Konfigurationsbeispiel für FlexVPN VRF-kompatiblen Remote-Zugriff

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für ein VRF-kompatibles VPN (VPN Routing and Forwarding) FlexVPN in einem Remote-Zugriffsszenario. Bei der Konfiguration wird ein Cisco IOS®-Router als Tunnel-Aggregationsgerät mit Remote-Zugriff auf AnyConnect-Clients verwendet.

Voraussetzungen

Anforderungen

In dieser Beispielkonfiguration werden die VPN-Verbindungen auf einem Multiprotocol Label Switching (MPLS) Provider Edge (PE)-Gerät terminiert, auf dem sich der Tunnel-Terminationspunkt in einem MPLS-VPN (dem Front-VRF [FVRF]) befindet. Nachdem der verschlüsselte Datenverkehr entschlüsselt wurde, wird der Klartext-Datenverkehr an ein anderes MPLS-VPN (die interne VRF-Instanz [IVRF]) weitergeleitet.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Aggregation Services Router der Serie ASR 1000 mit IOS-XE3.7.1 (15.2(4)S1) als FlexVPN-Server
- Cisco AnyConnect Secure Mobility Client und Cisco AnyConnect VPN Client Version 3.1
- Microsoft Network Policy Server (NPS) RADIUS-Server

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

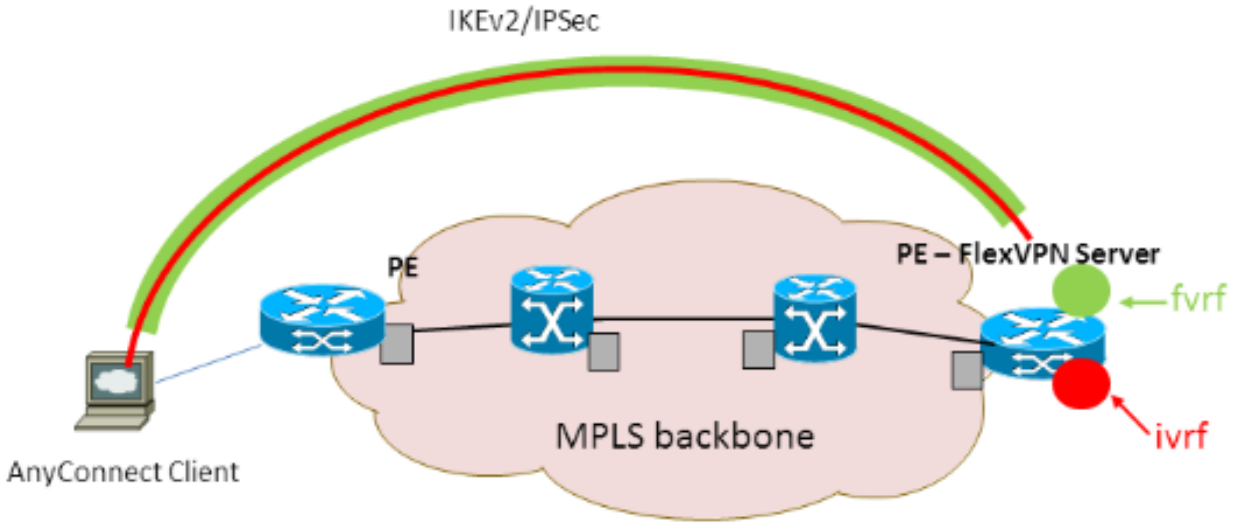
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerktopologie

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfiguration des FlexVPN-Servers

Dies ist ein Beispiel für eine FlexVPN-Serverkonfiguration:

```
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
```

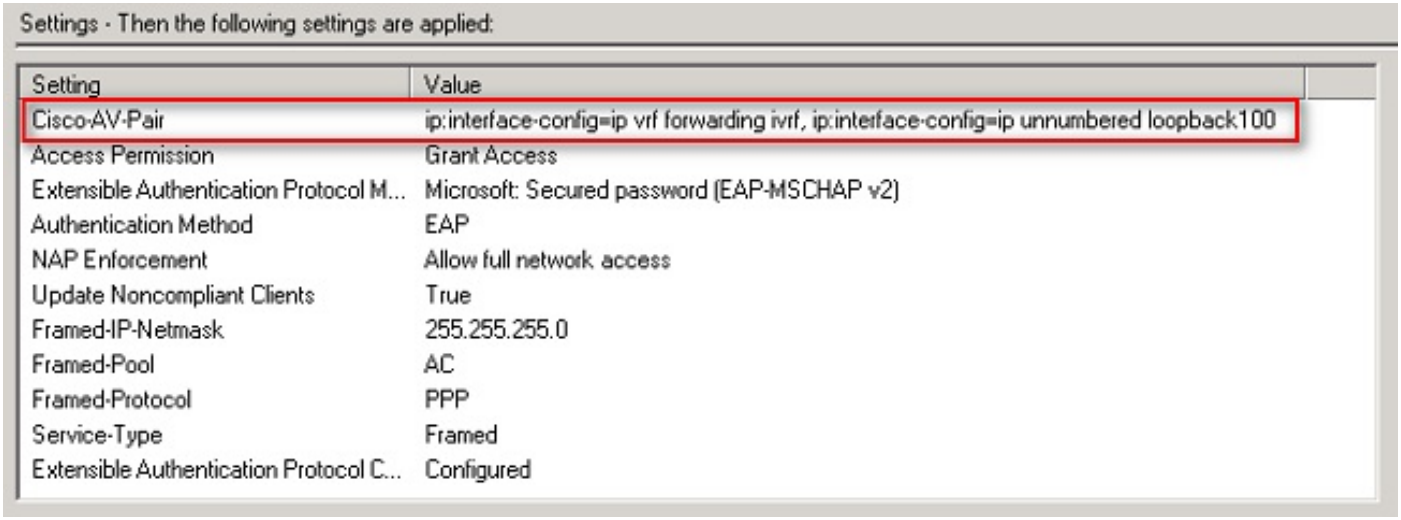
```
 exit-address-family
!
ip local pool AC 192.168.1.100 192.168.1.150
```

Radius-Benutzerprofilkonfiguration

Die für das RADIUS-Profil verwendete Schlüsselkonfiguration sind die beiden VSA-Paare (VSA), die die dynamisch erstellte virtuelle Zugriffsschnittstelle in die IVRF-Instanz einbinden und die IP-Adresse auf der dynamisch erstellten virtuellen Zugriffsschnittstelle aktivieren:

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

In Microsoft NPS befindet sich die Konfiguration in den Netzwerkrichtlinieneinstellungen, wie in diesem Beispiel gezeigt:



Achtung: Der Befehl **ip vrf forwarding** muss vor dem Befehl **ip unnumbered (unnummerierte** IP-Befehle) ausgeführt werden. Wenn die virtuelle Zugriffsschnittstelle aus der virtuellen Vorlage geklont und der Befehl **ip vrf** für die **Weiterleitung** angewendet wird, wird jede IP-Konfiguration aus der virtuellen Zugriffsschnittstelle entfernt. Obwohl der Tunnel eingerichtet ist, ist die CEF-Adjacency für die Point-to-Point (P2P)-Schnittstelle unvollständig. Dies ist ein Beispiel für den Befehl **show adjacency** mit einem unvollständigen Ergebnis:

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

Wenn die CEF-Adjacency unvollständig ist, wird der gesamte ausgehende VPN-Datenverkehr verworfen.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert. Überprüfen Sie die abgeleitete virtuelle Zugriffsschnittstelle, und überprüfen Sie dann die Einstellungen für IVRF und FVRF.

Abgeleitete virtuelle Zugriffsschnittstelle

Überprüfen Sie, ob die erstellte virtuelle Zugriffsschnittstelle von der virtuellen Vorlagenschnittstelle ordnungsgemäß geklont wurde und alle vom RADIUS-Server heruntergeladenen Attribute pro Benutzer angewendet hat:

```
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
```

Krypto-Sitzungen

Überprüfen Sie die IVRF- und FVRF-Einstellungen mit diesen Ausgaben der Kontrollebene.

Dies ist ein Beispiel für die Ausgabe des Befehls **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
```

Dies ist ein Beispiel für die Ausgabe des Befehls **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#
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems