目次

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）の代わりとなるアルゴリズムです。 SEAL 暗号化は他のソフトウェアベースのアルゴリズムと比較されたとき 160-bit 暗号化キーを使用し、CPU により低い影響があります。 この資料に SEAL を使用して LAN-to-LAN な（サイト間の）IPSecトンネルを設定する方法を説明されています。

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 を実行する 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。

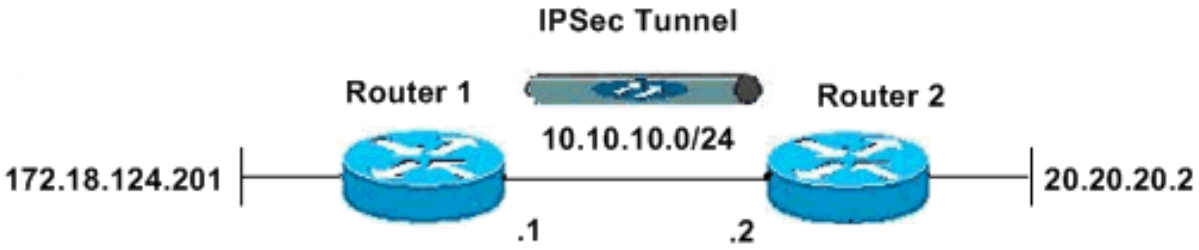
設定

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
ルータ 2

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** か。ルータの設定を確認します。この出力はルータ 1.から奪取 されます。

```
R1#show crypto mapCrypto Map "cisco" 10 ipsec-isakmpPeer = 10.10.10.2Extended IP access list
100access-list 100 permit ip 172.18.124.0 0.0.0.255 20.20.20.0 0.0.0.255Current peer:
10.10.10.2Security association lifetime: 4608000 kilobytes/3600 secondsPFS (Y/N): NTransform
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 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 デバッグ

- **show debugging** か。ルータのために有効に なる デバッグの種類についての情報を表示する。

```
R1#show debuggingCryptographic Subsystem:Crypto ISAKMP debugging is onCrypto 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 payloadnext-payload : 8type : 1address : 10.10.10.2protocol : 17port : 500length : 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 1spi 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 payloadnext-payload : 8type : 1address : 10.10.10.1protocol : 17port : 500length : 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 SAfrom 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(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_MESG_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** か。同位の間で構築される Internet Security Association Management Protocol （ ISAKMP ） Security Association （ SA ）を示します。R1#**show crypto isakmp sa**dst src state conn-id slot10.10.10.1 10.10.10.2 QM_IDLE 1 0R2#**show crypto isakmp sa**dst src state conn-id slot10.10.10.1 10.10.10.2 QM_IDLE 1 0
- **show crypto ipsec sa** か。同位の間で構築される IPSec SA 示します。R1#**show crypto ipsec sa**interface: Ethernet1/0Crypto map tag: cisco, local addr. 10.10.10.1protected 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: 10.10.10.2:500PERMIT, 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 0local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.2path mtu 1500, media mtu 1500current outbound spi: 7259AADDinbound 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: ciscocrypto engine type: Software, engine_id: 1sa timing: remaining key lifetime (k/sec): (4565513/3382)ike_cookies: 67432FCF F809B638 B84C0CD6 B0BCFFC3IV size: 0 bytesreplay detection support: Yinbound 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: ciscocrypto engine type: Software, engine_id: 1sa timing: remaining key lifetime (k/sec): (4565518/3382)ike_cookies: 67432FCF F809B638 B84C0CD6 B0BCFFC3IV size: 0 bytesreplay detection support: Youtbound ah sas:outbound pcp sas:R1# R2#**show crypto ipsec sa**interface: Ethernet0/0Crypto map tag: cisco, local addr. 10.10.10.2protected 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: 10.10.10.1:500PERMIT, 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 0local crypto endpt.: 10.10.10.2, remote crypto endpt.: 10.10.10.1path mtu 1500, media mtu 1500current outbound spi: DD3645C8inbound 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: ciscocrypto engine type: Software, engine_id: 1sa timing: remaining key lifetime (k/sec): (4536995/3410)ike_cookies: B84C0CD6 B0BCFFC3 67432FCF F809B638IV size: 0 bytesreplay detection support: Yinbound 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: ciscocrypto engine type:
Software, engine_id: 1sa timing: remaining key lifetime (k/sec): (4537000/3409)ike_cookies:
B84C0CD6 B0BCFFC3 67432FCF F809B638IV size: 0 bytesreplay detection support: Youtbound ah
sas:outbound pcp sas:
```

設定 される特別シール トランスフォームの制限

設定 される特別**シール** トランスフォームの使用の 3 つの制限あります:

- 設定 される特別**シール** トランスフォームは暗号アクセラレータがないときだけ使用することができます。 この制限は暗号アクセラレータがあれば現在の暗号アクセラレータが設定 される SEAL 暗号化 トランスフォームを設定しない、IKE とネゴシエートされるすべての IPSec接続を処理しますのであり。 暗号アクセラレータがある場合、Cisco IOSソフトウェアは設定されるために設定 された トランスフォームを可能にしますが暗号アクセラレータが有効に なる限り使用されないことを警告します。
- 設定 される特別**シール** トランスフォームは設定 される 認証 トランスフォームと共にだけこれらの即ち 1 使用することができます: **esp-md5-hmac、esp-sha-hmac、ah-md5-hmac、または ah-sha-hmac。** この制限は SEAL 暗号化が暗号化されたパケットの修正に対して保護に関しては特に弱いのであります。 従って、そのような脆弱性を防ぐために、設定 される 認証 トランスフォームが必要となります (そのような不正侵入を失敗させるように認証 トランスフォーム セットは。設計されています)。 設定 される 認証 トランスフォームなしで SEAL を使用して設定 される IPSec トランスフォームを設定するように試みる場合エラーは生成され、設定 される トランスフォームは拒否されます。
- 設定 される特別**シール** トランスフォームは手作業キーによる な クリプト マップと使用することができません。 この制限はそのような設定がセキュリティを危殆化する各再度ブートするのための同じ keystream を再使用するのであります。 セキュリティ上の問題が理由で、そのような設定は禁止されています。 設定 されるシール ベースのトランスフォームで手作業キーによる な クリプト マップを設定するように試みる場合エラーは生成され、設定 されるトランスフォームは拒否されます。

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