ASA和IOS路由器之間的動態站點到站點IKEv2 VPN隧道配置示例

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[背景資訊](#)
[設定](#)
[案例 1](#)
[網路圖表](#)
[組態](#)
[案例 2](#)
[網路圖表](#)
[組態](#)
[驗證](#)
[靜態ASA](#)
[動態路由器](#)
[動態路由器（帶遠端動態ASA）](#)
[疑難排解](#)

簡介

本文檔介紹如何在自適應安全裝置(ASA)和思科路由器之間配置站點到站點Internet金鑰交換版本2(IKEv2)VPN隧道，其中路由器具有動態IP地址，而ASA在面向公眾的介面上具有靜態IP地址。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS®版本15.1(1)T或更高版本

- Cisco ASA 8.4(1)版或更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

本檔案將討論以下案例：

- 案例 1:ASA配置了使用命名隧道組的靜態IP地址，而路由器配置了動態IP地址。
- 案例 2:ASA配置了動態IP地址，路由器配置了動態IP地址。
- 案例 3:此處未討論此方案。在此方案中，ASA配置了靜態IP地址，但使用DefaultL2LGroup隧道組。此配置的配置與兩個ASA之間的動態站點到站點IKEv2 VPN隧道配置示例文章中介紹的內容類似。

案例1和案例3之間的最大配置差異是遠端路由器使用的網際網路安全關聯和金鑰管理協定(ISAKMP)ID。在靜態ASA上使用DefaultL2LGroup時，路由器上對等體的ISAKMP ID必須是ASA的地址。但是，如果使用命名隧道組，路由器上對等體的ISAKMP ID必須與ASA上配置的隧道組名稱相同。在路由器上使用以下命令可完成此操作：

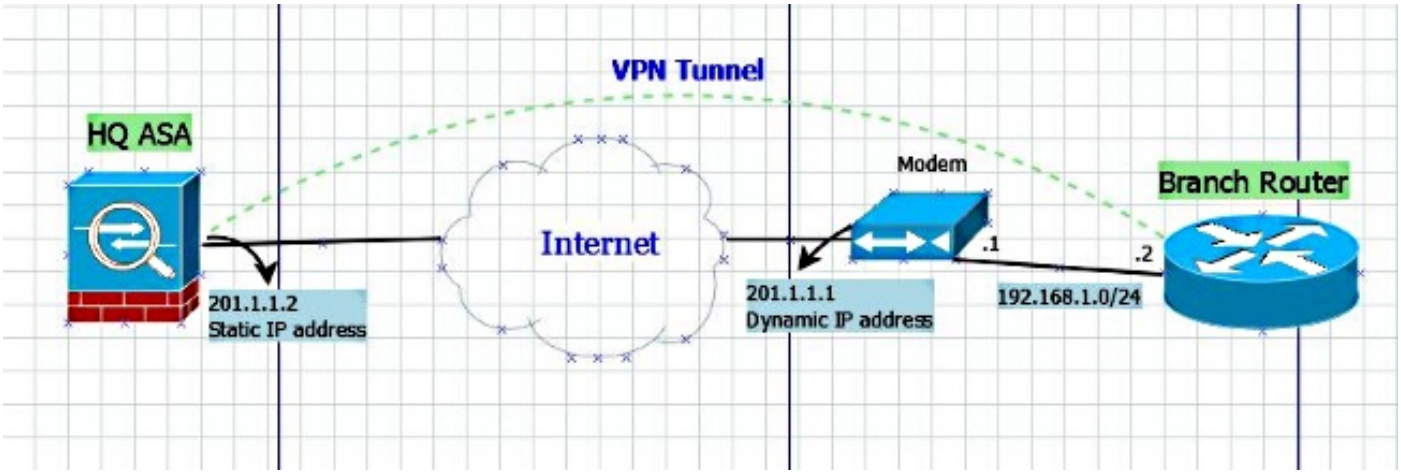
```
identity local key-id
```

在靜態ASA上使用命名隧道組的優勢在於，在使用DefaultL2LGroup時，遠端動態ASA/路由器上的配置（包括預共用金鑰）必須完全相同，並且它不允許在策略設定中有太多粒度。

設定

案例 1

網路圖表



組態

本節介紹基於命名隧道組配置的ASA和路由器上的配置。

靜態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
```

動態路由器配置

如果路由器是IKEv2 L2L隧道的動態站點，則動態路由器的配置方式與通常的配置方式幾乎相同，新增了一個命令，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，在每個動態對等體上，key-id是不同的，必須在具有正確名稱的靜態ASA上建立相應的隧道組，這也會增加ASA上實施的策略的粒度。

案例 2

> **註**：只有在至少一端是路由器時，才能進行此配置。如果兩端都是ASA，則此安裝程式此時不工作。在8.4版中，ASA無法通過**set peer**命令使用完全限定域名(FQDN)，但已請求對未來版本進行CSCus37350增強。

如果遠端ASA的IP地址是動態的，但為其VPN介面分配了完全限定域名，則您現在不是定義遠端ASA的IP地址，而是使用路由器上的以下命令定義遠端ASA的FQDN:

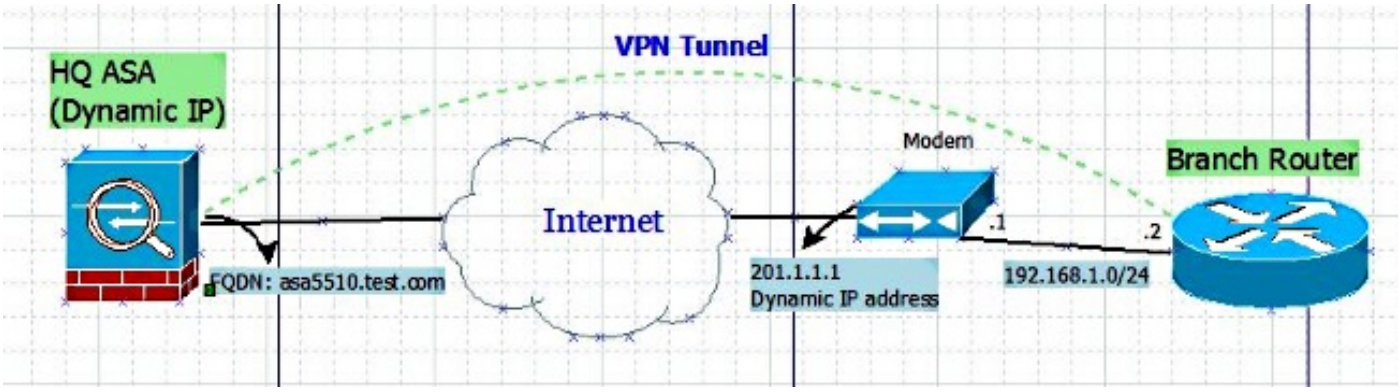
```
C1941(config)#do show run | sec crypto map

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

> **提示：dynamic**關鍵字是可選的。當您通過**set peer**命令指定遠端IPsec對等體的主機名時，還

可以發出dynamic關鍵字，該關鍵字將主機名的域名伺服器(DNS)解析延遲到建立IPsec隧道之前。

延遲解析使Cisco IOS軟體能夠檢測遠端IPsec對等體的IP地址是否已更改。因此，軟體可以聯絡新IP地址的對等方。如果未發出dynamic關鍵字，則主機名在指定後立即解析。因此，Cisco IOS軟體無法檢測IP地址更改，因此會嘗試連線到之前解析的IP地址。

網路圖表



組態

動態ASA配置

ASA上的配置與靜態ASA配置相同，只有一個例外，即物理介面上的IP地址未靜態定義。

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
```

驗證

使用本節內容，確認您的組態是否正常運作。

靜態ASA

- 以下是**show crypto IKEv2 sa det**命令的結果：

```
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**命令的結果：

```
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
```

動態路由器

- 以下是**show crypto IKEv2 sa detail**命令的結果：

```
 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**命令的結果：

```
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:
```

動態路由器（帶遠端動態ASA）

- 以下是**show crypto IKEv2 sa detail**命令的結果：

```
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
```

附註：此輸出中的遠端和本地ID是您在ASA上定義的**命名隧道組**，用於驗證您是否位於正確的隧道組。如果在任一端調試IKEv2，也可以驗證這一點。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

輸出直譯器工具(僅供已註冊客戶使用)支援某些**show**命令。使用輸出直譯器工具來檢視**show**命令輸出的分析。

附註：使用 debug 指令之前，請先參閱有關 Debug 指令的重要資訊。

在Cisco IOS路由器上，使用：

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

在ASA上，使用：

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