Swift Migration of IKEv1 to IKEv2 L2L Tunnel Configuration on ASA 8.4 Code

Contents

Introduction

This document provides information about IKEv2 and the migration process from IKEv1.

Prerequisites

Requirements

Ensure that you have a Cisco ASA Security Appliance that runs IPsec with the IKEv1 Pre-shared key (PSK) authentication method, and ensure the IPsec tunnel is in the operational state.

For an example configuration of a Cisco ASA Security Appliance that runs IPsec with IKEv1 PSK authentication method, refer to PIX/ASA 7.x and above: PIX-to-PIX VPN Tunnel Configuration Example.

Components Used

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

- Cisco ASA 5510 Series Security Appliance that runs with version 8.4.x and later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

Why Migrate to IKEv2?

- IKEv2 provides better network attack resilience. IKEv2 can mitigate a DoS attack on the network when it validates the IPsec initiator. In order to make DoS vulnerability difficult to exploit, the responder can ask for a cookie to the initiator who has to assure the responder that this is a normal connection. In IKEv2, the responder cookies mitigate the DoS attack so that the responder does not keep a state of the IKE initiator or does not perform a D-H operation unless the initiator returns the cookie sent by the responder. The responder uses minimal CPU and commits no state to a Security Association (SA) until it can completely validate the initiator.
- IKEv2 reduces the complexity in IPsec establishment between different VPN products. It increases interoperability and also allows a standard way for legacy authentication methods. IKEv2 provides a seamless IPsec interoperability among vendors since it offers built-in technologies such as Dead Peer Detection (DPD), NAT Traversal (NAT-T), or Initial Contact.
- IKEv2 has less overhead. With less overhead, it offers improved SA setup latency. Multiple requests are allowed in transit (for example, when a multiple of child-SAs are set up in parallel).
- IKEv2 has a reduced SA delay. In IKEv1 the delay of SA creation amplifies as the packet volume amplifies. IKEv2 keeps the same average delay when the packet volume amplifies. When the packet volume amplifies, the time to encrypt and process the packet header amplifies. When a new SA establishment is to be created, more time is required. The SA generated by IKEv2 is less than the one generated by IKEv1. For an amplified packet size, the time taken to create an SA is almost constant.
- IKEv2 has faster rekey time. IKE v1 takes more time to rekey SAs than IKEv2. IKEv2 rekey for SA offers improved security performance and decreases the number of packets lost in transition. Due to the redefinition of certain mechanisms of IKEv1 (such as ToS payload, choice of SA lifetime, and SPI uniqueness) in IKEv2, fewer packets are lost and duplicated in IKEv2. Therefore, there is less need to rekey SAs.

Note: Because network security can only be as strong as the weakest link, IKEv2 does not interoperate with IKEv1.

Migration Overview

If your IKEv1, or even SSL, configuration already exists, the ASA makes the migration process simple. On the command line, enter the **migrate** command:

```
migrate {l2l | remote-access {ikev2 | ssl} | overwrite}
```

Things of note:

- Keyword definitions:**l2l** - This converts current IKEv1 l2l tunnels to IKEv2.**remote access** - This converts the remote access configuration. You can convert either the IKEv1 or the SSL tunnel groups to IKEv2.**overwrite** - If you have a IKEv2 configuration that you wish to overwrite, then this keyword converts the current IKEv1 configuration and removes the superfluous IKEv2 configuration.
- It is important to note that IKEv2 has the ability to use both symmetric as well as asymmetric keys for PSK authentication. When the **migration** command is entered on the ASA, the ASA automatically creates an IKEv2 VPN with a symmetric PSK.
- After the command is entered, the current IKEv1 configurations are not deleted. Instead both IKEv1 and IKEv2 configurations run in parallel and on the same crypto map. You can do this manually as well. When both IKEv1 and IKEv2 run in parallel, this allows an IPsec VPN initiator to fallback from IKEv2 to IKEv1 when a protocol or configuration issue exists with IKEv2 that can lead to connection attempt failure. When both IKEv1 and IKEv2 run in parallel, it also provides a rollback mechanism and makes migration easier.
- When both IKEv1 and IKEv2 run in parallel, ASA uses a module called tunnel manager/IKE common on the initiator to determine the crypto map and IKE protocol version to use for a connection. The ASA always prefers to initiate IKEv2, but if it cannot, it falls back to IKEv1.
- Multiple peers used for redundancy is not supported with IKEv2 on the ASA. In IKEv1, for redundancy purposes, one can have more than one peer under the same crypto map when you enter the **set peer** command. The first peer will be the primary and if it fails, the second peer will kick in. Refer to Cisco bug ID CSCud22276 (registered customers only) , ENH: Multiple Peers support for IKEv2.

Migration Process

Configuration

In this example, IKEv1 VPN that uses Pre-Shared Key (PSK) authentication exists on the ASA.

Note: The configuration shown here is only relevant to the VPN tunnel.

ASA Configuration with a Current IKEv1 VPN (Before Migration)

```
ASA-2(config)# sh run
ASA Version 8.4(2)
!
hostname ASA-2
!
crypto ipsec IKEv1 transform-set goset esp-3des esp-sha-hmac
crypto map vpn 12 match address NEWARK
crypto map vpn 12 set pfs group5
crypto map vpn 12 set peer <peer_ip-address>
crypto map vpn 12 set IKEv1 transform-set goset
crypto map vpn interface outside
crypto isakmp disconnect-notify
crypto IKEv1 enable outside
crypto IKEv1 policy 1
 authentication pre-share
 encryption 3des
 hash sha
 group 5
 lifetime 86400
```

```
!
tunnel-group <peer_ip-address> type ipsec-l2l
tunnel-group <peer_ip-address> ipsec-attributes
 IKEv1 pre-shared-key *****
 isakmp keepalive threshold 10 retry 3
```

ASA IKEv2 Configuration (After Migration)

Note: Changes marked in bold italics.

```
ASA-2(config)# migrate l2l
ASA-2(config)# sh run
ASA Version 8.4(2)
!
hostname ASA-2
!
crypto ipsec IKEv1 transform-set goset esp-3des esp-sha-hmac
crypto ipsec IKEv2 ipsec-proposal goset protocol esp encryption 3des protocol esp
integrity sha-1 crypto map vpn 12 match address NEWARK crypto map vpn 12 set pfs
group5 crypto map vpn 12 set peer <peer_ip-address> crypto map vpn 12 set IKEv1
transform-set goset crypto map vpn 12 set IKEv2 ipsec-proposal goset crypto map vpn
interface outside crypto isakmp disconnect-notify crypto IKEv2 policy 1 encryption
3des integrity sha group 5 prf sha lifetime seconds 86400 crypto IKEv2 enable outside
crypto IKEv1 enable outside crypto IKEv1 policy 1 authentication pre-share encryption
3des hash sha group 5 lifetime 86400 ! tunnel-group <peer_ip-address> type ipsec-l2l
tunnel-group <peer_ip-address> ipsec-attributes IKEv1 pre-shared-key ***** isakmp
keepalive threshold 10 retry 3 IKEv2 remote-authentication pre-shared-key ***** IKEv2
local-authentication pre-shared-key *****
```

IKEv2 Tunnel Establishment Verification

```
ASA1# sh cry IKEv2 sa detail

IKEv2 SAs:
Session-id:12, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id   Local                Remote     Status        Role
102061223 192.168.1.1/500  192.168.2.2/500  READY    INITIATOR
     Encr: 3DES, Hash: SHA96, DH Grp:5, Auth sign: PSK,Auth verify: PSK
     Life/Active Time: 86400/100 sec
     Status Description: Negotiation done
     Local spi: 297EF9CA996102A6       Remote spi: 47088C8FB9F039AD
     Local id: 192.168.1.1
     Remote id: 192.168.2.2
      DPD configured for 10 seconds, retry 3
     NAT-T is not detected
Child sa: local selector  10.10.10.0/0 - 10.10.10.255/65535
         remote selector 10.20.20.0/0 - 10.20.20.255/65535
         ESP spi in/out: 0x637df131/0xb7224866

ASA1# sh crypto ipsec sa
interface: outside
   Crypto map tag: vpn, seq num: 12, local addr: 192.168.1.1
     access-list NEWARK extended permit ip 10.10.10.0 255.255.255.0
     10.20.20.0 255.255.255.0
     local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
     remote ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
     current_peer: 192.168.2.2
     #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
```

PSK Verification After Migration

In order to verify your PSK, you can run this command in the global configuration mode:

```
more system: running-config | beg tunnel-group
```

IKEv2 and Tunnel Manager Process

As mentioned before, the ASA uses a module called tunnel manager/IKE common on the initiator to determine the crypto map and IKE protocol version to use for a connection. Enter this command to monitor the module:

```
debug crypto ike-common <level>
```

The **debug**, **logging**, and **show** commands were collected when traffic is passed to initiate the IKEv2 tunnel. For clarity, some of the output has been omitted.

```
ASA1(config)# logging enable
ASA1(config)# logging list IKEv2 message 750000-752999
ASA1(config)# logging console IKEv2
ASA1(config)# exit
ASA1# debug crypto IKEv2 platform 4
ASA1# debug crypto IKEv2 protocol  4
ASA1# debug crypto ike-common 5

%ASA-5-752003: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2.
Map Tag = vpn.  Map Sequence Number = 12.
%ASA-5-750001: Local:192.168.1.1:500 Remote:192.168.2.2:500 Username:Unknown
Received request to establish an IPsec tunnel; local traffic selector = Address
Range:
10.10.10.11-10.10.10.11 Protocol: 0
Port Range: 0-65535; remote traffic selector = Address Range:
10.20.20.21-10.20.20.21 Protocol: 0 Port Range: 0-65535
Mar 22 15:03:52 [IKE COMMON DEBUG]Tunnel Manager dispatching a KEY_ACQUIRE
message to IKEv2.  Map Tag = vpn.  Map Sequence Number = 12.
IKEv2-PLAT-3: attempting to find tunnel group for IP: 192.168.2.2
IKEv2-PLAT-3: mapped to tunnel group 192.168.2.2 using peer IP
    26%ASA-5-750006: Local:192.168.1.1:500 Remote:192.168.2.2:500
Username:192.168.2.2 SA UP. Reason: New Connection Established
43%ASA-5-752016: IKEv2 was successful at setting up a tunnel.
Map Tag = vpn. Map Sequence Number = 12.
%ASA-7-752002: Tunnel Manager Removed entry.  Map Tag = vpn.
Map Sequence Number = 12.
IKEv2-PLAT-4: SENT PKT [IKE_SA_INIT] [192.168.1.1]:500->[192.168.2.2]:500
InitSPI=0x297ef9ca996102a6 RespSPI=0x0000000000000000 MID=00000000
IKEv2-PROTO-3: (12): Insert SA
IKEv2-PLAT-4: RECV PKT [IKE_SA_INIT] [192.168.2.2]:500->[192.168.1.1]:500
InitSPI=0x297ef9ca996102a6 RespSPI=0x47088c8fb9f039ad MID=00000000
IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [192.168.1.1]:500->[192.168.2.2]:500
InitSPI=0x297ef9ca996102a6 RespSPI=0x47088c8fb9f039ad MID=00000001
IKEv2-PLAT-4: RECV PKT [IKE_AUTH] [192.168.2.2]:500->[192.168.1.1]:500
InitSPI=0x297ef9ca996102a6 RespSPI=0x47088c8fb9f039ad MID=00000001
IKEv2-PROTO-3: (12): Verify peer's policy
IKEv2-PROTO-3: (12): Get peer authentication method
IKEv2-PROTO-3: (12): Get peer's preshared key for 192.168.2.2
IKEv2-PROTO-3: (12): Verify authentication data
IKEv2-PROTO-3: (12): Use preshared key for id 192.168.2.2, key len 5
IKEv2-PROTO-2: (12): SA created; inserting SA into database
IKEv2-PLAT-3:
CONNECTION STATUS: UP... peer: 192.168.2.2:500, phase1_id: 192.168.2.2
IKEv2-PROTO-3: (12): Initializing DPD, configured for 10 seconds
IKEv2-PLAT-3: (12) DPD Max Time will be: 10
```

```
IKEv2-PROTO-3: (12): Checking for duplicate SA
Mar 22 15:03:52 [IKE COMMON DEBUG]IKEv2 was successful at setting up a tunnel.
Map Tag = vpn. Map Sequence Number = 12.
Mar 22 15:03:52 [IKE COMMON DEBUG]Tunnel Manager Removed entry.
Map Tag = vpn.  Map Sequence Number = 12.
```

IKEv2 to IKEv1 Fallback Mechanism

With both IKEv1 and IKEv2 in parallel, the ASA always prefers to initiate IKEv2. If the ASA cannot, it falls back to IKEv1. The Tunnel manager/IKE common module manages this process. In this example on the initiator, the IKEv2 SA was cleared and IKEv2 is now purposely mis-configured (the IKEv2 proposal is removed) to demonstrate the fall back mechanism.

```
ASA1# clear  crypto  IKEv2 sa

%ASA-5-750007: Local:192.168.1.1:500 Remote:192.168.2.2:500
Username:192.168.2.2 SA DOWN. Reason: operator request
ASA1(config)# no crypto map vpn 12 set IKEv2 ipsec-proposal GOSET
ASA1# (config ) logging enable
ASA1# (config ) logging list IKEv2 message 750000-752999
ASA1# (config ) logging console IKEv2
ASA1# (config ) exit
ASA1# debug crypto IKEv2 platform 4
ASA1# debug crypto IKEv2 protocol  4
ASA1# debug crypto ike-common 5
%ASA-5-752004: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1.
Map Tag = vpn.  Map Sequence Number = 12.
%ASA-4-752010: IKEv2 Doesn't have a proposal specified
Mar 22 15:11:44 [IKE COMMON DEBUG]Tunnel Manager dispatching a KEY_ACQUIRE
message to IKEv1.  Map Tag = vpn.  Map Sequence Number = 12.
Mar 22 15:11:44 [IKE COMMON DEBUG]IKEv2 Doesn't have a proposal specified
%ASA-5-752016: IKEv1 was successful at setting up a tunnel.  Map Tag = vpn.
Map Sequence Number = 12.
%ASA-7-752002: Tunnel Manager Removed entry.  Map Tag = vpn.
Map Sequence Number = 12.
Mar 22 15:11:44 [IKE COMMON DEBUG]IKEv1 was successful at setting up a tunnel.
Map Tag = vpn. Map Sequence Number = 12.
Mar 22 15:11:44 [IKE COMMON DEBUG]Tunnel Manager Removed entry.  Map Tag = vpn.
Map Sequence Number = 12.

ASA1(config)# sh cry IKEv2 sa
There are no IKEv2 SAs
ASA1(config)# sh cry IKEv1 sa
IKEv1 SAs:
  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: 192.168.2.2
   Type    : L2L             Role    : initiator
   Rekey   : no              State   : MM_ACTIVE
```

Harden IKEv2

In order to provide additional security when IKEv2 is used, these optional commands are highly recommended:

- **Crypto IKEv2 cookie-challenge**: Enables the ASA to send cookie challenges to peer devices in response to half-open SA initiated packets.

- **Crypto IKEv2 limit max-sa**: Limits the number of IKEv2 connections on the ASA. By default, the maximum allowed IKEv2 connection equals the maximum number of connections specified by the ASA license.
- **Crypto IKEv2 limit max-in-negotiation-sa**: Limits the number of IKEv2 in-negotiation (open) SAs on the ASA. When used in conjunction with the **crypto IKEv2 cookie-challenge** command, ensure the cookie-challenge threshold is lower than this limit.
- Use asymmetric keys. After migration, the configuration can be modified to use asymmetric keys as shown here:

  ```
  ASA-2(config)# more system:running-config
  tunnel-group <peer_ip-address> type ipsec-l2l
  tunnel-group <peer_ip-address> ipsec-attributes
   IKEv1 pre-shared-key cisco1234
   IKEv2 remote-authentication pre-shared-key cisco1234
   IKEv2 local-authentication pre-shared-key cisco123
  ```

It is important to realize that the configuration needs to be mirrored on the other peer for the IKEv2 pre-shared-key. It will not work if you select and paste the configuration from one side to the other.

Note: These commands are disabled by default.

Related Information

- **Technical Support & Documentation**