

FlexVPN VRF感知远程访问配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络拓扑](#)

[FlexVPN服务器配置](#)

[RADIUS用户配置文件配置](#)

[验证](#)

[派生的虚拟访问接口](#)

[crypto塞申斯](#)

[故障排除](#)

[相关信息](#)

简介

本文为VPN路由与转发(VRF)提供一配置示例-在远程访问方案的意识FlexVPN。配置使用一个Cisco IOS路由器作为通道聚合设备与远程访问AnyConnect客户端。

先决条件

要求

在此配置示例中，VPN连接在隧道终止点在MPLS VPN的多协议标签交换(MPLS)服务商边缘设备终止(前面VRF [FVRF])。在加密流量解密后，明文流量转发到另一MPLS VPN (内部VRF [IVRF])。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco ASR 1000系列聚合服务路由器与IOS-XE3.7.1 (15.2(4)S1)作为FlexVPN服务器
- Cisco AnyConnect安全移动客户端和Cisco AnyConnect VPN客户版本3.1
- Microsoft网络策略服务器(NP) RADIUS服务器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始(默认)配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用 [命令查找工具](#) ([仅限注册用户](#)) 可获取有关本部分所使用命令的详细信息。

网络拓扑

本文档使用以下网络设置：

FlexVPN服务器配置

这是FlexVPN服务器配置示例：

```
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 fvrfl fvrfl proposal AC ! ! crypto ikev2 profile AC match fvrfl fvrfl 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 fvrfl ip address
7.7.7.7 255.255.255.255 ! interface Loopback100 description loopback interface in the IVRF ip
vrf forwarding ivrfl 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 vvrfl fvrfl 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 vvrfl fvrfl
redistribute connected redistribute static exit-address-family ! address-family ipv4 vvrfl ivrfl
redistribute connected redistribute static exit-address-family ! ip local pool AC 192.168.1.100
192.168.1.150

```

[RADIUS用户配置文件配置](#)

用于RADIUS配置文件的关键配置是在IVRF放置动态地已创建虚拟访问接口并且启用在动态地已创建虚拟访问接口的IP的两个思科供应商专用属性(VSA) attribute-value (AV)对：

```

ip:interface-config=ip unnumbered loopback100
ip:interface-config=ip vrf forwarding ivrfl

```

如此示例所显示，在Microsoft NP，配置在网络策略设置：

警告： ip vrf forwarding命令必须在ip unnumbered命令前来。如果虚拟访问接口从虚拟模板被克隆，并且ip vrf forwarding命令然后应用，所有IP配置从虚拟访问接口删除。虽然通道设立，点到点(P2P)接口的CEF邻接不完整。这是示例show adjacency命令与一种不完整结果：

```

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

```

如果CEF邻接不完整，所有出站VPN流量丢弃。

[验证](#)

使用本部分可确认配置能否正常运行。验证派生的虚拟访问接口，然后验证IVRF和FVRF设置。

[派生的虚拟访问接口](#)

验证创建的虚拟访问接口从虚拟模板接口正确地被克隆和应用从RADIUS服务器下载的所有每个用户的属性：

```
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
```

[crypto塞申斯](#)

验证与这些控制层面输出的IVRF和FVRF设置。

这是输出的示例从detail命令显示crypto的sessiond的：

```
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
```

这是输出的示例从显示crypto IKEv2会话详细信息命令的：

```
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=asrlk.labdomain.cisco.com,hostname=asrlk.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#
```

[故障排除](#)

目前没有针对此配置的故障排除信息。

[相关信息](#)

- [技术支持和文档 - Cisco Systems](#)