IKEv2 IPSEC Site-to-Site VPNs

Introduction to Internet Key Exchange Version 2

IKEv2, a next-generation key management protocol based on RFC 4306, is an enhancement of the IKE protocol.

IKEv2 supports crypto map-and tunnel protection-based crypto interfaces. The crypto map-based applications include static and dynamic crypto maps, and the tunnel protection-based applications pertain to IPsec static VTI (sVTI), dynamic VTI (dVTI), point-point, and multipoint generic routing encapsulation (mGRE) tunnel interfaces. The VPN solutions include site-to-site VPN, DMVPN, and remote access VPN headend.

IKEv2 Proposal

An IKEv2 proposal is a collection of transforms used in the negotiation of IKE SAs as part of the IKE_SA_INIT exchange. The transform types used in the negotiation are as follows:

- Encryption algorithm
- Integrity algorithm
- Diffie-Hellman (DH) group

Cisco IOS Suite-B Support for IKEv2 Proposal

Suite-B adds support for the SHA-2 family (HMAC variant) hash algorithm used to authenticate packet data and verify the integrity verification mechanisms for the IKEv2 proposal configuration. HMAC is a variant that provides an additional level of hashing.

IKEv2 Policy

An IKEv2 policy contains proposals that are used to negotiate the encryption, integrity, PRF algorithms, and DH group in SA_INIT exchange. It can have match statements which are used as selection criteria to select a policy during negotiation.

IKEv2 Profile

An IKEv2 profile is a repository of the nonnegotiable parameters of the IKE SA, such as local or remote identities and authentication methods and the services that are available to the authenticated peers that match the profile. An IKEv2 profile must be attached to either crypto map or IPsec profile on both IKEv2 initiator and responder.

IKEv2 Keyring

An IKEv2 keyring is a repository of symmetric and asymmetric preshared keys and is independent of the IKEv1 keyring. The IKEv2 keyring is associated with an IKEv2 profile and hence, caters to a set of peers that match the IKEv2 profile. The IKEv2 keyring gets its VRF context from the associated IKEv2 profile.
IKEv2 Supported Standards

Cisco implements the IP Security Protocol (IPsec) standard for use in IKEv2.

The component technologies implemented in IKEv2 are as follows:

- AES-CBC--Advanced Encryption Standard-Cipher Block Chaining
- DES--Data Encryption Standard
- Diffie-Hellman--A public-key cryptography protocol
- MD5 (HMAC variant) -- Message digest algorithm 5
- SHA (HMAC variant)--Secure Hash Algorithm

IKEv2 versus IKEv1

Purpose and benefits
The purpose of IKE remains the same whether IKEv1 or IKEv2—to authenticate peers and establish security associations (SAs) used for protecting traffic. However, there are many benefits of IKEv2 over IKEv1, including built-in DoS prevention, support for EAP authentication, in-built NAT-T and so on.

Messages exchanged

Another difference between the two versions of IKE is the number of messages exchanged. IKEv1 has two phases: Phase 1 and Phase 2. Phase 1 can either be Main mode (6 messages) or Aggressive mode (3 messages). IKEv1 Phase 2 has only one mode – Quick mode (3 messages). For more details about these modes, you can read the following articles: Main Mode, Aggressive Mode and Quick mode.

In IKEv2, there are no defined phases as in IKEv1. IKEv2 makes use of four types of messages: IKE_SA_INIT, IKE_AUTH, CREATE_CHILD_SA, and INFORMATIONAL and these messages are exchanged in a request-response manner. In most cases, four messages (a pair of IKE_SA_INIT messages and a pair of IKE_AUTH messages) are enough to set up both the IKE SA and the first child SA but there may be variations. As we go on in this IKEv2 series, we will talk more about these message exchanges.

Authentication methods
IKEv1 supports authentication via pre-shared keys, digital signatures, and public key encryption. IKEv2 supports pre-shared keys, digital signatures and EAP. Apart from this, both IPSec peers in IKEv1 must use the same type of authentication, e.g., both pre-shared key or both digital signature. However, IKEv2 supports asymmetric authentication: One side can authenticate using pre-shared keys while the other side uses digital signatures.
Configuration on the Cisco IOS

The way IKEv2 is configured on the Cisco IOS is also considerably different from the way IKEv1 is configured. There are new terminologies that we need to be aware of to successfully configure IKEv2 and in fact, IKEv2 configuration is easier than IKEv1, Cisco call it as Smart implementation of Phase I.

Configuration Example:

Task-1: Configure IKEv2 Site-to-Site VPN using legacy Crypto Map to encrypt traffic between 10.1.1.0/24 & 10.3.3.0/24.

Task-2: Configure IKEv2 Site-to-Site VPN using S-VTI based setup to encrypt traffic between 10.2.2.0/24 & 10.4.4.0/24.

Initial Configuration:

R1:

```
interface Ethernet0/0
 ip address 192.1.10.1 255.255.255.0
 end

ip route 0.0.0.0 0.0.0.0 192.1.10.5
```

R2:

```
interface Ethernet0/0
 ip address 192.1.20.2 255.255.255.0
 end

ip route 0.0.0.0 0.0.0.0 192.1.20.5
```
R3:

```
interface Ethernet0/0
  ip address 192.1.30.3 255.255.255.0
end

ip route 0.0.0.0 0.0.0.0 192.1.30.5
```

R4:

```
interface Ethernet0/0
  ip address 192.1.40.4 255.255.255.0
end

ip route 0.0.0.0 0.0.0.0 192.1.40.5
```

R5:

```
interface Ethernet0/0
  ip address 192.1.10.5 255.255.255.0
end

interface Ethernet0/1
  ip address 192.1.20.5 255.255.255.0
end

interface Ethernet0/2
  ip address 192.1.30.5 255.255.255.0
end

interface Ethernet0/3
  ip address 192.1.40.5 255.255.255.0
end
```

**Task-1:** Configure IKEv2 Site-to-Site VPN using legacy Crypto Map to encrypt traffic between 10.1.1.0/24 & 10.3.3.0/24.

**Solution:**

**R1:**

**Step-1:** Configure Phase I

**Step-1[A]:** Configure IKEv2 Proposal:

```
crypto ikev2 proposal PROP-1
  encryption 3des aes-cbc-192
  integrity md5 sha256
  group 2 5
```
**Step-1[B]:** Configure IKEv2 Policy:

```plaintext
crypto ikev2 policy POLICY-1
  proposal PROP-1
```

**Step-1[C]:** Configure IKEv2 keyring:

```plaintext
crypto ikev2 keyring KR-1
  peer T0-R3
    address 192.1.30.3
    pre-shared-key local cisco11
    pre-shared-key remote cisco222
```

**Step-1[D]:** Configure IKEv2 Profile:

```plaintext
crypto ikev2 profile IKE_PROF
  match identity remote address 192.1.30.3 255.255.255.255
  authentication remote pre-share
  authentication local pre-share
  keyring local KR-1
```

**Step-2:** Configure Phase II

```plaintext
crypto ipsec transform-set TSET esp-3des esp-md5-hmac
```

**Step-3:** Configure Interested Traffic:

```plaintext
access-list 101 permit ip 10.1.1.0 0.0.0.255 10.3.3.0 0.0.0.255
```

**Step-4:** Configure Crypto Map:

```plaintext
crypto map CMAP 1 ipsec-isakmp
  set peer 192.1.30.3
  set transform-set TSET
  set ikev2-profile IKE_PROF
  match address 101
```

**Step-5:** Apply Crypto Map to Interface:

```plaintext
interface Ethernet0/0
  crypto map CMAP
end
```

**R3:**

**Step-1:** Configure Phase I

**Step-1[A]:** Configure IKEv2 Proposal:

```plaintext
crypto ikev2 proposal PROP-1
  encryption 3des aes-cbc-192
  integrity md5 sha256
  group 2 5
```
Step-1[B]: Configure IKEv2 Policy:

```plaintext
crypto ikev2 policy POLICY-1
  proposal PROP-1
```

Step-1[C]: Configure IKEv2 keyring:

```plaintext
crypto ikev2 keyring KR-1
  peer TO-R1
    address 192.1.10.1
    pre-shared-key local cisco222
    pre-shared-key remote cisco111
```

Step-1[D]: Configure IKEv2 Profile:

```plaintext
crypto ikev2 profile IKE_PROF
  match identity remote address 192.1.10.1 255.255.255.255
  authentication remote pre-share
  authentication local pre-share
  keyring local KR-1
```

Step-2: Configure Phase II

```plaintext
crypto ipsec transform-set TSET esp-3des esp-md5-hmac
```

Step-3: Configure Interested Traffic:

```plaintext
access-list 101 permit ip 10.3.3.0 0.0.0.255 10.1.1.0 0.0.0.255
```

Step-4: Configure Crypto Map:

```plaintext
crypto map CMAP 1 ipsec-isakmp
  set peer 192.1.10.1
  set transform-set TSET
  set ikev2-profile IKE_PROF
  match address 101
```

Step-5: Apply Crypto Map to Interface:

```plaintext
interface Ethernet0/0
  crypto map CMAP
end
```

Verification:

```
R1#ping 10.3.3.3 source 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
!!!!!
```
R1#show crypto ikev2 sa
IPv4 Crypto IKEv2 SA

<table>
<thead>
<tr>
<th>Tunnel-id</th>
<th>Local</th>
<th>Remote</th>
<th>fvrf/ivrf</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.1.10.1/500</td>
<td>192.1.30.3/500</td>
<td>none/none</td>
<td>READY</td>
</tr>
</tbody>
</table>

Encr: 3DES, PRF: MD5, Hash: MD596, DH Grp:2, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/2171 sec

R1#show crypto ipsec sa

interface: Ethernet0/0
Crypto map tag: CMAP, local addr 192.1.10.1

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.3.3.0/255.255.255.0/0/0)
current_peex 192.1.30.3 port 500

#pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 14
#pkts decaps: 14, #pkts decrypt: 14, #pkts verify: 14
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 192.1.10.1, remote crypto endpt.: 192.1.30.3
plaintext mtu 1446, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0x82C256FE(2193774334)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xB2CF9B8E(2999950222)
  transform: esp-3des esp-md5-hmac
  in use settings ={Tunnel, }
  conn id: 2, flow_id: SW:2, sibling_flags 80000040, crypto map: CMAP
  sa timing: remaining key lifetime (k/sec): (4185654/1409)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x82C256FE(2193774334)
  transform: esp-3des esp-md5-hmac
  in use settings ={Tunnel, }
  conn id: 1, flow id: SW:1, sibling_flags 80000040, crypto map: CMAP
  sa timing: remaining key lifetime (k/sec): (4185654/1409)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE(ACTIVE)
**Task-2:** Configure IKEv2 Site-to-Site VPN using S-VTI based setup to encrypt traffic between 10.2.2.0/24 & 10.4.4.0/24.

**Solution:**

R2:

**Step-1:** Configure Phase I

**Step-1[A]:** Configure IKEv2 Proposal:

```plaintext
crypto ikev2 proposal PROP-1
  encryption 3des aes-cbc-192
  integrity md5 sha256
  group 2 5
```

**Step-1[B]:** Configure IKEv2 Policy:

```plaintext
crypto ikev2 policy POLICY-1
  proposal PROP-1
```

**Step-1[C]:** Configure IKEv2 keyring:

```plaintext
crypto ikev2 keyring KR-1
  peer TO-R4
  address 192.1.40.4
  pre-shared-key cisco123
```

**Step-1[D]:** Configure IKEv2 Profile:

```plaintext
crypto ikev2 profile IKE_PROF
  match identity remote address 192.1.40.4 255.255.255.255
  authentication remote pre-share
  authentication local pre-share
  keyring local KR-1
```

**Step-2:** Configure Phase II

```plaintext
crypto ipsec transform-set TSET esp-3des esp-md5-hmac
```

**Step-3:** Configure IPSEC Profile:

```plaintext
crypto ipsec profile IPSEC
  set transform-set TSET
  set ikev2-profile IKE_PROF
```
Step-4: Configure Tunnel interface and apply IPSEC profile to it.

```plaintext
interface Tunnel1
 ip address 192.168.1.1 255.255.255.0
tunnel source 192.1.20.2
tunnel destination 192.1.40.4
tunnel protection ipsec profile IPSEC
end
```

Step-5: Configure Routing protocol:

```plaintext
router eigrp 1
 network 10.0.0.0
 network 192.168.1.0
```

R4:

Step-1: Configure Phase I

Step-1[A]: Configure IKEv2 Proposal:

```plaintext
crypto ikev2 proposal PROP-1
 encryption 3des aes-cbc-192
 integrity md5 sha256
 group 2 5
```

Step-1[B]: Configure IKEv2 Policy:

```plaintext
crypto ikev2 policy POLICY-1
 proposal PROP-1
```

Step-1[C]: Configure IKEv2 keyring:

```plaintext
crypto ikev2 keyring KR-1
 peer TO-R2
 address 192.1.20.2
 pre-shared-key cisco123
```

Step-1[D]: Configure IKEv2 Profile:

```plaintext
crypto ikev2 profile IKE_PROF
 match identity remote address 192.1.20.2 255.255.255.255
 authentication remote pre-share
 authentication local pre-share
 keyring local KR-1
```

Step-2: Configure Phase II

```plaintext
crypto ipsec transform-set TSET esp-3des esp-md5-hmac
```
**Step-3:** Configure IPSEC Profile:

```
crypto ipsec profile IPSEC
set transform-set TSET
set ikev2-profile IKE PROF
```

**Step-4:** Configure Tunnel interface and apply IPSEC profile to it.

```
interface Tunnel1
 ip address 192.168.1.2 255.255.255.0
 tunnel source 192.1.40.4
 tunnel destination 192.1.20.2
 tunnel protection ipsec profile IPSEC
end
```

**Step-5:** Configure Routing protocol:

```
router eigrp 1
 network 10.0.0.0
 network 192.168.1.0
```

**Verification:**

```
R2#show crypto ikev2 sa
 IPv4 Crypto IKEv2 SA
Tunnel-id Local               Remote                fvrf/ivrf    Status
     1 192.1.20.2/500         192.1.40.4/500        none/none   READY
 Encri: 3DES, PRF: MD5, Hash: MD596, DH Grp:2, Auth sign: PSK, Auth verify: PSK
 Life/Active Time: 86400/3814 sec

R2#show crypto ipsec sa
interface: Tunnel1
  Crypto map tag: Tunnel1-head-0, local addr 192.1.20.2
  protected vrf: (none)
  local ident (addr/mask/prot/port): (192.1.20.2/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (192.1.40.4/255.255.255.255/47/0)
  current peer 192.1.40.4 port 500
       PERMIT, flags={origin_is_acl,}
 #pkts encaps: 841, #pkts encrypt: 841, #pkts digest: 841
 #pkts decaps: 842, #pkts decrypt: 842, #pkts verify: 842
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 0, #recv errors 0
 local crypto endpt.: 192.1.20.2, remote crypto endpt.: 192.1.40.4
 plaintext mtu 1446, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
 current outbound spi: 0xD233E225(3526615589)
 PFS (Y/N): N, DH group: none

 inbound esp sas:
   spi: 0x6228E1E1(1646846433)
   transform: esp-3des esp-md5-hmac,
               in use settings ={Tunnel, }
   conn id: 6, flow_id: SW:6, sibling_flags 80000040, crypto map: Tunnel1-
              head-0
```
sa timing: remaining key lifetime (k/sec): (4360291/3177)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x233E225(3526615589)
transform: esp-3des esp-md5-hmac,
in use settings ={Tunnel, }
conn id: 5, flow_id: SW:5, sibling_flags 80000040, crypto map: Tunnel1-
head-0

sa timing: remaining key lifetime (k/sec): (4360291/3177)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

R2#ping 10.4.4.4 source 10.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 10.2.2.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/6 ms

Thank You!!!