# 一、 开始

包过滤策略和对象策略是过去使用的域间策略，它基于全局进行配置，基于域间实例进行应用。新 Web 使用的安全策略已经脱离了域间实例的概念，是根据报文的属性信息对报文进行转发控制和 DPI 的防控策略。NGFW 防火墙新 Web 版本新增安全策略（security-policy），以安全策略配置取代对象策略（object-policy）实现防火墙访问控制的功能。盒式防火墙又称集中式转发防火墙，安全策略故障的排查思路如下：首先判断防火墙当前使用版本是否是新安全策略，如果不是安全策略版本，本文档不适用，建议升级到新版本。其次，需要判断配置中是否存在域间策略，安全策略的优先级要高于域间策略，一旦开启安全策略功能可能导致域间策略不生效，一般建议统一配置，将域间策略转换为安全策略后再进行后续操作。在使用并配置安全策略的前提下，第一步先判断是否存在会话表项，如果会话存在，则需要判断是否接受到双向报文；如果没有会话表项，需要检查报文是否上到防火墙，或者安全域以及安全策略是否配置正确。在接下来的正文中将以 IPv4 协议为例进行详细说明。

# 二、流程图相关操作说明：

## 1、当前版本是否支持安全策略

本文档针对安全策略故障进行排查，所以首先应确认当前版本是否支持安全策略。安全策略随 Web 界面更新换代产生，而我们所说的防火墙新 Web 版本， 从版本型号上来说是内部版本号 D022 以后的版本。那么如何查看内部版本号呢？普通的用户视图和系统视图下无法查看，必须在 probe 视图下查看。在系统视图下输入 probe 命令进入 probe 视图，通过命令可以查看对应内部版本号。

命令：*display system internal version*

例如：通过命令查看，防火墙 F5020 的内部版本号为 D022SP16，属于新 Web 版本分支，支持安全策略。

```
<H3C>system-view
System View: return to User View with Ctrl+Z.
[H3C]probe
[H3C-probe]display system internal version
H3C SecPath F5020 V900R003B02D622SP16
Comware V700R001B64D022SP16
```

## 2、升级版本

如果当前版本不支持安全策略，又需要在 Web 界面上配置安全策略，或者使用多域到多域的策略（目前只有安全策略支持多域到多域的访问控制策略），建议将设备版本升级到官网最新。登录 H3C 官网 http://www.h3c.com/cn/ ，在“首页>产品支持与服务>文档与软件>软件下载>安全”路径下选择 Comware V7 系列，根据盒式防火墙的型号选择进入对应的软件下载页面。


官网上软件下载页面一般有 2 个或者 2 个以上的版本文件，不容易分辨。如表 1 所示，这里给出了常用的几款盒式防火墙的内部版本号对应列表，比如 F1000 系列防火墙 R9323（外部版本号）以后的版本都是 D022 版本分支，F5000 系列防火墙 R9320（外部版本号）以后的版本都是 D022 版本分支。

表 1 内部版本号对应列表举例

| 型号 | D012 | D022 |
|---|---|---|
| H3C SecPath F1020 F1030 F1070 | R9313P20 | R9323P14 |
| H3C SecPath F5040 F5020 F5010 | R9310P20 | R9320P15 |
| | 域间策略 | 安全策略（新 web） |

V7 NGFW 盒式防火墙的版本升级可以使用两种方式，Web 方式和命令行方式，旧版本升级 D022 版本推荐使用命令行方式。从 H3C 官网获取软件版本 ipe 文件，通过 FTP/TFTP 将软件版本文件上传到本地，用 boot-loader 命令来指定设备下次启动时使用的版本文件。其中，main 参数表示指定该软件包为主用启动软件包，并将该软件包的名称添加到主用启动软件包列表。主用启动软件包用于下一次设备启动。

命令：*boot-loader file file-name { all | slot } main*

例如：通过 boot-loader 命令将 R9320P15 版本设置为下一次防火墙 F5020 启动的主用启动软件版本，配置完成后使用 reboot 命令重启设备，完成重启后即完成升级，可以通过 display version 命令查看升级是否成功。

```
<H3C>boot-loader file cfa0:/SECPATH5010F_5020F_5040F-CMW710-R9320P15.ipe all
main
Verifying the file cfa0:/SECPATH5010F_5020F_5040F-CMW710-R9320P15.ipe on slot
1.........Done.
H3C SecPath F5020 images in IPE:
  f5000fw-cmw710-boot-R9320P15.bin
  f5000fw-cmw710-system-R9320P15.bin
This command will set the main startup software images. Please do not reboot
any MPU during the upgrade. Continue? [Y/N]:y
```

**3、是否存在域间策略**

域间策略是在域间实例下发的进行流量识别和控制的策略，V7 防火墙上配置域间策略有两种方式，一种是基于 ACL 的包过滤策略，一种是基于对象组的对象策略。

```
[H3C] zone-pair security source trust destination untrust
[H3C-zone-pair-security-Trust-Untrust] packet-filter 3999
```

**包过滤策略**

```
[H3C] zone-pair security source trust destination untrust
[H3C-zone-pair-security-Trust-Untrust] object-policy apply ip internet
```

**对象策略**

值得注意的是，安全策略功能与对象策略功能在设备上不能同时使用，首次开启安全策略功能后，对象策略功能立即失效。而当安全策略与包过滤策略同时配置时，因为安全策略对报文的处理在包过滤之前，报文与安全策略规则匹配成功后，不再进行包过滤处理，所以应合理配置安全策略和包过滤策略，否则可能会导致配置的包过滤策略不生效。此外，在 D022 新版本中 Web 界面配置仅支持安全策略的配置，也就是说命令行中配置不论是配置对象策略还是包过滤策略，Web 界面都不会显示策略。除此之外要注意命令行配置和 Web 界面配置不能混配。因此，如果当前配置中存在域间策略，而后续要求 Web 界面显示安全策略配置，或者习惯性使用 Web 界面进行配置，强烈建议将域间策略转换为安全策略。

**4、将域间策略转换为安全策略**

配置安全策略前，请首先确认是否需要将设备上已存在的对象策略转换为安全策略，若需

要，请务必先将对象策略转换为安全策略。需要说明的是，目前仅支持将对象策略转换为安全策略，不支持包过滤策略的转换，如要做包过滤策略的转换，需先将包过滤策略修改为对象策略，再按照以下步骤进行转换。

转换步骤如下：

1) 升级到 D022 版本；

2) 通过 security-policy switch-from object-policy 命令将旧的配置文件 startup.cfg 转换为新的 security.cfg，如图所示；

```
[H3C]security-policy switch-from object-policy startup.cfg security.cfg
Configuration switching begins...

Object policies in the specified configuration file have been switched to security policies.
Reboot the device to make the configuration take effect. Reboot now? [Y/N]:
```

上图显示配置转换成功。转换成功后，新生成的配置文件自动被指定为下次启动文件，用户可直接输入 Y 进行设备重启，如果想验证下次启动配置可输入 N，再通过如下命令查看下次启动文件是否正确。

```
<H3C>display startup
MainBoard:
 Current startup saved-configuration file: flash:/startup.cfg
 Next main startup saved-configuration file: flash:/security.cfg
 Next backup startup saved-configuration file: NULL
<H3C>
```

可以看到当前启动文件是之前的 startup.cfg，但是下次启动文件已经变成转换成后的 security.cfg 文件。以上就完成了对象策略到安全策略的配置转换。

3) 重启设备，完成重启后设备运行新的配置文件 security.cfg；

4) 开启安全策略功能。

默认情况下安全策略不生效，升级到 D022 版本后设备中缺省存在 security-policy disable 命令。转换完成后将这条命令 undo 掉后安全策略才会生效。

```
[H3C] undo security-policy disable
This conmmand will enable security-policy and disable object-policy. Do it?
[Y/N]:Y
```

转换前后的命令对比：

转换前使用的是域间策略 zone-pair，配置如下：

```
#
zone-pair security source Any destination Any
 packet-filter 3000
#
zone-pair security source Trust destination Local
 object-policy apply ip Trust-Local
#
zone-pair security source Trust destination Untrust
 object-policy apply ip Trust-Untrust
#
```

转换后配置文件中没有对象策略，而是新的安全策略。

如下图所示，可以看到对象策略 object-policy 全部转换为了安全策略，对应的 zone-pair 下不再引用对象策略，而包过滤策略 packet-filter 没有进行转换。

```
security-policy ip
 rule 0 name Trust-Local-0
  action pass
  counting enable
  source-zone Trust
  destination-zone Local
  source-ip 172.31.0.0
 rule 1 name Trust-Untrust-1
  action pass
  counting enable
  source-zone Trust
  destination-zone Untrust
  source-ip 172.31.0.0
 rule 2 name Trust-Untrust-2
  source-zone Trust
  destination-zone Untrust
  source-ip 192.168.1.11
```

```
#
zone-pair security source Any destination Any
 packet-filter 3000
#
zone-pair security source Trust destination Local
#
zone-pair security source Trust destination Untrust
#
```

**5、是否存在会话表项**

V7 NGFW 盒式防火墙属于典型的状态检测防火墙，其会话表项是设备对网络中各条业务流执行状态检测的重要依据。当防火墙从某个业务端口接收到报文后，首先与当前会话表进行匹配。如果报文命中某条会话表项，即可继续执行转发流程；如果无法命中任何会话表项，则该报文后续将转交给安全策略模块进行策略规则匹配。若匹配结果为允许，防火墙将创建一条新的会话表项并继续正常转发处理该报文；若匹配结果为拒绝，则将直接丢弃该报文，也不会创建会话表项。

因此排查安全策略故障的第一步就是查看是否存在会话表项，如果存在会话表项，说明已通过安全策略检测，可以正常转发，需要排查其它原因；如果不存在会话表项，那么报文可能没有上到防火墙上或者报文被安全策略阻断。

为了更精确地快速地查找会话表项，V7 NGFW 盒式防火墙支持基于会话发起方源/目的 IP 地址、源/目的端口号、协议、VPN 实例等参数执行筛选查找。注意执行命令必须在会话表

项老化之前，以 UDP、ICMP 协议会话为例，如果防火墙没有接收到后续命中该会话的业务报文，则会话表项将于 60 秒后老化删除，该时间参数支持用户自行修改。若查询命令执行后显示会话表项数为 0，则说明当前不存在符合查询条件的会话表项。

命令： *display session table ipv4 source-ip x.x.x.x destination-ip x.x.x.x verbose*

例如： 从网关设备 Ping 防火墙设备，执行 5 次 Ping 操作，会话发起方源目的地址分别为 172.31.0.1 和 172.31.0.22。因此在会话表中可以查询到如下表项，会话发起方 IP 为 172.31.0.1，会话响应方 IP 为 172.31.0.22，发起方位于 Management 区域，响应方位于 Local 区域，发起方发送了 5 个报文，防火墙从 Reth1 端口接收，响应方回复了 5 个报文，防火墙从本地发送。若防火墙没有继续收到命中该会话表项的后续报文，会话将在 25 秒后老化删除。

```
[H3C]display session table ipv4 source-ip 172.31.0.1 destination-ip 172.31.0.22
verbose
Slot 1:
Total sessions found: 0

[H3C]display session table ipv4 source-ip 172.31.0.1 destination-ip 172.31.0.22
verbose
Slot 1:
Initiator:
  Source      IP/port: 172.31.0.1/28
  Destination IP/port: 172.31.0.22/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: Reth1
  Source security zone: Management
Responder:
  Source      IP/port: 172.31.0.22/28
  Destination IP/port: 172.31.0.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: InLoopBack0
  Source security zone: Local
State: ICMP_REPLY
Application: ICMP
Start time: 2018-05-13 17:11:33  TTL: 25s
Initiator->Responder:            5 packets        420 bytes
Responder->Initiator:            5 packets        420 bytes

Total sessions found: 1
```

需要注意的是，查看会话表项的命令一定要加 verbose 参数，不加 verbose 参数打印的会话表项信息较少，比如无法查看报文出入接口、没有报文统计计数等。此外，会话表项中的报文计数功能需要开启 session statistics enable（会话统计功能），否则会话表项的计数为 0。

所以如果看到会话表项中的报文计数为 0 不代表报文未送达防火墙，存在会话表项已经表明报文到达防火墙并通过了安全策略检查。

```
[H3C]display session table ipv4 source-ip 172.31.0.1 destination-ip 172.31.0.22
Slot 1:
Initiator:
  Source      IP/port: 172.31.0.1/29
  Destination IP/port: 172.31.0.22/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: Reth1
  Source security zone: Management

Total sessions found: 1
```

### 6、是否接收到双向报文

不同的数据流具有不同的会话状态和会话创建机制，防火墙收到第一个数据包的时候开始创建会话，然后根据后续报文进行会话状态的切换，最终达到一个稳定的状态。对于 TCP 数据流，防火墙收到第一个 SYN 报文后开始创建会话，三次握手完成后会话进入一个稳定的状态，然后就可以传输数据了，当通信双方关闭 TCP 连接时，防火墙也开始拆除会话。对于 ICMP、UDP 以及其它应用的数据流，防火墙收到发起方的第一个报文时开始建立会话，收到响应方回应的报文后会话进入稳定的状态。另外，防火墙的会话有一个老化时间，收到报文后会对老化时间进行更新，当老化时间减小到 0 还没有收到报文，防火墙就将该会话拆除。

报文交互过程与会话表项的创建关系如图 1 所示，防火墙接收到 Host 发送的第一个报文，报文通过防火墙的安全策略后建立会话表项，Server 回应的反向报文命中会话表项被转发回发起方 Host。因此，如果防火墙中存在会话表项但是业务仍然不通，就需要排查防火墙是否接收到了双向报文，更准确的说，防火墙是否接收到了反向报文。

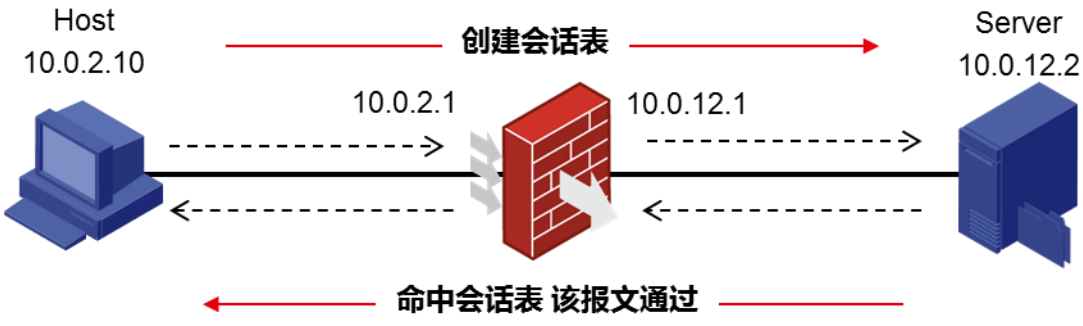



图 1 会话表项创建过程

针对这种情况，可以通过会话表项里的报文统计功能帮助排查。在全局下开启软件快速转发的会话统计功能（缺省情况下，软件快速转发的会话统计功能的开启状态与设备的型号有关）， 查看会话表项中报文计数，如果发起方到响应方（Initiator->Responder）有报文计数，而响应方到发起方（Responder->Initiator）没有报文计数，那么很可能报文没收到回包。

命令：*session statistics enable*

例如：从网关设备 10.0.2.10 经由防火墙 ping ACG 设备 10.0.12.2 不通，查看会话表项的报文计数，发起方到响应方（Initiator->Responder）有 3 个报文，而响应方到发起方（Responder->Initiator）没有报文计数。

```
[H3C]session statistics enable
[H3C]display session table ipv4 source-ip 10.0.2.10 destination-ip 10.0.12.2
verbose
Slot 1:
Initiator:
  Source      IP/port: 10.0.2.10/46
  Destination IP/port: 10.0.12.2/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Trust
Responder:
  Source      IP/port: 10.0.12.2/46
  Destination IP/port: 10.0.2.10/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/10
  Source security zone: Untrust
State: ICMP_REQUEST
Application: ICMP
Start time: 2018-05-14 10:13:11  TTL: 59s
Initiator->Responder:            3 packets        252 bytes
Responder->Initiator:            0 packets          0 bytes

Total sessions found: 1
```

为了进一步确认是否没有收到反向报文，可以通过 debugging 命令输出信息来排查回程报

文是否上到防火墙。debugging 命令回显信息很多，一般要求后面写明细 ACL 匹配报文（写明源目的地址和协议）。

命令：*debugging ip packet acl*

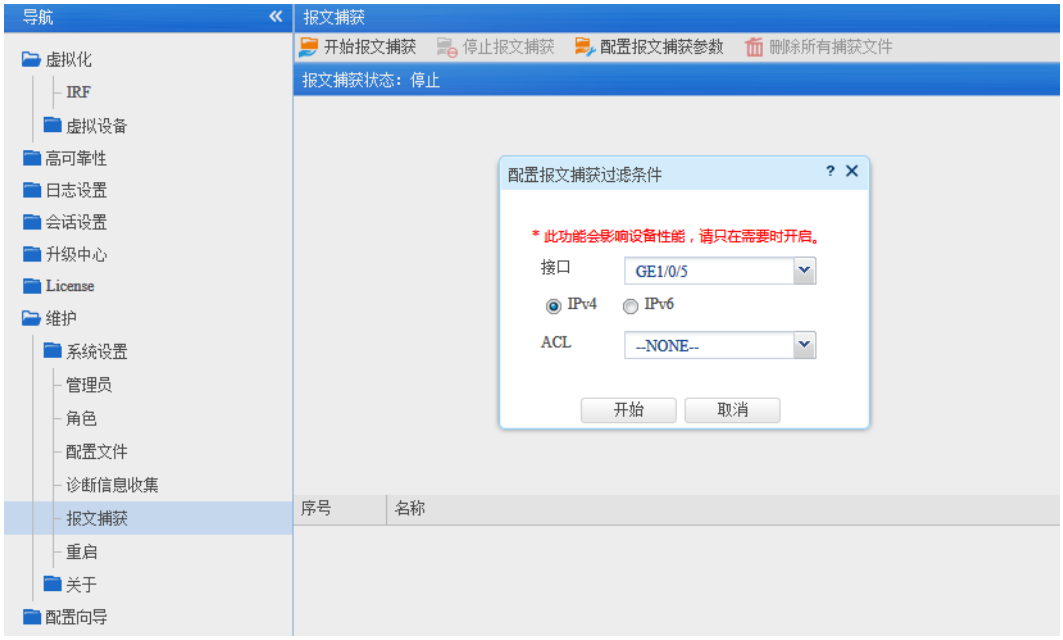
```
[H3C]acl advanced 3000
[H3C-acl-ipv4-adv-3000] rule 0 permit icmp source 10.0.12.2 0 destination
10.0.2.10 0
The rule was edited successfully.
<H3C>debugging ip packet acl 3000
This command is CPU intensive and might affect ongoing services. Are you sure
you want to continue? [Y/N]:y
<H3C>terminal monitor
The current terminal is enabled to display logs.
<H3C>terminal debugging
The current terminal is enabled to display debugging logs.
```

例如：正常情况下，如果有匹配 ACL 的 debug 信息说明回程报文到达了防火墙，debug 信息表明了防火墙从 G1/0/10 收到回包并从 G1/0/2 转发出去，报文源地址 10.0.12.2，目的地址 10.0.2.10，符合实际回包情况。

```
<H3C>*May 14 11:20:59:620 2018 H3C IPFW/7/IPFW_PACKET: -Context=1;
Receiving, interface = GigabitEthernet1/0/10
version = 4, headlen = 20, tos = 0
pktlen = 84, pktid = 8373, offset = 0, ttl = 64, protocol = 1
checksum = 14313, s = 10.0.12.2, d = 10.0.2.10
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Receiving IP packet from interface GigabitEthernet1/0/10.
Payload: ICMP
  type = 0, code = 0, checksum = 0x7ea1.


*May 14 11:20:59:620 2018 H3C IPFW/7/IPFW_PACKET: -Context=1;
Sending, interface = GigabitEthernet1/0/2
version = 4, headlen = 20, tos = 0
pktlen = 84, pktid = 8373, offset = 0, ttl = 63, protocol = 1
checksum = 14569, s = 10.0.12.2, d = 10.0.2.10
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Sending IP packet received from interface GigabitEthernet1/0/10 at
interface GigabitEthernet1/0/2.
Payload: ICMP
  type = 0, code = 0, checksum = 0x7ea1.
```

如果没有匹配 ACL 的 debug 信息，则回程报文没到防火墙，需排查其他设备的问题。

除此之外，D022 分支的 Web 版本支持抓包功能，同样也可以通过抓取接口报文，确认是否接收到双向报文。在 Web 管理平台中，在“系统>维护>报文捕获”下点击[开始报文捕获]配置报文捕获过滤条件，选择接口，业务流量较大的时候建议匹配 ACL。




配置完报文捕获过滤条件，点击[开始]。完成抓包后点击[停止报文捕获]，然后可以下载抓包文件到本地。使用 Wireshark 软件打开抓包文件，具体判断方式不再赘述。



## 7、检查其他设备

如果防火墙没有接收到业务报文，则应检查其他设备原因，通常是由于组网、路由规划、其他设备故障等因素导致报文没有到达或绕过防火墙。针对此类问题，建议从发起方开始逐跳排查，逐步确认发起方至响应方报文的具体转发路径、是否被中途丢弃等。如果是由于非 H3C 品牌设备引起的故障，建议尽快与对应的服务提供商取得联系，协助排查处理。

## 8、报文是否上到设备

如果防火墙上没有查到会话表项，那么有两种可能性，一种就是报文没有上到设备，另一种就是被安全策略阻断了。报文是否上到防火墙可以通过 debugging 命令输出信息来排查。Debugging 回显信息很多，一般要求后面写明细 ACL 匹配报文（写明源目的地址和协议）。

命令：*debugging ip packet acl*

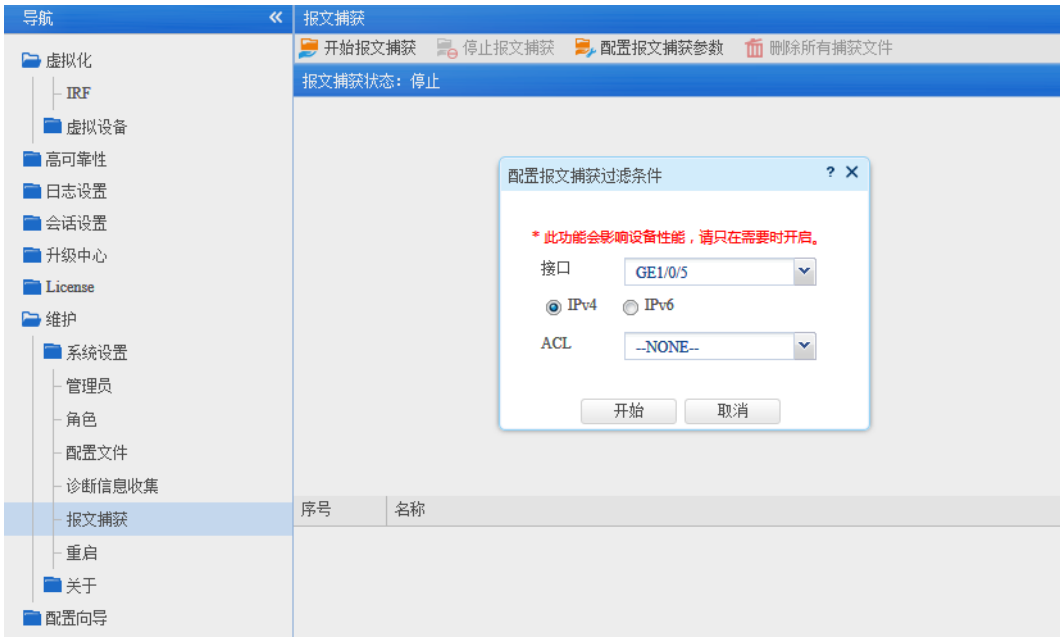
```
[H3C]acl advanced 3000
[H3C-acl-ipv4-adv-3000] rule 0 permit icmp source 10.0.2.10 0 destination
10.0.12.2 0
The rule was edited successfully.
<H3C>debugging ip packet acl 3000
This command is CPU intensive and might affect ongoing services. Are you sure
you want to continue? [Y/N]:y
<H3C>terminal monitor
The current terminal is enabled to display logs.
<H3C>terminal debugging
The current terminal is enabled to display debugging logs.
```

例如：正常情况下，Host 10.0.2.10 发送给 Server 10.0.12.2 的报文到达了防火墙，debugging ip packet 有匹配 ACL 的 debug 信息，debug 信息表明了防火墙从 G1/0/2 收到 icmp 报文并从 G1/0/10 转发出去，报文源地址 10.0.2.10，目的地址 10.0.12.2。

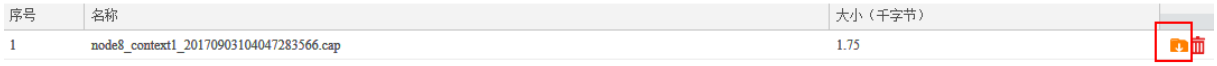
```
<H3C>*May 14 18:40:51:732 2018 H3C IPFW/7/IPFW_PACKET: -Context=1;
Receiving, interface = GigabitEthernet1/0/2
version = 4, headlen = 20, tos = 0
pktlen = 84, pktid = 30028, offset = 0, ttl = 255, protocol = 1
checksum = 9297, s = 10.0.2.10, d = 10.0.12.2
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Receiving IP packet from interface GigabitEthernet1/0/2.
Payload: ICMP
  type = 8, code = 0, checksum = 0xc4e2.

*May 14 18:40:51:732 2018 H3C IPFW/7/IPFW_PACKET: -Context=1;
Sending, interface = GigabitEthernet1/0/10
version = 4, headlen = 20, tos = 0
pktlen = 84, pktid = 30028, offset = 0, ttl = 254, protocol = 1
checksum = 9553, s = 10.0.2.10, d = 10.0.12.2
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Sending IP packet received from interface GigabitEthernet1/0/2 at
interface GigabitEthernet1/0/10.
Payload: ICMP
  type = 8, code = 0, checksum = 0xc4e2.
```

如果没有匹配 ACL 的 debug 信息，则报文没上到防火墙，需排查其他设备的问题。

除此之外，D022 分支的 Web 版本支持抓包功能，同样也可以通过抓取接口报文，确认防火墙是否接收到报文。在 Web 管理平台中，在“系统>维护>报文捕获”下点击[开始报文捕获]配置报文捕获过滤条件，选择接口，业务流量较大的时候建议匹配 ACL。




配置完报文捕获过滤条件，点击[开始]。完成抓包后点击[停止报文捕获]，然后可以下载抓包文件到本地。使用 Wireshark 软件打开抓包文件，具体判断方式不再赘述。


## 9、报文是否被安全策略阻断

V7 NGFW 防火墙默认全禁止，即空配情况下业务不通。（除 Management 区域以外，缺省情况下 Management 区域和 Local 区域互通）缺省情况下安全策略中不存在规则，设备接收到的所有非 Management 安全域和 Local 安全域之间的报文将均会被丢弃。安全域是防火

墙区别于交换机路由器的基本特征之一，接口只有加入了业务安全区域后才会转发数据。安全域可以用于管理防火墙设备上安全需求相同的多个接口，网络管理员将安全需求相同的接口划分到相同的安全域。配置安全策略后两个安全域才能互相访问。因此，为使设备能够正常处理报文，必须将接口加入安全域并在安全策略中配置相应的安全策略规则。

如果通过 debugging 或者抓包确认报文已送达防火墙，接下来就要确认是否是安全策略阻断了报文。通过 debugging security-policy 可以查看报文是否被安全策略阻断，阻断的原因是什么。debugging 命令回显信息很多，一般要求后面写明细 ACL 匹配报文（写明源目的地址和协议）。

命令：*debugging security-policy packet ip acl*

```
[H3C]acl advanced 3000
[H3C-acl-ipv4-adv-3000] rule 0 permit icmp source 10.0.2.10 0 destination
10.0.12.2 0
The rule was edited successfully.
<H3C>debugging security-policy packet ip acl 3000
This command is CPU intensive and might affect ongoing services. Are you sure
you want to continue? [Y/N]:Y
<H3C>terminal monitor
The current terminal is enabled to display logs.
<H3C>terminal debugging
The current terminal is enabled to display debugging logs.
```

例如：debugging security-policy 正常情况下的回显信息如下图所示，根据信息可知，报文通过安全策略检查，源安全域为 Trust 域，目的安全域为 Untrust 域，此外还包括报文的源目的地址、源目的端口号、协议五元组信息，命中的安全策略规则 ID 为 0。

<H3C>*May 14 19:28:39:791 2018 H3C FILTER/7/PACKET: -Context=1; The packet is permitted. Src-Zone=Trust, Dst-Zone=Untrust;If-In=GigabitEthernet1/0/2(3), If-Out=GigabitEthernet1/0/10(11); Packet Info:Src-IP=10.0.2.10, Dst-IP=10.0.12.2, VPN-Instance=,Src-Port=8, Dst-Port=0, Protocol=ICMP(1), Application=ICMP(22742), SecurityPolicy=1, Rule-ID=0.

图 2 业务正常时 debugging 回显

以下举例说明三种报文被安全策略阻断时的 debugging 信息：

debugging 回显信息中出现“The packet was dropped by ASPF for nonexistent zone pair.”说明接口没有加入安全域。

①没有安全域

<H3C>*May 14 19:25:23:003 2018 H3C ASPF/7/PACKET: -Context=1; The packet was dropped by ASPF for nonexistent zone pair. Src-Zone=-, Dst-Zone=Untrust;If-In=GigabitEthernet1/0/2(3), If-Out=GigabitEthernet1/0/10(11); Packet Info:Src-IP=10.0.2.10, Dst-IP=10.0.12.2, VPN-Instance=none,Src-Port=57, Dst-Port=2048. Protocol=ICMP(1).

debugging 回显信息中出现“The packet is denied.”说明报文被安全策略阻断，而“Rule-ID=none.”说明没有命中任何安全策略，因此是由于没有配置安全策略造成的故障。

②没有配置安全策略

<H3C>*May 14 19:31:50:811 2018 H3C FILTER/7/PACKET: -Context=1; The packet is denied. Src-Zone=Trust, Dst-Zone=Untrust;If-In=GigabitEthernet1/0/2(3), If-Out=GigabitEthernet1/0/10(11); Packet Info:Src-IP=10.0.2.10, Dst-IP=10.0.12.2, VPN-Instance=,Src-Port=8, Dst-Port=0, Protocol=ICMP(1), Application=ICMP(22742), ACL=none, Rule-ID=none.

debugging 回显信息中出现“The packet is denied.”说明报文被安全策略阻断，而“Rule-ID=2.”说明是规则 ID 为 2 的安全策略 deny 了报文，因此是由于安全策略配置了阻断造成的故障。

③安全策略配置了阻断

<H3C>*May 14 19:36:24:860 2018 H3C FILTER/7/PACKET: -Context=1; The packet is denied. Src-Zone=Trust, Dst-Zone=Untrust;If-In=GigabitEthernet1/0/2(3), If-Out=GigabitEthernet1/0/10(11); Packet Info:Src-IP=10.0.2.10, Dst-IP=10.0.12.2, VPN-Instance=,Src-Port=8, Dst-Port=0, Protocol=ICMP(1), Application=ICMP(22742), SecurityPolicy=1, Rule-ID=2.

## 10、检查安全域

V7 NGFW 盒式防火墙默认安全域有 Trust、DMZ、Untrust 和 Management，G1/0/0 默认加入 Management 区域。此外，设备上所有接口都默认属于 Local 区域，不需要将接口加入 Local 域。V7 NGFW 盒式防火墙默认所有端口（包括二三层物理端口、二三聚合端口、隧道口、VLAN 虚接口、虚接口模板、冗余口、主控板管理口等）均无安全区域属性，必须由管理员

手工配置后才能转发业务报文。需要说明的是，将端口加入某个安全区域，不是指防火墙端口本身属于这个区域，而是意味着这个端口所连接的网络处于该安全区域内。

命令：*display current-configuration configuration seczone*

例如：在 CLI 管理界面中，通过命令检查设备当前安全区域配置情况。防火墙与 Host 相连的接口 G1/0/2 加入了 Trust 区域，防火墙与 Sever 相连的接口 G1/0/10 加入了 Untrust 区域。

```
<H3C>display current-configuration configuration seczone
#
security-zone name Local
#
security-zone name Trust
 import interface GigabitEthernet1/0/2
 import interface GigabitEthernet1/0/5
 import interface GigabitEthernet2/0/5
 import interface GigabitEthernet2/0/11
 import interface Reth10
#
security-zone name DMZ
#
security-zone name Untrust
 import interface GigabitEthernet1/0/1
 import interface GigabitEthernet1/0/8
 import interface GigabitEthernet1/0/10
 import interface GigabitEthernet1/0/11
 import interface GigabitEthernet2/0/10
#
security-zone name Management
 import interface Reth1
#
return
```

当然，也可以通过 Web 管理界面检查安全域配置情况，通过导航栏“网络>接口>安全域”进入安全域配置界面，同样可以看到，防火墙与 Host 相连的接口 G1/0/2 加入了 Trust 区域，防火墙与 Sever 相连的接口 G1/0/10 加入了 Untrust 区域。


## 11、检查安全策略

安全策略对报文的控制是通过安全策略规则实现的，规则中可以设置匹配报文的过滤条件，处理报文的动作和对于报文内容进行深度检测等功能。每条规则中均可以配置多种过滤条件，具体包括：源安全域、目的安全域、源 IP 地址、目的 IP 地址、用户、用户组、应用、应用组、服务和 VPN。每种过滤条件中（除 VPN 外）均可以配置多个匹配项，比如源安全域过滤条件中可以指定多个源安全域等。安全策略的配置检查步骤如下：

1） 检查安全策略规则配置

当安全策略规则中未配置任何过滤条件时，则该规则将匹配所有报文。

检查安全策略的具体规则配置是否准确。安全策略规则可以指定引用的对象组包括：源/目的 IP 地址对象组、服务对象组、VRF 等。在检查规则配置时，要仔细核对规则中所引用的对象组名称是否已经定义，如果引用的对象组不存在，则此条规则不会匹配任意报文，若规则中不指定对象组，则该条规则可以匹配所有报文。如果希望设备能够输出安全策略日志，需注意在规则配置中开启记录日志功能。安全策略中可配置多条规则， 对业务报文进行规则匹配时按显示的从上至下顺序依次匹配，与规则 ID 号无关。此外安全策略支持加速特性，当安全策略中包含数量较多的规则时，使能加速特性可以在一定程度上缓解因规则数量多所造成的转发性能以及新建连接性能的下降。

命令：*display current-configuration configuration security-policy-ip*

例如：在 CLI 管理界面中检查安全策略及规则配置。可以看到设备上配置的安全策略包含两条规则，第一条为允许从源安全域 Untrust 到目的安全域 Trust，符合源地址对象组 10.0.12.0 和目的地址对象组 10.0.2.0 的业务报文通过，第二条为允许从源安全域 Trust 到目的安全域 Untrust 的所有报文通过，并开启记录日志功能。

```
<H3C>display current-configuration configuration security-policy-ip
#
security-policy ip
 rule 1 name 2
  action pass
  counting enable
  time-range workday
  source-zone Untrust
  destination-zone Trust
  source-ip 10.0.12.0
  destination-ip 10.0.2.0
 rule 2 name 1
  action pass
  logging enable
  source-zone Trust
  destination-zone Untrust
#
return
```

同时在 Web 管理界面上也可以进行安全策略的查看，通过导航栏“策略>安全策略”进入安全策略配置界面，界面展示了所有策略的配置情况，与 CLI 命令行显示一致。需要说明的是，命令行只有配置 security-policy Web 界面上才会显示安全策略，如果命令行里延用旧的域间策略，Web 界面将不显示任何策略配置情况。


2) 检查对象组配置

对象组分为地址对象组和服务对象组两类。对象组可以被安全策略所引用，作为报文匹配的条件。地址对象组主要与 IP 地址或主机名称（需要开启设备的 DNS 解析服务）绑定，用于匹配报文中的 IP 地址。服务对象组主要与协议类型以及协议的特性绑定（协议特性如 TCP 或 UDP 的源端口/目的端口、ICMP 协议的消息类型/消息码等），用于匹配 IP 报文的四层信息。系统已经预定义了部分常用服务对象组，同时支持用户自定义服务对象组。在问题排查时，要仔细核对对象组中的 IP 地址、四层端口号信息等配置是否准确，是否正

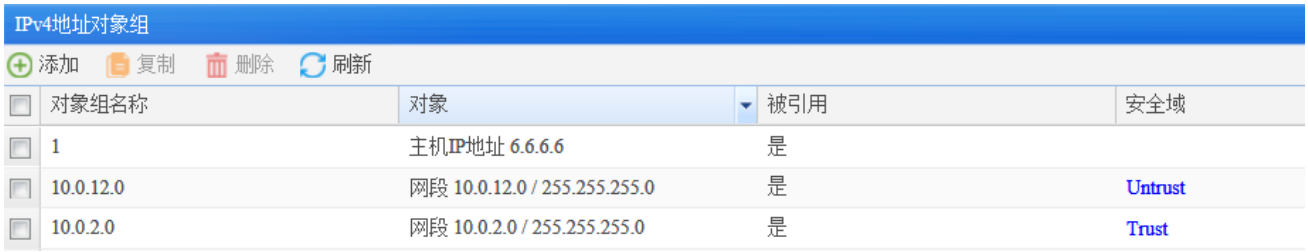
确地被对象策略所引用，对象组间的引用关系是否合理等。

命令： *display current-configuration configuration obj-grp*

例如：在 CLI 管理界面中检查对象组配置。

```
<H3C>display current-configuration configuration obj-grp
#
object-group ip address 1
 0 network host address 6.6.6.6
#
object-group ip address 10.0.12.0
 security-zone Untrust
 0 network subnet 10.0.12.0 255.255.255.0
#
object-group ip address 10.0.2.0
 security-zone Trust
 0 network subnet 10.0.2.0 255.255.255.0
#
```

同时在 Web 管理界面上也可以进行对象组的查看，通过导航栏“对象>对象组>IPv4 地址对象组”进入配置界面，IPv4 地址对象组的配置与 CLI 命令行显示一致。




3） 检查时间段配置

当问题排查涉及时间段特性时，应首先查看防火墙当前系统时间、时区配置是否正确。若不正确应立即调整，建议启用 NTP 服务为防火墙实时同步系统时钟。若系统时间正常，需检查时间对象配置是否正确。

注意，当一个时间段配置中包含有多个周期时间段和绝对时间段时，系统将先分别取各周期时间段的并集和各绝对时间段的并集，再取这两个并集的交集作为该时间段最终生效的时间范围。如果当前系统时间正处于该时间对象生效的时间范围内，在用户界面上将有“Active”提示信息。

命令： *display clock*

例如：检查当前系统时间是否正常。

```
<H3C>display clock
11:43:16 Hangzhou Tue 05/15/2018
Time Zone : Hangzhou add 08:00:00
```

若系统时间不正确应立即调整。

命令：*clock datetime*

例如：通过命令调整系统时间至 2018 年 5 月 15 日 12 时。

```
<H3C>clock datetime 12:00 2018/5/15
```

命令： *display time-range all*

例如：在 CLI 管理界面中检查时间对象当前是否生效。“Active”代表此刻该时间段有效，“Inactive”代表此刻该时间段无效。

```
<H3C>display time-range all
Current time is 11:47:17 5/15/2018 Tuesday

Time-range: workday (Active)
 09:00 to 18:00 working-day

Time-range: off-work (Inactive)
 18:00 to 24:00 working-day
```

同时在 Web 管理界面上也可以进行时间段的查看，通过导航栏“对象>对象组>时间段”进入配置界面，可以看到时间段的配置显示与 CLI 命令行一致。