Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Configurar](#)
[Diagrama de la red](#)
[Configuraciones](#)
[Verificación](#)
[Salida del comando show con túneles activos](#)
[Troubleshooting](#)
[Comandos para resolución de problemas](#)
[Información Relacionada](#)

Introducción

Las configuraciones IPsec normales no pueden transferir protocolos de ruteo como EIGRP (Enhanced Interior Gateway Routing Protocol) y OSPF (Open Shortest Path First) ni tráfico que no sea IP como IPX (Internetwork Packet Exchange), AppleTalk, etc. Este documento ilustra cómo rutear entre diferentes redes mediante un protocolo de ruteo y tráfico no IP dentro de IPSec. Esta técnica utiliza Generic Routing Encapsulation (GRE) como método para lograrlo.

prerrequisitos

Requisitos

Antes de utilizar esta configuración, asegúrese de que cumple con los siguientes requisitos:

- Aseegurese los trabajos del túnel antes de que usted aplique las correspondencias de criptografía.
- Necesidad Crypto de la lista de acceso de tener GRE como el protocolo a permitir: y.y.y.y del host del permit gre host x.x.x.x del access-list 101 x.x.x.x = y.y.y.y = <tunnel_destination> del <tunnel_source>
- Utilice los IP Addresses del loopback para identificar a los pares del Internet Key Exchange (IKE) y origen de túnel y destino del túnel para mejorar la Disponibilidad.
- Para una discusión de los problemas posibles de la Unidad máxima de transmisión (MTU) (MTU), refiera a ajustar el IP MTU, TCP MSS y PMTUD en los sistemas de Windows y de Sun.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y

hardware.

- Software Release 12.1.8 y 12.2.1 de Cisco IOS®

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Configurar

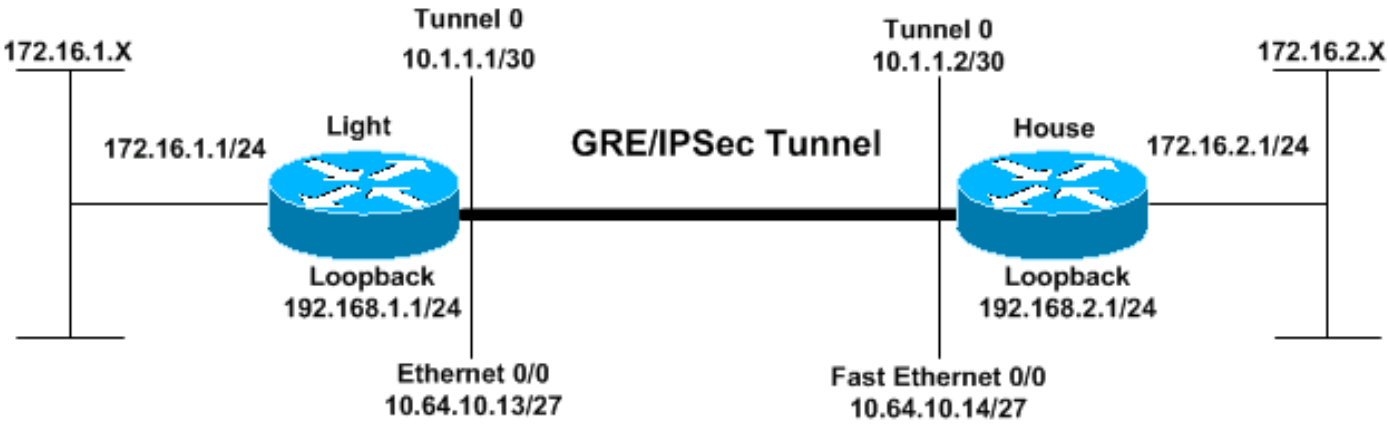
En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para clientes registrados).

Nota sobre la configuración IOS: Con los códigos del Cisco IOS Software Release 12.2(13)T y Posterior (códigos numerados más altos del T-tren, los códigos del Cisco IOS Software Release 12.3 y Posterior) el IPSec configurado “correspondencia de criptografía” necesita solamente ser aplicado a la interfaz física. Se requiere no más para ser aplicado en la interfaz de túnel GRE. Tener la “correspondencia de criptografía” en la comprobación y la interfaz del túnel cuando usted utiliza la versión de Cisco IOS Software 12.2.(13)T y posterior todavía cifra los trabajos. Sin embargo, se recomienda altamente para aplicarlo solamente en la interfaz física.

Diagrama de la red

Este documento utiliza la configuración de red que se muestra en el siguiente diagrama.



Configuraciones

- Luz
- Base

Luz

```
Current configuration:!version 12.2no service single-
slot-reload-enableservice timestamps debug uptimeservice
timestamps log uptimeno service password-
encryption!hostname Light!logging rate-limit console 10
except errors!ip subnet-zero!!no ip finger!no ip dhcp-
client network-discoveryipx routing 00e0.b06a.40fc!!---
IKE policies.crypto isakmp policy 25hash
md5authentication pre-sharecrypto isakmp key cisco123
address 192.168.2.1!!--- IPSec policies.crypto ipsec
transform-set WWW esp-des esp-md5-hmac mode
transport!crypto map GRE local-address Loopback0crypto
map GRE 50 ipsec-isakmp   set peer 192.168.2.1set
transform-set WWW !--- What to encrypt?match address
101!call rsvp-sync!fax interface-type modemmta receive
maximum-recipients 0!interface Loopback0ip address
192.168.1.1 255.255.255.0!interface Tunnel0ip address
10.1.1.1 255.255.255.252ip mtu 1440ipx network CCtunnel
source Loopback0tunnel destination 192.168.2.1crypto map
GRE!interface FastEthernet0/0ip address 10.64.10.13
255.255.255.224no ip route-cacheno ip mroute-cacheduplex
autospeed autocrypto map GRE!interface FastEthernet0/1ip
address 172.16.1.1 255.255.255.0duplex autospeed autoipx
network AA!         router eigrp 10network 10.1.1.0
0.0.0.3network 172.16.1.0 0.0.0.255network 192.168.1.0no
auto-summaryno eigrp log-neighbor-changes!ip kerberos
source-interface anyip classlessip route 192.168.2.0
255.255.255.0 10.64.10.14ip http server!!--- What to
encrypt?access-list 101 permit gre host 192.168.1.1 host
192.168.2.1!dial-peer cor custom!line con 0transport
input noneline aux 0line vty 0 4login!endLight#!
```

Base

```
Current configuration:version 12.1service timestamps
debug uptimeservice timestamps log uptimeno service
password-encryption!hostname House!ip subnet-zero!ipx
routing 00e0.b06a.4114!!--- IKE policies.crypto isakmp
policy 25hash md5authentication pre-sharecrypto isakmp
key cisco123 address 192.168.1.1    !!--- IPSec
policies.crypto ipsec transform-set WWW esp-des esp-md5-
hmac mode transport!crypto map GRE local-address
Loopback0crypto map GRE 50 ipsec-isakmp   set peer
192.168.1.1set transform-set WWW !--- What to
encrypt?match address 101!!interface Loopback0ip address
192.168.2.1 255.255.255.0!interface Tunnel0ip address
10.1.1.2 255.255.255.252ip mtu 1440ipx network CCtunnel
source Loopback0tunnel destination 192.168.1.1crypto map
GRE!interface FastEthernet0/0ip address 10.64.10.14
255.255.255.224no ip route-cacheno ip mroute-cacheduplex
autospeed autocrypto map GRE!interface FastEthernet0/1ip
address 172.16.2.1 255.255.255.0duplex autospeed autoipx
network BB!interface FastEthernet4/0no ip
addressshutdownduplex autospeed auto!router eigrp
10network 10.1.1.0 0.0.0.3network 172.16.2.0
0.0.0.255network 192.168.2.0no auto-summaryno eigrp log-
neighbor-changes!ip classlessip route 192.168.1.0
255.255.255.0 10.64.10.13ip http server!--- What to
encrypt?access-list 101 permit gre host 192.168.2.1 host
192.168.1.1!line con 0line aux 0line vty 0
4login!endHouse#
```

Verificación

En esta sección encontrará información que puede utilizar para comprobar que su configuración funcione correctamente.

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- ¿**active del show crypto engine connections**? Muestra los paquetes encriptados y desencriptados entre los peeres IPSec.
- ¿**muestre isakmp crypto sa**? Asociaciones de seguridad de la fase 1 de las demostraciones.
- ¿**muestre IPSec crypto sa**? Asociaciones de seguridad de la fase 2 de las demostraciones.
- ¿**show ipx route [network] [default] [detailed]**? Muestra el contenido del tabla de IPX Routing.

Salida del comando show con túneles activos

```
Light#show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area        N1 - OSPF NSSA external
type 1, N2 - OSPF NSSA external type 2       E1 - OSPF external type 1, E2 - OSPF external type
2, E - EGP       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR       P - periodic downloaded static
routeGateway of last resort is not set     172.16.0.0/24 is subnetted, 2 subnetsC
172.16.1.0 is directly connected, FastEthernet0/1D       172.16.2.0 [90/297246976] via 10.1.1.2,
00:00:31, Tunnel0     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masksC       10.1.1.0/30 is
directly connected, Tunnel0C       10.64.10.0/27 is directly connected, FastEthernet0/0C
192.168.1.0/24 is directly connected, Loopback0S    192.168.2.0/24 [1/0] via
10.64.10.14Light#ping        Protocol [ip]: Target IP address: 172.16.2.1Repeat count [5]:
Datagram size [100]: Timeout in seconds [2]: Extended commands [n]: ySource address or
interface: 172.16.1.1Type of service [0]: Set DF bit in IP header? [no]: Validate reply data?
[no]: Data pattern [0xABCD]: Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of
sizes [n]: Type escape sequence to abort.Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout
is 2 seconds:!!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4
msLight#House#show ip routeCodes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area        N1 - OSPF NSSA
external type 1, N2 - OSPF NSSA external type 2       E1 - OSPF external type 1, E2 - OSPF
external type 2, E - EGP       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area       * - candidate default, U - per-user static route, o - ODR       P - periodic
downloaded static routeGateway of last resort is not set     172.16.0.0/24 is subnetted, 2
subnetsD       172.16.1.0 [90/297246976] via 10.1.1.1, 00:00:36, Tunnel0C       172.16.2.0 is
directly connected, FastEthernet0/1     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masksC
10.1.1.0/30 is directly connected, Tunnel0C       10.64.10.0/27 is directly connected,
FastEthernet0/0S    192.168.1.0/24 [1/0] via 10.64.10.13C    192.168.2.0/24 is directly
connected, Loopback0House#ping Protocol [ip]: Target IP address: 172.16.1.1Repeat count [5]:
Datagram size [100]: Timeout in seconds [2]: Extended commands [n]: ySource address or
interface: 172.16.2.1Type of service [0]: Set DF bit in IP header? [no]: Validate reply data?
[no]: Data pattern [0xABCD]: Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of
sizes [n]: Type escape sequence to abort.Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout
is 2 seconds:!!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 msLight#show
ipx routeCodes: 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 static3 Total IPX
routes. Up to 1 parallel paths and 16 hops allowed.No default route known.C         AA (NOVELL-
ETHER),  Fa0/1C         CC (TUNNEL),        Tu0R         BB [151/01] via
CC.00e0.b06a.4114,   17s, Tu0House#show ipx routeCodes: 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 static3 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.No
```

default route known.C BB (NOVELL-ETHER), Fa0/1C CC (TUNNEL), Tu0R AA [151/01] via CC.00e0.b06a.40fc, 59s, Tu0Light#**ping ipx BB.0004.9af2.8261**Type escape sequence to abort.Sending 5, 100-byte IPX Novell Echoes to BB.0004.9af2.8261, timeout is 2 second:!!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 msHouse#**ping ipx AA.0004.9af2.8181** Type escape sequence to abort.Sending 5, 100-byte IPX Novell Echoes to AA.0004.9af2.8181, timeout is 2 second:!!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 msLight#**show crypto isa sa** dst src state conn-id slot192.168.2.1 192.168.1.1 QM_IDLE 1 0192.168.1.1 192.168.2.1 QM_IDLE 2 0House#**show crypto isa sa** dst src state conn-id slot192.168.1.1 192.168.2.1 QM_IDLE 1 0192.168.2.1 192.168.1.1 QM_IDLE 2 0Light#**show crypto engine connections active** ID Interface IP-Address State Algorithm Encrypt Decrypt 1 <none> <none> set HMAC_MD5+DES_56_CB 0 0 2 <none> <none> set HMAC_MD5+DES_56_CB 0 02000 FastEthernet0/0 10.64.10.13 set
HMAC_MD5+DES_56_CB 0 1612001 FastEthernet0/0 10.64.10.13 set
HMAC_MD5+DES_56_CB 161 02002 FastEthernet0/0 10.64.10.13 set
HMAC_MD5+DES_56_CB 0 02003 FastEthernet0/0 10.64.10.13 set
HMAC_MD5+DES_56_CB 0 02004 FastEthernet0/0 10.64.10.13 set
HMAC_MD5+DES_56_CB 0 02005 FastEthernet0/0 10.64.10.13 set
HMAC_MD5+DES_56_CB 0 0House#**show crypto engine connections active** ID Interface IP-Address State Algorithm Encrypt Decrypt 1 <none> <none> set HMAC_MD5+DES_56_CB 0 0 2 <none> <none> set
HMAC_MD5+DES_56_CB 0 02000 FastEthernet0/0 10.64.10.14 set
HMAC_MD5+DES_56_CB 0 1592001 FastEthernet0/0 10.64.10.14 set
HMAC_MD5+DES_56_CB 159 02002 FastEthernet0/0 10.64.10.14 set
HMAC_MD5+DES_56_CB 0 02003 FastEthernet0/0 10.64.10.14 set
HMAC_MD5+DES_56_CB 0 02004 FastEthernet0/0 10.64.10.14 set
HMAC_MD5+DES_56_CB 0 02005 FastEthernet0/0 10.64.10.14 set
HMAC_MD5+DES_56_CB 0 0House#**show crypto ipsec sa detail** interface: Tunnel0 Crypto map tag: GRE, local addr. 192.168.2.1 local ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/47/0) remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/47/0) current_peer: 192.168.1.1 PERMIT, flags={origin_is_acl,transport_parent,} #pkts encaps: 192, #pkts encrypt: 192, #pkts digest 192 #pkts decaps: 190, #pkts decrypt: 190, #pkts verify 190 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0 #pkts no sa (send) 12, #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.: 192.168.2.1, remote crypto endpt.: 192.168.1.1 path mtu 1514, media mtu 1514 current outbound spi: 1FA721CA inbound esp sas: spi: 0xEE52531(249898289) transform: esp-des esp-md5-hmac , in use settings ={Transport, } slot: 0, conn id: 2000, flow_id: 1, crypto map: GRE sa timing: remaining key lifetime (k/sec): (4607961/2797) IV size: 8 bytes replay detection support: Y spi: 0xFEE24F3(267265267) transform: esp-des esp-md5-hmac , in use settings ={Transport, } slot: 0, conn id: 2002, flow_id: 3, crypto map: GRE sa timing: remaining key lifetime (k/sec): (4608000/2826) IV size: 8 bytes replay detection support: Y spi: 0x19240817(421791767) transform: esp-des esp-md5-hmac , in use settings ={Transport, } slot: 0, conn id: 2004, flow_id: 5, crypto map: GRE sa timing: remaining key lifetime (k/sec): (4608000/2759) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x1FA721CA(531046858) transform: esp-des esp-md5-hmac , in use settings ={Transport, } slot: 0, conn id: 2001, flow_id: 2, crypto map: GRE sa timing: remaining key lifetime (k/sec): (4607972/2797) IV size: 8 bytes replay detection support: Y spi: 0x12B10EB0(313593520) transform: esp-des esp-md5-hmac , in use settings ={Transport, } slot: 0, conn id: 2003, flow_id: 4, crypto map: GRE sa timing: remaining key lifetime (k/sec): (4608000/2826) IV size: 8 bytes replay detection support: Y spi: 0x1A700242(443548226) transform: esp-des esp-md5-hmac , in use settings ={Transport, } slot: 0, conn id: 2005, flow_id: 6, crypto map: GRE sa timing: remaining key lifetime (k/sec): (4608000/2759) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas: local ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/0/0) remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0) current_peer: 192.168.1.1 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    #pkts no sa (send) 0, #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.: 192.168.2.1, remote crypto endpt.: 192.168.1.1     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:interface: FastEthernet0/0    Crypto
map tag: GRE, local addr. 192.168.2.1             local  ident (addr/mask/prot/port):
(192.168.2.1/255.255.255.255/47/0)   remote ident (addr/mask/prot/port):
(192.168.1.1/255.255.255.255/47/0)   current_peer: 192.168.1.1     PERMIT,
flags={origin_is_acl,transport_parent,}    #pkts encaps: 193, #pkts encrypt: 193, #pkts digest
193    #pkts decaps: 192, #pkts decrypt: 192, #pkts verify 192    #pkts compressed: 0, #pkts
decompressed: 0    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#pkts no sa (send) 12, #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.: 192.168.2.1, remote crypto endpt.: 192.168.1.1     path mtu
1514, media mtu 1514     current outbound spi: 1FA721CA     inbound esp sas:      spi:
0xEE52531(249898289)        transform: esp-des esp-md5-hmac ,        in use settings
={Transport, }        slot: 0, conn id: 2000, flow_id: 1, crypto map: GRE        sa timing:
remaining key lifetime (k/sec): (4607961/2789)        IV size: 8 bytes        replay detection
support: Y      spi: 0xFEE24F3(267265267)        transform: esp-des esp-md5-hmac ,        in use
settings ={Transport, }        slot: 0, conn id: 2002, flow_id: 3, crypto map: GRE        sa
timing: remaining key lifetime (k/sec): (4608000/2817)        IV size: 8 bytes        replay
detection support: Y      spi: 0x19240817(421791767)        transform: esp-des esp-md5-hmac ,
in use settings ={Transport, }        slot: 0, conn id: 2004, flow_id: 5, crypto map: GRE
sa timing: remaining key lifetime (k/sec): (4608000/2750)        IV size: 8 bytes        replay
detection support: Y     inbound ah sas:     inbound pcp sas:     outbound esp sas:      spi:
0x1FA721CA(531046858)        transform: esp-des esp-md5-hmac ,        in use settings
={Transport, }        slot: 0, conn id: 2001, flow_id: 2, crypto map: GRE        sa timing:
remaining key lifetime (k/sec): (4607972/2789)        IV size: 8 bytes        replay detection
support: Y      spi: 0x12B10EB0(313593520)        transform: esp-des esp-md5-hmac ,        in
use settings ={Transport, }        slot: 0, conn id: 2003, flow_id: 4, crypto map: GRE        sa
timing: remaining key lifetime (k/sec): (4608000/2817)        IV size: 8 bytes        replay
detection support: Y      spi: 0x1A700242(443548226)        transform: esp-des esp-md5-hmac ,
in use settings ={Transport, }        slot: 0, conn id: 2005, flow_id: 6, crypto map: GRE
sa timing: remaining key lifetime (k/sec): (4608000/2750)        IV size: 8 bytes        replay
detection support: Y     outbound ah sas:     outbound pcp sas:   local  ident
(addr/mask/prot/port): (192.168.2.1/255.255.255.255/0/0)   remote ident (addr/mask/prot/port):
(192.168.1.1/255.255.255.255/0/0)   current_peer: 192.168.1.1     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    #pkts no sa (send) 0, #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.: 192.168.2.1, remote crypto endpt.: 192.168.1.1     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:
```

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

Nota: Antes de ejecutar un comando de depuración, consulte Información importante sobre comandos de depuración.

- ¿**isakmp del debug crypto**? Visualiza los errores durante la fase 1.
- ¿**IPSec del debug crypto**? Visualiza los errores durante la fase 2.
- ¿**motor del debug crypto**? Visualiza la información del motor de criptografía.
- ¿**debug ip your routing protocol**? Visualiza la información sobre las transacciones de ruteo de su Routing Protocol.
- **clear crypto connection connection-id [slot** | *rsm* | *¿vip]*? Termina a una sesión encriptada actualmente en curso. Las sesiones encriptadas terminan normalmente cuando los tiempos de la sesión hacia fuera. Utilice el comando show crypto cisco connections para conocer el valor de la conexión id.
- ¿**borre el isakmp crypto**? Borra las asociaciones de seguridad de la fase 1.
- ¿**borre el sa crypto**? Borra las asociaciones de seguridad de la fase 2.

Información Relacionada

- Página de soporte de IPSec
- Una Introducción al Cifrado de Seguridad IP (IPSec)
- Configuración de seguridad de red IPSec
- Configuración del protocolo de seguridad de intercambio de claves de Internet
- Comando lookup tool (sólo para clientes registrados)
- Soporte Técnico - Cisco Systems