V7防火墙设备AFT功能实现IPv6网络访问IPv4 Internet

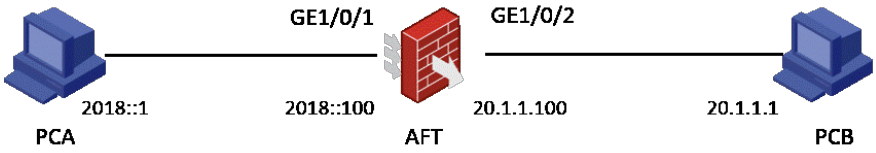
AFT 王奎银 2018-11-05 发表

组网及说明

一、AFT简介

IPv6的应用是个循序渐进的过程，在很长时间内，IPv4网络和IPv6网络会同时存在且需要相互通信。AFT（Address Family Translation，地址族转换）提供了IPv4和IPv6地址之间的相互转换功能。在IPv4网络完全过渡到IPv6网络之前，两个网络之间直接的通信可以通过AFT来实现。 对AFT地址转换方式的理解可以参考配置手册；

二、组网图



本案例要在防火墙上配置IPv6侧发起访问的AFT报文转换配置，使IPv6主机可以通过AFT转换后成IPv4地址访问IPv4 Internet。使用NAT64前缀与IPv4网络中的主机地址组合成为IPv6地址，此IPv6地址将与IPv4 Internet内的主机建立相应的映射关系，IPv6网络中的主机访问该IPv6地址即可实现对IPv4 Internet的访问。报文到达设备后，设备将根据NAT64前缀将该目的IPv6地址转换为对应的IPv4地址； 使用IPv6到IPv4源地址动态转换策略将IPv6网络到IPv4网络报文的源地址转换为IPv4地址10.1.1.1。

配置步骤

配置步骤及验证

1. 进行接口安全域配置，将G1/0/1加入untrust区域，G1/0/2加入trust区域，放通相应的安全策略。

1）配置ipv4侧的安全策略：

[H3C] security-policy ip
[H3C-security-policy-ip] rule 0 name trust-local
[H3C-security-policy-ip-0-trust-local] source-zone trust
[H3C-security-policy-ip-0-trust-local] source-zone local
[H3C-security-policy-ip-0-trust-local] destination-zone trust
[H3C-security-policy-ip-0-trust-local] destination-zone local
[H3C-security-policy-ip-0-trust-local] action pass
[H3C-security-policy-ip-0-trust-local] quit
[H3C-security-policy-ip] quit

2）配置ipv6侧的安全策略：

[H3C] security-policy ipv6
[H3C-security-policy-ipv6] rule 0 name untrust-local
[H3C-security-policy-ipv6-0-untrust-local] source-zone untrust
[H3C-security-policy-ipv6-0-untrust-local] source-zone local
[H3C-security-policy-ipv6-0-untrust-local] destination-zone untrust
[H3C-security-policy-ipv6-0-untrust-local] destination-zone local
[H3C-security-policy-ipv6-0-untrust-local] action pass
[H3C-security-policy-ipv6-0-untrust-local] quit
[H3C-security-policy-ipv6] quit

2. 配置地址组0包含IPv4地址10.1.1.1。

[H3C] aft address-group 0
[H3C-aft-address-group-0] address 10.1.1.1 10.1.1.1
[H3C-aft-address-group-0] quit

3. 配置IPv6 ACL 2000匹配源IPv6地址属于2018::/96网段的报文。

[H3C] acl ipv6 basic 2000
[H3C-acl-ipv6-basic-2000] rule permit source 2018:: 96
[H3C-acl-ipv6-basic-2000] rule deny
[H3C-acl-ipv6-basic-2000] quit

4. 配置IPv6到IPv4的源地址动态转换策略，将匹配ACL 2000的IPv6报文源地址转换为地址组0中的地址，即将2018::/96网段内主机所发送报文的源IPv6地址转换为IPv4地址10.1.1.1。

[H3C] aft v6tov4 source acl ipv6 number 2000 address-group 0

5. 配置NAT64前缀为2017::/96，报文的目的地址根据该NAT64前缀转换为IPv4地址。

[H3C] aft prefix-nat64 2017:: 96

6. 接口需要使能AFT功能

结果验证

1. 检查IPv6 Host与IPv4 Server的连通性。以IPv6 host A ping IPv4 server A为例：

C:\Users\H3C>ping 2017::20.1.1.1
正在 Ping 2017::20.1.1.1 具有 32 字节的数据:
来自2017::20.1.1.1 的回复: 时间=1ms
来自2017::20.1.1.1 的回复: 时间=1ms
来自2017::20.1.1.1 的回复: 时间=1ms
来自2017::20.1.1.1 的回复: 时间=1ms
2017::20.1.1.1 的 Ping 统计信息:
数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
最短 = 1ms，最长 = 1ms，平均 = 1ms
2. 通过查看AFT会话，可以看到创建了一个IPv6会话和IPv4会话，分别对应转换前和转换后的报文。
显示内容如下：

```
[H3C] display aft session ipv6 verbose
Slot 2:
Initiator:
  Source        IP/port: 2018::1/65512
  Destination IP/port: 2017::1401:101/21
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/0
  Source security zone: Untrust
Responder:
  Source IP/port: 2017::1401:101/21
  Destination IP/port: 2018::1/65512
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/2
  Source security zone: Local
State: TCP_ESTABLISHED
Application: FTP
Rule ID: -/-/-
Rule name:
Start time: 2018-09-01 08:24:18 TTL: 3597s
Initiator->Responder:          10 packets          636 bytes
Responder->Initiator:           9 packets          631 bytes
Total sessions found: 1
[H3C] display aft session ipv4 verbose
Slot 2:
Initiator:
  Source        IP/port: 10.1.1.1/1027
  Destination IP/port: 20.1.1.1/21
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/0
  Source security zone: Local
Responder:
   Source        IP/port: 20.1.1.1/21
   Destination IP/port: 10.1.1.1/1027
   DS-Lite tunnel peer: -
   VPN instance/VLAN ID/Inline ID: -/-/-
   Protocol: TCP(6)
   Inbound interface: GigabitEthernet2/0/2
   Source security zone: Trust
State: TCP_ESTABLISHED
Application: FTP
Rule ID: 0
Rule name: trust-local
Start time: 2018-09-01 08:24:18 TTL: 3586s
Initiator->Responder:          9 packets          396 bytes
Responder->Initiator:          8 packets          411 bytes
Total sessions found: 1
```

配置关键点

1. AFT相当于代理，需要放通local到对应域的安全策略，两个协议族之间没有直接三层转发；
2. NAT64前缀不能与设备上的接口地址同网段。