

使用静态路由在 Cisco IOS 路由器与 VPN 5000 集中器之间配置 GRE over IPsec

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

[故障排除命令](#)

[调试输出示例](#)

[隧道模式的误配置](#)

[相关信息](#)

简介

本文描述如何配置在IPsec的通用路由封装(GRE)在Cisco VPN 5000系列集中器和Cisco路由器运行Cisco IOS软件之间。GRE-over-IPsec功能在VPN 5000集中器6.0(19)软件版本中引入。

在本例中，静态路由用于路由在通道间的数据包。

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)
- Cisco 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。

IPSec的GRE配置在1720-1路由器运行Cisco IOS软件和VPN 5002集中器之间。在路由器和VPN集中器后，有通过开放最短路径优先(OSPF)通告的多个网络。OSPF在GRE隧道内运行在路由器和VPN集中器之间。

- 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

配置

本文档使用以下配置。

- [1720-1路由器](#)
- [VPN 5002集中器](#)

注意：使用Cisco IOS软件版本12.2(13)T和以后(更高的被编号的T系列代码，12.3及以后代码)，您必须仅应用已配置的IPSec加密映射到物理接口。您必须不再应用在GRE隧道接口的加密映射。有在物理和隧道接口的加密映射，当您使用Cisco IOS软件版本12.2.(13)T时，并且以后应该仍然工作，但是Cisco系统建议您应用在仅物理接口的加密映射。

1720-1路由器

```
Current configuration : 1305 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$RqD0Lq1qbSFCCjVELFLfH/
!
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 map vpn 10 ipsec-isakmp set peer
172.16.172.21 set transform-set myset match address 102
! cns event-service server !!! interface Tunnel0 ip
address 50.1.1.1 255.255.255.252 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 ! ip classless ip route 0.0.0.0
0.0.0.0 172.16.172.33 ip route 10.1.0.0 255.255.0.0
10.1.1.1 ip route 20.1.0.0 255.255.0.0 Tunnel0 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 ! no scheduler
allocate end

```

VPN 5002集中器

```

[ General ]
VPNGateway                = 172.16.172.17
EthernetAddress           = 00:05:32:3e:90:40
DeviceType                = VPN 5002/8 Concentrator
ConfiguredOn              = Timeserver not configured
ConfiguredFrom            = Command Line, from Console

[ IKE Policy ] Protection = SHA_DES_G1 Protection =
MD5_DES_G2 Protection = MD5_DES_G1 [ Tunnel Partner VPN
1 ] KeyLifeSecs = 3500 KeepaliveInterval = 120
TunnelType = GREinIPSec InactivityTimeout = 120
Transform = ESP(MD5,DES) BindTo = "Ethernet 1:0"
SharedKey = "cisco123" Certificates = Off Mode = Main
KeyManage = Reliable Partner = 172.16.172.39 [ IP VPN 1
] HelloInterval = 10 SubnetMask = 255.255.255.252
IPAddress = 50.1.1.2 DirectedBroadcast = Off Numbered =
On Mode = Routed [ IP Ethernet 1:0 ] Mode = Routed
SubnetMask = 255.255.255.240 IPBroadcast = 172.16.172.32
IPAddress = 172.16.172.21 [ IP Ethernet 0:0 ] Mode =
Routed IPBroadcast = 20.1.1.255 SubnetMask =
255.255.255.0 IPAddress = 20.1.1.1 [ Logging ] Level =
Debug LogToAuxPort = On Enabled = On [ Ethernet
Interface Ethernet 0:0 ] DUPLEX = half SPEED = 10meg [
IP Static ] 0.0.0.0 0.0.0.0 20.1.1.5 1 10.1.1.0
255.255.255.0 VPN 1 1 10.1.2.0 255.255.255.0 VPN 1 1
10.1.3.0 255.255.255.0 VPN 1 1 Configuration size is
1696 out of 65500 bytes.

```

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。

- 这些命令在Cisco IOS路由器可以运行。**show crypto isakmp sa** —显示所有当前互联网安全协会和密钥管理协议(ISAKMP)安全关联(SA)。**show crypto ipsec sa** - 显示所有当前 IPsec SA。**show crypto engine connection active** —显示每数据包加密/解密计数器IPsec SAS。

- 您能运行这些on命令VPN 5002集中器。**show system log buffer** - 显示基本 syslog 信息。**vpn trace dump** —显示关于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](#)

注意： 在发出 **debug** 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

您能运行这些on命令Cisco IOS路由器。

- **debug crypto isakmp** —显示关于互联网密钥交换(IKE)阶段的详细信息我(主模式)协商。
- **debug crypto ipsec** —显示关于IKE第II阶段(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](#)

路由器和VPN集中器的Debug输出示例显示此处。

- [Cisco IOS 路由器](#)
- [VPN 5002集中器](#)

[在Cisco IOS路由器的调试](#)

debug crypto isakmp和**debug crypto ipsec on**命令输出路由器显示此处。

```
5d20h: ISAKMP (0:0): received packet from 172.16.172.21 (N) NEW SA
5d20h: ISAKMP: local port 500, remote port 500
5d20h: ISAKMP (0:81): processing SA payload. message ID = 0
5d20h: ISAKMP (0:81): found peer pre-shared key matching 172.16.172.21
5d20h: ISAKMP (0:81): Checking ISAKMP transform 1 against priority 1 policy
5d20h: ISAKMP:      encryption DES-CBC
5d20h: ISAKMP:      hash SHA
5d20h: ISAKMP:      auth pre-share
5d20h: ISAKMP:      default group 1
5d20h: ISAKMP (0:81): atts are not acceptable. Next payload is 3
5d20h: ISAKMP (0:81): Checking ISAKMP transform 2 against priority 1 policy
5d20h: ISAKMP:      encryption DES-CBC
5d20h: ISAKMP:      hash MD5
5d20h: ISAKMP:      auth pre-share
5d20h: ISAKMP:      default group 2
5d20h: ISAKMP (0:81): atts are not acceptable. Next payload is 3
5d20h: ISAKMP (0:81): Checking ISAKMP transform 3 against priority 1 policy
5d20h: ISAKMP:      encryption DES-CBC
5d20h: ISAKMP:      hash MD5
5d20h: ISAKMP:      auth pre-share
5d20h: ISAKMP:      default group 1
5d20h: ISAKMP (0:81): atts are acceptable. Next payload is 0
5d20h: ISAKMP (0:81): processing vendor id payload
5d20h: ISAKMP (0:81): SA is doing pre-shared key authentication
using id type ID_IPV4_ADDR
5d20h: ISAKMP (0:81): sending packet to 172.16.172.21 (R) MM_SA_SETUP
```

```
5d20h: ISAKMP (0:81): received packet from 172.16.172.21 (R) MM_SA_SETUP
5d20h: ISAKMP (0:81): processing KE payload. message ID = 0
5d20h: ISAKMP (0:81): processing NONCE payload. message ID = 0
5d20h: ISAKMP (0:81): found peer pre-shared key matching 172.16.172.21
5d20h: ISAKMP (0:81): SKEYID state generated
5d20h: ISAKMP (0:81): sending packet to 172.16.172.21 (R) MM_KEY_EXCH
5d20h: ISAKMP (0:81): received packet from 172.16.172.21 (R) MM_KEY_EXCH
5d20h: ISAKMP (0:81): processing ID payload. message ID = 0
5d20h: ISAKMP (0:81): processing HASH payload. message ID = 0
5d20h: ISAKMP (0:81): SA has been authenticated with 172.16.172.21
5d20h: ISAKMP (81): ID payload
    next-payload : 8
    type          : 1
    protocol      : 17
    port          : 500
    length        : 8
5d20h: ISAKMP (81): Total payload length: 12
5d20h: ISAKMP (0:81): sending packet to 172.16.172.21 (R) QM_IDLE
5d20h: ISAKMP (0:81): received packet from 172.16.172.21 (R) QM_IDLE
5d20h: ISAKMP (0:81): processing HASH payload. message ID = 241
5d20h: ISAKMP (0:81): processing SA payload. message ID = 241
5d20h: ISAKMP (0:81): Checking IPsec proposal 1
5d20h: ISAKMP: transform 1, ESP_DES
5d20h: ISAKMP:   attributes in transform:
5d20h: ISAKMP:     SA life type in seconds
5d20h: ISAKMP:     SA life duration (VPI) of  0x0 0x0 0xD 0xAC
5d20h: ISAKMP:     SA life type in kilobytes
5d20h: ISAKMP:     SA life duration (VPI) of  0x0 0x10 0x0 0x0
5d20h: ISAKMP:     encaps is 2
5d20h: ISAKMP:     authenticator is HMAC-MD5
5d20h: ISAKMP (0:81): atts are acceptable.
5d20h: 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
5d20h: ISAKMP (0:81): processing NONCE payload. message ID = 241
5d20h: ISAKMP (0:81): processing ID payload. message ID = 241
5d20h: ISAKMP (81): ID_IPV4_ADDR src 172.16.172.21 prot 47 port 0
5d20h: ISAKMP (0:81): processing ID payload. message ID = 241
5d20h: ISAKMP (81): ID_IPV4_ADDR dst 172.16.172.39 prot 47 port 0
5d20h: ISAKMP (0:81): asking for 1 spis from ipsec
5d20h: IPSEC(key_engine): got a queue event...
5d20h: IPSEC(spi_response): getting spi 895566248 for SA
    from 172.16.172.21  to 172.16.172.39  for prot 3
5d20h: ISAKMP: received ke message (2/1)
5d20h: ISAKMP (0:81): sending packet to 172.16.172.21 (R) QM_IDLE
5d20h: ISAKMP (0:81): received packet from 172.16.172.21 (R) QM_IDLE
5d20h: ISAKMP (0:81): Creating IPsec SAs
5d20h:     inbound SA from 172.16.172.21 to 172.16.172.39
    (proxy 172.16.172.21 to 172.16.172.39)
5d20h:     has spi 0x356141A8 and conn_id 362 and flags 0
5d20h:     lifetime of 3500 seconds
5d20h:     lifetime of 1048576 kilobytes
5d20h:     outbound SA from 172.16.172.39  to 172.16.172.21
    (proxy 172.16.172.39  to 172.16.172.21 )
5d20h:     has spi 337 and conn_id 363 and flags 0
5d20h:     lifetime of 3500 seconds
5d20h:     lifetime of 1048576 kilobytes
5d20h: ISAKMP (0:81): deleting node 241 error FALSE reason
"quick mode done (await())"
5d20h: IPSEC(key_engine): got a queue event...
```

```
5d20h: 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= 0x356141A8(895566248), conn_id= 362, keysize= 0, flags= 0x0
5d20h: 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= 0x151(337), conn_id= 363, keysize= 0, flags= 0x0
5d20h: IPSEC(create_sa): sa created,
(sa) sa_dest= 172.16.172.39, sa_prot= 50,
sa_spi= 0x356141A8(895566248),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 362
5d20h: IPSEC(create_sa): sa created,
(sa) sa_dest= 172.16.172.21, sa_prot= 50,
sa_spi= 0x151(337),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 363
5d20h: IPSEC(add_sa): peer asks for new SAs -- expire current in 120 sec.,
(sa) sa_dest= 172.16.172.21, sa_prot= 50,
sa_spi= 0x150(336),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 361,
(identity) local= 172.16.172.39, remote= 172.16.172.21,
local_proxy= 172.16.172.39/255.255.255.255/47/0 (type=1),
remote_proxy= 172.16.172.21/255.255.255.255/47/0 (type=1)
1720-1#
```

```
1720-1#show crypto isakmp sa dst src state conn-id slot 172.16.172.39 172.16.172.21 QM_IDLE 81 0
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 81 FastEthernet0 172.16.172.39 set HMAC_MD5+DES_56_CB 0 0 362 FastEthernet0
172.16.172.39 set HMAC_MD5+DES_56_CB 0 23194 363 FastEthernet0 172.16.172.39 set
HMAC_MD5+DES_56_CB 23195 0
```

[在VPN 5002集中器的调试](#)

在VPN集中器的系统日志输出显示此处。

```
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
```

```
VPN5002_8_323E9040: Main#show vpn partner verbose 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 00:00:13:26 Auth/Encrypt:
MD5e/DES User Auth: Shared Key Access: Static Peer: 172.16.172.39 Local: 172.16.172.21
Start:14518 seconds Managed:15299 seconds State:imnt_maintenance IOP slot 1: No active
connections found. VPN5002_8_323E9040: Main#show vpn statistics verbose Current In High Running
Script Script Script Active Negot Water Total Starts OK Error -----
----- Users 0 0 0 0 0 0 Partners 1 0 1 81 81 1 158 Total 1 0 1 81 81 1
158 Stats VPN0:1 Wrapped 79733 Unwrapped 79734 BadEncap 0 BadAuth 0 BadEncrypt 0 rx IP 79749 rx
IPX 0 rx Other 0 tx IP 79761 tx IPX 0 tx Other 0 IKE rekey 0 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 Partners 0 0 0 0 0 0 0 Total 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
```

[隧道模式的误配置](#)

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路由器为隧道模式时是不正确的配置的，然后此错误出现。

在Cisco IOS路由器的Debug输出显示此处。

```
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 5002集中器上的日志显示条目类似于此输出。

```
lan-lan-VPN0:1:[172.16.172.39]: received notify from partner --
```

notify: NO PROPOSAL CHOSEN

[相关信息](#)

- [Cisco VPN 5000 系列集中器终止销售公告](#)
- [Cisco VPN 5000 集中器支持页](#)
- [Cisco VPN 5000 客户端支持页](#)
- [IPSec 支持页面](#)
- [技术支持 - Cisco Systems](#)