ASA 和 IOS 路由器之间的动态站点到站点 IKEv2 VPN 隧道配置示例

目录

简介

本文档介绍如何配置自适应安全设备 (ASA) 和思科路由器之间的站点到站点互联网密钥交换版本 2 (IKEv2) VPN 隧道，其中路由器拥有动态 IP 地址，ASA 在公共接口上有静态 IP 地址。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS® 15.1(1)T版或更高

- Cisco ASA 版本 8.4(1) 或以上版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

本文档讨论以下场景：

- 情形 1：ASA 配置为使用命名隧道组的静态 IP 地址，而路由器配置为动态 IP 地址。
- 方案 2：ASA 配置为动态 IP 地址，而路由器也配置为动态 IP 地址。
- 情形 3：此处不讨论此方案。在此方案中，ASA配置了静态IP地址，但使用DefaultL2LGroup隧道组。此场景的配置类似于 Dynamic Site to Site IKEv2 VPN Tunnel Between Two ASAs Configuration Example（两个 ASA 之间的动态站点到站点 IKE v2 VPN 隧道配置示例）文章中所述的场景。

场景 1 和 3 之间的最大配置差别是远程路由器使用的互联网安全关联和密钥管理协议 (ISAKMP) ID。当 DefaultL2LGroup 用于静态 ASA 上时，路由器上的对等体 ISAKMP ID 必须是 ASA 的地址。但是，如果使用了已命名隧道组，则路由器上的对等体 ISAKMP ID 必须与 ASA 上配置的隧道组名称相同。这是通过在路由器上使用此命令来实现：

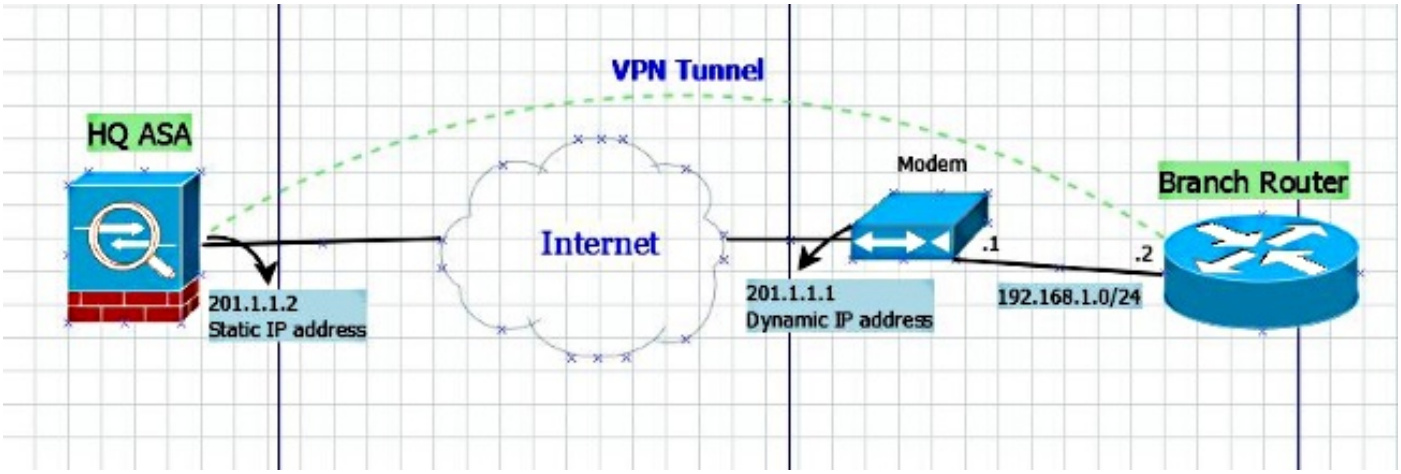
```
identity local key-id
```

在静态 ASA 上使用命名隧道组的优势在于，当使用 DefaultL2LGroup 时，远程动态 ASA/路由器上的配置（包括预共享密钥）必须相同且不允许在设置策略时进行细化。

配置

场景 1

网络图



配置

此部分基于命名隧道组配置介绍 ASA 和路由器上的配置。

静态 ASA 配置

```
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
```

动态路由器配置

动态路由器的配置方法与您通常在路由器是 IKEv2 L2L 隧道的动态站点情况下外加一条命令进行配置的方法几乎相同，如下所示：

```
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
 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 201.1.1.2
 set transform-set ESP-AES-SHA
 set ikev2-profile L2L-Prof
 match address vpn
!
interface GigabitEthernet0/0
 ip address 192.168.1.2 255.255.255.0
 duplex auto
 speed auto
 crypto map vpn
```

因此在每个动态对等体上，key-id 不同，并且必须在静态 ASA 上创建具有正确名称的对应隧道组，这也会增加 ASA 上实施的政策的精细度。

场景 2

> **注意**：仅当至少一端是路由器时，才可能进行此配置。如果两端都是 ASA，这时候此设置不起作用。在版本 8.4 中，ASA 不能通过 set peer 命令使用完全限定域名 (FQDN)，但我们已要求在未来版本中提供 CSCus37350 增强。

但是，如果远程 ASA 的 IP 地址也是动态的，且已为其 VPN 接口分配完全限定域名，那么现在不是定义远程 ASA 的 IP 地址，而是在路由器上使用以下命令定义远程 ASA 的 FQDN：

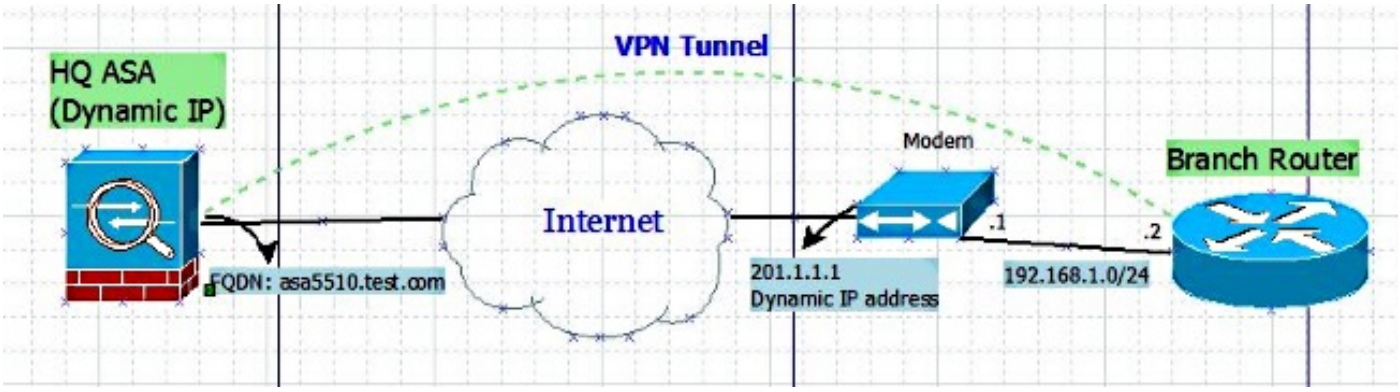
```
C1941(config)#do show run | sec crypto map

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

> **提示：dynamic**关键字是可选的。当通过**set** peer命令指定远程IPsec对等体的主机名时，您还

可以发出dynamic关键字，该关键字将定义主机名的域名服务器(DNS)解析，直到建立IPsec隧道之前。

延迟解析使 Cisco IOS 软件能够检测出远程 IPsec 对等体的 IP 地址是否更改。因此，软件可以在新的IP地址与对等体联系。如果未发出dynamic关键字，则在指定主机名后立即解析主机名。因此，Cisco IOS 软件无法检测 IP 地址更改，并且会尝试连接到之前解析的 IP 地址。

网络图



配置

动态 ASA 配置

ASA 上的配置与静态 ASA 配置相同，唯一的不同是在物理接口上的 IP 地址不是以静态方式定义。

路由器配置

```
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
```

验证

使用本部分可确认配置能否正常运行。

静态ASA

- 以下是 **show crypto IKEv2 sa det** 命令的结果：

```
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
```

- 以下是 **show crypto ipsec sa** 命令的结果：

```
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 0x0000001F
  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
```

动态路由器

- 以下是 **show crypto IKEv2 sa detail** 命令的结果：

```
 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: 86400/1013 sec
     CE id: 1023, Session-id: 23
     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
```

- 以下是 **show crypto ipsec sa** 命令的结果：

```
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:
```

动态路由器（带远程动态 ASA）

- 以下是 **show crypto IKEv2 sa detail** 命令的结果：

```
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: 98322AED6163EE83       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
```

注意：此输出中的远程和本地 ID 是您在 ASA 上定义的命名隧道组，用于验证您是否处于正确的隧道组中。这还可以验证您是否在任一端调试 IKEv2。

故障排除

本部分提供了可用于对配置进行故障排除的信息。

命令输出解释程序工具（仅限注册用户）支持某些 show 命令。使用输出解释器工具来查看 show 命令输出的分析。

注意：使用 debug 命令之前，请参阅有关 Debug 命令的重要信息。

在 Cisco IOS 路由器上，使用以下命令：

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

在 ASA 上，使用以下命令：

```
deb crypto ikev2 protocol
deb crypto ikev2 platform
```