Exemplo de configuração VRF-ciente do Acesso remoto de FlexVPN

Índice

Introdução

Este documento fornece uma configuração de exemplo para um VPN Routing and Forwarding (VRF) - FlexVPN ciente em uma encenação do Acesso remoto. A configuração usa um roteador de Cisco IOS® como o dispositivo de agregação do túnel com os clientes de AnyConnect do Acesso remoto.

Pré-requisitos

Requisitos

Neste exemplo de configuração, as conexões de VPN são terminadas em um dispositivo da ponta de provedor do Multiprotocol Label Switching (MPLS) (PE) onde o ponto de terminação de túnel esteja em um MPLS VPN (o [FVRF] dianteiro VRF). Depois que o tráfego criptografado é decifrado, o tráfego do texto claro está enviado em um outro MPLS VPN (o [IVRF] interno VRF).

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- A agregação do 1000 Series de Cisco ASR presta serviços de manutenção ao roteador com o IOS-XE3.7.1 (15.2(4)S1) como o server de FlexVPN

- Versão 3.1 do Cliente de mobilidade Cisco AnyConnect Secure e do Cisco AnyConnect VPN Client
- Servidor Radius do servidor da política da rede Microsoft (NP)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Topologia de rede

Este documento utiliza a seguinte configuração de rede:

Configuração do servidor de FlexVPN

Este é um exemplo da configuração do servidor de 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
```

Configuração do perfil de usuário radius

A configuração chave usada para o perfil de RADIUS é os dois pares do valor de atributo dos atributos específicos de fornecedor (VSA) de Cisco (AV) que põem a interface de acesso virtual dinamicamente criada no IVRF e permitem o IP na interface de acesso virtual dinamicamente criada:

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

Em Microsoft NP, a configuração está nos ajustes da política de rede segundo as indicações deste exemplo:

Cuidado: O comando ip vrf forwarding deve vir antes do **comando ip unnumbered**. Se a interface de acesso virtual está clonada do molde virtual, e o **comando ip vrf forwarding** está aplicado então, toda a configuração IP está removida da interface de acesso virtual. Embora o túnel seja estabelecido, a adjacência de CEF para a relação (P2P) ponto a ponto está incompleta. Este é um exemplo do **comando show adjacency** com um resultado incompleto:

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

Se a adjacência de CEF está incompleta, todo o tráfego de partida VPN está deixado cair.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente. Verifique a interface de acesso virtual derivada, a seguir verifique os ajustes IVRF e FVRF.

Interface de acesso virtual derivada

Verifique que a interface de acesso virtual criada está clonada corretamente da relação virtual do molde e aplicou todos os atributos por usuário transferidos do 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
```

Sessões de criptografia

Verifique os ajustes IVRF e FVRF com estes saídas planas do controle.

Este é um exemplo da saída do comando detail **cripto do sessiond da mostra**:

```
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 é um exemplo da saída do **comando detail cripto da sessão IKEv2 da mostra**:

```
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#
```

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems