使用具有动态IP地址的对等设备配置站点到站点FlexVPN隧道

目录

简介

本文档介绍当远程对等设备具有动态IP地址时，如何在2台Cisco路由器之间配置FlexVPN站点到站点VPN隧道。

先决条件

要求

Cisco 建议您了解以下主题：

- FlexVPN
- IKEv2协议

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CSR1000V设备
- Cisco IOS® XE软件，版本17.3.4

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

网络图

动态对等体的拓扑

本示例中的拓扑显示了一台Cisco路由器和另一台Cisco路由器，该Cisco路由器在其面向公众的接口上具有动态IP地址。

配置

本节介绍当远程对等体使用动态IP地址时，如何在Cisco路由器上配置站点到站点FlexVPN隧道。

在此配置示例中，使用的身份验证方法是预共享密钥(PSK)，但是也可以使用公共密钥基础设施(PKI)。

总部路由器配置

在本例中，使用了来自路由器的IKEv2智能默认值。IKEv2 Smart Defaults功能通过覆盖大多数使用案例来最大程度减少FlexVPN配置。可以针对特定使用案例自定义IKEv2智能默认值，但不建议这样做。智能默认值包括IKEv2授权策略、IKEv2提议、IKEv2策略、Internet协议安全(IPsec)配置文件和IPsec转换集。

要查看设备中的默认值，可以运行下列命令。

- 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

第1步配置IKEv2密钥环。

- 在这种情况下，由于总部路由器是动态的，所以它不知道对等ip，因此它匹配任何ip地址。
- 还配置了远程和本地密钥。

- 建议使用强密钥来避免出现任何漏洞。

```
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
```

第2步配置身份验证、授权和记帐(AAA)模型。

- 这会为可以连接此实例的用户创建管理框架。
- 由于连接协商是从此设备发起的，因此模型会引用其本地数据库来确定授权用户。

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

第3步配置IKEv2配置文件。

- 鉴于远程对等体IP地址是动态的，您不能使用特定IP地址来标识对等体。
- 但是，您可以按域、FQDN或在对等设备上定义的密钥ID来识别远程对等设备。

- 需要为配置文件的授权方法添加身份验证、授权和记帐(AAA)组，指定PSK是所用的方法。
- 如果此处身份验证方法是PKI，则将其指定为cert而不是PKI。
- 由于目标是创建动态虚拟隧道接口(dVTI)，因此此配置文件链接到虚拟模板

```
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
```

第4步配置IPsec配置文件。

- 如果不使用默认配置文件，可以配置自定义IPsec配置文件。
- 第3步中创建的IKEv2配置文件映射到此IPsec配置文件。

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

第5步配置环回接口和虚拟模板接口。

- 由于远程设备具有动态IP地址，因此需要从模板创建dVTI。
- 此虚拟模板接口是从中创建动态虚拟访问接口的配置模板。

```
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
```

分支机构路由器配置

对于分支路由器，按照上述步骤中说明的配置IKEv2 Keyring、AAA模型、IPsec配置文件和IKEv2配置文件，并进行必要的配置更改和下面所述的更改：

1.配置发送到总部路由器的本地身份作为标识符。

```
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
```

第5步配置静态虚拟隧道接口。

- 假设总部路由器的IP地址已知且不会更改，则配置静态VTI接口。

```
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，通过配置访问控制列表，在建立IKEv2安全关联(SA)期间定义路由。这定义要通过VPN发送的流量。您也可以配置动态路由协议，但它不在本文档的讨论范围之内。

第五步：定义 ACL。

总部路由器：

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

分支路由器:

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

第六步：修改每台路由器上的IKEv2授权配置文件以设置ACL。

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

总部路由器完成配置

```
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
```

验证

要检验隧道，您必须检验阶段1和阶段2是否正常运行且正常。

```
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阶段，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:
```

您还需要验证虚拟访问接口是否处于UP状态。

```
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
```

故障排除

本节介绍如何排除隧道建立故障

如果IKE协商失败，请完成以下步骤：

1. 使用以下命令验证当前状态：

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

2.使用以下命令调试隧道协商过程：

- debug crypto ikev2
- debug crypto ipsec

相关信息

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。