

Tunnel da sito a sito tra router IOS con configurazione di esempio SEAL

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Comandi per la risoluzione dei problemi](#)

[Limitazioni del set di trasformazioni con sigillo esp](#)

[Informazioni correlate](#)

Introduzione

L'algoritmo SEAL (Software Encryption Algorithm) è un algoritmo alternativo agli standard DES (Data Encryption Standard), 3DES (Triple DES) e AES (Advanced Encryption Standard). La crittografia SEAL utilizza una chiave di crittografia a 160 bit e ha un impatto minore sulla CPU rispetto ad altri algoritmi basati su software. In questo documento viene spiegato come configurare un tunnel IPsec da LAN a LAN (da sito a sito) usando il protocollo SEAL.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Router Cisco serie 7200 con software Cisco IOS® versione 12.3(7)T

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](#).

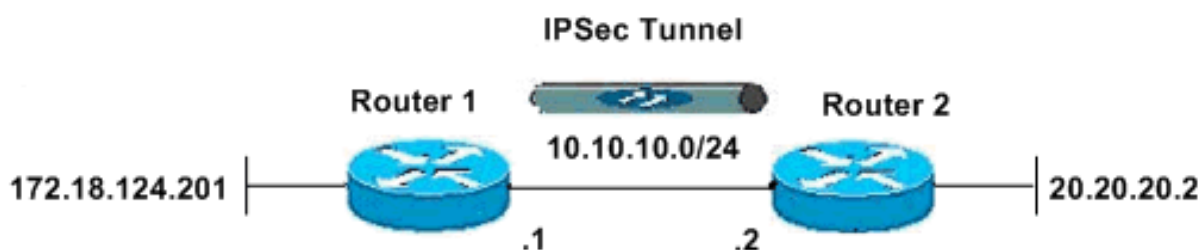
Configurazione

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

Il documento usa la seguente configurazione di rete:



Configurazioni

In questo documento vengono usate le seguenti configurazioni:

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

```
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 !--- ac  
  
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
```

```
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 !--- ac

```
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
```

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 crypto map: verifica la configurazione sul router.

Questo output viene generato dal router 1.

```
<#root>

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
```

Risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per risolvere i problemi di configurazione.

Comandi per la risoluzione dei problemi

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

Nota: prima di usare i comandi di debug, consultare le [informazioni importanti sui comandi di debug](#).

Debug di ISAMP e IPsec

- show debugging: visualizza informazioni sui tipi di debug abilitati per il router.

```
<#root>

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_MSG_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_MSG_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_MSG_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_MESG_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_MESG_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

```

Comandi show

- show crypto isakmp sa: visualizza la Security Association (SA) di Internet Security Association Protocol (ISAKMP) creata tra peer.

```
<#root>
```

```
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: visualizza l'associazione di protezione IPsec creata tra peer.

```
<#root>
```

```
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 pcp 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 pcp 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: B84COCD6 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: B84COCD6 B0BCFFC3 67432FCF F809B638
IV size: 0 bytes
replay detection support: Y
```

outbound ah sas:

outbound pcg sas:

Limitazioni del set di trasformazioni con sigillo esp

Esistono tre limiti per l'uso del set di trasformazioni esp-seal:

- Il set di trasformazioni esp-seal può essere utilizzato solo se non sono presenti acceleratori di crittografia. Questa limitazione è presente perché nessun acceleratore di crittografia corrente implementa il set di trasformazioni della crittografia SEAL e, se è presente un acceleratore di crittografia, gestirà tutte le connessioni IPsec negoziate con IKE. Se è presente un acceleratore di crittografia, il software Cisco IOS consentirà di configurare il set di trasformazioni, ma avvertirà che non verrà utilizzato finché l'acceleratore di crittografia è

abilitato.

- Il set di trasformazioni esp-seal può essere utilizzato solo insieme a un set di trasformazioni di autenticazione, ovvero uno dei seguenti: esp-md5-hmac, esp-sha-hmac, ah-md5-hmac o ah-sha-hmac. Questa limitazione è presente perché la crittografia SEAL è particolarmente debole quando si tratta di proteggere contro le modifiche del pacchetto crittografato. Pertanto, per evitare tale debolezza, è necessario un set di trasformazioni di autenticazione (i set di trasformazioni di autenticazione sono progettati per sventare tali attacchi). Se si tenta di configurare un set di trasformazioni IPSec utilizzando SEAL senza un set di trasformazioni di autenticazione, verrà generato un errore e il set di trasformazioni verrà rifiutato.
- Il set di trasformazioni esp-seal non può essere utilizzato con una mappa crittografica digitata manualmente. Questa limitazione è presente perché una configurazione di questo tipo riutilizzerebbe lo stesso flusso di chiave per ogni riavvio, compromettendo la sicurezza. A causa del problema di sicurezza, una configurazione di questo tipo è vietata. Se si tenta di configurare una mappa crittografica con chiave manuale con un set di trasformazioni basato su SEAL, viene generato un errore e il set di trasformazioni viene rifiutato.

Informazioni correlate

- [Pagina di supporto per IPSec](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).