) 19:16:24: ISAKMP (0:2): processing NONCE payload. message
ID = 0 19:16:24: ISAKMP (0:2): found peer pre-shared key matching 172.16.172.21 19:16:24:
CryptoEngine0: create ISAKMP SKEYID for conn id 2 19:16:24: CryptoEngine0:
CRYPTO_ISA_SA_CREATE(hw)(ipsec) 19:16:24: ISAKMP (0:2): SKEYID state generated 19:16:24: ISAKMP
(0:2): sending packet to 172.16.172.21 (R) MM_KEY_EXCH 19:16:24: ISAKMP (0:2): received packet
from 172.16.172.21 (R) MM_KEY_EXCH 19:16:24: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
19:16:24: ISAKMP (0:2): processing ID payload. message ID = 0 19:16:24: ISAKMP (0:2): processing
HASH payload. message ID = 0 19:16:24: CryptoEngine0: generate hmac context for conn id 2
19:16:24: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec) 19:16:24: ISAKMP (0:2): SA has been
authenticated with 172.16.172.21 19:16:24: ISAKMP (2): ID payload next-payload : 8 type : 1
protocol : 17 port : 500 length : 8 19:16:24: ISAKMP (2): Total payload length: 12 19:16:24:
CryptoEngine0: generate hmac context for conn id 2 19:16:24: CryptoEngine0:
CRYPTO_ISA_IKE_HMAC(hw)(ipsec) 19:16:24: CryptoEngine0: clear dh number for conn id 1 19:16:24:
CryptoEngine0: CRYPTO_ISA_DH_DELETE(hw)(ipsec) 19:16:24: CryptoEngine0:
CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec) 19:16:24: ISAKMP (0:2): sending packet to 172.16.172.21 (R)
QM_IDLE 19:16:24: ISAKMP (0:2): received packet from 172.16.172.21 (R) QM_IDLE 19:16:24:
CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec) 19:16:24: CryptoEngine0: generate hmac context
for conn id 2 19:16:24: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec) 19:16:24: ISAKMP (0:2):
processing HASH payload. message ID = 49 19:16:24: ISAKMP (0:2): processing SA payload. message
ID = 49 19:16:24: ISAKMP (0:2): Checking IPSec proposal 1 19:16:24: ISAKMP: transform 1, ESP_DES
19:16:24: ISAKMP: attributes in transform: 19:16:24: ISAKMP: SA life type in seconds 19:16:24:
ISAKMP: SA life duration (VPI) of 0x0 0x0 0xD 0xAC 19:16:24: ISAKMP: SA life type in kilobytes
```

19:16:24: ISAKMP: SA life duration (VPI) of 0x0 0x10 0x0 0x0 19:16:24: ISAKMP: encaps is 2 19:16:24: ISAKMP: authenticator is HMAC-MD5 19:16:24: validate proposal 0 19:16:24: ISAKMP (0:2): atts are acceptable. 19:16:24: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest= 172.16.172.39, src= 172.16.172.21, dest_proxy= 172.16.172.39/255.255.255.255/47/0 (type=1), src_proxy= 172.16.172.21/255.255.255.255/47/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0 19:16:24: validate proposal request 0 19:16:24: ISAKMP (0:2): processing NONCE payload. message ID = 49 19:16:24: ISAKMP (0:2): processing ID payload. message ID = 49 19:16:24: ISAKMP (2): ID_IPV4_ADDR src 172.16.172.21 prot 47 port 0 19:16:24: ISAKMP (0:2): processing ID payload. message ID = 49 19:16:24: ISAKMP (2): ID_IPV4_ADDR dst 172.16.172.39 prot 47 port 0 19:16:24: ISAKMP (0:2): asking for 1 spis from ipsec 19:16:24: IPSEC(key_engine): got a queue event... 19:16:24: IPSEC(spi_response): getting spi 3854485305 for SA from 172.16.172.21 to 172.16.172.39 for prot 3 19:16:24: ISAKMP: received ke message (2/1) 19:16:24: CryptoEngine0: generate hmac context for conn id 2 19:16:24: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec) 19:16:24: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec) 19:16:24: ISAKMP (0:2): sending packet to 172.16.172.21 (R) QM_IDLE 19:16:24: ISAKMP (0:2): received packet from 172.16.172.21 (R) QM_IDLE 19:16:24: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec) 19:16:24: CryptoEngine0: generate hmac context for conn id 2 19:16:24: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec) 19:16:24: ipsec allocate flow 0 19:16:24: ipsec allocate flow 0 19:16:24: CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec) 19:16:25: CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec) 19:16:25: ISAKMP (0:2): Creating IPSec SAs 19:16:25: inbound SA from 172.16.172.21 to 172.16.172.39 (proxy 172.16.172.21 to 172.16.172.39) 19:16:25: has spi 0xE5BEC739 and conn_id 200 and flags 0 19:16:25: lifetime of 3500 seconds 19:16:25: lifetime of 1048576 kilobytes 19:16:25: outbound SA from 172.16.172.39 to 172.16.172.21 (proxy 172.16.172.39 to 172.16.172.21) 19:16:25: has spi 298 and conn_id 201 and flags 0 19:16:25: lifetime of 3500 seconds 19:16:25: lifetime of 1048576 kilobytes 19:16:25: ISAKMP (0:2): deleting node 49 error FALSE reason "quick mode done (await()" 19:16:25: IPSEC(key_engine): got a queue event... 19:16:25: IPSEC(initialize_sas): , (key eng. msg.) dest= 172.16.172.39, src= 172.16.172.21, dest_proxy= 172.16.172.39/0.0.0.0/47/0 (type=1), src_proxy= 172.16.172.21/0.0.0.0/47/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 3500s and 1048576kb, spi= 0xE5BEC739(3854485305), conn_id= 200, keysize= 0, flags= 0x0 19:16:25: IPSEC(initialize_sas): , (key eng. msg.) src= 172.16.172.39, dest= 172.16.172.21, src_proxy= 172.16.172.39/0.0.0.0/47/0 (type=1), dest_proxy= 172.16.172.21/0.0.0.0/47/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 3500s and 1048576kb, spi= 0x12A(298), conn_id= 201, keysize= 0, flags= 0x0 19:16:25: IPSEC(create_sa): sa created, (sa) sa_dest= 172.16.172.39, sa_prot= 50, sa_spi= 0xE5BEC739(3854485305), sa_trans= esp-des esp-md5-hmac , sa_conn_id= 200 19:16:25: IPSEC(create_sa): sa created, (sa) sa_dest= 172.16.172.21, sa_prot= 50, sa_spi= 0x12A(298), sa_trans= esp-des esp-md5-hmac , sa_conn_id= 201 1720-1# VPN5002_8_323E9040: Main# **show sys log buffer** VPN5002_8_323E9040: Main# VPN 0:1 opened for 172.16.172.39 from 172.16.172.39. User assigned IP address 50.1.1.2 1720-1#**show crypto isakmp sa** dst src state conn-id slot 172.16.172.39 172.16.172.21 QM_IDLE 1 0 1720-1#**show crypto ipsec sa** interface: Tunnel0 Crypto map tag: vpn, local addr. 172.16.172.39 local ident (addr/mask/prot/port): (172.16.172.39/255.255.255.255/47/0) remote ident (addr/mask/prot/port): (172.16.172.21/255.255.255.255/47/0) current_peer: 172.16.172.21 PERMIT, flags={transport_parent,} #pkts encaps: 3051, #pkts encrypt: 3051, #pkts digest 3051 #pkts decaps: 3055, #pkts decrypt: 3055, #pkts verify 3055 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts decompress failed: 0, #send errors 0, #recv errors 0 local crypto endpt.: 172.16.172.39, remote crypto endpt.: 172.16.172.21 path mtu 1514, media mtu 1514 current outbound spi: 129 inbound esp sas: spi: 0x9161FD66(2439118182) transform: esp-des esp-md5-hmac , in use settings ={Transport, } slot: 0, conn id: 216, flow_id: 17, crypto map: vpn sa timing: remaining key lifetime (k/sec): (1048543/912) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x129(297) transform: esp-des esp-md5-hmac , in use settings ={Transport, } slot: 0, conn id: 217, flow_id: 18, crypto map: vpn sa timing: remaining key lifetime (k/sec): (1048543/912) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas: interface: FastEthernet0 Crypto map tag: vpn, local addr. 172.16.172.39 local ident (addr/mask/prot/port): (172.16.172.39/255.255.255.255/47/0) remote ident (addr/mask/prot/port): (172.16.172.21/255.255.255.255/47/0) current_peer: 172.16.172.21 PERMIT, flags={transport_parent,} #pkts encaps: 3052, #pkts encrypt: 3052, #pkts digest 3052 #pkts decaps: 3056, #pkts decrypt: 3056, #pkts verify 3056 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts decompress failed: 0, #send errors 0, #recv errors 0 local crypto endpt.: 172.16.172.39, remote crypto endpt.: 172.16.172.21 path mtu 1514, media mtu 1514 current outbound spi: 129 inbound esp sas: spi: 0x9161FD66(2439118182) transform: esp-des esp-md5-hmac , in use settings ={Transport, } slot: 0, conn id: 216, flow_id:

17, crypto map: vpn sa timing: remaining key lifetime (k/sec): (1048543/903) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x129(297) transform: esp-des esp-md5-hmac , in use settings ={Transport, } slot: 0, conn id: 217, flow_id: 18, crypto map: vpn sa timing: remaining key lifetime (k/sec): (1048543/903) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas: 1720-1#**show crypto ipsec sa** interface: FastEthernet0 Crypto map tag: vpn, local addr. 172.16.172.39 local ident (addr/mask/prot/port): (172.16.172.39/255.255.255.255/0/0) remote ident (addr/mask/prot/port): (172.16.172.21/255.255.255.255/0/0) current_peer: 172.16.172.21 PERMIT, flags={transport_parent,} #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0 #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts decompress failed: 0, #send errors 0, #recv errors 0 local crypto endpt.: 172.16.172.39, remote crypto endpt.: 172.16.172.21 path mtu 1514, media mtu 1514 current outbound spi: 0 inbound esp sas: inbound ah sas: inbound pcp sas: outbound esp sas: outbound ah sas: outbound pcp sas: local ident (addr/mask/prot/port): (172.16.172.39/255.255.255.255/47/0) remote ident (addr/mask/prot/port): (172.16.172.21/255.255.255.255/47/0) current_peer: 172.16.172.21 PERMIT, flags={origin_is_acl,transport_parent,parent_is_transport,} #pkts encaps: 34901, #pkts encrypt: 34901, #pkts digest 34901 #pkts decaps: 34900, #pkts decrypt: 34900, #pkts verify 34900 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts decompress failed: 0, #send errors 0, #recv errors 0 local crypto endpt.: 172.16.172.39, remote crypto endpt.: 172.16.172.21 path mtu 1500, media mtu 1500 current outbound spi: 151 inbound esp sas: spi: 0x356141A8(895566248) transform: esp-des esp-md5-hmac , in use settings ={Transport, } slot: 0, conn id: 362, flow_id: 163, crypto map: vpn sa timing: remaining key lifetime (k/sec): (1046258/3306) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x151(337) transform: esp-des esp-md5-hmac , in use settings ={Transport, } slot: 0, conn id: 363, flow_id: 164, crypto map: vpn sa timing: remaining key lifetime (k/sec): (1046258/3306) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas: interface: Tunnel0 Crypto map tag: vpn, local addr. 172.16.172.39 local ident (addr/mask/prot/port): (172.16.172.39/255.255.255.255/0/0) remote ident (addr/mask/prot/port): (172.16.172.21/255.255.255.255/0/0) current_peer: 172.16.172.21 PERMIT, flags={transport_parent,} #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0 #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts decompress failed: 0, #send errors 0, #recv errors 0 local crypto endpt.: 172.16.172.39, remote crypto endpt.: 172.16.172.21 path mtu 1514, media mtu 1514 current outbound spi: 0 inbound esp sas: inbound ah sas: inbound pcp sas: outbound esp sas: outbound ah sas: outbound pcp sas: local ident (addr/mask/prot/port): (172.16.172.39/255.255.255.255/47/0) remote ident (addr/mask/prot/port): (172.16.172.21/255.255.255.255/47/0) current_peer: 172.16.172.21 PERMIT, flags={origin_is_acl,transport_parent,parent_is_transport,} #pkts encaps: 35657, #pkts encrypt: 35657, #pkts digest 35657 #pkts decaps: 35656, #pkts decrypt: 35656, #pkts verify 35656 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts decompress failed: 0, #send errors 0, #recv errors 0 local crypto endpt.: 172.16.172.39, remote crypto endpt.: 172.16.172.21 path mtu 1500, media mtu 1500 current outbound spi: 151 inbound esp sas: spi: 0x356141A8(895566248) transform: esp-des esp-md5-hmac , in use settings ={Transport, } slot: 0, conn id: 362, flow_id: 163, crypto map: vpn sa timing: remaining key lifetime (k/sec): (1046154/3302) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x151(337) transform: esp-des esp-md5-hmac , in use settings ={Transport, } slot: 0, conn id: 363, flow_id: 164, crypto map: vpn sa timing: remaining key lifetime (k/sec): (1046154/3302) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas: 1720-1#**show crypto engine connections active** ID Interface IP-Address State Algorithm Encrypt Decrypt 1 FastEthernet0 172.16.172.39 set HMAC_MD5+DES_56_CB 0 0 216 FastEthernet0 172.16.172.39 set HMAC_MD5+DES_56_CB 0 267 217 FastEthernet0 172.16.172.39 set HMAC_MD5+DES_56_CB 266 0 1720-1#**show ip ospf ne** Neighbor ID Pri State Dead Time Address Interface 20.1.1.1 0 FULL/ - 00:00:37 50.1.1.2 Tunnel0 10.1.3.1 1 FULL/ - 00:00:36 10.1.1.1 Serial0 1720-1# 1720-1#**show ip ospf database** OSPF Router with ID (50.1.1.1) (Process ID 1) Router Link States (Area 0) Link ID ADV Router Age Seq# Checksum Link count 10.1.3.1 10.1.3.1 1056 0x80000025 0xAB29 4 20.1.1.1 20.1.1.1 722 0x80000032 0x1AD3 3 20.1.3.1 20.1.3.1 1004 0x80000004 0xB6C4 3 50.1.1.1 50.1.1.1 1707 0x8000002C 0xFD27 4 Net Link States (Area 0) Link ID ADV Router Age Seq# Checksum 20.1.1.1 20.1.1.1 722 0x80000003 0x718A 1720-1#**show ip route** Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area, * - candidate default, U - per-user static route, o - ODR, P - periodic downloaded static route Gateway of last resort is 172.16.172.33 to

network 0.0.0.0 50.0.0.0/30 is subnetted, 1 subnets C 50.1.1.0 is directly connected, Tunnel0 20.0.0.0/8 is variably subnetted, 3 subnets, 2 masks O 20.1.1.0/24 [110/11121] via 50.1.1.2, 00:50:19, Tunnel0 O 20.1.2.1/32 [110/11122] via 50.1.1.2, 00:50:19, Tunnel0 O 20.1.3.1/32 [110/11122] via 50.1.1.2, 00:50:19, Tunnel0 172.16.0.0/28 is subnetted, 1 subnets C 172.16.172.32 is directly connected, FastEthernet0 10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks O 10.1.2.1/32 [110/65] via 10.1.1.1, 00:50:21, Serial0 O 10.1.3.1/32 [110/65] via 10.1.1.1, 00:50:21, Serial0 C 10.1.1.0/24 is directly connected, Serial0 C 10.1.1.1/32 is directly connected, Serial0 S* 0.0.0.0/0 [1/0] via 172.16.172.33

VPN 5000 集中器

VPN5002_8_323E9040: Main#**show vpn partner ver** Port Partner Partner Default Bindto Connect Number Address Port Partner Address Time ---------- VPN 0:1 172.16.172.39 500 No 172.16.172.21 00:08:20:51 Auth/Encrypt: MD5e/DES User Auth: Shared Key Access: Static Peer: 172.16.172.39 Local: 172.16.172.21 Start:39307 seconds Managed:69315 seconds State:imnt_maintenance IOP slot 1: No active connections found. VPN5002_8_323E9040: Main#**show vpn stat ver** Current In High Running Script Script Script Active Negot Water Total Starts OK Error ---------- Users 0 0 0 0 0 0 0 Partners 1 0 1 4 22 4 38 Total 1 0 1 4 22 4 38 Stats VPN0:1 Wrapped 3072 Unwrapped 3068 BadEncap 0 BadAuth 0 BadEncrypt 0 rx IP 3068 rx IPX 0 rx Other 0 tx IP 3072 tx IPX 0 tx Other 0 IKE rekey 8 Input VPN pkts dropped due to no SA: 0 Input VPN pkts dropped due to no free queue entries: 0 IOP slot 1: Current In High Running Script Script Script Active Negot Water Total Starts OK Error ---------- Users 0 0 0 0 0 0 0 Partners 0 0 0 0 0 0 0 Total 0 0 0 0 0 0 0 Stats Wrapped Unwrapped BadEncap BadAuth BadEncrypt rx IP rx IPX rx Other tx IP tx IPX tx Other IKE rekey Input VPN pkts dropped due to no SA: 0 Input VPN pkts dropped due to no free queue entries: 0 VPN5002_8_323E9040: Main#**show ospf nbr** ========== OSPF NEIGHBORS ---------- Ether0:0 RtrID: 20.1.3.1 Addr: 20.1.1.2 State: FULL VPN0:1 RtrID: 50.1.1.1 Addr: 50.1.1.1 State: FULL ========== VPN5002_8_323E9040: Main#**show ospf db all** OSPF Router, Net and Summary Databases: Area 0: STUB AdvRtr 50.1.1.1 Len 24(24) Age 3600 Seq 00000000 LS ID: 50.1.1.0 Mask: 255.255.255.252 Network: 50.1.1.0 Nexthops(1): 50.1.1.1 Interface: VPN0:1 STUB AdvRtr 50.1.1.1 Len 24(24) Age 3600 Seq 00000000 LS ID: 10.1.1.0 Mask: 255.255.255.0 Network: 10.1.1.0 Nexthops(1): 50.1.1.1 Interface: VPN0:1 STUB AdvRtr 20.1.1.1 Len 24(24) Age 3600 Seq 00000000 LS ID: 20.1.1.0 Mask: 255.255.255.0 Network: 20.1.1.0 STUB AdvRtr 20.1.1.1 Len 24(24) Age 3368 Seq 00000000 LS ID: 50.1.1.2 Mask: 255.255.255.252 Network: 50.1.1.0 STUB AdvRtr 20.1.3.1 Len 24(24) Age 3372 Seq 00000000 LS ID: 20.1.3.1 Mask: 255.255.255.255 Network: 20.1.3.1 Nexthops(1): 20.1.1.2 Interface: Ether0:0 STUB AdvRtr 20.1.3.1 Len 24(24) Age 3374 Seq 00000000 LS ID: 20.1.2.1 Mask: 255.255.255.255 Network: 20.1.2.1 Nexthops(1): 20.1.1.2 Interface: Ether0:0 STUB AdvRtr 10.1.3.1 Len 24(24) Age 3442 Seq 00000000 LS ID: 10.1.3.1 Mask: 255.255.255.255 Network: 10.1.3.1 Nexthops(1): 50.1.1.1 Interface: VPN0:1 STUB AdvRtr 10.1.3.1 Len 24(24) Age 3442 Seq 00000000 LS ID: 10.1.2.1 Mask: 255.255.255.255 Network: 10.1.2.1 Nexthops(1): 50.1.1.1 Interface: VPN0:1 RTR AdvRtr 50.1.1.1 Len 72(72) Age 63 Seq 8000002d LS ID: 50.1.1.1 Area Border: Off AS Border: Off Connect Type: RTR Cost: 11111 RouterID: 20.1.1.1 Address: 50.1.1.1 Connect Type: STUB or HOST Cost: 11111 Network: 50.1.1.0 NetMask: 255.255.255.252 Connect Type: RTR Cost: 64 RouterID: 10.1.3.1 Address: 10.1.1.2 Connect Type: STUB or HOST Cost: 64 Network: 10.1.1.0 NetMask: 255.255.255.0 Nexthops(1): 50.1.1.1 Interface: VPN0:1 RTR AdvRtr 20.1.1.1 Len 60(72) Age 1093 Seq 80000032 LS ID: 20.1.1.1 Area Border: Off AS Border: Off Connect Type: TRANS NET Cost: 10 DR: 20.1.1.1 Address: 20.1.1.1 Connect Type: STUB or HOST Cost: 10 Network: 50.1.1.2 NetMask: 255.255.255.252 Connect Type: RTR Cost: 10 RouterID: 50.1.1.1 Address: 50.1.1.2 RTR AdvRtr 20.1.3.1 Len 60(60) Age 1375 Seq 80000004 LS ID: 20.1.3.1 Area Border: Off AS Border: Off Connect Type: STUB or HOST Cost: 1 Network: 20.1.3.1 NetMask: 255.255.255.255 Connect Type: STUB or HOST Cost: 1 Network: 20.1.2.1 NetMask: 255.255.255.255 Connect Type: TRANS NET Cost: 1 DR: 20.1.1.1 Address: 20.1.1.2 Nexthops(1): 20.1.1.2 Interface: Ether0:0 RTR AdvRtr 10.1.3.1 Len 72(72) Age 1430 Seq 80000025 LS ID: 10.1.3.1 Area Border: Off AS Border: Off Connect Type: RTR Cost: 64 RouterID: 50.1.1.1 Address: 10.1.1.1 Connect Type: STUB or HOST Cost: 64 Network: 10.1.1.0 NetMask: 255.255.255.0 Connect Type: STUB or HOST Cost: 1 Network: 10.1.3.1 NetMask: 255.255.255.255 Connect Type: STUB or HOST Cost: 1 Network: 10.1.2.1 NetMask: 255.255.255.255 Nexthops(1): 50.1.1.1 Interface: VPN0:1 NET AdvRtr 20.1.1.1 Len 32(32) Age 1094 Seq 80000003 LS ID: 20.1.1.1 Mask: 255.255.255.0 Network: 20.1.1.0 Attached Router: 20.1.1.1 Attached Router: 20.1.3.1 Nexthops(1): 20.1.1.2 Interface: Ether0:0 VPN5002_8_323E9040: Main#**show ip routing** IP Routing Table for Main Directly Connected Routes: Destination Mask Ref Uses Type Interface 20.1.1.0 FFFFFF00 4587 STIF Ether0:0

```
20.1.1.0 FFFFFFFF 0 STIF Local 20.1.1.1 @FFFFFFFF 36 LocalLocal 20.1.1.255 FFFFFFFF 0 STIF Local
50.1.1.0 FFFFFFFC 5 STIF VPN0:1 50.1.1.0 FFFFFFFF 0 STIF Local 50.1.1.2 @FFFFFFFF 5 LocalLocal
50.1.1.3 FFFFFFFF 0 STIF Local 127.0.0.1 FFFFFFFF 0 STIF Local 172.16.172.16 FFFFFFF0 0 STIF
Ether1:0 172.16.172.16 FFFFFFFF 0 STIF Local 172.16.172.21 @FFFFFFFF 1 LocalLocal 172.16.172.32
FFFFFFFF 0 STIF Local 224.0.0.5 FFFFFFFF 8535 STIF Local 224.0.0.6 FFFFFFFF 0 STIF Local
224.0.0.9 FFFFFFFF 0 STIF Local 255.255.255.255 @FFFFFFFF 5393 LocalLocal Static Routes:
Destination Mask Gateway Metric Ref Uses Type Interface 172.16.172.39 @FFFFFFFF 172.16.172.21 2
0 *Stat VPN0:1 Dynamic Routes: Flash Cfg: 31: Error: Invalid syntax: too few fields Src/
Destination Mask Gateway Metric Ref Uses Type TTL Interface 10.1.1.0 FFFFFF00 50.1.1.1 74 0 OSPF
STUB VPN0:1 10.1.2.1 @FFFFFFFF 50.1.1.1 75 0 OSPF HOST VPN0:1 10.1.3.1 @FFFFFFFF 50.1.1.1 75 0
OSPF HOST VPN0:1 20.1.2.1 @FFFFFFFF 20.1.1.2 11 0 OSPF HOST Ether0:0 20.1.3.1 @FFFFFFFF 20.1.1.2
11 0 OSPF HOST Ether0:0 Configured IP Routes: None. Total Routes in use: 23 Mask -> @Host route
Type -> Redist *rip #ospf VPNGateway set to 172.16.172.17 using interface Ether1:0
VPN5002_8_323E9040: Main#
```

可能出现的错误

- 在使用 GRE over IPSec 时，VPN 5000 集中器在默认情况下会建议传输模式。当 Cisco IOS 路由器的隧道模式配置不正确时，就会发生这些错误。**IOS 调试**
```
2d21h: ISAKMP (0:23): Checking IPSec proposal 1
2d21h: ISAKMP: transform 1, ESP_DES
2d21h: ISAKMP: attributes in transform:
2d21h: ISAKMP: SA life type in seconds
2d21h: ISAKMP: SA life duration (VPI) of 0x0 0x1 0x51 0x80
2d21h: ISAKMP: SA life type in kilobytes
2d21h: ISAKMP: SA life duration (VPI) of 0x0 0x10 0x0 0x0
2d21h: ISAKMP: encaps is 2
2d21h: ISAKMP: authenticator is HMAC-MD5
2d21h: IPSEC(validate_proposal): invalid transform
   proposal flags -- 0x0
```
VPN 5000 日志
```
lan-lan-VPN0:1:[172.16.172.39]: received notify from partner --
notify: NO PROPOSAL CHOSEN
```
- 如果 Cisco IOS 路由器未配置为忽略 OSPF 最大传输单元 (MTU)，则在路由器与 VPN 5000 集中器之间形成邻接时，就会发生这些错误。路由器上的 **show ip ospf ne** 命令陷入 EXSTART 状态而停滞不动。在 Cisco IOS 路由器上，**debug ip ospf adj** 命令显示以下输出。
```
2d22h: OSPF: Nbr 20.1.1.1 has larger interface MTU
2d22h: OSPF: Rcv DBD from 20.1.1.1 on Tunnel0 seq 0x104A opt
   0x2 flag 0x0 len 132 mtu 1500 state EXSTART
```
解决方法是在路由器的隧道接口下使用 **ip ospf mtu-ignore** 命令以禁用 MTU 检查。

相关信息

- Cisco VPN 5000 系列集中器支持页面
- Cisco VPN 5000 客户端支持页
- IPSec（IP 安全协议）支持页
- 技术支持 - Cisco Systems