H3C SecPath 安全产品 用户 FAQ(V7)

资料版本：6W100-20230628

前 言

本手册介绍了安全产品的用户 FAQ。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

特别申明

本文档不严格与具体软、硬件版本对应，文档中出现的设备名称、接口名称、版本号等设备相关信息仅作为示例。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。

本文中的内容为通用性技术信息，某些信息可能不适用于您所购买的产品。

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... }*	表示从多个选项中至少选取一个。
[x | y | ...]*	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。

	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

1 系统维护类 FAQ

1.1 如何清除Telnet进程？

通过在用户视图下执行命令 **free user-interface vty** *number* 可以清除 Telnet 进程。

1.2 能否支持Telnet用户名包含@字符？

不支持本地用户名包含@字符。

1.3 管理以太网接口没有配置IP地址能够直接UP吗？

管理以太网接口只要二层连接就能够 UP，且软件已经作了流量限制，不会因为报文冲击导致系统运行异常。

1 设备转发 FAQ

1.1 M9000系列设备的业务报文处理流程是什么？

处理流程为：业务报文首先到接口板，然后到达网板，然后从网板到达业务板，业务板进行安全处理后，再送到网板，最后从接口板发送出去。

1.2 系统缺省安全域有哪些？

缺省情况下，系统包含 5 个安全域：Trust、Untrust、DMZ、Local 和 Management 域。

1.3 安全域特性方面，和V5版本相比有哪些差异？

V7 版本中：

- 创建安全域时，无域 ID 的概念。
- 安全域没有优先级、共享等属性。
- 同一安全域之间，默认策略是 deny 的。

1.4 管理口默认在安全域中吗?

管理口默认应该在 Management 域。

1.5 安全域之间，默认域间策略是怎么样的？

默认是 deny 的。

1.6 域间策略有哪种方式？

包括 3 种方式：安全策略、对象策略和包过滤策略，建议根据实际组网情况选择使用。

1.7 有时明明匹配时间段和地址组了，为何显示为未匹配？

可能的原因是：存在 VPN 实例。如果入接口存在 VPN 实例的，则必须指定 VRF，否则无法匹配。

1.8 如果包过滤和对象策略两者在域间策略中同时存在时，优先匹配哪一个？

优先匹配对象策略，而不是包过滤。

1.9 对象组支持引用对象组，那么当对象组多级引用对象组时，深度上，最深支持几层引用？

支持 5 层深度的引用。

1.10 域间策略和NAT操作的顺序是怎样的？

NAT server 是在域间策略前作转换，域间策略匹配 NAT server 转换后的 IP。

NAT outbound 是在域间策略后进行转换，域间策略匹配 NAT outbund 转换前的 IP。

1.11 链路聚合时流量如何分担？

缺省情况下，设备按照源 MAC 地址、目的 MAC 地址、源 IP 地址和目的 IP 地址进行聚合负载分担。通过全局配置 **link-aggregation global load-sharing mode** 命令，可以改变聚合负载分担模式。

采用不同的聚合负载分担类型可以实现灵活地对聚合组内流量进行负载分担。聚合负载分担的类型可以归为以下几类：

- 逐流负载分担：按照报文的源/目的 MAC 地址、源/目的服务端口、入端口、源/目的 IP 地址、IP 协议类型或 MPLS 标签中的一种或某几种的组合区分流，使属于同一数据流的报文从同一条成员链路上通过。
- 按照报文类型（如二层、IPv4、IPv6、MPLS 等）自动选择所采用的聚合负载分担类型。
- 逐包负载分担：不区分数据流，而是以报文为单位，将流量分担到不同的成员链路上进行传输。

1.12 相同五元组的流来回走两次设备，如果转发失败，该如何处理？

缺省情况下，系统不关心报文入接口。五元组相同、入接口不同的流量建立的是相同的快转表项，从而导致转发失败。

```
[Device] display ip fast-forwarding cache
Total number of fast-forwarding entries: 1
SIP SPort DIP Dport Pro Input_If Output_If Flg
198.1.1.2 1024 197.1.20.1 2048 Tun2 RAGG3 1
```

当配置命令 undo ip fast-forwarding load-sharing 后，系统关心报文入接口。五元组相同，入接口不同的流量会建立新的快转表项。

```
[Device] display ip fast-forwardingcache
Total number of fast-forwarding entries: 2
SIP Sport DIP Dport Pro Input_If Output_If Flg
198.1.1.2 1024 197.1.20.1 2048 1 RAGG4 RAGG2 1
198.1.1.2 1024 197.1.20.1 2048 1 Tun2 RAGG3 1
IPSec
```

1.13 打应用层流量时，配置的应用的老化时间为何不生效？

使用 **display session aging-time application** 命令显示应用层协议老化时间，是该应用会话建立稳态时的老化时间，否则使用对应的 4 层协议的老化时间。所有协议在未建立稳态的时候都使用 4 层协议的老化时间。

1.14 ASPF ICMP差错报文检测能够识别哪些ICMP差错报文？

当前识别的 icmp-err 的组合有下面这些：()中为 ICMP 报文的类型，[]中为 ICMP 的代码范围。

type	code
ICMP_UNREACH(3)	[0, 12]
ICMP_SOURCEQUENCH(4)	[0, 0]
ICMP_REDIRECT(5)	[0, 3]
ICMP_TIMXCEED(11)	[0, 1]
ICMP_PARAMPROB(12)	[0, 1]

1.15 为什么会话的收发包统计不正确？

目前为了提高设备的性能，缺省情况下，会话不统计报文数。

如果需要统计报文数，请在系统视图下配置命令：**session statistic enable**。

1.16 IPv4、IPv6报文是不是都可以建立会话？

是的，都可以建立会话。

1.17 IPv4地址组对象包含哪些地址类型？

主要包括主机地址类型、域名地址类型、网段地址类型、范围地址类型。一个地址组对象可以包含多种地址类型。地址组对象可以嵌套，即一个地址组对象可以包含另外一个地址组对象。

1.18 对象策略的规则匹配顺序是什么？

当一个对象策略中包含多条规则时，报文会按照一定的顺序与这些规则进行匹配，一旦匹配上某条规则便结束匹配过程。对象策略规则的匹配顺序与规则的创建顺序有关，先创建的规则优先进行匹配。对象策略规则的显示顺序与匹配顺序一致，即按照域间实例视图下通过 **display this** 命令显示的顺序，从上到下依次匹配。同时，对象策略支持通过命令移动规则位置来调整规则的匹配顺序。

1.19 对象策略的类型是什么？

对象策略有 2 种类型：IPv4 地址对象策略、IPv6 地址对象策略。

1.20 对象策略中，VRF参数所指vpn-instance指的是入接口还是出接口的vpn-instance？

入接口的 vpn-instance。

1.21 对象策略目前的筛选包括哪些特征？

包括特征有：源地址组、目的地址组、服务组、vrf、时间段。

其中，服务组指的是区分四层的承载协议，根据 IP 头中的协议号来识别。vrf 指的是 vpn-instance。

1.22 对象策略中的rule的匹配顺序是怎么样的？

根据先上后下的顺序，而不是 ID 号，例如，存在 rule 0 与 rule 1 都可以匹配，那么 rule 0 在上方就先匹配 rule 0，如果 rule 1 在上方就先匹配 rule 1。

1 License 管理 FAQ

1.1 哪些业务需要License?

SSL VPN，SLB 以及应用安全（包括 IPS、防病毒，应用识别等）业务的使用需要有 License 许可。

1.2 如何将License文件导入设备

(1) 首先根据需要申请相应的 License 文件，申请时需提供设备的信息文件：

设备的 License 目录下，后缀为 did 的文件即是。可以通过 FTP 或 TFTP 取出；如果是双机的话，需要两框的 did 文件。

```
<H3C>cd license/
<H3C>dir
<H3C>dir
Directory of cfa0:/license
   0 -rw-         963 Jul 02 2015 06:34:14   210231A1NPH12A000029.did
   1 drw-           - Jul 02 2015 06:34:12   history
```

(2) 申请到 License（*.ak）文件后，将该文件以 FTP 或 TFTP 的方式传到设备上，通过如下命令安装 License

```
[H3C]license activation-file install ACG.ak slot 1
```

(3) 通过如下命令查看 License 的安装情况

```
[H3C]display license feature
Slot 1:
Total: 5  Usage: 3
Feature                         Licensed        State
ACG                             Y               Trial
IPS                             Y               Trial
SLB                             N               -
SSLVPN                          N               -

[H3C]
```

(4) 如果需要删除 License，执行命令：

```
[H3C]license activation-file uninstall ACG.ak slot 1
```

(5) 如果 License 过期，不会自动删除，会显示已过期。

1.3 在合一License环境中，如果需要对已激活的License进行扩容申请，需要提交哪些授权码？

当原有已激活 License 仅包含正式授权时：

- 若需进行某些软件功能的规模扩容或时限延长，则需要提交这些软件功能的正式 License 扩容授权码进行扩容申请。
- 若需进行功能扩展（即新增软件功能授权），则需要提交新增软件功能的临时或正式 License 授权码进行扩容申请。

当原有已激活 License 包含临时 License 授权时：

- 若对某些软件功能已激活的正式 License 进行规模扩容或时限延长，则需要提交这些软件功能的正式 License 扩容授权码以及其它软件功能原有临时 License 授权码进行扩容申请。
- 若对某些软件功能已激活的临时 License 进行规模扩容或时限延长，则需要提交这些软件功能的临时或正式 License 扩容授权码以及其它软件功能原有临时 License 授权码进行扩容申请。
- 若需进行功能扩展（即新增软件功能授权），则需要提交新增软件功能的临时或正式 License 授权码以及其它软件功能原有临时 License 授权码进行扩容申请。

1.4 在合一License环境中，同一特性是否可以通过临时授权码对已激活的正式License进行规模扩容或时限延长？

不可以，临时授权码只可对已激活的临时 License 进行规模扩容或时限延长，且不能与原有临时 License 叠加，仅可替换原有临时 License。

1.5 在合一License环境中，同一特性是否可以通过正式授权码对已激活的临时License进行规模扩容或时限延长？

正式 License 可以替换已激活的临时 License，但不能与临时 License 叠加。

1.6 在合一License环境中，正式License和临时License是否可以同时使用？

对于同一特性，正式 License 和临时 License 不能同时使用，若同时注册安装则仅正式 License 生效。

对于不同特性，正式 License 和临时 License 可以同时使用。

1.7 在合一License环境中，相同特性多个License授权是否可以叠加？

仅多个正式 License 授权可以叠加，临时 License 授权不支持叠加。

1.8 在合一License环境中，对License进行新增或扩容后，原有临时License失效了，如何操作？

在合一 License 环境中，对 License 进行新增或扩容时设备中原有临时 License 的授权信息不会自动合入到新生成的合一 License 中，因此，会导致原有临时 License 失效。为避免上述情况出现，在进行新增或扩容 License 时，请同时将临时 License 的授权码一起提交激活申请。

1.9 授权码和激活文件是什么关系？

激活文件是绑定了授权码和硬件设备信息的授权凭证，将激活文件安装到设备后，设备上的软件功能才能获得授权。

- 通过 H3C 官方渠道购买授权书，授权书中包含授权码。
- 激活文件需要您从 H3C License 管理平台（网址为 http://www.h3c.com/cn/License）申请。H3C License 管理平台会根据您申请授权时输入的授权码和硬件设备信息，自动生成激活文件。

1.10 在双机备份场景中只在其中一个成员设备上安装License激活文件可以吗？

不可以，推荐为每台成员设备分别购买安装 License，否则当安装授权的成员设备故障，会导致软件功能无法正常运行。

仅在 IRF 场景中，SSL VPN 用户数授权支持叠加，若成员设备发生故障，此成员设备上的 SSL VPN 用户数授权将在 IRF 设备上继续生效，有效期为 60 天。

1.11 对于数量型或时间型License，在同一台设备上注册多个授权可以叠加吗？

仅多个正式授权可以叠加；多个临时授权不可以叠加。

1.12 安装授权后，可以随意修改设备的系统时间吗？

对于有效期为永久和有效期为具体天数的授权，修改系统时间，不影响授权的有效期计数。对于有效期为绝对时间的授权（即有效期截止到具体日期的授权），安装授权后，为保证相关业务的正常使用，请勿修改设备的系统时间。

1.13 DID/设备信息文件会变化吗？如果变化了会产生哪些影响？

DID/设备信息文件不会自动变化，如果执行 **`license compress`** 命令清理 License 存储区，可能会导致 DID/设备信息文件变化。

如果 DID/设备信息文件变化了：

- 对于设备上已安装的授权，不会产生影响。
- 对于使用旧 DID/设备信息文件申请的激活文件，将不能安装。请联系 H3C 技术支持人员处理。
- 如果需要申请新的激活文件，则必须使用新的 DID/设备信息文件。

1.14 设备软件版本升级后需要重新购买授权并安装授权吗？

设备软件版本升级后，设备上现有的未过期的授权继续生效，无需重新购买、安装。

1.15 设备重启或更新版本后，已激活的License激活文件会丢失吗？

不会。

1.16 如何找回授权码？

如果用户在未获得激活文件前将授权码丢失，请联系 H3C 技术支持人员，通过 License 购买合同找回授权码。

如果用户在获得激活文件后将授权码丢失，请提供激活文件或者设备信息，联系 H3C 技术支持人员找回授权码。

1.17 License激活文件被误删除后，相应功能无法使用也无法卸载对应授权该怎么办？

请参照以下步骤来处理：

(1) 执行 **copy** 命令将备份的激活文件拷贝到设备存储介质根目录下的 license 文件夹中（比如 flash:/license）

(2) 重启设备来进行功能恢复或卸载对应授权。

1.18 如何找回激活文件？

用户因误操作或其它原因，将正在使用的激活文件删除或丢失，会导致对应的授权不可用。您可以通过以下方式找回激活文件：

- 直接使用备份的激活文件。
- 从“申请联系人 E-mail”中找回激活文件。
- 提供授权码或者设备信息，联系 H3C 技术支持人员找回激活文件。

1.19 当设备发生故障或其它因素需要设备授权变更时，如何操作？

请联系当地的 H3C 技术支持人员解决。

1 RBM 双机热备 FAQ

1.1 RBM双机热备和IRF双机热备能同时使用吗？

不能同时使用。

1.2 配置远端备份管理功能RBM时，对组网设备和配置有什么要求吗？

对组网设备和配置有要求。主备设备的如下信息必须一致：

- 主/备设备的型号必须一致；
- 主/备设备的软件版本必须一致；
- 主/备设备的接口编号必须一致；
- 主/备设备业务板的位置、数量和类型一致；
- 主/备设备接口板的位置、数量和类型一致；
- 主/备设备之间建立控制通道的接口必须一致；
- 主/备设备之间建立数据通道的接口必须一致；
- 主/备设备对应槽位上的接口必须加入到相同的安全域。

1.3 RBM的控制通道和数据通道可以不一致吗？

可以不一致。当配置的数据通道和控制通道一致时，设备会使用 RBM 控制通道的物理链路建立数据通道传输热备报文和透传报文；如果配置的数据通道和控制通道不一致，将只能使用配置的接口建立数据通道，即使此数据通道物理链路故障了，也不会使用控制通道的物理链路建立数据通道传输相关报文。

1.4 在VRRP备份组中的防火墙上可以配置不同的VRRP版本吗？

可以配置不同的 VRRP 版本，但备份组不能正常工作，请保证 VRRP 版本一致。

1.5 VRRP的负载均衡模式可以在VRRP+RBM的组网下使用吗？

不能。RBM 仅支持与 VRRP 的标准模式配合使用，不支持与 VRRP 的负载均衡模式配合使用。

1.6 流量较大时，链路状态发生了变化该怎么避免Master路由器的重新选举？

可以通过将 VRRP 通告报文的发送间隔设置大些，避免 Master 路由器的重新选举。

1.7 VRRP备份组与RBM双机热备关联/不关联有影响吗？

有影响。当不进行 VRRP 双机热备关联时，链路状态根据备份组优先级决定；当进行 VRRP 双机热备关联时，链路状态仅和关联的 VRRP 状态 active/standby 有关。

1.8 VRRP备份组抢占延迟时间设置有什么需要注意的吗？

设置延迟时间不可太小，避免成员设备频繁的进行主备切换。

1.9 如何避免RBM双机热备下配置不一致的问题？

开启自动同步和配置信息一致性检查，配置或修改配置请在主设备上进行。

1 NAT FAQ

1.1 配置静态NAT444要注意什么？

静态 NAT444 公网地址不支持 ARP 响应，如果 NAT444 地址组和出接口地址在同一网段，需要在对端设备加一条路由，目的地址为 NAT 转换之后的地址，下一跳为出接口地址。

1.2 当NAT Server 的global地址配置为loopback口地址时，有哪些配置限制？

NAT Server 的 global 地址配置为 loopback 口地址时，需要在设备的上一跳加一条正向路由，这条路由的目的地址为 loopback 口地址，下一跳为设备入接口地址。

1.3 NAT接口分配原则是什么？

区分协议和区分原始端口号。

对于 TCP/UDP，如果原始端口号在 1～1023，转换后也是在 1～1023，如果原始接口大于 1024，就是从 1024 开始分配。

1.4 测试NAT ALG FTP时，FTP主动方式什么情况下会匹配关联表对报文载荷进行地址转换?

出口接服务器，服务器在外网，在出口做 nat outbound 时，会匹配关联表对报文载荷进行地址转换，因为主动方式数据通道第一条报文从服务器端发起。

1.5 测试NAT ALG FTP时，FTP被动方式什么情况下会匹配关联表对报文载荷进行地址转换?

服务器在内网，在入口做 NAT Server 时，会匹配关联表对报文载荷进行地址转换，因为被动方式数据通道第一条报文从客户端发起。

1.6 NAT ALG是否可处理分片报文？

不可以。

NAT ALG 需要根据协议类型解析报文载荷，将载荷中的地址/端口信息解析出来并进行相应的处理。如果需要进行 ALG 处理的协议报文是后续分片，ALG 是无法对载荷进行解析的，因此对后续分片报文不做 ALG 处理。

同样，即使是首分片报文，如果 NAT ALG 需要解析的载荷内容正好由于分片被截断了，那么 ALG 处理仍然会失败。

1.7 nat outbound配置对本机报文是否生效？

本机报文不做 nat outbound 业务，因为本机都是直连口，本身就会发送 ARP 报文，本机接口地址对外已经公开了，没有保护的必要性。

1.8 如何查看动态NAT444是否根据源IP地址上送到一块安全引擎上？

如下显示信息所示，查看统计信息，总共 1999 个用户，目前总统计刚好为 1999。

```
<Device> display nat port-block dynamic | in "Total mappings found:"
Total mappings found: 0
Total mappings found: 0
Total mappings found: 0
Total mappings found: 0
Total mappings found: 0
Total mappings found: 0
Total mappings found: 0
Total mappings found: 0
Total mappings found: 0
Total mappings found: 0
Total mappings found: 0
Total mappings found: 0
Total mappings found: 0
Total mappings found: 0
Total mappings found: 0
Total mappings found: 1000
Total mappings found: 0
Total mappings found: 999
Total mappings found: 0
Total mappings found: 0
Total mappings found: 0
Total mappings found: 0
Total mappings found: 0
Total mappings found: 0
```

1 用户接入与认证 FAQ

1.1 Portal有哪些过滤规则，按照怎样的顺序对用户报文进行匹配？

设备会根据配置以及 Portal 用户的认证状态，生成不同类型的 Portal 过滤规则。设备收到用户报文后，将依次按照如下顺序对报文进行匹配，一旦匹配上某条规则便结束匹配过程：

(1) 匹配 Free rule。
- 如果匹配上了，允许报文通过。
- 如果没匹配上，则继续下一步。

(2) 匹配 User rule。
- 如果匹配上，允许用户访问网络。
- 如果没匹配上，则继续下一步。

(3) 匹配 Portal 防攻击 rule 。
- 如果匹配上，丢弃用户的攻击报文，静默一段时间不允许用户认证。
- 如果没匹配上，则继续下一步。

(4) 匹配 Redirection rule。
- 如果匹配上，将报文上送 CPU 处理。
- 如果没匹配上，则继续下一步。

(5) 匹配 Portal 无感知认证 rule。
- 如果匹配上，将报文上送 CPU 处理。
- 如果没匹配上，则继续下一步。

(6) 匹配 Deny rule。
- 如果匹配上，则丢弃报文。
- 如果没匹配上，报文直接放行。

1.2 Portal中的Web降噪机制是如何实现的？

Portal 用户通过 HTTP/HTTPS 协议访问外部网络，设备响应其 HTTP/HTTPS 请求时，将 Portal Web 服务器的 URL 封装在 JavaScript 脚本中传递给用户，该脚本仅能被浏览器程序识别，因此，仅浏览器程序会向 Portal Web 服务器发起连接请求，从而避免了 QQ/迅雷等其它软件发送大量 HTTP/HTTPS 报文对 Portal Web 服务器造成压力。

1 攻击检测与防范 FAQ

1.1 扫描攻击防范，动作为“将发起攻击的源IP加入黑名单”，是否需要在安全域或者整机开启黑名单功能？

需要，

所有的黑名单功能都要在安全域或者全局开启黑名单功能后才能生效。如果开启的话，发起攻击的源 IP 地址在黑名单模块被丢包，如果不开启，报文会在扫描攻击模块被丢包，只是不会记录黑名单。

1.2 攻击防范策略中的“客户端验证功能”如何才能生效？

只有在安全域上开启了客户端验证功能才能生效。

1.3 泛洪攻击的门限值如何设置比较合理？

泛洪攻击防范的门限取值需要根据实际网络应用场景进行调整，对于被保护对象的报文流量较大的应用场景，建议调大门限值，以免门限值太小对正常的业务流量造成影响；对于网络状况较差，且对攻击流量比较敏感的场景，可以适当调小门限值。

1.4 攻击防范例外列表中引用的ACL不存在或者为空，例外列表还会生效吗？

如果攻击防范例外列表中引用的 ACL 不存在，或引用的 ACL 中未定义任何规则，例外列表不会生效。

1.5 例外列表引用的ACL规则中，哪些参数用于匹配报文？

例外列表引用的 ACL 规则中仅源地址、目的地址、源端口、目的端口、协议号、VRF 和非首片分片标记参数用于匹配报文。

1.6 攻击防范阈值自学习功能，对哪些攻击仅对缺省检测端口生效？

对于 DNS flood、SIP flood、HTTP flood 类型，防范阈值自学习功能仅对缺省检测端口生效。

1.7 泛洪攻击阈值学习功能，会改变泛洪受保护IP地址的检测阈值吗？

不会。

1.8 各攻击防范检测特性的优先级是如何定义的？

优先级从高到低的顺序为：

黑名单、白名单、单包、泛洪受保护 IP、泛洪、扫描。

1.9 IRF/RBM双机组网下的攻击防范配置需要注意些什么？

- 双机组网下，主设备开启 ATK 阈值学习自应用，学习的阈值数据不会被同步给备设备；且备设备没有实际流量，会导致备设备阈值学习结果为很小的数值且自动应用；VRRP 主设备故障后，流量切换到备设备后大量流量被 ATK 策略错误的丢弃。
- 对于动态生成的受保护 IP，也不会同步到备设备，主设备上面需要经过客户端验证等方式才可以访问的主机，在主备切换时，在备设备没有检测出并生成受保护 IP 列表前，主机会受到大量的攻击。

1.10 命中攻击防范的攻击报文都是在攻击模块被丢弃的吗？

不是的。以下情况下的攻击报文不是在攻击防范模块丢弃：

- 13 种单包攻击，开启攻防后，如果开启畸形报文防护，会在畸形报文防护模块进行丢包，否则在平台转发模块进行丢包，但是攻防里面可以看到攻击日志；
- 扫描攻击，如果开启黑名单功能，丢包是在黑名单模块进行，同样攻防模块可以看到攻击日志；
- 泛洪开启客户端验证功能后，丢包是在客户端验证模块进行，同样攻防模块可以看到攻击日志。

1.11 Web页面上单包攻击日志、扫描攻击日志、泛洪攻击日志为何不显示slot信息？

Web 页面上单包攻击日志、扫描攻击日志、泛洪攻击日志不支持显示 Slot 信息。攻击防范不支持双机热备，如果 Slot1、Slot2 同时受到相同的攻击，在 Web 上会显示两条一样的日志。

1 IPS FAQ

1.1 长时间打流，威胁日志不更新？

两个原因：

- 确保流量能够打通，确实到达设备上了。
- 观察设备是否报内存门限告警，设备一旦报内存门限，日志报表上面的数据就不会再更新，除非设备重启。

1.2 IPS入侵防御系统和DPI其它业务的异同？

1.2.1 不同点

(1) IPS 功能需要安装 License 才能使用。License 过期后，IPS 功能可以用，但无法升级到 License 过期后官网发布的新版本特征库。关于 License 的详细介绍请参见“基础配置指导”中的“License 管理”。

(2) 设备支持预定义 IPS 特征，其由系统中的 IPS 特征库自动生成。预定义 IPS 特征的内容不能被创建、修改和删除，但是预定义 IPS 特征的动作属性和生效状态属性可以被修改。

(3) IPS 动作是指设备对匹配上 IPS 特征的报文做出的处理。IPS 处理动作包括如下几种类型：

a. 黑名单：阻断符合特征的报文。如果设备上同时开启了黑名单过滤功能，则将该报文的源 IP 地址加入 IP 黑名单，再次收到来自此 IP 地址的报文时直接丢弃；如果设备上没有开启黑名单过滤功能，则仅阻断报文，而不会把报文的源 IP 地址加入 IP 黑名单。有关黑名单功能的详细介绍请参见“安全配置指导”中的“攻击检测与防范”。

b. 丢弃：丢弃符合特征的报文。

c. 允许：允许符合特征的报文通过。

d. 重置：通过发送 TCP 的 reset 报文或 UDP 的 ICMP 端口不可达报文断开 TCP 或 UDP 连接。

e. 重定向：把符合特征的报文重定向到指定的 Web 页面上。

f. 捕获：捕获符合特征的报文。

g. 日志：对符合特征的报文生成日志信息。

h. 邮件：对符合特征的报文生成邮件信息。

1.2.2 相同点

都与应用层检测引擎有关，需要由应用层检测引擎进行检测，并在域间策略中引用业务的策略，各业务以应用层检测引擎的会话信息来进行识别。此外，攻击的识别也与 APR 的设置相关。

1.3 IPS处理与黑名单的优先级

黑名单优先级高于 IPS 处理。

1.4 IPS动作之间的关系

重置、重定向、黑名单、丢弃、允许 5 个动作是与的关系，与捕获、日志、邮件是或的关系。

1.5 IPS动作优先级

动作优先级从高到低的顺序为：重置>重定向>(黑名单/丢弃)>允许，其中黑名单与丢弃的优先级相同。

1.6 报文同时与多个IPS特征匹配成功如何执行

如果报文同时与多个 IPS 特征匹配成功，则根据这些动作中优先级最高的动作进行处理。

1.7 在特征库没有发生变化时，以前可以识别的攻击突然识别不了了

一般情况下是由于 port-mapping 对于本可以识别的攻击报文的端口进行了设置，删除该 port-mapping 设置，攻击就可以正常识别了。

1.8 通过**display license**查看到License状态在有效期，为什么不能升级IPS特征库？

为了避免修改系统时间绕过 License 检查，是否能升级特征库不以 License 状态为准。而是通过对比 License 授权时间和特征库发布时间，如果特征库发布时间不在 License 授权时长内则不能升级特征库。

1.9 攻击日志中真实源IP地址是怎么获取和展示的？

通过报文中 CDN-src-ip、X-Forwarded-For 字段 IP 进行提取。

1.10 报文命中威胁攻击日志，动作为抓包，为什么无法下载报文？

目前抓包功能需要在设备挂载硬盘的情况下才能生效，同时需要在命令行下开启 ips capture-cache X（X 为 1-10，指每次抓包的数量）。

1 防病毒 FAQ

1.1 防病毒的工作原理是什么？

防病毒通过深度包检测（DPI）技术对报文的载荷做协议分析、特征查找、内容提取来进行策略匹配并执行告警、阻断、重定向动作。防病毒需要创建和引用 app-profile，同时可配置自定义的防病毒策略，也有系统预定义的 default 策略；且与应用层检测引擎有关，域间策略需引用防病毒策略。

1.2 防病毒能识别的报文有哪些？

目前我司防病毒实现是，支持 FTP/HTTP/IMAP/POP3/SMTP 等协议传输的报文进行检测。HTTP 协议仅能对 body 部分进行检测，ftp 协议对传输的文件内容进行检测，3 种邮件协议能对正文和附件内容进行检测，NFS 协议仅支持 NFS v3 的协议识别。

1.3 在域间引用了防病毒策略，为什么无法命中？

初步认为有两个原因：

- 首先查看设备有无 license，若无 license 设备则无法正常命中病毒报文；
- 防病毒的命中规则没有下发到应用层检测引擎内核，在域间引用防病毒策略以后，下发配置生效，设备会将引用的防病毒策略的规则下发应用层检测引擎内核；若防病毒规则未能正常下发，应用层检测引擎内核中没有防病毒的命中规则，当设备接收到病毒报文时，没有对应的规则命中匹配，病毒报文也就无法正常匹配了。

1.4 防病毒的病毒例外和应用例外作用的先后顺序？

病毒报文经过设备首先会被检测是否匹配病毒例外，若符合病毒例外，则直接按病毒例外的动作执行；当不匹配病毒例外时，再去检测是否匹配应用例外的动作，如果匹配则执行应用例外的动作，若不匹配则按照防病毒策略的规则动作执行。

1.5 域间不引用防病毒策略，应用层检测引擎也有防病毒命中统计？

在域间不引用任何防病毒策略，回放防病毒规则匹配的病毒报文，防病毒无命中统计信息，但应用层检测引擎中有防病毒的命中统计；因为只要配置中存在 app-profile 引用防病毒策略，防病毒的规则就会在应用层检测引擎中生效，所以应用层检测引擎中有命中统计。

1.6 配置协议检测方向动作时，防病毒命中统计和应用层检测引擎命中统计不一致？

配置协议的检测方向为上传或下载时，打流后发现防病毒的命中统计信息和应用层检测引擎中防病毒的命中统计不一致。

因为防病毒模块设置了方向过滤，配置了检测方向，就只命中检测方向的报文，应用层检测引擎是全局统计没有设置方向过滤，对报文进行双向检测。所以二者的统计结果不一致。

1.6.1 长时间打流的情况下，流量日志和威胁日志无法正常更新，为什么？

可能原因包括如下：

- ntopd 进程异常
- 设备日志的存储空间满
- 设备内存进入内存门限

1.6.2 双主聚合组网，能对防病毒业务进行识别么？

双主聚合组网需要开启双主功能，且在设备的上下行交换机均配置相应的聚合才能正常识别。开启双主命令后，来回流量不一致的流量会通过堆叠口将流量上送到主机，保证流量能在同一台设备进行 DPI 业务处理，从而保障了识别率，但由于通过堆叠口上送流量，流量会受到堆叠口带宽的限制。

1.6.3 设备软件已经支持 MD5，升级 MD5 病毒特征库后，样本出现无法阻断的现象，可能是什么原因？

检测 MD5 病毒前需要配置 **inspect md5-verify all-files** 命令，开启设备对所有文件进行 MD5 哈希运算功能。

目前只支持可执行文件、office 文件和压缩文件的 MD5 哈希运算。

1.6.4 什么情况下需要开启云端查询功能？如何知道云端查询功能是否生效？

当设备上的特征库较小或者无法识别病毒时，需要开启云端查杀功能。云端查询功能生效的标志是使用 **display anti-virus cache** 命令，可以看到 Cloud-query state 的状态是 enable，当有流量经过时，在这个命令下也可以看到命中记录。

1 URL 过滤 FAQ

1.1 URL过滤的特征是什么？

URL 过滤只针对路径进行过滤，比如 wwwbaidu.com/news，过滤的就是输入的网址路径，不会对 body 字段进行过滤。而且 URL 过滤仅支持 HTTP 协议。如需支持 HTTPS 协议，需要配置 SSL 解密功能。

1.2 黑名单、白名单、预定义分类、自定义分类动作执行优先级是怎么排序的？

- 优先级由高到低依次为：白名单 >黑名单 〉自定义分类 〉预定义分类（未修改分类优先级）。
- 自定义分类匹配原则：按照分类优先级匹配。
- 预定义分类匹配原则：
  - 同一规则两个预定义分类中，如果两个分类都被 URL 策略引用（或者都没有被策略引用），则按照分类优先级进行匹配。
  - 如果一个被策略引用，另一个未被策略引用，则优先匹配被 URL 策略引用的分类。

1.3 URL规则使用正则表达式时的限制是什么？

- Host 字段：regex 是正则表达式，取值为 3～224 个字符的字符串，区分大小写，只能以字母、数字和下划线开头，不能以特殊符号开头，支持特殊字符配置，且必须包含连续的 3 个非通配符
- Uri 字段：regex 是正则表达式，取值为 3～224 个字符的字符串，区分大小写，支持特殊字符配置，且必须包含连续的 3 个非通配符。

1.4 正则表达式下的特殊字符应该怎么输入？

要匹配在正则表达式中有特殊含义的字符时要在前面加“\”，例如：匹配“.”是在 web 上输入“\.”，而命令行中要输入\\.。

1.5 什么是云端查询？

设备收到 HTTP 报文时，如果 HTTP 报文中请求的域名不在预定义库，用户手动配置中都没有找到相应的分类时，就会向云端服务器发送请求报文，云端服务器在云端的 URL 库中查找并返回报文的分类信息。另外，云端返回的信息会暂时存储在本地的缓存中，以便于下次快速查询进行分类。直至该条记录被新的信息覆盖（缓存信息超出设备的缓存大小时，会删除旧的记录），期间再次查询时，都不需要再次到云端查询。

对于用户 Context，所有的用户 Context 与默认 Context 共用云端查询模块，即 Context 中如果 HTTP 报文中请求的域名不在预定义库，用户手动配置中都没有找到相应的分类时，会查询缓存记录，如果缓存中也不存在，会触发云端查询，返回的云端查询信息也会缓存至设备，供所有 Context 使用

可以手动配置云端服务器：

```
<Device> system-view
[Device] url-filter category server 184.37.0.40
```

注意

云端的 URL 库版本（版本标号方式采用 x.y.z，比如 1.0.30），要与设备的特征库版本满足版本号的前 2 位是一致的。比如本地 URL 特征库版本 1.0.30，云端版本 1.0.40 时，可以正常触发查询，当本地版本 1.0.30，云端服务器版本 1.1.30,时，无法正常查询。

1.5.1 打算阻断百度或者新浪网站，我应该怎么配置？

因为有些网站域名可能以.com.cn 结尾（如新浪），所以在 URL 过滤配置文件中添加黑名单，匹配模式为文本，主机名为*.baidu.*或*.sina.*即可。

1 文件过滤 FAQ

1.1 配置了阻断JPG文件的文件过滤，为什么打开的网页中仍然有图片？

- 文件过滤只支持 HTTP、FTP、SMTP、IMAP、NFS、POP3、RTMP 和 SMB 八种协议，若网页是加密的 HTTPS 协议，则需要配置 SSL 卸载才支持。
- 若图片文件位于 URI 的参数部分（URL 中“？”以后的部分为参数），则文件过滤不对其生效。

1.2 为什么会发生文件过滤偶尔不生效或产生错误动作的现象？

文件过滤是基于应用层检测引擎的特征识别功能的，新增或修改配置后，需执行 **inspect active** 才能生效。在新增或修改完成，到 **inspect active** 生效的这段时间内通过的报文，会发生不生效或产生错误动作的现象。

1.3 为什么文件过滤日志和报表中没有内容？

报表和日志功能需要命令行执行 **session statistics enable** 才能生效。文件过滤日志功能需要在配置文件过滤策略时勾选开启日志。

1.3.1 为什么文件过滤配置了文件扩展名不匹配动作不生效？

只有被检测文件的扩展名以及真实类型都在在所引用的文件类型组中时，才会执行文件扩展名与真实类型不匹配时动作。

1 带宽管理 FAQ

1.1 设备上长时间有流量经过，但是流量日志不更新？

观察设备是否报内存门限告警，设备一旦报内存门限，日志报表上面的数据就不会再更新，除非设备重启。

1.2 AVC带宽管理和DPI其它业务的异同？

- 不同点：AVC 带宽管理不需要创建和引用 app-profile，配置开启即生效。
- AVC 带宽管理 traffic-policy 是在系统视图下配置的，全局生效，不论端口类型，只与策略的匹配条件有关；AVC 带宽管理策略和通道的条数不受限制，只与设备内存有关。
- 相同点：都与 DIM（Deep Inspect Machine，深度检测引擎）有关，域间策略需引用开启深度检测 inspect 功能，AVC 带宽管理以 DIM 的会话拓展信息来限速，此外，基于应用应用组的限速则需要 DIM 识别后才能成功限速。

1.3 配置了接口带宽，为什么不生效？

接口带宽供其它模块调用，并不单独生效，需要配置带宽策略才生效，且需开启带宽策略，空策略亦可。此外，接口带宽只在流量方向的出接口生效，意思就是在流量方向的出接口配置接口带宽才会生效，反向亦可。

1.4 带宽策略、接口带宽和Qos作用的先后顺序？

流量从入接口进入，首先受到入接口的默认接口带宽（如 1G 口默认接口带宽是 1G，10G 口是 10G）的限制，接着受到入接口配置 inbound 方向 qos 的限制，然后根据带宽策略的匹配条件对流量进行筛选，筛选通过的流量进入对应的带宽通道，受到带宽通道的限速，如果出接口配置了接口带宽（如：**bandwidth** 100000，即 100M 接口带宽），会继续受到出接口的接口带宽限制，最终受到 qos 的 outbound 方向的限制。（一般情况下，DPI 业务不与 Qos 配合使用，功能有重复，且 Qos 业务会影响到 AVC 带宽管理的一些配置）。

1.5 带宽策略里面的优先级和带宽通道里面转发优先级、重标记DSCP有什么用途和区别？

- 带宽策略下的优先级只是作为一个流量的匹配项，其实质就是检测报文中相应字段有没有 DSCP 的标记（如：af11、ef 等），有则限速，无则不作处理。其用处和其它匹配项（如：源目的安全域、源目的地址等）相同。
- 带宽通道里面的转发优先级是针对带宽通道而言的，就是当链路发生阻塞时，优先转发优先级高的通道，这个是真正意义上的优先级，并不是带宽策略里面的优先级。

- 带宽通道里面的重标记 DSCP 和带宽策略里面优先级时对应的，它的作用就是改变初始报文中的 DSCP 标记，用来区分不同的流量，可通过抓包工具在 IP 层发现修改 DSCP 标记是否生效。

1.6 带宽策略里面不同匹配项之间“与”和“或”的关系？

带宽策略里面有多个匹配项，除了用户与用户组、应用于应用组之间是“或”的关系，其它匹配项之间是“与”的关系，意思就是用户和用户组只要匹配上至少一个即可，应用和应用组之间只要匹配上至少一个即可；此外，各匹配项自身可配置多个选项，自身多个选项只要匹配上至少一个，即此匹配项匹配成功。

1.7 带宽策略生效优先级和父子策略生效优先级？

带宽策略配置多条策略后，同时开启，最先配置的带宽策略先生效，从 web 和命令行直观就是从上到下，依次匹配；父子策略开启，先匹配父策略，父策略匹配上了才能继续匹配子策略，子策略匹配上了走子策略引用的带宽通道，子策略配置的带宽通道受父策略配置的带宽通道的限制。

1.8 打了流量好长时间，为什么流量报表和流量日志没有统计显示？

两个原因：

- 确保流量打通了，确确实实打到设备里面了
- 查看流量报表和流量日志，必须开启会话统计，就是必须敲“**session statistics enable**”这个命令，过一小段时间便会有流量统计。

1.9 配置基于每用户/每IP限速时，怎么限速不准确？

要学会计算整体限速，比如每用户限速是 100kbps，10 个用户就是 1M；每 IP 限速 100kbps，10 个 IP 就是 1M。如果限制了整体最大带宽，那么每用户限速*用户数量<整体最大带宽，同理，每 IP 限速*IP 数量<整体最大带宽，意思就是如果每用户/每 IP 限速乘积大于整体带宽，显示的就是整体带宽的数值，而不是计算后的每用户/每 IP 限速。

1.10 为什么使用实时带宽查询命令显示不了当前连接数？

可以用 **display traffic-policy statistics connection-limit maximum per-rule all** 来统计显示每条策略 CC（当前连接数）、RC（拒绝连接数）、CL（总连接数限制），目前版本需要先配置 CL（总连接数限制）后，可在带宽通道“会话连接数限制-整体并发连接数”设置即可，才能查看到 CC 和 RC；

此外，可以使用命令 **display traffic-policy statistics bandwidth rule all** 来统计显示每条策略生效时的实时带宽（目前版本暂不支持每用户、每 IP 的带宽限速显示）。

1.11 每用户和每IP最大带宽限速、并发连接数限制、新建速率限制？

针对带宽策略 rule 而言，最大带宽限速指的是整体最大带宽的限速，是每条 rule 的整体限速，而每用户、每 IP 最大带宽限速最终都要受到整体最大带宽的限制，且每用户和每 IP 相互排斥，只能选择其中一项；同理，并发连接数和新建速率也区分整体 rule 的和每用户、每 IP 的。

1.12 转发优先级和保证带宽谁的优先级高？

首先要明确两者使用的情况，转发优先级是配置即生效，而保证带宽只是在链路发生拥塞时确保关键业务不受影响才生效的。比如同样的两条关键业务的保证带宽同时生效，转发优先级高的通道就优先转发，两者不是一个时间段的概念。保证带宽只是确保它有一条最低的带宽供其占用，具体转发不转发在不配置转发优先级的情况下是自由竞争谁先转发，配置了转发优先级后，才明确谁具有优先转发的级别。

1 SSL VPN FAQ

1.1 在用户Context下需要安装证书吗？

用户 Context 相当于一个独立的虚拟的设备，需要安装证书。

1.2 访问Web资源后，页面显示的内容不全

访问 Web 资源，会对资源进行改写，目前只支持以下改写：

- text/html --> .html/htm/jsp/php。
- text/css --> .css。
- text/javascript -->.js。
- 除此之前的资源，不能显示。

1.3 手机浏览器登录网关能访问哪些资源

手机登录网关只能访问 Web 资源。

1.4 SSL VPN用户有哪些认证方式

SSL VPN 用户可以进行以下认证：RADIUS 认证、LDAP 认证、证书认证、本地认证。

其中，RADIUS 和 LDAP 认证方式通过 AAA 认证和授权。

1.5 更改SSL策略后，不能访问网关？

更改 SSL 策略后，要重新使能网关，才能正常访问网关。

1.6 更改资源后，为什么不能访问？

更改资源后，要重新登录网关，才能访问更改后的资源，因为不退出的话，访问的仍是登录时 SSL 实例分 VPN 配给用户的资源。

1.7 IP接入方式登录成功后为什么不能访问资源？

确定当前服务器上有没有开启相应服务（IP 接入方式用来实现远程主机与企业内部服务器网络层之间的安全通信，进而实现所有基于 IP 的远程主机与服务器的互通，如在远程主机上 ping 内网服务器。）；AC 口是否加入安全域，AC 口是个虚拟口，需要加入安全域；

AC 口与 address-pool 地址不能冲突，一旦虚拟网卡的地址与 AC 口冲突，报文就不能正常发出；

确定在资源组下引用 IP 接入资源时，是否使用 ACL 或 URI ACL 过滤，默认不配置 ACL 或 URI ACL 过滤时禁止所有客户端访问 IP 接入资源；

路由是否可达，server 端到 AC 口应是路由可达的。

1.8 访问server的出接口配置VPN多实例，SSL VPN应该怎么配置？

访问 server 的出接口配 VPN 多实例时，SSL VPN Context 下要引用相同的 VPN 多实例，AC 接口也要引用相同的 VPN 多实例；

注意安全策略要允许相应 VPN 多实例通过。

1.9 连接网关的接口配置VPN多实例，SSL VPN应该怎么配置？

连接网关的接口配置 VPN 多实例时，SSL VPN gateway 下要配置相应 VPN 多实例；

注意安全策略要允许相应 VPN 多实例通过。

1.10 当client端不能访问SSL VPN网关时，怎么排查？

确认设备是否安装证书；

确认配置的 SSL VPN 网关的 IP 地址和端口号应该与设备的管理 IP 地址和端口号不同；

确认 Client 与网关设备是否路由可达；

确认是否开启了证书认证方式，并确认是否在客户端安装相应证书；

确认网关是否使能。

1.11 访问Web、TCP资源失败，提示**connect server failed**，怎么排查？

确认访问的 server 资源是否存在；

确认到 server 的路由是否可达；

确认 TCP 资源是不是类似于 FTP 类有双通道且前后端口号有变化的业务，目前 TCP 资源不支持此类资源。

1.12 更改SSL 服务器端策略后，SSL VPN不能访问网关怎么解决？

更改 SSL 服务器端策略后，要重新使能网关，才能正常访问网关。

1.13 SSL VPN不同接入方式对客户端的要求是怎样的？

Web 接入使用浏览器访问；

TCP 接入不能事先安装 TCP 接入软件，只能通过浏览器登录网关后，下载客户端，需要 PC 上安装 1.7 及以上版本的 Java 程序；

IP 接入需要安装客户端（如 iNode 客户端），可以提前安装或通过浏览器登录网关后下载安装。

1.14 SSL VPN使用证书认证有什么限制？

SSLVPN 证书认证：TCP 接入、移动客户端不支持强认证，只支持弱认证；只有 WEB 登录和 PC 版 iNode 客户端支持证书强认证方式。

证书的强认证和弱认证是在 SSL 服务器端策略配置**`client-verify { enable | optional }`**。

执行了 **client-verify enable** 命令的情况下，则 SSL 客户端必须将自己的数字证书提供给服务器，以便服务器对客户端进行基于数字证书的身份验证。只有身份验证通过后，SSL 客户端才能访问 SSL 服务器。

执行了 **client-verify optional** 命令的情况下，若 SSL 客户端未提供数字证书给服务器，SSL 客户端也能访问 SSL 服务器；若 SSL 客户端提供数字证书给服务器，只有身份验证通过后，SSL 客户端才能访问 SSL 服务器。

1.15 不安装SSL VPN License，就不可以成功登录SSL VPN网关吗？

不是。不安装 SSL VPN License，只有特定数量的用户才能成功登录 SSL VPN 网关并访问内部资源（各款型设备默认支持的 SSL VPN 用户数不同，具体参考产品介绍）。

1 IPsec FAQ

1.1 IPsec配置AH协议支持NAT穿越吗？

IPsec 配置 AH 协议不支持 NAT 穿越。

穿越 NAT 后，报文的 IP 地址肯定是要改变的，由于 AH 对整个 IP 都进行验证，NAT 网关改变 IP 头的地址后，会造成接收端 AH 验证失败。因此 AH 和 AH-ESP 协议不支持 NAT 穿越。而 ESP 只对 IP 负载进行验证，因而不存在这个问题。

1.2 IPsec策略中的ACL支持应用对象组的方式吗？

IPsec 策略中的 ACL 不支持应用对象组的方式。

1.3 IPsec策略的对端地址支持使用域名方式吗？

IPsec 策略的对端地址支持使用域名方式，此域名为 DNS 解析的域名。

1.4 IKE keychain配置中的hostname是指的是DNS域名吗？

IKE keychain 配置中的 hostname 是 FQDN 的意思，并不是指 DNS 域名。

1.5 IPsec生命周期配置太短会有什么影响吗？

目前 IPsec SA 的时间生命周期最短为 180s，流量生命周期最小为 2560 千字节。若配置 IPsec 生命周期为最短，大量流量情况下触发多隧道建立，SA 建立后很快就由于生命周期超时重协商，这样增加了设备 CPU 占用率，在大流量下 IKE 协商报文还有可能丢失，导致协商失败。因此建议不要将 IPsec 的生命周期配置太短。

1.6 发起方IKE profile下配置多个keychain的情况下，是怎样匹配的？

按照配置顺序匹配。

1.7 查看transform-set显示不完整是什么原因？

配置了 ESP 的情况下，必须配置加密算法，不能只配置认证算法。

1.8 发起方带有多个transform-set时，transform-set带有PFS，响应方怎样进行协商？

- 如果发起方第一个配置的 transform-set 带有 PFS，则响应方带有相应的 PFS，可以正常协商。
- 如果发起方第一个配置的 transform-set 不带有 PFS，则响应方必须不带有 PFS 才能正常协商，而不会去和发起方其它带有 PFS 的 transform-set 进行协商。

1.9 IPsec安全策略发起IKE协商时使用PFS特性，发起方和响应方应该怎样配置？

发起方的 PFS 强度必须大于或等于响应方的 PFS 强度，否则 IKE 协商会失败。

1.10 IPsec策略的相应配置中带有vpn-instance时，ACL规则需要带vpn-instance吗?

ACL 的规则里面不需要带 vpn-instance 配置。

1.11 发起方是怎样将proposal发送给响应方的？

作为发起方，如果没有配置 proposal，就会将所有 proposal 列表发给对方，让响应方选择；如果配置了 proposal，只发所配置的 proposal。

1.12 NAT穿越组网，NAT Keepalive时间间隔设置有什么需要注意的吗？

双方的 NAT Keepalive 报文间隔一定要小于 NAT 设备的会话老化时间，若 NAT Keepalive 发送的时间间隔小于中间 NAT 设备会话老化时间，NAT 会话会先老化，后续数据流量过来后会由于没有会话或者新建的会话端口号和两端记录的不一致而失败。

1.13 抗重放功能是否适用于乱序严重的场景？

IPsec 抗重放是使用滑动窗口机制来检查报文是否是重复报文或者是已经过期的报文，当乱序严重时，收到的报文落到了接收方抗重放滑动窗口的左侧时会被丢弃。因此乱序严重的环境中，建议关闭抗重放功能，或者将抗重放窗口设置为最大。

1.14 IPsec的国密算法都有哪些算法？

国密算法有加密算法：SM1-CBC-128，SM4-CBC；认证算法：SM3；国密证书认证使用 SM2-DE 数字信封。

1.15 IPsec的国密算法都需要有硬件国密卡才能支持吗？

不需要。只有 SM1-CBC-128 加密算法需要硬件国密卡，其他算法软件都可以实现。

1.16 目前我们支持哪些硬件国密卡？可以在哪些设备上使用呢？

目前我们支持如下硬件国密卡：

适配 F1000 系列的硬件国密卡：NSQM1F1KGMB、NSQM1F1KGMC、NSQM1F1KGM0。

适配 F5000 系列的硬件国密卡：NSQM1F5KGMC、NSQM1F5KGM0。

适配 F50X0 系列/F50X0-D 系列的硬件国密卡：NSQM1HTIMGMG2A、NSQM1HTIMGMG2B。

1 负载均衡特性 FAQ

1.1 服务器负载均衡

SLB 虚服务器、实服务组、实服务器的概念？

- 虚服务器：虚服务器是负载均衡设备上提供的一种虚拟服务，是为了判断是否需要对到达负载均衡设备的报文进行负载均衡而引入的概念。只有与虚服务器 IP 地址匹配的报文才会进行负载均衡处理。
- 实服务器：实服务器用来在负载均衡设备上模拟用户的业务服务器，用于指导报文转发。一台实服务器只能属于一个实服务组，而一个实服务组可以包含多台实服务器。
- 实服务器组：为了便于对多台服务器进行管理，可以依据这些服务器的共有属性划分成不同的组，称为实服务组。比如，可按照存储内容的不同划分为歌曲服务器组，视频服务器组或图片服务器组等。

如何排查 SLB 业务不通的问题？

(1) **display real-server brief** 查看虚服务、实服务的状态，状态是否处于 Active 状态；

(2) **display virtual-server statistics** 查看对应虚服务统计信息是否有变化，有变化说明报文已经匹配到虚服务，应从匹配的虚服务找问题原因。否则，查看为何没有命中虚服务；

(3) 查看 Debug 调试信息。

SLB 的 http 类型下，设置规则为 cookie，如果一个报文中包含多个请求，只检查第一个请求的 cookie 吗？

如果一个报文中包含多个请求，默认只处理第一个请求，按照第一个请求进行负载分担，要处理每个请求需要配置 http parameter:rebalance per-request。

SLB 负载均衡动作中，删除头部，如果一个报文中包含多个请求，只删除第一个请求的头部吗？

如果一个报文中包含多个请求，默认只处理第一个请求，要处理每个请求需要配置 http parameter:header per-reques。

SLB 的参数模板中的 set ip tos 命令与 action 中的 set ip tos 命令有什么区别？

set ip tos 在参数模板中设置改变的是发向客户端的报文的 tos 值，在 action 中设置改变的是发向服务器的报文的 tos 值。

为什么已经在实服务组下使能就近性功能了，却仍然没有生成就近性表项？

可以先检查就近性下有没有配置就近性探测方法。

因为就近性表项的产生依赖于就近性探测，因此如果此处没有配置有效的就近性探测方法，则不会生成就近性表项。

七层虚服务下负载均衡策略和默认实服务组同时引用时业务怎么处理的？

虚服务器引用策略后策略的优先级比默认实服务器组优先级高。

根据虚服务器引用策略到引用默认实服务器组上的配置差异，划分下虚服务器的转发方式。如下：

- 动作配置了实服务器组，根据实服务器组下实服务器指导转发。
- 动作没有配置实服务器组或配置实服务器组不存在，转发方式为丢弃。
- 策略下没有配置动作，或虚服务器引用策略不存在，按默认实服务器组转发。

HTTP NAT64 功能怎么实现的？

HTTP 类型虚服务器支持 NAT64 功能，具体实现如下：

Client----------(IPv4)--------->LB----------(IPv6)-------->Server

Client----------(IPv6)--------->LB----------(IPv4)-------->Server

注意：

- HTTP 服务器尽可能的使用和客户端协议一致的类型进行负载分担，即客户端是 IPv4，选择的服务器在既支持 IPv4 也支持 IPv6 的情况下，会使用 IPv4 地址和服务器进行连接。如果配置的服务器的 IPv4 地址如果路由不可达，接收到客户端的 IPv4 请求时也会继续使用 IPv4 和后台服务器进行连接。这种情况下建议用户配置实服务器下配置健康检测来进行规避。
- NAT64 转换的实现依赖于对应的 SNAT 地址池，即如果实现 IPv4 转成 IPv6 和服务器链接，那么实服务器组必须配置 IPv6 的 SNAT，否则无法转换。

虚服务配置有哪些注意事项？

虚服务器可用条件是配置 IP 地址和开启服务。因为虚服务如配置为重定向是不需要配置实服务器组和策略的。如配置可用虚服务器且被报文命中，转发流程就进入 LB 流程处理。

虚服务器传输层类型（TCP/UDP/任意）、VPN、IP 地址、端口、掩码唯一确定一个服务，五者的组合在虚服务器的配置中要满足唯一性。

任意两个类型为 TCP、HTTP 或快速 HTTP 的虚服务器不可以进行 VPN、IP 地址、端口、掩码均相同的配置操作，命令行会提示错误。因为基于的四层协议都是 TCP，这种相同配置会影响到报文对虚服务器的匹配和流量的转发。除此外，IP 或 UDP 类型的虚服务器如配置和其他类型虚服务器的 IP 地址、端口、掩码相同，虽然不会提示错误，但匹配虚服务的报文，会走哪个虚服务处理，是不确定的，不建议用户做此类配置动作。总结来说，对于快速 HTTP、HTTP、IP 和 TCP 这四种类型，请避免配置 VPN、VSIP 和端口号都相同、但类型不同的虚服务器，否则将无法预知负载均衡设备处理报文的方法。

负载均衡策略和持续性配置有哪些注意事项？

通用类型的负载均衡策略只能引用通用类型的负载均衡类和负载均衡动作，HTTP 类型的负载均衡策略则无此限制。

四层虚服务器无法引用七层持续性方法、七层策略及七层参数。如用户进行此类错误配置，配置将不生效。

HTTPS 卸载组网流量不通怎么排查？

- 如果虚服务器引用了 SSL 策略，则必须为其配置一个非缺省端口号（通常用 443），如不配置，将不能正常处理。
- 修改 SSL 的配置，虚服务器目前无法感知，要想让 SSL 的配置在虚服务器上生效，请主动在虚服务器下执行 undo service enable 和 service enable。
- 实服务器端口号配置是否与真实服务器开放的端口一致。

Cookie 插入和 Cookie 重写持续性有什么区别？

Cookie 插入持续性与 Cookie 重写持续性区别在于，Cookie 重写需要服务器应答报文携带指定 name 的 Set-cookie 或 Set-cookie2 头域，LB 设备改写对应的 value 值，并发给客户端。而 Cookie 插入持续性不需要服务器端提供此配合。

Cookie 插入和 Cookie 重写如何生效？

Cookie 插入持续性方法被虚服务器或者负载均衡策略引用后，LB 会插入 set-cookie 字段给客户端，客户端请求中携带此字段的请求报文会匹配持续性表项，转发给相应的服务器处理。

Cookie 重写持续性方法被虚服务器或者负载均衡策略引用后，LB 会重写服务器应答报文的 set-cookie 字段给客户端，客户端请求中携带此字段的请求报文会匹配持续性表项，转发给相应的服务器处理。

配置参与算法调度的最小与最大实服务器数量有哪些注意事项？

配置了最小与最大参与算法调度的实服务器数量后，参与算法调度的实服务器不能少于最小值，除非实服务器组下的实服务器总数少于配置的最小值，那么所有的实服务器都参与调度，否则按优先级选取参与算法调度的实服务器且不能大于最大值。

实服务器权值对哪些调度算法有效？

实服务的权值对加权轮转算法，带宽算法，加权最小连接算法，基于成员的加权最小连接算法有效。

故障处理方式为断开已有连接时，对于 UDP 和 ICMP 流量需要辅佐开启什么命令？

系统视图下需要开启 **ip unreachables enable**，否则无法向客户端发出断开连接的报文。

IRF 组网中如何配置会话备份？

LB IRF 组网中，主备框的会话同步，必须要同时配置 **session sync** 和 **connection-sync** 这两个命令。一般情况，客户肯定需要主备框会话同步的，那就是这两条命令是必须配置的。

七层虚服务 VS 类型不支持该热备命令。

SLB、outbound 和 inbound 的健康检查方法，以及动态就近性探测方法，分别都有哪些？

SLB 的对于实服务组和实服务器的健康检查方法，都支持哪些？

支持全部 nqa 探测模板类型

Outbound 对于实服务组和实服务器的健康检查方法，都支持哪些？

支持全部 nqa 探测模板类型。

Outbound 的动态就近性探测，都支持哪些？

支持负载均衡探测模板。

Inbound 的链路的健康检查方法，都支持哪些？

支持全部 nqa 探测模板类型。

1.2 出链路负载均衡

OutBound 链路负载虚服务和静态路由、策略路由的关系是什么？

OutBound 链路负载均衡虚服务优先级高于静态路由和策略路由，因此如果报文匹配到 OutBound 链路负载均衡的虚服务，则负载均衡模块优先处理；如果报文没有匹配到虚服务，则会依次匹配策略路由、静态路由。

流量匹配上就近性表项，可是为什么就近性表项仍然会老化呢？

LB 只是转发中间的业务处理之一，LLB 是处于慢转预处理和查 fib 之后的处理阶段。

某一会话的首报文到到达 LB，LB 会为其选路，选择好 RS 后，会话会有快转表项生成，此会话的后续报文就不用再次选择 RS 了，就直接按照快转表项中的进行转发。因此如果开启就近性，也不会匹配就近性表项，而是直接走快转了。

因为就近性表项的刷新，是靠流量匹配来刷新的。此时，因为没有流量来匹配就近性，所以就近性表项可能会老化掉。

就近性计算时的参数影响是什么样的？

在就近性计算时是根据各参数来计算各链路的。某一参数的权值增大，就说明其影响力变大。比如 TTL 和 COST：

RS1: TTL(3) COST(99) COST 优；

RS2: TTL(2) COST(100) TTL 优；

就近性下 TTL 权值 1 COST 权值 50；那么最终应该是 RS1 比较优；

如果就近性下 TTL 权值 100，COST 权值 50，那么最终应该是 RS2 比较优。

就近性表项已经存在时，修改就近性探测方法，会怎么样？

已经存在就近性表项时，修改就近性探测方法，则会立即清空就近性表项，然后再由报文触发，利用新的探测方法进行就近性探测。

为什么修改 Link 的 cost 会清除就近性表项，而修改带宽不会呢？

在就近性计算中，cost 是其中一个计算参考值，所以在修改 Link 的 cost 时，会立即清除已有的就近性表项，以便将来有流量触发时重新计算就近性；

虽然就近性计算中，带宽也是计算参考值，但是这里的带宽指的是剩余带宽，剩余带宽会根据网络状况实时变化，就近性计算不可能实时去响应其变化。在修改 Link 的 rate-limit band 时，修改的是 Link 的总带宽，并不是剩余带宽。

为什么 Link 没有被引用，却也是 active 的呢？

Link 如果被 link-group 引用了，受 outbound 配置的限制。如果 outbound 配置不完全就会显示该 Link 为 inactive 的。

Link 如果没有被 link-group 引用，只要有 IP 且触发了探测，按照探测决定状态。若没有探测就直接 Active。

为什么 nqa 的 debug 中总打印一些 abandon 的 error 信息呢？

*Jun 11 16:44:48:264 2015 H3C NQA/7/Error: -Context=1; NQA entry (t1-instance12d 9e7090?) abandon the unknown packet

协议栈对 icmp 报文全局上送，每个 rawip icmp socket，都会收到其他模块 icmp 报文或者本模块其他 icmp socket 报文，对于这些报文会丢弃。

Link1 是持续性表项，同时 Link1 配置带宽保护，为什么有时带宽保护不生效呢？

持续性组下有个功能 override-limit enable，开启该功能后，如果该连接匹配了已有的持续性表项，将不受 Link 上的带宽（指的带宽保护 bandwidth busy-rate 和 max-bandwidth，以及带宽速率 rate-limit bandwidth）及连接参数(**rate-limit connection 和 connection-limit max**) 以及虚服务器上的连接数限制（指的 lb-limit-policy）影响。

虚服务上同时配置连接限制，和连接数限制策略 limit-policy，是怎么生效的？

是虚服务下直接配置的连接限制先过滤一次，然后再通过 limit-policy 过滤一次，两重过滤。

负载均衡动作中配置 **fallback-action continue**，查找链路失败时继续匹配策略中下一条引用规则？

这个是指动作中查找链路失败时，继续匹配策略中的下一条引用规则。

在负载均衡策略中转发报文时会按照配置顺序来匹配流量特征和动作，匹配成功则执行相应动作，否则继续匹配下一条负载均均衡流量特征？

这个是指策略中的流量特征如果第一条匹配不上默认继续向下匹配。

带宽繁忙如何测试？

带宽繁忙生效依据：当前流量带宽大于通过命令 **`max-bandwidth`** 配置的链路最大期望带宽。

当前流量的带宽获取方式有两种：

链路自己统计的带宽；从接口获取的带宽，这个需要在虚服务下使能从接口获取带宽，同时注意接口获取带宽默认是 300s,如果链路对应的是物理口则可以使用 **`flow-interval`** 设置获取统计的时间。如果 link 对应的是物理口外的其他端口则只能是默认 300s。如果接口的带宽值大于这个值则达

到了链路繁忙状态，如果链路一直繁忙那么此时该链路不分发新建连接，已有连接不受影响，新建速率为 0，直到恢复不繁忙状态会有新建连接。

首先 vs 下要开启繁忙保护及从接口获取带宽的功能，链路中设置最大带宽 **max-bandwidth** 和带宽繁忙比 **bandwidth busy-rate**，当前流量的带宽大于最大带宽*带宽繁忙比则链路繁忙。

注意以下几点：

- 链路繁忙需要设置链路中的 **max-bandwidth**。
- 如果链路下设置带宽限制 **rate-limit bandwidth**，当前流量的带宽如果大于最大带宽*繁忙比，即链路繁忙，如果所有链路都繁忙的情况下，链路设置了 **rate-limit**，此时接口最多转发 **rate-limit** 值，大于这个值会丢包。
- 繁忙保护仅对出接口 output 生效，对 input 不做限制。只负载 client 往外的请求。
- Outbound 链路繁忙无 debug 信息。
- 链路里面设置带宽繁忙 inbound 方向、outbound 方向或者 inbound+outbound 方向，只要有一个达到了繁忙保护值，link 就处于受限状态不再有新建连接。

测试过程中可能遇到的现象：

- 繁忙生效后，出接口 output 方向统计为 0 ，本来应该是至少有 max*busy 的值，可能因为测试仪器对原有连接后续没有流量
- 链路下配置 **max-bandwidth**、**bandwidth busy-rate** 有 inbound、outbound 只是对出接口 input、output 进行统计，对于 output 值会限定在 max*busy-rate 值内，对于 input 统计不限制。

链路组中，如果链路设置了优先级最高，当这个链路带宽达到了繁忙保护的值或者连接的最大值后，会切换到其他链路？

当优先级高的链路达到最大连接数后，vs 丢包，不会将连接发到低优先级链路上。如果链路组中设置了参与调度的链路也不重新选择其他链路。

链路组中，如果链路设置了优先级最高，同时设置了参与调度的链路？

当高优先级链路 down 或者探测失败会选择低优先级链路。

带宽算法和最大带宽算法解释？

- 带宽算法

bandwidth：带宽算法，即报文根据实服务器的权值与剩余带宽比例分发到各实服务器上。

进入虚服务器视图 **virtual-server** *vritual-server-name*；配置链路的带宽由接口统计：**bandwidth interface statistics enable**

缺省情况下，链路的带宽由负载均衡模块自行统计。

剩余带宽 = 链路的最大带宽 - 当前带宽

如果要测试带宽，一般都配置 link 的最大带宽

rate-limit bandwidth [**inbound** | **outbound**] *bandwidth-value*

是配置 RS 的最大带宽，和接口带宽没有关系

只有 VS 下打开了 **bandwidth interface statistics enable**，RS 的当前带宽不再使用 LB 自行统计的带宽，而是使用 RS IP 地址所在的接口的带宽作为 RS 的当前带宽。

LB 自行统计带宽，是指的 LB 分发给该链路的报文，每秒做一次，然后下一秒分配连接时，就根据前一秒的这个值来确定链路带宽。

加入 rs1 的 weight 是 3，剩余带宽 100M；rs2 的 weight 是 2，剩余带宽 200M；rs3 的 weight 是 1，剩余带宽是 300M，那么三个实服务器怎么分配？

大致比例：大致：3*100 ： 2*200 ： 1* 300

但是具体实现不是这么做的。可以这样理解

- 最大带宽算法

max-bandwidth：最大带宽算法，即报文总是分发给当前空闲带宽最大的实服务器。

不论是否配置接口下获取带宽，总带宽都是根据 rs 下配置的 rate-limit band。

而如果虚服务下配置了从接口获取带宽，那么当前使用的带宽就从接口的 Last 来获取；如果没有配置从接口获取带宽，就从 display real-server statist 的 Throughput 来获取。

如果在虚服务下配置从接口统计带宽，那么 LB 是从接口的 Last 统计中来获取带宽的。

接口的 Last 统计间隔，根据在接口上配置 **flow-interval** 来配置，比如 **flow-interval 5** 就是每 5 秒统计一次；

LB 则是固定的每一秒都向接口 Last 获取一次值，得到当前使用带宽，再用配置在实服务器下的 rate-limit band 总带宽，来减去当前使用带宽，得到当前空闲带宽，进行比较。

接口最小统计间隔是 5 秒，这 5 秒内都只有同一个接口的流量是最小的，所以这 5 秒内 LB 分配也只有这个实服务器 rs1 被选中。下一个 5 秒时，实服务器 rs1 的流量就会统计为较大，那么就会在剩下的实服务器里选择一个最大剩余带宽的，选中后就再次开始这个过程的循环。总之，接口统计 5 秒时间内，都只会选择同一个实服务器；下一个 5 秒时间内，再次选择剩余带宽最小的实服务器。

可能会出现多个链路中，只有某几个链路有流量，其他几个链路一直没有流量的情况？

最大带宽算法就是会选择一个 SF 中剩余带宽最大的 RS，如果有多个 RS 剩余带宽一样大，就会把排在前边的选出来（可能和你创建 RS 的顺序有关），之前被选过的 RS 的剩余带宽会在其他 RS 被选期间再次变大，从而再次被选，导致有几个一直没有机会被选。

如果使能了动态就近性，且设置了链路的优先级，如果动态就近行探测到的链路优先级低应该如何处理？

就近性选择优先级高的链路为最优链路。

保持上一跳和静态路由、策略路由的优先级顺序是什么？

保持上一跳优先级高于静态路由和策略路由，策略路由优先级高于静态路由；如果没有保持上一跳，则会依次匹配策略路由、静态路由。

就近性和持续性都存在，流量先是去匹配哪个呢？

先匹配持续性，如果持续性表项不匹配，再去匹配就近性表项，如果就近性表项也不匹配，就按照算法来选择链路。

既使能持续性又使能就近性时，如果持续表项和就近性表项都不存在的情况下，是先根据算法生成持续表项。然后根据探测结果生成就近性表项。

持续性表项和就近性表项同时存在的情况下，持续表项优先。

就近性与链路带宽限制在选择链路时有什么样的相互影响？

如果链路配置了带宽速率限制，即使就近性表项中该链路为最优，也会因为带宽限制而不走它，而是选择次优。等这个链路的带宽低于限制后，则再次被选择。

就近性表项已经存在时，修改就近性探测方法，会怎么样？

已经存在就近性表项时，修改就近性探测方法，则会立即清空就近性表项，然后再由报文触发，利用新的探测方法进行就近性探测。

为什么已经在链路组下使能就近性功能了，却仍然没有生成就近性表项？

可以先检查就近性下有没有配置就近性探测方法。

因为就近性表项的产生依赖于就近性探测，因此如果此处没有配置有效的就近性探测方法，则不会生成就近性表项。

修改链路的 COST、RTT、带宽等参数对就近性表项有什么影响？

当就近性参数变化时，如果对选择链路优先级产生影响会更新就近性表项，产生新的最优链路。当手工清除就近性表项或者就近性表项自然老化，就近性表项会删除。

为什么所有 link-group 都去使能就近性，就近性表项仍然存在呢？

就近性表项是针对全局的，针对所有 link-group 的。当所有 link-group 都去使能就近性时，表项不会立即删除，也不会进行就近性探测，表项不会生效。而是继续保留直到老化删除，或者手工删除。

SIP 流量时，为什么有时不能产生就近性表项呢？

如果此时会话里已经有会话了，则会直接按照会话转发，不再触发就近性探测。

如果没有会话，但是已经有会话关联表了，则首包会匹配会话关联表，而建立会话，以后的报文直接走会话。

子会话会根据关联表建立会话，然后走非首包流程。

为什么链路没有被引用，是什么状态？

链路如果被 link-group 引用了，受 llb outbound 配置的限制。如果 llb outbound 配置不完全就会显示该链路为 inactive。

链路如果没有被 link-group 引用，只要有 IP 且触发了探测，按照探测决定状态。若没有探测状态为 unknown。

带宽繁忙保护对算法对选路的影响？

link-group 中配置最大带宽算法，链路 link1 配置带宽繁忙比，并且剩余带宽最大：

根据最大带宽算法，先分配给 link1，当 link1 的带宽超过保护带宽后，此时 link1 停止分配连接，连接分配给 link2；当 link1 的带宽下降至保护带宽以下时，因为剩余带宽最大，再次因为最大带宽算法而分配连接。

link-group 下使能就近性功能，当 link1 带宽超过保护带宽后，将不参与算法，也将不参与就近性探测。当带宽小于保护带宽后，重新加入算法，重新被就近性探测。

link-group 下配置持续性，link1 配置带宽保护，若持续性表项为 link1，则将不受带宽保护的影响，而继续按照持续性向 link1 分配连接。

当链路使用带宽超过设置的繁忙比例即认为链路繁忙，默认繁忙比为 70%，如果所有链路都超过繁忙比，那链路保护失效，算法重新回到最初配置的算法。当 link1 的当前带宽下降至最大带宽繁忙比以下后不会重新分发，要等到下降到新版本中支持的最大带宽繁忙恢复比，才会再重新分配。

关于链路负载均衡健康检测的参数有什么设置建议？

参数建议：

(1) Frequency > “probe timeout”

(2) 故障切换时间=(“reaction trigger probe-fail” – 1) * frequency + “probe timeout”

(3) Max（恢复时间）= frequency * “reaction trigger probe-pass”

(4) Frequency、probe timeout、 reaction trigger probe-fail 过小可能导致网络震荡。

测试时发现就近性表项空或无预期链路，怎样排查错误？

请排查如下几项：

(1) 流量匹配的链路组下是否已使能就近性

(2) 就近性视图下是否已配置探测方法

(3) 链路状态是否为 active

(4) 链路是否配置各种限制，且已到限（带宽，连接数，繁忙阈值等）

测试时发现就近性表项最优链路发生变化，怎样排查错误？

请排查如下几项：

(1) 原最优链路不在优先级链表里了，请看就近性表项空或无预期链路的相关排查项

(2) 大流量导致链路的剩余带宽发生改变，从而影响优先级。可将就近性视图下带宽的权值设置为 0，排查是否是受其影响

1.3 DNS透明代理

使用 DNS 透明代理时，客户端 DNS 地址可以设置为 LB 设备的接口地址吗？

DNS 透明代理默认全部为 0.0.0.0 的话，客户端 DNS 地址设置为 LB 设备的接口地址，这样就不会进行 DNS 代理，因此不建议配置为设备接口地址

如果客户端 DNS 地址设置为 LB 设备接口的地址，需要将 DNS proxy 视图下的地址同样设置为该地址才会处理（32 位掩码），但目前建议是 DNS proxy 地址为 0.0.0.0，web 也是默认 0.0.0.0

1.4 本地智能DNS

智能 DNS（LLB Inbound）就近性有哪几种？

目前的新版本上关于就近性算法有两种，静态就近性算法选择 topology；动态就近性算法选择 proximity。

虚服务池（virtual-server-pool）中调度算法的优先级如何选择？

配置虚服务器池的调度算法时，可以分别指定首选调度算法、备选调度算法和次选调度算法。其中，首选调度算法优先级最高，当采用首选算法不能选出可用的虚服务器时，采用次选调度算法，备选调度算法优先级最低。

智能 DNS（LLB Inbound）开启会话备份功能，而智能 DNS 报文的未会话备份？

系统视图下已开启 **session synchronization dns http** 和 **session synchronization enable**，而智能 DNS 未对会话进行备份？

统计是各板独立的，会话备份请查看会话表项，UDP DNS 流量会话备份意义不大，一般一个请求+一个应答。

虚服务池中如果指定首选调度算法为拓扑，未指定备选和次选，首选 vs 达到链路繁忙保护后，接下来的请求如何处理？

如果虚服务池中某个 vs 对应的 link 达到链路繁忙保护后，继续根据报文源 ip 匹配的 topo 下在其他未达繁忙保护的 vs 里面选择。vsp 中使用优选调度算法是拓扑，如果拓扑中没有匹配的 vs,没有指定次选和备选调度算法，这时候选不出 vs 失败了，因此需要配置次选和备选的调度算法。

当首选算法为动态就近性时，有丢包怎么办？

动态就近性算法，由报文触发，立刻生成就近性表项，十秒后生成可用的就近性表项，期间 DNS 请求会被拒绝，所以要填写备选和次选算法，如加权轮转算法，保证业务的正常处理，待生成可用的就近性表项后，首选调度算法可用。

1 镜像 FAQ

1.1 是否支持端口镜像？

不支持端口镜像，只支持流镜像。

1.2 是否支持远程镜像？

不支持远程镜像功能。

1 IRF FAQ

1.1 IRF功能的主要目的是什么？

- 简化管理：IRF 形成之后，用户通过任意成员设备的任意端口都可以登录 IRF 系统，对 IRF 内所有成员设备进行统一管理。
- 1:N 备份：IRF 由多台成员设备组成，其中，主设备负责 IRF 的运行、管理和维护，从设备在作为备份的同时也可以处理业务。一旦主设备故障，系统会迅速自动选举新的主设备，以保证业务不中断，从而实现了设备的 1:N 备份。
- 跨成员设备的链路聚合：IRF 和上、下层设备之间的物理链路支持聚合功能，并且不同成员设备上的物理链路可以聚合成一个逻辑链路，多条物理链路之间可以互为备份也可以进行负载分担，当某个成员设备离开 IRF，其它成员设备上的链路仍能收发报文，从而提高了聚合链路的可靠性。
- 强大的网络扩展能力：通过增加成员设备，可以轻松自如地扩展 IRF 的端口数、带宽。因为各成员设备都有 CPU，能够独立处理协议报文、进行报文转发，所以 IRF 还能轻松自如的扩展处理能力。

1.2 组成IRF的设备有什么特别要求？

- IRF 中所有成员设备的软件版本必须相同，如果有软件版本不同的设备要加入 IRF，请确保 IRF 的启动文件同步加载功能处于开启状态。
- 请确保 IRF 中各成员设备上安装的特性 License 一致，否则，可能会导致这些 License 对应的特性不能正常运行。
- 设备哪些端口可以作为 IRF 物理端口与设备的型号有关，请以设备的实际情况为准。通常情况下，要求是设备上的高速率端口。某些型号的设备出厂时已经将 IRF 端口与 IRF 物理端口绑定，用户不需要配置也不能修改；某些型号的设备出厂时没有将 IRF 端口与 IRF 物理端口绑定，需要用户通过命令行手工配置后才能用于 IRF。
- 如果使用 IRF 专用接口作为 IRF 物理端口，则需要使用 IRF 专用线缆连接；IRF 专用线缆能够为成员设备间报文的传输提供很高的可靠性和性能。如果使用光口作为 IRF 物理端口，则需要使用光模块和光纤连接；这种连接方式可以将距离很远的物理设备连接组成 IRF，使得应用更加灵活。如果使用电口作为 IRF 物理端口，则只需使用以太网网线连接。这种连接方式提高了现有资源的利用率。

1.3 IRF模式下升级，要注意什么？

所有成员设备均要在自己存储空间内保存用于升级的版本文件，或者升级时同意进行覆盖升级，否则可能导致升级失败。

堆叠设备通过 ISSU 升级，可保证现网中不会发生断网。

1.4 IRF双主模式，要注意什么？

- 二层双主模式下，双上行和双下行链路组网时，要求上下行交换机都支持跨设备链路聚合。
- 双主组网中，必须要开启双主开关即 session dual-active enable；同时流量下，禁止随意切换该双主开关。
- 当同时开启 hash 选板和 UDP 透传命令时，优先保证报文进行 hash 选板，UDP 透传命令失效。
- 双主目前不支持 F50X0-D 系列、F5000-AK 系列、松耦合产品，IRF 双主二三层都可以支持，但 VRRP 双机热备目前只能是三层接口，因为 VRRP 协议是三层协议。
- 双主环境不支持逐包负载分担。
- NAT EasyIP M9K 支持主备环境下端口拆分，不支持双主环境端口拆分。
- AFT 业务不支持双主功能。
- 双主聚合组网时，交换机也必须相应的做聚合。

1 安全策略 FAQ

1.1 安全域之间，默认安全策略是怎么样的？

默认是 deny 的。

1.2 安全域之间的策略有哪些？

主要包括包过滤、ASPF、对象策略和安全策略。

1.3 对象组嵌套的情况下，最多支持几层嵌套？

支持 5 层深度的引用。

1.4 安全策略匹配和NAT操作的顺序是怎样的？

nat server 是在安全策略匹配前进行转换操作，安全策略匹配 nat server 转换后的 IP 地址；
nat outbound 是在安全策略匹配后进行转换，安全策略匹配 nat outbound 转换前的 IP 地址。

1.5 GRE、L2TP等隧道流量安全策略的配置，需要关注哪些问题？

对隧道流量，需要配置两条策略。在解封装方向，需要配置如下两条策略：

- 物理入接口所在安全域到 Local 域之间的安全策略；
- Tunnel 或者 VT 所在安全域到物理出接口所在安全域之间的安全策略。

加封装方向需要配置如下两条策略：

- 物理入接口所在安全域到 tunnel 或者 VT 口所在安全域之间的安全策略；
- Local 域到物理出接口所在安全域之间的安全策略。

1.6 安全策略和对象策略功能是否能在设备上同时使用？

安全策略功能与对象策略功能在设备上不能同时使用，当安全策略功能处于开启状态时，首次进入安全策略视图后，对象策略功能立即失效。

1.7 配置安全策略后，包过滤功能还生效吗？

当安全策略与包过滤同时配置时，因为安全策略对报文的处理在包过滤之前，报文与安全策略规则匹配成功后，不再进行包过滤处理，所以请合理配置安全策略和包过滤，否则可能会导致配置的包过滤不生效。

1.8 安全策略规则的配置原则是什么？

配置安全策略时，请按照“深度优先”的原则（即控制范围小的、条件细化的在前，范围大的在后）进行配置。

1.9 配置安全策略时，需要注意什么？

配置安全策略前，请首先确认是否需要将设备上已存在的对象策略转换为安全策略，若需要，请务必先将对象策略转换为安全策略。因为首次进入安全策略视图后对象策略功能立即失效。

1.10 安全策略引用的对象组为空时，报文如何处理？

安全策略引用的地址对象组和服务对象组内容为空时，任何报文都不会匹配这条规则，报文会进行正常转发或丢弃取决于能否匹配上其他的安全策略规则、对象策略规格、包过滤规则。

1.11 在跨VLAN模式Bridge转发的应用场景中，安全策略怎么进行命中统计的？

在跨 VLAN 模式 Bridge 转发的应用场景中，策略匹配统计功能仅统计安全策略和内容安全丢弃的报文，不统计安全策略和内容安全允许通过的报文。

1.12 对新建或者新编辑的安全策略激活失败时，会影响原来已经激活生效的安全策略吗？

不会。

1.13 在多Context的应用场景中，安全策略的配置需要注意什么？

在多 Context 应用场景中，配置非缺省 Context 的内容安全业务前，必须先激活缺省 Context 的应用层检测引擎。可通过在缺省 Context 的安全策略页面单击<提交>按钮，激活缺省 Context 的应用层检测引擎。

1.14 安全策略引用的对象组内容发生变化时，也需要进行加速吗？

设备上的安全策略加速功能默认开启，且不能手动关闭。

安全策略规则中引用对象组的内容发生变化后，需要通过 **accelerate anhanced enable** 命令重新激活安全策略的加速功能。

1 安全域 FAQ

1.1 系统默认安全域有哪些？

目前，系统默认支持 Trust、Untrust、DMZ、Local 和 Management 这 5 个安全域。

1.2 管理口默认在哪个安全域中?

管理口默认在 Management 域，Local 域和 Management 之间默认是 permit 的。

1 ASPF FAQ

1.1 ASPF ICMP差错报文检测能够识别哪些ICMP差错报文？

当前识别的 icmp-err 的组合有下面这些：()中为 ICMP 报文的类型，[]中为 ICMP 的代码范围。

type	code
ICMP_UNREACH(3)	[0, 12]
ICMP_SOURCEQUENCH(4)	[0, 0]
ICMP_REDIRECT(5)	[0, 3]
ICMP_TIMXCEED(11)	[0, 1]
ICMP_PARAMPROB(12)	[0, 1]

1 PKI FAQ

1.1 PKI域下usage配置为何不生效？

PKI 域下缺省是未指定证书的扩展用途，表示可用于 IKE、SSL 客户端和 SSL 服务器端用途。usage 命令是用来指定证书的扩展用途，证书中携带的扩展用途与 CA 服务器的策略相关，申请到的证书中的扩展用途可能与此处指定的不完全一致，最终以 CA 服务器的实际情况为准。usage 命令在 PKI 域中不是必备项，如果出现 PKI 域下配置了 usage 但是未生效，请注意 CA 服务器颁发的证书的扩展用途。

1.2 使用PKI命令申请证书后，需要保存PKI的配置吗？

建议保存 PKI 配置。申请证书是个动作，PKI 命令和申请证书是配套的，证书申请后就直接保存下来了。若命令不保存的话，有可能会出现不配套导致功能异常。

1 应用识别 FAQ

1.1 APR和DPI其他业务的异同？

- 不同点：APR 分成 PBAR（Port Based Application Recognition，基于端口的应用层协议识别）和 NBAR（Network Based Application Recognition，基于内容特征的应用层协议识别）两部分。
- 相同点：NBAR 与应用层检测引擎有关，需要由应用层检测引擎进行检测。

1.2 NBAR支持哪些协议？

NBAR 支持 HTTP，TCP，UDP 协议的特征定义。

关于 HTTP 协议的 NBAR 特征定义：

```
[Sysname]nbar application body protocol http
[Sysname-nbar-application-body]signature 1 field ?
     Uri uri
     raw-uri raw-uri
     raw-body raw-body
     statusline  statusline
     raw-header raw-header
     raw-cookie raw-cookie
     raw-content raw-content
     stat-code stat-code
     stat-msg stat-msg
```

关于 UDP 协议的 NBAR 特征定义

```
[Sysname]nbar application uuu protocol udp
[Sysname-nbar-application-uuu]si
[Sysname-nbar-application-uuu]signature 1 ?
  hex Add a signature pattern in hexadecimal
  offset Add signature offset
  regex Add signature pattern by regex
  string Add signature pattern by string
```

关于 TCP 协议的 NBAR 特征定义，类似于 UDP 协议的特征定义。

1.3 PBAR是基于源端口还是目的端口的应用？

PBAR 是基于目的端口的应用识别，配置某个目的端口的 PBAR 后，经过该目的端口的消息流都被识别为该 PBAR 应用。该部分功能已经在 Web 上有所展现。

相关命令行如下：

```
[Sysname]port-mapping application {应用名} port 3000 ?
Acl      Specify acl filtering
Host     Specify a host range
Protocol  Specify a Layer 4 protocol
```

```
subnet    Specify a subnet
```

1.4 自定义的PBAR应用能设置最多可以配置多少端口

自定义的 PBAR 应用最多可以配置 1024 个端口。

1.5 NBAR的signature最多可以设置多少个？

NBAR 的 signature 最多可以设置 8 个。

1.6 PBAR可以配置TCP、UDP、DCCP、SCTP、UDP-Lite五种协议，在其他模块引用时，这几种协议是否都能识别？

PBAR 的这五种协议都是可以识别的，但是其它模块引用时，DCCP、SCTP、UDP-Lite 都是不生效的（比如 AVC 限速、域间阻断等）。

1.7 域间阻断配置阻断ftp-data报文，为什么不能阻断？

多通道的应用层协议报文（如 FTP、RTSP 等），设备上开启 ALG（Application Level Gateway，应用层网关）之后，会生成关联表，将控制通道和数据通道关联起来，当控制通道放行或阻断时，数据通道也一并放行或阻断。当配置了 DPI 之后，会默认开启多通道协议的 ALG，由于控制通道放行，所以数据通道就直接放行了，因此配置只阻断数据通道是不生效的。

1.8 PBAR与NBAR之间的优先级？

优先级关系：预定义 PBAR > 预定义 NBAR > 自定义 NBAR > 自定义 PBAR。

当配置设备拉起 DPI 模块时，对于打的测试流量，只要没有创建符合报文目的端口号的自定义 PBAR，应用识别功能通过 NBAR 实现；若配置了自定义 NBAR，若流中既存在符合预定义 NBAR 的特征字段，又存在符合自定义 NBAR 的特征字段，则系统判定识别结果为自定义 NBAR 的应用。

1.9 除DPI业务外，其他什么模块可触发NBAR检测？

- 安全策略中配置应用及应用组。
- 应用审计与管理；
- 带宽策略配置应用及应用组。

1.10 自定义应用、自定义NBAR、自定义PBAR的区别？

不论在 CLI 控制台还是 Web 下，对于自定义应用都是通过自定义 PBAR 与自定义 NBAR 创建的，当为某一应用创建了 port-mapping 或者 nbar application 后，自定义应用既被创建，可通过 **`display application user-defined`** 查看；值得注意的是，若一个应用既配了 port-mapping，又为其配了 nbar 的相关特征，仅删除其中一条 PBAR 或 NBAR，该应用还是会存在，要将 port-mapping 与 nbar application 同时删除才可以彻底删除此应用。

1.11 PBAR一对多，多对一的关系

(1) 对于同一个自定义应用，可以为其配置多条对应目的端口号

举例：设 app 的名字=shr，shr-123,shr-456，故目的端口号为 123 和 456 的流都会将应用识别为 shr

(2) 但多个自定义应用不可同时匹配同一个目的端口号，若配置 **`port-mapping application app1 port 123`**，则再配置 **`port-mapping application app2 port 123`** 的时候，前一条映射关系会被自动替换删除。

1.12 如何配置阻断某个特定应用，但放行其他所有应用？比如QQ应用

举例，如 QQ 应用进行阻断，其他应用放行。可以先配置一条安全策略绑定 QQ 应用动作为阻断，再配置一条安全策略动作为允许放行其他所有应用。

1 应用层检测引擎 FAQ

1.1 规格中关于内存门限后，DPI尽力检测，怎么理解?

DPI 的报文处理流程中，需要申请内存。但是何时申请内存是不一定的，这跟所处理的报文具体在这条流中的先后顺序、报文载荷内容相关，并不是每个报文的处理都会涉及内存的申请。但是每条流的处理必然有申请新的内存(DPI 基于流处理)。内存门限后，软件不会再向系统申请新的内存，但是 DPI、Session 软件实现时，都有一个小的内存缓存池，可以支撑一少部分流量的处理(老会话的删除，给新会话的建立腾出了资源)。内存门限后，可能大部分新的流量都会因为内存申请失败而不做 DPI 检测了，应用层检测引擎会尽可能的利用已有的资源去检测报文。对于新老会话而言，一定条件下都是可能进行 DPI 检测的，一概而论，内存门限下进行 DPI 检测或者不进行 DPI 检测都是不准确的。

1.2 为什么我能通过邮件发送病毒而不被检测?

DPI 对于编码的识别能力是有限的，目前仅支持 base64，qp，百分号解码方式。对于经过压缩的报文，DPI 仅支持 gzip 方式的压缩报文。DPI 本身并没有解密的功能，因此对于加密报文，DPI 同样无法识别。而邮件基础编码方式一般为 7bit，DPI 是无法识别的。

1 应用审计与管理 FAQ

1.1 应用审计和应用识别的区别？

应用审计与管理是在 APR（Application Recognition，应用层协议识别）的基础上进一步识别出应用的具体行为（比如 IM 聊天软件的用户登录、发消息等）和行为对象（比如 IM 聊天软件登录的行为对象是账号信息等），据此对用户的上网行为进行审计和记录。

应用审计和应用识别都是使用应用识别特征库，但出厂的应用识别特征库 1.0.0 不支持审计

安装 APR license 后升级应用识别特征库到最新版本即可使用应用审计。

1.2 应用阻断使用域间阻断还是审计阻断呢？

针对应用的具体行为进行阻断请使用审计，如果针对应用所有行为时使用安全域阻断即可。

1.3 审计阻断有何缺陷？

审计微信或者 QQ，登录以后，审计阻断发\收消息以及语音时无法正常阻断；由于登录流和发\收消息以及语音的流量是同一条长连接流量，登录已经成功无法再阻断发\收消息以及语音。

1.4 审计规则的两种匹配模式有何区别？

审计规则的匹配模式分为顺序匹配和全匹配两种，不同模式下审计规则的匹配原则如下：

- 顺序匹配：按照审计规则 ID 从小到大的顺序进行匹配，一旦报文与某条审计规则匹配成功便结束此匹配过程，并根据该审计规则中的动作对此报文进行相应处理。
- 全匹配：按照审计规则 ID 从小到大的顺序进行匹配，若报文与某条动作为允许的规则匹配成功，则继续匹配后续规则直到最后一条；若报文与某条动作为阻断的规则匹配成功，则不再进行后续规则的匹配。设备将根据所有匹配成功的审计规则中优先级最高的动作（阻断的优先级高于允许）对此报文进行处理。

1.5 审计规则匹配的关键字组最大配置多少？

关键字组最大配置 64 条。

1 数据过滤 FAQ

1.1 为什么使用百度搜索时，搜索结果无法过滤？

因为百度使用的是 TLS 加密的报文（抓包可以看出），此时需要通过开启 ssl 卸载实现数据过滤。

1.2 为什么更改了数据过滤策略或关键字组后，无法按照配置的内容过滤关键字？

每次更改数据过滤策略或者关键字组后，都需要点击“配置激活”按钮（或者命令行上执行 **`inspect activate`**），点击之后，更改的配置才会激活生效。

1.3 我想要过滤一个网页，阻止对其的访问（对应配置为**action drop logging**），为什么完全按照上述配置配完后，网页还是能够正常打开？

这种情况是由于浏览器缓存引起的，清空浏览器缓存后，就能正确过滤网页了。

1.4 关键字组下可以配置多个pattern，多个pattern是怎么匹配的？

pattern 之间是或的关系，即只要匹配任意一个，就算整个关键字组匹配上。

1.5 为什么我无法阻断论坛上传的中文内容？

有些论坛和新浪微博等上传中文时使用的是 URL 编码方式，数据过滤不支持该编码方式。

1.6 为什么我配置的包含中文的正则表达式无法生效？

中文不支持正则表达式方式匹配。当正则表达式中包含中文时，只能对上传该配置时的编码方式生效，因此当配置包含中文的正则表达式时可能会无法生效。

1 数据分析中心 FAQ

1.1 数据分析中心提供什么业务？

DAC（Data Analysis Center，数据分析中心）提供了业务日志信息的数据挖掘和可视化展示服务。它支持日志信息存储与分析、流量监控和报表分析功能，可帮助用户清晰地了解业务流量分布情况以及网络安全现状，为用户制定各业务策略提供了有力的数据支持。

1.2 数据分析中心支持的存储介质？

数据分析中心的日志数据不仅仅支持设备本身的 flash 方式存储，同时还支持硬盘和 U 盘外部存储介质，存储顺序为硬盘、U 盘、flash，即优先存储硬盘，无硬盘或者硬盘无存储空间时存储 U 盘，无 U 盘或者 U 盘无存储空间时存储 flash。另外，存储空间达到存储介质的 80%时，设备会发送告警日志。设备重启时，硬盘和 U 盘的存储数据不丢失。

1.3 数据分析中心配置限制和指导？

数据分析中心的结果展示功能仅在 Web 管理方式下支持。CLI（Command Line Interface，命令行接口）管理方式下仅提供相关参数的配置功能，不提供任何分析结果展示功能。

硬盘和 U 盘支持热插拔，但建议拔出外部存储介质前，配置硬盘卸载功能后，再手动拔出存储介质。

1 WAF FAQ

1.1 WAF和IPS的区别

WAF 是针对 Web 页面的防护，除了针对 Web 的攻击防护外，还有针对一些异常操作（如高频登录）的防护；总的来说与 IPS 功能有重叠部分也有明显区别，所以如果同时引用了 IPS 策略和 WAF 策略，部分攻击会命中两个策略。

1.2 在域间引用了WAF策略，为什么无法命中？

初步认为有两个原因：

(1) 首先查看设备有无 License，若无 License 设备则无法正常命中 WAF；

(2) WAF 的命中规则没有下发到应用层检测引擎内核，在安全策略中引用 WAF 策略以后，下发配置生效，设备会将引用的 WAF 策略的规则下发到应用层检测引擎内核；若 WAF 规则未能正常下发，应用层检测引擎内核中没有 WAF 的命中规则，当设备接收到攻击报文时，没有对应的规则命中匹配，攻击报文也就无法正常匹配了。

1.3 引用了WAF策略，进行攻击，为什么威胁日志中没有日志？

目前 WAF 还不支持在 Web 页面上查询日志，需要在系统 > 日志设置 > Web 应用防护日志中勾选输出 Web 应用防护快速日志，然后在系统 > 日志设置 > 基本配置 > 快速日志中配置日志主机并勾选 Web 应用防护日志，在日志主机上查看日志。

1.4 如果攻击同时命中WAF策略和IPS策略，如何处理？

如果攻击同时命中例 WAF 和 IPS 策略，则两个策略都会报日志，报文会按照两者中较为严格的一个动作来处理，动作顺序为丢弃 > 重置 > 重定向 > 允许。

1 AFT FAQ

1.1 同一接口下能同时做AFT和NAT地址转化吗?

不能，做了 AFT 就不会再做 NAT 了。

1.2 IPv6网络访问IPv4网络进行目的地址转换时，支持多对一的目的地址转换吗？

不支持，只支持一对一目的地址转换。

1 SSL 卸载（SSL 解密）FAQ

1.1 SSL卸载功能组网需要注意什么？

SSL 卸载功能目前只支持三层组网模式，二层组网不生效，Bridge 等接口对组网方式均不生效。

1.2 SSL卸载配置需要注意什么？

安全策略中源/目的安全域除绑定接口所在安全域外，还需要源安全域配置 Local 域。

1.3 如何判定一次访问是否经过了SSL卸载？

判定一次访问是否经过了 SSL 卸载的简单方法是，查看当前浏览器上显示的证书信息。不同浏览器查看证书的方法不同，一般都是在界面地址栏挂锁的地方，单击查看下拉菜单。如果一次 HTTPS 访问经过了 SSL 卸载，“颁发者”字段会被替换为设备中导入的解密证书的主题（“颁发给”字段）。

1.4 如何判定一次访问是否加入了IP地址白名单？

在 cmd 窗口中，ping 一下当前访问的域名，获得服务器的 IP 地址，通过 **display app-proxy ssl whitelist ip all** 命令，查看显示的列表中是否包含了该 IP 地址。如果包含，则说明本次 HTTPS 连接的服务器地址被加入了 IP 地址白名单。

1.5 如何判定一次访问是否匹配了域名白名单？

- 在当前访问的浏览器窗口获取证书信息，打开详细信息标签页，首先查看该证书是否有“使用者备用名称”，如果有，那么这里所列的第一条 DNS Name 就是当前证书的域名信息，如果没有，继续查看证书的“使用者信息”，这里“CN=”后面的内容是域名信息，也就是说 DNS Name 优先于 Common Name(CN)字段作为证书的域名。
- SSL 卸载的域名白名单对证书域名是模糊匹配的，只要证书域名包含白名单中的字符串，即认为匹配。可通过命令行 **display app-proxy ssl whitelist hostname predefined** 或者 Web 页面“策略 > 应用代理 > 白名单 > 预定义白名单”来查看域名白名单信息。

1.6 如何去使能域名白名单？

为保证去使能后流量不再走 IP 地址白名单，需要严格按照如下步骤操作：

(1) 通过命令行 **undo app-proxy ssl whitelist predefined-hostname** 去使能域名，或者在 Web 页面直接勾选域名进行禁用。

(2) 使用 **app-proxy ssl whitelist activate** 或者单击 Web 列表上的<提交>按钮，进行配置激活。

(3) 使用命令行 **reset app-proxy ssl whitelist ip** 清除所有 IP 地址白名单。

1.7 如何判定一次访问是双向代理？

- 服务器双向代理，SSL 卸载功能不支持卸载。
- 在设备或 PC 侧抓包，查看 SSL 握手过程，如果服务器侧发过 Certificate Request,则说明此次 HTTPS 连接是双向代理的。

1 共享上网管理 FAQ

1.1 共享上网管理的检测方法是什么？

共享上网管理分为两种检测方法：

- 应用特征检测方法：

  在 APR 的基础上，根据内置的特征库，提取一些应用的特征来计算一个主机下的终端数量。当用户使用我们提取的应用时，流量通过设备，我们提取出账号、cookie 等信息，计算该主机下终端数量，并判断是否存在共享上网行为。

- IPID 轨迹检测方法：

  IPID 指的是 IP 报文首部的标识域，长度为 16bit，用来唯一标识一个 IP 报文。同一主机发出的 IPID 字段是连续变化且呈递增趋势，根据这一规律，如果在一段时间内，检测到某个源 IP 对应多个 ID 字段范围，则说明该 IP 对应的用户为共享接入用户，根据 IPID 字段区间个数能够大致确定共享接入主机的数目。

1.2 共享上网管理模块的使用限制？

- 如果不开 IPID 检测，那么只有当终端上有这些应用时，设备能识别（这种方法是基于应用来识别，配合审计功能做的），如果没有这些应用，在不开启 IPID 的情况下，是检测不出终端的。QQ，微信，微博，百度贴吧，大众点评，美团 cookie，58cookie，HTTP 报文的 useragent。
- 每个应用有一个权值（由于一台终端可能有多个应用，比如开发设计的时候，认为 QQ 一般可能会有两个，微信一般只有一个，所以设置了 QQ 的权值为 50%，微信的权值为 80%），通过数量×权值，然后向上取整。比如现在检测到终端有 5 个 QQ、2 个微信登录，那终端数量为 max[5*50％，2×80％]＝2.5，向上取整数量为 3。这种检测方法是通过经验判断，然后设置的权值，因此结果不够精确。
- 开启 IPID 轨迹检测后，设备性能会下降。
- IPID 轨迹检测仅限于 PC 端检测，无法检测移动终端（如手机，因为移动终端的 IPID 轨迹不连续）。

1 内网安全综合评分（安全概况）FAQ

1.1 内网安全综合评分的主要目的是什么？

平台目前缺乏直观展示内网安全状态的功能。为满足需求，数据分析中心后台则需要利用存储的威胁日志数据，得到四类威胁程度类型的个数，然后计算出安全评分，一并返回给 Web 进行展示；其中安全评分反应内网总体安全状态，四类威胁程度类型的次数统计则反应具体的得分细节，从而使 Web 界面能直观地展现安全元素以及实时地显示网络安全情况（如界面呈现近日受攻击的类型、次数等，对于网络安全状况实现整体打分）。

1.2 内网安全综合评分的实现原理是什么？

数据分析中心后台需要提供：

(1) 内网安全评分计算；

(2) 不同威胁等级攻击次数统计。

需求的实现分析如下：

(1) 需增加一个 netconf 表，Web 需下发一个计算类型参数（枚举值，为以后评分计算功能可能出现的扩展预留，目前只需下发 0）；后台返回计算得到的综合评分以及各威胁级别对应的次数，其中各威胁级别对应的次数封装在 JSON 格式中，Web 需要对其进行解析，得到不同类别的数据，然后在网页上展示分布情况；

(2) 根据下发的类型的不同，采用回调函数的方式来实现数据的查询处理，便于以后可能出现的新需求造成的修改；

(3) 拼装 SQL，然后对本 Context 数据进行查询。目前威胁日志以天为单位，存储在不同的数据库中，后台设定的时间段为一小时，所以只会出现在一天内与跨一天的两种情况，但为了应对以后时间段可能会修改为超过一天的情况，采用分别对时间段内的所有数据库进行查询的方法，然后将不同威胁等级的结果分别相加，最后得到总的结果；

(4) 在 SQL 执行完得到符合条件的不同威胁等级对应的条数后，根据如下公式计算安全评分：

安全评分 = 起评分–攻击危险指数；

攻击危险指数 = 威胁日志中不同攻击程度对应的分值总和；

目前 IPS 与防病毒模块生成的威胁日志统一存储在数据分析中心数据库，威胁日志中的严重程度来自于特征库的匹配结果，数据分析中心根据该字段对严重级别进行判定，判定方法与应用层检测引擎、IPS 等模块的已有的判定方法保持一致。

其中威胁日志中的威胁严重程度（**Severity**）为 UINT 型的数据，其与威胁级别和分值的对应关系为：

- Severity<30：低，对应分值 0.2；
- 30<=Severity<60：中，对应分值 0.4；
- 60<=Severity<90：高，对应分值 0.6；
- 90<=Severity：严重，对应分值 4；

注意

- 如果有严重攻击，则从 70 起评。
- 如果有高危攻击，则从 90 起评。
- 如果安全评分计算结果小于 10，则设置为 10。
- 目前威胁日志中的严重程度只会出现 0~100 的情况，若出现异常产生大于 100 的情况，则处理为严重。

(5) 评分计算完后将不同威胁级别次数的数据封装到 JSON，同安全评分一起返回给 Web（对于安全评分的解读由 Web 进行实现）。

1.3 安全评分的计算公式是什么？

公式为：Score = Total －Low*0.2-Medium*0.4-High*0.6- Critical*4;

- 当 Critical>0 时,Total = 70;
- 当 Critical=0,High>0 时，Total = 90;
- 当 Critical=0，High=0 时，Total = 100；
- 最后对 Total 取整；
- 得到 Total<10 时，取 Total 为 10；

1.4 为什么我的设备Web界面没有安全概况的安全评分？

目前，只有 F1010 系列的设备才能显示安全概况的评分模块。

1 Web 操作 FAQ

1.1 为什么进行了版本的升级或者降级的操作后，登录Web的时候，有时Web页面的显示与当前版本不一致？

浏览器存在缓存机制，会将设备上请求过的文档进行存储来加速浏览，当访问者再次请求这个页面时，浏览器可以从本地磁盘显示文档。这样造成的问题是，当设备版本升级后，当前缓存的文件并不一定与设备上的页面一致，所以需先清除缓存使浏览器重新从设备上请求文档，保证设备侧与本地一致。

1.2 为什么设备转发了流量，Web流量日志、流量统计页面为空白？

流量日志、流量统计功能需要开启会话统计 **session statistics enable**。

1.3 流量监控是为什么有时候显示为空白，为什么没有实时更新？

没有开启自动刷新功能。需要手动点击刷新按钮，或者开启自动刷新功能。

每个小模块右上角都有设置按钮，可以开启自动刷新功能，配置自动刷新的时间间隔 10-180 秒。