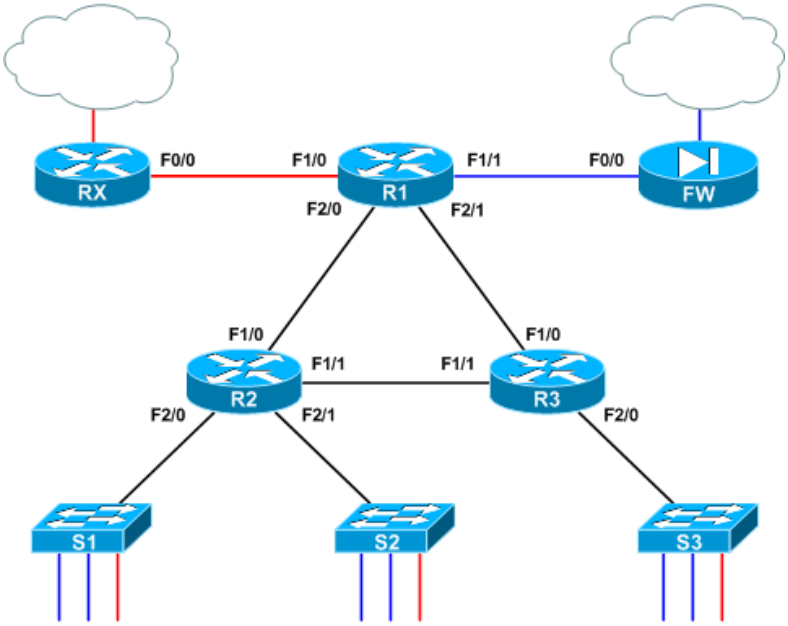
Úvod do VRF Lite

VRF (VPN Routing and Forwarding) je mechanismus pro izolaci provozů v síti. Obvykle se používá ve spojení s MPLS (MultiProtocol Label Switching), ale může pracovat samostatně (v terminologii Cisco jde o VRF Lite). Fakticky se jedná o vytvoření virtuálních sítí na 3. vrstvě, obdoby VLAN na 2. vrstvě. Každá taková virtuální síť dopravuje pakety posvém, může používat jiný směrovací protokol apod. – to vše na společné fyzické/linkové infrastruktuře.

Scénář

Instituce provozuje síť, podléhající stanoveným pravidlům. Příchozí a odchozí provoz je veden přes firewall, jehož nastavení implementuje striktní bezpečnostní politiku. V instituci však pravidelně hostují cizí uživatelé, u nichž není omezení žádoucí (nemají ovšem přístup k vnitřním zdrojům). Na přístupové vrstvě je oddělení vlastních a cizích uživatelů realizováno prostřednictvím VLAN, avšak požaduje se i oddělení datových toků v rámci sítě instituce. Instituce používá síť 10.0.0.0/16, pro cizí uživatele pak 192.168.0.0/16.



Na všech rozhraních směrovače, která budou využívána pro dopravu dat obou sítí, budou nakonfigurována dvě podrozhraní (subinterface), realizující zapouzdření 802.1Q, a to .10 pro VLAN 10 (BLUE) a .20 pro VLAN 20 (RED). Je vhodné poznamenat, že ačkoliv je použito uvedené zapouzdření 802.1Q, každý spoj představuje směrovaný segment s IP rozhraními na obou koncích. Například konfigurace rozhraní Fa2/0 směrovače R1 může vypadat takto:

```
interface FastEthernet2/0
 description To R2
 no ip address
!
interface FastEthernet2/0.10
 encapsulation dot1Q 10
 ip address 10.0.12.1 255.255.255.252
!
interface FastEthernet2/0.20
 encapsulation dot1Q 20
 ip address 192.168.12.1 255.255.255.252
```

Pokud by se jednalo o obecnou směrovanou síť, správce sítě by nyní musel začít s dalšími úpravami. Je zřejmé, že umožněním neomezeného přístup k Internetu z části sítě se vytvářejí "zadní vrátka", dokonce přímo obrovská bezpečnostní díra. Nicméně v daném případě lze jednotnou fyzickou infrastrukturu segmentovat do dvou virtuálních, izolovaných sítí. VRF používá v podstatě stejný koncept jako je VLAN (tj. trunking), ale na 3. vrstvě.

Podstata VRF Lite je prostá: každé směrované rozhraní (ať už fyzické nebo virtuální), patří právě do jedné VRF instance. Pokud nebyly použity importní či exportní mapy, není možné cesty (a tedy pakety) přesunout z jedné instance VRF do druhé (obdobně jako nelze rámce mezi VLAN). Pakety vstupující do VRF A mohou putovat pouze cestami uvedenými ve směrovací tabulce A, viz dále.

Jak se dá očekávat, před konfigurací VRF mají všechny směrovače ve svých [globálních] směrovacích tabulkách uvedeny všechny k nim připojené cesty (tj. místní sítě).

```
R1# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
   D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
   N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
   E1 - OSPF external type 1, E2 - OSPF external type 2
   i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
   ia - IS-IS inter area, * - candidate default, U - per-user static route
   o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

192.168.12.0/30 is subnetted, 1 subnets
    C       192.168.12.0 is directly connected, FastEthernet2/0.20
 192.168.13.0/30 is subnetted, 1 subnets
    C       192.168.13.0 is directly connected, FastEthernet2/1.20
 10.0.0.0/30 is subnetted, 3 subnets
    C       10.0.12.0 is directly connected, FastEthernet2/0.10
    C       10.0.13.0 is directly connected, FastEthernet2/1.10
    C       10.0.0.0 is directly connected, FastEthernet1/1
 192.168.0.0/30 is subnetted, 1 subnets
    C       192.168.0.0 is directly connected, FastEthernet1/0
```

Konfigurace

Konfigurace lze začít např. ve směrovači R1 vytvořením VRF BLUE a RED

```
R1(config)# ip vrf BLUE
R1(config-vrf)# description Trusted Traffic
R1(config-vrf)# ip vrf RED
R1(config-vrf)# description Guest Traffic
```

Dále lze přidat rozhraní Fa1/0, kterým bude vedena komunikace hostujících uživatelů

```
R1(config)# int f1/0
R1(config-if)# ip vrf forwarding RED
% Interface FastEthernet1/0 IP address 192.168.0.2 removed due to enabling
VRF RED
```

Při přiřazování rozhraní do VRF IOS automaticky odstraní jakékoliv předem nakonfigurované IP adresy, aby byla zrušena daná cesta z globální směrovací tabulky. Následně je třeba přiřadit tomuto rozhraní požadovanou IP adresu, čímž se jí příslušná síť dostane do specifické směrovací tabulky pro danou instanci VRF.

Takže na rozhraní Fa1/0 byla aplikována znovu daná adresa:

```
R1(config-if)# ip add 192.168.0.2 255.255.255.252
R1(config-if)# ^Z
R1# show run interface f1/0
Building configuration...
```

Směrovací tabulka však nyní vypadá takto:

```
R1# show ip route
[...]
192.168.12.0/30 is subnetted, 1 subnets
```

```
    C       192.168.12.0 is directly connected, FastEthernet2/0.20
 192.168.13.0/30 is subnetted, 1 subnets
    C       192.168.13.0 is directly connected, FastEthernet2/1.20
 10.0.0.0/30 is subnetted, 3 subnets
    C       10.0.12.0 is directly connected, FastEthernet2/0.10
    C       10.0.13.0 is directly connected, FastEthernet2/1.10
    C       10.0.0.0 is directly connected, FastEthernet1/1
```

Cesta (síť) 192.168.0.0/30 z globální směrovací tabulky zmizela, byla přemístěna do směrovací tabulky VRF RED, kterou musíme zkoumat zvlášť a to doplněním argumentu `vrf` za příkaz `show ip route`.

```
R1# show ip route vrf RED
[...]
192.168.0.0/30 is subnetted, 1 subnets
    C       192.168.0.0 is directly connected, FastEthernet1/0
```

Jak lze očekávat, předchozí krok je nutno příslušným způsobem opakovat pro všechna další rozhraní, tj. přidat do VRF. Výsledek je uveden níže:

```
interface FastEthernet1/0
 description To RX
 ip vrf forwarding RED
 ip address 192.168.0.2 255.255.255.252
!
interface FastEthernet1/1
 description To FW
 ip vrf forwarding BLUE
 ip address 10.0.0.2 255.255.255.252
!
interface FastEthernet2/0
 description To R2
 no ip address
!
interface FastEthernet2/0.10
 encapsulation dot1Q 10
 ip vrf forwarding BLUE
 ip address 10.0.12.1 255.255.255.252
!
interface FastEthernet2/0.20
 encapsulation dot1Q 20
 ip vrf forwarding RED
 ip address 192.168.12.1 255.255.255.252
!
interface FastEthernet2/1
 description To R3
 no ip address
!
interface FastEthernet2/1.10
 encapsulation dot1Q 10
 ip vrf forwarding BLUE
 ip address 10.0.13.1 255.255.255.252
!
interface FastEthernet2/1.20
 encapsulation dot1Q 20
 ip vrf forwarding RED
 ip address 192.168.13.1 255.255.255.252
```

Protože všechna rozhraní nyní náleží do izolovaných instancí VRF, je globální směrovací tabulka zcela prázdná. Lze ověřit, zda se všechny 10.0.0.0/16 cesty (sítě) nalézají v VRF BLUE, a všechny 192.168.0.0/16 cesty (sítě) v VRF RED:

```
R1# show ip route vrf BLUE
Routing Table: BLUE
[...]
10.0.0.0/30 is subnetted, 3 subnets
    C       10.0.12.0 is directly connected, FastEthernet2/0.10
    C       10.0.13.0 is directly connected, FastEthernet2/1.10
    C       10.0.0.0 is directly connected, FastEthernet1/1

R1# show ip route vrf RED
Routing Table: RED
[...]
192.168.12.0/30 is subnetted, 1 subnets
    C       192.168.12.0 is directly connected, FastEthernet2/0.20
 192.168.13.0/30 is subnetted, 1 subnets
    C       192.168.13.0 is directly connected, FastEthernet2/1.20
 192.168.0.0/30 is subnetted, 1 subnets
    C       192.168.0.0 is directly connected, FastEthernet1/0
```

Ačkoliv je v tomto okamžiku pro VRF pouze konfigurován pouze R1, byl by provoz pro R2 a R3 směrován bez problémů. Je to proto, že obdobně jako VLAN pro přepínač mají i VRF pro směrovač pouze lokální význam. Následně je třeba adekvátním způsobem nakonfigurovat VRF v dalších dvou směrovačích a poté přikročit k nastavení vybraného interního směrovacího protokolu. V tomto příkladu bude spuštěna jedna instance OSPF pro každou instanci VRF. Docílí se toho připojením klíčového slova `vrf` v každém příkazu `router`.

```
R1(config)# router ospf 1 vrf BLUE
R1(config-router)# router-id 0.0.1.1
R1(config-router)# network 10.0.0.0 0.0.255.255 area 0
R1(config-router)# router ospf 2 vrf RED
R1(config-router)# router-id 0.0.1.2
R1(config-router)# network 192.168.0.0 0.0.255.255 area 0
```

Jedná se o zcela nezávislé OSPF procesy, tudíž každý z nich musí jedinečný identifikátor směrovače, tj. router ID. Je vhodné připomenout, že tímto identifikátorem je libovolné 32bitové číslo zapsané stejným způsobem jako IPv4 adresa, čili čtveřicí dekadických čísel. Není-li uveden explicitně, je podle stanovených pravidel odvozen od některé IPv4 adresy přítomné ve směrovači. V daném případě představuje třetí pozice číslo směrovače a čtvrtá pozice pak konkrétní instanci VRF.

Po nakonfigurování dalších dvou směrovačů vždy se dvěma OSPF procesy lze pozorovat dva vztahy sousedství (adjacencies), vytvořené na každém spoji pro každou instanci VRF:

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State      Dead Time   Address         Interface
0.0.3.2           1   FULL/DR    00:00:39    192.168.13.2    FastEthernet2/1.20
0.0.2.2           1   FULL/DR    00:00:39    192.168.12.2    FastEthernet2/0.20
0.0.3.1           1   FULL/DR    00:00:31    10.0.13.2       FastEthernet2/1.10
0.0.2.1           1   FULL/DR    00:00:32    10.0.12.2       FastEthernet2/0.10
```

Za předpokladu, že v hraničních směrovačích neběží OSPF, bude nutno vytvořit dvě statické výchozí cesty ukazující na R1, pro každou instanci VRF jednu:

```
R1(config)# ip route vrf BLUE 0.0.0.0 0.0.0.0 10.0.0.1
R1(config)# ip route vrf RED 0.0.0.0 0.0.0.0 192.168.0.1
```

Až dosud se zdálo, že konfigurace VRF se většinou tvoří doplněním klíčového slova `vrf` k obvyklým příkazům, je-li to vhodné. Bohužel se toto klíčové slovo se nevkládá úplně všude, takže je třeba využít kontextově orientovanou nápovědu.

Lze ověřit, že v příslušných instancích VRF jsou přítomny vložené statické cesty současně s cestami z OSPF:

```
R1# show ip route vrf BLUE

Routing Table: BLUE
[...]

10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
   C       10.0.12.0/30 is directly connected, FastEthernet2/0.10
   C       10.0.13.0/30 is directly connected, FastEthernet2/1.10
   O       10.0.2.0/24 [110/2] via 10.0.12.2, 00:04:52, FastEthernet2/0.10
   O       10.0.3.0/24 [110/2] via 10.0.13.2, 00:04:52, FastEthernet2/1.10
   C       10.0.0.0/30 is directly connected, FastEthernet1/1
   O       10.0.1.0/24 [110/2] via 10.0.12.2, 00:04:52, FastEthernet2/0.10
   O       10.0.23.0/30 [110/2] via 10.0.13.2, 00:04:52, FastEthernet2/1.10
                [110/2] via 10.0.12.2, 00:04:52, FastEthernet2/0.10
S*   0.0.0.0/0 [1/0] via 10.0.0.1
R1# show ip route vrf RED

Routing Table: RED
[...]

192.168.12.0/30 is subnetted, 1 subnets
   C       192.168.12.0 is directly connected, FastEthernet2/0.20
 192.168.13.0/30 is subnetted, 1 subnets
   C       192.168.13.0 is directly connected, FastEthernet2/1.20
 192.168.23.0/30 is subnetted, 1 subnets
   O       192.168.23.0 [110/2] via 192.168.13.2, 00:04:16,
FastEthernet2/1.20
                [110/2] via 192.168.12.2, 00:04:16, FastEthernet2/0.20
 192.168.0.0/30 is subnetted, 1 subnets
   C       192.168.0.0 is directly connected, FastEthernet1/0
   O    192.168.1.0/24 [110/2] via 192.168.12.2, 00:04:16,
FastEthernet2/0.20
   O    192.168.2.0/24 [110/2] via 192.168.12.2, 00:04:16,
FastEthernet2/0.20
   O    192.168.3.0/24 [110/2] via 192.168.13.2, 00:04:17,
FastEthernet2/1.20
S*   0.0.0.0/0 [1/0] via 192.168.0.1
```

Nakonec je zapotřebí výchozí cesty ze směrovače R1 inzerovat v obou OSPF procesech, takže se je mohou směrovače R2 a R3 naučit. Při vstupu do konfigurace OSPF procesů není potřeba připojit klíčové slovo `vrf`, neboť již bylo použito dříve při jejich počáteční konfiguraci:

```
R1(config)# router ospf 1
R1(config-router)# default-information originate
R1(config-router)# router ospf 2
R1(config-router)# default-information originate
```

Prostřednictvím R2 lze zjistit, že každá instance VRF má nyní svoji vlastní kompletní směrovací tabulku:

```
R2# show ip route vrf BLUE

Routing Table: BLUE
[...]
10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
   C       10.0.12.0/30 is directly connected, FastEthernet1/0.10
   O       10.0.13.0/30 [110/2] via 10.0.23.2, 00:14:23, FastEthernet1/1.10
                [110/2] via 10.0.12.1, 00:13:53, FastEthernet1/0.10
   C       10.0.2.0/24 is directly connected, FastEthernet2/1.10
   O       10.0.3.0/24 [110/2] via 10.0.23.2, 00:14:23, FastEthernet1/1.10
   O       10.0.0.0/30 [110/2] via 10.0.12.1, 00:13:53, FastEthernet1/0.10
   C       10.0.1.0/24 is directly connected, FastEthernet2/0.10
```

```
   C       10.0.23.0/30 is directly connected, FastEthernet1/1.10
O*E2 0.0.0.0/0 [110/1] via 10.0.12.1, 00:03:33, FastEthernet1/0.10

R2# show ip route vrf RED

Routing Table: RED
[...]
192.168.12.0/30 is subnetted, 1 subnets
   C       192.168.12.0 is directly connected, FastEthernet1/0.20
 192.168.13.0/30 is subnetted, 1 subnets
   O       192.168.13.0 [110/2] via 192.168.23.2, 00:36:59,
FastEthernet1/1.20
                [110/2] via 192.168.12.1, 00:20:54, FastEthernet1/0.20
 192.168.23.0/30 is subnetted, 1 subnets
   C       192.168.23.0 is directly connected, FastEthernet1/1.20
 192.168.0.0/30 is subnetted, 1 subnets
   O       192.168.0.0 [110/2] via 192.168.12.1, 00:20:54,
FastEthernet1/0.20
   C    192.168.1.0/24 is directly connected, FastEthernet2/0.20
   C    192.168.2.0/24 is directly connected, FastEthernet2/1.20
   O    192.168.3.0/24 [110/2] via 192.168.23.2, 00:41:13,
FastEthernet1/1.20
   O*E2 0.0.0.0/0 [110/1] via 192.168.12.1, 00:01:41, FastEthernet1/0.20
```

Obě instance VRF jsou nyní plně funkční. Například paket od hostitele v BLUE VLAN 10 v přepínači 2 vstoupí do BLUE VRF subinterface v R2 a je směrován přes R1 BLUE VRF ven do firewallu. Při řešení problémů (jako `ping`) je nutno specifikovat VRF:

```
R2# ping 10.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R2# ping vrf BLUE 10.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/15/20 m
```

http://packetlife.net/blog/2009/apr/30/intro-vrf-lite/