云下一代防火墙

用户使用指南

天翼云科技有限公司

前言

概述

本文档主要用来描述天翼混合云防火墙的功能并提供控制台操作指导。

读者对象

本文档主要适用于以下人员：

- 技术支持工程师
- 维护工程师
- 云平台运维人员
- 解决方案工程师

修订记录

日期	修订版本	修改记录
2024-05-16	01	初次发布。

目录

1 Web登录与简介

1.1 登录Web

1.1.1 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。

1.1.2 初次登录Web

为了保证设备安全性，请在初次登录完成后，修改登录密码。

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。缺省的Web登录信息包括：

- 用户名：admin
- 密码：admin
- 用户角色：network-admin
- 设备管理接口的IP地址：192.168.0.1/24

采用缺省登录信息Web登录设备的步骤如下：

步骤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。

步骤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。

步骤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“https://192.168.0.1”，然后回车，进入设备的Web登录页面。

步骤4　输入登录信息

在登录页面中输入用户名admin和密码admin，在下拉列表中选择登录语言，单击<登录>按钮。

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

1.1.3　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户退出Web。

1.2　如何使用Web

1.2.1 Web页面布局介绍

（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：

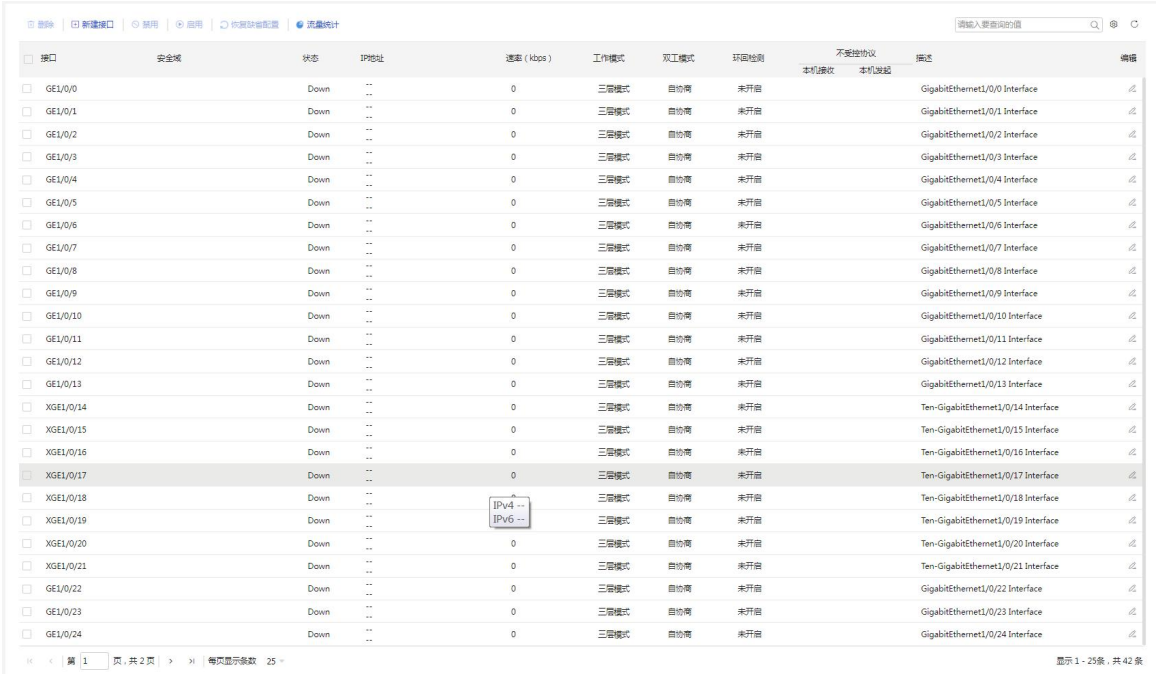
- 标识和面板区：该区域用来显示公司Logo、设备名称、功能面板、当前登录用户信息，并提供更改登录用户密码、保存当前配置、退出登录功能。单击“”，可以在下拉列表中退出登录、修改密码或者切换到指定的虚拟系统；单击“”，可以保存当前配置；单击“”可以打开整本联机帮助。
- 导航栏：以树的形式组织设备的Web功能菜单。用户在导航栏中可以方便的选择功能菜单，选择结果显示在执行区中。用户也可以在导航栏的顶端输入要查询的菜单名称，然后单击“”或者回车后，可以快速定位到目标菜单。
- 执行区：进行配置操作、信息查看、操作结果显示的区域。
- CLI控制台：单击“CLI控制台”，可从Web页面跳转到CLI控制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

1.2.2 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。

1.2.2.1 表项显示页面

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。



1.2.2.2 配置页面

如所示，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。

1.2.3 Web常用操作

Web页面上常用的操作包括保存当前配置、显示表项详情、重启设备等。

1.2.3.1 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。

1.2.3.2 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 > 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。

1.2.3.3 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
- 通过第三方管理平台登录本设备WEB页面
- 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

1.3 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。

2 概览

本帮助主要介绍以下内容：

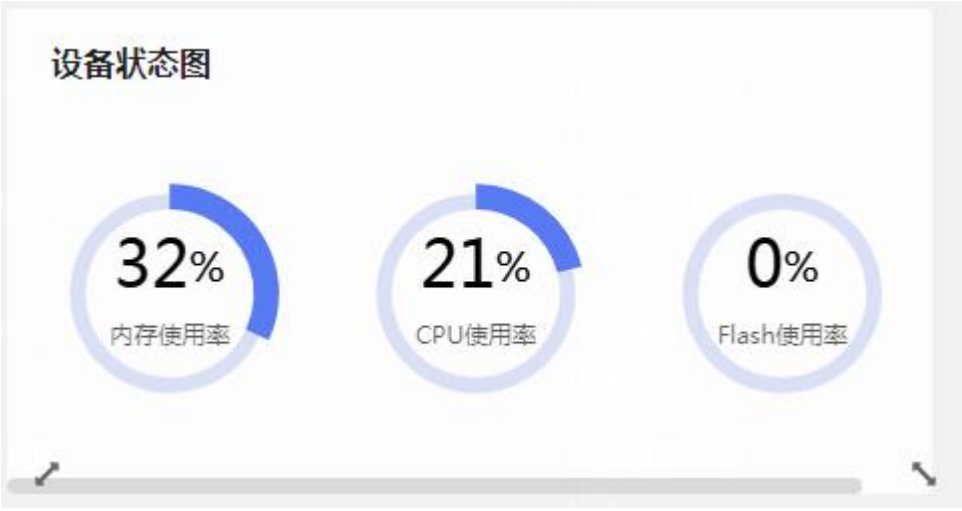
2.1 特性简介

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。

2.1.1 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。

2.1.2 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。

2.1.3 运行监控—系统流量统计

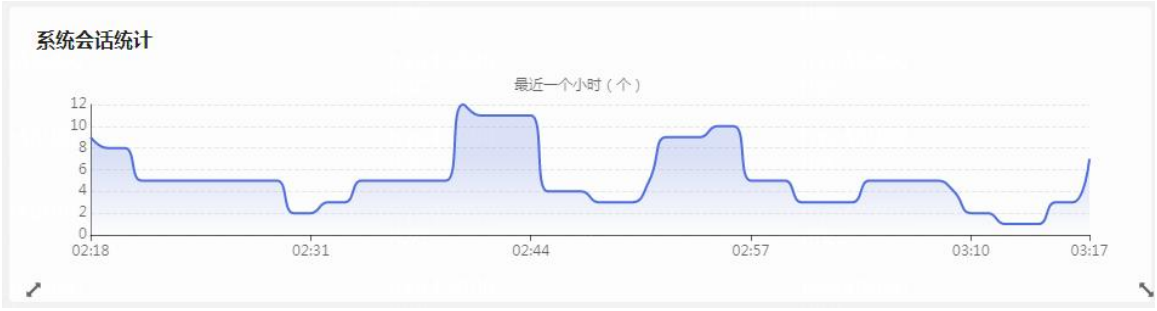
系统流量统计页面通过折线图的方式展示过去一段时间内流入和流出设备的流量统计结果。方便管理员通过查看流量的高峰和低谷时间以及速率等流量分布规律，分析网络状况。

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。

2.1.4 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。

2.1.5 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。

2.1.6 运行监控—系统信息

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

2.1.7 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”。

2.1.8 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。

2.1.9 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。

2.1.10 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。

2.1.11 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。

2.1.12 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。

2.1.13 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。

2.1.14 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。

2.1.15 安全监控—业务安全

业务安全用于查看最近一段时间业务主机的风险概况。

2.1.15.1 注意事项

业务安全页面下的功能仅在设备安装了硬盘或者U盘时支持展示。

2.1.15.2 业务风险分析

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），对业务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，查看业务主机的安全状况详情。

需要注意，当业务风险分析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。
- 未配置业务主机地址范围，请到“对象 > 应用安全 > 高级配置”页面进行配置。
- 入侵防御业务、防病毒等业务未产生日志数据。

2.1.15.3 业务攻击趋势

设备基于入侵防御日志和防病毒日志，对业务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，可能的原因包括如下：

- 未配置业务主机地址范围，请到“对象 > 应用安全 > 高级配置”页面进行配置。
- 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。

2.1.15.4 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业务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，方便管理员了解业务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：

- 未配置业务主机地址范围，请到“对象 > 应用安全 > 高级配置”页面进行配置。
- 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。

2.1.16 安全监控—用户安全

用户安全用于查看最近一段时间用户的风险概况。

2.1.16.1 注意事项

用户安全页面下的功能仅在设备安装了硬盘或者U盘时支持展示。

2.1.16.2 用户风险分析

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），对用户存在的安全风险进行分析，帮助管理员快速了解用户的风险状况。单击统计数据，可跳转到安全分析页面，查看用户的安全状况详情。

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：

- 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。

2.1.16.3 用户攻击趋势

设备基于入侵防御日志和防病毒日志，对用户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用户受到的攻击情况。

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。

2.1.16.4 用户热点事件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内网用户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，方便管理员了解用户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。

2.2 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。

3 监控

3.1 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

3.1.1 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 > 日志管理”界面开启黑名单日志功能，同时需要在“存储空间设置”页面内开启“攻击检测与防范 | 黑名单日志”后生效，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。

3.1.2 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。

3.1.3 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。

3.1.4 配置指南

3.1.4.1 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。

3.1.4.2 日志导出

设备支持将日志导出到PC本地。具体步骤如下：

步骤1 单击“监控 > 安全日志 > 黑名单日志”，进入黑名单日志页面。

步骤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。

步骤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：

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

步骤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。

3.2 单包攻击日志

本帮助主要介绍以下内容：

3.2.1 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“日志管理 > 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。

3.2.2 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。

3.2.3 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。

3.2.4 配置指南

3.2.4.1 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。

3.2.4.2 日志导出

设备支持将日志导出到PC本地。具体步骤如下：

步骤1 单击“监控 > 安全日志 > 单包攻击日志”，进入单包攻击日志页面。

步骤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。

步骤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：

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

步骤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。

3.3　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

3.3.1　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“日志管理 > 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。

3.3.2 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。

3.3.3 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。

3.3.4 配置指南

3.3.4.1 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。

3.3.4.2 日志导出

设备支持将日志导出到PC本地。具体步骤如下：

步骤1 单击“监控 > 安全日志 > 扫描攻击日志”，进入扫描攻击日志页面。

步骤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。

步骤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：

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

步骤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。

3.4 泛洪攻击日志

本帮助主要介绍以下内容：

3.4.1 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“日志管理 > 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。

3.4.2 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。

3.4.3 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。

3.4.4 配置指南

3.4.4.1 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。

3.4.4.2 日志导出

设备支持将日志导出到PC本地。具体步骤如下：

步骤1 单击“监控 > 安全日志 > 泛洪攻击日志”，进入泛洪攻击日志页面。

步骤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。

步骤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：

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

步骤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。

3.5　Web应用防护日志

本帮助主要介绍以下内容：

3.5.1　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。

3.5.2 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。

3.5.3 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”。

3.5.4 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。

3.5.5 配置指南

3.5.5.1 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。

3.5.5.2 日志导出

设备支持将日志导出到PC本地。具体步骤如下：

步骤1 单击“监控 > 安全日志 > Web应用防护日志”，进入Web应用防护日志。

步骤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。

步骤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：

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

步骤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。

3.5.5.3　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：

步骤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。

步骤2　开启日志聚合功能，并配置聚合时间。

步骤3　单击<确定>按钮，完成配置。

3.6　威胁日志

本帮助主要介绍以下内容：

3.6.1　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。

3.6.2 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。

3.6.3 License支持情况

3.6.3.1 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”。

3.6.3.2 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”。

3.6.4 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。
- 当查询多天的日志时，页面默认展示第一天的日志，用户可单击<前一天>和<后一天>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。

3.6.5 配置指南

3.6.5.1 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。

3.6.5.2 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。

3.6.5.3 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。

3.6.5.4 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。

3.6.5.5 日志导出

设备支持将日志导出到PC本地。具体步骤如下：

步骤1 单击“监控 > 安全日志 > 威胁日志”，进入威胁日志页面。

步骤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。

步骤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：

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

步骤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。

3.6.5.6 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：

步骤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。

步骤2　开启日志聚合功能，并配置聚合时间。

步骤3　单击<确定>按钮，完成配置。

3.7　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

3.7.1　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。

3.7.2　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。

3.7.3　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”。

3.7.4 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。

3.7.5 配置指南

3.7.5.1 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。

3.7.5.2 日志导出

设备支持将日志导出到PC本地。具体步骤如下：

步骤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。

步骤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：

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

步骤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。

3.8 URL过滤日志

本帮助主要介绍以下内容：

3.8.1 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。

3.8.2 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。

3.8.3 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。

3.8.4 配置指南

3.8.4.1 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<确认>，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。

3.8.4.2 日志导出

设备支持将日志导出到PC本地。具体步骤如下：

步骤1 单击“监控 > 安全日志 > URL过滤日志”，进入URL过滤日志页面。

步骤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。

步骤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：

参数	说明

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

步骤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。

3.8.4.3　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：

步骤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。

步骤2　开启日志聚合功能，并配置聚合时间。

步骤3　单击<确定>按钮，完成配置。

3.9　文件过滤日志

本帮助主要介绍以下内容：

3.9.1 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。

3.9.2 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。

3.9.3 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。

3.9.4 配置指南

3.9.4.1 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。

3.9.4.2 日志导出

设备支持将日志导出到PC本地。具体步骤如下：

步骤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。

步骤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：

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

步骤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。

3.9.4.3　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：

步骤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。

步骤2　开启日志聚合功能，并配置聚合时间。

步骤3　单击<确定>按钮，完成配置。

3.10　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

3.10.1　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。

3.10.2 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。

3.10.3 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。

3.10.4 配置指南

3.10.4.1 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。

3.10.4.2 日志导出

设备支持将日志导出到PC本地。具体步骤如下：

步骤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。

步骤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：

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

步骤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。

3.10.4.3 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：

步骤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。

步骤2　开启日志聚合功能，并配置聚合时间。

步骤3　单击<确定>按钮，完成配置。

3.11　安全策略日志

本帮助主要介绍以下内容：

3.11.1　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“安全策略模块日志 | 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。

3.11.2　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。

3.11.3　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。

3.11.4 配置指南

3.11.4.1 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。

3.11.4.2 日志导出

日志支持导出功能，具体步骤如下：

步骤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。

步骤2 单击<导出>按钮，进入“导出日志”页面。

步骤3 配置日志导出参数，具体参数如下表所示：

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

步骤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。

3.12 沙箱日志

本帮助主要介绍以下内容：

3.12.1 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”。

3.12.2 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。

3.12.3 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。

3.12.4 配置指南

3.12.4.1 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。

3.12.4.2 日志导出

设备支持将日志导出到PC本地。具体步骤如下：

步骤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。

步骤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：

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

参数	说明
	● 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

步骤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。

3.12.5　附录

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

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

ID	威胁行为
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

ID	威胁行为
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

3.13 NAT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

3.13.1 特性简介

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

NAT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NAT或AFT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日志页面。

3.13.2 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。

3.13.3 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。

3.13.4 配置指南

3.13.4.1 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。

3.13.4.2 日志导出

设备支持将日志导出到PC本地。具体步骤如下：

步骤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。

步骤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：

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

步骤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。

3.14 SSL VPN用户接入日志

本帮助主要介绍以下内容：

- 特性简介

3.14.1 特性简介

当有SSL VPN用户登入登出设备时会有相应的日志输出，日志的内容主要包括SSL VPN用户的登录时间、登录用户名、登录IP地址、所属访问实例、登入登出动作、登录结果、说明等。管理员可以通过查看用户接入日志，了解用户的历史登入登出记录，登录失败原因等信息，有利于管理员管理和维护设备。

3.14.2 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。

3.14.3 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。

3.14.4 配置指南

3.14.4.1 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。

3.14.4.2 日志导出

日志支持导出功能，具体步骤如下：

步骤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。

步骤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：

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

参数	说明
	● 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

步骤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。

3.15　SSL VPN访问资源日志

本帮助主要介绍以下内容：

3.15.1　特性简介

当SSL VPN用户访问内网资源时会有相应的日志输出，日志的内容主要包括SSL VPN用户的登录时间、登录用户名、登录IP地址、虚拟网卡IP地址、所属访问实例、访问资源类型、访问资源、资源的端口号、访问结果等。管理员可以通过查看访问资源日志，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进行管理和控制。

3.15.2　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。

3.15.3　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。

3.15.4 配置指南

3.15.4.1 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。

3.15.4.2 日志导出

日志支持导出功能，具体步骤如下：

步骤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。

步骤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：

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

步骤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。

3.16 终端日志

本帮助主要介绍以下内容：

- 导出异常流量日志

3.16.1 特性简介

3.16.1.1 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，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。

3.16.1.2 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，管理员需要先配置带宽管理策略，并在“存储空间设置”页面使能“带宽管理 | 异常流量日志”后，当终端在某一分钟的带宽峰值高于阈值上限或带宽谷值低于阈值下限，都会被当做异常流量并产生日志信息。

3.16.2 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。

3.16.3 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。

3.16.4 配置指南

3.16.4.1 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：

步骤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。

步骤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。

3.16.4.2 导出异常流量日志

异常流量日志支持导出功能，具体步骤如下：

步骤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。

步骤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。

3.17 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

3.17.1 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。

3.17.2 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。

3.17.3 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”。

3.17.4 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。

3.17.5 配置指南

3.17.5.1 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。

3.17.5.2 日志导出

设备支持将日志导出到PC本地。具体步骤如下：

步骤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。

步骤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：

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

参数	说明
	● 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

步骤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。

3.18　系统日志

本帮助主要介绍以下内容：

3.18.1　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“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。

3.18.2　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。

3.18.3　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。

3.18.4 配置指南

3.18.4.1 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<是>，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。

3.18.4.2 日志导出

日志支持导出功能，具体步骤如下：

步骤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。

步骤2 单击<导出>按钮，进入“导出日志”页面。

步骤3 配置日志导出参数，具体参数如下表所示：

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数时，设备会将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，设备会按照配置的到处条数，将日志分批导出到多个文件中

步骤4 单击<确认>按钮，即可导出日志。

3.19 配置日志

本帮助主要介绍以下内容：

3.19.1 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。

3.19.2 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。

3.19.3 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”。

3.19.4 配置指南

3.19.4.1 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。

3.19.4.2 日志导出

日志支持导出功能，具体步骤如下：

步骤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。

步骤2 单击<导出>按钮，进入“导出日志”页面。

步骤3 配置日志导出参数，具体参数如下表所示：

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

参数	说明
	照配置的导出条数，将日志分批导出到多个文件中 每个文件中可以包含的日志条数：

步骤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。

3.20　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

3.20.1　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。

管理员需要在“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，流量日志才可以显示在页面中。

3.20.2　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。

3.20.3　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。

3.20.4 配置指南

3.20.4.1 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。

3.20.4.2 日志导出

设备支持将日志导出到PC本地。具体步骤如下：

步骤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。

步骤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：

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

步骤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。

3.20.4.3 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：

步骤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。

步骤2 开启日志聚合功能，并配置聚合时间。

步骤3 单击<确定>按钮，完成配置。

3.21 流量统计

本帮助主要介绍以下内容：

3.21.1 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。

管理员可单击<统计条件>按钮，配置多种统计条件，对源/目的IP地址和虚拟设备进行流量统计排行。

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。

3.21.1.1 源IP地址排行

管理员可根据源IP地址对流量进行统计排行，方便管理员对源IP地址的访问情况进行分析。支持配置的统计条件如下表所示：

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
应用类别	根据指定的应用类别对源 IP 地址进行流量排行
具体应用	根据指定应用类别的指定应用对源 IP 地址进行流量排行
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地址的流量使用情况进行统计。

生成统计结果后，管理员可单击指定的源IP地址，进入“应用排行”页面，查看指定源IP地址访问应用的流量排名情况。

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。

3.21.1.2 目的IP地址排行

管理员可根据目的IP地址对流量进行统计排行，方便管理员对目的IP地址的访问情况进行分析。支持配置的统计条件如下表所示：

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
应用类别	根据指定的应用类别对目的 IP 地址进行流量排行
具体应用	根据指定应用类别的指定应用对目的 IP 地址进行流量排行
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地址的流量使用情况进行统计。

生成统计结果后，管理员可单击指定的目的IP地址，进入“应用排行”页面，查看应用的流量排名情况。

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。

3.21.1.3 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：

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

参数	说明
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。

3.21.1.4 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：

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。

3.21.2 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。

3.22 安全策略命中统计

3.22.1 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“安全策略模块日志 | 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：

参数	说明
类型	统计的安全策略 IP 协议类型，取值包括： ● IPv4 ● IPv6
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。

3.23 威胁统计

本帮助主要介绍以下内容：

3.23.1 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。

3.23.1.1 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：

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。

3.23.1.2 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：

参数	说明
威胁类型	统计的威胁类型，取值包括：

参数	说明
	● 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。

3.23.1.3 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：

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。

3.23.1.4 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：

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。

3.23.2 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。

3.23.3 License支持情况

3.23.3.1 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”。

3.23.3.2 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”。

3.24 URL过滤统计

本帮助主要介绍以下内容：

3.24.1 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。

3.24.1.1 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：

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。

3.24.1.2 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：

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。

3.24.1.3 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：

参数	说明
统计时间	统计的时间范围，取值包括：

参数	说明
	● 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。

3.24.1.4 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：

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。

3.24.1.5 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：

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。

3.24.1.6 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：

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。

3.24.1.7 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：

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。

3.24.1.8 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：

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。

3.24.1.9 URL访问趋势

URL访问趋势用来查看用户访问URL的高峰时间段和访问次数等信息，方便管理员了解用户上网情况。管理员可配置统计条件，查看虚服务器、统计节点和访问源的URL访问趋势。设备支持配置的统计条件如下表所示：

参数	说明
统计对象	统计的对象，取值包括： ● 虚服务器 ● 统计节点 ● 访问源

参数	说明
查询范围	统计对象为虚服务器时，查询范围为： ● Top5虚服务器：对URL访问量位于前5名的虚服务器进行URL访问趋势统计 ● 指定虚服务器：对指定虚服务器进行URL访问趋势统计
虚服务器名	指定进行 URL 访问趋势统计的虚服务器名称 仅当查询范围为指定虚服务器时，支持配置本参数

参数	说明

参数	说明
虚服务器名	对指定虚服务器下的统计节点进行 URL 访问趋势统计
查询范围	统计对象为统计节点时，查询范围为： ● Top5统计节点：对指定虚服务器下URL访问量位于前5名的统计节点进行URL访问趋势统计 ● 指定统计节点：对指定虚服务器下的U指定统计节点进行URL访问趋势统计
统计节点名	指定进行 URL 访问趋势统计的统计节点名称 仅当查询范围为指定统计节点时，支持配置本参数

参数	说明
虚服务器名	指定访问源访问的虚服务器名称
统计节点名	指定访问源访问的统计节点名称
查询范围	统计对象为访问源时，查询范围为： ● Top5访问源：对访问量位于前5名的访问源进行URL访问趋势统计 ● 指定访问源：对指定访问源进行URL访问趋势统计
统计节点名	指定进行 URL 访问趋势统计的源地址对象组名称或源 IP 地址 仅当查询范围为指定访问源时，支持配置本参数

单击<开始统计>按钮，设备将根据配置的统计条件对用户访问URL情况进行统计。

3.24.2 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。

3.24.3 License支持情况

URL过滤功能需要购买并正确安装License才能使用。License过期后，URL过滤功能可以使用设备中已存在的特征库正常工作，但无法升级特征库且云端查询功能无法使用。关于License的详细介绍请参见“License联机帮助”。

3.25 文件过滤统计

本帮助主要介绍以下内容：

3.25.1 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。

3.25.2 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。

3.25.3 配置指南

3.25.3.1 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：

步骤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：

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

步骤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。

步骤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。

3.25.3.2 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：

步骤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：

参数	说明

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

步骤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。

步骤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。

3.26　攻击防范统计

本帮助主要介绍以下内容：

3.26.1　特性简介

3.26.1.1　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。

3.26.1.2　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。

3.26.1.3 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。

3.26.2 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。

3.27 服务器负载均衡

3.27.1 特性简介

3.27.1.1 虚服务器统计

显示虚服务器的实时统计信息。包括以下内容：

参数		说明
虚服务器名称		显示虚服务器的统计信息
状态		显示虚服务器的状态，包括： ● 可用 ● 不可用 ● 未开启
连接数	并发	虚服务器的当前活动连接数
	新建	虚服务器的每秒新建连接数
	半开	虚服务器与客户端之间的半开连接数，只有 TCP 类型的虚服务器才会显示本字段
带宽（Kbps）	出方向	虚服务器的出方向带宽
	入方向	虚服务器的入方向带宽

单击<SSL卸载能力统计>按钮，显示SSL卸载的实时统计信息。包括以下内容：

参数	说明
新建连接数	SSL 卸载的每秒新建连接数
并发连接数	SSL 卸载的当前活动连接数
入方向带宽（bps）	SSL 卸载的入方向带宽
出方向带宽（bps）	SSL 卸载的出方向带宽

3.27.1.2 实服务组统计

显示实服务组的实时统计信息，包括以下内容：

参数		说明
实服务组名称		显示指定实服务组的统计信息
状态		显示实服务组的状态，包括： ● 可用 ● 不可用
成员总数		实服务组中成员数量
可用成员数		实服务组中状态为可用的成员数量
连接数	并发	实服务组的当前活动连接数
	新建	实服务组的每秒新建连接数
总带宽（Kbps）		实服务组的总带宽

3.27.1.3 实服务器统计

显示实服务器的实时统计信息，包括以下内容：

参数		说明
实服务器名称		显示指定实服务器的统计信息
状态		显示实服务器的状态，包括： ● 可用 ● 不可用 ● 服务慢宕 ● 服务关闭 ● 健康检测失败 ● 处于温暖上线爬升阶段 ● 繁忙 ● 未知
IPv4 地址		实服务器的 IPv4 地址
IPv6 地址		实服务器的 IPv6 地址
连接数	并发	实服务器的当前活动连接数
	新建	实服务器的每秒新建连接数
带宽（Kbps）	出方向	实服务器的出方向带宽
	入方向	实服务器的入方向带宽

3.27.1.4 URL访问统计

URL访问统计功能用来对用户访问的URL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，方便管理员查看用户的访问情况。

管理员可配置统计条件，对访问虚服务器或统计节点进行URL统计排行。设备支持配置的统计条件如下表所示：

参数	说明
虚服务器名	按照虚服务器进行统计，统计虚服务器的 URL 访问总数
统计节点名	按照统计节点进行统计，统计属于指定虚服务器的 HTTP 统计节点的 URL 访问总数
统计时间	统计的时间范围，统计指定时间范围内的 URL 访问总数

单击<开始统计>按钮，设备将根据配置的统计条件对用户的访问次数进行排名。

3.27.2 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。

3.28 出链路负载均衡

3.28.1 特性简介

3.28.1.1 链路统计

链路统计页面用来查看链路的统计信息，包括链路名称、状态、IPv4出接口、IPv6出接口、并发连接数、新建连接数、上行带宽以及下行带宽。

单击<详细信息>按钮，进入“详情展示页面“，可查看当前链路的详细信息，包括链路的流量、报文数、带宽、连接数、出接口速率、出接口、统计时间以及链路丢包率。

3.28.1.2 链路组统计

链路组统计页面用来显示链路组的统计信息，包括链路组名称、带宽、并发连接数、总计连接数、上行流量、下行流量、上行报文数、下行报文数以及丢弃报文数。

单击<详细信息>按钮，进入“详情展示页面“，可查看当前链路组下所有成员的详细信息，包括链路组成员名称、并发连接数、新建连接数、每秒连接数以及最大每秒连接数。

3.28.2 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。

3.29 DNS透明代理统计

3.29.1 特性简介

3.29.1.1 DNS服务器统计

DNS服务器统计页面用来显示DNS服务器的统计信息，包括以下内容：

参数	说明
DNS 服务器名称	显示指定 DNS 服务器的统计信息
接收请求数	DNS 服务器接受 DNS 请求报文的数目
丢弃请求数	DNS 服务器丢弃 DNS 请求报文的数目
接收应答数	DNS 服务器接受 DNS 应答报文的数目
发送应答数	DNS 服务器分发 DNS 应答报文的数目
丢弃应答数	DNS 服务器丢弃 DNS 应答报文的数目

3.29.1.2 DNS服务器池统计

DNS服务器池统计页面用来显示DNS服务器池的统计信息，包括以下内容：

参数	说明
DNS 服务器池名称	显示指定 DNS 服务器池的统计信息
接收请求数	DNS 服务器池接受 DNS 请求报文的总数
丢弃请求数	DNS 服务器池丢弃 DNS 请求报文的总数
接收应答数	DNS 服务器池接受 DNS 应答报文的总数
发送应答数	DNS 服务器池分发 DNS 应答报文的总数
丢弃应答数	DNS 服务器池丢弃 DNS 应答报文的总数

3.30 新建连接速率排行

3.30.1 特性简介

新建连接速率排行功能用来对指定时间内的新建连接速率进行统计排行，管理员可配置如下统计条件：

- 统计类型
  - 源地址统计：根据报文源地址统计新建连接速率。
  - 目的地址统计：根据报文目的地址统计新建连接速率。
- 统计时间
  - 最近五分钟
  - 最近十五分钟
  - 最近一小时
  - 最近一天
  - 最近一周
  - 最近30天
- 排名个数：可统计Top10～Top500排名。

3.30.2 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。

3.31 流量趋势

本帮助主要介绍以下内容：

3.31.1 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。

3.31.1.1 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：

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。

3.31.1.2 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：

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。

3.31.1.3 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：

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。

3.31.1.4 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：

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。

3.31.1.5 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：

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

参数	说明
	● 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。

3.31.1.6 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：

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。

3.31.2 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。

3.31.3 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。

3.32 威胁趋势

本帮助主要介绍以下内容：

3.32.1 特性简介

威胁趋势功能用来对设备上的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。

3.32.1.1 用户趋势

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：

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：

参数	说明
	● 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。

3.32.1.2 应用趋势

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

参数	说明
应用范围	统计的应用，取值包括： ● Top5应用 ● 指定应用类型
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

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。

3.32.1.3 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：

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。

3.32.1.4 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：

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。

3.32.1.5 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：

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。

3.32.1.6 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：

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。

3.32.2 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。

3.32.3 License支持情况

3.32.3.1 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”。

3.32.3.2 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”。

3.33 安全策略命中趋势

3.33.1 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“安全策略模块日志 | 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：

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
策略类型	统计的安全策略 IP 协议类型，取值包括： ● IPv4 ● IPv6
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。

3.34 URL过滤趋势

本帮助主要介绍以下内容：

3.34.1 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。

3.34.1.1 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：

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。

3.34.1.2 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：

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。

3.34.1.3 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：

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。

3.34.1.4 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：

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。

3.34.1.5 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：

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。

3.34.1.6 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：

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：

参数	说明
	● 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。

3.34.1.7 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：

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。

3.34.2 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。

3.34.3 License支持情况

URL过滤功能需要购买并正确安装License才能使用。License过期后，URL过滤功能可以使用设备中已存在的特征库正常工作，但无法升级特征库且云端查询功能无法使用。关于License的详细介绍请参见“License联机帮助”。

3.35 文件过滤趋势

本帮助主要介绍以下内容：

3.35.1 特性简介

文件过滤趋势用来对指定时间内经由设备传输的文件类型进行统计，并展示文件过滤趋势，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。

3.35.2 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。

3.35.3 配置指南

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。文件过滤趋势的具体配置步骤如下：

步骤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：

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

步骤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。

步骤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。

3.36 链路趋势

3.36.1 特性简介

链路趋势页面用来显示链路统计信息随时间的变化情况，方便管理员更直观的获取链路信息，并根据

链路信息调整链路负载均衡策略。

管理员可以先“选择显示模块”，然后设置“统计条件”，从而实现查看指定链路、指定时间段的链路趋势信息的目的。

若要查看链路的趋势统计，需要先在“存储空间设置”页面开启“负载均衡 | 链路趋势统计”、“负载均衡 | 链路趋势统计（链路应用流量占比）”、负载均衡 | 链路趋势统计（链路信息）”、负载均衡 | 链路趋势统计（链路状态）”相关业务信息。

3.36.1.1 选择显示模块

单击“选择显示模块”，管理员可在下拉列表中选择想要查看的模块。

3.36.1.1.1 流量趋势

通过“流量趋势”模块，管理员可以查看链路流量随时间变化的情况。

单击模块右上角的<设置>页面，可以对流速类型进行设置。设备支持的流速类型包括：

- 上行流量：显示链路的上行流量随时间变化的趋势
- 下行流量：显示链路的下行流量随时间变化的趋势
- 总流量：显示链路的总流量随时间变化的趋势

3.36.1.1.2 带宽利用率趋势

带宽利用率是实际流量占用带宽与最大带宽的比例，反映的是链路带宽的使用效率。通过“带宽利用率趋势”模块，管理员可以查看链路带宽利用率随时间变化的情况。

单击模块右上角的<设置>页面，可以对流速类型进行设置。设备支持的流速类型与“流量趋势”模块一致。

3.36.1.1.3 丢包率趋势

丢包率是指丢失的数据包占发送总数据包的比例，是反映链路质量的参数。链路质量越好，丢包率越低。通过“丢包率趋势”模块，管理员可以查看链路丢包率随时间变化的情况。

3.36.1.1.4 延时趋势

延时是指数据包在链路上传输所耗费的时间，延时是很重要的性能指标。延时越小，链路性能越好。通过“延时趋势”模块，管理员可以查看链路延时随时间变化的情况。

3.36.1.1.5 新建连接数趋势

新建连接数是指设备在1秒内新建的连接数量。通过“新建连接数趋势”模块，管理员可以查看链路新建连接数随时间变化的情况。

3.36.1.1.6 并发连接数趋势

并发连接数是指设备当前的活动连接总数。通过“并发连接数趋势”模块，管理员可以查看链路并发连接数随时间变化的情况。

3.36.1.1.7 RST报文数量趋势

通过“RST报文数量趋势”模块，管理员可以查看RST报文数量随时间变化的情况。

3.36.1.1.8 应用流量占比统计

通过“应用流量占比”模块，管理员可以查看指定链路的各个应用的流量占比。

“应用流量占比”只能对单条链路进行统计。

3.36.1.1.9 稳定性趋势

通过“稳定性趋势”模块，管理员可以查看指定链路的稳定性变化情况。

“稳定性趋势”只能对单条链路进行统计。

3.36.1.1.10 链路实时质量

通过“链路实时质量”模块，管理员可以实时查看链路的状态。

3.36.1.2 设置统计条件

设备根据管理员在“统计条件”页面指定的链路范围和统计时间展示链路趋势信息。设备支持配置的统计条件如下表所示：

参数	说明
自动刷新	开启/关闭链路趋势页面自动刷新功能 开启自动刷新功能后，设备会按照管理员配置的时间间隔自动刷新链路趋势页面
时间间隔	链路趋势页面自动刷新的时间间隔
链路范围	指定链路趋势页面统计的链路范围，可以同时对多条链路进行统计
统计时间	统计的时间范围，取值包括： ● 最近十分钟 ● 最近一小时 ● 今天 ● 最近一周 ● 最近三十天 ● 自定义，当选择“统计时间”为“自定义”时，需要选择具体的统计时间

单击<开始统计>按钮，设备将根据配置的统计条件对链路的流量进行统计，并展示流量趋势图。

3.36.2 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。

3.37 选路策略趋势

3.37.1 特性简介

选路策略趋势页面用来显示选路策略中流量特征的匹配次数占比。

设备根据管理员在“统计条件”页面指定的统计时间分别展示IPv4选路策略和IPv6选路策略的流量特征匹配占比。

若要查看选路策略的趋势统计，需要先在“存储空间设置”页面开启“负载均衡 | 选路策略趋势统计”。

3.37.2 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。

3.38 虚服务趋势

3.38.1 特性简介

虚服务趋势页面用来显示虚服务器统计信息随时间的变化情况，方便管理员更直观的获取虚服务器信息。

设备根据管理员在“统计条件”页面指定的虚服务范围和统计时间展示虚服务器的流量趋势、新建连接数趋势以及并发连接数趋势等。

若要查看虚服务趋势统计，需要先在“存储空间设置”页面开启“负载均衡 | 虚服务器趋势统计”、“负载均衡 | 虚服务器趋势统计（Web缓存）”、“负载均衡 | 虚服务器趋势统计（HTTP信息）”、“负载均衡 | 虚服务器趋势统计（虚服务状态）”相关业务信息。

3.38.1.1 选择显示模块

通过单击“选择显示模块”，管理员可在下拉列表中选择想要查看的模块。

3.38.1.1.1 流量趋势

选择“流量趋势”模块，管理员可以查看是虚服务器流量随时间变化的情况。

通过单击模块右上角的<设置>页面，可以对流速类型进行设置。设备支持的流速类型包括：

- 上行流量：显示虚服务器的上行流量随时间变化的趋势
- 下行流量：显示虚服务器的下行流量随时间变化的趋势
- 总流量：显示虚服务器的总流量随时间变化的趋势

3.38.1.1.2 新建连接数趋势

选择“新建连接数趋势”模块，管理员可以查看虚服务器新建连接数随时间变化的情况。新建连接数是指设备在1秒内新建的连接数量。

3.38.1.1.3 并发连接数趋势

选择“并发连接数趋势”模块，管理员可以查看虚服务器并发连接数随时间变化的情况。并发连接数是指设备当前的活动连接总数。

3.38.1.1.4 稳定性趋势

选择“稳定性趋势”模块，管理员可以查看指定虚服务器的稳定性变化情况。

“稳定性趋势”只能对单个虚服务器进行统计。

3.38.1.1.5 流量压缩比

选择“流量压缩比”模块，管理员可以查看指定虚服务器上压缩的应答报文占总应答报文的百分比情况。

3.38.1.1.6 HTTP应答状态码

选择“HTTP应答状态码”模块，管理员可以查看指定虚服务器返回的重定向报文中的的状态码情况。

3.38.1.2 设置统计条件

步骤1 单击“统计条件”，指定的统计虚服务器范围和统计时间。设备支持配置的统计条件如下表所示：

参数	说明
自动刷新	开启/关闭趋势统计页面自动刷新功能 开启自动刷新功能后，设备会按照管理员配置的时间间隔自动刷新虚服务器趋势统计页面
时间间隔	趋势统计页面自动刷新的时间间隔
虚服务器范围	指定趋势统计页面统计的虚服务器范围，范围包括： ● Top3虚服务器：只统计排名前三的虚服务器 ● 指定虚服务器：可以同时对多个虚服务器进行统计

参数	说明
统计时间	统计的时间范围，取值包括： ● 最近十分钟 ● 最近一小时 ● 今天 ● 最近一周 ● 最近三十天 ● 自定义，当选择“统计时间”为“自定义”时，需要选择具体的统计时间

步骤2　单击<开始统计>按钮，设备将根据配置的统计条件对虚服务器的流量进行统计，并展示流量趋势图。

3.38.2　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。

3.39　实服务组趋势

3.39.1　特性简介

实服务组趋势页面用来显示实服务组统计信息随时间的变化情况，方便管理员更直观的获取实服务组信息。

管理员可以先“选择显示模块”，然后在“统计条件”页面指定的实服务组范围和统计时间，从而实现查看指定实服务组、指定时间段的趋势信息的目的。

若要查看实服务组趋势统计，需要先在“存储空间设置”页面开启“负载均衡 | 实服务组趋势统计”、“负载均衡 | 实服务组趋势统计（实服务组状态）”。

3.39.1.1　选择显示模块

单击“选择显示模块”，管理员可在下拉列表中选择想要查看的模块。

3.39.1.1.1　流量趋势

选择“流量趋势”模块，管理员可以查看是实服务组流量随时间变化的情况。

通过单击模块右上角的<设置>页面，可以对流速类型进行设置。设备支持的流速类型包括：

- ◆ 上行流量：显示实服务组的上行流量随时间变化的趋势
- ◆ 下行流量：显示实服务组的下行流量随时间变化的趋势
- ◆ 总流量：显示实服务组的总流量随时间变化的趋势

3.39.1.1.2 新建连接数趋势

选择“新建连接数趋势”模块，管理员可以查看实服务组新建连接数随时间变化的情况。新建连接数是指设备在1秒内新建的连接数量。

3.39.1.1.3 并发连接数趋势

选择“并发连接数趋势”模块，管理员可以查看实服务组并发连接数随时间变化的情况。并发连接数是指设备当前的活动连接总数。

3.39.1.1.4 稳定性趋势

选择“稳定性趋势”模块，管理员可以查看指定实服务组的稳定性变化情况。

“稳定性趋势”只能对单个实服务组进行统计。

3.39.1.2 设置统计条件

步骤1 单击“统计条件”，指定的统计实服务组范围和统计时间。设备支持配置的统计条件如下表所示：

参数	说明
自动刷新	开启/关闭趋势统计页面自动刷新功能 开启自动刷新功能后，设备会按照管理员配置的时间间隔自动刷新实服务组趋势统计页面
时间间隔	趋势统计页面自动刷新的时间间隔
统计范围	指定趋势统计页面统计的实服务组范围，范围包括： ● Top3实服务组：只统计排名前三的实服务组 ● 指定实服务组：可以同时对多个实服务组进行统计
统计时间	统计的时间范围，取值包括： ● 最近十分钟 ● 最近一小时 ● 今天 ● 最近一周 ● 最近三十天 ● 自定义，当选择“统计时间”为“自定义”时，需要选择具体的统计时间

步骤2 单击<开始统计>按钮，设备将根据配置的统计条件对实服务组的流量进行统计，并展示流量趋势图。

3.39.2 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。

3.40 实服务器趋势

3.40.1 特性简介

实服务器趋势页面用来显示实服务器统计信息随时间的变化情况，方便管理员更直观的获取实服务器信息。

管理员可以先“选择显示模块”，然后在“统计条件”页面指定实服务器范围和统计时间，从而实现查看指定实服务器、指定时间段的趋势信息的目的。

若要查看实服务器统计趋势，需要先在“存储空间设置”页面开启“负载均衡 | 实服务器趋势统计”、“负载均衡 | 实服务器趋势统计（实服务器状态）”。

3.40.1.1 选择显示模块

单击“选择显示模块”，管理员可在下拉列表中选择想要查看的模块。

3.40.1.1.1 流量趋势

选择“流量趋势”模块，管理员可以查看是实服务器流量随时间变化的情况。

通过单击模块右上角的<设置>页面，可以对流速类型进行设置。设备支持的流速类型包括：

- 上行流量：显示实服务器的上行流量随时间变化的趋势
- 下行流量：显示实服务器的下行流量随时间变化的趋势
- 总流量：显示实服务器的总流量随时间变化的趋势

3.40.1.1.2 新建连接数趋势

选择“新建连接数趋势”模块，管理员可以查看实服务器新建连接数随时间变化的情况。新建连接数是指设备在1秒内新建的连接数量。

3.40.1.1.3 并发连接数趋势

选择“并发连接数趋势”模块，管理员可以查看实服务器并发连接数随时间变化的情况。并发连接数是指设备当前的活动连接总数。

3.40.1.1.4 稳定性趋势

选择“稳定性趋势”模块，管理员可以查看指定实服务器的稳定性变化情况。

“稳定性趋势”只能对单个实服务器进行统计。

3.40.1.1.5 HTTP时延趋势

选择“HTTP时延趋势”模块，管理员可以查看实服务器时延随时间变化的情况。时延是指数据包在实服务器上处理所耗费的时间。时延是很重要的性能指标，时延越小，实服务器性能越好。

3.40.1.2 设置统计条件

单击“统计条件”，指定的统计实服务器范围和统计时间。设备支持配置的统计条件如下表所示：

参数	说明
自动刷新	开启/关闭趋势统计页面自动刷新功能 开启自动刷新功能后，设备会按照管理员配置的时间间隔自动刷新实服务器趋势统计页面
时间间隔	趋势统计页面自动刷新的时间间隔
统计范围	指定趋势统计页面统计的实服务器范围，范围包括： ● Top3实服务器：只统计排名前三的实服务器 ● 指定实服务器：可以同时对多个实服务器进行统计
统计时间	统计的时间范围，取值包括： ● 最近十分钟 ● 最近一小时 ● 今天 ● 最近一周 ● 最近三十天 ● 自定义，当选择“统计时间”为“自定义”时，需要选择具体的统计时间

单击<开始统计>按钮，设备将根据配置的统计条件对实服务器的流量进行统计，并展示流量趋势图。

3.40.2 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。

3.41 智能DNS域名请求数趋势

3.41.1 特性简介

智能DNS域名请求数趋势页面用来显示访问指定域名的请求数随时间变化的统计信息，方便管理员更直观获取智能DNS域名请求次数的信息。

设备根据管理员在“统计条件”页面指定的域名范围和统计时间展示指定域名的请求数趋势图。

若要查看智能DNS域名请求数趋势统计，需要先在“存储空间设置”页面开启“负载均衡 | 域名请求数趋势统计”。

3.41.2 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。

3.42 URL访问趋势

3.42.1 特性简介

URL访问趋势用来查看用户访问URL的高峰时间段和访问次数等信息，方便管理员了解用户上网情况。

管理员可配置统计条件，查看虚服务器、统计节点和访问源的URL访问趋势。设备支持配置的统计条件如下表所示：

参数	说明
统计对象	统计的对象，取值包括： ● 虚服务器 ● 统计节点 ● 访问源

参数	说明
查询范围	统计对象为虚服务器时，查询范围为： ● Top5虚服务器：对URL访问量位于前5名的虚服务器进行URL访问趋势统计 ● 指定虚服务器：对指定虚服务器进行URL访问趋势统计
虚服务器名	指定进行 URL 访问趋势统计的虚服务器名称 仅当查询范围为指定虚服务器时，支持配置本参数

参数	说明
虚服务器名	对指定虚服务器下的统计节点进行 URL 访问趋势统计
查询范围	统计对象为统计节点时，查询范围为： ● Top5统计节点：对指定虚服务器下URL访问量位于前5名的统计节点进行URL访问趋势统计 ● 指定统计节点：对指定虚服务器下的U指定统计节点进行URL访问趋势统计

参数	说明
统计节点名	指定进行 URL 访问趋势统计的统计节点名称 仅当查询范围为指定统计节点时，支持配置本参数

参数	说明
虚服务器名	指定访问源访问的虚服务器名称
统计节点名	指定访问源访问的统计节点名称
查询范围	统计对象为访问源时，查询范围为： ● Top5访问源：对访问量位于前5名的访问源进行URL访问趋势统计 ● 指定访问源：对指定访问源进行URL访问趋势统计
统计节点名	指定进行 URL 访问趋势统计的源地址对象组名称或源 IP 地址 仅当查询范围为指定访问源时，支持配置本参数

单击<开始统计>按钮，设备将根据配置的统计条件对用户访问URL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。

3.42.2 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。

3.43 SSL VPN在线用户数趋势

3.43.1 特性简介

SSL VPN在线用户数趋势功能用来对同时登录到设备的SSL VPN在线用户数量进行统计，并向用户展示SSL VPN在线用户数趋势图，方便管理员查看SSL VPN在线用户数发生高峰和低谷的时间段。

管理员可配置统计条件，查看不同统计时间内的SSL VPN在线用户数趋势。

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

单击<开始统计>按钮，设备将根据配置的统计条件对设备的SSL VPN在线用户数进行统计，并展示SSL VPN在线用户数趋势图。

3.43.2 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。

3.44 僵尸网络

本帮助主要介绍以下内容：

3.44.1 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。

3.44.2 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。

3.44.3 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。
- 本功能仅对trust安全域与untrust安全域之间流量产生的日志进行分析。
- 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。

3.44.4 配置指南

3.44.4.1 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。

3.44.4.2 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：

步骤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。

步骤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：

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

步骤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。

3.45 安全分析

本帮助主要介绍以下内容：

3.45.1 特性简介

设备支持对业务主机和用户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。用户可以查看业务主机和用户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。

3.45.2 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。

3.45.3 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。
  - 系统仅对trust安全域与untrust安全域之间流量产生的日志进行分析，当前流量可能不在分析的安全域范围内。
  - 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。

3.45.4 配置指南

步骤1 选择“监控 > 综合分析 > 安全分析”，进入安全分析页面，可查看所有业务主机和用户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。

步骤2 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。

步骤3 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、类型、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。

步骤4 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。

步骤5　管理员可以根据上述分析数据，采取针对性的防范措施。

3.45.5　附录

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

3.46　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

3.46.1　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。

3.46.2　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。

3.46.3　License支持情况

3.46.3.1　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”。

3.46.3.2 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”。

3.46.4 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。

3.46.5 配置指南

威胁案件管理的具体步骤如下：

步骤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。

步骤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。

步骤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。

步骤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。

3.47 威胁案件管理

本帮助主要介绍以下内容：

3.47.1 特性简介

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，并生成多种类型的分析报表，支持的报表类型如下：

- 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。

3.47.2 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。

3.47.3 使用限制和注意事项

当日志量非常大时，报表生成有一定延迟，属于正常现象，请耐心等待。

3.47.4 配置指南

生成报表的具体配置步骤如下：

步骤1 选择“监控 > 报表”，在指定类型的报表页签下，配置报表导出参数。具体配置内容如下表所示：

参数	说明
导出条数	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
统计时间	统计的时间范围，取值包括： ● 天 ● 最近一周 ● 最近三十天 ● 自定义
报表内容	报表中需要包含的统计数据类型，取值包括： ● 量统计 ● 流量趋势

参数	说明
	● 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

步骤2　单击<生成报表>按钮，设备将根据上述导出条件生成报表。

3.48　会话列表

3.48.1　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。

3.48.2　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。

3.49　负载均衡会话信息

3.49.1　特性简介

负载均衡会话信息页面主要显示七层服务器负载均衡的TCP连接信息。单击列表上的<  >按钮，可选择需要展示的会话信息，包括以下内容：

参数	说明
客户端侧客户端 IP	客户端与设备建立的 TCP 连接的客户端 IP 地址
客户端侧客户端端口	客户端与设备建立的 TCP 连接的客户端端口

参数	说明
客户端侧服务器端 IP	客户端与设备建立的 TCP 连接的服务器端 IP 地址
客户端侧服务器端端口	客户端与设备建立的 TCP 连接的服务器端端口
服务器侧客户端 IP	设备与服务器建立的 TCP 连接的客户端 IP 地址
服务器侧客户端端口	设备与服务器建立的 TCP 连接的客户端端口
服务器侧服务器端 IP	设备与服务器建立的 TCP 连接的服务器端 IP 地址
服务器侧服务器端端口	设备与服务器建立的 TCP 连接的服务器端端口
客户端侧连接状态	客户端与设备建立的 TCP 连接的状态，包括： ● CLOSED状态 ● LISTENING状态 ● SYN_SENT状态 ● SYN_RECEIVED状态 ● ESTABLISHED状态 ● CLOSE_WAIT状态 ● FIN_WAIT_1状态 ● CLOSING状态 ● LAST_ACK状态 ● FIN_WAIT_2状态 ● TIME_WAIT状态
服务器侧连接状态	设备与服务器建立的 TCP 连接的状态，包括： ● CLOSED状态 ● LISTENING状态 ● SYN_SENT状态 ● SYN_RECEIVED状态 ● ESTABLISHED状态 ● CLOSE_WAIT状态 ● FIN_WAIT_1状态 ● CLOSING状态 ● LAST_ACK状态 ● FIN_WAIT_2状态 ● TIME_WAIT状态
客户端侧 VRF	客户端与设备建立的 TCP 连接所属 VRF
服务器侧 VRF	设备与服务器建立的 TCP 连接所属 VRF
创建时间	开始建立 TCP 连接的时间
空闲时间	TCP 连接已空闲的时间
空闲超时时间	TCP 连接的空闲超时时间

3.49.2 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。

3.50 用户行为与画像

本帮助主要介绍以下内容：

3.50.1 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。

3.50.2 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。

3.50.3 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”。

3.51 DNS缓存信息

3.51.1 特性简介

DNS缓存信息用来记录域名和IP地址的对应关系，包括以下内容：

参数	说明
域名	缓存的域名
类型	缓存的 IP 地址类型，包括： ● IPv4 ● IPv6
缓存数据	域名对应的 IP 地址
生存时间	DNS 缓存表项的老化时间，单位为分钟

3.51.2 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。

3.52 IPv4在线用户

本帮助主要介绍以下内容：

3.52.1 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。

3.52.2 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。

3.53 IPv6在线用户

本帮助主要介绍以下内容：

3.53.1 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。

3.53.2 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。

3.54 Ping

3.54.1 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。

3.54.2 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。

3.54.3 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。

3.54.4 配置指南

步骤1 单击“监控 > 诊断中心 > Ping”。

步骤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。

步骤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。

步骤4 单击<开始>按钮，启动探测。

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，判断探测的目标网络是否可达。

3.55 Tracert

3.55.1 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“* * *”。

3.55.1.1 IPv4 Tracert不可达结果

在IPv4 Tracert过程中，并且中间设备开启了ICMP不可达报文处理功能（参考**ip unreachables enable**命令），如果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。

3.55.1.2 IPv6 Tracert不可达结果

在IPv6 Tracert过程中，并且中间设备开启了ICMP不可达报文处理功能（参考**ipv6 unreachables enable**命令），如果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目的地址不是链路本地地址时返回此字符。

3.55.2 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。

3.55.3 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。

3.55.4 配置指南

步骤1 单击“监控 > 诊断中心 > Tracert”。

步骤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。

步骤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。

步骤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。

3.56 报文捕获

本帮助主要介绍以下内容：

- 配置报文捕获参数

3.56.1 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。

3.56.2 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。

3.56.3 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。

3.56.4 配置指南

3.56.4.1 开始报文捕获

步骤1 选择“监控 > 诊断中心 > 报文捕获”。

步骤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。

步骤3　在“配置报文捕获过滤条件”页面，具体配置内容如下表所示：

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

步骤4　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。

步骤5　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。

3.56.4.2　配置报文捕获参数

步骤1　选择“监控 > 诊断中心 > 报文捕获”。

步骤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。

步骤3　在“配置报文捕获参数”页面，具体配置内容如下表所示：

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截断
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。捕获文件存储的捕获条目越多占用的内存也就越大，因此在系统内存剩

参数	说明
	余较少的情况下，请将捕获文件存储捕获条目的最大数调小
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，当捕获文件总大小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 服务器时，需要配置登录 FTP 服务器的用户名和密码
VRF	表示 FTP/TFTP 服务器所属的 VRF

步骤4　单击<确定>按钮，完成报文捕获参数配置。

3.57　丢包统计

3.57.1　特性简介

丢包统计功能用来分析和记录设备的转发流程和安全业务模块（如：攻击防范、会话管理和并发连接限制等）丢弃报文的详细原因，通过查看各个模块丢弃报文的详细原因，有利于管理员对网络故障的快速排查和定位。

管理员可以根据IP地址和用户查看符合统计方式的丢包信息，可在丢包统计页面单击<统计条件>按钮来设置统计方式。配置统计方式并开始统计后，统计方式仅对后续报文有效。删除统计方式后可以看到所有的统计信息。

在丢包统计页面可以查看设备上各个模块有关丢包数量的统计信息和详细的丢包原因。

在丢包统计页面可以下载某些支持保存丢包模块所丢弃的最后一个报文，对于不支持保存丢包模块的丢弃报文无法下载。

3.57.2　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。

3.57.3　配置指南

步骤1　选择“系统 > 诊断中心 > 丢包统计”。

步骤2　在“丢包统计”页面单击<统计条件>按钮，可以配置具体的统计方式，具体配置内容如下表所示：

参数	说明

参数	说明
槽号/CPU 号	选择需要进行丢包统计的槽号/CPU 号
统计方式	选择统计方式，包括 IP 地址和用户两种
源地址	选择需要进行丢包统计的源 IP 地址
目的地址	选择需要进行丢包统计的目的 IP 地址
用户	选择需要进行丢包统计的用户

步骤3　单击<开始统计>按钮，在丢包统计页面可以查看设备上各个模块有关丢包数量的统计信息和详细的丢包原因。

3.58　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

3.58.1　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。

3.58.2　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。

3.58.3　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。

3.58.4 配置指南

步骤1 选择“监控 > 诊断中心 > 网页诊断”。

步骤2 配置诊断参数，具体内容如下表所示：

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

步骤3 单击<诊断>按钮，对网页进行诊断。

步骤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。

步骤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。

3.59 诊断信息收集

3.59.1 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。

3.59.2 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。

3.59.3 配置指南

步骤1 选择“监控 > 诊断中心 > 诊断信息收集”，进入诊断信息收集页面。

步骤2 单击<收集>按钮，进入“请输入诊断信息文件名”页面。

步骤3 输入文件名称，单击<确定>按钮。

步骤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。

3.60 报文示踪

本帮助主要介绍以下内容：

3.60.1 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。

3.60.1.1 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。

3.60.1.2 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。

3.60.2 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。

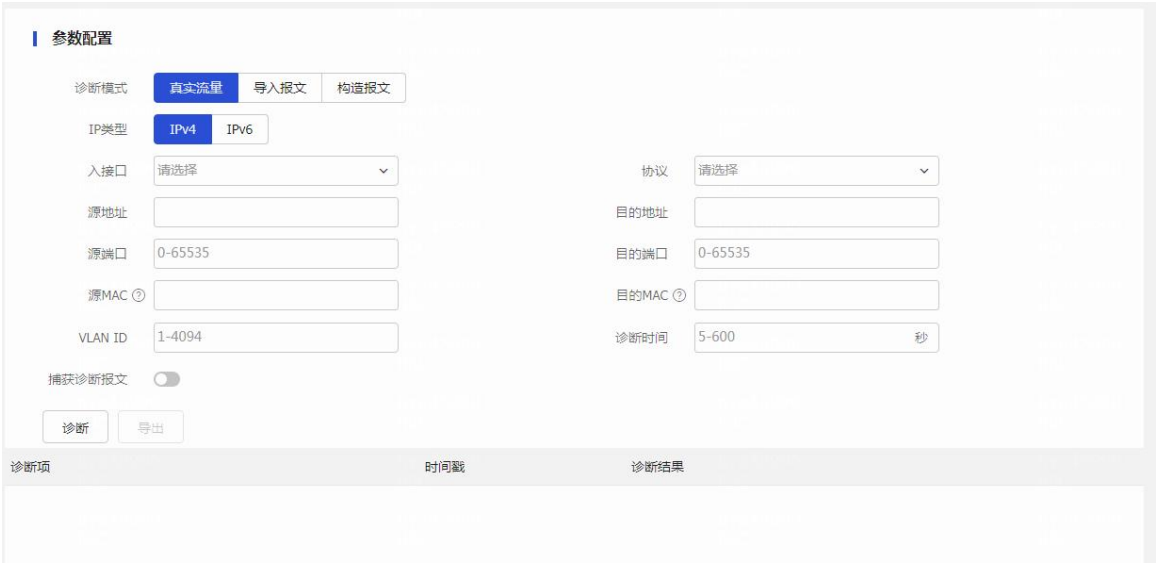
3.60.3 使用限制和注意事项

- 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.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）。

3.60.4 配置指南

步骤1　选择“监控 > 诊断中心 > 报文示踪”。

步骤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。



步骤3　具体配置内容如下表所示：

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

参数	说明
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。此功能仅真实流量诊断模式支持
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 文件供管理员分析使用。管理员可点击<导出>按钮并选择“捕获报文”选项下载此.cap 文件

步骤4　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。

3.61　测试负载均衡配置

3.61.1　特性简介

管理员可以通过指定报文的协议类型、源IPv4/IPv6地址、源端口、目的IPv4/IPv6地址和目的端口，测试报文的负载均衡配置效果。

3.61.2　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。

3.61.3　配置指南

步骤1　单击“监控 > 诊断中心 > 测试负载均衡配置”。

步骤2　配置测试参数。

参数	说明
槽号	待测试的槽位号
IP 类型	IP 地址类型，包括：

参数	说明
	● IPv4 ● IPv6
VRF	待测试的 VPN 实例
目的 IP 地址	待测试的目的 IP 地址。通常情况下，配置为虚服务器的 IP 地址
源 IP 地址	待测试的源 IP 地址
协议层级	负载均衡可识别信息的层级，包括： ● 四层：可识别网络层和传输层信息 ● 七层：除了可识别网络层和传输层信息之外，还可识别应用层信息
四层协议	选择协议的方式，包括： ● 协议名称 ● 协议号 只有“协议层级”选择四层，才会显示本参数
协议名称	待测试协议类型，包括 ● ICMP ● TCP ● UDP
协议号	待测试协议的协议号
七层协议	配置 HTTP 报文的方式，包括： ● 导入HTTP报文 ● 构造HTTP报文 只有“协议层级”选择七层，才会显示本参数
导入 HTTP 报文	待测试的 HTTP 报文 HTTP 报文内容所在的文件后缀必须为.txt，且文件大小不能大于 5000 字节
HTTP 报文请求方法	待测试 HTTP 报文的请求方法，包括： ● GET ● POST
URL	待测试 HTTP 报文的 URL，区分大小写，可以包含字母、数字、“-”“_”及“.”，不能出现连续“.”，不支持字符“?”
HTTP 报文首部	待测试 HTTP 报文的首部，不支持字符“?”。最多允许配置 10 个首部，每个首部之间以换行分隔
HTTP 报文内容	待测试 HTTP 报文体的内容，不支持字符“?”
目的端口号	待测试目的端口号，并非所有协议都支持本参数
源端口号	待测试源端口号，并非所有协议都支持本参数

步骤3　单击<开始测试>按钮，测试结果会在弹出页面显示。

字段	描述

字段	描述
槽号	显示设备的槽位号，本字段显示内容与实际配置相关
匹配的虚服务器名称	显示已匹配的虚服务器名称，本字段显示内容与实际配置相关
未匹配任何虚服务器	-
匹配的负载均衡类名称	显示已匹配的负载均衡类名称，本字段显示内容与实际配置相关
匹配了缺省负载均衡动作	-
匹配的缺省实服务组名称	显示已匹配的缺省实服务组名称，本字段显示内容与实际配置相关
匹配的缺省链路组名称	显示已匹配的缺省链路组名称，本字段显示内容与实际配置相关
转发类型	● 不支持此目的地址，不进行负载均衡 ● 匹配了HTTP类型的虚服务器，不支持负载均衡 ● 转发报文 ● 将报文转发给实服务器 ● 将报文转发给链路 ● 丢弃报文 ● 重定向
选择的实服务器名称	显示已匹配的实服务器名称，本字段显示内容与实际配置相关
选择的链路名称	显示已匹配的链路名称，本字段显示内容与实际配置相关
选择该实服务器的依据	● 根据调度算法 ● 根据持续性方法
选择该链路的依据	● 根据调度算法 ● 根据持续性方法 ● 根据就近性方法
丢弃报文的原因	● 虚服务器连接数或带宽受限 ● 输入的五元组未匹配任何负载均衡类，且没有配置有效的缺省实服务组 ● 输入的五元组未匹配任何负载均衡类，且没有配置有效的缺省链路组 ● 选择的实服务器组中没有可用的实服务器 ● 选择的链路组中没有可用的链路 ● 负载均衡动作为丢弃报文 ● 匹配的持续性表项所对应的实服务器连接数或带宽受限 ● 匹配的持续性表项所对应的链路连接数或带宽受限 ● 匹配的负载均衡类所对应的负载均衡动作中没有可用的实服务组 ● 匹配的负载均衡类所对应的负载均衡动作中没有可用的链路组 ● HTTP报文的内容不合法 ● HTTP报文请求行不合法

字段	描述
	● HTTP报文首部不合法 ● HTTP报文体的chunk编码不合法

3.62 IPsec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

3.62.1 特性简介

IPsec故障诊断功能可以检测IPsec连接的状态，当IPsec连接发生故障时，可以协助用户排查IPsec配置中的问题，并提供可能的原因。

设备支持三种诊断模式：数据流、接口、IP地址。在三种模式下，设备首先将根据用户指定的信息查找对应的IPsec策略。然后，在数据流和接口模式下，设备会主动向对端发起IPsec连接并进行诊断；在IP地址模式下，本端将等待指定对端发起IPsec连接，然后进行IPsec诊断。

参数	说明
IPsec 对端路由可达	路由表中是否存在到对端 IP 地址的路由
接口状态	检测接口物理层和 IP 协议层的状态，接口的确定方式有两种： ● 数据流和IP诊断模式下，根据路由查找对应的出接口 ● 接口诊断模式下，由用户指定
接口上应用了 IPsec 安全策略	检测接口上是否已经应用了 IPsec 安全策略
IPsec 安全策略的 ACL 规则匹配指定数据流	只有采用数据流诊断模式才会显示此项，若显示为“否”，请检查 IPsec 策略的配置
存在待加密数据流	只有采用接口诊断模式才会显示此项，检测 IPsec 策略中的 ACL 规则是否存在 permit 规则，以实现流量匹配，保证 IPsec 的可以正常工作
IPsec 策略配置完整性	检验 IPsec 策略的完整性，包括 ACL、IPsec 安全提议、隧道两端 IP、SA 参数，如果是 IP 地址诊断模式，则检测 IPsec 安全提议、SA 参数

参数	说明
IKE 协商结果	若显示“协商成功”或“IKE SA 已存在”，则说明 IKE 协商正常 若显示其他，这说明 IKE 协商存在问题，请根据具体的提示信息检查本端以及对端的策略是否正确且匹配
IPsec 协商结果	若显示“协商成功”或“隧道已存在”，则说明 IPsec 协商正常 若显示其他，这说明 IPsec 协商存在问题，请根据具体的提示信息检查本端以及对端的策略是否正确且匹配

3.62.2 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。

3.62.3 使用限制和注意事项

- 数据流诊断方式中，源和目的IP地址为数据包实际的IP地址，而不是经过IPsec封装后的IP地址。
- 数据流方式和接口方式的IPsec诊断，根据指定信息查找到的IPsec策略必须可以主动发起IPsec连接，不能是模板方式建立的IPsec安全策略。
- 数据流方式和接口方式的IPsec诊断，设备的处理时间最长为20分钟，若20分钟内没有结果，将停止诊断，并输出已有结果。
- IP地址方式的IPsec诊断，设备将一直等待对端发起IPsec连接，不会自动停止诊断。
- 同一时间只能进行一个IPsec诊断。
- 只能针对使用IPv4地址的IPsec进行诊断。
- 本功能只支持对IPsec安全策略进行诊断，不支持诊断IPsec安全框架。
- VRF应配置为应用IPsec安全策略的接口所在的VPN实例。

3.62.4 配置指南

步骤1 单击“监控 > 诊断中心 > IPsec诊断”。

步骤2 在“IPsec诊断”页面进行配置。

参数	说明
诊断模式	设备支持三种诊断模式，包括： ● 数据流：根据指定的数据流信息获取相应的IPsec策略，主动向对端发起协商 ● 接口：根据指定的接口信息获取相应的IPsec策略，主动向对端发起协商 ● IP地址：接收到对端设备发送的报文后，将启动协商
源地址	封装前数据包实际的源 IP 地址

参数	说明
目的地址	封装前数据包实际的目的 IP 地址
源端口	封装前数据包实际的源端口
目的端口	封装前数据包实际的目的端口
协议	封装前数据包使用的协议
VRF	封装前数据包所属的 VRF
应用策略的接口	选择引用 IPsec 安全策略的接口
对端地址	IPsec 隧道的对端 IP 地址，即封装后的对端 IP 地址
VRF	对端地址所属的 VRF

步骤3　单击“诊断”按钮，查看诊断结果。

4 策略

4.1 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
- 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

- 配置安全策略
- 插入安全策略
- 配置安全策略组
- 安全策略自动部署

4.1.1 特性简介

安全策略通过指定源/目的安全域、源IP/MAC地址、目的IP地址、源微分段、目的微分段、服务、应用、URL分类、终端、用户和时间段等过滤条件匹配出特定的报文，并根据预先设定的策略动作对此报文进行处理；若报文未匹配上任何策略，则丢弃该报文。当安全策略中未配置过滤条件时，则该策略将匹配所有报文。

4.1.1.1 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。

4.1.1.2 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。

4.1.1.3 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。

4.1.1.4 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。

4.1.1.5 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。

4.1.1.6 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。

4.1.1.7 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。

4.1.1.8 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。

4.1.1.9 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。

4.1.2 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。

4.1.3 使用限制和注意事项

4.1.3.1 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。

4.1.3.2 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。

4.1.3.3 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。

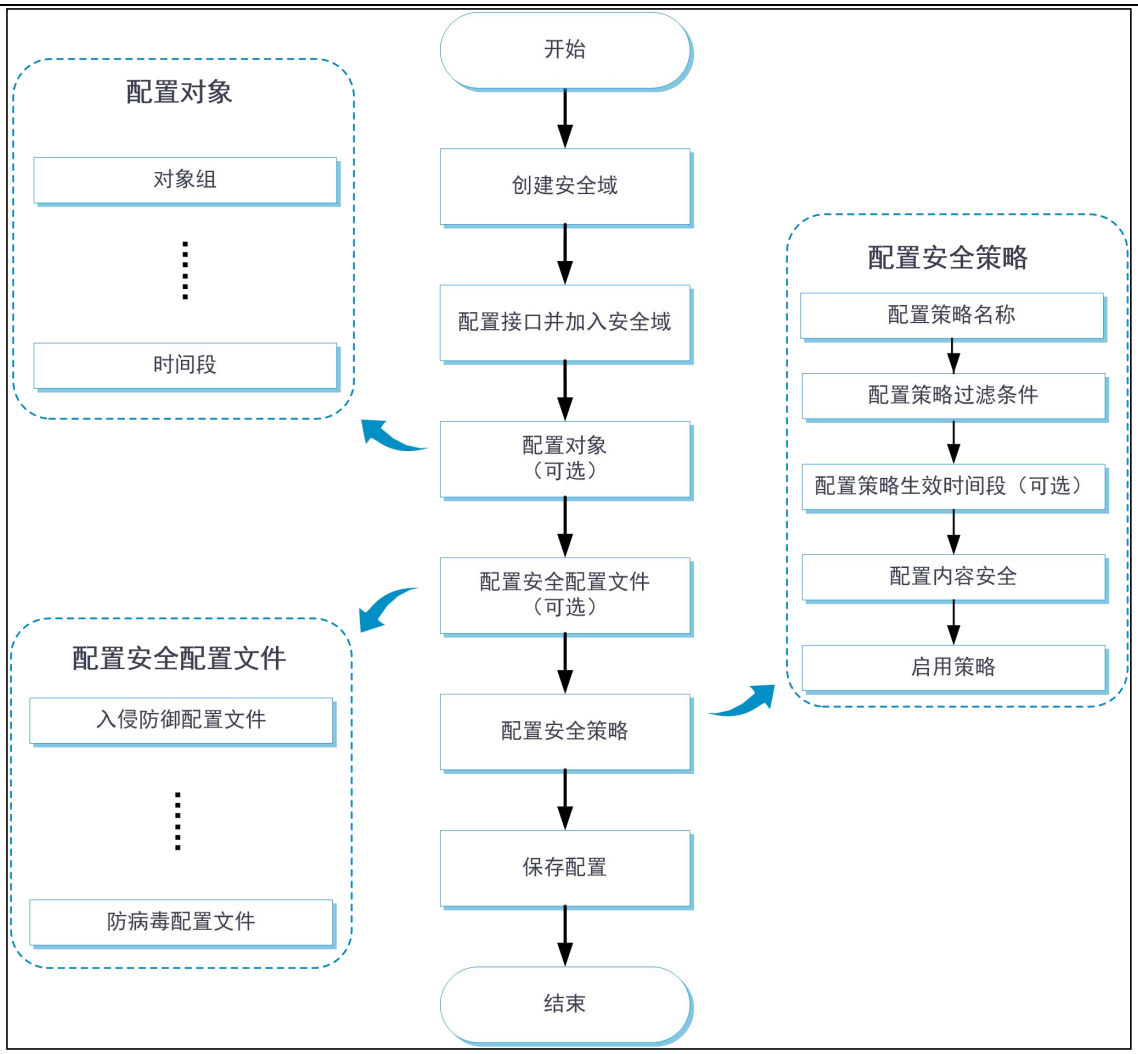
4.1.3.4 安全业务管理平台下发安全策略

- 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。

4.1.4 配置指南

4.1.4.1 配置思路

安全策略功能的配置思路如下图所示：

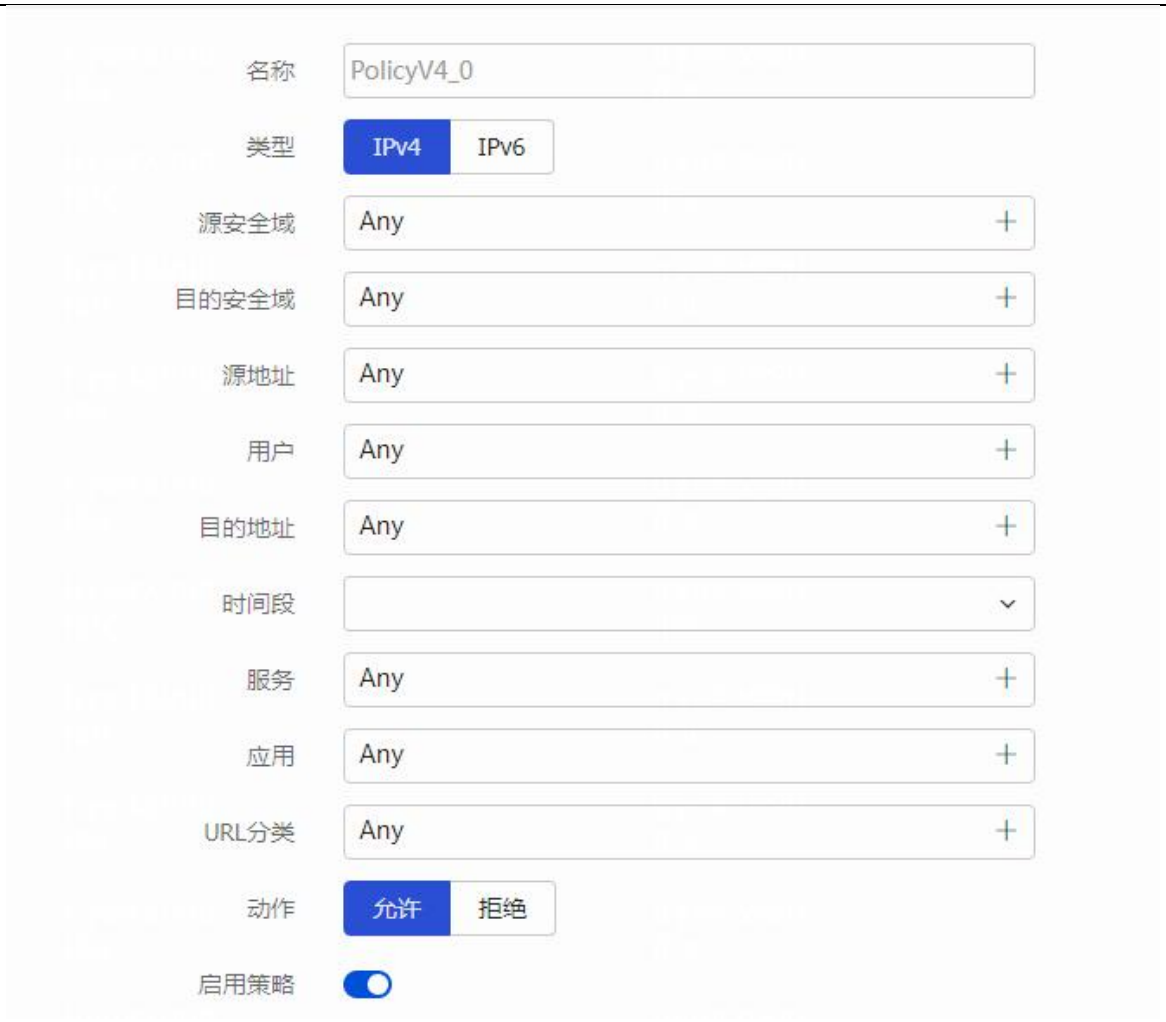


4.1.4.2 配置安全策略

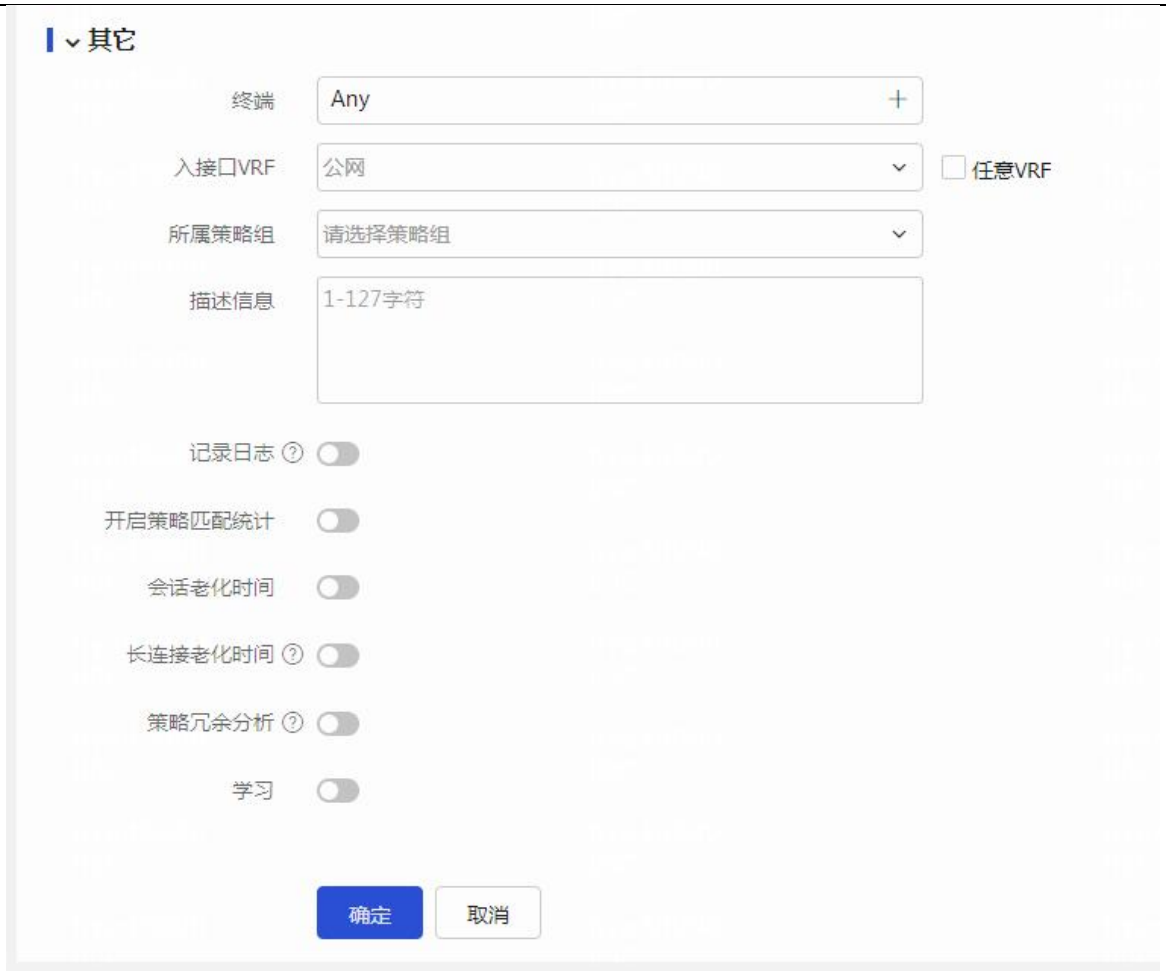
安全策略的具体配置步骤如下：

步骤1 选择“策略 > 安全策略”。

步骤2 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。


名称
PolicyV4_0
类型
IPv4
IPv6
源安全域
Any
目的安全域
Any
源地址
Any
用户
Any
目的地址
Any
时间段
服务
Any
应用
Any
URL分类
Any
动作
允许
拒绝
启用策略


内容安全
Web应用防护配置文件
入侵防御配置文件
数据过滤配置文件
文件过滤配置文件
防病毒配置文件
URL过滤配置文件
APT防御配置文件



步骤3　新建安全策略，具体配置内容如下表所示：

参数	说明
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，默认系统会对此安全策略进行自动命名，如需手动命名直接编辑名称即可
类型	安全策略包括 IPv4 和 IPv6 两种类型
源安全域	配置源安全域作为安全策略的过滤条件
目的安全域	配置目的安全域作为安全策略的过滤条件
源地址	配置源地址对象组、源 IP/MAC 地址、源地区或源微分段作为安全策略的过滤条件，源 MAC 地址对象组过滤条件仅 IPv4 类型的安全策略支持
用户	配置身份识别用户作为安全策略的过滤条件
目的地址	配置目的 IP 地址对象组、目的 IP 地址、目的地区或目的微分段作为安全策略的过滤条件
时间段	配置安全策略生效的时间段
服务	配置服务对象组和协议/端口号作为安全策略的过滤条件
应用	配置应用或应用组作为安全策略的过滤条件

参数	说明
URL 分类	配置 URL 分类作为安全策略的过滤条件
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
Web 应用防护配置文件	配置对符合安全策略过滤条件报文执行的 Web 应用防护配置文件
入侵防御配置文件	配置对符合安全策略过滤条件报文执行的入侵防御配置文件
数据过滤配置文件	配置对符合安全策略过滤条件报文执行的数据过滤配置文件
文件过滤配置文件	配置对符合安全策略过滤条件报文执行的文件过滤配置文件
防病毒配置文件	配置对符合安全策略过滤条件报文执行的防病毒配置文件
URL 过滤配置文件	配置对符合安全策略过滤条件报文执行的 URL 过滤配置文件
APT 防御配置文件	配置对符合安全策略过滤条件报文执行的 APT 防御配置文件
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”表示匹配所有入接口 VPN 实例
所属策略组	配置当前新建的策略所属的策略组
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
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，配置统计的时间长度，取值包括： ◆ 永久 ◆ 自定义
会话老化时间	若策略中配置了会话老化时间，则匹配了该策略且进入稳定状态的会话需要遵循策略中配置的老化时间进行老化 若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的老化时间进行老化
长连接老化时间	若策略中配置了长连接老化时间，则匹配了该策略且进入稳定状态的长连接会话需要遵循策略中配置的长连接老化时间进行老化 若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配置的长连接老化时间进行老化
策略冗余分析	选择开启后，新建安全策略完成将进入策略冗余分析页面
学习	开启学习功能后，可对匹配安全策略的报文进行学习从而进行宽泛策略分析

步骤4　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。

4.1.4.3　插入安全策略

插入安全策略的具体配置步骤如下：

步骤1　选择“策略 > 安全策略”。

步骤2　在“安全策略”页面，勾选已经创建的安全策略，选择插入方式。

步骤3　配置待插入的安全策略。

步骤4　单击<确定>按钮，插入安全策略成功，并会在安全策略页面中显示。

4.1.4.4　配置安全策略组

安全策略组的具体配置步骤如下：

步骤1　选择“策略 > 安全策略”。

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

步骤3　新建安全策略组，具体配置内容如下表所示：

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 两种类型
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，并且起始策略和结束策略之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

步骤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。

4.1.4.5　安全策略自动部署

安全策略自动部署的具体配置步骤如下：

步骤1　选择“策略 > 安全策略”。

步骤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。

步骤3　单击<开始学习>按钮，进入“配置自动部署参数”页面。

步骤4　配置自动部署参数，具体配置内容如下表所示：

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

步骤5　单击<确定>按钮，自动部署参数配置完成。

步骤6　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。

步骤7　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。

4.2　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

4.2.1　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。

4.2.2　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。

4.2.3　配置指南

步骤1　选择“策略 > 安全策略 > 策略冗余分析”。

步骤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。

步骤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。

步骤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。

4.3　策略命中分析

本帮助主要介绍以下内容：

4.3.1　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。

4.3.2 配置指南

4.3.2.1 配置准备

配置策略命中分析功能前，需要先开启策略匹配统计功能。

4.3.2.2 配置步骤

策略命中分析的具体配置步骤如下：

步骤1 选择“策略 > 安全策略 > 策略命中分析”。

步骤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。在此页面的配置内容如下表所示：

参数	说明
时间范围	在页面的右上角可以选择查看命中分析结果的时间范围，其取值包括如下： ◆ 最近1天 ◆ 最近3天 ◆ 最近一周 ◆ 最近30天 ◆ 最近3个月 ◆ 最近半年 ◆ 最近1年 ◆ 最近3年
修改策略	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
删除策略	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

步骤3 修改或删除安全策略后，在“策略命中分析”页面，需要单击第一个<立即加速>按钮，使修改的策略立即生效。

4.4 应用风险调优

本帮助主要介绍以下内容：

- 特性简介

4.4.1 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。

4.4.1.1 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：

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；

步骤1 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；

步骤2 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。

4.4.1.2 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：

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，相反得分越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

参数	说明
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。可根据实际情况选择是否继续调优

4.4.1.3 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：

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，请参考“带宽管理联机帮助”。

4.4.1.4 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。

4.4.2 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。

4.4.3 配置指南

4.4.3.1 配置准备

- 开启安全策略匹配统计功能。
- 激活应用层检测引擎，即配置一个带有应用的安全策略。

4.4.3.2 自动批量调优

步骤1 选择“策略 > 安全策略 > 应用风险调优”。

步骤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。

4.4.3.3 手工逐条调优

步骤1 选择“策略 > 安全策略 > 应用风险调优”。

步骤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。

步骤3 具体调优内容如下表所示：

参数	说明

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

步骤4　单击<确定>按钮，完成策略调优。

4.5　宽泛策略分析

本帮助主要介绍以下内容：

- ◆ 特性简介
- ◆ 配置指南
  - ● 宽泛策略分析

4.5.1　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。

4.5.2 配置指南

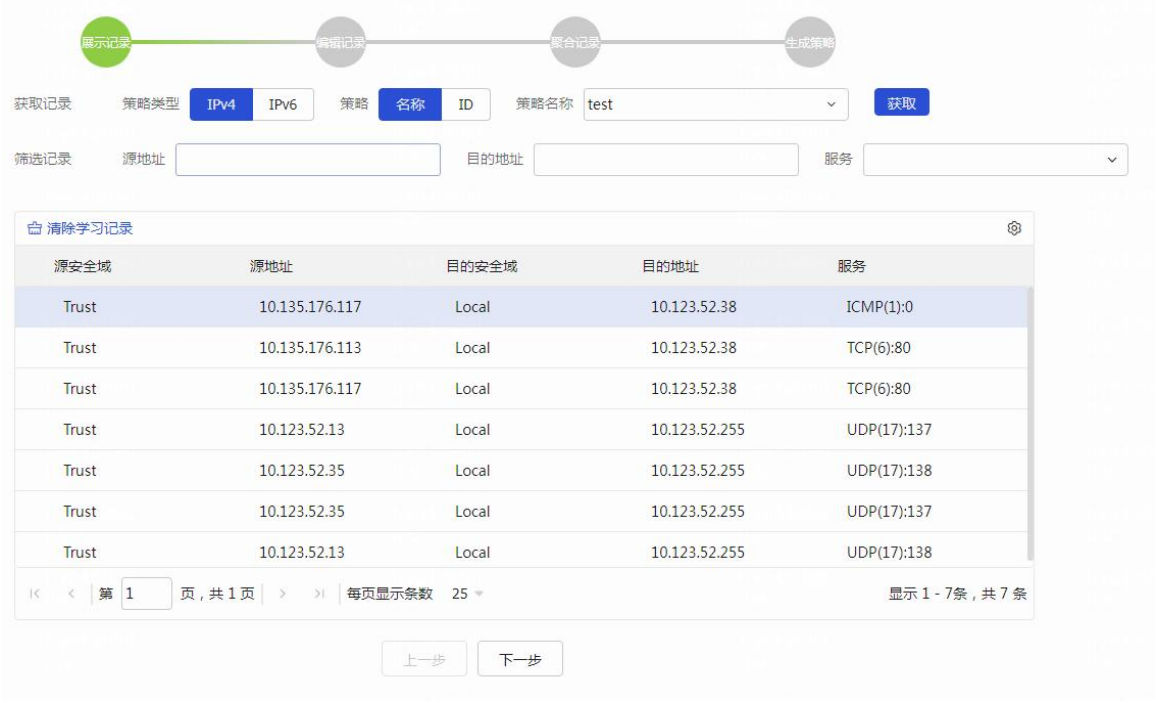
4.5.2.1 配置宽泛策略分析

宽泛策略分析的具体配置步骤如下：

步骤1 选择“策略 > 安全策略”。

步骤2 在“安全策略”页面单击宽泛安全策略对应的<编辑>按钮，勾选“学习”选项，开启宽泛策略学习功能。

步骤3 选择“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。

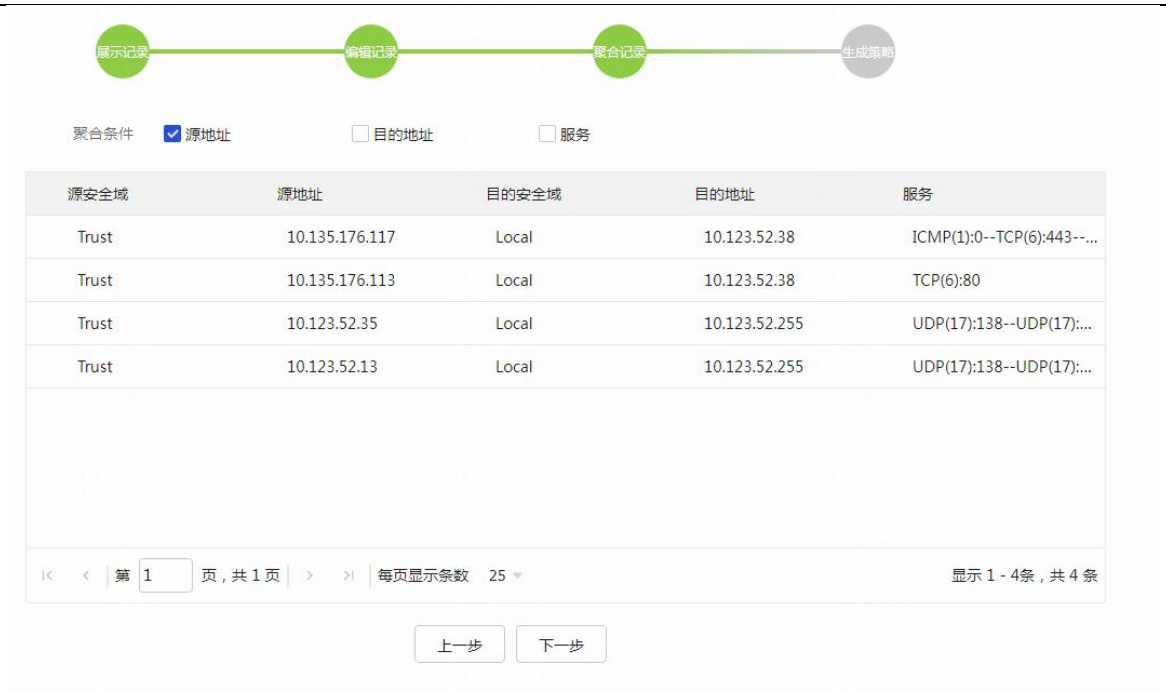


步骤4　单击<下一步>按钮，进入编辑学习记录页面。

步骤5　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。

步骤6　单击<下一步>按钮，进入聚合记录页面。

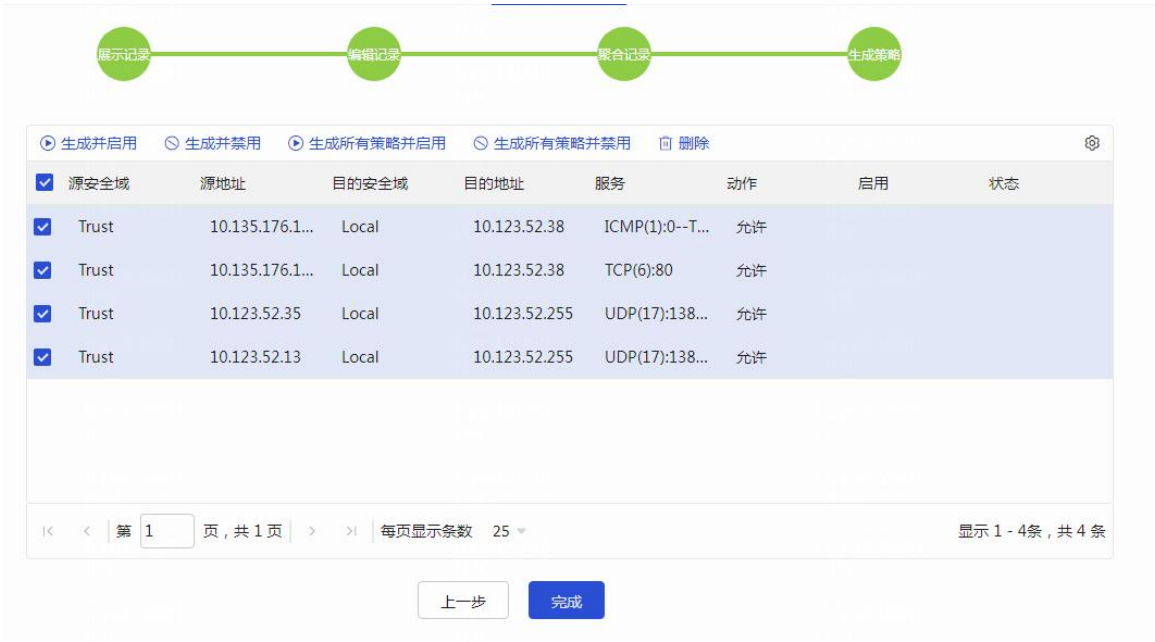
步骤7　通过勾选“源地址”、“目的地址”或“服务”可将相同源地址、相同目的地址或相同服务的多条学习记录聚合为一条。



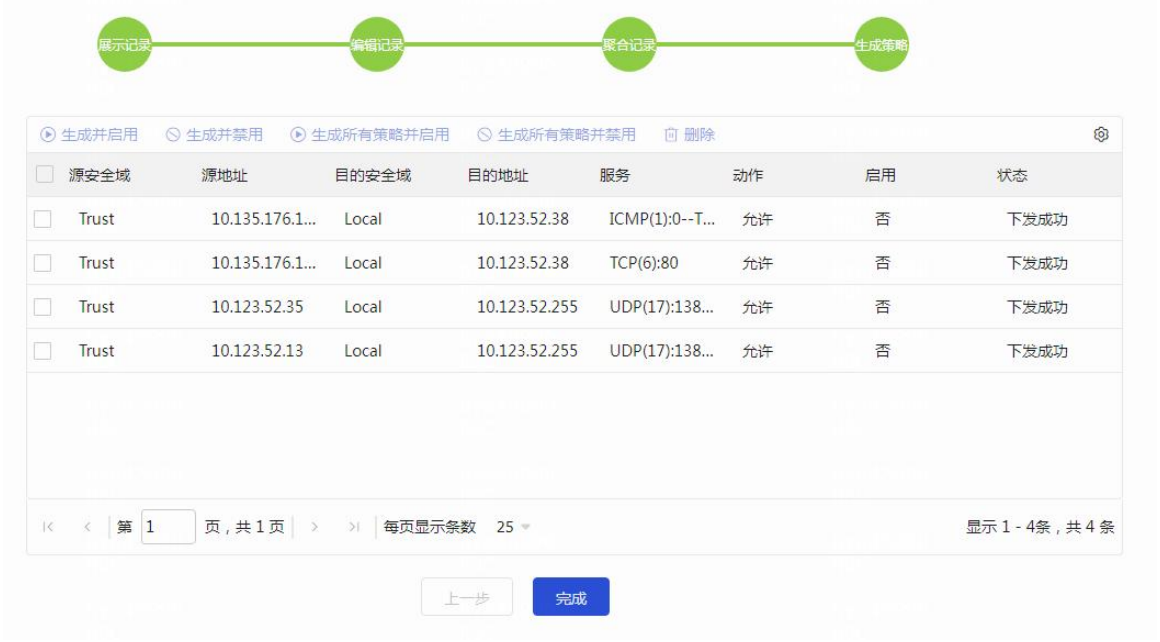
步骤8　单击<下一步>按钮，进入生成策略页面。

步骤9　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。



步骤10　当状态为“下发成功”后表示安全策略生成完成。



步骤11　单击<完成>按钮完成宽泛策略分析。

4.6　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
  - NAT44策略
  - NAT66策略
  - NAT64策略

4.6.1 特性简介

4.6.1.1 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。

4.6.1.2 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。

4.6.1.3 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，关于二者的详细介绍请参见“NAT联机帮助”。

- 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。

使用场景	配置项	
	外网（原始报文的目的IP地址、服务）	内网（目的地址转换后的IP地址、端口）
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，一个内网端口号
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，一个内网端口号
	一个外网地址，N 个外网端口号	一个内网地址，N 个内网端口号
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 个内网端口号
	N 个外网地址，一个外网端口号	N 个内网地址，一个内网端口号

◆ 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。

4.6.1.4 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“双机热备联机帮助”。

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。

4.6.2 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。

4.6.3 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或嵌套地址对象组。

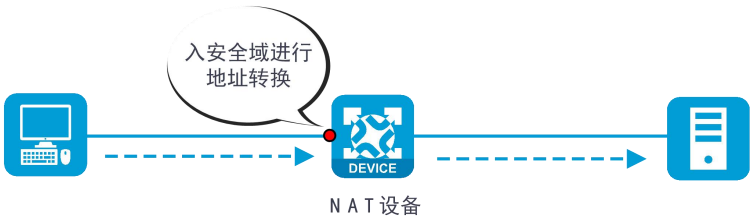
4.6.4 配置指南

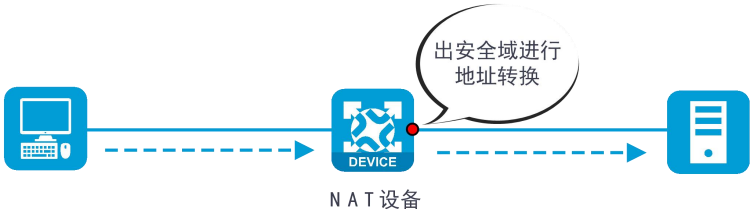
本章节重点介绍配置NAT地址转换的思路和步骤。

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。

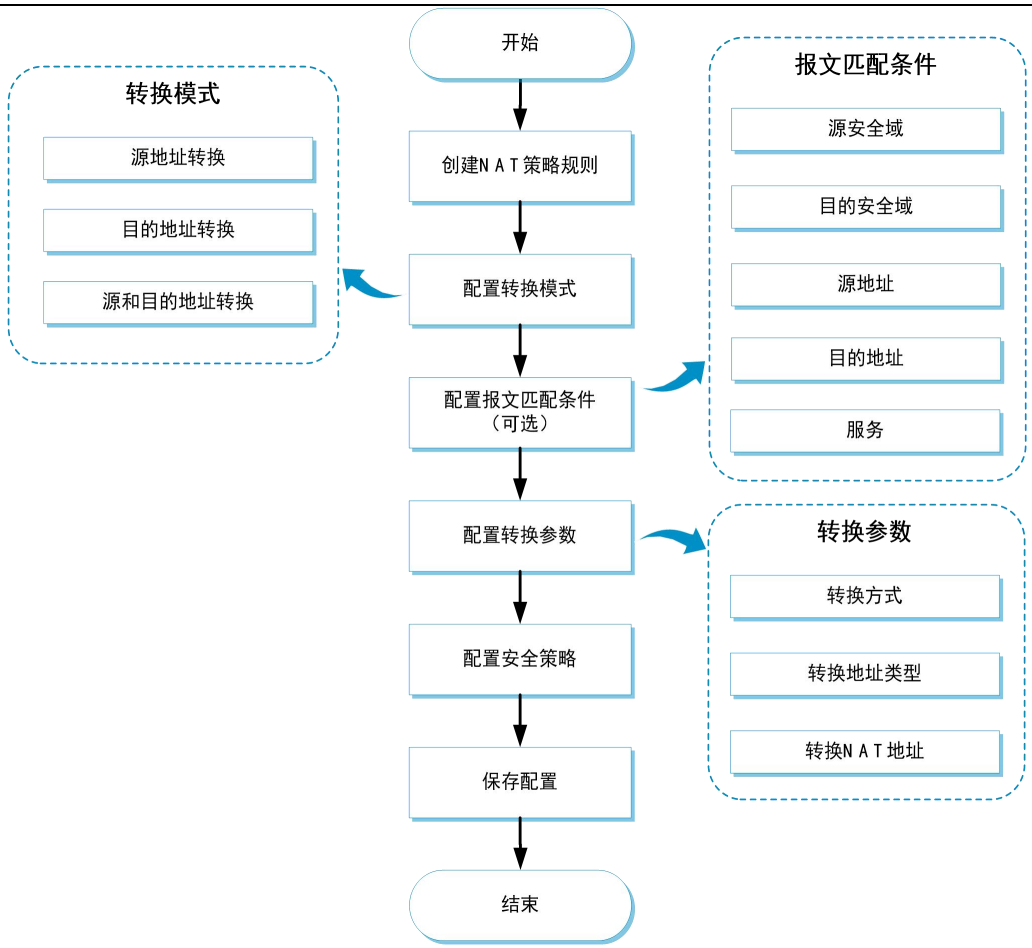
◆ 出方向：对安全域上发送的报文进行转换，即出安全域上配置地址转换。





4.6.4.1 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。



4.6.4.2 NAT44策略

步骤1 创建安全域（可选），具体配置过程略。

步骤2 创建地址对象组（可选），具体配置过程略。

步骤3 创建服务对象组（可选），具体配置过程略。

步骤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。
c. 单击<确定>，完成 NAT 地址组配置。

步骤5 创建NAT44策略规则

d. 选择“策略 > 策略 NAT”。
e. 单击<新建>，选择转换模式，进入对应的转换规则页面。

转换模式	说明
源地址转换	仅转换原始报文的源地址信息

转换模式	说明
目的地址转换	仅转换原始报文的目的地址信息
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目的地址信息

f. 选择“NAT44”页签，进行 NAT44 策略规则配置。

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
	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 如果转换模式选择为目的地址转换或源和目的地址转换，必须指定原始报文的目的地址
	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： ◆ 接口IP地址：使用设备出接口的IP地址进行源地址转换 ◆ 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 ◆ 不做转换：不使用此规则，也不使用任何优先级较低的规则转换报文源地址
	地址类型	选择源地址转换使用的 NAT 地址的类型，分为如下四种： ◆ 地址对象组：使用地址对象组中的IP地址进行源地址转换 ◆ NAT地址组：使用NAT地址组中的IP地址进行源地址转换 ◆ IP地址：使用固定的IP地址进行源地址转换 ◆ 网段地址：使用网段中的IP地址进行源地址转换
	转换为地址	配置源地址转换使用的 NAT 地址
	IPv4 源备份组	配置此功能后，所绑定 VRRP 备份组（IPv4 源备份组）中的 Master 设备将使用虚拟 IP 地址和虚拟 MAC 地址响应报文。双机热备组网环境中需要配置此功能。此功能不同设备的支持情况不同，请以设备 Web 页面的实际支持情况为准

配置项		说明
	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建立地址转换表项的情况下，允许外网向该内网用户发起的连接使用已建立的地址转换表项进行目的地址转换 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，既转换报文源 IP 地址又转换报文源端口；不开启时使用 NO-PAT 方式动态转换报文源地址，只转换报文源 IP 地址
	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端口，当原始端口已被分配给其他用户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 IP 地址”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： ◆ IP地址：将报文目的IP地址转换为固定的IP地址 ◆ 地址对象组转换：将报文目的IP地址转换为地址对象组中的地址 ◆ 不做转换：不使用此规则，也不使用任何优先级较低的规则转换报文目的地址
	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
	IPv4 目的备份组	配置此功能后，所绑定 VRRP 备份组（IPv4 目的备份组）中的 Master 设备将使用虚拟 IP 地址和虚拟 MAC 地址响应报文。双机热备组网环境中需要配置此功能。此功能不同设备的支持情况不同，请以设备 Web 页面的实际支持情况为准
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报文相关信息自动生成安全策略
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

配置项		说明
	统计	开启此 NAT44 策略规则的命中次数统计功能

g. 单击<确定>，完成 NAT44 策略规则配置。

4.6.4.3 NAT66策略

步骤1 创建安全域（可选），具体配置过程略。

步骤2 创建地址对象组（可选），具体配置过程略。

步骤3 创建服务对象组（可选），具体配置过程略。

步骤4 创建NAT66策略规则

a. 选择“策略 > 策略 NAT”。

b. 单击<新建>，选择转换模式，进入对应的转换规则页面。

转换模式	说明
源地址转换	仅转换原始报文的源地址信息
目的地址转换	仅转换原始报文的目的地址信息
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目的地址信息

c. 选择“NAT66”页签，进行 NAT66 策略规则配置。

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
	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 如果转换模式选择为目的地址转换或源和目的地址转换，必须指定原始报文的目的地址
	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，将源IPv6地址前缀替换为配置的地址前缀。此方式必须配置IP地址类型的原始报文源地址匹配条件 ◆ 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

配置项		说明
		地址 ◆ 不做转换：不使用此规则，也不使用任何优先级较低的规则转换报文源地址
	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，既转换报文源 IP 地址又转换报文源端口；不开启时使用 NO-PAT 方式动态转换报文源地址，只转换报文源 IP 地址
	IPv6 源备份组	配置此功能后，所绑定 VRRP 备份组（IPv6 源备份组）中的 Master 设备将使用虚拟 IP 地址和虚拟 MAC 地址响应报文。双机热备组网环境中需要配置此功能。此功能不同设备的支持情况不同，请以设备 Web 页面的实际支持情况为准
	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址，将目的IPv6地址前缀替换为配置的地址前缀 ◆ IP地址：将报文目的IP地址和目的端口转换为固定的IP地址和端口 ◆ 不做转换：不使用此规则，也不使用任何优先级较低的规则转换报文目的IP地址
	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	表示转换后报文所属的 VRF

配置项		说明
	所属 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。

4.6.4.4 NAT64策略

步骤1 创建安全域（可选），具体配置过程略。

步骤2 创建地址对象组（可选），具体配置过程略。

步骤3 创建服务对象组（可选），具体配置过程略。

步骤4 创建NAT64策略规则

a. 选择“策略 > 策略 NAT”。

b. 单击<新建>，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。

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，转换原始报文的源和目的地址信息
	V6toV4	适用于 IPv6 网络主动访问 IPv4 网络的场景，转换原始报文的源和目的地址信息
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，分为如下四种： ◆ 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 地址又转换报文源端口；不开启时使用 NO-PAT 方式动态转换报文源地址，只转换报文源 IP 地址
	IPv4 源备份组	配置此功能后，所绑定 VRRP 备份组（IPv4 源备份组）

配置项		说明
		中的 Master 设备将使用虚拟 IP 地址和虚拟 MAC 地址响应报文。双机热备组网环境中需要配置此功能。此功能不同设备的支持情况不同，请以设备 Web 页面的实际支持情况为准
	IPv6 源备份组	配置此功能后，所绑定 VRRP 备份组（IPv6 源备份组）中的 Master 设备将使用虚拟 IP 地址和虚拟 MAC 地址响应报文。双机热备组网环境中需要配置此功能。此功能不同设备的支持情况不同，请以设备 Web 页面的实际支持情况为准
	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”或“NAT64 前缀”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： ◆ 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IP地址和端口 ◆ 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”

配置项		说明
		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
	IPv4 目的备份组	配置此功能后，所绑定 VRRP 备份组（IPv4 目的备份组）中的 Master 设备将使用虚拟 IP 地址和虚拟 MAC 地址响应报文。双机热备组网环境中需要配置此功能。此功能不同设备的支持情况不同，请以设备 Web 页面的实际支持情况为准
	IPv6 目的备份组	配置此功能后，所绑定 VRRP 备份组（IPv6 目的备份组）中的 Master 设备将使用虚拟 IP 地址和虚拟 MAC 地址响应报文。双机热备组网环境中需要配置此功能。此功能不同设备的支持情况不同，请以设备 Web 页面的实际支持情况为准
	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。

4.7 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

4.7.1 特性简介

带宽管理是指对通过设备的流量实现基于源/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，进行精细化的管理和控制。

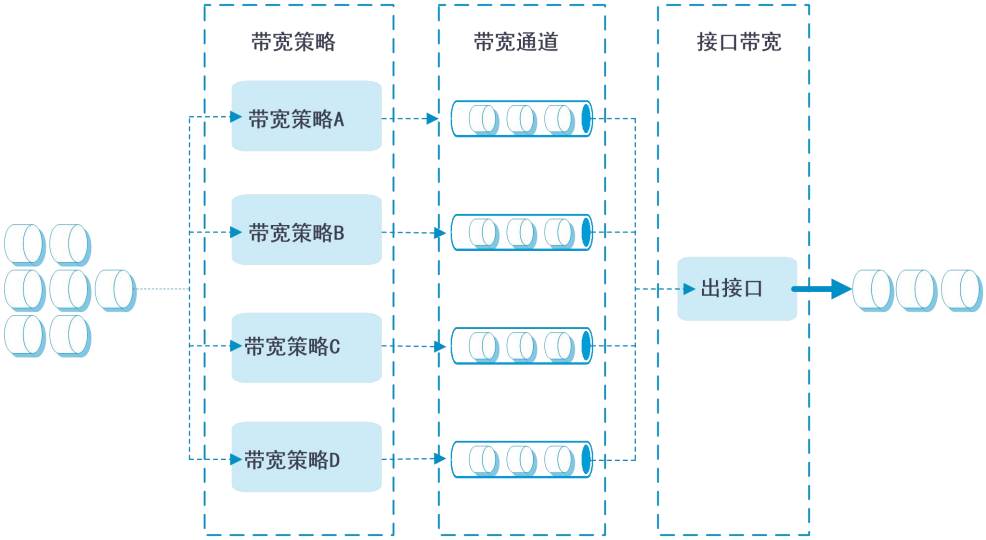
带宽管理的典型应用场景如下：

- 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。

4.7.1.1 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。



带宽管理实现流程如下：

步骤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。

步骤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。

步骤3　流量从出接口发送时受该接口带宽的限制。

4.7.1.2 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。

4.7.1.3 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：

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，即与该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，即与多条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，确保此类业务不受影响
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，避免该类业务消耗大量的带宽，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，充分利用了闲置的带宽资源
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，实现更加精细化的带宽管理
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，实现更加精细化的带宽管理
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。带宽通道中的连接数限制即可以基于带宽策略整体限制会话的最大连

参数	说明
	接数和最大新建连接速率，又可以基于每 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，则优先级高的流量优先被发送。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，是网络设备进行流量分类的依据。位于报文传输路径上的各个网络设备，可以通过 DSCP 优先级来区分流量，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，将以快速日志输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，可通过开启本功能，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小容忍度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，系统会在学习时长内自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），以确保设备学习到一整天的流量。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
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最大容忍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，则表示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

4.7.1.4 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。

4.7.1.5 IPv6全数据流带宽管理功能

缺省情况下，带宽管理仅对ICMP、ICMPv6协议的数据流以及四层协议为TCP、UDP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ICMPv6协议的数据流以及所有四层协议的数据流生效。

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。

4.7.1.6 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”。

4.7.2 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。

4.7.3 使用限制和注意事项

4.7.3.1 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。

4.7.3.2 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。

4.7.3.3 配置接口带宽使用限制和注意事项

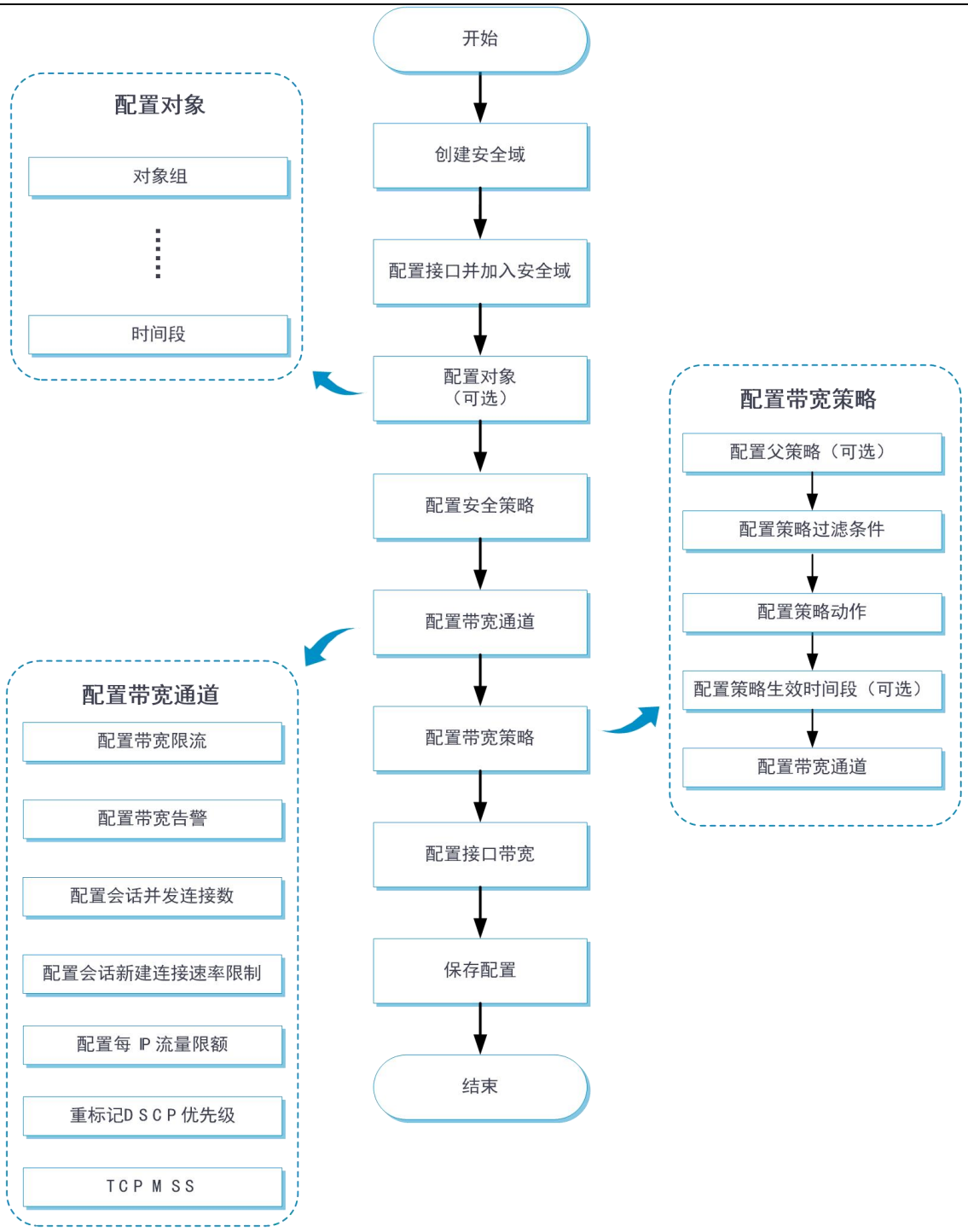
接口期望带宽的缺省值较小时，在流量较大的情况下，很容易出现丢包现象，这时可以将此接口的期望带宽值调大。比如Tunnel口的默认带宽是64kbps，流量比较大的情况下，易出现丢包现象，这时可将Tunnel接口的期望带宽值调大。

4.7.3.4 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。

4.7.4 配置指南

带宽管理策略功能的配置思路如下图所示：



在配置带宽管理功能之前，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”。

4.7.4.1 配置带宽通道

配置带宽通道具体步骤如下：

步骤1　选择“策略 > 带宽管理 > 带宽通道”。

步骤2　在“带宽通道”页面单击<新建>按钮，进入“新建带宽通道”页面。

步骤3　新建带宽通道，具体配置内容如下表所示：

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种
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，充分利用了闲置的带宽资源
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
开启带宽检测功能	开启本功能后，设备基于源 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容忍度得到动态带宽阈值的上限
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容忍度得到动态带宽阈值的下限
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

参数	说明
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

步骤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。

4.7.4.2　配置带宽策略

配置带宽策略的具体步骤如下：

步骤1　选择“策略 > 带宽管理> 带宽策略”。

步骤2　在“带宽策略”页面单击<新建>按钮，进入“新建带宽策略”页面。

步骤3　新建带宽策略，具体配置内容如下表所示：

参数	说明
名称	配置带宽策略的名称
所属父策略	配置带宽策略的父带宽策略
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

参数	说明
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

步骤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。

步骤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。

4.7.4.3　配置接口带宽

配置接口带宽的具体步骤如下：

步骤1　选择“策略 > 带宽管理> 接口带宽”。

步骤2　在“接口带宽”页面单击<新建>按钮，进入“新建接口带宽”页面。

步骤3　新建接口带宽，具体配置内容如下表所示：

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

步骤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。

4.8　应用审计

本帮助主要介绍以下内容：

4.8.1 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。

4.8.1.1 基本概念

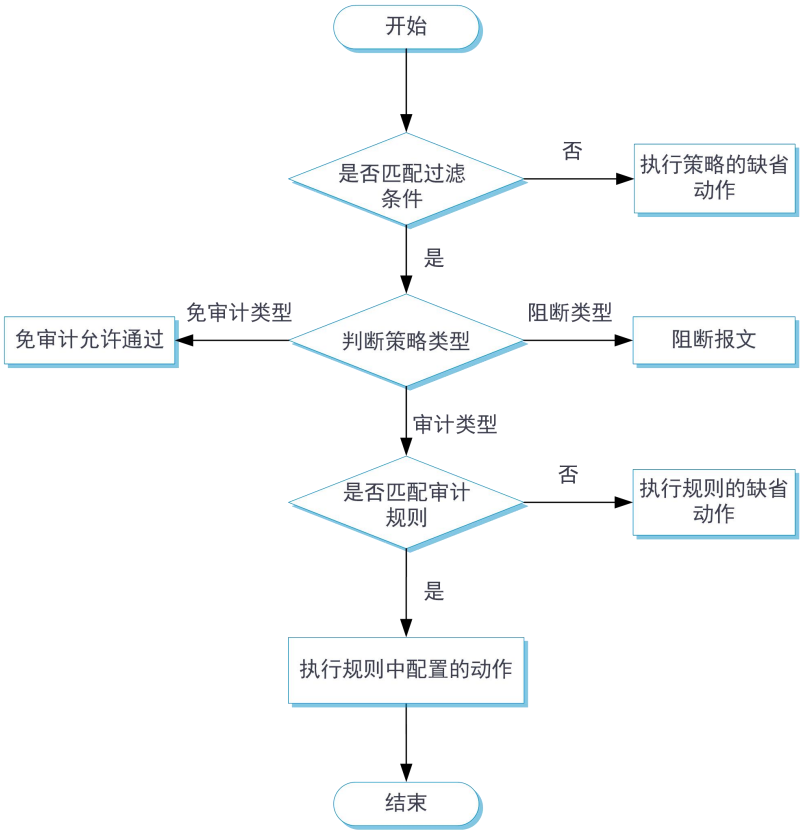
4.8.1.1.1 应用行为

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。

4.8.1.1.2 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。

4.8.1.2 报文审计流程



4.8.1.3 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。

4.8.1.3.1 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。

4.8.1.3.2 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。

4.8.1.4 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。

4.8.1.5 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。

4.8.2 vSystem相关说明

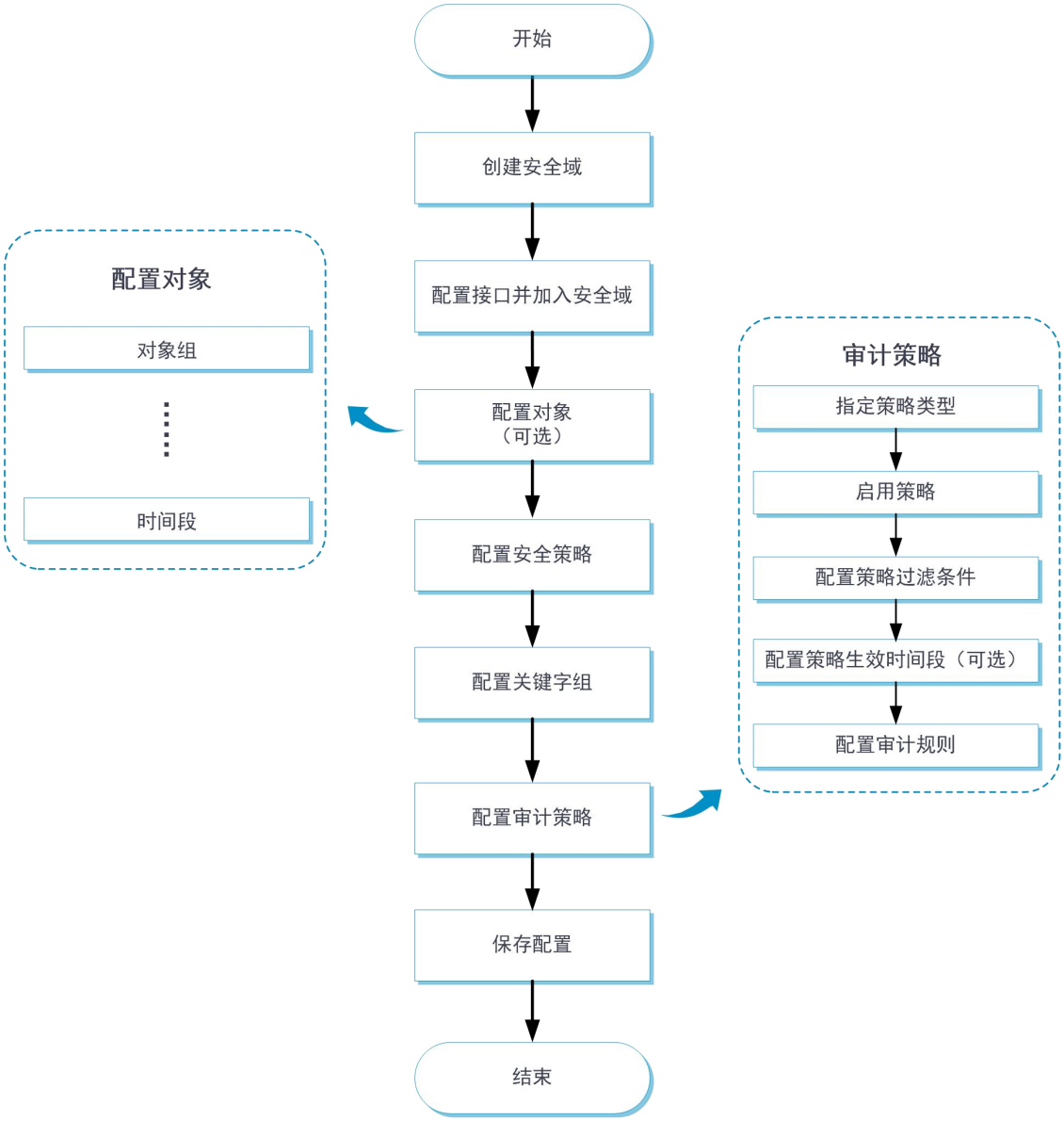
非缺省vSystem对于本特性的支持情况，请以页面的实际显示为准。

4.8.3 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”。

4.8.4 配置指南

应用审计功能的配置思路如下图所示：



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”。

4.8.4.1 配置关键字组

配置关键字组具体步骤如下：

步骤1 选择“策略 > 应用审计”，进入“应用审计”页面。

步骤2 在“应用审计”页面，单击<关键字组>按钮，进入“关键字组”页面。

步骤3 单击<新建>按钮，进入“新建关键字组”页面，具体配置内容如下表所示：

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

步骤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。

4.8.4.2 配置审计策略

配置审计策略的具体步骤如下：

步骤1 选择“策略 > 应用审计”，进入“应用审计”页面。

步骤2 在“应用审计”页面，单击<新建>按钮，进入“新建审计策略”页面。

步骤3　具体配置内容如下表所示：

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
审计规则	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
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。需要配置的参数如下： ◆ 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值
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

步骤4　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。

4.9　应用代理

本帮助主要介绍以下内容：

4.9.1　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。

4.9.1.1　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。

4.9.1.2 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。

4.9.1.3 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。

4.9.1.4 白名单

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。

4.9.1.4.1 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。

4.9.1.4.2 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。

4.9.1.5 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。

4.9.1.6 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。

4.9.1.6.1 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联机帮助”。

4.9.1.6.2 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。

4.9.2 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。

4.9.3 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。

4.9.4 配置指南

4.9.4.1 配置代理策略

代理策略的具体配置步骤如下：

步骤1　选择“策略 > 应用代理 > 代理策略”。

步骤2　在“代理策略”页面单击<新建>按钮，进入“新建代理策略”页面。

步骤3　新建代理策略，具体配置内容如下表所示：

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
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

步骤4　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。

4.9.4.2　配置白名单

4.9.4.2.1　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：

步骤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。

步骤2　单击<新建>按钮，进入“新建自定义白名单表项”页面。

步骤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。

步骤4　单击<提交>按钮，使新建的自定义白名单生效。

4.9.4.2.2　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：

步骤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。

步骤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。

步骤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。

步骤4　单击<提交>按钮，使预定义白名单生效。

4.9.4.3　配置SSL解密证书

SSL解密证书的具体配置步骤如下：

步骤1　选择“策略 > 应用代理 > SSL解密证书”，进入SSL解密证书页面。

步骤2　单击<导入>按钮，进入导入SSL解密证书页面。

步骤3　具体配置内容如下：

- 选择SSL解密证书文件。
- 输入SSL解密证书密码。
- 配置证书标记为可信或者不可信。

步骤4　单击<确认>按钮，完成SSL解密证书的导入。

4.9.4.4　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：

步骤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。

步骤2　单击<导入>按钮，进入导入内部服务器证书页面。

步骤3　具体配置内容如下：

- 选择内部服务器证书文件。
- 输入内部服务器证书密码。

步骤4　单击<确认>按钮，完成内部服务器证书的导入。

4.10　威胁情报

本帮助主要介绍以下内容：

- IP信誉
  - 特性简介

4.10.1 IP信誉

4.10.1.1 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。

4.10.1.1.1 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。

4.10.1.1.2 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。

4.10.1.1.3 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底依次为：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。

4.10.1.1.4 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。

4.10.1.1.5 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。

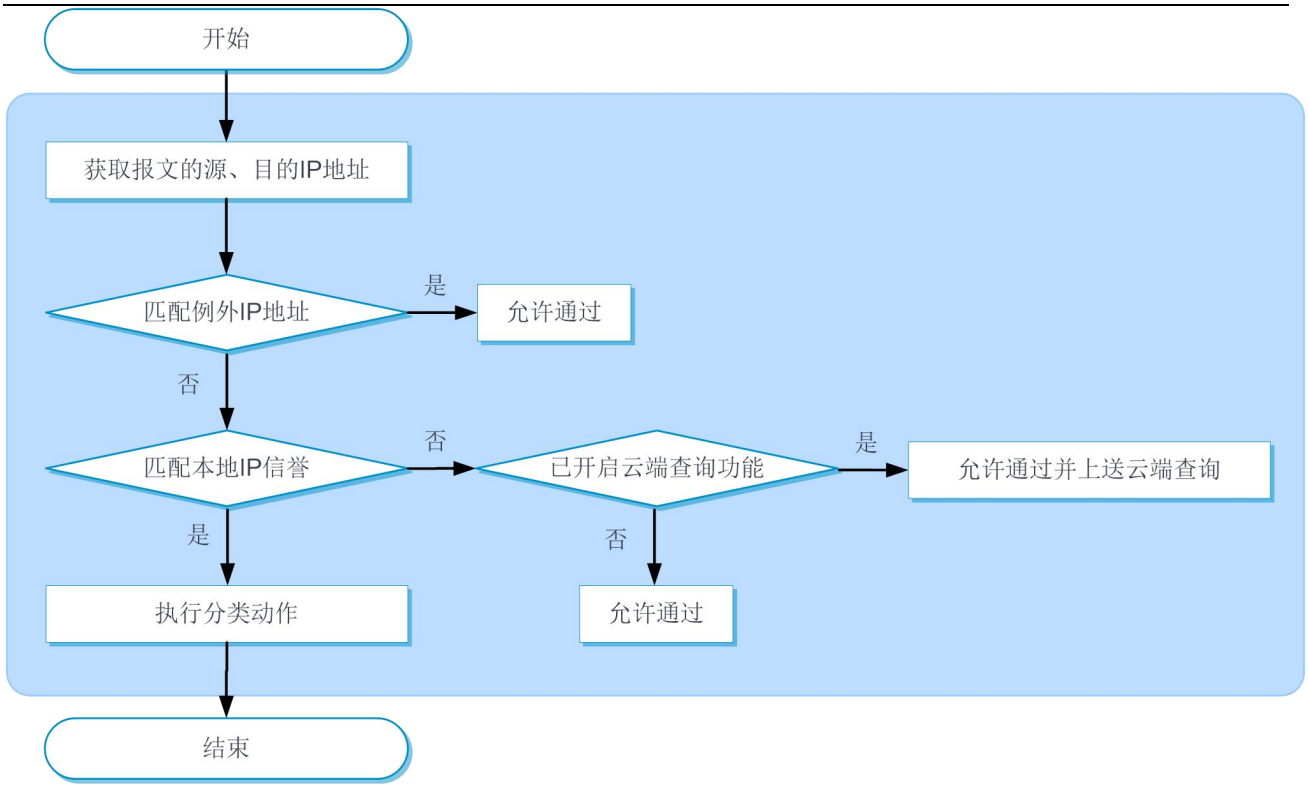
IP信誉库中的IP地址均为公网地址，使用IP信誉功能添加的黑名单表项VRF为公网。

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”。

4.10.1.1.6 IP信誉的报文处理流程

IP信誉对报文的处理流程如下图所示：



IP信誉功能对报文的处理过程如下：

步骤1　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。

步骤2　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。

4.10.1.2 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。

4.10.1.3 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”。

4.10.1.4 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。

4.10.1.5 配置指南

4.10.1.5.1 开启IP信誉功能

开启IP信誉功能的具体配置步骤如下：

步骤1 选择“策略 > 主动防护 > 威胁情报”。

步骤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。

步骤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。

4.10.1.5.2 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：

步骤1 选择“策略 > 主动防护 > 威胁情报”。

步骤2　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。

4.10.1.5.3　开启Top统计功能

开启Top统计功能的具体配置步骤如下：

步骤1　选择“策略 > 主动防护 > 威胁情报”。

步骤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。

步骤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。

步骤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。

4.10.1.5.4　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：

步骤1　选择“策略 > 主动防护 > 威胁情报”。

步骤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。

步骤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。

步骤4　完成配置后，单击<应用>按钮，使配置生效。

4.10.1.5.5　配置IP例外

配置IP例外的具体配置步骤如下：

步骤1　选择“策略 > 主动防护 > 威胁情报”。

步骤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。

步骤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。

步骤4　完成配置后，单击<应用>按钮，使配置生效。

4.10.2　URL信誉

4.10.2.1　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。

4.10.2.1.1 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。

4.10.2.1.2 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。

4.10.2.2 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。

4.10.2.3 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”。

4.10.2.4 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”。

4.10.2.5 配置指南

URL信誉的具体配置步骤如下：

步骤1 选择“对象 > 安全配置文件 > URL过滤 > URL过滤”。

步骤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. 勾选开启 URL 信誉功能。

c. 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。

步骤3　单击<确认>按钮，完成配置。

4.10.3　域名信誉

4.10.3.1　特性简介

域名信誉功能用于根据本地域名信誉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。

4.10.3.1.1　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”。

4.10.3.1.2　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。

4.10.3.1.3　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。

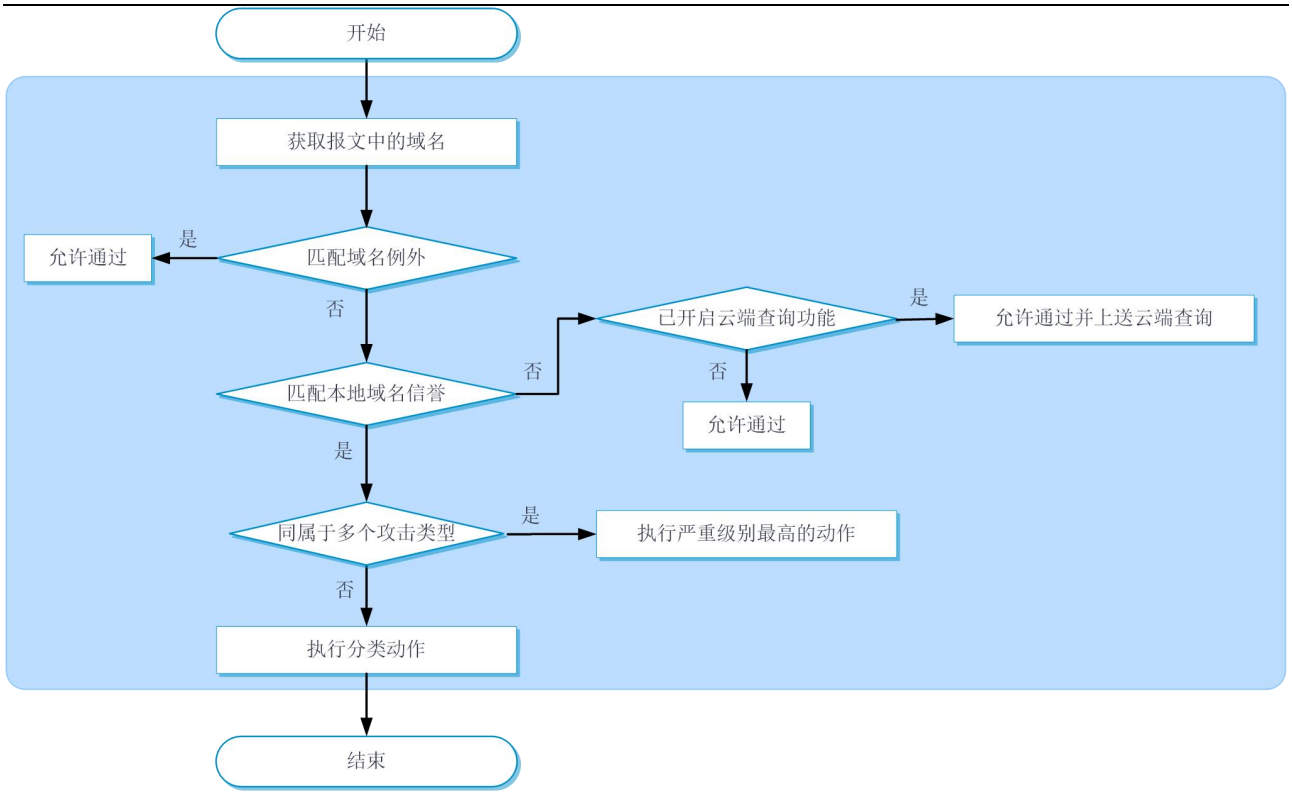
域名信誉特征库中，一个域名可对应多种攻击分类，每种攻击分类都有对应执行的动作。

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底依次为：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。

4.10.3.1.4　域名信誉的报文处理流程

域名信誉对报文的处理流程如下图所示：



域名信誉功能对报文的处理过程如下：

步骤1　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。

步骤2　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。

4.10.3.1.5 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。

4.10.3.2 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。

4.10.3.3 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”。

4.10.3.4 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。

4.10.3.5 配置指南

域名信誉功能的具体配置步骤如下：

步骤1 选择“策略 > 主动防护 > 威胁情报”。

步骤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。

步骤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。

步骤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。

步骤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。

步骤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。

步骤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。

步骤8　完成配置后，单击<应用>按钮，使配置生效。

4.10.3.5.2　配置例外域名

配置例外域名的具体配置步骤如下：

步骤1　选择“策略 > 主动防护 > 威胁情报”。

步骤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。

步骤3　单击<应用>按钮，完成配置。

4.10.4　统一威胁平台下发情报

4.10.4.1　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。

4.10.4.2　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。

4.10.4.3　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。

4.11 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IP黑名单
  - 批量导入IP黑名单
  - 配置地址对象组黑名单

4.11.1 特性简介

4.11.1.1 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。

4.11.1.2 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。

4.11.2 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。

4.11.3 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。
- 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。

4.11.4 配置指南

通过配置黑名单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。

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。

导出功能，导出指定的csv格式文件，然后填写需要导入的IP地址，供导入时使用。导入功能，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。导入文件的格式必须为.csv。

4.11.4.1 配置IP黑名单

步骤1 单击“策略 > 主动防护 > 黑名单”。

步骤2 在“IP黑名单”页签单击<新建>按钮。

步骤3 手工添加IP黑名单。

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 > VRF”页面查看
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”时，支持配置本参数 仅当“IP 地址方向”选择“源地址”时，支持配置本参数
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，除非用户手动将其删除
备注信息	添加 IP 黑名单相关描述信息

步骤4　单击<确定>按钮，新建的黑名单会在“IP黑名单”页签显示。

步骤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。

4.11.4.2　批量导入IP黑名单

步骤1　单击“策略 > 主动防护 > 黑名单”。

步骤2　选择“IP黑名单”页签，在“IP黑名单”页面单击<导入配置>按钮，进入“导入指定配置”页面。

步骤3　在“导入指定配置”页面的具体配置内容如下表所示：

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 > VRF”页面查看
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

步骤4　单击<确定>按钮，批量导入IP黑名单成功，且会在“IP黑名单”页面中显示。

4.11.4.3　配置地址对象组黑名单

步骤1　单击“策略 > 主动防护 > 黑名单”。

步骤2　在“地址对象组黑名单”页签单击<新建>按钮。

步骤3　手工添加地址对象组黑名单。

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 > 对象组”对应的 IPv4/IPv6 地址对象组页面查看

步骤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。

步骤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。

4.12　并发连接限制

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

4.12.1　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。

4.12.1.1　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。

4.12.1.2 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

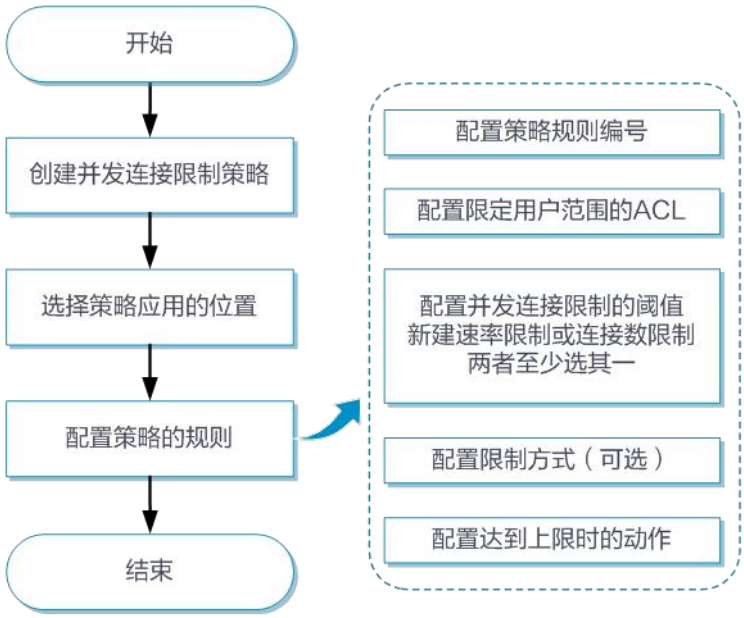
理安排规则的编号顺序，推荐按照限制粒度和范围由小到大的顺序来设置规则序号。

4.12.2 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 I P 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。

4.12.3 配置指南

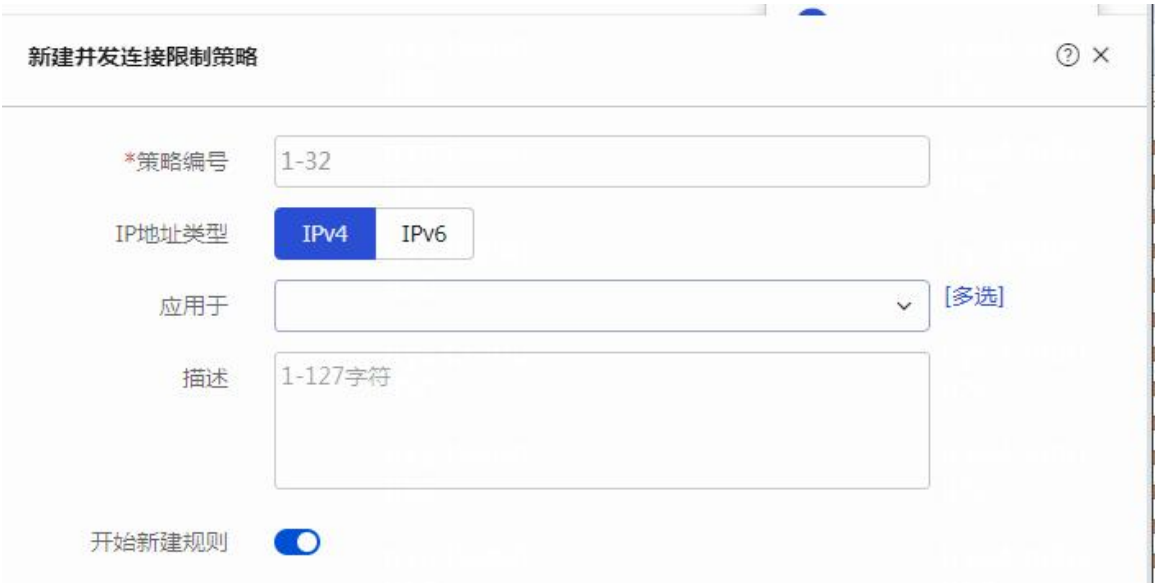
并发连接限制功能的配置思路如下图所示。



具体步骤如下：

步骤1　单击“策略 > 主动防护 > 并发连接限制”。

步骤2　在“并发连接限制”页面单击<新建>按钮。



步骤3　配置并发连接限制策略参数，具体参数如下表所示：

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 并发连接限制规则配置页面
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，将不能建立新的连接 ◆ 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连接
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，即具有相同服务端口的连接数目将受到指定阈值的限制
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。若黑名单功能未开启时，IP加入黑名单不生效，

参数	说明
	请进入策略 > 主动防护 > 黑名单页面开启全部应用）
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

步骤4　单击<确定>按钮，新建成并发连接限制策略功，且会在“并发连接限制”页面中显示。

4.13　服务器外联防护

本帮助主要介绍以下内容：

- 特性简介
- 配置指南
  - 服务器外联学习
  - 配置服务器外联防护策略

4.13.1　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。

4.13.2　配置指南

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。

4.13.2.1　服务器外联学习

服务器外联学习的具体配置步骤如下：

步骤1　选择“策略 > 主动防护 > 服务器外联防护”。

步骤2　在“服务器外联防护”页面选择<服务器外联学习>页签。

步骤3　输入需要监测的服务器的IP地址，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。

4.13.2.2 配置服务器外联防护策略

服务器异常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系行为时，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：

步骤1 选择“策略 > 主动防护 > 服务器外联防护”。

步骤2 在“防护策略”页签，单击<新建>按钮。

步骤3 新建防护策略，具体配置内容如下表所示：

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。关于新建和编辑功能，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

4.14 IP限速

4.14.1 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。

4.14.2 vSystem相关说明

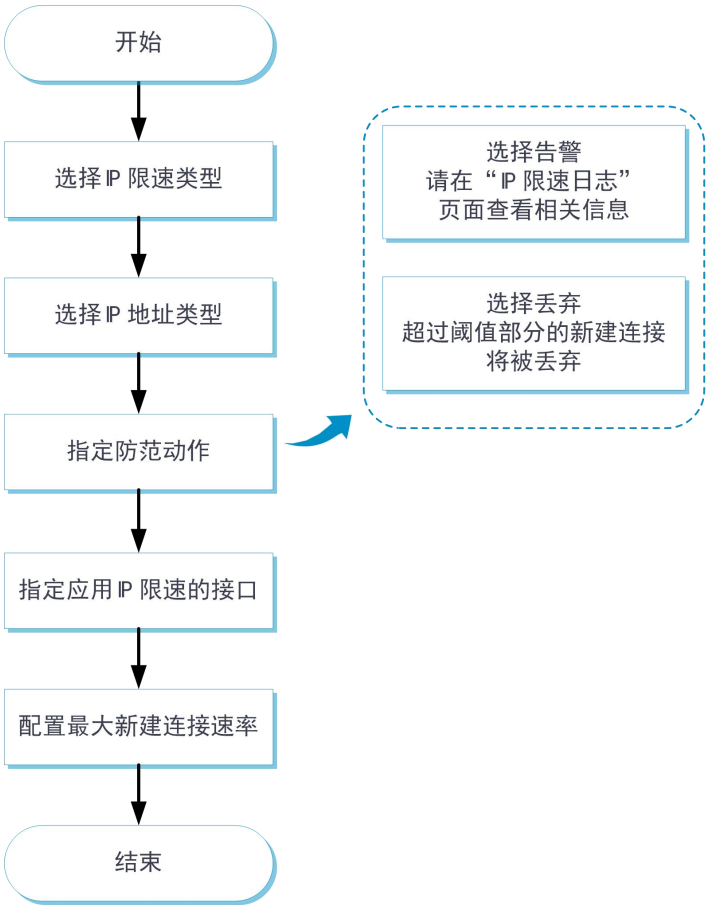
非缺省VSystem对于本特性的支持情况，请以页面的实际显示为准。

4.14.3 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。

4.14.4 配置指南

配置思路如下图所示。



4.14.4.1 配置步骤

步骤1 单击“策略 > 主动防护 > IP限速”。

步骤2 根据需求请选择公网防护或内网防护。

步骤3 具体配置内容如下表所示：

参数	说明
IP 类型	◆ IPv4 ◆ IPv6

参数	说明
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

步骤4　单击<确定>按钮，完成配置。

4.15　服务器负载均衡

本帮助主要介绍以下内容：

- 特性简介
  - 部署模式
  - 服务器负载均衡关系图
- vSystem相关说明
- License支持情况
- 配置指南
  - 实服务组
  - 实服务器
  - 负载均衡策略（可选）
  - 连接数限制策略（可选）
  - 防护策略（可选）
  - 参数模板（可选）
  - 智能探测模板（可选）
  - 虚服务器

4.15.1 特性简介

服务器负载均衡是一种集群技术，它将特定的业务（网络服务、网络流量等）分担给多台服务器或防火墙，从而提高了业务处理能力，保证了业务的高可靠性。

根据识别信息的层级不同，服务器负载均衡又分为以下两种：

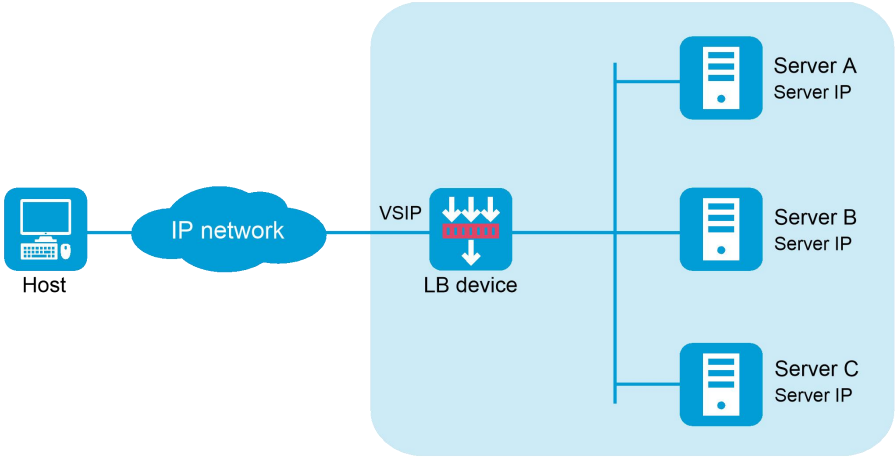
- 四层服务器负载均衡：可识别网络层和传输层信息，是基于流的负载均衡，通过对报文进行逐流分发，将同一条流的报文分发给同一台服务器。由于四层服务器负载均衡对七层业务无法按内容分发，从而限制了其适用范围。
- 七层服务器负载均衡：除了可识别网络层和传输层信息之外，还可识别应用层信息，是基于内容的负载均衡，通过对报文承载的内容进行深度解析，根据其中的内容进行逐包分发，按既定策略将连接导向指定的服务器，从而实现了业务范围更广泛的服务器负载均衡。

服务器负载均衡支持IPv4与IPv6，但四层服务器负载均衡不支持IPv4报文与IPv6报文的互相转换。

4.15.1.1 部署模式

服务器负载均衡在网络中的部署模式有NAT（Network Address Translation，网络地址转换）模式和旁路模式两种，以下分别进行介绍。

4.15.1.2 NAT模式

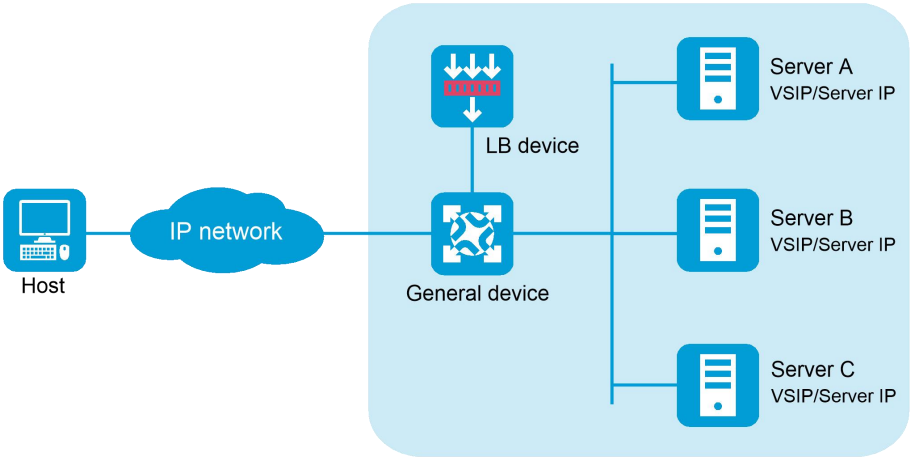


如图所示，NAT模式服务器负载均衡包含以下要素：

- LB device（负载均衡设备）：负责将各种服务请求分发到多台服务器。
- Server（服务器）：负责响应和处理各种服务请求。
- VSIP（Virtual Service IP，虚服务IP）：集群对外提供服务的IP地址，供用户请求服务时使用。

- Server IP（服务器IP）：供负载均衡设备分发服务请求时使用。

4.15.1.3 旁路模式

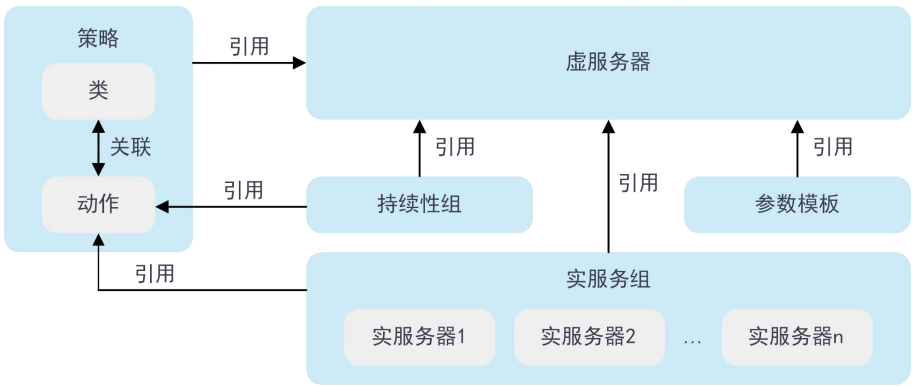


如图所示，旁路模式服务器负载均衡包含以下要素：

- LB device（负载均衡设备）：负责将各种服务请求分发到多台服务器。
- General device（通用设备）：按照正常的转发规则转发数据。
- Server（服务器）：负责响应和处理各种服务请求。
- VSIP（Virtual Service IP，虚服务IP）：集群对外提供服务的IP地址，供用户请求服务时使用。
- Server IP（服务器IP）：供负载均衡设备分发服务请求时使用。

旁路模式又称单臂模式。在此模式下，需在负载均衡设备和服务器上都配置VSIP（要求服务器不能通过VSIP发送和响应ARP请求，比如可将VSIP配置在服务器的LoopBack接口上）。

4.15.1.4 服务器负载均衡关系图



4.15.2 vSystem相关说明

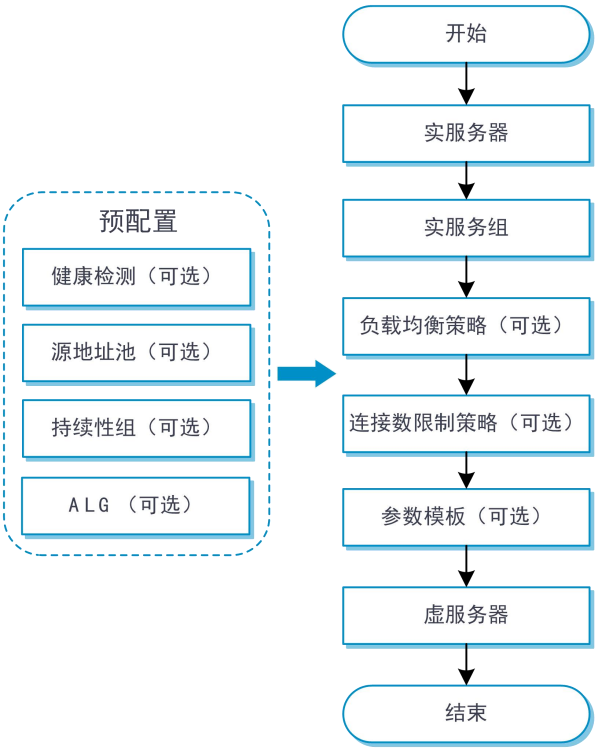
非缺省vSystem对于本特性的支持情况，请以页面的实际显示为准。

4.15.3 License支持情况

服务器负载均衡功能需要购买并正确安装License才能使用，关于License的详细介绍请参见“License联机帮助”。

4.15.4 配置指南

服务器负载均衡功能的配置思路如下图所示：



4.15.4.1 实服务组

为了便于对实服务器进行统一管理，可将具有相同或相似功能的实服务器抽象成一个组，称为实服务组。比如，可按存储内容的不同划分为歌曲服务器组、视频服务器组和图片服务器组等。实服务组可被虚服务器或动作引用。

4.15.4.1.1 配置步骤

步骤1　单击“策略 > 负载均衡 > 服务器负载均衡 > 实服务组”。

步骤2　在“实服务组”页面单击<新建>按钮。

步骤3　新建实服务组。

参数	说明
实服务组名称	实服务组的名称，不区分大小写
调度算法	选择实服务组的调度算法，包括： ◆ 加权轮转：即根据实服务器权值的大小把新连接依次分发给每台实服务器，权值越大，分配的新连接越多 ◆ 随机：把新连接随机分发给每个实服务器 ◆ 加权最小连接：总是把新连接分发给加权活动连接数（当前活动连接数/权值）最小的实服务器。该算法中使用的权值为实服务器页面配置的权值 ◆ 带宽：根据实服务器的权值与剩余带宽的比例把用户请求分发给每个实服务器 ◆ 最大带宽：总是将用户请求分发给处于空闲状态且剩余带宽最大实服务器 ◆ 动态反馈：**根据实服务器的内存使用率、CPU使用率和磁盘使用率等信息计算出当前的负载能力权值，负载越小，权值越大，分配到的新连接越多** ◆ 最快响应：**根据实服务器的响应时间计算出当前负载能力的权值，响应时间越短，权值越大，分配到的新连接越多** ◆ 源IP地址哈希：根据源IP地址进行的哈希算法，设备将具有相同源IP地址的用户请求分配给相同的实服务器，适用于同一源IP地址发起的请求必须要调度到同一台实服务器的场景 ◆ 源IP地址CARP哈希：根据源IP地址进行的CARP哈希算法，适用于同一源IP地址发起的请求必须要调度到同一台实服务器的场景。当可用实服务器不变时，设备将具有相同源IP地址的用户请求分配给相同的实服务器。对于同一源IP地址发起的访问请求，采用CARP哈希算法，当可用实服务器发生变化时，设备可使当前所有可用实服务器负载分担变动最小 ◆ 源IP地址和端口哈希：根据源IP地址和端口号进行的哈希算法，设备将具有相同源IP地址和端口的用户请求分配给相同的实服务器，适用于同一源IP地址和端口发起的请求必须要调度到同一台实服务器的场景 ◆ 源IP地址和端口CARP哈希：根据源IP地址和端口号进行的CARP哈希算法，适用于同一源IP地址和端口发起的请求必须要调度到同一台实服务器的场景。当可用实服务器不变时，设备将具有相同源IP地址和端口的用户请求分配给相同的实服务器。对于同一源IP地址和端口发起的访问请求，采用CARP哈希算法，当可用实服务器发生变化时，设备可使当前所有可用实服务器负载分担变动最小 ◆ 目的IP地址哈希：根据目的IP地址进行的哈希算法，设备将具有相同目的IP地址的用户请求分配给相同的实服务器，适用于客户端一系列相关业务处理都需要和同一台实服务器反复通信的场景 ◆ 目的IP地址CARP哈希：根据目的IP地址进行的CARP哈希算法，适用于客户端一系列相关业务处理都需要和同一台实服务器反复通信的场景。当可用实服务器不变时，设备将具有相同目的IP地址的用户请求分配给相同的实服务器。对于访问同一目的IP地址的用户请求，采用CARP哈希算法，当可用实服务器发生变化时，设备可使当前所有可用实服务器负载分担变动最小

参数	说明
	◆ HTTP哈希：根据HTTP载荷进行的哈希算法，设备将具有相同HTTP载荷的用户请求分配给相同的实服务器。只有被HTTP类型的虚服务器引用时生效 ◆ HTTP CARP哈希：根据HTTP载荷进行的CARP哈希算法，当可用实服务器不变时，设备将HTTP载荷相同的用户请求分配给相同的实服务器。当可用实服务器发生变化时，设备可使当前所有可用实服务器负载分担变动最小。只有被HTTP类型的虚服务器引用时生效 ◆ 加权最小连接（基于成员）：总是把新连接分发给加权活动连接数（当前活动连接数/权值）最小的实服务器。该算法中使用的权值为实服务组成员页面配置的权值 ◆ 最快响应（基于成员）：根据实服务组成员的响应时间计算出当前的负载能力权值的算法，响应时间越小，权值越大，分配到的新连接越多 缺省情况下，调度算法为加权轮转算法
偏移量	**基于 HTTP 载荷起始位置的偏移量** 仅当调度算法为 HTTP 哈希或 HTTP CARP 哈希时，才支持本参数
起始标记	**HTTP 载荷起始位置的正则表达式，即从偏移量起到本标记为开始，**不支持正则元字符？ 仅当调度算法为 HTTP 哈希或 HTTP CARP 哈希时，才支持本参数
长度/结束标记	◆ **长度：参与运算的HTTP载荷的长度** ◆ **结束标记：HTTP载荷结束位置的正则表达式，即从起始标记起到本标记为结束，**不支持正则元字符？ 仅当调度算法为 HTTP 哈希或 HTTP CARP 哈希时，才支持本参数
优先级调度	缺省情况下，一个实服务组中调用优先级最高的实服务器全部被调度算法调用。用户通过本配置可以限制实服务组中可被调度算法调用的实服务器的数量： ◆ 如果调用优先级最高的可用实服务器数量大于“调用实服务器最大数量”时，则只选用“调用实服务器最大数量”个实服务器 ◆ 如果调用优先级最高的可用实服务器数量小于“调用实服务器最小数量”时，除了调用全部优先级最高的可用实服务器外，还会调用优先级次高的可用实服务器，直至调用的可用实服务器数量达到“调用实服务器最小数量”，或者没有可用的实服务器可调用为止 其中，实服务器的优先级在“实服务器”配置页面指定
成员列表	设备支持以下两种添加实服务组成员的方式： 新建实服务器并将实服务器添加为实服务组成员： 1） 单击<添加>按钮，选择“新建实服务器” 2） 配置实服务组成员信息，具体配置项说明请参见“实服务器”

参数	说明
	3） 单击<确定>按钮，新建的实服务器会在“成员列表”中显示 选择已存在的实服务器： 1） 单击<添加>按钮，选择“添加已存在的实服务器” 2） 在下拉列表中选择已创建的实服务器并配置实服务组成员信息，具体配置项说明请参见“实服务器” 3） 单击<确定>按钮，添加的实服务器会在“成员列表”中显示
健康检测方法	实服务组引用的健康检测模板。通过健康检测可以对实服务器进行检测，保证其能够提供有效的服务。 用户可在实服务组配置页面对组内的所有实服务组成员进行配置，也可在实服务组成员配置页面只对当前实服务组成员进行配置，或者在实服务器配置页面只对当前实服务器进行配置，后两者的配置优先级相同且高于实服务组页面的健康检测配置。建议优先在实服务组页面下配置健康检测 实服务器的健康检测结果影响实服务组成员的使用，实服务组成员的健康检测结果不影响实服务器的使用 1） 单击<新建>按钮，新建健康检测方法 ● 健康检测模板名称：实服务组引用的健康检测模板。可选择已创建的健康检测模板，也可以新创建健康检测模板 ● 使用模板的端口检测：若配置了本功能，则使用健康检测模板的目的端口进行检测；若未配置本功能，则使用实服务器的端口进行检测 2） 单击<确定>按钮，新建的健康检测方法会在“健康检测方法”中显示
描述	实服务组的描述信息

参数	说明
成功条件	实服务器的健康检测成功条件 ◆ 全部检测通过：只有全部健康检测方法都通过检测才认为健康检测成功 ◆ 至少n个检测通过：健康检测成功所需通过检测的最少方法数为n。当用户指定的最少方法数n大于设备上实际存在的方法数量时，只要实际存在的全部方法通过检测，系统也将认为健康检测成功

参数	说明
健康检测手动恢复	开启/关闭健康检测手动恢复功能 关闭健康检测手动恢复功能，当实服务组成员健康检测成功后，设备会自动将其恢复为可用状态。若开启健康检测手动恢复功能，当实服务组成员健康检测成功后，需要在“编辑实服务组”页面成员列表中，手动恢复其为可用状态
源地址转换方式	实服务组得源地址转换方式，包括： ◆ 源地址池：根据配置的源地址池进行源地址转换。设备将匹配报文的源地址修改为源地址池中的地址后再转发出去 ◆ 自动映射：采用设备与实服务器通信的接口地址进行源地址转换 ◆ TCP Option：根据收到报文的TCP Option字段携带的地址进行源地址转换 若未在实服务组页面配置源地址转换方式，则采用 SNAT 全局策略进行源地址转换
源地址池名称	实服务组进行源地址转换的源地址池名称 可选择已创建的源地址池，也可以新创建源地址池 仅当源地址转换方式配置为源地址池时，支持配置本参数
目的地址转换	在旁路模式下，需要在实服务组中关闭目的地址转换功能；在 NAT 模式下，需要在实服务组中开启目的地址转换功能
RST 报文监控	实服务组引用的 RST 类型的智能探测模板。通过引用 RST 类型的智能探测模板，对实服务组内所有实服务组成员进行监控 可选择已创建的智能探测模板，也可以新创建智能探测模板
零窗口报文监控	实服务组引用的零窗口类型的智能探测模板。通过引用零窗口类型的智能探测模板，对实服务组内所有实服务组成员进行监控 可选择已创建的智能探测模板，也可以新创建智能探测模板
HTTP 监控	实服务组引用的 HTTP passive 类型的智能探测模板。通过引用 HTTP passive 类型的智能探测模板，对实服务组内所有实服务组成员进行监控 可选择已创建的智能探测模板，也可以新创建智能探测模板
自定义监控	实服务组引用的自定义类型的智能探测模板。通过引用自定义类型的智能探测模板，对实服务组内所有实服务组成员进行自定义监控 可选择已创建的智能探测模板，也可以新创建智能探测模板 本参数对实服务组内配置域名的实服务组成员不生效
智能监控自动恢复	开启/关闭智能监控自动恢复功能。当配置了智能监控功能后，可以通过开启本功能使被 Auto shutdown 的实服务器在达到指定恢复时间后自动恢复为正常状态

参数	说明
	若没有配置健康检测，实服务器恢复后的状态置为未知状态 若配置了健康检测且健康检测成功，实服务器恢复后的状态置为可用状态，如果健康检测失败，则置为健康检测失败状态 仅当实服务组引用 HTTP passive 类型、RST 或零窗口类型的智能探测模板时，才支持开启本功能
恢复时间	实服务器自动恢复时间。0 表示实服务器不能自动恢复 仅当智能监控自动恢复功能处于开启状态时，才支持配置本参数
实服务器故障处理方式	选择实服务器的故障处理方式，包括： ◆ 保持已有连接：不主动断开与故障实服务器的连接，连接继续保持还是断开将由协议自身的超时机制决定 ◆ 重定向连接：把连接重定向到实服务组中其它可用的实服务器上 ◆ 断开已有连接：主动断开与故障实服务器的连接。对于TCP报文，将发送RST报文；对于其它类型的报文，将发送ICMP不可达报文
温暖上线	当向实服务组中添加实服务器时，某些新增的实服务器无法立即承担大量业务，此时可以开启温暖上线功能。这样，当实服务器上线后，在准备时间内，负载均衡设备不会向其分配任何业务；准备时间超时后，负载均衡设备在爬升时间内会逐步增加向其分配的业务量；爬升时间超时后，负载均衡设备开始向其正常分配业务 ◆ 准备时间：取值范围为0～600，单位为秒 ◆ 爬升时间：取值范围为3～600，单位为秒
繁忙处理方式	用于指定实服务组处于繁忙状态时的处理方式，只有当组内所有实服务器均处于繁忙状态时，实服务组才处于繁忙状态，包括： ◆ 强制调度：所有实服务器均参与调度 ◆ 排队等待：将繁忙时的连接缓存起来，加入等待队列 ● 队列长度：当等待队列的长度超过配置的队列长度时，后续的连接将被丢弃 ● 超时时间：当排队等待的时间超过配置的超时时间时，连接将被丢弃 ◆ 调度失败：设备将停止向该实服务组分发流量，而是继续匹配负载均衡策略中的下一条引用规则或直接丢弃请求报文 实服务器的繁忙状态判断依据为，实服务器最大连接数、每秒最大连接数、每秒HTTP请求数、实服务下最大带宽、最大上行带宽、最大下行带宽和SNMPDCA探测模板返回的探测状态
可用条件	通过配置实服务组的可用条件，可将流量在主用实服务组和备用实服务组之间进行切换 ◆ 最小可用百分比：当主用实服务组中可用的实服务器数量占实服务器总数量的百分比低于此值时，该实服务组将被认为不可用，从而切换到备用实服务组

参数	说明
	◆ 最大可用百分比：必须大于等于最小可用百分比。当主用实服务组中可用的实服务器数量占实服务器总数量的百分比高于此值时，将从备用实服务组切换回主用实服务组
所有实服务组成员均不可用	配置查找所有可用实服务组成员失败时的处理方式，包括： ◆ 丢弃：直接丢弃报文 ◆ 转发：转发给最近一次选中的实服务组成员

步骤4　单击<确定>按钮，新建的实服务组会在“实服务组”页面显示。

4.15.4.2　实服务器

实服务器是负载均衡设备上处理用户业务的实体。一个实服务器可以属于多个实服务组，一个实服务组也可以包含多个实服务器。

4.15.4.2.1　配置步骤

步骤1　单击“策略 > 负载均衡 > 服务器负载均衡 > 实服务器”。

步骤2　在“实服务器”页面单击<新建>按钮。

步骤3　新建实服务器。

参数	说明
实服务器名称	实服务器的名称，不区分大小写
类型	实服务器的类型，包括： ◆ 地址 ◆ 域名
实服务器 IPv4 地址	实服务器的 IPv4 地址 不能为环回地址、组播地址、广播地址和 0.X.X.X
实服务器 IPv6 地址	实服务器的 IPv6 地址 不能为环回地址、组播地址、链路本地地址和全 0 地址
域名	实服务器的域名 配置实服务器域名后，设备会立刻向 DNS 服务器发送域名查询请求，并依据查询结果创建名称为“auto_*X.X.X.X*”的实服务器。若实服务器的域名解析为多个 IP 地址，设备会自动创建多个实服务器 配置实服务器的域名，则必须在“DNS”页面指定进行域名解析的 DNS 服务器 不同的实服务器不可以配置相同的域名
实服务器端口	实服务器的端口号，0 表示继续使用原报文携带的端口号
VRF	使实服务器服务于特定的 VRF
VRF 继承	开启/关闭 VRF 继承功能

参数	说明
	若在“实服务器”配置页面指定了实服务器所属的 VRF，则实服务器服务于该 VRF。若未指定实服务器所属的 VRF，当实服务器的 VRF 继承功能处于开启状态时，实服务器所属的 VRF 与虚服务器所属的 VRF 一致
健康检测日志	开启/关闭健康检测日志功能 开启健康检测日志功能后，可在实服务器的健康状态发生变化时输出日志信息
实服务器功能	开启/关闭实服务器
描述	实服务器的描述信息

参数	说明
权值	实服务器的权值。在进行调度时，该数值越大，实服务器越被优先调用
优先级	实服务器在实服务组中的调用优先级，数值越大，越被优先调用 优先使用高优先级的实服务器处理流量。如果最高优先级实服务器的个数少于配置的“调用实服务器最大数量”，则在次高优先级中选择实服务器，达到配置的“调用实服务器最小数量” 其中，“调用实服务器最大数量”和“调用实服务器最小数量”在“实服务组”配置页面指定
实服务组	实服务器所属的实服务组。可选择已创建的实服务组，也可以新创建实服务组
健康检测-健康检测方法	实服务器引用的健康检测模板。通过健康检测可以对实服务器进行检测，保证其能够提供有效的服务。 用户可在实服务组配置页面对组内的所有实服务组成员进行配置，也可在实服务组成员配置页面只对当前实服务组成员进行配置，或者在实服务器配置页面只对当前实服务器进行配置，后两者的配置优先级相同且高于实服务组页面的健康检测配置。建议优先在实服务组页面下配置健康检测 实服务器的健康检测结果影响实服务组成员的使用，实服务组成员的健康检测结果不影响实服务器的使用 1） 单击<新建>按钮，新建健康检测方法 ● 健康检测模板名称：实服务器引用的健康检测模板。可选择已创建的健康检测模板，也可以新创建健康检测模板 ● 使用模板的端口检测：若配置了本功能，则使用健康检测模板的目的端口进

参数	说明
	行检测；若未配置本功能，则使用实服务器的端口进行检测 2) 单击<确定>按钮，新建的健康检测方法会在“健康检测方法”中显示
健康检测-成功条件	实服务器的健康检测成功条件 ◆ 全部检测通过：只有全部健康检测方法都通过检测才认为健康检测成功 ◆ 至少n个检测通过：健康检测成功所需通过检测的最少方法数为n。当用户指定的最少方法数n大于设备上实际存在的方法数量时，只要实际存在的全部方法通过检测，系统也将认为健康检测成功
自定义监控	实服务器引用的自定义类型的智能探测模板。通过引用自定义类型的智能探测模板，对实服务器进行监控 可选择已创建的智能探测模板，也可以新创建智能探测模板 配置域名的实服务器不支持引用本参数
健康检测手动恢复	开启/关闭健康检测手动恢复功能。关闭健康检测手动恢复功能，当实服务组成员健康检测成功后，设备会自动将其恢复为可用状态。若开启健康检测手动恢复功能，当实服务组成员健康检测成功后，需要在“编辑实服务组”页面成员列表中，手动恢复其为可用状态 仅实服务组成员支持本参数
关联变量	本参数可用于通用负载均衡动作的 TCP 载荷重写，重写 TCP 载荷的动作通过调用实服务组成员的关联变量将 TCP 报文载荷的指定内容替换为实服务组成员关联的变量值。例如：配置变量名为 var1，变量值为_1，再配置重写 TCP 载荷动作为将 QMGR.SO1 重写为 QMGR.SO1%[var1]，重写后，将把 TCP 请求报文中的字符串 QMGR.SO1 替换为 QMGR.SO1_1 1) 单击<新建>按钮，新建关联变量 ● 变量名：实服务组成员关联的变量名称，区分大小写 ● 变量值：实服务组成员关联的变量值，区分大小写 2) 单击<确定>按钮，新建的关联变量会在“关联变量”中显示 仅实服务组成员支持本参数
QoS-最大连接数	实服务器所允许的最大连接数，0 表示实服务器所允许的最大连接数不受限制
QoS-每秒最大连接数	实服务器所允许的每秒最大连接数，0 表示实服务器所允许的每秒最大连接数不受限制

参数	说明
QoS-每秒 HTTP 请求数	实服务器所允许的每秒 HTTP 请求数，0 表示实服务器所允许的每秒 HTTP 请求数不受限制
QoS-最大带宽	实服务器所允许的最大总带宽，0 表示最大带宽不受限制
QoS-最大上行带宽	实服务器所允许的最大上行带宽，0 表示最大带宽不受限制
QoS-最大下行带宽	实服务器所允许的最大下行带宽，0 表示最大带宽不受限制

步骤4　单击<确定>按钮，新建的实服务器会在“实服务器”页面显示。

4.15.4.3　负载均衡策略（可选）

将流量特征和动作关联起来就构成了负载均衡策略。负载均衡策略是指导报文转发的一种方式，用户可以为匹配特定流量特征的报文指定执行的动作，以及为未匹配任何流量特征的报文指定默认动作。用户可以在一个负载均衡策略中指定多个流量特征，转发报文时会按照配置顺序来匹配流量特征，匹配成功则执行相应的动作，不会继续匹配下一条流量特征，否则继续匹配下一条流量特征。因此，当流量特征之间存在包含关系时，建议将更精细的流量特征放在前面，宽泛的流量特征放在后面。如果所有流量特征均未匹配，则执行默认动作。

负载均衡策略可被虚服务器引用。

Diameter类型负载均衡策略仅对Diameter协议类型的请求报文有效。

4.15.4.3.1　流量特征配置步骤

步骤1　单击“策略 > 负载均衡 > 服务器负载均衡 > 高级策略 > 流量特征”。

步骤2　在“流量特征”页面单击<新建>按钮。

步骤3　新建流量特征。

参数	说明
流量特征名称	流量特征的名称，不区分大小写
类型	流量特征的类型，包括： ◆ 通用：用于四层服务器负载均衡 ◆ HTTP：用于七层服务器负载均衡 ◆ RADIUS：用于七层服务器负载均衡 ◆ MySQL：用于七层服务器负载均衡 ◆ Diameter：用于七层服务器负载均衡，Diameter协议是计算机网络中使用认证、授权、计费的一种协议，从功能更少的RADIUS协议升级进化而来

参数	说明
匹配方式	流量特征的匹配方式，包括： ◆ 匹配任意一条规则：匹配任一规则就算匹配该流量特征 ◆ 匹配所有规则：匹配所有规则才算匹配该流量特征
匹配规则	通过匹配规则将报文按照一定条件进行匹配，以便将不同类型的报文在不同的动作流程中处理。一个流量特征中最多允许创建 65535 条匹配规则 3) 单击<新建>按钮，新建匹配规则 ● Match ID：匹配规则的编号，报文按照Match ID从小到大的顺序依次进行匹配 ● 类型：匹配规则的类型，包括：源IPv4、源IPv6、流量特征、IPv4 ACL、IPv6 ACL、Cookie、HTTP Header、Method、URL、Content、用户、RADIUS属性、入接口、HTTP版本、ISP、TCP载荷和MySQL、应用ID和目的域 ● IPv4地址：匹配指定的IPv4地址，只有匹配规则的类型选择“源IPv4”时，才会出现该参数 ● 掩码长度：IPv4地址的掩码长度，只有匹配规则的类型选择“源IPv4”时，才会出现该参数 ● IPv6地址：匹配指定的IPv6地址，只有匹配规则的类型选择“源IPv6”时，才会出现该参数 ● 前缀长度：IPv6地址的前缀长度，只有匹配规则的类型选择“源IPv6”时，才会出现该参数 ● 流量特征：匹配指定的流量特征，只有匹配规则的类型选择“流量特征”时，才会出现该参数 ● ACL：匹配指定的ACL，可选择已创建的ACL，也可以新创建ACL。只有匹配规则的类型选择“IPv4 ACL”或“IPv6 ACL”时，才会出现该参数 ● Cookie名称:HTTP报文的Cookie名称,区分大小写。不包括(、)、<、>、@、,、;、:、\、"、/、[、]、?、=、{、}、SP（空格符）、HT（水平制表符），以及ASCII码中小于等于31、大于等于127的字符。只有匹配规则的类型选择“Cookie”时，才会出现该参数 ● Cookie值：Cookie值的正则表达式，不支持正则元字符?。只有匹配规则的类型选择“Cookie”时，才会出现该参数 ● Header名称:HTTP报文首部的名称,不区分大小写。不包括(、)、<、>、@、,、;、:

参数	说明
	\、"、/、[、]、?、=、{、}、SP（空格符）、HT（水平制表符），以及ASCII码中小于等于31、大于等于127的字符。只有匹配规则的类型选择“HTTP Header”时，才会出现该参数 ● Header值：首部值的正则表达式，不支持正则元字符?。只有匹配规则的类型选择“HTTP Header”时，才会出现该参数 ● 扩展类型:包括预定义和自定义两种类型。只有匹配规则的类型选择“Method”时，才会出现该参数 ● 方法：预定义方法包括GET、CONNECT、DELETE、HEAD、OPTIONS、POST、PUT和TRACE；自定义方法区分大小写。不包括(、)、<、>、@、,、;、:、\、"、/、[、]、?、=、{、}、SP（空格符）、HT（水平制表符），以及ASCII码中小于等于31、大于等于127的字符。只有匹配规则的类型选择“Method”时，才会出现该参数 ● URL:URL的正则表达式，不支持正则元字符?。只有匹配规则的类型选择“URL”时，才会出现该参数 ● Content偏移：HTTP实体基于HTTP报文起始位置的偏移量。只有匹配规则的类型选择“Content”时，才会出现该参数 ● Content值：HTTP实体的正则表达式，不支持正则元字符?。只有匹配规则的类型选择“Content”时，才会出现该参数 ● 用户：匹配指定的用户或用户组，可选择已创建的身份识别用户或身份识别用户组，也可以新创建用户或用户组。只有匹配规则的类型选择“用户”时，才会出现该参数 ● 属性编号：RADIUS属性类型的编号，只有匹配规则的类型选择“RADIUS属性”时，才会出现该参数 ● 属性值：匹配RADIUS属性值的正则表达式，只有匹配规则的类型选择“RADIUS属性”时，才会出现该参数 ● 入接口：匹配指定的入接口，只有匹配规则的类型选择“入接口”时，才会出现该参数 ● HTTP版本：匹配指定的HTTP版本，只有匹配规则的类型选择“HTTP版本”时，才会出现该参数 ● ISP：匹配指定的ISP，可选择已创建的ISP，也可以新创建ISP。只有匹配规

参数	说明
	则的类型选择“ISP”时，才会出现该参数 ● TCP载荷：匹配TCP载荷的正则表达式，只有匹配规则的类型选择“TCP载荷”时，才会出现该参数 ● 不区分大小写：表示匹配正则表达式时对大小写不敏感。只有匹配规则的类型选择“TCP载荷”或“MySQL”时，才会出现该参数 ● 条件取反：若未配置本条件取反，则流量匹配上指定的正则表达式之后，执行相应的负载均衡动作。若配置了条件取反，则在流量未匹配指定的正则表达式时，执行相应的负载均衡动作。只有匹配规则的类型选择“TCP载荷”或“MySQL”时，才会出现该参数 ● 正则表达式:匹配MySQL语句的正则表达式。只有匹配规则的类型选择“MySQL”时，才会出现该参数 ● 应用ID：匹配指定的应用编号，当Diameter请求报文中的应用ID与该流量特征指定的应用ID匹配成功，则执行相应动作。指定的应用ID应为Diameter基础协议和扩展协议中定义的应用识别号。只有匹配规则的类型选择“Diameter”时，才会出现该参数 ● 目的域：匹配指定的目的域名，当Diameter报文中的目的域名与该流量特征指定的目的域匹配成功，则执行相应动作。只有匹配规则的类型选择“Diameter”时，才会出现该参数 4) 单击<确定>按钮，新建的匹配规则会在“匹配规则”中显示
描述	流量特征的描述信息

步骤4 单击<确定>按钮，新建的流量特征会在“流量特征”页面显示。

4.15.4.3.2 动作配置步骤

步骤1 单击“策略 > 负载均衡 > 服务器负载均衡 > 高级策略 > 动作”。

步骤2 在“动作”页面单击<新建>按钮。

步骤3 新建动作。

参数	说明
动作名称	动作的名称，不区分大小写
类型	动作类型，包括： ◆ 通用

参数	说明
	◆ HTTP ◆ HTTP重定向 ◆ RADIUS ◆ Diameter
转发动作	转发动作，包括： ◆ 负载均衡 ◆ 丢弃报文 ◆ 转发，仅通用类型和RADIUS类型支持 ◆ 直接代答，仅HTTP类型支持 ◆ 若负载均衡策略在SIP、HTTP、Performance(HTTP)、HTTP重定向、HTTPS、MySQL或七层TCP类型的虚服务器中引用，则转发动作配置为转发不生效
非压缩文件代答	如果客户端请求 URL 中的资源路径匹配指定的 URL 资源路径，则用指定的非压缩代答文件对客户端请求进行应答 1) 单击<新建>按钮，新建非压缩文件代答 ● URL资源路径：用来匹配客户端请求URL中的资源路径，区分大小写，该路径必须以/开始 ● 非压缩代答文件：用来对客户端请求进行代答的非压缩文件的绝对路径+文件名称，不区分大小写，如：flash:/file.html。对于同一URL只允许用一个非压缩文件进行代答。同一个非压缩文件可以代答不同的URL 2) 单击<确定>按钮 仅当转发动作为直接代答时支持本参数
压缩文件代答	如果客户端请求 URL 中的资源路径匹配配置的工作路径+ZIP 压缩包内相对路径，则使用 ZIP 压缩包内的文件答复客户端。例如：用户配置对指定的 HTTP 请求进行代答的工作路径为/index,压缩代答文件为 flash:/za/zb/test.zip，test.zip 中存在如下压缩目录关系/css/col.css,则实际匹配的 URL 资源路径为/index/css/col.css，代答文件为 col.css ◆ 工作路径：用“工作路径+ZIP压缩包内相对路径”来匹配客户端请求URL中的资源路径，区分大小写，该路径必须以/开始 ◆ 压缩代答文件：用来对客户端请求进行代答的压缩文件的绝对路径+文件名称，不区分大小写，且必须为ZIP格式。如：flash:/file.zip 仅当转发动作为直接代答时支持本参数
查找实服务器失败的处理	◆ 丢弃报文：配置查找可用实服务器失败时，负载均衡设备会直接丢弃报文 ◆ 继续匹配下一条规则：配置查找可用实服务器失败时，可继续顺序匹配策略中的下一条引用规则 ◆ 用指定文件进行代答：配置查找可用实服务器失败时，用指定

参数	说明
	的默认代答文件答复客户端 ● 默认代答文件：配置格式为非压缩文件绝对路径+文件名称，不区分大小写，如：flash:/file.html ◆ 关闭TCP连接（FIN）：配置查找可用实服务器失败时，发送FIN关闭TCP连接 ◆ 关闭TCP连接（RST）：配置查找可用实服务器失败时，发送RST关闭TCP连接 仅当转发动作为负载均衡时支持本参数 若负载均衡策略在 SIP 类型的虚服务器中被引用，则查找实服务器失败的处理配置为继续匹配下一条规则不生效
查找代答文件失败的处理	◆ 丢弃报文：配置查找可用实服务器失败时，负载均衡设备会直接丢弃报文 ◆ 继续匹配下一条规则：配置查找代答文件失败时，可继续顺序匹配策略中的下一条引用规则 ◆ 用指定文件进行代答：配置查找代答文件失败时，用指定的默认代答文件答复客户端 ● 默认代答文件：配置格式为非压缩文件绝对路径+文件名称，不区分大小写，如：flash:/file.html ◆ 关闭TCP连接（FIN）：配置查找代答文件失败时，发送FIN关闭TCP连接 ◆ 关闭TCP连接（RST）：配置查找代答文件失败时，发送RST关闭TCP连接 仅当转发动作为直接代答时支持本参数
TCP 连接关闭的方式	◆ FIN：FIN方式关闭TCP连接 ◆ RST：RST方式关闭TCP连接 仅当转发动作为丢弃报文时支持本参数
ToS	发往服务器的 IP 报文中的 ToS 字段
描述	动作的描述信息
默认实服务组-主用实服务组	当主用实服务组可用（该实服务组存在且有可用的实服务器）时，使用主用实服务组指导转发；当主用实服务组不可用而备用实服务组可用时，使用备用实服务组指导转发 可选择已创建的实服务组，也可以新创建实服务组 仅当转发动作为负载均衡时支持本参数
默认实服务组-备用实服务组	可选择已创建的实服务组，也可以新创建实服务组 仅当转发动作为负载均衡时支持本参数
默认实服务组-持续性组	可选择已创建的持续性组，也可以新创建持续性组 仅当转发动作为负载均衡时支持本参数

参数	说明
HTTP 重定向配置-重定向 URL	在 HTTP 重定向类型的动作中配置了重定向 URL 后，所有匹配对应动作的 HTTP 请求报文都将被重定向到指定 URL 重定向 URL 区分大小写，也可以使用？和以下特定含义的字符串： ◆ %h：表示客户端请求报文中的主机名 ◆ %p：表示客户端请求报文中的URL ◆ %%：表示字符% 仅 HTTP 重定向类型的动作支持本参数
HTTP 重定向配置-重定向方式	◆ 临时重定向-302 ◆ 临时重定向-307 ◆ 永久重定向-301 仅 HTTP 重定向类型的动作支持本参数

参数	说明
TCP 载荷重写	1） 单击<新建>按钮，新建 TCP 载荷重写 ● 方向：包括双向、请求和应答方向的TCP报文 ● 重写前内容：要被重写的TCP报文载荷的内容，为正则表达式，区分大小写 ● 重写后内容：重写后的报文内容，区分大小写，支持携带以下变量： ● %[*variable*]，为实服务组成员关联的变量，其中，*variable*该变量的名称 ● %[1-9]，表示按照*value*中匹配上的内容替换成%[1-9]中对应()中的内容。例如：若配置重写前的内容为(Wel)(co)(me)，重写后的内容为%2，则将把Welcome字符串替换为第2个括号中的内容co 2） 单击<确定>按钮 仅通用类型的动作支持本参数 仅七层 TCP 类型的虚服务器支持引用包含该动作的负载均衡策略
插入 X-Forwarded-For	在 HTTP 首部插入 X-Forwarded-For 字段 仅 HTTP 类型的动作支持本参数
应答报文体重写-重写前内容	要被替换的 HTTP 报文体的内容 仅 HTTP 类型的动作支持本参数
应答报文体重写-重	替换后的 HTTP 报文体的内容。可以使用以下特定含义的字符串： ◆ %is：源IP地址或源IPv6地址

参数	说明
写后内容	◆ %ps：源端口号 ◆ %id：目的IP地址或目的IPv6地址 ◆ %pd：目的端口号 ◆ %%：字符% ◆ %[1-9]，替换成%[1-9]中对应()中的内容 仅 HTTP 类型的动作支持本参数
Header 删除	1） 单击<新建>按钮，新建 Header 删除 ● 方向：包括双向、请求和应答方向的HTTP报文 ● Header名称：HTTP报文首部的名称，包括标准和自定义的首部，需要与报文中的首部完全匹配。不区分大小写。不包括(、)、<、>、@、,、;、:、\、"、/、[、]、?、=、{、}、SP（空格符）、HT（水平制表符），以及ASCII码中小于等于31、大于等于127的字符 2） 单击<确定>按钮 仅 HTTP 类型的动作支持本参数
Header 插入	1） 单击<新建>按钮，新建 Header 插入 ● 方向：包括双向、请求和应答方向的HTTP报文 ● Header名称:要插入HTTP报文中的首部名称,包括标准和自定义的首部。不区分大小写。不包括(、)、<、>、@、,、;、:、\、"、/、[、]、?、=、{、}、SP（空格符）、HT（水平制表符），以及ASCII码中小于等于31、大于等于127的字符 ● Header值：要插入HTTP报文中的首部内容，不支持字符?。支持以下改写变量 ● %is：客户端侧的源IP地址 ● %ps：客户端侧的源端口号 ● %id：客户端侧的目的IP地址 ● %pd：客户端侧的目的端口号 ● %sps：服务器侧的源端口 ● %spd：服务器侧的目的端口

参数	说明
	● %sis：服务器侧的源IP地址 ● %sid：服务器侧的目的IP地址 ● %{x509v}：证书的版本 ● %{x509snum}：证书的序列号 ● %{x509sigalgo}：证书的签名算法 ● %{x509issuer}：证书的签发者 ● %{x509before}：证书的有效时间（在此时间之前无效） ● %{x509after}：证书的有效时间（在此时间之后无效） ● %{x509sub}：证书的主题 ● %{x509spktype}：证书的主题的公钥类型 ● %{x509spk}：证书的主题的公钥 ● %{x509spkRSA}：证书的主题的RSA公钥的长度（仅当公钥为RSA类型才有该字段） ● %{x509hash}：客户端证书的MD5散列（指纹） ● %{x509whole}：证书的全部内容 ● %{x509cipher}：证书的加密套件 ● %{dncn}：颁发给 ● %{dne}：电子邮件 ● %{dno}：公司/机构 ● %{dnou}：部门 ● %{dnc}：国家 ● %{dns}：州/省份 ● %{dnl}：城市 ● 变量编码方式：对改写变量的编码方式，包括原文、URL和Base64。原

参数	说明
	文即不对改写变量进行编码；URL编码方式只会对改写变量中的特殊字符进行编码，需要编码的特殊字符为：;、/、?、:、@、&、=、+、$、|、{、}、,、\、^、[、]、`、<、>、#、%、"、空格；Base64编码方式会对整个改写变量进行编码 2） 单击<确定>按钮 仅 HTTP 类型的动作支持本参数
Header 重写	1） 单击<新建>按钮，新建 Header 重写 ● 方向：包括双向、请求和应答方向的HTTP报文 ● Header名称：HTTP报文首部的名称，包括标准和自定义的首部，需要与报文中的首部完全匹配。不区分大小写。不包括(、)、<、>、@、,、;、:、\、"、/、[、]、?、=、{、}、SP（空格符）、HT（水平制表符），以及ASCII码中小于等于31、大于等于127的字符 ● Header值：要被重写的HTTP报文首部的内容，不支持字符? ● 替换成的资源串：重写后的内容。支持以下改写变量 ● %is：客户端侧的源IP地址 ● %ps：客户端侧的源端口号 ● %id：客户端侧的目的IP地址 ● %pd：客户端侧的目的端口号 ● %sps：服务器侧的源端口 ● %spd：服务器侧的目的端口 ● %sis：服务器侧的源IP地址 ● %sid：服务器侧的目的IP地址 ● %1-9：Header值中正则表达式取出的变量值，最多支持9个 ● %{x509v}：证书的版本 ● %{x509snum}：证书的序列号

参数	说明
	● %{x509sigalgo}：证书的签名算法 ● %{x509issuer}：证书的签发者 ● %{x509before}：证书的有效时间（在此时间之前无效） ● %{x509after}：证书的有效时间（在此时间之后无效） ● %{x509sub}：证书的主题 ● %{x509spktype}：证书的主题的公钥类型 ● %{x509spk}：证书的主题的公钥 ● %{x509spkRSA}：证书的主题的RSA公钥的长度（仅当公钥为RSA类型才有该字段） ● %{x509hash}：客户端证书的MD5散列（指纹） ● %{dncn}：颁发给 ● %{dne}：电子邮件 ● %{dno}：公司/机构 ● %{dnou}：部门 ● %{dnc}：国家 ● %{dns}：州/省份 ● %{dnl}：城市 ● 变量编码方式：对改写变量的编码方式，包括原文、URL和Base64。原文即不对改写变量进行编码；URL编码方式只会对改写变量中的特殊字符进行编码，需要编码的特殊字符为：;、/、?、:、@、&、=、+、$、|、{、}、,、\、^、[、]、`、<、>、#、%、"、空格；Base64编码方式会对整个改写变量进行编码 2） 单击<确定>按钮 仅 HTTP 类型的动作支持本参数
URL 重写	1） 单击<新建>按钮，新建 URL 重写

参数	说明
	● 匹配内容：要被重写的URL的内容，不支持字符? ● 改写内容：重写后的内容，支持以下改写变量 ● %is：客户端侧的源IP地址 ● %ps：客户端侧的源端口号 ● %id：客户端侧的目的IP地址 ● %pd：客户端侧的目的端口号 ● %sps：服务器侧的源端口 ● %spd：服务器侧的目的端口 ● %sis：服务器侧的源IP地址 ● %sid：服务器侧的目的IP地址 ● %1-9：要被重写的URL中正则表达式取出的变量值，最多支持9个 ● %{x509v}：证书的版本 ● %{x509snum}：证书的序列号 ● %{x509sigalgo}：证书的签名算法 ● %{x509issuer}：证书的签发者 ● %{x509before}：证书的有效时间（在此时间之前无效） ● %{x509after}：证书的有效时间（在此时间之后无效） ● %{x509sub}：证书的主题 ● %{x509spktype}：证书的主题的公钥类型 ● %{x509spk}：证书的主题的公钥 ● %{x509spkRSA}：证书的主题的RSA公钥的长度（仅当公钥为RSA类型才有该字段） ● %{x509hash}：客户端证书的MD5散列（指纹） ● %{dncn}：颁发给

参数	说明
	● %{dne}：电子邮件 ● %{dno}：公司/机构 ● %{dnou}：部门 ● %{dnc}：国家 ● %{dns}：州/省份 ● %{dnl}：城市 ● 变量编码方式：对改写变量的编码方式，包括原文、URL和Base64。原文即不对改写变量进行编码；URL编码方式只会对改写变量中的特殊字符进行编码，需要编码的特殊字符为：;、/、?、:、@、&、=、+、$、|、{、}、,、\、^、[、]、`、<、>、#、%、"、空格；Base64编码方式会对整个改写变量进行编码 2） 单击<确定>按钮 仅 HTTP 类型的动作支持本参数
SSL 属性-SSL 客户端策略	可选择已创建的 SSL 客户端策略，也可以新创建 SSL 客户端策略 仅 HTTP 类型的动作支持本参数
SSL 属性- SSL URL 重定向列表	1） 单击<新建>按钮，新建 SSL URL 重定向 ● URL：Location首部URL的正则表达式 ● HTTP端口：原HTTP端口号 ● SSL端口：重写后的SSL端口号 2） 单击<确定>按钮 仅 HTTP 类型的动作支持本参数
应答 Location 改写列表	1） 单击<新建>按钮，新建应答 Location ● 改写前的正则表达式：待改写的应答报文Location首部的内容，为正则表达式，区分大小写 ● 改写后的内容：改写后的Location首部内容，区分大小写

参数	说明
	2) 单击<确定>按钮 应答 Location 改写会在 SSL URL 重定向改写之后执行，匹配 SSL URL 改写后的结果再进行应答 Location 首部内容的改写 仅 HTTP 类型的动作支持本参数
SSL 客户端策略	引用 SSL 客户端策略，可以对设备（作为 SSL 客户端）转发到 SSL 服务器的匹配流量进行加密 可选择已创建的 SSL 客户端策略，也可以新创建 SSL 客户端策略 仅 Diameter 类型的动作支持本参数
TCP 类型参数模板（服务器侧）	引用 TCP 类型参数模板，用来对动作为转发到服务器组的流量，根据该参数模板进行相应的处理，服务器侧 TCP 类型的参数模板是对设备与服务器之间建立的 TCP 连接进行处理和优化 可选择已创建的 TCP 类型的参数模板，也可以新创建 TCP 类型的参数模板 仅 Diameter 类型的动作支持本参数
Diameter-Session 类型参数模板	引用 Diameter-Session 类型参数模板，用来对动作为转发到服务器组的流量根据该参数模板进行相应的处理 可选择已创建的 Diameter-Session 类型参数模板，也可以新创建 Diameter-Session 类型参数模板 仅 Diameter 类型的动作支持本参数

步骤4 单击<确定>按钮，新建的动作会在“动作”页面显示。

4.15.4.3.3 负载均衡策略配置步骤

步骤1 单击“策略 > 负载均衡 > 服务器负载均衡 > 高级策略 > 负载均衡策略”。

步骤2 在“负载均衡策略”页面单击<新建>按钮。

步骤3 新建负载均衡策略。

参数	说明
名称	负载均衡策略的名称，不区分大小写
类型	负载均衡策略的类型，包括： ◆ 通用：用于四层服务器负载均衡 ◆ HTTP：用于七层服务器负载均衡 ◆ RADIUS：用于七层服务器负载均衡 ◆ MySQL：用于七层服务器负载均衡 ◆ Diameter：用于七层服务器负载均衡
默认动作	通用类型的负载均衡策略只能用通用类型的动作作为其默认动作，HTTP 类型的

参数	说明
	负载均衡策略则无此限制 可选择已创建的动作，也可以新创建动作
规则	为匹配特定流量特征的报文指定其执行的动作 1） 单击<新建>按钮，新建规则 ● 流量特征：可选择已创建的流量特征，也可以新创建流量特征。 ● 动作：可选择已创建的动作，也可以新创建动作。 ● 位于XX之前：将新创建的规则移至指定的规则之前，设备将按照先后顺序依次匹配流量特征，并执行相应的动作。其中，XX为指定规则的流量特征名称 2） 单击<确定>按钮，新建的规则会在“规则”列表中显示
描述	负载均衡策略的描述信息

步骤4　单击<确定>按钮，新建的负载均衡策略会在“负载均衡策略”页面显示。

4.15.4.4　连接数限制策略（可选）

通过引用连接数限制策略，可以对设备上建立的连接数进行统计和限制，能够有效解决因某些用户在短时间内经过设备向内部网络发起大量连接，导致设备系统或服务器资源迅速消耗，其它用户无法正常使用网络资源的问题，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。一个连接数限制策略中可配置多条限制规则，每条限制规则中指定一个连接数限制的范围，属于该范围的用户可建立的连接数将受到该规则中指定参数的限制。当某类型的连接数达到上限时，设备将不接受该类型的新建连接请求，直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连接数下限后，才允许新建连接。对于未匹配限制规则的用户所建立的连接，设备不对其连接数进行限制。连接数限制策略支持根据ACL来限定用户范围，虚服务器引用连接数限制策略后，对匹配ACL规则的访问实服务器的连接数进行统计和限制。

4.15.4.4.1　配置步骤

步骤1　单击“策略 > 负载均衡 > 服务器负载均衡 > 高级策略 > 连接数限制策略”。

步骤2　在“连接数限制策略”页面单击<新建>按钮。

步骤3　新建连接数限制策略。

参数	说明
名称	连接数限制策略的名称，不区分大小写
限制规则	一个连接数限制策略中可配置多条限制规则，每条规则中根据 ACL 指定一个连接数限制的用户范围，对匹配 ACL 规则的访问实服务器的连接数进行统计和限制。当某类型的连接数达到上限时，设备将不接受该类型的新建连接请求，直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连接数下限后，才允许新建连接。对于未匹配连接数限制规则的用户所建立的连接，设备不对其连接数进行限制 1） 单击<新建>按钮，新建限制规则 ● 规则编号：连接数限制规则的编号 ● 类型：连接数限制规则的类型，包括IPv4 ACL和IPv6 ACL ● ACL：用于匹配用户范围的ACL。可选择已创建的ACL，也可以新创建ACL ● 限制依据：包括源地址、目的地址和服务。源地址是指按源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连接数范围的限制；目的地址是指按目的IP地址进行统计和限制，一个目的IP地址的连接数目将受到指定连接数范围的限制;服务是指按服务统计和限制,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连接数范围的限制 ● 连接数范围-上限：连接数上限。某范围或某种类型的连接数值超过此值时，用户将不能建立新的连接 ● 连接数范围-下限：连接数下限，不能大于上限的取值。连接数的统计值降到此值之下时，允许用户建立新的连接 2） 单击<确定>按钮，新建的限制规则会在“限制规则”中显示
描述	连接数限制策略的描述信息

步骤4　单击<确定>按钮，新建的连接数策略会在“连接数限制策略”页面显示。

4.15.4.5　防护策略（可选）

通过引用防护策略，可以对防护策略中指定的URL进行防护。在防护周期内，设备允许不超过防护阈值的HTTP请求报文通过。设备检测到HTTP请求超过防护阈值时，会触发执行相应的防护动作，从而保护负载均衡设备和内网服务器的安全。

4.15.4.5.1 配置步骤

步骤1 单击“策略 > 负载均衡 > 服务器负载均衡 > 高级策略 > 防护策略”。

步骤2 在“防护策略”页面单击<新建>按钮。

步骤3 新建防护策略。

参数	说明
名称	防护策略的名称，不区分大小写
类型	防护策略的类型 目前仅支持 HTTP 类型的防护策略
防护动作	可以在 HTTP 类型的防护策略中配置防护规则，为来自同一用户超过阈值限制的访问指定 URL 的报文执行相应的防护动作，包括： ◆ 告警：输出告警日志，生成的告警信息并发送到信息中心 ◆ 丢弃：丢弃请求报文 ◆ 客户端验证：设备检测到请求报文个数达到阈值限制时，向客户端返回携带指定Cookie的响应报文。若客户端后续请求报文中携带的Cookie值与设备返回的Cookie值相同，则认为客户端请求报文通过验证。若请求报文中未携带Cookie值或携带的Cookie值与设备返回值不同，则认为客户端请求报文未通过验证，直接丢弃报文。设备支持通过插入HTTP头部和注入JS脚本的方式向客户端返回Cookie值
防护规则	一个防护策略中可配置多条防护规则，每条规则中指定一个防护 URL。在统计时间内，若同一用户访问指定 URL 的次数超过配置的阈值，则执行防护动作。设备支持基于源 IP 地址或者 Cookie 来判断请求报文是否来自同一用户 1） 单击<新建>按钮，新建防护规则 ● 规则编号：防护规则的编号 ● 防护URL：需要限制用户请求次数的URL，区分大小写，不支持正则元字符？ ● 统计时间：在统计时间内，若同一用户访问指定URL的次数超过配置的阈值，则执行防护动作 ● 基于源IP的请求阈值：设备将来自相同源IP地址的请求报文判断为来自同一用户 ● Cookie名称:HTTP报文的Cookie名称,区分大小写。不包括(、)、<、>、@、,、;、:、\、"、/、[、]、?、=、{、}、SP（空格符）、HT（水平制表符），以及ASCII码中小于等于31、大于等于127的字符 ● 基于Cookie的请求阈值：若请求报文中对应于指定Cookie名称的Cookie值相

参数	说明
	同，则认为请求报文来自同一用户 2） 若同时配置基于源 IP 的防护阈值和基于 Cookie 的防护阈值，则当携带相同 Cookie 值或者相同源 IP 的报文达到配置的阈值时，执行相应的动作 3） 单击<确定>按钮，新建的防护规则会在“防护规则”中显示
描述	防护策略的描述信息

步骤4　单击<确定>按钮，新建的防护策略会在“防护策略”页面显示。

4.15.4.6　参数模板（可选）

通过配置参数模板可以进行一些高级参数的配置。这样，当参数模板被虚服务器引用之后，可以对虚服务器的业务流量进行更深入的解析、处理和优化。

4.15.4.6.1　配置步骤

步骤1　单击“策略 > 负载均衡 > 服务器负载均衡 > 参数模板”。

步骤2　在“参数模板”页面单击<新建>按钮。

步骤3　新建参数模板。

参数	说明
参数模板名称	参数模板的名称，不区分大小写
类型	参数模板的类型，包括： ◆ IP：应用于四层服务器负载均衡 ◆ TCP：应用于七层服务器负载均衡 ◆ HTTP：应用于七层服务器负载均衡 ◆ HTTP-Compression：应用于七层服务器负载均衡 ◆ HTTP-Statistics：应用于七层服务器负载均衡 ◆ OneConnect：应用于七层服务器负载均衡 ◆ TCP-Application：应用于七层服务器负载均衡 ◆ MySQL：应用于七层服务器负载均衡 ◆ Diameter-Session：应用于七层服务器负载均衡 ◆ HTTP2.0：应用于七层服务器负载均衡
描述	参数模板的描述信息

参数	说明
发往客户端的 ToS	发往客户端的 IP 报文中的 ToS 字段

参数	说明
Option 操作列表	在负载均衡设备发送给服务器的 TCP 报文头中插入或删除 TCP 选项 1) 单击<新建>按钮，新建 Option 操作 ● Option操作类型 ● 插入：在负载均衡设备发送给服务器的TCP报文头的指定选项中插入内容 ● 删除：清除负载均衡设备发送给服务器的TCP报文头中的指定选项 ● Option编号：在负载均衡设备发送给服务器的TCP报文头中插入或删除的TCP选项编号 ● 编码类型 ● 二进制编码：TCP Option的编码方式为二进制编码 ● 字符串编码：TCP Option的编码方式为字符串编码 ● 插入内容：在TCP Option中插入指定内容，支持输入以下改写变量：%{is}（客户端侧的源IP地址）、%{isl}（源IP地址长度）、%{ps}（源端口号）以及%{psl}（源端口号长度） 2) 单击<确定>按钮，新建的 Option 操作会在“Option 操作列表”中显示
只插入数据报文	开启/关闭只插入数据报文功能。开启本功能后，TCP 选项插入模式为只插入数据报文；关闭后，TCP 选项插入模式为插入数据报文和握手阶段报文 当 TCP 参数模板被 IP、UDP 以及工作在四层的 TCP 类型虚服务器引用时，本功能不生效
时间戳选项	配置 TCP 报文头中的时间戳选项的动作，包括： ◆ 保持：*保持*负载均衡设备发送给服务器的TCP报文头中的时间戳选项的值不变 ◆ 删除：清除负载均衡设备发送给服务器的TCP报文头中的时间戳选项 ◆ 重写：修改负载均衡设备发送给服务器的TCP报文头中的时间戳选项的值为设备当前时间戳值 ◆ 使用全局配置：使用全局配置的TCP时间戳选项的动作，点击<全局配置>可直接跳转到“对象 > 负载均衡 > 高级设置”页面，查看全局时间戳选项的配置
本地最大窗口值	TCP 连接中的本地最大窗口值
超出 MSS 的报文处	允许超出 MSS 的报文通过或丢弃超出 MSS 的报文

参数	说明
理方式	◆ 允许：对客户端发来的HTTP请求报文中超出MSS的数据段的处理方式为允许超出MSS的数据段通过 ◆ 丢弃：对客户端发来的HTTP请求报文中超出MSS的数据段的处理方式为丢弃超出MSS的数据段
空闲超时时间	若在 TCP 连接的空闲超时时间内没有应用数据传输，负载均衡设备会主动断开与客户端或服务器的 TCP 连接
TCP MSS	设备与对端建立 TCP 连接时的 MSS 值
TIME-WAIT 超时时间	TCP 连接断开时，由于 TCP 协议的 TIME-WAIT 状态超时时间较长，导致 TCP 连接释放过慢，影响负载均衡业务处理效率。通过本配置可灵活设置 TIME-WAIT 状态超时时间 仅当 TCP 参数模板被 HTTP 或 HTTPS 类型的虚服务器引用时，本配置才生效
SYN 超时时间	TCP 连接 SYN 报文的超时时间。如果超过这个时间，仍然没有收到 SYN-ACK 报文，则关闭 TCP 连接 仅当 TCP 参数模板被 HTTP 或 HTTPS 类型的虚服务器引用时，本配置才生效
保活空闲时间	TCP 连接在一段时间没有数据传输后，会发送 TCP 保活报文，保活空闲时间用来约定多久发送一次 TCP 保活报文 仅当 TCP 参数模板被 HTTP 或 HTTPS 类型的虚服务器引用时，本配置才生效
保活重传间隔	TCP 保活报文的重传时间间隔 仅当 TCP 参数模板被 HTTP 或 HTTPS 类型的虚服务器引用时，本配置才生效
保活重传次数	TCP 保活报文的重传次数 仅当 TCP 参数模板被 HTTP 或 HTTPS 类型的虚服务器引用时，本配置才生效
FIN-WAIT-1 超时时间	TCP 连接 FIN-WAIT1 状态的超时时间 仅当 TCP 参数模板被 HTTP 或 HTTPS 类型的虚服务器引用时，本配置才生效
FIN-WAIT-2 超时时间	TCP 连接 FIN-WAIT2 状态的超时时间 仅当 TCP 参数模板被 HTTP 或 HTTPS 类型的虚服务器引用时，本配置才生效
触发 SYN Cookie 半开连接阈值	触发 SYN Cookie 保护功能的半开连接数阈值 半开连接，即客户端与虚服务器建立 TCP 连接过程中，虚服务器在收到 TCP 连接请求 SYN 报文之后到收到 ACK 报文之前，连接尚未建立的状态 仅当 TCP 参数模板被 TCP 类型的虚服务器引用，且虚服务器配置了工作在四层模式时，本配置才生效
源地址转换的 Option 编号	指定进行源地址转换的 TCP Option 编号。设备可以解析收到的报文中指定编号的 TCP Option 字段携带的 IP 地址，并配合 TCP Option 类型的源地址转换方式将解析处理后的地址进行源地址转换
编码方式	TCP Option 的编码方式，包括：

参数	说明
	◆ 二进制编码：TCP Option的编码方式为二进制编码 ◆ 字符串编码：TCP Option的编码方式为字符串编码

参数	说明
Header 最大解析长度	HTTP 首部的最大解析长度
Content 最大解析长度	HTTP 实体的最大解析长度
Secondary Cookie 分隔符	URL 中分隔 Secondary Cookie 的字符，包括：!、"、#、;、<、>、?、[、\、]、^、`、|、:、@、&、$、+、*、'、(、)、,、/。该字符串中的每个字符都被认为是分隔字符
Secondary Cookie 起始字符	URL 中 Secondary Cookie 的起始位置标示字符，包括：!、"、#、;、<、>、?、[、\、]、^、`、|
Cookie name	Cookie 名称，对指定名称的 Cookie 进行加密，区分大小写
Cookie 加密密钥	Cookie 加密密钥，包括： ◆ 明文密钥：以明文的方式对Cookie进行加密 ◆ 密文密钥：以密文的方式对Cookie进行加密
明文密钥/密文密钥	密钥字符串，区分大小写
首部超出最大长度的报文处理方式	◆ 允许：对客户端发来的HTTP请求报文的首部超出最大长度的处理方式为继续执行负载均衡操作 ◆ 丢弃：对客户端发来的HTTP请求报文的首部超出最大长度的处理方式为丢弃首部超出最大长度的报文 当 HTTP 报文首部的长度超过负载均衡的处理能力时，系统将无条件丢弃该报文
逐请求负载均衡	开启/关闭逐请求负载均衡功能。开启状态下，设备对每个 HTTP 请求报文都进行负载均衡
连接复用	开启/关闭连接复用功能。开启状态下，允许负载均衡设备与服务器的连接复用，即允许负载均衡设备与服务器建立长连接，使多个客户端复用同一条与服务器的连接，以减少客户端与服务器之间打开的连接数
忽略大小写	开启/关闭忽略大小写功能，即匹配字符串时是否对大小写不敏感。本配置将影响以下内容： ◆ 对于类匹配，影响HTTP首部的取值、HTTP Cookie的名称和取值、URL ◆ 对于HTTP首部持续性方法，影响首部的取值、URL以及用于生成持续性表项的Key值 ◆ 对于Cookie截取持续性方法，影响Cookie的名称和取值的匹

参数	说明
	配以及用于生成持续性表项的Key值
每请求执行动作	开启/关闭每请求执行动作功能。开启状态下，设备对每个 HTTP 请求报文都执行相应的负载均衡动作

参数	说明
级别	应答报文的压缩级别，数值越大表示压缩速度越慢、压缩比越高
首选方法	应答报文首选的压缩算法。如果客户端的请求支持配置的压缩算法，则用配置的算法进行压缩，否则采用请求中携带的算法 ◆ gzip：gzip压缩算法 ◆ deflate：deflate 压缩算法
最小 Content-Length	进行压缩的应答报文体的最小长度，0 代表不限制 如果应答报文中携带 Content-Length 首部，则报文体的长度必须达到配置的最小长度才会进行压缩，否则不进行压缩。如果应答报文中不携带 Content-Length 首部，此配置不生效，即无论报文多大都会进行压缩
插入 Vary Header	开启/关闭在应答报文中插入 Vary 首部的功能 开启该功能后，无论应答本身是否携带 Vary 首部或应答是否进行压缩处理，都会在应答头插入 Vary 首部，内容为 Accept-Encoding 再发往客户侧
所有 HTTP 版本	开启/关闭对 HTTP1.0 的请求报文的应答进行压缩处理
删除 Accept-encoding	开启/关闭删除 HTTP 请求中的 Accept-Encoding 首部的功能 当客户端发送的请求报文中携带 Accept-Encoding 首部，并开启该功能后，由负载均衡设备发往服务器的报文会删除 Accpet-Encoding 首部。由服务器发往负载均衡设备的应答报文不会进行压缩，而由负载均衡设备发往客户端的应答报文在符合匹配规则的情况下进行了压缩。如果客户端发送的请求报文不携带 Accept-Encoding 首部，无论是否开启该功能，负载均衡设备都不会对应答报文进行压缩
内存大小	应答报文压缩所占用的内存大小，取值仅能为 1、2、4、8、16、32、64 中的某一个值
窗口大小	压缩使用的窗口大小，取值仅能为 1、2、4、8、16、32 中的某一个值
压缩的过滤条件	1） 单击<新建>按钮，新建过滤条件 ● Rule ID：过滤规则的编号 ● 动作：包括允许和拒绝。允许表示对符合匹配规则的报文进行压缩；

参数	说明
	拒绝表示对符合匹配规则的报文不进行压缩 ● 类型：包括URL和Content-Type。URL表示匹配范围限于报文携带的URL；Content-Type表示匹配范围限于Content-Type首部中携带的报文体类型 ● URL：匹配的内容为HTTP报文中携带的URL，正则表达式，不支持正则元字符?，区分大小写。只有过滤条件的类型选择“URL”时，才会出现该参数 ● Content-Type：匹配的内容为Content-Type首部中携带的HTTP报文体类型，正则表达式，不支持正则元字符?，区分大小写。只有过滤条件的类型选择“Content-Type”时，才会出现该参数 2） 单击<确定>按钮，新建的过滤条件会在“压缩的过滤条件”中显示

参数	说明
地址对象组	若 HTTP 流量匹配了指定 URL，并且 HTTP 流量的源 IP 地址匹配了指定地址对象组，则将地址对象组记录在统计数据库中，否则将源 IP 地址记录在统计数据库中 一个 HTTP 统计类型的参数模板中最多允许指定 1024 个地址对象组
HTTP 统计节点列表	1） 单击<新建>按钮，新建统计节点 ● 节点名称：统计节点名称，不区分大小写，一个HTTP统计类型的参数模板最多允许配置256个统计节点 ● 描述：统计节点描述信息，区分大小写 ● 统计规则列表：URL统计规则的集合，一个统计节点中最多允许配置256条统计匹规则 ● ID：统计规则的编号 ● URL：URL的正则表达式，不支持正则元字符? 2） 单击<确定>按钮，新建统计节点会在“统计节点列表”中显示

参数	说明
最大复用数目	设备与服务器之间 TCP 连接的最大复用数目是指一个 TCP 连接最多可被复用多少次，即最多允许多少个客户端复用同一条与服务器的连接。当设备与服务器之间 TCP 连接的复用数目达到最大复用数目时，此 TCP 连接将会被删除，后续客户端发起的连接请求将触发建立新的 TCP 连接
空闲超时时间	当设备与服务器之间 TCP 连接的空闲时间达到空闲超时时间时，设备与服务器之间建立的 TCP 连接将会被删除，后续客户端发起的连接请求将触发建立新的 TCP 连接
IPv4 掩码长度	通过配置本参数，可以使属于相同 IPv4 网段的客户端请求复用同一 TCP 连接。设备收到客户端连接请求时，若客户端网段与已建立的 TCP 空闲连接的客户端网段相同，则复用已建立的空闲连接。否则，触发建立新的 TCP 连接
IPv6 前缀长度	通过配置本参数，可以使属于相同 IPv6 网段的客户端请求复用同一 TCP 连接。设备收到客户端连接请求时，若客户端网段与已建立的 TCP 空闲连接的客户端网段相同，则复用已建立的空闲连接。否则，触发建立新的 TCP 连接

参数	说明
TCP 流缓冲时间	TCP 流的缓冲时间。设备缓冲客户端发给虚服务器 TCP 流量的时长。缓冲的 TCP 流量用于进行 CP 载荷匹配
TCP 流缓冲大小	TCP 流的缓冲大小。当设备收到的 TCP 载荷达到配置的缓冲数据大小时，则停止对该 TCP 流量的缓冲
TCP 流缓冲结束符	TCP 流的缓冲结束符。当设备收到的 TCP 载荷匹配配置的缓冲结束符时，则停止对该 TCP 流量的缓冲

参数	说明
连接池大小	当 MySQL 数据传输完成后，不立即断开 TCP 连接，而是将 TCP 连接保存在 MySQL 连接池中。当需要建立新的连接时，优先从 MySQL 连接池中获取可用连接，而不是重新建立一个新连接 MySQL 连接池的大小用来限制 MySQL 连接池可存储的 TCP 连接的个数
连接复用	开启/关闭连接复用功能 通过开启负载均衡设备与服务器的连接复用功能，在负载均衡设备与服务器之间建立连接，使多个客户端复用同一条与服务器的连接，以减少客户端与服务器之间打开的连接数
最大复用数目	设备与服务器之间 TCP 连接的最大复用数目是指一个 TCP 连接最多可被复用

参数	说明
	多少次，即最多允许多少个客户端复用同一条与服务器的连接。当设备与服务器之间 TCP 连接的复用数目达到最大复用数目时，此 TCP 连接将会被删除，后续客户端发起的连接请求将触发建立新的 TCP 连接
空闲超时时间	当设备与服务器之间 TCP 连接的空闲时间达到空闲超时时间时，设备与服务器之间建立的 TCP 连接将会被删除，后续客户端发起的连接请求将触发建立新的 TCP 连接
IPv4 掩码长度	通过配置本参数，可以使属于相同 IPv4 网段的客户端请求复用同一 TCP 连接。设备收到客户端连接请求时，若客户端网段与已建立的 TCP 空闲连接的客户端网段相同，则复用已建立的空闲连接。否则，触发建立新的 TCP 连接
IPv6 前缀长度	通过配置本参数，可以使属于相同 IPv6 网段的客户端请求复用同一 TCP 连接。设备收到客户端连接请求时，若客户端网段与已建立的 TCP 空闲连接的客户端网段相同，则复用已建立的空闲连接。否则，触发建立新的 TCP 连接

参数	说明
协商超时时间	当设备与客户端或服务器端建立 TCP 连接后，首先会通过 CER 和 CEA 协商报文进行信息交换。配置 Diameter 协商超时时间，在超时时间到期时，设备和对端一直没有 CER 和 CEA 协商报文交互，设备将认为该 TCP 连接已失效，并直接断开该连接，从而避免系统资源被持续占用而造成的浪费 Diameter-Session 类型参数模板仅对 Diameter 协议类型的请求报文有效
源主机名	通过配置 Diameter-Session 类型参数模板，管理员可以自由指定设备 Diameter 协商时发送给对端的的参数信息。指定设备的源主机名称，当设备与对端进行 Diameter 协商时，设备将配置的源主机名作为本端设备主机名发送给对端 源主机名应为 FQDN（Fully Qualified Domain Name，完全合格域名）形式，即为同时带有主机名和源域名的名称
源域名	指定设备的源域名，当设备与对端进行 Diameter 协商时，设备将配置的域名作为本机域名发送给对端
厂商 ID	指定设备的厂商 ID，当设备与对端进行 Diameter 协商时，设备将配置的厂商 ID 发送给对端
产品名称	指定设备的产品名称，当设备与对端进行 Diameter 协商时，设备将配置的名称作为本机名称发送给对端
本机地址	指定本机 IP 地址，当设备与对端进行 Diameter 协商时，设备将配置的 IP 地

参数	说明
	址作为本机地址通过协商报文发送给对端 本机 IP 地址必须为设备接口上已配置的地址且接口处于可用状态
重传功能	开启/关闭 Diameter 数据报文重传功能 Diameter 协商后，当设备向服务器发送 Diameter 数据报文一段时间，仍没有得到服务器的响应，则有必要开启 Diameter 数据报文重传功能，在重传超时时间到期后重新发送数据报文，以保证用户尽可能地获得相应的服务
重传超时时间	Diameter 数据报文重传超时时间 开启 Diameter 数据报文重传功能后，设备向实服务器发送数据报文，如果在重传超时时间内没有收到实服务器应答，则选择同一实服务组内另一台实服务器重新发送该数据报文，并重新开始计时，若在重传超时时间到期时依旧没有收到应答，则认为 Diameter 数据发送失败，通知客户端不可达 设备仅支持对数据报文重传一次

参数	说明
最大并发请求数	允许一条 TCP 连接的最大并发请求报文数
最大接收窗口值	本地允许 HTTP2.0 协议报文的最大接收窗口值
插入头部字段	开启/关闭向 HTTP2.0 协议版本的请求报文头部中插入字段
头部字段名称	插入 HTTP2.0 报文头部字段的名称
空闲连接时间	非活动状态保持 TCP 连接的时间
连接帧大小	允许 HTTP2.0 报文最大的连接帧值
表头规格	HTTP2.0 报文头部表的大小
主动关闭服务器连接	◆ 禁用：不主动关闭服务器连接 ◆ FIN关闭：通过发送FIN报文关闭服务器连接 ◆ RST关闭：通过发送RST报文关闭服务器连接 本功能只针对客户端发起 HTTP2.0 协议版本的请求报文，而设备与实服务器仅支持 HTTP1.1 协议的情况下生效

步骤4　单击<确定>按钮，新建的参数模板会在“参数模板”页面显示。

4.15.4.7　智能探测模板（可选）

通过配置HTTP passive类型、RST类型、零窗口类型或自定义类型的智能探测模板，当模板在实服务

组成员中被引用时，可以对当前实服务组成员进行监控；当模板在实服务组中被引用时，可以对实服务组内所有实服务组成员进行监控。

探测模板类型的支持情况与设备型号有关，请以页面的实际显示为准。

4.15.4.7.1 配置步骤

步骤1 单击“策略 > 负载均衡 > 服务器负载均衡 > 智能探测模板”。

步骤2 在“智能探测模板”页面单击<新建>按钮。

步骤3 新建智能探测模板。

参数	说明
探测模板名称	智能探测模板的名称，不区分大小写
类型	智能探测模板的类型，包括： ◆ RST：探测实服务器发送的RST报文的个数 ◆ 零窗口：探测实服务器发送的零窗口报文的个数 ◆ HTTP passive：探测HTTP响应报文中的异常URL次数 ◆ 自定义：通过调用用户配置的监控脚本文件，完成对实服务器状态的监控 ◆ AntDB数据库类型：探测AntDB数据库的可用性 ◆ MySQL数据库类型：探测MySQL数据库的可用性 ◆ Oracle数据库类型：探测Oracle数据库的可用性
描述	智能探测模板的描述信息

参数	说明
统计时间	当 RST 类型或零窗口类型的智能探测模板被引用后，在统计时间内，系统会对实服务组中每个实服务器成员发送的 RST 报文和零窗口报文的个数进行统计
阈值	若统计时间内实服务器发送的 RST 报文或零窗口报文达到配置的上限阈值，则执行相应的动作
动作	智能探测模板的动作，包括： ◆ 强制下线：若配置智能**探测模板的**动作为强制下线，则当实服务器发送的RST报文或零窗口报文达到**配置的阈值时，**系统会自动关闭实服务器 ◆ 过载保护：若配置智能**探测模板的**动作为过载保护，则当实服务器发送的RST报文或零窗口报文达到**配置的阈值时，系统会**将实服务器的状态标记为繁忙，然后以繁忙保护时间为周期再次对实服务器进行检查。若实服务器在繁忙保护时间内发送的RST报文或零窗口报文未达到**配置的阈值，则实服务器恢复正常状态。否则继续以**繁忙保护时间为周期检查实服务器，直到达到实服务器的繁忙保护次数为止。达到繁忙保护次数后，系统会自动关闭实服务器

参数	说明
	在因为达到阈值或达到繁忙保护次数导致实服务器关闭的情况下，若删除实服务组引用负载均衡探测模板，则实服务组的状态会立即恢复为正常
繁忙保护时间	实服务器因过载保护动作进入繁忙状态后，再次进行智能探测的时间间隔
繁忙保护次数	实服务器因过载保护动作进入繁忙状态后，可以继续进行智能探测的次数。0表示实服务器的智能繁忙保护次数不受限制

参数	说明
统计时间	当 HTTP passive 类型的智能探测模板被引用后，若设备收到携带指定 URL 的 HTTP 请求报文，则会对其响应报文进行 HTTP 智能监控。在统计时间内，设备会对 URL 异常的次数进行统计
阈值	对于 HTTP passive 类型的智能探测模板，若统计时间内检测到异常 URL 的次数超过配置的上限阈值，则自动关闭实服务器
超时时间	当设备收到携带指定 URL 的 HTTP 请求报文后，会对其响应报文进行 HTTP 智能监控。若 HTTP 报文的响应时间超过配置的超时时间，则认为检测到一次异常 URL
检查 URL	若实服务器收到的 HTTP 请求报文中携带本配置指定的 URL，则对其响应报文进行 HTTP 智能监控 **检查 URL** 不支持配置正则元字符？ 同一 HTTP passive 类型的智能探测模板下最多允许配置 10 个 URL
响应状态码	当设备收到携带指定 URL 的 HTTP 请求报文后，会对其响应报文进行 HTTP 智能监控。若 HTTP 响应报文中携带的状态码为配置的值，则认为检测到一次异常 URL 同一 HTTP passive 类型的智能探测模板下最多允许配置 10 个响应状态码

参数	说明
监控周期	当自定义类型的智能探测模板被引用后，系统会在每个监控周期到来时执行一次监控脚本文件
超时时间	应答超时时间 建议配置探测报文的应答超时时间小于监控周期
脚本文件参数	在执行监控脚本文件时，设备进程会将配置的脚本文件参数传递给脚本文件 设备允许同时输入多个参数，参数之间用空格分隔
脚本文件	通过在自定义类型的智能探测模板下配置监控脚本文件，可根据脚本文件定

参数	说明
	义的检测内容成对实服务器状态的检测 设备目前仅支持引用后缀名为.py 的脚本文件
环境变量	可以通过配置环境变量，指定监控脚本的执行环境

参数	说明
目的 IP 地址	目的数据库 IP 地址
目的端口号	目的数据库端口号
监控周期	以监控周期为时间间隔，向目的数据库发送探测报文，探测数据库服务是否可用
应答超时时间	数据库应答超时时间 建议配置探测报文的应答超时时间小于监控周期
数据库连接字符串	数据库的连接字符串，支持输入数据库名称、数据库 ID 和以下改写变量： ◆ %{ip}：表示探测的目的IP地址 ◆ %{port}：表示探测的目的端口号 仅 Oracle 数据库类型的探测模板支持本参数
数据库名称	指定探测的数据库名称 MySQL 和 AntDB 数据库类型的探测模板支持本参数
用户名	登录数据库的用户名
密码	登录数据库的密码
执行语句	登录数据库后，执行的数据库查询语句
期望执行结果	执行数据库查询语句后，期望执行结果中包含的内容
期望执行结果所在列号	期望数据库返回的执行结果所在列号
期望执行结果所在行号	期望数据库返回的执行结果所在行号
连接复用	与数据库的连接复用次数，可设置不复用或最大连接复用次数
描述	数据库类型探测模板的描述信息

步骤4　单击<确定>按钮，新建的智能探测模板会在“智能探测模板”页面显示。

4.15.4.8　虚服务器

虚服务器是负载均衡设备上面向用户业务的虚拟载体，是为了判断是否需要对进入负载均衡设备的报文进行负载均衡而引入的概念。只有匹配上虚服务器的报文才会被进行负载均衡处理。

服务器负载均衡支持的虚服务器类型为IP、TCP、UDP、SIP-TCP、SIP-UDP、HTTP、Performance(HTTP)、HTTPS、HTTP重定向、RADIUS、MySQL和Diameter类型。需要注意的是，请避免配置VSIP和端口号都相同的UDP类型和SIP-UDP类型的虚服务器；请避免配置VSIP和端口号都相同的TCP、SIP-TCP、HTTP、Performance(HTTP)、HTTPS、HTTP重定向、RADIUS、MySQL和Diameter类型的虚服务器；请避免将Performance(HTTP)类型的虚服务器需避免和TCP客户端验证功能（该功能的介绍请参见“攻击防范联机帮助”）同时使用。否则导致无法预知负载均衡设备处理报文的方法。

4.15.4.8.1 配置步骤

步骤1 单击“策略 > 负载均衡 > 服务器负载均衡 > 虚服务器”。

步骤2 在“虚服务器”页面单击<新建>按钮。

步骤3 新建虚服务器。

参数	说明
虚服务器名称	虚服务器的名称，不区分大小写
类型	虚服务器的类型，包括 IP、TCP、UDP、SIP-TCP、SIP-UDP、HTTP、Performance(HTTP)、HTTPS、HTTP 重定向、RADIUS、MySQL 和 Diameter 类型
虚服务器 IPv4 地址	虚服务器的 IPv4 地址/掩码长度 0～32
虚服务器 IPv6 地址	虚服务器的 IPv6 地址/前缀长度 0～128
虚服务器端口号	虚服务器的端口号。0 表示任意端口号 对于 IP/TCP/UDP/RADIUS 类型的虚服务器，可输入多个端口号，以英文逗号分隔，如：5,10,20-28。最多支持输入 32 段不连续的端口号
UDP 强制负载均衡	开启/关闭 UDP 强制负载均衡功能。当 UDP 强制负载均衡功能关闭时，匹配虚服务器的流量按照数据流来进行负载均衡，即一个应用的流量会被负载均衡到同一个实服务器上；而当 UDP 强制负载均衡功能开启后，匹配虚服务器的流量不再按照流来进行负载均衡，而是按照每报文来进行负载均衡 仅 UDP、SIP-UDP 和 RADIUS 类型的虚服务器支持本参数
SSL 服务器端策略	虚服务器引用的 SSL 服务器端策略，可以对负载均衡设备（作为 SSL 服务器）与 SSL 客户端之间传输的流量进行加密传输 可选择已创建的 SSL 服务器端策略，也可以新创建 SSL 服务器端策略。 仅 TCP、HTTPS 和 Diameter 类型的虚服务器支持本参数
重定向 URL	在 HTTP 重定向类型的虚服务器中配置了重定向 URL 后，所有匹配该虚服务器的 HTTP 请求报文都将被重定向到指定 URL

参数	说明
	重定向 URL 区分大小写，也可以使用？和以下特定含义的字符串： ◆ %h：表示客户端请求报文中的主机名 ◆ %p：表示客户端请求报文中的URL ◆ %%：表示字符% 仅 HTTP 重定向类型的虚服务器支持本参数
重定向方式	◆ 临时重定向-302 ◆ 临时重定向-307 ◆ 永久重定向-301 仅 HTTP 重定向类型的虚服务器支持本参数
实服务组	虚服务器缺省引用的主用实服务组，可选择已创建的实服务组，也可以新创建实服务组 HTTP 重定向和 Diameter 类型的虚服务器不支持本参数
实服务组的持续性组	实服务组所对应的主用持续性组，可选择已创建的持续性组，也可以新创建持续性组 HTTP 重定向和 Diameter 类型的虚服务器不支持本参数
VRRP 备份组关联接口	VRRP 备份组关联的接口 配置了本参数后，必须指定虚服务器绑定的 VRRP 备份组号
VRRP 备份组号	虚服务器绑定的 VRRP 备份组号 在双主模式的双机热备组网中，两台设备同时处理业务且互为主备。在未配置虚服务器下绑定的 VRRP 备份组时，两台设备同时处理业务。业务对应的源地址池在两台设备上进行拆分。在配置了虚服务器下绑定的 VRRP 备份组时，业务仅在指定备份组的主节点上进行处理。此时，业务对应的源地址池只在主节点上进行分配。有关双机热备的详细介绍，请参见“双机热备”联机帮助 在配置了 VRRP 备份组关联接口后，才允许配置本参数
VRRP IPv6 备份组关联接口	VRRP IPv6 备份组关联的接口 配置了本参数后，必须指定虚服务器绑定的 VRRP IPv6 备份组号
VRRP IPv6 备份组号	虚服务器绑定的 VRRP IPv6 备份组号 在双主模式的双机热备组网中，两台设备同时处理业务且互为主备。在未配置虚服务器下绑定的 VRRP IPv6 备份组时，两台设备同时处理业务。业务对应的源地址池在两台设备上进行拆分。在配置了虚服务器下绑定的 VRRP IPv6 备份组时，业务仅在指定备份组的主节点上进行处理。此时，业务对应的源地址池只在主节点上进行分配 VRRP IPv6 备份组仅对 IPv6 类型的虚服务器地址生效 在配置了 VRRP IPv6 备份组关联接口后，才允许配置本参数
MySQL 数据库	负载均衡设备代替 MySQL 服务器对客户端进行认证的数据库版本。若通过本配

参数	说明
版本	置指定了 MySQL 数据库的版本，则设备会向客户端发送该版本的数据库初始化报文 仅 MySQL 类型的虚服务器支持本参数
读写分离	开启 MySQL 虚服务器的读写分离功能后，读 SQL 命令和写 SQL 命令将分别由读实服务组和写实服务组执行，一定程度上缓解读写并发时对数据库性能的影响 开启了读写分离功能后，必须同时配置读实服务组和写实服务组 仅 MySQL 类型的虚服务器支持本参数
读实服务组	虚服务器引用的读实服务组。可选择已创建的实服务组，也可以新创建实服务组。 仅在开启读写分离功能后，支持配置本参数
读持续性组	虚服务器引用的读持续性组，可选择已创建的持续性组，也可以新创建持续性组。 仅在开启读写分离功能后，支持配置本参数 配置读持续性组时，必须配置读实服务组
写实服务组	虚服务器引用的写实服务组。可选择已创建的实服务组，也可以新创建实服务组。 仅在开启读写分离功能后，支持配置本参数
写持续性组	虚服务器引用的写持续性组，可选择已创建的持续性组，也可以新创建持续性组。 仅在开启读写分离功能后，支持配置本参数 配置写持续性组时，必须配置写实服务组
发送免费 ARP 或 ND 报文的接口	设备发送免费 ARP 报文或 ND 报文的接口 若配置虚服务器的 IP 地址与客户端连接设备的入接口地址同网段，需要将本参数配置为设备连接客户端的接口，并同时开启响应 ARP 功能
负载分担模式	◆ 四层：配置TCP类型的虚服务器工作在四层 ◆ 七层：配置TCP类型的虚服务器工作在七层 仅 TCP 类型的虚服务器支持本参数 如果 TCP 类型的虚服务器配置了工作在七层模式，则必须为虚服务器配置非 0 端口号，否则该模式不生效
启用代理协议	启用 TCP 类型虚服务器的代理协议功能后，设备可将真实的源 IP 地址信息透传到后端实服务器 启用版本 1 或版本 2 代理协议之前，请确保后端实服务器支持指定版本的代理协议，否则将导致设备与实服务器之间的新建连接失败

参数	说明
	仅工作在七层的 TCP 类型虚服务器，支持配置本参数
响应 ARP	开启/关闭响应 ARP 功能。开启响应 ARP 功能后，设备会将虚服务器的 IP 地址发布给 OSPF 模块参与路由计算，当数据中心进行切换的时候，保证访问虚服务器的流量也可以自动切换
冗余组引流策略	将匹配虚服务器的流量引流到指定备份组。若冗余组不存在或该冗余组下没有生效的备份组，则本功能不生效 本功能的支持情况与设备的型号有关，请以设备的实际显示为准
会话扩展信息备份	开启/关闭虚服务器的会话扩展信息备份功能 仅 IP、TCP、UDP、SIP-TCP、SIP-UDP 和 RADIUS 类型的虚服务器支持本功能
持续性表项备份	开启/关闭虚服务器的持续性表项备份功能 若设备的配置发生以下变化，则设备会删除当前已有的持续性表项，后续流量将会重新触发生成新的持续性表项 ◆ 关闭持续性表项备份功能 ◆ 持续性表项备份由组间备份切换为全局备份 ◆ 持续性表项备份由全局备份切换为组间备份 HTTP 重定向类型的虚服务器不支持本功能
持续性表项备份类型	持续性表项的备份类型，包括： ◆ 组间备份：表示仅在备份组内备份持续性表项 ◆ 全局备份：在多台负载均衡设备之间备份持续性表项，而非只在备份组内的两台设备间备份 只有持续性表项备份功能处于开启状态时，才支持配置本功能 HTTP 重定向类型的虚服务器不支持本功能 本功能的支持情况与设备的型号有关，请以设备的实际显示为准
虚服务功能	开启/关闭虚服务器。配置完虚服务器后，需要将其开启后才能进入工作状态
重置连接	开启/关闭重置连接。开启后，当虚服务器不可用，在收到客户端的 SYN 报文时会立即应答 RST 报文，并断开 TCP 连接 仅 TCP、SIP-TCP、HTTP、HTTPS 和 Performance(HTTP)类型的虚服务器支持本功能
快速日志输出内容	指定快速日志输出内容。当输入多个变量时，变量之间用分号分隔。设备支持配置以下变量： ◆ %{is}：客户端侧的源IP地址 ◆ %{ps}：客户端侧的源端口号 ◆ %{id}：客户端侧的目的IP地址 ◆ %{pd}：客户端侧的目的端口号 ◆ %{sis}：服务端侧的源IP地址 ◆ %{sps}：服务端侧的源端口号 ◆ %{sid}：服务端侧的目的IP地址

参数	说明
	◆ %{spd}：服务端侧的目的端口号 ◆ %{vsn}：虚服务器的名称 ◆ %{sfn}：实服务组的名称 ◆ %{reqtmstamp}：HTTP访问请求时间，采用GMT时间格式 ◆ %{reqtime}：HTTP访问请求时间，采用CST时区时间格式 ◆ %{uri}：HTTP URI ◆ %{ver}：HTTP协议的版本号 ◆ %{args}：HTTP访问参数 ◆ %{method}：HTTP请求方法 ◆ %{xff}：XFF（X-Forwarded-For）的IP地址 ◆ %{ctype}：HTTP请求报文Content-Type字段 ◆ %{clen}：HTTP请求报文的Content-Length字段 ◆ %{ref}：HTTP请求报文的Referer首部字段 ◆ %{ua}：HTTP请求报文的User-Agent字段 ◆ %{host}：HTTP请求报文Host首部字段 ◆ %{path}：HTTP请求报文的Path ◆ %{reqsz}：HTTP请求报文的大小，单位为字节 ◆ %{reqtm}：HTTP访问的请求时长，单位为毫秒，从设备收到客户端请求报文开始计时，收到服务器端响应报文计时结束 ◆ %{reqtm_s}：HTTP访问的请求时长，单位为秒，从设备收到客户端请求报文开始计时，收到服务器端响应报文计时结束 ◆ %{conntm_s}：HTTP访问的连接时长，单位为秒，从设备与客户端建立连接开始计时，发送完响应报文计时结束 ◆ %{repstatus}：HTTP应答报文状态码 ◆ %{rspclen}：HTTP响应报文Content-Length字段 ◆ %{rspsz}：HTTP响应报文的大小，单位为字节 ◆ %{rsptm}：HTTP访问响应时长，单位为毫秒，从设备收到服务器端响应报文开始计时，发送完响应报文计时结束 ◆ %{stscode}：HTTP响应状态码 ◆ %{reqbsz}：HTTP请求报文的Body大小，单位为字节 ◆ %{rspbsz}：HTTP响应报文的Body大小，单位为字节 ◆ %{rspsntbsz}：设备应答客户端的HTTP响应报文的Body大小，单位为字节 ◆ %{cookie_*cookie-name*}：HTTP访问的Cookie，*cookie-name*表示Cookie名称，如%{cookie_cookie1}。Cookie名称中不能包括(、)、<、>、@、,、;、:、\、"、/、[、]、?、=、{、}、SP（空格符）、HT（水平制表符），以及ASCII码中小于等于31、大于等于127的字符，区分大小写。设备允许配置多个不同名称的Cookie 仅 HTTP 和 HTTPS 类型的虚服务器支持本参数
描述	虚服务器的描述信息
用户列表	配置登录 MySQL 数据库时使用的用户名和密码 1） 单击<新建>按钮，新建用户 ● 用户名：登录MySQL数据库的用户 ● 密码：登录MySQL数据库的用户密码

参数	说明
	2) 单击<确定>按钮，新建的登录用户会在“用户列表”中显示 设备最多支持配置 100 个 MySQL 数据库的登录用户 仅 MySQL 类型的虚服务器支持本参数

参数	说明
插入 X-Forwarded-For	开启/关闭在 HTTP 报文头部 X-Forwarded-For 字段插入源 IP 地址功能 开启本功能后，当设备收到客户端的请求报文后，会在 HTTP 报文头部的 X-Forwarded-For 字段插入客户端的源 IP 地址 仅 HTTP、HTTPS 类型的虚服务器支持配置本参数
调度资源-备用实服务组	虚服务器引用的备用实服务组，当主用实服务组可用（该实服务组存在且有可用的实服务器）时，虚服务器通过主用实服务组进行转发；当主用实服务组不可用而备用实服务组可用时，虚服务器通过备用实服务组进行转发 可选择已创建的实服务组，也可以新创建实服务组 Diameter 类型的虚服务器不支持本参数
调度资源-实服务组的备用持续性组	实服务组所对应的备用持续性组的名称，不区分大小写 如果用户既配置了主用持续性组，也配置了备用持续性组，则会根据两个持续性组同时生成主用持续性表项和备用持续性表项。当有新的流量匹配已生成持续性表项时，如果未能匹配到主用持续性表项，则进行备用持续性表项匹配 仅 HTTP、HTTPS 和 RADIUS 类型的虚服务器支持配置本参数
调度资源-负载均衡策略	虚服务器引用负载均衡策略。根据策略中的规则，使命中虚服务器的报文根据不同的报文内容进行不同的负载均衡处理，从而有效地丰富了负载均衡的负载功能 可选择已创建的负载均衡策略，也可以新创建负载均衡策略。 虚服务器只能引用与自身类型相关的策略模板，如：Performance(HTTP)和 HTTP 类型的虚服务器，可以引用通用或 HTTP 类型的负载均衡策略；IP、TCP、UDP、SIP-TCP 和 SIP-UDP 类型的虚服务器，只能引用通用类型的负载均衡策略；RADIUS 类型的虚服务器，可以引用通用或 RADIUS 类型的负载均衡策略模板；Diameter 类型的虚服务器，只能引用 Diameter 类型的负载均衡策略模板 HTTP 重定向类型的虚服务器不支持本功能

参数	说明
调度资源-连接数限制策略	虚服务器引用连接数限制策略后，访问虚服务器的连接数将会受到连接数限制策略的限制 可选择已创建的连接数限制策略，也可以新创建连接数限制策略。 HTTP 重定向类型的虚服务器不支持本功能
调度资源-SSL 客户端策略	虚服务器引用的 SSL 客户端策略，可以对负载均衡设备（作为 SSL 客户端）与 SSL 服务器之间传输的流量进行加密传输 可选择已创建的 SSL 客户端策略，也可以新创建 SSL 客户端策略 仅 HTTPS 类型的虚服务器支持本参数
调度资源-SSL 服务器端扩展策略	配置虚服务器引用的携带 SNI 的 SSL 服务器端策略 1） 单击<新建>按钮，新建 SSL 服务器端扩展策略 ● 策略名称：SSL服务器端策略的名称，不区分大小写 ● 服务器名称指示：SNI（Server Name Indicator），不区分大小写 2） 单击<确定>按钮，新建的 SSL 服务器端扩展策略会在列表中显示 若虚服务器同时引用不带 SNI 的 SSL 服务器端策略，设备会选取不带 SNI 的 SSL 服务器端策略作为默认策略 在相同虚服务器中，不允许配置SNI相同的多个SSL服务器端策略 仅HTTPS类型的虚服务器支持本参数
调度资源-Cookie 持续性组	虚服务器所对应的持续性组名称，不区分大小写 设备支持通过以下三种方式引用持续性组： ◆ 在虚服务器页面指定实服务组对应的持续性组 ◆ 在动作页面指定实服务组对应的持续性组 ◆ 在虚服务器页面指定虚服务器对应的持续性组方式 其中，通过本配置指定的虚服务器引用的持续性组优先级最高。即在进行流量分配时，优先根据虚服务器引用的持续性组生成持续性表项 本命令仅支持引用 HTTP-Cookie 类型的持续性组 不支持引用持续性方法为 Cookie 截取的 Cookie 持续性组 仅 HTTP 和 HTTPS 类型的虚服务器支持本参数
调度资源-VRF	配置虚服务器的 VRF 后，可使虚服务器服务于特定的 VPN 可选择已创建的 VRF，也可以新创建 VRF
调度资源-iShell 文件	配置虚服务器引用的 iShell 文件。通过在虚服务器中引用 iShell 脚本文件，可对匹配虚服务器流量按照脚本的定义进行个性化的处理

参数	说明
	可以选择已创建的 iShell 文件，也可以新创建 iShell 文件 仅 TCP、UDP、HTTP、HTTPS 类型的虚服务器支持本参数
防护策略-HTTP 类型防护策略	虚服务器引用了 HTTP 类型防护策略后，就要根据该策略的配置对对匹配指定虚服务器的流量进行防护 可选择已创建的 HTTP 类型的防护策略，也可以新创建 HTTP 类型的防护策略 仅 HTTP 和 HTTPS 类型的虚服务器支持本参数
参数模板-IP 类型参数模板	虚服务器引用了 IP 类型参数模板后，就要根据该参数模板的配置对匹配流量进行相应的处理 可选择已创建的 IP 类型的参数模板，也可以新创建 IP 类型的参数模板 HTTP 重定向类型的虚服务器不支持本功能
参数模板-TCP 类型参数模板	虚服务器引用了 TCP 类型参数模板后，就要根据该参数模板的配置对匹配流量进行相应的处理和优化 可选择已创建的 TCP 类型的参数模板，也可以新创建 TCP 类型的参数模板 仅负载分担模式选择四层的 TCP 类型虚服务器支持本参数
参数模板-TCP 类型参数模板（客户端侧）	虚服务器引用了 TCP 类型参数模板后，就要根据该参数模板的配置对匹配流量进行相应的处理，客户端 TCP 类型的参数模板仅对设备与客户端之间建立的 TCP 连接进行处理和优化 可选择已创建的 TCP 类型的参数模板，也可以新创建 TCP 类型的参数模板 仅 Performance(HTTP)、HTTP、HTTPS、MySQL、Diameter 和负载分担模式选择七层的 TCP 类型的虚服务器支持本参数
参数模板-TCP 类型参数模板（服务器侧）	虚服务器引用了 TCP 类型参数模板后，就要根据该参数模板的配置对匹配流量进行相应的处理，服务端 TCP 类型参数模板仅对设备与服务器之间建立的 TCP 连接进行处理和优化 可选择已创建的 TCP 类型的参数模板，也可以新创建 TCP 类型的参数模板 仅 Performance(HTTP)、HTTP、HTTPS、MySQL 和负载分担模式选择七层的 TCP 类型的虚服务器支持本参数
参数模板-TCP Application 类型参数模板	虚服务器引用了 TCP Application 类型参数模板后，就要根据该参数模板的配置对匹配流量进行相应的处理 可选择已创建的 TCP Application 类型的参数模板，也可以新创建 TCP Application 类型的参数模板 仅当工作在七层的 TCP 类型的虚服务器引用 TCP Application 类型的参数模板时，该参数模板才生效

参数	说明
参数模板-HTTP 类型参数模板	虚服务器引用了 HTTP 类型参数模板后，就要根据该参数模板的配置对匹配流量进行相应的处理 可选择已创建的 HTTP 类型的参数模板，也可以新创建 HTTP 类型的参数模板 仅 Performance(HTTP)、HTTP 和 HTTPS 类型的虚服务器支持本参数
参数模板-HTTP2.0 类型参数模板（客户端侧）	虚服务器引用了客户端侧 HTTP2.0 类型的参数模板后，设备根据该参数模板的配置对客户端发起的 HTTP2.0 协议版本的报文进行处理和优化，但转发给服务器时为 HTTP1.0 或 HTTP1.1 版本的报文 可选择已创建的 HTTP2.0 类型的参数模板，也可以新创建 HTTP2.0 类型的参数模板 仅 HTTP 和 HTTPS 类型的虚服务器支持本参数
参数模板-HTTP2.0 类型参数模板（服务器侧）	虚服务器引用客户端侧 HTTP2.0 类型的参数模板，并同时引用服务器侧 HTTP2.0 类型参数模板后，设备对客户端发起的 HTTP2.0 协议版本的报文进行处理和优化，并转发给实服务器时为 HTTP2.0 版本的报文。若仅引用服务器侧 HTTP2.0 类型参数模板，未引用客户端侧 HTTP2.0 类型参数模板，则引用的该参数模板不生效 可选择已创建的 HTTP2.0 类型的参数模板，也可以新创建 HTTP2.0 类型的参数模板 仅 HTTP 和 HTTPS 类型的虚服务器支持本参数
参数模板-HTTP 统计类型参数模板	虚服务器引用了 HTTP 统计类型参数模板后，就要根据该参数模板的配置对匹配流量进行相应的处理 可选择已创建的 HTTP 统计类型的参数模板，也可以新创建 HTTP 统计类型的参数模板 仅 HTTP 和 HTTPS 类型的虚服务器支持本参数
参数模板-HTTP 压缩类型参数模板	虚服务器引用了 HTTP 压缩类型参数模板后，就要根据该参数模板的配置对匹配流量进行相应的处理 可选择已创建的 HTTP 压缩类型的参数模板，也可以新创建 HTTP 压缩类型的参数模板 仅 HTTP 和 HTTPS 的虚服务器支持本参数
参数模板-OneConnect 类型参数模板	虚服务器引用了 OneConnect 类型参数模板后，就要根据该参数模板的配置对匹配流量进行相应的处理 可选择已创建的 OneConnect 类型的参数模板，也可以新创建 OneConnect 类型的参数模板

参数	说明
	仅 HTTP 和 HTTPS 类型的虚服务器支持本参数
参数模板-MySQL 类型参数模板	虚服务器引用了 MySQL 类型参数模板后，就要根据该参数模板的配置对匹配流量进行相应的处理 可选择已创建的 MySQL 类型的参数模板，也可以新创建 MySQL 类型的参数模板 仅 MySQL 类型的虚服务器支持本参数
参数模板-Diameter-Session 类型参数模板	虚服务器引用了 Diameter-Session 类型参数模板后，客户端发起的 Diameter 请求报文匹配虚服务器后，就要根据该参数模板的配置对匹配流量进行相应的处理 可选择已创建的 Diameter-Session 类型参数模板，也可以新创建 Diameter-Session 类型参数模板 仅 Diameter 类型的虚服务器支持本参数
QoS-最大连接数	虚服务器所允许的最大连接数，0 表示虚服务器所允许的最大连接数不受限制 HTTP 重定向类型的虚服务器不支持本功能
QoS-每秒最大连接数	虚服务器所允许的每秒最大连接数，0 表示虚服务器所允许的每秒最大连接数不受限制 HTTP 重定向类型的虚服务器不支持本功能
QoS-最大总带宽	虚服务器所允许的最大总带宽，0 表示最大带宽不受限制 HTTP 重定向和 Diameter 类型的虚服务器不支持本功能
QoS-最大入带宽	虚服务器所允许的最大入带宽，0 表示最大带宽不受限制 HTTP 重定向和 Diameter 类型的虚服务器不支持本功能
QoS-最大出带宽	虚服务器所允许的最大出带宽，0 表示最大带宽不受限制 HTTP 重定向和 Diameter 类型的虚服务器不支持本功能
外链代理-外链代理功能	开启/关闭外链代理功能。外链代理功能通过代理 IPv6 客户端的 IPv4 外链访问请求，使 IPv6 单栈用户可以正常访问 IPv4 外链，帮助用户实现从 IPv4 网络到 IPv6 网络的平滑过渡 仅 HTTP 类型的虚服务器支持本参数 当设备检测到服务器返回的 HTTP 应答报文中包含外链时，会对外链域名进行改写。在原始的外链域名后添加 URI 标识、域名后缀和虚服务器端口号。以便 IPv6 客户端以改写后的域名发送 DNS 请求报文，设备在收到包含指定 URI 标识的请求报文时，会代理 IPv6 客户端请求 IPv4 外链资源 改写后的域名为：协议类型://原始外链域名+URI 标识+域名后缀+:虚服

参数	说明
	务器端口号。协议类型包括 HTTP 和 HTTPS 例如，协议类型为 HTTP，原始的 IPv4 外链域名为 www.example1.com，若配置 URI 标识为 proxy，域名后缀为 example2.com，虚服务器端口号为 8080，则改写后的外链域名为 http://www.example1.com.proxy.example2.com:8080
外链代理-外链代理的 URI 标识	外链代理的 URI 标识，不区分大小写，字符串中可以包含字母、数字、连字符“-”、下划线“_”，不能为英文句号“.” 外链代理的 URI 标识用来标识经过设备改写后的外链。当设备收到 IPv6 站点服务器返回的应答报文时，设备会对应答报文中包含的 IPv4 外链域名进行改写。假设原始的 IPv4 外链域名为 http://www.example1.com，若配置 URI 标识为 proxy，域名后缀为 example2.com，虚服务器端口号为 8080，则改写后的外链域名为 http://www.example1.com.proxy.example2.com:8080。当设备收到请求改写后外链域名的 DNS 请求报文后，设备会提取出原始的外链域名并代替 IPv6 客户端请求 IPv4 外链资源，并将获得的资源返回给客户端 仅 HTTP 类型的虚服务器支持本参数
外链代理-外链代理的域名后缀	外链改写后的域名后缀，由“.”分隔的字符串组成（如 aabbcc.com），每个字符串的长度不超过 63 个字符，不区分大小写，字符串中可以包含字母、数字、连字符“-”、下划线“_”或英文句号“.” 仅 HTTP 类型的虚服务器支持本参数
外链代理-外链地址池	外链代理的 SNAT 地址池，不区分大小写 当设备收到包含改写后外链域名的 DNS 请求报文后，设备会提取出原始的外链域名并使用外链地址池中的地址作为客户端 IP，代替客户端请求 IPv4 外链资源 若未配置外链地址池，则会将设备通往服务器的出接口 IP 地址作为客户端 IP 仅 HTTP 类型的虚服务器支持本参数
外链代理-外链地址池	外链代理的 SNAT 地址池，不区分大小写 当设备收到包含改写后外链域名的 DNS 请求报文后，设备会提取出原始的外链域名并使用外链地址池中的地址作为客户端 IP，代替客户端请求 IPv4 外链资源 若未配置外链地址池，则会将设备通往服务器的出接口 IP 地址作为客户端 IP

参数	说明
	仅 HTTP 类型的虚服务器支持本参数
外链代理-白名单列表	外链代理的白名单，若将指定域名添加到外链代理白名单中，则设备不会对加入白名单中的外链进行代理 1） 在输入框中输入外链代理白名单的域名。由“.”分隔的字符串组成（如 aabbcc.com），每个字符串的长度不超过 63 个字符，不区分大小写，字符串中可以包含字母、数字、“-”、“_”或“.” 2） 单击<添加>按钮，输入的域名会在“白名单列表”中显示 仅 HTTP 类型的虚服务器支持本参数

步骤4　单击<确定>按钮，新建的虚服务器会在“虚服务器”页面显示。

4.16　出链路负载均衡

本帮助主要介绍以下内容：

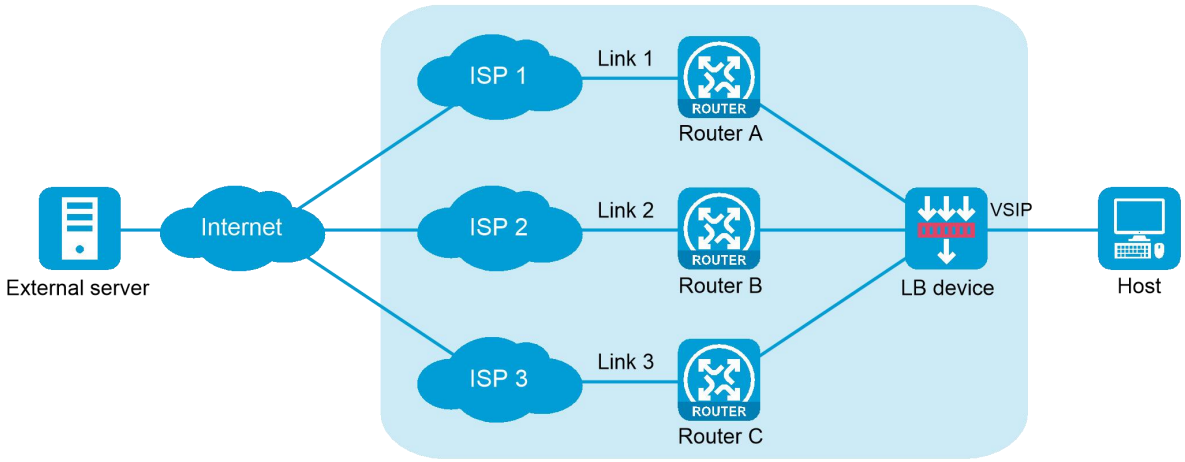
- 特性简介
  - 出方向链路负载均衡原理
  - 出方向链路负载均衡配置关系图
- vSystem相关说明
- 配置指南
  - 健康检测（可选）
  - 就近性（可选）
  - 持续性组（可选）
  - ISP
  - ALG
  - 流量特征

- 链路
- 链路组
- 选路策略

4.16.1 特性简介

4.16.1.1 出方向链路负载均衡原理

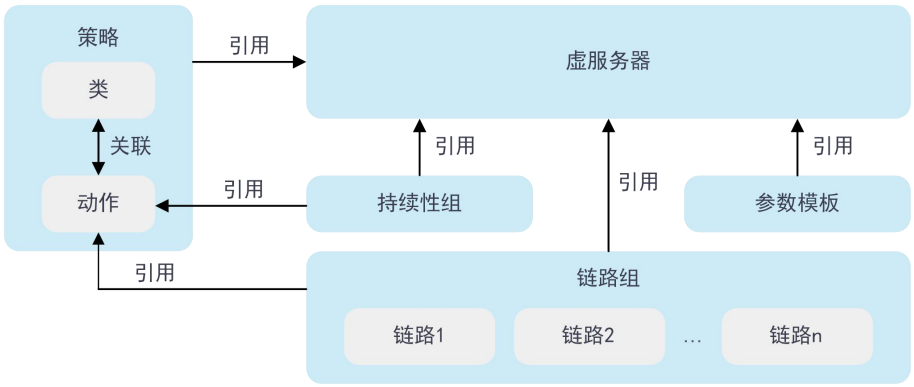
出方向链路负载均衡将特定的业务（网络服务、网络流量等）分担给多条链路，从而提高了业务处理能力，保证了业务的高可靠性。出方向链路负载均衡功能可在多条链路上分担内网用户访问外部互联网的流量。



出方向链路负载均衡包含以下要素：

- LB device（负载均衡设备）：负责将内网用户访问外部互联网的流量分发到多条链路。
- Link（链路）：运营商提供的实体链路。
- VSIP（Virtual Service IP，虚服务IP）：集群对外提供的虚服务IP地址，即内网用户发送报文的目的网段。
- Server IP（服务器IP）：供负载均衡设备分发服务请求时使用。

4.16.1.2 出方向链路负载均衡配置关系图

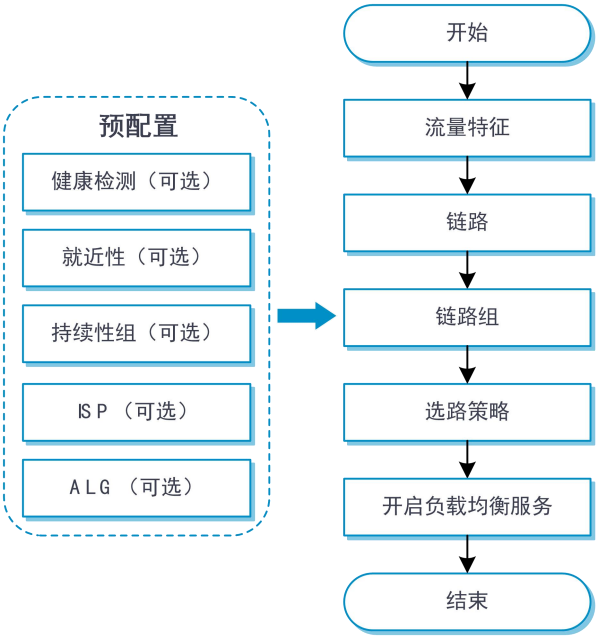


4.16.2 vSystem相关说明

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。

4.16.3 配置指南

出方向链路负载均衡功能的配置思路如下图所示：



4.16.3.1 健康检测（可选）

健康检测模板可被链路或链路组引用。

配置健康检测功能的详细步骤请参见“健康检测”联机帮助。

4.16.3.2 就近性（可选）

配置就近性的详细步骤请参见“对象 > 负载均衡”联机帮助。

4.16.3.3 持续性组（可选）

持续性组可被IPv4/IPv6选路策略引用。

配置持续性组的详细步骤请参见“对象 > 负载均衡”联机帮助。

4.16.3.4 ISP

ISP可被匹配规则引用。

配置ISP的详细步骤请参见“对象 > 负载均衡”联机帮助。

4.16.3.5 ALG

配置ALG的详细步骤请参见“网络 > ALG”联机帮助。

4.16.3.6 流量特征

流量特征的作用是将报文分类，即通过匹配规则将报文按照一定条件进行匹配，以便将不同类型的报文在不同的动作流程中处理。

步骤1 单击“策略 > 负载均衡 > 链路负载均衡 > 出链路负载均衡 > 流量特征”。

步骤2 在“流量特征”页面单击<新建>。

步骤3 新建流量特征。

参数	说明
流量特征名称	流量特征的名称，不区分大小写
匹配方式	流量特征的匹配方式，包括： ◆ 匹配任意一条规则：匹配任一规则就算匹配该流量特征 ◆ 匹配所有规则：匹配所有规则才算匹配该流量特征
匹配规则	通过匹配规则将报文按照一定条件进行匹配，以便将不同类型的报文在不同的动作流程中处理。一个流量特征中最多允许创建 65535 条匹配规则 1） 单击<新建>按钮，新建匹配规则 ● Match ID：匹配规则的编号，取值范围为1～65535。报文按照Match ID从小到大的顺序依次进行匹配 ● 类型：匹配规则的类型，包括：源IPv4、源IPv6、流量特征、IPv4 ACL、IPv6

参数	说明
	ACL、ISP、应用组、目的IPv4、目的IPv6、目的域名、入接口和用户 ● IPv4地址：匹配指定的IPv4地址，只有匹配规则的类型选择“源IPv4”或“目的IPv4”时，才会出现该参数 ● 掩码长度：IPv4地址的掩码长度，取值范围为0～32，只有匹配规则的类型选择“源IPv4”或“目的IPv4”时，才会出现该参数 ● IPv6地址：匹配指定的IPv6地址，只有匹配规则的类型选择“源IPv6”或“目的IPv6”时，才会出现该参数 ● 前缀长度：IPv6地址的前缀长度，取值范围为0～128，只有匹配规则的类型选择“源IPv6”或“目的IPv6”时，才会出现该参数 ● 流量特征：匹配指定的流量特征，只有匹配规则的类型选择“流量特征”时，才会出现该参数 ● IPv4 ACL：匹配指定的IPv4 ACL，可选择已创建的IPv4 ACL，也可以新创建IPv4 ACL。只有匹配规则的类型选择“IPv4 ACL”时，才会出现该参数 ● IPv6 ACL：匹配指定的IPv6 ACL，可选择已创建的IPv6 ACL，也可以新创建IPv6 ACL。只有匹配规则的类型选择“IPv6 ACL”时，才会出现该参数 ● ISP：匹配指定的ISP，可选择已创建的ISP，也可以新创建ISP。只有匹配规则的类型选择“ISP”时，才会出现该参数 ● 应用组：匹配指定的应用组，可选择已创建的应用组，也可以新创建应用组。只有匹配规则的类型选择“应用组”时，才会出现该参数 ● 目的域名：匹配指定的域名。设备会将域名与IP地址的对应关系记录在DNS缓存表中，当业务流量匹配DNS缓存表中的IP地址时，查找出对应的域名。再将查找到的域名与配置的目的域名进行匹配。其中，DNS缓存表可在“监控 > DNS缓存信息”页面查看。只有匹配规则的类型选择“目的域名”时，才会出现该参数 ● 入接口：匹配指定的入接口。只有匹配规则的类型选择“入接口”时，才会出现该参数 ● 用户：匹配指定的用户或用户组，可选择已创建的身份识别用户或身份识别用户组，也可以新创建用户或用户组。只有匹配规则的类型选择“用户”时，才会出现该参数

参数	说明
	2） 单击<确定>，新建的匹配规则会在“匹配规则”中显示
描述	流量特征的描述信息

步骤4 单击<确定>，新建的流量特征会在“流量特征”页面显示。

4.16.3.7 链路

配置链路的详细步骤请参见“对象 > 负载均衡”联机帮助。

4.16.3.8 链路组

为了便于对链路进行统一管理，可将具有相同或相似功能的链路抽象成一个组，称为链路组。比如，可按不同的运营商划分为ISP1链路组、ISP2链路组和ISP3链路组等。

4.16.3.8.1 配置步骤

步骤1 单击“策略 > 负载均衡 > 链路负载均衡 > 出链路负载均衡 > 链路组”。

步骤2 在“链路组”页面单击<新建>。

步骤3 新建链路组。

参数	说明
链路组名称	链路组的名称，不区分大小写
动态就近性	开启/关闭动态就近性功能 开启本功能前，需要先在“就近性参数”页面中配置就近性参数。生成的就近性表项可在“就近性表项”页面查看
调度算法	选择链路组的调度算法，包括： ◆ 加权轮转：即根据链路权值的大小把新连接依次分发给每个链路，权值越大，分配的新连接越多 ◆ 随机：把新连接随机分发给每个链路 ◆ 加权最小连接：总是把新连接分发给加权活动连接数（当前活动连接数/权值）最小的链路 ◆ 加权最小连接（基于成员）：总是把新连接分发给加权活动连接数（链路组成员在指定链路组中的活动连接数/权值）最小的链路组成员。该算法中使用的权值为链路组成员下配置的权值 ◆ 源IP地址哈希：根据源IP地址进行的哈希算法 ◆ 源IP地址和端口哈希：根据源IP地址和端口号进行的哈希算法 ◆ 目的IP地址哈希：根据目的IP地址进行的哈希算法 ◆ 带宽算法：报文根据链路的权值与剩余带宽比例分发到各链路上 ◆ 最大带宽算法：报文总是分发给当前空闲带宽最大的链路 ◆ 链路质量算法：即根据链路的网络延迟、路由跳数和丢包率综合计算出链路的质量，根据链路质量把新连接依次分发给每条

参数	说明
	链路，链路质量越好，分配的新连接越多 缺省情况下，负载均衡算法为加权轮转算法
最小可用百分比	当主用链路组中可用的链路数量占链路总数量的百分比低于此值时，该链路组将被认为不可用，从而切换到备用链路组
最大可用百分比	当主用链路组中可用的链路数量占链路总数量的百分比高于此值时，将从备用链路组切换回主用链路组。最大可用百分比必须大于等于最小可用百分比
优先级调度	缺省情况下，一个链路组中调用优先级最高的链路全部被调度算法调用。用户通过本配置可以限制链路组中可被调度算法调用的链路的数量： ◆ 如果调用优先级最高的可用链路数量大于“调用链路最大数量”时，则只选用“调用链路最大数量”条链路 ◆ 如果调用优先级最高的可用链路数量小于“调用链路最小数量”时，除了调用全部优先级最高的可用链路外，还会调用优先级次高的可用链路，直至调用的可用链路数量达到“调用链路最小数量”，或者没有可用的链路可调用为止 其中，链路的优先级在“链路”配置页面指定
健康检测方法	链路组引用的健康检测模板。通过健康检测可以对链路进行检测，保证其能够提供有效的服务 用户既可在“链路组”配置页面对组内的所有链路进行配置，也可在“链路组成员”配置页面只对当前链路组成员进行配置，或者在“ 链路”配置页面只对当前链路进行配置，后两者的配置优先级相同，且高于“链路组”配置页面的健康检测配置。建议优先在“链路组”页面配置健康检测 链路的健康检测结果影响链路组成员的使用，链路组成员的健康检测结果不影响链路的使用 可选择已创建的健康检测模板，也可以新创建健康检测模板
健康检测成功条件	链路的健康检测成功条件 ◆ 全部检测通过：只有全部健康检测方法都通过检测才认为健康检测成功 ◆ 至少n个检测通过：健康检测成功所需通过检测的最少方法数为n。当用户指定的最少方法数n大于设备上实际存在的方法数量时，只要实际存在的全部方法通过检测，系统也将认为健康检测成功
成员列表	设备支持以下两种添加链路组成员的方式： 新建链路并将链路添加为链路组成员： 1） 单击<添加>按钮，选择“新建链路” 2） 配置链路组成员信息，具体配置项说明请参见“链路”

参数	说明
	3) 单击<确定>按钮，新建的链路会在“成员列表”中显示 选择已存在的链路： 1) 单击<添加>按钮，选择“添加已存在的链路” 2) 在下拉列表中选择已创建的链路并配置链路组成员信息，具体配置项说明请参见“链路” 3) 单击<确定>按钮，添加的链路会在“成员列表”中显示
目的地址转换	开启/关闭目的地址转换功能 出链路负载均衡通常需要在链路组中关闭目的地址转换功能
链路故障处理方式	选择链路的故障处理方式，包括： ◆ 保持已有连接：不主动断开与故障链路的连接，连接继续保持还是断开将由协议自身的超时机制决定 ◆ 重定向连接：把连接重定向到链路组中其它可用的链路上 ◆ 断开已有连接：主动断开与故障链路的连接。对于TCP报文，将发送RST报文；对于其它类型的报文，将发送ICMP不可达报文 缺省情况下，链路组的故障处理方式为保持已有连接
描述	链路组的描述信息

步骤4 单击<确定>，新建的链路组会在“链路组”页面显示。

4.16.3.9 选路策略

将流量特征和动作关联起来就构成了选路策略。选路策略是指导报文转发的一种方式，用户可以为匹配特定流量特征的报文指定执行的动作。

用户只能在一个选路策略中指定一个流量特征，转发报文时会按照选路策略的配置顺序来匹配流量特征，匹配成功则执行相应的动作，否则继续匹配下一条流量特征。如果所有流量特征均未匹配，则执行“*Default*”流量特征对应的动作。

4.16.3.9.1 全局配置步骤

步骤1 单击“策略 > 负载均衡 > 链路负载均衡 > 出链路负载均衡 > IPv4/IPv6选路策略”。

步骤2 在“IPv4/IPv6选路策略”页面进行全局配置。

参数	说明
负载均衡服务	开启/关闭出链路负载均衡

参数	说明
带宽繁忙保护	开启/关闭链路的带宽繁忙保护功能。带宽繁忙保护功能就是对链路的带宽繁忙比进行限制。当流量超过某条链路的带宽繁忙比后，新建流量（非匹配持续性的流量）将不再向该链路分发，而原有流量则仍由该链路继续分发
会话扩展信息备份	开启/关闭链路的会话扩展信息备份功能
持续性信息备份	开启/关闭链路的持续性表项备份功能
持续性表项备份类型	持续性表项的备份类型，包括： ◆ 组间备份：表示仅在备份组内备份持续性表项 ◆ 全局备份：在多台负载均衡设备之间备份持续性表项，而非只在备份组内的两台设备间备份 只有持续性表项备份功能处于开启状态时，才支持配置本功能

4.16.3.9.2 IPv4/IPv6选路策略配置步骤

步骤1 单击“策略 > 负载均衡 > 链路负载均衡 > 出链路负载均衡 > IPv4/IPv6选路策略”。

步骤2 在“IPv4/IPv6选路策略”页面单击<新建>。

步骤3 新建IPv4/IPv6选路策略。

参数	说明
流量特征	可选择已创建的流量特征，也可以新创建流量特征
转发动作	转发动作，包括： ◆ 负载均衡 ◆ 丢弃报文 ◆ 转发
ToS	发往服务器的 IP 报文中的 ToS 字段。IPv6 选路策略不支持本参数
主用链路组	当主用链路组可用（该链路组存在且有可用的链路）时，使用主用链路组指导转发；当主用链路组不可用而备用链路组可用时，使用备用链路组指导转发 可选择已创建的链路组，也可以新创建链路组
备用链路组	可选择已创建的链路组，也可以新创建链路组
持续性组	出方向链路负载均衡仅支持地址端口类型的持续性组 可选择已创建的持续性组，也可以新创建持续性组
选择链路失败的处理	配置查找链路失败时继续匹配下一条规则 在转发中，若根据当前策略判断查找可用链路失败时，可继续顺序匹配下一条规则 本功能对于 SIP 类型的虚服务不生效

参数	说明
选择链路全部繁忙的处理	配置选择链路全部繁忙时继续匹配下一条规则 在转发中，若根据当前策略选择的链路全部处于繁忙状态时，可继续顺序匹配下一条规则
位于 XX 之前	将新创建的策略移至指定的 IPv4/IPv6 选路策略之前，设备将按照先后顺序依次匹配流量特征，并执行相应的动作。其中，XX 为指定 IPv4/IPv6 选路策略的流量特征名称

步骤4　单击<确定>，新建的IPv4/IPv6选路策略会在“IPv4/IPv6选路策略”页面显示。

4.17　本地智能DNS

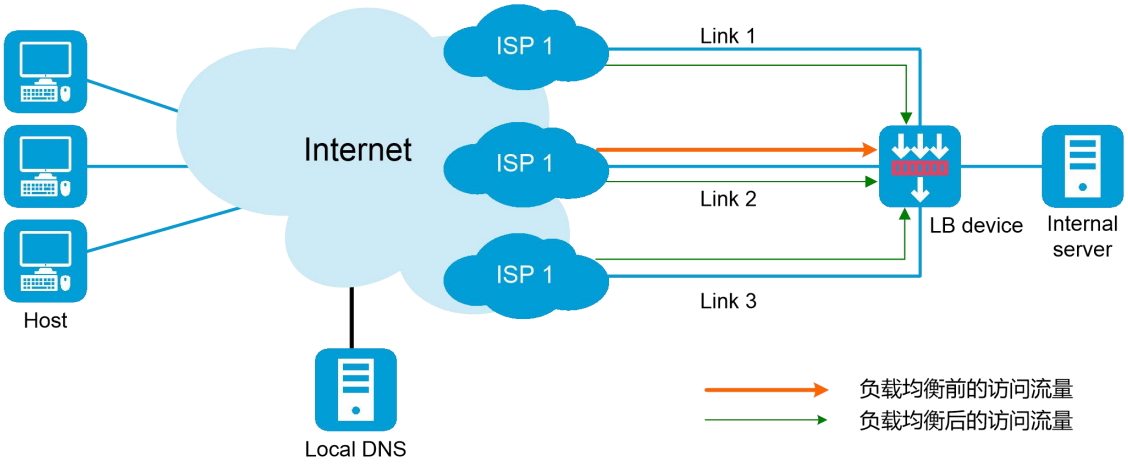
本帮助主要介绍以下内容：

- 特性简介
  - 本地智能DNS原理
  - 设备上的业务处理流程
- 使用限制和注意事项
- vSystem相关说明
- 配置指南
  - DNS正向域（可选）
  - DNS反向域（可选）
  - DNS映射
  - 静态就近性策略
  - DNS监听器

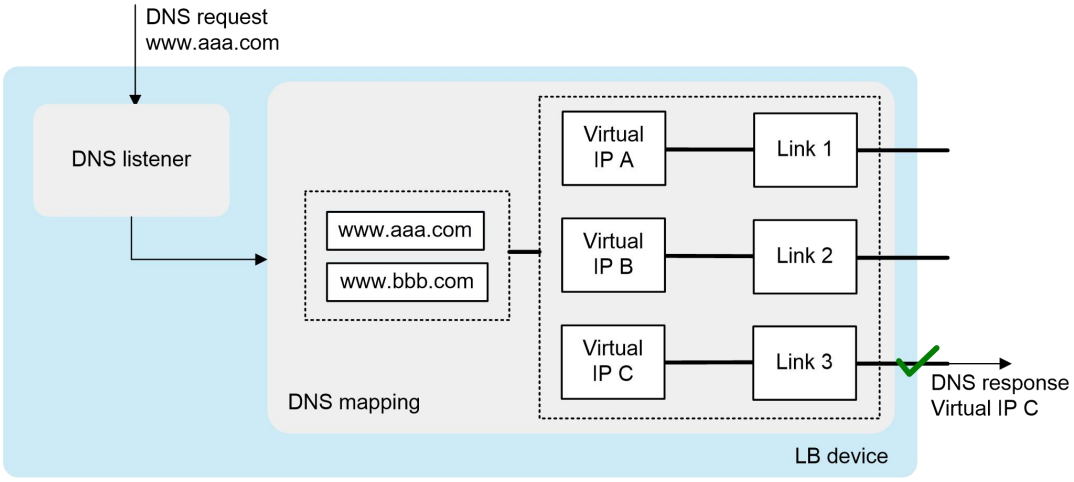
4.17.1 特性简介

4.17.1.1 本地智能DNS原理

通过配置本地智能DNS，可以使外部互联网用户访问内网服务器的流量较为均匀地分配到多条链路上，从而提高流量转发效率，提升服务质量；可以避免出现一条链路拥塞而其他链路闲置的情况；可以在某条链路出现故障时，使外部互联网用户使用其它链路来访问内网服务器，避免因链路故障导致流量转发失败。



4.17.1.2 设备上的业务处理流程



如图所示，当DNS监听器监听到负载均衡设备上收到了目的地址匹配DNS监听地址的DNS正向解析请求时，首先在DNS映射中查找域名所关联的虚IP。负载均衡设备依据调度算法选出最佳链路所对应的虚IP，将选定的虚IP地址通过DNS应答报文发送给用户，用户得到虚IP地址后将其作为目的地址，通过

该虚IP关联的链路访问内网服务器。

4.17.2 使用限制和注意事项

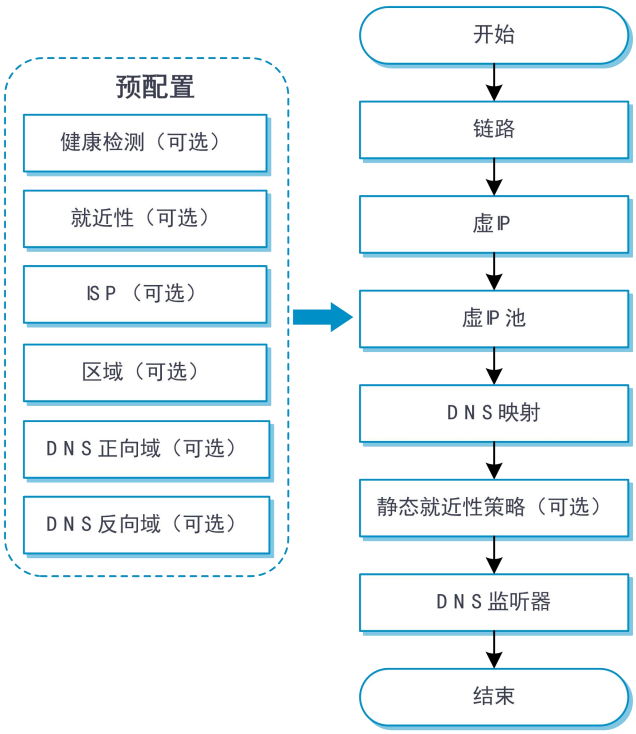
如果同时配置本地智能DNS功能和服务器负载均衡功能，请避免配置虚服务器的IP地址与DNS监听器地址为同一地址，以免影响本地智能DNS功能的正常使用。

4.17.3 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。

4.17.4 配置指南

本地智能DNS功能的配置思路如下图所示：



4.17.4.1 DNS正向域（可选）

负载均衡设备使用DNS正向域中配置的资源记录来查找域名对应的主机名。DNS资源记录是负载均衡设备用于解析DNS请求的数据记录表项，DNS正向域中可以配置以下几种类型的资源记录：

- CNAME（Canonial Name，规范名称）资源记录允许将多个别名映射到同一正规主机名，即同一服务器。例如，企业内网有一台主机名为host.example.com的服务器，它同时对外提供Web服务和邮件服务，为了便于用户访问，可以为该服务器配置CNAME资源记录，分别配置别名为www.example.com和mail.example.com。当用户请求Web服务时，访问www.example.com，

当用户请求邮件服务时，访问mail.example.com，而实际访问的均为host.example.com。

- MX（Mail Exchanger，邮件交换）资源记录用于指定该DNS正向域的邮件服务器。
- NS（Name Server，权威名称服务器）资源记录用于指定为该DNS正向域服务的权威名称服务器。
- SOA（Start of Authority，起始授权）资源记录用来配置一个DNS正向域的主域名服务器、管理员邮箱等参数。

4.17.4.1.1 配置步骤

步骤1 单击“策略 > 负载均衡 > 链路负载均衡 > 本地智能DNS > DNS正向域”。

步骤2 在“DNS正向域”页面单击<新建>按钮。

步骤3 新建DNS正向域。

参数	说明
DNS 正向域域名	DNS 正向域的域名，不区分大小写，由“.”分隔的字符串组成，每个字符串的长度不超过 63 个字符，包括“.”在内的总长度不超过 253 个字符。字符串中可以包含字母、数字、“-”、“_”和“.”
缓存时间	DNS 正向域中所有资源记录的缓存时间
资源记录列表	1） 单击<新建>按钮，新建资源记录 ● 类型： 资源记录的类型，包括：MX、NS、CNAME ● 子域名：DNS正向域的子域名。不区分大小写，由“.”分隔的字符串组成。每个字符串的长度不超过63个字符，包括“.”在内的总长度不超过254个字符，可以包含字母、数字、“-”、“_”或“.”。只有资源记录的类型选择“MX”或“NS”时，才会出现该参数 ● 邮件服务器主机名：邮件服务器的主机名。不区分大小写，由“.”分隔的字符串组成。每个字符串的长度不超过63个字符，包括“.”在内的总长度不超过254个字符，可以包含字母、数字、“-”、“_”或“.”。只有资源记录的类型选择“MX”时，才会出现该参数 ● 优先级：MX资源记录的优先级。该值越小，优先级越高。只有资源记录的类型选择“MX”时，才会出现该参数 ● 权威名称服务器主机名：权威名称服务器的主机名。不区分大小写，由“.”分隔的字符串组成。每个字符串的长度不超过63个字符，包括“.”在内的总长度不超过254个字符，可以包含字母、数字、“-”、“_”或“.”。只有资源记录的类型选择 “NS”时，才会出现该参数

参数	说明
	• 别名：正规主机的别名。不区分大小写，由“.”分隔的字符串组成。每个字符串的长度不超过63个字符，包括“.”在内的总长度不超过254个字符，可以包含字母、数字、“-”、“_”或“.”。只有资源记录的类型选择“CNAME”时，才会出现该参数 • 规范名称：正规主机名，不区分大小写，由“.”分隔的字符串组成。每个字符串的长度不超过63个字符，包括“.”在内的总长度不超过254个字符，可以包含字母、数字、“-”、“_”或“.”。只有资源记录的类型选择“CNAME”时，才会出现该参数 • 缓存时间：当前资源记录的缓存时间 2） 单击<确定>按钮，新建的资源记录会在“资源记录列表”中显示
SOA-主域名服务器主机名	DNS 正向域的主域名服务器主机名。可以是相对域名（不以“.”结束），也可以是绝对域名（以“.”结束）。当主机名为绝对域名时，不会自动扩充主机名，其长度不能大于 254 个字符；当主机名为相对域名时，会进行自动扩充，在用户配置的主机名后自动添加当前 DNS 正向域域名。主机名加 DNS 正向域域名的长度总和不能大于 254 个字符
SOA-管理员邮箱地址	DNS 正向域的管理员邮箱地址。可以是相对域名（不以“.”结束），也可以是绝对域名（以“.”结束）。当管理员邮箱地址为绝对域名时，不会自动扩充主机名，其长度不能大于 254 个字符；当管理员邮箱地址为相对域名时，会进行自动扩充，在用户配置的管理员邮箱地址后自动添加当前 DNS 正向域域名。管理员邮箱地址加区域名长度总和不能大于 254 个字符
SOA-序列号	DNS 正向域的序列号。用于标识该 DNS 正向域配置的新旧，DNS 正向域越新，序列号越大。辅助域名服务器会周期性地查询主域名服务器上 DNS 正向域的序列号，然后和本地的 DNS 正向域序列号相比较
SOA-刷新间隔	辅助域名服务器以刷新间隔为周期，从主域名服务器上获取 SOA 资源记录，然后和本地辅助域名服务器上的 SOA 资源记录相比较
SOA-重试间隔	重试时间为辅助域名服务器进行 DNS 正向域复制失败后的等待时间
SOA-过期时间	过期时间是指当辅助域名服务器与主域名服务器失去联系后，辅助域名服务器可继续进行 DNS 解析的时长
SOA-最小缓存时间	主域名服务器上的资源记录在辅助域名服务器上被缓存的时间

步骤4　单击<确定>按钮，新建的DNS正向域会在“DNS正向域”页面显示。

4.17.4.2　DNS反向域（可选）

负载均衡设备根据DNS反向域对收到的报文进行反向DNS解析，即根据IP地址查找对应的域名。DNS反向域中设置的PTR（Pointer Record，指针记录）用来记录域名和IP地址的映射关系。

DNS反向地址解析通常用于解决网络中的垃圾邮件攻击，即对邮件发送方的合法性进行检查，来拒绝转发或接收非法邮件。例如，当邮件服务器收到来自外网用户的邮件时，向设备发送反向解析请求，设备收到来自邮件服务器的反向解析请求后，查找在DNS反向域中配置的PTR资源记录，将邮件发送方的源IP地址解析为域名并将解析结果返回给邮件服务器。邮件服务器将收到的域名与邮件报文中的发送方域名进行比较，结果一致则接收该邮件，否则认为该邮件为垃圾邮件并将其丢弃。

4.17.4.2.1　配置步骤

步骤1　单击“策略 > 负载均衡 > 链路负载均衡 > 本地智能DNS > DNS反向域”。

步骤2　在“DNS反向域”页面单击<新建>按钮。

步骤3　新建DNS反向域。

参数	说明
类型	DNS 反向域的类型，包括 IPv4 和 IPv6
IPv4 地址	DNS 反向域的 IPv4 地址。只有 DNS 反向域的类型选择 “IPv4”时，才会出现该参数
IPv6 地址	DNS 反向域的 IPv6 地址。只有 DNS 反向域的类型选择 “IPv6”时，才会出现该参数
掩码	DNS 反向域的掩码长度。只有 DNS 反向域的类型选择 “IPv4”时，才会出现该参数
前缀	DNS 反向域的前缀长度。只有 DNS 反向域的类型选择 “IPv6”时，才会出现该参数
PTR 资源记录列表	1）　单击<新建>按钮，新建 PTR 资源记录 ● IPv4地址：只有DNS反向域的类型选择 “IPv4”时，才会出现该参数。且该IPv4地址应在其所属DNS反向域的IPv4地址范围内 ● IPv6地址：只有DNS反向域的类型选择 “IPv6”时，才会出现该参数。且该IPv6地址应在其所属DNS反向域的IPv6地址范围内 ● 域名：IP地址对应的域名。不区分大小写。由“.”分隔的字符串组成，每

参数	说明
	个字符串的长度不超过63个字符，包括“.”在内的总长度不超过253个字符。字符串中可以包含字母、数字、“-”、“_”或“.” ● 缓存时间：当前PTR资源记录的缓存时间 2) 单击<确定>按钮，新建的 PTR 资源记录会在“PTR 资源记录列表”中显示

步骤4 单击<确定>按钮，新建的DNS反向域会在“DNS反向域”页面显示。

4.17.4.3 DNS映射

DNS映射的作用是把指定的域名与虚IP/虚服务关联在一起，当负载均衡设备收到DNS请求时可以根据域名获取到所关联的虚IP/虚服务，并根据调度算法选择一个虚IP/虚服务。

4.17.4.3.1 配置步骤

步骤1 单击“策略 > 负载均衡 > 链路负载均衡 > 本地智能DNS > DNS映射”。

步骤2 在“DNS映射”页面单击<新建>按钮。

步骤3 新建DNS映射。

参数	说明
DNS 映射名称	DNS 映射名称，不区分大小写
域名列表	1) 在输入框中输入 DNS 映射的域名。域名支持通配符配置，允许使用的通配字符包括问号“?”和星号“*”，通配符使用规则如下： ● 域名中允许使用多个问号“?”，问号“?”用于代替域名中的单个字符，域名中的点“.”除外 ● 域名中允许使用多个星号“*”，星号“*”用于代替域名中的多个字符，域名中的点“.”除外 ● 域名中允许同时使用问号“？”和星号“*” ● 域名中以点“.”分隔的字符串的长度为1～63个字符 ● 域名中起始字符与结束字符支持字母、数字、横线、下划线、通配符星号“*”与通配符问号“？”；中间字符支持字母、数字、横线、下划线、点号“.”、通配符星号“*”与通配符问号“？”

参数	说明
	2) 单击<添加>按钮，输入的域名会在“域名列表”中显示
虚 IP/虚服务列表	1) 单击<新建>按钮，新建虚 IP 或虚服务 ● 虚服务：入链路负载均衡的虚服务。可选择已创建的虚服务器，也可以新创建虚服务器 ● IP地址：入链路负载均衡的虚IP地址。在无需配置服务器负载均衡的场景下，可以不配置虚服务器，直接配置虚IP地址简化配置 ● 链路：虚服务或虚IP关联的链路。可选择已创建的链路，也可以新创建链路 ● 权值：虚服务或虚IP的调用权值。在加权轮转和加权最小连接调度时，该数值越大，虚服务或虚IP越被优先调用 2) 单击<确定>按钮，新建的虚服务或虚 IP 会在“虚 IP/虚服务列表”中显示
首选调度算法	虚 IP 和虚服务的首选调度算法，首选调度算法优先级最高，当采用首选算法不能选出可用的虚 IP 或虚服务器时，采用次选调度算法，备选调度算法优先级最低。首选调度算法包括： ◆ 加权轮转算法：根据虚IP/虚服务权值的大小将DNS请求依次分发给每个虚IP/虚服务，权值越大，分配的DNS请求越多 ◆ 随机算法：把DNS请求随机分发给每个虚IP/虚服务 ◆ 加权最小连接算法：总是把DNS请求分发给加权活动连接数（当前活动连接数/权值）最小的虚IP/虚服务 ◆ 静态就近性算法：跟据静态就近性表项把DNS请求分发给虚IP/虚服务 ◆ 动态就近性：根据动态就近性表项把DNS请求分发给虚IP/虚服务 ◆ 源IP地址哈希：根据源IP地址哈希算法将DNS请求分发给虚IP/虚服务 ◆ 源IP地址和端口哈希：根据源IP地址和端口号哈希算法将DNS请求分发给虚IP/虚服务 ◆ 目的IP地址哈希：根据目的IP地址哈希算法将DNS请求分发给虚IP/虚服务 ◆ 带宽算法：根据虚IP的权值与剩余带宽的比例把DNS请求分发给每个虚IP/虚服务 ◆ 最大带宽算法：总是将DNS请求分发给处于空闲状态且带宽最大的链路所对应的虚IP/虚服务 缺省情况下，首选调度算法为加权轮转算法
次选调度算法	选择虚 IP 和虚服务的次选调度算法，支持的调度算法种类与首选调度算法一致

参数	说明
备选调度算法	虚 IP 和虚服务的备选调度算法，支持的调度算法种类与首选调度算法一致
带宽繁忙保护	开启/关闭带宽繁忙保护功能 开启带宽繁忙保护功能后，设备根据用户配置的调度方式选择虚 IP/虚服务时，会查看所选取的虚 IP/虚服对应的链路是否超过配置的繁忙比，如果超出则不选择该 IP。其中，链路的带宽繁忙比在“链路”页面配置
缓存时间	缓存域名解析记录的缓存时间，取值范围为 0～4294967295，单位为秒，该缓存时间将会被填充到 DNS 应答报文的域名解析记录中。例如，当虚 IP 配置变化时，用户可以通过配置小一些的缓存时间，使 DNS 请求客户端尽快获得新的解析记录；而在网络稳定的环境下，用户可将缓存时间设置为更大的值，提高域名的解析稳定性及速度
DNS 映射功能	开启/关闭 DNS 映射功能

步骤4　单击<确定>按钮，新建的DNS映射会在“DNS映射”页面显示。

4.17.4.4　静态就近性策略

静态就近性策略定义了本地DNS服务器源地址区域与虚IP所在IP地址段的对应关系。当DNS映射中指定调度算法为静态就近性调度算法时，需要配置静态就近性策略。若DNS请求匹配多个静态就近性策略时，优先选择优先级值高的策略。

4.17.4.4.1　配置步骤

步骤1　单击“策略 > 负载均衡 > 链路负载均衡 > 本地智能DNS > 静态就近性策略”。

步骤2　在“静态就近性策略”页面单击<新建>按钮。

步骤3　新建静态就近性策略。

参数	说明
区域名称	本地 DNS 服务器源地址区域。可选择已创建的区域，也可以新创建区域
对应地址段	◆ 虚IP所在的IPv4地址段/掩码长度0～32。当掩码长度为32时，IP地址的高八位必须小于224，且不能为0或127 ◆ 虚IP所在的IPv6地址/前缀长度0~128
优先级	静态就近性策略的优先级。若 DNS 请求匹配多个静态就近性策略时，优先级越高，越被优先调用

步骤4　单击<确定>按钮，新建的静态就近性策略会在“静态就近性策略”页面显示。

4.17.4.5 DNS监听器

用于监听负载均衡设备上收到的DNS请求。当DNS请求的目的地址匹配DNS监听地址时，会进行本地智能DNS处理，在所有的DNS映射中查找对应的域名与虚IP的映射表项。其作用是在用户与服务器建立连接前，就能通过DNS监听器获取到域名所对应的虚IP并以回复DNS请求的方式将此地址告之给用户。

4.17.4.5.1 配置步骤

步骤1 单击“策略 > 负载均衡 > 链路负载均衡 > 本地智能DNS > DNS监听器”。

步骤2 在“DNS监听器”页面单击<新建>按钮。

步骤3 新建DNS监听器。

参数	说明
DNS 监听器名称	DNS 监听器的名称，不区分大小写
DNS 监听器 IPv4 地址	DNS 监听器的 IPv4 地址。不能为环回地址、组播地址、广播地址和 0.X.X.X
DNS 监听器 IPv6 地址	DNS 监听器的 IPv6 地址。不能为环回地址、IPv6 组播地址、链路本地地址和全 0 地址
监听端口	DNS 监听器的端口。通过配置 DNS 监听器的端口，指定设备对外提供 DNS 解析服务的端口
VRF	使 DNS 监听器服务于特定的 VRF 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 > VRF”页面查看
DNS 监听功能	开启/关闭 DNS 监听功能
域名不存在的处理方式	DNS 监听器查找 DNS 请求资源记录失败时的处理方式，包括： ◆ 不回应：不回应DNS请求 ◆ 拒绝：回应DNS拒绝报文 ◆ DNS代理：通过DNS代理回应请求报文

步骤4 单击<确定>按钮，新建的DNS监听器会在“DNS监听器”页面显示。

4.18 DNS透明代理

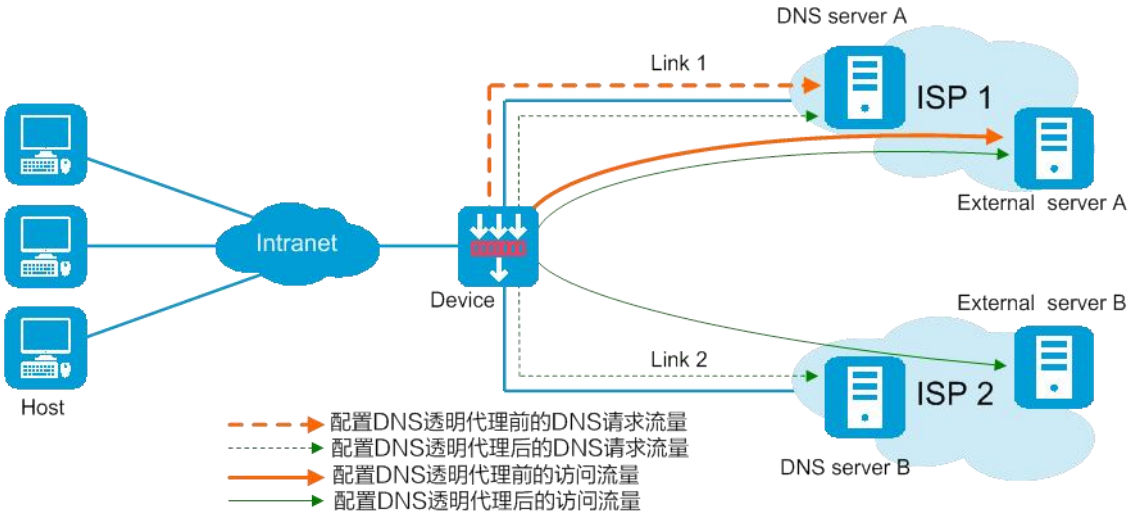
本帮助主要介绍以下内容：

- 特性简介

4.18.1 特性简介

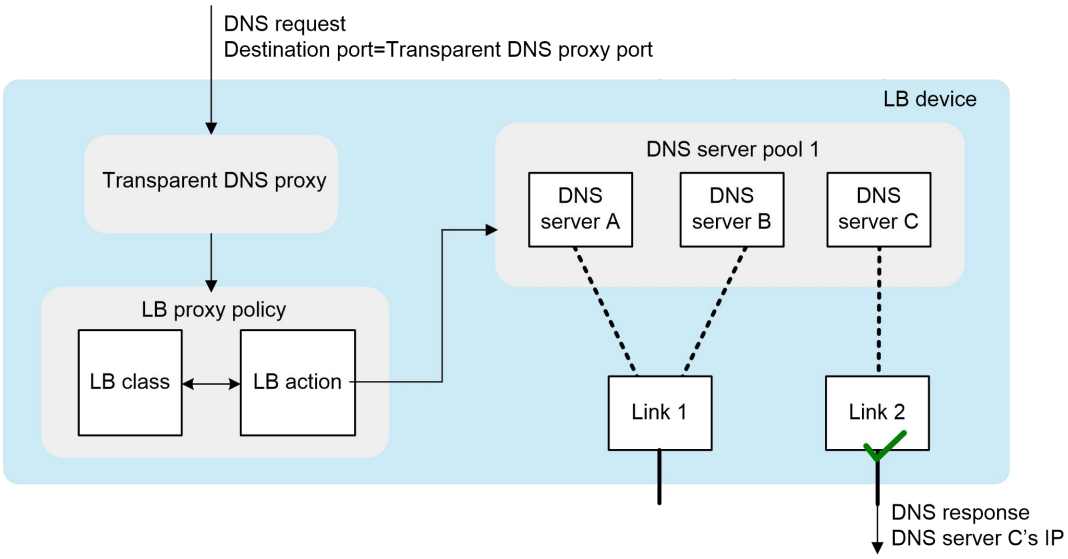
企业内网用户可以通过运营商ISP 1的链路Link 1和ISP 2的链路Link 2分别访问提供相同网络服务的外网服务器External server A和External server B。企业内网用户通过域名访问外网服务器时，内网用户的所有DNS请求报文会发往同一DNS服务器。DNS服务器收到DNS请求报文后，将其解析为同一运营商网络内外网服务器的IP地址，这将使内网用户的所有流量都通过一条链路转发，导致一条链路拥塞，而其他链路闲置。

DNS透明代理功能可以有效解决由于客户端DNS服务器的配置导致流量分配不均的问题。通过DNS透明代理功能可以使DNS请求报文发往不同运营商网络内的DNS服务器，从而使内网用户访问外网服务器的流量较为均匀地分配到多条链路上，提高流量转发效率，提升服务质量；可以避免出现一条链路拥塞而其他链路闲置的情况；也可以在某条链路出现故障时，使用其他链路来访问外网服务器，避免因链路故障导致访问失败。



4.18.1.1 设备上的业务处理流程

设备通过改变DNS请求报文的目的地址控制访问流量在多条链路上的转发，为内网用户访问外网服务器选择最佳链路。



如图所示，当收到DNS请求的目的端口号匹配DNS透明代理的代理端口号时，负载均衡设备会对DNS请求报文进行DNS透明代理处理。首先在DNS透明代理中查找关联的DNS服务器池。再依据池中配置的调度算法选出应将DNS请求分发给哪台DNS服务器。设备将选定DNS服务器的IP地址作为目的地址发送DNS请求报文，DNS服务器接收并处理DNS请求报文，将其解析为同网络内外网服务器的IP地址，并返回DNS应答报文。内网用户收到应答报文后，就可以访问该外网服务器了。

4.18.2 使用限制和注意事项

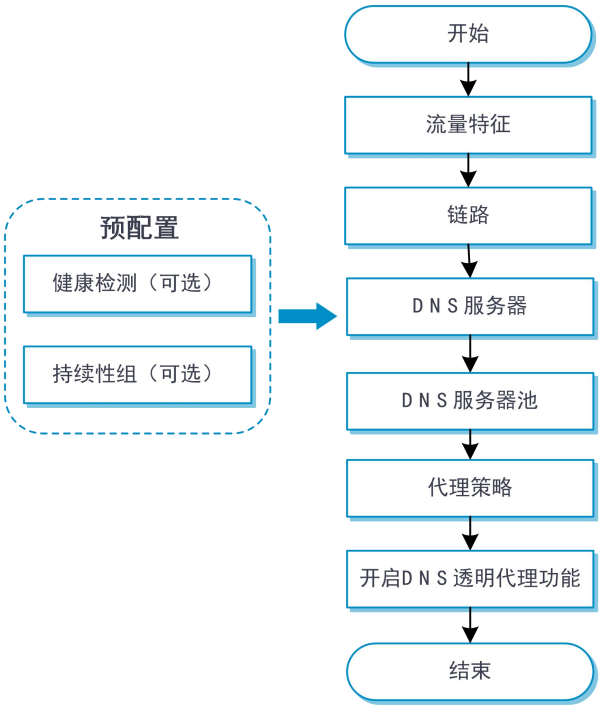
DNS透明代理功能和DNS代理功能互斥，不允许同时配置。有关DNS代理的详细介绍，请参见“DNS”联机帮助。

4.18.3 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。

4.18.4 配置指南

DNS透明代理功能的配置思路如下图所示：



4.18.4.1 健康检测（可选）

健康检测模板可被DNS服务器或DNS服务器池引用。

配置健康检测功能的详细步骤请参见“健康检测”联机帮助。

4.18.4.2 持续性组（可选）

持续性组可被IPv4/IPv6代理策略引用。

配置持续性组的详细步骤请参见“对象 > 负载均衡”联机帮助。

4.18.4.3 流量特征

流量特征的作用是将报文分类，即通过匹配规则将报文按照一定条件进行匹配，以便对不同类型的报文执行不同的转发动作。

步骤1 单击“策略 > 负载均衡 > 链路负载均衡 > DNS透明代理 > 流量特征”。

步骤2 在“流量特征”页面单击<新建>。

步骤3 新建流量特征。

参数	说明
流量特征名称	流量特征的名称，不区分大小写
匹配方式	流量特征的匹配方式，包括： ◆ 匹配任意一条规则：匹配任一匹配规则就算匹配该流量特征 ◆ 匹配所有规则：匹配所有匹配规则才算匹配该流量特征
匹配规则	通过匹配规则将报文按照一定条件进行匹配，以便对不同类型的报文执行不同的转发动作。一个流量特征中最多允许创建 65535 条匹配规则 1） 单击<新建>按钮，新建匹配规则 ● 规则ID：匹配规则的编号。报文按照规则ID从小到大的顺序依次进行匹配 ● 类型：匹配规则的类型，包括：源IPv4、源IPv6、目的IPv4、目的IPv6、流量特征、IPv4 ACL、IPv6 ACL、域名、用户和入接口 ● IPv4地址：匹配指定的IPv4地址。只有匹配规则的类型选择“源IPv4”或“目的IPv4”时，才会出现该参数 ● 掩码长度：IPv4地址的掩码长度。只有匹配规则的类型选择“源IPv4” 或“目的IPv4”时，才会出现该参数 ● IPv6地址：匹配指定的IPv6地址。只有匹配规则的类型选择“源IPv6” 或“目的IPv6”时，才会出现该参数 ● 前缀长度：IPv6地址的前缀长度。只有匹配规则的类型选择“源IPv6” 或“目的IPv6”时，才会出现该参数 ● 流量特征：匹配指定的流量特征。只有匹配规则的类型选择“流量特征”时，才会出现该参数 ● IPv4 ACL：匹配指定的IPv4 ACL。可选择已创建的IPv4 ACL，也可以新创建IPv4 ACL。只有匹配规则的类型选择“IPv4 ACL”时，才会出现该参数

参数	说明
	● IPv6 ACL：匹配指定的IPv6 ACL。可选择已创建的IPv6 ACL，也可以新创建IPv6 ACL。只有匹配规则的类型选择“IPv6 ACL”时，才会出现该参数 ● 域名：匹配指定的域名。不区分大小写。由“.”分隔的字符串组成，每个字符串的长度不超过63个字符，包括“.”在内的总长度不超过253个字符。字符串中可以包含字母、数字、“-”、“_”或“.”。域名支持通配符配置，允许使用的通配字符包括问号“?”和星号“*”， 通配符使用规则为：问号“？”用于代替域名中的单个字符，域名中的点“.”除外，域名中允许使用多个问号“?”；星号“*”用于代替域名中的多个字符，域名中的点“.”除外，域名中允许使用多个星号“*”；域名中允许同时使用问号“？”和星号“*”。只有匹配规则的类型选择“域名”时，才会出现该参数 ● 用户：匹配指定的用户或用户组，可选择已创建的身份识别用户或身份识别用户组，也可以新创建用户或用户组。只有匹配规则的类型选择“用户”时，才会出现该参数 ● 入接口：匹配指定的入接口，只有匹配规则的类型选择“入接口”时，才会出现该参数 2) 单击<确定>，新建的匹配规则会在“匹配规则”中显示
描述	流量特征的描述信息

步骤4 单击<确定>，新建的流量特征会在“流量特征”页面显示。

4.18.4.4 链路

配置链路的详细步骤请参见“对象 > 负载均衡”联机帮助。

4.18.4.5 DNS服务器

通过配置DNS服务器，指定设备上处理和响应DNS请求报文的实体。一个DNS服务器可以属于多个DNS服务器池，一个DNS服务器池也可以包含多个DNS服务器。

4.18.4.5.1 配置步骤

步骤1 单击“策略 > 负载均衡 > 链路负载均衡 > DNS透明代理 > DNS服务器”。

步骤2 在“DNS服务器”页面单击<新建>按钮。

步骤3 新建DNS服务器。

参数	说明

参数	说明
DNS 服务器名称	DNS 服务器的名称，不区分大小写
IP 地址配置方式	DNS 服务器的 IP 地址配置方式，包括： ◆ 手工配置 ◆ 自动获取：若选择以自动获取方式配置IP地址，则必须在链路配置页面指定自动获取IP地址的出接口
IPv4 地址	DNS 服务器的 IPv4 地址 IPv4 地址不能为环回地址、组播地址、广播地址和 0.X.X.X
IPv6 地址	DNS 服务器的 IPv6 地址 IPv6 地址不能为环回地址、组播地址、链路本地地址和全 0 地址
端口	DNS 服务器的端口号。0 表示继续使用原报文携带的端口号
VRF	DNS 服务器所属的 VRF
健康检测方法	DNS 服务器引用的健康检测模板。通过健康检测可以对 DNS 服务器进行检测，保证其能够提供有效的服务。用户既可在“DNS 服务器池”配置页面对池内的所有 DNS 服务器进行配置，也可在“DNS 服务器”配置页面只对当前 DNS 服务器进行配置，后者的配置优先级较高 可选择已创建的健康检测方法，也可以新建健康检测方法
成功条件	DNS 服务器的健康检测成功条件 ◆ 全部检测通过：只有全部健康检测方法都通过检测才认为健康检测成功 ◆ 至少n个检测通过：健康检测成功所需通过检测的最少方法数为n。当用户指定的最少方法数n大于设备上实际存在的方法数量时，只要实际存在的全部方法通过检测，系统也将认为健康检测成功
链路	配置与 DNS 服务器关联的链路 可选择已创建的链路，也可以新创建链路
描述	DNS 服务器的描述信息

步骤4　单击<确定>按钮，新建的DNS服务器会在“DNS服务器”页面显示。

4.18.4.6　DNS服务器池

为了便于对DNS服务器进行统一管理，可将具有相同或相似功能的DNS服务器抽象成一个组，称为DNS服务器池。

4.18.4.6.1　配置步骤

步骤1　单击“策略 > 负载均衡 > 链路负载均衡 > DNS透明代理 > DNS服务器池”。

步骤2　在“DNS服务器池”页面单击<新建>按钮。

步骤3　新建DNS服务器池。

参数	说明
DNS 服务器池名称	DNS 服务器池的名称，不区分大小写
调度算法	选择 DNS 服务器池的调度算法，包括： ◆ 带宽算法：根据DNS服务器的权值与剩余带宽的比例把DNS请求分发给每台DNS服务器。当剩余带宽相同时，该算法等价于加权轮转算法；当DNS服务器权值相同时，总是将用户请求分发给剩余带宽最大的链路所对应的DNS服务器；当DNS服务器权值和剩余带宽均不相同时，两者共同决定DNS服务器的调度 ◆ 随机：把新连接随机分发给每个DNS服务器 ◆ 加权轮转：即根据DNS服务器权值的大小把新连接依次分发给每台DNS服务器，权值越大，分配的新连接越多 ◆ 最大带宽算法：总是将DNS请求分发给处于空闲状态且带宽最大的链路所对应的DNS服务器 ◆ 源IP地址哈希：根据源IP地址进行的哈希算法 ◆ 源IP地址和端口哈希：根据源IP地址和端口号进行的哈希算法 ◆ 目的IP地址哈希：根据目的IP地址进行的哈希算法 缺省情况下，DNS 透明代理的调度算法为加权轮转算法
优先级调度	缺省情况下，一个 DNS 服务器池中调用优先级最高的 DNS 服务器全部被调度算法调用。用户通过本配置可以限制 DNS 服务器池中可被调度算法调用的 DNS 服务器的数量： ◆ 如果调用优先级最高的可用DNS服务器数量大于“最大数量”时，则只选用“最大数量”个DNS服务器 ◆ 如果调用优先级最高的可用DNS服务器数量小于“最小数量”时，除了调用全部优先级最高的可用DNS服务器外，还会调用优先级次高的可用DNS服务器，直至调用的可用DNS服务器数量达到“最小数量”，或者没有可用的DNS服务器可调用为止 其中，DNS 服务器的优先级在“DNS 服务器”配置页面指定
健康检测方法	DNS 服务器池引用的健康检测模板。通过健康检测可以对 DNS 服务器进行检测，保证其能够提供有效的服务。用户既可在“DNS 服务器池”配置页面对组内的所有 DNS 服务器进行配置，也可在“DNS 服务器”配置页面只对当前 DNS 服务器进行配置，后者的配置优先级较高 可选择已创建的健康检测方法，也可以新建健康检测方法
健康检测成功条件	DNS 服务器池的健康检测成功条件 ◆ 全部检测通过：只有全部健康检测方法都通过检测才认为健康检测成功 ◆ 至少n个检测通过：健康检测成功所需通过检测的最少方法数为n。当用户指定的最少方法数n大于设备上实际存在的方法数量时，只要实际存在的全部方法通过检测，系统也将认为健康检测成功
成员列表	设备支持以下两种添加 DNS 服务器池成员的方式：

参数	说明
	新建 DNS 服务器并将 DNS 服务器添加为 DNS 服务器池成员： 1） 单击<添加>按钮，选择“新建 DNS 服务器”。 2） 配置 DNS 服务器池成员信息，具体配置项说明请参见“DNS 服务器” 3） 单击<确定>按钮，新建的 DNS 服务器会在“成员列表”中显示 选择已存在的 DNS 服务器： 1） 单击<添加>按钮，选择“添加已存在的 DNS 服务器” 2） 在下拉列表中选择已创建的 DNS 服务器并配置 DNS 服务器池成员信息，具体配置项说明请参见“DNS 服务器” 3） 单击<确定>按钮，添加的 DNS 服务器会在“成员列表”中显示
描述	DNS 服务器池的描述信息

步骤4 单击<确定>按钮，新建的DNS服务器池会在“DNS服务器池”页面显示。

4.18.4.7 代理策略

将流量特征和动作关联起来就构成了代理策略。代理策略是指导报文转发的一种方式，用户可以为匹配特定流量特征的报文指定执行的动作。

用户只能在一个代理策略中指定一个流量特征，转发报文时会按照代理策略的配置顺序来匹配流量特征，匹配成功则执行相应的转发动作，否则继续匹配下一条流量特征。如果所有流量特征均未匹配，则执行“*Default*”流量特征对应的动作。

4.18.4.7.1 全局配置步骤

步骤1 单击“策略 > 负载均衡 > 链路负载均衡 > DNS透明代理 > IPv4/IPv6代理策略”。

步骤2 在“IPv4/IPv6代理策略”页面进行全局配置。

参数	说明
状态	用来标识 DNS 透明代理功能的状态，包括： ◆ 可用 ◆ 不可用，请检查配置
代理端口	DNS 透明代理端口号。只有当用户发送的 DNS 请求报文的目的端口号匹配 DNS 透明代理的端口号时，设备才进行 DNS 透明代理处理

参数	说明
DNS 透明代理功能	开启/关闭 DNS 透明代理功能。IPv6 代理策略不支持本参数
带宽繁忙保护	开启/关闭 DNS 服务器对应链路的带宽繁忙保护功能。带宽繁忙保护功能就是对 DNS 服务器对应链路的带宽繁忙比进行限制。当流量超过某条链路的带宽繁忙比后，新建流量（非匹配持续性的流量）将不再向该链路分发，而原有流量则仍由该链路继续分发
会话扩展信息备份	开启/关闭会话扩展信息备份功能
持续性信息备份	开启/关闭持续性表项备份功能、 若设备的配置发生以下变化，则设备会删除当前已有的持续性表项，后续流量将会重新触发生成新的持续性表项 ◆ 关闭持续性表项备份功能 ◆ 持续性表项备份由组间备份切换为全局备份 ◆ 持续性表项备份由全局备份切换为组间备份
持续性表项备份类型	持续性表项的备份类型，包括： ◆ 组间备份：表示仅在备份组内备份持续性表项 ◆ 全局备份：在多台负载均衡设备之间备份持续性表项，而非只在备份组内的两台设备间备份 只有持续性表项备份功能处于开启状态时，才支持配置本功能

4.18.4.7.2 IPv4/IPv6代理策略配置步骤

步骤1 单击“策略 > 链路负载均衡 > DNS透明代理 > IPv4/IPv6代理策略”。

步骤2 在“IPv4/IPv6代理策略”页面单击<新建>。

步骤3 新建IPv4/IPv6代理策略。

参数	说明
流量特征	可选择已创建的流量特征，也可以新创建流量特征
转发动作	转发动作，包括： ◆ 负载均衡 ◆ 丢弃报文 ◆ 转发 ◆ 跳过DNS透明代理 对于 SIP 类型的虚服务不支持配置报文的转发模式为转发
ToS	发往 DNS 服务器的 IP 报文中的 ToS 字段
DNS 服务器池	可选择已创建的 DNS 服务器池，也可以新创建 DNS 服务器池
持续性组	DNS 透明代理仅支持地址端口类型的持续性组

参数	说明
	可选择已创建的持续性组，也可以新创建持续性组
选择 DNS 服务器失败的处理	配置查找 DNS 服务器失败时继续匹配下一条策略 在转发中，若根据当前代理策略查找可用 DNS 服务器失败时，可继续顺序匹配下一条策略
选择 DNS 服务器全部繁忙的处理	配置选择 DNS 服务器全部繁忙时继续匹配下一条规则 在转发中，若根据当前代理策略选择的 DNS 服务器全部处于繁忙状态时，可继续顺序匹配下一条规则
位于 XX 之前	将新创建的策略移至指定的 IPv4/IPv6 代理策略之前，设备将按照先后顺序依次匹配流量特征，并执行相应的动作。其中，XX 为指定 IPv4/IPv6 代理策略的流量特征名称

步骤4　单击<确定>，新建的IPv4/IPv6代理策略会在“IPv4/IPv6代理策略”页面显示。

4.19　共享上网管理

本帮助主要介绍以下内容：

- 特性简介
  - 基本概念
  - 共享上网检测方式
  - 共享上网管理实现流程
- vSystem相关说明
- 使用限制和指导
- 配置指南

4.19.1　特性简介

共享上网管理功能可对通过NAT技术或代理技术进行共享上网的行为进行识别和管理。

4.19.1.1　基本概念

4.19.1.1.1　单IP允许的最大终端数

单IP允许的最大终端数是指每个IP地址可被共享的最大终端数。当设备检测到某IP地址下共享的终端数大于所配置的最大终端数时，将对该IP地址执行共享上网管理策略中配置的动作；如果检测到的终端数小于配置的最大终端数，则允许此共享行为。

4.19.1.1.2 冻结/解冻

设备支持两种方式进行冻结/解冻：

- 自动冻结/解冻：当报文源IP地址下共享的终端数超过配置的单IP允许的最大共享终端数，且共享策略动作为冻结时，该IP地址将被自动冻结，后续来自该IP地址的报文将被丢弃。当达到冻结时间后，被冻结的IP地址将自动解冻。
- 手工冻结/解冻：当IP地址处于未冻结状态时，可通过手工的方式进行冻结；当IP地址处于冻结状态且未达到冻结时间时，可通过手工的方式进行解冻。可在“共享上网管理 > 共享列表”页面，对每个IP地址的状态执行相应的操作。

4.19.1.1.3 共享列表

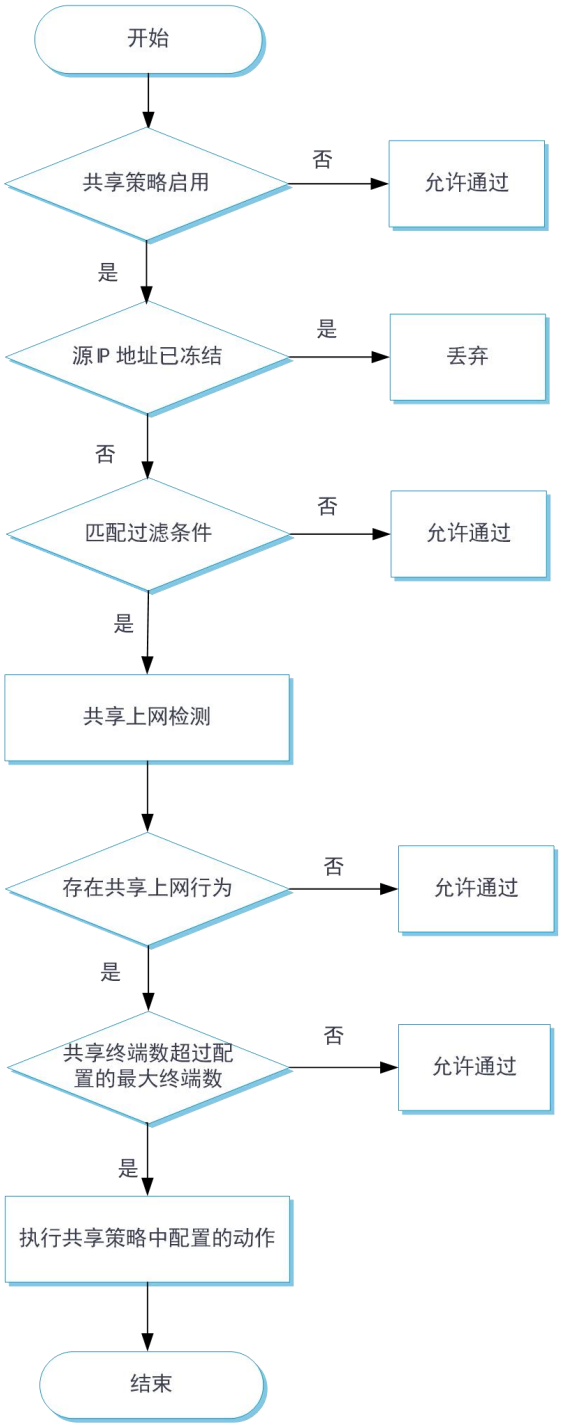
共享列表中显示设备检测到的存在共享上网行为的所有IP地址以及相关信息，包括：位置、用户名、VRF、终端数量、共享策略名称、冻结剩余时间以及状态。管理员可在“共享上网管理 > 共享列表“页面查看相关内容。

4.19.1.2 共享上网检测方式

共享上网管理支持以下检测方式：

- 应用检测方式：设备在APR（Application Recognition，应用层协议识别）的基础上进一步提取应用中的信息，用于检测终端的共享上网行为。
- IPID检测方式：设备可对报文的IPID字段的变化情况进行分析，检测终端的共享上网行为。同一主机发出报文的IPID字段连续变化并呈递增趋势，且起始值随机。如果在一段时间内，检测到相同源IP地址报文的IPID字段在同一区间连续变化并呈递增趋势，则认为此IP地址不存在共享行为；如果相同源IP地址报文的IPID字段在多个区间连续变化并呈递增趋势，则认为此IP地址存在共享行为。

4.19.1.3 共享上网管理实现流程



共享上网管理对报文的处理过程如下：

步骤1　如果未启用共享策略，则允许报文通过；如果共享策略处于启用状态，则进入步骤2处理。

步骤2　判断报文的源IP地址是否已经处于冻结状态。如果已冻结，则丢弃报文；如果未冻结，则进

入步骤3处理。

步骤3　报文与共享策略中的过滤条件进行匹配。如果匹配失败，则允许报文通过；如果匹配成功，则对报文进行共享上网检测。

步骤4　如果未检测到报文的源IP地址存在共享行为，则允许报文通过；如果检测到报文的源IP地址存在共享行为，则将该IP地址下共享的终端数量与共享策略中配置的单IP允许的最大共享终端数进行比较：

- 如果超过配置的最大终端数，则对报文执行共享策略中配置的动作；
- 如果未超过，则允许报文通过。

4.19.2　vSystem相关说明

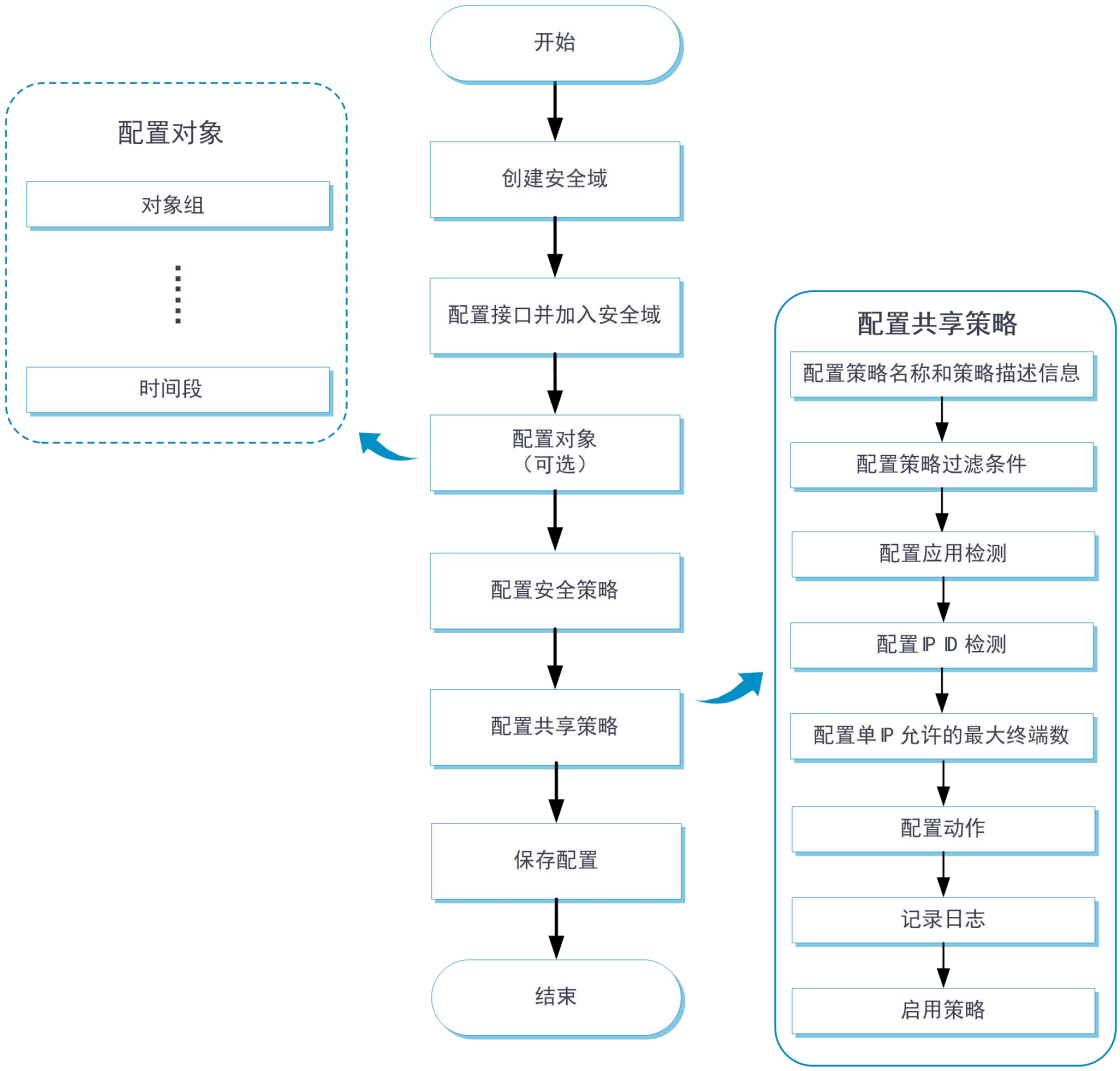
非缺省vSystem对于本特性的支持情况，请以页面的实际显示为准。

4.19.3　使用限制和指导

- 共享策略在新建和删除后均需要进行“提交“操作。执行此操作会暂时中断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。
- 目前仅支持配置一个共享策略。
- 使用本功能前，需要将APR特征库升级到最新版本。
- 应用检测方式有如下限制：
  - 仅支持对部分应用（QQ、微信、58同城和美团）进行共享上网行为检测。
  - 如果应用本身进行了加密处理，则应用检测方式无法对其进行共享上网行为检测。
- IPID检测方式有如下限制条件：
  - 检测的终端为Windows系统，且报文IPID呈规律性变化。
  - 仅支持检测IPv4类型地址。
  - 不支持对移动终端进行共享上网行为检测。

4.19.4 配置指南

共享上网管理功能的配置思路如下图所示：



在配置共享上网管理功能之前，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”。

配置共享策略具体步骤如下：

步骤1　在“策略 > 共享上网管理 > 共享策略”页面，单击<新建>按钮，进入“新建共享策略”页面。

步骤2　新建共享策略，具体配置内容如下表所示：

参数	说明
名称	配置共享策略的名称

参数	说明
描述信息	通过合理编写描述信息，便于管理员快速理解和识别本共享策略
源安全域	配置源安全域作为共享策略的过滤条件
目的安全域	配置目的安全域作为共享策略的过滤条件
源 IP 地址	配置源 IP 地址作为共享策略的过滤条件
目的 IP 地址	配置目的 IP 地址作为共享策略的过滤条件
用户	配置用户作为共享策略的过滤条件
应用检测	开启应用检测功能后，设备将针对用户特定应用（包括 QQ、微信、58 同城和美团）进行共享上网行为检测。有关应用的相关介绍请参见“应用识别联机帮助”
IPID 检测	开启 IPID 检测功能后，设备将使用报文的 IPID 字段（报文首部的标识字段）对共享上网行为进行检测
单 IP 允许的最大终端数	用来限制可以同时使用相同 IP 地址的终端数量
动作	如果检测到某 IP 地址下共享上网的终端数超过了单 IP 允许的最大终端数，设备将执行以下动作对该 IP 地址进行管理 ◆ 允许：表示允许报文通过 ◆ 冻结：表示对该IP地址进行冻结，即来自该IP地址的报文将被丢弃
冻结时间	如果共享策略动作为冻结，则需要配置相应的冻结时间。达到冻结时间后，已冻结的 IP 地址将自动解冻
记录日志	表示记录共享上网日志，当某 IP 地址下共享上网的终端数超过了单 IP 允许的最大终端数时，设备将记录该 IP 地址的相关信息以及命中的共享上网策略的相关信息，方便用户查看
启用策略	选择开启后，此共享策略才能生效

步骤3　在“新建共享策略”页面，单击<确定>按钮，新建共享策略成功，并会在“共享策略”页面中显示。

步骤4　新建共享策略后，单击<提交>按钮，使共享策略生效。

4.20　零信任策略

本帮助主要介绍以下内容：

◆ 特性简介

4.20.1 特性简介

零信任策略用来根据用户和用户访问资产的风险状况，定义用户对资产的访问权限。设备根据风险引擎对用户风险状况和资产风险状况的评估信息，在业务流量的处理过程中，执行零信任策略实现对资产的访问控制。

4.20.2 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。

4.20.3 配置指南

步骤1 单击“策略 > 零信任 > 零信任策略”。

步骤2 在“零信任策略”页面进行配置。

参数	说明
风险引擎地址	风险引擎的 URL 地址，设备可以通过风险引擎地址与风险引擎联动，获取用户风险状况和资产风险状况的评估信息 风险引擎地址配置需要满足的格式要求为：“协议类型://服务器 IP 地址:端口号/资源路径”，不区分大小写 ◆ 协议类型包括HTTP和HTTPS，如果未指定协议类型，缺省为HTTP类型 ◆ 目前服务器地址仅支持IPv4地址
VRF	风险引擎所属的 VPN 实例名称，区分大小写
开启零信任策略	开启/关闭零信任策略 当开启零信任策略后，可通过单击右侧的<获取连接状态>按钮，测试设备与风险引擎是否成功建立连接 设备预定义了 16 条策略。支持修改预定义策略的访问动作，访问动作修改后，需要单击“应用”按钮，不支持创建和删除策略 若零信任策略处于关闭状态,则设备无法与风险引擎进行联动获取用户风险状况和资产风险状况的评估信息

步骤3 在“风险用户信息”和“风险资产信息”页面，可查看从风险引擎获取到的用户风险状况和资产风险状况的评估信息。

4.21 SDP零信任

本帮助主要介绍以下内容：

- 特性简介
- vSystem相关说明
- 配置指南

4.21.1 特性简介

SDP（Software Defined Perimeter，软件定义边界）零信任功能是指设备作为SDP网关与SDP可信访问控制器联动，对访问指定应用或API的用户进行身份认证和鉴权，以实现对用户身份和访问权限的集中控制，防止非法用户访问。

4.21.2 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。

4.21.3 配置指南

步骤1 单击“策略 > 零信任 > SDP零信任”。

步骤2 在“SDP零信任”页面进行配置。

参数	说明
开启 SDP 零信任	开启 SDP 零信任功能，并配置 SDP 零信任的相关内容后，单击“应用”按钮，设备将作为 SDP 网关与 SDP 可信访问控制器联动，SDP 可信访问控制器向 SDP 网关下发用户对内网资源的访问权限，用户再通过 SDP 网关访问内网资源
访问方式	访问方式包括以下三种类型： - 混合方式 - Web接入方式 - IP接入方式
API 缺省访问动作	API 缺省访问动作包括以下两种： - 允许 - 拒绝
开启单包认证	开启单包认证后，客户端访问 SDP 网关之前，必须向 SDP 网关发送 SPA 报文，SDP 网关通过验证 SPA 报文判断客户端是否合法，若客户端合法，SDP 网关将接收客户端的后续访问请求，否则 SDP 网关将拒绝客户端的访问请求

步骤3 单击“应用”按钮，完成配置。

5 对象

5.1 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

5.1.1 特性简介

5.1.1.1 本地用户

5.1.1.1.1 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。

5.1.1.1.2 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。

5.1.1.1.3 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。

5.1.1.2 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。

5.1.1.2.1 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。

5.1.1.2.2 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。

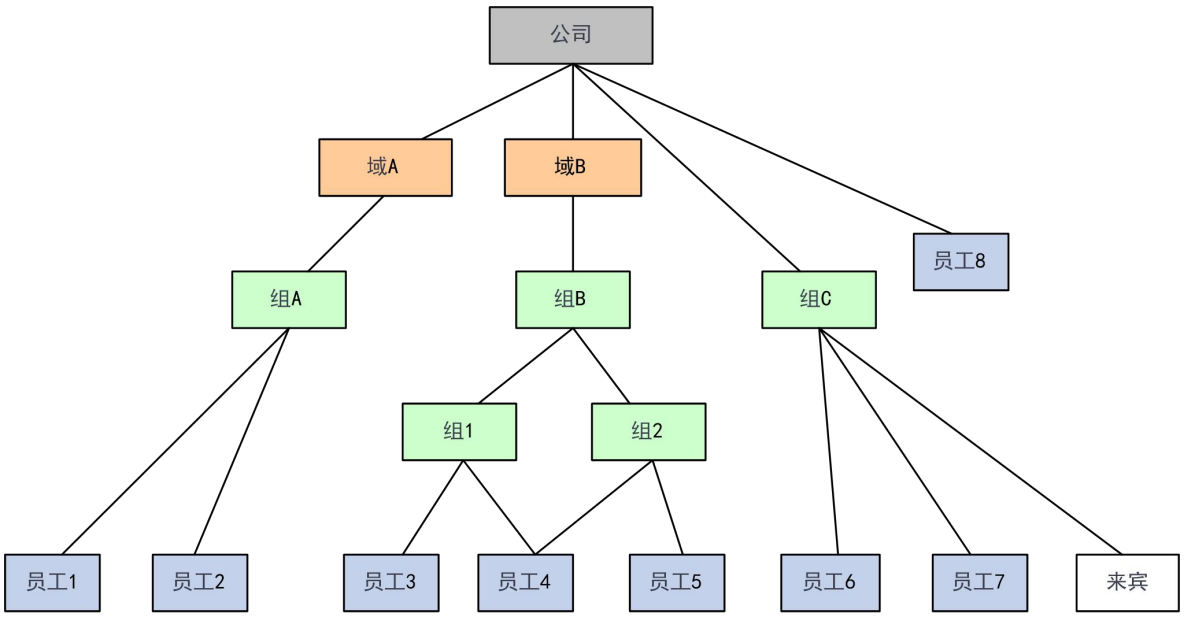
身份识别用户组被应用模块引用之后，该用户组将处于激活状态，所有基于该组的业务将会生效。当应用模块取消对该身份识别用户组的引用，该身份识别用户组将处于非激活状态。

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。

5.1.1.2.3 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，如图所示：



5.1.1.2.4 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：

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。

步骤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。

步骤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。

5.1.1.3 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。

5.1.1.4 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。

5.1.1.5 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。

5.1.2 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。

5.1.3 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。

5.1.4 配置指南

5.1.4.1 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。

5.1.4.1.1 新建本地用户

新建本地用户的具体配置步骤如下：

步骤1 选择“对象 > 用户 > 用户管理 > 本地用户”。

步骤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。

步骤3 在“新建用户”页面的具体配置内容如下表所示：

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。当需要进行本地认证时，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晚于起始时间 ● 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（密码管理属性和用户授权属性）
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，接受基于组的用户身份识别业务处理
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，如果没有用户可以使用的服务类型，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达最大值，则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

步骤4　（可选）配置授权属性，具体包括如下表所示：

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、报文的封装类型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 > ACL”对应的 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。此属性仅对 SSL VPN 用户有效

步骤5　（可选）配置绑定属性，具体包括如下表所示：

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

步骤6　（可选）配置用户密码设置控制参数，具体包括如下表所示：

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，系统将不允许设置该密码
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，系统将不允许设置该密码

参数	说明
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
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会有不同的结果
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

步骤7　单击<确定>按钮，新建用户成功，且会在“用户”页面中显示。

5.1.4.1.2　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：

步骤1　选择“对象 > 用户 > 用户管理 > 本地用户”。

步骤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。

步骤3　在“导入用户”页面的具体配置内容如下表所示：

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，不能随意修改模板的注释头，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，并将用户加入该用户组。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，系统不会创建对应的用户组，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掉已有的同名用户配置。若不配置该参数，则表示不导入文件中

参数	说明
	的同名用户信息，即保留设备上已有的同名用户配置
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，则表示导入文件中的所有用户信息

步骤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。

5.1.4.1.3　配置密码管理功能

密码管理功能具体配置步骤如下：

步骤1　选择“对象 > 用户 > 用户管理 > 本地用户”。

步骤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。

步骤3　在“用户密码管理”页面的具体配置内容如下表所示：

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的元素数量进行限制
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，系统将不允许设置该密码
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，系统将不允许设置该密码
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，新的密码历史记录将覆盖该用户最老的一条密码历史记录

参数	说明
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，需要用户更换密码
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，设备不允许用户修改密码
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况会有不同的结果
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
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，设备会针对每个 IP 地址记录用户信息，当设备记录的该用户信息条数超过最大值之后，若该用户采用新的 IP 地址再次登录认证失败，则该用户名相关的最早一条用户信息会被删除，新的记录被加入
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式。锁定用户信息可在 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示样式，之前的锁定用户信息将被清空

步骤4　单击<确定>按钮，密码管理功能将对所有本地用户生效。

5.1.4.2　配置本地用户组

配置本地用户组的具体配置步骤如下：

步骤1　选择“对象 > 用户 > 用户管理 > 身份识别用户”。

步骤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。

步骤3　在“新建用户组”页面的具体配置内容如下表所示：

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

步骤4　授权属性与SSL VPN授权属性。

步骤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。

5.1.4.3　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：

步骤1　选择“对象 > 用户 > 用户管理 > 身份识别用户”。

步骤2　在“身份识别用户”页面，可查看组织结构。

步骤3　选择需要编辑的身份识别用户或用户组，具体配置内容如下表所示：

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，也可新建用户角色

5.1.4.4　管理在线用户

在线用户的具体配置步骤如下：

步骤1　选择“对象 > 用户与管理 > 用户管理 > 在线用户”。

步骤2　在“在线用户”页面的具体配置内容如下表所示：

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，用户的认证域为abc，用户输入的用户名为test@123，则使用用户名test@123进行身份识别用户账户匹配 ● 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，

参数	说明
	用户的认证域为abc，用户输入的用户名为test@123，则使用用户名test@abc进行身份识别用户账户匹配 ● 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用户名与设备上未加入任何身份识别域的身份识别用户进行匹配。例如，用户的认证域为abc，用户输入的用户名为test@123，则使用用户名test与未加入身份识别域的用户账户进行匹配

静态身份识别用户的具体配置步骤如下：

步骤3　选择“对象 > 用户 > 用户管理 > 在线用户”。

步骤4　选择“对象 > 用户与管理 > 用户管理 > 在线用户”。

步骤5　在“在线用户”页面选择“静态身份识别用户”，具体配置内容如下表所示：

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

步骤6　单击<确定>按钮，新建“静态身份识别用户”成功。

5.1.4.5　配置用户导入策略

5.1.4.5.1　新建用户导入策略

用户导入策略的具体配置步骤如下：

步骤1　选择“对象 > 用户与管理 > 用户管理 > 用户导入策略”。

步骤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。

步骤3　在“新建用户导入策略”页面的具体配置内容如下表所示：

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在线用户信息
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户信息

参数	说明
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所有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
导入周期	自动导入身份识别用户账户的周期

步骤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。

5.1.4.5.2　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。

5.1.4.6　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：

步骤1　选择“对象 > 用户 > 用户管理 > 邮件服务器”。

步骤2　在“邮件服务器”页面的具体配置内容如下表所示：

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

5.2 认证管理

本帮助主要介绍以下内容：

5.2.1 特性简介

5.2.1.1 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。

5.2.1.2 RADIUS简介

5.2.1.2.1 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。

5.2.1.2.2 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，则会在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。

5.2.1.3 LDAP简介

5.2.1.3.1 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）组成的。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。

5.2.1.3.2 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。

5.2.1.4 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”。

5.2.1.5 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。

5.2.2 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。

5.2.3 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RADUIS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。

5.2.4 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。

5.2.4.1 配置ISP域

ISP域的具体配置步骤如下：

步骤1 选择“对象 > 用户 > 认证管理 > ISP域”。

步骤2 在“ISP域”页面单击<新建>按钮，进入“添加ISP域”页面。

步骤3 在“添加ISP域”页面的具体配置内容如下表所示：

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，不能包括“/”、“\”、“|”、“”“、“:”、“*”、“?”、“<”、“>”以及“@”字符，且不能为字符串“d”、“de”、“def”、“defa”、“defau”、“defaul”、“default”、“i”、“if”、“if-”、“if-u”、“if-un”、“if-unk”、“if-unkn”、“if-unkno”、“if-unknow”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，登录用户方式适用于需要认证登录设备的管理用户等

步骤4 （可选）配置高级配置，具体内容如下表所示：

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置检测时间内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

步骤5 单击<确定>按钮，新建ISP域成功，且会在“ISP域”页面中显示。

5.2.4.2 配置RADIUS

RADIUS的具体配置步骤如下：

步骤1　选择“对象 > 用户 > 认证管理 > RADIUS”。

步骤2　在“RADIUS”页面单击<新建>按钮，进入“新建RADIUS”页面。

步骤3　在“新建RADIUS方案”页面的具体配置内容如下表所示：

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

步骤4　RADIUS高级设置，具体包括如下表所示：

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 服务器的响应，则有必要重传 RADIUS 请求报文，以保证用户尽可能地获得 RADIUS 服务，这段时间被称为 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 服务器性能要求也越高
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最大值时切断用户连接
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 ISP 域名，设备可以通过该域名来决定将用户归于哪个 ISP 域的，也有 RADIUS 服务器不能接受携带有 ISP 域名的用户名，此时需要将用户名中携带的域名去除
发送给 RADIUS 服务器的	发送到 RADIUS 服务器的数据流的单位

参数	说明
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 Access-Challenge 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 报文通知该方案所使用的 RADIUS 计费服务器，要求 RADIUS 服务器停止计费且强制该设备的用户下线
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，报文重新发送的时间间隔
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，报文发送的最大次数
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证

步骤5　单击<确定>按钮，新建RADIUS方案成功，且会在“RADIUS”页面中显示。

5.2.4.3　配置LDAP

LDAP方案的具体配置步骤如下：

步骤1　选择“对象 > 用户 > 认证管理 > LDAP”。

步骤2　在“LDAP方案”页面单击<新建>按钮，进入“新建LDAP方案”页面。

步骤3　在“新建LDAP方案”页面的具体配置内容如下表所示：

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 属性映射为 AAA 模块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，用于设备与远程 LDAP 认证服务器建立连接
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，用于设备与远程 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

参数	说明
	SearchResultReference 字段，保存当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SearchResultReference字段中所有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拒绝。

步骤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：

步骤5　在“LDAP服务器”页面单击<新建>按钮，进入“新建LDAP服务器”页面。

步骤6　在“新建LDAP服务器”页面的具体配置内容如下表所示：

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，若不配置该参数时，则表示 LDAP 服务器属于公网
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
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 一致
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 版本号需要与远程 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未收到 LDAP 服务器的回应，则认为本次认证、授权请求超时
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 服务器会根据设置的用户组过滤条件筛选出符合条件的用户组信息发送给设备
编码格式	配置 LDAP 服务器使用的字符编码格式

参数	说明
用户 DN 查询的起始节点	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户 DN 的查找，耗费的时间将会较长，因此必须配置用户查找的起始点 DN，以提高查找效率
用户 DN 查询的范围	所有子目录表示在起始 DN 的所有子目录下进行查询；下一级子目录表示只在起始 DN 的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 域名表示发送给服务器的用户名不带 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

步骤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：

步骤8　在“新建LDAP属性映射表”页面的具体配置内容如下表所示：

参数	说明
名称	用于唯一标识一个 LDAP 属性映射表
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，则表示映射的 LDAP 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 User Profile 类型

步骤9　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。

5.2.4.4　配置RESTful服务器

RESTful服务器的具体配置步骤如下：

步骤1　选择“对象 > 用户 > 认证管理 > RESTful服务器”。

步骤2　在“RESTful服务器”页面单击<新建>按钮，进入“新建RESTful服务器”页面。

步骤3　在“新建RESTful服务器”页面的具体配置内容如下表所示：

参数	说明
名称	用来唯一标识一个 RESTful 服务器

参数	说明
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，则设备会将这些上线用户信息上传给 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，则设备会将这些下线用户信息上传给 RESTful 服务器
VRF	表示远程 RESTful 服务器所属的 VPN，若不配置该参数时，则表示 RESTful 服务器属于公网
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 RESTful 服务器的连接状态值，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

步骤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。

5.2.4.5　配置Sec Manage服务器

Sec Manage服务器的具体配置步骤如下：

步骤1　选择“对象 > 用户 > 认证管理 > Sec Manage服务器”。

步骤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。

步骤3　在“新建Sec Manage服务器”页面的具体配置内容如下表说是：

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

步骤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。

5.3　Web应用防护

本帮助主要介绍以下内容：

5.3.1　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。

5.3.1.1　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。

5.3.1.1.1 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。

5.3.1.2 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。

5.3.1.3 配置文件动作

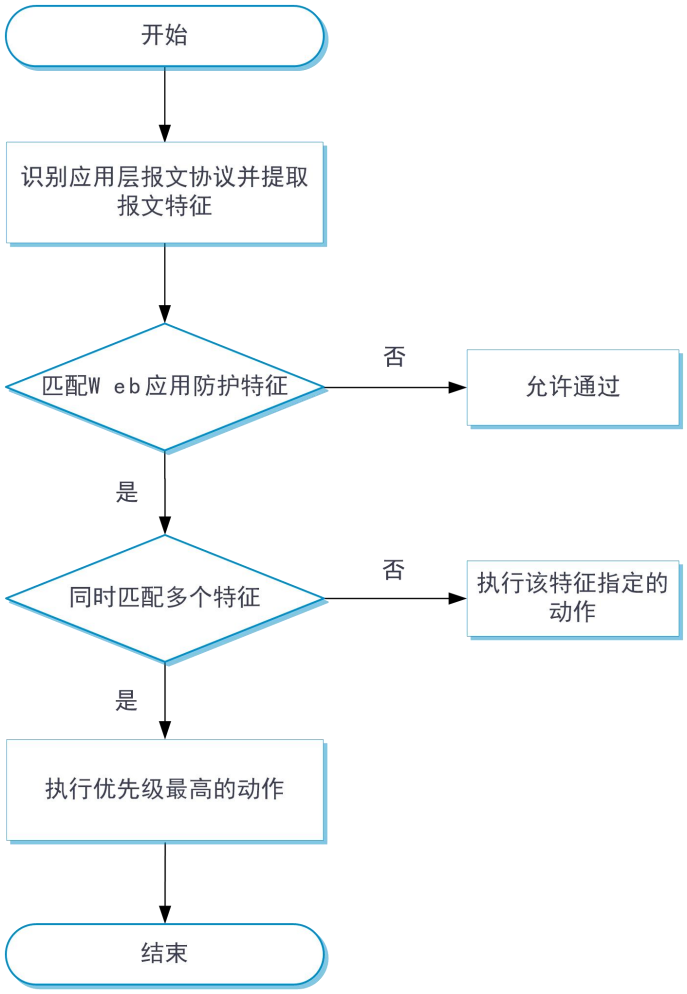
配置文件动作是指设备对匹配上Web应用防护特征或经过语义分析检测识别出攻击的报文做出的处理。

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“攻击防范联机帮助”。
- 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。

5.3.1.4 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。处理流程如下图所示：



Web应用防护处理的整体流程如下：

步骤1　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。

步骤2　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。

步骤3　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。

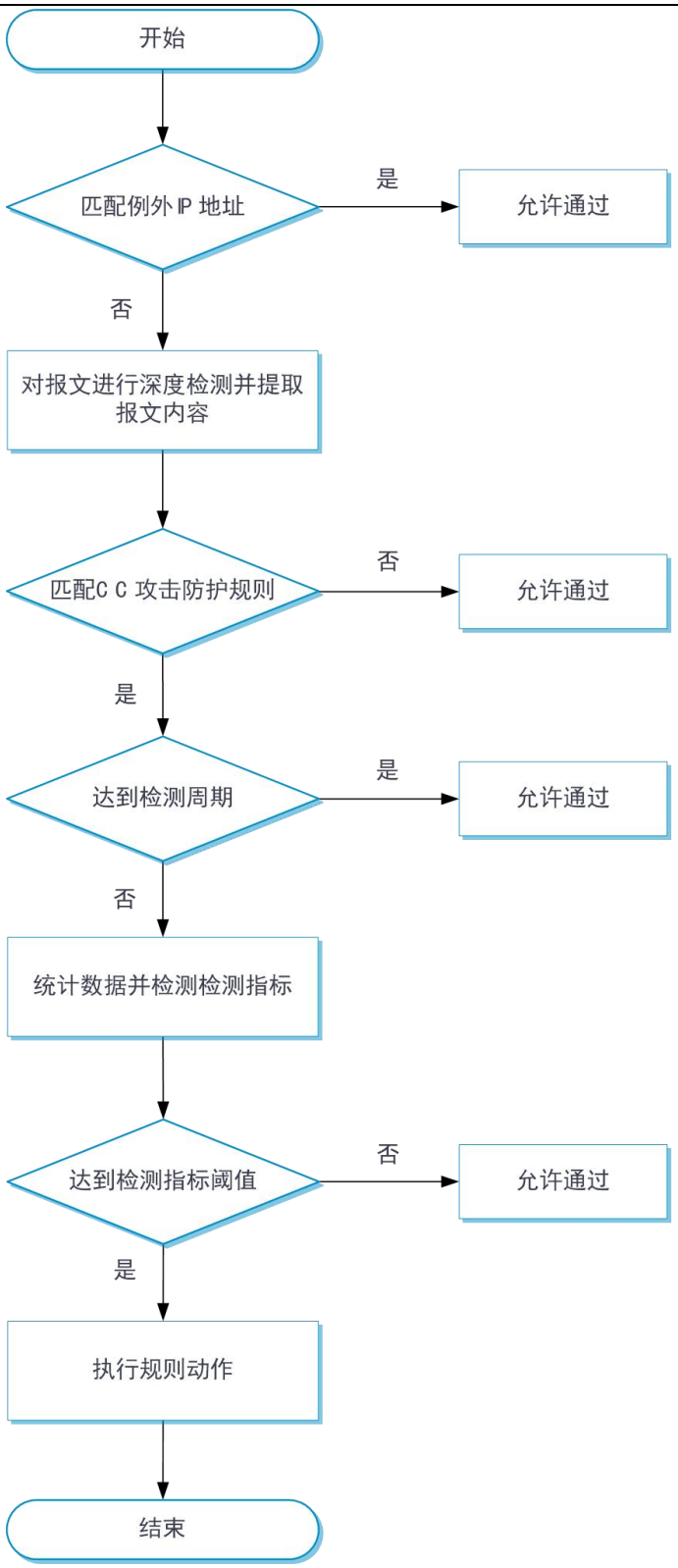
5.3.1.5　防篡改

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。

5.3.1.6　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：



步骤1　如果报文与例外IP地址匹配成功，则直接放行该报文。

步骤2　设备对报文进行深度内容检测，并提取报文内容。

步骤3　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。

步骤4　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。

步骤5　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。

5.3.2　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。

5.3.3　License支持情况

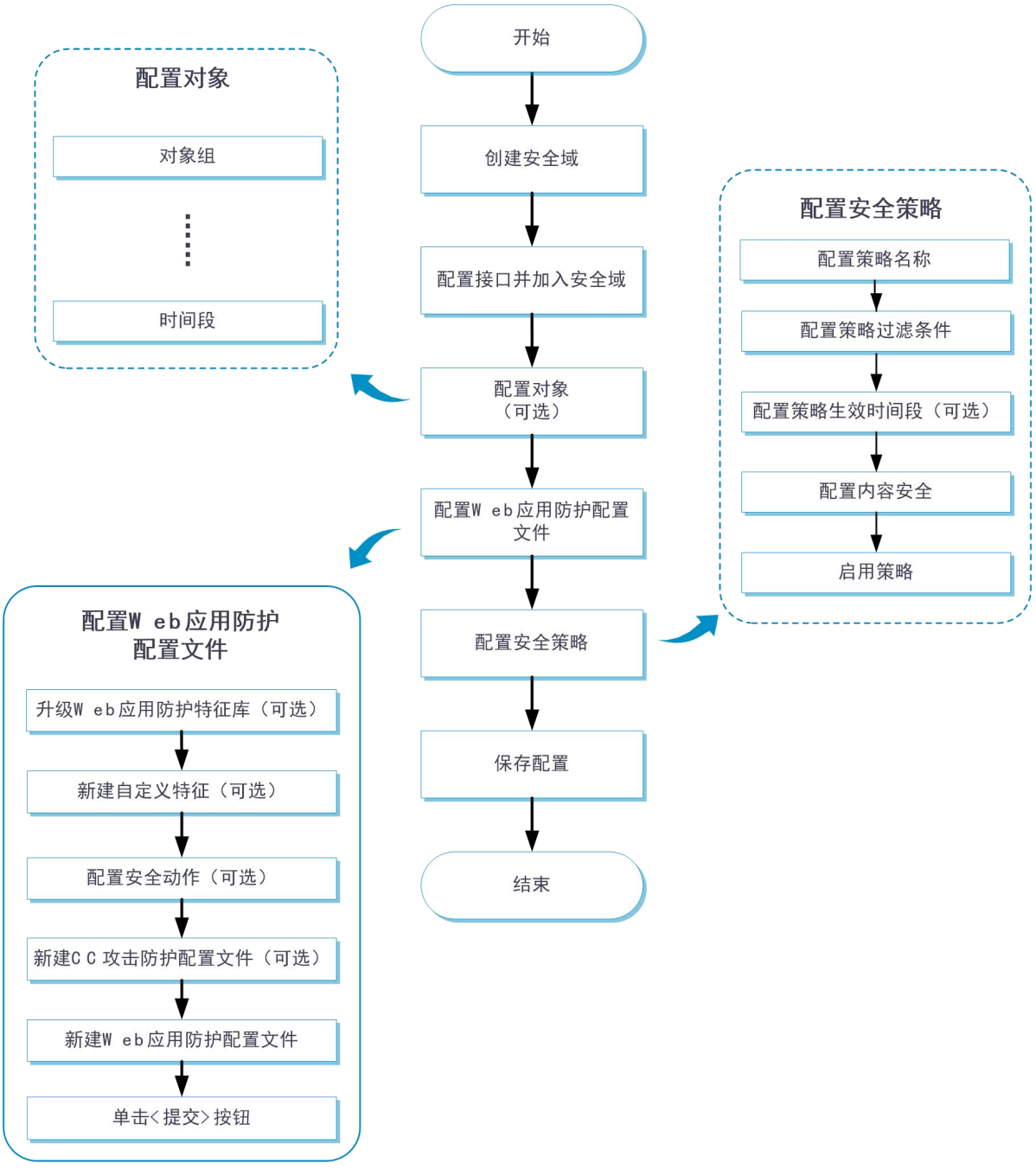
Web应用防护功能需要购买并正确安装License后才能使用。License过期后，Web应用防护功能可以采用设备中已有的Web应用防护特征库正常工作，但无法升级到官方网站在过期时间后发布的新版本的特征库。关于License的详细介绍请参见“License联机帮助”。

5.3.4　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“高级配置联机帮助”。
- 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。

5.3.5 配置指南

Web应用防护功能的配置思路如下图所示：



5.3.5.1 配置Web应用防护配置文件

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

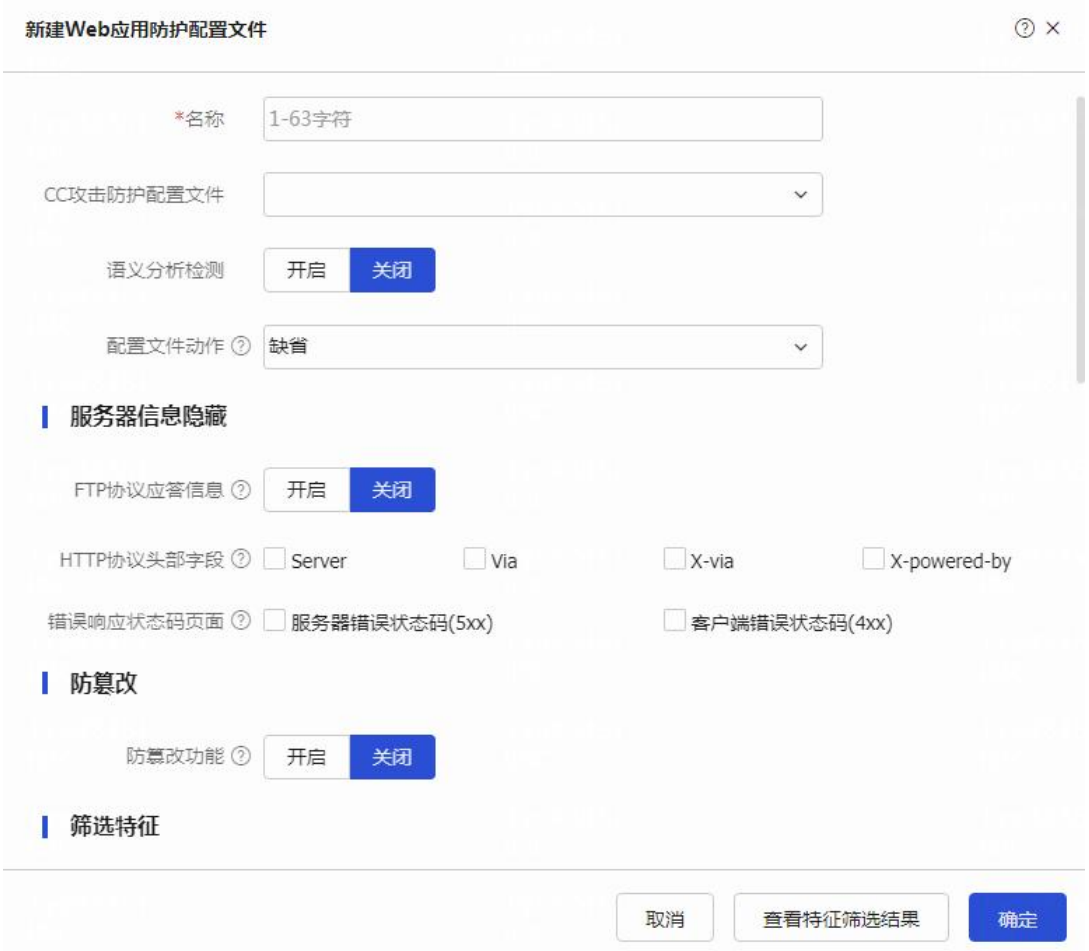
所有缺省处于启用状态的Web应用防护特征，缺省Web应用防护配置文件不能修改和删除。

管理员也可以根据实际需求创建自定义的Web应用防护配置文件。

5.3.5.1.1 配置步骤

步骤1 选择“对象 > 应用安全 > Web应用防护 > 配置文件”。

步骤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。



步骤3 新建Web应用防护配置文件，在基础参数区域配置如下内容：

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，可以提升该类攻击的识别率

参数	说明
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动作 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动作；对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
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，有关捕获参数的详细配置，请参见“安全动作联机帮助”

步骤4　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：

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，设备会对应答信息进行隐藏，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，设备会对指定头部字段内容进行隐藏，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码返回的页面内容进行隐藏，防止客户端通过该页面获取服务器版本等信息

步骤5　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：

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来筛选配置文件所需的 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，可通过选择不同的缺省动作来筛选配置文件所需的 Web 应用防护特征

参数	说明
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，可通过选择不同的严重级别来筛选配置文件所需的 Web 应用防护特征

步骤6　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。

步骤7　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。

步骤8　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“安全策略联机帮助”。

步骤9　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。

5.3.5.2　配置防篡改功能

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。

5.3.5.2.1　配置步骤

步骤1　选择“对象 > 应用安全 > Web应用防护 > 配置文件”。

步骤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。

步骤3　在防篡改区域进行如下配置。

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，同时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
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存为基线文件。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。当设备挂载了硬盘时，基线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。其中，URL 仅学习到路径（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）

参数	说明
	● 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，会将响应报文中的网页内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。此模式仅当设备配置了TCP代理时生效。有关TCP代理的详细介绍，请参见“应用代理联机帮助”
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

步骤4　单击确定按钮，完成配置。

5.3.5.3　配置CC攻击防护配置文件

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。

5.3.5.3.1　配置步骤

步骤1　选择“对象 > 应用安全 > Web应用防护 > CC攻击防护配置文件”。

步骤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。

步骤3　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：

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，有利于后期维护
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；如果匹配失败，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 攻击防护规则时开始计时

步骤4　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：

参数	说明
规则名称	CC 攻击防护规则的名称

参数	说明
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-for 字段获取真正的源 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，才计算请求集中度 ● 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次数的百分比
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，还需要配置黑名单的老化时间
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

步骤5　单击<确定>按钮，完成CC攻击防护规则的配置。

步骤6　单击<确定>按钮，完成CC攻击防护配置文件的配置。

步骤7　选择“对象 > 应用安全 > Web应用防护 > 配置文件”。

步骤8　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“配置Web应用防护配置文件”。

步骤9　单击<提交>按钮，激活Web应用防护配置文件的配置内容。

5.3.5.4 新建和删除自定义特征

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：

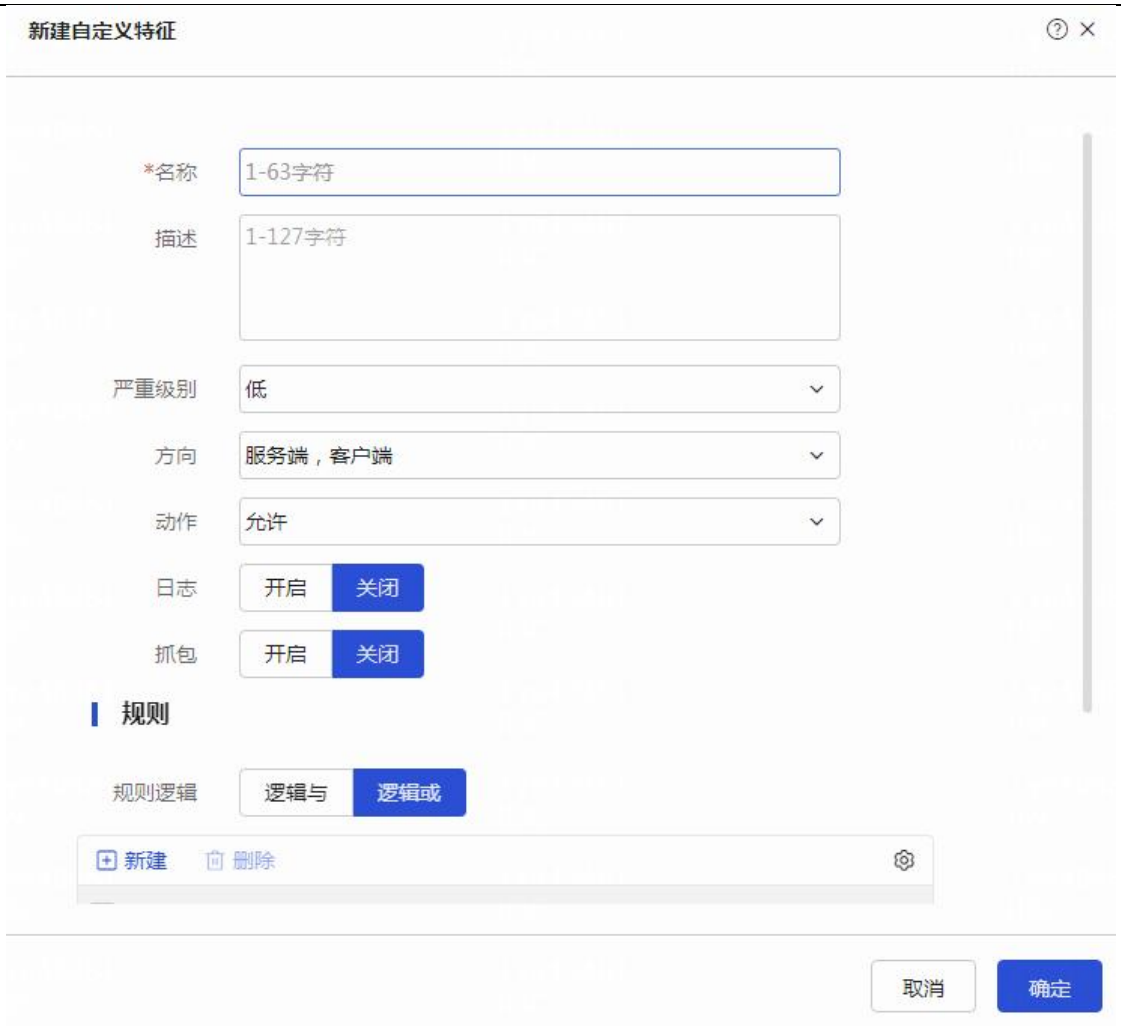
- 关键字类型：配置关键字类型规则时，需要配置检查项和检查项触发条件。只有匹配检查项触发条件后才会继续匹配检查项。仅当所有检查项都匹配成功，才表示该规则成功匹配。
- 数值类型：配置数值类型规则时，可以配置检查项，只有所有检查项都匹配成功，才表示规则成功匹配。

5.3.5.4.1 新建自定义特征

新建自定义特征的配置步骤如下：

步骤1　选择“对象 > 应用安全 > Web应用防护 > 特征”。

步骤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。



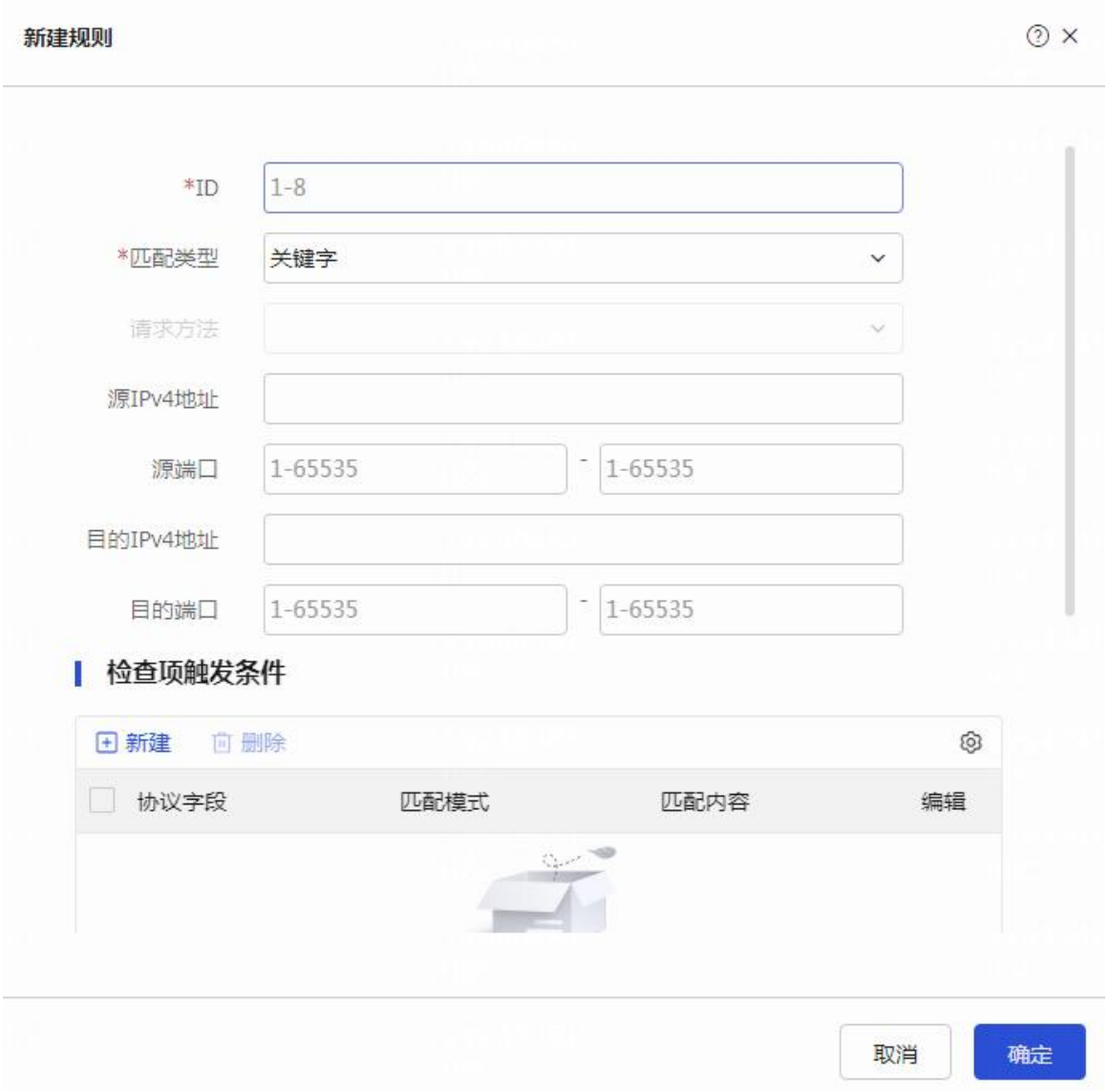
步骤3　在“基本配置”区域可配置自定义特征的属性，具体配置内容如下：

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，有利于后期维护
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。严重级别分为如下四种：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，

参数	说明
	有关捕获参数的详细配置，请参见“安全动作联机帮助”

步骤4　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。

步骤5　单击<新建>按钮，进入新建规则页面，具体配置内容如下：



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

参数	说明
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

步骤6　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：

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起始检测位置

步骤7　单击<确定>按钮，完成检查项触发条件的配置。

步骤8　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：

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，取值包括： ● 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

参数	说明
	位置开始偏移的长度
相对检测深度	表示当前检查项的检测深度

步骤9　单击<确定>按钮，完成检查项的配置。

步骤10　单击<确定>按钮，完成自定义特征规则的配置。

步骤11　单击<确定>按钮，完成自定义特征的配置。

步骤12　单击<提交>按钮，使新建的自定义特征生效。

5.3.5.4.2　删除自定义特征

删除自定义特征的配置步骤如下：

步骤1　选择“对象 > 应用安全 > Web应用防护 > 特征”。

步骤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<删除特征>按钮，选择删除选中的自定义特征。

5.4　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
  - 配置入侵防御配置文件
  - 导入和删除Snort特征

- 新建和删除自定义特征
- 导出特征库中所有特征
- 配置入侵防御白名单
- 配置入侵防御捕获报文时缓存报文数

5.4.1 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。

5.4.1.1 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。

5.4.1.2 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。

5.4.1.2.1 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。

5.4.1.3 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。

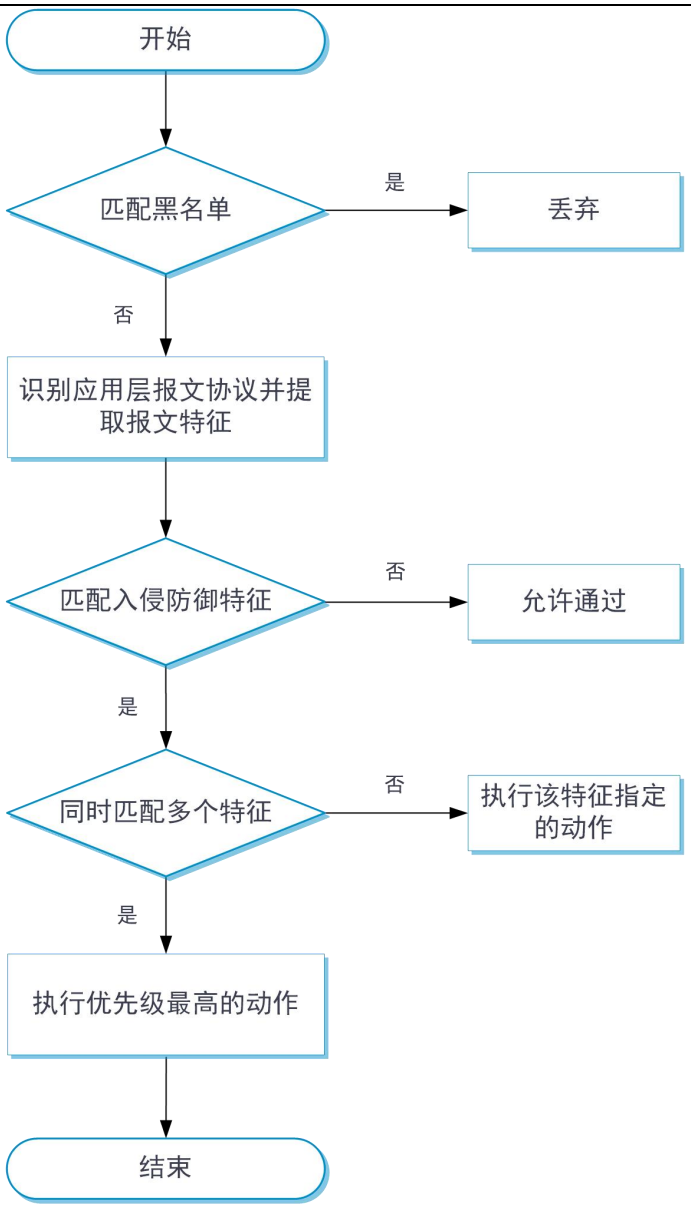
5.4.1.4 入侵防御动作

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“攻击防范联机帮助”。
- 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。

5.4.1.5 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。处理流程如下图所示：



入侵防御处理的整体流程如下：

步骤1　如果报文与IP黑名单匹配成功，则直接丢弃该报文。

步骤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。

步骤3　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。

5.4.2 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。

5.4.3 License支持情况

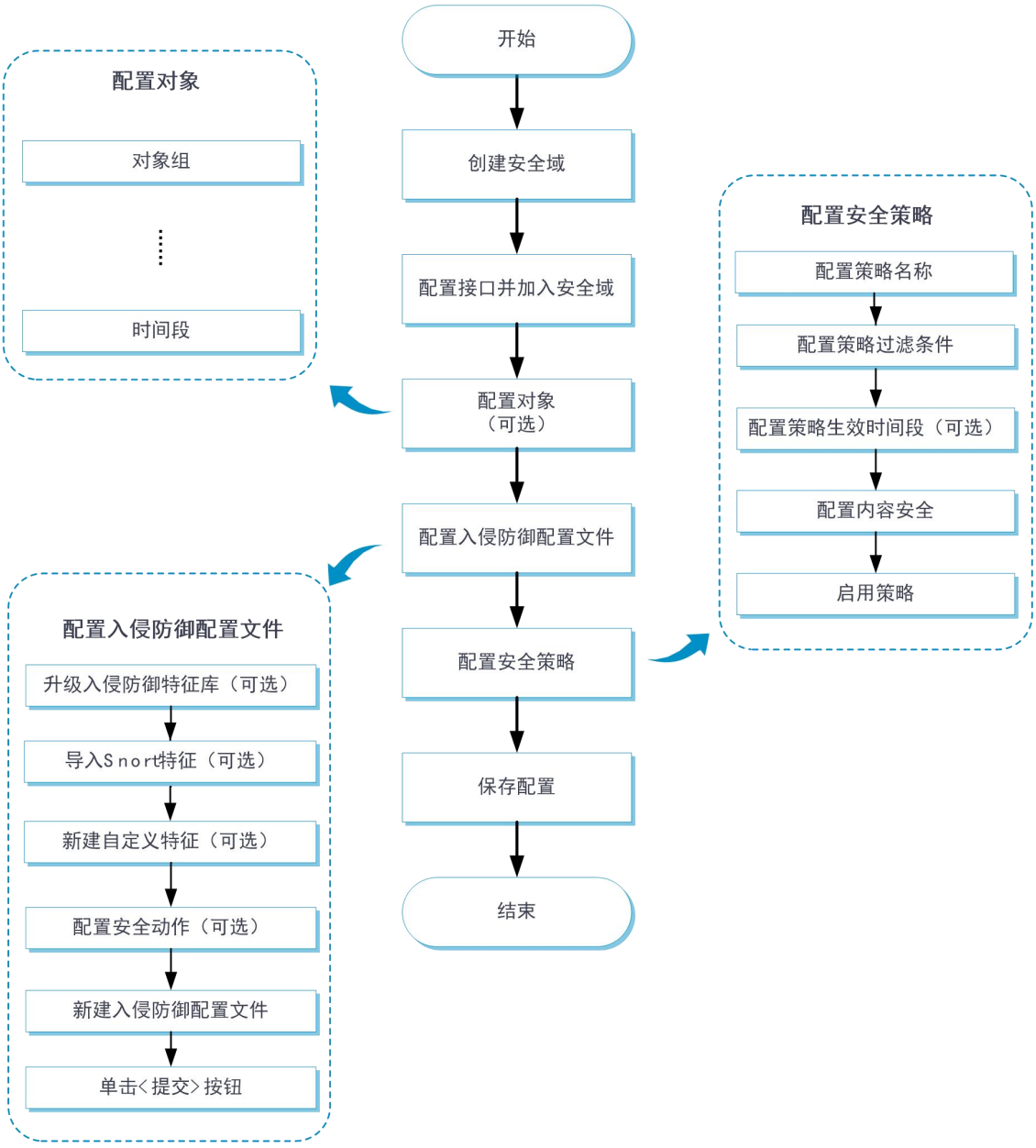
入侵防御功能需要购买并正确安装License后才能使用。License过期后，入侵防御功能可以采用设备中已有的入侵防御特征库正常工作，但无法升级到官方网站在过期时间后发布的新版本的特征库。关于License的详细介绍请参见“License联机帮助”。

5.4.4 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联机帮助”。
- 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。
- 当报文匹配到多条白名单时，仅编号最小的白名单命中统计次数增加。
- 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。

5.4.5 配置指南

入侵防御功能的配置思路如下图所示：



5.4.5.1 配置入侵防御配置文件

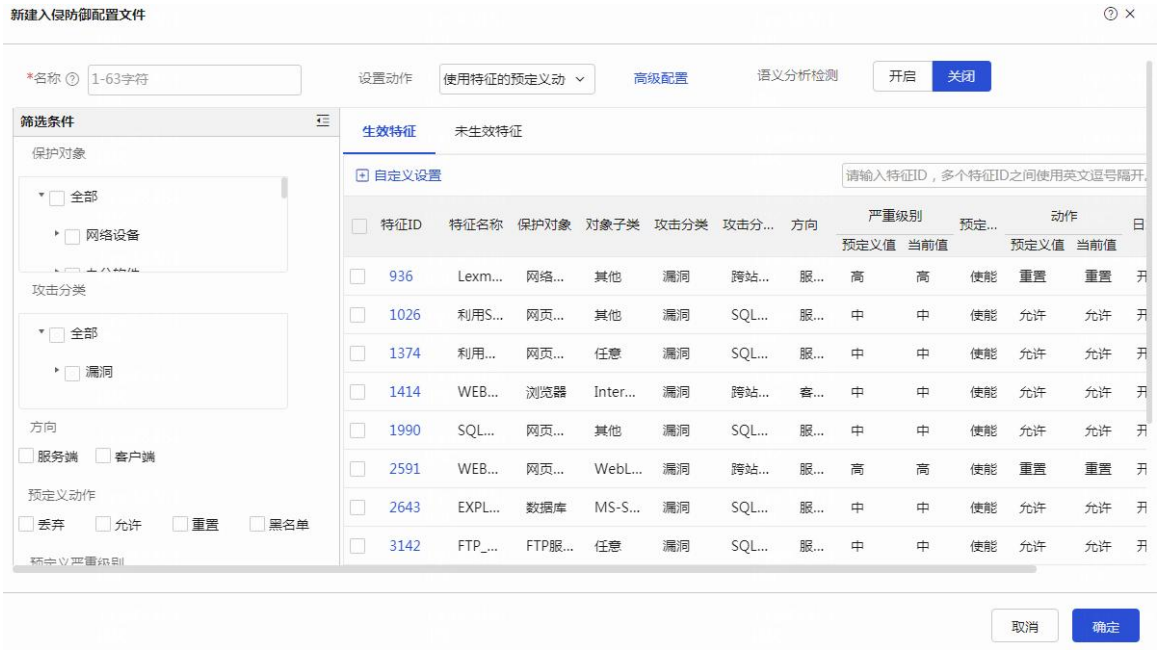
设备上存在一个名称为default的入侵防御配置文件，缺省入侵防御配置文件使用当前系统中所有缺省处于启用状态的入侵防御特征，新增自定义入侵防御特征会自动添加到缺省入侵防御配置文件下。缺省入侵防御配置文件中的入侵防御特征的动作属性和生效状态属性不能被修改。

管理员也可以根据实际需求创建自定义的入侵防御配置文件。

5.4.5.1.1 配置步骤

步骤1　选择“对象 > 安全配置文件> 入侵防御 > 配置文件”。

步骤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。



步骤3　配置入侵防御配置文件的基本参数，具体参数如下所示：

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，否则导出的入侵防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，可以提升该类攻击的识别率
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、重置和重定向。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

步骤4　配置入侵防御特征筛选条件，具体参数如下：

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

参数	说明
	来筛选配置文件所需的入侵防御特征
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，可通过选择不同的预定义动作来筛选配置文件所需的入侵防御特征
严重级别	入侵防御特征的严重级别分为如下四种：严重、高、中、低，可通过选择不同的严重级别来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状态来筛选配置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。

步骤5　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。

步骤6　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。

步骤7　单击<高级配置>按钮，进入高级配置界面，具体配置参数如下：

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，包括： ● 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 > 威胁日志 > 入侵防御日志“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服务器进行配置 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 配置文件将使用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

参数	说明
	配报文。如果希望将其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： 4) 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版本号；否则，直接执行下一步操作 5) 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，配置状态为生效
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

步骤8　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。

步骤9　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“安全策略联机帮助”。

步骤10　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。

步骤11　如需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。

5.4.5.2　导入和删除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：

步骤1　选择“对象 > 安全配置文件 > 入侵防御 > 特征”。

步骤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。

步骤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。

删除Snort特征的配置步骤如下：

步骤4　选择“对象 > 安全配置文件 > 入侵防御 > 特征”。

步骤5　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。

5.4.5.3 新建和删除自定义特征

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：

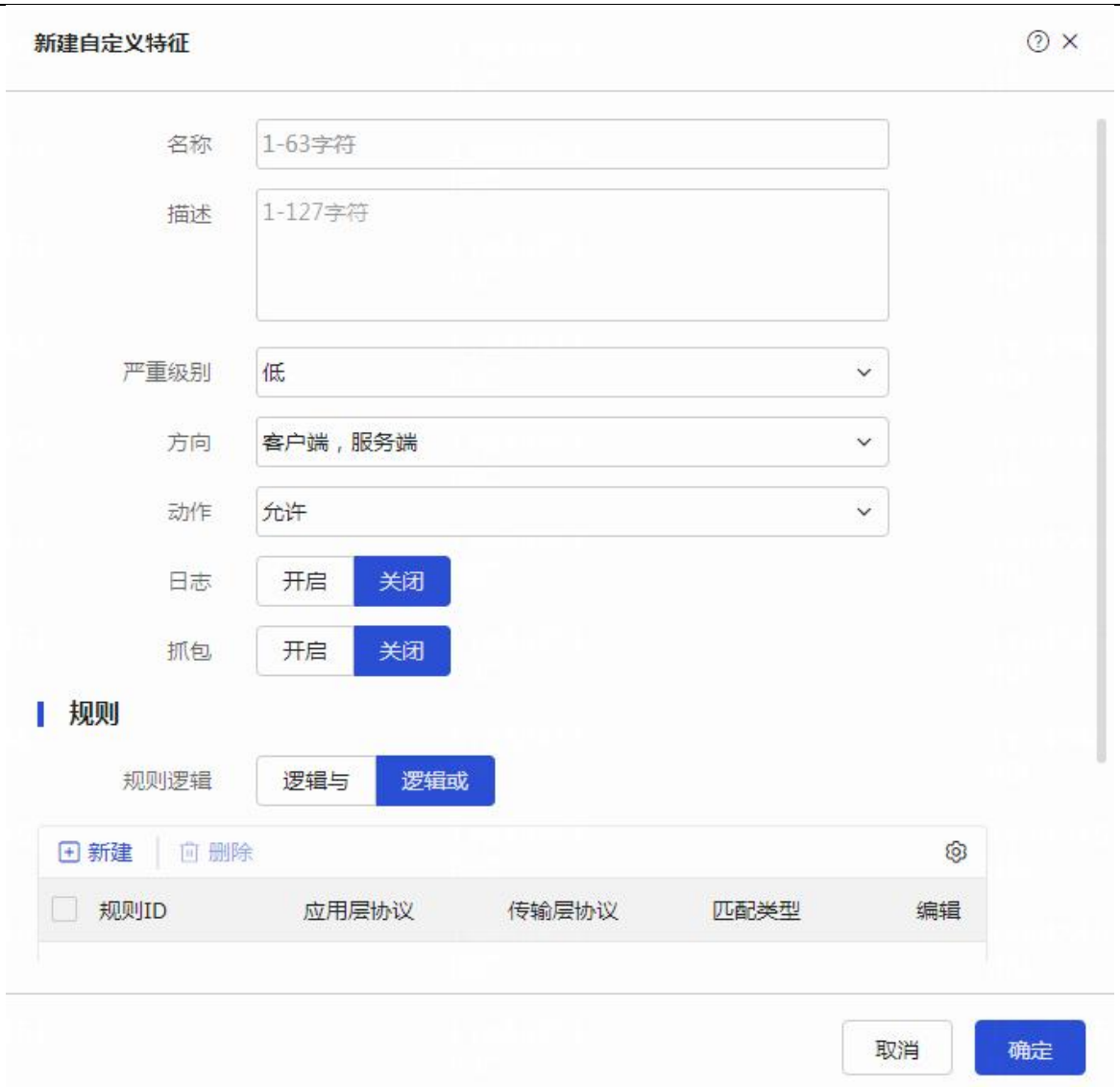
- 关键字类型：配置关键字类型规则时，需要配置检查项和检查项触发条件。只有匹配检查项触发条件后才会继续匹配检查项。仅当所有检查项都匹配成功，才表示该规则成功匹配。
- 数值类型：配置数值类型规则时，可以配置检查项，只有所有检查项都匹配成功，才表示规则成功匹配。

5.4.5.3.1 新建自定义特征

新建自定义特征的配置步骤如下：

步骤1　选择“对象 > 安全配置文件 > 入侵防御 > 特征”。

步骤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。



步骤3　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：

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，有利于后期维护
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。严重级别分为如下四种：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

参数	说明
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，有关捕获参数的详细配置，请参见“安全动作联机帮助”

步骤4　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。

步骤5　单击<新建>按钮，进入新建规则页面，具体配置内容如下：

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

步骤6　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：

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起始检测位置

步骤7　单击<确定>按钮，完成检查项触发条件的配置。

步骤8　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：

参数	说明

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，取值包括： ● 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偏移的长度
相对检测深度	表示当前检查项的检测深度

步骤9　单击<确定>按钮，完成检查项的配置。

步骤10　单击<确定>按钮，完成自定义特征规则的配置。

步骤11　单击<确定>按钮，完成自定义特征的配置。

步骤12　单击<提交>按钮，使新建的自定义特征生效。

5.4.5.3.2　删除自定义特征

删除自定义特征的配置步骤如下：

选择“对象 > 安全配置文件 > 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。

5.4.5.4　导出特征库中所有特征

选择“对象 > 安全配置文件 > 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。

5.4.5.5 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。

5.4.5.5.1 配置步骤

步骤1　选择“对象 > 安全配置文件 > 入侵防御 > 白名单”。

步骤2　在“白名单”页面单击<新建>按钮，进入“新建白名单”页面。

步骤3　新建白名单，具体配置内容如下：

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，有利于后期维护
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功。可在威胁日志中获取 URL，URL 由报文头域和报文首行组成。由字母、数字、“_”、“-”、“:”、“[”、“]”和“.” 开头，例如：111.15.93.166/wnm/get.j
	子串匹配	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。

参数		说明
	URL	可在威胁日志中获取 URL，URL 由报文头域和报文首行组成。由字母、数字、“_”、“-”、“:”、“[”、“]”和“.”开头，例如：111.15.93.166/wnm/get.j
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地址优先匹配真实源IP地址，在没有提取到真实源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地址匹配源IP地址 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，则需要设备开启真实源 IP 地址检测功能（在“对象 > 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

步骤4　单击<确定>按钮，完成白名单的创建。

步骤5　单击<开启白名单功能>按钮，启用白名单功能。

5.4.5.6　配置入侵防御捕获报文时缓存报文数

当入侵防御业务捕获报文时，会缓存数据流中的命中报文及其前后的报文，方便用户分析威胁信息。其中，缓存的报文数量可以根据用户的实际需求进行配置。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。当设备正确安装了硬盘或U盘时，用户可通过单击威胁日志页面中指定日志右侧的<下载>按钮，获取捕获文件。

缓存报文数的具体配置步骤如下：

步骤1　选择“对象 > 安全配置文件 > 入侵防御 > 配置文件”。

步骤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。

步骤3　根据实际需求配置缓存报文数。

步骤4　单击<确定>按钮，完成缓存报文数的配置。

5.5　防病毒

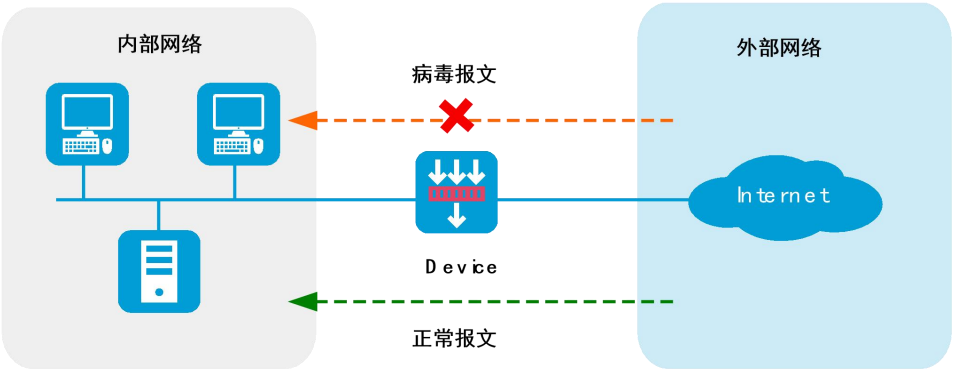
本帮助主要介绍以下内容：

- 特性简介

5.5.1 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。

5.5.1.1 应用场景



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。

5.5.1.2 基本概念

5.5.1.2.1 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。

5.5.1.2.2 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。

5.5.1.2.3 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。

5.5.1.2.4 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。

5.5.1.2.5 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。

5.5.1.2.6 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。

5.5.1.3 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。

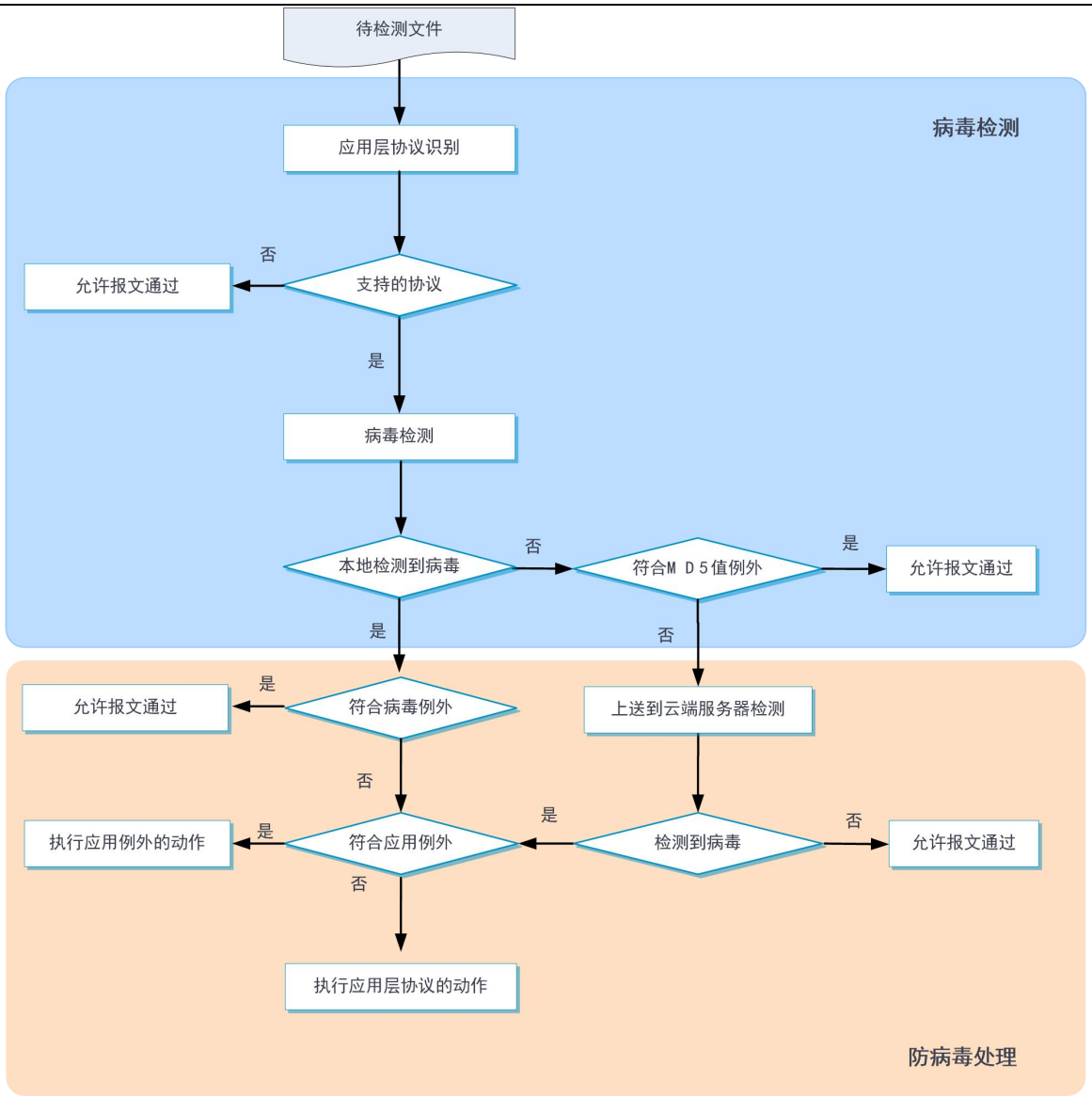
- MD5值匹配：设备首先对待检测文件进行MD5哈希运算，再将计算出的MD5值与特征库中的MD5规则进行匹配，如果匹配成功，则表示该文件携带病毒。

5.5.1.4 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。

5.5.1.5 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下图所示：



防病毒处理的整体流程如下：

步骤1　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。

步骤2　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。

步骤3　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。

步骤4　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。

步骤5　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）。

步骤6　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）。

5.5.2　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。

5.5.3　License支持情况

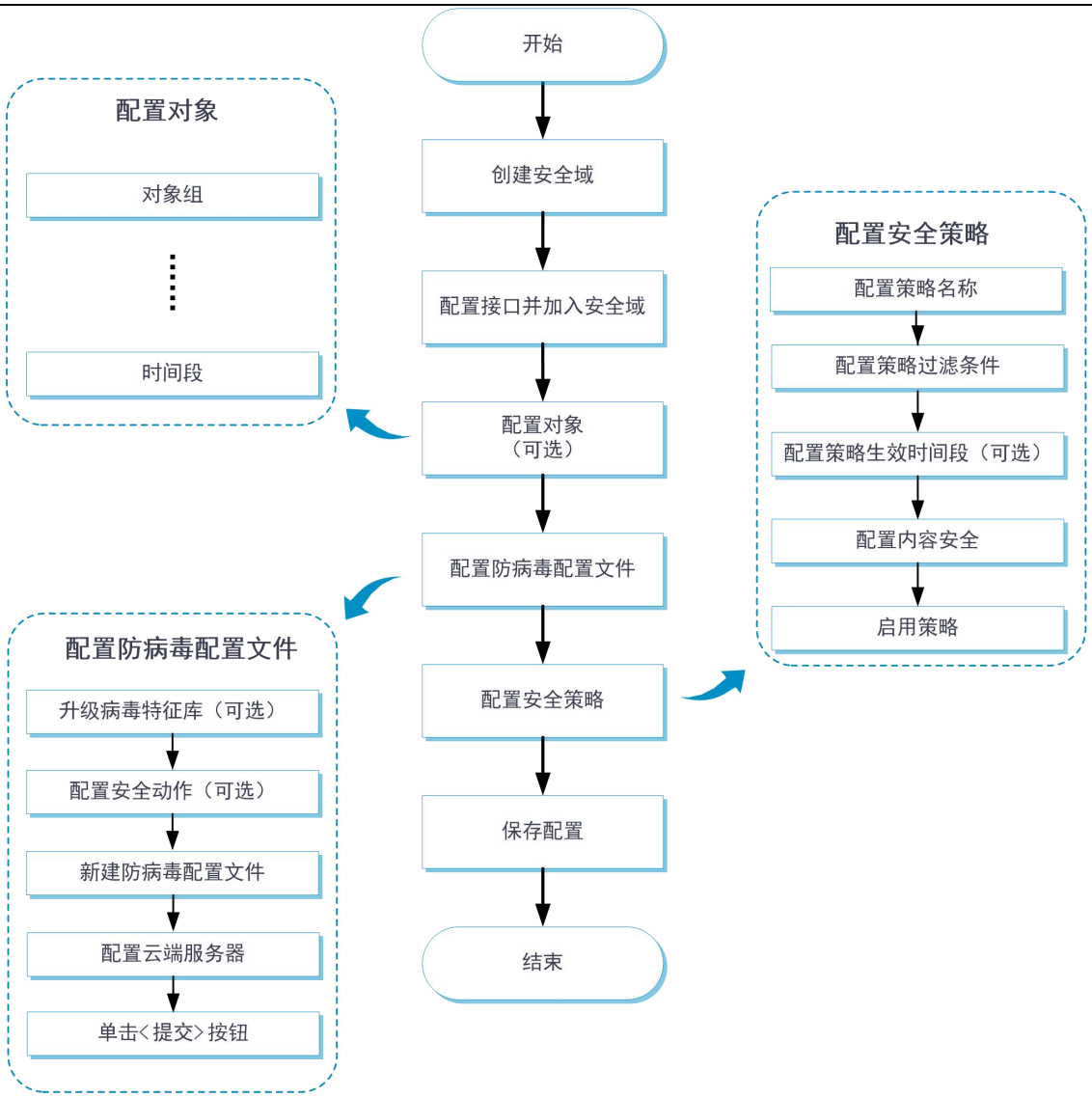
防病毒功能需要购买并正确安装License才能使用。License过期后，防病毒功能可以采用设备中已有的病毒特征库正常工作，但无法升级特征库且云端查询功能以及联动沙箱阻断功能无法使用。关于License的详细介绍请参见“License配置联机帮助”。

5.5.4　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。

5.5.5　配置指南

防病毒功能的配置思路如下图所示：



5.5.5.1 配置防病毒配置文件

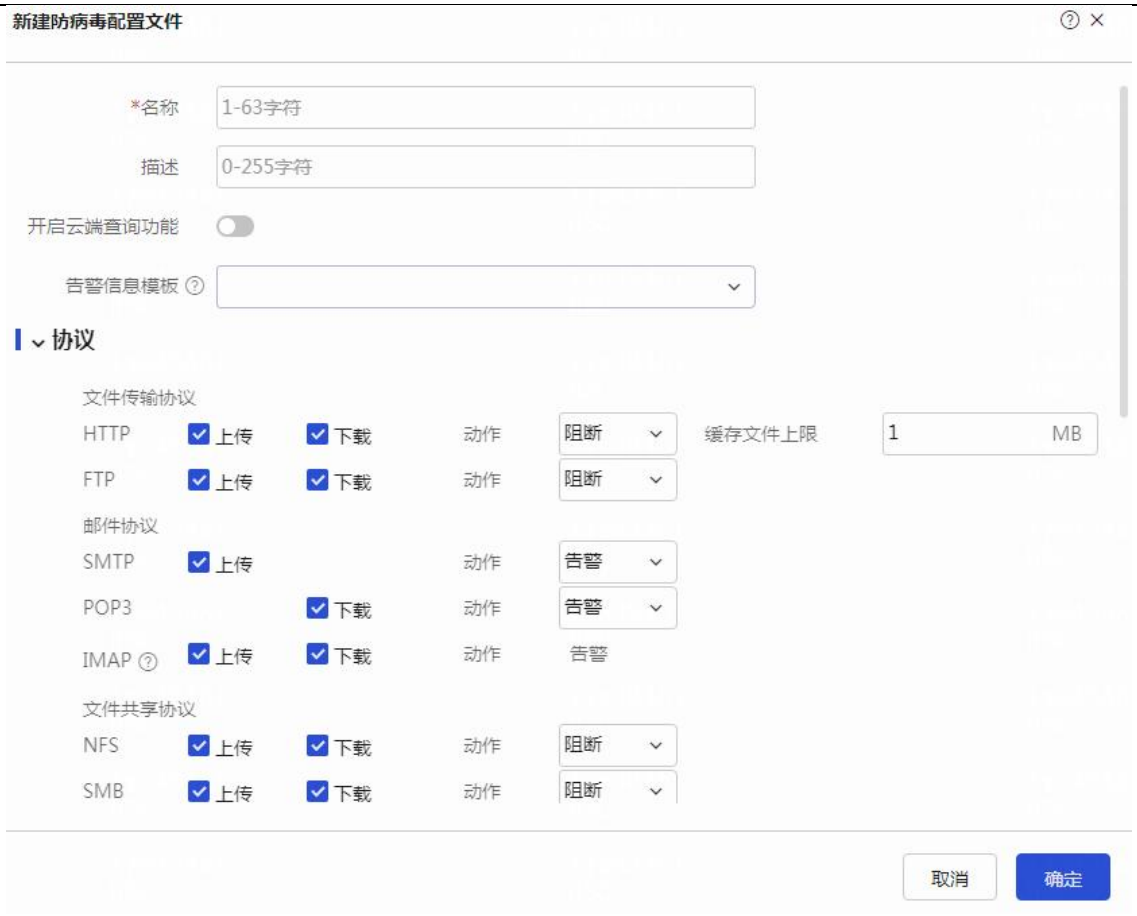
设备上存在一个名称为default的防病毒配置文件，不可对其进行修改和删除操作。管理员可以根据实际需求新建自定义的防病毒配置文件。

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。

5.5.5.1.1 配置步骤

步骤1　选择“对象 > 应用安全 > 防病毒 > 配置文件”。

步骤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。



步骤3　新建防病毒配置文件，具体配置内容如下：

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，有利于后期维护
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 值发往云端服务器进行查询
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。其中，SMTP 协议只支持上传方向
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。

参数	说明
	其中，POP3 协议只支持下载方向
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，如果检测到病毒，则对此报文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。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，这时就可以把所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特征设置为病毒例外。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作
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

步骤4　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。

步骤5　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“安全策略联机帮助”。

步骤6　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。

5.5.5.2　配置云端服务器

云端服务器的具体配置步骤如下：

步骤1　选择“对象 > 应用安全 > 防病毒 > 配置文件”。

步骤2　在“配置文件”页面单击<配置>按钮，进入“配置云端服务器”页面。

步骤3　云端服务器的具体配置内容如下：

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命中列表：

参数	说明
	● 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 缓存不会被删除 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 MD5 缓存，即使该 MD5 缓存未达到最短保留时间，也将被删除

步骤4　单击<确定>按钮，完成云端服务器的配置。

5.5.5.3　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。

步骤1　选择“对象 > 应用安全 > 防病毒 > 病毒家族”。

步骤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。

5.6　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

5.6.1 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）

5.6.1.1 基本概念

5.6.1.1.1 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。

5.6.1.1.2 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。

5.6.1.1.3 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。

5.6.1.2 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：

步骤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。

步骤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。

5.6.2　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。

5.6.3　使用限制和注意事项

5.6.3.1　关于提交操作的注意事项

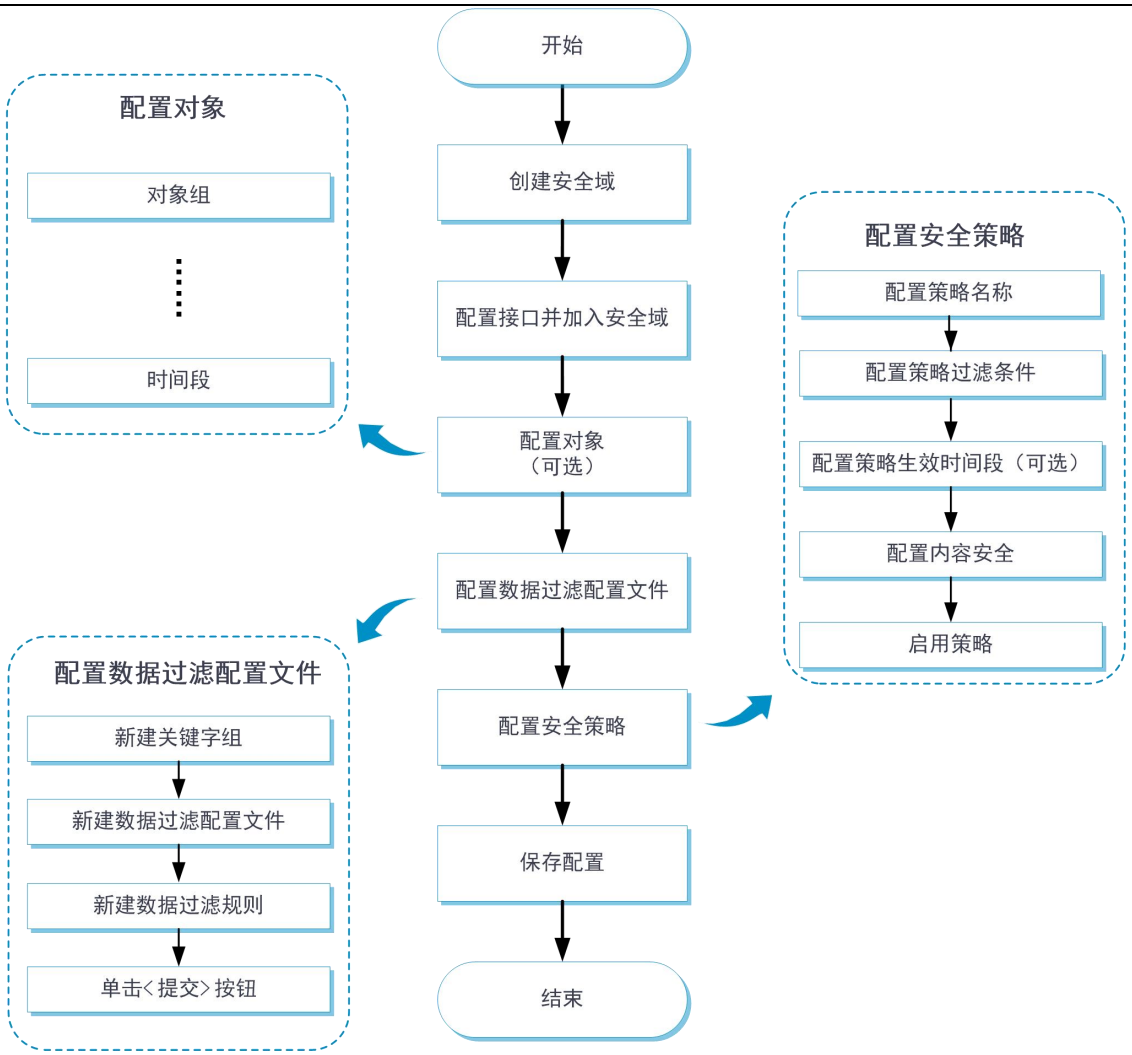
- 执行“提交”操作会暂时中断DPI业务的处理，可能导致其他基于DPI功能的业务同时出现中断。例如，安全策略无法对应用进行访问控制等。
- 执行“提交”操作后，界面上会提示设置成功，但是配置文件此时可能尚未完成激活，如果此时报文经过设备，可能会出现暂时无法识别的情况。

5.6.3.2　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。

5.6.4　配置指南

数据过滤功能的配置思路如下图所示：



5.6.4.1 配置关键字组

步骤1　选择“对象 > 应用安全 > 数据过滤 > 关键字组”。

步骤2　在“关键字组”页面单击<新建>按钮，进入“新建关键字组”页面。

步骤3　新建关键字组，具体配置内容如下：

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

步骤4　在“预定义关键字列表”区域，启用预定义关键字。

步骤5　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。

步骤6　新建关键字，具体配置内容如下：

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

步骤7　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。

步骤8　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。

5.6.4.2　配置数据过滤配置文件

步骤1　选择“对象 > 应用安全 > 数据过滤 > 配置文件”。

步骤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。

步骤3　新建数据过滤配置文件，具体配置内容如下：

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

步骤4　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。

步骤5　新建数据过滤规则，具体配置内容如下：

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、RTMP、SMB 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的报文进行数据过滤
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数据过滤
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进行丢弃
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，对与此规则匹配成功的报文不会生成日志信息

步骤6　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。

步骤7　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。

步骤8　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“安全策略联机帮助”。

步骤9　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。

5.7　URL过滤

本帮助主要介绍以下内容：

- 配置云端服务器
- 配置URL过滤配置文件

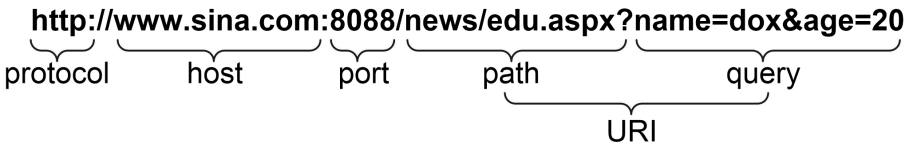
5.7.1 特性简介

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。

5.7.1.1 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”，格式示意如下图所示：



URL各字段含义如下表所示：

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文件地址
[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，每个参数的名和值用“=”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资源名称的字符

5.7.1.2 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。

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。

5.7.1.3 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。

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。

5.7.1.4 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）。

5.7.1.5 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。

5.7.1.6 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。

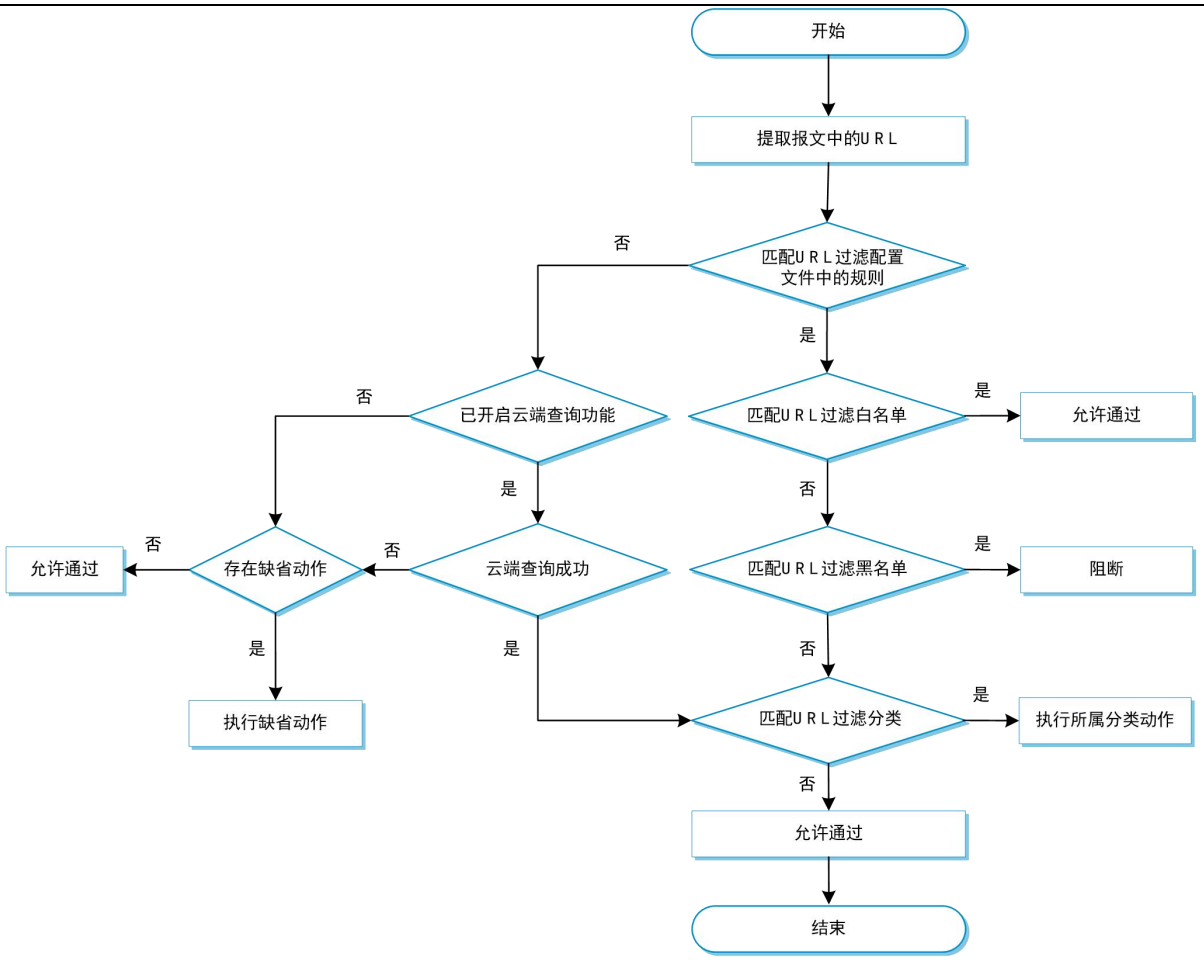
5.7.1.7 URL过滤动作

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“攻击防范联机帮助”。
- 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。

5.7.1.8 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过滤处理流程如下图所示：



URL过滤实现流程如下：

步骤1　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。

步骤2　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：

步骤3　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。

步骤4　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。

步骤5　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。

步骤6　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。

步骤7　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。

5.7.2　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。

5.7.3　使用限制和注意事项

5.7.3.1　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。

5.7.3.2　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。

5.7.3.3 关于正则表达式的使用限制

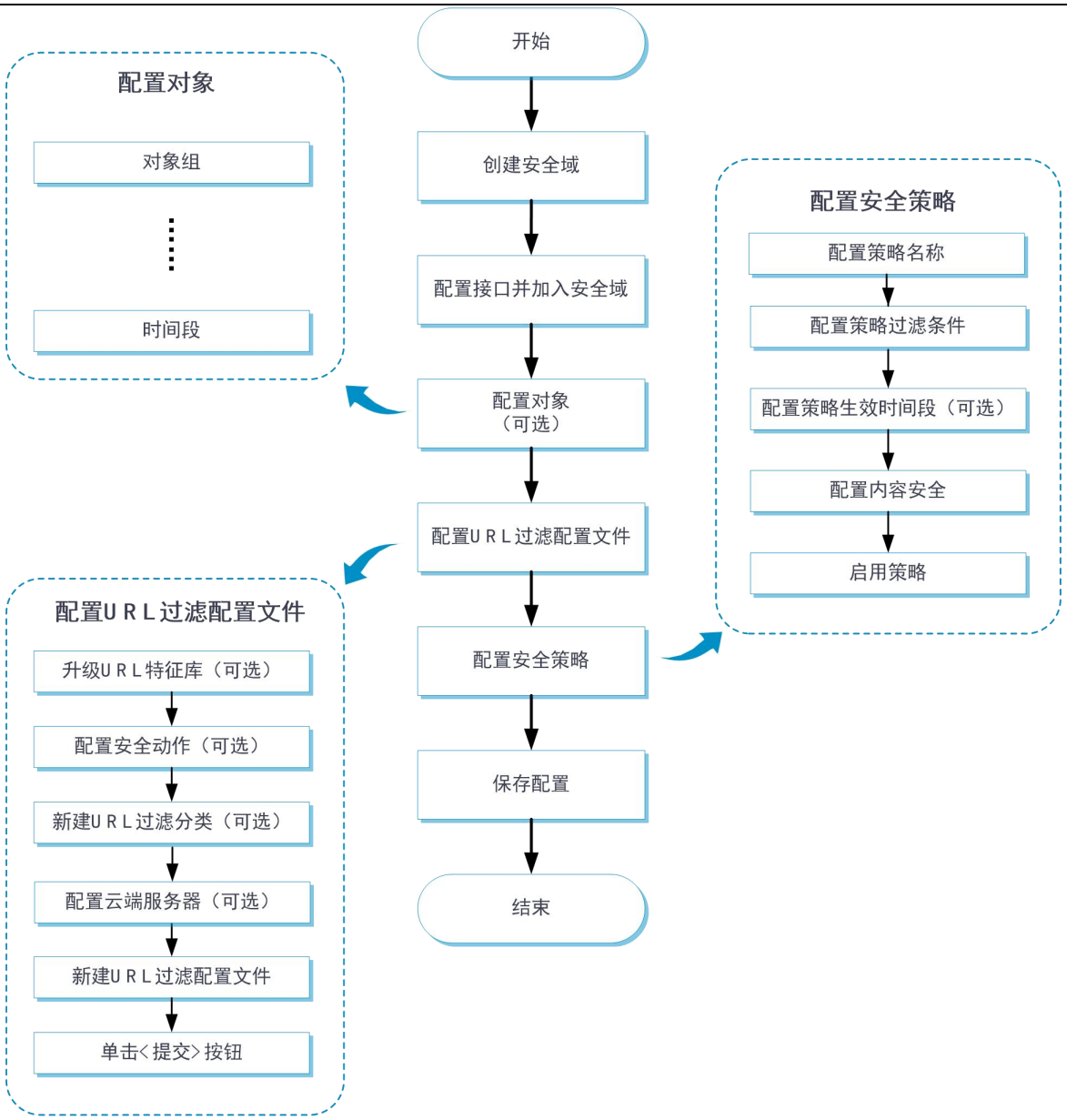
- 正则表达式中，总的分支不能超过四个。例如'abc(c|d|e|\x3D)'有效，'abc(c|onreset|onselect|onchange|style\x3D)'无效。
- 正则表达式中，括号不能嵌套，即括号中不能有括号。例如'ab((abcs*?))'无效。
- 正则表达式中，分支不支持串联，即分支后面不能有分支。例如'ab(a|b)(c|d)^\\r\\n]+?'无效。
- 正则表达式中，零次重复量词'*'和'?'前面必须有四个确定字符。例如'abc*'无效，'abcd*DoS\x2d\d{5}\x20\x2bxi\\r\\nJOIN'有效。

5.7.3.4 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“日志设置基本配置联机帮助”。

5.7.4 配置指南

URL过滤功能的配置思路如下图所示：



5.7.4.1 配置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。

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：

步骤1　选择“对象 > 应用安全 > URL过滤 > URL分类”。

步骤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。

步骤3　新建自定义URL过滤分类，具体配置内容如下：

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，有利于后期维护
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越高，且不同的 URL 过滤分类的严重级别不能相同

参数	说明
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

步骤4　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。

步骤5　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。

步骤6　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。

5.7.4.2　配置云端服务器

云端服务器的具体配置步骤如下：

步骤1　选择“对象 > 应用安全 > URL过滤 > URL分类”。

步骤2　在“URL分类”页面单击<配置>按钮，进入“配置云端服务器”页面。

步骤3　云端服务器的具体配置内容如下：

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 过滤缓存中可以缓存的 URL 条数

参数	说明
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。但是当配置的 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，即使该 URL 未达到最短保留时间，也将被删除

5.7.4.3 配置URL过滤配置文件

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：

步骤1　选择“对象 > 应用安全 > URL过滤 > 配置文件”。

步骤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。

步骤3　新建URL过滤配置文件，具体配置内容如下：

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缺省动作对此报文进行处理。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
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 过滤规则匹配成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“安全动作联机帮助”
开启 HTTPS 流量	开启本功能后，设备可以对未解密的 HTTPS 流量进行 URL 过滤

参数	说明
过滤功能	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，请参见“代理策略联机帮助”
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问
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 URL 过滤分类中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 过滤分类，则根据该规则所属的 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、重置、重定向和记录日志。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 URL 信誉特征库进行匹配，匹配成功则执行 URL 所属攻击类型的动作，如果匹配失败，则放行该报文
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 信誉特征库匹配成功时，则对报文执行 URL 所属攻击类型的动作

步骤4　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。

步骤5　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“安全策略联机帮助”。

步骤6　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。

5.8　文件过滤

本帮助主要介绍以下内容：

- 特性简介

5.8.1 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）

5.8.1.1 基本概念

5.8.1.1.1 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。

5.8.1.1.2 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。

5.8.1.1.3 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。

5.8.1.2 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：

步骤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。

步骤2 设备提取文件的扩展名信息并记录。

步骤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。

步骤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。

5.8.2 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。

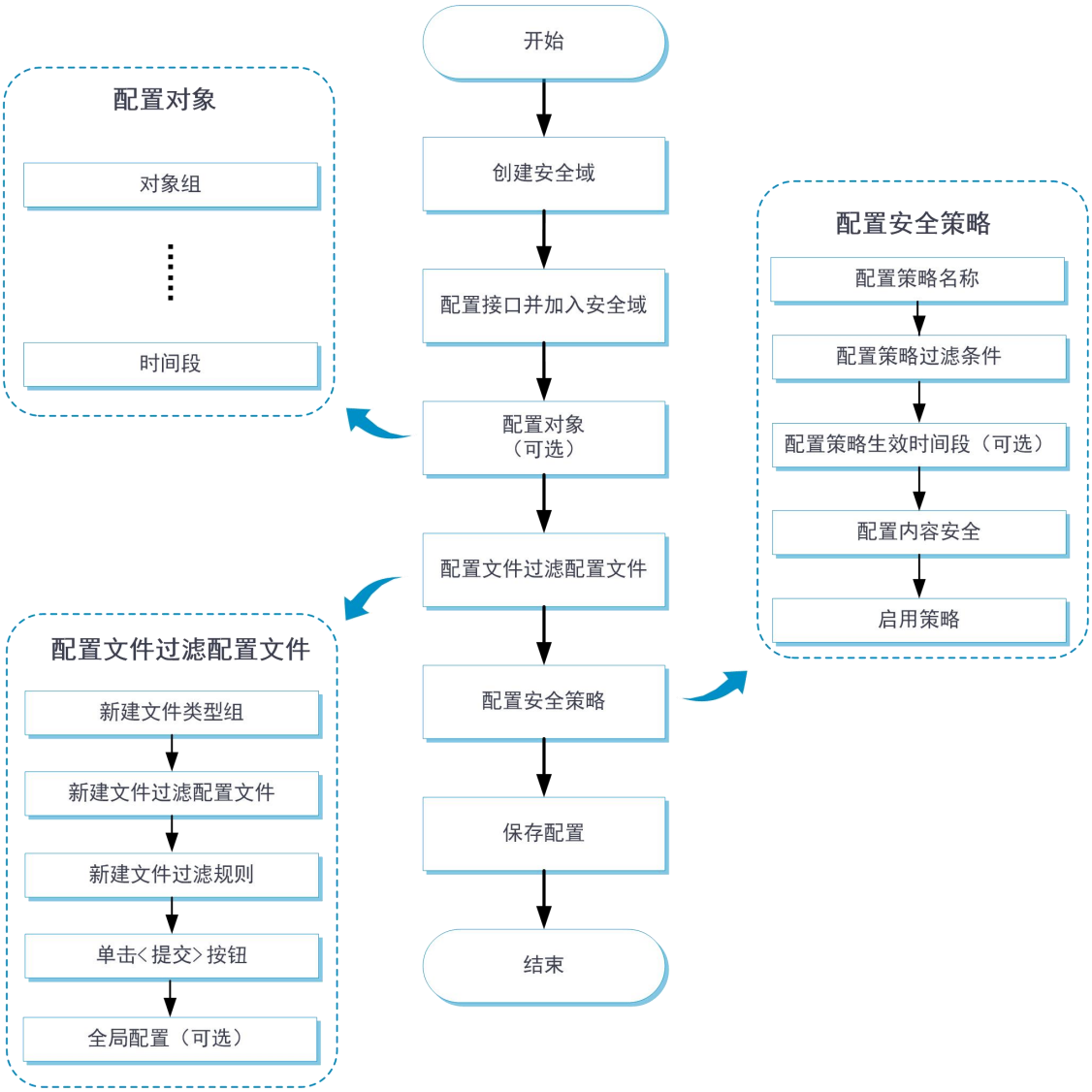
5.8.3 使用限制和注意事项

◆ 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。

5.8.4 配置指南

文件过滤功能的配置思路如下图所示：



5.8.4.1 配置文件类型组

文件类型组的配置步骤如下：

步骤1　选择“对象 > 应用安全 > 文件过滤 > 文件类型组”。

步骤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。

步骤3　新建文件类型组，具体配置内容如下：

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

步骤4　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。

5.8.4.2　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：

步骤1　选择“对象 > 应用安全 > 文件过滤 > 配置文件”。

步骤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。

步骤3　新建文件过滤配置文件，具体配置内容如下：

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

步骤4　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。

步骤5　新建文件过滤规则，具体配置内容如下：

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、RTMP、SMB 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的报文进行文件过滤
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文件过滤
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进行丢弃
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，对与此规则匹配成功的报文不会记录日志信息

步骤6　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。

步骤7　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。

步骤8　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“安全策略联机帮助”

步骤9　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。

5.8.4.3　全局配置

全局配置的配置步骤如下：

步骤1　选择“对象 > 应用安全 > 文件过滤 > 配置文件”。

步骤2　选择“全局配置”页签，配置文件扩展名不匹配时动作。

步骤3　单击<应用>按钮，完成配置。

5.9　APT防御

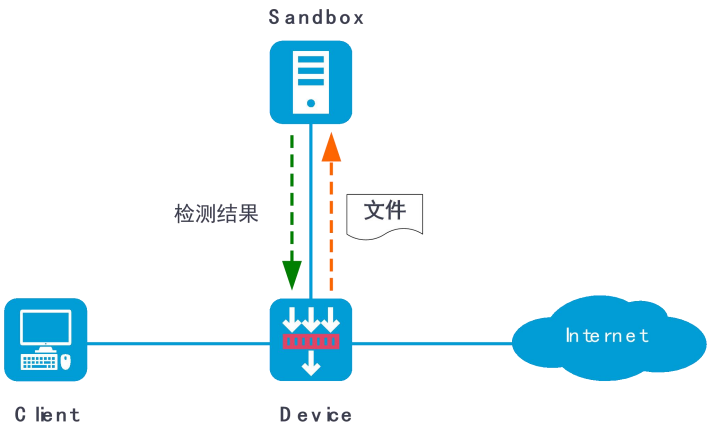
本帮助主要介绍以下内容：

5.9.1 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。

5.9.1.1 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：



步骤1　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。

步骤2　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。

步骤3　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。

步骤4　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。

5.9.1.2 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。

5.9.1.3 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。

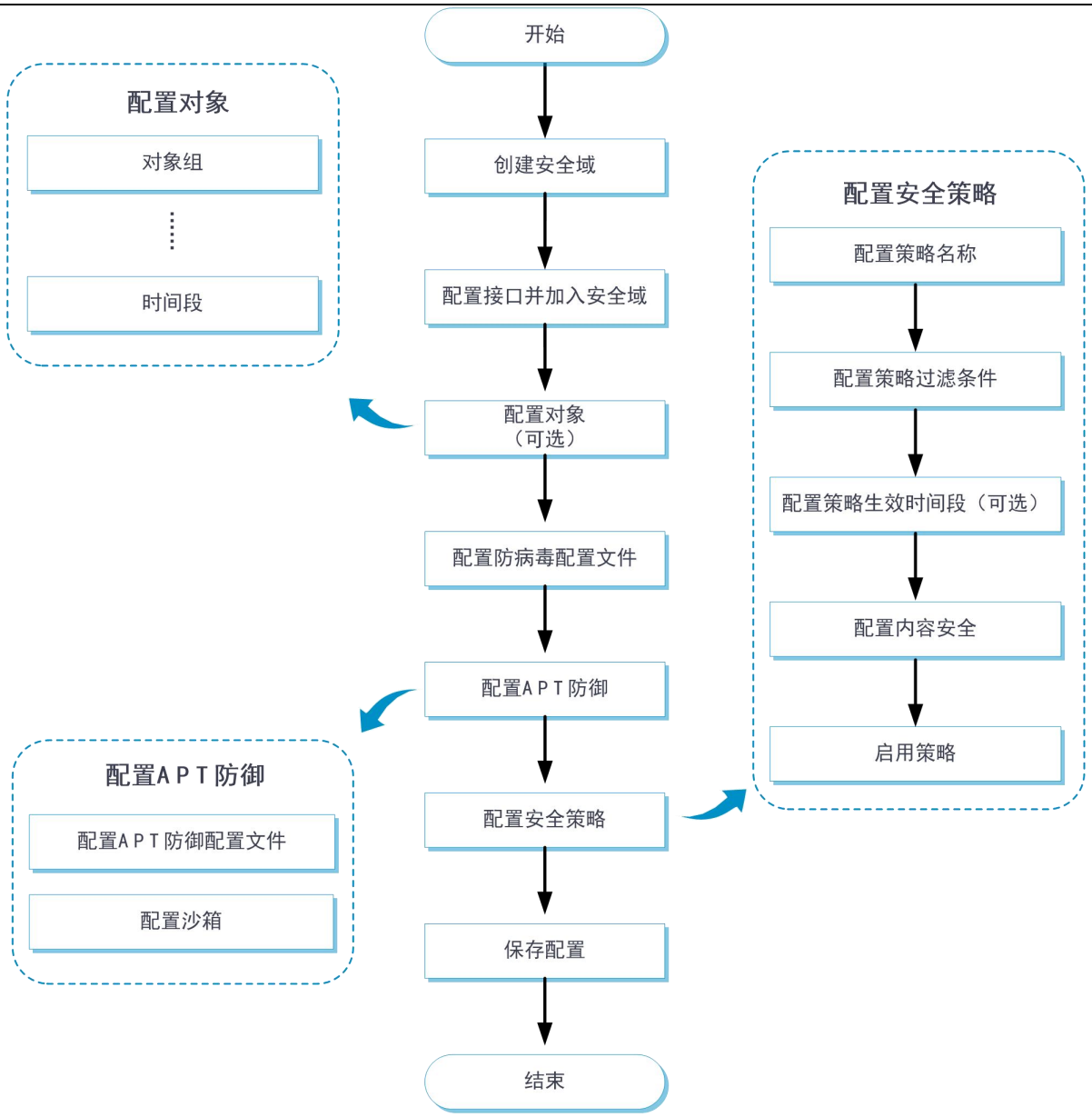
有关防病毒功能的详细介绍，请参见“防病毒联机帮助”。

5.9.2 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。

5.9.3 配置指南

APT防御功能的配置思路如下图所示：



5.9.3.1 配置沙箱

沙箱的具体配置步骤如下：

步骤1 选择“对象 > 应用安全 > APT防御 > 沙箱”。

步骤2　沙箱的具体配置内容如下：

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

参数	说明
	● 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

步骤3　单击<应用>按钮，完成沙箱的配置。

5.9.3.2　配置APT防御配置文件

APT防御配置文件的配置步骤如下

步骤1　选择“对象 > 应用安全 > APT防御 > 配置文件”。

步骤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。

步骤3　新建APT防御配置文件，具体配置内容如下：

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，有利于后期维护
应用	APT 防御检测的应用层协议类型

参数	说明
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

步骤4　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。

步骤5　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“安全策略联机帮助”。

5.10　应用识别

本帮助主要介绍以下内容：

5.10.1　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。

5.10.1.1 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。

5.10.1.2 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。

5.10.1.3 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。

5.10.2 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。

5.10.3 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联机帮助”。

5.10.4 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。

5.10.5 配置指南

5.10.5.1 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。

5.10.5.1.1 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。

5.10.5.1.2 新增PBAR类型应用步骤

步骤1 选择“对象 > 应用安全 > 应用识别 > 应用”。

步骤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。

步骤3 在端口映射区域，单击<新建>按钮，进入“添加端口映射”页面。

步骤4　新建端口映射关系，具体配置内容如下：

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 Congestion Control Protocol，数据报拥塞控制协议）、SCTP（Stream Control Transmission Protocol，流控制传输协议）、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报文均被识别为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 IPv4 网段的主机端口映射、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 IPv6 网段的主机端口映射和基于 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，匹配方式为基于网段的主机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为 ACL
VRF 实例	指定主机所属的 VPN

步骤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。

步骤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。

5.10.5.1.3 修改预定义应用步骤

步骤1 选择“对象 > 应用安全 > 应用识别 > 应用”。

步骤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。

步骤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。

5.10.5.2 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。

步骤1 选择“对象 > 应用安全 > 应用识别 > 应用组”。

步骤2 在“应用组”页面单击<新建>按钮，进入“新建应用组”页面。

步骤3 新建应用组，具体配置内容如下：

参数	说明

参数	说明
应用组名称	表示应用组的名称
描述	通过合理编写描述信息，便于管理员快速理解和识别该应用组的作用，有利于后期维护
类别	通过筛选类别，可以快速选择所需的应用
风险类型	通过筛选风险类型，可以快速选择属于某个风险类型的应用
风险级别	通过筛选风险级别，可以快速选择属于某个风险级别的应用
筛选	“可选应用”栏中所显示的内容是通过“类别”、“风险类型”和“风险级别“筛选出的应用。可单击右侧的<全部选择>或者<选择>按钮，将所需的应用筛选到<已选应用>栏中

步骤4　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。

5.11　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
  - 配置终端组
  - 配置终端识别对象组
  - 配置终端识别白名单

5.11.1　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。

5.11.1.1 基本概念

5.11.1.1.1 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 > 应用安全 > 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。

5.11.1.1.2 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。

5.11.1.1.3 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。

5.11.1.1.4 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。

5.11.1.2 工作模式

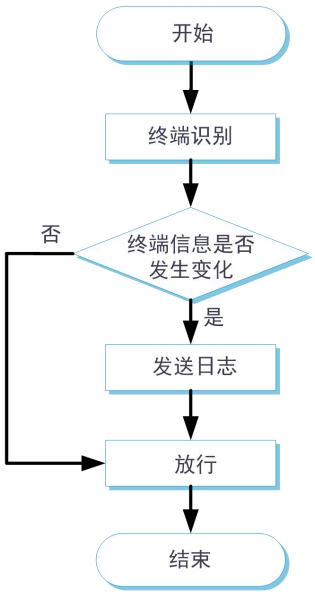
终端识别支持如下工作模式：

- 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。

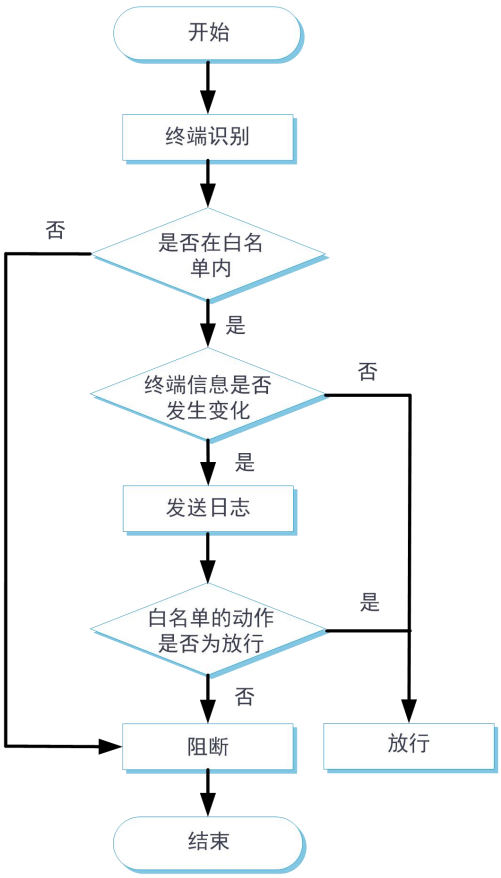
选择“对象 > 应用安全 > 终端识别 > 终端”，进入终端页面。在终端页面，单击<工作模式>按钮，在弹出的工作模式页面上，选择相应的工作模式。

5.11.1.3 工作流程

告警模式工作流程图



白名单模式工作流程图



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。

5.11.2 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。

5.11.3 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”。

5.11.4 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。

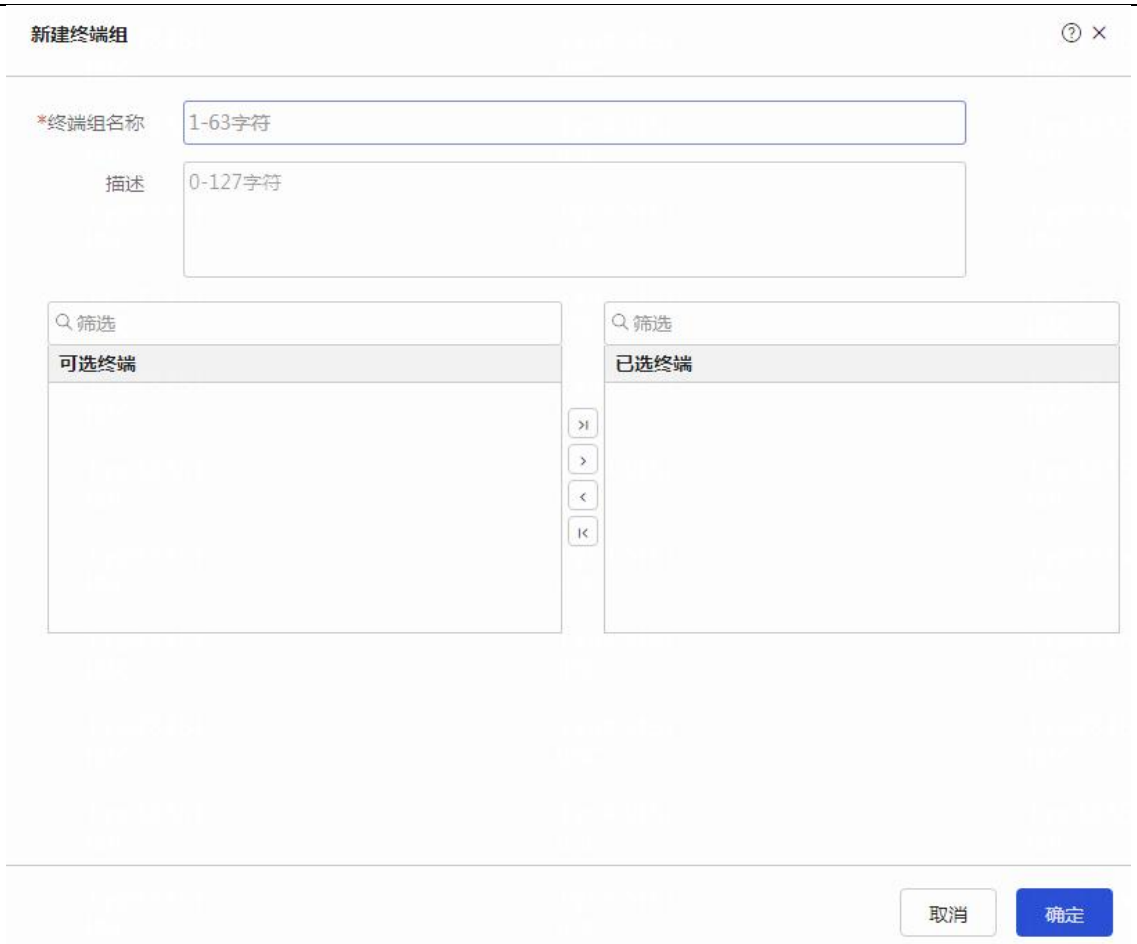
5.11.5 配置指南

5.11.5.1 配置终端组

配置终端组的具体步骤如下：

步骤1 选择“对象 > 应用安全 > 终端识别 > 终端组”，进入终端组页面。

步骤2 单击<新建>按钮，进入新建终端组页面。



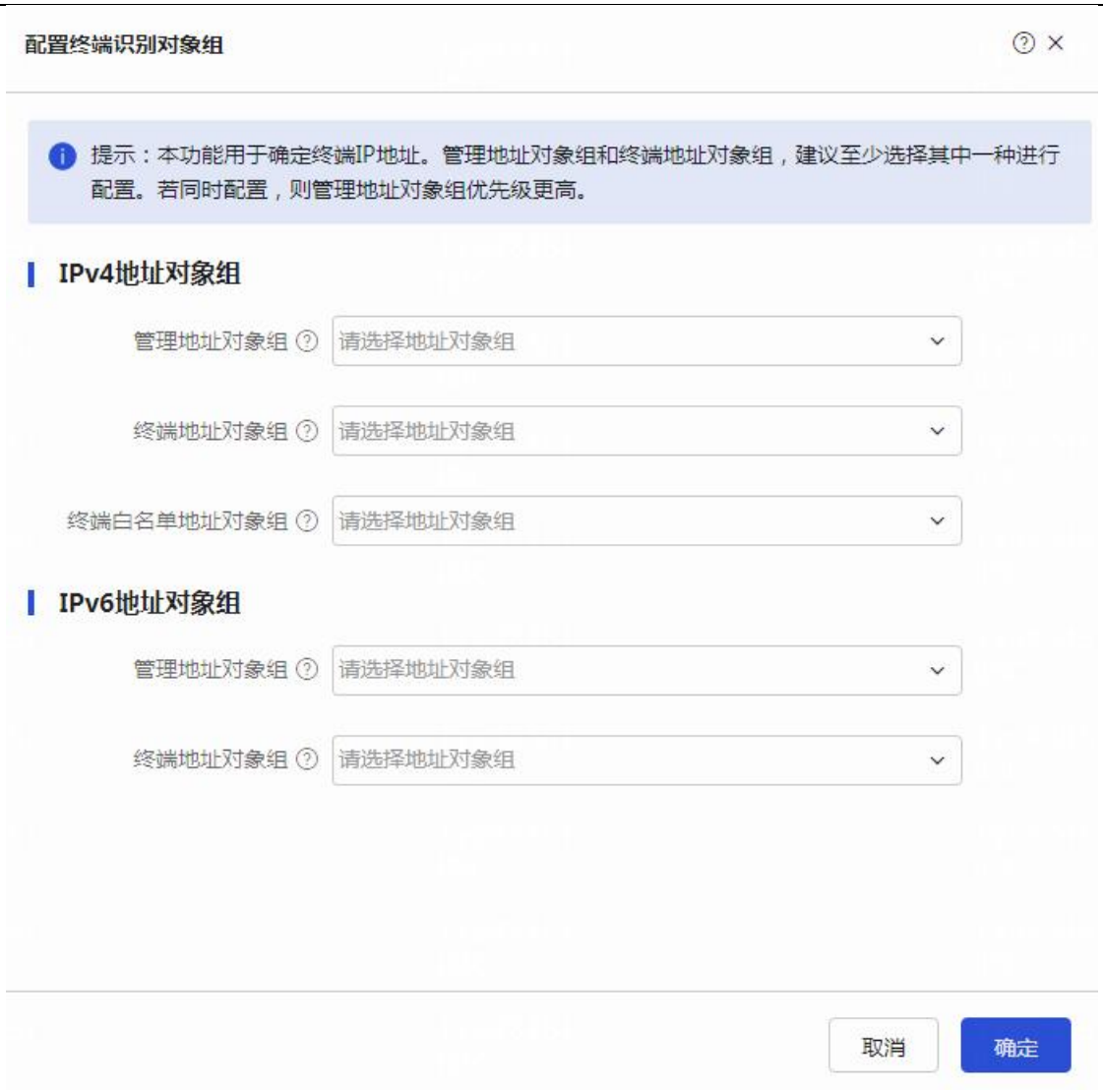
步骤3　在左侧可选终端列表中选择指定的终端，单击右侧的<选择>按钮，将终端加入终端组。

5.11.5.2　配置终端识别对象组

配置终端识别对象组的具体步骤如下：

步骤1　选择“对象 > 应用安全 > 终端识别 > 终端”，进入终端页面。

步骤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。



步骤3　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。

5.11.5.3　配置终端识别白名单

配置终端识别白名单的具体步骤如下：

步骤1　选择“对象 > 应用安全 > 终端识别 > 终端”，进入终端页面。

步骤2　单击<工作模式>按钮，进入工作模式配置页面。

步骤3　选择白名单工作模式，并配置白名单的动作。

步骤4　单击<确定>按钮，返回到终端页面。

步骤5　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。

步骤6　配置终端白名单地址对象组。

5.12　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
  - 阻断
  - 重定向
  - 捕获
  - 告警

5.12.1　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UL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。

5.12.2 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。

5.12.3 使用限制和注意事项

- 当设备检测到硬盘/U盘在位时，会直接将IPS捕获文件保存到硬盘/U盘中，而不会上送到指定的URL。
- 当设备检测到云平台已开启捕获文件上送功能时，会直接通过HTTPS协议将IPS捕获文件上送到云平台，而不会上送到指定的URL。
- 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”。

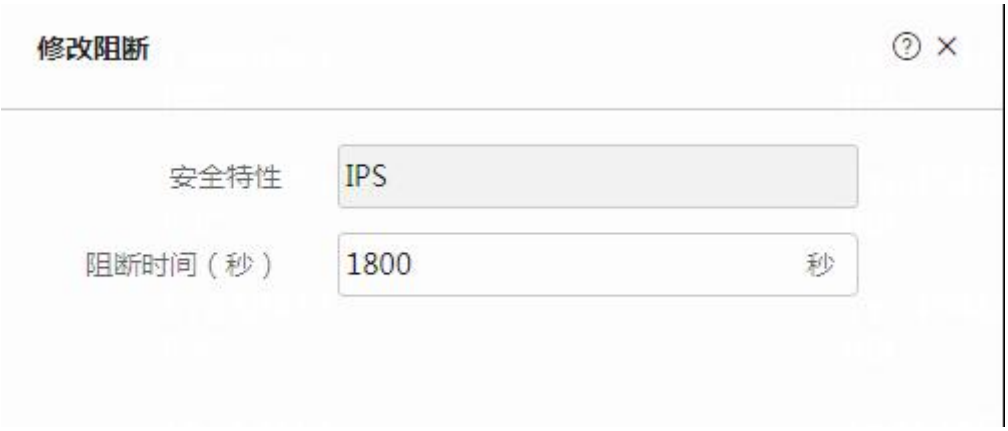
5.12.4 配置指南

5.12.4.1 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：

步骤1　单击指定安全特性右侧的<编辑>按钮，进入修改阻断页面。



步骤2　根据实际需求配置阻断时间。

步骤3　单击<确定>按钮，完成配置。

步骤4　单击<恢复缺省>按钮，可将阻断时间恢复为缺省值。

5.12.4.2　重定向

重定向动作参数的具体配置步骤如下：

步骤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。

步骤2　根据实际需求配置URL，以http://或https://开头。

步骤3　单击<确定>按钮，完成配置。

5.12.4.3　捕获

当入侵防御或Web应用防护业务执行捕获动作后，设备会对捕获到的报文进行缓存，当达到配置的最大捕获字节数或者定时上传时间后，设备将上传本地缓存的捕获报文到指定URL，并清空本地缓存文件。

捕获动作参数的具体配置步骤如下：

步骤1　单击指定安全特性右侧的<编辑>按钮，进入修改捕获页面。

步骤2　根据实际需求配置捕获动作参数，具体配置内容如下：

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 URL 上，并清空本地缓存，然后重新开始捕获报文 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 URL 上
上传 URL	捕获文件的上送地址，格式为 ftp://username:password@server 或者 tftp://server 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，但是会上传失败，本地缓存的捕获文件也会被清空
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，并清空本地缓存

步骤3　单击<确定>按钮，完成配置。

步骤4　单击<恢复缺省>按钮，捕获动作参数将全部恢复为缺省值。

5.12.4.4 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：

步骤1 单击<新建>按钮，进入新建告警信息模板页面。

步骤2 配置模板的名称，并选择指定的安全特性。

步骤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。

步骤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。

步骤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。

步骤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。

步骤7 单击<选择文件>按钮，导入保存后的告警信息模板文件。

步骤8 单击<确定>按钮，完成告警信息的导入。

步骤9 单击<确定>按钮，完成告警信息模板的配置。

步骤10 单击<确定>按钮，完成告警信息的导入。

5.13 高级配置

本帮助主要介绍以下内容：

- 特性简介
  - Bypass

5.13.1 特性简介

5.13.1.1 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。

5.13.1.2 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。

5.13.1.3 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。

5.13.1.4 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。

5.13.1.4.1 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。

5.13.1.4.2 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。

5.13.1.4.3 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。

5.13.1.4.4 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。

- 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。

5.13.1.5 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。

5.13.1.6 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。

5.13.1.7 业务地址范围配置

当用户需要对内网中的OA服务器、网络设备等业务主机的流量进行统计分析时，需要指定主机的地址范围。若未配置业务主机地址，设备将认为不存在业务主机，无法对业务主机流量进行分析。

5.13.2 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。

5.13.3 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。

5.14 对象组

本帮助主要介绍以下内容：

5.14.1 特性简介

5.14.1.1 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。

5.14.1.2 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。

5.14.1.3 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。

5.14.1.3.1 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。

5.14.1.3.2 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。

5.14.2 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。
- 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。
- 地区中的手动添加的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。

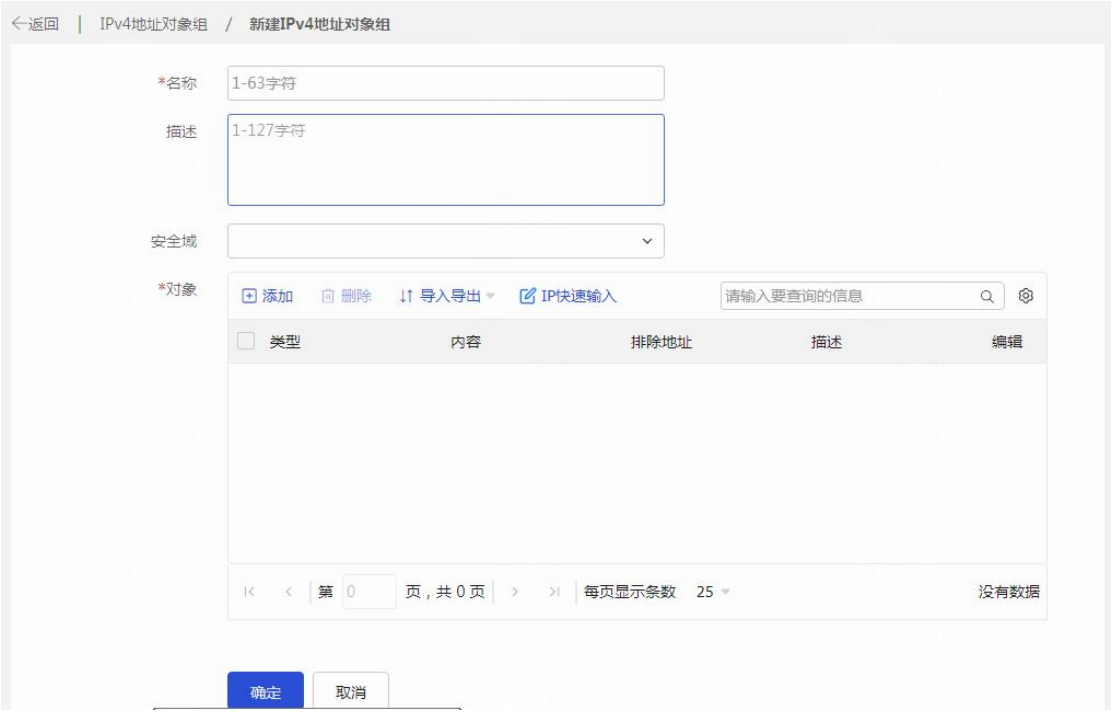
◆ 地区组最大嵌套层次为3层，譬如地区组1、2分别引用地区组2、3，则地区组3不能再引用其他地区组，地区组1也不能再被其他地区组引用。

5.14.3 配置指南

5.14.3.1 IPv4地址对象组配置

步骤1 单击“对象 > 对象组 > IPv4地址对象组”。

步骤2 在“IPv4地址对象组”页面单击<新建>按钮。



步骤3 新建IPv4地址对象组。

参数	说明
对象组名称	对象组的名称，为 1～63 个字符的字符串，不区分大小写，且对象组的名称必须全局唯一
描述	对象组的描述信息，为 1～127 个字符的字符串，区分大小写
安全域	地址对象组所属的安全域

步骤4 单击<添加>按钮，进入添加对象页面，配置参数如下表所示。

参数	说明
对象	添加对象的类型，包括： ● 网段：子网IPv4地址

参数	说明
	● 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、IP 地址范围、IP 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

步骤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。

5.14.3.2　IPv6地址对象组配置

步骤1　单击“对象 > 对象组 > IPv6地址对象组”。

步骤2　在“IPv6地址对象组”页面单击<新建>按钮。

步骤3　新建IPv6地址对象组。

参数	说明
对象组名称	对象组的名称，为 1～63 个字符的字符串，不区分大小写，且对象组的名称必须全局唯一

参数	说明
描述	对象组的描述信息，为 1～127 个字符的字符串，区分大小写
安全域	地址对象组所属的安全域

步骤4　单击<添加>按钮，进入添加对象页面，配置参数如下表所示。

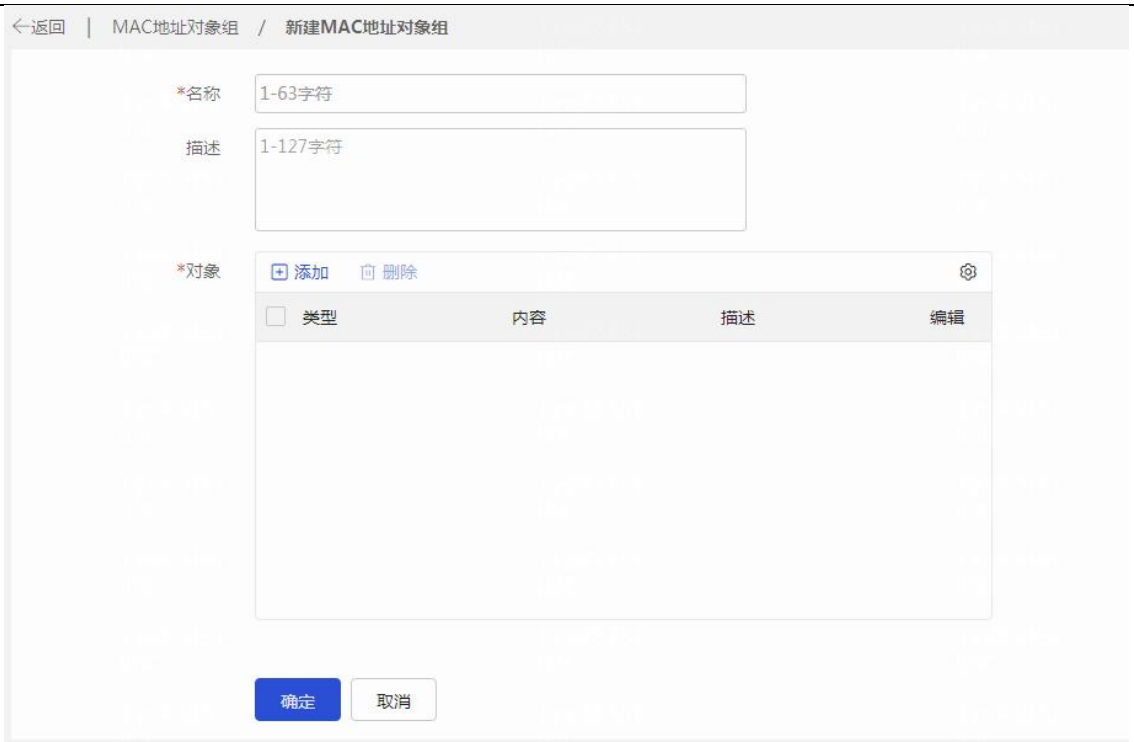
参数	说明
对象	添加对象的类型，包括： ● 网段：子网IPv6地址 ● 对象组：其他IPv6对象组 ● IP地址范围：范围IPv6地址 ● 主机IP地址：主机IPv6地址 ● 主机名：主机名称
排除地址	地址对象中排除的 IPv6 地址，该参数仅在“对象”参数为网段、IP 地址范围时可选
描述	对象的描述信息，为 1～127 个字符的字符串，区分大小写

步骤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。

5.14.3.3　MAC地址对象组配置

步骤1　单击“对象 > 对象组 > MAC地址对象组”。

步骤2　在“MAC地址对象组”页面单击<新建>按钮。



步骤3　新建MAC地址对象组。

参数	说明
对象组名称	对象组的名称，为 1～63 个字符的字符串，不区分大小写，且对象组的名称必须全局唯一
描述	对象组的描述信息，为 1～127 个字符的字符串，区分大小写

步骤4　单击<添加>按钮，进入添加对象页面，配置参数如下表所示。

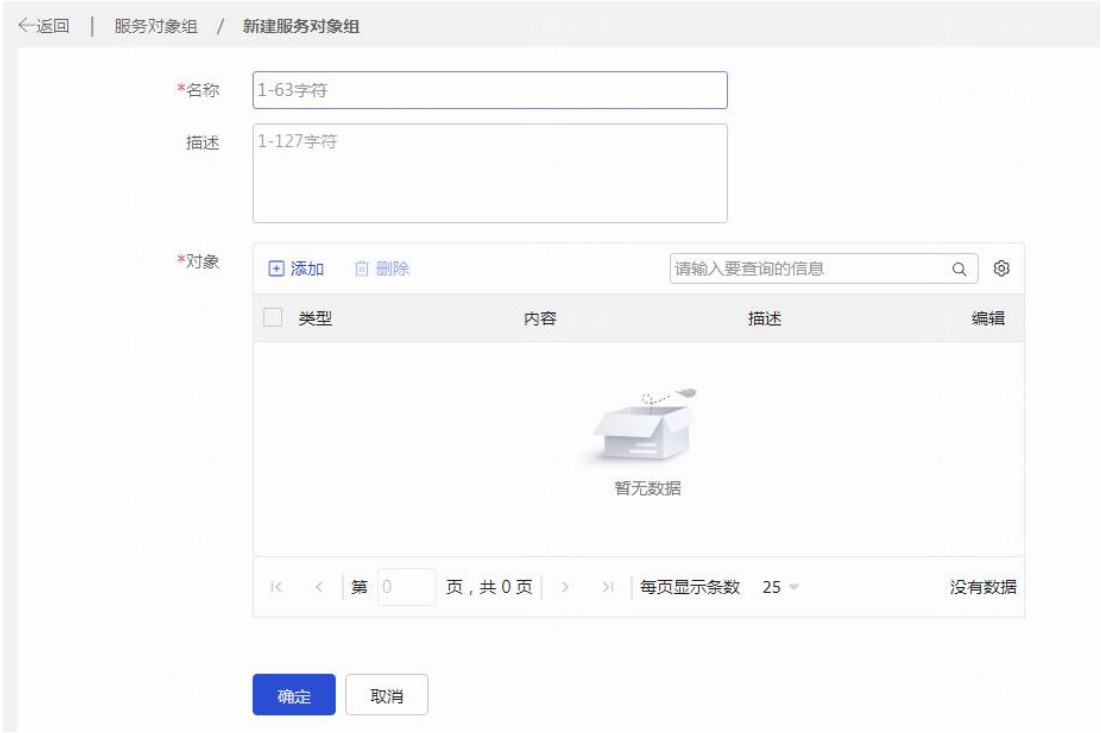
参数	说明
类型	添加对象的类型，包括： ● 对象组：其他MAC地址对象组 ● MAC地址：MAC地址
对象组	指定引用 MAC 地址对象组的名称，为 1～63 字符，不区分大小写，该参数仅在“类型”参数为对象组时可配置
MAC 地址	MAC 地址，格式为 H-H-H，该参数仅在“类型”参数为 MAC 地址时可配置
描述	对象的描述信息，为 1～127 个字符的字符串，区分大小写

步骤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。

5.14.3.4 服务对象组配置

步骤1 单击“对象 > 对象组 > 服务对象组”。

步骤2 在“服务对象组”页面单击<新建>按钮。



步骤3 新建服务对象组。

参数	说明
对象组名称	对象组的名称，为 1～63 个字符的字符串，不区分大小写，且对象组的名称必须全局唯一
描述	对象组的描述信息，为 1～127 个字符的字符串，区分大小写

步骤4 单击<添加>按钮，进入添加对象页面，配置参数如下表所示。

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

参数	说明
	● 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“ICMPv6”时可配置
消息码	ICMP/ICMPv6 消息码，取值范围为 0～255，仅在类型参数为“ICMP”或“ICMPv6”时，且消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“TCP”、“UDP”、“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“TCP”、“UDP”、“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

步骤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。

5.14.3.5　地区配置

5.14.3.5.1　地区配置步骤

步骤1　单击“对象 > 对象组 > 地区”。

步骤2　在“地区””页面单击<新建>按钮。

步骤3　新建地区。

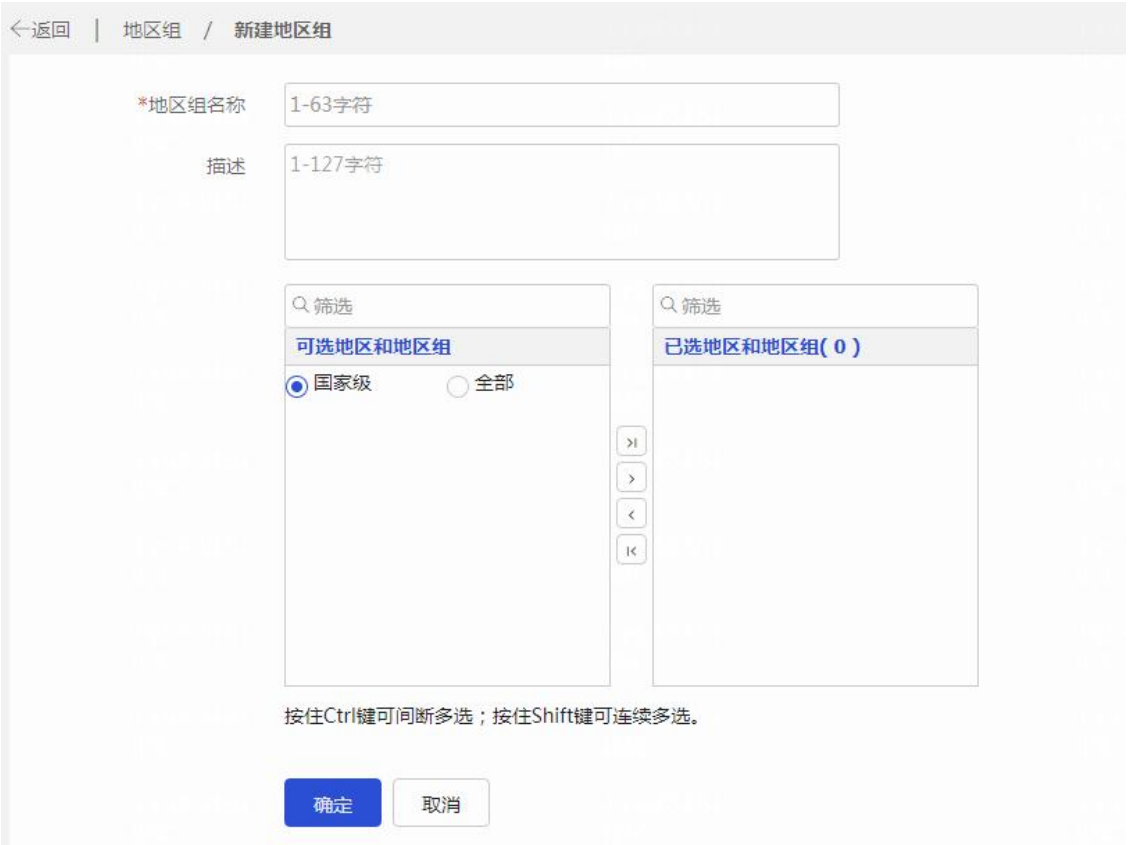
参数	说明
名称	表示地区的名称，为 1～63 个字符的字符串，不区分大小写，不能包含“-”字符
经度	表示地区的经度，取值范围为-180.00～180.00，单位为度。东经为正数，西经为负数
纬度	表示地区的纬度，取值范围为-90.00～90.00，单位为度。北纬为正数，南纬为负数
描述	地区的描述信息，为 1～127 个字符的字符串，区分大小写
IPv4 地址	地区的 IPv4 地址配置可为单个 IP 地址或 IP 地址范围

步骤4　单击<确定>按钮，新建的地区会在“地区”页面显示。

5.14.3.5.2　地区组配置步骤

步骤1　单击“对象 > 对象组 > 地区”。

步骤2　在“地区组”页面单击<新建>按钮。



步骤3　新建地区组。

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，不能包含“-”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

步骤4　单击<确定>按钮，新建的地区组会在“地区组”页面显示。

5.15　ACL

本帮助主要介绍以下内容：

5.15.1 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。

5.15.1.1 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：

ACL类型		编号范围	规则制定依据
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、四层信息制订规则
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、四层信息制订规则
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层信息
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，并将提取出的字符串与用户定义的字符串进行比较，从而找出相匹配的报文

5.15.1.2 ACL规则匹配顺序

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	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，再比较协议范围，指定有 IPv4 承载的协议类型者优先 3) 如果协议范围相同，再比较源 IPv4 地址范围，较小者优先 4) 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 5) 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，较小者优先 6) 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，先配置者优先
IPv6 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 IPv6 地址的范围，较小者（即前缀较长者）优先 3) 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	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，再比较协议范围，指定有 IPv6 承载的协议类型者优先 3) 如果协议范围相同，再比较源 IPv6 地址范围，较小者优先

ACL类型		排序法则
		4) 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 5) 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，较小者优先 6) 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，先配置者优先
二层 ACL		1) 先比较源 MAC 地址范围，较小者（即掩码中"1"位较多者）优先 2) 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 3) 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

5.15.1.3 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。

5.15.2 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。

5.15.3 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。

5.15.4 配置指南

5.15.4.1 新建IPv4 ACL

步骤1 选择“对象 > ACL > IPv4”。

步骤2 在“IPv4”页面单击“新建”按钮。

步骤3 在“新建IPv4 ACL”页面的具体配置内容如下表所示：

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
继续添加规则	没有添加规则的情况下该 ACL 为空，如要配置 IPv4 ACL 的规则就需勾选此按钮。

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

配置项	说明
	选择“1 ICMP”协议后，需配置 ICMP 类型；选择“6 TCP”或“17 UDP”协议后，可配置 TCP/UDP 类型
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DSCP优先级 ● 匹配IP优先级 ● 匹配ToS优先级
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，下拉后点击“+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
继续添加下一条规则	选中前面的复选框，可继续添加并配置下一条 ACL

步骤4　单击“确定”按钮，完成新建IPv4 ACL规则的配置。

5.15.4.2　新建IPv6 ACL

步骤1　选择“对象 > ACL > IPv6”。

步骤2　在“IPv6”页面单击“新建”按钮。

步骤3　在“新建IPv6 ACL”页面的具体配置内容如下表所示：

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
继续添加规则	没有添加规则的情况下该 ACL 为空，如要配置 IPv6 ACL 的规则就需勾选此按钮。

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 选择“1 ICMP”协议后，需配置 ICMP 类型；选择“6 TCP”或“17 UDP”协议后，可配置 TCP/UDP 类型
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 ● 匹配路由头类型

配置项	说明
	● 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
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，下拉后点击“+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
继续添加下一条规则	选中前面的复选框，可继续添加并配置下一条 ACL

步骤4　单击“确定”按钮，完成新建IPv4 ACL规则的配置。

5.15.4.3　新建二层 ACL

步骤1　选择“对象 > ACL > 二层”。

步骤2　在“二层”页面单击“新建”按钮。

步骤3　在“新建二层 ACL”页面的具体配置内容如下表所示：

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

配置项	说明
	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
继续添加规则	没有添加规则的情况下该 ACL 为空，如要配置二层 ACL 的规则就需勾选此按钮。

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，下拉后点击“+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

配置项	说明
继续添加下一条规则	选中前面的复选框，可继续添加并配置下一条 ACL

步骤4　单击“确定”按钮，完成新建二层 ACL规则的配置。

5.16　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

5.16.1　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。

5.16.2 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。

5.16.3 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，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，否则新的配置不生效。

5.16.4 配置指南

5.16.4.1 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。

5.16.4.1.1 配置步骤

新建服务器端策略的具体配置步骤如下：

步骤1　选择“对象 > SSL > 服务器端策略”。

步骤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。

步骤3　在“新建服务器端策略”页面的具体配置内容如下表所示：

参数	说明
策略名称	SSL 服务器端策略的名称
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 域获取服务器端的数字证书
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，用户可以根据实际情况，选择不同类型的加密套件，包括全部、中等强度、高等强度、国密或自定义
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
EMS 扩展项	EMS（Extended Master Secret，扩展主密钥）是一种 SSL 扩展类型，开启本功能后，SSL 协商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	缺省情况下，SSL 服务器与客户端进行 SSL 协商时按照客户端支持的加密套件的顺序来进行匹配，即按照优先级从高到低的顺序，依次选取 SSL 客户端的加密套件，然后从 SSL 服务器端查找与之匹配的加密套件，直到匹配成功
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

步骤4　单击<确定>按钮，完成配置。

5.16.4.2　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。

5.16.4.2.1　配置步骤

新建客户端策略的具体配置步骤如下：

步骤1　选择“对象 > SSL > 客户端策略”。

步骤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。

步骤3　在“新建客户端策略”页面的具体配置内容如下表所示：

参数	说明
策略名称	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
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 域获取客户端的数字证书
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，用户可以根据实际情况，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，开启本功能后，SSL 协商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

步骤4　单击<确定>按钮，完成配置。

5.16.4.3　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。

5.16.4.3.1　配置步骤

步骤1　选择“对象 > SSL > 高级设置”。

步骤2　在“高级设置”页面，具体配置内容如下：

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 协商必须进行完整的 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以关闭 SSL3.0 版本

步骤3　单击<应用>按钮，完成配置。

5.17　公钥管理

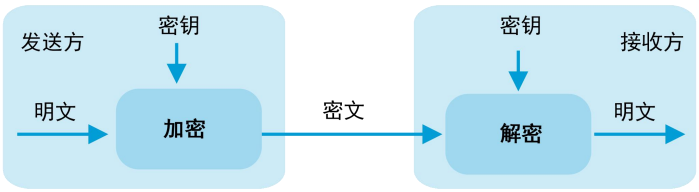
本帮助主要介绍以下内容：

5.17.1　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。

5.17.1.1 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。如下图所示，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。



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）。

5.17.1.2 管理本地非对称密钥对

5.17.1.2.1 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。

5.17.1.2.2 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。

5.17.1.2.3 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。

5.17.1.2.4 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。

5.17.1.3 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。

5.17.2 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。

5.17.3 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。

5.17.4 配置指南

5.17.4.1 配置本地密钥对

5.17.4.1.1 生成本地密钥对

在本地设备上，可以生成RSA、DSA、ECDSA和SM2四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：

步骤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。

步骤2　在“生成本地密钥对”页面的具体配置内容如下表所示：

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 ● SM2
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。创建 SM2 密钥对时，使用固定密钥长度的椭圆曲线
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
存储设备	创建 SM2 密钥对时，可以选择存储设备

步骤3　单击<确定>按钮，完成配置。

5.17.4.1.2　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：

步骤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。

步骤2　在“导入本地密钥对”页面的具体配置内容如下表所示：

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
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

参数	说明
	能成功导入

步骤3　单击<确定>按钮，完成配置。

5.17.4.1.3　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：

步骤1　选择待导出的本地密钥对。

步骤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。

步骤3　在“导出本地密钥”页面的具体配置内容如下表所示：

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 ● SM2
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

步骤4　单击<确定>按钮，完成配置。

5.17.4.1.4　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。

5.17.4.2 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。

5.17.4.2.1 配置步骤

导入远端公钥的具体配置步骤如下：

步骤1　在“远端公钥”页面单击<导入>按钮，进入“导入远端公钥”页面。

步骤2　在“导入远端公钥”页面的具体配置内容如下表所示：

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

步骤3　单击<确定>按钮，完成配置。

5.18 PKI

本帮助主要介绍以下内容：

5.18.1 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。

5.18.1.1 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。

5.18.1.2 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。

5.18.1.2.1 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：

步骤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

步骤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

步骤3 IP地址

5.18.1.2.2 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。

5.18.1.2.3 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。

5.18.1.2.4 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。

5.18.1.3 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。

5.18.1.3.1 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。

5.18.1.3.2 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。

5.18.1.4 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。

5.18.1.4.1 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证书拼接成完成的证书链，则不能导入到设备。

5.18.1.4.2 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。

5.18.1.4.3 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。

5.18.1.5 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。

5.18.2 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。

5.18.3 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。

5.18.4 配置指南

5.18.4.1 配置证书

5.18.4.1.1 配置PKI域

新建PKI域的具体配置步骤如下：

步骤1 在“证书”页面单击<新建>按钮，进入“新建PKI域”页面。

步骤2 在“新建PKI域”页面的具体配置内容如下表所示：

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 ● SM2

步骤3　单击<确定>按钮，完成配置。

5.18.4.1.2　配置导入证书

导入证书的具体配置步骤如下：

步骤1　在“证书”页面单击<导入证书>按钮，进入“导入证书”页面。

步骤2　在“导入证书”页面的具体配置内容如下表所示：

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

步骤3　单击<确定>按钮，完成配置。

5.18.4.1.3　配置提交申请

提交申请的具体配置步骤如下：

步骤1　在“证书”页面单击<提交申请>按钮，进入“提交申请”页面。

步骤2　在“提交申请”页面的具体配置内容如下表所示：

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

步骤3　单击<确定>按钮，完成配置。

5.18.4.2　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

5.18.4.2.1 配置步骤

证书访问策略的具体配置步骤如下：

步骤1 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。

步骤2 在“新建证书访问控制策略”页面，配置策略名称。

步骤3 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。

步骤4 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表所示：

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

步骤5 单击<确定>按钮，完成证书属性配置。

步骤6 单击<确定>按钮，完成规则配置。

步骤7　单击<确定>按钮，完成证书访问策略配置。

5.18.4.3　配置证书主题

新建证书主题的具体配置步骤如下：

步骤1　在“证书主题”页面单击<新建>按钮，进入“新建证书主题”页面。

步骤2　在“新建证书主题”页面的具体配置内容如下表所示：

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

步骤3　单击<确定>按钮，完成配置。

6 网络

6.1 VRF

本帮助主要介绍以下内容：

6.1.1 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。

6.1.2 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。

6.1.3 配置指南

步骤1 单击“网络 > 接口与VRF > VRF”。

步骤2 在VRF页面，点击<新建>按钮。

步骤3 在“VRF”页面的具体配置内容如下表所示：

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订的，会导致不同的 VPN 使用相同的地址域，即地址重叠现象。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 地址成为全局唯一的 VPN-IPv4 地址
路由门限	指定当前 VPN 实例的激活路由前缀的最大数

超过门限后的处理	● 允许新建路由，当VPN实例的激活路由前缀数超过最多支持的激活路由前缀数目时，可以继续激活新的路由前缀，并产生日志信息
	● 不允许新建路由，需要设置告警门限值，当超过门限值和超过最大路由门限时有不同处理方法：
	  ● 当（VPN实例中的激活路由前缀数/最多支持激活路由前缀数×100）达到告警门限值时，产生告警日志信息，但仍然允许激活路由前缀
	  ● 当VPN实例中的激活路由前缀数达到最多支持激活路由前缀数目时，不再激活新的路由前缀

告警门限值	产生告警信息的门限值，单位为百分比，超过门限后的处理为允许继续新建路由时，此功能不支持
关联接口列表	选择当前创建的 VPN 实例关联的接口

步骤4 单击<确定>按钮，新建VRF成功，且会在“VRF”页面中显示。

6.2 接口

本帮助主要介绍以下内容：

- IPv6地址
- 链路聚合
- VLAN终结

◆ 使用限制和注意事项

6.2.1 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：

6.2.1.1 IPv4地址

6.2.1.1.1 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。

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，并且永远不是有效目的地址 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不会输出到链路上，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

6.2.1.1.2 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。

6.2.1.1.3 IPv4地址的配置方式

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。

6.2.1.1.4 接口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，请根据实际组网环境设置合适的接口MTU值，以减少分片的发生。

6.2.1.1.5 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RBM组网下，虚拟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主设备的业务接口，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 Redundancy Protocol，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，不支持在备设备上配置、修改或删除。

6.2.1.2 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。

6.2.1.2.1 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。

6.2.1.2.2 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。

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	::/128	不能分配给任何节点。在节点获得

地址类型		格式前缀（二进制）	IPv6前缀标识	简介
		bits）		有效的 IPv6 地址之前，可在发送的 IPv6 报文的源地址字段填入该地址，但不能作为 IPv6 报文中的目的地址
	环回地址	00...1 （128 bits）	::1/128	不能分配给任何物理接口。它的作用与在 IPv4 中的环回地址相同，即节点用来给自己发送 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中链路本地上节点之间的通信。使用链路本地地址作为源或目的地址的数据报文不会被转发到其他链路上
	全球单播地址	其他形式	-	等同于 IPv4 公网地址，提供给网络服务提供商。这种类型的地址允许路由前缀的聚合，从而限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		-

6.2.1.2.3 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。

6.2.1.2.4 IPv6全球单播地址的配置方法

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地址的前缀需要手工配置，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功能生成的接口标识，自动为接口生成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。

6.2.1.2.5 IPv6链路本地地址的配置方法

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，自动为接口生成链路本地地址；
- 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生成方式。

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，之后手工指定，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，则自动配置不生效，接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址会生效。

6.2.1.2.6 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RBM组网下，虚拟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主设备的业务接口，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 Redundancy Protocol，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，不支持在备设备上配置、修改或删除。

6.2.1.3 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。

6.2.1.3.1 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。

6.2.1.3.2 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”。

6.2.1.3.3 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。

6.2.1.3.4 属性类配置

属性类配置：包含的配置内容如下表所示。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。

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

配置项	内容
	配置

6.2.1.3.5 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。

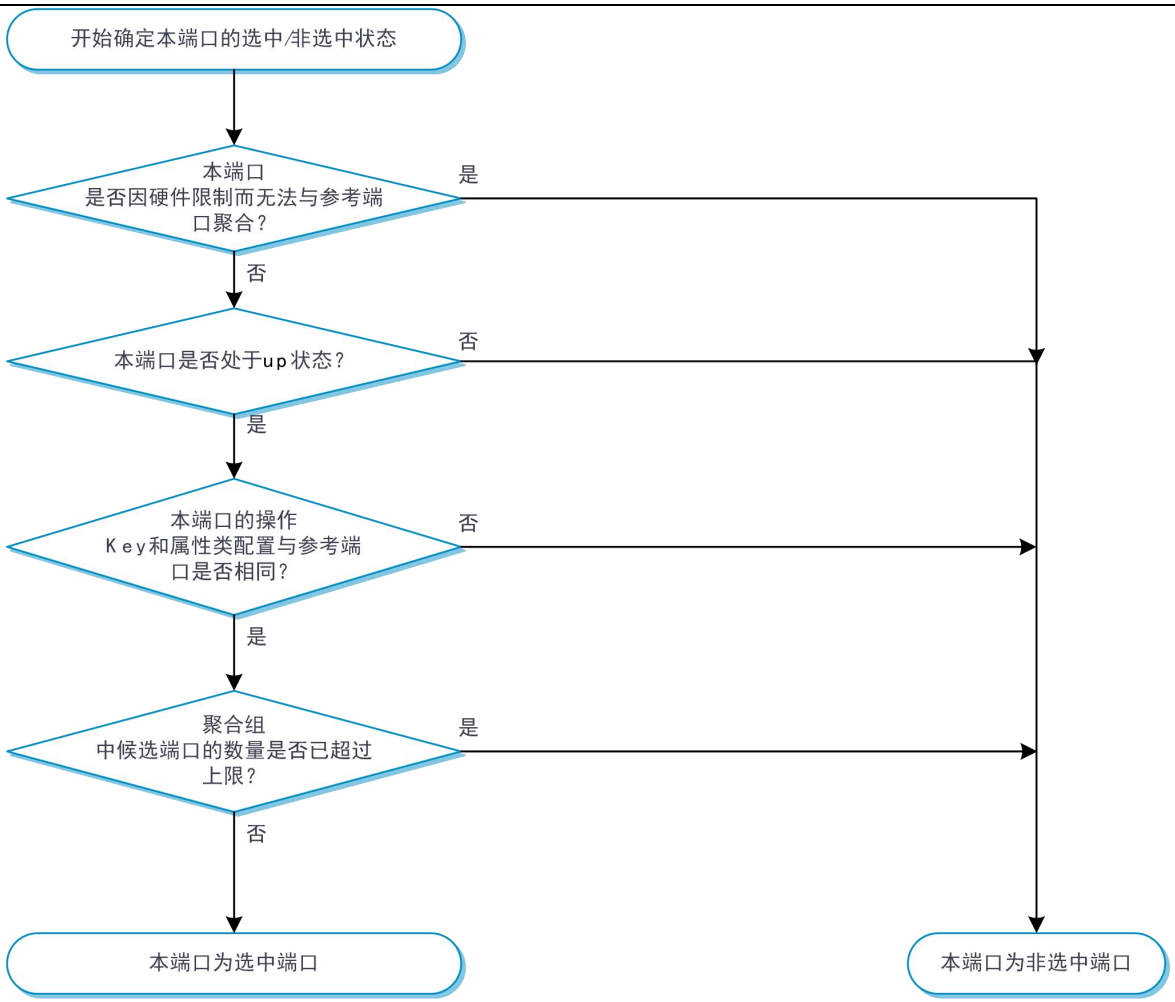
步骤1 选择参考端口

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。

步骤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下图所示。



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。

6.2.1.3.6 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。

步骤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。

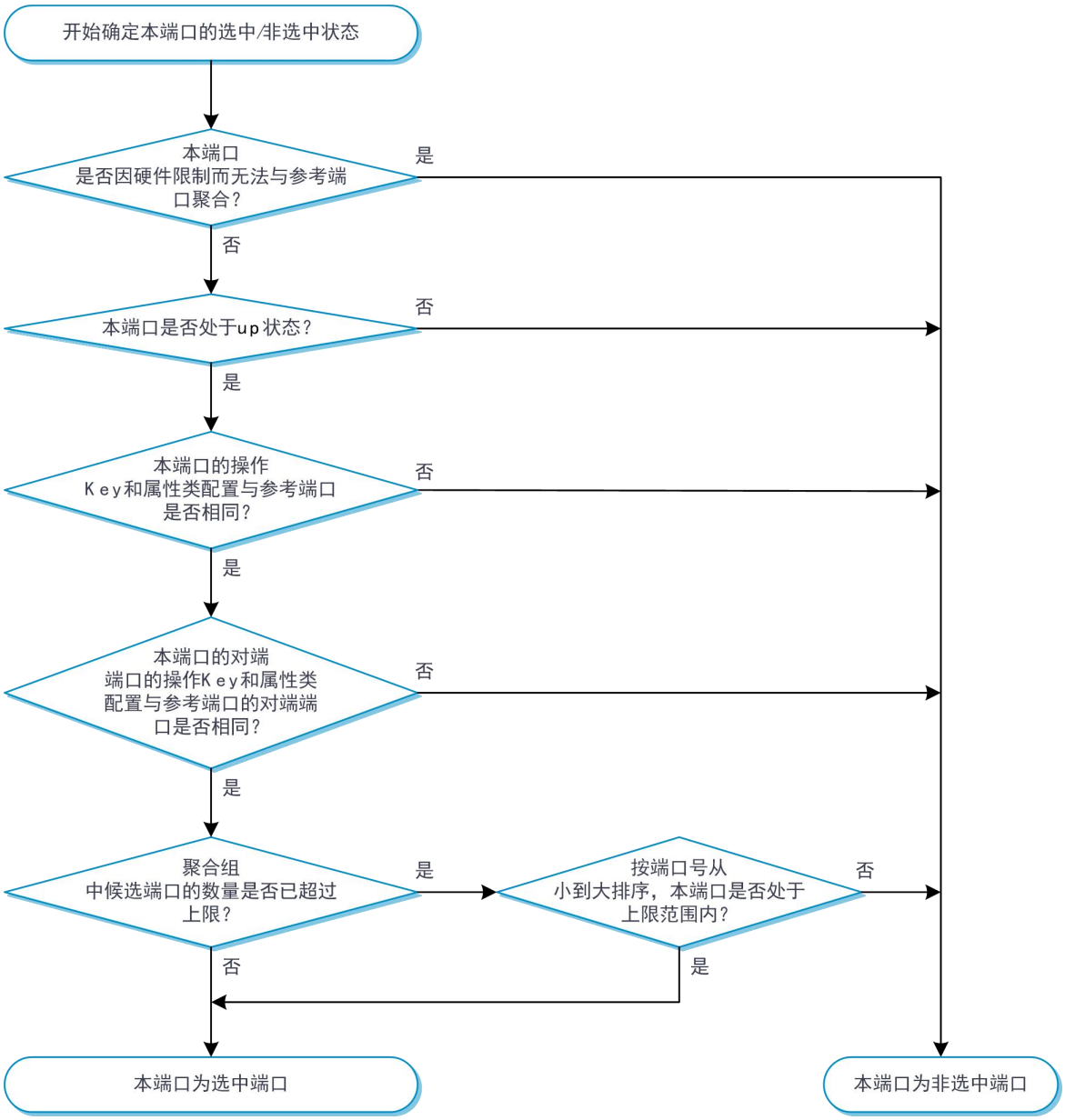
- 首先，从聚合链路的两端选出设备ID（由系统的LACP优先级和系统的MAC

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。

步骤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下图所示



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。

6.2.1.4 VLAN终结

6.2.1.4.1 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。

6.2.1.4.2 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。

6.2.1.4.3 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。

6.2.2 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。

6.2.3 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。

6.3 接口对

6.3.1 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。

6.3.1.1 隧道报文转发模式

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。

6.3.1.2 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。

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。

6.3.1.3 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：

6.3.1.3.1 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。

6.3.1.3.2 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。

6.3.2 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。

6.3.3 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。

6.3.4 配置指南

步骤1　选择“网络 > 接口 > 接口对”，进入“接口对”页面。

步骤2　单击<新建>按钮，进入“新建接口对”页面。

步骤3　具体配置内容如下表所示：

参数	说明
工作模式	接口对支持的工作模式，包括： ● 反射模式 ● 黑洞模式 ● 转发模式
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 当工作模式为转发时，才支持本参数

步骤4　单击<确定>按钮，新建接口对，会在“接口对”页面中显示。

步骤5　选择“网络 > 接口 > 接口对”，进入“高级设置”页面。

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

6.4　接口联动组

本帮助主要介绍以下内容：

6.4.1　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。

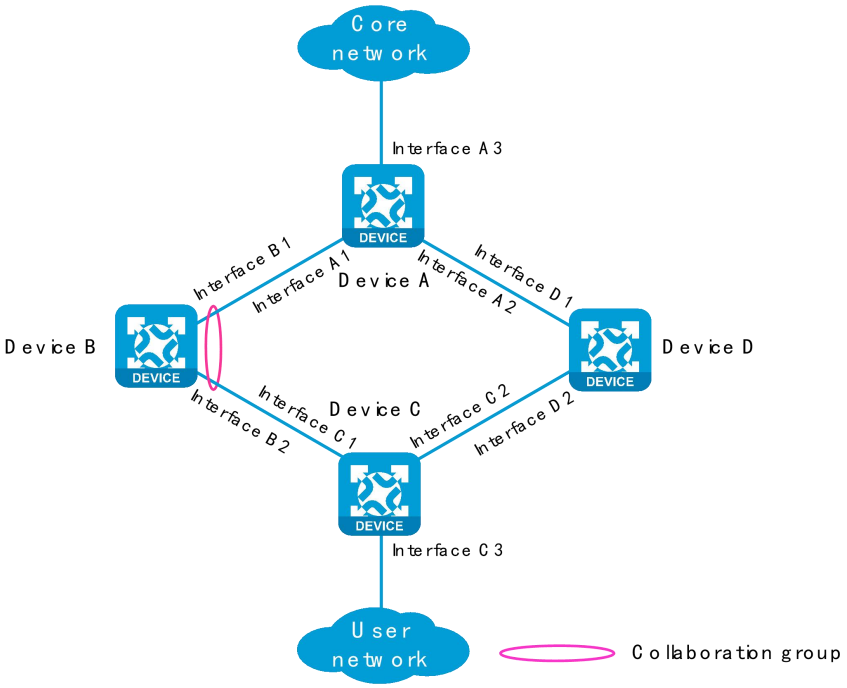
6.4.1.1 工作原理

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。

6.4.1.2 典型组网

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。



6.4.1.3 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。

6.4.2 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。

6.4.3 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。

6.4.4 配置指南

步骤1 单击“网络 > 接口与VRF > 接口联动组”。

步骤2 在接口联动组页面，点击<新建>按钮。

步骤3 在“新建接口联动组”页面的具体配置内容如下表所示：

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，可能会造成流量丢失。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，也会使联动组的成员接口在延迟指定时间后才变为 UP 状态

步骤4 单击<确定>，接口联动组会在“接口联动组”页面显示。

6.5 安全域

本帮助主要介绍以下内容：

6.5.1 特性简介

6.5.1.1 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。

6.5.1.2 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。

6.5.1.3 威胁防护

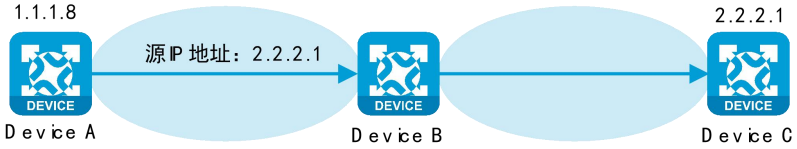
客户端验证功能用来防御服务器受到的TCP、HTTP、SIP、DNS、HTTPS类型的泛洪攻击。启动了客户端验证功能的设备，位于客户端和服务器之间，能够对客户端发起的连接进行验证，当检测到服务器受到攻击时，将服务器的IP地址添加为动态受保护的IP地址，并对所有向该服务器发起的报文进行验证，从而达到保护服务器免受各种泛洪攻击的目的。

6.5.1.4 uRPF

6.5.1.4.1 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。



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。

6.5.1.4.2 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。

6.5.1.4.3 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。

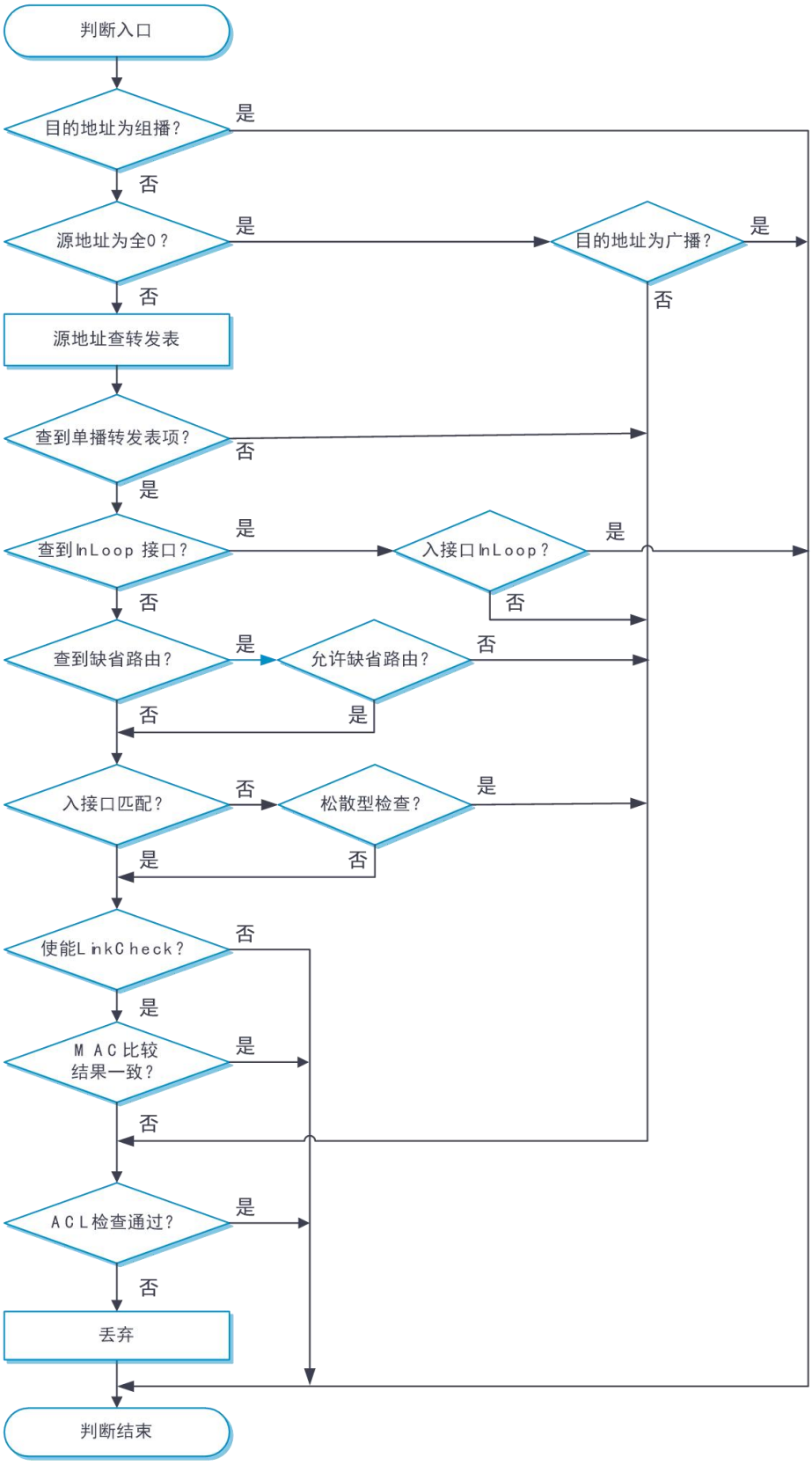
链路层检查功能对于运营商用一个三层以太网接口接入大量PC机用户时部署非常合适。

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。

6.5.1.4.4 IPv4 uRPF处理流程


判断入口
目的地址为组播？
是
否
源地址为全0？
是
否
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
否
入接口InLoop？
是
否
查到缺省路由？
是
否
允许缺省路由？
否
是
入接口匹配？
否
是
松散型检查？
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

步骤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。

步骤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；

步骤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；

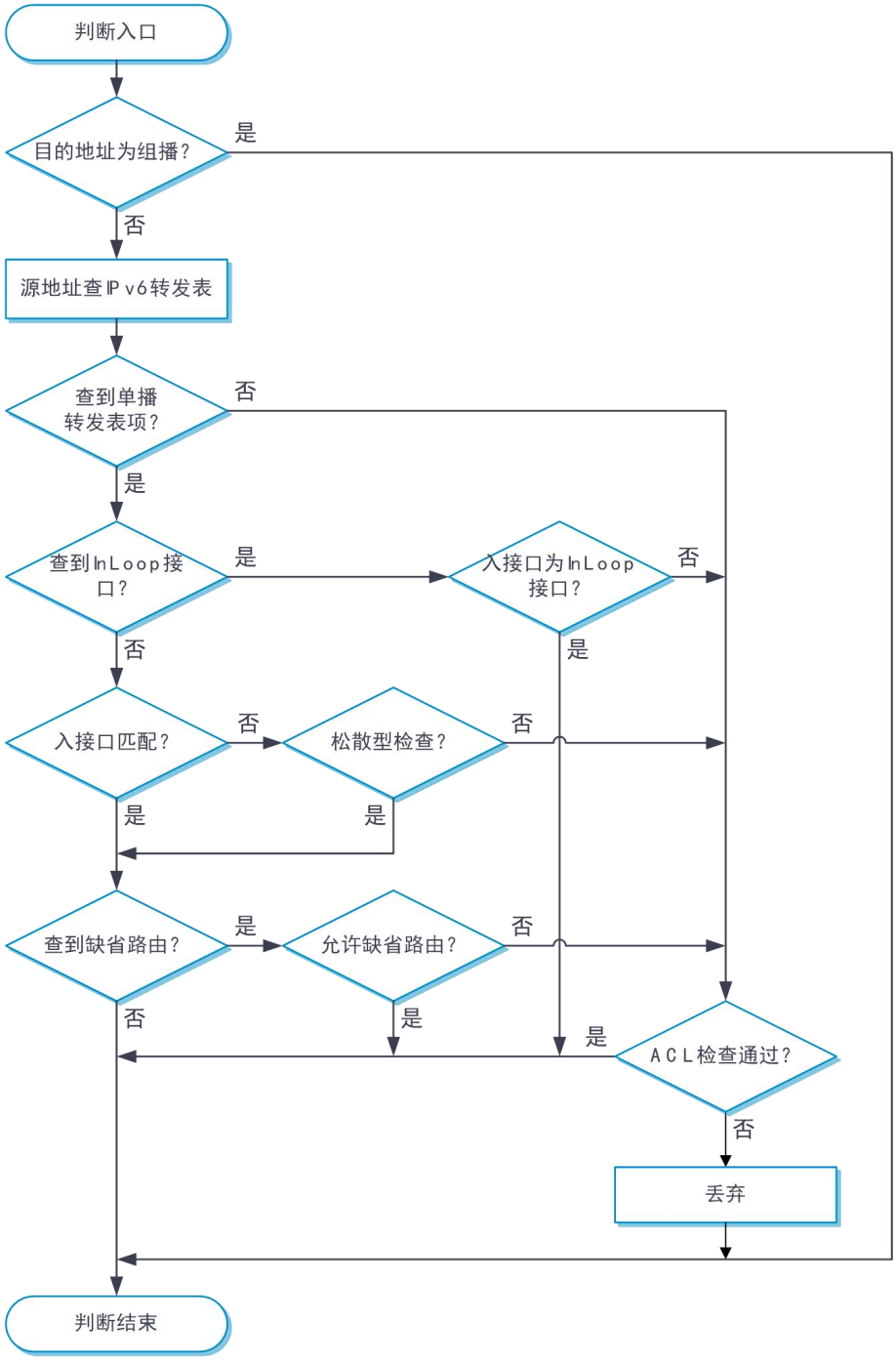
步骤4　如果转发表中匹配的是缺省路由，则检查用户是否配置了允许匹配缺省路由：如果没有配置，则进入步骤7，否则进入步骤5；如果转发表中匹配的不是缺省路由，则进入步骤5；

步骤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；

步骤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；

步骤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。

6.5.1.4.5　IPv6 uRPF处理流程



步骤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；

步骤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；

步骤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；

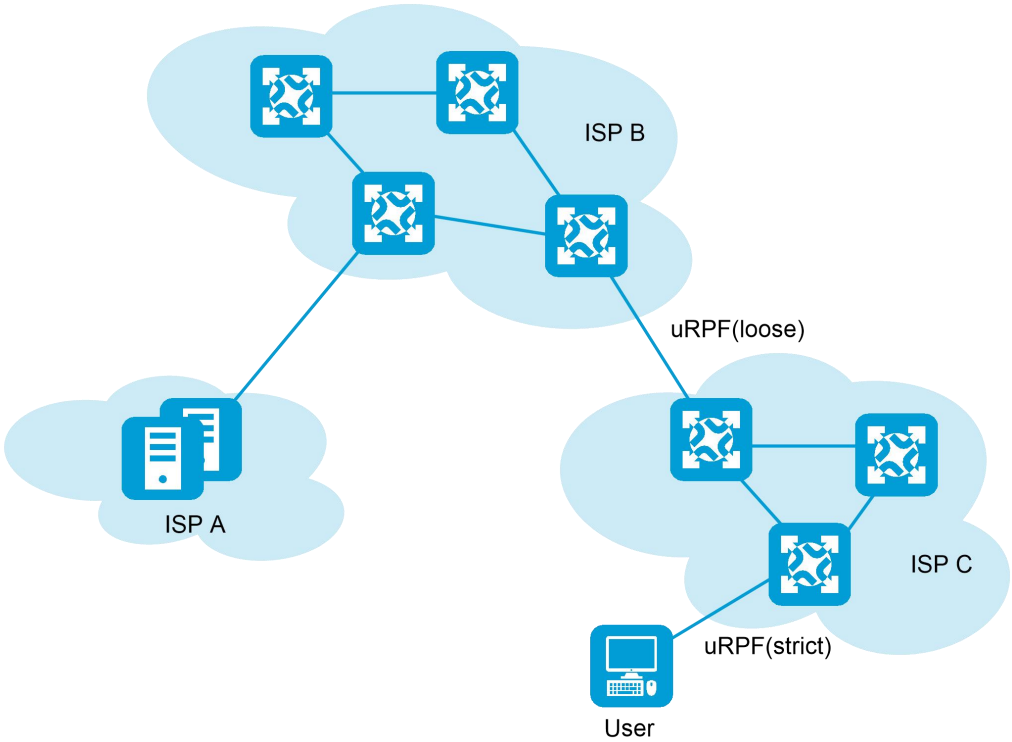
如果源地址是Link-Local地址，倘若这个地址是入接口的地址，并且入接口不是InLoop接口则进入步骤6，否则直接放行；

步骤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；

步骤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；

步骤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。

6.5.1.4.6　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。

6.5.1.5 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。

6.5.2 使用限制和注意事项

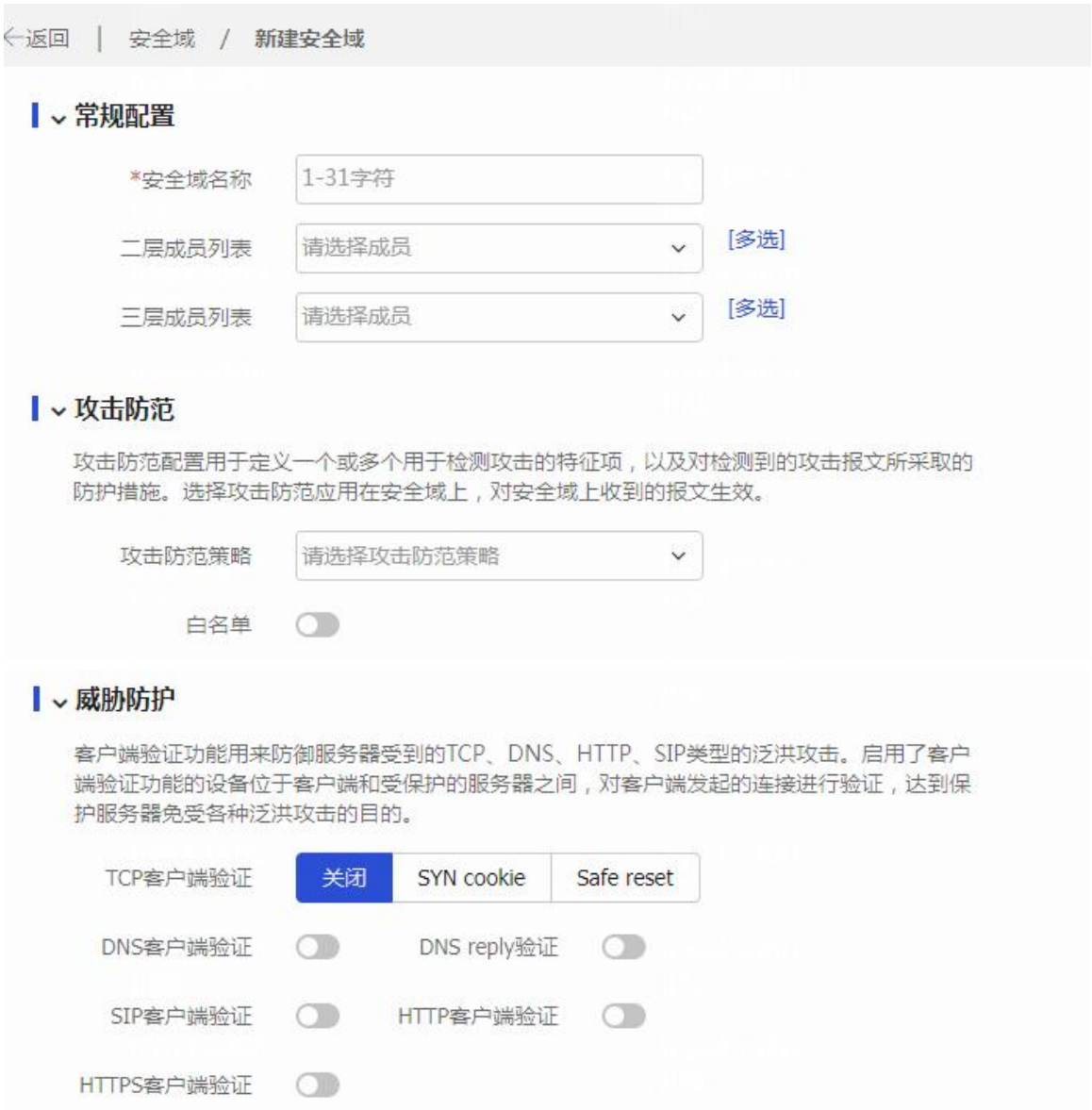
- 设备管理口缺省属于Management安全域，用户可以通过该接口登录Web管理页面管理设备，若移出Management安全域，则会立即断开Web访问，无法远程管理设备。
- 同一个三层接口只允许加入一个安全域。
- 同一个“二层接口和VLAN”的组合只能加入到一个安全域中。
- 当报文未匹配对应安全域间实例时，若存在**any**到**any**的安全域间实例，则匹配**any**到**any**安全域间实例，否则直接丢弃报文。
- Management和Local安全域间之间的报文缺省会被允许。
- Management和Local安全域间之间的报文只能匹配Management与Local之间的安全域间实例，不会匹配**any**到**any**的安全域间实例。

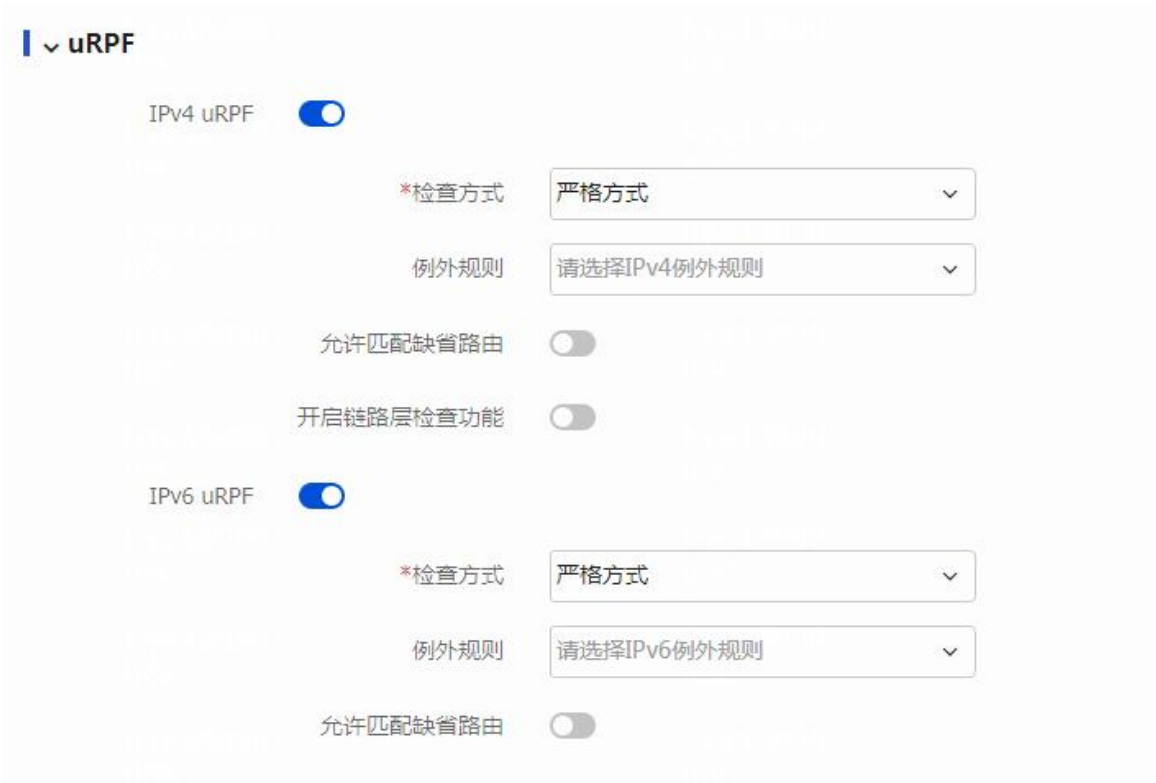
6.5.3 配置指南

6.5.3.1 安全域

步骤1　单击“网络 > 安全域”。

步骤2　在“安全域”页面单击<新建>按钮，进入新建安全域页面。


返回 | 安全域 / 新建安全域
常规配置
*安全域名称
1-31字符
二层成员列表
请选择成员
[多选]
三层成员列表
请选择成员
[多选]
攻击防范
攻击防范配置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护措施。选择攻击防范应用在安全域上，对安全域上收到的报文生效。
攻击防范策略
请选择攻击防范策略
白名单
威胁防护
客户端验证功能用来防御服务器受到的TCP、DNS、HTTP、SIP类型的泛洪攻击。启用了客户端验证功能的设备位于客户端和受保护的服务器之间，对客户端发起的连接进行验证，达到保护服务器免受各种泛洪攻击的目的。
TCP客户端验证
关闭
SYN cookie
Safe reset
DNS客户端验证
DNS reply验证
SIP客户端验证
HTTP客户端验证
HTTPS客户端验证



步骤3　新建安全域，具体配置内容如下表所示：

参数	说明
安全域名称	表示安全域的名称
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

参数	说明
	● 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

步骤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。

6.5.3.2　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。

6.5.3.2.1　配置步骤

步骤1　单击“网络 > 安全域 > 白名单”。

步骤2　在“白名单”页面单击<新建>按钮。

步骤3　手工添加白名单，具体配置内容如下表所示：

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，可在“对象 > 对象组”页页面查看

步骤4　单击<确定>按钮，新建的白名单会在“白名单”页面显示。

6.5.3.3 客户端验证

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。

6.5.3.3.1 配置步骤

步骤1　单击“网络 > 安全域 > 客户端验证”。

步骤2　在“客户端验证”页面单击<新建>按钮。

步骤3　新建客户端验证，具体配置内容如下表所示：

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 > VRF”页面查看
IP 地址类型	● IPv4 ● IPv6

参数	说明
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

步骤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。

6.6　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

6.6.1　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。

6.6.1.1 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。

6.6.1.2 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。

6.6.2 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。

6.6.3 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。

6.6.4 配置指南

6.6.4.1 新建并划分VLAN

步骤1　选择“网络 > 链路 > VLAN”，进入“VLAN”页面。

步骤2　单击<新建>按钮，进入“新建VLAN”页面。

步骤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。

步骤4　单击<确定>按钮，新建VLAN成功，并会在“VLAN”页面中显示。

步骤5　在“VLAN”页面，单击<编辑>按钮，进入“编辑VLAN”页面。

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 VLAN Tag 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 Access 类型的端口能发送多个 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 1)　在 Trunk 下拉框中选择接口 2)　单击<添加>按钮，添加的接口将显示在 Trunk 列表
链路类型：Hybrid-Untagged	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 的报文不带 VLAN Tag 1)　在 Untagged 下拉框中选择接口 2)　单击<添加>按钮，添加的接口将显示在 Untagged 列表
链路类型：Hybrid-Tagged	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 1)　在 Tagged 下拉框中选择接口 2)　单击<添加>按钮，添加的接口将显示在 Tagged 列表

步骤6　单击<确定>按钮，编辑VLAN完成。

6.6.4.2 创建VLAN接口

步骤1 选择“网络 > 链路 > VLAN”，进入“VLAN”页面。

步骤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。

步骤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”。

步骤4 单击<确定>按钮，此处新建的VLAN接口，可在“网络 > 接口 > 接口”页面查看。

6.7 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

6.7.1 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。

6.7.1.1 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

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。

6.7.1.2 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。

6.7.1.3 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。

6.7.1.4 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。

6.7.2 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。

6.7.3 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。

6.7.4 配置指南

步骤1 选择“网络 > 链路 > MAC”，进入“MAC”页面。

步骤2 在“MAC”页面，单击<新建>按钮，进入“新建MAC地址”页面。

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 MAC 地址
VLAN	VLAN 的编号
接口	指定 VLAN 下的出接口

步骤3 单击<确定>按钮，新建MAC地址成功，并会在“MAC”页面中显示。

步骤4 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”。

6.8 DNS

本帮助主要介绍以下内容：

6.8.1 特性简介

6.8.1.1 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。

6.8.1.2 DNS代理

使用DNS代理功能时，DNS客户端配置的DNS server的地址为DNS服务器的IP地址。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，从而实现DNS服务功能。

6.8.1.3 DNS服务

DNS服务用来处理和转发DNS客户端与DNS服务器之间的DNS报文。DNS客户端需要将设备当作DNS服务器（即DNS客户端配置的DNS server的地址为设备的IP地址）。

设备收到来自DNS客户端的请求报文后，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请求报文的目的IP地址修改为DNS服务器的IP地址，源IP地址修改为自身的IP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DNS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，从而实现DNS服务对域名的解析。

使用DNS服务功能后，当DNS服务器的IP地址发生变化时，只需改变设备上的配置，无需改变局域网内每个DNS客户端的配置，从而简化了网络管理。

6.8.1.4 DNS Snooping

DNS Snooping功能适用于基于域名做策略的场景（如安全策略、带宽策略等）。设备使用基于域名的策略过滤用户流量时，需要获取域名对应的IP地址才能真正实现流量过滤。开启DNS Snooping功能后，设备会监听过路的DNS请求报文和DNS应答报文，如果DNS请求报文中的域名与策略中的域名相同，设备会在收到该域名的响应报文时记录域名解析结果，并上报给策略，使得策略可以基于此域名对应的IP地址实现流量过滤。如果DNS请求报文中的域名与过滤规则中的域名不同，设备不会记录域名解析

结果。

6.8.2 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。

6.8.3 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：先配置的域名服务器优先级高于后配置的域名服务器；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，失败后再依次向其它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。

6.8.4 配置指南

6.8.4.1 配置静态域名解析

步骤1 选择“网络 > DNS > 已解析域名”，进入“已解析域名”页面。

步骤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：

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

步骤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”。

6.8.4.2 配置动态域名解析

步骤1 选择“网络 > DNS > DNS客户端”，进入DNS客户端页面。

步骤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。

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

步骤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。

6.8.4.3　配置DNS代理

DNS代理用来在DNS客户端和DNS服务器之间转发DNS请求和应对报文，具体配置步骤如下：

步骤1　选择“网络 > DNS > DNS代理”。

步骤2　在“DNS代理”页面，开启DNS代理。

6.8.4.4　配置DNS服务

具体配置步骤如下：

步骤1　选择“网络 > DNS > 高级设置”。

步骤2　在“高级设置”页面，开启DNS服务。

6.8.4.5　配置DNS Snooping

步骤1　选择“网络 > DNS > 高级设置”。

步骤2　在“高级设置”页面，开启DNS Snooping功能。

6.8.4.6 配置域名后缀

步骤1 选择“网络 > DNS > 高级设置”。

步骤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。

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

步骤3 在域名后缀列表中输入域名后缀名。

步骤4 单击<添加>按钮，新增的域名后缀在域名后缀列表中显示。

6.8.4.7 配置DNS TTL

步骤1 选择“网络 > DNS > 高级设置”。

步骤2 在“高级设置”页面配置TTL最小值（即域名解析表项有效时间的最小值）与TTL最大值（即域名解析表项有效时间的最大值）。

6.9 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
  - IP-MAC绑定表项
  - ARP表项
  - ARP防护

6.9.1 特性简介

6.9.1.1 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。

6.9.1.1.1 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。

6.9.1.1.2 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。

6.9.1.2 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。

6.9.1.3 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。

6.9.2 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。

6.9.3 配置指南

6.9.3.1 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。

6.9.3.1.1 配置步骤

步骤1 选择“网络 > ARP”，进入ARP页面。

步骤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，具体配置内容如下表所示：

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,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

参数	说明
	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“成员列表” 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理方式，包括： ● 放行 ● 丢弃

步骤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，具体配置内容如下表所示：

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

步骤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。

6.9.3.2 ARP表项

步骤1 选择“网络 > ARP”，进入ARP页面。

步骤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，具体配置内容如下表所示：

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

参数	说明
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”才会显示本参数
接口	报文转发的接口，只有勾选“指定报文转发的 VLAN 和接口”才会显示本参数

步骤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”。

步骤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。

步骤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。

6.9.3.3　ARP防护

步骤1　选择“网络 > ARP”，进入ARP页面。

步骤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。

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

步骤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。

6.10　ND

本帮助主要介绍以下内容：

- 特性简介

6.10.1 特性简介

6.10.1.1 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。

6.10.1.2 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。

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，向邻居节点通告本节点的变化信息
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，请求前缀和其他配置信息，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，路由器会周期性地发布 RA 消息，其中包括前缀信息选项和一些标志位的信息

ICMPv6消息	类型号	作用
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送重定向消息，使主机重新选择正确的下一跳地址进行后续报文的发送

6.10.2 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。

6.10.3 配置指南

6.10.3.1 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。

6.10.3.1.1 配置步骤

步骤1 选择“网络 > ND”，进入ND页面。

步骤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，具体配置内容如下表所示：

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

参数	说明
	单击<全部添加>按钮，“接口列表”中所有接口将添加到“成员列表” 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

步骤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，具体配置内容如下表所示：

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

步骤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。

6.10.3.2　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。

6.10.3.2.1　配置步骤

步骤1　选择“网络 > ND”，进入ND页面。

步骤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，具体配置内容如下表所示：

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

步骤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。

步骤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。

6.11　转发高级设置

6.11.1　特性简介

6.11.1.1　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。

6.11.1.2　报文转发模式

报文转发模式的支持情况与设备型号有关，请以设备的实际情况为准。

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。

6.11.1.3 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。

6.11.2 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。

6.11.3 配置指南

步骤1 选择“网络 > 转发高级设置”。

步骤2 进入转发高级设置页面，具体配置内容如下表所示：

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：

参数	说明
	● 逐流：基于一元组、基于三元组、基于五元组 ● 逐包
优先使用虚拟 MAC 作为报文源 MAC	开启/关闭接口发送报文的源 MAC 地址优先使用虚拟 MAC 功能 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，其他组网场景中请勿使用本功能

6.12 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

6.12.1 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、ICMP差错报文、DNS、H323、SIP、RTSP

6.12.2 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。

6.12.3 配置指南

步骤1 单击“网络 > ALG”。

步骤2　在“ALG”页面开启指定协议的ALG功能。

步骤3　单击<应用>按钮，完成配置。

6.13　GRE

本帮助主要介绍以下内容：

- 特性简介
    - 封装格式
    - 工作原理
    - 保活机制
    - 安全机制
- vSystem相关说明
- 使用限制和注意事项
- 配置指南

6.13.1　特性简介

GRE（Generic Routing Encapsulation，通用路由封装）协议用来对任意一种网络层协议（如IPv6）的数据报文进行封装，使这些被封装的数据报文能够在另一个网络（如IPv4）中传输。封装前后数据报文的网络层协议可以相同，也可以不同。封装后的数据报文在网络中传输的路径，称为GRE隧道。GRE隧道是一个虚拟的点到点的连接，其两端的设备分别对数据报文进行封装及解封装。

6.13.1.1　封装格式

GRE封装后的报文包括如下几个部分：

- 净荷数据（Payload packet）：需要封装和传输的数据报文。净荷数据的协议类型，称为乘客协议（Passenger Protocol）。乘客协议可以是任意的网络层协议。
- GRE头（GRE header）：采用GRE协议对净荷数据进行封装所添加的报文头，包括封装层数、版本、乘客协议类型、校验和信息、Key信息等内容。添加GRE头后的报文称为GRE报文。对净荷数据进行封装的GRE协议，称为封装协议（Encapsulation Protocol）。
- 传输协议的报文头（Delivery header）：在GRE报文上添加的报文头，以便传输协议对GRE

报文进行转发处理。传输协议（Delivery Protocol或者Transport Protocol）是指负责转发GRE报文的网络层协议。设备支持IPv4和IPv6两种传输协议：当传输协议为IPv4时，GRE隧道称为GRE over IPv4隧道；当传输协议为IPv6时，GRE隧道称为GRE over IPv6隧道。

6.13.1.2 工作原理

IPv4/IPv6协议报文通过GRE隧道进行传输的过程：

步骤1 GRE隧道源端设备收到IPv4/IPv6协议报文后，将该报文发给相应的Tunnel接口。

步骤2 GRE隧道模式的Tunnel接口收到此报文后，先在报文前封装上GRE头，再封装上传输协议头。传输协议头中的源地址为隧道的源端地址，目的地址为隧道的目的端地址。

步骤3 隧道源端设备将封装后的IPv4/IPv6协议报文通过GRE隧道的实际物理接口转发出去。

步骤4 封装后的IPv4/IPv6协议报文通过GRE隧道到达隧道的目的端设备后，由于报文的目的地是本设备，故将此报文交给GRE协议进行解封装处理。

步骤5 GRE协议先剥离掉此报文的传输协议头，再对报文进行GRE Key验证、校验和验证、报文序列号检查等处理，处理通过后再剥离掉报文的GRE头，将报文交给相应的载荷协议进行后续的转发处理。

6.13.1.3 保活机制

Keepalive功能用来对GRE隧道状态进行监控。若本端设备在按照用户设置的发送周期和最大发送次数向对端设备发送Keepalive报文后仍然没有收到对端的回应，则把本端Tunnel接口的状态置为down。如果Tunnel接口为down状态时，收到对端回复的Keepalive确认报文，则Tunnel接口的状态将转换为up，否则保持down状态。无论是否开启Keepalive功能，隧道一端收到Keepalive报文，必须向对端发送应答报文。

6.13.1.4 安全机制

GRE支持GRE Key验证、校验和验证两种安全机制。

6.13.1.4.1 GRE Key验证

发送方在发送的报文中携带其本地配置的GRE Key。接收方收到报文后，将报文中的GRE Key与接收方本地配置的GRE Key进行比较，如果一致则对报文进行进一步处理，否则丢弃该报文。

6.13.1.4.2 GRE校验和验证

通过GRE校验和验证可以检查报文的完整性。

发送方根据GRE头及Payload信息计算校验和，并将包含校验和信息的报文发送给对端。接收方对接收

到的报文计算校验和，并与报文中的校验和比较，如果一致则对报文进行进一步处理，否则丢弃该报文。

6.13.2 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。

6.13.3 使用限制和注意事项

- 隧道的接口地址可以指定为IPv4地址或者IPv6地址。若净荷数据协议类型为IPv4，则隧道接口地址应配置为IPv4地址；若净荷数据协议类型为IPv6，则隧道接口地址应配置为IPv6地址。
- 隧道两端必须都配置隧道的源端地址和目的端地址，且本端配置的源端地址（目的端地址）应该与对端配置的目的端地址（源端地址）相同。
- 如果封装前报文的目的地址与Tunnel接口的地址不在同一个网段，则必须配置通过Tunnel接口到达报文目的地址的路由，以便需要进行封装的报文能正常转发。用户可以配置静态路由，指定到达报文目的地址的路由出接口为本端Tunnel接口；也可以配置动态路由，在Tunnel接口、与私网相连的接口上分别使能动态路由协议，由动态路由协议来建立通过Tunnel接口转发的路由表项。
- 在Tunnel接口上配置的隧道目的端地址不能与Tunnel接口的地址在同一网段。
- Keepalive功能不要求两端同时开启，用户可以根据需要在任意一端开启Keepalive功能。
- 若开启GRE key功能，则隧道两端必须设置相同的GRE key，或者都不设置GRE key。
- 隧道两端可以根据各自的实际应用需要决定是否要开启GRE报文校验和功能。如果本端开启了GRE报文校验和功能，则会在发送的报文中携带校验和信息，由对端来对报文进行校验和验证。对端是否对收到的报文进行校验和验证，取决于报文中是否携带校验和信息，与对端的配置无关。

6.13.4 配置指南

步骤1 单击“网络 > VPN > GRE”。

步骤2 在“GRE”页面，单击<新建>按钮，进入“新建GRE隧道接口”页面，具体配置内容如下：

参数	说明
传输协议	传输协议支持 IPv4 和 IPv6
接口编号	GRE 隧道接口编号
加入安全域	配置接口所属的安全域
描述	接口的描述信息

参数	说明
接口 IPv4 地址	GRE 隧道接口的 IPv4 地址
接口 IPv6 地址	GRE 隧道接口的 IPv6 地址
隧道源端地址	如果选择指定 IP 地址，则该地址将作为封装后隧道报文的源地址；如果设置的是隧道的源接口，则该接口的地址将作为封装后隧道报文的源地址
隧道目的端地址	GRE 隧道的目的端地址
VRF	指定隧道目的端地址所属的 VRF 后，设备将查找指定 VRF 的路由表转发隧道封装后的报文
开启 Keepalive 功能	开启本功能后，设备会定期发送探测报文探测 GRE 隧道是否正常
发送周期	Keepalive 报文发送周期，即多长时间发送一次探测报文
最大传送次数	Keepalive 报文的最大传送次数，即报文发送一定的次数，且未收到返回报文时，设备将判断 GRE 隧道已断开
GRE key	GRE key 主要用于检查报文的合法性
开启报文校验和功能	开启报文校验和功能，可以有效检查报文的完整性
封装后隧道报文的 ToS	ToS 值用于标识 IP 报文的服务类型，配置本功能后，同一个 GRE 隧道中转发的报文将具有相同的 ToS 值
封装后隧道报文的 TTL	如果两台设备之间的跳数超过配置的 TTL 值，它们将无法通信
封装后隧道报文不允许分片	配置本功能后，不允许对隧道报文进行分片，可以避免引入分片延时

步骤3　单击“确定”按钮，完成配置。

6.14　IPsec

本帮助主要介绍以下内容：

- 特性简介
  - 安全协议及封装模式
  - 认证与加密
  - IPsec SA

- IKE协商
- IPsec隧道的建立
- IPsec智能选路
- IPsec自动生成安全策略

- vSystem相关说明
- 使用限制和注意事项
- 配置指南
  - 点到点IPsec配置指南
  - 点到多点IPsec配置指南
  - 配置IKE提议
  - 配置隧道信息
  - 高级设置

6.14.1 特性简介

IPsec（IP Security，IP安全）是IETF制定的三层隧道加密协议，是一种传统的实现三层VPN（Virtual Private Network，虚拟专用网络）的安全技术。IPsec通过在特定通信方之间（例如两个安全网关之间）建立“通道”，来保护通信方之间传输的用户数据，该通道通常称为IPsec隧道。

IPsec协议为IP层上的网络数据安全提供了一整套安全体系结构，包括安全协议AH（Authentication Header，认证头）和ESP（Encapsulating Security Payload，封装安全载荷）、IKE（Internet Key Exchange，互联网密钥交换）以及用于网络认证及加密的一些算法等。其中，AH协议和ESP协议用于提供安全服务，IKE协议用于密钥交换。

6.14.1.1 安全协议及封装模式

6.14.1.1.1 安全协议

IPsec包括AH和ESP两种安全协议，它们定义了对IP报文的封装格式以及可提供的安全服务。

- AH协议定义了AH头在IP报文中的封装格式。AH可提供数据来源认证、数据完整性校验和抗重放功能，它能保护报文免受篡改，但不能防止报文被窃听，适合用于传输非机密数据。
- ESP协议定义了ESP头和ESP尾在IP报文中的封装格式。ESP可提供数据加密、数据来源认证、

数据完整性校验和抗重放功能。虽然AH和ESP都可以提供认证服务，但是AH提供的认证服务要强于ESP。

在实际使用过程中，可以根据具体的安全需求同时使用这两种协议或仅使用其中的一种。设备支持的AH和ESP联合使用的方式为：先对报文进行ESP封装，再对报文进行AH封装。

6.14.1.1.2 封装模式

IPsec支持两种封装模式：

- 传输模式（Transport Mode）

该模式下的安全协议主要用于保护上层协议报文。若要求端到端的安全保障，即数据包进行安全传输的起点和终点为数据包的实际起点和终点时，才能使用传输模式。通常传输模式用于保护两台主机之间的数据。

- 隧道模式（Tunnel Mode）

该模式下的安全协议用于保护整个IP数据包。在安全保护由设备提供的情况下，数据包进行安全传输的起点或终点不为数据包的实际起点和终点时（例如安全网关后的主机），则必须使用隧道模式。通常隧道模式用于保护两个安全网关之间的数据。

6.14.1.2 认证与加密

6.14.1.2.1 认证算法

IPsec使用的认证算法主要是通过杂凑函数实现的。杂凑函数是一种能够接受任意长度的消息输入，并产生固定长度输出的算法，该算法的输出称为消息摘要。IPsec对等体双方都会计算一个摘要，接收方将发送方的摘要与本地的摘要进行比较，如果二者相同，则表示收到的IPsec报文是完整未经篡改的，以及发送方身份合法。目前，IPsec使用基于HMAC（Hash-based Message Authentication Code，基于散列的消息鉴别码）的认证算法和SM3认证算法。HMAC认证算法包括HMAC-MD5、HMAC-SHA。其中，HMAC-MD5算法的计算速度快，而HMAC-SHA算法的安全强度高。

6.14.1.2.2 加密算法

IPsec使用的加密算法属于对称密钥系统，这类算法使用相同的密钥对数据进行加密和解密。目前设备的IPsec使用四种加密算法：

- DES：使用56比特的密钥对一个64比特的明文块进行加密。
- 3DES：使用三个56比特（共168比特）的密钥对明文块进行加密。
- AES：使用128比特、192比特或256比特的密钥对明文块进行加密。
- SM：使用128比特的密钥对明文块进行加密。

这四个加密算法的安全性由高到低依次是：AES/SM、3DES、DES，安全性高的加密算法实现机制复杂，运算速度慢。

6.14.1.3 IPsec SA

IPsec SA（Security Association，安全联盟）是IPsec对等体间对某些要素的约定，例如，使用的安全协议、协议报文的封装模式、认证算法、加密算法、特定流中保护数据的共享密钥以及密钥的生存时间等。

IPsec SA是单向的，在两个对等体之间的双向通信，最少需要两个IPsec SA来分别对两个方向的数据流进行安全保护。同时，如果两个对等体希望同时使用AH和ESP来进行安全通信，则每个对等体都会针对每一种协议来构建一个独立的SA。

IPsec SA由一个三元组来唯一标识，这个三元组包括SPI（Security Parameter Index，安全参数索引）、目的IP地址和安全协议号。其中，SPI是用于标识SA的一个32比特的数值，它在AH和ESP头中传输。

对等体之间通过IKE协议生成IPsec SA，IPsec SA会在一定时间或一定流量之后老化掉。IPsec SA失效前，IKE将为IPsec对等体协商建立新的SA，这样，在旧的SA失效前新的SA就已经准备好。在新的SA开始协商而没有协商好之前，使用当前旧的SA保护通信。一旦协商出新的SA，立即采用新的SA保护通信。

6.14.1.4 IKE协商

IKE为IPsec协商建立SA，并把建立的参数交给IPsec，IPsec使用IKE建立的SA对IP报文加密或认证处理。IKE使用了两个阶段为IPsec进行密钥协商以及建立SA：

步骤1 第一阶段，通信双方彼此间建立了一个已通过双方身份认证和对通信数据安全保护的通道，即建立一个IKE SA。第一阶段有主模式（Main Mode）、野蛮模式（Aggressive Mode）和国密主模式三种IKE协商模式。在对身份保护要求不高的场合，使用交换报文较少的野蛮模式可以提高协商的速度；在对身份保护要求较高的场合，则应该使用主模式。当本端使用RSA-DE或者SM2-DE数字信封方式认证时，必须将本端的协商模式配置为国密主模式。

步骤2 第二阶段，用在第一阶段建立的IKE SA为IPsec协商安全服务，即为IPsec协商IPsec SA，建立用于最终的IP数据安全传输的IPsec SA。

6.14.1.5 IPsec隧道的建立

设备通过应用IPsec策略来实现IPsec隧道的建立。一个IPsec策略主要用于指定策略应用的接口，定义用于保护数据流的安全参数，以及指定要保护的数据流的范围。

当IPsec对等体根据策略识别出要保护的报文时，就建立一个相应的IPsec隧道并将其通过该隧道发送给对端。此处的IPsec隧道由数据流触发IKE协商建立。这些IPsec隧道实际上就是两个IPsec对等体之间建立的IPsec SA。由于IPsec SA是单向的，因此出方向的报文由出方向的SA保护，入方向的报文由入方向的SA来保护。

- 当从一个接口发送数据报文时，接口将按照策略优先级序号从小到大的顺序逐一匹配引用的每一个IPsec策略。如果报文匹配上了某一个IPsec策略保护的数据流，则停止匹配，并根据匹配上的策略协商IPsec SA。之后，由该接口发送的报文，如果能匹配上某出方向的IPsec SA，则由IPsec对其进行封装处理，否则直接被正常转发。
- 应用了IPsec策略的接口收到数据报文时，对于目的地址是本机的IPsec报文，查找本地的入方向IPsec SA，并根据匹配的IPsec SA对报文进行解封装处理；对于那些本应该被IPsec保护但未被保护的报文进行丢弃。

在IPsec策略中，由动作参数（“保护”或“不保护”）来指定是否对数据流进行IPsec保护。一个IPsec策略中，可以定义多条保护的数据流，报文匹配上的首条数据流的动作参数决定了对该报文的处理方式。

- 出入方向的报文都需要匹配IPsec策略中定义的保护的数据流。具体是，出方向的报文正向匹配数据流范围，入方向的报文反向匹配数据流范围。
- 在出方向上，与动作为“保护”的数据流匹配的报文将被IPsec保护，未匹配上任何数据流或与动作为“不保护”的数据流匹配上的报文将不被IPsec保护。
- 在入方向上，与动作为“保护”的数据流匹配上的未被IPsec保护的报文将被丢弃；目的地址为本机的被IPsec保护的报文将被进行解封装处理。

6.14.1.6 IPsec智能选路

为了提高网络的稳定性和可靠性，企业通常会在网络出口配置多条链路。不同链路之间存在通信质量差异，实时状态也不尽相同，选择一条高质量的链路对于企业通信来说尤为重要。IPsec智能选路功能（IPsec Smart Link）在有多条可使用的链路能够到达目的网络的情况下，实时地自动探测链路的时延、丢包率，动态切换到满足通信质量要求的链路上建立IPsec隧道。用户也可以根据自己的实际需求手工指定使用的链路。

IPsec智能选路可以很好地解决以下问题：

- 网络出口多链路进行流量负载分担时，可能会出现一部分链路拥塞、另一部分链路闲置的情况；
- 用户无法基于链路传输质量或者服务费用自己选择链路；
- 当网络出口设备与目的设备之间的链路出现故障时，如果流量被转发该故障链路上，会造成访问失败。

6.14.1.7 IPsec自动生成安全策略

新建IPsec策略规则时，如果勾选<自动生成安全策略>，设备将自动生成放通IKE协商报文的安全策略。

6.14.2 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。

6.14.3 使用限制和注意事项

- 若指定的对端主机名由DNS服务器来解析，则本端按照DNS服务器通知的域名解析有效期，在该有效期超时之后向DNS服务器查询主机名对应的最新的IP地址； 若指定的对端主机名由本地配置的静态域名解析来解析，则更改此主机名对应的IP地址之后，需要在IPsec策略中重新指定的对端主机名，才能使得本端解析到更新后的对端IP地址。
- 为保证IPsec对等体上能够成功建立SA，建议两端设备上用于IPsec的ACL配置为镜像对称，即保证两端定义的要保护的数据流范围的源和目的尽量对称。若IPsec对等体上的ACL配置非镜像，那么只有在一端的ACL规则定义的范围是另外一端的子集时，且仅当保护范围小（细粒度）的一端向保护范围大（粗粒度）的一端发起的协商才能成功。
- 如果IPsec策略下没有配置本端身份，则默认使用高级配置中的全局本端身份。
- 在对IPsec策略的封装模式、安全协议、算法、PFS、SA生存时间、SA超时时间进行修改时，对已协商成功的IPsec SA不生效，即仍然使用原来的参数，只有新协商的SA使用新的参数。若要使修改对已协商成功的IPsec SA生效，则需要首先清除掉已有的IPsec SA。
- 在IPsec隧道的两端，IPsec策略所采用的封装模式、安全协议、算法要一致。
- 当IKE协商IPsec SA时，如果接口上的IPsec策略下未配置IPsec SA的生存周期，将采用全局的IPsec SA生存周期与对端协商。如果IPsec策略下配置了IPsec SA的生存周期，则优先使用策略下的配置值与对端协商。
- IKE为IPsec协商建立IPsec SA时，采用本地配置的生存时间和对端提议的IPsec SA生存时间中较小的一个。
- 配置IPsec智能选路功能时，当link中的下一跳地址为接口网关地址时，修改网关地址，用

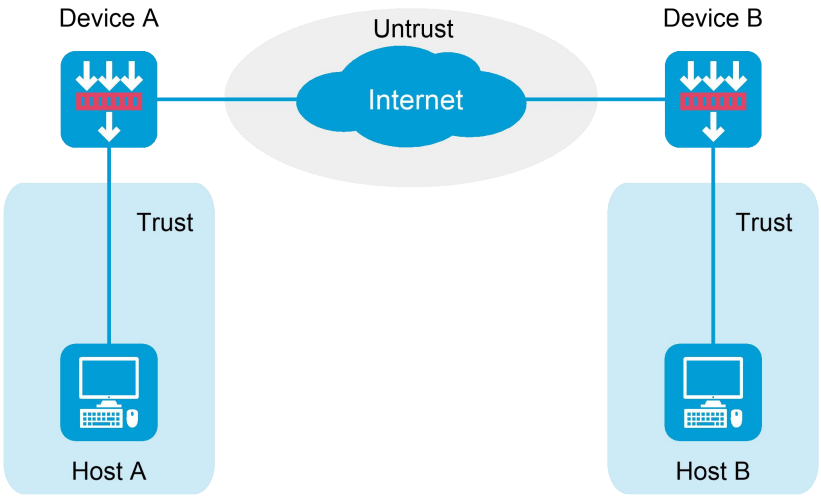
户需要手动修改link中的下一跳地址。

6.14.4 配置指南

6.14.4.1 点到点IPsec配置指南

6.14.4.1.1 背景信息

IPsec按照实际需求的不同存在两种组网方式，分别是点到点和点到多点的组网方式。这两种组网方式的配置方式存在差异，下面介绍点到点IPsec配置。点到点IPsec的典型组网如下图所示，Host A与Host B通过Internet通信，可以在Device A和Device B之间建立一条IPsec隧道，对Host A与Host B之间通过Internet传输的数据流进行安全保护。



6.14.4.1.2 基本配置

步骤1 选择“网络 > VPN > IPsec > 策略”，单击“新建”按钮，进入“新建IPsec策略”页面。

步骤2 在“新建IPsec策略”页面，选择“设备角色”为“对等/分支节点”，点到点IPsec隧道的具体配置内容如下：

参数	说明
策略名称	IPsec 策略的名称，一个设备可以存在多条策略，策略名称用于本地区分 IPsec 策略
优先级	IPsec 策略的顺序号，一个 IPsec 策略是若干具有相同名称、不同顺序号的 IPsec 策略表项的集合。在同一个 IPsec 策略中，顺序号越小的 IPsec 策略表项优先级越高，流量需要匹配 IPsec 策略时会从顺序号小的 IPsec 策略开始匹配，匹配到了就会进入 IPsec 隧道转发

参数	说明
别名	IPsec 策略的别名
设备角色	表示该设备在 IPsec 组网中的角色，取值包括： ● 对端/分支节点：点到多点组网的分支设备是分支节点，点到点组网的设备是对等节点 ● 中心节点：点到多点组网的中心设备是中心节点
IP 地址类型	建立 IPsec 隧道的本端地址类型，取值包括： ● IPv4：地址类型为IPv4 ● IPv6：地址类型为IPv6
智能选路	配置是否开启智能选路功能 IPsec 智能选路功能（IPsec Smart Link）在有多条可使用的链路能够到达目的网络的情况下，实时的自动探测链路的时延、丢包率，动态切换到满足通信质量要求的链路上建立 IPsec 隧道。IPv6 地址不支持智能选路
接口	指定应用该 IPsec 策略的接口。如果开启了智能选路功能，需要将本端待选择接口都添加进去，供智能选路选择
本端地址	指定应用该 IPsec 策略接口的 IP 地址。如果开启了智能选路功能，需要将本端待选择接口的 IP 地址都添加进去，供智能选路选择
对端 IP 地址/主机名	指定 IPsec 隧道的对端 IP 地址/主机名。如果开启了智能选路，需要将对端接口的 IP 地址都添加进去
描述	IPsec 策略的描述信息，方便网络管理人员了解策略的使用目的

6.14.4.1.3 IKE策略配置

步骤1 进入“IKE策略”配置页面。

步骤2 在“IKE策略”配置页面，配置协商模式、认证方式、预共享密钥等，具体配置内容如下：

参数	说明
协商模式	IKE 协商模式，取值包括： ● 主模式：强制使用主模式协商，主模式更安全 ● 野蛮模式：强制使用野蛮模式协商，野蛮模式更快速 ● 国密主模式：必须使用RSA-DE或者SM2-DE数字信封方式认证的认证方式，协商方式与主模式一致，安全性更高
认证方式	IKE 认证方式，取值包括： ● 预共享密钥：手动分配所需的共享密钥的认证方式。点到点对等体的预共享密钥必须一致 ● 数字认证：通信双方使用由CA颁发的数字证书向对端证明自己的身份。不需要配置预共享密钥，需要额外配置PKI域和证书访问策略，有关PKI域和证书访问策略配置，请参考PKI联机帮助
预共享密钥	选择认证方式为预共享密钥需要配置。需要保证点到点对等体的预共享密钥一致

参数	说明
PKI 域	选择认证方式为数字认证需要配置。PKI 是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，有关 PKI 的配置，请参考 PKI 联机帮助
证书访问策略	选择认证方式为数字认证可以配置。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，有关证书访问策略配置，请参考 PKI 联机帮助
IKE 提议	IKE 定义了一套属性数据来描述 IKE 第一阶段使用怎样的参数来与对端进行协商，这套属性称为 IKE 提议，取值如下： ● 新建IKE提议：新建IKE提议，参数需与对端设备保持一致 ● NONE：不配置IKE提议，使用默认提议与对端协商
本端 ID	本端 ID 用于标识本端设备的身份，供对端设备认证自身的合法性。类型与值都需要与对端设备上配置的“对端 ID”参数保持一致，取值包括： ● IPV4地址：本端接口的IPV4地址 ● IPV6地址：本端接口的IPV6地址 ● FQDN： Fully Qualified Domain Name，完全合格域名 ● User-FQDN：本端用户FQDN
对端 ID	对端 ID 用于认证对端设备的身份，此参数需要向对端管理员获取。类型与值都需要与对端设备上设置的“本端 ID”参数保持一致，取值包括： ● IPV4地址：对端接口的IPV4地址 ● IPV6地址：对端接口的IPV6地址 ● FQDN： Fully Qualified Domain Name，完全合格域名 ● User-FQDN：对端用户FQDN

6.14.4.1.4 配置保护的数据流

步骤1 进入“保护的数据流”配置页面。

步骤2 在“保护的数据流”页面点击“新建”，在“新建保护的数据流”页面配置VRF、源IP地址、目的IP地址、协议、动作，具体配置内容如下：

参数	说明
VRF	受保护的数据流按照何种路由转发，取值包括： ● 公网：数据流按照设备的公网路由转发 ● 选择已创建VRF或新创建VRF：数据流按照设备的VPN路由转发，需在弹出的“新建VRF”页面填写该VPN信息，有关新建VRF的配置，请参考VRF联机帮助
源 IP 地址	受保护数据流的源 IP 地址。可以是地址也可以是地址段，如果不限制则填写 any
目的 IP 地址	受保护数据流的目的 IP 地址。可以是地址也可以是地址段，如果不限制则填写 any

参数	说明
协议	受保护数据流的协议类型，取值包括： ● any：允许任意协议受到保护 ● TCP：允许TCP协议受到保护 ● UDP：允许UDP协议受到保护 ● ICMP：允许ICMP协议受到保护
动作	选择对满足上述条件的数据流进行处理，取值包括： ● 保护：表示允许该数据流进入隧道 ● 不保护：表示不允许该数据流进入隧道
触发模式	选择 IPsec 隧道建立的触发方式，取值包括： ● 流量触发：仅在有对应的保护流量通过时才会与对端协商建立IPsec隧道 ● 自动触发：在配置完成后就与对端协商建立IPsec隧道

6.14.4.1.5 高级配置

步骤1 进入“高级配置”页面。

步骤2 在“高级配置”页面，配置IPsec参数，包括了封装模式、安全协议、ESP认证算法、ESP加密算法等，具体配置内容如下：

参数	说明
封装模式	IPsec 报文的封装模式，取值包括： ● 隧道模式：该模式下的安全协议用于保护整个IP数据包 ● 传输模式：该模式下的安全协议用于保护IP协议层以上的数据
安全协议	IPsec 对保护的报文采用何种封装格式以及安全服务，取值包括： ● ESP：提供对报文载荷部分的认证和加密功能，认证能力不如AH ● AH：提供对整个报文的认证能力，但没有加密能力，无法防止窃听 ● AH-ESP：提供对整个报文的认证和加密功能，提高了整体的安全性
ESP 认证算法	ESP 协议的认证算法，安全协议选择 ESP 或者 AH-ESP 需要配置，配置的 ESP 认证算法类型需与对端保持一致，取值包括： ● md5：采用HMAC-MD5-96认证算法 ● sha1：采用HMAC-SHA1-96认证算法 ● sha256：采用HMAC-SHA-256认证算法 ● sha384：采用HMAC-SHA-384认证算法 ● sha512：采用HMAC-SHA-512认证算法 ● sm3：采用HMAC-SM3-96认证算法
ESP 加密算法	ESP 协议的加密算法，安全协议选择 ESP 或者 AH-ESP 需要配置，配置的 ESP 加密算法类型需与对端保持一致，取值包括： ● 3des-cbc：采用CBC模式的3DES算法 ● aes-cbc-128：采用CBC模式的AES算法 ● aes-cbc-192：采用CBC模式的AES算法 ● aes-cbc-256：采用CBC模式的AES算法 ● des-cbc：采用CBC模式的DES算法 ● null：采用NULL加密算法，表示不进行加密 ● sm1-cbc-128：采用CBC模式的SM1算法，本参数仅适用于IKEv1协商

参数	说明
	● sm4-cbc：采用CBC模式的SM4算法，本参数仅适用于IKEv1协商
AH 认证算法	AH 协议的认证算法，安全协议选择 AH 或者 AH-ESP 需要配置，配置的 AH 认证算法类型需与对端保持一致，取值包括： ● md5：采用HMAC-MD5-96认证算法 ● sha1：采用HMAC-SHA1-96认证算法 ● sha256：采用HMAC-SHA-256认证算法 ● sha384：采用HMAC-SHA-384认证算法 ● sha512：采用HMAC-SHA-512认证算法 ● sm3：采用HMAC-SM3-96认证算法，本参数仅适用于IKEv1协商
PFS	PFS（Perfect Forward Secrecy，完善的前向安全性）是一种安全特性，它解决了密钥之间相互无关性的需求。组号越大密钥越长，安全性越高，但计算时间也越长。取值包括： ● group1：采用768-bit Diffie-Hellman组 ● group2：采用1024-bit Diffie-Hellman组 ● group5：采用1536-bit Diffie-Hellman组 ● group14：采用2048-bit Diffie-Hellman组 ● group24：采用2048-bit和256_bit子群Diffie-Hellman组
IPsec SA 生存时间	只要 IPsec SA 存在时间或者保护流量达到设定值，该条 IPsec SA 就会失效，取值包括： ● 基于时间：IPsec SA存在时间的设定值 ● 基于流量：IPsec SA保护流量的设定值
IPsec SA 空闲超时时间	在指定时间内未接收到需要保护的流量，则删除 IPsec SA
DPD 检测	Dead Peer Detection，对等体存活检测，在超时重传时间内主动检测对端是否存活，取值包括： ● 按需检测：指定按需探测模式，根据流量来探测对端是否存活 ● 按时检测：指定定时探测模式，按照触发IKE DPD探测的时间间隔定时探测对端是否存活 ● 检测时间间隔：指定触发IKE DPD探测的时间间隔 ● 重传时间间隔：指定DPD报文的重传时间间隔
内网 VRF	IPsec 对等体的地址包含在哪种路由表中，取值包括： ● 公网：IPsec对等体的地址包含在公网路由表 ● 选择已创建VRF或新创建VRF：IPsec对等体的地址包含在VPN路由表，需在弹出的“新建VRF”页面填写该VPN信息，有关新建VRF的配置，请参考VRF联机帮助
QoS 预分类	开启后 QoS 基于原始报文的 IP 头部 QoS 信息进行分类，关闭则基于封装后的外层 IP 头部 Qos 信息进行分类

6.14.4.1.6 安全策略配置

步骤1 进入“安全策略”配置页面。

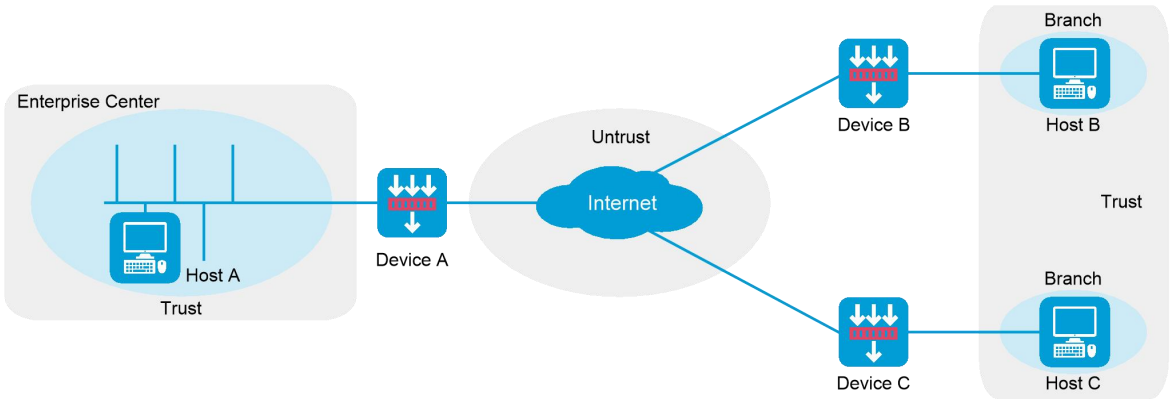
步骤2　在“安全策略”配置页面，选择是否自动生成安全策略，自动生成安全策略则会自动生成放通IPsec报文的安全策略。

步骤3　单击“确定”按钮，完成IPsec策略配置。

6.14.4.2　点到多点IPsec配置指南

6.14.4.2.1　背景信息

IPsec按照实际需求的不同存在两种组网方式，分别是点到点和点到多点的组网方式。这两种组网方式的配置方式存在差异。点到多点组网方式中分支的配置和点到点组网方式中设备的配置一致，下面介绍点到多点IPsec中心节点的配置。点到多点IPsec典型组网如下图所示，Host A位于企业总部，Host B和Host C分别位于该企业的分部。可以通过建立Device A到Device B和Device A到Device C点到多点IPsec隧道，对Host A与Host B、Host A与Host C之间通过Internet传输的数据流分别进行安全保护。



6.14.4.2.2　基本配置

步骤1　选择“网络 > VPN > IPsec > 策略”，单击 “新建”按钮，进入“新建IPsec策略”页面。

步骤2　在“新建IPsec策略”页面，选择“设备角色”为“中心节点”，点到多点IPsec隧道的具体配置内容如下：

参数	说明
策略名称	IPsec 策略的名称，一个设备可以存在多条策略，策略名称用于本地区分 IPsec 策略
优先级	IPsec 策略的顺序号，一个 IPsec 策略是若干具有相同名称、不同顺序号的 IPsec 策略表项的集合。在同一个 IPsec 策略中，顺序号越小的 IPsec 策略表项优先级越高，流量需要匹配 IPsec 策略时会从顺序号小的 IPsec 策略开始

参数	说明
	匹配，匹配到了就会进入 IPsec 隧道转发
设备角色	表示该设备在 IPsec 组网中的角色，取值包括： ● 对端/分支节点：点到多点组网的分支设备是分支节点，点到点组网的设备是对等节点 ● 中心节点：点到多点组网的中心设备是中心节点
别名	IPsec 策略的别名
IP 地址类型	建立 IPsec 隧道的本端地址类型，取值包括： ● IPv4：地址类型为IPv4 ● IPv6：地址类型为IPv6
接口	指定应用该 IPsec 策略的接口。
本端地址	指定应用该 IPsec 策略接口的 IP 地址。
描述	IPsec 策略的描述信息，方便网络管理人员了解策略的使用目的

6.14.4.2.3 IKE策略配置

步骤1 进入“IKE策略”配置页面。

步骤2 在“IKE策略”配置页面，配置协商模式、认证方式、预共享密钥等，具体配置内容如下：

参数	说明
协商模式	IKE 协商模式，取值包括： ● 主模式：强制使用主模式协商，主模式更安全 ● 野蛮模式：强制使用野蛮模式协商，野蛮模式更快速 ● 国密主模式：必须使用RSA-DE或者SM2-DE数字信封方式认证的认证方式，协商方式与主模式一致，安全性更高
预共享密钥	分支节点认证方式为预共享密钥时需要配置,需要保证点到多点对等体的预共享密钥一致
PKI 域	分支节点选择认证方式为数字认证需要配置。PKI 是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，有关 PKI 的配置，请参考 PKI 联机帮助
证书访问策略	分支节点选择认证方式为数字认证可以配置。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，有关证书访问策略配置，请参考 PKI 联机帮助
IKE 提议	IKE 定义了一套属性数据来描述 IKE 第一阶段使用怎样的参数来与对端进行协商，这套属性称为 IKE 提议，取值如下： ● 新建IKE提议：新建IKE提议，参数需与对端设备保持一致 ● NONE：不配置IKE提议，使用默认提议与对端协商
本端 ID	本端 ID 用于标识本端设备的身份，供对端设备认证自身的合法性。需要与对端设备上设置的“对端 ID”参数保持一致

参数	说明
	● IPV4地址：本端接口的IPV4地址 ● IPV6地址：本端接口的IPV6地址 ● FQDN： Fully Qualified Domain Name，完全合格域名 ● User-FQDN：本端用户FQDN

6.14.4.2.4 高级配置

步骤1 进入“高级配置”页面。

步骤2 在“高级配置”页面，配置IPsec参数，包括了封装模式、安全协议、ESP认证算法、ESP加密算法等，具体配置内容如下：

参数	说明
封装模式	IPsec 报文的封装模式，取值包括： ● 隧道模式：该模式下的安全协议用于保护整个IP数据包 ● 传输模式：该模式下的安全协议用于保护IP协议层以上的数据
安全协议	IPsec 对保护的报文采用何种封装格式以及安全服务，取值包括： ● ESP：提供对报文载荷部分的认证和加密功能，认证能力不如AH ● AH：提供对整个报文的认证能力，但没有加密能力，无法防止窃听 ● AH-ESP：提供对整个报文的认证和加密功能，提高了整体的安全性
ESP 认证算法	ESP 协议的认证算法，安全协议选择 ESP 或者 AH-ESP 需要配置，配置的 ESP 认证算法类型需与对端保持一致，取值包括： ● md5：采用HMAC-MD5-96认证算法 ● sha1：采用HMAC-SHA1-96认证算法 ● sha256：采用HMAC-SHA-256认证算法 ● sha384：采用HMAC-SHA-384认证算法 ● sha512：采用HMAC-SHA-512认证算法 ● sm3：采用HMAC-SM3-96认证算法
ESP 加密算法	ESP 协议的加密算法，安全协议选择 ESP 或者 AH-ESP 需要配置，配置的 ESP 加密算法类型需与对端保持一致，取值包括： ● 3des-cbc：采用CBC模式的3DES算法 ● aes-cbc-128：采用CBC模式的AES算法 ● aes-cbc-192：采用CBC模式的AES算法 ● aes-cbc-256：采用CBC模式的AES算法 ● des-cbc：采用CBC模式的DES算法 ● null：采用NULL加密算法，表示不进行加密 ● sm1-cbc-128：采用CBC模式的SM1算法，本参数仅适用于IKEv1协商 ● sm4-cbc：采用CBC模式的SM4算法，本参数仅适用于IKEv1协商
AH 认证算法	AH 协议的认证算法，安全协议选择 AH 或者 AH-ESP 需要配置，配置的 AH 认证算法类型需与对端保持一致，取值包括： ● md5：采用HMAC-MD5-96认证算法 ● sha1：采用HMAC-SHA1-96认证算法 ● sha256：采用HMAC-SHA-256认证算法 ● sha384：采用HMAC-SHA-384认证算法

参数	说明
	● sha512：采用HMAC-SHA-512认证算法 ● sm3：采用HMAC-SM3-96认证算法，本参数仅适用于IKEv1协商
PFS	PFS（Perfect Forward Secrecy，完善的前向安全性）是一种安全特性，它解决了密钥之间相互无关性的需求。组号越大密钥越长，安全性越高，但计算时间也越长。取值包括： ● group1：采用768-bit Diffie-Hellman组 ● group2：采用1024-bit Diffie-Hellman组 ● group5：采用1536-bit Diffie-Hellman组 ● group14：采用2048-bit Diffie-Hellman组 ● group24：采用2048-bit和256_bit子群Diffie-Hellman组
IPsec SA 生存时间	只要 IPsec SA 存在时间或者保护流量达到设定值，该条 IPsec SA 就会失效，取值包括： ● 基于时间：IPsec SA存在时间的设定值 ● 基于流量：IPsec SA保护流量的设定值
IPsec SA 空闲超时时间	在指定时间内未接收到需要保护的流量，则删除 IPsec SA
DPD 检测	Dead Peer Detection，对等体存活检测，在超时重传时间内主动检测对端是否存活，取值包括： ● 按需检测：指定按需探测模式，根据流量来探测对端是否存活 ● 按时检测：指定定时探测模式，按照触发IKE DPD探测的时间间隔定时探测对端是否存活 ● 检测时间间隔：指定触发IKE DPD探测的时间间隔 ● 重传时间间隔：指定DPD报文的重传时间间隔
内网 VRF	IPsec 对等体的地址包含在哪种路由表中，取值包括： ● 公网：IPsec对等体的地址包含在公网路由表 ● 选择已创建VRF或新创建VRF：IPsec对等体的地址包含在VPN路由表，需在弹出的“新建VRF”页面填写该VPN信息，有关新建VRF的配置，请参考VRF联机帮助
QoS 预分类	开启后 QoS 基于原始报文的 IP 头部 QoS 信息进行分类，关闭则基于封装后的外层 IP 头部 Qos 信息进行分类

6.14.4.2.5 安全策略配置

步骤1 进入“安全策略”配置页面。

步骤2 进入“安全策略”配置页面选择是否自动生成安全策略，自动生成安全策略则会自动生成放通IPsec报文的安全策略。

步骤3 单击“确定”按钮，完成IPsec策略配置。

6.14.4.3 配置IKE提议

6.14.4.3.1 背景信息

IKE定义了一套属性数据来描述IKE第一阶段使用的参数，用于和对端进行协商。用户可以创建多条不同优先级的IKE提议。协商双方必须至少有一条匹配的IKE提议才能协商成功。

6.14.4.3.2 新建IKE提议

步骤1 选择“网络 > VPN > IPsec > IKE提议”，单击“新建”按钮，进入“新建IKE提议”页面。

步骤2 在“新建IKE提议”页面，配置优先级、认证方式、认证算法、加密算法、DH、IKE SA生存周期，具体配置内容如下：

参数	说明
优先级	IKE 提议的优先级，协商响应方以对端发送的 IKE 提议优先级，按照从高到低的顺序与本端所有的 IKE 提议进行匹配，直到找到一个匹配的提议来使用。匹配的 IKE 提议将被用来建立 IKE SA
认证方式	IKE 提议使用的认证方式，取值包括： ● 预共享密钥：指定认证方法为预共享密钥方法 ● RSA数字签名：指定认证方法为RSA数字签名方法 ● DSA数字签名：指定认证方法为DSA数字签名方法 ● RSA数字信封：指定认证方法为RSA数字信封方法 ● SM2数字信封：指定认证方法为SM2数字信封方法
认证算法	IKE 提议使用的认证算法，取值包括： ● md5：指定认证算法为HMAC-MD5 ● sha1：指定认证算法为HMAC-SHA1 ● sha256：指定认证算法为HMAC-SHA256 ● sha384：指定认证算法为HMAC-SHA384 ● sha512：指定认证算法为HMAC-SHA512 ● sm3：指定认证算法为HMAC-SM3
加密算法	IKE 提议使用的加密算法，取值包括： ● 3des-cbc：指定IKE安全提议采用的加密算法为CBC模式的3DES算法，3DES算法采用168比特的密钥进行加密 ● aes-cbc-128：指定IKE安全提议采用的加密算法为CBC模式的AES算法，AES算法采用128比特的密钥进行加密 ● aes-cbc-192：指定IKE安全提议采用的加密算法为CBC模式的AES算法，AES算法采用192比特的密钥进行加密 ● aes-cbc-256：指定IKE安全提议采用的加密算法为CBC模式的AES算法，AES算法采用256比特的密钥进行加密 ● des-cbc：指定IKE安全提议采用的加密算法为CBC模式的DES算法，DES算法采用56比特的密钥进行加密 ● sm1-cbc-128：指定IKE安全提议采用的加密算法为CBC模式的SM1算法，SM1算法采用128比特的密钥进行加密 ● sm4-cbc：指定IKE安全提议采用的加密算法为CBC模式的SM4算法，SM4算法采用128比特的密钥进行加密
DH	IKE 一阶段密钥协商时所使用的 DH 密钥交换参数，取值包括：

参数	说明
	● DH group1：指定阶段1密钥协商时采用768-bit的Diffie-Hellman group ● DH group2：指定阶段1密钥协商时采用1024-bit的Diffie-Hellman group ● DH group5：指定阶段1密钥协商时采用1536-bit的Diffie-Hellman group ● DH group14：指定阶段1密钥协商时采用2048-bit的Diffie-Hellman group ● DH group19：指定阶段1密钥协商时采用256-bit的Diffie-Hellman group ● DH group20：指定阶段1密钥协商时采用384-bit的Diffie-Hellman group ● DH group24：指定阶段1密钥协商时采用含256-bit的sub-group的2048-bit Diffie-Hellman group
IKE SA生存周期	IKE提议的IKE SA存活时间

步骤3　单击“确定”按钮，完成IKE提议配置。

6.14.4.4　配置隧道信息

在隧道信息页面，可以查看已建立的IPsec的隧道信息，可以删除指定的隧道，或者删除所有隧道。

隧道信息页面的具体配置步骤如下：

步骤1　选择“网络 > VPN > IPsec > 隧道信息”。

步骤2　在“隧道信息”页面单击<清除所有隧道>按钮，单击“确定”按钮后，可以删除所有隧道。

步骤3　在“隧道信息”页面单击<根据对端IP地址清除隧道>按钮，进入“根据对端IP地址清除隧道”页面，具体配置内容如下：

参数	说明
网络类型	对端IP地址类型，取值包括： ● IPv4：地址类型为IPv4 ● IPv6：地址类型为IPv6
对端地址	指定IPsec隧道的对端IP地址

步骤4　单击“确定”按钮，可以删除指定的隧道

6.14.4.5　高级设置

6.14.4.5.1　IKE高级设置

步骤1　选择“网络 > VPN > IPsec > 高级设置”，进入“高级设置”页面。

步骤2　在“IKE”页面，配置DPD检测、检测方式、检测时间间隔、重传时间间隔等，具体配置内容如下：

参数	说明

参数	说明
DPD 检测	本功能用于检测对端是否存活
检测方式	DPD 的检测方式，取值包括： ● 按需检测：在本端需要发送报文时触发探测 ● 定时检测：定时触发探测
检测时间间隔	触发 IKE DPD 探测的时间间隔，有如下两种方式： ● 对于按需探测模式，指定经过多长时间没有从对端收到IPsec报文，则触发一次DPD探测 ● 对于定时探测模式，指触发一次DPD探测的时间间隔
重传时间间隔	DPD 报文的重传时间间隔
开启针对无效 IPsec SPI 的 IKE SA 恢复功能	SA 由 SPI 唯一标识，接收方根据 IPsec 报文中的 SPI 在 SA 数据库中查找对应的 IPsec SA，若接收方找不到处理该报文的 IPsec SA，则认为此报文的 SPI 无效。如果接收端当前存在 IKE SA，则会向对端发送删除对应 IPsec SA 的通知消息，如果接收端当前不存在 IKE SA，就不会触发本端向对端发送删除 IPsec SA 的通知消息，如果开启了 IPsec 无效 SPI 恢复 IKE SA 功能，就会触发本端与对端协商新的 IKE SA 并发送删除消息给对端，从而使链路恢复正常。通常情况下，建议关闭针对无效 IPsec SPI 的 IKE SA 恢复功能
从本端证书的主题中获取本端身份信息	设备使用由本端证书中获得的身份信息参与数字签名认证
发送 Keepalive 报文的时间间隔	IKE SA 向对端发送 IKE Keepalive 报文的时间间隔
Keepalive 报文的超时时间	本端等待对端发送 IKE Keepalive 报文的超时时间
发送 NAT Keepalive 报文的时间间隔	仅需在 NAT 之后的设备上进行配置。NAT 之后的 IKE 网关设备需要定时向 NAT 之外的 IKE 网关设备发送 NAT Keepalive 报文，以便维持 NAT 设备上对应的 IPsec 流量的会话存活，从而让 NAT 之外的设备可以访问 NAT 之后的设备。需要确保配置的时间小于 NAT 设备上会话表项的存活时间
IKE SA 最大数	允许建立的 IKE SA 的最大数
同时处于协商状态的 IKE SA 和 IPsec SA 的最大总和数	同时处于协商状态的 IKE SA 和 IPsec SA 的最大总和数，建议参考设备实际性能进行配置，以充分利用设备处理能力
本端 ID	本端身份信息，用于在 IKE 认证协商阶段向对端标识自己的身份，取值包括： ● NONE：表示未配置本端ID，此时使用系统视图下**ike identity**命令配置的身份信息作为本端身份信息。若没有配置，则使用IP地址标识本端的

参数	说明
	身份，该IP地址为IPsec安全策略应用的接口的IP地址 ● IPv4地址：标识本端身份的IPv4地址 ● IPv6地址：标识本端身份的IPv6地址 ● FQDN：标识本端身份的FQDN名称 ● User-FQDN：标识本端身份的user FQDN名称 ● DN：使用从本端数字证书中获得的DN名作为本端身份

6.14.4.5.2 IPsec高级设置

步骤1 进入“IPsec”配置页面。

步骤2 在“IPsec”配置页面，配置根据保护数据流的范围检查解封装后的IPsec报文、记录报文日志、开启抗重放检测功能等，具体配置内容如下：

参数	说明
根据保护数据流的范围检查解封装后的 IPsec 报文	开启该功能后可以保证 ACL 检查不通过的报文被丢弃，从而提高网络安全性
记录报文日志	开启 IPsec 报文日志记录功能后，设备会在丢弃 IPsec 报文的情况下输出相应的日志信息
开启抗重放检测功能	开启 IPsec 抗重放检测功能，将检测到的重放报文在解封装处理之前丢弃，可以降低设备资源的消耗
抗重放窗口宽度	抗重放检测功能允许接收报文的窗口宽度
开启冗余备份功能	开启冗余备份功能后，当发生主备切换时，可以保证主备 IPsec 流量不中断和抗重放保护不间断
分片处理	IPsec 分片处理，有如下两种方式： ● 加密前分片：设备会在报文分片前判断报文在经过IPsec封装之后大小是否会超过发送接口的MTU值，如果该报文的DF位被置位。那么设备会丢弃该报文，并发送ICMP差错控制报文 ● 加密后分片：无论报文封装后大小是否超过发送接口的MTU值，设备会直接对其先进行IPsec封装处理，再由后续业务对其进行分片
设置外层 IP 头的 DF 位	本功能用来为所有接口设置 IPsec 封装后外层 IP 头的 DF 位，取值包括： ● CLEAR：表示清除外层IP头的DF位，IPsec封装后的报文可被分片 ● COPY：表示外层IP头的DF位从原始报文IP头中拷贝 ● SET：表示设置外层IP头的DF位，IPsec封装后的报文不能分片
IPsec SA 空闲超时时间	全局 IPsec SA 空闲超时时间
IPsec SA 生存时	只要 IPsec SA 存在时间或者保护流量达到设定值，该条 IPsec SA 就会失效

参数	说明
间	
基于时间	IPsec SA 存在时间的设定值
基于流量	IPsec SA 保护流量的设定值
IPsec 隧道最大数	本端允许建立 IPsec 隧道的最大数，内存充足时可以设置较大的数值，提高 IPsec 的并发性能；内存不足时可以设置较小的数值，降低 IPsec 占用内存的资源

6.14.4.5.3 量子密钥高级设置

步骤1 进入“量子密钥”配置页面。

步骤2 在“量子密钥”配置页面，配置服务器地址类型、服务器地址、设备唯一入网标识等，具体配置内容如下：

参数	说明
开启量子加密	开启国盾量子加密功能后，IPsec 将使用国盾量子服务器提供的对称密钥，对需要 IPsec 保护的数据进行加密保护，进一步提升 IPsec 业务的安全性
服务器地址	国盾量子服务器的 IP 地址
服务器端口号	国盾量子服务器的端口号
设备唯一入网标识	设备唯一入网标识由国盾量子服务器统一分配，每个设备一个，且全网唯一。设备唯一入网标识需要联系国盾量子服务器的管理员获取
身份认证密钥	身份认证密钥用于国盾量子服务器验证设备身份，与设备唯一入网标识一一对应。身份认证密钥需要联系国盾量子服务器的管理员获取
解密密钥	国盾量子密钥的解密密钥，解密密钥需要联系国盾量子服务器的管理员获取

步骤3 单击“应用”按钮，完成高级设置配置。

6.15 ADVPN

本帮助主要介绍以下内容：

- 特性简介
  - ADVPN组网结构

6.15.1 特性简介

ADVPN（Auto Discovery Virtual Private Network，自动发现虚拟专用网络）是一种基于VAM（VPN Address Management，VPN地址管理）协议的动态VPN技术。VAM协议负责收集、维护和分发动态变化的公网地址等信息，采用Client/Server模型。ADVPN网络中的节点（称为ADVPN节点）作为VAM Client。当公网地址变化时，VAM Client将当前公网地址注册到VAM Server。ADVPN节点通过VAM协议从VAM Server获取另一端ADVPN节点的当前公网地址，从而实现在两个节点之间动态建立跨越IP核心网络的ADVPN隧道。

在企业网各分支机构使用动态地址接入公网的情况下，可以利用ADVPN在各分支机构间建立VPN。

6.15.1.1 ADVPN组网结构

ADVPN通过ADVPN域区分不同的VPN网络，ADVPN域由域ID来标识。属于同一个VPN的VAM Client需要规划到相同的ADVPN域中，且一个VAM Client只能属于一个ADVPN域；VAM Server可以同时为多个ADVPN域服务，管理多个ADVPN域的VAM Client。

ADVPN节点分为如下两类：

- Hub：ADVPN网络的中心设备。它是路由信息交换的中心。
- Spoke：ADVPN网络的分支设备，通常是企业分支机构的网关。该节点不会转发收到的其它ADVPN节点的数据。

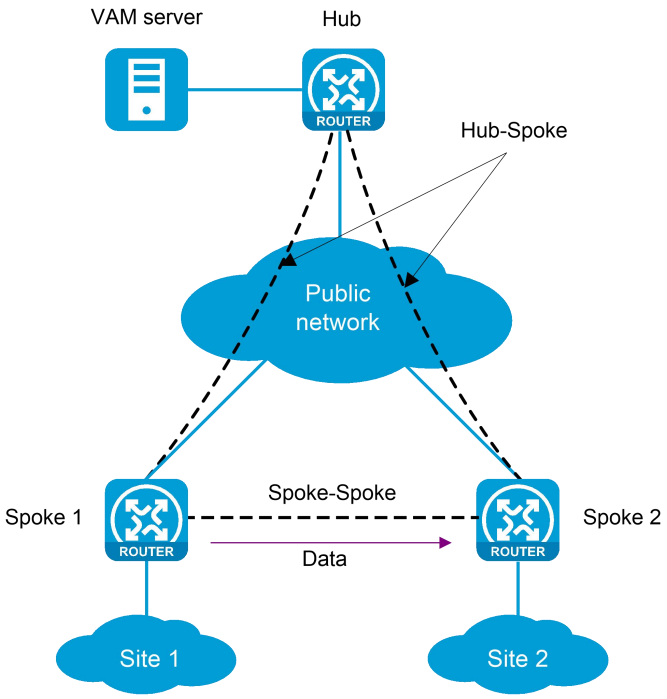
根据数据转发方式的不同，ADVPN组网结构分为如下两种：

- Full-Mesh（全互联）网络：Spoke和Spoke之间可以建立隧道直接通信。
- Hub-Spoke网络：Spoke之间不能建立隧道直接通信，只能通过Hub转发数据。

当一个ADVPN域中的ADVPN节点数目较多时，由于某些原因（如动态路由协议邻居数限制等），Hub无法管理全部的ADVPN节点。此时，可以将ADVPN网络划分为多个Hub组，每个Hub组中包含一个或多个Hub，及一部分Spoke节点，以减轻Hub节点的负担。

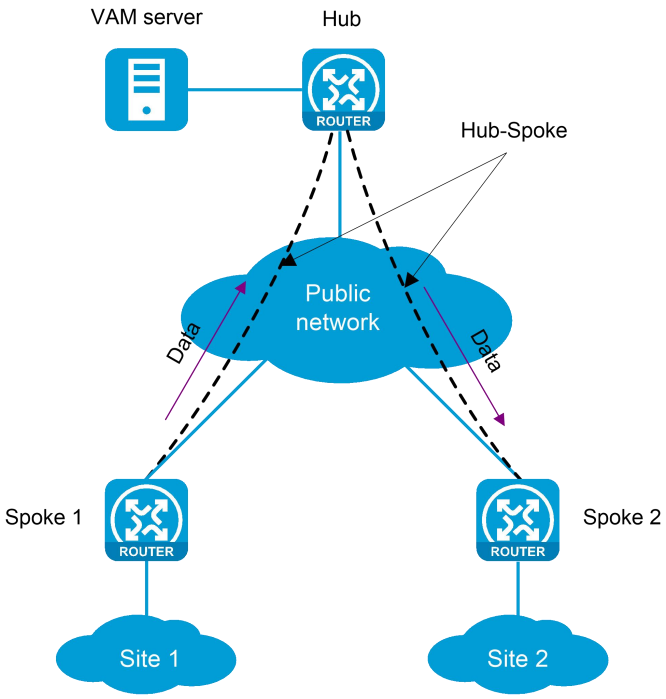
6.15.1.1.1 Full-Mesh网络

如下图所示，在Full-Mesh网络中，Spoke向VAM Server注册后获得Spoke所属ADVPN域所在Hub组中Hub的信息，并与Hub建立永久的ADVPN隧道。当两个Spoke之间有数据报文交互时，Spoke从VAM Server获取对端Spoke的公网地址，并在Spoke之间直接建立隧道。Spoke之间的隧道是动态的，当在一段时间（Spoke-Spoke隧道空闲超时时间）内没有数据报文交互时，则删除该隧道。



6.15.1.1.2 Hub-Spoke网络

如下图所示，在Hub-Spoke网络中，Spoke向VAM Server注册后获得Spoke所属ADVPN域所在Hub组中Hub的信息，并与Hub建立永久的ADVPN隧道。两个Spoke之间有数据报文交互时，该报文通过Hub转发，不会在Spoke之间建立隧道。Hub既作为路由信息交换的中心，又作为数据转发的中心。



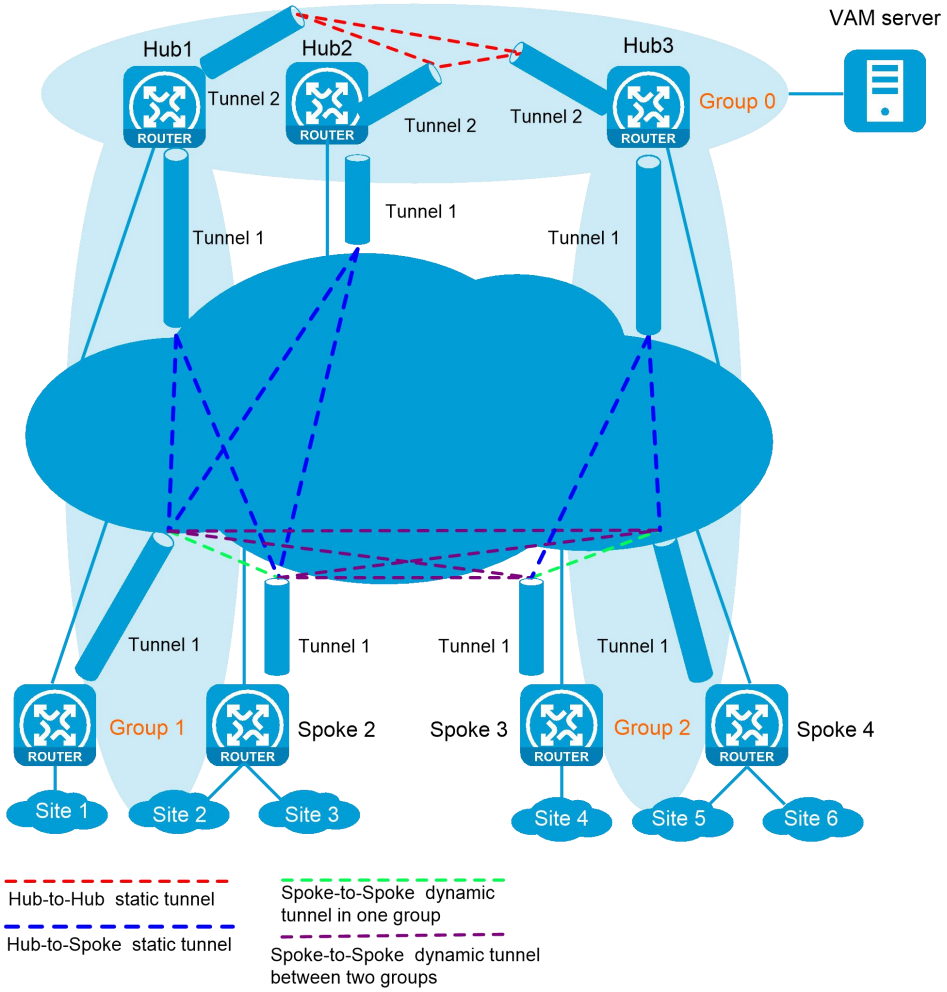
6.15.1.1.3 划分多个Hub组网络

如下图所示，划分多个Hub组网络中，Hub组的划分方式为：

- 所有Hub必须属于同一个Hub组，该Hub组作为骨干区域。骨干区域采用Full-Mesh组网，即Hub向VAM Server注册后获得骨干区域中所有Hub的信息，并在每两个Hub之间都建立永久的ADVPN隧道。
- 将Spoke部署到除骨干区域外的其他Hub组中。这些Hub组内至少有1个Hub，可以使用Full-Mesh组网也可以使用Hub-Spoke组网。Spoke向VAM Server注册后获得Spoke所属ADVPN域所在Hub组中Hub的信息，并与Hub建立永久的ADVPN隧道。一个Hub组内的Spoke只与本组的Hub建立ADVPN隧道，不与其他Hub组的Hub建立ADVPN隧道。

同一个Hub组内，隧道建立方式和数据转发方式由其组网方式决定。不同Hub组间，数据需要通过本组的Hub转发到目的组的Hub，再由目的组Hub转发到对应的Spoke。

为了减少Hub跨组转发数据时的压力，可以允许不同组的Spoke直接建立隧道，但该隧道是动态的，当在一段时间（Spoke-Spoke隧道空闲超时时间）内没有数据报文交互时，则删除该隧道。



6.15.1.2 ADVPN工作机制

ADVPN对VAM Server和VAM Client的地址具有一定要求：

- VAM Server只需要具有公网地址，且该公网地址必须静态配置，不能动态变化。
- VAM Client需要具有公网地址和私网地址。公网地址是VAM Client连接IP核心网络的接口的地址，既可以静态配置也可以动态获取。私网地址是ADVPN隧道接口的地址，必须静态配置。在同一个ADVPN域内，同一个Hub组内的VAM Client的私网地址应该属于同一个网段。

ADVPN的关键是通过VAM Client的私网地址获取动态变化的公网地址，以便建立ADVPN隧道、转发报文。ADVPN的工作过程分为连接初始化、注册、隧道建立、路由学习和报文转发四个阶段，下面对这四个阶段做简单说明。

- 连接初始化阶段：VAM Client和VAM Server之间协商完整性验证、加密算法及密钥。
- 注册阶段：VAM Client向VAM Server进行身份认证，并注册相关信息。
- 隧道建立阶段：同一个Hub组内，每个Spoke和每个Hub之间都要建立永久隧道，任意两个Hub

之间也要建立永久隧道。

- 路由学习和报文转发：路由学习通过路由协议实现，路由协议决定组网方式，组网方式决定报文转发方法。

6.15.1.3 穿越NAT的ADVPN隧道

当隧道发起方在NAT网关后侧时，则可以建立穿越NAT的Spoke-Spoke隧道；如果隧道接收方在NAT网关后侧，则数据包要由Hub转发，直到接收方发起隧道建立请求。如果双方都在NAT网关后侧，则它们都无法与对方建立隧道，所有的数据包都只能从Hub转发。

如果NAT网关采用Endpoint-Independent Mapping（不关心对端地址和端口转换模式），隧道接收方在NAT网关后侧时，也可以建立穿越NAT的Spoke-Spoke隧道。

6.15.2 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。

6.15.3 使用限制和注意事项

- 在配置好VAMC之后，请将隧道接口加入安全域，并配置到其他VAMC的安全策略，否则网络不通。
- 在同一个ADVPN域中，VAMS和VAMC的预共享密钥要一致。
- 在同一个ADVPN域中，所有Tunnel接口的Keepalive报文发送周期及最大发送次数必须一致。
- 除IP地址外，备VAMS的ADVPN配置与主VAMS相同。
- VAMS的监听端口号与VAMC上指定的VAMS的端口号必须一致。
- VAMC的私网地址需要与VAMS中Hub组划分的私网地址保持一致，否则注册失败。
- 在认证VAMC身份的时候，VAMS会根据VAMC提交的信息对认证和加密算法进行选择，若无法匹配成功，则VAMC的注册将会失败。
- 在同一个Hub组中，OSPF的网络类型要保持一致，否则可能导致网络不通。
- 当ADVPN隧道采用GRE封装模式并使用GRE key对报文进行验证时，则同一Hub组内的其他VAMC必须使用相同的GRE key。
- 如果一个设备上配置了多个使用GRE封装的ADVPN隧道接口，且隧道的源端地址或源接口相同时，不同GRE封装的ADVPN隧道接口的GRE Key必须不同。

6.15.4 配置指南

在实际进行配置之前，请先规划加密、认证相关信息以及组网信息，包括：

- ADVPN域

- VAMS公网地址、预共享密钥、加密和认证方式
- VAMC公网、私网地址及其所连接的私网信息

在规划好上述信息之后，则可以在VAMS和VAMC上进行相关配置了。

6.15.4.1 配置VAMS

VAMS 功能的支持情况与设备的款型有关，请以设备的实际界面为准。

VAMS的具体配置步骤如下：

步骤1 选择“网络 > VPN > ADVPN > VAMS”。

步骤2 在“VAMS”页面单击<新建>按钮，进入“新建VAMS”页面。

步骤3 新建VAMS，具体配置内容如下表所示：

参数	说明
ADVPN 域	VAMS 所属的 ADVPN 域，不可重复
ID	VAMS 的编号，不可重复
预共享密钥	VAMS 的预共享密钥，用于与 VAMC 进行连接初始化。如果选择对后续的报文进行加密和验证，则预共享密钥还用来生成验证和加密后续报文的连接密钥
身份认证方式	VAMS 认证 VAMC 身份的方式
ISP 域	当认证方式为“PAP”或“CHAP”时，此项可以输入，指定具体的 ISP 域对 VAMC 进行验证。详细信息请参见“ISP 域”
Hub 组	当前页面显示已有的 Hub 组，并提供新建、编辑和删除功能。
报文认证算法	VAMS 和 VAMC 进行通信时采用的认证算法。算法在配置中的出现顺序决定其使用优先级。配置中越靠前的验证算法，其优先级越高。其中 NONE 表示不认证，直接通过，所以若要选择 NONE，请将其放在所有算法之后，否则 NONE 之后的算法不生效 VAMS 在与 VAMC 协商时，从 VAMC 支持的验证算法列表中选择 VAMS 上配置最靠前的算法作为协商结果，若没有匹配成功，则拒绝连接
报文加密算法	VAMS 和 VAMC 进行通信时采用的加密算法。优先级和选择方式与报文认证算法相同
Keepalive 报文：时间间隔	此参数将决定 VAMC 向 VAMS 发送 Keepalive 报文的时间间隔，当此参数发生改变时，则修改后的参数只对新注册的 VAMC 生效，已经注册的 VAMC 不受影响
Keepalive 报文：	此参数将决定 VAMC 向 VAMS 发送 Keepalive 报文的重发次数，当此参数发生

参数	说明
重发次数	改变时，则修改后的参数只对新注册的 VAMC 生效，已经注册的 VAMC 不受影响
VAM 报文重发间隔	VAMS 重发报文的时间间隔
启用 VAMS	是否启用 VAMS，勾选为启用

参数	说明
组名	Hub 组的名称
直连隧道规则	跨 Hub 组建立 Spoke-Spoke 隧道的规则，分为三种选项：NONE 表示不可以建立 Spoke-Spoke 隧道，ACL 表示根据具体的 ACL 规则允许或禁止建立 Spoke-Spoke 隧道，All 表示没有限制，可以任意建立 Spoke-Spoke 隧道
Hub	当前页面显示本 Hub 组中已存在的 Hub，并提供新建、编辑和删除功能。关于新建和编辑功能，请注意，当 Hub 在 NAT 网关之后时，“公网地址”和“ADVPN 端口”两项需要填写，具体填写为 Hub 经过 NAT 转换后的公网地址和端口
Spoke	当前页面显示本 Hub 组中已存在的 Spoke，并提供新建和删除功能。单击“新建”按钮配置 Spoke 的私网起始地址和私网结束地址

步骤4　在VAMS页面，可以开启、关闭、编辑已有的VAMS。

6.15.4.2　配置VAMC

VAMC的具体配置步骤如下：

步骤1　选择“网络 > VPN > ADVPN > VAMC”。

步骤2　在“VAMC”页面单击<新建>按钮，进入“新建VAMC”页面。

步骤3　在基本配置页签，具体配置内容如下表所示：

参数	说明
VAMC 名称	表示 VAMC 的名称，不可重复
ADVPN 域	VAMC 所属的 ADVPN 域
预共享密钥	VAMC 和 VAMS 进行连接初始化时使用的密钥，如果选择对后续的报文进行加密和验证，则预共享密钥还用来生成验证和加密后续报文的连接密钥
认证用户名	VAMC 向 VAMS 注册时使用的用户名和密钥
认证密钥	VAMC 向 VAMS 注册时使用的密钥
启用 VAMC	是否开启 VAMC，勾选为启用

参数	说明
超时静默时间	VAMC 在与 VAMS 连接超时（指 Keepalive 超时）后，会进入静默状态，此时 VAMC 不处理任何报文。当静默时间到达后，VAMC 将重新发起连接请求
VAM 报文重发间隔	VAMC 向 VAMS 发送请求报文后，如果在指定的时间间隔内没有收到响应报文，VAMC 将重新发送请求报文
VAM 报文重发次数	VAMC 向 VAMS 重新发送请求报文的次数
主/备服务器地址	主/备 VAMS 的公网地址，需要静态分配
主/备服务器端口	主/备 VAMS 的监听端口号
模式	ADVPN 隧道的封装模式
隧道接口 ID	ADVPN 隧道接口的编号
隧道私网地址	ADVPN 隧道接口的私网地址以及子网掩码
隧道公网地址	ADVPN 隧道接口的公网地址，可以为隧道源接口的地址，也可以手动配置
VRF	ADVPN 隧道使用的虚拟路由转发表，具体配置请参见“VRF”
OSPF 路由协议	ADVPN 隧道采用的 OSPF 路由协议，具体配置请参见“OSPF”
网络类型	在选择 OSPF 实例后可见，表示 OSPF 协议的网络类型，将决定 Hub 组的组网方式
DR 优先级	在选择 OSPF 实例后可见，表示 OSPF 协议中当前节点的 DR 优先级
GRE key	当使用 GRE 封装模式时，使用的 GRE 验证密钥。不配置的情况下，表示不使用 GRE key 进行验证，具体请参见“GRE”
开启报文校验和功能	当使用 GRE 封装模式时，开启 GRE 校验和验证功能来检查报文的完整性，具体请参见“GRE”
源 UDP 端口号	当使用 UDP 封装时，报文的源端口号。若勾选了兼容 ADVPN V0，则该参数不能和其他隧道的源端口号相同
注册私网信息列表	VAMC 向 VAMS 注册 ADVPN 隧道的私网信息。当其他 VAMC 向 VAMS 解析私网报文目的地址时，如果解析的地址属于注册私网，则 VAMS 将注册 VAMC 的节点信息返回给查询方 当前页面显示已有私网，并提供新建、编辑和删除功能。关于新建和编辑功能，请注意，弹出框中的“优先级”，建议高于其他动态路由协议，且低于静态路由。优先级数值越大，优先级越低
兼容 ADVPN V0	是否兼容 ADVPN V0 版本
隧道静默时间	ADVPN 隧道建立失败的静默时间

参数	说明
隧道空闲超时时间	Spoke-Spoke 类型 ADVPN 隧道的空闲超时时间，如果在空闲超时时间内，Spoke-Spoke 类型 ADVPN 隧道上没有数据传输，则断开该隧道
封装后报文的 TOS	ADVPN 隧道报文的 TOS 值
封装后报文的 TTL	ADVPN 隧道报文的 TTL 值
封装后报文不允许分片	设置封装后隧道报文的 DF 标志，勾选表示不允许分片
IPsec 功能	是否开启 IPsec 功能，勾选为开启
名称	IPsec 策略的名称
IKE 配置	表示以下多个配置为 IKE 相关配置
认证方式	IKE 认证方式，有“预共享密钥”和“数字证书认证”两种方式
预共享密钥	在 IKE 认证方式为“预共享密钥”的情况下，对应的密钥
PKI 域	在 IKE 认证方式为“数字证书认证”的情况下，证书所属的 PKI 域，具体配置请参见“PKI”
证书访问策略	在 IKE 认证方式为“数字证书认证”的情况下，证书的访问控制策略，具体配置请参见“PKI”
IKE 提议	IPsec 策略引用的 IKE 提议，具体配置请参见“IPsec”
协商模式	IKE 协商时采用的模式
IPsec 配置	表示以下多个配置为 IPsec 相关配置
封装模式	IPsec 的封装模式
安全协议	IPsec 采用的安全协议
ESP 认证算法	采用 ESP 或 AH-ESP 安全协议时，具体采用的 ESP 认证算法
ESP 加密算法	采用 ESP 或 AH-ESP 安全协议时，具体采用的 ESP 加密认证算法
AH 认证算法	采用 AH 或 AH-ESP 安全协议时，具体采用的 AH 认证算法
PFS	是否使用 PFS 特性。PFS 是一种安全特性，它解决了密钥之间相互无关性的需求使用 PFS 特性后，IKE 第二阶段协商过程中会增加一次 DH 交换，使得 IKE SA 的密钥和 IPsec SA 的密钥之间没有派生关系。
DPD 检测	是否开启 IKE DPD 检测功能，勾选为开启
检测方式	IKE DPD 检测的方式
检测时间间隔	触发 IKE DPD 探测的时间间隔。对于按需探测模式，指定经过多长时间没有从对端收到 IPsec 报文，则触发一次 DPD 探测；对于定时探测模式，指触发

参数	说明
	一次 DPD 探测的时间间隔
重传时间间隔	IKE DPD 报文的重传时间间隔，如果本端在 DPD 报文的重传时间间隔内未收到对端发送的 DPD 回应报文，则重传 DPD 请求报文，若重传两次之后仍然没有收到对端的 DPD 回应报文，则删除该 IKE SA 和对应的 IPsec SA

步骤4　单击“下一步”，进入服务器信息页签，具体配置内容如下表所示：

参数	说明
主服务器地址	主 VAMS 的公网地址，需要静态分配
备服务器地址	备 VAMS 的公网地址，需要静态分配
主服务器端口	主 VAMS 的监听端口号
备服务器端口	备 VAMS 的监听端口号

步骤5　单击“下一步”，进入隧道配置页签，具体配置内容如下表所示：

参数	说明
模式	ADVPN 隧道的封装模式，取值包括： ● GRE ● UDP
隧道接口 ID	ADVPN 隧道接口的编号
隧道私网地址	ADVPN 隧道接口的私网地址以及子网掩码
隧道公网地址	ADVPN 隧道接口的公网地址，可以为隧道源接口的地址，也可以手动配置
VRF	ADVPN 隧道使用的虚拟路由转发表，具体配置请参见“VRF”
OSPF 路由协议	ADVPN 隧道采用的 OSPF 路由协议，具体配置请参见“OSPF”
网络类型	在选择 OSPF 实例后可见，表示 OSPF 协议的网络类型，将决定 Hub 组的组网方式
DR 优先级	在选择 OSPF 实例后可见，表示 OSPF 协议中当前节点的 DR 优先级
GRE key	当使用 GRE 封装模式时，使用的 GRE 验证密钥。不配置的情况下，表示不使用 GRE key 进行验证，具体请参见“GRE”
开启报文校验和功能	当使用 GRE 封装模式时，开启 GRE 校验和验证功能来检查报文的完整性，具体请参见“GRE”
源 UDP 端口号	当使用 UDP 封装时，报文的源端口号。若勾选了兼容 ADVPN V0，则该参数不能和其他隧道的源端口号相同
注册私网信息列	VAMC 向 VAMS 注册 ADVPN 隧道的私网信息。当其他 VAMC 向 VAMS 解析私网报

参数	说明
表	文目的地址时，如果解析的地址属于注册私网，则 VAMS 将注册 VAMC 的节点信息返回给查询方 当前页面显示已有私网，并提供新建、编辑和删除功能。关于新建和编辑功能，请注意，弹出框中的“优先级”，建议高于其他动态路由协议，且低于静态路由。优先级数值越大，优先级越低
兼容 ADVPN V0	是否兼容 ADVPN V0 版本
隧道静默时间	ADVPN 隧道建立失败的静默时间
隧道空闲超时时间	Spoke-Spoke 类型 ADVPN 隧道的空闲超时时间，如果在空闲超时时间内，Spoke-Spoke 类型 ADVPN 隧道上没有数据传输，则断开该隧道
封装后报文的 TOS	ADVPN 隧道报文的 TOS 值
封装后报文的 TTL	ADVPN 隧道报文的 TTL 值
封装后报文不允许分片	设置封装后隧道报文的 DF 标志，勾选表示不允许分片

步骤6　单击“下一步”，进入IPsec配置页签，具体配置内容如下表所示：

参数	说明
IPsec 功能	是否开启 IPsec 功能，勾选为开启
名称	IPsec 策略的名称
IKE 配置	表示以下多个配置为 IKE 相关配置
认证方式	IKE 认证方式，取值范围包括： ● 预共享密钥 ● 数字证书认证
预共享密钥	当选择 IKE 认证方式为“预共享密钥”时，需要配置该密钥
PKI 域	当选择 IKE 认证方式为“数字证书认证”时，需要配置证书所属的 PKI 域，具体配置请参见“PKI”
证书访问策略	当选择 IKE 认证方式为“数字证书认证”时，需要配置证书的访问控制策略，具体配置请参见“PKI”
IKE 提议	IPsec 策略引用的 IKE 提议，具体配置请参见“IPsec”
协商模式	IKE 协商时采用的模式，取值包括： ● 主模式 ● 野蛮模式 ● 国密主模式

参数	说明
IPsec 配置	表示以下多个配置为 IPsec 相关配置
封装模式	IPsec 的封装模式，取值包括： ● 隧道模式 ● 传输模式
安全协议	IPsec 采用的安全协议，取值包括： ● ESP ● AH ● AH-ESP
ESP 认证算法	采用 ESP 或 AH-ESP 安全协议时，具体采用的 ESP 认证算法
ESP 加密算法	采用 ESP 或 AH-ESP 安全协议时，具体采用的 ESP 加密认证算法
AH 认证算法	采用 AH 或 AH-ESP 安全协议时，具体采用的 AH 认证算法
PFS	是否使用 PFS 特性。PFS 是一种安全特性，它解决了密钥之间相互无关性的需求使用 PFS 特性后，IKE 第二阶段协商过程中会增加一次 DH 交换，使得 IKE SA 的密钥和 IPsec SA 的密钥之间没有派生关系
DPD 检测	是否开启 IKE DPD 检测功能，勾选为开启
检测方式	IKE DPD 检测的方式，取值包括： ● 按需检测，表示仅在需要发送报文时，才进行检测 ● 按时检测，表示按照一定的实际间隔进行检测，会消耗更多的带宽和计算资源
检测时间间隔	触发 IKE DPD 探测的时间间隔。对于按需探测模式，指定经过多长时间没有从对端收到 IPsec 报文，则触发一次 DPD 探测；对于定时探测模式，指触发一次 DPD 探测的时间间隔
重传时间间隔	IKE DPD 报文的重传时间间隔，如果本端在 DPD 报文的重传时间间隔内未收到对端发送的 DPD 回应报文，则重传 DPD 请求报文，若重传两次之后仍然没有收到对端的 DPD 回应报文，则删除该 IKE SA 和对应的 IPsec SA

步骤7　单击“完成”按钮，完成VAMC配置。

步骤8　在VAMC页面，可以开启、关闭、编辑已有的VAMC。

6.15.4.3　配置监控

在ADVPN监控页面，可以查看已建立的ADVPN的隧道信息，可以删除指定的隧道，或者删除所有隧道。

监控页面的具体配置步骤如下：

步骤1　选择“网络 > VPN > ADVPN > 监控”。

步骤2　在“监控”页面单击<清除所有隧道>按钮，单击“确定”按钮后，可以删除所有隧道。

步骤3　在“监控”页面单击<清除指定隧道>按钮，进入“清除指定隧道”页面，选择需要删除的ADVPN隧道的ID，单击“确定”按钮，可以删除指定的隧道。

6.16　L2TP

本帮助主要介绍以下内容：

6.16.1　特性简介

L2TP（Layer 2 Tunneling Protocol，二层隧道协议）通过在公共网络（如Internet）上建立点到点的L2TP隧道，将PPP（Point-to-Point Protocol，点对点协议）数据帧封装后通过L2TP隧道传输，使得远端用户（如企业驻外机构和出差人员）利用PPP接入公共网络后，能够通过L2TP隧道与企业内部网络通信，访问企业内部网络资源。

6.16.1.1　L2TP组网中的角色

在L2TP的组网中，角色分为以下三个部分：

6.16.1.1.1　远端系统

远端系统是要接入企业内部网络的远端用户和远端分支机构，通常是一个拨号用户的主机或私有网络

中的一台设备。

6.16.1.1.2 LAC（L2TP Access Concentrator，L2TP访问集中器）

LAC是具有PPP和L2TP协议处理能力的设备，通常是一个当地ISP的NAS（Network Access Server，网络接入服务器），主要用于为PPP类型的用户提供接入服务。

LAC作为L2TP隧道的端点，位于LNS和远端系统之间，用于在LNS和远端系统之间传递报文。它把从远端系统收到的报文按照L2TP协议进行封装并送往LNS，同时也将从LNS收到的报文进行解封装并送往远端系统。

6.16.1.1.3 LNS（L2TP Network Server，L2TP网络服务器）

LNS是具有PPP和L2TP协议处理能力的设备，通常位于企业内部网络的边缘。

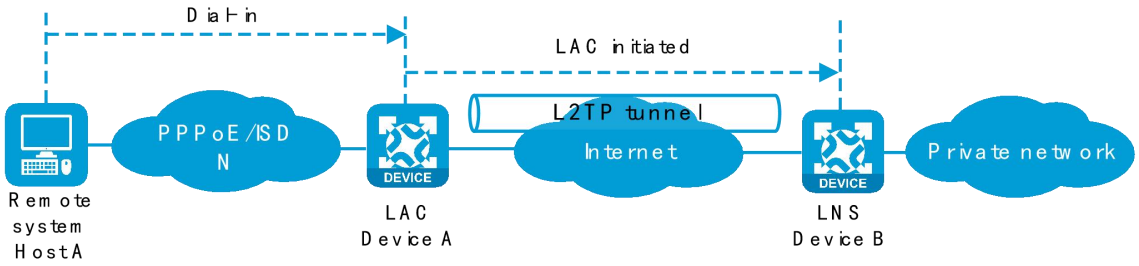
LNS作为L2TP隧道的另一侧端点，是LAC通过隧道传输的PPP会话的逻辑终点。L2TP通过在公共网络中建立L2TP隧道，将远端系统的PPP连接由原来的NAS延伸到了企业内部网络的LNS设备。

6.16.1.2 L2TP隧道模式

L2TP隧道包括NAS-Initiated、Client-Initiated和LAC-Auto-Initiated三种模式。

6.16.1.2.1 NAS-Initiated模式

如下图所示，NAS-Initiated模式L2TP隧道的建立由LAC（即NAS）发起。远端系统的拨号用户通过PPPoE/ISDN拨入LAC后，由LAC向LNS发起建立L2TP隧道的请求。



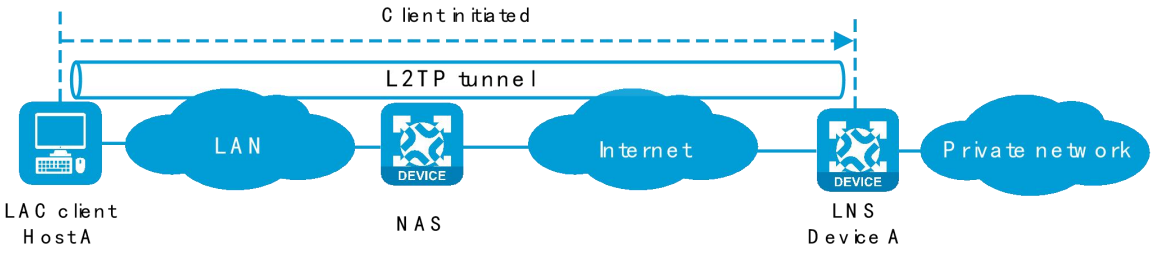
NAS-Initiated模式L2TP隧道具有如下特点：

远端系统只需支持PPP协议，不需要支持L2TP。

对远端拨号用户的身份认证与计费既可由LAC代理完成，也可由LNS完成。

6.16.1.2.2 Client-Initiated模式

如下图所示，Client-Initiated模式L2TP隧道的建立直接由LAC client（指本地支持L2TP协议的远端系统）发起。LAC client具有公网地址，并能够通过Internet与LNS通信后，如果在LAC client上触发L2TP拨号，则LAC client直接向LNS发起L2TP隧道建立请求，无需经过LAC设备建立隧道。



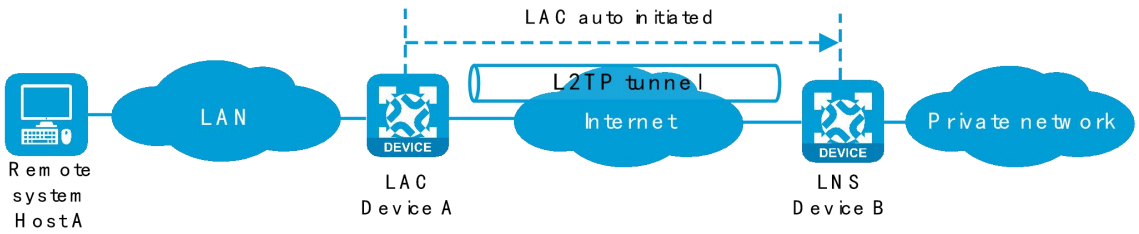
Client-Initiated模式L2TP隧道具有如下特点：

- L2TP隧道在远端系统和LNS之间建立，具有较高的安全性。
- Client-Initiated模式L2TP隧道对远端系统要求较高（远端系统必须是支持L2TP协议的LAC client，且能够与LNS通信），因此它的扩展性较差。

6.16.1.2.3 LAC-Auto-Initiated模式

采用NAS-Initiated方式建立L2TP隧道时，要求远端系统必须通过PPPoE/ISDN等拨号方式拨入LAC，且只有远端系统拨入LAC后，才能触发LAC向LNS发起建立隧道的请求。

如下图所示，在LAC-Auto-Initiated模式下，不需要远端系统拨号触发，LAC采用特定L2TP组下配置的隧道参数建立L2TP隧道。远端系统访问LNS连接的内部网络时，LAC将通过L2TP隧道转发这些访问数据。



LAC-Auto-Initiated模式L2TP隧道具有如下特点：

- 远端系统和LAC之间可以是任何基于IP的连接，不局限于拨号连接。
- 不需要远端系统上的拨号接入来触发建立L2TP隧道。
- L2TP隧道创建成功后立即建立L2TP会话，然后在LAC和LNS之间进行PPP协商，LAC和LNS分别作为PPP客户端和PPP服务器端。
- 一条L2TP隧道上只承载一个L2TP会话。
- LNS为LAC分配企业网内部的IP地址，而不是为远端系统分配。

6.16.2 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。

6.16.3 常见问题解答

如下列举了基本的Troubleshooting以供参考。

6.16.3.1 常见故障之一

6.16.3.1.1 故障现象

通过“VPN > L2TP > 隧道信息”，查看不到隧道信息（即隧道未成功建立）。

6.16.3.1.2 故障排除

可能有以下原因：

- LAC端配置的L2TP服务器端地址不正确。
- LAC端和LNS端配置的PPP认证方式不一致。
- LAC端配置的用户名和密码错误，或者是LNS端不存在相应的用户。
- LNS端上的组号不为1时，配置的LAC端隧道名称与LNS端配置的隧道名称不一致。
- 隧道验证不通过：
  - 如果LAC和LNS两端都开启了隧道验证功能，则两端密钥不为空并且完全一致的情况下，二者之间才能成功建立L2TP隧道。
  - 如果LAC和LNS中的一端开启了隧道验证功能，则另一端可不开启隧道验证功能，但需要两端密钥不为空并且完全一致，二者之间才能成功建立L2TP隧道。

6.16.3.2 常见故障之二

6.16.3.2.1 故障现象

通过“VPN > L2TP > 隧道信息”，查看隧道成功建立，但是数据传输失败（如不能Ping通私网侧主机）

6.16.3.2.2 故障排除

可能有如下原因：

- 路由问题：LAC和LNS上需要存在到达对端私网的路由，否则会导致数据传输失败。在LAC和LNS上查看设备上是否存在到达对端私网的路由。若不存在，则需要配置静态路由或动态路由协议，在设备上添加该路由。
- 安全策略：LNS端的VT接口需要加入到安全域，并在安全策略中放行该安全域到Local安全域

的相关流量，否则数据会因为安全策略的原因被设备丢弃。

- 网络拥挤：Internet主干网产生拥挤，丢包现象严重。L2TP是基于UDP进行传输的，UDP不对报文进行差错控制。如果是在线路质量不稳定的情况下进行L2TP应用，有可能会产生Ping不通对端的情况。

6.16.4 配置指南

6.16.4.1 配置L2TP

步骤1 单击“网络 > VPN > L2TP > L2TP”。

步骤2 在“L2TP”页面，单击<新建>按钮，进入“新建L2TP”页面，具体配置如下：

参数	说明
组类型	L2TP 的组类型包括 LAC 和 LNS，LAC 作为 L2TP 隧道的端点，位于 LNS 和远端系统之间，用于在 LNS 和远端系统之间传递报文
L2TP 组号	L2TP 的组号
本端隧道名称	如果不配置本端隧道名称，缺省情况下使用设备名称作为本端隧道名称
对端隧道名称	当 L2TP 组号不为 1 时，必须配置对端隧道名称
隧道密码认证	L2TP 隧道验证功能用来防止本端设备与非法的对端设备建立 L2TP 隧道，提高网络的安全性
隧道密码	如果用户需要修改隧道验证的密钥，请在隧道开始协商前进行，否则修改的密钥不生效
确认隧道密码	再次输入隧道密码进行确认
L2TP 服务器端地址	指定 LNS 端的 IP 地址，最多可以配置 5 个地址
PPP 认证方式	采用 PAP 或 CHAP 认证时，需要与 LNS 侧的用户信息一致
PPP 服务器地址	虚拟 PPP 接口的 IP 地址，用于协商 PPP 连接
子网掩码	虚拟 PPP 接口的 IP 地址的子网掩码
用户地址池	用户可以使用的地址池范围，可以是单个地址，也可以是地址范围
Hello 报文间隔	设备按照本功能配置的时间间隔周期性发送 Hello 报文，以免 LAC 和 LNS 之间的 L2TP 隧道和会话在超时后被删除
AVP 隐藏功能	如果用户不希望这些信息（如用户密码）被窃取，则可以使用本功能将 AVP 数据的传输方式配置为隐藏传输，本功能仅在开启隧道密码认证功能后生效
流控功能	L2TP 会话的流控功能是指在 L2TP 会话上传递的报文中携带序列号，通过序列号检测是否存在丢包，并根据序列号对乱序报文进行排序

步骤3　单击“确定”按钮，完成配置。

6.16.4.2　隧道信息

在“隧道信息”页面，可以查看L2TP隧道的隧道ID、对端地址、对端端口、组类型、隧道状态等信息。

6.17　SSL VPN

本帮助主要介绍以下内容：

- 特性简介
  - SSL VPN工作机制
  - SSL VPN典型组网
  - SSL VPN接入方式
  - 资源访问控制
- vSystem相关说明
- 使用限制和注意事项
  - SSL VPN网关使用限制和注意事项
  - TCP代理方式使用限制和注意事项
  - 隧道业务方式使用限制和注意事项
  - 域名使用限制和注意事项
  - 页面模板使用限制和注意事项
  - LDAP认证使用限制与注意事项
  - 单点登录使用限制和注意事项
  - 企业微信认证使用限制和注意事项
- 配置指南
  - 配置访问实例-基本配置

6.17.1 特性简介

SSL VPN是以SSL（Secure Sockets Layer，安全套接字层）为基础的VPN（Virtual Private Network，虚拟专用网络）技术。SSL VPN充分利用了SSL协议提供的基于证书的身份认证、数据加密和消息完整性验证机制，能够为应用层之间的通信建立安全连接。

SSL VPN可以为企业或机构提供安全、快捷的远程网络接入服务，并适合移动接入。企业员工可以使用移动客户端在任意能够访问互联网的位置安全地接入到企业内部网络，访问内部网络的共享资源。

6.17.1.1 SSL VPN工作机制

步骤1 管理员登录SSL VPN网关，在SSL VPN网关上创建与企业网内服务器对应的资源。

步骤2 远程接入用户与SSL VPN网关建立HTTPS连接，通过SSL提供的基于证书的身份验证功能，SSL VPN网关和远程接入用户可以验证彼此的身份。

步骤3 远程接入用户输入用户名、密码等身份信息，SSL VPN网关对用户的身份进行认证，并对用户可以访问的资源进行授权。

步骤4 用户获取到可以访问的资源，通过SSL连接将访问请求发送给SSL VPN网关。

步骤5 SSL VPN网关将资源访问请求转发给企业网内的服务器。

步骤6 SSL VPN网关接收到服务器的应答后，通过SSL连接将其转发给用户。

6.17.1.2 SSL VPN典型组网

SSL VPN的典型组网方式主要有两种：网关模式和单臂模式。

- 在网关模式中，SSL VPN网关直接作为网关设备连接用户和内网服务器，所有流量将通过SSL VPN网关进行转发。网关模式可以提供对内网的完全保护，但是由于SSL VPN网关处在内网与外网通信的关键路径上，其性能对内外网之间的数据传输有很大的影响。
- 在单臂模式中，SSL VPN网关不作为网关设备。用户访问内网服务器时，流量将先由网关设备转发到SSL VPN网关，经SSL VPN网关处理后再转发到网关设备，由网关设备转发到内网服务器。在单臂模式中，SSL VPN网关不处在网络通信的关键路径上，其性能不会影响内外网的通信。但是这种组网使得SSL VPN网关不能全面地保护企业内部的网络资源。

6.17.1.3 SSL VPN接入方式

6.17.1.3.1 隧道业务方式

隧道业务方式用来实现远程主机与企业内部服务器网络层之间的安全通信，进而实现所有基于IP的远程主机与服务器的互通，如在远程主机上ping内网服务器。

用户通过隧道业务方式访问内网服务器前，需要安装专用的隧道业务客户端软件，该客户端软件会在SSL VPN客户端上安装一个虚拟网卡。

6.17.1.3.2 Web代理方式

Web代理方式是指用户使用浏览器，通过HTTPS协议访问SSL VPN网关提供的Web资源。用户登录后，Web页面上会显示用户可访问的资源列表，用户选择需要访问的资源直接访问。Web代理方式中，所有数据的显示和操作均通过Web页面进行。

目前，通过Web代理方式可以访问的资源只有Web服务器。

6.17.1.3.3 TCP代理方式

TCP代理方式是指用户对企业内部服务器开放端口的安全访问。通过TCP代理方式，用户可以访问任意基于TCP的服务，包括远程访问服务（如Telnet）、桌面共享服务、电子邮件服务、Notes服务以及其他使用固定端口的TCP服务。

用户利用TCP代理方式访问内网服务器时，需要在SSL VPN客户端（用户使用的终端设备）上安装专用的TCP代理客户端软件，由该软件实现使用SSL连接传送应用层数据。

6.17.1.3.4 BYOD接入方式

BYOD接入方式用来实现移动客户端对企业内部服务器进行安全访问。

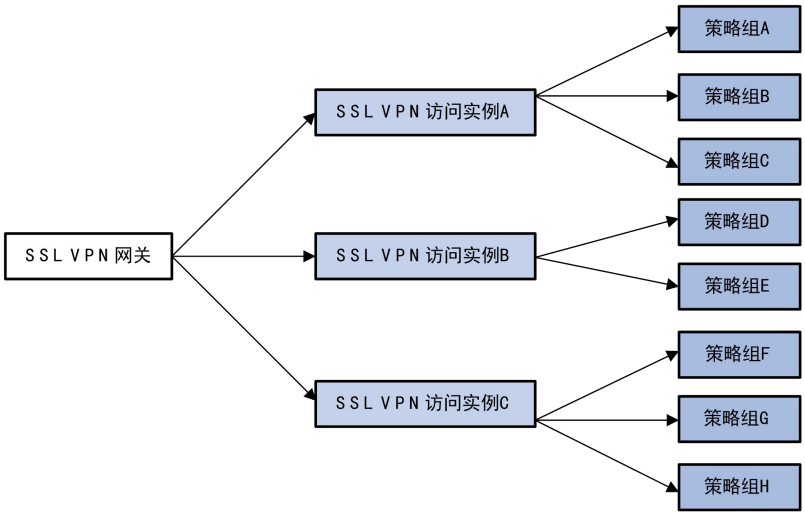
移动客户端利用BYOD接入方式访问内网服务器时，需要在客户端上安装移动客户端专用的客户端软件，

并在SSL VPN网关上为客户端指定EMO（Endpoint Mobile Office，终端移动办公）服务器。移动客户端通过EMO服务器来获取可以访问的内网资源。

6.17.1.4 资源访问控制

SSL VPN采用基于用户的权限管理方法，可以根据用户的身份，限制用户可以访问的资源。

如下图所示，SSL VPN对资源的管理方式为：同一台SSL VPN网关上可以创建多个SSL VPN访问实例（SSL VPN context）。每个SSL VPN访问实例包含多个资源组。资源组包含一系列规则，这些规则为用户定义了可访问的资源，包含Web接入资源、TCP代理资源、隧道业务资源等。



SSL VPN用户访问网关的方式，及每种访问方式下SSL VPN网关判断该用户所属的SSL VPN访问实例的方法为：

- 直接访问：SSL VPN用户直接输入网关的IP地址和端口号访问网关。只有SSL VPN网关上仅存在一个SSL VPN访问实例时，可以采用此方式。SSL VPN用户属于该SSL VPN访问实例。
- 通过域名列表访问：为不同的SSL VPN访问实例指定不同的域名。远端用户输入网关的IP地址和端口号登录SSL VPN网关后，进入Domain List页面，在该页面上选择自己所在的域。SSL VPN网关根据用户选择的域判断该用户所属的SSL VPN访问实例。
- 通过主机名访问：为不同的SSL VPN访问实例指定不同的主机名称。远端用户访问SSL VPN网关时，输入主机名称。SSL VPN网关根据主机名称判断该用户所属的SSL VPN访问实例。

SSL VPN网关判断出用户所属的SSL VPN访问实例后，根据SSL VPN访问实例所在的ISP域对用户进行认证和授权，授权结果为资源组名称。如果某个用户被授权访问某个资源组，则该用户可以访问该资源组下的资源。如果没有为用户进行授权，则用户可访问的资源由缺省资源组决定。

SSL VPN网关对用户的认证和授权通过AAA来完成。目前，SSL VPN支持的AAA协议包括RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）协议和LDAP（Lightweight Directory Access Protocol，轻量级目录访问协议）协议。在实际应用中，RADIUS协议较为常用。

6.17.2 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。

6.17.3 使用限制和注意事项

6.17.3.1 SSL VPN网关使用限制和注意事项

修改SSL VPN网关引用的SSL服务器端策略，或修改该策略内的SSL相关配置后，需要重新使能网关，否则新的配置不能生效。

6.17.3.2 访问实例使用限制和注意事项

- 配置访问实例关联网关时，设备默认采用直接访问方式，即SSL VPN用户直接输入网关的IP地址和端口号访问网关。如需配置通过域列表或主机名访问网关，请到CLI管理界面下进行配置，Web管理界面暂不支持配置访问方式。
- 新建访问实例时，设备默认仅支持关联一个网关，如需关联多个网关，请在完成新建访问实例后重新编辑该访问实例，指定多个关联的网关。

6.17.3.3 TCP代理方式使用限制和注意事项

- 客户端主机地址建议配置为127.0.0.0/8网段的地址，或者配置为主机名或域名。
- 主机通过TCP代理方式访问内网资源时，可能会修改主机上的Host文件，此时需要使用该主机的用户具有管理员权限。
- 主机上要求安装Java运行环境。

6.17.3.4 隧道业务方式使用限制和注意事项

禁用IP接入接口可能会导致IP接入业务中断，请谨慎执行本操作。

为客户端地址池配置的网段需要满足以下要求：

- 不能和客户端物理网卡的IP地址在同一个网段。
- 不能包含SSL VPN网关所在设备的接口地址，否则会导致地址冲突。
- 不能和欲访问的内网地址在同一个网段。

配置SSL VPN用户绑定的IP地址必须属于用户登录的SSL VPN访问实例引用的地址池或用户被授权的资

源组引用的地址池。

未关联VPN实例或在同一VPN实例中，不同SSL VPN用户不能绑定相同的IP地址。

6.17.3.5 域名使用限制和注意事项

配置域名（如配置Web接入资源中的URL、端口转发表项中的客户端主机名）时，需要由用户保证域名的合法性，SSL VPN不检查域名是否存在以及是否合法。

6.17.3.6 页面模板使用限制和注意事项

- 用户上传的自定义模板文件必须以.zip为拓展名。
- 用户上传的自定义模板文件中必须在其根路径下包含home.html和login.html两个文件。

6.17.3.7 LDAP认证使用限制与注意事项

SSL VPN用户使用LDAP认证时，必须使用LDAP授权。管理员需要使用CLI方式在设备上进行LDAP的相关配置。

6.17.3.8 单点登录使用限制和注意事项

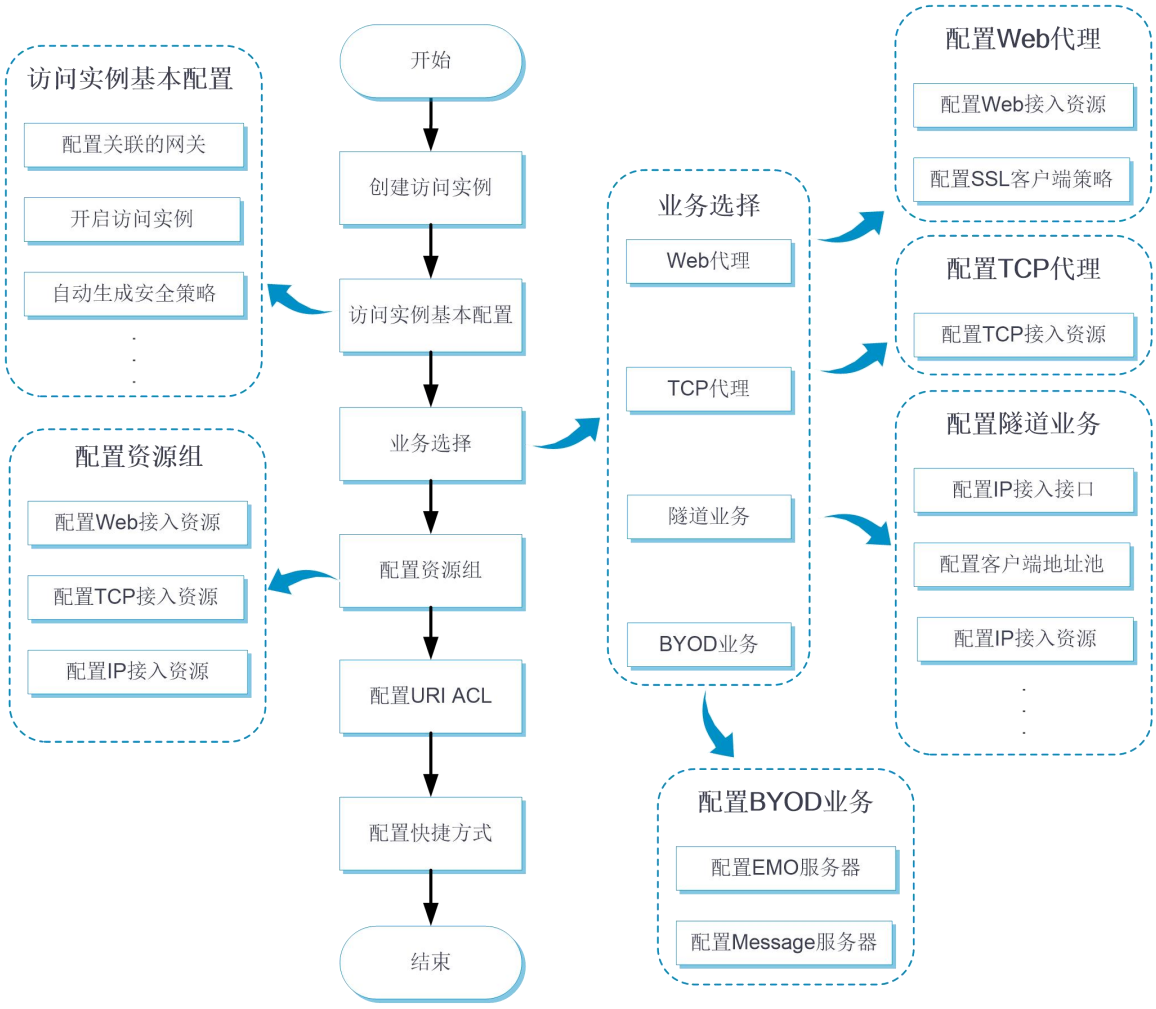
- 自动构建登录请求方式下的单点登录，选择用户组作为登录参数时，只支持远程用户。
- 自动构建登录请求方式下的单点登录，只支持从SSL VPN资源页面单击URL链接时才会自动登录，不支持在地址栏或URL输入框中打开资源。
- 自动构建登录请求方式下的单点登录，不支持登录需要图形校验码校验的页面。
- 自动构建登录请求方式下的单点登录，不支持登录需要挑战码验证或调用脚本的页面。

6.17.3.9 企业微信认证使用限制和注意事项

若SSL VPN访问实例开启了企业微信认证功能，则该访问实例仅支持通过直接访问网关方式关联SSL VPN网关。

6.17.4 配置指南

为方便使用，SSL VPN提供了向导式的Web配置页面。如下图所示，进入“新建访问实例”页面后，按照Web页面提示，逐步完成如下配置后即可使用SSL VPN功能：



除了按照配置向导逐步完成SSL VPN配置外，管理员还可以进行以下操作：

- 通过“网关”、“客户端地址池”、“IP接入接口”页面创建和修改网关、客户端地址池、IP接入接口。
- 在“编辑访问实例”页面配置SSL VPN用户登录的SSL VPN网关Web页面的形式，包括页面模板、页面标题、登录页面欢迎信息、登录页面是否显示密码输入框、Logo。
- 在“编辑访问实例”的“页面配置”页面配置登录页面和资源页面的中英文页面公告信息、供用户下载的中英文页面文件、中英文页面密码复杂度提示信息以及改写服务器返回信息。
- 在“全局配置”页面，管理员可以上传自定义隧道业务客户端供用户下载使用，也可选择已上传的页面模板作为全局页面模板。
- 当使用高可靠性功能时，可以在“全局配置”页面，配置SSL VPN备份通道使用的HA端口号。设备将使用此端口号以及高可靠性模块配置的“对端IP地址”，与HA的对端设备建立SSL VPN备份通道，此通道专用于SSL VPN用户信息的备份。此功能不同设备的支持情况不同，请以

设备Web页面的实际支持情况为准。

- 在“模板管理”页面，点击创建按钮，弹出“新建自定义模板页面”，管理员可以上传自定义页面模板。上传后，管理员可在“全局配置”或“编辑访问实例”页面引用该页面模板。
- 通过“统计信息”页面，管理员可以查看在线用户信息，以及隧道业务相关的统计信息。
- 单点登录功能支持在“全局配置”页面，配置导出用户自定义配置和导入用户自定义配置。导出用户自定义配置用于导出当前用户在SSL VPN资源页面配置的自定义用户名和密码；导入用户自定义配置用于导入用户在SSL VPN资源页面配置的自定义用户名和密码。
- 使用量子加密功能时，需要在“网关”页面开启量子加密功能，并在“全局配置”页面中的”量子密钥”页签配置交换密码机IP地址及端口号、交换密码机ID、密码服务平台软件ID和应用账户。上述量子密钥相关参数需要联系国盾量子管理员获取。

6.17.4.1 配置访问实例-基本配置

配置访问实例的基本属性，包括访问实例关联的网关、开启访问实例等。

6.17.4.1.1 配置步骤

步骤1 选择“网络 > VPN > SSL VPN > 访问实例”。

步骤2 在“访问实例”页面单击<新建>按钮，进入“新建访问实例”页面。

步骤3 在“基本配置”页签，配置访问实例基本配置，具体配置内容如下：

参数	说明
访问实例	访问实例名称
关联网关	访问实例引用的网关 在关联网关下拉框中选择网关，如果未创建网关，单击<添加关联网关>按钮，可进入“新建网关”页面，创建网关 多个访问实例引用同一个网关时，可以为不同访问实例指定域名或主机名。如果不指定域名或主机名，则网关只能被一个访问实例引用
开启访问实例	开启访问实例
自动生成安全策略	开启自动生成安全策略功能后，设备将在创建 SSL VPN 访问实例时，自动生成放通 SSL VPN 业务报文的安全策略

步骤4 单击<下一步>按钮，进入“业务选择”页签。

6.17.4.2 配置访问实例-业务选择

SSL VPN支持的业务类型包括隧道业务、Web代理、TCP代理和BYOD业务。

6.17.4.2.1 隧道业务

隧道业务，即IP接入方式。在该业务下需要完成如下配置：

- 指定SSL VPN访问实例引用的IP接入接口，并为其配置IP地址。
- 指定SSL VPN访问实例引用的地址池，以便SSL VPN网关从该地址池中选择IP地址分配给客户端。
- 以路由列表的形式配置IP接入资源。路由表项包括包含和排除两种类型。包含路由下发给客户端后，匹配该路由的报文将通过虚拟网卡发送给SSL VPN网关；排除路由下发给客户端后，匹配该路由的报文不会发送给SSL VPN网关。
- 开启IP客户端自启动。开启此功能，SSL VPN用户通过Web方式成功登录SSL VPN网关后，设备会自动启动用户主机上的IP客户端，且会自动连接SSL VPN网关，连接成功后SSL VPN用户也可以使用隧道业务方式访问授权的资源。若用户主机上未安装IP客户端，则先提示用户下载并安装IP客户端，安装完成后IP客户端会自动启动；若已经安装IP客户端，则直接启动。为使IP客户端自启动后成功连接SSL VPN网关，需要保证设备上已创建IP接入资源。
- 开启推送资源列表。开启此功能，SSL VPN用户通过IP方式成功登录SSL VPN网关后，设备会自动推送资源列表，以便用户通过Web方式访问所授权的资源。为使设备推送的资源列表上有内容，需要保证设备上已创建Web代理资源。
- 配置流量限制后，若访问实例的IP接入速率大于设置的速率，则设备将丢弃收到的数据。
- 指定用户绑定地址。本配置可以指定用户登录SSL VPN网关时，网关分配给用户的地址。若选择自动绑定IP地址，网关会从地址池中获取指定数量的空闲IP地址，为该用户绑定。若未选择自动绑定IP地址，则优先从指定IP地址范围内分配；如果指定IP地址范围中的地址已被分配给其他用户，则断开其他用户的连接并释放其IP地址。

6.17.4.2.2 隧道业务配置步骤

步骤1 在“业务选择”页签，滑动选择隧道业务。支持同时配置IPv4和IPv6地址。

步骤2 在IP接入接口区域，选择指定的接口。

步骤3 客户端使用隧道业务方式访问SSL VPN网关时，网关需要为客户端分配IP地址。在隧道模式区域，选择隧道模式为IPv4或者IPv6，并选择相应的客户端地址池，SSL VPN网关将使用该地址池为客户端分配地址。

步骤4 在IPv4接入资源区域，单击<新建>按钮，进入“新建IPv4路由列表”页面，需要配置IPv4路由列表名称。

步骤5 在“IPv4路由列表表项”区域，单击<新建>按钮，进入“新建IPv4路由表项”页面，具体配

置内容如下：

参数	说明
类型	类型包括包含和排除。包含表示在路由列表中添加路由，路由的目的网段需要是企业内部服务器所在的网络。排除表示客户端在本地添加这些路由表项，匹配这些路由表项的报文将不会被发送给 SSL VPN 网关
子网地址	路由的目的地址
掩码长度	路由目的地址的掩码长度

步骤6　单击<确定>按钮，完成配置路由表项。

步骤7　单击<确定>按钮，完成配置路由列表。

步骤8　在IPv6接入资源区域，单击<新建>按钮，进入“新建IPv6路由列表”页面，需要配置IPv6路由列表名称。

步骤9　在“IPv6路由列表表项”区域，单击<新建>按钮，进入“新建IPv6路由表项”页面，具体配置内容如下：

参数	说明
类型	类型包括包含和排除。包含表示在路由列表中添加路由，路由的目的网段需要是企业内部服务器所在的网络。排除表示客户端在本地添加这些路由表项，匹配这些路由表项的报文将不会被发送给 SSL VPN 网关
子网地址	路由的目的地址
前缀长度	路由目的地址的前缀长度

步骤10　单击<确定>按钮，完成配置IPv6路由表项。

步骤11　单击<确定>按钮，完成配置IPv6路由列表。

6.17.4.2.3　Web代理

Web代理，即Web接入方式。在该业务下需要以URL表项和列表的形式创建Web接入资源。缺省情况下SSL VPN网关会对URL进行常规改写。常规改写可能会造成URL改写遗漏和改写错误等问题，从而导致SSL VPN客户端不能访问内网资源。因此可以通过配置域名映射或端口映射的方式尽可能的解决此问题。

以SSL VPN网关名gw（域名为https://www.gateway.com:4430，对应的IP地址为1.1.1.1），内网资源服务器URL=http://www.server.com:8080为例：

- 当不配置URL映射方式时（默认为常规改写），客户端访问内网资源服务器的URL显示为：

https://www.gateway.com:4430/_proxy2/http/8080/www.server.com

- 当配置域名映射，映射的域名为www.domain.com时，www.domain.com与内网资源http://www.server.com:8080为一一映射关系。客户端访问内网资源服务器的URL显示为：https://www.domain.com:4430
- 当配置端口映射，又分为配置虚拟主机名和不配置虚拟主机名两种情况：
  - 不配置虚拟主机名，引用SSL VPN网关gw2时，客户端访问内网资源服务器的URL显示为：https://2.2.2.2:4430（网关gw2的IP地址为2.2.2.2，端口号是4430）
  - 配置虚拟主机名，虚拟主机名为vhosta，vhosta与内网资源http://www.server.com:8080为一一映射关系。引用SSL VPN网关gw时，客户端访问内网资源服务器的URL显示为：https://vhosta:4430

当内网资源为HTTPS服务器时，需要为Web代理指定SSL客户端策略，以便SSL VPN网关使用指定的SSL客户端策略与HTTPS服务器建立连接。如果没有指定SSL客户端策略，则SSL VPN网关使用缺省的SSL客户端策略，该策略支持的加密套件为**rsa_rc4_128_md5**。

6.17.4.2.4 Web代理配置步骤

步骤1 在“业务选择”页签，滑动选择Web代理。

步骤2 在SSL客户端策略区域，选择指定的SSL客户端策略，以便SSL VPN网关使用指定的SSL客户端策略与HTTPS服务器建立连接。如果没有指定SSL客户端策略，则SSL VPN网关使用缺省的SSL客户端策略，该策略支持的加密套件为**rsa_rc4_128_md5**。

步骤3 在URL表项区域，单击<新建>按钮，进入“新建URL表项”页面，具体配置内容如下：

参数	说明
URL 表项名称	URL 对应的链接名
URL	URL 表项中资源的 URL
URI ACL	过滤 URL 资源的 URI ACL
接入类型	接入类型包括以下三种： ● 常规改写 ● 域名映射 ● 端口映射
开启 URL 伪装	开启此功能后，用户将无法看到访问的内网服务器的真实地址
单点登录	开启此功能后，SSL VPN 用户只需要完成一次登录认证，即可访问所有相互信任的应用系统
登录方法	单点登录的登录方法包括以下两种：

参数	说明
	● Basic访问请求 ● 选择该登录方法时，需要配置登录参数获取方式 ● 自动构建访问请求 ● 选择该登录方法时，需要配置请求方式、编码方式、请求参数和上传加密文件
登录参数获取方式	登录参数获取方式包括以下两种： ● SSL VPN网关登录用户名和密码 ● 该获取方式表示网关使用SSL VPN网关登录用户名和密码作为登录参数 ● 自定义用户名和密码 ● 该获取方式表示网关使用用户自定义的用户名和密码作为登录参数，用户需要在SSL VPN登录界面输入自定义的用户名和密码
请求方式	单点登录的请求方式包括以下两种： ● GET ● POST
编码方式	单点登录的编码方式包括以下两种： ● GB18030 ● UTF-8
请求参数	单击请求参数右侧的新建按钮，进入“新建请求参数”界面，在“新建请求参数”界面配置名称、类型及是否加密参数值。名称指单点登录请求参数属性名。 请求参数类型包括： ● 登录名、登录密码、认证标题、证书序列号、证书指纹、电话号码、用户组 ● 登录名、登录密码、认证标题、证书序列号、证书指纹、电话号码、用户组分别表示取SSL VPN登录用户名、SSL VPN登录密码、登录SSL VPN网关使用的证书标题、登录SSL VPN网关使用的证书序列号、登录SSL VPN网关使用的证书指纹、短信认证配置的手机号码、SSL VPN用户所在的用户组作为单点登录请求参数属性名对应的属性值 ● 自定义用户名、自定义密码 ● 自定义用户名、自定义密码分别表示取用户在SSL VPN资源界面输入的自定义用户名和自定义密码作为单点登录请求参数属性名对应的属性值 ● 自定义 ● 自定义表示用户可以手动配置单点登录请求参数属性名对应的属性值
上传加密文件	加密文件用于对请求参数的参数值进行加密。单击选择文件按钮，选择加密文件，加密文件必须为 js 格式，且文件大小不能超过 200KB。选择文件后，单击上传按钮，上传文件。取消引用用于取消当前引用的加密文件
当前加密文件	当前加密文件用于显示当前引用的加密文件

步骤4　单击<确定>按钮，完成URL表项配置。

步骤5　在URL列表区域，单击<新建>按钮，进入“新建URL列表”页面，具体配置内容如下：

参数	说明

参数	说明
URL 列表名称	URL 列表的名称
标题	URL 列表的标题
URL 表项	URL 列表引用的 URL 表项

步骤6　单击<确定>按钮，完成URL列表配置。

6.17.4.2.5　TCP代理

TCP代理，即TCP代理接入方式。在该业务下需要以端口转发列表的形式创建TCP代理资源。端口转发列表用来将企业网内的基于TCP的服务（如Telnet、SSH、POP3）映射为SSL VPN客户端上的本地地址和本地端口，以便SSL VPN客户端通过本地地址和本地端口访问企业网内的服务器。例如，配置客户端主机为127.0.0.1、客户端代理端口为80、服务器地址为192.168.0.213、服务器端口为80，则表示在SSL VPN客户端上通过127.0.0.1、端口80可以访问企业网内的HTTP服务器192.168.0.213。

在端口转发表项中，可以配置资源链接，链接内容直接显示在Web界面中，用户可以点击链接直接访问对应资源。

6.17.4.2.6　TCP代理配置步骤

步骤1　在“业务选择”页签，滑动选择TCP代理。需要配置端口转发表项和端口转发列表。

步骤2　在端口转发表项区域，单击<新建>按钮，进入“新建端口转发表项”页面，具体配置内容如下：

参数	说明
端口转发表项名称	端口转发表项的名称
客户端主机	企业网内的 TCP 服务映射的本地地址或本地主机名称
客户端代理端口	企业网内的 TCP 服务映射的本地端口号
服务器地址	企业网内 TCP 服务的 IP 地址或完整域名
服务器端口	企业网内 TCP 服务器的端口号
描述	端口转发实例的描述信息
资源链接	端口转发表项对应的资源链接，用户可以在 Web 页面上单击指定的链接访问资源

步骤3　单击<确定>按钮，完成端口转发表项配置。

步骤4　在端口转发列表区域，单击<新建>按钮，进入“新建端口转发列表”页面，具体配置内容如下：

参数	说明
端口转发列表名称	端口转发列表的名称
端口转发表项	端口转发列表引用的端口转发表项

步骤5　单击<确定>按钮，完成端口转发列表配置。

6.17.4.2.7　BYOD业务

BYOD业务，即BYOD接入方式。在该业务下需要配置EMO服务器的地址和端口号、Message服务器的地址和端口号。

6.17.4.2.8　BYOD业务配置步骤

步骤1　在“业务选择”页签，滑动选择BYOD业务。

步骤2　配置EMO服务器地址、EMO服务器端口、Message服务器地址和Message服务器端口。

步骤3　单击<下一步>按钮，进入“资源授权”页签。

6.17.4.3　配置访问实例-资源授权

资源授权分为两个部分：配置资源组和角色授权。首先需要创建资源组，然后在角色授权页面，将用户角色与资源组进行关联，引用了某个资源组的用户角色将拥有该资源组内所有资源的访问权限。指定访问实例引用的资源组，并在资源组中引用已经创建的访问资源，以限制用户只能访问授权的资源组中的资源。在资源组中还可以通过ACL进一步控制用户访问权限。在资源组中配置隧道业务时，可以采用以下方式配置下发给客户端的路由表项：

- 指定路由方式：既可以直接配置路由表项，将一条路由下发给客户端，也可以引用“隧道业务”中创建的路由列表，将路由列表中的多条路由同时下发给客户端。
- 强制接入方式：强制将客户端的流量转发给SSL VPN网关。SSL VPN网关在客户端上添加优先级最高的缺省路由，路由的出接口为虚拟网卡，从而使得所有没有匹配到路由表项的流量都通过虚拟网卡发送给SSL VPN网关。SSL VPN网关还会实时监控SSL VPN客户端，不允许SSL VPN客户端删除此缺省路由，且不允许SSL VPN客户端添加优先级高于此路由的缺省路由。

此外，在资源组中配置隧道业务时，还可以配置资源组引用的客户端地址池。若SSL VPN资源组下引用了地址池，则SSL VPN网关只会从该地址池中为客户端分配IP地址，当该地址池中无可用地址时，

分配失败，用户无法通过隧道接入。若SSL VPN资源组下未引用地址池，则SSL VPN网关将使用SSL VPN访问实例中引用的地址池为客户端分配IP地址。

6.17.4.3.1 配置资源组

步骤1 在“资源组”区域，单击<新建>按钮，进入“新建资源组”页面，需要配置资源组名称、快速访问资源和引用的快捷方式列表。

参数	说明
资源组名称	资源组的名称。SSL VPN 网关通过给用户授权资源组的方式控制用户可以访问资源
快速访问资源	用户可以快速访问的资源。SSL VPN 用户登录网关后直接跳转到用户指定的页面，而不需要在 SSL VPN 资源页面进行选择
快捷方式列表	选择资源组引用的快捷方式列表名称

步骤2 在“隧道业务”区域，具体配置内容如下：

参数	说明
强制 IPv4 流量接入 VPN	开启该功能后，设备会强制将客户端的流量转发给 SSL VPN 网关
指定 IPv4 路由接入 VPN	将指定 IPv4 路由列表中的 IPv4 路由表项下发给客户端
客户端 IPv4 地址池	策略组引用的 IPv4 客户端地址池。客户端使用隧道业务方式访问 SSL VPN 网关时，网关需要为客户端分配 IP 地址
强制 IPv6 流量接入 VPN	开启该功能后，设备会强制将客户端的 IPv6 流量转发给 SSL VPN 网关
指定 IPv6 路由接入 VPN	将指定 IPv6 路由列表中的 IPv6 路由表项下发给客户端
客户端 IPv6 地址池	策略组引用的客户端 IPv6 地址池。客户端使用隧道业务方式访问 SSL VPN 网关时，网关需要为客户端分配 IP 地址
IPv4 ACL	配置对隧道业务进行 IPv4 高级 ACL 过滤规则
IPv6 ACL	配置对隧道业务进行 IPv6 高级 ACL 过滤规则
URI ACL	配置对隧道业务进行 URI ACL 过滤规则

步骤3 在“Web代理”区域，需要配置Web资源引用的URL列表、高级ACL和URI ACL。

步骤4 在“TCP代理”区域，需要配置TCP资源引用的端口转发列表、高级ACL和URI ACL。

步骤5　单击<确定>按钮，完成配置资源组。

6.17.4.3.2　配置角色授权

步骤1　在“角色授权”区域，单击<新建>按钮，进入“新建角色授权”页面，具体配置内容如下：

参数	说明
角色	选择引用的用户角色
资源组	选择用户角色可以使用的资源组
接入方式	选择用户角色可以使用的资源接入方式

6.17.4.4　配置访问实例-更多配置

6.17.4.4.1　基础相关

步骤1　选择“基础相关”页签，具体配置内容如下：

参数	说明
VRF	访问实例关联的 VPN 实例
最大用户数	同一个 SSL VPN 访问实例支持的最大用户数，当达到配置的最大用户数时，新的用户将无法登录
每用户在线控制	配置每个用户名的最大在线数 开启强制下线功能后，当某个用户达到最大在线数，该用户再次登录时，则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
每会话最大连接限制	开启每会话最大连接限制后，SSL VPN 会话收到报文时，如果收到报文的板卡上该会话的连接数超过单个会话的最大连接数，则回应客户端 503 Service Unavailable，并关闭该连接
空闲超时时间	SSL VPN 会话保持空闲状态的最长时间，如果超过配置的最长时间，则断开连接
空闲流量阈值	SSL VPN 会话保持空闲状态的流量阈值。配置该功能后，在空闲超时时间范围内，若 SSL VPN 用户发给 SSL VPN 网关的流量未超过该配置的流量阈值，则 SSL VPN 网关将断开该会话
每会话限速	配置每会话限速功能后，当 SSL VPN 会话相应方向的报文传输速率超过阈值时，该方向的报文将被丢弃。上行流量：即用户发给服务器的流量；下行流量：即服务器发给用户的流量
登录日志	开启登录日志功能后，用户上线下线时，SSL VPN 网关会生成日志信息
资源访问日志	开启资源访问日志功能后，用户访问资源信息时，SSL VPN 网关会生成日志信

参数	说明
	息
允许在线修改密码	实现在线修改密码功能，需同时勾选访问实例视图和用户视图下的允许在线修改密码
开启全局URL伪装	开启访问实例下所有WEB资源的URL伪装功能
允许访问的客户端	客户端类型包括： ● 浏览器 ● PC版iNode客户端 ● 移动版iNode客户端 浏览器被禁用后，所有用户均无法使用浏览器登录SSL VPN网关。其他类型客户端被禁用后，仅对新登录用户生效

6.17.4.4.2 业务相关

步骤1 选择“业务相关”页签，具体配置内容如下：

参数	说明
隧道模式	IP地址类型，取值包括IPv4和IPv6
主DNS服务器	企业网内主DNS服务器的地址
备DNS服务器	企业网内备DNS服务器的地址
主WINS服务器	企业网内主WINS服务器的地址，仅支持IPv4地址
备WINS服务器	企业网内备WINS服务器的地址，仅支持IPv4地址
保活周期	保活报文发送的时间间隔。保活报文由客户端发送给网关，用于维持客户端和网关之间的会话
开启IP客户端自启动	开启此功能后，用户通过WEB方式成功登录SSL VPN网关后，设备会自动启动用户主机上的IP客户端，并自动连接SSL VPN网关
开启推送资源列表	开启此功能后，用户通过IP方式成功登录SSL VPN网关后，设备会自动向用户主机推送资源列表
流量限制	IP接入方式的限速功能，包括上行流量限速和下行流量限速。上行流量表示SSL VPN用户访问内网服务器的流量，下行流量表示内网服务器发给SSL VPN用户的流量
丢包日志	开启此功能后，通过IP接入SSL VPN发生丢包时，SSL VPN网关会生成日志信息
IP连接关闭日志	开启此功能后，通过IP接入SSL VPN时建立的连接被关闭时，SSL VPN网关会生成日志信息

参数	说明
IP 地址分配和释放日志	IP 接入方式下,SSL VPN 网关为客户端虚拟网卡分配和释放 IP 地址时,SSL VPN 网关会生成日志信息

6.17.4.4.3 认证相关

配置用户登录访问实例的认证方式，包括密码认证、证书认证、短信认证等。

具体配置步骤如下：

步骤1 选择“认证相关”页签，配置用户认证的相关配置，具体配置内容如下：

参数	说明
认证服务器类型	针对用户的认证需求，可以选择不同认证服务器类型，取值包括： ● AAA：选择认证服务器类型为AAA时，需要配置ISP认证域 ● CUSTOM：选择认证服务器类型为CUSTOM时，需要通过命令行界面配置相关参数，具体参见SSL VPN配置手册 ● SMP：选择认证服务器类型为SMP时，需要配置安全业务平台地址、安全业务平台密钥以及认证系统类型
安全业务平台地址	配置本地址后，SSL VPN 网关将与安全业务平台进行信息交互，完成对用户的身份认证
VRF	安全业务平台所属的 VPN 实例
安全业务平台密钥	SSL VPN 网关与安全业务平台建立连接时，SSL VPN 网关需要向安全业务平台提供本功能配置的密钥，安全业务平台会使用该密钥验证 SSL VPN 网关的身份，验证通过后，才能建立连接
认证系统类型	安全业务平台对接的第三方*认证*平台类型，目前仅支持派拉
ISP 认证域	访问实例将使用指定 ISP 域内 AAA 方案对 SSL VPN 用户进行认证、授权和计费
开启证书认证	开启证书认证功能后，需要同时在 SSL 服务器端策略页面配置“验证客户端”。SSL VPN 网关会对 SSL 客户端（SSL VPN 用户）进行基于数字证书的身份验证，并检查 SSL VPN 用户的用户名是否与 SSL VPN 用户的数字证书中的用户名信息一致
用户名属性	配置 SSL VPN 用户证书中指定字段取值作为 SSL VPN 用户名。缺省情况，将用户证书中主题部分内的 CN 字段的值作为 SSL VPN 用户名
开启密码认证	开启密码认证功能后，用户可以通过用户名、密码登录
证书和密码认证	可以同时使用，也可以只使用任意一种
开启验证码验	开启验证码验证功能后，用户登录时需要输入验证码。只有验证码验证成功

参数	说明
证	后，才允许用户登录 SSL VPN 页面
iMC 用户改密	实现 iMC 认证用户修改密码功能，需要配置 iMC 服务器地址、端口号及所属 VPN 实例，且需要开启允许在线修改密码功能
开启短信认证-iMC	本功能需要在 iMC 服务器上提前配置好短信验证功能 开启 iMC 短信认证功能后，当用户登录 SSL VPN 网关进行身份验证时，可以获取短信验证码
开启短信认证-短信网关	本功能需要在短信网关上提前配置好短信验证功能 开启短信网关认证功能后，当用户登录 SSL VPN 网关进行身份验证时，可以获取短信验证码
开启企业微信认证	本功能需要在企业微信管理后台提前配置企业应用，并在各应用中配置应用主页重定向链接和 SSL VPN 网关的可信域名，并完成可信域名的校验（在企业微信管理后台下载校验文件，并在 SSL VPN 全局配置界面将文件上传至设备） 开启企业微信认证功能后，设备将从第三方企业微信获取企业用户信息，并使用该用户信息对用户进行认证和授权
应用 ID	如需使用企业微信扫码认证方式对用户进行认证和授权，则必须配置应用 ID
API 服务器地址	配置 API 服务器地址后，当设备收到从企业微信服务器重定向而来的报文时，设备将企业微信 API 服务器进行信息交互，获取用户信息，并使用获取到的信息对用户进行认证和授权
企业 ID	企业微信上唯一标识一个企业
访问密钥	企业应用中用于保障数据安全的“钥匙”，每一个应用都有一个独立的访问密钥，为了保证数据的安全，此密钥务必不能泄漏
认证请求超时时间	SSL VPN 网关向企业微信 API 服务器发送 HTTP 请求报文后，如果在超时时间内没有收到服务器的应答报文，则认为本次企业微信认证失败
userid 字段名	企业微信 userid 字段名，用于 SSL VPN 网关向内网服务器发起访问请求时，组装携带用户信息的登录参数
授权策略组字段名	企业微信授权策略组字段名，用于 SSL VPN 网关从企业微信 API 服务器获取的应答报文中解析企业微信授权策略组名称
微信开放平台 URL	配置微信开放平台的 URL 后，当内网服务器需要再次认证客户端身份时，客户端将能够正常访问微信开放平台，完成后续的认证 用户可以进行如下配置： ● 预定义：表示预定义的URL地址，为https://open.weixin.qq.com，用户无法修改 ● 自定义：表示自定义的URL地址，用户可以根据实际情况配置URL地址

参数	说明
防止暴力破解	为了防止暴力破解攻击，可以配置如下限制： ● 用户在连续登录错误达到指定的次数时启用图形验证码 ● 可限制同IP用户登录连续出错指定次数后，拒绝同IP登录，并在指定的时长后恢复正常状态

6.17.4.4.4 URI ACL资源

URI形式的ACL用于对SSL VPN的各种接入方式进行更精细的控制。对URL进行匹配，符合要求的URL请求可以访问对应的资源。

在SSL VPN访问实例中可以创建多个URI ACL，并且每个URI ACL下又可以配置多条URI ACL规则。若一个URI ACL中配置了多条URI ACL规则，则按照规则编号由小到大进行匹配。

在Web代理和资源组中，可以引用URI ACL进行过滤。

具体配置步骤如下：

步骤1　选择“URI ACL资源”页签。

步骤2　单击<新建>按钮，进入“新建URI ACL列表”页面，配置URI ACL列表名称。

步骤3　在“URI ACL资源”区域，单击<新建>按钮，进入“新建URI ACL规则”页面，具体配置内容如下：

参数	说明
规则 ID	规则编号。URI ACL 在匹配过滤时会按照规则编号从小到大的顺序依次匹配报文，一旦匹配上某条规则便结束匹配过程
动作	对匹配规则的报文的处理动作，动作包括允许报文通过和拒绝报文通过
规则内容	格式为 protocol://host:port/path，protocol 和 host 必须指定

步骤4　单击<确定>按钮，完成配置URI ACL规则。

步骤5　单击<确定>按钮，完成配置URI ACL列表。

6.17.4.4.5 快捷方式

本功能通过将用户常用的URL配置为快捷方式，方便用户使用。配置后，用户可以在Web页面上单击指定的快捷方式访问资源。

具体配置步骤如下：

步骤1　选择“快捷方式”页签。配置快捷方式和快捷方式列表。

步骤2　在快捷方式区域，单击<新建>按钮，进入“新建快捷方式”页面，具体配置内容如下：

参数	说明
快捷方式名称	快捷方式的名称
描述	快捷方式的描述信息
资源地址	资源地址包括三种类型： ● 资源链接：快捷方式对应的资源链接，用户可以在Web页面上单击指定的链接访问资源，需要按照**url**('*url-value*')模板配置。*url-value*由协议类型、主机名称或地址、端口号、资源路径四部分组成，完整格式为“协议类型://主机名称或地址:端口号/资源路径” ● 应用程序路径：快捷方式对应的应用程序路径，需要按照**app**('*app-value*')模板配置。程序路径可以使用绝对路径也可以使用环境变量，例如“c:\windows\system32\notepad++.exe” ● 自定义：SSL VPN网关管理员可以自己编写任意一个可执行的JavaScript脚本，实现访问特定的资源

步骤3　单击<确定>按钮，完成配置快捷方式。

步骤4　在快捷方式列表区域，单击<新建>按钮，进入“新建快捷方式列表”页面，具体配置内容如下：

参数	说明
列表名称	快捷方式列表的名称
选择快捷方式	在已配置的快捷方式中选择快捷方式

步骤5　单击<确定>按钮，完成配置快捷方式列表。

6.17.4.4.6　用户管理

步骤1　在“用户管理”页签，单击<新建>按钮，进入“新建用户管理”页面，具体配置内容如下：

参数	说明
用户名	SSL VPN 的用户名称
手机号码	SSL VPN 用户绑定的手机号码
自动绑定 IPv4 地址	开启自动绑定 IPv4 地址功能后，SSL VPN 网关为客户端自动分配空闲的 IPv4 地址，并绑定，可以配置绑定的空闲 IPv4 地址的个数
自动绑定 IPv6 地址	开启自动绑定 IPv6 地址功能后，SSL VPN 网关为客户端自动分配空闲的 IPv6 地址，并绑定，可以配置绑定的空闲 IPv6 地址的个数
绑定的 IPv4 地址	不能包含组播、广播、环回地址。可以包含 IPv4 地址和地址范围，地址或地址范围之间以“,”隔开，地址范围中的起始和结束地址用“-”隔开，结束地址必须大于或等于起始地址。例如：10.1.1.5,10.1.1.10-10.1.1.20

参数	说明
绑定的 IPv6 地址	只能是单播或任播地址，不能是未指定、多播、环回地址。可以包含 IPv6 地址和 IPv6 地址范围，地址和地址范围之间以“,”隔开，地址范围中的起始和结束地址用“-”隔开，结束地址必须大于或等于起始地址。例如： 1234::10,1234::100-1234::200

步骤2　单击<确定>按钮，完成配置用户管理。

步骤3　单击<完成>按钮，完成配置访问实例。

6.17.4.5　配置网关

步骤1　选择“网络 > VPN > SSL VPN > 网关”。

步骤2　在“网关”页面单击<新建>按钮，进入“新建网关”页面，具体配置内容如下：

参数	说明
网关	SSL VPN 网关的名称
IP 地址选择方式	SSL VPN 网关 IP 地址的选择方式，包括使用接口 IP 地址和自定义 IP 地址
IP 地址类型	SSL VPN 网关的 IP 地址类型，包括 IPv4 和 IPv6
使用接口 IP	可通过在下拉框中选择指定的接口获取相应的 IP 地址作为 SSL VPN 网关的 IP 地址 不可选择设备的管理地址
IP 地址	SSL VPN 网关的 IP 地址
HTTPS 端口	SSL VPN 网关的 HTTPS 端口号
SSL 服务器端策略	SSL VPN 网关引用的 SSL 服务器端策略
开启量子加密	开启国盾量子加密功能后，SSL VPN 将使用量子密钥对 SSL VPN 报文进行加解密 其中，用户可以根据实际需求选择是否强制使用量子加密 ● 如果选择强制，则SSL VPN网关只能接受使用量子加密功能的iNode客户端与之进行SSL协商，其他客户端无法接入 ● 如果选择非强制，则当iNode客户端与SSL VPN网关进行SSL协商时使用了量子加密功能，那么该协商过程会使用量子密钥；当iNode客户端没有使用量子加密功能或SSL VPN用户通过Web接入，则该协商过程会使用非量子密钥方式进行SSL协商 国盾量子加密功能的支持情况与设备型号有关，请以设备实际情况为准
VRF	SSL VPN 网关所属的 VRF 本参数仅支持在编辑网关页面进行配置

参数	说明
使能	开启 SSL VPN 网关

步骤3　单击<确定>按钮，完成网关配置。

6.17.4.6　客户端地址池

步骤1　选择“网络 > VPN > SSL VPN > 客户端地址池”。

步骤2　在“客户端IPv4地址池”页面单击<新建>按钮，进入“新建客户端IPv4地址池”页面，具体配置内容如下：

参数	说明
地址池名称	客户端 IPv4 地址池的名称
起始地址	客户端 IPv4 地址池的起始地址
结束地址	客户端 IPv4 地址池的结束地址

步骤3　单击<确定>按钮，完成客户端IPv4地址池配置。

步骤4　在“客户端IPv6地址池”页面单击<新建>按钮，进入“新建客户端IPv6地址池”页面，具体配置内容如下：

参数	说明
地址池名称	客户端 IPv6 地址池的名称
起始 IPv6 地址	客户端 IPv6 地址池的起始地址
结束 IPv6 地址	客户端 IPv6 地址池的结束地址

步骤5　单击<确定>按钮，完成客户端IPv6地址池配置。

6.17.4.7　IP接入接口

步骤1　选择“网络 > VPN > SSL VPN > IP接入接口”。

步骤2　单击<新建>按钮，进入“新建接口”页面，输入接口编号，单击<确定>按钮，进入<修改接口设置>页面，配置接口安全域和IP地址。

步骤3　单击<确定>按钮，完成IP接入接口配置。

6.17.4.8 模板管理

步骤1 选择“网络 > VPN > SSL VPN > 模板管理”。

步骤2 单击<新建>按钮，进入“新建自定义模板”页面，管理员可以上传自定义页面模板。

步骤3 单击<确定>按钮，完成配置。上传后，管理员可在“全局配置”或“编辑访问实例”页面引用该页面模板。

6.17.4.9 统计信息

在“统计信息”页面，管理员可以查看在线用户统计、在线用户信息、锁定用户信息、锁定IP信息，以及IP接入相关的统计信息。

6.17.5 常见问题解答

6.17.5.1 某些资源的访问权限发生变化后，为什么不会立即生效？

这是因为SSL VPN不支持动态授权，权限变化的生效范围及生效时间如下表所示。

权限变化方式	生效范围及时间
远程服务器授权变化	对已经登录用户不生效，仅对新登录的用户生效
资源组引用的 ACL 变化或 ACL 内的规则变化	隧道业务方式、TCP 代理方式和 Web 代理方式，均立即生效
Web 接入资源变化	SSL VPN 用户刷新页面后，可以看到资源变化
TCP 代理资源变化	SSL VPN 用户重新启动客户端软件后，变化生效
隧道业务方式中的路由表项、DNS 服务器地址、WINS 服务器地址变化	立即生效

6.17.5.2 SSL VPN用户登录SSL VPN网关时，是否需要进行证书认证？

SSL VPN用户作为SSL客户端登录SSL VPN网关时，SSL客户端证书认证的三种方式及其区别如下表所示。

认证方式	说明
关闭客户端证书认证	在使用浏览器访问 SSL VPN 网关时，不会提示用户选择证书，不对客户端进行证书认证
开启客户端证书认证	在使用浏览器访问 SSL VPN 网关时，会提示用户选择证书。如果用户没有证书，则会断开 SSL 连接
不强制要求客户端证书认证	在使用浏览器访问 SSL VPN 网关时，会提示用户选择证书。如果用

认证方式	说明
	户不使用证书，则 SSL 连接依然有效，此时并不会断开 SSL 连接。 如果用户选择证书，但是服务器检查客户端证书未通过，则会断开 SSL 连接

当SSL VPN管理员认为需要对SSL VPN用户进行证书认证时，应该将SSL VPN网关引用的SSL服务器端策略配置为后两种方式，并使能SSL VPN的证书认证功能。SSL VPN证书认证功能会比较证书中的CN字段和用户名是否匹配，如果不匹配，则会禁止访问。

对于SSL VPN证书认证功能，仅在Web接入和隧道业务方式下，支持SSL服务器端强制要求对SSL客户端进行基于数字证书的身份验证；在TCP代理和移动客户端接入方式下，不支持SSL服务器端强制要求对SSL客户端进行基于数字证书的身份验证。

6.18 路由表

6.18.1 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。

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，显示内容包括如下：

参数	说明
目的地址	路由的目的 IPv4/IPv6 地址

参数	说明
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

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，统计内容包括如下：

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

6.18.2 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。

6.19 静态路由

6.19.1 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。

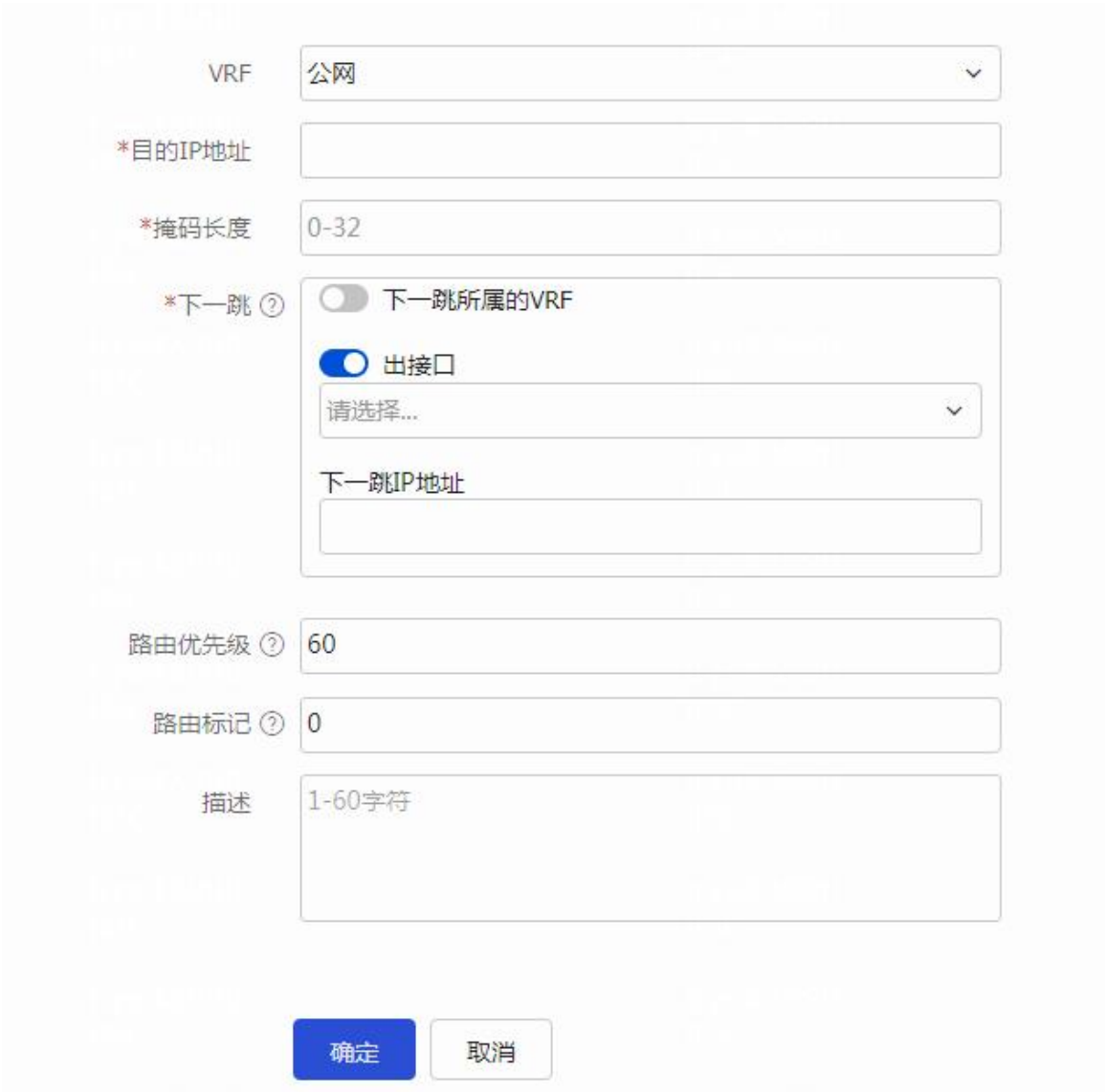
缺省路由是在没有找到匹配的路由表项时使用的路由。配置IPv4缺省路由时，指定目的地址为0.0.0.0/0；配置IPv6缺省路由时，指定目的地址为::/0。

6.19.2 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。

6.19.3 配置指南

步骤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。



步骤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所示：

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”页面才会显示本参数 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由。当没有匹配的路由表项时，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”页面才会显示本参数
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

参数	说明
	显示本参数
前缀长度	目的 IPv6 地址的前缀长度，只有在“新建 IPv6 静态路由”页面才会显示本参数
vSystem 互通	开启/关闭缺省 vSystem 与非缺省 vSystem 以及非缺省 vSystem 之间的相互通信 开启 vSystem 互通时，不需要指定下一跳 IP 地址
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，为同一目的地配置多条路由，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，则实现路由备份
路由标记	静态路由的标记
描述	静态路由的描述信息

步骤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。

6.20　策略路由

本帮助主要介绍以下内容：

6.20.1 特性简介

6.20.1.1 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）。

6.20.1.2 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。

6.20.1.3 节点匹配

6.20.1.3.1 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。

6.20.1.3.2 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。

6.20.1.4 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。

6.20.2 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。

6.20.3 配置指南

步骤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。

步骤2 单击<新建>按钮，新建IPv4/IPv6策略路由。

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

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操作
模式	指定策略节点的匹配模式，包括： ● 允许 ● 拒绝

参数	说明
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ACL策略，也可以新创建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，也可以新创建服务对象组。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，也可以新创建应用组。仅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，每个数值对应一个优先级类型
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，起到主备或负载分担的作用 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示
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，起到主备或负载分担的作用 1） 单击<新建>按钮，新建报文转发的出接口

参数	说明
	● 接口 ● 缺省 ● Track项 2) 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 NBMA 类型的接口），比如以太网接口、Virtual-Template 接口，由于有多个可能的下一跳，可能会造成报文转发不成功的现象

步骤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。

步骤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。

6.21　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OSPF实例

- 配置OSPFv2区域
- 配置OSPFv3区域

6.21.1 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。

6.21.1.1 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。

6.21.1.2 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。

6.21.1.3 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。

6.21.1.4 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。

6.21.1.5 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。

6.21.1.6 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。

6.21.2 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。

6.21.3 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。

6.21.4 配置指南

6.21.4.1 配置OSPF实例

步骤1 选择“网络 > 路由 > OSPF”。

步骤2 在“OSPF实例”页面单击<新建>按钮，进入“新建OSPF实例”页面。

步骤3　新建OSPF实例，具体配置内容如下表所示：

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

步骤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。

6.21.4.2　配置OSPFv2区域

步骤1　选择“网络 > 路由 > OSPF”。

步骤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。

步骤3　在“OSPFv2区域”页面单击<新建>按钮，进入“新建OSPFv2区域”页面。

步骤4　新建OSPFv2区域，具体配置内容如下表所示：

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 ● 验证密码：为了避免路由信息外泄或者OSPF路由器受到恶意攻击，OSPF提供报文验证功能，邻居路由器两端接口的验证模式和验证密钥必须一致 ● 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

参数	说明
	的收敛速度以及协议报文带来的网络负荷

步骤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。

步骤6　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。

步骤7　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所示。

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

步骤8　单击<确定>按钮，OSPFv2引入外部路由配置成功。

6.21.4.3　配置OSPFv3区域

步骤1　选择“网络 > 路由 > OSPF”。

步骤2　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。

步骤3　在“OSPFv3区域”页面单击<新建>按钮，进入“新建OSPF区域”页面。

步骤4　新建OSPFv3区域，具体配置内容如下表所示：

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

步骤5　单击<确定>按钮，新建OSPFv3区域成功，并会在OSPFv3区域页面中显示。

步骤6　点击“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。

步骤7　在“OSPFv3接口”页面单击<新建>按钮，进入“新建接口”页面。

步骤8　新建OSPFv3接口，具体配置内容如下表所示：

参数	说明

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

步骤9　单击<确定>按钮，新建接口成功，并会在OSPFv3接口页面中显示。

6.22　RIP

6.22.1　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。

6.22.2　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。

6.22.3　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。

6.22.4　配置指南

步骤1　选择“网络 > 路由 > RIP”，进入RIP页面。

步骤2　单击<新建>按钮，新建RIP实例。

参数	说明
实例 RIP	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

参数	说明
	● 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或RIP协议类型才需要输入本参数 ● 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

步骤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。

步骤4　进入“RIP接口设置”页面。

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规定的报文格式 ● MD5（RFC 2453）：指定MD5验证报文使用RFC 2082规定的报文格式 当 RIP 的版本为 RIPv1 时,虽然仍然可以配置验证方式,但由于 RIPv1 不支持认证，因此该配置不会生效
	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

步骤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。

步骤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。

6.23 DHCP

本帮助主要介绍以下内容：

6.23.1 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。

6.23.2 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。

6.23.2.1 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：

步骤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。

步骤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。

6.23.2.2 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：

步骤1 与客户端MAC地址或客户端ID静态绑定的IP地址。

步骤2 DHCP服务器记录的曾经分配给客户端的IP地址。

步骤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。

步骤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。

步骤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。

6.23.2.3　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。

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

6.23.2.4　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。

6.23.3 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。

6.23.4 配置指南

6.23.4.1 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。

6.23.4.2 地址分配

步骤1 选择“网络 > DHCP > 服务”。

步骤2 在服务页面，启用DHCP服务。

步骤3 单击指定设备接口的<编辑>按钮，可配置设备接口工作在DHCP服务器模式。

步骤4 选择“网络 > DHCP > 地址池”。

步骤5 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，新建DHCP服务池。

步骤6 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。

步骤7 选择“地址分配”页签，进入地址分配页面，具体配置内容如下表所示：

参数	说明

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个字符的字符串，字符串中只能包括十六进制数和“-”，且形式为H-H-H…，除最后一个H表示2位或4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个字符的字符串，字符串中只能包括十六进制数和“-”，且形式为H-H-H…，除最后一个H表示2位或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

步骤8 单击<确定>按钮，保存配置。

6.23.4.3 地址池选项

步骤1 选择“地址池选项”页签，进入地址池选项页面，具体配置内容如下表所示：

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，DHCP客户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析
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

参数	说明
	行转发 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 服务器应在为客户端指定 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 NetBIOS 协议通信的主机提供主机名到 IP 地址的解析。所以，大部分 Windows 网络客户端需要进行 WINS 的设置。为了使 DHCP 客户端实现主机名到 IP 地址的解析，DHCP 服务器应该为 DHCP 客户端指定 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 协议通信时，需要在主机名和 IP 地址之间建立映射关系。根据获取映射关系方式的不同，NetBIOS 节点包括： ● 广播（Broadcast）：此类节点采用广播方式获取映射关系。源节点通过发送带有目的节点主机名的广播报文来获取目的节点的IP地址，目的节点收到广播报文后，就将自己的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服务器通信的方式获取映射关系。源节点给WINS服务器发送单播报文，WINS服务器收到单播报文后，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，如果没有获取到，则再发送单播报文与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服务器通信来获取映射关系，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 1） 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IP地址 ● 选项内容：DHCP选项内容

参数	说明
	2) 单击<确定>按钮，新建的 DHCO 选项显示在 DHCP 选项列表中

步骤2 单击<确定>按钮，保存地址池选型配置。

步骤3 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。

6.24 HTTP/HTTPS

本帮助主要介绍以下内容：

6.24.1 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。

6.24.2 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。

6.24.3 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。

6.24.4 配置指南

6.24.4.1 HTTP登录

步骤1 单击“网络 > 服务 > HTTP/HTTPS”。

步骤2 在“HTTP/HTTPS”页面进行HTTP服务配置。

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

参数	说明
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

步骤3　单击<应用>按钮，保存当前配置。

6.24.4.2　HTTPS登录

步骤1　在“HTTP/HTTPS”页面进行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

步骤2　单击<应用>按钮，保存当前配置。

6.24.4.3　HTTP/HTTPS登录空闲超时时间

步骤1　在“HTTP/HTTPS”页面，设置HTTP/HTTPS登录用户连接的超时时间。

步骤2　单击<应用>按钮，保存当前配置。

6.25　SSH

本帮助主要介绍以下内容：

6.25.1　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。

6.25.2　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。

6.25.3　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。

6.25.4 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。

6.25.4.1 配置步骤

步骤1 单击“网络 > 服务 > SSH”。

步骤2 在“SSH”页面开启Stelnet/SFTP/SCP服务，具体配置内容如下：

参数	说明
服务器发送的 IPv4 报文的 DSCP 优先级	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，决定报文传输的优先程度
服务器发送的 IPv6 报文的 DSCP 优先级	DSCP 携带在 IPv6 报文中的 Trafic class 字段，用来体现报文自身的优先等级，决定报文传输的优先程度
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，运行所有 IPv4 客户端向设备发起 SSH 访问，否则只运行匹配 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，运行所有 IPv6 客户端向设备发起 SSH 访问，否则只运行匹配 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	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。开启本功能后，SSH 服务器需要等待后续有新的 SSH1 用户登录，才

参数	说明
隔	会更新当前的 RSA 服务器密钥对，然后使用新的 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，其中等待的最小时长就为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 用户登录才会再次触发 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地猜测和破解
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的连接。 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，妨碍其它合法用户的正常登录，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，从而有效避免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，可适当减小该值，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

步骤3　单击“应用”按钮，完成配置。

6.26　NTP

6.26.1　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。

6.26.2 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。

6.26.3 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。

6.26.4 配置指南

步骤1 单击“网络 > 服务 > NTP”。

步骤2 在“NTP”页面单击<开启>，开启NTP服务。

步骤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。

步骤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。

步骤5 单击<应用>按钮，本地时钟配置成功。

步骤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。

步骤7 单击<新建>按钮，配置身份验证密钥如下：

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

步骤8　单击<确定>按钮，完成身份验证密钥的配置。

6.27　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

6.27.1　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。

6.27.2　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。

6.27.3　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。

6.27.4　配置指南

要实现FTP服务器功能，需要进行如下配置：

配置步骤

步骤1　选择“网络>服务>FTP”

步骤2　单击<开启>按钮启用FTP服务。

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

参数	说明
	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”

步骤3　点击<应用>按钮，完成FTP服务与高级设置的配置。

6.28　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

6.28.1　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，其它用户不允许访问设备，可以避免非法用户通过Telnet访问设备。

6.28.2 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。

6.28.3 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。

6.28.4 配置指南

要实现Telnet服务器功能，需要进行如下配置：

配置步骤

步骤1 选择“网络 > 服务 > Telnet”

步骤2 单击<开启>按钮启用Telnet服务。

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”

步骤3 单击<应用>按钮，完成Telnet服务高级设置的配置。

6.29 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

6.29.1 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，它既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。

6.29.1.1 授权VLAN

是指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。

6.29.1.2 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。

6.29.1.3 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。

6.29.1.4 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。

6.29.2 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。

6.29.3 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Critial VLAN的注意事项

- 配置Critial 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Critial 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Criital 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Critial VLAN功能不生效。

6.29.4 配置指南

步骤1 选择“网络 > 安全接入 > MAC接入 > MAC地址认证”。

步骤2 在“MAC地址认证”页面勾选“开启”，开启全局MAC地址认证功能。

步骤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。

步骤4 单击接口对应的“编辑”按钮，进入“编辑MAC地址认证”页面。

步骤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：

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

参数	说明
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

步骤6　单击<确定>按钮，配置接口MAC地址认证完成。

步骤7

6.30　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
  - 手动新建MAC地址白名单配置步骤

6.30.1　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。

6.30.2　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。

6.30.3　配置指南

6.30.3.1　手动新建MAC地址白名单配置步骤

步骤1　选择“网络 > 安全接入 > MAC接入 > MAC地址白名单”。

步骤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。

步骤3　在“新建MAC地址白名单”页面的具体配置内容如下表所示：

参数	说明

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”，且不支持配置
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

步骤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。

6.31　静默MAC信息

本帮助主要介绍以下内容：

6.31.1　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。

6.31.2　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。

6.31.3　配置指南

6.31.3.1　静默MAC显示信息

步骤1　选择“网络 > 安全接入 > MAC接入 > 静默MAC信息”。

步骤2　进入“静默MAC信息”页面，具体显示内容如下表所示：

参数	说明
MAC 地址	静默用户的 MAC 地址

参数	说明
VLAN	静默用户所在的 VLAN
接口	静默用户接入的端口名称

6.32 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
  - 高级设置配置步骤

6.32.1 特性简介

6.32.1.1 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。

6.32.1.2 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。

6.32.1.3 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。

6.32.1.4 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。

6.32.1.5 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。

6.32.2 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。

6.32.3 配置指南

6.32.3.1 高级设置配置步骤

步骤1 单击“网络 > 安全接入 > MAC接入 > 高级设置”。

步骤2 在开启全局MAC地址认证功能后。

步骤3 在“高级设置”页面的具体配置内容如下表所示：

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 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	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 > 认证管理 > ISP 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，没有收到没有收到 RADIUS 服务器的应答，则设备将禁止此用户访问网络
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

步骤4 单击<应用>按钮，MAC接入高级设置配置完成。

6.33 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

6.33.1 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。

6.33.2 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。

6.33.3 配置指南

6.33.3.1 配置IP地址认证

IP地址认证的具体配置如下：

步骤1 选择“网络 > 安全接入 > IP接入 > IP地址认证”。

步骤2 单击接口对应的“编辑”按钮，进入“编辑IP认证设置”页面。

步骤3 配置该接口的IP地址认证参数，具体配置内容如下表所示：

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连接接入设备。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，用户可直接连接接入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

步骤4　单击<确定>按钮，配置接口IP地址认证完成。

6.33.3.2　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：

步骤1　选择“网络 > 安全接入 > IP接入 > IP地址认证”。

步骤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。

步骤3　配置IP接入日志的基本信息，具体配置内容如下表所示：

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

步骤4　单击<确定>按钮，完成IP接入日志的基本信息配置。

6.34　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

6.34.1　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。

6.34.2　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。

6.34.3 配置指南

IPv4地址白名单的具体配置如下：

步骤1 选择“网络 > 安全接入 > IP接入 > IPv4地址白名单”。

步骤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。

步骤3 新建IPv4地址白名单，具体配置内容如下表所示：

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”
描述	配置该用户白名单的描述信息

步骤4 单击<确定>按钮，新建IPv4地址白名单完成。

6.35 IPv6地址白名单

本帮助主要介绍以下内容：

6.35.1 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。

6.35.2 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。

6.35.3 配置指南

IPv6地址白名单的具体配置如下：

步骤1 选择“网络 > 安全接入 > IP接入 > IPv6地址白名单”。

步骤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。

步骤3　新建IPv6地址白名单，具体配置内容如下表所示：

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”
描述	配置该用户白名单的描述信息

步骤4　单击<确定>按钮，新建IPv6地址白名单完成。

7 系统

7.1 高可靠性

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

7.1.1 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。

7.1.1.1 基本概念

双机热备技术包含的基本概念如下：

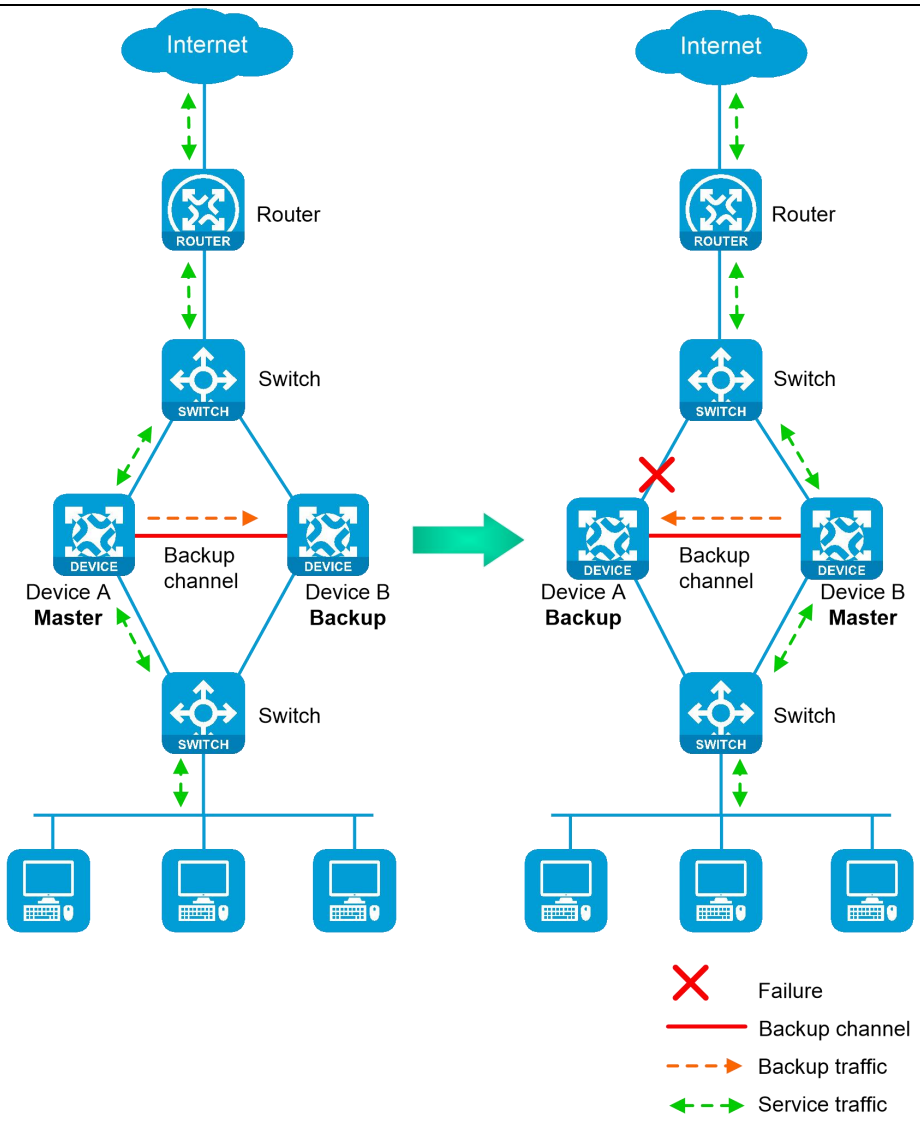
- 主、从管理设备：双机热备中的设备分为主、从两种管理角色，用于控制设备之间关键配置信息的同步。双机热备建立成功后，只能在主管理设备配置相关业务（支持配置信息同步的功能），从管理设备不能配置。配置信息将从“主管理设备”同步到“从管理设备”，并覆盖从管理设备上的相关配置信息。
- 主、备业务设备：双机热备中包含主、备两种设备，其中主设备对应VRRP备份组中的Master设备；备设备对应VRRP备份组中的Backup设备。主设备为业务提供支持，转发业务流量，并向备设备实时备份业务表项信息；备设备除接收主设备的业务表项备份信息外，在主设备发生故障后，备设备会转换成主设备，继续转发业务流量，保证业务不中断。
- 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：支持主备和双主两种运行模式。主备模式下，仅由主设备处理业务，备设备处于空闲状态，实时待命；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。

7.1.1.2 运行模式

双机热备支持主备和双主两种运行模式，具体介绍如下。

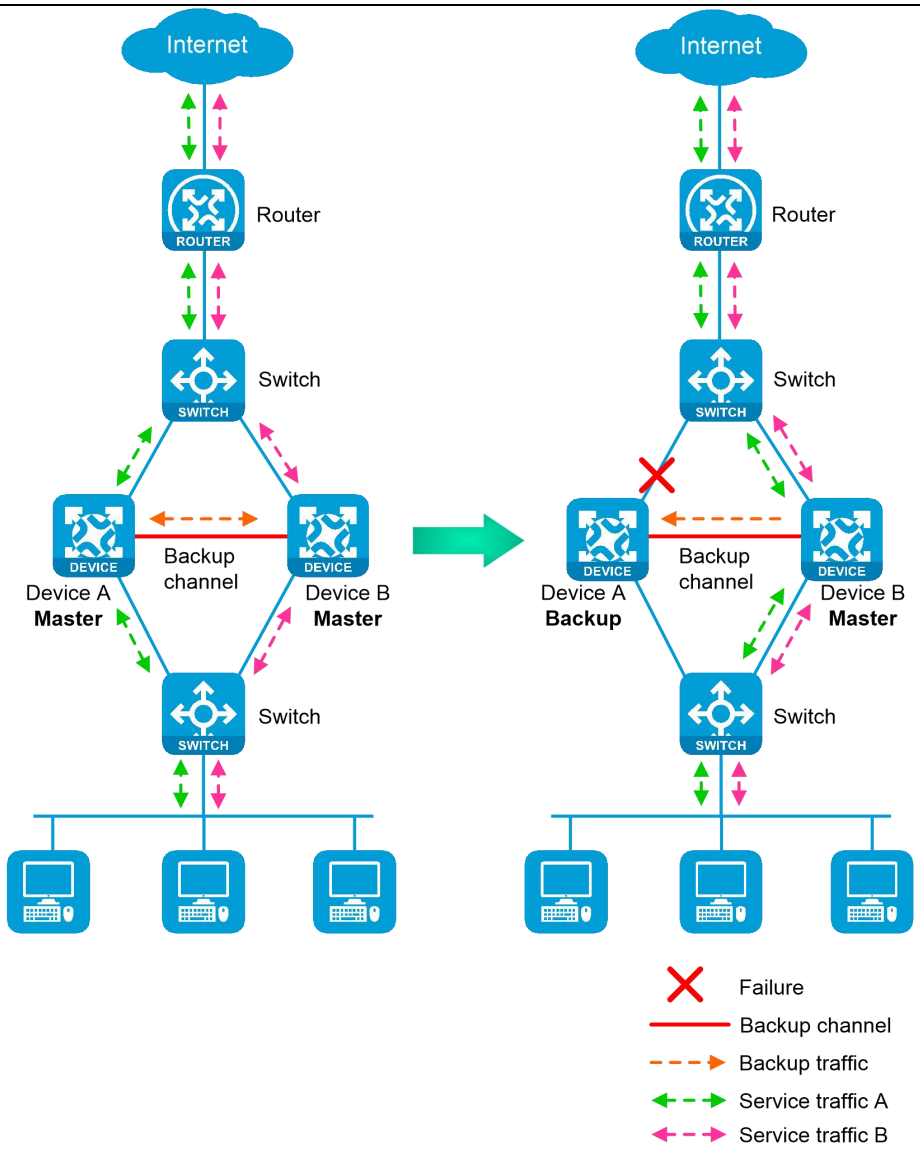
7.1.1.2.1 主备模式

如下图所示，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。



7.1.1.2.2 双主模式

如下图所示，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。



7.1.1.3 双机热备通道

7.1.1.3.1 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，包括以下两种类型的通道：

- 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。数据通道直接使用底层驱动进行数据传输，因此仅支持二层转发。

7.1.1.3.2 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。

7.1.1.4 业务表项备份

7.1.1.4.1 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。

7.1.1.4.2 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。

7.1.1.5 配置信息备份

7.1.1.5.1 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。

7.1.1.5.2 备份方式

双机热备支持自动和手动两种方式进行配置信息备份。

7.1.1.5.3 支持配置信息备份的模块

目前双机热备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。
- 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：VLAN、信息中心、云平台连接、IPoE。

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。

7.1.1.6 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。

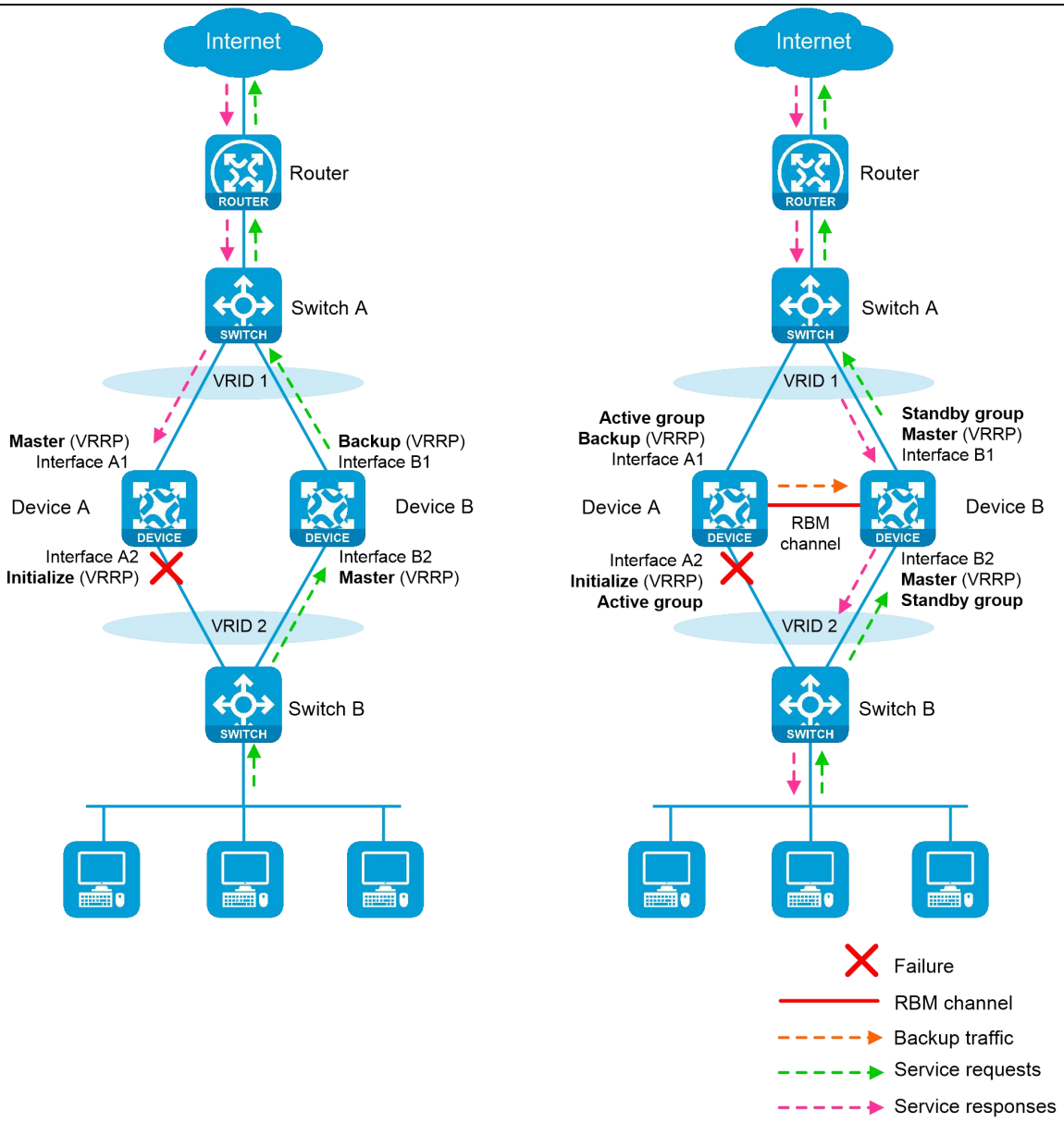
7.1.1.7 双机热备联动VRRP

7.1.1.7.1 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。

- 如下图的左图所示，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。
- 如下图的右图所示，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。



7.1.1.7.2 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。

7.1.1.7.3 双机热备联动VRRP组网中Master设备的选举机制

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：

步骤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。

步骤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。

步骤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。

步骤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。

7.1.1.7.4 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。

7.1.1.8 双机热备联动虚拟地址

7.1.1.8.1 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。

7.1.1.8.2 运行机制

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：

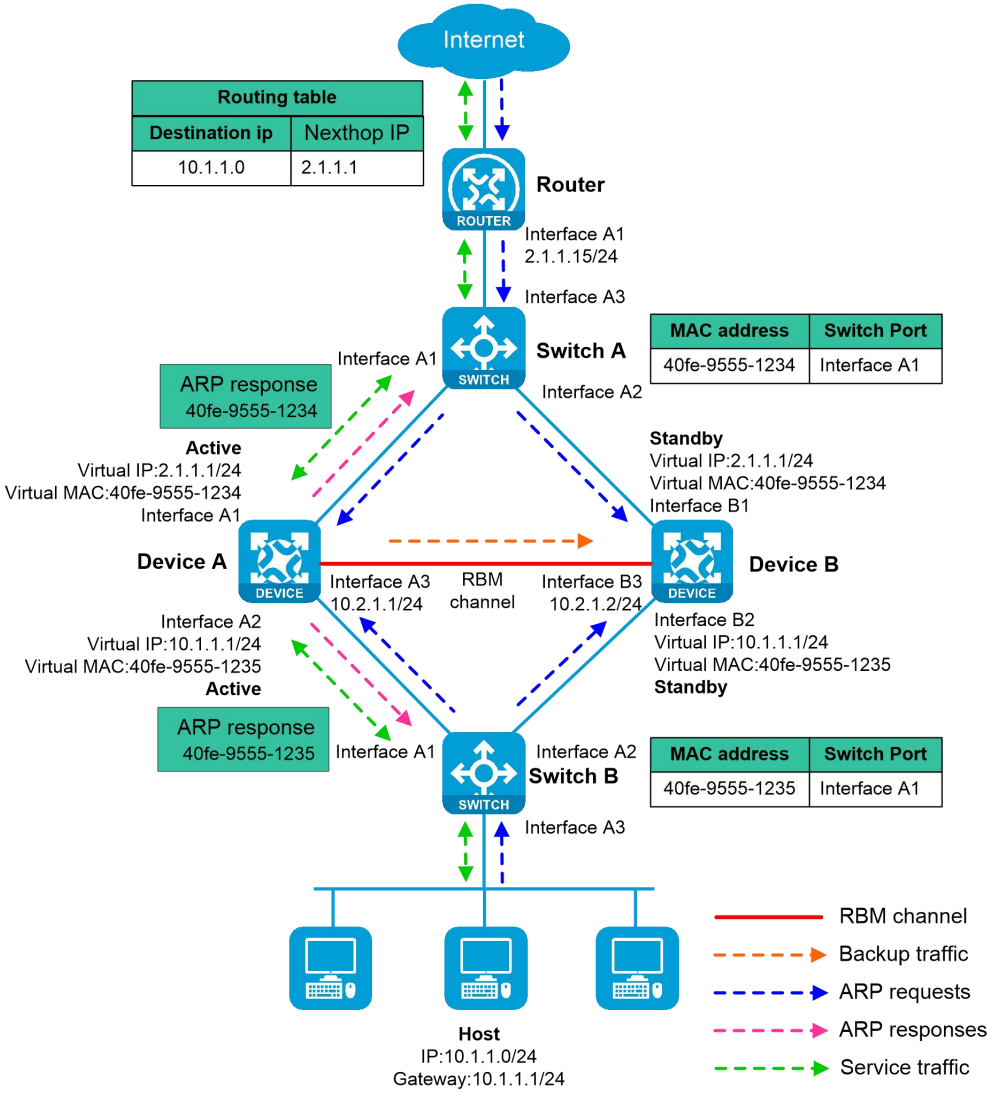
步骤1 当内网Host访问外网时，在Host发送业务请求报文前，首先会广播ARP请求报文，学习网关虚拟IP地址10.1.1.1对应的MAC地址。

步骤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。

步骤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。

步骤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。

步骤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。



7.1.1.9 双机热备联动路由

7.1.1.9.1 功能简介

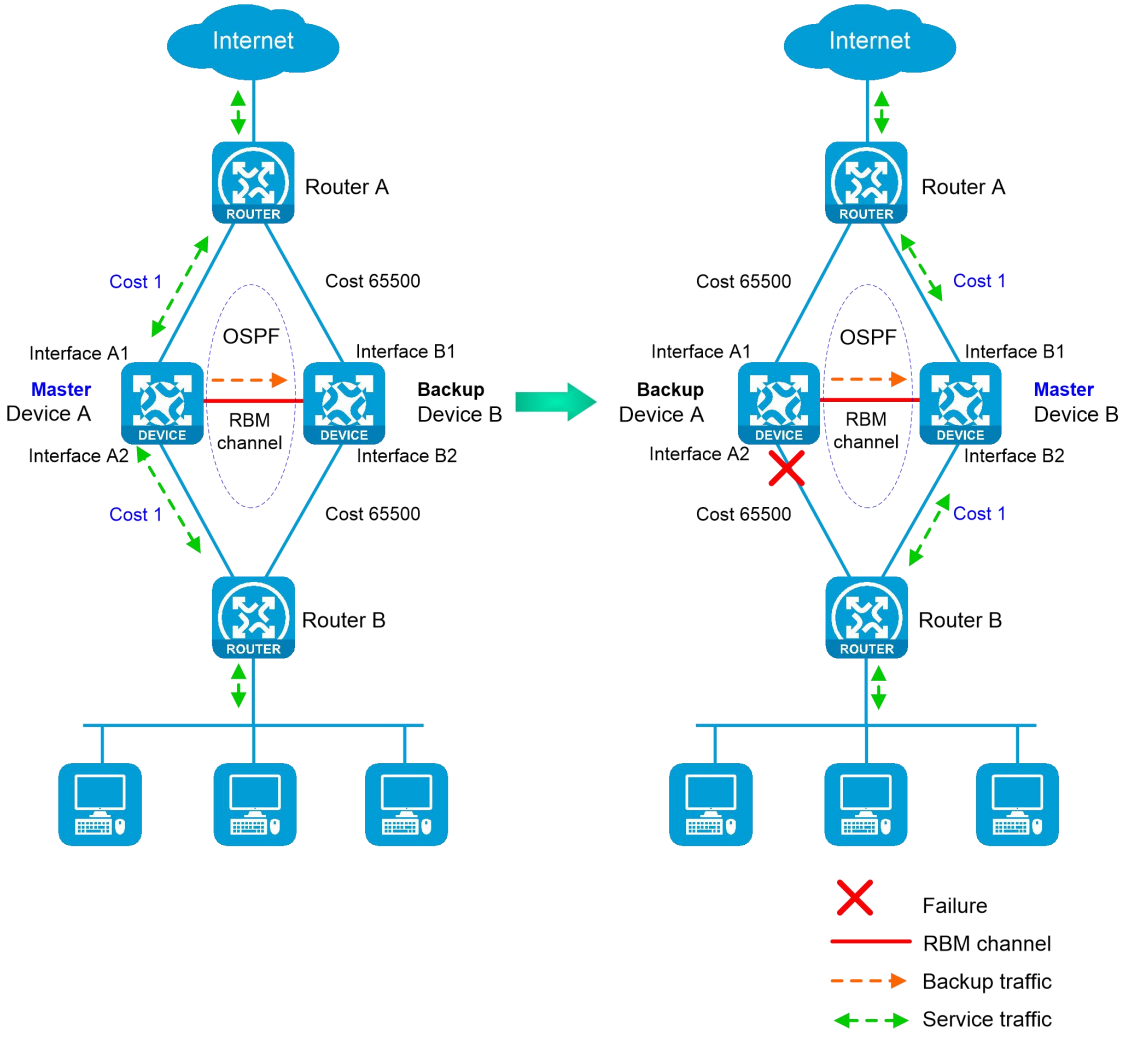
在双机热备与动态路由联动的组网环境中，双机热备将会调整备设备上动态路由协议对外通告的链路开销值。这样可以保证主备切换时使设备的上下行流量同时切换到新的主设备，保证业务不中断。

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。

- 如下图左图所示，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。

- 如下图右图所示，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。



7.1.1.9.2 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。

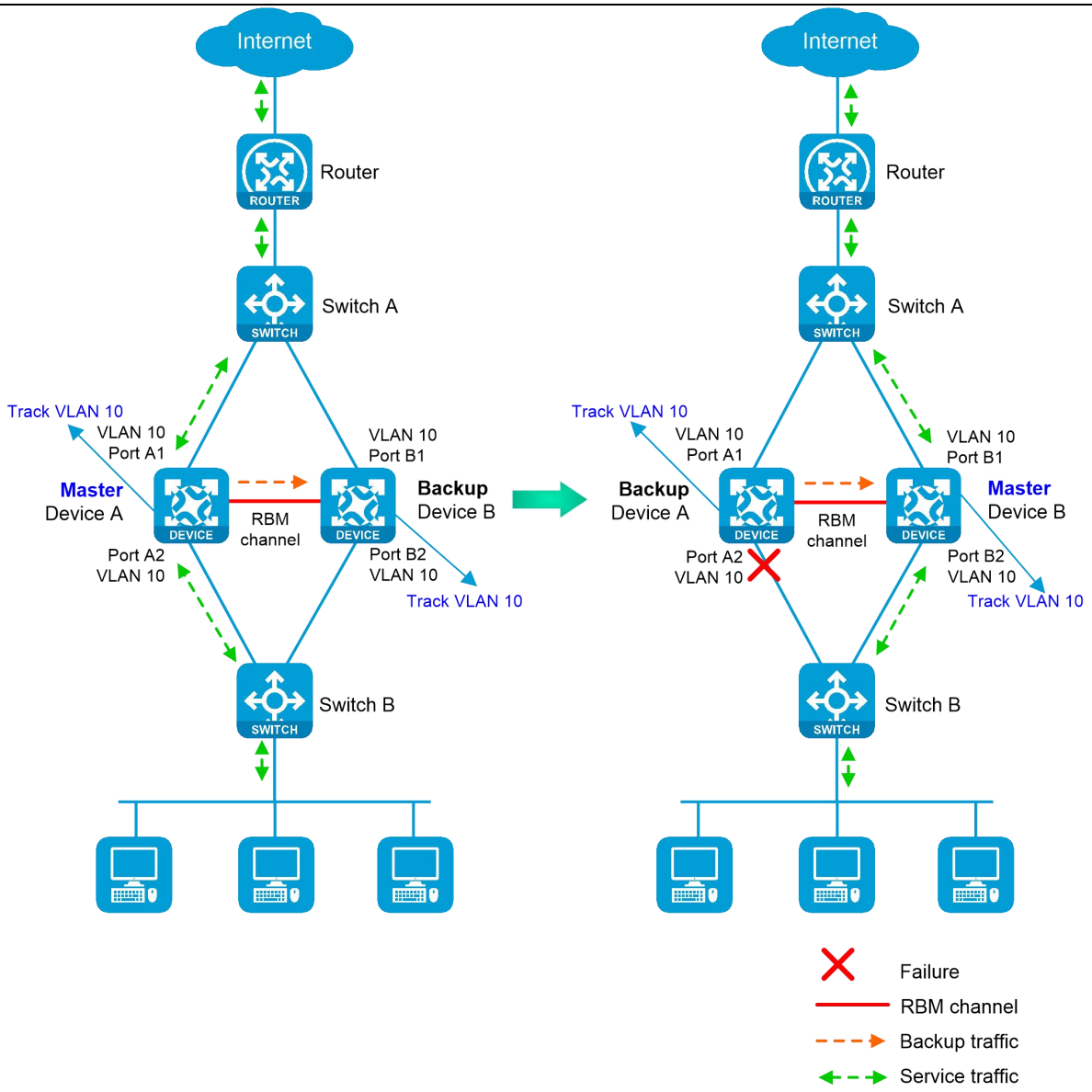
7.1.1.10 双机热备透明组网

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。

- 如下图左图所示，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。
- 如下图右图所示，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。



7.1.2 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。

7.1.3 使用限制和注意事项

7.1.3.1 硬件环境一致

部署HA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。

7.1.3.2 软件环境一致

部署HA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。

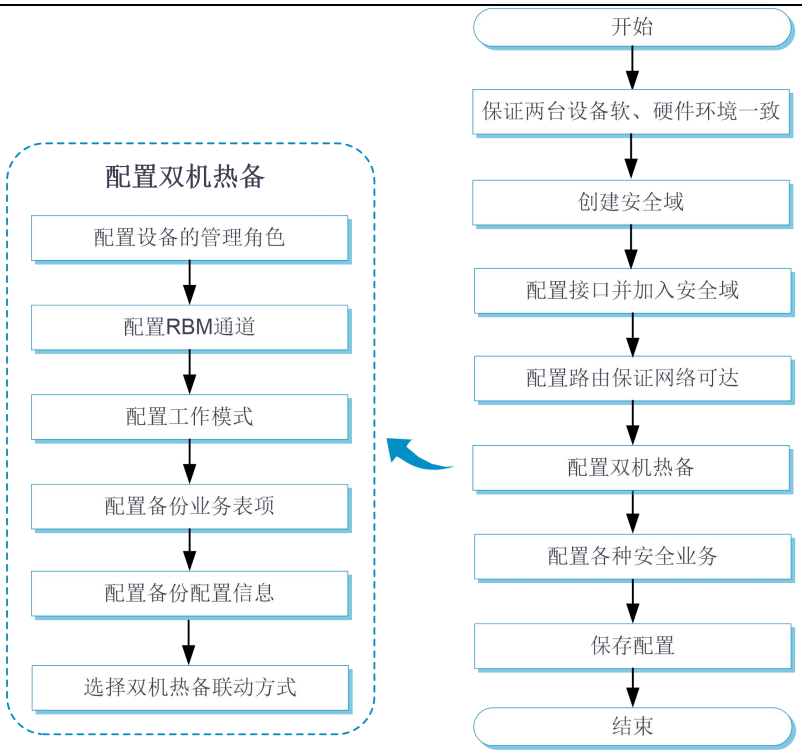
7.1.3.3 双机热备注意事项

- 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。

7.1.4 配置指南

7.1.4.1 配置思路

双机热备功能的配置思路如下图所示：

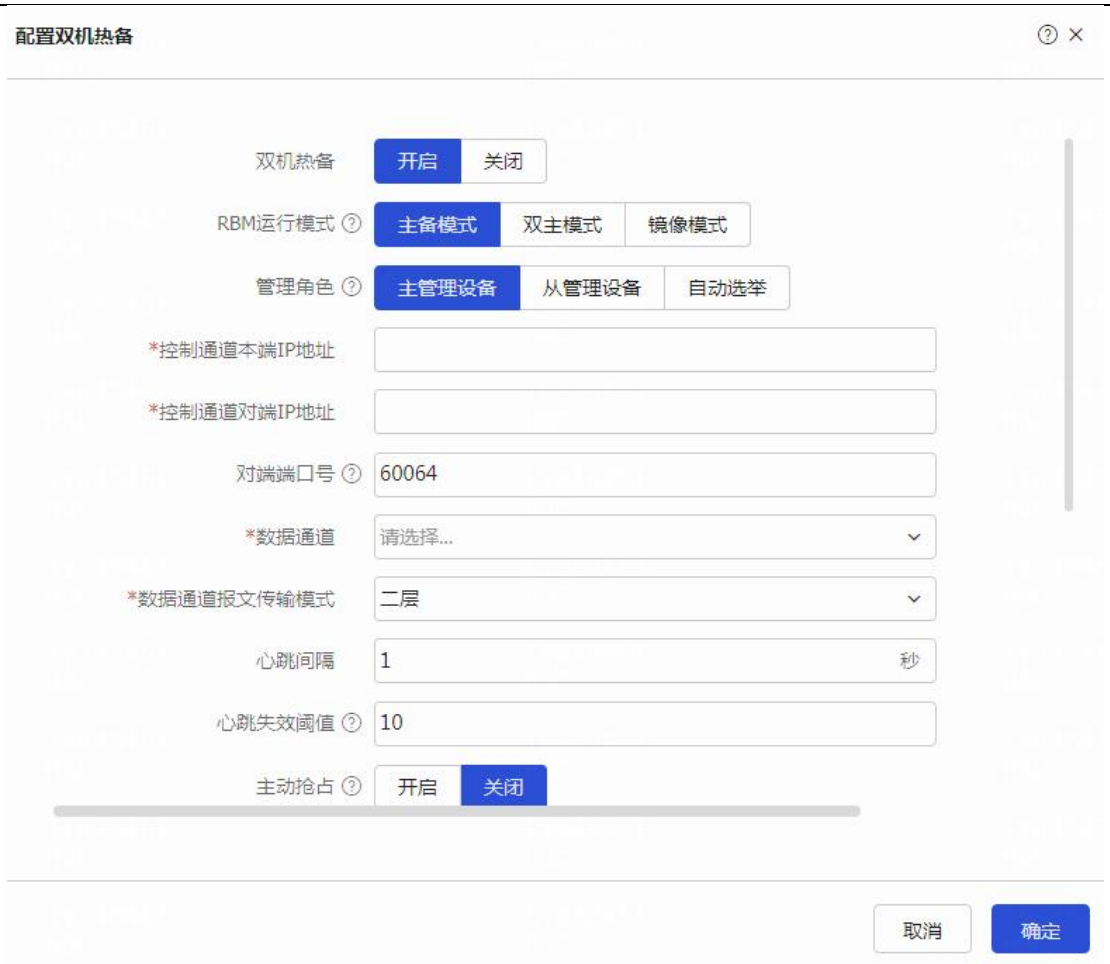


7.1.4.2 配置双机热备

双机热备的具体配置步骤如下：

步骤1 选择“系统 > 高可靠性 > 高可靠性”。

步骤2 在“高可靠性”页面单击<配置>按钮，进入“配置双机热备”页面，配置双机热备，具体配置内容如下表所示：



参数	说明
双机热备开关	高可靠性开关包括两种状态：开启和关闭
RBM 运行模式	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，实时待命 ● 双主模式：两台设备同时处理业务，充分利用设备资源，提高系统负载能力，此模式通过“互为主备”方法实现
角色模式	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：此方式需要通过命令手工指定设备的管理角色，一旦指定后设备的管理角色将固定不变。如需更改，则通过执行命令手工更改。此方式适用于设备上有独立管理接口的网络环境，此方式在双机热备的主备和双主运行模式下均可使用 ● 自动选择：此方式下设备的管理角色根据运行角色自动选择，并跟随运行角色一同切换。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，运行备是从管理设备。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，此方式仅支持在双机热备的主备运行模式下使用，双主运行模式中不能使用。在此方式下管理员可在“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角色为主管

参数	说明
	理设备还是从管理设备
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的同步。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信息。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，当角色模式为自动选择时，两台设备的角色模式都应设置为自动选择
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 监听服务。支持 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
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，但不能同时配置 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一致
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，此数据通道仅用于传输设备之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
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发送双机热备 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值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
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。开启此功能后，当原来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。为了保证业务能够平滑切换，所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，当主设备发生故障时备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项实时备份到备设备 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，只要双机热备热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，以保证同一条流量的正反向报文在两台设备上能够被正常处理

参数	说明
	● 在双机热备主备模式或对称路径的双机热备网络环境中，关闭此功能后，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响。因此，请管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HTTP类型的应用协议，通常在很少的报文交互之后就会断开连接，当发生主备切换造成当前连接中断时，客户端会立即重新发起请求，用户通常感知不到连接异常。所以可以关闭这两个协议触发创建会话的备份功能
备份 AFT 端口块表项	开启此功能后，主设备会将其生成的 AFT 端口块表项实时同步到备设备，当主设备发生故障时备设备可以平滑地接替主设备的工作，保证业务不中断
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，当该接口接收到正向流量的第一个 IP 报文，会保存上一跳信息，同时将该上一跳信息备份到从设备，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信息指导报文进行转发。此功能不同设备的支持情况不同，请以设备 Web 页面的实际支持情况为准
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，用于防止发生两台设备配置信息不一致，导致主备切换后业务不通的情况。当配置信息不一致时，会发送日志信息，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批量备份，之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，批量备备份时间会很长可能需要一到两个小时。因此在初始规划网络配置时，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+虚拟 IP 地址引流的组网场景中使用，其他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置信息时，会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以进行自动同步，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静态路由同步到从管理设备。

步骤3　在“配置双机热备”页面中配置双机热备联动Track项，具体配置内容如下表所示：

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 状态时，双机热备将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，保证业务不中断

步骤4　在“配置双机热备”页面，单击<确定>按钮完成双机热备的配置。

步骤5　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。

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触发配置信息一致性检查。若配置信息不一致，则系统会发送日志信息，以提示管理员进行配置信息的手动同步
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

步骤6　在“双机热备”页面，可以手工进行主备业务状态切换。管理员可通过本命令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的双机热备组网中，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。

参数	说明
状态切换	在主备组网中，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本功能使其成为备设备，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本功能使其保持不变仍为主设备，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选举

7.1.4.3 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联机帮助”。

7.1.4.4 配置双机热备联动虚拟地址

双机热备联动虚拟地址的具体配置步骤如下：

步骤1 选择“网络 > 接口 > 接口”，进入“接口配置”页面。

步骤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。

步骤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。

7.1.4.5 配置双机热备联动路由

双机热备联动路由的具体配置步骤如下：

步骤1 选择“系统 > 高可靠性 > 双机热备”。

步骤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，具体配置内容如下表所示：

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，即设备直接对外通告此绝对值
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，即设备在原有开销值上增加此增量值后对外通告

步骤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。

7.1.4.6 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：

步骤1 选择“系统 > 高可靠性 > 双机热备”。

步骤2　在“双机热备”页面单击<配置>按钮，进入“配置双机热备”页面，配置双机热备透明组网的相关配置，具体配置内容如下表所示：

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，这些接口将同时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，这些接口才能转发报文。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，并将成员端口的状态相互联动并保持一致，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。只有 VLAN 所有成员端口状态均为 UP 时，此 VLAN 的成员端口才能转发报文。否则，此 VLAN 的所有成员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。因为设备上所有 Access 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 Down，这时也会导致 VLAN 1 中正常使用的端口无法转发报文

步骤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。

7.2　VRRP

本帮助主要介绍以下内容：

7.2.1 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。

7.2.1.1 VRRP备份组

VRRP将局域网内的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。

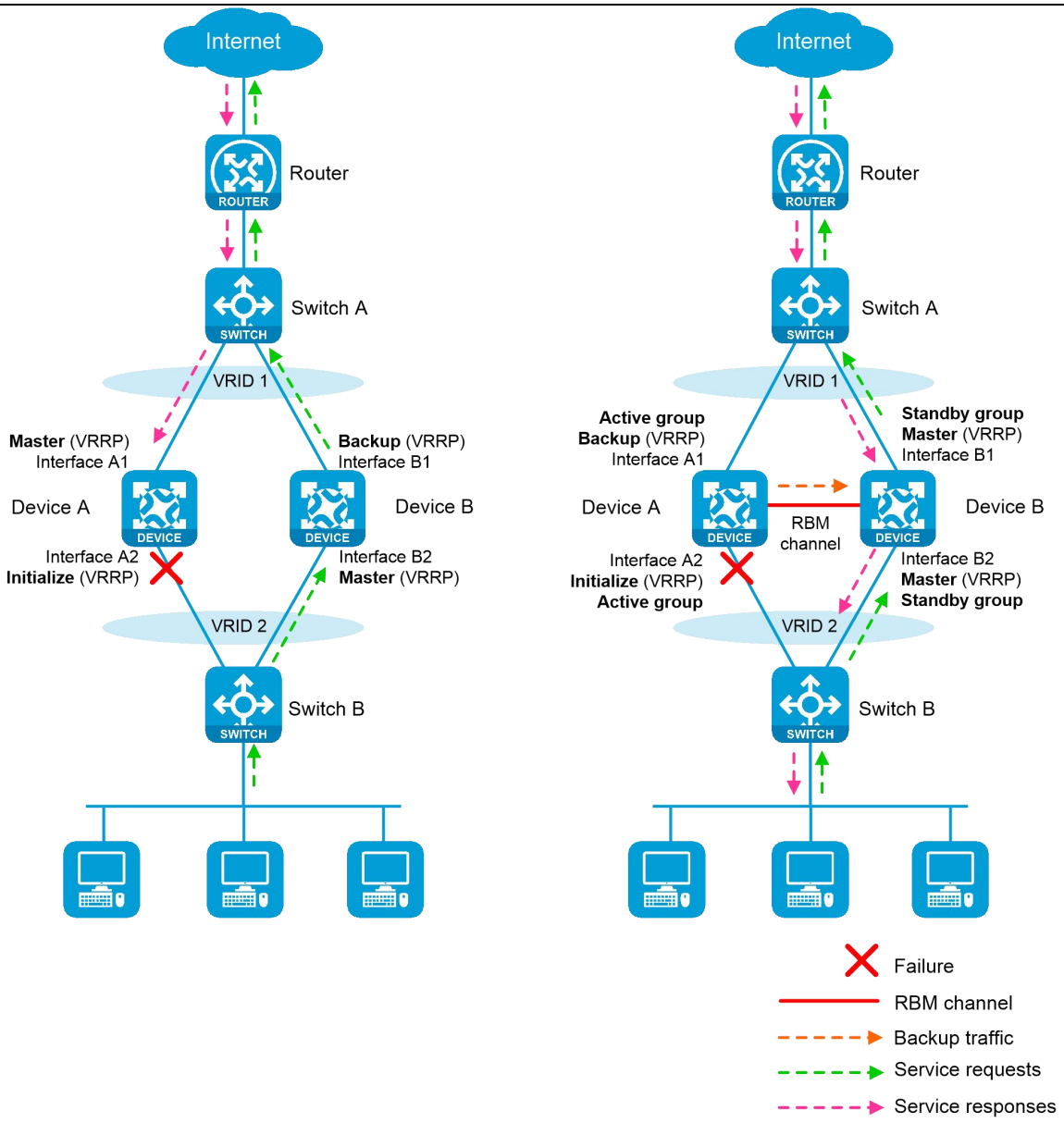
7.2.1.2 联动双机热备

7.2.1.2.1 简介

如下图的左图所示，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。

如下图的右图所示，将双机热备术和VRRP技术关联，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。



7.2.1.2.2 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。

7.2.1.2.3 VRRP在双机热备环境中Master设备的选举机制

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：

步骤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。

步骤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。

步骤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。

步骤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。

7.2.1.3 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。

7.2.1.4 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。

7.2.1.5 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。

7.2.1.6 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。

7.2.1.7 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。

7.2.1.8 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。

7.2.1.9 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。

7.2.2 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。

7.2.3 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。

7.2.4 配置指南

7.2.4.1 VRRP基本配置

VRRP基本配置的具体配置步骤如下：

步骤1 选择“系统 > 高可靠性 > VRRP”。

步骤2 在“VRRP”页面单击<新建>按钮，进入“新建VRRP备份组”页面。

步骤3 新建VRRP备份组，具体配置内容如下表所示：

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一个 VRRP 备份组
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 VRRP 备份组之间进行联动
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，才会抢占为 Master 设备。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，通知备份组内的路由器自己工作正常。使用 VRRPv2 版本时，该参数的实际生效值只能是 100 的整倍数，例如，配置该参数取值在 10～100、101～200、4001～4095 范围内时，实际生效值分别为 100、200、4100；使用 VRRPv3 版本时，该参数的实际生效值与所配置数值相同

步骤4 单击<确定>按钮，新建VRRP备份组成功，且会在“VRRP”页面中显示。

7.2.4.2 VRRP高级配置

VRRP高级配置的具体配置步骤如下：

步骤1 选择“系统 > 高可靠性 > VRRP高级设置”。

步骤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。

步骤3　在“VRRP高级设置”页面进行配置，具体配置内容如下表所示：

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，VRRPv3 版本支持 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

步骤4　单击<应用>按钮，接口的VRRP高级设置配置成功。

7.3　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

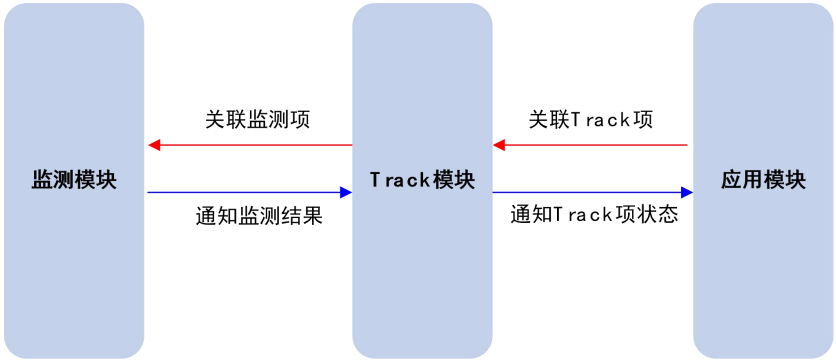
7.3.1　特性简介

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。

7.3.1.1　联动功能实现机制

如下图所示，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。



7.3.1.2 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。

7.3.1.3 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。

7.3.2 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。

7.3.3 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。

7.3.4 配置指南

步骤1 选择“系统 > 高可靠性 > Track”。

步骤2 在“Track”页面单击<新建>按钮，进入“新建Track项”页面。

步骤3 在“新建Track项”页面配置Track项，具体配置内容如下表所示：

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 ● Track项与NQA联动 ● Track项与接口联动 ● Track项与路由联动 ● Track项与与类型的对象列表联动 ● Track项与或类型的对象列表联动 ● Track项与比例类型的对象列表联动 ● Track项与权重类型的对象列表联动
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，则可能会由于路由无法及时恢复等原因，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，延迟一定的时间通知应用模块。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，则可能会由于路由无法及时恢复等原因，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，延迟一定的时间通知应用模块。当 Track 项没有与应用模块联动时，此配置不生效

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 会话建立关联

参数	说明
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

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

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 IPv6 协议状态

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

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 项的状态为 Positive；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 Negative
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 项状态的判断 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 项状态的判断

参数	说明
对象列表类型	需要将对象列表类型设置为“或”

参数	说明
	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 Track 项的状态为 Positive，如果所有的监测对象的状态都是 Negative，那么此 Track 项的状态为 Negative
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 项状态的判断 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 项状态的判断

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，Track 项状态变为 Positive；小于或等于 Negative 状态门限值时，Track 项状态变为 Negative。当关联列表中的 Positive 对象比例小于 Positive 状态门限值且大于 Negative 状态门限值时，Track 项状态保持不变
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

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 状态的监测项的权重之和大于或等于 Positive 门限值时,Track 项状态变为 Positive；当处于 Positive 状态的监测项的权重之和小于或等于 Negative 门限值时，Track 项状态变为 Negative。当关联列表中的 Positive 对象权重小于 Positive 参数指定值且大于 Negative 参数指定值时，Track 项状态保持不变
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

参数	说明
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

7.4 BFD

本帮助主要介绍以下内容：

7.4.1 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。

7.4.2 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。

7.4.3 配置指南

步骤1 选择“系统 > 高可靠性 > BFD”。

步骤2 在“BFD”页面配置相关内容，具体配置内容如下表所示：

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。为了避免对端发送大量的 ICMP 重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一个接口所在网段
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 ICMPv6 重定向报文造成网络拥塞，建议不要将 echo 报文的源 IPv6 地址配置为属于该设备任何一个接口所在网段

7.5 NQA

7.5.1 特性简介

7.5.1.1 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。

7.5.1.2 运行机制

如上图所示，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TCP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：

步骤1　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；

步骤2　目的端设备收到探测报文后，回复应答报文；

步骤3　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。

7.5.1.3　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。

7.5.1.4　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。

7.5.2　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。

7.5.3　配置指南

NQA功能的具体配置步骤如下：

步骤1　选择“系统 > 高可靠性 > NQA”。

步骤2　在“NQA”页面单击<新建>按钮，进入“新建NQA”页面。配置相关内容，具体配置内容如下表所示：

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来标识
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
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，此时不会生成统计结果
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。如果到达探测超时时间时，仍然没有收到回应，则发起第二次探测。如此反复，直到完成指定次数的探测
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，系统不会记录该测试组的历史信息，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会被删除
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到达时启动
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进行测试，当持续时间到达后将结束本次NQA测试

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，如果累计数目达到或超过设定的值，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，如果该次数达到或超过设定的值，则该监测对象超出阈值
失败次数	探测失败的次数

参数	说明
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消息 ● 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改变时，还向网络管理系统发送Trap消息。采用本动作时，需要在“系统 > 维护 > SNMP“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

7.6 日志设置基本配置

本帮助主要介绍以下内容：

7.6.1 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：系统日志、流日志、快速日志。

7.6.1.1 系统日志

系统日志传输格式为ASCII码，其通过设备的信息中心进行统一收集、管理和输出。设备发送系统日志信息的方向包括：控制台（console）、监视终端（monitor）、日志缓冲区（logbuffer）、日志主机（loghost）和日志文件（logfile）。

7.6.1.2 流日志

7.6.1.2.1 流日志简介

设备根据报文的5元组（源IP地址、目的IP地址、源端口、目的端口、协议号）对用户访问网络的流进行分类统计，并生成流日志。流日志目前主要用来记录用户访问网络所产生的NAT会话相关信息，包括5元组信息和发送、接收的字节数等。管理员利用这些信息可以实时跟踪、记录、分析用户访问网络的情况。

7.6.1.2.2 流日志版本

流日志根据日志信息所包含字段多少分为1.0、3.0和5.0三个版本。三种流日志的内容稍有不同。

下表中介绍的字段是设备向日志主机方向发送的原始信息所包含的字段，可能与用户最终看到的信息格式有差异，最终显示格式与用户使用的日志解析工具有关，请以实际情况为准。

字段	描述
SrcIP	NAT 转换前的源 IP 地址
DestIP	NAT 转换前的目的 IP 地址
SrcPort	NAT 转换前的 TCP/UDP 源端口号
DestPort	NAT 转换前的 TCP/UDP 目的端口号
StartTime	流起始时间，以秒为单位，从 1970/1/1 0:0 开始计算
EndTime	流结束时间，以秒为单位，从 1970/1/1 0:0 开始计算 当 Operator 字段取值为 6 时，该字段为 0
Protocol	IP 承载的协议类型
Operator	操作字，记录生成 Flow 日志的原因： ● 0：保留不用 ● 1：正常流结束 ● 2：定时器超时老化 ● 3：清除配置/配置变动引起的流老化 ● 4：资源不足带来的流老化 ● 5：保留不用

字段	描述
	● 6：活跃流定期记录其连接情况 ● 7：新的流创建触发强制删除原有流 ● 8：流创建 ● FE：其他 ● 10~FE-1：以后扩充用
Reserved	保留

字段	描述
Protocol	IP 承载的协议类型
Operator	操作字，记录生成 Flow 日志的原因： ● 0：保留不用 ● 1：正常流结束 ● 2：定时器超时老化 ● 3：清除配置/配置变动引起的流老化 ● 4：资源不足带来的流老化 ● 5：保留不用 ● 6：活跃流定期记录其连接情况 ● 7：新的流创建触发强制删除原有流 ● 8：流创建 ● FE：其他 ● 10~FE-1：以后扩充用
IPVersion	IP 报文版本
TosIPv4	IPv4 报文的 Tos 字段
SourceIP	NAT 转换前的源 IP 地址
SrcNatIP	NAT 转换后的源 IP 地址
DestIP	NAT 转换前的目的 IP 地址
DestNatIP	NAT 转换后的目的 IP 地址
SrcPort	NAT 转换前的 TCP/UDP 源端口号
SrcNatPort	NAT 转换后的 TCP/UDP 源端口号
DestPort	NAT 转换前的 TCP/UDP 目的端口号
DestNatPort	NAT 转换后的 TCP/UDP 目的端口号
StartTime	流起始时间，以秒为单位，从 1970/01/01 00:00 开始计算
EndTime	流结束时间，以秒为单位，从 1970/01/01 00:00 开始计算 当 Operator 字段取值为 6 时，该字段为 0
InTotalPkg	接收的报文包数
InTotalByte	接收的报文字节数
OutTotalPkg	发出的报文包数
OutTotalByte	发出的报文字节数

字段	描述
InVPNID	入 VPN ID
OutVPNID	出 VPN ID
Reserved1	保留字段
AppID	应用协议 ID
Reserved3	保留字段

字段	描述
Protocol	IP 承载的协议类型
Operator	操作字，记录生成 Flow 日志的原因： ● 0：保留不用 ● 1：正常流结束 ● 2：定时器超时老化 ● 3：清除配置/配置变动引起的流老化 ● 4：资源不足带来的流老化 ● 5：保留不用 ● 6：活跃流定期记录其连接情况 ● 7：新的流创建触发强制删除原有流 ● 8：流创建 ● FE：其他 ● 10~FE-1：以后扩充用
IPVersion	IP 报文版本
TosIPv4	IPv4 报文的 Tos 字段
SourceIP	NAT 转换前的源 IP 地址
SrcNatIP	NAT 转换后的源 IP 地址
DestIP	NAT 转换前的目的 IP 地址
DestNatIP	NAT 转换后的目的 IP 地址
SrcPort	NAT 转换前的 TCP/UDP 源端口号
SrcNatPort	NAT 转换后的 TCP/UDP 源端口号
DestPort	NAT 转换前的 TCP/UDP 目的端口号
DestNatPort	NAT 转换后的 TCP/UDP 目的端口号
StartTime	流起始时间，以秒为单位，从 1970/01/01 00:00 开始计算
EndTime	流结束时间，以秒为单位，从 1970/01/01 00:00 开始计算 当 Operator 字段取值为 6 时，该字段为 0
InTotalPkg	接收的报文包数
InTotalByte	接收的报文字节数
OutTotalPkg	发出的报文包数

字段	描述
OutTotalByte	发出的报文字节数
InVPNID	入 VPN ID
OutVPNID	出 VPN ID
AppID	应用协议 ID
UserName	用户名
Reserved1、2、3	保留字段

7.6.1.3 快速日志

快速日志输出功能用于快速地将用户关心的日志发往日志主机。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。

7.6.1.4 存储空间设置

存储空间用于保存各业务的日志数据。

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。

存储空间包括硬盘和内存两种类型。各业务的历史数据优先保存在硬盘中，只有当硬盘不在位时，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，则需要先进行分区和格式化处理。

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。

存储空间设置的支持情况与设备型号有关，请以设备实际情况为准。

7.6.1.4.1 数据保存周期

存储空间中仅保存数据保存周期内的数据，当某类业务的数据保存时间超过设置的数据保存周期时，设备会根据上限处理动作对该业务的数据进行处理。

7.6.1.4.2 存储上限

设备为各业务占用的存储空间提供了设置上限功能。当某类业务所占的存储空间超过其设置的上限时，设备将根据上限处理动作对该业务的数据进行处理。管理员可根据实际业务情况，对各业务的存储上限进行设置。

7.6.1.4.3 上限处理动作

当存储空间中某类业务的历史数据超过数据保存周期，或者达到存储上限时，设备将根据该业务配置的上限处理动作对数据进行处理。

设备支持以下两种上限处理动作：

- 删除：设备将删除保存时间最长的数据以便保存最新的数据，并发送日志信息。删除日志信息时，设备将按天删除，且不可删除当天的日志信息。
- 提示：设备不对历史数据进行删除，也不保存新数据，仅发送日志信息提示用户。管理员可在“监控 > 设备日志 > 系统日志”页面中查看日志信息。

7.6.1.5 日志等级

日志信息按严重性可划分为如下表所示的八个等级，各等级的严重性依照数值从0～7依次降低。在系统输出信息时，所有信息等级高于或等于配置等级的信息都会被输出。例如，输出规则中指定允许等级为6（informational）的信息输出，则等级0～6的信息均会被输出。

数值	信息等级	描述
0	emergency	表示设备不可用的信息，如系统授权已到期
1	alert	表示设备出现重大故障，需要立刻做出反应的信息，如流量超出接口上限
2	critical	表示严重信息，如设备温度已经超过预警值，设备电源、风扇出现故障等
3	error	表示错误信息，如接口链路状态变化，存储卡拔出等
4	warning	表示警告信息，如接口连接断开，内存耗尽告警等
5	notification	表示正常出现但是重要的信息，如通过终端登录设备，设备重启等
6	informational	表示需要记录的通知信息，如通过命令行输入命令的记录信息，执行 **ping** 操作的日志信息等
7	debugging	表示调试过程产生的信息

7.6.1.6 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。

7.6.2 日志输出配置限制和指导

设备支持通过系统日志、流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 > 流日志 > 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。

7.6.3 配置指南

7.6.3.1 系统日志

步骤1 单击“系统 > 日志设置 > 基本配置”，进入“基本配置”页面。

步骤2 在“基本配置”页面，选择“系统日志”页签。

步骤3　配置系统日志的基本信息。

参数	说明
将系统日志输出到日志缓冲区	配置此功能后，设备会将业务模块生成的日志保存到日志缓冲区。其中，设备会为一些业务模块（例如会话、攻击防御等）创建单独的日志缓冲区，用来分别存储这些业务模块的日志，其它业务模块的日志会统一存储到通用日志缓冲区中
日志缓冲区上限	日志缓冲区可存储的信息条数，当存储的日志达到容量限制时，系统会直接使用最新日志覆盖最早生成的日志，此处设置的为通用日志缓冲区的上限
日志发送速率上限	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

步骤4　单击<应用>按钮，完成系统日志的基本信息配置。

步骤5　单击<新建>按钮，配置系统日志主机。

参数	说明

参数	说明
日志主机	支持 IP 地址和主机名
端口号	日志主机接收系统日志信息的端口号
VRF	日志主机所属的 VPN 实例

步骤6　单击<确定>按钮，新建的系统日志主机会在“系统日志”页面显示。

7.6.3.2　流日志

步骤1　单击“系统 > 日志设置 > 基本配置”，进入“基本配置”页面。

步骤2　在“基本配置”页面，选择“流日志”页签。

步骤3　配置流日志的基本信息。

参数	说明
日志版本	选择流日志的版本，包括： ● 1.0 ● 3.0 ● 5.0 请根据日志接收设备的实际能力配置流日志的版本

参数	说明
开启日志负载分担	缺省情况下，每一条流日志会输出给所有已配置的流日志主机 开启此功能后，流日志按照日志信息的源 IP 地址进行逐流负载分担，即源 IP 地址相同的会话对应的流日志始终发送到特定的一台流日志主机。这样可以降低用户日志发送的压力，并减少冗余日志的处理 在开启此功能时请注意，如果配置的流日志主机不可达，流日志仍会进行负载分担，但负载分担到不可达的流日志主机的流日志将被丢弃
日志信息的源 IP 地址	缺省情况下，流日志信息的源 IP 地址为发送该报文的出接口 IP 地址 流日志使用源地址来唯一标识报文的发送者，以便对流日志进行过滤。配置日志信息的源 IP 地址后，当设备向流日志主机发送流日志时，就使用这个唯一 IP 地址作为报文的源 IP 地址 推荐将流日志报文的源 IP 地址配置为设备上 Loopback 接口的地址，以屏蔽某个物理接口状态改变对流日志报文的影响

步骤4　单击<应用>按钮，完成流日志的基本信息配置。

步骤5　单击<新建>按钮，配置流日志主机。

参数	说明
日志主机	支持 IP 地址和主机名
端口号	日志主机接收流日志信息的端口号
VRF	日志主机所属的 VPN 实例

步骤6　单击<确定>按钮，新建的流日志主机会在“流日志”页面显示。

7.6.3.3　快速日志

步骤1　单击“系统 > 日志设置 > 基本配置”，进入“基本配置”页面。

步骤2　在“基本配置”页面，选择“快速日志”页签。

步骤3　配置快速日志的基本信息。

参数	说明
日志信息时间戳	选择快速日志使用的时间戳，包括： ● 格林威治时间（GMT）：即UTC（Coordinated Universal Time,国际协调时间） ● 设备本地时间：格林威治时间加上时区偏移的时间
日志信息的源 IP 地址	缺省情况下，快速日志信息的源 IP 地址为发送该报文的出接口的主 IP 地址 快速日志使用源地址来唯一标识报文的发送者，以便对快速日志进行过滤。配置日志信息的源 IP 地址后，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，请配置此功能 推荐将快速日志报文的源 IP 地址配置为设备上 Loopback 接口的主 IP 地址，以屏蔽某个物理接口状态改变对快速日志报文的影响
日志语言编码格式	选择快速日志使用的编码方式，包括默认格式（GB18030）和 UTF-8 此编码格式需要与日志的接收服务器相同，否则会导致日志服务器的日志出现中文字符乱码的情况。请管理员根据实际情况进行配置
输出中文日志	勾选此配置项后，快速日志将使用中文进行发送 需要注意，目前仅部分日志的部分字段支持本功能。例如，会话日志中仅应用和分类字段支持中文

步骤4　单击<应用>按钮，完成快速日志的基本信息配置。

步骤5　单击<新建>按钮，配置快速日志主机。

参数	说明

参数	说明
日志主机	支持 IP 地址和主机名
端口号	日志主机接收快速日志信息的端口号
VRF	日志主机所属的 VPN 实例
会话日志	允许设备向指定的快速日志主机发送会话日志
AFT 日志	允许设备向指定的快速日志主机发送 AFT 日志，目前仅支持 AFT 端口块日志
应用审计日志	允许设备向指定的快速日志主机发送应用审计日志
URL 过滤日志	允许设备向指定的快速日志主机发送 URL 过滤日志
数据过滤	允许设备向指定的快速日志主机发送数据过滤日志
攻击防范日志	允许设备向指定的快速日志主机发送攻击防范日志
安全策略匹配日志	允许设备向指定的快速日志主机发送包过滤、对象策略和安全策略匹配日志
心跳日志	允许设备向指定的快速日志主机发送心跳日志
入侵防御日志	允许设备向指定的快速日志主机发送入侵防御日志
带宽管理日志	允许设备向指定的快速日志主机发送带宽管理日志
沙箱日志	允许设备向指定的快速日志主机发送沙箱日志
Web 应用防护日志	允许设备向指定的快速日志主机发送 Web 应用防护日志
物联网设备安全管理日志	允许设备向指定的快速日志主机发送物联网设备安全管理日志。物联网设备安全管理日志包括标准格式检查日志、设备准入控制日志、敏感信令控制日志和标准流量管控日志
文件过滤日志	允许设备向指定的快速日志主机发送文件过滤日志
终端识别日志	允许设备向指定的快速日志主机发送终端识别日志
防病毒日志	允许设备向指定的快速日志主机发送防病毒日志
信誉日志	允许设备向指定的快速日志主机发送 IP 信誉、URL 信誉和域名信誉日志
有害信息鉴别日志	允许设备向指定的快速日志主机发送有害信息鉴别日志
安全策略国电配置日志	允许设备向指定的快速日志主机发送国家电网格式安全策略配置日志
服务器外联防护日志	允许设备向指定的快速日志主机发送服务器外联防护日志

步骤6　单击<确定>按钮，新建的快速日志主机会在“快速日志”页面显示。

7.6.3.4 存储空间设置

步骤1 单击“系统 > 日志设置 > 基本配置”，进入“基本配置”页面。

步骤2 在“基本配置”页面，选择“存储空间设置”页签。

业务	数据保存周期（天，1-65535...	存储上限（%）	上限处理动作	已用空间百分比（%）	使能	编辑
系统日志 | 流量日志	365	20	删除	0.1	☐	✎
DPI深度安全 | 威胁业务	365	20	删除	0.1	☑	✎
DPI深度安全 | URL过滤业务	365	20	删除	0.1	☑	✎
系统日志 | 系统日志	365	20	删除	0.0	☑	✎
DPI深度安全 | 文件过滤业务	365	20	删除	0.0	☑	✎

步骤3 进入“存储空间设置”页面，单击指定业务右侧的<编辑>按钮，进入“编辑业务信息”页面，确认修改内容。具体配置内容如下：

参数	说明
业务	支持的各业务
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	当存储空间中某类业务的历史数据超过其数据保存周期，或者达到其存储上限时，设备对该类业务历史数据执行的处理动作 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匹配日志的采集功能，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的采集功能不生效

步骤4 单击<确定>按钮，完成存储空间的配置。

7.7 特性简介

日志管理页面用于配置各业务模块的日志输出功能，支持将日志以系统日志、快速日志或流日志类型输出到日志主机，或开启本地存储可直接展示在Web页面中。

开启了输出系统日志、流日志或快速日志之后，还需在“系统 > 日志设置 > 基本设置”页面下的系

统日志、流日志或快速日志页签配置日志主机。

7.8 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。

7.9 心跳

7.9.1 特性简介

开启心跳日志功能后，日志服务器将会接收此心跳日志。如果定期接收不到，则认为设备处于宕机状态。

开启输出快速日志之后，还需在快速日志页面配置日志主机。

7.9.2 配置指南

步骤1 单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。

步骤2 在“日志管理”页面展开心跳模块，配置心跳日志的基本信息。

步骤3 勾选“输出快速日志”。

步骤4 单击<应用>按钮，完成心跳日志的基本信息配置。

7.10 系统

7.10.1 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，配置存储空间设置，可将勾选的日志数据保存至本机并展示在Web页面中。

7.11 配置

7.11.1 特性简介

配置日志页面用于记录管理员配置设备的过程，配置存储空间设置，可将勾选的日志数据保存至本机并展示在Web页面中。

7.12 IP接入

7.12.1 特性简介

开启IP接入日志功能后，设备将会向日志主机发送通过IP地址认证接入的用户登录及退出产生的日志信息。

7.12.2 配置指南

步骤1 单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。

步骤2 在“日志管理”页面展开IP接入模块，配置IP接入日志的基本信息。

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

步骤3 单击<应用>按钮，完成IP接入日志的基本信息配置。

7.13 MAC接入

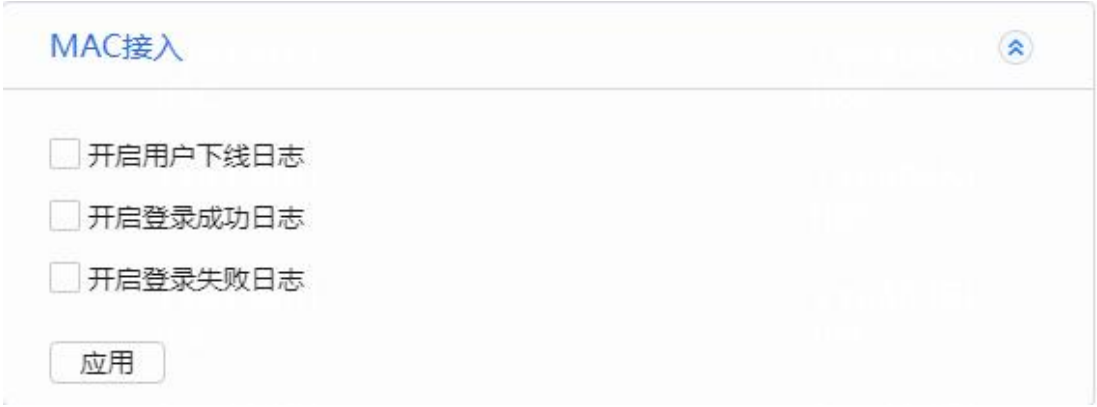
7.13.1 特性简介

开启MAC接入日志功能后，设备将会向日志主机发送通过MAC地址认证接入的用户登录及下线产生的日志信息。

7.13.2 配置指南

步骤1 单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。

步骤2 在“日志管理”页面展开MAC接入模块，配置MAC接入日志的基本信息。



参数	说明
开启用户下线日志	配置此功能后，通过 MAC 地址认证接入的用户下线时会记录会话日志
开启登录成功日志	配置此功能后，通过 MAC 地址认证接入的用户登录成功时会记录会话日志
开启登录失败日志	配置此功能后，通过 MAC 地址认证接入的用户登录失败时会记录会话日志

步骤3 单击<应用>按钮，完成MAC接入日志的基本信息配置。

7.14 Context限速

7.14.1 特性简介

开启Context限速系统日志功能后，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。

7.14.2 配置指南

步骤1 单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。

步骤2 在“日志管理”页面展开Context限速模块，配置Context限速日志的基本信息。

步骤3 选择输出Context限速系统日志，开启Context限速系统日志功能。

步骤4 单击<应用>按钮，完成Context限速系统日志配置。

7.15 SSL VPN用户接入

7.15.1 特性简介

当有SSL VPN用户登入登出设备时，设备会生成相应的SSL VPN用户接入日志。配置存储空间设置，可将勾选的日志数据保存至本机并展示在Web页面中。

7.16 SSL VPN资源访问

7.16.1 特性简介

当SSL VPN用户访问内网资源时，设备会生成相应的SSL VPN资源访问日志。配置存储空间设置，可将勾选的日志数据保存至本机并展示在Web页面中。

7.17 虚拟系统

7.17.1 特性简介

虚拟系统日志功能目前支持对vSystem的入方向吞吐量限制开启吞吐量告警功能和吞吐量限速丢包日志功能。

入方向吞吐量告警功能：开启此功能并设置告警阈值后，当vSystem的入方向吞吐量与入方向吞吐量限制值的比值超过了所设置的告警阈值，设备会生成告警日志；之后，当vSystem的入方向吞吐量与入方向吞吐量限制值的比值恢复到告警阈值以下，设备会生成恢复日志。

入方向吞吐量限速丢包日志功能：开启此功能后，当vSystem的入方向吞吐量达到入方向吞吐量限制值，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vSystem的入方向吞吐量降低到入方向吞吐量限制值以下，设备会生成恢复日志。

目前虚拟系统的日志仅支持以系统日志的方式输出。

7.17.2 配置指南

步骤1 单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。

步骤2 在“日志管理”页面展开虚拟系统模块，配置虚拟系统日志的基本信息。

步骤3 在“虚拟系统日志”页面进行配置。

参数	说明
开启吞吐量丢包日志	开启此功能后，当 vSystem 的入方向吞吐量达到入方向吞吐量限制值，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 vSystem 的入方向吞吐量降低到入方向吞吐量限制值以下，设备会生成恢复日志
开启吞吐量利用率	开启此功能并设置告警阈值后，当 vSystem 的入方向吞吐量与入方向吞吐量限

参数	说明
告警日志	制值的比值超过了所设置的告警阈值，设备会生成告警日志；之后，当 vSystem 的入方向吞吐量与入方向吞吐量限制值的比值恢复到告警阈值以下，设备会生成恢复日志
告警门限	开启开启吞吐量利用率告警日志功能后，需要配置该告警门限

步骤4　单击“应用”按钮，完成配置。

7.18　带宽告警

7.18.1　特性简介

带宽告警功能可对整机入方向的流量进行检测。当入方向流量在持续时间内一直大于或等于带宽告警阈值，则输出带宽告警日志，且之后会每5秒输出一次带宽告警日志；直到入方向流量低于带宽告警阈值后，才停止输出带宽告警日志。带宽告警日志仅支持系统日志。

7.18.2　配置指南

步骤1　单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。

步骤2　在“日志管理”页面展开带宽告警模块，配置带宽告警日志的基本信息。

步骤3　勾选“输出告警”，并配置产生告警的带宽阈值以及到达阈值的持续时间。

步骤4　单击<应用>按钮，完成带宽告警日志的基本信息配置。

7.19　零信任策略

7.19.1　特性简介

开启外部鉴权快速日志输出功能后，设备将把指定内容的日志信息采用快速日志方式发往日志主机。设备支持输出鉴权日志、策略通知日志和零信任策略日志。鉴权日志用来输出可信访问控制器的鉴权结果，策略通知日志用来输出用户下线和用户权限变更等信息，零信任策略日志用来输出匹配零信任策略的用户信息、资产信息以及策略执行动作。

开启输出快速日志之后，还需要在快速日志页面配置日志主机，有关快速日志的配置方法，请参见“日志设置基本配置联机帮助”。

7.19.2　配置指南

步骤1　单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。

步骤2　在“日志管理”页面展开零信任策略模块，配置零信任策略日志的基本信息。

步骤3　在“零信任策略日志”页面进行配置。

参数	说明
输出鉴权快速日志	开启此功能后，设备将输出可信访问控制器的鉴权结果日志
输出策略通知快速日志	开启此功能后，设备将输出用户下线和用户权限变更等信息日志
输出零信任策略快速日志	开启此功能后，设备将输出匹配零信任策略的用户信息、资产信息以及策略执行动作
策略日志	开启此功能后，设备即可保存日志信息，并可在本机查看

步骤4　单击“应用”按钮，完成配置。

7.20　安全策略国电配置

7.20.1　特性简介

开启输出安全策略国电配置快速日志功能后，设备会在每天指定的时间以国家电网日志的格式发送此时所有处于生效状态安全策略的配置内容日志到快速日志主机。

开启输出快速日志之后，还需在快速日志页面配置日志主机。

7.20.2　配置指南

步骤1　单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。

步骤2　在“日志管理”页面展开安全策略国电配置模块，配置安全策略国电配置日志的基本信息。

步骤3　勾选“输出快速日志”，并配置每天发送日志的时间。

步骤4　单击<应用>按钮，完成安全策略国电配置日志的基本信息配置。

7.21　会话

7.21.1　特性简介

会话日志是为满足网络管理员安全审计的需要，对用户的访问信息、用户的IP地址信息、用户的网络流量信息等进行记录，并可采用流日志或快速日志的方式输出。存活时间或收发数目达到一定阈值的会话才会以日志的形式进行记录并输出，该阈值包括流量阈值和时间阈值两种。

同时配置了时间阈值和流量阈值的情况下，只要有一个阈值到达，就会输出相应的会话日志，并将所有的阈值统计信息清零。

必须在接口上开启会话日志功能，才能生成会话日志。

7.21.2 配置指南

步骤1 单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。

步骤2 在“日志管理”页面展开会话模块，配置会话日志的基本信息。

步骤3 选择会话日志输出的类型，包括流日志和快速日志两种，缺省为流日志。

步骤4 单击<添加接口>按钮，在指定接口上开启会话日志功能。

参数	说明
IP 类型	表示在接口上对哪类报文开启会话日志功能，其包括 IPv4 和 IPv6 两种类型
接口	在指定接口上开启会话日志功能，且可根据接口的入方向和出方向流量分别会输出会话日志
ACL	表示与指定 ACL 相匹配的流量才会触发输出会话日志，如果不指定 ACL，则表示经过接口的所有流量均会触发输出会话日志

步骤5 单击<确定>按钮，开启会话日志功能的接口会在生成日志的接口列表中显示。

参数	说明
记录新建会话的日志	配置此功能后，新建会话时会记录会话日志
记录删除会话的日志	配置此功能后，删除会话时会记录会话日志
流量阈值	流量阈值分为报文数阈值和字节数阈值两种，二者只能选其一。当一个会话收发的报文数或字节数达到设定的流量阈值时，输出会话日志
时间阈值	如果设置的时间阈值为 n，则每经过 n 分钟，设备就输出一次相应的会话日志

步骤6 单击<应用>按钮，完成会话日志的基本信息配置。

7.22 流量

7.22.1 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。

开启会话统计功能后可配置存储空间设置，可将勾选的日志数据保存至本机并展示在Web页面中。

7.23 安全策略匹配

7.23.1 特性简介

安全策略匹配日志用于记录报文与包过滤、对象策略和安全策略匹配成功的日志信息。

产生安全策略匹配日志需要先在安全策略中开启记录日志功能后，报文与安全策略成功匹配后才会输出安全策略日志。

安全策略匹配支持输出系统日志或快速日志，开启输出系统日志、快速日志之后，还需在系统日志、快速日志页面配置日志主机。

7.23.2 配置指南

步骤1 单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。

步骤2 在“日志管理”页面展开安全策略匹配模块，配置安全策略匹配日志的基本信息。

步骤3 选择输出安全策略匹配日志的类型。

步骤4 单击<应用>按钮，完成安全策略匹配日志的基本信息配置。

7.24 威胁

7.24.1 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。

威胁日志支持以系统日志或者快速日志的方式发送到指定的日志主机。

7.24.2 License支持情况

7.24.2.1 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”。

7.24.2.2 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、增强检测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”。

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无法使用。关于License的详细介绍请参见“License配置联机帮助”。

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”。

7.24.3 配置指南

7.24.3.1 配置准备

配置本模块功能前，还需要完成如下配置：

- 开启入侵防御功能和防病毒功能的记录日志功能。
- 如果选择使用系统日志方式发送日志，需要配置系统日志的日志主机。
- 如果选择使用快速日志方式发送日志，需要配置快速日志的日志主机，并在日志主机中勾选发送威胁日志。
- 如果选择使用邮件方式发送日志，需要配置邮件服务器。其中，Web界面仅支持使用系统默认支持的名称为“mailsetting_default_parameter”的邮件服务器发送日志，管理员需要编辑该服务器，配置相应的参数。

有关入侵防御功能和防病毒功能的记录日志功能的详细介绍，请参见“入侵防御联机帮助”和“防病毒联机帮助”；有关系统日志和快速日志日志主机的详细介绍，请参见“日志设置基本配置联机帮助”；有关邮件服务器的详细介绍，请参见“邮件服务器联机帮助”。

7.24.3.2 配置步骤

步骤1 单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。

步骤2 在安全类日志列表下，展开威胁模块，分别配置入侵防御日志和防病毒日志参数。

参数	说明
系统日志	选择此方式后，入侵防御日志将以系统日志方式发送到日志主机 此方式输出日志可能会对设备性能产生影响，不建议使用
快速日志	选择此方式后，入侵防御日志以快速日志方式发送到日志主机 快速日志支持标准格式和非标准格式 ● 标准格式：系统默认的日志格式 ● 国家电网：国家电网定制的日志格式，仅在国家电网场景中需要选择此格式。此格式的支持情况与设备型号有关，请以设备实际情况为准。 ● 其中，选择国家电网格式后，还需要选择一种或多种输出的日志内容，

参数	说明
	取值包括： ● 告警日志：选择此日志后，当报文匹配到入侵防御配置文件后，设备会生成日志信息并向外发送 ● 特征库更新日志：选择此日志后，当入侵防御特征库升级或者回滚时，设备将记录特征库变更的时间，并在每日按照配置的发送时间向外发送日志
输出邮件	勾选此功能后，系统将使用邮件发送入侵防御日志到指定的收件人地址
输出中文日志	勾选此功能后，日志主机收到的日志中，仅攻击名称、攻击分类、攻击子分类、源地区、目的地区和应用支持显示为中文

参数	说明
系统日志	选择此方式后，防病毒日志将以系统日志方式发送到日志主机 此方式输出日志可能会对设备性能产生影响，不建议使用
快速日志	选择此方式后，防病毒日志以快速日志方式发送到日志主机
输出邮件	勾选此功能后，系统将使用邮件发送防病毒日志到指定的收件人地址

步骤3　单击<应用>按钮，完成配置。

7.25　沙箱

7.25.1　特性简介

沙箱日志用于记录APT防御功能中沙箱检测的结果，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。

沙箱日志支持以快速日志的方式发送到指定的日志主机。

7.25.2　配置指南

7.25.2.1　配置准备

如果选择输出快速日志，则需要配置快速日志的日志主机，并在日志主机中勾选发送沙箱日志。有关快速日志日志主机的详细介绍，请参见“日志设置基本配置联机帮助”。

7.25.2.2　配置步骤

步骤1　单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。

步骤2　在安全类日志列表下，展开沙箱模块，配置如下参数。

参数	说明
输出快速日志	勾选此功能后，沙箱日志将以快速日志方式发送到日志主机

步骤3　单击<应用>按钮，完成配置。

7.26　应用审计

7.26.1　特性简介

应用审计日志可以对用户的上网行为进行记录并发送到指定的日志主机。应用审计日志支持系统日志和快速日志，缺省为系统日志。

7.26.2　License支持情况

应用审计功能需要基于APR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”。

7.26.3　配置指南

7.26.3.1　配置准备

配置本功能前，还需要完成如下配置：

- 开启应用审计策略的记录日志功能。
- 如果选择使用系统日志方式发送日志，需要配置系统日志的日志主机。
- 如果选择使用快速日志方式发送日志，需要配置快速日志的日志主机，并在日志主机中勾选发送应用审计日志。

有关应用审计的记录日志功能的详细介绍，请参见“应用审计联机帮助”。

7.26.3.2　配置步骤

应用审计日志的具体配置步骤如下：

步骤1　单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。

步骤2　在“日志管理”页面展开应用审计模块，配置应用审计日志的基本信息。

步骤3　选择应用审计日志输出的类型，包括系统日志和快速日志两种，缺省为系统日志。

步骤4　单击<应用>按钮，完成应用审计日志的配置。

7.27　URL过滤

7.27.1 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过滤日志支持以系统日志或者快速日志的方式发送到指定的日志主机。

7.27.2 License支持情况

URL过滤功能需要购买并正确安装License才能使用。License过期后，URL过滤功能可以使用设备中已存在的特征库正常工作，但无法升级特征库且云端查询功能无法使用。关于License的详细介绍请参见“License联机帮助”。

7.27.3 配置指南

7.27.3.1 配置准备

配置本模块功能前，还需要完成如下配置：

- 开启URL过滤的记录日志功能。
- 如果选择使用系统日志方式发送日志，需要配置系统日志的日志主机。
- 如果选择使用快速日志方式发送日志，需要配置快速日志的日志主机，并在日志主机中勾选发送URL过滤日志。

有关URL过滤的记录日志功能的详细介绍，请参见“URL过滤联机帮助”；有关系统日志和快速日志的日志主机的详细介绍，请参见“日志设置基本配置联机帮助”。

7.27.3.2 配置步骤

步骤1 单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。

步骤2 在安全类日志列表下，展开URL过滤模块，配置如下参数。其中，系统日志和快速日志仅支持选择其中一种方式进行配置。

参数	说明
系统日志	选择此方式后，URL 过滤日志将以系统日志方式发送到日志主机 此方式输出日志可能会对设备性能产生影响，不建议使用
快速日志	选择此方式后，URL 过滤日志以快速日志方式发送到日志主机 快速日志支持标准格式和非标准格式 ● 标准格式：系统默认的日志格式 ● 非标准格式：运营商定制的日志格式，当前仅支持中国联通 ● 如需输出运营商格式的日志，可以勾选“输出非标准格式”

步骤3　单击<应用>按钮，完成配置。

7.28　数据过滤

7.28.1　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。

数据过滤日志支持以系统日志或者快速日志的方式发送到指定的日志主机。

7.28.2　配置指南

7.28.2.1　配置准备

配置本模块功能前，还需要完成如下配置：

- 开启数据过滤的记录日志功能。
- 如果选择使用系统日志方式发送日志，需要配置系统日志的日志主机。
- 如果选择使用快速日志方式发送日志，需要配置快速日志的日志主机，并在日志主机中勾选发送数据过滤日志。

有关数据过滤的记录日志功能的详细介绍，请参见“数据过滤联机帮助”；有关系统日志和快速日志的日志主机的详细介绍，请参见“日志设置基本配置联机帮助”。

7.28.2.2　配置步骤

步骤1　单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。

步骤2　在安全类日志列表下，展开数据过滤模块，配置如下参数。其中，系统日志和快速日志仅支持选择其中一种方式进行配置。

参数	说明
系统日志	选择此方式后，数据过滤日志将以系统日志方式发送到日志主机 此方式输出日志可能会对设备性能产生影响，不建议使用
快速日志	选择此方式后，数据过滤日志以快速日志方式发送到日志主机

步骤3　单击<应用>按钮，完成配置。

7.29 文件过滤

7.29.1 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。

文件过滤日志支持以系统日志或者快速日志的方式发送到指定的日志主机。

7.29.2 配置指南

7.29.2.1 配置准备

配置本模块功能前，还需要完成如下配置：

- 开启文件过滤的记录日志功能。
- 如果选择使用系统日志方式发送日志，需要配置系统日志的日志主机。
- 如果选择使用快速日志方式发送日志，需要配置快速日志的日志主机，并在日志主机中勾选发送文件过滤日志。

有关文件过滤的记录日志功能的详细介绍，请参见“文件过滤联机帮助”；有关系统日志和快速日志的日志主机的详细介绍，请参见“日志设置基本配置联机帮助”。

7.29.2.2 配置步骤

步骤1 单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。

步骤2 在安全类日志列表下，展开文件过滤模块，配置如下参数。其中，系统日志和快速日志仅支持选择其中一种方式进行配置。

参数	说明
系统日志	选择此方式后，文件过滤日志将以系统日志方式发送到日志主机 此方式输出日志可能会对设备性能产生影响，不建议使用
快速日志	选择此方式后，文件过滤日志以快速日志方式发送到日志主机

步骤3 单击<应用>按钮，完成配置。

7.30 Web应用防护

7.30.1 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应用防护日志同时支持使用如下多种方式对外发送：

- 以快速日志方式发送到指定的日志主机。
- 以邮件的方式发送给指定的收件人。

7.30.2 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”。

7.30.3 配置指南

7.30.3.1 配置准备

配置本模块功能前，还需要完成如下配置：

- 开启Web应用防护的记录日志功能。
- 如果使用快速日志方式发送日志时，需要配置快速日志的日志主机，并在日志主机中勾选发送Web应用防护日志。
- 如果使用邮件方式发送日志时，需要配置邮件服务器。其中，Web界面仅支持使用系统默认支持的名称为“mailsetting_default_parameter”的邮件服务器发送日志，管理员需要编辑该服务器，配置相应的参数。

有关Web应用防护的记录日志功能的详细介绍，请参见“Web应用防护联机帮助”；有关快速日志日志主机的详细介绍，请参见“日志设置基本配置联机帮助”。有关邮件服务器的详细介绍，请参见“邮件服务器联机帮助”。

7.30.3.2 配置步骤

步骤1　单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。

步骤2　在安全类日志列表下，展开Web应用防护模块，配置如下参数。

参数	说明
输出 Web 应用防护快速日志	勾选此方式后，Web 应用防护日志将以快速日志方式发送到日志主机 其中，Web 应用防护日志支持输出中文日志，勾选“输出中文日志”后，日志主机收到的日志中，仅特征名称、攻击分类、攻击分类子类、源地区和目的地区支持显示为中文

参数	说明
输出邮件	勾选此方式后，Web 应用防护日志将以邮件的方式发送到指定的收件人地址

步骤3　单击<应用>按钮，完成配置。

7.31　带宽管理

7.31.1　特性简介

带宽管理支持对匹配上带宽管理策略的报文记录日志，并以快速日志的方式输出带宽管理日志到日志主机。

7.31.2　配置指南

7.31.2.1　配置准备

如果选择使用快速日志方式发送日志，需要配置快速日志的日志主机，并在日志主机中勾选发送带宽管理日志。

7.31.2.2　配置步骤

带宽管理日志的具体配置步骤如下：

步骤1　单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。

步骤2　在“日志管理”页面展开带宽管理模块，配置带宽管理日志的基本信息。

步骤3　选择带宽管理日志输出的类型，当前仅支持快速日志。

步骤4　单击<应用>按钮，完成带宽管理日志的基本信息配置。

7.32　异常流量

7.32.1　特性简介

异常流量日志用于记录终端流量发生异常的日志信息，配置存储空间设置，可将勾选的日志数据保存至本机并展示在Web页面中。

7.33　DGA域名检测

7.33.1 特性简介

DGA域名检测日志用来记录DGA域名检测功能产生的日志信息，方便管理员根据检测结果调整相应的策略，防止用户遭到恶意网站的攻击。

7.33.2 配置指南

7.33.2.1 配置准备

配置本模块功能前，还需要完成如下配置：

- 开启DGA域名检测功能的记录日志功能。
- 如果选择输出快速日志，则需要配置快速日志的日志主机，并在日志主机中勾选发送DGA域名检测日志。

有关DGA域名检测功能的记录日志功能的详细介绍，请参见“威胁情报联机帮助”；有关快速日志日志主机的详细介绍，请参见“日志设置基本配置联机帮助”。

7.33.2.2 配置步骤

步骤1 单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。

步骤2 在安全类日志列表下，展开DGA域名检测模块，配置如下参数。

参数	说明
输出快速日志	勾选此功能后，DGA 域名检测日志将以快速日志的方式发送到日志主机

步骤3 单击<应用>按钮，完成配置。

7.34 终端识别

7.34.1 特性简介

终端识别日志用户在终端信息发生变更时（比如将原厂商的摄像头换为其他厂商的摄像头）向用户发送日志，提示用户。

终端识别日志仅支持以快速日志输出的方式发送到日志主机，开启输出快速日志之后，还需在快速日志页面配置日志主机。

7.34.2 配置指南

步骤1 单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。

步骤2　在“日志管理”页面展开终端识别模块，配置终端识别日志的基本信息。

步骤3　勾选“输出快速日志”。

步骤4　单击<应用>按钮，完成终端识别日志的基本信息配置。

7.35　信誉

7.35.1　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。

信誉日志支持以快速日志的方式输出到日志主机。

7.35.2　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”。

7.35.3　配置指南

7.35.3.1　配置准备

配置本模块功能前，还需要完成如下配置：

- 开启各信誉功能的日志记录功能。
- 如果选择输出快速日志，则需要配置快速日志的日志主机，并在日志主机中勾选发送信誉日志。

有关各信誉功能的日志记录的详细介绍，请参见“威胁情报联机帮助”；有关快速日志日志主机的详细介绍，请参见“日志设置基本配置联机帮助”。

7.35.3.2　配置步骤

步骤1　单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。

步骤2　在安全类日志列表下，展开信誉模块。

步骤3　勾选输出快速日志，信誉日志将以快速日志方式输出到指定的日志主机中。

步骤4　单击<应用>按钮，完成配置。

7.36　Web防篡改

7.36.1　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。配置存储空间设置，可将勾选的日志数据保存至本机并展示在Web页面中。

7.37 DLP

7.37.1 特性简介

DLP日志用于记录匹配DLP策略的数据泄露事件产生的日志信息，方便管理员根据数据泄露情况调整相应的防范策略，降低机密信息泄露和病毒文件进入公司内部网络的风险。

配置存储空间设置，可将勾选的日志数据保存至本机并展示在Web页面中。

7.38 攻击防范

7.38.1 特性简介

7.38.1.1 黑名单日志

开启黑名单日志功能后，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。

7.38.1.2 单包攻击防范日志聚合输出

在单包攻击防范中，可以开启日志功能，使设备在检测到攻击发生时生成告警日志。但在单包攻击较为频繁的情况下，大量的日志生成与输出会占用较高的系统资源，此时可以通过开启“单包攻击防范日志聚合输出”功能，将在一定时间内，在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，以降低对系统资源的占用。

7.38.2 配置指南

步骤1 单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。

步骤2 在“日志管理”页面展开攻击检测模块，配置攻击防范日志的基本信息。

步骤3 选择会话日志输出的类型，包括系统日志和快速日志两种，缺省为系统日志。

步骤4 在“攻击防范日志”页面的具体配置内容如下表所示：

参数	说明
开启黑名单日志	开启黑名单日志功能后，当增加黑名单、删除黑名单、扫描攻击防范动态添加黑名

参数	说明
功能	单、黑名单老化被删除时会有相应的日志输出
单包攻击防范日志聚合输出	单包攻击频繁的情况下，会输出大量的日志信息，开启此功能，可将相同类型的单包攻击日志聚合成一条输出，减少资源占用，一般情况下建议开启

步骤5　单击<应用>按钮，使指定日志的配置生效。

7.39　有害信息鉴别

7.39.1　特性简介

开启输出快速日志功能后，设备将把有害信息鉴别日志信息采用快速日志方式发往日志主机。请在“系统 > 日志设置 > 基本配置 > 快速日志”界面中进行日志主机相关配置。

7.39.2　配置指南

7.39.2.1　配置准备

配置本功能前，还需要在有害信息鉴别日志页面开启有害信息鉴别的日志接收开关。

7.39.2.2　配置步骤

有害信息鉴别日志的具体配置步骤如下：

步骤1　单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。

步骤2　在“日志管理”页面展开有害信息鉴别模块，配置有害信息鉴别日志的基本信息。

步骤3　选择有害信息鉴别日志输出的类型，当前仅支持快速日志。

步骤4　单击<应用>按钮，完成有害信息鉴别日志的基本信息配置。

7.40　IP限速

7.40.1　特性简介

IP限速支持配置公网防护和内网防护两种类型

- 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。

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，设备将输出日志信息。配置存储空间设

置，可将勾选的日志数据保存至本机并展示在Web页面中。

7.41 服务器外联防护

7.41.1 特性简介

服务器外联防护日志用于记录设备上服务器外联防护业务识别内网服务器外联行为产生的日志信息。产生服务器外联防护日志需要在服务器外联防护策略中开启记录日志告警功能，才会输出服务器外联防护日志。

服务器外联防护仅支持输出快速日志。

7.41.2 配置指南

步骤1 单击“系统 > 日志设置 > 日志管理”，进入“日志管理”页面。

步骤2 在“日志管理”页面展开服务器外联防护模块，配置服务器外联防护日志的基本信息。

步骤3 勾选“输出快速日志”。

步骤4 单击<应用>按钮，完成心跳日志的基本信息配置。

7.42 连接数限制

7.42.1 特性简介

连接数限制日志用于记录设备上的连接数到达限制阈值后产生的日志信息，配置存储空间设置，可将勾选的日志数据保存至本机并展示在Web页面中。

7.43 物联网设备安全管理

7.43.1 特性简介

开启物联网设备安全管理日志输出功能后，设备将把指定内容的日志信息采用快速日志方式发往日志主机。设备支持分别开启标准格式检查快速日志输出功能、设备准入控制快速日志输出功能、敏感信令控制快速日志输出功能和标准流量管控快速日志输出功能。

7.43.2 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”。

7.43.3 配置指南

7.43.3.1 配置准备

如果选择使用快速日志方式发送日志，需要配置快速日志的日志主机，并在日志主机中勾选发送物联网设备安全管理日志。

7.43.3.2 配置步骤

物联网设备安全管理日志的具体配置步骤如下：

步骤1 选择“系统 > 日志设置 > 物联网设备安全管理日志”。

步骤2 开启指定日志输出功能。

参数	说明
开启物联网设备安全管理快速日志输出功能	开启指定物联网设备安全管理业务快速日志输出功能 ● 标准格式检查快速日志输出功能 ● 设备准入控制快速日志输出功能 ● 敏感信令控制快速日志输出功能 ● 标准流量管控快速日志输出功能

步骤3 单击<应用>按钮，完成配置。

7.44 邮件服务器

本帮助主要介绍以下内容：

7.44.1 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。

7.44.2 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。

7.44.3 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。

7.44.4 配置指南

邮件服务器的配置步骤如下：

步骤1　单击“系统 > 日志设置 > 邮件服务器”，进入“邮件服务器”页面。

步骤2　单击<新建>按钮，进入“新建邮件服务器“页面。

步骤3　配置邮件服务器信息。

参数	说明

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，然后再在此通道中传输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发送，设备会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。如果新邮件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、最新缓存的邮件 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送邮件的最大数量
语言类型	邮件使用的语言，取值包括英文和中文

步骤4　单击<确定>按钮，完成邮件服务器信息配置。

步骤5　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。

7.45　报表设置

本帮助主要介绍以下内容：

◆ 特性简介

- 报表订阅
- 安全报表导出

7.45.1 特性简介

7.45.1.1 报表订阅

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。

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、业务主机和用户主机的风险详情以及业务主机和用户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。

7.45.1.2 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、业务主机和用户主机的风险详情以及业务主机和用户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。

7.45.1.3 邮件服务器

当需要使用报表订阅功能时，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动到指定邮箱地址。

7.45.2 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。

7.45.3 使用限制和注意事项

配置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“日志设置基本配置联机帮助”。

- 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。

7.45.4 配置指南

7.45.4.1 报表订阅

报表订阅功能的具体配置步骤如下：

步骤1 选择“系统 > 报表设置 > 报表订阅”，进入报表订阅页面。

步骤2 在需要订阅的报表类型区域，单击<添加>按钮，在输入框中输入报表订阅者的邮箱地址，并选择报表的订阅语言。

步骤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“业务安全概况”和“用户安全概况“中统计的用户主机和业务主机数量。

7.45.4.2　邮件服务器

邮件服务器的具体配置步骤如下：

步骤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。

步骤2　“邮件服务器”页面中，具体配置内容如下：

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，则需要管理员配合邮件服务器端的要求，在设备上同时开启本功能；如果服务器不需要对用户进行身份验证，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

步骤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。

步骤4　单击<应用>按钮，保存配置。

7.46　会话设置

本帮助主要介绍以下内容：

7.46.1 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。

7.46.1.1 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。

7.46.1.2 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。

7.46.1.3 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。

7.46.1.3.1 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。

7.46.1.3.2 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。

7.46.2 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。

7.46.3 配置指南

7.46.3.1 修改协议会话老化时间

步骤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。

步骤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。

7.46.3.2 修改应用会话老化时间

步骤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。

步骤2 单击指定应用的编辑按钮，即可修改老化时间。

7.46.3.3 高级设置

步骤1 单击“系统 > 会话设置 > 高级设置”，进入高级设置页面。

步骤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。

7.47 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
  - 特征库版本回退

7.47.1 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。

7.47.1.1 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。

7.47.1.2 特征库版本回退

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，则可以将其进行回退到出厂版本。

7.47.2 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。

7.47.3 License支持情况

应用识别、入侵防御、防病毒、Web应用防护、URL过滤、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联机帮助”。

7.47.4 使用限制和注意事项

- 执行特征库升级与回滚操作会暂时中断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。
- 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回滚，否则易造成设备特征库升级或回滚失败，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。
- 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。

7.47.5 配置指南

7.47.5.1 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。

7.47.5.1.1 配置步骤

步骤1 选择“系统 >升级中心 > 特征库升级”。

步骤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。

步骤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。

步骤4　单击<确定>，此特征库定时升级时间即可配置成功。

7.47.5.2　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。

7.47.5.2.1　配置步骤

步骤1　选择“系统 >升级中心 > 特征库升级”。

步骤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。

7.47.5.3　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。

7.47.5.3.1　配置步骤

步骤1　选择“系统 >升级中心 > 特征库升级”。

步骤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。

步骤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。

步骤4　单击<确定>，即可完成特征库升级。

7.47.5.4　配置特征库服务器

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。本功能用于配置特征库服务器参数。

7.47.5.4.1　配置步骤

步骤1　选择“系统 >升级中心 > 特征库升级”。

步骤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。

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。包括如下取值： ● 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。选择此方式后，需要在“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，需要选择IP地址的类型，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，则必须通过本参数指定服务器所属的 VRF，否则会导致特征库升级失败

步骤3　单击<确定>，即可完成特征库服务器的配置。

7.47.5.5　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。通过点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：

步骤1　选择“系统 >升级中心 > 特征库升级”。

步骤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。

7.47.5.6　配置代理服务器

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，进行特性库在线升级。

7.47.5.6.1　配置步骤

步骤1　选择“系统 >升级中心 > 特征库升级”。

步骤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。

步骤3　单击<确定>，即可完成代理服务器的配置。

7.47.5.7　版本回退

版本回退的具体配置步骤如下：

步骤1　选择“系统 >升级中心 > 特征库升级”。

步骤2　在“特征库升级”页面，单击目标特征库右边操作中的<版本回退>功能，进入“回滚XXX特征库”页面。

步骤3　在“回滚XXX特征库”页面，选择<回滚到出厂版本>。

步骤4　单击<确定>，即可完成特征库版本回退。

7.48　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
  - 软件版本
  - 管理启动文件

- 立即升级

7.48.1 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。

7.48.1.1 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。

7.48.1.2 启动文件

7.48.1.2.1 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。

7.48.1.2.2 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。

7.48.2 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。

7.48.3 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。

7.48.4 配置指南

7.48.4.1 软件版本

选择“系统 >升级中心 > 软件更新”，进入软件更新页面，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。

7.48.4.2 管理启动文件

设备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。设置下次启动文件后，需要手工重启设备才可完成整个升级过程。

步骤1 选择“系统 >升级中心 > 软件更新”。

步骤2 单击<管理文件>按钮，进入管理启动文件页面，支持的功能如下：

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

参数	说明
	为.ipe 的启动文件，设备将对该文件进行解压，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。设置下次启动文件后，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行的情况下，对系统软件进行安装。 ● 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件提供的功能。但是文件仍然存在于存储介质上

7.48.4.3 立即升级

7.48.4.3.1 通过ipe文件方式立即升级

步骤1 选择“系统 >升级中心 > 软件更新”。

步骤2 单击“立即升级“按钮，进入立即升级页面，启动文件类型选择ipe文件。

步骤3　单击<选择>按钮，选择待升级的ipe软件升级包。

步骤4　其他配置保持系统默认即可。

步骤5　单击<确定>按钮，进行软件升级。

7.48.4.3.2　通过bin文件方式立即升级

步骤1　选择“系统 >升级中心 > 软件更新”。

步骤2　单击“立即升级“按钮，进入立即升级页面，启动文件类型选择bin文件。

步骤3　单击<选择>按钮，选择待升级的boot启动文件及system启动文件。

步骤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。

步骤5　其他配置保持系统默认即可。

步骤6　单击<确定>按钮，进行软件升级。

7.49　License本地授权

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
  - 临时License和正式License

7.49.1 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。

7.49.1.1 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。

License特性	授权功能	未安装License	License过期后	授权时间
ACG	应用识别	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、无法升级防病毒特征库	1 年、3 年
IPRPT	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	可使用 Web 应用防护功能	1 年、3 年

License特性	授权功能	未安装License	License过期后	授权时间
		应用防护特征库	无法升级 Web 应用防护特征库	
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

7.49.1.2 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。

7.49.1.3 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。

7.49.2 使用限制和注意事项

7.49.2.1 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。

7.49.2.2 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。

7.49.3 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。

7.49.4 配置指南

7.49.4.1 通过激活文件授权

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。
- 获取DID和SN。
- 根据产品类型、授权码、SN和DID文件申请激活文件。
- 通过License配置菜单的安装按钮安装激活文件，获得授权。

7.49.4.2 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。

7.50 License Server授权

本帮助主要介绍以下内容：

- 特性简介
- 使用限制和注意事项
- vSystem相关说明
    - 配置License server信息
    - License client获取授权

7.50.1 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。

设备获取授权（License）有两种方式：

- 本地授权：需要在本设备上安装License来获取授权。
- 通过License server授权：用户需要先在 License server上安装激活文件来获得License授权，设备作为License client，向License server申请授权。

License client根据需要与License server建立连接并通过认证后，从服务器端获取相应的授权并安装，授权使用完毕后，归还给License server。这样就实现了多台License client共用License资源的效果，避免了License资源的浪费。本文档将介绍通过License server授权的方法。

7.50.2 使用限制和注意事项

- 如需修改License server的地址和端口，请先关闭License client功能。
- 最多可配置四个License server，当配置了多个License server时，请确保同一时刻，仅有一台运行稳定的License server路由可达，以免授权信息交互混乱。

7.50.3 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。

7.50.4 配置指南

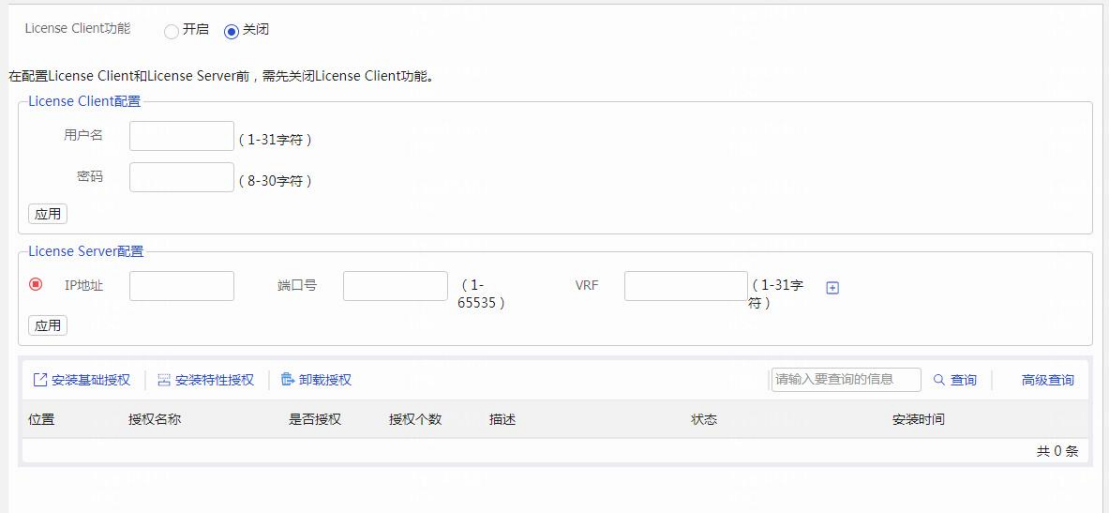
7.50.4.1 配置License server信息

License server的具体配置步骤如下：

步骤1 选择“系统 > License Server授权”。

步骤2 在“ License Server授权”页面，配置License client的用户名及密码，请确保该用户已在License server上注册，单击<应用>按钮。

步骤3 配置License server的IP地址、端口号及VRF，单击<应用>按钮，完成License server信息配置。



7.50.4.2 License client获取授权

License client获取授权的具体配置步骤如下：

步骤1 选择“系统 > License Server授权”。

步骤2 在“License Server授权”页面，选择“License Client功能”对应的开启选项。

步骤3 单击<安装基础授权>按钮，选择需要安装的基础授权，单击<确定>按钮。

步骤4　单击<安装特性授权>按钮，选择需要安装的特性授权，输入授权个数，单击<确定>按钮，完成License client获取授权配置。

7.51　IRF高级设置

本帮助主要介绍以下内容：

- 特性简介
  - 原理介绍
  - 工作模式
- 冗余组
  - 成员设备
  - 成员接口
  - 冗余口

7.51.1 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联机帮助”。

7.51.1.1 原理介绍

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。

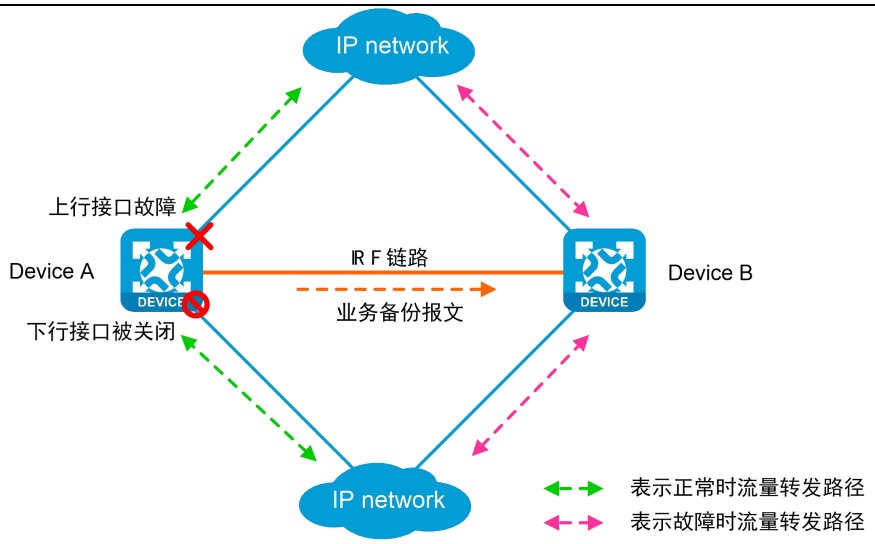
IRF双机热备的实现机制如下图所示：

步骤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。

步骤2 当Track检测到Device A的上行接口故障。

步骤3 冗余组关闭Device A的下行接口。

步骤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。



7.51.1.2 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。

7.51.2 冗余组

7.51.2.1 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。

7.51.2.2 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。

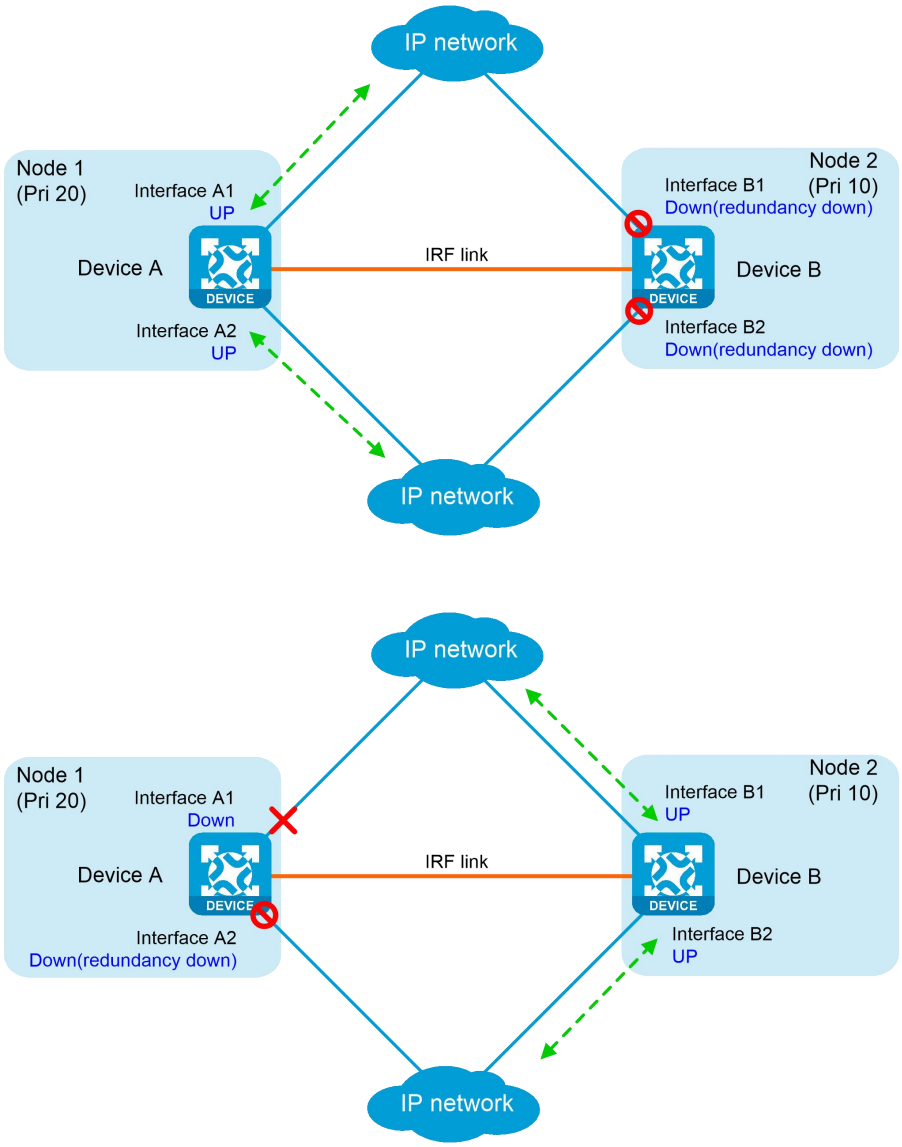
主成员设备下的成员接口指的是主成员设备的上行接口和下行接口，可加入多个接口。

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。

如下图所示，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，如下图所示。



7.51.2.3 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：

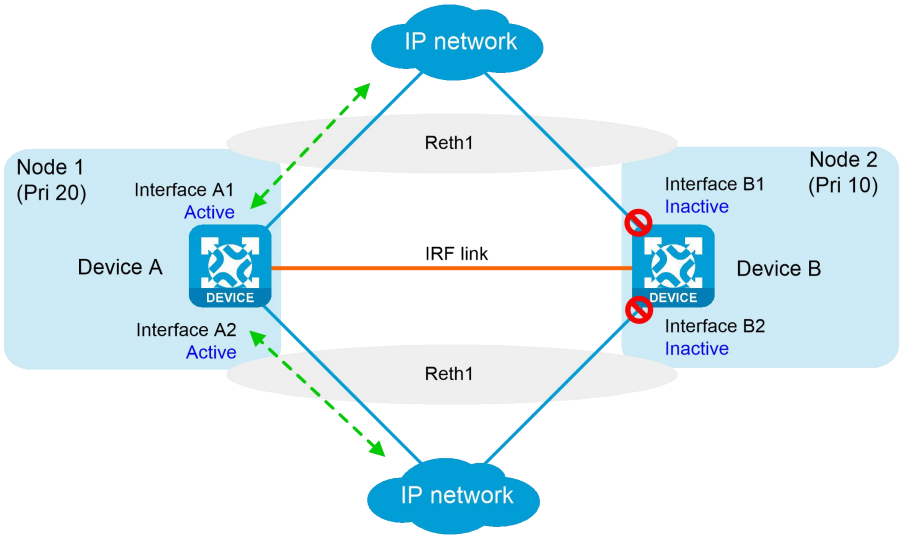
- 主成员接口：主成员设备的上行接口或下行接口，只能加入一个接口。
- 备成员接口：备成员设备的上行接口或下行接口，只能加入一个接口。

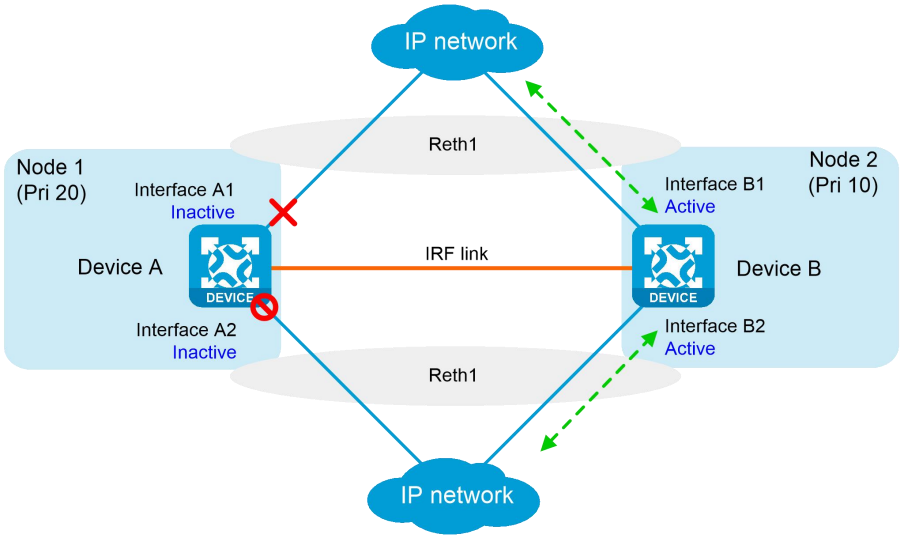
一个冗余组下可以配置多个冗余口，通常至少需要配置两个冗余口，一个冗余口的子成员均为上行接

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。

如下图所示，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，如下图所示。





7.51.2.4 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。

7.51.2.5 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。

7.51.3 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。

7.51.4 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。
- 当会话创建方式为Hash模式同时又开启了透传UDP报文时，报文使用Hash方式选板。
- IRF双机热备的双主模式仅支持基于流的流分类策略。

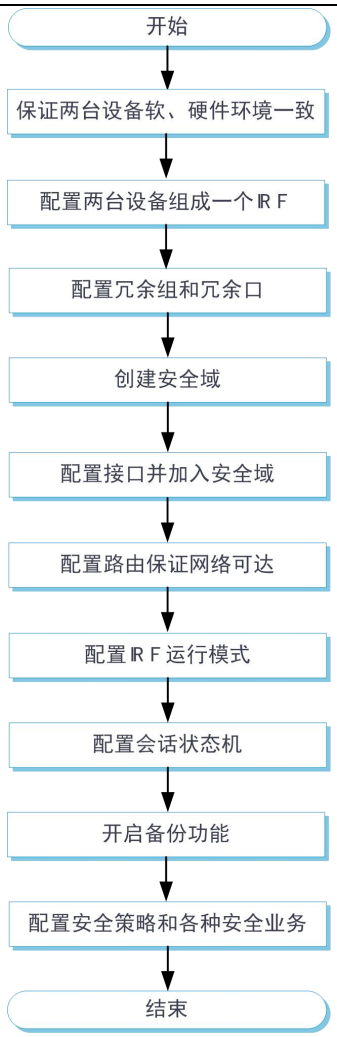
7.51.5 配置指南

7.51.5.1 配置准备

配置IRF双机热备之前，请确保两台设备已经组成一个IRF。

7.51.5.2 配置思路

IRF双机热备功能的配置思路如下图所示：



7.51.5.3 配置IRF双机热备

步骤1 选择“系统 > 高级虚拟化 > IRF高级设置”。

步骤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。

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，实时待命 ● 双主模式：两台设备同时处理业务，充分利用设备资源，提高系统负载能力
会话状态机	会话包括如下三种状态机： ● 严格模式：在对称路径流量网络环境中，建议使用此模式，可提高网络安全性 ● 宽松模式：在主备组网环境中，当出现非对称路径流量时，需要将会话状态机的模式配置为此种模式，可以避免异常会话丢包 ● 简化模式：在双主组网环境中，当出现非对称路径流量时，需要将

参数	说明
	会话状态机的模式配置为此种模式，会话断开后可以及时老化会话
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业务的目的，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，设备支持的会话创建方式包括如下几种： ● 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，同一条流量的接收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布不太均匀的网络情况 ● 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，同一条流量的接收设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分布比较均匀的网络情况 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 报文透传到另一台设备进行处理，若在另一台设备上也未匹配会话，则会在此设备上为其创建会话 此功能仅在双主模式下支持

7.51.5.4 开启热备功能

在IRF双机热备组网环境中必须开启会话表项热备功能才真正能够实现业务的平滑迁移。

步骤1 选择“系统 > 高级虚拟化 > IRF高级设置”。

步骤2 在“IRF高级设置”页面配置热备功能，具体信息如下表所示。

参数	说明
备份会话表项	会话业务热备份功能实现了多台设备之间会话以及基于会话的业务的动态表项的热备份。在 IRF 双机热备环境中，必须开启此功能
备份 DNS 协议 备份 HTTP 协议	对于 DNS 和 HTTP 类型的应用协议，通常在很少的报文交互之后就会断开连接，当发生主备切换造成当前连接中断时，客户端会立即重新发起请求，用户通常感知不到连接异常。因此，在大多数情况下这些应用协议不需要进行会话备份

7.51.5.5 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：

步骤1 选择“系统 > 高级虚拟化 > IRF高级设置”。

步骤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。

步骤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，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。

步骤4　在编辑冗余组页面可以配置冗余组和冗余口。

步骤5　冗余组具体配置信息如下表所示。

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，一个为备成员设备。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。至少需要将此设备的上行和下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。具体配置请参见下面的冗余口配置
Track	通过和 Track 联动来自动触发冗余组的整体倒换/倒回

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

步骤6　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。

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置为 Down，物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设备的速度。如果关闭此功能，则将主设备接口的协议状态和物理状态均设置为 Down

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。

7.52 管理员

本帮助主要介绍以下内容：

7.52.1 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。

7.52.1.1 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。

7.52.1.2 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。

7.52.1.2.1 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。

7.52.1.2.2 缺省角色

系统预定义了多种角色，角色名和对应的权限如下表所示。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。

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

7.52.1.2.3 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。

7.52.1.3 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。

7.52.1.3.1 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。

7.52.1.3.2 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

7.52.1.3.3 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。

7.52.1.3.4 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。

7.52.1.3.5 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

7.52.1.3.6 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。

7.52.1.3.7 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。

7.52.1.3.8 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。

7.52.1.3.9 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。

7.52.1.3.10 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。

7.52.1.4 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。

7.52.2 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。

7.52.3 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。

7.52.4 配置指南

7.52.4.1 新建管理员

步骤1 选择“系统 > 管理员 > 管理员”。

步骤2 在“管理员”页面配置相关内容，具体配置内容如下表所示：

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有不同的系统功能
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务类型，则该用户无法通过认证
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，则使用该用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

步骤3 （可选）高级设置，具体包括如下表所示：

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启相关功能才能生效
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

参数	说明
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功能才能生效
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，此功能需要在密码管理中开启相关功能才能生效
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

步骤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。

7.52.4.2　密码管理

步骤1　单击“系统 > 管理员 > 管理员”。

步骤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。

步骤3　在“管理员密码管理”页面的具体配置内容如下表所示：

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	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

参数	说明
含连续三个或以上相同的相同字符	
密码中不能包含用户名或者字符顺序颠倒的用户名	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
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录
开启密码老化	当密码历史记录的条数超过设置的最大历史记录条数时，新的密码历史记录将覆盖该用户最老的一条密码历史记录
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

步骤4　单击<确定>按钮，完成密码管理的配置。

7.52.4.3　新建管理员角色

步骤1　选择“系统 > 管理员 > 管理员角色”。

步骤2　在“管理员角色”页面配置相关内容，具体配置内容如下表所示：

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，通过控制菜单项中读写、只读或无的操作，来完成管理员角色权限的定制

步骤3　单击<确定>按钮，完成新建管理员角色的配置。

7.53　设备信息

7.53.1　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。

7.54　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

7.54.1 特性简介

7.54.1.1 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）。

7.54.1.2 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。

7.54.1.3 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。

模式	工作过程	时间同步方向	应用场合
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	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间同步	该模式通常用于下级的设备从上级的时间服务器获取时间同步
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	该模式通常用于同级的设备间互相同步，以便在同级的设备间形成备份。如果某台设备与所有上级时间服务器的通信出现故障，则该设备仍然可以从同级的时间服务器获得时间同步

7.54.1.4 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。

7.54.2 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。

7.54.3 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。

7.54.4 配置指南

7.54.4.1 手工设置日期和时间

步骤1 选择“系统 > 系统与维护 > 系统设置 > 日期和时间”。

步骤2 在“日期和时间”页面勾选<手工设置日期和时间>按钮。

步骤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：

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

步骤4 单击<应用>按钮，可完成手工设置日期和时间操作。

7.54.4.2 自动同步网络日期和时间

步骤1 选择“系统 > 系统与维护 > 系统设置 > 日期和时间”。

步骤2 在“日期和时间”页面勾选<自动同步网络日期和时间>按钮。

步骤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：

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）

配置项	说明	
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	
身份验证密钥 ID 和密钥	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	
时钟源	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。	
	VRF	下拉选择 VRF。可选择已有的恶 VRF，如需新建 VRF，具体的配置步骤请参见“网络 > VRF”
	类型	● 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
	时钟源工作模式	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
	身份验证密钥 ID	身份验证密钥 ID 是密钥的编号
	NTP 版本号	NTP 协议的版本（现有版本 1-4）
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	

配置项	说明
	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

步骤4　单击<应用>按钮，可完成自动同步网络日期和时间操作。

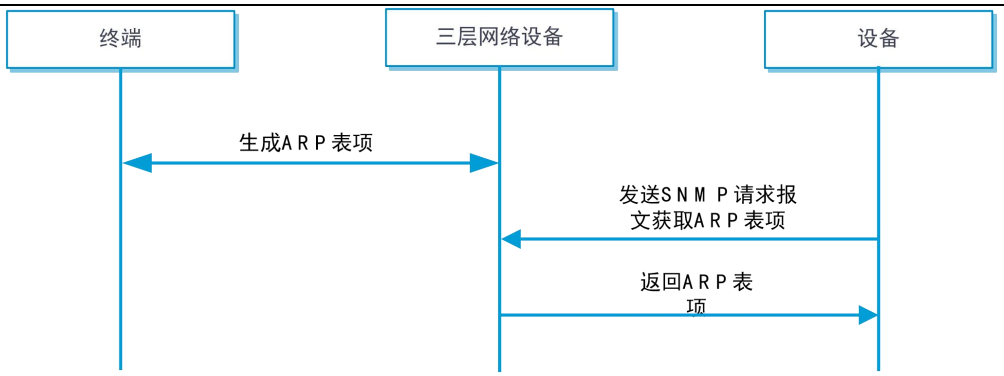
7.55　跨三层MAC学习

本帮助主要介绍以下内容：

7.55.1　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。



跨三层MAC学习具体流程如下：

步骤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；

步骤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；

步骤3　三层网络设备响应SNMP请求报文，返回ARP表项；

步骤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。

7.55.2　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。

7.55.3　配置指南

7.55.3.1　配置跨三层MAC学习

7.55.3.1.1　配置准备

在配置跨三层MAC学习功能之前，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。

7.55.3.1.2　配置步骤

跨三层MAC学习的具体配置步骤如下：

步骤1　选择“系统 > 系统与维护 > 跨三层MAC学习 > 三层设备访问设置”。

步骤2　在“三层设备访问设置”页面开启跨三层MAC学习功能。

步骤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。

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

参数	说明
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

步骤4　单击<应用>按钮。

步骤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。

步骤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。

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，以获取此三层设备上的 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。只有与目标三层设备上 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 的配置信息相同时，才能认证成功进行互相访问
认证密码	
加密方式	
加密密码	

步骤7　单击<确定>按钮。

步骤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。

7.56　SNMP

7.56.1　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。

7.56.1.1 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。

7.56.1.2 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。

7.56.2 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。

7.56.3 配置指南

步骤1 单击“系统 > 系统与维护 > SNMP”。

步骤2 开启SNMP功能。

步骤3 配置SNMP版本及各版本公共信息。

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

步骤4　单击<应用>按钮，使SNMP版本及各版本公共信息的配置生效。

步骤5　选择SNMP版本并进行版本配置。

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

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

参数	说明
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

步骤6　单击<应用>按钮，使SNMP版本配置生效。

7.57　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

7.57.1 特性简介

7.57.1.1 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。

7.57.1.2 配置的类型

7.57.1.2.1 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。

7.57.1.2.2 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。

7.57.1.2.3 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。

7.57.2 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。

7.57.3 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。

7.57.4 配置指南

7.57.4.1 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。

7.57.4.1.1 配置步骤

步骤1 选择“系统 > 系统与维护 > 配置文件”。

步骤2 在“配置文件”页面单击<保存当前配置>按钮。

步骤3 在“保存当前配置”页面的具体配置内容如下表所示：

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

步骤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。

7.57.4.2 导出当前配置

步骤1 选择“系统 > 系统与维护 > 配置文件”。

步骤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。

7.57.4.3 导入配置

步骤1 选择“系统 > 系统与维护 > 配置文件”。

步骤2 在“配置文件”页面单击<导入配置>按钮。

步骤3 单击<选择>按钮，选中需要导入的配置文件。

步骤4　单击<确定>按钮，可完成导入配置操作。。

7.57.4.4　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，设备当前的配置将会全部丢失，重启后，请根据重新进行 Web 登录。

7.57.4.4.1　配置步骤

步骤1　选择“系统 > 系统与维护 > 配置文件”。

步骤2　在“配置文件”页面单击<恢复出厂配置>。

步骤3　单击确定后，可完成恢复出厂配置操作。

7.57.4.5　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），可立即备份也可周期性自动备份。

7.57.4.5.1　配置步骤

步骤1　选择“系统 > 系统与维护 > 配置文件”。

步骤2　在“配置文件”页面单击<备份当前配置>按钮。

步骤3　配置备份信息，具体内容如下表所示：

参数	说明
备份方式	备份文件的存放位置，包括“备份至本地”和“备份至服务器”
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”和“TFTP”两种服务器类型
地址	存放备份文件的服务器的 IP 地址

参数	说明
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
备份路径	备份文件在服务器上的存放路径

步骤4　单击<确定>按钮，可完成备份设备当前配置操作。

7.57.4.6　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，回滚前的配置将
  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访
  FTP/TFTP服务。

7.57.4.6.1　配置步骤

步骤1　选择“系统 > 系统与维护 > 配置文件”。

步骤2　在“配置文件”页面单击<配置回滚>按钮。

步骤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。

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 服务器的用户名
密码	访问 FTP/TFTP 服务器的密码

参数	说明
端口	FTP/TFTP 服务器对外提供服务器的端口号
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，则必须配置指定时间
取消服务器回滚	勾选该选项可取消指定时间从服务上获取配置文件进行回滚

7.58 重启

本帮助主要介绍以下内容：

7.58.1 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。

7.58.2 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。

7.58.3 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。

7.58.4 配置指南

7.58.4.1 重启设备

步骤1 单击“系统 > 系统与维护 > 重启”。

步骤2　在“重启”页面单击<重启设备>按钮。

步骤3　重启设备前保存方式的配置选择，具体如下表所示：

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。

步骤4　选择保存方式，单击<确定>按钮，设备重启。

7.59　关于

7.59.1　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。

7.59.2　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。

7.60　快速接入Internet

7.60.1　特性简介

快速接入Internet用于配置设备方便快速的接入Internet。

7.60.1.1　接入模式

接入模式分为路由模式和透明模式。

7.60.1.1.1 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三种，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

WAN口接入互联网的三种方式如下表所示：

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，请选择此连接类型
DHCP	如果您从网络服务提供商（或 DHCP 服务器）自动获取 IP 地址，请选择此连接类型
PPPoE	如果您从网络服务提供商处获得一个上网账户，请选择此连接类型

- 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。

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提供，IP 地址用点分十进制表示（例如，10.1.1.1），掩码长度范围为 1～31
默认路由	WAN 口的默认路由下一跳的 IP 地址。内网用户访问互联网的报文都通过 WAN 口发送到默认路由下一跳，再由下一跳转发。此参数由网络服务提供商提供，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，请参考“DNS 联机帮助”。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，设备会使用备用 DNS 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。

参数	说明
接口	选择 WAN 口

- 选择通过PPPoE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。

参数	说明
接口	选择 WAN 口
用户名	上网账户的用户名，由网络服务提供商提供
密码	上网账户用户名的密码，由网络服务提供商提供
在线方式	● 永久在线：成功建立PPPoE会话后，此会话将一直存在。 ● 空闲自动断线：在设定的时间内如果没有流量通过，设备自动断开PPPoE会话。当您是按时计费用户时建议选择此方式。
自动获取 IP 地址	上网接口自动从网络服务提供商获取 IP 地址
使用指定的 IP 地址	手工配置上网接口的 IP 地址
IP 地址/掩码长度	此参数由网络服务提供商提供，IP 地址用点分十进制表示（例如，10.1.1.1），掩码长度范围为 1～31

◆ LAN口配置

LAN口各配置项参数的说明如下表所示：

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 地址用点分十进制表示（例如，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 DHCP 的详细介绍，请参考“DHCP 联机帮助”
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

7.60.1.1.2 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。透明模式下各配置项参数的说明如下表所示：

参数	说明
WAN 接口	选择 WAN 口
LAN 接口	选择连接局域网的接口

7.60.2 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。

7.60.3 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。