防火墙映射udp500 4500端口ipsec模块丢包问题

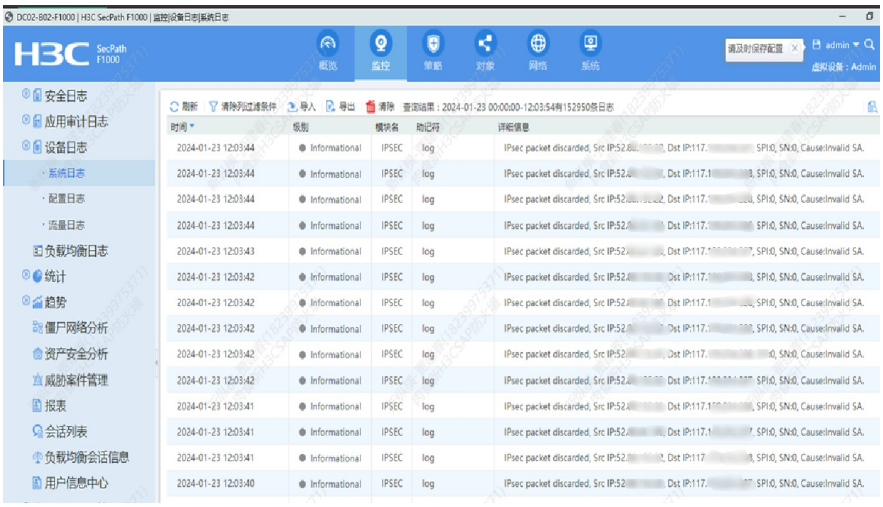
IKE IPSec VPN NAT 陈泽勇 2024-01-29 发表

组网及说明

防火墙f1090-2将内网服务器server2-4的IPSec udp500 4500端口映射成公网地址加端口，国外的f1090-1防火墙访问映射后的公网地址建立IPSec隧道

问题描述

流量到达防火墙后，日志一直在报IPSec丢包，日志提示如下，报错的原因是没有合适的IPSec隧道导致被丢包：



过程分析

1、后续让现场收集debug信息，查看防火墙的报文转发情况，发现对应的流量被IPSec模块丢弃了。

%Jan 23 14:25:09:134 2024 DC02-B02-F1000 IPSEC/6/log: -COntext=1;
IPsec packet discarded, Src IP:52.80.xx.xx, Dst IP:117.159.xx.xx, SPI:0, SN:0, Cause:Invalid SA.

*Jan 23 14:25:09:134 2024 DC02-B02-F1000 IPFW/7/IPFW_INFO: -COntext=1;
MBUF was intercepted! Phase Num is 1(pre routing), Service ID is 8(ipsec), Bitmap is d0004000000000, return 1(0:continue, 1:dropped, 2:consumed, 3:enqueued, 4:relay)!
Interface is GigabitEthernet1/0/22,
s= 52.80.xx.xx, d= 117.159.xx.xx, protocol= 17, pktid = 0
VsysID = 1.

2、防火墙本身是有建立ipsec隧道的，但是不是用同一个地址与对端防火墙建立的ipsec隧道且流量从公网往内网访问、不匹配感兴趣流，按理来说不会走ipsec隧道才对：

```
==========display ipsec sa brief==========
Interface/Global          Dst Address       SPI          Protocol    Status
GE1/0/22                  43.255.x.x        3039033391   ESP         Active
GE1/0/22                  117.159.x.x       3508793302   ESP         Active
GE1/0/22                  43.255.x.x        3331687263   ESP         Active
GE1/0/22                  117.159.x.x       2966093317   ESP         Active
GE1/0/22                  43.255.x.x        3508599419   ESP         Active
GE1/0/22                  117.159.x.x       2979879242   ESP         Active
GE1/0/22                  43.255.x.x        3972010883   ESP         Active
GE1/0/22                  117.159.x.x       1451922887   ESP         Active
```

acl advanced name IPsec_lenovoSAP_IPv4_1
rule 0 permit ip source 30.255.7.0 0.0.0.127 destination 10.120.26.0 0.0.0.15

rule 1 permit ip source 30.255.7.0 0.0.0.127 destination 30.255.7.128 0.0.0.127

3、查看配置发现映射配置无问题，使用的全局nat做的匹配：

```
#
object-group service UDP500_4500
 0 service udp destination eq 500
 10 service udp destination eq 4500
#
```

```
 service icmp-address-mask
 service icmp-dest-unreachable
 service icmp-fragment-needed
 service icmp-fragment-reassembly
 service icmp-host-unreachable
 service icmp-info
 service icmp-parameter-problem
 service icmp-port-unreachable
 service icmp-protocol-unreach
 service icmp-redirect
 service icmp-redirect-host
 service icmp-redirect-tos-host
 service icmp-redirect-tos-net
 service icmp-source-quench
 service icmp-source-route-fail
 service icmp-time-exceeded
 service icmp-timestamp
 service icmp-traceroute
 service ike
 service ping
 service UDP500_4500
 source-zone RS_SAP_yd
 source-ip SAP VPN公网地址
 destination-ip host 117.15
 action dnat ip-address 10.
 disable
```

4、经沟通确认如果设备既做NAT设备，又做ipsec的情况下，由于设备的报文处理流程机制，先查询端口服务匹配，再匹配地址，所以500端口和4500端口流量到设备后会认为是IPSEC相关流量，会优先匹ipsec模块流程，即使删除了接口下的地址，只要设备有ipsec或者ipsec残留都会导致这个情况，因地址对应不上所以被ipsec丢弃。

解决方法

使用vrf技术将内外网接口加入到同一个vpn实例起IPSec与NAT实现逻辑上隔离后问题解决。