고정 라우팅을 사용하여 Cisco IOS 라우터와 VPN 5000 Concentrator 간 GRE over IPSec 구성

목차

소개

이 문서에서는 Cisco VPN 5000 Series Concentrator와 Cisco IOS® 소프트웨어를 실행하는 Cisco 라우터 간에 IPSec을 통한 GRE(Generic Routing Encapsulation)를 구성하는 방법에 대해 설명합니다. GRE-over-IPSec 기능은 VPN 5000 Concentrator 6.0(19) 소프트웨어 릴리스에 도입되었습니다 .

이 예에서는 고정 라우팅을 사용하여 터널을 통해 패킷을 라우팅합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS Software 릴리스 12.2(3)
- Cisco VPN 5000 Concentrator 소프트웨어 버전 6.0(19)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

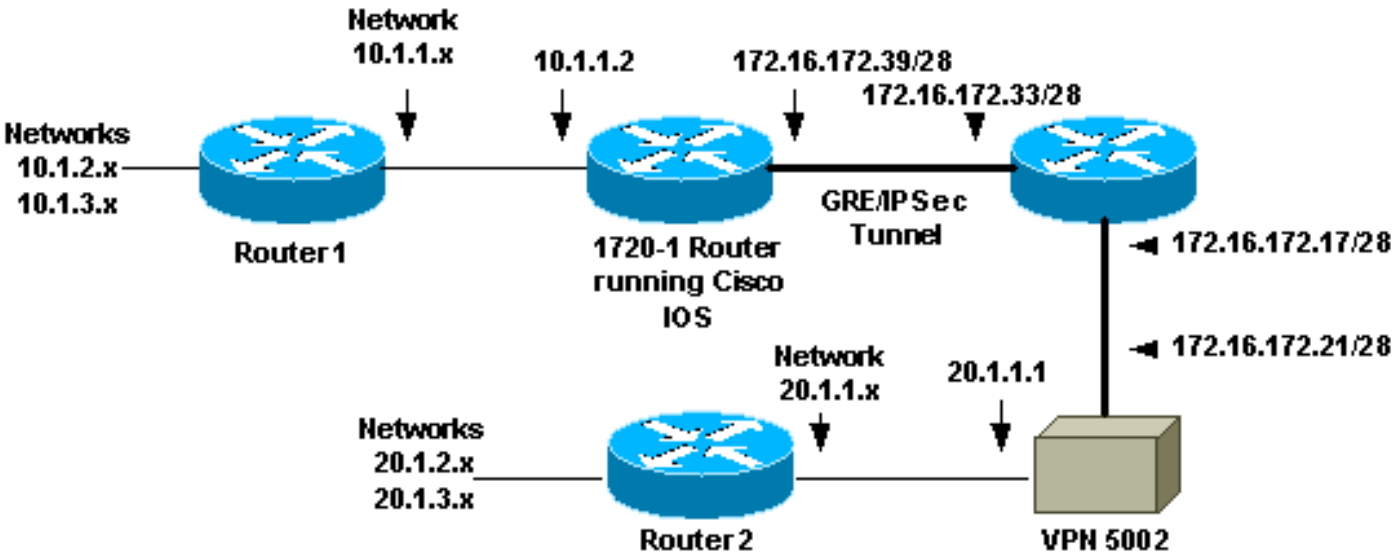
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 이 문서에 사용된 명령에 대한 추가 정보를 찾으려면 명령 조회 도구(등록된 고객만 해당)를 사용합니다.

네트워크 다이어그램

이 문서에서는 이 다이어그램에 표시된 네트워크 설정을 사용합니다.



GRE over IPSec은 Cisco IOS 소프트웨어를 실행하는 1720-1 라우터와 VPN 5002 Concentrator 간에 구성됩니다. 라우터와 VPN Concentrator 뒤에는 OSPF(Open Shortest Path First)를 통해 광고되는 여러 네트워크가 있습니다. OSPF는 라우터와 VPN Concentrator 간의 GRE 터널 내에서 실행됩니다.

- 이러한 네트워크는 1720-1 라우터에 뒤집니다.10.1.1.0/2410.1.2.0/2410.1.3.0/24
- 이러한 네트워크는 VPN 5002 Concentrator 뒤에 있습니다.20.1.1.0/2420.1.2.0/2420.1.3.0/24

구성

이 문서에서는 이러한 구성을 사용합니다.

- 1720-1 라우터
- VPN 5002 Concentrator

참고: Cisco IOS Software Release 12.2(13)T 이상(번호가 높은 T-Train 코드, 12.3 이상 코드)의 경

우 구성된 IPSec 암호화 맵을 물리적 인터페이스에만 적용해야 합니다. 더 이상 GRE 터널 인터페이스에 암호화 맵을 적용할 필요가 없습니다. Cisco IOS Software Releases 12.2.(13)T 이상을 사용할 때 물리적 인터페이스와 터널 인터페이스에 암호화 맵이 있어야 합니다. 그러나 Cisco Systems에서는 물리적 인터페이스에만 암호화 맵을 적용할 것을 권장합니다.

1720-1 라우터

```
Current configuration : 1305 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 1720-1
!
no logging buffered
no logging monitor
enable secret 5 $1$vIzI$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 map vpn 10 ipsec-isakmp
 set peer 172.16.172.21
 set transform-set myset
 match address 102
!
cns event-service server
!
!
!
interface Tunnel0
 ip address 50.1.1.1 255.255.255.252
 tunnel source FastEthernet0
 tunnel destination 172.16.172.21
 crypto map vpn
!
interface FastEthernet0
 ip address 172.16.172.39 255.255.255.240
 speed auto
 crypto map vpn
!
interface Serial0
 ip address 10.1.1.2 255.255.255.0
 encapsulation ppp
!
```

```
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.172.33
ip route 10.1.0.0 255.255.0.0 10.1.1.1
ip route 20.1.0.0 255.255.0.0 Tunnel0
no ip http server
!
access-list 102 permit gre host 172.16.172.39 host
172.16.172.21
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
!
no scheduler allocate
end
```

VPN 5002 Concentrator

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

[ IKE Policy ]
Protection              = SHA_DES_G1
Protection              = MD5_DES_G2
Protection              = MD5_DES_G1

[ Tunnel Partner VPN 1 ]
KeyLifeSecs             = 3500
KeepaliveInterval       = 120
TunnelType              = GREinIPSec
InactivityTimeout       = 120
Transform               = ESP(MD5,DES)
BindTo                  = "Ethernet 1:0"
SharedKey               = "cisco123"
Certificates            = Off
Mode                    = Main
KeyManage               = Reliable
Partner                 = 172.16.172.39

[ IP VPN 1 ]
HelloInterval           = 10
SubnetMask              = 255.255.255.252
IPAddress               = 50.1.1.2
DirectedBroadcast       = Off
Numbered                = On
Mode                    = Routed

[ IP Ethernet 1:0 ]
Mode                    = Routed
SubnetMask              = 255.255.255.240
IPBroadcast             = 172.16.172.32
IPAddress               = 172.16.172.21

[ IP Ethernet 0:0 ]
Mode                    = Routed
IPBroadcast             = 20.1.1.255
SubnetMask              = 255.255.255.0
```

```
IPAddress                = 20.1.1.1

[ Logging ]
Level                    = Debug
LogToAuxPort             = On
Enabled                  = On

[ Ethernet Interface Ethernet 0:0 ]
DUPLEX                   = half
SPEED                    = 10meg


[ IP Static ]
0.0.0.0 0.0.0.0 20.1.1.5 1
10.1.1.0 255.255.255.0 VPN 1 1
10.1.2.0 255.255.255.0 VPN 1 1
10.1.3.0 255.255.255.0 VPN 1 1

Configuration size is 1696 out of 65500 bytes.
```

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

- 이러한 명령은 Cisco IOS 라우터에서 실행할 수 있습니다.**show crypto isakmp sa** - 모든 현재 ISAKMP(Internet Security Association and Key Management Protocol) SA(Security Associations)를 표시합니다.**show crypto ipsec sa** - 현재 모든 IPSec SA를 표시합니다.**show crypto engine connection active(암호화 엔진 연결 활성** 표시) - 각 IPSec SA에 대한 패킷 암호화/암호 해독 카운터를 표시합니다.
- VPN 5002 Concentrator에서 이러한 명령을 실행할 수 있습니다.**show system log buffer**—기본 syslog 정보를 표시합니다.**vpn trace dump** - VPN 프로세스에 대한 자세한 정보를 표시합니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 명령

참고: debug 명령을 실행하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

Cisco IOS 라우터에서 이러한 명령을 실행할 수 있습니다.

- **debug crypto isakmp** - IKE(Internet Key Exchange) 단계 I(Main Mode) 협상에 대한 자세한 정보를 표시합니다.
- **debug crypto ipsec** - IKE phase II(Quick Mode) 협상에 대한 자세한 정보를 표시합니다.
- **debug crypto engine**—패킷 암호화/암호 해독 및 DH(Diffie-Hellman) 프로세스를 디버깅합니다.

디버그 출력 샘플

라우터 및 VPN Concentrator에 대한 샘플 디버그 출력이 여기에 표시됩니다.

- Cisco IOS 라우터
- VPN 5002 Concentrator

Cisco IOS 라우터의 디버깅

라우터의 **debug crypto isakmp** 및 **debug crypto ipsec** 명령의 출력은 여기에 나와 있습니다.

```
5d20h: ISAKMP (0:0): received packet from 172.16.172.21 (N) NEW SA
5d20h: ISAKMP: local port 500, remote port 500
5d20h: ISAKMP (0:81): processing SA payload. message ID = 0
5d20h: ISAKMP (0:81): found peer pre-shared key matching 172.16.172.21
5d20h: ISAKMP (0:81): Checking ISAKMP transform 1 against priority 1 policy
5d20h: ISAKMP:      encryption DES-CBC
5d20h: ISAKMP:      hash SHA
5d20h: ISAKMP:      auth pre-share
5d20h: ISAKMP:      default group 1
5d20h: ISAKMP (0:81): atts are not acceptable. Next payload is 3
5d20h: ISAKMP (0:81): Checking ISAKMP transform 2 against priority 1 policy
5d20h: ISAKMP:      encryption DES-CBC
5d20h: ISAKMP:      hash MD5
5d20h: ISAKMP:      auth pre-share
5d20h: ISAKMP:      default group 2
5d20h: ISAKMP (0:81): atts are not acceptable. Next payload is 3
5d20h: ISAKMP (0:81): Checking ISAKMP transform 3 against priority 1 policy
5d20h: ISAKMP:      encryption DES-CBC
5d20h: ISAKMP:      hash MD5
5d20h: ISAKMP:      auth pre-share
5d20h: ISAKMP:      default group 1
5d20h: ISAKMP (0:81): atts are acceptable. Next payload is 0
5d20h: ISAKMP (0:81): processing vendor id payload
5d20h: ISAKMP (0:81): SA is doing pre-shared key authentication
using id type ID_IPV4_ADDR
5d20h: ISAKMP (0:81): sending packet to 172.16.172.21 (R) MM_SA_SETUP
5d20h: ISAKMP (0:81): received packet from 172.16.172.21 (R) MM_SA_SETUP
5d20h: ISAKMP (0:81): processing KE payload. message ID = 0
5d20h: ISAKMP (0:81): processing NONCE payload. message ID = 0
5d20h: ISAKMP (0:81): found peer pre-shared key matching 172.16.172.21
5d20h: ISAKMP (0:81): SKEYID state generated
5d20h: ISAKMP (0:81): sending packet to 172.16.172.21 (R) MM_KEY_EXCH
5d20h: ISAKMP (0:81): received packet from 172.16.172.21 (R) MM_KEY_EXCH
5d20h: ISAKMP (0:81): processing ID payload. message ID = 0
5d20h: ISAKMP (0:81): processing HASH payload. message ID = 0
5d20h: ISAKMP (0:81): SA has been authenticated with 172.16.172.21
5d20h: ISAKMP (81): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
5d20h: ISAKMP (81): Total payload length: 12
5d20h: ISAKMP (0:81): sending packet to 172.16.172.21 (R) QM_IDLE
5d20h: ISAKMP (0:81): received packet from 172.16.172.21 (R) QM_IDLE
5d20h: ISAKMP (0:81): processing HASH payload. message ID = 241
5d20h: ISAKMP (0:81): processing SA payload. message ID = 241
5d20h: ISAKMP (0:81): Checking IPSec proposal 1
5d20h: ISAKMP: transform 1, ESP_DES
5d20h: ISAKMP:   attributes in transform:
5d20h: ISAKMP:      SA life type in seconds
```

```
5d20h: ISAKMP:      SA life duration (VPI) of  0x0 0x0 0xD 0xAC
5d20h: ISAKMP:      SA life type in kilobytes
5d20h: ISAKMP:      SA life duration (VPI) of  0x0 0x10 0x0 0x0
5d20h: ISAKMP:      encaps is 2
5d20h: ISAKMP:      authenticator is HMAC-MD5
5d20h: ISAKMP (0:81): atts are acceptable.
5d20h: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 172.16.172.39, src= 172.16.172.21,
    dest_proxy= 172.16.172.39/255.255.255.255/47/0 (type=1),
    src_proxy= 172.16.172.21/255.255.255.255/47/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0
5d20h: ISAKMP (0:81): processing NONCE payload. message ID = 241
5d20h: ISAKMP (0:81): processing ID payload. message ID = 241
5d20h: ISAKMP (81): ID_IPV4_ADDR src 172.16.172.21 prot 47 port 0
5d20h: ISAKMP (0:81): processing ID payload. message ID = 241
5d20h: ISAKMP (81): ID_IPV4_ADDR dst 172.16.172.39 prot 47 port 0
5d20h: ISAKMP (0:81): asking for 1 spis from ipsec
5d20h: IPSEC(key_engine): got a queue event...
5d20h: IPSEC(spi_response): getting spi 895566248 for SA
        from 172.16.172.21   to 172.16.172.39   for prot 3
5d20h: ISAKMP: received ke message (2/1)
5d20h: ISAKMP (0:81): sending packet to 172.16.172.21 (R) QM_IDLE
5d20h: ISAKMP (0:81): received packet from 172.16.172.21 (R) QM_IDLE
5d20h: ISAKMP (0:81): Creating IPSec SAs
5d20h:         inbound SA from 172.16.172.21 to 172.16.172.39
        (proxy 172.16.172.21 to 172.16.172.39)
5d20h:         has spi 0x356141A8 and conn_id 362 and flags 0
5d20h:         lifetime of 3500 seconds
5d20h:         lifetime of 1048576 kilobytes
5d20h:         outbound SA from 172.16.172.39   to 172.16.172.21
(proxy 172.16.172.39   to 172.16.172.21  )
5d20h:         has spi 337 and conn_id 363 and flags 0
5d20h:         lifetime of 3500 seconds
5d20h:         lifetime of 1048576 kilobytes
5d20h: ISAKMP (0:81): deleting node 241 error FALSE reason
"quick mode done (await()"
5d20h: IPSEC(key_engine): got a queue event...
5d20h: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.16.172.39, src= 172.16.172.21,
    dest_proxy= 172.16.172.39/0.0.0.0/47/0 (type=1),
    src_proxy= 172.16.172.21/0.0.0.0/47/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3500s and 1048576kb,
    spi= 0x356141A8(895566248), conn_id= 362, keysize= 0, flags= 0x0
5d20h: IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.16.172.39, dest= 172.16.172.21,
    src_proxy= 172.16.172.39/0.0.0.0/47/0 (type=1),
    dest_proxy= 172.16.172.21/0.0.0.0/47/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3500s and 1048576kb,
    spi= 0x151(337), conn_id= 363, keysize= 0, flags= 0x0
5d20h: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.16.172.39, sa_prot= 50,
    sa_spi= 0x356141A8(895566248),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 362
5d20h: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.16.172.21, sa_prot= 50,
    sa_spi= 0x151(337),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 363
5d20h: IPSEC(add_sa): peer asks for new SAs -- expire current in 120 sec.,
  (sa) sa_dest= 172.16.172.21, sa_prot= 50,
    sa_spi= 0x150(336),
```

```
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 361,
  (identity) local= 172.16.172.39, remote= 172.16.172.21,
    local_proxy= 172.16.172.39/255.255.255.255/47/0 (type=1),
    remote_proxy= 172.16.172.21/255.255.255.255/47/0 (type=1)
1720-1#

1720-1#show crypto isakmp sa
dst             src             state          conn-id    slot
172.16.172.39   172.16.172.21   QM_IDLE             81       0

1720-1#show crypto ipsec sa

interface: FastEthernet0
    Crypto map tag: vpn, local addr. 172.16.172.39

   local  ident (addr/mask/prot/port): (172.16.172.39/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (172.16.172.21/255.255.255.255/0/0)
   current_peer: 172.16.172.21
     PERMIT, flags={transport_parent,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 0, #recv errors 0

     local crypto endpt.: 172.16.172.39, remote crypto endpt.: 172.16.172.21
     path mtu 1514, media mtu 1514
     current outbound spi: 0

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:

   local  ident (addr/mask/prot/port): (172.16.172.39/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.172.21/255.255.255.255/47/0)
   current_peer: 172.16.172.21
     PERMIT, flags={origin_is_acl,transport_parent,parent_is_transport,}
    #pkts encaps: 34901, #pkts encrypt: 34901, #pkts digest 34901
    #pkts decaps: 34900, #pkts decrypt: 34900, #pkts verify 34900
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 0, #recv errors 0

     local crypto endpt.: 172.16.172.39, remote crypto endpt.: 172.16.172.21
     path mtu 1500, media mtu 1500
     current outbound spi: 151

     inbound esp sas:
      spi: 0x356141A8(895566248)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Transport, }
        slot: 0, conn id: 362, flow_id: 163, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (1046258/3306)
        IV size: 8 bytes
        replay detection support: Y
```

```
     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x151(337)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Transport, }
        slot: 0, conn id: 363, flow_id: 164, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (1046258/3306)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:



interface: Tunnel0
    Crypto map tag: vpn, local addr. 172.16.172.39

   local  ident (addr/mask/prot/port): (172.16.172.39/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (172.16.172.21/255.255.255.255/0/0)
   current_peer: 172.16.172.21
     PERMIT, flags={transport_parent,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 0, #recv errors 0

     local crypto endpt.: 172.16.172.39, remote crypto endpt.: 172.16.172.21
     path mtu 1514, media mtu 1514
     current outbound spi: 0

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:



   local  ident (addr/mask/prot/port): (172.16.172.39/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.172.21/255.255.255.255/47/0)
   current_peer: 172.16.172.21
     PERMIT, flags={origin_is_acl,transport_parent,parent_is_transport,}
    #pkts encaps: 35657, #pkts encrypt: 35657, #pkts digest 35657
    #pkts decaps: 35656, #pkts decrypt: 35656, #pkts verify 35656
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 0, #recv errors 0

     local crypto endpt.: 172.16.172.39, remote crypto endpt.: 172.16.172.21
     path mtu 1500, media mtu 1500
     current outbound spi: 151
```

```
     inbound esp sas:
      spi: 0x356141A8(895566248)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Transport, }
        slot: 0, conn id: 362, flow_id: 163, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (1046154/3302)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x151(337)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Transport, }
        slot: 0, conn id: 363, flow_id: 164, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (1046154/3302)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:

1720-1#show crypto engine connections active

  ID Interface             IP-Address    State  Algorithm    Encrypt Decrypt
  81 FastEthernet0  172.16.172.39   set  HMAC_MD5+DES_56_CB      0       0
 362 FastEthernet0  172.16.172.39   set  HMAC_MD5+DES_56_CB      0   23194
 363 FastEthernet0  172.16.172.39   set  HMAC_MD5+DES_56_CB  23195       0
```

VPN 5002 Concentrator의 디버깅

VPN Concentrator의 Syslog 출력이 여기에 표시됩니다.

```
VPN5002_8_323E9040: Main# VPN 0:1 opened for 172.16.172.39 from 172.16.172.39.
User assigned IP address 50.1.1.2

VPN5002_8_323E9040: Main#show vpn partner verbose


Port        Partner         Partner  Default  Bindto          Connect
Number      Address         Port     Partner  Address         Time
-------------------------------------------------------------------------
VPN 0:1     172.16.172.39   500      No       172.16.172.21   00:00:13:26
     Auth/Encrypt: MD5e/DES  User Auth: Shared Key
     Access: Static Peer: 172.16.172.39    Local: 172.16.172.21
     Start:14518 seconds Managed:15299 seconds State:imnt_maintenance


IOP slot 1:
No active connections found.


VPN5002_8_323E9040: Main#show vpn statistics verbose

          Current  In       High     Running  Script   Script   Script
          Active   Negot    Water    Total    Starts   OK       Error
          ---------------------------------------------------------------
Users     0        0        0        0        0        0        0
```

```
Partners  1        0        1        81       81       1        158
Total     1        0        1        81       81       1        158

Stats             VPN0:1
Wrapped            79733
Unwrapped          79734
BadEncap               0
BadAuth                0
BadEncrypt             0
rx IP              79749
rx IPX                 0
rx Other               0
tx IP              79761
tx IPX                 0
tx Other               0
IKE rekey              0

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

IOP slot 1:

          Current  In       High     Running  Script   Script   Script
          Active   Negot    Water    Total    Starts   OK       Error
          -----------------------------------------------------------
Users     0        0        0        0        0        0        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
```

터널 모드 구성 오류

GRE over IPSec을 사용할 경우 VPN 5000 Concentrator는 기본적으로 전송 모드를 제안합니다. 터널 모드에 대해 Cisco IOS 라우터가 잘못 구성된 경우 이 오류가 발생합니다.

Cisco IOS 라우터의 디버그 출력이 여기에 표시됩니다.

```
2d21h: ISAKMP (0:23): Checking IPSec proposal 1
2d21h: ISAKMP: transform 1, ESP_DES
2d21h: ISAKMP: attributes in transform:
2d21h: ISAKMP: SA life type in seconds
2d21h: ISAKMP: SA life duration (VPI) of 0x0 0x1 0x51 0x80
2d21h: ISAKMP: SA life type in kilobytes
2d21h: ISAKMP: SA life duration (VPI) of 0x0 0x10 0x0 0x0
```

```
2d21h: ISAKMP: encaps is 2
2d21h: ISAKMP: authenticator is HMAC-MD5
2d21h: IPSEC(validate_proposal): invalid transform proposal flags -- 0x0
```

VPN 5002 Concentrator의 로그에는 이 출력과 비슷한 항목이 표시됩니다.

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

관련 정보

- Cisco VPN 5000 Series Concentrator 판매 중단 발표
- Cisco VPN 5000 Concentrator 지원 페이지
- Cisco VPN 5000 클라이언트 지원 페이지
- IPSec 지원 페이지
- Technical Support - Cisco Systems