主模式)排除故障TechNote的ASA IPsec和IKE调试(IKEv1

目录

简介

本文描述在可适应安全工具(ASA)的调试，当使用主模式和预先共享密钥(PSK)时。某些调试线路的转换到配置里也讨论。

在本文没讨论的主题包括通过流量在通道以后设立了和IPsec或Internet Key Exchange (IKE)基本概念。

先决条件

要求

本文读者应该有这些主题知识。

- 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：

- 思科ASA 9.3.2
- 运行Cisco IOS 12.4T的路由器

核心问题

IKE和IPsec调试有时隐秘，但是您能使用他们了解IPSec VPN隧道建立问题哪里查找。

方案

当证书使用验证时，主模式典型地使用在LAN-to-LAN隧道之间或，一旦远程访问(EzVPN)。

调试是从运行软件版本9.3.2的两ASA。两个设备将形成LAN-to-LAN隧道。

两个主要方案描述：

- ASA作为IKE的发起者
- ASA作为IKE的响应方

使用的调试指令

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 [IKEv1] IP = 10.0.0.2 IKE1Intf IKE10.0.0.2192.168.1.0192.168.2.0(MAP)	
MM1 IKENAT-T	[IKEv1] IP = 10.0.0.2**SA ISAKMP**[IKEv1] IP = 10.0.0.2NATVID Ver 02 [IKEv1] IP = 10.0.0.2NATVID Ver 03 [IKEv1] IP = 10.0.0.2NATVID Ver RFC [IKEv1] IP = 10.0.0.2VID +	
MM1	[IKEv1] IP = 10.0.0.2(msgid=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] 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 [IKEv1] IP = 10.0.0.2VID [IKEv1] IP = 10.0.0.2VID [IKEv1] IP = 10.0.0.2NATVer 03 VID [IKEv1] IP = 10.0.0.2VID [IKEv1] IP = 10.0.0.2NATVer 02 VID [IKEv1] IP = 10.0.0.2SA IKE [IKEv1] IP = 10.0.0.2 SA IKE# 1# 1IKE# 2	MM1 ISAKMP/IKE NAT-T *crypto isakmp policy 10* ***authentication pre-share*** *3des* ***hash sha*** *2* *86400*
	[IKEv1] IP = 10.0.0.2SA ISAKMP [IKEv1] IP = 10.0.0.2NATVID Ver 02 [IKEv1] IP = 10.0.0.2VID +	MM2 ISAKMP NAT-T
	[IKEv1] IP = 10.0.0.2(msgid=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] 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 includesNATDiffie-Hellman (DH)(KE) (initatorgpA)DPD	30 10:38:29 [IKEv1] IP = 10.0.0.2ke 30 10:38:29 [IKEv1] IP = 10.0.0.2 30 10:38:29 [IKEv1] IP = 10.0.0.2Cisco Unity VID 30 10:38:29 [IKEv1] IP = 10.0.0.2Xauth V6 VID 30 10:38:29 [IKEv1] IP = 10.0.0.2IOS VID 30 10:38:29 [IKEv1] IP = 10.0.0.2ASA IOSID(1.0.020000001) 30 10:38:29 [IKEv1] IP = 10.0.0.2VID 30 10:38:29 [IKEv1] IP = 10.0.0.2Altiga /Cisco VPN3000/Cisco ASA GW VID	

30 10:38:29 [IKEv1] IP = 10.0.0.2Nat
30 10:38:29 [IKEv1] IP = 10.0.0.2NAT
30 10:38:29 [IKEv1] IP = 10.0.0.2Nat
30 10:38:29 [IKEv1] IP = 10.0.0.2NAT
MM3 [IKEv1] IP = 10.0.0.2(msgid=0)IKE_DECODE HDR + KE (4) + NONCE (10) +(13) +(13) +(13) +(13) + NAT-D (20) + NAT-D (20) +(0)304
==========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] IP = 10.0.0.2ke
[IKEv1] IP = 10.0.0.2ISA_KE
[IKEv1] IP = 10.0.0.2NONCE
[IKEv1] IP = 10.0.0.2VID
[IKEv1] IP = 10.0.0.2DPD VID MM3
[IKEv1] IP = 10.0.0.2VID NAT-DinitatorNAT
[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 = 10.0.0.2
[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 = 10.0.0.2ASA IOSID(1.0.020000001) NAT DH KE“B””s” (
[IKEv1] IP = 10.0.0.2VID “B”initator)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_group10.0.0.2
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2… 10.0.0.2 L2L“s”
[IKEv1] IP = 10.0.0.2(msgid=0)IKE_DECODE HDR + KE (4) + NONCE (10) +(13) +(13) +(13) +(13) + NAT-D (130) + NAT-D (130) +(0)304 MM4
<==========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
[IKEv1] IP = 10.0.0.2ike
[IKEv1] IP = 10.0.0.2ISA_KE
[IKEv1] IP = 10.0.0.2NONCE
[IKEv1] IP = 10.0.0.2VID
[IKEv1] IP = 10.0.0.2Cisco UnityVID
MM4 [IKEv1] IP = 10.0.0.2VID
NAT-D initatoriniator [IKEv1] IP = 10.0.0.2DPD VID
NATNAT [IKEv1] IP = 10.0.0.2VID
[IKEv1] IP = 10.0.0.2IOS/PIXID(1.0.000000f7f)
DH KE“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
10.0.0.2 L2L“s” [IKEv1] IP = 10.0.0.2tunnel_group10.0.0.2
initator [IKEv1] Group= 10.0.0.2 IP = 10.0.0.2…
MM5 [IKEv1] Group= 10.0.0.2 IP = 10.0.0.2ID
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2 ISAKMP
crypto isakmp [IKEv1] IP = 10.0.0.2IOSproposal=32767/32767

MM5

[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2dpd vid
[IKEv1] IP = 10.0.0.2(msgid=0)IKE_DECODE HDR + ID (5) + HASH (8)
+ IOS KEEPALIVE (128) +VENDOR (13) +(0)96
==========MM5==========
====>

NATNAT-T

[IKEv1] Group=
10.0.0.2 IP =
10.0.0.2NATNAT
NAT

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

MM5
(ID)

[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2ID
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2ID_IPV4_ADDR ID
10.0.0.2
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2 ISAKMP
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2,Automatic NAT
[IKEv1] IP = 10.0.0.2tunnel_group10.0.0.2
NATNAT

MM5
;
10.0.0.2ipsec-l2l
NAT-T

[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2ID
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2 ISAKMP
[IKEv1] IP = 10.0.0.2IOSproposal=32767/32767
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2dpd vid
[IKEv1] IP = 10.0.0.2(msgid=0)IKE_DECODE HDR + ID (5) + HASH (8)
+ IOS KEEPALIVE (128) +VENDOR (13) +(0)96
<==========MM6==========
=====

MM6
MM6

1
isakmp

crypto isakmp policy
10
authentication pre-
share
3des
hash sha
2
86400
ciscoasa # sh run
crypto isakmp
crypto isakmp

MM6

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

[IKEv1] Group= 10.0.0.2 IP =
10.0.0.21
[IKEv1] IP = 10.0.0.2keep-aliveDPD
[IKEv1] Group= 10.0.0.2 IP =
10.0.0.2P164800

[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2ID
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2ID_IPV4_ADDR ID
10.0.0.2
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2 ISAKMP
[IKEv1] IP = 10.0.0.2tunnel_group10.0.0.2
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2 Oakley
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2QMIKEid= 7b80c2b0

1
ISAKMP

10.0.0.2ipsec-l2l
10.0.0.2 ipsec
cisco

[IKEv1] Group= 10.0.0.2 IP = 10.0.0.21
[IKEv1] IP = 10.0.0.2keep-aliveDPD
DPD1
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2P182080

IPSEC SA@ 0x53FC3C00
SCB 0x53F90A00

2()

SPI 0xFD2D851F
ID:0x00006000
VPIF 0x00000003

l2l

240
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2 IKESPI SPI = 0xfd2d851f
QM1 [IKEv1] Group= 10.0.0.2 IP = 10.0.0.2 oakley constucting
IDIPsec [IKEv1] Group= 10.0.0.2 IP = 10.0.0.2
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2SA IPSec
esp-sha-hmac crypto [IKEv1] Group= 10.0.0.2 IP = 10.0.0.2IPSec
ipsec transform-set [IKEv1] Group= 10.0.0.2 IP = 10.0.0.2ID
ESP aes [IKEv1] Group= 10.0.0.2 IP = 10.0.0.2Id
VPNpermit icmp 192.168.1.0255.255.255.01 Port0
192.168.1.0 192.168.2.0255.255.255.01 Port0
255.255.255.0 (192.168.1.0/24)expcted(192.168.2.0/24)
192.168.2.0 [IKEv1] Group= 10.0.0.2 IP = 10.0.0.2IKE
255.255.255.0 [IKEv1] Group= 10.0.0.2 IP = 10.0.0.2qm
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.21 QM pktIKEid= 7b80c2b0
QM1 [IKEv1] IP = 10.0.0.2(msgid=7b80c2b0)IKE_DECODE HDR + HASH (8)
+ SA (1) + NONCE (10) + ID (5) + ID (5) +(11) +(0)200
==========QM1==========
====>
[IKEv1] IP = 10.0.0.2QMIKE id= 52481cf5
QM1
[IKEv1] IP = 10.0.0.2 IKE_DECODE(msgid=52481cf5)HDR + HASH (8) 2(QM)
+ SA (1) + NONCE (10) + ID (5) + ID (5) +(0)172
QM1
IPsec
esp-sha-hmac crypto
ipsec transform-set
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2 ESP aes
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2SA VPNpermit icmp
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2NONCE 192.168.1.0
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2ID 255.255.255.0
192.168.2.0
255.255.255.0
MAP 10VPN
[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
IDIP192.168.2.0255.255.255.01 Port0
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2ID (192.168.2.0/24
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2 ID_IPV4_ADDR_SUBNET ID 192.168.1.0/24)
received--192.168.1.0--255.255.255.0
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2IDIP192.168.1.0255.255.255.01
Port0
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2QM IsRekeyedsa
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2= MAP= 10…
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2MAP= 10 crypto
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2IKEMAP
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2SA IPSec
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2 SA IPSec# 1# 1SA IPSec# 10
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2 IKE SPI!
IPSEC SA@ 0x53FC3698
SCB 0x53FC2998

SPI 0x1698CAC7
ID:0x00004000
VPIF 0x00000003
l2l QM2
ACL

240
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2 IKESPI SPI = 0x1698cac7
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2oakley
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2SA IPSec
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2IPSec

[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2ID
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2Id
192.168.2.0255.255.255.01 Port0
192.168.1.0255.255.255.01 Port0
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2qm
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.22 QM pktIKEid= 52481cf5
[IKEv1] IP = 10.0.0.2(msgid=52481cf5)IKE_DECODE HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) +(0)172 QM2

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

QM2

[IKEv1] IP = 10.0.0.2 IKE_DECODE(msgid=7b80c2b0)HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) +(11) +(0)200
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2SA
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2NONCE
[IKEv1] Group= 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

QM2

[IKEv1] Group= 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--192.168.2.0--255.255.255.0

2

[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2
[IKEv1] (outb SPI[4]lattributes)
[IKEv1] 0000 DDE50931 80010001 0002000400000E10… 1 .....
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2IPSec288003600
ASAIPSEC
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2IPSec SAS
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2!

“MAP”10access-list “VPN”

[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2 NPMAP 10ACL VPN cs_id=53f11198;rule=53f11a90
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2!
IPSEC SA@ 0x53FC3698
SCB 0x53F910F0

SPI 0xDDE50931
ID:0x00006000
VPIF 0x00000003
l2l

240
IPSEC OBSA SPI 0xDDE50931
IPSEC VPN SPI 0xDDE50931
0x00000005
SA 0x53FC3698
SPI 0xDDE50931
MTU:1500

0xfd2d851f 0xdde50931for

VCID 0x00000000
0x00000000
SCB 0x01CF218F
0x4C69CB80
IPSEC VPN SPI 0xDDE50931
VPN0x000161A4
IPSEC SPI 0xDDE50931
Src192.168.1.0
Src255.255.255.0
Dst192.168.2.0
Dst255.255.255.0
Src
0
0

Dst
0
0

1

SPI 0x00000000
SPI
IPSEC SPI 0xDDE50931
ID 0x53FC3AD8
IPSEC permit SPI 0xDDE50931
Src10.0.0.1
Src255.255.255.255
Dst10.0.0.2
Dst255.255.255.255
Src
0
0

Dst
0
0

50

SPI 0xDDE50931
SPI
IPSEC permit SPI 0xDDE50931
ID 0x53F91538
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2 NPMAP 10ACL VPN
cs_id=53f11198;rule=53f11a90
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2LANLAN(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
0x000161A4
SCB 0x01CEA8EF
0x4C69CB80
IPSEC VPN SPI 0xFD2D851F
VPN0x00018BBC
IPSEC VPN0x000161A4 SPI 0xDDE50931
0x00000005
SA 0x53FC3698
SPI 0xDDE50931
QM3 MTU:1500
VCID 0x00000000
0x00018BBC
SCB 0x01CF218F
0x4C69CB80
IPSEC VPN SPI 0xDDE50931
VPN0x000161A4
IPSEC SPI 0xDDE50931
ID 0x53FC3AD8
IPSEC SPD SPI 0xDDE50931
ID 0x53F91538
IPSEC SPI 0xFD2D851F
Src192.168.2.0
Src255.255.255.0
Dst192.168.1.0
Dst255.255.255.0
Src
0

0

Dst
0
0

1

SPI 0x00000000
SPI
IPSEC SPI 0xFD2D851F
ID 0x53F91970
IPSEC SPI 0xFD2D851F
Src10.0.0.2
Src255.255.255.255
Dst10.0.0.1
Dst255.255.255.255
Src
0
0

Dst
0
0

50

SPI 0xFD2D851F
SPI
IPSEC SPI 0xFD2D851F
ID 0x53F91A08
IPSEC permit SPI 0xFD2D851F
Src10.0.0.2
Src255.255.255.255
Dst10.0.0.1
Dst255.255.255.255
Src
0
0

Dst
0
0

50

SPI 0xFD2D851F
SPI
IPSEC permit SPI 0xFD2D851F
ID 0x53F91AA0

QM3 [IKEv1] Group= 10.0.0.2 IP = 10.0.0.23 QM pktIKEid= 7b80c2b0

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

====>

[IKEv1] IP = 10.0.0.2(msgid=7b80c2b0)IKE_DECODE
HDR + HASH (8) +(0)76
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2 IKESA
KEY_ADDSPI = 0xdde50931
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2KEY_UPDATE
spi 0xfd2d851f
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2P23060
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.22
(msgid=7b80c2b0)

[IKEv1] IP = 10.0.0.2 IKE_DECODE (msgid=52481cf5) HDR + HASH (8) +(0)52 QM3 receivd fom 2 SPI

[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2 QM
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2IPSec SAS SAS

[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2!
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2 NPMAP 10ACL VPN
cs_id=53f11198;rule=53f11a90
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2!
IPSEC SA@ 0x53F18B00
SCB 0x53F8A1C0

SPI 0xDB680406
ID:0x00004000
VPIF 0x00000003
l2l

240
IPSEC OBSA SPI 0xDB680406
IPSEC VPN SPI 0xDB680406
0x00000005
SA 0x53F18B00
SPI 0xDB680406
MTU:1500
VCID 0x00000000
0x00000000
SCB 0x005E4849
0x4C69CB80
IPSEC VPN SPI 0xDB680406
VPN0x0000E9B4
IPSEC SPI 0xDB680406
Src192.168.1.0
Src255.255.255.0
Dst192.168.2.0
Dst255.255.255.0
Src
0
0

Dst
0
0

1

SPI 0x00000000
SPI
IPSEC SPI 0xDB680406
ID 0x53F89160
IPSEC permit SPI 0xDB680406
Src10.0.0.1
Src255.255.255.255
Dst10.0.0.2
Dst255.255.255.255
Src
0
0

Dst
0
0

50

SPI 0xDB680406
SPI
IPSEC permit SPI 0xDB680406
ID 0x53E47E88
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2 NPMAP 10ACL VPN

cs_id=53f11198;rule=53f11a90
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2LANLAN(10.0.0.2)SPI =
0x1698cac7SPI = 0xdb680406
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2 IKESAKEY_ADDSPI =
0xdb680406
IPSEC IBSA SPI 0x1698CAC7
IPSEC VPN SPI 0x1698CAC7
0x00000006
SA 0x53FC3698
SPI 0x1698CAC7
MTU:0
VCID 0x00000000
0x0000E9B4
SCB 0x005DAE51
0x4C69CB80
IPSEC VPN SPI 0x1698CAC7
VPN0x00011A8C
IPSEC VPN0x0000E9B4 SPI 0xDB680406
0x00000005
SA 0x53F18B00
SPI 0xDB680406
MTU:1500
VCID 0x00000000
0x00011A8C
SCB 0x005E4849
0x4C69CB80
IPSEC VPN SPI 0xDB680406
VPN0x0000E9B4
IPSEC SPI 0xDB680406
ID 0x53F89160
IPSEC SPD SPI 0xDB680406
ID 0x53E47E88
IPSEC SPI 0x1698CAC7 SAS
Src192.168.2.0
Src255.255.255.0
Dst192.168.1.0
Dst255.255.255.0
Src
0
0

Dst
0
0

1

SPI 0x00000000
SPI
IPSEC SPI 0x1698CAC7
ID 0x53FC3E80
IPSEC SPI 0x1698CAC7
Src10.0.0.2
Src255.255.255.255
Dst10.0.0.1
Dst255.255.255.255
Src
0
0

Dst
0
0

50

SPI 0x1698CAC7
SPI
IPSEC SPI 0x1698CAC7
ID 0x53FC3F18
IPSEC permit SPI 0x1698CAC7
Src10.0.0.2
Src255.255.255.255
Dst10.0.0.1
Dst255.255.255.255
Src
0
0

Dst
0
0

50

SPI 0x1698CAC7
SPI
IPSEC permit SPI 0x1698CAC7
ID 0x53F8AEA8
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2KEY_UPDATE spi 0x1698cac7
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.2P23060 IPsec
[IKEv1] Group= 10.0.0.2 IP = 10.0.0.22(msgid=52481cf5) 2/

通道验证

Note:因为ICMP用于触发通道，只有一IPSec SA是UP。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

- 开始的合适场所是在IPSec的wikipedia条款。 英文虎报和参考包含很多有用的信息
- IPSec故障排除：了解和使用调试指令
- **技术支持和文档 - Cisco Systems**