配置 GRE 与 IPSec，以实现 IPX 路由

目录

简介

本文档介绍了在两个路由器之间使用通用路由封装 (GRE) 隧道的 IP 安全 (IPSec) 配置。IPSec可以用于加密GRE隧道，为非IP数据流（例如Novell互联网络信息包交换(IPX)、AppleTalk等等）提供网络层安全。此示例中的 GRE 隧道仅用于传输非 IP 流量。因此，隧道并没有配置任何 IP 地址。以下是一些配置注意事项：

- 使用IOS 12.2(13)T软件和更新版本(更高编号的T系列软件、12.3版本和更新版本)，所配置的IPSec加密映射只需适用于物理接口，不再要求适用于GRE隧道接口。在此版本之前的软件版本中，IPSec 加密映射需同时应用于隧道接口和物理接口。在使用12.2.(13)T 软件时物理接口和隧道接口发生加密映射，稍后它将开始工作。但是，Cisco 强烈建议您仅在物理接口上应用它。
- 在应用加密映射之前，请确保 GRE 隧道可以正常工作。
- 加密访问控制列表 (ACL) 应将 GRE 纳为允许的协议。例如，**access-list 101 permit gre*host #.#.#.# host #.#.#.#***（其中，第一个主机号码是 GRE 隧道的隧道源的 IP 地址，第二个主机号码是隧道目标的 IP 地址）。
- 使用物理接口（或环回接口）IP 地址识别 Internet Key Exchange (IKE) 对等体。
- 由于 bug，在 Cisco IOS 版本的某些早期版本中，必须禁用隧道接口的快速交换，才能使其正常工作。关闭隧道接口的的快速交换。有关此问题的 bug 详情，请参阅 CSCdm10376（仅限注册用户）。

开始使用前

先决条件

尝试此配置之前，请确保满足下列前提条件：

- IPX 配置和路由的相关知识
- GRE 隧道的相关知识和配置
- IPSec 的工作知识和配置

使用的组件

本文档中的信息基于以下软件和硬件版本。

- Cisco IOS® 软件版本 12.2(7)
- 思科 3600 系列路由器

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

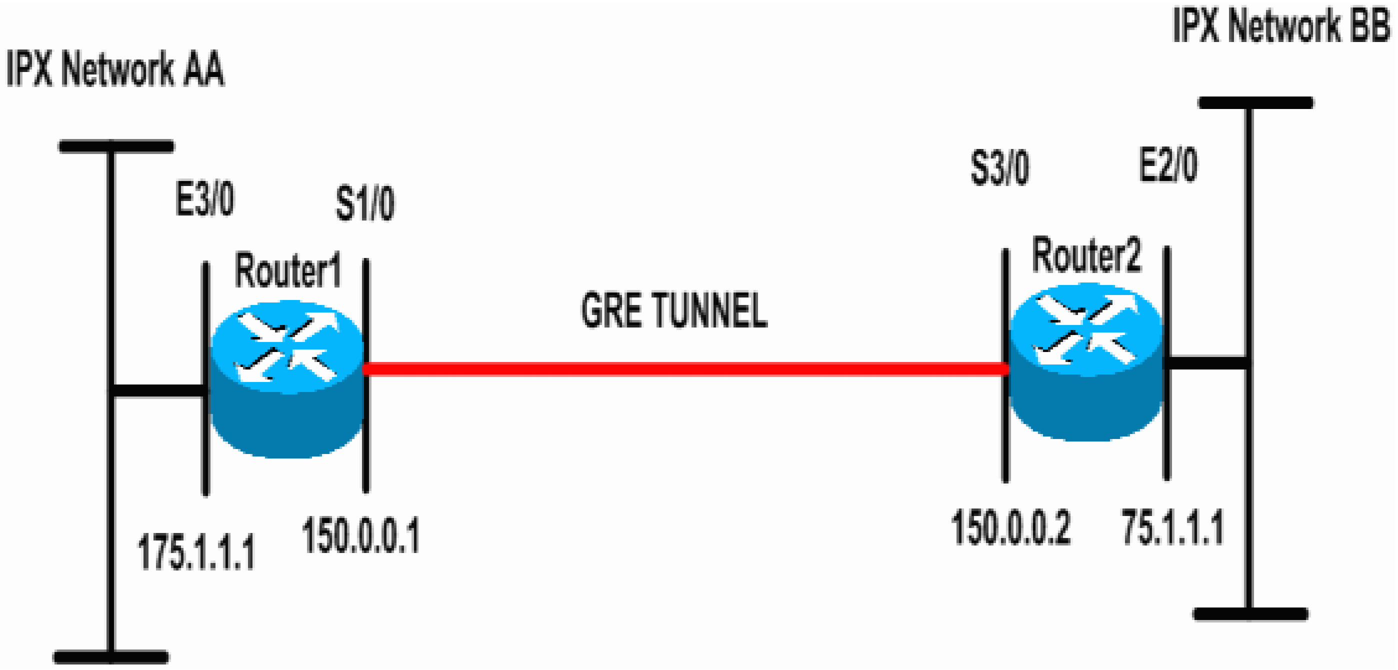
配置

本部分提供有关如何配置本文档所述功能的信息。

注：要查找有关本文档中使用的命令的其他信息，请使用命令查找工具(仅注册客户)。

网络图

本文档使用下图所示的网络设置。



配置

本文档使用如下所示的配置。

路由器 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
```

路由器 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
```

验证

本部分所提供的信息可用于确认您的配置是否正常工作。

命令输出解释程序工具（仅限注册用户）支持某些 **show 命令，使用此工具可以查看对 show 命令输出的分析。**

- **show ipx interface** — 显示设备上配置的 IPX 接口的状态和参数，如 IPX 网络和节点地址。
- **show ipx route** — 显示 IPX 路由表的内容。
- **show crypto isakmp sa** — 通过显示路由器的 IKE SA 显示第 1 阶段的安全关联。显示的状态应为 QM_IDLE，IKE SA 才会被视为打开且能够正常运行。
- **show crypto ipsec sa** — 通过显示路由器的活动 IPSec SA 的详细列表，显示第 2 阶段的安全关联。
- **show crypto map** — 显示路由器上配置的加密映射，及其详情（如加密访问列表、转换集和对等体等）。
- **show crypto engine connections active** — 显示活动 SA 的列表，以及与这些 SA 关联的接口、转换和计数器。

show 输出示例

当在发往Router2的Router1上执行IPX **ping**命令时，本部分捕获设备Router1上的**show**命令输出。Router2的输出类似。输出中的关键参数以**粗体**显示。有关命令输出的解释，请参阅 IP 安全故障排除 — 了解和使用 debug 命令文档。

```
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
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

注意：在发出debug**命**令之前，请参阅有关Debug命令的重要信息。

- debug crypto engine — 显示有关执行加密或解密过程的加密引擎的信息。
- debug crypto ipsec — 查看第 2 阶段的 IPSec 协商。
- debug crypto isakmp — 查看第 1 阶段的 IKE 协商。

调试输出示例

本部分捕获了配置 IPSec 的路由器上的 debug 命令输出。在 Router1 上对 Router2 执行 IPX **ping 命令**。

- 路由器1
- 路由器2

路由器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#
```

路由器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#
```

相关信息

- GRE 技术支持页
- IP 安全 (IPSec) 技术支持页
- 技术支持 - Cisco Systems