FlexVPN VRF 인식 원격 액세스 컨피그레이션 예

목차

소개

이 문서에서는 원격 액세스 시나리오에서 VRF(VPN 라우팅 및 포워딩) 인식 FlexVPN에 대한 샘플 컨피그레이션을 제공합니다. 컨피그레이션에서는 Cisco IOS® 라우터를 원격 액세스 AnyConnect 클라이언트가 있는 터널 어그리게이션 디바이스로 사용합니다.

사전 요구 사항

요구 사항

이 예제 컨피그레이션에서는 VPN 연결이 MPLS VPN(전면 VRF[FVRF])에 있는 MPLS(Multiprotocol Label Switching) PE(Provider Edge) 디바이스에서 종료됩니다. 암호화된 트래픽이 해독되면 일반 텍스트 트래픽이 다른 MPLS VPN(내부 VRF [IVRF])으로 전달됩니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASR 1000 Series Aggregation Services Router with IOS-XE3.7.1(15.2(4)S1)를 FlexVPN 서버로 사용
- Cisco AnyConnect Secure Mobility Client 및 Cisco AnyConnect VPN Client 버전 3.1
- Microsoft NPS(네트워크 정책 서버) RADIUS 서버

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

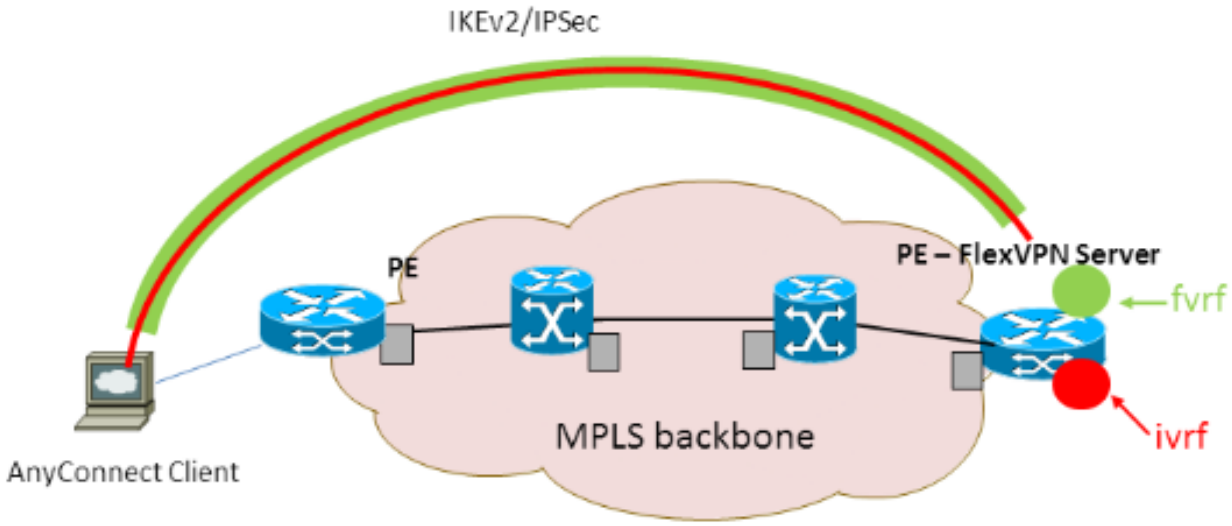
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 토폴로지

이 문서에서는 다음 네트워크 설정을 사용합니다.



FlexVPN 서버 컨피그레이션

다음은 FlexVPN 서버 컨피그레이션의 예입니다.

```
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
```

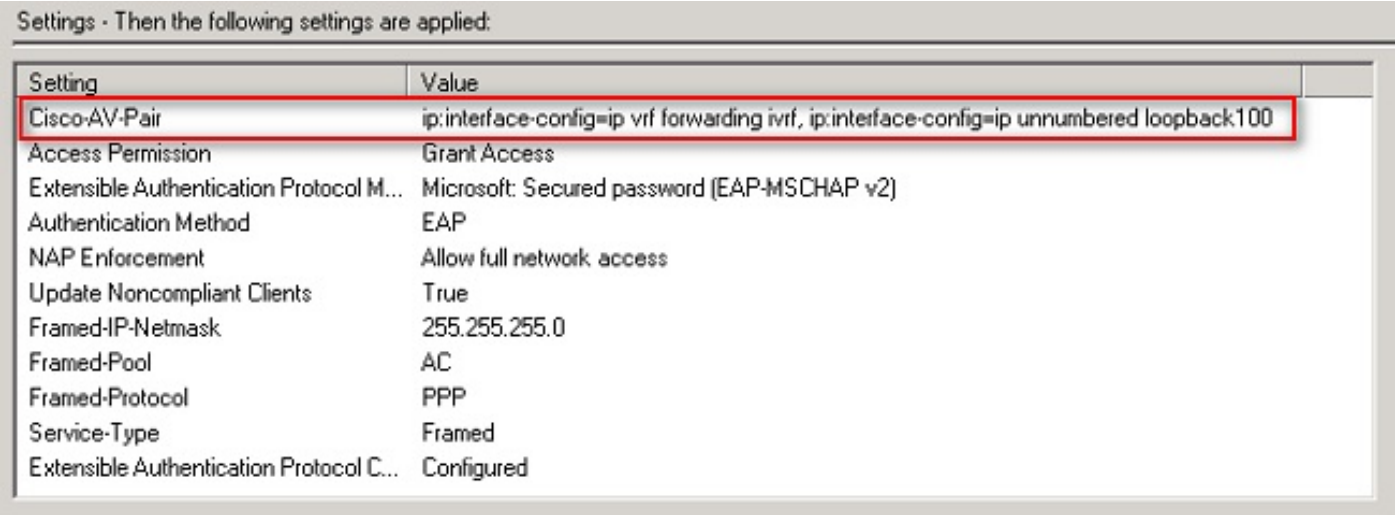
```
 set transform-set AC
 set ikev2-profile AC
!
!
interface Loopback0
 description BGP source interface
 ip address 10.5.5.5 255.255.255.255
!
interface Loopback99
 description VPN termination point in the FVRF
 ip vrf forwarding fvrf
 ip address 7.7.7.7 255.255.255.255
!
interface Loopback100
 description 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 사용자 프로필 컨피그레이션

RADIUS 프로필에 사용되는 키 컨피그레이션은 동적으로 생성된 가상 액세스 인터페이스를 IVRF에 배치하고 동적으로 생성된 가상 액세스 인터페이스에서 IP를 활성화하는 두 개의 Cisco VSA(Vendor-Specific Attributes) AV(Attribute-Value) 쌍입니다.

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

Microsoft NPS에서 구성은 다음 예와 같이 네트워크 정책 설정에 있습니다.



주의: ip vrf **forwarding** 명령은 ip unnumbered 명령 앞에 와야 합니다. 가상 액세스 인터페이스가 가상 템플릿에서 복제되고 **ip vrf forwarding** 명령이 적용되면 가상 액세스 인터페이스에서 모든 IP 컨피그레이션이 제거됩니다. 터널이 설정되었지만 P2P(point-to-point) 인터페이스의 CEF 인접성이 완전하지 않습니다. 다음은 불완전한 결과를 가진 **show adjacency** 명령의 예입니다.

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

CEF 인접성이 불완전하면 모든 아웃바운드 VPN 트래픽이 삭제됩니다.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다. 파생된 가상 액세스 인터페이스를 확인한 다음 IVRF 및 FVRF 설정을 확인합니다.

파생된 가상 액세스 인터페이스

생성된 가상 액세스 인터페이스가 가상 템플릿 인터페이스에서 올바르게 복제되고 RADIUS 서버에서 다운로드한 모든 사용자별 특성을 적용했는지 확인합니다.

```
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
```

암호화 세션

이러한 컨트롤 플레인 출력으로 IVRF 및 FVRF 설정을 확인합니다.

다음은 show crypto session detail 명령의 출력의 예입니다.

```
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
```

다음은 show crypto IKEv2 session detail 명령의 출력 예입니다.

```
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#
```

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems