Dynamic Site to Site IKEv2 VPN Tunnel Between an ASA and an IOS Router Configuration Example

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Configure
Scenario 1
Network Diagram
Configuration
Scenario 2
Network Diagram
Configuration
Verify
Static ASA
Dynamic Router
Dynamic Router (with Remote Dynamic ASA)
Troubleshoot

Introduction

This document describes how to configure a site-to-site Internet Key Exchange Version 2 (IKEv2) VPN tunnel between an Adaptive Security Appliance (ASA) and a Cisco router where the router has a dynamic IP address and the ASA has a static IP address on the public-facing interfaces.

Prerequisites

Requirements

There are no specific requirements for this document.

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

- Cisco IOS® Version 15.1(1)T or later
- Cisco ASA Version 8.4(1) or 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.

**Background Information**

This document discusses these scenarios:

- **Scenario 1:** An ASA is configured with a static IP address that uses a named tunnel group and the router is configured with a dynamic IP address.

- **Scenario 2:** An ASA is configured with a dynamic IP address and the router is configured with a dynamic IP address.

- **Scenario 3:** This scenario is not discussed here. In this scenario, the ASA is configured with a static IP address but uses the DefaultL2LGroup tunnel group. The configuration for this is similar to what is described in the Dynamic Site to Site IKEv2 VPN Tunnel Between Two ASAs Configuration Example article.

The biggest configuration difference between Scenarios 1 and 3 is the Internet Security Association and Key Management Protocol (ISAKMP) ID used by the remote router. When the DefaultL2LGroup is used on the static ASA, the peer's ISAKMP ID on the router must be the address of the ASA. However, if a named tunnel group is used, the peer's ISAKMP ID on the router must be the same as the tunnel group name configured on the ASA. This is accomplished with this command on the router:

```plaintext
identity local key-id <name of the tunnel-group on the static ASA>
```

The advantage of using named tunnel groups on the static ASA is that when the DefaultL2LGroup is used, the configuration on the remote dynamic ASAs/routers, which includes the pre-shared keys, must be identical and it does not allow for much granularity with the setup of policies.

**Configure**

**Scenario 1**

**Network Diagram**

**Configuration**

This section describes the configuration on the ASA and the router based on the Named tunnel-group configuration.
Static ASA Configuration

interface Ethernet0/0
  nameif outside
  security-level 0
  ip address 201.1.1.2 255.255.255.0
!
crypto ipsec ikev2 ipsec-proposal ESP-AES-SHA
  protocol esp encryption aes
  protocol esp integrity sha-1
  crypto ipsec security-association pmtu-aging infinite
  crypto dynamic-map dmap 1 set ikev2 ipsec-proposal ESP-AES-SHA
  crypto map vpn 1 ipsec-isakmp dynamic dmap
  crypto map vpn interface outside
  crypto ca trustpool policy
  crypto ikev2 policy 1
     encryption 3des
     integrity sha
     group 5 2
     prf sha
     lifetime seconds 86400
  crypto ikev2 enable outside

  group-policy Site-to-Site internal
  group-policy Site-to-Site attributes
     vpn-tunnel-protocol ikev2
  tunnel-group S2S-IKEv2 type ipsec-l2l
  tunnel-group S2S-IKEv2 general-attributes
    default-group-policy Site-to-Site
  tunnel-group S2S-IKEv2 ipsec-attributes
    ikev2 remote-authentication pre-shared-key cisco321
    ikev2 local-authentication pre-shared-key cisco123

Dynamic Router Configuration

The Dynamic Router is configured almost the same way as you normally configure in cases where the router is a dynamic site for IKEv2 L2L tunnel with the addition of one command as shown here:

  ip access-list extended vpn
     permit ip host 10.10.10.1 host 201.1.1.2

  crypto ikev2 proposal L2L-Prop
     encryption 3des
     integrity sha1
     group 2 5
  
  crypto ikev2 policy L2L-Pol
     proposal L2L-Prop
  
  crypto ikev2 keyring L2L-Keyring
     peer vpn
        address 201.1.1.2
        pre-shared-key local cisco321
        pre-shared-key remote cisco123
  
  crypto ikev2 profile L2L-Prof
     match identity remote address 201.1.1.2 255.255.255.255
     identity local key-id S2S-IKEv2
     authentication remote pre-share
So on every dynamic peer, the key-id is different and a corresponding tunnel-group must be created on the Static ASA with the right name, which also increases the granularity of the policies that are implemented on an ASA.

Scenario 2

**Note:** This configuration is only possible when at least one side is a router. If both sides are ASAs, this setup does not work at this time. In Version 8.4, the ASA is not able to use the Fully Qualified Domain Name (FQDN) with the `set peer` command, but CSCus37350 enhancement has been requested for future releases.

If the remote ASA’s IP address is dynamic as well however has a Fully Qualified Domain Name assigned for its VPN interface, then rather than define the IP address of the remote ASA, you now define the FQDN of the remote ASA with this command on the router:

```
C1941(config)#do show run | sec crypto map
```

```
crypto map vpn 10 ipsec-isakmp
  set peer <FQDN> dynamic
```

**Tip:** The `dynamic` keyword is optional. When you specify the hostname of a remote IPsec peer via the `set peer` command, you can also issue the dynamic keyword, which defers the Domain Name Server (DNS) resolution of the hostname until right before the IPsec tunnel has been established.

Deferring resolution enables the Cisco IOS software to detect whether the IP address of the remote IPsec peer has changed. Thus, the software can contact the peer at the new IP address. If the dynamic keyword is not issued, the hostname is resolved immediately after it is specified. So, the Cisco IOS software cannot detect an IP address change and, therefore, attempts to connect to the IP address that it previously resolved.

**Network Diagram**

**Configuration**
Dynamic ASA Configuration

The configuration on the ASA is the same as the Static ASA Configuration with only one exception, which is that the IP address on the physical interface is not statically defined.

Router Configuration

crypto ikev2 keyring L2L-Keyring
peer vpn
  hostname asa5510.test.com
  pre-shared-key local cisco321
  pre-shared-key remote cisco123
!
crypto ikev2 profile L2L-Prof
  match identity remote fqdn domain test.com
  identity local key-id S2S-IKEv2
  authentication remote pre-share
  authentication local pre-share
  keyring local L2L-Keyring

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
  mode tunnel

crypto map vpn 10 ipsec-isakmp
  set peer asa5510.test.com dynamic
  set transform-set ESP-AES-SHA
  set ikev2-profile L2L-Prof
  match address vpn

Verify

Use this section in order to confirm that your configuration works properly.

Static ASA

- Here is the result of the show crypto IKEv2 sa det command:

  IKEv2 SAs:

  Session-id:23, Status:UP-ACTIVE, IKE count:1, CHILD count:1

  Tunnel-id          Local               Remote               Status          Role
  120434199          201.1.1.2/4500     201.1.1.1/4500       READY          RESPONDER
  Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
  Life/Active Time: 86400/915 sec
  Session-id: 23
  Status Description: Negotiation done
  Local spi: 97272A4B4DED4A5C    Remote spi: 67E01CB8E8619AF1
  Local id: 201.1.1.2
  Remote id: S2S-IKEv2
  Local req mess id: 43          Remote req mess id: 2
  Local next mess id: 43         Remote next mess id: 2
  Local req queued: 43           Remote req queued: 2
  Local window: 1                Remote window: 5
DPD configured for 10 seconds, retry 2
NAT-T is detected outside
Child sa: local selector 201.1.1.2/0 - 201.1.1.2/65535
remote selector 10.10.10.1/0 - 10.10.10.1/65535
ESP spi in/out: 0x853c02/0x41aa84f4
AH spi in/out: 0x0/0x0
CPI in/out: 0x0/0x0
Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
ah_hmac: None, comp: IPCOMP_NONE, mode tunnel

- Here is the result of the show crypto ipsec sa command:

```
interface: outside
    Crypto map tag: dmap, seq num: 1, local addr: 201.1.1.2
    local ident (addr/mask/prot/port): (201.1.1.2/255.255.255.255/0/0)
    remote ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0)
    current_peer: 201.1.1.1
    #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
    #TFC rcvd: 0, #TFC sent: 0
    #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
    #send errors: 0, #recv errors: 0
    local crypto endpt.: 201.1.1.2/4500, remote crypto endpt.: 201.1.1.1/4500
    path mtu 1500, ipsec overhead 82(52), media mtu 1500
    PMTU time remaining (sec): 0, DF policy: copy-df
    ICMP error validation: disabled, TFC packets: disabled
    current outbound spi: 41AA84F4
    current inbound spi : 00853C02
inbound esp sas:
    spi: 0x00853C02 (8731650)
    transform: esp-aes esp-sha-hmac no compression
    in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, }
    slot: 0, conn_id: 94208, crypto-map: dmap
    sa timing: remaining key lifetime (kB/sec): (4101119/27843)
    IV size: 16 bytes
    replay detection support: Y
    Anti replay bitmap:
        0x00000000 0x00000000
outbound esp sas:
    spi: 0x41AA84F4 (1101694196)
    transform: esp-aes esp-sha-hmac no compression
    in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, }
    slot: 0, conn_id: 94208, crypto-map: dmap
    sa timing: remaining key lifetime (kB/sec): (4055039/27843)
    IV size: 16 bytes
    replay detection support: Y
    Anti replay bitmap:
        0x00000000 0x00000001
```

Dynamic Router

- Here is the result of the show crypto IKEv2 sa detail command:
### IPv4 Crypto IKEv2 SA

<table>
<thead>
<tr>
<th>Tunnel-id</th>
<th>Local</th>
<th>Remote</th>
<th>pvrf/ivrf</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.1.2/4500</td>
<td>201.1.1.2/4500</td>
<td>none/none</td>
<td>READY</td>
</tr>
</tbody>
</table>

- **Encr:** 3DES, **Hash:** SHA96, **DH Grp:**2, **Auth sign:** PSK, **Auth verify:** PSK
- **Life/Active Time:** 86400/1013 sec
- **Status Description:** Negotiation done
- **Local spi:** 67E01CB8E8619AF1, **Remote spi:** 97272A4B4DED4A5C
- **Local id:** S2S-IKEv2, **Remote id:** 201.1.1.2
- **Local req msg id:** 2, **Remote req msg id:** 48
- **Local next msg id:** 2, **Remote next msg id:** 48
- **Local req queued:** 2, **Remote req queued:** 48
- **Local window:** 5, **Remote window:** 1
- **DPD configured for 0 seconds, retry 0**
- **Fragmentation not configured.**
- **Extended Authentication not configured.**
- **NAT-T is detected inside**
- **Cisco Trust Security SGT is disabled**
- **Initiator of SA:** Yes

### IPv6 Crypto IKEv2 SA

- **Here is the result of the `show crypto ipsec sa` command:**

```plaintext
interface: GigabitEthernet0/0
  Crypto map tag: vpn, local addr 192.168.1.2

  protected vrf: (none)
  local ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (201.1.1.2/255.255.255.255/0/0)
  current_peer 201.1.1.2 port 4500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 6
    #pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 6
    #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.: 192.168.1.2, remote crypto endpt.: 201.1.1.2
  plaintext mtu 1422, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
  current outbound spi: 0x853C02(8731650)
  PFS (Y/N): N, DH group: none

  inbound esp sas:
    spi: 0x41AA84F4(1101694196)
      transform: esp-aes esp-sha-hmac ,
      in use settings ={Tunnel UDP-Encaps, }
      conn id: 2006, flow_id: Onboard VPN:6, sibling_flags 80000040, crypto map: vpn
      sa timing: remaining key lifetime (k/sec): (4263591/2510)
      IV size: 16 bytes
      replay detection support: Y
      Status: ACTIVE(ACTIVE)

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
```

spi: 0x853C02(8731650)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel UDP-Encaps, }
conn id: 2005, flow_id: Onboard VPN:5, sibling_flags 80000040, crypto map: vpn
sa timing: remaining key lifetime (k/sec): (4263591/2510)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

Dynamic Router (with Remote Dynamic ASA)

• Here is the result of the show crypto IKEv2 sa detail command:

C1941#show cry ikev2 sa detailed
IPv4 Crypto IKEv2 SA
Tunnel-id Local Remote fvrf/ivrf Status
1 192.168.1.2/4500 201.1.1.2/4500 none/none READY
Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/1516 sec
CE id: 1034, Session-id: 24
Status Description: Negotiation done
Local spi: 98322AE66163EE83 Remote spi: 092A1E5620F6AA9C
  Local id: S2S-IKEv2
  Remote id: asa5510.test.com
  Local req msg id: 2 Remote req msg id: 73
  Local next msg id: 2 Remote next msg id: 73
  Local req queued: 2 Remote req queued: 73
  Local window: 5 Remote window: 1
DPD configured for 0 seconds, retry 0
Fragmentation not configured.
Extended Authentication not configured.
NAT-T is detected inside
Cisco Trust Security SGT is disabled
Initiator of SA : Yes

IPv6 Crypto IKEv2 SA

Note: The remote and local ID in this output is the named tunnel-group you defined on the ASA to verify if you fall on the right tunnel-group. This can also be verified if you debug IKEv2 on either end.

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

The Output Interpreter Tool (registered customers only) supports certain show commands. Use the Output Interpreter Tool in order to view an analysis of show command output.

Note: Refer to Important Information on Debug Commands before you use debug commands.
On the Cisco IOS Router, use:

  deb crypto ikev2 error
  deb crypto ikev2 packet
  deb crypto ikev2 internal

On the ASA, use:

  deb crypto ikev2 protocol
  deb crypto ikev2 platform