Configuración del túnel FlexVPN de sitio a sitio con un par con dirección IP dinámica

Contenido

Introducción

Este documento describe cómo configurar un túnel VPN de sitio a sitio FlexVPN entre 2 routers Cisco cuando el par remoto tiene una dirección IP dinámica.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- FlexVPN
- Protocolo IKEv2

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- dispositivo CSR1000V
- Software Cisco IOS® XE, versión 17.3.4

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Diagrama de la red

Topología para Peer Dinámico

La topología de este ejemplo muestra un router de Cisco y otro router de Cisco que tiene una dirección IP dinámica en su interfaz pública.

Configuraciones

Esta sección describe cómo configurar el túnel FlexVPN de sitio a sitio en un router Cisco cuando el par remoto utiliza una dirección IP dinámica.

En este ejemplo de configuración, el método de autenticación utilizado es Pre-Shared-Key (PSK); sin embargo, también se puede utilizar Public Key Infrastructure (PKI).

Configuración en el router de la sede central

En este ejemplo, se han utilizado los Smart Defaults IKEv2 del router. La función IKEv2 Smart Defaults minimiza la configuración de FlexVPN y cubre la mayoría de los casos prácticos. Los valores predeterminados inteligentes de IKEv2 se pueden personalizar para casos prácticos específicos, aunque no se recomienda. Los valores predeterminados inteligentes incluyen la directiva de autorización IKEv2, la propuesta IKEv2, la directiva IKEv2, el perfil de seguridad de protocolo de Internet (IPsec) y el conjunto de transformación IPsec.

Para revisar los valores predeterminados del dispositivo, puede ejecutar los comandos que se enumeran a continuación.

- show crypto ikev2 authorization policy default
- show crypto ikev2 offer default
- show crypto ikev2 policy default

- show crypto ipsec profile default
- show crypto ipsec transform-set default

Paso 1 Configure el anillo de claves IKEv2.

- En este caso, dado que el router de la sede central no conoce la IP del par debido a que es dinámica, la identidad coincide con cualquier dirección IP.
- También se configuran las claves local y remota.
- Se recomienda contar con claves sólidas para evitar cualquier vulnerabilidad.

```
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
```

Paso 2 Configure el modelo de Autenticación, Autorización y Contabilización (AAA).

- Esto crea el marco de administración para los usuarios que pueden conectarse para esta instancia.
- Dado que la negociación de conexión se inicia desde este dispositivo, el modelo hace referencia a su base de datos local para determinar los usuarios autorizados.

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

Paso 3 Configure el perfil IKEv2.

- Dado que la dirección IP del par remoto es dinámica, no puede utilizar una dirección IP específica para identificar al par.
- Sin embargo, puede identificar el par remoto por dominio, FQDN o ID de clave definida en el dispositivo par.

- Es necesario agregar el grupo de autenticación, autorización y contabilidad (AAA) para el método de autorización del perfil, especificando que PSK es el método utilizado.
- Si el método de autenticación es PKI aquí, se especifica como cert en lugar de PKI .
- Dado que el objetivo es crear una interfaz de túnel virtual dinámico (dVTI), este perfil está vinculado a una plantilla virtual

```
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
```

Paso 4 Configure el perfil IPsec.

- Se puede configurar un perfil IPsec personalizado si no utiliza el perfil predeterminado.
- El perfil IKEv2 creado en el paso 3 se asigna a este perfil IPsec.

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

Paso 5 Configure la interfaz de loopback y la interfaz de plantilla virtual.

- Dado que el dispositivo remoto tiene una dirección IP dinámica, es necesario crear un dVTI a partir de una plantilla.
- Esta interfaz de plantilla virtual es una plantilla de configuración a partir de la cual se crean interfaces de acceso virtual dinámicas.

```
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
```

Configuración del router de sucursal

Para el router de sucursal, configure el anillo de claves IKEv2, el modelo AAA, el perfil IPsec y el perfil IKEv2 como se indica en los pasos anteriores con los cambios de configuración necesarios y los que se describen a continuación:

1. Configure la identidad local que se envía al router de la sede central como identificador.

```
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
```

Paso 5 Configuración de la Interfaz de Túnel Virtual Estática.

- Dado que la dirección IP del router de la sede central se conoce y no cambia, se configura una interfaz VTI estática.

```
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
```

Configuración de Ruteo

En este ejemplo, el routing se define durante el establecimiento de la asociación de seguridad (SA) IKEv2 con la configuración de una lista de control de acceso. Esto define el tráfico que se enviará a través de la VPN. También puede configurar los protocolos de ruteo dinámico, sin embargo no está en el alcance de este documento.

Paso 5. Definir la ACL.

Router de la sede central:

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

Router de sucursal:

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

Paso 6. Modifique los perfiles de autorización IKEv2 en cada router para establecer la ACL.

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

Configuración completa del router de la sede

```
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
```

Configuración completa del router de sucursal

```
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
```

Verificación

Para verificar el túnel, debe verificar que la Fase 1 y la Fase 2 estén funcionando correctamente.

```
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
```

Fase 2, 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:
```

También debe verificar que la interfaz de acceso virtual esté en estado ACTIVO.

```
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
```

Troubleshoot

En esta sección se describe cómo solucionar problemas en el establecimiento del túnel

Complete estos pasos si la negociación IKE falla:

1. Verifique el estado actual con estos comandos:

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

2. Utilice estos comandos para depurar el proceso de negociación de túnel:

- debug crypto ikev2
- debug crypto ipsec

Información Relacionada

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).