FlexVPN の VRF 認識型リモート アクセスの設定例

内容

概要

このドキュメントでは、リモート アクセス シナリオでの VPN ルーティングおよび転送（VRF）対応 FlexVPN の設定例を紹介します。この設定では、リモートアクセスAnyConnectクライアントを備えたトンネル集約デバイスとしてCisco IOS®ルータを使用します。

前提条件

要件

この設定例では、VPN 接続はマルチプロトコル ラベル スイッチング（MPLS）プロバイダー エッジ（PE）デバイスで終端されます。この場合、トンネル終端ポイントは MPLS VPN（フロント VRF（FVRF））内です。 暗号化トラフィックが復号化されると、クリア テキスト トラフィックが別の MPLS VPN（内部 VRF（IVRF））に転送されます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ（FlexVPN サーバとして IOS-XE3.7.1 (15.2(4)S1) を使用）

- Cisco AnyConnect セキュア モビリティ クライアントおよび Cisco AnyConnect VPN Client バージョン 3.1
- Microsoft ネットワーク ポリシー サーバ（NPS）RADIUS サーバ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

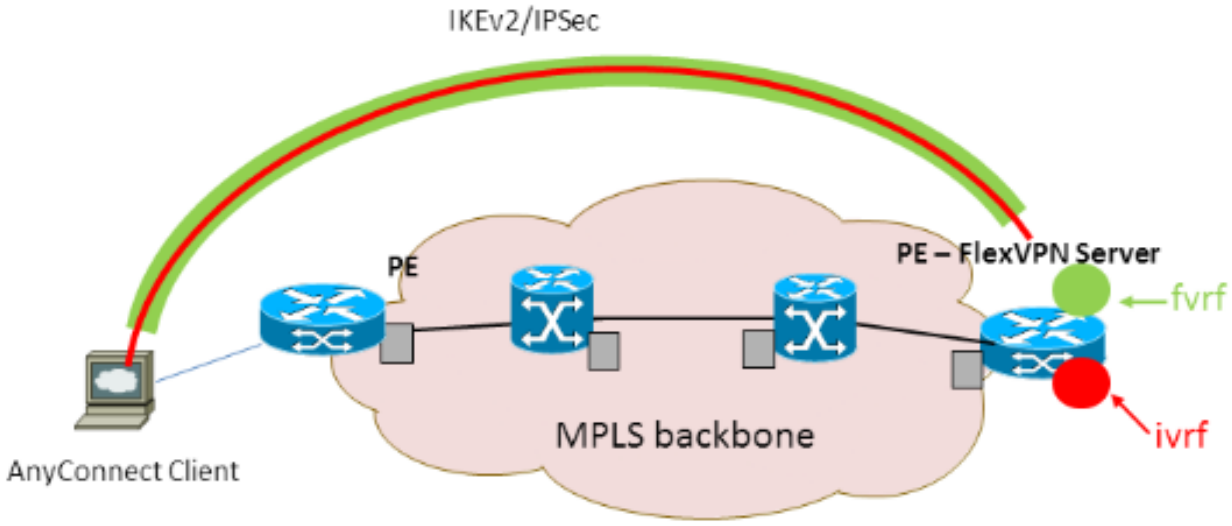
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

Network Topology

このドキュメントでは、次のネットワーク セットアップを使用します。



FlexVPN サーバの設定

FlexVPN サーバの設定の例を次に示します。

```
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
```

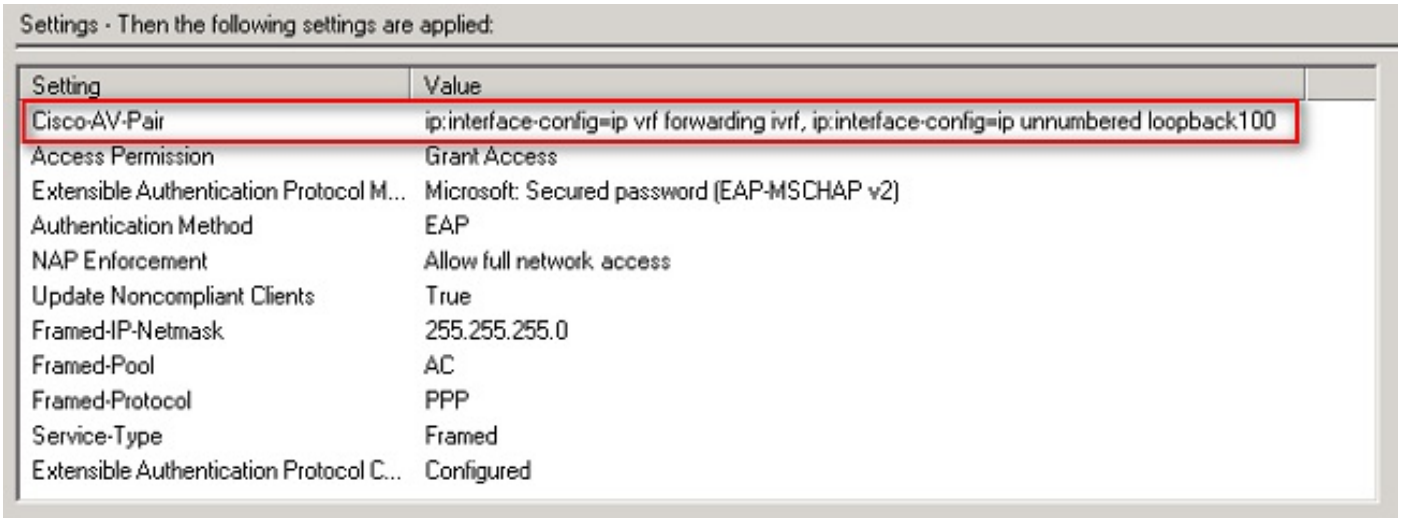
```
!
ip local pool AC 192.168.1.100 192.168.1.150
```

Radius ユーザ プロファイルの設定

RADIUS プロファイルに使用される主な設定は、2 つの Cisco ベンダー固有属性（VSA）の属性と値（AV）ペアです。これにより、動的に作成された仮想アクセス インターフェイスは IVRF に配置され、動的に作成された仮想アクセス インターフェイスの IP が有効になります。

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

Microsoft NPS では、ネットワーク ポリシーの設定が次の例に示すようになります。



注意：ip vrf forwardingコマンドは、ip unnumberedコマンドの前に指定する必要があります。仮想アクセス インターフェイスが仮想テンプレートから複製され、その後 **ip vrf forwarding コマンドが適用されると、仮想アクセス インターフェイスからすべての IP 設定が削除されます。**トンネルは確立されますが、ポイントツーポイント（P2P）インターフェイスの CEF 隣接関係が不完全です。次に、**show adjacency コマンドと不完全な結果の例を示します。**

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

CEF 隣接関係が不完全な場合、すべてのアウトバウンド VPN トラフィックはドロップされます。

確認

ここでは、設定が正常に機能しているかどうかを確認します。派生した仮想アクセス インターフェイスを確認し、次に IVRF と FVRF の設定を確認します。

派生した仮想アクセス インターフェイス

作成された仮想アクセス インターフェイスが、仮想テンプレート インターフェイスから正しく複製されたものであり、RADIUS サーバからダウンロードされたユーザ別属性がすべて適用されていることを確認します。

```
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
```

暗号化セッション

コントロール プレーン出力で IVRF 設定と FVRF 設定を確認します。

以下は **show crypto sessiond コマンドの出力例です。**

```
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
```

以下は **show crypto IKEv2 session detail コマンドの出力例です。**

```
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#
```

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- テクニカル サポートとドキュメント – Cisco Systems