Exemple Vrf-averti de configuration d'Accès à distance de FlexVPN

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour un routage VPN et un expédition (VRF) - FlexVPN averti dans un scénario d'Accès à distance. La configuration utilise un routeur de Cisco IOS® comme périphérique d'agrégation de tunnel avec des clients d'AnyConnect d'Accès à distance.

Conditions préalables

Conditions requises

En cet exemple de configuration, les connexions VPN sont terminées sur un périphérique de Provider Edge de Commutation multiprotocole par étiquette (MPLS) (PE) où le point d'arrêt de tunnel est dans un MPLS VPN (le VRF avant [FVRF]). Après que le trafic chiffré soit déchiffré, le trafic des textes clairs est expédié dans un autre MPLS VPN (le VRF interne [IVRF]).

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeur de services d'agrégation de la gamme Cisco ASR 1000 avec IOS-XE3.7.1

(15.2(4)S1) en tant que serveur de FlexVPN
- Version 3.1 de Client à mobilité sécurisé Cisco AnyConnect et de Cisco AnyConnect VPN Client
- Serveur de RAYON du policy server de réseau Microsoft (NPS)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

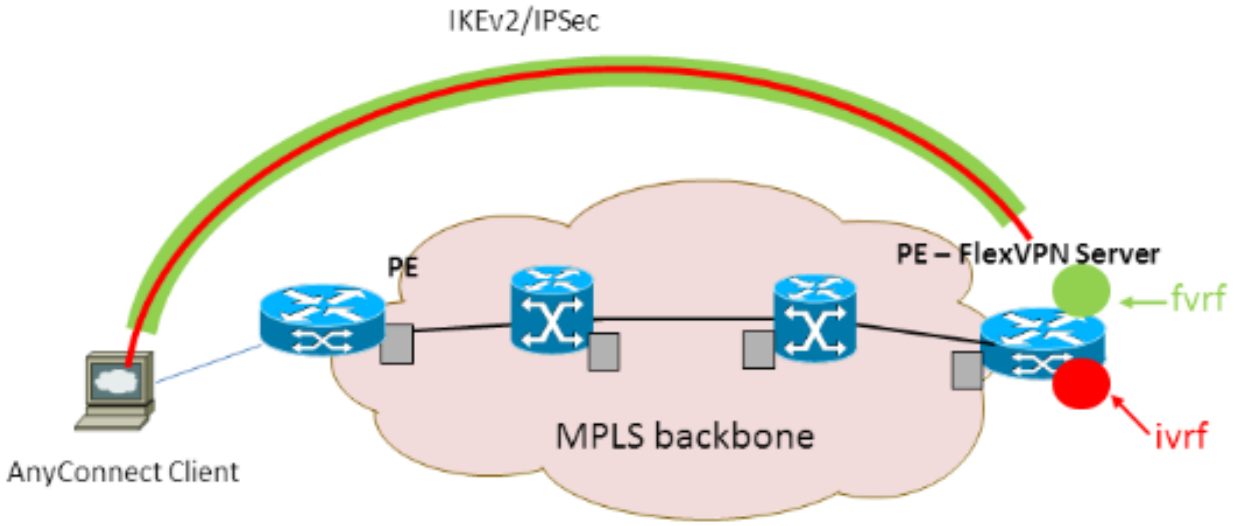
Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Topologie du réseau

Ce document utilise la configuration réseau suivante :



Configuration du serveur de FlexVPN

C'est un exemple de configuration du serveur 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

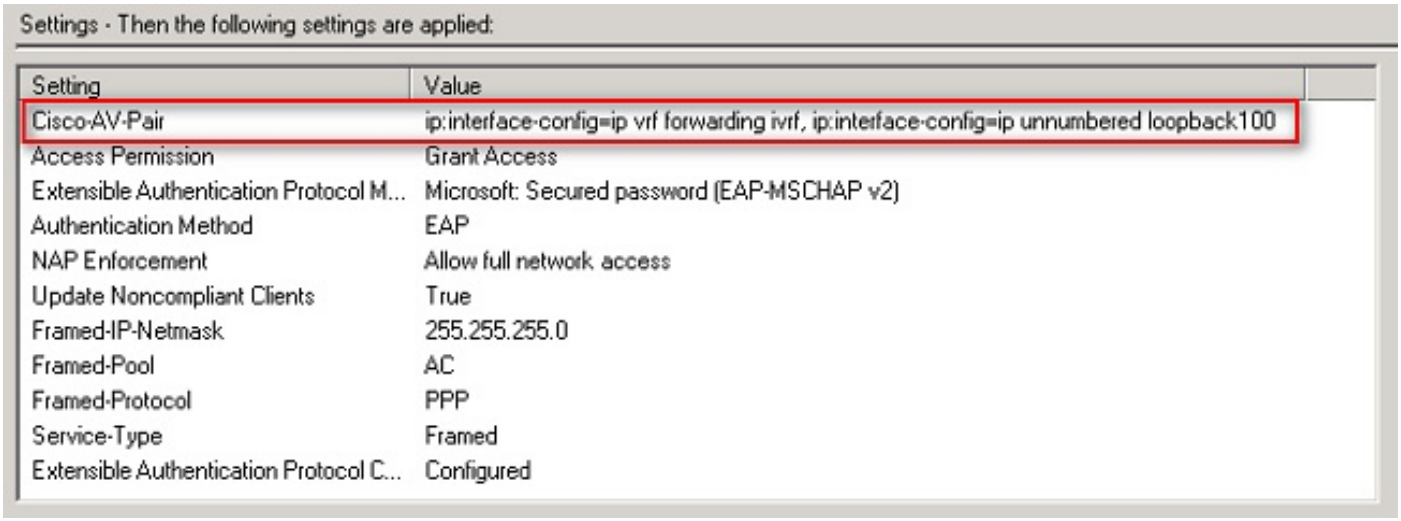
```
log-neighbor-changes redistribute connected redistribute static neighbor 10.2.2.2 remote-as 2
neighbor 10.2.2.2 update-source Loopback0 ! address-family vpnv4 neighbor 10.2.2.2 activate
neighbor 10.2.2.2 send-community extended exit-address-family ! address-family ipv4 vrf fvrf
redistribute connected 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
```

Configuration de profil d'utilisateur RADIUS

La configuration principale utilisée pour le profil RADIUS est les deux paires de l'attribut-valeur des attributs de constructeur-particularité de Cisco (le VSA) (poids du commerce) qui mettent l'interface d'accès virtuelle dynamiquement créée dans l'IVRF et l'IP d'enable sur l'interface d'accès virtuelle dynamiquement créée :

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

ÀMicrosoft NPS, la configuration est dans les configurations de politique réseau suivant les indications de cet exemple :



Attention : La commande d'**ip vrf forwarding** doit être livré avant la commande d'**ip unnumbered**. Si l'interface d'accès virtuelle est copiée du modèle virtuel, et la commande d'**ip vrf forwarding** est alors appliquée, toute configuration IP est retirée de l'interface d'accès virtuelle. Bien que le tunnel soit établi, la contiguïté CEF pour l'interface point par point (de P2P) est inachevée. C'est un exemple de la commande de **show adjacency** avec un résultat inachevé :

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

Si la contiguïté CEF est inachevée, tout le trafic VPN sortant est abandonné.

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration. Vérifiez l'interface d'accès virtuelle dérivée, puis vérifiez les configurations IVRF et FVRF.

Interface d'Access virtuelle dérivée

Vérifiez que l'interface d'accès virtuelle créée est copiée correctement de l'interface de modèle virtuel et a appliqué tous les attributs de par-utilisateur téléchargés à partir du serveur de RAYON :

```
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
```

Cryptos sessions

Vérifiez les configurations IVRF et FVRF avec ces derniers les sorties plates de contrôle.

C'est un exemple de la sortie de la **crypto** commande de détail de **sessiond d'exposition** :

```
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
```

C'est un exemple de la sortie de la **crypto** commande de **détail de la session IKEv2 d'exposition** :

```
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#
```

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Support et documentation techniques - Cisco Systems