SEAL 샘플 컨피그레이션을 사용하여 IOS 라우터 간 사이트 대 사이트 터널

목차

소개

SEAL(Software Encryption Algorithm)은 DES(Data Encryption Standard), 3DES(Triple DES) 및 AES(Advanced Encryption Standard)의 대체 알고리즘입니다.SEAL 암호화는 160비트 암호화 키를 사용하며 다른 소프트웨어 기반 알고리즘에 비해 CPU에 미치는 영향이 낮습니다.이 문서에서는 SEAL을 사용하여 LAN-to-LAN(Site-to-Site) IPSec 터널을 구성하는 방법을 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® Software 릴리스 12.3(7)T를 실행하는 Cisco 7200 Series 라우터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 표기 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

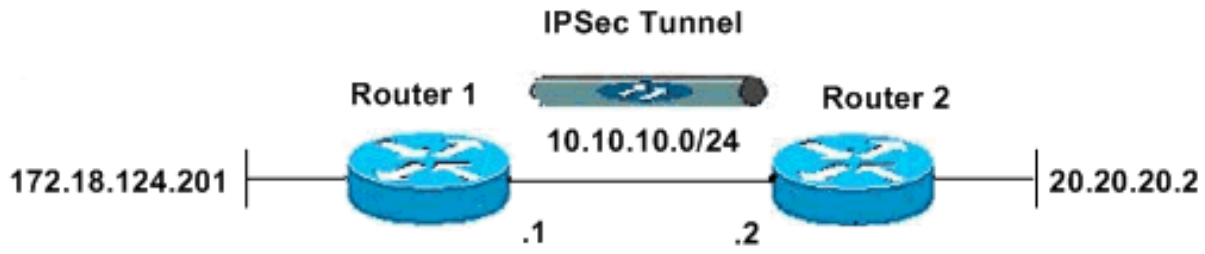
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 문서에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

이 문서에서는 다음 구성을 사용합니다.

- 라우터 1
- 라우터 2

라우터 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
```

라우터 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
```

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

- **show crypto map** - 라우터의 컨피그레이션을 확인합니다.이 출력은 라우터 1에서 가져옵니다.

```
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
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 명령

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

참고: debug 명령을 실행하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

ISAMP 및 IPSec 디버깅

- **show debugging** - 라우터에 대해 활성화된 디버깅 유형에 대한 정보를 표시합니다.

```
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_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(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 명령

- **show crypto isakmp sa** - 피어 간에 구축된 ISAKMP(Internet Security Association Management Protocol) SA(Security Association)를 표시합니다.

```
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** - 피어 간에 구축된 IPSec SA를 표시합니다.

```
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 변환 세트의 제한 사항

esp-seal 변형 집합의 사용에는 세 가지 제한 사항이 있습니다.

- esp-**seal** 변환 세트는 암호화 가속기가 없는 경우에만 사용할 수 있습니다.현재 암호화 가속기는 SEAL 암호화 변형 집합을 구현하지 않으므로 이 제한이 있으며, 암호화 가속기가 있는 경우 IKE와 협상되는 모든 IPSec 연결을 처리합니다.암호화 가속기가 있는 경우 Cisco IOS 소프트웨어는 변형 집합을 구성할 수 있지만 암호화 가속기가 활성화된 한 사용하지 않을 것임을 경고합니다.
- esp-**seal** 변형 집합은 인증 변형 집합(예: 다음 중 하나)과 함께만 사용할 수 있습니다.**esp-md5-hmac, esp-sha-hmac, ah-md5-hmac** 또는 **ah-sha-hmac**.SEAL 암호화는 암호화된 패킷의 수정으로부터 보호하기 위해 특히 취약하기 때문에 이 제한이 있습니다.따라서 이러한 약점을 방지하려면 인증 변형 집합이 필요합니다(인증 변형 집합은 이러한 공격을 무력화하도록 설계됨). 인증 변형 집합 없이 SEAL을 사용하여 IPSec 변형 집합을 구성하려고 하면 오류가 생성되고 변형 집합이 거부됩니다.
- esp-**seal** 변환 세트는 수동으로 키가 지정된 암호화 맵과 함께 사용할 수 없습니다.이러한 컨피그레이션은 각 리부팅에 동일한 키 스트림을 재사용하므로 보안이 손상될 수 있으므로 이러한 제한이 있습니다.보안 문제로 인해 이러한 컨피그레이션이 금지됩니다.SEAL 기반 변형 집합을 사용하여 수동으로 키가 지정된 암호화 맵을 구성하려고 하면 오류가 생성되고 변형 집합이 거부됩니다.

관련 정보

- IPSec 지원 페이지
- 기술 지원 및 문서 – Cisco Systems