AFT IPv6 Internet访问IPv4内网服务器 不匹配V6侧的安全策略

AFT 李瑞 2021-12-15 发表

组网及说明

IPv6 Internet访问IPv4内网服务器，可参考官网配置手册的典配

问题描述

AFT IPv6 Internet访问IPv4内网服务器 不匹配V6侧的安全策略，AFT会话V6侧的策略显示“无”。

过程分析

AFT会话：

```
<H3C>dis aft session ipv4 ver
Slot 1:
Initiator:
  Source      IP/port: 172.20.50.1/2
  Destination IP/port: 172.20.50.4/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Local
Responder:
  Source      IP/port: 172.20.50.4/2
  Destination IP/port: 172.20.50.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: ipv4
State: ICMP_REPLY
Application: ICMP
Rule ID: 0
Rule name: minxi
Start time: 2021-12-09 17:53:57  TTL: 29s
Initiator->Responder:           4 packets       240 bytes
Responder->Initiator:           4 packets       240 bytes

Total sessions found: 1
<H3C>dis aft session ipv6 ver
Slot 1:
Initiator:
  Source      IP/port: 240E:xxx::1/1
  Destination IP/port: 240E:xxx::35/32768
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: ipv6
Responder:
  Source      IP/port: 240E:xxx::35/1
  Destination IP/port: 240E:xxx::1/33024
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Local
State: ICMPV6_REPLY
Application: ICMP
Rule ID: -/-/-
Rule name:
Start time: 2021-12-09 17:53:57  TTL: 20s
Initiator->Responder:           4 packets       320 bytes
Responder->Initiator:           4 packets       320 bytes

Total sessions found: 1
```

会话：

```
<H3C>dis session table ipv4 ver
Slot 1:
Total sessions found: 0
<H3C>dis session table ipv4 ver
Slot 1:
Initiator:
  Source      IP/port: 172.20.50.1/3
  Destination IP/port: 172.20.50.4/2048
  DS-lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Local
Responder:
  Source      IP/port: 172.20.50.4/3
  Destination IP/port: 172.20.50.1/0
  DS-lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: ipv4
State: ICMP_REPLY
Application: ICMP
Rule ID: 0
Rule name: minxi
Start time: 2021-12-09 17:57:24  TTL: 29s
Initiator->Responder:          2 packets        120 bytes
Responder->Initiator:          2 packets        120 bytes

Total sessions found: 1
<H3C>dis session table ipv6 ver
Slot 1:
Initiator:
  Source      IP/port: 240E:xxx::1/1
  Destination IP/port: 240E:xxx::35/32768
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: ipv6
Responder:
  Source      IP/port: 240E:xxx::35/1
  Destination IP/port: 240E:xxx::1/33024
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Local
State: ICMPV6_REPLY
Application: ICMP
Rule ID: -/-/-
Rule name:
Start time: 2021-12-09 17:57:24  TTL: 26s
Initiator->Responder:          4 packets        320 bytes
Responder->Initiator:          4 packets        320 bytes

Total sessions found: 1
```

解决方法

安全设备在运行AFT V6到V4的时候没有设置V6的安全策略检查业务点，也就是用户无法通过V6的安全策略去限制AFT的访问，可通过如下的方式进行限制：

1. V6接口上配置包过滤；

2. AFT策略里边配置明细ACL进行限制

```
#
acl ipv6 basic 2000
rule 0 permit     //这里可以放通明细的
#
aft v6tov4 source acl ipv6 number 2000 address-group 1
```