

# SEAL を使用している IOS ルータ間のサイトツーサイト トンネルの構成例

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[esp-seal トランスフォーム セットの制限](#)

[関連情報](#)

## 概要

ソフトウェア暗号化アルゴリズム ( SEAL ) は、データ暗号規格 ( DES )、トリプル DES ( 3DES )、および高度暗号化規格 ( AES ) の代替りとなるアルゴリズムです。 SEAL 暗号化では、160 ビットの暗号キーが使用され、他のソフトウェアベースのアルゴリズムに比べて、CPU に与える影響は小さくなります。このドキュメントでは、SEAL を使用して LAN 間 ( サイト間 ) に IPsec トンネルを設定する方法について説明します。

## 前提条件

### 要件

このドキュメントに関する固有の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS® ソフトウェア リリース 12.3(7)T が稼働する Cisco 7200 シリーズ ルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな ( デフォルト ) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

## 表記法

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

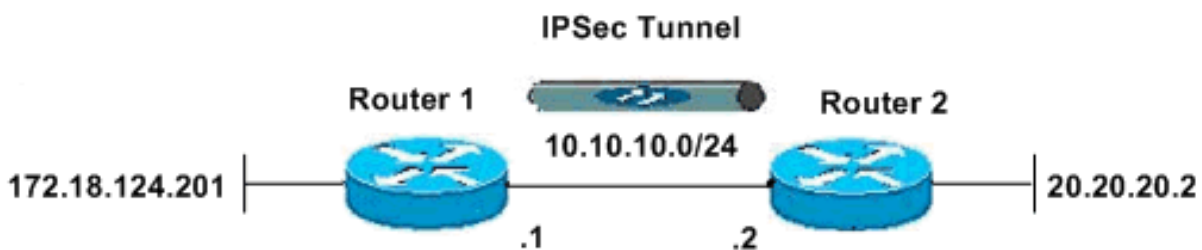
## 設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ( [登録ユーザ専用](#) ) を使用してください。

## ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



## 設定

このドキュメントでは、次の設定を使用します。

- [ルータ 1](#)
- [ルータ 2](#)

```
ルータ 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

```

## ルータ 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
```

## 確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供しています。

特定の **show** コマンドは、[Output Interpreter Tool](#) ( [登録ユーザ専用](#) ) によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

- **show crypto map** : ルータ上の設定を検証します。これはルータ 1 からの出力です。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

## トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

### トラブルシューティングのためのコマンド

特定の **show** コマンドは、[Output Interpreter Tool](#) ( [登録ユーザ専用](#) ) によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

注: **debug** コマンドを使用する前に、[『debug コマンドの重要な情報』](#)を参照してください。

### ISAMP および IPSec のデバッグ

- **show debugging** : ルータで有効にされているデバッグのタイプに関する情報を表示します。

```
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\_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\_MSG\_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\_MSG\_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\_MSG\_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, keysizes= 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, keysizes= 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(mtree_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
```

## [show コマンド](#)

- **show crypto isakmp sa** : ピア間で構築された Internet Security Association Management Protocol ( ISAKMP ) セキュリティ アソシエーション ( SA ) を表示します。 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** : ピア間に確立された IPSec SA を表示します。 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:

## [esp-seal トランスフォーム セットの制限](#)

esp-seal トランスフォーム セットの使用には次の 3 つの制限事項があります。

- esp-seal トランスフォーム セットは、crypto アクセラレータが存在しない場合にのみ使用可能です。この制限が適用される理由は、現在の crypto アクセラレータが SEAL 暗号化トランスフォーム セットを実装していないためです ( crypto アクセラレータが存在する場合、IKE との間でネゴシエートされるすべての IPSec 接続がこれによって処理されます )。crypto アクセラレータが存在する場合、Cisco IOS ソフトウェアではこのトランスフォーム セットを設定できますが、crypto アクセラレータが有効である限りこれが使用されないという警告が表示されます。
- esp-seal トランスフォーム セットは、次のいずれかの認証トランスフォーム セットと併用する場合にのみ使用可能です : **esp-md5-hmac**、**esp-sha-hmac**、**ah-md5-hmac**、**ah-sha-hmac**。この制限が適用される理由は、暗号化パケットの変更に対する防御の点で SEAL 暗号化が特に脆弱であるためです。したがって、このような脆弱性を防ぐために認証トランスフォーム セットが必要です ( 認証トランスフォーム セットは、このような攻撃を防ぐように設計されています )。認証トランスフォーム セットなしで SEAL を使用して IPSec トランスフォーム セットを設定しようとすると、エラーが生成され、トランスフォーム セットは拒否されます。
- 手動でキー設定した暗号マップとともに **esp-seal** トランスフォーム セットを使用することはできません。この制限が適用される理由は、このような設定の場合、再起動のたびに同じキーストリームが再利用されるため、セキュリティが侵害される可能性があることです。セキュリティ上の問題により、このような設定は禁止されています。SEAL ベースのトランスフォーム セットとともに、手動でキー設定した暗号マップを設定しようとすると、エラーが生成され、トランスフォーム セットは拒否されます。

## [関連情報](#)

- [IPSec に関するサポート ページ](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)