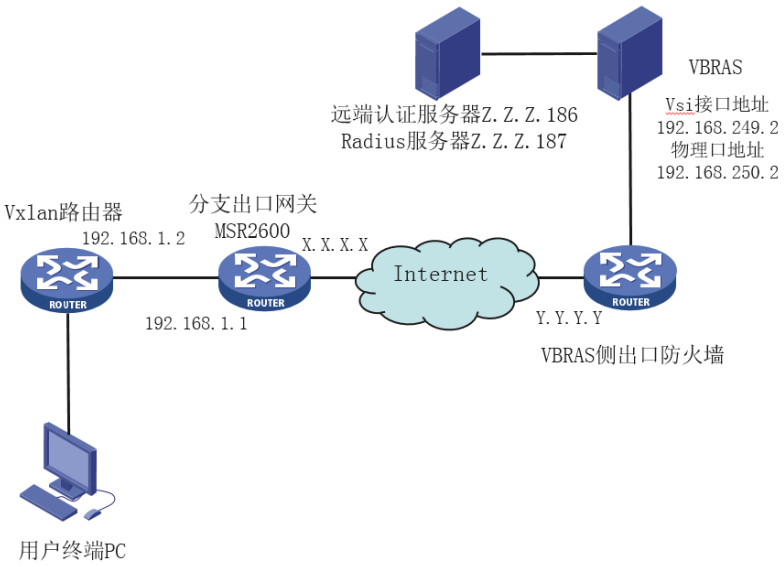
VBRAS与MSR 建立vxlan隧道穿越NAT公网做IPOE+WEB认证典型案例

vBRAS 王喆兴 2019-09-29 发表

组网及说明



组网如图，MSR2600作为用户侧出口网关（公网地址X.X.X.X）下挂一台路由器与运营商防火墙（公网地址Y.Y.Y.Y）内侧VBRAS建立vxlan隧道。用户通过二层广播dhcp报文触发ipoe web认证。VBRAS作为DHCP server下发192.168.249.0网段给用户侧使用，同时作为ipoe web认证的BRAS接入设备。

配置步骤

两侧公网网关设备只需将内侧VXLAN地址静态NAT映射出去即可。此处以MSR2600 NAT配置为例，防火墙配置同理。

```
nat address-group 1
 address X.X.X.X X.X.X.X
#
 nat static outbound 192.168.1.2 X.X.X.X

interface GigabitEthernet0/1 与vxlan设备对接接口
 port link-mode route
 ip address 192.168.1.1 255.255.255.252

interface GigabitEthernet0/0
 port link-mode route
 ip address X.X.X.X 255.255.255.224
 nat static enable
```

MSR2600侧vxlan设备主要配置。

```
vlan 10
#
 l2vpn enable
#
vsi vpna
 vxlan 10
  tunnel 1
interface GigabitEthernet0/1
 port link-mode route
 ip address 192.168.1.2 255.255.255.252
#
 ip route-static 0.0.0.0 0 192.168.1.1
#
interface GigabitEthernet0/2
```

```
 port link-mode route
 xconnect vsi vpna
#
interface Tunnel1 mode vxlan
 source 192.168.1.2
 destination Y.Y.Y.Y
#
```

VBRAS侧配置。

```
dhcp enable

#
traffic classifier web_deny operator or
 if-match acl name web_deny
#
traffic classifier web_http operator or
 if-match acl name web_http
#
traffic classifier web_https operator or
 if-match acl name web_https
#
traffic classifier web_out operator or
 if-match acl name web_out
#
traffic classifier web_permit operator and
 if-match acl name web_permit
#
traffic behavior web_deny
 filter deny
#
traffic behavior web_http
 redirect http-to-cpu
#
traffic behavior web_https
 redirect https-to-cpu
#
traffic behavior web_out
 filter permit
#
traffic behavior web_permit
 filter permit
#
qos policy out
 classifier web_out behavior web_out
 classifier web_deny behavior web_deny
#
qos policy web
 classifier web_permit behavior web_permit
 classifier web_http behavior web_http
 classifier web_https behavior web_https
 classifier web_deny behavior web_deny
#
dhcp server ip-pool pool1
 gateway-list 192.168.249.2 export-route
 network 192.168.249.0 mask 255.255.255.0
 dns-list 114.114.114.114
 forbidden-ip 192.168.249.2
 forbidden-ip 192.168.249.3
#
 l2vpn enable
#
vsi vpna
 gateway vsi-interface 1
```

```
 vxlan 10
  tunnel 1

#
interface GigabitEthernet1/1/0
 port link-mode route
 ip address 192.168.250.2 255.255.255.0
#
interface Vsi-interface1
 ip address 192.168.249.2 255.255.255.0
 qos apply policy web inbound
 qos apply policy out outbound
 ip subscriber l2-connected enable
 ip subscriber initiator dhcp enable
 ip subscriber authentication-method web
 ip subscriber pre-auth domain 认证前域
 ip subscriber web-auth domain 认证后域.com
#
interface Tunnel1 mode vxlan
 source 192.168.250.2
 destination X.X.X.X
#
 ip route-static 0.0.0.0 0 192.168.250.254
#

acl advanced name web_deny match-order auto
 rule 100 permit ip user-group web
#
acl advanced name web_http match-order auto
 rule 10 permit tcp destination-port eq www user-group web
#
acl advanced name web_https match-order auto
 rule 10 permit tcp destination-port eq 443 user-group web
#
acl advanced name web_out match-order auto
 rule 10 permit ip source Z.Z.Z.186 0 user-group web
 rule 20 permit ip source Z.Z.Z.187 0 user-group web
 rule 30 permit ip source 114.114.114.114 0 user-group web
#
acl advanced name web_permit match-order auto
 rule 10 permit ip destination Z.Z.Z.186 0 user-group web
 rule 20 permit ip destination Z.Z.Z.187 0 user-group web
 rule 30 permit ip destination 114.114.114.114 0 user-group web
#
radius scheme rs1
 primary authentication Z.Z.Z.187 key cipher $c$3$TbMowzL3wjRtCOOBiAO0p0Fbxq3Qr160j6o=
 primary accounting Z.Z.Z.187 key cipher $c$3$DZGcuyccVl4bjVL+SgiKl+TdaJW0Jb8AyaE=
#
domain name 认证后域.com
 authentication ipoe radius-scheme rs1
 authorization ipoe radius-scheme rs1
 accounting ipoe radius-scheme rs1
#
domain name 认证前域
 authorization-attribute user-group web
 authorization-attribute ip-pool pool1
 authentication ipoe none
 authorization ipoe none
 accounting ipoe none
 web-server url http://Z.Z.Z.186:89/aci10/login
 web-server ip Z.Z.Z.186
 web-server url-parameter mac source-mac
 web-server url-parameter url original-url
 web-server url-parameter wlanuserip source-address
```

```
#
user-group web
#
 portal device-id vbras
#
portal web-server newpt
#
portal server newpt
 ip Z.Z.Z.187
#
 http-redirect https-port 89
#
```

配置关键点

1. 注意VBRAS侧qos policy的配置一定要正确,CB对的顺序都要严格和案例一致。
2. 两侧vxlan隧道的目的地址需写对端公网地址。