H3C SecPath 防火墙产品

故障处理手册(V7)

资料版本：6W403-20220223

目 录

1 适用款型及版本

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请以设备实际情况为准。

本文档所描述的内容适用于如下款型及版本：

款型	软件版本
F5030-D、F5060-D、F5080-D、F5000-AK515、F5000-AK525	R9620
F5030、F5030-6GW、F5060、F5080、F5000-M、F5000-A、F5000-AI-20、F5000-AI-40、F5000-V30	R9628
F5010、F5020-GM、F5020、F5040、F5000-C、F5000-S	R9342
F1000-AI-20、F1000-AI-30、F1000-AI-50	R9345
F1000-AI-60、F1000-AI-70、F1000-AI-80、F1000-AI-90	R8601
F1005、F1010、F1003-L、F1005-L、F1010-L	R9536
F1020、F1020-GM、F1030、F1030-GM、F1050、F1060、F1070、F1070-GM、F1070-GM-L、F1080、F1000-V70	R9345
F1090、F1000-V90	R8601
F1000-AK1010、F1000-AK1020、F1000-AK1030	R9536
F1000-AK1110、F1000-AK1120、F1000-AK1130、F1000-AK1140	R9536
F1000-AK1212、F1000-AK1222、F1000-AK1232、F1000-AK1312、F1000-AK1322、F1000-AK1332	R9345
F1000-AK1414、F1000-AK1424、F1000-AK1434、F1000-AK1514、F1000-AK1524、F1000-AK1534、F1000-AK1614	R8601
F1000-AK108、F1000-AK109、F1000-AK110、F1000-AK115、F1000-AK120、F1000-AK125、F1000-AK710	R9536
F1000-AK130、F1000-AK135、F1000-AK140、F1000-AK145、F1000-AK150、F1000-AK155、F1000-AK160、F1000-AK165、F1000-AK170、F1000-AK175、F1000-AK180、F1000-AK185、F1000-AK711、F1000-GM-AK370、F1000-GM-AK380	R9345
F1000-E-G5、F1000-H-G5	R8601
F100-C-G5、F100-M-G5、F100-S-G5	R9345
F1000-A-G3、F1000-C-G3、F1000-E-G3、F1000-S-G3	R8601
F1000-9390-AI、F1000-9385-AI	R8601
F1000-990-AI、F1000-980-AI、F1000-970-AI、F1000-960-AI、F1000-950-AI、F1000-930-AI、F1000-920-AI	R9345
F1000-910-AI、F1000-905-AI	R9536
F1000-720-HI、F1000-710-HI	R9536
F100-C-XI、F100-S-XI	R9536
F1000-E-G2、F1000-A-G2、F1000-S-G2、F1000-C-G2、F100-A-G2、F100-E-G2、F100-A-G3、F100-E-G3	R9345

款型	软件版本
F1000-C8180、F1000-C8170、F1000-C8160、F1000-E-VG	R9345
F1000-C-EI、F1000-C-HI、F100-A-EI、F100-E-EI、F100-A-HI、F100-A-SI、F100-A80-WiNet	R9345
F1000-C8150、F1000-C8130、F1000-C8120、F1000-C8110、F1000-S-VG	R9536
F1000-C8395	R8601
F100-C-A6、F100-C-A5、F100-C-A3、F100-C-G3、F100-S-G3、F100-M-G3、F100-M-G2、F100-S-G2、F100-C-G2、F100-C-EI、F100-C-HI、F100-S-HI	R9536
F100-C80-WiNet、F100-C60-WiNet、F100-C50-WiNet、F100-S80-WiNet	R9536
F100-C-A6-WL、F100-C-A5-W、F100-C-A3-W	R9602
LSU3FWCEA0、LSUM1FWCEAB0、LSX1FWCEA1	R8239
LSPM6FWD	R8533
LSXM1FWDF1、LSUM1FWDEC0、IM-NGFWX-IV、LSQM1FWDSC0、LSWM1FWD0、LSQM2FWDSC0	R8534
LSPM6FWD8	R8535
LSQM2FWDSC8	R8520

2 简介

本文档介绍防火墙产品软、硬件常见故障的诊断及处理措施。

2.1 故障处理注意事项

- 更换和维护设备部件时，请佩戴防静电手腕，以确保您和设备的安全。
- 设备正常运行时，建议您在完成重要功能的配置后，及时保存当前配置，以便设备出现故障后能迅速恢复配置。
- 设备出现故障时，请尽可能全面、详细地记录现场信息（包括但不限于以下内容），搜集信息越全面、越详细，越有利于故障的快速定位。
  - 记录具体的故障现象、故障时间、配置信息。
  - 记录完整的网络拓扑，包括组网图、端口连接关系、故障位置。
  - 记录现场采取的故障处理措施（比如配置操作、插拔线缆、手工重启设备）及实施后的现象效果。
  - 记录故障处理过程中配置的所有命令行显示信息。
  - 搜集设备日志信息和诊断信息。
  - 记录抓取的报文信息、系统输出的 Debug 信息、主控板与网板持续异常重启的输出信息。
  - 记录设备故障时单板、电源指示灯的状态，或给现场设备拍照记录。
- 故障处理过程中，请注意：

- 明确每项配置操作的影响，保证操作出问题时能够被恢复，故障影响不会扩大。
- 操作执行后请等待一定时间以确认执行效果。
- 请不要保存故障处理过程中的配置，特别是出现 IRF 分裂，否则会引起配置丢失。

2.2 收集设备运行信息

说明

为方便故障快速定位，请使用命令 **info-center enable** 开启信息中心。缺省情况下信息中心处于开启状态。

设备运行过程中会产生 logfile 日志信息及记录设备运行状态的诊断信息。

日志在保存到日志文件前，先保存在日志文件缓冲区。系统会按照指定的频率将日志文件缓冲区的内容写入日志文件，用户也可以手工触发立即保存。诊断日志在保存到诊断日志文件前，先保存在诊断日志文件缓冲区。系统会按照指定的频率将诊断日志文件缓冲区的内容写入诊断日志文件，用户也可以手工触发立即保存。

在任意视图下执行 **logfile save** 命令，手动将日志文件缓冲区中的内容保存到日志文件。

在任意视图下执行 **diagnostic-logfile save** 命令，手动将诊断日志文件缓冲区中的内容保存到诊断日志文件。

这些日志文件存储在 Flash 或 CF 卡中，可以通过 FTP 或 TFTP 等方式导出。

表1 设备运行信息介绍

分类	文件名	内容
logfile日志	logfileX.log	命令行记录、Trap信息、设备运行中产生的记录信息
诊断信息	XXX.gz	设备状态、CPU状态、内存状态、配置情况、软件表项、硬件表项等

2.2.1 logfile 日志

请先通过 **logfile save** 将设备缓存的 logfile 日志保存在存储介质中，并将日志搜集完整。

```
[H3C] logfile save
The contents in the log file buffer have been saved to the file flash:/logfile/l
ogfile.log.
```

设备的 logfile 日志：

```
<H3C> dir flash:/logfile/
Directory of flash:/logfile
   0 -rw-    10483632 Jul 08 2014 15:05:22   logfile.log

253156 KB total (77596 KB free)
```

2.2.2 诊断信息

执行 **display diagnostic-information** 命令后，请输入“Y”，以选择将诊断保存到 Flash 中（选择 display 会出现信息搜集不全）。

```
<H3C> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:y
Please input the file name(*.gz)[flash:/diag.gz]:flash:/diag.gz
Diagnostic information is outputting to flash:/diag.gz.
Save successfully.
<H3C> dir flash:/
Directory of flash:
......
   6 -rw-      898180 Jun 26 2013 09:23:51   diag.gz

1021808 KB total (259072 KB free)
```

也可以将诊断信息直接显示出来（不建议这样搜集），搜集前请先执行 **screen-length disable**，避免屏幕输出被打断，如下：

```
<H3C> screen-length disable
% Screen-length configuration is disabled for current user.
<H3C> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:N
============================================================================
  ===============display cpu===============
Slot 1 CPU 0 CPU usage:
       6% in last 5 seconds
       6% in last 1 minute
       6% in last 5 minutes

============================================================
============================================================================
  ===============display cpu-usage history slot 1 ===============
100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|
 30%|
 25%|
 20%|
```

```
 15%|
 10%|
  5%|############################################################
     ------------------------------------------------------------
               10        20        30        40        50        60   (minutes)
                    cpu-usage (Slot 1 CPU 0) last 60 minutes (SYSTEM)
```

2.3 故障定位和处理

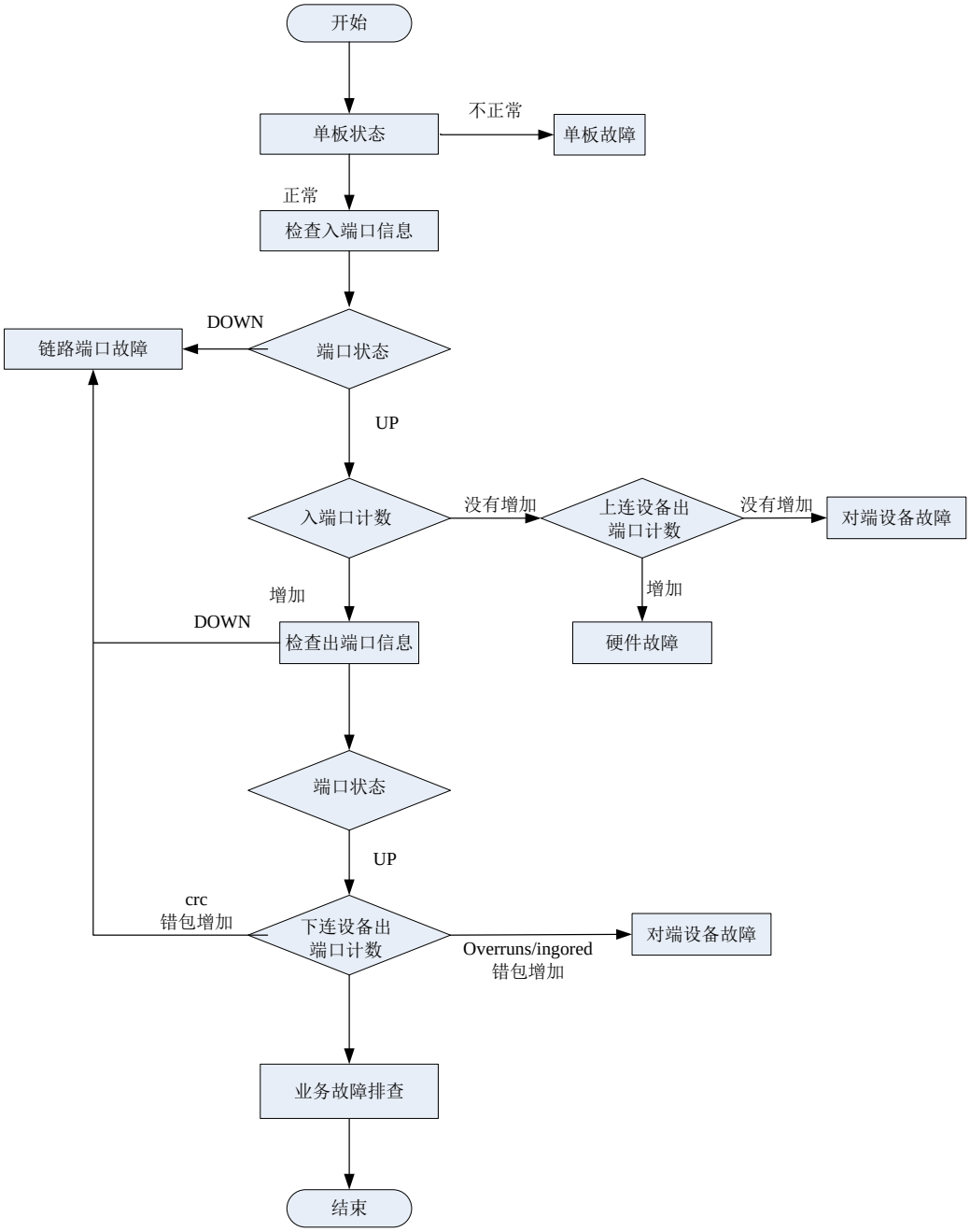
设备出现故障时，请先搜集设备运行的相关信息，判断大致的故障类型，然后参照对应类型的故障处理流程进行确认。

如遇到故障无法确认，请将故障描述连同搜集的信息发送给公司技术支持人员分析。

2.3.1 故障处理流程图

图 1 为故障处理的一般流程，可以大致判断出故障的类型。

图1 故障处理流程图



2.3.2 故障原因分类

1. 主机故障

如主机出现异常重启、状态异常、无法启动、反复重启，请参照 3.1 主机故障。

2. 温度告警

如设备打印温度告警，请参照 3.3 温度告警。

3. 链路端口故障

4. 如端口出现无法 UP、频繁 UP/DOWN、端口错包，请参照 3 硬件类故障处理。

如出现 ping、tracert 丢包或不通、二层丢包或不通、三层丢包或不通、业务异常等，请参照 5 报文转发故障处理。

5. IRF 故障

如设备无法形成 IRF、IRF 分裂等，请参照 6 IRF 类故障处理。

6. 双机热备故障

如果出现主备切换异常、冗余口转发异常、冗余口切换异常，请参照 8 双机热备故障处理。

7. 负载均衡故障处理

主要是 4 层负载均衡的故障处理、7 层负载均衡的故障处理。请参照 12 负载均衡故障处理。

8. CPU 占用率高

如主控设备或引擎的 CPU 占用率很高，请参照 13.1 CPU 占用率高。

9. 内存占用率高

如设备单板内存占用率很高，请参照 13.2 内存占用率高。

2.3.3 常见的故障恢复措施

表2 常见的故障恢复措施

故障原因	业务恢复动作	故障排除动作
硬件	隔离故障单板 调整业务流向来隔离故障设备（如可以调整路由的优先级，避免流量经过故障设备，实现流量切换）	更换备件（备件上线应用前应进行必要的测试）
软件	重启故障设备的协议 调整业务流向来隔离故障设备	升级版本（含补丁版本） 调整组网或配置，消除引发故障因素
链路	调整业务流向来隔离故障线路	检修线路
其他	修改错误配置 正确连接设备端口 调整业务流向来隔离故障线路	修改错误配置 正确连接设备端口 检修机房的电源、空调等支撑系统

3 硬件类故障处理

3.1 主机故障

3.1.1 故障描述

主机重启

3.1.2 故障处理步骤

当主机出现重启，请查看重启原因，如果是软件异常导致设备重启请搜集主机的诊断信息，并发给研发处理。

```
<H3C>display version
H3C Comware Software, Version 7.1.064, Ess 8601P08
Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.
H3C SecPath F1090 uptime is 0 weeks, 0 days, 0 hours, 5 minutes
Last reboot reason: User reboot

Boot image: flash:/F1090FW-CMW710-BOOT-E8601P08.bin
Boot image version: 7.1.064, Ess 8601P08
  Compiled Sep 10 2019 15:00:00
System image: flash:/F1090FW-CMW710-SYSTEM-E8601P08.bin
System image version: 7.1.064, Ess 8601P08
  Compiled Sep 10 2019 15:00:00

SLOT 1
CPU type:           Multi-core CPU
DDR4 SDRAM Memory:   8192M bytes
FLASH:              7296M bytes
CPLD_A           Version:  1.0
CPLD_B           Version:  1.0
Release          Version:SecPath F1090-8601P08
Basic  BootWare  Version:0.30
Extend BootWare  Version:1.01
BuckleBoard Version:Ver.A
BackBoard1 Version:Ver.A
BackBoard2 Version:Ver.A
HD_BackBoard Version:Ver.D
Pcb Version:Ver.A
[SUBCARD 0] NSQ1F1MSPUOTXA(Hardware)Ver.A, (Driver)1.0, (Cpld)1.0
Boot Type: Warm
[H3C]isplay  system internal  version
H3C SecPath F1090 V800R006B01D645SP08
Comware V700R001B64D045SP08
```

3.2 风扇故障

3.2.1 故障描述

风扇框指示灯异常，设备打印风扇异常信息，如：

```
%May 06 10:12:24:805 2017 H3C DEV/3/FAN_ABSENT: -MDC=1; Slot 2 Fan 2 is absent.
%May 06 10:12:32:805 2017 H3C DEVD/2/DRV_DEV_FAN_CHANGE: -MDC=1;  Slot 2: Fan communication state changed: Fan 1 changed to fault.
%May 06 10:12:42:405 2017 H3C DEV/2/FAN_FAILED: -MDC=1; Slot 2 Fan 1 failed.
```

3.2.2 故障处理步骤

(1) 风扇框在位时，用手放在设备出风口，判断是否有出风，如果出风口无风，则风扇异常。

(2) 检查风扇的入风口、出风口是否被挡住或积累太多灰尘。

(3) 通过 **display fan** 命令检查风扇框是否正常在位，各个风扇的状态是否正常、转速和正常转速相差达到 50%以上。如存在异常，建议通过风扇框拔插、更换交叉进一步确认。

```
<H3C> display  fan
SLOT 1 Fan 0      Status: Normal  Speed:9500
SLOT 1 Fan 1      Status: Normal  Speed:9500
SLOT 1 Fan 2      Status: Normal  Speed:9500
```

(4) 如果故障不能恢复，需要更换该风扇框，但当前没有风扇框，请关闭设备以免发生温度高导致单板烧坏；如果有降温措施保证系统工作在 50 度以下，可以暂时继续使用设备。

3.3 温度告警

3.3.1 故障描述

设备打印温度过低、过高等告警信息，如：

```
%Mar 18 04:22:05:893 2017 H3C DEV/4/TEMPERATURE_WARNING: -Context=1; Temperature is greater
than the high-temperature warning threshold on slot 2 sensor inflow 1. Current temperature
is 43 degrees centigrade.
```

3.3.2 故障处理步骤

(1) 检查环境温度是否正常。如果环境温度较高，请确认原因，比如机房通风不畅、空调制冷故障等。

(2) 检查设备当前的 temperature 温度是否超出上下的 Warning、Alarm 门限。也可以用手触摸单板，确认单板是不是很烫，如单板温度很高，请立即检查原因。持续处于较高的温度下，可能会导致单板损坏。

a. 如果温度值为 error 或出现明显不合实际的值，可能是通过 I2C 总线访问单板温度传感器异常。设备光模块信息访问也是通过 I2C 总线，请继续检查单板读取光模块信息是否正常。如光模块访问正常，请使用 **temperature-limit** 命令重新设置单板的温度告警门限值，并通过 **display environment** 查看是否设置成功。

```
[H3C] temperature-limit slot 1 inflow 1 -5 43 51
[H3C] display environment
System Temperature information (degree centigrade):
-----------------------------------------------------------------------------
---------
 Slot     Sensor   Temperature LowerLimit Warning-UpperLimit  Alarm-UpperLimit S
hutdown-UpperLimit
1       inflow  1       29          -5              43                51
      NA
2       inflow  1       28          -5              48                56
      NA
```

如果仍然无法确认故障原因，请搜集温度告警日志、**display environment**、环境实际温度等信息并发送给技术支持人员协助分析。

3.4 故障诊断命令

命令	说明
display device	显示设备信息，检查各单板的状态是否正常
display environment	显示设备的温度信息，检查环境温度是否正常（是否超出温度告警阈值）
display power	显示交换机上的电源系统信息。详细信息包括下列信息： • 电源管理使能状态 • 电源类型、额定输入电压和额定输出功率 • 冗余电源模块数，各模块可用的、冗余的、已用的、剩余的功率 • 在位电源模块的状态 • 接口板的供电状态
display version	显示系统版本信息、单板的运行时间以及最后一次重启的原因
save	将当前配置保存到指定文件
temperature-limit	设置设备的温度告警门限

4 端口故障处理

4.1 端口错包

4.1.1 故障描述

使用 **display interface** 命令查询端口的入、出方向流量统计信息，发现错包统计计数不为 0。

```
<H3C>display interface GigabitEthernet 1/0/2
GigabitEthernet1/0/2
Current state: DOWN
Line protocol state: DOWN
Description: GigabitEthernet1/0/2 Interface
Maximum transmission unit: 1500
Internet address: 192.168.2.1/24 (primary)
IP packet frame type: Ethernet II, hardware address: 50da-00dd-1327
IPv6 packet frame type: Ethernet II, hardware address: 50da-00dd-1327
Media type is twisted pair, loopback not set, promiscuous mode not set
Speed Negotiation, Duplex Negotiation, link type is autonegotiation
Output flow-control is disabled, input flow-control is disabled
Last link flapping: Never
Last clearing of counters: Never
 Peak input rate: 0 bytes/sec, at 00-00-00 00:00:00
 Peak output rate: 0 bytes/sec, at 00-00-00 00:00:00
 Last 300 second input: 0 packets/sec 0 bytes/sec -%
 Last 300 second output: 0 packets/sec 0 bytes/sec -%
```

```
Input (total):  0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Input (normal):  0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Input:  0 input errors, 0 runts, 0 giants, - throttles
         0 CRC, 0 frame, 0 overruns, 0 aborts
         0 ignored, - parity errors
Output (total): 0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Output (normal): 0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Output: 0 output errors, 0 underruns, - buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         0 lost carrier, 0 no carrier
```

1. 端口入方向报文计数错误字段解释

- **input errors**：端口接收的错误报文的统计值。
- **runts**：接收到的超小帧的数量。超小帧是指长度小于 64 字节、格式正确且包含有效的 CRC 字段的帧。
- **giants**：接收到的超大帧的数量。超大帧是指有效长度大于端口允许通过最大报文长度的帧，对于禁止长帧通过的以太网端口，超大帧是指有效长度大于 1518 字节（不带 VLAN Tag）或大于 1522 字节（带 VLAN Tag 报文）的帧；对于允许长帧通过的以太网端口，超大帧是指有效长度大于指定最大长帧长度的帧。
- **throttles**：接收到的长度为非整数字节的帧的个数。
- **CRC**：接收到的 CRC 校验错误、长度正常的帧的数量。
- **frame**：接收到的 CRC 校验错误、且长度不是整字节数的帧的数量。
- **overruns**：当端口的接收速率超过接收队列的处理能力时，导致报文被丢弃。
- **aborts**：接收到的非法报文总数，非法报文包括：报文碎片、jabber 帧、符号错误帧、操作码未知帧、长度错误帧。
- **ignored**：由于端口接收缓冲区不足等原因而丢弃的报文数量。
- **parity errors**：接收到的奇偶校验错误的帧的数量。

2. 端口出方向报文计数错误字段解释

- **output errors**：各种发送错误的报文总数。
- **underruns**：当端口的发送速率超过了发送队列的处理能力，导致报文被丢弃，是一种非常少见的硬件异常。
- **buffer failures**：由于端口发送缓冲区不足而丢弃的报文数量。
- **aborts**：发送失败的报文总数，即报文已经开始发送，但由于各种原因（如冲突）而导致发送失败。
- **deferred**：延迟报文的数量，延迟报文是指发送前检测到冲突而被延迟发送的报文。
- **collisions**：冲突帧的数量，冲突帧是指在发送过程中检测到冲突的而停止发送的报文。
- **late collisions**：延迟冲突帧的数量，延迟冲突帧是指帧的前 512 bits 已经被发送，由于检测到冲突，该帧被延迟发送。

- **lost carrier**：载波丢失，一般适用于串行 WAN 接口，发送过程中，每丢失一个载波，此计数器加一。
- **no carrier**：无载波，一般适用于串行 WAN 接口，当试图发送帧时，如果没有载波出现，此计数器加一。

4.1.2 故障处理步骤

1. 端口入方向出现 CRC、frame、throttles 错包且计数持续增加

(1) 使用仪器测试链路，链路质量差或者线路光信号衰减过大会导致报文在传输过程中出错。如链路故障请更换网线或光纤。

(2) 如端口使用光模块，参照 4.4 光模块故障认是否光模块故障导致。

(3) 与别的正常的端口更换网线或光纤光模块，如端口更换后错包消失，端口更换回来错包又再次出现端口相关，应为单板端口故障，请更换端口并将故障信息发送技术支持人员分析；如更换到其他正常端口仍会出现错包，则对端设备、中间传输链路故障的可能性较大，请排查。

(4) 排查对端设备或者中间的传输设备。

(5) 如故障无法确认，请将故障信息发送技术支持人员分析。

2. 端口入方向出现 giants 错包且计数持续增加

(1) 检查两端的 jumbo 配置是否一致，如 jumbo 是否使能，端口默认的最大报文长度是否一致，允许最大报文长度是否一致。

(2) 如果仍然无法确认，请将故障信息发送技术支持人员分析。

3. 端口出方向出现错包且计数持续增加

(1) 检查端口是否配置为半双工模式，如为半双工，请更改为全双工模式。

(2) 如果仍然无法确认，请将故障信息发送技术支持人员分析。

4.2 端口无法UP

4.2.1 故障描述

端口无法正常 UP。

4.2.2 故障处理步骤

1. 端口无法 UP

(1) 测试端口之间网线、光纤链路是否正常，光纤两端的发送/接收端是否错连；更换端口之间的网线、光纤或将网线、光纤放到别的正常端口，以确认是否中间传输链路故障

(2) 检查本端、对端端口配置是否正确，如端口是否 shutdown，速率、双工、协商模式、MDI 是否正确。

表3 双工支持情况：

Speed / Duplex	10G	1000M	100M	10M
Full	Not supported	Supported	Supported	Supported

Speed Duplex	10G	1000M	100M	10M
Half	Not supported	Not supported	Supported	Supported

(3) 如端口使用光模块，请检查两端光模块类型是否一致，如速率、波长、单模多模状态等；与正常的光模块交叉更换，并参照 4.4 光模块故障排除是否为光模块故障导致。

```
<H3C>display transceiver interface GigabitEthernet 1/0/17
GigabitEthernet1/0/17 transceiver information:
  Transceiver Type              : 1000_BASE_SX_SFP
  Connector Type                : LC
  Wavelength(nm)                : 850
  Transfer Distance(m)          : 550(OM2),270(OM1)
  Digital Diagnostic Monitoring : YES
  Vendor Name                   : JDSU
```

如果确认光模块有问题，需要更换光模块。

4.2.3 故障处理步骤

(1) 查看本设备及对端设备日志，确认有无端口 **shutdown** 操作。

(2) 查看两端端口状态，确认是否为协议异常或在线诊断模块检测到异常将端口 **shutdown**。当设备在线诊断模块检测到端口故障时，将端口 **shutdown** 隔离，以便流量切换到备份链路。请将故障信息发送技术支持人员分析。

```
<H3C> display interface GigabitEthernet 1/0/2
GigabitEthernet1/0/2
Current state: DOWN
Line protocol state: DOWN
Description: GigabitEthernet1/4/0/1 Interface
Bandwidth: 1000000kbps
Maximum Transmit Unit: 1500
Internet protocol processing: disabled
IP Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: 8042-0004-5601
IPv6 Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: 8042-0004-5601
Media type is not sure,Port hardware type is No connector
Last clearing of counters: 16:45:01 Wed 12/11/2013
Peak value of input: 0 bytes/sec, at 2013-12-11 16:45:03
Peak value of output: 0 bytes/sec, at 2013-12-11 16:45:03
Last 300 second input:  0 packets/sec 0 bytes/sec
Last 300 second output:  0 packets/sec 0 bytes/sec
```

(3) 参照 4.2 端口无法，排查两端端口配置，网线、光模块、光纤等链路是否正常。

(4) 如仍无法确认，请搜集本端、对端设备信息，并将信息发送技术支持人员分析。

4.3 端口频繁UP/Down

4.3.1 故障描述

端口频繁 UP/Down。

4.3.2 故障处理步骤

(1) 对于光口，请参照 4.4 光模块故障确认光模块是否异常。

(2) 对于电口，一般在自协商情况下容易出现协商不稳定，这种情况请尝试设置强制速率双工。

(3) 如仍无法确认，请将故障信息发送技术支持人员分析。

4.4 光模块故障

4.4.1 故障描述

安装光模块的接口不能正常 UP，出现告警信息。

4.4.2 故障处理步骤

(1) 检查是否万兆光口插入了千兆光模块，该使用方式不支持，请对应接口类型选择光模块。

(2) 检查光模块 Alarm 告警信息。告警信息中如果存在接收有问题那一般是对端端口、光纤或中转传输设备导致；如果是发送有问题或者电流、电压异常那就需要排查本端端口。

```
<H3C> display transceiver alarm interface Ten-GigabitEthernet 1/0/25
Ten-GigabitEthernet1/0/25 transceiver current alarm information:
  RX signal loss
```

表4 光模块告警信息说明

字段	描述
SFP/SFP+	
RX loss of signal	接收信号丢失
RX power high	接收光功率高告警
RX power low	接收光功率低告警
TX fault	发送错误
TX bias high	偏置电流高告警
TX bias low	偏置电流低告警
TX power high	发送光功率高告警
TX power low	发送光功率低告警
Temp high	温度高告警
Temp low	温度低告警
Voltage high	电压高告警

字段	描述
Voltage low	电压低告警
Transceiver info I/O error	模块信息读写错误
Transceiver info checksum error	模块信息校验和错误
Transceiver type and port configuration mismatch	模块类型和端口配置不匹配
Transceiver type not supported by port hardware	端口不支持该模块类型
XFP	
RX loss of signal	接收信号丢失
RX not ready	接收状态未就绪
RX CDR loss of lock	RX CDR时钟失锁
RX power high	接收光功率高告警
RX power low	接收光功率低告警
TX not ready	发送状态未就绪
TX fault	发送错误
TX CDR loss of lock	TX CDR时钟失锁
TX bias high	偏置电流高告警
TX bias low	偏置电流低告警
TX power high	发送光功率高告警
TX power low	发送光功率低告警
Module not ready	模块状态未就绪
APD supply fault	APD（Avalanche Photo Diode，雪崩光电二极管）错误
TEC fault	TEC（Thermoelectric Cooler，热电冷却器）错误
Wavelength unlocked	光信号波长失锁
Temp high	温度高告警
Temp low	温度低告警
Voltage high	电压高告警
Voltage low	电压低告警
Transceiver info I/O error	模块信息读写错误
Transceiver info checksum error	模块信息校验错误

字段	描述
Transceiver type and port configuration mismatch	模块类型和端口配置不匹配
Transceiver type not supported by port hardware	端口不支持该模块类型

(3) 对怀疑故障的光模块进行交叉验证，如更换端口、与正常的光模块互换，确认是光模块本身故障还是相邻设备或中间链路故障。

(4) 如果确认是光模块本身故障，请通过 **display transceiver diagnosis** 命令收集光模块当前的数字诊断信息（非 H3C 定制光模块可能无法查询到数字诊断信息），并发送给技术支持人员分析。

```
<H3C>display transceiver diagnosis interface GigabitEthernet 1/0/17
GigabitEthernet1/0/17 transceiver diagnostic information:
  Current diagnostic parameters:
    Temp.(°C) Voltage(V)  Bias(mA)  RX power(dBm)  TX power(dBm)
    54        3.35        5.39      -5.91          -5.29
  Alarm thresholds:
           Temp.(°C) Voltage(V)  Bias(mA)  RX power(dBm)  TX power(dBm)
    High   73        3.80        11.00     0.00           0.00
    Low    -3        2.81        1.00      -16.99         -12.52
<H3C>
```

(5) 建议使用 H3C 定制光模块。可以使用 **display transceiver manuinfo interface** 命令来查看光模块制造厂家信息。

```
<H3C>display  transceiver manuinfo interface
GigabitEthernet1/0/16 transceiver manufacture information:
The transceiver is absent.
GigabitEthernet1/0/17 transceiver manufacture information:
The transceiver does not support this function.
GigabitEthernet1/0/18 transceiver manufacture information:
The transceiver is absent.
GigabitEthernet1/0/19 transceiver manufacture information:
The transceiver is absent.
GigabitEthernet1/0/20 transceiver manufacture information:
The transceiver is absent.
GigabitEthernet1/0/21 transceiver manufacture information:
The transceiver is absent.
GigabitEthernet1/0/22 transceiver manufacture information:
The transceiver is absent.
GigabitEthernet1/0/23 transceiver manufacture information:
The transceiver is absent.
GigabitEthernet2/0/16 transceiver manufacture information:
The transceiver is absent.
GigabitEthernet2/0/17 transceiver manufacture information:
The transceiver does not support this function.
GigabitEthernet2/0/18 transceiver manufacture information:
The transceiver is absent.
GigabitEthernet2/0/19 transceiver manufacture information:
```

```
The transceiver is absent.
GigabitEthernet2/0/20 transceiver manufacture information:
The transceiver is absent.
GigabitEthernet2/0/21 transceiver manufacture information:
The transceiver is absent.
GigabitEthernet2/0/22 transceiver manufacture information:
The transceiver is absent.
GigabitEthernet2/0/23 transceiver manufacture information:
The transceiver is absent.
```

4.5 故障诊断命令

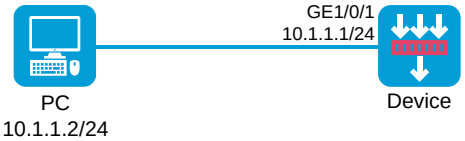
命令	说明
display current-configuration	显示设备当前生效的配置，指定interface可以显示指定接口当前生效的配置
display interface	查询端口的入、出方向流量统计信息、端口状态。可查看是否存在错包及错包统计信息。
display transceiver alarm	显示可插拔接口模块的当前故障告警信息
display transceiver diagnosis	显示可插拔光模块的数字诊断参数的当前测量值，包括温度、电压、偏置电流、接收光功率、发送光功率
display transceiver interface	显示指定接口可插拔接口模块的主要特征参数。检查两端光模块类型是否一致，如速率、波长、单模多模状态等
display transceiver manuinfo	显示可插拔接口模块的电子标签信息。可用来查询光模块的定制厂商。

5 报文转发故障处理

5.1 PC与设备直连，无法访问Ping通设备

5.1.1 故障描述

PC 通过网线与设备业务接口相连，IP 地址为同一网段，在 PC 上无法 Ping 通设备。



5.1.2 故障处理步骤

1. 安全域和安全策略配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“网络 > 安全域”。

(3) 单击某个安全域（如 Trust）对应的<编辑>按钮，进入“修改安全域”页面。

(4) 选择接口列表中与 PC 相连的接口，单击<→>按钮添加至成员列表中。

(5) 单击<确定>按钮。

(6) 选择“策略 > 安全策略 > 安全策略”。

(7) 在“安全策略”页面单击<新建>按钮，选择新建策略，进入“新建安全策略”页面。

(8) 配置安全策略的匹配条件及执行动作：

a. 源安全域：Trust

b. 名称：trust-local

c. 目的安全域：Local

d. 动作：允许

e. 源 IPv4 地址：10.1.1.2

f. 目的 IPv4 地址：10.1.1.1

(9) 若需要设备主动访问 PC，则需要配置反方向放行的安全策略：

a. 名称：local-trust

b. 源安全域：Local

c. 目的安全域：Trust

d. 动作：允许

e. 源 IPv4 地址：10.1.1.1

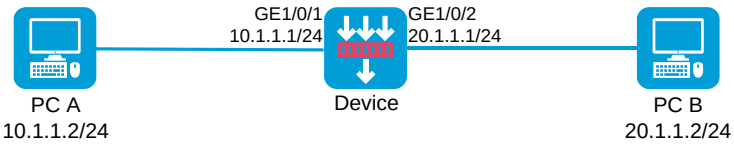
f. 目的 IPv4 地址：10.1.1.2

(10) 单击<确定>按钮，完成配置。

5.2 PC通过设备与其他终端连接，无法互相访问

5.2.1 故障描述

PC 通过与设备其他终端相连，IP 地址与路由已正确配置，但无法互相访问。



5.2.2 故障处理步骤

1. 安全域和安全策略配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“网络 > 安全域”。

(3) 单击某个安全域（如 Trust）对应的<编辑>按钮，进入“修改安全域”页面。

(4) 选择接口列表中与 PC 相连的接口，单击<→>按钮添加至成员列表中。

(5) 单击<确定>按钮。

(6) 采用同样的方法将其他接口加入不同安全域（如 Untrust）。

(7) 选择“策略 > 安全策略 > 安全策略”。

(8) 在“安全策略”页面单击<新建>按钮，选择新建策略，进入“新建安全策略”页面。

(9) 配置安全策略的匹配条件及执行动作（建议配置精确的匹配条件）：

a. 名称：trust-untrust

b. 源安全域：Trust

c. 目的安全域：Unturst

d. 动作：允许

e. 源 IPv4 地址：10.1.1.2

f. 目的 IPv4 地址：20.1.1.2

(10) 若通过设备相连的终端需要互相访问，则需要创建双向放行的安全策略：

a. 名称：untrust-trust

b. 源安全域：Unturst

c. 目的安全域：Trust

d. 动作：允许

e. 源 IPv4 地址：20.1.1.2

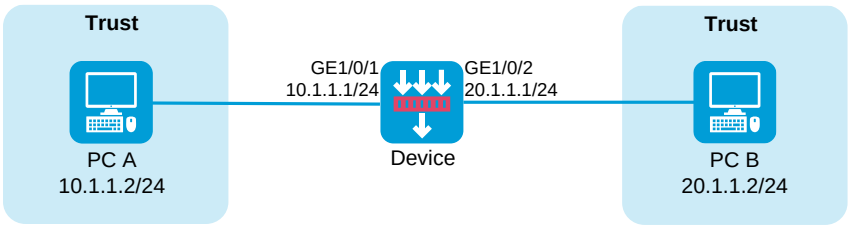
f. 目的 IPv4 地址：10.1.1.2

(11) 单击<确定>按钮，完成配置。

5.3 PC通过设备与其他终端连接，已配置在同一安全域，无法互相访问

5.3.1 故障描述

PC 通过与设备其他终端相连，IP 地址与路由已正确配置，且已加入相同的安全域，但无法互相访问。



5.3.2 故障处理步骤

1. 安全域和安全策略配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > 安全策略 > 安全策略”。

(3) 在“安全策略”页面单击<新建>按钮，选择新建策略，进入“新建安全策略”页面。

(4) 配置安全策略的匹配条件及执行动作（本例中通过设备相连的终端都属于 Trust 安全域）：

a. 名称：trust-trust

b. 源安全域：Trust

c. 目的安全域：Trust

d. 动作：允许

e. 源 IPv4 地址：10.1.1.2,20.1.1.2

f. 目的 IPv4 地址：20.1.1.2,10.1.1.2

g. 单击<确定>按钮，完成配置。

5.4 ping不通或丢包

5.4.1 故障描述

报文转发丢包，ping 不通或 ping 丢包，tracert 异常。

```
<H3C> ping 10.0.0.5
PING 10.0.0.5 (10.0.0.5): 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- 10.0.0.5 ping statistics ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

5.4.2 故障处理步骤

1. 确认参与转发的出入端口是否加入到安全域和设置了安全策略

对于有 M-GigabitEthernet 接口的设备，M-GigabitEthernet 接口默认加入到 Management 域，没有 M-GigabitEthernet 接口的设备，GigabitEthernet 1/0/0 默认加入到 Management 域，其它端口默认没有加入到任何安全域，要确认端口是否加入到安全域。

执行 **display security-zone** 命令，查看参与转发法的接口是否加入到了安全域内

```
<H3C>display security-zone
Name: Local
Members:
  None
Name: Trust
Members:
  GigabitEthernet1/0/8
  Reth1
Name: DMZ
Members:
  None
Name: Untrust
Members:
  GigabitEthernet1/0/10
  Reth2
Name: Management
Members:
  GigabitEthernet1/0/0
```

如果端口加入到安全域中，要确认是否配置了安全策略。

执行 **display security-policy** 命令，查看是否配置了安全策略

```
<H3C>display security-policy ip
Security-policy ip
 rule 0 name 1
  action pass
<H3C>display security-policy ipv6
Security-policy ipv6
 rule 0 name IPv6
  action pass
```

缺省情况下，创建安全域后，设备上各接口的报文转发遵循以下规则：

- 一个安全域中的接口与一个不属于任何安全域的接口之间的报文，会被丢弃。
- 属于同一个安全域的各接口之间的报文缺省会被丢弃。
- 安全域之间的报文由安全策略进行安全检查，并根据检查结果放行或丢弃。若安全策略不存在或不生效，则报文会被丢弃。
- 非安全域的接口之间的报文被丢弃。
- 目的地址或源地址为本机的报文，缺省会被丢弃，若该报文与安全策略匹配，则由安全策略进行安全检查，并根据检查结果放行或丢弃。

2. 设备入出报文统计

报文转发异常通常会涉及多台设备，需要逐一排查。为方便排查，排查前建议先明确报文的转发走向，如经过哪些中间设备，在设备的哪些接口进入设备，又会从哪些接口出去。检查出入接口的报文统计。确认统计是否正确。

检查入方向报文统计计数，可以通过 **reset counter interface** 命令清除计数

3. 报文计数分析

如果设备未收到 ping 报文，请排查上游的相邻设备；如果设备发送的 ping 报文计数正确，建议排查下游的相邻设备；如果 ping 报文入出计数不正确，分下面几种情况进行分析：

- 有入报文统计，没有出报文统计，进行如下排查

  a. 如果链路层处理没有丢包，执行 **display ip statistics** 命令，查看 IP 层丢包原因

```
<H3C> display ip statistics
  Input:    sum            263207520        local            1772
            bad protocol   0                bad format       0
            bad checksum   0                bad options      0
  Output:   forwarding     24511617         local            476
            dropped        21949            no route         156
            compress fails 0
  Fragment:input           0                output           0
            dropped        0
            fragmented     0                couldn't fragment 0
  Reassembling:sum         0                timeouts         0
```

  b. 打开 debugging aspf packet acl、debugging aspf event 来确定 aspf 是否有丢包

- 无出、入报文统计

需要查看上游相邻设备出接口报文统计，分析是否上游没有把报文发送过来。

5.5 有NAT转换情况下，ping丢包或不通

5.5.1 故障描述

处于不同网段的两台 PC：PC1 和 PC2，PC1 的地址为 10.1.1.1，PC2 的地址为 220.1.1.2。

中间穿越 FW 设备互相 ping 包，FW 设备对 PC1 的地址静态 NAT 转换为 220.1.1.1；发现 PC1 ping PC2 不通，查看 PC2 可以收到 PC1 的 ping 报文，但是 PC1 收不到 PC2 的回应报文。

5.5.2 故障处理步骤

1. 配置检查

确保 PC1 和 PC2 接入的端口加入了安全域，并且配置了安全策略。可以通过命令来查看是否配置了相关的安全策略：

```
<H3C> display security-policy ip
Security-policy ip

 rule 0 name tom-tom1
  action pass
  counting enable
  source-zone tom
  destination-zone tom1
```

2. 路由表检查

在 FW 上检查是否有到 PC1 的路由表项，如路由不存在，请检查路由协议配置、状态是否正确。

```
<H3C> display ip routing-table 10.1.1.0
```

3. FIB 表检查

在 FW 上检查是否有到 PC1 的 FIB 表项，如路由存在，FIB 表项异常，请将故障信息发送技术支持人员分析。

```
<H3C> display fib 10.1.1.0
```

4. arp 表项检查

在 FW 上查看 10.1.1.1 的 ARP 表项是否存在

```
<H3C> display arp 10.1.1.1
```

5. 会话表项检查

在 FW 上通过 **display session** 命令确认会话是否正常建立。

6. ASPF 检查

安全策略默认 ASPF 对所有的报文进行检测。但如果在安全策略中配置了 **aspf apply policy** 命令，那么只对策略中配置的 detect 协议进行 ASPF 检测，其他协议不进行检测。如果不配置 **detect icmp**，也没有配置反向安全策路，报文就被 deny 了。可以在 FW 上使用下面命令打开 debug：

```
<H3C> debugging security-policy packet ip acl ?
  INTEGER<2000-2999>  Specify a basic ACL
  INTEGER<3000-3999>  Specify an advanced ACL
```

来看是否有 deny 信息，如果有类似下面信息：

```
*Jul 21 11:00:00:838 2017 F1090-IRF FILTER/7/PACKET: -Context=1; The packe
```

```
t is deny. Src-Zone=tom1, Dst-Zone=tom;If-In=, If-Out=Reth11(134); Packet
Info:Src-IP=220.1.1.2, Dst-IP=10.1.1.1, VPN-Instance=,Src-Port=1024, Dst-Port=1025,
Protocol= UDP(17), ACL=none, Rule-ID=0.
```

说明没有正确配置 aspf 策略，导致被反向安全策略 deny 了。

5.6 设备在转发过程中，有丢包现象

5.6.1 故障描述

设备在转发报文过程中，发现存在丢包现象。

5.6.2 故障处理步骤

(1) 执行 **debugging security-policy packet**，确认是否存在丢包。

```
<H3C>*Jan 13 16:06:32:298 2020 8350-2 FILTER/7/PACKET: -Context=1; The packet is denied.
Src-Zone=Untrust, Dst-Zone=Trust;If-In=GigabitEthernet1/0/14(17),
If-Out=GigabitEthernet1/0/10(13); Packet Info:Src-IP=10.1.1.3, Dst-IP=100.1.1.3,
VPN-Instance=, Src-MacAddr=3897-d6a9-1e58,Src-Port=1024, Dst-Port=1024, Protocol=TCP(6),
Application=general_tcp(2086),Terminal=invalid(0), SecurityPolicy=r0, Rule-ID=0.
```

如果存在 The packet is denied 字段，说明存在由于安全策略导致的丢包。

(2) 打开 **debugging ip packet** 调试命令，确认是否有丢包。

该命令用来打开 ip 报文转发调试开关。该报文的调试信息各字段解释如下

字段	描述
Sending	发送报文的操作
Receiving	接收报文的操作
Delivering	IP层将报文送到上层
interface	接收/发送报文的接口
version	IP协议版本号
headlen	报文首部长度
tos	服务类型
pktlen	报文总长度
pktid	标识
offset	片偏移
ttl	生存时间
protocol	协议域
checksum	首部校验和
s	报文源地址
d	报文目的地址
Sending the packet from local at *interface-type interface-number*	从本地接口发送报文

字段	描述
Receiving IP packet from *interface-type interface-number*	从接口接收到报文
IP packet is delivering up!	将接收的报文送到上层处理

可以通过该信息来分析报文是否丢弃。

(3) 打开调试命令 **debugging ip error**，**debug ip info acl** 查看丢包的原因。

该命令用来打开 IP 转发错误调试信息开关。调试信息字段描述如下：

字段	描述
The number of queues of reassemble is MAX!	重组队列数目超过了总的重组队列数目
The queue of reassemble is full!	重组队列中分片数目超过了最大值
Reassemble Failed!	重组失败
Get Interface CB failed!	从接口管理获取转发控制块失败
Release MBUF! Phase Num is *num*, Service ID is *id*, Bitmap is *%#lx*!	业务释放报文，业务阶段、顺序号、以及当前业务掩码位
Broadcast NOT allowed to be forwarded!	不允许出接口子网广播报文转发
Error interface is assigned!	上层指定了错误的发送接口

通过 debugging 信息来判断丢包的原因。

5.7 故障诊断命令

命令	说明
display arp	显示ARP表项。检查设备ARP学习的接口是否正确
display current-configuration | include lsr-id	显示当前的MPLS LSR ID
display fib	显示FIB信息。检查设备到某一目的IP网段的FIB表项是否存在
display interface	显示指定接口的相关信息
display ip interface brief	显示三层接口的IP基本配置信息
display ip routing-table	显示路由表中当前激活路由的摘要信息。检查设备到某一目的IP网段的路由是否存在
display session	显示会话信息
display this	显示当前视图下生效的配置
interface	进入接口视图
dis nat outbound	查看nat outbound配置信息

6 IRF 类故障处理

6.1 IRF无法形成

6.1.1 故障描述

IRF 无法正常建立。

6.1.2 故障处理步骤

1. 确认设备型号是否一致，两台设备的型号应一致。

通过 **display version** 查看设备型号是否一致。

```
<H3C>display version
H3C Comware Software, Version 7.1.064, Ess 8601P08
Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.
H3C SecPath F1090 uptime is 0 weeks, 0 days, 0 hours, 5 minutes
Last reboot reason: User reboot

Boot image: flash:/F1090FW-CMW710-BOOT-E8601P08.bin
Boot image version: 7.1.064, Ess 8601P08
  Compiled Sep 10 2019 15:00:00
System image: flash:/F1090FW-CMW710-SYSTEM-E8601P08.bin
System image version: 7.1.064, Ess 8601P08
  Compiled Sep 10 2019 15:00:00

SLOT 1
CPU type:            Multi-core CPU
DDR4 SDRAM Memory:    8192M bytes
FLASH:               7296M bytes
CPLD_A           Version:  1.0
CPLD_B           Version:  1.0
Release          Version:SecPath F1090-8601P08
Basic  BootWare  Version:0.30
Extend BootWare  Version:1.01
BuckleBoard Version:Ver.A
BackBoard1 Version:Ver.A
BackBoard2 Version:Ver.A
HD_BackBoard Version:Ver.D
Pcb Version:Ver.A
[SUBCARD 0] NSQ1F1MSPUOTXA(Hardware)Ver.A, (Driver)1.0, (Cpld)1.0
Boot Type: Warm
[H3C]isplay  system internal  version
H3C SecPath F1090 V800R006B01D645SP08
Comware V700R001B64D045SP08
```

2. 确认成员设备数目超过 IRF 支持的最大成员设备数目

目前防火墙设备 IRF 最多支持两台设备。

3. 确认成员设备的成员编号是否不唯一。

通过 **display irf** 命查看设备成员编号 MemberID，两台设备的成员编号应不同，否则通过 **irf member** 命令修改成员编号。

```
<H3C>display  irf
MemberID    Role    Priority  CPU-Mac         Description
 *+1        Master  1         00ff-fbec-b003  ---
--------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The bridge MAC of the IRF is: 00ff-fbec-b001
 Auto upgrade                : yes
 Mac persistent              : 6 min
   Domain ID                   : 0
```

4. 确认是否选用了不能作为 IRF 物理端口的端口作为 IRF 物理端口。

通过查看产品规格限制，确认选用的 IRF 物理端口是否支持作为 IRF 物理端口。

5. 确认成员设备的软件版本是否一致，两台设备应使用相同的软件版本。

```
<H3C>display version
H3C Comware Software, Version 7.1.064, Ess 8601P08
Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.
H3C SecPath F1090 uptime is 0 weeks, 0 days, 0 hours, 5 minutes
Last reboot reason: User reboot

Boot image: flash:/F1090FW-CMW710-BOOT-E8601P08.bin
Boot image version: 7.1.064, Ess 8601P08
  Compiled Sep 10 2019 15:00:00
System image: flash:/F1090FW-CMW710-SYSTEM-E8601P08.bin
System image version: 7.1.064, Ess 8601P08
  Compiled Sep 10 2019 15:00:00

SLOT 1
CPU type:           Multi-core CPU
DDR4 SDRAM Memory:   8192M bytes
FLASH:              7296M bytes
CPLD_A           Version:  1.0
CPLD_B           Version:  1.0
Release          Version:SecPath F1090-8601P08
Basic  BootWare  Version:0.30
Extend BootWare  Version:1.01
BuckleBoard Version:Ver.A
BackBoard1 Version:Ver.A
BackBoard2 Version:Ver.A
HD_BackBoard Version:Ver.D
```

```
Pcb Version:Ver.A
[SUBCARD 0] NSQ1F1MSPUOTXA(Hardware)Ver.A, (Driver)1.0, (Cpld)1.0
Boot Type: Warm
[H3C]isplay  system internal  version
H3C SecPath F1090 V800R006B01D645SP08
Comware V700R001B64D045SP08
```

6. 确认 IRF 物理端口是否 UP。

通过 **display interface** 查询 IRF 物理端口状态是否 UP，若端口为 DOWN，应先检查端口不 UP 的原因，请参照 4.2 端口无法 UP。

```
<H3C> display interface GigabitEthernet 1/0/10
GigabitEthernet1/0/10
Current state: UP
Line protocol state: UP
Description: GigabitEthernet1/0/10 Interface
Bandwidth: 1000000kbps
Maximum Transmit Unit: 1500
Internet protocol processing: disabled
IP Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: 8042-0000-560a
IPv6 Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: 8042-0000-560a
Media type is twisted pair
Port hardware type is 1000_BASE_T
Last clearing of counters: Never
Peak value of input: 0 bytes/sec, at 2013-12-13 15:15:02
Peak value of output: 0 bytes/sec, at 2013-12-13 15:15:02
Last 300 seconds input:  0 packets/sec 0 bytes/sec
Last 300 seconds output:  0 packets/sec 0 bytes/sec
```

7. 确认 IRF 端口连接是否异常，一台设备的 IRF-Port1 口只能与另一台设备的 IRF-Port2 口连接。

```
<H3C> display irf configuration
```

6.2 IRF出现分裂

6.2.1 故障描述

IRF 运行过程中出现分裂。

6.2.2 故障处理步骤

(1) IRF 分裂时会打印 IRF 端口 down，可以确定 IRF 分裂的时间。

```
%Jun 26 10:13:46:233 2013 H3C STM/2/STM_LINK_STATUS_TIMEOUT: IRF port 1 is down because
heartbeat timed out.
%Jun 26 10:13:46:436 2013 H3C STM/3/STM_LINK_STATUS_DOWN: -MDC=1; IRF port 2 is down.
```

(2) 检查各个 IRF 物理端口的状态是否正常。若端口状态不正常，请按照 3 硬件类故障处理

(3) 确认故障原因。

```
<H3C> display interface GigabitEthernet1/0/10
GigabitEthernet1/0/10 current state: UP
Line protocol current state: UP
```

```
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0000-e80d-c000
Description: GigabitEthernet2/6/0/1 Interface
Loopback is not set
Media type is optical fiber, Port hardware type is 1000_BASE_SX_SFP
……
```

(4) 如果设备存在接口板，通过设备运行时间或日志检查 IRF 中各个成员设备及 IRF 物理端口所在的接口板在 IRF 分裂时是否重启过，确认是否为电源故障导致。

(5) 如故障确认，可以通过如更换光模块、更换 IRF-Port 端口的方式使设备重新形成 IRF。

(6) 如故障无法确认，请搜集各个成员设备的信息，并将信息发送给 H3C 技术支持人员协助分析。

6.3 故障诊断命令

表5 故障诊断命令

命令	说明
display device	显示设备信息用于检查各成员设备的软件版本、主控板类型是否一致
display interface	显示指定接口的相关信息用于检查IRF物理端口状态是否UP
display irf configuration	显示所有成员设备的IRF配置信息用于检查IRF端口连接是否异常，一台设备的IRF-Port1口只能与另一台设备的IRF-Port2口连接
display version	显示系统版本信息、单板的运行时间通过设备运行时间确认IRF中各个成员设备是否重启过，主控板及IRF端口所在接口板是否发生重启

7 RBM 类故障处理

7.1 RBM无法形成

7.1.1 故障描述

RBM 无法正常建立。

7.1.2 故障处理步骤

1. 确认设备型号是否一致，两台设备的型号应一致。

通过 **display version** 查看设备型号是否一致。

```
<H3C>display version
H3C Comware Software, Version 7.1.064, Feature 8660P08
Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.
H3C SecPath F1000-AI-60 uptime is 0 weeks, 1 day, 17 hours, 11 minutes
Last reboot reason: User reboot

Boot image: flash:/F1090FW-CMW710-BOOT-F8660P08.bin
Boot image version: 7.1.064, Feature 8660P08
  Compiled Jan 18 2021 15:00:00
System image: flash:/F1090FW-CMW710-SYSTEM-F8660P08.bin
```

```
System image version: 7.1.064, Feature 8660P08
  Compiled Jan 18 2021 15:00:00
Feature image(s) list:
  flash:/F1090FW-CMW710-DEVKIT-F8660P08.bin, version: 7.1.064
    Compiled Jan 18 2021 15:00:00
  flash:/F1090FW-CMW710-SECESCAN-F8660P08.bin, version: 7.1.064
    Compiled Jan 18 2021 15:00:00

SLOT 1
CPU type:            Multi-core CPU
DDR4 SDRAM Memory:    8192M bytes
FLASH:               7296M bytes
CPLD_A           Version:  1.0
CPLD_B           Version:  2.0
Release          Version:SecPath F1000-AI-60-8660P08
Basic  BootWare  Version:1.07
Extend BootWare  Version:1.07
BuckleBoard Version:Ver.A
BackBoard1 Version:Ver.A
BackBoard2 Version:Ver.D
HD_BackBoard Version:Ver.A
Pcb Version:Ver.B
[SUBCARD 0] NSQ1F1MSPUOTXA(Hardware)Ver.B, (Driver)1.0, (Cpld)1.0
[SUBCARD 2] NSQM1TG4FBA(Hardware)Ver.B, (Driver)1.0, (Cpld)1.0
Boot Type: Warm
```

2. 确认 RBM 双机热备支持的最大成员设备数目

目前只支持两台设备进行双机热备。

3. 确认成员设备的成员编号是否唯一

通过 **display irf** 命查看设备成员编号 MemberID，两台设备的成员编号应相同，否则通过 **irf member** 命令修改成员编号。

```
<H3C>display  irf
MemberID    Role    Priority  CPU-Mac         Description
 *+1        Master  1         80e4-55d8-54ae  ---
--------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The bridge MAC of the IRF is: 80e4-55d8-54ac
 Auto upgrade               : yes
 Mac persistent             : 6 min
 Domain ID                  : 0
```

4. 确认是否选用了一致的设备端口作为 RBM 数据通道和控制通道

通过 display interface brief 查询设备成员接口，选择成员接口一致的接口作为 RBM 数据通道和控制通道。

5. 确认成员设备的软件版本是否一致，两台设备应使用相同的软件版本

```
<H3C>display version
H3C Comware Software, Version 7.1.064, Feature 8660P08
Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.
H3C SecPath F1000-AI-60 uptime is 0 weeks, 1 day, 17 hours, 11 minutes
Last reboot reason: User reboot

Boot image: flash:/F1090FW-CMW710-BOOT-F8660P08.bin
Boot image version: 7.1.064, Feature 8660P08
  Compiled Jan 18 2021 15:00:00
System image: flash:/F1090FW-CMW710-SYSTEM-F8660P08.bin
System image version: 7.1.064, Feature 8660P08
  Compiled Jan 18 2021 15:00:00
Feature image(s) list:
  flash:/F1090FW-CMW710-DEVKIT-F8660P08.bin, version: 7.1.064
    Compiled Jan 18 2021 15:00:00
  flash:/F1090FW-CMW710-SECESCAN-F8660P08.bin, version: 7.1.064
    Compiled Jan 18 2021 15:00:00

SLOT 1
CPU type:            Multi-core CPU
DDR4 SDRAM Memory:    8192M bytes
FLASH:               7296M bytes
CPLD_A           Version:  1.0
CPLD_B           Version:  2.0
Release          Version:SecPath F1000-AI-60-8660P08
Basic  BootWare  Version:1.07
Extend BootWare  Version:1.07
BuckleBoard Version:Ver.A
BackBoard1 Version:Ver.A
BackBoard2 Version:Ver.D
HD_BackBoard Version:Ver.A
Pcb Version:Ver.B
[SUBCARD 0] NSQ1F1MSPUOTXA(Hardware)Ver.B, (Driver)1.0, (Cpld)1.0
[SUBCARD 2] NSQM1TG4FBA(Hardware)Ver.B, (Driver)1.0, (Cpld)1.0
Boot Type: Warm
[H3C-probe]dis system internal version
H3C SecPath F1000-AI-60 V800R006B01D660SP08
Comware V700R001B64D060SP08
```

6. 确认 RBM 数据通道和控制通道接口是否 UP

通过 **display interface** 查询 RBM 通道接口状态是否 UP，若端口为 DOWN，应先检查端口不 UP 的原因，请参照 4.2 端口无法 UP。

```
<H3C>display interface GigabitEthernet 1/0/1
GigabitEthernet1/0/1
Current state: UP
Line protocol state: UP
Description: GigabitEthernet1/0/1 Interface
```

```
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
Allow jumbo frames to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
Internet protocol processing: Disabled
IP packet frame type: Ethernet II, hardware address: 80e4-55d8-54b3
IPv6 packet frame type: Ethernet II, hardware address: 80e4-55d8-54b3
Media type is twisted pair, loopback not set, promiscuous mode not set
1000Mb/s, Full-duplex, link type is autonegotiation
Output flow-control is disabled, input flow-control is disabled
Last link flapping: 1 days 17 hours 29 minutes
Last clearing of counters: Never
Current system time:2021-02-01 08:42:30 Beijing+08:00:00
Last time when physical state changed to up:2021-01-30 15:12:46 Beijing+08:00:00
Last time when physical state changed to down:2021-01-30 15:12:08 Beijing+08:00:00
 Peak input rate: 8499998 bytes/sec, at 2021-01-30 15:18:39
 Peak output rate: 5172061 bytes/sec, at 2021-01-30 15:12:53
 Last 300 second input: 0 packets/sec 22 bytes/sec 0%
 Last 300 second output: 0 packets/sec 25 bytes/sec 0%
```

7. 确认 RBM 控制通道连接是否异常，两台设备的控制通道对端端口必须相同

```
RBM_P[F1090]display remote-backup-group status
Remote backup group information:
  Backup mode: Dual-active
  Device role: Primary
  Data channel interface: Route-Aggregation64
  Local IPv6: 100::1
  Remote IPv6: 100::2    Destination port: 60064
  Control channel status: Connected
  Hot backup status:Enabled
  Auto configuration synchronization: Enable
  Configuration consistency check interval: 1 hour
  Delay-time: 1 min
```

7.2 RBM出现分裂

7.2.1 故障描述

RBM 双机运行过程中出现 RBM 通道分裂。

7.2.2 故障处理步骤

(1) RBM 分裂时会打印 RBM 端口 down，可以确定 RBM 分裂的时间。

```
RBM_P<F1010-VRRP-ZHU-1>%Feb          1     07:57:49:310     2021     F1010-VRRP-ZHU-1
LLDP/6/LLDP_DELETE_NEIGHBOR: Nearest bridge agent neighbor deleted
 on port GigabitEthernet1/0/7 (IfIndex 8), neighbor's chassis ID is d461-fe39-d20c, port
ID is GigabitEthernet1/0/7.
```

```
%Feb  1 07:57:50:487 2021 F1010-VRRP-ZHU-1 IFNET/3/PHY_UPDOWN: Physical state on the
interface GigabitEthernet1/0/7 changed to down.
%Feb  1 07:57:50:487 2021 F1010-VRRP-ZHU-1 IFNET/5/LINK_UPDOWN: Line protocol state on
the interface GigabitEthernet1/0/7 changed to
 down.
%Feb  1 07:58:00:269 2021 F1010-VRRP-ZHU-1 RBM/6/RBM_CHANNEL: Local IPv6=202::1, remote
IPv6=202::2, status=Disconnected
```

(2) 检查各个 RBM 物理端口的状态是否正常。若端口状态不正常，请按照 3 硬件类故障处理

(3) 确认故障原因。

```
RBM_P<F1010-VRRP-ZHU-1>display interface GigabitEthernet 1/0/7
GigabitEthernet1/0/7
Current state: UP
Line protocol state: UP
Description: link-f1010-bei
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
Allow jumbo frames to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
Internet address: 202.1.1.1/24 (Primary)
IP packet frame type: Ethernet II, hardware address: e8f7-24d9-2875
IPv6 packet frame type: Ethernet II, hardware address: e8f7-24d9-2875
Media type is twisted pair, loopback not set, promiscuous mode not set
1000Mb/s, Full-duplex, link type is autonegotiation
Output flow-control is disabled, input flow-control is disabled
Output queue - Urgent queuing: Size/Length/Discards 0/1024/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last link flapping: 0 hours 0 minutes 19 seconds
Last clearing of counters: Never
Current system time:2021-02-01 08:00:09
Last time when physical state changed to up:2021-02-01 07:59:51
Last time when physical state changed to down:2021-02-01 07:57:50
 Peak input rate: 1694290 bytes/sec, at 2021-01-30 14:35:26
 Peak output rate: 6245465 bytes/sec, at 2021-01-30 14:40:01
 Last 300 second input: 1 packets/sec 132 bytes/sec 0%
 Last 300 second output: 1 packets/sec 132 bytes/sec 0%
 Input (total):  2404856 packets, 808021430 bytes
```

(4) 如果设备存在接口板，通过设备运行时间或日志检查 RBM 双机环境中各个成员设备及 RBM 控制通道端口所在的接口板在 RBM 分裂时是否重启过，确认是否为电源故障导致。

(5) 如故障确认，可以通过如更换光模块、更换 RBM 控制通道端口的方式使设备重新形成 RBM。

(6) 如故障无法确认，请搜集各个成员设备的信息，并将信息发送给 H3C 技术支持人员协助分析。

8 双机热备故障处理

8.1 没有加入冗余组的冗余口直连无法ping通

8.1.1 故障描述

未加入冗余组的冗余口具有单独的冗余功能。冗余组只在接口 UP/DOWN 事件到来时进行激活切换。所有业务逻辑均基于冗余口实现，成员口只负责发送和接收报文。

问题集中在报文收发环节，存在冗余口直连无法 ping 通的情况。

8.1.2 故障处理步骤

1. 首先判断冗余口是否有报文收发，如果有，问题可能存在转发环节，请按如下操作定位：

(1) 打开 **debugging ethernet packet** 查看冗余口是否有报文上收与发送的调试信息对冗余口 1，采用如下命令：

```
debugging ethernet packet interface Reth 1
```

(2) 打开 **arp error debug** 命令查看是否存在错误信息采用如下 debug 命令：

```
debugging arp error
```

如果有错误信息，说明 ARP 学习异常。

(3) 打开 **ip error** 查看是否有错误信息采用如下 debug 命令：

```
debugging ip error
```

如果有错误信息，根据此信息来确定丢包的原因。

(4) 查看 **display ethernert statistics** 查看是否有错误计数随报文收发增长，命令如下：

```
[H3C] display ethernet statistics slot 1
ETH receive packet statistics:
    Totalnum        : 1000888       ETHIINum     : 1000888
    SNAPNum         : 0             RAWNum       : 0
    LLCNum          : 0             UnknownNum   : 0
    ForwardNum      : 884856        ARP          : 0
    MPLS            : 0             ISIS         : 0
    ISIS2           : 0             IP           : 0
    IPV6            : 0
ETH receive error statistics:
    NullPoint       : 0             ErrIfindex   : 3
    ErrIfcb         : 0             IfShut       : 5
    ErrAnalyse      : 0             ErrSrcMAC    : 0
    ErrHdrLen       : 0

ETH send packet statistics:
    L3OutNum        : 325126        VLANOutNum   : 0
    FastOutNum      : 92115615      L2OutNum     : 0
ETH send error statistics:
    MbufRelayNum    : 0             NullMbuf     : 0
    ErrAdjFwd       : 0             ErrPrepend   : 0
```

```
    ErrHdrLen        : 0              ErrPad        : 0
    ErrQosTrs        : 0              ErrVLANTrs    : 0
    ErrEncap         : 287            ErrTagVLAN    : 0
IfShut           : 0              IfErr         : 0
```

通过 **display ethernet statistics slot 2**，来查看成员设备的信息。

2. 如果冗余口没有报文信息，如下进行如下信息的确认

(1) 需要确认是否建立了冗余表项。查看命令如下：

```
<H3C>display reth interface Reth 1
Reth1 :
  Redundancy group  : fqs
  Member            Physical status         Forwarding status    Presence status
  GE1/1/1.500       UP                      Active               Normal
  GE2/0/1.500       UP                      Inactive             Normal
```

要分析Physical status状态，如果都为down，说明系统异常。分析Forwarding status状态，如果都为 Inactive 状态，说明成员口异常。

(2) 如果表项存在且成员状态正常，即部分报文能够上收，查看表项是否有错误。

可以通过 shutdown 冗余口，尝试刷新表项，看表项是否能够重新建立。如果冗余口的成员口为子接口，还需要查看表项是否带 tag。

(3) 如果冗余口、ARP 表项正常，需要确认驱动有没有上发报文，可查看物理接口计数，看报文是否已经上收。

3. 如果上述手段均无法定位，请联系 H3C 技术支持人员进行分析。

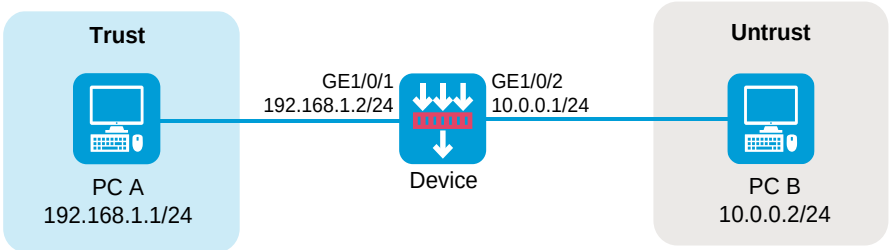
报文的收发一般都是双向的过程，A-B 两端报文需要互通，可以先确定是报文丢在哪一环，再针对某一环节进行定位。如 A-B 两端，可先 ping A->B 查看是否能 ping 通，再 ping B->A 查看是否能 ping 通。若两端都能通，则证明报文收发没问题。 某一端不能通， 以 B->A 为例，先看 B 是否将报文发出，定位方式按照以上步骤来，再看 A 是否上收，定位方式也是如此。

9 策略 NAT 故障处理

9.1 内网用户无法访问外网

9.1.1 故障描述

内网 PC A 无法通过网关设备 Device 访问外网 PC B



9.1.2 故障处理步骤

1. 安全策略配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > 安全策略 > 安全策略”。

(3) 在“安全策略”页面单击<新建>按钮，选择新建策略，进入“新建安全策略”页面，必要的配置项如下：

a. 名称：secpolicy1

b. 源安全域： Trust

c. 目的安全域：Untrust

d. 动作：允许

e. 源 IPv4 地址：192.168.1.1（此处为 PC A 的 IP 地址）

f. 目的 IPv4 地址：10.0.0.2（此处为 PC B 的 IP 地址）

(4) 单击<确定>，完成安全策略配置。

2. 策略 NAT 配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > NAT > NAT 策略”。

(3) 在“NAT 策略”页面单击<新建>，新建 NAT 策略规则，必要的配置项如下：

a. 规则名称：policy1

b. 转换模式：源地址转换

c. 源安全域： Trust

d. 目的安全域：Untrust

e. 源 IPv4 地址：192.168.1.1（此处为 PC A 的 IP 地址）

f. 目的 IPv4 地址：10.0.0.2（此处为 PC B 的 IP 地址）

g. 转换方式：PAT

h. 地址类型：地址组

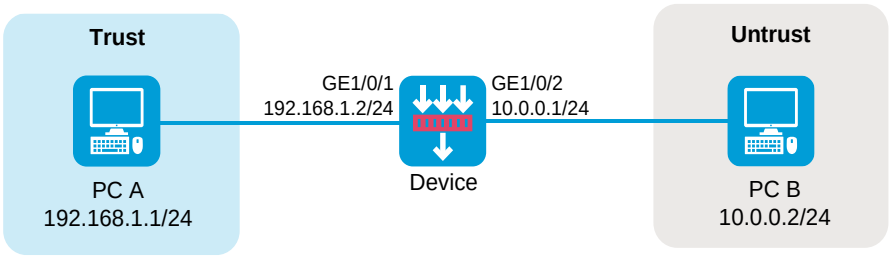
i. 转换后源地址：用于源 IP 地址转换的公网 NAT 地址组

(4) 单击<确定>，完成 NAT 策略规则配置。

9.2 NAT源地址转换不生效

9.2.1 故障描述

在网关设备 Device 上配置 NAT 源地址转换后，内网 PC A 无法访问外网 PC B。



9.2.2 故障处理步骤

1. 安全策略配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > 安全策略 > 安全策略”。

(3) 在“安全策略”页面单击<新建>按钮，选择新建策略，进入“新建安全策略”页面，必要的配置项如下：

a. 名称：secpolicy2

b. 源安全域： Trust

c. 目的安全域：Untrust

d. 动作：允许

e. 源 IPv4 地址：192.168.1.1（此处为 PC A 的 IP 地址）

f. 目的 IPv4 地址：10.0.0.2（此处为 PC B 的 IP 地址）

(4) 单击<确定>，完成安全策略配置。

2. 策略 NAT 配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > NAT > NAT 策略 ”。

(3) 在“NAT 策略”页面编辑 NAT 源地址转换规则。

(4) 查看该规则的转换后 IP 地址、网段、地址对象组或 NAT 地址组中是否包含不在 10.0.0.1/24 网段内的地址。

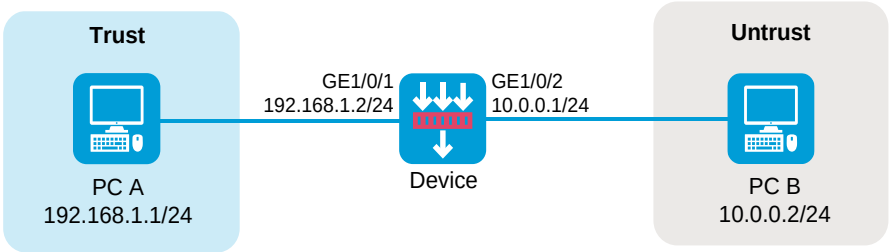
(5) 如存在上述情况，需修改转换后源地址配置，确保回程报文能被转发到 Device 的外网侧接口 GE1/0/2 上。

(6) 单击<确定>，完成 NAT 策略修改

9.3 NAT目的地址转换不生效

9.3.1 故障描述

在网关设备 Device 上配置 NAT 目的地址转换后，外网 PC B 无法访问内网 PC A。



9.3.2 故障处理步骤

1. 安全策略配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > 安全策略 > 安全策略”。

(3) 在“安全策略”页面单击<新建>按钮，选择新建策略，进入“新建安全策略”页面，必要的配置项如下：

a. 名称：secpolicy3

b. 源安全域： Untrust

c. 目的安全域：Trust

d. 动作：允许

e. 源 IPv4 地址：10.0.0.2（此处为 PC B 的 IP 地址）

f. 目的 IPv4 地址：192.168.1.1（此处为 PC A 的 IP 地址）

(4) 单击<确定>，完成安全策略配置。

2. 策略 NAT 配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > NAT > NAT 策略”。

(3) 在“NAT 策略”页面编辑 NAT 目的地址转换规则。

(4) 查看该规则所引用的服务匹配条件是否与实际情况不符。

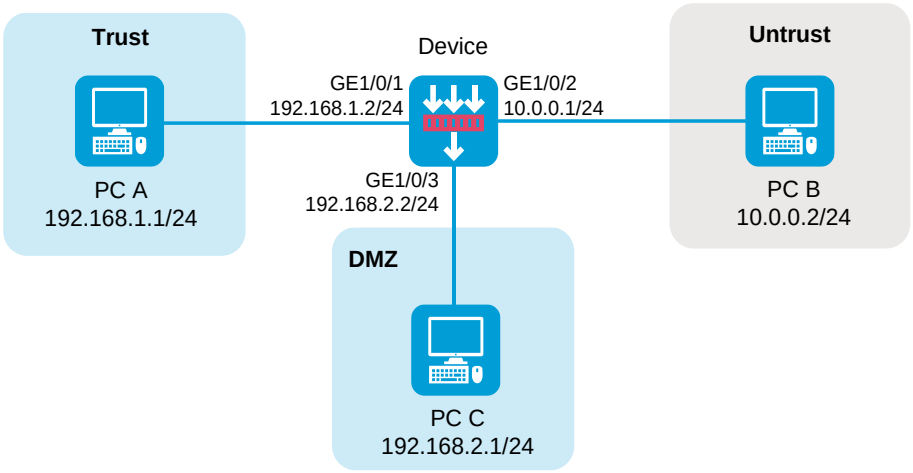
(5) 如存在上述情况，需修改服务匹配条件，确保与实际情况一致。

(6) 单击<确定>，完成 NAT 策略修改。

9.4 NAT源地址转换与NAT目的地址转换配合使用，NAT目的地址转换不生效

9.4.1 故障描述

B 在网关设备 Device 上配置 NAT 源地址转换与 NAT 目的地址转换（NAT Server）后，外网 PC B 无法通过外网地址 10.0.0.100 和目的端口 80 访问内网 PC C。



9.4.2 故障处理步骤

1. 安全策略配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > 安全策略 > 安全策略”。

(3) 在“安全策略”页面单击<新建>按钮，选择新建策略，进入“新建安全策略”页面，必要的配置项如下：

a. 名称：secpolicy4

b. 源安全域： Untrust

c. 目的安全域：DMZ

d. 动作：允许

e. 源 IPv4 地址：10.0.0.2（此处为 PC B 的 IP 地址）

f. 目的 IPv4 地址：192.168.2.1（此处为 PC C 的 IP 地址）

(4) 单击<确定>，完成安全策略配置。

2. 策略 NAT 配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > NAT > NAT 策略 ”。

(3) 在“NAT 策略”页面查看是否存在转换方式为 PAT 的源地址转换规则。

(4) 如存在上述规则，单击<编辑>，在修改 NAT 策略界面查看该规则引用的 NAT 地址组的端口范围是否包含 80。

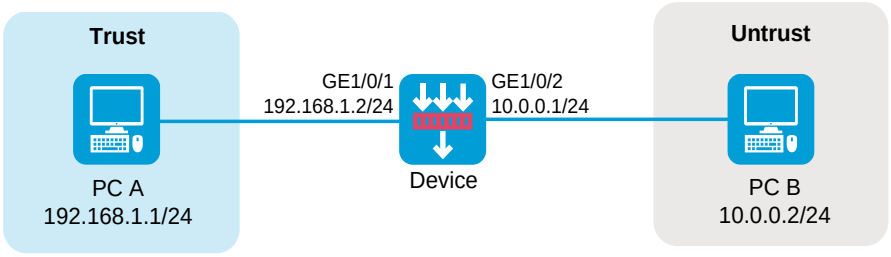
(5) 如包含在内，需要将端口 80 从端口范围中剔除。

(6) 单击<确定>，完成 NAT 策略修改。

9.5 NAT与IPsec配合使用，IPsec配置不生效

9.5.1 故障描述

在 Device 上配置 NAT 源地址转换和 IPsec 功能，对 PC A 访问 PC B 的报文进行 NAT 源地址转换后，利用 IPsec 保护其安全性。PC A 主动访问 PC B，发现 IPsec 配置不生效。



9.5.2 故障处理步骤

1. 匹配 IPsec 策略的报文源和目的 IP 地址需为 NAT 转换后的 IP 地址。

(1) 登录设备 Web 管理页面。

(2) 选择“网络 > VPN > IPsec > 策略 ”。

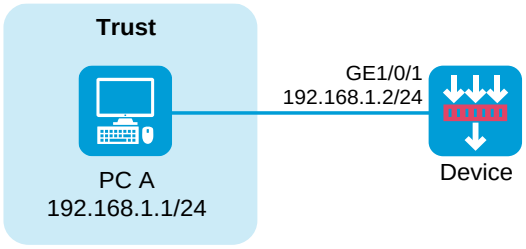
(3) 在“IPsec 策略”页面编辑 IPsec 策略配置。

(4) 查看 IPsec 策略配置中的被保护数据流配置，将被保护数据流的源和目的 IP 地址改为 NAT 转换后的 IP 地址。

9.6 配置策略NAT后，内网用户无法访问设备

9.6.1 故障描述

在网关设备 Device 上配置策略 NAT 后，内网 PC A 无法访问 Device。



9.6.2 故障处理步骤

1. 安全策略配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > 安全策略 > 安全策略”。

(3) 在“安全策略”页面单击<新建>按钮，选择新建策略，进入“新建安全策略”页面，必要的配置项如下：

a. 名称：secpolicy5

b. 源安全域： Trust

c. 目的安全域：Local

d. 动作：允许

e. 源 IPv4 地址：192.168.1.1（此处为 PC A 的 IP 地址）

f. 目的 IPv4 地址：192.168.1.2（此处为 Device 内网侧接口的 IP 地址）

(4) 单击<确定>，完成安全策略配置。

2. 策略 NAT 配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > NAT > NAT 策略 ”。

(3) 在“NAT 策略”页面查看是否存在报文目的安全域匹配条件为 ANY 的目的地址转换规则。

(4) 如存在上述规则，则需要重新配置该目的地址转换规则的报文匹配条件，具体要求如下：

(5) 目的安全域：不得包含 Local 安全域

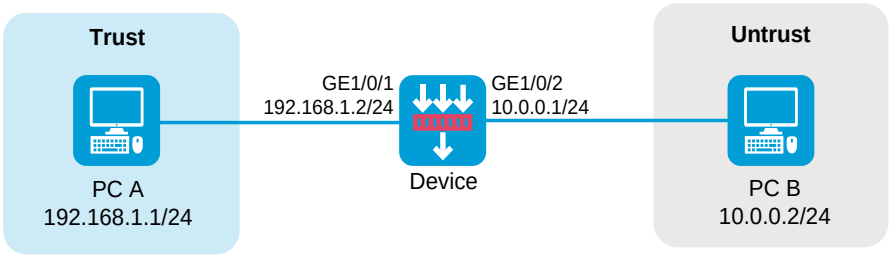
(6) 源 IPv4 地址：不得为 192.168.1.1

(7) 目的 IPv4 地址：不得为 192.168.1.2

9.7 配置NAT源地址转换后，外网用户无法访问设备

9.7.1 故障描述

在网关设备 Device 上配置 NAT 源地址转换后，外网 PC B 无法访问 Device。



9.7.2 故障处理步骤

1. 安全策略配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > 安全策略 > 安全策略”。

(3) 在“安全策略”页面单击<新建>按钮，选择新建策略，进入“新建安全策略”页面，必要的配置项如下：

a. 名称：secpolicy6

b. 源安全域： Untrust

c. 目的安全域：Local

d. 动作：允许

e. 源 IPv4 地址：10.0.0.2（此处为 PC B 的 IP 地址）

f. 目的 IPv4 地址：10.0.0.1（此处为 Device 外网侧接口的 IP 地址）

(4) 单击<确定>，完成安全策略配置。

2. 策略 NAT 配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > NAT > NAT 策略”。

(3) 在“NAT 策略”页面查看是否存在源地址转换方式为 NO-PAT 的 NAT 策略规则。

(4) 如存在上述规则，单击<编辑>，在修改 NAT 策略界面查看该规则所引用的用于源地址转换的地址对象组或 NAT 地址组中是否包含 Device 的外网侧接口 IP 地址 10.0.0.1。

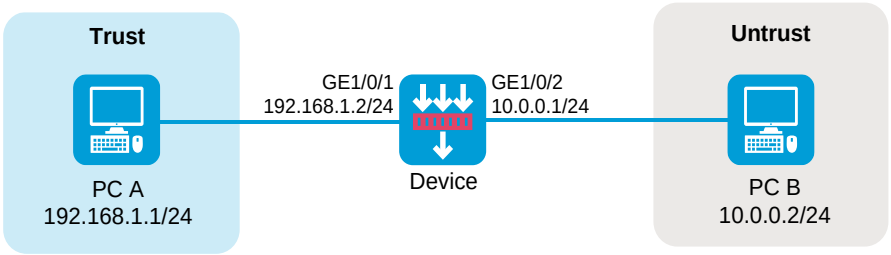
(5) 如包含在内，需要把 10.0.0.1 从该地址对象组或 NAT 地址组中剔除。

(6) 单击<确定>，完成 NAT 策略修改。

9.8 配置NAT目的地址转换后，外网用户无法访问设备

9.8.1 故障描述

在网关设备 Device 上配置 NAT 目的地址转换后，外网 PC B 无法访问 Device



9.8.2 故障处理步骤

1. 安全策略配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > 安全策略 > 安全策略”。

(3) 在“安全策略”页面单击<新建>按钮，选择新建策略，进入“新建安全策略”页面，必要的配置项如下：

a. 名称：secpolicy7

b. 源安全域： Untrust

c. 目的安全域：Local

d. 动作：允许

e. 源 IPv4 地址：10.0.0.2（此处为 PC B 的 IP 地址）

f. 目的 IPv4 地址：10.0.0.1（此处为 Device 外网侧接口的 IP 地址）

(4) 单击<确定>，完成安全策略配置。

2. 策略 NAT 配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > NAT > NAT 策略 ”。

(3) 在“NAT 策略”页面查看是否存在转换方式为多对一地址转换的目的地址转换规则。

(4) 如存在上述规则，单击<编辑>，在修改策略 NAT 界面查看目的地址匹配规则中是否包含 Device 的外网侧接口 IP 地址 10.0.0.1。

(5) 如包含在内，继续查看服务匹配规则中是否包含 PC B 访问 Device 时使用的服务。

(6) 如包含在内，请根据实际情况选择如下方式进行处理：

a. 改变 PC B 访问 Device 时使用的服务。

b. 把该服务从服务匹配规则中剔除，不对该服务进行目的地址转换。

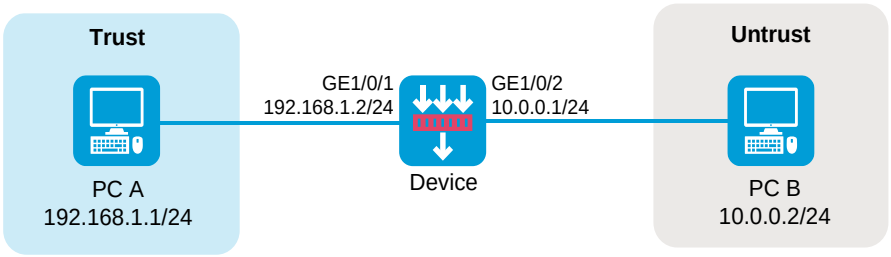
(7) 单击<确定>，完成 NAT 策略修改。

10 接口 NAT 故障处理

10.1 内网用户无法访问外网

10.1.1 故障描述

内网 PC A 无法通过网关设备 Device 访问外网 PC B



10.1.2 故障处理步骤

1. 安全策略配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > 安全策略 > 安全策略”。

(3) 在“安全策略”页面单击<新建>按钮，选择新建策略，进入“新建安全策略”页面，必要的配置项如下：

a. 名称：secpolicy1

b. 源安全域： Trust

c. 目的安全域：Untrust

d. 动作：允许

e. 源 IPv4 地址：192.168.1.1（此处为 PC A 的 IP 地址）

f. 目的 IPv4 地址：10.0.0.2（此处为 PC B 的 IP 地址）

(4) 单击<确定>，完成安全策略配置。

2. 接口 NAT 配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > NAT > NAT 动态转换 > 策略配置”。

(3) 在“NAT 出方向动态转换（基于 ACL）”页签单击<新建>，新建 NAT 出方向动态转换，必要的配置项如下：

a. 接口：GE1/0/2

b. ACL： 此处配置为放行 PC A 访问 PC B 报文的 ACL

c. 转换后源地址：NAT 地址组（此处配置为用于源 IP 地址转换的公网地址组）

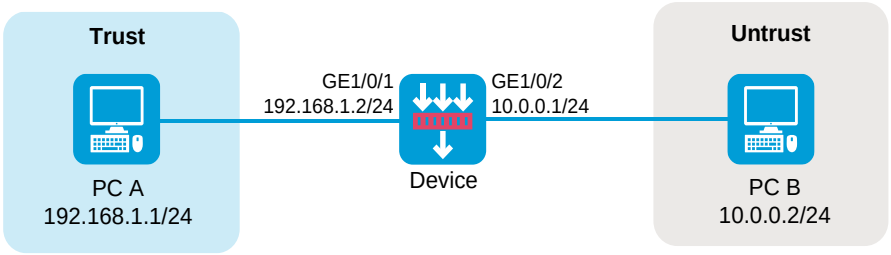
d. 转换模式：PAT

(4) 单击<确定>，完成 NAT 出方向动态转换配置。

10.2 NAT源地址转换不生效

10.2.1 故障描述

在网关设备 Device 上配置 NAT 源地址转换后，内网 PC A 无法访问外网 PC B。



10.2.2 故障处理步骤

1. 安全策略配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > 安全策略 > 安全策略”。

(3) 在“安全策略”页面单击<新建>按钮，选择新建策略，进入“新建安全策略”页面，必要的配置项如下：

a. 名称：secpolicy2

b. 源安全域： Trust

c. 目的安全域：Untrust

d. 动作：允许

e. 源 IPv4 地址：192.168.1.1（此处为 PC A 的 IP 地址）

f. 目的 IPv4 地址：10.0.0.2（此处为 PC B 的 IP 地址）

(4) 单击<确定>，完成安全策略配置。

(5) 接口 NAT 配置检查

(6) 登录设备 Web 管理页面。

(7) 选择“策略 > NAT > NAT 动态转换 > 策略配置 ”。

(8) 在右侧页签中编辑 NAT 源地址转换规则。

(9) 查看该规则的转换后 IP 地址、网段、地址对象组或 NAT 地址组中是否包含不在 10.0.0.1/24 网段内的地址。

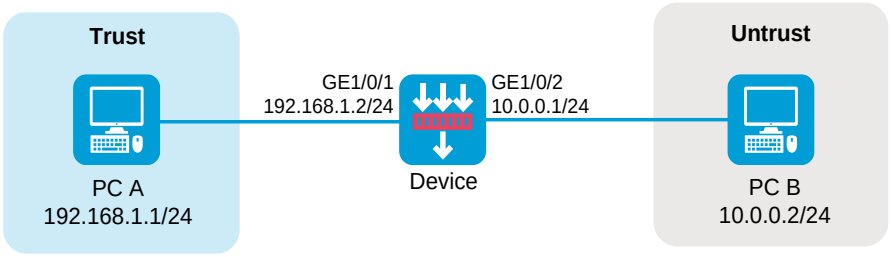
(10) 如存在上述情况，需修改转换后源地址配置，确保回程报文能被转发到 Device 的外网侧接口 GE1/0/2 上。

(11) 单击<确定>，完成接口 NAT 修改。

10.3 NAT目的地址转换不生效

10.3.1 故障描述

在网关设备 Device 上配置 NAT 目的地址转换后，外网 PC B 无法访问内网 PC A。



10.3.2 故障处理步骤

1. 安全策略配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > 安全策略 > 安全策略”。

(3) 在“安全策略”页面单击<新建>按钮，选择新建策略，进入“新建安全策略”页面，必要的配置项如下：

a. 名称：secpolicy3

b. 源安全域： Untrust

c. 目的安全域：Trust

d. 动作：允许

e. 源 IPv4 地址：10.0.0.2（此处为 PC B 的 IP 地址）

f. 目的 IPv4 地址：192.168.1.1（此处为 PC A 的 IP 地址）

(4) 单击<确定>，完成安全策略配置。

2. 接口 NAT 配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > NAT > NAT 内部服务器 > 策略配置”。

(3) 查看 NAT 内部服务器的外网端口是否与实际情况不符。

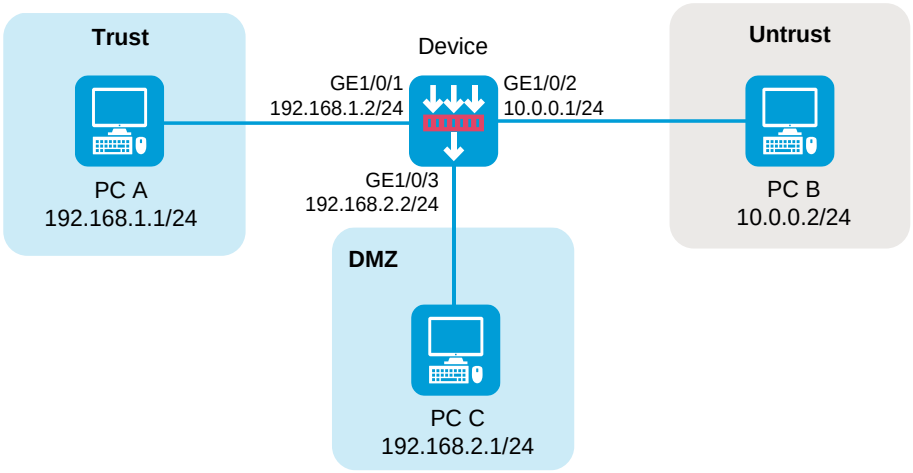
(4) 如存在上述情况，需修改端口匹配条件，确保与实际情况一致。

(5) 单击<确定>，完成接口 NAT 修改。

10.4 NAT源地址转换与NAT目的地址转换配合使用，NAT目的地址转换不生效

10.4.1 故障描述

在网关设备 Device 上配置 NAT 源地址转换与 NAT 目的地址转换（NAT Server）后，外网 PC B 无法通过外网地址 10.0.0.100 和目的端口 80 访问内网 PC C。



10.4.2 故障处理步骤

1. 安全策略配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > 安全策略 > 安全策略”。

(3) 在“安全策略”页面单击<新建>按钮，选择新建策略，进入“新建安全策略”页面，必要的配置项如下：

a. 名称：secpolicy4

b. 源安全域： Untrust

c. 目的安全域：DMZ

d. 动作：允许

e. 源 IPv4 地址：10.0.0.2（此处为 PC B 的 IP 地址）

f. 目的 IPv4 地址：192.168.2.1（此处为 PC C 的 IP 地址）

(4) 单击<确定>，完成安全策略配置。

2. 接口 NAT 配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > NAT > NAT 动态转换 > 策略配置”。

(3) 在“NAT 出方向动态转换（基于对象组）”页签中查看是否存在动作为 PAT 的转换规则。

(4) 如存在上述规则，单击<编辑>，在修改 NAT 出方向动态转换界面查看转换后源地址处引用的 NAT 地址组的端口范围是否包含 80。

(5) 如包含在内，需要将端口 80 从端口范围中剔除。

(6) 单击<确定>，完成 NAT 出方向动态转换规则修改。

(7) 在“NAT 出方向动态转换（基于 ACL）”页签中查看是否存在转换模式为 PAT 的转换规则。

(8) 如存在上述规则，单击<编辑>，在修改 NAT 出方向动态转换界面查看转换后源地址处引用的 NAT 地址组的端口范围是否包含 80。

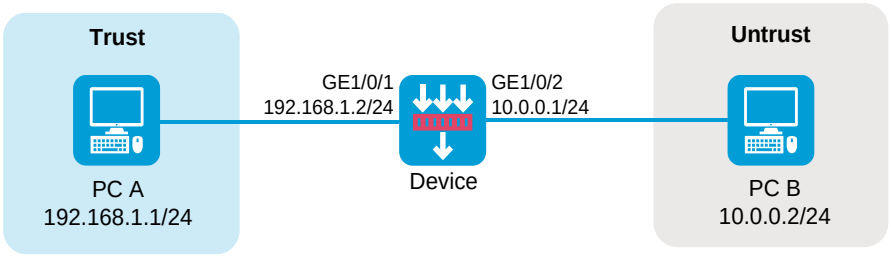
(9) 如包含在内，需要将端口 80 从端口范围中剔除。

(10) 单击<确定>，完成 NAT 出方向动态转换规则修改。

10.5 NAT与IPsec配合使用，IPsec配置不生效

10.5.1 故障描述

在 Device 上配置 NAT 源地址转换和 IPsec 功能，对 PC A 访问 PC B 的报文进行 NAT 源地址转换后，利用 IPsec 保护其安全性。PC A 主动访问 PC B，发现 IPsec 配置不生效。



10.5.2 故障处理步骤

1. 匹配 IPsec 策略的报文源和目的 IP 地址需为 NAT 转换后的 IP 地址。

(1) 登录设备 Web 管理页面。

(2) 选择“网络 > VPN > IPsec > 策略 ”。

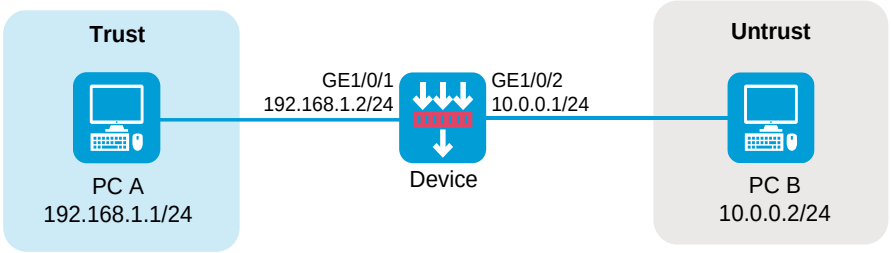
(3) 在“IPsec 策略”页面编辑 IPsec 策略配置。

(4) 查看 IPsec 策略配置中的被保护数据流配置，将被保护数据流的源和目的 IP 地址改为 NAT 转换后的 IP 地址。

10.6 配置NAT源地址转换后，外网用户无法访问设备

10.6.1 故障描述

在网关设备 Device 上配置 NAT 源地址转换后，外网 PC B 无法访问 Device。



10.6.2 故障处理步骤

1. 安全策略配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > 安全策略 > 安全策略”。

(3) 在“安全策略”页面单击<新建>按钮，选择新建策略，进入“新建安全策略”页面，必要的配置项如下：

a. 名称：secpolicy5

b. 源安全域： Untrust

c. 目的安全域：Local

d. 动作：允许

e. 源 IPv4 地址：10.0.0.2（此处为 PC B 的 IP 地址）

f. 目的 IPv4 地址：10.0.0.1（此处为 Device 外网侧接口的 IP 地址）

(4) 单击<确定>，完成安全策略配置。

2. 接口 NAT 配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > NAT > NAT 动态转换 > 策略配置”。

(3) 在“NAT 出方向动态转换（基于对象组）”页签中查看是否存在动作为 NO-PAT 的转换规则。

(4) 如存在上述规则，单击<编辑>，在修改 NAT 出方向动态转换界面查看转换后源地址处引用的 NAT 地址组中是否包含 Device 的外网侧接口 IP 地址 10.0.0.1。

(5) 如包含在内，需要把 10.0.0.1 从该 NAT 地址对象组中剔除。

(6) 单击<确定>，完成 NAT 出方向动态转换规则修改。

(7) 在“NAT 出方向动态转换（基于 ACL）”页签中查看是否存在转换模式为 NO-PAT 的转换规则。

(8) 如存在上述规则，单击<编辑>，进入修改 NAT 出方向动态转换界面。

(9) 若转换后源地址为 NAT 地址组，查看所引用的 NAT 地址组内是否包含 Device 的外网侧接口 IP 地址 10.0.0.1；若转换后源地址为接口 IP 地址，查看所引用的接口是否为 Device 的外网侧接口 GE1/0/2。

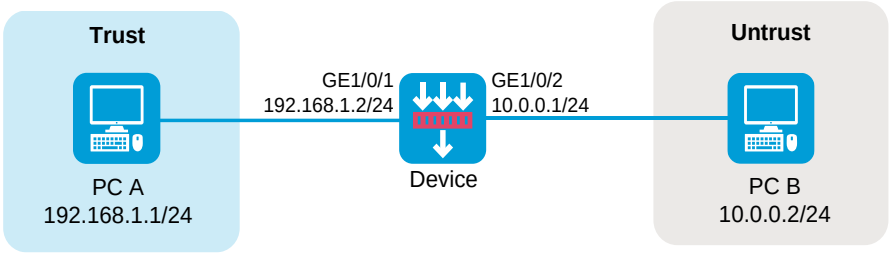
(10) 如出现上述两种情况之一，需要把 10.0.0.1 从转换后源地址中剔除。

(11) 单击<确定>，完成 NAT 出方向动态转换规则修改。

10.7 配置NAT目的地址转换后，外网用户无法访问设备

10.7.1 故障描述

在网关设备 Device 上配置 NAT 目的地址转换后，外网 PC B 无法访问 Device



10.7.2 故障处理步骤

1. 安全策略配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > 安全策略 > 安全策略”。

(3) 在“安全策略”页面单击<新建>按钮，选择新建策略，进入“新建安全策略”页面，必要的配置项如下：

a. 名称：secpolicy6

b. 源安全域： Untrust

c. 目的安全域：Local

d. 动作：允许

e. 源 IPv4 地址：10.0.0.2（此处为 PC B 的 IP 地址）

f. 目的 IPv4 地址：10.0.0.1（此处为 Device 外网侧接口的 IP 地址）

(4) 单击<确定>，完成安全策略配置。

2. 接口 NAT 配置检查

(1) 登录设备 Web 管理页面。

(2) 选择“策略 > NAT > NAT 内部服务器 > 策略配置”。

(3) 查看是否存在外网地址为 Device 的外网侧接口 IP 地址 10.0.0.1 的 NAT 内部服务器规则。

(4) 如存在上述规则，单击<编辑>，在修改 NAT 内部服务器界面查看外网端口是否为 PC B 访问 Device 时使用的端口。

(5) 如该端口确为 PC B 访问 Device 时使用的端口，请根据实际情况选择如下方式进行处理：

(6) 改变 PC B 访问 Device 时使用的协议或目的端口。

(7) 修改报文匹配规则（ACL）处引用的 ACL，不对 PC B 访问 Device 的报文进行目的地址转换。

(8) 单击<确定>，完成 NAT 内部服务器规则修改。

10.8 动态NAT转换故障(以动态nat outbound为例)

10.8.1 故障描述

NAT 不能正常转换或者 NAT 转换的报文不能正常转发。内网 PC A 无法通过网关设备 Device 访问外网 PC B

10.8.2 故障处理步骤

1. 首先确认 nat outbound 的配置是否正确

```
[H3C] display nat outbound
NAT outbound information:
There are 1 NAT outbound rules.
Interface: Route-Aggregation12
  ACL: ---          Address group: 257    Port-preserved: N
  NO-PAT: N         Reversible: N
```

2. 打开 debugging nat packet，确认 debugging 信息是否正确，应有类似如下 debugging 信息：

```
*May 13 09:58:48:083 2017 H3C NAT/7/COMMON: -slot =1;
 PACKET: (Route-Aggregation12-in) Protocol: TCP
         4.4.4.6:   21 -        4.4.5.11:11000(VPN:    0) ------>
            4.4.4.6:   21 -     192.168.1.2:13249(VPN:   0)
```

注： 可以看到正向的流量做了 NAT 转换

3. 通过 display session table ipv4 verbose 命令，确认会话信息是否正确。

```
<H3C> display session table ipv4 verbose
Initiator:
  Source      IP/port: 192.168.1.2/13790
  Destination IP/port: 4.4.4.6/21
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
Responder:
  Source      IP/port: 4.4.4.6/21
  Destination IP/port: 4.4.4.27/1060
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
State: TCP_ESTABLISHED
Application: FTP
Start time: 2013-12-15 10:49:00  TTL: 3592s
Interface(in) : Route-Aggregation11
Interface(out): Route-Aggregation12
Zone(in) : Trust
Zone(out): menglei
Initiator->Responder:            3 packets        128 bytes
Responder->Initiator:            2 packets        130 bytes
```

4. 如果上述定位手段均不能作出结论，请联系相关技术支持人员协助分析

10.9 设备作为出口网关设备，NAT业务不通，但是接口地址可以ping通

10.9.1 故障描述

FW 作为出口网关设备，内网部分用户无法上网，外网用户无法访问内网服务器，但是从外网 ping 出接口的地址可以 ping 通。

10.9.2 故障处理步骤

(1) 确定 NAT 地址组是否和接口地址是同一个网段：

(2) 如果 NAT 地址组的地址和配置 NAT 的接口地址不在同一网段，NAT 地址池的地址无法响应。如果不在同一网段，要确保对端设置了 NAT 地址组的路由。

(3) 如果地址组中的地址或 NAT Server 地址和接口在同一网段，确认地址组中的地址或者 NAT Server 地址是否发送了免费 arp，可以通过直连对端设备进行确认。还需要确认对端学习到的 arp 的 mac 地址的正确性：

(4) 设备上线时，对端设备需要更新 ARP。当两端不是直连，对端设备不能感知到链路 Down 过，所以不能删除相关 ARP 表项。当设备上线后，本端接口会发送接口地址的免费 ARP，对端设备收到该免费 ARP 后可以正常更新该 ARP 表项;但可能存在地址池中的地址 ARP 没有刷新。

(5) 在防火墙上 debug 或者抓包分析，是否 ping 报文只有发出去的而没有回来的，存在转发异常的情况。

(6) 在对端设备上持续地 ping NAT 地址组或者 NAT Server 的地址，打开 arp 的 debug 开关，确认是否没有收到 arp 请求报文。

(7) 如果无法确认定位，请联系技术支持人员进行分析。

10.10 故障诊断命令

命令	说明
display nat outbound	显示nat outbound设置信息
display nat server	显示nat server设置信息及状态
display session	显示会话信息
save	将当前配置保存到指定文件

11 IPsec/IKE 类故障处理

11.1 IPsec SA可以成功建立，但是IPsec保护的流量不通

11.1.1 故障描述

(1) 组网需求：

FW-1 和 FW-2 两台防火墙设备之间建立 IPsec 隧道，对 PC1 和 PC2 之间访问的流量进行 IPsec 保护。

(2) 配置描述：

FW-1 上，IKE 的 local-address 为：81.2.0.1， remote-address 为：14.5.1.1

安全 ACL 规则为：

```
rule 0 permit ip source 81.2.0.0 0.0.0.255 destination 82.2.0.0 0.0.0.255
```

FW-2 上，IKE 的 local-address 为：14.5.1.1， remote-address 为：81.2.0.1

安全 ACL 规则为：

```
rule 0 permit ip source 82.2.0.0 0.0.0.255 destination 81.2.0.0 0.0.0.255
```

(3) 故障描述：IKE SA 和 IPsec SA 都可以建立，但是 PC1 和 PC 2 互相 ping，均不能 ping 通。

11.1.2 故障处理步骤

(1) 首先查看路由是否可达，若路由没问题，再查看保护的 ACL 是否有匹配次数统计来检查 ACL 是否匹配，和用户要保护的流量是否一致。

(2) 如果保护的 ACL 有匹配次数，且 ACL 和用户要保护的流量一致，再检查 FW 上的安全策略，确认安全策略是否允许 IPsec 封装后的 ESP 或 AH 报文通过。

(3) 如果上述都没有发现问题，可以使用命令 **reset ipsec sa**、**reset ike sa** 清除 IPsec SA 和 IKE SA；重新建立 SA，看是否正常。如果无法解决问题，请联系技术支持人员。

11.2 故障诊断命令

命令	说明
display ike sa	显示IKE SA的信息
display ipsec sa	显示IPsec SA的信息
reset ike sa	清除IKE SA
reset ipsec sa	清除IPsec SA
save	将当前配置保存到指定文件

11.3 IKE SA可以成功建立，但是IPsec SA未能建立成功

11.3.1 故障描述

(1) 组网需求：

FW-1 和 FW-2 两台防火墙设备之间建立 IPsec 隧道，对 PC1 和 PC2 之间访问的流量进行 IPsec 保护。

(2) 配置描述：

FW-1 上，IKE 的 local-address 为：81.2.0.1， remote-address 为：14.5.1.1

安全 ACL 规则为：

```
rule 0 permit ip source 81.2.0.0 0.0.0.255 destination 82.2.0.0 0.0.0.255
```

FW-2 上，IKE 的 local-address 为：14.5.1.1， remote-address 为：81.2.0.1

安全 ACL 规则为：

```
rule 0 permit ip source 82.2.0.0 0.0.0.255 destination 81.2.0.0 0.0.0.255
```

(3) 故障描述：IKE SA 可以建立，但 IPsec SA 未能建立。

11.3.2 故障处理步骤

(1) 首先查看保护的 ACL 是否有匹配次数统计来检查 ACL 是否匹配，和用户要保护的流量是否一致。

(2) 如果保护的 ACL 有匹配次数，且 ACL 和用户要保护的流量一致，再检查两端 FW 的算法是否一致，主要有安全协议、加密和验证算法、封装模式是否一致；若算法一致，请排查是否有错误或不完整的配置，比如：缺少或配错对端地址、缺少或配错 ike 策略。

(3) 如果上述都没有发现问题，可以使用命令 **reset ipsec sa**、**reset ike sa** 清除 IPsec SA 和 IKE SA；重新建立 SA，看是否正常。如果无法解决问题，请联系技术支持人员。

11.4 故障诊断命令

命令	说明
display ike sa	显示IKE SA的信息
display ipsec sa	显示IPsec SA的信息
reset ike sa	清除IKE SA
reset ipsec sa	清除IPsec SA
display ipsec transform-set	显示IPsec安全提议的信息
display ipsec policy	显示IPsec安全策略的信息
save	将当前配置保存到指定文件

11.5 IKE SA未能成功建立

11.5.1 故障描述

(1) 组网需求：

FW-1 和 FW-2 两台防火墙设备之间建立 IPsec 隧道，对 PC1 和 PC2 之间访问的流量进行 IPsec 保护。

(2) 配置描述：

FW-1 上，IKE 的 local-address 为：81.2.0.1， remote-address 为：14.5.1.1

安全 ACL 规则为：

```
rule 0 permit ip source 81.2.0.0 0.0.0.255 destination 82.2.0.0 0.0.0.255
```

FW-2 上，IKE 的 local-address 为：14.5.1.1， remote-address 为：81.2.0.1

安全 ACL 规则为：

```
rule 0 permit ip source 82.2.0.0 0.0.0.255 destination 81.2.0.0 0.0.0.255
```

(3) 故障描述：IKE SA 未能建立。

11.5.2 故障处理步骤

(1) 查看两端 FW 的提议是否匹配：加密算法和验证算法是否匹配；身份认证方法是否匹配；

(2) 查看身份验证是否成功，主要查看两端 FW 预共享密钥配置是否相同；若是证书验证的话，关注证书是否过期、证书是否有可信 CA、证书是否被吊销、两端证书的密钥是否匹配、两端证书是否为同一个 CA 签发；还有常见的情况是对端身份冲突，请查看是否有多个 ike 策略的 remote 规则相同。

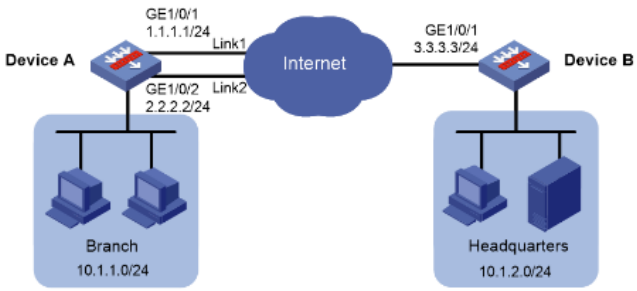
(3) 如果上述查看未能发现问题所在，无法解决问题，请联系技术支持人员。

11.6 故障诊断命令

命令	说明
display ike sa	显示IKE SA的信息
display ipsec sa	显示IPsec SA的信息
reset ike sa	清除IKE SA
reset ipsec sa	清除IPsec SA
display ike proposal	显示所有IKE提议的配置信息
save	将当前配置保存到指定文件

11.7 IPsec智能选路，链路不检测

11.7.1 故障描述



(1) 组网需求：

企业分支使用 IPsec VPN 接入企业总部，通过在分支 Device A 上配置 IPsec 智能选路功能，实现 IPsec 隧道在 Link 1 和 Link 2 两条链路上动态切换，具体需求如下：

a. Device A 首先使用 Link1 与总部建立 IPSec 隧道。

b. 当基于 Link1 建立的 IPSec 隧道丢包严重或时延过高时，能自动切换到 Link2 建立新的 IPSec 隧道。

(2) 配置描述：

分支 Device A 上：

配置接口 IP 地址和网关地址，1.1.1.3 和 2.2.2.3 为本例中的直连下一跳地址：

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 1.1.1.1 24
[DeviceA-GigabitEthernet1/0/1] gateway 1.1.1.3
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] ip address 2.2.2.2 24
[DeviceA-GigabitEthernet1/0/2] gateway 2.2.2.3
[DeviceA-GigabitEthernet1/0/2] quit
```

配置 IPsec 智能选路策略

配置一个 IPsec 智能选路策略名称为 policy1，添加链路。

```
[DeviceA] ipsec smart-link policy policy1
[DeviceA-ipsec-smart-link-policy-policy1] link 1 interface gigabitethernet 1/0/1 remote 3.3.3.3
[DeviceA-ipsec-smart-link-policy-policy1] link 2 interface gigabitethernet 1/0/2 remote 3.3.3.3
```

设置链路循环切换的最大次数为 4。

```
[DeviceA-ipsec-smart-link-policy-policy1] link-switch cycles 4
```

开启 IPsec 智能选路功能。

```
[DeviceA-ipsec-smart-link-policy-policy1] smart-link enable
[DeviceA-ipsec-smart-link-policy-policy1] quit
```

总部 Device B 上：

配置接口的 IP 地址

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 3.3.3.3 24
[DeviceB-GigabitEthernet1/0/1] quit
```

配置一个 IPv4 的 ACL，定义要保护的数据流

```
[DeviceB] acl advanced 3000
[DeviceB-acl-ipv4-adv-3000] rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
[DeviceB-acl-ipv4-adv-3000] rule permit ip source 3.3.3.0 0.0.0.255 destination 1.1.1.0 0.0.0.255
[DeviceB-acl-ipv4-adv-3000] rule permit ip source 3.3.3.0 0.0.0.255 destination 2.2.2.0 0.0.0.255
[DeviceB-acl-ipv4-adv-3000] quit
```

配置到达 Device A 所在子网的静态路由。3.3.3.1 为本例中的直连下一跳地址：

```
[DeviceB] ip route-static 10.1.1.0 255.255.255.0 gigabitethernet 1/0/1 3.3.3.1
[DeviceB] ip route-static 1.1.1.0 255.255.255.0 gigabitethernet 1/0/1 3.3.3.1
[DeviceB] ip route-static 2.2.2.0 255.255.255.0 gigabitethernet 1/0/1 3.3.3.1
```

(3) 故障描述：智能选路不探测。

11.7.2 故障处理步骤

(1) 查看是否缺少有效链路，比如接口地址缺少未配、接口 DOWN 未 UP；

(2) 查看配置是否完整：IPsec 策略是否应用智能选路、是否缺少路由下一跳；

(3) 若上述查看未见问题，请继续排查 IPsec 策略相关配置是否齐全和正确；

(4) 如果问题仍未解决，请调大探测轮数，以排除探测达到最大轮数的原因；

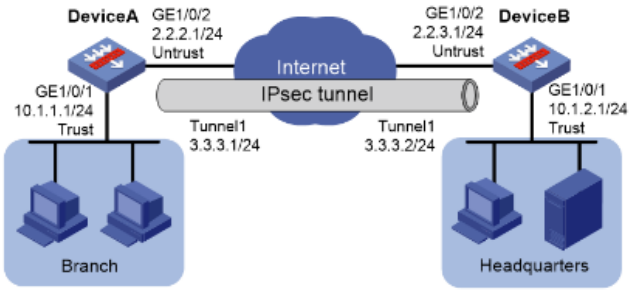
(5) 如果上述查看未能发现问题所在，无法解决问题，请联系技术支持人员。

11.8 故障诊断命令

命令	说明
display ike sa	显示IKE SA的信息
display ipsec sa	显示IPsec SA的信息
reset ike sa	清除IKE SA
reset ipsec sa	清除IPsec SA
display ipsec smart-link policy	查看IPsec智能选路策略的配置信息
display ipsec policy	可以查看到IPsec安全策略引用IPsec智能选路策略
display acl 3000	可以查看动态生成的ACL规则
save	将当前配置保存到指定文件

11.9 IPsec隧道保护隧道接口上的报文，隧道未建立成功

11.9.1 故障描述



(1) 组网需求：

某企业分支和总部均使用固定的 IP 地址接入 Internet。

a. 企业分支与企业总部之间的所有流量通过 IPsec 安全隧道进行传送；

b. 当企业分支的私网 IP 地址段调整时，不需要改变企业总部网关的 IPsec 配置。

为实现如上组网需求，可采用如下配置思路实现：

c. 在 Device A 和 Device B 之间使用 IPsec 隧道接口建立 IPsec 连接，将发送给对端私网的数据流路；

d. 由到 IPsec 虚拟隧道接口上，由 IPsec 虚拟隧道接口上动态协商建立的 IPsec 安全隧道对分支子网；

e. （10.1.1.0/24）与总部子网（10.1.2.0/24）之间的所有数据流进行安全保护。

(2) 配置描述：

在 Device A 上：

配置 IPsec 隧道接口

创建模式为 IPsec 隧道的接口 Tunnel1。

```
[DeviceA] interface tunnel 1 mode ipsec
```

配置 Tunnel1 接口的 IP 地址。

```
[DeviceA-Tunnel1] ip address 3.3.3.1 255.255.255.0
```

配置 Tunnel1 接口的源端地址（GE1/0/2 接口的 IP 地址）。

```
[DeviceA-Tunnel1] source 2.2.2.1
```

配置 Tunnel1 接口的目的端地址（DeviceB 的 GE1/0/2 接口的 IP 地址）。

```
[DeviceA-Tunnel1] destination 2.2.3.1
```

在 IPsec 隧道接口上应用 IPsec 安全框架。

```
[DeviceA-Tunnel1] tunnel protection ipsec profile abc
[DeviceA-Tunnel1] quit
```

配置 Device A 到 Device B 的静态路由。

```
[DeviceA] ip route-static 10.1.2.0 255.255.255.0 tunnel 1
```

在 Device B 上：

配置 IPsec 隧道接口

创建模式为 IPsec 隧道的接口 Tunnel1。

```
[DeviceB] interface tunnel 1 mode ipsec
```

配置 Tunnel1 接口的 IP 地址。

```
[DeviceB-Tunnel1] ip address 3.3.3.2 255.255.255.0
```

配置 Tunnel1 接口的源端地址（GE1/0/2 接口的 IP 地址）。

```
[DeviceB-Tunnel1] source 2.2.3.1
```

配置 Tunnel1 接口的目的端地址（DeviceB 的 GE1/0/2 接口的 IP 地址）。

```
[DeviceB-Tunnel1] destination 2.2.2.1
```

在 IPsec 隧道接口上应用 IPsec 安全框架。

```
[DeviceB-Tunnel1] tunnel protection ipsec profile abc
[DeviceB-Tunnel1] quit
```

配置 Device B 到 Device A 的静态路由。

```
[DeviceB] ip route-static 10.1.1.0 255.255.255.0 tunnel 1
```

(3) 故障描述：IPsec 隧道未能建立。

11.9.2 故障处理步骤

(1) 查看两端 FW 中的 Tunnel 口是否异常，若为 DOWN 状态，请首先检查 Tunnel 配置是否完整：是否配置了 Source、是否配置了 Destination（可能配置时配成了 Description）、是否配置了 IP 地址；

(2) 若 Tunnel 口配置无问题，请检查 Tunnel 源物理口是否 UP、Tunnel 目的地址是否可达；

(3) Tunnel 口检查完毕后，若问题依然存在，请排查 IPsec 和 IKE 基础配置是否正确；

(4) 如果上述操作，未能发现问题所在，无法解决问题，请联系技术支持人员。

11.10 故障诊断命令

命令	说明
display ike sa	显示IKE SA的信息
display ipsec sa	显示IPsec SA的信息
reset ike sa	清除IKE SA
reset ipsec sa	清除IPsec SA
display ip interface brief	查看接口状态
display interface Tunnel 1	查看隧道状态
save	将当前配置保存到指定文件

12 负载均衡故障处理

12.1 CPU/内存较高时对负载均衡的影响

12.1.1 故障描述

CPU 高，内存高，负载均衡功能影响：虚服务有丢包、NQA 探测失败或者震荡、新请求失败、并发性能无法提升。

12.1.2 故障处理步骤

(1) 查看实服务的状态，CPU 高可能导致 NQA 探测失败或者震荡，此时虚服务器会有丢包。

(2) 内存高会导致并发上不去，新请求会失败。

12.2 故障诊断命令

命令	说明
display virtual-server statistics	显示虚服务的统计信息
display real-server statistics	显示实服务器的统计信息
debugging lb all	开启LB的所有调试信息
debugging lb error	开启LB的错误调试信息
debugging lb event	开启LB的事件调试信息

命令	说明
debugging lb fsm	开启LB的状态机调试信息
debugging lb packet	开启LB的报文调试信息

12.3 负载分担不均匀时如何排查优化

12.3.1 故障描述

发现负载均衡分担不均匀时，如何排查并进行优化。

12.3.2 故障处理步骤

(1) 可以查看各个实服务器的统计信息是否均匀。如果想让各个服务器均匀的分担一般用轮转的调度算法，将客户端请求均匀分担到多个实服务器。

(2) LB 插卡是多核 CPU 系统，每个核单独按照自己的表项进行轮转，所以全局来看，有可能出现每个实服务分到的连接数不均衡的问题。请考虑修改调度算法为最小连接或者随机等观察一下。

(3) 源地址 HASH 算法流量不均匀，请确认源地址个数是否足够。

(4) 通过配置负载均衡策略，进行更精细的分类，将请求进行分类送给哪些服务器，尽量满足用户实际需求：对于特殊业务，服务器的状态，需要依据实际环境进行调整。

12.4 故障诊断命令

配置	命令
显示实服务器的统计信息	**display real-server statistics** [**name** *real-server-name*]
显示虚服务器的统计信息	**display virtual-server statistics** [**name** *virtual-server-name*]
清除实服务器的统计信息	**reset real-server statistics** [*real-server-name*]
清除虚服务器的统计信息	**reset virtual-server statistics** [*virtual-server-name*]

13 系统管理维护类故障处理

13.1 CPU占用率高

13.1.1 故障描述

设备 CPU 占用率持续在 60%以上，下发命令时设备反应很慢。

```
<H3C> display cpu-usage
Slot 1 CPU 0 CPU usage:
      13% in last 5 seconds
      13% in last 1 minute
```

```
      13% in last 5 minutes
```

通过 **display cpu-usage history** 可以查看单板最近 60 分钟的 CPU 占用情况。

```
<H3C> display cpu-usage history
100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|
 30%|
 25%|
 20%|
 15%|
 10%|
  5%|    #
    ------------------------------------------------------------
              10        20        30        40        50        60   (minutes)
                   cpu-usage (CPU 0) last 60 minutes (SYSTEM)
```

13.1.2 故障处理步骤

CPU 占用率高的原因通常有：

- 路由震荡
- 配置过多的路由策略
- 报文攻击
- 链路环路
- 报文没有走快转
- 接口没有加入安全域或者没有安全策略，大量报文在设备上丢弃
- 打开了 Debugging 调试开关
- 对象策略/ACL 未开加速
- 对象组地址中存在排除地址或者非连续掩码
- 静态 Nat444 端口块资源不足
- 大量广播/组播报文上送
- 突发流量导致 CPU 高

1. 路由策略排查

通过 **display route-policy** 命令可以查看设备配置的路由策略，请检查配置的路由策略是否过多，导致 CPU 处理的负担增加。

```
<H3C> display route-policy
Route-policy: policy1
  permit : 1
          if-match cost 10
          continue: next node 11
          apply comm-list a delete
```

2. 链路环路排查

链路成环时，网络震荡，大量的协议报文上送 CPU 处理也可能导致 CPU 占用率升高。存在环路时流量成环，可能会出现广播，设备很多端口的流量会变得很大，端口使用率达到 90%以上：

```
<H3C> display interface GigabitEthernet1/0/2
GigabitEthernet1/0/2 current state: UP
Line protocol current state: UP
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0000-e80d-c000
Description: GigabitEthernet2/6/0/1 Interface
Loopback is not set
Media type is optical fiber, Port hardware type is 1000_BASE_SX_SFP
1000Mbps-speed mode, full-duplex mode
……
Last clearing of counters: Never
 Peak value of input: 123241940 bytes/sec, at 2013-06-27 14:33:15
 Peak value of output: 80 bytes/sec, at 2013-06-27 14:13:00
 Last 300 second input:  26560 packets/sec 123241940 bytes/sec 99%
 Last 300 second output:  0 packets/sec 80 bytes/sec 0%
……
```

如链路出现环路：

- 排查链路连接、端口配置是否正确
- 设备对接的交换机是否使能 STP 协议，配置是否正确
- 设备路由是否设置正确，是否存在路由环路。

3. 报文是否走快转排查

可以通过 **display ip fast-forwarding cache** 命令来确定报文是否走快转，如果 cache 表项中不存在该报文相关的表项，说明报文没有走快转。

```
<H3C> display ip fast-forwarding cache
Total number of fast-forwarding entries: 78
SIP             SPort DIP             DPort Pro Input_If    Output_If    Flg
40.1.20.2       65535 30.1.2.2        1024  6   Reth4       Reth3        1
192.168.96.40   53342 192.168.205.33  23    6   GE1/0/0     N/A          1
30.1.2.2        1024  40.1.20.2       65535 6   Reth3       Reth4        1
192.168.205.33  23    192.168.96.52   60824 6   InLoop0     GE1/0/0      1
120.0.0.1       1701  120.0.0.2       1701  17  InLoop0     GE1/0/2.120  1
40.1.20.2       65529 30.1.2.2        1024  6   Reth4       Reth3        1
130.2.1.115     1701  130.2.1.1       1701  17  Reth4       N/A          1
30.1.2.2        1024  40.1.20.2       65533 6   Reth3       Reth4        1
```

```
40.1.20.2        65526 30.1.2.2         1024  6   Reth4        Reth3        1
50.1.1.2         1024  60.1.1.2         1024  6   Reth1        Tun1         1
192.168.205.33   37932 192.168.100.53   0     1   InLoop0      GE1/0/0      1
30.1.2.2         1024  40.1.20.2        65529 6   Reth3        Reth4        1
30.1.2.2         1024  40.1.20.2        65527 6   Reth3        Reth4        1
60.1.1.2         1024  50.1.1.2         1024  6   Tun1         Reth1        1
40.1.20.2        65532 30.1.2.2         1024  6   Reth4        Reth3        1
```

可以根据某一个地址进行确认以该地址为源或目的 IP 报文是否走快转，命令如下：

```
<H3C> display ip fast-forwarding cache 12.1.1.1
Total number of fast-forwarding entries: 2
SIP              SPort DIP              DPort Pro Input_If     Output_If    Flg
12.1.1.2         49216 12.1.1.1         3784  17  InLoop0      N/A          1
12.1.1.1         3784  12.1.1.2         49216 17  RAGG5.3101   InLoop0      1
```

如果仍然无法排除故障，请将 **display cpu-usage** 命令显示信息及搜集的其他信息反馈给技术支持人员分析。

4. 对象策略/ACL 未开加速

```
#
object-policy ip EXTERNAL-Local
 rule 0 pass vrf external_vpn
rule 1 pass vrf 7tgaklptgb9o19babgnm3kbst8
accelerate
#
```

如果对象策略或者 ACL 中存在 50 条以上的 rule 规则，但是未开启加速，会导致设备 CPU 高的现象，可以用命令 **display object-policy accelerate summary ip** 和 **display acl accelerate summary** 查看当前哪些对象策略和 ACL 已开启加速。

5. 对象组地址中存在排除地址或者非连续掩码

如果对象组地址中配置了 exclude、或者不连续掩码 wildcard，会存在加速失败导致设备 CPU 高的现象，需要删除相关的配置。

6. 静态 Nat444 端口块资源不足

如果客户网络中配置了静态 Nat444，当网络中存在突发流量（报文源端口大量跳变，源目的 IP 和目的端口号均不变）时会导致 Nat444 端口资源耗尽。

在 probe 视图查看 **display system internal nat statistics chassis X slot X cpu 1 | in failed**，看是否有类似 NAT444 failed to translate port 计数的大量增长。

如果存在上述错误计数大量增长的话，用命令 **display nat port-block static c 1 s X c 1** 查看是哪个地址映射占用了大量端口资源，检查该地址所在的 NAT 地址组配置，看当前占用的端口资源是否达到了端口资源的上限。

如果确认是端口资源达到上限的话，需要整改现场配置扩大端口块资源。

7. 大量广播/组播报文上送

检查设备物理口是否有大量广播/组播报文进入设备。相关命令如下：

display counters rate inbound interface

在上述命令回显中查看是否有 broadcasts 和 multicasts 报文计数的大量增长。

如果确认有大量广播/组播报文进入防火墙设备，需要对该报文进行 qos 限速，并排查该广播/组播报文的来源。

8. 突发流量导致 CPU 高

如果上送的报文在安全策略中未放通，也会造成设备 CPU 高的现象。查看设备的 aspf 和 packet-drop 丢包统计，看是否有大量丢包记录。相关命令如下：

```
[H3C-probe]display system internal aspf statistics zone-pair ipv4 chassis X slot X cpu 1
[H3C-probe]display system internal ip packet-drop statistics chassis X slot X cpu 1
```

此时可以通过下面的命令确定报文特征：

debug ip packet

debug ip info

debug aspf packet

确认报文特征后，根据需要对报文进行安全策略放行、配置攻击防范策略、QOS 限速等处理。

13.2 内存占用率高

13.2.1 故障描述

多次查看单板内存占用率，发现内存占用率持续偏高，始终处于 70%以上（FreeRatio 低于 30%）。Total 表示总的内存，Used 表示当前使用的内存，FreeRatio 表示未使用的内存占用率。

查看内存命令如下：

```
<H3C> display memory slot 2
The statistics about memory is measured in KB:
Slot 2:
             Total      Used      Free    Shared   Buffers    Cached   FreeRatio
Mem:      16375408   2514664  13860744         0      1396    177968       84.6%
-/+ Buffers/Cache:   2335300  14040108
Swap:           0         0         0
```

13.2.2 故障处理步骤

这类问题通常为软件问题引起，如内存泄露，也可能是由于会话数目、路由数目过多导致。请按照下面步骤进一步搜集信息发送给技术支持人员分析。

1. 查询单板各进程的内存使用信息

通过 **display process memory** 命令多次查询单板各进程的内存使用信息。Dynamic 类型的内存为设备动态申请的，在内存出现泄露时会持续增加，通过前后比较观察可以确认哪个进程的内存占用持续增加。如果持续增加，说明该进程可能发生了泄露，请记录下进程的 JID。下面以查询 JID 为 18919 的 diagd 进程为例说明。

```
<H3C> display process memory slot 2
   JID       Text       Data      Stack    Dynamic    Name
     1        132        700         32        156    scmd
     2          0          0          0          0    [kthreadd]
     3          0          0          0          0    [migration/0]
     4          0          0          0          0    [ksoftirqd/0]
     5          0          0          0          0    [watchdog/0]
```

```
     6          0          0          0          0     [migration/1]
     7          0          0          0          0     [ksoftirqd/1]
     8          0          0          0          0     [watchdog/1]
     9          0          0          0          0     [migration/2]
    10          0          0          0          0     [ksoftirqd/2]
    11          0          0          0          0     [watchdog/2]
    12          0          0          0          0     [migration/3]
    13          0          0          0          0     [ksoftirqd/3]
    14          0          0          0          0     [watchdog/3]
    15          0          0          0          0     [migration/4]
    16          0          0          0          0     [ksoftirqd/4]
    17          0          0          0          0     [watchdog/4]
……
    18919        128     76416          64       2240    diagd
……
```

2. 确认哪种字节大小的内存块发生泄露

再进一步确认 JID 为 18919 的 diagd 进程的哪种字节大小的内存块发生泄露。如下命令所示，Size 表示内存块的字节大小，Total 表示总的申请个数，Used 表示使用数目，Free 表示未使用的数目，Free Ratio 表示未使用的内存块百分比。通过多次查询并比较查询值可以看出哪个 Size 的内存块 Used 个数持续增加。查询完毕后，请将搜集到的信息发送给技术支持人员分析。

```
Heap usage:
Size       Free       Used       Total      Free Ratio
32         541        39         580        93.3%
48         6          43         49         12.2%
64         534        32499      33033      1.6%
80         538        47         585        92.0%
112        0          534        534        0.0%
128        0          4          4          0.0%
160        0          4          4          0.0%
176        0          4          4          0.0%
256        0          2          2          0.0%
288        0          1          1          0.0%
304        0          1          1          0.0%
336        0          1          1          0.0%
688        0          4          4          0.0%
1184       0          2          2          0.0%
1456       0          2          2          0.0%
1984       0          1          1          0.0%
2032       0          2          2          0.0%
4144       0          1          1          0.0%
13792      1          0          1          100.0%
Large Memory Usage:
Used Blocks          :  0
Used Memory(in bytes):  0
Free Blocks          :  3
Free Memory(in bytes):  211200
Summary:
```

```
Total virtual memory heap space(in bytes)   :  2490368
Total physical memory heap space(in bytes) :  2293760
Total allocated memory(in bytes)           :  2170560
```

13.3 故障诊断命令

命令	说明
display cpu-usage	显示CPU利用率的统计信息。用于查询CPU占用率高的任务
display cpu-usage history	以图形方式显示CPU利用率统计历史信息
display interface	显示指定接口的信息。检查接口的流量是否正常
display memory	显示单板内存占用率
display process memory	显示单板各进程的内存使用信息。通过多次查询，发现可能存在内存泄露的进程
display process memory heap	显示Dynamic类型内存的详细信息，确认哪种字节大小的内存块发生了泄露
display system internal kernel memory pool	查看内核内存分配情况

14 SSL VPN 类故障处理

14.1 SSL VPN登录，无法打开SSL VPN页面

14.1.1 故障描述

客户端可以 ping 通 SSL VPN 网关，但是无法打开 SSL VPN 页面。

14.1.2 故障处理步骤

(1) 首先查看 SSL 服务器端策略视图下是否未引用 PKI 域，通过以下命令查看，SSL 服务器端策略下需要引用 PKI 域。

```
[H3C] ssl server-policy XXX
[H3C-ssl-server-policy-XXX] display this
#
ssl server-policy XXX
 pki-domain XXX
#
return
```

如果 **pki-domain** 命令不存在，需要添加。

(2) 查看是否在 SSL 服务器策略引用的 PKI 域下导入了 CA 证书，LOCAL 证书。并且保证 LOCAL 证书是 CA 服务器颁发给服务器的证书，而不是客户端证书，通过以下命令查看。

```
display pki certificate domain XXXX  ca
```

```
display pki certificate domain XXXX  local
```

(3) 如果上述都没有发现问题，可能是在 SSL VPN gateway 的 **service enable** 之后，再进行了导入证书的操作，只要导入了证书或者 SSL 策略进行了配置变化，就必须在 SSL VPN gateway XXX 里面进行 **undo service enable**，然后再 **service enable** 一下便可，证书和配置才能生效。如果无法解决问题，请联系技术支持人员。

14.1.3 故障诊断命令

表14-1 故障诊断命令

命令	说明
ssl server-policy *policy-name*	创建SSL服务器端策略，并进入SSL服务器端策略视图
pki-domain *domain-name*	配置SSL服务器端策略所使用的PKI域
display pki certificate domain *domain-name* { **ca** | **local** | **peer** [**serial** *serial-num*] }	显示证书内容
sslvpn gateway *gateway-name*	创建SSL VPN网关，并进入SSL VPN网关视图
service enable	开启当前的SSL VPN网关

14.2 浏览器无法登陆SSL VPN网关

14.2.1 故障描述

浏览器可以打开 SSL VPN 网关页面，但是无法登录。

14.2.2 故障处理步骤

(1) 确认 SSL VPN 网关地址是否可达，设备允许 Ping 的情况下可通过 Ping 确认，不允许 Ping 的情况下可通过抓包确认。

(2) 通过查看 SSL VPN 网关的显示信息，确认 SSL VPN 网关的状态：

a. 确认 SSL VPN 网关是否处于 Up 状态。通过查看显示信息中 Operation state 字段的值，若值为 Up，则表示 SSL VPN 网关处于 Up 状态，否则需要在 Web 界面单击 SSL VPN 网关的使能按钮，或者在 SSL VPN 网关视图下执行 service enable 命令开启 SSL VPN 网关；

b. 重新配置或修改 SSL 服务端策略后，只有执行 undo service enable 命令关闭 SSL VPN 网关，并执行 service enable 命令重新开启 SSL VPN 网关后，新的策略才会生效；

c. SSL 相关配置是否正确，缺省情况下设备使用自带的缺省证书，当需要使用非缺省证书时，可以引用 SSL 服务端策略。当不需要使用非缺省证书时，删除 SSL 服务端策略引用即可；SSL VPN 网关的显示信息如下：

```
[Device] display sslvpn gateway
Gateway name: gw
  Operation state: Up
  IP: 1.1.1.2  Port: 2000
  SSL server policy configured: sslnew
```

```
SSL server policy in use: ssl
Front VPN instance: Not configured
```

(3) 通过查看 SSL VPN 访问实例的显示信息，确认 SSL VPN 访问实例的状态：

a. 确认 SSL VPN 访问实例是否处于 Up 状态。通过查看显示信息中 Operation state 字段的值，若值为 Up，则表示 SSL VPN 访问实例处于 Up 状态，否则需要在 Web 界面单击 SSL VPN 访问实例的使能按钮，或者在 SSL VPN 访问实例视图下执行 service enable 命令开启 SSL VPN 访问实例

b. 确认 SSL VPN 访问实例是否引用了 SSL VPN 网关。通过查看显示信息中 Associated SSL VPN gateway 字段的值，若有引用的网关名称，则表示成功引用了 SSL VPN 网关，否则，需要在 Web 界面 SSL VPN 访问实例下引用 SSL VPN 网关，或者在 SSL VPN 访问实例视图下执行 gateway 命令，引用 SSL VPN 网关

SSL VPN 访问实例的显示信息如下：

```
[Device] display sslvpn context
Context name: ctx
  Operation state: Up
  Associated SSL VPN gateway: gw
  SSL client policy configured: sslnew
  SSL client policy in use: ssl
```

(4) 确认 SSL VPN 网关地址和端口是否被正确侦听，需要确认每个业务板的侦听端口是否正确开启，TCP 代理连接的显示信息如下：

```
<Device> display tcp-proxy slot 1
Local Addr:port       Foreign Addr:port     State            Service type
1.1.1.2:2000           0.0.0.0:0                  LISTEN       SSLVPN
```

(5) 确认 SSL VPN 用户是否配置正确：

a. 本地用户：确保用户类型为网络接入类，服务类型为 SSL VPN，且为 SSL VPN 用户配置资源组。

b. 远程用户：确保远程认证服务器上用户隶属的用户组，已在 SSL VPN 访问实例中配置对应名称的资源组。

(6) 若开启了客户端和服务器端证书认证，确保两端已正确安装证书。

14.2.3 故障诊断命令

表14-2 故障诊断命令

命令	说明
display tcp-proxy	显示TCP代理连接的简要信息
display sslvpn context	显示SSL VPN访问实例的信息
display sslvpn gateway	显示SSL VPN网关的信息

14.3 浏览器无法访问内网资源

14.3.1 故障描述

通过浏览器登录 SSL VPN 网关后，无法访问内网服务器资源。

14.3.2 故障处理步骤

(1) 确认 SSL VPN 访问实例下配置了资源，以下方式至少一种：

a. 配置了访问资源的资源列表，如下：

创建 URL 表项 urlitem，并配置资源的 URL。

```
[Device-sslvpn-context-ctxweb1] url-item urlitem
[Device-sslvpn-context-ctxweb1-url-item-urlitem] url http://20.2.2.2
[Device-sslvpn-context-ctxweb1-url-item-urlitem] quit
```

创建 URL 列表 urllist。

```
[Device-sslvpn-context-ctxweb1] url-list urllist
```

配置 URL 列表标题为 web。

```
[Device-sslvpn-context-ctxweb1-url-list-urllist] heading web
```

配置 URL 列表引用的 URL 表项。

```
[Device-sslvpn-context-ctxweb1-url-list-urllist] resources url-item urlitem
[Device-sslvpn-context-ctxweb1-url-list-urllist] quit
```

SSL VPN 访问实例 ctxweb1 下创建策略组 resourcegrp1，引用 URL 列表 urllist。

```
[Device-sslvpn-context-ctxweb1] policy-group resourcegrp1
[Device-sslvpn-context-ctxweb1-policy-group-resourcegrp1] resources url-list urllist
[Device-sslvpn-context-ctxweb1-policy-group-resourcegrp1] quit
```

b. 配置了能够放行通往后台服务器的 ACL 或者 URI ACL 规则，并且引用规则已经添加：

```
[Device-sslvpn-context-ctxweb1] policy-group resourcegrp1
[Device-sslvpn-context-ctxweb1-policy-group-resourcegrp1] filter web-access acl 3000
```

(2) SSL VPN 网关是否可以 Ping 通后台资源地址，是否需要在对端设备上添加路由。

(3) 通过查看 SSL VPN 网关的显示信息，确认 SSL VPN 网关的状态：

a. 确认 SSL VPN 网关是否处于 Up 状态。通过查看显示信息中 Operation state 字段的值，若值为 Up，则表示 SSL VPN 网关处于 Up 状态，否则需要在 Web 界面单击 SSL VPN 网关的使能按钮，或者在 SSL VPN 网关视图下执行 service enable 命令开启 SSL VPN 网关

b. 重新配置或修改 SSL 服务端策略后，只有执行 undo service enable 命令关闭 SSL VPN 网关，并执行 service enable 命令重新开启 SSL VPN 网关后，新的策略才会生效

c. SSL 相关配置是否正确，缺省情况下设备使用自带的缺省证书，当需要使用非缺省证书时，可以引用 SSL 服务端策略。当不需要使用非缺省证书时，删除 SSL 服务端策略引用即可

SSL VPN 网关的显示信息如下：

```
[Device] display sslvpn gateway
Gateway name: gw
  Operation state: Up
  IP: 1.1.1.2  Port: 2000
  SSL server policy configured: sslnew
  SSL server policy in use: ssl
```

```
  Front VPN instance: Not configured
```

(4) 通过查看 SSL VPN 访问实例的显示信息，确认 SSL VPN 访问实例的状态：

a. 确认 SSL VPN 访问实例是否处于 Up 状态。通过查看显示信息中 Operation state 字段的值，若值为 Up，则表示 SSL VPN 访问实例处于 Up 状态，否则需要在 Web 界面单击 SSL VPN 访问实例的使能按钮，或者在 SSL VPN 访问实例视图下执行 service enable 命令开启 SSL VPN 访问实例

b. 确认 SSL VPN 访问实例是否引用了 SSL VPN 网关。通过查看显示信息中 Associated SSL VPN gateway 字段的值，若有引用的网关名称，则表示成功引用了 SSL VPN 网关，否则，需要在 Web 界面 SSL VPN 访问实例下引用 SSL VPN 网关，或者在 SSL VPN 访问实例视图下执行 gateway 命令，引用 SSL VPN 网关

SSL VPN 访问实例的显示信息如下：

```
[Device] display sslvpn context
Context name: ctx
  Operation state: Up
  Associated SSL VPN gateway: gw
  SSL client policy configured: sslnew
  SSL client policy in use: ssl
```

(5) 排查上下行链路是否正常，以下情况会导致上下行链路不通：

a. SSL VPN 网关没有配置到达内网资源的路由，可通过查看设备路由表确认

b. 内网服务器未配置回程路由导致链路不通

c. 地址冲突导致链路不通

d. 配置了策略路由导致链路不通

e. 配置了负载均衡导致链路不通

f. 设备是双主模式，请将设备修改为主备模式，并将上下行接口修改成冗余口

14.3.3 故障诊断命令

表14-3 故障诊断命令

命令	说明
url-item	用来创建URL表项，并进入URL表项视图。如果指定的URL表项已经存在，则直接进入URL表项视图。
url-list	用来创建URL列表并进入URL列表视图。如果指定的URL列表已经存在，则直接进入URL列表视图。
url	用来配置资源的URL。
heading	用来配置URL列表标题。
resources url-item	用来配置URL列表引用的URL表项。
policy-group	用来创建策略组，并进入SSL VPN策略组视图。如果指定的策略组已经存在，则直接进入策略组视图。
resources url-list	用来配置策略组引用URL列表。
filter web-access acl	用来配置对Web接入进行高级ACL过滤。
display sslvpn context	显示SSL VPN访问实例的信息

命令	说明
display sslvpn gateway	显示SSL VPN网关的信息

14.4 iNode客户端无法获取SSL VPN网关信息

14.4.1 故障描述

在浏览器中输入 SSL VPN 网关地址，无法打开 SSL VPN 网关页面，或通过 iNode 输入 SSL VPN 网关地址后，提示无法获取 SSL VPN 网关信息。

14.4.2 故障处理步骤

(1) 确认 SSL VPN 网关地址是否可达，设备允许 Ping 的情况下可通过 Ping 确认，不允许 Ping 的情况下可通过抓包确认。

(2) 通过查看 SSL VPN 网关的显示信息，确认 SSL VPN 网关的状态：

a. 确认 SSL VPN 网关是否处于 Up 状态。通过查看显示信息中 Operation state 字段的值，若值为 Up，则表示 SSL VPN 网关处于 Up 状态，否则需要在 Web 界面单击 SSL VPN 网关的使能按钮，或者在 SSL VPN 网关视图下执行 service enable 命令开启 SSL VPN 网关

b. 重新配置或修改 SSL 服务端策略后，只有执行 undo service enable 命令关闭 SSL VPN 网关，并执行 service enable 命令重新开启 SSL VPN 网关后，新的策略才会生效

c. SSL 相关配置是否正确，缺省情况下设备使用自带的缺省证书，当需要使用非缺省证书时，可以引用 SSL 服务端策略。

SSL VPN 网关的显示信息如下：

```
[Device] display sslvpn gateway
Gateway name: gw
  Operation state: Up
  IP: 1.1.1.2  Port: 2000
  SSL server policy configured: sslnew
  SSL server policy in use: ssl
  Front VPN instance: Not configured
```

(3) 通过查看 SSL VPN 访问实例的显示信息，确认 SSL VPN 访问实例的状态：

a. 确认 SSL VPN 访问实例是否处于 Up 状态。通过查看显示信息中 Operation state 字段的值，若值为 Up，则表示 SSL VPN 访问实例处于 Up 状态，否则需要在 Web 界面单击 SSL VPN 访问实例的使能按钮，或者在 SSL VPN 访问实例视图下执行 service enable 命令开启 SSL VPN 访问实例

b. 确认 SSL VPN 访问实例是否引用了 SSL VPN 网关。通过查看显示信息中 Associated SSL VPN gateway 字段的值，若有引用的网关名称，则表示成功引用了 SSL VPN 网关，否则，需要在 Web 界面 SSL VPN 访问实例下引用 SSL VPN 网关，或者在 SSL VPN 访问实例视图下执行 gateway 命令，引用 SSL VPN 网关

SSL VPN 访问实例的显示信息如下：

```
[Device] display sslvpn context
Context name: ctx
```

```
  Operation state: Up
  Associated SSL VPN gateway: gw
  SSL client policy configured: sslnew
  SSL client policy in use: ssl
```

(4) 确认网关地址和端口是否被正确侦听，需要确认每个业务板侦听端口是否正确开启。

TCP 代理连接的显示信息如下：

```
<Device> dis tcp-proxy slot 1
Local Addr:port       Foreign Addr:port     State            Service type
1.1.1.2:2000           0.0.0.0:0                  LISTEN       SSLVPN
```

14.4.3 故障诊断命令

表14-4 故障诊断命令

命令	说明
display tcp-proxy	显示TCP代理连接的简要信息
display sslvpn context	显示SSL VPN访问实例的信息
display sslvpn gateway	显示SSL VPN网关的信息

14.5 iNode客户端无法登陆SSL VPN网关

14.5.1 故障描述

在 iNode 客户端上输入 SSL VPN 网关地址后，可以获取 SSL VPN 网关信息，但是无法登陆。

14.5.2 故障处理步骤

(1) 确认 SSL VPN 网关地址是否可达，设备允许 Ping 的情况下可通过 Ping 确认，不允许 Ping 的情况下可通过抓包确认。

(2) 通过查看 SSL VPN 网关的显示信息，确认 SSL VPN 网关的状态：

a. 确认 SSL VPN 网关是否处于 Up 状态。通过查看显示信息中 Operation state 字段的值，若值为 Up，则表示 SSL VPN 网关处于 Up 状态，否则需要在 Web 界面单击 SSL VPN 网关的使能按钮，或者在 SSL VPN 网关视图下执行 service enable 命令开启 SSL VPN 网关

b. 重新配置或修改 SSL 服务端策略后，只有执行 undo service enable 命令关闭 SSL VPN 网关，并执行 service enable 命令重新开启 SSL VPN 网关后，新的策略才会生效

c. SSL 相关配置是否正确，缺省情况下设备使用自带的缺省证书，当需要使用非缺省证书时，可以引用 SSL 服务端策略。当不需要使用非缺省证书时，删除 SSL 服务端策略引用即可

SSL VPN 网关的显示信息如下：

```
[Device] display sslvpn gateway
Gateway name: gw
  Operation state: Up
  IP: 1.1.1.2  Port: 2000
  SSL server policy configured: sslnew
  SSL server policy in use: ssl
```

```
Front VPN instance: Not configured
```

(3) 通过查看 SSL VPN 访问实例的显示信息，确认 SSL VPN 访问实例的状态：

a. 确认 SSL VPN 访问实例是否处于 Up 状态。通过查看显示信息中 Operation state 字段的值，若值为 Up，则表示 SSL VPN 访问实例处于 Up 状态，否则需要在 Web 界面单击 SSL VPN 访问实例的使能按钮，或者在 SSL VPN 访问实例视图下执行 service enable 命令开启 SSL VPN 访问实例

b. 确认 SSL VPN 访问实例是否引用了 SSL VPN 网关。通过查看显示信息中 Associated SSL VPN gateway 字段的值，若有引用的网关名称，则表示成功引用了 SSL VPN 网关，否则，需要在 Web 界面 SSL VPN 访问实例下引用 SSL VPN 网关，或者在 SSL VPN 访问实例视图下执行 gateway 命令，引用 SSL VPN 网关

SSL VPN 访问实例的显示信息如下：

```
[Device] display sslvpn context
Context name: ctx
  Operation state: Up
  Associated SSL VPN gateway: gw
  SSL client policy configured: sslnew
  SSL client policy in use: ssl
```

(4) 确认 SSL VPN 网关地址和端口是否被正确侦听，需要确认每个业务板的侦听端口是否正确开启。

TCP 代理连接的显示信息如下：

```
<Device> display tcp-proxy slot 1
Local Addr:port       Foreign Addr:port     State            Service type
1.1.1.2:2000           0.0.0.0:0                    LISTEN       SSLVPN
```

(5) 确认是否配置了 SSL VPN AC 接口（需要配置 IP 地址），且在 SSL VPN 访问实例下引用了该 SSL VPN AC 接口。

SSL VPN AC 接口的配置及显示如下：

```
[Device] interface SSLVPN-AC 1
[Device-SSLVPN-AC1] ip address 1.1.1.1 24
[Device-SSLVPN-AC1] quit
[Device] sslvpn context ctx
[Device-sslvpn-context-ctx] ip-tunnel interface SSLVPN-AC 1
[Device-sslvpn-context-ctx] quit
[Device] display interface SSLVPN-AC 1 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface                   Link   Protocol    Primary IP      Description
SSLVPN-AC1           UP    UP            1.1.1.1
```

(6) 确认是否配置了地址池，并且在 SSL VPN 访问实例或用户可授权的资源组下引用了该地址池，地址池中不能包含 SSL VPN 网关地址。

地址池的配置及引用举例如下：

```
[Device] sslvpn ip address-pool name 1.1.1.1 1.1.1.10
[Device] sslvpn context ctx
[Device-sslvpn-context-ctx] ip-tunnel address-pool name mask 24
```

(7) 确认 SSL VPN 用户是否配置正确：

a. 本地用户：确保用户类型为网络接入类，服务类型为 SSL VPN，且为用户配置 SSL VPN 资源组。

b. 远程用户：确保远程认证服务器上用户隶属的用户组，已在 SSL VPN 访问实例中配置对应名称的 SSL VPN 资源组。

(8) 若开启了客户端和服务器端证书认证，确保两端已正确安装证书。

(9) iNode 客户端是否为最新版本。

14.5.3 故障诊断命令

表14-5 故障诊断命令

命令	说明
display tcp-proxy	显示TCP代理连接的简要信息
display sslvpn context	显示SSL VPN访问实例的信息
display sslvpn gateway	显示SSL VPN网关的信息
sslvpn ip address-pool	用来创建IPv4地址池
ip-tunnel address-pool	用来配置IP接入引用IPv4地址池。

14.6 iNode客户端无法访问内网资源

14.6.1 故障描述

通过 iNode 客户端登录 SSL VPN 网关后，无法访问内网服务器资源。

14.6.2 故障处理步骤

(1) SSL VPN AC 接口是否加入了安全域，且被安全策略放行。

(2) iNode 客户端分配到的虚拟网卡 IP 地址是否被安全策略放行。

(3) 确认是否配置了能够放行通往后台服务器的 ACL 或者 URI ACL 规则，并且引用规则已经添加：

```
[Device-sslvpn-context-ctxip1] policy-group resourcegrp1
[Device-sslvpn-context-ctxip1-policy-group-resourcegrp1] filter web-access acl 3000
```

(4) SSL VPN 网关是否可以 Ping 通后台资源地址，是否需要在对端设备上添加路由。

(5) iNode 客户端是否为最新版本。

(6) 排查上下行链路是否正常，以下情况会导致上下行链路不通：

a. SSL VPN 网关没有配置到达内网资源的路由，可通过查看设备路由表确认

b. 内网服务器未配置回程路由导致链路不通

c. 设备是双主模式，请将设备修改为主备模式，并将上下行接口修改成冗余口

d. 地址冲突导致链路不通

e. 配置了策略路由导致链路不通

f. 配置了负载均衡导致链路不通

14.6.3 故障诊断命令

表14-6 故障诊断命令

命令	说明
policy-group	用来创建策略组，并进入SSL VPN策略组视图。如果指定的策略组已经存在，则直接进入策略组视图。
filter web-access acl	用来配置对Web接入进行高级ACL过滤。

14.7 iNode用户无法老化下线

14.7.1 故障描述

部分 iNode 用户，长时间不访问内网资源时，不老化下线，占用 License 资源。

14.7.2 故障处理步骤

iNode 客户端会定时发送保活报文，无法老化下线，可通过配置空闲超时时间，将长时间不访问内网资源用户强制下线

通过配置 SSL VPN 会话保持空闲状态的流量阈值，对 iNode 客户端空闲用户进行老化下线。具体配置如下：

```
<Device> system-view
[Device] sslvpn context ctx1
[Device-sslvpn-context-ctx1] idle-cut traffic-threshold 1000
```

14.7.3 故障诊断命令

表14-7 故障诊断命令

命令	说明
sslvpn context	用来创建SSL VPN访问实例，并进入SSL VPN访问实例视图。如果指定的SSL VPN访问实例已经存在，则直接进入SSL VPN访问实例视图。
idle-cut traffic-threshold	用来配置SSL VPN会话保持空闲状态的流量阈值。

14.8 配置用户过滤、监控、绑定IP地址等功能不生效

14.8.1 故障描述

本地用户在 local-user 下配置了 ACL、监控、绑定 IP 地址等功能不生效。

14.8.2 故障处理步骤

SSL VPN 用户的部分管理配置，需要在 SSL VPN 访问实例下配置，不能在 local-user 用户视图下配置。

14.8.3 故障诊断命令

表14-8 故障诊断命令

命令	说明
sslvpn context	用来创建SSL VPN访问实例，并进入SSL VPN访问实例视图。如果指定的SSL VPN访问实例已经存在，则直接进入SSL VPN访问实例视图。

14.9 用户曾经登录SSL VPN网关成功，再次登录时失败

14.9.1 故障描述

用户曾经登录 SSL VPN 网关成功，后续再次登录时失败。

14.9.2 故障处理步骤

(1) 查看 SSL VPN 访问实例下是否配置了同一用户名登录限制个数。

```
[Device] sslvpn context ctx
[Device-sslvpn-context-ctx] max-onlines 1
```

(2) 如果不需要限制同一用户名最大上线数，可删除 max-onlines 配置，如果确实需要限制，可配置如下功能。开启本功能后，将从该用户的在线连接中选择一个空闲时间最长的，强制其下线，新登录用户上线：

```
[Device] sslvpn context ctx
[Device-sslvpn-context-ctx] force-logout max-onlines enable
```

14.9.3 故障诊断命令

表14-9 故障诊断命令

命令	说明
sslvpn context	用来创建SSL VPN访问实例，并进入SSL VPN访问实例视图。如果指定的SSL VPN访问实例已经存在，则直接进入SSL VPN访问实例视图。
force-logout max-onlines enable	用来开启达到最大在线数时的用户强制下线功能。

14.10 用户配置企业微信认证失败

14.10.1 故障描述

用户配置企业微信认证功能，使用企业微信客户端访问资源失败

14.10.2 故障处理步骤

(1) 查看设备是否配置 DNS 服务器。

(2) 确认是够有可信 SSL 证书。

(3) SSLVPN 访问实例中引用的网关访问方式是否为直接访问网关。

```
[H3C]sslvpn context ctx
#
[H3C-sslvpn-context-ctx]display this
sslvpn context ctx
 gateway gw domain sslvpn
```

(4) 确认 SSLVPN 访问实例中的参数是否配置正确，包括 API 服务器地址、企业 ID、访问密钥、授权策略组字段名，资源组名称，如果配置了授权策略组，资源组的名称需要与企业微信管理平台上用户所在部门 ID 值一致，如果未配置授权策略组，需要有一个缺省的资源组。

```
[H3C]sslvpn context ctx
[H3C-sslvpn-context-ctx]display this
#
sslvpn context ctx
 gateway gw domain sslvpn
 wechat-work-authentication enable
 wechat-work-authentication url https://qyapi.weixin.qq.com
 wechat-work-authentication corp-id ww918e2ea10664acd3
 wechat-work-authentication app-secret agZO0L15DmOBw-BBx9s5UmOForvCx-WEtKQWqfBQy
Ts
 wechat-work-authentication authorize-field department
 wechat-work-authentication              open-platform-url              user-defined
https://open.weixin.qq.com
```

(5) 登录企业微信管理平台，查看应用配置的主页链接是否正确。

14.10.3 故障诊断命令

表14-10 故障诊断命令

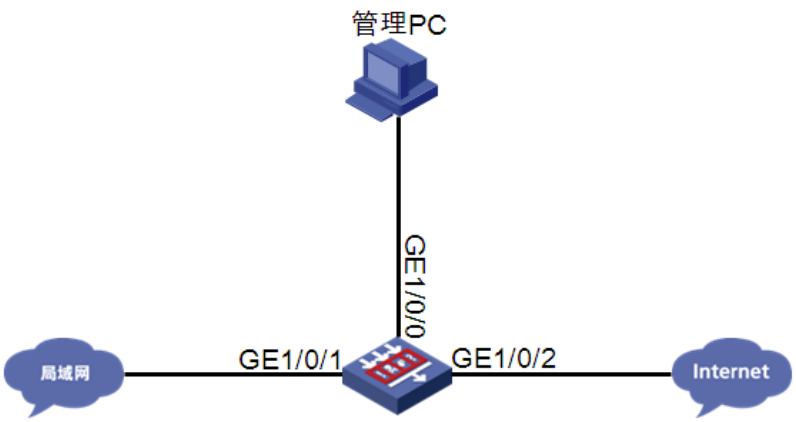
命令	说明
sslvpn context	用来创建SSL VPN访问实例，并进入SSL VPN访问实例视图。如果指定的SSL VPN访问实例已经存在，则直接进入SSL VPN访问实例视图。
gateway	命令用来配置SSL VPN访问实例引用SSL VPN网关。
wechat-work-authentication enable	用来开启企业微信认证功能。
wechat-work-authentication url	用来配置企业微信API服务器的URL地址。

命令	说明
wechat-work-authentication corp-id	用来配置企业微信认证使用的企业ID。
wechat-work-authentication app-secret	用来配置企业微信认证中企业应用数据的访问密钥。
wechat-work-authentication authorize-field	用来配置企业微信授权策略组字段名。
wechat-work-authentication open-platform-url	用来配置微信开放平台的URL地址。

15 DPI 故障处理

15.1 正常业务流量被IPS/AV误报攻击拦截

15.1.1 故障描述



组网需求：

局域网内 PC 通过防火墙访问 Internet，防火墙上开启 IPS、AV 业务。保护内网用户免遭受攻击。

配置描述

安全策略中开启 IPS、AV 检测。

```
#
app-profile 0_IPv4
 ips apply policy default mode protect
 anti-virus  apply policy default mode protect
#
  security-policy ip
 rule 0 name ips
  action pass
  profile 0_IPv4
#
```

故障描述

内网用户发起的正常业务流量访问不成功，设备上报 IPS/AV 攻击日志。

15.1.2 故障处理步骤

(1) 首先观察设备上报的 IPS/AV 攻击日志，源目的 IP 端口是否为客户端、服务器的 IP 端口，如果是则记录 IPS/AV 日志中对应的 AttackID。

(2) 如果是 IPS 误报，创建 IPS 策略，将报攻击的 IPS 特征关闭或者将动作设置为 permit 加 log，并在安全策略中引用。

(3) 如果是 AV 误报，创建 AV 策略，将报攻击的 AV 特征设置为例外或者将动作设置为 permit 加 log，并在安全策略中引用。

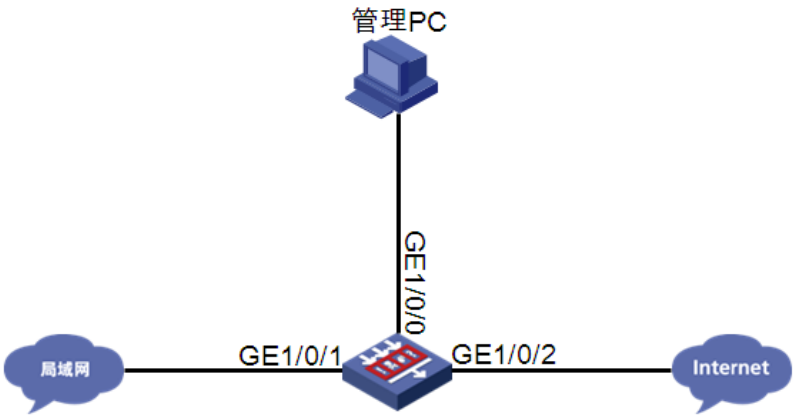
(4) 抓取客户端访问业务的报文并反馈给研发进行分析，确认是否为误报，如果为误报则修改对应特征，如果非误报则对用户进行解释并在配置中对该条特征进行放行。

15.1.3 故障诊断命令

命令	说明
ips policy *policy-name*	缺省情况下，存在一个缺省IPS策略，名称为default，且不能被修改和删除
signature override { **pre-defined** | **user-defined** } **signature-id** { { **disable** | **enable** } [{ **block-source** | **drop** | **permit** | **redirect** | **reset** } | **capture** | **logging**] * }	缺省情况下，预定义IPS特征使用系统预定义的状态和动作，自定义IPS特征的动作和状态在管理员导入的特征库文件中定义。 缺省IPS策略中的IPS特征的动作属性和生效状态属性不能被修改
anti-virus policy *policy-name*	缺省情况下，存在一个缺省防病毒策略，名称为default，且不能被修改和删除
exception signature *signature-id*	命令用来配置病毒例外

15.2 IPS/WAF攻击流量不能被阻断，设备不报攻击日志

15.2.1 故障描述



组网需求：

局域网内 PC 通过防火墙访问 Internet，防火墙上开启 IPS/WAF 业务。保护内网用户免遭受攻击。

配置描述

安全策略中开启 IPS、WAF 检测。

```
#
app-profile 0_IPv4
 ips apply policy default mode protect
 waf apply policy default mode protect
#
  security-policy ip
 rule 0 name ips
  action pass
  profile 0_IPv4
#
```

故障描述

攻击者从 Internet 向局域网发起典型攻击，如跨站脚本攻击，暴力破解攻击等，攻击报文成功通过 IPS 设备到达靶机服务器，成功破解靶机服务器密码，IPS 设备上无日志输出。

15.2.2 故障处理步骤

(1) 检查设备是否安装了 License。

(2) 查看设备当前的 DPI 状态，设备运行状态为 normal。

```
[H3C]display inspect status
Chassis 0 Slot 1:
Running status: normal
```

(3) 查看特征库版本是否为发布的最新版本，如果版本较老，请进行特征库升级。

```
<H3C>display  ips signature  library
IPS signature library information:
```

```
Type      SigVersion         ReleaseTime               Size
Current   1.0.81             Thu Oct 31 08:35:05 2019  4639264
Last      1.0.80             Sat Oct 12 07:58:23 2019  4565664
Factory   1.0.0              Fri Dec 28 06:27:33 2018  76496

<H3C>display  waf signature library
WAF signature library information:
Type      SigVersion         ReleaseTime               Size(bytes)
Current   1.0.2              Thu Oct 31 03:22:10 2019  1018752
Last      1.0.0              Fri Dec 28 08:53:30 2018  19824
Factory   1.0.0              Fri Dec 28 08:53:30 2018  19824
```

(4) 查看 IPS/WAF 规则是否下发引擎，如果没有下发 IPS/WAF 规则，需要在系统视图下执行 inspect activate 或通过 Web 激活引擎，重新下发规则。

```
[H3C-probe]display  system  internal  inspect  dim-rule
Slot 1:
MdcID       MoudleName  Total MD5 rules
0           Anti-Virus  0

MdcID       RuleID      ModuleName          L4ProName           uiAppIdL5

0           1               IPS                 TCP              HTTP

0           2147483649      FFILTER             TCP

0           2               IPS                 TCP               HTTP

0           2147483650      FFILTER             TCP

0           2147483651      FFILTER             TCP

0           4               IPS                 TCP              HTTP

0           2147483652      FFILTER             TCP

0           5               IPS                 TCP            HTTP

[H3C-probe]display  system  internal  inspect  dim-rule | include WAF
0           1           WAF                 TCP                 HTTP

0           16          WAF                 TCP                 HTTP

0           37          WAF                 TCP                 HTTP

0           38          WAF                 TCP                 HTTP

0           43          WAF                 TCP                 HTTP
```

(5) 查看会话是否建立，确保会话的源目 IP 在指定的安全域内，并且在该域间启用深度检查功能，引用 IPS/WAF 策略。

```
[H3C]display session table ipv4 source-ip 1.1.1.101 verbose
Slot 1:
Initiator:
  Source      IP/port: 1.1.1.101/34679
  Destination IP/port: 2.2.2.12/5190
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
```

```
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/10
  Source security zone: Trust
Responder:
  Source      IP/port: 2.2.2.12/5190
  Destination IP/port: 1.1.1.101/34679
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/11
  Source security zone: Untrust
State: TCP_ESTABLISHED
Application: AOL
Start time: 2016-01-21 16:13:16  TTL: 1194s
Initiator->Responder:            3 packets        930 bytes
Responder->Initiator:            1 packets         92 bytes

Total sessions found: 1
```

(6) 查看 rule hit 情况。

```
[H3C-probe]display  system  internal inspect  hit-statistics
Slot 1:
Rule ID     Module      Rule hits  AC hits    PCRE try   PCRE hits
5041        APR         0          3          0          0
5126        APR         0          9          0          0
5127        APR         0          9          0          0
8584        IPS         1          2          0          0
9410        APR         0          1          0          0
21768       IPS         0          2          0          0
21852       IPS         1          2          0          0
22114       IPS         0          2          0          0
22406       IPS         1          1          0          0
23089       IPS         2          2          4          2
23213       IPS         0          4          2          2
23271       IPS         0          2          1          0
23341       IPS         1          2          1          1
23722       IPS         2          8          2          2
23804       IPS         0          1          0          0
18096       WAF         0          4          2          0
23311       WAF         1          14         1          1
23791       WAF         0          2          1          0
23915       WAF         0          8          4          0
```

(7) 如果有 rule hits 统计，查看该规则是状态是否使能，如果未使能，手工将该条规则使能并设置动作（只有自定义的 IPS、WAF 策略能修改规则状态）。

```
[H3C]display  ips signature pre-defined 8
 Type        : Pre-defined
 Signature ID: 8
 Status      : Disable
 Action      : Permit & Logging
```

```
 Name         : (MS11-015)DVR-MS_Vulnerability
 Protocol     : TCP
 Severity     : Critical
 Fidelity     : Medium
 Direction    : To-client
 Category     : Vulnerability
 Reference    : CVE-2011-0042;MS11-015;

[H3C]display  waf  signature  pre-defined 56
 Type         : Pre-defined
 Signature ID: 56
 Status       : Disable
 Action       : Permit & Logging
 Name         : CVE-2012-3351_LongTail_JW_Player_XSS_Vulnerability
 Protocol     : TCP
 Severity     : Medium
 Fidelity     : Medium
 Direction    : To-server
 Category     : Vulnerability
 Reference    : CVE-2012-3351;
```

创建自定义 IPS/WAF 策略并在安全策略引用，在自定义 IPS/WAF 策略中手工将该条规则使能。

```
[H3C-ips-policy-ips]signature override pre-defined 8 enable reset logging
[H3C-waf-policy-waf]signature override pre-defined 56 enable  reset logging
```

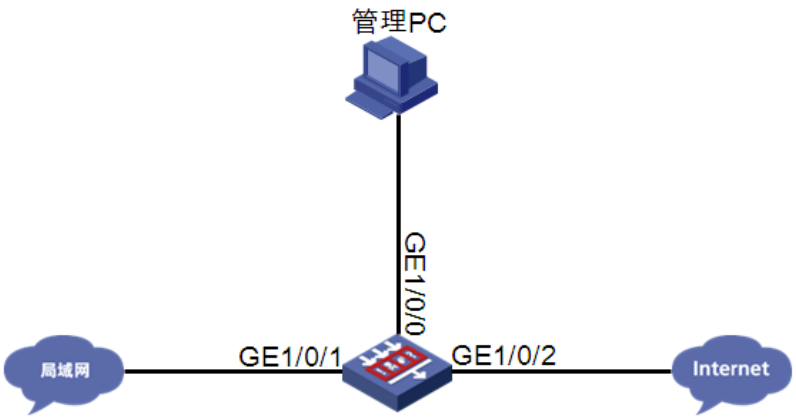
(8) 前面都检查没有问题后设备还是不能识别，有可能构造的攻击不对或特征库不支持该攻击，此时需要协助抓取对应的攻击交互报文反馈报文给研发进行分析。

15.2.3 故障诊断命令

命令	说明
ips policy *policy-name*	缺省情况下，存在一个缺省IPS策略，名称为default，且不能被修改和删除
waf policy *policy-name*	缺省情况下，存在一个缺省WAF策略，名称为default，且不能被修改和删除
signature override { **pre-defined** | **user-defined** } *signature-id* { { **disable** | **enable** } [{ **block-source** | **drop** | **permit** | **redirect** | **reset** } | **capture** | **logging**] * }	缺省情况下，预定义IPS、WAF特征使用系统预定义的状态和动作，自定义IPS、WAF特征的动作和状态在管理员导入的特征库文件中定义 缺省IPS、WAF策略中的IPS、WAF特征的动作属性和生效状态属性不能被修改
inspect activate	缺省情况下，DPI各业务模块自定义的规则或手动离线升级的特征库不生效
display system internal inspect hit-statistics [**module-id**] [**rule-id**] [**slot slot-number** [**cpu cpu-number**]]	显示应用层检测规则命中的统计信息
display inspect status	显示应用层检测引擎的运行状态

15.3 特定应用限速不生效

15.3.1 故障描述



组网需求：

局域网内 PC 通过防火墙访问 Internet，设备开启带宽管理功能，限制迅雷下载速度。

配置描述

创建 AVC 策略，对迅雷下载进行限速。

```
traffic-policy
 rule 1 name Thunder
  action qos profile Thunder_20M
  source-zone Trust
  destination-zone Untrust
  application app-group 1
 profile name thunder_20m
  bandwidth downstream maximum 20000
  bandwidth upstream maximum
```

故障描述

迅雷下载速度不受带宽管理限制。

15.3.2 故障处理步骤

(1) 查看 APR 版本信息，是否为最新版本，如果版本较老，请从官网上获取最新版本进行升级。

(2) 查看设备引擎状态，是否 bypass，如果进行了手工 bypass 或 cpu、memory 自动 bypass，可以通过 **undo inspect bypss** 命令重新激活引擎。

(3) 查看规则状态是否为使能状态，对应流量是否优先走了其他规则。

```
[H3C]display traffic-policy statistics bandwidth total per-rule
Slot 1 :
Codes: PP(Passed Packets), PB(Passed Bytes), DP(Dropped Packets), DB(Dropped Byt
es), PR(Passed Rate:kbps), DR(Dropped Rate:kbps), FPP(Final Passed Packets), FPB
```

```
(Final Passed Bytes),FPR(Final Passed Rate:kbps)
------------------------------------------------------------------------------
-------------------------------------------------
 Rule name  State    Profile name PP          PB          DP          DB          PR
         DR          FPP         FPB         FPR
------------------------------------------------------------------------------
-------------------------------------------------
 Thunder    Enabled  Thunder_20M  0           0           0           0           0.
0         0.0         0           0           0.0
------------------------------------------------------------------------------
-------------------------------------------------
------------------------------------------------------------------------------
-----------------------------------------
```

如果流量优先走了其他规则，可以移动迅雷限速规则，将迅雷优先级提前。

```
[H3C-traffic-policy]rule move Thunder before b
```

(4) 查看会话信息中的 Application 信息，将对应的 Application 加入到自定义应用组中，并配置对应的应用组限速。

(5) 如果会话的 Application 大多数为 GENERAL_TCP 或 GENERAL_UDP，有可能是迅雷出现了新的特征，这个时候需要一线协助帮忙转包反馈给研发进行分析。

```
<H3C>display session table ipv4 verbose
Slot 1:
Initiator:
  Source      IP/port: 1.1.1.195/51353
  Destination IP/port: 2.2.2.51/59287
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/10
  Source security zone: Trust
Responder:
  Source      IP/port: 2.2.2.51/59287
  Destination IP/port: 1.1.1.195/51353
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/11
  Source security zone: Untrust
State: TCP_SYN_RECV
Application: GENERAL_TCP
Start time: 2016-01-21 17:51:44  TTL: 951s
Initiator->Responder:            1 packets         56 bytes
Responder->Initiator:            1 packets         56 bytes
```

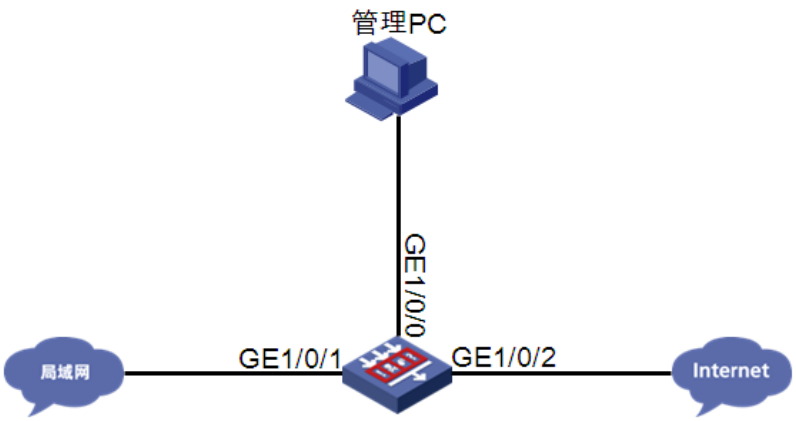
15.3.3 故障诊断命令

命令	说明
traffic-policy	进入带宽策略视图

命令	说明
rule move *rule-name1* { **after** | **before** } *rule-name2*	移动带宽策略规则的排列顺序
display traffic-policy statistics bandwidth { **downstream** | **total** | **upstream** } { **per-ip** { **ipv4** [**ipv4-address**] | **ipv6** [**ipv6-address**] } **rule rule-name** | **per-rule** [**name rule-name**] | **per-user** [**user user-name**] **rule rule-name** }	显示带宽策略规则下流量速率的统计信息（分布式设备-独立运行模式/集中式IRF设备）

15.4 文件过滤/数据过滤不生效，且没有产生日志

15.4.1 故障描述



组网需求：

局域网内 PC 通过防火墙访问 Internet，防火墙上开启文件过滤/数据过滤业务。保护内外网用户文件&数据传输信息安全。

配置描述

安全策略中开启文件过滤检测。

```
 #
file-filter policy ffilter
 rule ffilter
  filetype-group ffilter
  application all
  direction both
  action drop logging
#
file-filter filetype-group ffilter
 pattern 0 text pe
 pattern 1 text elf
 pattern 10 text vsdx
 pattern 11 text msg
 pattern 12 text pub
 pattern 13 text zip
```

```
 pattern 14 text rar
 pattern 15 text tar.gz
 pattern 16 text tgz
 pattern 2 text doc
 pattern 3 text pdf
 pattern 4 text xls
 pattern 5 text ppt
 pattern 6 text docx
 pattern 7 text xlsx
 pattern 8 text pptx
 pattern 9 text vsd
#
```

安全策略中开启数据过滤检测。

```
#
data-filter keyword-group dfilter
 pre-defined-pattern name bank-card-number
 pre-defined-pattern name credit-card-number
 pre-defined-pattern name id-card-number
 pre-defined-pattern name phone-number
#
data-filter policy dfilter
 rule dfilter
  keyword-group dfilter
  application all
  direction both
  action drop logging
#
app-profile 0_IPv4
 file-filter apply policy ffilter
 data-filter apply policy dfilter
#
security-policy ip
 rule 0 name ffilter
  action pass
  profile 0_IPv4
#
```

故障描述

使用者从局域网向 Internet 上传机密文件，例如.docx 文件和.xls 文件等，文件成功上传，且设备无日志。

使用者从局域网向 Internet 上传含有敏感信息的数据，例如含有银行卡号和身份证号等数据，数据成功上传，且设备无日志。

15.4.2 故障处理步骤

(1) 查看设备当前的 DPI 状态，设备运行状态为 normal。

```
[H3C]display inspect status
Chassis 0 Slot 1:
```

```
Running status: normal
```

(2) 查看传输的文件类型是否被引用的文件类型组所包含。

(3) 通过抓包查看传输的协议是否为支持的协议类型，目前，文件过滤和数据过滤功能支持对基于 HTTP、FTP、SMTP、IMAP、NFS、POP3、RTMP 和 SMB 协议传输的文件进行检测和过滤。

(4) 查看文件过滤规则是否下发引擎，如果没有下发文件过滤和数据过滤规则，ruleid 有 10 位数的为预定义文件过滤和数据过滤规则，需要在系统视图下执行 inspect activate 或通过 Web 激活引擎，重新下发规则。

```
[H3C-probe]display  system  internal  inspect dim-rule | include FFILTER

 23          FFILTER             TCP                 HTTP

0            2147483671  FFILTER             TCP

1            24          FFILTER             TCP                 FTP

0            2147483672  FFILTER             TCP

1            25          FFILTER             TCP                 SMTP

0            2147483673  FFILTER             TCP

1            26          FFILTER             TCP                 IMAP

0            2147483674  FFILTER             TCP

1            27          FFILTER             TCP                 POP3

0            2147483675  FFILTER             TCP

1            28          FFILTER             TCP                 NFS

0            2147483676  FFILTER             TCP

1            29          FFILTER             TCP                 MICROSOFT-DS

1            30          FFILTER             TCP                 RTMP

[H3C-probe]display  system  internal  inspect  dim-rule | include DFILTER
1            24          DFILTER             TCP                 HTTP

1            25          DFILTER             TCP                 FTP-DATA

1            26          DFILTER             TCP                 SMTP

1            27          DFILTER             TCP                 IMAP

1            28          DFILTER             TCP                 POP3

1            29          DFILTER             TCP                 NFS

1            30          DFILTER             TCP                 MICROSOFT-DS

1            31          DFILTER             TCP                 RTMP
```

(5) 查看会话是否建立，确保会话的源目 IP 在指定的安全域内，并且在该域间启用深度检查功能，引用文件过滤策略或数据过滤策略。

```
[H3C-probe]display  session table ipv4 source-ip 7.0.1.2 verbose
Slot 2:
Initiator:
  Source      IP/port: 7.0.1.2/50779
```

```
  Destination IP/port: 7.0.0.2/80
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/2
  Source security zone: Trust
Responder:
  Source      IP/port: 7.0.0.2/80
  Destination IP/port: 7.0.1.2/50779
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/3
  Source security zone: Untrust
State: TCP_ESTABLISHED
Application: HTTP
Rule ID: 0
Rule name: ips
Start time: 2019-11-15 11:31:01  TTL: 1197s
Initiator->Responder:            7 packets       1073 bytes
Responder->Initiator:            7 packets       2413 bytes

Total sessions found: 1
```

(6) 查看 rule hit 情况。

```
[H3C-probe]display system  internal  inspect hit-statistics
Slot 2:
Rule ID     Module      Rule hits  AC hits    PCRE try   PCRE hits
2147483650  FFILTER     2          2          0          0
2147483657  FFILTER     1          1          0          0
2147483669  FFILTER     2          2          0          0
3432        APR         2          2          0          0
```

如果没有自定义的规则命中，则需要检查传输的文件的真实文件类型与扩展名是否一致，敏感信息是否有误，文件过滤还可以通过如下配置后，观察是否可以拦截，和产生日志。

```
[H3C]file-filter false-extension action drop
```

(7) 前面都检查没有问题后设备还是不能识别，有可能此时传输的文件编码方式设备暂不支持，此时需要协助抓取对应的交互报文反馈报文给研发进行分析。

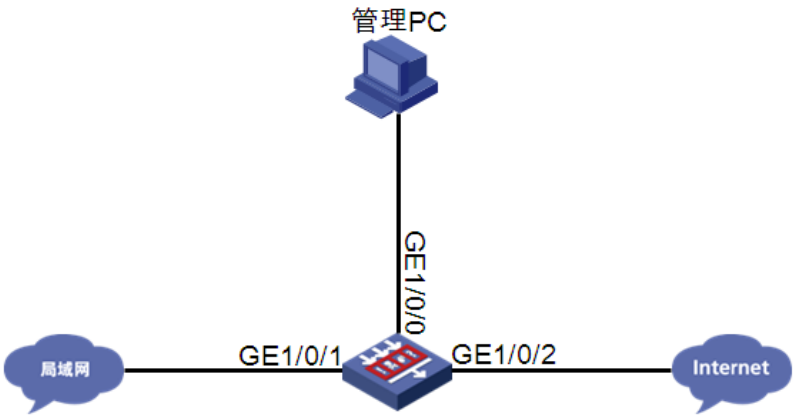
15.4.3 故障诊断命令

命令	说明
file-filter policy *policy-name*	缺省情况下，存在一个缺省文件过滤策略，名称为default，且不能被修改和删除
filetype-group *group-name*	文件过滤规则中引用缺省文件类型组。名称为default，且不能被修改和删除
inspect activate	缺省情况下，DPI各业务模块自定义的规则或手动离线升级的特征库不生效

命令	说明
display system internal inspect hit-statistics [module-id] [rule-id] [slot slot-number [cpu cpu-number]]	显示应用层检测规则命中的统计信息
display inspect status	显示应用层检测引擎的运行状态
file-filter false-extension action { drop | permit }	配置文件的真实类型与扩展名不一致时执行的动作
data-filter apply policy policy-name	缺省情况下，DPI应用profile中未引用数据过滤策略
data-filter keyword-group *keywordgroup-name*	数据过滤规则中引用缺省关键字组。名称为default，且不能被修改和删除
inspect activate	缺省情况下，DPI各业务模块自定义的规则或手动离线升级的特征库不生效
display inspect status	显示应用层检测引擎的运行状态

15.5 开启SSL卸载，Web页面没有成功卸载

15.5.1 故障描述



组网需求：

局域网内 PC 通过防火墙访问 Internet，防火墙上开启 SSL 过滤业务和 IPS 业务。保护内外网用户 HTTPS 传输安全。

配置描述

安全策略中开启 SSL 卸载。

```
#
app-proxy-policy
   rule 1 name ssl-proxy
  action ssl-decrypt
```

```
  #
app-profile 0_IPv4
 ips apply policy default mode protect
#
security-policy ip
 rule 0 name ips
  action pass
  profile 0_IPv4
#
```

故障描述

攻击者从 Internet 向局域网发起 HTTPS 加密流量攻击，如跨站脚本攻击，暴力破解攻击等，攻击报文成功通过 IPS 设备到达靶机服务器，成功破解靶机服务器密码，IPS 设备上无日志输出。SSL 卸载失效。

15.5.2 故障处理步骤

(1) 使用 HTTP 非加密流量，查看设备是否拦截，如果依然不能拦截，请参考 13.2，排查 IPS 问题原因。如果能拦截，则依照下面的方法排除原因。

(2) 使用如下命令，查看设备是否成功代理。

```
[H3C]display  app-proxy server-certificate
Slot 1:
    Total server certificates: 1
    Certificate info: BreakingPoint_serverA_2048.server.int
         Proxy count: 6996
         Most recent proxy time: 2019/11/18 10:23:48
         First proxy at: 2019/11/15 17:21:12
```

(3) 检查设备组网是否为三层组网。目前 SSL 卸载不支持二层组网，如果是二层组网，请修改组网。

(4) 查看设备当前的 DPI 状态，设备运行状态为 normal。

```
[H3C]display inspect status
Chassis 0 Slot 1:
Running status: normal
```

(5) 使用如下命令，查看 HTTPS 的 Server 是否被加进白名单。

```
[H3C]display  app-proxy ssl whitelist hostname predefined
Chrome HSTS-defined hostnames:
  status      Hostname
  enabled     2mdn.net
  enabled     accounts.firefox.com
  enabled     aclu.org
  enabled     activiti.alfresco.com
  enabled     adamkostecki.de
  enabled     addvocate.com
  enabled     adsfund.org
  enabled     aie.de
```

……

```
<H3C>display  app-proxy ssl whitelist ip all
Slot 1:
    IP address            Port
    --------------------------
    9.9.9.5               443
    9.9.9.6               443
    9.9.9.7               443
    9.9.9.8               443
    9.9.9.9               443
    9.9.9.10              443
    9.9.9.11              443
     9.9.9.12              443
```

如果被添加进白名单，可以使用如下命令清除白名单。

```
[H3C]undo app-proxy ssl whitelis user-defined-hostname
<H3C>reset app-proxy ssl whitelist ip
[H3C]app-proxy ssl whitelist activate
```

(6) 查看流量是否跨板，目前 SSL 卸载不支持跨板流量。

```
<H3C>display  session table ipv4 source-ip 7.0.1.2 verbose
Slot 1:
Initiator:
  Source      IP/port: 7.0.1.2/55933
  Destination IP/port: 8.8.8.2/443
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/2
  Source security zone: Trust
Responder:
  Source      IP/port: 8.8.8.2/443
  Destination IP/port: 7.0.1.2/55933
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Reth1
  Source security zone: Trust
State: INACTIVE
Application: HTTPS
Rule ID: 0
Rule name: ips
Start time: 2019-11-18 10:59:43  TTL: 299s
Initiator->Responder:            0 packets          0 bytes
Responder->Initiator:            0 packets          0 bytes

Initiator:
  Source      IP/port: 7.0.1.2/55852
  Destination IP/port: 8.8.8.2/80
  DS-Lite tunnel peer: -
```

```
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/2
  Source security zone: Trust
Responder:
  Source      IP/port: 8.8.8.2/80
  Destination IP/port: 7.0.1.2/55852
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Reth1
  Source security zone: Trust
State: INACTIVE
Application: HTTP
Rule ID: 0
Rule name: ips
Start time: 2019-11-18 10:59:02  TTL: 257s
Initiator->Responder:            0 packets          0 bytes
Responder->Initiator:            0 packets          0 bytes

Initiator:
  Source      IP/port: 7.0.1.2/55932
  Destination IP/port: 8.8.8.2/443
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/2
  Source security zone: Trust
Responder:
  Source      IP/port: 8.8.8.2/443
  Destination IP/port: 7.0.1.2/55932
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Reth1
  Source security zone: Trust
State: INACTIVE
Application: HTTPS
Rule ID: 0
Rule name: ips
Start time: 2019-11-18 10:59:43  TTL: 299s
Initiator->Responder:            0 packets          0 bytes
Responder->Initiator:            0 packets          0 bytes

Total sessions found: 3

Slot 2:
Initiator:
```

```
  Source      IP/port: 7.0.1.2/55933
  Destination IP/port: 8.8.8.2/443
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/2
  Source security zone: Trust
Responder:
  Source      IP/port: 8.8.8.2/443
  Destination IP/port: 7.0.1.2/55933
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Reth1
  Source security zone: Trust
State: TCP_TIME_WAIT
Application: HTTPS
Rule ID: 0
Rule name: ips
Start time: 2019-11-18 10:59:43  TTL: 0s
Initiator->Responder:            6 packets        776 bytes
Responder->Initiator:            7 packets        899 bytes

Initiator:
  Source      IP/port: 7.0.1.2/55852
  Destination IP/port: 8.8.8.2/80
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/2
  Source security zone: Trust
Responder:
  Source      IP/port: 8.8.8.2/80
  Destination IP/port: 7.0.1.2/55852
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Reth1
  Source security zone: Trust
State: TCP_ESTABLISHED
Application: HTTP
Rule ID: 0
Rule name: ips
Start time: 2019-11-18 10:59:02  TTL: 1157s
Initiator->Responder:            8 packets       1256 bytes
Responder->Initiator:            9 packets       3456 bytes

Initiator:
```

```
  Source      IP/port: 7.0.1.2/55932
  Destination IP/port: 8.8.8.2/443
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/2
  Source security zone: Trust
Responder:
  Source      IP/port: 8.8.8.2/443
  Destination IP/port: 7.0.1.2/55932
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Reth1
  Source security zone: Trust
State: TCP_TIME_WAIT
Application: HTTPS
Rule ID: 0
Rule name: ips
Start time: 2019-11-18 10:59:43  TTL: 1s
Initiator->Responder:            7 packets        816 bytes
Responder->Initiator:            7 packets        899 bytes
Total sessions found: 3
```

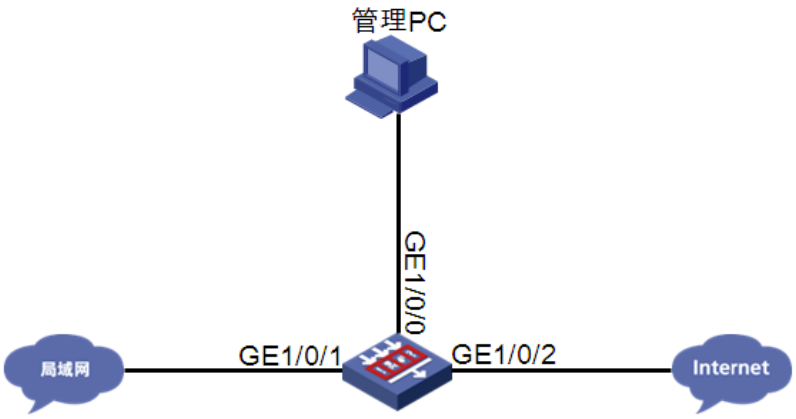
(7) 前面都检查没有问题后设备还是不能拦截，有可能此时加密攻击设备暂不支持，此时需要协助抓取对应的交互报文反馈报文给研发进行分析。

15.5.3 故障诊断命令

命令	说明
app-proxy-policy	进入代理策略视图
app-proxy ssl whitelist user-defined-hostname host-name	使用*host-name*与SSL请求报文中携带的服务器证书的“DNS Name”或“Common Name”字段进行匹配，只要含有*host-name*的域名均会匹配成功。若匹配成功，则透传该SSL连接
display app-proxy ssl whitelist ip { all | ip-address }	显示SSL代理IP地址白名单
display inspect status	显示应用层检测引擎的运行状态

15.6 应用审计没有生效，且没有产生日志

15.6.1 故障描述



组网需求：

局域网内 PC 通过防火墙访问 Internet，防火墙上开启应用审计业务。保护内外网用户数据传输信息安全。

配置描述

安全策略中开启应用审计检测。

```
#
uapp-control
 policy name default audit
  rule 1 app-category IM behavior FileTransfer bhcontent any keyword include any
 action deny audit-logging
#
```

故障描述

使用者从局域网向 Internet 执行敏感动作， 例如传文件和登录等操作时，动作执行成功，且设备无日志。

15.6.2 故障处理步骤

(1) 查看 APR 版本信息，是否为最新版本，如果版本较老，请从官网上获取最新版本进行升级。

(2) 查看设备引擎状态，是否 bypass，如果进行了手工 bypass 或 cpu、memory 自动 bypass，可以通过 **undo inspect bypss** 命令重新激活引擎。

(3) 查看应用审计与管理策略是否下发引擎，如果没有下发数据过滤规则，需要在系统视图下执行 **inspect activate** 或通过 Web 激活引擎，重新下发规则。

```
[H3C-probe]display  system  internal  inspect  dim-rule
Slot 1:
MdcID       MoudleName  Total MD5 rules
0           Anti-Virus  0

MdcID       RuleID      ModuleName          L4ProName           uiAppIdL5

1           1           AUDIT               TCP                 WECHAT_LOGIN_IOS
```

```
_TCP_M
0           1           IPS                 TCP                 HTTP

0           2147483649  FFILTER             TCP

1           2           AUDIT               TCP                 WECHAT_LOGIN_AND
ROID_TCP_M
0           2           IPS                 TCP                 HTTP

0           2147483650  FFILTER             TCP

1           3           AUDIT               TCP                 WECHAT_SENDTEXT_
WINDOWS_TCP_M
0           2147483651  FFILTER             TCP

1           4           AUDIT               TCP                 WECHAT_SENDTEXT_
IOS_TCP_M
0           4           IPS                 TCP                 HTTP
```

(4) 查看规则状态是否为使能状态，对应流量是否优先走了其他规则。

(5) 查看会话是否建立，确保会话的源目 IP 在指定的安全域内，并且在该域间启用深度检查功能，引用应用审计与管理策略。

```
[H3C-probe]display  session table ipv4 source-ip 7.0.1.2 verbose
Slot 2:
Initiator:
  Source      IP/port: 7.0.1.2/50779
  Destination IP/port: 7.0.0.2/80
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/2
  Source security zone: Trust
Responder:
  Source      IP/port: 7.0.0.2/80
  Destination IP/port: 7.0.1.2/50779
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/3
  Source security zone: Untrust
State: TCP_ESTABLISHED
Application: HTTP
Rule ID: 0
Rule name: ips
Start time: 2019-11-15 11:31:01  TTL: 1197s
Initiator->Responder:            7 packets       1073 bytes
Responder->Initiator:            7 packets       2413 bytes

Total sessions found: 1
```

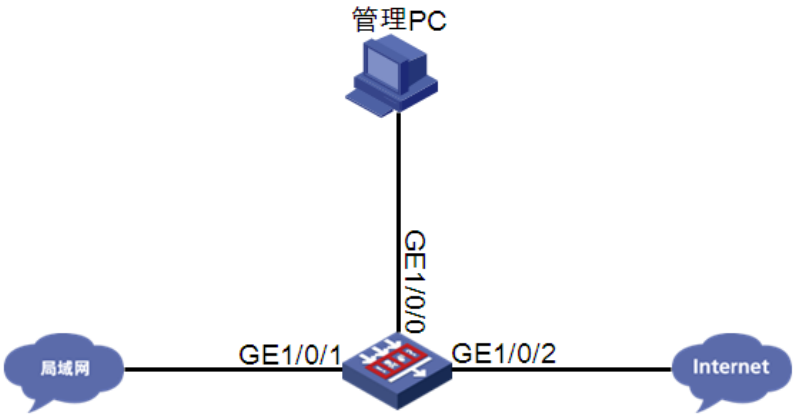
(6) 前面都检查没有问题后设备还是不能拦截，有可能此时应用的应用审计设备暂不支持，此时需要协助抓取对应的交互报文反馈报文给研发进行分析。

15.6.3 故障诊断命令

命令	说明
inspect activate	缺省情况下，DPI各业务模块自定义的规则或手动离线升级的特征库不生效
display inspect status	显示应用层检测引擎的运行状态

15.7 指定的网页设备没有阻断，且没有产生日志

15.7.1 故障描述



组网需求：

局域网内 PC 通过防火墙访问 Internet，防火墙上开启 URL 过滤业务。保护用户访问网页安全。

配置描述

安全策略中开启 URL 过滤检测。

```
#
url-filter policy url
 default-action permit logging
 category Pre-Botnet action reset logging
 category Pre-ChildAbuse action reset logging
 category Pre-CriminalActivity action reset logging
 category Pre-Discrimination action reset logging
 category Pre-Divining action reset logging
 category Pre-Drugs action reset logging
 category Pre-Gamble action reset logging
 category Pre-Hacking action reset logging
 category Pre-IllegalSoftware action reset logging
 category Pre-Lottery action reset logging
 category Pre-MaliciousURL action reset logging
 category Pre-Phishing action reset logging
 category Pre-Pornography action reset logging
```

```
 category Pre-Religion action reset logging
 category Pre-SchoolCheating action reset logging
 category Pre-Spam action reset logging
 category Pre-Suicide action reset logging
 category Pre-Violence action reset logging
#
app-profile 0_IPv4
 url-filter apply policy url
#
security-policy ip
 rule 0 name url
  action pass
  counting enable
  profile 0_IPv4
#
```

故障描述

使用者从局域网向 Internet 访问有害网页， 例如色情网站等，用户成功访问，且设备无日志。

15.7.2 故障处理步骤

(1) 查看 URL 特征库版本信息，是否为最新版本，如果版本较老，请从官网上获取最新版本进行升级。

(2) 查看设备引擎状态，是否 bypass，如果进行了手工 bypass 或 cpu、memory 自动 bypass，可以通过 **undo inspect bypss** 命令重新激活引擎。

(3) 查看访问页面是否为 HTTPS 加密网页，如果是加密网页可以开启 SSL 卸载功能。

(4) 查看 URL 过滤规则是否下发引擎，如果没有下发 URL 过滤规则，需要在系统视图下执行 inspect activate 或通过 Web 激活引擎，重新下发规则。

```
[H3C-probe]display  system  internal  inspect  dim-rule
Slot 1:
MdcID       MoudleName  Total MD5 rules
0           Anti-Virus  0

MdcID       RuleID      ModuleName          L4ProName           uiAppIdL5

0           356581376   UFLT                TCP                 HTTP

0           268435456   UFLT                TCP                 HTTP

0           356646912   UFLT                TCP                 HTTP

0           268435457   UFLT                TCP                 HTTP

0           431030273   UFLT                TCP                 HTTP

0           384958465   UFLT                TCP                 HTTP

0           2147483649  FFILTER             TCP
```

```
0           447873026   UFLT                TCP                 HTTP

0           268435458   UFLT                TCP                 HTTP
```

(5) 查看会话是否建立，确保会话的源目 IP 在指定的安全域内，并且在该域间启用深度检查功能，引用 URL 过滤策略。

```
[H3C-probe]display  session table ipv4 source-ip 7.0.1.2 verbose
Slot 2:
Initiator:
  Source      IP/port: 7.0.1.2/50779
  Destination IP/port: 7.0.0.2/80
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/2
  Source security zone: Trust
Responder:
  Source      IP/port: 7.0.0.2/80
  Destination IP/port: 7.0.1.2/50779
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/3
  Source security zone: Untrust
State: TCP_ESTABLISHED
Application: HTTP
Rule ID: 0
Rule name: ips
Start time: 2019-11-15 11:31:01  TTL: 1197s
Initiator->Responder:            7 packets       1073 bytes
Responder->Initiator:            7 packets       2413 bytes

Total sessions found: 1
```

(6) 如果是自定义 URL 分类，检查用户使用的 URL 是否与分类的 URL 完全匹配。

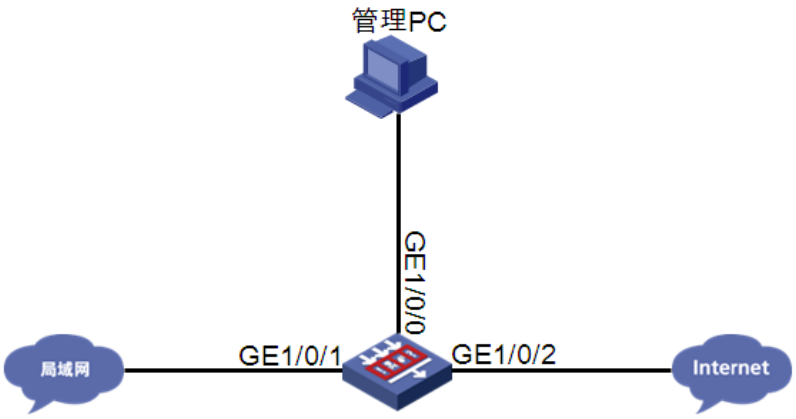
(7) 前面都检查没有问题后设备还是不能拦截，有可能此时网页 URL 特征库不支持，此时需要协助抓取对应的交互报文反馈报文给研发进行分析。

15.7.3 故障诊断命令

命令	说明
url-filter apply policy *policy-name*	缺省情况下，DPI应用profile中未引用URL过滤策略
inspect activate	缺省情况下，DPI各业务模块自定义的规则或手动离线升级的特征库不生效
display inspect status	显示应用层检测引擎的运行状态

15.8 服务器发出异常外联行为，设备没有输出告警日志

15.8.1 故障描述



组网需求：

服务器通过防火墙主动连接客户端，防火墙上开启服务器外联防护业务。保护内外网用户免遭受攻击。

配置描述

安全策略中开启服务器外联防护检测。

```
#
scd policy name default-7.0.0.2
 protected-server 7.0.0.2
 logging enable
 policy enable
 rule 1
  permit-dest-ip 7.0.0.255
  protocol udp port 137 to 138
#
```

故障描述

开启服务器外联业务，服务器通过设备的异常外联行为， 设备没有日志告警。

15.8.2 故障处理步骤

(1) 检查设备是否开启服务器外联的快速日志。快速日志与系统日志不能同时生成，如果需要系统日志，请关闭服务器外联防护的快速日志。

(2) 查看设备防护策略和日志是否启用，protected-server、permit-dest-ip 与服务器异常外联行为的源目 IP 一致。

```
<H3C>display scd  policy
Id      Name            Protected server       Rules        Logging      Policy status
1       12                    1.2.2.3           1          Enabled         Enabled
2       default-7.0.0.2       7.0.0.2           1          Enabled         Enabled
```

(3) 排查设备对应流量是否优先走了其他规则。

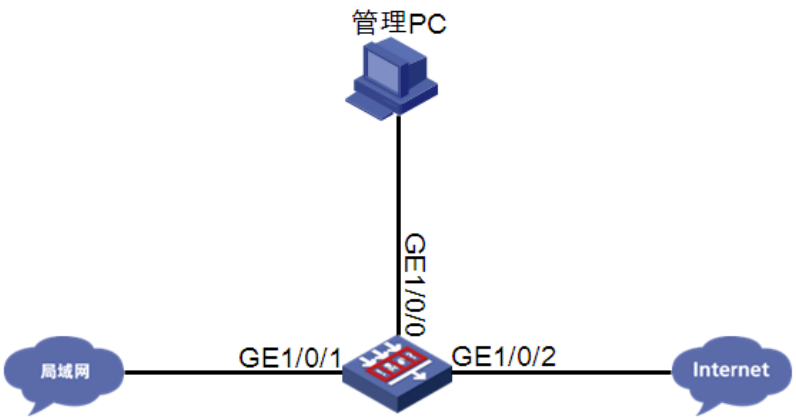
(4) 前面都检查没有问题后设备还是不能识别，有可能产生的流量设备暂不支持，此时需要协助抓取对应的攻击交互报文反馈报文给研发进行分析。

15.8.3 故障诊断命令

命令	说明
scd policy name ***policy-name***	创建服务器外联防护策略
display scd policy [**name** *policy-name*]	显示服务器外联防护策略的配置信息

15.9 具有风险的IP与本地用户连接成功，无告警日志

15.9.1 故障描述



组网需求：

局域网内 PC 通过防火墙访问 Internet，防火墙上开启威胁情报业务。保护内外网用户免遭受攻击。

配置描述

安全策略中开启威胁情报检测。

```
#
ip-reputation
 global enable
 top-hit-statistics enable
 attack-category 1 action deny logging enable
 attack-category 2 action deny logging disable
 attack-category 3 action deny logging enable
 attack-category 4 action deny logging enable
 attack-category 5 action deny logging enable
 attack-category 6 action deny logging enable
 attack-category 7 action deny logging enable
 attack-category 8 action deny logging enable
```

```
 attack-category 9 action deny logging enable
 attack-category 10 action deny logging enable
 attack-category 11 action deny logging enable
 attack-category 12 action deny logging enable
 attack-category 13 action deny logging enable
 attack-category 14 action deny logging enable
 attack-category 15 action deny logging enable
 attack-category 16 action deny logging enable
 attack-category 17 action deny logging enable
 attack-category 18 action deny logging enable
 attack-category 19 action deny logging enable
 attack-category 20 action deny logging enable
 attack-category 21 action deny logging enable
 attack-category 22 action deny logging enable
#
```

故障描述

开启威胁情报业务，具有风险的 IP 与本地用户连接成功，无告警日志。

15.9.2 故障处理步骤

(1) 检查设备是否安装了 License。

(2) 检查 ip 地址是否被设置成 IP 信誉例外地址。

```
<H3C>display ip-reputation exception
  IP address
  2.2.2.2
```

(3) 检查配置动作是否为丢弃告警。

```
[H3C-ip-reputation]display  ip-reputation attack-category
  Attack id    Attack name          Action    Logging
  ---------------------------------------------------
  1            C&C                  deny      enable
  2            Network_Worm         deny      disable
  3            Risk_Software        deny      enable
  4            Malware              deny      enable
  5            Trojan               deny      enable
  6            Infectious_Virus     deny      enable
```

(4) 前面都检查没有问题后设备还是不能识别，有可能 ip 信誉库中还不含有该 ip，此时需要协助抓取对应的攻击交互报文反馈报文给研发进行分析。

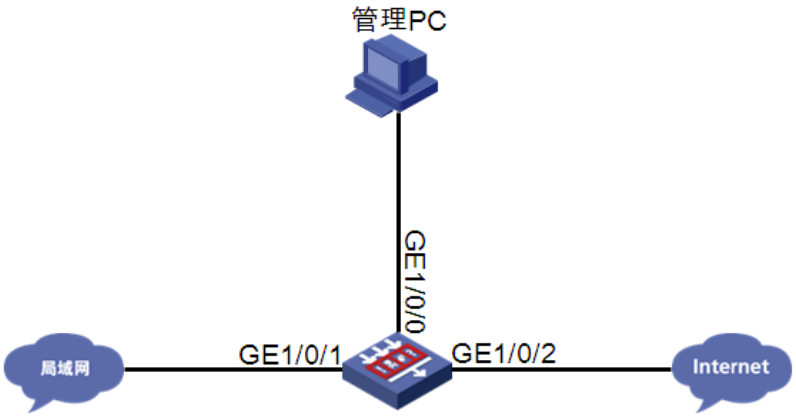
15.9.3 故障诊断命令

命令	说明
display ip-reputation attack-category	仅在IP信誉功能处于开启状态时，才能查看到IP信誉库中的攻击分类信息。 如果未配置对指定攻击分类执行的动作，则显示特征库中的缺省配置。
display ip-reputation	仅在IP信誉功能处于开启状态时，才能查看到IP信誉例外IP地址。

命令	说明
exception	

15.10 数据中心无日志or日志长时间不更新

15.10.1 故障描述



组网需求：

局域网内 PC 通过防火墙访问 Internet，防火墙上开启 DPI 业务。保护内外网用户信息安全。

配置描述

安全策略中开启 DPI 检测。

```
#
app-profile 0_IPv4
 ips apply policy default mode protect
 data-filter apply policy default
 url-filter apply policy default
 file-filter apply policy default
 anti-virus apply policy default mode protect
#
security-policy ip
 rule 0 name 1
  action pass
  profile 0_IPv4
  source-zone Trust
  source-zone Untrust
  destination-zone Trust
  destination-zone Untrust
#
```

故障描述

开启 DPI 业务，数据中心无日志输出，或者数据中心日志长时间不更新

15.10.2 故障处理步骤

(1) 查看设备当前的 DPI 状态，设备运行状态为 normal。

```
[H3C]display inspect status
Chassis 0 Slot 1:
Running status: normal
```

(2) 查看 rule hit 情况：

```
[H3C-probe]display  system  internal  inspect  hit-statistics
Slot 1:
Rule ID     Module      Rule hits  AC hits    PCRE try   PCRE hits
0           FFILTER     0          78225      0          0
0           DFILTER     0          545415     0          0
1           FFILTER     0          78225      0          0
1           DFILTER     0          545415     0          0
2           FFILTER     52341      78225      52341      52341
2           DFILTER     0          545415     0          0
3           FFILTER     0          78225      0          0
3           DFILTER     0          545415     0          0
4           FFILTER     25884      78225      25884      25884
4           DFILTER     0          545415     0          0
2147483652  FFILTER     359139     359139     0          0
5           FFILTER     0          78225      0          0
5           DFILTER     0          545415     0          0
2147483653  FFILTER     9          9          0          0
6           FFILTER     0          78225      0          0
6           DFILTER     0          545415     0          0
2147483654  FFILTER     207554     207554     0          0
7           FFILTER     0          78225      0          0
7           DFILTER     0          545415     0          0
2147483656  FFILTER     159715     159715     0          0
2147483657  FFILTER     985048     985048     0          0
```

(3) 等待一段时间，查看数据中心是否有日志输出，数据中心日志不能实时更新，需要等待一段时间。

(4) 查看设备时间和日期与本地 PC 是否一致。

```
<H3C>display  clock
18:37:21 UTC Tue 11/26/2019
```

可以使用命令行或者在 Web 上进行设备时间和日期的修改。

```
<H3C>clock  datetime 19:52:33 2019/11/26
```

(5) 流量日志等日志输出需要开启会话统计。

```
[H3C]session statistics enable
```

(6) URL 过滤为减少日志输出，将 css、gif、ico、jpg、js、png、swf、xml 默认不输出数据中心日志。使用下面命令可以使之输出。

undo url-filter log except pre-defined{ css | gif | ico | jpg | js | png | swf | xml }

(7) 设备日志存储空间达到上限，并且对上限的处理动作为提示。

配置数据分析中心存储空间的命令行为：

dac storage service *service-type service-name*__limit__ { **hold-time** *time-value* | **usage** *usage-value* |**action** { **delete** | **log-only** } }

缺省情况下，数据分析中心各业务存储空间上限为 20%、存储空间时间上限为 365 天、处理动作为删除。

可以对日志存储空间设置恢复为缺省情况。

(8) 前面都检查没有问题后数据中心还是不能输出日志，有可能 ntopd 有异常，此时需要协助抓取对应的交互报文反馈报文和设备诊断信息给研发进行分析。

15.10.3 故障诊断命令

命令	说明
url-filter log except pre-defined { **css** | **gif** | **ico** | **jpg** | **js** | **png** | **swf** | **xml** }	配置URL过滤对预定义类型网页资源的访问不进行日志记录
session statistics enable	开启软件快速转发的会话统计功能
display inspect status	显示应用层检测引擎的工作状态。
dac storage service service-type service-name limit { **hold-time time-value** | **usage usage-value** | **action** { **delete** | **log-only** } }	配置数据分析中心存储空间