使用具有動態IP地址的對等裝置配置站點到站點FlexVPN隧道

目錄

簡介

本文檔介紹當遠端對等裝置具有動態IP地址時，如何在2台Cisco路由器之間配置FlexVPN站點到站點VPN隧道。

必要條件

需求

思科建議您瞭解以下主題：

- FlexVPN
- IKEv2通訊協定

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- CSR1000V裝置
- Cisco IOS® XE軟體版本17.3.4

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

網路圖表

動態對等點的拓撲

本示例中的拓撲顯示了一台Cisco路由器和另一台Cisco路由器，該路由器在其面向公眾的介面上有一個動態IP地址。

組態

本節介紹當遠端對等體使用動態IP地址時，如何在思科路由器上配置站點到站點FlexVPN隧道。

在此組態範例中，使用的驗證方法是預先共用金鑰(PSK)，但是也可以使用公開金鑰基礎架構(PKI)。

總部路由器上的配置

在本示例中，使用了路由器的IKEv2智慧預設值。IKEv2智慧預設功能通過覆蓋大多數使用案例將FlexVPN配置降至最低。可以針對特定使用案例自定義IKEv2智慧預設值，但不建議這樣做。智慧預設值包括IKEv2授權策略、IKEv2提議、IKEv2策略、Internet協定安全(IPsec)配置檔案和IPsec轉換集。

要檢視裝置中的預設值，可以運行下列命令。

- show crypto ikev2 authorization policy default
- show crypto ikev2 proposal default
- show crypto ikev2 policy default
- show crypto ipsec profile default
- show crypto ipsec transform-set default

步驟1配置IKEv2金鑰環。

- 在這種情況下，由於總部路由器是動態的，所以它不知道對等ip，因此它匹配任何ip地址。
- 還配置了遠端金鑰和本地金鑰。

- 建議使用強鍵以避免任何漏洞。

```
crypto ikev2 keyring FLEXVPN_KEYRING
 peer spoke
  address 0.0.0.0 0.0.0.0
  pre-shared-key local Cisco123
  pre-shared-key remote Cisco123
```

步驟2設定驗證、授權及記帳(AAA)模式。

- 這將為可以連線此例項的使用者建立管理框架。
- 由於從該裝置啟動連線協商，因此模型會引用其本地資料庫以確定授權使用者。

```
aaa new-model
aaa authorization network FLEXVPN local
```

步驟3配置IKEv2配置檔案。

- 由於遠端對等體IP地址是動態的，因此不能使用特定IP地址標識對等體。
- 但是，您可以按域、FQDN或在對等裝置上定義的金鑰ID來識別遠端對等裝置。

- 需要新增身份驗證、授權和記帳(AAA)組，用於指定PSK的配置檔案的授權方法。
- 如果此處驗證方法是PKI，則將其指定為cert而不是PKI。
- 由於目標是建立動態虛擬通道介面(dVTI)，因此該配置檔案連結到虛擬模板

```
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote key-id Peer123
 identity local address 172.16.1.1
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FLEXVPN default
 virtual-template 1
```

步驟4配置IPsec配置檔案。

- 如果不使用預設配置檔案，則可以配置自定義IPsec配置檔案。
- 在步驟3中建立的IKEv2配置檔案對映到此IPsec配置檔案。

```
crypto ipsec profile defualt
 set ikev2-profile FLEXVPN_PROFILE
```

第5步配置環回介面和虛擬模板介面。

- 由於遠端裝置具有動態IP地址，因此需要從模板建立dVTI。
- 此虛擬模板介面是從中建立動態虛擬訪問介面的配置模板。

```
interface Loopback1
 ip address 192.168.1.1 255.255.255.0
```

```
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback1
 tunnel protection ipsec profile default
```

分支機構路由器配置

對於分支路由器，使用必要的配置更改和下面介紹的配置更改配置IKEv2金鑰環、AAA模型、IPsec配置檔案和IKEv2配置檔案，如前面的步驟所示：

1.將傳送到總部路由器的本地身份配置為識別符號。

```
crypto ikev2 profile FLEXVPN_PROFILE
 identity local key-id Peer123
 match identity remote address 172.16.1.1
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FLEXVPN default
```

步驟5設定靜態虛擬通道介面。

- 假設總部路由器的IP地址已知且未更改，則配置靜態VTI介面。

```
interface Tunnel0
 ip address 192.168.1.10 255.255.255.0
 tunnel source GigabitEthernet0
 tunnel destination 172.16.1.1
 tunnel protection ipsec profile default
```

路由配置

在本示例中，路由是在建立IKEv2安全關聯(SA)期間通過配置訪問控制清單定義的。這定義要通過VPN傳送的流量。您也可以配置動態路由協定，但它不在本文檔的討論範圍之內。

步驟 5.定義ACL。

總部路由器：

```
ip access-list standard Flex-ACL
 permit 10.10.10.0 255.255.255.0
```

分支機構路由器：

```
ip access-list standard Flex-ACL
 permit 10.20.20.0 255.255.255.0
```

步驟 6.修改每台路由器上的IKEv2授權配置檔案以設定ACL。

```
crypto ikev2 authorization policy default
 route set interface
 route set access-list Flex-ACL
```

總部路由器完成配置

```
aaa new-model
aaa authorization network FLEXVPN local

crypto ikev2 authorization policy default
 route set interface
 route set access-list Flex-ACL

crypto ikev2 keyring FLEXVPN_KEYRING
 peer spoke
  address 0.0.0.0 0.0.0.0
  pre-shared-key local Cisco123
  pre-shared-key remote Cisco123

crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote key-id Peer123
 identity local address 172.16.1.1
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FLEXVPN default
 virtual-template 1

crypto ipsec profile default
 set ikev2-profile FLEXVPN_PROFILE
```

```
interface Loopback1
 ip address 192.168.1.1 255.255.255.0

interface Loopback10
 ip address 10.10.10.10 255.255.255.255

interface GigabitEthernet0
 ip address 172.16.1.1 255.255.255.0

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback1
 tunnel protection ipsec profile default

ip access-list standard Flex-ACL
 5 permit 10.10.10.0 255.255.255.0
```

分支機構路由器完成配置

```
aaa new-model
aaa authorization network FLEXVPN local

crypto ikev2 authorization policy default
 route set interface
 route set access-list Flex-ACL

crypto ikev2 keyring FLEXVPN_KEYRING
 peer HUB
  address 0.0.0.0 0.0.0.0
  pre-shared-key local Cisco123
  pre-shared-key remote Cisco123

crypto ikev2 profile FLEXVPN_PROFILE
 identity local key-id Peer123
 match identity remote address 172.16.1.1
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FLEXVPN default

crypto ipsec profile default
 set ikev2-profile FLEXVPN_PROFILE

interface Loopback20
 ip address 10.20.20.20 255.255.255.255

interface Tunnel0
 ip address 192.168.1.10 255.255.255.0
 tunnel source GigabitEthernet0
 tunnel destination 172.16.1.1
 tunnel protection ipsec profile default

interface GigabitEthernet0
 ip address dhcp
 negotiation auto

ip access-list standard Flex-ACL
 10 permit 10.20.20.0 255.255.255.0
```

驗證

要驗證隧道，必須驗證階段1和階段2是否正常運行且工作正常。

```
Headquarter#show crypto ikev2 sa detail
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         172.16.1.1/500        172.16.2.1/500        none/none            READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: PSK, Auth verify: P
      Life/Active Time: 86400/74645 sec
      CE id: 61256, Session-id: 1
      Status Description: Negotiation done
      Local spi: D5129F36B1180175       Remote spi: F9298874F90BFEC7
      Local id: 172.16.1.1
      Remote id: 172.16.2.1
      Local req msg id:  16             Remote req msg id:  31
      Local next msg id: 16             Remote next msg id: 31
      Local req queued:  16             Remote req queued:  31
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      Fragmentation not  configured.
      Dynamic Route Update: enabled
      Extended Authentication not configured.
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : No
      Remote subnets:                  -------------> This section shows the traffic to be routed acros
      192.168.1.10 255.255.255.255
      10.20.20.20 255.255.255.255

 IPv6 Crypto IKEv2  SA
```

第2階段，Ipsec

```
Headquarter#show crypto ipsec sa

interface: Virtual-Access1
    Crypto map tag: Virtual-Access1-head-0, local addr 172.16.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.2.1/255.255.255.255/47/0)
   current_peer 172.16.2.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 225, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 225, #pkts decrypt: 225, #pkts verify: 225
    #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.: 172.16.1.1, remote crypto endpt.: 172.16.2.1
    plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0
    current outbound spi: 0xC124D7C1(3240417217)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0xC2AADCAB(3265977515)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Transport, }
       conn id: 2912, flow_id: CSR:912, sibling_flags FFFFFFFF80000008, crypto map: Virtual-Access1-he
       sa timing: remaining key lifetime (k/sec): (4607993/628)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0xC124D7C1(3240417217)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Transport, }
       conn id: 2911, flow_id: CSR:911, sibling_flags FFFFFFFF80000008, crypto map: Virtual-Access1-he
       sa timing: remaining key lifetime (k/sec): (4608000/628)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    outbound ah sas:

    outbound pcp sas:
```

您還需要驗證虛擬訪問介面是否處於UP狀態。

```
show interface Virtual-Access1
Virtual-Access2 is up, line protocol is up
  Hardware is Virtual Access interface
  Interface is unnumbered. Using address of Loopback1 (192.168.1.1)
  MTU 9934 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL
  Tunnel vaccess, cloned from Virtual-Template1
  Vaccess status 0x4, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 172.16.1.1, destination 172.16.2.1
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1434 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "default")
  Last input 20:53:34, output 20:53:34, output hang never
  Last clearing of "show interface" counters 20:55:43
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
```

```
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     586 packets input, 149182 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     15 packets output, 1860 bytes, 0 underruns
     Output 0 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

疑難排解

本節介紹如何對通道建立進行疑難排解

如果IKE協商失敗，請完成以下步驟：

1. 使用以下命令驗證當前狀態：

- show crypto ikev2 sa
- show crypto ipsec sa
- show crypto session

2.使用以下命令可對通道交涉流程進行偵錯：

- debug crypto ikev2
- debug crypto ipsec

相關資訊

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。