ASA IPsec および IKE のデバッグ（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

目次

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[主な問題](#)
[シナリオ](#)
[使用する debug コマンド](#)
[ASA の設定](#)
[デバッグ](#)
[関連情報](#)

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 を実行するルータ

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 を実行する 2 ASA からあります。 2 つのデバイスによって LAN-to-LAN トンネルが構成されます。

次の 2 つの主なシナリオについて説明します。

- IKE の発信側としての ASA
- IKE の応答側としての ASA

使用した debug コマンド

debug crypto ikev1 127

debug crypto ipsec 127

ASA の設定

IPSec構成:

```
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]: Pitcher: spi 0x0
IPSEC(crypto_map_check)-3: 5 : Prot=1saddr=192.168.1.2sport=2816 daddr=192.168.2.1dport=2816
IPSEC(crypto_map_check)-3: MAP 10 :
[[IKEv1]: IP = 10.0.0.2IKE : 1 IntfIKE 10.0.0.2 192.168.1.0 192.168.2.0 MAP

MM1

このプロセスには、IKE およびサポートされる NAT-T ベンダーの初期提案が含まれます。

[IKEv1]: **ISAKMP SA** [IKEv1 IP = 10.0.0.2]: VID ver 02 IP = 10.0.0.2
[IKEv1]: VID ver 03 IP = 10.0.0.2
[IKEv1]: VID ver RFC IP = 10.0.0.2
[IKEv1]: IP = 10.0.0.2 VID +

MM1

[[IKEv1]: IP = 10.0.0.2msgid=0 IKE_DECODE: HDR + SA 1 + 13 + 13 + 13 + 13 + 0 : 168

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

[[IKEv1]: IP = 10.0.0.2 IKE_DECODE msgid=0: HDR + SA 1 + 13 +VENDOR 13 + 13 + 13 + 0 : 164

MM1

[IKEv1]: SA IP = 10.0.0.2
[IKEv1]: IP = 10.0.0.2 Oakley
[IKEv1]: VID IP = 10.0.0.2
[IKEv1]: IP = 10.0.0.2 RFC VID
[IKEv1]: VID IP = 10.0.0.2
[IKEv1]: VID IP = 10.0.0.2
[IKEv1]: IP = 10.0.0.2 ver 03 VID
[IKEv1]: VID IP = 10.0.0.2
[IKEv1]: IP = 10.0.0.2 ver 02 VID
[IKEv1]: IKE SA IP = 10.0.0.2
[IKEv1]: IP = 10.0.0.2IKE SA # 1# 1 IKE # 2

MM1
ISAKMP/IKE
NAT-T

crypto isakmp policy 10
authentication pre-share
3des
sha
2
86400

[IKEv1]: ISAKMP SA IP = 10.0.0.2
[IKEv1]: VID ver 02 IP = 10.0.0.2
[IKEv1]: IP = 10.0.0.2 VID +

MM2
isakmp NAT-T

[[IKEv1]: IP = 10.0.0.2msgid=0 IKE_DECODE: HDR + SA 1 + 13 + 13 + NONE(0) : 128

MM2

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

MM2

[[IKEv1]: IP = 10.0.0.2 IKE_DECODE msgid=0: HDR + SA 1 + 13 + 0 : 104

MM2

[IKEv1]: SA IP = 10.0.0.2

[IKEv1]: IP = 10.0.0.2 Oakley
[IKEv1]: VID IP = 10.0.0.2
[IKEv1]: IP = 10.0.0.2 RFC VID
11 30 10:38:29 [IKEv1]: ke IP = 10.0.0.2
11 30 10:38:29 [IKEv1]: IP = 10.0.0.2
11 30 10:38:29 [IKEv1]: Cisco Unity VID IP = 10.0.0.2
11 30 10:38:29 [IKEv1]: Xauth V6 VID IP = 10.0.0.2
11 30 10:38:29 [IKEv1]: IP = 10.0.0.2 IOS VID
11 30 10:38:29 [IKEv1]: IOS Vendor ID ASA IP = 10.0.0.2: 1.0.0,
capabilities: 20000001
11 30 10:38:29 [IKEv1]: VID IP = 10.0.0.2
11 30 10:38:29 [IKEv1]: IP = 10.0.0.2 Altiga/Cisco VPN3000/Cisco ASA
GW VID
11 30 10:38:29 [IKEv1]: NAT   IP = 10.0.0.2
11 30 10:38:29 [IKEv1]: IP = 10.0.0.2 NAT
11 30 10:38:29 [IKEv1]: NAT   IP = 10.0.0.2
11 30 10:38:29 [IKEv1]: IP = 10.0.0.2 NAT
[[IKEv1]: IP = 10.0.0.2msgid=0 IKE_DECODE: HDR + KE 4 + NONCE
10 + 13 + 13 + 13 + 13 + NAT-D 20 + NAT-D 20 + 0 : 304

MM3

MM3includesNAT Diffie-Hellman DH KE initator gp A DPD

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

[[IKEv1]: IP = 10.0.0.2 IKE_DECODE msgid=0: HDR + KE 4 + NONCE
10 + 13 + 13 + 13 + NAT-D 130 + NAT-D 130 + 0 : 284

MM3

[IKEv1]: ke IP = 10.0.0.2
[IKEv1]: ISA_KE IP = 10.0.0.2
[IKEv1]: IP = 10.0.0.2processing NONCE
[IKEv1]: VID IP = 10.0.0.2
[IKEv1]: IP = 10.0.0.2 DPD VID
[IKEv1]: VID IP = 10.0.0.2
[IKEv1]: IOS/PIX Vendor ID IP = 10.0.0.2: 1.0.0, capabilities: 00000f6f
[IKEv1]: VID IP = 10.0.0.2
[IKEv1]: IP = 10.0.0.2 Xauth V6 VID
[IKEv1]: NAT   IP = 10.0.0.2
[IKEv1]: IP = 10.0.0.2 NAT
[IKEv1]: NAT   IP = 10.0.0.2
[IKEv1]: IP = 10.0.0.2 NAT

MM3
NAT-D ペイロードから、応答側は、発信側が NAT の背後にあるかどうか、および応答側が NAT の背後にあるかどうかを判別できます。

DH KE pg A

MM4
このプロセスには NAT ディスカバリ ペイロードが含まれ、DH KE 応答側は「B」と「s」（発信側に「B」を返信します）および DPD VID を生成します。

[IKEv1]: ke IP = 10.0.0.2
[IKEv1]: IP = 10.0.0.2
[IKEv1]: Cisco Unity VID IP = 10.0.0.2
[IKEv1]: Xauth V6 VID IP = 10.0.0.2
[IKEv1]: IP = 10.0.0.2 IOS VID
[IKEv1]: IOS Vendor ID ASA IP = 10.0.0.2: 1.0.0, capabilities: 20000001
[IKEv1]: VID IP = 10.0.0.2
[IKEv1]: IP = 10.0.0.2 Altiga/Cisco VPN3000/Cisco ASA GW VID
[IKEv1]: NAT   IP = 10.0.0.2
[IKEv1]: IP = 10.0.0.2 NAT
[IKEv1]: NAT   IP = 10.0.0.2
[IKEv1]: IP = 10.0.0.2 NAT
[[IKEv1]: IP = 10.0.0.2tunnel_group 10.0.0.2
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2…

10.0.0.2 L2L s

[[IKEv1]: IP = 10.0.0.2msgid=0 IKE_DECODE: HDR + KE 4 + NONCE
10 + 13 + 13 + 13 + 13 + NAT-D 130 + NAT-D 130 + 0 : 304

MM4

<==========MM4==========
=====

[[IKEv1]: IP = 10.0.0.2 IKE_DECODE msgid=0: HDR + KE 4 + NONCE
10 + 13 + 13 + 13 + 13 + NAT-D 20 + NAT-D 20 + 0 : 304

MM4

MM4
NAT-D ペイロードから、発信側は、発信側が NAT の背後にあるかどうか、お

[IKEv1]: ike IP = 10.0.0.2
[IKEv1]: ISA_KE IP = 10.0.0.2
[IKEv1]: IP = 10.0.0.2processing NONCE
[IKEv1]: VID IP = 10.0.0.2
[IKEv1]: IP = 10.0.0.2 Cisco Unity VID
[IKEv1]: VID IP = 10.0.0.2
[IKEv1]: IP = 10.0.0.2 DPD VID

よび応答側が NAT の背後にあるかどうかを判別できるようになりました。

DH KE から、発信側は「B」を受信し、「s」を生成できるようになりました。

[IKEv1]: VID IP = 10.0.0.2
[IKEv1]: IOS/PIX Vendor ID IP = 10.0.0.2: 1.0.0, capabilities: 00000f7f
[IKEv1]: VID IP = 10.0.0.2
[IKEv1]: IP = 10.0.0.2 Xauth V6 VID
[IKEv1]: NAT   IP = 10.0.0.2
[IKEv1]: IP = 10.0.0.2 NAT
[IKEv1]: NAT   IP = 10.0.0.2
[IKEv1]: IP = 10.0.0.2 NAT

10.0.0.2 L2L s

[[IKEv1]: IP = 10.0.0.2tunnel_group 10.0.0.2
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2…
[IKEv1]: = 10.0.0.2ID IP = 10.0.0.2
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2
[IKEv1]: = 10.0.0.2IP = 10.0.0.2ISAKMP
[IKEv1]: IOS   IP = 10.0.0.2: proposal=32767/32767
[IKEv1]: = 10.0.0.2dpd vid IP = 10.0.0.2

MM5

crypto isakmp identity auto

[[IKEv1]: IP = 10.0.0.2msgid=0 IKE_DECODE: HDR + ID 5 + HASH 8 + IOS 128 +VENDOR 13 + 0 : 96

MM5

==========MM5==========>

MM5
このプロセスには、リモート ピア ID と、特定のトンネル グループでの接続ランディングが含まれています。

[[IKEv1]: = 10.0.0.2IP = 10.0.0.2 NAT : NAT NAT

NAT NAT-T

[[IKEv1]: IP = 10.0.0.2 IKE_DECODE msgid=0: HDR + ID 5 + HASH 8 + 0 : 64

[IKEv1]: = 10.0.0.2IP = 10.0.0.2 ID
[IKEv1]: = 10.0.0.2IP = 10.0.0.2 ID_IPV4_ADDR ID 10.0.0.2
[IKEv1]: = 10.0.0.2IP = 10.0.0.2processing HASH 2
[IKEv1]: = 10.0.0.2IP = 10.0.0.2ISAKMP
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 tunnel group 10.0.0.2
[[IKEv1]: = 10.0.0.2IP = 10.0.0.2,Automatic NAT type ipsec-l2l
[[IKEv1]: IP = 10.0.0.2tunnel_group 10.0.0.2
: NAT NAT NAT-T
[IKEv1]: = 10.0.0.2ID IP = 10.0.0.2
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 MM6
[IKEv1]: = 10.0.0.2IP = 10.0.0.2ISAKMP
[IKEv1]: IOS   IP = 10.0.0.2: proposal=32767/32767
[IKEv1]: = 10.0.0.2dpd vid IP = 10.0.0.2
[[IKEv1]: IP = 10.0.0.2msgid=0 IKE_DECODE: HDR + ID 5 + HASH 8 + IOS 128 +VENDOR 13 + 0 : 96 MM6

<==========MM6==========

1
isakmp

crypto isakmp policy 10
authentication pre-share
3des
sha
2
86400

MM6

[[IKEv1]: IP = 10.0.0.2 IKE_DECODE msgid=0: HDR + ID 5 + HASH 8 + 0 : 64

[[IKEv1]: = 10.0.0.2IP = 10.0.0.2 1
[[IKEv1]: IP = 10.0.0.2: DPD
[IKEv1]: = 10.0.0.2 P1 IP = 10.0.0.2 : 64800

ciscoasa # sh run

isakmp
crypto isakmp
identity auto

[IKEv1]: = 10.0.0.2IP = 10.0.0.2 ID
[IKEv1]: = 10.0.0.2IP = 10.0.0.2 ID_IPV4_ADDR ID
10.0.0.2
MM6 [IKEv1]: = 10.0.0.2IP = 10.0.0.2processing HASH
[IKEv1]: = 10.0.0.2IP = 10.0.0.2ISAKMP
[[IKEv1]: IP = 10.0.0.2tunnel_group 10.0.0.2
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2Oakley Quick Mode
[IKEv1]: = 10.0.0.2IP = 10.0.0.2QM IKE : ID = 7b80c2b0
1
ISAKMP
関連する設定：
tunnel group 10.0.0.2 [[IKEv1]: = 10.0.0.2IP = 10.0.0.2 1
type ipsec-l2l [[IKEv1]: IP = 10.0.0.2: DPD
10.0.0.2 ipsec DPD 1
cisco [IKEv1]: = 10.0.0.2 P1 IP = 10.0.0.2 : 82080

IPSEC SA @ 0x53FC3C00
SCB: 0x53F90A00
[Direction]
SPI: 0xFD2D851F
2 Session id: 0x00006000
VPIF num: 0x00000003
Tunnel type: l2l
esp
Lifetime 240
QM1
このプロセスには、プロキシ ID と IPsec ポリシーが含まれています。
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 IKE SPI : SPI = 0xfd2d851f
[IKEv1]: = 10.0.0.2IP = 10.0.0.2oakley constucting Quick Mode
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2
[IKEv1]: = 10.0.0.2IPSec SA IP = 10.0.0.2
[IKEv1]: = 10.0.0.2IPSec IP = 10.0.0.2
[IKEv1]: = 10.0.0.2 ID IP = 10.0.0.2
[IKEv1]: = 10.0.0.2IP = 10.0.0.2 ID:
IPSec esp-aes esp- : 192.168.1.0 255.255.255.0 1 0
sha-hmac : 192.168.2.0 255.255.255.0 1 0
access-list VPN icmp 192.168.1.0/24 expcted 192.168.2.0/24
192.168.1.0 [IKEv1]: = 10.0.0.2IP = 10.0.0.2 IKE
255.255.255.0 [IKEv1]: = 10.0.0.2qm IP = 10.0.0.2
192.168.2.0 [IKEv1]: = 10.0.0.2IP = 10.0.0.2 1 QM pkt IKE : ID = 7b80c2b0
255.255.255.0

[[IKEv1]: IP = 10.0.0.2msgid=7b80c2b0 IKE_DECODE: HDR + HASH
QM1 (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0)
total length : 200
==========QM1==========>
[IKEv1]: IP = 10.0.0.2QM IKE : ID = 52481cf5 QM1
[[IKEv1]: IP = 10.0.0.2 IKE_DECODE msgid=52481cf5: HDR + HASH 2QM
(8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 172

QM1

このプロセスでは、リモート プロキシをローカル プロキシと比較し、許容可能な IPsec ポリシーを選択します。

IPSec esp-aes esp-sha-hmac
access-list VPN icmp
192.168.1.0
255.255.255.0
192.168.2.0
255.255.255.0
MAP 10 VPN

192.168.2.0/24
192.168.1.0/24

QM2

このプロセスには、プロキシ ID とトンネル タイプの確認が含まれ、ミラーリングされたクリプト ACL のチェックが実行されます。

QM2

QM2

2

```
[IKEv1 ]: = 10.0.0.2IP = 10.0.0.2processing HASH
[IKEv1 ]: = 10.0.0.2SA IP = 10.0.0.2
[IKEv1 ]: = 10.0.0.2IP = 10.0.0.2processing NONCE
[IKEv1 ]: = 10.0.0.2IP = 10.0.0.2 ID
[IKEv1 ]: = 10.0.0.2IP = 10.0.0.2ID_IPV4_ADDR_SUBNET ID received--192.168.2.0--255.255.255.0[IKEv1]: = 10.0.0.2 IP = 10.0.0.2ID IP : 192.168.2.0 255.255.255.0 1 0
[IKEv1 ]: = 10.0.0.2IP = 10.0.0.2 ID
[IKEv1 ]: = 10.0.0.2IP = 10.0.0.2ID_IPV4_ADDR_SUBNET ID received--192.168.1.0--255.255.255.0
[[IKEv1]: = 10.0.0.2 IP = 10.0.0.2ID IP : 192.168.1.0 255.255.255.0 1 0
[[IKEv1]: = 10.0.0.2IP = 10.0.0.2 QM IsRekeyed sa
[[IKEv1]: = 10.0.0.2IP = 10.0.0.2 = MAP seq = 10…
[[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 MAPseq = 10
[[IKEv1]: = 10.0.0.2IP = 10.0.0.2 IKE : MAP
[IKEv1 ]: = 10.0.0.2IPSec SA IP = 10.0.0.2
[IKEv1 ]: = 10.0.0.2IP = 10.0.0.2IPSec SA # 1# 1 IPSec SA # 10
[[IKEv1]: = 10.0.0.2IP = 10.0.0.2IKE: requesting SPI!
IPSEC SA @ 0x53FC3698
SCB: 0x53FC2998
[Direction]
SPI: 0x1698CAC7
Session id: 0x00004000
VPIF num: 0x00000003
Tunnel type: l2l
esp
Lifetime 240
[IKEv1 ]: = 10.0.0.2 IP = 10.0.0.2 IKE SPI : SPI = 0x1698cac7
[IKEv1 ]: = 10.0.0.2IP = 10.0.0.2Quick Mode oakley
[IKEv1 ]: = 10.0.0.2 IP = 10.0.0.2
[IKEv1 ]: = 10.0.0.2IPSec SA IP = 10.0.0.2
[IKEv1 ]: = 10.0.0.2IPSec IP = 10.0.0.2
[IKEv1 ]: = 10.0.0.2 ID IP = 10.0.0.2
[IKEv1 ]: = 10.0.0.2IP = 10.0.0.2 ID:
: 192.168.2.0 255.255.255.0 1 0
: 192.168.1.0 255.255.255.0 1 0
[IKEv1 ]: = 10.0.0.2qm IP = 10.0.0.2
[IKEv1 ]: = 10.0.0.2IP = 10.0.0.2 2 QM pkt IKE : ID = 52481cf5
[[IKEv1]: IP = 10.0.0.2msgid=52481cf5 IKE_DECODE: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 172
<============================QM2=========================
=====
[[IKEv1]: IP = 10.0.0.2 IKE_DECODE msgid=7b80c2b0: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
[IKEv1 ]: = 10.0.0.2IP = 10.0.0.2processing HASH
[IKEv1 ]: = 10.0.0.2SA IP = 10.0.0.2
[IKEv1 ]: = 10.0.0.2IP = 10.0.0.2processing NONCE
[IKEv1 ]: = 10.0.0.2IP = 10.0.0.2 ID
```

[IKEv1]: = 10.0.0.2IP = 10.0.0.2ID_IPV4_ADDR_SUBNET ID received--
192.168.1.0--255.255.255.0
[IKEv1]: = 10.0.0.2IP = 10.0.0.2 ID
[IKEv1]: = 10.0.0.2IP = 10.0.0.2ID_IPV4_ADDR_SUBNET ID received--
192.168.2.0--255.255.255.0
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2
[IKEv1]: outb SPI[4]|attributes:
[IKEv1]: 0000: DDE50931 80010001 00020004 00000E10… 1 .....
[[IKEv1]: = 10.0.0.2IP = 10.0.0.2 28800 3600 IPSec
ASA IPSEC
[IKEv1]: = 10.0.0.2 IPSec SA IP = 10.0.0.2
[IKEv1]: = 10.0.0.2Quick Mode IP = 10.0.0.2!
MAP 10 VPN
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 MAP 10 ACL VPN NP :
cs_id=53f11198; rule=53f11a90
[IKEv1]: = 10.0.0.2Quick Mode IP = 10.0.0.2!
 IPSEC SA @ 0x53FC3698
 SCB: 0x53F910F0
 [Direction]
 SPI: 0xDDE50931
 Session id: 0x00006000
 VPIF num: 0x00000003
 Tunnel type: l2l
  esp
 Lifetime 240
 IPSEC OBSA SPI 0xDDE50931
 IPSEC VPN SPI 0xDDE50931
  0x00000005
 SA: 0x53FC3698
 SPI: 0xDDE50931
 MTU 1500
 VCID : 0x00000000
 Peer : 0x00000000
 SCB: 0x01CF218F
  0x4C69CB80
 IPSEC VPN SPI 0xDDE50931
 VPN handle: 0x000161A4
 IPSEC SPI 0xDDE50931
Src addr: 192.168.1.0
 SPI 0xfd2d851f
Src mask: 255.255.255.0
0xdde50931
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
 IPSEC SPI 0xDDE50931
 Rule ID: 0x53FC3AD8
 IPSEC 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
 IPSEC SPI 0xDDE50931
 Rule ID: 0x53F91538
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 MAP 10 ACL VPN NP :
cs_id=53f11198; rule=53f11a90
[[IKEv1]: = 10.0.0.2IP = 10.0.0.2LAN-to-LAN 10.0.0.2 SPI = 0xfd2d851f
SPI = 0xdde50931
IPSEC IBSA SPI 0xFD2D851F
 IPSEC VPN SPI 0xFD2D851F
  0x00000006
 SA: 0x53FC3C00
 SPI: 0xFD2D851F
 MTU 0
 VCID : 0x00000000
 Peer : 0x000161A4
 SCB: 0x01CEA8EF
  0x4C69CB80
 IPSEC VPN SPI 0xFD2D851F
 VPN handle: 0x00018BBC
 IPSEC VPN 0x000161A4 SPI 0xDDE50931
  0x00000005
 SA: 0x53FC3698
 SPI: 0xDDE50931
 MTU 1500
 VCID : 0x00000000
 Peer : 0x00018BBC
 SCB: 0x01CF218F
  0x4C69CB80
 IPSEC VPN SPI 0xDDE50931
 VPN handle: 0x000161A4
 IPSEC SPI 0xDDE50931
 Rule ID: 0x53FC3AD8
 IPSEC SPD SPI 0xDDE50931
 Rule ID: 0x53F91538
 IPSEC   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
 IPSEC   SPI 0xFD2D851F
 Rule ID: 0x53F91970
 IPSEC SPI 0xFD2D851F
Src addr: 10.0.0.2
Src mask: 255.255.255.255
Dst addr: 10.0.0.1

QM3
リモート ピアに対して作成されたすべての SPI を確認します。

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
IPSEC SPI 0xFD2D851F
Rule ID: 0x53F91A08
IPSEC 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
IPSEC SPI 0xFD2D851F
Rule ID: 0x53F91AA0

QM3

[IKEv1]: = 10.0.0.2IP = 10.0.0.2 3 QM pkt IKE : ID = 7b80c2b0

==========QM3==========

====>

[[IKEv1]: IP = 10.0.0.2msgid=7b80c2b0

IKE_DECODE: HDR + HASH (8) + NONE (0) total length : 76

[IKEv1]: = 10.0.0.2 IP = 10.0.0.2IKE SA KEY_ADD : SPI = 0xdde50931

[IKEv1]: = 10.0.0.2IP = 10.0.0.2: KEY_UPDATEspi 0xfd2d851f

[IKEv1]: = 10.0.0.2 P2 IP = 10.0.0.2 : 3060

[[IKEv1]: = 10.0.0.2IP = 10.0.0.2 2 msgid=7b80c2b0

[[IKEv1]: IP = 10.0.0.2

IKE_DECODE msgid=52481cf5: HDR + HASH (8) + NONE (0) total length : 52

2 SPI

QM3

[IKEv1]: = 10.0.0.2IP = 10.0.0.2processing HASH

[IKEv1]: = 10.0.0.2 IPSec SA IP = 10.0.0.2

[IKEv1]: = 10.0.0.2Quick Mode IP = 10.0.0.2!

[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 MAP 10 ACL VPN NP : cs_id=53f11198; rule=53f11a90

[IKEv1]: = 10.0.0.2Quick Mode IP = 10.0.0.2!

IPSEC SA @ 0x53F18B00

SCB: 0x53F8A1C0

[Direction] SA

SPI: 0xDB680406

Session id: 0x00004000

SPI

VPIF num: 0x00000003

Tunnel type: l2l

esp

Lifetime 240

IPSEC OBSA SPI 0xDB680406

IPSEC VPN SPI 0xDB680406

0x00000005

SA: 0x53F18B00
SPI: 0xDB680406
MTU 1500
VCID : 0x00000000
Peer : 0x00000000
SCB: 0x005E4849
0x4C69CB80
IPSEC VPN SPI 0xDB680406
VPN handle: 0x0000E9B4
IPSEC 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
IPSEC SPI 0xDB680406
Rule ID: 0x53F89160
IPSEC 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
IPSEC SPI 0xDB680406
Rule ID: 0x53E47E88
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 MAP 10 ACL VPN NP :
cs_id=53f11198; rule=53f11a90
[[IKEv1]: = 10.0.0.2IP = 10.0.0.2LAN-to-LAN 10.0.0.2 SPI = 0x1698cac7
SPI = 0xdb680406
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2IKE SA KEY_ADD : SPI = 0xdb680406
IPSEC IBSA SPI 0x1698CAC7
IPSEC VPN SPI 0x1698CAC7
0x00000006
SA: 0x53FC3698
SPI: 0x1698CAC7 SPI SA
MTU 0
VCID : 0x00000000
Peer : 0x0000E9B4
SCB: 0x005DAE51
0x4C69CB80
IPSEC VPN SPI 0x1698CAC7
VPN handle: 0x00011A8C

IPSEC VPN 0x0000E9B4 SPI 0xDB680406
0x00000005
SA: 0x53F18B00
SPI: 0xDB680406
MTU 1500
VCID : 0x00000000
Peer : 0x00011A8C
SCB: 0x005E4849
0x4C69CB80
IPSEC VPN SPI 0xDB680406
VPN handle: 0x0000E9B4
IPSEC SPI 0xDB680406
Rule ID: 0x53F89160
IPSEC SPD SPI 0xDB680406
Rule ID: 0x53E47E88
IPSEC 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
IPSEC SPI 0x1698CAC7
Rule ID: 0x53FC3E80
IPSEC 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
IPSEC SPI 0x1698CAC7
Rule ID: 0x53FC3F18
IPSEC 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
IPSEC SPI 0x1698CAC7
Rule ID: 0x53F8AEA8
[IKEv1]: = 10.0.0.2IP = 10.0.0.2: KEY_UPDATEspi 0x1698cac7
[IKEv1]: = 10.0.0.2 P2 IP = 10.0.0.2 : 3060 IPsec
[[IKEv1]: = 10.0.0.2IP = 10.0.0.2 2 msgid=52481cf5 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

- 開始するべき適切な場所は IPSec の wikipedia 技術情報です。 規格および参照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