ASA IPsec および IKE デバッグ（IKEv1 メインモード）のトラブルシューティング テクニカル ノート

内容

概要

このドキュメントでは、メイン モードと事前共有キー（PSK）の両方を使用する場合の適応型セキュリティ アプライアンス（ASA）でのデバッグについて説明します。設定への特定のデバッグ行の変換についても説明します。

このドキュメントで説明しないトピックには、トンネル確立後の通過トラフィック、および IPsec またはインターネット キー交換（IKE）の基本概念が含まれます。

前提条件

要件

このドキュメントの読者は次のトピックについて理解している必要があります。

- PSK
- IKE

使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づいています。

- Cisco ASA 9.3.2
- Cisco IOS® 12.4T で稼働するルータ

主な問題

IKE および IPsec のデバッグはわかりにくいことがありますが、これらのデバッグを使用して、IPsec VPN トンネル確立の問題が発生している場所を理解できます。

シナリオ

メイン モードは通常、LAN-to-LAN トンネル間に使用されるか、リモート アクセス (EzVPN) の場合は認証に証明書を使用するときに使用されます。

デバッグは、ソフトウェアバージョン9.3.2が稼働する2つのASAから行われます。2つのデバイスはLAN-to-LANトンネルを形成します。

説明する主なシナリオは、次の 2 つです。

- IKE の発信側としての ASA
- IKE の応答側としての ASA

使用する debug コマンド

debug crypto ikev1 127

debug crypto ipsec 127

ASA の設定

IPsec の設定：

```
crypto ipsec transform-set TRANSFORM esp-aes esp-sha-hmac
crypto map MAP 10 match address VPN
crypto map MAP 10 set peer 10.0.0.2
crypto map MAP 10 set transform-set TRANSFORM
crypto map MAP 10 set reverse-route
crypto map MAP interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
tunnel-group 10.0.0.2 type ipsec-l2l
tunnel-group 10.0.0.2 ipsec-attributes
 pre-shared-key cisco
access-list VPN extended permit tcp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
access-list VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
```

IP 設定：

```
ciscoasa#

show ip
```

```
System IP Addresses:
Interface                  Name      IP address      Subnet mask      Method
GigabitEthernet0/0       inside     192.168.1.1     255.255.255.0   manual
GigabitEthernet0/1       outside   10.0.0.1          255.255.255.0   manual
Current IP Addresses:
Interface                  Name       IP address      Subnet mask      Method
GigabitEthernet0/0       inside     192.168.1.1    255.255.255.0   manual
GigabitEthernet0/1       outside   10.0.0.1          255.255.255.0   manual
```

NAT の設定

```
object network INSIDE-RANGE
 subnet 192.168.1.0 255.255.255.0 object network FOREIGN_NETWORK
 subnet 192.168.2.0 255.255.255
nat (inside,outside) source static INSIDE-RANGE INSIDE-RANGE destination static
FOREIGN_NETWORK FOREIGN_NETWORK no-proxy-arp route-lookup
```

デバッグ

MM_NO_STATE ASA	[IKEv1 DEBUG]:Pitcher:received a key acquire message, spi 0x0 IPSEC(crypto_map_check)-3:Looking for crypto map matching 5-tuple:Prot=1, saddr=192.168.1.2, sport=2816, daddr=192.168.2.1, dport=2816 IPSEC(crypto_map_check)-3:Checking crypto map MAP 10:matched. [IKEv1]:IP = 10.0.0.2, IKE Initiator:New Phase 1, Intf inside, IKE Peer 10.0.0.2 local Proxy Address 192.168.1.0, remote Proxy Address 192.168.2.0, Crypto map (MAP) [IKEv1 DEBUG]:IP = 10.0.0.2, constructing **ISAKMP SA payload** **[IKEv1 DEBUG]:**IP = 10.0.0.2, constructing NAT-Traversal VID ver 02 payload [IKEv1 DEBUG]:IP = 10.0.0.2, constructing NAT-Traversal VID ver 03 payload [IKEv1 DEBUG]:IP = 10.0.0.2, constructing NAT-Traversal VID ver RFC payload [IKEv1 DEBUG]:IP = 10.0.0.2, constructing Fragmentation VID + extended capabilities payload
MM1 ncludes iIKEsNAT-T	
MM1	[IKEv1]:IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=0) with payloads :HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length :168

==========MM1==========
====>

[IKEv1]:IP = 10.0.0.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads :HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0)164	MM1
[IKEv1 DEBUG]:IP = 10.0.0.2, processing SA payload	MM1
[IKEv1 DEBUG]:IP = 10.0.0.2, Oakley proposal is acceptable	ISAKMP/IKE
[IKEv1 DEBUG]:IP = 10.0.0.2, processing VID payload	NAT-T
[IKEv1 DEBUG]:IP = 10.0.0.2, Received NAT-Traversal RFC VID	
[IKEv1 DEBUG]:IP = 10.0.0.2, processing VID payload	*crypto isakmp policy*
[IKEv1 DEBUG]:IP = 10.0.0.2, processing VID payload	*10*
[IKEv1 DEBUG]:IP = 10.0.0.2, Received NAT-Traversal ver 03 VID	*authentication pre-*
[IKEv1 DEBUG]:IP = 10.0.0.2, processing VID payload	*share*
[IKEv1 DEBUG]:IP = 10.0.0.2, Received NAT-Traversal ver 02 VID	*encryption 3des*
[IKEv1 DEBUG]:IP = 10.0.0.2, processing IKE SA payload	*hash sha*
[IKEv1 DEBUG]:IP = 10.0.0.2, IKE SA Proposal # 1, Transform # 1 acceptable Matches global IKE entry # 2	*group 2* *lifetime 86400*
[IKEv1 DEBUG]:IP = 10.0.0.2, constructing ISAKMP SA payload	
[IKEv1 DEBUG]:IP = 10.0.0.2, constructing NAT-Traversal VID ver 02 payload	MM2 isakmp NAT-T
[IKEv1 DEBUG]:IP = 10.0.0.2, constructing Fragmentation VID + extended capabilities payload	

[IKEv1]:IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=0) with payloads :HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE(0) total length :128 MM2

<=========================MM2==========================
=====

MM2

[IKEv1]:IP = 10.0.0.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads :HDR + SA (1) + VENDOR (13) + NONE (0) total length :104

[IKEv1 DEBUG]:IP = 10.0.0.2, processing SA payload

MM2

[IKEv1 DEBUG]:IP = 10.0.0.2, Oakley proposal is acceptable

[IKEv1 DEBUG]:IP = 10.0.0.2, processing VID payload

[IKEv1 DEBUG]:IP = 10.0.0.2, Received NAT-Traversal RFC VID

Nov 30 10:38:29 [IKEv1 DEBUG]:IP = 10.0.0.2, constructing ke payload

Nov 30 10:38:29 [IKEv1 DEBUG]:IP = 10.0.0.2, constructing nonce payload

Nov 30 10:38:29 [IKEv1 DEBUG]:IP = 10.0.0.2, constructing Cisco Unity VID payload

Nov 30 10:38:29 [IKEv1 DEBUG]:IP = 10.0.0.2, constructing xauth V6 VID payload

Nov 30 10:38:29 [IKEv1 DEBUG]:IP = 10.0.0.2, Send IOS VID

Nov 30 10:38:29 [IKEv1 DEBUG]:IP = 10.0.0.2, Constructing ASA spoofing IOS Vendor ID payload (version:1.0.0, capabilities:20000001)

MM3
ncludesNAT -
Hellman(DH)(KE)
(i)nitatorgpA) DPD

Nov 30 10:38:29 [IKEv1 DEBUG]:IP = 10.0.0.2, constructing VID payload

Nov 30 10:38:29 [IKEv1 DEBUG]:IP = 10.0.0.2, Send Altiga/Cisco VPN3000/Cisco ASA GW VID

Nov 30 10:38:29 [IKEv1 DEBUG]:IP = 10.0.0.2, constructing NAT-Discovery payload

Nov 30 10:38:29 [IKEv1 DEBUG]:IP = 10.0.0.2, computing NAT Discovery hash

Nov 30 10:38:29 [IKEv1 DEBUG]:IP = 10.0.0.2, constructing NAT-Discovery payload

Nov 30 10:38:29 [IKEv1 DEBUG]:IP = 10.0.0.2, computing NAT Discovery hash

MM3

[IKEv1]:IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=0) with payloads :HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length :304

==========================MM3==================
====>

[IKEv1]:IP = 10.0.0.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads :HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length :284 MM3

[IKEv1 DEBUG]:IP = 10.0.0.2, processing ke payload

[IKEv1 DEBUG]:IP = 10.0.0.2, processing ISA_KE payload

[IKEv1 DEBUG]:IP = 10.0.0.2, processing nonce payload

[IKEv1 DEBUG]:IP = 10.0.0.2, processing VID payload

[IKEv1 DEBUG]:IP = 10.0.0.2, Received DPD VID

[IKEv1 DEBUG]:IP = 10.0.0.2, processing VID payload MM3

[IKEv1 DEBUG]:IP = 10.0.0.2, Processing IOS/PIX Vendor ID payload NAT-D NAT NAT (version:1.0.0, capabilities:00000f6f) DH KE pg A

[IKEv1 DEBUG]:IP = 10.0.0.2, processing VID payload

[IKEv1 DEBUG]:IP = 10.0.0.2, Received xauth V6 VID

[IKEv1 DEBUG]:IP = 10.0.0.2, processing NAT-Discovery payload

[IKEv1 DEBUG]:IP = 10.0.0.2, computing NAT Discovery hash

[IKEv1 DEBUG]:IP = 10.0.0.2, processing NAT-Discovery payload

[IKEv1 DEBUG]:IP = 10.0.0.2, computing NAT Discovery hash

[IKEv1 DEBUG]:IP = 10.0.0.2, constructing ke payload

[IKEv1 DEBUG]:IP = 10.0.0.2, constructing nonce payload MM4

[IKEv1 DEBUG]:IP = 10.0.0.2, constructing Cisco Unity VID payload ncludes NAT , DH KE

[IKEv1 DEBUG]:IP = 10.0.0.2, constructing xauth V6 VID payload responderBsB DPD

[IKEv1 DEBUG]:IP = 10.0.0.2, Send IOS VID VID

[IKEv1 DEBUG]:IP = 10.0.0.2, Constructing ASA spoofing IOS Vendor ID payload (version:1.0.0, capabilities:20000001)

[IKEv1 DEBUG]:IP = 10.0.0.2, constructing VID payload
[IKEv1 DEBUG]:IP = 10.0.0.2, Send Altiga/Cisco VPN3000/Cisco ASA GW VID
[IKEv1 DEBUG]:IP = 10.0.0.2, constructing NAT-Discovery payload
[IKEv1 DEBUG]:IP = 10.0.0.2, computing NAT Discovery hash
[IKEv1 DEBUG]:IP = 10.0.0.2, constructing NAT-Discovery payload
[IKEv1 DEBUG]:IP = 10.0.0.2, computing NAT Discovery hash
[IKEv1]:IP = 10.0.0.2, Connection landed on tunnel_group 10.0.0.2
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, Generating keys for Responder…
10.0.0.2 L2L s
[IKEv1]:IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=0) with payloads :HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length :304
MM4
<==========MM4==========
[IKEv1]:IP = 10.0.0.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads :HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length :304
MM4
[IKEv1 DEBUG]:IP = 10.0.0.2, processing ike payload
[IKEv1 DEBUG]:IP = 10.0.0.2, processing ISA_KE payload
[IKEv1 DEBUG]:IP = 10.0.0.2, processing nonce payload
[IKEv1 DEBUG]:IP = 10.0.0.2, processing VID payload
[IKEv1 DEBUG]:IP = 10.0.0.2, Received Cisco Unity client VID
[IKEv1 DEBUG]:IP = 10.0.0.2, processing VID payload
[IKEv1 DEBUG]:IP = 10.0.0.2, Received DPD VID
NAT-D NAT NAT
[IKEv1 DEBUG]:IP = 10.0.0.2, processing VID payload
[IKEv1 DEBUG]:IP = 10.0.0.2, Processing IOS/PIX Vendor ID payload (version:1.0.0, capabilities:00000f7f)
DH KEBs
[IKEv1 DEBUG]:IP = 10.0.0.2, processing VID payload
[IKEv1 DEBUG]:IP = 10.0.0.2, Received xauth V6 VID
[IKEv1 DEBUG]:IP = 10.0.0.2, processing NAT-Discovery payload
[IKEv1 DEBUG]:IP = 10.0.0.2, computing NAT Discovery hash
[IKEv1 DEBUG]:IP = 10.0.0.2, processing NAT-Discovery payload
[IKEv1 DEBUG]:IP = 10.0.0.2, computing NAT Discovery hash
[IKEv1]:IP = 10.0.0.2, Connection landed on tunnel_group 10.0.0.2
10.0.0.2 L2L s
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, Generating keys for Initiator...
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, constructing ID payload
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, constructing hash payload
MM5
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, Computing hash for ISAKMP
crypto isakmp identity auto
[IKEv1 DEBUG]:IP = 10.0.0.2, Constructing IOS keep alive payload:proposal=32767/32767 sec.
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, constructing dpd vid payload
[IKEv1]:IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=0) with payloads :HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) +VENDOR (13) + NONE (0) total length :96
MM5
==========MM5==========>
[IKEv1]:Group = 10.0.0.2, IP = 10.0.0.2, Automatic NAT Detection Status:Remote end is NOT behind a NAT device This end is NOT behind a NAT device
NAT NAT-T
[IKEv1]:IP = 10.0.0.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads :HDR + ID (5) + HASH (8) + NONE (0) total length :64
MM5 ncludes rID(ID)c
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, processing ID payload
MM5

[IKEv1 DECODE]:Group = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR ID received
10.0.0.2
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, processing hash payload
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, Computing hash for ISAKMP
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, processing notify payload
[IKEv1]:Group = 10.0.0.2, IP = 10.0.0.2,Automatic NAT
[IKEv1]:IP = 10.0.0.2, Connection landed on tunnel_group 10.0.0.2
Detection Status:Remote end is NOT behind a NAT device This end is NOT behind a NAT device
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, constructing ID payload
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, constructing hash payload
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, Computing hash for ISAKMP
[IKEv1 DEBUG]:IP = 10.0.0.2, Constructing IOS keep alive payload:proposal=32767/32767 sec.
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, constructing dpd vid payload
[IKEv1]:IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=0) with payloads :HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) +VENDOR (13) + NONE (0) total length :96
<==========MM6==========
=====

2

tunnel group 10.0.0.2 type ipsec-l2l

No NAT-T

MM6
ID
ID

MM6

1
isakmp

crypto isakmp policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
ciscoasa# sh run all
crypto isakmp
crypto isakmp identity auto

[IKEv1]:IP = 10.0.0.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads :HDR + ID (5) + HASH (8) + NONE (0) total length :64

[IKEv1]:Group = 10.0.0.2, IP = 10.0.0.2, PHASE 1 COMPLETED
[IKEv1]:IP = 10.0.0.2, Keep-alive type for this connection:DPD
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, Starting P1 rekey timer:64800 seconds.

MM6
ncludes rfID

[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, processing ID payload
[IKEv1 DECODE]:Group = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR ID received
10.0.0.2
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, processing hash payload
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, Computing hash for ISAKMP
[IKEv1]:IP = 10.0.0.2, Connection landed on tunnel_group 10.0.0.2
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, Oakley begin quick mode
[IKEv1 DECODE]:Group = 10.0.0.2, IP = 10.0.0.2, IKE Initiator starting QM:msg id = 7b80c2b0

1
ISAKMP
c
tunnel group 10.0.0.2
type ipsec-l2l
tunnel group 10.0.0.2
ipsec-attributes
pre-shared-key cisco

[IKEv1]:Group = 10.0.0.2, IP = 10.0.0.2, PHASE 1 COMPLETED
[IKEv1]:IP = 10.0.0.2, Keep-alive type for this connection:DPD
DPD has bee negotiated and Phase 1 is now complete.
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, Starting P1 rekey timer:82080

2

IPSECNew embryonic SA created @ 0x53FC3C00,
SCB:0x53F90A00,
[Direction]inbound
SPI:0xFD2D851F

Session ID:0x00006000
VPIF num:0x00000003
Tunnel type:l2l
:esp
Lifetime240
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, IKE got SPI from key engine:SPI = 0xfd2d851f
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, oakley constucting quick mode
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, constructing blank hash payload
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, constructing IPSec SA payload
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, constructing IPSec nonce payload
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, constructing proxy ID
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, Transmitting Proxy Id:
Local subnet:192.168.1.0 mask 255.255.255.0 Protocol 1 Port 0
Remote subnet:192.168.2.0 Mask 255.255.255.0 Protocol 1 Port 0
The local subnet (192.168.1.0/24) and expcted remote subnet (192.168.2.0/24) are being sent
[IKEv1 DECODE]:Group = 10.0.0.2, IP = 10.0.0.2, IKE Initiator sending Initial Contact
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, constructing qm hash payload
[IKEv1 DECODE]:Group = 10.0.0.2, IP = 10.0.0.2, IKE Initiator sending 1st QM pkt:msg id = 7b80c2b0
[IKEv1]:IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=7b80c2b0) with payloads :HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length :200
==========QM1==========>

QM1
IDIP .

crypto ipsec transform-set TRANSFORM esp-aes esp-sha-hmac
access-list VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0

QM1

[IKEv1 DECODE]:IP = 10.0.0.2, IKE Responder starting QM: msg id = 52481cf5
[IKEv1]:IP = 10.0.0.2, IKE_DECODE RECEIVED Message (msgid=52481cf5) with payloads :HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length :172

QM1
2QM

QM1
IP
crypto ipsec transform-set TRANSFORM esp-aes esp-sha-hmac
access-list VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
crypto map MAP 10 match address VPN

[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, processing hash payload
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, processing SA payload
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, processing nonce payload
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, processing ID payload
[IKEv1 DECODE]:Group = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID received--192.168.2.0--255.255.255.0[IKEv1]:Group = 10.0.0.2, IP = 10.0.0.2, Received remote IP Proxy Subnet data in ID Payload:Address 192.168.2.0, Mask 255.255.255.0, Protocol 1, Port 0

192.168.2.0/24
192.168.1.0/24

[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, processing ID payload
[IKEv1 DECODE]:Group = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID received--192.168.1.0--255.255.255.0
[IKEv1]:Group = 10.0.0.2, IP = 10.0.0.2, Received local IP Proxy Subnet data in ID Payload:Address 192.168.1.0, Mask 255.255.255.0, Protocol 1, Port 0
[IKEv1]:Group = 10.0.0.2, IP = 10.0.0.2, QM IsRekeyed old sa not found by addr

[IKEv1]:Group = 10.0.0.2, IP = 10.0.0.2, Static Crypto Map check, checking map = MAP, seq = 10...
[IKEv1]:Group = 10.0.0.2, IP = 10.0.0.2, Static Crypto Map check, map MAP, seq = 10 is a successful match
[IKEv1]:Group = 10.0.0.2, IP = 10.0.0.2, IKE Remote Peer configured for crypto map:MAP
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, processing IPSec SA payload
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, IPSec SA Proposal # 1, Transform # 1 acceptable Matches global IPSec SA entry # 10
[IKEv1]:Group = 10.0.0.2, IP = 10.0.0.2, IKE:requesting SPI!
IPSECNew embryonic SA created @ 0x53FC3698,
SCB:0x53FC2998,
[Direction]inbound
SPI:0x1698CAC7
Session ID:0x00004000
VPIF num:0x00000003
Tunnel type:l2l
:esp
Lifetime240
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, IKE got SPI from key engine:SPI = 0x1698cac7
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, oakley constructing quick mode QM2
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, constructing blank hash ncludes cID ACL payload
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, constructing IPSec SA payload
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, constructing IPSec nonce payload
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, constructing proxy ID
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, Transmitting Proxy Id:
Remote subnet:192.168.2.0 Mask 255.255.255.0 Protocol 1 Port 0
Local subnet:192.168.1.0 mask 255.255.255.0 Protocol 1 Port 0
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, constructing qm hash payload
[IKEv1 DECODE]:Group = 10.0.0.2, IP = 10.0.0.2, IKE Responder sending 2nd QM pkt:msg id = 52481cf5
[IKEv1]:IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=52481cf5) with payloads :HDR + HASH (8) + SA (1) + NONCE QM2
(10) + ID (5) + ID (5) + NONE (0) total length :172
<==========QM2==========
=====
[IKEv1]:IP = 10.0.0.2, IKE_DECODE RECEIVED Message
QM2 (msgid=7b80c2b0) with payloads :HDR + HASH (8) + SA (1) + NONCE
(10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length :200
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, processing hash payload
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, processing SA payload
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, processing nonce payload
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, processing ID payload
[IKEv1 DECODE]:Group = 10.0.0.2, IP = 10.0.0.2,
ID_IPV4_ADDR_SUBNET ID received--192.168.1.0--255.255.255.0
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, processing ID payload
QM2 [IKEv1 DECODE]:Group = 10.0.0.2, IP = 10.0.0.2,
r ID_IPV4_ADDR_SUBNET ID received--192.168.2.0--255.255.255.0
2 [IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, processing notify payload
[IKEv1 DECODE]:Responder Lifetime decode follows (outb
SPI[4]|attributes):
[IKEv1 DECODE]:0000:DDE50931 80010001 00020004 00000E10
...1.....
[IKEv1]:Group = 10.0.0.2, IP = 10.0.0.2, Responder forcing change of IPSec rekeying duration from 28800 to 3600 seconds
based on response from peer, the ASA is changing certain IPSEC attributes.In this case the rekey interval

MAP 10 VPN

SPI 0xfd2d851f 0xdde50931

[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, loading all IPSEC SAs
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, Generating Quick Mode Key!
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, NP encrypt rule look up for crypto map MAP 10 matching ACL VPN:returned cs_id=53f11198;rule=53f11a90
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, Generating Quick Mode Key!
IPSECNew embryonic SA created @ 0x53FC3698,
SCB:0x53F910F0,
[Direction]
SPI:0xDDE50931
Session ID:0x00006000
VPIF num:0x00000003
Tunnel type:l2l
:esp
Lifetime240
IPSECCompleted host OBSA update, SPI 0xDDE50931
IPSECCreating outbound VPN context, SPI 0xDDE50931
Flags:0x00000005
SA:0x53FC3698
SPI:0xDDE50931
MTU :1500 bytes
VCID :0x00000000
0x00000000
SCB:0x01CF218F
0x4C69CB80
IPSECCompleted outbound VPN context, SPI 0xDDE50931
VPN handle:0x000161A4
IPSECNew outbound encrypt rule, SPI 0xDDE50931
Src addr:192.168.1.0
Src mask:255.255.255.0
Dst addr:192.168.2.0
Dst mask:255.255.255.0
Src ports
Upper:0
Lower:0
Op:
Dst ports
Upper:0
Lower:0
Op:
:1
Use protocol:true
SPI:0x00000000
Use SPI:false
IPSECCompleted outbound encrypt rule, SPI 0xDDE50931
Rule ID:0x53FC3AD8
IPSECNew outbound permit rule, SPI 0xDDE50931
Src addr:10.0.0.1
Src mask:255.255.255.255
Dst addr:10.0.0.2
Dst mask:255.255.255.255
Src ports
Upper:0
Lower:0
Op:
Dst ports
Upper:0
Lower:0
Op:
:50
Use protocol:true
SPI:0xDDE50931

Use SPI:true
IPSECCompleted outbound permit rule, SPI 0xDDE50931
Rule ID:0x53F91538
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, NP encrypt rule look up for crypto map MAP 10 matching ACL VPN:returned cs_id=53f11198;rule=53f11a90
[IKEv1]:Group = 10.0.0.2, IP = 10.0.0.2, Security negotiation complete for LAN-to-LAN Group (10.0.0.2) Initiator, Inbound SPI = 0xfd2d851f, Outbound SPI = 0xdde50931
IPSECCompleted host IBSA update, SPI 0xFD2D851F
IPSECCreating inbound VPN context, SPI 0xFD2D851F
Flags:0x00000006
SA:0x53FC3C00
SPI:0xFD2D851F
MTU :0
VCID :0x00000000
0x000161A4
SCB:0x01CEA8EF
0x4C69CB80
IPSECCompleted inbound VPN context, SPI 0xFD2D851F
VPN handle:0x00018BBC
IPSECUpdating outbound VPN context 0x000161A4, SPI 0xDDE50931
Flags:0x00000005
SA:0x53FC3698
SPI:0xDDE50931
MTU :1500 bytes
VCID :0x00000000
0x00018BBC
SCB:0x01CF218F
0x4C69CB80
IPSECCompleted outbound VPN context, SPI 0xDDE50931
VPN handle:0x000161A4
IPSECCompleted outbound inner rule, SPI 0xDDE50931
Rule ID:0x53FC3AD8
IPSECCompleted outbound outer SPD rule, SPI 0xDDE50931
Rule ID:0x53F91538

QM3
Confirm SPI

IPSECNew inbound tunnel flow rule, SPI 0xFD2D851F
Src addr:192.168.2.0
Src mask:255.255.255.0
Dst addr:192.168.1.0
Dst mask:255.255.255.0
Src ports
Upper:0
Lower:0
Op:
Dst ports
Upper:0
Lower:0
Op:
:1
Use protocol:true
SPI:0x00000000
Use SPI:false
IPSECCompleted inbound tunnel flow rule, SPI 0xFD2D851F
Rule ID:0x53F91970
IPSECNew inbound decrypt rule, SPI 0xFD2D851F
Src addr:10.0.0.2
Src mask:255.255.255.255
Dst addr:10.0.0.1
Dst mask:255.255.255.255
Src ports
Upper:0
Lower:0
Op:

Dst ports
Upper:0
Lower:0
Op:
:50
Use protocol:true
SPI:0xFD2D851F
Use SPI:true
IPSECCompleted inbound decrypt rule, SPI 0xFD2D851F
Rule ID:0x53F91A08
IPSECNew inbound permit rule, SPI 0xFD2D851F
Src addr:10.0.0.2
Src mask:255.255.255.255
Dst addr:10.0.0.1
Dst mask:255.255.255.255
Src ports
Upper:0
Lower:0
Op:
Dst ports
Upper:0
Lower:0
Op:
:50
Use protocol:true
SPI:0xFD2D851F
Use SPI:true
IPSECCompleted inbound permit rule, SPI 0xFD2D851F
Rule ID:0x53F91AA0
[IKEv1 DECODE]:Group = 10.0.0.2, IP = 10.0.0.2, IKE Initiator sending 3rd QM pkt:msg id = 7b80c2b0

QM3

==========QM3==========>

[IKEv1]:IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=7b80c2b0) with payloads :HDR + HASH (8) + NONE (0)76
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, IKE got a KEY_ADD msg for SA:SPI = 0xdde50931
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, Pitcher:received KEY_UPDATE, spi 0xfd2d851f
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, Starting P2 rekey timer:3060 seconds.
[IKEv1]:Group = 10.0.0.2, IP = 10.0.0.2, PHASE 2 COMPLETED (msgid=7b80c2b0)

2
SPI

[IKEv1]:IP = 10.0.0.2, IKE_DECODE RECEIVED Message (msgid=52481cf5) with payloads :HDR + HASH (8) + NONE (0) total length :52

QM3

[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, processing hash payload
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, loading all IPSEC SAs
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, Generating Quick Mode Key!
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, NP encrypt rule look up for crypto map MAP 10 matching ACL VPN:returned cs_id=53f11198;rule=53f11a90
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, Generating Quick Mode Key!

QM3
SA

IPSECNew embryonic SA created @ 0x53F18B00, SCB:0x53F8A1C0, [Direction]
SPI:0xDB680406
Session ID:0x00004000
VPIF num:0x00000003
Tunnel type:l2l
:esp
Lifetime240

SPI

IPSECCompleted host OBSA update, SPI 0xDB680406

IPSECCreating outbound VPN context, SPI 0xDB680406
Flags:0x00000005
SA:0x53F18B00
SPI:0xDB680406
MTU :1500 bytes
VCID :0x00000000
0x00000000
SCB:0x005E4849
0x4C69CB80
IPSECCompleted outbound VPN context, SPI 0xDB680406
VPN handle:0x0000E9B4
IPSECNew outbound encrypt rule, SPI 0xDB680406
Src addr:192.168.1.0
Src mask:255.255.255.0
Dst addr:192.168.2.0
Dst mask:255.255.255.0
Src ports
Upper:0
Lower:0
Op:
Dst ports
Upper:0
Lower:0
Op:
:1
Use protocol:true
SPI:0x00000000
Use SPI:false
IPSECCompleted outbound encrypt rule, SPI 0xDB680406
Rule ID:0x53F89160
IPSECNew outbound permit rule, SPI 0xDB680406
Src addr:10.0.0.1
Src mask:255.255.255.255
Dst addr:10.0.0.2
Dst mask:255.255.255.255
Src ports
Upper:0
Lower:0
Op:
Dst ports
Upper:0
Lower:0
Op:
:50
Use protocol:true
SPI:0xDB680406
Use SPI:true
IPSECCompleted outbound permit rule, SPI 0xDB680406
Rule ID:0x53E47E88
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, NP encrypt rule look up for crypto map MAP 10 matching ACL VPN:returned cs_id=53f11198;rule=53f11a90
[IKEv1]:Group = 10.0.0.2, IP = 10.0.0.2, Security negotiation complete for LAN-to-LAN Group (10.0.0.2) Responder, Inbound SPI = 0x1698cac7, Outbound SPI = 0xdb680406
[IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, IKE got a KEY_ADD msg for SA:SPI = 0xdb680406
IPSECCompleted host IBSA update, SPI 0x1698CAC7
IPSECCreating inbound VPN context, SPI 0x1698CAC7 SPI SA
Flags:0x00000006
SA:0x53FC3698
SPI:0x1698CAC7
MTU :0
VCID :0x00000000

0x0000E9B4
SCB:0x005DAE51
0x4C69CB80
IPSECCompleted inbound VPN context, SPI 0x1698CAC7
VPN handle:0x00011A8C
IPSECUpdating outbound VPN context 0x0000E9B4, SPI 0xDB680406
Flags:0x00000005
SA:0x53F18B00
SPI:0xDB680406
MTU :1500 bytes
VCID :0x00000000
0x00011A8C
SCB:0x005E4849
0x4C69CB80
IPSECCompleted outbound VPN context, SPI 0xDB680406
VPN handle:0x0000E9B4
IPSECCompleted outbound inner rule, SPI 0xDB680406
Rule ID:0x53F89160
IPSECCompleted outbound outer SPD rule, SPI 0xDB680406
Rule ID:0x53E47E88
IPSECNew inbound tunnel flow rule, SPI 0x1698CAC7
Src addr:192.168.2.0
Src mask:255.255.255.0
Dst addr:192.168.1.0
Dst mask:255.255.255.0
Src ports
Upper:0
Lower:0
Op:
Dst ports
Upper:0
Lower:0
Op:
:1
Use protocol:true
SPI:0x00000000
Use SPI:false
IPSECCompleted inbound tunnel flow rule, SPI 0x1698CAC7
Rule ID:0x53FC3E80
IPSECNew inbound decrypt rule, SPI 0x1698CAC7
Src addr:10.0.0.2
Src mask:255.255.255.255
Dst addr:10.0.0.1
Dst mask:255.255.255.255
Src ports
Upper:0
Lower:0
Op:
Dst ports
Upper:0
Lower:0
Op:
:50
Use protocol:true
SPI:0x1698CAC7
Use SPI:true
IPSECCompleted inbound decrypt rule, SPI 0x1698CAC7
Rule ID:0x53FC3F18
IPSECNew inbound permit rule, SPI 0x1698CAC7
Src addr:10.0.0.2
Src mask:255.255.255.255
Dst addr:10.0.0.1
Dst mask:255.255.255.255
Src ports

Upper:0 Lower:0 Op: Dst ports Upper:0 Lower:0 Op: :50 Use protocol:true SPI:0x1698CAC7 Use SPI:true IPSECCompleted inbound permit rule, SPI 0x1698CAC7 Rule ID:0x53F8AEA8 [IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, Pitcher:received KEY_UPDATE, spi 0x1698cac7 [IKEv1 DEBUG]:Group = 10.0.0.2, IP = 10.0.0.2, Starting P2 rekey timer:3060 seconds. [IKEv1]:Group = 10.0.0.2, IP = 10.0.0.2, PHASE 2 COMPLETED (msgid=52481cf5)	IPsec	2

トンネルの確認

注：トンネルのトリガーには ICMP が使用されるため、1 つの IPSec SA のみがアップされています（プロトコル 1 = ICMP）。

show crypto ipsec sa

```
interface: outside
  Crypto map tag: MAP, seq num: 10, local addr: 10.0.0.1
   access-list VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
   local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/
```

1

```
/0)
   remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/
```

1

```
/0)
   current_peer: 10.0.0.2
   #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
   #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
   #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
   #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #send errors: 0, #recv errors: 0
   local crypto endpt.: 10.0.0.1/0, remote crypto endpt.: 10.0.0.2/0
   path mtu 1500, ipsec overhead 74, media mtu 1500
   current outbound spi: DB680406
   current inbound spi : 1698CAC7
  inbound esp sas:
   spi: 0x
```

1698CAC7

```
 (379112135)
```

```
      transform: esp-aes esp-sha-hmac no compression
      in use settings ={L2L, Tunnel, }
      slot: 0, conn_id: 16384, crypto-map: MAP
      sa timing: remaining key lifetime (kB/sec): (3914999/3326)
      IV size: 16 bytes
      replay detection support: Y
      Anti replay bitmap:
       0x00000000 0x0000001F
  outbound esp sas:
   spi: 0xDB680406 (3681027078)
      transform: esp-aes esp-sha-hmac no compression
      in use settings ={L2L, Tunnel, }
      slot: 0, conn_id: 16384, crypto-map: MAP
      sa timing: remaining key lifetime (kB/sec): (3914999/3326)
      IV size: 16 bytes
      replay detection support: Y
      Anti replay bitmap:
      0x00000000 0x00000001
```

show crypto isakmp sa

```
  Active SA: 1
   Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 10.0.0.2
   Type    :
```

L2L

```
             Role    :
```

responder

```
   Rekey   : no              State   :
```

MM_ACTIVE

関連情報

- 始めるのにふさわしい場所は IPsec に関する Wikipedia 記事.標準と参照には多くの有用な情報が含まれています
- IPSec のトラブルシューティング：debug コマンドの説明と使用
- テクニカル サポートとドキュメント – Cisco Systems