

# Túnel de site para site entre IOS Router usando a configuração de exemplo do SELO

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[As limitações com ESP-selo transformam o grupo](#)

[Informações Relacionadas](#)

## [Introdução](#)

O algoritmo de criptografia de software (SEAL) é um algoritmo alternativo à criptografia padrão de dados (DES), ao DES triplo (3DES) e ao padrão de criptografia avançada (AES). SELE a criptografia usa uma chave de criptografia do 160-bit e tem um impacto mais baixo ao CPU quando comparado a outros algoritmos com base no software. Este documento ilustra como configurar um túnel de IPsec do LAN para LAN (site para site) usando o SELO.

## [Pré-requisitos](#)

### [Requisitos](#)

Não existem requisitos específicos para este documento.

### [Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 7200 Series Router que executam o Software Release 12.3(7)T de Cisco IOS®

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Convenções

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

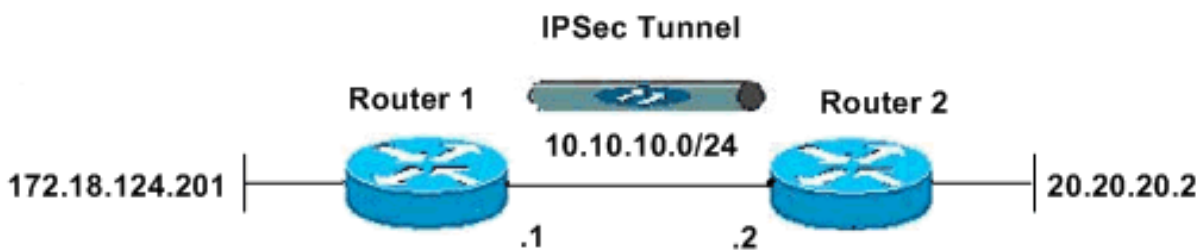
## Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

**Note:** Use a ferramenta [Command Lookup Tool](#) ([apenas para clientes registrados](#)) para obter mais informações sobre os comandos usados neste documento.

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



## Configurações

Este documento utiliza as seguintes configurações:

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

### **Roteador 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

```

## Roteador 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
```

## Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A [Output Interpreter Tool \(somente clientes registrados\)](#) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- **crypto map da mostra** — Verifica a configuração no roteador. Esta saída é tomada do roteador1.

```
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

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

### Comandos para Troubleshooting

A [Output Interpreter Tool \(somente clientes registrados\)](#) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

**Note:** [Antes de emitir comandos de depuração, consulte as informações importantes sobre eles.](#)

## O ISAMP e o IPsec debugam

- **eliminação de erros da mostra** — Indica a informação sobre os tipos de eliminação de erros que são permitidos para seu roteador.

```
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_MESG_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_MSG_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_MSG_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_MSG_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

```

## comandos show

- **show crypto isakmp sa** – Mostra a estrutura Internet Security Association Management Protocol (ISAKMP) Security Association (SA) construída entre correspondentes.

```

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** - Mostra o SA de IPSec criado entre os correspondentes.

```

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: B84C0CD6 B0BCFFC3 67432FCF F809B638  
IV size: 0 bytes  
replay detection support: Y

inbound ah sas:

inbound pcp 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:

## As limitações com ESP-selo transformam o grupo

Há três limitações no uso do ESP-selo transformam o grupo:

- O **esp-selo** transformam o grupo pode ser usado somente se nenhum acelerador de criptografia esta presente. Esta limitação esta presente porque nenhum acelerador de criptografia atual executa o SELO que a criptografia transformam o grupo, e se um acelerador de criptografia esta presente, segurar todas as conexões IPsec que são negociadas com o IKE. Se um acelerador de criptografia esta presente, o Cisco IOS Software permitirá que a transformação ajuste-se para ser configurada, mas advertirá que não estará usado enquanto o acelerador de criptografia é permitido.
- O **esp-selo** transformam o grupo pode ser usado somente conjuntamente com uma autenticação transformam o grupo, a saber um destes: **esp-md5-hmac**, **esp-sha-hmac**, **ah-md5-hmac**, ou **Ah-sha-hmac**. Esta limitação esta presente porque a criptografia do SELO é especialmente fraca quando se trata da proteção contra alterações do pacote criptografado. Conseqüentemente, para impedir tal fraqueza, uma autenticação transformam o grupo é exigida (a autenticação transformam grupos é projetada foil tais ataques.). Se você tenta configurar um IPsec transforme o grupo que usa o SELO sem uma autenticação transformam o grupo, um erro é gerado, e o grupo da transformação é rejeitado.
- O **esp-selo** transformam o grupo não pode ser usado com um crypto map manualmente fechado. Esta limitação esta presente porque tal configuração reutilizaria a mesma sequência de chave para cada repartição, que comprometeria a Segurança. Devido à questão de segurança, tal configuração é proibida. Se você tenta configurar um crypto map manualmente fechado com Selo-baseado transforme o grupo, um erro é gerado, e o grupo da transformação é rejeitado.

## Informações Relacionadas

- [Página de suporte do IPsec](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)