Esempio di configurazione di accesso remoto compatibile con FlexVPN VRF

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio per una FlexVPN con rilevamento routing e inoltro VPN (VRF) in uno scenario di accesso remoto. La configurazione utilizza un router Cisco IOS® come dispositivo di aggregazione del tunnel con client AnyConnect di accesso remoto.

Prerequisiti

Requisiti

In questa configurazione di esempio, le connessioni VPN vengono terminate su un dispositivo MPLS (Multiprotocol Label Switching) Provider Edge (PE) dove il punto di terminazione del tunnel si trova in una VPN MPLS (VRF [FVRF] anteriore). Dopo aver decrittografato il traffico crittografato, il traffico in testo non crittografato viene inoltrato a un'altra VPN MPLS (il VRF [IVRF] interno).

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ASR serie 1000 Aggregation Services Router con IOS-XE3.7.1 (15.2(4)S1) come server FlexVPN
- Cisco AnyConnect Secure Mobility Client e Cisco AnyConnect VPN Client versione 3.1
- Server dei criteri di rete RADIUS Microsoft

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

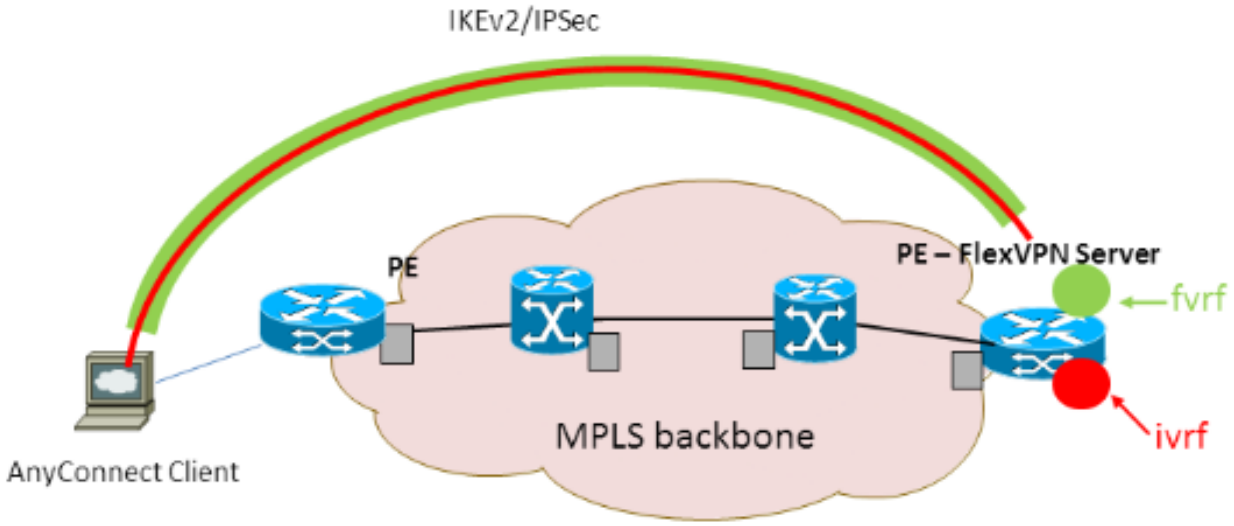
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Topologia della rete

Nel documento viene usata questa impostazione di rete:



Configurazione server FlexVPN

Questo è un esempio di configurazione del server 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
```

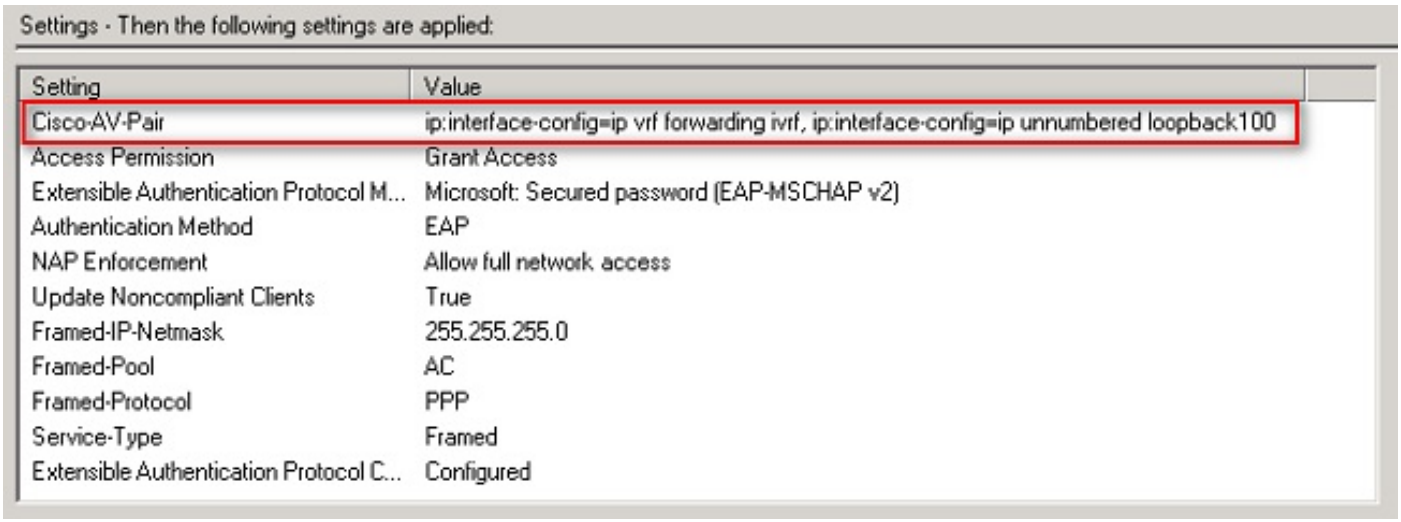
```
 exit-address-family
!
ip local pool AC 192.168.1.100 192.168.1.150
```

Configurazione profilo utente Radius

La configurazione chiave utilizzata per il profilo RADIUS è rappresentata dalle due coppie di attributi specifici del fornitore (VSA) Cisco, che inseriscono l'interfaccia di accesso virtuale creata in modo dinamico nell'IVRF e abilitano l'IP nell'interfaccia di accesso virtuale creata in modo dinamico:

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

In Server dei criteri di rete Microsoft la configurazione è nelle impostazioni dei criteri di rete, come illustrato nell'esempio seguente:



Attenzione: il comando **ip vrf forwarding** deve precedere il comando **ip senza numero**. Se l'interfaccia di accesso virtuale viene clonata dal modello virtuale e viene quindi applicato il comando **ip vrf forwarding**, qualsiasi configurazione IP viene rimossa dall'interfaccia di accesso virtuale. Anche se il tunnel è stato stabilito, l'adiacenza CEF dell'interfaccia point-to-point (P2P) è incompleta. Questo è un esempio di comando **show adiacency** con risultato incompleto:

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

Se l'adiacenza CEF è incompleta, tutto il traffico VPN in uscita viene interrotto.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione. Verificare l'interfaccia di accesso virtuale derivata, quindi verificare le impostazioni IVRF e FVRF.

Interfaccia di accesso virtuale derivata

Verificare che l'interfaccia di accesso virtuale creata sia clonata correttamente dall'interfaccia del modello virtuale e che abbia applicato tutti gli attributi per utente scaricati dal server 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
```

Sessioni di crittografia

Verificare le impostazioni IVRF e FVRF con queste uscite del control plane.

Questo è un esempio dell'output del comando **show crypto session** 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
```

Questo è un esempio dell'output 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#
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems