Web 登录与简介

- 为了保证设备安全性，请在初次登录完成后，修改登录密码。
- Web 界面提供了对设备常用业务功能的配置支持，但并不包含所有功能。若需更详细的功能配置，请参考《配置指导》使用命令行进行操作。



- 本文档中介绍的部分功能或参数的支持情况与设备型号有关，请以设备实际情况为准。本文档中的界面截图仅供参考，不同设备型号或版本的界面可能存在差异，具体情况请以设备上显示的内容为准。
- 本文档主要根据 Web 界面的菜单结构介绍配置方法，完整的配置案例请参阅《典型配置案例集》。

登录Web

对浏览器和操作系统的要求

- 建议使用以下浏览器访问 Web：Chrome 40 及以上版本、Firefox 19 及以上版本、Internet Explorer 10 及以上版本。

- 使用的浏览器必须要设置能接受第一方 Cookie（即来自站点的 Cookie），并启用活动脚本（或 JavaScript），才能正常访问 Web。以上功能在不同浏览器中的名称及设置方法可能不同，请以实际情况为准。
- 使用 Internet Explorer 浏览器时，还必须启用以下两个功能，才能正常访问 Web：对标记为可安全执行脚本的 ActiveX 控件执行脚本、运行 ActiveX 控件和插件。
- 更改设备的软件版本后，建议在登录 Web 页面之前先清除浏览器的缓存，以便正确地显示 Web 页面。
- 设备缺省采用 gb18030 编码格式，为确保通过 CLI 配置的中文字符在 Web 页面上正常显示，管理员在 CLI 窗口输入中文时应确保使用 gb18030 编码格式。

初次登录 Web

设备支持 HTTP（Hypertext Transfer Protocol，超文本传输协议）和 HTTPS（Hypertext Transfer Protocol Secure，超文本传输协议的安全版本）两种 Web 访问方式。

设备出厂时已经缺省启用了 HTTPS 服务，并且设置有缺省的 Web 登录信息，用户可以直接使用缺省登录信息通过 HTTPS 服务登录设备的 Web 界面。

采用缺省登录信息 Web 登录设备的步骤如下：

1. 连接设备和 PC

用以太网线将 PC 和设备上的以太网口相连。

2. 为 PC 配置 IP 地址，保证其能与设备互通

   将 PC 的 IP 地址设置为与设备 IP 地址在同一个网段。

3. 启动浏览器

   在 PC 上启动浏览器，在浏览器的地址栏中输入设备管理接口的 IP 地址，然后回车，进入设备的 Web 登录页面。

4. 输入登录信息

   在登录页面中输入设备缺省用户名和密码，在下拉列表中选择登录语言，单击<登录>按钮。

5. 修改登录信息

   首次登录时，设备会自动弹出“修改密码”窗口，强制要求用户修改为复杂度更高的密码，以提高安全性。密码修改完成后，单击<确定>按钮即可登录设备 Web 页面。

   登录设备后，可以进入“接口”页面修改设备的 IP 地址；还可以进入“管理员”页面创建新的用户，以方便对设备进行管理。

退出 Web

为保证设备的安全性，用户在 Web 上完成操作后应及时退出登录。

在 Web 页面上单击右上角的“  ”，在下拉列表中选择“退出登录”，即可退出 Web。

需要注意的是：

- 退出 Web 时，系统不会自动保存当前配置。因此，建议用户在退出 Web 前先单击页面右上方的“ ”，或进入“系统 > 系统与维护 > 配置文件”页面保存当前配置。
- 直接关闭浏览器不能使用用户退出 Web。

如何使用Web

Web 页面布局介绍

图-1 Web 页面布局



（1）标识和面板区	（2）导航栏	（3）执行区	（4）CLI控制台

如上图所示，Web 页面有以下几个功能区域：

- 标识和面板区：该区域用来显示公司 Logo、设备名称、功能面板、当前登录用户信息，并提供更改登录用户密码、保存当前配置、退出登录功能。单击“”，可以在下拉列表中退出登录、修改密码或者切换到指定的虚拟系统；单击“”，可以保存当前配置；单击“”可以打开整本联机帮助。
- 导航栏：以树的形式组织设备的 Web 功能菜单。用户在导航栏中可以方便的选择功能菜单，选择结果显示在执行区中。用户也可以在导航栏的顶端输入要查询的菜单名称，然后单击“”或者回车后，可以快速定位到目标菜单。
- 执行区：进行配置操作、信息查看、操作结果显示的区域。
- CLI 控制台：单击“CLI控制台”，可从 Web 页面跳转到 CLI 控制台窗口，方便管理员使用 CLI 命令方式对设备进行管理。

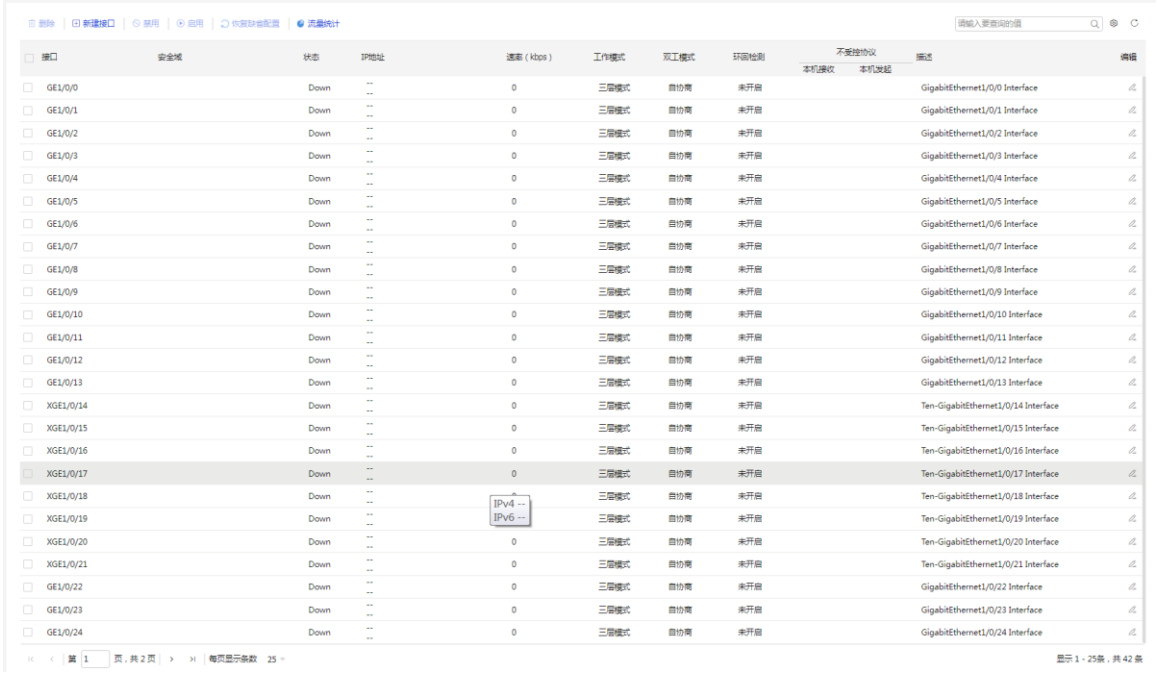
Web 页面分类

根据执行区内容的不同，Web 页面分为表项显示页面和配置页面。

表项显示页面

如图-2 所示，表项显示页面用来显示表项的具体信息。单击标题项右侧的下拉三角“”，可以根据该标题项对表项信息进行正序或倒序排列，也可以定制当前页面的显示列。

图-2 表项显示页面示意图



配置页面

如图-3 所示，配置页面用来完成某项配置任务，如添加、修改一条表项。某项配置任务需要的所有配置均可在该页面上完成，不需要在页面之间跳转，以方便用户使用。

图-3 配置页面示意图



Web 常用操作

Web 页面上常用的操作包括快捷入口、保存当前配置、显示表项详情、重启设备等。

快捷入口

快捷入口功能让您能够更快捷、更高效地访问常用的菜单和功能，省去了在多个页面之间反复查找的时间。

1. 单击“  ”按钮，进入“快捷入口”页面。
2. 编辑快捷入口：您可以通过搜索轻松找到并添加菜单至快捷入口，也可以根据个人需求随时添加或移除快捷入口中的菜单项。
3. 快速访问：添加到快捷入口的菜单将在“快捷入口”页面中直接显示。下次使用时，您无需再层层导航，只需一次点击即可直达目标功能。

保存当前配置

对设备执行配置操作后，建议及时保存当前配置，以免配置丢失。保存当前配置的方法有以下两种：

- 单击页面右上方的“  ”。
- 进入“系统 > 系统与维护 > 配置文件”页面，单击<保存当前配置>按钮。

重启设备

执行某些操作（如配置 IRF）后，需要重启设备才能使配置生效。重启设备的方法为：进入“系统 > 系统与维护 > 重启”页面，单击<重启设备>按钮。

在重启设备前，建议先保存当前配置，以免配置丢失。

页面搜索栏

页面搜索栏能够帮助用户快速定位所需页面，提高查找效率。用户只需输入关键字，系统便会自动查找并显示所有包含该关键字的页面路径。单击搜索结果，即可直接跳转至目标页面。

登录 CLI 控制台

当管理员需要通过命令行管理设备时，可以通过此方法快速进入 CLI 控制台窗口。

登录 CLI 控制台的方法为：进入任意页面，单击 “ CLI控制台 ”。



当CLI控制台连接失败时，可能是由以下问题导致：

- 使用不支持本功能的浏览器，建议使用谷歌浏览器或火狐浏览器
- 使用的浏览器版本过低，建议升级至最新版本
- 设备的连接数达到上限
- PC 配置了代理服务器，且配置了访问设备时仅对 HTTP 和 HTTPS 协议不使用代理服务器

Web页面导航

用户登录 Web 后，能够看到的页面导航内容、能够执行的操作与该用户的用户角色有关。所有配置操作的缺省用户角色要求为 network-admin 或 context-admin。查看操作的缺省用户角色为所有角色。

用户角色为 network-admin 或 context-admin 的用户登录后，单击面板，会在左侧导航栏显示对应的一级菜单，子菜单由分类和特性名称组成。依次单击“一级菜单 > 二级菜单 > 特性名称”可以进入相应的 Web 页面对该特性进行配置。

常用操作介绍

设备 Web 页面是管理员与设备之间的交互界面，允许管理员执行多种管理和配置操作。本文档旨在详细介绍设备 Web 页面中的常见操作，帮助管理员快速了解和掌握这些操作的使用方法。

<确定>和<取消>

在配置页面下方，常见<确定>和<取消>按钮：

- <确定>：参数配置完成后，可通过单击<确定>按钮，使配置生效。
- <取消>：可通过单击<取消>按钮，取消未生效的配置。

<应用>

<应用>按钮用于将所选的配置项应用到相应的设备或系统中。管理员在完成配置后，可以通过单击<应用>按钮，使配置生效。

<新建>和<删除>

配置列表页面的操作行中，常见<新建>和<删除>按钮：

- <新建>：可通过单击<新建>按钮，打开新建页面，增加一条新的配置。
- <删除>：选中待删除的配置后，可以通过单击<删除>按钮，删除该配置。

<启用>和<禁用>

配置列表页面的操作行中或列表中，常见<启用>和<禁用>按钮。两个位置的按钮含义不同：

操作行

- <启用>：选中待启用的对象后，通过单击<启用>按钮，可以使该对象的状态变为启用状态。
- <禁用>：对于已经处于启用状态的对象，可通过单击<禁用>按钮，使该对象的状态变为禁用状态。

列表中

在列表中，若显示启用/禁用，表示某功能或对象当前的状态。

- <启用>：表示某功能或对象当前处于启用状态。若单击<启用>按钮，则使该对象的状态变为禁用状态。
- <禁用>：表示某功能或对象当前处于禁用状态。若单击<禁用>按钮，则使该对象的状态变为启用状态。

除了启用状态和禁用状态，部分功能还有其他的中间状态。详细内容请参见具体特性介绍。

<复制>

<复制>按钮通常用于需要新建类似配置。

首先，需要选中待复制的配置，一次只能选中一行配置；然后，单击<复制>按钮，设备会基于选中的配置，新建一模一样的配置；管理员可对复制的配置进行编辑，从而省去大量的重复配置。

<插入>

<插入>按钮用于在列表页面的指定位置添加新的配置项。

管理员可以在列表中选择插入位置，然后单击<插入>按钮，选择插入的位置，系统将在选定位置插入一行新的配置项或打开一个配置页面。管理员可以在新行或页面中输入所需的配置参数，以创建新的配置项。通过使用<插入>按钮，管理员能够灵活地在现有配置中添加新的配置项。

<移动>、<上移>和<下移>

<移动>、<上移>和<下移>按钮用于在配置列表页面中调整配置项的顺序，

- <移动>按钮可能包括上移、下移、移动到最前、移动到最后和移动到指定位置。管理员可以在列表中选择需要调整位置的配置项，然后单击<移动>按钮，选择插入的目标位置。此操作允许管理员根据需要重新排列配置项，以便更好地组织和管理配置列表。
- <上移>按钮用于在配置列表页面中将选定的配置项向上移动一行。
- <下移>按钮用于在配置列表页面中将选定的配置项向下移动一行。

通过使用<移动>、<上移>和<下移>按钮，管理员可以灵活地优化配置顺序。

<统计>、<取消统计>和<清空统计数据>

配置列表页面的操作行中，常见<统计>、<取消统计>和<清空统计数据>按钮，用于进行数据统计和分析：

- <统计>：在配置列表页面中，管理员需要先选中配置项（例如，特定的策略），然后单击<统计>按钮。系统将允许管理员设置统计的时间范围，随后生成该策略相关的统计信息。此功能帮助管理员深入分析配置项的使用情况，评估其效果，从而优化策略或进行调整。
- <取消统计>：如果管理员希望停止当前的统计操作，可以单击<取消统计>按钮。此操作将取消已进行的统计请求。

- <清空统计数据>：通过单击<清空统计数据>按钮，管理员可以清除已生成的统计结果及相关数据。清除后，管理员可以重新进行统计，以获取最新的数据分析结果。

<导入>和<导出>

配置列表页面的操作行中，常见<导入>和<导出>按钮：

- <导入>：通过单击<导入>按钮，选择要导入的本地配置文件、日志文件、统计数据文件等，可将配置、日志及统计数据批量导入设备。
- <导出>：通过单击<导出>按钮，可将部分或全部已生效的配置、日志或统计数据导出到本地备份，也可以导出配置模板。管理员根据配置模板输入配置后，再批量导入设备中。

<刷新>和<自动刷新>

配置列表页面的操作行中，常见<刷新>和<自动刷新>按钮：

- <刷新>：通常在无法自动获取到最新配置、状态或统计数据时，单击<刷新>按钮可使当前页面更新至最新。
- <自动刷新>：用于设置页面的自动更新功能。当管理员启用此功能后，系统将根据预设的时间间隔（例如每隔 10 秒钟）自动获取并更新列表中的最新数据、状态或统计信息。

<清除>

配置列表页面上方的操作行中，常见<清除>按钮，通常用于清除数据。包括：

- 清除选中数据：需要先选中待清除的数据，然后单击<清除>按钮，选中数据将会被清除。
- 清除全部数据：单击<清除>按钮，或者选中所有数据后单击<清除>按钮，当前页面的所有统计数据均会被清零。

<查询>和<过滤器>

<查询>和<过滤器>按钮都是用来对当前页面进行筛选：

- <查询>：通过在<查询>按钮左侧的输入框中输入或选择查询条件，然后单击<查询>按钮，可显示出符合查询条件的条目。若清空输入框中的内容，列表会恢复显示所有条目。
- <过滤器>：过滤器功能适用于查询条件更为复杂的场景，可同时自定义多个过滤条件。管理员可通过单击列名右侧的<过滤器>按钮，在“过滤器”输入框中输入过滤条件，单击<确定>按钮。通过在不同列的“过滤器”中输入过滤条件，列表中会显示同时符合多个过滤条件的条目，过滤条件会显示在列表上方。通过单击过滤条件右侧的<X>，可以关闭指定的过滤条件。

列定制

在运行概览、日志信息或配置列表等列表页面，管理员可根据需求定制显示列，仅显示关注的列，隐藏不关注的列。

单击列表页面操作行右侧的“  ”，可以展开当前列表页面支持的所有显示列，管理员根据需求选择显示列即可。

概览

本帮助主要介绍以下内容：

- 特性简介
  - 运行监控—设备状态图
  - 运行监控—系统日志
  - 运行监控—系统流量统计
  - 运行监控—系统会话统计
  - 运行监控—系统新建速率统计
  - 运行监控—系统信息
  - 运行监控—丢包会话统计
  - 运行监控—上网行为监控
  - 运行监控—License 信息
  - 运行监控—接口信息
  - 流量监控—流量实时用户排行
  - 流量监控—流量实时应用排行
  - 威胁监控—安全概况

    - 威胁监控—威胁排行
    - 威胁监控—安全状态
    - 威胁监控—风险主机 Top10
    - 安全监控—安全分析
    - 安全监控—安全能力
- vSystem 相关说明

特性简介

概览页面通过图形化模块清晰展示了设备关键数据信息及各类状态，并支持灵活排版布局，以便管理员可以实时查看关心的数据。预定义监控默认展示了设备基础信息模块，也可以手动添加其他模块。管理员还可以新建自定义选项卡，并在自定义选项卡中手动添加模块。安全监控展示了业务和用户安全统计数据、设备关键数据信息以及各类流量和会话的统计数据等，不支持定制显示模块。

如下各模块的支持情况与设备型号有关，请以设备实际情况为准。

运行监控—设备状态图

设备状态图模块用于查看设备 CPU、内存和 Flash 的资源利用率。单击<详细信息>按钮，进入“系统利用率”页面，可查看设备状态、类型、软件版本等信息并进行告警设置。

设置的告警门限包含以下两种类型，管理员可根据设备的实际情况设置告警门限值：

- 设置 CPU 阈值：系统每隔 1 分钟会对 CPU 的利用率进行采样，并将采样值和用户配置的 CPU 利用率阈值/CPU 利用率恢复阈值比较：
  - 当采样值大于或等于 CPU 利用率阈值时，则认为 CPU 利用率过高。
  - 当采样值回落，小于或等于CPU利用率恢复阈值时，则认为CPU利用率已经恢复到正常范围。

  当 CPU 利用率从过高变成正常或者从正常变为过高，均会发送 Trap 报文，并通知业务模块进行相应处理。
- 设置空闲内存告警门限值：系统实时监控系统剩余空闲内存大小，当条件达到一级、二级、三级告警门限或者恢复正常状态门限时，就产生相应的告警/告警解除通知，通知关联的业务模块/进程采取相应的措施，以便最大限度的利用内存，又能保证设备的正常运行。一级（**minor**）、二级（**severe**）和三级（**critical**）门限，对应的系统剩余空闲内存越来越少，紧急程度越来越严重。
  - 当剩余空闲内存值从大于变成小于一级告警门限时，产生一级告警。
  - 当剩余空闲内存值从大于变成小于二级告警门限时，产生二级告警。
  - 当剩余空闲内存值从大于变成小于三级告警门限时，产生三级告警。
  - 当剩余空闲内存值从小于变成大于二级告警门限时，产生三级告警解除通知。
  - 当剩余空闲内存值从小于变成大于一级告警门限时，产生二级告警解除通知。
  - 当剩余空闲内存值小于变成大于正常内存大小时，产生一级告警解除通知。

同一级别的告警/告警解除通知是交替进行的：当系统剩余空闲内存小于某级告警门限，设备产生相应级别的告警，后续只有该告警解除了，系统剩余空闲内存再次小于某级告警门限时，才会再次生成该级别的告警。

当设备出现内存告警时，可删除暂时不用的配置或关闭部分功能来释放内存。但因为内存不足，部分配置可能删除失败。

运行监控—系统日志

系统日志模块记录了设备在运行过程中产生的相关日志信息，且仅展示 Error 以上级别的日志内容。

可单击<详细信息>按钮，查看所有级别日志的详细信息，方便管理员分析设备运行状况，为故障诊断和维护提供依据。

运行监控—系统流量统计

系统流量统计页面通过折线图的方式展示过去一段时间内流入和流出设备的流量统计结果。方便管理员通过查看流量的高峰和低谷时间以及速率等流量分布规律，分析网络状况。

管理员可单击<设置>按钮，配置统计时间、类型和接口等参数，筛选出所需的统计内容。

单击<详细信息>按钮，可查看各个接口的详细流量统计信息。

运行监控—系统会话统计

系统会话统计模块用于查看最近一段时间内系统新建的会话个数。单击<详细信息>按钮，进入“系统会话统计详情“页面，可查看最近一小时、一天和三十天的新建会话个数。

- 单击<详细信息>按钮，进入“系统会话统计详情“页面，可查看最近一小时、一天和三十天的新建会话个数。
    - 单击<开启 Top10 统计>按钮，设备将对基于会话的业务进行会话数目统计，分别基于源地址和目的地址对新建会话数目进行排序。
    - 单击<查看 Top10 统计>按钮，将进入“Top10”页面，管理员可选择查看“最近一小时”、“最近一天”或者“最近三十天”的“按源地址统计”或者“按目的地址统计”的排名信息。
- 单击<刷新>按钮，可刷新展示数据，查看当前最新统计数据。
- 单击<设置>按钮，进入“设置”页面，可勾选“启用自动刷新”开启自动刷新统计数据功能，并可设置自动刷新的时间间隔。

运行监控—系统新建速率统计

系统新建速率统计模块用于查看最近一段时间内系统新建会话的速率。单击<详细信息>按钮，进入“系统新建速率详情“页面，可查看最近一小时、一天和三十天的会话新建速率。

- 单击<详细信息>按钮，进入“系统新建速率详情“页面，可查看最近一小时、一天和三十天的会话新建速率。
    - 单击<开启 Top10 统计>按钮，设备将对基于会话的业务进行会话新建速率统计，分别基于源地址和目的地址对新建会话速率进行排序。
    - 单击<查看 Top10 统计>按钮，将进入“Top10”页面，管理员可选择查看最近一段时间内系统新建会话总数和平均新建速率的前十名排行信息。
- 单击<刷新>按钮，可刷新展示数据，查看当前最新统计数据。
- 单击<设置>按钮，进入“设置”页面，可勾选“启用自动刷新”开启自动刷新统计数据功能，并可设置自动刷新的时间间隔。

运行监控—系统信息

系统信息用于查看设备名称、设备型号、软件版本和运行模式等设备信息。并可通过单击右侧的<设置>按钮，对部分信息进行配置。

运行监控—丢包会话统计

丢包会话统计模块用于查看最近一段时间内丢包会话个数。单击<详细信息>按钮，进入“丢包会话统计详情“页面，可查看最近一小时、一天和三十天的丢包会话个数。

- 单击<详细信息>按钮，进入“丢包话统计详情“页面，可查看最近一小时、一天和三十天的新建会话个数。
    - 单击<开启 Top10 统计>按钮，设备将对基于丢包会话的业务进行会话数目统计，分别基于源地址和目的地址对丢包会话数目进行排序。
    - 单击<查看 Top10 统计>按钮，将进入“Top10”页面，管理员可选择查看“最近一小时”、“最近一天”或者“最近三十天”的“按源地址统计”或者“按目的地址统计”的排名信息。
- 单击<刷新>按钮，可刷新展示数据，查看当前最新统计数据。
- 单击<设置>按钮，进入“设置”页面，可勾选“启用自动刷新”开启自动刷新统计数据功能，并可设置自动刷新的时间间隔。

运行监控—上网行为监控

上网行为监控页面用于查看用户的上网行为记录，包括访问的应用、网站和 IP 地址等。在报文与应用审计策略或 URL 过滤策略成功匹配后，设备会将日志记录发送到上网行为监控页面。单击<详细信息>按钮，可查看用户详细的上网行为，方便管理员对用户的上网行为进行审计。管理员可根据用户上网的情况调整策略，规范用户的上网行为。

有关应用审计日志功能的详细介绍，请参见“应用审计日志联机帮助”。有关 URL 过滤日志功能的详细介绍，请参见“URL 过滤日志联机帮助”。

运行监控—License 信息

License 信息模块用于查看各特性 License 的授权信息。单击<详细信息>按钮，可查看 License 的类型、状态和有效期等详细信息。

运行监控—接口信息

在接口信息模块管理员可以更加直观形象的观察到设备每个接口的实时状态、接口 IP 地址和接口上的详细信息，单击<查看设备面板图>按钮可以查看设备面板上各接口的状态，也可以直接单击设备面板上的指定接口，对接口配置进行修改。

流量监控—流量实时用户排行

用于查看用户实时使用带宽的情况，并根据总流速的百分比展示用户排行结果。显示内容包括用户、下行流速、上行流速、总流速和百分比。

单击<设置>按钮，进入设置页面，可配置如下功能：

- 自动刷新：勾选“启用自动刷新”前的复选框，可开启自动刷新功能，并配置自动刷新的时间间隔。

- 实时流量统计：勾选“采集实时数据”前的复选框，可对流量进行实时统计。勾选“展示实时数据详情”前的复选框，可查看实时流量的统计结果。单击指定的用户，可在弹出的页面中查看该用户对不同应用的访问情况。

流量监控—流量实时应用排行

用于查看应用实时占用带宽的情况，并根据总流速的百分比展示应用排行结果。显示内容包括应用、下行流速、上行流速、总流速和百分比。

单击<设置>按钮，进入设置页面，可配置如下功能：

- 自动刷新：勾选“启用自动刷新”前的复选框，可开启自动刷新功能，并配置自动刷新的时间间隔。
- 实时流量统计：勾选“采集实时数据”前的复选框，可对流量进行实时统计。勾选“展示实时数据详情”前的复选框，可查看实时流量的统计结果。单击指定的应用，可在弹出的页面中查看不同用户对该应用的访问情况。

威胁监控—安全概况

安全概况用于查看最近一个小时的内网安全状态，方便管理员及时调整防护策略，保护内网安全。

设备通过对威胁事件的级别分布情况进行统计和分析，计算出安全评分并以风险等级体现出当前网络安全状态，评分越高表示越安全。

安全评分

安全评分与风险等级的关系如下所示：

- 安全评分为 0~50 分，风险等级为高危；
- 安全评分为 50~70 分，风险等级为中危；
- 安全评分为 70~90 分，风险等级为低危；
- 安全评分为 90~100 分，风险等级为安全。

安全评分的计算公式如下：

安全评分=起评分–攻击危险指数

- 起评分：
  - 如果威胁日志中有严重攻击记录，则起评分为 70。
  - 如果威胁日志中有高危攻击记录，则起评分为 90。
  - 如果威胁日志中有中危、低危攻击记录，则起评分为 100。

  起评分的优先级：严重 > 高危 > 中危/低危
- 攻击危险指数=威胁日志中不同严重级别对应的分值总和。

  威胁日志中的严重级别来源于特征库的匹配结果，NTOP 根据该字段判定威胁级别。其与分值的对应关系如下：
  - 低危，对应分值 0.2；

- 中危，对应分值 0.4；
- 高危，对应分值 0.6；
- 严重，对应分值 4；

需要注意的是：

- 攻击危险指数根据威胁日志中每条记录的严重级别计算分值，然后累加所有记录的分值。
- 安全评分计算结果如果小于 10 分，则强制设置为 10 分。
- 目前威胁日志中的严重级别只会出现 0~100 的情况，若出现异常产生大于 100 的情况，则处理为严重。

安全评分计算举例

假设威胁日志中仅包含以下 4 条严重级别的日志记录：

- 低危，分值 = 0.2
- 中危，分值 = 0.4
- 高危，分值 = 0.6
- 严重，分值 = 4

攻击危险指数= 0.2 + 0.4 + 0.6 + 4 = 5.2

起评分：存在严重攻击的记录，所以起评分 = 70

安全评分= 70 – 5.2 = 64.8

安全概况功能的支持情况与设备型号有关，请以设备实际情况为准。

威胁监控—威胁排行

此模块用于显示设备根据威胁事件的次数对威胁名称进行统计排行的结果，方便管理员对威胁情况进行分析，调整相应的防护策略。

威胁监控—安全状态

安全状态用于展示设备的风险系数及所监测到的安全事件的分布状态柱状图。点击柱状图数据可跳转到安全分析页面，查看具体分析数据。

- 风险系数：用于对设备整体的安全防护能力进行评估，包括设备是否配置了安全策略、入侵防御、防病毒、IP 信誉等安全事件的检测功能，以及设备是否检测到了安全事件等，分数越低表示设备越安全。方便用户了解设备的整体安全状况，及时调整相应的防护策略。
- 安全事件分布状态柱状图：用于展示设备对处于不同风险级别(包括有漏洞、被攻击、已受控、已扩散和已受损）的内网主机/资产数量的统计结果。方便用户了解内网主机/资产的整体安全状态，及时调整相应的防护策略。点击柱状图数据可跳转到安全分析页面，查看具体分析数据。

当界面无显示数据时，可以进行如下排查：

- 检查是否正确挂载了硬盘或者 U 盘。

- 检查是否开启了业务日志采集功能。有关业务日志采集功能的详细说明，请参见“日志设置基本配置联机帮助”。
- 检查是否配置了针对内外网的安全防护策略，例如入侵防御、防病毒、IP 信誉等。

威胁监控—风险主机 Top10

此模块用于展示设备下游的风险主机列表，包括主机名、综合风险等级和攻击事件统计。点击主机名可跳转到安全分析页面，查看该主机的风险分析状况。

安全监控—安全分析

安全分析用于查看最近一段时间主机的风险概况。

注意事项

本功能的支持情况与设备型号有关，请以设备实际情况为准。

安全分析页面下的功能仅在设备安装了硬盘或者 U 盘时支持展示。

内网资产地址范围

当用户需要对资产流量进行统计分析时，需要配置资产地址范围，设备会将指定的地址范围识别为内网，范围外的地址识别为外网，并对内网-内网、内网-外网、外网-内网间的流量进行分析。若未配置资产地址范围，设备将只分析 Trust-Trust、Trust-Untrust、Untrust-Trust 安全域间的流量，并将 Trust 域识别为内网，Untrust 域识别为外网，其他安全域的流量不进行分析。

风险主机

设备基于所有与安全风险相关的日志（包括入侵防御日志、防病毒日志、Web 应用防护日志、文件过滤日志、URL 过滤日志、信誉日志以及 DGA 域名检测日志），对主机存在的安全风险进行分析，帮助用户快速了解业务主机的风险状况。单击统计数据，可跳转到安全分析页面，查看主机的安全状况详情。

需要注意，当风险主机模块没有显示的数据时，可能的原因包括如下：

- 设备未安装硬盘或者 U 盘。
- 入侵防御业务、防病毒等业务未产生日志数据。

攻击趋势

设备基于入侵防御日志和防病毒日志，对主机受到的攻击进行分析，展示了指定时间范围内的攻击趋势，方便管理员快速了解业务受到的攻击情况。

需要注意，当此模块没有显示的数据时，可能是由于指定的时间范围内入侵防御业务和防病毒业务未产生日志数据导致。

业务热点事件 Top 10

入侵防御特征库中记录了近期网络中的 Top 10 热点攻击事件，当设备基于入侵防御日志检测到主机也遭到了同样的攻击时，会将相应的热点事件展示到 Web 界面中，方便管理员了解主机的安全风险现状并及时调整相应的防护策略。

需要注意，当此模块没有显示的数据时，可能的原因包括如下：

- 当前入侵防御特征库版本较低，建议将特征库升级到最新版本。
- 指定的时间范围内，入侵防御业务未产生日志数据。

安全监控—安全能力

安全能力模块用于展示各安全功能模块的授权版本详情，同时提供更新升级功能。

点击任一特性 License，可查看 License 的类型、状态和有效期等详细信息。

选择“系统 > 云网联动”，进入“云网联动”页面，可以完成云运维、云 WAF 服务的开通及查看。

在开通云运维、云 WAF 等云服务实现对设备的云管理及防护后，在该模块，可以查看设备与云运维、云 WAF 服务的连接状态。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

黑名单日志

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 日志导入
  - 日志导出

特性简介

黑名单功能是根据报文的 IP 地址进行报文过滤的一种攻击防范特性，可以由设备动态或者由用户手动添加或删除，有关黑名单的详细介绍请参见“黑名单”联机帮助。

黑名单日志展示功能需要在“系统 > 日志设置 > 存储空间设置”页面内开启“攻击检测与防范 | 黑名单日志”，当增加黑名单、删除黑名单、扫描攻击防范动态添加黑名单、黑名单老化被删除时会

有相应的日志输出，日志的内容主要包括黑名单的源 IP 地址、DS-Lite 隧道对端地址、VPN 实例名称、添加或删除的原因以及老化时间等。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 日志的导入、导出和清除操作不能同时进行。同一时间只能选择一种操作方式。
- 同一时间，只能有一个用户对日志进行导入、导出或清除的操作。

配置指南

日志导入

日志支持导入功能，用户可单击<导入>按钮，在弹出的提示框中单击<确定>，进入导入界面。选择导入的日志文件并输入日志文件的密码，即可将日志导入设备中。

日志导出

设备支持将日志导出到 PC 本地。具体步骤如下：

1. 单击“监控 > 日志 > 安全类”，进入安全类日志页面，在列表上方的下拉框中选择“黑名单日志”。

2. 单击显示列的<  >过滤器按钮，配置日志的查询条件，单击<确定>按钮，筛选出需要导出的日志。单击列表右上方的<  >过滤器按钮，可以保存当前的查询条件。

3. 单击<导出>按钮，进入“导出日志”页面。配置日志导出参数，具体参数如下表所示：

表-1 日志导出参数表

参数	说明
设置密码	用于设置日志文件的密码，日志文件会被加密导出，导出后的文件需要输入 可以查看
导出条数	用于设置每个日志文件中可以包含的日志条数 • 当日志实际数量小于或等于配置的导出条数时，设备会将所有日志导出 • 当日志实际数量大于配置的导出条数时，设备会按照配置的导出条数， 出到多个文件中

4. 完成日志导出参数的配置后，单击<导出>按钮，设备会将日志文件导出到 PC 本地。

单包攻击日志

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 日志导入
  - 日志导出

特性简介

单包攻击也称畸形报文攻击，主要包括以下三种类型：

- 攻击者通过向目标系统发送带有攻击目的的 IP 报文，如分片重叠的 IP 报文、TCP 标志位非法的报文，使得目标系统在处理这样的 IP 报文时出错、崩溃。
- 攻击者可以通过发送正常的报文，如 ICMP 报文、特殊类型的 IP option 报文，来干扰正常网络连接或探测网络结构，给目标系统带来损失。

- 攻击者还可通过发送大量无用报文占用网络带宽，造成拒绝服务攻击。

若在“对象 > 安全配置文件 > 攻击防范”界面，单包攻击防范的配置中日志功能为开启状态，同时在“系统 > 日志设置 > 存储空间设置”页面内开启“攻击检测与防范 | 单包攻击日志”，则当设备检测到某报文符合单包攻击的特征时，设备会输出相应的日志信息。

缺省情况下，单包攻击日志采用聚合输出方式。即：在一定时间内，对在同一安全域上检测到的相同攻击类型、相同攻击防范动作、相同的源/目的地址以及属于相同 VPN 的单包攻击的所有日志聚合成一条日志输出。

设备支持在“系统 > 日志设置 > 更多设置”页面关闭单包攻击日志聚合输出功能，逐条输出单包攻击日志。但在单包攻击较为频繁的情况下，逐条输出会占用大量显示资源。所以通常不建议关闭聚合输出功能。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 日志的导入、导出和清除操作不能同时进行。同一时间只能选择一种操作方式。
- 同一时间，只能有一个用户对日志进行导入、导出或清除的操作。

配置指南

日志导入

日志支持导入功能，用户可单击<导入>按钮，在弹出的提示框中单击<确定>，进入导入界面。选择导入的日志文件并输入日志文件的密码，即可将日志导入设备中。

日志导出

设备支持将日志导出到 PC 本地。具体步骤如下：

1. 单击“监控 > 日志 > 安全类”，进入安全类日志页面，在列表上方的下拉框中选择“单包攻击日志”。
2. 单击显示列的<  >过滤器按钮，配置日志的查询条件，单击<确定>按钮，筛选出需要导出的日志。单击列表右上方的<  >过滤器按钮，可以保存当前的查询条件。
3. 单击<导出>按钮，进入“导出日志”页面。配置日志导出参数，具体参数如下表所示：

表-1 日志导出参数表

参数	说明
设置密码	用于设置日志文件的密码，日志文件会被加密导出，导出后的文件需要输入 可以查看
导出条数	用于设置每个日志文件中可以包含的日志条数 • 当日志实际数量小于或等于配置的导出条数时，设备会将所有日志导出 • 当日志实际数量大于配置的导出条数时，设备会按照配置的导出条数， 出到多个文件中

4. 完成日志导出参数的配置后，单击<导出>按钮，设备会将日志文件导出到 PC 本地。

扫描攻击日志

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 日志导入
  - 日志导出

特性简介

扫描攻击是指，攻击者运用扫描工具对网络进行主机地址或端口的扫描，通过准确定位潜在目标的位置，探测目标系统的网络拓扑结构和开放的服务端口，为进一步侵入目标系统做准备。

扫描攻击分为地址扫描攻击和端口扫描攻击，有关扫描攻击的详细介绍，请参见“攻击防范”联机帮助。

若在“对象 > 安全配置文件 > 攻击防范”界面，扫描防范的配置中开启输出告警日志，同时在“系统 > 日志设置 > 存储空间设置”页面内开启“攻击检测与防范 | 扫描攻击日志”，则当设备监测到某 IP 地址主动发起的连接速率达到或超过了一定阈值时，设备会输出相应的日志信息。

若端口扫描和地址扫描同时达到扫描阈值，则仅输出地址扫描的告警日志。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 日志的导入、导出和清除操作不能同时进行。同一时间只能选择一种操作方式。
- 同一时间，只能有一个用户对日志进行导入、导出或清除的操作。

配置指南

日志导入

日志支持导入功能，用户可单击<导入>按钮，在弹出的提示框中单击<确定>，进入导入界面。选择导入的日志文件并输入日志文件的密码，即可将日志导入设备中。

日志导出

设备支持将日志导出到 PC 本地。具体步骤如下：

1. 单击“监控 > 日志 > 安全类”，进入安全类日志页面，在列表上方的下拉框中选择“扫描攻击日志”。
2. 单击显示列的<  >过滤器按钮，配置日志的查询条件，单击<确定>按钮，筛选出需要导出的日志。单击列表右上方的<  >过滤器按钮，可以保存当前的查询条件。
3. 单击<导出>按钮，进入“导出日志”页面。配置日志导出参数，具体参数如下表所示：

表-1 日志导出参数表

参数	说明
设置密码	用于设置日志文件的密码，导出后的文件需要输入设置的密码才可以查看
导出条数	用于设置每个日志文件中可以包含的日志条数 • 当日志实际数量小于或等于配置的导出条数时，设备会将所有日志导出 • 当日志实际数量大于配置的导出条数时，设备会按照配置的导出条数，出到多个文件中

4. 完成日志导出参数的配置后，单击<导出>按钮，设备会将日志文件导出到 PC 本地。

泛洪攻击日志

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 日志导入
  - 日志导出

特性简介

泛洪攻击是指攻击者在短时间内向目标系统发送大量的虚假请求，导致目标系统疲于应付无用信息，从而无法为合法用户提供正常服务，即发生拒绝服务。有关泛洪攻击的详细介绍请参见“攻击防范”联机帮助。

泛洪攻击防范主要用于保护服务器。若在“对象 > 安全配置文件 > 攻击防范”界面，泛洪攻击防范的配置中开启日志功能，同时在“系统 > 日志设置 > 存储空间设置”页面内开启“攻击检测与防范

| 泛洪攻击日志”，则当向某服务器发送报文的速率或源自某发送方的报文速率持续达到或超过了相应的触发门限值时，设备会输出相应的日志信息。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 日志的导入、导出和清除操作不能同时进行。同一时间只能选择一种操作方式。
- 同一时间，只能有一个用户对日志进行导入、导出或清除的操作。

配置指南

日志导入

日志支持导入功能，用户可单击<导入>按钮，在弹出的提示框中单击<确定>，进入导入界面。选择导入的日志文件并输入日志文件的密码，即可将日志导入设备中。

日志导出

设备支持将日志导出到 PC 本地。具体步骤如下：

1. 单击“监控 > 日志 > 安全类”，进入安全类日志页面，在列表上方的下拉框中选择“泛洪攻击日志”。

2. 单击显示列的<  >过滤器按钮，配置日志的查询条件，单击<确定>按钮，筛选出需要导出的日志。单击列表右上方的<  >过滤器按钮，可以保存当前的查询条件。

3. 单击<导出>按钮，进入“导出日志”页面。配置日志导出参数，具体参数如下表所示：

   表-1 日志导出参数表

参数	说明
设置密码	用于设置日志文件的密码，日志文件会被加密导出，导出后的文件需要输入 可以查看
导出条数	用于设置每个日志文件中可以包含的日志条数 • 当日志实际数量小于或等于配置的导出条数时，设备会将所有日志导出 • 当日志实际数量大于配置的导出条数时，设备会按照配置的导出条数， 出到多个文件中

4. 完成日志导出参数的配置后，单击<导出>按钮，设备会将日志文件导出到 PC 本地。

Web 应用防护日志

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- License 支持情况
- 使用限制和注意事项
- 配置指南
  - 日志导入
  - 日志导出
  - 日志聚合

特性简介

Web 应用防护日志用来查看 Web 应用层攻击的检测和防御情况的记录，了解曾经发生和正在发生的攻击事件，方便管理员调整相应的策略，更好地防护内网安全。

Web 应用防护日志的展示功能需要在 Web 应用防护配置文件中开启日志功能后生效，当报文与 Web 应用防护配置文件成功匹配后将输出日志到 Web 应用防护日志页面。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

License支持情况

Web 应用防护功能需要购买并正确安装 License 后才能使用。License 过期后，Web 应用防护功能可以采用设备中已有的 Web 应用防护特征库正常工作，但无法升级到官方网站在过期时间后发布的新版本的特征库。关于 License 的详细介绍请参见“License 联机帮助”。

使用限制和注意事项

- 日志的导入、导出和清除操作，不能同时进行。同一时间只能选择一种操作方式。
- 同一时间，只能有一个用户对日志进行导入、导出或清除的操作。

配置指南

日志导入

日志支持导入功能。具体步骤如下：

1. 单击“监控 > 日志 > 安全类”，进入安全类日志页面，在页面中选择“Web 应用防护日志”。
2. 单击<导入>按钮，进入“导入日志”页面，选择导入的日志文件并输入日志文件的密码，单击<确定>按钮，即可将日志导入设备中。

日志导出

设备支持将日志导出到 PC 本地。具体步骤如下：

1. 单击“监控 > 日志 > 安全类”，进入安全类日志页面，在页面中选择“Web 应用防护日志”。
2. 单击显示列的<  >过滤器按钮，配置日志的查询条件，单击<确定>按钮，筛选出需要导出的日志。
3. 单击<导出>按钮，进入“导出日志”页面，配置日志导出参数，具体参数如下表所示：

表-1 日志导出参数表

参数	说明
设置密码	用于设置日志文件的密码，日志文件会被加密导出，导出后的文件需要输入 可以查看
导出条数	用于设置每个日志文件中可以包含的日志条数 • 当日志实际数量小于或等于配置的导出条数时，设备会将所有日志导出 • 当日志实际数量大于配置的导出条数时，设备会按照配置的导出条数， 出到多个文件中

4. 完成日志导出参数的配置后，单击<导出>按钮，设备会将日志文件导出到 PC 本地。

日志聚合

开启日志聚合功能后，设备将对指定聚合时间内采集到的满足相同聚合条件的业务日志进行聚合，可以减少 Web 界面中展示的日志条目，方便用户对日志进行查看。其中，日志聚合条件包括：源 IP 地址、目的 IP 地址、应用、VrfName、源安全域和目的安全域。

具体配置步骤如下：

1. 单击“监控 > 日志 > 安全类”，进入安全类日志页面，在页面中选择“Web 应用防护日志”。
2. 单击<更多操作>按钮，选择日志聚合配置，进入日志聚合配置页面。
3. 开启日志聚合功能，并配置聚合时间。

4. 单击<确定>按钮，完成配置。

威胁日志

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- License 支持情况
- 使用限制和注意事项
- 配置指南
  - 查看详情
  - 下载捕获文件
  - 加入白名单
  - 日志导入
  - 日志导出
  - 日志聚合

特性简介

威胁日志用来查看入侵防御和防病毒等网络威胁的检测和防御情况的记录，了解曾经发生和正在发生的威胁事件，方便管理员调整相应的策略，更好地防护内网安全。

威胁日志的展示功能需要在入侵防御配置文件和防病毒配置文件中开启日志功能后生效，当报文与入侵防御配置文件或防病毒配置文件成功匹配后将输出日志到威胁日志页面。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

License支持情况

入侵防御

入侵防御功能需要购买并正确安装 License 后才能使用。License 过期后，入侵防御功能可以采用设备中已有的入侵防御特征库正常工作，但无法升级到官方网站在过期时间后发布的新版本的特征库。关于 License 的详细介绍请参见“License 联机帮助”。

防病毒

防病毒功能需要购买并正确安装 License 才能使用。License 过期后，防病毒功能可以采用设备中已有的病毒特征库正常工作，但无法升级特征库且云端查询功能以及联动沙箱阻断功能无法使用。关于 License 的详细介绍请参见“License 配置联机帮助”。

使用限制和注意事项

- 日志的导入、导出和清除操作，不能同时进行。同一时间只能选择一种操作方式。
- 同一时间，只能有一个用户对日志进行导入、导出或清除的操作。
- 页面默认展示近一天的日志，当需要查询多天日志时，用户可单击<近 7 天>、<近 30 天>和<自定义>按钮切换日期，查看指定日期的日志信息。
- 对于防病毒日志，威胁 ID 为 4294967295，表示通过云端查询功能检测到的病毒；威胁 ID 为 4294967294 表示通过 APT 防御功能检测到的病毒。
- 对于入侵防御日志，威胁 ID 为 4294967290，表示通过语义分析检测功能检测到的攻击。

配置指南

查看详情

威胁日志中可查看日志详情，用户可单击指定日志前的详情按钮，在弹出的详情页面中查看日志的详细信息。其中，威胁名称和报文详情中部分字段显示内容可能较多，用户可以将鼠标移到对应字段，查看悬浮信息，也可通过单击<复制>按钮，在弹出的复制窗口中获取完整的内容。

下载捕获文件

当入侵防御功能执行捕获动作后，设备将生成捕获文件。当设备上安装了硬盘或 U 盘后，用户可通过单击指定日志右侧的<下载>按钮，获取捕获文件，方便用户分析威胁信息。

加入白名单

当发现入侵防御日志中存在误报的情况时，可单击指定日志右侧的<加入白名单>按钮，将误报日志中提取到的威胁 ID（入侵防御特征 ID）和 URL 加入白名单。设备将对匹配白名单的报文放行，可以减少误报。

日志导入

日志支持导入功能。具体步骤如下：

1. 单击“监控 > 日志 > 安全类”，进入安全类日志页面，在页面中选择“威胁日志”。
2. 单击<导入>按钮，进入“导入日志”页面，选择导入的日志文件并输入日志文件的密码，单击<确定>按钮，即可将日志导入设备中。

日志导出

设备支持将日志导出到 PC 本地。具体步骤如下：

1. 单击“监控 > 日志 > 安全类”，进入安全类日志页面，在页面中选择“威胁日志”。
2. 单击显示列的<  >过滤器按钮，配置日志的查询条件，单击<确定>按钮，筛选出需要导出的日志。
3. 单击<导出>按钮，进入“导出日志”页面，配置日志导出参数，具体参数如下表所示：

表-1 日志导出参数表

参数	说明
设置密码	用于设置日志文件的密码，日志文件会被加密导出，导出后的文件需要输入 可以查看

导出条数	用于设置每个日志文件中可以包含的日志条数 • 当日志实际数量小于或等于配置的导出条数时，设备会将所有日志导出 • 当日志实际数量大于配置的导出条数时，设备会按照配置的导出条数，出到多个文件中

4. 完成日志导出参数的配置后，单击<导出>按钮，设备会将日志文件导出到 PC 本地中。

日志聚合

开启日志聚合功能后，设备将对指定聚合时间内采集到的满足相同聚合条件的业务日志进行聚合，可以减少 Web 界面中展示的日志条目，方便用户对日志进行查看。其中，日志聚合条件包括：源 IP 地址、目的 IP 地址、应用、源端口、目的端口、威胁 ID、威胁名称和威胁类型。

具体配置步骤如下：

1. 单击“监控 > 日志 > 安全类”，进入安全类日志页面，在页面中选择“威胁日志”。
2. 单击<更多操作>按钮，选择日志聚合配置，进入日志聚合配置页面。
3. 开启日志聚合功能，并配置聚合时间。
4. 单击<确定>按钮，完成配置。

物联网设备安全管理日志

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- License 支持情况
- 使用限制和注意事项
- 配置指南
  - 日志导入
  - 日志导出

特性简介

物联网设备安全管理是一种针对物联网设备进行智能检测、安全管理的技术，主要功能包括：标准格式检查、设备准入控制、敏感信令控制、标准流量管控。

物联网设备安全管理日志用来查看设备检测到的物联网设备存在安全隐患的日志信息，方便管理员及时调整策略，防止信息泄露和网络攻击。

物联网设备安全管理日志的展示功能需要在标准格式检查、设备准入控制、敏感信令控制、标准流量管控页面中开启日志告警功能后生效，当对报文执行管理员配置的动作时，设备将输出日志到物联网设备安全管理日志页面。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

License支持情况

敏感信令控制功能需要基于应用识别（APR）特征库来进行识别。License 过期后，敏感信令控制功能可以采用设备中已有的 APR 特征库正常工作，但无法升级特征库。关于 License 的详细介绍请参见“License 联机帮助”。

使用限制和注意事项

- 日志的导入、导出和删除操作，不能同时进行。同一时间只能选择一种操作方式。
- 同一时间，只能有一个用户对日志进行导入、导出或删除的操作。

配置指南

日志导入

日志支持导入功能，用户可单击<导入>按钮，在弹出的提示框中单击<确定>，进入导入界面。选择导入的日志文件并输入日志文件的密码，即可将日志导入设备中。

日志导出

设备支持将日志导出到 PC 本地。具体步骤如下：

1. 单击显示列的<  >过滤器按钮，配置日志的查询条件，单击<确定>按钮，筛选出需要导出的日志。

2. 单击<导出>按钮，进入“导出日志”页面，配置日志导出参数，具体参数如下表所示：

表-1 日志导出参数表

参数	说明
设置密码	用于设置日志文件的密码，日志文件会被加密导出，导出后的文件需要输入 可以查看
导出条数	用于设置每个日志文件中可以包含的日志条数

	• 当日志实际数量小于或等于配置的导出条数时，设备会将所有日志导出 • 当日志实际数量大于配置的导出条数时，设备会按照配置的导出条数，出到多个文件中

3. 完成日志导出参数的配置后，单击<导出>按钮，设备会将日志文件导出到 PC 本地。

Web 防篡改日志

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 日志导入
  - 日志导出
  - 配置缓存网页文件功能
  - 标识缓存网页文件状态

特性简介

Web 防篡改日志用来查看网页防篡改功能产生的日志记录，了解曾经发生和正在发生的网页内容篡改事件，方便管理员调整相应的策略，更好地防护内网安全。

管理员需要到“系统 > 日志设置 > 存储空间设置”页面开启防篡改业务的日志采集功能才能查看Web 防篡改日志。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 日志的导入、导出和清除操作，不能同时进行。同一时间只能选择一种操作方式。
- 同一时间，只能有一个用户对日志进行导入、导出或清除的操作。

配置指南

日志导入

日志支持导入功能。具体步骤如下：

1. 单击“监控 > 日志 > 安全类”，进入安全类日志页面，在页面中选择“Web 防篡改日志”。

2. 单击<导入>按钮，进入“导入日志”页面，选择导入的日志文件并输入日志文件的密码，单击<确定>按钮，即可将日志导入设备中。

日志导出

设备支持将日志导出到 PC 本地。具体步骤如下：

1. 单击“监控 > 日志 > 安全类”，进入安全类日志页面，在页面中选择“Web 防篡改日志”。
2. 单击显示列的<  >过滤器按钮，配置日志的查询条件，单击<确定>按钮，筛选出需要导出的日志。
3. 单击<导出>按钮，进入“导出日志”页面，配置日志导出参数，具体参数如下表所示：

表-1 日志导出参数表

参数	说明
设置密码	用于设置日志文件的密码，日志文件会被加密导出，导出后的文件需要输入 可以查看
导出条数	用于设置每个日志文件中可以包含的日志条数 • 当日志实际数量小于或等于配置的导出条数时，设备会将所有日志导出 • 当日志实际数量大于配置的导出条数时，设备会按照配置的导出条数， 出到多个文件中

4. 完成日志导出参数的配置后，单击<导出>按钮，设备会将日志文件导出到 PC 本地。

配置缓存网页文件功能

开启缓存网页文件功能后，当设备检测出服务器返回的响应报文中的网页文件与基线文件不一致时，会缓存该网页文件。管理员可到“监控 > 日志 > 安全类”页面，页面中选择“Web 防篡改日志”后单击指定日志右侧“缓存的网页文件”列下的<下载>按钮，获取该文件进行查看。

仅当硬盘或 U 盘在位时，设备才支持缓存网页文件。

标识缓存网页文件状态

当设备检测到缓存的网页文件与基线文件不一致时，会生成一条日志记录，并默认缓存的网页文件是一个篡改文件。管理员可以通过该日志页面查看缓存网页文件内容，判断该文件是否为篡改文件，如果确认该文件是正确的、未经过篡改的文件，可以将文件状态修改为“非篡改”，设备会使用该文件替换基线文件。

标识缓存网页文件状态的具体配置步骤如下：

1. 单击“监控 > 日志 > 安全类”，进入安全类日志页面，在页面中选择“Web 防篡改日志”。
2. 在指定日志右侧的“标识缓存网页文件状态”列，单击<篡改>或<非篡改>按钮，修改文件的标识。
3. 如需批量修改多条日志中的缓存网页文件状态时，可以选择多条日志，单击页面上方的<篡改>或<非篡改>按钮，修改文件的标识。

仅当硬盘或 U 盘在位时，支持标识缓存网页文件状态。

信誉日志

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- License 支持情况
- 使用限制和注意事项
- 配置指南
  - 日志导入
  - 日志导出

特性简介

信誉日志包括 IP 信誉日志、URL 信誉日志和域名信誉日志。

信誉日志的展示功能需要在各信誉功能中开启日志功能后生效，当报文与各信誉特征库成功匹配后将输出日志到信誉日志页面。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

License支持情况

IP 信誉、URL 信誉和域名信誉功能需要购买并正确安装 License 后才能使用。License 过期后，各信誉功能可以使用设备中已有的特征库正常工作，但无法升级到 License 有效期之后发布的新版本的特征库。关于 License 的详细介绍请参见“License 联机帮助”。

使用限制和注意事项

- 日志的导入、导出和清除操作，不能同时进行。同一时间只能选择一种操作方式。
- 同一时间，只能有一个用户对日志进行导入、导出或清除的操作。

配置指南

日志导入

日志支持导入功能。具体步骤如下：

1. 单击“监控 > 日志 > 安全类”，进入安全类日志页面，在页面中选择“信誉日志”。
2. 单击<导入>按钮，进入“导入日志”页面，选择导入的日志文件并输入日志文件的密码，单击<确定>按钮，即可将日志导入设备中。

日志导出

设备支持将日志导出到 PC 本地。具体步骤如下：

1. 单击“监控 > 日志 > 安全类”，进入安全类日志页面，在页面中选择“信誉日志”。
2. 单击显示列的<  >过滤器按钮，配置日志的查询条件，单击<确定>按钮，筛选出需要导出的日志。
3. 单击<导出>按钮，进入“导出日志”页面，配置日志导出参数，具体参数如下表所示：

表-1 日志导出参数表

参数	说明
设置密码	用于设置日志文件的密码，日志文件会被加密导出，导出后的文件需要输入 可以查看
导出条数	用于设置每个日志文件中可以包含的日志条数 • 当日志实际数量小于或等于配置的导出条数时，设备会将所有日志导出 • 当日志实际数量大于配置的导出条数时，设备会按照配置的导出条数， 出到多个文件中

4. 完成日志导出参数的配置后，单击<导出>按钮，设备会将日志文件导出到 PC 本地。

URL 过滤日志

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 日志导入
  - 日志导出
  - 日志聚合

特性简介

URL 过滤日志用来查看用户访问 URL 产生的日志信息，方便管理员根据用户的访问情况调整 URL 过滤策略，规范用户的上网行为。

URL 过滤日志的展示功能需要在 URL 过滤策略中开启日志功能后生效，当报文与策略成功匹配后将输出日志到 URL 过滤日志页面。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 本功能的支持情况与设备型号有关，请以设备实际情况为准。
- 日志的导入、导出和清除操作，不能同时进行。同一时间只能选择一种操作方式。
- 同一时间，只能有一个用户对日志进行导入、导出或清除的操作。

配置指南

日志导入

日志支持导入功能。具体步骤如下：

1. 单击“监控 > 日志 > 安全类”，进入安全类日志页面，在页面中选择“URL 过滤日志”。
2. 单击<导入>按钮，进入“导入日志”页面，选择导入的日志文件并输入日志文件的密码，单击<确定>按钮，即可将日志导入设备中。

日志导出

设备支持将日志导出到 PC 本地。具体步骤如下：

1. 单击“监控 > 日志 >安全类”，进入安全类日志页面，在页面中选择“URL 过滤日志”。
2. 单击显示列的<  >过滤器按钮，配置日志的查询条件，单击<确定>按钮，筛选出需要导出的日志。
3. 单击<导出>按钮，进入“导出日志”页面，配置日志导出参数，具体参数如下表所示：

表-1 日志导出参数表

参数	说明
设置密码	用于设置日志文件的密码，日志文件会被加密导出，导出后的文件需要输入 可以查看
导出条数	用于设置每个日志文件中可以包含的日志条数 • 当日志实际数量小于或等于配置的导出条数时，设备会将所有日志导出 • 当日志实际数量大于配置的导出条数时，设备会按照配置的导出条数， 出到多个文件中

4. 完成日志导出参数的配置后，单击<导出>按钮，设备会将日志文件导出到 PC 本地。

日志聚合

开启日志聚合功能后，设备将对指定聚合时间内采集到的满足相同聚合条件的业务日志进行聚合，可以减少 Web 界面中展示的日志条目，方便用户对日志进行查看。其中，日志聚合条件包括：源 IP 地址、目的 IP 地址、应用、源端口、目的端口、URL 分类和 URL。

具体配置步骤如下：

1. 单击“监控 > 日志 >安全类”，进入安全类日志页面，在页面中选择“URL 过滤日志”。
2. 单击<更多操作>按钮，选择日志聚合配置，进入日志聚合配置页面。
3. 开启日志聚合功能，并配置聚合时间。
4. 单击<确定>按钮，完成配置。

文件过滤日志

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 日志导入
  - 日志导出
  - 日志聚合

特性简介

文件过滤日志用于查看用户经由设备传输文件产生的日志信息，方便管理员根据文件传输的情况调整文件过滤策略，降低机密信息泄露和病毒文件进入公司内部网络的风险。

文件过滤日志的展示功能需要在文件过滤策略中开启日志功能后生效，当报文与策略成功匹配后将输出日志到文件过滤日志页面。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 日志的导入、导出和清除操作，不能同时进行。同一时间只能选择一种操作方式。
- 同一时间，只能有一个用户对日志进行导入、导出或清除的操作。

配置指南

日志导入

日志支持导入功能。具体步骤如下：

1. 单击“监控 > 日志 > 安全类”，进入安全类日志页面，在页面中选择“文件过滤日志”。
2. 单击<导入>按钮，进入“导入日志”页面，选择导入的日志文件并输入日志文件的密码，单击<确定>按钮，即可将日志导入设备中。

日志导出

设备支持将日志导出到 PC 本地。具体步骤如下：

1. 单击“监控 > 日志 > 安全类”，进入安全类日志页面，在页面中选择“文件过滤日志”。
2. 单击显示列的<  >过滤器按钮，配置日志的查询条件，单击<确定>按钮，筛选出需要导出的日志。
3. 单击<导出>按钮，进入“导出日志”页面，配置日志导出参数，具体参数如下表所示：

表-1 日志导出参数表

参数	说明
设置密码	用于设置日志文件的密码，日志文件会被加密导出，导出后的文件需要输入 可以查看
导出条数	用于设置每个日志文件中可以包含的日志条数 • 当日志实际数量小于或等于配置的导出条数时，设备会将所有日志导出 • 当日志实际数量大于配置的导出条数时，设备会按照配置的导出条数， 出到多个文件中

4. 完成日志导出参数的配置后，单击<导出>按钮，设备会将日志文件导出到 PC 本地。

日志聚合

开启日志聚合功能后，设备将对指定聚合时间内采集到的满足相同聚合条件的业务日志进行聚合，可以减少 Web 界面中展示的日志条目，方便用户对日志进行查看。其中，日志聚合条件包括：源 IP 地址、目的 IP 地址、应用、源端口、目的端口和文件类型。

具体配置步骤如下：

1. 单击“监控 > 日志 > 安全类”，进入安全类日志页面，在页面中选择“文件过滤日志”。
2. 单击<更多操作>按钮，选择日志聚合配置，进入日志聚合配置页面。
3. 开启日志聚合功能，并配置聚合时间。
4. 单击<确定>按钮，完成配置。

数据过滤日志

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 日志导入
  - 日志导出
  - 日志聚合

特性简介

数据过滤日志用于查看用户通过文件传输、收发邮件、访问网站等涉及敏感信息传输时产生的日志信息，方便管理员根据数据传输的情况调整数据过滤配置文件，降低机密信息和用户敏感信息泄露的风险。

数据过滤日志的展示功能需要在数据过滤配置文件中开启日志功能后生效，当报文与配置文件成功匹配后将输出日志到数据过滤日志页面。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 日志的导入、导出和清除操作，不能同时进行。同一时间只能选择一种操作方式。
- 同一时间，只能有一个用户对日志进行导入、导出或清除的操作。

配置指南

日志导入

日志支持导入功能，具体步骤如下：

1. 单击“监控 > 日志 > 安全类”，进入安全类日志页面，在页面中选择“数据过滤日志”。

2. 单击<导入>按钮，进入“导入日志”页面，选择导入的日志文件并输入日志文件的密码，即可将日志导入设备中。

日志导出

设备支持将日志导出到 PC 本地，具体步骤如下：

1. 单击“监控 > 日志 > 安全类”，进入安全类日志页面，在页面中选择“数据过滤日志”。
2. 单击显示列的<  >过滤器按钮，配置日志的查询条件，单击<确定>按钮，筛选出需要导出的日志。
3. 单击<导出>按钮，进入“导出日志”页面，配置日志导出参数，具体参数如下表所示：

表-1 日志导出参数表

参数	说明
设置密码	用于设置日志文件的密码，日志文件会被加密导出，导出后的文件需要输入 可以查看
导出条数	用于设置每个日志文件中可以包含的日志条数 • 当日志实际数量小于或等于配置的导出条数时，设备会将所有日志导出 • 当日志实际数量大于配置的导出条数时，设备会按照配置的导出条数， 出到多个文件中

4. 完成日志导出参数的配置后，单击<导出>按钮，设备会将日志文件导出到 PC 本地中。

日志聚合

开启日志聚合功能后，设备将对指定聚合时间内采集到的满足相同聚合条件的业务日志进行聚合，可以减少 Web 界面中展示的日志条目，方便用户对日志进行查看。其中，日志聚合条件包括：源 IP 地址、目的 IP 地址、应用、源端口、目的端口、源安全域、目的安全域、文件名、关键字组、关键字类型和关键字内容。

具体配置步骤如下：

1. 单击“监控 > 日志 > 安全类”，进入安全类日志页面，在页面中选择“数据过滤日志”。
2. 单击<更多操作>按钮，选择日志聚合配置，进入日志聚合配置页面。
3. 开启日志聚合功能，并配置聚合时间。
4. 单击<确定>按钮，完成配置。

应用审计日志

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- License 支持情况
- 使用限制和注意事项
- 配置指南
  - 日志导入
  - 日志导出

特性简介

应用审计日志用来查看用户的上网行为记录，方便管理员根据用户上网的情况调整应用审计与管理策略，规范用户的上网行为。

应用审计日志的展示功能需要在应用审计策略中开启日志功能后生效，当报文与策略成功匹配后将输出日志到应用审计日志页面。

单击<详情>按钮，可查看上网行为的详细内容。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

License支持情况

应用审计功能需要基于 APR（应用识别）特征库来进行识别。License 过期后，应用审计功能可以采用设备中已有的 APR 特征库正常工作，但无法升级特征库。关于 License 的详细介绍请参见“License 联机帮助”。

使用限制和注意事项

查看日志详情时，用户组字段将显示如下内容：

- 如果用户不属于任何用户组，则用户组字段将显示为用户名。
- 如果用户属于一个用户组，只有所属用户组被应用审计策略引用后，用户组字段才会显示为用户组名，否则显示为用户名。
- 如果用户属于多个用户组，则用户组字段将显示为用户直属的某一个用户组名。

对日志进行导入、导出和删除操作时，有如下注意事项：

- 日志的导入、导出和清除操作，不能同时进行。同一时间只能选择一种操作方式。
- 同一时间，只能有一个用户对日志进行导入、导出或清除的操作。

配置指南

日志导入

日志支持导入功能，用户可单击<导入>按钮，在弹出的提示框中单击<确定>，进入导入界面。选择导入的日志文件并输入日志文件的密码，即可将日志导入设备中。

日志导出

设备支持将日志导出到 PC 本地。具体步骤如下：

1. 单击显示列的<  >过滤器按钮，配置日志的查询条件，单击<确定>按钮，筛选出需要导出的日志。
2. 单击<导出>按钮，进入“导出日志”页面，配置日志导出参数，具体参数如下表所示：

表-1 日志导出参数表

参数	说明
设置密码	用于设置日志文件的密码，日志文件会被加密导出，导出后的文件需要输入 可以查看
导出条数	用于设置每个日志文件中可以包含的日志条数 • 当日志实际数量小于或等于配置的导出条数时，设备会将所有日志导出 • 当日志实际数量大于配置的导出条数时，设备会按照配置的导出条数， 出到多个文件中

3. 完成日志导出参数的配置后，单击<导出>按钮，设备会将日志文件导出到 PC 本地。

IP 限速日志

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 日志导入
  - 日志导出

特性简介

为了防止 DDoS 攻击造成大量新建连接消耗设备的处理性能，影响正常业务，可对设备上的新建会话速率进行限制。IP 限速日志可对限速的数据进行展示。本功能的支持情况与设备实际情况有关，请以设备实际情况为准。

IP 限速日志的展示功能需要在“系统 > 日志设置 > 存储空间设置”页面内开启“攻击检测与防范 | IP 限速日志”后生效，当源自或发往某 IP 地址的新建连接的速率超过配置的阈值后，设备将输出日志到 IP 限速日志页面。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 日志的导入、导出和清除操作不能同时进行。同一时间只能选择一种操作方式。
- 同一时间，只能有一个用户对日志进行导入、导出或删除的操作。

配置指南

日志导入

日志支持导入功能，用户可单击<导入>按钮，在弹出的提示框中单击<确定>，进入导入界面。选择导入的日志文件并输入日志文件的密码，即可将日志导入设备中。

日志导出

设备支持将日志导出到 PC 本地。具体步骤如下：

1. 单击“监控 > 日志 > 安全类”，进入安全类日志页面，在列表上方的下拉框中选择“IP 限速日志”。

2. 单击显示列的<  >过滤器按钮，配置日志的查询条件，单击<确定>按钮，筛选出需要导出的日志。单击列表右上方的<  >过滤器按钮，可以保存当前的查询条件。

3. 单击<导出>按钮，进入“导出日志”页面。配置日志导出参数，具体参数如下表所示：

表-1 日志导出参数表

参数	说明
设置密码	用于设置日志文件的密码，日志文件会被加密导出，导出后的文件需要输入 可以查看
导出条数	用于设置每个日志文件中可以包含的日志条数 • 当日志实际数量小于或等于配置的导出条数时，设备会将所有日志导出 • 当日志实际数量大于配置的导出条数时，设备会按照配置的导出条数， 出到多个文件中

4. 完成日志导出参数的配置后，单击<导出>按钮，设备会将日志文件导出到 PC 本地。

沙箱日志

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 日志导入
  - 日志导出
- 附录

特性简介

用户可通过沙箱日志查看沙箱检测的结果，包括报文基本信息、检测文件的基本信息以及检测文件是否携带威胁等。

其中，威胁分类和威胁行为字段取值的具体内容请参见“附录”。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 日志的导入、导出和清除操作，不能同时进行。同一时间只能选择一种操作方式。
- 同一时间，只能有一个用户对日志进行导入、导出或清除的操作。
- 沙箱日志的详细信息仅支持以 JSON 格式显示。
- 附录中字段的取值与沙箱的软件版本有关，请以实际情况为准。

配置指南

日志导入

日志支持导入功能。具体步骤如下：

1. 单击“监控 > 日志 > 安全类”，进入安全类日志页面，在页面中选择“沙箱日志”。

2. 单击<导入>按钮，进入“导入日志”页面，选择导入的日志文件并输入日志文件的密码，单击<确定>按钮，即可将日志导入设备中。

日志导出

设备支持将日志导出到 PC 本地。具体步骤如下：

1. 单击“监控 > 日志 >安全类”，进入安全类日志页面，在页面中选择“沙箱日志”。
2. 单击显示列的<  >过滤器按钮，配置日志的查询条件，单击<确定>按钮，筛选出需要导出的日志。
3. 单击<导出>按钮，进入“导出日志”页面，配置日志导出参数，具体参数如下表所示：

表-1 日志导出参数表

参数	说明
设置密码	用于设置日志文件的密码，日志文件会被加密导出，导出后的文件需要输入 可以查看
导出条数	用于设置每个日志文件中可以包含的日志条数 • 当日志实际数量小于或等于配置的导出条数时，设备会将所有日志导出 • 当日志实际数量大于配置的导出条数时，设备会按照配置的导出条数， 出到多个文件中

4. 完成日志导出参数的配置后，单击<导出>按钮，设备会将日志文件导出到 PC 本地中。

附录

表-2 威胁分类取值对应表

ID	威胁分类
0	其它
1	病毒
2	木马
3	蠕虫
4	后门
5	勒索软件
6	下载器
7	广告
8	脚本
9	宏病毒
10	恶意漏洞文件
11	网络钓鱼
12	风险工具

13	加壳软件
14	启发式行为
15	数字货币
16	僵尸网络
17	APT情报
18	DGA恶意域名

表-3 威胁行为取值对应表

ID	威胁行为
1	设置开机自启动行为
2	包含远程注入其他进程行为
3	设置降低防火墙安全级别，或者加入白名单
4	设置绕过UAC，提升自身到管理员权限行为
5	禁用修改系统保护机制
6	检测系统中是否安装或运行杀软
7	检测自身是否在沙箱中运行，或者被调试器调试
8	有自己删除本地文件的行为

9	有DLL劫持或者映像劫持行为
10	替换自身为windows自带的exe或dll文件
11	文件名和系统关键进程相近，假冒关键进程
12	感染现有PE文件
13	加载驱动程序
14	修改IE安全策略
15	添加修改windows账号
16	添加修改windows服务
17	文档类进程有可疑网络连接行为
18	文档类进程创建可疑进程释放可疑文件
19	文档类释放可执行程序
20	自动关机重启注销
21	PE文件执行释放文档脚本类文件
22	修改host文件
23	Hook程序关键函数，修改程序流程
24	提升程序本身权限
25	脚本文件调用powershell行为

26	脚本文件恶意网络行为
27	访问敏感文件如浏览器的用户名密码文件
28	Android软件话费吸取
29	Android软件恶意广告
30	Android软件窃取隐私
31	文件类型欺骗
32	修改文件隐藏属性
33	可执行文件恶意的网络行为
34	恶意的快捷方式文件
35	可疑的宏文件
200	病毒
201	间谍木马
202	蠕虫
203	后门
204	勒索软件
205	downloader
206	广告

207	脚本病毒
208	恶意漏洞文件
209	病毒生成器
210	加壳软件
211	启发式行为
212	风险工具
213	网络钓鱼
214	宏病毒
215	其他威胁类型

连接数限制日志

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 日志导入
  - 日志导出

特性简介

连接数限制日志用于展示设备上的连接数到达限制阈值后产生的日志信息，首先需要在“策略 > 主动防护 > 并发连接限制”页面配置并发连接限制策略，然后还需要在“系统 > 日志设置 > 存储空间设置”页面开启“连接数限制 | 连接数限制日志”，当设备连接数到达策略限制阈值时便会产生日志并展示在该页面。本功能的支持情况与设备实际情况有关，请以设备实际情况为准。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 日志的导入、导出和清除操作，不能同时进行。同一时间只能选择一种操作方式。
- 同一时间，只能有一个用户对日志进行导入、导出或清除的操作。

配置指南

日志导入

日志支持导入功能，用户可单击<导入>按钮，在弹出的提示框中单击<确定>，进入导入界面。在界面选择导入的日志文件并输入日志文件的密码，即可将日志导入设备中。

日志导出

日志支持导出功能，具体步骤如下：

1. 单击“监控 > 安全类日志 > 连接数限制日志”，进入连接数限制日志页面。
2. 单击显示列的<  >过滤器按钮，配置日志的查询条件，单击<确定>按钮，筛选出需要导出的日志。
3. 单击<导出>按钮，进入“导出日志”页面。
4. 配置日志导出参数，具体参数如下表所示：

图-1 日志导出参数表

参数	说明
设置密码	日志文件会被加密导出，导出后的文件需要输入设置的密码才可以查看
导出条数	用于设置每个日志文件中可以包含的日志条数 • 当日志实际数量小于或等于配置的导出条数时，设备会将所有日志导出 • 当日志实际数量大于配置的导出条数时，设备会按照配置的导出条数，出到多个文件中

5. 完成日志导出参数的配置后，单击<导出>按钮，设备会将日志文件导出到 PC 本地中。

安全策略日志

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 日志导入
  - 日志导出

特性简介

在安全策略中开启记录日志功能后，然后还需要在“存储空间设置”页面使能“安全策略 | 安全策略日志”，报文与安全策略成功匹配后就会输出安全策略日志并显示在该页面中。管理员可以在安全策略日志页面查看设备上生成的所有安全策略日志信息，这些安全策略日志信息有利于管理员对用户行为进行审计或进行网络故障排查。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 日志的导入、导出和清除操作，不能同时进行。同一时间只能选择一种操作方式。
- 同一时间，只能有一个用户对日志进行导入、导出或清除的操作。

配置指南

日志导入

日志支持导入功能，用户可单击<导入>按钮，在弹出的提示框中单击<确定>，进入导入界面。在界面选择导入的日志文件并输入日志文件的密码，即可将日志导入设备中。

日志导出

日志支持导出功能，具体步骤如下：

1. 单击显示列的<  >过滤器按钮，配置日志的查询条件，单击<确定>按钮，筛选出需要导出的日志。
2. 单击<导出>按钮，进入“导出日志”页面。
3. 配置日志导出参数，具体参数如下表所示：

表-1 日志导出参数表

参数	说明
设置密码	日志文件会被加密导出，导出后的文件需要输入设置的密码才可以查看
导出条数	用于设置每个日志文件中可以包含的日志条数 • 当日志实际数量小于或等于配置的导出条数时，设备会将所有日志导出到一个文件中 • 当日志实际数量大于配置的导出条数时，设备会按照配置的导出条数，将日志分批导出到多个文件中

4. 完成日志导出参数的配置后，点击<导出>按钮，即可导出日志。

NAT 转换日志

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 日志导入
  - 日志导出

特性简介

NAT 转换日志记录了 NAT44 会话的相关信息，包括 IP 地址和端口的转换信息、用户的访问信息以及用户的网络流量信息。

NAT 转换日志的展示功能需要在 “系统 > 日志设置 > 存储空间设置” 里面开启 “网络地址转换 | NAT 转换日志"功能后生效，当报文与策略成功匹配后将输出日志到 NAT 转换日志页面。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 日志的导入、导出和清除操作，不能同时进行。同一时间只能选择一种操作方式。
- 同一时间，只能有一个用户对日志进行导入、导出或清除的操作。

配置指南

日志导入

日志支持导入功能，用户可单击<导入>按钮，在弹出的提示框中单击<确定>，进入导入界面。选择导入的日志文件并输入日志文件的密码，即可将日志导入设备中。

日志导出

设备支持将日志导出到 PC 本地。具体步骤如下：

1. 单击显示列的<  >过滤器按钮，配置日志的查询条件，单击<确定>按钮，筛选出需要导出的日志。

2. 单击<导出>按钮，进入“导出日志”页面，配置日志导出参数，具体参数如下表所示：

   表-1 日志导出参数表

参数	说明
设置密码	用于设置日志文件的密码，日志文件会被加密导出，导出后的文件需要输入 可以查看
导出条数	用于设置每个日志文件中可以包含的日志条数 • 当日志实际数量小于或等于配置的导出条数时，设备会将所有日志导出 • 当日志实际数量大于配置的导出条数时，设备会按照配置的导出条数， 出到多个文件中

3. 完成日志导出参数的配置后，单击<导出>按钮，设备会将日志文件导出到 PC 本地。

流量日志

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 日志导入
  - 日志导出
  - 日志聚合

特性简介

流量日志页面记录了每条数据流产生的流量信息以及流量大小，管理员可通过流量日志信息制定合理、精确的带宽限速策略。

管理员需执行如下任一操作后，流量日志数据才能在页面中显示：

- 在“系统 > 日志设置 > 日志管理”页面的输出到本地区域，开启流量日志及全局开关，并在“系统 > 日志设置 > 存储空间设置”页面开启“流量监控-流量日志”的采集功能。
- 在安全策略中开启流量开始或结束日志输出功能，并在“系统 > 日志设置 > 存储空间设置”页面开启“流量监控-流量日志”的采集功能。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 日志的导入、导出和清除操作，不能同时进行。同一时间只能选择一种操作方式。
- 同一时间，只能有一个用户对日志进行导入、导出或清除的操作。

配置指南

日志导入

日志支持导入功能，用户可单击<导入>按钮，在弹出的提示框中单击<确定>，进入导入界面。选择导入的日志文件并输入日志文件的密码，即可将日志导入设备中。

日志导出

设备支持将日志导出到 PC 本地。具体步骤如下：

1. 单击显示列的<  >过滤器按钮，配置日志的查询条件，单击<确定>按钮，筛选出需要导出的日志。

2. 单击<导出>按钮，进入“导出日志”页面，配置日志导出参数，具体参数如下表所示：

表-1 日志导出参数表

参数	说明
设置密码	用于设置日志文件的密码，日志文件会被加密导出，导出后的文件需要输入密码可以查看
导出条数	用于设置每个日志文件中可以包含的日志条数

	• 当日志实际数量小于或等于配置的导出条数时，设备会将所有日志导出 • 当日志实际数量大于配置的导出条数时，设备会按照配置的导出条数，出到多个文件中

3. 完成日志导出参数的配置后，单击<导出>按钮，设备会将日志文件导出到 PC 本地。

日志聚合

开启日志聚合功能后，设备将对指定聚合时间内采集到的满足相同聚合条件的业务日志进行聚合，可以减少 Web 界面中展示的日志条目，方便用户对日志进行查看。其中，日志聚合条件包括：源 IP 地址、目的 IP 地址、应用和用户。

具体配置步骤如下：

1. 单击<更多操作>按钮，选择日志聚合配置，进入日志聚合配置页面。
2. 开启日志聚合功能，并配置聚合时间。
3. 单击<确定>按钮，完成配置。

系统日志

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 日志导入
  - 日志导出

特性简介

系统日志页面记录了设备在运行过程中产生的相关日志信息，通过查看系统日志信息可以跟踪设备的运行过程、分析网络状况以及定位问题发生的原因，为进行故障诊断和维护提供依据。

首先需要确保在“存储空间设置”页面的“系统日志 | 系统日志”为使能状态（缺省为使能状态），设备产生的系统日志才会显示在该页面中。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 日志的导入、导出和删除操作，不能同时进行。同一时间只能选择一种操作方式。
- 同一时间，只能有一个用户对日志进行导入、导出或删除的操作。
- 待导入的日志文件应为日志导出功能导出的文件，不建议将用户自行加密的日志文件导入设备。

配置指南

日志导入

日志支持导入功能，用户可单击<导入>按钮，在弹出的提示框中单击<确定>，进入导入界面。在界面选择要导入的日志文件并输入日志文件的密码，即可将之前导出的日志重新导入设备中。

日志导出

日志支持导出功能，具体步骤如下：

1. 单击显示列的<  >过滤器按钮，配置日志的查询条件，筛选出需要导出的日志。
2. 单击<导出>按钮，进入“导出日志”页面。
3. 配置日志导出参数，具体参数如下表所示：

表-1 日志导出参数表

参数	说明
设置密码	日志文件会被加密导出，导出后的文件需要输入设置的密码才可以查看
导出条数	每个文件中可以包含的日志条数。当日志实际数量小于等于配置的导出条 日志导出到一个文件中；当日志实际数量大于配置的导出条数时，设备会 条数，将日志分批导出到多个文件中

4. 单击<导出>按钮，即可导出日志。

配置日志

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 日志导入
  - 日志导出

特性简介

配置日志页面记录了管理员配置设备的过程，通过查看配置日志信息可以跟踪管理员对设备的操作，有利于对管理员操作设备的行为进行审计以及进行设备故障排查。

管理员需要先在“存储空间设置”页面使能“系统日志 | 配置日志”功能，才能在配置日志页面查看配置日志信息。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 日志的导入、导出和清除操作，不能同时进行。同一时间只能选择一种操作方式。
- 同一时间，只能有一个用户对日志进行导入、导出或清除的操作。
- 待导入的日志文件应为日志导出功能导出的文件，不建议将用户自行加密的日志文件导入设备。
- 若要查看配置日志，需要先在“存储空间设置”页面开启“系统日志 | 配置日志”。

配置指南

日志导入

日志支持导入功能，用户可单击<导入>按钮，在弹出的提示框中单击<确定>，进入导入界面。在界面选择导入的日志文件并输入日志文件的密码，即可将之前导出的日志重新导入设备中。

日志导出

日志支持导出功能，具体步骤如下：

1. 单击显示列的<  >过滤器按钮，配置日志的查询条件，单击<确定>按钮，筛选出需要导出的日志。
2. 单击<导出>按钮，进入“导出日志”页面。
3. 配置日志导出参数，具体参数如下表所示：

表-1 日志导出参数表

参数	说明
设置密码	日志文件会被加密导出，导出后的文件需要输入设置的密码才可以查看
导出条数	用于设置每个日志文件中可以包含的日志条数 • 当日志实际数量小于或等于配置的导出条数时，设备会将所有日志导出 • 当日志实际数量大于配置的导出条数时，设备会按照配置的导出条数，出到多个文件中每个文件中可以包含的日志条数：

4. 完成日志导出参数的配置后，单击<导出>按钮，设备会将日志文件导出到 PC 本地中。

终端识别日志

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 配置指南

特性简介

终端识别日志记录了在视频安全场景中系统所识别终端的详细信息，包括终端 ID、IP 地址、接入接口、MAC 地址等。通过终端识别日志，管理员可实时掌握设备所接入终端的详细信息以及终端信息发生的变化。

管理员必须先购买并正确安装终端识别 License，确保终端识别功能处于可用状态，然后在终端页面开启终端识别日志功能，并在“存储空间设置”页面使能“DPI 深度安全 | 终端识别日志”后，当有新的终端被识别或终端信息发生变化时，才会输出终端识别日志并显示在该页面中。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 日志的导入、导出和清除操作，不能同时进行。同一时间只能选择一种操作方式。
- 同一时间，只能有一个用户对日志进行导入、导出或清除的操作。

配置指南

导出终端识别日志

终端识别日志支持导出功能，具体步骤如下：

1. 单击显示列的<  >过滤器按钮，配置日志的查询条件，筛选出需要导出的日志。
2. 单击<导出 Excel>按钮，用户可以选择不同的导出方式：
    - 下载当前页不包含隐藏列：导出的 Excel 文件中仅包含当前页面显示的列内容，不包含隐藏的列内容。

- 下载当前页包含隐藏列：导出的 Excel 文件中包含当前页面显示的列内容以及隐藏的列内容。

攻击与溯源

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 公共配置
  - 视图配置
  - 应用分析
  - 用户分析
  - 源地址分析
  - 目的地址分析
  - 源安全域分析
  - 目的安全域分析
  - 安全策略分析
  - 威胁分析

- Web 应用防护分析
- 关键字分析

特性简介

攻击与溯源用于针对不同的视角，对业务的统计数据进行综合展示。

可通过如下视图（即显示模块）多维度分析业务统计数据：应用分析、用户分析、源地址分析、目的地址分析、安全策略分析、源安全域分析、目的安全域分析、威胁分析、关键字分析和 Web 应用防护分析。

各视图下，支持显示如下业务的统计信息：

- 流量：可帮助用户了解流量分布情况。
- 会话：可帮助用户查看会话占用情况，了解哪些应用、用户和 IP 地址等在大量的新建会话，占用会话数量。
- 威胁业务：可帮助用户了解各类威胁攻击情况。
- URL 过滤业务：可帮助用户了解网站访问情况。
- 文件过滤业务：可帮助用户了解敏感文件过滤情况。
- 数据过滤业务：可帮助用户了解敏感信息的过滤情况。
- WAF（Web 应用防护）业务：可帮助用户了解 Web 攻击情况。

各视图下支持显示的业务不同，请以设备实际情况为准。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

当设备从不支持攻击与溯源功能的软件版本升级到支持的版本后，设备只对升级后新生成的数据进行应用分析。

当数据量较大、查询时间范围较广或开启了兼容旧数据查询功能时，可能出现分析时间过长的情况，请耐心等待或暂时切换到其他页面进行其他操作，本功能页面会保持活跃并继续执行查询。

配置指南

公共配置

在攻击与溯源界面支持如下公共配置，配置后将对所有视图生效。

选择查询时间范围

表示仅展示指定时间范围内的统计信息。单击时间右侧的下拉框，可配置查询时间范围。

选择虚拟设备

表示仅展示指定虚拟设备下的统计信息。单击虚拟设备右侧的下拉框，选择虚拟设备。

选择虚拟系统

表示仅展示指定虚拟系统下的统计信息。单击虚拟系统右侧的下拉框，选择虚拟系统。

选择显示模块

表示仅展示指定视角的统计信息。单击<选择显示模块>按钮，可勾选需要查看的视图。

添加全局过滤条件

表示仅展示符合指定过滤条件的统计信息。单击<+过滤条件>按钮，在下拉框中选择过滤条件类型，在输入框或下拉框中输入或选择具体的过滤条件。如需删除过滤条件，可将鼠标悬浮在指定过滤条件上，单击右侧的<X>按钮，删除指定的过滤条件。

兼容旧数据查询

当软件版本从旧分支升级到新分支版本时，硬盘中会保留原有旧分支的数据。缺省情况下，设备仅对版本升级后新生成的数据进行分析；开启本功能后，设备将对硬盘中原有的旧数据以及新生成的数据均进行分析。

视图配置

在各视图下，支持配置如下功能，配置后仅对指定的视图生效。

查看更多数据

各视图下，默认显示 TOP 10 的数据，可单击视图标题栏右侧的<  >按钮，查看更多的统计数据。

添加本地过滤器

各视图下，可以配置仅对当前视图生效的过滤条件，单击视图标题栏右侧的<  >按钮，添加过滤条件。

切换业务

单击视图标题栏下方的<  >按钮，可以切换到不同业务，针对各业务查看统计详细信息。目前，支持的业务包括：流量、会话、威胁、URL 过滤、文件过滤、数据过滤和 WAF。切换业务后，会

根据业务的统计值进行排序。例如，在应用分析视图下，单击统计表中的“流量”，视图中的统计图和统计表将按照流量值对应用进行排序。

支持统计图和统计表展示数据

视图中提供统计图和统计表展示统计数据。

视图中提供多种统计图展示统计数据，支持的统计图类型包括：矩形树图（  ）、面积图（  ）、折线图（  ）和柱状图（  ）。各视图对统计图类型的支持情况不同，请以各视图的实际情况为准。

单击视图标题栏下方的各个统计图按钮，可切换到不同的统计图界面。其中，面积图支持下钻功能。例如，在应用分析视图下，用户单击 E-Mail 区域，图中将出现 126 邮箱和 163 邮箱等子分类，统计表会将 E-mail 作为过滤条件，仅显示出其子分类的统计数据。以此类推，用户可以继续单击 126 邮箱区域，统计表中将显示出 126 邮箱的统计数据。

统计表默认展示 TOP 10 的数据，如果需要查看更多数据，可单击表格下方的“其他”下拉框中的“查看更多数据”。

鼠标悬浮在非计数列 (如应用名称)，显示下拉按钮，单击此按钮，可以选择“添加到全局过滤器”、“添加到本地过滤器”或者其他选项。

应用分析

应用分析视图下可直观展示出各应用的使用状况以及各业务中针对应用的统计信息。方便管理员针对应用调整相关策略配置。

使用面积图展示统计数据时，用户可以直观地了解到哪些类型的应用占用了大量的带宽资源，并可以单击指定的应用类型下钻查看具体应用的统计信息。

用户分析

用户分析视图下可直观展示出各用户的流量使用状况、会话数、访问 URL 次数等统计信息。方便管理员针对用户调整相关策略配置。

源地址分析

源地址分析视图下可直观展示出各源地址的流量使用状况、会话数、访问 URL 次数等统计信息。方便用户针对源地址调整相关策略配置。

目的地址分析

目的地址分析视图下可直观展示出各目的地址的流量使用状况、会话数、访问 URL 次数等统计信息。方便用户针对目的地址调整相关策略配置。

源安全域分析

源安全域分析视图下可直观展示出各源安全域的流量使用状况、会话数、访问 URL 次数等统计信息。方便用户针对源安全域调整相关策略配置。

目的安全域分析

目的安全域分析视图下可直观展示出各目的安全域的流量使用状况、会话数、访问 URL 次数等统计信息。方便用户针对目的安全域调整相关策略配置。

安全策略分析

安全策略分析页面用于查看各安全策略的匹配情况，方便管理员调整安全策略配置。

威胁分析

威胁分析页面用于查看设备检测到的威胁攻击情况，方便管理员针对具体的威胁行为调整相关策略。

Web 应用防护分析

Web 应用防护分析页面用于查看设备检测到的 Web 攻击情况，方便管理员针对具体的攻击行为调整相关策略。

关键字分析

关键字分析页面用于查看用户传输文件、收发邮件、访问网站等操作时是否涉及敏感信息的传输，方便管理员灵活调整相关策略，降低机密信息和用户敏感信息泄露的风险。

僵尸网络

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 日志导入
  - 日志导出
  - 配置内网资产地址范围

特性简介

设备对所有与僵尸网络相关的安全日志（包括入侵防御日志、防病毒日志、Web 应用防护日志、文件过滤日志、URL 过滤日志以及信誉日志）进行综合分析，展示了疑似僵尸主机的 IP 地址、对端地址等信息。可帮助用户识别和定位具体的僵尸网络主机，并采取相应防范措施。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 本功能仅当设备正确安装硬盘或 U 盘后可用。
- 为了提高分析结果的准确性，请确保僵尸网络相关的安全业务（如入侵防御、防病毒等业务）的日志记录功能已开启。

配置指南

日志导入

管理员可以通过导入日志文件，对文件中的日志信息进行僵尸网络分析。

单击<导入>按钮，在弹出的提示框中单击<确定>，进入导入界面。选择导入的日志文件并输入日志文件的密码，即可将日志导入到设备中。

日志导出

设备支持将所有与僵尸网络相关的安全日志导出到 PC 本地。具体步骤如下：

1. 单击显示列的<  >过滤器按钮，配置日志的查询条件，单击<确定>按钮，筛选出需要导出的日志。

2. 单击<导出>按钮，进入“导出日志”页面，配置日志导出参数，具体参数如下表所示：

表-1 日志导出参数表

参数	说明
设置密码	用于设置日志文件的密码，日志文件会被加密导出，导出后的文件需要输入 可以查看
导出条数	用于设置每个日志文件中可以包含的日志条数 • 当日志实际数量小于或等于配置的导出条数时，设备会将所有日志导出 • 当日志实际数量大于配置的导出条数时，设备会按照配置的导出条数， 出到多个文件中

3. 完成日志导出参数的配置后，单击<导出>按钮，设备会将日志文件导出到 PC 本地中。

配置内网资产地址范围

当用户需要对资产流量进行统计分析时，需要配置资产地址范围。设备会将指定的地址范围识别为内网，范围外的地址识别为外网，并对内网-内网、内网-外网、外网-内网间的流量进行分析。若未配置资产地址范围，设备将只分析 Trust-Trust、Trust-Untrust、Untrust-Trust 安全域间的流量，并将 Trust 域识别为内网，Untrust 域识别为外网，其他安全域的流量不进行分析。

具体配置步骤如下：

1. 单击页面上方的<资产地址>按钮，进入内网资产地址范围页面。
2. 根据实际需求配置资产地址。

安全分析

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
- 附录

特性简介

设备支持对主机的安全状况进行分析，统计存在安全威胁的主机数目以及安全事件的分布状态，并以图表形式展示。用户可以查看主机的安全状况综述，也可查看单一主机的详细安全分析报告。

其中，用户需要根据实际需求配置资产地址范围，设备会将指定的地址范围识别为内网，范围外的地址识别为外网，并对内网-内网、内网-外网、外网-内网间的流量进行分析。若未配置资产地址范围，设备将只分析 Trust-Trust、Trust-Untrust、Untrust-Trust 安全域间的流量，并将 Trust 域识别为内网，Untrust 域识别为外网，其他安全域的流量不进行分析。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 单一主机的详细安全分析报告中支持展示最近 7 天、14 天和 30 天的数据。
- 当页面没有可以显示的数据时，可能的原因如下：
  - 当前设备未检测到攻击，所以没有可以展示的数据。
  - 当前流量可能不在分析的资产地址范围内。
  - 设备未正确安装硬盘或 U 盘。
- 当设备重新启动后，系统会对重启前未完成分析的历史数据继续进行分析，如果历史数据较多，可能导致系统无法及时对新产生的统计数据进行分析，请耐心等待。

配置指南

1. 选择“监控 > 综合分析 > 安全分析”，进入安全分析页面，可查看所有主机的安全事件分布状态统计数据、漏洞分析等级统计信息。

2. 单击页面右上角的<资产地址>按钮，配置资产地址范围。

3. 管理员可以通过配置主机 IP、综合风险等级和漏洞分析等级过滤条件，对展示的主机进行筛选。其中，综合风险等级对应的含义请参见附录。

4. 单击页面下方指定的主机 IP，可进入该主机的安全分析详情页面，查看该主机的详细安全分析报告。包括该主机的基本信息（例如主机名、综合风险等级等）、威胁信息和攻击事件列表。其中，单击“威胁信息”下的指定攻击阶段以及“详情”下的事件类型标签，可以筛选出符合条件的攻击事件。单击部分事件类型标签支持展示该类型事件的解决方案。

5. 单击指定主机右侧操作下的<封锁>按钮，可选择将该主机地址作为源地址或者目的地址下发到黑名单中，实现对该地址的封锁。需要注意，该主机地址在黑名单中永不老化，如需修改老化时间，请到黑名单页面进行修改。缺省情况下，只能封锁公网主机地址。

6. 管理员可以根据上述分析数据，采取针对性的防范措施。

附录

表-1 综合风险等级取值对应表

综合风险等级	说明
有漏洞	检测出主机存在漏洞，目前尚未遭到攻击。例如通过漏洞扫描检测到主机开放了138、139危险端口等
被攻击	检测出主机受到了恶意攻击，例如DDoS、SQL注入攻击、僵尸程序等

已受控	有证据证明主机存在异常外联行为，例如与C&C服务器通信、与已知恶意软件和网络蠕虫等关联的IP、URL或域名通信
已扩散	检测到主机存在攻击其他主机的行为，例如端口扫描、暴力破解等
已受损	检测到主机存在文件泄露、危害其他主机或数据库等行为。例如，挖矿、勒索等

URL 过滤

本帮助主要介绍以下内容：

- 特性简介
  - 分类排行
  - 网站排行
  - 源 IP 地址排行
  - 目的 IP 地址排行
  - 分类趋势
  - 网站趋势
  - 源地址趋势
  - 目的地址趋势
- vSystem 相关说明

特性简介

本功能用来对用户访问的 URL 进行统计排行和访问趋势分析。管理员可通过柱状图、饼状图和列表查看统计排行结果，也可查看用户访问 URL 的高峰时间段，频繁访问的网站和网站类型等信息，方便管理员了解用户上网情况并制定相应的 URL 过滤策略，禁止用户访问某些网页资源，规范用户上网行为。

管理员可单击<统计条件>按钮，配置多种统计条件，基于 URL 分类等维度进行 URL 过滤统计排行和访问趋势分析。

单击<报表导出>按钮，设备将立即根据当前统计条件查询到的统计数据生成一份 PDF 格式的报表文件，并导出到浏览器。管理员可通过查看报表文件了解当前用户的上网情况。

分类排行

管理员可根据网站分类对用户访问次数进行统计排行，方便管理员针对网站分类调整防护策略。支持配置的统计条件如下表所示：

表-1 分类排行统计条件

参数	说明
统计时间	统计的时间范围，取值包括：

	• 今天 • 最近一周 • 最近三十天 • 自定义
排行显示	显示排名的分类数

单击<开始统计>按钮，设备将根据配置的统计条件对网站分类进行访问次数排名。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

网站排行

管理员可根据网站对用户访问次数进行统计排行，方便管理员查看用户访问网站的情况，调整防护策略。支持配置的统计条件如下表所示：

表-2 网站排行统计条件

参数	说明
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天

	• 自定义
排行显示	显示排名的网站数

单击<开始统计>按钮，设备将根据配置的统计条件对网站进行访问次数排名。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

源 IP 地址排行

管理员可根据发起访问的源 IP 地址对用户访问次数进行统计排行，方便管理员针对源 IP 地址调整防护策略，规范用户的上网行为。支持配置的统计条件如下表所示：

表-3 源 IP 地址排行统计条件

参数	说明
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义
排行显示	显示排名的源IP地址数

单击<开始统计>按钮，设备将根据配置的统计条件对源 IP 地址进行访问次数排名。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

目的 IP 地址排行

管理员可根据被访问的目的 IP 地址对用户访问次数进行统计排行，方便管理员针对目的 IP 地址调整防护策略，规范用户的上网行为。支持配置的统计条件如下表所示：

表-4 目的 IP 地址排行统计条件

参数	说明
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义
排行显示	显示排名的目的IP地址数

单击<开始统计>按钮，设备将根据配置的统计条件对目的 IP 地址进行访问次数排名。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

分类趋势

管理员可根据 URL 分类应用查看 URL 过滤趋势，方便基于 URL 分类调整 URL 过滤策略。支持配置的统计条件如下表所示：

表-5 分类趋势统计条件

参数	说明
分类范围	统计的URL分类，取值包括： • Top5 URL 分类 • 指定 URL 分类
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义

单击<开始统计>按钮，设备将根据配置的统计条件对访问的 URL 分类情况进行统计。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

网站趋势

管理员可根据网站查看 URL 过滤趋势，方便查看频繁访问的网站 URL，从而调整 URL 过滤策略。

支持配置的统计条件如下表所示：

表-6 网站趋势统计条件

参数	说明
网站范围	统计的网站范围，取值包括： • Top5 网站 • 指定网站
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义

单击<开始统计>按钮，设备将根据配置的统计条件对访问的网站 URL 进行统计。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

源地址趋势

管理员可根据发起访问的源地址查看 URL 过滤趋势，方便针对源地址调整 URL 过滤策略。支持配置的统计条件如下表所示：

表-7 源地址趋势统计条件

参数	说明
源地址范围	统计的源地址范围，取值包括： • Top5 源地址 • 指定源地址
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义

单击<开始统计>按钮，设备将根据配置的统计条件对源地址访问 URL 的情况进行统计。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

目的地址趋势

管理员可根据受到访问的目的地址查看 URL 过滤趋势，方便针对目的地址调整 URL 过滤策略。支持配置的统计条件如下表所示：

表-8 目的地址趋势统计条件

参数	说明
目的地址范围	统计的目的地址范围，取值包括： • Top5 目的地址 • 指定目的地址
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义

单击<开始统计>按钮，设备将根据配置的统计条件对目的地址受到访问的情况进行统计。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

文件过滤

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 配置指南

特性简介

文件过滤功能用来对指定时间内经由设备传输的文件类型进行统计，并使用柱状图、饼状图和列表的形式向用户展示统计排行结果，同时支持展示文件过滤趋势，方便管理员了解用户传输文件的情况，并制定相应的文件过滤策略，降低机密信息泄露风险和内网感染病毒的风险。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

文件类型排行

管理员可根据文件类型查看文件过滤统计排行情况，方便基于文件类型调整文件过滤策略。具体配置步骤如下：

1. 单击<统计条件>按钮，配置多种统计条件，对文件类型进行统计排行。支持配置的统计条件如下表所示：

表-1 文件类型排行统计条件

参数	说明
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义
排行显示	显示排名的文件类型数

2. 单击<开始统计>按钮，设备将根据配置的统计条件对文件类型进行次数排名。

3. 单击<报表导出>按钮，设备将立即根据当前统计条件查询到的统计数据生成一份 PDF 格式的报表文件，并导出到 PC 本地。管理员可通过查看报表文件了解当前用户的文件传输情况。

文件类型趋势

管理员可根据文件类型查看文件过滤趋势，方便基于文件类型调整文件过滤策略。具体配置步骤如下：

1. 单击<统计条件>按钮，配置多种统计条件。支持配置的统计条件如下表所示：

表-2 文件类型排行统计条件

参数	说明
文件类型范围	统计的文件类型，取值包括： • Top5 文件类型 • 指定文件类型
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义

2. 单击<开始统计>按钮，设备将根据配置的统计条件对设备传输的文件类型进行统计。

3. 单击<报表导出>按钮，设备将立即根据当前统计条件查询到的统计数据生成一份 PDF 格式的报表文件，并导出到 PC 本地。管理员可通过查看报表文件了解当前的文件传输情况。

攻击防范统计

本帮助主要介绍以下内容：

- 特性简介
  - 攻击防范
  - 客户端验证
  - 黑名单
  - 白名单
- vSystem 相关说明

特性简介

攻击防范

攻击防范统计页面用来记录设备受到的攻击类型、攻击次数以及因为攻击导致的丢包数。

客户端验证

客户端验证统计页面用来记录客户端验证的受保护 IP 表项，包括客户端验证类型、受保护 IP 所属的 VRF、受保护 IP 地址、端口、受保护 IP 的添加方式、匹配受保护 IP 的报文数目和通过客户端验证的请求报文数目。

黑名单

黑名单统计页面用来记录 IP 黑名单表项，包括 VRF、加入黑名单的 IP 地址、DS-Lite 隧道对端地址、表项的添加方式、表项的剩余老化时间、备注信息和因匹配黑名单而丢包的报文数。

白名单

白名单统计页面用来记录白名单表项，包括加入白名单对象组的类型、名称和匹配的报文数。

vSystem相关说明

非缺省 VSystem 对于本特性的支持情况，请以页面的实际显示为准。

用户行为与画像

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- License 支持情况

特性简介

用户行为与画像用于查看用户的上网行为，包括访问的应用、网站、邮件和传输文件情况等，方便管理员对用户进行审计。

管理员可在选择日期与指定的用户后单击<查询>按钮，查看详细的用户信息，包括用户上网行为的统计信息，访问应用和网站的流量分析等。

应用流量分析需要管理员在“系统 > 会话设置 > 高级设置”页面中开启会话统计功能，并在“系统 > 日志设置 > 存储空间设置”页面中开启流量日志业务的日志采集功能后才可以显示在页面中。

用户访问网站分析需要管理员在 URL 过滤策略中开启日志功能，并在“系统 > 日志设置 > 存储空间设置”页面中开启 URL 过滤日志业务的日志采集功能后才可以显示在页面中。有关 URL 过滤策略的详细介绍，请参见“URL 过滤联机帮助”。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

License支持情况

应用审计功能需要基于 APR（应用识别）特征库来进行识别。License 过期后，应用审计功能可以采用设备中已有的 APR 特征库正常工作，但无法升级特征库。关于 License 的详细介绍请参见“License 联机帮助”。

IPv4 在线用户

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明

特性简介

IPv4 在线用户列表显示了当前所有在线 IPv4 用户的信息，通过查看该列表可获取当前在线用户接入网络的设备接口、IPv4 地址、登录时间等信息。

首先需要在“网络 > 安全接入 > IP 接入 > IP 地址认证”页面开启 IPv4 接口的 IP 接入认证功能，当用户从该接口接入并认证成功，当前页面即可显示该在线用户的信息。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

IPv6 在线用户

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明

特性简介

IPv6 在线用户列表显示了当前所有在线 IPv6 用户的信息，通过查看该列表可获取当前在线用户接入网络的设备接口、IPv6 地址、登录时间等信息。

首先需要在“网络 > 安全接入 > IP 接入 > IP 地址认证”页面开启 IPv6 接口的 IP 接入认证功能，当用户从该接口接入并认证成功，当前页面即可显示该在线用户的信息。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

MAC 认证在线用户

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明

特性简介

MAC 认证在线用户列表显示了当前所有在线 MAC 认证用户的信息，通过查看该列表可获取当前在线用户接入网络的设备接口、MAC 地址、授权 VLAN、登录时间等信息。管理员可对指定在线用户执行强制下线操作。

首先需要在“网络 > 安全接入 > MAC 接入 > MAC 地址认证”页面开启全局和接口 MAC 认证功能，当用户从该接口接入并认证成功，当前页面即可显示该在线用户的信息。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

用户统计

本帮助主要介绍以下内容：

- 特性简介
  - 流量
  - 威胁
  - URL 过滤
- vSystem 相关说明

特性简介

用户统计功能用于对特定时间段内设备上的用户流量、用户相关威胁事件（包括入侵防御和防病毒事件）以及用户访问的 URL 进行统计排行。统计结果以柱状图、饼状图和列表的形式展示，便于管理员了解不同用户的带宽消耗、安全风险以及 URL 访问行为，从而调整相应的带宽管控类策略、安全防护类策略以及 URL 过滤策略等。

管理员可单击<统计条件>按钮，配置多种统计条件进行流量、威胁次数和 URL 访问次数统计排行。

单击<报表导出>按钮，设备将立即根据当前统计条件查询到的统计数据生成一份 PDF 格式的报表文件，并导出到 PC 本地。管理员可通过查看报表文件了解用户的流量使用情况、安全风险以及上网行为。

流量

管理员可根据用户对流量进行统计排行，方便管理员对用户的带宽占用情况进行分析。支持配置的统计条件如下表所示：

表-1 流量统计条件

参数	说明
流量类型	统计的流量类型，取值包括： • 上行流量 • 下行流量 • 总流量
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义

排行显示	显示排名的用户数

单击<开始统计>按钮，设备将根据配置的统计条件对用户的流量使用情况进行排名。

生成统计结果后，管理员可单击指定的用户，进入“应用排行”页面，查看用户访问应用的流量使用情况。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

威胁

管理员可根据用户查看威胁趋势，方便基于用户调整防护策略。支持配置的统计条件如下表所示：

表-2 威胁统计条件

参数	说明
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义
排行显示	显示排名的用户数

单击<开始统计>按钮，设备将根据配置的统计条件对用户受到的威胁情况进行统计。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

URL 过滤

管理员可根据用户对访问的网站进行统计排行，方便管理员查看用户的上网情况。支持配置的统计条件如下表所示：

表-3 URL 过滤统计条件

参数	说明
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义
排行显示	显示排名的用户数

单击<开始统计>按钮，设备将根据配置的统计条件对用户进行访问次数排名。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

用户统计

本帮助主要介绍以下内容：

- 特性简介
  - 流量
  - 威胁
  - URL 过滤
- vSystem 相关说明

特性简介

用户统计功能用于对特定时间段内设备上的用户流量、用户相关威胁事件（包括入侵防御和防病毒事件）以及用户访问的 URL 进行统计排行。统计结果以柱状图、饼状图和列表的形式展示，便于

管理员了解不同用户的带宽消耗、安全风险以及 URL 访问行为，从而调整相应的带宽管控类策略、安全防护类策略以及 URL 过滤策略等。

管理员可单击<统计条件>按钮，配置多种统计条件进行流量、威胁次数和 URL 访问次数统计排行。

单击<报表导出>按钮，设备将立即根据当前统计条件查询到的统计数据生成一份 PDF 格式的报表文件，并导出到 PC 本地。管理员可通过查看报表文件了解用户的流量使用情况、安全风险以及上网行为。

流量

管理员可根据用户对流量进行统计排行，方便管理员对用户的带宽占用情况进行分析。支持配置的统计条件如下表所示：

表-1 流量统计条件

参数	说明
流量类型	统计的流量类型，取值包括： • 上行流量 • 下行流量 • 总流量
统计时间	统计的时间范围，取值包括： • 今天

	• 最近一周 • 最近三十天 • 自定义
排行显示	显示排名的用户数

单击<开始统计>按钮，设备将根据配置的统计条件对用户的流量使用情况进行排名。

生成统计结果后，管理员可单击指定的用户，进入“应用排行”页面，查看用户访问应用的流量使用情况。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

威胁

管理员可根据用户查看威胁趋势，方便基于用户调整防护策略。支持配置的统计条件如下表所示：

表-2 威胁统计条件

参数	说明
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天

	• 自定义
排行显示	显示排名的用户数

单击<开始统计>按钮，设备将根据配置的统计条件对用户受到的威胁情况进行统计。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

URL 过滤

管理员可根据用户对访问的网站进行统计排行，方便管理员查看用户的上网情况。支持配置的统计条件如下表所示：

表-3 URL 过滤统计条件

参数	说明
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义
排行显示	显示排名的用户数

单击<开始统计>按钮，设备将根据配置的统计条件对用户进行访问次数排名。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

用户趋势

本帮助主要介绍以下内容：

- 特性简介
  - 流量
  - 威胁
  - URL 过滤
- vSystem 相关说明

特性简介

用户趋势功能用于对特定时间段内设备上的用户流量以及用户相关的威胁事件（包括入侵防御和防病毒事件）进行统计。统计结果以折线图的形式展示，便于管理员轻松识别流量、威胁事件和 URL 访问的关键时段，特别是流量发生的高峰与低谷、威胁事件的频发时段和高风险级别事件的发生时段以及 URL 访问的频发时段，从而调整相应的带宽管控类策略、安全防护相关策略以及 URL 过滤策略，有助于更好地分配带宽资源、保护内部网络安全以及管控用户的上网行为。

管理员可单击<统计条件>按钮，配置多种统计条件，查看相应的流量、威胁和 URL 过滤趋势。

单击<报表导出>按钮，设备将立即根据当前统计条件查询到的统计数据生成一份 PDF 格式的报表文件，并导出到 PC 本地。

流量

管理员可根据用户查看流量趋势，方便基于用户的流量情况进行访问控制。支持配置的统计条件如下表所示：

表-1 流量统计条件

参数	说明
用户范围	统计的用户，取值包括： • Top5 用户 • 指定用户
流量类型	统计的流量类型，取值包括： • 上行流量 • 下行流量 • 总流量
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周

	• 最近三十天 • 自定义
应用类型	统计的应用类型
应用	统计指定应用类型中的应用

单击<开始统计>按钮，设备将根据配置的统计条件对用户的流量使用情况进行统计，并展示流量趋势图。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

威胁

管理员可根据用户查看威胁趋势，方便基于用户调整防护策略。支持配置的统计条件如下表所示：

表-2 威胁统计条件

参数	说明
用户范围	统计的用户，取值包括： • Top5 用户 • 指定用户
威胁类型	统计的威胁类型，取值包括：

	• 入侵防御 • 防病毒 • 所有威胁
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义

单击<开始统计>按钮，设备将根据配置的统计条件对用户受到的威胁情况进行统计。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

URL 过滤

管理员可根据用户对访问的网站进行统计排行，方便管理员查看用户的上网情况。支持配置的统计条件如下表所示：

表-3 URL 过滤统计条件

参数	说明
用户范围	统计的用户，取值包括：

	• Top5 用户 • 指定用户
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义

单击<开始统计>按钮，设备将根据配置的统计条件对用户的 URL 访问次数进行统计。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

用户趋势

本帮助主要介绍以下内容：

- 特性简介

    - 流量
    - 威胁
    - URL 过滤
- vSystem 相关说明

特性简介

用户趋势功能用于对特定时间段内设备上的用户流量以及用户相关的威胁事件（包括入侵防御和防病毒事件）进行统计。统计结果以折线图的形式展示，便于管理员轻松识别流量、威胁事件和 URL 访问的关键时段，特别是流量发生的高峰与低谷、威胁事件的频发时段和高风险级别事件的发生时段以及 URL 访问的频发时段，从而调整相应的带宽管控类策略、安全防护相关策略以及 URL 过滤策略，有助于更好地分配带宽资源、保护内部网络安全以及管控用户的上网行为。

管理员可单击<统计条件>按钮，配置多种统计条件，查看相应的流量、威胁和 URL 过滤趋势。

单击<报表导出>按钮，设备将立即根据当前统计条件查询到的统计数据生成一份 PDF 格式的报表文件，并导出到 PC 本地。

流量

管理员可根据用户查看流量趋势，方便基于用户的流量情况进行访问控制。支持配置的统计条件如下表所示：

表-1 流量统计条件

参数	说明
用户范围	统计的用户，取值包括： • Top5 用户 • 指定用户
流量类型	统计的流量类型，取值包括： • 上行流量 • 下行流量 • 总流量
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义
应用类型	统计的应用类型

应用	统计指定应用类型中的应用

单击<开始统计>按钮，设备将根据配置的统计条件对用户的流量使用情况进行统计，并展示流量趋势图。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

威胁

管理员可根据用户查看威胁趋势，方便基于用户调整防护策略。支持配置的统计条件如下表所示：

表-2 威胁统计条件

参数	说明
用户范围	统计的用户，取值包括： • Top5 用户 • 指定用户
威胁类型	统计的威胁类型，取值包括： • 入侵防御 • 防病毒 • 所有威胁

统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义

单击<开始统计>按钮，设备将根据配置的统计条件对用户受到的威胁情况进行统计。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

URL 过滤

管理员可根据用户对访问的网站进行统计排行，方便管理员查看用户的上网情况。支持配置的统计条件如下表所示：

表-3 URL 过滤统计条件

参数	说明
用户范围	统计的用户，取值包括： • Top5 用户 • 指定用户
统计时间	统计的时间范围，取值包括：

	• 今天 • 最近一周 • 最近三十天 • 自定义

单击<开始统计>按钮，设备将根据配置的统计条件对用户的 URL 访问次数进行统计。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

应用统计

本帮助主要介绍以下内容：

- 特性简介
  - 流量
  - 威胁
- vSystem 相关说明

特性简介

应用统计功能用于对特定时间段内设备上的应用流量以及应用相关的威胁事件（包括入侵防御和防病毒事件）进行统计排行。统计结果以柱状图、饼状图和列表的形式展示，便于管理员了解不同应用的带宽消耗和安全风险，从而调整相应的带宽管控类策略和安全防护相关策略。

管理员可单击<统计条件>按钮，配置多种统计条件（例如应用、源 IP 地址）进行流量统计排行和威胁次数统计排行。

单击<报表导出>按钮，设备将立即根据当前统计条件查询到的统计数据生成一份 PDF 格式的报表文件，并导出到 PC 本地。管理员可通过查看报表文件了解设备上的流量使用情况和检测到的威胁事件。

流量

管理员可根据应用对流量进行统计排行，方便管理员对应用占用带宽的情况进行分析。支持配置的统计条件如下表所示：

表-1 流量统计条件

参数	说明
流量类型	统计的流量类型，取值包括： • 上行流量 • 下行流量 • 总流量
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义

查询对象	对指定源IP地址访问的应用进行统计排行
排行对象	统计排行的对象，取值包括： • 应用类别：表示按照应用类型进行统计排行 • 指定应用：表示按照应用进行统计排行
排行显示	显示排名的应用数

单击<开始统计>按钮，设备将根据配置的统计条件对应用占用带宽的情况进行排名。

生成统计结果后，管理员可在排名列表中单击指定的应用，选择跳转页面：

- 源地址：跳转到“源地址流量排行”页面，查看指定应用的源地址访问量排行情况。
- 用户：跳转到“用户排行”页面，查看指定应用的用户访问量排行情况。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

威胁

管理员可根据应用对威胁事件进行统计排行，方便管理员针对应用调整防护策略。支持配置的统计条件如下表所示：

表-2 威胁统计条件

参数	说明
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义
排行显示	显示排名的应用数

单击<开始统计>按钮，设备将根据配置的统计条件对应用进行威胁次数排名。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

应用趋势

本帮助主要介绍以下内容：

- 特性简介
  - 流量
  - 威胁
- vSystem 相关说明

特性简介

应用趋势功能用于对特定时间段内设备上的应用流量以及应用相关的威胁事件（包括入侵防御和防病毒事件）进行统计。统计结果以折线图的形式展示，便于管理员轻松识别流量和威胁事件的关键时段，特别是流量发生的高峰与低谷以及威胁事件的频发时段和高风险级别事件的发生时段，从而调整相应的带宽管控类策略和安全防护相关策略，有助于更好地分配带宽资源和保护内部网络安全。

管理员可单击<统计条件>按钮，配置多种统计条件（例如应用、源 IP 地址），查看相应的流量趋势和威胁趋势。

单击<报表导出>按钮，设备将立即根据当前统计条件查询到的统计数据生成一份 PDF 格式的报表文件，并导出到 PC 本地。管理员可通过查看报表文件了解设备上的流量使用情况和检测到的威胁事件。

流量

管理员可根据应用查看流量趋势，方便管理员针对应用的流量使用情况进行访问控制。支持配置的统计条件如下表所示：

表-1 流量统计条件

参数	说明
应用范围	统计的应用，取值包括： • Top5 应用 • 指定应用
流量类型	统计的流量类型，取值包括： • 上行流量 • 下行流量 • 总流量
统计时间	统计的时间范围，取值包括： • 今天

	• 最近一周 • 最近三十天 • 自定义
查询对象	统计的主机IP地址

单击<开始统计>按钮，设备将根据配置的统计条件对应用的流量使用情况进行统计，并展示流量趋势图。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

威胁

管理员可根据应用查看威胁趋势，方便管理员针对应用调整防护策略。支持配置的统计条件如下表所示：

表-2 威胁统计条件

参数	说明
应用范围	统计的应用，取值包括： • Top5 应用 • 指定应用
统计时间	统计的时间范围，取值包括：

	• 今天 • 最近一周 • 最近三十天 • 自定义

单击<开始统计>按钮，设备将根据配置的统计条件对应用的威胁情况进行统计。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

应用类型趋势

本帮助主要介绍以下内容：

- 特性简介
  - 应用类型趋势
- vSystem 相关说明

特性简介

应用类型趋势功能用于对特定时间段内设备上的不同类型的应用流量进行统。统计结果以折线图展示，便于管理员轻松识别流量的高峰和低谷时段。

管理员可单击<统计条件>按钮，配置多种统计条件，查看基于应用类型的流量趋势。

单击<报表导出>按钮，设备将立即根据当前统计条件查询到的统计数据生成一份 PDF 格式的报表文件，并导出到 PC 本地。管理员可通过查看报表文件了解设备上的流量使用情况。

应用类型趋势

管理员可根据应用类型查看流量趋势，方便基于应用类型的流量情况进行访问控制。支持配置的统计条件如下表所示：

表-1 统计条件

参数	说明
应用类型范围	统计的应用类型，取值包括： • Top5 应用类型 • 指定应用类型
流量类型	统计的流量类型，取值包括： • 上行流量 • 下行流量 • 总流量
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义
查询对象	统计的主机IP地址

单击<开始统计>按钮，设备将根据配置的统计条件对应用类型的流量使用情况进行统计，并展示流量趋势图。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

威胁案件管理

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- License 支持情况
- 使用限制和注意事项
- 配置指南

特性简介

威胁案件管理功能用来对设备生成的威胁日志进行归类管理。设备提供告警资源池来单独存储可疑的威胁日志，并以案件的形式进行管理，可详细追溯、分析日志内容，供用户后续跟踪和总结。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

License支持情况

入侵防御

入侵防御功能需要购买并正确安装 License 后才能使用。License 过期后，入侵防御功能可以采用设备中已有的入侵防御特征库正常工作，但无法升级到官方网站在过期时间后发布的新版本的特征库。关于 License 的详细介绍请参见“License 联机帮助”。

防病毒

防病毒功能需要购买并正确安装 License 才能使用。License 过期后，防病毒功能可以采用设备中已有的病毒特征库正常工作，但无法升级特征库且云端查询功能以及联动沙箱阻断功能无法使用。关于 License 的详细介绍请参见“License 配置联机帮助”。

使用限制和注意事项

告警资源池中的威胁日志如果属于特定的虚拟设备，则只能被加入到该虚拟设备的案件中。

配置指南

威胁案件管理的具体步骤如下：

1. 进入“监控 > 安全类日志 > 威胁日志”页面，选择需要分析的威胁日志，单击<加入告警资源池>按钮，将需要分析的威胁日志加入到“监控 > 威胁分析 > 威胁案件管理 > 告警资源池”中。
2. 进入“监控 > 威胁分析 > 威胁案件管理 > 告警资源池”页面，对资源池的日志进行分析，确认上报的日志是否为真正的攻击。
3. 完成分析后，可单击<加入案件>按钮，将日志以案件的形式进行归档。用户可选择将日志加入已有案件或新建的案件中。加入案件后，可通过如下方式将案件归档，便于后续跟踪分析：
    - 单击案件右侧的<编辑>按钮，进入编辑页面，修改归档状态为归档。
    - 单击案件右侧的<日志>按钮，进入日志页面，单击<归档>按钮，进行归档。
4. 用户可进入“监控 > 威胁分析 > 威胁案件管理 > 案件”页签，查看所有案件信息。单击指定案件右侧的<详情>按钮，可查看案件中的所有日志详情。单击指定案件右侧的<编辑>按钮，可修改案件的归档状态或删除案件中的日志。

威胁统计

本帮助主要介绍以下内容：

- 特性简介
  - 威胁类型排行
  - 威胁名称排行
  - 攻击者排行
  - 攻击对象排行
- vSystem 相关说明
- License 支持情况

特性简介

威胁统计功能用来对设备上检测出的威胁事件（包括入侵防御和防病毒事件）进行统计，并使用柱状图、饼状图和列表的形式向用户展示统计排行结果，方便管理员对威胁情况进行分析，调整相应的防护策略。

管理员可单击<统计条件>按钮，配置多种统计条件，对威胁类型、攻击者、攻击对象和威胁名称进行威胁次数统计排行。

单击<报表导出>按钮，设备将立即根据当前统计条件查询到的统计数据生成一份 PDF 格式的报表文件，并导出到 PC 本地。管理员可通过查看报表文件了解当前用户的威胁情况。

威胁类型排行

管理员可根据威胁类型（入侵防御和防病毒）进行威胁次数统计排行，方便管理员针对频繁发生威胁事件的威胁类型调整入侵防御策略和防病毒策略。支持配置的统计条件如下表所示：

表-1 威胁类型排行统计条件

参数	说明
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义
排行显示	显示排名的威胁类型数

单击<开始统计>按钮，设备将根据配置的统计条件对威胁类型的威胁次数进行统计排行。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

威胁名称排行

管理员可根据威胁名称对威胁次数进行统计排行，方便管理员根据威胁名称调整防护策略。支持配置的统计条件如下表所示：

表-2 威胁名称排行统计条件

参数	说明
威胁类型	统计的威胁类型，取值包括： • 入侵防御 • 防病毒 • 所有威胁
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义
攻击类型	统计的攻击类型，取值包括： • 攻击者 • 攻击对象

	• 所有攻击
排行显示	显示排名的威胁名称数

单击<开始统计>按钮，设备将根据配置的统计条件对威胁名称进行威胁次数统计排名。

生成统计结果后，管理员可单击指定的威胁名称，选择跳转页面：

- 攻击者：跳转到“攻击者排行”页面，查看指定威胁名称的攻击者排行情况。
- 攻击对象：跳转到“攻击对象排行”页面，查看指定威胁名称的攻击对象排行情况。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

攻击者排行

管理员可根据攻击者的 IP 地址对威胁事件进行统计排行，方便管理员根据攻击者调整防护策略。支持配置的统计条件如下表所示：

表-3 攻击者排行统计条件

参数	说明
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周

	• 最近三十天 • 自定义
威胁类型	统计的威胁类型，取值包括： • 入侵防御 • 防病毒 • 所有威胁
排行显示	显示排名的攻击者数

单击<开始统计>按钮，设备将根据配置的统计条件对攻击者进行威胁次数统计排名。

生成统计结果后，管理员可单击指定的攻击者 IP 地址，选择跳转页面：

- 威胁名称：跳转到“威胁名称排行”页面，查看指定攻击者 IP 地址发起威胁的名称排行情况。
- 攻击对象：跳转到“攻击对象排行”页面，查看指定攻击者 IP 地址所攻击的攻击对象排行情况。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

攻击对象排行

管理员可根据攻击对象的 IP 地址对威胁事件进行统计排行，方便管理员根据攻击对象调整防护策略，更好地保护内网用户。支持配置的统计条件如下表所示：

表-4 攻击对象排行统计条件

参数	说明
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义
威胁类型	统计的威胁类型，取值包括： • 入侵防御 • 防病毒 • 所有威胁
排行显示	显示排名的攻击对象数

单击<开始统计>按钮，设备将根据配置的统计条件对攻击对象进行威胁次数统计排名。

生成统计结果后，管理员可单击指定的攻击对象 IP 地址，选择跳转页面：

- 威胁名称：跳转到“威胁名称排行”页面，查看指定攻击对象受到威胁的威胁名称排行情况。
- 攻击者：跳转到“攻击者排行”页面，查看指定攻击对象受到威胁的攻击者排行情况。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

License支持情况

入侵防御

入侵防御功能需要购买并正确安装 License 后才能使用。License 过期后，入侵防御功能可以采用设备中已有的入侵防御特征库正常工作，但无法升级到官方网站在过期时间后发布的新版本的特征库。关于 License 的详细介绍请参见“License 联机帮助”。

防病毒

防病毒功能需要购买并正确安装 License 才能使用。License 过期后，防病毒功能可以采用设备中已有的病毒特征库正常工作，但无法升级特征库且云端查询功能以及联动沙箱阻断功能无法使用。关于 License 的详细介绍请参见“License 配置联机帮助”。

威胁趋势

本帮助主要介绍以下内容：

- 特性简介
  - 威胁类型趋势
  - 攻击者趋势
  - 攻击对象趋势
  - 威胁 ID 趋势
- vSystem 相关说明
- License 支持情况

特性简介

威胁趋势功能用来对设备上受到的威胁情况进行统计，方便管理员查看威胁事件发生的高峰时间段和高危险级别威胁事件发生的时间段等信息，从而调整防护策略，更好地保护内部网络安全。

管理员可单击<统计条件>按钮，配置多种统计条件，查看用户、应用、威胁类型、攻击者、攻击对象和威胁 ID 的趋势。

单击<报表导出>按钮，设备将立即根据当前统计条件查询到的统计数据生成一份 PDF 格式的报表文件，并导出到 PC 本地。管理员可通过查看报表文件了解当前的威胁情况。

威胁类型趋势

管理员可根据威胁类型查看威胁趋势，方便查看频繁发生威胁事件的威胁类型，从而调整防护策略。

支持配置的统计条件如下表所示：

表-1 威胁类型趋势统计条件

参数	说明
威胁类型	统计的威胁类型，取值包括： • 入侵防御 • 防病毒
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义

单击<开始统计>按钮，设备将根据配置的统计条件对指定威胁类型的威胁次数进行统计。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

攻击者趋势

管理员可根据攻击者的 IP 地址查看威胁趋势，方便针对频繁发起攻击的攻击者调整防护策略。支持配置的统计条件如下表所示：

表-2 攻击者趋势统计条件

参数	说明
攻击者范围	统计的攻击者，取值包括： • Top5 攻击者 • 指定攻击者
威胁类型	统计的威胁类型，取值包括： • 入侵防御 • 防病毒 • 所有威胁
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义

单击<开始统计>按钮，设备将根据配置的统计条件对攻击者的威胁情况进行统计。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

攻击对象趋势

管理员可根据攻击对象查看威胁趋势，方便针对频繁受到攻击的攻击对象调整防护策略。支持配置的统计条件如下表所示：

表-3 攻击对象趋势统计条件

参数	说明
攻击对象范围	统计的攻击对象，取值包括： • Top5 攻击对象 • 指定攻击对象
威胁类型	统计的威胁类型，取值包括： • 入侵防御 • 防病毒 • 所有威胁
统计时间	统计的时间范围，取值包括： • 今天

	• 最近一周 • 最近三十天 • 自定义

单击<开始统计>按钮，设备将根据配置的统计条件对攻击对象受到的威胁情况进行统计。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

威胁 ID 趋势

管理员可根据发起威胁的威胁 ID 查看威胁趋势，方便针对威胁 ID 调整防护策略。支持配置的统计条件如下表所示：

表-4 威胁 ID 趋势统计条件

参数	说明
威胁ID范围	统计的威胁ID，取值包括： • Top5 威胁 ID • 指定威胁 ID
威胁类型	统计的威胁类型，取值包括： • 入侵防御 • 防病毒

攻击类型	统计的攻击类型，取值包括： • 攻击者 • 攻击对象 • 所有攻击
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义

单击<开始统计>按钮，设备将根据配置的统计条件对威胁 ID 的威胁情况进行统计。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

License支持情况

入侵防御

入侵防御功能需要购买并正确安装 License 后才能使用。License 过期后，入侵防御功能可以采用设备中已有的入侵防御特征库正常工作，但无法升级到官方网站在过期时间后发布的新版本的特征库。关于 License 的详细介绍请参见“License 联机帮助”。

防病毒

防病毒功能需要购买并正确安装 License 才能使用。License 过期后，防病毒功能可以采用设备中已有的病毒特征库正常工作，但无法升级特征库且云端查询功能以及联动沙箱阻断功能无法使用。关于 License 的详细介绍请参见“License 配置联机帮助”。

资产发现

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南

特性简介

资产发现可对指定 IP 地址或 IP 地址范围中的设备进行扫描分析，获取设备的操作系统、MAC 地址、厂商等信息，并进一步检测其是否存在开放端口、弱密码等风险因素。设备管理员可根据扫描结果获悉指定网络中的设备参数和可能存在的安全风险，进而巩固设备的安全配置。

设备支持对指定 IPv4 或 IPv6 地址、指定 TCP 和 UDP 端口进行扫描。

各种风险类型建议的防护措施如下表所示：

表-1 风险类型对应建议的防护措施表

风险类型	防护措施
端口开放风险	在安全策略中拒绝访问当前端口的报文
弱密码风险	修改弱密码风险用户的弱密码

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 资产发现扫描的 IPv4 地址范围起始地址的任一字段均不可大于结束地址，否则将无法扫描到结果。
- 在执行资产发现扫描任务过程中，请不要修改安全策略配置，否则可能导致无法获得准确的扫描结果。
- 若用户既未指定 TCP 扫描端口又未指定 UDP 扫描端口，设备将针对以下端口进行扫描：

- TCP 端口：23、80、139、443、445、554、631、3389、3872、5800、7080、8000、8080、8088、8180、8443
- UDP 端口：137

配置指南

资产发现的具体配置步骤如下：

1. 选择“监控 > 资产管理 > 资产发现”。
2. 配置“地址范围”，可指定单个 IPv4/IPv6 地址、IPv4/IPv6 地址范围或 IPv4/IPv6 网段。
3. 选择或配置“TCP 端口”。
4. 选择或配置“UDP 端口”。
5. 配置是否启用“自动扫描”，若启用自动扫描功能，设备将按指定周期进行资产扫描，缺省情况下，设备每隔 12 小时进行一次资产扫描任务。可选如下周期类型：
   - 周：表示每周扫描一次，可以选择实施扫描的日期。
   - 天：表示每天扫描一次，可以配置实施扫描的时间。
   - 小时：表示每隔多少小时扫描一次，可以选择间隔的小时数。
6. 配置是否“启用弱密码扫描”，若启用弱密码扫描功能，可单击<配置>按钮配置弱密码扫描的扫描范围和扫描模式。

7. 单击<开始扫描>按钮，设备将立即开始资产扫描任务。扫描完成后，可在“扫描记录”区块中单击<刷新>按钮，查看资产扫描结果。

流量统计

本帮助主要介绍以下内容：

- 特性简介
  - IP 会话统计
  - 虚拟系统排行
- vSystem 相关说明

特性简介

流量统计功能用来对指定时间段内设备上的流量使用情况进行统计排行，并使用柱状图、饼状图和列表的形式向用户展示统计排行结果，方便管理员对设备带宽使用情况进行分析。

若要查看 IP 会话统计，需要先在“系统 > 日志设置 > 存储空间设置”页面开启“会话管理 | IPTOP 日志”。

IP 会话统计

管理员可根据 IP 地址对会话情况进行统计排行，方便管理员对会话的情况进行分析。支持配置的统计条件如下表所示：

表-1 IP 会话统计条件

参数	说明
源IP地址/掩码	对指定的源IP地址子网进行会话排行统计
目的IP地址/掩码	对指定的目的IP地址子网进行会话排行统计
源IPv6地址/前缀	对指定的源IPv6地址子网进行会话排行统计
目的IPv6地址/前缀	对指定的目的IPv6地址子网进行会话排行统计
位置	对指定的单板进行会话排行统计
IP会话类型	会话统计的类型，IPv4类型取值包括： • 源 IP 新建：对源 IP 地址新建会话速率进行统计排行 • 源 IP 并发：对源 IP 地址会话并发数量进行统计排行 • 目的 IP 新建：对目的 IP 地址新建会话速率进行统计排行 • 目的 IP 并发：对目的 IP 地址会话并发数量进行统计排行 IPv6类型取值包括： • 源 IPv6 新建：对源 IPv6 地址新建会话速率进行统计排行 • 源 IPv6 并发：对源 IPv6 地址会话并发数量进行统计排行

	• 目的 IPv6 新建：对目的 IPv6 地址新建会话速率进行统计排行 • 目的 IPv6 并发：对目的 IPv6 地址会话并发数量进行统计排行
起始时间	显示统计IP会话数据的起始时间
时间间隔	显示统计会话数据的时间间隔

单击<确定>按钮，设备将根据配置的统计条件对 IP 会话情况进行统计显示。

虚拟系统排行

管理员可根据虚拟系统对流量进行统计排行，方便管理员对虚拟系统的访问情况进行分析。支持配置的统计条件如下表所示：

表-2 虚拟系统排行统计条件

参数	说明
流量类型	统计的流量类型，取值包括： • 上行流量 • 下行流量 • 总流量
统计时间	统计的时间范围，取值包括： • 今天

	• 最近一周 • 最近三十天 • 自定义
排行显示	显示排名的虚拟系统数

单击<开始统计>按钮，设备将根据配置的统计条件对虚拟系统的流量使用情况进行排名。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

流量趋势

本帮助主要介绍以下内容：

- 特性简介
  - 源 IP 地址趋势
  - 目的 IP 地址趋势
  - 虚拟系统趋势
  - 带宽策略趋势
  - 整机流量吞吐趋势
  - 整机流量时间分布趋势
- vSystem 相关说明
- 使用限制和注意事项

特性简介

流量趋势功能用来对设备上的流量使用情况进行统计，并使用折线图的形式向用户展示流量使用趋势，方便管理员查看流量发生高峰和低谷的时间段。

管理员可单击<统计条件>按钮，配置多种统计条件，查看源 IP 地址、目的 IP 地址、虚拟系统、带宽策略、整机流量吞吐和整机流量时间分布的流量趋势。

单击<报表导出>按钮，设备将立即根据当前统计条件查询到的统计数据生成一份 PDF 格式的报表文件，并导出到 PC 本地。管理员可通过查看报表文件了解设备上的流量使用情况。

源 IP 地址趋势

管理员可根据源 IP 地址查看流量趋势，方便基于源 IP 地址的流量情况进行访问控制。支持配置的统计条件如下表所示：

表-1 源 IP 地址趋势统计条件

参数	说明
源IP地址范围	统计的源IP地址，取值包括： • Top5 源 IP 地址 • 指定源 IP 地址
流量类型	统计的流量类型，取值包括： • 上行流量 • 下行流量 • 总流量
统计时间	统计的时间范围，取值包括：

	• 今天 • 最近一周 • 最近三十天 • 自定义
应用类型	统计的应用类型
应用	统计指定应用类型中的应用

单击<开始统计>按钮，设备将根据配置的统计条件对源 IP 地址的流量使用情况进行统计，并展示流量趋势图。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

目的 IP 地址趋势

管理员可根据目的 IP 地址查看流量趋势，方便基于目的 IP 地址的流量情况进行访问控制。支持配置的统计条件如下表所示：

表-2 目的 IP 地址趋势统计条件

参数	说明
目的IP地址范围	统计的目的IP地址，取值包括： • Top5 目的 IP 地址

	• 指定目的 IP 地址
流量类型	统计的流量类型，取值包括： • 上行流量 • 下行流量 • 总流量
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义
应用类型	统计的应用类型
应用	统计指定应用类型中的应用

单击<开始统计>按钮，设备将根据配置的统计条件对目的 IP 地址的流量使用情况进行统计，并展示流量趋势图。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

虚拟系统趋势

管理员可根据虚拟系统查看流量趋势，方便基于虚拟系统的流量情况进行访问控制。支持配置的统计条件如下表所示：

表-3 虚拟系统趋势统计条件

参数	说明
虚拟系统范围	统计的虚拟系统，取值包括： • Top5 虚拟系统 • 指定虚拟系统
流量类型	统计的流量类型，取值包括： • 上行流量 • 下行流量 • 总流量
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义

单击<开始统计>按钮，设备将根据配置的统计条件对虚拟系统的流量使用情况进行统计，并展示流量趋势图。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

带宽策略趋势

管理员可根据带宽策略查看命中策略的流量趋势，方便确定策略配置是否正确及达到理想效果，进而对策略配置进行调整优化。支持配置的统计条件如下表所示：

表-4 带宽策略趋势统计条件

参数	说明
带宽策略范围	统计的带宽策略，取值包括： • Top5 带宽策略 • 指定带宽策略
流量类型	统计的流量类型，取值包括： • 上行流量 • 下行流量 • 总流量
统计时间	统计的时间范围，取值包括： • 今天

	• 最近一周 • 最近三十天 • 自定义

单击<开始统计>按钮，设备将根据配置的统计条件对命中带宽策略的情况进行统计，并展示流量趋势图。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

整机流量吞吐趋势

管理员可根据配置的统计条件查看整机流量的吞吐趋势，了解当前网络的流量状态，从而制定相关的流量管理措施。支持配置的统计条件如下表所示：

表-5 整机流量吞吐趋势统计条件

参数	说明
分析类型	统计的数据类型，取值包括： • 流量 • 流速
流量类型	统计的流量类型，取值包括： • 上行流量

	• 下行流量 • 总流量
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义

单击<开始统计>按钮，设备将根据配置的统计条件对整机流量的吞吐情况进行统计，并展示统计结果。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

整机流量时间分布趋势

管理员可根据配置的统计条件查看整机流量的时间分布趋势，了解当前网络业务繁忙和空闲的时间分布，从而制定相关的流量管理措施。支持配置的统计条件如下表所示：

表-6 整机流量时间分布趋势统计条件

参数	说明
分布时间类型	统计的分布时间类型，取值包括：

	• 小时：查看统计时间内，0 时到 23 时，每小时的流量分布情况 • 日：查看统计时间内，1 日到 31 日，每日的流量分布情况 • 周：查看统计时间内，周一到周日，每日的流量分布情况
流量类型	统计的流量类型，取值包括： • 上行流量 • 下行流量 • 总流量
统计时间	统计的时间范围，取值包括： • 最近一周 • 最近三十天 • 自定义

单击<开始统计>按钮，设备将根据配置的统计条件对整机流量时间分布情况进行统计，并展示统计结果。

单击<报表导出>按钮，可将统计结果以报表的形式导出，方便用户查看。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

虚拟系统趋势功能的支持情况与设备型号有关，请以设备实际情况为准。

安全策略命中趋势

特性简介

安全策略命中趋势用来查看设备中所有安全策略被报文命中的次数变化，方便管理员直观掌握各个安全策略对报文的匹配情况。

若要查看安全策略命中统计，需要先在“存储空间设置”页面开启“安全策略 | 安全策略命中统计”。

管理员可配置统计条件，查看指定安全策略、Top5 策略的命中趋势。设备支持配置的统计条件如下表所示：

表-1 安全策略命中趋势统计条件

参数	说明
策略范围	统计的安全策略范围，取值包括： • Top5 策略：统计命中次数排行前 5 的安全策略 • 指定策略：统计用户指定的安全策略，用户需输入安全策略名称
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周

	• 最近一个月 • 最近一年 • 自定义

单击<开始统计>按钮，设备将根据配置的统计条件对安全策略命中情况进行统计。

安全策略命中统计

特性简介

安全策略命中统计功能用来对指定时间段内设备上安全策略被报文命中的情况进行统计排行，并使用柱状图、饼状图和列表的形式向用户展示统计排行结果，方便管理员对安全策略命中情况进行分析。

若要查看安全策略命中统计，需要先在“存储空间设置”页面开启“安全策略 | 安全策略命中统计”。

管理员可配置统计条件，对不同类型安全策略的命中次数进行统计排行。支持配置的统计条件如下表所示：

表-1 安全策略命中统计条件

参数	说明
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 最近一年

	• 自定义
排行显示	显示排名的安全策略数

单击<开始统计>按钮，设备将根据配置的统计条件对安全策略的命中情况进行排名。

生成统计结果后，管理员可单击指定的安全策略，进入“修改安全策略”页面，对某个安全策略进行编辑。

会话列表

特性简介

会话列表页面记录了每条数据流的详细信息，不仅包括数据流的五元组信息，还包括了此条数据流命中的安全策略和承载的应用等信息。

会话列表页面提供了暂停某条会话的功能。单击“状态”列中的<正常>按钮后，可以将此条会话置于暂停状态，命中处于暂停状态会话的报文将被丢弃。

会话主备状态包括的取值如下：

- 主：表示此会话为主会话，是在本设备上创建。
- 备：表示此会话为备份会话，是从备份设备上同步而来。

使用限制和注意事项

- 使用“按 CLI 显示导出”功能导出会话列表时，最多只能导出 1000 条会话。
- 使用“按 Web 显示导出”功能导出会话列表时，仅支持导出前 10000 条会话信息。

终端状态

本帮助主要介绍以下内容：

- 特性简介
  - 终端热力图
  - 终端信息表
- vSystem 相关说明
- 使用限制和注意事项

特性简介

终端热力图

终端热力图以可视化图形界面的方式，直观展示了每个终端的运行状态，包括：正常、异常、不可达，并可以根据终端状态或是否封堵对终端进行查询。用户可以点击终端对应的 IP 地址，对该 IP 地址执行审批为合法、重识别以及封堵操作。

- 审批为合法:当用户信任当前识别出的终端信息时,可将其审批为合法,便于终端信息变化时,作为参考。当终端识别功能处于白名单模式且动作配置为阻断时,终端信息变化会导致终端流量被阻断,此时,如果用户信任变化后的终端信息,可单击此按钮,将终端审批为合法,设备将放行该终端流量。
- 重识别:当用户需要对终端进行重识别时,可单击此按钮,设备将清空当前 IP 地址的全部终端识别信息及合法终端信息,重新识别终端。
- 封堵:当用户希望阻断某终端流量时,可单击此按钮。封堵后,设备将丢弃该终端的流量,直至封堵时间结束或用户对其解封。

在终端热力图中,不同的颜色代表对应终端所处的状态不同,包括:

- 灰色:代表未使用,指该 IP 地址未被终端使用,设备如果从未检测到该 IP 地址的流量或该 IP 地址对应终端保持不可达状态七天以上,则认为是“未使用”状态。
- 绿色:代表正常,指该 IP 地址已被终端使用,则认为是“正常”状态。
- 橙色:代表异常,指该 IP 地址对应的终端处于异常状态,终端异常包含两种情况:
  - 不畅通:当该 IP 地址的流量处于带宽管理的阈值范围之外时,则认为是“异常”状态。
  - 非法占用:通过对终端的深度识别,当发现终端信息发生变化,表示该 IP 地址被其他非法终端占用,则认为是“异常”状态。
- 红色:代表不可达,指该 IP 地址对应的终端无法连接,当设备曾采集到该 IP 地址的流量信息,后来无法采集到流量,则认为是“不可达”状态。若不可达状态持续七天未采集到流量,则状态更新为“未使用”。

- 紫色：代表已封堵，当用户对某个 IP 地址实施一键封堵后，则该 IP 地址显示为“已封堵”状态。
- 棕色：代表未知，指某个 IP 地址对应的终端的状态无法确定，即无法确定该终端是否与设备保持连接。

终端信息表

终端信息表展示了所有终端的信息以及运行状态，对每个终端进行全方位监控。通过监控设备的 MAC 地址、厂商、型号,是否审批为合法等信息，防止该终端的 IP 地址被非法占用或终端被非法替换。用户可根据实际需求，选择指定的终端，对其进行一键封堵或解封、审批为合法以及重识别。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

必须在“策略 > 主动防护 > 黑名单”页面单击<开启全局应用>按钮开启全局黑名单功能后，一键封堵功能方可生效。

Ping

特性简介

Ping 工具可以指定一个目的 IP 地址或者主机名，探测从该设备到目的端之间的链路是否正常，用来检查网络是否连通，可以很好地帮助我们分析和判定网络故障。

通过使用 Ping 功能，用户可以检查指定地址的设备是否可达，测试链路是否通畅。

Ping 功能是基于 ICMP（Internet Control Message Protocol，互联网控制消息协议）协议来实现的：源端向目的端发送 ICMP 回显请求（ECHO-REQUEST）报文后，根据是否收到目的端的 ICMP 回显应答（ECHO-REPLY）报文来判断目的端是否可达；对于可达的目的端，再根据发送报文个数、接收到响应报文个数以及 Ping 过程报文的往返时间来判断链路的质量。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置限制和指导

如果要使用目的端的主机名执行 Ping 操作，事先必须在设备上配置 DNS（Domain Name System，域名系统）功能，否则会 Ping 失败。

配置指南

Ping 功能是网络管理和故障排除中的一个基本功能，在网络出现问题时，用来检查网络是否连通，可以很好地帮助我们分析和判定网络故障。

1. 单击“系统 > 诊断中心 > Ping”。
2. 选择“IP 类型”，选择“IPv4”表示检查 IPv4 网络的可达性；选择“IPv6”表示检查 IPv6 网络的可达性。
3. 配置“目的 IP/IPv6 地址或者主机名”，表示探测目的端的 IP 地址或主机名。其中，主机名字符串仅可包含字母、数字、“-”、“_”或“.”，不区分大小写。
4. 单击<开始>按钮，启动探测。
5. 探测完成后，探测结果会显示在“结果”框中，管理员可以查看探测结果，判断探测的目标网络是否可达。

Tracert

特性简介

通过使用 Tracert 功能，用户可以查看 IP 报文从源端到达目的端所经过的三层设备，从而检查网络连接是否可用。当网络出现故障时，用户可以使用该功能分析出现故障的网络节点。

管理员可以指定一个目的 IP 地址或者主机名，探测从该设备到目的端之间所有的路由节点，用来跟踪报文转发路径。

当用户使用 Ping 功能测试发现网络出现故障后，可以用 Tracert 功能分析出现故障的网络节点。

Tracert 的输出信息包括到达目的端所经过的所有三层设备的 IP 地址。如果某设备不能回应 ICMP 错误消息（可能因为路由不可达或者没有开启 ICMP 错误报文处理功能），则输出“* * *”。

IPv4 Tracert 不可达结果

在 IPv4 Tracert 过程中，如果中间设备开启了 ICMP 不可达报文处理功能（参考 **ip unreachables enable** 命令），且命令执行结果中显示以下字符，则表示目的设备已不可达，设备会停止发包，Tracert 过程停止。

- !N：表示网络不可达。
- !H：表示目的主机不可达。

- !P：表示协议不可达（未知的协议号）。
- !F：表示需要进行分片但中间设备设置了不分片导致的不可达。
- !W：表示未知的目的主机不可达，即目的主机不存在。
- !Q：表示目的网络不可达的服务类型不可达，即不可用的服务类型（网络）。
- !T：表示目的主机不可达的服务类型不可达，即不可用的服务类型（主机）。
- !X：表示管理禁止通信不可达，即通信被过滤策略禁止。
- !V：表示违反主机优先级不可达，即报文优先级为 src/dst/port 不准许的优先级，则报文不被允许转发。
- !C：表示优先级终止生效不可达，即报文优先级被终止生效而不允许转发。

IPv6 Tracert 不可达结果

在 IPv6 Tracert 过程中，如果中间设备开启了 ICMP 不可达报文处理功能（参考 **`ipv6 unreachables enable`** 命令），且命令执行结果中显示以下字符，则表示目的设备已不可达，设备会停止发包，Tracert 过程停止。

- !N：表示目的端路由不可达，即路由表中没有匹配的目的地址。
- !P：表示因安全类业务流量管理禁止导致通信不可达，即通信被过滤策略禁止。
- !A：表示目的地址不可达，即未知的不可达消息。
- !S：表示超出源地址范围不可达，即当源地址为链路本地地址而目的地址不是链路本地地址时返回此字符。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置限制和指导

如果要使用目的端的主机名执行 Tracert 操作，事先必须在设备上配置 DNS（Domain Name System，域名系统）功能，否则会 Tracert 失败。

配置指南

Tracert 用于检测从你的计算机到目标主机之间数据包经过的路径。可以帮助你了解数据经过的每一跳以及到达每一跳所需的时间。

1. 单击“系统 > 诊断中心 > Tracert”。
2. 选择“IP 类型”，选择“IPv4”表示查看 IPv4 报文从源端传到目的端所经过的路径；选择“IPv6”表示查看 IPv6 报文从源端传到目的端所经过的路径。
3. 配置“目的 IP/IPv6 地址或者主机名”，表示目的端的 IP/IPv6 地址或主机名。其中，主机名的字符串仅可包含字母、数字、“-”、“_”或“.”，不区分大小写。
4. 单击<开始>按钮，启动 Tracert 探测。

探测完成后，探测结果会显示在“结果”框中，管理员可以查看探测结果，获取报文转发路径及故障节点信息。

报文捕获

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置准备
  - 开始报文捕获
  - 配置报文捕获参数

特性简介

报文捕获功能用于捕获设备的双向流量，并将捕获到的报文生成 Wireshark（一种网络封包分析软件）可识别的.cap 后缀文件，保存到本地或外部服务器，供用户分析诊断出入设备的流量。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 报文捕获功能不支持多用户同时配置。
- 报文捕获功能启动后，报文捕获的参数不能再被修改。
- 启动报文捕获功能会对设备的性能产生影响，因此建议只在需要捕获报文的情况下启动该功能。
- 捕获文件存储在本地的情况下，报文捕获启动后系统会删除捕获文件存储路径下所有.cap 后缀的文件，因此请及时导出所需的捕获文件。
- 报文捕获功能不支持对非缺省 Context 的共享接口进行报文捕获。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

开始报文捕获

通过捕获网络报文，可以快速定位网络故障的原因，分析网络性能瓶颈，并且可以对网络流量进行监控和审计，保障网络安全。

1. 选择“系统 > 诊断中心 > 报文捕获”。
2. 在“报文捕获”页面单击<开始报文捕获>按钮，进入“配置报文捕获过滤条件”页面，具体配置内容如下表所示：

表-1 配置参数表

参数	说明
接口	表示捕获指定接口上接收和发送的所有报文
类型	表示报文类型，取值包括： • IPv4 & IPv6：表示捕获匹配所有类型的报文

	• IPv4：表示捕获匹配 IPv4 类型的报文 • IPv6：表示捕获匹配 IPv6 类型的报文
ACL	表示捕获匹配高级ACL中**permit**规则的报文
VLAN	表示捕获指定VLAN上的报文
方向	配置设备捕获报文的方向，取值包括： • 双向：表示捕获设备接收和发送的报文 • 入方向：表示捕获设备接收的报文 • 出方向：表示捕获设备发送的报文

3. 单击<开始>按钮，设备将开始进行报文捕获，报文捕获页面上的报文捕获状态为开始。

4. 在“报文捕获”页面单击<停止报文捕获>按钮，设备将停止对报文进行捕获，报文捕获页面上的报文捕获状态为停止，捕获文件将显示在捕获报文页面下方。

配置报文捕获参数

当捕获文件存储的捕获条目达到最大存储个数后，系统会将内存中的捕获文件上传到指定的存储路径上，并将内存中的捕获文件删除。捕获文件可以存储在设备本地，也可以选择上传至外部的 FTP 或 TFTP 服务器。

1. 选择“系统 > 诊断中心 > 报文捕获”。

2. 在“报文捕获”页面单击<配置报文捕获参数>按钮，进入“配置报文捕获参数”页面，具体配置内容如下表所示：

表-2 配置参数表

参数	说明
每报文最大长度	当待捕获报文的长度超过设置的最大长度后，报文捕获模块会对报文进行
每捕获文件存储报文数	当捕获文件存储的捕获条目达到最大存储个数后，系统会将内存中的捕获 的存储路径上，并将内存中的捕获文件删除。捕获文件存储的捕获条目越 就越大，因此在系统内存剩余较少的情况下，请将捕获文件存储捕获条目
保存在设备	表示将捕获文件存储在设备本地，且需要配置捕获文件最大存储空间，当 超过最大存储空间限制时，自动停止报文捕获
保存到外部服务器	表示将捕获文件存储到外部的FTP/TFTP服务器。当外部存储服务器为FTP 配置登录FTP服务器的用户名和密码
VRF	表示FTP/TFTP服务器所属的VRF

3. 单击<确定>按钮，完成报文捕获参数配置。

网页诊断

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置准备
  - 网页诊断

特性简介

网页诊断功能主要用于当内网用户访问网页出现故障时，对网络进行基本的诊断，并给出故障原因。

当内网用户访问网页出现故障时，通常需要结合多种诊断手段（如 Ping，查看 Log 信息等）排查网络故障。网页诊断可以通过一键诊断功能对网页访问故障进行快速、系统的排查和分析，并输出简单易懂的故障提示信息，方便管理员处理网络故障。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 用户 IP 地址和网页 URL 仅支持 IPv4 类型的地址。
- 网页诊断功能仅支持对基于 HTTP 协议的网页进行诊断。
- 开始网页诊断之前，请先配置安全策略保证用户和 Web 服务器所在安全域与 Local 安全域之间的报文互通。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。

- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

网页诊断

1. 选择“系统 > 诊断中心 > 网页诊断”。
2. 配置诊断参数，具体内容如下表所示：

表-1 诊断参数表

参数	说明
用户IP地址	上网用户的真实IP地址
用户VRF	用户所属的VRF
网页URL	上网用户所访问真实网页的URL。示例：http://www.example.com
网页VRF	访问网页所属的VRF

3. 单击<诊断>按钮，对网页进行诊断。
4. 通过查看输出的诊断信息，对网页访问故障进行分析和处理。
5. （可选）可以单击<导出>按钮，将网页诊断结果以 Excel 的格式导出。

诊断信息收集

特性简介

在设备日常维护或系统出现故障时，为了便于问题定位，用户需要查看各个模块的诊断信息。因为各个功能模块都有其对应的运行信息，为便于一次性收集更多信息，用户可以使用此功能收集多个模块的诊断信息。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

诊断信息收集

1. 选择“系统 > 诊断中心 > 诊断信息收集”，进入诊断信息收集页面。
2. 单击<收集>按钮，进入“请输入诊断信息文件名”页面。
3. 输入文件名称，单击<确定>按钮。
4. 开始收集设备诊断信息，收集的信息将展示在诊断信息收集列表中。

报文示踪

本帮助主要介绍以下内容：

- 特性简介
  - 应用场景
  - 报文示踪模式
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置准备
  - 报文示踪

特性简介

报文示踪功能用来分析和追踪设备中各个安全业务模块（如：攻击防范、uRPF、会话管理和并发连接限制等）对报文的处理过程，通过查看报文示踪记录的详细信息，有利于管理员对网络故障的快速排查和定位。

应用场景

当出现网络故障时，通常由于设备上配置了较多的安全业务，导致管理员无法快速、准确地定位故障。报文示踪功能可以帮助管理员有效解决上述问题。

报文示踪模式

为满足不同情况下网络故障定位的需求，报文示踪功能提供了如下三种诊断模式：

- 真实流量诊断：指在实际网络环境中，对经过设备的真实流量进行追踪和分析。此种方式适用于在实际网络中定位网络故障。
- 导入报文诊断：指将捕获的文件（必须是“.cap”或“.pcap”格式的文件）导入设备，对报文进行分析，对报文被处理的过程进行回放。此种方式适用于在本设备上已经捕获所需报文的场景，或者需要对其他设备（如不支持报文示踪功能的设备等）上的报文进行协助分析的场景。
- 构造报文诊断：指设备根据管理员输入的参数信息构造一个报文，用来验证和查看已配置的安全业务功能对此报文的处理结果。此种方式适用于在设备上配置完各项所需的功能后，模拟一个真实流量的报文，来验证设备对报文的处理是否可以达到预期效果的场景。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 仅在诊断报文前选择捕获诊断报文功能后，报文示踪过程才会生成.cap 文件，否则不会生成。
- 捕获报文生成的.cap 文件被下载后，设备上保存的此文件即被删除，管理员将无法再次导出。
- 导入报文诊断模式仅能导入文件中的前 10 条流，每条流又仅能导入前 10 个报文，且仅能对导入的完整报文进行示踪，不完整的报文无法进行示踪。
- 当接口开启保持上一跳功能并转发成功时，设备无法读取下一跳的 IP 地址，此时下一跳会显示为 255.255.255.255（IPv4）或::（IPv6）。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

报文示踪

1. 选择“系统 > 诊断中心 > 报文示踪”。
2. 在“报文示踪”页面，可以通过配置参数信息，选择对哪些报文进行示踪，具体配置内容如下表所示：

表-1 配置参数表

参数	说明
诊断模式	配置报文示踪的诊断模式，取值包括： • 真实流量 • 导入报文 • 构造报文
IP类型	配置IP地址类型，包括IPv4和IPv6两种： • IPv4：表示仅对 IPv4 类型的报文进行示踪 • IPv6：表示仅对 IPv6 类型的报文进行示踪
入接口	选择需要示踪报文的入接口
协议	选择需要示踪报文的协议
源地址	选择需要示踪报文的源地址
源端口	选择需要示踪报文的源端口

目的地址	选择需要示踪报文的目的地址
目的端口	选择需要示踪报文的目的端口
源MAC	选择需要示踪报文的源MAC地址
目的MAC	选择需要示踪报文的目的MAC地址
VLAN ID	选择需要示踪报文的VLAN ID
诊断时间	选择需要示踪报文的时间长短，达到指定时间后，报文示踪功能停止。此 诊断模式支持
捕获诊断报文	选择此功能后，设备在报文示踪的同时会把报文捕获下来，并形成.cap文 使用。管理员可单击<导出>按钮并选择“捕获报文”选项下载此.cap文件

3. 单击<诊断>按钮，设备将开始进行报文示踪。

对报文诊断结束后，通过诊断信息可以查看各安全业务模块对报文的处理情况。对正确处理报文的业务模块，系统会给出示意；对丢弃报文的业务模块，系统会给出示意，并给出丢包原因。

漏洞扫描

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置思路
  - 配置准备
  - 配置漏洞扫描并查看扫描结果
  - 配置批量风险处理并查看防护记录

特性简介

漏洞扫描可对指定 IP 地址或 IP 地址范围中的设备进行扫描分析，判断其是否存在开放端口、未防护漏洞、Web 应用风险、弱密码等风险因素，设备管理员可根据扫描结果巩固设备的安全配置。

设备支持对指定 IPv4 或 IPv6 地址、指定 TCP 和 UDP 端口进行扫描。

各种风险类型建议的防护措施如下表所示：

表-1 风险类型对应建议的防护措施表

风险类型	防护措施
端口开放风险	在安全策略中拒绝访问当前端口的报文
未防护漏洞	在安全策略中配置入侵防御
Web应用风险	在安全策略中配置Web应用防护
弱密码风险	修改弱密码风险用户的弱密码

弱密码扫描功能用于发现指定服务下的用户弱密码风险。开启弱密码扫描功能后，设备检查指定 IP 地址或 IP 地址范围中的主机、服务器和设备上各类服务的用户密码是否存在不安全的情况，用户可根据扫描结果更换安全强度更高的密码。

vSystem相关说明

非缺省 VSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

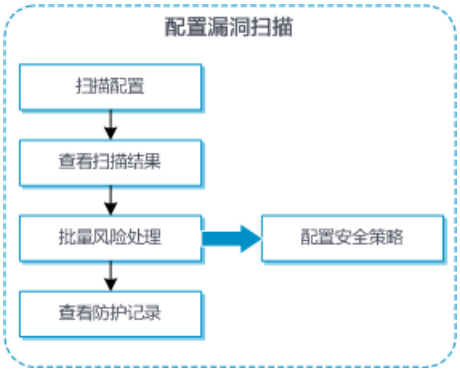
- 漏洞扫描配置的IPv4和IPv6地址范围起始地址均不可大于结束地址，否则将无法扫描到结果。
- 在执行漏洞扫描任务过程中，请不要修改安全策略配置，否则可能导致无法获得准确的扫描结果。
- 若在漏洞扫描任务结束后进行了安全策略导入/导出操作，建议重新执行风险扫描，再对新的扫描结果进行批量处理。

配置指南

配置思路

漏洞扫描功能的配置思路如下图所示：

图-1 漏洞扫描功能配置思路图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置漏洞扫描并查看扫描结果

具体配置步骤如下：

1. 选择“系统 > 诊断中心 > 漏洞扫描”，进入“漏洞扫描”页面。
2. 在"扫描配置"区域配置相关参数，具体的配置参数如下表所示。

表-2 扫描配置参数

参数	说明
地址类型	• IPv4 • IPv6
地址范围	漏洞扫描的地址范围，可输入单个IP地址（如1.1.1.1）或IP地址范围（如1.1.1.1-1.1.1.100），其中IPv6地址范围所包含的地址个数不得超过256个
TCP端口	选择或配置漏洞扫描的的目标TCP端口号
UDP端口	选择或配置漏洞扫描的的目标UDP端口号

3. （可选）配置是否“启用弱密码扫描”，若启用弱密码扫描功能，可单击<配置>按钮配置弱密码扫描的扫描范围和扫描模式，具体的配置参数如下表所示。完成相关参数的配置后单击<确定>按钮，弱密码扫描配置成功。

表-3 弱密码扫描配置参数

风险类型	防护措施
扫描范围	设备检查用户使用指定服务时的密码是否存在不安全的情况，服务类型：FTP、SQL Server、HTTP、MySQL和SSH
扫描模式	• 常规密码字典 使用设备预定义弱密码字典进行扫描

	• 自定义密码字典 使用用户自定义弱密码字典进行扫描 • 常规密码字典+自定义密码字典 可以同时使用预定义和自定义的弱密码字典进行扫描
自定义用户名	配置弱密码扫描所针对的用户名 扫描模式为常规密码字典时，不支持此功能
自定义密码	配置用户自定义弱密码 扫描模式为常规密码字典时，不支持此功能

4. 单击<开始扫描>按钮，扫描进行时可最小化扫描进度窗口，以便进行其他模块的配置。扫描完成后，可在“扫描记录”区块中勾选一个或多个记录表项，然后单击<显示扫描结果>按钮查看漏洞扫描结果。

配置批量风险处理并查看防护记录

具体配置步骤如下：

1. 完成漏洞扫描后，在“扫描结果”区域，单击<批量风险处理>按钮，进入“批量风险处理”页面。
2. 选择“地址类型”和“安全策略”，显示该安全策略相关的风险。勾选需要处理的风险，单击<风险处理>按钮，进入“风险处理”页面。

3. 通过配置安全策略处理风险，新建或修改安全策略，具体配置内容如下表所示：

表-4 风险处理配置参数表

参数	说明
处理方式	处理方式包括如下： • 新建策略：基于策略模板新建一个安全策略 • 修改策略：基于策略模板修改当前安全策略配置
名称	表示安全策略的名称，同一类型安全策略的名称不能相同
IP类型	安全策略包括IPv4和IPv6两种类型
策略模板	配置风险处理的安全策略模板，建议选择当前风险对应的安全策略
源安全域	配置源安全域作为安全策略的过滤条件
源IP/MAC地址	配置源IP地址或源MAC地址作为安全策略的过滤条件，源MAC地址过滤条件仅IPv4类型的安全策略支持 • 地址对象组：选择地址对象组 • IPv4 地址：输入以英文逗号分隔的 IPv4 地址、范围或子网
目的IP地址	配置目的IP地址作为安全策略的过滤条件 • 地址对象组：选择地址对象组 • IPv4 地址：输入以英文逗号分隔的 IPv4 地址、范围或子网
服务	配置服务作为安全策略的过滤条件

	• 服务对象组
	• 协议和端口号
	• 动作：安全策略动作
	  ○ 允许：表示对符合安全策略过滤条件的报文进行允许通过处理
	  ○ 拒绝：表示对符合安全策略过滤条件的报文进行阻断处理

内容安全	若内容安全中引用了相关策略，则会对符合安全策略过滤条件的报文进行相应的DPI（Deep Packet Inspection，深度报文检测）业务处理 • Web 应用防护 • 入侵防御配置文件

4. 单击<确定>按钮，完成风险处理。

5. 单击<防护记录日志>可查看具体的防护信息。

安全策略

本帮助主要介绍以下内容：

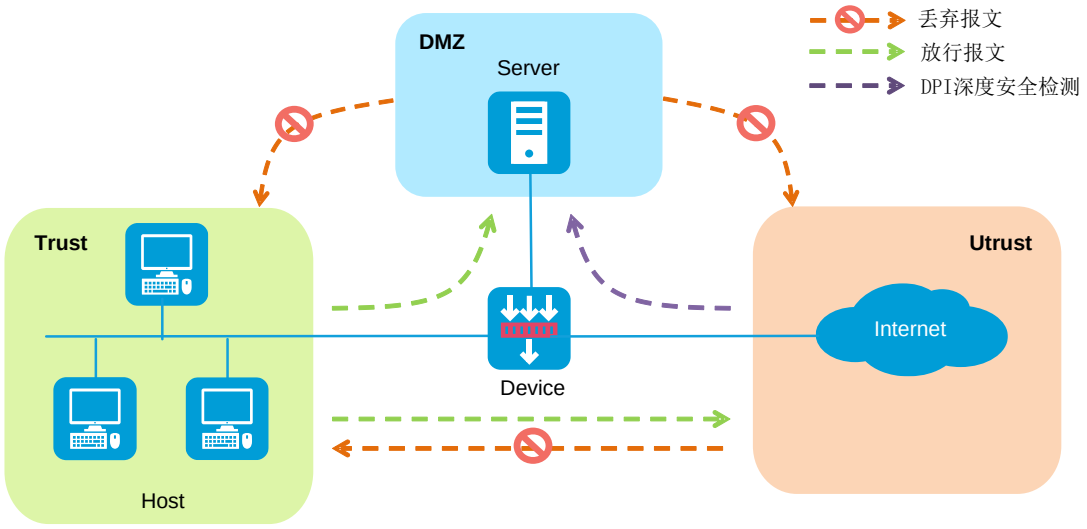
- 特性简介
  - 安全策略的名称
  - 安全策略的过滤条件
  - 安全策略的匹配顺序
  - 安全策略组
  - 安全策略自动部署
  - 策略导入导出功能
  - 移动安全策略功能
  - 安全业务管理平台下发安全策略
  - 缺省策略配置记录日志功能
  - 流量日志
- vSystem 相关说明
- 使用限制和注意事项
  - 配置安全策略

    - 配置策略组
    - 策略导入导出功能
    - 安全业务管理平台下发安全策略
- 配置指南
    - 配置思路
    - 配置准备
    - 安全策略自动部署
    - 安全策略放行或阻断特定流量
    - 安全策略对特定流量进行 DPI 深度安全检测
    - 安全策略组批量管理安全策略

特性简介

安全策略基于报文的属性信息对报文进行转发控制和 DPI（Deep Packet Inspection，深度报文检测）深度安全检测，有效识别和应对安全威胁。安全策略通过多种过滤条件（如源/目的安全域等）精确匹配报文的属性，并采取指定的动作对报文进行处理。安全策略广泛应用于企业网络和数据中心等场景，为网络的安全性提供全方位的保障。

图-1 安全策略示意图



安全策略的名称

设备上可以配置多个安全策略，每个策略均由名称和类型两类要素唯一标识。

安全策略的过滤条件

安全策略中可同时配置多种过滤条件，具体包括：源安全域、目的安全域、源 IP/MAC 地址、目的 IP 地址、源微分段、目的微分段、用户、应用、URL 分类、终端、服务和时间段等。一条策略被匹配成功的条件是：策略中已配置的所有过滤条件必须均被匹配成功。

一类过滤条件中可以配置多个匹配项，比如一类过滤条件中可以指定多个目的安全域。一类过滤条件被匹配成功的条件是：过滤条件的任何一个匹配项被匹配成功即可。

安全策略的匹配顺序

设备上可以配置多个安全策略，设备缺省按照策略的创建顺序对报文进行匹配，先创建的先匹配。因此，首先需要将规划的所有策略按照“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）进行排序，然后按照此顺序配置每一个安全策略。

安全策略组

安全策略组可以实现对安全策略的批量操作，例如批量启用、禁用、删除和移动安全策略。将安全策略加入安全策略组时，会将指定范围内若干连续的安全策略加入同一个安全策略组。

只有当安全策略及其所属的安全策略组均处于启用状态时，安全策略才能生效。

安全策略自动部署

若用户首次部署设备，对网络流量或安全策略功能不够了解，无法配置合理的安全策略，此时可借助安全策略自动部署功能，自动完成安全策略配置。安全策略自动部署功能首先学习经过设备的业务流量，学习完成后，根据流量报文属性自动生成对应的安全策略，从而放行合法的业务流量。

策略导入导出功能

安全策略导入导出功能主要用于实现安全策略配置的快速迁移。

导出功能支持导出.cfg 格式和.csv 格式：

- 导出.cfg 格式既可以一次性导出安全策略及其引用对象的配置；也可以单独导出某一具体模块的配置，导出后可在其他设备上导入以迁移安全策略配置。
- 导出.csv 格式可以导出安全策略信息列表，导出后用于查看或本地留存，该格式不支持在设备上导入。

导入功能，以增量方式向当前配置文件中写入导入的配置，并会对重复的配置进行覆盖。导入过程中如果某条配置写入失败，则停止导入，且已成功写入的配置无法回退。导入文件的格式必须为.cfg。

移动安全策略功能

移动安全策略可用于调整安全策略的顺序，从而改变安全策略匹配的优先级，也可将某个安全策略移动到其他某个安全策略组里。移动安全策略支持两种方式：

- 通过<移动>按钮进行移动

  选中待移动的安全策略，然后单击<移动>按钮，选择移动的位置即可。

- 通过拖拽方式进行移动

在安全策略列表中直接拖拽待移动的安全策略至左侧的安全策略组中，可将该安全策略移动至目标安全策略组中最后的位置；也可拖拽左侧安全策略组至其他组之前或者之后。

安全业务管理平台下发安全策略

当设备被安全业务管理平台纳管后，安全业务管理平台可向设备下发安全策略。设备安全策略页面中橙色底纹或绿色底纹的安全策略即安全业务管理平台下发的策略。橙色底纹的安全策略匹配优先级高于本地配置的安全策略；绿色底纹的安全策略匹配优先级低于本地配置的安全策略。

缺省策略配置记录日志功能

用户可以通过配置安全策略来处理业务流量，并通过开启记录日志功能生成日志。另外，当业务流量未经过安全策略处理时，可以通过缺省策略配置记录日志功能生成日志。通过同时开启这两个功能，可以确保所有业务流量经过设备时都会生成相应的日志。

流量日志

流量日志包括流量开始日志、流量结束日志和流量拒绝日志。

- 流量开始和结束日志适用于需要精确记录每个网络会话信息的场合，如金融机构、政府部门和大型企业的网络安全管理。它允许设备在会话建立时和结束时产生日志，记录关键流量信息。其中，对于流量开始日志，当流量匹配的安全策略变更时也会发送流量日志。
- 流量拒绝日志则用于记录因安全策略或其他原因被阻断的流量信息，适用于需要详细审计丢包原因的场景，便于排查网络问题、加强安全防护。

当安全策略动作为允许时，支持记录流量开始日志和流量结束日志；当安全策略动作为拒绝时支持记录流量拒绝日志。

流量日志中涵盖了大部分安全策略日志的内容，为避免产生不必要的重复日志及其带来的额外数据处理负担，建议仅开启流量日志。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

配置安全策略

- 安全策略只支持在相同 IP 类型的策略之间进行移动。

- 新建安全策略时，会将该策略放在相同 IP 类型策略的下面。
- 安全策略引用的地址对象组和服务对象组内容为空时，则此安全策略不会与任何报文匹配成功。有关对象组的详细介绍请参见“对象组联机帮助”。
- 安全策略中配置的会话老化时间优先级高于会话老化时间设置中配置的会话老化时间。
- 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。
- 源 MAC 地址过滤条件仅 IPv4 类型的安全策略支持。

配置策略组

- 配置策略所属的策略组后，其会被添加到该策略组的最后位置。
- 删除策略所属的策略组属性时：若该策略是原策略组的起始策略，则此策略会放在策略组的前面。若其位于原策略组的其他位置，则此策略会放在策略组的后面。
- 不允许移动空策略组，也不允许将策略组移动至空策略组前后。
- 不允许将策略组移动至其他策略组的起始策略后/结束策略前以及中间策略前后。
- 移动策略到其他策略组的策略前后，其会自动加入该策略组。

策略导入导出功能

- 设备仅支持导出自定义应用、自定义终端和自定义安全域，不支持导出预定义的应用、终端和安全域。
- 设备仅支持对导出的配置进行导入。
- 导出安全域和 VRF 时，只导出安全域或 VRF 的配置，不导出其与接口的绑定关系。因此，导入安全域或 VRF 配置后，请继续配置其与接口的绑定关系。
- 导出安全策略时，只导出安全策略的配置，不导出安全策略引用对象的具体配置。
- 同一时刻只允许一个用户进行导入导出操作。

安全业务管理平台下发安全策略

- 当设备处理被安全业务管理平台纳管状态时，安全管理平台下发的安全策略不允许在设备 Web 页面中编辑；仅当设备处于脱管状态时，这部分安全策略才可被编辑。
- 安全业务管理平台向设备下发安全策略时可指定下发在设备本地安全策略之前或之后，所以安全策略根据位置可分为三类：本地策略之前、本地策略、本地策略之后。当对某个安全策略执行移动操作时，仅可在本类位置范围内移动，即不可将本地策略之后的安全策略移动至本地策略中或本地策略之前。

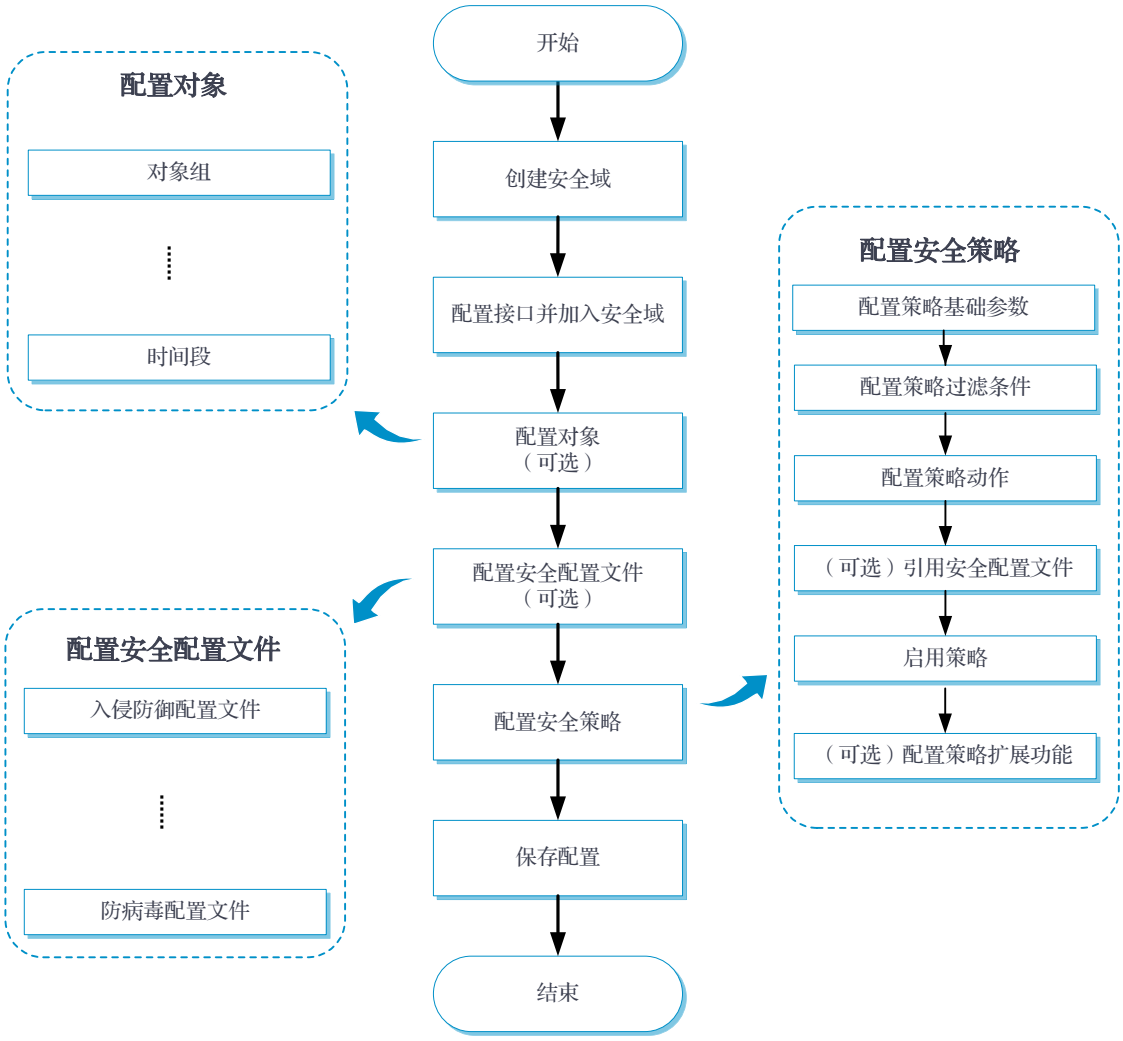
- 导入导出安全策略功能仅支持设备本地的安全策略，无法导入或导出安全业务管理平台下发的安全策略。

配置指南

配置思路

安全策略功能的配置思路如下图所示：

图-2 安全策略配置指导图



配置准备

在配置安全策略之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。

- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。

安全策略自动部署

当用户首次部署设备，对网络流量或安全策略功能不够了解，无法配置合理的安全策略时，可借助安全策略自动部署功能，自动完成安全策略配置。安全策略自动部署功能首先学习经过设备的业务流量，学习完成后，根据流量报文属性自动生成对应的安全策略，从而放行合法的业务流量。

1. 选择“策略 > 安全策略”。
2. 在“安全策略”页面单击<自动部署>按钮，进入“策略自动部署”页面。
3. 单击<开始学习>按钮，进入“配置自动部署参数”页面。
4. 配置自动部署参数，具体配置内容如下表所示：

表-1 自动部署参数表

参数	说明
学习时长	表示学习流量的时间长度
接入外网的安全域	表示设备接入外网的接口所属的安全域

接入服务器的安全域	表示设备接入内网服务器的接口所属的安全域
高级设置	表示是否配置安全策略聚合参数，包括： • IPv4 地址聚合的掩码长度 • IPv6 地址聚合的前缀长度
IPv4地址聚合的掩码长度	表示学习记录将源/目的IPv4地址聚合的掩码长度
IPv6地址聚合的前缀长度	表示学习记录将源/目的IPv6地址聚合的前缀长度

5. （可选）单击高级设置右侧的滑钮，配置自动部署高级设置。

为了精简安全策略的配置，设备在学习完成经过设备的业务流量后，可根据用户配置的自动聚合掩码长度/前缀长度进行智能聚合。具体内容如下：

表-2 自动部署高级设置参数说明

参数	说明
IPv4地址聚合的掩码长度	设备在聚合源或目的IPv4地址时，将按照此掩码长度进行聚合
IPv6地址聚合的前缀长度	设备在聚合源或目的IPv6地址时，将按照此前缀长度进行聚合

6. 单击<确定>按钮，自动部署参数配置完成。

7. 单击<开始学习>按钮，设备将开始学习流量报文，此时尽可能让设备转发所有合法的业务流量报文。

8. 学习完成后，勾选学习记录，单击<生成策略>按钮，完成安全策略自动部署。

安全策略放行或阻断特定流量

如果管理员需要对特定的流量进行阻断或者放行时，可通过在安全策略中设置过滤条件来限定处理范围，并指定相应的处理动作。具体配置步骤如下：

1. 选择“策略 > 安全策略”。

2. 在“安全策略”页面单击<新建安全策略>按钮，进入“新建安全策略”页面。

3. 配置安全策略基础参数，具体配置内容如下表所示：

表-3 安全策略基础参数说明

参数	说明
名称	用于唯一标识安全策略，同一类型安全策略的名称不能相同，默认系统会对名，管理员也可手动命名便于快速识别出策略
类型	表示安全策略匹配的报文类型，包括IPv4和IPv6

4. 配置安全策略过滤条件。

通过设置过滤条件，可对安全策略处理报文的范围进行限制，若不设置过滤条件，则安全策略会对所有流经设备的报文都进行处理。具体内容如下表所示：

表-4 安全策略配置参数表

参数	说明
源安全域	表示安全策略仅对来自特定安全域的报文进行处理。例如，当组网环境中需内网用户访问DMZ域的内网服务器时，需要将源安全域配置为Trust，目的行该域间的报文
目的安全域	表示安全策略仅对发往特定安全域的报文进行处理。例如，当组网环境中允用户访问设备本地时，需要将目的安全域配置为Local，源安全域配置为Tru
源地址	表示安全策略仅对来自特定地址对象组、IP/MAC地址、地区或微分段的报文网环境中不允许内网地址访问外网时，可将内网地址设置为源地址，阻断匹 其中，源MAC地址对象组过滤条件仅IPv4类型的安全策略支持 源地区、源地区组、源IP地址与源MAC地址匹配一项即认为匹配成功
用户	表示安全策略仅对特定身份识别用户的报文进行处理。例如，当组网环境中内部资源时，可将特定用户设置为过滤条件，阻断匹配该用户的报文 其中，用户与用户组匹配一项即认为匹配成功
目的地址	表示安全策略仅对发往特定IP地址对象组、IP地址、地区或微分段的报文进环境中仅允许外网用户访问特定的内网地址时，可将内网地址设置为目的地报文 其中，目的地区、目的地区组、目的IP地址匹配一项即认为匹配成功
时间段	配置安全策略生效的时间段 例如，组网环境中仅允许用户在工作时间内访问内网服务器时，可配置时间

	配该时间段的报文
服务	表示安全策略仅对特定服务对象组和协议/端口号的报文进行处理
应用	表示安全策略仅对特定应用或应用组的报文进行处理。例如，当组网环境中 定的应用时，可将特定的应用设置为过滤条件，阻断匹配该应用的报文 其中，应用与应用组匹配一项即认为匹配成功
URL分类	表示安全策略仅对特定URL分类的报文进行处理。例如，当组网环境中不允 URL分类时，可将特定的URL分类设置为过滤条件，阻断匹配该URL分类的
动作	安全策略动作包括如下： • 允许：表示对符合安全策略过滤条件的报文进行允许通过处理 • 拒绝：表示对符合安全策略过滤条件的报文进行阻断处理
启用策略	选择开启后，此安全策略才能生效
终端	配置终端或终端组作为安全策略的过滤条件
入接口VRF	配置入接口VPN实例作为安全策略的过滤条件，勾选“任意VRF”表示匹配

其中，终端和入接口 VRF 需要在“其它”下拉框中配置。

5. 配置安全策略动作，如需对匹配安全策略过滤条件的报文进行阻断，则动作配置为拒绝；否则，动作配置为允许。

6. 启用安全策略，使安全策略配置生效。

7. （可选）配置安全策略扩展参数，具体内容如下所示：

表-5 安全策略扩展参数说明

参数	说明
所属策略组	配置当前新建的策略所属的策略组。当需要通过策略组批量管理安全策略时 的策略组进行统一管理
描述信息	通过配置描述信息，便于管理员快速理解和识别此安全策略的作用
记录日志	开启记录日志功能后，对符合安全策略过滤条件的报文记录日志信息
记录流量日志-流量开始日志	开启本功能后，设备会在会话表创建或匹配的安全策略变更时生成并发送流 仅当安全策略动作为允许时，支持记录流量开始日志
记录流量日志-流量结束日志	开启本功能后，设备会在删除会话表时生成并发送流量日志 如果未配置本功能，设备是否输出流量日志由全局流量日志输出功能控制（ 需要在“系统 > 日志设置 > 日志管理”界面开启），即如果开启了全局流量 会在删除会话表时生成并发送流量日志；如果未开启全局流量日志输出功能 志 仅当安全策略动作为允许时，支持记录流量结束日志
记录流量日志-流量拒绝日志	开启本功能后，设备会在安全策略阻断流量时生成并发送流量日志 仅当安全策略动作为拒绝时支持记录流量拒绝日志
开启策略匹配统计	开启此功能后，对符合安全策略过滤条件的报文进行数据统计，并可指定统 • 永久 • 自定义
会话老化时间	会话老化时间用于及时清理长时间未活动的会话表项。当会话达到指定的老 该会话表项，以节约系统资源并维持网络设备的高效运行和稳定

	若安全策略策略中未配置会话老化时间，则该会话基于会话管理模块中配置
长连接老化时间	长连接老化时间用于处理某些特殊业务（如FTP文件下载或数据库查询）中的情况，通过设定超长的老化时间确保这些会话信息长时间不被清理，以保时避免其他不需要如此长老化时间的会话占用系统资源 若安全策略中未配置长连接老化时间，则该长连接会话基于会话管理模块中进行老化
策略冗余分析	策略冗余分析可以通过分析安全策略中的过滤条件识别出冗余的策略，从而开启本功能后，新建的安全策略可添加到策略冗余分析页面的分析列表中，策略进行冗余分析
学习	开启学习功能后，设备将对匹配安全策略的报文进行学习并记录，管理员可更精细化的安全策略。

8. 单击<确定>按钮，新建安全策略成功，并会在安全策略页面中显示。

安全策略对特定流量进行 DPI 深度安全检测

当管理员需要对特定的流量进行DPI深度安全检测时，可通过配置过滤条件限定安全策略处理范围，并引用安全配置文件进行相应的业务处理。例如，当需要对特定安全域之间的流量进行应用层攻击检测和防御时，可通过在安全策略中配置源、目的安全域过滤条件，并引用入侵防御配置文件实现。

1. 新建安全策略，配置基础参数和过滤条件。具体配置步骤请参见“安全策略放行或阻断特定流量”章节。

2. 动作配置为允许，并在“内容安全”区域引用指定的安全配置文件。

通过引用特定的配置文件，可进行相应业务的处理。安全策略支持同时引用多个业务配置文件进行检测，但每个业务仅支持引用一个配置文件。具体内容如下所示：

表-6 安全策略引用安全配置文件参数说明

参数	说明
Web应用防护配置文件	通过引用此配置文件，可对匹配安全策略的流量进行Web应用防护业务检测 Web应用防护业务可对Web攻击进行防御，实时阻断非法的请求，实现对W 本参数的支持情况，请以设备实际情况为准。
入侵防御配置文件	通过引用此配置文件，可对匹配安全策略的流量进行入侵防御业务检测 入侵防御业务可实时检测入侵行为，例如木马、蠕虫等，并通过一定的响应 实现保护企业信息系统和网络免遭攻击的目的
数据过滤配置文件	通过引用此配置文件，可对对匹配安全策略的流量进行数据过滤业务检测 数据过滤业务可对应用层协议报文中携带的内容进行过滤，以防止企业机密 敏感信息的传播
文件过滤配置文件	通过引用此配置文件，可对匹配安全策略的流量进行文件过滤业务检测 文件过滤业务可根据文件类型对设备传输的文件进行过滤，可批量允许或阻
防病毒配置文件	通过引用此配置文件，可对匹配安全策略的流量进行防病毒业务检测 防病毒业务可通过对报文应用层信息进行检测来识别和处理病毒报文，防止 有效保护网络安全
URL过滤配置文件	通过引用此配置文件，可对匹配安全策略的流量进行URL过滤业务检测 URL过滤可以对用户的URL请求进行访问控制，允许或禁止用户访问某些网 行为的目的

APT防御配置文件	通过引用此配置文件，可对匹配安全策略的流量进行APT防御业务检测 设备通过与沙箱进行联动，将流量送入沙箱进行隔离分析，并根据沙箱返回阻断等处理，防止内网遭到APT攻击。APT防御配置文件中可以配置上送沙的条件

3. 启用安全策略，使安全策略配置生效。

4. 单击<确定>按钮，新建安全策略成功，可到安全策略页面中进行查看。

安全策略组批量管理安全策略

安全策略组可以实现对安全策略的批量操作，例如批量启用、禁用、删除和移动安全策略。

新建安全策略组

1. 选择“策略 > 安全策略”。

2. 在“安全策略”页面单击<新建安全策略>下拉按钮，选择新建安全策略组，进入“新建安全策略组”页面。

3. 新建安全策略组，具体配置内容如下表所示：

表-7 安全策略组配置参数表

参数	说明
名称	表示安全策略组的名称
描述信息	通过配置描述信息，便于管理员快速理解和识别此安全策略组的作用
类型	表示将哪种类型的安全策略加入安全策略组，安全策略包括IPv4和IPv6两种
开始策略	表示加入安全策略组策略的起始策略的名称 将安全策略加入安全策略组时，起始策略要在结束策略前面，并且起始策略 间的策略不能属于其他安全策略组。
结束策略	表示加入安全策略组策略的结束策略的名称

4. 单击<确定>按钮，新建安全策略组成功，并会在安全策略页面中显示。

批量管理安全策略

在“安全策略”页面，单击安全策略组列表右侧的<启用/禁用>、<移动>和<删除>按钮，批量启用/

禁用安全策略、批量移动安全策略的位置以及批量删除安全策略。

策略冗余分析

本帮助主要介绍以下内容：

- 特性简介
- 使用限制和注意事项
- 配置指南
  - 配置准备
  - 安全策略冗余分析

特性简介

安全策略冗余分析可以通过分析安全策略中的过滤条件识别出冗余的策略，从而有利于达到精简策略的目的。过滤条件具体包括：源安全域、目的安全域、源 IP/MAC 地址、目的 IP 地址、用户、应用、URL 分类、终端、服务、VRF 和时间段。

设备会将高优先级的策略依次与低优先级的策略进行遍历比较，只要符合以下两种情况的任意一种，则认定为冗余：

- 所有过滤条件完全相同的安全策略，则低优先级的安全策略会被认定为冗余。

- 安全策略 A 的所有过滤条件被安全策略 B 完全包含，且安全策略 A 的优先级低于安全策略 B，则安全策略 A 会被认定为冗余。

策略冗余分析可以在没有流量经过设备时进行分析，因此该功能可以在安全策略配置完成后立即进行。在冗余分析结果中修改安全策略配置后，设备会自动再次进行策略冗余分析，以便使冗余分析结果更加准确。

使用限制和注意事项

- 此功能仅对处于生效状态的安全策略进行冗余分析。
- 安全策略冗余分析功能，每次最多只能分析出一百条冗余的安全策略。若设备上冗余的安全策略大于一百条，请先修改已分析出冗余的策略，然后再重新进行策略冗余分析。
- 安全策略配置很多时，使用安全策略冗余分析功能时，将会消耗较多的 CPU 资源，建议在业务量较低时使用。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

安全策略冗余分析

通过对现有的安全策略进行分析，从而有利于达到精简策略的目的，消除安全策略中的重复或多余部分，以提升系统的效率和安全性。

1. 选择“策略 > 安全策略 > 策略冗余分析”。
2. 在“策略冗余分析”页面，单击<开始分析>按钮，进行策略冗余分析。
3. 策略冗余分析完成后，可以在“策略冗余分析”页面查看冗余分析结果，冗余分析结果会按照安全策略的优先级由上到下显示与之存在冗余的安全策略。
4. 根据冗余分析结果，可以对冗余的安全策略做如下两种操作：
    - 若确定安全策略需要继续保留，则单击目标安全策略右侧的<编辑>按钮，进行修改即可。
    - 若确定安全策略不需要保留，则选中目标安全策略后，单击<删除>按钮，进行删除即可。

策略命中分析

本帮助主要介绍以下内容：

- 特性简介
- 配置指南
  - 配置准备
  - 安全策略命中分析

特性简介

安全策略命中分析功能可以分析出指定时间段内的安全策略是否被命中过，并将未命中的安全策略按照从高到低的优先级顺序进行呈现，以帮助管理员对设备上的安全策略进行深度分析和处理。

只要符合如下两种情况中的任意一种，则认为策略未命中：

- 流量不符合安全策略的过滤条件。
- 安全策略之间存在深度冗余，例如 IP 地址和用户的冗余、应用和服务的冗余等。这样会由于高优先级的策略被命中，而导致低优先级的策略未命中。

通过导出功能，可以导出.csv 格式未命中安全策略信息列表，导出后用于查看或本地留存。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。
- 配置策略命中分析功能前，需要先开启“策略匹配统计”功能。

安全策略命中分析

策略命中分析的具体配置步骤如下：

1. 选择“策略 > 安全策略 > 策略命中分析”。
2. 在“策略命中分析”页面，可以看到指定时间段内所有未命中的安全策略。

- 若确定安全策略需要继续保留，则单击目标安全策略右侧的<编辑>按钮，进行修改即可。
- 若确定安全策略不需要保留，则选中目标安全策略后，单击<删除>按钮，进行删除即可。

应用风险调优

本帮助主要介绍以下内容：

- 特性简介
  - 风险分析
  - 风险展示
  - 风险调优
  - 应用场景
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置思路
  - 配置准备
  - 自动应用风险调优
  - 手工应用风险调优

特性简介

应用风险调优功能通过应用层检测引擎智能地分析安全策略允许通过的流量中存在的潜在风险，为设备中所有安全策略的安全系数进行总体评估。总体安全评分越高表示安全策略的安全系数越高，相反评分越低表示存在的风险越大。

应用风险调优功能由风险分析、风险展示和风险调优三大功能模块组成。

风险分析

应用风险调优功能对安全策略风险分析的具体流程如下：

1. 通过应用层检测引擎识别出安全策略允许通过的流量中包含的应用信息；
2. 根据应用识别特征中定义的应用风险类型和建议的防护措施与安全策略中的策略信息进行对比；
3. 根据对比结果为每个安全策略的风险级别和所有安全策略的安全系数进行评估。

风险展示

设备可以将应用风险分析的结果进行直观展示，其各项信息的详细介绍如下表所示：

表-1 应用风险分析结果信息表

参数	说明
总体安全评分	对设备中所有安全策略的综合评分，得分越高表示安全策略的安全系数越高，相低表示存在的风险越大
安全策略名称	存在安全风险的安全策略的名称
风险级别	取值范围为1-5，数值越大表示风险级别越高
总流量	命中安全策略的总流量
应用	在命中安全策略并允许通过流量中识别出的所有应用
流量	每个应用在安全策略中的流量及其所占的比例
风险类型	安全策略中所有应用对应的风险类型的汇总
状态	安全策略的调优状态，其取值包括如下： • 未处理：表示从未调优过的安全策略 • 已处理：表示为已调优过的安全策略，但仍然存在风险的安全策略。可根据选择是否继续调优

风险调优

管理员可以根据应用风险分析结果对安全策略中的应用配置相应的防护，以此调优安全策略，设备支持如下两种调优方式：

- 自动批量调优：会将设备中所有待调优的安全策略，按照设备默认的安全策略调优规则进行策略调优，此方式比较方便快捷。
- 手工逐条调优：可以对设备中待调优的每条安全策略进行单独调优，此方式适用于对安全策略进行灵活调优。

应用风险调优功能对各种风险类型建议的防护措施如下表所示：

表-2 风险类型对应建议的防护措施表

风险类型	防护措施
可能包含漏洞	入侵防御、防病毒
可被恶意软件利用	入侵防御、防病毒
可传输文件	文件过滤、内容过滤
消耗带宽	URL过滤
易误操作	URL过滤
以其他应用为管道传输	入侵防御

易规避	URL过滤
降低工作效率	URL过滤

对于消耗带宽和降低工作效率的风险类型也可以进行带宽管理限制。有关带宽管理的详细介绍，请参见“带宽管理联机帮助”。

应用场景

应用风险调优功能常用的应用场景如下：

- 当对网络流量中存在的应用不是非常清楚时，可以先在设备上配置一个宽泛的安全策略，比如较大的 IP 地址范围或服务等，使设备稳定运行一段时间，尽可能还原企业日常运作中的网络环境。然后根据应用风险调优功能识别出的应用和风险，配置更加精准的安全策略。
- 对设备上已有的精细化安全策略进行风险评估和调优。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

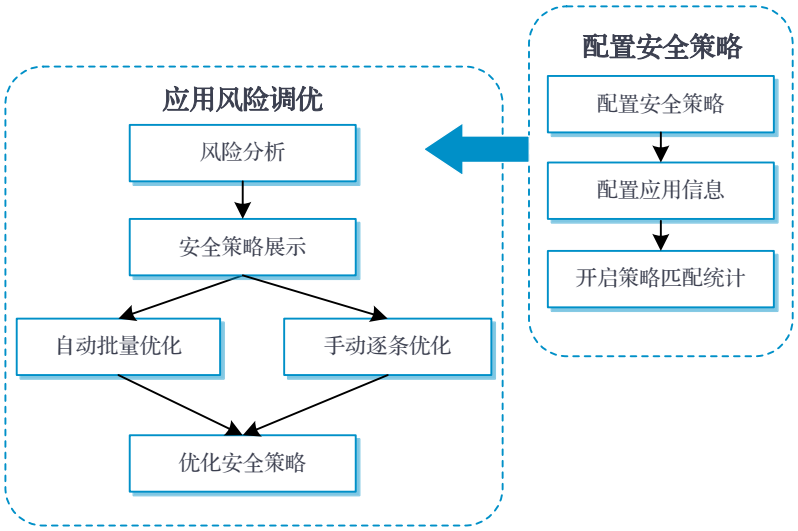
- 应用风险调优功能仅对安全策略允许通过的流量进行风险分析。
- 安全策略配置较多时，使用安全策略批量调优功能时，将会消耗较多的 CPU 资源，建议在业务量较低时使用。
- 批量调优过程中，不能新增安全策略。
- 批量调优过程中，当发生主备切换或内存门限告警时，批量调优会终止，但调优生成的规则仍然会被保存。如果需要重新批量调优，请在主备切换完成或内存恢复正常后，单击<自动批量调优>按钮。
- 如果在应用风险调优过程中，发生了主备切换，可能会导致主备设备配置不一致，需要用户手动检查主备设备配置的一致性。可以在“系统 > 高可靠性 > 双机热备”界面，通过<手工一致性检查>按钮，进行手工检查配置信息的一致性。有关手工一致性检查功能，请参见“双机热备”。

配置指南

配置思路

应用风险调优功能的配置思路如下图所示：

图-1 应用风险调优配置指导图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。
- 开启安全策略的“策略匹配统计”功能。
- 激活应用层检测引擎，即配置一个带有应用的安全策略。

自动应用风险调优

本功能通过应用层检测引擎识别安全策略允许通过的流量中包含的应用信息，进行风险分析，可将应用风险分析的结果进行直观展示，通过自动批量调优可以快速批量调整和优化安全策略，能有效的提供操作效率。

1. 选择“策略 > 安全策略 > 应用风险调优”。
2. 在“应用风险调优”页面，单击左上角的<自动批量调优>按钮，之后将按照设备默认的调优规则对所有待调优的安全策略进行批量调优。

手工应用风险调优

手动逐条调整允许更精细的控制和调整，每项安全策略可以根据具体情况进行单独配置，从而实现更加精细和准确的流量控制。

1. 选择“策略 > 安全策略 > 应用风险调优”。
2. 在目标安全策略右边，单击<调优处理>按钮，进入“安全策略调优处理”页面。
3. 具体调优内容如下表所示：

表-3 安全策略配置参数表

参数	说明
安全策略名称	存在安全风险的安全策略的名称
应用	安全策略中识别出的应用及其名称，选择需要防护的应用
流量	每个应用在安全策略中的流量
风险级别	取值范围为1-5，数值越大表示风险级别越高
风险类型	应用中存在的潜在风险
策略防护动作	为需要防护的应用配置防护动作，即安全策略中相关的内容安全策略。缺省情况下，引用的均是设备上缺省的内容安全策略，如果原安全策略中已引用内容安全策略，则继续使用原安全策略中的内容安全策略
新策略选项	其包括如下两个选项： • 生成一条新的策略放在原策略之前：不改变当前策略的配置，生成一条新的安全策略，优先级高于当前策略 • 在原策略的基础上直接修改：修改当前策略，为其配置相应防护措施的内容安全配置文件，但不会修改策略所匹配的应用
调优建议	按照设备默认的调优规则进行调优，与自动批量调优方式类似

4. 单击<确定>按钮，完成策略调优。

宽泛策略分析

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 配置指南
  - 配置思路
  - 配置准备
  - 配置宽泛策略分析

特性简介

宽泛策略分析功能用来对匹配安全策略规则的报文进行学习并记录，通过学习结果分析制定更精细化的安全策略。

vSystem相关说明

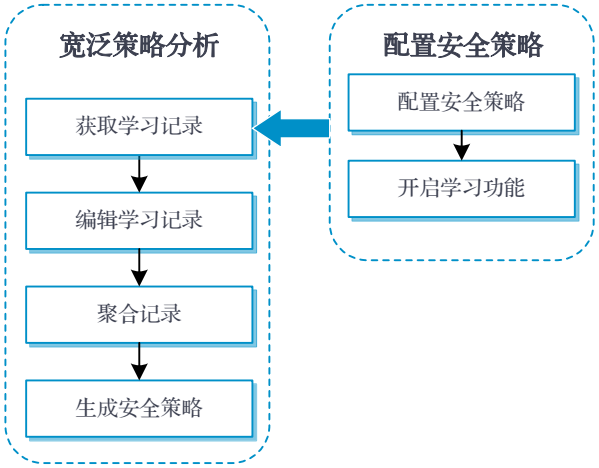
非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置思路

宽泛策略分析功能的配置思路如下图所示：

图-1 宽泛策略分析配置指导图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。
- 配置宽泛策略分析功能前，需要先在安全策略开启“学习”功能。

配置宽泛策略分析

宽泛策略分析通过对当前安全策略规则匹配的报文进行学习和记录，管理员可以编辑调整记录聚合生成安全策略。根据实际流量生成的安全策略更加精细化。

1. 选择“策略 > 安全策略 > 宽泛策略分析”页签，通过策略名称或策略 ID 选择安全策略，单击<获取>按钮获取学习记录。
2. 单击<下一步>按钮，进入编辑学习记录页面。
3. 单击学习记录对应的<编辑>按钮修改单个学习记录，或单击<替换学习记录>按钮修改全部学习记录的源地址、目的地址或目的端口。

4. 单击<下一步>按钮，进入聚合记录页面。

5. 通过勾选“源地址”、“目的地址”或“服务”可将相同源地址、相同目的地址或相同服务的多条学习记录聚合为一条。

6. 单击<下一步>按钮，进入生成策略页面。

7. 勾选需要生成安全策略的学习记录，单击<生成并启用>或<生成并禁用>按钮生成安全策略；或单击<生成所有策略并启用>或<生成所有策略并禁用>按钮生成所有学习记录的安全策略。

8. 当状态为“下发成功”后表示安全策略生成完成。

9. 单击<完成>按钮完成宽泛策略分析。

策略 NAT

本帮助主要介绍以下内容：

- 特性简介
  - 功能简介
  - 策略 NAT 类型
  - 策略 NAT 转换模式
  - 配置 NAT 支持双机热备
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置思路
  - 配置准备
  - 配置 NAT44 策略
  - 配置 NAT66 策略
  - 配置 NAT64 策略

特性简介

功能简介

NAT（Network Address Translation，网络地址转换）是将 IP 数据报文头中的 IP 地址转换为另一个 IP 地址的过程。在实际应用中，NAT 主要应用在连接两个网络的边缘设备上，用于实现允许内部网络用户访问外部公共网络以及允许外部公共网络访问部分内部网络资源（例如内部服务器）的目的。NAT 最初的设计目的是实现私有网络访问公共网络的功能，后扩展为实现任意两个网络间进行访问时的地址转换应用。

策略 NAT 用于定义一个或多个 NAT 转换规则，这些规则指定了报文匹配条件和转换行为。策略 NAT 支持的报文匹配条件包括源安全域和目的安全域、源地址和目的地址以及服务，满足所有已配置的匹配条件的报文将按指定行为转换其地址信息。

策略 NAT 适用于外部接口不固定的场景，当外部接口发生变化时，用户无需更改相关配置，降低了维护成本。

策略 NAT 类型

存在三种策略 NAT，不同策略 NAT 有不同的应用场景，具体如下：

- NAT44 策略：用于 IPv4 网络互通的 NAT 地址转换。

- NAT64 策略：用于 IPv4 与 IPv6 网络互通的 NAT 地址转换。
- NAT66 策略：用于 IPv6 网络互通的 NAT 地址转换。

策略 NAT 转换模式

策略 NAT 包含三种转换模式，不同转换模式有不同的转换行为，具体如下：

- 源地址转换

  该模式下，NAT 设备只转换报文的源 IP 地址和源端口，能够隐藏内网用户的 IP 地址。源地址转换支持 PAT 和 NO-PAT 模式。

- 目的地址转换

  该模式下，NAT 设备只转换报文的目的 IP 地址和目的端口，通常用于内网服务器对外部网络用户提供服务的场景。目的地址转换支持多对一地址转换和多对多地址转换两种模式。

  - 多对一地址转换：即将所有满足匹配条件的报文的目的 IP 地址和目的端口转换为同一个 IP 地址和端口，此时管理员只需要配置一个目的地址转换的地址和端口。
  - 多对多地址转换：根据管理员配置的原始报文的目的地址和服务（端口）数目以及目的地址转换的地址和端口数目来决定转换方式。此时管理员需要保证外网地址的数目×外网端口的数目和内网地址的数目×内网端口的数目相同，否则无法下发配置。该模式下管理员可以配置多个地址一个端口转换或一个地址多个端口转换，不支持地址和端口同时配置多个。

根据使用场景的不同，多对多地址转换支持以下几种内网和外网的地址转换配置。

表-1 多对多地址转换配置指导

使用场景	配置项	
	外网（原始报文的目的 IP 地址、服务）	内网（目的地址
允许外部用户通过一个外网地址访问内部服务器	一个外网地址	一个内网地址
允许外部用户通过一个外网地址、一个端口号访问内部服务器	一个外网地址，一个外网端口号	一个内网地址，一个
允许外部用户通过一个外网地址、多个不同的端口号访问内部服务器	一个外网地址，N个外网端口号	N个内网地址，一个
	一个外网地址，N个外网端口号	一个内网地址，N个
允许外部用户通过多个不同的外网地址访问内部服务器	N个外网地址	N个内网地址
允许外部用户通过多个不同的外网地址、一个端口号访问内部服务器	N个外网地址，一个外网端口号	一个内网地址，N个
	N个外网地址，一个外网端口号	N个内网地址，一个

- 源和目的地址转换

  该模式下，NAT 设备既转换报文的源 IP 地址和源端口，又转换报文的目的 IP 地址和目的端口。其中源地址转换支持 NO-PAT 和 PAT 模式，目的地址转换支持多对一地址转换和多对多地址转换模式。

配置 NAT 支持双机热备

在单台 NAT 设备的组网中，一旦发生单点故障，内网用户将无法与外网通信。采用双机热备可以很好的避免上述情况的发生。在双机热备组网中的两台设备均可承担 NAT 业务，并通过 RBM 通道进行会话热备、会话关联表项热备、NAT 端口块表项热备以及 NAT 配置的同步。当其中一台设备故障后，流量会切换到另一台正常工作的设备。关于双机热备的详细介绍，请参见“双机热备”中的详细介绍。

双机热备组网中的两台设备均可承担 NAT 业务，实际处理 NAT 业务的设备由 VRRP 备份组中的 Master 设备承担。在主备模式的双机热备组网中，静态 IP 地址转换、源 IP 地址转换、目的 IP 地址转换的部分转换规则会将转换后的公网 IP 地址或内部服务器对外提供服务的公网 IP 地址下发到地址管理。然后，主、备设备均会向同一局域网内所有节点或本地链路范围内所有节点通告公网 IP 与自身物理接口 MAC 地址的对应关系。导致与双机热备直连的上行三层设备可能会将下行报文发送给 HA 中的 Backup 设备，从而影响业务的正常运行。在双主模式的双机热备组网中，两台设备互为主备，仍然可能出现与双机热备直连的上行三层设备将下行报文发送给双机热备中的 Backup 设备，从而影响业务正常运行的情况。

为了避免上述情况的发生，需要将地址转换方式与 VRRP 备份组绑定。执行绑定操作后，仅 Master 设备收到对转换后 IP 地址或内部服务器对外提供服务的公网 IP 地址的 ARP 请求或 NS 请求后，才会回应 ARP 响应报文或 NA 响应报文，响应报文中携带的 MAC 地址为此 VRRP 备份组的虚拟 MAC 地址。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 策略 NAT 的优先级高于接口 NAT，同时配置策略 NAT 和接口 NAT 有可能导致接口 NAT 失效。因此，建议在策略 NAT 和接口 NAT 中任选其一进行配置。
- NAT 策略规则默认按配置顺序排序，可任意改变规则的先后次序。若设备上配置了多条 NAT 策略规则，规则的次序越靠前，生效优先级越高。
- 新建或复制 NAT 策略规则时，如果勾选<自动生成安全策略>，设备将依据上方配置的原始报文相关信息自动生成安全策略。如果勾选<自动生成安全策略>后又修改了上方配置的原始报文相关信息，请单击<更新>按钮自动同步修改安全策略。
- 一个 NAT 地址组被转换方式为“PAT”的 NAT 规则引用后，不能再被转换方式为“NO-PAT”的 NAT 规则引用，反之亦然。
- 若同时存在策略 NAT 和接口 NAT 配置可能导致接口 NAT 配置失效，具体关系如下：
    - 策略 NAT 中的 NAT 规则仅转换源地址，那么接口 NAT 中源地址转换的配置不生效，但是不会影响接口 NAT 中目的地址转换的配置。

    - 策略 NAT 中的 NAT 规则仅转换目的地址，那么接口 NAT 中转换目的地址的配置不生效，但是不会影响接口 NAT 中源地址转换的配置。
    - 策略 NAT 中的 NAT 规则既转换源地址又转换目的地址，那么接口 NAT 中转换源地址和转换目的地址的配置均不生效。
- 配置地址组时，各地址组成员的 IP 地址段不能互相重叠。
- NAT 规则引用的地址对象组中不能配置主机名。
- 当引用的地址对象组中包含对象组或通配符掩码时，可能会对配置性能和流量匹配性能产生影响。为了保证网络的稳定和流畅，建议引用的地址对象组中尽量避免使用对象组或通配符掩码添加对象。

配置指南

本章节重点介绍配置 NAT 地址转换的思路和步骤。

NAT 地址转换中涉及入方向和出方向两个概念，下面以两个示意图为例进行说明。

- 入方向：对安全域上收到的报文进行地址转换，即入安全域上配置地址转换，如图-1 所示。
- 出方向：对安全域上发送的报文进行转换，即出安全域上配置地址转换，如图-2 所示。

图-1 入安全域地址转换示意图

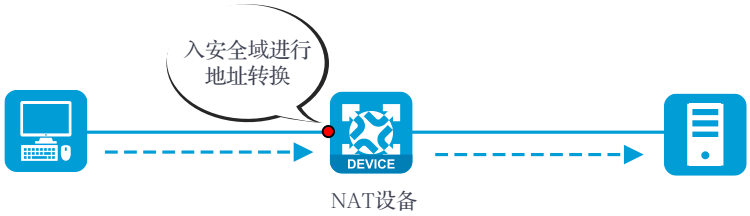
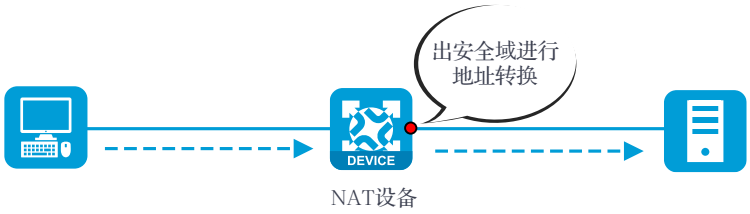


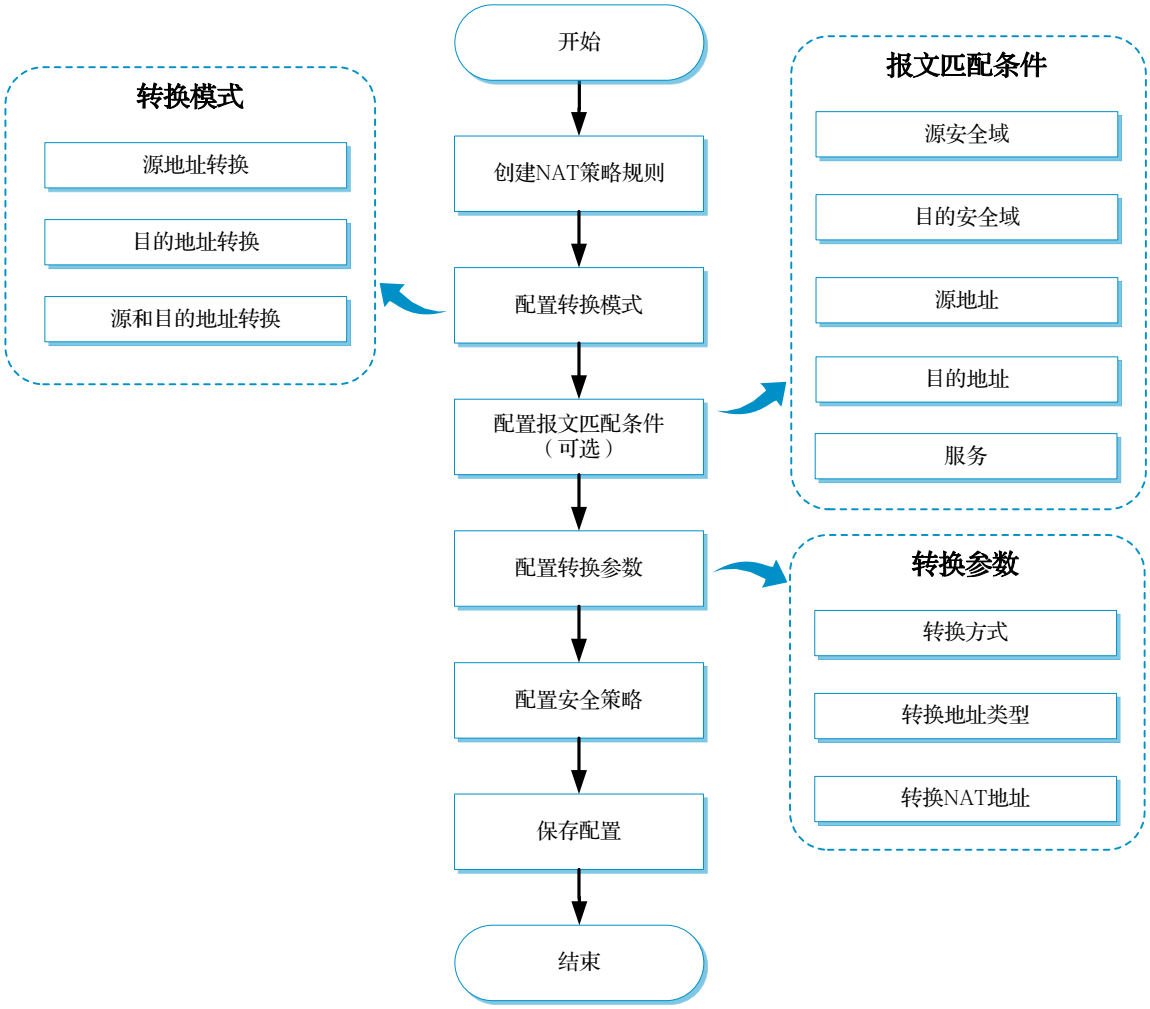
图-2 出安全域地址转换示意图



配置思路

策略 NAT 支持基于安全域、地址对象组和服务对象组的报文匹配条件，支持源地址转换、目的地址转换以及源和目的地址转换，配置思路如下图所示。

图-3 策略 NAT 配置指导图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。

- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置 NAT44 策略

具体配置步骤如下：

1. 创建安全域（可选），具体配置过程略。
2. 创建地址对象组（可选），具体配置内容请参见“对象组”中的详细介绍。
3. 创建服务对象组（可选），具体配置过程略。
4. 创建 NAT 地址组（可选）
   a. 选择“对象 > 对象组 > NAT 地址组”。
   b. 单击<新建>，创建 NAT 地址组。具体配置内容请参见“对象组”中的“NAT 地址组配置”。
   c. 单击<确定>，完成 NAT 地址组配置。
5. 创建 NAT44 策略规则
   a. 选择“策略 > 策略 NAT”。
   b. 在策略 NAT 页面选择转换模式，进入对应的转换规则页面。

表-2 转换模式说明

转换模式	说明
新建源地址转换	仅转换原始报文的源地址信息
新建目的地址转换	仅转换原始报文的目的地址信息
新建源和目的地址转换	既转换原始报文的源地址信息又转换原始报文的

c. 选择“NAT44”页签，进行 NAT44 策略规则配置。

表-3 NAT44 策略配置说明

配置项		说明
当IP地址符合以下条件时	源安全域	配置源安全域作为报文匹配条件
	目的安全域	配置目的安全域作为报文匹配条件 仅在转换模式为新建源地址转换时显示
	源地址	配置IP地址、网段或对象组作为报文源地址
	目的地址	配置IP地址、网段或对象组作为报文目的地 如果转换模式选择为目的地址转换或源和目 地址
	服务	配置服务对象组作为报文匹配条件

	转换方式	选择源地址转换方式，分为如下四种： • 接口 IP 地址：使用设备出接口的 IP 地址 • 动态 IP：使用 PAT 或 NO-PAT 方式动态 • 静态 IP：将报文源 IP 地址转换为固定的 • 不做转换：不使用此规则，也不使用任何
	地址类型	选择源地址转换使用的NAT地址的类型，分为 • 地址对象组：使用地址对象组中的 IP 地 • NAT 地址组：使用 NAT 地址组中的 IP 地 • IP 地址：使用固定的 IP 地址进行源地址 • 网段地址：使用网段中的 IP 地址进行源
将源地址转换为	转换为地址	配置源地址转换使用的NAT地址
	绑定的IPv4 vrrp备份组	配置此功能后，所绑定VRRP备份组（IPv4） IP地址和虚拟MAC地址响应报文。双机热备 同设备的支持情况不同，请以设备Web页面
	允许反向地址转换	在内网用户主动向外网发起连接并成功触发 向该内网用户发起的连接使用已建立的地址 该项仅转换方式选择为“动态IP”时可配置
	端口转换	开启时使用PAT方式动态转换报文源地址， 不开启时使用NO-PAT方式动态转换报文源
	优先使用原始端口	PAT方式分配端口时优先使用报文的原始源 时才使用其他端口进行转换 该项仅转换方式选择为“动态IP”或“接口

将目的地址转换为	转换方式	选择目的地址转换方式，分为如下三种： • IP 地址：将报文目的 IP 地址转换为固定 • 地址对象组转换：将报文目的 IP 地址转 • 不做转换：不使用此规则，也不使用任
	转换为地址	配置目的地址转换使用的NAT地址
	转换为端口	设置转换后报文的目的端口
	绑定的IPv4 vrrp备份组	配置此功能后，所绑定VRRP备份组（IPv4 拟IP地址和虚拟MAC地址响应报文。双机热 不同设备的支持情况不同，请以设备Web页
通用设置	名称	NAT44策略规则的名称，支持中文
	启用	启用此NAT44策略规则
	自动生成安全策略	配置此功能后，设备将依据上方配置的原始
高级设置	描述	NAT44策略规则的备注信息
	转换前报文所属VRF	表示转换前报文所属的VRF
	转换后报文所属VRF	表示转换后报文所属的VRF
	统计	开启此NAT44策略规则的命中次数统计功能

d. 单击<确定>，完成 NAT44 策略规则配置。

配置 NAT66 策略

具体配置步骤如下：

1. 创建安全域（可选），具体配置过程略。
2. 创建地址对象组（可选），具体配置内容请参见“对象组”中的详细介绍。
3. 创建服务对象组（可选），具体配置内容请参见“对象组”中的详细介绍。
4. 创建 NAT66 策略规则
   a. 选择“策略 > 策略 NAT”。
   b. 在策略 NAT 页面选择转换模式，进入对应的转换规则页面。

表-4 转换模式说明

转换模式	说明
新建源地址转换	仅转换原始报文的源地址信息
新建目的地址转换	仅转换原始报文的目的地址信息
新建源和目的地址转换	既转换原始报文的源地址信息又转换原始报文的

   c. 选择“NAT66”页签，进行 NAT66 策略规则配置。

表-5 NAT66 策略配置说明

配置项		说明
当IP地址符合以下条件时	源安全域	配置源安全域作为报文匹配条件
	目的安全域	配置目的安全域作为报文匹配条件 仅在转换模式为新建源地址转换时显示
	源地址	配置IP地址、网段或对象组作为报文源地址匹配
	目的地址	配置IP地址、网段或对象组作为报文目的地址匹 如果转换模式选择为目的地址转换或源和目的地址
	服务	配置服务对象组作为报文匹配条件
将源地址转换为	转换方式	选择源地址转换方式，分为如下四种： • NPTv6：使用 NPTv6 方式转换报文源地址，地址前缀。此方式必须配置 IP 地址类型的原始 • 动态 IP：使用 PAT 或 NO-PAT 方式动态转换 • 静态 IP：将报文源 IP 地址转换为固定的 IP • 不做转换：不使用此规则，也不使用任何优
	地址类型	选择源地址转换使用的NAT地址的类型，分为如 • 地址对象组：使用地址对象组中的 IP 地址进 • 网段地址：使用网段中的 IP 地址进行源地址
	转换为地址	配置源地址转换使用的NAT地址

	端口转换	开启时使用PAT方式动态转换报文源地址，既转 不开启时使用NO-PAT方式动态转换报文源地址
	绑定的IPv6 vrrp备份组	配置此功能后，所绑定VRRP备份组（IPv6源备 地址和虚拟MAC地址响应报文。双机热备组网环 备的支持情况不同，请以设备Web页面的实际支
	IPv6前缀	配置“前缀转换”所对应的IPv6地址前缀 该项仅转换方式选择为“NPTv6”时可配置
	前缀长度	配置“IPv6前缀”的长度 该项仅转换方式选择为“NPTv6”时可配置
将目的地址转换为	转换方式	选择目的地址转换方式，分为如下三种： • NPTv6：使用 NPTv6 方式转换报文目的地 的地址前缀 • IP 地址：将报文目的 IP 地址和目的端口转 • 不做转换：不使用此规则，也不使用任何 址
	转换为地址	设置转换后报文的目的IP地址
	转换为端口	设置转换后报文的目的端口
	IPv6前缀	配置NPTv6转换所使用的IPv6地址前缀 该项仅动作选择为“NPTv6”时可配置
	前缀长度	配置“IPv6前缀”的长度 该项仅动作选择为“NPTv6”时可配置

通用设置	名称	NAT66策略规则的名称，支持中文
	启用	启用此NAT66策略规则
高级设置	描述	NAT66策略规则的备注信息
	转换前报文所属VRF	表示转换前报文所属的VRF
	转换后报文所属VRF	表示转换后报文所属的VRF
	统计	开启此NAT66策略规则的命中次数统计功能

d. 单击<确定>，完成 NAT66 策略规则配置。

配置 NAT64 策略

具体配置步骤如下：

1. 创建安全域（可选），具体配置过程略。
2. 创建地址对象组（可选），具体配置内容请参见“对象组”中的详细介绍。
3. 创建服务对象组（可选），具体配置内容请参见“对象组”中的详细介绍。
4. 创建 NAT64 策略规则
   a. 选择“策略 > 策略 NAT”。
   b. 在策略 NAT 页面选择“新建源和目的地址转换”，进入对应的转换规则页面。

c. 选择“NAT64”页签，进行 NAT64 策略规则配置。

表-6 NAT64 策略配置说明

配置项		说明
转换模式	V4toV6	适用于IPv4网络主动访问IPv6网络的场景，转换原始报文的源
	V6toV4	适用于IPv6网络主动访问IPv4网络的场景，转换原始报文的源
当IP地址符合以下条件时	源安全域	配置源安全域作为报文匹配条件
	源地址	配置IP地址、网段或对象组作为报文源地址匹配条件
	目的地址	配置IP地址、网段或对象组作为报文目的地址匹配条件
	服务	配置服务对象组作为报文匹配条件
将源地址转换为	转换方式	选择源地址转换方式，分为如下三种： • 动态 IP：使用 PAT 或 NO-PAT 方式动态转换报文源地址 • 静态 IP：将报文源 IP 地址转换为固定的 IP 地址 • 前缀：利用 IPv6 前缀转换报文源 IP 地址
	转换为地址	配置源地址转换使用的NAT地址 该项仅转换方式选择为“动态IP”或“静态IP”时可配置
	端口转换	开启时使用PAT方式动态转换报文源地址，既转换报文源IP地 口；不开启时使用NO-PAT方式动态转换报文源地址，只转换报
	绑定的IPv4 vrrp	配置此功能后，所绑定VRRP备份组（IPv4源备份组）中的Ma 拟IP地址和虚拟MAC地址响应报文。双机热备组网环境中需要

	备份组	能不同设备的支持情况不同，请以设备Web页面的实际支持情
	绑定的IPv6 vrrp备份组	配置此功能后，所绑定VRRP备份组（IPv6源备份组）中的Ma 拟IP地址和虚拟MAC地址响应报文。双机热备组网环境中需要 能不同设备的支持情况不同，请以设备Web页面的实际支持情
	前缀转换	选择前缀转换的类型，分为如下三种： • General 前缀：使用 General 前缀进行源地址转换 • IVI 前缀：使用 IVI 前缀进行源地址转换 • NAT64 前缀：使用 NAT64 前缀进行源地址转换 该项仅转换方式选择为“前缀转换”时可配置
	IPv6前缀	配置“前缀转换”所对应的IPv6地址前缀 该项仅前缀转换选择为“General前缀”或“NAT64前缀”时可
	前缀长度	配置“IPv6前缀”的长度 该项仅前缀转换选择为“General前缀”或“NAT64前缀”时可
将目的地址转换为	转换方式	选择目的地址转换方式，分为如下三种： • 前缀：利用 IPv6 前缀转换报文目的 IP 地址 • 服务器地址：将报文目的 IP 地址和目的端口转换为固定的 • 静态 IP：将报文目的 IP 地址转换为固定的 IP 地址
	前缀转换	选择前缀转换的类型，分为如下三种： • General 前缀：使用 General 前缀进行源地址转换 • IVI 前缀：使用 IVI 前缀进行源地址转换 • NAT64 前缀：使用 NAT64 前缀进行源地址转换 该项仅动作选择为“前缀转换”时可配置

	IPv6前缀	配置“前缀转换”所对应的IPv6地址前缀 该项仅前缀转换选择为“General前缀”或“IVI前缀”时可配置
	前缀长度	配置“IPv6前缀”的长度 该项仅前缀转换选择为“General前缀”时可配置
	绑定的IPv4 vrrp备份组	配置此功能后，所绑定VRRP备份组（IPv4目的备份组）中的M 虚拟IP地址和虚拟MAC地址响应报文。双机热备组网环境中需要 功能不同设备的支持情况不同，请以设备Web页面的实际支持情
	绑定的IPv6 vrrp备份组	配置此功能后，所绑定VRRP备份组（IPv6目的备份组）中的M 虚拟IP地址和虚拟MAC地址响应报文。双机热备组网环境中需要 功能不同设备的支持情况不同，请以设备Web页面的实际支持情
	转换为地址	设置转换后报文的目的IP地址
	转换为端口	设置转换后报文的目的端口 该项仅动作选择为“服务器地址转换”时可配置
通用设置	名称	NAT64策略规则的名称，支持中文
	启用	启用此NAT64策略规则
高级设置	描述	NAT64策略规则的备注信息
	转换前报文所属VRF	表示转换前报文所属的VRF
	转换后报文所属VRF	表示转换后报文所属的VRF
	统计	开启此NAT64策略规则的命中次数统计功能

d. 单击<确定>，完成 NAT64 策略规则配置。

Web 应用防护

本帮助主要介绍以下内容：

- 特性简介
  - Web 应用防护特征
  - 语义分析检测
  - 配置文件动作
  - Web 应用防护实现流程
  - 防篡改
  - CC 攻击防护
- vSystem 相关说明
- License 支持情况
- 使用限制和注意事项
- 配置指南
  - 配置思路
  - 配置准备
  - 缺省 Web 应用防护配置任务

- 定制化 Web 应用防护配置任务
- 管理 Web 应用防护自定义特征
- 配置 Web 应用防护白名单

特性简介

Web 应用防护功能用于阻断 Web 应用层攻击，保护内网用户和内部 Web 服务器。当设备收到来自外部的 HTTP 或 HTTPS 请求后，会执行防护策略，对请求内容的安全性和合法性进行检测和验证，对非法的请求予以实时阻断，从而对内网的用户和 Web 服务器进行有效防护。

Web 应用防护特征

Web 应用防护特征用来扫描网络中的攻击行为以及对攻击行为采取防御措施，设备通过将数据流与 Web 应用防护特征进行比较来检测和防御攻击。

Web 应用防护特征包含多种属性，例如攻击分类、动作、保护对象、严重级别和方向。这些属性可作为过滤条件来筛选 Web 应用防护特征。

设备支持如下类型的特征：

- 预定义特征：由系统中的特征库自动生成，不可进行修改和删除。
- 自定义特征：由用户手工配置。可以创建、修改和删除。

特征例外

缺省情况下，设备基于配置文件统一动作对符合 Web 应用防护特征的报文进行处理。当需要对符合某个 Web 应用防护特征的报文采取不同的动作时，可以将此特征设置为特征例外。或者，当 Web 应用防护配置文件中不包含某个 Web 应用防护特征时，可以将此特征设置为特征例外，添加到该 Web 应用防护配置文件中。

特征例外中动作的优先级高于配置文件统一动作的优先级。

语义分析检测

语义分析检测基于对报文中的 SQL 语法进行分析来检测 SQL 注入攻击行为。

开启本功能后，设备将同时使用特征匹配和语义分析检测对 SQL 注入攻击进行识别，可以提升该类攻击的识别率。

配置文件动作

配置文件动作是指设备对匹配上 Web 应用防护特征或经过语义分析检测识别出攻击的报文做出的处理。动作包括如下几种类型：

- 黑名单：丢弃报文并将报文的源 IP 地址加入 IP 黑名单。如果设备上同时开启了 IP 黑名单过滤功能，则阻断时间内（在安全动作中的阻断功能中配置）来自此 IP 地址的所有报文将被直

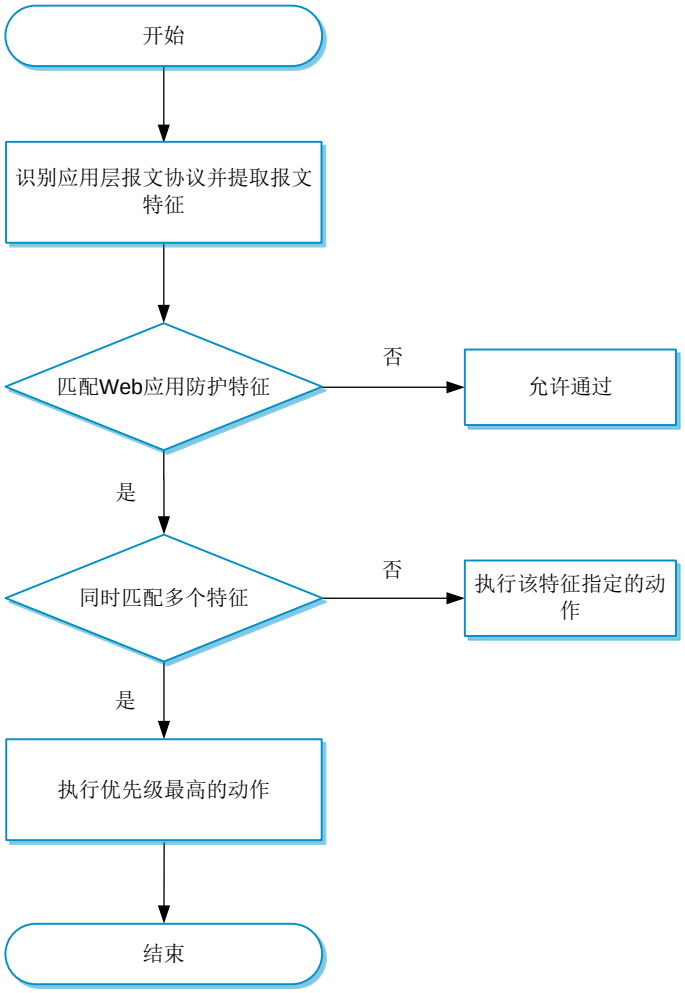
接丢弃;如果设备上未开启黑名单过滤功能,报文的源 IP 地址仍会被添加到 IP 黑名单表项中,但后续来自该源 IP 地址的报文不会被直接丢弃。有关黑名单功能的详细介绍请参见“攻击防范”。

- 丢弃:丢弃报文。
- 允许:允许报文通过。
- 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。
- 重定向:把报文重定向到指定的 Web 页面上。
- 缺省:对通过特征匹配方式检测出攻击的报文执行该特征的缺省动作;对通过语义分析检测方式识别出攻击的报文,会以快速日志输出的方式发送 Web 应用防护日志。
- 抓包:捕获报文。
- 日志:记录日志信息。

Web 应用防护实现流程

在设备配置了 Web 应用防护功能的情况下,当用户的数据流量经过设备时,设备将进行 Web 应用防护处理。处理流程如图-1 所示:

图-1 Web 应用防护数据处理流程图



Web 应用防护处理的整体流程如下：

2. 如果报文匹配了某条安全策略，且此策略的动作是**允许并引用了 Web 应用防护配置文件**，则设备将对报文进行深度内容检测：首先，识别报文的协议，然后根据协议分析方案进行更精细的分析，并深入提取报文特征。其中，如果配置文件中开启了语义分析检测功能，则同时提取报文中的 SQL 语句信息。

3. 设备将提取的报文特征与 Web 应用防护特征进行匹配，并对匹配成功的报文进行如下处理：

- 如果报文同时与多个 Web 应用防护特征匹配成功，则根据这些动作中优先级最高的动作进行处理。动作优先级从高到低的顺序为：重置 > 重定向 > 丢弃 > 允许。但是，对于**黑名单**、**日志**和**捕获**三个动作只要匹配成功的特征中存在就会执行。
- 如果报文只与一个Web应用防护特征匹配成功，则根据此特征中指定的动作进行处理。

其中，如果配置文件中开启了语义分析检测功能，则设备将同时对报文中的 SQL 语句进行语法分析。如果检测到攻击，则进行如下判断：

- 如果指定了配置文件动作，则执行指定的动作。
- 如果未指定配置文件动作，则以快速日志方式输出 Web 应用防护日志。
- 当设备通过特征匹配和语义分析功能同时检测出攻击时，则执行两种检测方式下严重级别最高的动作。其中，只要一种检测方式下开启了日志记录功能，设备就会记录日志。

4. 如果报文未与任何 Web 应用防护特征匹配成功且语义分析检测也未识别出攻击时，则设备直接允许报文通过。

防篡改

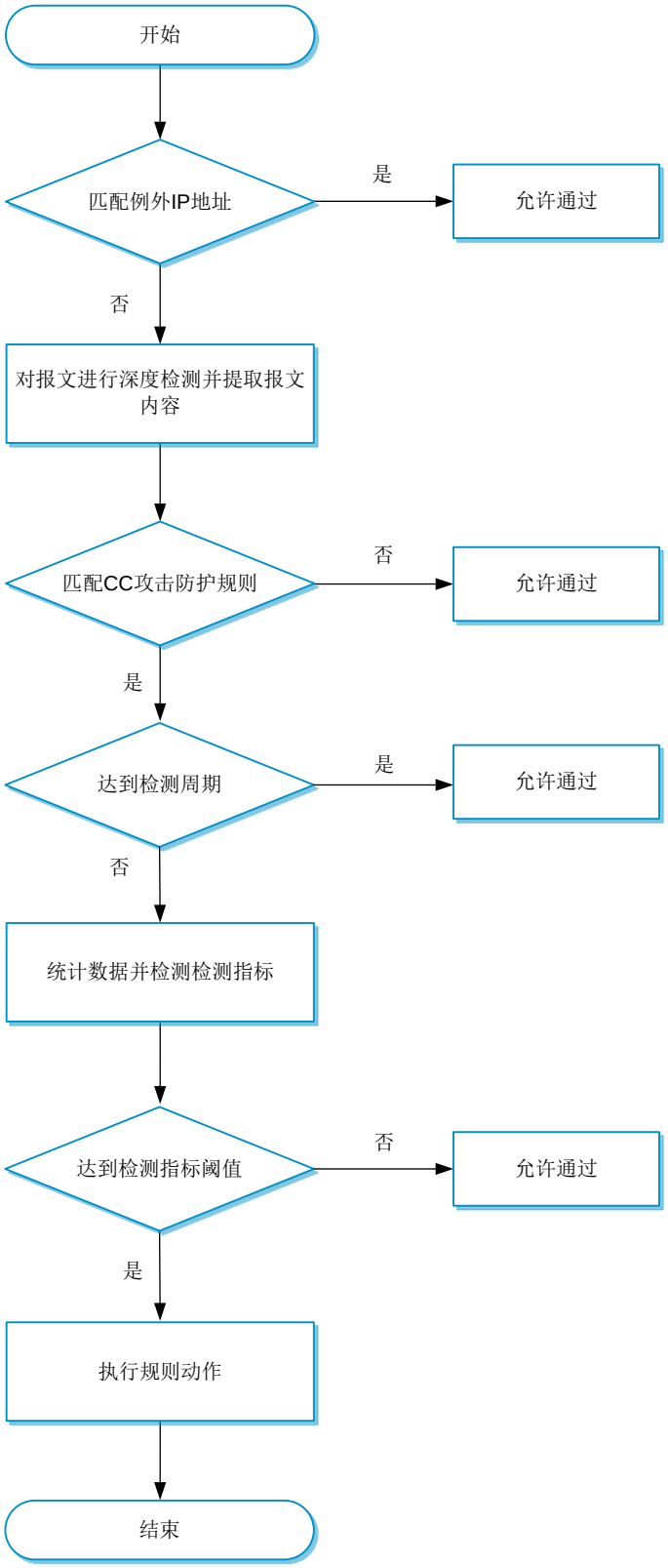
防篡改功能用于对客户端访问的服务器网页内容进行检测，判断其内容是否被篡改。如果被篡改，设备支持对篡改后的页面进行恢复，防止被篡改后的网页信息发布到客户端。

CC 攻击防护

CC(Challenge Collapsar)攻击防护是一种对以网站页面为目标的攻击进行阻断的应用层安全防护功能。CC 攻击防护通过对来自 Web 应用程序客户端的请求进行内容检测、规则匹配和统计计算，对攻击请求予以实时阻断，从而对内网的 Web 服务器进行有效防护。

CC 攻击防护功能是通过在安全策略中引用 Web 应用防护配置文件，并且在 Web 应用配置文件中引用 CC 攻击防护配置文件来实现的。当用户的数据流量经过设备时，设备将进行 CC 攻击防护处理。处理流程如下图所示：

图-2 CC 攻击防护数据处理流程图



2. 如果报文与例外 IP 地址匹配成功，则直接放行该报文。

3. 设备对报文进行深度内容检测，并提取报文内容。

4. 设备将提取的报文内容与 CC 攻击防护规则进行匹配，并进行如下处理：

   - 如果未匹配到任何 CC 攻击防护规则，则设备对报文执行允许动作。
   - 如果匹配到一条 CC 攻击防护规则，则不再进行后续规则匹配，进入步骤 4 处理。

5. 如果当前处于检测周期内，则对报文数据进行统计，并与规则下配置的检测指标阈值进行比较，并进行如下处理：

   - 如果达到阈值，则执行规则下配置的动作，包括允许、黑名单和记录日志。
   - 如果未达到阈值，则放行报文。

6. 如果当前处理超过检测周期，则不对报文内容进行统计，直接放行报文。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

License支持情况

Web 应用防护功能需要购买并正确安装 License 后才能使用。License 过期后，Web 应用防护功能可以采用设备中已有的 Web 应用防护特征库正常工作，但无法升级到官方网站在过期时间后发布的新版本的特征库。关于 License 的详细介绍请参见“License 配置”。

使用限制和注意事项

- 执行"提交"操作会暂时中断 DPI 业务的处理，可能导致其他基于 DPI 功能的业务同时出现中断。例如，安全策略无法对应用进行访问控制等。
- 执行“提交”操作后，界面上会提示设置成功，但是配置文件此时可能尚未完成激活，如果此时报文经过设备，可能会出现暂时无法识别的情况。
- 数值类型的自定义特征规则仅支持配置一个检查项。
- 如果配置文件中仅修改语义分析检测功能或 CC 攻击防护功能的相关配置时，不需要提交配置变更即可生效。
- 配置 Web 应用防护白名单时，特征 ID、URL 和 IP 地址请至少选择其中一项进行配置。
- 通过语义分析功能检测出的攻击，其特征 ID 固定为 4294967295。如果希望将此特征 ID 添加到白名单表项中，则需要先在白名单表项中配置源 IP 地址或 URL。

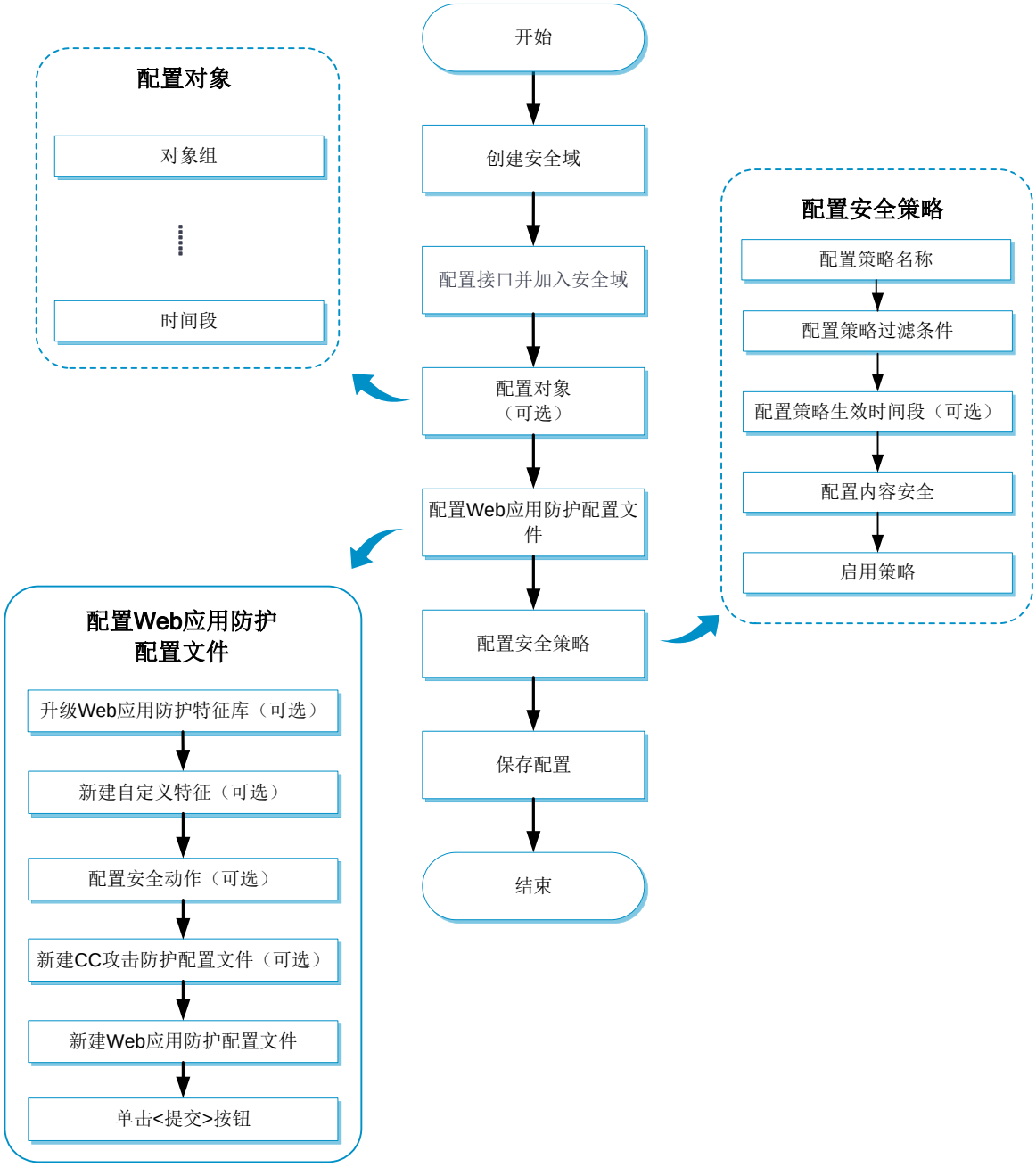
- 当 Web 应用防护白名单中配置的 IP 地址为真实源 IP 地址时，用户必须同时配置真实源 IP 地址检测功能。有关真实源 IP 地址检测功能的详细介绍，请参见“高级配置”。
- 当服务器采用分块传输方式发送 HTTP 响应报文时，设备会因为无法获取到报文主体数据的开始和结束位置导致不能正常学习相应的静态网页资源，设备无法进行网页防篡改检测。

配置指南

配置思路

Web 应用防护功能的配置思路如下图所示：

图-3 Web 应用防护功能配置指导图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

缺省 Web 应用防护配置任务

设备上存在一个名称为 default 的 Web 应用防护配置文件，缺省 Web 应用防护配置文件使用当前系统中所有缺省处于启用状态的 Web 应用防护特征，缺省 Web 应用防护配置文件不能修改和删除。

如果需要检测当前系统中的所有 Web 应用防护特征，可使用缺省 Web 应用防护配置文件，从而简化操作并节省时间。

1. 选择“策略 > Web 应用防护 > 配置文件”。default 的 Web 应用防护配置文件不可编辑。
2. 在安全策略的内容安全配置中引用此 Web 应用防护配置文件，有关安全策略的详细配置介绍请参见“安全策略”。

定制化 Web 应用防护配置任务

使用缺省 default 的 Web 应用防护配置文件不满足需求时，可创建自定义的配置文件。管理员可以基于业务环境和安全需求灵活调整自定义 Web 应用防护配置文件中例外特征的相关属性，。包括特征的状态、动作、日志和抓包功能等。

1. 选择“策略 > Web 应用防护 > 配置文件”。

2. 在“Web 应用防护配置文件”页面单击<新建>按钮，进入“新建 Web 应用防护配置文件”页面。在基础参数区域配置如下内容：

表-1 Web 应用防护配置文件-基础参数区域配置内容

参数	说明
名称	Web应用防护配置文件的名称
CC攻击防护配置文件	用于引用CC攻击防护配置文件
语义分析检测	语义分析检测基于对报文中的SQL语法进行分析来检测SQL注入攻击行为 开启本功能后，设备将同时使用特征匹配和语义分析检测对SQL注入攻击进行识别，攻击的识别率
配置文件动作	当设备通过特征匹配或语义分析检测功能识别出攻击后，将对报文执行本命令配置的 其中，如果动作为缺省，则表示对特征匹配方式检测出攻击的报文执行该特征的缺省分析检测方式识别出攻击的报文，会以快速日志输出的方式发送Web应用防护日志

日志	开启日志功能后，设备将对检测出Web攻击的报文生成日志信息
抓包	开启抓包功能后，设备会将捕获到的报文保存在本地并输出到指定的路径，有关捕获 置，请参见“安全动作”

3. 在服务器信息隐藏区域，可配置服务器信息隐藏功能的具体参数，使设备对指定协议或字段中包含的服务器信息进行隐藏，防止服务器信息泄露。具体配置内容如下：

表-2 Web 应用防护配置文件-服务器信息隐藏区域配置内容

参数	说明
FTP协议应答信息	FTP协议报文的应答信息中包含了服务器版本等信息，开启本功能后，设备会对应答 防止服务器信息暴露
HTTP协议头部字段	HTTP响应报文的头部字段中可能包含服务器信息，配置本功能后，设备会对指定头部 隐藏，防止客户端通过指定字段获取服务器信息
错误响应状态码页面	错误状态码返回页面中可能包含服务器信息，配置本功能后，设备会对指定错误状态 内容进行隐藏，防止客户端通过该页面获取服务器版本等信息

4. 在筛选特征区域，可通过配置筛选条件（例如保护对象、攻击分类和方向等）灵活选择此 Web 应用防护配置文件中所需的 Web 应用防护特征。单击<查看特征筛选结果>按钮，可查看当前配置文件中已选择的 Web 应用防护特征。若不配置任何一项筛选条件（即保持缺省情况），则此配置文件中将会包含所有缺省处于启用状态的 Web 应用防护特征。具体配置内容如下：

表-3 Web 应用防护配置文件-筛选特征区域配置内容

参数	说明
保护对象	通过选择保护对象可快速选择所需的Web应用防护特征
攻击分类	通过选择攻击分类可快速选择所需的Web应用防护特征
方向	Web应用防护特征库中的特征分为服务端和客户端两类，可通过选择服务端和客户端 件所需的Web应用防护特征
缺省动作	Web应用防护特征的缺省动作分为如下四种：丢弃、允许、重置、黑名单，可通过选 动作来筛选配置文件所需的Web应用防护特征
严重级别	Web应用防护特征的严重级别分为如下四种：严重、高、中、低，可通过选择不同的 选配置文件所需的Web应用防护特征

5. 在设置例外特征区域，可通过如下两种方式添加例外特征。

   - 在特征例外输入框中直接输入 Web 应用防护特征的 ID 号，然后单击右边<添加>按钮，即可把此特征加入特征例外中。
   - 先单击<查看特征筛选结果>按钮，进入“查看特征”页面，在此页面选中需要加入特征例外的 Web 应用防护特征，然后单击此页面上方的<添加到例外列表>按钮，在弹出的“修改例外特征”页面中修改特征的动作和状态等。单击<确定>按钮，即可把此特征加入特征例外中。

在特征例外列表中，单击目标 Web 应用防护特征右边的<编辑>按钮，进入“修改例外特征”页面，在此页面可配置此特征的动作、状态、日志和抓包功能。单击<确定>，此例外特征修改成功。

6. 单击<确定>按钮，新建 Web 应用防护配置文件成功，且会在“Web 应用防护配置文件”页面中显示。

7. 在安全策略的内容安全配置中引用此 Web 应用防护配置文件，具体配置步骤请参见“缺省 Web 应用防护配置任务”章节。

8. 单击<提交>按钮，激活 Web 应用防护配置文件的配置内容。配置此功能会暂时中断 DPI 业务的处理，为避免重复配置此功能对 DPI 业务造成影响，请完成部署 DPI 各业务模块的配置文件后统一配置此功能。

防篡改配置任务

防篡改功能分为学习阶段和工作阶段。开启网页自学习功能后，防篡改功能将进入处于学习阶段。在此阶段中，设备会对服务器网页内容进行学习，生成基线文件。管理员可以通过查看自学习 URL 列表，判断设备是否已完成学习，如果已完成学习，可以关闭网页自学习功能，防篡改将进入工作阶段。在工作阶段，设备会对服务器返回给客户端的响应报文中的网页文件进行缓存，再使用基线文件与其进行对比。如果一致，则认为服务器网页文件未被篡改，否则，则认为网页文件已被篡改。

1. 选择“策略 > Web 应用防护 > 配置文件”。

2. 新建一个 Web 应用防护配置文件，或者编辑已有的 Web 配置文件。在防篡改区域进行如下配置：

表-4 配置防篡改功能

参数	说明
防篡改功能	开启本功能后，设备可对客户端访问的网页内容进行检测，判断内容是否被篡改，[后的页面进行恢复，防止被篡改后的网页信息发布到客户端
网页自学习功能	开启本功能后，设备会对客户端访问的网页内容进行学习，并将学习到的页面内容保 当设备未挂载硬盘时，基线文件保存在内存中，设备重启后会被清空。当设备挂载 文件会被保存在硬盘中，可以长时间保存 学习到的URL可以到“Web应用防护 > 配置文件 > 自学习URL列表”页面查看。其[到路径（path）字段
文件类型	防篡改功能检测的文件类型，包括如下取值： • XLS（支持扩展名为 xl 和 xla） • HLP（支持扩展名为 hlp 和 chm） • PPT（支持扩展名为 ppt、ppz、pps、pot 和 pptx） • DOC（支持扩展名为 doc 和 dot） • PE（支持扩展名为 bin、exe、com 和 dll） • PDF（支持扩展名为 pdf） • SWF（支持扩展名为 swf 和 cab） • ZIP（支持扩展名为 zip） • GIF（支持扩展名为 gif） • JPEG（支持扩展名为 jpeg、jpg 和 jpe）

	• CSS（支持扩展名为 css） • HTML（支持扩展名为 html 和 htm） • TXT（支持扩展名为 txt）
工作模式	防篡改功能的工作模式，包括如下取值： • 监控模式：此模式下，当设备检测到用户访问网页的内容被篡改时，仅记录日志 • 保护模式：此模式下，当设备检测到用户访问网页的内容被篡改时，会将响应报容替换为通过网页自学习功能学习到的基线内容，返回给客户端，并记录日志。备配置了 TCP 代理时生效。有关 TCP 代理的详细介绍，请参见“应用代理”
自定义静态资源	用来添加防篡改功能检测的静态网页资源路径，配置步骤如下： 1. 单击<添加>按钮，进入添加自定义静态资源页面 2. 配置主机名、请求方法和 URI。其中，URI 必须以“/”开头 3. 单击<确定>按钮，完成配置

3. 单击<确定>按钮，完成配置。

CC 攻击防护配置任务

设备基于 CC 攻击防护配置文件对攻击报文进行处理，且 CC 攻击防护配置文件仅在被 Web 应用防护配置文件引用后才能生效。

CC 攻击防护配置文件中可以配置匹配报文的过滤条件以及检测指标等，管理员可以根据实际需求进行配置。

1. 选择“策略 > Web 应用防护 > CC 攻击防护配置文件”。

2. 在“CC 攻击防护配置文件”页面单击<新建>按钮，进入“新建 CC 攻击防护配置文件”页面。

   在“基本配置”区域可配置 CC 攻击防护配置文件的基本信息，具体配置内容如下：

表-5 新建 CC 攻击防护配置文件

参数	说明
名称	CC攻击防护配置文件的名称
描述	通过合理编写描述信息，便于管理员快速理解和识别CC攻击防护配置文件的作用，在
例外IP地址	如果用户HTTP报文中的源IP地址与例外IP地址匹配成功，则直接允许此报文通过；则继续进行后续的CC攻击检测
检测周期	用于检测是否存在CC攻击行为的计时周期，从一条流的首个报文命中CC攻击防护规

3. 在“CC 攻击防护规则”区域可配置 CC 攻击防护规则，单击<新建>按钮，进入新建 CC 攻击防护规则页面，具体配置内容如下：

表-6 新建 CC 攻击防护规则

参数	说明
规则名称	CC攻击防护规则的名称
目的IPv4地址	配置作为CC攻击防护规则过滤条件的目的IPv4地址

目的IPv6地址	配置作为CC攻击防护规则过滤条件的目的IPv6地址
目的端口	配置作为CC攻击防护规则过滤条件的目的端口
请求方法	配置作为CC攻击防护规则过滤条件的请求方法
防护路径	配置防护的网站资源的路径
X-Forwarded-For 检测	开启X-forward-For字段检测功能后，设备将从客户端HTTP请求报文头的X-forward-f 的源IP地址，本功能适用于客户端使用代理方式访问服务器的场景
检测指标	用于检测是否存在CC攻击的指标项，包括请求速率和请求集中度 • 请求速率：用于检测客户端是否过于频繁地访问某网站，包括如下参数： ○ 速率阈值：表示一个检测周期内，访问任意防护路径的最大次数 • 请求集中度：用于检测客户端是否主要针对某网站进行访问，包括如下参数： ○ 访问基数：表示所有访问路径的命中总次数，仅当达到访问基数后，才计 ○ 集中度阈值：表示最常访问的防护路径的访问次数占所有防护路径访问总
动作	配置CC攻击的防护动作，包括允许和黑名单。配置动作为黑名单后，还需要配置黑
日志	开启日志记录功能后，当设备检测出存在CC攻击时，将记录日志

4. 单击<确定>按钮，完成 CC 攻击防护规则的配置。

5. 单击<确定>按钮，完成 CC 攻击防护配置文件的配置。

6. 选择“对象 > 安全配置文件 > Web 应用防护 > 配置文件”。

7. 在“Web 应用防护配置文件”页面编辑或者新建一个 Web 应用防护配置文件，在配置文件中引用 CC 攻击防护配置文件。新建 Web 应用防护配置文件的步骤请参见“定制化 Web 应用防护配置任务”。

8. 单击<提交>按钮，激活 Web 应用防护配置文件的配置内容。

管理 Web 应用防护自定义特征

当需要的特征在设备当前特征库中不存在时，用户可通过手工配置的方式新建自定义特征。

自定义特征包括属性和规则。

一个自定义特征下可配置多条规则，规则间包含如下规则逻辑：

- 逻辑与：表示报文需要匹配该自定义特征的所有规则才认为与该特征匹配成功。
- 逻辑或：表示报文匹配到该自定义特征的任何一条规则即认为与该特征匹配成功。

自定义特征规则下支持配置规则的匹配条件（包括源/目的 IPv4 地址、源/目的端口、请求方法等）、检查项和检查项触发条件。

自定义特征规则包括如下类型：

- 关键字类型：配置关键字类型规则时，需要配置检查项和检查项触发条件。只有匹配检查项触发条件后才会继续匹配检查项。仅当所有检查项都匹配成功，才表示该规则成功匹配。
- 数值类型：配置数值类型规则时，可以配置检查项，只有所有检查项都匹配成功，才表示规则成功匹配。

新建自定义特征

新建自定义特征的配置步骤如下：

1. 选择“策略 > Web 应用防护 > 特征”。

2. 在“Web 应用防护特征”页面，单击<新建自定义特征>按钮，进入“新建自定义特征”页面。

   在“基本配置”区域可配置自定义特征的属性，具体配置内容如下：

表-7 配置自定义特征属性

参数	说明
名称	自定义特征的名称
描述	通过合理编写描述信息，便于管理员快速理解和识别自定义特征的作用，有利于后
严重级别	可根据具有该特征报文对网络攻击造成危害的严重程度配置不同的严重级别。严重 种：严重、高、中、低
方向	可根据具有该特征报文的传输方向进行配置，包括服务端和客户端
动作	对具有该特征的报文执行的动作。动作类型包括：黑名单、丢弃、允许和重置
日志	开启日志功能后，设备将对与Web应用防护特征匹配成功的报文生成日志信息
抓包	开启抓包功能后，设备会将捕获到的报文保存在本地并输出到指定的路径，有关捕 置，请参见“安全动作”

3. 在“规则”区域可配置自定义特征规则。一个自定义特征下可配置多条规则，用户需要先配置规则逻辑，包括逻辑或和逻辑与。单击<新建>按钮，进入新建规则页面，具体配置内容如下：

表-8 新建自定义特征规则

参数	说明
ID	自定义特征规则的ID
匹配类型	表示自定义特征的类型，包括关键字类型和数值类型
请求方法	HTTP报文的请求方法，如：GET、POST等
源IPv4地址	自定义特征匹配的源IPv4地址
源端口	自定义特征匹配的源端口
目的IPv4地址	自定义特征匹配的目的IPv4地址
目的端口	自定义特征匹配的目的端口

4. 在“检查项触发条件”区域配置检查项的触发条件，仅当自定义特征规则为关键字类型时需要配置。具体配置内容如下：

表-9 新建检查项触发条件

参数	说明
协议字段	检查项触发条件检测的协议字段
匹配模式	检查项触发条件检测内容的匹配模式，包括文本方式和十六进制方式
匹配内容	检查项触发条件检测的内容
检测深度	检查项触发条件的检测深度，从起始检测位置开始，检测数据的长度
偏移量	检查项触发条件的偏移量，从协议字段开始，偏移指定长度,作为检查项触发条件的

5. 单击<确定>按钮，完成检查项触发条件的配置。

6. 在“检查项”区域配置自定义特征规则的检查项，具体配置内容如下：

表-10 新建检查项

参数	说明
ID	检查项的ID
协议字段	检查项检测的协议字段
操作符	表示检查项和检测内容的匹配方式，不同类型的自定义特征规则支持的操作符不同， • 关键字类型规则的操作符包括：包含和不包含 • 数值类型规则的操作符包括：大于、小于、等于、不等于、大于等于和小于等于

匹配模式	检查项检测内容的匹配模式，包括文本、正则表达式和十六进制
匹配内容	检查项检测的内容
偏移量	检查项的偏移量，从协议字段开始，偏移指定长度，作为检查项的检测起始位置
检测深度	检查项的检测深度，从检查项检测的起始位置开始，检测数据的长度
相对偏移量	表示当前检查项与上一个检查项之间的相对偏移量，从上一个检查项的结束位置开始
相对检测深度	表示当前检查项的检测深度

7. 单击<确定>按钮，完成检查项的配置。

8. 单击<确定>按钮，完成自定义特征规则的配置。

9. 单击<确定>按钮，完成自定义特征的配置。

10. 单击<提交>按钮，使新建的自定义特征生效。

11. 新建 Web 应用防护配置文件，配置基础参数和过滤条件。并将配置文件引用至策略中。具体配置步骤请参见“定制化 Web 应用防护配置任务”章节。

删除自定义特征

删除自定义特征的配置步骤如下：

1. 选择“对象 > 安全配置文件 > Web 应用防护 > 特征”。

2. 在“Web 应用防护特征”页面，选择需要删除的自定义特征，单击<删除>按钮，选择删除选中的自定义特征。

配置 Web 应用防护白名单

当发现 Web 应用防护日志中存在误报的情况时，可通过开启白名单功能，将误报日志中提取到的特征 ID、URL 或 IP 地址加入白名单。设备对匹配白名单的报文放行，可以减少误报。

配置白名单功能后，设备会对白名单的命中情况进行统计，用户可在白名单界面中查看统计信息。

1. 选择“策略 > Web 应用防护 > 白名单”。

2. 在“白名单”页面单击<新建>按钮，进入“新建白名单”页面。具体配置内容如下：

表-11 配置白名单

参数	说明
编号	白名单的编号
描述	通过合理编写描述信息，便于管理员快速理解和识别白名单的作用，有利于后期维
特征ID	从误报的日志中提取到的Web应用防护特征ID
URL	从误报的日志中提取到的URL URL由报文头域和报文首行组成，例如：111.15.93.166/wnm/get.j 对于新增、修改和删除URL，设备会在完成修改的10秒后自动激活，使配置生效

IP地址类型	IP地址类型，取值包括IPv4和IPv6
IP地址	从日志中提取到的源IP地址或者真实源IP地址 当用户将IP地址配置为真实源IP地址时，必须先到“对象 > 应用安全 > 高级配置”页 源IP地址检测功能，使设备可以识别出报文中的真实源IP地址，与白名单进行正确的 实源IP地址功能的详细介绍，请参见“高级配置”
状态	表示白名单是否生效。当勾选启用时，此白名单将处于生效状态；当未勾选启用时， 于禁用状态

3. 单击<确定>按钮，完成白名单的创建。

4. 单击<开启白名单功能>按钮，启用白名单功能。

入侵防御

本帮助主要介绍以下内容：

- 特性简介
  - 入侵防御的优势
  - 入侵防御特征
  - 语义分析检测
  - 入侵防御动作
  - 入侵防御实现流程
- vSystem 相关说明
- License 支持情况
- 使用限制和注意事项
- 配置指南
  - 配置思路
  - 配置准备
  - 缺省入侵防御配置任务
  - 定制化入侵防御配置任务
  - 管理入侵防御特征
  - 配置入侵防御白名单

- 配置入侵防御捕获报文

特性简介

IPS（Intrusion Prevention System，入侵防御系统）是一种可以对应用层攻击进行检测并防御的安全防御技术。入侵防御通过分析流经设备的网络流量来实时检测入侵行为，并通过一定的响应动作来阻断入侵行为，实现保护企业信息系统和网络免遭攻击的目的。

入侵防御的优势

入侵防御具有以下优势：

- 深度防护：可以检测报文应用层的内容，以及对网络数据流进行协议分析和重组，并根据检测结果来对报文做出相应的处理。
- 实时防护：实时检测流经设备的网络流量，并对入侵活动和攻击性网络流量进行实时拦截。
- 全方位防护：可以对多种攻击类型提供防护措施，例如蠕虫、病毒、木马、僵尸网络、间谍软件、广告软件、CGI（Common Gateway Interface）攻击、跨站脚本攻击、注入攻击、目录遍历、信息泄露、远程文件包含攻击、溢出攻击、代码执行、拒绝服务、扫描工具、后门等。
- 内外兼防：对经过设备的流量都可以进行检测，不仅可以防止来自企业外部的攻击，还可以防止发自企业内部的攻击。

入侵防御特征

入侵防御特征用来扫描网络中的攻击行为以及对攻击行为采取防御措施，设备通过将数据流与入侵防御特征进行比较来检测和防御攻击。

设备支持如下类型的入侵防御特征：

- 预定义特征：由系统中的入侵防御特征库自动生成，不可进行修改和删除。
- 自定义特征：由用户手工配置。可以创建、修改和删除。
- Snort 特征：由 Snort 文件导入。可以导入和删除。

自定义设置

缺省情况下，设备基于入侵防御配置文件中指定的动作对符合此配置文件中入侵防御特征的报文进行处理。当需要对符合某个入侵防御特征的报文采取不同的动作时，可通过自定义设置修改特征动作。自定义设置的特征动作优先级高于配置文件中配置的动作优先级。

当入侵防御配置文件中某个特征处于非生效状态时，可以通过自定义设置将此特征设置为生效状态。

当需要修改入侵防御配置文件中某个特征的严重级别时，可以通过自定义设置修改此特征的严重级别。

语义分析检测

语义分析检测功能基于对报文中的 SQL 语句进行语法分析来检测 SQL 注入攻击行为。

开启本功能后，设备将同时使用特征匹配和语义分析检测对 SQL 注入攻击进行识别，可以提升该类攻击的识别率。

用户可通过查看“监控 > 安全日志 > 威胁日志”中的“检测引擎”字段，判断设备通过何种方式检测到攻击：

- 当字段取值为特征匹配时，表示设备通过特征匹配方式检测出攻击。
- 当字段取值为语义分析时，表示设备通过语义分析检测方式检测出攻击。

入侵防御动作

入侵防御动作是指设备对匹配上入侵防御特征的报文做出的处理。入侵防御处理动作包括如下几种类型：

- 黑名单：阻断符合特征的报文。如果设备上同时开启了 IP 黑名单过滤功能，则阻断时间内（在安全动作中的阻断功能中配置）来自此 IP 地址的所有报文将被直接丢弃；如果设备上未开启黑名单过滤功能，报文的源 IP 地址仍会被添加到 IP 黑名单表项中，但后续来自该源 IP 地址的报文不会被直接丢弃。有关黑名单功能的详细介绍请参见“攻击防范”。
- 丢弃：丢弃符合特征的报文。
- 允许：允许符合特征的报文通过。

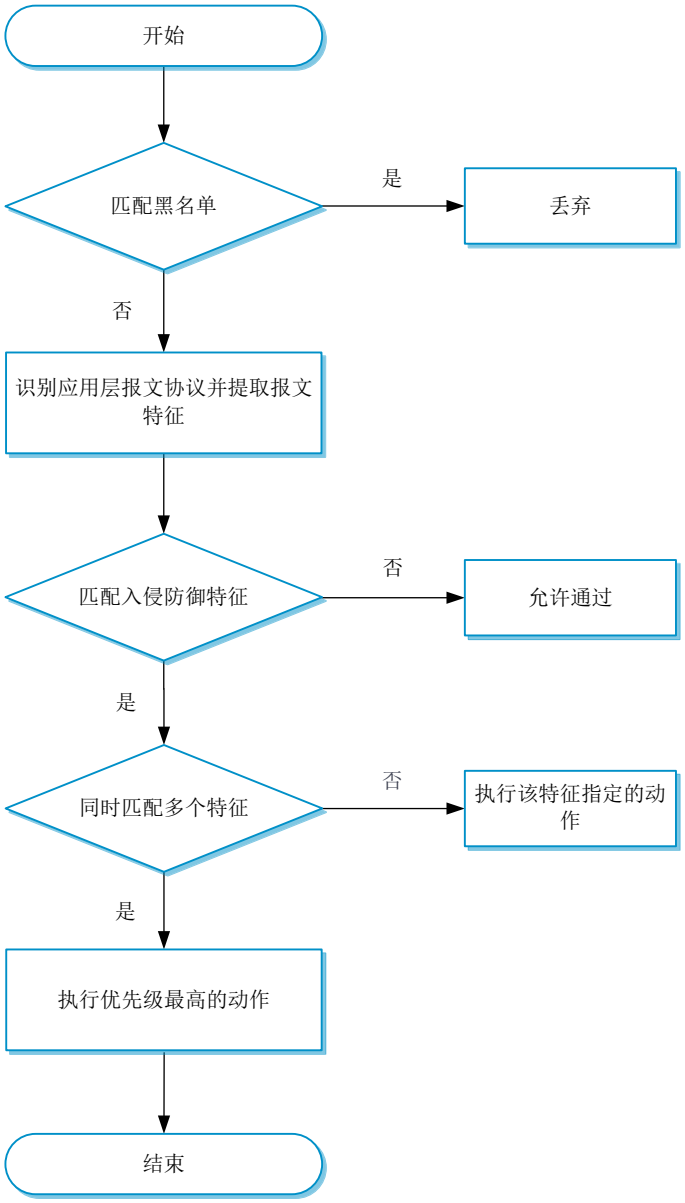
- 重置：通过发送 TCP 的 reset 报文或 UDP 的 ICMP 端口不可达报文断开 TCP 或 UDP 连接。
- 重定向：把符合特征的报文重定向到指定的 Web 页面上。
- 使用特征的预定义动作：对符合特征的报文执行特征库中该特征的预定义动作。
- 抓包：捕获符合特征的报文。
- 日志：对符合特征的报文生成日志信息。

入侵防御实现流程

在设备配置了入侵防御功能的情况下，当用户的数据流量经过设备时，设备将进行入侵防御处理。

处理流程如图-1 所示：

图-1 入侵防御数据处理流程图



入侵防御处理的整体流程如下：

2. 如果报文与 IP 黑名单匹配成功，则直接丢弃该报文。

3. 如果报文匹配了某条安全策略，且此策略的动作是允许并引用了入侵防御配置文件，则设备将对报文进行深度内容检测：首先，识别报文的协议，然后根据协议分析方案进行更精细的

分析，并深入提取报文特征。其中，如果配置文件中开启了语义分析检测功能，则同时提取报文中的 SQL 语句信息。

4. 设备将提取的报文特征与入侵防御特征进行匹配，同时，如果配置文件中开启了语义分析检测功能，设备也会对报文中的 SQL 语句进行语法分析，并进行如下处理：
   - 如果设备通过特征匹配方式检测到了攻击，则对报文进行如下处理：
     - 如果报文同时与多个入侵防御特征匹配成功，则根据这些动作中优先级最高的动作进行处理。动作优先级从高到低的顺序为：重置 > 重定向 > 丢弃 > 允许。但是，对于黑名单、抓包和日志三个动作只要匹配成功的特征中存在就会执行。
     - 如果报文只与一个入侵防御特征匹配成功，则根据此特征中指定的动作进行处理。
   - 如果设备通过语义分析检测功能识别到了攻击，则允许报文通过并记录入侵防御日志。
   - 如果设备通过上述两种方式均检测到了攻击，则对报文执行特征匹配成功时所需执行的动作，同时记录入侵防御日志。
   - 如果设备通过上述两种方式均未检测到攻击，则直接允许报文通过。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

License支持情况

入侵防御功能需要购买并正确安装 License 后才能使用。License 过期后，入侵防御功能可以采用设备中已有的入侵防御特征库正常工作，但无法升级到官方网站在过期时间后发布的新版本的特征库。关于 License 的详细介绍请参见“License 配置”。

使用限制和注意事项

- 执行"提交"操作会暂时中断 DPI 业务的处理，可能导致其他基于 DPI 功能的业务同时出现中断。例如，安全策略无法对应用进行访问控制等。
- 执行“提交”操作后，界面上会提示设置成功，但是配置文件此时可能尚未完成激活，如果此时报文经过设备，可能会出现暂时无法识别的情况。
- 入侵防御功能需要购买并正确安装 License 才能使用。License 过期后，入侵防御功能可以用，但无法升级特征库，只能使用设备中已存在的特征库。关于 License 的详细介绍请参见“License 配置”。
- 配置入侵防御白名单时，威胁 ID、URL 和 IP 地址请至少选择其中一项进行配置。
- 在报文匹配到多条白名单时，当白名单威胁 ID 相同时，仅编号最小的白名单命中统计次数增加。而当白名单威胁 ID 不同时，则白名单命中统计次数分别增加。
- 编辑指定的入侵防御白名单后（无论是否修改配置内容），设备将清空已有的命中统计次数，并重新进行统计。

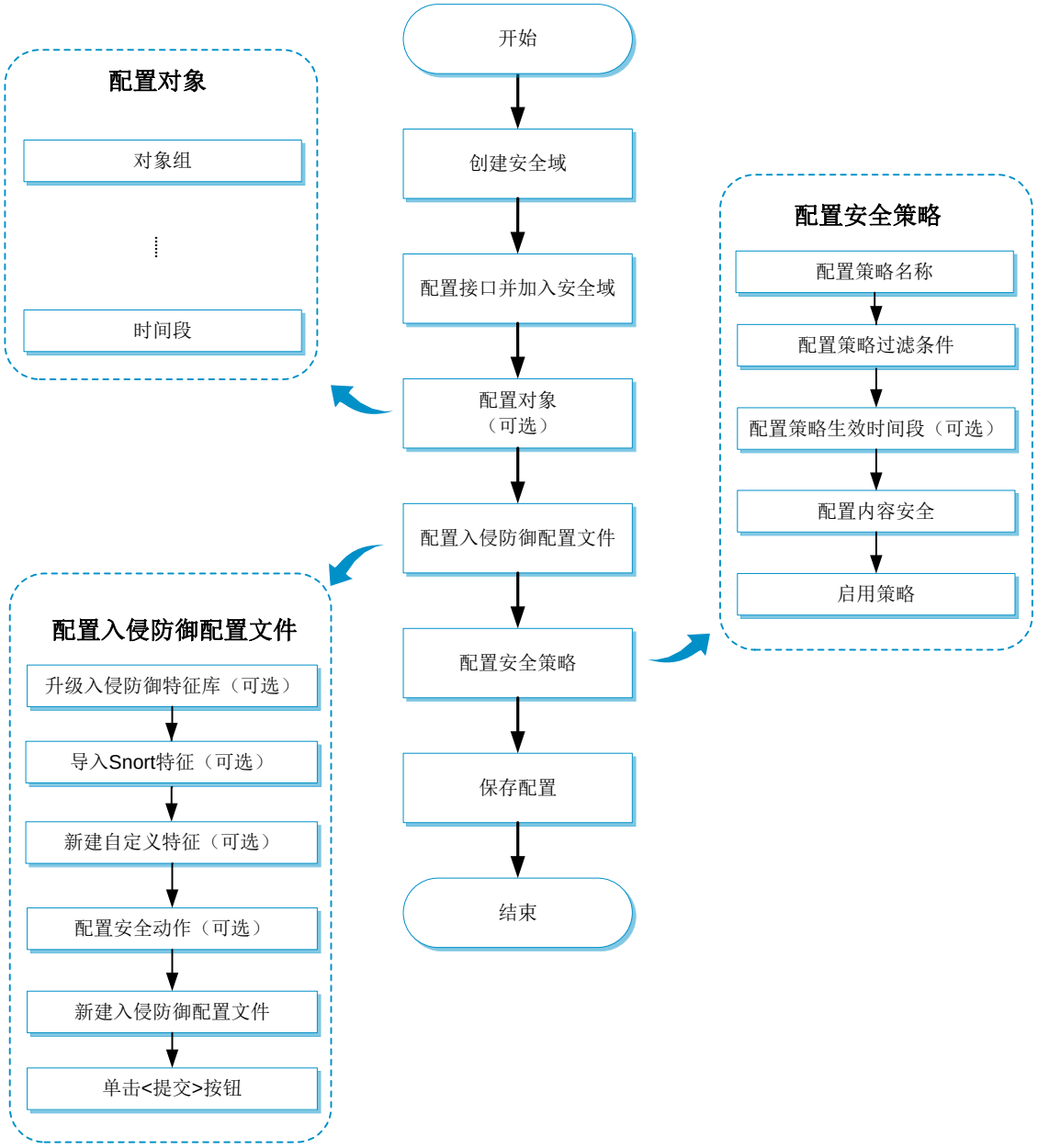
- 通过语义分析检测功能识别出的攻击，其特征 ID 固定为 4294967290。如果希望将此特征 ID 添加到白名单表项中，则需要先在白名单表项中配置源 IP 地址或 URL。

配置指南

配置思路

入侵防御功能的配置思路如下图所示：

图-2 入侵防御功能配置指导图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

缺省入侵防御配置任务

设备上存在一个名称为 default 的入侵防御配置文件，缺省入侵防御配置文件使用当前系统中所有缺省处于启用状态的入侵防御特征，新增自定义入侵防御特征会自动添加到缺省入侵防御配置文件下。缺省入侵防御配置文件中的入侵防御特征的动作属性和生效状态属性不能被修改。

1. 选择“策略 > 入侵防御 > 配置文件”。default 的入侵防御配置文件不可编辑。
2. 在安全策略的内容安全配置中引用此入侵防御配置文件，有关安全策略的详细配置介绍请参见“安全策略”。

定制化入侵防御配置任务

使用缺省 default 的入侵防御配置文件不满足需求时，可创建自定义的配置文件。管理员可以基于业务环境和安全需求灵活调整自定义入侵防御配置文件中特征的相关属性，包括生效特征列表/未生效特征列表中特征的状态、动作、严重级别或将特征移入、移出生效特征列表/未生效特征列表等。

1. 选择“策略 > 入侵防御 > 配置文件”。
2. 在“入侵防御配置文件”页面单击<新建>按钮，进入“新建入侵防御配置文件”页面。配置入侵防御配置文件的基本参数，具体参数如下所示：

表-1 入侵防御配置文件基本参数

参数	说明
名称	配置入侵防御配置文件的名称中不建议包含“< > \ / | * ? " : , ;”这些特殊字符，否则 御配置文件其名称中将用“_”替换这些特殊字符
语义分析检测	开启本功能后，设备将同时使用特征匹配和语义分析检测对SQL注入攻击进行识别， 攻击的识别率
设置动作	入侵防御配置文件的动作类型包括：使用特征的预定义动作、黑名单、丢弃、允许、 符合此配置文件的报文将被按照此配置文件中指定的动作进行处理

3. 配置入侵防御特征筛选条件，配置完成后单击<查看筛选结果>按钮，在生效特征和未生效特征列表中可以查看特征筛选结果。具体参数如下：

表-2 入侵防御特征筛选条件

参数	说明
保护对象	通过选择保护对象可快速选择所需的入侵防御特征
攻击分类	通过选择攻击分类可快速选择所需的入侵防御特征
方向	入侵防御特征库中的特征分为服务端和客户端，可通过选择服务端和客户端来筛选 入侵防御特征
预定义动作	入侵防御特征的预定义动作分为如下四种：丢弃、允许、重置、黑名单，可通过选 动作来筛选配置文件所需的入侵防御特征
预定义严重级别	入侵防御特征的预定义严重级别分为如下四种：严重、高、中、低，可通过选择不 筛选配置文件所需的入侵防御特征
预定义状态	入侵防御特征的预定义状态分为使能和未使能两种状态，可通过选择不同的预定义 文件所需的入侵防御特征

若不配置任何一项筛选条件（保持缺省情况），则此配置文件中将会包含所有入侵防御特征。

4. 如需修改生效特征列表/未生效特征列表中特征的状态、动作、严重级别或将特征移入、移出生效特征列表/未生效特征列表，可单击<自定义设置>按钮，进入自定义设置界面进行修改，单击<确定>按钮，完成修改。

5. 单击<高级配置>按钮，进入高级配置界面，具体配置参数如下：

表-3 高级设置参数

参数	说明
开启策略匹配统计	开启此功能，可以统计报文命中入侵防御配置文件的次数
日志参数	通过设置日志参数，可为特征的日志动作提供执行参数。可选择配置日志参数的方式 • 使用自定义参数：直接配置日志参数 • 使用全局参数：可在“系统 > 日志设置 > 日志管理”区域下查看或修改全局参数
日志输出类型	选择使用自定义参数后，可直接配置日志的输出方向，包括： • 输出到系统日志 • 输出到邮件 可同时选择两种输出类型
邮件服务器	当选择输出邮件后，需要配置邮件服务器，可通过新建邮件服务器或者引用已有邮件 置 已有邮件服务器可到“系统 > 日志设置 > 邮件服务器“页面查看或修改
特征库基线版本号	配置基线版本号可帮助用户快速筛选出基线版本与当前版本之间有差异的特征，IPS 基线版本的特征与报文进行匹配，而不必回滚至基线版本的特征库 配置本功能后，所有高于基线版本的特征将处于非生效状态，即不能用于匹配报文。 中某个非生效状态的特征调整为生效状态，需要进行如下操作： 1. 如果待调整特征的版本号高于基线版本号，需要先将基线版本号调整为特征的 直接执行下一步操作 2. 选中待调整的特征，单击<自定义设置>按钮，进入自定义设置页面，配置状态
邮件输出条件 特征最低严重级别	设备支持根据特征的严重级别对输出的邮件进行限制 当特征的严重级别高于或等于配置的最低严重级别时才可以输出邮件

6. 单击<确定>按钮，新建入侵防御配置文件成功，且会在“入侵防御配置文件”页面中显示。
7. 在安全策略的内容安全配置中引用此入侵防御配置文件，具体配置步骤请参见“缺省入侵防御配置任务”章节。
8. 单击<提交>按钮，激活入侵防御配置文件的配置内容。配置此功能会暂时中断 DPI 业务的处理，为避免重复配置此功能对 DPI 业务造成影响，请完成部署 DPI 各业务模块的配置文件后统一提交激活。

管理入侵防御特征

新建 Snort 特征

当需要的特征在设备当前特征库中不存在时，可通过编辑 Snort 格式的入侵防御特征文件，并将其导入设备中来生成所需的入侵防御特征。导入 Snort 特征后将删除原有的全部 Snort 特征。

需要注意的是，Snort 文件需要遵循 Snort 公司的语法。

导入 Snort 特征的配置步骤如下：

1. 选择“策略 > 入侵防御 > 特征”。
2. 在“入侵防御特征”页面单击<导入 Snort 特征>按钮，进入“导入 Snort 特征”页面。
3. 选择指定的 Snort 文件，单击<导入特征>按钮，导入并解析 Snort 特征。
4. 新建入侵防御配置文件，配置基础参数和过滤条件。并将配置文件引用至策略中。具体配置步骤请参见“定制化入侵防御配置任务”章节。

新建自定义特征

当需要的特征在设备当前特征库中不存在，或者 Snort 特征无法满足具体需求时，可以通过手工配置的方式新建自定义特征。这种方法允许用户在不完全依赖现有特征库的情况下，灵活地添加新特征，以满足特定的安全检测需求，从而增强设备的防护能力。

自定义特征包括属性和规则。

一个自定义特征下可配置多条规则，规则间包含如下规则逻辑：

- 逻辑与：表示报文需要匹配该自定义特征的所有规则才认为与该特征匹配成功。
- 逻辑或：表示报文匹配到该自定义特征的任何一条规则即认为与该特征匹配成功。

自定义特征规则下支持配置规则的匹配条件（包括源/目的 IPv4 地址、源/目的端口、请求方法等）、检查项和检查项触发条件。

自定义特征规则包括如下类型：

- 关键字类型：配置关键字类型规则时，需要配置检查项和检查项触发条件。只有匹配检查项触发条件后才会继续匹配检查项。仅当所有检查项都匹配成功，才表示该规则成功匹配。
- 数值类型：配置数值类型规则时，可以配置检查项，只有所有检查项都匹配成功，才表示规则成功匹配。

新建自定义特征的配置步骤如下：

1. 选择“策略 > 入侵防御 > 特征”。
2. 在“入侵防御特征”页面，单击<新建自定义特征>按钮，进入“新建自定义特征”页面。在“基本配置”区域可配置自定义特征的属性，具体配置内容如下：

表-4 配置自定义特征属性

参数	说明
名称	自定义特征的名称
描述	通过合理编写描述信息，便于管理员快速理解和识别自定义特征的作用，有利于后
严重级别	可根据具有该特征报文对网络攻击造成危害的严重程度配置不同的严重级别。严重 种：严重、高、中、低
方向	可根据具有该特征报文的传输方向进行配置，包括服务端和客户端
动作	对具有该特征的报文执行的动作。动作类型包括：黑名单、丢弃、允许和重置
日志	开启日志功能后，设备将对与入侵防御特征匹配成功的报文生成日志信息
抓包	开启抓包功能后，设备会将捕获到的报文保存在本地并输出到指定的路径，有关捕 置，请参见“安全动作”

3. 在“规则”区域可配置自定义特征规则。一个自定义特征下可配置多条规则，用户需要先配置规则逻辑，包括逻辑或和逻辑与。

4. 单击<新建>按钮，进入新建规则页面，具体配置内容如下：

表-5 新建自定义特征规则

参数	说明
ID	自定义特征规则的ID

应用层协议	自定义特征匹配的应用层协议
传输层协议	自定义特征匹配的传输层协议
匹配类型	表示自定义特征的类型，包括关键字类型和数值类型
请求方法	HTTP报文的请求方法，如：GET、POST等
源IPv4地址	自定义特征匹配的源IPv4地址
源端口	自定义特征匹配的源端口
目的IPv4地址	自定义特征匹配的目的IPv4地址
目的端口	自定义特征匹配的目的端口

5. 在“检查项触发条件”区域配置检查项的触发条件，仅当自定义特征规则为关键字类型时需要配置。具体配置内容如下：

表-6 新建检查项触发条件

参数	说明
协议字段	检查项触发条件检测的协议字段
匹配模式	检查项触发条件检测内容的匹配模式，包括文本方式和十六进制方式
匹配内容	检查项触发条件检测的内容
检测深度	检查项触发条件的检测深度，从起始检测位置开始，检测数据的长度

偏移量	检查项触发条件的偏移量，从协议字段开始，偏移指定长度,作为检查项触发条件的

6. 单击<确定>按钮，完成检查项触发条件的配置。

7. 在“检查项”区域配置自定义特征规则的检查项，具体配置内容如下：

表-7 新建检查项

参数	说明
ID	检查项的ID
协议字段	检查项检测的协议字段
操作符	表示检查项和检测内容的匹配方式，不同类型的自定义特征规则支持的操作符不同， • 关键字类型规则的操作符包括：包含和不包含 • 数值类型规则的操作符包括：大于、小于、等于、不等于、大于等于和小于等于
匹配模式	检查项检测内容的匹配模式，包括文本、正则表达式和十六进制
匹配内容	检查项检测的内容
偏移量	检查项的偏移量，从协议字段开始，偏移指定长度，作为检查项的检测起始位置
检测深度	检查项的检测深度，从检查项检测的起始位置开始，检测数据的长度
相对偏移量	表示当前检查项与上一个检查项之间的相对偏移量，从上一个检查项的结束位置开始
相对检测深度	表示当前检查项的检测深度

8. 单击<确定>按钮，完成检查项的配置。

9. 单击<确定>按钮，完成自定义特征规则的配置。

10. 单击<确定>按钮，完成自定义特征的配置。

11. 单击<提交>按钮，使新建的自定义特征生效。

12. 新建入侵防御配置文件，配置基础参数和过滤条件。并将配置文件引用至策略中。具体配置步骤请参见“定制化入侵防御配置任务”章节。

删除 Snort 和自定义特征

删除 Snort 特征的配置步骤如下：

1. 选择“策略 > 入侵防御 > 特征”。

2. 在“入侵防御特征”页面，单击<删除特征>按钮，选择删除全部 Snort 特征。可删除所有 Snort 特征。

删除自定义特征的配置步骤如下：

选择“策略 > 入侵防御 > 特征”。在“入侵防御特征”页面，选择需要删除的自定义特征，单击<删除特征>按钮，选择删除选中的自定义特征。

导出特征库中所有特征

选择“策略 > 入侵防御 > 特征”，在“入侵防御特征”页面可导出当前设备上入侵防御特征库中的所有特征。单击<导出所有特征>按钮，将以 csv 表格的形式导出特征库中所有特征。

导出入侵防御配置文件所筛选的特征

导出入侵防御配置文件所筛选的特征，可在“入侵防御配置文件”页面导出特征一列中单击<导出>按钮，将以 csv 表格形式导出特征库中的所有特征，并在表格生效特征一列中用“是”标识属于该入侵防御配置文件的特征。

配置入侵防御白名单

当发现入侵防御日志中存在误报的情况时，可通过开启白名单功能，将误报日志中提取到的威胁 ID（入侵防御特征 ID）、URL、源/目的 IP 地址或目的端口号加入白名单。设备对匹配白名单的报文放行，可以减少误报。

配置白名单功能后，设备会对白名单的命中情况进行统计，用户可在白名单界面中查看统计信息。

配置步骤

1. 选择“策略 > 入侵防御 > 白名单”。
2. 在“白名单”页面单击<新建>按钮，进入“新建白名单”页面，具体配置内容如下：

表-8 配置白名单

参数	说明
编号	白名单的编号

描述		通过合理编写描述信息，便于管理员快速理解和识别白名单的作用，有利
威胁ID		从误报的日志中提取到的入侵防御特征ID
URL	精确匹配URL	精确匹配是指报文中检测到的URL必须和配置的URL完全一致才能匹配成 由报文头域和报文首行组成。由字母、数字、“_”、“-”、“:”、“[”、“]”和“.”
	子串匹配URL	子串匹配是指报文中检测到的URL只要包含配置的URL即可匹配成功。可 头域和报文首行组成。由字母、数字、“_”、“-”、“:”、“[”、“]”和“.”
源IP	匹配模式	源IP的匹配方式，取值包括： • 真实源 IP 或报文源 IP：IPS 白名单表项中配置的源 IP 地址优先匹配 IP 地址的情况下使用网络层 IP 地址匹配源 IP 地址。 • 真实源 IP：IPS 白名单表项中配置的源 IP 地址匹配真实源 IP 地址 • 报文源 IP：IPS 白名单表项中配置的源 IP 地址使用网络层 IP 地址匹 如果需要使用真实源IP地址与白名单中的源IP地址进行匹配，则需要设备开 应用安全 > 高级配置”页面下进行配置）
	IPv4	配置IPv4地址、范围或子网作为IPS白名单的匹配条件
	IPv6	配置IPv6地址、范围或子网作为IPS白名单的匹配条件
目的IP	IPv4	配置IPv4地址、范围或子网作为IPS白名单的匹配条件
	IPv6	配置IPv6地址、范围或子网作为IPS白名单的匹配条件
状态		白名单规则的状态为启用或禁用

3. 单击<确定>按钮，完成白名单的创建。

4. 单击<开启白名单功能>按钮，启用白名单功能。

配置入侵防御捕获报文参数

入侵防御业务捕获报文时，管理员可以根据实际情况设置捕获报文的缓存参数。

- 当管理员仅关心命中报文和其上下文（即命中报文前后几个报文）时，可以根据实际需求限制缓存报文的数量。
- 当管理员需要对整条流的信息进行分析时，可以设置对整条流的报文都进行缓存并指定捕获报文的起始位置。此功能的支持情况与设备型号有关，请以设备实际情况为准。

当报文缓存结束后，设备会将所有缓存报文写入入侵防御捕获文件，并根据实际情况将捕获文件上送到如下路径。

表-9 捕获文件上送路径

参数	说明
指定的URL	当管理员已设置上传URL，且与设备对接的云平台（即安全威胁发现与运营管理平台）t 获文件上送功能时，设备会将捕获文件上送到指定的URL
硬盘/U盘	当设备检测到硬盘/U盘在位时，会将捕获文件保存到硬盘/U盘中 管理员可直接从硬盘或U盘中获取捕获文件，或通过单击监控面板下威胁日志页面中指定 的<下载>按钮，获取捕获文件
云平台（即安全威胁发现与运营管理平台）	当设备检测到与其对接的云平台已开启捕获文件上送功能时，会通过HTTPS协议将IPS捕 送到云平台

有关上述捕获文件上送路径的相关说明，请参见“安全动作”。

缓存报文数的具体配置步骤如下：

1. 选择“策略 > 入侵防御 > 配置文件”。
2. 在“入侵防御配置文件”页面单击<高级配置>按钮，进入“高级配置”页面。根据实际需求配置缓存报文数。

表-10 捕获报文缓存参数

参数	说明
缓存报文数	表示可缓存的报文数量。当取值为1时，设备仅缓存命中报文
从会话创建开始对整条流量进行捕获	表示从会话创建开始对整条流的报文都进行缓存 本参数仅对入侵防御业务生效 本参数的支持情况与设备型号有关，请以设备实际情况为准
从命中报文开始对整条流量进行捕获	表示从命中报文开始对整条流的报文都进行缓存 本参数仅对入侵防御业务生效 本参数的支持情况与设备型号有关，请以设备实际情况为准

3. 单击<确定>按钮，完成配置。

防病毒

本帮助主要介绍以下内容：

- 特性简介
  - 应用场景
  - 基本概念
  - 防病毒检测方式
  - 云端查询
  - 增强检测
  - 防病毒数据处理流程
- vSystem 相关说明
- License 支持情况
- 使用限制和注意事项
- 配置指南
  - 配置思路
  - 配置准备
  - 缺省防病毒配置任务

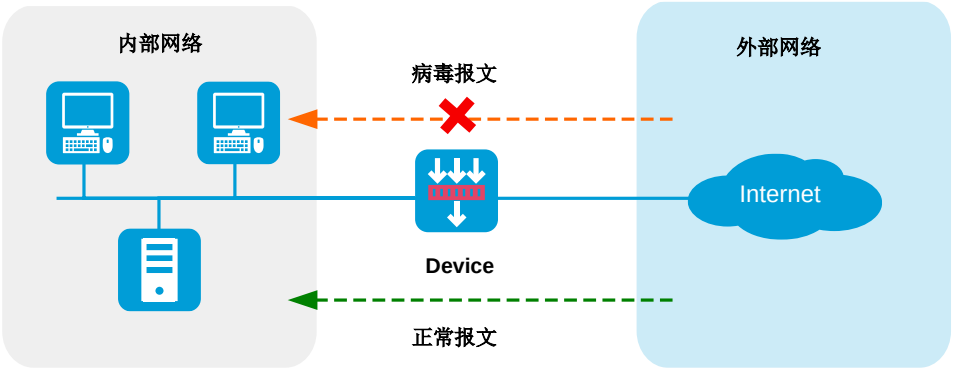
- 定制化防病毒配置任务
- 配置病毒检测扩展功能
- 查看病毒家族信息

特性简介

防病毒功能是一种通过对报文应用层信息进行检测来识别和处理病毒报文的安全机制。防病毒功能凭借庞大且不断更新的病毒特征库可有效保护网络安全，防止病毒在网络中的传播。将具有防病毒功能的设备部署在企业网入口，可以将病毒隔离在企业网之外，为企业内网的数据安全提供坚固的防御。

应用场景

图-1 防病毒典型应用场景



如图-1 所示，在如下应用场景中，隔离内网和外网的网关设备上需要部署防病毒配置文件来保证内部网络安全：

- 内网用户需要访问外网资源，且经常需要从外网下载各种应用数据。
- 内网的服务器需要经常接收外网用户上传的数据。

当在设备上部署防病毒配置文件后，正常的用户数据可以进入内部网络，携带病毒的报文会被检测出来，并被采取阻断、重定向或生成告警信息等动作。

基本概念

病毒特征

病毒特征是设备上定义的用于识别应用层信息中是否携带病毒的字符串，由系统中的病毒特征库预定义。

MD5 规则

MD5 规则是设备上定义的用于识别传输文件是否携带病毒的检测规则，由系统中的病毒特征库预定义。

病毒例外

缺省情况下，设备对所有匹配病毒特征的报文均进行防病毒动作处理。但是，当管理员认为已检测到的某个病毒为误报时，可以将该病毒特征设置为病毒例外，之后携带此病毒特征的报文经过时，设备将对此报文执行允许动作。

应用例外

缺省情况下，设备基于应用层协议的防病毒动作对符合病毒特征的报文进行处理。当需要对某应用层协议上承载的某一具体应用采取不同的动作时，可以将此应用设置为应用例外。例如，对 HTTP 协议采取的动作是允许，但是需要对 HTTP 协议上承载的游戏类应用采取阻断动作，这时就可以把所有游戏类的应用均设置为应用例外。

MD5 值例外

如果发现某类检测出病毒的报文被误报时，用户可以通过查看威胁日志获取病毒的 MD5 值，并将该 MD5 值设置为例外。当后续再有检测出符合该 MD5 值的报文通过时，设备将对其执行允许动作。

防病毒动作

防病毒动作是指对符合病毒特征的报文做出的处理，包括如下几种类型：

- 告警：允许病毒报文通过，同时生成病毒日志。
- 阻断：禁止病毒报文通过，同时生成病毒日志。

- 重定向：将携带病毒的 HTTP 连接重定向到指定的 URL，同时生成病毒日志。
- 允许：允许病毒报文通过。

防病毒检测方式

设备支持使用以下方式进行防病毒检测：

- 病毒特征匹配：设备将报文与特征库中的病毒特征进行匹配，如果匹配成功，则表示该报文携带病毒。
- MD5 值匹配：设备首先对待检测文件进行 MD5 哈希运算，再将计算出的 MD5 值与特征库中的 MD5 规则进行匹配，如果匹配成功，则表示该文件携带病毒。

云端查询

在防病毒配置文件中开启防病毒 MD5 值云端查询功能后，当设备无法识别出病毒时，会将未识别出的文件的 MD5 值发往云端服务器进行查询。云端服务器响应该请求，并向设备发送查询结果，该结果中包含了 MD5 值并确认其是否为病毒，设备根据该结果执行相应的处理动作。如果云端未查询到该 MD5 值，或查询结果为非病毒，则设备将放行此报文。

DTLS 协议：表示（Datagram Transport Layer Security，数据报传输层安全）是一种用于保护数据报协议的安全协议。适用于低延迟的场景，如实时通信（VoIP、视频会议）、物联网设备（无线传感器网络）和流媒体服务。

HTTPS 协议：表示（HyperText Transfer Protocol Secure）是一种用于通过安全通信通道传输超文本数据的协议。适用于所有需要保护数据传输安全的场景，如在线银行、社交媒体平台、邮件服务和任何需要用户身份验证和数据加密的 Web 应用。

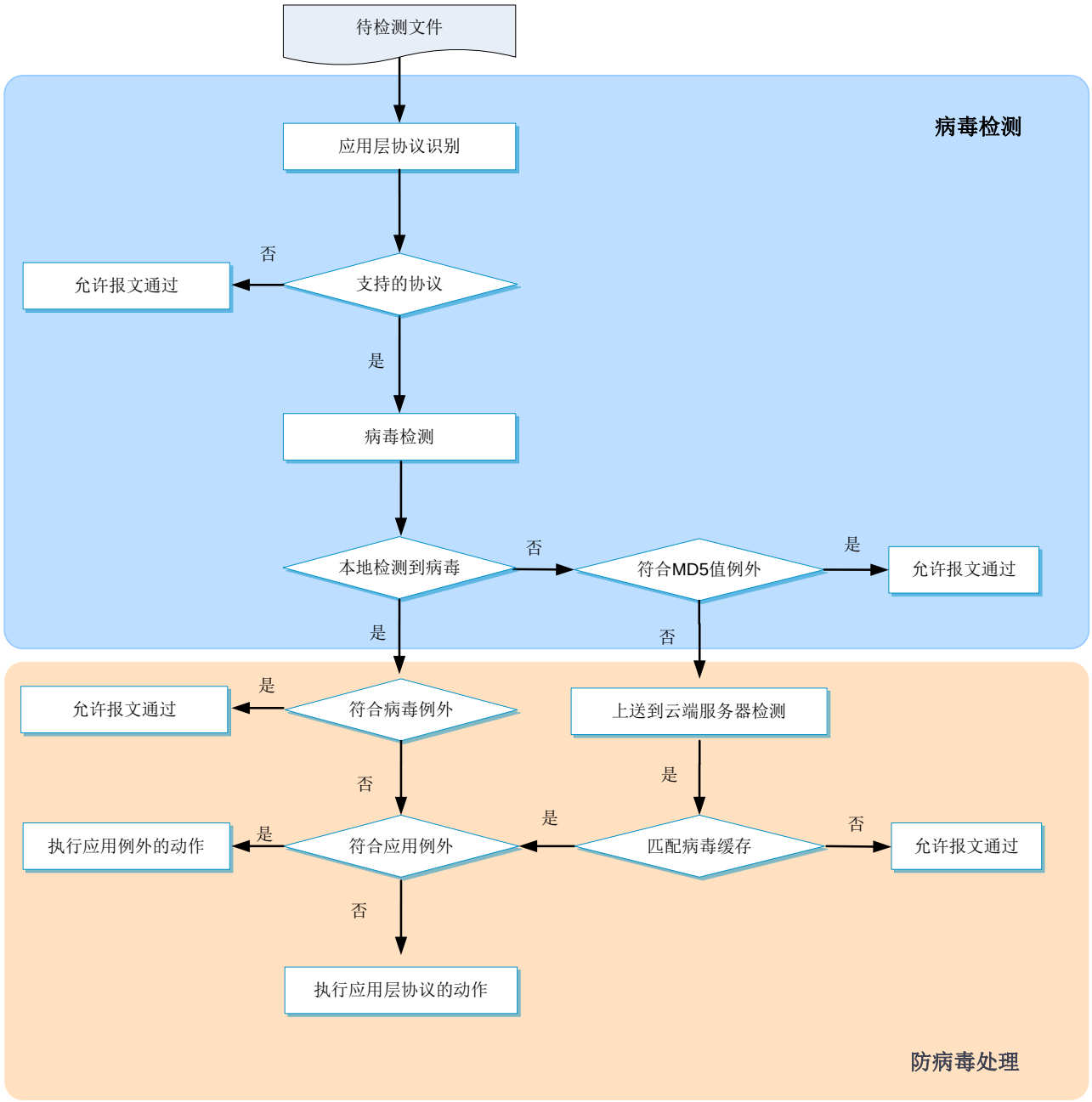
增强检测

当防病毒业务未识别出病毒时，可将待检测文件发往智能业务平台继续进行病毒检测，从而提高病毒识别成功率。

防病毒数据处理流程

设备上部署防病毒配置文件后，对接收到的用户数据报文处理流程如图-2 所示：

图-2 防病毒数据处理流程图



防病毒处理的整体流程如下：

2. 如果报文匹配了某个安全策略，且此策略的动作是**允许并引用**了防病毒配置文件，则设备将继续识别此报文的应用层协议。

3. 设备对应用层协议进行识别，判断协议是否为防病毒功能所支持，如果支持，则进行下一步处理；否则直接允许报文通过，不对其进行防病毒检测。

4. 设备对报文进行病毒检测，将报文同时与特征库中的病毒特征和 MD5 规则进行匹配，任意一种匹配成功，则认为该报文携带病毒，并进行下一步处理；如果二者均匹配失败，则判断是否匹配 MD5 值例外，如果符合，则允许报文通过；如果不符合，则上送到云端服务器检测（即进入步骤（6）处理）；如果未开启云端查询功能或云端服务器不可用，则对该报文执行允许动作。

5. 如果报文符合病毒例外，则对此报文执行允许动作，否则继续进行下一步处理。

6. 如果报文符合应用例外，则执行应用例外的防病毒动作（告警、阻断和允许），否则执行报文所属应用层协议的防病毒动作（告警、阻断和重定向）。

7. 如果云端服务器检测到病毒，则判断是否符合应用例外。如果报文符合应用例外，则执行应用例外的动作（告警、阻断和允许）；如果不符合，则执行报文所属应用层协议的防病毒动作（告警、阻断和重定向）。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

License支持情况

防病毒功能需要购买并正确安装 License 才能使用。License 过期后，防病毒功能可以采用设备中已有的病毒特征库正常工作，但无法升级特征库且云端查询功能以及联动沙箱阻断功能无法使用。关于 License 的详细介绍请参见“License 配置”。

使用限制和注意事项

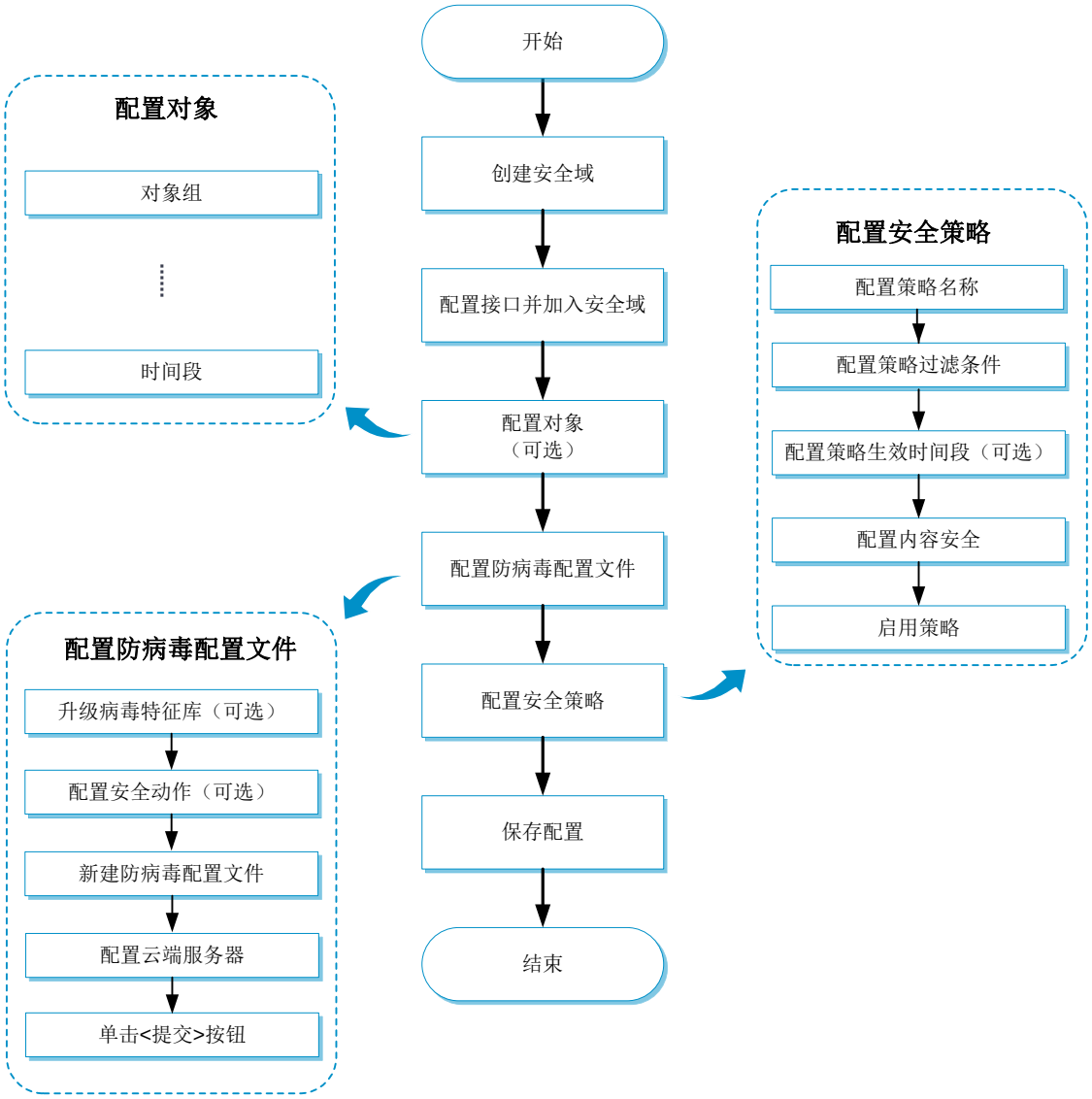
- 执行“提交”操作会暂时中断 DPI 业务的处理，可能导致其他基于 DPI 功能的业务同时出现中断。例如，安全策略无法对应用进行访问控制等。
- 执行“提交”操作后，界面上会提示设置成功，但是配置文件此时可能尚未完成激活，如果此时报文经过设备，可能会出现暂时无法识别的情况。
- 设备支持对压缩文件以及解压缩后的最终子文件进行云端查询。
- 配置告警信息模板后，设备会对匹配防病毒配置文件的 HTTP 流量进行代理，将对设备性能产生较大影响，请根据实际情况判断是否需要配置告警信息模板。
- 云端查询功能的支持情况与设备型号有关，请以页面的实际显示为准。
- 在使用基于 HTTPS 协议的防病毒 MD5 值云端查询功能时，当网络状态发生变更，可通过手动触发设备重新注册云端服务器，或等待网络流量自动触发云端请求。

配置指南

配置思路

防病毒功能的配置思路如下图所示：

图-3 防病毒功能配置指导图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

缺省防病毒配置任务

设备上存在一个名称为 default 的防病毒配置文件，不可对其进行修改和删除操作，缺省防病毒配置文件使用当前系统中的所有病毒特征。如果需要检测当前系统中的所有病毒特征，可使用缺省防病毒配置文件，从而简化操作并节省时间。

1. 选择“策略 > 防病毒 > 配置文件”。default 的防病毒配置文件不可编辑。
2. 在安全策略的内容安全配置中引用此防病毒配置文件，有关安全策略的详细配置介绍请参见“安全策略”。

定制化防病毒配置任务

当缺省防病毒配置文件不满足需求时，管理员可以根据业务环境和安全要求，灵活调整自定义防病毒配置文件中的病毒设置，以更好地适应实际情况。

因为防病毒模块所支持协议的连接请求均由客户端发起，为了使连接可以成功建立并能对此连接上的报文进行病毒检测，需要管理员在配置安全策略时确保客户端所在的安全域为源安全域、服务器所在的安全域为目的安全域。

1. 选择“策略 > 防病毒 > 配置文件”

2. 在“防病毒配置文件”页面单击<新建>按钮，进入“新建防病毒配置文件”页面。具体配置内容如下：

表-1 防病毒配置文件配置

参数	说明
名称	防病毒配置文件的名称
描述	通过合理编写描述信息，便于管理员快速理解和识别防病毒配置文件的作用，有利于
开启云端查询功能	开启此功能后，当设备无法识别出病毒时，会将未识别出的文件的MD5值发往云端服
告警信息模板	配置本模板后，当设备检测出病毒时，支持向客户端返回告警信息 此功能仅在配置HTTP协议的上传或下载方向的动作为阻断时支持 可在新建或引用告警信息模板后，单击右侧的<配置>按钮，导入告警信息 告警信息仅支持以TXT和HTML类型文件的方式导入 配置本功能后，入侵防御功能对HTTP协议报文的抓包动作将失效
上传	对HTTP、FTP、SMTP、NFS、SMB和IMAP协议上传方向的报文进行病毒检测。其 议只支持上传方向
下载	对HTTP、FTP、POP3、NFS、SMB和IMAP协议下载方向的报文进行病毒检测。其

	只支持下载方向
动作	设备可根据报文的应用层协议类型和传输方向来对其进行病毒检测，如果检测到病 执行此处指定的动作。动作包括：告警、阻断、重定向。IMAP协议只支持告警动作
缓存文件上限	表示缓存的待检测文件大小 仅当配置HTTP协议的上传或下载方向的动作为阻断时支持
应用例外	缺省情况下，设备基于应用层协议的防病毒动作对符合病毒特征的报文进行处理。 层协议上承载的某一具体应用采取不同的动作时，可以将此应用设置为应用例外。 协议进行允许通过处理，但是需要对HTTP协议上承载的游戏类应用采取阻断动作， 有游戏类的应用设置为应用例外
病毒例外	如果发现某类检测出病毒的报文被误报时，可以通过执行此命令把该报文对应的病 毒例外。当后续再有检测出包含此病毒特征的报文通过时，设备将对其执行允许动
MD5值例外	如果发现某类检测出病毒的报文被误报时，用户可以通过查看威胁日志获取病毒的M MD5值设置为例外。当后续再有检测出符合该MD5值的报文通过时，设备将对其执

3. 单击<确定>按钮，新建防病毒配置文件成功，且会在“防病毒配置文件”页面中显示。

4. 在安全策略的内容安全配置中引用此防病毒配置文件，具体配置步骤请参见“缺省防病毒配置任务”章节。

5. 单击<提交>按钮，激活防病毒配置文件的配置内容。配置此功能会暂时中断 DPI 业务的处理，为避免重复配置此功能对 DPI 业务造成影响，请完成部署 DPI 各业务模块的配置文件后统一配置此功能。

配置病毒检测扩展功能

配置云端服务器

在防病毒配置文件中开启防病毒 MD5 值云端查询功能后，当设备无法识别出病毒时，会将未识别出的文件的 MD5 值发往云端服务器进行查询。

1. 选择“策略 > 防病毒 > 配置文件”
2. 在“配置文件”页面单击“云端服务器连接状态”右边的<配置>按钮，进入“配置云端服务器”页面。
3. 云端服务器的具体配置内容如下：

表-2 云端服务器配置内容

参数	说明
服务器地址	云端服务器的地址，支持输入IP地址或者域名。目前，仅支持配置我司云端服务器
缓存MD5条数	设备会将云端服务器返回的查询结果缓存在防病毒缓存中，缓存中分为命中列表和非 • 非命中列表：表示该 MD5 值不属于病毒或不确定是否属于病毒 • 命中列表：表示该 MD5 值属于病毒 本参数用于配置两个列表中分别可以缓存的MD5条数
缓存最短保留时间	本参数用于配置MD5缓存的最短保留时长，未达到最短保留时间的MD5缓存不会被 当配置的MD5缓存条数小于当前已缓存的数目时，设备将从防病毒缓存中删除最老的

	使该MD5缓存未达到最短保留时间，也将被删除
协议	云端服务器的协议，支持DTLS和HTTPS协议 • DTLS 协议：适用于低延迟的场景。如实时通信（VoIP、视频会议）、物联网设器网络）和流媒体服务 • HTTPS 协议：适用于所有需要保护数据传输安全的场景。如在线银行、社交媒服务和任何需要用户身份验证和数据加密的 Web 应用
配置代理服务器	配置代理服务器的地址、端口和登录代理服务器使用的用户名及密码。仅设置云端HTTPS时支持此参数

4. 单击<确定>按钮，完成云端服务器的配置。

配置增强检测功能

当防病毒业务未识别出病毒时，可将待检测文件发往智能业务平台继续进行病毒检测，从而提高病毒识别成功率。

1. 选择“策略 > 防病毒 > 配置文件”
2. 在“配置文件”页面单击“增强检测”右侧的<配置>按钮，进入“增强检测”页面。
3. 增强检测功能的具体配置内容如下：

表-3 增强检测功能配置内容

参数	说明
服务IPv4地址	增强检测服务的IP地址，该服务由智能业务平台提供，此IP地址为该平台对外提供

	该平台内联口的IP地址。设备将根据此IP地址将待检测文件上送到智能业务平台进行
缓存文件大小上限	开启增强检测功能后，设备会先将缓存的文件上送智能业务平台进行病毒检测，如果缓存大小上限，则不上送
开启增强检测功能	开启本功能后，当防病毒业务未识别出病毒时，会将待检测文件发往智能业务平台检测，从而提高病毒识别成功率

4. 单击<确定>按钮，完成增强检测功能的配置。

查看病毒家族信息

病毒家族是指具有相似特征和行为的一组病毒样本的集合。病毒家族通常由同一作者或团队开发，它们共享相似的代码、传播方式和攻击目标。病毒家族的命名通常基于其特征或首次发现的样本。通过对病毒家族进行研究和分析，安全厂商可以开发相应的病毒特征库，以便及时识别和阻止这些病毒的传播。

1. 选择“策略 > 防病毒 > 配置文件”
2. 进入“病毒家族”页面，查看病毒家族ID及病毒家族名称信息，支持输入病毒家族ID或名称检索病毒家族信息。

威胁情报

本帮助主要介绍以下内容：

- IP 信誉
  - 特性简介
  - vSystem 相关说明
  - License 支持情况
  - 使用限制和注意事项
  - 配置指南
- URL 信誉
  - 特性简介
  - vSystem 相关说明
  - License 支持情况
  - 使用限制和注意事项
  - 配置指南
- 域名信誉
  - 特性简介

    - vSystem 相关说明
    - License 支持情况
    - 使用限制和注意事项
    - 配置指南
- 统一威胁平台下发情报
    - 特性简介
    - vSystem 相关说明
    - 使用限制和注意事项

IP信誉

特性简介

IP 信誉功能用于根据本地 IP 信誉中记录的 IP 地址信息对网络流量进行过滤。本地 IP 信誉包括设备加载的 IP 信誉特征库以及云端服务器历史查询结果，即本地 IP 信誉缓存。

IP 信誉特征库

IP 信誉特征库主要是具有僵尸主机 DDoS 攻击、命令注入攻击、木马下载和端口扫描等风险的 IP 地址集合。特征库中包含每个 IP 地址的攻击类型以及攻击类型的建议动作和是否记录日志等信息。

云端服务器

云端服务器向设备提供 IP 信誉云端查询功能，用于扩充本地加载的 IP 信誉特征库。当 IP 信誉特征库无法匹配报文中的 IP 地址信息时，可通过 IP 信誉云端查询功能，将 IP 地址信息上送云端服务器进行查询。云端服务器完成检测后，会将检测结果发送给设备，设备会将检测结果保存到本地 IP 信誉缓存中，便于后续报文直接在本地进行 IP 信誉匹配，而不必再上送云端服务器查询。

攻击类型动作

攻击类型动作是指当报文的源/目的 IP 地址命中本地 IP 信誉后，设备对报文执行的动作。支持的动作类型为丢弃和允许，并支持日志记录功能。

本地 IP 信誉中，一个 IP 地址可对应多种攻击分类，每种攻击分类都有对应执行的动作。

当 IP 地址只属于一种攻击分类时，设备将对匹配上该 IP 地址的报文执行攻击分类对应的动作；当 IP 地址属于多种攻击分类时，设备将对匹配上该 IP 地址的报文执行多种攻击分类中优先级最高的动作。其中，动作的优先级从高到低依次为：丢弃>允许。

只要IP地址所属的任一攻击分类配置了日志动作,则对匹配上该IP地址的报文执行记录日志动作。

IP 例外

若报文的源/目的 IP 地址与例外 IP 地址匹配成功，则设备直接放行该报文，不再进行后续 IP 信誉的检测。

加入/移出黑名单

设备支持将 IP 信誉库中的 IP 地址手工加入或移出黑名单，并根据 IP 地址的方向属性分别加入源地址/目的地址黑名单。

IP 信誉库中的 IP 地址均为公网地址，使用 IP 信誉功能添加的黑名单表项 VRF 为公网。

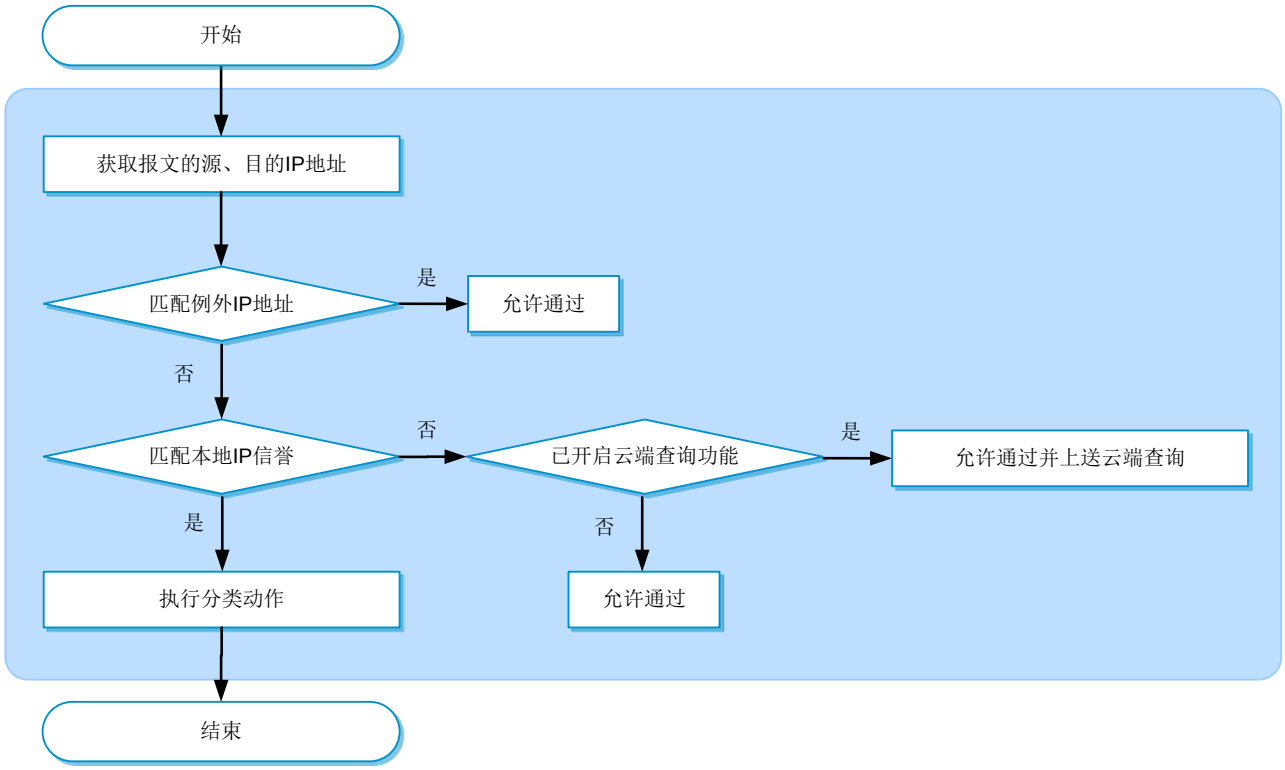
黑名单的默认老化时间为 7 天。如需修改，请到“策略 > 主动防护 > 黑名单”页面进行相关操作。

有关黑名单的详细介绍，请参见“攻击防范联机帮助”。

IP 信誉的报文处理流程

IP 信誉对报文的处理流程如图-1 所示：

图-1 IP 信誉的报文处理流程图



IP 信誉功能对报文的处理过程如下：

2. 设备将报文的源 IP 地址和目的 IP 地址与例外 IP 地址进行匹配。任何一个 IP 地址与例外 IP 地址匹配成功，均放行报文。如果匹配失败，则进入下一步处理。

3. 设备将报文的源 IP 地址和目的 IP 地址与本地 IP 信誉进行匹配。

   本地 IP 信誉中的 IP 地址具有方向属性，包含源、目的和双向（即既可作为源地址也可作为目的地址）。仅当报文的 IP 地址与本地 IP 信誉的 IP 地址和方向属性均一致时，才认为匹配成功（如果本地 IP 信誉中 IP 地址的方向属性是双向，则报文的源 IP 地址和目的 IP 地址均可匹配成功）。

   设备将根据匹配结果执行如下操作：

- 如果匹配成功，设备将执行本地 IP 信誉中 IP 地址所属攻击分类的动作，设备支持的攻击分类动作如下：
  - 若动作为“允许”，则设备将允许此报文通过。
  - 若动作为“丢弃”，则设备将丢弃此报文。
  - 若动作为“日志”，则设备将记录 IP 信誉日志。
- 如果匹配失败，设备将判断是否已开启云端查询功能。如果已开启，则放行报文并将 IP 地址信息上送云端服务器进行查询，设备会将服务器返回的查询结果保存到本地 IP 信誉缓存中，便于后续报文在本地进行 IP 信誉匹配，而不必再上送云端服务器；如果未开启，则直接放行报文。

vSystem 相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

License 支持情况

IP 信誉功能需要购买并正确安装威胁情报 License 后才能使用。License 过期后，IP 信誉功能可以使用设备中已有的特征库正常工作，但无法升级到 License 有效期之后发布的新版本的特征库。同时，云端查询功能也不可用。关于 License 的详细介绍请参见“License 联机帮助”。

使用限制和注意事项

- 关闭 Top 统计功能后，统计信息将自动清空。
- 使用 IP 信誉功能添加的源地址黑名单，不携带 DS-Lite 对端地址等信息，如需修改，请到“策略 > 主动防护 > 黑名单”页面进行相关操作。
- 启用 IP 信誉云端查询功能前，请先到“对象 > 应用安全 > 云端服务器”页面，确认云端服务器处于“已连接”状态。如果连接状态异常，可单击<检查>按钮，根据提示信息进行排查。
- 当设备中所有的 Context 下都关闭了 IP 信誉云端查询功能时，设备会清空本地所有 IP 信誉缓存。
- 当前系统时间需要自动同步网络时间。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。

- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

开启 IP 信誉功能

开启 IP 信誉功能的具体配置步骤如下：

1. 选择“策略 > 主动防护 > 威胁情报”。
2. 在 IP 信誉区域，单击“IP 信誉功能”后的划选按钮，开启 IP 信誉功能。
3. 单击<IP 地址查询>按钮，进入 IP 地址查询页面，在输入框中输入查询的 IP 地址，单击<查询>按钮，可以查询指定 IP 地址的相关信息。也可将指定的 IP 地址加入/移出黑名单和 IP 例外。

开启 IP 信誉云端查询功能

开启 IP 信誉云端查询功能的具体配置步骤如下:

1. 选择“策略 > 主动防护 > 威胁情报”。
2. 在 IP 信誉区域，单击“IP 信誉功能”后的划选按钮，开启 IP 信誉功能。
3. 在 IP 信誉区域，单击“开启 IP 信誉云端查询功能”后的划选按钮，开启 IP 信誉云端查询功能。

开启 Top 统计功能

开启 Top 统计功能的具体配置步骤如下：

1. 选择“策略 > 主动防护 > 威胁情报”。

2. 在 IP 信誉区域，单击“IP 信誉功能”后的划选按钮，开启 IP 信誉功能。

3. 单击“IP 地址命中统计功能”后的划选按钮，开启 IP 信誉 Top 统计功能。

4. 单击<Top 统计>按钮，进入 Top 统计页面，配置统计条件后，可获取到命中 IP 信誉库的 IP 地址统计排名信息。也可将指定的 IP 地址加入/移出黑名单和 IP 例外。

配置攻击类型动作

配置攻击类型动作的具体配置步骤如下：

1. 选择“策略 > 主动防护 > 威胁情报”。

2. 在 IP 信誉区域，单击“IP 信誉功能”后的划选按钮，开启 IP 信誉功能。

3. 在动作配置区域，为指定的攻击类型配置相应的动作和日志功能。

   支持的操作如下：

   - 可配置动作为允许或丢弃，并选择开启或关闭日志功能。
   - 也可通过单击<恢复缺省>按钮，恢复为 IP 信誉库中攻击类型的默认动作和日志功能。

4. 完成配置后，单击<应用>按钮，使配置生效。

配置 IP 例外

配置 IP 例外的具体配置步骤如下：

1. 选择“策略 > 主动防护 > 威胁情报”。

2. 在 IP 信誉区域，单击“IP 信誉功能”后的划选按钮，开启 IP 信誉功能。

3. 在 IP 例外区域，向输入框中添加 IP 地址，以回车分割，可配置多个 IP 例外。

4. 完成配置后，单击<应用>按钮，使配置生效。

URL信誉

特性简介

URL 信誉功能用于对恶意的 URL 进行过滤，允许或禁止用户访问某些网站，达到规范用户上网行为的目的。当报文中的 URL 匹配到本地 URL 信誉后，设备将对报文执行相应的操作。本地 URL 信誉包括设备加载的 URL 信誉特征库以及云端服务器历史查询结果，即本地 URL 信誉缓存。

URL 信誉特征库

URL 信誉特征库主要是一些恶意 URL 的集合，包含每个 URL 所属的攻击类型等信息。

云端服务器

云端服务器向设备提供 URL 信誉云端查询功能，用于扩充本地加载的 URL 信誉特征库。当 URL 信誉特征库无法匹配报文中的 URL 信息时，可通过 URL 信誉云端查询功能，将 URL 信息上送云端

服务器进行查询。云端服务器完成检测后，会将检测结果发送给设备，设备会将检测结果保存到本地 URL 信誉缓存中，便于后续报文直接在本地进行 URL 信誉匹配，而不必再上送云端服务器查询。

vSystem 相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

License 支持情况

URL 信誉功能需要购买并正确安装威胁情报 License 才能使用。License 过期后，URL 信誉功能可以采用设备中已有的特征库正常工作，但无法升级特征库。关于 License 的详细介绍请参见“License 联机帮助”。

使用限制和注意事项

URL 信誉功能需要购买并正确安装威胁情报 License 才能使用。License 过期后，URL 信誉功能可以采用设备中已有的特征库正常工作，但无法升级到 License 有效期之后发布的新版本的特征库。关于 License 的详细介绍请参见“License 联机帮助”。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

开启 URL 信誉功能

URL 信誉的具体配置步骤如下：

1. 选择“对象 > 安全配置文件 > URL 过滤 > URL 过滤”。
2. 在“URL 过滤配置文件”页面，可以选择新建或编辑一个 URL 过滤配置文件。

   具体操作步骤如下：

   a. 如需新建 URL 过滤配置文件，则单击<新建>按钮，进入“新建 URL 过滤配置文件”页面，配置文件名称；如需编辑 URL 过滤配置文件，则单击指定配置文件右侧的<编辑>按钮，进入“编辑 URL 过滤配置文件页面”。

b. 配置URL所属攻击类型的动作。当报文中提取的URL与URL信誉特征库匹配成功时，则对报文执行 URL 所属攻击类型的动作。

c. 勾选开启 URL 信誉功能。

3. 单击<确认>按钮，完成配置。

域名信誉

特性简介

域名信誉功能用于根据本地域名信誉或域名威胁源中记录的域名对网络流量进行过滤。本地域名信誉包括设备加载的域名信誉特征库以及云端服务器历史查询结果，即本地域名信誉缓存。

域名信誉特征库

域名信誉特征库主要是具有僵尸主机 DDoS 攻击、命令注入攻击、木马下载和端口扫描等风险的域名集合。特征库中包含每个域名的攻击类型以及攻击类型的建议动作和是否记录日志等信息。

有关特征库升级的详细介绍，请参见“特征库升级联机帮助”。

域名威胁源

域名威胁源是指各种域名信息的集合。

当需要的域名在设备当前特征库中不存在时，用户可通过手工配置的方式将域名信息添加到威胁源中。当后续检测出符合该域名的报文通过时，设备将对其执行配置的处理动作。

有关域名威胁源的详细介绍，请参见“威胁源管理联机帮助”。

云端服务器

云端服务器向设备提供域名信誉云端查询功能，用于扩充本地加载的域名信誉特征库。当域名信誉特征库无法匹配报文中的域名信息时，可通过域名信誉云端查询功能，将域名信息上送云端服务器进行查询。云端服务器完成检测后，会将检测结果发送给设备，设备会将检测结果保存到本地域名信誉缓存中，便于后续报文直接在本地进行域名信誉匹配，而不必再上送云端服务器查询。

攻击类型动作

攻击类型动作是指当 DNS 报文中的域名匹配到本地域名信誉中的域名后，设备对报文执行的动作。支持的动作类型为丢弃和允许，并支持日志记录功能。

域名信誉特征库中，一个域名可对应多种攻击分类，每种攻击分类都有对应执行的动作。

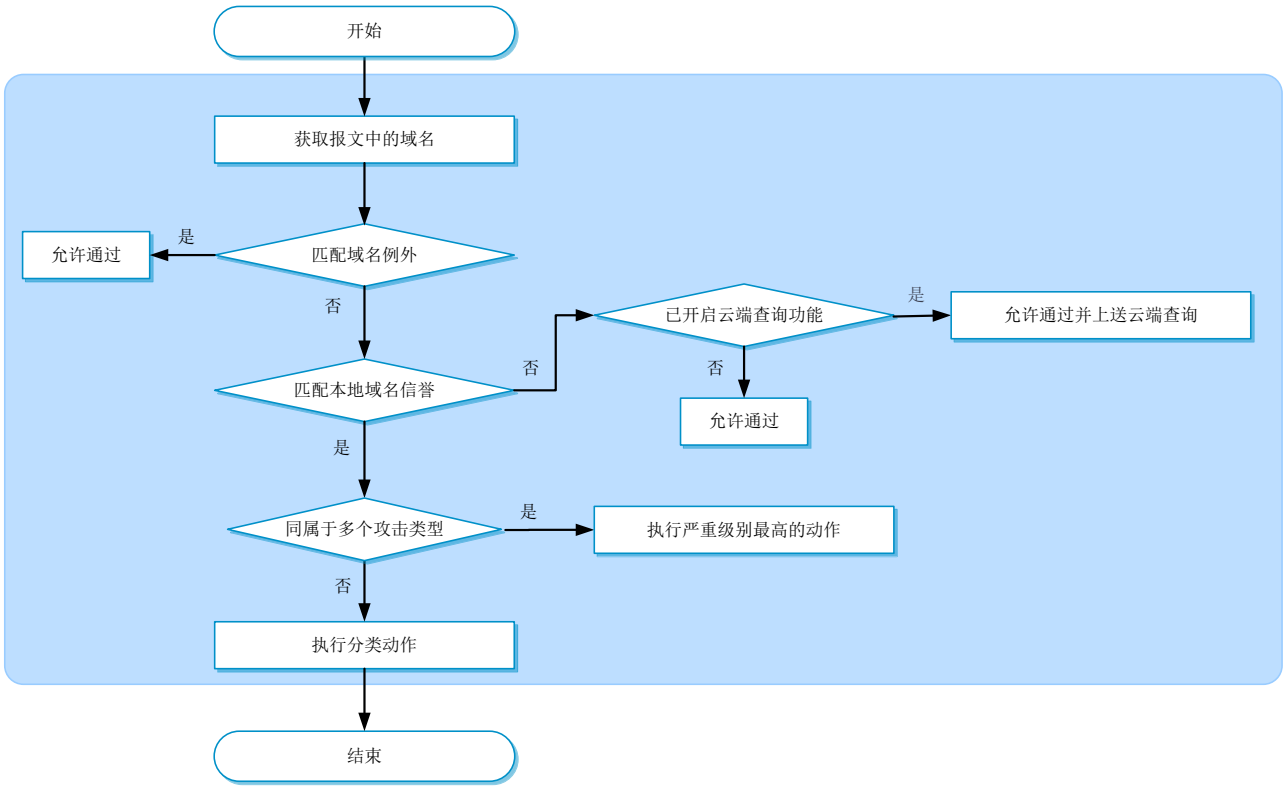
当域名只属于一种攻击分类时，设备将对匹配上该域名的报文执行攻击分类对应的动作；当域名属于多种攻击分类时，设备将对匹配上该域名的报文执行多种攻击分类中优先级最高的动作。其中，动作的优先级从高到低依次为：丢弃>允许。

只要域名所属的任一攻击分类配置了日志动作，则对匹配上该域名的报文执行记录日志动作。

域名信誉的报文处理流程

域名信誉对报文的处理流程如图-2 所示：

图-2 域名信誉的报文处理流程图



域名信誉功能对报文的处理过程如下：

2. 设备将报文中提取的域名与例外域名进行匹配。如果匹配成功，则放行报文；如果匹配失败，则进入下一步处理。

3. 设备将报文中提取的域名与本地域名信誉进行匹配。

   设备将根据匹配结果执行如下操作：

- 如果匹配成功，则进行如下判断：
  - 如果域名属于一个攻击类型，则执行该攻击类型的动作。
  - 如果域名同属于多个攻击类型，则执行严重级别最高的动作。

  其中，如果动作为“允许”，则设备将允许此报文通过；如果动作为“丢弃”，则设备将丢弃此报文；如果动作为“日志”，则设备将记录域名信誉日志。
- 如果匹配失败，设备将判断是否已开启云端查询功能。如果已开启，则放行报文并将域名上送云端服务器进行查询，设备会将服务器返回的查询结果保存到本地域名信誉缓存中，便于后续报文在本地进行域名信誉匹配，而不必再上送云端服务器；如果未开启，则直接放行报文。

例外域名

当管理员不希望对某些域名进行域名信誉检测时，可以将其加入例外域名。当设备检测到客户端发送的 DNS 请求报文中的域名与例外域名匹配时，将不对该域名进行域名信誉业务处理。

vSystem 相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

License 支持情况

域名信誉功能需要购买并正确安装 License 才能使用。License 过期后，域名信誉功能可以采用设备中已有的特征库正常工作，但无法升级到 License 有效期之后发布的新版本的特征库。同时，云端查询功能也不可用。关于 License 的详细介绍请参见“License 联机帮助”。

使用限制和注意事项

- 关闭域名信誉的 Top 统计功能后，统计信息将自动清空。
- 当前系统时间需要自动同步网络时间。
- 启用域名信誉云端查询功能前，请先到“对象 > 应用安全 > 云端服务器”页面，确认云端服务器处于“已连接”状态。如果连接状态异常，可单击<检查>按钮，根据提示信息进行排查。
- 当设备中所有的 Context 下都关闭了域名信誉云端查询功能时，设备会清空本地所有域名信誉缓存。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

开启域名信誉功能

域名信誉功能的具体配置步骤如下：

1. 选择“策略 > 主动防护 > 威胁情报”。
2. 在域名信誉区域，单击“域名信誉功能”后的划选按钮，开启域名信誉功能。
3. 单击<域名查询>按钮，进入域名查询页面，在输入框中输入查询的域名，单击<查询>按钮，可以查询指定域名的相关信息。也可将指定的域名加入/移出例外域名。
4. 单击“开启域名信誉云端查询功能”后的划选按钮，开启域名信誉云端查询功能。
5. 单击“域名命中统计功能”后的划选按钮，开启域名信誉 Top 统计功能。

6. 单击<Top 统计>按钮，进入 Top 统计页面，配置统计条件后，可获取到命中域名信誉库的域名统计排名信息。也可将指定的域名加入/移出例外域名。

7. 在动作配置区域，为指定的攻击类型配置相应的动作和日志功能。

   支持的操作如下：

   - 可配置动作为允许或丢弃，并选择开启或关闭日志功能。
   - 也可通过单击<恢复缺省>按钮，恢复为域名信誉库中攻击类型的默认动作和日志功能。

8. 如果需要的域名设备当前特征库中不存在时，可以新建自定义域名威胁源，单击“自定义”，然后选择<新建域名威胁源>，具体配置如下：

   表-1 域名威胁源配置

参数	说明
名称	域名威胁源的名称
来源	域名威胁源的配置方式，取值包括： • 本地新建：表示手动输入威胁信息 • 本地导入：表示通过表格批量导入威胁信息，仅支持导入 CSV 格式文件 • 外部服务器：表示通过第三方威胁服务器同步获取
域名	域名威胁源的配置方式为本地新建，手动输入需要的威胁信息
本地导入	选择需要导入的域名文件，批量导入域名信息

服务器地址	服务器的地址
VRF实例	服务器所属的VPN实例
刷新率	威胁源刷新间隔时间
认证方式	服务器的认证方式，取值包括： • 无：表示访问服务器不需要身份认证 • 用户名和密码：表示访问服务器时需要用户名和密码认证
用户名	服务器的用户名
密码	服务器的密码
启用	激活威胁源，使其被相关功能引用后生效

9. 单击<确定>按钮，新建域名威胁源成功，单击<添加>按钮，完成域名威胁源的配置。

10. 完成配置后，单击<应用>按钮，使配置生效。

配置例外域名

配置例外域名的具体配置步骤如下：

1. 选择“策略 > 主动防护 > 威胁情报”。

2. 在“域名信誉> 高级配置”区域，向例外域名输入框中添加域名，以回车分割，可配置多个例外域名。

3. 单击<应用>按钮，完成配置。

统一威胁平台下发情报

特性简介

设备支持接收并展示由统一威胁平台（即安全威胁发现与运营管理平台）下发的威胁情报，包括 IP 信誉、URL 信誉、域名信誉和 MD5 信誉。可用于扩充本地加载的信誉特征库和防病毒特征库，更好的防护内网用户安全。

vSystem 相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 为保证成功接收平台下发的 IP 信誉和 MD5 信誉，需要在设备上开启 NETCONF over SOAP 功能。即在命令行界面的系统视图下，配置 **netconf soap http enable** 和 **netconf soap https enable** 命令。
- 为保证成功接收平台下发的 URL 信誉和域名信誉，需要在设备上配置平台服务器域名。即在命令行界面的系统视图下，配置 **cloud-management server domain** 命令。同时，还需

要配置快速日志输出时携带设备序列号，即在系统视图下，执行 **customlog with-sn** 命令。

- 为保证设备可使用平台下发的威胁情报进行报文匹配，请先配置 IP 信誉、URL 信誉、域名信誉和防病毒功能。

黑名单

本帮助主要介绍以下内容：

- 特性简介
  - IP 黑名单
  - 地址对象组黑名单
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置思路
  - 配置准备
  - 配置基于 IP 黑名单的访问控制
  - 配置基于地址对象组黑名单的访问控制
  - 配置基于扫描攻击防范的动态黑名单的访问控制

特性简介

IP 黑名单

IP 黑名单功能是根据报文的 IP 地址进行报文过滤的一种攻击防范特性。根据报文过滤条件的不同，可分为源 IP 黑名单和目的 IP 黑名单。

若全局的黑名单过滤功能处于开启状态，则所有安全域上的 IP 黑名单过滤功能均处于开启状态。若全局的黑名单过滤功能处于关闭状态，则需要开启指定安全域上的黑名单过滤功能。

同基于 ACL 的包过滤功能相比，黑名单进行报文匹配的方式更为简单，可以实现报文的高速过滤和有效屏蔽。

黑名单可以由设备动态或由用户手工进行添加、删除，具体机制如下：

- 动态添加黑名单是与扫描攻击防范功能配合实现的，动态生成的黑名单表项会在一定的时间之后老化。当设备根据报文的行为特征检测到某特定 IP 地址的扫描攻击企图之后，便将攻击者的 IP 地址自动加入黑名单，之后该 IP 地址发送的报文会被设备过滤掉。
- 手动配置的黑名单表项分为永久黑名单表项和非永久黑名单表项。永久黑名单表项建立后，一直存在，除非用户手工删除该表项。非永久黑名单表项的老化时间由用户指定，超出老化时间后，设备会自动将该黑名单表项删除。

地址对象组黑名单

地址对象组黑名单是基于地址对象组进行报文过滤的一种攻击防范特性。该特性需要和地址对象组功能配合使用，由后者为其提供地址对象组和 IP 地址的对应关系。同 IP 黑名单的包过滤功能相比，地址组黑名单可以对网段进行访问控制，提高了易用性。有关对象组的详细介绍请参见“对象组”联机帮助。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 设备仅支持对导出的配置文件进行导入，且以增量的方式向当前配置文件中写入导入的配置，并会对重复的配置进行覆盖，导入过程中如果某条配置写入失败，则跳过该条并继续导入，并提示错误信息，且已成功写入的配置无法回退。
- 导出功能，仅导出指定 csv 格式的模板文件。
- 导入功能，导入文件的格式必须为.csv，导入文件大小上限为 2M。
- 同一时刻只允许一个用户进行导入导出的操作。

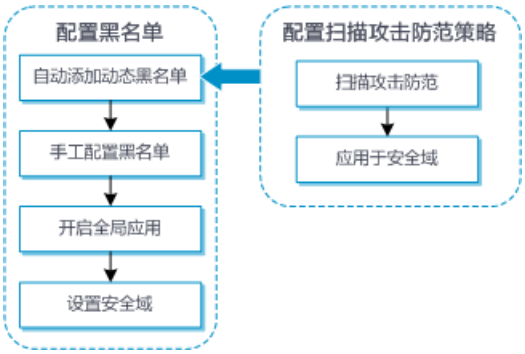
- 设备只允许引用一个 IPv4 地址对象组和一个 IPv6 地址对象组配置黑名单。

配置指南

配置思路

黑名单功能的配置思路如下图所示：

图-1 黑名单功能配置思路图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。

- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置基于 IP 黑名单的访问控制

通过配置基于 IP 黑名单的访问控制功能可以对来自指定 IP 地址和地址对象组的报文进行过滤。具体配置步骤如下：

1. 单击“策略 > 主动防护 > 黑名单”。
2. 在“IP 黑名单”页签单击<新建>按钮，手工添加 IP 黑名单。

表-1 IP 黑名单配置

参数	说明
VRF	黑名单所属的VPN实例 可选择已创建的VRF，也可以新创建VRF。此处新建的VRF，可在“网络 > 接口与V面查看
IP地址类型	• IPv4 • IPv6
IP地址方向	• 源地址

	• 目的地址
IP地址	黑名单的IP地址，用于匹配报文的源IP地址或目的IP地址
DS-Lite对端地址	黑名单的IPv4地址所属的DS-Lite隧道B4端IPv6地址 仅当“IP地址类型”选择“IPv4”、“IP地址方向”选择“源地址”时，支持配置
老化时间（秒）	黑名单表项的剩余老化时间。若不配置，那么该IP黑名单表项永不老化，除非用户
备注信息	添加IP黑名单相关描述信息

3. 如需批量导入 IP 黑名单，可在“IP 黑名单”页面下拉<导入导出>按钮后单击<导入配置>按钮，进入“导入指定配置”页面。

表-2 配置导入 IP 黑名单参数表

参数	说明
类型	• 源 IP 地址 • 目的 IP 地址
VRF	黑名单所属的VPN实例 可选择已创建的VRF，也可以新创建VRF。此处新建的VRF，可在“网络 > 接口与V面查看
文件路径	选择需要导入文件的路径
备注信息	添加IP黑名单相关描述信息

4. 单击<确定>按钮，新建的黑名单或批量导入 IP 黑名单会在“IP 黑名单”页签显示。

5. 在“IP 黑名单”页签单击<开启全局应用>按钮，“IP 黑名单”页签与“地址对象组黑名单”页签下的黑名单对所有安全域生效。

配置基于地址对象组黑名单的访问控制

通过配置基于地址对象组黑名单的访问控制功能可以对来自指定地址对象组的报文进行过滤。具体配置步骤如下：

1. 单击“策略 > 主动防护 > 黑名单”。

2. 在“地址对象组黑名单”页签单击<新建>按钮。

3. 手工添加地址对象组黑名单。

表-3 地址对象组黑名单配置

参数	说明
对象组类型	• IPv4，即 IPv4 地址对象组 • IPv6，即 IPv6 地址对象组
对象组名称	地址对象组的名称 可选择已创建的对象组，也可以新创建对象组。此处新建的对象组，可在“对象 > IPv4/IPv6地址对象组页面查看

4. 单击<确定>按钮，新建的黑名单会在“地址对象组黑名单”页签显示。

5. 在“地址对象组黑名单”页签单击<开启全局应用>按钮，“IP 黑名单”页签与“地址对象组黑名单”页签下的黑名单对所有安全域生效。

配置基于扫描攻击防范的动态黑名单的访问控制

黑名单表项除了可以手工添加之外，还可以通过扫描攻击防范自动添加。具体来讲就是，在黑名单功能使能的前提下，若配置了扫描攻击防范策略及相应的黑名单添加功能，则可以将检测到的扫描攻击方地址添加到黑名单中。有关扫描攻击防范的详细介绍请参见“攻击防范联机帮助”。

具体配置步骤如下：

1. 在“IP 黑名单”或“地址对象组黑名单”页签单击<开启全局应用>按钮，“IP 黑名单”页签与“地址对象组黑名单”页签下的黑名单对所有安全域生效。

2. 单击“对象 > 安全配置文件 > 攻击防范”。

3. 在“攻击防范”页面单击<新建>按钮，进入“新建攻击防范策略”页面，单击“扫描防范”页签，进入扫描攻击防范配置页面，选择非关闭的检测敏感度后配置相关参数并开启<将发起攻击的源 IP 地址添加到黑名单>按钮。具体的配置参数如下表所示。

表-4 扫描防范配置

参数	说明
检测敏感度	扫描攻击防范的检测级别，包括关闭、低、中、高和自定义。关闭表示关闭扫描攻 表示低防范级别，该级别提供基本的扫描攻击检测，有很低的误报率，但对于一些 能检出；中表示中防范级别，该级别有适中的攻击检出率与误报率；高表示高防范 检测出大部分的扫描攻击，但对活跃主机误报率较高，即将可提供服务的主机的报 击报文的概率比较高；自定义表示用户自定义防范级别，该级别的扫描攻击防范阈 定 • 开启端口扫描：开启/关闭端口扫描功能。检测敏感度为低、中、高级别时，该 态；检测敏感度为自定义时，该功能是否开启可以由用户指定 • 阈值：端口扫描攻击的阈值。当检测敏感度为低时，阈值为 100000；当检测敏 值为 40000；当检测敏感度为高时，阈值为 5000；当检测敏感度为自定义时， 活指定端口扫描攻击阈值；当检测敏感度为关闭时，不显示本参数 • 开启地址扫描：开启/关闭地址扫描功能。检测敏感度为低、中、高级别时，该 态；检测敏感度为自定义时，该功能是否开启可以由用户指定 • 阈值：地址扫描攻击的阈值。当检测敏感度为低时，阈值为 100000；当检测敏 值为 40000；当检测敏感度为高时，阈值为 5000；当检测敏感度为自定义时， 活指定地址扫描攻击阈值；当检测敏感度为关闭时，不显示本参数 • 检测周期：扫描攻击防范的检测周期。当检测敏感度为低、中、高时，检测周期 测敏感度为自定义时，可通过配置灵活指定扫描攻击防范的检测阈值；当检测敏 不显示本参数
动作	对扫描攻击的处理行为，包括： • 输出告警日志 • 丢弃攻击者发送的报文 • 将发起攻击的源 IP 地址添加到黑名单 • X 分钟后老化：动态添加的黑名单表项的老化时间。只有勾选“将发起攻击的源 黑名单”时，才会显示该参数

	当“检测敏感度”选择“关闭”时，不显示本参数

4. 单击<确定>按钮，完成配置。此后当设备根据报文的行为特征检测到某特定 IP 地址的扫描攻击企图之后，便将攻击者的 IP 地址自动加入黑名单且会在“IP 黑名单”页签显示，之后该 IP 地址发送的报文会被设备过滤掉。

并发连接限制

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置思路
  - 配置准备
  - 配置基于接口的连接数限制
  - 配置基于整机的连接数限制

特性简介

为了实现保护内部网络资源（主机或服务器）以及合理分配设备系统资源的目的，通常采用并发连接限制对设备上建立的连接数进行统计和限制。

并发连接限制策略

设备支持创建 IPv4 和 IPv6 两种类型的并发连接限制策略，将配置好的并发连接限制策略应用到整机或接口上，实现对用户的并发连接限制。

接口上应用的并发连接限制策略仅对本接口上处理的指定连接生效，整机应用的并发连接限制策略对本设备处理的所有指定的连接生效。

如果在入接口、整机和出接口上分别应用了不同的并发连接限制策略，则经过设备的连接将会依次受到入接口、整机、出接口并发连接限制策略的多重限制，只要该连接的数目达到任何一处连接数上限，都将受到并发连接限制策略的限制。

并发连接限制规则

一个并发连接限制策略中可定义多条并发连接限制规则，每条并发连接限制规则中指定一个并发连接限制的用户范围，属于该范围的用户可建立的连接数及新建连接速率将受到该规则中指定参数的限制。具体如下：

- 并发连接限制：对某类型的连接数进行限制，达到触发限制阈值时，设备将根据用户配置的动作允许、拒绝新建连接请求或将源 IP 地址加入黑名单。若动作配置为拒绝新建连接，则需要等到设备上已有连接因老化而删除，使得当前该类型的连接数低于解除限制阈值后，才允许新建连接；若动作配置为 IP 加入黑名单，则需要等到黑名单老化后，该源 IP 地址才允许新

建连接。连接数达到触发限制阈值时，设备将记录日志；连接数下降到解除限制阈值时，只有动作配置为拒绝新建连接时才会记录日志。

- 新建速率限制：对新建连接的速率进行限制，每秒新建的连接数达到限制值时，设备将根据用户配置的动作允许、拒绝新建连接请求并记录日志或将源 IP 地址加入黑名单。

对于未匹配并发连接限制规则的用户所建立的连接，设备不对其进行限制。

目前，并发连接限制支持根据 ACL 来限定用户范围，对匹配 ACL 规则的用户连接数进行统计和限制。

设备对于某一范围内的用户连接，可根据不同的控制粒度，按照如下各类型进行并发连接限制：

- 按源 IP 地址进行统计和限制，即同一个源 IP 地址发起的连接数目将受到指定阈值的限制。
- 按目的 IP 地址进行统计和限制，即到同一个目的 IP 地址的连接数目将受到指定阈值的限制。
- 按服务端口进行统计和限制，即同一种服务（具有相同传输层协议和服务端口）的连接数目将受到指定阈值的限制。

如果在一条规则中同时指定以上三种类型中的多个，则多种统计和限制类型同时生效。例如，同时指定“按目的 IP 地址进行统计和限制”和“按服务端口进行统计和限制”，则表示对到同一个目的地址的同一种服务的连接数进行统计和限制。若一条规则中不指定以上任何一种限制类型，则表示指定范围内的所有用户连接将整体受到指定的阈值限制。

对设备上建立的连接与某并发连接限制策略进行匹配时，将按照规则编号从小到大的顺序依次遍历该策略中的所有规则，因此在配置并发连接限制规则时，需要从整体策略考虑，根据各规则的内容来合理安排规则的编号顺序，推荐按照限制粒度和范围由小到大的顺序来设置规则序号。

vSystem相关说明

非缺省 VSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

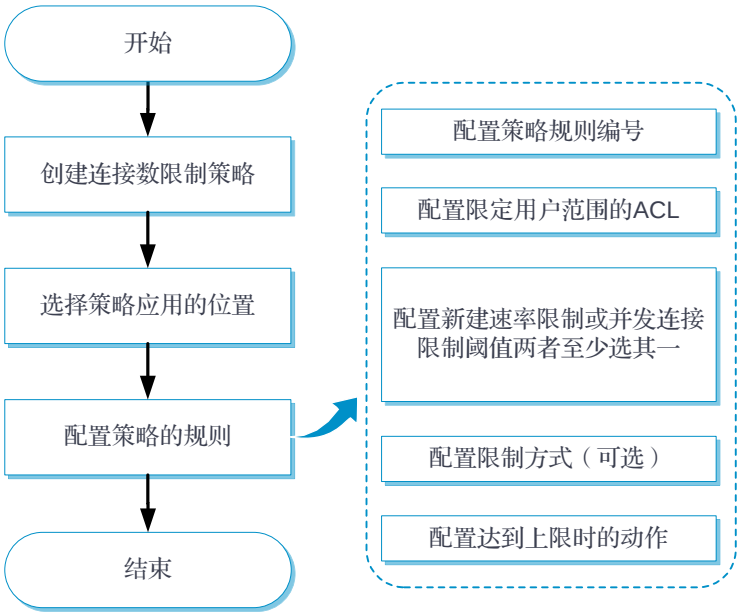
- 对于支持多安全业务板的设备，以安全业务板为单元按照配置的连接数阈值进行限制。
- 应用并发连接限制策略后，仅对新创建的连接生效，已经创建的连接不受此限制。
- 在双机热备组网环境中，从主设备切换到备份设备的会话，不受备份设备上并发连接限制策略的限制。
- 一条 ACL 规则在同一个并发连接限制策略中仅能应用一次，在不同策略中可多次应用。
- 并发连接限制策略不支持应用于 LoopBack 接口。
- 仅限制方式为“按源 IP 地址进行统计和限制”时才可以配置“IP 加入黑名单”动作，且配置该动作必须开启 IP 黑名单才能生效。
- 配置并发连接限制规则时，触发限制阈值需要大于设备 CPU 核数，建议该阈值大于 32。

配置指南

配置思路

并发连接限制功能的配置思路如下图所示：

图-1 并发连接限制配置思路图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置基于接口的连接数限制

基于接口的连接数限制的具体步骤如下：

1. 单击“策略 > 主动防护 > 并发连接限制”。
2. 在“并发连接限制”页面单击<新建>按钮，进入“新建并发连接限制策略”页面，配置并发连接限制策略参数，"应用于"选择指定接口，具体的配置参数如下表所示。启用<开始新建规则>按钮，在单击<确认>按钮后会进入新建 IPv4/IPv6 并发连接限制规则配置页面。

表-1 并发连接限制策略参数

参数	说明
策略编号	并发连接限制策略编号（IPv4、IPv6并发连接限制策略的编号空间各自独立）
IP地址类型	• IPv4 • IPv6

应用于	• 接口上应用的并发连接限制策略仅对本接口上处理的指定连接生效 • 整机应用的并发连接限制策略对本设备处理的所有指定的连接生效
描述	配置连接数限制策略的描述信息
开始新建规则	启用此功能，则新建并发连接限制策略配置完成点击确认后进入新建IPv4/IPv6并发连 置页面
规则编号	IPv4/IPv6并发连接限制规则编号
ACL	配置ACL（支持下拉选择已有的ACL或新建ACL）
新建速率限制	配置最大用户新建连接速率
并发连接限制	• 触发限制阈值：触发并发连接限制的阈值，即连接数值超过此数值时，将不能建 • 解除限制阈值：解除并发连接限制的阈值，即连接数降到此数值时允许建立新的
限制方式	• 按源 IP 地址进行统计和限制，即同一个源 IP 地址发起的连接数目将受到指定阈 • 按目的 IP 地址进行统计和限制，即到同一个目的 IP 地址的连接数目将受到指定 • 按服务端口进行统计和限制，即具有相同服务端口的连接数目将受到指定阈值的
达到上限时的动作	• 允许建立连接 • 拒绝新建连接 • IP 加入黑名单 (仅限制方式勾选按源 IP 地址进行统计和限制时支持此动作。若黑 启时，IP 加入黑名单不生效，请进入策略 > 主动防护 > 黑名单页面开启全部应
继续新建下一条规则	启用此功能，则继续进入新建IPv4/IPv6并发连接限制规则配置页面

3. 单击<确定>按钮，新建并发连接限制策略成功，且会在“并发连接限制”页面中显示。

配置基于整机的连接数限制

具体配置步骤如下：

1. 单击“策略 > 主动防护 > 并发连接限制”。
2. 在“并发连接限制”页面单击<新建>按钮，进入“新建并发连接限制策略”页面，配置并发连接限制策略参数，"应用于"选择"整机"，具体的配置参数请参见表-1。
3. 单击<确定>按钮，新建并发连接限制策略成功，且会在“并发连接限制”页面中显示。

服务器外联防护

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 配置指南
  - 配置思路
  - 配置准备
  - 配置服务器外联学习
  - 配置服务器外联防护策略

特性简介

服务器外联防护是一种针对内网服务器的保护机制，可以有效识别服务器的主动外联行为，为管理员检查服务器提供依据，进而防止服务器成为僵尸网络的一部分，对外发动攻击或对内进行渗透。

为了区分正常的业务报文和攻击报文，首先需要使用服务器外联学习功能来检测指定服务器的主动外联的流量，识别出服务器的所有主动外联行为。然后由管理员对学习结果进行分析和判断，制定相应的外联防护策略来识别异常报文，并输出告警信息，以便管理员进行进一步的处理。

vSystem相关说明

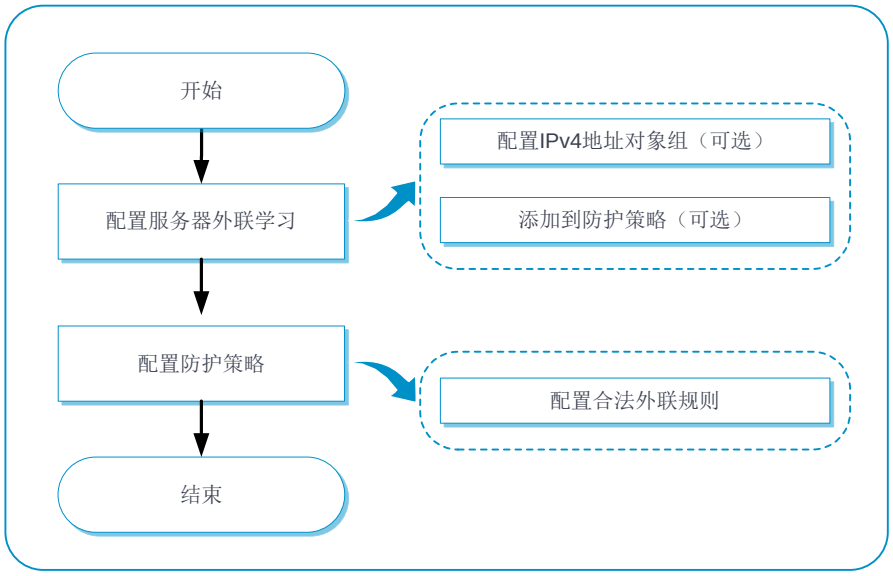
非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置思路

服务器外联防护功能的配置思路如下图所示：

图-1 服务器外联防护功能配置思路图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置服务器外联学习

服务器外联学习功能会对指定服务器主动外联的流量进行检测，识别出服务器的所有外联行为。管理员可以通过学习结果来判断服务器的哪些外联是正常的，哪些外联是异常的，可为管理员配置服务器异常防护策略提供数据依据。

服务器外联学习的具体配置步骤如下：

1. 选择“策略 > 主动防护 > 服务器外联防护”。
2. 在“服务器外联防护”页面选择<服务器外联学习>页签。
3. 选择或输入需要监测的服务器的IP地址，如需新建IPv4地址对象组，具体的配置介绍请参见“对象组“，并选择合适的学习时长，点击<开始>按钮。检测到的信息将显示在下方列表中，管理员可以通过点击<添加到防护策略>按钮，将选中的信息添加为一条防护策略。

配置服务器外联防护策略

服务器外联防护策略中可以配置监测对象、监测规则、防护开关和日志功能。当发现待保护服务器出现异常外联行为时，设备可以对其进行告警。

服务器外联防护策略的具体配置步骤如下：

1. 选择“策略 > 主动防护 > 服务器外联防护”。
2. 在“防护策略”页签，单击<新建>按钮。

3. 新建防护策略，具体的配置参数如下表所示。

表-1 新建防护策略配置参数表

参数	说明
名称	防护策略的名称
服务器地址	防护策略保护的服务器的地址
启用策略	开启或关闭防护策略
记录日志告警	是否生成告警日志
合法外联规则	• 未在合法外联规则中列出的 IP 地址和端口号均为非法外联地址 • 当前页面中显示已存在的合法外联规则，并提供新建、编辑和删除功能。关于新 请注意，必须输入外联地址和至少一个“协议与端口”，外联规则才能正常生效

IP 限速

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置思路
  - 配置准备
  - 配置新建连接速率限制

特性简介

本配置可对设备上的新建会话速率进行限制，防止 DDoS 攻击造成大量新建连接消耗设备的处理性能，影响正常业务。

设备支持配置公网防护和内网防护两种类型的新建连接速率限制：

- 公网防护：用来对公网主动访问内网的连接进行限制，基于报文目的 IP 地址进行新建会话数统计，向同一个目的 IP 地址发起的连接数目将受到指定阈值的限制。

- 内网防护：用来对内网主动访问公网的连接进行限制，基于报文源 IP 地址进行新建会话数统计，同一个源 IP 地址发起的连接数目将受到指定阈值的限制。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

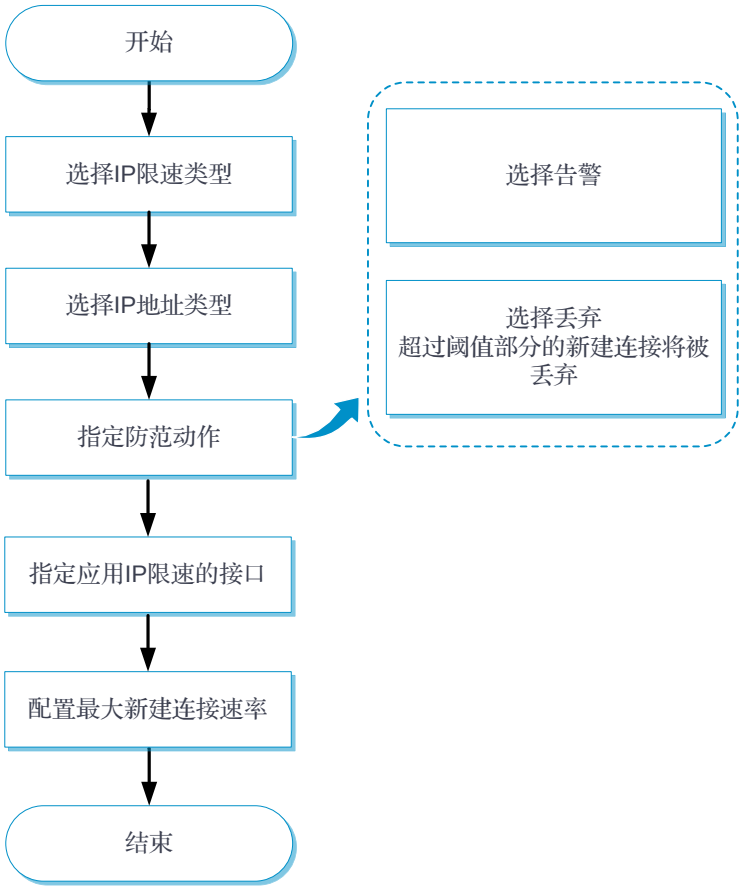
同一个接口上，基于源 IP 地址的新建会话限速功能与基于目的 IP 地址的新建会话限速功能不能同时开启。

配置指南

配置思路

IP 限速的配置思路如下图所示：

图-1 配置指导图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。

- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置新建连接速率限制

支持配置公网防护和内网防护两种类型的新建连接速率限制。公网防护是通过配置对公网主动访问内网的连接进行限制来实现的，内网防护是通过配置对内网主动访问公网的连接限制来实现的。具体的配置步骤如下：

1. 单击“策略 > 主动防护 > IP 限速”。
2. 根据需求请选择公网防护或内网防护，具体的配置参数如下表所示。

表-1 配置参数

参数	说明
IP类型	• IPv4 • IPv6
防范动作	• 告警：超出限速阈值时将发送日志，可在 IP 限速日志界面查看 • 丢弃：丢弃超出限速阈值的新建会话报文
接口	选择需要开启会话限速功能的接口
最大新建连接速率	新建会话限速功能的限速阈值

3. 单击<确定>按钮，完成配置。

应用审计

本帮助主要介绍以下内容：

- 特性简介
  - 基本概念
  - 报文审计流程
  - 审计策略
  - 过滤条件
  - 审计规则
- vSystem 相关说明
- License 支持情况
- 配置指南
  - 配置准备
  - 配置审计策略
  - 配置关键字组

特性简介



本特性会解析出用户报文中的敏感信息和私密信息，请保证将本特性仅用于合法用途。

应用审计是在 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和行为内容，据此对用户的上网行为进行审计和记录。

基本概念

应用行为

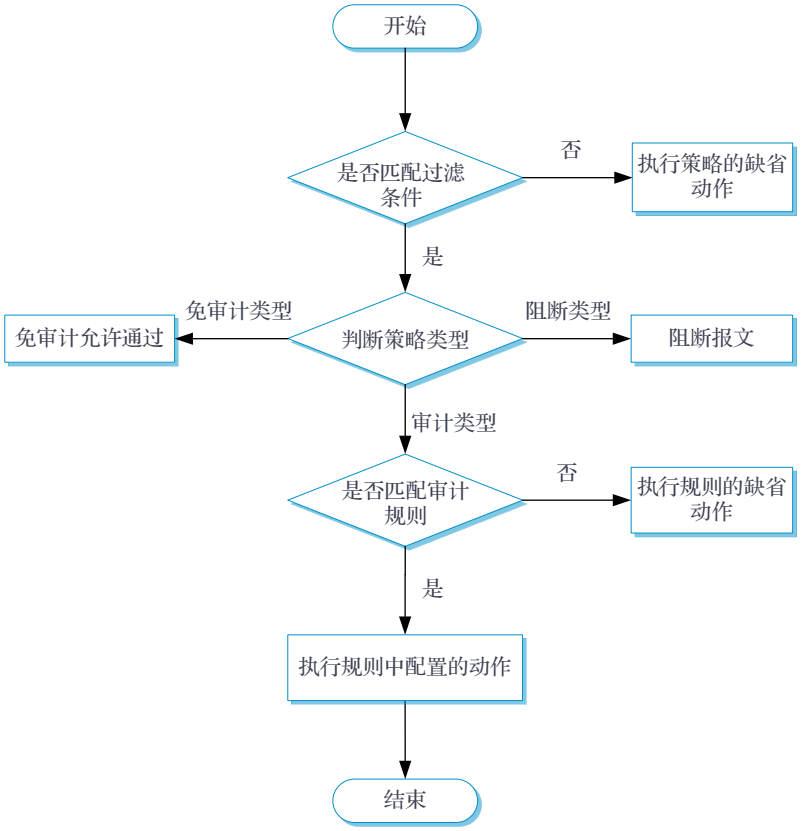
各种应用和软件在使用过程中会表现不同的行为特征，比如 IM 聊天软件的登录、发消息；FTP 的上传文件、下载文件等。

行为内容

行为内容是指某一行为的具体内容，比如 IM 聊天软件登录的行为内容是账号信息，FTP 上传文件的行为内容是文件名信息等。行为内容的匹配方式包括两种：字符串和数字。

报文审计流程

图-1 报文审计流程图



审计策略

不同类型的审计策略能对符合过滤条件的报文进行差异化处理。

策略类型

审计策略分为如下三种类型：

- 审计策略：对匹配策略中所有过滤条件的报文进行审计。
- 免审计策略：对匹配策略中所有过滤条件的报文进行免审计。
- 阻断策略：对匹配策略中所有过滤条件的报文进行阻断。

策略的匹配原则

设备上可以存在多个审计策略，报文按照策略的配置顺序进行匹配，一旦与某个策略匹配成功便结束匹配过程。若报文未与任何策略匹配成功，则设备将根据审计策略的缺省动作对报文进行处理。

审计策略的配置顺序可在“审计策略”页面查看，配置顺序与策略的创建顺序有关，先创建的策略优先进行匹配，也可以通过移动策略的位置来调整策略的配置顺序。根据以上审计策略的匹配原理，为使设备上部署的审计策略对流经设备的报文能够达到更好、更精准的审计效果，需要在配置审计策略时遵循“深度优先”的原则，即先配置审计范围小的，再配置审计范围大的。

过滤条件

审计策略中可以配置多种过滤条件，具体包括：源安全域、目的安全域、源 IP 地址、目的 IP 地址、服务、用户、应用和生效时间段。策略被匹配成功的条件是：策略中已配置的过滤条件均被匹配成功。

每种过滤条件中也可以配置多个匹配项，比如一个源 IP 地址中可以指定多个地址对象组等。每种过滤条件被匹配成功的条件是：过滤条件的任何一个匹配项被匹配成功即可。

审计规则

在审计类型的审计策略中可以配置一系列的审计规则对某一应用的具体行为和行为内容进行精细化审计，并输出审计信息。

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。

设备根据报文与审计规则的匹配结果，将对报文进行如下处理：

- 若报文与审计规则的所有审计项匹配成功，则执行审计规则配置的动作。
- 若报文仅与审计规则的应用/应用分类审计项匹配成功，则放行报文。
- 若报文与审计规则的应用/应用分类审计项匹配失败，则执行审计规则缺省动作。

审计规则中同时支持配置邮件保护功能。设备可对接收到的邮件进行检测，并基于收件人进行统计，保护收件人不受到邮件攻击，具体功能如下：

- 限制邮件发送功能：用于限制用户向其他域名邮箱地址发送邮件。例如，邮箱地址为 user1@abc.com 的用户不能接收来自 user2@123.com 地址的邮件。
- 邮件炸弹攻击防御功能：用于防御收件人在短时间内收到同一发件人的大量邮件。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

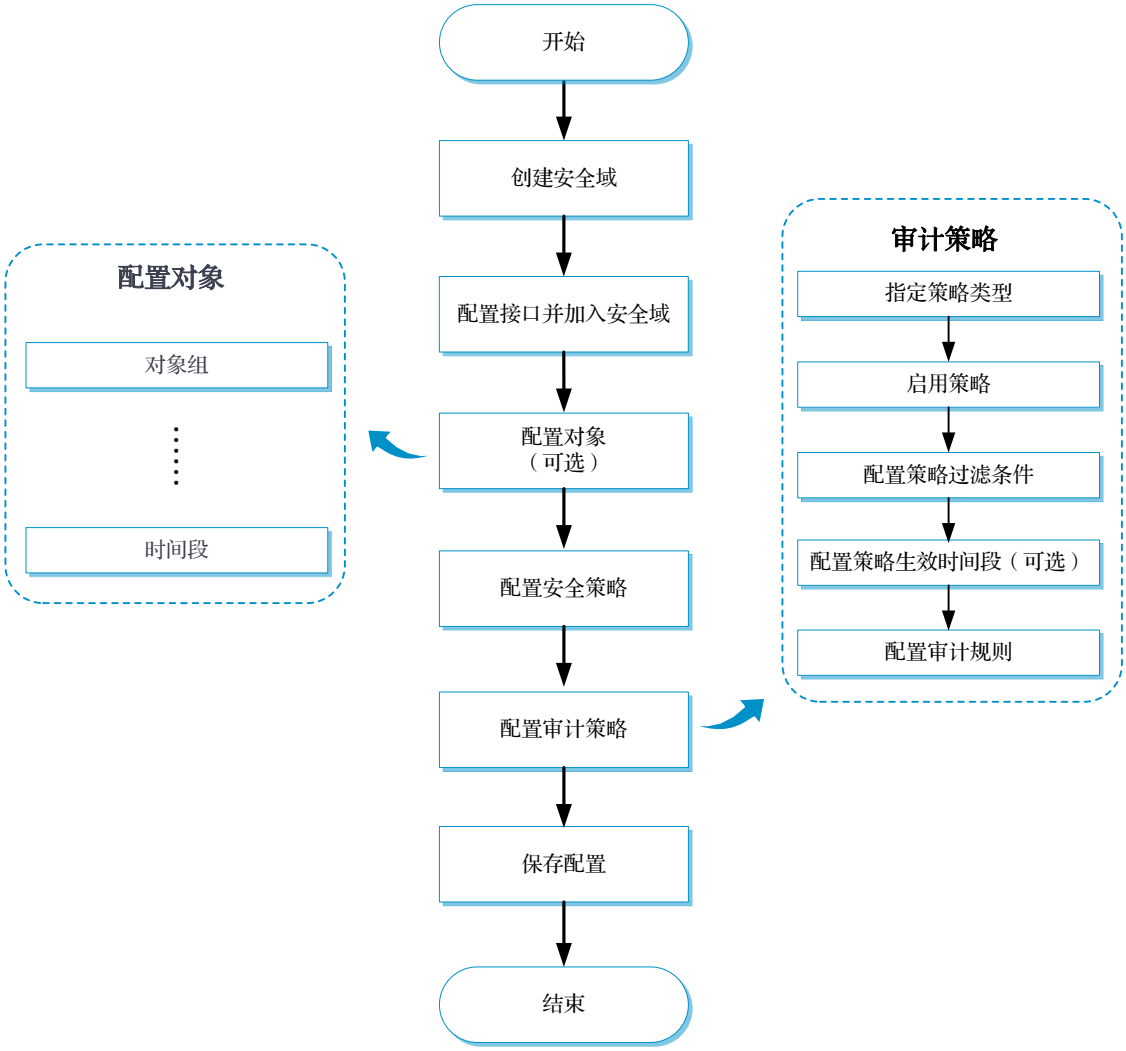
License支持情况

应用审计功能需要基于 APR（应用识别）特征库来进行识别。License 过期后，应用审计功能可以采用设备中已有的 APR 特征库正常工作，但无法升级特征库。关于 License 的详细介绍请参见“License 联机帮助”。

配置指南

应用审计功能的配置思路如下图所示：

图-2 应用审计配置指导图



在配置应用审计功能之前，需要先配置安全策略使流量可在设备上通过。有关安全策略的相关介绍请参见“安全策略联机帮助”。

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。
- 请购买并正确安装应用识别 License。
- 建议升级应用特征库到官网最新版本。

配置审计策略

配置审计策略的具体步骤如下：

1. 选择“策略 > 应用审计”，进入“应用审计”页面。
2. 在“应用审计”页面，单击<新建>按钮，进入“新建审计策略”页面，具体配置内容如下所示：

表-1 审计策略配置参数表

参数	说明
名称	配置审计策略的名称
类型	根据对报文审计需求选择对应的策略类型，类型包括审计、免审计和阻断
启用	选择开启后，此审计策略才能生效
源安全域	配置源安全域作为审计策略的过滤条件
目的安全域	配置目的安全域作为审计策略的过滤条件
源IP地址	配置源IP地址作为审计策略的过滤条件
目的IP地址	配置目的IP地址作为审计策略的过滤条件
服务	配置服务作为审计策略的过滤条件
用户	配置身份识别用户作为审计策略的过滤条件
应用	配置应用或应用组作为审计策略的过滤条件
时间段	配置审计策略生效的时间段

3. 在“新建审计策略”页面，单击审计规则处的<新建>按钮，进入“新建审计规则”页面，配置审计规则对某一应用的具体行为和行为内容进行精细化审计，此项仅审计类型的策略可配置。具体配置内容如下所示：

表-2 审计规则配置参数表

参数	说明
规则ID	审计规则的ID
应用	表示对指定的应用进行审计
行为	表示对应用的具体行为进行审计
行为内容	表示对行为的具体内容进行审计
匹配类型	表示行为内容的类型，包括如下取值： • 关键字：行为内容为字符串 • 数字：行为内容为数字
匹配关键字	表示审计规则与行为内容见的匹配方式，取值包括： • 关键字类型行为内容：包含、不包含、等于和不等于 • 数字类型行为内容：大于、小于、等于、大于等于、小于等于和不等于
邮件保护	表示邮件保护功能，包括限制邮件发送和防御邮件炸弹
限制邮件发送	开启本功能后，设备将限制用户向其他域名邮箱地址发送邮件
防御邮件炸弹	开启本功能后，设备防御收件人在短时间内收到同一发件人的大量邮件。需 如下： • 检测时间：表示邮件炸弹攻击的检测时长 • 邮件数量：表示检测时长内，同一收件人允许接收到的邮件数量的最大
动作	表示对与审计规则匹配成功的报文执行的动作，取值包括允许和阻断

日志	表示是否记录日志

4. 在“新建审计规则”页面，单击<确定>按钮，新建审计规则成功。
5. 在“新建审计策略”页面，单击<确定>按钮，新建审计策略成功，并会在“审计策略”页面中显示。

配置关键字组

配置关键字组具体步骤如下：

1. 选择“策略 > 应用审计”，进入“应用审计”页面。
2. 在“应用审计”页面，单击<关键字组>按钮，进入“关键字组”页面。
3. 单击<新建>按钮，进入“新建关键字组”页面，具体配置内容如下所示：

表-3 关键字组配置参数表

参数	说明
名称	关键字组的名称
描述	通过合理编写描述信息，便于管理员快速理解和识别本关键字组
关键字	配置需要审计的关键字信息，多个关键字之间用回车分隔

4. 在“新建关键字组”页面，单击<确定>按钮，新建关键字组成功，并会在“关键字组”页面中显示。

带宽管理

本帮助主要介绍以下内容：

- 特性简介
  - 带宽管理实现流程
  - 带宽策略匹配原则
  - 带宽通道
  - 带宽策略加速功能
  - IPv6 全数据流带宽管理功能
  - 源 NAT 带宽管理功能/目的 NAT 带宽管理功能
  - 实时流量趋势展示功能
- vSystem 相关说明
- 使用限制和注意事项
  - 配置父子策略使用限制和注意事项
  - 配置带宽通道使用限制和注意事项
  - 配置接口带宽使用限制和注意事项
  - 带宽策略管理使用限制和注意事项

- 配置指南
  - 配置思路
  - 配置准备
  - 单通道模式带宽管理
  - 父子通道模式带宽管理
  - 带宽告警功能

特性简介

带宽管理基于源/目的安全域、源/目的 IP 地址、用户、应用、服务、DSCP 优先级和时间段等过滤条件，对通过设备的流量进行精细化的管理和控制。

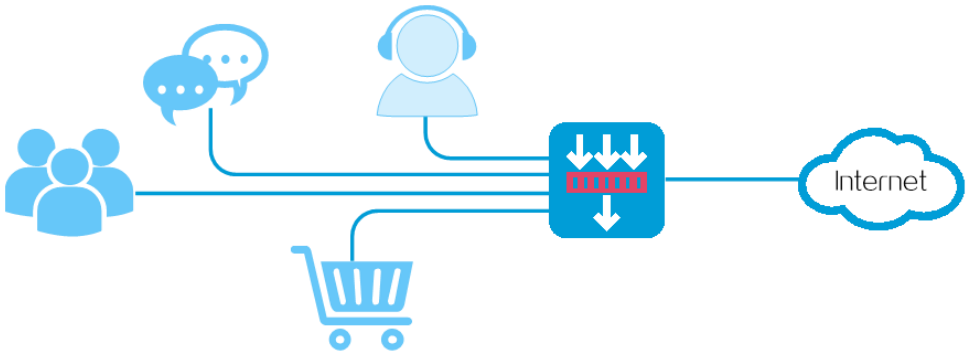
带宽管理的典型应用场景如下：

- 企业内网用户所需的带宽远大于从运营商租用的出口带宽，这时网络出口就会存在带宽瓶颈的问题。
- 网络出口中 P2P 业务类型的数据流量消耗了绝大部分的带宽资源，致使企业的关键业务得不到带宽保证。

为了解决以上问题，可以在网络出口设备上部署带宽管理，针对不同的内网业务流量应用不同的带宽策略，实现合理分配出口带宽和保证关键业务正常运行的目的。带宽管理技术的出现，可以有效

解决带宽资源浪费、关键业务受影响和网络性能下降等问题，提高网络出口带宽的利用率，保障关键业务的正常运行，提升整个企业内网的网络性能和用户体验。

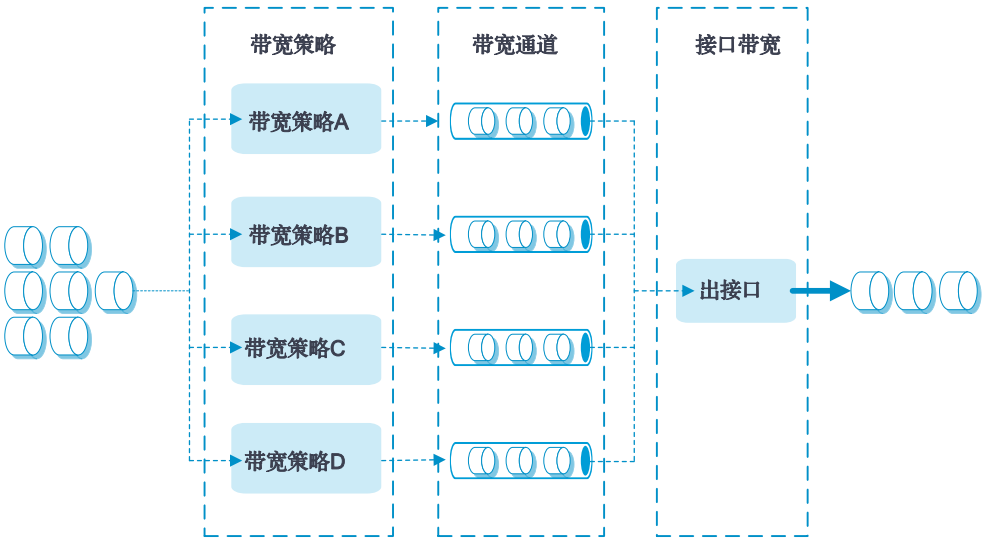
图-1 带宽资源示意图



带宽管理实现流程

带宽策略可以对符合匹配条件的流量应用带宽通道，在带宽通道中可以配置带宽保证和带宽限制功能，进而提高带宽利用率以及在线路拥堵时保证关键业务的正常运行。

图-2 带宽管理实现流程图



带宽管理实现流程如下：

1. 流量匹配上某个带宽策略后，如果此策略中引用了带宽通道，则流量继续进入相应的带宽通道进行后续的处理，否则设备不对该流量进行带宽管理。
2. 流量进入带宽通道后，设备会根据此带宽通道中配置的带宽限制策略对流量进行相应的处理。
3. 流量从出接口发送时受该接口带宽的限制。

带宽策略匹配原则

设备上可以配置多个带宽策略，这些策略用于定义匹配流量的匹配项以及流量控制的动作。不同策略之间的匹配顺序为：设备根据这些策略在设备上显示的顺序从上到下对流量进行匹配，一旦流量

匹配上某个策略便结束此匹配过程，并根据该策略中指定的带宽通道对此流量进行处理；若流量没有匹配上任何策略，则设备不对该流量进行带宽管理。

一个带宽策略中可以配置多种类型的匹配项，例如源/目的安全域、源/目的 IP 地址和用户等。一个策略被匹配成功的条件是：策略中已配置的所有匹配项必须均被匹配成功。

每个匹配项中可以配置多个条件，比如源 IP 地址中可以指定多个 IP 地址等，一个匹配项被匹配成功的条件是：某匹配项中的任何一个条件被匹配成功即可。

带宽策略支持嵌套关系，目前支持配置四级带宽策略。即一个策略中可以指定一个父策略，最多支持嵌套四级。流量与存在父策略的带宽策略匹配时，遵守如下原则：

- 首先匹配父策略，如果父策略匹配上了再匹配子策略。如果父策略没有匹配上，也不会进行后续的子策略匹配，该匹配过程失败。
- 如果子策略匹配上了，先按照子策略中的带宽通道配置对流量进行控制，再按照父策略中的带宽通道配置对流量进行控制，如果父子策略对同一个参数进行限制，则按照最严格的限制对流量进行控制。如果子策略没有匹配上但父策略匹配上了则按照父策略中的带宽通道配置对流量进行控制。

带宽通道

带宽通道定义了具体的带宽资源，是进行带宽管理的基础。通过带宽通道，可以将物理的带宽资源从逻辑上划分为多个虚拟的带宽通道，每个带宽通道中都可自定义带宽资源限制参数、流量优先级参数和带宽告警参数。目前，带宽通道中支持配置的参数如下表所示：

表-1 带宽通道参数说明表

参数	说明
限流方式	带宽通道中对流量的限制方式，包括如下两种： • 分别设置上下行带宽：对带宽通道中的上下行流量进行分别限制 • 设置总带宽：对带宽通道中的上下行流量进行整体限制
引用方式	带宽通道被带宽策略引用的方式，包括如下两种： • 策略独占：每一个引用某带宽通道的带宽策略都独自受到该带宽通道的约束 带宽策略匹配成功的流量，独享带宽通道中的带宽限制和连接数限制 • 策略共享：所有引用某带宽通道的带宽策略都共同受到该带宽通道的约束， 带宽策略匹配成功的多条流量，共享带宽通道中的带宽限制和连接数限制
整体的保证带宽	是指保证业务的最小带宽，在线路拥堵时，可以保证公司关键业务所需的带宽， 业务不受影响
整体的最大带宽	是指限制业务的最大带宽，比如限制网络中非关键业务占用的带宽资源，避免该 耗大量的带宽，影响其他关键业务的正常运行
IP间带宽分配策略	基于整体的最大带宽和在线的IP数量，为每一个IP动态的均分带宽，充分利用了 宽资源
每IP或每用户的保证带宽	设备除了支持配置整体的保证带宽之外，还支持基于IP地址和用户的保证带宽， 精细化的带宽管理
每IP或每用户的最大带宽	设备除了支持配置整体的最大带宽之外，还支持基于IP地址和用户的最大带宽， 精细化的带宽管理
连接数限制	带宽通道中的连接数限制策略可以对设备上建立的连接数进行统计和限制。带宽 连接数限制即可以基于带宽策略整体限制会话的最大连接数和最大新建连接速率 基于每IP、每用户限制会话的最大连接数和最大新建连接速率

每IP流量限额	设备支持基于IP地址，对每月总流量进行限制 配置本功能后，可到“每IP流量限额统计”页签查看流量统计值
月限额	每IP每月的流量使用上限值
转发优先级	当多个带宽通道中的流量同时从某个接口发送时，如果此接口发生阻塞，则优先 量优先被发送。优先级相同的流量将会自由竞争出接口的带宽资源
重标记DSCP优先级	是指修改报文中DSCP（Differentiated Services Code Point）字段的值，是网络 流量分类的依据。位于报文传输路径上的各个网络设备，可以通过DSCP优先级 量，进而对不同DSCP优先级的流量采取差异化的处理
TCP MSS	带宽通道的TCP最大报文段长度
带宽检测功能	开启本功能后，设备将基于源IP地址对经过设备的流量带宽进行实时检测
静态阈值	用户手工配置的固定带宽阈值，包括最大静态阈值和最小静态阈值 当设备检测到流量带宽阈值超过最大静态阈值或者低于最小静态阈值后，将以快 出的方式向用户的日志主机发送日志进行告警
动态阈值学习功能	在不了解网络正常流量大小的情况下，无法正确配置固定的带宽阈值上下限，可 本功能，让设备自动学习网络中流量的带宽，将学习到的带宽基线值结合最大最 得到带宽阈值上下限，该上下限的优先级高于静态阈值 可到“策略 > 带宽管理 > 带宽阈值学习”页面查看学习结果
学习时长	设备自动学习网络中流量带宽的时长。开启动态阈值学习功能后，系统会在学习 动统计流量的带宽值。建议学习时长设置大于1440分钟（24小时），以确保设备 整天的流量。如果在学习过程中修改了该值，系统将会以新的时长为准重新进行
学习容忍度	当设备通过动态阈值学习功能学习到带宽基线值后，可使用该值分别乘以最小和 度得到动态带宽阈值的上限和下限值 如果未配置最小容忍度，则表示对带宽的下限值不关心；如果未配置最大容忍度

	对带宽的上限值不关心。因此，最大和最小容忍度至少需要配置其中一个

带宽策略加速功能

为了提高报文对带宽策略的匹配速度，设备支持带宽策略加速功能。当设备上包含大量的带宽策略时，此功能可以实现报文对带宽策略的快速匹配。若带宽策略加速功能失败，变化后的带宽策略不生效，系统继续使用原来的带宽策略进行快速匹配。

激活带宽策略的加速功能包括如下方式：

- 手动激活：是指带宽策略发生变化后，单击<立即加速>按钮使这些策略立即加速。
- 自动激活：是指系统按照固定时间间隔进行周期性判断是否需要带宽策略加速，在一个时间间隔内若带宽策略发生变化，则间隔时间到达后会进行带宽策略加速，否则，不会进行加速。当带宽策略小于等于 100 条时，此时间间隔为 2 秒；当带宽策略大于 100 条时，此时间间隔为 20 秒。

IPv6 全数据流带宽管理功能

缺省情况下，带宽管理仅对四层协议为 TCP、UDP、ICMP 和 ICMPv6 协议的数据流生效。开启本功能后，对于 IPv4 流量无影响。对于 IPv6 流量，带宽管理功能对所有四层协议的数据流均生效。

在“带宽策略”页面功能按钮区，单击<高级设置>按钮，选择启用或禁用“IPv6 全数据流带宽管理功能”，可配置带宽管理功能管控数据流的范围。

源 NAT 带宽管理功能/目的 NAT 带宽管理功能

缺省情况下，带宽策略使用报文经过 NAT 源/目的地址转换前的 IP 地址、服务端口号及 VRF 匹配带宽策略过滤条件。

如果需要控制 NAT 源/目的地址转换后的 IP 地址的带宽，请在“带宽策略”页面功能按钮区，单击<高级设置>按钮，选择启用“源 NAT 带宽管理功能”/“目的 NAT 带宽管理功能”。

实时流量趋势展示功能

实时流量趋势展示功能用来对匹配带宽策略的流量使用情况进行统计，并使用折线图的形式向用户展示流量使用趋势。方便管理员识别流量的使用趋势，例如哪个时段会有更多的访问量，以及这些流量变化是否具备重复性，并基于流量情况进行精细化的管理和控制，有助于更好地分配带宽资源、管控用户的上网行为。

管理员可在“带宽策略”页面，单击实时监控栏下的“实时监控”按钮，查看不同带宽策略的实时流量趋势。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

配置父子策略使用限制和注意事项

- 子策略引用的带宽通道中的最大带宽不能大于父策略引用的带宽通道中的最大带宽。
- 父策略引用的带宽通道中的保证带宽不能小于子策略引用的带宽通道中的保证带宽。
- 子策略与父策略不能引用同一个带宽通道。
- 父子策略下，设备仅对子策略进行带宽检测以及动态阈值学习。
- 如果被复制的带宽策略中含有子带宽策略，则只会复制父带宽策略的内容。
- 只能在创建带宽策略时指定带宽策略的父策略，不能为已存在的带宽策略添加或修改父策略。
- 父子策略引用的带宽通道的限流方式必须一致。
- 父策略不支持 IP 动态均分带宽功能。

配置带宽通道使用限制和注意事项

- 在支持部署多块安全业务板的设备上，带宽通道中配置的相关阈值参数对报文的限制都是在每块安全业务板上独立计算的。在这种情况下，设备实际对报文的带宽限制结果会大于管理员配置的阈值。请管理员根据设备上部署的安全业务板数量和整机的目标带宽限制需求，合理配置带宽通道中的相关阈值参数以达到预期效果。例如，设备上部署了三块安全业务板，同时希望设备整体上行最大带宽为 30000kbps，这时需要在带宽通道中设置上行最大带宽为 10000kbps。
- 如果同时配置了接口的 TCP MSS，则以更小的 MSS 值为准。
- 如果要开启带宽检测功能，需要保证引用本带宽通道的带宽策略规则中配置了作为带宽策略规则过滤条件的 IP 地址或地址对象组，否则带宽检测功能不生效。
- 带宽策略规则中配置的 IP 地址或地址对象组不同，会有以下情况：
  - 带宽策略规则中配置了源 IP 地址或源 IP 地址对象组：设备根据源 IP 地址对流量进行检测。
  - 带宽策略规则中配置了目的 IP 地址或目的 IP 地址对象组：设备根据目的 IP 地址对流量进行检测。
  - 带宽策略规则中同时配置了源和目的 IP 地址（包含地址对象组）：设备根据源 IP 地址对流量进行检测。
- 如果报文同时匹配代理策略规则和带宽管理规则，则以接口下的 MSS 值为准。

配置接口带宽使用限制和注意事项

接口期望带宽的缺省值较小时，在流量较大的情况下，很容易出现丢包现象，这时可以将此接口的期望带宽值调大。比如 Tunnel 口的默认带宽是 64kbps，流量比较大的情况下，易出现丢包现象，这时可将 Tunnel 接口的期望带宽值调大。

带宽策略管理使用限制和注意事项

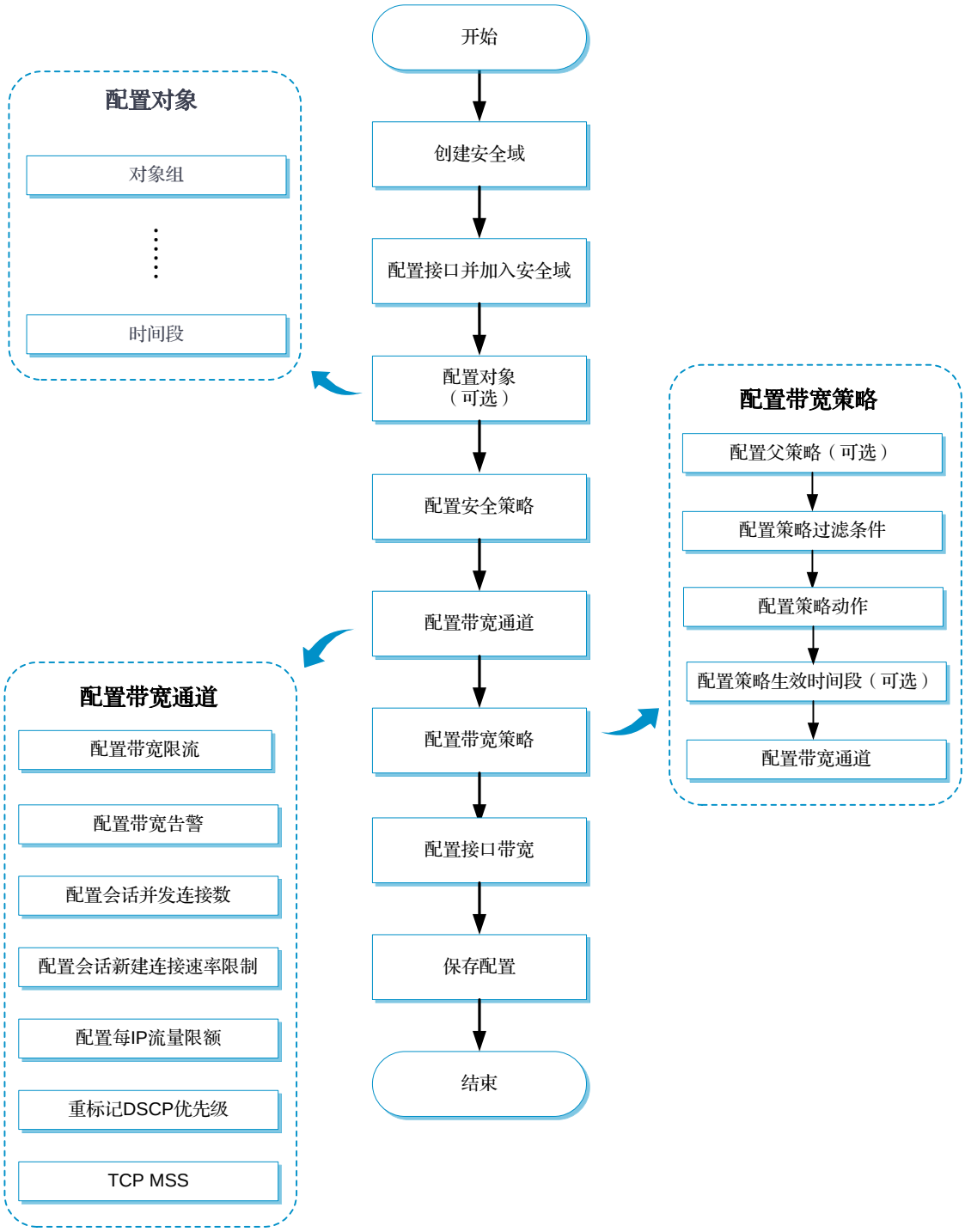
通过复制创建的新带宽策略紧跟在被复制的带宽策略之后。

配置指南

配置思路

带宽管理策略功能的配置思路如下图所示：

图-3 带宽管理策略配置指导图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

单通道模式带宽管理

对于流量分类较为简单的网络环境，管理员可通过单通道模式带宽管理配置对通道上的所有流量进行统一的带宽限制和优先级设置。

配置带宽通道

带宽通道是对网络中的带宽资源进行管理和调度的通道。通过创建带宽通道，可以对网络中的带宽资源进行限流、检测和引用等配置，从而实现对带宽资源的有效管理和调度。

配置带宽通道具体步骤如下：

1. 选择“策略 > 带宽管理 > 带宽通道”。
2. 在“带宽通道”页面单击<新建>按钮，进入“新建带宽通道”页面。
3. 配置带宽通道，具体配置内容如下表所示：

表-2 带宽通道配置参数表

参数	说明
名称	配置带宽通道的名称
限流方式	带宽通道中对流量的限制的方式，包括分别设置上下行带宽和设置总带宽两
整体带宽引用方式	带宽通道被带宽策略引用的方式，包括策略独占和策略共享两种
整体的最大上行带宽	配置带宽通道整体的最大上行带宽值
整体的保证上行带宽	配置带宽通道整体的保证上行带宽值
整体的最大下行带宽	配置带宽通道整体的最大下行带宽值
整体的保证下行带宽	配置带宽通道整体的保证下行带宽值
转发优先级	配置带宽通道中流量的转发优先级，数值越大优先级越高
IP间带宽分配策略	基于整体的最大带宽和在线的IP数量，为每一个IP动态的均分带宽，充分利宽资源
每IP的最大上行带宽	配置带宽通道中每IP的最大上行带宽值
每IP的最大下行带宽	配置带宽通道中每IP的最大下行带宽值
每用户的最大上行带宽	配置带宽通道中每用户的最大上行带宽值
每用户的最大下行带宽	配置带宽通道中每用户的最大下行带宽值
整体新建连接数	配置带宽通道中整体新建会话连接数的最大值

每IP/每用户连接数	配置带宽通道中每IP/用户新建会话连接数的最大值
整体新建连接速率	配置带宽通道中整体的最大新建会话连接速率值
每IP/每用户新建连接速率	配置带宽通道中每IP/用户的最大新建会话连接速率值
月限额	配置带宽通道中每个IP地址每月允许使用流量的最大值
重标记DSCP优先级	修改报文中DSCP（Differentiated Services Code Point）字段的值
TCP MSS	配置带宽通道的TCP最大报文段长度

4. 单击<确定>按钮，新建带宽通道成功，并会在带宽通道页面中显示。

配置带宽策略

带宽策略是针对不同业务流量进行匹配的规则。通过创建带宽策略，可以对不同业务流量进行过滤条件、动作、生效时间等配置，实现对不同业务流量的带宽管理。

配置带宽策略的具体步骤如下：

1. 选择“策略 > 带宽管理> 带宽策略”。
2. 在“带宽策略”页面单击<新建>按钮，进入“新建带宽策略”页面。
3. 新建带宽策略，具体配置内容如下表所示：

表-3 带宽策略配置参数表

参数	说明
名称	配置带宽策略的名称
源安全域	配置源安全域作为带宽策略的过滤条件
目的安全域	配置目的安全域作为带宽策略的过滤条件
源地址对象组	配置源IP地址对象组作为带宽策略的过滤条件
目的地址对象组	配置目的IP地址对象组作为带宽策略的过滤条件
源IP地址	配置源IP地址作为带宽策略的过滤条件
目的IP地址	配置目的IP地址作为带宽策略的过滤条件
用户	配置身份识别用户或用户组作为带宽策略的过滤条件
应用	配置应用或应用组作为带宽策略的过滤条件
服务	配置服务作为带宽策略的过滤条件
时间段	配置带宽策略生效的时间段
DSCP优先级	配置DSCP优先级作为带宽策略的过滤条件
IPv6报文头流标签	配置IPv6报文头流标签作为带宽策略的过滤条件
IPv6扩展报文头	配置IPv6扩展报文头作为带宽策略的过滤条件
终端	配置终端或终端组作为带宽策略的过滤条件

VRF	配置VPN实例作为带宽策略的过滤条件
动作	配置带宽策略执行的动作，取值包括： • 限流：通过引用带宽通道，对符合带宽策略过滤条件的报文进行限制 • 不限流：对符合带宽策略过滤条件的报文不进行限制 • 阻断：对符合带宽策略过滤条件的报文进行阻断
带宽通道	引用带宽通道对符合带宽策略过滤条件的报文进行带宽管理

4. 单击<确定>按钮，新建带宽策略成功，并会在带宽策略列表页面中显示。

5. 带宽策略配置变更之后如需立即生效，请单击<立即加速>按钮。

配置接口带宽

配置接口带宽的具体步骤如下：

1. 选择“策略 > 带宽管理> 接口带宽”。

2. 在“接口带宽”页面单击<新建>按钮，进入“新建接口带宽”页面。

3. 新建接口带宽，具体配置内容如下表所示：

表-4 接口带宽配置参数表

参数	说明
接口名称	选择需要带宽管理的接口

期望带宽	配置接口的最大期望带宽值

4. 单击<确定>按钮，新建接口带宽成功，并会在接口带宽页面中显示。

父子通道模式带宽管理

对于流量分类复杂且需要对特定应用、用户组或设备细分带宽的网络环境，管理员可通过父子通道模式带宽管理配置对流量进行精细化划分，保障各自的网络需求。

配置带宽通道

配置带宽通道的具体步骤请参见“配置带宽通道”章节。

配置带宽策略

配置带宽策略的具体步骤如下：

1. 配置带宽策略，具体配置内容请参见“配置带宽策略”章节。
2. 在“新建带宽策略”页面，配置带宽策略的父带宽策略。
3. 单击<确定>按钮，新建带宽策略成功，并会在带宽策略列表页面中显示。

配置接口带宽

配置接口带宽的具体步骤请参见“配置接口带宽”章节。

带宽告警功能

开启带宽告警功能后，设备可基于 IP 地址对进入带宽通道的流量进行实时的带宽阈值（包括最大值和最小值）检测。当带宽超过配置的阈值时，设备将以快速日志输出的方式向用户发送日志进行告警。

配置带宽通道

配置带宽通道具体步骤如下：

1. 配置带宽通道，具体配置内容请参见“配置带宽通道”章节。
2. 在“新建带宽通道”页面，配置带宽告警功能，具体配置内容如下所示：

表-5 带宽告警配置参数表

参数	说明
开启带宽检测功能	开启本功能后，设备基于每个IP地址对经过设备的流量带宽进行实时检测
最大静态阈值	用户手工配置的固定带宽阈值上限

最小静态阈值	用户手工配置的固定带宽阈值下限
开启动态阈值学习功能	开启本功能后，设备将自动学习网络中流量的带宽，并统计带宽基线值
学习时长	设备自动学习网络中流量带宽的时长
最大学习容忍度	当设备通过动态阈值学习功能学习到带宽基线值后，可使用基线值乘以最大 态带宽阈值的上限
最小学习容忍度	当设备通过动态阈值学习功能学习到带宽基线值后，可使用基线值乘以最小 态带宽阈值的下限

配置带宽策略

配置带宽策略的具体步骤请参见“配置带宽策略”章节。

配置接口带宽

配置接口带宽的具体步骤请参见“配置接口带宽”章节。

应用代理

本帮助主要介绍以下内容：

- 特性简介
  - 代理策略的过滤条件
  - 代理策略的匹配顺序
  - 代理策略的动作
  - 白名单
  - SSL 解密保护对象
  - SSL 证书
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置思路
  - 配置准备
  - 配置保护内网客户端的代理策略
  - 配置保护内网服务器的代理策略

- 配置 TCP 的代理策略
- 配置白名单

特性简介

应用代理功能支持 TCP 代理和 SSL 代理。用户可通过配置代理策略，配置不同的代理功能。

代理策略的过滤条件

代理策略中可同时配置多类过滤条件，具体包括：源安全域、目的安全域、源地址、目的地址、用户和服务。一类过滤条件可以配置多个匹配项，任何一个匹配项被匹配成功则认为该过滤条件匹配成功。一条策略被匹配成功的条件是：策略中已配置的所有过滤条件必须均被匹配成功。

代理策略的匹配顺序

设备上可以配置多个代理策略，设备缺省按照策略的创建顺序对报文进行匹配，先创建的先匹配。因此，首先需要将规划的所有策略按照“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）进行排序，然后按照此顺序配置每一个代理策略。

代理策略的动作

设备将根据代理策略中配置的动作对命中策略的流量进行如下处理：

- 代理策略的动作配置为TCP代理时，设备将对命中策略的流量进行TCP代理，为客户端和服务器端之间提供 TCP 层隔离，有效的拦截恶意连接和攻击。
- 代理策略的动作配置为 SSL 解密时，设备将对命中策略的流量进行 SSL 代理，并基于此对 SSL 流量进行解密，并对解密后的流量进行应用安全深度检测。此动作仅对基于 SSL 加密的协议生效，如 HTTPS、SMTPS 和 POP3S 等。
- 代理策略的动作配置为不代理时，设备将对命中策略的流量进行透传。

白名单

白名单的支持情况与设备型号有关，请以页面的实际显示为准。

当用户不需要或者不能以代理的方式访问某些服务器时，可以将这些服务器域名加入自定义白名单。设备将对匹配白名单的所有连接直接透传。

设备支持预定义白名单和自定义白名单。

预定义白名单

设备预置的白名单，包含如下类型：

- Chrome-HSTS 类型：表示 Chrome 浏览器强制使用 HTTPS 方式访问的域名。当关闭 Chrome-HSTS 全局白名单后，将禁用所有 Chrome-HSTS 类型白名单；当开启 Chrome-HSTS 全局白名单后，可单独启用或禁用指定的 Chrome-HSTS 类型白名单。
- 其他类型：除 Chrome-HSTS 类型之外的白名单。

自定义白名单

用户手动添加的需要透传连接的服务器域名。

设备使用用户配置的服务器域名字符串与 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，只要含有指定字符串的域名均会匹配成功。匹配成功后，则透传该连接。

SSL 解密保护对象

SSL 解密功能支持如下类型：

- 保护内网客户端：用于保护内网客户端的场景，可与 DPI 深度安全功能配合使用。设备解密报文后再对报文进行 DPI 深度安全业务的检测，防止内网客户端受到外部恶意网站的攻击。在此场景下，设备需要使用代理服务器证书与客户端进行 SSL 协商。
- 保护内网服务器：用于保护内网服务器的场景，可与 DPI 深度安全功能配合使用。设备解密报文后再对报文进行 DPI 深度安全业务的检测，防止外部恶意流量对内网服务器进行攻击。在此场景下，设备需要使用导入的内网服务器证书与客户端进行 SSL 协商。

请务必根据不同的使用场景正确配置 SSL 解密功能的保护对象，并配置相应类型的证书与客户端进行 SSL 协商。

SSL 证书

SSL 解密功能的保护对象不同，需要配置相应类型的证书与客户端进行 SSL 协商。

SSL 解密证书

在保护内网客户端的场景下，设备作为 SSL 代理服务器时，需要向客户端发送证书表明自身的身份。但设备并不是直接将客户端访问的服务器的证书发送给客户端，也不是简单地将自己的证书发送给客户端。而是根据客户端访问的服务器证书的内容，使用导入的 SSL 解密证书重新签发一本新的“服务器证书”发送给客户端。

用户导入 SSL 解密证书时，需要为其标识为可信或者不可信，用于签发不同可信度的新的“服务器证书“。

- 可信：表示客户端信任的证书。
- 不可信：表示客户端不信任的证书。

设备将使用 PKI 域中的 CA 证书替客户端验证服务器是否可信，验证结果不同，设备使用不同标识的 SSL 解密证书。当服务器不可信时，设备将使用标识为“不可信”的 SSL 解密证书签发一个新的“服务器证书”给客户端，由客户端决定是否继续访问不可信的服务器；当服务器可信时，设备

将使用标识为“可信”的 SSL 解密证书签发一个新的“服务器证书”发送给客户端。有关 PKI 域的详细介绍，请参见“PKI”。

内部服务器证书

在 SSL 代理保护内网服务器的场景下，需要用户导入受保护的内网服务器证书。导入证书后，设备将对证书进行解析，并生成一个 CER 格式的证书文件和一个密钥文件。CER 证书用于校验服务器身份，密钥文件用于后续 SSL 代理过程中加解密报文。设备将计算 CER 证书文件的 MD5 值，并将 MD5 值作为证书的唯一标识。

在 SSL 代理过程中，设备收到服务器发来的证书后，会先计算证书的 MD5 值，并与已导入的内网服务器证书的 MD5 值进行匹配。如果 MD5 值相同，则认为该证书可信，并使用导入的内网服务器证书与客户端进行 SSL 协商；如果 MD5 值不同，则认为证书不可信，不进行 SSL 代理。

用户可导入多个内网服务器证书，若导入证书的 MD5 值已存在，则覆盖 MD5 值相同的已有证书。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

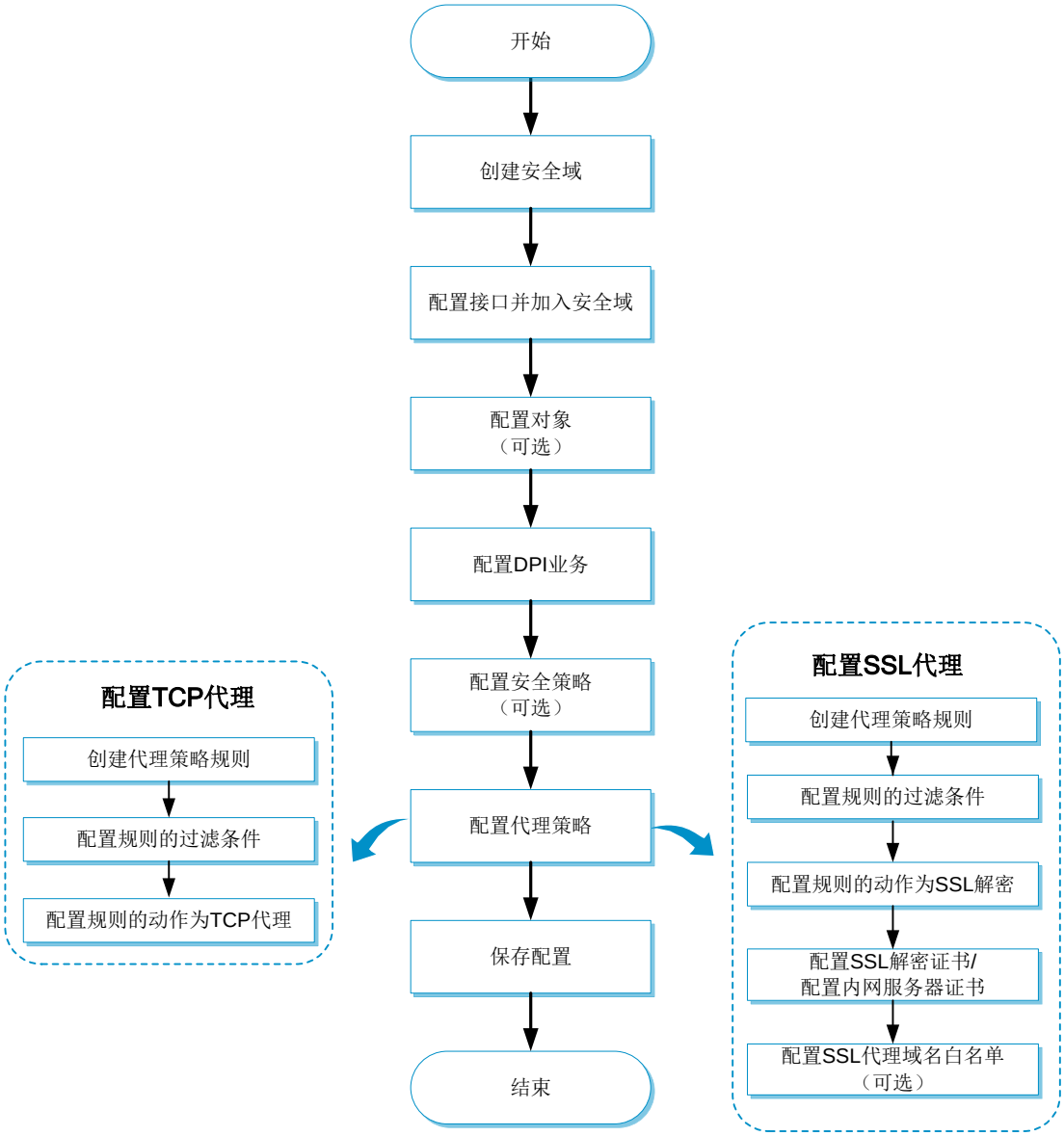
- TCP 代理与 SSL 代理对设备的转发性能会产生较大的影响，请根据实际情况判断是否需要开启上述功能。
- 配置代理策略时，请尽量细化策略的过滤条件，避免配置过滤条件宽泛的代理策略，影响设备的正常转发。
- 需要在客户端浏览器上安装并信任 SSL 解密证书。防止设备启用 SSL 解密功能后，客户端通过浏览器访问 HTTPS 类网站时，会弹出服务器证书不是由受信任机构颁发的告警信息，甚至有些应用程序不提示告警信息就直接中断了连接，影响用户的正常使用。
- 默认情况下，火狐浏览器不共享系统中的证书库，如果已经在其他浏览器上导入 SSL 解密证书，则可以通过修改火狐浏览器中的高级设置，使其共享系统中的证书库，不再单独导入证书，具体操作步骤：在地址栏中输入：about:config，搜索框中输入：security.enterprise_roots.enabled，双击选中的条目，或者单击鼠标右键，选择切换，修改其值为 true。
- 开启 SSL 代理后，入侵防御功能的抓包动作将失效。
- 在非对称组网环境（即报文来回路径不一致）下，TCP 代理与 SSL 代理功能将失效。
- 设备不支持对 HTTP 2.0 版本协议流量进行 SSL 代理。开启 SSL 代理功能后，如果服务器仅支持 HTTP 2.0 版本协议，则会导致客户端无法访问服务器。

配置指南

配置思路

应用代理功能的配置思路如下图所示：

图-1 应用代理功能配置指导图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置保护内网客户端的代理策略

为了防止内网客户端受到外部恶意网站的攻击，在这种情况下，可以配置设备使用代理服务器证书与客户端进行 SSL 协商（即 SSL 解密防护类型是 client）。

配置 SSL 解密证书

SSL 解密证书的具体配置步骤如下：

1. 选择“策略 > 应用代理 > SSL 解密证书”，进入 SSL 解密证书页面。
2. 单击<导入>按钮，进入导入 SSL 解密证书页面，具体配置内容如下：

表-1 导入 SSL 解密参数表

参数	说明
证书文件	SSL解密证书文件

密码	SSL解密证书密码
证书标记	证书标记为可信或者不可信

3. 单击<确认>按钮，完成 SSL 解密证书的导入。

配置代理策略

代理策略的具体配置步骤如下：

1. 选择“策略 > 应用代理 > 代理策略”。
2. 在“代理策略”页面单击<新建>按钮，进入“新建代理策略”页面，具体配置内容如下表所示：

表-2 代理策略配置参数表

参数	说明
策略名称	表示代理策略的名称
源安全域	配置源安全域作为代理策略的过滤条件
目的安全域	配置目的安全域作为代理策略的过滤条件
源地址	配置源地址作为代理策略的过滤条件
目的地址	配置目的地址作为代理策略的过滤条件

用户	配置身份识别用户作为代理策略的过滤条件
服务	配置服务作为代理策略的过滤条件
动作	代理策略动作包括如下： • 不代理：表示对符合代理策略过滤条件的报文进行透传 • TCP 代理：表示对符合代理策略过滤条件的报文进行 TCP 代理 • SSL 解密：表示对符合代理策略过滤条件的报文进行 SSL 代理，并基于此对 S 密，并对解密后的流量进行应用安全深度检测
解密业务类型	类型包括如下： • 保护内网客户端：表示 SSL 解密功能用于保护内网客户端的场景 • 保护内网服务器：表示 SSL 解密功能用户保护内网服务器的场景 本功能仅在动作为SSL解密时配置
启用策略	选择开启后，此代理策略才能生效

3. 单击<确定>按钮，新建代理策略成功，并会在代理策略页面中显示。

配置保护内网服务器的代理策略

为了防止内网服务器受到外部恶意流量的攻击，在这种情况下，可以配置设备使用内网服务器证书与客户端进行 SSL 协商（即 SSL 解密防护类型是 server）。

配置内部服务器证书

内部服务器证书的具体配置步骤如下：

1. 选择“策略 > 应用代理 > 内部服务器证书”，进入内部服务器证书页面。

2. 单击<导入>按钮，进入导入内部服务器证书页面，具体配置内容如下：

表-3 导入内部服务器参数表

参数	说明
证书文件	内部服务器证书文件
密码	内部服务器证书密码

3. 单击<确认>按钮，完成内部服务器证书的导入。

配置代理策略

在“策略 > 应用代理 > 代理策略”页面中单击<新建>按钮，进入“新建代理策略”页面，动作选择保护内网服务器。新建代理策略的具体参数解释请参见“配置保护内网客户端的代理策略”中的配置代理策略。

配置 TCP 的代理策略

设备作为 TCP 代理，分别与客户端和服务器之间建立 TCP 连接，为客户端和服务器之间提供 TCP 层隔离，有效地拦截恶意连接和攻击。

1. 选择“策略 > 应用代理 > 代理策略”。
2. 在“代理策略”页面单击<新建>按钮，进入“新建代理策略”页面，具体配置内容如下表所示：

表-4 代理策略配置参数表

参数	说明
策略名称	表示代理策略的名称
源安全域	配置源安全域作为代理策略的过滤条件
目的安全域	配置目的安全域作为代理策略的过滤条件
源地址	配置源地址作为代理策略的过滤条件
目的地址	配置目的地址作为代理策略的过滤条件
用户	配置身份识别用户作为代理策略的过滤条件
服务	配置服务作为代理策略的过滤条件
动作	代理策略动作包括如下：

	• 不代理：表示对符合代理策略过滤条件的报文进行透传 • TCP 代理：表示对符合代理策略过滤条件的报文进行 TCP 代理 • SSL 解密：表示对符合代理策略过滤条件的报文进行 SSL 代理，并基于此对 S 密，并对解密后的流量进行应用安全深度检测
解密业务类型	类型包括如下： • 保护内网客户端：表示 SSL 解密功能用于保护内网客户端的场景 • 保护内网服务器：表示 SSL 解密功能用户保护内网服务器的场景 本功能仅在动作为SSL解密时配置
启用策略	选择开启后，此代理策略才能生效

3. 单击<确定>按钮，新建 TCP 代理策略成功，并会在代理策略页面中显示。

配置白名单

新建自定义白名单

新建自定义白名单的具体配置步骤如下：

1. 选择“策略 > 应用代理 > 自定义白名单”，进入自定义白名单页面。
2. 单击<新建>按钮，进入“新建自定义白名单表项”页面。
3. 配置白名单名称。单击<确认>按钮，完成自定义白名单的配置。

4. 单击<提交>按钮，使新建的自定义白名单生效。

启用预定义白名单

启用预定义白名单的具体配置步骤如下：

1. 选择“策略 > 应用代理 > 预定义白名单”，进入预定义白名单页面。
2. 如果启用 Chrome-HSTS 类型的白名单，需要先单击<开启 Chrome-HSTS 全局白名单>按钮，再勾选指定白名单右侧的“启用“复选框。
3. 如果启用其他类型的白名单，则直接勾选指定白名单右侧的“启用“复选框。
4. 单击<提交>按钮，使预定义白名单生效。

物联网设备安全管理

本帮助主要介绍以下内容：

- 特性简介
  - 标准格式检查
  - 设备准入控制
  - 敏感信令控制
  - 标准流量管控
- vSystem 相关说明
- License 支持情况
- 使用限制和注意事项
- 配置指南
  - 配置准备
  - 配置标准格式检查
  - 配置设备准入控制
  - 配置敏感信令控制
  - 配置标准流量管控

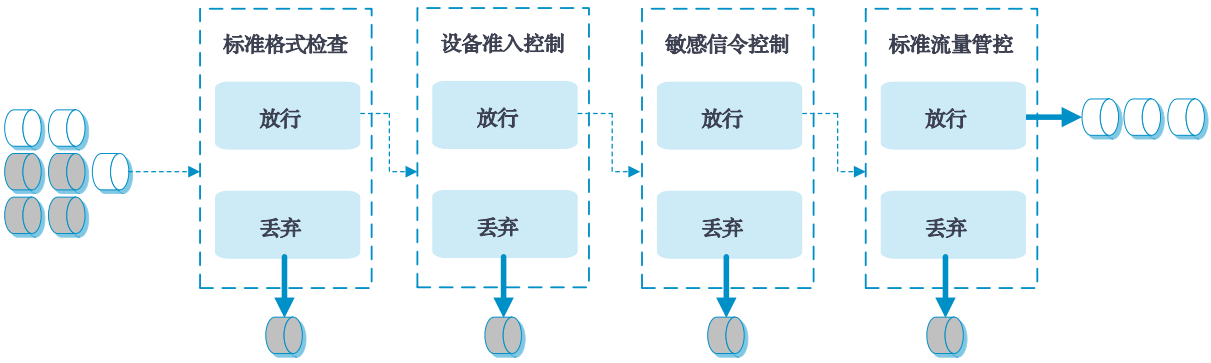
特性简介

物联网（IoT）是数字转型时代最重要的技术之一，意在将一切都连接到互联网。相较于传统的互联网，物联网连接的设备种类繁多、数量巨大、作用范围广，很多设备都处于偏僻无人看管的状态。因此它们面临的危险和漏洞也随之增加。例如视频安全系统中很多的终端摄像机都是处在偏僻角落监控周围环境。

物联网设备安全管理是一种针对物联网设备进行智能检测、安全管理的技术，主要功能包括：标准格式检查、设备准入控制、敏感信令控制、标准流量管控。

如果设备同时配置了标准格式检查、设备准入控制、敏感信令控制和标准流量管控中的多个功能，设备会按照上述出现顺序依次对报文进行处理，直到报文被丢弃。

图-1 各功能处理顺序图



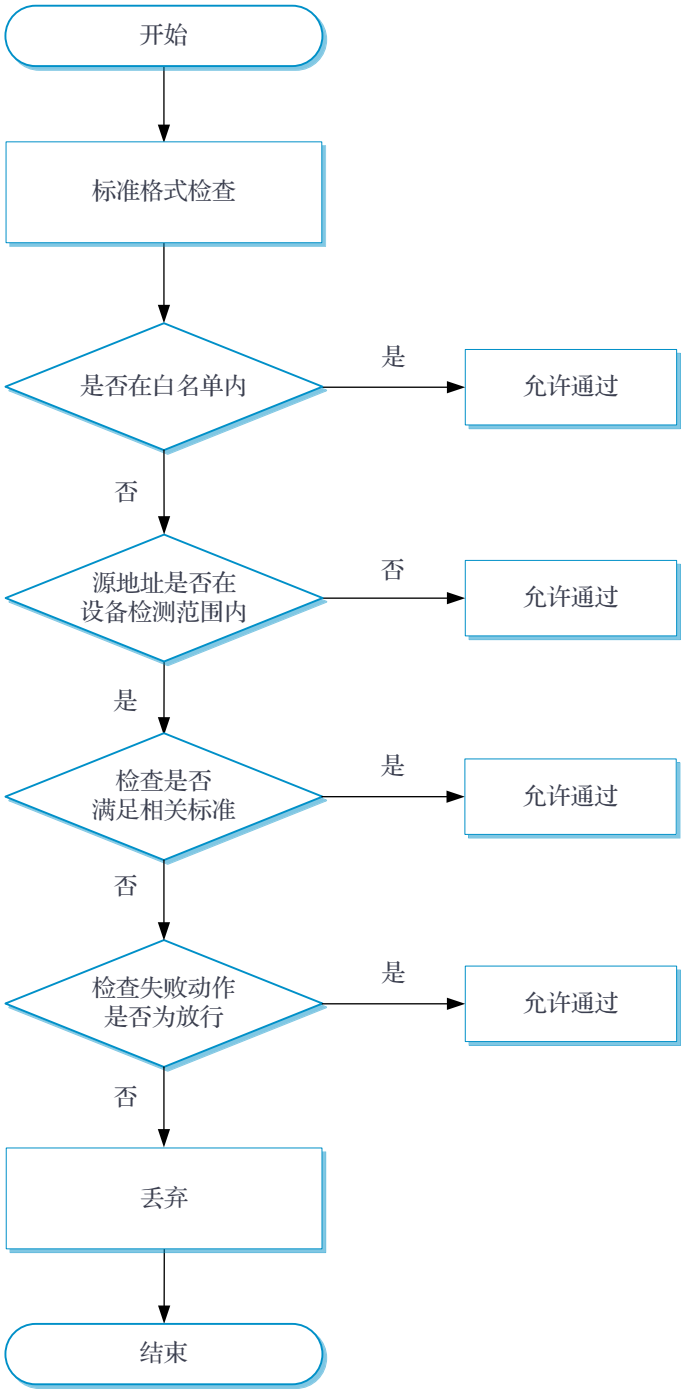
标准格式检查

标准格式检查功能可以根据不同的物联网设备标准，对物联网设备流量进行检查，确定流量是否符合相关物联网标准。此功能可以有效的避免非标准设备的接入。

标准格式检查实现流程如下：

1. 对于流经设备的物联网相关流量，设备会判断它的源地址是否在白名单之内，在白名单内的流量将会直接放行。
2. 对于不在白名单内的流量，设备会根据它的源地址来判断是否需要进行格式检查。不需要进行格式检查的流量将会直接放行。可以分别配置 IPv4、IPv6、MAC 源地址对象组作为匹配报文源地址的过滤条件。相同类型的地址对象组只能存在一个。不同类型的地址对象组之间是“或”的关系，即只要有一个对象组匹配就算匹配成功。
3. 如果需要进行格式检查，设备会根据管理员配置的行政区域属性、设备编码、物联网设备类型、接口方法等检测属性来判断流量是否满足相关的物联网标准，所有检测属性都满足标准的流量会直接放行。
4. 对于不满足标准的流量，设备会根据管理员配置的动作将其丢弃或者放行。

图-2 标准格式检查数据处理流程图



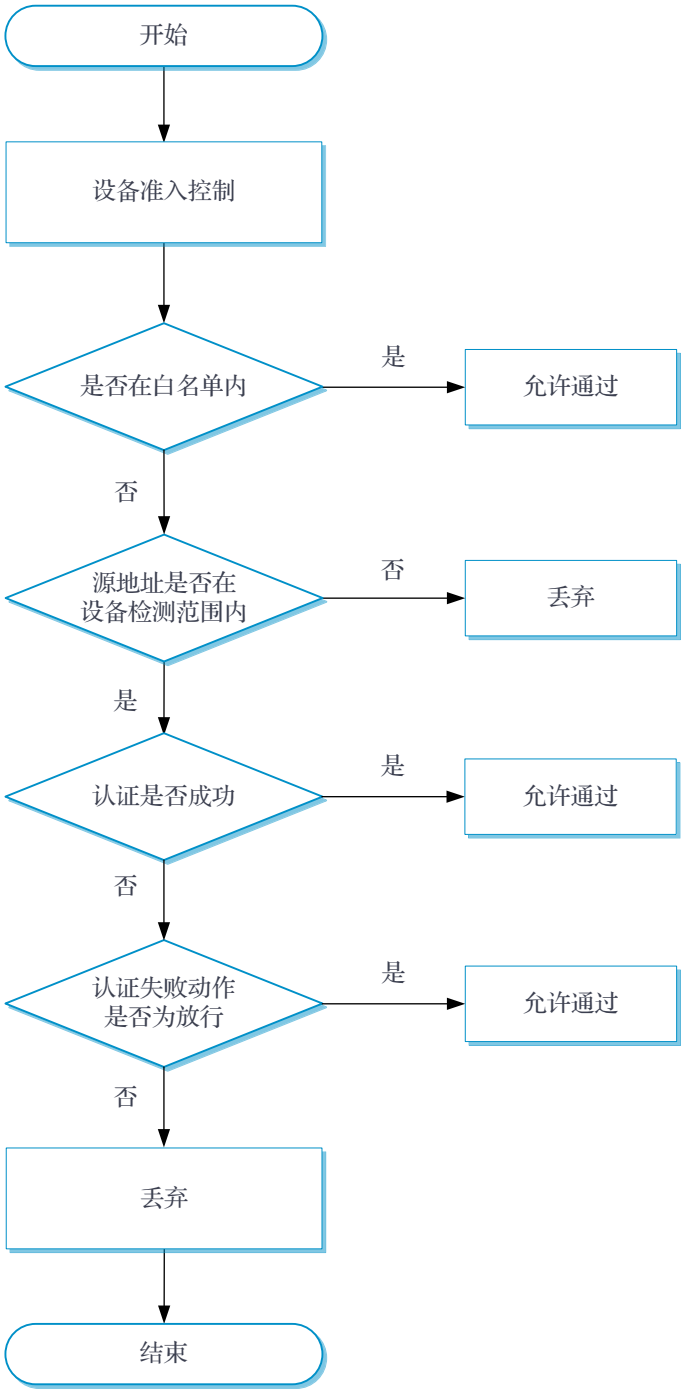
设备准入控制

设备准入控制功能可以根据不同的物联网设备标准以及管理员配置的设备信息对物联网设备流量进行检查，从而达到只有允许的物联网设备发出的流量才能通行的目的。此功能可以有效地避免设备被篡改的情况。

设备准入控制实现流程如下：

1. 对于流经设备的全部流量，设备会判断它的源地址是否在白名单之内，在白名单内的流量将会直接放行。
2. 对于不在白名单内的流量，设备会根据它的源地址来判断是否需要进行设备准入控制。不需要进行设备准入控制的流量将会直接丢弃。可以分别配置 IPv4、IPv6、MAC 源地址对象组作为匹配报文源地址的过滤条件。相同类型的地址对象组只能存在一个。不同类型的地址对象组之间是“或”的关系，即只要有一个对象组匹配就算匹配成功。
3. 如果需要进行设备准入控制，设备会根据管理员配置的 IP 地址、MAC 地址、设备编码、标准等设备认证信息来判断流量是否可以在设备上转发，满足所有认证信息的流量会直接放行。
4. 对于不满足认证信息的流量，设备会根据管理员配置的动作将其丢弃或者放行。

图-3 设备准入控制数据处理流程图



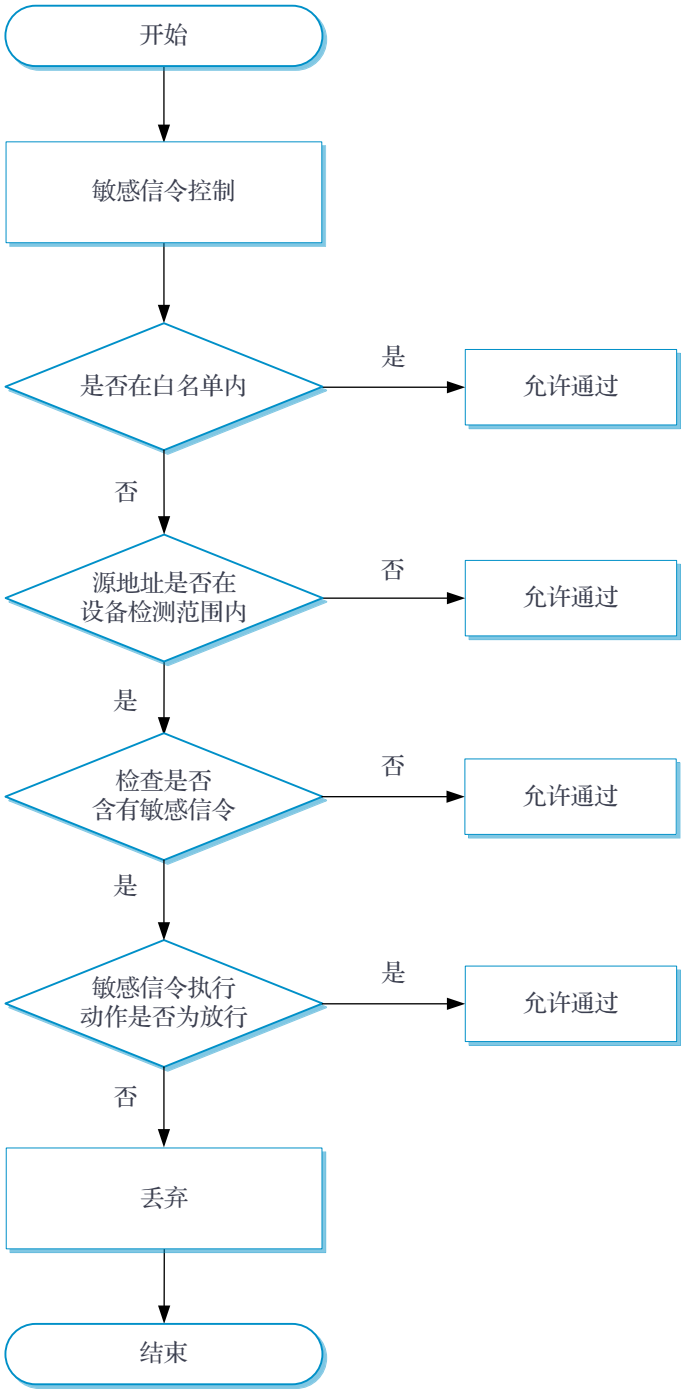
敏感信令控制

敏感信令控制功能可以根据不同的物联网设备标准，对物联网设备流量进行敏感信令识别，通过将流量信息与管理员配置的敏感信令进行匹配，实现对相关敏感信令过滤的功能。此功能可以查询出物联网设备流量中的查询、准入、控制等敏感行为，从而有效的避免数据泄露和数据篡改。

敏感信令控制实现流程如下：

1. 对于流经设备的物联网相关流量，设备会判断它的源地址是否在白名单之内，在白名单内的流量将会直接放行。
2. 对于不在白名单内的流量，设备会根据它的源地址来判断是否需要进行敏感信令控制。不需要进行敏感信令控制的流量将会直接放行。可以分别配置 IPv4、IPv6、MAC 源地址对象组作为匹配报文源地址的过滤条件。相同类型的地址对象组只能存在一个。不同类型的地址对象组之间是“或”的关系，即只要有一个对象组匹配就算匹配成功。
3. 如果需要进行敏感信令控制，设备会检查流量中是否含有用户指定的敏感信令，不含有敏感信令的流量会直接放行。
4. 对于含有敏感信令的流量，设备会根据管理员配置的动作将其丢弃或者放行。

图-4 敏感信令控制数据处理流程图



标准流量管控

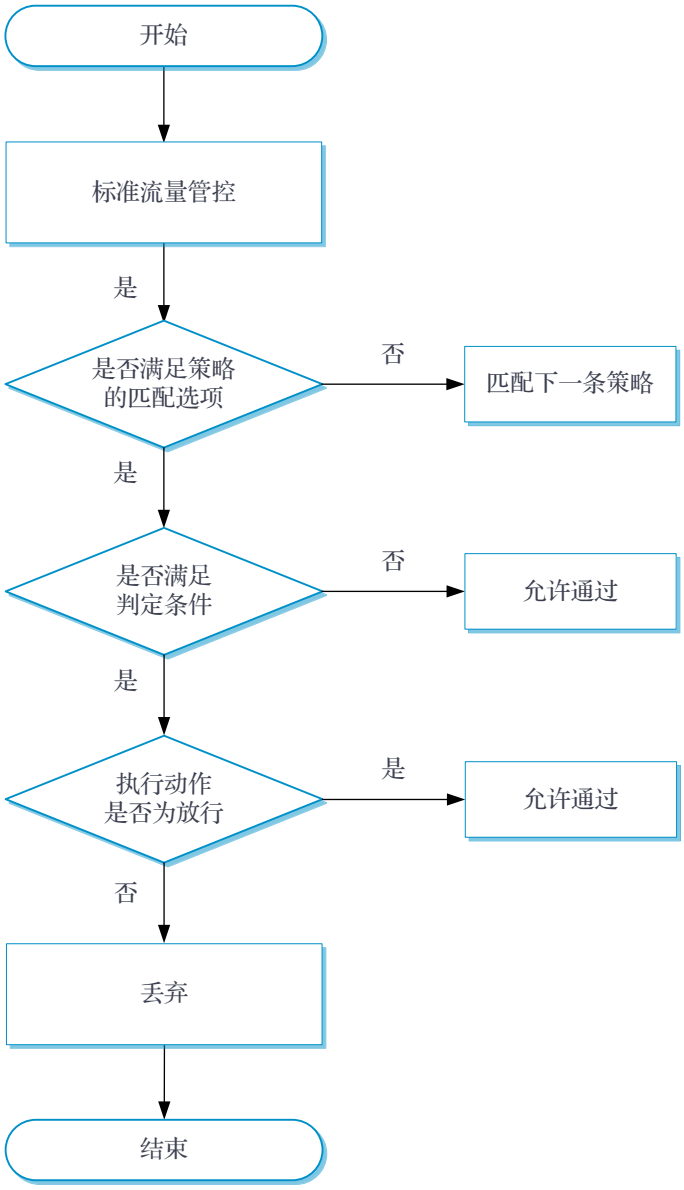
标准流量管控功能可以根据不同的标准流量管控策略，对物联网设备流量进行检测，通过将单一设备编码的请求发生次数、频率等信息与管理员设置的阈值进行比较，实现对请求方设备进行流量管控的功能。此功能可以有效的避免拒绝服务攻击。

对于流经设备的物联网相关流量，设备会根据标准流量管控策略在设备上显示的顺序从上到下对流量进行匹配。一旦匹配上某个标准流量管控策略便结束此匹配过程，并根据该策略中指定的动作对此流量进行处理；如果流量没有匹配上任何策略，则允许该流量通过。

标准流量管控实现流程如下：

1. 对于流经设备的物联网相关流量，设备会根据管理员配置的标准流量管控策略中的请求方设备编码、IP 地址、MAC 地址、物联网相关标准等匹配选项来判断是否需要进行标准流量管控。
2. 如果报文与某条标准流量管控策略中所有种类的过滤条件都匹配成功(其中地址对象组为一类过滤条件，不同类型的地址对象组之间是“或”的关系，即只要有一个对象组成功匹配就算符合过滤条件），则报文与此条标准流量管控策略匹配成功。若有一类过滤条件不匹配，则报文与此条标准流量管控策略匹配失败，报文继续匹配下一条标准流量管控策略。以此类推，直到最后一条标准流量管控策略，若报文还未与规则匹配成功，则不对流量进行标准流量管控。
3. 如果需要进行标准流量管控，设备会根据用户配置的单设备发出请求次数和单设备发出请求频率等判定条件来判断流量是否需要执行管理员配置的标准流量管控策略的执行动作。对于未达到判定条件阈值的流量，设备会直接放行。
4. 对于达到判定条件阈值的流量，设备会根据管理员配置的动作将其丢弃或者放行。

图-5 标准流量管控数据处理流程图



vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

License支持情况

敏感信令控制功能需要基于应用识别（APR）特征库来进行识别。License 过期后，敏感信令控制功能可以采用设备中已有的 APR 特征库正常工作，但无法升级特征库。关于 License 的详细介绍请参见“License 联机帮助”。

使用限制和注意事项

- 仅支持对采用 GB/T 28181、GB 35114、GA/T 1400 标准的物联网设备进行智能检测和管理。
- 设备准入控制功能会将不满足过滤条件的所有流量进行阻断，包括不属于 GBT28181、GB35114、GAT1400 标准的流量，因此建议用户在不需要时关闭该功能。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。

- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置标准格式检查

标准格式检查功能可以根据不同的物联网设备标准，对物联网设备流量进行检查，确定流量是否符合相关物联网标准。此功能可以有效的避免非标准设备的接入。具体配置步骤如下：

1. 配置全局白名单
   a. 选择“策略 > 物联网设备安全管理 > 标准格式检查”。
   b. 在“标准格式检查”页面可配置全局白名单，当管理员对物联网接入设备非常信任或发现格式检查存在误报的情况时，可以将选中的地址对象组加入到白名单以提高设备处理效率或减少误报。
2. 配置不同标准的标准格式检查功能，当前仅支持检查 GB/T 28181、GB 35114、GA/T 1400 标准。
   a. 选择“策略 > 物联网设备安全管理 > 标准格式检查”。
   b. 在“标准格式检查”页面可配置不同标准的格式检查功能。具体配置内容如下所示：

表-1 标准格式检查功能配置参数表

参数		说明
标准	GB/T 28181	开启指定标准的格式检查功能
	GB 35114	
	GA/T 1400	
日志告警		开启日志告警功能，当格式检查失败时发送日志
执行动作		当格式检查失败时设备对报文的执行动作，会有以下两种情况： • 正常放行 • 丢弃非法报文
检测属性		配置设备进行标准格式检查时的检测属性，只有设备对所有选中的 才认为格式检查成功
设备检测范围		配置作为设备检测范围的源地址对象组，不同类型的地址对象组之 只要有一个对象组成功匹配就算符合过滤条件，设备就会对报文进 行源地址不在检测对象组之内的报文

3. 单击<应用>按钮，指定标准的格式检查功能配置成功。

配置设备准入控制

设备准入控制功能可以根据不同的物联网设备标准以及管理员配置的设备信息对物联网设备流量进行检查，从而达到只有允许的物联网设备发出的流量才能通行的目的。此功能可以有效地避免设备被篡改的情况。具体配置步骤如下：

1. 选择“策略 > 物联网设备安全管理 > 设备准入控制”。

2. 在“设备准入控制”页面可配置详细的设备准入控制功能。具体配置内容如下所示：

表-2 设备准入控制功能配置参数表

参数	说明
设备准入控制	开启设备准入控制功能
全局白名单	当管理员对物联网接入设备非常信任或发现设备准入控制存在误报的情况时 的地址对象组加入到白名单以提高设备处理效率或减少误报
设备检测范围	配置作为设备检测范围的源地址对象组，不同类型的地址对象组之间是“或 只要有一个对象组成功匹配就算符合过滤条件，设备就会对报文进行检测。 断源地址不在设备检测范围之内的报文
设备认证信息	表示用于认证的物联网设备的信息，例如设备地址、设备编码、设备所使用 当报文中采集到的物联网设备信息与设备认证信息一致时设备将会直接放行 设备认证信息较多，可通过<导入>按钮批量导入设备认证信息 管理员通过物联网相关的管理平台修改物联网设备本身的设备编码、使用的 息时，由于该物联网设备之前已经认证成功，因此可能会出现认证不准确的 理员可以通过<重认证>按钮对已经配置的物联网设备进行重认证操作，按照

	对报文进行处理
设备检测时间	当报文中采集到的物联网设备信息不完整时，设备将无法对接入的设备完 时设备会在检测时间范围内持续采集每个报文中的物联网设备信息进行认
认证失败动作	当认证失败时设备对报文的执行动作，会有以下两种情况： • 正常放行 • 阻断设备流量
日志告警	开启日志告警功能，当设备认证失败时发送日志

3. 单击<应用>按钮，设备准入控制功能配置成功。

配置敏感信令控制

敏感信令控制功能可以根据不同的物联网设备标准，对物联网设备流量进行敏感信令识别，通过将流量信息与管理员配置的敏感信令进行匹配，实现对相关敏感信令过滤的功能。此功能可以查询出物联网设备流量中的查询、准入、控制等敏感行为，从而有效的避免数据泄露和数据篡改。具体配置步骤如下：

1. 配置全局白名单

   a. 选择“策略 > 物联网设备安全管理 > 敏感信令控制”。

b. 在“敏感信令控制”页面可配置全局白名单，当管理员对物联网接入设备非常信任或发现敏感信令控制存在误报的情况时，可以将选中的地址对象组加入到白名单以提高设备处理效率或减少误报。

2. 配置不同标准的敏感信令控制功能，当前仅支持检查 GB/T 28181、GB 35114、GA/T 1400 标准。

a. 选择 “策略 > 物联网设备安全管理 > 敏感信令控制” 。

b. 在 “敏感信令控制” 页面可配置不同标准的敏感信令控制功能。具体配置内容如下所示：

表-3 敏感信令控制功能配置参数表

参数		说明
标准	GB/T 28181	开启指定标准的敏感信令控制功能
	GB 35114	
	GA/T 1400	
日志告警		开启日志告警功能，当检测到敏感信令时发送日志
执行动作		当检测到敏感信令时设备对报文的执行动作，会有以下两种情况： • 正常放行 • 丢弃敏感信令
设备检测范围		配置作为设备检测范围的源地址对象组，不同类型的地址对象组之间 只要有一个对象组成功匹配就算符合过滤条件，设备就会对报文进行 行源地址不在检测对象组之内的报文

敏感信令选择	选择设备所需要检测的敏感信令，即检测报文中是否包含指定的敏 等

3. 单击<应用>按钮，指定标准的敏感信令控制功能配置成功。

配置标准流量管控

标准流量管控功能可以根据不同的标准流量管控策略，对物联网设备流量进行检测，通过将单一设备编码的请求发生次数、频率等信息与管理员设置的阈值进行比较，实现对请求方设备进行流量管控的功能。此功能可以有效的避免拒绝服务攻击。具体配置步骤如下：

1. 选择“策略 > 物联网设备安全管理 > 标准流量管控”。
2. 在“标准流量管控”页面单击<新建>按钮，进入“新建标准流量管控策略”页面。
3. 新建标准流量管控策略，具体配置内容如下所示：

表-4 标准流量管控策略配置参数表

参数	说明
策略名称	配置标准流量管控策略的名称
生效状态	是否开启该标准流量管控策略
设备检测范围	配置作为设备检测范围的源地址对象组，不同类型的地址对象组之间是“或 要有一个对象组成功匹配就算符合过滤条件，设备就会对报文进行检测。设

		地址不在检测对象组之内的报文
匹配选项	标准类型	报文所采用的标准类型
	设备信息	设备的基本信息，包括设备编码和地址
判定条件	单ID请求总次数	单个物联网设备发出请求的总次数
	单ID请求频次	单个物联网设备发出请求的频率，即每分钟发出请求的次数
条件关系		判定条件之间的关系，可选择以下两种关系： • 或：请求次数或者请求频率任意一项达到判断条件，标准流量管控策略 • 且：请求次数和请求频率必须同时达到判定条件，标准流量管控策略才
动作		当有报文命中标准流量管控策略并且满足判定条件时，设备对报文的执行动 种情况： • 正常放行 • 阻断报文
告警		开启日志告警功能，当有报文命中标准流量管控策略并且满足判定条件时发

4. 单击<确定>按钮，新建标准流量管控策略成功，并会在标准流量管控页面中显示。

5. （可选）管理员可在标准流量管控页面设置告警周期时间，当有物联网接入设备命中策略需要发送标准流量管控日志时，设备会判断距上一次该接入设备命中相同的策略时发送日志的时间是否超过告警周期，超过则发送日志，不超过则不发送日志。

对象组

本帮助主要介绍以下内容：

- 特性简介
  - 对象组
  - 时间段
  - NAT 地址组
  - NAT 地址组地址检测
  - 地区
  - 域名地址
- 使用限制和注意事项
- 配置指南
  - 配置 IPv4 地址对象组
  - 配置 IPv6 地址对象组
  - 配置 MAC 地址对象组
  - 配置服务对象组
  - 配置地区或地区组

- 配置时间段
- 配置 NAT 地址组

特性简介

对象组

对象组定义了一系列报文匹配规则，可以被其他业务模块等引用，作为匹配报文的条件。

对象组由一条或多条对象组成，每条对象定义了一个报文匹配规则。报文只要满足对象组中一条对象的匹配规则，则该报文匹配该对象组。

对象组分为以下几种：

- IPv4 地址对象组：包含 IPv4 地址对象，用于匹配报文中的 IPv4 地址。
- IPv6 地址对象组：包含 IPv6 地址对象，用于匹配报文中的 IPv6 地址。
- MAC 地址对象组：包含 MAC 地址对象，用于匹配报文中的 MAC 地址。
- 服务对象组：包含服务对象，用于匹配报文中的协议类型以及协议的特性（如 TCP 或 UDP 的源端口/目的端口、ICMP 协议的消息类型/消息码等）。

为了简化配置，对象组还支持多级嵌套功能，即一个对象组可以引用另一个对象组，从而复用该对象组中的报文匹配规则。

时间段

时间段（Time Range）定义了一个时间范围。用户通过创建一个时间段并在某业务中将其引用，就可使该业务在此时间段定义的时间范围内生效。但如果一个业务所引用的时间段尚未配置或已被删除，该业务将不会生效。

在一个时间段中，可以使用以下两种方式定义时间范围：

- 周期时间段：表示以一周为周期（如每周一的 8 至 12 点）循环生效的时间段。
- 绝对时间段：表示在指定时间范围内（如 2015 年 1 月 1 日 8 点至 2015 年 1 月 3 日 18 点）生效的时间段。

每个时间段都以一个名称来标识，用户最多可创建 1024 个不同名称的时间段。一个时间段内可包含一或多个周期时间段（最多 32 个）和绝对时间段（最多 12 个），当一个时间段内包含有多个周期时间段和绝对时间段时，系统将先分别取各周期时间段的并集和各绝对时间段的并集，再取这两个并集的交集作为该时间段最终生效的时间范围。

NAT 地址组

NAT 地址组由一个或多个 IP 地址段和端口范围组成，可以被 NAT 模块引用，用于 NAT 动态转换。

- 对于采用 PAT 模式的 NAT 动态转换，需要配置地址组成员和端口范围。此外，对于 NAT444 动态转换方案，还需配置端口块大小和增量端口块数。

- 对于采用 NO-PAT 模式的 NAT 动态转换，仅需配置地址组成员。

关于 PAT 模式与 NO-PAT 模式的详细介绍，请参见“NAT”。

NAT 地址组地址检测

NAT 地址组检测功能用于检测 NAT 地址组中地址的可用性，是通过在地址池中引用 NQA 模板来实现的，详细过程如下：

1. NAT 地址组引用 NQA 探测模板后，设备会周期性的向 NQA 模板中指定的目的地址依次发送探测报文，其中探测报文的源 IP 地址是地址池中的 IP 地址。
2. 若设备没有收到 NQA 探测应答报文，则将探测报文的源 IP 地址从地址池中排除，暂时禁止该 IP 地址用于地址转换。
3. 被排除的 IP 地址还会继续作为探测报文的源 IP 地址对目的 IP 地址在下个探测周期进行探测，如果收到回应报文，则允许该 IP 地址重新用于地址转换。

地区

地区功能主要用于识别报文的发送源和目的所在的地理位置，从而实现通过配置安全策略对报文进行地理区域化控制。

地区

地区包括预定义地区和自定义地区：

- 预定义地区：通过设备中的地区特征库定义，包括国家、省和城市，预定义地区中包含预设的 IPv4 地址。
- 自定义地区：用户手动创建的地区，可将对应的 IP 地址加入自定义地区中。

地区组

可以将具有相似特征的地区添加到一个地区组中。一个地区组，就是若干个地区的集合。如果报文被识别为属于某个地区，而该地区又属于某个地区组，则报文相当于被识别为属于某个地区组。基于地区的业务可以对属于同一个地区组的报文做统一处理。

域名地址

域名地址查询功能可根据域名查找对应的 IPv4 地址和 IPv6 地址。在对象组中配置了域名后，可在此页面查看指定域名对应的 IP 地址。

查询结果有以下几种情况：

- 如果该域名解析到 IP 地址，将显示相应的 IP 地址。
- 如果该域名未被 IP 地址对象组正确引用或未建立域名和 IP 地址之间的对应关系，将显示“该域名未解析到 IP 地址”。

使用限制和注意事项

- 对象组的嵌套层次最大为 5 层，譬如对象组 1、2、3、4 分别引用对象组 2、3、4、5，则对象组 5 不能再引用其他对象组，对象组 1 也不能再被其他对象组引用。
- 嵌套的对象组不能形成循环。
- NAT 地址组可以引用多个 NQA 探测模板。当引用多个 NQA 探测模板时，只要有一个 NQA 探测模板探测成功，则表示该地址可用于地址转换。
- 自定义地区名称不能与预定义地区名称相同。
- 不同自定义地区中手动添加的 IPv4 地址不允许重叠。
- 地区中手动添加的 IPv4 地址允许与预定义地区中的预设 IPv4 地址重叠。当重叠时，预设 IPv4 地址不生效。
- 地区组的引用不能形成循环嵌套，譬如地区组 a 引用地区组 b，则地区组 b 不能再引用地区组 a。
- 地区组最大嵌套层次为 3 层，譬如地区组 1、2 分别引用地区组 2、3，则地区组 3 不能再引用其他地区组，地区组 1 也不能再被其他地区组引用。

配置 IPv4 地址对象组

1. 单击“对象 > 对象组 > IPv4 地址对象组”。
2. 在“IPv4 地址对象组”页面单击<新建>按钮。
3. 新建 IPv4 地址对象组。

表-1 新建 IPv4 地址对象组配置

参数	说明
名称	对象组的名称，为1～63个字符的字符串，不区分大小写 称必须全局唯一
描述	对象组的描述信息，为1～127个字符的字符串，区分大小
安全域	地址对象组所属的安全域
对象	IPv4地址对象组的内容，可通过<添加>按钮进行配置

4. 单击<添加>按钮，进入添加对象页面，配置参数如下。

表-2 添加对象配置

参数	说明
对象	添加对象的类型，包括： • 网段：子网 IPv4 地址 • 对象组：其他 IPv4 对象组 • IP 地址范围：范围 IPv4 地址 • 主机 IP 地址：主机 IPv4 地址 • 主机名：主机名称 • IP 地址/通配符掩码：通配符掩码形式的 IPv4 地址
排除地址	地址对象中排除的IPv4地址，该参数仅在“对象”参数为网段、地址/通配符掩码时可选
描述	对象的描述信息，为1～127个字符的字符串，区分大小写

5. 单击<确定>按钮，新建的 IPv4 地址对象组会在“IPv4 地址对象组”页面显示。

配置 IPv6 地址对象组

1. 单击“对象 > 对象组 > IPv6 地址对象组”。
2. 在“IPv6 地址对象组”页面单击<新建>按钮。
3. 新建 IPv6 地址对象组。

表-3 新建 IPv6 地址对象组配置

参数	说明
名称	对象组的名称，为1～63个字符的字符串，不区分大小写 称必须全局唯一
描述	对象组的描述信息，为1～127个字符的字符串，区分大小
安全域	地址对象组所属的安全域
对象	IPv6地址对象组的内容，可通过<添加>按钮进行配置

4. 单击<添加>按钮，进入添加对象页面，配置参数如下。

表-4 添加对象配置

参数	说明
对象	添加对象的类型，包括： • 网段：子网 IPv6 地址 • 对象组：其他 IPv6 对象组 • IP 地址范围：范围 IPv6 地址 • 主机 IP 地址：主机 IPv6 地址 • 主机名：主机名称
排除地址	地址对象中排除的IPv6地址，该参数仅在“对象”参数为网段、 选

描述	对象的描述信息，为1～127个字符的字符串，区分大小写

5. 单击<确定>按钮，新建的 IPv6 地址对象组会在“IPv6 地址对象组”页面显示。

配置 MAC 地址对象组

1. 单击“对象 > 对象组 > MAC 地址对象组”。
2. 在“MAC 地址对象组”页面单击<新建>按钮。
3. 新建 MAC 地址对象组。

表-5 新建 MAC 地址对象组配置

参数	说明
名称	对象组的名称，为1～63个字符的字符串，不区分大小写，必须全局唯一
描述	对象组的描述信息，为1～127个字符的字符串，区分大小
对象	MAC地址对象组的内容，可通过<添加>按钮进行配置

4. 单击<添加>按钮，进入添加对象页面，配置参数如下。

表-6 添加对象配置

参数	说明
类型	添加对象的类型，包括： • 对象组：其他 MAC 地址对象组 • MAC 地址：MAC 地址
对象组	指定引用MAC地址对象组的名称，为1～63字符，不区分大小写，该参数仅在“ 象组时可配置
MAC地址	MAC地址，格式为HH-HH-HH-HH-HH-HH，该参数仅在“类型”参数为MAC地
描述	对象的描述信息，为1～127个字符的字符串，区分大小写

5. 单击<确定>按钮，新建的 MAC 地址对象组会在“MAC 地址对象组”页面显示。

配置服务对象组

1. 单击“对象 > 对象组 > 服务对象组”。
2. 在“服务对象组”页面单击<新建>按钮。
3. 新建服务对象组。

表-7 新建服务对象组配置

参数	说明
名称	对象组的名称，为1～63个字符的字符串，不区分大小写 称必须全局唯一
描述	对象组的描述信息，为1～127个字符的字符串，区分大小
对象	服务对象组的内容，可通过<添加>按钮进行配置

4. 单击<添加>按钮，进入添加对象页面，配置参数如下。

表-8 添加对象配置

参数	说明
对象	添加对象的类型，包括： • 协议类型：协议类型 • 对象组：其他服务对象组
类型	协议类型，包括： • TCP：协议号为 6 • UDP：协议号为 17 • ICMP：协议号为 1 • ICMPv6：协议号为 58 • SCTP：协议号为 132

	• IP 协议号：协议号取值范围为 0～255
协议号	IP协议号，取值范围为0～255，仅在类型参数为“IP协议号”时可配置
消息类型	ICMP/ICMPv6消息类型，取值范围为0～255，仅在类型参数为“ICMP”或“IC置
消息码	ICMP/ICMPv6消息码，取值范围为0～255，仅在类型参数为“ICMP”或“ICM息类型已配置时才可配置
源端口	源端口地址范围，起始和终止端口号取值范围为0～65535，仅在类型参数为“TC“SCTP”可配置
目的端口	目的端口地址范围，起始和终止端口号取值范围为0～65535，仅在类型参数为“T“SCTP”可配置
描述	对象的描述信息，为1～127个字符的字符串，区分大小写

5. 单击<确定>按钮，新建的服务对象组会在“服务对象组”页面显示。

配置地区或地区组

地区配置

1. 单击“对象 > 对象组 > 地区”。
2. 在“地区”页面单击<新建>按钮。
3. 新建地区。

表-9 新建地区配置

参数	说明
名称	表示地区的名称，为1～63个字符的字符串，不区分大小写，不 符
经度	表示地区的经度，取值范围为-180.00～180.00，单位为度。东 经为负数
纬度	表示地区的纬度，取值范围为-90.00～90.00，单位为度。北纬 为负数
描述	地区的描述信息，为1～127个字符的字符串，区分大小写
IPv4地址	地区的IPv4地址配置可为单个IP地址或IP地址范围

4. 单击<确定>按钮，新建的地区会在“地区”页面显示。

地区组配置

1. 单击“对象 > 对象组 > 地区”。
2. 在“地区组”页面单击<新建>按钮。
3. 新建地区组。

表-10 新建地区组配置

参数	说明
地区组名称	表示地区组的名称，为1～63个字符的字符串，不区分大小写字符
描述	地区组的描述信息，为1～127个字符的字符串，区分大小写
可选地区和地区组	选择地区组成员

4. 单击<确定>按钮，新建的地区组会在“地区组”页面显示。

配置时间段

1. 单击“对象 > 对象组 > 时间段”。
2. 在“时间段”页面单击<新建>按钮。
3. 新建时间段。

表-11 新建时间段配置

参数	说明
名称	时间段名称

周期时间段	以一周为周期循环生效的时间段
绝对时间段	指定时间范围内生效的时间段

4. 单击<确定>按钮，新建的时间段会在“时间段”页面显示。

配置 NAT 地址组

1. 单击“对象 > 对象组 > NAT 地址组”。
2. 在“NAT 地址组”页面单击<新建>按钮。
3. 新建 NAT 地址组。

表-12 新建 NAT 地址组配置

参数	说明
地址组编号	表示地址组的编号
地址组名称	表示地址组的名称
地址组描述	表示地址组的描述信息
VRRP备份组	配置此功能后，所绑定VRRP备份组中的Mast 拟IP地址和虚拟MAC地址响应ARP请求报文。 环境中需要配置此功能。此功能不同设备的支 以设备Web页面的实际支持情况为准

端口范围	该NAT地址组内的所有公网IP地址可用于地址 必须位于所指定的端口范围之内
端口块大小	表示分配端口块中所包含的端口数，当分配端口 源耗尽（所有端口都被使用）时，如果对应的私 网发起新的连接，则无法从分配端口块中获取
增量端口块数	当分配端口块中的端口资源耗尽（所有端口都被 以为对应的私网IP地址进行增量端口块分配
地址检测	此功能用于检测NAT地址组中地址的可用性，是 中引用NQA模板来实现的。本功能仅对用于出方 地址成员的可用性进行检测
地址组成员	对到达外部网络的数据报文进行地址转换时，报 被转换为地址组成员中的某个地址
排除地址组成员	某些地址成员不能用做地址转换时，配置禁止用 IP地址

4. 单击<确定>按钮，完成 NAT 地址组配置。

5. 在策略 NAT 中引用 NAT 地址组，实现 NAT 动态转换。有关策略 NAT 的详细配置介绍，请参见“策略 NAT”。

用户管理

本帮助主要介绍以下内容：

- 特性简介
  - 本地用户
  - 身份识别用户
  - 在线用户
  - 用户导入策略
  - 邮件服务器
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置本地用户
  - 配置身份识别用户
  - 管理在线用户
  - 配置用户导入策略
  - 配置邮件服务器

特性简介

本地用户

用户

所谓本地用户，是指在本地设备上设置的一组用户属性的集合。该集合以用户名作为用户的唯一标识。本地用户供通过设备访问网络服务的用户使用，即作为网络接入类用户。

当选择使用本地认证、本地授权、本地计费方法对用户进行认证、授权或计费时，应在设备上创建本地用户并配置相关属性。

用户组

为了简化本地用户的配置，增强本地用户的可管理性，引入了用户组的概念。用户组是一个本地用户属性的集合，某些需要集中管理的属性可在用户组中统一配置和管理，用户组内的所有本地用户都可以继承这些属性。目前，用户组中可以管理的用户属性为授权属性。

每个新增的本地用户都默认属于一个系统自动创建的用户组 system，且继承该组的所有属性。

密码管理

为了提高用户登录密码的安全性，可通过配置密码管理功能对用户的登录密码进行管理。

- 密码长度检查

  用于限制用户密码的最小长度。当设置用户密码时，如果输入的密码长度小于设置的密码最小长度，系统将不允许设置该密码。缺省情况下，密码的最小长度为 10 个字符。

- 密码组合检查

  用于设置用户密码的组成元素的组合类型，以及至少要包含每种元素的个数。密码的组成元素包括以下 4 种类型：

  - [A ~ Z]
  - [a ~ z]
  - [0 ~ 9]
  - 32 个特殊字符（空格~`!@#$%^&*()_+-={}|[]\:";'<>,./）

  密码元素的组合类型有 4 种，具体涵义如下：

  - 组合类型为 1 表示密码中至少包含 1 种元素；
  - 组合类型为 2 表示密码中至少包含 2 种元素；
  - 组合类型为 3 表示密码中至少包含 3 种元素；
  - 组合类型为 4 表示密码中包含 4 种元素。

  当用户设置密码时，系统会检查设定的密码是否符合配置要求，只有符合要求的密码才能设置成功。缺省情况下，密码元素的组合类型为 1 种，每种元素的个数为 1 个。

- 密码复杂度检查

为确保用户的登录密码具有较高的复杂度，设置的密码必须符合一定的复杂度要求，只有符合要求的密码才能设置成功。目前，可配置的复杂度要求包括：

- 不允许密码中包含用户名或颠倒的用户名。例如，用户名为“abc”，那么“abc982”或者“2cba”之类的密码就不符合复杂度要求。



本功能在本地用户密码管理界面和全局密码管理界面均开启才生效

- 不允许密码中包含连续三个或以上的相同字符。例如，密码“a111”就不符合复杂度要求。



本功能在本地用户密码管理或全局密码管理界面任一位置开启都生效

- 密码历史记录

用于设置系统保存用户密码历史记录。当用户修改密码时，系统会要求用户设置新的密码，如果新设置的密码以前使用过，且在当前用户密码历史记录中，系统将提示用户密码更改失败。另外，用户更改密码时，系统会将新设置的密码与所有历史记录密码以及当前密码逐一比较，要求新密码至少与旧密码有 4 字符不同。并且，这 4 个字符必须互不相同，否则密码更改失败。

可以配置每个用户密码历史记录的最大条数，当密码历史记录的条数超过配置的最大历史记录条数时，新的密码历史记录将覆盖该用户最老的一条密码历史记录。

- 密码更新

用于设置用户登录设备后修改自身密码的最小间隔时间。在如下情况中，密码更新并不受该功能的约束：

- 开启密码管理后，用户首次登录设备时系统要求用户修改密码。
- 密码老化后系统要求用户修改密码。

- 用户登录控制

  账号闲置时间：用于全局设置本地用户账号闲置时间，本地用户创建后，需要成功登录一次设备，账号闲置时间才能生效，在配置的闲置时间内，用户从未成功登录，该用户将被锁定。若要恢复登录操作，需要在本地用户界面，解除用户闲置锁定状态。

身份识别用户

通过用户身份识别与管理功能，可提供基于用户进行的网络访问控制和网络权限分配。该功能具有以下优点：

- 基于用户进行其他业务策略的制定，可提高策略的易用性。
- 基于用户进行网络攻击行为以及流量的统计和分析，可实现对用户网络访问行为的追踪审计。
- 解决了用户 IP 地址动态变化带来的策略控制问题，即以不变的用户应对变化的 IP 地址。

身份识别用户

身份识别用户用于存储和管理不同来源的网络接入用户的身份信息，包括用户名、用户组名以及所属身份识别域名。设备上，不同来源的身份识别用户被身份识别模块统一管理。

目前，支持以下方式生成身份识别用户：

- 从本地用户数据库学习：用户身份识别模块学习设备上的本地用户信息，将其保存为身份识别用户。
- 从 CSV 文件中导入：管理员将记录了用户信息的 CSV 文件导入到设备中，可批量创建身份识别用户。
- 从第三方服务器导入：通过向第三方服务器发起用户信息请求，将服务器上的网络接入用户账户信息直接导入本地，并生成对应的身份识别用户。如果实际网络环境中的用户信息存放在第三方认证服务器上，则可采用此方式统一管理。支持的第三方服务器包括 LDAP 服务器和 iMC 的 RESTful 服务器。

身份识别用户账户将会由于以下原因被删除：

- 管理员手工删除身份识别用户。
- 本地用户数据库中删除某本地用户之后，用户身份识别模块会同步删除对应的身份识别用户账户。

身份识别用户组

在用户身份识别业务中，可以将用户加入到组中进行批量配置和层级式管理，这样的组称为身份识别用户组。设备上，不同来源的身份识别用户组被用户身份识别模块统一管理。

目前，支持以下方式生成身份识别用户组：

- 从本地用户数据库学习：当设备上创建本地用户组时，会通知用户身份识别模块生成相应的身份识别用户组。
- 从 CSV 文件中导入：设备在从 CSV 文件中导入身份识别用户账户的同时，可以根据管理员的配置自动生成相应的身份识别用户组。
- 从第三方服务器导入：设备在从第三方服务器上导入身份识别用户账户的同时，会根据账户中的组信息自动生成相应的身份识别用户组。

身份识别用户组被应用模块引用之后，该用户组将处于激活状态，所有基于该组的业务将会生效。当应用模块取消对该身份识别用户组的引用，该身份识别用户组将处于非激活状态。

身份识别用户组将会由于以下原因被删除：

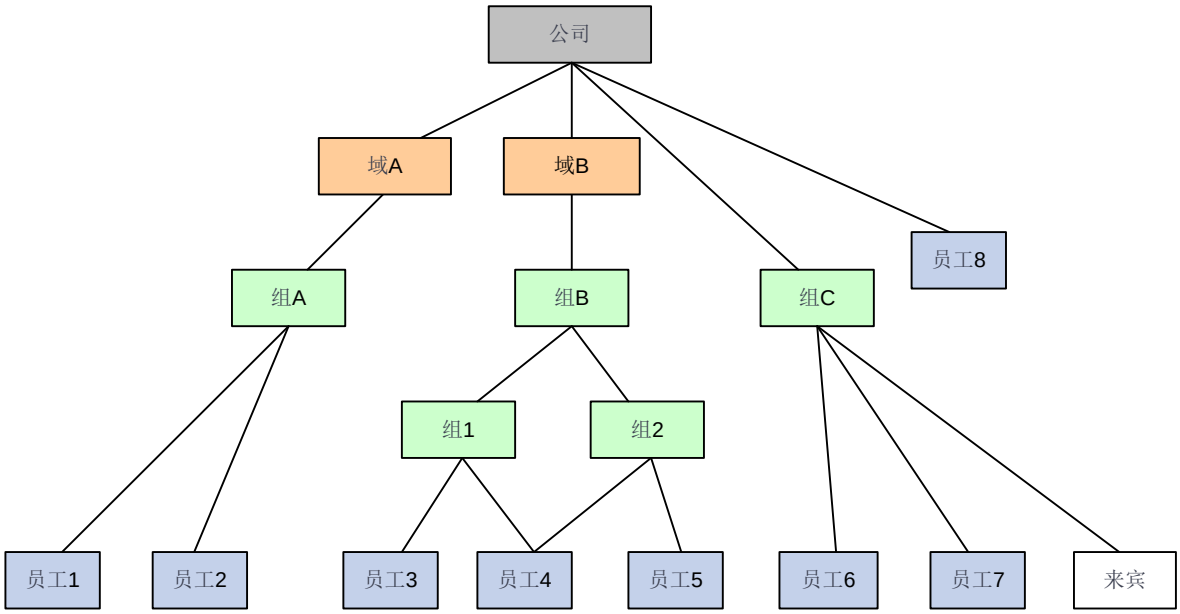
- 管理员手工删除身份识别用户组。
- 本地用户数据库中删除本地用户组之后，用户身份识别模块会同步删除对应的身份识别用户组。

基于用户组的管理架构

设备上的所有身份识别用户按树形结构组织，每一个身份识别用户隶属于一个或多个身份识别用户组，每个身份识别用户组也可以隶属于一个更高结构层次的身份识别用户组。这种树形组织结构易

于管理员查询、定位，是企业内常用的用户组织方式。网络管理员可以根据企业的组织结构在设备上创建身份识别用户组和身份识别用户，分别对应不同管理级别的部门和员工，如图-1 所示：

图-1 基于用户组的管理架构图



基于用户身份的访问控制

基于用户身份的访问控制流程主要包括如下步骤：

1. 用户身份认证：网络接入用户通过一定的认证方式（本地认证、远程服务器认证、单点登录）提供用户名和密码信息，完成身份验证，并成为在线用户。

2. 用户身份识别：设备记录在线用户的用户名和 IP 地址信息，并与本地存储的用户和用户组配置进行关联，实现 IP 地址和用户的映射。管理员也可以直接配置用户和 IP 地址的映射关系，便于无需认证的网络接入用户使用。

3. 业务策略执行：在线用户访问网络服务时，设备识别出用户流量的源 IP 地址，并根据已建立的 IP 地址和用户的映射关系解析出对应的用户名以及所属的用户组，然后按照业务对用户/用户组的策略配置，对该用户的网络访问权限进行控制。

在线用户

在线用户是指用户身份识别模块管理的上线用户（包括 Portal、PPP、IPoE 类型）。设备记录的在线用户信息可包括用户名、身份识别域名、IP 地址、MAC 地址等。

在线用户有以下两种来源：

- 动态生成：
  - 在本设备接入，且通过本地认证或远程服务器认证的在线网络接入用户。用户上线后，用户身份识别模块会在本地身份识别用户数据库中查询该用户名和域名对应的表项，如果查询成功，则会生成一条在线用户表项。
  - 从第三方服务器上导入的在线网络接入用户。导入在线用户信息时，用户身份识别模块会在本地身份识别用户数据库中查询用户名和域名对应的表项，如果查询成功，则会生成对应的在线用户表项。可采用此方式将第三方服务器上的所有在线用户信息导入到本设备进行统一管理和监控。支持的第三方服务器为 iMC 的 RESTful 服务器。
- 静态配置：网络管理员手工配置静态类型的身份识别用户表项，它记录用户名和 IP 地址的绑定关系。一个静态类型的身份识别用户表项创建后，用户身份识别模块会在本地身份识别用户数据库中查询该用户名和域名对应的表项，如果查询成功，则会生成一条静态类型的在线用户

表项。一些组网需求下，例如有少量指定人员临时接入网络时，网络管理员希望这些用户无需进行认证也能够在安全特性的管理下访问网络，则可以通过配置静态类型的在线用户满足该需求。

在线用户可被应用模块引用，进行相关业务策略的处理。在线用户表项被删除后，用户身份识别模块将通知应用模块停止该用户相关的业务处理。

在线用户表项将会由于以下原因被删除：

- 管理员手工删除在线用户表项。
- 本设备接入的用户下线后，接入模块通知用户身份识别模块删除对应的在线用户表项。
- 设备重启后，所有动态类型的在线用户表项均被删除。
- 用户身份识别功能关闭，所有在线用户表项均被删除。
- 第三方服务器上用户下线时，服务器会主动通知设备删除相应的在线用户表项。

用户导入策略

用户导入策略用于配置用户身份识别模块从第三方服务器上导入身份识别用户信息的策略，可导入的用户信息包括身份识别用户信息、身份识别用户组信息和在线用户信息。目前，系统支持的可导入的第三方服务器为 iMC 的 RESTful 服务器和 LDAP 服务器。

目前，用户导入策略支持如下几种导入方式：

- 自动导入：采用自动导入方式后，设备首先会从导入策略中指定的服务器上导入服务器上的所有身份识别用户账户信息和所有在线用户信息，然后定期从该服务器上自动导入身份识别用户账户。
- 手动导入：采用手动导入方式后，设备将向导入策略中指定的服务器发起一次连接请求，之后导入服务器上的所有身份识别用户账户信息和在线用户信息。

邮件服务器

通过 Web 页面管理设备上的网络接入类本地用户时，系统提供了为网络接入类本地用户分配随机密码的功能，并支持通过邮件的方式将生成的随机密码信息告知给用户。之后，用户可以使用此随机密码登录设备。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 用户密码管理界面下的配置为全局配置，对所有用户生效。新建或修改指定用户界面下的配置本文称之为本地用户密码管理配置，只对当前用户生效。本地用户密码管理中的配置优先级高于全局配置。
- 若不设置本地用户密码，则本地用户认证时无需输入密码，只要用户名有效且其它属性认证通过即可认证成功。因此为提高用户账户的安全性，建议设置本地用户密码。
- 对于 Portal 类型的用户，仅授权 ACL 和授权用户闲置切断时间。
- 对于 SSL VPN 接入类型的用户，仅授权 SSL VPN 资源组有效。
- 在“用户“页面，使用 CSV 模板批量导入用户时，需要按照模板格式导入且不能随意修改模板的注释头，否则会造成导入数据丢失。
- 本特性支持的 iMC 的 RESTful 服务器必须为支持 SSM 组件的 iMC PLAT 7.0 (E0201)及其补丁版本。
- 当设备上的 RESTful 服务器配置完成，且与远程 RESTful 服务器建立连接后，iMC 的 RESTful 服务器会实时向设备同步用户上线和下线的信息，刷新设备上的在线用户表项。
- 配置收件人邮箱地址前，需要先对邮件服务器进行相关配置。
- 在“身份识别用户”页面，删除身份识别用户时，仅删除导入的用户，本地用户不会被删除。
- 管理员页面和本地用户页面中的密码管理部分功能相互关联且参数共用，具体可参见用户页面<密码管理>中各配置栏的提示信息。

- 开启密码管理之后，设置的登录用户密码必须至少由四个不同的字符组成。
- 若要使得具体的密码管理功能生效，需在本地用户页面菜单栏的<密码管理>中开启密码管理功能。

配置指南

配置本地用户

配置本地用户包括两种方法：新建本地用户和批量导入本地用户。

新建本地用户

新建本地用户的具体配置步骤如下：

1. 选择“对象 > 用户与认证 > 用户管理 > 本地用户”。
2. 选择“用户”页签，在“用户”页面单击<新建>按钮，进入“新建用户”页面。
3. 在“新建用户”页面的具体配置内容如下所示：

表-1 配置用户参数表

参数	说明
用户名	网络接入类用户，用于通过设备接入网络，访问网络资源的用户。当需要进 需要在设备上配置本地用户
设置随机密码	为用户分配随机密码
收件人邮箱地址	在创建随机密码后，设备需要向用户发送邮件告知随机密码 配置收件人邮箱地址前，需要先对邮件服务器进行相关配置
密码	用户进行接入认证所使用的密码
确认密码	再次输入用户进行接入认证所使用的密码
有效期	为用户设置有效期，用户仅在有效期内才能认证成功 • 若同时指定了有效期的开始时间和结束时间，则有效期的结束时间必须 • 如果仅指定了有效期的开始时间，则表示该时间到达后，用户一直有效 • 如果仅指定了有效期的结束时间，则表示该时间到达前，用户一直有效
授权用户组	每一个本地用户都属于一个本地用户组，并继承组中的所有属性（密码管理 权属性）
身份识别用户组	本地用户加入身份识别用户组后，将成为该组的成员，接受基于组的用户策 理
可用服务	可用服务是用户可使用的网络服务类型。该属性是本地认证的检测项，如果 使用的服务类型，则该用户无法通过认证
同时在线最大用户数	使用当前用户名接入设备的最大用户数目。若当前该用户名的接入用户数已 使用该用户名的新用户将被禁止接入

手机号	配置此用户的手机号
描述	配置有关此用户的描述信息

4. （可选）配置授权属性，具体包括如下所示：

表-2 配置授权属性参数表

参数	说明
ACL类型	IPv4 ACL：可根据报文的源IP地址，目的IP地址、协议类型等信息来制定规则，对报文进行匹配 二层ACL：可根据报文的源MAC地址、目的MAC地址、链路层协议类型、报文等二层信息来制定规则，对报文进行匹配
授权ACL	本地用户认证成功后，将被授权仅可以访问符合指定ACL规则的网络资源 可选择已创建的ACL，也可以新创建ACL。此处新建的ACL，可在“对象 > IPv4/IPv6页面查看
用户闲置切断时间	如果用户在线后连续闲置的时长超过该值，设备会强制该用户下线
授权VLAN	本地用户认证成功后，将被授权仅可以访问指定VLAN内的网络资源
SSL VPN资源组	本地用户认证成功后，将被授权仅可以访问指定SSL VPN资源组内的网络资源，仅对SSL VPN用户有效

5. （可选）配置绑定属性，具体包括如下所示：

表-3 配置绑定属性参数表

参数	说明
用户接入的接口	如果用户接入的接口与此处绑定的接口不一致，则认证失败
用户的IPv4地址/掩码长度	如果用户的IPv4地址及其掩码长度与此处绑定的IPv4地址及其掩码长度不一致，则认证失败
用户的MAC地址	如果用户的MAC地址与此处绑定的MAC地址不一致，则认证失败
用户所属的VLAN	如果用户接入的VLAN与此处绑定的VLAN不一致，则认证失败

6. （可选）配置用户密码设置控制参数，具体包括如下所示：

表-4 配置用户密码设置控制参数表

参数	说明
密码最小长度	如果输入的密码长度小于设置的密码最小长度，系统将不允许设置该密码
密码组成元素的最少类型	如果输入的密码组成元素类型少于设置的密码最少类型，系统将不允许设
每种类型至少包含个数	如果输入的密码每种类型包含的元素数量少于设置的最少个数，系统将不
开启密码老化	可以限制用户密码的使用时间
密码老化时间	当密码的使用时间超过老化时间后，需要用户更换密码
不允许密码中包含用户名或	开启本功能后，输入的密码不允许包含用户名或颠倒的用户名

颠倒的用户名	
不允许密码中包含连续三个或以上相同字符	开启本功能后，输入的密码中不允许包含连续三个或以上相同字符
用户登录尝试的最大次数	用户登录失败的最大次数，超过设置的最大值后，根据处理方式的设置情况果
登录次数超过最大值后的处理方式	登录失败次数超过最大值后处理结果： • 永久禁止登录 • 规定时间内禁止登录 • 不禁止登录
禁止登录时长	禁止登录的时间，超过设置的时间后，可以继续登录
账号闲置时间	用户在创建后，需要成功登录一次设备，账号闲置时间才能生效。在配置的用户从未成功登录，该用户将被锁定。若要恢复登录操作，需要在本地用户闲置锁定状态

7. 单击<确定>按钮，新建用户成功，且会在“用户”页面中显示。

批量导入本地用户

批量导入本地用户的具体配置步骤如下：

1. 选择“对象 > 用户与认证 > 用户管理 > 本地用户”。
2. 选择“用户”页签，在“用户”页面单击<导入>按钮，进入“导入用户”页面。
3. 在“导入用户”页面的具体配置内容如下所示：

表-5 配置导入用户参数表

参数	说明
导入文件	通过导入文件可批量创建本地用户。按照CSV模板格式导入用户时，不能 注释头，否则会造成导入数据丢失
自动创建用户组	表示当设备上不存在用户所属的用户组时，系统会自动创建用户组，并将 组。若不配置该参数，则表示当设备上不存在用户所属的用户组时，系统 用户组，而是将用户其加入缺省用户组system
覆盖同名用户	表示当导入的用户名已经存在于设备上时，系统使用导入的用户信息覆盖 户配置。若不配置该参数，则表示不导入文件中的同名用户信息，即保留 名用户配置
导入用户信息的起始行	表示从文件的指定行开始导入用户信息。若不配置该参数，则表示导入文 信息

4. 单击<确定>按钮，批量导入用户成功，且会在“用户”页面中显示处导入的用户。

配置密码管理功能

密码管理功能具体配置步骤如下：

1. 选择“对象 > 用户与认证 > 用户管理 > 本地用户”。

2. 选择“用户”页签，在“用户”页面单击<密码管理>按钮，进入“用户密码管理”页面。

3. 在“用户密码管理”页面的具体配置内容如下所示：

表-6 配置用户密码管理功能参数表

参数	说明
开启密码管理	开启本功能后，设备将对用户设置的密码进行限制
开启密码长度检查	开启本功能后，设备将对用户设置的密码长度进行检查
用户密码的最小长度	如果输入的密码长度小于设置的密码最小长度，系统将不允许设置该密码
开启密码组合检查	开启本功能后，设备将对用户设置的密码元素类型数量以及每种类型中包含 行限制
密码组成元素的类型至少包含	如果输入的密码组成元素类型少于设置的密码最少类型，系统将不允许设置
每种类型包含的元素个数至少为	如果输入的密码每种类型包含的元素数量少于设置的最少个数，系统将不允
密码中不能包含连续三个或以上的相同字符	开启本功能后，输入的密码中不允许包含连续三个或以上相同字符
密码中不能包含用户名或者字符顺序颠倒的用户名	开启本功能后，输入的密码不允许包含用户名或颠倒的用户名
开启本地用户首次登录修改密码	开启本功能后，用户首次登录成功，系统要求修改密码
开启密码历史记录	开启本功能后，设备将保存用户设置过的密码
密码历史记录最大条数	当密码历史记录的条数超过设置的最大历史记录条数时，新的密码历史记录 最老的一条密码历史记录
开启密码老化	全局开启设置用户密码的使用时间

密码老化时间	全局设置密码老化时间，当密码的使用时间超过老化时间后，需要用户更
密码过期提醒	配置密码过期前的提醒时间
密码过期后允许用户登录的时间	设置当用户密码过期后仍允许用户登录的时间
密码过期后允许用户登录的次数	设置当用户密码过期后仍允许用户登录的次数
密码更新最小间隔时间	当用户修改密码的间隔时间小于设置的最小间隔时间时，设备不允许用户
密码尝试次数	用户登录失败的最大次数，超过设置的最大值后，根据处理方式的设置情 果
登录失败处理	登录失败次数超过最大值后处理结果： • 永久禁止登录 • 在设置的规定时间内禁止登录
账号闲置时间	全局设置本地用户账号闲置时间，本地用户创建后，需要成功登录一次设 间才能生效，在配置的闲置时间内，用户从未成功登录，该用户将被锁定。 操作，需要在本地用户界面，解除用户闲置锁定状态
同一用户名的用户信息最大条数	不同IP地址的用户采用同一个用户名登录时，若登录设备失败，设备会针 录用户信息，当设备记录的该用户信息条数超过最大值之后，若该用户采 次登录认证失败，则该用户名相关的最早一条用户信息会被删除，新的记
登录失败的锁定用户信息	登录失败后用户将被锁定，通过此下拉框可以切换锁定用户信息的展示样 息可在SSL VPN的统计信息界面查看。请注意，当切换锁定用户信息的显 锁定用户信息将被清空

4. 单击<确定>按钮，密码管理功能将对所有本地用户生效。

配置本地用户组

配置本地用户组的具体配置步骤如下：

1. 选择“对象 > 用户与认证 > 用户管理 > 本地用户”。

2. 选择“用户组”页签，在“用户组”页面单击<新建>按钮，进入“新建用户组”页面。

3. 在“新建用户组”页面的具体配置内容如下所示：

表-7 配置用户组参数表

参数	说明
用户组名称	用来标识本地用户组名称
用户	配置当前用户组的身份成员
用户组	配置当前用户组所属的用户组

4. 授权属性与 SSL VPN 授权属性请参考表-2。

5. 单击<确定>按钮，新建用户组成功，且会在“用户组”页面中显示。

配置身份识别用户

配置身份识别用户的具体配置步骤如下：

1. 选择“对象 > 用户与认证 > 用户管理 > 身份识别用户”。
2. 在“身份识别用户”页面，可查看组织结构。
3. 选择需要编辑的身份识别用户或用户组，具体配置内容如下所示：

表-8 身份识别用户或用户组参数表

参数	说明
用户/用户组	显示已创建的身份识别用户或用户组
继承的组角色	当前用户或用户组所继承的组角色
角色	给当前身份识别用户或用户组添加角色，可以单选或多选现有角色，也可

管理在线用户

在线用户的具体配置步骤如下：

1. 选择“对象 > 用户与认证 > 用户管理 > 在线用户”。

2. 在“在线用户”页面的具体配置内容如下所示：

表-9 在线用户参数表

参数	说明
单击<开启身份识别功能>	开启设备的身份识别功能
选择在线用户匹配模式	其包括如下三种模式： • 保持原有：表示仅使用用户输入的用户名进行身份识别用户匹配。例如 域为 abc，用户输入的用户名为 test@123，则使用用户名 test@123 进 户账户匹配 • 带域匹配：表示使用用户的认证域进行身份识别用户匹配。例如，用户的 用户输入的用户名为 test@123，则使用用户名 test@abc 进行身份识别 • 不带域匹配：表示不对用户账户的域名进行匹配，即使用用户输入的纯 上未加入任何身份识别域的身份识别用户进行匹配。例如，用户的认证 户输入的用户名为 test@123，则使用用户名 test 与未加入身份识别域的 匹配

静态身份识别用户的具体配置步骤如下：

3. 选择“对象 > 用户与认证 > 用户管理 > 在线用户”。

4. 在“在线用户”页面选择“静态身份识别用户”，单击<新建>按钮，进入新建静态身份识别用户页面，具体配置内容如下所示：

表-10 配置静态身份识别用户参数表

参数	说明
域名	指定用户所属的身份识别域
用户名	静态类型的身份识别用户名
IP地址类型	指定静态身份识别用户绑定的IP地址类型：IPv4或IPv6
IP地址	设置静态身份识别用户绑定的IP地址
MAC地址	设置静态身份识别用户绑定的MAC地址

5. 单击<确定>按钮，新建“静态身份识别用户”成功。

配置用户导入策略

新建用户导入策略

用户导入策略的具体配置步骤如下：

1. 选择“对象 > 用户与认证 > 用户管理 > 用户导入策略”。
2. 在“用户导入策略”页面单击<新建>按钮，进入“新建用户导入策略”页面。
3. 在“新建用户导入策略”页面的具体配置内容如下所示：

表-11 配置用户导入策略参数表

参数	说明
名称	用于唯一标识一个用户导入策略
RESTful服务器	指定RESTful服务器，用于从此RESTful服务器上导入身份识别用户信息和
LDAP方案	指定LDAP方案，用于从此LDAP方案中的LDAP服务器上导入身份识别用
导入类型	此配置项的内容仅对LDAP方案有效
开启自动导入功能	开启此功能后，设备首先会从导入策略中指定的服务器上导入服务器上的 息和所有在线用户信息，然后定期从该服务器上自动导入身份识别用户账
导入周期	自动导入身份识别用户账户的周期

4. 单击<确定>按钮，新建用户导入策略成功，且会在“用户导入”页面中显示。

手动导入用户

配置完用户导入策略后，若需要手动导入身份识别用户和在线用户，则管理员可在“用户导入策略”页面，选择如下功能：

- 手动导入身份识别用户：设备向第三方服务器发起用户信息请求，将服务器上的用户账户信息直接导入本地，并生成对应的身份识别用户。在导入过程中，若某个账户导入失败，则跳过该账户，继续导入。

- 手动导入在线用户：单击此按钮后，设备向指定的第三方服务器发起在线用户请求，实现导入服务器上当前所有在线用户信息的目的。目前，仅支持从 iMC 的 RESTful 服务器上导入在线身份识别用户。

配置邮件服务器

设备为用户创建随机密码后，需要向用户发送邮件告知随机密码。配置邮箱地址前，需要先对邮件服务器进行相关配置。

邮件服务器的具体配置步骤如下：

1. 选择“对象 > 用户与认证 > 用户管理 > 邮件服务器”。
2. 在“邮件服务器”页面的具体配置内容如下所示：

表-12 配置邮件服务器参数表

参数	说明
邮件标题	用于配置通知邮件的标题
邮件内容	用于配置通知邮件的内容
发件人地址	用来配置通知邮件的发件人地址
服务器地址	用于配置邮件服务器的URL，必须以smtp://开头
用户名	用于配置登录邮件服务器的用户名

密码	用于配置登录邮件服务器的密码

认证管理

本帮助主要介绍以下内容:

- 特性简介
  - ISP 域简介
  - RADIUS 简介
  - LDAP 简介
  - RESTful 服务器简介
  - Sec Manage 服务器简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置 ISP 域
  - 配置 RADIUS
  - 配置 LDAP
  - 配置 RESTful 服务器
  - 配置 Sec Manage 服务器

特性简介

ISP 域简介

设备对用户的管理是基于 ISP（Internet Service Provider，互联网服务提供者）域的，一个 ISP 域对应着一套实现 AAA（Authentication、Authorization、Accounting，认证、授权、计费）的配置策略，它们是管理员针对该域用户制定的一套认证、授权、计费方法，可根据用户的接入特征以及不同的安全需求组合使用。

设备支持的认证方法包括：

- 不认证：对用户非常信任，不对其进行合法性检查，一般情况下不采用这种方法。
- 本地认证：认证过程在接入设备上完成，用户信息（包括用户名、密码和各种属性）配置在接入设备上。优点是速度快，可以降低运营成本；缺点是存储信息量受设备硬件条件限制。
- RADIUS：RADIUS 认证是一种远端认证方案，认证过程在接入设备和远端的服务器之间完成，接入设备和远端服务器之间通过 RADIUS 协议通信。优点是用户信息集中在服务器上统一管理，可实现大容量、高可靠性、支持多设备的集中式统一认证。当远端主服务器无效时，可配置备份服务器完成认证。
- LDAP：LDAP 认证是一种远端认证方案，认证过程在接入设备和远端的服务器之间完成，接入设备和远端服务器之间通过 LDAP 协议通信。LDAP 协议的典型应用是用来保存系统中的用户信息，用于用户登录的认证和授权。

- 单点登录：认证过程在接入设备和远端的第三方服务器之间完成，认证通过后，第三方认证服务器将用户的身份信息发送给需要进行身份识别的设备，这样即可实现用户在此设备上的认证。

设备支持的授权方法包括：

- 不授权：接入设备不请求授权信息，不对用户可以使用的操作以及用户允许使用的网络服务进行授权。此时，认证通过的 login 用户只有系统所给予的缺省用户角色，其中 FTP/SFTP/SCP 用户的工作目录是设备的根目录，但并无访问权限；认证通过的非 login 用户，可直接访问网络。
- 本地授权：授权过程在接入设备上进行，根据接入设备上为本地用户配置的相关属性进行授权。
- RADIUS：RADIUS 授权是一种远端授权方案，授权过程在接入设备和远端服务器之间完成。RADIUS 协议的认证和授权是绑定在一起的，不能单独使用 RADIUS 进行授权。RADIUS 认证成功后，才能进行授权，RADIUS 授权信息携带在认证回应报文中下发给用户。当远端服务器无效时，可配置备选授权方式完成授权。
- LDAP：LDAP 授权是一种远端授权方案，授权过程在接入设备和远端的服务器之间完成。LDAP 协议中定义了多种操作来实现 LDAP 的各种功能，用于认证和授权的操作主要为绑定和查询。与认证过程稍有不同的是，授权过程不仅仅会查询用户 DN，还会同时查询相应的 LDAP 授权信息。

设备支持的计费方法包括：

- 不计费：不对用户计费。
- 本地计费：计费过程在接入设备上完成，实现了本地用户连接数的统计和限制，并没有实际的费用统计功能。

- RADIUS：RADIUS 计费是一种远端计费方案，计费过程在接入设备和远端的服务器之间完成。当远端服务器无效时，可配置备选计费方式完成计费。

每个用户都属于一个 ISP 域。为便于对不同接入方式的用户进行区分管理，提供更为精细且有差异化的认证、授权、计费服务，设备将用户划分为以下几个类型：

- 登录用户：例如 Telnet、FTP、终端接入用户（即从 Console 接口登录的用户）。
- LAN 接入用户。
- Portal 用户。
- PPP 用户。

在多 ISP 的应用环境中，不同 ISP 域的用户有可能接入同一台设备，因此系统中可以存在多个 ISP 域，其中包括一个缺省存在的名称为 system 的 ISP 域。如果某个用户在登录时没有提供 ISP 域名，系统将把它归于缺省的 ISP 域。系统缺省的 ISP 域可以手工修改为一个指定的 ISP 域。

用户认证时，设备将按照如下先后顺序为其选择认证域：接入模块指定的认证域-->用户名中指定的 ISP 域-->系统缺省的 ISP 域。

RADIUS 简介

RADIUS 概述

RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）是一种分布式的、客户端/服务器结构的信息交互协议，能保护网络不受未授权访问的干扰，常应用在既要求较高安全性、又允许远程用户访问的各种网络环境中。

- RADIUS 客户端：一般位于接入设备上，可以遍布整个网络，负责将用户信息传输到指定的 RADIUS 服务器，然后根据服务器返回的信息进行相应处理（如接受/拒绝用户接入）。
- RADIUS 服务器：一般运行在中心计算机或工作站上，维护用户的身份信息和与其相关的网络服务信息，负责接收接入设备发送的认证、授权、计费请求并进行相应的处理，然后给接入设备返回处理结果（如接受/拒绝认证请求）。

RADIUS 协议使用 UDP 作为封装 RADIUS 报文的传输层协议，通过使用共享密钥机制来保证客户端和 RADIUS 服务器之间消息交互的安全性。

当接入设备对用户提供 AAA（Authentication、Authorization、Accounting，认证、授权、计费）服务时，若要对用户采用 RADIUS 服务器进行认证、授权、计费，则作为 RADIUS 客户端的接入设备上需要配置相应的 RADIUS 服务器参数。

RADIUS 增强功能

- Accounting-on 功能

设备重启后，重启前的原在线用户可能会被 RADIUS 服务器认为仍然在线而短时间内无法再次登录。为了解决这个问题，需要开启 Accounting-on 功能。

开启了 Accounting-on 功能后，设备会在重启后主动向 RADIUS 服务器发送 Accounting-on 报文来告知自己已经重启，并要求 RADIUS 服务器停止计费且强制通过本设备上线的用户下线。若设备发送 Accounting-on 报文后 RADIUS 服务器无响应，则会按照一定的时间间隔尝试重发几次。

- Session control 功能

iMC RADIUS 服务器使用 session control 报文向设备发送授权信息的动态修改请求以及断开连接请求。设备上开启接收 session control 报文的开关后，会打开知名 UDP 端口 1812 来监听并接收 RADIUS 服务器发送的 session control 报文。

需要注意的是，该功能仅能和 iMC RADIUS 服务器配合使用。

- 在线修改用户密码

可以通过本功能控制设备是否使用 RADIUS 17 号标准属性来支持用户在线修改密码。开启本功能后，设备在收到用户的密码修改请求后，会向 RADIUS 服务器发送一个认证请求报文，在该报文中将用户的旧密码和新密码分别携带在 2 号、17 号标准属性中。如果 RADIUS 服务器支持用户在线修改密码，则会响应此认证请求。

LDAP 简介

LDAP 概述

LDAP（Lightweight Directory Access Protocol，轻量级目录访问协议）是一种目录访问协议，基于 Client/Server 结构提供跨平台的、基于标准的目录服务，所有的目录信息数据存储在 LDAP 服务器上。

LDAP 协议的典型应用是用来保存系统中的用户信息，如 Microsoft 的 Windows 操作系统就使用了 Active Directory Server（一种 LDAP 服务器软件）来保存操作系统的用户、用户组等信息，用于用户登录 Windows 时的认证和授权。

LDAP 中使用目录记录并管理系统中的组织信息、人员信息以及资源信息。目录按照树型结构组织，由多个条目（Entry）组成。条目是具有 DN（Distinguished Name，识别名）的属性（Attribute）集合。属性用来承载各种类型的数据信息，例如用户名、密码、邮件、计算机名、联系电话等。

LDAP 属性映射表

在用户的 LDAP 授权过程中，设备会通过查询操作得到用户的授权信息，该授权信息由 LDAP 服务器通过若干 LDAP 属性下发给设备。若设备从 LDAP 服务器查询得到某 LDAP 属性，则该属性只有在被设备的 AAA 模块解析之后才能实际生效。如果某 LDAP 服务器下发给用户的属性不能被 AAA 模块解析，则该属性将被忽略。因此，需要通过配置 LDAP 属性映射表来指定要获取哪些 LDAP 属

性，以及 LDAP 服务器下发的这些属性将被 AAA 模块解析为什么类型的 AAA 属性，具体映射为哪种类型的 AAA 属性由实际应用需求决定。

每一个 LDAP 属性映射表项定义了一个 LDAP 属性与一个 AAA 属性的对应关系。将一个 LDAP 属性表在指定的 LDAP 方案视图中引用后，该映射关系将在 LDAP 授权过程中生效。

RESTful 服务器简介

RESTful 服务器中定义了 RESTful 服务器的相关参数，包括登录账户和服务器 URI。设备与 RESTful 服务器成功建立连接之后，可以从该服务器上手动或定期自动导入身份识别用户信息和在线用户信息。有关身份识别用户的详细介绍，请参见“用户管理联机帮助”。

Sec Manage 服务器简介

Sec Manage 服务器中定义了第三方服务器的相关参数，包括服务器地址、服务器端口和监听端口等。设备与服务器成功建立连接之后，可以接收该服务器推送的用户登录/注销信息，用于更新设备上的在线用户信息。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 不支持对 FTP 类型的登录用户进行计费。
- 当配置 ISP 域时，若选择接入方式为 SSL VPN，需要配置 SSL VPN AAA 方案。在 SSL VPN AAA 方案中，若选择 RADIUS 认证和授权，需保证认证顺序和授权顺序一致。
- 在一个 ISP 域中，只有在认证和授权方法中指定了相同的 RADIUS 方案时，RADIUS 授权过程才能生效。
- 在一个 ISP 域中，当为 SSL VPN 用户指定了多个认证方法时，SSL VPN 用户登录成功后不支持修改密码。
- 如果当前 ISP 域的用户认证成功，但认证服务器（包括本地认证下的接入设备）未对该 ISP 域下发授权属性，则系统使用当前 ISP 下指定的授权属性为用户授权。
- 名称为 system 的 ISP 域不允许删除。
- 当指定某个 ISP 域处于阻塞状态时，不允许该域下的用户请求网络服务，但是不影响已经在线的用户。
- 必须保证设备上设置的共享密钥与 RADIUS 服务器上的完全一致。

- 如果在线用户正在使用的计费服务器被删除，则设备将无法发送用户的实时计费请求和停止计费请求，且停止计费报文不会被缓存到本地。
- 为保证认证和计费报文可被服务器正常接收并处理，接入设备上发送 RADIUS 报文使用的源地址必须与 RADIUS 服务器上指定的接入设备的 IP 地址保持一致。
- 设备上设置的发送给 RADIUS 服务器的数据流或者数据包的单位应与 RADIUS 服务器上的流量统计单位保持一致。
- 如果指定某个 RADIUS 方案不允许用户名中携带有 ISP 域名，那么请不要在两个或两个以上的 ISP 域中同时设置使用该 RADIUS 方案。否则，会出现虽然实际用户不同（在不同的 ISP 域中），但 RADIUS 服务器认为用户相同（因为传送到它的用户名相同）的错误。
- 当主服务器状态为“活动”时，设备首先尝试与主服务器通信，若主服务器不可达，设备更改主服务器的状态为“阻塞”，并启动该服务器恢复活动状态的定时器，然后按照备用服务器的配置先后顺序依次查找状态为“活动”的备用服务器进行认证或者计费。如果状态为“活动”的备用服务器也不可达，则将该备用服务器的状态置为“阻塞”，同时启动该服务器恢复活动状态的定时器，并继续查找状态为“活动”的备用服务器。当服务器恢复活动状态的定时器超时，或者手动将服务器状态置为“活动”时，该服务器将恢复为“活动”状态。在一次认证或计费过程中，如果设备在尝试与备份服务器通信时，之前已经查找过的服务器状态由“阻塞”恢复为“活动”，则设备并不会立即恢复与该服务器的通信，而是继续查找备份服务器。如果所有已配置的服务器都不可达，则认为本次认证或计费失败。

- 要根据配置的备用服务器数量合理设置发送 RADIUS 报文的最大尝试次数和 RADIUS 服务器响应超时时间，避免因为超时重传时间过长，在主服务器不可达时，出现设备在尝试与备用服务器通信的过程中接入模块（例如 Telnet 模块）的客户端连接已超时的现象。
- 要根据配置的备用服务器数量合理设置服务器恢复激活状态的时间。如果服务器恢复激活状态时间设置得过短，就会出现设备反复尝试与状态为活动但实际不可达的服务器通信而导致的认证或计费频繁失败的问题；如果服务器恢复激活状态设置的过长，则会导致已经恢复激活状态的服务器暂时不能为用户提供认证或计费服务。
- 当设备需要与 LDAP 授权服务器配合使用时，需要使用 CLI 方式在设备上进行 LDAP 的相关配置。
- 当设备配置了 Reply-Message 属性解析规则时，在线修改用户密码功能将不生效。

配置指南

对用户的认证、授权和计费策略是通过在 ISP 域中为不同的接入方式配置相应的认证、授权、计费方案来实现的。在一个 ISP 域中，除了设置认证、授权、计费方案之外，还包括一些自身的属性，例如域的状态、用户授权属性，这些域属性对于接入该域的所有用户均生效。若对用户采用本地认证方案，则需要完成本地认证的配置；若采用远端认证、授权或计费方案，则需要完成 RADIUS 的配置。

配置 ISP 域

ISP 域的具体配置步骤如下：

1. 选择“对象 > 用户与认证 > 认证管理 > ISP 域”。
2. 在“ISP 域”页面单击<新建>按钮，进入“添加 ISP 域”页面。
3. 在“添加 ISP 域”页面的具体配置内容如下所示：

表-1 配置 ISP 域参数表

参数	说明
域名	用于唯一标识一个ISP域。ISP域名为1～255个字符的字符串，不区分大小写 “\”、“|”、“”“、“:”、“*”、“?”、“<”、“>”以及“@” 字符串“d”、“de”、“def”、“defa”、“defau”、“defaul”、“de “if”、“if-”、“if-u”、“if-un”、“if-unk”、“if-unkn”、“if-unkno” 和“if-unknown”
状态	状态包括如下两种： • 活动状态：系统允许该域下的用户请求网络服务 • 阻塞状态：系统不允许该域下的用户请求网络服务
接入方式	可根据不同的接入认证需求，选择不同的接入方式。例如，登录用户方式选 登录设备的管理用户等

4. （可选）配置高级配置，具体内容如下所示：

表-2 高级配置参数表

参数	说明
用户闲置切断时间	用户上线后，设备会周期性检测用户的流量，若ISP域内某用户在指定的闲 产生的流量小于指定的数据流量，则会被强制下线
用户在闲置切断时间内产生的数据流量	用户闲置切断时用于设置检测流量的阈值
为用户分配IP地址的地址池	认证成功的PPP和Portal用户可以从指定的地址池中分配得到一个IP地址

5. 单击<确定>按钮，新建 ISP 域成功，且会在“ISP 域”页面中显示。

配置 RADIUS

RADIUS 的具体配置步骤如下：

1. 选择“对象 > 用户与认证 > 认证管理 > RADIUS”。
2. 在“RADIUS”页面单击<新建>按钮，进入“新建 RADIUS”页面。
3. 在“新建 RADIUS 方案”页面的具体配置内容如下所示：

表-3 配置 RADIUS 参数表

参数	说明
方案名称	用于唯一标识一个RADIUS方案
认证服务器	指定认证服务器的IP地址、端口号和共享密钥等信息
计费服务器	指定计费服务器的IP地址、端口号和共享密钥等信息
全局认证共享密钥	仅在认证服务器或计费服务器未指定相应密钥的情况下使用

4. RADIUS 高级设置，具体包括如下所示：

表-4 RADIUS 高级设置参数表

参数	说明
发送RADIUS报文使用的源IPv4地址	设备发送RADIUS报文使用的源IPv4地址
发送RADIUS报文使用的源IPv6地址	设备发送RADIUS报文使用的源IPv6地址
服务器响应超时时间	如果在RADIUS请求报文传送出去一段时间后，设备还没有得到RADIUS服 有必要重传RADIUS请求报文，以保证用户尽可能地获得RADIUS服务， RADIUS服务器响应超时时间
发送RADIUS报文的最大尝试次数	设备向RADIUS服务器重传RADIUS请求报文的最大次数

服务器恢复活动状态的时间	服务器恢复激活状态的时间，建议合理设置时间
发送实时计费更新报文的间隔	实时计费间隔时间越小，计费准确性越高，相对应的对设备和RADIUS服务 越高
发起实时计费更新请求的最大尝试次数	设备向RADIUS服务器发出的实时计费请求没有得到响应的次数超过指定的 用户连接
发送给RADIUS服务器的用户名格式	接入用户通常以“userid@isp-name”的格式命名，“@”后面的部分为IS 以通过该域名来决定将用户归于哪个ISP域，也有RADIUS服务器不能接受 的用户名，此时需要将用户名中携带的域名去除
发送给RADIUS服务器的数据流的单位	发送到RADIUS服务器的数据流的单位
发送给RADIUS服务器的数据包的单位	发送到RADIUS服务器的数据包的单位
在线修改用户密码	用户认证成功后，如果服务器向设备发送携带了Reply-Message属性的Ac 报文，设备会提示用户需要修改密码
Accounting-on	Accounting-on功能使得整个设备在重启之后通过发送Accounting-on报文通 用的RADIUS计费服务器，要求RADIUS服务器停止计费且强制该设备的用
Accounting-on报文的重发时间间隔	设备发送Accounting-on报文后RADIUS服务器无响应时，报文重新发送的
Accounting-on报文的最大发送次数	设备发送Accounting-on报文后RADIUS服务器无响应时，报文发送的最大
Reply-message属性解析规格	配置RADIUS属性的解析规则： • 要求用户输入新密码 • 采用双因子认证机制时，需要用户提交下一个身份认证因素进行二次验

5. 单击<确定>按钮，新建 RADIUS 方案成功，且会在“RADIUS”页面中显示。

配置 LDAP

LDAP 方案的具体配置步骤如下：

1. 选择“对象 > 用户与认证 > 认证管理 > LDAP”。

2. 在“LDAP 方案”页面单击<新建>按钮，进入“新建 LDAP 方案”页面。

3. 在“新建 LDAP 方案”页面的具体配置内容如下所示：

表-5 配置 LDAP 方案参数表

参数	说明
名称	用于唯一标识一个LDAP方案
属性映射表	引用LDAP属性映射表后，可将LDAP授权服务器下发给用户的LDAP属性映 可以解析的某类属性
认证服务器	表示LDAP认证服务器的名称。在LDAP认证服务器中可配置相关参数，用 LDAP认证服务器建立连接
认证服务器DN路径	表示从认证服务器上导入用户、用户组信息的路径，由域名和用户组名组成 级用户组,ou=2级用户组,ou=1级用户组,dc=N级域名,dc=2级域名,dc=1级域 单击<选择>按钮，可选择多条认证服务器上已存在的DN路径

	配置本参数前，需要用户先到指定的LDAP服务器页面配置Base DN
授权服务器	表示LDAP授权服务器的名称。在LDAP授权服务器中可配置相关参数，用 LDAP授权服务器建立连接
忽略 SearchResRef字段	开启此功能，设备将会忽略LDAP查询结果中携带的SearchResultReferenc 前查询到的用户数据，以避免因以下两种情况导致的整体查询失败： • LDAP 服务器部署异常，导致 LDAP 服务器应答查询请求时携带了 SearchResultReference 字段，而设备未能及时完成对 SearchResultR 中所有 URL 的域名解析。 • LDAP 服务器不支持匿名查询功能，设备发起的匿名查询请求被服务器

4. 单击<确定>按钮，新建 LDAP 方案成功，且会在“LDAP 方案”页面中显示。

LDAP 服务器的具体配置步骤如下：

5. 在“LDAP 服务器”页面单击<新建>按钮，进入“新建 LDAP 服务器”页面。

6. 在“新建 LDAP 服务器”页面的具体配置内容如下所示：

表-6 配置 LDAP 服务器参数表

参数	说明
名称	用于唯一标识一个LDAP服务器
VRF	表示远程LDAP服务器所属的VPN，若不配置该参数，则表示LDAP服务器
地址类型	远程LDAP服务器的地址类型包括IPv4和IPv6两种
服务器地址	远程LDAP服务器的IP地址

端口	远程LDAP服务器上使用的端口号 端口缺省值为389，引用SSL客户端策略后，端口的缺省值将变为636
SSL客户端策略	LDAP服务器引用的SSL客户端策略，可以对设备作为SSL客户端与LDAP 的流量进行加密传输
源地址类型	源地址类型包括源IP地址和源接口
源IPv4地址	该IPv4地址为设备向LDAP服务器发送报文时使用的源IP地址
源IPv6地址	该IPv6地址为设备向LDAP服务器发送报文时使用的源IP地址
源接口	源地址类型选择源接口时，需要选择源接口
管理员DN	表示具有管理员权限的用户DN，必须与远程LDAP服务器上管理员的DN一
管理员密码	LDAP服务器上管理员的DN的密码
LDAP版本号	目前设备支持LDAPv2和LDAPv3两个协议版本。设备上配置的LDAP版本 LDAP服务器支持的版本号保持一致
超时时间	设备向远程LDAP服务器发送绑定请求、查询请求，如果经过指定的时间后 务器的回应，则认为本次认证、授权请求超时
用户组过滤条件	设备从LDAP服务器上导入身份识别用户组信息时，LDAP服务器会根据设 条件筛选出符合条件的用户组信息发送给设备
用户过滤条件	缺省情况下，设备从LDAP服务器导入用户信息时，会使用“用户对象类型 成过滤条件进行筛选。配置此用户过滤条件后，设备将使用它来筛选 (objectclass=organizationalUnit)。如需配置多个条件，可以使用(|(条件1)(条
编码格式	配置LDAP服务器使用的字符编码格式
Base DN	远程LDAP服务器上的目录结构可能具有很深的层次，如果从根目录进行用

	耗费的时间将会较长，因此必须配置用户查找的起始点DN，以提高查找效
Base DN查询范围	所有子目录表示在Base DN的所有子目录下进行查询；下一级子目录表示只 下一级子目录下进行查询
用户名称属性	表示用户名属性的值，缺省为cn
用户名称格式	携带ISP域名表示发送给服务器的用户名带ISP域名；不携带ISP域名表示发 用户名不带ISP域名
用户对象类型	表示查询用户DN时使用的用户对象类型

7. 单击<确定>按钮，新建 LDAP 服务器成功，且会在“LDAP 服务器”页面中显示。

LDAP 属性映射表的具体配置步骤如下：

8. 在 LDAP 属性映射表页面，单击<新建>按钮，进入新建 LDAP 属性映射表页面。

9. 配置映射表名称，用于唯一标识一个 LDAP 属性映射表。单击属性区域的<新建>按钮，进入新建 LDAP 属性页面，具体配置内容如下所示：

表-7 配置 LDAP 属性参数表

参数	说明
属性名称	表示要映射的LDAP属性名称
前缀	表示LDAP属性字符串中的某内容前缀（例如cn=）
分隔符	表示LDAP属性字符串中的内容分隔符（例如逗号）。若不指定该参数，则表 属性字符串是一个整体，不需要内容分隔

AAA属性	表示要映射为的AAA属性，包含Mobile number类型、User group类型和U

10. 单击<确定>按钮，新建 LDAP 属性映射表成功，且会在“LDAP 属性映射表”页面中显示。

配置 RESTful 服务器

RESTful 服务器的具体配置步骤如下：

1. 选择“对象 > 用户与认证 > 认证管理 > RESTful 服务器”。
2. 在“RESTful 服务器”页面单击<新建>按钮，进入“新建 RESTful 服务器”页面。
3. 在“新建 RESTful 服务器”页面的具体配置内容如下所示：

表-8 配置 RESTful 服务器参数表

参数	说明
名称	用来唯一标识一个RESTful服务器
用户名	表示与远程RESTful服务器认证使用的管理员的名称
密码	表示与远程RESTful服务器认证使用的管理员的密码
获取用户账户的URI	表示远程RESTful服务器上提供用户账户的URI
获取在线用户的URI	表示远程RESTful服务器上提供在线用户的URI

获取用户组的URI	表示远程RESTful服务器上提供用户组的URI
上传在线用户的URI	新增一个在线用户时，若该用户来源不是指定的RESTful服务器，则设备会 户信息上传给RESTful服务器
上传下线用户的URI	删除一个在线用户时，若该用户来源不是指定的RESTful服务器，则设备会 户信息上传给RESTful服务器
VRF	表示远程RESTful服务器所属的VPN，若不配置该参数，则表示RESTful服
开启探测功能	开启此功能后，设备将与该RESTful服务器进行交互，并返回设备与RESTf 状态值，探测与RESTful服务器的连接状态（可达或者不可达）
探测时间间隔	设备探测RESTful服务器的时间间隔
最大探测次数	设备探测RESTful服务器重试的最大次数

4. 单击<确定>按钮，新建 RESTful 服务器成功，且会在“RESTful 服务器”页面中显示。

配置 Sec Manage 服务器

Sec Manage 服务器的具体配置步骤如下：

1. 选择“对象 > 用户与认证 > 认证管理 > Sec Manage 服务器”。
2. 在“Sec Manage 服务器”页面单击<新建>按钮，进入“新建 Sec Manage 服务器”页面。
3. 在“新建 Sec Manage 服务器”页面的具体配置内容如下所示：

表-9 配置 Sec Manage 服务器参数表

参数	说明
名称	用于唯一标识一个Sec Manage服务器
服务器地址	表示远程TSM服务器的IP地址
监听端口	表示远程TSM服务器发送消息的目的端口号
加密算法	表示解密远程TSM服务器发送消息时，使用的加密算法
共享密钥	表示解密远程TSM服务器发送消息时，使用的密钥

4. 单击<确定>按钮，新建 Sec Manage 服务器成功，且会在“Sec Manage 服务器”页面中显示。

数据过滤

本帮助主要介绍以下内容：

- 特性简介
  - 基本概念
  - 数据过滤的实现原理
- vSystem 相关说明
- 使用限制和注意事项
  - 关于提交操作的注意事项
  - 关于正则表达式的使用限制
- 配置指南
  - 配置思路
  - 配置准备
  - 缺省数据过滤配置任务
  - 定制化数据过滤配置任务

特性简介

数据过滤是一种对流经设备的报文的应用层信息进行过滤的安全防护机制。采用数据过滤功能可以有效防止内网机密信息泄露，禁止内网用户在 Internet 上浏览、发布和传播违规或违法信息。目前，数据过滤功能支持对基于以下应用层协议传输的应用层信息进行检测和过滤。

- HTTP（Hypertext Transfer Protocol，超文本传输协议）
- FTP（File Transfer Protocol，文件传输协议）
- SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）
- IMAP（Internet Mail Access Protocol，Internet 邮件访问协议）
- NFS（Network File System，网络文件系统）
- POP3（Post Office Protocol - Version 3，邮局协议版本 3）
- RTMP（Real Time Messaging Protocol，实时消息传输协议）
- SMB（Server Message Block，服务器信息块）

基本概念

关键字

关键字是用于识别应用层信息特征的字符串。包括预定义关键字和自定义关键字。

- 预定义关键字：由设备生成，包括手机号、银行卡号、信用卡号和身份证号。
- 自定义关键字：管理员自定义的需要识别的关键字，支持文本匹配方式和正则表达式匹配方式。

关键字组

关键字组用来对数据过滤关键字进行统一组织和管理。一个关键字组中可以包含 32 个关键字（包括自定义关键字和预定义关键字），且它们之间是或的关系。

数据过滤规则

数据过滤规则是报文应用层信息安全检测条件及处理动作的集合。在一条规则中可设置关键字组、方向、应用类型和动作（允许、丢弃、生成日志）。只有报文成功匹配规则中包含的所有检测条件才算与此规则匹配成功。

数据过滤的实现原理

设备对报文进行数据过滤处理的整体流程如下：

1. 如果报文匹配了某个安全策略，且此策略**引用**了数据过滤配置文件，则对报文进行数据过滤处理。
2. 设备提取报文中的应用层信息与数据过滤规则进行匹配，并根据匹配结果对报文执行动作：

- 如果报文同时与多条规则匹配成功，则执行这些规则中优先级最高的动作，动作优先级从高到低的顺序为：丢弃 > 允许，但是对于生成日志动作只要匹配成功的规则中已配置就会执行。
- 如果报文只与一条规则匹配成功，则执行此规则中指定的动作。
- 如果报文未与任何数据过滤规则匹配成功，则设备直接允许报文通过。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

关于提交操作的注意事项

- 执行“提交”操作会暂时中断 DPI 业务的处理，可能导致其他基于 DPI 功能的业务同时出现中断。例如，安全策略无法对应用进行访问控制等。
- 执行“提交”操作后，界面上会提示设置成功，但是配置文件此时可能尚未完成激活，如果此时报文经过设备，可能会出现暂时无法识别的情况。

关于正则表达式的使用限制

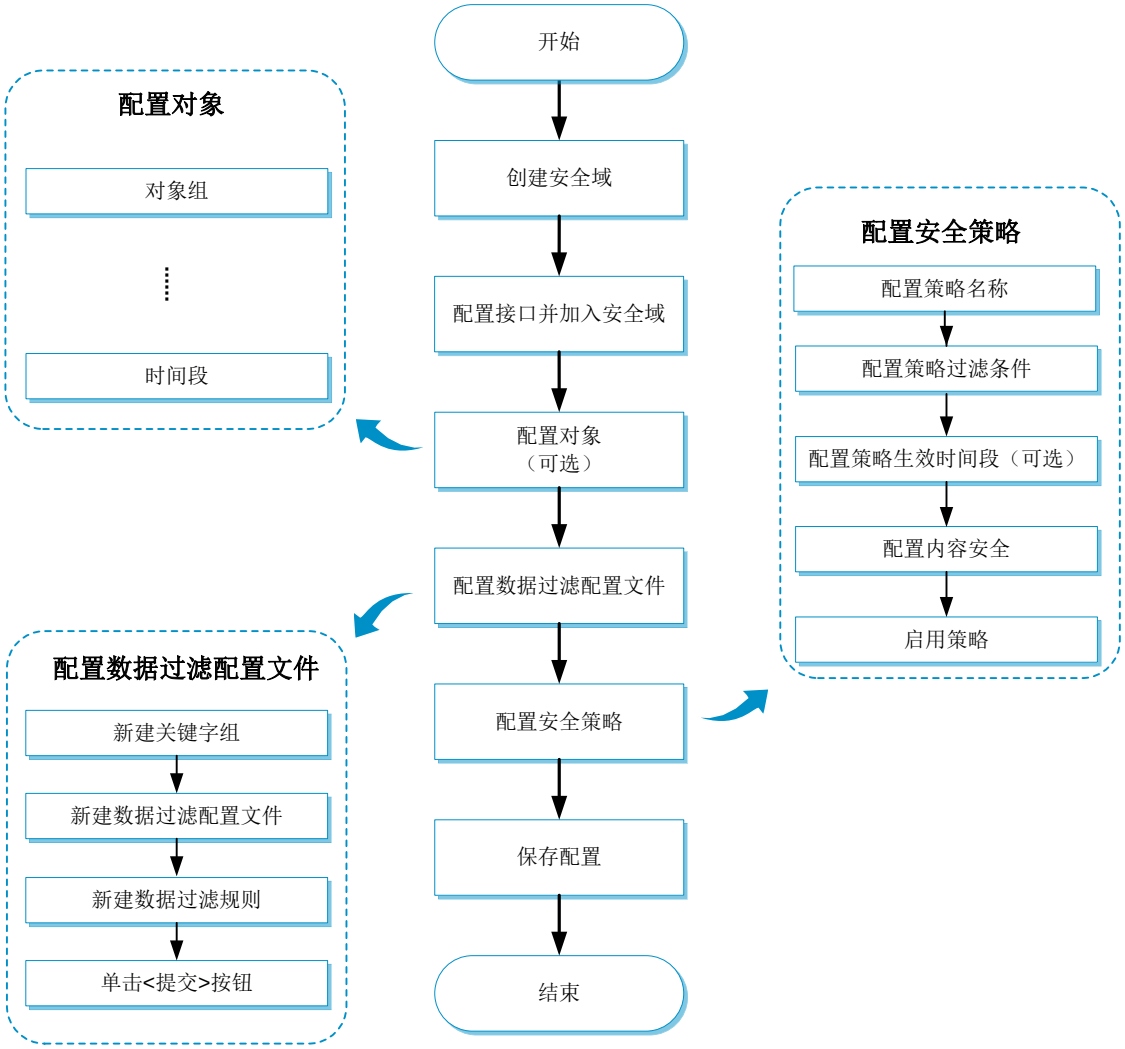
- 正则表达式中，总的分支不能超过四个。例如'abc(c|d|e|\x3D)'有效，'abc(c|onreset|onselect|onchange|style\x3D)'无效。
- 正则表达式中，括号不能嵌套，即括号中不能有括号。例如'ab((abcs*?))'无效。
- 正则表达式中，分支不支持串联，即分支后面不能有分支。例如'ab(a|b)(c|d)^\\r\\n]+?'无效。
- 正则表达式中，零次重复量词'*'和'?'前面必须有四个确定字符。例如'abc*'无效，'abcd*DoS\x2d\d{5}\x20\x2bxi\\r\\nJOIN'有效。

配置指南

配置思路

数据过滤功能的配置思路如下图所示：

图-1 数据过滤功能配置指导图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。

- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

缺省数据过滤配置任务

设备上存在一个名称为 default 的数据过滤配置文件，不可对其进行修改和删除操作。该配置文件对报文支持的所有应用层协议、预定义特征（如手机号、银行卡号、信用卡号和身份证号）的正则表达式匹配方式进行过滤。因此可以使用缺省数据过滤配置文件，从而简化操作并节省时间。

1. 选择“对象 > 安全配置文件> 数据过滤 > 配置文件”。default 的数据过滤配置文件不可编辑。
2. 在安全策略的内容安全配置中引用此数据过滤配置文件，有关安全策略的详细配置介绍请参见“安全策略”。

定制化数据过滤配置任务

当缺省数据过滤配置文件不满足需求时，管理员可以根据业务环境和安全要求，灵活调整自定义数据过滤配置文件中的关键字组等设置，以更好地适应实际情况。

配置关键字组

1. 选择“对象 > 安全配置文件 > 数据过滤 > 关键字组”。

2. 在“关键字组”页面单击<新建>按钮，进入“新建关键字组”页面，具体配置内容如下：

表-1 关键字组配置内容

参数	说明
名称	表示关键字组的名称
描述	通过合理编写描述信息，便于管理员快速理解和识别本关键字组的作用

3. 在“预定义关键字列表”区域，启用预定义关键字。

4. 在“自定义关键字列表”区域，单击<新建>按钮，进入“新建关键字”页面，具体配置内容如下：

表-2 关键字配置内容

参数	说明
名称	表示关键字的名称
匹配模式	包括文本和正则表达式两种： • 文本方式表示对报文进行精确匹配 • 正则表达式方式表示对报文进行模糊匹配

匹配内容	输入关键字的内容

5. 单击<确定>按钮，新建关键字成功，且会在自定义关键字列表中显示。

6. 在“新建关键字组”页面单击<确定>按钮，新建关键字组成功，且会在“关键字组”页面中显示。

新建数据过滤配置文件

1. 选择“对象 > 安全配置文件 > 数据过滤 > 配置文件”。

2. 在“数据过滤配置文件”页面单击<新建>按钮，进入“新建数据过滤配置文件”页面，具体配置内容如下：

表-3 数据过滤配置文件配置内容

参数	说明
名称	表示数据过滤配置文件的名称
描述	通过合理编写描述信息，便于管理员快速理解和识别本数据过滤配置文件的作用

3. 在“数据过滤规则”区域，单击<新建>按钮，进入“新建数据过滤规则”页面，具体配置内容如下：

表-4 数据过滤规则配置内容

参数	说明
名称	表示数据过滤规则的名称
关键字组	指定规则引用的关键字组来对报文的应用层信息进行关键字匹配
应用	指定数据过滤规则的应用层协议，具体包括：FTP、HTTP、IMAP、NFS、POP3、和SMTP协议。可以根据业务应用所属的应用层协议类型来灵活控制对哪些协议类型据过滤
方向	包括上传、下载和双向，可以根据报文传输的方向来灵活控制对哪个方向的报文进行
动作	包括允许和丢弃。允许表示对匹配规则的报文进行放行，丢弃表示对匹配规则的报文
日志	开启日志功能后，对与此规则匹配成功的报文生成日志信息；关闭日志功能后，对与功的报文不会生成日志信息

4. 单击<确定>按钮，新建数据过滤规则成功，且会在“新建数据过滤配置文件”页面的数据过滤规则列表中显示。

5. 在“新建数据过滤配置文件”页面单击<确定>按钮，新建数据过滤配置文件成功，且会在“数据过滤配置文件”页面中显示。

6. 在安全策略的内容安全配置中引用此数据过滤配置文件，具体配置步骤请参见“缺省数据过滤配置任务”章节。

7. 单击<提交>按钮，激活数据过滤配置文件的配置内容。配置此功能会暂时中断 DPI 业务的处理，为避免重复配置此功能对 DPI 业务造成影响，请完成部署 DPI 各业务模块的配置文件后统一配置此功能。

URL 过滤

本帮助主要介绍以下内容:

- 特性简介
  - URL 简介
  - URL 过滤规则
  - URL 过滤分类
  - URL 过滤配置文件
  - URL 过滤黑/白名单规则
  - URL 过滤分类云端查询
  - URL 过滤动作
  - URL 过滤实现流程
- vSystem 相关说明
- 使用限制和注意事项
  - 关于文本方式匹配中通配符的使用限制
  - 关于正则表达式的使用限制
  - 白名单功能注意事项

- 配置指南
  - 配置思路
  - 配置准备
  - 快速配置 URL 过滤功能
  - 配置 URL 过滤分类
  - 配置云端服务器

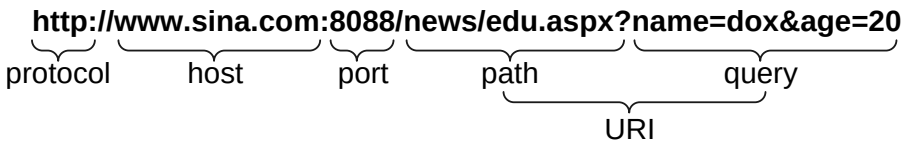
特性简介

URL 过滤功能是指对用户访问的 URL 进行控制，即允许或禁止用户访问的 Web 资源，达到规范用户上网行为的目的。

URL 简介

URL（Uniform Resource Locator，统一资源定位符）是互联网上标准资源的地址。URL 用来完整、精确的描述互联网上的网页或者其他共享资源的地址，URL 格式为：“protocol://hostname[:port]/path/[;parameters][?query]#fragment”，格式示意如图-1 所示：

图-1 URL 格式示意图



URL 各字段含义如表-1 所示：

表-1 URL 各字段含义表

字段	描述
protocol	表示使用的传输协议，例如HTTP
host	表示存放资源的服务器的主机名或IP地址
[:port]	（可选）传输协议的端口号，各种传输协议都有默认的端口号
/path/	是路径，由零或多个“/”符号隔开的字符串，一般用来表示主机上的一个目录或
[parameters]	（可选）用于指定特殊参数
[?query]	（可选）表示查询用于给动态网页传递参数，可有多个参数，用“&”符号隔开，的名和值用“=”符号隔开
URI	URI（Uniform Resource Identifier，统一资源标识符）是一个用于标示某一互联网的字符

URL 过滤规则

URL 过滤功能实现的前提条件是对 URL 的识别。可通过使用 URL 过滤规则匹配 URL 中 host 字段和 URI 字段的方法来识别 URL。

URL 过滤规则是指对用户 HTTP 报文中的 URL 进行匹配的原则，且其分为两种规则：

- 预定义规则：根据设备中的URL过滤特征库自动生成，包括百万级的Host或URI。预定义规则能满足多数情况下的 URL 过滤需求。
- 自定义规则：由管理员手动配置生成，可以通过使用正则表达式或者文本的方式来配置规则中 Host 或 URI 的内容。在配置时，可选择设置 Host 或 URI 字段中的任意一个；若同时配置了 Host 和 URI 字段，则只有两者均匹配上，才能视为命中规则。

URL 过滤规则支持两种匹配方式：

- 文本匹配：使用指定的字符串对 Host 和 URI 字段进行匹配。
    - 匹配主机名字段时，首先判断主机名开头或结尾位置是否含有通配符“*”，若均未出现，则 URL 中的主机名字段与规则中指定的主机名字符串必须完全一致，才能匹配成功；若“*”出现在开头位置，则该字符串或以该字符串结尾的 URL 会匹配成功；若“*”出现在结尾位置，则该字符串或以该字符串开头的 URL 会匹配成功。若“*”同时出现在开头或结尾位置，则该字符串或含有该字符串的 URL 均会匹配成功。
    - 匹配 URI 字段时，和主机名字段匹配规则一致。

- 正则表达式匹配：使用正则表达式对 Host 和 URI 字段进行匹配。例如，规则中配置 host 的正则表达式为 sina.*cn，则 Host 为 news.sina.com.cn 的 URL 会匹配成功。

URL 过滤分类

为便于管理员对数目众多的 URL 过滤规则进行统一部署，URL 过滤模块提供了 URL 过滤分类功能，以便对具有相似特征的 URL 过滤规则进行归纳以及为匹配这些规则的 URL 统一指定处理动作。每个 URL 过滤分类具有一个严重级别属性，该属性值表示对属于此过滤分类 URL 的处理优先级，数值越大表示严重级别越高。

URL 过滤分类包括两种类型：

- 预定义分类：根据设备中的 URL 过滤特征库自动生成，其严重级别不可被修改。
- 自定义分类：由管理员手动配置，可修改其严重级别，可添加 URL 过滤规则。

URL 过滤配置文件

URL 过滤配置文件是用于关联所有 URL 过滤配置的一个实体。一个 URL 过滤配置文件中可以配置 URL 过滤分类和处理动作的绑定关系，以及缺省动作（即对未匹配上任何 URL 过滤规则的报文采取的动作）。

URL 过滤黑/白名单规则

URL 过滤黑/白名单规则功能根据应用层的信息进行 URL 过滤。如果用户 HTTP 报文中的 URL 与 URL 过滤配置文件中的黑名单规则匹配成功，则丢弃此报文；如果与白名单规则匹配成功，则允许此报文通过。在配置时，可选择设置 Host 或 URI 字段中的任意一个；若同时配置了 Host 和 URI 字段，则只有两者均匹配上，才能视为命中规则。

URL 过滤分类云端查询

在 URL 过滤配置文件中开启 URL 过滤分类云端查询功能后，如果流经设备 HTTP 报文中的 URL 与该 URL 过滤配置文件中的过滤规则匹配失败，则此 URL 将会被发向云端 URL 过滤分类服务器进行查询。云端 URL 过滤分类服务器响应该请求，并向设备发送查询结果，该结果中包含了 URL 过滤规则及其所属的分类名称，设备根据该结果执行相应的分类处理动作。如果云端返回的分类在设备上没有与其对应的分类动作或者云端 URL 查询失败，则设备将对此报文执行 URL 过滤配置文件中的缺省动作。

DTLS 协议：表示（Datagram Transport Layer Security，数据报传输层安全）是一种用于保护数据报协议的安全协议。适用于低延迟的场景，如实时通信（VoIP、视频会议）、物联网设备（无线传感器网络）和流媒体服务。

HTTPS 协议：表示（HyperText Transfer Protocol Secure）是一种用于通过安全通信通道传输超文本数据的协议。适用于所有需要保护数据传输安全的场景，如在线银行、社交媒体平台、邮件服务和任何需要用户身份验证和数据加密的 Web 应用。

URL 过滤动作

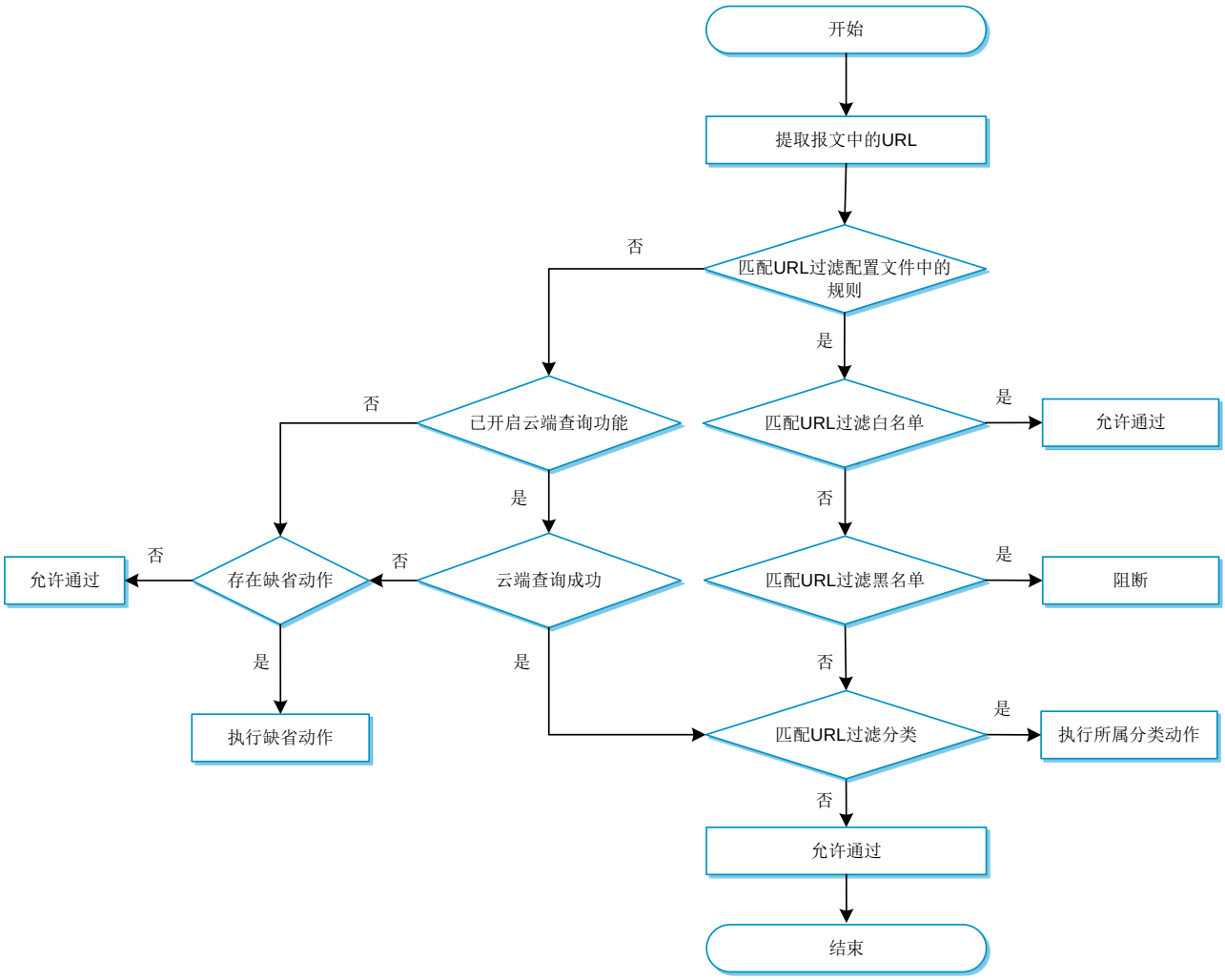
URL 过滤配置文件中可以设置配置文件的缺省动作和 URL 分类的动作，动作具体包括如下：

- 黑名单：表示将该报文的源 IP 地址加入 IP 黑名单。若设备上同时开启了 IP 黑名单过滤功能，则一定时间内（安全动作指定的 URL 过滤的阻断时间）来自此 IP 地址的所有报文将被直接丢弃；若没有开启 IP 黑名单过滤功能，则此 IP 黑名单不生效。有关 IP 黑名单过滤功能的详细介绍请参见“攻击防范”。
- 丢弃：表示丢弃报文。
- 允许：表示允许报文通过。
- 重定向：表示重定向动作，把符合特征的报文重定向到指定的 Web 页面上。
- 重置：表示通过发送 TCP 的 reset 报文从而使 TCP 连接断开。
- 记录日志：表示生成报文日志动作。开启记录日志功能后此动作才能生效。

URL 过滤实现流程

在开启 URL 过滤功能的情况下，当用户通过设备使用 HTTP 访问某个网络资源时，设备将进行 URL 过滤。URL 过滤处理流程如图-2 所示：

图-2 URL 过滤实现流程图



URL 过滤实现流程如下：

2. 如果报文匹配了某个安全策略，且此策略的动作是允许并引用了 URL 过滤配置文件，则设备提取报文中的 URL 字段进行 URL 过滤规则匹配。
3. 如果报文与设备上 URL 过滤配置文件中的过滤规则匹配成功，则将进一步做如下判断：
4. 首先判断此 URL 过滤规则是否属于 URL 过滤的黑/白名单规则。如果属于 URL 过滤白名单规则，则直接允许此报文通过；如果属于 URL 过滤的黑名单规则，则直接将此报文阻断。
5. 如果此 URL 过滤规则既不属于 URL 过滤白名单规则也不属于 URL 过滤黑名单规则，则设备将进行如下判断。
    - 如果此 URL 过滤规则属于自定义 URL 过滤分类，则进一步判断是否同时属于多个自定义 URL 过滤分类。如果属于多个自定义 URL 过滤分类，则根据严重级别最高的 URL 过滤分类的动作对此报文进行处理；如果仅属于一个自定义 URL 过滤分类，则根据该分类的动作对报文进行处理。
    - 如果设备上启用了 URL 信誉功能，则判断此 URL 过滤规则是否属于 URL 信誉特征库中的某个攻击分类。如果属于，则根据该攻击分类的动作对报文进行处理。
    - 如果此 URL 过滤规则属于预定义 URL 过滤分类，则进一步判断是否属于多个预定义 URL 过滤分类。如果属于多个预定义 URL 过滤分类，则根据严重级别最高的 URL 过滤分类的动作对报文进行处理；如果仅匹配一个预定义 URL 过滤分类，则根据该分类的动作对报文进行处理。
6. 如果报文未匹配上任何一条 URL 过滤配置文件中的过滤规则，则将进一步判断 URL 过滤配置文件中是否开启了 URL 过滤分类云端查询功能。如果分类云端查询功能已开启，则将报文中的 URL 发向云端 URL 过滤分类服务器进行查询，否则进行第 7 步的判断。

7. 如果URL云端查询成功，则进行步骤4中对自定义URL过滤分类和预定义URL分类的判断，否则进行步骤 7 的判断。

8. 如果设备上配置了 URL 过滤的缺省动作，则根据配置的缺省动作对此报文进行处理；否则直接允许报文通过。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

关于提交操作的注意事项

- 执行“提交”操作会暂时中断 DPI 业务的处理，可能导致其他基于 DPI 功能的业务同时出现中断。例如，安全策略无法对应用进行访问控制等。
- 执行“提交”操作后，界面上会提示设置成功，但是配置文件此时可能尚未完成激活，如果此时报文经过设备，可能会出现暂时无法识别的情况。

关于文本方式匹配中通配符的使用限制

使用文本方式对主机名和 URI 字段进行匹配时，对星号“*”有如下的限制：

- 匹配主机名字段时，“*”只能出现在开头或结尾，表示通配符，代表 0 到多个任意字符。
- 匹配 URI 字段时，当“*”出现在开头或结尾，表示通配符，代表 0 到多个任意字符；当“*”出现在其他位置时，则作为普通字符进行匹配。

关于正则表达式的使用限制

- 正则表达式中，总的分支不能超过四个。例如'abc(c|d|e|\x3D)'有效，'abc(c|onreset|onselect|onchange|style\x3D)'无效。
- 正则表达式中，括号不能嵌套，即括号中不能有括号。例如'ab((abcs*?))'无效。
- 正则表达式中，分支不支持串联，即分支后面不能有分支。例如'ab(a|b)(c|d)^\\r\\n]+?'无效。
- 正则表达式中，零次重复量词'*'和'?'前面必须有四个确定字符。例如'abc*'无效，'abcd*DoS\x2d\d{5}\x20\x2bxi\\r\\nJOIN'有效。

白名单功能注意事项

- 当报文匹配白名单规则时，URL 过滤日志中的 URL 过滤分类将显示为白名单。

- 开启内嵌白名单功能后，当报文与白名单内嵌的网页链接匹配成功时，URL 过滤日志中的 URL 过滤分类将显示为内嵌白名单。
- 开启白名单模式后，当报文与白名单规则匹配失败时，URL 过滤日志中的 URL 过滤分类将显示为黑名单。
- 开启白名单模式后，URL 过滤日志仅支持发送快速日志，不支持发送系统日志。有关 URL 过滤日志的详细介绍，请参见“日志设置基本配置”。

URL 过滤分类云端查询注意事项

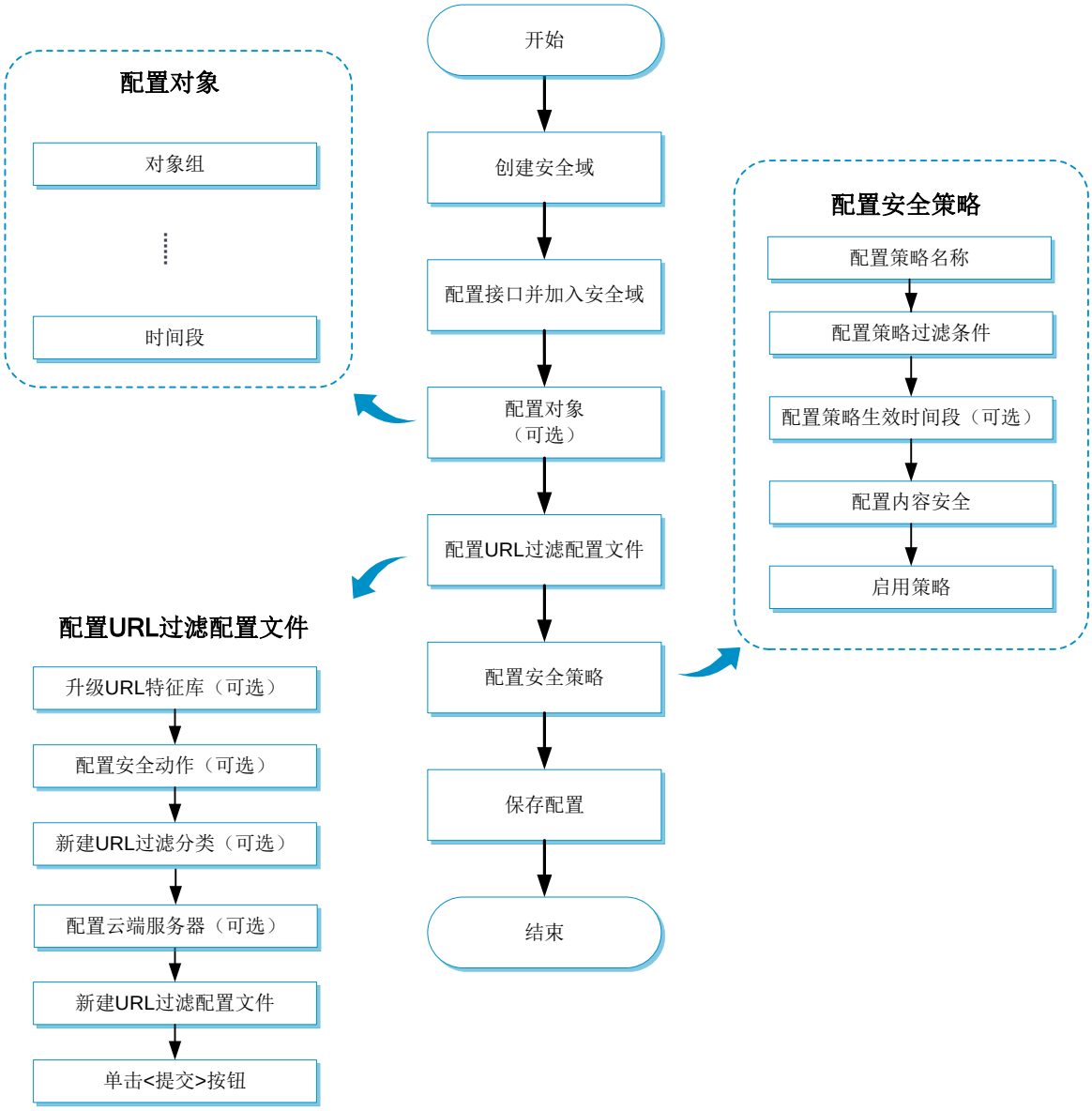
- URL 过滤分类云端查询功能的支持情况与设备型号有关，请以页面的实际显示为准。
- 在使用基于 HTTPS 协议的 URL 过滤分类云端查询功能时，当网络状态发生变更，可通过手动触发设备重新注册云端服务器，或等待网络流量自动触发云端请求。

配置指南

配置思路

URL 过滤功能的配置思路如下图所示：

图-3 URL 过滤功能配置指导图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

快速配置 URL 过滤功能

在一个 URL 过滤配置文件中可以开启云端查询功能，可以配置文件的缺省动作，可以配置黑/白名单，也可以为不同的 URL 分类指定不同的动作。

若报文成功匹配的 URL 过滤规则同属于多个 URL 分类，则根据严重级别最高的 URL 过滤中指定的动作对此报文进行处理。

白名单的优先级高于黑名单的优先级。

URL 过滤配置文件的具体配置步骤如下：

1. 选择“对象 > 安全配置文件 > URL 过滤 > 配置文件”。
2. 在“URL 过滤配置文件”页面单击<新建>按钮，进入“新建 URL 过滤配置文件”页面，具体配置内容如下：

表-2 URL 过滤配置文件配置内容

参数	说明
名称	URL过滤配置文件的名称
缺省动作	当报文没有与URL过滤配置文件中的规则匹配成功时，设备将根据配置文件中配置的 报文进行处理。缺省动作包括丢弃、允许、黑名单、重置和重定向
开启云端查询功能	开启此功能后，若流经设备HTTP报文中的URL与该URL过滤配置文件中的过滤规则 URL将会被发向云端URL过滤分类服务器进行查询
记录日志	URL过滤日志是为了满足管理员审计需求。开启记录日志功能后，设备将对与URL过 功的报文生成日志信息，配置记录日志动作前需要先配置缺省动作
告警信息模板	配置本模板后，当设备阻断某网站的访问时，可以向客户端返回告警信息 模板的具体配置说明请参见“安全动作”
开启HTTPS流量过滤功能	开启本功能后，设备可以对未解密的HTTPS流量进行URL过滤 如果同时开启了SSL解密功能，本功能将失效。有关SSL解密功能的详细介绍，请参
开启内嵌白名单功能	开启本功能后，设备允许用户访问白名单网页下内嵌的其他网页链接
白名单模式	开启本功能后，设备仅允许用户访问URL过滤白名单中的网站，其他网站均不允许访
白名单	若报文与白名单中的规则匹配成功，则直接允许此报文通过
黑名单	若报文与黑名单中的规则匹配成功，则直接丢弃此报文
URL过滤分类动作	若报文成功匹配的URL过滤规则同属于多个URL过滤分类，则根据严重级别最高的U 指定的动作对此报文进行处理；若报文成功匹配的URL过滤规则只属于一个URL过滤 该规则所属的URL过滤分类的动作对此报文进行处理。动作包括丢弃、允许、黑名单

	向和记录日志。其中，配置记录日志动作前需要先配置其他动作
URL信誉	URL信誉功能用于阻断恶意URL。开启URL信誉功能后，设备将提取报文中的URL与 库进行匹配，匹配成功则执行URL所属攻击类型的动作，如果匹配失败，则放行该报
动作配置	本功能用于配置URL所属攻击类型的动作，当报文中提取的URL与URL信誉特征库匹 对报文执行URL所属攻击类型的动作

3. 单击<确定>按钮，新建 URL 配置文件成功，且会在“URL 过滤配置文件”页面中显示。
4. 在安全策略的内容安全配置中引用此 URL 过滤配置文件，有关安全策略的详细配置介绍请参见“安全策略”。
5. 单击<提交>按钮，激活 URL 过滤配置文件的配置内容。配置此功能会暂时中断 DPI 业务的处理，为避免重复配置此功能对 DPI 业务造成影响，请完成部署 DPI 各业务模块的配置文件后统一配置此功能。

配置 URL 过滤分类

当 URL 特征库中预定义的 URL 过滤分类和 URL 过滤规则不能满足对 URL 的控制需求时，可以新建 URL 过滤分类，并在分类中创建 URL 过滤规则。每个 URL 过滤规则可以同时属于多个 URL 过滤分类。

新建自定义 URL 过滤分类的配置步骤如下：

1. 选择“对象 > 安全配置文件 > URL 过滤 > URL 分类”。

2. 在“URL 分类”页面单击<新建>按钮，进入“新建自定义 URL 过滤分类”页面，具体配置内容如下：

表-3 自定义 URL 过滤分类配置内容

参数	说明
名称	URL分类的名称，不能以字符”Pre-“开头，因为Pre-是预定义的URL分类名称
描述	通过合理编写描述信息，便于管理员快速理解和识别URL分类的作用，有利于后期维
优先级	URL的严重级别属性，创建URL过滤分类时必须配置此参数，数值越大表示严重级别的URL过滤分类的严重级别不能相同
包含预定义分类	为指定的URL过滤分类添加预定义分类中的所有URL规则

3. 单击<添加>按钮，添加URL。主机名表示对URL中的主机名字段进行过滤，URI表示对URL中的URI字段进行过滤。文本表示使用指定的字符串对主机名和URI字段进行匹配，正则表达式表示使用正则表达式对主机名和URI字段进行匹配。

4. 单击<确定>按钮，添加 URL 成功，返回新建自定义 URL 过滤分类页面。

5. 单击<确定>按钮，新建自定义 URL 过滤分类成功，且会在“URL 过滤分类”页面的自定义分类中显示。

配置云端服务器

在 URL 过滤策略中开启 URL 过滤分类云端查询功能后，可提高设备识别 HTTP 报文的准确率，实现对报文的准确控制。

从云端服务器学习到的 URL 过滤规则会被缓存在设备的 URL 过滤缓存中进行报文匹配。URL 过滤缓存的记录上限和规则的最短保留时间可以根据实际组网环境进行调整。

云端服务器的具体配置步骤如下：

1. 选择“对象 > 安全配置文件 > URL 过滤 > URL 分类”。
2. 在“URL 分类”页面单击“云端服务器连接状态”右边的<配置>按钮，进入“配置云端服务器”页面。云端服务器的具体配置内容如下：

表-4 云端服务器配置内容

参数	说明
服务器地址	云端服务器的地址，支持输入IP地址或者域名。目前，仅支持配置我司云端服务器
缓存URL条数	设备会将云端服务器返回的查询结果缓存在URL过滤缓存中，本参数用于配置URL过缓存的URL条数
缓存最短保留时间	本参数用于配置URL缓存的最短保留时长。未达到最短保留时间的URL不会被删除。URL缓存条数小于当前已缓存的数目时，设备将从URL过滤缓存中删除最老的URL，达到最短保留时间，也将被删除
协议	云端服务器的协议，支持DTLS和HTTPS协议

	• DTLS 协议：适用于低延迟的场景。如实时通信（VoIP、视频会议）、物联网设器网络）和流媒体服务 • HTTPS 协议：适用于所有需要保护数据传输安全的场景。如在线银行、社交媒服务和任何需要用户身份验证和数据加密的 Web 应用
配置代理服务器	配置代理服务器的地址、端口和登录代理服务器使用的用户名及密码。仅设置云端HTTPS时支持此参数

3. 单击<确定>按钮，完成云端服务器的配置。

文件过滤

本帮助主要介绍以下内容：

- 特性简介
  - 基本概念
  - 文件过滤的实现原理
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置思路
  - 配置准备
  - 缺省文件过滤配置任务
  - 定制化文件过滤配置任务
  - 全局配置（文件扩展名不匹配时动作）

特性简介

文件过滤是一种根据文件扩展名信息对经设备传输的文件进行过滤的安全防护机制。采用文件过滤功能可以对指定类型的文件进行批量过滤。目前，文件过滤功能支持对基于以下应用层协议传输的文件进行检测和过滤。

- HTTP（Hypertext Transfer Protocol，超文本传输协议）
- FTP（File Transfer Protocol，文件传输协议）
- SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）
- IMAP（Internet Mail Access Protocol，Internet 邮件访问协议）
- NFS（Network File System，网络文件系统）
- POP3（Post Office Protocol - Version 3，邮局协议版本 3）
- RTMP（Real Time Messaging Protocol，实时消息传输协议）
- SMB（Server Message Block，服务器信息块）

基本概念

文件类型组

文件类型组用来对扩展名进行统一组织和管理。一个文件类型组中可以包含 32 个扩展名（包括自定义扩展名和预定义扩展名），且它们之间是或的关系。

文件过滤规则

文件过滤规则是安全检测条件及处理动作的集合。在一条规则中可配置的检测条件包括文件类型组、方向、应用，可配置的处理动作包括丢弃、允许和记录日志。只有文件属性（包括文件的应用类型、传输方向和扩展名）成功匹配规则中包含的所有检测条件才算与此规则匹配成功。

全局配置

全局配置定义了文件扩展名不匹配时动作，对所有 DPI 业务生效。

文件扩展名不匹配时动作是指，当设备检测出文件的真实类型与其扩展名不一致时，如果动作配置为允许，则根据识别出的真实的文件类型与文件过滤规则进行匹配并执行文件过滤规则中的动作；如果动作配置为丢弃，则直接丢弃报文，不再进行文件过滤规则的匹配。

文件过滤的实现原理

设备对报文进行文件过滤处理的整体流程如下：

1. 如果报文匹配了某个安全策略，且此策略引用了文件过滤配置文件，则对报文进行文件过滤处理。
2. 设备提取文件的扩展名信息并记录。
3. 设备进一步识别文件真实类型，并将识别的结果与扩展名进行匹配。如果设备不能识别出文件真实类型，则根据文件扩展名与文件过滤规则进行匹配，并进入步骤 4 处理。
    - 如果识别结果与扩展名一致，则使用扩展名与文件过滤规则进行匹配，并进入步骤4处理；
    - 如果识别结果与扩展名不一致，则查看文件扩展名不匹配时动作，如果动作为丢弃，则直接丢弃报文，不再进行文件过滤规则的匹配；如果动作为允许，则使用文件的真实类型与文件过滤规则进行匹配，并进入步骤 4 处理。
4. 与文件过滤规则进行匹配，并根据匹配结果对报文执行以下动作：
    - 如果文件的扩展名信息/真实类型同时与多条文件过滤规则匹配成功，则执行这些规则中优先级最高的动作，动作优先级从高到低的顺序为：丢弃 > 允许，但是对于日志动作只要匹配成功的规则中存在就会执行；
    - 如果文件的扩展名信息/真实类型只与一条文件过滤规则匹配成功，则执行此规则中指定的动作。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

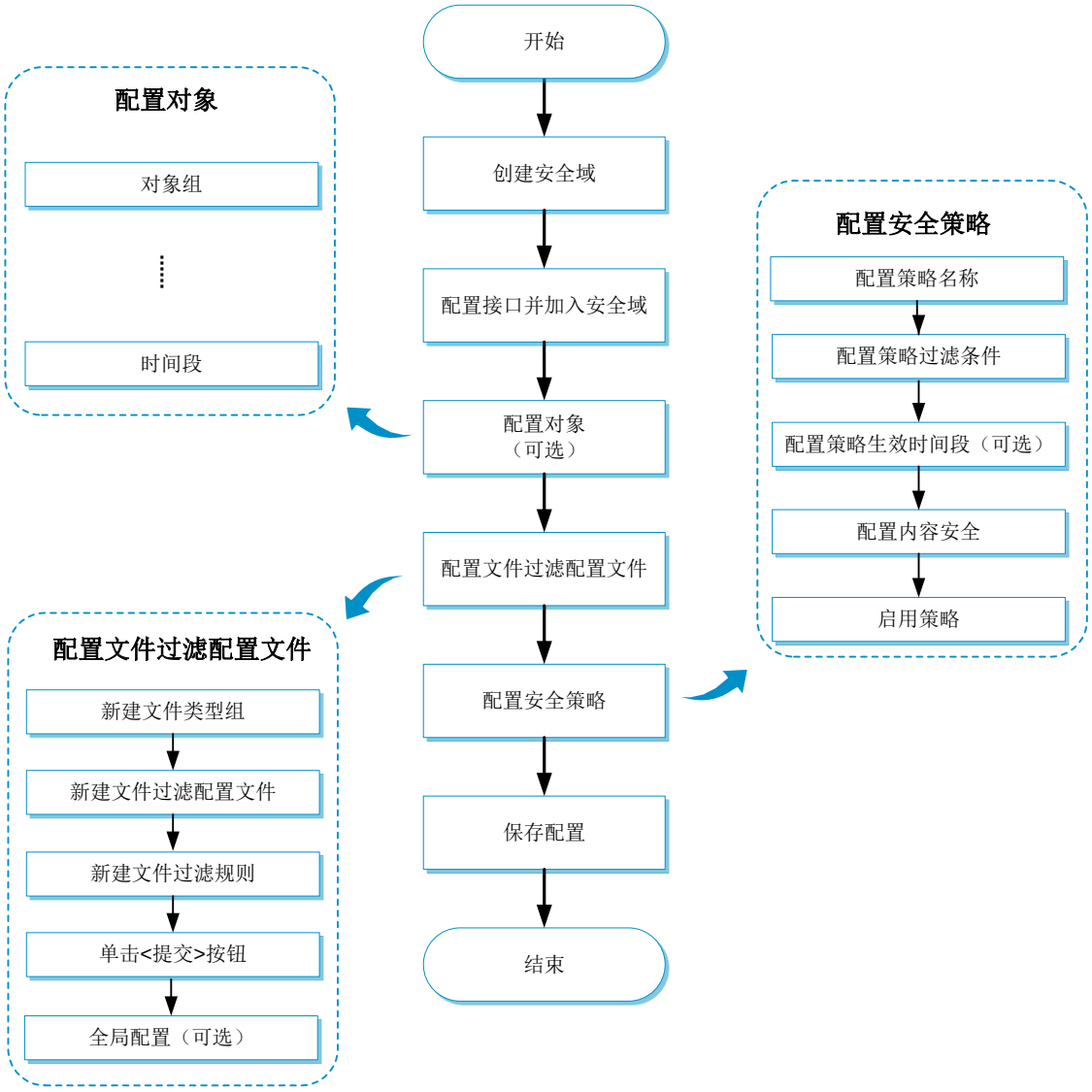
- 执行“提交”操作会暂时中断 DPI 业务的处理，可能导致其他基于 DPI 功能的业务同时出现中断。例如，安全策略无法对应用进行访问控制等。
- 执行“提交”操作后，界面上会提示设置成功，但是配置文件此时可能尚未完成激活，如果此时报文经过设备，可能会出现暂时无法识别的情况。

配置指南

配置思路

文件过滤功能的配置思路如下图所示：

图-1 文件过滤功能配置指导图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

缺省文件过滤配置任务

设备上存在一个名称为 default 的文件过滤配置文件，不可对其进行修改和删除操作。该配置文件对报文支持的所有应用层协议、设备上已预定义的扩展名进行过滤。因此可以使用缺省文件过滤配置文件，从而简化操作并节省时间。

1. 选择“对象 > 安全配置文件> 文件过滤 > 配置文件”。default 的文件过滤配置文件不可编辑。
2. 在安全策略的内容安全配置中引用此文件过滤配置文件，有关安全策略的详细配置介绍请参见“安全策略”。

定制化文件过滤配置任务

当缺省文件过滤配置文件不满足需求时，管理员可以根据业务环境和安全要求，灵活调整自定义文件过滤配置文件中的文件过滤规则等设置，以更好地适应实际情况。

配置文件类型组

文件类型组的配置步骤如下：

1. 选择“对象 > 安全配置文件 > 文件过滤 > 文件类型组”。
2. 在“文件类型组”页面单击<新建>按钮，进入“新建文件类型组”页面，具体配置内容如下：

表-1 文件类型组配置内容

参数	说明
名称	表示文件类型组的名称
描述	通过合理编写描述信息，便于管理员快速理解和识别本文件类型组的作用
预定义扩展名	可在此处快速选择设备上已预定义的扩展名
自定义扩展名	当设备上预定义扩展名不能满足需求时，可在此处配置自定义的扩展名

3. 单击<确定>按钮，新建文件类型组成功，且会在“文件类型组”页面中显示。

配置文件过滤配置文件

管理员可以根据实际需求创建自定义的文件过滤配置文件。

文件过滤配置文件的配置步骤如下：

1. 选择“对象 > 安全配置文件 > 文件过滤 > 配置文件”。

2. 在“文件过滤配置文件”页面单击<新建>按钮，进入“新建文件过滤配置文件”页面，具体配置内容如下：

表-2 文件过滤配置文件配置内容

参数	说明
名称	表示文件过滤配置文件的名称
描述	通过合理编写描述信息，便于管理员快速理解和识别本文件过滤配置文件的作用

3. 在“新建文件过滤配置文件”页面的“文件过滤规则”区域，单击<新建>按钮，进入“新建文件过滤规则”页面，具体配置内容如下：

表-3 文件过滤规则配置内容

参数	说明
名称	表示文件过滤规则的名称

应用	指定文件过滤规则的应用层协议，具体包括：FTP、HTTP、IMAP、NFS、POP3、和SMTP协议。可以根据业务应用所属的应用层协议类型来灵活控制对哪些协议类型件过滤
文件类型组	指定规则引用的文件类型组来对文件的扩展名信息进行精确匹配
方向	包括上传、下载和双向，可以根据报文传输的方向来灵活控制对哪个方向的报文进行
动作	包括允许和丢弃。允许表示对匹配规则的报文进行放行，丢弃表示对匹配规则的报文
日志	开启日志功能后，对与此规则匹配成功的报文记录日志信息；关闭日志功能后，对与功的报文不会记录日志信息

4. 单击<确定>按钮，新建文件过滤规则成功，且会在“新建文件过滤配置文件”页面的文件过滤规则列表中显示。

5. 在“新建文件过滤配置文件”页面单击<确定>按钮，新建文件过滤配置文件成功，且会在“文件过滤配置文件”页面中显示。

6. 在安全策略的内容安全配置中引用此文件过滤配置文件，具体配置步骤请参见“缺省文件过滤配置任务”章节。

7. 单击<提交>按钮，激活文件过滤配置文件的配置内容。配置此功能会暂时中断 DPI 业务的处理，为避免重复配置此功能对 DPI 业务造成影响，请完成部署 DPI 各业务模块的配置文件后统一配置此功能。

全局配置（文件扩展名不匹配时动作）

全局配置的配置步骤如下：

1. 选择“对象 > 安全配置文件 > 文件过滤 > 配置文件”。
2. 选择“全局配置”页签，配置文件扩展名不匹配时动作。
3. 单击<应用>按钮，完成配置。

APT 防御

本帮助主要介绍以下内容：

- 特性简介
  - APT 防御实现流程
  - 沙箱检测原理
  - APT 防御功能与防病毒功能联动
- vSystem 相关说明
- 配置指南
  - 配置思路
  - 配置准备
  - 缺省 APT 防御配置任务
  - 定制化 APT 防御配置任务

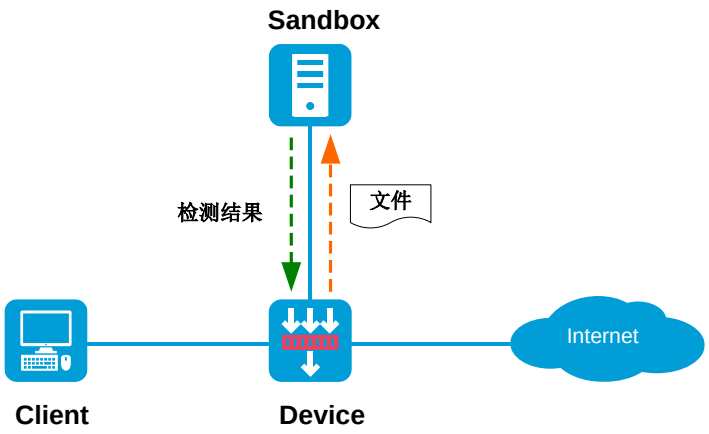
特性简介

APT（Advanced Persistent Threat，高级持续性威胁）攻击，是一种针对特定目标进行长期持续性的网络攻击。目前，沙箱技术是防御 APT 攻击最有效的方法之一，它用于构造隔离的威胁检测环境。设备通过与沙箱进行联动，将网络流量送入沙箱进行隔离分析，由沙箱给出是否存在威胁的结论。如果沙箱检测到某流量为恶意流量，设备将对流量实施阻断等处理。

APT 防御实现流程

在设备配置了 APT 防御功能的情况下，当流量经过设备时，设备将进行 APT 防御处理。处理流程如下图所示：

图-1 APT 防御实现流程



2. 外网的攻击者向企业内网发起 APT 攻击，攻击流量命中设备上的 APT 防御配置文件。

3. 设备对攻击流量中的文件进行还原，并将还原后的文件送往沙箱进行威胁分析。

4. 沙箱获取到文件后将运行该文件，并对运行后的行为进行检测分析。检测结束后，会向设备推送检测结果，并将检测结果缓存到 APT 缓存中。

5. 如果检测结果是恶意流量，则设备将根据配置的防病毒配置文件对后续流量进行阻断或告警等处理，保护企业内网免遭攻击。

沙箱检测原理

沙箱可以看作是一个模拟真实网络建造的虚拟检测系统，当未知文件上送沙箱处理后，沙箱会运行该文件，并会对运行后的行为进行记录。沙箱通过将未知文件的行为和沙箱独有的行为特征库进行匹配，最后给出文件是否为威胁的结论。沙箱的行为特征库是通过分析大量的病毒、漏洞、威胁特征，提炼出各种恶意行为的规律和模式，形成的一套判断规则，它能够提供准确的检测结果。

与根据被检测对象的特征进行识别的检测技术（如防病毒）不同的是，沙箱检测是根据被检测对象的行为进行识别。因此具有可以识别未知文件的优点，可以更好的防御未知威胁。

APT 防御功能与防病毒功能联动

设备收到沙箱推送的检测结果后，如果需要对攻击流量进行进一步的处理，则需要与防病毒功能进行联动。配置防病毒功能后，当后续恶意流量流经设备时，设备将识别恶意流量的应用层协议，并

与防病毒配置文件进行匹配，再根据匹配到的防病毒配置文件中对应的协议报文执行的动作对恶意流量进行处理。

如果用户只想根据检测结果确定当前流量是否为恶意流量，而不需要对流量进行阻断，则对防病毒功能是否配置不作要求。

有关防病毒功能的详细介绍，请参见“防病毒联机帮助”。

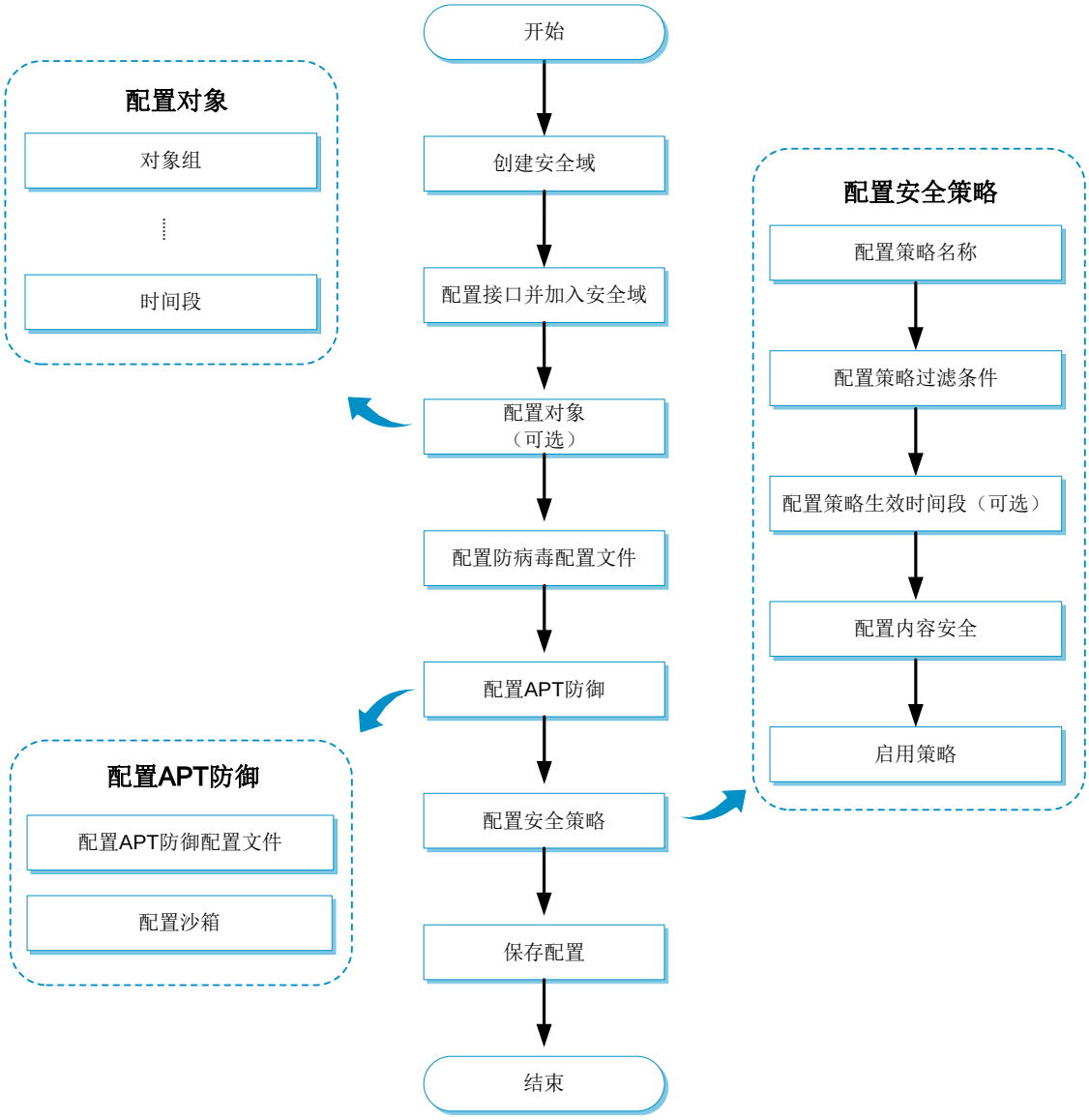
vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置思路

APT 防御功能的配置思路如下图所示：



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。

- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

缺省 APT 防御配置任务

设备上存在一个名称为 default 的 APT 防御配置文件，不可对其进行修改和删除操作。如果需要检测当前系统中的所有应用层协议、检测全部文件类型和送往沙箱检测的文件传输方向为上传和下载时，可使用缺省 APT 配置文件，从而简化操作并节省时间。

配置沙箱

沙箱的具体配置步骤如下：

1. 选择“对象 > 安全配置文件 > APT 防御 > 沙箱”。
2. 沙箱的具体配置内容如下：

表-1 沙箱配置参数

参数	说明
连接状态	显示沙箱的连接状态

开启沙箱联动功能	开启本功能后，设备将匹配APT防御配置文件的流量送往沙箱进行检测
沙箱地址	沙箱的IP地址或域名
协议	设备与沙箱传输数据的协议 目前仅支持使用HTTPS协议，可为数据传输过程加密
用户名	登录沙箱的用户名
密码	登录沙箱的用户密码
缓存记录条数	设备会将沙箱返回的查询结果缓存在设备中，缓存中分为命中列表和非命中列表： • 非命中列表：表示该 MD5 值不属于威胁或不确定是否属于威胁 • 命中列表：表示该 MD5 值属于威胁 本参数用于配置两个列表中分别可以缓存的MD5条数
配置送往沙箱检测的文件大小上限	设置流量还原和文件检测支持的文件类型及大小上限

3. 单击<应用>按钮，完成沙箱的配置。

在安全策略中引用 APT 配置文件

1. 选择“对象 > 安全配置文件> APT 防御 > 配置文件”。default 的 APT 防御配置文件不可编辑。
2. 在安全策略的内容安全配置中引用此 APT 防御配置文件，有关安全策略的详细配置介绍请参见“安全策略”。

定制化 APT 防御配置任务

当缺省 APT 配置文件不满足需求时，管理员可以根据业务环境和安全要求，灵活调整自定义 APT 配置文件中的 APT 防御检测的应用层协议类型、沙箱检测的文件类型或者检测流量的方向设置，以更好地适应实际情况。

1. 选择“对象 > 安全配置文件 > APT 防御 > 配置文件”。

2. 在“APT 防御配置文件”页面单击<新建>按钮，进入“新建 APT 防御配置文件”页面。具体配置内容如下：

表-2 APT 防御配置文件参数

参数	说明
名称	APT防御配置文件的名称
描述	通过合理编写描述信息，便于管理员快速理解和识别APT防御配置文件的作用，有利
应用	APT防御检测的应用层协议类型
文件类型	需要送往沙箱检测的文件类型
方向	需要检测流量的方向，取值包括： • 上传 • 下载 • 双向

3. 单击<确定>按钮，新建APT防御配置文件成功，且会在“APT防御配置文件”页面中显示。

4. 在安全策略的内容安全配置中引用此APT防御配置文件，具体配置步骤请参见“缺省APT防御配置任务”章节。

应用识别

本帮助主要介绍以下内容：

- 特性简介
  - PBAR
  - NBAR
  - 应用组
- vSystem 相关说明
- License 支持情况
- 使用限制和注意事项
- 配置指南
  - 配置准备
  - 配置应用
  - 配置应用组

特性简介

APR（Application Recognition）即应用层协议识别。一些基于应用的业务在进行报文处理时需要知道报文所属的应用层协议，APR 可以为这样的业务提供应用识别服务，并能够对接口上接收或者发送的某个应用层协议的报文进行数目和速率统计。APR 为了更好地识别报文所属的应用层协议，提供了两种应用识别方法：基于端口的应用识别和基于内容特征的应用识别。

- PBAR（Port Based Application Recognition，基于端口的应用层协议识别）：根据定义的应用层协议端口与应用的映射关系识别报文所属的应用层协议。
- NBAR（Network Based Application Recognition，基于内容特征的应用层协议识别）：提取应用报文区别于其它应用报文的特征，通过将报文的内容与特征库中的特征项进行匹配来识别报文所属的应用层协议。

下文中的应用均指设备可以通过 APR 识别出的应用层协议。应用分为预定义应用和自定义应用两种：预定义应用由系统缺省创建；自定义应用由管理员通过配置创建。

PBAR

PBAR（Port Based Application Recognition，基于端口的应用层协议识别）根据预定义的、自定义的端口与应用的映射关系识别出应用层协议。预定义的端口与应用的映射关系由系统预先定义，自定义的端口与应用的映射关系由管理员配置进行创建。

PBAR 提供了以下两种映射机制来维护和使用自定义的端口与应用映射关系：

- 通用端口映射：对管理员自定义端口号和应用层协议建立映射关系。例如：将 2121 端口映射为 FTP 协议，这样所有目的端口是 2121 的报文将被识别为 FTP 报文。
- 主机端口映射：对去往某些特定范围内主机的报文建立自定义端口号和应用层协议的映射。例如：将目的地址为 10.110.0.0/16 网段的、使用 2121 端口的报文映射为 FTP 报文。主机范围可以通过配置 ACL 或者指定主机地址、网段来确定。

NBAR

NBAR 根据报文的内容特征与预定义的特征项或管理员自定义的特征项进行匹配来识别报文所属的应用层协议。预定义的特征项由设备上的 APR 特征库自动生成。

目前设备仅支持预定义 NBAR 类型的应用。

应用组

可以将具有相似特征的应用添加到一个应用组中。一个应用组，就是若干个应用的集合。如果报文被识别为属于某个应用，而该应用又属于某个应用组，则报文相当于被识别为属于某个应用组。基于应用的业务可以对属于同一个应用组的报文做统一处理。

一个自定义应用组中可以包含多个预定义应用和自定义应用。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

License支持情况

NBAR 功能需要安装 License 才能使用。License 过期后，NBAR 功能可以采用设备中已有的 APR 特征库正常工作，但无法升级特征库。关于 License 的详细介绍请参见“License 配置”。

使用限制和注意事项

使用应用识别功能时，请将应用识别特征库升级到最新版本。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置应用

在应用页面可以通过端口映射创建自定义的 PBAR 类型的应用，也可以对预定义应用进行修改。

端口映射分类

根据与应用层协议进行映射的对象范围的不同，可以将端口映射的配置分为以下四类：

- 通用端口映射：如果报文的目的端口号与某个通用端口映射匹配，则该报文将被识别为相应的应用层协议报文。
- 基于 IP 地址的主机端口映射：对于目的地址为指定地址或指定范围的地址的报文，如果报文的目的端口号与某个映射关系匹配，则该报文将被识别为对应的应用层协议报文。
- 基于网段的主机端口映射：对于目的地址为指定网段的报文，如果报文的目的端口号与某个映射关系匹配，则该报文将被识别为对应的应用层协议报文。PBAR 以最精确的网络范围对

报文进行匹配，即如果配置了多条网段映射关系，且各映射关系中指定的网段范围互相包含，则使用网络范围最小的映射配置进行匹配。

- 基于 ACL 的主机端口映射：对于匹配指定 ACL 的报文（其目的 IP 地址与 ACL 中某规则指定的源 IP 地址参数相匹配），如果报文的目的端口号与某个映射关系匹配，则该报文将被识别为对应的应用层协议报文。

新增 PBAR 类型应用步骤

1. 选择“对象 > 安全配置文件 > 应用识别 > 应用”。
2. 在“新建自定义应用”页面配置应用的名称，并为应用配置所属的风险类型。设备将根据配置的风险类型自动计算应用的风险等级。
3. 在端口映射区域，单击<新建>按钮，进入“添加端口映射”页面。
4. 新建端口映射关系，具体配置内容如下：

表-1 端口映射关系配置

参数	说明
端口号	表示指定与应用层协议映射的端口
协议类型	表示指定应用层协议使用的传输层协议名称，其取值包括：all、DCCP（Datagram Con Protocol，数据报拥塞控制协议）、SCTP（Stream Control Transmission Protocol 议）、TCP协议、UDP协议和UDP-Lite协议。all表示所有传输层协议的指定端口的 指定应用层协议的报文

匹配方式	匹配方式包括如下几种：all（通用端口映射）、基于IPv4地址的主机端口映射、基于 机端口映射、基于IPv4 ACL的主机端口映射、基于IPv6地址的主机端口映射、基于 端口映射和基于IPv6 ACL的主机端口映射
匹配条件	选择匹配方式为基于IP地址的主机端口映射时匹配条件为IP地址范围，匹配方式为基 端口映射时匹配条件为IP地址网段，匹配方式为基于ACL的主机端口映射时匹配条件
VRF实例	指定主机所属的VPN

5. 单击<确定>按钮，可以为此 PBAR 应用添加一条端口映射表。

   在一个自定义 PBAR 应用的端口映射表中可添加多条端口映射条目，当存在以上四类端口映射条目时，对于同一个报文的生效优先级从高到低依次为：基于 IP 地址、基于网段、基于 ACL、通用。而对于其中的每一类，指定传输层协议名称的配置优先级高于不指定传输层协议名称的配置。

6. 在“新建自定义应用”页面单击<确定>按钮，可在设备上成功添加一个 PBAR 类型的应用。

   在“应用”页面勾选<只显示自定义应用>筛选条件即可清晰地看到添加的自定义应用。

修改预定义应用步骤

1. 选择“对象 > 安全配置文件 > 应用识别 > 应用”。

2. 在“应用”页面选中已存在的一个应用，单击此应用右面的<编辑>按钮，进入“修改预定义应用”页面。

3. 在“修改预定义应用”页面可以添加端口映射条目，有关添加端口映射条目的具体步骤请参见“新增 PBAR 类型应用步骤”中的第 4 步。

修改完预定义应用后，与此预定义应用原有识别规则和新增端口映射关系匹配成功的报文，都可以识别为此应用。

配置应用组

可以将具有相似特征或者相似限制要求的应用添加到一个应用组。

应用组配置步骤

1. 选择“对象 > 安全配置文件 > 应用识别 > 应用组”。
2. 在“应用组”页面单击<新建>按钮，进入“新建应用组”页面。新建应用组，具体配置内容如下：

表-2 应用组配置

参数	说明
应用组名称	表示应用组的名称，需同时满足以下条件： • 不能与已有的应用组名称相同 • 不能与预定义的应用名称（包含中文及英文名称）相同
描述	通过合理编写描述信息，便于管理员快速理解和识别该应用组的作用，有利于后期
添加方式	应用组添加应用的方式，取值包括：

	• 应用：按应用名称添加应用 • 过滤：按相同属性批量添加应用
应用	展示所有可选择的应用，单击添加可以快速选择所需的应用
风险类型	通过选择应用的风险类型，可以快速筛选出具有相同风险类型属性的应用
风险级别	通过选择应用的风险级别，可以快速筛选出具有相同风险级别属性的应用
数据传输方式	通过选择应用的数据传输方式，可以快速筛选出具有相同数据传输方式属性的应用
厂商	通过选择应用的厂商类型属性，可以快速筛选出具有相同厂商属性的应用
协议	通过选择应用的协议，可以快速筛选出具有相同协议属性的应用
类别	通过选择应用的类别，可以快速筛选出具有相同类别属性的应用

3. 单击<查看过滤结果>按钮，可查看所有符合当前筛选条件的应用。使用排除或还原操作来精准筛选所需应用。

表-3 查看过滤结果

参数	说明
批量排除	批量移除当前应用组中的应用
已排除应用	当前应用组中被移除的应用
批量还原	将已移除的应用重新添加到当前应用组中

已选应用	所有添加到当前应用组中的应用

4. 单击<确定>按钮，保存所选应用。

5. 单击<确定>按钮，此应用组创建成功，在应用组页面可看到新建的应用组。

终端识别

本帮助主要介绍以下内容：

- 特性简介
  - 基本概念
  - 工作模式
  - 工作流程
- vSystem 相关说明
- License 支持情况
- 使用限制和注意事项
- 配置指南
  - 配置准备
  - 配置白名单模式终端识别
  - 配置告警模式终端识别
  - 配置终端组

特性简介

终端识别是建立物联网安全连接的重要前提，主要用于识别物联网中的终端，例如视频摄像头和各类传感器等。当终端流量流经设备时，设备可以分析并提取出终端信息，例如终端的厂商、型号、MAC 地址等，并支持在终端信息发生变更时（包括初次识别终端信息和后续终端信息发生变化）向用户发送日志进行告警，提示用户。

基本概念

终端

设备特征库中支持预定义终端，用于标识终端的特征信息。

选择“对象 > 安全配置文件 > 终端识别 > 终端”，可查看设备支持的终端。单击<开启终端识别日志功能>按钮，可开启终端识别日志功能。

终端组

可以将具有相似特征的终端添加到一个终端组中。一个终端组，就是若干个终端的集合。如果报文被识别为属于某个终端，而该终端又属于某个终端组，则报文相当于被识别为属于某个终端组。基于终端的业务可以对属于同一个终端组的报文做统一处理。

终端识别对象组

终端识别对象组用于确认终端的 IP 地址。包括如下类型：

- 终端地址对象组：是指终端所在的地址对象组。当报文源/目的 IP 地址匹配终端地址对象组时，则源/目的 IP 地址为终端地址。
- 管理地址对象组：是指管理终端设备的管理员所在的地址对象组，当报文源/目的 IP 地址匹配管理地址对象组时，则目的/源 IP 地址为终端地址。

终端识别白名单

终端识别白名单用于过滤终端流量，若终端设备 IP 地址在白名单范围内，则系统放行该终端流量；否则，系统丢弃该终端流量。终端识别白名单支持配置两种动作，具体如下。

- 放行：放行白名单内的所有终端流量
- 阻断：仅白名单内的终端设备信息发生变化后，才丢弃终端流量；否则，放行终端流量。

工作模式

终端识别支持如下工作模式：

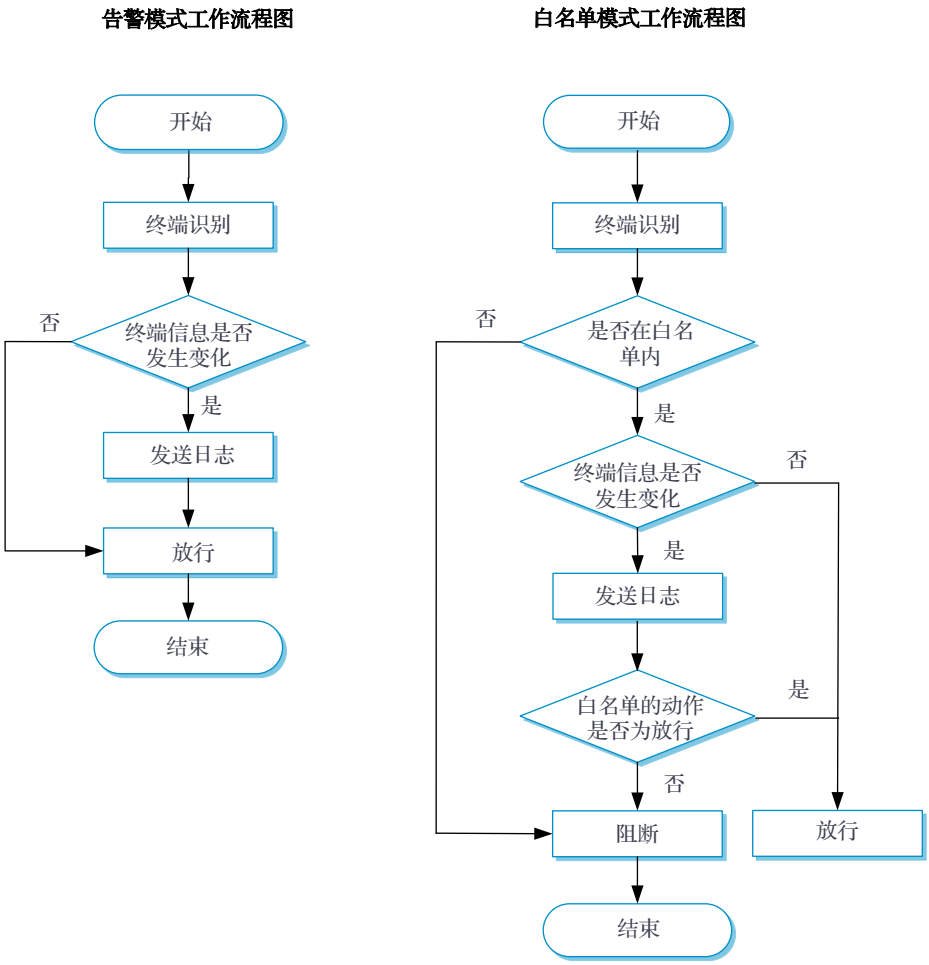
- 告警模式：此模式下，系统放行所有终端流量。若系统检测到终端信息发生变化（包含首次识别出终端设备），则向用户发送日志进行告警。在安全控制要求比较宽松的场景中，可以采用此工作模式。

- 白名单模式：此模式下，系统仅会放行白名单中的终端流量。若系统检测到白名单中的终端信息发生变化，则向用户发送日志进行告警。在安全控制要求较严格的场景中，可以采用此工作模式。

选择“对象 > 安全配置文件 > 终端识别 > 终端”，进入终端页面。在终端页面，单击<工作模式>按钮，在弹出的工作模式页面上，选择相应的工作模式。

工作流程

图-1 终端识别两种工作模式流程图



终端识别的工作流程具体如下：

- 告警模式下：系统识别并放行所有终端流量，如果系统识别出终端信息发生变化，则向用户发送日志进行告警；否则，不会发送日志。
- 白名单模式下，终端识别对终端流量的处理流程如下：

a. 系统对终端流量进行识别，对于无法识别出具体信息的终端将其归为 other 类终端。无论识别结果是明确的终端设备信息，还是 other 类终端，系统均检查终端设备的 IP 地址是否在白名单内。

b. 若终端设备 IP 地址不在白名单范围内，系统将直接丢弃终端流量；否则，系统将检测终端信息是否发生变化。若终端信息没有发生变化，则直接放行该终端流量。

c. 若终端信息发生变化，则向用户发送日志进行告警，系统将继续检测白名单的动作是否为放行。

d. 若白名单的动作为放行，则系统放行终端流量；否则，系统丢弃终端流量。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

License支持情况

终端识别基于 APR 特征库识别终端信息。License 过期后，终端识别功能可以采用设备中已有的 APR 特征库正常工作，但无法升级特征库。关于 License 的详细介绍请参见“License 联机帮助”。

使用限制和注意事项

- 在白名单模式下，如果白名单动作为阻断，当白名单中的终端设备初次上线时，系统会丢弃这些终端设备的流量。此时用户需要将其审批为合法，系统才能放行终端流量。
- 若管理地址对象组和终端地址对象组同时配置，管理地址对象组的优先级更高。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置白名单模式终端识别

在白名单模式下，设备仅会放行白名单中的终端流量。若设备检测到白名单中的终端信息（例如厂商、型号、MAC 地址等）发生变化，将以快速日志的方式向日志主机发送日志信息。在安全控制要求比较严格的场景中，建议采用此工作模式。

配置工作模式

1. 选择“对象 > 安全配置文件 > 终端识别 > 终端”，进入终端页面。
2. 单击<工作模式>按钮，进入工作模式配置页面。
3. 选择“白名单模式”，并配置白名单的动作。
4. 单击<确定>按钮，返回到终端页面。

配置终端识别对象组

1. 选择“对象 > 安全配置文件 > 终端识别 > 终端”，进入终端页面。
2. 单击<配置终端识别对象组>按钮，进入配置终端识别对象组页面。具体配置内容如下所示：

表-1 终端识别对象组配置参数表

参数		说明
IPv4地址对象组	管理地址对象组	管理终端设备的管理员所在的地址对象组

	终端地址对象组	终端所在的地址对象组
	终端白名单地址对象组	终端白名单地址对象组用于过滤终端流量，若终端设备IP地址 内，则系统放行该终端流量；否则，系统丢弃该终端流量 此功能仅在白名单模式下生效。
IPv6地址对象组	管理地址对象组	管理终端设备的管理员所在的地址对象组
	终端地址对象组	终端所在的地址对象组

3. 单击<确定>按钮，完成配置。

配置告警模式终端识别

在告警模式下，若设备检测到终端信息（例如厂商、型号、MAC 地址等）发生变化，将以快速日志的方式向日志主机发送日志信息。在安全控制要求比较宽松的场景中，可以采用此工作模式。

配置工作模式

1. 选择“对象 > 安全配置文件 > 终端识别 > 终端”，进入终端页面。
2. 单击<工作模式>按钮，进入工作模式配置页面。
3. 选择“告警模式”。
4. 单击<确定>按钮，返回到终端页面。

配置终端识别对象组

配置管理地址对象组和终端地址对象组，请至少选择其中一种进行配置。具体配置内容请参见“配置终端识别对象组”章节。

配置终端组

一个终端组，就是若干个终端的集合。可以将具有相似特征的终端添加到一个终端组中，方便管理员配置安全策略时引用终端对象。

配置终端组的具体步骤如下：

1. 选择“对象 > 安全配置文件 > 终端识别 > 终端组”，进入终端组页面。
2. 单击<新建>按钮，进入新建终端组页面，具体配置内容如下所示：

表-2 终端组配置参数表

参数	说明
终端组名称	配置终端组名称
描述	合理的描述信息能够帮助管理员快速理解此终端组的作用
可选终端	可以加入终端组的终端
已选终端	已经加入终端组的终端

3. 单击<确定>按钮，完成配置。

安全动作

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置准备
  - 配置阻断
  - 重定向
  - 配置捕获
  - 配置告警

特性简介

安全动作可为 DPI 各业务模块（如入侵防御和防病毒等）提供动作参数。支持的安全动作参数如下：

- 阻断：用于配置 DPI 各业务模块黑名单动作对报文的阻断时长。

- 重定向：用于配置 DPI 各业务模块重定向动作的 URL。
- 捕获：用于配置 DPI 各业务模块捕获动作的执行参数，比如捕获报文的最大字节数和上传捕获报文的 URL 等。
- 告警：用于配置防病毒和 URL 过滤功能向客户端返回告警信息页面时显示的告警信息内容。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 开启 SSL 代理后，入侵防御功能的捕获动作将失效。有关 SSL 代理的详细介绍，请参见“应用代理联机帮助”。
- 配置自定义 URL 过滤告警信息时，告警信息文件暂不支持自动填充 URL 字段。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置阻断

如果设备上同时开启了黑名单功能，则报文的源 IP 地址被添加到 IP 黑名单后的老化时间为此阻断参数中配置的阻断时长。报文的源 IP 地址被加入 IP 黑名单后，阻断时长之内，后续来自该源 IP 地址的报文将被丢弃。如果设备上未开启黑名单过滤功能，报文的源 IP 地址仍会被添加到 IP 黑名单表项中，但后续来自该源 IP 地址的报文不会被直接丢弃。有关黑名单功能的详细配置，请参见“攻击防范联机帮助”。

阻断动作参数的具体配置步骤如下：

1. 单击指定安全特性右侧的<编辑>按钮，进入修改阻断页面。
2. 根据实际需求配置阻断时间。
3. 单击<确定>按钮，完成配置。
4. 单击<恢复缺省>按钮，可将阻断时间恢复为缺省值。

配置重定向

重定向动作参数的具体配置步骤如下：

1. 单击指定安全特性右侧的<编辑>按钮，进入修改重定向页面。
2. 根据实际需求配置 URL，以 http://或 https://开头。
3. 单击<确定>按钮，完成配置。

配置捕获

当入侵防御或 Web 应用防护业务执行捕获动作后，设备会对报文进行缓存，并在满足捕获动作参数中设置的限制条件后，根据实际情况将捕获文件上送到如下路径。

表-1 捕获文件上送路径

参数	说明
指定的URL	当用户已设置上传URL，且与设备对接的云平台（即安全威胁发现与运营管理平台）未开件上送功能时，设备会将捕获文件上送到指定的URL
硬盘/U盘	当设备检测到硬盘/U盘在位时，会将捕获文件保存到硬盘/U盘中 管理员可直接从硬盘或U盘中获取捕获文件，或通过单击监控面板下威胁日志页面中指定的<下载>按钮，获取捕获文件
云平台（即安全威胁发现与运营管理平台）	当设备检测到与其对接的云平台已开启捕获文件上送功能时，会通过HTTPS协议将IPS捕送到云平台

捕获动作参数的具体配置步骤如下：

2. 单击指定安全特性右侧的<编辑>按钮，进入修改捕获页面。

3. 根据实际需求配置捕获动作参数，具体配置内容如下：

表-2 捕获动作参数配置内容

参数	说明
最大捕获千字节数	设备可缓存的捕获文件的最大千字节数 当设备缓存的报文的字节数达到指定的上限值时，系统会将缓存的报文上传到指定的空本地缓存，在上传期间，系统会暂停报文捕获，待上传完成后再重新开始捕获报文 如果配置的捕获报文的最大字节数为0，则系统会将捕获到的报文立刻上传到指定的

	当设备检测到与其对接的云平台已开启捕获文件上送功能时，本参数将对入侵防御 业务不受影响
上传URL	捕获文件的上送地址，仅支持FTP、TFTP，例如ftp://server、ftp://username:passw tftp://server。推荐在配置基于FTP协议的URL时单独使用服务器的用户名和密码 username password 如果未配置上传捕获报文的URL或者URL不可达，则设备依然会上传捕获到的报文 败，本地缓存的捕获文件也会被清空 当设备检测到与其对接的云平台已开启捕获文件上送功能时，本参数将对入侵防御 业务不受影响
用户名	仅在基于FTP协议的URL时，支持输入FTP服务器的用户名和密码。 FTP服务器的用户名
密码	FTP服务器的密码 仅支持输入FTP服务器的明文密码
定时上传时间	周期性上送捕获文件的时间 当到达指定的上传时间时，系统将向指定的URL上传缓存的捕获报文，并清空本地 当设备检测到与其对接的云平台已开启捕获文件上送功能时，本参数将对入侵防御 业务不受影响

4. 单击<确定>按钮，完成配置。

5. 单击<恢复缺省>按钮，捕获动作参数将全部恢复为缺省值。

配置告警

告警信息模板中可以导入告警信息文件，告警信息文件中可配置设备向客户端发送的具体告警信息。

告警动作参数的具体配置步骤如下：

1. 单击<新建>按钮，进入新建告警信息模板页面。
2. 配置模板的名称，并选择指定的安全特性。
3. 单击<确定>按钮，创建告警信息模板。新建的告警信息模板使用默认告警信息，如需自定义告警信息，请继续执行后续步骤进行配置。
4. 单击指定模板右侧的<编辑>按钮，进入编辑告警信息模板页面。
5. 单击模板列表下，指定模板类型右侧的<导入>按钮，进入导入告警信息页面。
6. 单击<下载模板>按钮，下载告警信息模板，编辑所需显示的告警信息后，保存文件。
7. 单击<选择文件>按钮，导入保存后的告警信息模板文件。
8. 单击<确定>按钮，完成告警信息的导入。
9. 单击<确定>按钮，完成告警信息模板的配置。
10. 单击<确定>按钮，完成告警信息的导入。

高级配置

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
    - 开启 Bypass
    - 配置激活
    - DPI 业务支持双机热备
    - 真实源 IP 地址检测功能
    - 设置解压缩参数
    - 显示报文详情
    - 配置代理服务器

特性简介

高级配置中的各功能作为全局设置，提供了一种统一的管理方式，在整个系统中确保功能的一致性和协调性。通过这种配置，用户可以在不同的模块和应用之间实现无缝集成，无需重复设置各项参数。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 开启 Bypass 功能后，系统将不会对接收到的报文进行 DPI 深度安全处理。可能导致其他基于 DPI 功能的业务出现中断。例如，安全策略无法对应用进行访问控制等。
- 执行配置激活操作会暂时中断 DPI 业务的处理，可能导致其他基于 DPI 功能的业务同时出现中断。例如，安全策略无法对应用进行访问控制等。
- 高级配置中配置代理服务器功能是全局设置，将对防病毒、URL 过滤和特征库升级业务中的代理服务器功能生效。防病毒业务中修改了代理服务配置，将对 URL 过滤和特征库升级业务中的代理服务器功能生效。同理在 URL 过滤或特征库升级业务进行修改，将对防病毒业务的

代理服务器功能生效。

- 设备不支持对 HTTP 2.0 版本流量进行 DPI 业务处理。

配置指南

开启 Bypass

开启本功能后，将关闭应用层检测引擎，系统将不会对接收到的报文进行 DPI 深度安全处理（例如入侵防御等业务）。应用层检测引擎功能缺省处于开启状态，如果出现系统 CPU 使用率过高等情况，可通过开启本功能来保证设备的正常运行。

1. 选择“对象 > 安全配置文件 > 高级配置”。
2. 在 Bypass 区域，单击“Bypass”后的划选按钮，开启 Bypass 功能。

配置激活

当 DPI 各业务模块（例如入侵防御等业务）的配置文件和规则被创建、修改和删除后，需要单击各个配置文件页面中的<配置激活>按钮，来使其策略和规则配置生效。为了避免重复执行该操作对 DPI 业务造成影响，请完成部署 DPI 各业务后统一在高级配置页面单击<配置激活>按钮。

1. 选择“对象 > 安全配置文件 > 高级配置”。

2. 在配置激活区域，单击<配置激活>按钮，开启配置激活功能。

DPI 业务支持双机热备

在双机热备双主模式下，可能出现 DPI 业务报文在非对称路径中无法准确处理的问题。开启本功能后，则可以解决上述问题。开启本功能会消耗一定的系统资源，请仅在需要时开启。

1. 选择“对象 > 安全配置文件 > 高级配置”。
2. 在 DPI 业务支持双击热备区域，单击“DPI 业务支持双击热备”后的划选按钮，开启 DPI 业务支持双击热备功能。

真实源 IP 地址检测功能

当客户端使用代理方式访问服务器时，源 IP 地址将会发生改变，设备无法获取客户端的真实 IP 地址。开启真实源 IP 检测功能后，设备将从客户端请求报文的相关字段获取真正的源 IP 地址，避免上述问题。

真实源 IP 地址复用功能

开启本功能后，当一个请求报文中提取不到真实源 IP 地址时，设备会将上一个请求报文中提取到的结果作为本次提取结果，直到这个会话的后续请求报文携带新的真实源 IP 地址时再重新进行提取。关闭此功能后，当设备在一个请求报文中提取不到真实源 IP 地址时，则将该次提取结果记为空。

真实源 IP 地址提取模式

本功能用于配置设备对真实源 IP 地址的提取模式。当管理员可以确定当前组网环境中仅需要针对报文中的一种字段提取真实源 IP 地址时，可将提取模式配置为仅提取该字段。否则，可将提取模式配置为“根据优先级提取真实源 IP 模式”。

- X-Forwarded-For only 模式：表示仅在 X-Forwarded-For 字段中提取真实源 IP 地址。
- Cdn-Src-IP only 模式：表示仅在 Cdn-Src-IP 字段中提取真实源 IP 地址。
- X-Real-IP only 模式：表示仅在 X-Real-IP 字段中提取真实源 IP 地址。
- TCP options only 模式：表示仅在 TCP option 字段中提取真实源 IP 地址。
- 根据优先级提取真实源 IP 模式：表示按照字段的优先级提取真实源 IP 地址，设备会从高优先字段中提取真实源 IP 地址，提取成功则记录提取结果。仅当高优先级字段中提取不到真实源 IP 地址时，才会在低优先级的字段中进行提取。缺省情况下，未配置各字段的优先级，设备按照各字段的显示顺序进行提取，如需修改提取顺序，可单击<编辑>按钮，修改各字段的优先级。数值越大，优先级越高。

X-Forwarded-For 字段参数

X-Forwarded-For 字段中携带多个地址，格式为 X-Forwarded-For: address1, address2，...addressN。代理服务器每成功收到一个请求，就把请求来源 IP 地址依次添加到右边。在不同的代理场景下，各字段取值的含义有所不同，可根据实际情况选择提取的字段位置。

设备支持将如下位置提取到的真实源 IP 地址记录为最终提取结果：

- 首个地址：表示将提取到的最左边的地址记录为最终提取结果。

- 最后 N 个地址：表示提取 X-Forwarded-For 字段最后多个地址，提取顺序与字段中显示的顺序一致。

TCP Options 字段参数

TCP Options 字段中，真实源 IP 地址位于一个标识的后面，只有检测到标识，设备才会继续向后检测真实源 IP 地址。如果没有检测到标识，则表示 TCP Option 字段中不存在真实源 IP 地址，设备会停止对 TCP Options 字段的检测。管理员可以根据实际情况配置如下参数：

- 标识检测偏移量：用于定位标识的检测起始位置。配置偏移量后，设备将从 TCP Options 字段起始位置开始偏移指定的字节后检测标识内容。缺省情况下，设备从 TCP Options 字段的起始位置开始检测标识。
- 标识检测深度：用于限定标识的检测结束位置。配置检测深度后，设备将在指定的字节数内检测标识。缺省情况下，设备不对检测结束位置进行限制，会一直检测到 TCP Options 字段的结束位置。
- 标识内容：表示作为标识的十六进制字符内容。从 TCP Options 字段提取真实源 IP 地址时，必须配置标识内容。
- IP 地址检测偏移量：表示真实源 IP 地址与标识的偏移量。配置偏移量后，设备将从标识的结束位置开始，在指定的字节数后提取真实源 IP 地址。

配置步骤

真实源 IP 地址检测功能配置步骤如下：

1. 选择“对象 > 安全配置文件 > 高级配置”。
2. 在真实源 IP 地址检测功能区域，单击“真实源 IP 地址检测功能”后的划选按钮，开启真实源 IP 地址检测功能功能。
3. 单击“真实源 IP 地址复用功能”后的划选按钮，开启真实源 IP 地址复用功能。
4. 在“真实源 IP 地址提取模式”配置页面，配置提取模式、字段优先级等，具体配置内容如下：

表-1 真实源 IP 地址提取模式参数

参数	说明
X-Forwarded-For 字段	设备支持将如下位置提取到的真实源IP地址记录为最终提取结果： 表示提取到的真实源IP地址记录结果，支持如下提取结果： • 首个地址：表示将提取到的最左边的地址记录为最终提取结果。 • 最后 N 个地址：表示提取 X-Forwarded-For 字段最后多个地址，提取顺序与字 一致。
标识检测偏移量	用于定位标识的检测起始位置。配置偏移量后，设备将从TCP Options字段起始位 的字节后检测标识内容
标识检测深度	用于限定标识的检测结束位置。配置检测深度后，设备将在指定的字节数内检测标
标识内容	表示作为标识的十六进制字符内容
IP地址检测偏移量	表示真实源IP地址与标识的偏移量。配置偏移量后，设备将从标识的结束位置开始 数后提取真实源IP地址
优先级	表示按照字段的优先级提取真实源IP地址，取值范围为1~100。数值越大，优先级

5. 单击<应用>按钮，使配置生效。

设置解压缩参数

本功能可配置应用层检测引擎解压缩文件时的最大可解压数据大小以及最大可解压层数，可通过调整解压缩参数提升引擎的检测效率。

- 最大可解压数据大小：设备解压一个文件时可解压缩数据的最大值。到达上限后，该文件的剩余数据不再进行解压。
- 最大可解压层数：当需要检测的内容存在多层压缩的文件时，可配置本参数设置可解压缩文件的层数。当超过配置的可解压缩文件的层数时，设备将不对超出层数上限的文件进行解压缩，直接按照压缩文件格式进行特征匹配等处理。到达上限后，设备将不对超出层数的文件进行解压缩。

配置步骤

1. 选择“对象 > 安全配置文件 > 高级配置”。
2. 在设置解压缩参数功能区域，配置最大可解压数据大小和最大可解压层数参数。
3. 单击<应用>按钮，使配置生效。

显示报文详情

开启本功能后，设备将在威胁日志（威胁类型为入侵防御）和 Web 应用防护日志中展示报文的更多详情信息。例如，HTTP 请求报文中支持展示请求头和请求体等，方便用户对报文进行分析。

1. 选择“对象 > 安全配置文件 > 高级配置”。
2. 在显示报文详情功能区域，单击“显示 Web 应用防护业务报文详情”后的划选按钮，开启显示 Web 应用防护业务报文详情功能。
3. 单击“显示入侵防御业务报文详情”后的划选按钮，开启显示入侵防御业务报文详情功能。

配置代理服务器

当设备不能直接访问特征库服务专区或云端服务器，可以配置代理服务器。当前该配置支持特征库在线升级、URL 过滤业务以及防病毒业务使用 HTTPS 协议进行云端查询。

1. 选择“对象 > 安全配置文件 > 高级配置”。
2. 在配置代理服务器功能区域，配置代理服务器的地址、端口和登录代理服务器使用的用户名及密码。
3. 单击<应用>按钮，使配置生效。

攻击防范

本帮助主要介绍以下内容：

- 特性简介
  - 扫描攻击防范
  - 泛洪攻击防范
  - 单包攻击防范
  - 攻击防范例外列表
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置思路
  - 配置准备
  - 创建攻击防范策略
  - 配置扫描攻击防范策略
  - 配置泛洪攻击防范策略
  - 配置单包攻击防范策略

- 配置攻击防范例外列表

特性简介

攻击防范是一个重要的网络安全特性，它通过分析经过设备的报文的内容和行为，判断报文是否具有攻击特征，并根据配置对具有攻击特征的报文执行一定的防范措施。

攻击防范策略用于定义一个或多个用于检测攻击的特征项，以及对检测到的攻击报文所采取的防范措施，例如输出告警日志、丢弃报文、加入黑名单或进行客户端验证。设备可以支持定义用于扫描攻击防范、泛洪攻击防范和单包攻击防范的策略。

攻击防范策略应用在安全域上，对安全域上收到的报文生效。

扫描攻击防范

扫描攻击是指，攻击者运用扫描工具对网络进行主机地址或端口的扫描，通过准确定位潜在目标的位置，探测目标系统的网络拓扑结构和开放的服务端口，为进一步侵入目标系统做准备。扫描攻击主要分为地址扫描攻击和端口扫描攻击。

- 地址扫描攻击

攻击者发送大量目的 IP 地址变化的探测报文，通过收到的回应报文来确定活跃的目标主机，以便针对这些主机进行下一步的攻击。

- 端口扫描攻击

攻击者获取了活动目标主机的 IP 地址后，向目标主机发送大量目的端口变化的探测报文，通过收到的回应报文来确定目标主机开放的服务端口，然后针对活动目标主机开放的服务端口选择合适的攻击方式或攻击工具进行进一步的攻击。

扫描攻击防范主要通过监测网络使用者向目标系统发起连接的速率来检测其探测行为，一般应用在设备连接外部网络的安全域上，且仅对应用了攻击防范策略的安全域上的入方向报文有效。若设备监测到某 IP 地址主动发起的连接速率达到或超过了一定阈值，则可以根据配置采取相应的动作 (输出告警日志、丢弃攻击者发送的报文，或者将攻击者的源 IP 地址加入黑名单)。

在配置扫描攻击防范策略时，需要指定扫描攻击的检测敏感度。当指定检测敏感度为低、中、高级别时，扫描攻击检测的阈值和检测周期为固定值；当指定检测敏感度为自定义时，可以通过配置灵活指定扫描攻击检测的阈值和检测周期。

若指定的扫描攻击的处理行为为加入黑名单，则需要开启安全域上的黑名单过滤功能来配合。

泛洪攻击防范

泛洪攻击是指攻击者在短时间内向目标系统发送大量的虚假请求，导致目标系统疲于应付无用信息，从而无法为合法用户提供正常服务，即发生拒绝服务。

泛洪攻击防范主要用于保护服务器，通过监测向服务器发起连接请求的速率来检测各类泛洪攻击，一般应用在设备连接外部网络的安全域上，且仅对应用了攻击防范策略的安全域上的入方向报文有效。在安全域上应用了泛洪攻击防范策略后，安全域处于攻击检测状态，当它监测到向某服务器发送报文的速率或源自某发送方的报文速率持续达到或超过了相应的触发门限值时，即认为该服务器受到了攻击或该源 IP 地址存在攻击服务器的风险，则进入攻击防范状态，并根据配置采取相应的动

作（输出告警日志、丢弃攻击者发送的报文或者进行客户端验证）。此后，当设备检测到向该服务器发送报文的速率低于恢复门限值（触发门限值的 3/4）时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

泛洪攻击防范策略中支持基于 IP 地址的攻击防范配置，即对受保护 IP 地址单独配置防范策略。对于所有非受保护 IP 地址，则可以选择采用泛洪防范公共配置来进行保护。

在配置泛洪攻击防范策略时，需要为各种类型的攻击配置防范门限。门限的设置是否合理将直接影响攻击防范的效果。系统提供了泛洪攻击阈值学习功能，为泛洪攻击防范门限值的设置提供参考。其实现原理是：系统对正常网络环境下的各种流量按时间进行统计，得出此段时间内各种流量的最高值，从而以此为依据计算出各种攻击类型对应的防范门限值。

阈值学习支持以下两种学习模式：

- 单次学习：只进行一次阈值学习。
- 周期学习：按周期学习间隔进行多次阈值学习。周期学习间隔是指从上次学习的结束时间到下次学习开始时间的间隔时间。

开启阈值学习，会对所有类型的泛洪攻击进行阈值学习。在周期学习模式下，最新一次的学习结果会覆盖上一次学习结果。对于学习到的阈值，您可以开启自动应用功能，也可以选择只学习不启用自动应用功能。

在不清楚实际流量的情况下，配置泛洪攻击防范参数时，建议使用缺省值，然后根据阈值学习功能进行调整。

单包攻击防范

单包攻击也称为畸形报文攻击，主要包括以下三种类型：

- 攻击者通过向目标系统发送带有攻击目的的 IP 报文，如分片重叠的 IP 报文、TCP 标志位非法的报文，使得目标系统在处理这样的 IP 报文时出错、崩溃；
- 攻击者可以通过发送正常的报文，如 ICMP 报文、特殊类型的 IP option 报文，来干扰正常网络连接或探测网络结构，给目标系统带来损失；
- 攻击者还可通过发送大量无用报文占用网络带宽，造成拒绝服务攻击。

单包攻击防范主要通过分析经过设备的报文特征来判断报文是否具有攻击性，一般应用在设备连接外部网络的安全域上，且仅对应用了攻击防范策略的安全域上的入方向报文有效。若设备检测到某报文具有攻击性，则根据配置采取相应的动作（输出告警日志、丢弃攻击者发送的报文）。

设备除了支持对知名单包攻击进行检测之外，还支持对用户自定义的报文特征进行检测。

攻击防范例外列表

攻击防范例外列表用于过滤不需要进行攻击防范检测的主机报文，与指定的“允许”类型的 ACL 规则匹配的报文将不会受到任何类型的攻击防范检测。该列表用于过滤某些被信任的安全主机发送的报文，可以有效的减小误报率，并提高服务器处理效率。

需要注意的是，例外列表引用的 ACL 中的“允许”类型的规则中仅源地址、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。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 对于分布式设备，当设备上安装了多块业务板时，每种泛洪攻击防范策略中门限值为每块业务板上的门限值，因而整机的该类泛洪攻击的门限值即为每块业务板上的门限值与业务板数目的乘积。
- 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。
- 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。
- 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。
- 对于如下攻击类型，防范阈值学习功能仅对缺省检测端口生效：
  - DNS flood 攻击
  - DNS reply flood 攻击

- SIP flood 攻击
- HTTP flood 攻击
- HTTP 慢速攻击
- HTTPS flood 攻击

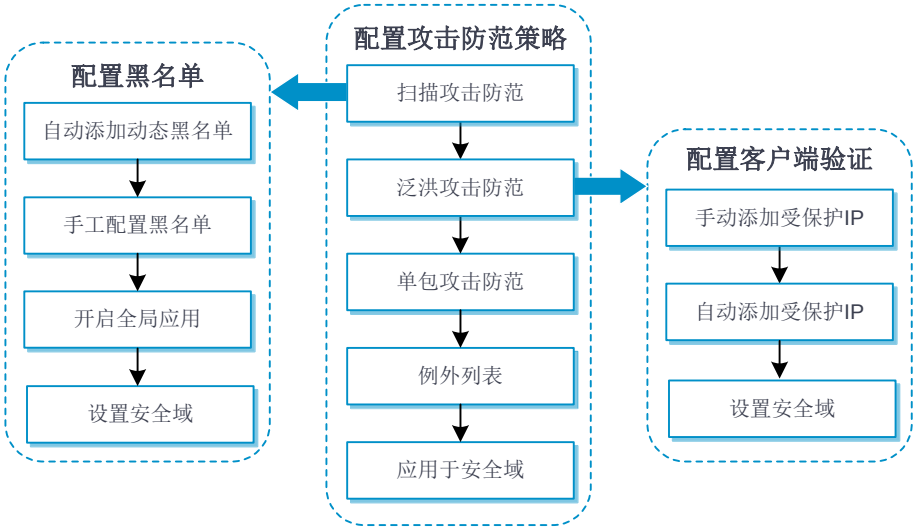
- 若用户将指定泛洪攻击类型的源门限值或目的门限值手工置零，那么开启防范阈值学习功能后，无论是否开启自动应用功能，设备都不会应用置零类型的门限值学习结果，并且用户无法手工应用该学习结果。

配置指南

配置思路

攻击防范功能的配置思路如下图所示：

图-1 攻击防范功能配置思路图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

创建攻击防范策略

在配置攻击防范之前，必须首先创建一个攻击防范策略。在策略中根据实际的网络安全需求来配置策略中的具体内容，主要包括针对攻击类型指定检测条件及采取的防范措施。

创建攻击防范策略的具体配置步骤如下：

1. 单击“对象 > 安全配置文件 > 攻击防范”。
2. 在“攻击防范”页面单击<新建>按钮，进入“新建攻击防范策略”页面，可根据实际的网络安全需求单击指定页签并配置针对攻击类型指定检测条件及采取的防范措施，各类型的攻击防范功能之间没有先后顺序，可根据实际组网需求，配置其中的一种或多种，关于各类型的攻击防范功能具体的配置步骤请参见配置扫描攻击防范策略、配置泛洪攻击防范策略、配置单包攻击防范策略和配置攻击防范例外列表。

表-1 攻击防范策略配置

参数	说明
策略名称	攻击防范策略名称，不区分大小写。合法取值包括大写字母、小写字母、数字、特殊
应用于	在指定安全域上应用当前攻击防范策略。一个安全域上只能应用一个攻击防范策略，范策略可应用于多个安全域上 下拉列表中显示的安全域包括设备缺省的安全域和用户在“网络 > 安全域”页面已

配置扫描攻击防范策略

1. 新建攻击防范策略，配置基础参数。具体配置步骤请参见“创建攻击防范策略”章节。

2. 单击“扫描防范”页签，进入扫描攻击防范配置页面，配置参数如下表所示。

表-2 扫描防范配置

参数	说明
检测敏感度	扫描攻击防范的检测级别，包括关闭、低、中、高和自定义。关闭表示关闭扫描攻 表示低防范级别，该级别提供基本的扫描攻击检测，有很低的误报率，但对于一些 能检出；中表示中防范级别，该级别有适中的攻击检出率与误报率；高表示高防范 检测出大部分的扫描攻击，但对活跃主机误报率较高，即将可提供服务的主机的报 击报文的概率比较高；自定义表示用户自定义防范级别，该级别的扫描攻击防范阈 定 • 开启端口扫描：开启/关闭端口扫描功能。检测敏感度为低、中、高级别时，该 态；检测敏感度为自定义时，该功能是否开启可以由用户指定 • 阈值：端口扫描攻击的阈值。当检测敏感度为低时，阈值为 100000；当检测敏 值为 40000；当检测敏感度为高时，阈值为 5000；当检测敏感度为自定义时， 活指定端口扫描攻击阈值；当检测敏感度为关闭时，不显示本参数 • 开启地址扫描：开启/关闭地址扫描功能。检测敏感度为低、中、高级别时，该 态；检测敏感度为自定义时，该功能是否开启可以由用户指定 • 阈值：地址扫描攻击的阈值。当检测敏感度为低时，阈值为 100000；当检测敏 值为 40000；当检测敏感度为高时，阈值为 5000；当检测敏感度为自定义时， 活指定地址扫描攻击阈值；当检测敏感度为关闭时，不显示本参数 • 检测周期：扫描攻击防范的检测周期。当检测敏感度为低、中、高时，检测周期 测敏感度为自定义时，可通过配置灵活指定扫描攻击防范的检测阈值；当检测敏 不显示本参数

动作	对扫描攻击的处理行为，包括： • 输出告警日志 • 丢弃攻击者发送的报文 • 将发起攻击的源 IP 地址添加到黑名单 • X 分钟后老化：动态添加的黑名单表项的老化时间。只有勾选“将发起攻击的源黑名单”时，才会显示该参数 当“检测敏感度”选择“关闭”时，不显示本参数

3. 单击<确定>按钮，新建的扫描攻击防范策略会在“攻击防范”页面显示。

配置泛洪攻击防范策略

泛洪攻击防范策略的具体配置步骤如下：

1. 新建攻击防范策略，配置基础参数。具体配置步骤请参见“创建攻击防范策略”章节。
2. 单击“泛洪防范配置”页签，进入泛洪攻击防范配置页面。泛洪攻击防范配置包括公共配置和受保护 IP 配置。在公共配置中配置泛洪攻击的全局防范参数，在受保护 IP 配置中配置单个 IP 地址的泛洪攻击防范参数，具体参数如表-3 和表-5 所示。

表-3 泛洪防范公共配置

参数	说明
攻击类型	设备支持的泛洪攻击类型，包括： • ACK：ACK flood 攻击。ACK 报文为只有 ACK 标志位置位的 TCP 报文，服务器时，需要查找对应的连接。若攻击者发送大量这样的报文，服务器需要进行大量消耗正常处理的系统资源，影响正常的报文处理 • DNS：DNS flood 攻击。DNS 服务器收到任何 DNS Query 报文时都会试图进行回复该DNS报文。攻击者通过构造并向DNS服务器发送大量虚假DNS Query报服务器的带宽或计算资源，使得正常的 DNS Query 得不到处理 • DNS reply：DNS reply flood 攻击。DNS 客户端收到任何 DNS reply 报文时都会击者在一定条件下将大量伪造的 DNS reply 报文发送给某个 DNS 客户端，消耗端的资源，使得正常的 DNS reply 报文得不到处理 • FIN：FIN flood 攻击。FIN 报文用于关闭 TCP 连接。若攻击者向服务器发送大量报文，可能会使服务器关闭掉正常的连接。同时，服务器收到 FIN 报文时，需要接，大量的无效查询操作会消耗系统资源，影响正常的报文处理 • HTTP：HTTP flood 攻击。HTTP 服务器收到 HTTP GET 命令时可能进行一系列包括字符串搜索、数据库遍历、数据组装、格式化转换等等，这些操作会消耗大因此当 HTTP 请求的速率超过了服务器的处理能力时，服务器就无法正常提供服过构造并发送大量虚假 HTTP GET 请求，使服务器崩溃，无法响应正常的用户 • HTTP slow：HTTP 慢速攻击。攻击者在建立了与 HTTP 服务器的连接后，长时不释放，大量这种连接将消耗服务器系统资源，影响正常报文的处理 • HTTPS：HTTPS flood 攻击。HTTP 服务器收到 HTTPS 请求时会进行一系列复些操作会消耗大量系统资源。攻击者利用这一特点，向 HTTP 服务器发送大量伪请求，造成 HTTP 服务器崩溃，使其无法响应 HTTPS 请求 • ICMP：ICMP flood 攻击。攻击者在短时间内向特定目标发送大量的 ICMP 请求报文)，使其忙于回复这些请求，致使目标系统负担过重而不能处理正常的业务 • ICMPv6：ICMPv6 flood 攻击。攻击者在短时间内向特定目标发送大量的 ICMPv6如 ping 报文)，使其忙于回复这些请求，致使目标系统负担过重而不能处理正常

	• RST：RST flood 攻击。RST 报文为 TCP 连接的复位报文，用于在异常情况下 如果攻击者向服务器发送大量伪造的 RST 报文，可能会使服务器关闭正常的 TC 服务器收到 RST 报文时，需要查找对应的连接，大量的无效查询操作会消耗系 常的报文处理 • SIP：SIP flood 攻击。SIP 服务器收到 SIP INVITE 连接请求时，服务器需要分配 于跟踪和建立会话，因此当 SIP 请求的速率超过了服务器的处理能力时，服务器 供服务。攻击者通过构造并发送大量虚假的 SIP INVITE 请求报文，导致服务器 正常的用户请求 • SYN：SYN flood 攻击。根据 TCP 协议工作原理，服务器收到 SYN 报文后需要 回应 SYN ACK 报文，然后等待客户端的 ACK 报文来建立正式连接。由于资源的 统的 TCP/IP 协议栈只能允许有限个 TCP 连接。攻击者向服务器发送大量伪造源 文后，由于攻击报文是伪造的，服务器不会收到客户端的 ACK 报文，从而导致服 大量无效的半连接，耗尽其系统资源，使正常的用户无法访问，直到半连接超时 • SYN-ACK：SYN-ACK flood 攻击。由于 SYN ACK 报文为 SYN 报文的后续报文 SYN ACK 报文时，需要查找对应的 SYN 报文。若攻击者发送大量这样的报文， 行大量的查询工作，消耗正常处理的系统资源，影响正常的报文处理 • UDP：UDP flood 攻击。攻击者在短时间内向特定目标发送大量的 UDP 报文，占 带宽，致使目标主机不能处理正常的业务
源门限值(pps)	泛洪攻击防范基于源统计的全局触发阈值，取值范围为0～1000000，ACK flood攻击 发阈值缺省为40000，其余flood攻击防范的全局触发阈值缺省为10000 配置了泛洪攻击防范后，设备处于攻击检测状态，当它监测到某IP地址发送报文的速 超过了该触发阈值时，即认为该IP地址发起了泛洪攻击，则进入攻击防范状态，并根 应的防范措施 源门限值为0表示不进行基于源统计的泛洪攻击检测
目的门限值(pps)	泛洪攻击防范基于目的统计的全局触发阈值，取值范围为0～1000000，ACK flood攻 触发阈值缺省为40000，其余flood攻击防范的全局触发阈值缺省为10000 配置了泛洪攻击防范后，设备处于攻击检测状态，当它监测到向某IP地址发送报文的 或超过了该触发阈值时，即认为该IP地址受到了泛洪攻击，则进入攻击防范状态，并 相应的防范措施 对于未专门配置泛洪防范受保护IP的IP地址，设备采用该全局阈值设置来进行保护。

	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， 值，以免阈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 可以适当调小触发阈值 目的门限值为0表示不进行基于目的统计的泛洪攻击检测
日志	泛洪攻击的处理行为是输出告警日志。即设备检测到攻击发生时，生成告警信息， 将被发送到日志系统
检测所有IP地址	对所有非受保护IP开启泛洪攻击检测
客户端验证	泛洪攻击的处理行为是客户端验证。若客户端验证功能已开启，设备自动将受到攻 到受保护IP列表中，并对客户端与受保护IP之间的连接进行代理
丢包	泛洪攻击的处理行为是丢包。即设备检测到攻击发生后，向被攻击者发送的后续所 都会被丢弃
检测端口	泛洪攻击防范的全局检测端口号。设备只对指定检测端口上收到的报文进行攻击检 表示方式为port1-port2或port，port取值范围为1～65535，port2的值要大于或等于p 检测端口之间以“,”分隔。例如：1-10,80。port1-port2或port参数最多可以输入32 对于所有非受保护IP地址，或未指定检测端口的受保护IP，设备采用全局的检测端 检测。对于所有指定检测端口的受保护IP，设备针对为每个受保护IP指定的端口进 仅当“攻击类型”为“DNS”、“DNS reply”、“HTTP”、“HTTP slow”、“HT 时，才能配置本参数
并发连接数	触发HTTP慢速攻击检测的HTTP并发连接数，缺省为5000 当设备的HTTP并发连接数达到所配置的并发连接数时，触发HTTP慢速攻击检测功 仅当“攻击类型”为“HTTP slow”时，才能配置本参数
Content长度	HTTP报文Content-Length字段的阈值，缺省为10000，单位为字节 仅当“攻击类型”为“HTTP slow”时，才能配置本参数

载荷长度	HTTP报文实际载荷的阈值，缺省为50，单位为字节 报文头部Content-Length字段的值大于所配置的Content长度，并且报文实际载荷长 载荷长度的HTTP报文被视作异常报文 仅当“攻击类型”为“HTTP slow”时，才能配置本参数
异常包数	异常报文的防范阈值，缺省为10 仅当“攻击类型”为“HTTP slow”时，才能配置本参数
检测周期	攻击检测周期，单位为秒 若设备在一个检测周期内收到的异常报文数目超过所配置的异常包数，则执行相应的 防范处理动作 仅当“攻击类型”为“HTTP slow”时，才能配置本参数
黑名单	当安全域上的黑名单过滤功能处于开启状态时，阻断并丢弃来自攻击者的后续报文 仅当“攻击类型”为“HTTP slow”时，才能配置本参数
黑名单老化时间	动态添加的黑名单表项的老化时间，单位为分钟，缺省值为10 仅当“攻击类型”为“HTTP slow”且勾选了“黑名单”时，才能配置本参数
配置学习参数	学习参数用于对阈值学习功能进行配置，请参考表-4进行相关参数配置 要使用阈值学习功能，必须先完成攻击防范策略的配置，然后在编辑页面进行学习参
应用学习结果	将泛洪攻击阈值学习结果设置为相应防范门限值 此功能仅对已启用“检测所有IP地址”且已有学习结果的攻击类型生效

3. 用户可在“泛洪防范配置”页面中，单击受公共配置下的<配置学习参数>按钮，配置学习参数。需在完成策略配置后在策略编辑页面才可进行学习参数的配置。

表-4 学习参数配置

参数	说明
学习功能	阈值学习功能用于为泛洪攻击防范阈值的设置提供参考值。建议开启阈值学习功能，
每次学习时长	学习时长是系统完成一次阈值学习的时间长度。系统会统计该段时间内各种流量的 依据计算出各种攻击类型对应的防范阈值
学习模式	学习模式如下两种类型： • 单次学习：只进行一次阈值学习 • 周期学习：按周期间隔进行多次阈值学习
自动应用	系统在完成阈值学习后自动根据最新的学习结果更新相应门限值 该功能仅对已启用“检测所有IP地址”且已有学习结果的攻击类型生效
学习容忍度	学习容忍度会在应用学习结果之前将阈值扩大指定的范围，然后再应用到门限中。 值学习功能更好的应对网络流量的波动

4. 用户可在“泛洪防范配置”页面中，单击受保护 IP 下的<新建>按钮，新建泛洪防范受保护 IP。

表-5 泛洪防范受保护 IP 配置

参数	说明
IP地址类型	• IPv4 • IPv6
IP地址	受保护的IP地址

	当“IP地址类型”为“IPv4”时，IP地址不能为255.255.255.255或0.0.0.0 当“IP地址类型”为“IPv6”时，IP地址不能为组播地址或::
攻击类型	请参见“表-3”中的“攻击类型”
VRF	受保护IP地址所属的VPN实例 可选择已创建的VRF，也可以新创建VRF。此处新建的VRF，可在“网络 > 接口与V面查看
目的门限值(pps)	攻击防范的触发阈值，基于目的IP地址统计，ACK flood攻击防范的全局触发阈值缺余flood攻击防范的全局触发阈值缺省为10000
阈值	HTTP慢速攻击防范的各项阈值，包括并发连接数、Content长度、载荷长度和异常种配置方式： • 公共配置：各项阈值与“泛洪防范公共配置”中所设置的阈值一致 • 自定义：自定义并发连接数（缺省为 5000）、Content 长度（缺省为 10000 字节省为 50 字节）和异常包数（缺省为 10） 仅当“攻击类型”为“HTTP slow”时，才能配置本参数
检测端口	泛洪攻击防范的检测端口号，设备只对指定检测端口上收到的报文进行攻击检测。方式： • 公共配置：缺省情况下，检测端口为协议的知名端口，比如针对 HTTP flood 攻80 • 自定义：检测端口为用户自定义端口，表示方式为 port1-port2 或 port。port2 的于 port1 的值，相邻检测端口之间以“,”分隔，例如：1-10,80 仅当“攻击类型”为“DNS”、“DNS reply”、“HTTP”、“HTTP slow”、“HT时，才能配置本参数
检测周期	攻击检测周期。有如下两种配置方式： • 公共配置：检测周期与“泛洪防范公共配置”中所设置的检测周期一致

	• 自定义：自定义检测周期。若未指定本参数，则表示采用“泛洪防范公共配置” 仅当“攻击类型”为“HTTP slow”时，才能配置本参数
动作	泛洪攻击的处理行为，有如下两个选项： • 公共配置：泛洪攻击的处理行为与“泛洪防范公共配置”一致 • 自定义：自定义泛洪攻击的处理行为，有如下几种行为： ○ 日志：设备检测到攻击发生时，生成告警信息，生成的告警信息将被发送 ○ 丢包：设备检测到攻击发生后，向被攻击者发送的后续所有同类型的报文 ○ 客户端验证：设备检测到攻击发生时，自动将受到攻击的 IP 地址添加到泛 列表中。若客户端验证功能已开启，则对客户端与受保护 IP 之间的连接进
黑名单	设备检测到攻击发生时，自动将发起攻击的源IP地址添加到黑名单中 当安全域上的黑名单过滤功能处于开启状态时，来自该IP地址的报文将被丢弃 仅当“攻击类型”为“HTTP slow”时，才能配置本参数
黑名单老化时间	动态添加的黑名单表项的老化时间，单位为分钟，缺省值为10 仅当“攻击类型”为“HTTP slow”且勾选了“黑名单”动作时，才能配置本参数

5. 单击<确定>按钮，新建的泛洪攻击防范策略会在“攻击防范”页面显示。

配置单包攻击防范策略

单包攻击防范策略的具体配置步骤如下：

1. 新建攻击防范策略，配置基础参数。具体配置步骤请参见“创建攻击防范策略”章节。

2. 单击“单包攻击防范”页签，进入单包攻击防范配置页面，具体的配置参数如下表所示。

表-6 知名单包攻击防范配置

参数	说明
攻击类型	设备支持的知名单包攻击类型，包括： • IP fragment：攻击者通过向目标主机发送分片偏移小于 5 的分片报文，导致主机行重组时发生错误而造成系统崩溃 • IP impossible：攻击者通过向目标主机发送源 IP 地址和目的 IP 地址相同的报文，统处理异常 • Teardrop：攻击者通过发送大量分片重叠的报文，致使服务器对这些报文进行重因而丢失有效的数据 • Tiny fragment：攻击者构造一种特殊的 IP 分片来进行微小分片的攻击，这种报文能包含完整的传输层信息，因此能够绕过某些包过滤防火墙的过滤规则，达到攻目的 • IP option abnormal：攻击者利用 IP 报文中的异常选项的设置，达到探测网络结可由于系统缺乏对错误报文的处理而造成系统崩溃 • Smurf：攻击者向目标网络发送 ICMP 应答请求，该请求包的目的地址设置为目标址，这样该网络中的所有主机都会对此 ICMP 应答请求作出答复，导致网络阻塞目标网络中主机拒绝服务的攻击目的 • Traceroute：攻击者连续发送 TTL 从 1 开始递增的目的端口号较大的 UDP 报文，个路由器，其 TTL 都会减 1，当报文的 TTL 为 0 时，路由器会给报文的源 IP 设备超时的 ICMP 报文，攻击者借此来探测网络的拓扑结构 • Ping of death：攻击者构造标志位为最后一片且长度大于 65535 的 ICMP 报文发可能导致系统处理数据时越界访问非法内存，造成系统错误甚至系统崩溃 • Large ICMP：某些主机或设备收到超大的报文，会引起内存分配错误而导致协议者通过发送超大 ICMP 报文，让目标主机崩溃，达到攻击目的 • Large ICMPv6：某些主机或设备收到超大的报文，会引起内存分配错误而导致

击者通过发送超大 ICMPv6 报文，让目标主机崩溃，达到攻击目的

- TCP invalid flags：攻击者通过发送 TCP 标志位非法的报文探测目标主机的操作
致目标主机系统崩溃
- TCP null flag：攻击者通过发送 TCP 标志位为零的报文探测目标主机的操作系统
标主机系统崩溃
- TCP all flags：攻击者通过发送 TCP 所有标志位均置位的报文探测目标主机的
导致目标主机系统崩溃
- TCP SYN-FIN：攻击者通过发送 TCP SYN 和 FIN 标志位被同时置位的报文探测
作系统，可能导致目标主机系统崩溃
- TCP FIN only flag：攻击者通过发送 TCP 仅 FIN 标志被置位的报文探测目标主
可能导致目标主机系统崩溃
- TCP Land：攻击者向目标主机发送大量源 IP 地址和目的 IP 地址都是目标主机自
报文，使得目标主机的半连接资源耗尽，最终不能正常工作
- WinNuke：攻击者向安装（或使用）Windows 系统的特定目标的 NetBIOS 端口
OOB（Out-Of-Band，带外）数据包，这些攻击报文的指针字段与实际的位置不
一个 NetBIOS 片断重叠，致使已与其他主机建立连接的目标主机在处理这些数据
溃
- UDP Bomb：攻击者发送畸形的 UDP 报文，其 IP 首部中的报文总长度大于 IP 首
首部中标识的 UDP 报文长度之和，可能造成收到此报文的系统处理数据时越界
导致系统异常
- UDP snork：攻击者向 Windows 系统发送目的端口为 135（Windows 定位服务）
7 或 19（UDP Chargen 服务）的报文，使被攻击系统不断应答报文，最终耗尽
- UDP fraggle：攻击者通过向目标网络发送源 UDP 端口为 7 且目的 UDP 端口为
报文，令网络产生大量无用的应答报文，占满网络带宽，达到攻击目的
- IPv6 扩展头异常：攻击者向目标系统发送扩展头顺序不符合 IPv6 协议规定或扩展
报文
- IPv6 扩展头数目超限：攻击者向目标系统发送扩展头数目超出限制的 IPv6 报文

IPv6扩展头异常与IPv6扩展头数目超限攻击检测仅对IPv6报文头部位于ESP扩展头前
测，不检测位于ESP扩展头之后的部分

日志	单包攻击的处理行为是输出告警日志。即设备检测到攻击发生时，生成告警信息，生 将被发送到日志系统
丢包	单包攻击的处理行为是丢包。即设备检测到攻击发生后，向被攻击者发送的后续所有 都会被丢弃
门限值（pps）	• “攻击类型”为“Large ICMP”时，表示 ICMP 报文长度的最大值，取值范围 • “攻击类型”为“Large ICMPv6”时，表示 ICMPv6 报文长度的最大值，取值范围

3. 用户可在“自定义单包攻击防范”区域，单击<新建>按钮，新建自定义单包攻击防范。

表-7 自定义单包攻击防范配置

参数	说明
特征	单包攻击检测的特征，包括： • IP 选项：IP 选项类型的报文攻击 • ICMP 类型：ICMP 类型的报文攻击 • ICMPv6 类型：ICMPv6 类型的报文攻击 • IPv6 扩展头类型：IPv6 扩展头类型的报文攻击
数值	特征的数值，取值范围为0～255 • “特征”为“IP 选项”时，表示 IP 选项代码值 • “特征”为“ICMP 类型”时，表示 ICMP 报文类型的数值 • “特征”为“ICMPv6 类型”时，表示 ICMPv6 报文类型的数值 • “特征”为“IPv6 扩展头类型”时，表示 IPv6 扩展头参数值

日志	单包攻击的处理行为是输出告警日志。即设备检测到攻击发生时，生成告警信息，生 将被发送到日志系统
丢包	单包攻击的处理行为是丢包。即设备检测到攻击发生后，向被攻击者发送的后续所有 都会被丢弃

4. 单击<确定>按钮，新建的单包攻击防范策略会在“攻击防范”页面显示。

配置攻击防范例外列表

攻击防范例外列表的具体配置步骤如下：

1. 新建攻击防范策略，配置基础参数。具体配置步骤请参见“创建攻击防范策略”章节。

   单击“例外列表”页签，进入攻击防范例外列表配置页面，具体的配置参数如下表所示。

表-8 例外列表配置

参数	说明
IPv4例外规则	使用IPv4 ACL过滤不需要进行攻击防范检测的主机报文。可选择已创建的IPv4 ACL IPv4 ACL。此处新建的IPv4 ACL，可在“对象 > ACL > IPv4”页面查看 如果配置的攻击防范例外列表中引用的ACL中未定义任何规则，例外列表不会生效
IPv6例外规则	使用IPv6 ACL过滤不需要进行攻击防范检测的主机报文。可选择已创建的IPv6 ACL IPv6 ACL。此处新建的IPv6 ACL，可在“对象 > ACL > IPv6”页面查看 如果配置的攻击防范例外列表中引用的ACL中未定义任何规则，例外列表不会生效

2. 单击<确定>按钮，新建的攻击防范例外列表会在“攻击防范”页面显示。

SSL

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置服务器端策略
  - 配置客户端策略
  - 高级设置

特性简介

SSL（Secure Sockets Layer，安全套接字层）是一个安全协议，为基于 TCP 的应用层协议（如 HTTP）提供安全连接。SSL 协议广泛应用于电子商务、网上银行等领域，为应用层数据的传输提供安全性保证。

SSL 提供的安全连接可以实现如下功能：

- 保证数据传输的机密性：利用对称密钥算法对传输的数据进行加密，并利用密钥交换算法，如 RSA（Rivest Shamir and Adleman），加密传输对称密钥算法中使用的密钥。
- 验证数据源的身份：基于数字证书利用数字签名方法对 SSL 服务器和 SSL 客户端进行身份验证。SSL 服务器和 SSL 客户端通过 PKI（Public Key Infrastructure，公钥基础设施）提供的机制获取数字证书。
- 保证数据的完整性：消息传输过程中使用 MAC（Message Authentication Code，消息验证码）来检验消息的完整性。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 目前，SSL 协议版本有 SSL2.0、SSL3.0、TLS1.0(TLS1.0 对应 SSL 协议的版本号为 3.1)、TLS1.1、TLS1.2、TLS1.3 和国密 1.1。设备作为 SSL 服务器时，可以与 SSL3.0、TLS1.0、TLS1.1、TLS1.2、TLS1.3 和国密 1.1 版本的 SSL 客户端通信，还可以识别同时兼容 SSL2.0 版本的 SSL 客户端发送的报文，并通知该客户端采用 SSL3.0、TLS1.0、TLS1.1、TLS1.2、TLS1.3 或国密 1.1 版本与 SSL 服务器通信。

- SSL 服务器端策略中可以配置 SSL 服务器启动时使用的 SSL 参数，如使用的 PKI 域、支持的加密套件、加密套件基准等。只有与 HTTPS 等应用关联后，SSL 服务器端策略才能生效。SSL 服务器端策略支持配置两个 PKI 域，可以根据客户端的配置，选择匹配的 PKI 域内证书与客户端进行 SSL 协商。加密套件支持以 SSL 客户端加密套件为准和以 SSL 服务端加密套件为准，缺省情况下，以客户端加密套件为准。当选择以服务端加密套件为准时，在协商 SSL 时将以服务端支持的加密套件顺序匹配，直到匹配成功；当选择以客户端加密套件为准时，在协商 SSL 时将以客户端支持的加密套件顺序匹配，直到匹配成功。SSL 服务器端策略支持配置发送完整证书链功能，仅当 SSL 客户端没有完整的证书链对服务器端的数字证书进行验证时，可通过开启此功能，要求 SSL 服务器端在握手协商时向对端发送完整的证书链，以保证 SSL 会话的正常建立。否则，建议关闭此功能，减轻协商阶段的网络开销。
- SSL 客户端策略中可以配置 SSL 客户端启动时使用的 SSL 参数，如使用的 PKI 域、支持的加密套件等。只有与应用层协议关联后，SSL 客户端策略才能生效。
- SSL 服务器端策略或 SSL 客户端策略配置发生改变时，需要重新启动引用策略的服务（即 SSL VPN 网关或 SSL VPN 访问实例），否则新的配置不生效。
- 当修改“高级设置”中的 SSL 协议版本时，需要重新启动引用缺省 SSL 策略的服务 (即 SSL VPN 网关或 SSL VPN 访问实例），否则新的配置不生效。

配置指南

配置服务器端策略

SSL 服务器端策略中可以配置 SSL 服务器启动时使用的 SSL 参数，如使用的 PKI 域、SSL 协议版本、支持的加密套件等。

配置步骤

新建服务器端策略的具体配置步骤如下：

1. 选择“对象 > SSL > 服务器端策略”。
2. 在“服务器端策略”页面单击<新建>按钮，进入“新建服务器端策略”页面。
3. 在“新建服务器端策略”页面的具体配置内容如下表所示：

表-1 配置服务器端策略参数表

参数	说明
名称	SSL服务器端策略的名称
服务器端PKI域	SSL服务器端策略所使用的PKI域，引用该服务器端策略的SSL服务器将通过该PKI域端的数字证书

SSL协议版本	SSL协议版本包括： • SSL3.0 • TLS1.0 • TLS1.1 • TLS1.2 • TLS1.3 • 国密 1.1
加密套件	SSL服务器端策略支持的加密套件，是SSL服务器端策略支持的各种算法组合， 际情况，选择不同类型的加密套件，包括全部、中等强度、高等强度、国密或自
最大缓存会话数目	如果缓存的会话数目达到最大值，SSL将拒绝缓存新协商出的会话
会话缓存超时时间	会话缓存的时间超过设定的时间后，SSL将删除该会话的信息
验证客户端	开启本功能后，SSL服务器端将通过数字证书对客户端进行身份验证
客户端认证PKI域	配置本功能后，SSL服务器端将通过指定的PKI域对SSL客户端进行基于数字证 只有身份验证通过后，SSL客户端才能访问SSL服务器
EMS扩展项	EMS（Extended Master Secret，扩展主密钥）是一种SSL扩展类型，开启本功 过程中会使用增强型主密钥计算方式，可以防范中间攻击者对报文进行改动
加密套件基准	此功能用于配置SSL协商中选择加密算法的规则 • 客户端算法优先：以客户端的加密套件列表为主，按优先级从高到低匹配服 密套件 • 服务器算法优先：以服务器的加密套件列表为主，按优先级从高到低匹配客 密套件
发送完整证书链	仅当SSL客户端没有完整的证书链对服务器端的数字证书进行验证时，请通过本 务器端在握手协商时向对端发送完整的证书链，以保证SSL会话的正常建立。否 功能，减轻协商阶段的网络开销

4. 单击<确定>按钮，完成配置。

配置客户端策略

SSL 客户端策略中可以配置 SSL 客户端启动时使用的 SSL 参数，如使用的 PKI 域、SSL 协议版本、支持的加密套件等。

配置步骤

新建客户端策略的具体配置步骤如下：

1. 选择“对象 > SSL > 客户端策略”。
2. 在“客户端策略”页面单击<新建>按钮，进入“新建客户端策略”页面。
3. 在“新建客户端策略”页面的具体配置内容如下表所示：

表-2 配置客户端策略参数表

参数	说明
名称	SSL客户端策略的名称
SSL协议版本	SSL协议版本包括： • SSL3.0 • TLS1.0

	• TLS1.1 • TLS1.2 • TLS1.3 • 国密 1.1
客户端PKI域	SSL客户端策略所使用的PKI域，引用该客户端策略的SSL客户端将通过该PKI域 字证书
加密套件	SSL客户端策略支持的加密套件，是SSL客户端策略支持的各种算法组合，用户 况，选择不同类型的加密套件，包括全部、中等强度、高等强度或自定义
EMS扩展项	EMS（Extended Master Secret，扩展主密钥）是一种SSL扩展类型，开启本功 过程中会使用增强型主密钥计算方式，可以防范中间攻击者对报文进行改动
验证服务器端	开启本功能后，SSL客户端将通过数字证书对服务器端进行身份验证

4. 单击<确定>按钮，完成配置。

高级设置

在“高级设置”页面，可以开启重协商功能，设置允许 SSL 服务器使用的 SSL 版本。

配置步骤

1. 选择“对象 > SSL > 高级设置”。

2. 在“高级设置”页面，具体配置内容如下：

表-3 高级设置参数表

参数	说明
开启重协商功能	TLS1.3版本不支持重协商功能 关闭SSL重协商是指，不允许复用已有的SSL会话进行SSL快速协商，每次SSL 整的SSL握手过程
SSL协议版本	SSL协议版本包括： • SSL3.0 • TLS1.0 • TLS1.1 • TLS1.2 • TLS1.3 • 国密 1.1 由于SSL3.0版本存在一些已知的安全漏洞，当设备对系统安全性有较高要求时可 版本

3. 单击<应用>按钮，完成配置。

公钥管理

本帮助主要介绍以下内容：

- 特性简介
  - 非对称密钥算法
  - 管理本地非对称密钥对
  - 管理远端主机公钥
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置本地密钥对
  - 配置远端公钥

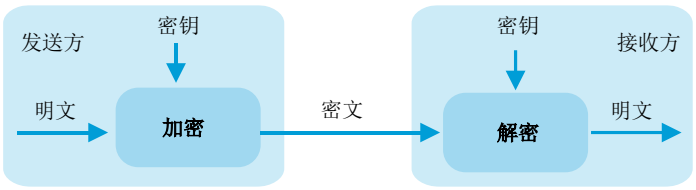
特性简介

公钥管理用于非对称密钥算法的密钥管理与发布。

非对称密钥算法

非对称密钥算法是数据加解密的一种方法，用来保证数据在网络中安全传输、不被攻击者非法窃听和恶意篡改。如图-1 所示，在非对称密钥算法中，加密和解密使用的密钥一个是对外公开的公钥，一个是由用户秘密保存的私钥，从公钥很难推算出私钥。公钥和私钥一一对应，二者统称为非对称密钥对。通过公钥（或私钥）加密后的数据只能利用对应的私钥（或公钥）进行解密。对称密钥算法中，加密和解密使用相同的密钥。

图-1 加密和解密转换关系示意图



非对称密钥算法包括 RSA（Rivest Shamir and Adleman）、DSA（Digital Signature Algorithm，数字签名算法）和 ECDSA（Elliptic Curve Digital Signature Algorithm，椭圆曲线数字签名算法）。

非对称密钥算法既可以用来对发送的数据进行加/解密，也可以用来对数据发送者的身份进行认证。非对称密钥算法广泛应用于各种应用中，例如 SSH（Secure Shell，安全外壳）、SSL（Secure Sockets Layer，安全套接字层）、PKI（Public Key Infrastructure，公钥基础设施）。

管理本地非对称密钥对

生成本地非对称密钥对

在本地设备上，可以生成 RSA、DSA 和 ECDSA 三种类型的本地非对称密钥对。

导入本地密钥对

在本地设备上，支持通过文件导入本地密钥对，如果导入的文件中密钥对是加密后的密钥对，需要输入密钥对口令才能成功导入。

显示或导出本地非对称密钥对中的主机公钥

在本地设备上，可以对本地非对称密钥对进行查看和导出操作，具体包括：

- 直接查看非对称密钥对中的公钥信息。记录下该主机公钥数据后，在远端主机上，可以通过文本粘贴的方式将记录的本地主机公钥导入到远端设备上。
- 按照指定格式将本地主机公钥导出到指定文件。将该文件上传到远端主机上后，可以通过从公钥文件中导入的方式将本地主机公钥保存到远端设备上。
- 按照指定格式将本地主机公钥导出到页面上显示。通过拷贝粘贴等方式将显示的主机公钥保存到文件中，并将该文件上传到远端主机上后，可以通过从公钥文件中导入的方式将本地主机公钥保存到远端设备上。

删除本地非对称密钥对

在如下几种情况下，建议用户删除旧的非对称密钥对，并生成新的密钥对：

- 本地设备的私钥泄露。这种情况下，非法用户可能会冒充本地设备访问网络。
- 保存密钥对的存储设备出现故障，导致设备上没有公钥对应的私钥，无法再利用旧的非对称密钥对进行加/解密和数字签名。
- 本地证书到达有效期，需要删除对应的本地密钥对。

管理远端主机公钥

在本地设备上，可以对远端非对称密钥对的公钥进行导入、查看和删除操作。

在某些应用（如 SSH）中，为了实现本地设备对远端主机的身份验证，需要在本地设备上保存远端主机的 RSA 或 DSA 主机公钥，即将远端主机公钥导入到本地设备。导入远端主机公钥的方式有如下两种：

- 从公钥文件中获取：事先将远端主机的公钥文件保存到本地设备(例如，通过 FTP 或 TFTP，以二进制方式将远端主机的公钥文件保存到本地设备)，本地设备从该公钥文件中导入远端主机的公钥。导入公钥时，系统会自动将远端主机的公钥文件转换为 PKCS（Public Key Cryptography Standards，公共密钥加密标准）编码形式。

- 文本输入：事先在远端主机上查看其公钥信息，并记录远端主机公钥的内容。在本地设备上采用手工输入的方式将远端主机的公钥数据输入到本地。手工输入远端主机公钥时，可以逐个字符输入，也可以一次拷贝粘贴多个字符。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

手工配置远端主机的公钥时，输入的主机公钥必须满足一定的格式要求。设备上查看到的主机公钥信息可以作为输入的公钥内容；通过其他方式显示的公钥可能不满足格式要求，导致主机公钥保存失败。因此，建议选用从公钥文件导入的方式配置远端主机的公钥。

配置本地密钥对

生成本地密钥对

在本地设备上，可以生成 RSA、DSA 和 ECDSA 三种类型的本地非对称密钥对。

生成本地密钥对的具体配置步骤如下：

1. 在“本地密钥对”页面单击<新建>按钮，进入“生成本地密钥对”页面。
2. 在“生成本地密钥对”页面的具体配置内容如下表所示：

表-1 生成本地密钥对参数表

参数	说明
名称	生成本地密钥对的名称
算法	生成本地密钥对的算法，取值包括： • RSA • DSA • ECDSA
密钥长度	创建RSA和DSA密钥对时，需要输入密钥长度。密钥长度越长，安全性越好，但是生成密钥的时间越长。

椭圆曲线	创建ECDSA密钥对时，可以选择不同类型的椭圆曲线，密钥越长，安全性越好，但是生成密钥的时间越长

3. 单击<确定>按钮，完成配置。

导入本地密钥对

在本地设备上，支持通过文件导入本地密钥对，如果导入的文件中密钥对是加密后的密钥对，需要输入密钥对口令才能成功导入。

导入本地密钥对的具体配置步骤如下：

1. 在“本地密钥对”页面单击<导入>按钮，进入“导入本地密钥对”页面。

2. 在“导入本地密钥对”页面的具体配置内容如下表所示：

表-2 导入本地密钥对参数表

参数	说明
名称	导入本地密钥对的名称
算法	导入本地密钥对的算法，取值包括： • RSA • ECDSA • SM2
导入文件	选择导入的密钥文件

覆盖原有密钥对	非默认名称密钥对的密钥类型和名称不能完全相同，否则需要确认是否覆盖原有的密钥对
密钥对口令	如果导入的文件中密钥对是加密后的密钥对，需要输入密钥对口令才能成功导入

3. 单击<确定>按钮，完成配置。

显示或导出本地非对称密钥对中的主机公钥

在本地设备上，可以对本地非对称密钥对进行查看和导出操作，具体包括：

- 直接查看非对称密钥对中的公钥信息。记录下该主机公钥数据后，在远端主机上，可以通过文本粘贴的方式将记录的本地主机公钥导入到远端设备上。
- 按照指定格式将本地主机公钥导出到指定文件。将该文件上传到远端主机上后，可以通过从公钥文件中导入的方式将本地主机公钥保存到远端设备上。
- 按照指定格式将本地主机公钥导出到页面上显示。通过拷贝粘贴等方式将显示的主机公钥保存到文件中，并将该文件上传到远端主机上后，可以通过从公钥文件中导入的方式将本地主机公钥保存到远端设备上。

导出本地密钥对的具体配置步骤如下：

1. 选择待导出的本地密钥对。
2. 在“本地密钥对”页面单击<导出>按钮，进入“导出本地密钥”页面。
3. 在“导出本地密钥”页面的具体配置内容如下表所示：

表-3 导出本地密钥参数表

参数	说明
名称	需要导出的本地密钥的名称
算法	导出本地密钥的算法，取值包括： • RSA • DSA • ECDSA
导出格式	可以选择导出格式为OpenSSH、SSH1或者SSH2
导出到	可以选择导出到文件或者页面
文件名	将本地密钥导出到指定的文件
覆盖原有文件	需要选择当文件名称相同时，是否覆盖原有文件

4. 单击<确定>按钮，完成配置。

删除本地非对称密钥对

在如下几种情况下，建议用户删除旧的非对称密钥对，并生成新的密钥对：

- 本地设备的私钥泄露。这种情况下，非法用户可能会冒充本地设备访问网络。
- 保存密钥对的存储设备出现故障，导致设备上没有公钥对应的私钥，无法再利用旧的非对称密钥对进行加/解密和数字签名。

- 本地证书到达有效期，需要删除对应的本地密钥对。

配置远端公钥

在本地设备上，可以对远端非对称密钥对的公钥进行导入、查看和删除操作。

在某些应用（如 SSH）中，为了实现本地设备对远端主机的身份验证，需要在本地设备上保存远端主机的 RSA 或 DSA 主机公钥，即将远端主机公钥导入到本地设备。导入远端主机公钥的方式有如下两种：

- 从公钥文件中获取：事先将远端主机的公钥文件保存到本地设备(例如，通过 FTP 或 TFTP，以二进制方式将远端主机的公钥文件保存到本地设备)，本地设备从该公钥文件中导入远端主机的公钥。导入公钥时，系统会自动将远端主机的公钥文件转换为 PKCS（Public Key Cryptography Standards，公共密钥加密标准）编码形式。
- 文本输入：事先在远端主机上查看其公钥信息，并记录远端主机公钥的内容。在本地设备上采用手工输入的方式将远端主机的公钥数据输入到本地。手工输入远端主机公钥时，可以逐个字符输入，也可以一次拷贝粘贴多个字符。

配置步骤

导入远端公钥的具体配置步骤如下：

1. 在“远端公钥”页面单击<导入>按钮，进入“导入远端公钥”页面。

2. 在“导入远端公钥”页面的具体配置内容如下表所示：

表-4 导入远端公钥参数表

参数	说明
公钥名称	导入的远端公钥的名称
导入方式	可以选择导入方式为文件或者文本
导入文件	当选择导入方式为文件时，需要选择文件进行导入
公钥数据	当选择导入方式为文本时，需要将公钥粘贴到公钥数据文本框中

3. 单击<确定>按钮，完成配置。

PKI

本帮助主要介绍以下内容：

- 特性简介
  - 数字证书和 CRL
  - PKI 体系结构
  - 主要应用
  - 管理证书
  - 证书访问控制策略
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置证书主题
  - 配置 PKI 域
  - 导入证书
  - 请求证书
  - 配置证书访问控制策略

特性简介

PKI（Public Key Infrastructure，公钥基础设施）是一个利用公钥理论和技术来实现并提供信息安全服务的具有通用性的安全基础设施。

PKI 系统以数字证书的形式分发和使用公钥。基于数字证书的 PKI 系统，能够为网络通信和网络交易(例如电子政务和电子商务)提供各种安全服务。目前，设备的 PKI 系统可为安全协议 SSL(Secure Sockets Layer，安全套接字层）提供证书管理机制。

数字证书和 CRL

数字证书是经 CA（Certificate Authority，证书颁发机构）签名的、包含公钥及相关的用户身份信息的文件，它建立了用户身份信息与用户公钥的关联。CA 对数字证书的签名保证了证书是可信任的。数字证书中包含多个字段，包括证书签发者的名称、被签发者的名称、公钥信息、CA 对证书的数字签名、证书的有效期等。

本文涉及两类证书：CA 证书、本地证书。

- CA 证书是 CA 持有的证书。若 PKI 系统中存在多个 CA，则会形成一个 CA 层次结构，最上层的 CA 是根 CA，它持有一个自签名的证书（即根 CA 对自己的证书签名），下一级 CA 证书分别由上一级 CA 签发。这样，从根 CA 开始逐级签发的证书就会形成多个可信任的链状结构，每一条路径称为一个证书链。

- 本地证书是本设备持有的证书，由 CA 签发。

由于用户名称的改变、私钥泄漏或业务中止等原因，需要存在一种方法将现行的证书吊销，即废除公钥及相关的用户身份信息的绑定关系。在 PKI 系统中，可以通过发布 CRL（Certificate Revocation List，证书吊销列表）的方式来公开证书的吊销信息。当一个或若干个证书被吊销以后，CA 签发 CRL 来声明这些证书是无效的，CRL 中会列出所有被吊销的证书的序列号。因此，CRL 提供了一种检验证书有效性的方式。设备支持开启 CRL 自动更新功能，并指定 CRL 的更新周期。到达指定的更新周期后，设备会自动连接 CRL 发布点来获取 CRL。

PKI 体系结构

一个 PKI 体系由证书主题、CA、RA 和证书/CRL 发布点四类实体共同组成。

证书主题

证书主题是 PKI 服务的最终使用者，可以是个人、组织、设备或计算机中运行的进程。一份证书是一个公钥与一个实体身份信息的绑定。证书主题的参数是证书主题的身份信息，CA 根据证书主题提供的身份信息来唯一标识证书申请者。

一个有效的证书主题参数中必须至少包括以下参数之一：

1. 证书主题名称，包含以下参数：
    - 通用名。证书主题的通用名必须配置。

- 国家代码，用标准的两字符代码表示。例如，“CN”是中国的合法国家代码，“US”是美国的合法国家代码
- 州或省的名称
- 地理区域名称
- 组织名称
- 组织部门名称

2. FQDN（Fully Qualified Domain Name，完全合格域名），是 PKI 实体在网络中的唯一标识
3. IP 地址

CA（Certificate Authority，证书颁发机构）

CA 是一个用于签发并管理数字证书的可信 PKI 实体。其作用包括：签发证书、规定证书的有效期和发布 CRL。

RA（Registration Authority，证书注册机构）

RA 是一个受 CA 委托来完成 PKI 实体注册的机构，它接收用户的注册申请，审查用户的申请资格，并决定是否同意 CA 给其签发数字证书，用于减轻 CA 的负担。建议在部署 PKI 系统时，RA 与 CA 安装在不同的设备上，减少 CA 与外界的直接交互，以保护 CA 的私钥。

证书/CRL 发布点

证书/CRL 发布点用于对用户证书和 CRL 进行存储和管理，并提供查询功能。通常，证书/CRL 发布点位于一个目录服务器上，该服务器可以采用 LDAP（Lightweight Directory Access Protocol，轻量级目录访问协议）协议、HTTP 等协议工作。其中，较为常用的是 LDAP 协议，它提供了一种访问发布点的方式。LDAP 服务器负责将 CA/RA 服务器传输过来的数字证书或 CRL 进行存储，并提供目录浏览服务。用户通过访问 LDAP 服务器获取自己和其他用户的数字证书或者 CRL。

主要应用

PKI 技术能满足人们对网络交易安全保障的需求。PKI 的应用范围非常广泛，并且在不断发展之中，下面给出几个应用实例。

安全电子邮件

电子邮件的安全也要求机密性、完整性、数据源认证和不可抵赖。目前发展很快的安全电子邮件协议 S/MIME（Secure/Multipurpose Internet Mail Extensions，安全/多用途 Internet 邮件扩充协议)是一个允许发送加密和有签名邮件的协议。该协议的实现需要依赖于 PKI 技术。

Web 安全

为了透明地解决 Web 的安全问题，在浏览器和服务器之间进行通信之前，先要建立 SSL 连接。SSL 协议允许在浏览器和服务器之间进行加密通信，并且利用 PKI 技术对服务器和浏览器端进行身份验证。

管理证书

设备基于 PKI 域管理证书，并为相关应用（比如 SSL）基于 PKI 域提供证书服务。PKI 域是一个本地概念，一个 PKI 域中包括了证书申请操作相关的信息，例如证书主题名称、证书申请使用的密钥对、证书的扩展用途等。

导入证书

导入证书是指，将证书主题有关的 CA 证书、本地证书导入到 PKI 域中保存。如果设备所处的环境中没有证书的发布点、CA 服务器不支持通过 SCEP 协议与设备交互、或者证书对应的密钥对由 CA 服务器生成，则可采用此方式获取证书。

证书导入之前：

- 需要通过 FTP、TFTP 等协议将证书文件传送到设备的存储介质中。

- 必须存在签发本地证书的 CA 证书链才能成功导入本地证书，这里的 CA 证书链可以是保存在设备上的 PKI 域中的，也可以是本地证书中携带的。因此，若设备和本地证书中都没有 CA 证书链，则需要首先执行导入 CA 证书的操作。

导入本地证书时：

- 如果用户要导入的本地证书中含有 CA 证书链，则可以通过导入本地证书的操作一次性将 CA 证书和本地证书均导入到设备。
- 如果要导入的本地证书中不含有 CA 证书链，但签发此本地证书的 CA 证书已经存在于设备上的任一 PKI 域中，则可以直接导入本地证书。
- 如果要导入的证书文件中包含了根证书，则需要确认该根证书的指纹信息是否与用户的预期一致。用户需要通过联系 CA 服务器管理员来获取预期的根证书指纹信息。
- 如果导入的本地证书中包含了密钥对，则需要输入密钥对口令。用户需要联系 CA 服务器管理员取得口令的内容。导入过程中，系统首先根据查找到的 PKI 域中已有的密钥对配置来保存该密钥对。若 PKI 域中已保存了对应的密钥对，则设备会提示用户选择是否覆盖已有的密钥对。若该 PKI 域中没有任何密钥对的配置，则设备会根据证书中的密钥对的算法及证书的密钥用途，生成与 PKI 域名同名的密钥对。如果已经存在密钥对，此时用户需要指定一个名称和本地保存的密钥对名称不同的密钥对。

导入 CA 证书时：

- 如果要导入的 CA 证书为根 CA 或者包含了完整的证书链（即含有根证书），则可以导入到设备。

- 如果要导入的 CA 证书没有包含完整的证书链（即不含有根证书），但能够与设备上已有的 CA 证书拼接成完整的证书链，则也可以导入到设备；如果不能与设备上已有的 CA 证书拼接成完整的证书链，则不能导入到设备。

导出证书

PKI 域中已存在的 CA 证书、本地证书可以导出到文件中保存，导出的证书可以用于证书备份或供其它设备使用。

请求证书

请求证书的过程就是证书主题向 CA 自我介绍的过程。证书主题向 CA 提供身份信息，以及相应的公钥，这些信息将成为颁发给该证书主题证书的主要组成部分。设备可以为证书主题生成证书申请信息，之后由用户通过带外方式（如电话、电子邮件等）将该信息发送给 CA 进行证书申请。

在请求本地证书之前，必须保证当前的 PKI 域中已经存在 CA 证书且指定了证书请求时使用的密钥对。

- PKI 域中的 CA 证书用来验证获取到的本地证书的真实性和合法性。
- PKI 域中指定的密钥对用于为 PKI 实体申请本地证书，其中的公钥和其他信息交由 CA 进行签名，从而产生本地证书。

生成证书申请时，如果本地不存在 PKI 域中所指定的密钥对，则系统会根据 PKI 域中指定的名字、算法和长度自动生成对应的密钥对。

证书访问控制策略

通过配置证书的访问控制策略，可以对安全应用中的用户访问权限进行进一步的控制，保证了与之通信的服务器端的安全性。例如，在 HTTPS（Hypertext Transfer Protocol Secure，超文本传输协议的安全版本）应用中，HTTPS 服务器可以通过引用证书访问控制策略，根据自身的安全需要对客户端的证书合法性进行检测。

一个证书访问控制策略中可以定义多个证书属性的访问控制规则，每一个访问控制规则都与一个证书属性组关联。一个证书属性组是一系列属性规则的集合，这些属性规则是对证书的颁发者名、主题名以及备用主题名进行过滤的匹配条件。

如果一个证书中的相应属性能够满足一条访问控制规则所关联的证书属性组中所有属性规则的要求，则认为该证书和该规则匹配。如果一个证书访问控制策略中有多个规则，则按照规则显示顺序从上到下遍历所有规则，一旦证书与某一个规则匹配，则立即结束检测，不再继续匹配其它规则。

规则的匹配结果决定了证书的有效性，具体如下：

- 如果证书匹配到的规则中指定了“允许”动作，则该证书将被认为通过了访问控制策略的检测且有效。
- 如果证书匹配到的规则中指定了“拒绝”动作，则该证书将被认为未通过访问控制策略的检测且无效。
- 若遍历完所有规则后，证书没有与任何规则匹配，则该证书将因不能通过访问控制策略的检测而被认为无效。

- 若安全应用（如 HTTPS）引用的证书访问控制策略不存在，则认为该应用中被检测的证书有效。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 证书主题的配置必须与 CA 证书颁发策略相匹配，因此建议根据 CA 证书颁发策略来配置证书主题，如哪些证书主题参数为必选配置，哪些为可选配置。申请者的身份信息必须符合 CA 证书颁发策略，否则证书申请可能会失败。
- Windows 2000 CA 服务器的 SCEP 插件对证书申请的数据长度有一定的限制。证书主题配置项超过一定数据长度时，CA 将不会响应证书主题的证书申请。这种情况下如果通过离线方式提交申请，Windows 2000 CA 服务器可以完成签发。其它 CA 服务器（例如 RSA 服务器和 OpenCA 服务器）目前没有这种限制。

配置证书主题

新建证书主题的具体配置步骤如下：

1. 选择“对象 > 证书与密钥 > PKI > 证书主题”。
2. 在“证书主题”页面单击<新建>按钮，进入“新建证书主题”页面。
3. 在“新建证书主题”页面的具体配置内容如下所示：

表-1 配置证书主题参数表

参数	说明
证书主题名称	证书主题的名称
通用名	PKI实体的通用名
国家代码	PKI实体所属的国家代码
州或省的名称	PKI实体所属的州或省的名称
地理区域名称	PKI实体所在的地理区域名称
组织名称	PKI实体所属组织的名称

组织部门名称	PKI实体所属的组织部门的名称
FQDN	PKI实体的FQDN
IP地址	PKI实体的IP地址，包括： • IPv4 地址 • 指定接口的主 IP 地址作为证书主题的 IP 地址

4. 单击<确定>按钮，完成配置。

配置 PKI 域

在 PKI 域中，可以配置证书主题的相关参数，例如是否对证书主题的相关证书进行 CRL 检查、证书的扩展用途、在申请证书时使用的密钥对等。

新建 PKI 域的具体配置步骤如下：

1. 选择“对象 > 证书与密钥 > PKI > 证书”。
2. 在“证书”页面单击<新建 PKI 域>按钮，进入“新建 PKI 域”页面。
3. 在“新建 PKI 域”页面的具体配置内容如下所示：

表-2 配置 PKI 域参数表

参数	说明
域名称	PKI域的名称
证书主题	指定用于申请证书的证书主题名称
CRL检查	开启CRL检查功能的目的是，查看设备上的实体证书或者即将要导入、获取到设备上的实体证书是否已经被CA吊销，若检查结果表明实体证书已被吊销，那么该证书就不被设备信任。
CRL更新周期	在对证书检查要求比较严格的场景（例如银行系统）中，需要及时更新CRL以便获取最新的证书吊销情况。此时可开启本功能，并指定CRL的更新周期。到达指定的更新周期后，设备会自动连接CRL发布点来获取CRL
本地证书可信	勾选“导入本地证书时不需要使用CA证书进行校验”后，设备将不使用CA证书对其进行校验，直接认为该证书可信
证书的扩展用途	证书支持多种扩展用途，取值包括： • IKE • SSL 服务端 • SSL 客户端
PKCS#7证书使用的加密算法	本功能指定PKCS#7证书封装与解封过程中需要使用的加密算法类型。加密算法类型需要与CA服务器支持的对称加密算法类型保持一致
申请证书使用的密钥对-算法	申请证书时使用的算法，取值包括： • RSA • DSA • ECDSA

4. 单击<确定>按钮，完成配置。

导入证书

导入证书的具体配置步骤如下：

1. 选择“对象 > 证书与密钥 > PKI > 证书”。
2. 在“证书”页面单击<导入证书>按钮，进入“导入证书”页面。
3. 在“导入证书”页面的具体配置内容如下所示：

表-3 配置导入证书参数表

参数	说明
PKI域	保存证书的PKI域的名称
证书类型	证书类型包括CA证书和本地证书
请选择上传的证书文件	选择需要上传的证书文件
证书的口令	当导入含有密钥对的本地证书时，需要输入口令。用户需要联系CA服务器管理员取得口令的内容
密钥对名称	密钥对随证书一起导入PKI域的情况下，需要配置密钥对

4. 单击<确定>按钮，完成配置。

请求证书

请求证书的具体配置步骤如下：

1. 选择“对象 > 证书与密钥 > PKI > 证书”。
2. 在“证书”页面单击<提交申请>按钮，进入“提交申请”页面。
3. 在“提交申请”页面的具体配置内容如下所示：

表-4 提交申请参数表

参数	说明
PKI域	申请证书的PKI域名称
证书主题	申请证书时使用的证书主题
算法	申请证书时使用的算法
用于证书撤销的口令	用于吊销证书时使用的口令
确认口令	确认用于吊销证书时使用的口令

4. 单击<确定>按钮，页面中将展示证书申请信息。可直接在结果区域复制申请信息或者在配置申请文件名后单击<导出>按钮，导出申请文件。

配置证书访问控制策略

通过配置证书的访问控制策略，可以对安全应用中的用户访问权限进行进一步的控制，保证了与之通信的服务器端的安全性。例如，在 HTTPS（Hypertext Transfer Protocol Secure，超文本传输协议的安全版本）应用中，HTTPS 服务器可以通过引用证书访问控制策略，根据自身的安全需要对客户端的证书合法性进行检测。

只有证书中的相应属性与某属性组中的所有属性规则都匹配上，才认为该证书与此属性组匹配。如果证书中的某属性中没有包含属性规则中指定的属性域，或者不满足属性规则中的匹配条件，则认为该证书与此属性组不匹配

配置步骤

证书访问策略的具体配置步骤如下：

1. 选择“对象 > 证书与密钥 > PKI > 证书访问控制策略”。
2. 在“证书访问控制策略”页面单击<新建>按钮，进入“新建证书访问控制策略”页面。
3. 在“新建证书访问控制策略”页面，配置策略名称。
4. 单击<新建>按钮，进入“新建规则”页面，配置规则动作为允许或拒绝。
5. 单击<新建>按钮，配置证书属性，证书属性规则的具体配置内容如下所示：

表-5 证书属性配置参数表

参数	说明
属性名称	证书属性的名称，取值包括： • 证书备用主题名 • 证书颁发者名 • 证书主题名
条件	证书属性的条件，即匹配证书属性规则时使用的匹配条件，取值包括： • 包含 • 相等 • 不包含 • 不相等
属性域	证书属性的属性域，取值包括： • DN • FQDN • IP 如果证书的相应属性中包含了属性规则里指定的属性域，且满足属性规则中定义的匹配条件，则认为该属性与属性规则相匹配。例如：属性规则2中定义，证书的主题名DN中包含字符串ab。如果某证书的主题名的DN中确实包含了字符串ab，则认为该证书的主题名与属性规则2匹配
值	证书属性中不同属性域对应的值

6. 单击<确定>按钮，完成证书属性配置。

7. 单击<确定>按钮，完成规则配置。

8. 单击<确定>按钮，完成证书访问策略配置。

ACL

本帮助主要介绍以下内容：

- 特性简介
  - ACL 分类
  - ACL 规则匹配顺序
  - ACL 规则编号
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置准备
  - 新建 IPv4 ACL
  - 新建 IPv6 ACL
  - 新建二层 ACL

特性简介

ACL（Access Control List，访问控制列表）是一或多条规则的集合，用于识别报文流。这里的规则是指描述报文匹配条件的判断语句，匹配条件可以是报文的源地址、目的地址、端口号等。设备依照这些规则识别出特定的报文，并根据预先设定的策略对其进行处理。

ACL 分类

ACL 包括下表所列的几种类型，它们的主要区别在于规则制订依据不同：

表-1 ACL 的分类

ACL 类型		编号范围	
IPv4 ACL	基本ACL	2000～2999	依据报文的源IPv4地址制订规则
	高级ACL	3000～3999	依据报文的源/目的IPv4地址、优先级、承载的IPv4协议类型等三、
IPv6 ACL	基本ACL	2000～2999	依据报文的源IPv6地址制订规则
	高级ACL	3000～3999	依据报文的源/目的IPv6地址、优先级、承载的IPv6协议类型等三、
二层 ACL		4000～4999	依据报文的源/目的MAC地址、802.1p优先级、链路层协议类型等二
用户自定义ACL		5000～5999	以报文头为基准，指定从报文的第几个字节开始与掩码进行"与"操作

ACL 规则匹配顺序

表-2 各类型 ACL 的“深度优先”排序法则

ACL 类型		排序法则
IPv4 ACL	基本ACL	1. 先判断规则的匹配条件中是否包含 VPN 实例，包含者优先 2. 如果 VPN 实例的包含情况相同，再比较源 IPv4 地址范围，较小者优先 3. 如果源 IPv4 地址范围也相同，再比较配置的先后次序，先配置者优先
	高级ACL	4. 先判断规则的匹配条件中是否包含 VPN 实例，包含者优先 5. 如果 VPN 实例的包含情况相同，再比较协议范围，指定有 IPv4 承载的协议类 6. 如果协议范围相同，再比较源 IPv4 地址范围，较小者优先 7. 如果源 IPv4 地址范围也相同，再比较目的 IPv4 地址范围，较小者优先 8. 如果目的 IPv4 地址范围也相同，再比较 TCP/UDP 端口号的覆盖范围，较小者 9. 如果 TCP/UDP 端口号的覆盖范围无法比较，则比较配置的先后次序，先配置者
IPv6 ACL	基本ACL	10. 先判断规则的匹配条件中是否包含 VPN 实例，包含者优先 11. 如果 VPN 实例的包含情况相同，再比较源 IPv6 地址的范围，较小者（即前缀 先 12. 如果源 IPv6 地址范围相同，再比较配置的先后次序，先配置者优先
	高级ACL	13. 先判断规则的匹配条件中是否包含 VPN 实例，包含者优先 14. 如果 VPN 实例的包含情况相同，再比较协议范围，指定有 IPv6 承载的协议类

		15. 如果协议范围相同，再比较源 IPv6 地址范围，较小者优先 16. 如果源 IPv6 地址范围也相同，再比较目的 IPv6 地址范围，较小者优先 17. 如果目的 IPv6 地址范围也相同，再比较 TCP/UDP 端口号的覆盖范围，较小者 18. 如果 TCP/UDP 端口号的覆盖范围无法比较，则比较配置的先后次序，先配置者
二层 ACL		19. 先比较源 MAC 地址范围，较小者（即掩码中"1"位较多者）优先 20. 如果源 MAC 地址范围相同，再比较目的 MAC 地址范围，较小者优先 21. 如果目的 MAC 地址范围也相同，再比较配置的先后次序，先配置者优先

ACL 规则编号

每条规则都有自己的编号，这个编号可由手工指定或由系统自动分配。由于规则编号可能影响规则的匹配顺序，因此当系统自动分配编号时，为方便后续在已有规则之间插入新规则，通常在相邻编号之间留有一定空间，这就是规则编号的步长。系统自动分配编号的方式为：从 0 开始，按照步长分配一个大于现有最大编号的最小编号。比如原有编号为 0、5、9、10 和 12 的五条规则，步长为 5，则系统将自动为下一条规则分配编号 15。如果步长发生了改变，则原有全部规则的编号都将自动从 0 开始按新步长重新排列。比如原有编号为 0、5、9、10 和 15 的五条规则，当步长变为 2 后，这些规则的编号将依次变为 0、2、4、6 和 8。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- ACL 既可以在本页面创建，也可以在引用 ACL 的特性页面创建。不论通过哪种方式创建的 ACL 都只能在本页面进行管理（如修改和删除 ACL）。
- 删除或修改 ACL 可能会对引用该 ACL 的业务造成影响，请谨慎删除或修改 ACL。
- 当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。

- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

新建 IPv4 ACL

新建 IPv4 ACL 的具体配置步骤如下：

1. 选择“对象 > ACL > IPv4”。
2. 在“IPv4”页面单击“新建”按钮，进入“新建 IPv4 ACL”页面，具体的配置参数如下表所示。

表-3 新建 IPv4 ACL 的详细配置

配置项	说明
类型	• 基本 ACL • 高级 ACL
ACL	配置ACL的名称 • 若新建的是基本ACL，请输入2000-2999或1-63个字符，必须以英文字母开头，且不能为‘all’，禁止输入‘?’和开头结尾输入空白字符

	• 若新建的是高级ACL，请输入3000-3999或1-63个字符，必须以英文字母开头，且不能为‘all’，禁止输入‘?’和开头结尾输入空白字符
规则匹配顺序	一个ACL中可以包含多条规则，设备将报文按照一定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。规则匹配顺序有两种： • 按照配置顺序：按照规则编号由小到大进行匹配。 • 自动排序：按照“深度优先”原则由深到浅进行匹配，见下表（自定义 ACL 不支持自动排序）
默认规则步长	配置规则编号的步长
描述	配置ACL的描述信息
确定并添加规则	没有添加规则的情况下该ACL为空，如要配置IPv4 ACL的规则就需单击此按钮，规则的详细配置请参见表-2

表-4 新建 IPv4 ACL 规则的详细配置

配置项	说明
ACL编号	配置ACL的名称（自动带入表1所配置的ACL，无需配置）
规则编号	输入所配置规则的编号，规则编号方式有两种： • 自动编号 • 手动输入 如果指定的规则ID已经存在，则将该规则修改为新指定的配置

描述	配置ACL的描述信息
动作	选择对匹配该规则的报文所进行的操作 • 允许：表示允许匹配该规则的报文通过 • 拒绝：表示禁止匹配该规则的报文通过
IP协议类型	选择IP承载的协议类型 如选择“icmp(1)”协议后，需配置ICMP类型；选择“tcp(6)”或“udp(17)”协议后，可配置TCP/UDP类型 注意：新建IPv4基本ACL的规则时不支持配置此参数
匹配条件	• 匹配源 IP 地址/通配符掩码 • 匹配源地址对象组 • 匹配目的 IP 地址/通配符掩码 • 匹配目的地址对象组 • 匹配 TCP/UDP 报文的源端口号 • 匹配 TCP/UDP 报文的目的端口号 • 匹配 TCP 报文的连接建立标识 • 匹配 TCP 报文标识 • 匹配 ICMP 报文的消息类型和消息码 • 匹配 DSCP 优先级 • 匹配 IP 优先级 • 匹配 ToS 优先级 注意：新建IPv4基本ACL的规则的匹配条件仅支持配置匹配源IP地址/通配符掩码、匹配源地址对象组。新建IPv4高级ACL的规则的匹配条件会根据所选择的IP协议而有所不同

规则生效时间段	选择规则生效的时间段，可下拉选择已有的时间段，如需新建，下拉后单击“+添加时间段”按钮，配置项如下： • 名称：配置时间段的名称 (1-63 字符，不能为'all'，禁止输入'?'，仅配有名称的时间段，重启后不会保存，且在 RBM 组网中不会备份至备设备，请同时配置周期时间段或绝对时间段）匹配 IP 优先级 • 周期时间段：表示以每周每月为周期（如每周一的 8 至 12 点）循环生效的时间段。 • 绝对时间段：表示在指定时间范围内 (如 2015 年 1 月 1 日 8 点至 2015 年 1 月 3 日 18 点）生效的时间段。 当一个时间段内包含有多个周期时间段和绝对时间段时，系统将先分别取各周期时间段的并集和各绝对时间段的并集，再取这两个并集的交集作为该时间段最终生效的时间范围。
VRF	指定VPN实例信息 如果选择“无”，则表示该规则仅对非VPN报文生效
分片报文	选中前面的复选框，设置该规则仅对非首片分片报文有效，对首片分片报文和非分片报文无效 如不设置，则规则对非分片报文和分片报文均有效
记录日志	选中前面的复选框，设置对匹配该规则的报文记录日志 日志内容包括：ACL规则的序号、报文通过或被丢弃、IP承载的上层协议类型、源/目的地址、源/目的端口号、报文的数目
匹配统计	选中前面的复选框，设置开启本规则的匹配统计功能
确定并继续添加	单击该按钮，可继续添加并配置下一条ACL

3. 单击“确定”按钮，完成新建 IPv4 ACL 规则的配置。

新建 IPv6 ACL

新建 IPv6 ACL 的具体配置步骤如下：

1. 选择“对象 > ACL > IPv6”。
2. 在“IPv6”页面单击“新建”按钮，进入“新建 IPv6 ACL”页面，具体的配置参数如下表所示。

表-5 新建 IPv6 ACL 的详细配置

配置项	说明
类型	• 基本 ACL • 高级 ACL
ACL	配置ACL的名称 • 若新建的是基本ACL，请输入2000-2999或1-63个字符，必须以英文字母开头，且不能为‘all’，禁止输入‘?’和开头结尾输入空白字符 • 若新建的是高级ACL，请输入3000-3999或1-63个字符，必须以英文字母开头，且不能为‘all’，禁止输入‘?’和开头结尾输入空白字符
规则匹配顺序	一个ACL中可以包含多条规则，设备将报文按照一定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。规则匹配顺序有两种： • 按照配置顺序：按照规则编号由小到大进行匹配。 • 自动排序：按照“深度优先”原则由深到浅进行匹配，见下表

	（自定义 ACL 不支持自动排序）
默认规则步长	配置规则编号的步长
描述	配置ACL的描述信息
确定并添加规则	没有添加规则的情况下该ACL为空，如要配置IPv6 ACL的规则就需单击此按钮，规则的详细配置请参见表-2

表-6 新建 IPv6 ACL 的规则的详细配置

配置项	说明
ACL编号	配置ACL的名称（自动带入表1所配置的ACL，无需配置）
规则编号	输入所配置规则的编号，规则编号方式有两种： • 自动编号 • 手动输入 如果指定的规则ID已经存在，则将该规则修改为新指定的配置
描述	配置ACL的描述信息
动作	选择对匹配该规则的报文所进行的操作 • 允许：表示允许匹配该规则的报文通过 • 拒绝：表示禁止匹配该规则的报文通过
IP协议类型	选择IP承载的协议类型 如选择“icmpv6(58)”协议后，需配置ICMPv6类型；选择“tcp(6)”

	或“udp(17)”协议后，可配置TCP/UDP类型 注意：新建IPv6基本ACL的规则时不支持配置此参数
匹配条件	• 匹配源 IPv6 地址/前缀长度 • 匹配源地址对象组 • 匹配目的 IPv6 地址/前缀长度 • 匹配目的地址对象组 • 匹配 TCP/UDP 报文的源端口号 • 匹配 TCP/UDP 报文的目的端口号 • 匹配 TCP 报文的连接建立标识 • 匹配 TCP 报文标识 • 匹配 ICMPv6 报文的消息类型和消息码 • 匹配路由头类型 • 匹配逐跳头类型 • 匹配 DSCP 优先级 • 匹配 IPv6 基本报文头中的流标签字段 注意：新建IPv6基本ACL的规则的匹配条件仅支持配置匹配源IPv6地址/前缀长度、匹配源地址对象组和匹配路由头类型。新建IPv6高级ACL的规则的匹配条件会根据所选择的IP协议而有所不同
规则生效时间段	选择规则生效的时间段，可下拉选择已有的时间段，如需新建，下拉后单击“+添加时间段”按钮，配置项如下： • 名称：配置时间段的名称 (1-63 字符，不能为'all'，禁止输入'?'，仅配有名称的时间段，重启后不会保存，且在 RBM 组网中不会备份至备设备，请同时配置周期时间段或绝对时间段）匹配 IP 优先级 • 周期时间段：表示以每周每月为周期（如每周一的 8 至 12 点）

	循环生效的时间段。 • 绝对时间段：表示在指定时间范围内 (如 2015 年 1 月 1 日 8 点至 2015 年 1 月 3 日 18 点）生效的时间段。 当一个时间段内包含有多个周期时间段和绝对时间段时，系统将先分别取各周期时间段的并集和各绝对时间段的并集，再取这两个并集的交集作为该时间段最终生效的时间范围。
VRF	指定VPN实例信息 如果选择“无”，则表示该规则仅对非VPN报文生效
分片报文	选中前面的复选框，设置该规则仅对非首片分片报文有效，对首片分片报文和非分片报文无效 如不设置，则规则对非分片报文和分片报文均有效
记录日志	选中前面的复选框，设置对匹配该规则的报文记录日志 日志内容包括：ACL规则的序号、报文通过或被丢弃、IP承载的上层协议类型、源/目的地址、源/目的端口号、报文的数目
匹配统计	选中前面的复选框，设置开启本规则的匹配统计功能
确定并继续添加	单击该按钮，可继续添加并配置下一条ACL

3. 单击“确定”按钮，完成新建 IPv6 ACL 规则的配置。

新建二层 ACL

新建二层 ACL 的具体配置步骤如下：

1. 选择“对象 > ACL > 二层”。

2. 在“二层”页面单击“新建”按钮，进入“新建二层 ACL”页面，具体的配置参数如下表所示。

表-7 新建二层 ACL 的详细配置

配置项	说明
ACL	配置ACL的名称（4000-4999或1-63个字符）
规则匹配顺序	一个ACL中可以包含多条规则，设备将报文按照一定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。规则匹配顺序有两种： • 按照配置顺序：按照规则编号由小到大进行匹配。 • 自动排序：按照“深度优先”原则由深到浅进行匹配，见下表（自定义 ACL 不支持自动排序）
默认规则步长	配置规则编号的步长
描述	配置ACL的描述信息
确定并添加规则	没有添加规则的情况下该ACL为空，如要配置二层 ACL的规则就需单击此按钮，规则的详细配置请参见表-2

表-8 新建二层 ACL 的规则的详细配置

配置项	说明
ACL编号	配置ACL的名称（自动带入表1所配置的ACL，无需配置）
规则编号	输入所配置规则的编号，规则编号方式有两种： • 自动编号 • 手动输入 如果指定的规则ID已经存在，则将该规则修改为新指定的配置
描述	配置ACL的描述信息
动作	选择对匹配该规则的报文所进行的操作 • 允许：表示允许匹配该规则的报文通过 • 拒绝：表示禁止匹配该规则的报文通过
匹配条件	• 匹配源 MAC 地址/掩码 • 匹配目的 MAC 地址/掩码 • 匹配 802.1p 优先级 • 匹配 LLC 封装中的 DSAP 字段和 SSAP 字段 • 匹配链路层协议类型
规则生效时间段	选择规则生效的时间段，可下拉选择已有的时间段，如需新建，下拉后单击“+添加时间段”按钮，配置项如下： • 名称：配置时间段的名称 (1-63 字符，不能为'all'，禁止输入'?'，仅配有名称的时间段，重启后不会保存，且在 RBM 组网中不会备份至备设备，请同时配置周期时间段或绝对时间段）匹配 IP 优先级

	• 周期时间段：表示以每周每月为周期（如每周一的 8 至 12 点）循环生效的时间段。 • 绝对时间段：表示在指定时间范围内 (如 2015 年 1 月 1 日 8 点至 2015 年 1 月 3 日 18 点）生效的时间段。 当一个时间段内包含有多个周期时间段和绝对时间段时，系统将先分别取各周期时间段的并集和各绝对时间段的并集，再取这两个并集的交集作为该时间段最终生效的时间范围。
匹配统计	选中前面的复选框，设置开启本规则的匹配统计功能
确定并继续添加	单击该按钮，可继续添加并配置下一条ACL

3. 单击“确定”按钮，完成新建二层 ACL 规则的配置。

安全域

本帮助主要介绍以下内容：

- 特性简介
  - 安全域
  - 攻击防范
  - 威胁防护
  - uRPF
  - 白名单
- 使用限制和注意事项
- 配置指南
  - 创建安全域
  - （可选）创建白名单
  - （可选）配置客户端验证

特性简介

安全域

安全域是一个逻辑概念，用于管理设备上安全需求相同的多个接口。管理员将安全需求相同的接口进行分类，并划分到不同的安全域，统一应用安全策略，简化配置，方便管理。

管理员创建安全域后，可以给安全域添加多个成员，成员的类型包括：二层物理接口加 VLAN、三层物理接口/三层以太网子接口/其它三层逻辑接口。

配置安全域后，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会被丢弃。

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。

攻击防范

攻击防范是一个重要的网络安全特性，它通过分析经过设备的报文的内容和行为，判断报文是否具有攻击特征，并根据配置对具有攻击特征的报文执行一定的防范措施。

攻击防范策略用于定义一个或多个用于检测攻击的特征项，以及对检测到的攻击报文所采取的防范措施，例如输出告警日志、丢弃报文、加入黑名单或进行客户端验证。设备可以支持定义用于扫描攻击防范、泛洪攻击防范和单包攻击防范的策略。

攻击防范策略应用在安全域上，对安全域上收到的报文生效。

威胁防护

客户端验证功能用来防御服务器受到的 TCP、HTTP、SIP、DNS、HTTPS 类型的泛洪攻击。启动了客户端验证功能的设备，位于客户端和服务器之间，能够对客户端发起的连接进行验证，当检测到服务器受到攻击时，将服务器的 IP 地址添加为动态受保护的 IP 地址，并对所有向该服务器发起的报文进行验证，从而达到保护服务器免受各种泛洪攻击的目的。

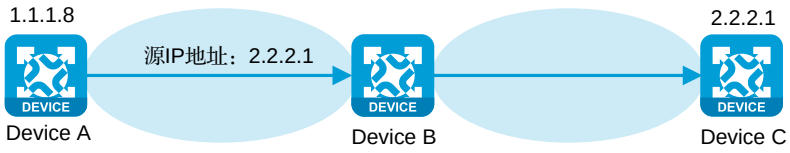
uRPF

uRPF 简介

uRPF（unicast Reverse Path Forwarding，单播反向路径转发）是一种单播逆向路由查找技术，用来防范基于源地址欺骗的攻击手段，例如基于源地址欺骗的 DoS（Denial of Service，拒绝服务）攻击和 DDoS（Distributed Denial of Service，分布式拒绝服务）攻击。

对于使用基于 IP 地址验证的应用来说，基于源地址欺骗的攻击手段可能导致未被授权用户以他人身份获得访问系统的权限。因此即使响应报文没有发送给攻击者或其它主机，此攻击方法也可能会造成对被攻击对象的破坏。

图-1 源地址欺骗攻击示意图



如图-1 所示，攻击者在 Device A 上伪造并向 Device B 发送大量源地址为 2.2.2.1 的报文，Device B 响应这些报文并向真正的 “2.2.2.1”（Device C）回复报文。因此这种非法报文对 Device B 和 Device C 都造成了攻击。如果此时网络管理员错误地切断了 Device C 的连接，可能会导致网络业务中断甚至更严重的后果。

攻击者也可以同时伪造不同源地址的攻击报文或者同时攻击多个服务器，从而造成网络阻塞甚至网络瘫痪。

uRPF 可以有效防范上述攻击。一般情况下，设备在收到报文后会根据报文的目的地址对报文进行转发或丢弃。而 uRPF 可以在转发表中查找报文源地址对应的接口是否与报文的入接口相匹配，如果不匹配则认为源地址是伪装的并丢弃该报文，从而有效地防范网络中基于源地址欺骗的恶意攻击行为的发生。

uRPF 检查方式

uRPF 检查方式有严格型和松散型两种。

- 严格型 uRPF 检查

不仅检查报文的源地址是否在转发表中存在，而且检查报文的入接口与转发表是否匹配。

在一些特殊情况下（如非对称路由，即设备上行流量的入接口和下行流量的出接口不相同），严格型 uRPF 检查会错误地丢弃非攻击报文。

一般将严格型 uRPF 检查布置在 ISP 的用户端和 ISP 端之间。

- 松散型 uRPF 检查

仅检查报文的源地址是否在转发表中存在，而不再检查报文的入接口与转发表是否匹配。

松散型 uRPF 检查可以避免错误的拦截合法用户的报文，但是也容易忽略一些攻击报文。

一般将松散型 uRPF 检查布置在 ISP-ISP 端。另外，如果用户无法保证路由对称，可以使用松散型 uRPF 检查。

uRPF 技术优点

- 与缺省路由的配合使用

  当设备上配置了缺省路由后，会导致 uRPF 根据转发表检查源地址时，所有源地址都能查到下一跳。针对这种情况，支持用户配置 uRPF 是否允许匹配缺省路由。如果允许匹配缺省路由，则当 uRPF 查询转发表得到的结果是缺省路由时，认为查到了匹配的表项；如果不允许匹配缺省路由，则当 uRPF 查询转发表得到的结果是缺省路由时，认为没有查到匹配的表项。

  缺省情况下，如果 uRPF 查询转发表得到的结果是缺省路由，则按没有查到表项处理，丢弃报文。

  运营商网络边缘位置一般不会有缺省路由指向客户侧设备，所以一般不需要配置“允许匹配缺省路由”。如果在客户侧边缘设备接口上面启用 uRPF，这时往往会有缺省路由指向运营商，此时需要配置“允许匹配缺省路由”。

- 与链路层检查配合使用（仅 IPv4 uRPF 支持）

  严格型 uRPF 检查中还可以进一步进行链路层检查，即用源地址查转发表得到的下一跳地址再查一次 ARP 表，确保报文的源 MAC 地址和查到的 ARP 表项中的 MAC 地址一样才允许报文通过。

  链路层检查功能对于运营商用一个三层以太网接口接入大量 PC 机用户时部署非常合适。

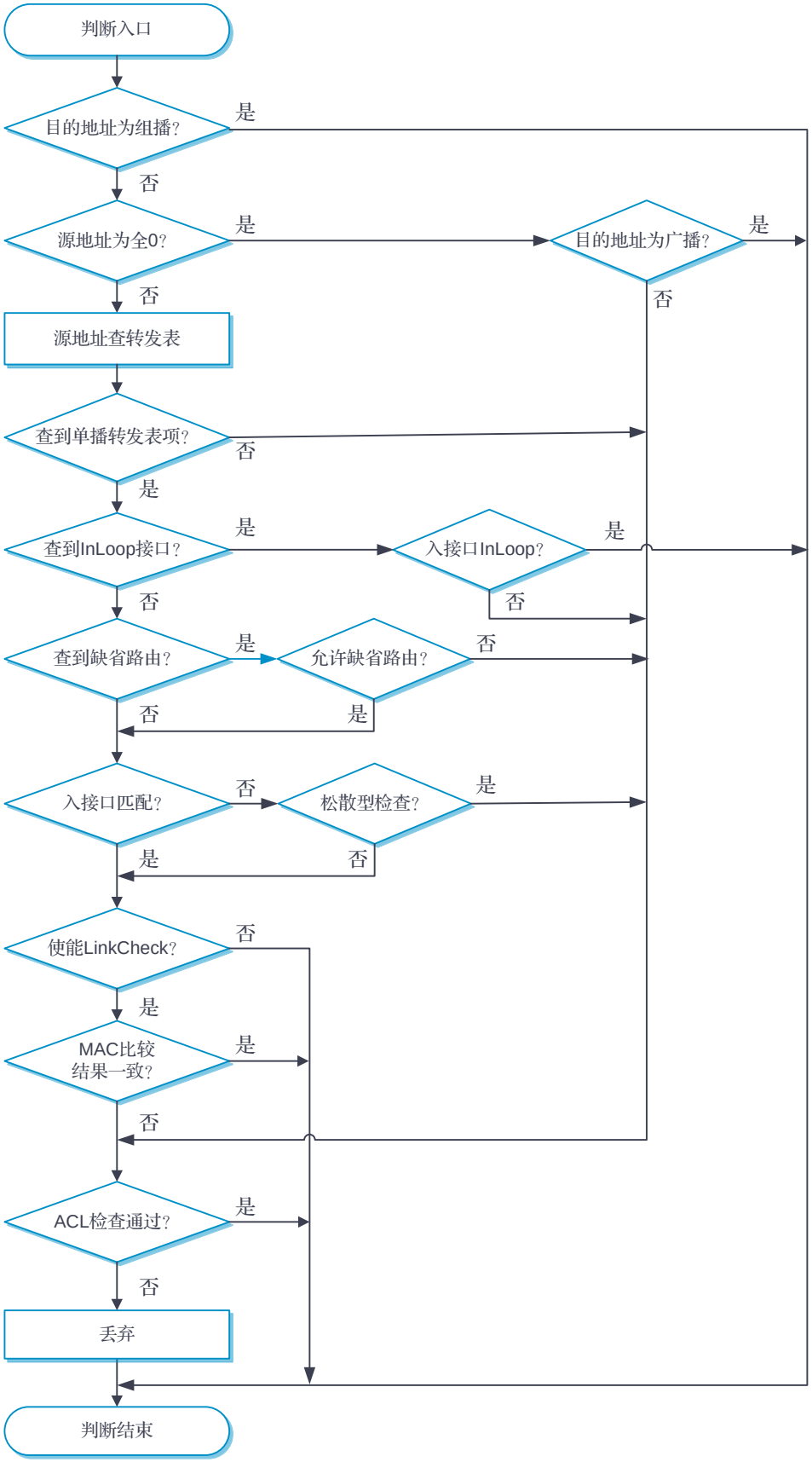
  松散型 uRPF 检查不支持链路层检查功能。

- 与 ACL 的配合使用

如果用户确认具有某些特征的报文是合法报文，则可以在 ACL 中指定这些报文，那么这些报文在逆向路由不存在的情况下，不做丢弃处理，按正常报文进行转发。

IPv4 uRPF 处理流程

图-2 IPv4 uRPF 处理流程图


判断入口
目的地址为组播?
是
否
源地址为全0?
是
目的地址为广播?
是
否
源地址查转发表
查到单播转发表项?
否
是
查到InLoop接口?
是
入接口InLoop?
是
否
否
查到缺省路由?
是
允许缺省路由?
否
否
是
入接口匹配?
否
松散型检查?
是
是
否
使能LinkCheck?
否
是
MAC比较
结果一致?
是
否
ACL检查通过?
是
否
丢弃
判断结束

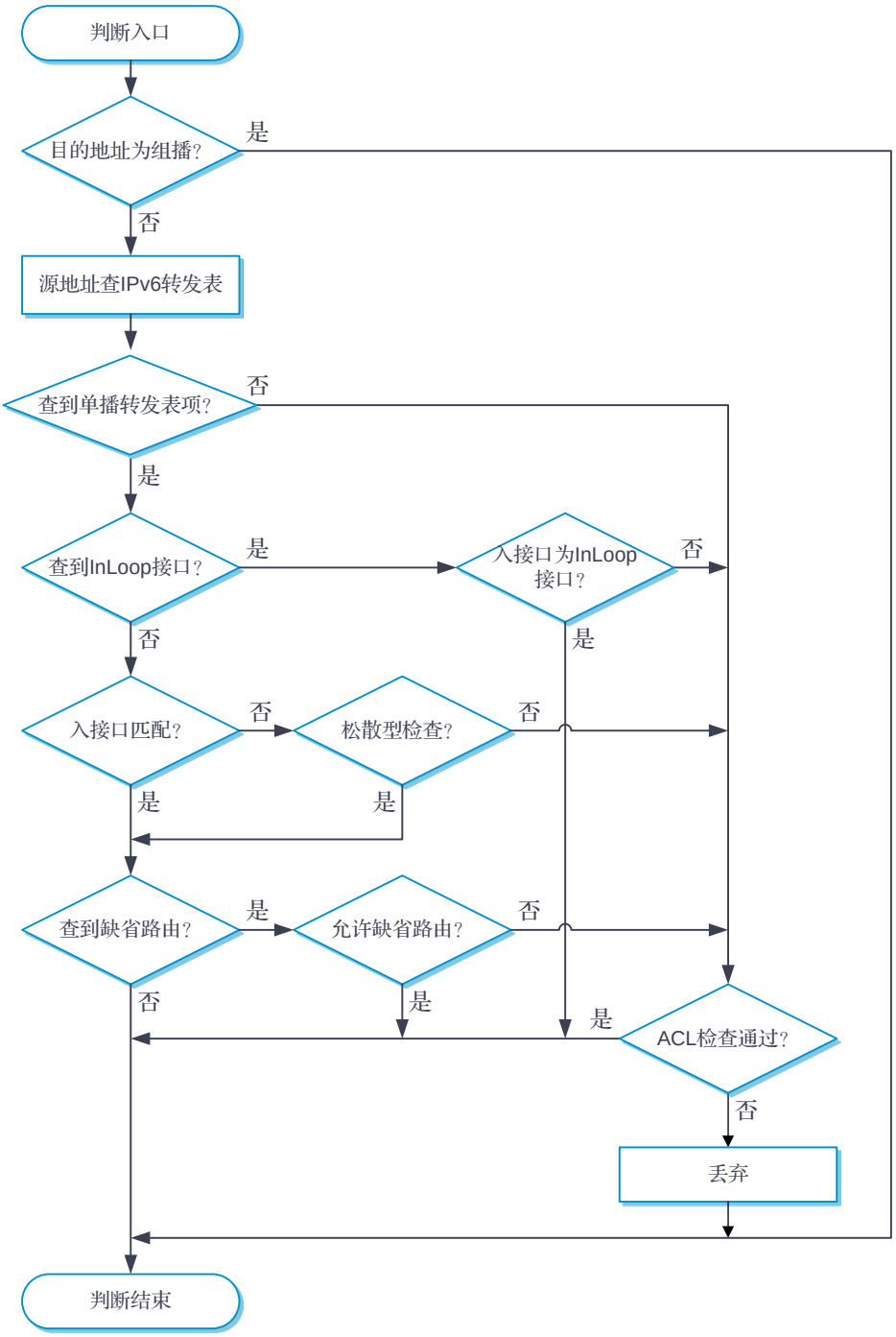
1. 检查地址合法性：
    - 对于目的地址是组播地址的报文，直接放行。
    - 对于源地址是全零地址的报文，如果目的地址是广播，则放行（源地址为 0.0.0.0，目的地址为 255.255.255.255 的报文，可能是 DHCP 或者 BOOTP 报文，不做丢弃处理）；如果目的地址不是广播，则进入步骤 7。
    - 对于不是上述情况的报文，则进入步骤 2。
2. 检查报文的源地址在转发表中是否存在匹配的单播路由：如果在转发表中查找失败（源地址是非单播地址则会匹配到非单播路由），则进入步骤 7，否则进入步骤 3；
3. 如果转发表中匹配的是上送本机路由，即查到 InLoop 接口，则检查报文入接口是否是 InLoop 接口：如果是，则直接放行，否则进入步骤 7；如果转发表中匹配的不是上送本机路由则继续步骤 4；
4. 如果转发表中匹配的是缺省路由，则检查用户是否配置了允许匹配缺省路由：如果没有配置，则进入步骤 7，否则进入步骤 5；如果转发表中匹配的不是缺省路由，则进入步骤 5；
5. 检查报文源地址与入接口是否匹配。反向查找报文出接口（反向查找是指查找以该报文源 IP 地址为目的 IP 地址的报文的出接口）或者缺省路由的出接口：如果其中至少有一个出接口和报文的入接口相匹配，则进入步骤 6；如果不匹配，则查看是否是松散型检查，如果是，则报文检查通过，进入步骤 7；否则说明是严格型检查，进入步骤 6；
6. 检查用户是否配置了对链路层信息进行检查：如果没有配置，则认为报文通过检查，进行正常的转发。如果已经配置，则根据转发表中的下一跳查询 ARP 表，并比较 IP 报文源 MAC 地址

与 ARP 表中的 MAC 地址是否一致。如果两者一致，则报文通过检查；如果查询失败或两者不一致，则进入步骤 7；

7. ACL 检查流程。如果报文符合 ACL，则报文继续进行正常的转发（此类报文称为被抑制丢弃的报文）；否则报文被丢弃。

IPv6 uRPF 处理流程

图-3 IPv6 uRPF 处理流程图



1. 检查地址合法性：对于目的地址是组播地址的报文直接放行。否则，进入步骤 2；

2. 检查报文的源地址在 IPv6 转发表中是否存在匹配的单播路由：如果在 IPv6 转发表中查找失败（源地址是非单播地址则会匹配到非单播路由），则进入步骤 6，否则进入步骤 3；

3. 如果 IPv6 转发表中匹配的是上送本机路由，则检查报文入接口是否是 InLoop 接口：如果是，则直接放行，否则进入步骤 6；如果 IPv6 转发表中匹配的不是上送本机路由则继续步骤 4；如果源地址是 Link-Local 地址，倘若这个地址是入接口的地址，并且入接口不是 InLoop 接口则进入步骤 6，否则直接放行；

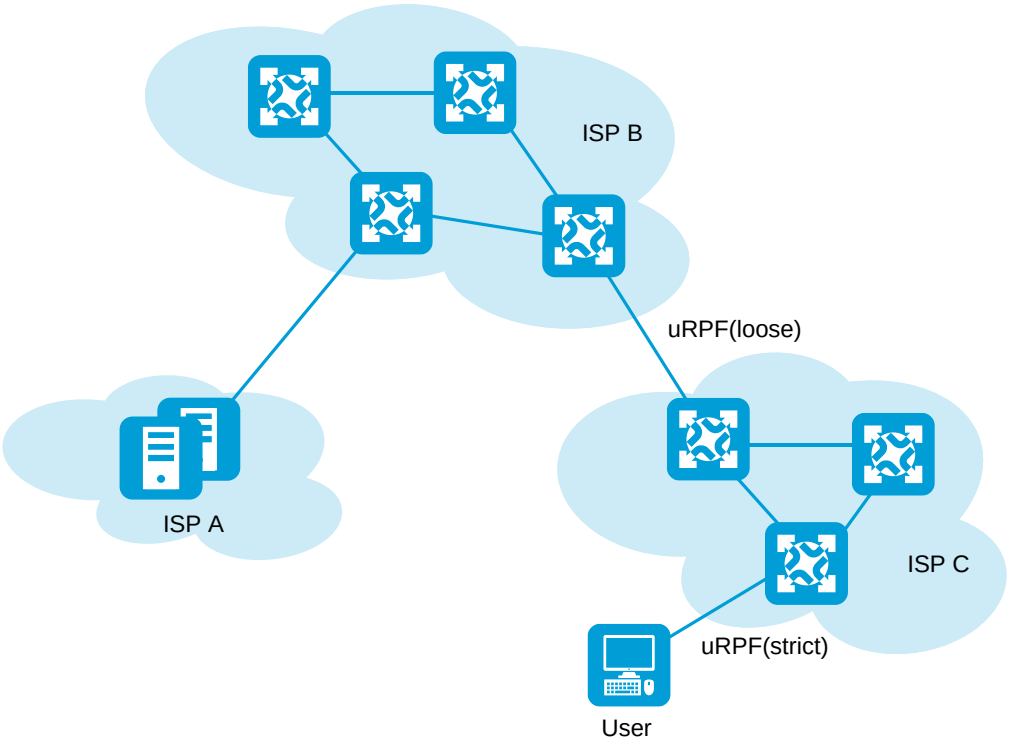
4. 检查报文源地址与入接口是否匹配：反向查找报文出接口（反向查找是指查找以该报文源 IPv6 地址为目的 IPv6 地址的报文的出接口）或者缺省路由的出接口，如果其中至少有一个出接口和报文的入接口相匹配，则进入步骤 5；如果不匹配，则查看是否是松散型检查，如果是，则进入步骤 5，否则说明是严格型检查，进入步骤 6；

5. 如果 IPv6 转发表中匹配的是缺省路由，则检查用户是否配置了允许匹配缺省路由，如果没有配置，则进入步骤 6，否则处理结束报文正常转发；如果 IPv6 转发表中匹配的不是缺省路由，则处理结束报文正常转发；

6. IPv6 ACL 检查流程。如果报文符合 IPv6 ACL，则报文继续进行正常的转发（此类报文称为被抑制丢弃的报文）；否则报文被丢弃。

uRPF 典型组网应用

图-4 uRPF 典型组网应用



通常在 ISP 上配置 uRPF，在 ISP 与用户端，配置严格型 uRPF 检查，在 ISP 与 ISP 端，配置松散型 uRPF 检查。

如果有特殊用户，或者具有一定特征，需要特殊处理的报文，可以配置 ACL 规则。

白名单

白名单功能即将特定的源 IP 地址加入白名单后，设备对于该地址发送的报文会跳过安全检查，而直接按照正常的转发流程进行处理，从而实现了报文的高速转发。

白名单不能直接指定 IP 地址，而需要通过引用地址对象组将 IP 地址加入白名单。白名单只能引用一个地址对象组，且只能由用户手工添加或删除。

使用限制和注意事项

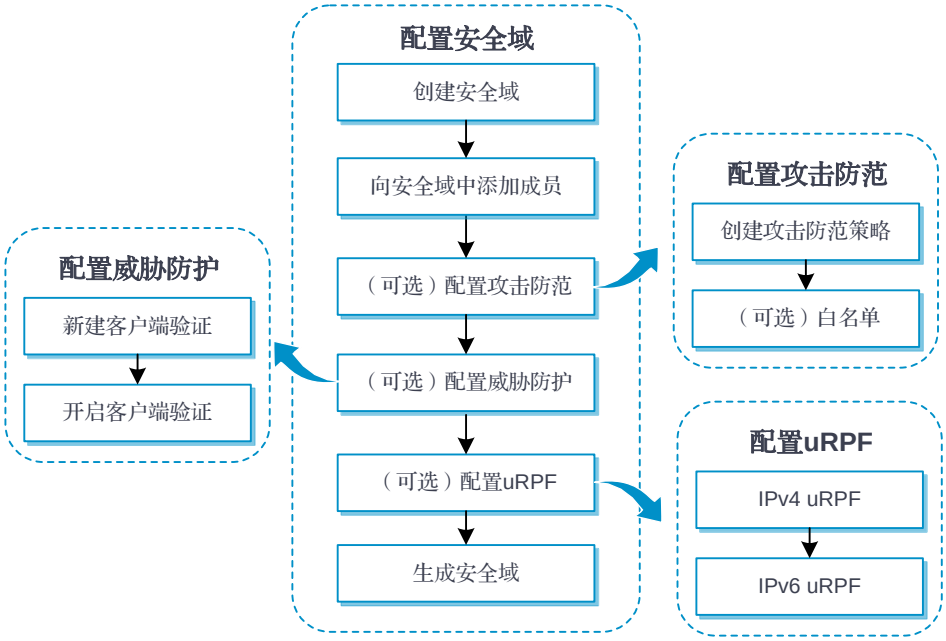
- 设备管理口缺省属于 Management 安全域，用户可以通过该接口登录 Web 管理页面管理设备，若移出 Management 安全域，则会立即断开 Web 访问，无法远程管理设备。
- 同一个三层接口只允许加入一个安全域。
- 同一个“二层接口和 VLAN”的组合只能加入到一个安全域中。
- 当报文未匹配对应安全域间实例时，若存在 **any** 到 **any** 的安全域间实例，则匹配 **any** 到 **any** 安全域间实例，否则直接丢弃报文。
- Management 和 Local 安全域间之间的报文缺省会被允许。
- Management 和 Local 安全域间之间的报文只能匹配 Management 与 Local 之间的安全域间实例，不会匹配 **any** 到 **any** 的安全域间实例。

配置指南

配置思路

安全域的配置思路如下图所示。

图-5 安全域配置指导图



创建安全域

安全域是一个逻辑概念，管理员将安全需求相同的接口进行分类，并划分到不同的安全域，能够实现域间策略的统一管理。可以通过域间策略实现对报文流的检查，并根据检查结果对报文执行相应动作。

1. 单击“网络 > 安全域”。
2. 在“安全域”页面单击<新建>按钮，进入新建安全域页面。
3. 新建安全域，具体配置内容如下：

表-1 安全域配置

参数	说明
安全域名称	表示安全域的名称
VLAN成员列表	配置安全域的VLAN成员
二层成员列表	配置安全域的二层接口成员
三层成员列表	配置安全域的三层接口成员
攻击防范策略	配置安全域执行的攻击防范策略
白名单	配置安全域是否开启白名单功能
TCP客户端验证	在指定安全域上开启/关闭TCP客户端验证功能，包括：

	• 关闭：关闭 TCP 客户端验证 • SYN Cookie：开启双向代理模式的 TCP 客户端验证 • Safe Reset：开启单向代理模式的 TCP 客户端验证
DNS客户端验证	在指定安全域上开启/关闭DNS客户端验证功能
DNS reply验证	在指定安全域上开启/关闭DNS reply验证功能
HTTP客户端验证	在指定安全域上开启/关闭HTTP客户端验证功能
HTTPS客户端验证	在指定安全域上开启/关闭HTTPS客户端验证功能
SIP客户端验证	在指定安全域上开启/关闭SIP客户端验证功能
IPv4 uRPF	滑动开启，并进行IPv4 uRPF配置
IPv6 uRPF	滑动开启，并进行IPv6 uRPF配置
检查方式	• 严格方式：不仅检查报文的源地址是否在转发表中存在，而且检查报文的入接口与转发表是否匹配 • 松散方式：仅检查报文的源地址是否在转发表中存在，而不再检查报文的入接口与转发表是否匹配
例外规则	访问控制列表，用来抑制报文丢弃 可选择已创建的IPv4 ACL，也可以新创建IPv4 ACL。此处新建的IPv4 ACL，可在“对象 > ACL > IPv4”页面查看
允许匹配缺省路由	允许源地址查转发表时匹配缺省路由表项
开启链路层检查功能	允许对链路信息进行检查

4. 单击<确定>按钮，新建安全域成功，并会在安全域页面中显示。

（可选）创建白名单

通过配置白名单功能可以使来自指定 IP 地址的报文跳过设备的安全检查。

白名单只能通过引用地址对象组进行添加，当一个 IP 地址加入白名单后，直到用户手工将其删除，否则一直存在。地址对象组在“对象 > 对象组”页面配置。

1. 单击“网络 > 安全域 > 白名单”。
2. 在“白名单”页面单击<新建>按钮。
3. 手工添加白名单，具体配置内容如下：

表-2 白名单配置

参数	说明
对象组类型	• IPv4 • IPv6
对象组名称	可以选择已创建的地址对象组，也可以新创建地址对象组。此处新建的地址对象组，象组”页面查看

4. 单击<确定>按钮，新建的白名单会在“白名单”页面显示。

（可选）配置客户端验证功能

通过手工添加受客户端验证保护的 IP 地址，对向该目的地址发送的连接请求进行代理。

受保护 IP 除了可以手工添加之外，还可以通过泛洪攻击防范自动添加。具体来讲就是，在客户端验证功能使能的前提下，若配置了泛洪攻击防范策略及相应的客户端验证功能，则设备检测到某服务器受到了指定类型的攻击时，设备会将该服务器 IP 地址添加到受保护 IP 列表中，并对后续指定类型的报文进行合法性检查。

1. 单击“网络 > 安全域 > 客户端验证”。
2. 在“客户端验证”页面单击<新建>按钮。
3. 新建客户端验证，具体配置内容如下：

表-3 受保护 IP 配置

参数	说明
协议类型	客户端验证的协议类型，包括： • TCP：TCP 客户端验证功能 • DNS：DNS 客户端验证功能 • DNS reply：DNS reply 验证功能 • HTTP：HTTP 客户端验证功能 • HTTPS：HTTPS 客户端验证功能 • SIP：SIP 客户端验证功能

VRF	受客户端验证保护的IP地址所属的VPN实例 可选择已创建的VRF，也可以新创建VRF。此处新建的VRF，可在“网络 > 接口与VRF > VRF”页面查看
IP地址类型	• IPv4 • IPv6
IP地址	受客户端验证保护的IP地址，即会对向该目的地址发送的连接请求进行代理 对于受TCP客户端验证保护的IP地址，发送的是TCP连接请求；对于受DNS客户端验证保护的IP地址，发送的是DNS query请求；对于受HTTP客户端验证保护的IP地址，发送的是HTTP GET/POST连接请求；对于受HTTPS客户端验证保护的IP地址，发送的是HTTPS请求；对于受SIP客户端验证保护的IP地址，发送的是UDP类型的INVITE请求
端口号	受客户端验证保护的端口号。缺省情况下，对于DNS客户端验证的受保护IP，则表示对端口53的DNS query连接请求做代理；对于HTTP客户端验证的受保护IP，则表示对端口80的HTTP GET/POST连接请求做代理；对于HTTPS客户端验证的受保护IP，则表示对端口443的HTTPS请求做代理；对于SIP客户端验证的受保护IP，则表示对端口5060的INVITE连接请求进行代理；对于TCP客户端验证的受保护IP，则表示对所有端口的TCP连接请求做代理

4. 单击<确定>按钮，新建的客户端验证会在“客户端验证”页面显示，该页面还会显示泛洪攻击防范自动添加的客户端验证。

接口

本帮助主要介绍以下内容：

- 特性简介
  - IPv4 地址
  - IPv6 地址
  - 链路聚合
  - VLAN 终结
- 使用限制和注意事项
- vSystem 相关说明
- 配置指南
  - 配置准备
  - 配置三层接口
  - 配置二层接口
  - 新建虚拟接口
  - 管理接口
  - 流量统计

特性简介

设备上支持的接口有以下几种：

- 二层以太网接口：是一种工作在数据链路层的物理接口，可以对接收到的报文进行二层交换转发。
- 三层以太网接口：是一种工作在网络层的物理接口，可以配置 IP 地址，可以对接收到的报文进行三层路由转发。
- 二、三层可切换以太网接口：是一种物理接口，可以工作在二层模式或三层模式下，作为一个二层以太网接口或三层以太网接口使用。
- 三层以太网子接口：是一种逻辑接口，工作在网络层，可以配置 IP 地址，处理三层协议。主要用来实现在三层以太网接口上支持收发 VLAN tagged 报文。
- 二层聚合接口：是一种逻辑接口，唯一对应一个二层聚合组，用于实现二层链路聚合。
- 三层聚合接口：是一种逻辑接口，可以配置 IP 地址，唯一对应一个三层聚合组，用于实现三层链路聚合。
- 三层聚合子接口：是一种逻辑接口，可以配置 IP 地址，主要用来实现在三层以太网聚合接口上支持收发 VLAN tagged 报文。
- LoopBack 接口：是一种逻辑接口，可以配置 IP 地址，LoopBack 接口创建后，除非手工关闭该接口，否则其物理层永远处于 up 状态。

- VLAN 接口：是一种逻辑接口，每个 VLAN 对应一个 VLAN 接口，在为 VLAN 接口配置了 IP 地址后，该 IP 地址即可作为本 VLAN 内网络设备的网关地址，此时该 VLAN 接口能对需要跨网段的报文进行三层转发。关于 VLAN 接口的详细信息，请参见“VLAN”。
- 冗余接口：是一种逻辑接口，可以配置 IP 地址，一个以太网冗余接口中包含两个成员接口，使用以太网冗余接口可以实现这两个接口之间的冗余备份。关于冗余接口的详细信息，请参见“双机热备”。
- 冗余子接口：是一种逻辑接口，可以配置 IP 地址，主要用来实现在以太网冗余接口上收、发带 VLAN Tag 的二层报文。关于冗余子接口的详细信息，请参见“双机热备”。

下面分别介绍各个接口可以配置的内容：

IPv4 地址

IPv4 地址分类和表示

IPv4 地址是每个连接到 IPv4 网络上的设备的唯一标识。IPv4 地址长度为 32 比特，通常采用点分十进制方式表示，即每个 IPv4 地址被表示为以小数点隔开的 4 个十进制整数，每个整数对应一个字节，如 10.1.1.1。

IPv4 地址由两部分组成：

- 网络号码字段（Net-id）：用于区分不同的网络。网络号码字段的前几位称为类别字段（又称为类别比特），用来区分 IPv4 地址的类型。

- 主机号码字段（Host-id）：用于区分一个网络内的不同主机。

IPv4 地址分为 5 类，每一类地址范围如下表所示。目前大量使用的 IPv4 地址属于 A、B、C 三类。

表-1 IPv4 地址类型

地址类型	地址范围	说明
A	0.0.0.0 ~ 127.255.255.255	IPv4地址0.0.0.0仅用于主机在系统启动时进行临时通信，并且无效目的地址 127.0.0.0网段的地址都保留作环回测试，发送到这个地址的分组到链路上，它们被当作输入分组在内部进行处理
B	128.0.0.0 ~ 191.255.255.255	-
C	192.0.0.0 ~ 223.255.255.255	-
D	224.0.0.0 ~ 239.255.255.255	组播地址
E	240.0.0.0 ~ 255.255.255.255	255.255.255.255用于广播地址，其它地址保留今后使用

子网和掩码

随着 Internet 的快速发展，IPv4 地址已近枯竭。为了充分利用已有的 IPv4 地址，可以使用子网掩码将网络划分为更小的部分（即子网）。通过从主机号码字段部分划出一些比特位作为子网号码字段，能够将一个网络划分为多个子网。子网号码字段的长度由子网掩码确定。

子网掩码是一个长度为 32 比特的数字，由一串连续的“1”和一串连续的“0”组成。“1”对应于网络号码字段和子网号码字段，而“0”对应于主机号码字段。

多划分出一个子网号码字段会浪费一些 IPv4 地址。例如，一个 B 类地址可以容纳 65534（216-2，去掉主机号码字段全 1 的广播地址和主机号码字段全 0 的网段地址）个主机号码。但划分出 9 比特长的子网字段后，最多可有 512（29）个子网，每个子网有 7 比特的主机号码，即每个子网最多可有 126（27-2，去掉主机号码字段全 1 的广播地址和主机号码字段全 0 的网段地址）个主机号码。因此主机号码的总数是 512*126=64512 个，比不划分子网时要少 1022 个。

若不进行子网划分，则子网掩码为默认值，此时子网掩码中“1”的长度就是网络号码的长度，即 A、B、C 类 IPv4 地址对应的子网掩码默认值分别为 255.0.0.0、255.255.0.0 和 255.255.255.0。

IPv6 地址

IPv6（Internet Protocol Version 6，互联网协议版本 6）是网络层协议的第二代标准协议，也被称为 IPng（IP Next Generation，下一代互联网协议），它是 IETF（Internet Engineering Task Force，互联网工程任务组）设计的一套规范，是 IPv4 的升级版本。IPv6 和 IPv4 之间最显著的区别为：地址的长度从 32 比特增加到 128 比特。

IPv6 地址表示方式

IPv6 地址被表示为以冒号（:）分隔的一连串 16 比特的十六进制数。每个 IPv6 地址被分为 8 组，每组的 16 比特用 4 个十六进制数来表示，组和组之间用冒号隔开，比如：2001:0000:130F:0000:0000:09C0:876A:130B。

为了简化 IPv6 地址的表示，对于 IPv6 地址中的“0”可以有下面的处理方式：

- 每组中的前导“0”可以省略，即上述地址可写为 2001:0:130F:0:0:9C0:876A:130B。
- 如果地址中包含一组或连续多组均为 0 的组，则可以用双冒号“::”来代替，即上述地址可写为 2001:0:130F::9C0:876A:130B。

IPv6 地址由两部分组成：地址前缀与接口标识。其中，地址前缀相当于 IPv4 地址中的网络号码字段部分，接口标识相当于 IPv4 地址中的主机号码部分。

地址前缀的表示方式为：IPv6 地址/前缀长度。其中，前缀长度是一个十进制数，表示 IPv6 地址最左边多少位为地址前缀。

IPv6 地址分类

IPv6 主要有三种类型的地址：单播地址、组播地址和任播地址。

- 单播地址：用来唯一标识一个接口，类似于 IPv4 的单播地址。发送到单播地址的数据报文将被传送给此地址所标识的接口。
- 组播地址：用来标识一组接口（通常这组接口属于不同的节点），类似于 IPv4 的组播地址。发送到组播地址的数据报文被传送给此地址所标识的所有接口。

- 任播地址：用来标识一组接口（通常这组接口属于不同的节点）。发送到任播地址的数据报文被传送给此地址所标识的一组接口中距离源节点最近（根据使用的路由协议进行度量）的一个接口。

IPv6 中没有广播地址，广播地址的功能通过组播地址来实现。

IPv6 地址类型是由地址前面几位（称为格式前缀）来指定的，主要地址类型与格式前缀的对应关系如下表所示。

表-2 IPv6 地址类型

地址类型		格式前缀（二进制）	IPv6 前缀标识	简介
单播地址	未指定地址	00...0（128 bits）	::/128	不能分配给任何节点。在节点获得有地址之前，可在发送的IPv6报文的源填入该地址，但不能作为IPv6报文中址
	环回地址	00...1（128 bits）	::1/128	不能分配给任何物理接口。它的作用中的环回地址相同，即节点用来给IPv6报文
	链路本地地址	1111111010	FE80::/10	用于邻居发现协议和无状态自动配置地上节点之间的通信。使用链路本地源或目的地址的数据报文不会被转发路上
	全球单播地址	其他形式	-	等同于IPv4公网地址，提供给网络服这种类型的地址允许路由前缀的聚合制了全球路由表项的数量

组播地址	11111111	FF00::/8	-
任播地址	从单播地址空间中进行分配，使用单播地址的格式		-

IEEE EUI-64 生成接口标识

IPv6 单播地址中的接口标识符用来唯一标识链路上的一个接口。目前 IPv6 单播地址基本上都要求接口标识符为 64 位。

不同接口的 IEEE EUI-64 格式的接口标识符的生成方法不同，分别介绍如下：

- 所有 IEEE 802 接口类型（例如，以太网接口、VLAN 接口）：IEEE EUI-64 格式的接口标识符是从接口的链路层地址 (MAC 地址) 变化而来的。IPv6 地址中的接口标识符是 64 位，而 MAC 地址是 48 位，因此需要在 MAC 地址的中间位置（从高位开始的第 24 位后）插入十六进制数 FFFE（1111111111111110）。为了使接口标识符的作用范围与原 MAC 地址一致，还要将 Universal/Local (U/L)位（从高位开始的第 7 位）进行取反操作。最后得到的这组数就作为 EUI-64 格式的接口标识符。
- Tunnel 接口：IEEE EUI-64 格式的接口标识符的低 32 位为 Tunnel 接口的源 IPv4 地址，ISATAP 隧道的接口标识符的高 32 位为 0000:5EFE，其他隧道的接口标识符的高 32 位为全 0。
- 其他接口类型（例如，Serial 接口）：IEEE EUI-64 格式的接口标识符由设备随机生成。

链路聚合

以太网链路聚合通过将多条以太网物理链路捆绑在一起形成一条以太网逻辑链路，实现增加链路带宽的目的，同时这些捆绑在一起的链路通过相互动态备份，可以有效地提高链路的可靠性。

聚合组

链路捆绑是通过接口捆绑实现的，多个以太网接口捆绑在一起后形成一个聚合组，而这些被捆绑在一起的以太网接口就称为该聚合组的成员端口。每个聚合组唯一对应着一个逻辑接口，称为聚合接口。聚合组与聚合接口的编号是相同的，例如聚合组 1 对应于聚合接口 1。

聚合组/聚合接口可以分为以下两种类型：

- 二层聚合组/二层聚合接口：二层聚合组的成员端口全部为二层以太网接口，其对应的聚合接口称为二层聚合接口。
- 三层聚合组/三层聚合接口：三层聚合组的成员端口全部为三层以太网接口，其对应的聚合接口称为三层聚合接口。

聚合接口的速率和双工模式取决于对应聚合组内的选中端口：聚合接口的速率等于所有选中端口的速率之和，聚合接口的双工模式则与选中端口的双工模式相同。

选中/非选中状态

聚合组内的成员端口具有以下两种状态：

- 选中（Selected）状态：此状态下的成员端口可以参与数据的转发，处于此状态的成员端口称为“选中端口”。
- 非选中（Unselected）状态：此状态下的成员端口不能参与数据的转发，处于此状态的成员端口称为“非选中端口”。

操作 Key

操作 Key 是系统在进行链路聚合时用来表征成员端口聚合能力的一个数值，它是根据成员端口上的一些信息（包括该端口的速率、双工模式等）的组合自动计算生成的，这个信息组合中任何一项的变化都会引起操作Key的重新计算。在同一聚合组中，所有的选中端口都必须具有相同的操作Key。

属性类配置

属性类配置：包含的配置内容如表-3 所示。在聚合组中，只有与对应聚合接口的属性类配置完全相同的成员端口才能够成为选中端口。

表-3 属性类配置

配置项	内容
端口隔离	端口是否加入隔离组、端口所属的端口隔离组
VLAN配置	端口上允许通过的VLAN、端口缺省VLAN、VLAN报文是否带Tag配

静态聚合

链路聚合分为静态聚合和动态聚合两种模式，处于静态聚合模式下的聚合组称为静态聚合组，处于动态聚合模式下的聚合组称为动态聚合组。

静态聚合和动态聚合工作时首先要选取参考端口，之后再确定成员端口的状态。

1. 选择参考端口

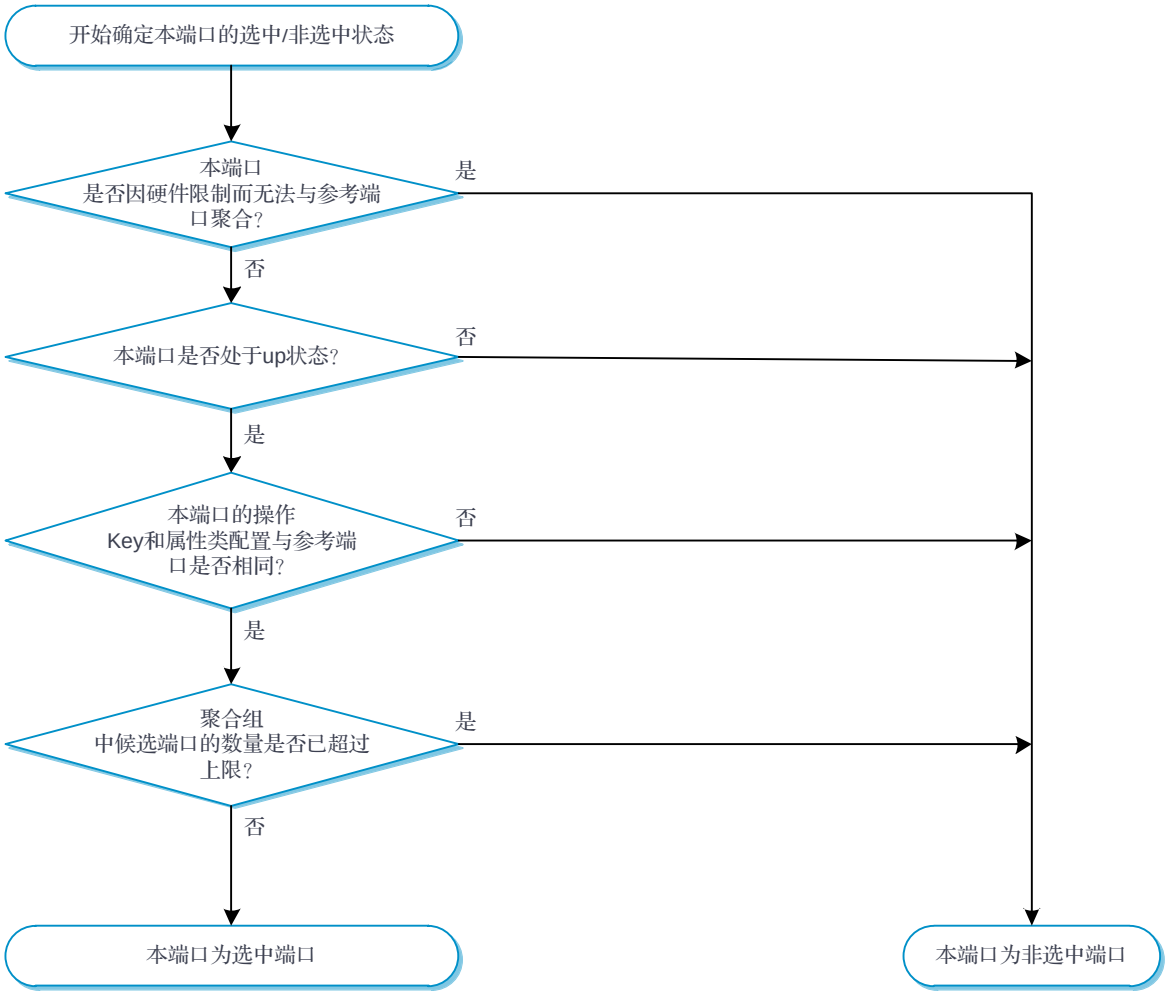
   参考端口从本端的成员端口中选出，其操作 Key 和属性类配置将作为同一聚合组内的其他成员端口的参照，只有操作 Key 和属性类配置与参考端口一致的成员端口才能被选中。

   对于聚合组内处于 up 状态的端口，按照端口的高端口优先级->全双工/高速率->全双工/低速率->半双工/高速率->半双工/低速率的优先次序，选择优先次序最高、且属性类配置与对应聚合接口相同的端口作为参考端口；如果多个端口优先次序相同，首先选择原来的选中端口作为参考端口；如果此时多个优先次序相同的端口都是原来的选中端口，则选择其中端口号最小的端口作为参考端口；如果多个端口优先次序相同，且都不是原来的选中端口，则选择其中端口号最小的端口作为参考端口。

2. 确定成员端口状态

   静态聚合组内成员端口状态的确定流程如图-1 所示。

图-1 静态聚合组内成员端口状态的确定流程



静态聚合模式一旦配置好后，端口的转发流量的状态就不会受网络环境的影响，比较稳定。

动态聚合

动态聚合模式通过 LACP（Link Aggregation Control Protocol，链路聚合控制协议）协议实现，动态聚合组内的成员端口可以收发 LACPDU（Link Aggregation Control Protocol Data Unit，链路聚合控制协议数据单元），本端通过向对端发送 LACPDU 通告本端的信息。当对端收到该 LACPDU

后，将其中的信息与所在端其他成员端口收到的信息进行比较，以选择能够处于选中状态的成员端口，使双方可以对各自接口的选中/非选中状态达成一致。

1. 选择参考端口

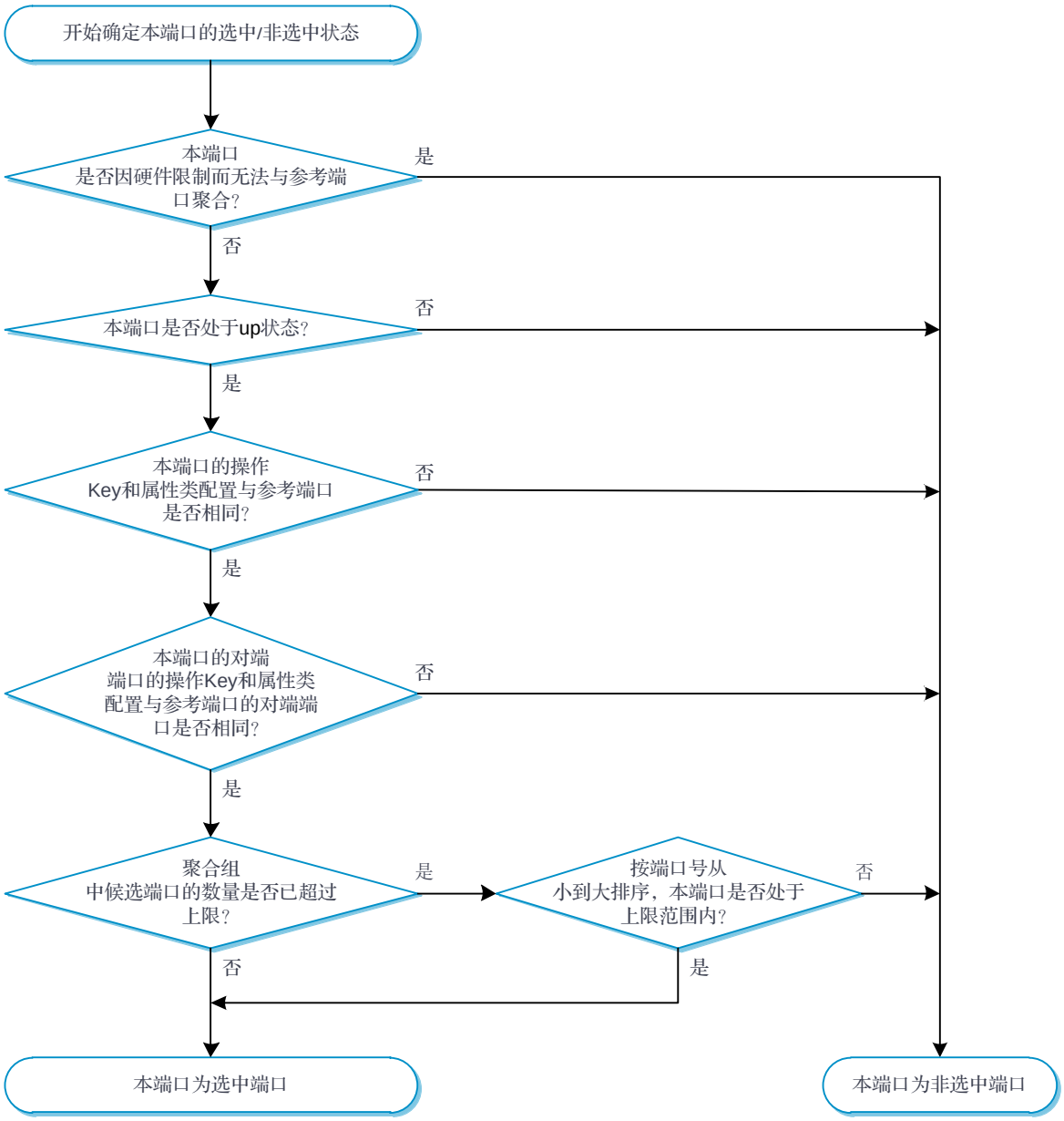
   参考端口从聚合链路两端处于 up 状态的成员端口中选出，其操作 Key 和属性类配置将作为同一聚合组内的其他成员端口的参照，只有操作 Key 和属性类配置与参考端口一致的成员端口才能被选中。

   - 首先，从聚合链路的两端选出设备 ID（由系统的 LACP 优先级和系统的 MAC 地址共同构成)较小的一端：先比较两端的系统 LACP 优先级，优先级数值越小其设备 ID 越小；如果优先级相同再比较其系统 MAC 地址，MAC 地址越小其设备 ID 越小。
   - 其次，对于设备 ID 较小的一端，再比较其聚合组内各成员端口的端口 ID（由端口优先级和端口的编号共同构成）：先比较端口优先级，优先级数值越小其端口 ID 越小；如果优先级相同再比较其端口号，端口号越小其端口 ID 越小。端口 ID 最小、且属性类配置与对应聚合接口相同的端口作为参考端口。

2. 确定成员端口的状态

   在设备 ID 较小的一端，动态聚合组内成员端口状态的确定流程如图-2 所示

图-2 动态聚合组内成员端口状态的确定流程



与此同时，设备 ID 较大的一端也会随着对端成员端口状态的变化，随时调整本端各成员端口的状态，以确保聚合链路两端成员端口状态的一致。

动态聚合模式能够根据对端和本端的信息调整端口的转发流量的状态，比较灵活。

VLAN 终结

VLAN 终结简介

VLAN 终结是指对接收到的报文，按照报文携带的 VLAN Tag 信息匹配对应的接口后，去除报文 VLAN Tag，再将报文进行三层转发或交由其他业务处理。转发出去的报文是否带有 VLAN Tag 由出接口决定，对从配置了 VLAN 终结的接口发送的报文，按照该接口上的终结配置，将相应的 VLAN Tag 添加到报文中后发送该报文。

VLAN 终结分类

根据对所终结的报文的不同处理方式，VLAN 终结分为以下类型：

- Dot1q 终结：用来终结带有一层及以上 VLAN Tag 的报文（要求最外层 VLAN ID 必须匹配配置值），从配置了 Dot1q 终结的接口发送的报文，都添加一层 VLAN Tag。
- Untagged 终结：用来终结收到的不带 VLAN Tag 的报文，从配置了 Untagged 终结的接口发送的报文，都不添加 VLAN Tag。
- Default 终结：用来终结同一主接口上其他子接口上无法处理的报文，从配置了 Default 终结的接口发送的报文，都不添加 VLAN Tag。

VLAN 终结工作机制

子接口（例如三层以太网子接口/三层聚合子接口）、VLAN 接口可以终结匹配最外层 VLAN ID 的报文或匹配最外两层 VLAN ID 的报文。其中，VLAN 接口只能终结最外层 VLAN ID 与接口编号相同的 VLAN 报文，例如 Vlan-interface10 只能终结最外层 VLAN ID 为 10 的报文。

主接口（例如三层以太网接口/三层聚合接口）本身不能对 VLAN 报文做终结处理，在主接口创建子接口后，由子接口来处理。

配置 VLAN 终结后，设备对收到的报文按如下优先级顺序匹配接口：

- 配置了 Dot1q 终结或者缺省支持 Dot1q 终结的子接口
- 配置了 Untagged 终结的子接口
- 配置了 Default 终结的子接口
- 主接口

当主接口的某个子接口配置了 Default 终结时，报文只能由主接口下的子接口处理，而不会匹配到主接口。

与 VLAN 接口绑定的主接口在收到 VLAN 报文后，根据 VLAN 接口的配置对报文进行处理。

使用限制和注意事项

- 接口禁用后，接口所连接网络需经过此设备的业务将会全部中断。

- 聚合链路的两端应配置相同的聚合模式。
- 对于静态聚合模式，用户需要保证在同一链路两端端口的选中/非选中状态的一致性，否则聚合功能无法正常使用。
- 用户删除聚合接口时，系统将自动删除对应的聚合组，且该聚合组内的所有成员端口将全部离开该聚合组。
- 在聚合接口上所作的有关属性配置，将被自动同步到对应聚合组内的所有成员端口上。当聚合接口被删除后，这些配置仍将保留在这些成员端口上。
- 配置了以太网冗余接口、冗余组节点的端口将不能加入三层聚合组。
- 二层聚合组和三层聚合组都分为静态聚合和动态聚合两种模式。
- 对于动态聚合模式，聚合链路两端的设备会自动协商同一链路两端的端口在各自聚合组内的选中/非选中状态，用户只需保证本端聚合在一起的端口的对端也同样聚合在一起，聚合功能即可正常使用。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置三层接口

三层以太网接口是一种工作在网络层的物理接口，可以配置 IP 地址，可以对接收到的报文进行三层路由转发。

1. 选择“网络 > 接口与 VRF > 接口”，进入“接口”页面。
2. 在“接口”页面选中需要配置的三层接口，单击<编辑>按钮，进入“修改接口设置”页面。
3. 选择工作模式为三层模式，具体配置内容如下：

表-4 配置参数表

参数	说明
不受控协议	勾选对应的协议后，接收或发送该协议的报文将直接被放行，不再被安全策略和带宽管理策略控
VRF	下拉选择VRF。可选中已有的VRF，如需新建VRF，具体的配置步骤请参见“网络 > 接口与VRF >
速率	接口传输数据的速度，包括： • 自协商：设备能够自动检测和选择最佳的传输速率 • 端口所支持的最大数据传输速率：不同的接口此处可选速率不一致，常见的以太网接口速率 100 Mbps、1 Gbps。
双工模式	下拉选择双工模式，包括： • 自协商：接口和对端接口自动协商来决定是工作在全双工还是半双工模式 • 全双工：接口在发送数据包的同时可以接收数据包 • 半双工：接口同一时刻只能发送或接收数据包
MAC地址	MAC地址，格式为H-H-H，子接口不支持修改mac地址
MTU	当设备收到一个报文后，如果发现报文长度比转发接口的MTU值大，则进行下列处理： • 如果报文不允许分片，则将报文丢弃； • 如果报文允许分片，则将报文进行分片转发。 为了减轻转发设备在传输过程中的分片和重组数据包的压力，更高效的利用网络资源，请根据实 合适的接口MTU值，以减少分片的发生
TCP MSS	设置通过接口发送的 TCP 数据段的最大数据负载大小

参数	说明
期望带宽	提供业务模块使用，不会对接口实际带宽造成影响
保持上一跳	开启保持上一跳功能后，该接口接收到正向流量的第一个IP报文，会在高速缓存中记录相应的流 跳信息，反向流量报文到达设备上进行转发时可以直接通过该上一跳信息指导报文进行转发。保 端的正向流量和本端到对端的反向流量走的是相同的路径，从而保证同一会话的流量能够进行相
IP地址	接口获取IPv4地址有以下几种方式： • 通过手动指定 IPv4 地址 • 通过 DHCP 分配得到 IPv4 地址 • 通过 PPPoE 获取 IPv4 地址 DHCP和PPPoE的支持情况与设备的款型有关，请以设备的实际界面为准
虚拟IP	虚拟IP地址是IP地址的一种属性，该属性仅在RBM组网下生效，不影响其他情况下的使用。在R 拟IP地址可以简化HA（High Availability，高可靠性）功能的配置。将虚拟IP地址配置在HA主设 该地址会自动同步到备设备，不需要在主/备设备的业务接口上配置VRRP（Virtual Router Redund 虚拟路由器冗余协议）虚拟地址。虚拟IP地址仅在主备模式的主设备上配置，不支持双主模式， 上配置、修改或删除
全球单播地址	IPv6全球单播地址可以通过下面几种方式配置： • 采用 EUI-64 格式形成：当配置采用 EUI-64 格式形成 IPv6 地址时，接口的 IPv6 地址的前缀 而接口标识符则由接口自动生成； • 手工配置：用户手工配置 IPv6 全球单播地址； • 无状态自动配置：根据接收到的 RA 报文中携带的地址前缀信息及使用 EUI-64 功能生成的接 为接口生成 IPv6 全球单播地址； • 有状态获取地址：通过 DHCPv6 服务器自动获取 IPv6 地址。 一个接口上可以配置多个全球单播地址

参数	说明
链路本地地址	IPv6的链路本地地址可以通过两种方式获得： • 自动生成：设备根据链路本地地址前缀（FE80::/10）及使用 EUI-64 功能生成的接口标识， 链路本地地址； • 手工指定：用户手工配置 IPv6 链路本地地址 每个接口只能有一个链路本地地址，为了避免链路本地地址冲突，推荐使用链路本地地址的自动 配置链路本地地址时，手工指定方式的优先级高于自动生成方式。即如果先采用自动生成方式， 则手工指定的地址会覆盖自动生成的地址；如果先手工指定，之后采用自动生成的方式，则自动 口的链路本地地址仍是手工指定的。此时，如果删除手工指定的地址，则自动生成的链路本地地
EEE功能	开启该功能后，如果在连续一段时间内接口状态始终为up且没有收发任何报文，则接口自动进入 当接口需要收发报文时，接口又自动恢复到正常工作模式
端口流量控制	开启流量控制功能后，如果本端设备发生拥塞，将发送消息通知对端设备暂时停止发送报文；对 息后将暂时停止向本端发送报文；反之亦然。用于避免报文丢失 开启接收时流量控制功能后，当本端收到对端的流量控制报文，会停止向对端发送报文；当本端 备不能向对端发送流量控制报文
超长帧	长度大于标准以太网帧长的帧。当报文长度大于超长帧允许的长度，会被丢弃
帧长度	帧的长度，一般为9216字节
广播风暴抑制	开启该功能后，当接口上的广播流量超过抑制阈值时，系统会丢弃超出流量限制的报文，将流量 内，保证网络业务的正常运行。配置ratio 100表示不限制 • ratio：接口允许通过的最大流量占该接口带宽的百分比，取值为 100 表示不抑制 • pps：接口每秒允许转发的最大包数，取值范围为 0~1.4881×接口带宽 • kbps：接口每秒允许转发的最大千比特数，取值范围为 0~接口带宽
组播风	开启该功能后，当接口上的组播流量超过抑制阈值时，系统会丢弃超出流量限制的报文，将流量

参数	说明
暴抑制	内，保证网络业务的正常运行。配置ratio 100表示不限制 • ratio：接口允许通过的最大流量占该接口带宽的百分比，取值为 100 表示不抑制 • pps：接口每秒允许转发的最大包数，取值范围为 0~1.4881×接口带宽 • kbps：接口每秒允许转发的最大千比特数，取值范围为 0~接口带宽
未知单播风暴抑制	开启该功能后，当接口上的单播流量超过抑制阈值时，系统会丢弃超出流量限制的报文，将流量 内，保证网络业务的正常运行 • ratio：接口允许通过的最大流量占该接口带宽的百分比，取值为 100 表示不抑制 • pps：接口每秒允许转发的最大包数，取值范围为 0~1.4881×接口带宽 • kbps：接口每秒允许转发的最大千比特数，取值范围为 0~接口带宽

4. 单击<确定>按钮，接口配置完成。

配置二层接口

二层以太网接口是一种工作在数据链路层的物理接口，可以对接收到的报文进行二层交换转发。

1. 在“接口”页面选中需要配置的接口，单击<编辑>按钮，进入“修改接口设置”页面。

2. 选择工作模式为二层模式，具体配置内容如下：

表-5 配置参数表

参数	说明
速率	接口传输数据的速度，包括： • 自协商：设备能够自动检测和选择最佳的传输速率 • 端口所支持的最大数据传输速率：不同的接口此处可选速率不一致，常见的以太网接口速率 100 Mbps、1 Gbps。
双工模式	下拉选择双工模式，包括： • 自协商：接口和对端接口自动协商来决定是工作在全双工还是半双工模式。 • 全双工：接口在发送数据包的同时可以接收数据包。 • 半双工：接口同一时刻只能发送或接收数据包。
MAC地址	MAC地址，格式为H-H-H，子接口不支持修改mac地址
MDIX	下拉选择MDIX，包括： • 自协商：端口自动适应直通线或交叉线。 • 直通：直通线用于连接不同类型设备。 • 交叉：交叉线用于连接同种类型设备。
期望带宽	提供业务模块使用，不会对接口实际带宽造成影响。
链路类型	根据端口在转发报文时对VLAN Tag的不同处理方式，可将端口的链路类型分为三种： • Access：端口只能发送一个 VLAN 的报文，发出去的报文不带 VLAN Tag。一般用于和不能的用户终端设备相连，或者不需要区分不同 VLAN 成员时使用。 • Trunk：端口能发送多个 VLAN 的报文，发出去的端口缺省 VLAN 的报文不带 VLAN Tag，报文都必须带 VLAN Tag。通常用于网络传输设备之间的互连。

参数	说明
	• Hybrid：端口能发送多个 VLAN 的报文，端口发出去的报文可根据需要配置某些 VLAN 的 Tag，其他 VLAN 的报文都必须带 VLAN Tag。通常用于网络传输设备之间的互连。
PVID	接口缺省VLAN的编号。端口收到不带VLAN Tag的报文时，会在缺省VLAN中传输；发送缺省V Access和Trunk端口会去掉VLAN Tag再发送。Access端口的缺省VLAN就是它所在的VLAN Hybrid端口可以允许多个VLAN通过，能够配置端口缺省VLAN。
BPDU 报文拦截	开启后，可以防止未经授权的BPDU报文在生成树协议中的传播。
EEE功能	开启该功能后，如果在连续一段时间内接口状态始终为up且没有收发任何报文，则接口自动进 当接口需要收发报文时，接口又自动恢复到正常工作模式
端口流量控制	开启流量控制功能后，如果本端设备发生拥塞，将发送消息通知对端设备暂时停止发送报文； 该消息后将暂时停止向本端发送报文；反之亦然。用于避免报文丢失。 开启接收时流量控制功能后，当本端收到对端的流量控制报文，会停止向对端发送报文；当本 设备不能向对端发送流量控制报文。
超长帧	长度大于标准以太网帧长的帧。当报文长度大于超长帧允许的长度，会被丢弃。
帧长度	帧的长度，一般为9216字节
广播风暴抑制	开启该功能后，当接口上的广播流量超过抑制阈值时，系统会丢弃超出流量限制的报文，将流 范围内，保证网络业务的正常运行。配置ratio 100表示不限制。 ratio：接口允许通过的最大流量占该接口带宽的百分比，取值为100表示不抑制。 pps：接口每秒允许转发的最大包数，取值范围为0~1.4881×接口带宽。 kbps：接口每秒允许转发的最大千比特数，取值范围为0~接口带宽。
组播风暴抑制	开启该功能后，当接口上的组播流量超过抑制阈值时，系统会丢弃超出流量限制的报文，将流 范围内，保证网络业务的正常运行。配置ratio 100表示不限制。

参数	说明
	ratio：接口允许通过的最大流量占该接口带宽的百分比，取值为100表示不抑制。 pps：接口每秒允许转发的最大包数，取值范围为0~1.4881×接口带宽。 kbps：接口每秒允许转发的最大千比特数，取值范围为0~接口带宽。
未知单播风暴抑制	开启该功能后，当接口上的单播流量超过抑制阈值时，系统会丢弃超出流量限制的报文，将流 范围内，保证网络业务的正常运行。 ratio：接口允许通过的最大流量占该接口带宽的百分比，取值为100表示不抑制。 pps：接口每秒允许转发的最大包数，取值范围为0~1.4881×接口带宽。 kbps：接口每秒允许转发的最大千比特数，取值范围为0~接口带宽。

3. 单击<确定>按钮，接口配置完成。

新建虚拟接口

虚拟接口分为多种类型，设备支持新建的虚拟接口包括、聚合接口、VLAN 接口、Loopback 接口等。

通过新建不同类型的虚拟接口，可满足不同的业务需求。

1. 在“接口”页面单击<新建>按钮，进入“新建接口”页面。

2. 选择接口类型，具体配置内容如下表所示：

表-6 接口配置参数表

参数	说明
类型	接口的类型，包括： • 物理子接口 • 三层聚合子接口 • 冗余子接口 • 冗余接口 • 二层聚合接口 • 三层聚合接口 • VLAN 接口 • SSLVPN IP 接入接口 • LoopBack 接口
父接口	基础的物理接口，在这个父接口的基础上创建逻辑接口，用于处理特定类 仅物理子接口、三层聚合子接口和冗余子接口支持本参数
编号	用于标识接口的标识符 当类型为物理子接口、三层聚合子接口、冗余子接口、冗余接口、LoopBa 持本参数
聚合组编号	用于标识二层和三层聚合组的标识符
接口编号	用于标识SSLVPN IP接入接口的标识符
VLAN	选择VLAN，用于创建VLAN接口

3. 单击<确定>按钮，新建接口配置完成。

管理接口

在“接口”页面，选中需要配置的接口，单击<启用>、<禁用>、<恢复缺省配置>和<删除>按钮，可批量启用/禁用接口、恢复接口缺省配置以及删除接口。

流量统计

在“接口”页面，单击<流量统计功能>，可以查看各接口的流量，方便管理员进行监控和管理。

接口对

本帮助主要介绍以下内容：

- 特性简介
  - 隧道报文转发依据
  - VLAN ID 检查功能
  - Bypass 功能
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置准备
  - 配置反射模式的接口对
  - 配置黑洞模式的接口对
  - 配置转发模式的接口对
  - 配置跨 VLAN 模式的接口对
  - 配置高级设置

特性简介

接口对是在数据链路层对流量进行安全监控的一种技术。目前这种技术主要应用在安全产品上，经过设备的二层网络流量会被引流到安全产品上，由安全产品过滤后再进行转发。

接口对支持以下几种工作模式：

- 反射模式：报文从同一接口收发。
- 黑洞模式：报文从一个接口接收，处理完后被丢弃。
- 转发模式：报文从一个接口接收，从另一个接口发送。
- 跨 VLAN 模式：在不同 VLAN 间进行报文转发。

隧道报文转发依据

缺省情况下，设备对隧道报文进行转发时，根据封装后的信息进行转发。配置隧道报文的转发模式，可以根据封装前的信息进行转发。

VLAN ID 检查功能

在 Inline 转发时，开启此功能后，仅当报文的 VLAN ID 与会话表项中的 VLAN ID 匹配成功才放行此报文，否则丢弃。关闭此功能后，无需匹配 VLAN ID，仅需报文与会话表项中的其他信息匹配成功就可以放行此报文。

Bypass 功能

开启 Bypass 功能后，用户流量可以不经过安全业务或者安全设备处理，直接被处理（转发或丢弃）。

Bypass 功能分为以下几种模式：

内部 Bypass 功能

用户流量经过安全设备，但不进行安全业务处理。安全设备会根据配置的转发模式，选择对应的接口将用户流量直接转发或者丢弃。

支持的接口对工作模式：反射、黑洞和转发。

外部 Bypass 功能

用户流量不经过安全设备，直接通过 PFC（Power Free Connector，无源连接设备）设备转发。

本功能仅在接口对处于转发工作模式下支持。

外部 Bypass 功能分为外部静态和外部自动 Bypass 功能：

- 静态外部 Bypass 功能：用户流量直接通过 PFC 转发，不经过安全设备处理。
- 动态外部 Bypass 功能：在安全设备上将与 PFC 相连的两个接口加入接口对成员。安全设备通过检查这两个接口的状态，决定自动启用外部 Bypass 功能。当某一接口状态变为 DOWN 时，用户流量不经过安全设备，直接通过 PFC 转发。同时，安全设备会周期性检查成员的接口状态，如果检查到两个接口都处于 UP 状态，则自动关闭外部 Bypass 功能，恢复由安全设备处理用户流量。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 仅支持添加二层或者三层物理接口以及二层聚合接口到反射/黑洞/转发模式的接口对。
- 使用设备硬件 Bypass 子卡时，需要配置 Bypass 功能为内部模式。
- 外部 Bypass 功能的支持情况与设备型号有关，请以设备实际情况为准。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置反射模式的接口对

接口对是一种在数据链路层对流量进行安全监控的技术。新建之后，经过设备的二层网络流量会被引流到安全产品上，由安全产品过滤后再进行转发。通过不同的工作模式，接口对可以灵活处理流量。在反射模式下，报文在同一个接口上进行收发。由于流量不需要通过其他接口，所以数据处理速度较快。这种方式配置简单，适合新手快速配置。

1. 选择“网络 > 接口与 VRF > 接口对 > 接口对”，进入“接口对”页面。

2. 单击<新建>按钮，进入“新建接口对”页面。

3. 选择工作模式为反射模式，选择收发报文的接口，具体配置内容如下表所示：

表-1 接口对配置参数表

参数	说明
反射模式	报文从同一接口收发
Bypass功能	开启/关闭Bypass功能
成员-接口一	报文收发接口一

4. 单击<确定>按钮，反射模式的接口对会在“接口对”页面中显示。

配置黑洞模式的接口对

在黑洞模式下，报文从一个接口接收并在经过处理后被丢弃。这种模式流量进入后不再被转发。通过配置黑洞模式，管理员可以有效地丢弃不可信来源的流量，保证网络的安全性。

1. 在“接口对”页面，单击<新建>按钮，进入“新建接口对”页面。

2. 选择工作模式为黑洞模式，选择收发报文的接口，具体配置内容如下表所示：

表-2 接口对配置参数表

参数	说明
黑洞模式	报文从一个接口接收，处理完后被丢弃
Bypass功能	开启/关闭Bypass功能
成员-接口一	报文收发接口一

3. 单击<确定>按钮，新建黑洞模式的接口对会在“接口对”页面中显示。

配置转发模式的接口对

在转发模式下，报文从一个接口接收，从另一个接口发送。这种配置方式比较灵活，可以适应更复杂的网络环境。

1. 在“接口对”页面，单击<新建>按钮，进入“新建接口对”页面。

2. 选择工作模式为转发模式，选择收发报文的接口。具体配置内容如下表所示：

表-3 接口对配置参数表

参数	说明
转发模式	报文从一个接口接收，从另一个接口发送
Bypass功能	开启/关闭Bypass功能
成员-接口一	报文收发接口一
成员-接口二	报文收发接口二

3. 单击<确定>按钮，转发模式的接口对会在“接口对”页面中显示。

配置跨 VLAN 模式的接口对

在跨 VLAN 模式下，设备可以实现不同 VLAN 之间的路由和数据转发。跨 VLAN 模式与其他三种模式互斥，如果创建了跨 vlan 模式的接口对，则不能再创建其他模式的接口对。

1. 在“接口对”页面，单击<新建>按钮，进入“新建接口对”页面。

2. 选择工作模式为跨 VLAN 模式，添加收发报文的 VLAN。具体配置内容如下表所示：

表-4 接口对配置参数表

参数	说明
跨VLAN模式	在不同VLAN间进行报文转发
VLAN列表	指定一个VLAN编号，也可以指定VLAN编号范围，不论VLAN是否被创建， 跨VLAN模式

3. 单击<确定>按钮，跨 VLAN 模式的接口对会在“接口对”页面中显示。

配置高级设置

新建接口对后，通过高级设置可以选择不同的隧道报文转发依据和 VLAN ID 检查功能来应对不同的网络场景需求。

如在双机热备组网环境下，当主设备与备设备上报文入接口属于不同 VLAN 时，必须关闭 VLAN ID 检查功能，才能使从主设备上切换过来的流量或非对称的反向流量匹配备设备上的备份会话，实现安全业务功能的正常运行。

1. 选择“网络 > 接口与 VRF > 接口对 > 高级设置”，进入“高级设置”页面。

2. 配置高级设置参数，具体配置内容如下表所示：

表-5 高级设置配置参数表

参数	说明
隧道报文转发依据	隧道报文转发依据，包括： • 封装前报文：根据封装前原始报文信息进行转发 • 封装后报文：根据封装后的报文头信息进行转发
VLAN ID检查功能	开启/关闭VLAN ID检查功能

接口联动组

本帮助主要介绍以下内容：

- 特性简介
  - 工作原理
  - 典型组网
  - Monitor Link
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置准备
  - 配置接口联动组

特性简介

接口联动组功能通过将同一台设备上不同的接口加入同一联动组，实现属于同一联动组内各接口的状态相互关联，使得这些接口同时具备或不具备报文的收发能力。

工作原理

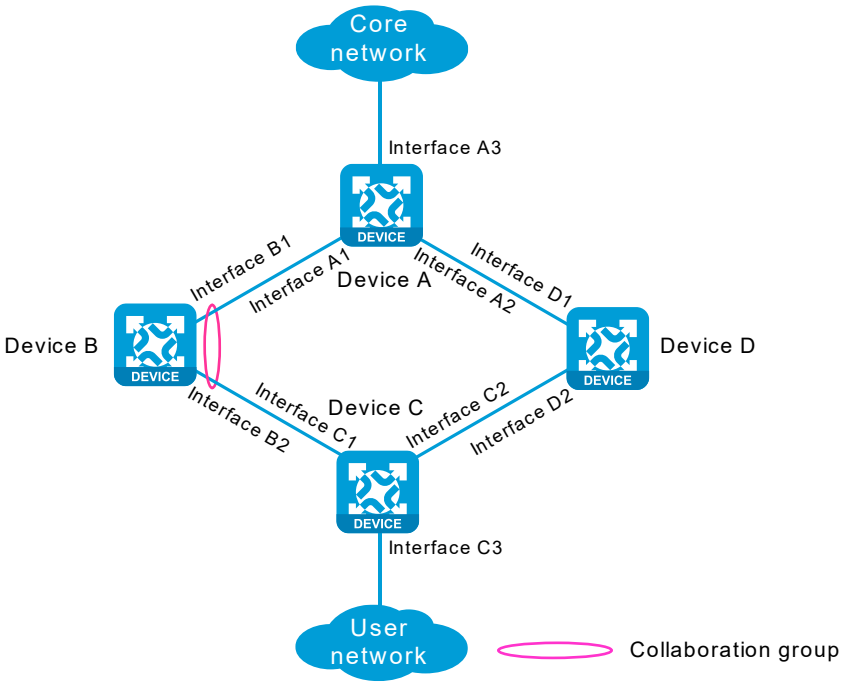
接口组联动功能的具体工作原理为：

- 当联动组内任一接口的物理状态为 down 时，联动组内的其它接口均被置为 Collaboration-down 状态，此时，联动组的状态为 Down。联动组内的所有接口都不能够收发报文。
- 当联动组内接口的状态由 down 变为 up 时，设备尝试将联动组内其它接口置为 up 状态。如果其它接口状态在 10 秒钟内均变为 up，则联动组状态为 Up，联动组内的所有接口都可以收发报文；如果超过 10 秒钟联动组内某一接口的状态不能 up，则将除该接口外的其它接口都置为 Collaboration-down 状态，此时联动组的状态为 Down，联动组内的所有接口都不能够收发报文。

典型组网

如图-1 所示，局域网用户通过 Device B 访问 Internet。当 Device B 上与 Device A 相连的接口 Interface B1 状态为 down 时，流量通过动态路由从 Device B 切换到备份设备 Device C。但是，由于 Device B 与局域网相连的接口 Interface B2 依然为 up 状态，导致动态路由更新时间较长，流量切换过程缓慢，影响局域网用户对 Internet 的访问。接口组联动功能通过在接口状态之间建立关联，保证 Device B 上与 Device A 相连的接口 Interface B1 状态为 down 时，Device B 与局域网相连的接口 Interface B2 也无法接收报文，从而加快动态路由更新和流量切换速度。

图-1 接口联动组典型组网



Monitor Link

是一种我司私有的接口联动方案，通过监控设备的上行接口，根据其 up/down 状态的变化来触发下行接口 up/down 状态的变化，从而触发下游设备上的拓扑协议进行链路的切换。要使用接口联动组，必须开启此功能。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 必须要开启 Monitor Link 协议，接口联动组功能才会生效。
- 一个接口只能属于一个联动组。
- 配置接口联动组的设备与其它设备通过多个接口相连时，不要将连接对端的所有接口都加入同一个联动组。否则，该联动组中有一个接口处于 down 状态时，对端接口都会变为 down 状态。
- 请勿将联动组成员接口加入聚合组或冗余组，否则会影响接口组联动功能的正常使用。
- 链路两端的接口，只有一端接口可以加入联动组。

配置指南

接口联动组功能通过将同一台设备上不同的接口加入同一联动组，实现属于同一联动组内各接口的状态相互关联，使得这些接口同时具备或不具备报文的收发能力。

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。

- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置接口联动组

接口联动组具体配置步骤如下：

1. 单击“网络 > 接口与 VRF > 接口联动组”。
2. 在接口联动组页面，单击<新建>按钮。
3. 在“新建接口联动组”页面的具体配置内容如下表所示：

表-1 接口联动组配置

参数	说明
联动组编号	接口联动组编号名称
成员接口	将接口加入到联动组内，一个接口只能属于一个联动组
回切延时	当设备重启后，如果联动组状态变为UP，但业务模块的功能尚未恢复正常，可能会 使用此功能设置延时时间，在设备重启后，即便所有成员接口准备就绪，也会使联 在延迟指定时间后才变为UP状态

4. 单击<确定>按钮，完成配置。

VRF

特性简介

VRF（Virtual Routing and Forwarding，虚拟路由和转发）用来实现不同 VPN 的路由隔离。每个 VRF 都有相对独立的路由表和 LFIB（Label Forwarding Information Base，标签转发信息库），确保 VPN 数据的独立性和安全性。

VRF 中的信息包括：LFIB、IP 路由表、与 VRF 关联的接口以及 VRF 的管理信息。其中 VRF 的管理信息包括 RD（Route Distinguisher，路由标识符）。

RD（Route Distinguisher，路由标识符）用来区分不同 VPN 的相同 IPv4 地址前缀，从而实现唯一标识网络中的一个站点。

RD 为 3～21 个字符的字符串。路由标识符有三种格式：

- 16 位自治系统号:32 位用户自定义数，例如：101:3。
- 32 位 IP 地址:16 位用户自定义数，例如：192.168.122.15:1。
- 32 位自治系统号:16 位用户自定义数字，其中的自治系统号最小值为 65536。例如：65536:1。

VRF 可以与支持多实例的协议（如组播、路由）进行绑定，实现该协议在不同 VRF 内可以独立运行并相互隔离。例如，在支持 OSPF 多实例的设备上，为每个 OSPF 进程绑定一个 VRF，通过该 OSPF 进程学习到的路由只能添加到相应 VRF 路由表。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置 VRF

VRF 配置步骤如下：

1. 单击“网络 > 接口与 VRF > VRF”。
2. 在 VRF 页面，单击<新建>按钮。
3. 进入“新建 VRF”页面，具体配置内容如下表所示：

表-1 VRF 配置

参数	说明
VRF	VPN实例名称
描述	配置VPN实例的描述信息
路由标识	VPN中IP地址的规划是由客户自行制定的，会导致不同的VPN使用相同的地址域，即 为解决此问题，通过将8个字节的RD作为IPv4地址前缀的扩展，使不唯一的IPv4地 的VPN-IPv4地址
IPv4路由门限	指定当前VPN实例的激活IPv4路由前缀的最大数量
IPv6路由门限	指定当前VPN实例的激活IPv6路由前缀的最大数量
关联接口列表	选择当前创建的VPN实例关联的接口

4. 单击<确定>按钮，新建 VRF 成功，且会在“VRF”页面中显示。

路由表

特性简介

在网络中路由器根据所收到的报文的目的地址选择一条合适的路径，并将报文转发到下一个路由器。路径中最后一个路由器负责将报文转发给目的主机。路由就是报文在转发过程中的路径信息，用来指导报文转发。

RIB（Routing Information Base，路由信息库），是一个集中管理路由信息的数据库，包含路由表信息以及路由周边信息（路由迭代信息、路由共享信息以及路由扩展信息）等。

对于相同的目的地，不同的路由协议、直连路由和静态路由可能会发现不同的路由，但这些路由并不都是最优的。为了判断最优路由，各路由协议、直连路由和静态路由都被赋予了一个优先级，具有较高优先级的路由协议发现的路由将成为最优路由。

除直连路由外，各路由协议的优先级都可由用户手工进行配置。另外，每条静态路由的优先级都可以不相同。数值越小表明优先级越高。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

查看路由表

路由表是设备根据目的 IP 地址决定数据包转发路径的重要依据。通过查阅路由表，设备能够确定数据包需要被发送到哪个下一跳设备。查看路由表可以帮助网络管理员诊断和解决网络连接问题，以及分析和调整路由表中的条目，优化数据传输路径，提高数据传输效率。

1. 选择“网络 > 路由 > 路由表”，单击“IPv4 路由表”或“IPv6 路由表”，可实现对 IPv4/IPv6 路由表概要信息的查看，显示内容如下：

表-1 IPv4 路由表/IPv6 路由表显示内容

参数	说明
目的地址	路由的目的IPv4/IPv6地址
掩码长度	IPv4地址的掩码长度，只有在“IPv4路由表”页面才会显示本参数
前缀长度	IPv6地址的前缀长度，只有在“IPv6路由表”页面才会显示本参数
协议类型	路由协议类型
路由度量	路由的度量值
优先级	路由的优先级
下一跳	路由的下一跳地址
出接口	到该目的网段的数据包将从此接口发出

2. 在“IPv4 路由表”或“IPv6 路由表”页面，单击<路由统计>按钮，可实现对 IPv4/IPv6 路由表统计信息的查看，统计内容如下：

表-2 IPv4/IPv6 路由统计信息显示内容

参数	说明
路由协议	路由协议类型
活跃路由	活跃的、正在使用的路由数目
已添加路由	路由器启动后或在上一次清除路由表后，路由表中添加的路由数目
已删除路由	标记为删除的路由数目（此类路由在等待一段时间后会被释放）
路由数	总的路由数目

静态路由

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 配置指南
  - 配置准备配置静态路由
  - 配置静态路由

特性简介

静态路由是一种特殊的路由，由管理员手工配置。当网络结构比较简单时，只需配置静态路由就可以使网络正常工作。静态路由不能自动适应网络拓扑结构的变化，当网络发生故障或者拓扑发生变化后，必须由管理员手工修改配置。

缺省路由是在没有找到匹配的路由表项时使用的路由。配置 IPv4 缺省路由时，指定目的地址为0.0.0.0/0；配置 IPv6 缺省路由时，指定目的地址为::/0。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置静态路由

静态路由是一种由网络管理员手动配置的路由方法，用于指定网络流量的具体路径。它简单易用、资源占用少，并能对数据流向进行精准控制。在拓扑结构稳定的环境中，它提供了稳定可靠的连接。

1. 选择“网络 > 路由 > 静态路由”，单击“IPv4 静态路由”或“IPv6 静态路由”，进入IPv4/IPv6 静态路由页面。

2. 在 IPv4/IPv6 静态路由页面，单击<新建>按钮，新建 IPv4/IPv6 静态路由，具体配置内容如下：

表-1 新建 IPv4/IPv6 静态路由参数表

参数	说明
VRF	静态路由所属的VRF
目的IP地址	IPv4静态路由的目的IP地址，只有在“新建IPv4静态路由”页面才会显示本 如果目的IP地址和掩码都为0.0.0.0（或掩码为0），则配置的路由为缺省路的路由表项时，将使用缺省路由进行报文转发。
目的IPv6地址	IPv6静态路由的目的IPv6地址，只有在“新建IPv6静态路由”页面才会显示
掩码长度	目的IPv4地址的掩码长度，只有在“新建IPv4静态路由”页面才会显示本参
前缀长度	目的IPv6地址的前缀长度，只有在“新建IPv6静态路由”页面才会显示本参
vSystem互通	开启/关闭缺省vSystem与非缺省vSystem以及非缺省vSystem之间的相互通

	开启vSystem互通时，不需要指定下一跳IP地址 本参数的支持情况与设备型号有关，请以页面的实际显示为准
下一跳	指定路由的下一跳，包括： • 下一跳所属的 VRF • 出接口 • 下一跳 IP 地址/下一跳 IPv6 地址
路由优先级	静态路由优先级 重新编辑路由优先级后，新设置的缺省优先级仅对新增的静态路由有效 对不同的优先级配置，可采用不同的路由管理策略。例如，为同一目的地 如果指定相同的优先级，则实现路由负载分担；如果指定不同的优先级，
路由标记	静态路由的标记
描述	静态路由的描述信息

3. 在新建 IPv4/IPv6 静态路由页面，单击<确定>按钮，新建静态路由会在 IPv4 静态路由/IPv6 静态路由列表显示。

策略路由

本帮助主要介绍以下内容：

- 特性简介
  - 策略路由简介
  - 策略
  - 节点匹配
  - 策略路由与 Track 联动
- vSystem 相关说明
- 配置指南
  - 配置策略路由

特性简介

策略路由简介

与单纯依照 IP 报文的目的地址查找路由表进行转发不同，策略路由是一种依据用户制定的策略进行路由转发的机制。策略路由可以对于满足一定条件（ACL 规则、报文长度、服务对象组、应用组）的报文，执行指定的操作（设置报文转发的下一跳、缺省下一跳、出接口和缺省出接口）。

策略

策略用来定义报文的匹配规则，以及对报文执行的操作。一个策略可以由一个或者多个节点组成。节点的构成如下：

- 每个节点由 NodeID 来标识。NodeID 越小节点的优先级越高，优先级高的节点优先被执行。
- 每个节点的具体内容由报文匹配规则和执行操作来指定。报文匹配规则定义该节点的匹配规则，执行操作定义该节点的动作。
- 每个节点对报文的处理方式由匹配模式决定。匹配模式分为允许和拒绝两种。

可以将已经配置的策略应用到本地，指导设备本身产生报文的发送。或是将已经配置的策略应用到接口，指导接口接收的所有报文的转发。

应用策略后，系统将根据策略中定义的匹配规则和执行操作，对报文进行处理：系统按照优先级从高到低的顺序依次匹配各节点，如果报文满足这个节点的匹配规则，就执行该节点的动作；如果报文不满足这个节点的匹配规则，就继续匹配下一个节点；如果报文不能满足策略中任何一个节点的匹配规则，则根据路由表来转发报文。

节点匹配

报文匹配规则

通过配置 ACL 规则、服务对象组、应用组或者报文长度来匹配报文，用于执行后续操作。

同一个节点中的各匹配规则之间是“与”的关系，即报文必须满足该节点的所有匹配规则才算满足这个节点的匹配规则。

执行操作

- 设置后续节点。如果当前节点中没有配置影响报文转发路径的五个执行操作(设置报文在指定 VRF 中进行转发、设置报文转发下一跳、设置报文转发的缺省下一跳、设置报文转发的出接口和设置报文转发的缺省出接口)，或者配置了这五个执行操作中的一个或多个，但配置都失效（下一跳不可达、出接口 down 或者报文在指定 VRF 内转发失败）时，会进行下一节点的处理。
- 设置报文的 IP 优先级。

- 设置报文头中的分片标志，允许或是不允许分片处理。
- 设置报文在指定 VRF 中进行转发，报文如果匹配了其中一个 VRF 下的转发表，报文将在该 VRF 中进行转发。
- 设置报文转发的下一跳或缺省下一跳，并为其配置与 Track 项关联或是指定当前下一跳是否为直连下一跳。
- 设置报文转发的出接口或缺省出接口，并为其配置与 Track 项关联。

策略路由与 Track 联动

策略路由通过与 Track 联动，增强了应用的灵活性和对网络环境变化的动态感知能力。

策略路由可以在配置报文的下一跳、缺省下一跳、出接口和缺省出接口时与 Track 项关联，根据 Track 项的状态来动态地决定策略的可用性。策略路由配置仅在关联的 Track 项状态为 Positive 或 NotReady 时生效。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置策略路由

策略路由是一种依据用户制定的策略进行路由转发的机制。允许网络管理员根据特定策略或条件来决定数据包的转发路径，不仅仅依赖于传统的路由表，能够在复杂的网络环境中优化流量管理和资源使用。

1. 选择“网络 > 路由 > 策略路由 > IPv4 策略路由/IPv6 策略路由”，进入 IPv4/IPv6 策略路由页面。

2. 单击<新建>按钮，新建 IPv4/IPv6 策略路由。

表-1 新建 IPv4/IPv6 策略路由参数表

参数	说明
策略名称	策略路由名称
应用于	将策略应用到本地报文或接口转发的报文

表-2 新建策略节点参数表

参数	说明
NodeID	策略节点编号。节点编号越小优先级越高，先对优先级高的节点进行匹配
模式	指定策略节点的匹配模式，包括： • 允许 • 拒绝
报文匹配规则	报文的匹配规则，包括： • 匹配报文长度：指定最短和最长的 IP 报文长度 • 匹配 IPv4/IPv6 ACL：指定 ACL 策略的编号或名称，可选择已创建 AC 新创建 ACL 策略 • 匹配服务对象组：指定服务对象组名称，可以选择已创建服务对象组， 服务对象组。仅 IPv4 策略路由支持本参数 • 匹配应用组：指定应用组名称，可以选择已创建应用组，也可以新创建 IPv4 策略路由支持本参数
执行操作-设置后续节点	设置匹配成功的当前节点指定转发路径失败后，继续进行后续节点的处理
执行操作-设置报文的IP优先级	设置IP报文的优先级值和类型，IP报文共有8（0～7）个优先级，每个数值对 类型
执行操作-设置IP报文头中的分片标志	设置IP报文头中的DF（Don’ t Fragment，不分片）标志，包括： • 0：允许分片操作 • 1：不允许分片操作 仅IPv4策略路由支持本参数

执行操作-设置报文在指定VRF中进行转发	设置报文在公网或指定VPN实例中进行转发
设置报文转发的下一跳地址	设置指导报文转发的下一跳，用户可以同时配置多个下一跳，起到主备或 1. 单击<新建>按钮，新建报文转发的下一跳地址 ○ VRF ○ IP 地址/IPv6 地址 ○ 缺省 ○ Track 项 ○ 直连下一跳 2. 单击<确定>按钮，新建下一跳地址将在报文转发的下一跳地址列表显
设置报文转发的出接口	设置指导报文转发的出接口，用户可以同时配置多个出接口，起到主备或 3. 单击<新建>按钮，新建报文转发的出接口 ○ 接口 ○ 缺省 ○ Track 项 4. 单击<确定>按钮，新建出接口将在报文转发的出接口列表显示 指定出接口类型需配置为P2P接口，对于非P2P接口（广播类型的接口和 口），比如以太网接口、Virtual-Template接口，由于有多个可能的下一跳 文转发不成功的现象

3. 在新建策略节点页面，单击<确定>按钮，新建策略节点显示在策略节点列表。

4. 在新建 IPv4/IPv6 策略路由页面，单击<确定>按钮，新建策略路由显示在 IPv4/IPv6 策略路由页面。

OSPF

本帮助主要介绍以下内容：

- 特性简介
  - OSPF 实例
  - OSPF 区域
  - OSPF 邻居
  - 不间断路由
  - OSPF 引入外部路由
  - DR/BDR
- vSystem 相关说明
- 配置指南
  - 配置思路
  - 配置准备
  - 配置 OSPF 功能
  - 配置 OSPFv3 功能

特性简介

OSPF 是一种基于链路状态的内部网关协议，其协议报文直接封装为 IP 报文，协议号为 89。

OSPF 支持 OSPFv2 和 OSPFv3 两个版本，目前针对 IPv4 协议使用的是 OSPFv2 版本，针对 IPv6 协议使用的是 OSPFv3 版本。

OSPF 实例

要在设备上使能 OSPF 功能，必须先创建 OSPF 实例、指定该实例关联的区域以及区域包括的网段和接口；对于当前设备来说，如果某个接口 IP 地址落在某个区域的网段内，则该接口属于这个区域并使能了 OSPF 功能，OSPF 将把这个接口的直连路由宣告出去。

OSPF 支持多实例，即可以在一台设备上通过为不同的 OSPF 实例指定不同的实例名称来启动多个 OSPF 实例。OSPF 实例是本地概念，不影响与其它设备之间的报文交换。因此，不同的设备之间，即使实例名称不同也可以进行报文交换。

OSPF 区域

OSPF 区域是从逻辑上将设备划分为不同的组，每个组用区域 ID 来标识。区域的边界是设备，而不是链路。一个设备可以属于不同的区域，但是一个网段（链路）只能属于一个区域，或者说每个运

行 OSPF 的接口必须指明属于哪一个区域。划分区域后，可以在区域边界设备上进行路由聚合，以减少通告到其他区域的 LSA 数量，还可以将网络拓扑变化带来的影响最小化。

OSPF 邻居

OSPF 网络中，设备在发送任何链路状态信息之前，必须先建立起正确的 OSPF 邻居邻接关系。

运行 OSPF 的设备使用 Hello 报文来建立邻居关系，设备会检查所收到的 Hello 报文中的各种参数。比如路由器标识、区域 ID、认证信息、网络掩码、Hello 时间间隔等，如果这些参数和接收接口上配置的对应参数都保持一致，则邻居关系就会建立起来，否则不会建立邻居关系。

不间断路由

NSR（Nonstop Routing，不间断路由）通过将 OSPF 链路状态信息从主进程备份到备进程，使设备在发生主备倒换时可以自行完成链路状态的恢复和路由的重新生成，邻接关系不会发生中断，从而避免了主备倒换对转发业务的影响。

OSPF 引入外部路由

当 OSPF 网络中的设备需要访问运行其他协议的网络中的设备时，需要将其他协议的路由引入 OSPF 网络中。例如，引入 IS-IS、BGP 生成的路由信息，将这些路由信息通过 Type5 LSA 或 Type7 LSA 向外宣告。

OSPF 是一个无环的动态路由协议，但这是针对域内路由和域间路由而言的。OSPF 对于引入的外部路由引发的路由环路没有很好的防范机制，因此在配置 OSPF 引入外部路由时一定要慎重，防止手工配置引发的环路。

DR/BDR

在广播网和 NBMA 网络中，任意两台路由器之间都要交换路由信息。如果网络中有 n 台路由器，则需要建立 n（n-1）/2 个邻接关系，当任何一台路由器的路由变化都会导致多次传递，浪费带宽资源。为了解决此问题，OSPF 提出了 DR 的概念，所有路由器只将信息发送给 DR，由 DR 将网络链路状态发送出去。BDR 是对 DR 的一个备份，当 DR 失效后，BDR 会立即成为新的 DR。既不是 DR 也不是 BDR 的路由器为 DR Other，DR Other 仅与 DR 和 BDR 建立邻接关系，DR Other 之间不交换任何路由信息，这样就减少了网络上各路由器之间邻接关系的数量，节约了带宽资源。

DR/BDR 是由同一网段中所有的路由器根据路由器优先级和 Router ID 通过 Hello 报文选举出来的，只有优先级大于 0 的路由器才具有选举资格。当进行 DR/BDR 选举时，路由器将自己选出的 DR 写

入 Hello 报文中，发给网段上每台运行 OSPF 协议的路由器，路由器优先级高者胜出，如果优先级相等，则 Router ID 大者胜出。

vSystem相关说明

非缺省 VSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

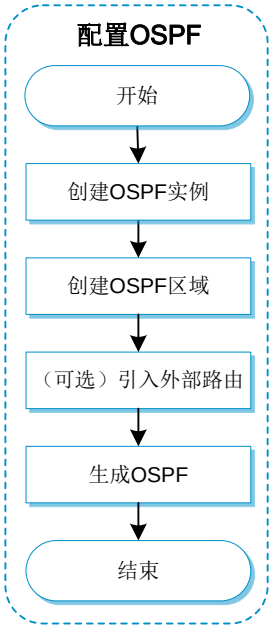
在配置 OSPF 引用外部路由时，只能引入路由表中状态为 active 的路由。

配置指南

配置思路

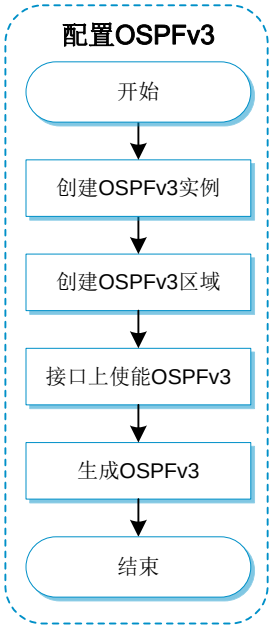
OSPF 功能的配置思路如下图所示：

图-1 OSPF 配置指导图



OSPFv3 功能的配置思路如下图所示：

图-2 OSPFv3 配置指导图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置 OSPF 功能

OSPF 是一种使用链路状态路由算法的内部网关协议，它能够快速计算出网络中的最短路径，IPv4 协议使用的是 OSPFv2 版本。

创建 OSPF 实例

1. 选择“网络 > 路由 > OSPF”。
2. 在“OSPF 实例”页面单击<新建>按钮，进入“新建 OSPF 实例”页面。
3. 新建 OSPF 实例，具体配置内容如下：

表-1 OSPF 实例配置参数表

参数	说明
版本	选择OSPF的版本，包括OSPFv2和OSPFv3
实例名称	表示OSPF实例的名称，同一版本的OSPF实例名称不能相同
VRF	配置OSPF实例所属的VPN实例
路由器标识	配置设备的Router ID
不间断路由	通过将OSPF链路状态信息从主进程备份到备进程，使设备在发生主备倒换时可以自行完成链路状态的恢复和路由的重新生成，邻接关系不会发生中断，从而避免主备倒换对转发业务的影响

4. 单击<确定>按钮，新建 OSPF 实例成功，并会在 OSPF 实例页面中显示。

创建 OSPFv2 区域

1. 选择“网络 > 路由 > OSPF”。
2. 在“OSPF 实例”页面单击 OSPFv2 版本实例对应的 OSPF 区域数目链接，进入“OSPFv2 区域”页面。
3. 在“OSPFv2 区域”页面单击<新建>按钮，进入“新建 OSPFv2 区域”页面。
4. 新建 OSPFv2 区域，具体配置内容如下：

表-2 OSPFv2 区域配置参数表

参数	说明
实例名称	表示OSPFv2区域所属的OSPFv2实例名称
区域ID	配置OSPFv2区域的ID
区域类型	配置区域的类型
网段	配置区域所包含的网段，一个网段只能属于一个区域；可手动逐条添加网段，也可添加设备的所有网段
接口	添加区域所包含的接口并配置接口参数 • 验证模式：设置接口对 OSPF 报文进行验证的验证模式

	• 密钥：设置验证模式时使用的密钥 • 接口类型：OSPF 的网络类型，用户可以根据需要更改接口的网络类型 • DR 优先级：接口的 DR 优先级决定了该接口在选举 DR/BDR 时所具有的资格，数值越大，优先级越高 • 协议开销值：手动配置接口的开销值，当没有指定开销值时，OSPF 根据带宽参考值自动计算接口的开销值，开销值低的将被优先选择 • 邻居失效时间：在邻居失效时间内，如果接口还没有收到邻居发送的 Hello 报文，路由器就会宣告该邻居无效 • Hello：接口向邻居发送 Hello 报文的时间间隔，可以调整 OSPF 网络的收敛速度以及协议报文带来的网络负荷

5. 单击<确定>按钮，新建 OSPFv2 区域成功，并会在 OSPFv2 区域页面中显示。

（可选）引入外部路由

1. 单击“OSPF 实例”页签返回 OSPF 实例页面，单击 OSPFv2 版本实例对应的引入外部路由数目链接，进入“OSPFv2 引入外部路由”页面。
2. 在“OSPFv2 引入外部路由”页面单击<新建>按钮，新建 OSPFv2 引入外部路由，具体配置内容如下。

表-3 OSPFv2 引入外部路由配置参数表

参数	说明
协议类型	引入不同类型的外部路由协议，将这些不同路由协议生成的路由信息向

	外宣告
实例名称	外部路由协议实例ID

3. 单击<确定>按钮，OSPFv2 引入外部路由配置成功。

配置 OSPFv3 功能

OSPFv3 是 OSPF 协议的一个扩展版本，在 OSPFv2 的基础上进行了增强，以适应 IPv6 网络的特性。

创建 OSPFv3 实例

1. 选择“网络 > 路由 > OSPF”。
2. 在“OSPF 实例”页面单击<新建>按钮，进入“新建 OSPF 实例”页面。
3. 新建 OSPFv3 实例，具体配置内容如下：

创建 OSPFv3 区域

1. 在“OSPF 实例”页面单击 OSPFv3 版本实例对应的 OSPF 区域数目链接，进入“OSPFv3 区域”页面。
2. 在“OSPFv3 区域”页面单击<新建>按钮，进入“新建 OSPF 区域”页面。

3. 新建 OSPFv3 区域，具体配置内容如下：

表-4 OSPFv3 区域配置参数表

参数	说明
区域类型	配置区域的类型
区域ID	配置OSPFv3区域的ID

4. 单击<确定>按钮，新建 OSPFv3 区域成功，并会在 OSPFv3 区域页面中显示。

接口上使能 OSPFv3 功能

1. 单击“OSPF 实例”页签返回 OSPF 实例页面，单击 OSPFv3 版本实例对应的已启用接口数目链接，进入“OSPFv3 接口”页面。
2. 在“OSPFv3 接口”页面单击<新建>按钮，进入“新建接口”页面。
3. 新建 OSPFv3 接口，具体配置内容如下：

表-5 OSPFv3 接口配置参数表

参数	说明
区域ID	配置接口所属的OSPFv3区域ID
接口名称	选择需要添加的接口名称

接口实例ID	配置接口实例的ID，同一接口下的不同接口实例可以添加至不同的OSPFv3实例中

4. 单击<确定>按钮，新建接口成功，并会在 OSPFv3 接口页面中显示。

IS-IS

本帮助主要介绍以下内容：

- 特性简介
  - 网络实体
  - IS-IS 区域
- vSystem 相关说明
- 配置指南
  - 配置 IS-IS

特性简介

IS-IS 属于 IGP（Interior Gateway Protocol，内部网关协议），用于自治系统内部。IS-IS 是一种链路状态协议，使用 SPF（Shortest Path First，最短路径优先）算法进行路由计算。

网络实体

网络实体名称（NET，Network Entity Title）指示的是 IS 本身的网络层信息，不包括传输层信息，可以看作是一类特殊的 NSAP，即 SEL 为 0 的 NSAP 地址。因此，NET 的长度与 NSAP 相同，为 8～20 个字节。

NET 由三部分组成：

- 区域 ID：它的长度是可变的，为 1～13 个字节。
- System ID：用来在区域内唯一标识主机或路由器，它的长度固定为 6 个字节。
- SEL：为 0，它的长度固定为 1 个字节。

例如 NET 为：ab.cdef.1234.5678.9abc.00，则其中区域 ID 为 ab.cdef，System ID 为 1234.5678.9abc，SEL 为 00。

通常情况下，一台路由器配置一个 NET 即可，当区域需要重新划分时，例如将多个区域合并，或者将一个区域划分为多个区域，这种情况下配置多个 NET 可以在重新配置时仍然能够保证路由的正确性。由于一台路由器最多可配置 3 个区域地址，所以最多也只能配置 3 个 NET。在配置多个 NET 时，必须保证它们的 System ID 都相同。

IS-IS 区域

为了支持大规模的路由网络，IS-IS 在路由域内采用两级的分层结构。一个大的路由域通常被分成多个区域 (Areas)。一般来说，我们将 Level-1 路由器部署在区域内，Level-2 路由器部署在区域间，Level-1-2 路由器部署在 Level-1 路由器和 Level-2 路由器的中间。

Level-1 路由器

Level-1 路由器负责区域内的路由，它只与属于同一区域的 Level-1 和 Level-1-2 路由器形成邻居关系，维护一个 Level-1 的 LSDB，该 LSDB 包含本区域的路由信息，到区域外的报文转发给最近的 Level-1-2 路由器。

属于不同区域的 Level-1 路由器不能形成邻居关系。

Level-2 路由器

Level-2 路由器负责区域间的路由，可以与同一区域或者其它区域的 Level-2 和 Level-1-2 路由器形成邻居关系，维护一个 Level-2 的 LSDB，该 LSDB 包含区域间的路由信息。所有 Level-2 路由器和 Level-1-2 路由器组成路由域的骨干网，负责在不同区域间通信，骨干网必须是物理连续的。

Level-2 路由器是否形成邻居关系与区域无关。

Level-1-2 路由器

同时属于 Level-1 和 Level-2 的路由器称为 Level-1-2 路由器。它可以与同一区域的 Level-1 和 Level-1-2 路由器形成 Level-1 邻居关系，也可以与同一区域或者其他区域的 Level-2 和 Level-1-2 路由器形成 Level-2 的邻居关系。Level-1 路由器必须通过 Level-1-2 路由器才能连接至其他区域。Level-1-2 路由器维护两个 LSDB，Level-1 的 LSDB 用于区域内路由，Level-2 的 LSDB 用于区域间路由。

vSystem相关说明

非缺省 VSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置 IS-IS

IS-IS 是一种链路状态路由协议，广泛应用于大型和复杂网络中。IS-IS 在路由域内采用两级的分层结构。一个大的路由域通常被分成多个区域。一般情况下，Level-1 路由器部署在区域内，Level-2 路由器部署在区域间，而 Level-1-2 路由器则部署在 Level-1 路由器和 Level-2 路由器的中间。

1. 选择“网络 > 路由 > IS-IS > IS-IS”。

2. 在“IS-IS”页面单击<新建>按钮，进入“新建 IS-IS 实例”页面。

3. 新建 IS-IS 实例，具体配置内容如下：

表-1 IS-IS 实例配置参数表

参数	说明
实例ID	IS-IS实例的ID
级别	路由器的Level级别，包括： • Level-1：配置路由器工作在 Level-1，它只计算区域内路由，维护 L1 的 LSDB • Level-2：配置路由器工作在 Level-2，只参加 L2 的 LSP 交换和 L2 的路由计算，维护 L2 的 LSDB • Level-1-2：配置路由器工作在 Level-1-2，同时参与 L1 和 L2 的路由计算，维护 L1 和 L2 两个 LSDB
网络实体名称	IS-IS进程的网络实体名称，格式为X…X.XXXX....XXXX.00，为十六进制数。前面的“X…X”是区域地址，中间的12个“X”是路由器的System ID，最后的“00”是SEL

4. 单击<确定>按钮，新建 IS-IS 实例成功，并会在 IS-IS 页面中显示。

5. 选择“网络 > 路由 > IS-IS > 接口列表”。

6. 进入“接口列表”页面，具体配置内容如下：

表-2 接口列表配置参数表

参数	说明
接口	IS-IS路由功能生效的接口
使能IS-IS	在指定接口使能IS-IS路由功能，并指定链路邻接关系类型，包括： • Level-1 • Level-2 • Level-1-2 如果路由器的Level级别是Level-1（Level-2），链路邻接关系类型只能为Level-1（Level-2），因此仅当路由器的Level级别是Level-1-2时，才需要通过配置链路邻接关系类型来限制接口上所能建立的邻接关系，让接口只发送和接收Level-1（Level-2）类型的Hello报文
Level-1链路开销值	在计算Level-1路由时使用的链路开销值
Level-2链路开销值	在计算Level-2路由时使用的链路开销值

7. 单击<应用>按钮，使指定接口的配置生效。

RIP

特性简介

RIP（Routing Information Protocol，路由信息协议）是一种较为简单的内部网关协议（Interior Gateway Protocol，IGP），主要用于规模较小的网络中，比如校园网以及结构较简单的地区性网络。对于更为复杂的环境和大型网络，一般不使用 RIP。

由于 RIP 的实现较为简单，在配置和维护管理方面也远比 OSPF 和 IS-IS 容易，因此在实际组网中仍有广泛的应用。

使用限制和注意事项

- 在多 RIP 进程情况下，不允许配置通告所有网段功能。
- 如果接口上配置了 RIP 版本，以接口配置的为准；如果接口没有进行 RIP 版本配置，接口运行的 RIP 版本将以全局配置的版本为准。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置 RIP 功能

RIP 是一种动态路由协议，用于在自治系统内交换路由信息。它基于距离矢量算法，使用跳数作为度量标准来选择最佳路径。

1. 选择“网络 > 路由 > RIP”，进入 RIP 页面。
2. 单击<新建>按钮，新建 RIP 实例。

表-1 新建 RIP 实例参数表

参数	说明
实例ID	RIP实例编号
VRF	RIP所属的VRF

网段	在指定网段上使能RIP，包括:
	• 通告网段
	  ○ 单击<添加>按钮，编辑网段地址和掩码
	  ○ 单击<确定>按钮，添加的网段将显示在通告网段列表中
	• 通告所有网段

引入外部路由	引入其它协议生成的路由 • 单击<添加>按钮，选择协议类型 • 输入实例 ID，只有 IS-IS、OSPF、EIGRP 或 RIP 协议类型才需要输入 • 单击<确定>按钮，引用的路由协议将显示在引入外部路由的列表中

接口	在指定接口上使能RIP。单击<添加>按钮，设置RIP接口

3. 在“新建 RIP 实例”页面，单击接口列表的<添加>按钮，在指定接口上使能 RIP。

4. 进入“RIP 接口设置”页面。

表-2 RIP 接口设置

参数		说明
接口名称		指定接口名称
RIP接口设置	版本	RIP版本，包括： • RIPv1：RIP 协议版本为 RIPv1 • RIPv2：RIP 协议版本为 RIPv2，报文发送方式为组播方式 • RIPv2 Broadcast：RIPv2 版本的报文发送方式为广播方式
	接收报文状态	开启/关闭接口接收RIP报文的状态
	发送报文状态	开启/关闭接口发送RIP报文的状态
RIP认证	验证模式	RIP-2报文的验证方式，包括： • Simple：简单验证方式 • MD5（RFC 2082）：指定 MD5 验证报文使用 RFC 2453 规定的报文 • MD5（RFC 2453）：指定 MD5 验证报文使用 RFC 2082 规定的报文 当RIP的版本为RIPv1时，虽然仍然可以配置验证方式，但由于RIPv1不 该配置不会生效

	密码	设置密码
	标识符	验证字标识符 只有“验证方式”选择MD5（RFC 2082），才会显示本参数

5. 在“RIP 接口设置”页面，单击<确定>按钮，添加的接口将在接口列表显示。

6. 在“新建 RIP 实例”页面，单击<确定>按钮，新建的 RIP 实例将在 RIP 列表显示。

ARP

- 特性简介
  - 地址解析协议
  - IP-MAC 绑定表项
  - ARP 防护
- vSystem 相关说明
- 配置指南
  - 配置准备
  - 配置 IP-MAC 绑定表项
  - 配置 ARP 表项
  - 配置 ARP 防护

特性简介

地址解析协议

ARP（Address Resolution Protocol，地址解析协议）是将 IP 地址解析为以太网 MAC 地址（或称物理地址）的协议。

设备通过 ARP 协议解析到目的 MAC 地址后，将会在自己的 ARP 表中增加 IP 地址和 MAC 地址映射关系的表项，以用于后续到同一目的地报文的转发。

ARP 表项分为两种：动态 ARP 表项、静态 ARP 表项。

动态 ARP 表项

动态 ARP 表项由 ARP 协议通过 ARP 报文自动生成和维护，可以被老化，可以被新的 ARP 报文更新，可以被静态 ARP 表项覆盖。当到达老化时间、接口状态 down 时，系统会删除相应的动态 ARP 表项。

动态 ARP 表项可以固化为静态 ARP 表项，但被固化后无法再恢复为动态 ARP 表项。

为了防止部分接口下的用户占用过多的 ARP 资源，可以通过设置接口学习动态 ARP 表项的最大个数来进行限制。

静态 ARP 表项

静态 ARP 表项通过手工创建或由动态 ARP 表项固化而来，不会被老化，不会被动态 ARP 表项覆盖。

配置静态 ARP 表项可以增加通信的安全性。静态 ARP 表项可以限制和指定 IP 地址的设备通信时只使用指定的 MAC 地址，此时攻击报文无法修改此表项的 IP 地址和 MAC 地址的映射关系，从而保护了本设备和指定设备间的正常通信。

在配置静态 ARP 表项时，如果管理员希望用户使用某个固定的 IP 地址和 MAC 地址通信，可以将该 IP 地址与 MAC 地址绑定；如果进一步希望限定用户只在指定 VLAN 的特定接口上连接，则需要进一步指定报文转发的 VLAN 和出接口。

一般情况下，ARP 动态执行并自动寻求 IP 地址到以太网 MAC 地址的解析，无需管理员的介入。

IP-MAC 绑定表项

为增强设备的安全性，系统提供了 IP-MAC 绑定功能，即在设备上建立 IP 地址与 MAC 地址的对应关系即 IP-MAC 绑定表项，并基于该表项实现报文的过滤控制。该功能适用于防御主机仿冒攻击，可有效过滤攻击者通过仿冒合法用户主机的 IP 地址或者 MAC 地址向设备发送的伪造 IP 报文。

IP-MAC 绑定表项可以通过手工配置和批量生成两种方式进行创建。

- 手工配置绑定表项是指通过手工方式逐条配置 IP-MAC 绑定表项。该方式适用于局域网络中主机较少的情况。

- 批量生成绑定表项是指通过指定接口下的 ARP 表项生成对应的 IP-MAC 绑定表项。该方式适用于局域网络中主机较多的情况。

配置 IP-MAC 绑定表项可以增加通信的安全性。设备收到报文后，提取报文头中的源 IP 地址和源 MAC 地址，并与 IP-MAC 绑定表项进行匹配。如果源 IP 地址和源 MAC 地址与 IP-MAC 绑定表项一致，则转发该报文；如果不一致，则认为该报文是非法报文，并将其丢弃。对于 IP 地址与 MAC 地址在 IP-MAC 绑定表项中都无匹配项的报文，则根据配置的缺省动作放行或丢弃。

ARP 防护

ARP 防护是根据 ARP 报文中源 IP 地址和源 MAC 地址检查用户是否是所属 VLAN 所在接口上的合法用户。

当设备作为 DHCP 服务器时，设备收到 ARP 报文后，直接对报文进行转发；其他场景下，设备收到 ARP 报文后，如果找到与报文匹配的长静态 ARP 表项（即指定了报文转发的 VLAN 和接口的静态 ARP 表项），则对报文进行转发；否则认为是非法报文，直接丢弃。

长静态 ARP 表项的支持情况与设备型号有关，请以页面实际显示为准。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置 IP-MAC 绑定表项

若要使 IP-MAC 绑定表项生效，则需要在指定接口下开启 IP-MAC 接口绑定功能。开启 IP-MAC 接口绑定功能后，设备会对该接口上入方向的报文进行 IP 地址与 MAC 地址绑定关系的检测。

IP-MAC 绑定表项的具体配置步骤如下：

1. 选择“网络 > ARP”，进入 ARP 页面。

2. 在 ARP 页面“配置 IP-MAC 绑定”下，配置批量生成 IP-MAC 绑定表项功能，具体的配置参数如下表所示。

表-1 配置 IP-MAC 绑定参数表

参数	说明
IP-MAC绑定功能	开启IP-MAC绑定功能
IP-MAC接口绑定功能	在指定接口下开启IP-MAC接口绑定功能。开启IP-MAC接口绑定功能后， 上入方向的报文进行IP地址与MAC地址绑定关系的检测 1. 在“接口列表”筛选指定接口 ○ 单击<添加>按钮，添加的接口在“成员列表”中显示 ○ 单击<全部添加>按钮，“接口列表”中所有接口将添加到“成员列 2. 单击<确认>按钮，保存设置
缺省动作	用于设置设备对IP地址、MAC地址都与IP-MAC绑定表项无匹配的报文的处 • 放行 • 丢弃

3. 在 ARP 页面的“IP-MAC 绑定列表”下，单击<新建>按钮，手工配置 IP-MAC 绑定表项，具体的配置参数如下表所示。

表-2 新建 IP-MAC 绑定参数表

参数	说明
IP地址	IP-MAC绑定表项的IP地址
MAC地址	IP-MAC绑定表项的MAC地址
VRF	IP-MAC绑定表项所属的VRF
VLAN	IP-MAC绑定表项所在的VLAN
时间段	IPv4-MAC绑定表项的生效时间段

状态	IPv4-MAC绑定表项的状态：
	• 生效
	• 不生效
	  ○ 时间段不生效
	  ○ VPN 不生效
	  ○ VPN 与时间段均不生效

4. 在“新建 IP-MAC 绑定”页面，单击<确定>按钮，新建 IP-MAC 绑定表项成功会在“IP-MAC 绑定列表”中显示。

配置 ARP 表项

ARP 表项的具体配置步骤如下：

1. 选择“网络 > ARP”，进入 ARP 页面。
2. 在 ARP 页面的“ARP 列表”下，单击<新建>按钮，手工配置静态 ARP 表项，具体的配置参数如下表所示。

表-3 新建 ARP 参数表

参数	说明
VRF	ARP表项所属的VRF
IP地址	ARP表项的IP地址
MAC地址	ARP表项的MAC地址
描述	ARP表项的描述信息
指定报文转发的VLAN和接口	指定报文只在指定VLAN的特定接口上转发 本功能的支持情况与设备型号有关，请以页面实际显示为准
VLAN	报文转发的VLAN，只有勾选“指定报文转发的VLAN和接口”才会显示本
接口	报文转发的接口，只有勾选“指定报文转发的VLAN和接口”才会显示本参

3. 在“新建 ARP”页面，单击<确定>按钮，新建 ARP 表项会在 ARP 列表显示，类型显示为“静态”。

4. 在“ARP 列表”中，勾选类型为“动态”的 ARP 表项前的复选框，单击<固化>按钮，可以将动态 ARP 表项固化为静态 ARP 表项，类型显示为“静态”，固化后无法再恢复为动态 ARP 表项。

5. 在“ARP 列表”中，勾选 ARP 表项前的复选框，单击<IP-MAC 绑定>按钮，ARP 表项生成对应的 IP-MAC 绑定表项，会在“IP-MAC 绑定列表”中显示。

配置 ARP 防护

ARP 防护的具体配置步骤如下：

1. 选择“网络 > ARP”，进入 ARP 页面。

2. 在 ARP 页面的“ARP 防护”下，可查看设备上所有 VLAN 是否开启了 ARP 防护功能。

表-4 ARP 防护参数表

参数	说明
VLAN	VLAN编号
ARP防护状态	VLAN的ARP防护状态，包括： • 开启

	• 关闭

3. 选择目标 VLAN，单击<开启>或<关闭>按钮，开启或关闭所选 VLAN 的 ARP 防护功能。

DHCP

本帮助主要介绍以下内容：

- 特性简介
- DHCP 服务器
  - DHCP 地址池
  - DHCP 服务器分配 IP 地址的次序
  - DHCP 选项
  - DHCP 服务器的 IP 地址冲突检测功能
- vSystem 相关说明
- 配置指南
  - 配置思路
  - 配置准备
  - 配置 DHCP 服务器

特性简介

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）用来为网络设备动态地分配 IP 地址等网络配置参数。

DHCP 采用客户端/服务器通信模式，由客户端向服务器提出请求分配网络配置参数的申请，服务器返回为客户端分配的 IP 地址等配置信息，以实现 IP 地址等信息的动态配置。

在 DHCP 的典型应用中，一般包含一台 DHCP 服务器和多台客户端（如 PC 和便携机）。如果 DHCP 客户端和 DHCP 服务器处于不同物理网段时，客户端可以通过 DHCP 中继与服务器通信，获取 IP 地址及其他配置信息。

DHCP服务器

在以下场合通常利用 DHCP 服务器来完成 IP 地址分配：

- 网络规模较大，手工配置需要很大的工作量，并难以对整个网络进行集中管理。
- 网络中主机数目大于该网络支持的 IP 地址数量，无法给每个主机分配一个固定的 IP 地址。
- 网络中只有少数主机需要固定的 IP 地址，大多数主机没有固定的 IP 地址需求。

DHCP 服务器通过地址池来保存为客户端分配的 IP 地址、租约有效期限、网关信息、域名后缀、DNS 服务器地址、WINS 服务器地址、NetBIOS 节点类型和 DHCP 选项信息。服务器接收到客户端发送的请求后，选择合适的地址池，并将该地址池中的信息分配给客户端。

DHCP 服务器在将 IP 地址分配给客户端之前，还需要进行 IP 地址冲突检测。

DHCP 地址池

地址池的地址管理方式有以下几种：

- 静态绑定 IP 地址，即通过将客户端的硬件地址或客户端 ID 与 IP 地址绑定的方式，实现为特定的客户端分配特定的 IP 地址；
- 动态选择 IP 地址，即在地址池中指定可供分配的 IP 地址段，当收到客户端的 IP 地址申请时，从该地址段中动态选择 IP 地址，分配给该客户端。

在 DHCP 地址池中还可以指定这两种类型地址的租约有效期限。

DHCP 服务器为客户端分配 IP 地址时，地址池的选择原则如下：

1. 如果存在将客户端 MAC 地址或客户端 ID 与 IP 地址静态绑定的地址池，则选择该地址池，并将静态绑定的 IP 地址和其他网络参数分配给客户端。
2. 如果不存在静态绑定的地址池，则按照以下方法选择地址池：
    - 如果客户端与服务器在同一网段，则将 DHCP 请求报文接收接口的 IP 地址与所有地址池配置的网段进行匹配，并选择最长匹配的网段所对应的地址池。
    - 如果客户端与服务器不在同一网段，即客户端通过 DHCP 中继获取 IP 地址，则将 DHCP 请求报文中 giaddr 字段指定的 IP 地址与所有地址池配置的网段进行匹配，并选择最长匹配的网段所对应的地址池。

DHCP 服务器分配 IP 地址的次序

DHCP 服务器为客户端分配 IP 地址的优先次序如下：

1. 与客户端 MAC 地址或客户端 ID 静态绑定的 IP 地址。
2. DHCP 服务器记录的曾经分配给客户端的 IP 地址。
3. 客户端发送的 DHCP-DISCOVER 报文中 Option 50 字段指定的 IP 地址。Option 50 为客户端请求的 IP 地址选项（Requested IP Address），客户端通过在 DHCP-DISCOVER 报文中添加该选项来指明客户端希望获取的 IP 地址。该选项的内容由客户端决定。
4. 按照动态分配地址选择原则，顺序查找可供分配的 IP 地址，选择最先找到的 IP 地址。
5. 如果未找到可用的 IP 地址，则从当前匹配地址池中依次查询租约过期、曾经发生过冲突的 IP 地址，如果找到则进行分配，否则将不予处理。

DHCP 选项

DHCP 利用选项字段传递控制信息和网络配置参数，实现地址动态分配的同时，为客户端提供更加丰富的网络配置信息。

Web 页面为 DHCP 服务器提供了灵活的选项配置方式，在以下情况下，可以使用 Web 页面 DHCP 选项功能：

- 随着 DHCP 的不断发展，新的 DHCP 选项会陆续出现。通过该功能，可以方便地添加新的 DHCP 选项。
- 有些选项的内容，RFC 中没有统一规定。厂商可以根据需要定义选项的内容，如 Option 43。通过 DHCP 选项功能，可以为 DHCP 客户端提供厂商指定的信息。
- Web 页面只提供了有限的配置功能，其他功能可以通过 DHCP 选项来配置。例如，可以通过 Option 4，IP 地址 1.1.1.1 来指定为 DHCP 客户端分配的时间服务器地址为 1.1.1.1。
- 扩展已有的 DHCP 选项。当前已提供的方式无法满足用户需求时 (比如通过 Web 页面最多只能配置 8 个 DNS 服务器地址，如果用户需要配置的 DNS 服务器地址数目大于 8，则 Web 页面无法满足需求），可以通过 DHCP 选项功能进行扩展。

下表为常用的 DHCP 选项编号。

表-1 DHCP 选项编号

选项编号	选项名称	推荐的选项填充类型
3	Router Option	IP地址
6	Domain Name Server Option	IP地址
15	Domain Name	ASCII字符串
43	Vendor Specific Information	十六进制数串
44	NetBIOS over TCP/IP Name Server Option	IP地址
46	NetBIOS over TCP/IP Node Type Option	十六进制数串

66	TFTP server name	ASCII字符串
67	Bootfile name	ASCII字符串

DHCP 服务器的 IP 地址冲突检测功能

为防止 IP 地址重复分配导致地址冲突，DHCP 服务器为客户端分配地址前，需要先对该地址进行探测。

DHCP 服务器的地址探测是通过 ping 功能实现的，通过检测是否能在指定时间内得到 ping 响应来判断是否存在地址冲突。DHCP 服务器发送目的地址为待分配地址的 ICMP 回显请求报文。如果在指定时间内收到回显响应报文，则认为存在地址冲突。DHCP 服务器从地址池中选择新的 IP 地址，并重复上述操作。如果在指定时间内没有收到回显响应报文，则继续发送 ICMP 回显请求报文，直到发送的回显请求报文数目达到最大值。如果仍然没有收到回显响应报文，则将地址分配给客户端，从而确保客户端获得的 IP 地址唯一。

vSystem相关说明

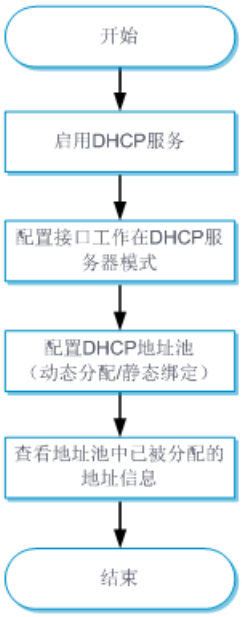
非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置思路

DHCP 服务器的配置思路如下图所示：

图-1 DHCP 服务器配置思路图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置 DHCP 服务器

要实现 DHCP 服务器功能，需要进行如下配置：

- 启用 DHCP 服务。
- 配置设备接口工作在 DHCP 服务器模式。
- 配置 DHCP 地址池。可以选择使用动态分配或静态绑定两种模式为 DHCP 客户端分配 IP 地址。也可以配置不参与自动分配的 IP 地址段，只有当前的地址池不能分配这些 IP 地址段，其他地址池仍然可以分配这些 IP 地址段。在 DHCP 地址池下还可以配置其他网络参数，包括租约有效期限、域名后缀、网关地址等。

配置地址分配

1. 选择“网络 > DHCP > 服务”，进入“服务”页面，启用 DHCP 服务。

2. 单击指定设备接口的<编辑>按钮，可选择配置设备接口是否工作在 DHCP 服务器模式。。缺省情况下，接口工作在 DHCP 服务器模式。

3. 选择“网络 > DHCP > 地址池”，进入“地址池”页面。

4. 在地址池页面，在页面顶部下拉框中选择已创建 DHCP 服务池，也可单击<新建地址池>按钮，进入“新建 DHCP 服务器地址池”页面，输入地址池名称，单击<确定>按钮，新建 DHCP 服务池。

5. 进入“新建 DHCP 服务器地址池”页面，输入地址池名称，单击<确定>按钮。

6. 选择“地址分配”页签，进入地址分配配置页面，具体的配置参数如下表所示。

表-2 地址分配参数表

参数	说明
动态分配的地址段	指定动态分配的地址范围
不参与自动分配的地址段	指定地址池中不参与自动分配的IP地址
静态绑定的地址列表	将客户端的硬件地址或客户端ID与IP地址绑定 1. 单击<新建>按钮 ○ IP 地址：静态绑定的 IP 地址 ○ 掩码：静态绑定 IP 地址的掩码 ○ 类型：客户端的类型包括以太网、令牌环网和客户端 ID ○ 硬件地址：静态绑定的客户端硬件地址，为 4 ~ 39 个字符的字符 只能包括十六进制数和“-”，且形式为 H-H-H…，除最后一个 H 位十六进制数外，其他均表示 4 位十六进制数

	○ 客户端 ID：静态绑定的客户端客户端 ID，为 4～254 个字符的字 中只能包括十六进制数和“-”，且形式为 H-H-H…，除最后一个 4 位十六进制数外，其他均表示 4 位十六进制数 2. 单击<确定>按钮，新建静态绑定关系显示在静态绑定的地址列表中

7. 单击<确定>按钮，保存地址分配配置。

配置地址池选项

1. 选择“地址池选项”页签，进入地址池选项配置页面，具体的配置参数如下表所示。

表-3 地址分配参数表

参数	说明
租约有效期限	DHCP地址池中分配的IP地址的租约有效期限，可配置无限期和具体的时间
域名后缀	DHCP客户端使用的域名后缀 在 DHCP 客户端进行域名解析时，用户只需要输入域名的部分字段 端会自动将输入的域名加上从 DHCP 服务器获得的域名后缀进行解
网关	DHCP客户端使用的网关地址 DHCP客户端访问本网段以外的服务器或主机时，数据必须通过网关进行转 每个DHCP地址池最多可以配置64个网关地址
DNS服务器	DHCP客户端使用的DNS服务器地址 为了使DHCP客户端能够通过域名访问Internet上的主机，DHCP服务器应在

	DNS（Domain Name System，域名系统）服务器地址
WINS服务器	DHCP客户端使用的WINS服务器地址 对于使用Microsoft Windows操作系统的客户端，由WINS服务器为通过Net 的主机提供主机名到IP地址的解析。所以，大部分Windows网络客户端需 设置。为了使DHCP客户端实现主机名到IP地址的解析，DHCP服务器应 端指定WINS服务器地址
NetBIOS节点类型	DHCP客户端使用的NetBIOS节点。DHCP客户端在网络上使用NetBIOS协 要在主机名和IP地址之间建立映射关系。根据获取映射关系方式的不同，N 括： • 广播（Broadcast）：此类节点采用广播方式获取映射关系。源节点通 的节点主机名的广播报文来获取目的节点的 IP 地址，目的节点收到广 将自己的 IP 地址返回给源节点 • 端到端（Peer-to-Peer）：此类节点采用发送单播报文与 WINS 服务器 取映射关系。源节点给 WINS 服务器发送单播报文，WINS 服务器收 返回源节点请求的目的节点名所对应的 IP 地址 • 混合（Mixed）：此类节点首先发送广播报文来获取映射关系，如果没有 发送单播报文与 WINS 服务器通信来获取映射关系 • 混合（Hybrid）：此类节点首先发送单播报文与 WINS 服务器通信来获 如果没有获取到，再发送广播报文来获取映射关系
DHCP选项	自定义DHCP地址池选项 3. 单击<新建>按钮 ○ DHCP 选项：DHCP 选项编号 ○ 类型：指定选项内容的类型，包括十六进制数串、ASCII 字符串和 ○ 选项内容：DHCP 选项内容 4. 单击<确定>按钮，新建的 DHCO 选项显示在 DHCP 选项列表中

2. 单击<确定>按钮，保存地址池选项配置。

查看已分配地址

选择“已分配地址”页签，可查看 IP 地址分配信息，包括分配的 IP 地址、客户端硬件地址/客户端 ID 以及租约到期时间。

DNS

本帮助主要介绍以下内容：

- 特性简介
  - 域名解析
  - DNS 过滤
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置思路
  - 配置准备
  - 配置静态域名解析
  - 配置动态域名解析
  - 配置 DNS 过滤
  - 配置域名后缀

特性简介

域名解析

DNS（Domain Name System，域名系统）是一种用于 TCP/IP 应用程序的分布式数据库，提供域名与 IP 地址之间的转换。IPv4 DNS 提供域名和 IPv4 地址之间的转换，IPv6 DNS 提供域名和 IPv6 地址之间的转换。

设备作为 DNS 客户端，当用户在设备上进行某些应用（如 Telnet 到一台设备或主机）时，可以直接使用便于记忆的、有意义的域名，通过域名系统将域名解析为正确的 IP 地址。

域名解析分为以下两种：

- 静态域名解析

  手工建立域名和 IP 地址之间的对应关系。当用户使用域名进行某些应用时，系统查找静态域名解析表，从中获取指定域名对应的 IP 地址。

- 动态域名解析

  使用动态域名解析时，需要手工指定域名服务器的 IP 地址。

  动态域名解析通过向域名服务器查询域名和 IP 地址之间的对应关系来实现将域名解析为 IP 地址。

  动态域名解析支持域名后缀列表功能。用户可以预先设置一些域名后缀，在域名解析的时候，用户只需要输入域名的部分字段，系统会自动将输入的域名加上不同的后缀进行解析。例如，

用户想查询域名 aabbcc.com，那么可以先在后缀列表中配置 com，然后输入 aabbcc 进行查询，系统会自动将输入的域名与后缀连接成 aabbcc.com 进行查询。

使用域名后缀的时候，根据用户输入域名方式的不同，查询方式分成以下几种情况：

- 如果用户输入的域名中没有“.”，比如 aabbcc，系统认为这是一个主机名，会首先加上域名后缀进行查询，如果所有加后缀的域名查询都失败，将使用最初输入的域名（如 aabbcc）进行查询。
- 如果用户输入的域名中间有“.”，比如 www.aabbcc，系统直接用它进行查询，如果查询失败，再依次加上各个域名后缀进行查询。
- 如果用户输入的域名最后有“.”，比如 aabbcc.com.，表示不需要进行域名后缀添加，系统直接用输入的域名进行查询，不论成功与否都直接返回结果。就是说，如果用户输入的字符中最后一个字符为“.”，就只根据用户输入的字符进行查找，而不会去匹配用户预先设置的域名后缀，因此最后这个“.”，也被称为查询终止符。带有查询终止符的域名，称为 FQDN（Fully Qualified Domain Name，完全合格域名）。

静态域名解析和动态域名解析可以配合使用。在解析域名时，首先采用静态域名解析（查找静态域名解析表），如果静态域名解析不成功，再采用动态域名解析。由于动态域名解析需要域名服务器的配合，会花费一定的时间，因而可以将一些常用的域名放入静态域名解析表中，这样可以大大提高域名解析效率。

DNS 过滤

DNS 过滤功能用于对 DNS 请求报文进行拦截或放行。设备目前支持基于白名单的域名访问控制，具体机制如下：

如果 DNS 代理收到的 DNS 请求报文中的域名命中白名单，则 DNS 代理放行该 DNS 请求报文，并在收到 DNS 响应报文后记录域名解析的结果，然后将 DNS 响应报文转发给 DNS 客户端。如果 DNS 代理收到的 DNS 请求报文中的域名未命中白名单，则 DNS 代理丢弃该 DNS 请求报文。

设备使用域名提供某些应用时（如 telnet 应用），如果希望实现严格的访问控制，建议使用白名单进行 DNS 过滤。

目前，设备支持的 DNS 过滤类型为 DNS 源地址透明代理：

DNS 源地址透明代理不仅能够提供代理服务，还会修改 DNS 请求报文的源地址，从而实现发送 DNS 请求报文的设备能够接收到相应的 DNS 响应报文。开启本功能后，当设备收到 DNS 客户端发往 DNS 服务器的请求报文时，首先查询本地缓存的域名解析表。如果存在相应的域名解析信息，则设备直接通过 DNS 应答报文将域名解析结果返回给 DNS 客户端。若设备在本地查询不到相应的域名解析信息，则将 DNS 请求报文的源 IP 地址修改为自身的地址再转发给 DNS 服务器，确保 DNS 应答报文能够返回设备。设备收到 DNS 服务器发来的应答报文后，在本地记录域名解析结果，并将报文转发给 DNS 客户端，DNS 客户端利用域名解析的结果进行相应的处理。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 使用动态域名解析查询主机名对应的 IPv4 地址时，优先向 IPv4 地址的域名服务器发送查询请求；如果查询失败，则再向 IPv6 地址的域名服务器发送查询请求。查询主机名对应的 IPv6 地址时，优先向 IPv6 地址的域名服务器发送查询请求；如果查询失败，则再向 IPv4 地址的域名服务器发送查询请求。
- 域名服务器的优先级顺序为：按照域名服务器优先级从高到低的顺序，依次向各个域名服务器发送查询请求。若优先级相同时，则按照域名服务器 IPv4/IPv6 地址从小到大的顺序，依次向各个域名服务器发送查询请求；设备上手工配置的域名服务器优先级高于通过 DHCP 等方式动态获取的域名服务器。设备首先向优先级最高的域名服务器发送查询请求，失败后再根据优先级从高到低的次序向其他域名服务器发送查询请求。
- 添加的域名后缀的优先级顺序为：先配置的域名后缀优先级高于后配置的域名后缀；设备上手工配置的域名后缀优先级高于通过 DHCP 等方式动态获取的域名后缀。设备首先添加优先级最高的域名后缀，查询失败后再依次添加其它域名后缀。

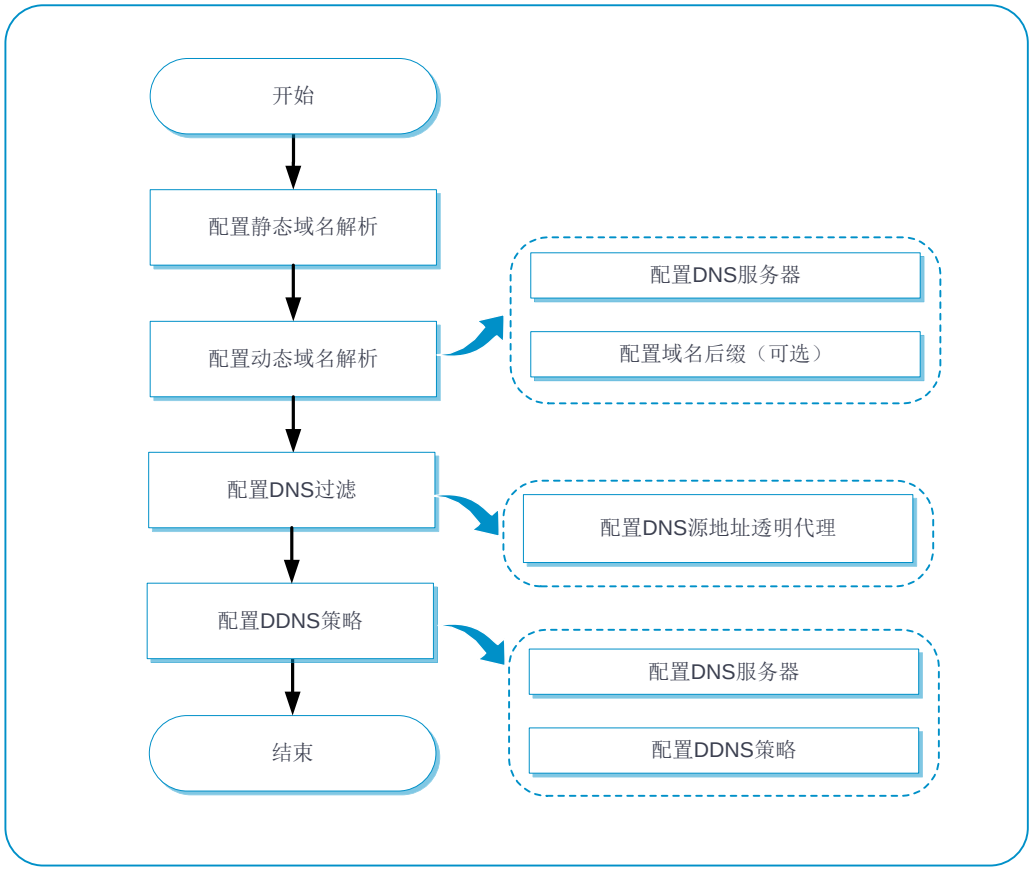
- 若配置 DNS 过滤的白名单时，界面提示“白名单和黑名单不能同时配置”，需要执行 **undo dns filter denylist** 命令来删除已有的主机名黑名单后才能配置主机名白名单。有关该命令的详细介绍，请参见“三层技术-IP 业务/域名解析”配置命令手册。
- 配置 DNS 过滤的主机白名单，意味着只有 DNS 代理收到的 DNS 请求报文中的域名命中白名单，DNS 代理才放行该 DNS 请求报文，否则将丢弃该 DNS 请求报文。在配置主机白名单时，需确保不会错误地阻断正常的业务流量。

配置指南

配置思路

DNS 的配置思路图如下图所示：

图-1 DNS 配置思路图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。

- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置静态域名解析

静态域名解析的具体配置步骤如下：

1. 选择“网络 > DNS > 已解析域名”，进入“已解析域名”页面。
2. 单击<新建>按钮，进入“新建静态域名”页面，具体配置内容如下表所示：

表-1 静态域名配置参数表

参数	说明
主机名	主机域名
主机地址	与主机名对应的IPv4/IPv6地址 主机地址配置为IPv4地址时，查询类型显示为A 主机地址配置为IPv6地址时，查询类型显示为AAAA
VRF	静态域名所属的VRF

3. 单击<确定>按钮，新建的静态域名会在“已解析域名”页面显示，类型显示为“静态”。

配置动态域名解析

动态域名解析的具体配置步骤如下：

1. 选择“网络 > DNS > DNS 客户端”，进入 DNS 客户端页面。

2. 在“DNS 客户端”页面配置 IPv4/IPv6 DNS 服务器地址，具体配置内容如下表所示。

表-2 DNS 服务器配置参数表

参数	说明
服务器类型	域名服务器的类型，包括： • IPv4 DNS 服务器 • IPv6 DNS 服务器
VRF	DNS服务器所属的VRF
域名服务器地址	域名服务器的IPv4地址。只有服务器类型选择“IPv4 DNS服务器”时，才会显示本参数 最多可以设置6个域名服务器的IPv4地址
域名服务器IPv6地址	域名服务器的IPv6地址。只有服务器类型选择“IPv6 DNS服务器”时，才会显示本参数 最多可以设置6个域名服务器的IPv6地址
报文出接口	报文的出接口。只有服务器类型选择“IPv6 DNS服务器”时，才会显示本参数

	如果未指定本参数，则根据路由表查找报文的出接口 域名服务器的IPv6地址为链路本地地址时，必须指定本参数 域名服务器的IPv6地址为全球单播地址时，无法指定本参数

3. 单击<添加>按钮，新建的 DNS 服务器地址在 DNS 客户端页面显示。

配置 DNS 过滤

DNS 过滤的具体配置步骤如下：

1. 选择“网络 > DNS > DNS 过滤”，进入“DNS 过滤”页面。

2. 在“DNS 过滤”页面配置 DNS 过滤参数，配置具体配置内容如下表所示：

表-3 DNS 过滤配置参数表

参数	说明
过滤方式	• DNS 源地址透明代理：单击<DNS 源地址透明代理>按钮即可启用该功能。有关 DNS 源地址透明代理的详细介绍请参见特性简介 • 不过滤：单击<不过滤>，可以关闭已启用的 DNS 源地址透明代理功能 注意：若开启DNS源地址透明代理但未配置主机名时，默认全放通
过滤类型	默认为白名单

主机名	主机域名，最多支持配置16个主机域名。支持使用“*”来定义模糊匹配主机名称，输入方式形如*abc*、*abc或者abc*，三种方式均表示主机名中包含指定的字符串。模糊匹配方式下，“*”只能位于字符串的首部或末尾，不能位于字符串中间。若输入的主机名中不存在“*”号，则表示精确匹配所配置的主机名

配置域名后缀

域名后缀的具体配置步骤如下：

1. 选择“网络 > DNS > 高级设置”。
2. 在“高级设置”页面配置域名后缀，具体配置内容如下表所示。

表-4 DNS 服务器配置参数表

参数	说明
VRF	域名后缀所属的VRF
域名后缀	域名解析的后缀名 最多可设置16个域名后缀

3. 在域名后缀列表中输入域名后缀名。
4. 单击<添加>按钮，新增的域名后缀在域名后缀列表中显示。

ALG

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 配置指南

特性简介

可通过开启指定应用协议类型的 ALG 功能，实现对应用层报文数据载荷字段的分析和具体业务处理。设备支持如下业务的 ALG 功能：

- NAT ALG
  - NAT44 转换支持如下协议的 ALG 功能：DNS、SIP、XDMCP、PPTP、SUN RPC、FTP、TFTP、ILS、RSH、ICMP 差错报文、RTSP、MGCP、SCCP、H323、SQLNET、NBT、SCTP
  - NAT64 转换支持如下协议的 ALG 功能：DNS、FTP、ICMP 差错报文、HTTP、SIP、RTSP、H323

- NAT66 转换支持如下协议的 ALG 功能：FTP、DNS、H323、HTTP、SIP、RTSP、SUN RPC、TFTP

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

指定协议类型的 ALG 功能支持情况与设备型号有关，请以页面的实际显示为准。

配置指南

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

具体配置步骤如下：

1. 单击“网络 > ALG”。

2. 在“ALG”页面开启指定协议的 ALG 功能，协议的支持情况与设备型号有关，请以页面的实际显示为准。

3. 单击<应用>按钮，完成配置。

VLAN

本帮助主要介绍以下内容：

- 特性简介
  - 基于端口划分 VLAN
  - VLAN 接口
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南

特性简介

VLAN (Virtual Local Area Network，虚拟局域网) 技术可以把一个物理 LAN 划分成多个逻辑的 LAN——VLAN，每个 VLAN 是一个广播域。处于同一 VLAN 的主机能够直接互通，而处于不同 VLAN 的主机不能够直接互通。

基于端口划分 VLAN

VLAN 可以基于端口进行划分。它按照设备端口来定义 VLAN 成员，将指定端口加入到指定 VLAN 中之后，端口就可以转发该 VLAN 的报文。

在某 VLAN 内，可根据需要配置端口加入 Untagged 端口列表或 Tagged 端口列表（即配置端口为 Untagged 端口或 Tagged 端口）。从 Untagged 端口发出的该 VLAN 报文不带 VLAN Tag，从 Tagged 端口发出的该 VLAN 报文带 VLAN Tag。

端口的链路类型分为三种。在端口加入某 VLAN 时，对不同链路类型的端口加入的端口列表要求不同：

- Access：端口只能发送一个 VLAN 的报文，发出去的报文不带 VLAN Tag。该端口只能加入一个 VLAN 的 Untagged 端口列表。
- Trunk：端口能发送多个 VLAN 的报文，发出去的端口缺省 VLAN 的报文不带 VLAN Tag，其他 VLAN 的报文都必须带 VLAN Tag。在端口缺省 VLAN 中，该端口只能加入 Untagged 端口列表；在其他 VLAN 中，该端口只能加入 Tagged 端口列表。
- Hybrid：端口能发送多个 VLAN 的报文，端口发出去的报文可根据需要配置某些 VLAN 的报文带 VLAN Tag，某些 VLAN 的报文不带 VLAN Tag。在不同 VLAN 中，该端口可以根据需要加入 Untagged 端口列表或 Tagged 端口列表。

VLAN 接口

不同VLAN间的主机不能直接通信，通过设备上的VLAN接口，可以实现VLAN间的三层互通。VLAN接口是一种三层的虚拟接口，它不作为物理实体存在于设备上。每个 VLAN 对应一个 VLAN 接口，VLAN 接口的 IP 地址可作为本 VLAN 内网络设备的网关地址，对需要跨网段的报文进行基于 IP 地址的三层转发。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

VLAN 1 为系统缺省 VLAN，用户不能手工创建和删除。

配置指南

新建并划分 VLAN

VLAN 是一种把物理 LAN 划分成多个逻辑 VLAN 的技术，每个 VLAN 是一个独立的广播域。处于同一 VLAN 的主机能够直接互通，而处于不同 VLAN 的主机不能够直接互通。

1. 选择“网络 > 链路 > VLAN”，进入“VLAN”页面。
2. 单击<新建>按钮，进入“新建 VLAN”页面。
3. 在“VLAN 列表”中输入 VLAN 编号，可以指定一个 VLAN 编号，也可以指定 VLAN 编号范围。
4. 单击<确定>按钮，新建 VLAN 成功，并会在“VLAN”页面中显示。
5. 在“VLAN”页面，单击<编辑>按钮，进入“编辑 VLAN”页面。

表-1 VLAN 配置参数表

参数	说明
VLAN ID	VLAN的编号
描述	VLAN的描述信息
链路类型：Access	添加到Access类型的端口只能发送一个VLAN报文，发出去的报文不带 1. 在 Access 下拉框中选择接口

	2. 单击<添加>按钮，添加的接口将显示在 Access 列表
链路类型：Trunk	添加到Trunk类型的端口能发送多个VLAN的报文，发出去的端口缺省V VLAN Tag，其他VLAN的报文都必须带VLAN Tag 3. 在 Trunk 下拉框中选择接口 4. 单击<添加>按钮，添加的接口将显示在 Trunk 列表
链路类型：Hybrid-Untagged	能发送多个VLAN的报文，端口发出去的报文可根据需要配置某些VL VLAN Tag 5. 在 Untagged 下拉框中选择接口 6. 单击<添加>按钮，添加的接口将显示在 Untagged 列表
链路类型：Hybrid-Tagged	能发送多个VLAN的报文，端口发出去的报文可根据需要配置某些VLAN Tag 7. 在 Tagged 下拉框中选择接口 8. 单击<添加>按钮，添加的接口将显示在 Tagged 列表

6. 单击<确定>按钮，编辑 VLAN 完成。

创建 VLAN 接口

VLAN 接口是一种三层的虚拟接口，每个 VLAN 对应一个 VLAN 接口。为了实现不同 VLAN 间的互通，需要为 VLAN 接口配置 IP 地址，该 IP 地址即可作为本 VLAN 内设备的网关地址，此时该 VLAN 接口能对报文进行三层转发。

1. 选择“网络 > 链路 > VLAN”，进入“VLAN”页面。

2. 勾选已创建 VLAN 前的复选框，单击<创建 VLAN 接口>按钮，进入“修改接口设置”页面。

3. 在“修改接口设置”页面，可修改 VLAN 接口的相关参数，详细配置可参考“接口联机帮助”。

4. 单击<确定>按钮，此处新建的 VLAN 接口，可在“接口”页面查看。

MAC

本帮助主要介绍以下内容：

- 特性简介
  - MAC 地址表分类
  - MAC 地址表项老化时间
  - 接口 MAC 地址学习
  - VLAN ID 检查功能
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南

特性简介

MAC（Media Access Control，媒体访问控制）地址表记录了 MAC 地址与接口的对应关系，以及接口所属的 VLAN 等信息。设备在转发报文时，根据报文的目的 MAC 地址查询 MAC 地址表，如果MAC地址表中包含与报文目的MAC地址对应的表项，则直接通过该表项中的出接口转发该报文；

如果 MAC 地址表中没有包含报文目的 MAC 地址对应的表项时，设备将采取广播的方式通过对应 VLAN 内除接收接口外的所有接口转发该报文。

MAC 地址表分类

MAC 地址表项分为以下几种：

- 动态 MAC 地址表项：可以由用户手工配置，也可以由设备通过源 MAC 地址学习自动生成，用于将目的是某个 MAC 地址的报文从对应接口转发出去，表项有老化时间。手工配置的动态 MAC 地址表项优先级等于自动生成的 MAC 地址表项。
- 静态 MAC 地址表项：由用户手工配置，用于将目的是某个 MAC 地址的报文从对应接口转发出去，表项不老化。静态 MAC 地址表项优先级高于自动生成的 MAC 地址表项。
- 黑洞 MAC 地址表项：由用户手工配置，用于丢弃源 MAC 地址或目的 MAC 地址为指定 MAC 地址的报文（例如，出于安全考虑，可以禁止某个用户发送和接收报文），表项不老化。

MAC 地址表项老化时间

MAC 地址表中自动生成的表项并非永远有效，每一条表项都有一个生存周期，这个生存周期被称作老化时间。配置动态 MAC 地址表项的老化时间后，超过老化时间的动态 MAC 地址表项会被自动删除，设备将重新进行 MAC 地址学习，构建新的动态 MAC 地址表项。如果在到达生存周期前某表项被刷新，则重新计算该表项的老化时间。

用户配置的老化时间过长或者过短，都可能影响设备的运行性能：

- 如果用户配置的老化时间过长，设备可能会保存许多过时的 MAC 地址表项，从而耗尽 MAC 地址表资源，导致设备无法根据网络的变化更新 MAC 地址表。
- 如果用户配置的老化时间太短，设备可能会删除有效的 MAC 地址表项，导致设备广播大量的数据报文，增加网络的负担。

用户需要根据实际情况，配置合适的老化时间。如果网络比较稳定，可以将老化时间配置得长一些或者配置为不老化；否则，可以将老化时间配置得短一些。比如在一个比较稳定的网络，如果长时间没有流量，动态 MAC 地址表项会被全部删除，可能导致设备突然广播大量的数据报文，造成安全隐患，此时可将动态 MAC 地址表项的老化时间设得长一些或不老化，以减少广播，增加网络稳定性和安全性。动态 MAC 地址表项的老化时间作用于全部接口上。

接口 MAC 地址学习

缺省情况下，MAC 地址学习功能处于开启状态。有时为了保证设备的安全，需要关闭 MAC 地址学习功能。常见的危及设备安全的情况是：非法用户使用大量源 MAC 地址不同的报文攻击设备，导致设备 MAC 地址表资源耗尽，造成设备无法根据网络的变化更新 MAC 地址表。关闭 MAC 地址学习功能可以有效防止这种攻击。在开启全局的 MAC 地址学习功能的前提下，用户可以关闭单个接口的 MAC 地址的学习功能。

如果MAC地址表过于庞大，可能导致设备的转发性能下降。通过配置接口的MAC地址数学习上限，用户可以控制设备维护的 MAC 地址表的表项数量。当接口学习到的 MAC 地址数达到上限时，该接

口将不再对 MAC 地址进行学习，同时，用户还可以根据需要选择是否允许系统转发源 MAC 不在 MAC 地址表里的报文。

VLAN ID 检查功能

在 MAC 转发时，开启此功能后，仅当报文的 VLAN ID 与会话表项中的 VLAN ID 匹配成功才放行此报文，否则丢弃。关闭此功能后，无需匹配 VLAN ID，仅需报文与会话表项中的其他信息匹配成功就可以放行此报文。

在双机热备组网环境下，当主设备与备设备上报文入接口属于不同 VLAN 时，必须关闭 VLAN ID 检查功能，才能使从主设备上切换过来的流量或非对称的反向流量匹配备设备上的备份会话，实现安全业务功能的正常运行。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

配置 MAC 地址表项时，如果不保存配置，设备重启后所有手工配置的 MAC 地址表项都会丢失；如果保存配置，设备重启后手工配置的静态 MAC 地址表项、黑洞 MAC 地址表项不会丢失，手工配置的动态 MAC 地址表项会丢失。

配置指南

MAC 地址表项类型包括动态、静态和黑洞。用于记录 MAC 地址与设备接口及 VLAN 的关联。在转发报文时，设备查询 MAC 地址表，以确定转发路径，若无匹配则广播。此外，可在高级设置配置 VLAN ID 检查功能，通过匹配报文与会话表项中的 VLAN ID 来增强安全性。

1. 选择“网络 > 链路 > MAC”，进入“MAC”页面。
2. 在“MAC”页面，单击<新建>按钮，进入“新建 MAC 地址”页面。

表-1 MAC 地址配置参数表

参数	说明
类型	MAC地址表项类型，包括： • 动态 • 静态

	• 黑洞
MAC地址	MAC地址，格式为H-H-H，不支持组播MAC地址、全0的MAC地址和全F的
VLAN	VLAN的编号
接口	指定VLAN下的出接口

3. 单击<确定>按钮，新建 MAC 地址成功，并会在“MAC”页面中显示。

4. （可选）选择“高级设置”，进入“高级设置”页面。

   选择开启/关闭“VLAN ID 检查功能”。

HTTP/HTTPS

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南

特性简介

设备支持的 Web 登录方式有以下两种：

- HTTP 登录方式：HTTP（Hypertext Transfer Protocol，超文本传输协议）用来在 Internet 上传递 Web 页面信息。目前，设备支持的 HTTP 协议版本为 HTTP1.0 和 HTTP1.1。
- HTTPS 登录方式：HTTPS（Hypertext Transfer Protocol Secure，超文本传输协议的安全版本）是支持 SSL（Secure Sockets Layer，安全套接字层）协议的 HTTP 协议。HTTPS 通过 SSL 协议，能对客户端与设备之间交互的数据进行加密。

用户采用 HTTPS 协议登录设备时，设备上需使能 HTTPS 服务。此时，设备使用的证书为自签名证书，使用的 SSL 参数为各个参数的缺省值。（自签名证书指的是服务器自己生成的证书，无需从 CA 获取）

为 HTTPS 服务指定 SSL 服务器端策略后，HTTPS 通过 SSL 协议，能对客户端与设备之间交互的数据进行加密，提高了数据传输的安全性和完整性，保证合法客户端可以安全地访问设备，禁止非法的客户端访问设备，从而实现了对设备的安全管理。

用户可通过以下 HTTPS 登录方式登录设备：

- 用户名密码方式：只能使用用户名和密码进行登录。
- 证书方式：只能使用数字证书进行登录。
- 用户名密码和证书方式：必须同时提供用户名、密码以及数字证书进行登录。

USB-Key 登录是一种数字证书登录方式。点击“USB-Key 登录”按钮后，请按照提示信息选择 USB-Key 中的数字证书来登录。

通过引用 ACL（Access Control List，访问控制列表），可以对访问设备的登录用户进行控制：

- 当未引用 ACL、引用的 ACL 不存在或者引用的 ACL 为空时，允许所有登录用户访问设备；
- 当引用的 ACL 非空时，则只有 ACL 中 permit 的用户才能访问设备，其它用户不允许访问设备，可以避免非法用户使用 Web 页面登录设备。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 使用用户名密码登录方式时，请不要开启 SSL 服务器端策略的验证客户端功能。使用其他登录方式时，必须配置 SSL 服务器端策略并开启验证客户端功能。
- 若通过命令行同时指定了一个 ACL 的编号和名称，则在引用 ACL 时只显示该 ACL 的编号。

配置指南

HTTP 登录

HTTP 登录是设备通过 Web 登录的基本功能。通过配置 ACL，仅允许特定用户访问设备，增强对访问设备的用户的控制，防止未经授权的访问。

1. 单击“网络 > 服务 > HTTP/HTTPS”。
2. 在“HTTP/HTTPS”页面进行 HTTP 服务配置。

表-1 HTTP 登录配置

参数	说明
HTTP登录	开启HTTP登录方式。禁止在页面上关闭HTTP登录方式
HTTP服务端口	HTTP服务的端口号
指定过滤ACL类型	指定过滤ACL类型包括： • IPv4/IPv6 • 二层 ACL
IPv4 ACL	指定IPv4 ACL。可选择已创建的IPv4 ACL，也可以新创建IPv4 ACL 只有指定过滤ACL类型选择“IPv4/IPv6”时，才会显示本参数
IPv6 ACL	指定IPv6 ACL。可选择已创建的IPv6 ACL，也可以新创建IPv6 ACL 只有指定过滤ACL类型选择“IPv4/IPv6”时，才会显示本参数
二层ACL	指定二层ACL。可选择已创建的二层ACL，也可以新创建二层ACL 只有指定过滤ACL类型选择“二层ACL”时，才会显示本参数

3. 单击<应用>按钮，保存当前配置。

HTTPS 登录

HTTPS 登录是 HTTP 登录的安全版本，用于在网络上进行安全的通信。通过配置 HTTPS 登录，用户可启用 SSL 服务器端策略，对客户端与设备之间交互的数据进行加密，提高设备的安全性。

1. 在“HTTP/HTTPS”页面进行 HTTPS 登录配置。

表-2 HTTPS 登录配置

参数	说明
HTTPS登录	开启HTTPS登录方式。禁止在页面上关闭HTTPS登录方式
HTTPS服务端口	HTTPS服务的端口号
指定过滤ACL类型	指定过滤ACL类型包括： • IPv4/IPv6 • 二层 ACL
IPv4 ACL	指定IPv4 ACL。可选择已创建的IPv4 ACL，也可以新创建IPv4 ACL 只有指定过滤ACL类型选择“IPv4/IPv6”时，才会显示本参数
IPv6 ACL	指定IPv6 ACL。可选择已创建的IPv6 ACL，也可以新创建IPv6 ACL 只有指定过滤ACL类型选择“IPv4/IPv6”时，才会显示本参数
二层ACL	指定二层ACL。可选择已创建的二层ACL，也可以新创建二层ACL 只有指定过滤ACL类型选择“二层ACL”时，才会显示本参数
SSL服务器端策略	选择已创建的SSL服务器端策略与之关联 SSL服务器端策略在“对象模板 > SSL策略 > 服务器端策略”页面配置
登录方式	登录设备方式，包括： • 用户名密码 • 证书

	• 用户名密码和证书
证书字段	作为通过数字证书登录设备时使用的用户名，包括： • cn：数字证书中的 CN 字段 • email-prefix：数字证书中 emailAddress 字段“@”字符前的字符串 • oid：数字证书中 oid 值对应的字段
oid值	指定oid值。只有指定证书字段选择“oid”时，才会显示本参数

2. 单击<应用>按钮，保存当前配置。

HTTP/HTTPS 登录空闲超时时间

HTTP/HTTPS 登录空闲超时时间指的是用户在登录状态下，如果在一段时间内没有进行任何操作，系统会自动将用户登出以保护账户安全。

1. 在“HTTP/HTTPS”页面，设置 HTTP/HTTPS 登录用户连接的超时时间。

2. 单击<应用>按钮，保存当前配置。

SSH

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南

特性简介

SSH 是 Secure Shell（安全外壳）的简称，是一种在不安全的网络环境中，通过加密机制和认证机制，实现安全的远程访问以及文件传输等业务的网络安全协议。

SSH 协议采用了典型的客户端/服务器模式，并基于 TCP 协议协商建立用于保护数据传输的会话通道。

本设备可作为 SSH 服务器，为 SSH 客户端提供以下几种应用：

- Stelnet：全称为 Secure Telnet ，可提供安全可靠的网络终端访问服务。
- SFTP：全称为 Secure FTP，基于 SSH2，可提供安全可靠的网络文件传输服务。
- SCP：全称为 Secure Copy，基于 SSH2，可提供安全的文件复制功能。

SSH 协议有两个版本，SSH1.x 和 SSH2.0（本文简称 SSH1 和 SSH2），两者互不兼容。SSH2 在性能和安全性方面比 SSH1 有所提高。

设备作为 SSH 服务器时，利用本地密码认证机制验证 SSH 客户端的用户名和密码的合法性。身份认证通过后，SSH 客户端将与 SSH 服务器建立相应的会话，并在该会话上进行数据信息的交互。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 虽然一个 SSH 客户端只会采用 DSA、ECDSA 或 RSA 公钥算法中的一种来认证 SSH 服务器，但是由于不同 SSH 客户端支持的公钥算法不同，为了确保 SSH 客户端能够成功登录 SSH 服务器，建议在 SSH 服务器上同时生成 DSA、ECDSA 和 RSA 三种密钥对。
- SSH 服务器仅支持默认名称的本地 DSA、ECDSA 或 RSA 密钥对，因此生成本地非对称密钥对时，不要指定密钥对的名称。
- 生成 DSA 密钥对时，输入的密钥模数的长度必须小于 2048 比特。
- SSH 客户端认证成功后，所具有的属性（例如角色、FTP 目录）均由设备上对应的管理员用户配置决定。

- 若指定的过滤 SSH 客户端的 ACL 不存在，或者 ACL 中无任何规则，则表示允许任意 SSH 客户端发起 SSH 访问。

设备作为 SFTP 服务器时，不支持 SSH1 版本的客户端发起的 SFTP 连接。

配置指南

设备作为 SSH 服务器时，为保证 SSH 客户端可以正常使用 Stelnet/SFTP/SCP 服务，需要完成以下配置任务：

- 生成 RSA、DSA 或 ECDSA 本地非对称密钥对。
- 开启 Stelnet/SFTP/SCP 服务。
- 配置 SSH 服务类型的管理员用户。

配置步骤

1. 单击“网络 > 服务 > SSH”。
2. 在“SSH”页面开启 Stelnet/SFTP/SCP 服务，具体配置内容如下：

表-1 SSH 配置

参数	说明
服务器发送的IPv4报文	DSCP携带在IP报文中的ToS字段，用来体现报文自身的优先等级，决定报文传

的DSCP优先级	
服务器发送的IPv6报文的DSCP优先级	DSCP携带在IPv6报文中的Traffic class字段，用来体现报文自身的优先等级，决定先程度
指定过滤IPv4客户端的ACL	当未指定ACL、指定的ACL不存在或ACL没有规则时，允许所有IPv4客户端向设备否则只允许匹配ACL permit规则的IPv4客户端访问设备
指定过滤IPv6客户端的ACL	当未指定ACL、指定的ACL不存在或ACL没有规则时，允许所有IPv6客户端向设备否则只允许匹配ACL permit规则的IPv6客户端访问设备
服务器RSA密钥对的最小更新时间间隔	该时间间隔仅对SSH1版本的SSH客户端有效，缺省情况下，不更新RSA密钥对。SSH服务器需要等待后续有新的SSH1用户登录，才会更新当前的RSA服务器密钥新的RSA服务器密钥对与新登录的这个SSH1用户进行密钥对的协商，其中等待的此处配置的最小更新间隔时间。之后，重复此过程，直到下一个新的SSH1用户登发RSA服务器密钥的更新
客户端认证尝试的最大次数	通过本功能可以限制用户尝试登录的次数，防止非法用户对用户名和密码进行恶意
客户端认证超时时间	如果SSH用户在设置的认证超时时间内没有完成认证，SSH服务器就拒绝该用户 为了防止不法用户建立起TCP连接后，不进行接下来的认证，而占用系统资源，妨户的正常登录，可以适当调小SSH用户认证超时时间。
SFTP用户连接的空闲超时时间	当SFTP用户连接的空闲时间超过设定的阈值后，系统会自动断开此用户的连接，用户长期占用连接而不进行任何操作。若同一时间内并发的SFTP连接数较多，可及时释放系统资源给新用户接入
兼容SSH1版本的客户端	该功能不会影响已经登录的SSH用户，仅对新登录的SSH用户生效

3. 单击“应用”按钮，完成配置。

NTP

特性简介

在大型的网络中，如果依靠管理员手工配置来修改网络中各台设备的系统时间，不但工作量巨大，而且也不能保证时间的精确性。NTP（Network Time Protocol，网络时间协议）可以用来在分布式时间服务器和客户端之间进行时间同步，使网络内所有设备的时间保持一致，并提供较高的时间同步精度。这里的“分布式”指的是运行 NTP 的设备既可以与其他设备的时间同步，又可以作为时间服务器为其他设备提供时间同步。

NTP 采用的传输层协议为 UDP，使用的 UDP 端口号为 123。

在某些网络中，例如无法与外界通信的孤立网络，网络中的设备无法与权威时钟进行时间同步。此时，可以从该网络中选择一台时钟较为准确的设备，指定该设备与本地时钟进行时间同步，即采用本地时钟作为参考时钟，使得该设备的时钟处于同步状态。该设备作为时间服务器为网络中的其他设备提供时间同步，从而实现整个网络的时间同步。

通过 Web 页面可以配置本地时钟作为参考时钟。

使用限制和注意事项

配置本地时钟作为参考时钟时，如果本地设备的时钟不正确，则会导致网络中设备的时间错误。在执行本配置时，建议先调整本地系统时间。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。

- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置 NTP 服务

NTP 服务的具体配置步骤：

1. 单击“网络 > 服务 > NTP”，进入“NTP”页面。
2. 单击<开启>，开启 NTP 服务。
3. 配置本地时钟的 IP 地址，本地时钟的 IP 地址为 127.127.1.u。u 的取值范围为 0～3，表示 NTP 的进程号。
4. 配置本地时钟所处的层级，NTP 通过时钟层数来定义时钟的准确度。取值越小，时钟准确度越高。
5. 单击<应用>按钮，本地时钟配置成功。
6. （可选）开启<身份验证>功能。在一些对安全性要求较高的网络中，运行 NTP 协议时需要启用 NTP 身份验证功能。通过客户端和服务器端的身份验证，保证客户端只与通过验证的设备进行时间同步，避免客户端从非法的服务器获得错误的时间同步信息。开启 NTP 身份验证功能后，设备采用 MD5 算法进行身份验证，但还需要设置身份验证密钥，并将其设置为可信密钥，才能正确地进行身份验证。
7. 单击<新建>按钮，配置身份验证密钥如下：

表-1 身份验证密钥配置

参数	说明
身份验证密钥ID	密钥编号，用来标识身份验证密钥
密钥	密钥字符串，区分大小写 NTP客户端和服务器上需要配置相同的密钥ID和密钥值，并且保证对端有权在本端使用该密钥ID进行身份验证，否则无法实现时间同步

8. 单击<确定>按钮，完成身份验证密钥的配置。

FTP

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南

特性简介

FTP 用于在 FTP 服务器和 FTP 客户端之间传输文件，是 IP 网络上传输文件的通用协议。本设备可作为 FTP 服务器，使用 20 端口传输数据，使用 21 端口传输控制消息。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

如果在用户切换时，输入的用户名/密码错误，则会断开当前连接，用户必须重新登录才能继续访问FTP 服务器。

配置指南

FTP 是一种常用的网络协议，基于客户端-服务器模型进行文件传输。开启本功能后，设备可作为FTP 服务器运行，实现和 FTP 客户端之间文件的传输。

1. 选择“网络>服务>FTP”
2. 单击<开启>按钮启用 FTP 服务。
3. 开启后，进入高级设置的配置页面。

表-1 高级设置

参数	说明
设备发送的FTP报文的DSCP优先级	DSCP携带在IP报文中的ToS字段中，用来体现报文自身的优先等级，决定报文传输的优先程度。缺省情况下，FTP服务器发送的FTP报文的DSCP优先级为0
设备发送的IPv6 FTP报文的DSCP优先级	DSCP携带在IP报文中的Traffic class字段中，用来体现报文自身的优先等级，决定报文传输的优先程度。缺省情况下，FTP

	服务器发送的FTP报文的DSCP优先级为0
使用ACL过滤IPv4 FTP用户	下拉选择ACL规则。可选中已有的ACL，如需新建ACL，具体的配置步骤请参见”对象 > ACL > IPv4/二层 “
使用ACL过滤IPv6 FTP用户	下拉选择ACL规则。可选中已有的ACL，如需新建ACL，具体的配置步骤请参见“对象 > ACL > IPv6/二层”
FTP用户连接的空闲超时时间	如果在指定时间内，设备和FTP客户端一直没有信息交互，设备将断开与该FTP客户端的连接。缺省情况下，连接空闲时间为30分钟
SSL服务策略	当支持FTP安全扩展协议的两台设备建立FTP连接时，通过将FTP服务与SSL服务器端策略关联，可以建立一条安全的SSL连接来传输数据，保证FTP传输的安全性。缺省情况下，FTP服务器未引用SSL服务器端策略。可选中已有的SSL服务策略，如需新建SSL服务策略，具体的配置步骤请参见“对象 > SSL > 服务器端策略”

4. 点击<应用>按钮，完成 FTP 服务与高级设置的配置。

Telnet

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南

特性简介

设备可以开启 Telnet 服务器功能，以便用户能够通过 Telnet 登录到设备进行远程管理和监控。

通过引用 ACL（Access Control List，访问控制列表），可以对访问设备的登录用户进行控制：

- 当未引用 ACL、引用的 ACL 不存在或者引用的 ACL 为空时，允许所有登录用户访问设备；
- 当引用的 ACL 非空时，则只有 ACL 中 permit 的用户才能访问设备，其他用户不允许访问设备，可以避免非法用户通过 Telnet 访问设备。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

开启 Telnet 服务器功能后，还需要对认证方式、用户角色及公共属性进行相应的配置，才能保证通过 Telnet 方式正常登录到设备。

配置指南

Telnet 是一种网络协议，允许用户通过命令行界面对远程设备进行交互和管理。设备开启 Telnet 服务器功能后，用户便能够通过 Telnet 登录到设备进行远程管理和监控。

1. 选择“网络 > 服务 > Telnet”
2. 单击<开启>按钮启用 Telnet 服务。
3. 配置高级设置参数。具体内容如下表所示：

表-1 高级设置

参数	说明
IPv4 DSCP优先级	DSCP携带在IP报文中的ToS字段中，用来体现报文自身的优先等级，决定报文传输的优先程度
IPv6 DSCP优先级	DSCP携带在IP报文中的Traffic class字段中，用来体现报文自身的优先等级，决定报文传输的优先程度
使用ACL过滤IPv4登录用户	下拉选择ACL规则。可选中已有的ACL，如需新建ACL，具体的配置步骤请参见“对象 > ACL > IPv4/二层”
使用ACL过滤IPv6登录用户	下拉选择ACL规则。可选中已有的ACL，如需新建ACL，具体的配置步骤请参见“对象 > ACL > IPv6/二层”

4. 单击<应用>按钮，完成 Telnet 服务高级设置的配置。

MAC 地址认证

本帮助主要介绍以下内容：

- 特性简介
  - 授权 VLAN
  - 端口工作模式
  - Guest VLAN
  - Critical VLAN
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置准备
  - 配置 MAC 地址认证

特性简介

MAC 地址认证是一种基于端口和 MAC 地址对用户的网络访问权限进行控制的认证方法，它不需要用户安装任何客户端软件。设备在启动了MAC地址认证的端口上首次检测到用户的MAC地址以后，即启动对该用户的认证操作。认证过程中，不需要用户手动输入用户名或密码。若该用户认证成功，则允许其通过端口访问网络资源，否则该用户的 MAC 地址就被设置为静默 MAC。在静默时间内，来自此MAC地址的用户报文到达时，设备直接做丢弃处理，以防止非法MAC短时间内的重复认证。

授权 VLAN

为了将受限的网络资源与未认证用户隔离，通常将受限的网络资源和未认证的用户划分到不同的 VLAN，当用户通过 MAC 地址认证后，设备将指定的受限网络资源所在的 VLAN 作为授权 VLAN 下发到用户进行认证的端口。该端口被加入到授权 VLAN 中后，用户便可以访问这些受限的网络资源。

端口工作模式

MAC 地址认证的端口可以工作在单 VLAN 模式或多 VLAN 模式：

- 单 VLAN 模式：
  - 在账号已通过 MAC 地址认证，且没有被下发授权 VLAN 情况下，如果此账号在相同端口上的不同VLAN再次接入，则设备将让原账号下线，使得该账号能够在新的VLAN内重新开始认证。

- 如果已通过 MAC 地址认证的账号被下发了授权 VLAN，则此账号在属于不同 VLAN 的相同端口再次接入时不会被强制下线。

- 多 VLAN 模式，如果相同 MAC 地址的账号在相同端口上的不同 VLAN 再次接入，设备将能够允许账号的流量在新的 VLAN 内通过，且允许该用户的报文无需重新认证而在多个 VLAN 中转发。

Guest VLAN

MAC 地址认证的 Guest VLAN 功能允许用户在认证失败的情况下访问某一特定 VLAN 中的资源，比如获取客户端软件，升级客户端或执行其他一些用户升级程序。这个 VLAN 称之为 Guest VLAN。

这里的认证失败是认证服务器因某种原因明确拒绝用户认证通过，比如用户密码错误，而不是认证超时或网络连接等原因造成的认证失败。如果接入用户的端口上配置了 Guest VLAN，则该端口上认证失败的用户会被加入 Guest VLAN，且设备允许 Guest VLAN 以不携带 Tag 的方式通过该端口，即该用户被授权访问 Guest VLAN 里的资源。

用户被加入 Guest VLAN 之后，设备将以指定的时间间隔对该用户发起重新认证：

- 认证成功，根据设备是否下发授权 VLAN 决定是否将用户加入到下发的授权 VLAN 中，如果处于未下发授权 VLAN 的情况下，则用户回到缺省 VLAN 中。

- 认证失败，该用户将仍然处于 Guest VLAN 中。

Critical VLAN

MAC 地址认证 Critical VLAN 功能允许用户在所有认证服务器都不可达的情况下访问某一特定 VLAN 中的资源，这个 VLAN 称之为 Critical VLAN。

如果该端口上有用户认证时，所有认证服务器都不可达，则端口允许 Critical VLAN 通过，用户将被授权访问 Critical VLAN 里的资源。

已经加入 Critical VLAN 的端口上有用户发起认证时：

- 如果所有认证服务器不可达，则端口仍然在 Critical VLAN 内。
- 如果服务器可达且认证失败，且端口配置了 Guest VLAN，则该端口将会加入 Guest VLAN，否则回到缺省 VLAN 中。
- 如果服务器可达且认证成功，则会根据设备是否下发授权 VLAN 决定是否将用户加入到下发的授权 VLAN 中，如果处于未下发授权 VLAN 的情况下，则用户回到缺省 VLAN 中。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

仅二层工作模式下的接口支持配置 MAC 地址认证。

只有全局和端口的 MAC 地址认证均开启后，MAC 地址认证配置才能在端口上生效。

关于 Guest VLAN 的注意事项

- 配置 Guest VLAN 之前需要保证端口类型为 Hybrid，端口上的 MAC VLAN 功能处于使能状态，且不建议将指定的 Guest VLAN 修改为携带 Tag 的方式。
- 配置 Guest VLAN 之前需要创建配置为 Guest VLAN 的 VLAN。
- 认证失败的用户可访问指定的 Guest VLAN 中的资源，且该用户的 MAC 地址不会被加入静默 MAC。
- 端口上生成的 MAC 地址认证 Guest VLAN 表项会覆盖已生成的阻塞 MAC 表项。开启了端口安全入侵检测的端口关闭功能时，若端口因检测到非法报文被关闭，则 MAC 地址认证的 Guest VLAN 功能不生效。
- 如果某个 VLAN 被指定为 Super VLAN，则该 VLAN 不能被指定为某个端口的 MAC 地址认证的 Critical VLAN；同样，如果某个 VLAN 被指定为某个端口的 MAC 地址认证的 Critical VLAN，则该 VLAN 不能被指定为 Super VLAN。

关于 Critical VLAN 的注意事项

- 配置 Critical VLAN 之前需要保证端口类型为 Hybrid，端口上的 MAC VLAN 功能处于使能状态，且不建议将指定的 Critical VLAN 修改为携带 Tag 的方式。
- 配置 Critical VLAN 之前需要创建配置为 Critical VLAN 的 VLAN。
- 当端口上的用户加入指定的 Critical VLAN 后，该用户的 MAC 地址不会被加入静默 MAC。

- 端口上生成的 MAC 地址认证 Critical VLAN 表项会覆盖已生成的阻塞 MAC 表项。开启了端口安全入侵检测的端口关闭功能时，MAC 地址认证的 Critical VLAN 功能不生效。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置 MAC 地址认证

全局 MAC 地址认证功能和单个接口的 MAC 地址认证功能必须同时开启，才会对接入用户进行 MAC 地址认证。

MAC 地址认证的具体配置步骤如下：

1. 选择“网络 > 安全接入 > MAC 接入 > MAC 地址认证”。

2. 在“MAC 地址认证”页面勾选“开启”，开启全局 MAC 地址认证功能。

3. 勾选接口对应的“开启接口 MAC 地址认证”，开启单个接口的 MAC 地址认证功能。

4. 单击接口对应的“编辑”按钮，进入“编辑 MAC 地址认证”页面。

5. 配置该接口的 MAC 地址认证参数，具体配置内容如下表所示：

表-1 MAC 地址认证配置参数表

参数	说明
延迟认证	配置延迟认证的等待时间，缺省为不开启延迟认证
VLAN模式	选择端口工作在单VLAN模式或多VLAN模式
Guest VLAN	配置用户认证失败的情况下加入的VLAN
Critical VLAN	配置所有认证服务器都不可达的情况下用户加入的VLAN
用户认证ISP域	配置该端口接入的用户使用的认证域
最大用户数	配置端口上最多允许同时接入的MAC地址认证用户数
重认证不可达动作	选择在重认证服务器不可达的情况下，在线用户的处理动作

6. 单击<确定>按钮，配置接口 MAC 地址认证完成。

MAC 地址白名单

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 配置指南
  - 配置准备
  - 手动新建 MAC 地址白名单

特性简介

MAC 地址白名单，是指在本地设备上一组用户的集合。该集合的用户成员可由鹰视平台进行下发，也可由管理员手动增加。

鹰视平台通过终端扫描功能将可信任终端的信息下发至设备 MAC 地址白名单，并统一配置密码等属性，从而确保可信任终端能够顺利接入网络。

在 MAC 地址白名单中新建的用户会同时被加入设备本地用户列表，可在“本地用户”页面查看。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

手动新建 MAC 地址白名单

通过指定用户的 MAC 地址和用户的接入接口，可将用户添加至 MAC 地址白名单，加入 MAC 地址白名单的用户将无需进行 MAC 地址认证。

手动新建 MAC 地址白名单的具体配置步骤如下：

1. 选择“网络 > 安全接入 > MAC 接入 > MAC 地址白名单”。
2. 在“MAC 地址白名单”页面单击<新建>按钮，进入“新建 MAC 地址白名单”页面。
3. 在“新建 MAC 地址白名单”页面的具体配置内容如下表所示：

表-1 配置用户参数表

参数	说明
MAC地址	接入设备的MAC地址
可用服务	可用服务是用户可使用的网络服务类型，默认勾选“LAN接入”，且不支
用户接入的接口	如果用户接入的接口与此处绑定的接口不一致，则认证失败

4. 单击<确定>按钮，新建 MAC 地址白名单成功，且会在“MAC 地址白名单”页面中显示。

静默 MAC 信息

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 配置指南
  - 配置准备
  - 查看静默 MAC 信息

特性简介

静默 MAC 信息列表显示了 MAC 地址被设置为静默 MAC 的用户信息。

当用户认证失败时，该用户的 MAC 地址就会被设置为静默 MAC。在静默时间内（可通过静默时间间隔设置），来自该列表中的静默 MAC 地址的用户报文到达时，设备直接做丢弃处理，以防止非法 MAC 短时间内的重复认证。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。
- 开启全局 MAC 地址认证。

查看静默 MAC 信息

若 MAC 地址认证失败，则会加入静默 MAC 列表中，最多可添加 1024 条静默 MAC 地址。

查看静默 MAC 信息的具体步骤如下：

1. 选择“网络 > 安全接入 > MAC 接入 > 静默 MAC 信息”。

2. 进入“静默 MAC 信息”页面，具体显示内容如下表所示：

表-1 静默信息参数表

参数	说明
MAC地址	静默用户的MAC地址
VLAN	静默用户所在的VLAN
接口	静默用户接入的端口名称

高级设置

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 配置指南
  - 配置准备
  - 配置高级设置

特性简介

用户名格式

MAC 地址认证支持通过两种用户名格式进行认证，包括：

- 固定用户名：所有 MAC 地址认证用户均使用设备上指定的一个固定用户名和密码替代用户的 MAC 地址作为身份信息进行认证。
- MAC 地址用户名：设备使用源 MAC 地址作为用户认证时的用户名和密码。

用户认证 ISP 域

为了便于接入设备的管理员更为灵活地部署用户的接入策略，设备支持指定 MAC 地址认证用户认证使用的 ISP 域。

用户下线检测时间间隔

用来设置用户空闲超时的时间间隔。若设备在一个下线检测时间间隔之内，没有收到某在线用户的报文，将切断该用户的连接，同时通知 RADIUS 服务器停止对其计费。

静默时间间隔

用来设置用户认证失败以后，设备停止对其提供认证服务的时间间隔。在静默期间，设备不对来自认证失败用户的报文进行认证处理，直接丢弃。静默期后，如果设备再次收到该用户的报文，则依然可以对其进行认证处理。

服务器超时时间间隔

用来设置设备同 RADIUS 服务器的连接超时时间。在用户的认证过程中，如果在服务器超时时间间隔内设备一直没有收到 RADIUS 服务器的应答，则设备将在相应的端口上禁止此用户访问网络。

vSystem相关说明

非缺省 VSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。
- 开启全局 MAC 地址认证。

配置高级设置

通过高级设置，可配置用户 MAC 地址认证的高级功能。

MAC 地址认证的高级功能的具体配置步骤如下：

1. 单击“网络 > 安全接入 > MAC 接入 > 高级设置”。
2. 在开启全局 MAC 地址认证功能后。
3. 在“高级设置”页面的具体配置内容如下表所示：

表-1 MAC 接入高级设置参数配置

参数	说明
用户名格式	• 固定用户名 所有MAC地址认证用户均使用设备上指定的一个固定用户名和密码替代用户的MA信息进行认证 • MAC 地址用户名 设备使用源MAC地址作为用户认证时的用户名和密码
用户认证ISP域	MAC地址认证用户认证使用的ISP域 可选择已创建的ISP域，也可以新创建ISP域。此处新建的ISP域，可在“对象 > 用户 > 域”页面查看
用户下线检测时间间隔	如果在设置的时间内，没有收到在线用户的报文，则切断该用户连接
静默时间间隔	用户认证失败，需要等待的时间，在此期间内，设备收到该用户的报文，直接丢弃
服务器超时时间间隔	如果在设置的时间内，没有收到RADIUS服务器的应答，则设备将禁止此用户访问网
开启用户下线日志	MAC地址认证用户下线的日志信息
开启登录成功日志	MAC地址认证用户上线成功的日志信息
开启登录失败日志	MAC地址认证用户上线失败的日志信息

4. 单击<应用>按钮，MAC 接入高级设置配置完成。

IP 地址认证

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 配置指南
  - 配置准备
  - 配置 IP 地址认证
  - 编辑 IP 接入日志参数

特性简介

IP 地址认证是设备根据用户接入的位置信息自动生成用户名和密码进行身份认证的一种认证方式，无需用户输入用户名和密码。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置 IP 地址认证

IP 地址认证的具体配置如下：

1. 选择“网络 > 安全接入 > IP 接入 > IP 地址认证”。

2. 单击接口对应的“编辑”按钮，进入“编辑 IP 认证设置”页面，配置该接口的 IP 地址认证参数，具体的配置参数如下表所示。

表-1 IP 地址认证配置参数表

参数	说明
IP类型	选择IP协议类型
IPoE功能	选择IPoE接入模式： • 开启二层接入：用户直接连接接入设备，或通过二层网络设备接入设备需要识别用户的 MAC 地址 • 开启三层接入：用户流量通过三层网络路由到接入设备，用户设备或通过三层转发设备连接接入设备 • 关闭：不开启 IPoE 认证
未知源IP接入	配置是否允许未知源IP接入
IP认证白名单	配置是否启用IP地址认证白名单，若选择启用则IP地址白名单生效

3. 单击<确定>按钮，配置接口 IP 地址认证完成。

编辑 IP 接入日志参数

编辑 IP 接入日志参数的具体配置如下：

1. 选择“网络 > 安全接入 > IP 接入 > IP 地址认证”。
2. 单击“编辑 IP 接入日志参数”按钮，进入“编辑 IP 接入日志参数”页面，配置 IP 接入日志的基本信息，具体的配置参数如下表所示。

表-2 IP 接入日志的基本信息配置

参数	说明
输出登录成功日志	配置此功能后，通过IP地址认证接入的用户登录成功时会记录会话日志
输出登录失败日志	配置此功能后，通过IP地址认证接入的用户登录失败时会记录会话日志
输出正常退出日志	配置此功能后，通过IP地址认证接入的用户正常退出时会记录会话日志
输出不正常退出日志	配置此功能后，通过IP地址认证接入的用户不正常退出时会记录会话日志

3. 单击<确定>按钮，完成 IP 接入日志的基本信息配置。

IPv4 地址白名单

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 配置指南
  - 配置准备
  - 配置 IPv4 地址白名单

特性简介

IPv4 地址白名单列表是指 IP 认证过程中，若用户的 IPv4 地址处于 IPv4 地址白名单中，则无需通过认证服务器进行认证，直接通过认证。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置 IPv4 地址白名单

IPv4 地址白名单的具体配置如下：

1. 选择“网络 > 安全接入 > IP 接入 > IPv4 地址白名单”。
2. 在“IPv4 地址白名单”页面单击<新建>按钮，进入“新建 IPv4 地址白名单”页面，新建 IPv4 地址白名单，具体的配置参数如下表所示。

表-1 IPv4 白名单配置参数表

参数	说明
接口	选择白名单用户接入网络的设备接口
IPv4地址	配置白名单用户的IPv4地址
ISP域	配置白名单用户使用的认证域，该域的认证服务器必须为“none”域的详细介绍，请参见“认证管理”
描述	配置该用户白名单的描述信息

3. 单击<确定>按钮，新建 IPv4 地址白名单完成。

IPv6 地址白名单

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 配置指南
  - 配置准备
  - 配置 IPv6 地址白名单

特性简介

IPv6 地址白名单列表是指 IP 认证过程中，若用户的 IPv6 地址处于 IPv6 地址白名单中，则无需通过认证服务器进行认证，直接通过认证。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置 IPv6 地址白名单

IPv6 地址白名单的具体配置如下：

1. 选择“网络 > 安全接入 > IP 接入 > IPv6 地址白名单”。
2. 在“IPv6 地址白名单”页面单击<新建>按钮，进入“新建 IPv6 地址白名单”页面，新建 IPv6 地址白名单，具体的配置参数如下表所示。

表-1 IPv6 白名单配置参数表

参数	说明
接口	选择白名单用户接入网络的设备接口
IPv6地址	配置白名单用户的IPv6地址
ISP域	配置白名单用户使用的认证域，该域的认证服务器必须为“none”域的详细介绍，请参见“认证管理”
描述	配置该用户白名单的描述信息

3. 单击<确定>按钮，新建 IPv6 地址白名单完成。

ND

本帮助主要介绍以下内容：

- 特性简介
  - IP-MAC 绑定
  - ND 协议
- vSystem 相关说明
- 配置指南
  - 配置准备
  - 配置 IP-MAC 绑定表项
  - 配置 ND 表项

特性简介

IP-MAC 绑定

为增强设备的安全性，系统提供了 IP-MAC 绑定功能，即在设备上建立 IPv6 地址与 MAC 地址的对应关系即 IP-MAC 绑定表项，并基于该表项实现报文的过滤控制。该功能适用于防御主机仿冒攻击，可有效过滤攻击者通过仿冒合法用户主机的 IPv6 地址或者 MAC 地址向设备发送的伪造 IP 报文。

ND 协议

IPv6 邻居发现（Neighbor Discovery，ND）协议使用五种类型的 ICMPv6 消息（如下表所示），实现地址解析、验证邻居是否可达、重复地址检测、路由器发现/前缀发现、地址自动配置和重定向等功能。

表-1 ICMPv6 消息

ICMPv6 消息	类型号	作用
邻居请求消息NS（Neighbor Solicitation）	135	获取邻居的链路层地址
		验证邻居是否可达

		进行重复地址检测
邻居通告消息NA（Neighbor Advertisement）	136	对NS消息进行响应
		节点在链路层变化时主动发送NA消息，向邻居节点的变化信息
路由器请求消息RS（Router Solicitation）	133	节点启动后，通过RS消息向路由器发出请求，请其他配置信息，用于节点的自动配置
路由器通告消息RA（Router Advertisement）	134	对RS消息进行响应
		在没有抑制RA消息发布的条件下，路由器会周期RA消息，其中包括前缀信息选项和一些标志位的
重定向消息（Redirect）	137	当满足一定的条件时，缺省网关通过向源主机发消息，使主机重新选择正确的下一跳地址进行后发送

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置 IP-MAC 绑定表项

IP-MAC 绑定表项可以通过手工配置和批量生成两种方式进行创建。

- 手工配置绑定表项是指通过手工方式逐条配置 IP-MAC 绑定表项。该方式适用于局域网络中主机较少的情况。
- 批量生成绑定表项是指通过指定接口下的ND表项生成对应的IP-MAC绑定表项。该方式适用于局域网络中主机较多的情况。

配置 IP-MAC 绑定表项可以增加通信的安全性。设备收到报文后，提取报文头中的源 IPv6 地址和源 MAC 地址，并与 IP-MAC 绑定表项进行匹配。如果源 IPv6 地址和源 MAC 地址与 IP-MAC 绑定表项一致，则转发该报文；如果不一致，则认为该报文是非法报文，并将其丢弃。对于 IPv6 地址与 MAC 地址在 IP-MAC 绑定表项中都无匹配项的报文，则根据配置的缺省动作放行或丢弃。

若要使 IP-MAC 绑定表项生效，则需要在指定接口下开启 IP-MAC 接口绑定功能。开启 IP-MAC 接口绑定功能后，设备会对该接口上入方向的报文进行 IP 地址与 MAC 地址绑定关系的检测。

IP-MAC 绑定表项的具体配置步骤如下：

1. 选择“网络 > ND”，进入 ND 页面。
2. 在 ND 页面“配置 IP-MAC 绑定”下，配置批量生成 IP-MAC 绑定表项功能，具体的配置参数如下表所示。

表-2 配置 IP-MAC 绑定参数表

参数	说明
IP-MAC绑定功能	开启IP-MAC绑定功能
IP-MAC 接口绑定功能	在指定接口下开启 IP-MAC 接口绑定功能 在“接口列表”筛选指定接口 单击<添加>按钮，添加的接口在“成员列表”中显示 单击<全部添加>按钮，“接口列表”中所有接口将添加到“成 单击<确认>按钮，保存设置

缺省动作	未匹配上 IP-MAC 绑定表项的报文处理方式，包括： 放行 丢弃

3. 在 ND 页面的“IP-MAC 绑定列表”下，单击<新建>按钮，手工配置 IP-MAC 绑定表项，具体的配置参数如下表所示。

表-3 新建 IP-MAC 绑定参数表

参数	说明
IPv6地址	IP-MAC绑定表项的IPv6地址
MAC地址	IP-MAC绑定表项的MAC地址
VRF	IP-MAC绑定表项所属的VRF
VLAN	IP-MAC绑定表项所在的VLAN
时间段	IPv6-MAC绑定表项的生效时间段

状态	IPv6-MAC绑定表项的状态
	• 生效
	• 不生效
	  ○ 时间段不生效
	  ○ VPN 不生效

	○ VPN 与时间段均不生效

4. 在“新建 IP-MAC 绑定”页面，单击<确定>按钮，新建 IP-MAC 绑定表项成功会在“IP-MAC 绑定列表”中显示。

配置 ND 表项

邻居表项保存的是设备在链路范围内的邻居信息，设备邻居表项可以通过邻居请求消息 NS 及邻居通告消息 NA 来动态创建，也可以通过手工配置来静态创建。

目前，静态邻居表项有两种配置方式：

- 配置本节点的三层接口相连的邻居节点的 IPv6 地址和链路层地址。
- 配置本节点 VLAN 中的二层端口相连的邻居节点的 IPv6 地址和链路层地址。

对于 VLAN 接口，可以采用上述两种方式来配置静态邻居表项：

- 采用第一种方式配置静态邻居表项后，设备还需要解析该 VLAN 下的二层端口信息。
- 采用第二种方式配置静态邻居表项后，需要保证该二层端口属于指定的 VLAN，且该 VLAN 已经创建了 VLAN 接口。

ND 表项的具体配置步骤如下：

1. 选择“网络 > ND”，进入 ND 页面。

2. 在ND页面的“ND列表”下，单击<新建>按钮，手工配置静态邻居表项，具体的配置参数如下表所示。

表-4 新建邻居表项参数表

参数	说明
VRF	邻居表项所属的VRF
IPv6地址	邻居表项的IPv6地址
MAC地址	邻居表项的MAC地址
接口	报文转发的接口

3. 在“新建邻居表项”页面，单击<确定>按钮，新建邻居表项会在ND列表显示。

4. 在“ND列表”中，勾选邻居表项前的复选框，单击<IP-MAC绑定>按钮，ND表项生成对应的IP-MAC绑定表项，会在“IP-MAC绑定列表”中显示。

转发高级设置

本帮助主要介绍以下内容：

- 特性简介
  - DF 标志位处理方式
  - 报文转发模式
  - IPv4 虚拟分片重组
  - IPv6 虚拟分片重组
  - 优先使用虚拟 MAC 作为报文源 MAC
- vSystem 相关说明
- 配置指南
  - 配置准备
  - 配置转发高级设置

特性简介

DF 标志位处理方式

设备转发 IP 报文时，由于链路 MTU 值可能会对 IP 报文进行分片。如果设备收到携带 DF（Don’t Fragment，不分片）标记的 IP 报文，设备不会转发该 IP 报文，但会向报文发送端发送 ICMP 差错报文，这样会导致通信中断。

当用户在设备上配置 IP 报文 DF 标志位后，设备会直接修改 IP 报文中的 DF 标志位，使得该 IP 报文可以被分片转发。

配置本功能后，设备会修改所有转发 IP 报文的 DF 标志位，不会修改本设备生成的 IP 报文的 DF 标志位。

报文转发模式



报文转发模式的支持情况与设备型号有关，请以页面的实际显示为准。

多核设备上，报文在 CPU 之间进行负载分担的策略包括：

- 逐流：根据以下不同的匹配原则，来区分和划定一条流，同一条流被分配到同一个或多个 CPU 进行处理，处理过程保证先进先出。

    - 基于一元组：基于源 IP 地址、目的 IP 地址、源端口或目的端口中的任意一种，将报文划分为不同的流。
    - 基于三元组：基于源 IP 地址、目的 IP 地址和协议号将报文划分为不同的流。
    - 基于五元组：基于源 IP 地址、源端口号、目的 IP 地址、目的端口号和协议号将报文划分为不同的流。
- 逐包：将报文依次发送到不同的 CPU 进行处理，不保证报文的处理顺序。

IPv4 虚拟分片重组

IPv4 虚拟分片重组功能可以提前对到达设备的分片报文进行检验、排序和缓存。开启本功能，可以保证后续的报文重组功能处理的都是顺序正确的分片报文。

在高可靠性组网环境中，如果出现同一条流的分片报文分别到达了两个设备的情况，则每个设备上收到的 IPv4 分片报文都不完整，此时设备的 IPv4 虚拟分片重组功能无法对不完整的分片报文进行重组，因此会对其进行丢弃。开启本功能后，未收到首个分片的设备，会将接收到的分片报文全部透传给收到同一条流首片报文所在的设备，实现同一条流的分片报文在一个设备上集中处理，即 IPv4 虚拟分片重组。

如果需要设备对接收到不完整的分片报文进行放行，则可以关闭设备的 IPv4 虚拟分片重组功能。

IPv6 虚拟分片重组

IPv6 虚拟分片重组功能可以提前对到达设备的分片报文进行检验、排序和缓存。开启本功能，可以保证后续的报文重组功能处理的都是顺序正确的分片报文。

在高可靠性组网环境中，如果出现同一条流的分片报文分别到达了两个设备的情况，则每个设备上收到的 IPv6 分片报文都不完整，此时设备的 IPv6 虚拟分片重组功能无法对不完整的分片报文进行重组，因此会对其进行丢弃。开启本功能后，未收到首个分片的设备，会将接收到的分片报文全部透传给收到同一条流首片报文所在的设备，实现同一条流的分片报文在一个设备上集中处理，即 IPv6 虚拟分片重组。

如果需要设备对接收到不完整的分片报文进行放行，则可以关闭设备的 IPv6 虚拟分片重组功能。

优先使用虚拟 MAC 作为报文源 MAC

在 HA 镜像模式、HA 联动 VRRP、HA 联动虚拟地址三种组网场景中，RBM 成员设备的业务接口在发送 ARP 应答报文时会使用虚拟 MAC 地址进行应答，但经过业务主设备处理过的报文会使用接口的实际 MAC 地址对报文进行封装，此时可能会出现问题。例如，RBM 成员设备的上下行设备开启 ARP 报文源 MAC 地址一致性检查功能时，由于报文的源 MAC 地址，也就是 RBM 成员设备接口的实际 MAC 地址与 ARP 应答报文中的虚拟 MAC 地址不一致，此时报文会被丢弃从而导致业务中断。

在 RBM 主管理设备上开启本功能，使主设备的业务接口发送的报文也使用虚拟 MAC 地址来封装，从而避免上述问题出现。

本功能支持配置同步，当在“系统 < 高可靠性 < 双机热备”页面开启“自动同步配置信息”功能后，只需在 RBM 主管理设备上开启本功能。当接口下配置多个 VRRP 备份组与 HA 关联时，不支持使用本功能。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。

- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置转发高级设置

转发高级设置的具体配置步骤如下：

1. 选择“网络 > 转发高级设置”。

2. 进入转发高级设置页面，具体的配置参数如下表所示。

表-1 转发高级设置参数表

参数	说明
DF位设置	DF标志位处理方式，包括： • 不修改（默认）：保留当前 IP 报文 DF 标志位取值 • 置位：配置 IP 报文头中的 DF 位为 1，表示不允许报文分片 • 清除：配置 IP 报文头中的 DF 位为 0，表示允许报文分片
转发模式	报文转发模式，包括： • 逐流：基于一元组、基于三元组、基于五元组 • 逐包
IPv4虚拟分片重组	开启/关闭IPv4虚拟分片重组功能
IPv6虚拟分片重组	开启/关闭IPv6虚拟分片重组功能
优先使用虚拟MAC作为报文	开启/关闭接口发送报文的源MAC地址优先使用虚拟MAC功能

源MAC	仅适用于HA镜像模式、HA联动VRRP、HA联动虚拟地址三种组网场景，其 勿使用本功能

管理员

本帮助主要介绍以下内容：

- 特性简介
  - 账户管理
  - 角色管理
  - 密码管理
  - 弱密码管理
  - RBM 同步功能
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 新建管理员
  - 配置管理员密码管理功能
  - 新建管理员角色

特性简介

管理员通过 SSH、Telnet、FTP、HTTP、HTTPS、终端接入（即从 Console 口接入）方式登录到设备上之后，可以对设备进行配置和管理。对登录用户的管理和维护主要涉及以下几个部分：

- 账户管理：对用户的基本信息（用户名、密码）以及相关属性的管理。
- 角色管理：对用户可执行的系统功能的管理。
- 密码管理：对用户密码设置控制、密码更新与老化以及用户登录控制等方面进行管理。

账户管理

为使请求某种服务的用户可以成功登录设备，需要在设备上添加相应的账户。所谓用户，是指在设备上设置的一组用户属性的集合，该集合以用户名唯一标识。一个有效的用户条目中可包括用户名、密码、角色、可用服务、密码管理等属性。

角色管理

对登录用户权限的控制，是通过为用户赋予一定的角色来实现。一个角色中定义了允许用户执行的系统功能，例如，定义用户角色规则允许用户配置 A 功能，或禁止用户配置 B 功能。

角色规则

一个角色规则中定义了允许/禁止用户操作某类实体的权限。

Web 界面支持的实体类型为 Web 菜单，即通过 Web 对设备进行配置时，各配置页面以 Web 菜单的形式组织，按照层次关系，形成多级菜单的树形结构。

对实体的操作权限包括：

- 读权限：可查看指定实体的配置信息和维护信息。
- 写权限：可配置指定实体的相关功能和参数。
- 执行权限：可执行特定的功能，如与 FTP 服务器建立连接。

定义一个规则，就等于约定允许或禁止用户针对某类实体具有哪些操作权限。对于 Web 菜单实体，控制 Web 菜单的规则就是用来控制指定的 Web 菜单选项是否允许被操作。因为每个菜单项中的操作控件具有相应的读，写或执行属性，所以定义基于 Web 菜单的规则时，可以精细地控制菜单项中读、写或执行控件的操作。

缺省角色

系统预定义了多种角色，角色名和对应的权限如表-1 所示。这些缺省角色均具有不同的系统功能操作权限。如果系统预定义的用户角色无法满足权限管理需求，管理员还可以自定义用户角色来对用户权限做进一步控制。

表-1 系统预定义的角色名和对应的权限

角色名	权限
超级管理员	超级管理员拥有操作设备所有功能的权限
安全管理员	安全管理员拥有配置安全业务功能和监控安全业务处理状态的权限
审计管理员	审计管理员仅拥有审计设备操作的权限
系统管理员	系统管理员拥有配置设备系统功能和监控设备运行状态的权限
虚拟设备超级管理员	虚拟设备超级管理员拥有操作虚拟设备所有功能的权限 虚拟设备超级管理员的支持情况与设备型号有关，请以设备的实际情况为准
虚拟系统超级管理员	虚拟系统超级管理员拥有操作虚拟系统所有功能的权限 虚拟系统超级管理员的支持情况与设备型号有关，请以设备的实际情况为准

为用户赋予角色

根据用户认证登录方式的不同，为用户授权角色分为以下几类：

对于通过本地 AAA 认证登录设备的用户，由本地用户配置决定为其授权的用户角色。

对于通过 AAA 远程认证登录设备的用户，由 AAA 服务器的配置决定为其授权的用户角色。

将有效的角色成功授权给用户后，登录设备的用户才能以各角色所具有的权限来配置、管理或者监控设备。如果用户没有被授权任何角色，将无法成功登录设备。

一个用户同时只能拥有一个角色。

密码管理

为了提高用户登录密码的安全性，可通过定义密码管理策略对用户的登录密码进行管理，并对用户的登录状态进行控制。

密码长度检查

管理员可以限制用户密码的最小长度。当设置用户密码时，如果输入的密码长度小于设置的密码最小长度，系统将不允许设置该密码。缺省情况下，密码的最小长度为 10 个字符。

密码复杂度检查

为确保用户的登录密码具有较高的复杂度，要求管理员为其设置的密码必须符合一定的复杂度要求，只有符合要求的密码才能设置成功。目前，可配置的复杂度要求包括：

- 不允许密码中包含用户名或颠倒的用户名。例如，用户名为“abc”，那么“abc982”或者“2cba”之类的密码就不符合复杂度要求。



本功能在本地用户密码管理界面和全局密码管理界面均开启才生效

- 不允许密码中包含连续三个或以上的相同字符。例如，密码“a111”就不符合复杂度要求。



本功能在本地用户密码管理或全局密码管理界面任一位置开启都生效

密码组合检查

管理员可以设置用户密码的组成元素的组合类型，以及至少要包含每种元素的个数。



本功能需在全局密码管理对应功能开启的情况下，本地用户密码管理下的配置才生效

密码的组成元素包括以下 4 种类型：

- [A ~ Z]
- [a ~ z]
- [0 ~ 9]
- 32 个特殊字符（空格~`!@#$%^&*()_+-={}|[]\:";'<>,./）

密码元素的组合类型有 4 种，具体涵义如下：

- 组合类型为 1 表示密码中至少包含 1 种元素；
- 组合类型为 2 表示密码中至少包含 2 种元素；
- 组合类型为 3 表示密码中至少包含 3 种元素；
- 组合类型为 4 表示密码中包含 4 种元素。

当用户设置密码时，系统会检查设定的密码是否符合配置要求，只有符合要求的密码才能设置成功。

密码更新

管理员可以设置用户登录设备后修改自身密码的最小间隔时间。有两种情况下的密码更新并不受该功能的约束：开启密码管理后，用户首次登录设备时系统要求用户修改密码和密码老化后系统要求用户修改密码。

密码老化

当用户登录密码的使用时间超过密码老化时间后，需要用户更换密码。如果用户输入的新密码不符合要求，或连续两次输入的新密码不一致，系统将要求用户重新输入。对于 FTP 用户，密码老化后，只能由管理员修改 FTP 用户的密码；对于 Telnet、SSH、Terminal（通过 Console 口登录设备）用户可自行修改密码。缺省情况下，密码的老化时间为 90 天。



本功能需在全局密码管理对应功能开启的情况下，本地用户密码管理下的配置才生效

密码过期提醒

在用户登录时，系统会判断其密码距离过期的时间是否在设置的提醒时间范围内。如果在提醒时间范围内，系统会提示该密码还有多久过期，并询问用户是否修改密码。如果用户选择修改，则记录新的密码及其设定时间。如果用户选择不修改或者修改失败，则在密码未过期的情况下仍可以正常登录。对于 FTP 用户，只能由管理员修改 FTP 用户的密码；对于 Telnet、SSH、Terminal（通过 Console 口登录设备）用户可自行修改密码。

密码过期后允许登录

管理员可以设置用户密码过期后在指定的时间内还能登录设备的次数。这样，密码老化的用户不需要立即更新密码，依然可以登录设备。例如，管理员设置密码老化后允许用户登录的时间为 15 天、次数为 3 次，那么用户在密码老化后的 15 天内，还能继续成功登录 3 次。

密码历史记录

管理员可以设置系统保存用户密码历史记录。当用户修改密码时，系统会要求用户设置新的密码，如果新设置的密码以前使用过，且在当前用户密码历史记录中，系统将提示用户密码更改失败。另外，用户更改密码时，系统会将新设置的密码与所有历史记录密码以及当前密码逐一比较，要求新密码至少与旧密码有 4 字符不同。并且，这 4 个字符必须互不相同，否则密码更改失败。

可以配置每个用户密码历史记录的最大条数，当密码历史记录的条数超过配置的最大历史记录条数时，新的密码历史记录将覆盖该用户最老的一条密码历史记录。

由于设备管理类本地用户配置的密码在哈希运算后以密文的方式保存，配置一旦生效后就无法还原为明文密码，因此，设备管理类本地用户的当前登录密码不会被记录到密码历史记录中。

密码尝试次数限制

密码尝试次数限制可以用来防止恶意用户通过不断尝试来破解密码。



本功能需在全局密码管理对应功能开启的情况下，本地用户密码管理下的配置才生效

每次用户认证失败后，系统会将该用户加入密码管理的黑名单。可加入密码管理功能黑名单的用户包括：FTP 用户和通过 VTY 方式访问设备的用户。不会加入密码管理功能黑名单的用户包括：用户名不存在的用户、通过 Console 口连接到设备的用户。

当用户连续尝试认证的失败累加次数达到用户登录尝试的最大次数时，系统对用户的后续登录行为有以下三种处理措施：

- 永久禁止登录。只有管理员把该用户从密码管理的黑名单中删除后，该用户才能重新登录。
- 暂时禁止登录。当配置的禁止时间超时或者管理员将其从密码管理的黑名单中删除，该用户才可以重新登录。
- 允许继续登录。在该用户登录成功后，该用户会从密码管理的黑名单中删除。

缺省情况下，用户登录尝试次数为 3 次。如果用户登录失败，则允许该用户在 1 分钟后重新登录。

账号闲置时间管理

管理员可以限制用户账号的闲置时间。管理员用户创建后，需要成功登录一次设备，账号闲置时间才能生效，在配置的闲置时间内，用户从未成功登录，该用户将被锁定，无法登录。

弱密码管理

若管理员设置的密码为弱密码，无论密码管理是否开启，设备都在用户登录时弹框提示，建议修改密码。

弱密码的判断条件包括以下几项，只要其中一项不符合，系统就识别为弱密码：

- 密码长度检查。有关此项详细介绍，请参见上文中的“密码长度检查”。
- 密码组合检查。有关此项详细介绍，请参见上文中的“密码组合检查”。
- 密码中不能包括用户名或者字符顺序颠倒的用户名。有关此项详细介绍，请参见上文中的“密码复杂度检查”。
- 不允许密码中包含连续三个或以上的相同字符。此项弱密码判断条件仅当密码管理功能开启后才生效。有关此项详细介绍，请参见上文中的“密码复杂度检查”。

可以根据实际使用场景，开启“弱密码时强制修改密码”功能。本功能仅对后续新登录的用户生效，不影响当前已登录用户。当用户使用弱密码登录，若未开启本功能，系统仅在登录时弹框建议修改弱密码，但不强制。用户可以忽略提示，继续登录设备。若开启了本功能，系统会强制要求修改为非弱密码才允许登录设备。管理员开启“弱密码时强制修改密码”功能时，必须至少配置一项弱密码判断条件。

RBM 同步功能

当 RBM 处于主备或双主运行模式时，设备默认不支持同步本地管理类用户的配置信息，如需同步配置信息，则需要开启 RBM 同步功能。具体配置步骤如下：

1. 选择“系统 > 管理员 > 管理员”。
2. 在“管理员”页面，单击<开启 RBM 同步功能>按钮。

3. 在弹出的确认框中单击<确定>按钮，完成配置。

开启 RBM 同步功能后，主设备会向备设备发起一次本地管理类用户相关配置和数据的平滑同步，从而使备设备的本地管理类用户相关配置和数据与主设备一致。

当 RBM 处于镜像运行模式时，设备默认支持同步本地管理类用户的配置信息，不需要开启 RBM 同步功能。

开启 RBM 同步功能前，需要先配置 RBM 自动同步配置信息功能，有关该功能的详细介绍，请参见双机热备模块的相关说明。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 管理员密码管理界面下的配置为全局配置，对所有用户生效。新建或修改指定管理员界面下的配置本文称之为本地用户密码管理配置，只对当前用户生效。本地用户密码管理中的配置优先级高于全局配置。
- 当前用户登录密码尝试失败次数到配置的最大值后，无法使用自己的 IP 地址访问设备。
- 修改后的规则对于当前已经在线的用户不生效，对于之后使用该角色登录设备的用户生效。

- 若要使得具体的密码管理功能生效，需在管理员页面菜单栏的<密码管理>中开启密码管理功能。
- 管理员页面和本地用户页面中的密码管理部分功能相互关联且参数共用，具体可参见管理员页面<密码管理>中各配置栏的提示信息。
- 开启密码管理之后，设置的登录用户密码必须至少由四个不同的字符组成。
- 对于 FTP 用户，密码过期后，系统不允许其继续登录，也不允许 FTP 用户自行更改密码，只能由管理员修改 FTP 用户的密码。
- 由于 FTP 用户不支持计费，因此 FTP 用户不受同时在线最大用户数限制。
- 新建管理员角色的权限必须是安全管理员权限的子集，不能超过安全管理员的权限范围。

配置指南

新建管理员

新建管理员的具体配置步骤如下：

1. 选择“系统 > 管理员 > 管理员”。
2. 在“管理员”页面配置相关内容，具体配置内容如下所示：

表-2 管理员参数配置

参数	说明
用户名	设备管理类用户，用于登录设备，对设备进行配置和监控
密码和确认密码	用户进行接入认证所使用的密码
管理员角色	对登录用户权限的控制，是通过为用户赋予一定的角色来实现。不同的管理员角色拥 功能
用户组	每一个用户都属于一个用户组，并继承组中的所有属性
可用服务	指用户可使用的服务类型。该属性是本地认证的检测项，如果没有用户可以使用的服 用户无法通过认证
同时在线最高值	使用当前用户名接入设备的最大用户数目。若当前该用户名的接入用户数已达最大值 户名的新用户将被禁止接入
FTP目录	授权用户可以访问的目录，且该目录必须已经存在

3. （可选）高级设置，具体包括如下所示：

表-3 高级设置参数表

参数	说明
密码最小长度	限制设置密码的最小长度
密码组成元素的最少类型	选择密码包含的种类个数

每种类型最少包含个数	每种类型密码包含的个数 当没有填写密码组成元素的最少类型时，此功能不支持
开启密码老化	开启设备密码老化功能，超过设定的时间后需要用户修改密码
密码老化时间	当密码的使用时间超过老化时间后，需要用户更换密码，此功能需要在密码管理中开 能生效
不允许密码中包含用户名或颠倒的用户名	密码中禁止出现用户名或颠倒的用户名相关字符
不允许密码中包含连续三个或以上相同的字符	密码中禁止连续出现三个或三个以上的相同字符，此功能需要在密码管理中开启相关
用户登录尝试的最大次数	当前用户尝试登录的最大次数，可在后续选择登录失败的处理方式，此功能需要在密 相关功能才能生效
登录次数超过最大值后的处理方式	• 永久禁止登录 • 在指定时间内禁止登录 • 允许继续登录 当没有填写用户尝试登录的最大次数时，此功能不支持
禁止登录时长	禁止用户登录设备的时长

4. 单击<确定>按钮，新建管理员成功，且会在“管理员”页面中显示。

配置管理员密码管理功能

1. 单击“系统 > 管理员 > 管理员”。

2. 在“管理员”页面单击<密码管理>按钮，进入“管理员密码管理”页面。

3. 在“管理员密码管理”页面的具体配置内容如下所示：

表-4 密码管理参数配置

参数	说明
开启密码管理	开启全局登录密码的一些相关配置
开启密码长度检查	开启密码最小长度管理功能
用户密码的最小长度为	限制设置密码的最小长度
开启密码组合检查	开启密码的组合检测管理功能
密码组成元素的类型至少包含	选择密码组成元素包含的种类个数
每种类型包含的元素个数至少为	每种类型密码包含的元素个数
密码中不能包含连续三个或以上相同的相同字符	全局开启密码中禁止连续出现三个或三个以上的相同字符
密码中不能包含用户名或者字符顺序	全局开启密码中禁止出现用户名或颠倒的用户名相关字符

颠倒的用户名	
开启密码历史记录	开启密码历史记录检测管理功能
密码历史记录最大条数	系统记录某用户历史密码的最大条数，达到最大值后，会覆盖最老的一条密码历史记
开启密码老化	开启设备密码老化功能，超过设定的时间后需要用户修改密码
密码老化时间	配置密码老化的时间
密码过期提醒	密码过期前的提醒时间
密码过期后允许用户登录的时间	密码过期后可以在设置的时间内继续登录
密码过期后允许用户登录的次数	密码过期后可以继续登录的次数
密码更新最小间隔时间	密码更新的最小时间间隔，0表示对密码更新的时间间隔无限制
密码尝试次数	设置用户登录设备尝试登录的最大次数
登录失败处理	登录次数超过密码尝试次数后，可选择永久禁止登录、暂时禁止登录和允许继续登录
账号闲置时间	管理员账号闲置时间，管理员用户创建后，需要成功登录一次设备，账号闲置时间大置的闲置时间内，用户从未成功登录，该用户将被锁定，无法登录
弱密码时强制修改密码	开启此功能后，如果当前用户密码符合弱密码的判断条件，会被强制修改密码

4. 单击<确定>按钮，完成密码管理的配置。

新建管理员角色

1. 选择“系统 > 管理员 > 管理员角色”。

2. 在“管理员角色”页面单击<新建>按钮，进入新建管理员角色页面，具体配置内容如下所示：

表-5 管理员角色配置

参数	说明
名称	管理员角色名，不可使用设备中的关键字作为名称
描述	配置有关此管理员角色的描述信息
权限控制项	此权限控制项，将Web菜单界面，按照层次关系形成多级菜单的树形结构，通过控制只读或无的操作，来完成管理员角色权限的定制

3. 单击<确定>按钮，完成新建管理员角色的配置。

双机热备

本帮助主要介绍以下内容：

- 特性简介
  - 基本概念
  - 运行模式
  - 双机热备通道
  - 业务表项备份
  - 配置信息备份
  - 配置信息一致性检查
  - 双机热备联动 VRRP
  - 双机热备联动虚拟地址
  - 双机热备联动路由
  - 双机热备透明组网
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南

- 配置思路
- 配置准备
- 配置主备模式双机热备
- 配置双主模式双机热备
- 配置镜像模式双机热备
- 双机热备高级功能

特性简介

双机热备（RBM）是一种通过我司私有的 RBM（Remote Backup Management，远端备份管理）协议，实现设备级的高可靠性（High Availability，简称 HA）的技术。此技术能够在通信线路或设备产生故障时提供备用方案，当其中一个网络节点发生故障时，另一个网络节点可以接替故障节点继续工作。

双机热备通过 RBM 协议管理多个 VRRP 备份组状态的切换或者调整动态路由协议的开销值等，选举出双机热备中每台设备的主备业务状态。双机热备通过 RBM 协议备份设备间的关键配置信息和业务表项等，从而保证用户业务数据的不间断传输。需要两台软硬件环境完全相同的设备进行双机热备组网。

基本概念

双机热备技术包含的基本概念如下：

- 主、从管理设备：双机热备中的设备分为主、从两种管理角色，用于控制设备之间关键配置信息的同步。双机热备建立成功后，只能在主管理设备配置相关业务（支持配置信息同步的功能），从管理设备不能配置。配置信息将从“主管理设备”同步到“从管理设备”，并覆盖从管理设备上的相关配置信息。
- 主、备业务设备：双机热备中包含主、备两种设备，其中主设备对应 VRRP 备份组中的 Master 设备；备设备对应 VRRP 备份组中的 Backup 设备。主设备为业务提供支持，转发业务流量，并向备设备实时备份业务表项信息；备设备除接收主设备的业务表项备份信息外，在主设备发生故障后，备设备会转换成主设备，继续转发业务流量，保证业务不中断。
- VRRP active 组和 VRRP standby 组：用于将双机热备与 VRRP 进行关联，实现双机热备对多个 VRRP 备份组状态进行统一管理的目的。
- 双机热备通道：两台设备之间交互双机热备的运行状态信息，关键配置信息和业务表信息的传输通道。
- 双机热备运行模式：支持主备、镜像和双主三种工作模式。主备模式下，仅由主设备处理业务，备设备处于待命状态；镜像模式下，两台设备的接口（镜像模式管理接口和 RBM 通道接口除外）使用相同的 IP 地址，同样由主设备处理业务，备设备处于待命状态；双主模式下，两台设备同时处理业务，充分利用设备资源，提高系统负载分担能力。

- 双机热备报文：双机热备使用 TCP 作为其传输层协议，TCP 连接建立后，主管理设备和从管理设备通过双机热备通道交互双机热备报文。
- 镜像模式管理接口：在 RBM 镜像模式下，主管理设备上的接口配置（镜像模式管理接口和 RBM 通道接口除外）会同步到从管理设备，两台设备上用于连接网管设备和日志主机的接口拥有相同的 IP 地址。此时只有主设备可以连接网管设备和日志主机，备设备无法连接。为避免上述问题，管理员可配置镜像模式管理接口，管理接口下的配置信息不会进行同步。

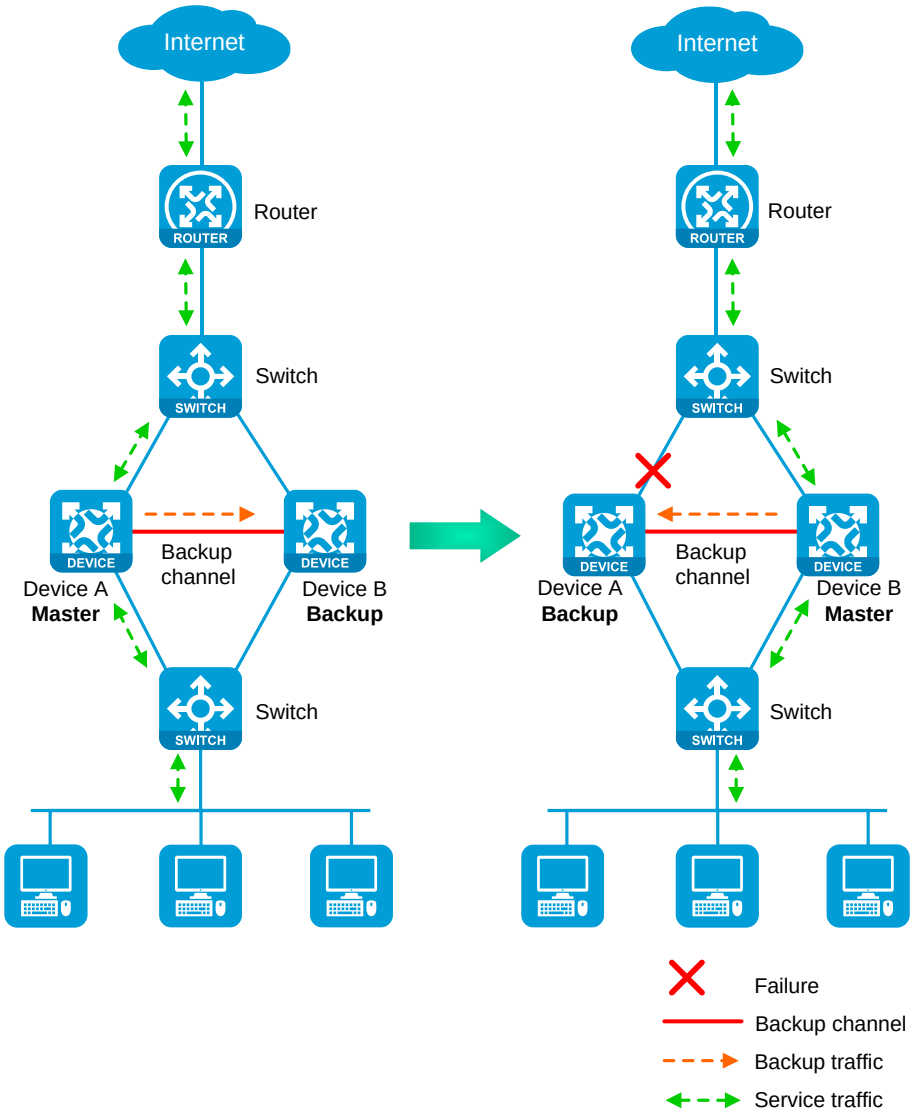
运行模式

双机热备支持主备、镜像和双主三种运行模式，具体介绍如下。

主备模式

如图-1 所示，主备模式下，正常情况仅由主设备处理业务，备设备处于待命状态；当主设备接口、链路或整机故障时，备设备立即切换为主设备，接替原主设备处理业务。

图-1 主备模式的双机热备示意图



镜像模式

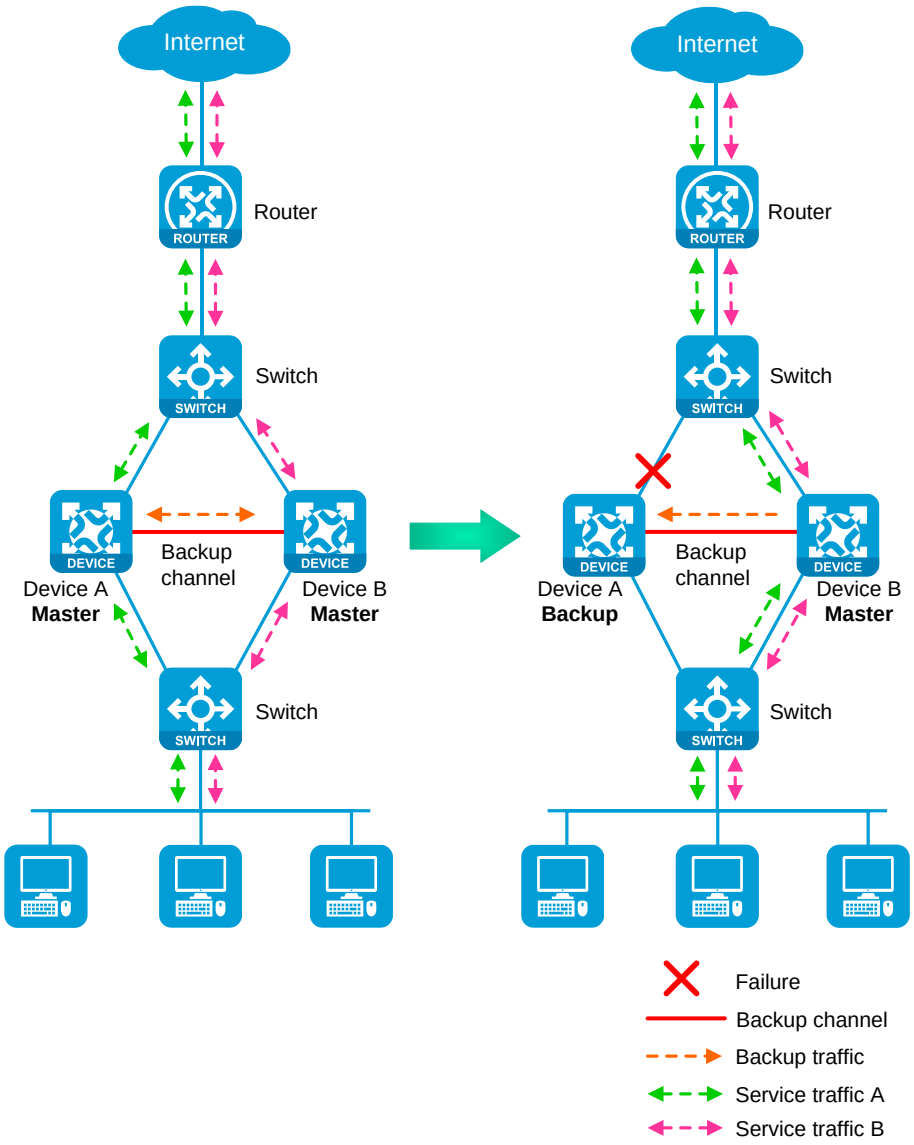
镜像模式是一种特殊的主备模式，部署方式与主备模式相同。在镜像模式下，两台设备的接口（镜像模式管理接口和 RBM 通道接口除外）使用相同的 IP 地址，正常情况下同样由主设备处理业务，备设备处于待命状态；当主设备接口、链路或整机故障时，备设备立即切换为主设备，接替原主设备处理业务。

此组网环境中双机热备必须关联 Track 项，否则上下行链路或接口故障时，双机热备不能主备切换。

双主模式

如图-2 所示，双主模式下，两台设备同时处理业务，充分利用设备资源，提高系统负载能力，此模式通过互为主备方法实现。并且当其中一台设备发生故障时，另外一台设备会立即承担其业务，保证业务不中断。

图-2 双主模式的双机热备示意图



双机热备通道

通道简介

双机热备通道用于两台设备之间交互双机热备的运行状态、关键配置和业务表项等信息，包括以下类型的通道：

- 控制通道：用来同步设备之间的所有数据，包括双机热备的心跳报文、运行状态报文、一致性检查报文、业务表项的热备报文、数据透传报文和同步配置信息的报文等。
- 数据通道：仅用于传输设备之间的热备报文和透传报文，不用于传输双机热备的其他报文。数据通道的报文传输模式支持使用二层或三层。

控制通道的建立和保活

控制通道基于 TCP 协议来监测链路的连通性。其使用 TCP 方式进行创建，在创建过程中，使用 IP 地址较大的设备作为 Server 建立 TCP 监听，而 IP 地址较小的设备作为 Client 向对端设备发起建立 TCP 连接请求。

控制通道建立后，设备会周期性向对端设备发送 Keepalive 报文，如果达到最大发送次数后仍然没有收到对端的回应，则双机热备通道断开，双机热备失效。

业务表项备份

功能简介

双机热备可以将主设备上生成的业务表项信息实时备份到备设备，避免了主备设备切换时因备设备上缺失业务表项而造成的业务中断问题。

需要对报文进行状态检测的设备（如防火墙等），对于每个动态生成的连接，都有一个会话表项与之对应。主设备在处理业务的过程中创建了很多会话表项；而备设备没有报文经过，因此也就没有创建会话表项。通过双机热备的业务表项实时备份功能，主设备会将会话表项备份到备设备，当主备切换后，已有连接的后续业务报文就可以通过匹配备份来的会话表项而保持业务不中断。

支持备份的表项

目前双机热备支持热备的业务表项包括：IPsec 隧道相关的信息表项、域名解析相关的表项、会话表项、会话关联表项、NAT 端口块表项、AFT 端口块表项和各个安全业务模块自身生成的业务表项。

此处仅是列出双机热备所支持热备份表项的所有业务模块，但是不同产品对这些表项的支持情况不同，请以设备对相关功能的实际支持情况为准。

配置信息备份

功能简介

双机热备可以将主管理设备上的关键配置信息备份到从管理设备，避免了主备设备切换时因对端设备缺失对应的配置信息而造成的业务中断问题。

为了保证备设备可以平滑地接替主设备的工作，双机热备必须能够将主设备的相关配置信息备份到备设备。尤其在双主组网环境中，两台设备都是主设备。如果允许两台主设备之间能够相互备份配置信息，那么就会造成两台设备上配置信息相互覆盖或冲突的问题。所以为了方便管理员对两台设备的配置信息进行统一管理，又能避免配置信息的混乱，我们引入了主管理设备和从管理设备的概念。

配置信息只能从“主管理设备”同步到“从管理设备”，并覆盖从管理设备上的相关配置，保证主从管理设备的配置信息一致。因此建议仅在主管理设备上配置相关功能，不建议在从管理设备上进行配置。

备份方式

双机热备支持实时备份和批量备份两种方式，以满足不同场景的需求。需要注意，仅当自动同步配置信息功能处于开启状态且 RBM 控制通道建立成功的情况下，双机热备才会执行实时备份或批量备份。具体说明如下：

- 实时备份：主管理设备上的配置变更（新增、删除、修改）会实时通过 RBM 控制通道同步至从管理设备，确保主从管理设备配置动态一致。

- 批量备份：主管理设备将所有关键配置完整备份至从管理设备，并自动删除从管理设备上的不一致配置，确保主从管理设备配置完全一致。

批量备份支持自动和手动两种触发方式。

- 手动触发：在主设备上单击<手工同步配置信息>按钮，即可触发主管理设备批量备份配置信息到从管理设备，且每单击一次就会执行一次批量备份。如果当前已有批量备份任务进行中，则重复单击无效。
- 自动触发：在以下场景中将自动触发批量备份。
  - 首次通道建立：当 RBM 控制通道首次成功建立且自动备份功能首次开启（包括默认开启）时，主管理设备将自己当前的所有关键配置批量覆盖备份至从管理设备。此操作仅执行一次，后续重复开启自动备份功能或重建通道，也不会再次触发批量备份。
  - 设备或进程重启：若设备或 RBM 进程重启期间，自动备份功能始终保持开启，则在重启完成且控制通道重建后，未重启的设备会将自己当前所有关键配置批量覆盖备份至已重启设备。

通过 Web 界面进行部分模块的批量导入（如.cfg 文件、特征库等）时，其是否支持实时备份及批量备份，需结合具体功能模块判断。下表列出了常见场景的支持情况，但是不同产品对这些业务模块的支持情况不同，请以设备实际情况为准。

表-1 Web 导入操作与双机热备同步能力说明

模块	是否支持实时备份	是否支持批量备份	说明
安全策略导入(.cfg文件)	是	是	

主动防护-黑名单	是	是	
DLP-DLP策略导入	否	否	不支持任何备份方式，必须在主、从管理设备分别导入
用户与认证-本地用户	是	是	
安全配置文件-入侵防御-特征-导入Snort特征	是	是	
证书与密钥-公钥管理-本地密钥对	是	是	
证书与密钥-PKI-证书	是	是	
地址对象组	否	是	不支持实时备份，但可通过“手工同步配置信息”或开启自动同步配置信息实现批量备份

对于通过 Web 界面执行的大规模配置导入操作（如导入.cfg 文件、黑名单、大量用户、Snort 特征等），建议按照以下步骤操作，以避免因同步通道拥塞、处理超时或数据截断导致的配置丢失等问题：

2. 临时关闭“自动同步配置信息”功能，防止主管理设备在导入过程中频繁触发配置同步，造成 RBM 通道阻塞或超时。
3. 在主管理设备和从管理设备上分别执行导入操作。
4. 导入完成后重新开启“自动同步配置信息”功能，并执行手工一致性检查，确保配置最终一致。

支持配置信息备份的模块

目前双机热备主备和双主模式下支持配置信息同步的业务模块如下：

- 资源类：VPN 实例、ACL、对象组、时间段、安全域、会话管理、APR、AAA、域名解析。
- DPI 相关模块：应用层检测引擎、IPS、URL 过滤、数据过滤、文件过滤、防病毒、数据分析中心、WAF、APT 防御。
- 策略类：安全策略、ASPF、攻击检测与防范、连接数限制、NAT、AFT、负载均衡、全局负载均衡、带宽管理、应用审计与管理、共享上网管理、代理策略。
- 日志类：快速日志输出、Flow 日志。
- VPN 类：SSL VPN、IPsec。
- 其他类：Password Control、VLAN、信息中心、云平台连接、IPoE。

在镜像模式下除上述模块支持配置信息同步外，还有以下模块支持配置信息同步：登录设备、配置文件管理、设备管理、MAC 地址表配置、VLAN 终结、二层转发、ARP、IP 地址、DHCP、IP 转发基础、快速转发、多 CPU 报文负载分担、IP 性能优化、IPv6 基础、DHCPv6、IPv6 快速转发、隧道、GRE、IP 路由基础、静态路由、RIP、OSPF、BGP、策略路由、IPv6 静态路由、RIPng、OSPFv3、IPv6 策略路由、路由策略、MPLS L3VPN、QOS、Keychain、PKI、SSH、ARP 攻击防御、MFF、BFD、NTP、SNMP、EVI、VXLAN。

此处仅是列出双机热备支持配置信息同步的所有业务模块，但是不同产品对这些业务模块的支持情况不同，请以设备实际情况为准。

配置信息一致性检查

双机热备通过交互一致性检查报文来检测两台设备的配置信息是否一致，用于防止由于两台设备配置信息不一致，而导致主备切换后业务不通的情况。当配置信息不一致时，设备会发送日志信息，以提示管理员进行配置信息的手动同步。

双机热备联动 VRRP

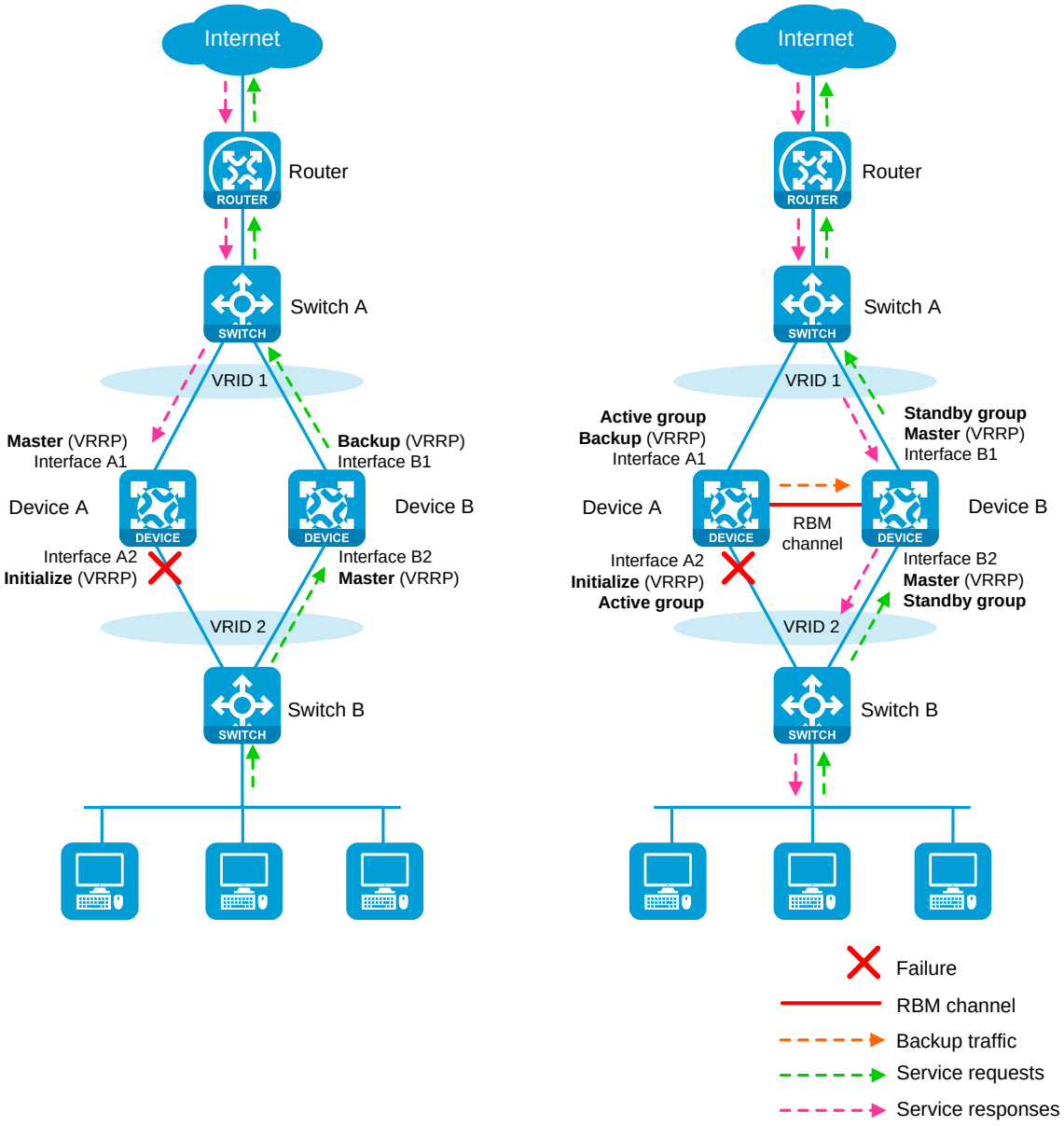
功能简介

在双机热备与 VRRP 联动的组网环境中，双机热备将会控制设备在多个 VRRP 备份组中 Master 和 Backup 状态的统一切换。此功能可以使设备的上下行流量同时切换到新的主设备，保证业务不中断。

此处以主备模式为例，介绍双机热备与 VRRP 的联动组网情况，具体如下。

- 如图-3 的左图所示，在仅有 VRRP 的组网环境中，当 VRRP 链路故障时会导致上、下行 VRRP 备份组中的 Master 设备不是同一台设备，造成流量中断。
- 如图-3 的右图所示，将双机热备和 VRRP 关联后可以解决以上问题。双机热备控制通道建立后，VRRP 备份组内的设备状态将由双机热备决定，VRRP 自身的主备选择机制不再生效。当双机热备的控制通道断开后，VRRP 自身的主备选择机制将会重新生效。

图-3 双机热备联动 VRRP 示意图



VRRP active/standby 组

VRRP active 组和 VRRP standby 组：用于将双机热备与 VRRP 进行关联，实现双机热备对多个 VRRP 备份组状态进行统一管理的目的。

VRRP active/standby 组分别有两种状态：Master 和 Backup。VRRP 成员设备在 VRRP 备份组中的状态与所属 VRRP active/standby 组的状态保持一致。例如，VRRP active 备份组的状态是 Master，则该组中所有设备在 VRRP 备份组中的状态均为 Master。

VRRP active/standby 组初始状态的实现机制如下：

- 主备模式下：主管理设备上 VRRP active 组和 VRRP standby 组的初始状态均为 Master；从管理设备上 VRRP active 组和 VRRP standby 组的初始状态均为 Backup。
- 双主模式下：此种模式下 VRRP active/standby 组的状态与主从管理设备角色无关，VRRP active 组的初始状态为 Master；VRRP standby 组的初始状态均为 Backup。

双机热备联动 VRRP 组网中 Master 设备的选举机制

如图-3 的右图所示，将双机热备与 VRRP 关联成功后，VRRP 备份组中 Master/Backup 状态的变化机制如下：

1. 正常情况下，Device A（假设其是主管理设备）上 VRRP active 组的状态是 Master，所以 Device A 在 VRRP 备份组 1 和 VRRP 备份组 2 中的状态是 Master 设备。Device B（假设其是从管理设备）上 VRRP standby 组的状态是 Backup，所以 Device B 在 VRRP 备份组 1 和 VRRP 备份组 2 中的状态是 Backup。
2. 当 Device A 的下行接口 Interface A2 故障后，双机热备会收到接口故障事件。然后双机热备发送 VRRP active/standby 组状态信息变更报文给 Device B，通知 Device B 将其 VRRP standby 组的状态变更为 Master。

3. Device B 收到 VRRP active/standby 组状态信息变更报文后，会将自身 VRRP standby 组的状态变更为 Master，同时将 Device B 在 VRRP 备份组 1 和 VRRP 备份组 2 中的状态变为 Master。变更完成后给 Device A 发送应答报文。

4. Device A 收到 Device B 的 VRRP standby 组状态变更成功应答报文后，将自己 VRRP active 组的状态变更为 Backup，同时将 Device A 在 VRRP 备份组 1 和 VRRP 备份组 2 中的状态变更为 Backup。

当 Device A 的下行接口 Interface A2 故障恢复后，流量会进行回切，VRRP 备份组中 Master/Backup 状态的变化与接口故障时的变化过程类似，不再重复介绍。

VRRP 中的 ARP 学习

当 VRRP 备份组中的设备接收到虚拟 IP 地址的 ARP 请求报文后，只能由 Master 设备使用 VRRP 备份组的虚拟 MAC 地址响应此 ARP 请求，与此同时 ARP 报文传输路径上的二层设备也就学习到了此虚拟 MAC 地址的 MAC 地址表项。

双机热备联动虚拟地址

功能简介

在云场景中往往存在众多的租户，每个租户都需要具有独立的网络（IP 地址）。传统双机热备联动 VRRP 的可靠性方式每一组 VRRP 备份组都需要三个 IP 地址，这种可靠性方式在云场景下会出现 IP 地址不够用的情况。这时，使用双机热备联动虚拟地址方式可以有效解决以上问题。

双机热备联动虚拟地址功能是指，在两台设备的相同编号的业务接口上配置虚拟 IP 地址（也叫浮动 IP 地址）后，这些业务接口上的虚拟地址将与 RBM 进行关联，并受 RBM 的统一管理和控制。具体为，双机热备的业务主设备将会使用业务接口的虚拟 IP 地址和虚拟 MAC 地址响应 ARP 请求，但是，双机热备的业务备设备将不会进行 ARP 请求的应答。这样就可以保证上下行流量始终都可以被引流到双机热备的业务主设备进行业务处理。

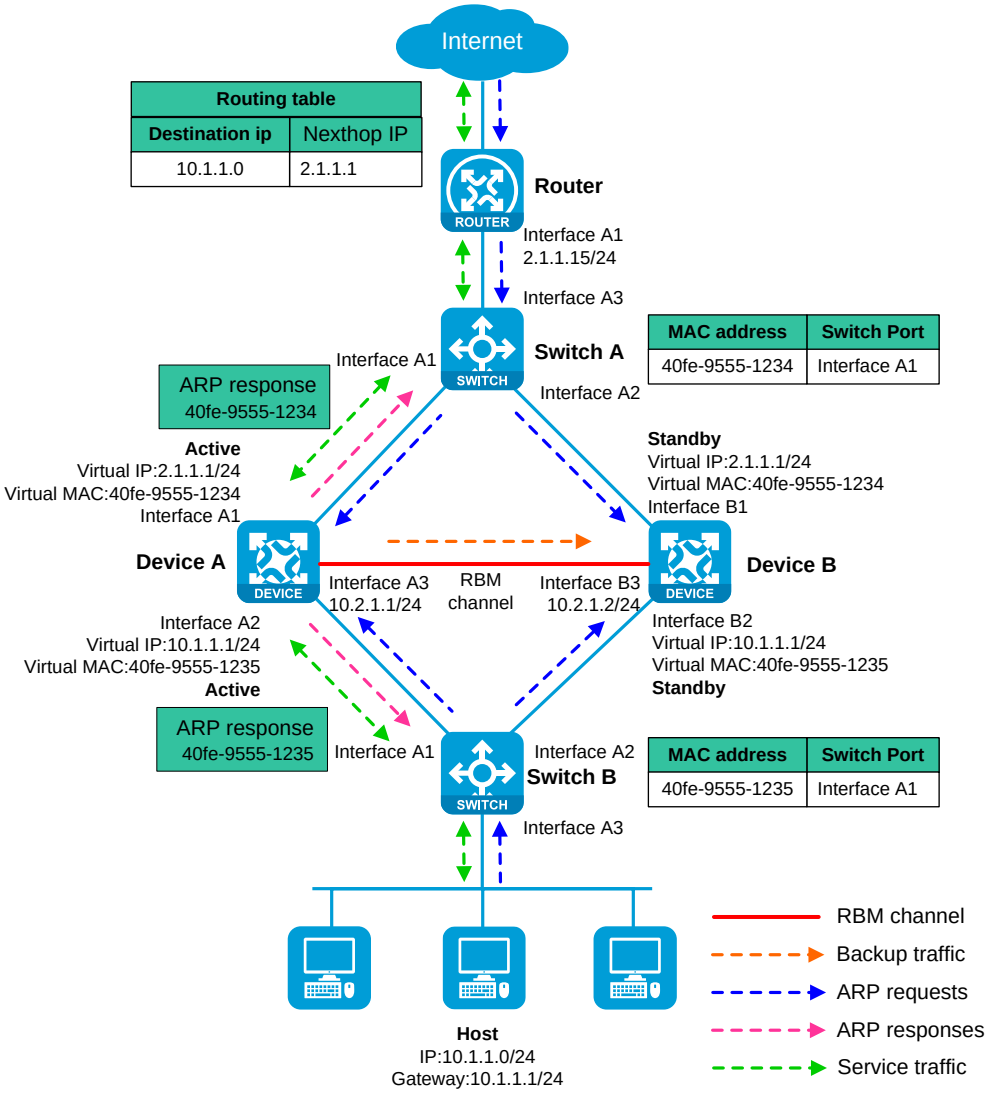
在双机热备组网环境中，当两台设备的相同编号的业务接口上配置虚拟 IP 地址（也叫浮动 IP 地址）时，这些业务接口上的虚拟地址将与 RBM 进行关联，并受 RBM 的统一管理和控制。

运行机制

如图-4 所示，双机热备联动虚拟地址后，内网访问外网的报文被处理的流程如下：

1. 当内网 Host 访问外网时，在 Host 发送业务请求报文前，首先会广播 ARP 请求报文，学习网关虚拟 IP 地址 10.1.1.1 对应的 MAC 地址。
2. 当 Device A 和 Device B 接收到此 ARP 请求报文后，只有双机热备中的业务主设备（Device A）使用业务接口的虚拟 MAC 地址响应此 ARP 请求给 Host。
3. 在此 ARP 学习过程中，中间的交换机 Switch B 也学习到了有关此虚拟 MAC 的 MAC 地址表项，用于指导后续报文的转发。
4. 最后，Host 只会收到双机热备中的业务主设备（Device A）响应的 ARP 报文，Host 就会以学习到的此虚拟 MAC 地址来封装报文，将报文送到 Device A，从而可以保证业务的正常运行。
5. 来自外网的响应报文在整个网络中的处理过程与上面所描述的过程相同，此处不再赘述。

图-4 双机热备联动虚拟地址示意图



双机热备联动路由

功能简介

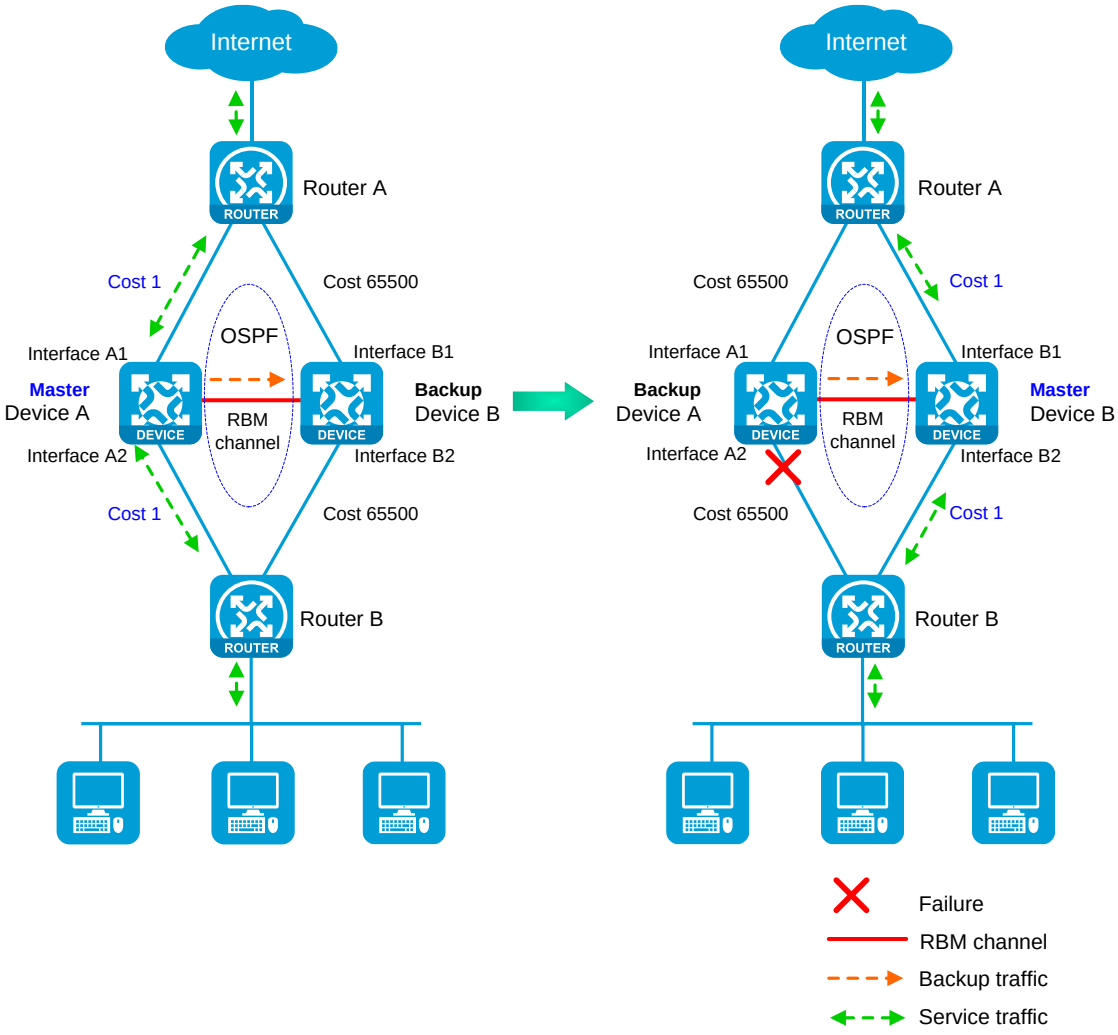
在双机热备与动态路由联动的组网环境中，双机热备将会调整备设备上动态路由协议对外通告的链路开销值。这样可以保证主备切换时使设备的上下行流量同时切换到新的主设备，保证业务不中断。

此组网环境中双机热备必须关联 Track 项，否则，上下行链路或者接口故障双机热备不能进行主备切换。

此处以双机热备联动 OSPF 为例，介绍双机热备与动态路由的联动情况，具体如下。

- 如图-5 左图所示，正常情况下，Device A（主设备）按照 OSPF 的配置正常通告链路开销值（如 1），而 Device B（备设备）通告的链路开销值是被双机热备调整后的值（如 65500）。这样可以使内外网之间的流量走 Device A 转发。
- 如图-5 右图所示，当 Device A 的下行接口 Interface A2 故障后，Device A 和 Device B 将进行主备切换。之后，Device B（主设备）按照 OSPF 的配置正常通告链路开销值（如 1），而 Device A（备设备）通告的链路开销值是被双机热备调整后的值（如 65500）。这样可以使内外网之间的流量走 Device B 转发。

图-5 双机热备联动路由示意图



运行机制

双机热备调整备设备上动态路由协议开销值有如下两种方式：

- 绝对值方式：设备将使用配置的绝对值对外通告。
- 增量值方式：设备将在原有开销值上增加配置的增量值后对外通告。

此功能仅调整备设备上动态路由协议对外通告的开销值，对主设备没有影响。

需要在主备设备上同时开启此功能，并设置相同的参数。

双机热备透明组网

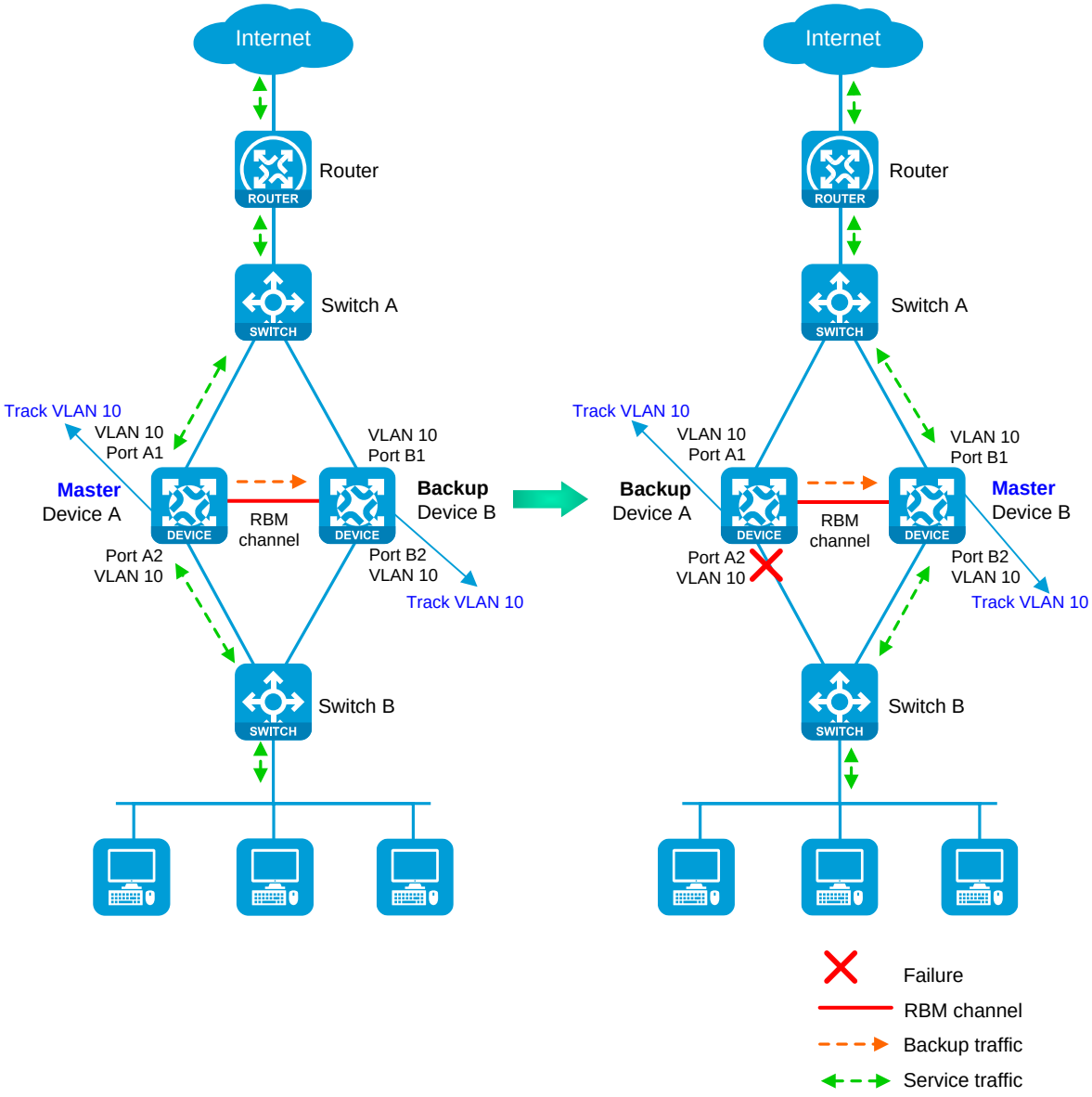
在双机热备透明组网环境中，可通过双机热备的监控接口或监控 VLAN 功能将上下行接口的状态进行联动。当其中一个接口故障后，另一个接口也会失去报文转发能力，从而使设备的上下行流量同时切换到新的主设备，保证业务不中断。

双机热备的监控接口或监控 VLAN 功能可以保证所监控对象之间的状态相互联动、保持一致，使其同时具备或同时不具备报文转发能力。

此处以双机热备监控 VLAN 功能为例，介绍双机热备透明组网的情况，具体如下。

- 如图-6 左图所示，正常情况下，Device A（主设备）上双机热备将监控的 VLAN10 设置为 Active 状态，Device B（备设备）上双机热备将监控的 VLAN10 设置为 Inactive 状态。这样可以使内外网之间的流量走 Device A 转发。
- 如图-6 右图所示，当 Device A 的下行接口 Port A2 故障后，Device A 和 Device B 将进行主备切换。之后，Device B（主设备）上双机热备将监控的 VLAN10 设置为 Active 状态，而 Device A（备设备）上双机热备将监控的 VLAN10 设置为 Inactive 状态。这样可以使内外网之间的流量走 Device B 转发。

图-6 双机热备透明组网示意图



vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

硬件环境一致

部署双机热备前，请先保证主/备设备硬件环境的一致性，具体要求如下：

- 主/备设备的型号必须一致。
- 主/备设备接口板的位置、数量和类型必须一致。
- 主/备设备上管理接口、业务接口、RBM 通道接口需要分别使用相互独立的接口，且所使用的接口编号和类型必须一致。
- 主/备设备上硬盘的位置、数量和类型建议一致。未安装硬盘的设备日志存储量将远低于安装了硬盘的设备，而且部分日志和报表功能不可用。

软件环境一致

部署双机热备前，请先保证主/备设备软件环境的一致性，具体要求如下：

- 主/备设备的系统软件环境及其版本必须一致，如：Boot包、System包、Feature包和补丁包等。
- 主/备设备上被授权的特征库和特性环境必须一致，如：特征库的种类，每类特征库的版本、授权时间范围、授权的资源数等。

- 主/备设备上的资源文件必须一致，比如：公钥信息、ISP 地址库文件等。
- 主/备设备的接口编号必须一致。
- 主/备设备的系统时间一致。
- 主/备设备之间建立 RBM 通道的接口类型、速率和编号等信息必须一致，推荐使用聚合接口。
- 主/备设备上聚合接口的编号、成员接口编号必须一致。
- 主/备设备相同位置的接口必须加入到相同的安全域。
- 主/备设备的 HASH 选择 CPU 模式以及 HASH 因子都必须相同。

双机热备注意事项

- 双机热备仅支持与 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。
- 监控 VLAN 与监控接口两个功能互斥，不可同时配置；监控接口与联动 Track 项目两个功能可以同时配置，但是两者监控的接口不能相同；监控接口与联动 VRRP 两个功能可以同时配置，但是两者配置的接口不能相同。
- 数据通道接口中的 IP 地址与对端接口的 IP 地址不能相同。
- 数据通道接口的 IPv4 地址和 IPv6 地址可以同时配置，设备会基于控制通道的本端 IP 地址类型获取数据通道接口中的 IP 地址，并与对端进行连接。
- 部分双机热备功能仅支持以 CLI 方式进行配置，不支持在 Web 界面上配置，具体支持情况请以设备实际 Web 界面为准。

镜像模式注意事项

- 请使用初始状态（未配置双机热备工作模式）的两台设备组成镜像模式双机热备。如果设备已在运行业务，请勿直接将非镜像模式切换成镜像模式，必须将设备恢复到初始状态后再切换成镜像模式，否则有可能会导致业务异常。
- 基于镜像模式实现双机热备时，两台设备上编号相同的接口使用相同的 IP 地址。此处的接口是指除镜像模式管理接口和 RBM 通道接口以外的接口。
- 基于镜像模式实现 IPv6 双机热备时，两台设备上编号相同的业务接口使用相同的 IPv6 地址和 IPv6 链路本地地址。请手工配置 IPv6 链路本地地址，不要为接口配置自动生成的链路本地地址，以免产生不一致。
- 镜像模式下，双机热备无法联动 VRRP 或虚地址。如果设备上有 VRRP 或虚地址配置，则不能启用镜像模式。启用镜像模式后，设备上不能再进行 VRRP 或虚地址配置。
- 启用镜像模式后，两台设备之间支持备份的配置增多。例如，接口 IP 地址配置命令在未启用镜像模式时不支持备份，启用镜像模式后支持备份。有关镜像模式具体支持哪些业务模块的配置信息同步，请参见配置信息备份小节中的详细介绍。
- 启用镜像模式后，设备能根据业务运行角色调整业务接口的状态。主设备上的业务接口正常收发报文，备设备上的业务接口只能收发三层以下的报文，如 LLDP、LACP 等。
- 设备与上下行设备之间的路由仅支持静态路由，不支持动态路由和智能选路。以动态路由为例，因为镜像模式下的备设备不会发送和接收路由协商报文，与上下行设备的动态路由邻居关系无法建立。主备切换时，新的主用设备需要和上下行设备重新协商路由，这将导致主备切换时业

务中断时间较长。因此，在两台设备的业务接口工作在三层、上下行连接路由器、与路由器之间运行动态路由协议的组网下，不支持使用镜像模式双机热备。

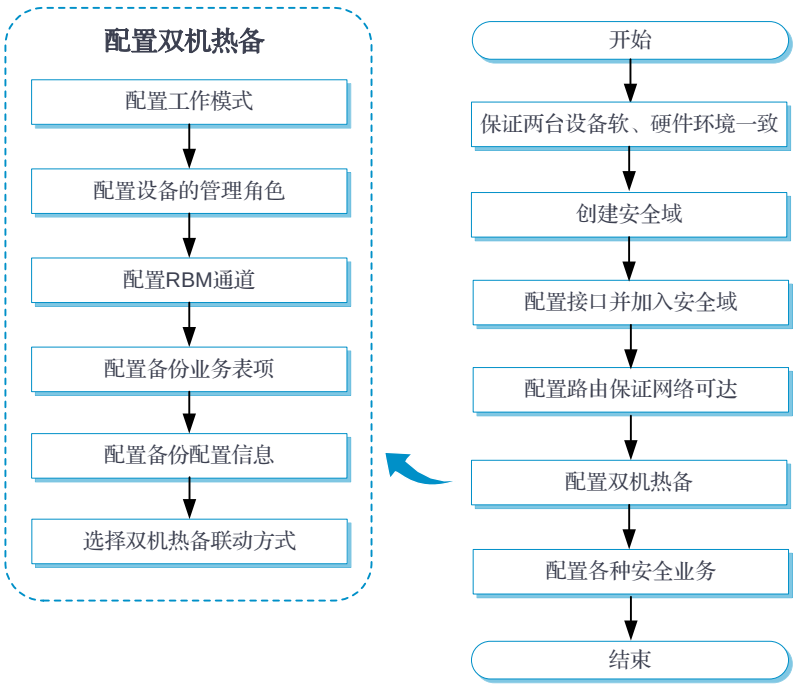
- 未配置控制通道或设备的管理角色时，无法配置 RBM 运行模式为镜像模式。

配置指南

配置思路

双机热备功能的配置思路如下图所示：

图-7 双机热备配置思路图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置主备模式双机热备

主备模式下，正常情况仅由主设备处理业务，备设备处于待命状态；当主设备接口、链路或整机故障时，备设备立即切换为主设备，接替原主设备处理业务。

双机热备配置

1. 选择“系统 > 高可靠性 > 双机热备”。
2. 在“双机热备”页面单击<配置>按钮，进入“配置双机热备”页面，配置 RBM 运行模式为主备模式。
3. 配置双机热备，具体配置内容如下所示：

表-2 双机热备配置参数表

参数	说明
双机热备开关	双机热备开关包括两种状态：开启和关闭
管理角色	双机热备中的设备分为主、从两种管理角色，用于控制设备之间关键配置信息只能从“主管理设备”同步到“从管理设备”，并覆盖从管理设备息。双机热备系统中只能有一台设备为主管理设备，另一台为从管理设备，自动选择时，两台设备的角色模式都应设置为自动选择 双机热备中设备的管理角色有手动配置和自动选择两种方式，具体内容如下 • 手工配置：此方式需要手工指定设备的管理角色，可指定为主、从两种旦指定后设备的管理角色将固定不变。如需更改，则需要在“配置双机工更改。此方式适用于设备上有独立管理接口的网络环境，此方式仅支的主备和双主工作模式下使用，不能在镜像工作模式下使用 • 自动选举：此方式下设备的管理角色根据运行角色自动选择，并跟随运换。管理角色与运行角色始终保持一致，即运行主是主管理设备，运行备。此方式适用于设备上使用业务接口作为管理接口的网络环境，此方机热备的主备和镜像运行模式下使用，双主运行模式中不能使用。在此可在“双机热备”页面的运行管理角色处查看设备当前实际运行的管理设备还是从管理设备
控制通道本端IP地址	配置用于建立控制通道的本端IP地址，Server端将使用此Local IP提供TCP IPv4和IPv6两种类型，但不能同时配置 本端IP地址与对端IP地址不能相同
控制通道对端IP地址	配置用于建立控制通道的对端IP地址。支持IPv4和IPv6两种类型，但不能同 本端IP地址与对端IP地址不能相同
对端端口号	配置用于建立控制通道的对端端口号，在主备设备上配置的对端端口号必须
管理接口	配置用于连接网关设备或日志主机的镜像模式管理接口，镜像模式管理接口

	不会进行同步 仅镜像模式下支持配置
数据通道	主/备设备使用此功能配置的接口建立双机热备的数据通道，此数据通道仅 间的热备报文和透传报文，不用于传输主/备设备之间的其他报文，支持中 机，但不可以跨越三层设备
心跳间隔	双机热备通道建立后，设备会以配置的心跳间隔为周期向对端设备 Keepalive报文，以探测双机热备通道的连通性
心跳失效阈值	双机热备通道建立后，如果设备发送Keepalive报文的次数达到心跳失效阈 到对端的回应，则双机热备通道断开，双机热备失效
主动抢占	双机热备组网中的主设备发生故障后，流量自动切换到对端设备。开启此 的主设备再次恢复为主设备后，流量会回切
流量回切延迟时间	由于业务表项在主/备设备之间进行备份需要一定的时间。为了保证业务能 以需要延迟流量的回切
备份会话表项	开启此功能后，主设备会将其生成的业务表项实时备份到备设备，当主设 设备可以平滑地接替主设备的工作，保证业务不中断
备份HTTP协议 备份DNS协议	配置此功能后，设备将会把DNS协议或HTTP协议报文触发创建的会话表 设备 除了DNS和HTTP应用协议，其它应用协议创建的会话不受本功能控制， 备业务表项功能处于开启状态，就会进行这些会话表项备份 此功能的应用场景建议如下： • 在非对称路径的双机热备网络环境中，需要开启此功能，以保证同一 报文在两台设备上能够被正常处理 • 在双机热备主备模式、镜像模式或对称路径的双机热备网络环境中， 可减少设备性能的消耗；但是设备间流量平滑的时效性将受到一些影 理员根据实际业务情况来判断是否需要关闭此功能。因为对于 DNS 和 用协议，通常在很少的报文交互之后就会断开连接，当发生主备切换

	断时，客户端会立即重新发起请求，用户通常感知不到连接异常。所以 个协议触发创建会话的备份功能
备份保持上一跳	当主设备在接口上开启保持上一跳功能，并全局开启备份保持上一跳功能后 到正向流量的第一个IP报文时，会保存上一跳信息，同时将该上一跳信息备 当反向流量报文到达主设备或从设备上进行转发时，可以直接通过该上一跳 进行转发。本功能不同设备的支持情况不同，请以设备Web页面的实际支持
配置信息一致性检查	此功能用于检测双机热备状态下的两台设备的配置信息是否一致，用于防止 配置信息不一致，导致主备切换后业务不通的情况。当配置信息不一致时， 息，以提示管理员进行配置信息的手动同步
配置信息一致性检查模式	设置配置信息一致性检查的模式，当前可配置的模式如下： • 固定时间间隔：每隔一段时间进行一次配置信息一致性检查 • 每天：每天的一个固定时间进行一次配置信息一致性检查 • 每周：每周的一个固定时间进行一次配置信息一致性检查
自动同步配置信息	开启此功能前，主管理设备上已经配置信息，将会在开启此功能后进行一次 后新增的配置信息将实时备份到从管理设备 配置信息很多时，批量备份时间会很长可能需要一到两个小时。因此在初始 时，建议先开启此功能，以减少后面配置信息进行批量备份的时间
自动同步静态路由	本功能仅需要在双机热备的镜像模式或双机热备+虚拟IP地址引流的组网场 双机热备组网场景中请勿开启本功能 开启本功能后，当双机热备的主管理设备向从管理设备自动或者手工同步配 将设备上已配置的静态路由同步到从管理设备。此时会出现以下两种情况： • 当开启配置信息自动备份功能后开启本功能时，后续新增的静态路由可 步，之前的需要通过手工同步配置信息功能进行手工批量备份； • 当开启本功能后开启配置信息自动备份功能时，设备会将已配置的所有 到从管理设备。

4. （可选）在“配置双机热备”页面中监控对象处配置双机热备联动 Track 项，具体配置内容如下所示：

表-3 双机热备联动 Track 项配置参数表

参数	说明
联动Track项	配置此功能后，当双机热备联动的其中一个Track项的状态为Negative状态 进行设备的主备切换，将上下行流量同时切换到新的主设备，保证业务不中

5. 在“配置双机热备”页面，单击<确定>按钮完成双机热备的配置。

配置双机热备联动 VRRP

请在 VRRP 中将 VRRP 与高可靠性关联，具体配置步骤，请参见“VRRP”中的详细介绍。

配置双机热备联动虚拟地址

此组网环境中 RBM 必须关联 Track 项，否则上下行链路或接口故障时，双机热备不能主备切换。

双机热备联动虚拟地址的具体配置步骤如下：

1. 选择“网络 > 接口与 VRF > 接口”，进入“接口配置”页面。
2. 在“接口配置”页面选择需要联动双机热备的业务接口，单击<编辑>按钮，进入“修改接口设置”页面。

3. 在“修改接口设置”页面的 IPv4/IPv6 地址页签勾选“虚拟 IP”后，这些业务接口上的虚拟地址将与 RBM 进行关联，并受 RBM 的统一管理和控制。

配置双机热备联动路由

此组网环境中 RBM 必须关联 Track 项，否则上下行链路或接口故障时，双机热备不能主备切换。

双机热备联动路由的具体配置步骤如下：

1. 选择“系统 > 高可靠性 > 双机热备”。
2. 在“双机热备”页面单击<配置>按钮，进入“配置双机热备”页面，配置双机热备的路由联动功能，具体配置内容如下所示：

表-4 双机热备联动路由的配置参数表

参数	说明
OSPF	表示双机热备调整备设备上OSPF协议的开销值
IS-IS	表示双机热备调整备设备上IS-IS协议的开销值
BGP	表示双机热备调整备设备上BGP协议的开销值
OSPFv3	表示双机热备调整备设备上OSPFv3协议的开销值
调整cost绝对值	表示备设备以绝对值的形式对外通告动态路由协议的开销值，即设备直接对值
调整cost增量值	表示备设备以增量值的形式对外通告动态路由协议的开销值，即设备在原有此增量值后对外通告

3. 在“配置双机热备”页面，单击<确定>按钮完成双机热备的配置。

配置双机热备透明组网

双机热备透明组网的具体配置步骤如下：

1. 选择“系统 > 高可靠性 > 双机热备”。

2. 在“双机热备”页面单击<配置>按钮，进入“配置双机热备”页面，在监控对象处配置双机热备透明组网的相关配置，具体配置内容如下所示：

表-5 双机热备透明组网的配置参数表

参数	说明
接口	配置此功能后，双机热备监控的所有接口的状态将相互联动并保持一致，这 都具备或都不具备报文传输能力。只有双机热备监控接口的状态均为UP时 转发报文。否则，双机热备监控的所有接口均不能转发报文 使用监控接口功能时，不能监控聚合接口的成员接口
VLAN	配置此功能后，双机热备会监控VLAN成员端口的状态，并将成员端口的 保持一致，此VLAN中的成员端口将同时都具备或都不具备报文传输能力。 成员端口状态均为UP时，此VLAN的成员端口才能转发报文。否则，此VL 端口均不能转发报文 基于以上双机热备监控VLAN的运行原理，请勿配置监控 VLAN 1。因为设备 端口缺省都属于VLAN 1，所以当VLAN 1中有端口未被使用时其接口状态为 会导致VLAN 1中正常使用的端口无法转发报文

3. 在“配置双机热备”页面，单击<确定>按钮完成双机热备透明组网的配置。

配置双主模式双机热备

双主模式下，两台设备同时处理业务，充分利用设备资源，提高系统负载能力，此模式通过互为主备方法实现。并且当其中一台设备发生故障时，另外一台设备会立即承担其业务，保证业务不中断。

双机热备配置

1. 选择“系统 > 高可靠性 > 双机热备”。
2. 在“双机热备”页面单击<配置>按钮，进入“配置双机热备”页面，配置 RBM 运行模式为双主模式。
3. 配置双机热备，具体配置内容请参见“双机热备配置”章节。
4. （可选）在“配置双机热备”页面中监控对象处配置双机热备联动 Track 项，具体配置内容请参见“双机热备配置”中配置双机热备联动 Track 项内容。
5. 在“配置双机热备”页面，单击<确定>按钮完成双机热备的配置。

配置双机热备联动 VRRP

请在 VRRP 中将 VRRP 与高可靠性关联，具体配置步骤，请参见“VRRP”中的详细介绍。

配置双机热备联动路由

此组网环境中 RBM 必须关联 Track 项，否则上下行链路或接口故障时，双机热备不能主备切换。

双机热备联动路由的具体配置请参见“配置双机热备联动路由”章节。

配置双机热备透明组网

双机热备透明组网的具体配置请参见“配置双机热备透明组网”章节。

配置镜像模式双机热备

镜像模式是一种特殊的主备模式，部署方式与主备模式相同。在镜像模式下，两台设备的接口（镜像模式管理接口和 RBM 通道接口除外）使用相同的 IP 地址，正常情况下同样由主设备处理业务，备设备处于待命状态；当主设备接口、链路或整机故障时，备设备立即切换为主设备，接替原主设备处理业务。

此组网环境中 RBM 必须关联 Track 项，否则上下行链路或接口故障时，双机热备不能主备切换。

具体配置步骤如下：

1. 选择“系统 > 高可靠性 > 双机热备”。
2. 在“双机热备”页面单击<配置>按钮，进入“配置双机热备”页面，配置 RBM 运行模式为镜像模式。
3. 配置双机热备，具体配置内容请参见“双机热备配置”章节。

4. 在“配置双机热备”页面中监控对象处配置双机热备联动 Track 项，具体配置内容请参见“双机热备配置”中配置双机热备联动 Track 项内容。

5. 在“配置双机热备”页面，单击<确定>按钮完成镜像模式双机热备的配置。

双机热备高级功能

1. 在“双机热备”页面，单击<手工一致性检查>按钮或<手工同步配置信息>按钮，可以进行手工检查配置信息的一致性和同步配置信息。

表-6 手工检查配置信息的一致性和同步配置信息

参数	说明
手工一致性检查	当需要确认主从管理设备上配置信息是否一致时，可以通过单击此按钮即时一致性检查。若配置信息不一致，则系统会发送日志信息，以提示管理员进手动同步
手工同步配置信息	单击此按钮后，主管理设备上的配置信息将同步到从管理设备

2. 在“双机热备”页面，可以手工进行主备业务状态切换。管理员可通过本功能触发主备倒换或其中一台设备的升主、降备，引导业务流量切换到相应的主设备上，以便更换备设备上的部件或升级软件等。在双机热备联动 VRRP 的组网环境中，当使用此功能进行主备运行状态倒换时，可能会导致短暂的 VRRP 虚拟 IP 地址冲突，属于正常现象。本功能的参数支持情况与 RBM 运行模式有关，请以页面实际情况为准。

表-7 手工进行主备业务状态切换

参数	说明
状态切换	当双机热备中主备设备无故障，可通过此按钮触发主备倒换，将业务切换到行处理，以便管理员可以更换主设备上的部件或升级软件等 在主备和镜像组网中，在主设备或备设备上执行本功能均会触发主备倒换
将对端升为运行主	在双主组网中，正常情况下两台设备均为主设备，可在其中一台设备上执行为备设备，另外一台设备仍为主设备
将对端降为运行备	在双主组网中，正常情况下两台设备均为主设备，可在其中一台设备上执行持不变仍为主设备，另外一台设备将自动成为备设备
重置	在主设备或备设备上执行本功能均会触发RBM对设备的业务角色进行重新

VRRP

本帮助主要介绍以下内容：

- 特性简介
  - VRRP 备份组
  - 联动双机热备
  - 备份组的虚拟 IP 地址
  - 备份组中设备的优先级
  - 备份组中设备的抢占/非抢占方式
  - VRRP 通告报文发送间隔
  - 备份组中设备的认证方式
  - VRRP 控制 VLAN
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - VRRP 基本配置
  - VRRP 高级配置

特性简介

在具有组播或广播能力的局域网(如以太网)中,借助 VRRP(Virtual Router Redundancy Protocol,虚拟路由器冗余协议)能在某台设备出现故障时仍然提供高可靠的链路,有效避免单一链路发生故障后网络中断的问题。

VRRP 将可以承担网关功能的一组设备加入到备份组中,形成一台虚拟设备。VRRP 通过选举机制决定哪台设备承担转发任务,局域网内的主机只需将虚拟设备配置为默认网关即可。因此,VRRP 在提高可靠性的同时,简化了主机的配置。

VRRP 备份组

VRRP 将局域网内可以承担网关功能的一组设备划分在一起,组成一个备份组。备份组由一台 Master 设备和多台 Backup 设备组成,对外相当于一台虚拟设备。

联动双机热备

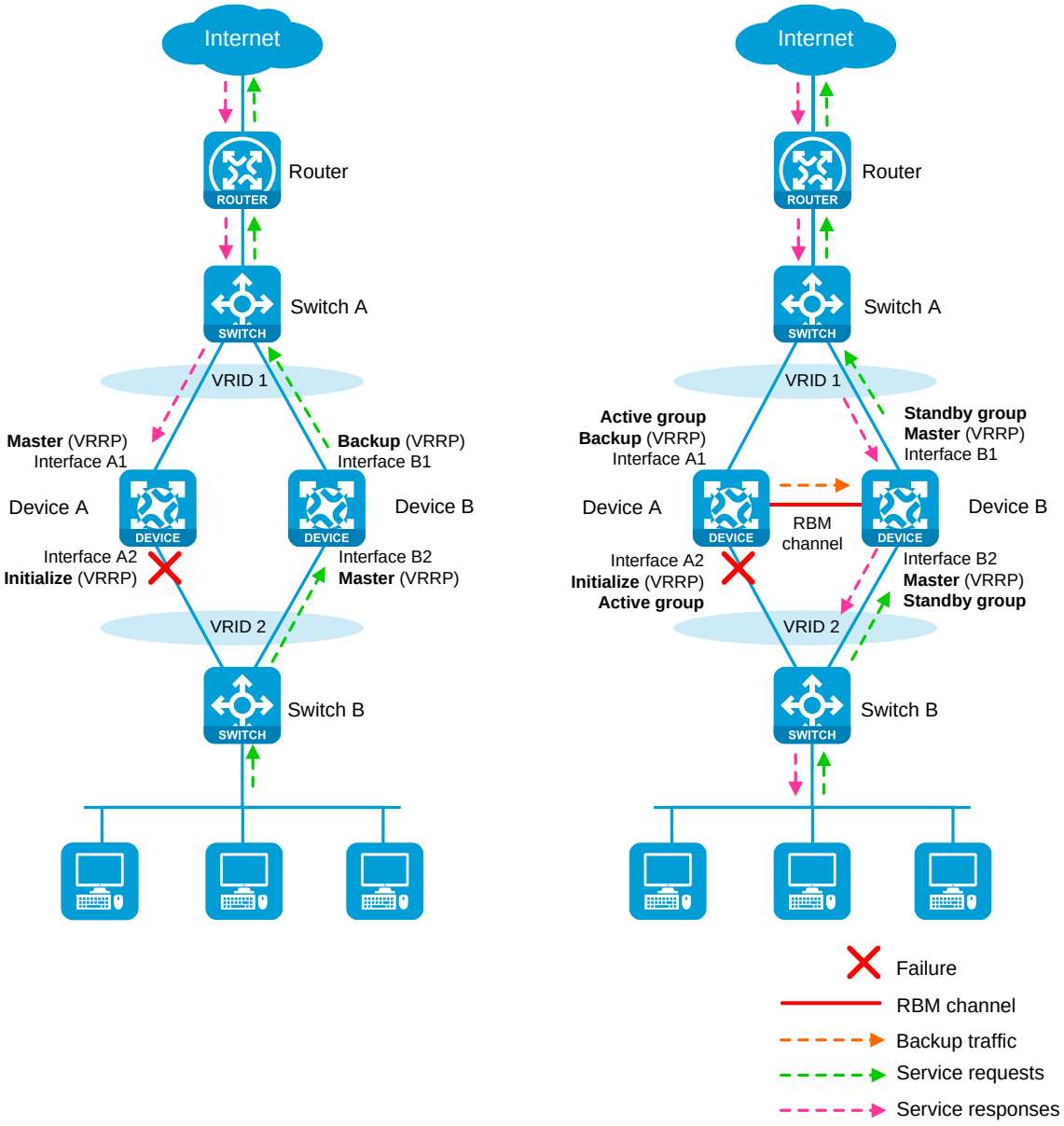
简介

如图-1 的左图所示,在仅有 VRRP 的组网环境中,当 VRRP 链路故障时会导致上、下行 VRRP 备份组中的 Master 设备不是同一台设备,造成流量中断。如图-1 的右图所示,将双机热备和 VRRP

关联，使用双机热备功能管理设备在 VRRP 备份组中的 Master 和 Backup 状态的统一切换，可以解决以上问题。

创建 VRRP 备份组时，通过把设备加入 VRRP active 组和 VRRP standby 组可以实现将 VRRP 与双机热备进行关联。当 RBM 的控制通道建立后，VRRP 备份组内的设备状态将由双机热备决定，VRRP 自身的主备选择机制不再生效；当 RBM 的控制通道断开后，VRRP 自身的主备选择机制将会重新生效。RBM 的控制通道建立后，联动双机热备的 VRRP 备份组优先级将由双机热备决定。此时，Master 状态的 VRRP 备份组优先级为 255，Backup 状态的 VRRP 备份组优先级为 100。

图-1 双机热备管理 VRRP 备份组示意图



VRRP active/standby 组

VRRP active/standby 组分别有两种状态：Master 和 Backup。VRRP 成员设备在 VRRP 备份组中的状态与所属 VRRP active/standby 组的状态保持一致。例如，VRRP active 备份组的状态是 Master，则该组中所有设备在 VRRP 备份组中的状态均为 Master。

VRRP active/standby 组初始状态的实现机制如下：

- 主备模式下：主管理设备上 VRRP active 组和 VRRP standby 组的初始状态均为 Master；从管理设备上 VRRP active 组和 VRRP standby 组的初始状态均为 Backup。
- 双主模式下：此种模式下 VRRP active/standby 组的状态与主从管理设备角色无关，VRRP active 组的初始状态为 Master；VRRP standby 组的初始状态均为 Backup。

VRRP 在双机热备环境中 Master 设备的选举机制

如图-1 的右图所示，将双机热备与 VRRP 成功关联后，VRRP 备份组中 Master/Backup 状态的变化机制如下：

1. 正常情况下，Device A（假设其是主管理设备）上 VRRP active 组的状态是 Master，所以 Device A 在 VRRP 备份组 1 和 VRRP 备份组 2 中的状态是 Master 设备。Device B（假设其是从管理设备）上 VRRP standby 组的状态是 Backup，所以 Device B 在 VRRP 备份组 1 和 VRRP 备份组 2 中的状态是 Backup 设备。

2. 当 Device A 的下行接口 Interface A2 故障后，双机热备会收到接口故障事件。然后双机热备发送 VRRP active/standby 组状态信息变更报文给 Device B，通知 Device B 将其 VRRP standby 组的状态变更为 Master。

3. Device B 收到 VRRP active/standby 组状态信息变更报文后，会将自身 VRRP standby 组的状态变更为 Master，同时将 Device B 在 VRRP 备份组 1 和 VRRP 备份组 2 中的状态变为 Master 设备。变更完成后给 Device A 发送应答报文。

4. Device A 收到 Device B 的 VRRP standby 组状态变更成功应答报文后，将自己 VRRP active 组的状态变更为 Backup，同时将 Device A 在 VRRP 备份组 1 和 VRRP 备份组 2 中的状态变更为 Backup。

当 Device A 的下行接口 Interface A2 故障恢复后，流量会进行回切，VRRP 备份组中 Master/Backup 状态的变化与接口故障时的变化过程类似，不再重复介绍。

备份组的虚拟 IP 地址

备份组具有 IP 地址，称为虚拟 IP 地址。局域网内的主机仅需要知道这台虚拟设备的 IP 地址，并将其设置为网关的 IP 地址即可。局域网内的主机通过这台虚拟设备与外部网络进行通信。

虚拟设备的 IP 地址可以是备份组所在网段中未被分配的 IP 地址，也可以和备份组内的某个设备的接口 IP 地址相同。接口 IP 地址与虚拟 IP 地址相同的设备被称为 IP 地址拥有者。

备份组中设备的优先级

VRRP 根据优先级来确定备份组中每台设备的角色（Master 设备或 Backup 设备）。优先级越高，则越有可能成为 Master 设备。

VRRP 优先级的取值范围为 0 到 255（数值越大表明优先级越高），可配置的范围是 1 到 254，优先级 0 为系统保留给特殊用途来使用，255 则是系统保留给 IP 地址拥有者。当设备为 IP 地址拥有者时，其优先级始终为 255。因此，当备份组内存在 IP 地址拥有者时，只要其工作正常，则为 Master 设备。在同一个 VRRP 备份组中，只能存在一个 IP 地址拥有者。

备份组中设备的抢占/非抢占方式

备份组中的设备具有以下两种方式：

- 抢占方式：在该方式下 Backup 设备一旦发现自己的优先级比当前 Master 设备的优先级高，就会触发 Master 设备的重新选举，并最终取代原有的 Master 设备。抢占方式可以确保承担转发任务的 Master 设备始终是备份组中优先级最高的设备。
- 非抢占方式：在该方式下只要 Master 设备没有出现故障，Backup 设备即使随后被配置了更高的优先级也不会成为 Master 设备。非抢占方式可以避免频繁地切换 Master 设备。

在抢占方式下，为了避免备份组内的成员频繁进行主备状态转换，让 Backup 设备有足够的时间搜集必要的信息（如路由信息），Backup 设备接收到优先级低于本地优先级的通告报文后，不会立即抢占成为 Master 设备，而是等待抢占延迟时间后，才会重新选举新的 Master 设备。

延迟时间

Backup 设备抢占成为 Master 设备时，需要等待指定延迟时间后，才会抢占为 Master 设备。0 表示立刻抢占为 Master 设备。

VRRP 通告报文发送间隔

VRRP 备份组中的 Master 设备会定时发送 VRRP 通告报文，通知备份组内的设备自己工作正常。需要注意的是：

- 建议配置 VRRP 通告报文的发送间隔大于 100 厘秒，否则会对系统的稳定性产生影响。
- 使用 VRRPv2 版本时，IPv4 VRRP 备份组中的所有设备必须配置相同的 VRRP 通告报文间隔。
- 使用 VRRPv3 版本时，VRRP 备份组中的设备上配置的 VRRP 通告报文间隔可以不同。Master 设备根据自身配置的报文间隔定时发送通告报文，并在通告报文中携带 Master 设备上配置的间隔；Backup 设备接收到 Master 设备发送的通告报文后，记录报文中携带的 Master 设备通告报文间隔，如果在 3×记录的间隔 + Skew_Time 内没有收到 Master 设备发送的 VRRP 通告报文，则认为 Master 设备出现故障，重新选举 Master 设备。
- 网络流量过大可能会导致 Backup 设备在指定时间内没有收到 Master 设备的 VRRP 通告报文，从而发生状态转换。可以通过将 VRRP 通告报文的发送间隔延长的办法来解决该问题。

备份组中设备的认证方式

VRRP 通过在 VRRP 报文中增加认证字的方式，验证接收到的 VRRP 报文，防止非法用户构造报文攻击备份组内的设备。VRRP 提供了三种认证方式：

- 无认证：发送 VRRP 报文的设备与接收报文的设备之间不进行报文合法性认证。
- 简单字符认证：发送 VRRP 报文的设备将认证字填入到 VRRP 报文中，而收到 VRRP 报文的设备会将收到的 VRRP 报文中的认证字和本地配置的认证字进行比较。如果认证字相同，则认为接收到的报文是真实、合法的 VRRP 报文；否则认为接收到的报文是一个非法报文，将其丢弃。
- MD5 认证：发送 VRRP 报文的设备利用认证字和 MD5 算法对 VRRP 报文进行摘要运算，运算结果保存在 VRRP 报文中。收到 VRRP 报文的设备会利用本地配置的认证字和 MD5 算法进行同样的运算，并将运算结果与认证头的内容进行比较。如果相同，则认为接收到的报文是合法的 VRRP 报文；否则认为接收到的报文是一个非法报文，然后将其丢弃。

VRRP 控制 VLAN

缺省情况下，在 Master 的三层以太网子接口上配置模糊 VLAN 终结后，该接口不支持发送广播和组播报文。为了保证 Master 可以周期性地向 Backup 发送 VRRP 通告报文（组播报文），需要在 Master 的三层以太网子接口上启用 VLAN 终结支持广播/组播报文功能。启用该功能后，VRRP 通

告报文将发送给所有终结的 VLAN。三层以太网子接口上模糊终结的 VLAN 较多时，会导致发送的 VRRP 通告报文数量过多，严重影响设备的性能。

配置 VRRP 的控制 VLAN 能够解决上述问题。关闭 VLAN 终结支持广播/组播功能，并配置 VRRP 的控制 VLAN 后，可以使得 Master 设备仅在控制 VLAN 内发送 VRRP 通告报文，避免发送过多的 VRRP 通告报文。

VRRP 的控制 VLAN 分为两种：

- 控制 VLAN：配置了模糊 Dot1q 终结的子接口上，需要指定此类控制 VLAN；
- 内层 VLAN：配置了模糊 QinQ 终结的子接口上，需要指定此类控制 VLAN。

vSystem相关说明

非缺省 VSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- VRRPv3 版本的 IPv4 VRRP 和 IPv6 VRRP 均不支持对 VRRP 报文进行认证。
- 一个接口上的不同备份组可以设置不同的认证方式和认证字；加入同一备份组的设备需要设置相同的认证方式和认证字。
- VRRP 负载均衡模式备份组不支持与双机热备关联。

- 关联双机热备的 VRRP 备份组中不能存在 IP 地址拥有者。

配置指南

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

VRRP 基本配置

VRRP 基本配置的具体配置步骤如下：

1. 选择“系统 > 高可靠性 > VRRP”。
2. 在“VRRP”页面单击<新建>按钮，进入“新建 VRRP 备份组”页面。
3. 新建 VRRP 备份组，具体配置内容如下表所示：

表-1 VRRP 备份组配置参数表

参数	说明
备份组所在的接口	VRRP功能基于接口实现，指定VRRP备份组所属的接口
备份组号	VRRP备份组的编号，是其唯一的标识。不同设备上编号相同的备份组形成 组
类型	支持IPv4和IPv6两种类型
联动双机热备	在双机热备与VRRP配合使用的高可靠性组网中必须配置此功能，使不同VR 进行联动
虚拟IP地址	局域网内的主机使用这个虚拟IP地址作为网关地址与外部网络进行通信
优先级	优先级越高，则越有可能成为Master设备，数值越大优先级越高
抢占模式	支持抢占模式和非抢占模式两种
延迟时间	Backup设备抢占成为Master设备时，需要等待指定延迟时间后，才会抢占 0表示立刻抢占为Master设备
通告报文发送间隔	Master设备根据配置的此时间定时发送VRRP通告报文，通知备份组内的路 正常。使用VRRPv2版本时，该参数的实际生效值只能是100的整倍数，例 取值在10～100、101～200、4001～4095范围内时，实际生效值分别为10 使用VRRPv3版本时，该参数的实际生效值与所配置数值相同

4. 单击<确定>按钮，新建 VRRP 备份组成功。

VRRP 高级配置

VRRP 高级配置的具体配置步骤如下：

1. 选择“系统 > 高可靠性 > VRRP 高级设置”。
2. 在“VRRP 高级设置”页面，单击目标接口右侧的<编辑>按钮，进入“VRRP 高级设置”页面。
3. 在“VRRP 高级设置”页面进行配置，具体配置内容如下表所示：

表-2 VRRP 高级设置配置参数表

参数	说明
接口	VRRP备份组绑定的接口编号
VRRP版本	VRRP包括VRRPv2和VRRPv3两个版本，VRRPv2版本只支持IPv4 VRRP支持IPv4 VRRP和IPv6 VRRP IPv4 VRRP备份组中的所有路由器上配置的IPv4 VRRP版本必须一致
控制VLAN	配置了模糊Dot1q终结的子接口上，需要指定此类控制VLAN
内层VLAN	配置了模糊QinQ终结的子接口上，需要指定此类控制VLAN

4. 单击<确定>按钮，接口的 VRRP 高级设置配置成功。

Track

本帮助主要介绍以下内容：

- 特性简介
  - 联动功能实现机制
  - Track 模块与监测模块联动
  - Track 模块与应用模块联动
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南

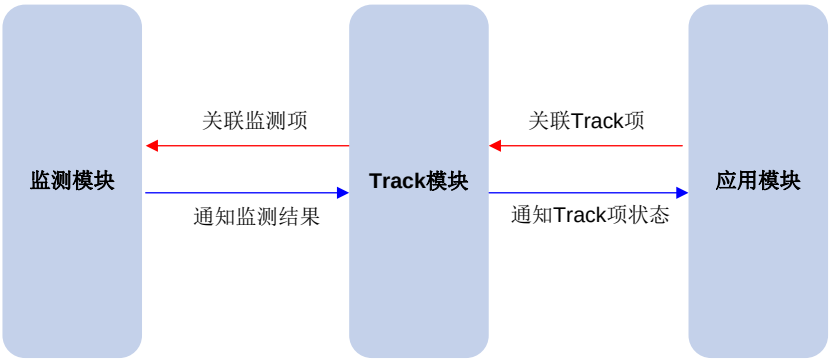
特性简介

Track 用于在监测模块、Track 模块和应用模块之间建立关联，来实现这些模块之间的联合动作。联动功能在应用模块和监测模块之间增加了 Track 模块，通过 Track 模块屏蔽不同监测模块的差异，将监测结果以统一的形式通知给应用模块，从而简化应用模块的处理。

联动功能实现机制

如图-1 所示，联动功能利用监测模块对链路状态、网络性能等进行监测，并通过 Track 模块将监测结果及时通知给应用模块，以便应用模块进行相应的处理。例如，在 NQA、Track 和静态路由之间建立联动，利用 NQA 监测静态路由的下一跳地址是否可达。NQA 监测到下一跳不可达时，通过 Track 通知静态路由模块该监测结果，以便静态路由模块将该条路由置为无效，确保报文不再通过该静态路由转发。

图-1 联动功能实现示意图



Track 模块与监测模块联动

Track 模块通过 Track 项与监测模块建立关联。Track 项定义了 Positive、Negative 和 NotReady 三种状态。监测模块负责对接口状态、链路状态等进行监测，并将监测结果通知给 Track 模块；Track 模块根据监测结果改变 Track 项的状态。

- 如果监测结果为监测对象工作正常（如接口处于 up 状态、网络可达），则对应 Track 项的状态为 Positive。
- 如果监测结果为监测对象出现异常（如接口处于 down 状态、网络不可达），则对应 Track 项的状态为 Negative。
- 如果监测结果无效（如 NQA 作为监测模块时，与 Track 项关联的 NQA 测试组不存在），则对应 Track 项的状态为 NotReady。

Track 模块支持与监测模块列表建立关联。监测对象列表是多个监测对象的集合，这些监测对象依据其状态和列表的类型共同决定 Track 项的状态，主要有 4 种类型的列表：

- 与类型列表：基于列表中对象状态的与运算结果决定 Track 项的状态。
- 或类型列表：基于列表中对象状态的或运算结果决定 Track 项的状态。
- 比例类型列表：此类 Track 项的状态由 Track 列表中 Positive 对象/Negative 对象的总比例和 Positive/Negative 状态门限值的大小决定。
- 权重类型列表：此类 Track 项的状态由 Track 列表中 Positive 对象/Negative 对象的总权重和 Positive/Negative 状态门限值的大小决定。

Track 模块与应用模块联动

应用模块通过引用 Track 项与 Track 模块建立关联。Track 项的状态改变后，通知应用模块；应用模块根据 Track 项的状态，及时进行相应的处理，从而避免通信的中断或服务质量的降低。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

配置 Track 与 BFD 联动时，VRRP 备份组的虚拟 IP 地址不能作为 BFD 会话探测的本地地址和远端地址。

配置指南

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

Track 具体配置步骤如下：

1. 选择“系统 > 高可靠性 > Track”。

2. 在“Track”页面单击<新建>按钮，进入“新建 Track 项”页面。

3. 在“新建Track项”页面配置Track项，监测模块不同时具体配置参数会有差异，具体配置内容如下所示：

表-1 Track 项公共配置参数表

参数	说明
Track项	Track项的序号，用于唯一标识此Track项
监测模块	表示与哪个监测模块建立关联，支持关联的检测模块如下： • Track 项与 BFD 联动，其相关具体配置参数请参见表-2 • Track 项与 NQA 联动，其相关具体配置参数请参见表-3 • Track 项与接口联动，其相关具体配置参数请参见表-4 • Track 项与路由联动，其相关具体配置参数请参见表-5 • Track 项与与类型的对象列表联动，其相关具体配置参数请参见表-6 • Track 项与或类型的对象列表联动，其相关具体配置参数请参见表-7 • Track 项与比例类型的对象列表联动，其相关具体配置参数请参见表-8 • Track 项与权重类型的对象列表联动，其相关具体配置参数请参见表-9 • Track 项与 BGP 联动，其相关具体配置参数请参见表-10 • Track 项与 OSPF 联动，其相关具体配置参数请参见表-11
类型	监控的IPv4/IPv6类型

Positive状态延迟通知时间	Track项状态变为Positive后，如果立即通知应用模块，则可能会由于路由 原因，导致通信中断。在这种情况下，用户可以配置Track项状态发生变化 时间通知应用模块。当Track项没有与应用模块联动时，此配置不生效
Negative状态延迟通知时间	Track项状态变为Negative后，如果立即通知应用模块，则可能会由于路由 原因，导致通信中断。在这种情况下，用户可以配置Track项状态发生变化 时间通知应用模块。当Track项没有与应用模块联动时，此配置不生效

表-2 Track 项与 BFD 联动的配置参数表

参数	说明
BFD报文出接口	BFD echo报文将从指定的接口发送，Track项只能与echo报文方式的BFD
本地IP地址	BFD会话探测的本地IP地址
远端IP地址	BFD会话探测的远端IP地址

表-3 Track 项与 NQA 联动的配置参数表

参数	说明
测试组管理员名称	NQA测试组的管理员的名字
操作标签	NQA测试操作的标签
联动项序号	指定NQA与Track项关联的联动项序号

表-4 Track 项与接口联动的配置参数表

参数	说明
监测接口	将Track项与指定的接口建立联动关系
接口类型	可以监控的接口类型包括：物理层状态、链路层协议状态、IPv4协议状态和

表-5 Track 项与路由联动的配置参数表

参数	说明
VRF	在指定VRF中创建和路由条目关联的Track项
路由地址	路由条目中的IP地址，点分十进制格式
掩码长度	IP地址掩码的长度

表-6 Track 项与与类型的对象列表联动的配置参数表

参数	说明
对象列表类型	需要将对象列表类型设置为“与” 如果此类型列表中的所有监测对象的状态都是Positive，那么此Track项的状 如果有一个或多个监测对象的状态为Negative，那么此Track项的状态为Ne
添加Track项	向对象列表类型的Track项中添加Track项成员

使用Track项反状态	若选择“是”，则表示此Track项使用所引用Track项的反状态进行本Track 若选择“否”，则表示直接使用所引用Track项的实际状态进行本Track项

表-7 Track 项与或类型的对象列表联动的配置参数表

参数	说明
对象列表类型	需要将对象列表类型设置为“或” 如果此类型列表中至少有一个监测对象的状态是Positive，那么此Tra Positive，如果所有的监测对象的状态都是Negative，那么此Track项的状
添加Track项	向对象列表类型的Track项中添加Track项成员
使用Track项反状态	若选择“是”，则表示此Track项使用所引用Track项的反状态进行本Track 若选择“否”，则表示直接使用所引用Track项的实际状态进行本Track项

表-8 Track 项与比例类型的对象列表联动的配置参数表

参数	说明
对象列表类型	需要将对象列表类型设置为“比例” 当列表中Positive对象所占百分比大于或等于Positive状态门限值时，Tr Positive；小于或等于Negative状态门限值时，Track项状态变为Negative。 的Positive对象比例小于Positive状态门限值且大于Negative状态门限值时， 持不变

添加Track项	向对象列表类型的Track项中添加Track项成员
Positive状态门限	表示Track项状态变为Positive所要达到的门限，以百分数形式表示
Negative状态门限	表示Track项状态变为Negative所要达到的门限，以百分数形式表示

表-9 Track 项与权重类型的对象列表联动的配置参数表

参数	说明
对象列表类型	需要将对象列表类型设置为“权重” 每个加入列表的Track对象都拥有一个权重值，当处于Positive状态的监测 于或等于Positive门限值时，Track项状态变为Positive；当处于Positive状 重之和小于或等于Negative门限值时，Track项状态变为Negative。当关联列 对象权重小于Positive参数指定值且大于Negative参数指定值时，Track项
添加Track项	向对象列表类型的Track项中添加Track项成员
权重	Track项的权重值
Positive状态门限	表示Track项状态变为Positive所要达到的门限值，以权重形式表示
Negative状态门限	表示Track项状态变为Negative所要达到的门限值，以权重形式表示

表-10 Track 项与 BGP 联动的配置参数表

参数	说明
VRF	表示BGP对等体所属的VPN
实例名称	表示BGP对等体所属的BGP实例
地址族类型	BGP对等体的IPv4地址或IPv6地址

表-11 Track 项与 OSPF 联动的配置参数表

参数	说明
接口名称	指定建立OSPF邻居的接口
OSPF邻居IP地址	OSPF邻居的IP地址，必须为有效的IPv4单播地址。不指定该参数时，Trac 口上的所有OSPF邻居状态变化。

BFD

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 配置指南

特性简介

BFD（Bidirectional Forwarding Detection，双向转发检测）是一个通用的、标准化的、介质无关和协议无关的快速故障检测机制，用于检测转发路径的连通状况，保证设备之间能够快速检测到通信故障，以便能够及时采取措施，保证业务持续运行。BFD 可以为各种上层协议（如路由协议）快速检测两台设备间双向转发路径的故障。上层协议通常采用 Hello 报文机制检测故障，所需时间为秒级，而 BFD 可以提供毫秒级检测。

BFD 会话通过 echo 报文实现。Echo 报文封装在 UDP 报文中传送，其 UDP 目的端口号为 3785。本端发送 echo 报文建立 BFD 会话，对链路进行检测。对端不建立 BFD 会话，只需把收到的 echo 报文转发回本端。如果在检测时间内没有收到对端转发回的 echo 报文，则认为会话 down。echo

报文方式的 BFD 会话不需要双方均支持 BFD 功能，不支持 BFD 功能的设备接收到 echo 报文后，直接将该报文环回，从而达到快速检测的目的。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

BFD 功能具体配置步骤如下：

1. 选择“系统 > 高可靠性 > BFD”。
2. 在“BFD”页面配置相关内容，具体配置内容如下所示：

表-1 BFD 配置参数表

参数	说明
Echo报文源IPv4地址	Echo报文的源IPv4地址支持任意合法的单播IPv4地址。为了避免对端发送 定向报文造成网络拥塞，建议配置echo报文的源IP地址不属于该设备任何 段
Echo报文源IPv6地址	Echo报文源IPv6地址仅支持全球单播地址。为了避免对端发送大量的ICM 造成网络拥塞，建议不要将echo报文的源IPv6地址配置为属于该设备任何 段

NQA

特性简介

NQA 简介

NQA（Network Quality Analyzer，网络质量分析）通过发送探测报文，对链路状态、网络性能、网络提供的服务及服务质量进行分析，并为用户提供标识当前网络性能和服务质量的参数，如时延、抖动时间、TCP 连接建立时间、FTP 连接建立时间和文件传输速率等。利用 NQA 的分析结果，用户可以及时了解网络的性能状况，针对不同的网络性能进行相应处理并对网络故障进行诊断和定位。

运行机制

图-1 NQA 测试典型组网图



如图-1 所示，NQA 测试的典型组网中包括以下两部分：

- NQA 测试的源端设备：又称为 NQA 客户端，负责发起 NQA 测试，并统计探测结果。NQA 测试组在 NQA 客户端上创建。
- NQA 测试的目的端设备：负责接收、处理和响应 NQA 客户端发来的探测报文。
    - 在进行 UDP-jitter 类型测试时，必须在目的端设备上配置 NQA 服务器功能，开启指定 IP 地址和端口上的监听服务。此时，目的端设备又称为 NQA 服务器。当 NQA 服务器接收到客户端发送给指定 IP 地址和端口的探测报文后，将对其进行处理，并发送响应报文。
    - 在其他类型的测试中，目的端设备只要能够处理 NQA 客户端发送的探测报文即可，不需要配置 NQA 服务器功能。例如，在 FTP 测试中，目的端设备上需要配置 FTP 服务器相关功能，以便处理客户端发送的 FTP 报文，而无需配置 NQA 服务器功能。

NQA 测试的过程为：

2. NQA 客户端构造指定测试类型的探测报文，并发送给目的端设备；
3. 目的端设备收到探测报文后，回复应答报文；
4. NQA 客户端根据是否收到应答报文，以及接收应答报文的时间，计算报文丢失率、往返时间等。

支持联动功能

联动功能是指在监测模块、Track 模块和应用模块之间建立关联，实现这些模块之间的联合动作。联动功能利用监测模块对链路状态、网络性能等进行监测，并通过 Track 模块将监测结果及时通知给应用模块，以便应用模块进行相应的处理。联动功能的详细介绍，请参见 “Track 联机帮助”。NQA

可以作为联动功能的监测模块，对 NQA 探测结果进行监测，当连续探测失败次数达到一定数目时，就通过 Track 模块触发应用模块进行相应的处理。

阈值告警功能

NQA 通过创建阈值告警项，并在阈值告警项中配置监测的对象、阈值类型及触发的动作，来实现阈值告警功能。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置思路

NQA 的配置思路如下图所示：

图-2 ARP/ICMP-echo 测试的配置思路图

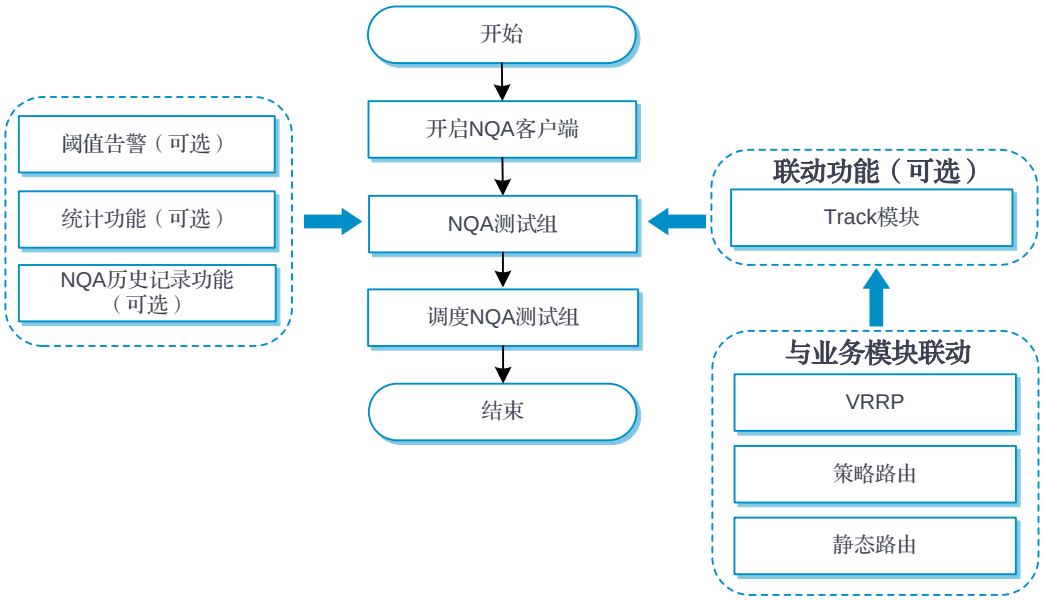


图-3 UDP-jitter 测试的配置思路图

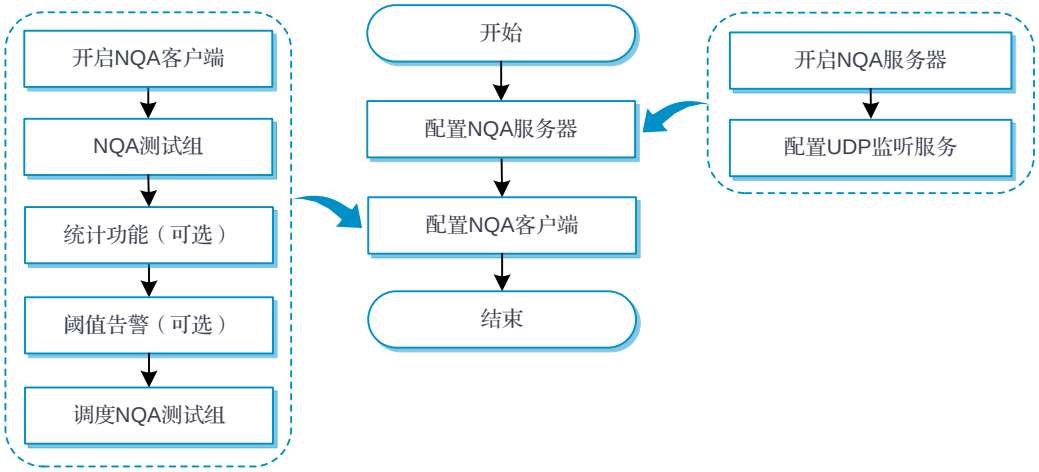
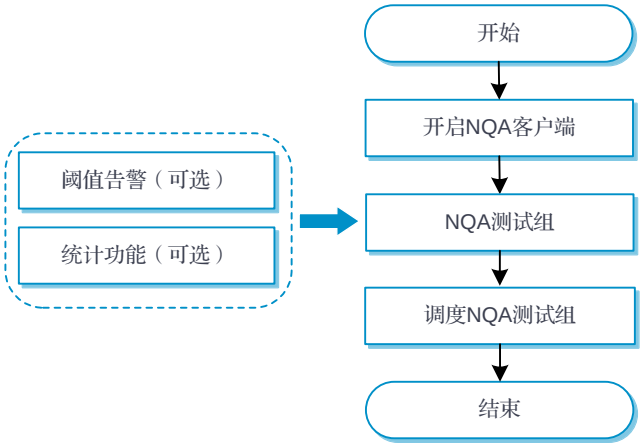


图-4 ICMP-jitter 测试的配置思路图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置 ICMP-echo 测试

ICMP-echo 测试是利用 ICMP 协议，根据应答报文或超时信息判断目的主机的可达性。

ICMP-echo 测试的具体配置步骤如下：

1. 选择“系统 > 高可靠性 > NQA”。

2. 在“NQA”页面单击<新建>按钮，进入“新建 NQA”页面。

表-1 ICMP-echo 测试配置参数表

参数	说明
测试组管理员名称	NQA测试组的管理员的名字，NQA测试组由一个管理员名称和一个操作标
操作标签	NQA测试操作的标签
测试类型	NQA支持通过不同的协议报文进行链路探测
目的IP地址	探测报文的目的IP地址
VRF	NQA测试所属VRF
目的端口	探测报文的目的端口
测试时间间隔	连续两次测试开始时间的时间间隔，取值为0表示只进行一次测试，此时不
探测次数	如果配置的次数大于1，那么系统在进行第一次探测之后，等待回应。如果 间时，仍然没有收到回应，则发起第二次探测。如此反复，直到完成指定

探测超时时间	一次探测中等待响应报文的超时时间
开启历史记录保存功能	开启此功能后，系统会记录该NQA测试组的历史信息；关闭此功能后，系统 试组的历史信息，原有的历史记录信息也会被删除
保存历史记录的个数	如果一个测试组中历史记录个数超过设定的最大数目，则最早的历史记录将
启动测试	启动测试支持如下几种方式： • 立即启动：选择此方式，配置下发后 NQA 测试工作立即开始 • 指定启动时间：选择此方式，配置下发后 NQA 测试工作会在指定时间
测试持续时间	测试持续时间支持如下几种方式： • 永久：此方式，NQA 测试工作启动后将一直进行测试 • 指定持续时间：此方式，NQA 测试工作启动后，将在指定持续时间内 持续时间到达后将结束本次 NQA 测试

3. 在“新建 NQA”页面，配置阈值告警功能。

4. 单击<新建>按钮，进入“新建告警监控组”页面。

表-2 NQA 阈值告警功能配置信息表

参数	说明
告警组编号	阈值告警组的编号信息
监控对象	表示对某些类型的事件进行阈值监控，，包括： • probe-duration：监控探测持续时间

	• probe-fail：监控探测失败的次数
阈值类型	NQA阈值告警功能支持的阈值类型包括： • 累计数目：监测一次测试中探测结果不在指定范围内的累计数目，如果 或超过设定的值，则该监测对象超出阈值 • 连续次数：NQA 测试组启动后，监测探测结果连续不在指定范围内的 次数达到或超过设定的值，则该监测对象超出阈值 • 平均时间：监测一次测试中探测结果的平均值，如果平均值不在指定的 监测对象超出阈值
失败次数	探测失败的次数
阈值范围	监控对象的阈值范围
触发的动作	NQA阈值告警功能可以触发如下动作： • 仅显示结果：只在本地记录监测结果，不向网络管理系统发送 Trap 消 • 显示结果并发送 Trap：不仅在本地记录监测结果，当阈值告警项的状态 网络管理系统发送 Trap 消息。采用本动作时，需要在“系统 > 系统与 “中配置 Trap 接收主机 • 触发其他模块联动：在记录监测结果的同时，触发其他模块联动。采用 要在“系统 > 高可靠性 > Track”中配置“Track 项”

5. 单击<确定>按钮，NQA 测试将根据配置的测试时间启动 NQA 测试。

配置 UDP-jitter 测试

Delay jitter（时延抖动）是指相邻两个报文的接收时间间隔减去这两个报文的发送时间间隔。

UDP-jitter 测试需要 NQA 服务器和客户端配合才能完成。进行 UDP-jitter 测试之前，必须保证 NQA 服务器端配置了 UDP 监听功能。

UDP-jitter 测试的具体配置步骤如下：

1. 配置 NQA 服务器



NQA 服务器的相关配置需在目的端设备上通过 CLI 控制台执行命令行配置。

NQA 服务器上配置的监听 IP 地址、端口号、VRF 参数必须与 NQA 客户端上的配置一致，且不能与已有的 UDP 监听服务冲突。

   a. 在目的端设备上，开启 NQA 服务器功能。

   b. 在目的端设备上，配置 UDP 监听服务。

2. 配置 NQA 客户端

   a. 单击“系统 > 高可靠性 > NQA”，进入“NQA”页面。

   b. 在“NQA”页面单击<新建>按钮，进入“新建 NQA”页面。

表-3 UDP-jitter 测试配置参数表

参数	说明
测试组管理员名称	NQA测试组的管理员的名字，NQA测试组由一个管理员名称和一个

操作标签	NQA测试操作的标签
测试类型	NQA支持通过不同的协议报文进行链路探测
目的IP地址	探测报文的目的IP地址
VRF	NQA测试所属VRF
目的端口	探测报文的目的端口
测试时间间隔	连续两次测试开始时间的时间间隔，取值为0表示只进行一次测试，止
探测次数	如果配置的次数大于1，那么系统在进行第一次探测之后，等待回应间时，仍然没有收到回应，则发起第二次探测。如此反复，直到完成
启动测试	启动测试支持如下几种方式： • 立即启动：选择此方式，配置下发后 NQA 测试工作立即开始 • 指定启动时间：选择此方式，配置下发后 NQA 测试工作会在指
测试持续时间	测试持续时间支持如下几种方式： • 永久：此方式，NQA 测试工作启动后将一直进行测试 • 指定持续时间：此方式，NQA 测试工作启动后，将在指定持续持续时间到达后将结束本次 NQA 测试

c. 单击<确定>按钮，NQA 测试将根据配置的测试时间启动 NQA 测试。

配置 ARP 测试

ARP 测试利用 ARP 协议，测试时 NQA 客户端向目的端设备发送 ARP 请求报文，根据能否收到应答报文判断目的端设备的 ARP 服务是否可用。

ARP 测试的配置步骤与 ICMP-echo 测试相同，具体配置步骤请参考配置 ICMP-echo 测试。

配置 ICMP-jitter 测试

语音、视频等实时性业务对时延抖动（Delay jitter）的要求较高。通过 ICMP-jitter 测试，可以获得网络的单向和双向时延抖动，从而判断网络是否可以承载实时性业务。

ICMP-jitter 测试的具体配置步骤如下：

1. 单击“系统 > 高可靠性 > NQA”，进入“NQA”页面。
2. 在“NQA”页面单击<新建>按钮，进入“新建 NQA”页面。

表-4 ICMP-jitter 测试配置参数表

参数	说明
测试组管理员名称	NQA测试组的管理员的名字，NQA测试组由一个管理员名称和一个操作标
操作标签	NQA测试操作的标签

测试类型	NQA支持通过不同的协议报文进行链路探测
目的IP地址	探测报文的目的IP地址
VRF	NQA测试所属VRF
测试时间间隔	连续两次测试开始时间的时间间隔，取值为0表示只进行一次测试，此时不
探测次数	如果配置的次数大于1，那么系统在进行第一次探测之后，等待回应。如果 间时，仍然没有收到回应，则发起第二次探测。如此反复，直到完成指定
启动测试	启动测试支持如下几种方式： • 立即启动：选择此方式，配置下发后 NQA 测试工作立即开始 • 指定启动时间：选择此方式，配置下发后 NQA 测试工作会在指定时间
测试持续时间	测试持续时间支持如下几种方式： • 永久：此方式，NQA 测试工作启动后将一直进行测试 • 指定持续时间：此方式，NQA 测试工作启动后，将在指定持续时间内 持续时间到达后将结束本次 NQA 测试

3. 单击<确定>按钮，NQA 测试将根据配置的测试时间启动 NQA 测试。

日志管理

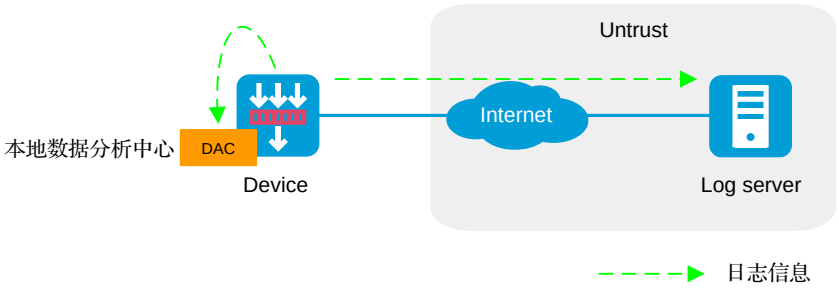
本帮助主要介绍以下内容：

- 特性简介
  - 输出到本地
  - 输出到日志主机
- vSystem 相关说明
- 配置限制和指导
- 配置指南
  - 配置思路
  - 配置准备
  - 日志信息输出到本地
  - 日志信息输出到快速日志主机
  - 日志信息输出到系统日志主机

特性简介

日志信息是设备记录的对报文处理的相关信息。网络管理员利用这些信息既可以有效监控网络运行情况和诊断网络故障；也可以实时跟踪、记录、分析用户访问网络的情况，审计用户的上网行为。设备支持输出日志的方式包括：输出到本地、输出到日志主机（包含快速日志主机和系统日志主机）。

图-1 日志输出示意图



输出到本地

输出到本地即将业务日志信息发送到数据分析中心，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。用户可以在 Web 界面的“概览”和“监控”页面上查看到数据分析中心汇总、分析后的数据。

输出到日志主机

快速日志主机

输出到快速日志主机用于快速地将用户关心的日志发往快速日志主机。配置该功能后，业务模块生成的日志通过快速输出通道直接发送给日志主机，不经过信息中心模块处理。相比通过信息中心输出，该方式可以节省系统资源，更快捷。建议将业务类日志发送到快速日志主机，如 NAT 日志，AFT 日志等。

系统日志主机

信息中心是设备的信息枢纽，它接收各模块生成的日志信息，能够按模块和等级将收到的日志信息输出到控制台、监视终端、日志主机等方向，为管理员监控设备运行情况和诊断网络故障提供了有力的支持。输出到系统日志主机即设备通过信息中心将各模块生成的日志信息按模块和等级输出到日志主机。建议将设备运行事件类日志发送到系统日志主机，如系统日志、配置日志等。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置限制和指导

设备支持通过系统日志和快速日志方式将某些业务模块的日志发送给日志主机，这些日志发送方式按优先级从高到低的顺序依次为：快速日志 > 系统日志。对于同一业务模块，如果用户配置了高优先级的输出方式，则不再采用其他方式输出。

配置指南

配置思路

日志管理的配置思路如下图所示：

图-2 输出到本地配置思路图

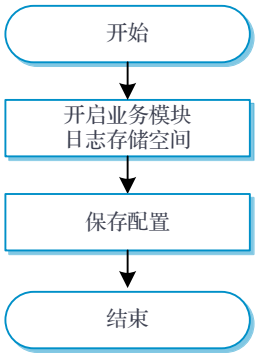
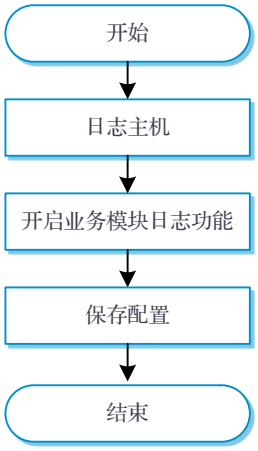


图-3 输出到日志主机配置思路图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

日志信息输出到本地

管理员可以自定义需要输出到本地数据中心的日志业务，并通过 WEB 监控的日志菜单下的展示页面查看到相关的日志信息。

“输出到本地”与“存储空间设置”页面的同名业务开关状态联动，操作任意一处，另一处即可自动同步状态。

日志信息输出到本地的具体配置步骤如下：

1. 单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。
2. 在“日志管理”页面，选择“输出到本地”页签。

表-1 输出到本地的基本信息配置

参数	说明
输出业务	配置输出到本地的日志类型，包括： • 全部：将定制部分的所有日志输出到本地 • 定制：定制需要输出到本地的日志

3. 单击<定制>按钮，单击“+”号添加输出到本地的业务日志。



日志模块的支持情况与设备型号有关，请以页面的实际显示为准。

表-2 定制输出到本地的日志配置

安全类日志	说明
威胁日志	威胁日志用来查看入侵防御和防病毒等网络威胁的检测和防御情况的记录 生和正在发生的威胁事件，方便管理员调整相应的策略，更好地防护内网 将定制选项中的“威胁日志+统计”选项选中后，在web监控的威胁日志菜 面，可以看到相关日志 注意事项： • 威胁日志包含入侵防御日志和防病毒日志 • 该功能开启后会同时开启监控下的威胁相关的统计功能
沙箱日志	沙箱日志用来查看沙箱检测的结果，包括报文基本信息、检测文件的基本 文件是否携带威胁等 将定制选项中的“沙箱日志”选项选中后，在web监控的沙箱日志菜单下 可以看到相关日志 注意事项：沙箱日志（检测详情）开启后，可在沙箱日志页面查看详情
信誉日志	信誉日志包括IP信誉日志、URL信誉日志和域名信誉日志 将定制选项中的“信誉日志”选项选中后，在web监控的信誉日志菜单下 可以看到相关日志
黑名单日志	黑名单日志用于查看增加黑名单、删除黑名单、扫描攻击防范动态添加黑 老化被删除时产生的相应日志 将定制选项中的“黑名单日志”选项选中后，在web监控的黑名单日志菜 面，可以看到相关日志
URL过滤日志	URL过滤日志用来查看用户访问URL产生的日志信息，方便管理员根据用 调整URL过滤策略，规范用户的上网行为 将定制选项中的“URL过滤日志+统计”选项选中后，在web监控的URL过

	的展示页面，可以看到相关日志 注意事项：该功能开启后会同时开启监控下的URL过滤相关的统计功能
数据过滤日志	数据过滤日志用于查看用户通过文件传输、收发邮件、访问网站等涉及敏 产生的日志信息，方便管理员根据数据传输的情况调整数据过滤配置文件 息和用户敏感信息泄露的风险 将定制选项中的“数据过滤日志”选项选中后，在web监控的数据过滤日 示页面，可以看到相关日志 注意事项：该功能开启后会同时开启监控下的数据过滤相关的统计功能
文件过滤日志	文件过滤日志用于查看用户经由设备传输文件产生的日志信息，方便管理 输的情况调整文件过滤策略，降低机密信息泄露和病毒文件进入公司内部 将定制选项中的“文件过滤日志+统计”选项选中后，在web监控的文件过 的展示页面，可以看到相关日志 注意事项：该功能开启后会同时开启监控下的文件过滤相关的统计功能
邮件过滤日志	邮件过滤日志用于记录垃圾邮件的拦截详情，管理员可通过分析日志数据 从而降低机密信息泄露风险 将定制选项中的“邮件过滤日志”选项选中后，在web监控的邮件过滤日 示页面，可以看到相关日志
Web应用防护日志	Web应用防护日志用来查看Web应用层攻击的检测和防御情况的记录，了 正在发生的攻击事件，方便管理员调整相应的策略，更好地防护内网安全 将定制选项中的“Web应用防护日志”选项选中后，在web监控的Web应 单下的展示页面，可以看到相关日志
防篡改日志	Web防篡改日志用来查看网页防篡改功能产生的日志记录，了解曾经发生 网页内容篡改事件，方便管理员调整相应的策略，更好地防护内网安全 将定制选项中的“防篡改日志”选项选中后，在web监控的Web防篡改日 示页面，可以看到相关日志

DGA域名检测日志	DGA域名检测日志用来查看DGA域名检测功能产生的日志信息，方便管 果调整相应的策略，防止用户遭到恶意网站的攻击 将定制选项中的“DGA域名检测日志”选项选中后，在web监控的DGA 单下的展示页面，可以看到相关日志
异常流量日志	异常流量日志记录了带宽管理中流量发生异常的日志信息 将定制选项中的“异常流量日志”选项选中后，在web监控下终端日志 日志页签下的展示页面，可以看到相关日志
应用审计日志	应用审计日志用来查看用户的上网行为记录，方便管理员根据用户上网 审计与管理策略，规范用户的上网行为 将定制选项中的“应用审计日志”选项选中后，在web监控的应用审计 示页面，可以看到相关日志
单包攻击日志	单包攻击也称畸形报文攻击，主要包括以下三种类型： • 攻击者通过向目标系统发送带有攻击目的的 IP 报文，如分片重叠的 标志位非法的报文，使得目标系统在处理这样的 IP 报文时出错、崩 • 攻击者可以通过发送正常的报文，如 ICMP 报文、特殊类型的 IP op 扰正常网络连接或探测网络结构，给目标系统带来损失 • 攻击者还可通过发送大量无用报文占用网络带宽，造成拒绝服务攻 将定制选项中的“单包攻击日志”选项选中后，在web监控的单包攻击 示页面，可以看到相关日志
扫描攻击日志	扫描攻击是指，攻击者运用扫描工具对网络进行主机地址或端口的扫描， 潜在目标的位置，探测目标系统的网络拓扑结构和开放的服务端口，为 系统做准备 将定制选项中的“扫描攻击日志”选项选中后，在web监控的扫描攻击 示页面，可以看到相关日志
泛洪攻击日志	泛洪攻击是指攻击者在短时间内向目标系统发送大量的虚假请求，导致 付无用信息，从而无法为合法用户提供正常服务，即发生拒绝服务

	将定制选项中的“泛洪攻击日志”选项选中后，在web监控的泛洪攻击 示页面，可以看到相关日志
IP限速日志	IP限速日志用于查看对新建会话速率进行限制所产生的日志信息 将定制选项中的“IP限速日志”选项选中后，在web监控的IP限速日志菜单 可以看到相关日志
连接数限制日志	连接数限制日志用于展示设备上的连接数到达限制阈值后产生的日志信息 将定制选项中的“连接数限制日志”选项选中后，在web监控的连接数 的展示页面，可以看到相关日志
物联网设备安全管理日志	物联网设备安全管理日志用来查看设备检测到的物联网设备存在安全隐患 方便管理员及时调整策略，防止信息泄露和网络攻击 将定制选项中的“物联网设备安全管理日志”选项选中后，在web监控 全管理日志菜单下的展示页面，可以看到相关日志
域名解析审计日志	域名解析审计日志用于查看设备上生成的域名解析的详细信息，包括DN 对应的应答报文 将定制选项中的“域名解析审计日志”选项选中后，在web监控的域名 单下的展示页面，可以看到相关日志 注意事项：域名解析审计日志需要先开启DNS日志才能生效

流量类日志	说明
安全策略日志	安全策略日志用于查看设备上生成的所有安全策略日志信息，这些安全 利于管理员对用户行为进行审计或进行网络故障排查 将定制选项中的“安全策略日志”选项选中后，在web监控的安全策略 示页面，可以看到相关日志
NAT转换日志	NAT转换日志用于记录NAT会话的相关信息，包括IP地址和端口的转换

	问信息以及用户的网络流量信息 将定制选项中的“NAT转换日志”选项选中后，在web监控的NAT转换 示页面，可以看到相关日志
流量日志	流量日志用于记录每条数据流产生的流量信息以及流量大小，管理员可 息制定合理、精确的带宽限速策略 将定制选项中的“流量日志”选项选中并开启全局开关后，在web监控 下的展示页面，可以看到相关日志

事件类日志	说明
系统日志	系统日志用于记录设备在运行过程中产生的相关日志信息，通过查看系 跟踪设备的运行过程、分析网络状况以及定位问题发生的原因，为进行 提供依据 将定制选项中的“系统日志”选项选中后，在web监控的系统日志菜单 可以看到相关日志
配置日志	配置日志用于记录管理员配置设备的过程，通过查看配置日志信息可以 备的操作，有利于对管理员操作设备的行为进行审计以及进行设备故障 将定制选项中的“配置日志”选项选中后，在web监控的配置日志菜单 可以看到相关日志
用户接入日志	当有SSL VPN用户登入登出设备时会有相应的日志输出。管理员可以通 日志，了解用户的历史登入登出记录，登录失败原因等信息，有利于管 设备 将定制选项中的“用户接入日志”选项选中后，在web监控的SSLVPN 单下的展示页面，可以看到相关日志
资源访问日志	当SSL VPN用户访问内网资源时会有相应的日志输出。管理员可以通过 志，了解用户访问内网资源的具体情况，方便管理员对用户访问的资源 将定制选项中的“资源访问日志”选项选中后，在web监控的SSLVPN

	单下的展示页面，可以看到相关日志
策略日志	零信任策略日志用于查看匹配零信任策略的流量产生的日志信息，当报文成功匹配后将输出日志到零信任策略日志页面。方便管理员查看实际的用状况，并根据用户和资产的风险状况调整访问动作 将定制选项中的“策略日志”选项选中后，在web监控的零信任策略日志页面，可以看到相关日志
终端识别日志	终端识别日志记录了在视频安全场景中系统所识别终端的详细信息。通过管理员可实时掌握设备所接入终端的详细信息以及终端信息发生的变化 将定制选项中的“终端识别日志”选项选中后，在web监控下终端日志页日志页签下的展示页面，可以看到相关日志

DLP 日志	说明
数据安全日志	数据安全日志用于查看数据泄露事件产生的日志信息，方便管理员根据数整相应的防范策略，降低机密信息泄露和病毒文件进入公司内部网络的风 将定制选项中的“数据安全日志+统计”选项选中后，在web监控的DLP的页面，可以看到相关日志 该功能开启后会同时开启监控下的DLP相关的统计功能
上传文件日志	上传文件日志用于查看文件上传的相关信息 将定制选项中的“上传文件日志+统计”选项选中后，在web监控的DLP的页面，可以看到相关日志 该功能开启后会同时开启监控下的DLP相关的统计功能
匹配摘要日志	匹配摘要日志是用于查看DLP模块对数据进行匹配的结果摘要信息 将定制选项中的“匹配摘要日志+统计”选项选中后，在web监控的DLP示页面，可以看到相关日志

	该功能开启后会同时开启监控下的DLP相关的统计功能
匹配详情日志	匹配详情日志是用于查看DLP模块对数据进行匹配的详细信息 将定制选项中的“匹配详情日志+统计”选项选中后，在web监控的DLP 示页面，可以看到相关日志 该功能开启后会同时开启监控下的DLP相关的统计功能

负载均衡日志	说明
智能DNS日志	智能DNS日志用于查看经过本地智能DNS和全局智能DNS调度的流量产 当报文经过本地智能DNS和全局智能DNS调度后，将输出日志到智能DN 便管理员查看流量的调度信息，获取调度结果以及分析调度失败的原因 将定制选项中的“智能DNS日志”选项选中后，在web监控的智能DNS 示页面，可以看到相关日志
出链路负载均衡日志	出链路负载均衡日志用于查看经过出链路负载均衡调度的流量产生的日 经过出链路负载均衡调度后，将输出日志到出链路负载均衡日志页面。 流量的调度信息，获取调度结果以及分析调度失败的原因 将定制选项中的“出链路负载均衡日志”选项选中后，在web监控的出 志页签下的展示页面，可以看到相关日志
DNS透明代理日志	DNS透明代理日志用于查看经过DNS透明代理调度的流量产生的日志信 DNS透明代理调度后，将输出日志到DNS透明代理日志页面。方便管理 度信息，获取调度结果以及分析调度失败的原因 将定制选项中的“DNS透明代理日志”选项选中后，在web监控的DNS 签下的展示页面，可以看到相关日志
防护告警日志	防护告警日志用来记录匹配防护策略的流量信息 将定制选项中的“防护告警日志”选项选中后，在web监控的负载均衡 的展示页面，可以看到相关日志

4. 单击<应用>按钮，完成输出到本地的基本信息配置。

日志信息输出到快速日志主机

配置日志信息输出到快速日志主机，可将指定的业务模块生成的日志，通过快速输出通道直接发送给日志主机，该方式可以更高效地发送日志信息，并且节省系统资源。

日志信息输出到快速日志主机的具体配置步骤如下：

1. 单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。
2. 在“日志管理”页面，选择“输出到日志主机”页签。
3. 在“输出到日志主机”页签，选择“快速日志主机”部分。
4. 单击<新建>按钮，新建快速日志主机的基本信息。（如果快速日志主机需要配置的日志存在中国联通，中国移动，中国电信，中国电信_vi，国家电网格式，需要先关闭“Web 界面定制”菜单下的“日志配置精简”开关才能展示和配置相关格式。）

表-3 快速日志主机的基本信息配置

参数	说明
日志主机	快速日志主机的地址，可以为IPv4地址、IPv6地址或主机名 日志主机不支持配置本机地址

端口号	快速日志主机接收日志信息的端口号，取值范围为1～65535，缺省值为
VRF	快速日志主机所属的VPN实例，如果指定为公网，则表示快速日志主机
输出业务	配置输出到快速日志主机的日志类型，包括： • 全部：将定制部分的所有日志输出到本地 • 定制：定制需要输出到本地的日志

5. 在“输出业务”单击<定制>按钮，单击“+”号添加输出到快速日志的业务模块。



日志模块的支持情况与设备型号有关，请以页面的实际显示为准。

表-4 定制输出到快速日志主机的日志配置

事件类日志	说明
SSL VPN日志	SSL VPN日志用于查看用户上下线、用户访问资源时记录的日志信息， 户行为进行监控，及时调整相应的访问授权；同时，日志中还记录了IP接 VPN网关为客户端虚拟网卡分配和释放IP地址时记录的信息，以及IP接 生丢包时记录的信息，便于管理员及时调整网关配置 将定制选项中的“SSLVPN日志”选项选中后，设备向指定的快速日志 志
零信任鉴权日志	零信任鉴权日志用来输出可信访问控制器的鉴权结果 将定制选项中的“零信任鉴权日志”选项选中后，设备向指定的快速日 日志

零信任策略通知日志	零信任策略通知日志用来输出用户下线和用户权限变更等信息 将定制选项中的“零信任策略通知日志”选项选中后，设备向指定的快 快速日志
带宽管理日志	带宽管理日志用于查看匹配带宽管理规则（比如报文命中动作为阻断的 而产生的日志，方便管理员分析快速日志判断带宽管理规则配置是否正 宽管理规则，提高网络安全性 将定制选项中的“带宽管理日志”选项选中后，设备向指定的快速日志 志
终端识别日志	终端识别日志用于在终端信息发生变更时（比如将原厂商的摄像头换为 头）向管理员发送日志，方便管理员对终端信息进行监控，提高网络安 将定制选项中的“终端识别日志”选项选中后，设备向指定的快速日志 志
心跳日志（国电格式）	心跳日志用来确认设备的正常运行，开启心跳日志功能后，日志服务器 日志。如果定期接收不到，则认为设备处于宕机状态 将定制选项中的“心跳日志（国电格式）”选项选中后，设备向指定的 送快速日志 注意事项：心跳日志（国电格式）需要关闭“web界面定制”下的“日 关才能展示和配置

安全类日志	说明
攻击防范日志	攻击防范日志用于查看黑名单日志和单包攻击防范日志。其中，黑名单 单的源IP地址、DS-Lite隧道对端地址、VPN实例名称、添加或删除的原 等信息。单包攻击防范日志默认采用聚合输出方式以降低对系统资源的 理员高速过滤和有效屏蔽报文，及时发现和分析攻击行为，提高网络安 将定制选项中的“攻击防范日志”选项选中后，设备向指定的快速日志 志

服务器外联防护日志	服务器外联防护日志用于查看服务器与非法外联地址建立的连接。方便管 外联的协议类型、服务器IP地址、外联IP地址和端口号 将定制选项中的“服务器外联防护日志”选项选中后，设备向指定的快速 快速日志
安全策略配置日志（国电格式）	安全策略配置日志用于查看记录设备上安全策略的配置信息，方便管理员 策略配置，从而掌握设备对报文的控制 将定制选项中的“安全策略配置日志（国电格式）”选项选中后，设备向 志主机发送快速日志 注意事项：安全策略配置日志（国电格式）需要关闭“web界面定制”下 精简”开关才能展示和配置
应用审计日志	应用审计日志用于查看记录用户上网行为的日志，方便管理员了解应用的 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 账号信息等），并据此对用户的上网行为进行审计，更好的防护网络安全 将定制选项中的“应用审计日志”选项选中后，设备向指定的快速日志主 志
URL过滤日志	URL过滤日志用来查看用户访问URL产生的日志信息，方便管理员根据用 调整URL过滤策略，规范用户的上网行为。 将定制选项中的“URL过滤日志”选项选中后，设备向指定的快速日志主 志 注意事项：URL过滤日志支持标准格式和中国联通格式。默认发送标准格 格式需要关闭“Web界面定制”下的“日志配置精简”开关才能展示和配
共享上网日志	共享上网日志可以对共享上网行为进行记录并发送到指定的日志主机，方 共享上网行为并冻结源IP地址，提高网络安全性 将定制选项中的“共享上网日志”选项选中后，设备向指定的快速日志主 志
入侵防御日志	入侵防御日志用于查看设备对入侵行为的检测和防御情况的记录，了解管

	发生的入侵事件，方便管理员调整相应的策略，更好地防护内网安全 将定制选项中的“入侵防御日志”选项选中后，设备向指定的快速日志主 志 注意事项： • 入侵防御日志支持标准格式和国家电网格式。默认发送标准格式。国 要关闭“Web 界面定制”下的“日志配置精简”开关才能展示和配置 • 单击选项右侧扩展按钮，可以同时配置输出邮件和中文日志功能
入侵防御特征库升级日志	入侵防御特征库升级日志用于查看入侵防御特征库的更新情况，方便管理 备的特征库版本，并根据实际情况判断是否需要对特征库进行升级或回滚 将定制选项中的“入侵防御特征库升级日志”选项选中后，设备向指定的 发送快速日志 注意事项：入侵防御日志选择国家电网格式时，才可选择入侵防御特征库
信誉日志	信誉日志包括IP信誉日志、URL信誉日志和域名信誉日志 将定制选项中的“信誉日志”选项选中后，设备向指定的快速日志主机发
Web应用防护日志	Web应用防护日志用来查看Web应用层攻击的检测和防御情况的记录，了 正在发生的攻击事件，方便管理员调整相应的策略，更好地防护内网安全 将定制选项中的“Web应用防护日志”选项选中后，设备向指定的快速日 速日志 注意事项：单击选项右侧扩展按钮，可以同时配置输出邮件和中文日志功
沙箱日志	沙箱日志用来查看沙箱检测的结果，包括报文基本信息、检测文件的基本 文件是否携带威胁等 将定制选项中的“沙箱日志”选项选中后，设备向指定的快速日志主机发
防病毒日志	防病毒日志用于查看设备对病毒文件的检测和防御情况的记录，了解曾经 生的威胁事件，方便管理员调整相应的策略，更好地防护内网安全 将定制选项中的“防病毒日志”选项选中后，设备向指定的快速日志主机

	注意事项：单击选项右侧扩展按钮，可以同时配置发送邮件功能
数据过滤日志	数据过滤日志用于查看用户通过文件传输、收发邮件、访问网站等涉及敏 产生的日志信息，方便管理员根据数据传输的情况调整数据过滤配置文件 息和用户敏感信息泄露的风险 将定制选项中的“数据过滤日志”选项选中后，设备向指定的快速日志主 志
文件过滤日志	文件过滤日志用于查看用户经由设备传输文件产生的日志信息，方便管理 输的情况调整文件过滤策略，降低机密信息泄露和病毒文件进入公司内部 将定制选项中的“文件过滤日志”选项选中后，设备向指定的快速日志主 志
DGA域名检测日志	DGA域名检测日志用来查看DGA域名检测功能产生的日志信息，方便管理 果调整相应的策略，防止用户遭到恶意网站的攻击 将定制选项中的“DGA域名检测日志”选项选中后，设备向指定的快速日 速日志
设备准入控制日志	设备准入控制日志用于查看由于设备认证失败而产生的日志信息，方便管 结果调整策略，从而有效地避免设备被篡改的情况 将定制选项中的“设备准入控制日志”选项选中后，设备向指定的快速日 速日志
标准流量管控日志	标准流量管控日志用于查看由于物联网设备大量发送请求或者短期内发送 而产生的日志信息，方便管理员根据检查结果调整策略，从而有效的避免 将定制选项中的“标准流量管控日志”选项选中后，设备向指定的快速日 速日志
标准格式检查日志	标准格式检查日志用于查看物联网设备流量不符合相关物联网标准而导致 产生的日志信息，方便管理员根据检查结果调整策略，从而有效的避免非 入 将定制选项中的“标准格式检查日志”选项选中后，设备向指定的快速日

	速日志
敏感信令控制日志	敏感信令控制日志用于查看由于物联网设备流量含有敏感行为而产生的 管理员根据检查结果调整策略，从而有效的避免数据泄露和数据篡改 将定制选项中的“敏感信令控制日志”选项选中后，设备向指定的快速 速日志

流量类日志	说明
AFT日志	AFT日志用于查看记录AFT连接（AFT连接是指报文经过设备时，源或 AFT转换的连接）信息的日志和端口块日志（当分配、回收端口块或端 发输出端口块日志），方便管理员进行安全审计，更好的防护网络安全 将定制选项中的“AFT日志”选项选中后，设备向指定的快速日志主机发 注意事项： • AFT 日志支持标准格式和中国联通，中国移动，中国电信格式。默 式。中国联通，中国移动，中国电信格式需要关闭“Web 界面定制” 置精简”开关才能展示和配置 • 中国联通，中国移动，中国电信格式下配置的日志需要开启 AFT 日 日志子开关 • 举例：开启中国电信格式的 AFT 端口块分配日志需要以下操作：（ 项为选中状态（2）单击左侧展开按钮（3）选择中国电信格式（4） 日志功能选项（5）勾选 AFT 端口块分配开关 • 在关闭“日志配置精简”开关后，如果关闭了标准格式下的 AFT 转 开启“日志配置精简”开关后，即使 AFT 日志选项选中也无法发送
NAT日志	NAT日志用于查看记录NAT会话（报文经过设备时，源或目的信息被NA 连接）信息的日志、NAT444用户日志和NAT444资源用尽日志，方便管 计或溯源，更好的防护网络安全 将定制选项中的“NAT日志”选项选中后，设备向指定的快速日志主机发

	注意事项： • NAT 日志支持标准格式和中国联通，中国移动，中国电信，中国电信 认发送标准格式。中国联通，中国移动，中国电信，中国电信_vi 格 “Web 界面定制”下的“日志配置精简”开关才能展示和配置 • 中国联通，中国移动，中国电信，中国电信_vi 格式下配置的日志需 志功能选项和各日志子开关 • 举例：开启中国电信格式的新建 NAT 会话日志需要以下操作：（1） 为选中状态（2）单击左侧展开按钮（3）选择中国电信格式（4）勾 志功能选项（5）勾选新建 NAT 会话开关 • 在关闭“日志配置精简”开关后，如果关闭了标准格式下的 NAT 转 开启“日志配置精简”开关后，即使 NAT 日志选项选中也无法发送
会话日志	会话日志可用于记录会话的创建、删除等操作，也可以在达到阈值时或 日志。用于帮助管理员分析和定位问题，方便管理员进行运维管理 将定制选项中的“会话日志”选项选中后，设备向指定的快速日志主机发 注意事项： • 会话日志先需要配置生成的日志接口列表才能生效。单击选项左侧的 看到配置生成的日志接口列表的相关配置 • 会话日志需要开启各日志子开关才能生效 • 举例：开启会话新建日志需要以下操作：（1）会话日志选项为选中 左侧展开按钮（3）勾选开启新建会话开关（4）需要配置生成的日志
安全策略日志	安全策略日志用于查看记录与安全策略匹配成功的报文信息。管理员可以 成的所有安全策略日志信息，这些安全策略日志信息有利于管理员对用户 或进行网络故障排查 将定制选项中的“安全策略日志”选项选中后，设备向指定的快速日志主 志 注意事项：安全策略日志支持标准格式和国家电网格式
流量日志	流量日志用于记录每条数据流产生的流量信息以及流量大小，管理员可通

	息制定合理、精确的带宽限速策略 将定制选项中的“流量日志”选项选中并开启全局开关后，设备向指定的发送快速日志

负载均衡日志	说明
全局负载均衡日志	全局负载均衡日志用于查看经过全局负载均衡调度的流量产生的日志信息 将定制选项中的“全局负载均衡日志”选项选中后，设备向指定的快速日志
DNS透明代理日志	DNS透明代理日志用于查看经过DNS透明代理调度的流量产生的日志信息 将定制选项中的“DNS透明代理日志”选项选中后，设备向指定的快速日志
智能DNS日志	智能DNS日志用于查看经过智能DNS调度的流量产生的日志信息 将定制选项中的“智能DNS日志”选项选中后，设备向指定的快速日志志
出链路负载均衡日志	出链路负载均衡日志用于查看经过出链路负载均衡调度的流量产生的日志 将定制选项中的“出链路负载均衡日志”选项选中后，设备向指定的快速日志
应用负载均衡日志	应用负载均衡日志用于查看经过应用负载均衡调度的流量产生的日志信息 将定制选项中的“应用负载均衡日志”选项选中后，设备向指定的快速日志

6. 单击<应用>按钮，完成输出到日志主机的基本信息配置。

日志信息输出到系统日志主机

通过配置日志信息输出到系统日志主机，各业务模块生成的日志信息将被发送到指定的日志主机中，以便于日志的统一管理和分析。

日志信息输出到系统日志主机的具体配置步骤如下：

1. 单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。
2. 在“日志管理”页面，选择“输出到日志主机”页签。
3. 在“输出到日志主机”页签，选择“系统日志主机”部分。
4. 单击<新建>按钮，新建系统日志主机的基本信息。

表-5 系统日志主机的基本信息配置

参数	说明
日志主机	系统日志主机的地址，可以为IPv4地址、IPv6地址或主机名
端口号	系统日志主机接收日志信息的端口号，取值范围为1～65535，缺省值为514
VRF	系统日志主机所属的VPN实例，如果指定为公网，则表示日志主机位于公网中

5. 单击<应用>按钮，完成输出到日志主机的基本信息配置。
6. 请前往指定业务模块的配置页面，开启日志功能。模块生成的日志信息将被输出到配置的系统日志主机中。

邮件服务器

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置准备
  - 配置邮件服务器

特性简介

当各业务的日志选择输出邮件时，需要配置邮件服务器。配置完成后，可以通过邮件将日志信息发送给接收人。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

系统默认存在一个名为 mailsetting_default_parameter 的邮件服务器，该服务器仅支持编辑，不支持删除。当入侵防御日志、防病毒日志等日志需要使用邮件方式发送日志信息时，系统将使用该服务器发送邮件。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。

- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置邮件服务器

邮件服务器的配置步骤如下：

1. 单击“系统 > 日志设置 > 邮件服务器”，进入“邮件服务器”页面。
2. 单击<新建>按钮，进入“新建邮件服务器“页面，配置邮件服务器信息。

表-1 邮件服务器配置信息

参数	说明
邮件服务器名称	配置邮件服务器名称
邮件服务器地址	支持IP地址和主机名
发件人地址	配置发送邮件的人的地址
收件人地址	配置邮件接收人的地址。可以配多个收件人地址，之间用分号隔开
身份验证	当邮件服务器需要登录用户进行身份验证时需要开启此功能
安全传输用户信息	配置此功能后，先在设备与邮件服务器之间创建一条安全通道，然后再在 登录邮件服务器的用户信息
用户名	配置登录邮件服务器的用户名

密码	配置登录邮件服务器的密码
邮件发送间隔	设备会将待发送的邮件进行缓存，到达指定的间隔时间时才发送
邮件发送数量	用于限制间隔时间内可发送的邮件最大数量 当待发送的邮件数量达到本功能配置的最大数量时，如果有新的邮件需要 根据邮件的严重级别（即报文匹配的入侵防御特征的严重级别）进行判断 的严重级别高于已缓存的邮件，则新邮件会覆盖已缓存中严重级别最低、 件 当多块业务板同时工作时，本参数分别限制每块业务板在间隔时间内可发 数量
语言类型	邮件使用的语言，取值包括英文和中文

3. 单击<确定>按钮，完成邮件服务器信息配置。

4. 完成上述配置后，可单击<发送测试邮件>按钮，测试邮件功能是否正常。其中，邮件服务器的测试邮件会发送到指定的收件人地址。

存储空间设置基本配置

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 配置指南
  - 配置准备
  - 存储空间设置

特性简介

通过设置存储空间，管理员可分别对各业务日志信息的数据保存周期、存储上限以及上限处理动作进行管理。

存储空间支持的存储设备类型包括：硬盘、U 盘、SD 卡和内存。各业务的历史数据优先保存在硬盘中，当硬盘不在位时保存在 U 盘中，当 U 盘不在位时保存在 SD 卡中，当 SD 卡也不在位时才会保存在内存中。

当数据保存在内存中时，如果数据存储量达到系统运行的最大规格，系统将会进行滚动覆盖，即自动删除最旧的数据以保存新数据；当数据保存在硬盘、U 盘或 SD 卡中时，如果数据存储量达到用户配置的存储上限，系统将根据用户配置的上限处理动作对数据进行处理。其中，处理动作为删除时，设备将会进行滚动覆盖，即自动删除最旧的数据以保存新数据。

如果是全新的硬盘或 U 盘，则需要先进行分区和格式化处理。



U 盘、SD 卡的支持情况与设备型号有关，请以设备的实际情况为准。

拔出存储设备之前，请先单击<卸载>按钮，解除各业务日志进程对存储设备文件系统的占用。并需要在 CLI 界面的用户视图下执行 umount 命令，卸载文件系统，避免存储数据损坏甚至存储设备损坏。



当设备在处理数据流量时，单击<卸载>按钮，可能会导致存储设备中部分统计数据丢失。

机械硬盘（HDD）的随机读写性能差且处理速度慢，因此，建议使用固态硬盘（SSD）以提升处理效率和用户体验。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

当各业务日志的存储空间已满时，将无法手动导入新的日志。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

存储空间设置

管理员可以自定义需要采集的业务日志，使能相关业务的日志存储功能后，数据分析中心将会采集指定业务的日志信息，并从中提取相关数据进行汇总和分析，用于在 Web 界面中进行展示以及生成相应的报表文件。用户可以在 Web 界面的“概览”和“监控”页面上查看到数据分析中心汇总、分析后的数据。

“输出到本地”与“存储空间设置”页面的同名业务开关状态联动，操作任意一处，另一处即可自动同步状态。



存储空间设置中各日志模块的支持情况与设备型号有关，请以页面实际显示为准。

存储空间设置的具体配置步骤如下：

1. 单击“系统 > 日志设置 > 存储空间设置”，进入“存储空间设置”页面。
2. 在“存储空间设置”页面，确认修改内容。安装存储设备后，单击指定业务右侧的<编辑>按钮，进入“编辑业务信息”页面，可配置各业务日志信息的存储规则。

表-1 存储空间设置参数表

参数	说明
业务	支持的日志模块及类型
数据保存周期	各业务历史数据能够保存的最长时间

	仅当硬盘或U盘在位时支持配置本功能
存储上限	各业务在存储空间中能够占用的最大空间 仅当硬盘或U盘在位时支持配置本功能
上限处理动作	各业务存储的数据达到保存周期或者存储上限后，对历史数据执行的动作， • 删除 • 提示 仅当硬盘或U盘在位时支持配置本功能
使能	开启指定业务的日志采集功能 有害信息鉴别业务的子文件匹配日志和帧匹配日志的采集功能需要依赖文件 集功能，若文件匹配日志的采集功能未开启，子文件匹配日志和帧匹配日志 生效

3. 单击<确定>按钮，完成存储空间的配置。

更多设置

本帮助主要介绍以下内容：

- 特性简介
  - 系统日志相关配置
  - 快速日志相关配置
  - 日志聚合相关配置
  - 安全管理及审计
- 配置指南
  - 配置准备
  - 系统日志相关配置
  - 快速日志相关配置
  - 日志聚合相关配置
  - 安全管理及审计相关配置

特性简介

日志信息是设备记录的对报文处理的相关信息。网络管理员利用这些信息即可以有效监控网络运行情况和诊断网络故障；也可以实时跟踪、记录、分析用户访问网络的情况，审计用户的上网行为。设备支持输出日志的方式包括：输出到本地、输出到日志主机（包含快速日志主机和系统日志主机）。在完成日志管理配置后，可以通过更多设置来配置部分可选功能来满足不同的日志发送需求。

系统日志相关配置

日志发送速率的最大值，此最大值为同一时刻所有支持的安全业务产生的日志总数。当安全业务发送日志的速率超过限制时，系统会丢弃多余的日志。



日志发送速率上限功能的支持情况与设备型号有关，请以页面实际显示为准。

快速日志相关配置

日志信息的时间戳为日志信息产生的时间，方便用户查看和定位系统事件。

日志信息的源 IP 地址为快速日志输出时使用的源 IP 地址，配置该功能后不管实际使用哪个物理接口发送日志信息，日志信息的源 IP 地址均为指定接口的主 IP 地址。当日志主机需要根据日志的源 IP 对日志进行过滤显示时，请配置该功能。

日志语言编码格式，如果日志接收服务器和设备使用的中文字符集编码不同，日志服务器上可能会出现中文字符乱码的情况。配置本功能可以快速日志输出模块发送日志信息时使用的字符集编码配置为 UTF-8 或者默认格式（GB18030）。

输出中文日志使输出的日志使用中文，目前仅部分业务支持发送中文的快速日志，且各业务日志中仅部分字段支持使用中文。

日志聚合相关配置

对日志进行聚合输出是指，在一定时间内，对在本机、同一个接口或同一个安全域上检测到的相同攻击类型、相同攻击防范动作、相同的源/目的地址以及属于相同 VPN 的单包攻击的所有日志聚合成一条日志输出。通常不建议开启本功能，因为在单包攻击较为频繁的情况下，它会导致大量日志信息输出，占用控制台的显示资源。

安全管理及审计

安全管理功能用于开启设备的安全管理业务进程，若设备未开启安全管理功能，用户将无法通过安全管理服务器完成设备安全业务的管理和审计。

安全审计日志功能可以对设备安全配置相关的日志进行记录，并上报给安全审计服务器。主要包括对管理员、系统和安全相关策略等模块进行操作产生的系统日志。



安全管理及审计功能的支持情况与设备型号有关，请以设备实际情况为准。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

系统日志相关配置

设备在处理某些安全业务时会产生大量的安全业务日志并发送至信息中心，此时会导致信息中心的负担过大。可以通过配置日志发送速率上限，减少同一时刻发往日志中心的安全业务日志总数。

系统日志相关配置的具体配置步骤如下：

1. 单击“系统 > 日志设置 > 更多设置”，进入“更多设置”页面。
2. 在“系统日志相关配置”部分，配置“日志发送速率上限”。
3. 单击<应用>按钮，完成系统日志相关配置。

快速日志相关配置

配置完成将快速日志输出到日志主机后，可以通过此功能进一步设置快速日志输出的内容和格式。

快速日志相关配置的具体配置步骤如下：

1. 在“系统 > 日志设置 > 日志管理”页面，在“输出到日志主机”页签，完成“快速日志主机”配置。
2. 单击“系统 > 日志设置 > 更多设置”，进入“更多设置”页面。
3. 在“快速日志相关配置”部分，进行快速日志相关配置。

表-1 快速日志相关配置

参数	说明
日志信息时间戳	配置快速日志的时间戳，包括： • 格林威治时间（GMT） • 设备本地时间
日志信息的源IP地址	配置快速日志输出时使用的源IP地址，配置信息为源IP地址对应的出接口
日志语言编码格式	配置快速日志输出使用的编码方式，包括： • 默认格式（GB18030） • UTF-8
输出中文日志	配置快速日志输出时使用的语言，开启时使用的语言为中文，关闭时使用
日志负载分担	开启/关闭快速日志的负载分担功能。当某个业务模块配置了多台快速日志 本功能后，每条快速日志都会复制输出给所有的日志主机；开启本功能后 按照指定方式进行负载分担
负载分担方式	快速日志的负载分担方式，包括： • 源 IP 地址：按照源 IP 地址进行负载分担 • 轮询：按照轮询方式进行负载分担 若配置了基于源IP地址的快速日志负载分担，对于没有源IP地址的快速日 输出到固定的一台日志主机

4. 单击<应用>按钮，完成快速日志相关配置。

日志聚合相关配置

开启单包攻击日志聚合功能后，会将同一接口或安全域上，攻击类型、防范动作、源/目的地址以及VPN 均相同的单包攻击所生成的日志合并为一条日志输出。

日志聚合相关配置的具体配置步骤如下：

1. 单击“系统 > 日志设置 > 更多设置”，进入“更多设置”页面。
2. 在“日志聚合相关配置”部分，配置“单包攻击日志聚合”。
3. 单击<应用>按钮，完成日志聚合相关配置。

安全管理及审计相关配置

配置本功能前，需在“Web 界面定制”页面开启安全管理。

安全管理及审计的具体配置步骤如下：

1. 单击“系统 > Web 界面定制”，进入 Web 界面定制页面，滑动开启“安全管理”功能。
2. 单击<确定>按钮，完成 Web 界面定制配置。
3. 单击“系统 > 日志设置 > 更多设置”，进入“更多设置”页面。
4. 在“安全管理及审计”部分，进行安全管理及审计相关配置。

表-2 安全管理及审计相关配置

参数	说明
安全管理功能	开启此功能后，设备将运行安全管理业务进程
安全审计日志功能	开启此功能后，设备将开始统计安全审计相关日志，并将日志上报给安全
安全审计服务器IP地址	安全审计服务器的IPv4地址

5. 单击<应用>按钮，完成安全管理及审计相关配置。

报表设置

本帮助主要介绍以下内容：

- 特性简介
  - 安全报表订阅
  - 安全报表导出
  - 邮件服务器
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 配置思路
  - 配置准备
  - 配置安全报表订阅
  - 配置安全报表导出
  - 配置邮件服务器

特性简介

安全报表订阅

安全报表订阅功能默认在每天业务量最低的凌晨 1 点到 5 点通过邮件向指定的安全报表订阅者发送报表文件，并在每月的 1 日发送上个月的月度报表文件。

安全报表订阅功能支持订阅四种类型的报表，用户可根据实际需求订阅：

- 综合安全风险报表：可以展示某时间段内的安全风险概况、主机的风险详情以及主机的风险评估结果和相应的安全防护建议。
- 汇总报表：可以将某时间段内流量业务以及应用安全相关业务的统计排名信息和趋势信息一次性全部导出。
- 对比报表：可以将两个时间段内的流量业务以及应用安全相关业务的统计排名信息和趋势信息进行对比。
- 智能报表：可以对某时间段内员工的工作效率、泄密风险和离职风险等情况进行分析。
- 综合报表：可以对某时间段内流量业务以及应用安全相关业务的重点数据进行抓取和分析，并综合展示设备整体运行状况和网络安全现状。

为保证成功发送报表，需要对邮件服务器进行配置。

安全报表导出

设备可针对用户不同的需求对各业务数据进行统计和趋势分析，并支持即时导出多种类型的分析报表，支持的报表类型如下：

- 综合安全风险报表：可以展示某时间段内的安全风险概况、主机的风险详情以及主机的风险评估结果和相应的安全防护建议。
- 汇总报表：可以将某时间段内各业务的统计排名信息和趋势信息进行汇总。
- 对比报表：可以将两个时间段内各业务的统计排名信息和趋势信息进行对比分析。其中，每个时间段的天数必须相同。
- 智能报表：可以对某时间段内员工的工作效率、泄密风险和离职风险等情况进行分析。
- 综合报表：可以对某时间段内各业务的重点数据进行抓取和分析，综合展示设备整体运行状况和网络安全现状。

邮件服务器

当需要使用安全报表订阅功能时，需要配置邮件服务器。配置完成后，设备可以通过邮件将报表发送到指定邮箱地址。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

配置安全报表订阅和安全报表导出功能前，需要开启相关业务的日志采集功能，有关日志采集功能的相关介绍，请参见“存储空间设置”中的详细介绍。

- 配置综合安全风险报表功能前，请先开启流量业务、威胁业务、Web 应用防护业务、URL 过滤业务、文件过滤业务和数据过滤业务的日志采集功能。
- 配置汇总报表功能前，请先开启流量业务、威胁业务、URL 过滤业务和文件过滤业务的日志采集功能。
- 配置对比报表功能前，请先开启流量业务、威胁业务、URL 过滤业务和文件过滤业务的日志采集功能。
- 配置智能报表功能前，请先开启流量业务和 URL 过滤业务的日志采集功能。
- 配置综合报表功能前，请先开启流量业务、威胁业务、URL 过滤业务和文件过滤业务的日志采集功能。

配置指南

配置思路

报表设置的配置思路如下图所示：

图-1 安全报表订阅配置思路图

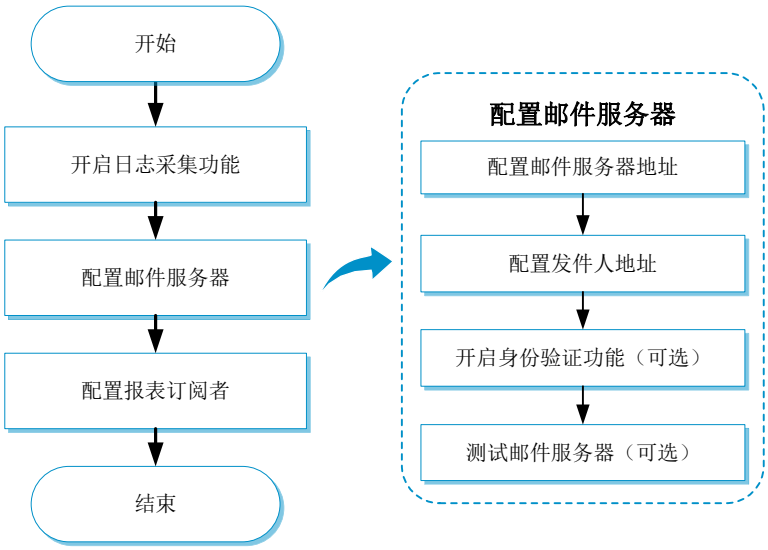
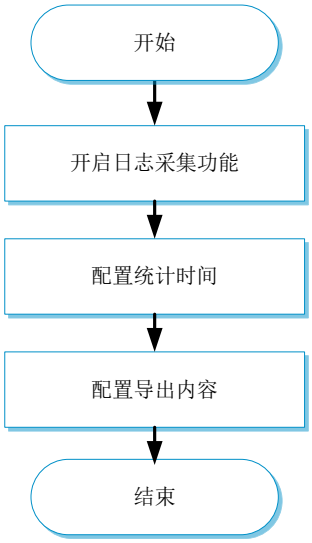


图-2 安全报表导出配置思路图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。
- 开启相关业务的日志采集功能。请参见“系统 > 日志设置 > 存储空间设置”中的详细介绍。

配置安全报表订阅

安全报表订阅功能用于生成周期性报表，并定期将生成的报表发送到指定的邮箱。

配置各报表功能前，需要在“存储空间设置”页面开启相关业务的日志采集功能。

安全报表订阅功能的具体配置步骤如下：

1. 选择“系统 > 报表设置 > 安全报表订阅”，进入安全报表订阅页面。
2. 在需要订阅的报表类型区域，单击<添加>按钮，在输入框中输入安全报表订阅者的邮箱地址，并选择报表的订阅语言。
3. 单击<配置导出条数>按钮，指定报表统计的数据范围，报表中仅统计排名 Top 5、10、15、20 或 25 的数据。对于综合安全风险报表，本参数仅用于限制“主机安全概况”中统计的主机数量。

配置安全报表导出

配置各安全报表导出功能前，需要在“存储空间设置”页面开启相关业务的日志采集功能。

生成安全报表的具体配置步骤如下：

1. 选择“系统 > 报表设置 > 安全报表导出”，在指定类型的报表区域下，配置报表导出参数。

表-1 报表导出参数表

参数	说明
导出条数	统计的数据范围，报表中仅统计排名前5、10、15、20或25的数据 对于综合安全风险报表，本参数仅用于限制“主机安全概况”主机数量
统计时间	统计的时间范围，取值包括： • 今天 • 最近一周 • 最近三十天 • 自定义
时间段1 时间段2	对比报表中需要指定的对比时间段 时间段1与时间段2的天数必须相同
导出格式	导出报表的格式，取值包括HTML 仅综合安全风险报表支持配置此参数，其他报表仅支持PDF格式
报表内容	报表中需要包含的统计数据类型，取值包括： • 流量统计 • 流量趋势 • 威胁统计 • 威胁趋势 • URL 过滤统计 • URL 过滤趋势 • 文件过滤统计

	• 文件过滤趋势 仅汇总报表需要配置本参数

2. 单击<生成报表>按钮，设备将根据上述导出条件生成报表。

配置邮件服务器

邮件服务器的具体配置步骤如下：

1. 选择“系统 > 报表设置 > 邮件服务器”，进入邮件服务器的配置页面。

2. 在“邮件服务器”页面中，配置邮件服务器。

表-2 邮件服务器配置参数表

参数	说明
邮件服务器地址	表示邮件服务器的IP地址或邮件服务器的主机名
发件人地址	表示邮件服务器对外发送邮件时使用的邮箱地址
身份验证功能	表示客户端身份验证功能，如果邮件服务器需要对登录的用户进行身份验证 员配合邮件服务器端的要求，在设备上同时开启本功能；如果服务器不需要 份验证，则不需要开启本功能
安全传输用户信息功能	表示安全传输登录邮件服务器的用户信息功能，用户信息包括用户名和密码
用户名	表示登录邮件服务器的用户名

密码	表示登录邮件服务器的密码

3. 完成上述配置后，可单击“发送测试邮件”，测试邮件功能是否正常。其中，邮件服务器的测试邮件会发送到指定的发件人地址。

4. 单击<应用>按钮，保存配置。

IRF

本帮助主要介绍以下内容：

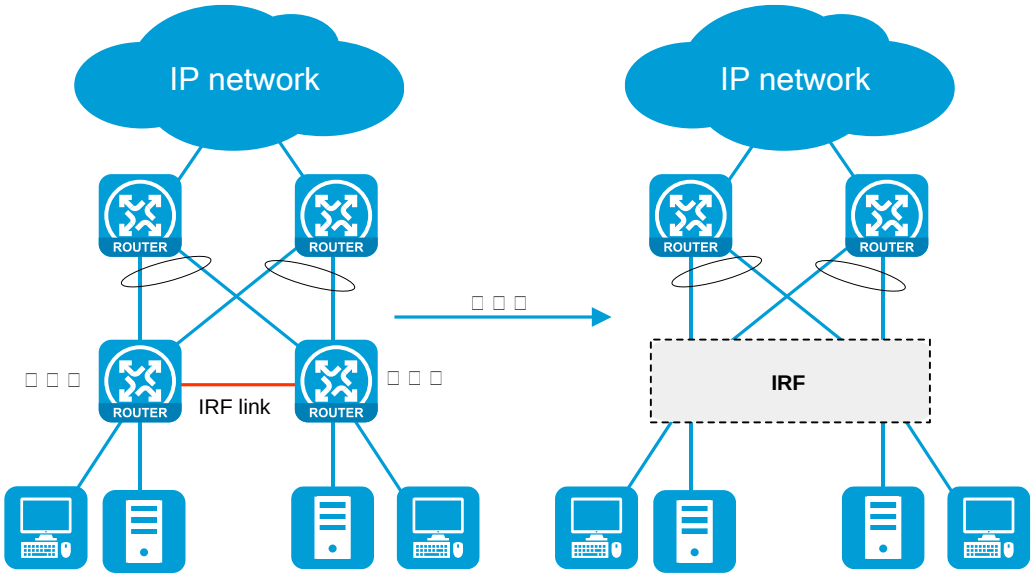
- 特性简介
  - 基本概念
  - 工作原理
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南

特性简介

IRF（Intelligent Resilient Framework，智能弹性架构）是一种软件虚拟化技术。它的核心思想是将多台设备连接在一起，进行必要的配置后，虚拟化成一台设备。使用这种虚拟化技术可以集合多台设备的硬件资源和软件处理能力，实现多台设备的协同工作、统一管理和不间断维护。

如下图所示，主设备和从设备组成 IRF，对上、下层设备来说，它们就是一台设备——IRF。

图-1 IRF 组网应用示意图



基本概念

成员设备角色

IRF 中每台设备都称为成员设备。成员设备按照功能不同，分为两种角色：

- 主用设备（简称为主设备）：负责管理和控制整个 IRF。
- 从属设备（简称为从设备）：处理业务、转发报文的同时作为主设备的备份设备运行。当主设备故障时，系统会自动从从设备中选举一个新的主设备接替原主设备工作。

主设备和从设备均由角色选举产生。一个 IRF 中同时只能存在一台主设备，其它成员设备都是从设备。

IRF 域

域是一个逻辑概念，一个 IRF 对应一个 IRF 域。为了适应各种组网应用，同一个网络里可以部署多个 IRF，IRF 之间使用域编号（DomainID）来以示区别。

成员 ID

标识不同成员设备，如果存在相同的成员 ID，则无法建立 IRF。

优先级

主要用于角色选举过程中确定成员设备的角色。优先级越高当选为主设备的可能性越大。

IRF 端口

一种专用于 IRF 成员设备之间进行连接的逻辑接口，每台成员设备上可以配置两个 IRF 端口，分别为 IRF-Port1 和 IRF-Port2。它需要和物理端口绑定之后才能生效。

IRF 端口采用二维编号，分为 IRF-Port*n*/1 和 IRF-Port*n*/2，其中 *n* 为设备的成员编号。

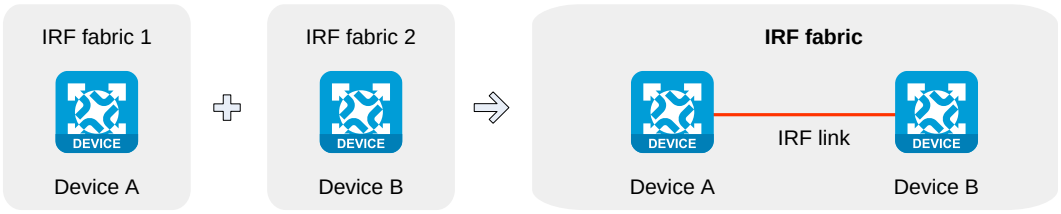
IRF 物理端口

与 IRF 端口绑定，用于 IRF 成员设备之间进行连接的物理接口。

IRF 合并

如下图所示，两个 IRF 各自已经稳定运行，通过物理连接和必要的配置，形成一个 IRF，这个过程称为 IRF 合并。

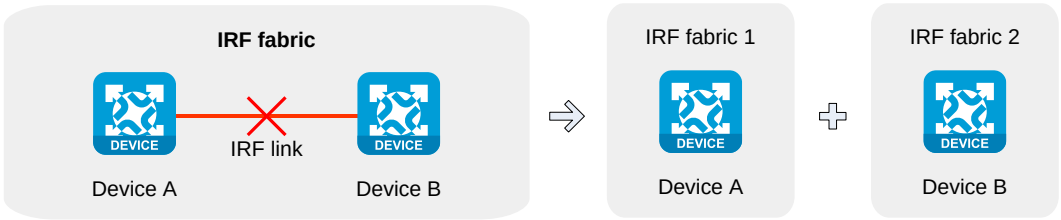
图-2 IRF 合并示意图



IRF 分裂

如下图所示，一个 IRF 形成后，由于 IRF 链路故障，导致 IRF 中两相邻成员设备不连通，一个 IRF 变成两个 IRF，这个过程称为 IRF 分裂。

图-3 IRF 分裂示意图

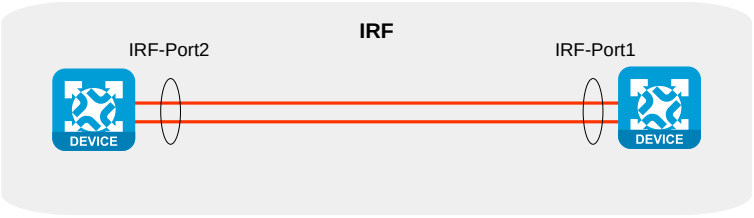


工作原理

连接要求

本设备上与 IRF-Port1 口绑定的 IRF 物理端口只能和邻居成员设备 IRF-Port2 口上绑定的 IRF 物理端口相连，本设备上与 IRF-Port2 口绑定的 IRF 物理端口只能和邻居成员设备 IRF-Port1 口上绑定的 IRF 物理端口相连，如下图所示。否则，不能形成 IRF。

图-4 IRF 物理连接示意图



角色选举

确定成员设备角色为主设备或从设备的过程称为角色选举。

IRF 建立、主设备离开或者故障、独立运行的两个 IRF 合并为一个 IRF 时，角色选举规则如下：

1. 当前主设备优先，IRF 不会因为有新的成员设备加入而重新选举主设备。不过，当 IRF 形成时，因为没有主设备，所有加入的设备都认为自己是主设备，则继续下一条规则的比较。
2. 成员优先级大的优先。如果优先级相同，则继续下一条规则的比较。

3. 系统运行时间长的优先。在 IRF 中，成员设备启动时间间隔精度为 10 分钟，即 10 分钟之内启动的设备，则认为它们是同时启动的，则继续下一条规则的比较。

4. CPU MAC 小的优先。

5. 通过以上规则选出的最优成员设备即为主设备，其它成员设备则均为从设备。

IRF 桥 MAC 的保留时间

桥 MAC 是设备作为网桥与外界通信时使用的 MAC 地址，桥 MAC 可标识不同设备。IRF 作为一台虚拟设备与外界通信时，IRF 使用主设备的桥 MAC 作为 IRF 桥 MAC。如果网络中存在桥 MAC 相同的设备，则会引起桥 MAC 冲突，从而导致通信故障。因此，用户需要根据网络实际情况配置 IRF 桥 MAC 的保留时间：

- 保留 6 分钟：当 IRF 桥 MAC 拥有者离开 IRF 时，IRF 桥 MAC 在 6 分钟内保持不变化；如果 6 分钟后 IRF 桥 MAC 拥有者没有回到 IRF，则使用新选举的主设备的桥 MAC 作为 IRF 桥 MAC。该配置适用于 IRF 桥 MAC 拥有者短时间内离开又回到 IRF 的情况（比如设备重启或者链路临时故障等），可以减少不必要的桥 MAC 切换导致的流量中断。
- 永久保留：无论 IRF 桥 MAC 拥有者是否离开 IRF，IRF 桥 MAC 始终保持不变。
- 不保留：当 IRF 桥 MAC 拥有者离开 IRF 时，系统会立即使用 IRF 中当前主设备的桥 MAC 做 IRF 桥 MAC。

IRF 启动文件自动加载

当新设备加入 IRF 时，如软件版本与主设备不一致，且在新设备上使能启动文件自动加载功能，则自动从主设备下载启动文件，然后使用新的系统启动文件重启，重新加入 IRF。



加载启动软件包需要一定时间，在加载期间，请不要手工重启处于加载状态的从设备，否则，会导致载启动软件包失败而不能启动。用户可打开日志信息显示开关，并根据日志信息的内容来判断加载过以及是否结束。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 修改成员 ID 会导致设备在下次重启后，部分配置丢失，且接口编号会发生改变。
- 修改成员 ID 后，如果保存当前配置，重启本设备，配置文件中，只有 IRF 端口的编号以及 IRF 端口下的配置、成员优先级会继续生效，其它与成员编号相关的配置 (比如普通物理接口的配置等）不再生效，需要重新配置。
- 将物理端口加入 IRF 端口后，会导致加入 IRF 端口的物理接口的相关业务中断。

- IRF 最多支持 2 个成员设备。
- 通常情况下，必须是同一系列产品型号的设备才能组成 IRF。
- 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。
- IRF 合并时，如果有成员设备的桥 MAC 相同，则它们不能合并为一个 IRF。IRF 的桥 MAC 不受此限制，只要成员设备自身桥 MAC 唯一即可。
- 在组成 IRF 的所有成员设备上，需要确保 IRF 端口绑定的物理端口类型、数量一致。
- 设备仅支持 IRF 物理端口直连组建 IRF，不支持跨中间设备。
- 如需关闭主设备的所有 IRF 端口，在进行此操作前请确保主设备优先级高于备设备。
- IRF 域编号是一个全局变量，IRF 中的所有成员设备都共用这个 IRF 域编号，因此，请按照网络规划来修改 IRF 域编号，不要随意修改。
- 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。
- IRF 形成之后，用户需通过主设备的管理口 IP 地址登录 IRF 系统 Web 页面，对 IRF 内所有成员设备进行统一配置管理。
- IRF 形成之后，如增加或删除堆叠物理端口时，需首先关闭非当前配置的成员设备对应物理口。
- 对于详细的产品特有的使用限制，请务必参考各产品配置手册使用限制中的内容。

- 部分 IRF 功能仅支持以 CLI 方式进行配置，不支持在 Web 界面上配置，具体支持情况请以设备实际 Web 界面为准。

配置指南

配置准备

在配置 IRF 之前，需要完成以下任务：

1. 进行网络规划，明确使用哪台设备作为主设备、各成员设备的编号以及成员设备之间的物理连接。
2. 连接 IRF 物理接口，确保 IRF 链路处于 up 状态。

配置 IRF

成员编号、成员优先级、IRF 端口配置方式不同，时效不同。IRF 的具体配置步骤如下：

1. 选择“系统 > 高级虚拟化 > IRF”。
2. 在“IRF”页面，单击列表右侧的<配置>按钮，打开“配置 IRF”页面。
3. 在“配置 IRF”页面，配置 IRF 参数。具体配置内容如下表所示：

图-5 配置 IRF 参数表

参数	说明
域ID	IRF的域编号。修改设备的IRF域编号，会导致设备离开当前IRF，不再属于当前IRF，不能和当前IRF中的设备交互IRF协议报文
成员ID	设备在IRF中的成员编号，IRF系统使用成员编号来唯一标识一台成员设备，每台成员设备需要使用不同的成员编号
优先级	IRF中成员设备的优先级 优先级值越大表示优先级越高，优先级高的设备竞选时成为主设备的可能性越大
IRF桥MAC的保留时间	IRF桥MAC拥有者离开IRF后，IRF可以继续使用当前桥MAC的时间，取值包括： • 保留 6 分钟：IRF 桥 MAC 的保留时间为 6 分钟。当 IRF 桥 MAC 拥有者离开 IRF 时，IRF 桥 MAC 在 6 分钟内不变化。如果 IRF 桥 MAC 拥有者在 6 分钟内重新又加入 IRF，则 IRF 桥 MAC 不会变化。如果 6 分钟后 IRF 桥 MAC 拥有者没有回到 IRF，则会使用 IRF 当前主设备的桥 MAC 作为 IRF 桥 MAC • 永久保留：IRF 桥 MAC 永久保留，无论 IRF 桥 MAC 拥有者是否离开 IRF，IRF 桥 MAC 始终保持不变 • 不保留：IRF 桥 MAC 地址不保留，立即变化，当 IRF 桥 MAC 拥有者离开 IRF 时，系统立即会使用 IRF 中当前主设备的桥 MAC 做 IRF 桥 MAC
IRF启动文件自动加载	开启/关闭IRF启动文件自动加载功能 开启IRF启动文件自动加载功能后，当新加入IRF的设备和主设备的软件版本不同时，新加入的设备会自动同步主设备的软件版本，再重新加入IRF。为了成功进行自动加载，请确

	保从设备存储介质上有足够的空闲空间用于存放IRF的启动文件。如果从设备存储介质上空闲空间不足，该设备将自动删除当前启动文件来再次尝试加载；如果空闲空间仍然不足，该从设备将无法进行自动加载。此时，需要管理员重启从设备并进入从设备的BootWare菜单，删除一些不重要的文件后，再将从设备重新加入IRF
描述	IRF的描述信息
IRF端口	一种专用于IRF成员设备之间进行连接的逻辑接口，每台成员设备上可以配置两个IRF端口，分别为IRF-Port1和IRF-Port2。它需要和物理端口绑定之后才能生效 IRF端口的状态由与它绑定的IRF物理端口的状态决定。与IRF端口绑定的所有IRF物理端口状态均为down时，IRF端口的状态才会变成down
物理端口	与IRF端口绑定，用于IRF成员设备之间进行连接的物理接口。IRF物理端口负责在成员设备之间转发IRF协议报文以及需要跨成员设备转发的业务报文 将IRF端口与物理端口绑定或解绑定时，需要先关闭相应的物理端口，在绑定或解绑定的操作完成后，再开启物理端口

4. 单击<确定>按钮，IRF 配置完成。

5. 将当前配置保存到设备的下次启动配置文件，以便设备重启后，IRF 配置能够继续生效。

IRF 高级设置

本帮助主要介绍以下内容：

- 特性简介
  - IRF 双机热备
  - 冗余组
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南

特性简介

本文所说的 IRF 高级设置就是 IRF 双机热备。IRF 双机热备方式是基于 IRF 技术实现双机热备组网需求。有关 IRF 的详细介绍，请参见“IRF”。

IRF 双机热备

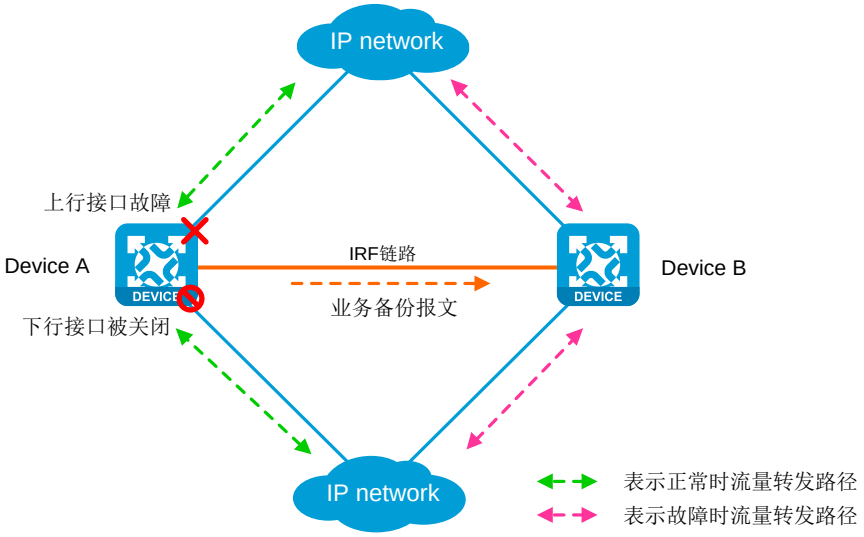
IRF 双机热备实现机制主要包括以下两个方面：

- 业务备份：用户选择业务后，IRF 双机热备的两台设备间会互相备份指定业务的数据和表项。以便流量切换后，对端设备上有对应的数据和表项，能够快速处理流量。
- 流量迁移：IRF 双机热备使用冗余组来触发流量的迁移。冗余组通过和 Track 联动，能够快速感知上、下行链路是否故障，如果故障，冗余组模块会通知组内所有成员接口和冗余口进行倒换，以便保证倒换后，报文的出接口和入接口仍然在同一台设备上。

IRF 双机热备的实现机制如图-1 所示：

1. 正常情况下，流量通过 Device A 转发，Device A 上业务的数据和表项实时备份到 Device B。
2. 当 Track 检测到 Device A 的上行接口故障。
3. 冗余组关闭 Device A 的下行接口。
4. 流量迁移到 Device B 上，通过 Device B 转发。因为 Device B 已经备份了业务的数据和表项，从而保证了流量迁移后，业务基本不受影响。

图-1 IRF 双机热备实现机制示意图



工作模式

IRF 双机热备包括主备模式和双主模式。主备模式下，只能有一台设备处理业务；双主模式下，两台设备可以同时处理业务。

冗余组

成员设备

一个冗余组必须且最多包含两个成员设备，其中一个为主成员设备，一个为备成员设备。通常情况下，主成员设备上的接口、CPU 处于工作状态（转发报文，创建会话表项等），备成员设备不处理业务，仅对主成员设备的接口和业务进行备份。

冗余组的成员设备通过成员编号和集群中的物理设备一一对应。冗余组的主成员设备可以是集群的主设备也可以是集群的备设备，通常情况下会配置为集群中的主设备。

成员接口

当上、下行设备运行动态路由协议，且要求一组接口整体倒换时，可通过成员接口来实现该需求。

主成员设备下的成员接口指的是主成员设备的上行接口和下行接口，可加入多个接口。

备成员设备下的成员接口指的是备成员设备的上行接口和下行接口，可加入多个接口。

当主成员设备下的某个成员接口故障时，冗余组会禁用主成员设备下的其它成员接口，让业务流量倒换到备成员设备下的成员接口上转发。

如图-2 所示，正常情况下，只有主成员设备上的成员接口转发报文，备成员设备上的成员接口被冗余组模块关闭。当主成员设备上的成员接口故障，备成员设备会立即切换成主成员设备接替原主成员设备工作，冗余组会关闭原主成员设备上的其它成员接口，使用新成员设备上的成员接口转发报文，如图-3 所示。

图-2 正常情况下，成员接口工作原理示意图

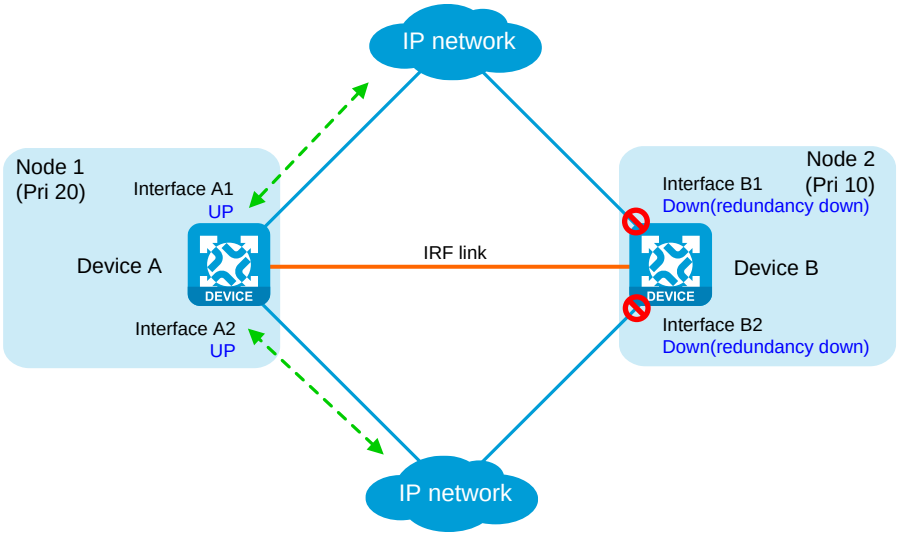
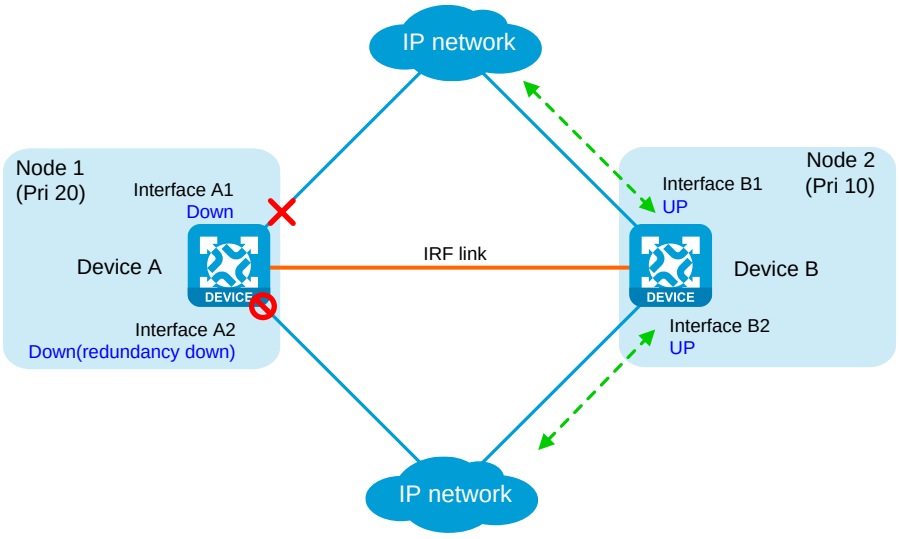


图-3 上行接口故障时，成员接口工作原理示意图



冗余口

当上、下行设备没有运行动态路由协议，又要求一组接口整体倒换时，可通过冗余口来实现该需求。

冗余口下包括两种子成员：

- 主成员接口：主成员设备的上行接口或下行接口，只能加入一个接口。
- 备成员接口：备成员设备的上行接口或下行接口，只能加入一个接口。

一个冗余组下可以配置多个冗余口，通常至少需要配置两个冗余口，一个冗余口的子成员均为上行接口，一个冗余口的子成员均为下行接口。

正常情况下，所有冗余口下的主成员接口转发报文，当某个主成员接口故障时，冗余组会禁用所有冗余口下的主成员接口，启用冗余口下的备成员接口来转发报文。

如图-4 所示，正常情况下，只有主成员设备上的以太网冗余接口的成员接口转发报文，备成员设备上以太网冗余接口的成员接口被冗余组模块关闭。当主成员设备上以太网冗余接口的成员接口故障，备成员设备会立即切换成主成员设备接替原主成员设备工作，冗余组会关闭原主成员设备上其它以太网冗余接口的成员接口，使用新主成员设备上所有以太网冗余接口的成员接口转发报文，如图-5 所示。

图-4 正常情况下，冗余组和冗余接口联动原理示意图

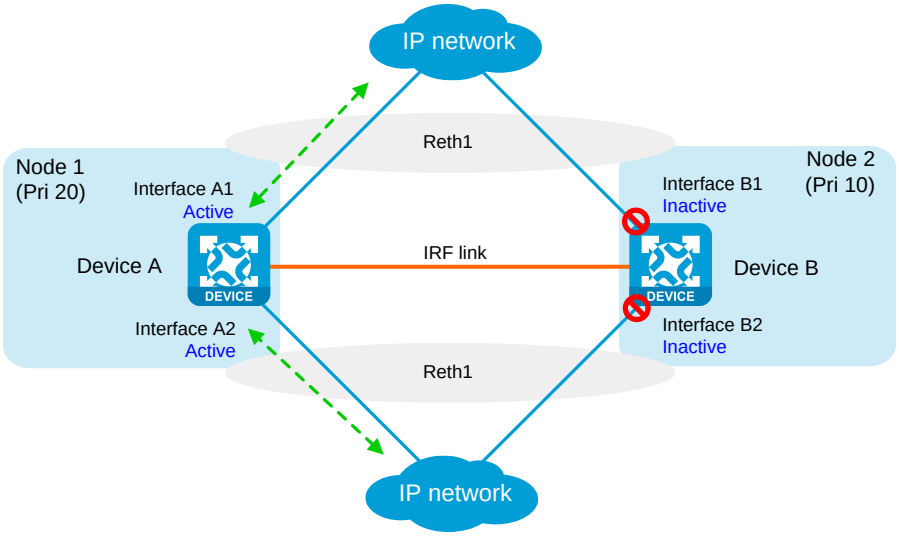
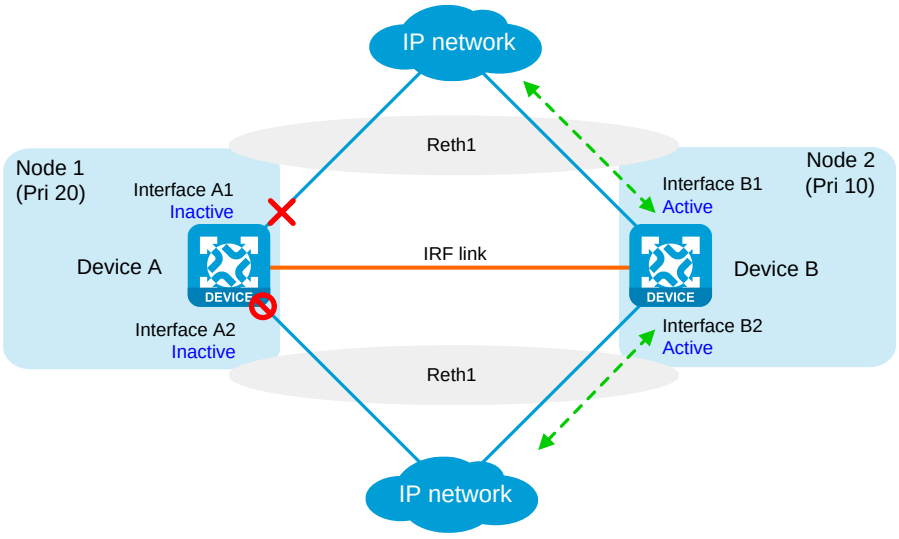


图-5 上行口故障时，冗余组和冗余接口联动原理示意图



倒换和倒回

当主成员设备上的接口或者链路故障，冗余组关闭冗余组内的接口，并将这些接口上的流量全部切换到备成员设备上传输的过程称为冗余组的整体倒换。

当主成员设备上的故障口恢复或者备成员设备上的接口或者链路故障，冗余组将主成员设备上关闭的接口激活，并将备成员设备上冗余组内的流量切回到主成员设备上传输的过程称为冗余组的整体倒回。

以下方式可触发倒换/倒回：

- 通过和 Track 联动来自动触发冗余组的整体倒换/倒回。
- 用户手工执行倒换/倒回操作，来触发冗余组的整体倒换/倒回。

触发倒换/倒回指的是给冗余组模块发送倒换/倒回事件，并不立即迁移流量。是否迁移流量还得判断状态持续时间和倒回等待时间。

倒回等待时间

冗余组收到倒回事件，在流量倒回前，主成员设备需要一定的时间来做准备工作（比如激活之前被冗余模块关闭的接口等），这个时间就是倒回等待时间。如果在倒回等待时间超时前，主成员设备准备完毕，则执行流量切换；否则，放弃本次倒回，流量不切换。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 在冗余组或冗余口中添加成员接口时，请不要添加管理口，否则在删除冗余口或冗余组时会导致设备的远程管理中断。
- IRF 双机热备的双主模式仅支持基于流的流分类策略。

配置指南

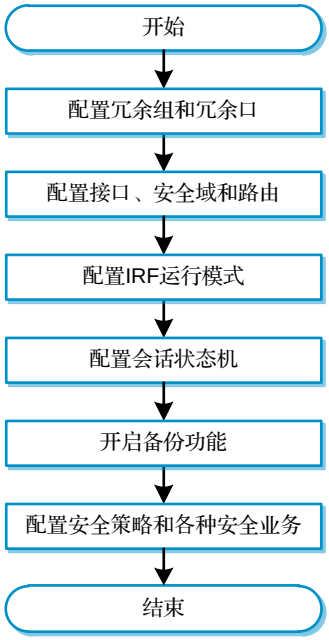
配置准备

配置 IRF 双机热备之前，请确保两台设备软、硬件环境一致。且两台设备已经组成一个 IRF。

配置思路

IRF 双机热备功能的配置思路如下图所示：

图-6 IRF 双机热备配置思路图



配置冗余组和冗余口

冗余组和冗余口的具体配置步骤如下：

1. 选择“系统 > 高级虚拟化 > IRF 高级设置”。
2. 在“IRF 高级设置”页面，单击<冗余组>按钮，进入冗余组配置页面。
3. 在冗余组页面，单击<新建>按钮，在弹出的添加冗余组页面设置冗余组的名称。

4. ，然后单击<确定>按钮。完成冗余组的创建并进入编辑冗余组页面，。

5. 在编辑冗余组页面可以配置冗余组和冗余口。冗余组成员设备具体配置信息如下表所示。

表-1 冗余组成员设备信息配置表

参数	说明
成员设备	一个冗余组必须且最多包含两个成员设备，其中一个为主成员设备，一个 通常情况下，主成员设备配置为IRF中的主设备
成员编号	指定此冗余组的成员设备在IRF中的成员编号
成员接口	此种方式适用于上行和下行设备运行动态路由协议的场景。至少需要将此 行两个物理以太网接口配置成此冗余组的成员接口
冗余口	冗余口适用于上行和下行设备没有运行动态路由协议的场景。至少需要配 一个冗余口的子成员均为上行接口，一个冗余口的子成员均为下行接口。 下面的冗余口配置
Track	通过和Track联动来自动触发冗余组的整体倒换/倒回。建议先创建Track项 项和冗余组关联。否则，可能会导致冗余组没有有效的Track项来触发倒换 当影响Track项状态改变的接口是以太网冗余接口的成员接口或是冗余组 时，建议配置该参数，并将该参数配置成与Track项接口一致

6. 单击“高级设置”页签，冗余组高级设置页面具体配置如下表所示。

表-2 冗余组高级设置信息配置表

参数	说明
状态持续时间	冗余组的保持时间，这段时间内不能发生主备倒换
倒回等待时间	冗余组将业务倒回到高优先级节点的等待时间
手工倒换	用户手工执行倒换/倒回操作，来触发冗余组的整体倒换/倒回

7. 在冗余口位置，单击<新建>按钮，进入添加冗余口页面，具体配置信息如下表所示。

一个冗余组下可以配置多个冗余口，通常至少需要配置两个冗余口，一个冗余口的主备成员接口均为主备设备上的上行接口，另一个冗余口的主备成员接口均为主备设备上的下行接口。

表-3 冗余口信息配置表

参数	说明
主成员接口	主成员设备的上行接口或下行接口，只能加入一个接口
备成员接口	备成员设备的上行接口或下行接口，只能加入一个接口
主切备保持主链路UP	主设备切换为备设备时，如果开启此功能，则仅将主设备接口的协议状态设 理状态不会被设置为Down。因此在主设备恢复正常时可以加快流量回切主 果关闭此功能，则将主设备接口的协议状态和物理状态均设置为Down

8. 单击<确定>按钮。完成冗余口配置。

9. 单击<确定>按钮。完成冗余组配置。

配置 IRF 双机热备

1. 选择“系统 > 高级虚拟化 > IRF 高级设置”。

2. 在“IRF 高级设置”页面，配置 IRF 双机热备的信息，具体信息如下表所示。

表-4 IRF 双机热备信息配置表

参数	说明
运行模式	IRF双机热备的运行模式包括如下两种： • 主备模式：正常情况下仅由主设备处理业务，备设备处于空闲状态，实 • 双主模式：两台设备同时处理业务，充分利用设备资源，提高系统负载
会话创建方式	在双主组网环境中，两台设备同时处理业务。为达到两台设备比较均衡处理 设备必须能够根据不同的组网环境支持不同的会话创建方式。目前，设备支 方式包括如下几种： • 哈希算法方式：根据哈希结果将首包流量送到相应设备创建会话，同一 设备和创建会话的设备可能不同。此种方式适用于流量在两台设备上分 网络情况 • 本地创建方式：首包流量在接收此报文的设备上进行创建会话，同一条 备和创建会话的设备是同一台设备。此种方式适用于流量在两台设备上 的网络情况 此功能仅在双主模式下支持
透传UDP报文	开启本功能后，当UDP报文在接收设备上未匹配到会话时，设备会将此UDP 一台设备进行处理，若在另一台设备上也未匹配会话，则会在此设备上为其

	此功能仅在双主模式下支持

3. 单击<应用>按钮。完成 IRF 双机热备配置。

虚拟设备

本帮助主要介绍以下内容：

- 特性简介
  - 缺省 Context 和非缺省 Context
  - 资源分配
  - 信息收集
  - 报文限速
- vSystem 相关说明
- 使用限制和注意事项
  - 分配 VLAN 时的注意事项
  - 分配接口时的注意事项
  - 信息收集
  - 停止 Context 时的注意事项
- 配置指南
  - 创建非缺省 Context
  - 为 Context 分配资源

- 对 Context 进行报文限速
- 切换虚拟设备

特性简介

通过虚拟化技术将一台物理设备划分成多台虚拟设备，每台虚拟设备就称为一个 Context。每个 Context 拥有自己专属的软硬件资源，独立运行。

对于用户来说，每个 Context 就是一台独立的设备，方便管理和维护；对于管理者来说，可以将一台物理设备虚拟成多台逻辑设备供不同的分支机构使用，可以保护现有投资，提高组网灵活性。

缺省 Context 和非缺省 Context

- 整台物理设备就是一个 Context，称为缺省 Context。当用户登录物理设备时，实际登录的就是缺省 Context。用户在物理设备上的配置实质就是对缺省 Context 的配置。缺省 Context 的名称为 Admin，编号为 1。缺省 Context 不需要创建，不能删除。
- 与缺省 Context 相对应的是非缺省 Context。非缺省 Context 是管理员在设备上创建的，可分配给不同的接入网络使用。

- 缺省 Context 拥有对整台物理设备的所有权限，它可以使用和管理设备所有的资源。缺省 Context 下可以创建/删除非缺省 Context，给非缺省 Context 分配 VLAN、接口、CPU、内存/磁盘资源，没有分配的 VLAN、接口、CPU、内存/磁盘资源由缺省 Context 使用和管理。
- 非缺省 Context 下不可再创建/删除非缺省 Context，它只能使用缺省 Context 分配给自己的资源，并在缺省 Context 指定的资源限制范围内工作，不能抢占其他 Context 或者系统剩余的资源。

因为缺省 Context 不需要创建和配置，所以，如无特殊说明，Web 页面中的 Context 均指非缺省 Context。

资源分配

管理员可以为每个 Context 分配 VLAN 资源、接口资源、CPU 资源和内存/磁盘资源。

VLAN 资源

用户在创建 Context 时，可选择是否和其它 Context 共享 VLAN：

- 共享：该模式下的 VLAN 由管理员在缺省 Context 中创建，统一配置和管理。非缺省 Context 只能使用指定的共享 VLAN，不能自行创建和配置。一个 VLAN 可以被多个 Context 共享，物理设备收到报文后，根据报文的入接口以及报文的 VLAN tag 交给相应的 Context 处理。此方式适用于同一个 VLAN 由多个 Context 共同使用的场景。

- 独占：该模式下的VLAN由各Context的管理员登录各自的Context后，自行创建、配置和管理。该模式要求各Context的管理员来规划和配置VLAN。此方式适用于Context需要各自管理和使用一个独立VLAN的场景。

接口资源

缺省情况下，设备上的所有接口都属于缺省 Context，不属于任何非缺省 Context。只有给非缺省Context分配接口后，它才能和网络中的其它设备通信。

在给 Context 分配接口时，可以选择：

- 独占分配：使用该方式分配的接口仅归该Context使用。用户登录该Context后，能查看到该接口，并执行接口支持的所有操作。
- 共享分配：表示将一个接口分配给多个Context使用，这些Context共享这个物理接口。设备从共享的物理接口接收报文后交给对应的虚拟接口处理；出方向，虚拟接口处理完报文后，会交给共享的物理接口发送。使用该方式，可以提高设备接口的利用率。通过共享方式分配的接口在非缺省Context内，会新建一个同名的虚接口，用户登录这些Context后，能查看到该接口，但只能执行禁用、修改描述信息以及网络/安全相关操作。

CPU 资源

当 CPU 无法满足所有 Context 的处理需求时，系统将按照 CPU 权重值为每个 Context 分配处理时间。通过调整 Context 的权重，可以使指定的 Context 获得更多的 CPU 资源，保证关键业务的运行。

例如：在三个 Context 中，将处理关键业务的 Context 的 CPU 权重设置为 2，其余两个 Context 的 CPU 权重设置为 1，则当 CPU 忙时，将为关键业务 Context 提供 2 倍于其它 Context 的处理时间。

内存/磁盘资源

为了防止一个 Context 过多的占用内存/磁盘，而导致其它 Context 无法运行，需要限制 Context 对内存/磁盘资源的使用。用户可配置每个 Context 最大可占用的内存/磁盘百分比。



- 建议在 Context 正常启动后再为 Context 分配磁盘空间上限，如果 Context 仅创建但未启动，那么值为 0，此时如果配置磁盘空间上限的值小于 Context 启动后正常实际使用的值，可能导致 Conte常启动。
- 建议在 Context 正常启动后再为 Context 分配内存空间上限，如果 Context 仅创建未启动，可能会不足，造成 Context 无法正常启动。在 Context 启动后，配置的内存上限值还不应过小，以免 Co务申请不到内存后引起功能不正常。

会话并发数

设备能够同时维持的会话连接总数是有限制的，为防止一个 Context 创建过多的会话，而导致其它 Context 无法创建新的会话，需要限制 Context 的会话并发数。用户可以为每个 Context 配置最大的会话并发数。

Context 会话并发数限制对本机流量不生效，例如：FTP、Telnet 等业务。

如果设置的最大值比当前存在的会话总数小，配置仍会成功，但不允许新建会话，且已经创建的会话不会被删除，依然生效。直到已建立的会话通过老化机制使得会话总数低于配置的最大值后，系统才允许新建会话。

会话新建速率

会话新建速率是指设备在单位时间内所能够完全处理的新会话请求数量。由于设备的处理能力有限，为防止一个 Context 的会话新建速率过高，而导致其它 Context 创建会话失败，需要限制 Context 的会话新建速率。用户可以为每个 Context 配置最大的会话新建速率。

Context 会话新建速率限制对本机流量不生效，例如：FTP、Telnet 等业务。

安全策略数

一个 Context 内可以配置多个安全策略。如果不加限制，会出现大量策略占用过多的内存的情况，影响 Context 的其它功能正常运行。所以，请根据需要为 Context 设置安全策略总数限制。当策略总数达到限制值时，后续不能新增策略。

如果设置的最大值比当前存在的安全策略总数小，配置仍会成功，多出的策略不会删除，依然生效，但不能新增策略。

吞吐量

为了防止一个 Context 的报文过多而导致其它 Context 的报文被丢弃，需要限制 Context 的吞吐量。当启用吞吐量限制时，系统优先处理协议报文，对于超过限制值的业务报文会被丢弃。

设备支持输出吞吐量限速丢包日志和吞吐量告警日志。

- 吞吐量限速丢包日志：启用Context吞吐量限制后，当Context的实际吞吐量大于吞吐量限制值，设备将超出限制值的报文丢弃，并周期性地输出吞吐量限速丢包日志。之后，当Context的实际吞吐量降低到限制值以下，设备输出恢复日志。
- 吞吐量告警日志：启用Context吞吐量限制后，当Context的实际吞吐量与吞吐量限制值的比值超过了告警门限，设备输出吞吐量告警日志。之后，当Context的实际吞吐量与吞吐量限制值的比值恢复到告警门限以下，设备输出恢复日志。

信息收集

缺省Context中提供了一键收集多个或所有Context相关信息的功能。目前在缺省Context中可收集的信息包括日志信息、诊断信息和配置信息。

报文限速

吞吐量限制告警

为了防止一个Context发送的报文过多而导致其它Context发送的报文被丢弃，需要限制Context出方向的吞吐量。

管理员可以开启吞吐量限速丢包日志功能和吞吐量告警日志功能，以便及时获知吞吐量变化。

- 吞吐量限速丢包日志功能：开启此功能后，当 Context 的出方向吞吐量达到出方向吞吐量限制值，设备会将超出限制值的报文丢弃，并对丢弃的报文生成日志信息；之后，如果该 Context 的出方向吞吐量降低到出方向吞吐量限制值以下，设备会生成恢复日志。
- 吞吐量告警日志功能：开启此功能并设置告警门限后，当 Context 的出方向吞吐量与出方向吞吐量限制值的比值超过了所设置的告警门限，设备会生成告警日志；之后，当 Context 的出方向吞吐量与出方向吞吐量限制值的比值恢复到告警门限以下，设备会生成恢复日志。

上面生成的日志信息将会被输出到信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。

因为此功能基于 CPU 进行吞吐量限制，所以其仅在非硬件快速转发的情况下生效。

整机限速和单机限速

此功能仅对使用共享接口且处于 Active 状态的 Context 生效。

如果一个 Context 接收和处理的广播报文和组播报文过多，将会导致其他 Context 处理业务能力的下降。因此需要限制 Context 接收广播报文和组播报文的数量。

Context 对入方向广播报文和组播报文进行限速是通过整机接收报文限速和单个 Context 接收报文限速共同实现。当广播报文或组播报文总速率和单个 Context 入方向广播报文或组播报文速率均达到各自的阈值后，发往此 Context 的广播报文或组播报文会被设备丢弃，否则不会被丢弃。

当整机或单个 Context 广播/组播限速阈值为零时表示对接收报文不做速率限制。

当运行广播或组播限速阈值低于 1000 时为系统缺省值，系统缺省值为广播/组播报文总速率阈值除以使用共享接口且处于 Active 状态的 Context 的数量。当运行广播或组播限速阈值大于等于 1000 时，有可能是系统缺省值，也有可能是系统管理员配置的阈值。

开启 Context 限速日志功能后，当 Context 接收的广播报文或组播报文因达到限速阈值而被丢弃时会生成 Context 限速日志。目前仅支持以系统日志方式输出。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

分配 VLAN 时的注意事项

- 共享 VLAN 必须是设备上存在的 VLAN。请先创建 VLAN，再指定共享 VLAN。
- VLAN 1 不能被共享。
- 端口的缺省 VLAN 不能被共享。
- 已经创建了 VLAN 接口的 VLAN 不能被共享。

分配接口时的注意事项

- 逻辑接口 (如子接口、聚合接口等) 仅支持共享方式分配，物理接口支持独占和共享两种方式分配。
- 如果子接口已经被分配，则不能再分配其父接口；如果父接口已经被分配，则不能再分配其子接口。
- 如果接口已经被共享分配，则不能再独占分配。需将共享分配配置取消后，才能独占分配。
- 当设备运行在集群模式时，禁止将集群物理端口分配给 Context。
- 聚合接口的成员接口不能分配给 Context。
- 冗余口的成员接口不能分配给 Context，当冗余口的成员接口为子接口时，其子接口的主接口也不能分配给 Context。

信息收集

- 在缺省 Context 中，无法对从未启动过的自定义 Context 进行日志信息收集。
- 在缺省 Context 中，无法对处于未启动状态的自定义 Context 进行配置信息收集。

停止 Context 时的注意事项

停止 Context 会导致该 Context 的业务中断，以及登录该 Context 的用户自动退出，请谨慎使用。

配置指南

创建虚拟设备后，可以在资源分配页面和资源使用情况页面，查看虚拟设备的资源分配情况和资源使用情况。

创建非缺省 Context

创建 Context 相当于构造了一台新的设备。创建 Context 的具体配置步骤如下：

1. 单击“系统 > 高级虚拟化 > 虚拟设备 > 虚拟设备”。
2. 在“虚拟设备”页面，单击<新建>按钮，进入“新建虚拟设备”页面
3. 配置虚拟设备。具体内容如下表所示：

表-1 虚拟设备配置

参数	说明
名称	此虚拟设备的名称
描述	此虚拟设备的描述信息
VLAN模式	VLAN模式分为共享和独占，共享模式表示虚拟设备之间可以共享VLAN，独占模式 之间不可以共享VLAN
VLAN列表	VLAN列表，可以是非连续的VLAN，也可以是连续的VLAN，例如3,5,10-100
独占接口列表	此列表中的接口是以独占方式分配给此虚拟设备。使用该方式分配的接口仅归该 使用。用户登录该虚拟设备后，能查看到该接口，并执行接口支持的所有功能
共享接口列表	此列表中的接口是以共享方式分配给此虚拟设备。表示将一个接口分配给多个虚 些虚拟设备共享这个接口，但是在各个虚拟设备内会创建一个同名的虚接口，这 同的MAC地址和IP地址。设备从共享的物理接口接收报文后交给对应的虚拟接口 虚拟接口处理完报文后，会交给共享的物理接口发送。使用该方式，可以提高设 通过共享方式分配的接口： • 在缺省虚拟设备内仍然存在该接口，该接口可执行接口支持的所有功能 • 在非缺省虚拟设备内，会新建一个同名接口，用户登录这些虚拟设备后，能 口，但只能使用关闭接口、增加接口描述信息以及网络/安全相关的功能
CPU权重	指定此虚拟系统的CPU权重，CPU权重越高虚拟设备获得的CPU资源越多
会话并发数	此虚拟设备下的会话并发数限制，当会话总数达到限制值时，该虚拟设备后续不
会话新建速率	此虚拟设备下的会话新建速率限制，当会话新建速率超过限制值时，该虚拟设备 会话不会被创建

安全策略数	可以根据需要为虚拟设备设置安全策略总数限制。当策略总数达到限制值时，后续
吞吐量	此虚拟设备下的吞吐量限制，当吞吐量达到限制值时，该虚拟设备后续将不能接

4. 单击<确定>按钮，完成配置。

5. 配置完成后可以在“虚拟设备”页面，查看创建的虚拟设备。

为 Context 分配资源

查看为 Context 分配的接口资源

在“接口分配”页面，可以查看接口的资源分配信息，并创建逻辑接口，具体配置步骤如下：

1. 单击“系统 > 高级虚拟化 > 虚拟设备 > 接口分配”。

2. 在“接口分配”页面，单击<新建>按钮，进入“新建逻辑接口”页面。

3. 配置以太网子接口，具体配置内容如下表所示：

表-2 以太网子接口配置

参数	说明
以太网口	选择需要创建子接口的以太网口
子接口编号	需要创建的子接口编号

4. 单击<确定>按钮，完成以太网子接口的创建。

为 Context 分配硬件资源

在“资源分配”页面，管理员可以为指定虚拟设备设置最大资源占用百分比，具体配置步骤如下：

1. 单击“系统 > 高级虚拟化 > 虚拟设备 > 资源分配”。
2. 在“资源分配”页面，选中需要调整硬件资源分配比例的 Context。
3. 单击<修改资源分配>按钮，进入“修改资源分配”页面。
4. 在“修改资源分配”页面中，为选中虚拟设备分配硬件资源占比。
5. 单击<确定>按钮，完成硬件资源分配。
6. 管理员可以在“系统 > 高级虚拟化 > 虚拟设备 > 资源使用情况”页面，查看各用户 Context 因配置产生的硬件资源占用情况，该页面主要反映的是配置本身对资源的消耗，并不代表会话转发、新建连接或并发会话等业务流量的硬件资源使用情况。

对 Context 进行报文限速

为了防止一个 Context 发送的报文过多而导致其它 Context 发送的报文被丢弃，需要限制 Context 出方向的吞吐量，具体配置步骤如下：

1. 单击“系统 > 高级虚拟化 > 虚拟设备 > 报文限速”，进入“报文限速”页面。

2. 配置吞吐量限速告警，具体配置内容如下：

表-3 配置吞吐量限制告警

参数	说明
吞吐量限速丢包日志	开启本功能后，当虚拟设备的出方向吞吐量达到出方向吞吐量限制值，设备会将 文丢弃，并对丢弃的报文生成日志信息；之后，如果该虚拟设备的出方向吞吐量 吐量限制值以下，设备会生成恢复日志
吞吐量告警日志	开启虚拟设备出方向吞吐量告警功能并设置告警门限后，当虚拟设备的出方向吞 吐量限制值的比值超过了所设置的告警门限，设备会生成告警日志；之后，当虚 吞吐量与出方向吞吐量限制值的比值恢复到告警门限以下，设备会生成恢复日志 虚拟设备的出方向吞吐量限制值是在虚拟设备页面设置的吞吐量
告警门限	生成吞吐量告警日志时配置的告警阈值

3. 单击<应用>按钮，完成吞吐量限制告警的配置。

4. 配置整机限速，具体配置内容如下：

表-4 配置整机限速

参数	说明
整机广播限速	虚拟设备对入方向广播报文进行限速是通过整机接收报文限速和单机接收报文限 广播报文总速率和单个虚拟设备广播报文速率均达到各自阈值后，发往此虚拟设 被设备丢弃，否则不会被丢弃
整机组播限速	虚拟设备对入方向组播报文进行限速是通过整机接收报文限速和单个虚拟设备

	同实现。当组播报文总速率和单个虚拟设备组播报文速率均达到各自阈值后，发往 组播报文会被设备丢弃，否则不会被丢弃

5. 单击<应用>按钮，完成整机限速的配置。

6. 单击虚拟设备右侧的<编辑>按钮，为指定虚拟设备配置单机限速值，具体配置内容如下：

表-5 配置单机限速

参数	说明
虚拟设备	显示进行单机限速的虚拟设备名称
运行广播限速	缺省Context入方向组播报文的速率限制，非缺省Context不可配置
配置广播限速	虚拟设备对入方向广播报文进行限速是通过整机接收报文限速和单机接收报文限 广播报文总速率和单个虚拟设备广播报文速率均达到各自阈值后，发往此虚拟设 被设备丢弃，否则不会被丢弃
运行组播限速	缺省Context入方向组播报文的速率限制，非缺省Context不可配置
配置组播限速	虚拟设备对入方向组播报文进行限速是通过整机接收报文限速和单个虚拟设备 同实现。当组播报文总速率和单个虚拟设备组播报文速率均达到各自阈值后，发往 组播报文会被设备丢弃，否则不会被丢弃

7. 单击<确定>按钮，完成单机限速的配置。

切换虚拟设备

切换虚拟设备的步骤如下：

1. 单击界面右上角当前登录用户。

2. 在下拉菜单中单击<切换虚拟设备>按钮，在“切换虚拟设备”页面指定目标虚拟设备。

3. 单击<确定>按钮，完成虚拟设备切换，用户可在目标虚拟设备界面进行相关配置。

虚拟系统

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
  - 分配 VLAN 时的注意事项
  - 分配接口时的注意事项
- 配置指南
  - 配置虚拟系统
  - 切换虚拟系统

特性简介

虚拟系统（vSystem）是在一台物理设备上划分出的多台相互独立的逻辑设备，从逻辑上将设备划分为多个虚拟系统。对于用户来说，每个虚拟系统相当于一台独立的真实设备，有自己的接口、地址集、用户/组、路由表项以及策略，并可通过虚拟系统管理员进行配置和管理；对于管理者来说，

可以将一台物理设备虚拟成多台逻辑设备供不同的分支机构使用，可以保护现有投资，提高组网灵活性。

缺省虚拟系统和非缺省虚拟系统

- 整台物理设备就是一个虚拟系统，称为缺省虚拟系统。当用户登录物理设备时，实际登录的就是缺省虚拟系统。用户在物理设备上的配置实质就是对缺省虚拟系统的配置。缺省虚拟系统的名称为 Admin，编号为 1。缺省虚拟系统不需要创建，不能删除。
- 与缺省虚拟系统相对应的是非缺省虚拟系统。非缺省虚拟系统是管理员在设备上创建的，可分配给不同的接入网络使用。
- 缺省虚拟系统拥有对整台物理设备的所有权限，它可以使用和管理设备所有的资源。缺省虚拟系统下可以创建/删除非缺省虚拟系统，给非缺省虚拟系统分配 VLAN 和接口资源，没有分配的 VLAN 和接口资源由缺省虚拟系统使用和管理。
- 非缺省虚拟系统下不可再创建/删除非缺省虚拟系统，它只能使用缺省虚拟系统分配给自己的资源，不能抢占其他虚拟系统或者系统剩余的资源。
- 缺省虚拟系统与非缺省虚拟系统分别对应一套独立的 Web 管理界面，方便管理者针对不同虚拟系统分别配置。设备支持在 Web 界面上进行缺省虚拟系统与非缺省虚拟系统间的切换。

因为缺省虚拟系统不需要创建和配置，所以，如无特殊说明，Web 页面中的虚拟系统均指非缺省虚拟系统。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

分配 VLAN 时的注意事项

- 请先创建相应 VLAN，再为虚拟系统分配该 VLAN。
- VLAN 分配给某个虚拟系统后，就不能再分配给其他的虚拟系统。
- VLAN 分配给某个虚拟系统后，对应的二层接口自动分配给该虚拟系统。
- VLAN 分配给某个虚拟系统后，绑定的 VLAN 接口自动分配给该虚拟系统。

分配接口时的注意事项

- 接口分配给某个虚拟系统后，就不能再分配给其他的虚拟系统。
- 支持将三层物理接口、三层物理子接口、三层聚合接口、三层聚合子接口、三层冗余接口、三层冗余子接口、Tunnel 接口和 LoopBack 接口分配给虚拟系统。

- 如果接口已经被共享分配，则不能再独占分配。需将共享分配配置取消后，才能独占分配。

配置指南

配置虚拟系统

配置虚拟系统前，需要调研实际业务需求，查看接口的分配情况并了解各接口的参数，以便据此为虚拟系统分配接口和 VLAN 资源。具体配置步骤如下：

1. 单击“系统 > 高级虚拟化 > 虚拟系统 > 虚拟系统”，进入“虚拟系统”页面。

2. 在“虚拟系统”页面，单击<新建>按钮，创建并配置虚拟系统。各项配置说明见下表：

表-1 新建虚拟系统配置说明

配置项	说明
名称	此虚拟系统的名称 创建虚拟系统时会同时创建一个同名VRF，单击“网络 > VRF”，可在“VRF”该VRF
描述	此虚拟系统的描述信息
VLAN	分配给此虚拟系统的VLAN列表
独占接口列表	此列表中的接口是以独占方式分配给此虚拟系统。使用该方式分配的接口仅归

	有、使用。用户登录该vSystem后，能查看到该接口，并执行接口支持的所有功
共享接口列表	此列表中的接口是以共享方式分配给此虚拟系统。表示将一个接口分配给多个vS 这些vSystem共享这个接口，但是在各个vSystem内会创建一个同名的虚接口， 具有不同的MAC地址和IP地址。设备从共享的物理接口接收报文后交给对应的 理；出方向，虚拟接口处理完报文后，会交给共享的物理接口发送。使用该方式 设备接口的利用率 通过共享方式分配的接口： • 在缺省 vSystem 内仍然存在该接口，该接口可执行接口支持的所有功能 • 在非缺省 vSystem 内，会新建一个同名接口，用户登录这些 vSystem 后， 接口，但只能使用关闭接口、增加接口描述信息以及网络/安全相关的功能
会话并发数	此虚拟系统下的会话并发数限制
会话新建速率	此虚拟系统下的会话新建速率限制
安全策略数	此虚拟系统下的安全策略规则数限制
吞吐量	此虚拟系统下的吞吐量限制

3. 单击<确定>按钮，完成虚拟系统配置。

切换虚拟系统

切换虚拟系统的步骤如下：

1. 单击界面右上角当前登录用户。

2. 在下拉菜单中单击<切换虚拟系统>按钮，在“切换虚拟系统”页面指定目标虚拟系统。

3. 单击<确定>按钮，完成虚拟系统切换，用户可在目标虚拟系统界面进行相关配置。

特征库升级

本帮助主要介绍以下内容：

- 特性简介
  - 特征库升级
  - 特征库恢复出厂
- vSystem 相关说明
- License 支持情况
- 使用限制和注意事项
- 配置指南
  - 配置准备
  - 设备特征库升级
  - 配置特征库服务器参数
  - 配置代理服务器参数
  - 设备的特征库恢复出厂

特性简介

特征库是用来对经过设备的应用层流量进行应用识别、URL 过滤、病毒检测、入侵防御、Web 应用防护和地区识别的资源库。随着网络攻击不断的变化和发展，需要及时升级设备中的特征库。设备也支持特征库版本回退功能。目前，设备中存在入侵防御特征库、防病毒特征库、应用识别特征库、Web 应用防护特征库、地区识别特征库、URL 特征库、IP 信誉特征库、URL 信誉特征库和域名信誉特征库。

特征库升级

特征库的升级包括如下几种方式：

- 定时升级：设备根据管理员设置的时间定期自动更新本地的特征库。
- 立即升级：管理员手工触发设备立即更新本地的特征库。
- 本地升级：当设备无法自动获取特征库时，需要管理员先手动获取最新的特征库，再更新设备本地的特征库。

特征库恢复出厂

如果管理员发现设备当前特征库对报文进行应用识别、URL 过滤和检测网络攻击时，误报率较高或出现异常情况，则可以将其回退到出厂版本。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

License支持情况

应用识别、入侵防御、防病毒、Web 应用防护、IP 信誉、域名信誉和 URL 信誉功能需要购买并正确安装 License 后才能使用。License 过期后，以上功能可以采用设备中各自已有的特征库正常工作，但无法升级到 license 有效期之后发布的新版本的特征库。关于 License 的详细介绍请参见“License 配置”。

使用限制和注意事项

- 执行特征库升级与恢复出厂会暂时中断 DPI 业务的处理，可能导致其他基于 DPI 功能的业务同时出现中断。例如，安全策略无法对应用进行访问控制等。
- 当系统内存使用状态处于告警门限状态时，请勿进行特征库升级或恢复出厂滚，否则易造成设备特征库升级或恢复出厂失败，进而影响 DPI 业务的正常运行。
- 同一时刻只能对一个特征库进行升级。
- 仅缺省 Context 支持特征库升级，用户 Context 仅支持查看特征库版本信息。

- IP 信誉、URL 信誉和域名信誉具有时效性，暂不支持出厂版本。建议在使用如上功能之前，先升级特征库。对 IP 信誉、URL 信誉和域名信誉特征库执行恢复出厂操作，将会删除当前已加载的特征库。
- 配置特征库定时升级或立即升级前，建议先单击<特征库服务器连接状态检测>按钮，测试设备与特征库服务器的连通性。确保设备可以通过特征库服务器获取特征库文件。如果服务器连接失败，可根据提示信息进行操作。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

设备特征库升级

特征库的升级包括定时升级、立即升级和本地升级。

特征库服务器连接状态检测

特征库服务器连接状态检测是指在进行特征库升级时，设备可以通过测试与特征库服务器的连接状态来确认是否能够成功连接到服务器。通过单击特征库服务器连接状态检测按钮，设备会尝试与特征库服务器建立连接，并返回连接状态的结果。如果连接失败，管理员可以根据界面提示进行排查，以解决连接问题，确保设备能够正常进行特征库升级。

特征库服务器连接状态检测的具体配置步骤如下：

1. 选择“系统 >升级中心 > 特征库升级”。
2. 在“特征库升级”页面，单击<特征库服务器连接状态检测>按钮，设备会尝试与特征库服务器建立连接，并返回连接状态的结果。

定时升级

如果设备可以访问官方网站，可以采用定期自动在线升级方式来对设备上的特征库进行升级。

1. 选择“系统 >升级中心 > 特征库升级”。
2. 在“特征库升级”页面，勾选目标特征库上的<开启定时升级>复选框，进入“XXX 特征库定时升级配置”页面。

3. 在“XXX 特征库定时升级配置”页面，配置特征库定时升级的时间。定时升级配置存在抖动时间（即实际自动升级开始时间的偏差范围），取值为指定的定时升级时间的前后一小时。

4. 单击<确定>，此特征库定时升级时间即可配置成功。

立即升级

当管理员发现官方网站上的特征库服务专区中的特征库有更新时，可以采用立即自动在线升级方式来及时升级特征库版本。

1. 选择“系统 >升级中心 > 特征库升级”。

2. 在“特征库升级”页面，单击目标特征库右边操作中的<立即升级>按钮，会弹出一个提示框，单击<确定>即可。

本地升级

如果设备不能访问官方网站上的特征库服务专区，管理员可以采用本地升级方式，使用本地保存的特征库文件手动离线升级系统上的特征库版本。

特征库文件只能存储在当前主用设备上，否则设备升级特征库会失败。

1. 选择“系统 >升级中心 > 特征库升级”。

2. 在“特征库升级”页面，单击目标特征库右边操作列下的<特征库服务专区>按钮，可以访问官方网站上的特征库服务专区，管理员可以根据实际需求将相应的特征库文件下载到本地。

3. 单击目标特征库右边操作列下的<本地升级>按钮，进入“升级特征库”页面，单击<选择文件>按钮，选择本地的特征库文件。

4. 单击<确定>，即可完成特征库升级。

配置特征库服务器参数

当设备对特征库进行立即升级或定时升级时，需要访问官网的特征库服务器来获取特征库文件。在升级特征库时使用特定的 IP 地址给特征库服务器发送报文或者客户的服务器处于特定的 VRF 时需要配置特征库服务器参数。

1. 选择“系统 >升级中心 > 特征库升级”。

2. 在“特征库升级”页面，单击<特征库服务器配置>按钮，进入“特征库服务器配置”页面，具体配置内容如下。

表-1 特征库服务器配置参数

参数	说明
源IP获取方式	用于选择设备向特征库服务器发送在线升级请求报文时使用的源IP地址的获取方式。 • 指定接口：选择指定接口的 IP 地址作为在线升级请求报文的源 IP 地址。选择此在“接口”下拉框中选择相应的接口 • 指定源 IP 地址：直接指定在线升级请求报文的源 IP 地址。选择此方式后，需要类型，并配置指定的 IP 地址

目的VRF	配置特征库服务器所属的VRF。如果设备通过VRF连接特征库服务器，则必须通过本 器所属的VRF，否则会导致特征库升级失败

3. 单击<确定>，即可完成特征库服务器的配置。

配置代理服务器参数

当设备不能连接到官方网站时，可配置一个代理服务器使设备连接到官方网站上的特征库服务专区，进行特征库在线升级。

配置步骤

1. 选择“系统 >升级中心 > 特征库升级”。
2. 在“特征库升级”页面，单击<配置代理服务器>按钮，进入“配置代理服务器”页面，配置代理服务器的地址、端口和登录代理服务器使用的用户名及密码。
3. 单击<确定>，即可完成代理服务器的配置。

设备的特征库恢复出厂

恢复出厂的具体配置步骤如下：

1. 选择“系统 >升级中心 > 特征库升级”。

2. 在“特征库升级”页面，单击目标特征库右边操作中的<恢复出厂>功能，进入“恢复 XXX 特征库”页面。

3. 在“恢复 XXX 特征库”页面，选择<恢复到出厂版本>。

4. 单击<确定>，即可完成操作。

软件更新

本帮助主要介绍以下内容：

- 特性简介
  - Boot ROM 程序
  - 启动文件
- 使用限制和注意事项
- vSystem 相关说明
- 配置指南
  - 配置准备
  - 设置启动文件

特性简介

设备软件包括 Boot ROM 程序和启动文件，它是设备启动、运行的必备软件，为整个设备提供支撑、管理以及丰富的业务。

当设备上存在主控板、接口板、网板和业务板时，主控板、接口板和网板的 Boot ROM 程序/启动软件包集成在主控板的 Boot ROM 程序/启动软件包中。系统在升级主控板时会自动升级接口板和网板，不会自动升级业务板。业务板使用独立的启动软件包，这个软件包会和主控板的启动软件包一起发布，需要单独升级。

Boot ROM 程序

设备开机最先运行的程序是 Boot ROM 程序，它能够引导硬件启动、引导启动文件运行、提供 Boot ROM 菜单功能。

Boot ROM 程序存储在设备的 Boot ROM（芯片）中。完整的 Boot ROM 程序包含 Boot ROM 基本段和 Boot ROM 扩展段。基本段提供 Boot ROM 菜单的基本操作项，扩展段提供更多的 Boot ROM 菜单操作项。整个 Boot ROM 程序通过 Boot 包 (*.bin) 发布，产品会将需要升级的单板的 Boot ROM 程序集成到 Boot 包中统一发布，以降低版本维护成本。

启动文件

启动文件的分类

启动文件是用于引导设备启动的程序文件，按其功能可以分为以下几类：

- Boot 文件：包含 Linux 内核程序，提供进程管理、内存管理、文件系统管理、应急 Shell 等功能。
- System 文件：包含内核和基本功能模块的程序，比如设备管理、接口管理、配置管理和路由模块等。
- Feature 文件（即特性文件）：用于业务定制的程序，能够提供更丰富的业务。一个 Feature 文件可能包含一种或多种业务。是否支持 Feature 文件以及支持哪些 Feature 文件与设备的型号有关，请以设备的实际情况为准。
- Patch 文件（即补丁文件）：用来修复设备软件缺陷的程序文件。补丁文件与软件版本一一对应，补丁文件只能修复与其对应的启动文件的缺陷，不涉及功能的添加和删除。

设备必须具有 Boot 文件和 System 文件才能正常运行，Feature 文件可以根据用户需要选择安装，补丁文件只在需要修复设备软件缺陷时安装。

启动文件的发布形式

启动文件有以下两种发布形式：

- BIN 文件：后缀为.bin 的文件。一个 BIN 文件就是一个启动文件。要升级的 BIN 文件之间版本必须兼容才能升级成功。
- IPE（Image Package Envelope，复合软件包套件）文件：后缀为.ipe 的文件。它是多个软件包的集合，产品通常会将同一个版本需要升级的所有类型的软件包都压缩到一个 IPE 文件中发布。用户使用 IPE 文件升级设备时，设备会自动将它解压缩成多个 BIN 文件，并使用这些 BIN 文件来升级设备，从而能够减少启动文件之间的版本管理问题。

使用限制和注意事项

- 软件升级期间，设备会重启，进而导致业务中断，请谨慎使用。
- 通过版本发布说明书了解将安装的软件包是否需要 License。如果需要，查看设备上是否有对应的有效的 License。如果没有，请先安装 License。否则，会导致软件包安装失败。
- 安装特性/补丁文件时，需要与当前设备启动文件版本一致。
- 堆叠环境下，请先卸载备板的特性文件，再卸载主板的特性文件。
- 删除正在使用的特性/补丁文件后，将导致文件不可卸载。
- 对启动文件进行操作 (导入、删除、安装、卸载和设置下次启动文件) 时，请不要对设备进行主备倒换。
- 当设备上存在主控板和业务板时，仅支持在主控板中导入启动文件。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置准备

在软件更新之前，需要完成启动文件的管理。在软件更新页面，可查看当前设备的软件版本、本次启动使用的软件列表以及下次启动主用的软件列表等信息。还可对启动文件进行导入、删除、安装、卸载以及设置为下次启动文件。

1. 选择“系统 >升级中心 > 软件更新”。
2. 单击<管理文件>按钮，进入管理启动文件页面。

表-1 管理启动文件

参数	说明
导入	导入启动文件到设备。支持导入后缀为.bin和.ipe的文件。如果导入后缀为.ipe的启 对该文件进行解压，以便保存解压后的.bin文件
删除	删除无用的启动文件
操作	包含如下功能： • 设置下次启动文件 • 安装特性/补丁文件 • 卸载特性/补丁文件

设置下次启动文件	指定设备下次启动时使用的文件。必须包含相同版本的boot文件和system文件。设 后，需要手工重启设备才可完成整个升级过程
安装特性/补丁文件	用于激活或升级特性/补丁文件。通过安装特性/补丁文件，可以实现在不中断系统运 系统软件进行安装。 • 设备可同时安装多个特性文件 • 如果需要安装新的补丁文件，需要先卸载旧的文件
卸载特性/补丁文件	当特性文件/补丁文件被卸载后，该文件将处于未激活状态，系统也将不再具备该文 但是文件仍然存在于存储介质上

设置启动文件

完成配置准备后，手工重启设备即可完成整个升级过程。

通过 ipe 文件方式升级

1. 选择“系统 >升级中心 > 软件更新” 。
2. 单击“设置启动文件“按钮，进入设置启动文件页面，启动文件类型选择 ipe 文件。
3. 单击<选择>按钮，选择待升级的 ipe 软件升级包。
4. 其他配置保持系统默认即可。
5. 单击<确定>按钮，进行软件升级。

通过 bin 文件方式升级

1. 选择“系统 >升级中心 > 软件更新”。
2. 单击“设置启动文件“按钮，进入设置启动文件页面，启动文件类型选择 bin 文件。
3. 单击<选择>按钮，选择待升级的 boot 启动文件及 system 启动文件。
4. （可选）如果 bin 文件大于磁盘剩余空间，建议勾选“自动删除当前所有启动文件”选项，删除当前所有启动文件。
5. 其他配置保持系统默认即可。
6. 单击<确定>按钮，进行软件升级。

License 配置

本帮助主要介绍以下内容：

- 特性简介
  - License 授权信息
  - License 的有效期
  - License 的状态
  - 临时 License 和正式 License
- 使用限制和注意事项
  - 通用注意事项
  - 对激活文件的要求
  - 升级特征库的要求
- vSystem 相关说明
- 配置指南
  - 配置准备
  - License 安装指南
  - 压缩 License 存储区

特性简介

用户需要为设备购买授权码、安装 License，才能使用设备上的指定特性。哪些特性需要安装 License 可通过 License 授权信息页面中的信息和设备实际支持的特性共同决定。

License 授权信息

关于各特性对应 License 的授权信息，请参见下表。各特性 License 的支持情况与设备型号有关，请以设备实际情况为准。

表-1 License 授权信息表

License 特性	授权功能	未安装 License	License 过期后	授权时间
ACG/APP	应用识别 （ACG与APP均表示应用识别功能，具体请以设备实际情况为准）	无法升级应用识别特征库	无法升级应用识别特征库	1年、3年
AV	防病毒	无法使用防病毒功能、无法升级防病毒特征库	可使用防病毒功能 无法使用防病毒云端查询、增强检测和联动沙箱功能、无法升	1年、3年

License 特性	授权功能	未安装 License	License 过期后	授权时间
			级防病毒特征库	
TI	威胁情报（包括IP信誉、URL信誉和域名信誉）	无法使用威胁情报功能、无法升级威胁情报特征库	可使用威胁情报功能 无法升级威胁情报特征库	1年、3年
IPS	入侵防御	无法使用入侵防御功能、无法升级入侵防御特征库	可使用入侵防御功能 无法升级入侵防御特征库	1年、3年
WAF	Web应用防护	无法使用Web应用防护功能、无法升级Web应用防护特征库	可使用Web应用防护功能 无法升级Web应用防护特征库	1年、3年
Web Cache	Web Cache	重启设备会自动删除Web Cache的相关配置	重启设备会自动删除Web Cache的相关配置	1年、3年

License 的有效期

License 的有效期分为：永久（Permanent）、绝对时间（Date restricted）和相对时间（Days restricted）三种。

- 永久 License 没有使用时间限制，永远有效。

- 绝对时间 License 在 License 指定时间之内使用有效，超出该时间范围无效。例如，2015-05-01 到 2015-05-30。
- 相对时间 License 则是允许从 License 安装之日开始使用一段时间，例如，30 天。

License 的状态

License 的状态分为：In use、Usable、 Expired、Uninstalled、Unusable 和 Invalid。关于各状态的说明信息，请参见下表。

表-2 License 的状态

License 的状态	说明
In use	当前License正在使用
Usable （绝对时间License）	未到启用时间
Usable （相对时间License）	当前License正在等待使用（当设备同时安装了多个相对时间License，且多个License均支持某一特性时，则只有一个License中的该特性处于In use状态，其它License中的该特性会处于Usable状态）
Expired	当前License已过期
Uninstalled	当前License已卸载
Unusable	当前License无法使用

License 的状态	说明
Invalid	不合法的数据，无法使用

临时 License 和正式 License

License 根据发布渠道不同分为临时的（Trial）和正式的（Formal），License 的种类以 License 的描述信息为准。

- 临时 License 授权的特性可以使用一段时间，临时 License 不允许迁移。请在试用期内购买正式 License 并安装到设备上，以便特性得到正式授权使用。
- 正式 License 是对特性正式授权的凭证。用户将正式 License 安装到设备上后，对特性进行正式授权，可以正常使用相应特性。

使用限制和注意事项

通用注意事项

- 对于一台设备，请不要多个用户同时进行 License 操作，以免操作失败。

- 正式 License 过期后不能卸载。过期后的 License 会一直占用 License 存储区。如果 License 存储区空间耗尽，会导致新的 License 安装失败。
- 压缩 License 存储区可以释放 License 存储空间。执行压缩操作时，系统会自动将已经过期的或者卸载的 License 信息删除，并修改 DID。因此：
    - 建议用户申请 License 前，先通过压缩页面查看可安装 License 的数目和已安装 License 的数目，申请的 License 数量和已安装 License 的数目之和不能大于可安装 License 的数目。
    - 在压缩 License 存储区前，请备份卸载码，并确保使用旧 DID 申请的 License 已经安装完毕，否则，License 存储区压缩后，使用旧 DID 申请的 License 将无法继续安装。
- 用户在安装 License 时，系统会自动搜索存储介质上是否存在该 License 对应的软件包，如果存在一个，则直接自动安装该软件包；如果存在多个，则直接自动安装最先搜索到的软件包。
- 用户在卸载 License 时，系统会自动搜索该 License 对应的软件包是否在运行，如果正在运行，则会直接自动卸载该软件包。
- 如果由于 HTTP 客户端的系统、浏览器等原因导致没有获取到激活文件，且无法重新申请激活文件时，请联系技术支持人员。
- “授权内容”列显示的起始时间为最近一次在官网申请激活文件的时间，并非首次激活 License 的时间。

对激活文件的要求

- 用户获取到激活文件之后请妥善保存并备份，以免不慎丢失。
- 请不要打开 DID 文件和激活文件，以免影响文件的格式，导致文件无效。
- 请不要修改 DID 文件和激活文件的名称，以免影响授权。
- 请不要删除设备上处于 In use 或 Usable 状态的激活文件，以免影响对应特性的正常运行。如果误删了这样的激活文件，请手工将备份的激活文件拷贝到 License 文件夹下进行恢复。如果恢复激活文件后，License 已处于 In use 状态，但某些需要该 License 的特性仍然不能正常使用，请重启设备来进行修复。

升级特征库的要求

License 过期后，设备中已有的特征库可正常工作，但无法升级到 license 有效期之后发布的新版本的特征库。仅当对应功能的的 License 处于 In use 状态时，才可进行特征库升级。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

License 安装指南

用户需要为每个位置上的硬件分别安装 License。安装 License 的时候，必须选择位置。请为每个位置上的硬件分别购买授权码，使用这个位置上硬件的 SN 和 DID 申请激活文件，并将激活文件安装在这个位置的硬件上，该硬件才能获得授权，可以运行指定的特性。已经获得授权的硬件插入其它设备时，仍然具有同样的授权。

- 通过 License 配置菜单查看哪些特性需要安装 License、是否已经安装 License、以及已安装的 License 的简要信息。
- 购买授权书，获得授权码。
- 选择“系统 > License 配置”。在“License 配置”页面，单击<获取设备信息文件（DID）文件>按钮，获取设备的 DID 文件和 SN。
- 根据产品类型、授权码、SN 和 DID 文件申请激活文件。
- 在“License 配置”页面，单击<安装>按钮，安装激活文件，获得授权。

压缩 License 存储区

在申请 License 授权之前，需要确保 License 存储区有足够的空间来存储 License 的相关信息。如果 License 存储区的空间不足，请压缩 License 存储区，系统会自动将已经过期的或者卸载的 License 信息删除。

1. 选择“系统 > License 配置”。
2. 在“License 配置”页面，单击<压缩 License 存储区>按钮，设备会尝试与特征库服务器建立连接，并返回连接状态的结果。

会话设置

本帮助主要介绍以下内容：

- 特性简介
  - 会话管理的工作原理
  - 会话管理在设备上的实现
  - 会话类型
- 使用限制和注意事项
- 配置指南
  - 配置准备
  - 修改协议会话老化时间
  - 修改应用会话老化时间
  - 配置高级设置

特性简介

会话管理是为了实现基于会话进行处理的业务而抽象出来的公共功能。此功能把传输层报文之间的交互关系抽象为会话，并根据发起方和响应方的报文信息对会话进行状态更新和老化，支持多个业务特性分别对同一个业务报文进行处理。

会话管理的工作原理

会话管理主要基于传输层协议对报文进行检测。其实质是通过检测传输层协议信息来对连接的状态进行跟踪，并对所有连接的状态信息进行基于会话表和关联表的统一维护和管理。

客户端向服务器发起连接请求报文的时候，系统会创建一个会话表项。该表项中记录了一个会话所对应的请求报文信息和回应报文信息，包括源 IP 地址/端口号、目的 IP 地址/端口号、传输层协议类型、应用层协议类型、会话的协议状态等。对于多通道协议（特指部分应用协议中，客户端与服务器之间需要在已有连接基础上协商新的连接来完成一个应用），会话管理还会根据协议的协商情况，创建一个或多个（由具体的应用协议决定）关联表表项，用于关联属于同一个应用的不同会话。关联表表项在多通道协议协商的过程中创建，当有报文匹配某一条关联表表项后会创建相应的子会话，完成对多通道协议的支持后即被删除。

上述会话管理的工作原理描述仅针对目的地址为单播地址的报文，对于目的地址是组播地址的报文稍有不同。组播报文到达设备后通常经由一个入接口到多个出接口进行转发，因此对于同一个应用的组播报文的连接，在入接口和多个出接口均会建立起各自的会话表项，我们称这类组播报文触发

建立的会话表项为组播会话表项，以区别于单播报文触发建立的单播会话表项。若无特殊说明，本文中的会话表项不区分单播和组播类型。

在实际应用中，会话管理作为公共功能，只能实现连接状态的跟踪，并不能单独实现某一具体功能，需要与其他业务模块配合使用。

会话管理在设备上的实现

目前会话管理在设备上实现的具体功能如下：

- 支持对各协议报文创建会话、更新会话状态以及根据协议状态设置老化时间。
- 支持应用层协议的端口映射（参见“应用安全”中的“应用识别联机帮助”），允许为应用层协议自定义对应的非通用端口号，同时可以根据应用层协议设置不同会话老化时间。
- 支持 ICMP/ICMPv6 差错报文的映射，可以根据 ICMP/ICMPv6 差错报文携带的信息查找原始的会话。
- 支持应用层协议（如 FTP）的控制通道和动态数据通道的会话管理。

会话类型

设备对报文的处理分为慢速转发处理和快速转发处理两个阶段。一条数据流的首报文首先会在设备上进行慢速转发处理，设备根据慢速转发处理结果会为此条数据流创建对应的会话表项。此条数据

流的后续报文将直接匹配对应的会话表项进入快速转发阶段，设备根据此阶段的处理结果实现对报文的快速放行或丢弃。根据是否允许报文通过，可将会话分为放行会话和丢包会话两种。

放行会话

若一条数据流的首报文经过设备处理之后被放行，则设备会为此条数据流生成会话表项，用于快速放行此条数据流的后续报文，我们将此类会话表项称之为放行会话。

在实际应用中，放行会话其本身只能实现连接状态的跟踪，并不能阻止潜在的攻击报文通过。会话配合具体安全业务特性，可实现是否允许报文通过设备。

丢包会话

若一条数据流的首报文经过设备处理之后被丢弃，则设备会为此条数据流生成会话表项用于快速丢弃此条数据流的后续报文，我们将此类会话表项称之为丢包会话。

关闭丢包会话功能后，对于设备丢弃的报文将不能生成丢包会话。

除非特别说明，本文的会话均指放行会话。

使用限制和注意事项

- 应用的会话老化时间仅在会话进入稳态时生效（TCP 会话的稳态为 TCP-EST，UDP 会话的稳态为 UDP-READY）。

- 会话进入稳态后，如果该会话属于设备上应用会话老化时间中的应用，则此会话的老化时间为指定的此应用会话的老化时间；否则为传输层协议状态的会话老化时间。
- 丢包会话功能仅支持 ASPF 和并发连接限制模块丢弃报文时生成丢包会话，其他模块丢弃报文时不能生成丢包会话。
- 如果未开启设备的丢包会话硬件转发功能，丢包会话处理将仅通过 CPU 进行软件丢包，不会通过硬件快速丢包。为了充分利用设备的硬件处理能力，管理员可通过在 CLI 窗口执行 `session fast-drop hardware-fast-forwarding` 命令开启丢包会话的硬件快速转发功能。需要注意的是，丢包会话的硬件快速转发功能的支持情况与设备型号有关，请以设备实际支持情况为准。
- 丢包会话不支持会话业务热备份功能。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。

- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

修改协议会话老化时间

该功能用于实现根据会话所处协议状态来设置会话表项的老化时间。处于某协议状态的会话，如果在该协议状态老化时间内未被任何报文匹配，则会由于老化而被系统自动删除。

修改协议会话老化时间的具体配置步骤如下：

1. 单击“系统 > 会话设置 > 协议会话老化时间”，进入修改协议会话老化时间页面。
2. 单击指定协议的编辑按钮，即可修改老化时间或恢复缺省老化时间。

修改应用会话老化时间

对于处于 TCP-EST 状态的 TCP 会话以及处于 UDP-READY 状态的 UDP 会话，根据所属的应用层协议类型或应用的老化时间进行老化，老化时间可配置。对于进入稳定状态的其它应用层协议的会话，则仍然遵循协议状态的会话老化时间进行老化。

修改应用会话老化时间的具体配置步骤如下：

1. 单击“系统 > 会话设置 > 应用会话老化时间”，进入修改应用会话老化时间页面。
2. 单击指定应用的编辑按钮，即可修改老化时间。

配置高级设置

高级设置的具体配置步骤如下：

1. 单击“系统 > 会话设置 > 高级设置”，进入高级设置页面。

2. 选择开启“会话统计”、“丢包会话”按钮以启用会话统计功能、丢包会话功能。

设备信息

特性简介

设备信息用于查看当前设备的名称、所在位置、联系方式信息。

配置指南

选择“系统 > 系统与维护 > 系统设置 > 设备信息”，进入设备信息页面，可配置当前设备的名称、所在位置、联系方式信息。

日期和时间

本帮助主要介绍以下内容：

- 特性简介
  - 日期和时间配置方式
  - NTP/SNTP 简介
  - NTP/SNTP 时钟源工作模式
  - NTP/SNTP 时钟源身份验证
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 手工设置日期和时间
  - 自动同步网络日期和时间

特性简介

日期和时间配置方式

为了便于管理，并保证与其它设备协调工作，设备需要准确的系统时间。

系统时间的配置方式有：

- 手工设置日期和时间。用户手工指定的时间即为当前的系统时间，不管是否同时修改了时区和夏令时。后续，设备使用内部晶体震荡器产生的时钟信号计时。如果用户没有手工配置系统时间，仅修改了时区或夏令时，设备会使用新时区和夏令时来调整系统时间。
- 自动同步网络日期和时间。设备使用协议周期性地同步服务器的 UTC（Coordinated Universal Time，国际协调时间）时间，并用同步得到的 UTC 时间和设备上配置的时区、夏令时参数进行运算，得出当前的系统时间。如果用户修改了时区或夏令时，设备会重新计算系统时间。该方式获取的时间比手工配置的时间更精准，推荐使用。

全球分为 24 个时区。请将设备的时区配置为当地地理时区。

在执行夏令时制的国家/地区需要配置夏令时。夏令时会相对非夏令时提前 1 小时，开始时间、结束时间和您所处国家/地区的夏令时要求一致即可。（如果夏令时开始时刻到达时，页面显示的系统时间没有加一，请刷新页面查看效果）。

NTP/SNTP 简介

NTP（Network Time Protocol，网络时间协议）可以用来在分布式时间服务器和客户端之间进行时间同步，使网络内所有设备的时间保持一致，从而使设备能够提供基于统一时间的多种应用。

SNTP（Simple NTP，简单 NTP）采用与 NTP 相同的报文格式及交互过程，但简化了 NTP 的时间同步过程，以牺牲时间精度为代价实现了时间的快速同步，并减少了占用的系统资源。在时间精度要求不高的情况下，可以使用 SNTP 来实现时间同步。

NTP/SNTP 时钟源工作模式

NTP 支持服务器模式和对等体模式两种时钟源工作模式，如下表所示。在服务器模式中，设备只能作为客户端；在对等体模式中，设备只能作为主动对等体。

SNTP 只支持服务器模式这一种时钟源工作模式。在该模式中，设备只能作为客户端，从 NTP 服务器获得时间同步，不能作为服务器为其他设备提供时间同步。

表-1 时钟源工作模式表

模式	工作过程	时间同步方向	应用场
服务器模式	客户端上需要手工指定NTP服务器的地址。客户端向NTP服务器发送NTP时间同步报文。NTP服务器收到报文后会自动工	客户端能够与NTP服务器的时间同步 NTP服务器无法与客户端的时	该模式通常用于 备从上级的时间 取时间同步

	作在服务器模式，并回复应答报文 如果客户端可以从多个时间服务器获取时间同步，则客户端收到应答报文后，进行时钟过滤和选择，并与优选的时钟进行时间同步	间同步	
对等体模式	主动对等体（Symmetric active peer）上需要手工指定被动对等体（Symmetric passive peer）的地址。主动对等体向被动对等体发送NTP时间同步报文。被动对等体收到报文后会自动工作在被动对等体模式，并回复应答报文 如果主动对等体可以从多个时间服务器获取时间同步，则主动对等体收到应答报文后，进行时钟过滤和选择，并与优选的时钟进行时间同步	主动对等体和被动对等体的时间可以互相同步 如果双方的时钟都处于同步状态，则层数大的时钟与层数小的时钟的时间同步	该模式通常用于 备间互相同步， 级的设备间形成 果某台设备与所 间服务器的通 障，则该设备优 同级的时间服务 间同步

NTP/SNTP 时钟源身份验证

NTP/SNTP 时钟源身份验证功能可以用来验证接收到的 NTP 报文的合法性。只有报文通过验证后，设备才会接收该报文，并从中获取时间同步信息；否则，设备会丢弃该报文。从而，保证设备不会与非法的时间服务器进行时间同步，避免时间同步错误。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 对于服务器模式：要使用身份验证功能，必须在服务器端和客户端上都开启身份验证功能，并配置相同的密钥 ID 和密钥，否则身份验证失败或无法进行身份验证。
- 对于对等体模式：要使用身份验证功能，必须在主动对等体和被动对等体上都开启身份验证功能，并配置相同的密钥 ID 和密钥，否则身份验证失败或无法进行身份验证。

配置指南

手工设置日期和时间

当系统时间不准确，且无法访问互联网的情况下，设备无法通过网络时间协议（NTP）自动同步时间，此时可以手工设置日期和时间。

1. 选择“系统 > 系统与维护 > 系统设置 > 日期和时间”。

2. 在“日期和时间”页面勾选<手工设置日期和时间>按钮。

3. 在“手工设置日期和时间”页面的具体配置内容如下表所示：

表-2 系统时区和夏令时的详细配置

配置项	说明
时区	设置系统所在的时区
夏令时	设置根据夏令时制调整系统时钟，即在指定时间段内将系统的当前时间增加1小时 单击“根据夏令时调整时钟”前的复选框，展开夏令时生效时间段的配置内容。夏令时生效时间段的有两种配置方式： • 以 1 年为周期，每年从一个相对的起始日期和时间到一个相对的结束日期和时间的时间段内采用夏令时，该时间段必须大于 1 天且小于 1 年，如：每年从 8 月的第一周的周一 06:00:00 开始到 9 月的最后一周的周日 06:00:00 结束采用夏令时 • 从某一个年份开始，以 1 年为周期，每年从一个绝对的起始日期和时间到一个绝对的结束日期和时间的时间段内采用夏令时，该时间段必须大于 1 天且小于 1 年，如：从 2006 年开始每年 8 月 1 日 06:00:00 开始到 9 月 1 日 06:00:00 结束采用夏令时

4. 单击<应用>按钮，可完成手工设置日期和时间操作。

自动同步网络日期和时间

为了防止设备时间不准确，自动同步功能可确保设备始终保持准确的时间。

1. 选择“系统 > 系统与维护 > 系统设置 > 日期和时间”。

2. 在“日期和时间”页面勾选<自动同步网络日期和时间>按钮。

3. 在“自动同步网络日期和时间”页面的具体配置内容如下表所示：

表-3 自动同步网络日期和时间的详细配置

配置项	说明
系统时钟状态	显示系统时钟的同步状态
虚拟设备	下拉选择需进行时间同步的虚拟设备
同步时钟所使用的网络协议	指定使用协议，包括：网络时间协议（NTP）、简单网络时间协议（SNTP）
对时钟源进行身份验证	NTP/SNTP时钟源身份验证功能可以用来验证接收到的NTP报文的合法性，避免时间同步错误，需勾选
为NTP报文指定源接口	设置NTP报文的源接口（此配置项仅当勾选网络时间协议时需要配置） 如果不想让本地设备上其它接口的IP地址成为应答报文的目的地址，可以指定NTP报文的源接口，此时报文中的源IP地址为该接口的主IP地址。如果指定的源接口处于down状态，则发送的NTP报文源IP地址为该报文出接口的主IP地址

<table>
<tr><td>身份验证密钥ID和密钥</td><td colspan="2">单击<新建>后填写身份验证密钥ID和密钥后，单击<确定>完成NTP身份验证设置NTP验证密钥

在一些对安全性要求较高的网络中，运行NTP/SNTP协议时需要启用验证功能。通过客户端和服务器端的密钥验证，保证客户端只与通过验证的设备进行同步，提高了网络安全性

可以设置两个验证密钥，每个密钥由身份验证密钥ID和密钥组成：

• 身份验证密钥 ID 是密钥的编号
• 密钥为 MD5 验证密钥的字符串</td></tr>
<tr><td rowspan="5">时钟源</td><td colspan="2">用于配置VRF、IP地址、时钟源工作模式、身份验证密钥ID、NTP版本号</td></tr>
<tr><td>VRF</td><td>下拉选择VRF。可选择已有的VRF，如需新建VRF，具体的配置步骤请参见“网络 > VRF”</td></tr>
<tr><td>类型</td><td>• IP 地址：设置 NTP 服务器的 IP 地址
• 主机名：设置 NTP 服务器的主机名</td></tr>
<tr><td>时钟源工作模式</td><td>用户可以根据需要选择一种或几种工作模式进行时间同步。
• NTP 支持服务器模式和对等体模式两种时钟源工作模式
• SNTP 只支持服务器模式这一种时钟源工作模式</td></tr>
<tr><td>身份验证密钥ID</td><td>身份验证密钥ID是密钥的编号</td></tr>
<tr><td></td><td>NTP版本号</td><td>NTP协议的版本（现有版本1-4）</td></tr>
</table>

时区	设置系统所在的时区
夏令时	设置根据夏令时制调整系统时钟，即在指定时间段内将系统的当前时间增加1小时 单击“根据夏令时调整时钟”前的复选框，展开夏令时生效时间段的配置内容。夏令时生效时间段的有两种配置方式： • 以 1 年为周期，每年从一个相对的起始日期和时间到一个相对的结束日期和时间的时间段内采用夏令时，该时间段必须大于 1 天且小于 1 年，如：每年从 8 月的第一周的周一 06:00:00 开始到 9 月的最后一周的周日 06:00:00 结束采用夏令时 • 从某一个年份开始，以 1 年为周期，每年从一个绝对的起始日期和时间到一个绝对的结束日期和时间的时间段内采用夏令时，该时间段必须大于 1 天且小于 1 年，如：从 2006 年开始每年 8 月 1 日 06:00:00 开始到 9 月 1 日 06:00:00 结束采用夏令时

4. 单击<应用>按钮，可完成自动同步网络日期和时间操作。

跨三层 MAC 学习

本帮助主要介绍以下内容：

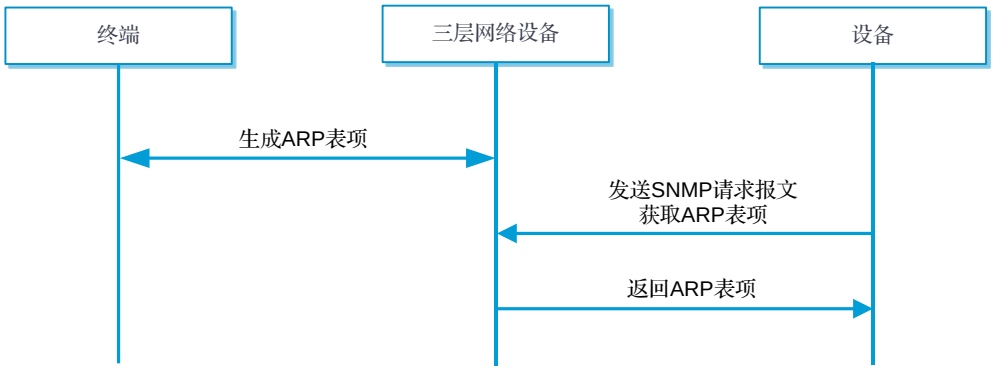
- 特性简介
- 使用限制和注意事项
- 配置指南
  - 配置准备
  - 开启跨三层 MAC 学习

特性简介

跨三层 MAC 学习功能是指当设备和终端（如 PC）之间有三层网络设备时，设备仍然可以学习到终端的 MAC 地址。

当终端采用动态 IP 地址访问网络时，使用 IP 地址作为过滤条件已经无法实现对网络流量的准确匹配和控制，此时需要使用 MAC 地址作为策略的过滤条件。但是在跨三层网络设备的组网环境中，设备无法直接获取终端的 MAC 地址，使用跨三层 MAC 学习功能可以获取终端的 MAC 地址。

图-1 跨三层 MAC 学习流程图



跨三层 MAC 学习具体流程如下：

1. 三层网络设备（一般为网关设备）学习终端的 IP-MAC 映射关系，生成 ARP 表项；
2. 设备定期向三层网络设备发送 SNMP 请求报文，获取其 ARP 表项；
3. 三层网络设备响应 SNMP 请求报文，返回 ARP 表项；
4. 设备收到 ARP 表项后将其保存在内存中，最终学习到终端的 MAC 地址。

使用限制和注意事项

- 跨三层 MAC 学习功能目前仅支持学习 IPv4 地址映射的 MAC 地址。
- 在使用跨三层 MAC 学习功能时，设备与目标三层网络设备之间不能跨越 NAT。
- 跨三层 MAC 学习功能不支持在 VRF 网络环境中使用。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。
- 需要保证组网中与设备对接的三层网络设备已开启 SNMP Agent 服务，已配置团体名且支持 SNMP v2c 或 SNMP v3 版本。

开启跨三层 MAC 学习

当终端采用动态 IP 地址访问网络时，使用 IP 地址作为过滤条件已经无法实现对网络流量的准确匹配和控制，此时需要使用 MAC 地址作为策略的过滤条件。但是在跨三层网络设备的组网环境中，设备无法直接获取终端的 MAC 地址，使用跨三层 MAC 学习功能可以解决此问题。

1. 选择“系统 > 系统与维护 > 跨三层 MAC 学习 > 三层设备访问设置”。

2. 在“三层设备访问设置”页面开启跨三层 MAC 学习功能。

3. 配置访问目标三层网络设备的时间间隔和超时时长，具体内容如下表所示。

表-1 配置访问目标三层网络设备的时间间隔和超时时长参数表

参数	说明
SNMP请求的时间间隔	配置发送SNMP请求报文的时间间隔，单位为秒
等待SNMP响应的超时时间	配置等待SNMP响应报文的超时时间，单位为秒

4. 单击<应用>按钮。

5. 在“三层设备访问设置”页面的三层设备列表下，单击<新建>按钮。

6. 在“新建三层设备”页面配置三层设备信息，具体内容如下表所示。

表-2 新建三层设备

认证方式	说明
SNMP版本	配置SNMP协议使用的版本，其包括v2c和v3版本
三层设备IP地址	配置目标三层网络设备的IP地址，一般为终端网络的网关设备，以获取 的ARP表。目前仅支持IPv4地址

团体名（v2c版本支持）	团体名相当于密码，团体内的设备通信使用团体名来进行认证。只有与 上SNMP Agent的团体名相同时，才能互相访问
用户名（v3版本支持）	只有与目标三层设备上SNMP Agent的用户名相同时，才能进行认证
认证方式	这几项信息的配置必须与目标三层设备上SNMP Agent的配置信息相同 成功进行互相访问
认证密码	
加密方式	
加密密码	

7. 单击<确定>按钮。

8. 学习完成后，选择“系统 > 系统与维护 > 跨三层 MAC 学习 > MAC 学习列表”，可查看学习记录，包含 IPv4 地址与 MAC 地址的映射关系，以及表项老化时间。

SNMP

特性简介

SNMP（Simple Network Management Protocol，简单网络管理协议）是互联网中的一种网络管理标准协议，广泛用于实现管理设备对被管理设备的访问和管理。SNMP 具有以下优势：

支持网络设备的智能化管理。利用基于 SNMP 的网络管理平台，网络管理员可以查询网络设备的运行状态和参数，配置参数值，发现故障，完成故障诊断，进行容量规划和制作报告。

支持对不同物理特性的设备进行管理。SNMP 只提供最基本的功能集，使得管理任务与被管理设备的物理特性和联网技术相对独立，从而实现对不同厂商设备的管理。

SNMP 的网络架构

SNMP 网络架构由三部分组成：NMS、Agent 和 MIB。

NMS（Network Management System，网络管理系统）是 SNMP 网络的管理者，能够提供友好的人机交互界面，方便网络管理员完成大多数的网络管理工作。

Agent 是 SNMP 网络的被管理者，负责接收、处理来自 NMS 的 SNMP 报文。在某些情况下，如接口状态发生改变时，Agent 也会主动向 NMS 发送告警信息。

MIB（Management Information Base，管理信息库）是被管理对象的集合。NMS 管理设备的时候，通常会关注设备的一些参数，比如接口状态、CPU 利用率等，这些参数就是被管理对象，在 MIB 中称为节点。每个 Agent 都有自己的 MIB。MIB 定义了节点之间的层次关系以及对象的一系列属性，比如对象的名称、访问权限和数据类型等。被管理设备都有自己的 MIB 文件，在 NMS 上编译这些 MIB 文件，就能生成该设备的 MIB。NMS 根据访问权限对 MIB 节点进行读/写操作，从而实现对 Agent 的管理。

SNMP 版本介绍

目前，设备支持 SNMPv1、SNMPv2c 和 SNMPv3 三种版本。只有 NMS 和 Agent 使用的 SNMP 版本相同，NMS 才能和 Agent 建立连接。

- SNMPv1 采用团体名（Community Name）认证机制。团体名类似于密码，用来限制 NMS 和 Agent 之间的通信。如果 NMS 配置的团体名和被管理设备上配置的团体名不同，则 NMS 和 Agent 不能建立 SNMP 连接，从而导致 NMS 无法访问 Agent，Agent 发送的告警信息也会被 NMS 丢弃。
- SNMPv2c 也采用团体名认证机制。SNMPv2c 对 SNMPv1 的功能进行了扩展：提供了更多的操作类型；支持更多的数据类型；提供了更丰富的错误代码，能够更细致地区分错误。
- SNMPv3 采用 USM（User-Based Security Model，基于用户的安全模型）认证机制。网络管理员可以配置认证和加密功能。认证用于验证报文发送方的合法性，避免非法用户的访问；

加密则是对NMS和Agent之间的传输报文进行加密，以免被窃听。采用认证和加密功能可以为 NMS 和 Agent 之间的通信提供更高的安全性。

vSystem相关说明

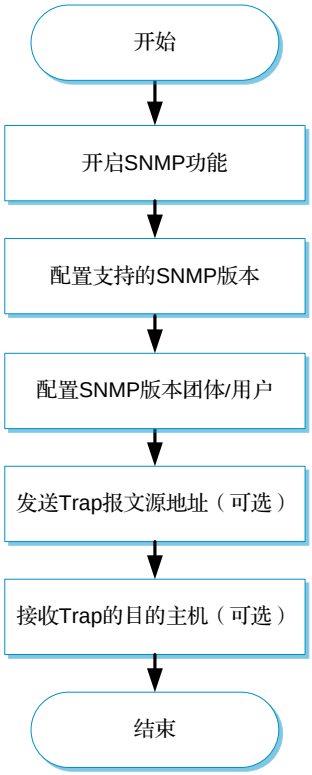
非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置思路

SNMP 的配置思路如下图所示：

图-1 SNMP 配置思路图



配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。

- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

SNMPv1/SNMPv2c 版本配置

SNMPv1 和 SNMPv2c 的配置方法相同。

SNMPv1/SNMPv2c 版本的具体配置步骤如下：

1. 单击“系统 > 系统与维护 > SNMP”。
2. 开启 SNMP 功能。
3. 配置 SNMP 版本及各版本公共信息。

表-1 SNMP 版本及各版本公共配置

参数	说明
版本	设置SNMP版本号，包括： • SNMPv1 • SNMPv2c • SNMPv3 设置指定的SNMP版本后，设备才能收发该版本的SNMP报文。只有NMS和Agent使用的SNMP版本相同，NMS才能和Agent建立连接。若同时配置多个版本，各版本配置均生效，设备会和NMS协商一个版本进行通信 SNMPv1和SNMPv2c报文中携带的团体名和数据均为明文形式，存在安全隐患，建议使用SNMPv3版本 如果在IPv6环境下，要使用SNMP告警功能，请将SNMP版本号配置为

	v2c或者v3
Trap报文源地址	使用指定接口的IP地址作为Trap报文的源IP地址 指定了接口后，系统会使用指定接口的主IP地址作为发送出去的告警信息的源IP地址。这样，在NMS上就可以使用该IP地址唯一标志Agent。即便Agent使用不同的出接口发送告警信息，NMS都可以使用该IP地址来过滤Agent发送的所有告警信息 在将某个接口配置为获取告警信息的源地址接口之前需要注意：如果配置的接口已经配置了合法的IP地址，则该IP地址将作为告警信息的源地址；如果配置的接口未配置合法的IP地址，则该命令不生效，在接口配置了合法IP地址后，本配置会自动生效
设备位置	配置设备的物理位置信息 为便于识别和管理设备，请使用本参数将设备所处的物理位置记录在设备中
联系信息	配置设备的维护联系信息 如果设备发生故障，设备维护人员可以利用设备的维护联系信息，及时与设备生产厂商取得联系

4. 单击<应用>按钮，使 SNMP 版本及各版本公共信息的配置生效。

5. 选择 SNMPv1 和 SNMPv2c 版本并进行配置。

表-2 SNMPv1 和 SNMPv2c 版本配置

参数	说明
SNMP只读团体名	SNMP的团体名，限制NMS访问Agent时所使用的团体名，区分大小写，需要转义的字符请加“\”后输入

	SNMP只读团体名对MIB对象的访问权限为只读，即NMS使用SNMP只读团体名访问Agent时只能执行读操作
SNMP读写团体名	SNMP的团体名，限制NMS访问Agent时所使用的团体名，区分大小写，需要转义的字符请加“\”后输入 SNMP读写团体名对MIB对象的访问权限为读写。即NMS使用SNMP读写团体名访问Agent时可以执行读、写操作
Trap接收主机	配置接收SNMP告警信息的目的主机。根据实际组网需要，管理员可以配置多个不同的Trap接收主机，使得设备可以向多个NMS发送告警信息。设备支持配置的目的主机属性包括： • 主机类型，包括： ○ IPv4 或 IPv6 地址：接收告警信息的目的主机的 IPv4 地址或 IPv6 地址 ○ IPv4 主机：接收告警信息的目的主机的主机名，发送时将获取主机名对应的 IPv4 地址，向对应的主机发送告警信息 ○ IPv6 主机：接收告警信息的目的主机的主机名，发送时将获取主机名对应的 IPv6 地址，向对应的主机发送告警信息 • Trap 接收主机：接收告警消息的目的主机的 IP 地址或主机名。若使用 IPv6 地址配置，则不能为链路本地地址。若使用主机名配置，主机名不区分大小写，字符串仅可包含字母、数字、“-”、“_”或“.” • 团体名：配置 SNMPv1、SNMPv2c 的团体名作为 Trap 接收主机的认证参数 • 端口：目的主机上用来接收告警信息的端口号

6. 单击<应用>按钮，使 SNMP 版本配置生效。

SNMPv3 版本配置

1. 配置 SNMP 版本及各版本公共信息，配置请参见表-1。
2. 单击<应用>按钮，使 SNMP 版本及各版本公共信息的配置生效。
3. 选择 SNMPv3 版本并进行版本配置。

表-3 SNMPv3 版本配置

参数	说明
安全用户名	SNMPv3用户名，区分大小写 配置的安全用户名若有变化，则认证密码和加密密码需要重新输入
认证算法	配置SNMPv3认证算法，包括： • MD5：采用 HMAC-MD5 算法 • SHA：采用 HMAC-SHA1 算法
认证密码	认证密码，区分大小写 认证密码必须和NMS上的一致才能建立SNMP连接
加密算法	配置SNMPv3加密算法，包括： • DES：采用 DES（Data Encryption Standard，数据加密标准）算法，密钥长度为 56 比特 • AES128：采用 AES（Advanced Encryption Standard，高级加密标准）算法，密钥长度为 128 比特 • 3DES：采用 3DES（Triple Data Encryption Standard，三重数据加

	密标准）算法，密钥长度为 168 比特
加密密码	加密密码，区分大小写 加密密码必须和NMS上的一致才能建立SNMP连接
Trap接收主机	配置接收SNMP告警信息的目的主机。根据实际组网需要，管理员可以配置多个不同的Trap接收主机，使得设备可以向多个NMS发送告警信息。设备支持配置的目的主机属性包括： • 主机类型，包括： ○ IPv4 或 IPv6 地址：接收告警信息的目的主机的 IPv4 地址或 IPv6 地址 ○ IPv4 主机：接收告警信息的目的主机的主机名，发送时将获取主机名对应的 IPv4 地址，向对应的主机发送告警信息 ○ IPv6 主机：接收告警信息的目的主机的主机名，发送时将获取主机名对应的 IPv6 地址，向对应的主机发送告警信息 • Trap 接收主机：接收告警消息的目的主机的 IP 地址或主机名。若使用 IPv6 地址配置，则不能为链路本地地址。若使用主机名配置，主机名不区分大小写，字符串仅可包含字母、数字、“-”、“_”或“.” • 安全用户名：配置SNMPv3的安全用户名作为Trap接收主机的认证参数 • 端口：目的主机上用来接收告警信息的端口号

4. 单击<应用>按钮，使 SNMP 版本配置生效。

配置文件

本帮助主要介绍以下内容：

- 特性简介
  - 配置文件概述
  - 配置的类型
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 保存当前配置
  - 导出与导入配置
  - 恢复出厂配置
  - 备份当前配置
  - 配置回滚

特性简介

配置文件概述

配置文件是用来保存配置的文件。配置文件主要用于：

- 保存当前配置，以便设备重启后，这些配置能够继续生效。
- 使用配置文件，用户可以非常方便地查阅配置信息。
- 当网络中多台设备需要批量配置时，可以将相同的配置保存到配置文件，再上传/下载到所有设备，在所有设备上执行该配置文件来实现设备的批量配置。

配置的类型

出厂配置

设备在出厂时，通常会带有一些基本的配置，称为出厂配置。它用来保证设备在没有配置文件或者配置文件损坏的情况下，能够正常启动、运行。

启动配置

设备启动时运行的配置即为启动配置。如果没有指定启动配置文件或者启动配置文件损坏，则系统会使用出厂配置作为启动配置。

当前配置

系统当前正在运行的配置称为当前配置。它包括启动配置和设备运行过程中用户进行的配置。当前配置存放在设备的临时缓存中，如果不保存，设备运行过程中用户进行的配置在设备重启后会丢失。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

在高可靠性的双机热备组网环境中，配置回滚完成后，需要在主管理设备的高可靠性功能页面单击<手工同步配置信息>按钮，将主管理设备上的配置信息手工批量备份到从管理设备，以保证主备设备的配置信息一致。

配置指南

保存当前配置

保存配置前，配置仅保存在内存中，设备重启后，设备将恢复为出厂配置。如果要使当前配置在设备重启后仍然生效，则需要将当前配置保存到下次启动配置文件中。

1. 选择“系统 > 系统与维护 > 配置文件”。
2. 在“配置文件”页面单击<保存当前配置>按钮。
3. 在“保存当前配置”页面的具体配置内容如下表所示：

表-1 配置信息

参数	说明
以原文件名保存	配置文件名默认以startup.cfg保存
以指定文件名保存	配置文件名可自行编辑命名，名称中可以包含数字、字母或特殊字符（除了*|\/?<>":）

4. 单击<确定>按钮，可完成保存并设置为下次启动配置文件操作。

导出与导入配置

保存配置后，可选则导出当前步骤将当前设备的设置和参数保存为一个文件。以后需要再配置这些设置和参数时，只需通过导入配置功能选择该文件，即可替换正在运行的配置。

1. 选择“系统 > 系统与维护 > 配置文件”。
2. 在“配置文件”页面单击<导出当前配置>按钮，可完成导出当前配置操作。
3. 在“配置文件”页面单击<导入配置>按钮。
4. 单击<选择>按钮，选中需要导入的配置文件，文件路径的总长度不能超过 255 个字符。
5. 单击<确定>按钮，可完成导入配置操作。

恢复出厂配置

恢复出厂配置模块提供将设备中的所有配置恢复到出厂时的缺省配置，删除当前的配置文件，并重新启动设备的功能。



恢复出厂配置后，设备会强制重启，设备当前的配置将会全部丢失，重启后，请根据出厂配置重新进行

1. 选择“系统 > 系统与维护 > 配置文件”。
2. 在“配置文件”页面单击<恢复出厂配置>。

3. 单击确定后，可完成恢复出厂配置操作。

备份当前配置

备份当前配置功能主要用于备份设备当前的配置信息，以便在需要时对设备配置进行回滚。

本功能支持将设备配置信息备份在设备本地或者远端服务器上（FTP 服务器、TFTP 服务器、SCP 服务器、SFTP 服务器），可立即备份也可周期性自动备份。

1. 选择“系统 > 系统与维护 > 配置文件”。

2. 在“配置文件”页面单击<备份当前配置>按钮。

3. 配置备份信息，具体内容如下表所示：

表-2 备份信息

参数	说明
备份方式	备份文件的存放位置，包括“备份至本地”、“备份至服务器”和“不备份”
自动备份周期	自动备份的时间间隔，若不配置该参数则不进行自动周期备份
最大备份文件数	本地可存放的备份文件数，若备份文件数到达该数值，新的备份文件会自动替换最早的备份文件
本地备份路径	指备份文件存放在设备本地已创建的路径

前缀名	备份文件的前缀名，备份文件命名方式为：“前缀名_编号.cfg”
立即备份	是否立即对设备当前配置进行备份
服务器类型	存放备份文件的服务器类型，包括“FTP”、“TFTP”、“SCP”和“SFTP”四种服务器类型
地址	存放备份文件的服务器的IP地址
VRF	服务器所属的VRF
用户名	访问FTP/TFTP/SCP/SFTP服务器的用户名
密码	访问FTP/TFTP/SCP/SFTP服务器的密码
端口	FTP/TFTP/SCP/SFTP服务器对外提供服务的端口号
备份路径	备份文件在服务器上的存放路径
不备份	删除<备份当前配置>页面已配置的备份信息

4. 单击<确定>按钮，可完成备份设备当前配置操作。

配置回滚

配置回滚功能主要用于通过配置备份文件将设备回滚至备份时的配置状态。

配置回滚功能支持从本地或者服务器上（FTP/TFTP）获取配置文件对设备配置进行回滚，若从服务器上获取配置文件，需指定时间进行配置回滚。



- 配置回滚是在不重启设备的情况下，将当前的配置回退到指定配置文件中的配置状态，回滚前的配
  失。配置回滚过程中，可能会导致业务中断，请谨慎使用。
- 若采用备份至服务器方式或从服务器上获取配置文件对设备进行配置回滚，需保证当前设备可正常
  器的 FTP/TFTP 服务。

1. 选择“系统 > 系统与维护 > 配置文件”。
2. 在“配置文件”页面单击<配置回滚>按钮。
3. 选择回滚文件来源：
   - 本地：点击回滚文件对应的“回滚”链接即可将设备配置回滚至指定文件。
   - 服务器：配置如下参数，然后单击<确定>按钮即可从服务器上获取配置文件进行配置回滚。

表-3 配置回滚（回滚文件来源于服务器）

参数	说明
服务器类型	存放备份文件的服务器类型，包括“FTP”和“TFTP”两种服务器
地址	存放备份文件的服务器的IP地址
VRF	服务器所属的VRF

用户名	访问FTP/TFTP服务器的用户名
密码	访问FTP/TFTP服务器的密码
端口	FTP/TFTP服务器对外提供服务的端口号
回滚文件路径	回滚文件在服务器上的存放路径
默认回滚文件	若不配置“回滚文件”，则会采用“默认回滚文件”进行回滚
回滚文件	对设备进行回滚的配置文件名称
指定日期	指定对设备配置进行回滚的日期
指定时间	指定对设备配置进行回滚的时间，若配置了指定日期，则必须配置指
取消服务器回滚	勾选该选项可取消指定时间从服务器上获取配置文件进行回滚

重启

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 使用限制和注意事项
- 配置指南
  - 重启设备

特性简介

重启功能用于远程重新启动设备并重新引导系统文件。在重启设备前建议保存设备配置，以免配置丢失。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

使用限制和注意事项

- 如果设备在准备重启时，用户正在进行文件操作，为了安全起见，系统将不会执行此次重启操作。
- 设备重启会导致业务中断，请慎重操作。

配置指南

重启设备

通过断电后重新上电来重启设备对设备影响较大，如果对运行中的设备进行强制断电，可能会造成数据丢失。采用重启功能，不需要到设备所在地便可进行重启。

1. 单击“系统 > 系统与维护 > 重启”。
2. 在“重启”页面单击<重启设备>按钮。
3. 重启设备前选择配置的保存方式。
4. 具体参数说明如下表所示：

表-1 重启设备配置

参数	说明
保存当前Context配置	将设备上当前context内的配置保存到设备的文件系统中
保存所有Context配置	将设备上所有context内的配置保存到设备的文件系统中
不保存配置	对配置不执行保存操作



当前配置存放在设备的临时缓存中，如果不保存，设备运行过程中用户进行的配置在设备重启后会丢失。

5. 选择保存方式，单击<确定>按钮，设备重启。

关于

特性简介

用于查看当前设备的名称、序列号、型号、描述、所在位置、联系方式、软件版本、厂商等信息。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

查看本设备信息

1. 选择“系统 > 系统与维护 > 关于 > 本设备”。
2. 在“本设备”页面，可查看当前设备名称、设备序列号、设备型号等信息。

查看版本信息

1. 选择“系统 > 系统与维护 > 关于 > 版本信息”。
2. 在“版本信息”页面，可查看当前设备软件版本和硬件规格等信息。

查看电子标签

1. 选择“系统 > 系统与维护 > 关于 > 电子标签”。
2. 在“电子标签”页面，可查看当前设备型号、生产序列号、MAC 地址等信息。

查看法律声明

1. 选择“系统 > 系统与维护 > 关于 > 法律声明”。
2. 在“法律声明”页面，可查看本设备的版权信息以及第三方软件的版权和许可信息。

智能业务平台

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 配置指南
  - 配置准备
  - 配置智能业务平台

特性简介

智能业务平台用于实现防病毒的增强检测以及 DGA 域名检测功能。如需实现上述功能，则需要保证设备已与智能业务平台成功连接。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。
- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置智能业务平台

智能业务平台的具体配置步骤如下：

1. 选择“系统 > 智能业务平台”。
2. 配置平台的 IPv4 地址。
3. 单击<应用>按钮，即可完成智能业务平台的配置。

快速接入 Internet

特性简介

快速接入 Internet 用于配置设备方便快速的接入 Internet。

接入模式

接入模式分为路由模式和透明模式。

路由模式

路由模式使用设备网关的路由功能。在该模式下，接入互联网的配置方式有如下几种，请根据网络服务提供商提供给您的信息选择具体的配置。

- WAN 口配置
- LAN 口配置

透明模式

透明模式不改变原有的网络结构，被配置为 WAN 口或 LAN 口的接口会成为二层接口。

使用限制和注意事项

再次配置快速接入 Internet 时,此前已下发的配置不会清空,仅会根据本次的配置增加或修改已有配置。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置步骤

配置准备

在配置本特性之前，需要完成以下任务：

- 配置接口 IP 地址。接口在“网络 > 接口与 VRF > 接口”页面配置。

- 配置路由，保证路由可达。路由在“网络 > 路由”页面配置。
- 创建安全域。安全域在“网络 > 安全域”页面配置。
- 配置接口加入安全域。可在安全域页面添加接口，也可在接口页面选择接口所属的安全域。
- 配置安全策略，放行业务流量。安全策略在“策略 > 安全策略”页面配置。

配置路由模式接入互联网

路由模式的具体配置步骤如下：

1. 单击“系统 > 配置向导 > 快速接入 Internet”。
2. 选择“路由模式”，单击“开始配置”。
3. 配置 WAN 口接入互联网。

表-1 接入互联网方式说明

参数	说明
指定IP地址	如果您从网络服务提供商处获得一个固定的IP地址，请选择
DHCP	如果您从网络服务提供商（或DHCP服务器）自动获取IP地接类型

- 选择指定 IP 地址的方式接入互联网时，WAN 口各配置项参数的说明如下表所示。

表-2 指定 IP 地址方式

参数	说明
接口	选择WAN口
IP地址/掩码长度	WAN口的IP地址和掩码。此参数由网络服务提供商 进制表示（例如，10.1.1.1），掩码长度范围为1～3
默认路由	WAN口的默认路由下一跳的IP地址。内网用户访问 WAN口发送到默认路由下一跳，再由下一跳转发。 商提供，用点分十进制表示（例如，10.1.1.254）
网关	接口的网关地址
首选DNS服务器	首选DNS服务器的IP地址。有关DNS的详细介绍，请 此参数由网络服务提供商提供
备用DNS服务器	备用DNS服务器的IP地址。当首选DNS服务器故障时 服务器解析域名。此参数由网络服务提供商提供

- 选择通过 DHCP 自动获取 IP 地址的方式接入互联网时，WAN 口配置项参数的说明如下表所示。

表-3 通过 DHCP 自动获取 IP 地址方式

参数	说明
接口	选择WAN口

4. 单击“下一步”，配置 LAN 口。

表-4 LAN 口配置

参数	说明
接口	选择连接局域网的接口
IP地址/掩码长度	连接局域网接口的IP地址和掩码长度。IP地址用点分十进制 192.168.1.1），掩码长度范围为1～30
DHCP	开启该服务后，该局域网内的用户能自动获取IP地址。有关 绍，请参考“DHCP”的详细介绍
地址池名称	DHCP地址池名称
动态分配的地址段	分配给DHCP客户端的地址段

5. 单击“下一步”，核对配置信息。

6. 单击“完成”，完成路由模式的配置。

配置透明模式接入互联网

透明模式的具体配置步骤如下：

1. 单击“系统 > 配置向导 > 快速接入 Internet”，选择“透明模式”。

2. 单击“开始配置”，配置透明模式。

3. 配置接口模式。

表-5 透明模式配置项

参数	说明
WAN接口	选择WAN口
LAN接口	选择连接局域网的接口

4. 单击“确定”，完成透明模式的配置。

Web 界面定制

本帮助主要介绍以下内容：

- 特性简介
- vSystem 相关说明
- 配置指南

特性简介

本功能用于定制 Web 界面的展示内容，具体功能如下：

- 隐藏/显示功能配置页面：当管理员希望精简 Web 界面配置，仅展示常用功能和关键配置时，可根据实际需求配置 Web 界面显示或隐藏指定的功能，避免受到不必要配置信息的干扰，从而提升 Web 界面的易用性和操作效率。
- 精简日志配置：Web 界面中支持仅展示关键日志配置项，隐藏非必要的日志配置。以便管理员关注重点配置，提升配置效率。

vSystem相关说明

非缺省 vSystem 对于本特性的支持情况，请以页面的实际显示为准。

配置指南

Web 界面定制功能的配置步骤如下：

1. 单击“系统 > Web 界面定制”，进入 Web 界面定制页面。
2. 根据实际情况滑动开启或关闭指定的配置项。

表-1 Web 界面定制功能配置项

参数	说明
接口NAT	开启本功能后，Web界面中将展示接口NAT功能的配置页面 接口NAT功能通过创建并执行NAT规则来实现地址转换。该功能仅适用于 的场景，与策略NAT功能互斥。当设备中已配置策略NAT时，建议隐藏接 配置页面，避免配置冲突
虚拟设备	开启本功能后，Web界面中将展示虚拟设备功能的配置页面 虚拟设备功能用于通过虚拟化技术将一台物理设备划分成多台虚拟设备， 就称为一个Context，每个Context拥有自己专属的软硬件资源，独立运行
IRF	开启本功能后，Web界面中将展示IRF功能的配置页面

	IRF是一种软件虚拟化技术，可将多台设备虚拟化成一台设备。使用这种 集合多台设备的硬件资源和软件处理能力，实现多台设备的协同工作、 断维护 本功能的支持情况与设备型号有关，请以设备实际情况为准
日志配置精简	开启本功能后，Web界面中将仅展示关键的日志配置，隐藏非必要的日 理员关注重点配置，提升配置效率

故障处理

本帮助主要介绍以下功能的故障处理办法：

- 安全策略故障处理
- NAT 故障处理
- SSL VPN 故障处理
- 日志导入/导出故障处理

安全策略故障处理

安全策略故障处理章节主要介绍以下故障的处理办法：

- 网络互通
  - PC 与设备直连，无法 Ping 通设备
  - PC 通过设备与其他终端连接，无法互相访问
  - PC 通过设备与其他终端相连，已配置在同一安全域，无法互相访问

网络互通

PC 与设备直连，无法 Ping 通设备

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。

图-1 组网图



故障原因

安全设备必须先将与 PC 相连的接口加入某个安全域，并配置放行该安全域与 Local 安全域报文的安全策略，PC 才能正常访问设备。

故障处理步骤

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”。

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：

    - 源安全域：Trust
    - 名称：trust-local
    - 目的安全域：Local
    - 动作：允许
    - 源 IPv4 地址：10.1.1.2
    - 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：

    - 名称：local-trust
    - 源安全域：Local
    - 目的安全域：Trust
    - 动作：允许
    - 源 IPv4 地址：10.1.1.1

- 目的 IPv4 地址：10.1.1.2

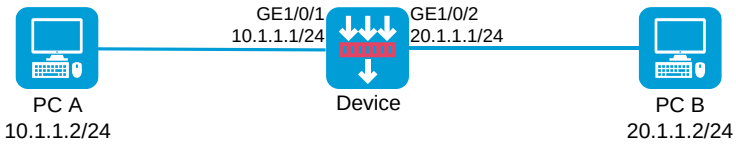
10. 单击<确定>按钮，完成配置。

PC 通过设备与其他终端连接，无法互相访问

故障描述

PC 通过设备与其他终端相连，IP 地址与路由已正确配置，但无法互相访问。

图-2 组网图



故障原因

安全设备必须先将接口加入相应的安全域，并配置放行对应安全域间报文的安全策略，流量才会被放行。

故障处理步骤

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”。

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）：

    - 名称：trust-untrust
    - 源安全域：Trust
    - 目的安全域：Untrust
    - 动作：允许
    - 源 IPv4 地址：10.1.1.2
    - 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：

    - 名称：untrust-trust
    - 源安全域：Untrust
    - 目的安全域：Trust

- 动作：允许
- 源 IPv4 地址：20.1.1.2
- 目的 IPv4 地址：10.1.1.2

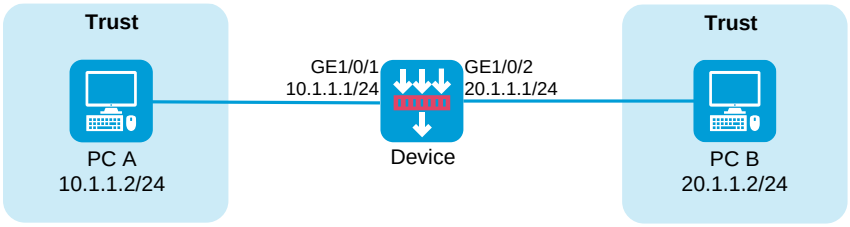
11. 单击<确定>按钮，完成配置。

PC 通过设备与其他终端相连，已配置在同一安全域，无法互相访问

故障描述

PC 通过设备与其他终端相连，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。

图-3 组网图



故障原因

安全设备缺省情况下，相同安全域间的报文是丢弃的，需要配置放行相应报文的安全策略，相同安全域的终端才能互相访问。

故障处理步骤

1. 登录设备 Web 管理页面。
2. 选择“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）：
    - 名称：trust-trust
    - 源安全域：Trust
    - 目的安全域：Trust
    - 动作：允许
    - 源 IPv4 地址：10.1.1.2,20.1.1.2
    - 目的 IPv4 地址：20.1.1.2,10.1.1.2
5. 单击<确定>按钮，完成配置。

NAT 故障处理

本帮助主要介绍以下故障的处理办法：

- 策略 NAT

- 内网用户无法访问外网
- NAT 源地址转换不生效
- NAT 目的地址转换不生效
- 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
- NAT 与 IPsec 配合使用，IPsec 配置不生效
- 配置策略 NAT 后，内网用户无法访问设备
- 配置 NAT 源地址转换后，外网用户无法访问设备
- 配置 NAT 目的地址转换后，外网用户无法访问设备

- 接口 NAT
  - 内网用户无法访问外网
  - NAT 源地址转换不生效
  - NAT 目的地址转换不生效
  - 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
  - NAT 与 IPsec 配合使用，IPsec 配置不生效
  - 配置 NAT 源地址转换后，外网用户无法访问设备
  - 配置 NAT 目的地址转换后，外网用户无法访问设备

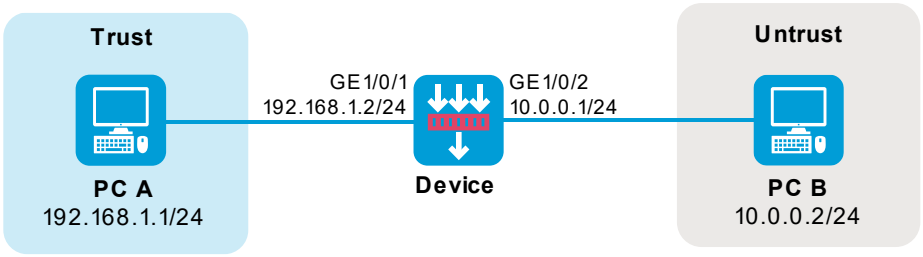
策略NAT

内网用户无法访问外网

故障描述

内网 PC A 无法通过网关设备 Device 访问外网 PC B。

图-4 组网图



故障原因

- 未配置允许 PC A 访问 PC B 的安全策略。
- 未配置策略 NAT 规则对报文源 IP 地址进行转换。

故障处理步骤（安全策略）

1. 登录设备 Web 管理页面。
2. 选择“策略 > 安全策略”。
3. 在“安全策略”页签单击<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：
    - 名称：secpolicy1
    - 源安全域： Trust
    - 目的安全域：Untrust
    - 动作：允许
    - 源 IPv4 地址：192.168.1.1（此处为 PC A 的 IP 地址）
    - 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。

故障处理步骤（策略 NAT）

1. 登录设备 Web 管理页面。
2. 选择“策略 > 策略 NAT”。
3. 单击<新建>，新建 NAT 策略规则，必要的配置项如下：
    - 规则名称：policy1

- 规则类型：NAT44
- 源安全域： Trust
- 目的安全域：Untrust
- 源 IPv4 地址：192.168.1.1（此处为 PC A 的 IP 地址）
- 目的 IPv4 地址：10.0.0.2（此处为 PC B 的 IP 地址）
- 源地址转换方式：动态 IP + 端口
- 地址类型：NAT 地址组
- 转换为地址：用于源 IP 地址转换的公网 NAT 地址组

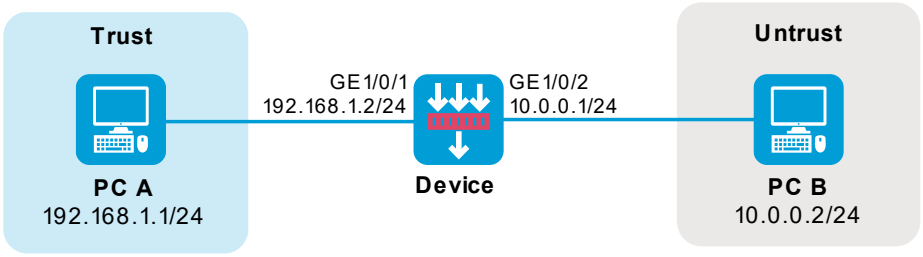
4. 单击<确定>，完成 NAT 策略规则配置。

NAT 源地址转换不生效

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。

图-5 组网图



故障原因

- 未配置允许 PC A 访问 PC B 的安全策略。
- 转换后源 IP 地址与 Device 的外网侧接口 IP 地址不在同一网段，导致回程报文不经过 Device。

故障处理步骤（安全策略）

1. 登录设备 Web 管理页面。
2. 选择“策略 > 安全策略”。
3. 在“安全策略”页签单击<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：
   - 名称：secpolicy2
   - 源安全域： Trust
   - 目的安全域：Untrust
   - 动作：允许

- 源 IPv4 地址：192.168.1.1（此处为 PC A 的 IP 地址）
- 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。

故障处理步骤（策略 NAT）

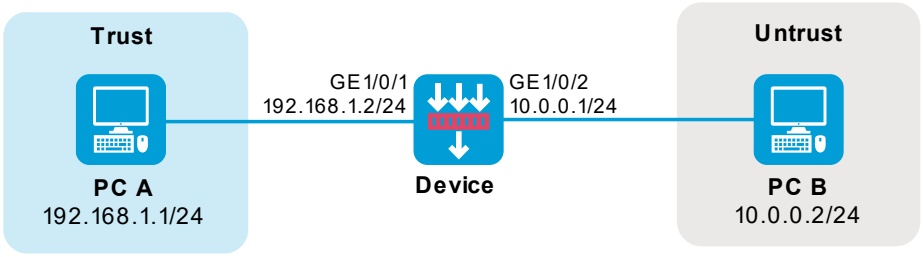
1. 登录设备 Web 管理页面。
2. 选择“策略 > 策略 NAT”。
3. 编辑 NAT 源地址转换规则。
4. 查看该规则的转换后 IP 地址、网段、地址对象组或 NAT 地址组中是否包含不在 10.0.0.1/24 网段内的地址。
5. 如存在上述情况，需修改转换后源地址配置，确保回程报文能被转发到 Device 的外网侧接口 GE1/0/2 上。
6. 单击<确定>，完成 NAT 策略修改。

NAT 目的地址转换不生效

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。

图-6 组网图



故障原因

- 未配置允许 PC B 访问 PC A 的安全策略。
- PC B 访问 PC A 所采用的服务与 NAT 目的地址转换配置不符，导致报文目的地址未被成功转换。

故障处理步骤（安全策略）

1. 登录设备 Web 管理页面。
2. 选择“策略 > 安全策略”。
3. 在“安全策略”页签单击<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：
    - 名称：secpolicy3
    - 源安全域： Untrust
    - 目的安全域：Trust

- 动作：允许
- 源 IPv4 地址：10.0.0.2（此处为 PC B 的 IP 地址）
- 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。

故障处理步骤（策略 NAT）

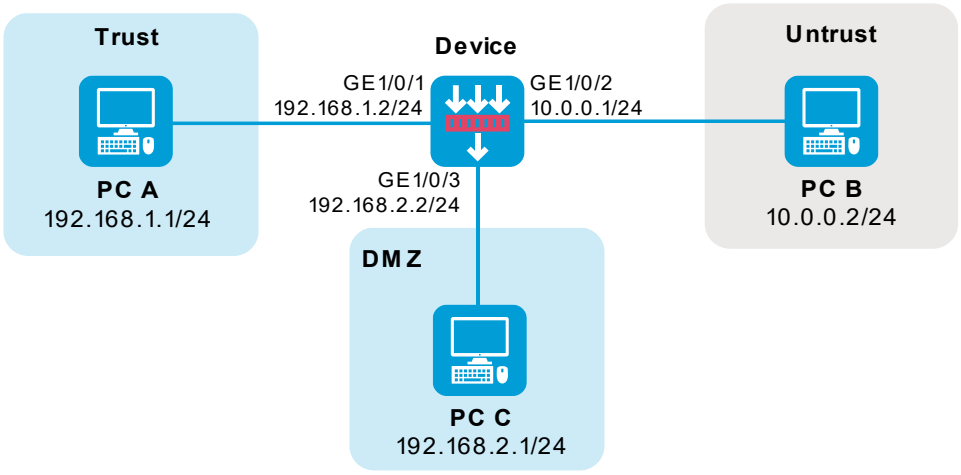
1. 登录设备 Web 管理页面。
2. 选择“策略 > 策略 NAT”。
3. 编辑 NAT 目的地址转换规则。
4. 查看该规则所引用的服务匹配条件是否与实际情况不符。
5. 如存在上述情况，需修改服务匹配条件，确保与实际情况一致。
6. 单击<确定>，完成 NAT 策略修改。

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

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。

图-7 组网图



故障原因

- 未配置允许 PC B 访问 PC C 的安全策略。
- NAT 源地址转换规则占用了 NAT 目的地址转换规则的 IP 地址和端口，导致 Device 访问 PC C 的流量匹配了 NAT 源地址转换规则而非 NAT 目的地址转换规则。

故障处理步骤（安全策略）

1. 登录设备 Web 管理页面。
2. 选择“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：
    - 名称：secpolicy4

- 源安全域： Untrust
- 目的安全域：DMZ
- 动作：允许
- 源 IPv4 地址：10.0.0.2（此处为 PC B 的 IP 地址）
- 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。

故障处理步骤（策略 NAT）

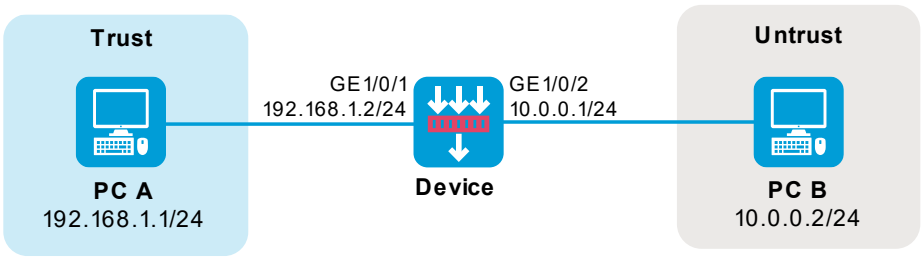
1. 登录设备 Web 管理页面。
2. 选择“策略 > 策略 NAT”。
3. 查看是否存在转换方式为动态 IP 的源地址转换规则。
4. 如存在上述规则，单击<编辑>，在修改 NAT 策略界面查看该规则引用的 NAT 地址组的端口范围是否包含 80。
5. 如包含在内，需要将端口 80 从端口范围中剔除。
6. 单击<确定>，完成 NAT 策略修改。

NAT 与 IPsec 配合使用，IPsec 配置不生效

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。

图-8 组网图



故障原因

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。

故障处理步骤

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。

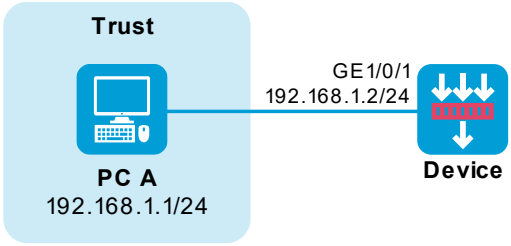
4. 查看 IPsec 策略配置中的被保护数据流配置，将被保护数据流的源和目的 IP 地址改为 NAT 转换后的 IP 地址。

配置策略 NAT 后，内网用户无法访问设备

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。

图-9 组网图



故障原因

- 未配置允许 PC A 访问 Device 的安全策略。
- 策略 NAT 规则对 PC A 访问 Device 的流量进行了目的地址转换。

故障处理步骤（安全策略）

1. 登录设备 Web 管理页面。
2. 选择“策略 > 安全策略”。
3. 在“安全策略”页签单击<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：
   - 名称：secpolicy5
   - 源安全域： Trust
   - 目的安全域：Local
   - 动作：允许
   - 源 IPv4 地址：192.168.1.1（此处为 PC A 的 IP 地址）
   - 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。

故障处理步骤（策略 NAT）

1. 登录设备 Web 管理页面。
2. 选择“策略 > 策略 NAT”。
3. 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：

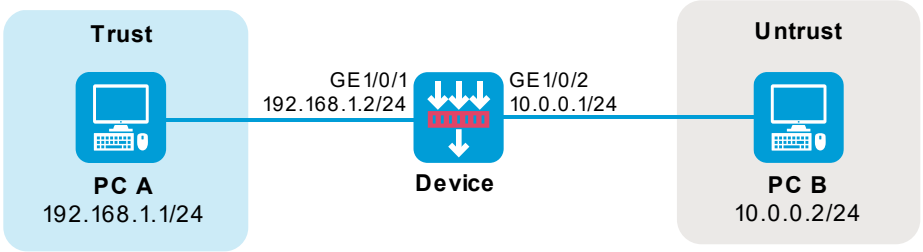
- 目的安全域：不得包含 Local 安全域
- 源 IPv4 地址：不得为 192.168.1.1
- 目的 IPv4 地址：不得为 192.168.1.2

配置 NAT 源地址转换后，外网用户无法访问设备

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。

图-10 组网图



故障原因

- 未配置允许 PC B 访问 Device 的安全策略。
- PC B 访问 Device 的流量因匹配了 NAT 源地址转换规则而被错误地进行了目的地址转换。

故障处理步骤（安全策略）

1. 登录设备 Web 管理页面。
2. 选择“策略 > 安全策略”。
3. 在“安全策略”页签单击<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：
    - 名称：secpolicy6
    - 源安全域： Untrust
    - 目的安全域：Local
    - 动作：允许
    - 源 IPv4 地址：10.0.0.2（此处为 PC B 的 IP 地址）
    - 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。

故障处理步骤（策略 NAT）

1. 登录设备 Web 管理页面。
2. 选择“策略 > 策略 NAT”。
3. 查看是否存在源地址转换方式为动态 IP 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。

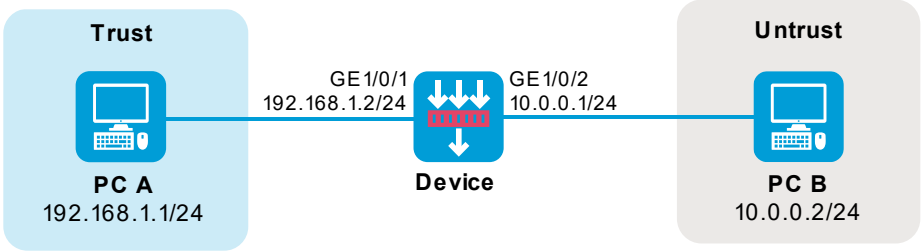
6. 单击<确定>，完成 NAT 策略修改。

配置 NAT 目的地址转换后，外网用户无法访问设备

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。

图-11 组网图



故障原因

- 未配置允许 PC B 访问 Device 的安全策略。

- PC B 利用与 NAT 目的地址转换规则相同的服务访问 Device，导致访问流量因匹配 NAT 目的地址转换规则而被错误地进行了目的地址转换。

故障处理步骤（安全策略）

1. 登录设备 Web 管理页面。
2. 选择“策略 > 安全策略”。
3. 在“安全策略”页签单击<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：
    - 名称：secpolicy7
    - 源安全域： Untrust
    - 目的安全域：Local
    - 动作：允许
    - 源 IPv4 地址：10.0.0.2（此处为 PC B 的 IP 地址）
    - 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。

故障处理步骤（策略 NAT）

1. 登录设备 Web 管理页面。
2. 选择“策略 > 策略 NAT”。

3. 编辑目的地址转换规则。

4. 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：

   - 改变 PC B 访问 Device 时使用的服务。
   - 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。

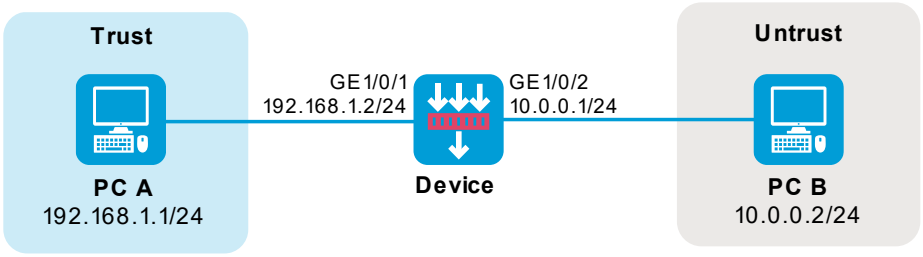
接口NAT

内网用户无法访问外网

故障描述

内网 PC A 无法通过网关设备 Device 访问外网 PC B。

图-12 组网图



故障原因

- 未配置允许 PC A 访问 PC B 的安全策略。
- 未配置接口 NAT 规则对报文源 IP 地址进行转换。

故障处理步骤（安全策略）

1. 登录设备 Web 管理页面。
2. 选择“策略 > 安全策略”。
3. 在“安全策略”页签单击<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：
   - 名称：secpolicy1
   - 源安全域： Trust
   - 目的安全域：Untrust
   - 动作：允许

- 源 IPv4 地址：192.168.1.1（此处为 PC A 的 IP 地址）
- 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。

故障处理步骤（接口 NAT）

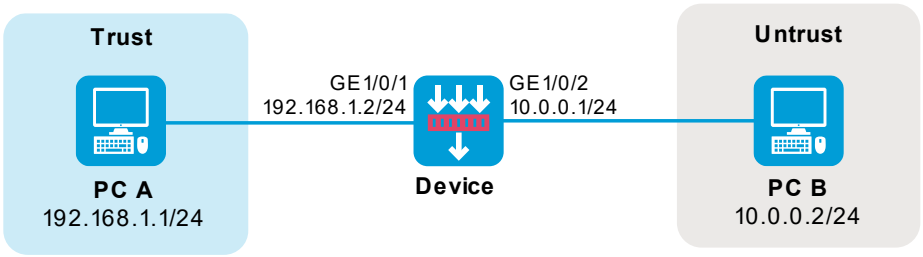
1. 登录设备 Web 管理页面。
2. 选择“策略 > 接口 NAT > IPv4”。
3. 在“NAT 出方向动态转换（基于 ACL）”页签单击<新建>，新建 NAT 出方向动态转换，必要的配置项如下：
   - 接口：GE1/0/2
   - ACL： 此处配置为放行 PC A 访问 PC B 报文的 ACL
   - 转换后源地址：NAT 地址组（此处配置为用于源 IP 地址转换的公网地址组）
   - 转换模式：PAT
4. 单击<确定>，完成 NAT 出方向动态转换配置。

NAT 源地址转换不生效

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。

图-13 组网图



故障原因

- 未配置允许 PC A 访问 PC B 的安全策略。
- 转换后源 IP 地址与 Device 的外网侧接口 IP 地址不在同一网段，导致回程报文不经过 Device。

故障处理步骤（安全策略）

1. 登录设备 Web 管理页面。
2. 选择“策略 > 安全策略”。

3. 在“安全策略”页签单击<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：
    - 名称：secpolicy2
    - 源安全域： Trust
    - 目的安全域：Untrust
    - 动作：允许
    - 源 IPv4 地址：192.168.1.1（此处为 PC A 的 IP 地址）
    - 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。

故障处理步骤（接口 NAT）

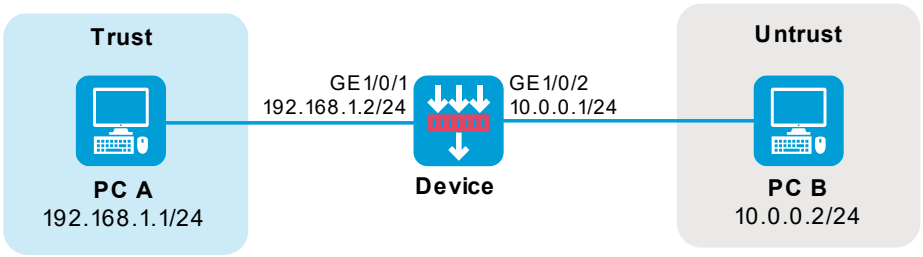
1. 登录设备 Web 管理页面。
2. 选择“策略 > 接口 NAT > IPv4” 。
3. 在右侧页签中编辑 NAT 源地址转换规则。
4. 查看该规则的转换后 IP 地址、网段、地址对象组或 NAT 地址组中是否包含不在 10.0.0.1/24 网段内的地址。
5. 如存在上述情况，需修改转换后源地址配置，确保回程报文能被转发到 Device 的外网侧接口 GE1/0/2 上。
6. 单击<确定>，完成接口 NAT 修改。

NAT 目的地址转换不生效

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。

图-14 组网图



故障原因

- 未配置允许 PC B 访问 PC A 的安全策略。
- PC B 访问 PC A 的目的端口与 NAT 目的地址转换配置不符，导致报文目的地址未被成功转换。

故障处理步骤（安全策略）

1. 登录设备 Web 管理页面。
2. 选择“策略 > 安全策略”。

3. 在“安全策略”页签单击<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：
    - 名称：secpolicy3
    - 源安全域： Untrust
    - 目的安全域：Trust
    - 动作：允许
    - 源 IPv4 地址：10.0.0.2（此处为 PC B 的 IP 地址）
    - 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。

故障处理步骤（接口 NAT）

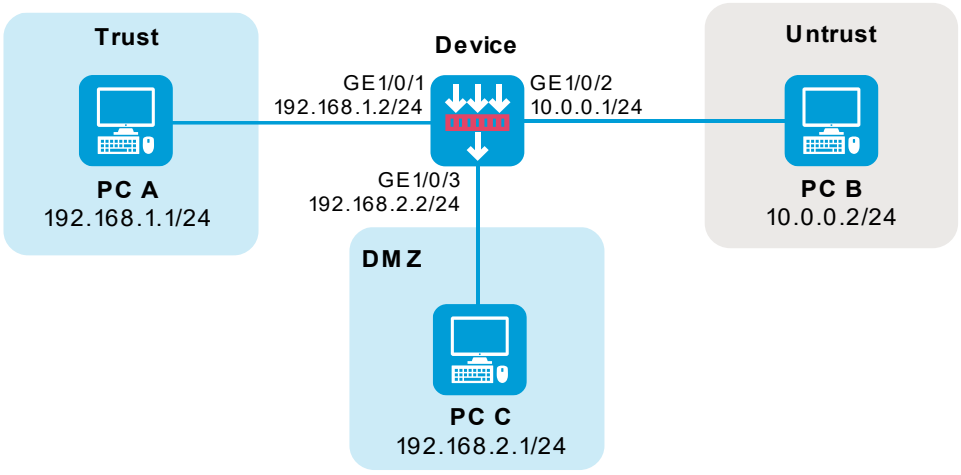
1. 登录设备 Web 管理页面。
2. 选择“策略 > 接口 NAT > IPv4” 。
3. 在“NAT 内部服务器”页签查看 NAT 内部服务器的外网端口是否与实际情况不符。
4. 如存在上述情况，需修改端口匹配条件，确保与实际情况一致。
5. 单击<确定>，完成接口 NAT 修改。

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

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。

图-15 组网图



故障原因

- 未配置允许 PC B 访问 PC C 的安全策略。
- NAT 源地址转换规则占用了 NAT 目的地址转换规则的 IP 地址和端口，导致 Device 访问 PC C 的流量匹配了 NAT 源地址转换规则而非 NAT 目的地址转换规则。

故障处理步骤（安全策略）

1. 登录设备 Web 管理页面。
2. 选择“策略 > 安全策略”。
3. 在“安全策略”页签单击<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：
    - 名称：secpolicy4
    - 源安全域： Untrust
    - 目的安全域：DMZ
    - 动作：允许
    - 源 IPv4 地址：10.0.0.2（此处为 PC B 的 IP 地址）
    - 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。

故障处理步骤（接口 NAT）

1. 登录设备 Web 管理页面。
2. 选择“策略 > 接口 NAT > IPv4”。
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。

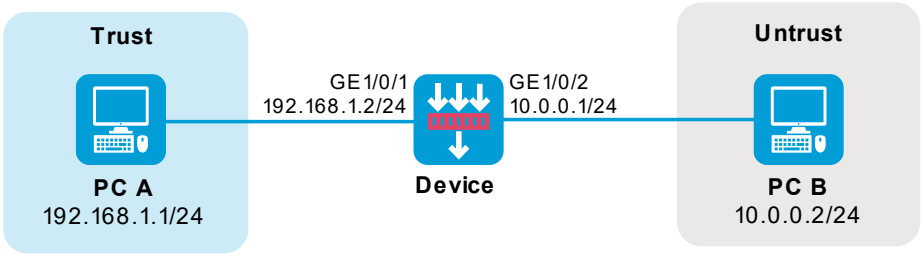
10. 单击<确定>，完成 NAT 出方向动态转换规则修改。

NAT 与 IPsec 配合使用，IPsec 配置不生效

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。

图-16 组网图



故障原因

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。

故障处理步骤

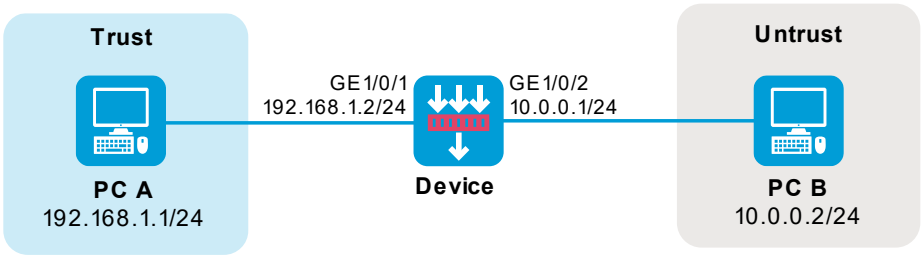
1. 登录设备 Web 管理页面。
2. 选择“网络 > VPN > IPsec > 策略 ”。
3. 在“IPsec 策略”页面编辑 IPsec 策略配置。
4. 查看 IPsec 策略配置中的被保护数据流配置，将被保护数据流的源和目的 IP 地址改为 NAT 转换后的 IP 地址。

配置 NAT 源地址转换后，外网用户无法访问设备

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。

图-17 组网图



故障原因

- 未配置允许 PC B 访问 Device 的安全策略。
- PC B 访问 Device 的流量因匹配了 NAT 源地址转换规则而被错误地进行了目的地址转换。

故障处理步骤（安全策略）

1. 登录设备 Web 管理页面。
2. 选择“策略 > 安全策略”。

3. 在“安全策略”页签单击<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：
    - 名称：secpolicy5
    - 源安全域： Untrust
    - 目的安全域：Local
    - 动作：允许
    - 源 IPv4 地址：10.0.0.2（此处为 PC B 的 IP 地址）
    - 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。

故障处理步骤（接口 NAT）

1. 登录设备 Web 管理页面。
2. 选择“策略 > 接口 NAT > IPv4” 。
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。

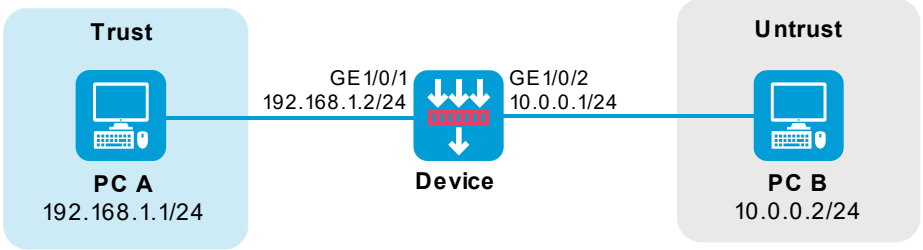
11. 单击<确定>，完成 NAT 出方向动态转换规则修改。

配置 NAT 目的地址转换后，外网用户无法访问设备

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。

图-18 组网图



故障原因

- 未配置允许 PC B 访问 Device 的安全策略。
- PC B 利用与 NAT 目的地址转换规则相同的服务访问 Device，导致访问流量因匹配 NAT 目的地址转换规则而被错误地进行了目的地址转换。

故障处理步骤（安全策略）

1. 登录设备 Web 管理页面。
2. 选择“策略 > 安全策略”。
3. 在“安全策略”页签单击<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：
    - 名称：secpolicy6
    - 源安全域： Untrust
    - 目的安全域：Local
    - 动作：允许
    - 源 IPv4 地址：10.0.0.2（此处为 PC B 的 IP 地址）
    - 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。

故障处理步骤（接口 NAT）

1. 登录设备 Web 管理页面。
2. 选择“策略 > 接口 NAT > IPv4”。
3. 在“NAT 内部服务器”页签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：
   - 改变 PC B 访问 Device 时使用的协议或目的端口。
   - 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。
6. 单击<确定>，完成 NAT 内部服务器规则修改。

SSL VPN 故障处理

SSL VPN 故障处理章节主要介绍以下故障的处理办法：

- 浏览器接入故障
  - 浏览器无法打开 SSL VPN 页面

- 浏览器无法登录 SSL VPN 网关
- 浏览器无法访问内网资源

- iNode 客户端接入故障
  - iNode 客户端无法获取 SSL VPN 网关信息
  - iNode 客户端无法登录 SSL VPN 网关
  - iNode 客户端无法访问内网资源
  - iNode 用户无法老化下线

- 其他故障
  - 配置用户过滤、监控、绑定 IP 地址等功能不生效
  - 用户曾经登录 SSL VPN 网关成功，再次登录时失败

浏览器接入故障

浏览器无法打开 SSL VPN 页面

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。

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：
   - 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。
   - 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。
   - 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：

   - 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。
   - 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

浏览器无法登录 SSL VPN 网关

故障描述

浏览器可以打开 SSL VPN 网关页面，但是无法登录。

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：
   - 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。
   - 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。

- 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：
   - 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。
   - 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：

   - 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。
   - 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。

浏览器无法访问内网资源

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。

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：
   - 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

- 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：

   - 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。
   - 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。
   - 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：

   - 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。
   - 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：

   - 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。
   - 内网服务器未配置回程路由导致链路不通。
   - 地址冲突导致链路不通。
   - 配置了策略路由导致链路不通。
   - 配置了负载均衡导致链路不通。
   - 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。

iNode客户端接入故障

iNode 客户端无法获取 SSL VPN 网关信息

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。

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：
   - 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。
   - 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。
   - 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：

   - 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。
   - 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

iNode 客户端无法登录 SSL VPN 网关

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，但是无法登录。

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：
   - 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。
   - 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。
   - 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：

   - 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。
   - 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：
   - 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。
   - 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。

iNode 客户端无法访问内网资源

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。

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 地址是否加入了安全域，且被安全策略放行。
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：
   - 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。
   - 内网服务器未配置回程路由导致链路不通。
   - 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。
   - 地址冲突导致链路不通。
   - 配置了策略路由导致链路不通。
   - 配置了负载均衡导致链路不通。

iNode 用户无法老化下线

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。

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

其他故障

配置用户过滤、监控、绑定 IP 地址等功能不生效

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。

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。

用户曾经登录 SSL VPN 网关成功，再次登录时失败

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。

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

日志导入/导出故障处理

日志导入/导出故障处理章节主要介绍以下故障的处理办法：

- 日志文件数据显示不准确

日志文件数据显示不准确

故障描述

用户使用 Excel 打开设备上导出的 CSV 格式日志文件时，设备 ID“34020000000010000025”错误地显示为“34020000000010000000”。

故障处理步骤

1. 当用户对数据精度要求较高时，建议使用其他编辑器（例如记事本等）打开 CSV 格式文件，避免上述问题。
2. 如果必须使用Excel查看文件，则建议执行如下操作：新建一个Excel文件，单击“数据 > 自文本”，选择从设备导出的 CSV 文件，在弹出的“文本导入向导弹窗”中保持默认配置，逐步单击<下一步>按钮，直至完成。