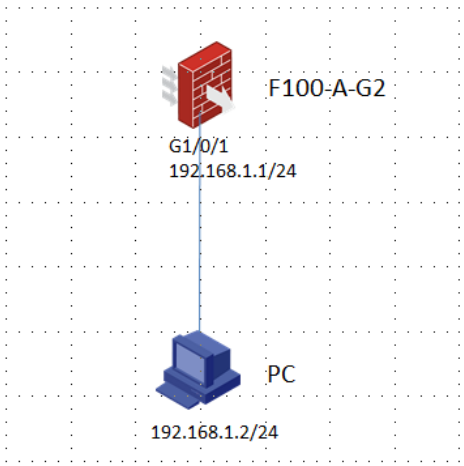
PC直连V7防火墙无法ping通的排查经验

域间策略/安全域　王林　2016-04-29 发表

组网



需要PC和F100能够相互ping通，可以通过PC去管理F100，目前PC和F100互ping，无法ping通对方。

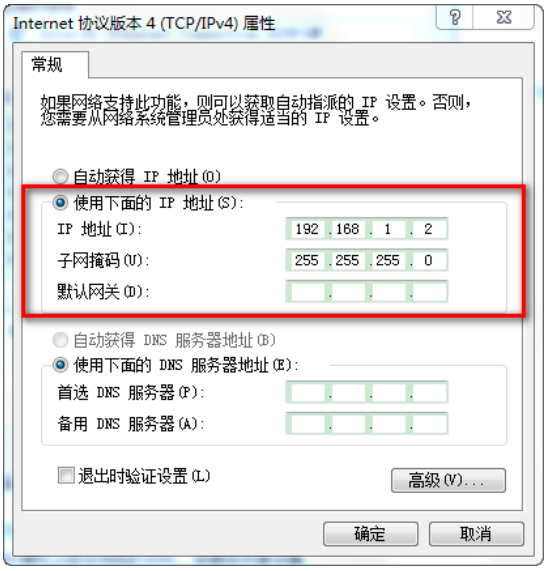
首先检查配置，确保配置正确，下面就配置一一进行排查

#配置防火墙G1/0/1接口和PC的ip地址

interface GigabitEthernet1/0/1

port link-mode route

ip address 192.168.1.1 255.255.255.0



由于V7防火墙默认各个接口不加入任何安全域，因此需要将G1/0/1接口加入到某一个安全域中，本案例将G1/0/1加入到Trust域中。

把接口G1/0/1加入到trust域中

[H3C] security-zone name trust

[H3C-security-zone-Trust] import interface GigabitEthernet 1/0/1

在这种组网情况下，由于G1/0/1接口属于trust域，因此该接口下面连接的PC属于trust域，

此时当PC去ping防火墙接口G1/0/1的ip地址时，实际产生的是trust域到local域的ip数据流， 因此需要配置trustl到local的域间策略 ，并放通对应的ip数据流。

#定义允许的ip流量，这里采用对象组策略，允许所有流量通过

[H3C] object-policy ip test

[H3C-object-policy-ip-1]rule 1 pass

创建源安全域trust到目的安全域local的安全域间实例，并在该域间实例上应用包过滤策略，允许源trust到目的local的ip数据通过

[H3C]zone-pair security source trust destination local

[H3C-zone-pair-security-Local-Trust] object-policy apply ip test

通过以上配置，测试发现PC可以ping通F100

```
C:\Users\w11327>ping 192.168.1.1

正在 Ping 192.168.1.1 具有 32 字节的数据:
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=255

192.168.1.1 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 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\w11327>
        半:
```

但F100无法ping通PC

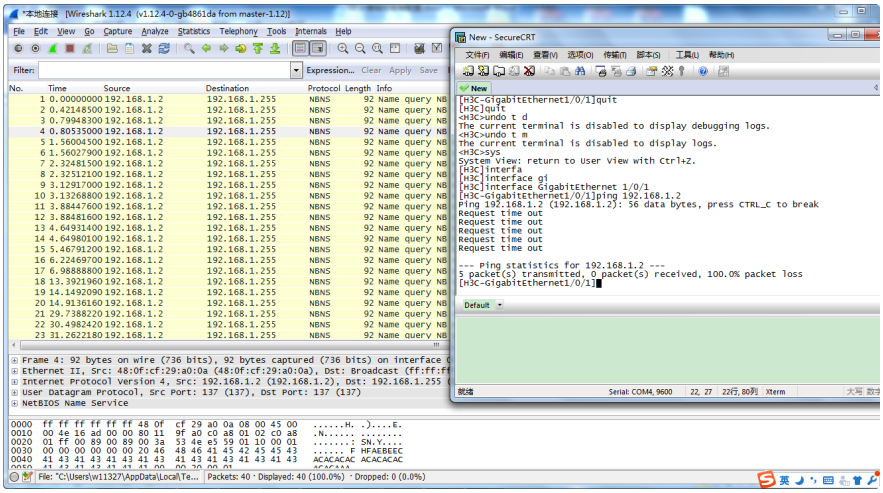
```
[H3C]
[H3C]
[H3C]
[H3C]
[H3C]
[H3C]
[H3C]ping 192.168.1.2
Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping statistics for 192.168.1.2 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
[H3C]%Dec 18 19:34:47:939 2015 H3C PING/6/PING_STATISTICS: -Context=1; Ping stat
istics for 192.168.1.2: 5 packet(s) transmitted, 0 packet(s) received, 100.0% pa
cket loss.

[H3C]
[H3C]
```

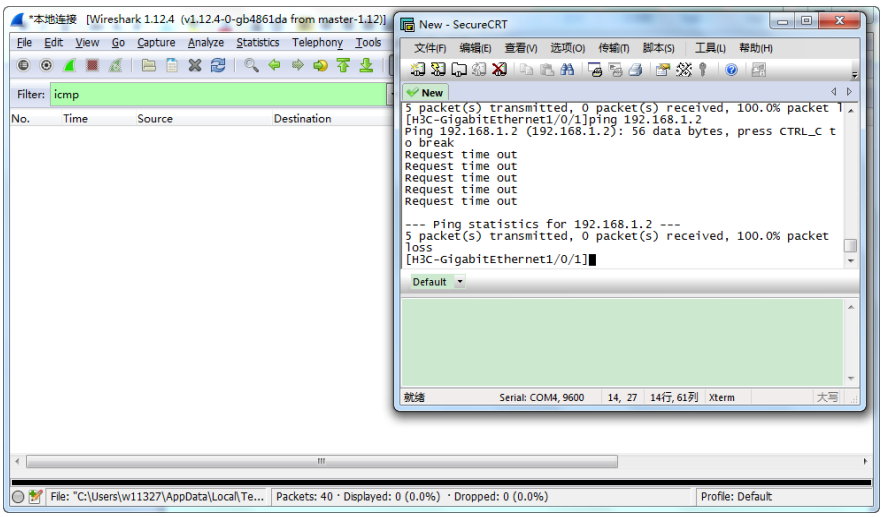
出现了F100无法ping通PC，两者单通的现象，导致该问题的原因有两个：

1.ping数据包没有出G1/0/1接口

2.PC收到F100的ping包，但是没回复

为了定位问题，在PC上抓包，发现PC没有收到来自F100的ping报文

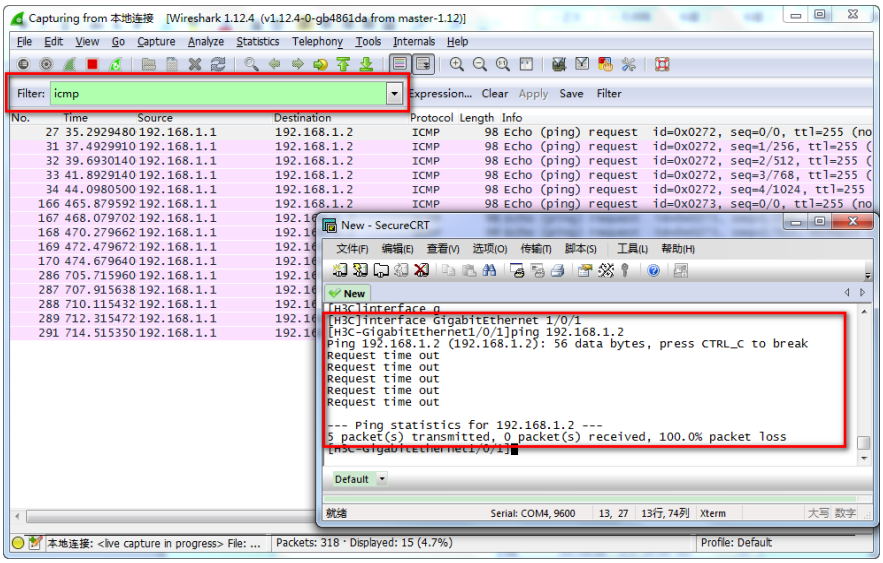




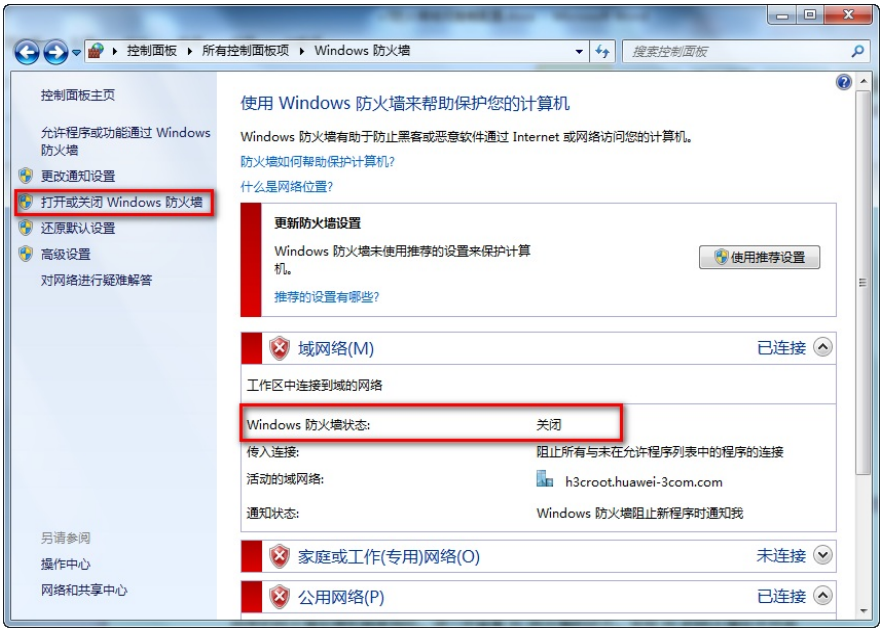
通过抓包分析，可以认为F100根本就没有ping报文从G1/0/1接口发出。

现在基本可以判断是域间策略的问题，通过查阅资料，发现V7防火墙默认所有域间策略都是deny的，

也就是说 local域到trust域是deny的，local到trust的ip数据流量没有放通。
因此需要配置local到trust的域间策略为permit
创建源安全域local到目的安全域trust的安全域间实例，并在该域间实例上应用包过滤策略，允许源local到目的trust的数据流通过
[H3C]zone-pair security source local destination trust
[H3C-zone-pair-security-Local-Trust] object-policy apply ip test
至此域间策略都配置完成了，通过ping测试，发现F100到PC还是无法ping通，通过PC抓包分析，发现PC能够收到F100的Echo request报文，但PC却没有回复，如下图：



PC没有回复对方的ping报文，那么PC应该是将报文丢弃掉了，这和windows自带的防火墙处理机制很相似，进一步查看PC防火墙的状态，发现PC的防火墙处于开启状态，通过关闭PC的windows防火墙。



此时，F100可以ping通PC

```
[H3C]dis zoe
[H3C]dis zone
[H3C]dis zone-pair se
[H3C]dis zone-pair security
Source zone                 Destination zone
Local                       Trust
Trust                       Local
[H3C]ping 192.168.1.2
Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.1.2: icmp_seq=0 ttl=128 time=0.647 ms
56 bytes from 192.168.1.2: icmp_seq=1 ttl=128 time=0.505 ms
56 bytes from 192.168.1.2: icmp_seq=2 ttl=128 time=0.573 ms
56 bytes from 192.168.1.2: icmp_seq=3 ttl=128 time=0.603 ms
56 bytes from 192.168.1.2: icmp_seq=4 ttl=128 time=0.601 ms

--- Ping statistics for 192.168.1.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.505/0.586/0.647/0.047 ms
[H3C]%Dec 18 18:08:01:459 2015 H3C PING/6/PING_STATISTICS: -Context=1; Ping statistics for 192.168.1.2: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/std-dev = 0.505/0.586/0.647/0.047 ms.
```

当然PC到F100也可以ping通，自此，PC和F100之间全部连通。

防火墙域间策略配置正确，并且关闭PC的防火墙功能。

1.V7防火墙默认所有接口都不在任何安全域，包括管理口G1/0/0
2.V7防火墙中，默认的安全域策略全部是deny的
3.V5防火墙中，默认local域的优先级较trust域的优先级高，在开启了interzone policy default by-priority时，默认local到trust是放通的，而在V7防火墙中，不存在域优先级的概念，而且各个域间默认deny。
4.在该测试中，PC到F100的流量属于trust到local，F100到PC的流量属于local到trust，要学会善于分析域间流量
5.在有PC参与的ping连通性测试中，尤其是PC是win7操作系统时，需要关闭PC的防火墙，以免PC自带的防火墙对测试造成干扰。
6.学会用抓包分析问题。