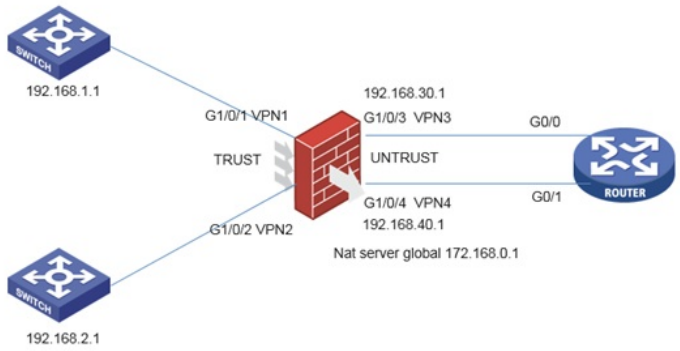
V7防火墙流量二次串墙互访典型配置举例

NAT 孙兆强 2020-05-31 发表

组网及说明



客户有多个业务网段，要求网段之间互访的控制不通过防火墙来做。流量二次穿过防火墙，流量控制在路由器上。以1.0和2.0为例。1.0网段访问2.0网段的流量需要通过访问映射映射后地址172.168.0.1来访问。

通过虚墙来实现的话因网段太多可能造成资源不足，客户采用在接口绑定vpn实例的方式实现。

配置步骤

防火墙关键配置

```
ip vpn-instance vpn1
 #
 address-family ipv4
  route-replicate from vpn-instance vpn3 protocol ospf 3
//将G1/0/3  vpn3中通过ospf学习的路由引入VPN1
#
ip vpn-instance vpn2
 #
 address-family ipv4
  route-replicate from vpn-instance vpn4 protocol ospf 4
//将G1/0/4  vpn4中通过ospf学习的路由引入VPN2
#
ip vpn-instance vpn3
 #
 address-family ipv4
  route-replicate from vpn-instance vpn1 protocol direct
//将vpn1的直连路由引入vpn3
#
ip vpn-instance vpn4
 #
 address-family ipv4
  route-replicate from vpn-instance vpn2 protocol direct
将vpn2的直连路由引入vpn4
#
ospf 3 vpn-instance vpn3
 area 0.0.0.0
  network 192.168.30.0 0.0.0.255
#
ospf 4 vpn-instance vpn4
 area 0.0.0.0
  network 192.168.40.0 0.0.0.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 description vpn1
 combo enable copper
 ip binding vpn-instance vpn1
 ip address 192.168.1.2 255.255.255.0
```

```
#
interface GigabitEthernet1/0/2
 port link-mode route
 description vpn2
 combo enable copper
 ip binding vpn-instance vpn2
 ip address 192.168.2.2 255.255.255.0
#
interface GigabitEthernet1/0/3
 port link-mode route
 description vpn3
 combo enable copper
 ip binding vpn-instance vpn3
 ip address 192.168.30.1 255.255.255.0
#
interface GigabitEthernet1/0/4
 port link-mode route
 description vpn4
 combo enable copper
 ip binding vpn-instance vpn4
 ip address 192.168.40.1 255.255.255.0
 nat server global 172.168.0.1 vpn-instance vpn4 inside 192.168.2.1 vpn-instance vpn2
#
security-zone name Trust
 import interface GigabitEthernet1/0/1
 import interface GigabitEthernet1/0/2
#
security-zone name Untrust
 import interface GigabitEthernet1/0/3
 import interface GigabitEthernet1/0/4
#
zone-pair security source Local destination Untrust
 packet-filter 3000
#
security-policy ip
 rule 1 name vpn1tovpn3 /第一次穿行流量
  action pass
  vrf vpn1
  source-zone trust
  destination-zone untrust
 rule 2 name vpn4tovpn2 //第二次穿行流量
  action pass
  vrf vpn2   //先匹配nat server再匹配安全策略，nat之后流量属于vpn2而不属于vpn4
  source-zone untrust
  destination-zone trust
 rule 3 name ospf1
  action pass
  vrf vpn3
  source-zone untrust
  source-zone local
  destination-zone local
  destination-zone untrust
 rule 4 name ospf2
  action pass
  vrf vpn4
  source-zone local
  source-zone untrust
  destination-zone local
  destination-zone untrust
路由器关键配置
ospf 1
 import-route static
 area 0.0.0.0
  network 192.168.30.0 0.0.0.255
```

network 192.168.40.0 0.0.0.255

ip route-static 172.168.0.1 32 192.168.40.1
ip route-static 192.168.1.0 24 192.168.30.1
ip route-static 192.168.2.0 24 192.168.40.1

配置关键点

从vpn引入的路由无法继续通过ospf传递，所有需要路由静态配置回程路由。
如果网关不是防火墙可以跟下面的设备建立ospf，vpn实例里引入ospf即可。
在路由器上配置包过滤即可完成流量控制