

Túnel del sitio a localizar entre los routers IOS que usan la configuración de muestra del SELLO

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshooting](#)

[Comandos para resolución de problemas](#)

[Las limitaciones con el ESP-sello transforman el conjunto](#)

[Información Relacionada](#)

[Introducción](#)

SEAL (Software Encryption Algorithm) es un algoritmo alternativo a DES (Data Encryption Standard), 3DES (Triple DES) y AES (Advanced Encryption Standard). SELLE el cifrado utiliza una clave de encriptación del 160-bit y tiene un impacto más bajo al CPU cuando está comparado a otros algoritmos basados en software. Este documento ilustra cómo configurar un túnel IPsec del LAN a LAN (sitio a localizar) usando el SELLO.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

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

- Cisco 7200 Series Router que funcionan con el Software Release 12.3(7)T 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 [Convenciones de Consejos Técnicos de Cisco](#).

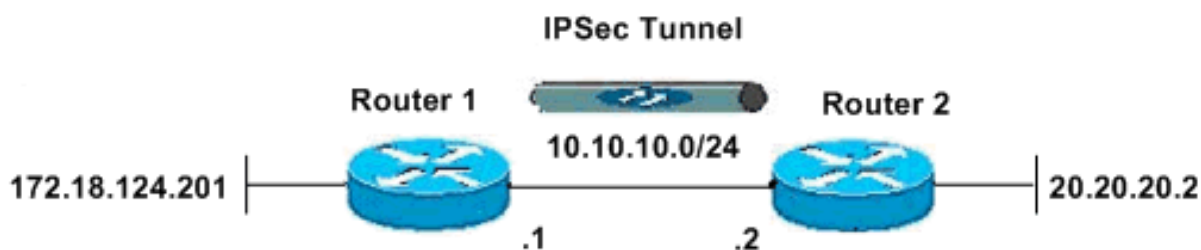
Configurar

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

Note: Use la herramienta [Command Lookup Tool](#) ([clientes registrados solamente](#)) para encontrar más información sobre los comandos usados en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

En este documento, se utilizan estas configuraciones:

- [Router 1](#)
- [Router 2](#)

Router 1

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST -5
no aaa new-model
ip subnet-zero
no ip domain lookup
```

```

!
!
ip cef
ip audit po max-events 100
no ftp-server write-enable
!
!
!
!
!--- ISAKMP policy configuration. crypto isakmp policy 1
encr aes 256 hash md5 authentication pre-share group 2
crypto isakmp key cisco123 address 10.10.10.2 ! !---
Define a transform set with SEAL. !--- If you use the
esp-seal transform set and a crypto !--- accelerator is
present, you receive a warning. !--- The configuration
is accepted, but it !--- is ignored as long as the
accelerator is present. !--- If you use the esp-seal
transform set with either of !--- the other two
limitations, you receive an error !--- and the
configuration is rejected. crypto ipsec transform-set
cisco esp-seal esp-sha-hmac ! !--- Define a transform
set with SEAL. crypto map cisco 10 ipsec-isakmp set peer
10.10.10.2 set transform-set cisco match address 100 ! !
! interface Ethernet0/0 ip address 172.18.124.201
255.255.255.0 ! !--- Apply crypto-map to the public
interface. interface Ethernet1/0 ip address 10.10.10.1
255.255.255.0 crypto map cisco ! ip classless ip route
0.0.0.0 0.0.0.0 10.10.10.2 no ip http server no ip http
secure-server ! ! !--- Access Control List (ACL) that
defines the networks to encrypt. access-list 100 permit
ip 172.18.124.0 0.0.0.255 20.20.20.0 0.0.0.255 ! ! !
control-plane ! ! line con 0 exec-timeout 0 0 line aux 0
line vty 0 4 password ww login ! ! end

```

Router 2

```

version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST -5
no aaa new-model
ip subnet-zero
no ip domain lookup
!
!
ip cef
ip audit po max-events 100
no ftp-server write-enable
!
!
!
!
!--- ISAKMP policy configuration. crypto isakmp policy 1
encr aes 256 hash md5 authentication pre-share group 2
crypto isakmp key cisco123 address 10.10.10.1 ! !---

```

```
Define a transform set with SEAL. !--- If you use the
esp-seal transform set and a crypto !--- accelerator is
present, you receive a warning. !--- The configuration
is accepted, but it !--- is ignored as long as the
accelerator is present. !--- If you use the esp-seal
transform set with either of !--- the other two
limitations, you receive an error !--- and the
configuration is rejected. crypto ipsec transform-set
cisco esp-seal esp-sha-hmac ! !--- Define a transform
set with SEAL. crypto map cisco 10 ipsec-isakmp set peer
10.10.10.1 set transform-set cisco match address 100 ! !
! ! !--- Apply crypto-map to the public interface.
interface Ethernet0/0 ip address 10.10.10.2
255.255.255.0 crypto map cisco ! interface Ethernet0/0
ip address 20.20.20.2 255.255.255.0 ! ip classless ip
route 0.0.0.0 0.0.0.0 10.10.10.1 no ip http server no ip
http secure-server ! ! !--- ACL defines the networks to
encrypt. access-list 100 permit ip 20.20.20.0 0.0.0.255
172.18.124.0 0.0.0.255 ! ! ! control-plane ! ! line con
0 exec-timeout 0 0 line aux 0 line vty 0 4 password ww
login ! ! end
```

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

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

- **correspondencia de criptografía de la demostración** — Verifica la configuración en el router. Esta salida se toma del router1.

```
R1#show crypto map
Crypto Map "cisco" 10 ipsec-isakmp
Peer = 10.10.10.2
Extended IP access list 100
access-list 100 permit ip 172.18.124.0 0.0.0.255 20.20.20.0 0.0.0.255
Current peer: 10.10.10.2
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
Transform sets={
cisco,
}
Interfaces using crypto map cisco:
Ethernet1/0
```

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.

Note: [Antes de ejecutar un comando de depuración, consulte Información importante sobre comandos de depuración.](#)

[Debugs ISAMP y del IPSec](#)

- **debugging de la demostración** — Visualiza la información sobre los tipos de debugging que se habilitan para su router.

```
R1#show debugging
```

```
Cryptographic Subsystem:  
Crypto ISAKMP debugging is on  
Crypto IPSEC debugging is on
```

```
R1#
```

```
*Apr 18 05:59:20.491: ISAKMP (0:0): received packet  
from 10.10.10.2 dport 500 sport 500 Global (N) NEW SA  
*Apr 18 05:59:20.491: ISAKMP: Created a peer struct for  
10.10.10.2, peer port 500  
*Apr 18 05:59:20.491: ISAKMP: Locking peer struct 0x25F0BD8,  
IKE refcount 1 for crypto_isakmp_process_block  
*Apr 18 05:59:20.491: ISAKMP: local port 500, remote port 500  
*Apr 18 05:59:20.519: insert sa successfully sa = 2398188  
*Apr 18 05:59:20.519: ISAKMP:(0:1:SW:1):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH  
*Apr 18 05:59:20.519: ISAKMP:(0:1:SW:1):Old State = IKE_READY  
New State = IKE_R_MM1  
  
*Apr 18 05:59:20.579: ISAKMP:(0:1:SW:1): processing SA payload. message ID = 0  
*Apr 18 05:59:20.579: ISAKMP:(0:1:SW:1): processing vendor id payload  
*Apr 18 05:59:20.579: ISAKMP:(0:1:SW:1): vendor ID seems Unity/DPD  
but major 157 mismatch  
*Apr 18 05:59:20.579: ISAKMP:(0:1:SW:1): vendor ID is NAT-T v3  
*Apr 18 05:59:20.579: ISAKMP:(0:1:SW:1): processing vendor id payload  
*Apr 18 05:59:20.579: ISAKMP:(0:1:SW:1): vendor ID seems Unity/DPD  
but major 123 mismatch  
*Apr 18 05:59:20.579: ISAKMP:(0:1:SW:1): vendor ID is NAT-T v2  
*Apr 18 05:59:20.579: ISAKMP: Looking for a matching key for  
10.10.10.2 in default : success  
*Apr 18 05:59:20.579: ISAKMP:(0:1:SW:1):found peer pre-shared key  
matching 10.10.10.2  
*Apr 18 05:59:20.579: ISAKMP:(0:1:SW:1): local preshared key found  
*Apr 18 05:59:20.579: ISAKMP : Scanning profiles for xauth ...  
*Apr 18 05:59:20.579: ISAKMP:(0:1:SW:1):Checking ISAKMP transform 1  
against priority 1 policy  
*Apr 18 05:59:20.579: ISAKMP: encryption AES-CBC  
*Apr 18 05:59:20.579: ISAKMP: keylength of 256  
*Apr 18 05:59:20.579: ISAKMP: hash MD5  
*Apr 18 05:59:20.579: ISAKMP: default group 2  
*Apr 18 05:59:20.579: ISAKMP: auth pre-share  
*Apr 18 05:59:20.579: ISAKMP: life type in seconds  
*Apr 18 05:59:20.579: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80  
*Apr 18 05:59:20.579: ISAKMP:(0:1:SW:1):atts are acceptable. Next payload is 0  
*Apr 18 05:59:20.579: ISAKMP:(0:1:SW:1): processing vendor id payload  
*Apr 18 05:59:20.579: ISAKMP:(0:1:SW:1): vendor ID seems Unity/DPD  
but major 157 mismatch  
*Apr 18 05:59:20.579: ISAKMP:(0:1:SW:1): vendor ID is NAT-T v3  
*Apr 18 05:59:20.579: ISAKMP:(0:1:SW:1): processing vendor id payload  
*Apr 18 05:59:20.579: ISAKMP:(0:1:SW:1): vendor ID seems Unity/DPD  
but major 123 mismatch  
*Apr 18 05:59:20.579: ISAKMP:(0:1:SW:1): vendor ID is NAT-T v2
```

*Apr 18 05:59:20.579: ISAKMP:(0:1:SW:1):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE

*Apr 18 05:59:20.579: ISAKMP:(0:1:SW:1):Old State = IKE_R_MM1 New
State = IKE_R_MM1

*Apr 18 05:59:20.619: ISAKMP:(0:1:SW:1): constructed NAT-T vendor-03 ID

*Apr 18 05:59:20.619: ISAKMP:(0:1:SW:1): sending packet to 10.10.10.2
my_port 500 peer_port 500 (R) MM_SA_SETUP

*Apr 18 05:59:20.619: ISAKMP:(0:1:SW:1):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE

*Apr 18 05:59:20.619: ISAKMP:(0:1:SW:1):Old State = IKE_R_MM1 New
State = IKE_R_MM2

*Apr 18 05:59:20.911: ISAKMP (0:134217729): received packet from
10.10.10.2 dport 500 sport 500 Global (R) MM_SA_SETUP

*Apr 18 05:59:20.911: ISAKMP:(0:1:SW:1):Input = IKE_MESG_FROM_PEER,
IKE_MM_EXCH

*Apr 18 05:59:20.911: ISAKMP:(0:1:SW:1):Old State = IKE_R_MM2
New State = IKE_R_MM3

*Apr 18 05:59:20.939: ISAKMP:(0:1:SW:1): processing KE payload. message ID = 0

*Apr 18 05:59:20.939: ISAKMP:(0:1:SW:1): processing NONCE
payload. message ID = 0

*Apr 18 05:59:20.991: ISAKMP: Looking for a matching key for
10.10.10.2 in default : success

*Apr 18 05:59:20.991: ISAKMP:(0:1:SW:1):found peer pre-shared
key matching 10.10.10.2

*Apr 18 05:59:20.991: ISAKMP:(0:1:SW:1):SKEYID state generated

*Apr 18 05:59:20.991: ISAKMP:(0:1:SW:1): processing vendor id payload

*Apr 18 05:59:20.991: ISAKMP:(0:1:SW:1): vendor ID is Unity

*Apr 18 05:59:20.991: ISAKMP:(0:1:SW:1): processing vendor id payload

*Apr 18 05:59:20.991: ISAKMP:(0:1:SW:1): vendor ID is DPD

*Apr 18 05:59:20.991: ISAKMP:(0:1:SW:1): processing vendor id payload

*Apr 18 05:59:20.991: ISAKMP:(0:1:SW:1): speaking to another IOS box!

*Apr 18 05:59:20.991: ISAKMP:received payload type 17

*Apr 18 05:59:20.991: ISAKMP:received payload type 17

*Apr 18 05:59:20.991: ISAKMP:(0:1:SW:1):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE

*Apr 18 05:59:20.991: ISAKMP:(0:1:SW:1):Old State = IKE_R_MM3 New
State = IKE_R_MM3

*Apr 18 05:59:21.051: ISAKMP:(0:1:SW:1): sending packet to
10.10.10.2 my_port 500 peer_port 500 (R) MM_KEY_EXCH

*Apr 18 05:59:21.051: ISAKMP:(0:1:SW:1):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE

*Apr 18 05:59:21.051: ISAKMP:(0:1:SW:1):Old State = IKE_R_MM3
New State = IKE_R_MM4

*Apr 18 05:59:21.279: ISAKMP (0:134217729): received packet
from 10.10.10.2 dport 500 sport 500 Global (R) MM_KEY_EXCH

*Apr 18 05:59:21.279: ISAKMP:(0:1:SW:1):Input = IKE_MESG_FROM_PEER,
IKE_MM_EXCH

*Apr 18 05:59:21.279: ISAKMP:(0:1:SW:1):Old State = IKE_R_MM4
New State = IKE_R_MM5

*Apr 18 05:59:21.311: ISAKMP:(0:1:SW:1): processing ID payload. message ID = 0

*Apr 18 05:59:21.311: ISAKMP (0:134217729): ID payload
next-payload : 8
type : 1
address : 10.10.10.2
protocol : 17
port : 500
length : 12

*Apr 18 05:59:21.311: ISAKMP:(0:1:SW:1):: peer matches *none* of the profiles

*Apr 18 05:59:21.311: ISAKMP:(0:1:SW:1): processing HASH
payload. message ID = 0

*Apr 18 05:59:21.311: ISAKMP:(0:1:SW:1): processing NOTIFY
INITIAL_CONTACT protocol 1
spi 0, message ID = 0, sa = 2398188

*Apr 18 05:59:21.311: ISAKMP:(0:1:SW:1):SA authentication status:
authenticated

*Apr 18 05:59:21.311: ISAKMP:(0:1:SW:1): Process initial contact,
bring down existing phase 1 and 2 SA's with local 10.10.10.1
remote 10.10.10.2 remote port 500

*Apr 18 05:59:21.311: ISAKMP:(0:1:SW:1):SA authentication status:
authenticated

*Apr 18 05:59:21.311: ISAKMP:(0:1:SW:1):SA has been authenticated
with 10.10.10.2

*Apr 18 05:59:21.311: ISAKMP: Trying to insert a peer
10.10.10.1/10.10.10.2/500/, and inserted successfully.

*Apr 18 05:59:21.311: ISAKMP:(0:1:SW:1):: peer matches
none of the profiles

*Apr 18 05:59:21.311: ISAKMP:(0:1:SW:1):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE

*Apr 18 05:59:21.311: ISAKMP:(0:1:SW:1):Old State =
IKE_R_MM5 New State = IKE_R_MM5

*Apr 18 05:59:21.331: IPSEC(key_engine): got a queue event with 1 kei messages

*Apr 18 05:59:21.391: ISAKMP:(0:1:SW:1):SA is doing
pre-shared key authentication using id type ID_IPV4_ADDR

*Apr 18 05:59:21.391: ISAKMP (0:134217729): ID payload
next-payload : 8
type : 1
address : 10.10.10.1
protocol : 17
port : 500
length : 12

*Apr 18 05:59:21.391: ISAKMP:(0:1:SW:1):Total payload length: 12

*Apr 18 05:59:21.391: ISAKMP:(0:1:SW:1): sending packet to
10.10.10.2 my_port 500 peer_port 500 (R) MM_KEY_EXCH

*Apr 18 05:59:21.391: ISAKMP:(0:1:SW:1):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE

*Apr 18 05:59:21.391: ISAKMP:(0:1:SW:1):Old State = IKE_R_MM5
New State = IKE_P1_COMPLETE

*Apr 18 05:59:21.439: ISAKMP:(0:1:SW:1):Input = IKE_MESG_INTERNAL,
IKE_PHASE1_COMPLETE

*Apr 18 05:59:21.439: ISAKMP:(0:1:SW:1):Old State = IKE_P1_COMPLETE
New State = IKE_P1_COMPLETE

*Apr 18 05:59:21.779: ISAKMP (0:134217729): received packet from
10.10.10.2 dport 500 sport 500 Global (R) QM_IDLE

*Apr 18 05:59:21.779: ISAKMP: set new node 1056009800 to QM_IDLE

*Apr 18 05:59:21.779: ISAKMP:(0:1:SW:1): processing HASH payload.
message ID = 1056009800

*Apr 18 05:59:21.779: ISAKMP:(0:1:SW:1): processing SA payload.
message ID = 1056009800

*Apr 18 05:59:21.779: ISAKMP:(0:1:SW:1):Checking IPsec proposal 1

*Apr 18 05:59:21.779: ISAKMP: transform 1, **ESP_SEAL**

*Apr 18 05:59:21.779: ISAKMP: attributes in transform:

*Apr 18 05:59:21.779: ISAKMP: encaps is 1 (Tunnel)

*Apr 18 05:59:21.779: ISAKMP: SA life type in seconds

*Apr 18 05:59:21.779: ISAKMP: SA life duration (basic) of 3600

*Apr 18 05:59:21.779: ISAKMP: SA life type in kilobytes

*Apr 18 05:59:21.779: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0

*Apr 18 05:59:21.779: ISAKMP: authenticator is HMAC-SHA

*Apr 18 05:59:21.779: ISAKMP:(0:1:SW:1):atts are acceptable.

*Apr 18 05:59:21.779: IPSEC(validate_proposal_request): proposal part #1,

```
(key eng. msg.) INBOUND local= 10.10.10.1, remote= 10.10.10.2,
local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4),
remote_proxy= 20.20.20.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-seal esp-sha-hmac (Tunnel),
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
*Apr 18 05:59:21.779: IPSEC(kei_proxy): head = cisco,
map->ivrf = , kei->ivrf =
*Apr 18 05:59:21.779: ISAKMP:(0:1:SW:1): processing NONCE
payload. message ID = 1056009800
*Apr 18 05:59:21.779: ISAKMP:(0:1:SW:1): processing ID
payload. message ID = 1056009800
*Apr 18 05:59:21.779: ISAKMP:(0:1:SW:1): processing ID
payload. message ID = 1056009800
*Apr 18 05:59:21.779: ISAKMP:(0:1:SW:1): asking for 1 spis from ipsec
*Apr 18 05:59:21.779: ISAKMP:(0:1:SW:1):Node 1056009800,
Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
*Apr 18 05:59:21.779: ISAKMP:(0:1:SW:1):Old State =
IKE_QM_READY New State = IKE_QM_SPI_STARVE
*Apr 18 05:59:21.799: IPSEC(key_engine): got a queue event with 1 kei messages
*Apr 18 05:59:21.799: IPSEC(spi_response): getting spi 3711321544 for SA
from 10.10.10.1 to 10.10.10.2 for prot 3
*Apr 18 05:59:21.811: ISAKMP: received ke message (2/1)
*Apr 18 05:59:22.079: IPsec: Flow_switching Allocated flow
for flow_id 134217729
*Apr 18 05:59:22.079: IPsec: Flow_switching Allocated flow
for flow_id 134217730
*Apr 18 05:59:22.199: %CRYPTO-5-SESSION_STATUS: Crypto tunnel
is UP . Peer 10.10.10.2:500 Id: 10.10.10.2
*Apr 18 05:59:22.199: ISAKMP: Locking peer struct 0x25F0BD8,
IPSEC refcount 1 for for stuff_ke
*Apr 18 05:59:22.199: ISAKMP:(0:1:SW:1): Creating IPsec SAs
*Apr 18 05:59:22.199: inbound SA from 10.10.10.2 to 10.10.10.1 (f/i) 0/ 0
(proxy 20.20.20.0 to 172.18.124.0)
*Apr 18 05:59:22.199: has spi 0xDD3645C8 and conn_id 2000 and flags 2
*Apr 18 05:59:22.199: lifetime of 3600 seconds
*Apr 18 05:59:22.199: lifetime of 4608000 kilobytes
*Apr 18 05:59:22.199: has client flags 0x0
*Apr 18 05:59:22.199: outbound SA from 10.10.10.1 to 10.10.10.2 (f/i) 0/0
(proxy 172.18.124.0 to 20.20.20.0)
*Apr 18 05:59:22.199: has spi 1918479069 and conn_id 2001 and flags A
*Apr 18 05:59:22.199: lifetime of 3600 seconds
*Apr 18 05:59:22.199: lifetime of 4608000 kilobytes
*Apr 18 05:59:22.199: has client flags 0x0
*Apr 18 05:59:22.199: ISAKMP:(0:1:SW:1): sending packet to
10.10.10.2 my_port 500 peer_port 500 (R) QM_IDLE
*Apr 18 05:59:22.199: ISAKMP:(0:1:SW:1):Node 1056009800,
Input = IKE_MSG_FROM_IPSEC, IKE_SPI_REPLY
*Apr 18 05:59:22.199: ISAKMP:(0:1:SW:1):Old State = IKE_QM_SPI_STARVE
New State = IKE_QM_R_QM2
*Apr 18 05:59:22.211: IPSEC(key_engine): got a queue event with 2 kei messages
*Apr 18 05:59:22.211: IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 10.10.10.1, remote= 10.10.10.2,
local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4),
remote_proxy= 20.20.20.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-seal esp-sha-hmac (Tunnel),
lifedur= 3600s and 4608000kb,
spi= 0xDD3645C8(3711321544), conn_id= 134219728, keysize= 0, flags= 0x2
*Apr 18 05:59:22.211: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 10.10.10.1, remote= 10.10.10.2,
local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4),
remote_proxy= 20.20.20.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-seal esp-sha-hmac (Tunnel),
lifedur= 3600s and 4608000kb,
```



```

spi= 0x7259AADD(1918479069), conn_id= 134219729, keysize= 0, flags= 0xA
*Apr 18 05:59:22.211: IPSEC(kei_proxy): head = cisco,
map->ivrf = , kei->ivrf =
*Apr 18 05:59:22.211: IPSEC(crypto_ipsec_sa_find_ident_head):
reconnecting with the same proxies and 10.10.10.2
*Apr 18 05:59:22.211: IPSEC(mtrees_add_ident): src 172.18.124.0,
dest 20.20.20.0, dest_port 0

*Apr 18 05:59:22.211: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.10.10.1, sa_prot= 50,
sa_spi= 0xDD3645C8(3711321544),
sa_trans= esp-seal esp-sha-hmac , sa_conn_id= 134219728
*Apr 18 05:59:22.211: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.10.10.2, sa_prot= 50,
sa_spi= 0x7259AADD(1918479069),
sa_trans= esp-seal esp-sha-hmac , sa_conn_id= 134219729
*Apr 18 05:59:22.339: ISAKMP (0:134217729): received packet
from 10.10.10.2 dport 500 sport 500 Global (R) QM_IDLE
*Apr 18 05:59:22.339: ISAKMP:(0:1:SW:1):deleting node 1056009800
error FALSE reason "quick mode done (await)"
*Apr 18 05:59:22.339: ISAKMP:(0:1:SW:1):Node 1056009800, Input =
IKE_MSG_FROM_PEER, IKE_QM_EXCH
*Apr 18 05:59:22.339: ISAKMP:(0:1:SW:1):Old State = IKE_QM_R_QM2
New State = IKE_QM_PHASE2_COMPLETE

```

Comandos show

- **show crypto isakmp sa** - Muestra la Asociación de seguridad (SA) del Protocolo de administración de asociaciones de seguridad de Internet (ISAKMP) construida entre los pares.

```

R1#show crypto isakmp sa
dst src state conn-id slot
10.10.10.1 10.10.10.2 QM_IDLE 1 0

```

```

R2#show crypto isakmp sa
dst src state conn-id slot
10.10.10.1 10.10.10.2 QM_IDLE 1 0

```

- **show crypto ipsec sa**—Muestra los IPSec SA construidos entre pares.

```

R1#show crypto ipsec sa
interface: Ethernet1/0
Crypto map tag: cisco, local addr. 10.10.10.1

protected vrf:
local ident (addr/mask/prot/port): (172.18.124.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (20.20.20.0/255.255.255.0/0/0)
current_peer: 10.10.10.2:500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 776, #pkts encrypt: 776, #pkts digest: 776
#pkts decaps: 776, #pkts decrypt: 776, #pkts verify: 776
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.2
path mtu 1500, media mtu 1500
current outbound spi: 7259AADD

inbound esp sas:
spi: 0xDD3645C8(3711321544)
transform: esp-seal esp-sha-hmac ,
in use settings = {Tunnel, }

```

slot: 0, conn id: 2000, flow_id: 1, crypto map: cisco
crypto engine type: Software, engine_id: 1
sa timing: remaining key lifetime (k/sec): (4565513/3382)
ike_cookies: 67432FCF F809B638 B84C0CD6 B0BCFFC3
IV size: 0 bytes
replay detection support: Y

inbound ah sas:

inbound pcg sas:

outbound esp sas:

spi: 0x7259AADD(1918479069)
transform: esp-seal esp-sha-hmac ,
in use settings = {Tunnel, }
slot: 0, conn id: 2001, flow_id: 2, crypto map: cisco
crypto engine type: Software, engine_id: 1
sa timing: remaining key lifetime (k/sec): (4565518/3382)
ike_cookies: 67432FCF F809B638 B84C0CD6 B0BCFFC3
IV size: 0 bytes
replay detection support: Y

outbound ah sas:

outbound pcg sas:

R1#

R2#**show crypto ipsec sa**

interface: Ethernet0/0
Crypto map tag: cisco, local addr. 10.10.10.2

protected vrf:

local ident (addr/mask/prot/port): (20.20.20.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (172.18.124.0/255.255.255.0/0/0)
current_peer: 10.10.10.1:500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 776, #pkts encrypt: 776, #pkts digest: 38
#pkts decaps: 776, #pkts decrypt: 776, #pkts verify: 38
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 10.10.10.2, remote crypto endpt.: 10.10.10.1
path mtu 1500, media mtu 1500
current outbound spi: DD3645C8

inbound esp sas:

spi: 0x7259AADD(1918479069)
transform: esp-seal esp-sha-hmac ,
in use settings = {Tunnel, }
slot: 0, conn id: 2000, flow_id: 3, crypto map: cisco
crypto engine type: Software, engine_id: 1
sa timing: remaining key lifetime (k/sec): (4536995/3410)
ike_cookies: B84C0CD6 B0BCFFC3 67432FCF F809B638
IV size: 0 bytes
replay detection support: Y

inbound ah sas:

inbound pcg sas:

```
outbound esp sas:
spi: 0xDD3645C8(3711321544)
transform: esp-seal esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: 4, crypto map: cisco
crypto engine type: Software, engine_id: 1
sa timing: remaining key lifetime (k/sec): (4537000/3409)
ike_cookies: B84C0CD6 B0BCFFC3 67432FCF F809B638
IV size: 0 bytes
replay detection support: Y

outbound ah sas:

outbound pcp sas:
```

Las limitaciones con el ESP-sello transforman el conjunto

Hay tres limitaciones en el uso del ESP-sello transforma el conjunto:

- El **esp-sello** transforma el conjunto puede ser utilizado solamente si no hay aceleradores criptográficos presentes. Esta limitación es presente porque ningunos aceleradores criptográficos actuales implementan el SELLO que el cifrado transforma el conjunto, y si un acelerador criptográfico está presente, maneja todas las conexiones del IPSec que se negocien con el IKE. Si un acelerador criptográfico está presente, el Cisco IOS Software permitirá que la transformación fije para ser configurada, pero advertirá que no sea utilizado mientras se habilite el acelerador criptográfico.
- El **esp-sello** transforma el conjunto se puede utilizar solamente conjuntamente con una autenticación transforma el conjunto, a saber uno de éstos: **esp-md5-hmac**, **esp-sha-hmac**, **ah-md5-hmac**, o **Ah-sha-hmac**. Esta limitación está presente porque el cifrado del SELLO es especialmente débil cuando se trata de la protección contra las modificaciones del paquete encriptado. Por lo tanto, para prevenir tal debilidad, se requiere una autenticación transforma el conjunto (la autenticación transforma los conjuntos se diseña foil tales ataques.). Si usted intenta configurar un IPSec transforme el conjunto usando el SELLO sin una autenticación transforman el conjunto, se genera un error, y se rechaza el conjunto de la transformación.
- El **esp-sello** transforma el conjunto no se puede utilizar con una correspondencia de criptografía manualmente cerrada. Esta limitación es presente porque tal configuración reutilizaría el mismo keystream para cada reinicialización, que comprometería la Seguridad. Debido al problema de seguridad, se prohíbe tal configuración. Si usted intenta configurar una correspondencia de criptografía manualmente cerrada con Sello-basado transforme el conjunto, se genera un error, y se rechaza el conjunto de la transformación.

Información Relacionada

- [Página de soporte de IPSec](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)