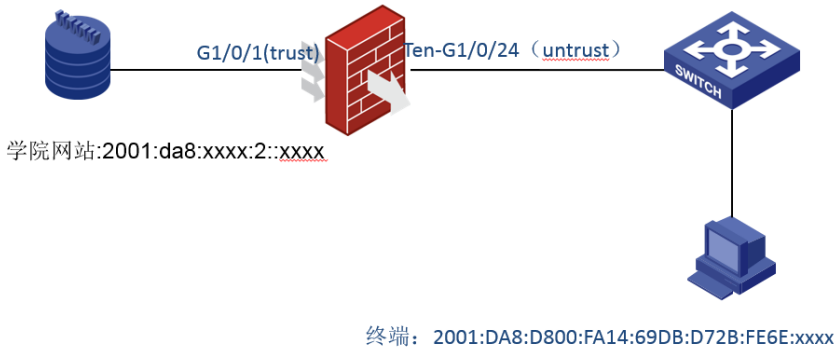
某局点SecPath F1000-AK1332(V7) 明细控制ipv6安全策略后，打不开网站的经验案例

SSL　域间策略/安全域　王燕　2021-01-27 发表

组网及说明

组网如下：



问题描述

FW透传模式，配置安全策略时，当只配置untrust-trust,控制端口80,443时，就出现时通时不通，大多数不通的情况，当再添加一条全放通的策略就访问没问题

终端的ipv6：2001:DA8:D800:FA14:69DB:D72B:FE6E:xxxx

池州学院ipv6: 2001:da8:xxxx:2::xxxx

过程分析

1、 查看设备配置信息，接口加安全域，正常放通80和443，以及pingv6

object-group ipv6 address 官网ipv6

10 network host address 2001:DA8:xxxx:2::xxxx

security-zone name Untrust

import interface Ten-GigabitEthernet1/0/24 vlan 201 to 202 301 3999 to 4001

security-zone name Trust

import interface GigabitEthernet1/0/1 vlan 201 to 202 301 3999 to 4001

security-policy ipv6

rule 3 name 外到内—ipv6官网放通80,443

action pass

logging enable

counting enable

source-zone Untrust

destination-zone Trust

destination-ip 官网ipv6

service http

service https

service pingv6

在策略最后添加下面这条就可以通：

rule 0 name 外到内放通ipv6

action pass

counting enable

source-zone Untrust

destination-zone Trust

2、

不通和通的时候抓包的acl:

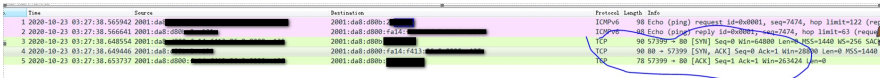
acl ipv6 advanced 3000

rule 10 permit ipv6 source 2001:DA8:D800:FA14:69DB:D72B:FE6E:XXXX/128 destination 2001:da8:xxxx:2::xxxx /128

rule 30 permit ipv6 source 2001:da8:xxxx:2::xxxx/128 destination 202001:DA8:D800:FA14:69DB:D72B:FE6E:XXXX /128

从抓包看，不通时候内外网都发出去了SYN包，服务器没有回；不通的时候，学院这边没有回syn-ack，三次捂手失败自然无法通信；

结合通的时候抓包排查，没有多余的服务器数据包发起两个地址的数据包；



3、查看会话学院网站没有回包：

<H3C>dis session table ipv6 source-ip 2001:DA8:D800:FA14:69DB:D72B:FE6E:XXXX destination-ip 2001:da8:xxxx:2::xxxx verbose

Slot 1:

Initiator:

Source IP/port: 2001:DA8:D800:FA14:69DB:D72B:FE6E:XXXX /59034

Destination IP/port: 2001:da8:xxxx:2::xxxx /443

VPN instance/VLAN ID/Inline ID: -/4001/-

Protocol: TCP(6)

Inbound interface: Ten-GigabitEthernet1/0/24

Source security zone: Untrust

Responder:

Source IP/port: 2001:da8:xxxx:2::xxxx /443

Destination IP/port: 2001:DA8:D800:FA14:69DB:D72B:FE6E:XXXX /59034

VPN instance/VLAN ID/Inline ID: -/4001/-

Protocol: TCP(6)

Inbound interface: GigabitEthernet1/0/1

Source security zone: Trust

State: TCP_SYN_SENT

Application: HTTPS

Rule ID: 3

Rule name: 外到内—ipv6官网放通80,443

Start time: 2020-10-28 20:01:23 TTL: 16s

Initiator->Responder: 1 packets 90 bytes

Responder->Initiator: 0 packets 0 bytes

解决方法

放通ND相关协议类型后解决：

Type = 133	RS （Router Solicitation，路由器请求）
Type = 134	RA （Router Advertisement，路由器公告）
Type = 135	NS （Neighbor Solicitation， 邻居请求）
Type = 136	NA （Neighbor Advertisement，邻居公告）
Type = 137	Redirect （ 重定向报文）

上述报文中，NS/NA 报文主要用于地址解析，RS/RA 报文主要用于无状态地址自动配置，Redirct 报文用于路由器重定向。