

一、 开始

盒式防火墙又称集中式转发防火墙，V7 NGFW 防火墙是针对中小型企业、园区网互联网出口以及广域网分支市场推出的下一代高性能防火墙产品。NAT（Network Address Translation，网络地址转换）是将 IP 数据报文头中的 IP 地址转换为另一个 IP 地址的过程。在实际应用中，NAT 主要应用在连接两个网络的边缘设备上，用于实现允许内部网络用户访问外部公共网络以及允许外部公共网络访问部分内部网络资源（例如内部服务器）的目的。NAT 是 NGFW 防火墙最常用的功能，防火墙的会话表项记录了 NAT 转换的所有信息，排查 NAT 问题时要结合会话查看。NAT 不通问题的排查思路如下：首先判断是否存在会话表项，如果会话存在，则需要判断 NAT 是否转换成功以及是否接收到反向报文；如果没有会话表项，则需要检查报文是否上到防火墙，是否被安全策略阻断等。

二、流程图相关操作说明：

1、是否存在会话表项

V7 NGFW 盒式防火墙属于典型的检测状态防火墙，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，首先与当前会话表项进行匹配。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 NAT 不通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，接着需要查看 NAT 是否转换等原因；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 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`

例如：从公网网关设备 Ping 私网内部服务器，会话发起方源目的地址分别为 60.3.128.1 和 60.3.128.16。因此在会话表中可以查询到如下表项，会话发起方 IP 为 60.3.128.1，

会话响应方 IP 为 60.3.128.16，协议为 ICMP，发起方位于 Untrust 区域，防火墙从 GigabitEthernet1/0/2 端口接收，显示两个 slot 的相同会话说明两台设备做了堆叠，并且开启了会话同步功能。

```
<H3C> display session table ipv4 source-ip 60.3.128.1 destination-ip
60.3.128.16
Slot 1:
Initiator:
  Source      IP/port: 60.3.128.1/149
  Destination IP/port: 60.3.128.16/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust

Total sessions found: 1

Slot 2:
Initiator:
  Source      IP/port: 60.3.128.1/149
  Destination IP/port: 60.3.128.16/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust

Total sessions found: 1
```

可以看到，上述会话表信息很少，无法查看报文出接口、没有报文统计计数等，更重要的是，无法查看到 NAT 的转换情况。因此，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。

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

例如：上述会话加 verbose 后显示信息如下所示，在会话表中可以查询到如下表项，会话发起方 IP 为 60.3.128.1，会话响应方 IP 为 10.0.1.2，发起方位于 Untrust 区域，响应方位于 Trust 区域，NGFW 防火墙从 GigabitEthernet1/0/2 接口接收，从 GigabitEthernet1/0/10 接口发送。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 23 秒后老化删除。

需要说明的是，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。所以查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 60.3.128.1 destination-ip
60.3.128.16 verbose
Slot 1:
Initiator:
  Source      IP/port: 60.3.128.1/150
  Destination IP/port: 60.3.128.16/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust
Responder:
  Source      IP/port: 10.0.1.2/150
  Destination IP/port: 60.3.128.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/10
  Source security zone: Trust
State: ICMP_REPLY
Application: ICMP
Start time: 2019-01-14 17:55:43  TTL: 23s
Initiator->Responder:          0 packets          0 bytes
Responder->Initiator:          0 packets          0 bytes

Total sessions found: 1

.....
```

2、查看 NAT 是否转换成功

NAT 最初的设计目的是实现私有网络访问公共网络的功能，后扩展为实现任意两个网络间进行访问时的地址转换应用。根据其功能分类，可以将 NAT 分为：动态 NAT、静态 NAT、内部服务器形式的 NAT。进一步，动态 NAT 又可以根据其转换方式分为 NO-PAT 模式、PAT 模式、Easy IP 模式。本文以内部服务器 NAT 为例，在公网口配置 `nat server`，允许外网用户通过指定的 NAT 地址 60.3.128.16 访问内部服务器 10.0.1.2，组网图如下所示：

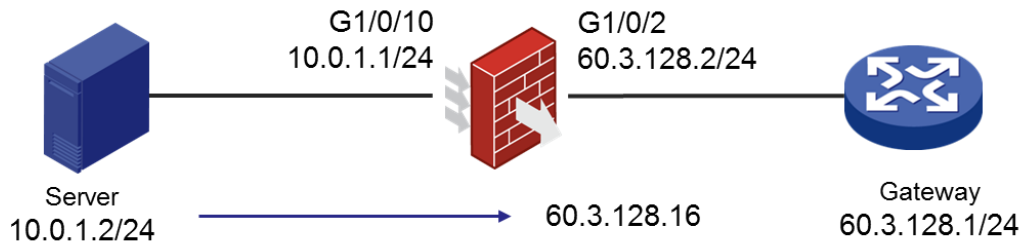


图 1 组网图

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

例如：从公网网关设备 60.3.128.1 Ping 内网服务器 10.0.1.2，内部服务器在防火墙公网口映射为公网地址 60.3.128.16。ICMP 报文的源地址 60.3.128.1、目的地址 60.3.128.16，在防火墙入接口方向目的地址 60.3.128.16 应被转换为内部服务器地址 10.0.1.2。从会话表项上看，会话发起方 Initiator 的目的地址为 60.3.128.16，会话响应方 Responder 的源地址为 10.0.1.2，说明 ICMP 报文的 NAT 转换成功。如果会话表项上的地址未发生变化，则说明 NAT 转换失败。

```

<H3C>display session table ipv4 source-ip 60.3.128.1 destination-ip
60.3.128.16 verbose
Slot 1:
Initiator:
  Source      IP/port: 60.3.128.1/150
  Destination IP/port: 60.3.128.16/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust
Responder:
  Source      IP/port: 10.0.1.2/150
  Destination IP/port: 60.3.128.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/10
  Source security zone: Trust
State: ICMP_REPLY
Application: ICMP
Start time: 2019-01-14 17:55:43  TTL: 23s
Initiator->Responder:          0 packets          0 bytes
Responder->Initiator:          0 packets          0 bytes

Total sessions found: 1

.....

```

3、检查 NAT 配置

如果防火墙会话表项显示未转换成功，先查看 NAT 的配置是否正确。NAT 分类较多，本文介绍以下几种常见情况：

(1) 检查 nat outbound 配置

出方向动态地址转换通常应用在外网侧接口上，用于实现一个内部私有网络地址到一个外部公有网络地址的源地址转换，具体过程如下：对于经过该接口发送的内网访问外网的报文，将与指定 ACL permit 规则匹配的报文源 IP 地址转换为地址组中的地址。

命令：*display nat outbound*

display nat address-group x

display acl xxxx

例如：通过命令查看 NAT 的地址池、ACL 规则以及下发接口是否正确。

```
<H3C>display nat outbound
NAT outbound information:
  Totally 1 NAT outbound rules.
  Interface: GigabitEthernet1/0/2
  ACL: 3999
  Address group ID: 1
  Port-preserved: N          NO-PAT: N  Reversible: N
  Config status: Active

<H3C>display nat address-group 1
Address group ID: 1
  Port range: 1-65535
  Address information:
    Start address      End address
    60.3.128.10       60.3.128.10

<H3C>display acl 3999
Advanced IPv4 ACL 3999, 1 rule,
ACL's step is 5
  rule 0 permit ip source 10.0.1.2 0
```

(2) 检查 nat server 配置

普通的内部服务器是将内网服务器的地址和端口映射为外网地址和端口，允许外部网络中的主机通过配置的外网地址和端口访问位于内网的服务器，即从外网访问内网时将目的地址转换为内网地址，一般配置在报文入接口下。

命令：*display nat server*

例如：通过命令查看 nat server 的映射是否正确，下发的接口是否正确。

```
<H3C>display nat server
NAT internal server information:
  Totally 1 internal servers.
  Interface: GigabitEthernet1/0/2
  Protocol: 0(IPv4)
  Global IP/port: 60.3.128.16/0
  Local IP/port : 10.0.1.2/0
  Rule name      : 内部服务器规则_5
  Config status : Active
```

(3) 检查 nat static 配置

出方向一对一静态地址转换通常应用在外网侧接口上，用于实现一个内部私有网络地址到一个外部公有网络地址的转换。对于经过该接口发送的内网访问外网的报文，转换源地址；对于该接口接收到的外网访问内网的报文，转换目的地址。

命令：display nat static

例如：通过命令查看 nat static 的映射是否正确，是否在正确的接口上引用。

```
<H3C>display nat static
Static NAT mappings:
  Totally 1 outbound static NAT mappings.
  IP-to-IP:
    Local IP      : 10.0.1.2
    Global IP     : 60.3.128.16
    Config status: Active

Interfaces enabled with static NAT:
  Totally 1 interfaces enabled with static NAT.
  Interface: GigabitEthernet1/0/2
  Config status: Active
```

除此之外，需要特别注意集中式转发的盒式防火墙在防火墙双出口 NAT 场景下，NAT 配置上有以下注意事项：

- (1) 流量从 Slot2 入，Slot1 出，出口为物理接口或物理子接口做 NAT，NAT 不能成功转换。规避方案是将物理接口加入逻辑接口（物理子接口可加入冗余口），在逻辑接口上做 NAT。
- (2) 双出口在同一个安全域且同时配置 NAT Outbound 时，当链路发生切换时，因为不会删会话，若后续流量持续命中该会话，业务不通。规避方案为：对于双出口不同 NAT 的场景，应关闭会话备份；对于双出口相同 NAT 的场景，应配置冗余组，采用主备方案。

4、是否接收到反向报文

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 2 所示，防火墙接收到 Gateway 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 Gateway。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。

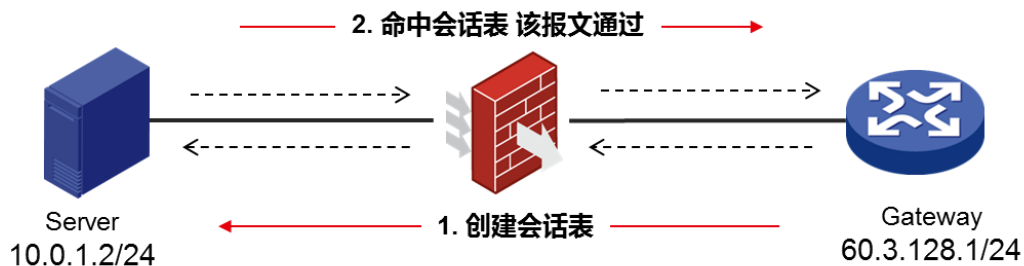


图 2 会话表项创建过程

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 60.3.128.1 经由防火墙 ping 内网 Server 10.0.1.2 不通，查看会话表项的报文计数，发起方到响应方（Initiator→Responder）有 5 个报文，而响应方到发起方（Responder→Initiator）报文计数为 0，会话状态为 ICMP_REQUEST，而不是正常的 ICMP_REPLY。


```

<H3C>session statistics enable
This command is CPU intensive and might affect ongoing services. Are you sure
you want to continue? [Y/N]:y
<H3C>display session table ipv4 source-ip 60.3.128.1 destination-ip
60.3.128.16 verbose
Slot 1:
Initiator:
  Source      IP/port: 60.3.128.1/152
  Destination IP/port: 60.3.128.16/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust
Responder:
  Source      IP/port: 10.0.1.2/152
  Destination IP/port: 60.3.128.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/10
  Source security zone: Trust
State: ICMP_REQUEST
Application: ICMP
Start time: 2019-01-14 18:47:44  TTL: 49s
Initiator->Responder:           5 packets           420 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），注意如果接口配置了 `vpn-instance`，ACL 里的 `rule` 也要增加 `vpn-instance` 参数。

命令：`debugging ip packet acl`

```
[H3C]acl advanced 3000
[H3C-acl-ipv4-adv-3000] rule 0 permit icmp source 10.0.1.2 0 destination
60.3.128.1 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 GigabitEthernet1/0/10 收到 ICMP 回包，报文源地址 10.0.1.2，目的地址 60.3.128.1，符合实际回包情况。

```
<H3C>*Jan 14 19:03:52:156 2019 H3C IPFW/7/IPFW_PACKET: -Context=1;
Receiving, interface = GigabitEthernet1/0/10
version = 4, headlen = 20, tos = 0
pktlen = 84, pktid = 18421, offset = 0, ttl = 64, protocol = 1
checksum = 27566, s = 10.0.1.2, d = 60.3.128.1
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Receiving IP packet from interface GigabitEthernet1/0/10.
Payload: ICMP
type = 0, code = 0, checksum = 0x314f.
```

如果没有匹配 ACL 的 debug 信息，则回程报文没到防火墙，需排查回程路由等问题。

除此之外，新 Web 界面版本（D022 分支及以上）支持抓包功能，同样也可以通过抓取接口报文，确认是否接收到反向报文。在 Web 管理平台中，通过“系统>维护>报文捕获”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。

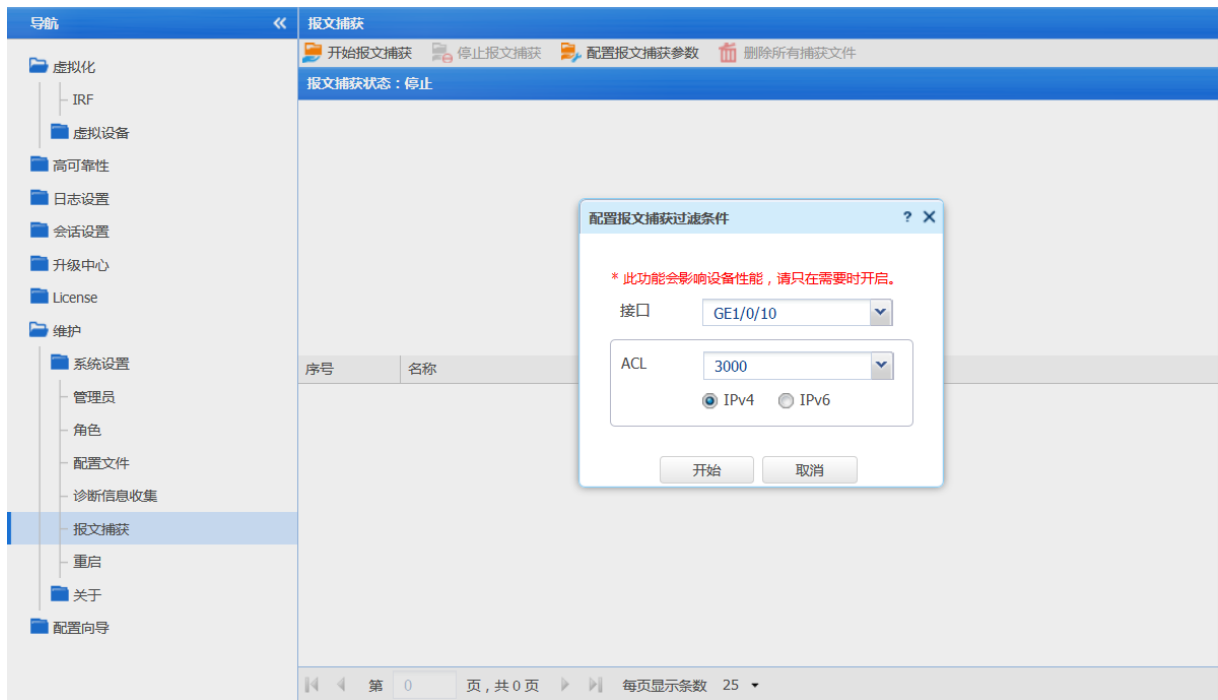


图 3 报文捕获匹配反向报文

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，检查是否抓取到相应报文。

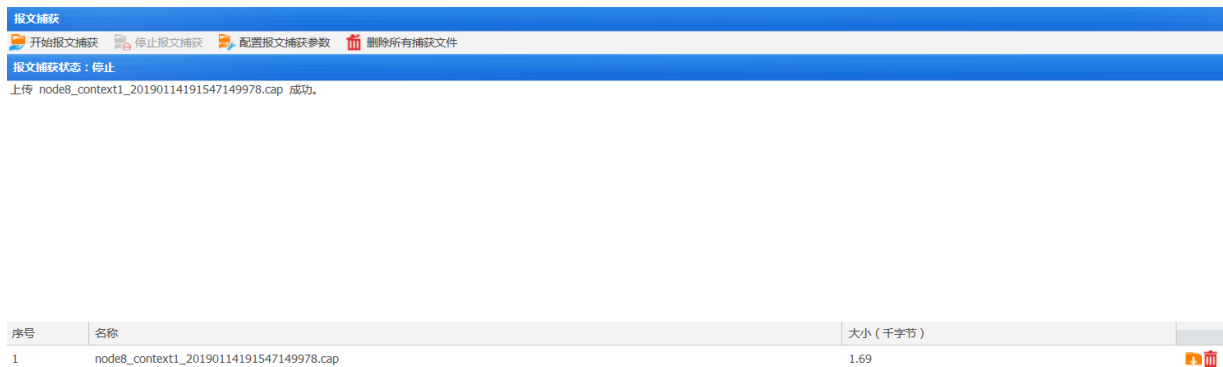


图 4 反向报文抓包情况显示

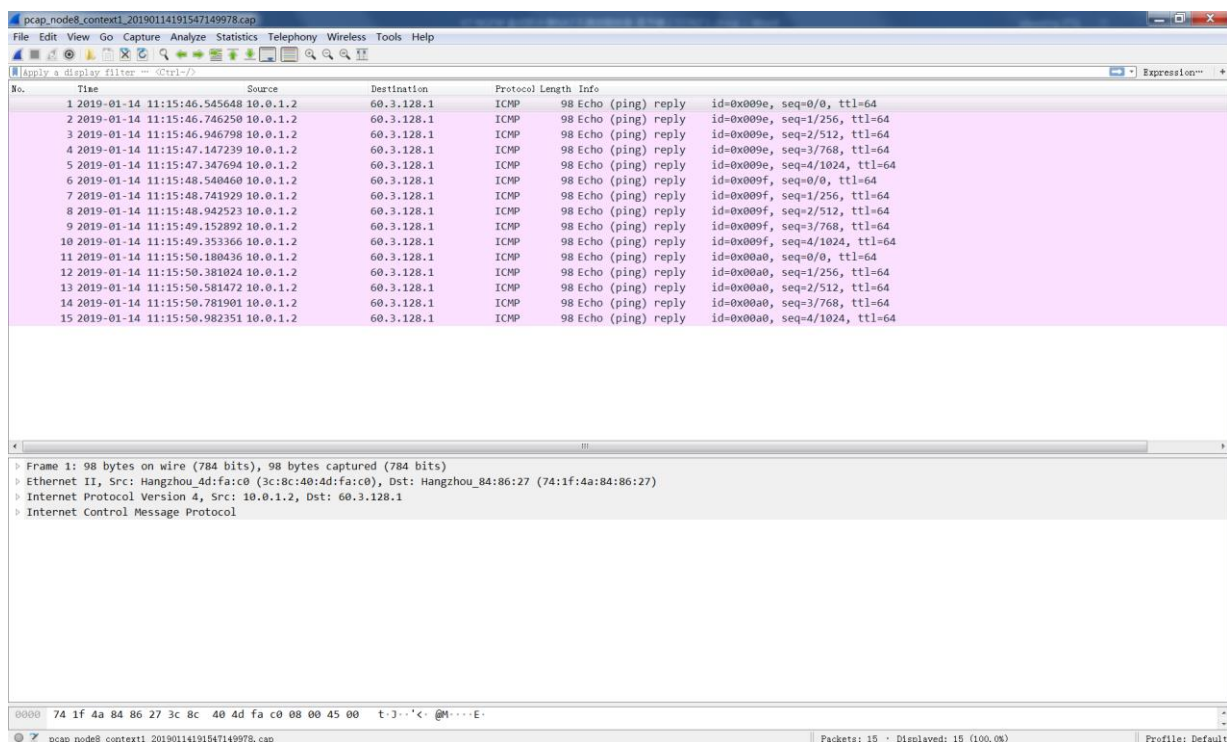


图 5 抓取到回程报文

5、检查其它设备

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。

6、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），注意如果接口配置了 vpn-instance，ACL 里的 rule 也要增加 vpn-instance 参数。

命令：`debugging ip packet acl`

```
[H3C]acl advanced 3000
[H3C-acl-ipv4-adv-3000] rule 0 permit icmp source 60.3.128.1 0 destination
60.3.128.16 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，网关 Gateway 60.3.128.1 发送给 Server 公网地址 60.3.128.16 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 GigabitEthernet1/0/2 收到 ICMP 报文，报文源地址 60.3.128.1，目的地址 60.3.128.16。

```
<H3C>*Jan 14 19:20:46:912 2019 H3C IPFW/7/IPFW_PACKET: -Context=1;
Receiving, interface = GigabitEthernet1/0/2
version = 4, headlen = 20, tos = 0
pktlen = 84, pktid = 8721, offset = 0, ttl = 255, protocol = 1
checksum = 8576, s = 60.3.128.1, d = 60.3.128.16
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Receiving IP packet from interface GigabitEthernet1/0/2.
Payload: ICMP
    type = 8, code = 0, checksum = 0xad3d.
```

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，新 Web 界面版本（D022 分支及以上）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。

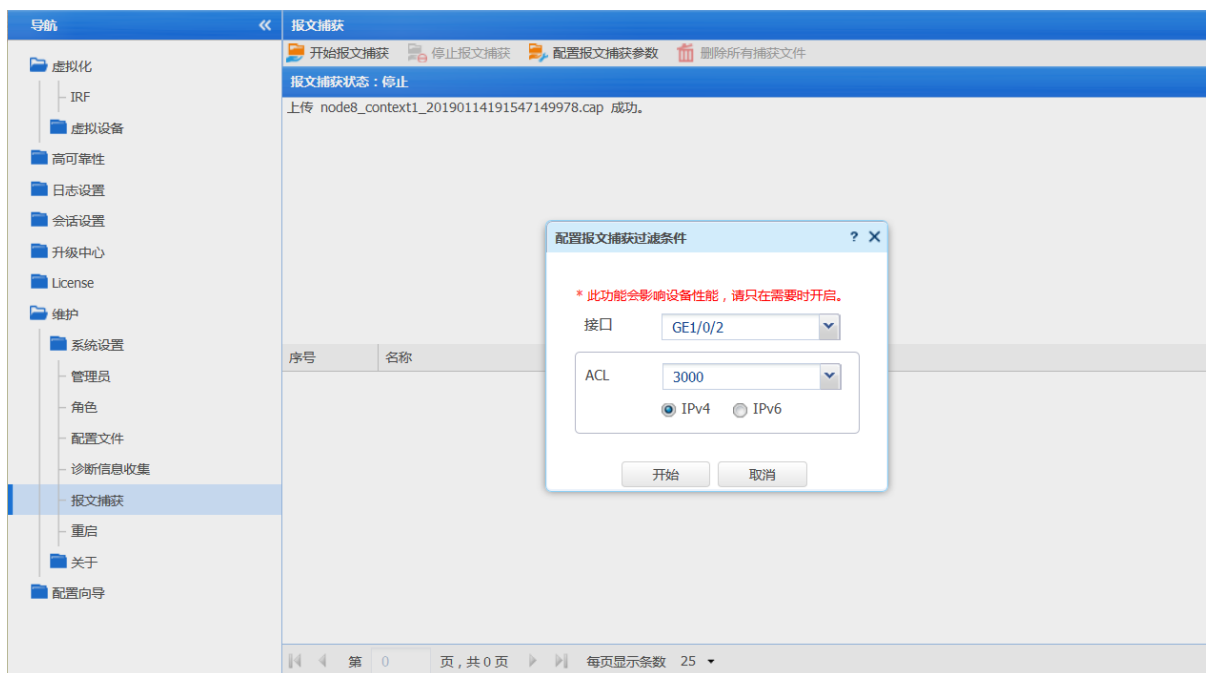


图 6 报文捕获匹配正向报文

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，检查是否抓取到相应报文。

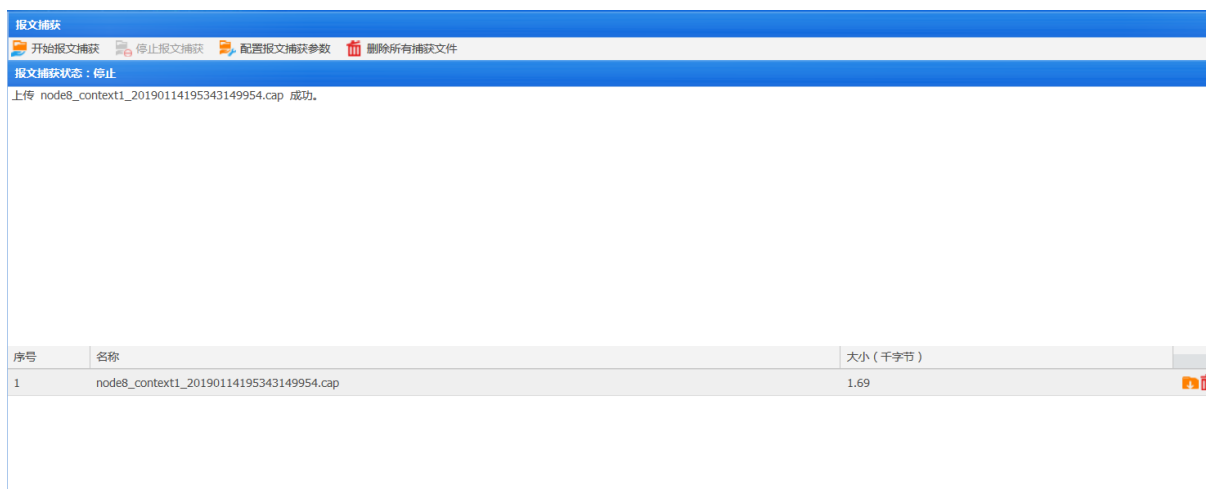


图 7 正向报文抓包情况显示

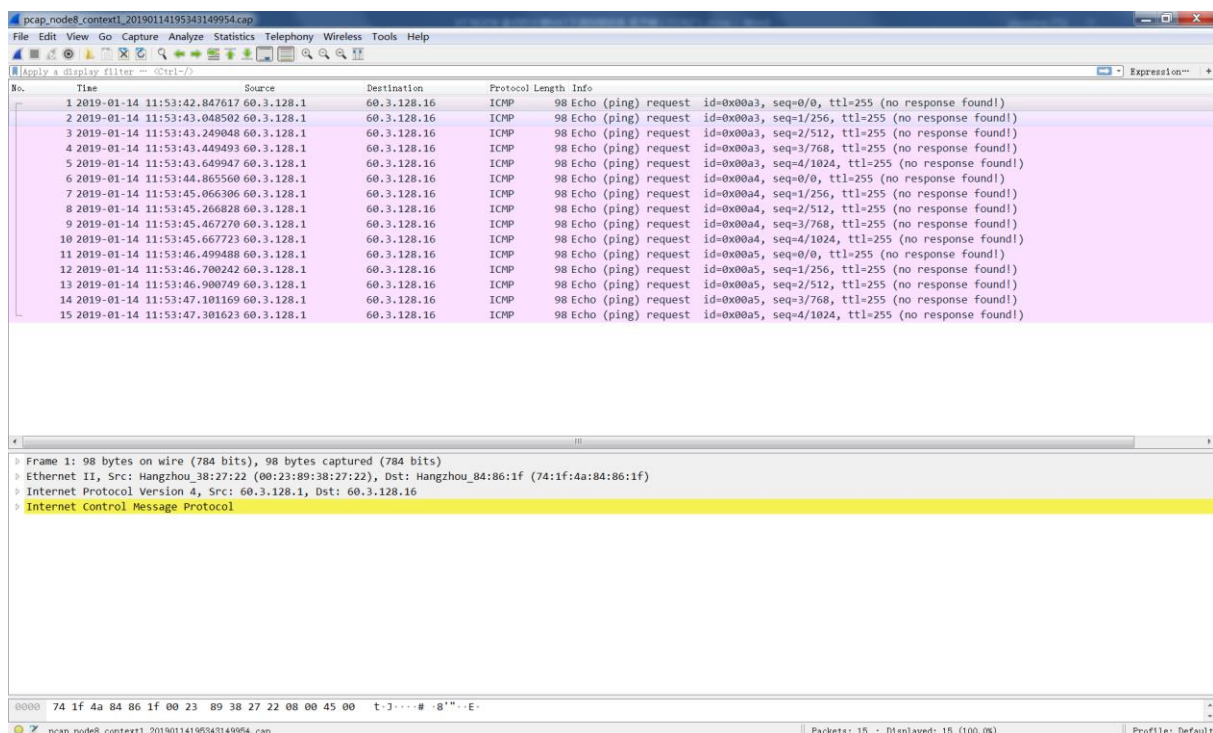


图 8 抓取到的正向报文

7、报文是否被安全策略阻断

V7 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）。

在 NAT 场景下，报文的地址做了转换，因此不同的 NAT 功能 ACL 匹配的源和目的地址不同。NAT 转换和安全策略的匹配有先后顺序，如图 9 所示，报文过防火墙的顺序为：入方向 NAT > 安全策略 > 出方向 NAT。简单的说，就是 nat server 匹配转换后的地址，nat outbound 匹配转换前的地址。

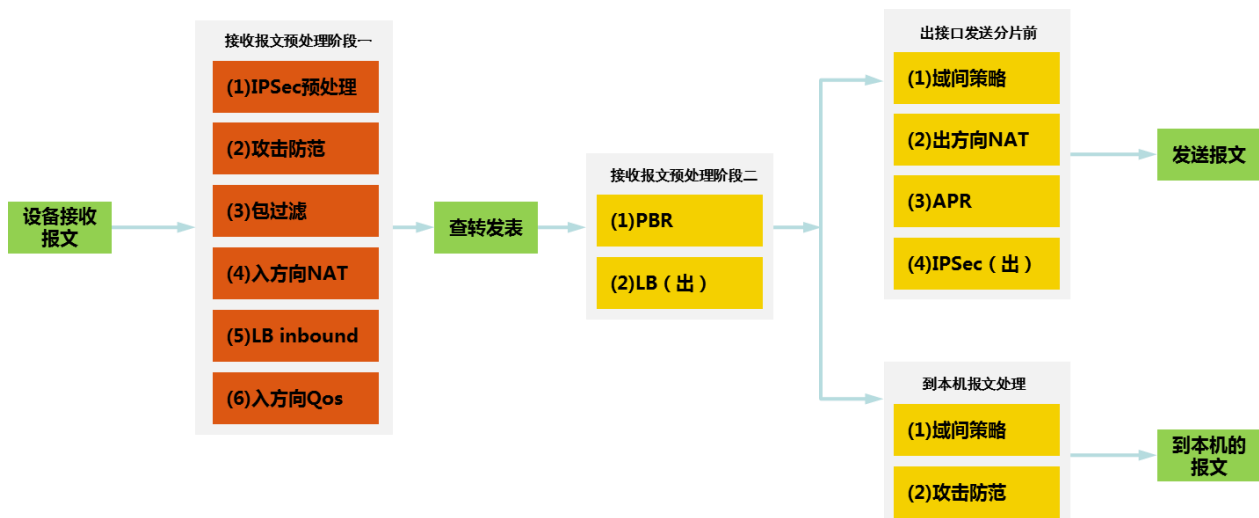


图 9 报文过防火墙处理流程

命令：`debugging security-policy packet ip acl`

例如：在外网口配置内部服务器 nat server, 将内网服务器 10.0.1.2 映射成 60.3.128.16, 从网关 60.3.128.1 ping 服务器公网地址 60.3.128.16, 防火墙的安全策略应放通源地址 60.3.128.1 到目的地址 10.0.1.2 的规则, 而不是放通源地址 60.3.128.1 到目的地址 60.3.128.16 的规则。因此, debug 报文是否被防火墙阻断的明细 ACL 也应匹配源地址 60.3.128.1 到目的地址 10.0.1.2 的报文。

```
[H3C]acl advanced 3000
[H3C-acl-ipv4-adv-3000] rule 0 permit icmp source 60.3.128.1 0 destination 10.0.1.2 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 debug 信息可知, 报文通过安全策略检查, 源安全域为 Untrust 域, 目的安全域为 Trust 域, 此外还包括报文的源目的地址、源目的端口号、协议等五元组信息, 命中的安全策略名称为 tong, 规则 ID 为 3。

正常debug

```
<H3C>*Jan 14 20:00:11:252 2019 H3C FILTER/7/PACKET: -Context=1; The packet is permitted.  
Src-Zone=Untrust, Dst-Zone=Trust;If-In=GigabitEthernet1/0/2(3), If-  
Out=GigabitEthernet1/0/10(11); Packet Info:Src-IP=60.3.128.1, Dst-IP=10.0.1.2, VPN-  
Instance=,Src-Port=8, Dst-Port=0, Protocol=ICMP(1), Application=ICMP(22742),  
SecurityPolicy=tong, Rule-ID=3.
```

图 10 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。如图所示，可以看出 debug 信息中的 Src-Zone 源安全域参数缺失，说明是入接口 GigabitEthernet1/0/2 没有加入安全域。

命令：*debugging aspf packet acl*

①没加安全域

```
<H3C>*Jan 14 20:06:12:071 2019 H3C ASPF/7/PACKET: -Context=1; The packet was dropped  
by ASPF for nonexistent zone pair. Src-Zone=-, Dst-Zone=Trust;If-In=GigabitEthernet1/0/2(3),  
If-Out=GigabitEthernet1/0/10(11); Packet Info:Src-IP=60.3.128.1, Dst-IP=10.0.1.2, VPN-  
Instance=none,Src-Port=168, Dst-Port=2048. Protocol=ICMP(1).
```

debug 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中断。

命令：*debugging security-policy packet ip acl*

②没有安全策略

```
<H3C>*Jan 14 20:10:33:243 2019 H3C FILTER/7/PACKET: -Context=1; The packet is denied.  
Src-Zone=Untrust, Dst-Zone=Trust;If-In=GigabitEthernet1/0/2(3), If-  
Out=GigabitEthernet1/0/10(11); Packet Info:Src-IP=60.3.128.1, Dst-IP=10.0.1.2, 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=3.” 说明是规则 ID 为 3 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中断。

命令：*debugging security-policy packet ip acl*

③安全策略配置了阻断

```
<H3C>*Jan 14 20:12:51:018 2019 H3C FILTER/7/PACKET: -Context=1; The packet is denied.  
Src-Zone=Untrust, Dst-Zone=Trust;If-In=GigabitEthernet1/0/2(3), If-  
Out=GigabitEthernet1/0/10(11); Packet Info:Src-IP=60.3.128.1, Dst-IP=10.0.1.2, VPN-  
Instance=,Src-Port=8, Dst-Port=0, Protocol=ICMP(1), Application=ICMP(22742),  
SecurityPolicy=tong, Rule-ID=3.
```

8、检查安全域

V7 NGFW 盒式防火墙默认安全域有 Trust、DMZ、Untrust 和 Management，GigabitEthernet0/0 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 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。防火墙与网关相连的接口 GigabitEthernet1/0/2 加入了 Untrust 区域，防火墙与内部服务器相连的接口 GigabitEthernet1/0/10 加入了 Trust 区域。

```

<H3C>display current-configuration configuration seczone
#
security-zone name Local
#
security-zone name Trust
import interface GigabitEthernet1/0/10
import interface GigabitEthernet2/0/5
import interface Route-Aggregation5
import interface Ten-GigabitEthernet1/0/24
import ip 1.1.1.1 32
attack-defense apply policy ATK
#
security-zone name DMZ
#
security-zone name Untrust
import interface GigabitEthernet1/0/2
import interface GigabitEthernet1/0/4
import interface GigabitEthernet2/0/6
#
security-zone name Management
import interface GigabitEthernet1/0/0
import interface GigabitEthernet2/0/0
import interface Reth255
#
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，防火墙与网关相连的接口 GigabitEthernet1/0/2 加入了 Untrust 区域，防火墙与内部服务器相连的接口 GigabitEthernet1/0/10 加入了 Trust 区域。

安全域名称	成员个数	成员列表	编辑
Local	--		编辑
Trust	4	GE1/0/10 XGE1/0/24 GE2/0/5 RAGGS	编辑
DMZ	0		编辑
Untrust	3	GE1/0/2 GE1/0/4 GE2/0/6	编辑
Management	3	GE1/0/0 GE2/0/0 Reth255	编辑

图 11 Web 界面安全域显示

9、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三条规则，第一条为允许从源安全域 Untrust 到目的安全域 DMZ，源地址对象为 finance 的报文通过，并开启记录日志和策略匹配统计功能；第二条为允许从源安全域 Trust 到目的安全域 Local，源地址对象为 ceo_office 目的地址对象为 finance 的报文通过；第三条为允许从任意源安全域到任意目的安全域的所有报文通过。

```

<H3C>display current-configuration configuration security-policy-ip
#
security-policy ip
rule 5 name test
action pass
logging enable
counting enable
source-zone Untrust
destination-zone DMZ
source-ip finance
rule 4 name 2
action pass
source-zone Trust
destination-zone Local
source-ip ceo_office
destination-ip finance
rule 3 name tong
action pass
#
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，如果命令行里使用域间策略 zone-pair，Web 界面将不显示任何策略配置情况。

名称	源安全域	目的安全域	类型	ID	描述	源地址	目的地址	服务	用户	动作	内容安全	命中次数	流量	统计	启用	编辑
test	Untrust	DMZ	IPv4	5		finance				允许		0	0.00B	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	Trust	Local	IPv4	4		ceo_office	finance			允许				<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
tong			IPv4	3						允许				<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

图 12 Web 界面安全策略显示

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 10.0.1.2
  0 network host address 10.0.1.2
#
object-group ip address 60.3.128.1
  security-zone Trust
  0 network host address 60.3.128.1
#
object-group ip address 60.3.128.16
  security-zone Inside
  0 network host address 60.3.128.16
#
object-group ip address ceo_office
  0 network subnet 192.168.1.0 255.255.255.0
#
object-group ip address finance
  0 network subnet 192.168.2.0 255.255.255.0
#
object-group ip address huwei
  0 network host name www.h3c.com
#
object-group service 1
#
object-group service tcp-445
  0 service tcp destination eq 445
#
object-group service web
  0 service tcp destination eq 80
#
return
```

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。



对象组名称	对象	被引用	安全域	描述	编辑
10.0.1.2	主机IP地址 10.0.1.2	否			编辑
60.3.128.1	主机IP地址 60.3.128.1	否	Trust		编辑
60.3.128.16	主机IP地址 60.3.128.16	否	Inside		编辑
ceo_office	网段 192.168.1.0 / 255.255.255.0	是			编辑
finance	网段 192.168.2.0 / 255.255.255.0	是			编辑

图 13 Web 界面 IPv4 地址对象组显示

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
20:44:46 China Mon 01/14/2019
_ _ _ _ _
```

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 2019 年 1 月 14 日 21 时。

```
<H3C>clock datetime 21:00 2019/1/14
```

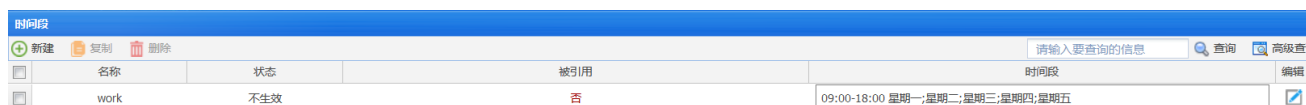
命令：*display time-range all*

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 20:46:07 1/14/2019 Monday

Time-range: work (Inactive)
09:00 to 18:00 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。



名称	状态	被引用	时间段
work	不生效	否	09:00-18:00 星期一;星期二;星期三;星期四;星期五

图 14 Web 界面时间段显示