Contents

Introduction

This document describes debugs on the Adaptive Security Appliance (ASA) when both main mode and pre-shared key (PSK) are used. The translation of certain debug lines into configuration is also discussed.

Topics not discussed in this document include passing traffic after the tunnel has been established and basic concepts of IPsec or Internet Key Exchange (IKE).

Prerequisites

Requirements

Readers of this document should have knowledge of these topics.

- PSK
- IKE

Components Used

The information in this document is based on these hardware and software versions:

- Cisco ASA 9.3.2
- Routers that run Cisco IOS® 12.4T

Core Issue

IKE and IPsec debugs are sometimes cryptic, but you can use them to understand where an IPsec VPN tunnel establishment problem is located.

Scenario

Main mode is typically used between LAN-to-LAN tunnels or, in the case of remote access (EzVPN), when certificates are used for authentication.

The debugs are from two ASAs that run software version 9.3.2. The two devices will form a LAN-to-LAN tunnel.

Two main scenarios are described:

- ASA as the initiator for IKE
- ASA as the responder for IKE

Debug Commands Used

debug crypto ikev1 127

debug crypto ipsec 127

ASA Configuration

IPsec configuration:

```
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 Configuration:

```
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 Configuration:

```
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
```

Debugging

Initiator Message Description	Debugs	Responder M Description
Main mode exchange begins; no policies have been shared, and the peers still in MM_NO_STATE. As the initiator, the ASA starts to construct the payload.	[IKEv1 DEBUG]: Pitcher: received a key acquire message, spi 0x0 IPSEC(Prot saddr daddr dport IPSEC(MAP 10: matched. [IKEv1]: IP = 10.0.0.2, IKE Initiator: New Phase 1, Intf inside, IKE Peer 10.0.0.2 local Proxy Address 192.168.1.0, remote Proxy Address 192.168.2.0, Crypto map (MAP)	
Construct MM1 This process i	[IKEv1 DEBUG]: IP = 10.0.0.2, constructing **ISAKMP SA payload** [IKEv1 DEBUG]: IP = 10.0.0.2, constructing NAT-Traversal VID ver 02 payload [IKEv1 DEBUG]: IP = 10.0.0.2, constructing NAT-Traversal VID ver 03 payload [IKEv1 DEBUG]: IP = 10.0.0.2, constructing NAT-Traversal VID ver RFC payload [IKEv1 DEBUG]: IP = 10.0.0.2, constructing Fragmentation VID + extended capabilities payload	
Send MM1.	[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (==========MM1==========>	
	[IKEv1]: IP = 10.0.0.2, IKE_DECODE RECEIVED Message (	MM1 receive initiator. Process MM1 The comparis ISAKMP/IKE policies begin The remote p advertises tha use NAT-T. Related configuration *crypto isakmp 10 authenticatio share encryption 3a hash sha group 2 lifetime 8640*
	[IKEv1 DEBUG]: IP = 10.0.0.2, processing SA payload [IKEv1 DEBUG]: IP = 10.0.0.2, Oakley proposal is acceptable [IKEv1 DEBUG]: IP = 10.0.0.2, processing VID payload [IKEv1 DEBUG]: IP = 10.0.0.2, Received NAT-Traversal RFC VID [IKEv1 DEBUG]: IP = 10.0.0.2, processing VID payload [IKEv1 DEBUG]: IP = 10.0.0.2, processing VID payload [IKEv1 DEBUG]: IP = 10.0.0.2, Received NAT-Traversal ver 03 VID [IKEv1 DEBUG]: IP = 10.0.0.2, processing VID payload [IKEv1 DEBUG]: IP = 10.0.0.2, Received NAT-Traversal ver 02 VID [IKEv1 DEBUG]: IP = 10.0.0.2, processing IKE SA payload [IKEv1 DEBUG]: IP = 10.0.0.2, IKE SA Proposal # 1, Transform # 1 acceptable Matches global IKE entry # 2	Construct In this messag responder sel which isakmp settings to us also advertise NAT-T versi can use. Send MM2.
	[IKEv1 DEBUG]: IP = 10.0.0.2, constructing ISAKMP SA payload [IKEv1 DEBUG]: IP = 10.0.0.2, constructing NAT-Traversal VID ver 02 payload [IKEv1 DEBUG]: IP = 10.0.0.2, constructing Fragmentation VID + extended capabilities payload	
	[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (<==========MM2==========	
MM2 received from responder.	[IKEv1]: IP = 10.0.0.2, IKE_DECODE RECEIVED Message (	
Process MM2.	[IKEv1 DEBUG]: IP = 10.0.0.2, processing SA payload [IKEv1 DEBUG]: IP = 10.0.0.2, Oakley proposal is acceptable [IKEv1 DEBUG]: IP = 10.0.0.2, processing VID payload [IKEv1 DEBUG]: IP = 10.0.0.2, Received NAT-Traversal RFC VID	
Construct MM3. This process i	Nov 30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, constructing ke payload Nov 30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, constructing nonce payload Nov 30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, constructing Cisco Unity VID payload Nov 30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, constructing xauth V6 VID payload	

Nov 30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, Send IOS VID
Nov 30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, Constructing ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Nov 30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, constructing VID payload
Nov 30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, Send Altiga/Cisco VPN3000/Cisco ASA GW VID
Nov 30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, constructing NAT-Discovery payload
Nov 30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, computing NAT Discovery hash
Nov 30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, constructing NAT-Discovery payload
Nov 30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, computing NAT Discovery hash

Send MM3.

[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (
==========MM3==========>

[IKEv1]: IP = 10.0.0.2, IKE_DECODE RECEIVED Message (

MM3 receive
initiator.

[IKEv1 DEBUG]: IP = 10.0.0.2, processing ke payload
[IKEv1 DEBUG]: IP = 10.0.0.2, processing ISA_KE payload
[IKEv1 DEBUG]: IP = 10.0.0.2, processing nonce payload
[IKEv1 DEBUG]: IP = 10.0.0.2, processing VID payload
[IKEv1 DEBUG]: IP = 10.0.0.2, Received DPD VID
[IKEv1 DEBUG]: IP = 10.0.0.2, processing VID payload
[IKEv1 DEBUG]: IP = 10.0.0.2, Processing IOS/PIX Vendor ID payload (version: 1.0.0, capabilities: 00000f6f)
[IKEv1 DEBUG]: IP = 10.0.0.2, processing VID payload
[IKEv1 DEBUG]: IP = 10.0.0.2, Received xauth V6 VID
[IKEv1 DEBUG]: IP = 10.0.0.2, processing NAT-Discovery payload
[IKEv1 DEBUG]: IP = 10.0.0.2, computing NAT Discovery hash
[IKEv1 DEBUG]: IP = 10.0.0.2, processing NAT-Discovery payload
[IKEv1 DEBUG]: IP = 10.0.0.2, computing NAT Discovery hash
[IKEv1 DEBUG]: IP = 10.0.0.2, constructing ke payload
[IKEv1 DEBUG]: IP = 10.0.0.2, constructing nonce payload
[IKEv1 DEBUG]: IP = 10.0.0.2, constructing Cisco Unity VID payload
[IKEv1 DEBUG]: IP = 10.0.0.2, constructing xauth V6 VID payload
[IKEv1 DEBUG]: IP = 10.0.0.2, Send IOS VID
[IKEv1 DEBUG]: IP = 10.0.0.2, Constructing ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)
[IKEv1 DEBUG]: IP = 10.0.0.2, constructing VID payload
[IKEv1 DEBUG]: IP = 10.0.0.2, Send Altiga
[IKEv1 DEBUG]: IP = 10.0.0.2, constructing NAT-Discovery payload
[IKEv1 DEBUG]: IP = 10.0.0.2, computing NAT Discovery hash
[IKEv1 DEBUG]: IP = 10.0.0.2, constructing NAT-Discovery payload
[IKEv1 DEBUG]: IP = 10.0.0.2, computing NAT Discovery hash

Process MM3
From NAT-D
payloads resp
is able to dete
if the
From the DH
the payload
responder get
values of p, g

Construct MM
This process i

[IKEv1]: IP = 10.0.0.2, Connection landed on tunnel_group 10.0.0.2
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, Generating keys for Responder…

The peer is
associated wi
10.0.0.2 L2L
group, and th
encryption an
keys are gene
from the "s" a
and the pre-sh
key.

[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (
<==========MM4==========

Send MM4.

MM4 received

[IKEv1]: IP = 10.0.0.2, IKE_DECODE RECEIVED Message (
[IKEv1 DEBUG]: IP = 10.0.0.2, processing ike payload
[IKEv1 DEBUG]: IP = 10.0.0.2, processing ISA_KE payload
[IKEv1 DEBUG]: IP = 10.0.0.2, processing nonce payload
[IKEv1 DEBUG]: IP = 10.0.0.2, processing VID payload
[IKEv1 DEBUG]: IP = 10.0.0.2, Received Cisco Unity client VID
[IKEv1 DEBUG]: IP = 10.0.0.2, processing VID payload
[IKEv1 DEBUG]: IP = 10.0.0.2, Received DPD VID
[IKEv1 DEBUG]: IP = 10.0.0.2, processing VID payload
[IKEv1 DEBUG]: IP = 10.0.0.2, Processing IOS/PIX Vendor ID payload (version: 1.0.0, capabilities: 00000f7f)
[IKEv1 DEBUG]: IP = 10.0.0.2, processing VID payload
[IKEv1 DEBUG]: IP = 10.0.0.2, Received xauth V6 VID

Process MM4.
From the NAT-D
payloads, the initator
is now able to
determine if the

From the DH KE, i

[IKEv1 DEBUG]: IP = 10.0.0.2, processing NAT-Discovery payload
[IKEv1 DEBUG]: IP = 10.0.0.2, computing NAT Discovery hash
[IKEv1 DEBUG]: IP = 10.0.0.2, processing NAT-Discovery payload
[IKEv1 DEBUG]: IP = 10.0.0.2, computing NAT Discovery hash

The peer is associated with the 10.0.0.2 L2L tunnel group, and the initator generates encryption and hash keys using "s" above and the pre-shared-key.

[IKEv1]: IP = 10.0.0.2, Connection landed on tunnel_group 10.0.0.2
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, Generating keys for Initiator...

Construct MM5. Related configuration:
crypto isakmp identity auto

[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, constructing ID payload
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, constructing hash payload
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, Computing hash for ISAKMP
[IKEv1 DEBUG]: IP = 10.0.0.2, Constructing IOS keep alive payload: proposal=32767/32767 sec.
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, constructing dpd vid payload

Send

[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (
==========MM5==========>

Responder is not behind any NAT. No NAT-T required.

[IKEv1]: Group = 10.0.0.2, IP = 10.0.0.2, Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device

[IKEv1]: IP = 10.0.0.2, IKE_DECODE RECEIVED Message (

MM5 receive
This process i

Process MM5
Authenticatio
pre-shared ke
begins now.
Authenticatio
occurs on bot
therefore, you
see two sets o
correspondin
authentication
processes.
Related
configuration
tunnel group
type ipsec-l2l
No NAT-T re
in this case.
Construct MM
Send identity
includes reke
started and id
sent to remote
Send MM6.

[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, processing ID payload
[IKEv1 DECODE]: Group = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR ID received
10.0.0.2
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, processing hash payload
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, Computing hash for ISAKMP
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, processing notify payload
[IKEv1]: Group = 10.0.0.2, IP = 10.0.0.2,Automatic NAT
[IKEv1]: IP = 10.0.0.2, Connection landed on tunnel_group 10.0.0.2

Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device

[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, constructing ID payload
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, constructing hash payload
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, Computing hash for ISAKMP
[IKEv1 DEBUG]: IP = 10.0.0.2, Constructing IOS keep alive payload: proposal=32767/32767 sec.
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, constructing dpd vid payload
[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (
<==========MM6==========

MM6 received

[IKEv1]: IP = 10.0.0.2, IKE_DECODE RECEIVED Message (

[IKEv1]: Group = 10.0.0.2, IP = 10.0.0.2, PHASE 1 COMPLETED
[IKEv1]: IP = 10.0.0.2, Keep-alive type for this connection: DPD
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, Starting P1 rekey timer: 64800 seconds.

Phase 1 comp
Start rekey ti
Related
configuration
crypto isakmp
10
authentication
share
encryption 3d
hash sha
group 2
lifetime 8640
ciscoasa sh ru
crypto isakmp
crypto isakmp

identity auto

[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, processing ID payload
[IKEv1 DECODE]: Group = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR ID received
10.0.0.2

Process MM6.
This process i

[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, processing hash payload
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, Computing hash for ISAKMP
[IKEv1]: IP = 10.0.0.2, Connection landed on tunnel_group 10.0.0.2
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, Oakley begin quick mode
[IKEv1 DECODE]: Group = 10.0.0.2, IP = 10.0.0.2, IKE Initiator starting QM: msg id = 7b80c2b0

Phase 1 complete.
Start ISAKMP rekey timer.
Related c
tunnel group 10.0.0.2 type ipsec-l2l
tunnel group 10.0.0.2 ipsec
pre-shared-key cisco

[IKEv1]: Group = 10.0.0.2, IP = 10.0.0.2, PHASE 1 COMPLETED
[IKEv1]: IP = 10.0.0.2, Keep-alive type for this connection: DPD
DPD has bee negotiated and Phase 1 is now complete.
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, Starting P1 rekey timer: 82080 seconds.

Phase 2 (quick mode) begins.

IPSEC: New embryonic SA created @ 0x53FC3C00,
SCB: 0x53F90A00,
Direction: inbound
SPI : 0xFD2D851F
Session ID: 0x00006000
VPIF num : 0x00000003
Tunnel type: l2l
Protocol : esp
Lifetime : 240 seconds

Construct QM1.
This process includes policies.
Related configuration:
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

[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, IKE got SPI from key engine: SPI = 0xfd2d851f
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, oakley constucting quick mode
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, constructing blank hash payload
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, constructing IPSec SA payload
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, constructing IPSec nonce payload
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, constructing proxy ID
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, Transmitting Proxy Id:
Local subnet: 192.168.1.0 mask 255.255.255.0 Protocol 1 Port 0
Remote subnet: 192.168.2.0 Mask 255.255.255.0 Protocol 1 Port 0
The local subnet (192.168.1.0/24) and expcted remote subnet (192.168.2.0/24) are being sent
[IKEv1 DECODE]: Group = 10.0.0.2, IP = 10.0.0.2, IKE Initiator sending Initial Contact
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, constructing qm hash payload
[IKEv1 DECODE]: Group = 10.0.0.2, IP = 10.0.0.2, IKE Initiator sending 1st QM pkt msg id = 7b80c2b0

Send

[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (
==========QM1==========>

QM1 receive
initiator.
Responder st
phase 2 (QM

[IKEv1 DECODE]: IP = 10.0.0.2, IKE Responder starting QM:
[IKEv1]: IP = 10.0.0.2, IKE_DECODE RECEIVED Message (

[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, processing hash payload
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, processing SA payload
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, processing nonce payload
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, processing ID payload

Process QM1
This process
Related
configuration
ipsec transfor
TRANSFORI
aes esp-sha-h
access-list VI
extended perr
icmp 192.168
255.255.255.
192.168.2.0
255.255.255.
crypto map M
match addres

[IKEv1 DECODE]: 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: Address 192.168.2.0, Mask 255.255.255.0, Protocol 1, Port 0
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, processing ID payload
[IKEv1 DECODE]: 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]: Group = 10.0.0.2, IP = 10.0.0.2, Received local IP Proxy Subnet data in ID Payload: Address 192.168.1.0, Mask 255.255.255.0, Protocol 1, Port 0

The remote a
subnets
(192.168.2.0/
192.168.1.0/2
received.

[IKEv1]: Group = 10.0.0.2, IP = 10.0.0.2, QM IsRekeyed old sa not found by addr
[IKEv1]: Group = 10.0.0.2, IP = 10.0.0.2, Static Crypto Map check, checking map = MAP, seq = 10...
[IKEv1]: Group = 10.0.0.2, IP = 10.0.0.2, Static Crypto Map check, map MAP seq = 10 is a successful match

A matching s
crypto entry i
looked for an
found.

[IKEv1]: Group = 10.0.0.2, IP = 10.0.0.2, IKE Remote Peer configured for crypto map: MAP
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, processing IPSec SA payload
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, IPSec SA Proposal # 1, Transform # 1 acceptable Matches global IPSec SA entry # 10
[IKEv1]: Group = 10.0.0.2, IP = 10.0.0.2, IKE: requesting SPI!
IPSEC: New embryonic SA created @ 0x53FC3698,
SCB: 0x53FC2998,
Direction: inbound
SPI : 0x1698CAC7
Session ID: 0x00004000
VPIF num : 0x00000003
Tunnel type: l2l
Protocol : esp
Lifetime : 240 seconds
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, IKE got SPI from key engine: SPI = 0x1698cac7

Construct QM
This process i

[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, oakley constructing quick mode
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, constructing blank hash payload
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, constructing IPSec SA payload
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, constructing IPSec nonce payload
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, constructing proxy ID
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, Transmitting Proxy Id:
Remote subnet: 192.168.2.0 Mask 255.255.255.0 Protocol 1 Port 0
Local subnet: 192.168.1.0 mask 255.255.255.0 Protocol 1 Port 0
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, constructing qm hash payload
[IKEv1 DECODE]: Group = 10.0.0.2, IP = 10.0.0.2, IKE Responder sending 2nd QM pkt msg id = 52481cf5
[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (

Send QM2.

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

QM2 received from responder.

[IKEv1]: IP = 10.0.0.2, IKE_DECODE RECEIVED Message (

Process QM2.
In this process, shortest proposed phase 2 lifetimes is picked.

[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, processing hash payload
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, processing SA payload
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, processing nonce payload
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, processing ID payload
[IKEv1 DECODE]: 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]: Group = 10.0.0.2, IP = 10.0.0.2, processing ID payload

[IKEv1 DECODE]: 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 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, processing notify payload
[IKEv1 DECODE]: Responder Lifetime decode follows (SPI[4]lattributes):
[IKEv1 DECODE]: 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
based on response from peer, the ASA is changing certain IPSEC attributes. In this case the rekey interval
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, loading all IPSEC SAs
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, Generating Quick Mode Key!

Found matching crypto map "MAP" and entry 10 and matched it against access-list "VPN."

[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, NP encrypt rule look up for crypto map MAP 10 matching ACL VPN: returned cs_id

[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, Generating Quick Mode Key!
IPSEC: New embryonic SA created @ 0x53FC3698,
SCB: 0x53F910F0,
Direction: outbound
SPI : 0xDDE50931
Session ID: 0x00006000
VPIF num : 0x00000003
Tunnel type: l2l
Protocol : esp
Lifetime : 240 seconds
IPSEC: Completed host OBSA update, SPI 0xDDE50931
IPSEC: Creating outbound VPN context, SPI 0xDDE50931
Flags: 0x00000005
SA : 0x53FC3698
SPI : 0xDDE50931
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x00000000
SCB : 0x01CF218F
Channel: 0x4C69CB80
IPSEC: Completed outbound VPN context, SPI 0xDDE50931
VPN handle: 0x000161A4
IPSEC: New outbound encrypt rule, SPI 0xDDE50931
Src addr
Src mask: 255.255.255.0
Dst addr
Dst mask: 255.255.255.0
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 1
Use protocol: true
SPI: 0x00000000
Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0xDDE50931
Rule ID: 0x53FC3AD8
IPSEC: New outbound permit rule, SPI 0xDDE50931
Src addr
Src mask: 255.255.255.255
Dst addr
Dst mask: 255.255.255.255
Src ports
Upper: 0

The appliance has generated the SPIs 0xfd2d851f and 0xdde50931for inbound and outbound traffic respectively.

Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0xDDE50931
Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0xDDE50931
Rule ID: 0x53F91538
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, NP encrypt rule look up for crypto map MAP 10 matching ACL VPN: returned cs_id
[IKEv1]: Group = 10.0.0.2, IP = 10.0.0.2, Security negotiation complete for LAN-to-LAN Group (10.0.0.2) Initiator, Inbound SPI = 0xfd2d851f, Outbound SPI = 0xdde50931
IPSEC: Completed host IBSA update, SPI 0xFD2D851F
IPSEC: Creating inbound VPN context, SPI 0xFD2D851F
Flags: 0x00000006
SA : 0x53FC3C00
SPI : 0xFD2D851F
MTU : 0 bytes
VCID : 0x00000000
Peer : 0x000161A4
SCB : 0x01CEA8EF
Channel: 0x4C69CB80
IPSEC: Completed inbound VPN context, SPI 0xFD2D851F
VPN handle: 0x00018BBC
IPSEC: Updating outbound VPN context 0x000161A4, SPI 0xDDE50931
Flags: 0x00000005
SA : 0x53FC3698
SPI : 0xDDE50931
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x00018BBC
SCB : 0x01CF218F
Channel: 0x4C69CB80
IPSEC: Completed outbound VPN context, SPI 0xDDE50931
VPN handle: 0x000161A4

Construct QM3. Confirm

IPSEC: Completed outbound inner rule, SPI 0xDDE50931
Rule ID: 0x53FC3AD8
IPSEC: Completed outbound outer SPD rule, SPI 0xDDE50931
Rule ID: 0x53F91538
IPSEC: New inbound tunnel flow rule, SPI 0xFD2D851F
Src addr
Src mask: 255.255.255.0
Dst addr
Dst mask: 255.255.255.0
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 1
Use protocol: true
SPI: 0x00000000
Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0xFD2D851F
Rule ID: 0x53F91970
IPSEC: New inbound decrypt rule, SPI 0xFD2D851F
Src addr

Src mask: 255.255.255.255
Dst addr
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0xFD2D851F
Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0xFD2D851F
Rule ID: 0x53F91A08
IPSEC: New inbound permit rule, SPI 0xFD2D851F
Src addr
Src mask: 255.255.255.255
Dst addr
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0xFD2D851F
Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0xFD2D851F
Rule ID: 0x53F91AA0

Send QM3.

[IKEv1 DECODE]: Group = 10.0.0.2, IP = 10.0.0.2, IKE Initiator sending 3rd QM pkt msg id = 7b80c2b0

==========QM3==========>

Phase 2 complete. The initiator is now ready to encrypt and decrypt packets using these SPI values.

[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, IKE got a KEY_ADD msg for SA: SPI = 0xdde50931
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, Pitcher: received KEY_UPDATE, spi 0xfd2d851f
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, Starting P2 rekey timer: 3060 seconds.
[IKEv1]: Group = 10.0.0.2, IP = 10.0.0.2, PHASE 2 COMPLETED (
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, processing hash payload
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, loading all IPSEC SAs
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, Generating Quick Mode Key!
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, NP encrypt rule look up for crypto map MAP 10 matching ACL VPN: returned cs_id
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, Generating Quick Mode Key!
IPSEC: New embryonic SA created @ 0x53F18B00,
SCB: 0x53F8A1C0,
Direction: outbound
SPI : 0xDB680406
Session ID: 0x00004000
VPIF num : 0x00000003
Tunnel type: l2l
Protocol : esp
Lifetime : 240 seconds
IPSEC: Completed host OBSA update, SPI 0xDB680406
IPSEC: Creating outbound VPN context, SPI 0xDB680406

[IKEv1]: IP = 10.0.0.2, IKE_DECODE RECEIVED Message (

QM3 receivd initiator.

Process QM3
Encryption ke
generated for
data SAs.
During this p
SPIs are set i
to pass traffic

Flags: 0x00000005
SA : 0x53F18B00
SPI : 0xDB680406
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x00000000
SCB : 0x005E4849
Channel: 0x4C69CB80
IPSEC: Completed outbound VPN context, SPI 0xDB680406
VPN handle: 0x0000E9B4
IPSEC: New outbound encrypt rule, SPI 0xDB680406
Src addr
Src mask: 255.255.255.0
Dst addr
Dst mask: 255.255.255.0
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 1
Use protocol: true
SPI: 0x00000000
Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0xDB680406
Rule ID: 0x53F89160
IPSEC: New outbound permit rule, SPI 0xDB680406
Src addr
Src mask: 255.255.255.255
Dst addr
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0xDB680406
Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0xDB680406
Rule ID: 0x53E47E88
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, NP encrypt rule look up for crypto map MAP 10 matching ACL VPN: returned cs_id
[IKEv1]: Group = 10.0.0.2, IP = 10.0.0.2, Security negotiation complete for LAN-to-LAN Group (10.0.0.2) Responder, Inbound SPI = 0x1698cac7, Outbound SPI = 0xdb680406
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, IKE got a KEY_ADD msg for SA: SPI = 0xdb680406
IPSEC: Completed host IBSA update, SPI 0x1698CAC7
IPSEC: Creating inbound VPN context, SPI 0x1698CAC7
Flags: 0x00000006
SA : 0x53FC3698
SPI : 0x1698CAC7
MTU : 0 bytes
VCID : 0x00000000
Peer : 0x0000E9B4
SCB : 0x005DAE51
Channel: 0x4C69CB80

SPIs are assig
the data SAs.

IPSEC: Completed inbound VPN context, SPI 0x1698CAC7
VPN handle: 0x00011A8C
IPSEC: Updating outbound VPN context 0x0000E9B4, SPI 0xDB680406
Flags: 0x00000005
SA : 0x53F18B00
SPI : 0xDB680406
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x00011A8C
SCB : 0x005E4849
Channel: 0x4C69CB80
IPSEC: Completed outbound VPN context, SPI 0xDB680406
VPN handle: 0x0000E9B4
IPSEC: Completed outbound inner rule, SPI 0xDB680406
Rule ID: 0x53F89160
IPSEC: Completed outbound outer SPD rule, SPI 0xDB680406
Rule ID: 0x53E47E88
IPSEC: New inbound tunnel flow rule, SPI 0x1698CAC7
Src addr
Src mask: 255.255.255.0
Dst addr
Dst mask: 255.255.255.0
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 1
Use protocol: true
SPI: 0x00000000
Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x1698CAC7
Rule ID: 0x53FC3E80
IPSEC: New inbound decrypt rule, SPI 0x1698CAC7
Src addr
Src mask: 255.255.255.255
Dst addr
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x1698CAC7
Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x1698CAC7
Rule ID: 0x53FC3F18
IPSEC: New inbound permit rule, SPI 0x1698CAC7
Src addr
Src mask: 255.255.255.255
Dst addr
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore

Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x1698CAC7
Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x1698CAC7
Rule ID: 0x53F8AEA8
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, Pitcher: received KEY_UPDATE, spi 0x1698cac7
[IKEv1 DEBUG]: Group = 10.0.0.2, IP = 10.0.0.2, Starting P2 rekey timer: 3060 seconds.

Start rekey ti
Phase 2 comp

[IKEv1]: Group = 10.0.0.2, IP = 10.0.0.2, PHASE 2 COMPLETED (

Both respond
initiator are a
encrypt/decry
traffic.

Tunnel Verification

Note: Since ICMP is used to trigger the tunnel, only one IPSec SA is up. Protocol 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: 0x1698CAC7 (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 0x00000001show 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
```

Related Information

- A good place to start is wikipedia article on IPSec. Standard and references contains a lot of useful information
- IPsec Troubleshooting: Understanding and Using debug Commands
- **Technical Support & Documentation - Cisco Systems**