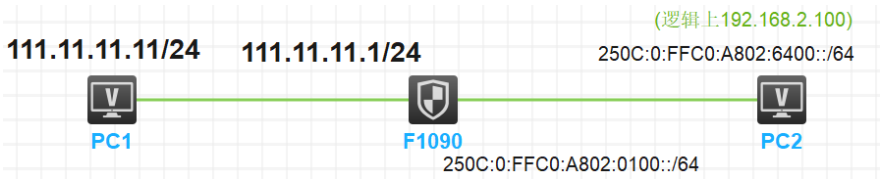
防火墙AFT实现IPv4和IPv6网络互访详细版

AFT 彭钦 2024-03-01 发表

组网及说明



需求：现场部署了IPV4和IPV6网络，需要让IPV4和IPV6网络互访。
实现方式：
***为IPv6网络分配一个IVI前缀（250C::）和IPv4网段（192.168.2.0/24），IPv6网络中所有IPv6主机的地址均配置为由IVI前缀和IPv4网段中地址组合而成的IPv6地址。
***为IPv4网络分配一个NAT64前缀（2024::），IPv4网络主动访问IPv6网络时，IPv4源地址使用NAT64前缀转换为IPv6地址；IPv6网络主动访问IPv4网络时，目的地址使用NAT64前缀和IPv4地址组合成的IPv6地址。

配置步骤

注意事项：

（1）IPv6侧分配IVI前缀以及使用的IPv4地址需要规划好；（PC2真实是IPv6地址，逻辑上给它规划IPv4地址，相当于IPv6地址=IVI前缀+IPv4地址）

（2）IPV4侧PC需要有路由到IPv6网络逻辑分配的IPv4网段（192.168.2.0/24），IPV6侧PC需要有路由到NAT64前缀（2024::）；

（3）PC防火墙需要关闭。

配置流程：
(1)配置ACL 2000用来过滤需要访问IPv6网络的用户，同时匹配该ACL 2000的报文的目的地址将会根据配置的IVI前缀转换为IPv6地址。

```
acl basic 2500

 rule 0 permit
```

(2)配置NAT64前缀为2024::/96，用于进行IPv4到IPv6的源地址转换和IPv6到IPv4的目的地址转换。

```
aft prefix-nat64 2024:: 96
```

(3) 配置IVI前缀，用于进行IPv6到IPv4源地址转换，且在IPv4到IPv6动态目的地址转换策略中引用该前缀。

```
aft prefix-ivi 250C::
```

(4)配置IPv4到IPv6动态目的地址转换策略，IPv4到IPv6报文的目的IPv4地址转换为IPv6地址。

```
aft v4tov6 destination acl number 2500 prefix-ivi 250C::
```

(5)接口开启aft

```
interface GigabitEthernet6/0

 port link-mode route

 aft enable

 ipv6 address 250C:0:FFC0:A802:100::/64
```

interface GigabitEthernet1/0

port link-mode route

ip address 111.11.11.1 255.255.255.0

aft enable

(5)IPv4终端新增路由

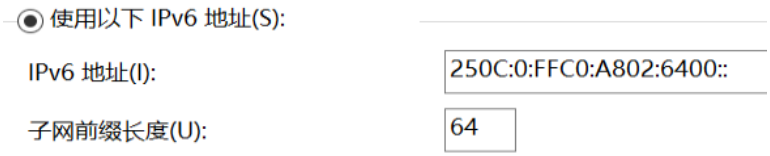
route add 192.168.2.0 mask 255.255.255.0 111.11.11.1

route print -4查看路由：

```
  172.31.0.255   255.255.255.255          在链路上          7.1.1.10     281
   192.168.2.0     255.255.255.0    111.11.11.1          7.1.1.10      26
     224.0.0.0       240.0.0.0          在链路上        127.0.0.1     331
```

(6)IPv6终端新增路由

电脑IPv6地址：



route -6 add 2024::/64 250C:0:FFC0:A802:0100::   ////首先要有ipv6邻居才能下发成功，否则报错

netsh interface ipv6 show neighbors /////查看电脑ipv6邻居缓存

route print -6查看路由：

```
 7     26 2024::/64                    250c:0:ffc0:a802:100::
 7    281 250c:0:ffc0:a802::/64        在链路上
```

防火墙ipv6邻居表：

```
RBM_P[H3C]display ipv6 neighbors all
Type: S-Static    D-Dynamic    O-Openflow     R-Rule    IS-Invalid static
IPv6 address              MAC address    VID  Interface           State T  Age
250C:0:FFC0:A802:6400::   000c-2976-3697 --   GE6/0               REACH D  17
```

测试：

（1）ipv6访问ipv4

```
C:\Users\Administrator>ping 2024::111.11.11.11

正在 Ping 2024::6f0b:b0b 具有 32 字节的数据:
来自 2024::6f0b:b0b 的回复: 时间<1ms
来自 2024::6f0b:b0b 的回复: 时间<1ms
来自 2024::6f0b:b0b 的回复: 时间<1ms
来自 2024::6f0b:b0b 的回复: 时间<1ms
```

```
RBM_P[H3C]display aft session ipv6 verbose
Slot 0:
Initiator:
  Source       IP/port: 250C:0:FFC0:A802:6400::/1
  Destination IP/port: 2024::6F0B:B0B/32768
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet6/0
  Source security zone: Trust
Responder:
  Source       IP/port: 2024::6F0B:B0B/1
  Destination IP/port: 250C:0:FFC0:A802:6400::/33024
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet1/0
  Source security zone: Local
State: ICMPV6_REPLY
Application: ICMP
Rule ID: -/-/-
Rule name:
Start time: 2024-03-01 00:32:53  TTL: 26s
Initiator->Responder:            4 packets         320 bytes
Responder->Initiator:            4 packets         320 bytes
```

```
RBM_P[H3C]display aft session ipv4 verbose
Slot 0:
Initiator:
  Source       IP/port: 192.168.2.100/1
  Destination IP/port: 111.11.11.11/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet6/0
  Source security zone: Local
Responder:
  Source       IP/port: 111.11.11.11/1
  Destination IP/port: 192.168.2.100/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0
  Source security zone: Trust
State: ICMP_REPLY
Application: ICMP
Rule ID: 0
Rule name: any
Start time: 2024-03-01 00:32:53  TTL: 21s
Initiator->Responder:            4 packets         240 bytes
Responder->Initiator:            4 packets         240 bytes
```

```
RBM_P<H3C>*Mar  1 00:36:41:477 2024 H3C AFT/7/COMMON:
 PACKET: (GigabitEthernet6/0) Protocol: ICMPv6
 250c:0:ffc0:a802:6400::/1 - 2024::6f0b:b0b/32768(VPN:0) ------>
 192.168.2.100/1 - 111.11.11.11/2048(VPN:0)
*Mar  1 00:36:41:477 2024 H3C FILTER/7/PACKET: The packet is permitted. Src-Zone=Local, Dst-Zone=Trust;If-In=GigabitEthernet6/0(97),
If-Out=GigabitEthernet1/0(17); Packet Info:Src-IP=192.168.2.100, Dst-IP=111.11.11.11, VPN-Instance=, Src-MacAddr=000c-2976-3697,Src-P
ort=8, Dst-Port=0, Protocol=ICMP(1), Application=ICMP(22742),Terminal=invalid(0), Url-category=invalid(65535), SecurityPolicy=any, Ru
le-ID=0.

*Mar  1 00:36:41:477 2024 H3C AFT/7/COMMON:
 PACKET: (GigabitEthernet1/0) Protocol: ICMP
 111.11.11.11/1 - 192.168.2.100/0(VPN:0) ------>
 2024::6f0b:b0b/1 - 250c:0:ffc0:a802:6400::/33024(VPN:0)
```

（2）ipv4访问ipv6

```
C:\Users\Administrator.WIN-EG71OU2NVNT>ping 192.168.2.100

正在 Ping 192.168.2.100 具有 32 字节的数据:
来自 192.168.2.100 的回复: 字节=32 时间<1ms TTL=127
来自 192.168.2.100 的回复: 字节=32 时间<1ms TTL=127
来自 192.168.2.100 的回复: 字节=32 时间<1ms TTL=127
来自 192.168.2.100 的回复: 字节=32 时间<1ms TTL=127
```

```
RBM_P<H3C>display aft session ipv4 verbose
Slot 0:
Initiator:
  Source       IP/port: 111.11.11.11/1
  Destination IP/port: 192.168.2.100/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0
  Source security zone: Trust
Responder:
  Source       IP/port: 192.168.2.100/1
  Destination IP/port: 111.11.11.11/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet6/0
  Source security zone: Local
State: ICMP_REPLY
Application: ICMP
Rule ID: -/-/-
Rule name:
Start time: 2024-03-01 00:45:37  TTL: 25s
Initiator->Responder:            1 packets         60 bytes
Responder->Initiator:            1 packets         60 bytes
```

```
RBM_P<H3C>display aft session ipv6 verbose
Slot 0:
Initiator:
  Source       IP/port: 2024::6F0B:B0B/1
  Destination IP/port: 250C:0:FFC0:A802:6400::/32768
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet1/0
  Source security zone: Local
Responder:
  Source       IP/port: 250C:0:FFC0:A802:6400::/1
  Destination IP/port: 2024::6F0B:B0B/33024
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet6/0
  Source security zone: Trust
State: ICMPV6_REPLY
Application: ICMP
Rule ID: 0
Rule name: 111
Start time: 2024-03-01 00:45:37  TTL: 20s
Initiator->Responder:            1 packets          80 bytes
Responder->Initiator:            1 packets          80 bytes
```

```
RBM_P<H3C>*Mar  1 00:45:37:195 2024 H3C AFT/7/COMMON:
 PACKET: (GigabitEthernet1/0) Protocol: ICMP
 111.11.11.11/1 - 192.168.2.100/2048(VPN:0) ------>
 2024::6f0b:b0b/1 - 250c:0:ffc0:a802:6400::/32768(VPN:0)
*Mar  1 00:45:37:195 2024 H3C FILTER/7/PACKET: The packet is permitted. Src-Zone=Local, Dst-Zone=Trust;If-In=GigabitEthernet1/0(17),
If-Out=GigabitEthernet6/0(97); Packet Info:Src-IP=2024::6f0b:b0b, Dst-IP=250c:0:ffc0:a802:6400::, VPN-Instance=, Src-MacAddr=000c-292
3-a0aa,Src-Port=128, Dst-Port=0, Protocol=IPv6-ICMP(58), Application=ICMP(22742),Terminal=invalid(0), Url-category=invalid(65535), Se
curityPolicy=111, Rule-ID=0.

*Mar  1 00:45:37:195 2024 H3C AFT/7/COMMON:
 PACKET: (GigabitEthernet6/0) Protocol: ICMPv6
 250c:0:ffc0:a802:6400::/1 - 2024::6f0b:b0b/33024(VPN:0) ------>
 192.168.2.100/1 - 111.11.11.11/0(VPN:0)
```

配置关键点

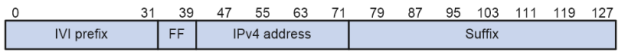
2.4.2 IVI前缀转换

在罗马数字中，“IV”代表4，“VI”代表6，因此“IVI”代表着IPv4/IPv6转换。IVI前缀转换技术是一种将IPv6报文转换为IPv4报文的技术，使得IPv6网络和IPv4网络能够互操作。

1. IVI前缀

IVI前缀是长度为32位的IPv6地址前缀，用于IPv4地址和IPv6地址之间的映射。IVI地址是IPv6主机实际使用的IPv6地址，这个IPv6地址中内嵌了一个IPv4地址，可以用于与IPv4主机通信。由IVI前缀构成的IVI地址格式如图6所示。其中Suffix固定为全0。

图5 IVI地址格式



2. IVI前缀转换原理

IVI前缀用于IPv6侧主动发起向IPv4侧访问的场景，AFT设备使用IVI前缀将报文的源IPv6地址转换为IPv4地址。例如，IVI前缀为2001:250::/32，嵌入到IVI前缀的IPv4地址为202.38.114.1，则IVI地址为2001:250:ff<202.38.114.1>，转换为正确的IPv6地址为：2001:250:ffca:2672:0100::。

IPv6侧主动发起对IPv4侧访问的场景中，源IPv6地址的转换过程如下：

(1) IPv6主机首先发起对IPv4主机的访问请求，源IPv6地址为IPv6主机的IVI地址。

(2) AFT设备收到IPv6主机发送的IPv6报文后，检查报文的目的IPv6地址是否能够匹配到IPv6目的地址转换配置（例如NAT64前缀转换配置）。

- 如果能匹配到IPv6目的地址转换配置，说明该报文需要进行AFT转换。接下来AFT设备执行步骤(3)。
- 如果匹配不到IPv6目的地址转换配置，则AFT设备进入报文转发流程，不再执行后续步骤。

(3) 转换报文目的地址。

AFT设备根据报文匹配到的IPv6目的地址转换配置将报文目的IPv6地址转换为IPv4地址。

(4) 根据目的地址预查路由。

AFT设备根据转换后的IPv4目的地址查找路由表，确定报文的出接口。

- 如果查找成功，则AFT设备执行步骤(5)。
- 如果查找失败，则丢弃报文。

(5) 转换报文源地址。

AFT设备将源IPv6地址去除前32位前缀和“FF”后，再取32位并转换为正确的IPv4地址，该地址即为转换后的源IPv4地址。

客户端和防火墙涉及的地址

250C:0:FFC0:A802:6400::　　192.168.2.100

250C:0:FFC0:A802:0100::　　192.168.2.1