基于安全策略的AFT功能典型配置

域间策略/安全域 卢鹏 2018-11-10 发表

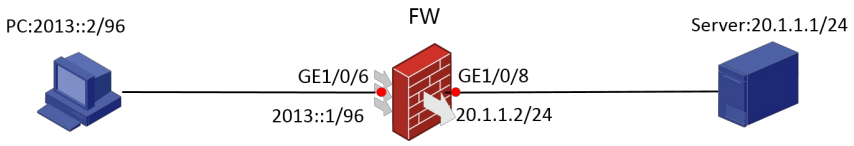
组网及说明

Internet已经升级到了IPv6，但是某公司内部网络仍然是IPv4网络。而该公司仍希望为IPv6 Internet内的用户提供FTP服务。该公司访问IPv6 Internet使用的IPv6地址为2012::1。

为满足上述要求，实现方式如下：

· 通过IPv4到IPv6源地址静态转换策略，为IPv4网络中的FTP服务器地址指定一个对应的IPv6地址，IPv6 Internet中的主机通过访问该IPv6地址可以访问IPv4网络中的FTP服务器。Device收到发往该IPv6地址的报文时将其目的地址转换为对应的IPv4地址。

· 通过IPv6到IPv4源地址动态转换策略，将IPv6 Internet发送过来的IPv6报文源地址转换为IPv4地址30.1.1.1和30.1.1.2。



配置步骤

按照组网图配置各接口的IP地址。

[Device] interface gigabitethernet 1/0/6

[Device-GigabitEthernet1/0/6] ipv6 address 2013::1 96

[Device-GigabitEthernet1/0/6] quit

[Device] interface gigabitethernet 1/0/8

[Device-GigabitEthernet1/0/8] ip address 20.1.1.2 255.255.255.0

[Device-GigabitEthernet1/0/8] quit

配置IPv4到IPv6源地址静态转换策略，手动指定IPv4与IPv6地址一一对应的转换关系，此策略可将报文的目的地址转换为对应的IPv4地址。

system-view

[Device] aft v4tov6 source 20.1.1.1 2012::1

配置地址组0包含2个IPv4地址：30.1.1.1和30.1.1.2。

[Device] aft address-group 0

[Device-aft-address-group-0] address 30.1.1.1 30.1.1.2

[Device-aft-address-group-0] quit

配置IPv6 ACL 2000，匹配IPv6网络到IPv4网络的报文。此处允许所有IPv6网络内主机访问IPv4 FTP Server。

[Device] acl ipv6 basic 2000

[Device-acl-ipv6-basic-2000] rule permit

[Device-acl-ipv6-basic-2000] quit

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IPv4地址30.1.1.2或30.1.1.3。

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

在IPv6侧接口GigabitEthernet1/0/6开启AFT。

[Device] interface gigabitethernet 1/0/6

[Device-GigabitEthernet1/0/6] aft enable

[Device-GigabitEthernet1/0/6] quit

在IPv4侧接口GigabitEthernet1/0/8开启AFT。

[Device] interface gigabitethernet 1/0/8

[Device-GigabitEthernet1/0/8] aft enable

[Device-GigabitEthernet1/0/8] quit

配置地址对象组

#

object-group ip address fwq 0

network host address 20.1.1.1

#

object-group ip address local

0 network range 30.1.1.1 30.1.1.2

#

object-group ipv6 address dip

0 network host address 2012::1

#

```
object-group ipv6 address sip
 0 network host address 2013::2
 #将接口加入安全域
 #
security-zone name Trust
 import interface GigabitEthernet1/0/8
 #
security-zone name Untrust
 import interface GigabitEthernet1/0/6
 #配置安全策略，注意安全策略要配置ip安全策略和ipv6的安全策略，放通的安全域不是untrust到trust
，而分别是untrust到local和local到trust。
 #
security-policy ip
 rule 0 name 0
 action pass
 source-zone local
 destination-zone trust
 source-ip local
 destination-ip fwq
#
security-policy ipv6
 rule 0 name 0
 action pass
 source-zone untrust
 destination-zone local
 source-ip sip
 destination-ip dip
 # 以上配置完成后，检查IPv6 host与IPv4 FTP server的连通性。以IPv6 host A ping IPv4 FTP server
为例：
 D:\>ping 2012::1
 Pinging 2012::1 with 32 bytes of data:
 Reply from 2012::1: time=3ms
 Reply from 2012::1: time=3ms
 Reply from 2012::1: time=3ms
 Reply from 2012::1: time=3ms
# 通过查看会话，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。从会话
中可以看出所属的安全域信息。
 [Device]display session table ipv4 verbose
Slot 1:
Initiator:
 Source IP/port: 30.1.1.1/1
 Destination IP/port: 20.1.1.1/2048
 DS-Lite tunnel peer: -
 VPN instance/VLAN ID/Inline ID: -/-/-
 Protocol: ICMP(1)
 Inbound interface: GigabitEthernet1/0/6
 Source security zone: Local
Responder:
 Source IP/port: 20.1.1.1/1
 Destination IP/port: 30.1.1.1/0
 DS-Lite tunnel peer: -
 VPN instance/VLAN ID/Inline ID: -/-/-
 Protocol: ICMP(1)
 Inbound interface: GigabitEthernet1/0/8
 Source security zone: Trust
State: ICMP_REPLY
Application: ICMP
Start time: 2018-11-06 15:02:36 TTL: 14s
Initiator->Responder:          5 packets          420 bytes
Responder->Initiator:          5 packets          420 bytes
 Total sessions found: 1
[Device]display session table ipv6 verbose
Slot 1:
Initiator: Source IP/port: 2013::2/395
```

Destination IP/port: 2012::1/32768
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: IPV6-ICMP(58)
Inbound interface: GigabitEthernet1/0/6
Source security zone: Untrust
Responder:
Source IP/port: 2012::1/395
Destination IP/port: 2013::2/33024
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: IPV6-ICMP(58)
Inbound interface: GigabitEthernet1/0/8
Source security zone: Local
State: ICMPV6_REPLY
Application: ICMP
Start time: 2018-11-06 15:02:36 TTL: 7s
Initiator->Responder: 5 packets 520 bytes
Responder->Initiator: 5 packets 520 bytes
Total sessions found: 1

配置关键点

附件下载： 配置及会话信息.txt