

Configuring GRE Over IPSec Between a Cisco IOS Router and a VPN 5000 Concentrator Using Dynamic Routing

Document ID: 3968

Cisco has announced the end of sales for the Cisco VPN 5000 Series Concentrators. For more information, please see the [End-of-Sales Announcement](#).

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations

Verify

- Cisco IOS Router
- VPN 5000 Concentrator

Troubleshoot

- Troubleshooting Commands
- Sample Debug Output
- What Can Go Wrong

Related Information

Introduction

This sample configuration describes how to configure generic routing encapsulation (GRE) over IPSec between a Cisco VPN 5000 Concentrator and a Cisco router running Cisco IOS® software. The GRE-over-IPSec feature was introduced in the VPN 5000 Concentrator 6.0(19) software release. The Open Shortest Path First (OSPF) dynamic routing protocol is used in this sample to route traffic across the VPN tunnel.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco IOS® Software Release 12.2(3)
- VPN 5000 Concentrator Software Release 6.0(19)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

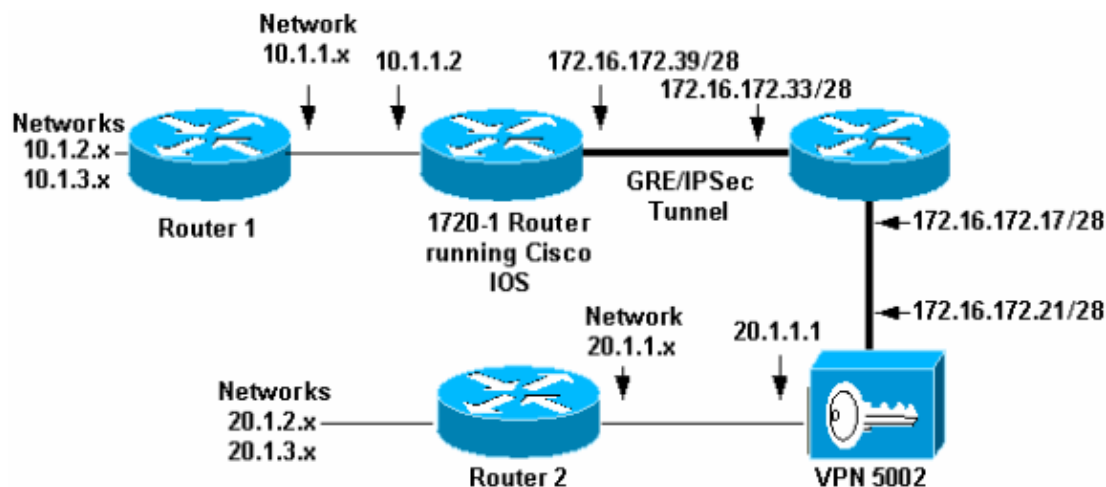
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

Network Diagram

This document uses the network setup shown in this diagram.



GRE over IPSec is configured between the Cisco IOS router (1720–1) and the VPN 5002 Concentrator. Behind these devices, multiple networks are advertised via OSPF, which runs within the GRE tunnel between 1720–1 and VPN 5002.

These networks are behind the 1720–1 router.

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

These networks are behind the VPN 5002 Concentrator.

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

Note: For this topology, all network segments are put in OSPF area 0.

Configurations

This document uses these configurations.

- 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#

```

Both the IOS device and the VPN 5000 Concentrator are configured to bring up a GRE tunnel with each other. The IOS router also has a dynamic crypto map configured for the IP address of the VPN 5000 Concentrator. The VPN 5000's tunnel configuration reflects that it initiates a GRE-with-transport-mode-IPSec tunnel to the IOS device. When the IOS device starts, it has no routes for destinations through the tunnel. It does not forward private network traffic in the clear. When the VPN Concentrator starts, it automatically negotiates the crypto security association (SA) to protect GRE traffic between the two peers. At this point, the tunnel is up and running and the two peers exchange routes for the participating networks. The VPN Concentrator continually re-keys the connection on the basis of the "InactivityTimeout" and "KeepAliveInterval" keywords. If the IOS router forces a re-key, the two peers do not agree on which SA to use and the VPN Concentrator re-negotiates the tunnel due to x seconds of inactivity (where x represents the value specified in "InactivityTimeout").

Note: This tunnel configuration stays up forever. There is no inactivity-disconnection option. This tunnel should not be used on expensive usage-billed links, or where the remote (IOS) router is expected to disconnect after idle periods.

Verify

This section provides information you can use to confirm your configuration is working properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only), which allows you to view an analysis of **show** command output.

Cisco IOS Router

- **show crypto isakmp sa** Shows all current Internet Security Association and Key Management Protocol (ISAKMP) SAs.
- **show crypto ipsec sa** Shows all current IPsec SAs.
- **show crypto engine connection active** Shows packet encryption/decryption counter per IPsec SA.

VPN 5000 Concentrator

- **show system log buffer** Shows basic syslog information.
- **vpn trace dump** Shows detailed information on VPN processes.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

These commands can be used on the Cisco IOS router.

Note: Before issuing **debug** commands, please see Important Information on Debug Commands.

- **debug crypto isakmp** Shows detailed information on Internet Key Exchange (IKE) phase I (Main Mode) negotiation.
- **debug crypto ipsec** Shows detailed information on IKE phase II (Quick Mode) negotiation.
- **debug crypto engine** Debugs packet encryption/decryption and Diffie–Hellman (DH) process.

Sample Debug Output

This section provides sample debug output for the configuration devices.

- Cisco IOS Router
- VPN 5000 Concentrator

Cisco IOS Router

This output was generated using the **debug crypto isakmp** and **debug crypto ipsec** commands on the Cisco IOS router. This is good debug on both the Cisco IOS router and 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 pcg 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 pcg 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 pcg 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 pcg 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 pcg sas:

outbound esp sas:

outbound ah sas:

outbound pcg 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#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	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	FFFFFFF0	4587	STIF	Ether0:0	
20.1.1.0	FFFFFFF0	0	STIF	Local	
20.1.1.1	@FFFFFFF	36	LocalLocal		
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	LocalLocal		
50.1.1.3	FFFFFFF0	0	STIF	Local	
127.0.0.1	FFFFFFF0	0	STIF	Local	
172.16.172.16	FFFFFFF0	0	STIF	Ether1:0	
172.16.172.16	FFFFFFF0	0	STIF	Local	
172.16.172.21	@FFFFFFF	1	LocalLocal		
172.16.172.32	FFFFFFF0	0	STIF	Local	
224.0.0.5	FFFFFFF0	8535	STIF	Local	
224.0.0.6	FFFFFFF0	0	STIF	Local	
224.0.0.9	FFFFFFF0	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         FFFFFFF0  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#

What Can Go Wrong

- The VPN 5000 Concentrator proposes transport mode by default when GRE over IPsec is used. When the Cisco IOS router is misconfigured for tunnel mode, these errors result.

◆ IOS Debug

```
2d21h: ISAKMP (0:23): Checking IPsec proposal 1
2d21h: ISAKMP: transform 1, ESP_DES
2d21h: ISAKMP: attributes in transform:
2d21h: ISAKMP: SA life type in seconds
2d21h: ISAKMP: SA life duration (VPI) of 0x0 0x1 0x51 0x80
2d21h: ISAKMP: SA life type in kilobytes
2d21h: ISAKMP: SA life duration (VPI) of 0x0 0x10 0x0 0x0
2d21h: ISAKMP: encaps is 2
2d21h: ISAKMP: authenticator is HMAC-MD5
2d21h: IPSEC(validate_proposal): invalid transform
proposal flags -- 0x0
```

◆ VPN 5000 Log

```
lan-lan-VPN0:1:[172.16.172.39]: received notify from partner --
notify: NO PROPOSAL CHOSEN
```


- If the Cisco IOS router is not configured to ignore OSPF maximum transmission units (MTUs), these errors result when adjacency between the router and the VPN 5000 Concentrator is formed. The **show ip ospf ne** command on the router is stuck on EXSTART state.

On the Cisco IOS router, the **debug ip ospf adj** command shows this output.

```
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
```

The workaround is to use the **ip ospf mtu-ignore** command under the router's tunnel interface to disable MTU checking.

Related Information

- [Cisco VPN 5000 Series Concentrators Support Page](#)
 - [Cisco VPN 5000 Client Support Page](#)
 - [IPSec \(IP Security Protocol\) Support Page](#)
 - [Technical Support – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: May 02, 2008

Document ID: 3968
