FlexVPN осведомленный о VRF пример конфигурации удаленного доступа

Содержание

Введение

Этот документ предоставляет пример конфигурации для VPN Routing и Forwarding (VRF) - осведомленный FlexVPN в сценарии удаленного доступа. Конфигурация использует маршрутизатор Cisco IOS® в качестве туннельного устройства агрегации с клиентами AnyConnect удаленного доступа.

Предварительные условия

Требования

В конфигурации данного примера VPN-подключения завершены на устройстве Границы провайдера (PE) Многопротокольной коммутации по меткам (MPLS), где оконечная точка туннеля находится в MPLS VPN (передний VRF [FVRF]). После того, как зашифрованный поток данных дешифрован, трафик открытого текста передан в другой MPLS VPN (внутренний VRF [IVRF]).

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Сервисный маршрутизатор агрегации Cisco ASR серии 1000 с IOS-XE3.7.1 (15.2 (4) S1) как сервер FlexVPN
- Защищенный мобильный клиент Cisco AnyConnect Secure Mobility и версия 3.1 Cisco AnyConnect VPN Client
- Сервер политик Сети Microsoft (NPS) сервер RADIUS

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

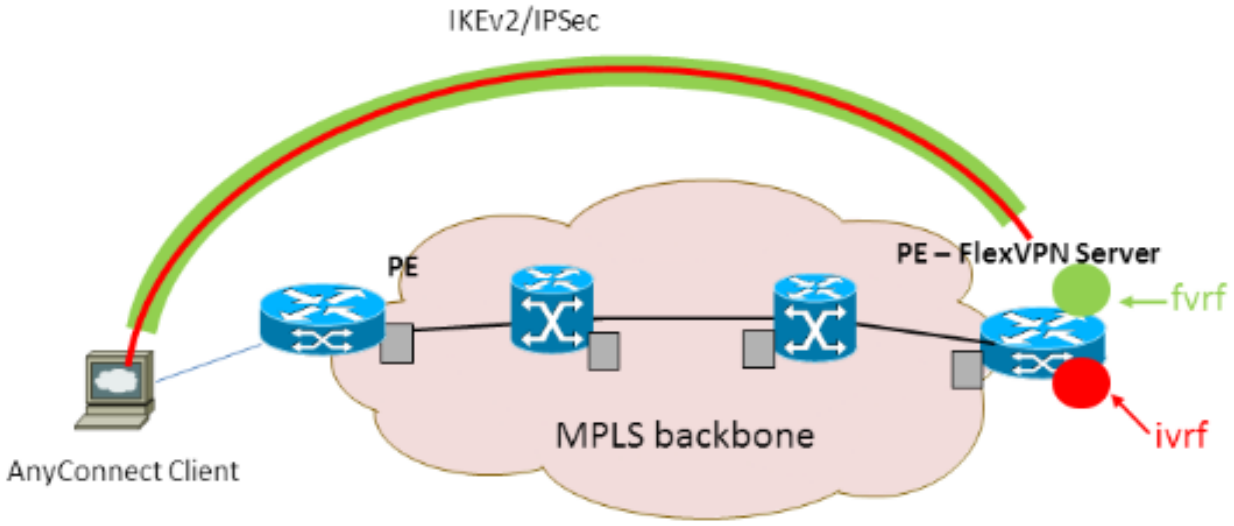
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Топология сети

В настоящем документе используется следующая схема сети:



Конфигурация сервера FlexVPN

Это - пример конфигурации сервера 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
```

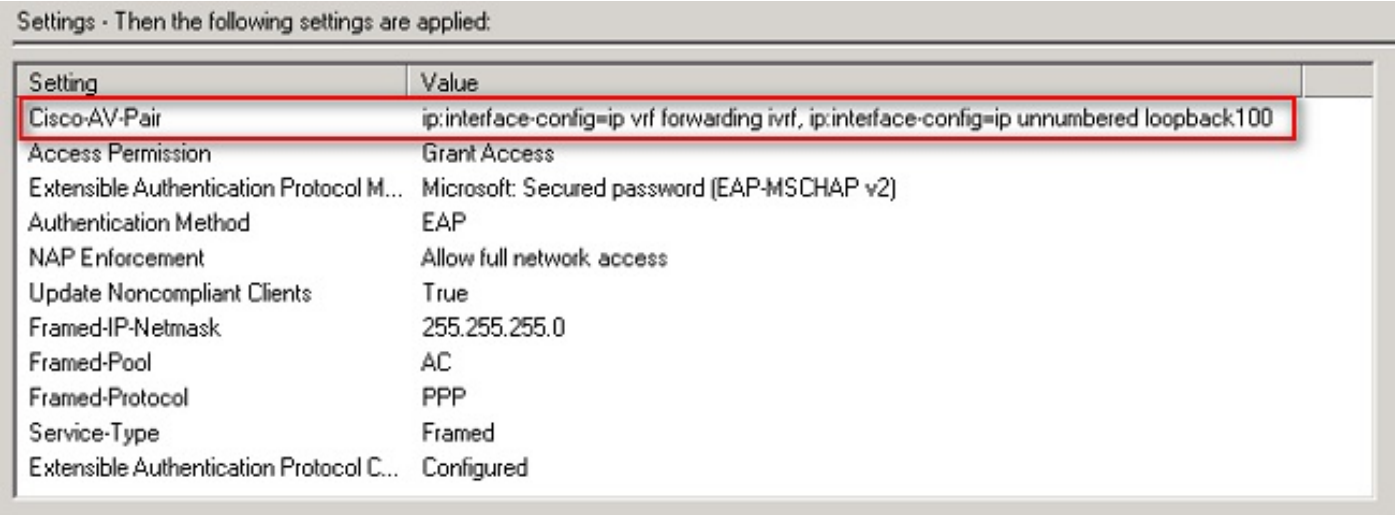
```
negotiation auto mpls ip cdp enable ! ! ! interface Virtual-Template40 type tunnel no ip address
tunnel mode ipsec ipv4 tunnel vrf fvrf tunnel protection ipsec profile AC ! router bgp 2 bgp
log-neighbor-changes redistribute connected redistribute static neighbor 10.2.2.2 remote-as 2
neighbor 10.2.2.2 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
```

Конфигурация профиля пользователя RADIUS

Ключевая конфигурация, используемая для Профиля RADIUS, является двумя парами значения атрибута (AV) определяемых поставщиком атрибутов (VSA) Cisco, которые помещают динамично созданный интерфейс виртуального доступа в IVRF и включают IP на динамично созданном интерфейсе виртуального доступа:

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

В Microsoft NPS конфигурация находится в параметрах настройки Сетевой политики как показано в данном примере:



Внимание. : Команда ip vrf forwarding должна прибыть перед **командой ip unnumbered**. Если интерфейс виртуального доступа клонирован от виртуального шаблона, и **команда ip vrf forwarding** тогда применена, любой IP - конфигурация удален из интерфейса виртуального доступа. Несмотря на то, что туннель установлен, соседство CEF для точка-точка (P2P), интерфейс является неполным. Это - пример **команды show adjacency** с неполным результатом:

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

Если соседство CEF является неполным, весь исходящий трафик VPN отброшен.

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно. Проверьте полученный интерфейс виртуального доступа, затем проверьте параметры настройки FVRF и IVRF.

Полученный интерфейс виртуального доступа

Проверьте, что созданный интерфейс виртуального доступа клонирован правильно от интерфейса виртуального шаблона и применил все атрибуты по каждому пользователю, загруженные от сервера 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
```

Сеансы шифрования

Проверьте IVRF и параметры настройки FVRF с этими выходными данными уровня управления.

Это - пример выходных данных от **показа крипто-открытая сеанс** подробная команда:

```
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
```

Это - пример выходных данных от **команды 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#
```

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация