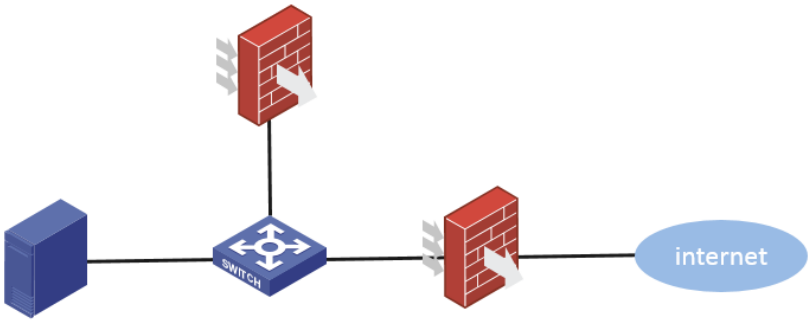
防火墙旁挂核心做ssl vpn inode能拨上号无法访问内网

SSL VPN 郭尧 2020-03-31 发表

组网及说明



防火墙旁挂做ssl vpn

问题描述

设备做了SSLVPN后，能够拨号获取地址，但是无法访问内网资源

过程分析

查看基本配置无误

```
sslvpn context ctx
 gateway gw
 ip-tunnel interface SSLVPN-AC1
 ip-tunnel address-pool ippool mask 255.255.255.0
 ip-tunnel dns-server primary 114.114.114.114
 ip-route-list rtlist
 include 192.43.0.0 255.255.0.0
 include 192.168.1.0 255.255.255.0
 policy-group pgroup
 filter ip-tunnel 3000
 ip-tunnel access-route ip-route-list rtlist
 service enable
```

PC路由表的路由也正常下发，但是还是访问不通资源。

在防火墙上测试能ping通服务器192.43网段，服务器本身也能ping通ac口地址，由此来看路由回程和安全策略没有问题

进行debug 和会话查看

发现进程路由走向为sslvpn ac-----1/0/4

回程路由为 1/0/4 ----1/0/6

怀疑路由走向有误，查看发现在内网口配置了PBR

```
policy-based-route aaa permit node 3007
if-match acl 3007
apply next-hop 201.28.124.51
这个是pbr
#
acl advanced 3007
rule 0 permit ip source 192.43.151.0 0.0.0.255
```

解决方法

将PBR进行修改，剔除服务器网段后解决。

遇到SSLVPN拨入，能够获取地址ping不通内网，可能如下问题：

1.服务器没有到AC口或者地址池的回程路由；

2.配置了不规范的策略路由；

原因：回包应该查路由走AC口的匹配策略路由走公网口出去了；

```
interface Vlan-interface934
policy-based-route user permit node 50
ip policy-based-route user
#
if-match acl 3013
apply next-hop 140.206.62.9 track 1
```

#
acl advanced 3013
rule 3 permit ip source 10.9.176.0 0.0.15.255
rule 4 permit ip source 172.29.240.0 0.0.15.255
rule 5 permit ip source 10.9.240.0 0.0.3.255 内网SSL VPN网段资源

解决方案：把对应的内网资源网段rule 5删除或者deny掉

3.SSL VPN策略组里调用的ACL过滤有问题

原因：ACL 3999规则为只允许目的地址为*.*.*.0（前24位任意，最后八位必须为0的ip地址）的地址访问，但不是真实的内网资源地址

#

acl advanced 3999

rule 0 permit ip destination 0.0.0.0 255.255.255.0 反掩码

#

policy-group SSLVPNZIYUAN

filter ip-tunnel acl 3999

ip-tunnel access-route ip-route-list NEIWANG

service enable

#

此外如果debugging sslvpn error中出现IPAC: Failed to get ACL.也说明没有获取到过滤IP接入的ACL规则，需要检查ACL配置。

解决方案：ACL中规则的目的地址放通对应的内网资源地址

4. AC口没有加入安全域

原因：AC口对客户端发来的报文进行解封装， SSL VPN 解封装之后的报文会被设备识别成是从SSL VPN的AC口收到的报文，AC口不加入安全域会导致报文被策略丢弃。

解决方案：把AC口加入相应的安全域，并放通AC到内网的安全策略（untrust-trust）

[F5020]security-zone name untrust

[F5020-security-zone-Trust]import interface SSLVPN-AC 1

[F5020-security-policy-ip]rule 1 name AC-trust

[F5020-security-policy-ip-1-AC-trust]source-zone untrust

[F5020-security-policy-ip-1-AC-trust]destination-zone trust

5. 新增服务器网段不可达。

原因：新增服务器网段的路由没有下发到终端，需要将sslvpn service重启。

[Sysname] sslvpn gateway gw

ip-route-list rtlist

include 172.16.1.0 255.255.255.0

Include 10.88.1.0/24

service enable