ASA IPsec和IKE調試（IKEv1主模式）故障排除技術說明

目錄

簡介

本文說明當同時使用主模式和預共用金鑰(PSK)時，自適應安全裝置(ASA)上的調試。還討論了將某些調試行轉換為配置的問題。

本檔案未討論的主題包括在建立通道後傳輸流量和IPsec或Internet金鑰交換(IKE)的基本概念。

必要條件

需求

本文檔的讀者應該瞭解這些主題。

- PSK
- IKE

採用元件

本檔案中的資訊是根據以下硬體和軟體版本：

- Cisco ASA 9.3.2
- 執行Cisco IOS® 12.4T的路由器

核心問題

IKE和IPsec調試有時是隱藏的，但您可以使用它們來瞭解IPsec VPN隧道建立問題的位置。

案例

主模式通常用於LAN到LAN通道之間，如果是遠端訪問(EzVPN)，當證書用於身份驗證時。

調試來自運行軟體版本9.3.2的兩台ASA。這兩台裝置將形成LAN到LAN隧道。

描述了兩種主要方案：

- ASA作為IKE的啟動器
- ASA作為IKE的響應方

使用的Debug命令

debug crypto ikev1 127

debug crypto ipsec 127

ASA配置

IPsec配置：

```
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配置：

```
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配置：

```
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
```

調試

MM_NO_STATE ASA	[IKEv1 DEBUG]:spi 0x0 IPSEC(crypto_map_check)-3:5 Prot=1,saddr=192.168.1.2,sport=2816,daddr=192.168.2.1,dport=2816 IPSEC(crypto_map_check)-3:10:	
MM1 iIKESNAT-T	[IKEv1]:IP = 10.0.0.2,IKE1Intf,IKE10.0.0.2192.168.1.0192.168.2.0(MAP) [IKEv1 DEBUG]:IP = 10.0.0.2**ISAKMP SA**[IKEv1 DEBUG]:IP = 10.0.0.2 NATVID02 [IKEv1 DEBUG]:IP = 10.0.0.2NATVID03 [IKEv1 DEBUG]:IP = 10.0.0.2NATVID ver RFC	
MM1	[IKEv1 DEBUG]:IP = 10.0.0.2VID + [IKEv1]:IP = 10.0.0.2,IKE_DECODE(msgid=0)HDR + SA(1)+(13)+(13)+ (13)+(13)+(13)+(0)168	
	==========MM1========== ====>	
	[IKEv1]:IP = 10.0.0.2,IKE_DECODE RECEIVED Message(msgid=0)HDR + SA(1)+(13)+(13)+(13)+(13)+(13)+(0)164	MM1
	[IKEv1 DEBUG]:IP = 10.0.0.2SA	MM1
	[IKEv1 DEBUG]:IP = 10.0.0.2,Oakley	ISAKMP/IKE
	[IKEv1 DEBUG]:IP = 10.0.0.2VID	NAT-T
	[IKEv1 DEBUG]:IP = 10.0.0.2NATRFC VID	
	[IKEv1 DEBUG]:IP = 10.0.0.2VID	*crypto isakmp policy*
	[IKEv1 DEBUG]:IP = 10.0.0.2VID	*10*
	[IKEv1 DEBUG]:IP = 10.0.0.2NAT03 VID	
	[IKEv1 DEBUG]:IP = 10.0.0.2VID	*3des*
	[IKEv1 DEBUG]:IP = 10.0.0.2NAT02 VID	*hash sha*
	[IKEv1 DEBUG]:IP = 10.0.0.2IKE SA	*2*
	[IKEv1 DEBUG]:IP = 10.0.0.2,IKE SA# 1# 1 acceptableIKE# 2	*lifetime 86400*
	[IKEv1 DEBUG]:IP = 10.0.0.2ISAKMP SA	MM2
	[IKEv1 DEBUG]:IP = 10.0.0.2NATVID02	isakmp NAT-T
	[IKEv1 DEBUG]:IP = 10.0.0.2VID +	
	[IKEv1]:IP = 10.0.0.2,IKE_DECODE(msgid=0)HDR + SA(1)+(13)+(13)+ (0)128	MM2
	<==========MM2========== =====	
MM2	[IKEv1]:IP = 10.0.0.2,IKE_DECODE RECEIVED Message(msgid=0)HDR + SA(1)+(13)+(0)104	
MM2	[IKEv1 DEBUG]:IP = 10.0.0.2SA [IKEv1 DEBUG]:IP = 10.0.0.2,Oakley [IKEv1 DEBUG]:IP = 10.0.0.2VID [IKEv1 DEBUG]:IP = 10.0.0.2NATRFC VID	
MM3 NAT -hellman(DH) (KE)(igpA) DPD	113010:38:29 [IKEv1]:IP = 10.0.0.2 113010:38:29 [IKEv1]:IP = 10.0.0.2 113010:38:29 [IKEv1]:IP = 10.0.0.2Cisco Unity VID 113010:38:29 [IKEv1]:IP = 10.0.0.2xauth V6 VID 113010:38:29 [IKEv1]:IP = 10.0.0.2IOS VID 113010:38:29 [IKEv1]:IP = 10.0.0.2ASAIOSID(1.0.020000001) 113010:38:29 [IKEv1]:IP = 10.0.0.2VID 113010:38:29 [IKEv1]:IP = 10.0.0.2Altiga/Cisco VPN3000/Cisco ASA GW VID	

113010:38:29 [IKEv1]:IP = 10.0.0.2NAT
113010:38:29 [IKEv1]:IP = 10.0.0.2NAT
113010:38:29 [IKEv1]:IP = 10.0.0.2NAT
113010:38:29 [IKEv1]:IP = 10.0.0.2NAT

MM3

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

==========MM3==========

====>

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

MM3

[IKEv1 DEBUG]:IP = 10.0.0.2Ke Payload
[IKEv1 DEBUG]:IP = 10.0.0.2ISA_KE
[IKEv1 DEBUG]:IP = 10.0.0.2
[IKEv1 DEBUG]:IP = 10.0.0.2VID
[IKEv1 DEBUG]:IP = 10.0.0.2DPD VID
[IKEv1 DEBUG]:IP = 10.0.0.2VID
[IKEv1 DEBUG]:IP = 10.0.0.2IOS/PIXID(1.0.000000f6f)
[IKEv1 DEBUG]:IP = 10.0.0.2VID
[IKEv1 DEBUG]:IP = 10.0.0.2xauth V6 VID
[IKEv1 DEBUG]:IP = 10.0.0.2NAT
[IKEv1 DEBUG]:IP = 10.0.0.2NAT
[IKEv1 DEBUG]:IP = 10.0.0.2NAT
[IKEv1 DEBUG]:IP = 10.0.0.2NAT
[IKEv1 DEBUG]:IP = 10.0.0.2ke payload
[IKEv1 DEBUG]:IP = 10.0.0.2
[IKEv1 DEBUG]:IP = 10.0.0.2Cisco Unity VID
[IKEv1 DEBUG]:IP = 10.0.0.2xauth V6 VID
[IKEv1 DEBUG]:IP = 10.0.0.2IOS VID

MM3 NAT-D NAT NAT DH KEpgA

MM4

[IKEv1 DEBUG]:IP = 10.0.0.2ASAIOSID(1.0.020000001)
[IKEv1 DEBUG]:IP = 10.0.0.2VID
[IKEv1 DEBUG]:IP = 10.0.0.2Altiga/Cisco VPN3000/Cisco ASA GW VID
[IKEv1 DEBUG]:IP = 10.0.0.2NAT
[IKEv1 DEBUG]:IP = 10.0.0.2NAT
[IKEv1 DEBUG]:IP = 10.0.0.2NAT
[IKEv1 DEBUG]:IP = 10.0.0.2NAT

NAT sponderBsB itator DPD VID

[IKEv1]:IP = 10.0.0.2tunnel_group 10.0.0.2
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2……

10.0.0.2 L2Ls

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

MM4

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

=====

MM4 received from responder

[IKEv1]:IP = 10.0.0.2,IKE_DECODE RECEIVED Message(msgid=0)HDR + KE(4)+(10)+(13)+(13)+(13)+(13)+(13)+ NAT-D(20)+ NAT-D(20)+(0)304

[IKEv1 DEBUG]:IP = 10.0.0.2ike
[IKEv1 DEBUG]:IP = 10.0.0.2ISA_KE
[IKEv1 DEBUG]:IP = 10.0.0.2
[IKEv1 DEBUG]:IP = 10.0.0.2VID
[IKEv1 DEBUG]:IP = 10.0.0.2Cisco UnityVID
[IKEv1 DEBUG]:IP = 10.0.0.2VID
[IKEv1 DEBUG]:IP = 10.0.0.2DPD VID
[IKEv1 DEBUG]:IP = 10.0.0.2VID
[IKEv1 DEBUG]:IP = 10.0.0.2IOS/PIXID(1.0.000000f7f)
[IKEv1 DEBUG]:IP = 10.0.0.2VID
[IKEv1 DEBUG]:IP = 10.0.0.2xauth V6 VID
[IKEv1 DEBUG]:IP = 10.0.0.2NAT
[IKEv1 DEBUG]:IP = 10.0.0.2NAT
[IKEv1 DEBUG]:IP = 10.0.0.2NAT
[IKEv1 DEBUG]:IP = 10.0.0.2NAT

MM4
NAT-D NAT NAT

DH KEiBs

[IKEv1]:IP = 10.0.0.2tunnel_group 10.0.0.2
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2……

10.0.0.2 L2Ls

[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2ID
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2

MM5

crypto isakmp identity auto

[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2ISAKMP
[IKEv1 DEBUG]:IP = 10.0.0.2IOSproposal=32767/32767 sec
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2dpd vid
[IKEv1]:IP = 10.0.0.2,IKE_DECODE(msgid=0)HDR + ID(5)+(8)+ IOS KEEPALIVE(128)+(13)+(0)96

MM5

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

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

[IKEv1]:IP = 10.0.0.2,IKE_DECODE RECEIVED Message(msgid=0)HDR + ID(5)+(8)+(0)64

MM5 received from initiator r(ID)c

NATNAT-T

[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2ID
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2ID_IPV4_ADDR ID 10.0.0.2
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2ISAKMP
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2NAT
[IKEv1]:IP = 10.0.0.2tunnel_group 10.0.0.2 NATNAT
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2ID
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2ISAKMP
[IKEv1 DEBUG]:IP = 10.0.0.2IOSproposal=32767/32767 sec
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2dpd vid
[IKEv1]:IP = 10.0.0.2,IKE_DECODE(msgid=0)HDR + ID(5)+(8)+ IOS KEEPALIVE(128)+(13)+(0)96

MM5

10.0.0.2ipsec-l2l

NAT-T

MM6

MM6

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

1
isakmp

crypto isakmp policy 10

MM6 received from responder

[IKEv1]:IP = 10.0.0.2,IKE_DECODE RECEIVED Message(msgid=0)HDR + ID(5)+(8)+(0)64

[IKEv1]:= 10.0.0.2,IP = 10.0.0.21
[IKEv1]:IP = 10.0.0.2DPD
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2P164800

3des
hash sha
2
lifetime 86400
ciscoasa# sh run all
crypto isakmp
crypto isakmp identity auto

[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2ID
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2ID_IPV4_ADDR ID 10.0.0.2
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2ISAKMP
[IKEv1]:IP = 10.0.0.2tunnel_group 10.0.0.2
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2,Oakley
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2QMIKEmsg id = 7b80c2b0

MM6
rf

1
ISAKMP
c
10.0.0.2ipsec-l2l
10.0.0.2 ipsec-attributes
cisco

[IKEv1]:= 10.0.0.2,IP = 10.0.0.21
[IKEv1]:IP = 10.0.0.2DPD
DPD1
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2P182080

2

IPSEC:0x53FC3C00SA
SCB:0x53F90A00,
Direction:

SPI:0xFD2D851F
ID:0x00006000
VPIF num:0x00000003
l2l
:esp
240

QM1 [IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2,IKESPI:SPI = 0xfd2d851f

IDIP [IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2

[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2

crypto ipsec [IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2IPSec SA

transform-set [IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2IPSec nonce

TRANSFORM esp- [IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2ID

aes esp-sha-hmac [IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2Id:

access-list VPN 192.168.1.0255.255.255.010

extended permit icmp 192.168.2.0255.255.255.010

192.168.1.0 (192.168.1.0/24)(192.168.2.0/24)

255.255.255.0 [IKEv1]:= 10.0.0.2,IP = 10.0.0.2,IKE

192.168.2.0 [IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2qm

255.255.255.0 [IKEv1]:= 10.0.0.2,IP = 10.0.0.2,IKEQM :msg id = 7b80c2b0

QM1 [IKEv1]:IP = 10.0.0.2,IKE_DECODE(msgid=7b80c2b0)HDR +(8)+ SA(1)+ (10)+ ID(5)+ ID(5)+ NOTIFY(11)+(0)200

==========QM1==========>

[IKEv1]:IP = 10.0.0.2,IKEQM: id = 52481cf5

[IKEv1]:IP = 10.0.0.2, IKE_DECODE RECEIVED Message(msgid=52481cf5)HDR +(8)+ SA(1)+(10)+ ID(5)+ ID(5)+(0)172

QM1 2(QM)

QM1 IP

crypto ipsec

transform-set

TRANSFORM esp-

[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2 aes esp-sha-hmac

[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2SA access-list VPN

[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2 extended permit icmp

[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2ID 192.168.1.0

255.255.255.0

192.168.2.0

255.255.255.0

crypto map MAP 10

match address VPN

[IKEv1]: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:192.168.2.0

255.255.255.010 (192.168.2.0/24

[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2ID 192.168.1.0/24)

[IKEv1]: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]:= 10.0.0.2,IP = 10.0.0.2,IDIP192.168.1.0255.255.255.010

[IKEv1]:Group = 10.0.0.2,IP = 10.0.0.2,QM IsRekeyed old sa not found by addr

[IKEv1]:= 10.0.0.2,IP = 10.0.0.2= MAPseq = 10...

[IKEv1]:= 10.0.0.2,IP = 10.0.0.2MAP,seq = 10

[IKEv1]:= 10.0.0.2,IP = 10.0.0.2IKE

[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2IPSec SA

[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2,IPSec SA# 1# 1IPSec SA# 10

[IKEv1]:= 10.0.0.2,IP = 10.0.0.2,IKE:SPI!

IPSEC:0x53FC3698SA

SCB:0x53FC2998,

Direction:

QM2

SPI:0x1698CAC7 c ACL

ID:0x00004000

VPIF num:0x00000003

l2l

:esp

240
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2,IKESPI:SPI = 0x1698cac7
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2,oakley
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2IPSec SA
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2IPSec nonce
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2ID
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2Id:
192.168.2.0255.255.255.010
192.168.1.0255.255.255.010
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2qm
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2,IKEQM :msg id = 52481cf5
[IKEv1]:IP = 10.0.0.2,IKE_DECODE(msgid=52481cf5)HDR +(8)+ SA(1)+ (10)+ ID(5)+ ID(5)+(0)172 QM2

<=============================QM2=========================
=====

[IKEv1]:IP = 10.0.0.2, IKE_DECODE RECEIVED
QM2 Message(msgid=7b80c2b0)HDR +(8)+ SA(1)+(10)+ ID(5)+ ID(5)+
NOTIFY(11)+(0)200
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2SA
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2ID
[IKEv1]: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]:= 10.0.0.2,IP = 10.0.0.2ID
QM2 [IKEv1]:Group = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID
r received - 192.168.2.0 - 255.255.0
2 [IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2
[IKEv1]:(outb SPI[4]lattributes):
[IKEv1]: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
ASAIPSEC
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2IPSEC SA
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2,NPMAP 10ACL VPN:
MAP10VPN cs_id=53f11198;rule=53f11a90
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2
IPSEC:0x53FC3698SA
SCB:0x53F910F0,
Direction:
SPI:0xDDE50931
ID:0x00006000
VPIF num:0x00000003
l2l
:esp
240
IPSEC:OBSASPI 0xDDE50931
IPSEC:VPNSPI 0xDDE50931
SPI 0xfd2d851f 0x00000005
50931xdde SA:0x53FC3698
SPI:0xDDE50931
MTU:1500
VCID:0x00000000
0x00000000
SCB:0x01CF218F
0x4C69CB80
IPSEC:VPNSPI 0xDDE50931
VPN0x000161A4
IPSEC:SPI 0xDDE50931
Src addr:192.168.1.0
Src mask:255.255.255.0
Dst addr:192.168.2.0

Dst255.255.255.0

0
0
Op :
Dst
0
0
Op :
:1
true
SPI:0x00000000
SPI:
IPSEC:SPI 0xDDE50931
ID:0x53FC3AD8
IPSEC:SPI 0xDDE50931
Src addr:10.0.0.1
Src mask:255.255.255.255
Dst addr:10.0.0.2
Dst255.255.255.255

0
0
Op :
Dst
0
0
Op :
:50
true
SPI:0xDDE50931
SPI:true
IPSEC:SPI 0xDDE50931
ID:0x53F91538
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2,NPMAP 10ACL VPN:
cs_id=53f11198;rule=53f11a90
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2(10.0.0.2)SPI = 0xfd2d851fSPI =
0xdde50931
IPSEC:IBSASPI 0xFD2D851F
IPSEC:VPNSPI 0xFD2D851F
0x00000006
SA:0x53FC3C00
SPI:0xFD2D851F
MTU:0
VCID:0x00000000
0x000161A4
SCB:0x01CEA8EF
0x4C69CB80
IPSEC:VPNSPI 0xFD2D851F
VPN0x00018BBC
QM3 IPSEC:VPN0001610x2A4,SPI 0xDDE50931
SPI 0x00000005
SA:0x53FC3698
SPI:0xDDE50931
MTU:1500
VCID:0x00000000
0x00018BBC
SCB:0x01CF218F
0x4C69CB80
IPSEC:VPNSPI 0xDDE50931
VPN0x000161A4
IPSEC:SPI 0xDDE50931
ID:0x53FC3AD8
IPSEC:SPDSPI 0xDDE50931

ID:0x53F91538
IPSEC:SPI 0xFD2D851F
Src addr:192.168.2.0
Src mask:255.255.255.0
Dst addr:192.168.1.0
Dst255.255.255.0

0
0
Op :
Dst
0
0
Op :
:1
true
SPI:0x00000000
SPI:
IPSEC:SPI 0xFD2D851F
ID:0x53F91970
IPSEC:SPI 0xFD2D851F
Src addr:10.0.0.2
Src mask:255.255.255.255
Dst addr:10.0.0.1
Dst255.255.255.255

0
0
Op :
Dst
0
0
Op :
:50
true
SPI:0xFD2D851F
SPI:true
IPSEC:SPI 0xFD2D851F
ID:0x53F91A08
IPSEC:SPI 0xFD2D851F
Src addr:10.0.0.2
Src mask:255.255.255.255
Dst addr:10.0.0.1
Dst255.255.255.255

0
0
Op :
Dst
0
0
Op :
:50
true
SPI:0xFD2D851F
SPI:true
IPSEC:SPI 0xFD2D851F
ID:0x53F91AA0
QM3 [IKEv1]:= 10.0.0.2,IP = 10.0.0.2,IKE3QM :msg id = 7b80c2b0

==========QM3==========
===>
2 [IKEv1]:IP = 10.0.0.2,IKE_DECODE(msgid=7b80c2b0) [IKEv1]:IP =
SPI HDR +(8)+(0)76 10.0.0.2, QM3

[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2,IKESA
KEY_ADD msg:SPI = 0xdde50931
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2
KEY_UPDATE,spi0xfd2d851f
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2P23060
[IKEv1]:= 10.0.0.2,IP = 10.0.0.22(msgid=7b80c2b0)

IKE_DECODE
RECEIVED
Message(msgid=5
2481cf5)HDR +
(8)+(0)52

[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2IPSEC SA
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2,NPMAP 10ACL VPN:
cs_id=53f11198;rule=53f11a90
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2
IPSEC:0x53F18B00SA
SCB:0x53F8A1C0,
Direction:
SPI:0xDB680406
ID:0x00004000
VPIF num:0x00000003
l2l
:esp
240
IPSEC:OBSASPI 0xDB680406
IPSEC:VPNSPI 0xDB680406
0x00000005
SA:0x53F18B00
SPI:0xDB680406
MTU:1500
VCID:0x00000000
0x00000000
SCB:0x005E4849
0x4C69CB80
IPSEC:VPNSPI 0xDB680406
VPN0x0000E9B4
IPSEC:SPI 0xDB680406 QM3
Src addr:192.168.1.0 SA
Src mask:255.255.255.0
Dst addr:192.168.2.0 SPI
Dst255.255.255.0

0
0
Op :
Dst
0
0
Op :
:1
true
SPI:0x00000000
SPI:
IPSEC:SPI 0xDB680406
ID:0x53F89160
IPSEC:SPI 0xDB680406
Src addr:10.0.0.1
Src mask:255.255.255.255
Dst addr:10.0.0.2
Dst255.255.255.255

0
0
Op :
Dst
0
0

Op :
:50
true
SPI:0xDB680406
SPI:true
IPSEC:SPI 0xDB680406
ID:0x53E47E88
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2,NPMAP 10ACL VPN:
cs_id=53f11198;rule=53f11a90
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2,LANLAN(10.0.0.2)SPI = 0x1698cac7SPI
= 0xdb680406
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2,IKESAKEY_ADD msg:SPI =
0xdb680406
IPSEC:IBSASPI 0x1698CAC7
IPSEC:VPNSPI 0x1698CAC7
0x00000006
SA:0x53FC3698
SPI:0x1698CAC7
MTU:0
VCID:0x00000000
0x0000E9B4
SCB:0x005DAE51
0x4C69CB80
IPSEC:VPNSPI 0x1698CAC7
VPN0x00011A8C
IPSEC:VPN0x0000E9B4,SPI 0xDB680406
0x00000005
SA:0x53F18B00
SPI:0xDB680406
MTU:1500
VCID:0x00000000
0x00011A8C
SCB:0x005E4849
0x4C69CB80
IPSEC:VPNSPI 0xDB680406
VPN0x0000E9B4
IPSEC:SPI 0xDB680406 SPISA
ID:0x53F89160
IPSEC:SPDSPI 0xDB680406
ID:0x53E47E88
IPSEC:SPI 0x1698CAC7
Src addr:192.168.2.0
Src mask:255.255.255.0
Dst addr:192.168.1.0
Dst255.255.255.0

0
0
Op :
Dst
0
0
Op :
:1
true
SPI:0x00000000
SPI:
IPSEC:SPI 0x1698CAC7
ID:0x53FC3E80
IPSEC:SPI 0x1698CAC7
Src addr:10.0.0.2
Src mask:255.255.255.255
Dst addr:10.0.0.1
Dst255.255.255.255

0
0
Op :
Dst
0
0
Op :
:50
true
SPI:0x1698CAC7
SPI:true
IPSEC:SPI 0x1698CAC7
ID:0x53FC3F18
IPSEC:SPI 0x1698CAC7
Src addr:10.0.0.2
Src mask:255.255.255.255
Dst addr:10.0.0.1
Dst255.255.255.255

0
0
Op :
Dst
0
0
Op :
:50
true
SPI:0x1698CAC7
SPI:true
IPSEC:SPI 0x1698CAC7
ID:0x53F8AEA8
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2KEY_UPDATE,spi 0x1698cac7
[IKEv1 DEBUG]:= 10.0.0.2,IP = 10.0.0.2P23060 IPsec
[IKEv1]:= 10.0.0.2,IP = 10.0.0.22(msgid=52481cf5) 2/

通道驗證

附註：由於ICMP用於觸發通道，因此只有一個IPSec SA處於啟用狀態。協定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

相關資訊

- 一個很好的起點是 關於IPSec的維基百科文章。標準和參考文獻中包含許多有用的資訊

- IPsec 疑難排解：瞭解和使用偵錯指令
- **技術支援與文件 - Cisco Systems**