Ejemplo de Configuración de Acceso Remoto que Reconoce VRF de FlexVPN

Contenido

Introducción

Este documento proporciona una configuración de ejemplo de FlexVPN con reconocimiento de reenvío y routing VPN (VRF) en un escenario de acceso remoto. La configuración utiliza un router Cisco IOS® como dispositivo de agregación de túnel con clientes AnyConnect de acceso remoto.

Prerequisites

Requirements

En este ejemplo de configuración, las conexiones VPN finalizan en un dispositivo de extremo del proveedor (PE) de switching de etiquetas multiprotocolo (MPLS) donde el punto de terminación del túnel se encuentra en una VPN MPLS (el VRF delantero [FVRF]). Después de descifrar el tráfico cifrado, el tráfico de texto despejado se reenvía a otra VPN MPLS (el VRF interno [IVRF]).

Componentes Utilizados

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

- Router de servicios de agregación de la serie ASR 1000 de Cisco con IOS-XE3.7.1 (15.2(4)S1) como servidor FlexVPN

- Cisco AnyConnect Secure Mobility Client y Cisco AnyConnect VPN Client versión 3.1
- Servidor RADIUS de Microsoft Network Policy Server (NPS)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

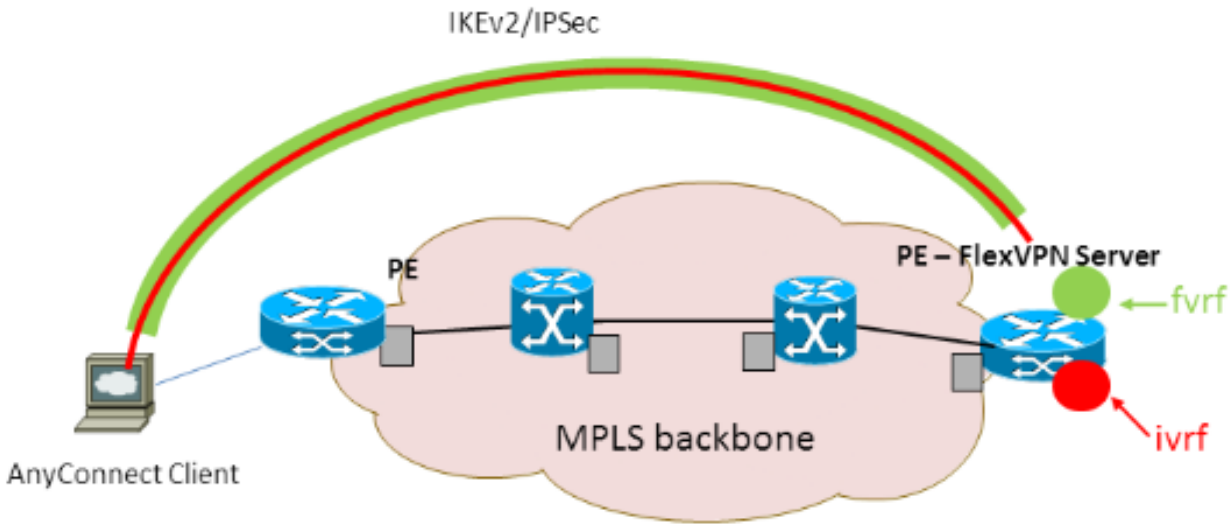
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Topología de red

En este documento, se utiliza esta configuración de red:



Configuración del servidor FlexVPN

Este es un ejemplo de la configuración del servidor FlexVPN:

```
hostname ASR1K
!
aaa new-model
!
!
aaa group server radius lab-AD
 server-private 172.18.124.30 key Cisco123
```

```
!
aaa authentication login default local
aaa authentication login AC group lab-AD
aaa authorization network AC local
!
aaa session-id common
!
ip vrf fvrf
 rd 2:2
 route-target export 2:2
 route-target import 2:2
!
ip vrf ivrf
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
!
crypto pki trustpoint AC
 enrollment mode ra
 enrollment url http://lab-ca:80/certsrv/mscep/mscep.dll
 fqdn asr1k.labdomain.cisco.com
 subject-name cn=asr1k.labdomain.cisco.com
 revocation-check crl
 rsakeypair AC
!
!
crypto pki certificate chain AC
 certificate 433D7311000100000259
 certificate ca 52DD978E9680C1A24812470E79B8FB02
!
!
crypto ikev2 authorization policy default
 pool flexvpn-pool
 def-domain cisco.com
 route set interface
!
crypto ikev2 authorization policy AC
 pool AC
 dns 10.7.7.129
 netmask 255.255.255.0
 banner ^CCC Welcome ^C
 def-domain example.com
!
crypto ikev2 proposal AC
 encryption aes-cbc-256
 integrity sha1
 group 5
!
crypto ikev2 policy AC
 match fvrf fvrf
 proposal AC
!
!
crypto ikev2 profile AC
 match fvrf fvrf
 match identity remote key-id cisco.com
 identity local dn
 authentication remote eap query-identity
 authentication local rsa-sig
 pki trustpoint AC
 dpd 60 2 on-demand
 aaa authentication eap AC
 aaa authorization group eap list AC AC
```

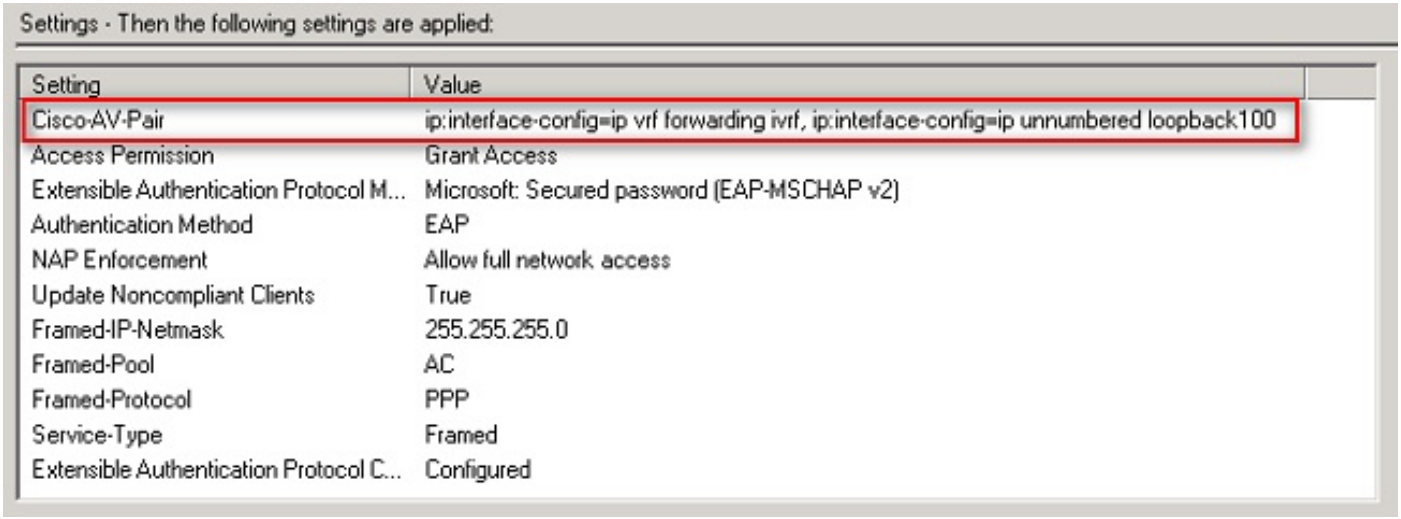
```
 virtual-template 40
!
!
crypto ipsec transform-set AC esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile AC
 set transform-set AC
 set ikev2-profile AC
!
!
interface Loopback0
 description BGP source interface
 ip address 10.5.5.5 255.255.255.255
!
interface Loopback99
 description VPN termination point in the FVRF
 ip vrf forwarding fvrf
 ip address 7.7.7.7 255.255.255.255
!
interface Loopback100
 description loopback interface in the IVRF
 ip vrf forwarding ivrf
 ip address 6.6.6.6 255.255.255.255
!
interface GigabitEthernet0/0/1
 description MPLS IP interface facing the MPLS core
 ip address 20.11.11.2 255.255.255.0
 negotiation auto
 mpls ip
 cdp enable
!
!
!
interface Virtual-Template40 type tunnel
 no ip address
 tunnel mode ipsec ipv4
 tunnel vrf fvrf
 tunnel protection ipsec profile AC
!
router bgp 2
 bgp log-neighbor-changes
 redistribute connected
 redistribute static
 neighbor 10.2.2.2 remote-as 2
 neighbor 10.2.2.2 update-source Loopback0
 !
 address-family vpnv4
  neighbor 10.2.2.2 activate
  neighbor 10.2.2.2 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf fvrf
  redistribute connected
  redistribute static
 exit-address-family
 !
 address-family ipv4 vrf ivrf
  redistribute connected
  redistribute static
 exit-address-family
!
ip local pool AC 192.168.1.100 192.168.1.150
```

Configuración Del Perfil Del Usuario Radius

La configuración clave utilizada para el perfil RADIUS son los dos pares de valor de atributo (AV) de atributos específicos del proveedor (VSA) de Cisco que colocan la interfaz de acceso virtual creada dinámicamente en el IVRF y habilitan IP en la interfaz de acceso virtual creada dinámicamente:

```
ip:interface-config=ip unnumbered loopback100
ip:interface-config=ip vrf forwarding ivrf
```

En Microsoft NPS, la configuración se encuentra en la configuración de la política de red, como se muestra en este ejemplo:



Precaución: El comando **ip vrf forwarding** debe aparecer antes del comando **ip unnumbered**. Si la interfaz de acceso virtual se clona de la plantilla virtual y se aplica el comando **ip vrf forwarding**, cualquier configuración IP se elimina de la interfaz de acceso virtual. Aunque se establece el túnel, la adyacencia CEF para la interfaz punto a punto (P2P) está incompleta. Este es un ejemplo del comando **show adjacency** con un resultado incompleto:

```
ASR1k#show adjacency virtual-access 1
Protocol Interface                 Address
IP       Virtual-Access1           point2point(6) (incomplete)
```

Si la adyacencia CEF está incompleta, se descarta todo el tráfico VPN saliente.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente. Verifique la interfaz de acceso virtual derivada y, a continuación, verifique la configuración de IVRF y FVRF.

Interfaz de acceso virtual derivada

Verifique que la interfaz de acceso virtual creada esté clonada correctamente desde la interfaz de plantilla virtual y haya aplicado todos los atributos por usuario descargados del servidor RADIUS:

```
ASR1K#sh derived-config interface virtual-access 1
```

```
Building configuration...Derived configuration : 250 bytes
!
interface Virtual-Access1
 ip vrf forwarding ivrf
 ip unnumbered Loopback100
 tunnel source 7.7.7.7
 tunnel mode ipsec ipv4
 tunnel destination 8.8.8.10
 tunnel vrf fvrf
 tunnel protection ipsec profile AC
 no tunnel protection ipsec initiate
end
```

Sesiones Crypto

Verifique la configuración de IVRF y FVRF con estas salidas del plano de control.

Este es un ejemplo del resultado del comando **show crypto sessiond** detail:

```
ASR1K#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Virtual-Access1
Uptime: 00:23:19
Session status: UP-ACTIVE
Peer: 8.8.8.10 port 57966 fvrf: fvrf ivrf: ivrf
      Phase1_id: cisco.com
      Desc: (none)
  IKEv2 SA: local 7.7.7.7/4500 remote 8.8.8.10/57966 Active
          Capabilities:(none) connid:1 lifetime:23:36:41
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 192.168.1.103
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 95 drop 0 life (KB/Sec) 4607990/2200
        Outbound: #pkts enc'ed 44 drop 0 life (KB/Sec) 4607997/2200
```

Este es un ejemplo del resultado del comando **show crypto IKEv2 session detail**:

```
ASR1K#show crypto ikev2 sess detail
 IPv4 Crypto IKEv2 Session

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         7.7.7.7/4500          8.8.8.10/57966        fvrf/ivrf            READY
      Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:5, Auth sign: RSA, Auth verify: EAP
      Life/Active Time: 86400/1298 sec
      CE id: 1004, Session-id: 4
      Status Description: Negotiation done
      Local spi: EE87373C2C2643CA       Remote spi: F80C8A4CB4143091
      Local id: cn=asr1k.labdomain.cisco.com,hostname=asr1k.labdomain.cisco.com
      Remote id: cisco.com
      Remote EAP id: user1
      Local req msg id:  1              Remote req msg id:  43
      Local next msg id: 1              Remote next msg id: 43
      Local req queued:  1              Remote req queued:  43
      Local window:      5              Remote window:      1
      DPD configured for 60 seconds, retry 2
```

```
      NAT-T is detected  outside
      Cisco Trust Security SGT is disabled
      Assigned host addr: 192.168.1.103
      Initiator of SA : No
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 192.168.1.103/0 - 192.168.1.103/65535
          ESP spi in/out: 0x88F2A69E/0x19FD0823
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-CBC, keysize: 256, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel

 IPv6 Crypto IKEv2 Session

ASR1K#
```

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems