ASA IPsec 및 IKE 디버깅(IKEv1 기본 모드) 문제 해결 TechNote

목차

소개

이 문서에서는 주 모드와 PSK(pre-shared key)가 모두 사용되는 경우 ASA(Adaptive Security Appliance)의 디버그에 대해 설명합니다.특정 디버그 행을 컨피그레이션으로 변환하는 방법도 설명합니다.

이 문서에서 다루지 않는 항목에는 터널이 설정된 후 트래픽을 전달하는 것과 IPsec 또는 IKE(Internet Key Exchange)의 기본 개념이 포함되어 있습니다.

사전 요구 사항

요구 사항

이 문서의 독자는 이러한 주제에 대해 알고 있어야 합니다.

- PSK
- IKE

사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- Cisco ASA 9.3.2
- Cisco IOS® 12.4T를 실행하는 라우터

핵심 문제

IKE 및 IPsec 디버그는 종종 암호이지만 IPsec VPN 터널 설정 문제가 있는 위치를 파악하는 데 사

용할 수 있습니다.

시나리오

주 모드는 일반적으로 LAN-to-LAN 터널 간에 사용되며, 원격 액세스(EzVPN)의 경우 인증에 인증서를 사용할 때 사용됩니다.

소프트웨어 버전 9.3.2을 실행하는 두 ASA의 디버그입니다. 두 디바이스는 LAN-to-LAN 터널을 형성합니다.

두 가지 주요 시나리오는 다음과 같습니다.

- ASA를 IKE의 개시자로 사용
- ASA를 IKE의 응답자로 사용

사용된 디버그 명령

debug crypto ikev1 127

debug crypto ipsec 127

ASA 컨피그레이션

IPsec 구성:

```
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 구성:

```
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 컨피그레이션:

```
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
```

디버깅

.
MM_NO_STATE .
ASA .

[IKEv1]:: (spi 0x0) .
IPSEC(crypto_map_check)-3:5 :=1, sadr=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, IKE : 1, Intf inside, IKE 10.0.0.2 192.168.1.0,
192.168.2.0, (MAP)

MM1
ncludes iIKE s
NAT-T

[IKEv1]:IP = 10.0.0.2, ISAKMP **SA** [IKEv1 DEBUG]:IP = 10.0.0.2,
NAT-Traversal VID 02
[IKEv1]:IP = 10.0.0.2, NAT-Traversal VID 03
[IKEv1]:IP = 10.0.0.2, NAT-Traversal VID over RFC
[IKEv1]:IP = 10.0.0.2, VID +

MM1 .

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

==========MM1==========
==========

[IKEv1]:IP = 10.0.0.2, IKE_DECODE RECEIVED (msgid=0) :HDR +
SA(1) + (13) +(13) + (13) + (13) + (0) :164

MM1 .

[IKEv1]:IP = 10.0.0.2, SA
[IKEv1]:IP = 10.0.0.2, Oakley
[IKEv1]:IP = 10.0.0.2, VID
[IKEv1]:IP = 10.0.0.2, NAT-Traversal RFC VID
[IKEv1]:IP = 10.0.0.2, VID
[IKEv1]:IP = 10.0.0.2, VID
[IKEv1]:IP = 10.0.0.2, NAT-Traversal ver 03 VID
[IKEv1]:IP = 10.0.0.2, VID
[IKEv1]:IP = 10.0.0.2, NAT-Traversal ver 02 VID
[IKEv1]:IP = 10.0.0.2, IKE SA
[IKEv1]:IP = 10.0.0.2, IKE SA Proposal # 1, Transform # 1 acceptable
Matches global IKE entry # 2

MM1.
ISAKMP/IKE .
NAT-T .
:
crypto isakmp 10
3des
sha
2
86400

[IKEv1]:IP = 10.0.0.2, ISAKMP SA
[IKEv1]:IP = 10.0.0.2, NAT-Traversal VID 02
[IKEv1]:IP = 10.0.0.2, VID +
[IKEv1]:IP = 10.0.0.2, IKE_DECODE (msgid=0) :HDR + SA(1) + (13) +
(13) + (0) :128

MM2.
isakmp . NAT-
T .

MM2 .

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

MM2 .

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

MM2.

[IKEv1]:IP = 10.0.0.2, SA
[IKEv1]:IP = 10.0.0.2, Oakley
[IKEv1]:IP = 10.0.0.2, VID
[IKEv1]:IP = 10.0.0.2, NAT-Traversal RFC VID

MM3 .
ncludesNAT , -

11 30 10:38:29 [IKEv1 DEBUG]:IP = 10.0.0.2,
11 30 10:38:29 [IKEv1 DEBUG]:IP = 10.0.0.2, nonce

11 30 10:38:29 [IKEv1 DEBUG]:IP = 10.0.0.2, Cisco Unity VID
11 30 10:38:29 [IKEv1 DEBUG]:IP = 10.0.0.2, xauth V6 VID
11 30 10:38:29 [IKEv1 DEBUG]:IP = 10.0.0.2, IOS VID
11 30 10:38:29 [IKEv1 DEBUG]:IP = 10.0.0.2, ASA IOS ID (:1.0.0,
DH(Hellman) KE(Key :20000001)
Exchange) (i)nitator g, 11 30 10:38:29 [IKEv1 DEBUG]:IP = 10.0.0.2, VID
p A to responder 11 30 10:38:29 [IKEv1 DEBUG]:IP = 10.0.0.2, Send Altiga/Cisco
), DPD . VPN3000/Cisco ASA GW VID
11 30 10:38:29 [IKEv1 DEBUG]:IP = 10.0.0.2, NAT-Discovery
11 30 10:38:29 [IKEv1 DEBUG]:IP = 10.0.0.2, NAT
11 30 10:38:29 [IKEv1 DEBUG]:IP = 10.0.0.2, NAT-Discovery
11 30 10:38:29 [IKEv1 DEBUG]:IP = 10.0.0.2, NAT
[IKEv1]:IP = 10.0.0.2, IKE_DECODE (msgid=0) :HDR + KE (4) +
MM3 . NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-
D (20) + NAT-D (20) + NONE (0) :304
==========MM3==========
==========>
[IKEv1]:IP = 10.0.0.2, IKE_DECODE RECEIVED (msgid=0) :HDR + KE
(4) + NONCE (10) + VENDOR (13) + VENDOR (13) + NAT-D (130) + MM3 .
NAT-D (130) + NONE (0) :284
[IKEv1]:IP = 10.0.0.2,
[IKEv1]:IP = 10.0.0.2, ISA_KE
[IKEv1]:IP = 10.0.0.2, nonce
[IKEv1]:IP = 10.0.0.2, VID
[IKEv1]:IP = 10.0.0.2, DPD VID MM3.
[IKEv1]:IP = 10.0.0.2, VID NAT-D Initator NAT
[IKEv1]:IP = 10.0.0.2, IOS/PIX ID (:1.0.0, :00000f6f) responder NAT .
[IKEv1]:IP = 10.0.0.2, VID DH KE p, g A .
[IKEv1]:IP = 10.0.0.2, Received xauth V6 VID
[IKEv1]:IP = 10.0.0.2, NAT
[IKEv1]:IP = 10.0.0.2, NAT
[IKEv1]:IP = 10.0.0.2, NAT
[IKEv1]:IP = 10.0.0.2, NAT
[IKEv1]:IP = 10.0.0.2,
[IKEv1]:IP = 10.0.0.2, nonce
[IKEv1]:IP = 10.0.0.2, Cisco Unity VID
[IKEv1]:IP = 10.0.0.2, xauth V6 VID
[IKEv1]:IP = 10.0.0.2, IOS VID MM4 .
[IKEv1]:IP = 10.0.0.2, ASA IOS ID (:1.0.0, :20000001) ncludes NAT , DH
[IKEv1]:IP = 10.0.0.2, VID esponder "B" "s" (
[IKEv1]:IP = 10.0.0.2, Send Altiga/Cisco VPN3000/Cisco ASA GW VID "B"), DPD VID.
[IKEv1]:IP = 10.0.0.2, NAT-Discovery
[IKEv1]:IP = 10.0.0.2, NAT
[IKEv1]:IP = 10.0.0.2, NAT-Discovery
[IKEv1]:IP = 10.0.0.2, NAT
[IKEv1]:IP = 10.0.0.2, tunnel_group 10.0.0.2 10.0.0.2 L2L "s"
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ...
[IKEv1]:IP = 10.0.0.2, IKE_DECODE (msgid=0) :HDR + KE (4) +
NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT- MM4 .
D (130) + NAT-D (130) + NONE (0) :304
<==========MM4==========
======
[IKEv1]:IP = 10.0.0.2, IKE_DECODE RECEIVED (msgid=0) :HDR + KE
MM4 . (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
NAT-D (20) + NAT-D (20) + NONE (0) :304
[IKEv1]:IP = 10.0.0.2, ike
[IKEv1]:IP = 10.0.0.2, ISA_KE
MM4. [IKEv1]:IP = 10.0.0.2, nonce
NAT-D Initiator [IKEv1]:IP = 10.0.0.2, VID
NAT responder NAT [IKEv1]:IP = 10.0.0.2, Cisco Unity VID
. [IKEv1]:IP = 10.0.0.2, VID
[IKEv1]:IP = 10.0.0.2, DPD VID
DH KE "B" "s" . [IKEv1]:IP = 10.0.0.2, VID
[IKEv1]:IP = 10.0.0.2, IOS/PIX ID (:1.0.0, :00000f7f)

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

10.0.0.2 L2L , "s"
.

[IKEv1]:IP = 10.0.0.2, tunnel_group 10.0.0.2
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ...
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ID

MM5 .
:
crypto isakmp ID

[IKEv1]: = 10.0.0.2, IP = 10.0.0.2,
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ISAKMP
[IKEv1]:IP = 10.0.0.2, IOS keep alive :proposal=32767/32767
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, dpd vid

MM5.

[IKEv1]:IP = 10.0.0.2, IKE_DECODE (msgid=0) :HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) +VENDOR (13) + NONE (0) :96
==========MM5==========

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

Responder NAT
.NAT-T .

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

MM5 .
ncludes r ID(ID) c
.

[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ID
[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 = 10.0.0.2, ISAKMP
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2,
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, NAT
[IKEv1]:IP = 10.0.0.2, tunnel_group 10.0.0.2
: NAT . NAT .

MM5.
.
. .
:
10.0.0.2 ipsec-l2l

NAT-T .

[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ID
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2,
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ISAKMP
[IKEv1]:IP = 10.0.0.2, IOS keep alive :proposal=32767/32767
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, dpd vid
[IKEv1]:IP = 10.0.0.2, IKE_DECODE (msgid=0) :HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) +VENDOR (13) + NONE (0) :96
<==========MM6==========
======

MM6 .
ID
rekey time started
identity sent to remote
peer .

MM6 .

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

MM6 .

[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, 1
[IKEv1]:IP = 10.0.0.2, Keep-alive
:DPD
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2,
P1 :64800

1 .
isakmp rekey .
:
crypto isakmp 10

3des
sha
2
86400
ciscoasa# sh crypto
isakmp
crypto isakmp ID

[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ID
[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 = 10.0.0.2, ISAKMP
[IKEv1]:IP = 10.0.0.2, tunnel_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, IKE Initiator QM:msg id = 7b80c2b0

MM6.
ncludes r f ID

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

2( ) .

QM1 .
ID 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

QM1.

[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, 1
[IKEv1]:IP = 10.0.0.2, Keep-alive :DPD
DPD 1 .
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, P1 :82080

IPSEC:0x53FC3C00 SA,
SCB:0x53F90A00,
:
SPI:0xFD2D851F
ID:0x00006000
VPIF :0x00000003
:l2l
:esp
:240
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, IKE SPI .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 = 10.0.0.2, IPSec SA
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, IPSec nonce
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ID
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ID:
:192.168.1.0 255.255.255.0 1 0
:192.168.2.0 255.255.255.0 1 0
(192.168.1.0/24) (192.168.2.0/24) .
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, IKE Initiator
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, qm
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, QM IKE :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==========
==========>
[IKEv1]:IP = 10.0.0.2, IKE Responder QM: 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

[IKEv1]: = 10.0.0.2, IP = 10.0.0.2,
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, SA
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, nonce
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ID

[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID
received—192.168.2.0—255.255.255.0[IKEv1]: = 10.0.0.2, IP = 10.0.0.2,
ID IP . 192.168.2.0, 255.255.255.0, 1, 0
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ID
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID
—192.168.1.0—255.255.255.0
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ID IP : 192.168.1.0, 255.255.255.0,
1, 0
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, QM IsRekeyed sa addr
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, , = MAP, = 10...
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, , MAP, seq = 10
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, IKE :
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, IPSec SA

QM1 .
2(QM) .

QM1 .
IP .
: crypto ipsec
transform-set
TRANSFORM esp-
aesesp-sha-hmac
access-list VPN
extended permit 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) .

.

[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, IPSec SA 1, 1 IPSec SA 10
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, IKE:SPI !
IPSEC:0x53FC3698 SA,
SCB:0x53FC2998,
:
SPI:0x1698CAC7
ID:0x00004000
VPIF :0x00000003
:l2l
:esp
:240
QM2 .
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, IKE SPI .SPI = 0x1698cac7
ncludes c ID, ACL
[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 = 10.0.0.2, IPSec SA
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, IPSec nonce
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ID
[IKEv1]: = 10.0.0.2, IP = 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]: = 10.0.0.2, IP = 10.0.0.2, qm
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, IKE Responder QM pkt :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)
QM2 . :HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY
(11) + NONE (0) :200
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2,
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, SA
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, nonce
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ID
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID
—192.168.1.0—255.255.255.0
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ID
QM2 . [IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID
r —192.168.2.0—255.255.255.0
2 . [IKEv1]: = 10.0.0.2, IP = 10.0.0.2,
[IKEv1]:Responder Lifetime (outb SPI[4]|attributes).
[IKEv1]:0000:DDE50931 8001001 000020004 00000E10 ...1.....
[IKEv1]:Group = 10.0.0.2, IP = 10.0.0.2, Responder IPSec 28800 3600 .
ASA IPSEC . rekey
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, IPSEC SA
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, !
"MAP" 10 [IKEv1]:Group = 10.0.0.2, IP = 10.0.0.2, NP MAP 10 ACL
"VPN" . VPN:cs_id=53f11198 .=53f11a90
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, !
IPSEC:0x53FC3698 SA,
SCB:0x53F910F0,
:
SPI:0xDDE50931
ID:0x00006000
VPIF :0x00000003
SPI 0xfd2d851f :l2l
0xdde50931 . :esp
:240
IPSEC: OBSA , SPI 0xDDE50931
IPSEC: VPN , SPI 0xDDE50931
:0x00000005
SA:0x53FC3698
SPI:0xDDE50931
MTU:1500

VCID:0x00000000
:0x00000000
SCB:0x01CF218F
:0x4C69CB80
IPSEC: VPN , SPI 0xDDE50931
VPN :0x000161A4
IPSEC: , SPI 0xDDE50931
 :192.168.1.0
 :255.255.255.0
dst :192.168.2.0
 :255.255.255.0

:0
:0
Op :
Dst
:0
:0
Op :
:1
 :
SPI:0x00000000
SPI :
IPSEC: , SPI 0xDDE50931
 ID:0x53FC3AD8
IPSEC: , SPI 0xDDE50931
 :10.0.0.1
 :255.255.255.255
dst :10.0.0.2
 :255.255.255.255

:0
:0
Op :
Dst
:0
:0
Op :
:50
 :
SPI:0xDDE50931
SPI :
IPSEC: , SPI 0xDDE50931
 ID:0x53F91538
[IKEv1]:Group = 10.0.0.2, IP = 10.0.0.2, NP   MAP 10 ACL
VPN:cs_id=53f11198 .=53f11a90
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, LAN-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
:0x000161A4
SCB:0x01CEA8EF
:0x4C69CB80
IPSEC: VPN , SPI 0xFD2D851F
VPN :0x00018BBC
IPSEC: VPN 0x000161A4, SPI 0xDDE50931
:0x00000005
SA:0x53FC3698
SPI:0xDDE50931

QM3 .
SPI.

MTU:1500
VCID:0x00000000
:0x00018BBC
SCB:0x01CF218F
:0x4C69CB80
IPSEC: VPN , SPI 0xDDE50931
VPN :0x000161A4
IPSEC: , SPI 0xDDE50931
 ID:0x53FC3AD8
IPSEC: SPD , SPI 0xDDE50931
 ID:0x53F91538
IPSEC: , SPI 0xFD2D851F
 :192.168.2.0
 :255.255.255.0
dst :192.168.1.0
 :255.255.255.0

:0
:0
Op :
Dst
:0
:0
Op :
:1
 :
SPI:0x00000000
SPI :
IPSEC: , SPI 0xFD2D851F
 ID:0x53F91970
IPSEC: , SPI 0xFD2D851F
 :10.0.0.2
 :255.255.255.255
dst :10.0.0.1
 :255.255.255.255

:0
:0
Op :
Dst
:0
:0
Op :
:50
 :
SPI:0xFD2D851F
SPI :
IPSEC: , SPI 0xFD2D851F
 ID:0x53F91A08
IPSEC: , SPI 0xFD2D851F
 :10.0.0.2
 :255.255.255.255
dst :10.0.0.1
 :255.255.255.255

:0
:0
Op :
Dst
:0
:0
Op :
:50
 :

SPI:0xFD2D851F
SPI :
IPSEC: . SPI 0xFD2D851F
ID:0x53F91AA0
QM3 . [IKEv1]: = 10.0.0.2, IP = 10.0.0.2, 3 QM pkt IKE :msg id = 7b80c2b0

==========QM3==========
==========>
[IKEv1]:IP = 10.0.0.2, IKE_DECODE [IKEv1]:IP =
(msgid=7b80c2b0) :HDR + HASH (8) + NONE (0) : 76 10.0.0.2,
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, IKE SA KEY_ADD IKE_DECODE
2 . .SPI = 0xdde50931 RECEIVED QM3 .
SPI . [IKEv1]: = 10.0.0.2, IP = 10.0.0.2, :KEY_UPDATE . spi (msgid=52481cf5)
0xfd2d851f :HDR + HASH
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, P2 :3060 (8) + NONE (0)
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, 2 (msgid=7b80c2b0) :52
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2,
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, IPSEC SA
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, !
[IKEv1]:Group = 10.0.0.2, IP = 10.0.0.2, NP MAP 10 ACL
VPN:cs_id=53f11198 .=53f11a90
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, !
IPSEC:0x53F18B00 SA,
SCB:0x53F8A1C0,
:
SPI:0xDB680406
ID:0x00004000
VPIF :0x00000003
:l2l
:esp
:240
IPSEC: OBSA , SPI 0xDB680406
IPSEC: VPN , SPI 0xDB680406
:0x00000005
SA:0x53F18B00
SPI:0xDB680406
MTU:1500
VCID:0x00000000
:0x00000000 QM3
SCB:0x005E4849 SA .
:0x4C69CB80
IPSEC: VPN , SPI 0xDB680406 SPI .
VPN :0x0000E9B4
IPSEC: , SPI 0xDB680406
:192.168.1.0
:255.255.255.0
dst :192.168.2.0
:255.255.255.0

:0
:0
Op :
Dst
:0
:0
Op :
:1
:
SPI:0x00000000
SPI :
IPSEC: , SPI 0xDB680406
ID:0x53F89160
IPSEC: , SPI 0xDB680406
:10.0.0.1

:255.255.255.255
dst :10.0.0.2
:255.255.255.255

:0
:0
Op :
Dst
:0
:0
Op :
:50
:
SPI:0xDB680406
SPI :
IPSEC: , SPI 0xDB680406
ID:0x53E47E88
[IKEv1]:Group = 10.0.0.2, IP = 10.0.0.2, NP MAP 10 ACL
VPN:cs_id=53f11198 .=53f11a90
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, LAN-to-LAN (10.0.0.2) Responder, SPI
= 0x1698cac7, SPI = 0xdb680406 .
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, IKE SA KEY_ADD .SPI = 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
VPN :0x00011A8C
IPSEC: VPN 0x0000E9B4, SPI 0xDB680406
:0x00000005
SA:0x53F18B00
SPI:0xDB680406
MTU:1500
VCID:0x00000000
:0x00011A8C
SCB:0x005E4849 SPI SA .
:0x4C69CB80
IPSEC: VPN , SPI 0xDB680406
VPN :0x0000E9B4
IPSEC: , SPI 0xDB680406
ID:0x53F89160
IPSEC: SPD , SPI 0xDB680406
ID:0x53E47E88
IPSEC: , SPI 0x1698CAC7
:192.168.2.0
:255.255.255.0
dst :192.168.1.0
:255.255.255.0

:0
:0
Op :
Dst
:0
:0
Op :
:1
:

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

:0
:0
Op :
Dst
:0
:0
Op :
:50
:
SPI:0x1698CAC7
SPI :
IPSEC: , SPI 0x1698CAC7
ID:0x53FC3F18
IPSEC: , SPI 0x1698CAC7
:10.0.0.2
:255.255.255.255
dst :10.0.0.1
:255.255.255.255

:0
:0
Op :
Dst
:0
:0
Op :
:50
:
SPI:0x1698CAC7
SPI :
IPSEC: , SPI 0x1698CAC7
ID:0x53F8AEA8
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, : KEY_UPDATE, spi 0x1698cac7
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, P2 :3060 IPsec rekey .
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, 2 (msgid=52481cf5) 2 .responder initiator / .

터널 확인

참고:ICMP는 터널을 트리거하는 데 사용되므로 IPSec SA가 하나만 작동됩니다.프로토콜 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

관련 정보

- 좋은 출발점은 IPSec에 대한 위키백과 문서2. 표준 및 참조 자료에는 많은 유용한 정보가 포함되어 있습니다.
- IPsec 문제 해결:디버그 명령 이해 및 사용
- **기술 지원 및 문서 – Cisco Systems**