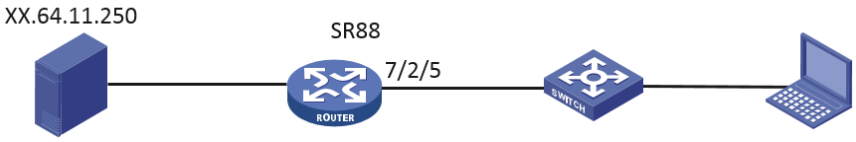
SR8808-X ipoe 认证无法弹页面

Portal 郭尧 2023-03-27 发表

组网及说明



组网如上：sr8808-x做bars设备接入，同时也充当终端的dhcp服务器。

问题描述

配置ipoe的web认证，终端使用dhcp下发的地址进行认证。使用IP地址都可以重定向到认证页面，使用域名重定向失败。

过程分析

检查ipoe相关配置，完整配置如下：

```
#bars作为dhcp
 dhcp server ip-pool gy-1
 gateway-list 10.68.0.1 export-route
 network 10.68.0.0 mask 255.255.0.0
 dns-list xxx.102.192.xx xxx.104.78.xx
 expired day 0 hour 8
 forbidden-ip 10.68.0.1

 # 配置IPoE用户在Web认证阶段使用的认证域
 domain name ipoeweb2
 authorization-attribute ip-pool gy-1
 authorization-attribute user-group web  # 配置认证前域授权地址池以及用户组。
 authentication ipoe none
 authorization ipoe none
 accounting ipoe none
 web-server url http://10.64.11.250/a79.htm

 # 配置IPoE用户在Web认证阶段使用的认证域。
domain name ipoeweb
 authentication ipoe radius-scheme ipoe
 authorization ipoe radius-scheme ipoe
 accounting ipoe radius-scheme ipoe

 #默认进认证前域
domain default enable ipoeweb2
 #radius相关配置
radius scheme ipoe
 primary authentication 10.64.11.250 key cipher $c$3$ax2sHpfkFRSnFJ6mF0jqPVkE0yxqIdp1DsqS
 primary accounting 10.64.11.250 key cipher $c$3$iBnj7HCNm8Aa7YPhfiJYK23rGE4nfiufIyun
 user-name-format without-domain
 nas-ip 10.64.11.XX

 # 创建认证前域用户组，名称为web
 user-group web

 # 配置Portal认证服务器：名称为portal，IP地址为10.64.11.250，密钥为明文123456。
 portal server portal
 ip 10.64.11.250 key cipher $c$3$ZIGS1GPynO06QUmvFisA574IMuYmlals052E
 port 2000

 # 为IPv4高级ACL web_permit创建规则如下：匹配用户组web中用户的目的地址为Portal服务器地址的报文
 acl advanced name web_permit
 rule 0 permit ip destination 10.64.11.250 0 user-group web 服务器地址
 rule 5 permit ip destination 218.104.78.xx 0 user-group web   dns服务器地址
 rule 10 permit ip destination 202.102.192.xx 0 user-group web  dns服务器地址

 # 为IPv4高级ACL web_http创建规则如下：匹配用户组web中用户的目的端口为80的TCP报文(即HTTP报文)。
 acl advanced name web_http
 rule 0 permit tcp destination-port eq www user-group web

 #为IPv4高级ACL web_https创建规则如下：匹配用户组web中用户的目的端口为443的TCP报文(即HTTPS报文)。
acl advanced name web_https
 rule 0 permit tcp destination-port eq 8443 user-group web

 # 为IPv4高级ACL ip创建规则如下：匹配用户组web中用户的IP报文。
 acl advanced name ip
```

rule 0 permit ip user-group web
#
traffic classifier neiwang operator and
if-match acl name neiwang
#
traffic classifier web_http operator and
if-match acl name web_http
#
traffic classifier web_https operator and
if-match acl name web_https
#
traffic behavior web_permit
filter permit
free-account
#
traffic behavior web_http
redirect http-to-cpu
#
traffic behavior web_https
redirect https-to-cpu
#
traffic behavior neiwang
filter permit
free-account
#
traffic behavior neiwang_out
filter permit
#
traffic behavior web_deny
filter deny
free-account
#为类指定对应的流行为，规则为：允许用户组web中源地址为portal服务器和内网服务器IP地址的报文通过，其余报文均禁止通过。
qos policy web
classifier web_permit behavior web_permit
classifier neiwang behavior neiwang
classifier web_http behavior web_http
classifier web_https behavior web_https
classifier ip behavior web_deny
#为类指定对应的流行为，规则为：允许用户组web中源地址为portal服务器和内网服务器IP地址的报文通过，其余报文均禁止通过。
qos policy out
classifier neiwang_out behavior neiwang_out
classifier web_out behavior web_out
classifier ip behavior web_deny

对接收的用户流量应用QoS策略，策略名为web。
[SR8804X] qos apply policy web global inbound
对发送的上线用户流量应用QoS策略，策略名为out。
[SR8804X] qos apply policy out global outbound

从上述配置看，在web_permit中已经针对相应dns进行放通，但是测试发现终端拿到对应地址，ping不通dns；
用户认证前域认证通过之后，通过以下的显示命令查看IPoE用户在线信息，可以看到的user-group已经是配置的“web”
[SR8804X] display ip subscriber session verbose
Basic:
 Description   : -

解决方法

以测试接口xx-7/2/5.2801为例，PBR选路是依据用户的user-group属性，用户流量匹配到PBR的acl并执行指定下一跳；NAT需要接口下qos policy匹配用户流量，引流到slot 2 cpu。用户流量到达bras后，只能匹配一次acl并执行对应动作（此处PBR优先级高），不能既PBR又NAT引流。因此现网的需求无法实现，建议新增防火墙板卡或者cgn板卡做nat。

另外单独的防火墙板卡或cgn板卡做nat是没问题的，现场用CPSEX业务板卡做nat有问题。

display device verbose==========

Slot No. Brd Type Brd Status Software Version
0 NONE Absent NONE
1 NONE Absent NONE
2 CSPEX-1304X Normal SR8800-CMW710-R7951P11
Sub 1 MIC-XP5U1 Normal

可以关注两个地方，一是做nat的流量不要超过200Mbps，二是看业务板卡nat进程对应的cpu剩余情况，idle建议不要低于30%。

monitor thread dumbtty slot 2

859 processes, 418 threads
Thread states: 3 running, 409 sleeping, 0 stopped, 0 zombie
CPU0: 87.07% idle, 0.71% user, 7.91% kernel, 4.31% interrupt, 0.00% steal
CPU1: 70.23% idle, 7.80% user, 12.05% kernel, 9.92% interrupt, 0.00% steal
CPU2: 91.43% idle, 0.00% user, 8.57% kernel, 0.00% interrupt, 0.00% steal
CPU3: 100.00% idle, 0.00% user, 0.00% kernel, 0.00% interrupt, 0.00% steal
CPU4: 92.91% idle, 0.00% user, 7.09% kernel, 0.00% interrupt, 0.00% steal
CPU5: 0.01% idle, 0.00% user, 99.29% kernel, 0.70% interrupt, 0.00% steal
CPU6: 99.30% idle, 0.00% user, 0.00% kernel, 0.70% interrupt, 0.00% steal
CPU7: 0.00% idle, 0.00% user, 100.00% kernel, 0.00% interrupt, 0.00% steal
CPU8: 100.00% idle, 0.00% user, 0.00% kernel, 0.00% interrupt, 0.00% steal
CPU9: 100.00% idle, 0.00% user, 0.00% kernel, 0.00% interrupt, 0.00% steal
CPU10: 100.00% idle, 0.00% user, 0.00% kernel, 0.00% interrupt, 0.00% steal
CPU11: 100.00% idle, 0.00% user, 0.00% kernel, 0.00% interrupt, 0.00% steal
CPU12: 99.29% idle, 0.00% user, 0.71% kernel, 0.00% interrupt, 0.00% steal
CPU13: 100.00% idle, 0.00% user, 0.00% kernel, 0.00% interrupt, 0.00% steal
CPU14: 100.00% idle, 0.00% user, 0.00% kernel, 0.00% interrupt, 0.00% steal
CPU15: 100.00% idle, 0.00% user, 0.00% kernel, 0.00% interrupt, 0.00% steal
Memory: 2834M total, 648M available, page size 4K

对于目的端口为80（HTTP报文）和443（HTTPS报文）的报文重定向到CPU；

除上述报文外，其余报文均禁止通过。

JID Name Tid Name %CPU PRI State HH:MM:SS MAX CPU Name
355 355 8 100 D 07:07:15 0 0.04% [NAT0]
356 356 9 100 D 07:40:39 0 0.04% [NAT1]
357 357 10 100 D 07:48:08 0 0.04% [NAT2]
358 358 11 100 D 07:27:22 0 0.04% [NAT3]
359 359 12 100 D 07:06:23 0 0.04% [NAT4]
360 360 13 100 D 07:38:54 0 0.04% [NAT5]
361 361 14 100 D 07:38:02 0 0.04% [NAT6]
362 362 15 100 D 07:22:56 0 0.04% [NAT7]

Username : 0015e947f4d4
Domain : ipoeweb2