

Configurando GRE sobre IPSec entre um roteador IOS Cisco e um concentrador VPN 5000 usando roteamento dinâmico

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Cisco IOS Router](#)

[VPN 5000 Concentrator](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Exemplo de debug](#)

[que pode dar errado](#)

[Informações Relacionadas](#)

[Introdução](#)

Esta configuração de exemplo descreve como configurar o Generic Routing Encapsulation (GRE) sobre o IPsec entre um concentrador do Cisco VPN 5000 e um roteador Cisco que executam o software de Cisco IOS®. Os recursos GRE sobre IPsec foram introduzidos no software release do VPN 5000 concentrator 6.0(19). O protocolo de roteamento dinâmico do Open Shortest Path First (OSPF) é usado nesta amostra para distribuir o tráfego através do túnel VPN.

[Pré-requisitos](#)

[Requisitos](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Software Release 12.2(3) de Cisco IOS®
- Software Release 6.0(19) do VPN 5000 concentrator

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

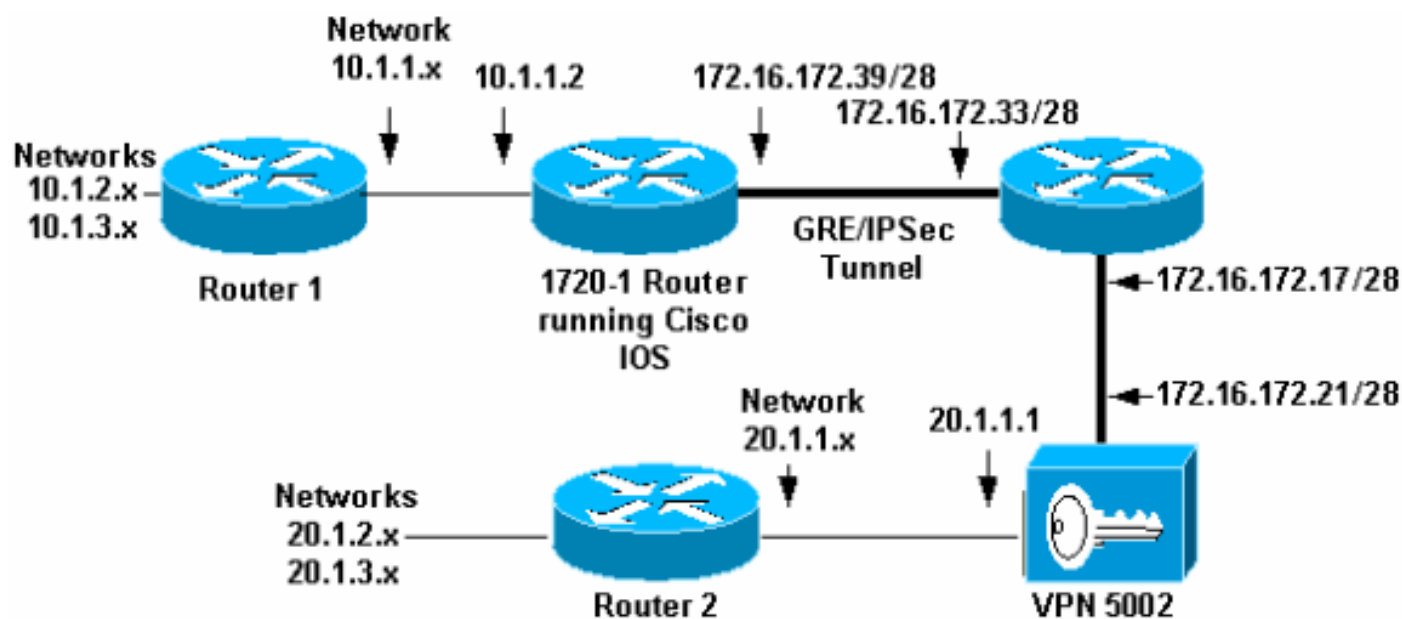
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Note: Para localizar informações adicionais sobre os comandos usados neste documento, utilize a Ferramenta Command Lookup (somente clientes [registrados](#)).

Diagrama de Rede

Este documento utiliza a configuração de rede mostrada neste diagrama.



O GRE sobre o IPsec é configurado entre o roteador do Cisco IOS (1720-1) e o VPN 5002 concentrator. Atrás destes dispositivos, as redes múltiplas são anunciadas através do OSPF, que é executado dentro do túnel GRE entre 1720-1 e do VPN 5002.

Estas redes são atrás do 1720-1 Router.

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

Estas redes são atrás do VPN 5002 concentrator.

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

Note: Para esta topologia, todos os segmentos de rede são postos na área do OSPF 0.

Configurações

Este documento utiliza estas configurações.

- [Cisco IOS Router](#)
- [VPN 5000 Concentrator](#)

Cisco IOS Router

```
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$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 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 Concentrator

```
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#

```

O dispositivo de IOS e o VPN 5000 concentrator são configurados para trazer acima um com o outro um túnel GRE. O IOS Router igualmente tem um mapa cripto dinâmico configurado para o endereço IP de Um ou Mais Servidores Cisco ICM NT do VPN 5000 concentrator. A configuração de túnel do VPN5000 reflete que inicia um túnel do GRE-com-transporte-MODE-IPsec ao dispositivo de IOS. Quando o dispositivo de IOS começa, não tem nenhuma rota para destinos através do túnel. Não envia o tráfego de rede privada na claro. Quando o concentrator VPN começa, negocia automaticamente a associação de segurança cripto (SA) para proteger o tráfego GRE entre os dois pares. Neste momento, o túnel é em serviço e as duas rotas de intercâmbio dos pares para as redes de participação. Do concentrator VPN as re-chaves continuamente a conexão com base nas palavras-chaves de "InactivityTimeout" e de "KeepAliveInterval". Se o IOS Router força uma re-chave, os dois pares não concordam com que SA a se usar e o concentrator VPN renegocia o túnel devido aos segundos *x da* inatividade (onde *x* representa o valor especificado em "InactivityTimeout").

Note: Esta configuração de túnel fica acima para sempre. Não há nenhuma opção de desconexão por inatividade. Este túnel não deve ser usado em link de usos faturado caro, ou onde o roteador (IO) remoto é esperado desligar após períodos ociosos.

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A [Output Interpreter Tool \(somente clientes registrados\)](#) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

Cisco IOS Router

- **mostre isakmp cripto sa** — Mostra todo o Internet Security Association and Key Management Protocol (ISAKMP) atual SA.
- **mostre IPsec cripto sa** — Mostra todo o IPsec atual SA.
- **show crypto engine connection active** — Mostra o contador da criptografia de pacote de informação/descriptografia por IPsec SA.

VPN 5000 Concentrator

- **Show System Log Buffer** — Mostra a informação do syslog básica.
- **descarga do traço do vpn** — Mostra a informação detalhada em processos VPN.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos para Troubleshooting

Estes comandos podem ser usados no roteador do Cisco IOS.

Note: Antes de emitir **comandos debug**, consulte [Informações importantes sobre comandos debug](#).

- **isakmp do debug crypto** — Mostra-me a informação detalhada na fase de intercâmbio de chave de Internet (IKE) negociação (do modo principal).
- **IPsec do debug crypto** — Mostra a informação detalhada na negociação da fase II IKE (Quick Mode).
- **motor do debug crypto** — Debuga a criptografia de pacote de informação/descriptografia e o processo do Diffie-Hellman (DH).

Exemplo de debug

Esta seção fornece o exemplo de debug para os dispositivos da configuração.

- [Cisco IOS Router](#)
- [VPN 5000 Concentrator](#)

Cisco IOS Router

Esta saída foi gerada usando os comandos **debug crypto isakmp** e **debug crypto ipsec** no roteador do Cisco IOS. Este é debug correto no Cisco IOS roteador e no VPN 5000 concentrator.

```
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 Concentrator

VPN5002_8_323E9040: Main#show vpn partner ver

Port Number	Partner Address	Partner Port	Default Partner	Bindto Address	Connect 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 Active	In Negot	High Water	Running Total	Script Starts	Script OK	Script 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 Active	In Negot	High Water	Running Total	Script Starts	Script OK	Script 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	FFFFFFF0	4587	STIF	Ether0:0	
20.1.1.0	FFFFFFF0	0	STIF	Local	
20.1.1.1	@FFFFFFF	36	Local	Local	
20.1.1.255	FFFFFFF0	0	STIF	Local	
50.1.1.0	FFFFFFFC	5	STIF	VPN0:1	
50.1.1.0	FFFFFFF0	0	STIF	Local	
50.1.1.2	@FFFFFFF	5	Local	Local	
50.1.1.3	FFFFFFF0	0	STIF	Local	


```

127.0.0.1      FFFFFFFF      0 STIF Local
172.16.172.16 FFFFFFFF0     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         FFFFFFFF0 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#

que pode dar errado

- O VPN 5000 concentrator propõe o modo de transporte à revelia quando o GRE sobre o IPsec é usado. Quando o roteador do Cisco IOS é desconfigurado para o modo de túnel, estes erros resultam. **Depuração IOS**

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 Active	In Negot	High Water	Running Total	Script Starts	Script OK	Script 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	FFFFFFF0	4587	STIF	Ether0:0	
20.1.1.0	FFFFFFFF	0	STIF	Local	
20.1.1.1	@FFFFFFFF	36	Local	Local	
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	Local	Local	
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	Local	Local	
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	Local	Local	

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	FFFFFFF0	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#

Log VPN5000

VPN5002_8_323E9040: Main#show vpn partner ver

Port Number	Partner Address	Partner Port	Default Partner	Bindto Address	Connect 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 Active	In Negot	High Water	Running Total	Script Starts	Script OK	Script 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 Active	In Negot	High Water	Running Total	Script Starts	Script OK	Script 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         FFFFFFF0  4587  STIF  Ether0:0
20.1.1.0         FFFFFFFF  0     STIF  Local
20.1.1.1         @FFFFFFF  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         @FFFFFFF  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   @FFFFFFF  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          FFFFFFF00  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#

- Se o roteador do Cisco IOS não está configurado para ignorar as unidades de transmissão máxima OSPF (MTU), estes erros resultam quando a adjacência entre o roteador e o VPN 5000 concentrator é formada. O comando `show ip ospf ne` no roteador é colado no estado de EXSTART.No roteador do Cisco IOS, o comando `debug ip ospf adj` mostra esta saída.

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
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 Active	In Negot	High Water	Running Total	Script Starts	Script OK	Script 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	FFFFFFF0	4587	STIF	Ether0:0	
20.1.1.0	FFFFFFFF	0	STIF	Local	
20.1.1.1	@FFFFFFFF	36	Local	Local	
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	Local	Local	
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	Local	Local	
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	Local	Local	

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	FFFFFFF0	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#

A ação alternativa é usar o comando **ip ospf mtu-ignore** sob a interface de túnel do roteador desabilitar a verificação MTU.

[Informações Relacionadas](#)

- [Página de suporte do Concentradores Cisco VPN série 5000](#)
- [Página de suporte ao cliente do Cisco VPN 5000](#)

- [Página de suporte do IPSec \(protocolo de segurança IP\)](#)
- [Suporte Técnico - Cisco Systems](#)