Configurazione di GRE e IPSec con routing IPX

Sommario

Introduzione

In questo documento viene illustrata una configurazione IP Security (IPSec) con l'uso di un tunnel GRE (Generic Routing Encapsulation) tra due router. IPSec può essere utilizzato per crittografare i tunnel GRE e fornire la sicurezza a livello di rete per il traffico non IP, ad esempio Novell Internetwork Packet Exchange (IPX), AppleTalk e così via. Nell'esempio, il tunnel GRE è usato esclusivamente per trasportare il traffico non IP. Pertanto, per il tunnel non è configurato alcun indirizzo IP. Ecco alcune considerazioni sulla configurazione:

- Con il software IOS versione 12.2(13)T e successive (software T-train con numero superiore, versione 12.3 e successive), la mappa crittografica IPSec configurata deve essere applicata solo all'interfaccia fisica e non è più necessario applicarla all'interfaccia del tunnel GRE. Nelle versioni software precedenti a questa versione, le mappe crittografiche IPSec devono essere applicate sia all'interfaccia del tunnel sia all'interfaccia fisica. disporre della mappa crittografica sull'interfaccia fisica e di tunnel quando si usa il software 12.2.2(13)T e versioni successive dovrebbe ancora funzionare; tuttavia, Cisco consiglia di applicarlo solo all'interfaccia fisica.
- Verificare che il tunnel GRE funzioni prima di applicare le mappe crittografiche.
- L'elenco di controllo di accesso (ACL) crittografico deve avere GRE come protocollo consentito. Ad esempio, **access-list 101 consente all'*host* gre *#.#.#.# host #.#.#.#*** (dove il primo numero host è l'indirizzo IP dell'origine del tunnel GRE e il secondo numero host è l'indirizzo IP della destinazione del tunnel).
- Utilizzare gli indirizzi IP dell'interfaccia fisica (o dell'interfaccia di loopback) per identificare i peer IKE (Internet Key Exchange).
- In alcune versioni precedenti di Cisco IOS, per funzionare, l'opzione di commutazione veloce

sull'interfaccia del tunnel deve essere disabilitata a causa di un bug. Disattivare l'opzione di commutazione veloce sull'interfaccia del tunnel. Per visualizzare i dettagli dei bug relativi a questo problema, consultare CSCdm10376 (solo utenti registrati).

Operazioni preliminari

Prerequisiti

Prima di provare la configurazione, verificare che siano soddisfatti i seguenti prerequisiti:

- conoscenza della configurazione e del routing IPX
- conoscenza e configurazione dei tunnel GRE
- conoscenza operativa e configurazione di IPSec

Componenti usati

Le informazioni fornite in questo documento si basano sulle versioni software e hardware riportate di seguito.

- Software Cisco IOS® versione 12.2(7)
- Cisco serie 3600 Router

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

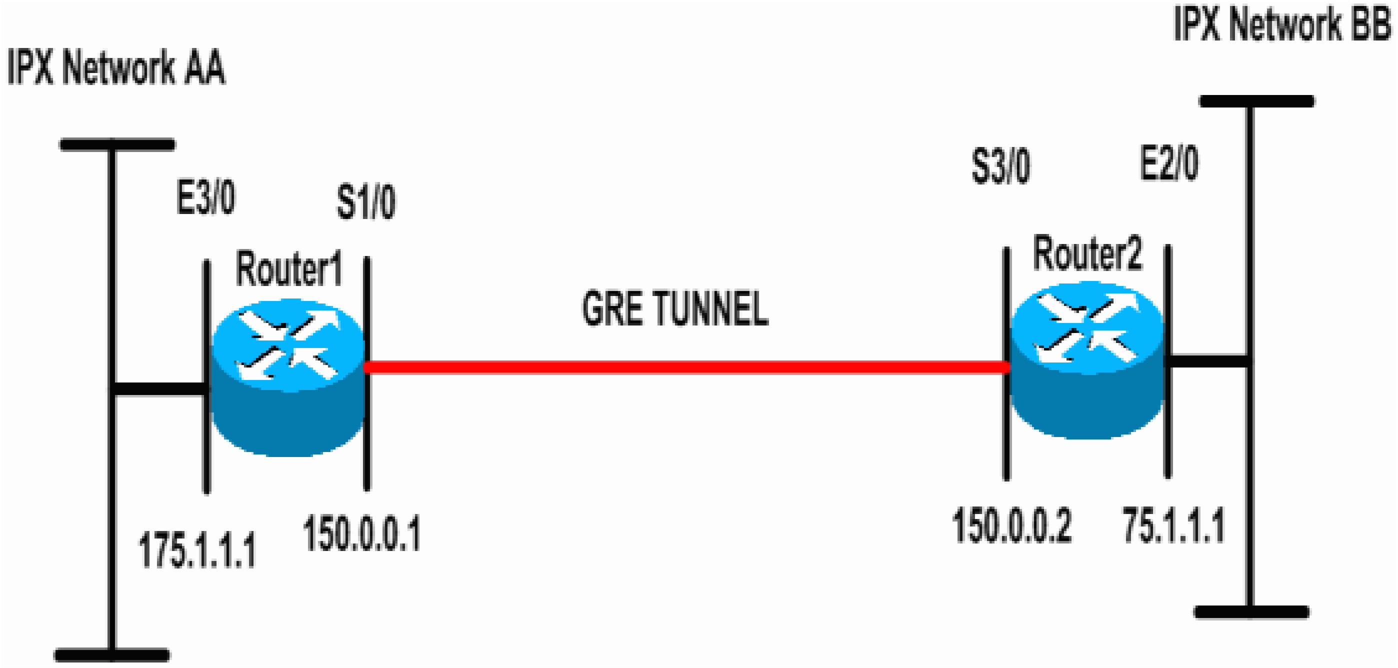
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Questo documento utilizza le impostazioni di rete mostrate nel diagramma sottostante.



Configurazioni

Questo documento utilizza le configurazioni mostrate di seguito.

Router 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
```

Router 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
```

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show sono supportati dallo** strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando **show.**

- **show ipx interface**: visualizza lo stato e i parametri delle interfacce IPX configurate sul dispositivo, ad esempio l'indirizzo della rete IPX e del nodo.
- **show ipx route**: visualizza il contenuto della tabella di routing IPX.

- **show crypto isakmp sa**: visualizza le associazioni di sicurezza della fase 1 mostrando l'associazione di sicurezza IKE del router. Affinché un'associazione di protezione IKE sia considerata attiva e funzionante, lo stato visualizzato deve essere QM_IDLE.
- **show crypto ipsec sa**: visualizza le associazioni di sicurezza della fase 2 mostrando un elenco dettagliato delle associazioni di sicurezza IPSec attive del router.
- **show crypto map**: visualizza le mappe crittografiche configurate sul router e i relativi dettagli, ad esempio gli elenchi degli accessi crittografici, i set di trasformazioni, i peer e così via.
- **show crypto engine connections active**: visualizza un elenco di associazioni di protezione attive con le interfacce, le trasformazioni e i contatori associati.

Output di esempio

In questa sezione vengono acquisiti gli output del comando **show** sul dispositivo Router1 quando il comando IPX **ping** viene eseguito sul router1 destinato al router2. Gli output sul router2 sono simili. I parametri chiave nell'output sono indicati in **grassetto**. Per ulteriori informazioni sugli output del comando, consultare il documento sulla risoluzione dei problemi di sicurezza IP - descrizione e uso dei comandi di debug.

```
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
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Comandi per la risoluzione dei problemi

Nota: prima di usare i comandi di **debug**, consultare le informazioni importanti sui comandi di debug.

- debug crypto engine: visualizza le informazioni sul motore di crittografia che esegue il processo di crittografia e decrittografia.
- debug crypto ipsec: visualizza le negoziazioni IPSec della fase 2.
- debug crypto isakmp: visualizza le negoziazioni IKE della fase 1.

Output di esempio del comando debug

In questa sezione vengono acquisiti gli output del comando debug sui router configurati con IPSec. Il comando **ping** IPX viene eseguito sul router1 destinato al router2.

- Router1
- Router2

Router1

```
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#
```

Router2

```
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#
```

Informazioni correlate

- Pagina di supporto per la tecnologia GRE
- Pagina di supporto per la tecnologia IP Security (IPSec)
- Supporto tecnico – Cisco Systems