

Configuración de GRE sobre IPSec entre un router del IOS de Cisco y un concentrador VPN 5000 mediante ruteo dinámico.

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Router del Cisco IOS](#)

[Concentrador VPN 5000](#)

[Troubleshooting](#)

[Comandos para resolución de problemas](#)

[Ejemplo de resultado del comando debug](#)

[Qué Puede Salir Mal](#)

[Información Relacionada](#)

[Introducción](#)

Esta configuración de muestra describe cómo configurar el Generic Routing Encapsulation (GRE) sobre el IPSec entre un concentrador del Cisco VPN 5000 y un router Cisco que funcionan con el software de Cisco IOS®. Función de GRE sobre IPSec fue introducido en la versión de software del VPN 5000 concentrator 6.0(19). El Dynamic Routing Protocol del Open Shortest Path First (OSPF) se utiliza en esta muestra para rutear el tráfico a través del túnel VPN.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

La información que contiene este documento se basa en las siguientes versiones de software y

hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

[Convenciones](#)

Para obtener más información sobre las convenciones del documento, consulte las [Convenciones de Consejos Técnicos de Cisco](#).

[Configurar](#)

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para clientes [registrados](#)).

[Diagrama de la red](#)

Este documento utiliza la configuración de red que se muestra en el siguiente diagrama.

El GRE sobre IPSec se configura entre el router del Cisco IOS (1720-1) y el concentrador VPN 5002. Detrás de estos dispositivos, las Redes múltiples se hacen publicidad vía el OSPF, que se ejecuta dentro del túnel GRE entre 1720-1 y del VPN 5002.

Estas redes están detrás del 1720-1 Router.

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

Estas redes están detrás del concentrador VPN 5002.

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

Nota: Para esta topología, todos los segmentos de red se ponen en la área OSPF 0.

[Configuraciones](#)

Este documento usa estas configuraciones.

- [Router del Cisco IOS](#)
- [Concentrador VPN 5000](#)

Router del Cisco IOS

```
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
```

Concentrador VPN 5000

```
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 ConcentratorConfiguredOn = 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#
```

El dispositivo IOS y el VPN 5000 concentrator se configuran para sacar a colación un túnel GRE con uno a. El router IOS también tiene una correspondencia cifrada dinámica configurada para la dirección IP del VPN 5000 concentrator. La configuración del túnel VPN5000 refleja que inicia un túnel del GRE-con-transporte-MODE-IPSec al dispositivo IOS. Cuando el dispositivo IOS comienza, no tiene ninguna ruta para los destinos a través del túnel. No remite el tráfico de red privada en el claro. Cuando el concentrador VPN comienza, negocia automáticamente la asociación de seguridad crypto (SA) para proteger el tráfico GRE entre los dos pares. En este momento, el túnel es en servicio y las dos rutas del intercambio de los pares para las redes participantes. El concentrador VPN reintroduce continuamente la conexión en base de las palabras claves de "InactivityTimeout" y de "KeepAliveInterval". Si el router IOS fuerza una reintroducción, los dos pares no están de acuerdo con qué SA a utilizar y el concentrador VPN renegocia el túnel debido a los segundos *x de la* inactividad (donde *x* representa el valor especificado en "InactivityTimeout").

Nota: Esta configuración del túnel permanece para arriba para siempre. No hay opción de inactividad-desconexión. Este túnel no se debe utilizar en los links cuyo uso es pago y costoso, o donde se espera que al router remoto (IOS) desconecte después de los períodos inactivos.

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

La herramienta [Output Interpreter](#) (sólo para clientes [registrados](#)) permite utilizar algunos comandos "show" y ver un análisis del resultado de estos comandos.

Router del Cisco IOS

- **muestre isakmp crypto sa** — Muestra todo el Internet Security Association and Key Management Protocol (ISAKMP) actual SA.
- **muestre IPsec crypto sa** — Muestra todo el IPsec actual SA.
- **show crypto engine connection active** — Muestra el contador de la encriptación de paquetes/del desciframiento por IPsec SA.

Concentrador VPN 5000

- **show system log buffer** — Muestra la información básica de Syslog.
- **volcado de la traza del vpn** — Muestra la información detallada en los procesos VPN.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de

configuración.

Comandos para resolución de problemas

Estos comandos se pueden utilizar en el router del Cisco IOS.

Nota: Antes de ejecutar un comando debug, consulte Información Importante sobre Comandos Debug.

- **isakmp del debug crypto** — Muestra la información detallada en la negociación de la fase de intercambio de claves de Internet (IKE) I (modo principal).
- **IPSec del debug crypto** — Muestra la información detallada en la negociación de la fase II IKE (Quick Mode).
- **motor del debug crypto** — Encriptación de paquetes de los debugs/desciframiento y proceso del Diffie-Hellman (DH).

Ejemplo de resultado del comando debug

Esta sección proporciona el ejemplo de salida del debug para los dispositivos de configuración.

- [Router del Cisco IOS](#)
- [Concentrador VPN 5000](#)

Router del Cisco IOS

Esta salida fue generada usando los **comandos debug crypto isakmp y debug crypto ipsec** en el router del Cisco IOS. Éste es debug correcta en el router y el VPN 5000 concentrator del Cisco IOS.

```
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

```

Concentrador VPN 5000

```

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 FFFFFFFF0 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 FFFFFFFF 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 FFFFFFFF0 0 STIF
Ether1:0 172.16.172.16 FFFFFFFF 0 STIF Local 172.16.172.21 @FFFFFFF 1 LocalLocal 172.16.172.32
FFFFFFF 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 @FFFFFFF 5393 LocalLocal Static Routes:
Destination Mask Gateway Metric Ref Uses Type Interface 172.16.172.39 @FFFFFFF 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 @FFFFFFF 50.1.1.1 75 0 OSPF HOST VPN0:1 10.1.3.1 @FFFFFFF 50.1.1.1 75 0
OSPF HOST VPN0:1 20.1.2.1 @FFFFFFF 20.1.1.2 11 0 OSPF HOST Ether0:0 20.1.3.1 @FFFFFFF 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#

```

Qué Puede Salir Mal

- El VPN 5000 concentrator propone el modo de transporte por abandono cuando se utiliza el GRE sobre IPsec. Cuando configuran mal al router del Cisco IOS para el modo túnel, estos errores resultan. **Depuración de IOS**

```

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 -- 0x0Registro VPN5000lan-lan-VPN0:1:[172.16.172.39]: received notify
from partner --
notify: NO PROPOSAL CHOSEN

```

- Si no configuran al router del Cisco IOS para ignorar las unidades de transmisión máxima OSPF (MTU), estos errores resultan cuando la adyacencia entre el router y el VPN 5000 concentrator se forma. Pegan al **comando show ip ospf ne** en el router en el estado EXSTART. En el router del Cisco IOS, el **comando debug ip ospf adj** muestra esta salida.

```

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

```

La solución alternativa es utilizar el **comando ip ospf mtu-ignore** bajo interfaz del túnel del router de inhabilitar la verificación de MTU.

Información Relacionada

- [Página de soporte del Concentradores Cisco VPN de la serie 5000](#)
- [Página de soporte para Cisco VPN 5000 Client](#)
- [Página de Soporte de IPsec \(Protocolo de Seguridad IP\)](#)
- [Soporte Técnico - Cisco Systems](#)