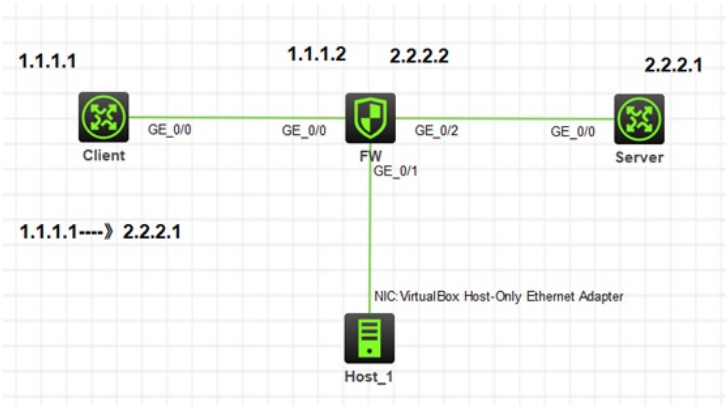
# 从协议说起（1）——ICMP（Ping）

会话 胡伟 2020-03-06 发表

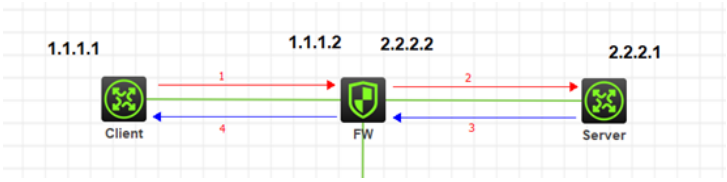
## 组网及说明

使用H3C设备搭建如下环境：
Client端IP地址为1.1.1.1，默认路由下一条指向FW端IP地址1.1.1.2；
Server端IP地址为2.2.2.1，默认路由下一条指向FW端IP地址2.2.2.2；
FW侧将对应接口加入相应安全域，安全策略默认放通。




## 配置步骤

Client向Server Ping一个报文。
ping -c 1 2.2.2.1
对于FW来说，一次Ping报文的交互，FW上会有四次报文交互过程，如下：



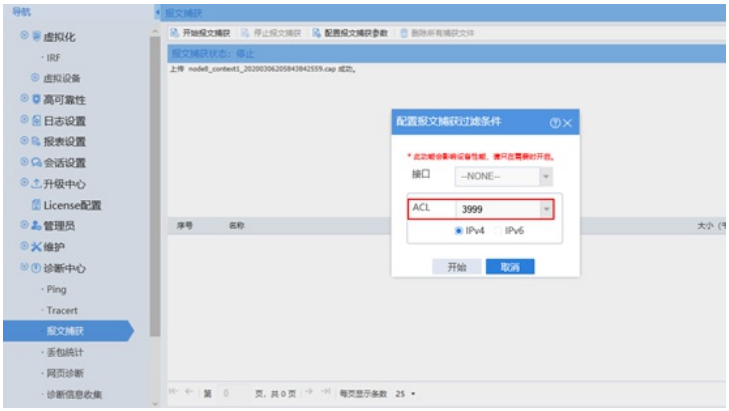

1， FW接收Client发出的请求报文：源IP-1.1.1.1，目的IP-2.2.2.1；
2， FW向Server转发的请求报文：源IP-1.1.1.1，目的IP-2.2.2.1；
3， FW接收Server发出的响应报文：源IP-2.2.2.1，目的IP-1.1.1.1；
4， FW向Client转发的响应报文：源IP-1.1.1.1，目的IP-2.2.2.1。
所以在FW上，可以写定一个ACL进行抓包，如下：

```
acl advanced 3999
 rule 0 permit icmp source 1.1.1.1 0 destination 2.2.2.1 0
 rule 5 permit icmp source 2.2.2.1 0 destination 1.1.1.1 0
```

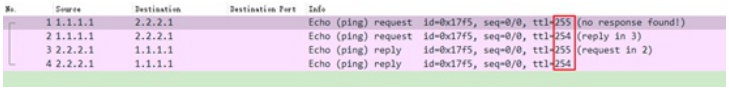
因为1/2，3/4对应的源IP和目的IP是相同的，所以ACL规则可以合并。但是如果防火墙上配置了NAT功能，比如IP地址为2.2.2.2的接口配置了nat outbound，将Client的源地址1.1.1.1改变为2.2.2.2，那ACL必须如下修改，把每一条流对应清楚，否则抓取不了完整的交互报文。

```
acl advanced 3999
 rule 0 permit icmp source 1.1.1.1 0 destination 2.2.2.1 0
 rule 5 permit icmp source 2.2.2.2 0 destination 2.2.2.1 0
 rule 10 permit icmp source 2.2.2.1 0 destination 2.2.2.2 0
 rule 15 permit icmp source 2.2.2.1 0 destination 1.1.1.1 0
```

Web界面选中指定的ACL编号3999，开始抓包：



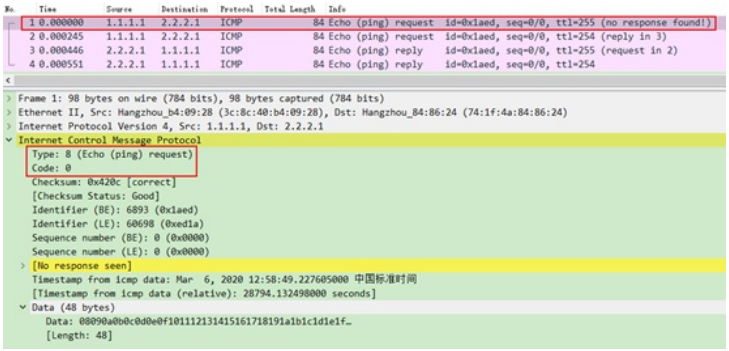

下载抓包文件，用Wireshark工具打开如下可以看到报文在防火墙上的交互过程：




## 配置关键点

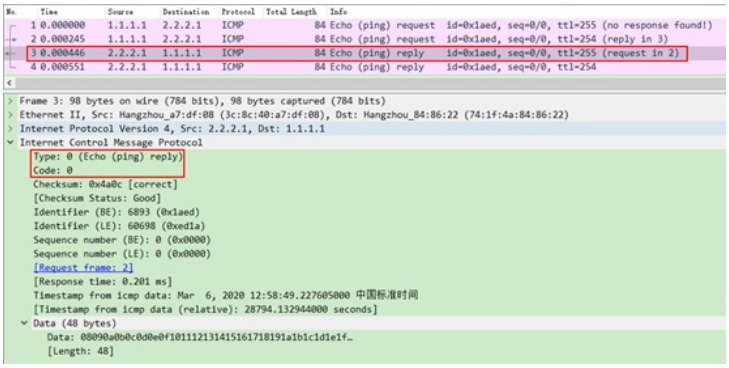
Ping是ICMP协议的一个应用，使用ICMP协议的Echo报文进行交互，发送一个Echo-Request报文，就响应一个Echo-Reply报文。

- Echo-Request报文格式如下：




其ICMP Type=8，Code=0，同时携带报文标识Identifier(BE)=6893，Identifier(LE)=60698。

- Echo-Reply报文格式如下：




其ICMP Type=0，Code=0，同时携带报文标识Identifier(BE)=6893，Identifier(LE)=60698。

防火墙需要根据业务报文的五元组（**源IP地址，源端口，目的IP地址，目的端口，协议号**）创建对应会话。但是ICMP协议是网络层协议，并没有对应的端口号，所以根据 ICMP报文中的Identifier字段10进制作为源端口， 将Type字段和Code字段的值做与运算，作为目的端口。 例如：Type=8，Code=0；则目标端口=1000 0000 0000 & 0 = 2048。上述抓包在防火墙上的会话显示如下：

Initiator:

Source IP/port: 1.1.1.1/**6893**

Destination IP/port: 2.2.2.1/**2048**

DS-Lite tunnel peer: -

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

Protocol: ICMP(1)

Inbound interface: GigabitEthernet1/0/0

Source security zone: 1

Responder:

Source IP/port: 2.2.2.1/**6893**

Destination IP/port: 1.1.1.1/**0**
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: ICMP(1)
Inbound interface: GigabitEthernet1/0/2
Source security zone: 2
State: ICMP_REPLY
Application: ICMP
Rule ID: 0
Rule name: 0
Start time: 2020-03-06 20:58:43 TTL: 15s
Initiator->Responder: 1 packets 84 bytes
Responder->Initiator: 1 packets 84 bytes

防火墙会话要求ICMP带端口的原因：因为ICMP需要做状态检测，所有需要五元组，其时ICMP端口对业务来说无实际意义。

附：ICMP类型字段(Type)以及代码字段(Code)对应表

| 类型TYPE | 代码CODE | 用途|描述 Description | 查询类Query | 差错类Error |
|---|---|---|---|---|
| 0 | 0 | Echo Reply——回显应答（Ping应答） | x | |
| 3 | 0 | Network Unreachable——网络不可达 | | x |
| 3 | 1 | Host Unreachable——主机不可达 | | x |
| 3 | 2 | Protocol Unreachable——协议不可达 | | x |
| 3 | 3 | Port Unreachable——端口不可达 | | x |
| 3 | 4 | Fragmentation needed but no frag. bit set——需要进行分片但设置不分片比特 | | x |
| 3 | 5 | Source routing failed——源站选路失败 | | x |
| 3 | 6 | Destination network unknown——目的网络未知 | | x |
| 3 | 7 | Destination host unknown——目的主机未知 | | x |
| 3 | 8 | Source host isolated (obsolete)——源主机被隔离（作废不用） | | x |
| 3 | 9 | Destination network administratively prohibited——目的网络被强制禁止 | | x |
| 3 | 10 | Destination host administratively prohibited——目的主机被强制禁止 | | x |
| 3 | 11 | Network unreachable for TOS——由于服务类型TOS，网络不可达 | | x |
| 3 | 12 | Host unreachable for TOS——由于服务类型TOS，主机不可达 | | x |
| 3 | 13 | Communication administratively prohibited by filtering——由于过滤，通信被强制禁止 | | x |
| 3 | 14 | Host precedence violation——主机越权 | | x |
| 3 | 15 | Precedence cutoff in effect——优先中止生效 | | x |
| 4 | 0 | Source quench——源端被关闭（基本流控制） | | |
| 5 | 0 | Redirect for network——对网络重定向 | | |
| 5 | 1 | Redirect for host——对主机重定向 | | |
| 5 | 2 | Redirect for TOS and network——对服务类型和网络重定向 | | |
| 5 | 3 | Redirect for TOS and host——对服务类型和主机重定向 | | |
| 8 | 0 | Echo request——回显请求（Ping请求） | x | |
| 9 | 0 | Router advertisement——路由器通告 | | |
| 10 | 0 | Route solicitation——路由器请求 | | |
| 11 | 0 | TTL equals 0 during transit——传输期间生存时间为0 | | x |
| 11 | 1 | TTL equals 0 during reassembly——在数据报组装期间生存时间为0 | | x |
| 12 | 0 | IP header bad (catchall error)——坏的IP首部（包括各种差错） | | x |
| 12 | 1 | Required options missing——缺少必需的选项 | | x |
| 13 | 0 | Timestamp request (obsolete)——时间戳请求（作废不用） | x | |
| 14 | | Timestamp reply (obsolete)——时间戳应答（作废不用） | x | |
| 15 | 0 | Information request (obsolete)——信息请求（作废不用） | x | |
| 16 | 0 | Information reply (obsolete)——信息应答（作废不用） | x | |
| 17 | 0 | Address mask request——地址掩码请求 | x | |

| | | | | |
|---|---|---|---|---|
| 18 | 0 | Address mask reply——地址掩码应答 | | |

**附件下载：**ICMP-Echo报文.rar