ASA IPsec和IKE调试（IKEv1主模式）故障排除技术说明

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[核心问题](#)
[场景](#)
[使用的调试命令](#)
[ASA 配置](#)
[调试](#)
[相关信息](#)

简介

本文档介绍在同时使用主模式和预共享密钥(PSK)时，在自适应安全设备(ASA)上进行的调试。还将讨论将某些调试行转换为配置。

本文档中未讨论的主题包括隧道建立后传递流量以及IPsec或互联网密钥交换(IKE)的基本概念。

先决条件

要求

本文档的读者应了解这些主题。

- PSK
- IKE

使用的组件

本文档中的信息基于下列硬件和软件版本：

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

核心问题

IKE和IPsec调试有时很晦涩，但您可以使用它们了解IPsec VPN隧道建立问题的位置。

场景

主模式通常用于LAN到LAN隧道之间，在远程访问(EzVPN)情况下，在证书用于身份验证时使用。

调试来自运行软件版本9.3.2的两个ASA。两台设备将形成LAN到LAN隧道。

介绍了两种主要方案：

- ASA作为IKE的启动器
- ASA作为IKE的响应方

使用的调试命令

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
```

调试

MM_NO_STATE ASA	[IKEv1]:spi 0x0 IPSEC(crypto_map_check)-3:5Prot=1, saddr=192.168.1.2, sport=2816, daddr=192.168.2.1, dport=2816 IPSEC(crypto_map_check)-3:MAP 10: .
MM1 iIKENAT-T	[IKEv1]:IP = 10.0.0.2,IKE1,IntfIKE10.0.0.2192.168.1.0192.168.2.0(MAP) [IKEv1]:IP = 10.0.0.2**ISAKMP SA**[IKEv1 DEBUG]:IP = 10.0.0.2NATVID 02 [IKEv1]:IP = 10.0.0.2NATVID03 [IKEv1]:IP = 10.0.0.2NATVID ver RFC [IKEv1]:IP = 10.0.0.2VID +
MM1	[IKEv1]:IP = 10.0.0.2IKE_DECODE(msgid=0):HDR + SA(1)+(13)+(13)+ (13)+(13)+(13)+(0)168
	==========
	==========
MM1	[IKEv1]:IP = 10.0.0.2IKE_DECODE RECEIVED(msgid=0):HDR + SA(1)+ (13)+(13)+(13)+(13)+(13)+(0)164
MM1	[IKEv1]:IP = 10.0.0.2SA
ISAKMP/IKE	[IKEv1]:IP = 10.0.0.2,Oakley
NAT-T	[IKEv1]:IP = 10.0.0.2VID
	[IKEv1]:IP = 10.0.0.2NATRFC VID
crypto isakmp10	[IKEv1]:IP = 10.0.0.2VID
authentication pre-	[IKEv1]:IP = 10.0.0.2VID
share	[IKEv1]:IP = 10.0.0.2NAT03 VID
3des	[IKEv1]:IP = 10.0.0.2VID
hash sha	[IKEv1]:IP = 10.0.0.2NAT02 VID
2	[IKEv1]:IP = 10.0.0.2IKE SA
lifetime 86400	[IKEv1]:IP = 10.0.0.2,IKE SA# 1# 1IKE# 2
MM2 isakmp NAT-T	[IKEv1]:IP = 10.0.0.2ISAKMP SA [IKEv1]:IP = 10.0.0.2NATVID02 [IKEv1]:IP = 10.0.0.2VID +
MM2	[IKEv1]:IP = 10.0.0.2IKE_DECODE(msgid=0):HDR + SA(1)+(13)+(13)+ (0)128
	<==========
	==========
MM2	[IKEv1]:IP = 10.0.0.2IKE_DECODE RECEIVED(msgid=0):HDR + SA(1)+ (13)+(0)104
MM2	[IKEv1]:IP = 10.0.0.2SA [IKEv1]:IP = 10.0.0.2,Oakley [IKEv1]:IP = 10.0.0.2VID [IKEv1]:IP = 10.0.0.2NATRFC VID
MM3 NAT -Hellman(DH) (KE)(initatorgpA), DPD	113010:38:29 [IKEv1]:IP = 10.0.0.2ke 113010:38:29 [IKEv1]:IP = 10.0.0.2nonce 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 = 10.0.0.2IKE_DECODE(msgid=0):HDR + KE(4)+ NONCE(10)+(13)+(13)+(13)+(13)+ NAT-D(20)+ NAT-D(20)+(0)304

==========

==========

[IKEv1]:IP = 10.0.0.2IKE_DECODE RECEIVED(msgid=0):HDR + KE(4)+ NONCE(10)+(13)+(13)+(13)+ NAT-D(130)+ NAT-D(130)+ NONE(0)284 MM3

[IKEv1]:IP = 10.0.0.2
[IKEv1]:IP = 10.0.0.2ISA_KE
[IKEv1]:IP = 10.0.0.2
[IKEv1]:IP = 10.0.0.2VID
[IKEv1]:IP = 10.0.0.2DPD VID MM3
[IKEv1]:IP = 10.0.0.2VID NAT-D initatorNAT
[IKEv1]:IP = 10.0.0.2IOS/PIXID(1.0.000000f6f) NAT
[IKEv1]:IP = 10.0.0.2VID DH KEpgA
[IKEv1]:IP = 10.0.0.2xauth V6 VID
[IKEv1]:IP = 10.0.0.2NAT
[IKEv1]:IP = 10.0.0.2NAT
[IKEv1]:IP = 10.0.0.2NAT
[IKEv1]:IP = 10.0.0.2NAT
[IKEv1]:IP = 10.0.0.2ke
[IKEv1]:IP = 10.0.0.2nonce
[IKEv1]:IP = 10.0.0.2Cisco Unity VID
[IKEv1]:IP = 10.0.0.2xauth V6 VID
[IKEv1]:IP = 10.0.0.2IOS VID MM4
[IKEv1]:IP = 10.0.0.2ASAIOSID(1.0.020000001 NAT DH KE responder"B""s""B"
[IKEv1]:IP = 10.0.0.2VID DPD VID
[IKEv1]:IP = 10.0.0.2Altiga/Cisco VPN3000/Cisco ASA GW VID
[IKEv1]:IP = 10.0.0.2NAT
[IKEv1]:IP = 10.0.0.2NAT
[IKEv1]:IP = 10.0.0.2NAT
[IKEv1]:IP = 10.0.0.2NAT
[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 = 10.0.0.2IKE_DECODE(msgid=0):HDR + KE(4)+ NONCE(10)+(13)+(13)+(13)+(13)+ NAT-D(130)+ NAT-D(130)+(0)304 MM4

<==========

==========

MM4

[IKEv1]:IP = 10.0.0.2IKE_DECODE RECEIVED(msgid=0):HDR + KE(4)+ NONCE(10)+(13)+(13)+(13)+(13)+ NAT-D(20)+ NAT-D(20)+(0)304
[IKEv1]:IP = 10.0.0.2IKE
[IKEv1]:IP = 10.0.0.2ISA_KE
[IKEv1]:IP = 10.0.0.2
[IKEv1]:IP = 10.0.0.2VID
[IKEv1]:IP = 10.0.0.2Cisco UnityVID
MM4 [IKEv1]:IP = 10.0.0.2VID
NAT-D iniatorNAT [IKEv1]:IP = 10.0.0.2DPD VID
NAT [IKEv1]:IP = 10.0.0.2VID
[IKEv1]:IP = 10.0.0.2IOS/PIXID(1.0.000000f7f)
DH KEnitiator“B”“s” [IKEv1]:IP = 10.0.0.2VID
[IKEv1]:IP = 10.0.0.2xauth V6 VID
[IKEv1]:IP = 10.0.0.2NAT
[IKEv1]:IP = 10.0.0.2NAT
[IKEv1]:IP = 10.0.0.2NAT
[IKEv1]:IP = 10.0.0.2NAT
[IKEv1]:IP = 10.0.0.2tunnel_group 10.0.0.2
10.0.0.2 L2L“s” [IKEv1]:= 10.0.0.2,IP = 10.0.0.2……
MM5 [IKEv1]:= 10.0.0.2,IP = 10.0.0.2ID
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2

crypto isakmp identity auto

[IKEv1]:= 10.0.0.2,IP = 10.0.0.2ISAKMP
[IKEv1]:IP = 10.0.0.2IOSproposal=32767/32767
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2dpd vid
[IKEv1]:IP = 10.0.0.2IKE_DECODE(msgid=0):HDR + ID(5)+ HASH(8)+ IOS(128)+ VENDOR(13)+ NONE(0)96
==========

MM5

NATNAT-T

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

[IKEv1]:IP = 10.0.0.2IKE_DECODE RECEIVED (msgid=0):HDR + ID(5)+ HASH(8)+ NONE(0)64

MM5 r(ID)c

[IKEv1]:= 10.0.0.2,IP = 10.0.0.2ID
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2,ID_IPV4_ADDR ID 10.0.0.2
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2ISAKMP
[IKEv1]:= 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

MM5

10.0.0.2ipsec-l2l

NAT-T

[IKEv1]:= 10.0.0.2,IP = 10.0.0.2ID
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2ISAKMP
[IKEv1]:IP = 10.0.0.2IOSproposal=32767/32767
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2dpd vid
[IKEv1]:IP = 10.0.0.2IKE_DECODE(msgid=0):HDR + ID(5)+ HASH(8)+ IOS(128)+ VENDOR(13)+ NONE(0)96

MM6

<==========

MM6

[IKEv1]:IP = 10.0.0.2IKE_DECODE RECEIVED(msgid=0):HDR + ID(5)+ HASH(8)+ NONE(0)64

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

1
isakmp

crypto isakmp10
authentication pre-share
3des
hash sha
2
lifetime 86400
ciscoasa# shisakmp
crypto isakmp identity auto

MM6
rf

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

1
ISAKMP
c
10.0.0.2ipsec-l2l
10.0.0.2 ipsec
cisco

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

IPSEC:0x53FC3C00SA
SCB:0x53F90A00,

2

SPI:0xFD2D851F

ID:0x00006000
VPIF:0x00000003
l2l
es
240
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2,IKESPI:SPI = 0xfd2d851f
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2,Oakley
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2IPSec SA
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2IPSecnonce
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2ID
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2ID:
:192.168.1.0255.255.255.010
:192.168.2.0255.255.255.010
(192.168.1.0/24)(192.168.2.0/24)
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2,IKE
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2qm
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2,IKE1QM:msg id = 7b80c2b0
[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)200
==========QM1==========

QM1
IDIP

crypto ipsec transform-set TRANSFORM esp-aes esp-sha-hmac
access-list VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.0

QM1

[IKEv1]:IP = 10.0.0.2,IKEQM: ms id = 52481cf5
[IKEv1]:IP = 10.0.0.2,IKE_DECODE RECEIVED(msgid=52481cf5)HDR + HASH(8)+ SA(1)+ NONCE(10)+ ID(5)+ ID(5)+ NONE(0)172

QM1
2(QM)

QM1
IP
crypto ipsec transform-set TRANSFORM esp-aes esp-sha-hmac
access-list VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.0
MAP 10VPN

[IKEv1]:= 10.0.0.2,IP = 10.0.0.2
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2SA
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2ID
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2,ID_IPV4_ADDR_SUBNET ID received - 192.168.2.0 - 255.255.0[IKEv1]:= 10.0.0.2,IP = 10.0.0.2,IDIP192.168.2.0 255.255.255.010
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2ID
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2,ID_IPV4_ADDR_SUBNET ID received - 192.168.1.0 - 255.255.0
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2,IDIP192.168.1.0255.255.255.010
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2,QMSAaddr
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2= MAPseq = 10...
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2MAP,= 10
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2IKE
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2IPSec SA
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2,IPSec SA11IPSec SA10
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2,IKE:SPI!
IPSEC:0x53FC3698SA
SCB:0x53FC2998,

(192.168.2.0/24
192.168.1.0/24)

SPI:0x1698CAC7
ID:0x00004000
VPIF:0x00000003
l2l
es
240
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2,IKESPI:SPI = 0x1698cac7
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2,Oakley
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2IPSec SA

QM2
c ACL

[IKEv1]:= 10.0.0.2,IP = 10.0.0.2IPSecnonce
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2ID
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2ID:
:192.168.2.0255.255.255.010
:192.168.1.0255.255.255.010
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2qm
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2,IKE Responder2QM:msg id = 52481cf5
[IKEv1]:IP = 10.0.0.2,IKE_DECODE(msgid=52481cf5)HDR + HASH(8)+ SA(1)+ NONCE(10)+ ID(5)+ ID(5)+ NONE(0)172 QM2

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

[IKEv1]:IP = 10.0.0.2,IKE_DECODE RECEIVED(msgid=7b80c2b0)HDR + HASH(8)+ SA(1)+ NONCE(10)+ ID(5)+ ID(5)+ NOTIFY(11)+ NONE(0) QM2
200
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2SA
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2ID
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2,ID_IPV4_ADDR_SUBNET ID received - 192.168.1.0 - 255.255.0
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2ID
QM2
r
2
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2,ID_IPV4_ADDR_SUBNET ID received - 192.168.2.0 - 255.255.0
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2
[IKEv1]:SPI[4]|
[IKEv1]:0000DDE50931 80010001 00020004 00000E10 ...1.....
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2IPSec288003600
ASAIPSEC
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2IPSEC SA
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2,NPMAP 10ACL VPN:
“MAP”10“VPN” cs_id=53f11198;rule=53f11a90
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2
IPSEC:0x53FC3698SA
SCB:0x53F910F0,

SPI:0xDDE50931
ID:0x00006000
VPIF:0x00000003
l2l
es
240
IPSEC:OBSASPI 0xDDE50931
IPSEC:VPNSPI 0xDDE50931
:0x00000005
SA:0x53FC3698
SPI:0xDDE50931
SPI 0xfd2d851f MTU:1500
0xdde50931 VCID:0x00000000
0x00000000
SCB:0x01CF218F
:0x4C69CB80
IPSEC:VPNSPI 0xDDE50931
VPN0x000161A4
IPSEC:SPI 0xDDE50931
:192.168.1.0
255.255.255.0
:192.168.2.0
255.255.255.0

0
0
Op:

0
0
Op:
1

SPI:0x00000000
SPI:
IPSEC:SPI 0xDDE50931
ID:0x53FC3AD8
IPSEC:SPI 0xDDE50931
:10.0.0.1
255.255.255.255
:10.0.0.2
255.255.255.255

0
0
Op:

0
0
Op:
50

SPI:0xDDE50931
SPI:
IPSEC:SPI 0xDDE50931
ID:0x53F91538
[IKEv1]:= 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 = 0xfd2d851fSPI =
0xdde50931
IPSEC:IBSASPI 0xFD2D851F
IPSEC:VPNSPI 0xFD2D851F
:0x00000006
SA:0x53FC3C00
SPI:0xFD2D851F
MTU:0 bytes
VCID:0x00000000
0x000161A4
SCB:0x01CEA8EF
:0x4C69CB80
IPSEC:VPNSPI 0xFD2D851F
VPN0x00018BBC
IPSEC:VPN0x000161A4,SPI 0xDDE50931
:0x00000005
SA:0x53FC3698
QM3 SPI:0xDDE50931
SPI 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
:192.168.2.0
255.255.255.0
:192.168.1.0
255.255.255.0

0
0
Op:

0
0
Op:
1

SPI:0x00000000
SPI:
IPSEC:SPI 0xFD2D851F
ID:0x53F91970
IPSEC:SPI 0xFD2D851F
:10.0.0.2
255.255.255.255
:10.0.0.1
255.255.255.255

0
0
Op:

0
0
Op:
50

SPI:0xFD2D851F
SPI:
IPSEC:SPI 0xFD2D851F
ID:0x53F91A08
IPSEC:SPI 0xFD2D851F
:10.0.0.2
255.255.255.255
:10.0.0.1
255.255.255.255

0
0
Op:

0
0
Op:
50

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

==========QM3==========
==========
[IKEv1]:IP = 10.0.0.2,IKE_DECODE(msgid=7b80c2b0) [IKEv1]:IP =
HDR + HASH(8)+ NONE(0)76 10.0.0.2,IKE_DE
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2,IKESAKEY_ADD:SPI CODE
2 = 0xdde50931 RECEIVED QM3
SPI [IKEv1]:= 10.0.0.2,IP = 10.0.0.2KEY_UPDATEspi (msgid=52481cf5)
0xfd2d851f HDR +
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2P23060 . HASH(8)+
[IKEv1]:= 10.0.0.2,IP = 10.0.0.22(msgid=7b80c2b0) NONE(0)52

[IKEv1]:= 10.0.0.2,IP = 10.0.0.2
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2IPSEC SA
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2
[IKEv1]:= 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
IPSEC:0x53F18B00SA
SCB:0x53F8A1C0,

SPI:0xDB680406
ID:0x00004000
VPIF:0x00000003
l2l
es
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
:192.168.1.0
255.255.255.0
:192.168.2.0 QM3
255.255.255.0 SA

0 SPI
0
Op:

0
0
Op:
1

SPI:0x00000000
SPI:
IPSEC:SPI 0xDB680406
ID:0x53F89160
IPSEC:SPI 0xDB680406
:10.0.0.1
255.255.255.255
:10.0.0.2
255.255.255.255

0
0
Op:

0
0
Op:
50

SPI:0xDB680406
SPI:
IPSEC:SPI 0xDB680406

ID:0x53E47E88
[IKEv1]:= 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]:= 10.0.0.2,IP = 10.0.0.2,IKESAKEY_ADD:SPI = 0xdb680406
IPSEC:IBSASPI 0x1698CAC7
IPSEC:VPNSPI 0x1698CAC7
:0x00000006
SA:0x53FC3698
SPI:0x1698CAC7
MTU:0 bytes
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
ID:0x53F89160
IPSEC:SPDSPI 0xDB680406
ID:0x53E47E88
IPSEC:SPI 0x1698CAC7 SPISA
:192.168.2.0
255.255.255.0
:192.168.1.0
255.255.255.0

0
0
Op:

0
0
Op:
1

SPI:0x00000000
SPI:
IPSEC:SPI 0x1698CAC7
ID:0x53FC3E80
IPSEC:SPI 0x1698CAC7
:10.0.0.2
255.255.255.255
:10.0.0.1
255.255.255.255

0
0
Op:

0
0

Op:
50

SPI:0x1698CAC7
SPI:
IPSEC:SPI 0x1698CAC7
ID:0x53FC3F18
IPSEC:SPI 0x1698CAC7
:10.0.0.2
255.255.255.255
:10.0.0.1
255.255.255.255

0
0
Op:

0
0
Op:
50

SPI:0x1698CAC7
SPI:
IPSEC:SPI 0x1698CAC7
ID:0x53F8AEA8
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2KEY_UPDATEspi 0x1698cac7
[IKEv1]:= 10.0.0.2,IP = 10.0.0.2P23060 . IPsec
[IKEv1]:= 10.0.0.2,IP = 10.0.0.22(msgid=52481cf5) 2/

隧道验证

注意：由于ICMP用于触发隧道，因此只有一个IPSec SA处于启用状态。协议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

相关信息

- 一个好的起点是 关于IPSec的维基百科条目。标准和参考包含许多有用的信息
- IPSec故障排除：了解和使用debug命令
- **技术支持和文档 - Cisco Systems**