IPX 라우팅을 사용하여 GRE 및 IPSec 구성

목차

소개

이 문서에서는 두 라우터 간의 GRE(Generic Routing Encapsulation) 터널을 사용하는 IP 보안(IPSec) 컨피그레이션을 설명합니다. IPSec을 사용하여 GRE 터널을 암호화하여 Novell IPX(Internetwork Packet Exchange), AppleTalk 등과 같이 비 IP 트래픽에 대한 네트워크 레이어 보안을 제공할 수 있습니다. 이 예의 GRE 터널은 비 IP 트래픽을 전송하는 데 전적으로 사용됩니다. 따라서 터널에 구성된 IP 주소가 없습니다. 다음은 몇 가지 컨피그레이션 고려 사항입니다.

- IOS 12.2(13)T 소프트웨어 이상(번호가 높은 T-Train 소프트웨어, 12.3 이상)의 경우, 구성된 IPSec 암호화 맵은 물리적 인터페이스에만 적용되어야 하며 GRE 터널 인터페이스에 더 이상 적용할 필요가 없습니다. 이 릴리스 이전의 소프트웨어 버전에서는 IPSec 암호화 맵을 터널 인터페이스와 물리적 인터페이스 모두에 적용해야 합니다. 12.2.(13)T 소프트웨어 이상을 사용할 때 물리적 및 터널 인터페이스에 암호화 맵이 있어야 합니다. 그러나 Cisco에서는 물리적 인터페이스에만 적용하는 것이 좋습니다.
- 암호화 맵을 적용하기 전에 GRE 터널이 작동하는지 확인합니다.
- 암호화 ACL(Access Control List)에는 허용되는 프로토콜로 GRE가 있어야 합니다. 예를 들어 **access-list 101은 gre *host #.#.#.# host #.#.##*(여기서 첫 번째 호스트 번호는 GRE** 터널의 터널 소스의 IP 주소이고 두 번째 호스트 번호는 터널 대상의 IP 주소입니다.)
- 물리적 인터페이스(또는 루프백 인터페이스) IP 주소를 사용하여 IKE(Internet Key Exchange) 피어를 식별합니다.
- 일부 이전 버전의 Cisco IOS 릴리스에서는 버그로 인해 터널 인터페이스의 빠른 스위칭을 비활성화해야 합니다. 터널 인터페이스에서 빠른 스위칭을 끕니다. 이 문제에 대한 버그 세부 정보는 CSCdm10376에서 볼 수 있습니다(등록된 고객만 해당).

시작하기 전에

사전 요구 사항

이 컨피그레이션을 시도하기 전에 다음 전제 조건을 충족하는지 확인하십시오.

- IPX 구성 및 라우팅 지식
- GRE 터널의 지식 및 구성
- IPSec의 지식 및 구성 작업

사용되는 구성 요소

이 문서의 정보는 아래 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® Software 릴리스 12.2(7)
- Cisco 3600 Series 라우터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 라이브 네트워크에서 작업하는 경우, 사용하기 전에 모든 명령의 잠재적인 영향을 이해해야 합니다.

표기 규칙

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

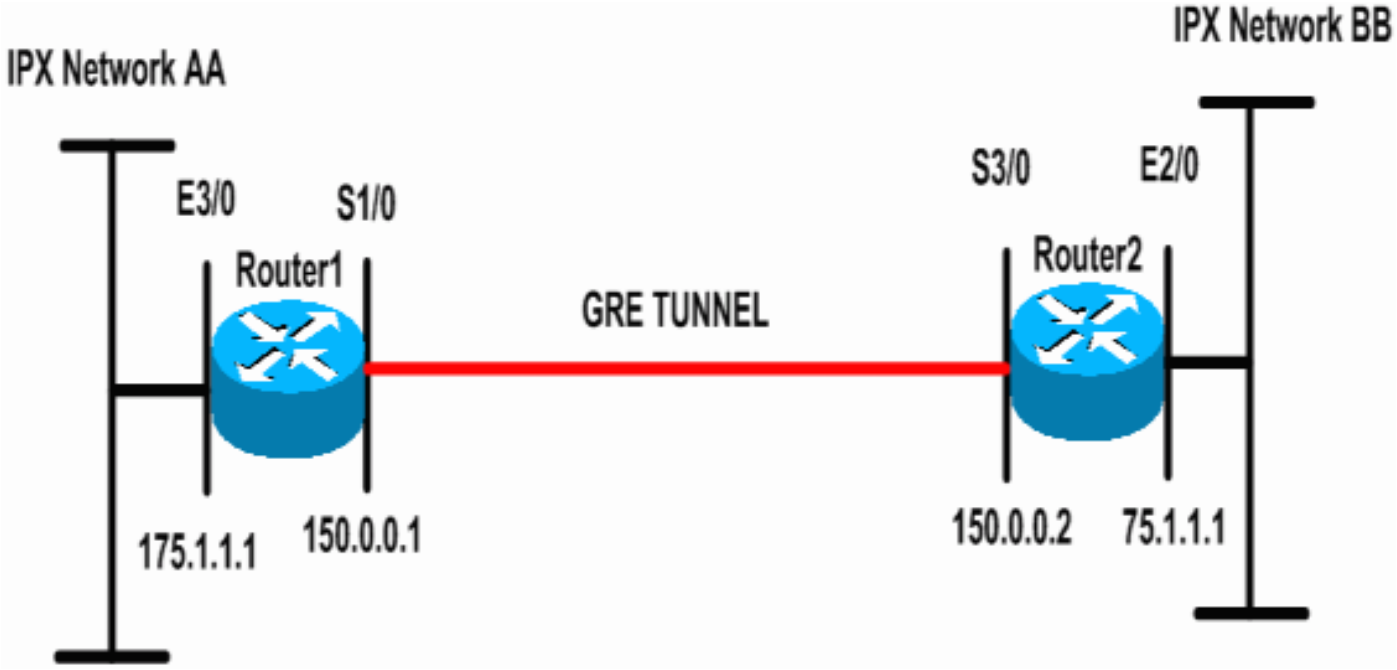
구성

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 아래 다이어그램에 표시된 네트워크 설정을 사용합니다.



구성

이 문서에서는 아래 표시된 구성을 사용합니다.

라우터 1

```
Current configuration: 1300 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router1
!
ip subnet-zero
!
!--- Enables IPX routing. ipx routing 00e0.b064.258e
!
!--- Defines the IKE policy identifying the parameters
for building IKE SAs.
crypto isakmp policy 10
 authentication pre-share
 group 2
 lifetime 3600
!--- Defines the pre-shared key for the remote peer.
crypto isakmp key cisco address 200.1.1.1
!
!--- Defines the transform set to be used for IPSec SAs.
crypto ipsec transform-set tunnelset esp-des esp-md5-
hmac
!
!--- Configures the router to use the address of
Loopback0 interface !--- for IKE and IPSec traffic.
crypto map toBB local-address Loopback0
!--- Defines a crypto map to be used for establishing
IPSec SAs.
crypto map toBB 10 ipsec-isakmp
 set peer 200.1.1.1
```

```
 set transform-set tunnelset
 match address 101
!
interface Loopback0
 ip address 100.1.1.1 255.255.255.0
!
!--- Configures a GRE tunnel for transporting IPX
traffic. interface Tunnel0
 no ip address

ipx network CC
 tunnel source Serial1/0
 tunnel destination 150.0.0.2

!
interface Serial1/0
 ip address 150.0.0.1 255.255.255.0
!--- Applies the crypto map to the physical interface
used !--- for carrying GRE tunnel traffic. crypto map
toBB
!
interface Ethernet3/0
 ip address 175.1.1.1 255.255.255.0
ipx network AA
!--- Output suppressed. ip classless ip route 0.0.0.0
0.0.0.0 150.0.0.2 no ip http server ! !--- Configures
GRE tunnel traffic to be encrypted using IPSec. access-
list 101 permit gre host 150.0.0.1 host 150.0.0.2
!
line con 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

라우터 2

```
Current configuration:1525 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router2
!
ip subnet-zero
!
!--- Enables IPX routing. ipx routing 0010.7b37.c8ae
!
!--- Defines the IKE policy identifying the parameters
for building IKE SAs.
crypto isakmp policy 10
 authentication pre-share
 group 2
 lifetime 3600
!--- Defines the pre-shared key for the remote peer.
crypto isakmp key cisco address 100.1.1.1
!
!--- Defines the transform set to be used for IPSec SAs.
```

```
crypto ipsec transform-set tunnelset esp-des esp-md5-
hmac
!
!--- Configures the router to use the address of
Loopback0 interface !--- for IKE and IPSec traffic.
crypto map toAA local-address Loopback0
!--- Defines a crypto map to be used for establishing
IPSec SAs.
crypto map toAA 10 ipsec-isakmp
 set peer 100.1.1.1
 set transform-set tunnelset
 match address 101
!
interface Loopback0
 ip address 200.1.1.1 255.255.255.0
!
!--- Configures a GRE tunnel for transporting IPX
traffic interface Tunnel0
 no ip address

 ipx network CC
 tunnel source Serial3/0
 tunnel destination 150.0.0.1
!
interface Ethernet2/0
 ip address 75.1.1.1 255.255.255.0
 ipx network BB
!
interface Serial3/0
 ip address 150.0.0.2 255.255.255.0
 clockrate 9600
!--- Applies the crypto map to the physical interface
used !--- for carrying GRE tunnel traffic. crypto map
toAA
!
!--- Output suppressed. ip classless ip route 0.0.0.0
0.0.0.0 150.0.0.1 no ip http server ! !--- Configures
GRE tunnel traffic to be encrypted using IPSec. access-
list 101 permit gre host 150.0.0.2 host 150.0.0.1
!
line con 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

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.**

- **show ipx interface** - 디바이스에 구성된 IPX 인터페이스의 상태 및 매개 변수(예: IPX 네트워크 및 노드 주소)를 표시합니다.
- **show ipx route** - IPX 라우팅 테이블의 내용을 표시합니다.
- **show crypto isakmp sa** - 라우터의 IKE SA를 표시하여 1단계 보안 연결을 표시합니다. IKE

SA를 작동 및 작동으로 간주하려면 표시되는 상태가 QM_IDLE이어야 합니다.

- **show crypto ipsec sa** - 라우터의 활성 IPSec SA의 자세한 목록을 표시하여 2단계 보안 연결을 표시합니다.
- **show crypto map**—암호화 액세스 목록, 변형 집합, 피어 등의 세부사항과 함께 라우터에 구성된 암호화 맵을 표시합니다.
- **show crypto engine connections active** - 연결된 인터페이스, 변환 및 카운터와 함께 활성 SA 목록을 표시합니다.

샘플 출력 표시

이 섹션에서는 Router2로 향하는 Router1에서 IPX **ping** 명령을 실행할 때 디바이스 Router1에서 **show** 명령 출력을 캡처합니다. Router2의 출력은 유사합니다. 출력의 주요 매개변수는 **굵게** 표시됩니다. 명령 출력에 대한 자세한 내용은 IP 보안 문제 해결 - 디버그 명령 이해 및 사용 문서를 참조하십시오.

```
Router1#show ipx interface ethernet 3/0
Ethernet3/0 is up, line protocol is up
  IPX address is AA.00b0.64cb.eab1, NOVELL-ETHER [up]
  Delay of this IPX network, in ticks is 1 throughput 0 link delay 0
  IPXWAN processing not enabled on this interface.
!--- Output suppressed. Router2#show ipx interface ethernet 2/0
Ethernet2/0 is up, line protocol is up
  IPX address is BB.0002.16ae.c161, NOVELL-ETHER [up]
  Delay of this IPX network, in ticks is 1 throughput 0 link delay 0
  IPXWAN processing not enabled on this interface.
!--- Output suppressed. Router1#show ipx route
Codes: C - Connected primary network,    c - Connected secondary network
       S - Static, F - Floating static, L - Local (internal), W - IPXWAN
       R - RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate
       s - seconds, u - uses, U - Per-user static/Unknown, H - Hold-down

3 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.

No default route known.

C         AA (NOVELL-ETHER),  Et3/0
C         CC (TUNNEL),        Tu0
R         BB [151/01] via       CC.0010.7b37.c8ae,   56s, Tu0

Router2#show ipx route
Codes: C - Connected primary network,    c - Connected secondary network
       S - Static, F - Floating static, L - Local (internal), W - IPXWAN
       R - RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate
       s - seconds, u - uses, U - Per-user static/Unknown, H - Hold-down

3 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.

No default route known.

C         BB (NOVELL-ETHER),  Et2/0
C         CC (TUNNEL),        Tu0
R         AA [151/01] via       CC.00e0.b064.258e,    8s, Tu0

Router1#ping ipx BB.0010.7b37.c8ae

Type escape sequence to abort.
Sending 5, 100-byte IPX Novell Echoes to BB.0002.16ae.c161, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/53/56 ms

Router2#ping ipx  AA.00b0.64cb.eab1

Type escape sequence to abort.
Sending 5, 100-byte IPX Novell Echoes to AA.00b0.64cb.eab1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/53/56 ms


Router1#show crypto isakmp sa
dst             src             state          conn-id    slot
200.1.1.1       100.1.1.1       QM_IDLE               5       0


Router1#show crypto ipsec sa detail

interface: Serial1/0
    Crypto map tag: toBB, local addr. 100.1.1.1

   local  ident (addr/mask/prot/port): (150.0.0.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (150.0.0.2/255.255.255.255/47/0)
   current_peer: 200.1.1.1
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 343, #pkts encrypt: 343, #pkts digest 343
    #pkts decaps: 343, #pkts decrypt: 343, #pkts verify 343
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #pkts no sa (send) 1, #pkts invalid sa (rcv) 0
    #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
    #pkts invalid prot (recv) 0, #pkts verify failed: 0
    #pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
    #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
    ##pkts replay failed (rcv): 0
    #pkts internal err (send): 0, #pkts internal err (recv) 0

     local crypto endpt.: 100.1.1.1, remote crypto endpt.: 200.1.1.1
     path mtu 1500, ip mtu 1500, ip mtu interface Serial1/0
     current outbound spi: CB6F6DA6

     inbound esp sas:
      spi: 0xFD6F387(265745287)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2010, flow_id: 11, crypto map: toBB
        sa timing: remaining key lifetime (k/sec): (4607994/1892)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xCB6F6DA6(3413077414)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2011, flow_id: 12, crypto map: toBB
        sa timing: remaining key lifetime (k/sec): (4607994/1892)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:
```

```
     outbound pcp sas:


Router1#show crypto map
Crypto Map: "toBB" idb: Loopback0 local address: 100.1.1.1

Crypto Map "toBB" 10 ipsec-isakmp
        Peer = 200.1.1.1
        Extended IP access list 101
            access-list 101 permit gre host 150.0.0.1 host 150.0.0.2
        Current peer: 200.1.1.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={ tunnelset, }
        Interfaces using crypto map toBB:
                Serial1/0


Router1#show crypto engine connections active

  ID Interface            IP-Address      State  Algorithm           Encrypt  Decrypt
   5 <none>               <none>          set    HMAC_SHA+DES_56_CB        0        0
2010 Serial1/0            150.0.0.1       set    HMAC_MD5+DES_56_CB        0       40
2011 Serial1/0            150.0.0.1       set    HMAC_MD5+DES_56_CB       45        0
```

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.

- debug crypto engine - 암호화 및 암호 해독 프로세스를 수행하는 암호화 엔진에 대한 정보를 표시합니다.
- debug crypto ipsec - 2단계의 IPSec 협상을 확인합니다.
- debug crypto isakmp - 1단계의 IKE 협상을 확인합니다.

디버그 출력 샘플

이 섹션에서는 IPSec으로 구성된 라우터의 디버그 명령 출력을 캡처합니다. IPX **ping** 명령은 router2로 향하는 router1에서 실행됩니다.

- 라우터 1
- 라우터 2

라우터 1

```
Router1#show debug
Cryptographic Subsystem:
```

```
  Crypto ISAKMP debugging is on
  Crypto Engine debugging is on
  Crypto IPSEC debugging is on
Router1#
!--- GRE traffic matching crypto ACL triggers IPSec processing *Mar  2 00:41:17.593:
IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 100.1.1.1, remote= 200.1.1.1,
    local_proxy= 150.0.0.1/255.255.255.255/47/0 (type=1),
    remote_proxy= 150.0.0.2/255.255.255.255/47/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x9AAD0079(2595029113), conn_id= 0, keysize= 0, flags= 0x400C
*Mar  2 00:41:17.597: ISAKMP: received ke message (1/1)
!--- IKE uses UDP port 500, begins main mode exchange. *Mar  2 00:41:17.597: ISAKMP: local port
500, remote port 500
*Mar  2 00:41:17.597: ISAKMP (0:1): beginning Main Mode exchange
*Mar  2 00:41:17.597: ISAKMP (0:1): sending packet to 200.1.1.1 (I) MM_NO_STATE
*Mar  2 00:41:17.773: ISAKMP (0:1): received packet from 200.1.1.1 (I) MM_NO_STATE
*Mar  2 00:41:17.773: ISAKMP (0:1): processing SA payload. message ID = 0
*Mar  2 00:41:17.773: ISAKMP (0:1): found peer pre-shared key matching 200.1.1.1
*Mar  2 00:41:17.773: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 10 policy
!--- IKE SAs are negotiated. *Mar  2 00:41:17.773: ISAKMP:      encryption DES-CBC
*Mar  2 00:41:17.773: ISAKMP:      hash SHA
*Mar  2 00:41:17.773: ISAKMP:      default group 2
*Mar  2 00:41:17.773: ISAKMP:      auth pre-share
*Mar  2 00:41:17.773: ISAKMP:      life type in seconds
*Mar  2 00:41:17.773: ISAKMP:      life duration (basic) of 3600
*Mar  2 00:41:17.773: ISAKMP (0:1): atts are acceptable. Next payload is 0
*Mar  2 00:41:17.773: CryptoEngine0: generate alg parameter
*Mar  2 00:41:17.905: CRYPTO_ENGINE: Dh phase 1 status: 0
*Mar  2 00:41:17.905: CRYPTO_ENGINE: Dh phase 1 status: 0
*Mar  2 00:41:17.905: ISAKMP (0:1): SA is doing pre-shared key authentication using id type
ID_IPV4_
ADDR
*Mar  2 00:41:17.905: ISAKMP (0:1): sending packet to 200.1.1.1 (I) MM_SA_SETUP
*Mar  2 00:41:18.149: ISAKMP (0:1): received packet from 200.1.1.1 (I) MM_SA_SETUP
*Mar  2 00:41:18.153: ISAKMP (0:1): processing KE payload. message ID = 0
*Mar  2 00:41:18.153: CryptoEngine0: generate alg parameter
*Mar  2 00:41:18.317: ISAKMP (0:1): processing NONCE payload. message ID = 0
*Mar  2 00:41:18.317: ISAKMP (0:1): found peer pre-shared key matching 200.1.1.1
*Mar  2 00:41:18.317: CryptoEngine0: create ISAKMP SKEYID for conn id 1
*Mar  2 00:41:18.321: ISAKMP (0:1): SKEYID state generated
*Mar  2 00:41:18.321: ISAKMP (0:1): processing vendor id payload
*Mar  2 00:41:18.321: ISAKMP (0:1): speaking to another IOS box!
*Mar  2 00:41:18.321: ISAKMP (1): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
*Mar  2 00:41:18.321: ISAKMP (1): Total payload length: 12
*Mar  2 00:41:18.321: CryptoEngine0: generate hmac context for conn id 1
*Mar  2 00:41:18.321: ISAKMP (0:1): sending packet to 200.1.1.1 (I) MM_KEY_EXCH
*Mar  2 00:41:18.361: ISAKMP (0:1): received packet from 200.1.1.1 (I) MM_KEY_EXCH
*Mar  2 00:41:18.361: ISAKMP (0:1): processing ID payload. message ID = 0
*Mar  2 00:41:18.361: ISAKMP (0:1): processing HASH payload. message ID = 0
*Mar  2 00:41:18.361: CryptoEngine0: generate hmac context for conn id 1
!--- Peer is authenticated. *Mar  2 00:41:18.361: ISAKMP (0:1): SA has been authenticated with
200.1.1.1
!--- Begins quick mode exchange. *Mar  2 00:41:18.361: ISAKMP (0:1): beginning Quick Mode
exchange, M-ID of -2078851837
*Mar  2 00:41:18.365: CryptoEngine0: generate hmac context for conn id 1
*Mar  2 00:41:18.365: ISAKMP (0:1): sending packet to 200.1.1.1 (I) QM_IDLE
*Mar  2 00:41:18.365: CryptoEngine0: clear dh number for conn id 1
```

```
*Mar  2 00:41:18.681: ISAKMP (0:1): received packet from 200.1.1.1 (I) QM_IDLE
*Mar  2 00:41:18.681: CryptoEngine0: generate hmac context for conn id 1
*Mar  2 00:41:18.685: ISAKMP (0:1): processing HASH payload. message ID = -2078851837
*Mar  2 00:41:18.685: ISAKMP (0:1): processing SA payload. message ID = -2078851837
!--- Negotiates IPSec SA. *Mar  2 00:41:18.685: ISAKMP (0:1): Checking IPSec proposal 1
*Mar  2 00:41:18.685: ISAKMP: transform 1, ESP_DES
*Mar  2 00:41:18.685: ISAKMP:   attributes in transform:
*Mar  2 00:41:18.685: ISAKMP:      encaps is 1
*Mar  2 00:41:18.685: ISAKMP:      SA life type in seconds
*Mar  2 00:41:18.685: ISAKMP:      SA life duration (basic) of 3600
*Mar  2 00:41:18.685: ISAKMP:      SA life type in kilobytes
*Mar  2 00:41:18.685: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
*Mar  2 00:41:18.685: ISAKMP:      authenticator is HMAC-MD5
*Mar  2 00:41:18.685: validate proposal 0
*Mar  2 00:41:18.685: ISAKMP (0:1): atts are acceptable.
*Mar  2 00:41:18.685: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 100.1.1.1, remote= 200.1.1.1,
    local_proxy= 150.0.0.1/255.255.255.255/47/0 (type=1),
    remote_proxy= 150.0.0.2/255.255.255.255/47/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar  2 00:41:18.689: validate proposal request 0
*Mar  2 00:41:18.689: ISAKMP (0:1): processing NONCE payload. message ID = -2078851837
*Mar  2 00:41:18.689: ISAKMP (0:1): processing ID payload. message ID = -2078851837
*Mar  2 00:41:18.689: ISAKMP (0:1): processing ID payload. message ID = -2078851837
*Mar  2 00:41:18.689: CryptoEngine0: generate hmac context for conn id 1
*Mar  2 00:41:18.689: ipsec allocate flow 0
*Mar  2 00:41:18.689: ipsec allocate flow 0
!--- IPSec SAs are generated for inbound and outbound traffic. *Mar  2 00:41:18.693: ISAKMP
(0:1): Creating IPSec SAs
*Mar  2 00:41:18.693:         inbound SA from 200.1.1.1 to 100.1.1.1
        (proxy 150.0.0.2 to 150.0.0.1)
*Mar  2 00:41:18.693:         has spi 0x9AAD0079 and conn_id 2000 and flags 4
*Mar  2 00:41:18.693:         lifetime of 3600 seconds
*Mar  2 00:41:18.693:         lifetime of 4608000 kilobytes
*Mar  2 00:41:18.693:         outbound SA from 100.1.1.1       to 200.1.1.1       (proxy
150.0.0.1
     to 150.0.0.2      )
*Mar  2 00:41:18.693:         has spi -1609905338 and conn_id 2001 and flags C
*Mar  2 00:41:18.693:         lifetime of 3600 seconds
*Mar  2 00:41:18.693:         lifetime of 4608000 kilobytes
*Mar  2 00:41:18.697: ISAKMP (0:1): sending packet to 200.1.1.1 (I) QM_IDLE
*Mar  2 00:41:18.697: ISAKMP (0:1): deleting node -2078851837 error FALSE reason ""
*Mar  2 00:41:18.697: IPSEC(key_engine): got a queue event...
*Mar  2 00:41:18.697: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 100.1.1.1, remote= 200.1.1.1,
    local_proxy= 150.0.0.1/0.0.0.0/47/0 (type=1),
    remote_proxy= 150.0.0.2/0.0.0.0/47/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x9AAD0079(2595029113), conn_id= 2000, keysize= 0, flags= 0x4
*Mar  2 00:41:18.697: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 100.1.1.1, remote= 200.1.1.1,
    local_proxy= 150.0.0.1/0.0.0.0/47/0 (type=1),
    remote_proxy= 150.0.0.2/0.0.0.0/47/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xA00ACB46(2685061958), conn_id= 2001, keysize= 0, flags= 0xC
*Mar  2 00:41:18.697: IPSEC(create_sa): sa created,
  (sa) sa_dest= 100.1.1.1, sa_prot= 50,
    sa_spi= 0x9AAD0079(2595029113),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2000
*Mar  2 00:41:18.701: IPSEC(create_sa): sa created,
```

```
  (sa) sa_dest= 200.1.1.1, sa_prot= 50,
    sa_spi= 0xA00ACB46(2685061958),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2001

Router1#
```

라우터 2

```
Router2#show debug

Cryptographic Subsystem:
  Crypto ISAKMP debugging is on
  Crypto Engine debugging is on
  Crypto IPSEC debugging is on
Router2#
!--- IKE processing begins here. *Mar  2 00:30:26.093: ISAKMP (0:0): received packet from
100.1.1.1 (N) NEW SA
*Mar  2 00:30:26.093: ISAKMP: local port 500, remote port 500
*Mar  2 00:30:26.093: ISAKMP (0:1): processing SA payload. message ID = 0
*Mar  2 00:30:26.093: ISAKMP (0:1): found peer pre-shared key matching 100.1.1.1
!--- IKE SAs are negotiated. *Mar  2 00:30:26.093: ISAKMP (0:1): Checking ISAKMP transform 1
against priority 10 policy
*Mar  2 00:30:26.093: ISAKMP:      encryption DES-CBC
*Mar  2 00:30:26.093: ISAKMP:      hash SHA
*Mar  2 00:30:26.093: ISAKMP:      default group 2
*Mar  2 00:30:26.093: ISAKMP:      auth pre-share
*Mar  2 00:30:26.093: ISAKMP:      life type in seconds
*Mar  2 00:30:26.093: ISAKMP:      life duration (basic) of 3600
*Mar  2 00:30:26.093: ISAKMP (0:1): atts are acceptable. Next payload is 0
*Mar  2 00:30:26.097: CryptoEngine0: generate alg parameter
*Mar  2 00:30:26.229: CRYPTO_ENGINE: Dh phase 1 status: 0
*Mar  2 00:30:26.229: CRYPTO_ENGINE: Dh phase 1 status: 0
*Mar  2 00:30:26.229: ISAKMP (0:1): SA is doing pre-shared key authentication using id type
ID_IPV4_
ADDR
*Mar  2 00:30:26.229: ISAKMP (0:1): sending packet to 100.1.1.1 (R) MM_SA_SETUP
*Mar  2 00:30:26.417: ISAKMP (0:1): received packet from 100.1.1.1 (R) MM_SA_SETUP
*Mar  2 00:30:26.417: ISAKMP (0:1): processing KE payload. message ID = 0
*Mar  2 00:30:26.417: CryptoEngine0: generate alg parameter
*Mar  2 00:30:26.589: ISAKMP (0:1): processing NONCE payload. message ID = 0
*Mar  2 00:30:26.589: ISAKMP (0:1): found peer pre-shared key matching 100.1.1.1
*Mar  2 00:30:26.593: CryptoEngine0: create ISAKMP SKEYID for conn id 1
*Mar  2 00:30:26.593: ISAKMP (0:1):
SKEYID state generated
*Mar  2 00:30:26.593: ISAKMP (0:1): processing vendor id payload
*Mar  2 00:30:26.593: ISAKMP (0:1): speaking to another IOS box!
*Mar  2 00:30:26.593: ISAKMP (0:1): sending packet to 100.1.1.1 (R) MM_KEY_EXCH
*Mar  2 00:30:26.813: ISAKMP (0:1): received packet from 100.1.1.1 (R) MM_KEY_EXCH
*Mar  2 00:30:26.817: ISAKMP (0:1): processing ID payload. message ID = 0
*Mar  2 00:30:26.817: ISAKMP (0:1): processing HASH payload. message ID = 0
*Mar  2 00:30:26.817: CryptoEngine0: generate hmac context for conn id 1
!--- Peer is authenticated. *Mar  2 00:30:26.817: ISAKMP (0:1): SA has been authenticated with
100.1.1.1
*Mar  2 00:30:26.817: ISAKMP (1): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
*Mar  2 00:30:26.817: ISAKMP (1): Total payload length: 12
*Mar  2 00:30:26.817: CryptoEngine0: generate hmac context for conn id 1
```

```
*Mar  2 00:30:26.817: CryptoEngine0: clear dh number for conn id 1
*Mar  2 00:30:26.821: ISAKMP (0:1): sending packet to 100.1.1.1 (R) QM_IDLE
*Mar  2 00:30:26.869: ISAKMP (0:1): received packet from 100.1.1.1 (R) QM_IDLE
*Mar  2 00:30:26.869: CryptoEngine0: generate hmac context for conn id 1
*Mar  2 00:30:26.869: ISAKMP (0:1): processing HASH payload. message ID = -2078851837
*Mar  2 00:30:26.873: ISAKMP (0:1): processing SA payload. message ID = -2078851837
!--- IPSec SAs are negotiated. *Mar  2 00:30:26.873: ISAKMP (0:1): Checking IPSec proposal 1
*Mar  2 00:30:26.873: ISAKMP: transform 1, ESP_DES
*Mar  2 00:30:26.873: ISAKMP:   attributes in transform:
*Mar  2 00:30:26.873: ISAKMP:      encaps is 1
*Mar  2 00:30:26.873: ISAKMP:      SA life type in seconds
*Mar  2 00:30:26.873: ISAKMP:      SA life duration (basic) of 3600
*Mar  2 00:30:26.873: ISAKMP:      SA life type in kilobytes
*Mar  2 00:30:26.873: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
*Mar  2 00:30:26.873: ISAKMP:      authenticator is HMAC-MD5
*Mar  2 00:30:26.873: validate proposal 0
*Mar  2 00:30:26.873: ISAKMP (0:1): atts are acceptable.
*Mar  2 00:30:26.873: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 200.1.1.1, remote= 100.1.1.1,
    local_proxy= 150.0.0.2/255.255.255.255/47/0 (type=1),
    remote_proxy= 150.0.0.1/255.255.255.255/47/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar  2 00:30:26.873: validate proposal request 0
*Mar  2 00:30:26.877: ISAKMP (0:1): processing NONCE payload. message ID = -2078851837
*Mar  2 00:30:26.877: ISAKMP (0:1): processing ID payload. message ID = -2078851837
*Mar  2 00:30:26.877: ISAKMP (0:1): processing ID payload. message ID = -2078851837
*Mar  2 00:30:26.877: ISAKMP (0:1): asking for 1 spis from ipsec
*Mar  2 00:30:26.877: IPSEC(key_engine): got a queue event...
*Mar  2 00:30:26.877: IPSEC(spi_response): getting spi 2685061958 for SA
        from 200.1.1.1       to 100.1.1.1       for prot 3
*Mar  2 00:30:26.877: ISAKMP: received ke message (2/1)
*Mar  2 00:30:27.129: CryptoEngine0: generate hmac context for conn id 1
*Mar  2 00:30:27.129: ISAKMP (0:1): sending packet to 100.1.1.1 (R) QM_IDLE
*Mar  2 00:30:27.185: ISAKMP (0:1): received packet from 100.1.1.1 (R) QM_IDLE
*Mar  2 00:30:27.189: CryptoEngine0: generate hmac context for conn id 1
*Mar  2 00:30:27.189: ipsec allocate flow 0
*Mar  2 00:30:27.189: ipsec allocate flow 0
!--- IPSec SAs are generated for inbound and outbound traffic. *Mar  2 00:30:27.193: ISAKMP
(0:1): Creating IPSec SAs
*Mar  2 00:30:27.193:         inbound SA from 100.1.1.1 to 200.1.1.1
        (proxy 150.0.0.1 to 150.0.0.2)
*Mar  2 00:30:27.193:         has spi 0xA00ACB46 and conn_id 2000 and flags 4
*Mar  2 00:30:27.193:         lifetime of 3600 seconds
*Mar  2 00:30:27.193:         lifetime of 4608000 kilobytes
*Mar  2 00:30:27.193:         outbound SA from 200.1.1.1       to 100.1.1.1       (proxy
150.0.0.2
     to 150.0.0.1      )
*Mar  2 00:30:27.193:         has spi -1699938183 and conn_id 2001 and flags C
*Mar  2 00:30:27.193:         lifetime of 3600 seconds
*Mar  2 00:30:27.193:         lifetime of 4608000 kilobytes
*Mar  2 00:30:27.193: ISAKMP (0:1): deleting node -2078851837 error FALSE reason "quick mode
done (a
wait()"
*Mar  2 00:30:27.193: IPSEC(key_engine): got a queue event...
*Mar  2 00:30:27.193: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 200.1.1.1, remote= 100.1.1.1,
    local_proxy= 150.0.0.2/0.0.0.0/47/0 (type=1),
    remote_proxy= 150.0.0.1/0.0.0.0/47/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xA00ACB46(2685061958), conn_id= 2000, keysize= 0, flags= 0x4
*Mar  2 00:30:27.197: IPSEC(initialize_sas): ,
```

```
  (key eng. msg.) OUTBOUND local= 200.1.1.1, remote= 100.1.1.1,
    local_proxy= 150.0.0.2/0.0.0.0/47/0 (type=1),
    remote_proxy= 150.0.0.1/0.0.0.0/47/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x9AAD0079(2595029113), conn_id= 2001, keysize= 0, flags= 0xC
*Mar  2 00:30:27.197: IPSEC(create_sa): sa created,
  (sa) sa_dest= 200.1.1.1, sa_prot= 50,
    sa_spi= 0xA00ACB46(2685061958),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2000
*Mar  2 00:30:27.197: IPSEC(create_sa): sa created,
  (sa) sa_dest= 100.1.1.1, sa_prot= 50,
    sa_spi= 0x9AAD0079(2595029113),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2001

Router2#
```

관련 정보

- GRE 기술 지원 페이지
- IP 보안(IPSec) 기술 지원 페이지
- Technical Support - Cisco Systems