Hillstone Networks, Inc.

S系列 WebUI 用户手册

Version 5.5R1-1.0

Hillstone Networks, Inc.

联系信息

公司总部（北京总部）：

地址： 北京市海淀区王庄路一号清华同方科技广场D座6层

邮编： 100083

联系我们：http://www.hillstonenet.com.cn/about/contact_Hillstone.html

关于本手册

本手册介绍Hillstone Networks, Inc. 公司的StoneOS系统的使用方法。

获得更多的文档资料，请访问：http://docs.hillstonenet.com.cn.cn

针对本文档的反馈，请发送邮件到：hs-doc@hillstonenet.com

Hillstone Networks, Inc.

http://www.hillstonenet.com.cn

TWNO: TW-WUG-SS-A-5.5R1-1.0-CN-V1.0-2016/1/28

发布日期： 2016年1月28日

目 录

第1章 新手入门指南

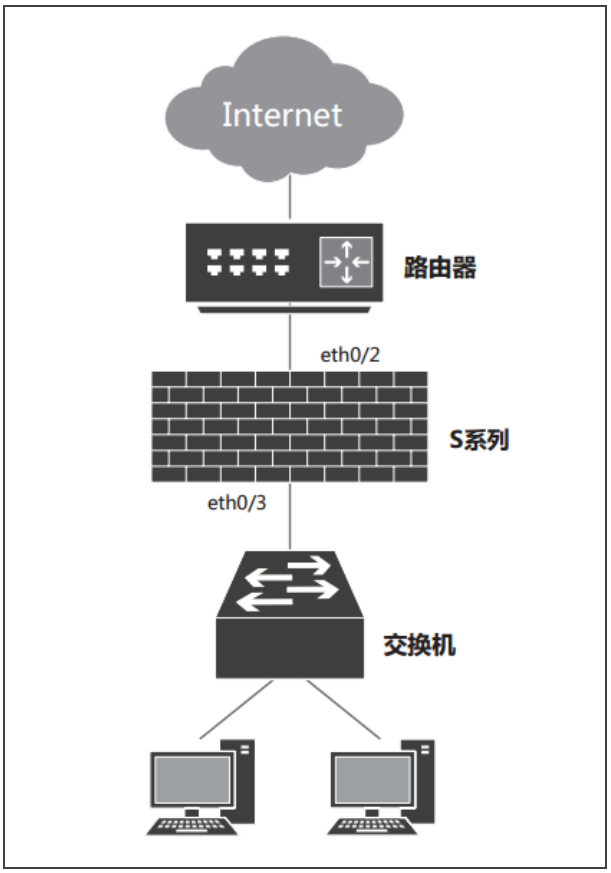
本新手入门指南帮助用户快速完成设备的上线及初始配置:

- 部署设备：设备有多种部署模式，每个部署模式适用于不同的应用场景。
  - "部署透明模式" 在第10页：主要适用于需要对报文进行快速分析和转发的场景。可对攻击进行记录日志/重置/阻断。设备已经预定义了安全域、接口、策略的配置，便于用户通过透明模式快速连通网络。
  - "部署旁路（Tap）模式" 在第12页：主要适用于设备检测攻击行为并记录日志的场景。
  - "部署路由模式" 在第13页：主要适用于需要设备提供路由和NAT功能的场景。
- "访问WebUI界面" 在第19页
- "初始配置" 在第20页
  - 安装许可证
  - 创建系统管理员
  - 配置可信主机
  - 升级特征库
- "恢复出厂配置" 在第23页

部署透明模式

一般情况下，设备通过透明模式部署在原有网络的路由器和交换机之间，对通过的流量进行检测。当检测到攻击行为时，可对攻击进行记录日志/重置/阻断。

设备已经预定义了安全域、接口、策略的配置，便于用户通过透明模式快速连通网络。请按照如下拓扑图连接网线，内网用户即可以通过设备访问互联网。



使用此透明模式时，接口、接口所在安全域、安全域间策略、以及入侵防御的配置请参照如下表格所示。

对于S2060/S2560/S3560/S3860，用户可另行选择其他接口对部署透明模式。

S1060/S1560			
接口	**安全域**	**安全策略**	
eth0/2	二层安全域：l2-direct-a	源安全域：l2-direct-a 目的安全域：l2-direct-a 源地址：Any 目的地址：Any 服务/服务组：Any	入侵防御：启用 模板：l2-direct-a-default-ips
eth0/3	二层安全域：l2-direct-a		

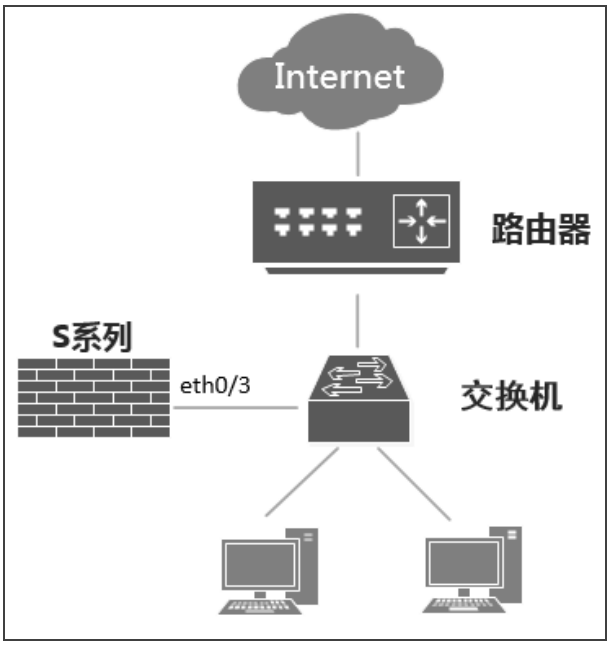
S2060/S2560			
接口	**安全域**	**安全策略**	
eth0/0	二层安全域：l2-direct-a	源安全域：l2-direct-a 目的安全域：l2-direct-a 源地址：Any 目的地址：Any 服务/服务组：Any	入侵防御：启用 模板：l2-direct-a-default-ips
eth0/1			
eth0/2	二层安全域：l2-direct-b	源安全域：l2-direct-b 目的安全域：l2-direct-b 源地址：Any 目的地址：Any 服务/服务组：Any	入侵防御：启用 模板：l2-direct-b-default-ips
eth0/3			

S3560/S3860			
接口	**安全域**	**安全策略**	
eth0/0	二层安全域：l2-direct-a	源安全域：l2-direct-a 目的安全域：l2-direct-a 源地址：Any 目的地址：Any 服务/服务组：Any	入侵防御：启用 模板：l2-direct-a-default-ips
eth0/1			
eth0/2	二层安全域：l2-direct-b	源安全域：l2-direct-b 目的安全域：l2-direct-b 源地址：Any 目的地址：Any 服务/服务组：Any	入侵防御：启用 模板：l2-direct-b-default-ips
eth0/3			
eth0/4	二层安全域：l2-direct-c	源安全域：l2-direct-c 目的安全域：l2-direct-c 源地址：Any 目的地址：Any 服务/服务组：Any	入侵防御：启用 模板：l2-direct-c-default-ips
eth0/5			

部署旁路（Tap）模式

设备工作在旁路模式时，对接收到的镜像流量进行检测，检测到攻击行为时，设备记录日志。同时，可根据入侵防御配置从镜像流量入接口发送Reset报文。

设备已经预定义了安全域、安全策略的配置，便于用户使用旁路模式。请按照如下拓扑图连接网线并完成配置，即可使用旁路模式。



步骤一：配置交换机，将流量镜像到与设备相连接的接口上。

步骤二：将物理接口绑定到tap-a安全域（旁路模式功能域）。绑定后，该物理接口就成为旁路接口。

1. 登录设备的WebUI。详细信息，请参阅"访问WebUI界面" 在第19页。
2. 选择“网络 > 接口”。
3. 双击ethernet0/3，弹出<Ethernet接口>对话框。
4. 在<基本配置>标签页，完成如下配置：

绑定安全域	安全域
TAP	tap-a

完成配置后，设备对从旁路接口收到的镜像流量进行检测。使用此旁路模式时，接口、接口所在安全域、安全域间策略、以及入侵防御的配置如下：

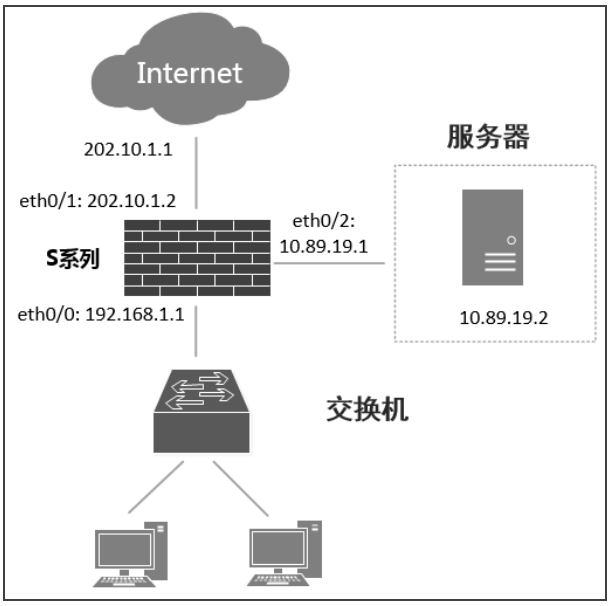
接口	安全域	安全策略	
eth0/3	TAP安全域：tap-a	源安全域：tap-a 目的安全域：tap-a 源地址：Any 目的地址：Any 服务/服务组：Any	入侵防御：启用 模板：tap-a-default-ips

部署路由模式

在路由模式下，设备被部署在网络边界，提供路由功能，NAT功能。

使用路由模式时，需要配置接口、内网trust区域、外网untrust区域、服务器DMZ区域、域间策略等。

本节中的示例将基于以下拓扑图，介绍路由模式的部署。



步骤一：连接设备

1. 将设备的接口（如ethernet0/1）连接到运营商网络中。将设备另一个接口（如ethernet0/0）连接到内网中。
2. 登录设备的WebUI。详细信息，请参阅"访问WebUI界面" 在第19页。。

步骤二：配置接口。

1. 点击“网络 > 接口”。
2. 双击ethernet0/1接口。ethernet0/1接口用于连接外网。

在<Ethernet接口>对话框填写接口的基本配置信息。

选项	配置值
绑定安全域	三层安全域
安全域	untrust
类型	静态IP
IP地址	202.10.1.2
网络掩码	255.255.255.0
管理方式	勾选相应协议复选框，指定接口对应的访问设备的方式。

3. 点击“确定”按钮完成相关配置。
4. 双击ethernet0/0接口。ethernet0/0接口用于连接内网。

在<Ethernet接口>对话框填写接口的基本配置信息。

选项	配置值
绑定安全域	三层安全域
安全域	trust
类型	静态IP
IP地址	192.168.1.1
网络掩码	255.255.255.0
管理方式	勾选相应协议复选框，指定接口对应的访问设备的方式。

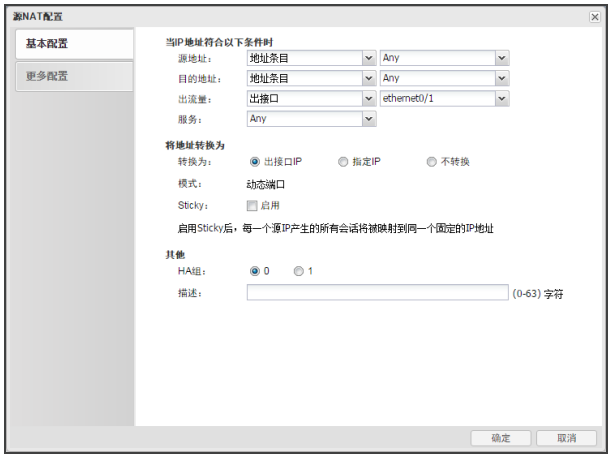
5. 双击ethernet0/2接口。ethernet0/2接口用于连接服务器。

在<Ethernet接口>对话框填写接口的基本配置信息。

选项	配置值
绑定安全域	三层安全域
安全域	dmz
类型	静态IP
IP地址	10.89.19.1
网络掩码	255.255.0.0
管理方式	勾选相应协议复选框，指定接口对应的访问设备的方式。

步骤三：配置源NAT规则，将内网IP转换为出接口IP。

1. 点击“策略 > NAT > 源NAT”。
2. 点击“新建”按钮。



在<源NAT配置>对话框填写源NAT规则的基本配置信息。

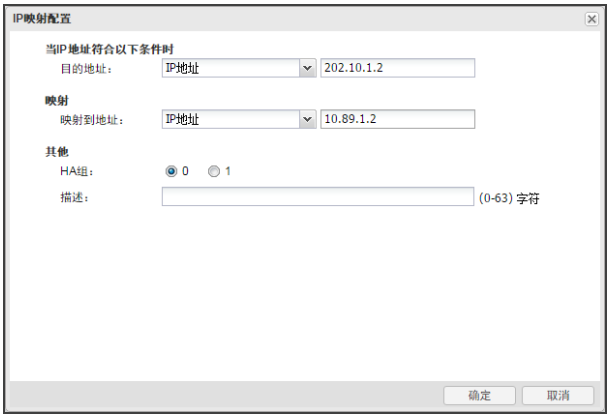
选项	配置值
源地址	地址条目, Any
目的地址	地址条目, Any
出流量	出接口, ethernet0/1

选项	配置值
转换为	出接口IP
Sticky	启用

3. 点击“确定”按钮。

步骤四：配置目的NAT规则，将内部服务器发布到公网IP地址。

1. 点击“策略 > NAT > 目的NAT”。
2. 点击“新建 > IP映射”。



在<IP映射配置>对话框填写目的NAT规则的基本配置信息。

选项	配置值
目的地址	从下拉菜单中选择“IP地址”，输入202.10.1.2。当流量目的IP地址为此IP地址时，对目的IP地址进行转换。
映射到地址	从下拉菜单中选择“IP地址”，输入10.89.19.2。将流量的目的地址转换为输入的地址。

3. 点击“确定”完成配置。

步骤五：配置安全策略，允许内网用户访问外网。

1. 点击“策略 > 安全策略”。
2. 点击“新建”按钮。

在<策略配置>对话框填写策略规则的基本配置信息。

选项	配置值
在<基本配置>标签页配置如下：	
名称	输入安全策略的名称。
源信息	
安全域	trust
地址	Any
目的信息	
安全域	untrust
地址	Any
其他信息	
服务/服务组	Any
应用/应用组	-----
在<威胁防护>标签页配置如下：	
入侵防御	选择“启用”并选择predef-default模板。该模板中的入侵防御规则对匹配特征规则的数据包做重置处理。

3. 点击“确定”按钮。

步骤六：配置安全策略，允许外网用户访问服务器。

1. 点击“策略 > 安全策略”。
2. 点击“新建”按钮。

在<策略配置>对话框填写策略规则的基本配置信息。

选项	配置值
在<基本配置>标签页配置如下：	
名称	输入安全策略的名称。
源信息	
安全域	untrust
地址	Any

选项	配置值
目的信息	
安全域	dmz
地址	Any
其他信息	
服务/服务组	选择内网服务器的服务。
应用/应用组	-----
在<威胁防护>标签页配置如下：	
入侵防御	选择“启用”并选择predef-default模板。该模板中的入侵防御规则对匹配特征规则的数据包做重置处理。

3. 点击“确定”按钮。

步骤七：配置默认路由。

1. 点击“网络 > 路由 > 目的路由”。
2. 点击“新建”按钮。

在<目的路由配置>对话框填写目的路由的基本配置信息。

选项	配置值
目的地	0.0.0.0
子网掩码	0.0.0.0（表示匹配所有的网段）
网关	202.10.1.1

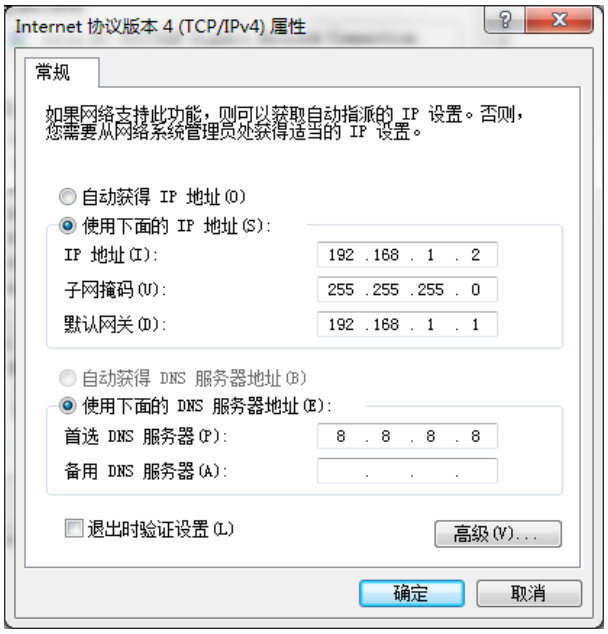
3. 点击“确定”按钮。

访问WebUI界面

设备的ethernet0/0接口或MGT0口配有默认IP地址192.168.1.1/24，并且该接口的各种管理功能均为开启状态。初次使用设备时，用户可以通过该接口访问设备的WebUI界面。

搭建WebUI配置环境，请按照以下步骤进行配置：

1. 将PC的IP地址设置为与192.168.1.1/24同网段的IP地址，在PC的本地连接属性中，设置Internet协议版本4（TCP/IPv4）如下：



2. 用网线将PC与设备的ethernet0/0接口或MGT0口进行连接。
3. 在PC的Web浏览器中输入地址“http://192.168.1.1”并按回车键，打开登录页面。

4. 输入用户名和密码。设备提供的默认用户名和密码均为“hillstone”。
5. 点击“登录”按钮，进入WebUI的主页面。

初始配置

安装许可证

在获得许可证字符串或者许可证文件后，按照以下步骤安装许可证：

1. 点击“系统 > 许可证”。
2. **在<许可证申请>处，选择以下两种方式中的一种导入许可证。**

   - 上传许可证文件：选中“上传许可证文件”单选按钮，点击“浏览”按钮，并且选中许可证文件（许可证为纯文本.txt文件）。
   - 手动输入：选中“手动输入”单选按钮，然后将许可证字符串内容输入到对应的文本框。

3. 点击“确定”按钮。
4. 点击“系统 > 设备管理”，在<设置及操作>标签页，点击“重启设备”。
5. 设备重启之后完成许可证的安装。

创建系统管理员

系统管理员拥有读、执行和写权限，可以在任何模式下对设备所有功能模块进行配置、查看当前或者历史配置信息。

创建系统管理员，请按照以下步骤进行操作：

1. 点击“系统 > 设备管理”。
2. 在<管理员>标签页，点击”新建“按钮。

在<管理员配置>对话框填写系统管理员的基本信息

选项	配置值
管理员	Admin
管理员角色	选择”系统管理员“
密码	123456
重新输入密码	123456
登录类型	选择Telnet、SSH、HTTP和HTTPS的方式登录

3. 点击“确定”按钮保存所做配置。

注意: 设备拥有一个默认系统管理员“hillstone”，用户可以对系统管理员“hillstone”进行编辑（只可编辑密码和访问方式），但是不能删除该管理员。

创建可信主机

系统管理员可以指定一个IP地址范围，在该指定范围内的主机为可信主机。只有可信主机才可以对设备进行管理。

创建可信主机，请按照以下步骤进行操作：

1. 点击“系统>设备管理”。
2. 选择”可信主机“标签页，点击”新建“按钮。

在<可信主机配置>对话框填写可信主机的基本信息

选项	配置值
类型	选择IP地址和掩码。
IP	192.168.1.2/24
登录类型	选择可信主机的登录类型:Telnet、SSH、HTTP和HTTPS。

3. 点击”确定“按钮保存所做配置。

特征库升级

默认情况下，系统会每日自动更新特征库。

注意: 所有特征库升级受许可证控制，如需升级特征库，请先为确保已购买并安装对应的许可证。

升级特征库，请按照以下步骤进行操作：

1. 选择“系统 > 升级管理”。
2. 选择<特征库升级>标签页，找到需要升级的特征库部分。

3. **选择以下两种方式中的一种升级特征库。**

   - 远程升级：点击“立即在线升级”按钮，立即升级特征库。
   - 本地升级：上传本地升级文件。点击“浏览”按钮，选中本地特征库特征文件，点击“上传”按钮，系统开始上传特征库信息。

恢复出厂配置

注意: 该操作将使设备恢复到出厂配置，即所有配置将被删除，包括已备份的系统配置文件。请谨慎操作！

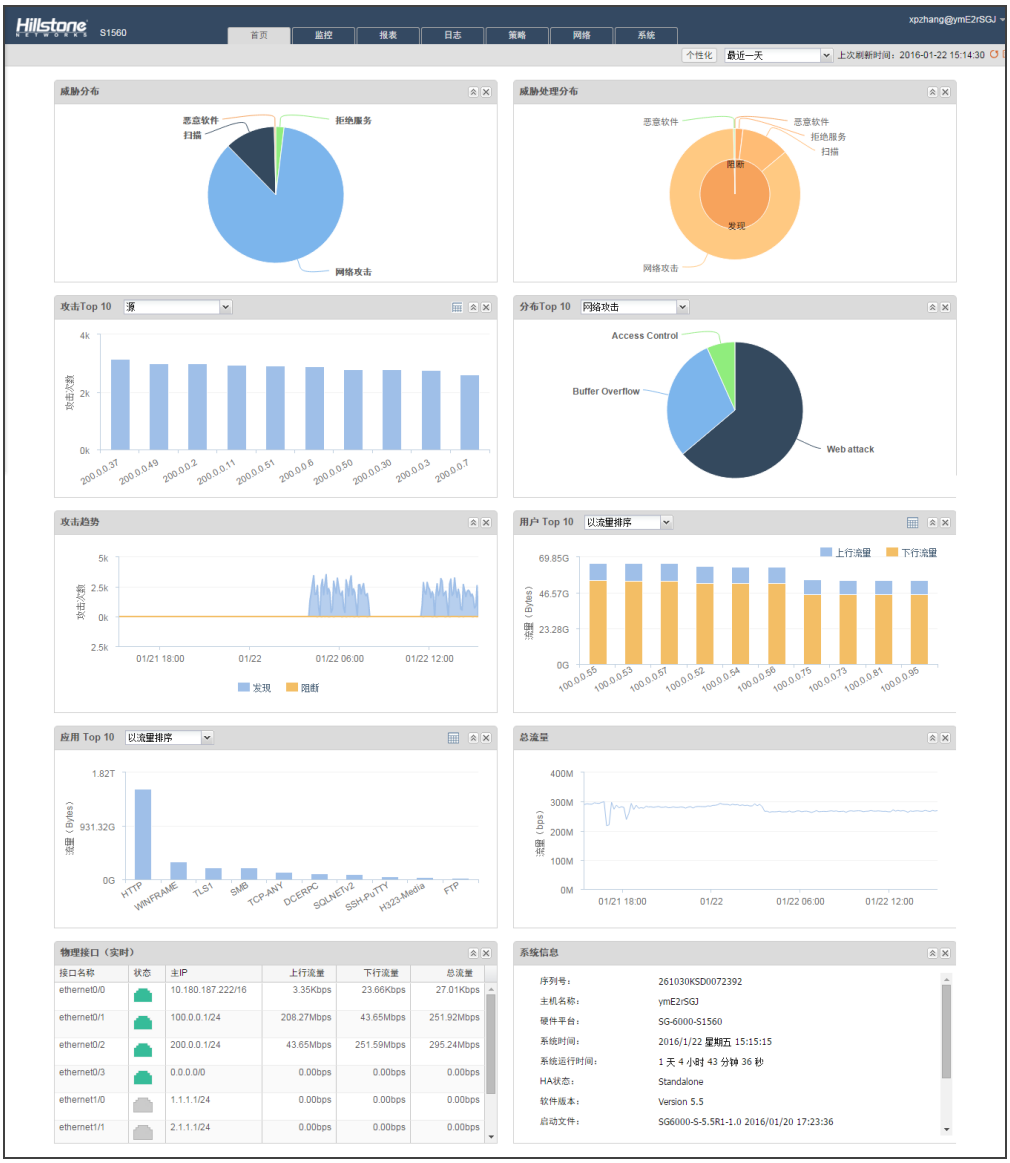
通过WebUI方式恢复出厂配置，请按照以下步骤进行操作：

1. 点击“系统 > 配置文件管理"。
2. 点击“备份恢复”按钮。
3. 在<配置备份/恢复>对话框，点击“恢复”按钮。

4. 在<恢复出厂配置>对话框，点击“确定”按钮。
5. 设备将自动重启，重启后完成恢复出厂配置。所有配置将被删除，包括已备份的系统配置文件。数据库内容不清除。如需清除数据库内容，包括威胁日志、报表、抓包等，请参阅"第13章 CLI" 在第203页。

第2章 首页

首页主要展示威胁防护的统计信息，并同时展示应用、用户、总流量、物理接口的统计信息，以及系统信息。



个性化配置

用户可以根据需要，选择首页所显示的图表类型，修改图表位置，指定统计周期，刷新统计数据。

» 选择首页显示的图表，请按照以下步骤进行操作：

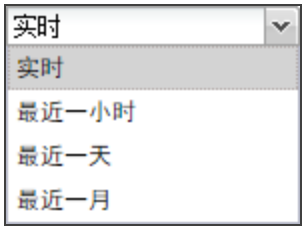
1. 点击首页右上角“个性化”按钮。
2. 在展开的下拉菜单中，选择需要显示在首页的图表。

» 修改图表位置，请按照以下步骤进行操作：

1. 鼠标悬停在图表标题部分。

2. 当出现 时，按住鼠标，将图标拖动到需要显示的位置。

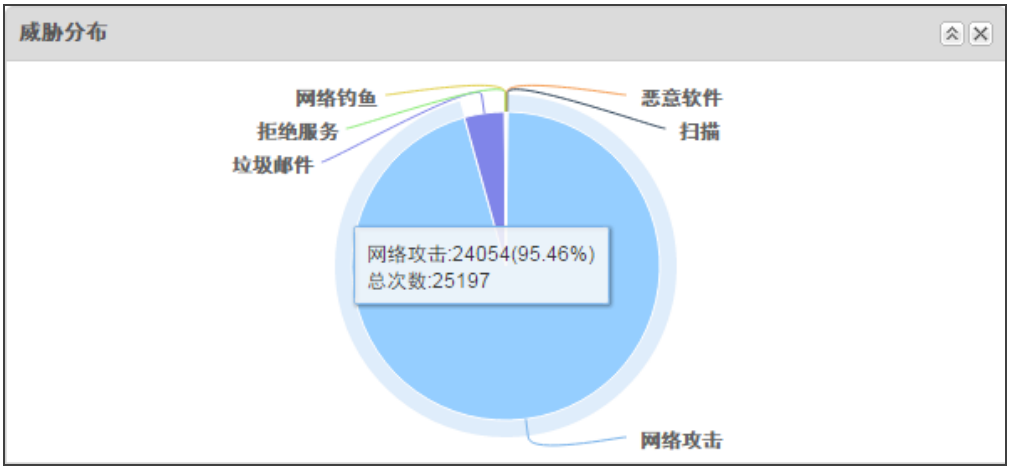
» 通过选择不同的统计周期，可以查看不同时间范围内的统计数据。



» 点击 刷新页面统计数据。

威胁分布

显示设备受到的各种威胁的类型、次数、及占比。

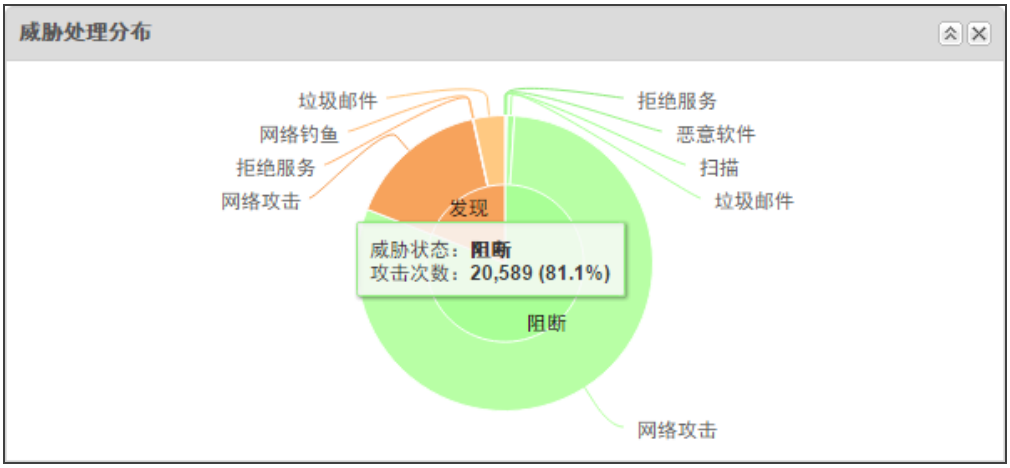


威胁处理分布

显示设备对各种威胁类型的处理方式。

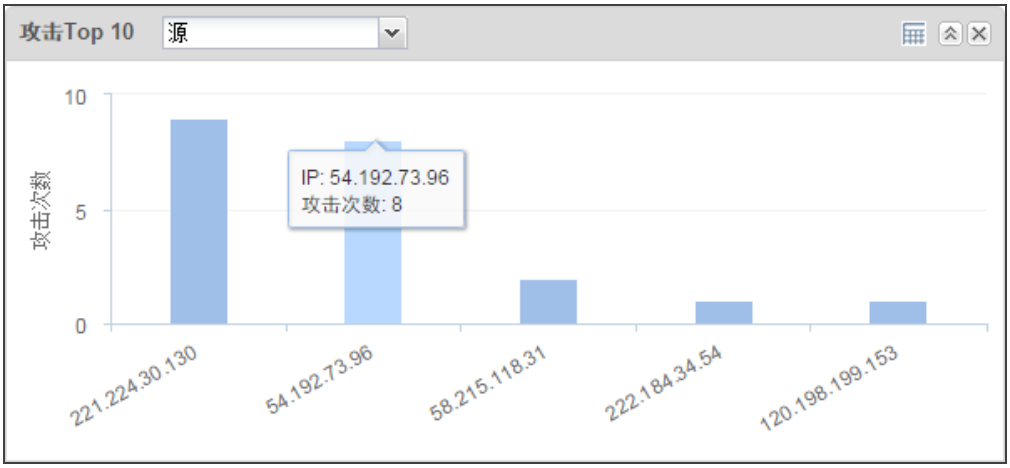
» 内层饼状图表示发现和阻断的攻击的次数。

» 外层饼状图代表在发现和阻断的攻击中，各种威胁类型的攻击次数及占比。

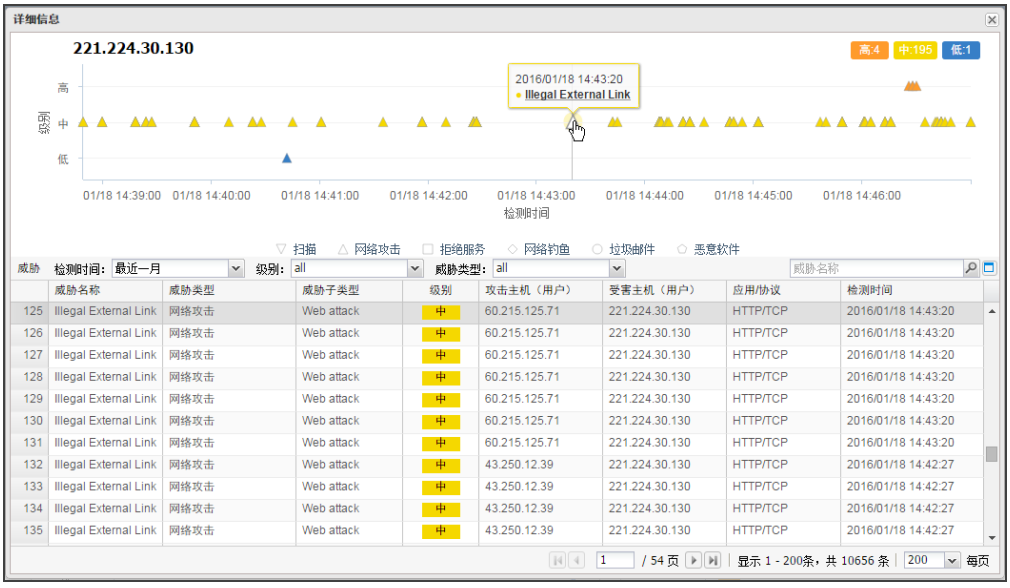


攻击Top 10

显示发起攻击次数排名前10的IP，或者受到攻击次数排名前10的IP。



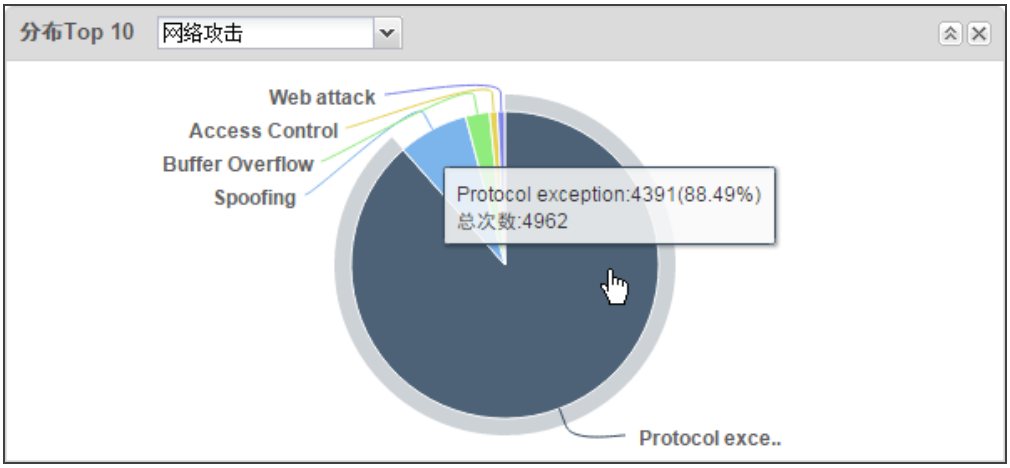
- 下拉菜单用于切换发起攻击次数排名前10的IP和受到攻击次数排名前10的IP。
- 区域右上角、用于将统计图在列表和图形之间切换。
- 当查看发起攻击次数排名前10的IP时，点击每个柱形，打开<详细信息>页面。在<详细信息>页面，显示该IP在检测时间内发起的各级别各类型的攻击的分布及攻击的详细信息。
  当查看受到攻击次数排名前10的IP时，点击每个柱形，打开<详细信息>页面。在<详细信息>页面，显示该IP在检测时间内受到的各级别各类型的攻击的分布及攻击的详细信息。



- 上方分布图显示指定检测时间内的威胁（攻击）分布情况。一个节点代表检测到的一次威胁。不同图形表示不同威胁类型。不同颜色代表不同级别。点击某一节点，查看威胁名称及检测时间，下方列表将高亮显示此威胁具体信息。 在分布图上，可选中一个区域，将显示选中区域所在时间段内的威胁分布情况。
- 下方列表显示指定检测时间内的威胁信息，与分布图中的信息对象。
- 指定检测时间、级别、或威胁类型，可刷新分布图和列表，显示符合条件的威胁分布和信息。
- 在“威胁名称”文本框中输入威胁名称，点击刷新分布图和列表，查看指定威胁的威胁分布图和信息。
- 点击，隐藏分布图，最大化列表。

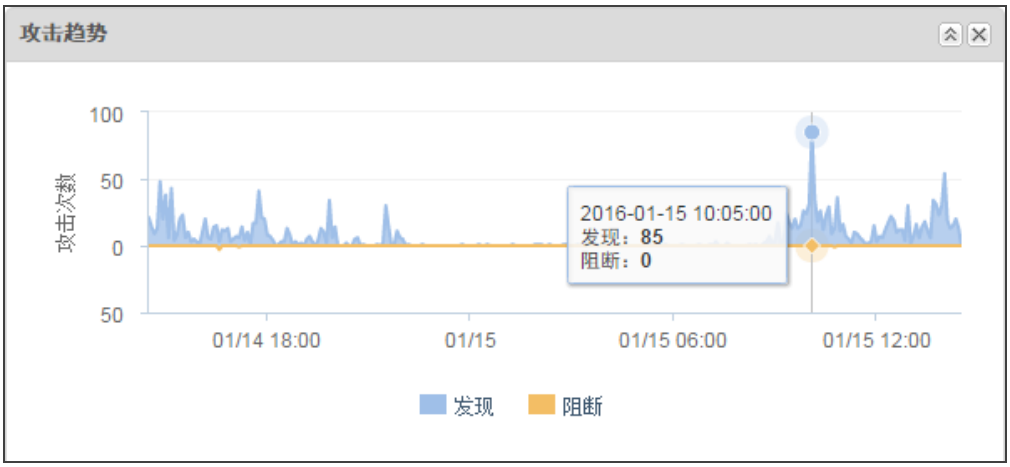
分布Top 10

显示各个威胁类型的子类型的分布。



攻击趋势

显示攻击趋势图和处理方式。



用户Top 10

显示流量或并发连接排名前10的用户。可以在此区域执行以下操作：

- 下拉菜单用于指定显示的应用排序依据：流量或并发连接
- 区域右上角、用于将统计图在列表和图形之间切换。
- 鼠标悬停在某用户对应的柱状图上，查看该用户的上行流量、下行流量、总流量、或并发连接。点击“详细信息”跳转到监控模块的用户详情页面。

应用Top 10

显示流量或并发连接排名前10的应用。可以在此区域执行以下操作：

- 下拉菜单用于指定显示的应用排序依据：流量或并发连接。
- 区域右上角、用于将统计图在列表和图形之间切换。
- 鼠标悬停在某应用对应的柱状图上，查看该应用的总流量或并发连接。点击“详细信息”跳转到监控模块的应用详情页面。

总流量

显示总流量的速率平均值的趋势图。

物理接口

显示设备所有接口的统计信息，包括接口状态、主IP、上行下行流量以及总流量。

系统信息

显示系统的主要信息，包括：

- 序列号：显示该设备的序列号。
- 主机名称：显示该设备指定的名称。
- 硬件平台：显示设备的硬件平台型号。
- 系统时间：显示该设备的系统日期和时间。
- 系统运行时间：显示系统已运行的时长。
- HA状态：显示设备的高可用性工作状态。包括以下六种状态：
  - Standalone：非HA模式，表示设备没有开启HA功能。
  - Init：HA初始状态。
  - Hello：HA协商状态，表示设备在协商HA的主备关系。
  - Master：HA主状态，表示当前设备为HA组的主设备。
  - Backup：HA备状态，表示当前设备为HA组的备份设备。
  - Failed：故障状态，表示当前设备故障。
- 软件版本：显示设备当前的软件版本。
- 病毒过滤特征库：显示设备防病毒特征库版本号，以及上次更新时间。
- 入侵防御特征库：显示设备入侵防御特征库版本号，以及上次更新时间。
- URL分类库：显示设备URL分类库版本号，以及上次更新时间。
- 应用特征库：显示设备应用特征库版本号，以及上次更新时间。

第3章 网络连接

本章介绍设备网络连接的相关要素以及配置。包括：

- 安全域：安全域将网络划分为不同部分，例如trust（通常为内网等可信任部分）、untrust（通常为因特网等存在安全威胁的不可信任部分）等。将配置的策略规则应用到安全域上后，系统就能够对出入安全域的流量进行管理和控制。
- 接口：接口允许流量进出安全域。因此，为使流量能够流入和流出某个安全域，必须将接口绑定到该安全域，并且，如果是三层安全域，还需要为接口配置IP地址。然后，必须配置相应的策略规则，允许流量在不同安全域中的接口之间传输。
- DNS：域名系统。
- DHCP：动态主机配置协议。
- 应用层网关：ALG技术能够保证采用多通道数据传送的应用程序进行正常的数据通信，且保证NAT地址转换后，VoIP应用能够正常通信。
- 全局网络参数：主要包括IP包数据处理选项，例如IP分片、TCP MSS值等。

安全域

在系统中，域是一个逻辑的实体，一个或多个接口可以绑定到域。被应用了策略规则的域即为安全域，为实现某个特定功能而存在的域即为功能域。域具有以下特点：

- 二层和三层安全域决定其接口工作在二层模式或是三层模式。
- 绑定在二层安全域的接口之间的数据按照二层转发规则进行转发。系统预定义的vswitchif1接口相当于交换机的上连口，通过此接口，数据包可以实现二层与三层之间的转发。
- 绑定在三层安全域的接口之间的数据按照三层转发规则进行转发。
- 系统支持域内部策略规则，比如“从trust到trust”的策略规则。

系统中为用户预定义了多个安全域。预定义安全域不允许删除和重命名，可以编辑，修改与接口的绑定关系。

用户也可以自定义域。预定义域与用户自定义域在功能上没有任何差别，用户可以自由选择。

配置安全域

新建安全域，请按照以下步骤进行操作：

1. 选择"网络 > 安全域"，进入安全域配置页面。
2. 点击“新建”按钮，弹出<安全域配置>对话框。
3. 指定安全域名称。在<安全域名称>对话框输入需要的名称。
4. 指定描述信息。
5. 指定安全域类型：二层安全域、三层安全域、TAP。TAP域为旁路模式功能域。
6. 绑定接口到安全域。从“绑定接口”下拉菜单选择需要添加到安全域的接口。
7. 如需要，选中“应用识别”复选框开启安全域的应用识别功能。
8. 如需要，选中“攻击防护”复选框开启安全域的攻击防护功能。详细说明，请参见"攻击防护" 在第135页。
9. 点击“确定”完成安全域的配置。

MGT接口

仅有S2060/S2560/S3560/S3860支持该功能。

为方便用户对设备进行管理和HA组网，设备预定义管理接口MGT0，默认加入到mgt域，预定义MGT1接口，默认加入HA域。

配置MGT接口

配置MGT接口，请按照以下步骤进行操作：

1. 选择“网络 > MGT接口”。
2. 在MGT接口页面，接口名称后的状态灯显示管理接口的状态。
3. 在“安全域”下拉菜单中选择MGT接口所属的安全域。MGT接口只能绑定到三层域。
4. 在“类型”处指定MGT接口获取IP地址的方式，分别为：静态IP和自动获取IP。选择“静态IP”单选按钮，系统为接口指定静态IP地址和网络掩码。点击“高级配置”指定二级IP，最多可以指定6个二级IP地址。选择“自动获取IP”单选按钮，接口将通过DHCP方式自动获取IP地址。
5. 在“管理方式”处指定接口的管理方式。选中需要的管理方式的复选框。
6. 在“工作模式”处指定管理接口的工作模式和速率。当接口的工作模式为“自动”时，接口的速率也必须是“自动”。
7. 在“接口关闭”处选中“立即关闭”复选框强制关闭MGT接口。
8. 点击“确定”。

接口

接口允许流量进出安全域。因此，为使流量能够流入和流出某个安全域，必须将接口绑定到该安全域，并且，如果是三层安全域，还需要为接口配置IP地址。然后，必须配置相应的策略规则，允许流量在不同安全域中的接口之间传输。多个接口可以被绑定到一个安全域，但是一个接口不能被绑定到多个安全域。

设备设备具有多种类型接口，根据性质的不同，分为物理接口和逻辑接口。

- 物理接口：安全设备上的每一个以太网接口都表示一个物理接口。物理接口的名称是预先定义的，由媒体类型、插槽号和位置参数组成，例如ethernet2/1或ethernet0/2。
- 逻辑接口：系统中的逻辑接口包括子接口、回环接口、集聚接口、冗余接口。

根据接口所处安全域的不同，接口还可以分为二层接口和三层接口。

- 二层接口：属于二层域的接口均为二层接口。
- 三层接口：属于三层域的接口为三层接口。只有三层接口可以在NAT/路由模式下工作。

不同类型的接口在设备中具有不同的功能。下表列出各种逻辑接口的描述：

逻辑接口类型	说明
子接口	子接口的名称是它来源的接口名字的扩展，例如ethernet0/2.1。系统支持以下类型子接口：以太网子接口、集聚子接口和冗余子接口。接口和它的子接口可以被绑定到同一个安全域中，也可以被绑定到不同的安全域中。
回环接口	回环接口是逻辑接口，并且只要回环接口所在的安全设备处于工作状态，回环接口就一直处于工作状态。因此，回环接口具有稳定的特性。
集聚接口	集聚接口是物理接口的集合，一个集聚可以包含1到16个物理接口。这些物理接口平均分担流到该集聚接口IP地址的流量负载。因此集聚接口可以提高单个IP地址的可用带宽。如果集聚接口中的一个物理接口出现故障，不能工作，其它接口可以继续处理流量，只是可使用的带宽变小了。
冗余接口	冗余接口能够实现两个物理接口的备份。一个物理接口为主接口处理流向该冗余接口的流量。另外一个接口作为备用接口在主接口发生故障时继续处理流量。

配置接口

不同类型的接口配置选项不同，具体配置方法参见以下说明。

接口通用属性

接口有多种类型，部分属性是通用的。下面介绍接口的通用属性。

1. 选择“网络 > 接口”，进入接口配置页面。
2. 双击一个接口，查看其配置对话框。

在<属性>标签页，配置接口的属性信息。

选项	说明
双工	为接口指定双工工作方式，可以是自动、全双工或者半双工。“自动”是系统默认工作方式，即系统自动选择最佳的双工模式。系统不支持千兆半双工工作模式。
速率	为接口指定工作速率，可以是自动、10M、100M或者1000M。“自动”是系统默认工作方式，即系统自动测定并使用接口的最佳工作速率。系统不支持千兆半双工工作模式。
Combo类型	该选项适用于光口+电口的Combo口。默认情况下，如果光口与电口均有线缆连接，设备会优先使用光口；如果设备最初使用的是电口，连接好光口电缆，重启设备后，设备会使用光口进行数据传输。该选项用于指定光口与电口的使用，选项说明如下： » 自动：上述默认状况。 » 电强制：强制使用电口。 » 电优先：优先使用电口。 » 光强制：强制使用光口。 » 光优先：优先使用光口。配置了该选项后，设备会将电口的流量自动切换到光口，无需重启设备。
MTU	指定接口的最大传输单元，单位为字节。范围是1280到1500/1800字节之间（不同型号的安全设备支持的MTU最大值不同），默认值是1500字节。
ARP学习	选中“启用”复选框开启接口的ARP学习功能。
ARP超时	配置接口的ARP超时时间，单位为秒。范围是5到65535秒，默认值是1200秒。
Keep-alive IP	指定接收接口的Keep-alive报文的IP地址。
MAC克隆	勾选复选框，开启MAC克隆功能，将指定的MAC地址克隆到以太网子接口，点击“恢复缺省MAC”按钮，恢复以太网子接口缺省的MAC地址。

在<高级>标签页，配置接口的高级选项，包括接口关闭和接口监控与备份。

选项	说明
接口关闭	系统支持接口关闭功能，用户不仅可以根据需要强制关闭特定接口，还可以通过时间表控制接口的关闭时间，或者根据监测接口的链路状态控制接口的关闭。 配置方法如下： 1. 选中“立即关闭”复选框开启接口关闭功能。 2. 如果需要通过时间表或者监控对象控制接口的关闭，选中“在时间表”或者“当监控对象”复选框，并且在相应的下拉菜单中选择需要的时间表或者监控对象。
接口监控与备份	配置方法如下： 1. 选中时间表或者监控对象相应的复选框，并从下拉菜单中选择需要的时间表或监控对象。 2. 选择控制方式： » 监控接口，使路由失效：指当到达时间表指定时间时或者指定的监控对象失败时，接口关闭，接口的相关路由失效； » 流量备份到接口：指当到达时间表指定时间时或者指定的监控对象失败时，将接口上的流量转移到备份接口，此时需要从“备份接口”下拉菜单选择备份接口并在“过渡时间”文本框输入过渡时间（指主接口切换到备份接口之前将流量转移到备份接口的过渡时间，单位为秒。取值范围为0到60。主接口会在切换到备份接口前的一段时间，即此处指定的过渡时间，将流量从主接口平滑转移到备份接口。默认情况下无平滑过渡时间，所有的流量会立刻从主接口转移到备份接口）。

在<RIP>标签页，配置接口的RIP功能。

选项	说明
认证方式	指定接口的报文认证方式，有明文（系统默认方式）和MD5两种。明文认证不能提供安全保障。未加密的认证字随RIP报文一同传送，所以明文认证不能用于安全性要求较高的情况。
认证码	指定接口的RIP认证码。
发送版本	指定接口发送RIP信息的版本号。默认情况下，缺省值为接口发送V1&V2 RIP信息。
接收版本	指定接口接收RIP信息的版本号。默认情况下，缺省值为接口接收V1&V2 RIP信息。
水平分割	指定是否开启接口的水平分割功能。水平分割是指不从本接口发送从该接口学到的路由。它可以在一定程度上避免产生路由环，保证路由的正确传播。

新建回环接口

新建回环接口，请按照以下步骤进行操作：

1. 选择“网络 > 接口”，进入接口配置页面。
2. 点击“新建”下拉菜单，并选择“回环接口”，弹出<回环接口>对话框。

在<基本配置>标签页，配置接口的基本配置信息。

选项	说明
接口名称	指定接口名称。
描述	用户可根据需要指定接口描述信息，范围是0到63个字符。
绑定安全域	如选择“二层安全域”、“三层安全域”或者“TAP”，则继续从“安全域”下拉菜单选择安全域的名称。如选择TAP安全域，可继续指定内网地址，使设备能够辨别内网流量，并在监控中进行展示。如选择“无绑定”，该接口将不绑定到任何安全域上。
安全域	从下拉菜单中选择安全域。
类型	根据IP类型不同进行如下的配置，包括静态IP和自动获取。
静态IP	IP地址：为接口指定IP地址。 网络掩码：为接口指定网络掩码。 高级选项： » 管理IP：为接口指定管理IP。在文本框中输入IP地址。 » 二级IP：为接口指定二级IP。最多可以指定6个二级IP地址。 DHCP：点击倒三角，选择“DHCP服务器”或“DHCP中继代理”进行相关配置。具体说明参见"DHCP" 在第45页。
自动获取	DHCP服务器提供的网关信息设置为默认网关路由：选中该选项复选框，系统会将DHCP服务器提供的网关信息设置为默认网关路由。 高级选项： » 路由距离：指定路由距离。范围是1到255，默认值是1。 » 路由权值：指定路由权值。范围是1到255，默认值是1。 » 管理优先级：指定DNS服务器的优先级。除了静态配置的DNS服务器，系统还可以通过DHCP学到DNS服务器，因此，需要配置这些DNS服务器的优先级，当系统做DNS解析时，会按照优先级从高到底的顺序使用DNS服务器。优先级用1到255的数字表示，数字越大，优先级越高。静态配置的DNS服务器的优先级是20。
管理方式	选中该接口需要的管理方式的复选框。
逆向路由	根据需要启用或关闭逆向路由。 » 启用：强制使用逆向路由。如果找不到逆向路由，则丢弃数据包。默认情

选项	说明
	况下，接口强制使用逆向路由。 » 关闭：不使用逆向路由。反向数据流到达接口后不进行逆向路由检查，原路返回（即从初始化数据包的入接口发送反向数据包）。 » 自动：优先使用逆向路由。如果能够找到逆向路由就使用逆向路由发送数据包；如果找不到逆向路由以初始化数据包的入接口作为发送反向数据包的出接口。

3. "在<属性>标签页，配置接口的属性信息。" 在第33页
4. "在<高级>标签页，配置接口的高级选项，包括接口关闭和接口监控与备份。" 在第34页
5. "在<RIP>标签页，配置接口的RIP功能。" 在第34页
6. 点击“确定”完成配置。

新建集聚接口

新建集聚接口，请按照以下步骤进行操作：

1. 选择“网络 > 接口”，进入接口配置页面。
2. 点击“新建”下拉菜单，并选择“集聚接口”，弹出<集聚接口>对话框。

在<基本配置>标签页，配置接口的基本配置信息。

选项	说明
接口名称	指定接口名称。
描述	用户可根据需要指定接口描述信息，范围是0到63个字符。
绑定安全域	指定安全域类型。 如选择“三层安全域”、“二层安全域”或者"TAP “，则继续从“安全域”下拉菜单选择安全域的名称。如选择TAP安全域，可继续指定内网地址，使设备能够辨别内网流量，并在监控中进行展示。如选择“无绑定”，可继续为接口选择所属的集聚接口或者冗余接口：

属于	说明
集聚接口	指定接口属于某集聚接口。从“接口组”下拉菜单中选择接口所属的集聚接口。
冗余接口	指定接口属于某冗余接口。从“接口组”下拉菜单中选择接口所

<table>
<tr><th>选项</th><th>说明</th></tr>
<tr><td></td><td>
<table>
<tr><th>属于</th><th>说明</th></tr>
<tr><td></td><td>属的冗余接口。</td></tr>
<tr><td>无</td><td>指定接口不属于任何对象。</td></tr>
</table>
</td></tr>
<tr><td>安全域</td><td>从下拉菜单中选择安全域。</td></tr>
<tr><td>聚合方式</td><td>选择接口的聚合方式：
» 强制模式： 将多个物理接口聚合为一个集聚接口，这些物理接口平均分担通过该集聚接口的流量。
» 在接口上启用LACP协议，动态协商聚合链路。用户可配置以下LACP相关选项：
» 系统优先级：指定LACP系统的优先级。取值范围为1到32768，默认值为32768。LACP系统优先级用于区分两端设备优先级的高低，以确保两端设备选中的接口一致。协议会以LACP系统优先级高的一端为标准选择接口。数值越小，优先级越高。当两端的LACP系统优先级一致时，比较两端设备的MAC地址，MAC地址小的一端优先级高。
» 最大链路数：指定最大活动链路数，即最大Active接口数。取值范围为1到16，默认值为16。当Active接口数达到最大值时，其它合法接口将变为Standby状态。
» 最小链路数：指定最小活动链路数，即最小Active接口数量。取值范围为1到8，默认值为1。当聚合组中的Active接口数量小于该最小值时，系统会自动将聚合组中的所有合法接口都设置为Standby状态，不可参与流量转发。</td></tr>
<tr><td>HA同步</td><td>选中该选项复选框开启HA同步，主设备和备用设备信息同步。</td></tr>
<tr><td>端口选择</td><td>为集聚接口指定物理端口。从下拉菜单中选择需要的端口，该端口需不属于任何其它接口也不属于任何安全域。</td></tr>
<tr><td>类型</td><td>根据IP类型不同进行如下的配置，包括静态IP和自动获取。</td></tr>
<tr><td>静态IP</td><td>IP地址：为接口指定IP地址。
网络掩码：为接口指定网络掩码。
启用DNS代理：选中该选项复选框开启接口的DNS代理功能。
» 使用DNS普通代理时，客户端收到的DNS应答来自其配置的DNS服务器，只有客户端的DNS服务器地址为设备的接口地址时，设备才承担DNS服务器功能；
» 使用DNS透明代理时，不管客户端的DNS服务器地址是否为设备接口地址，其收到的DNS应答均来自设备。在DNS透明代理模式下，用户无需逐个修改客户端的DNS参数，只要通过设备的DNS配置即可控制所管理网络上的DNS服务。
启用DNS透传：选中该选项复选框开启接口的DNS透传功能。
高级选项：
» 管理IP：为接口指定管理IP。在文本框中输入IP地址。
» 二级IP：为接口指定二级IP。最多可以指定6个二级IP地址。
DHCP：点击倒三角，选择“DHCP服务器”或“DHCP中继代理”进行相关配置。具体说明参见"DHCP" 在第45页。</td></tr>
<tr><td>自动获取</td><td>DHCP服务器提供的网关信息设置为默认网关路由：选中该选项复选框，系统会将DHCP服务器提供的网关信息设置为默认网关路由。</td></tr>
</table>

选项	说明
	高级选项 ： » 路由距离：指定路由距离。范围是1到255，默认值是1。 » 路由权值：指定路由权值。范围是1到255，默认值是1。 » 管理优先级：指定DNS服务器的优先级。除了静态配置的DNS服务器，系统还可以通过DHCP或者PPPoE方式动态学到DNS服务器，因此，需要配置这些DNS服务器的优先级，当系统做DNS解析时，会按照优先级从高到底的顺序使用DNS服务器。优先级用1到255的数字表示，数字越大，优先级越高。静态配置的DNS服务器的优先级是20。
管理方式	选中该接口需要的管理方式的复选框。
逆向路由	根据需要启用或关闭逆向路由。 » 启用：强制使用逆向路由。如果找不到逆向路由，则丢弃数据包。默认情况下，接口强制使用逆向路由。 » 关闭：不使用逆向路由。反向数据流到达接口后不进行逆向路由检查，原路返回（即从初始化数据包的入接口发送反向数据包）。 » 自动：优先使用逆向路由。如果能够找到逆向路由就使用逆向路由发送数据包；如果找不到逆向路由以初始化数据包的入接口作为发送反向数据包的出接口。
端口选择	为集聚接口指定物理端口。从下拉菜单中选择需要的端口，该端口需不属于任何其它接口也不属于任何安全域。

3. "在<属性>标签页，配置接口的属性信息。" 在第33页
4. "在<高级>标签页，配置接口的高级选项，包括接口关闭和接口监控与备份。" 在第34页
5. "在<RIP>标签页，配置接口的RIP功能。" 在第34页
6. 在<负载均衡>标签页，配置集聚接口的负载均衡方式。“基于流”表示从数据流中自动获取均衡方式。该方式为系统默认方式。“组合方式”表示系统按照报文的源IP、源MAC、源端口、目的IP、目的MAC、目的端口或者协议类型进行均衡转发，或按照以上方式的组合进行均衡转发。
7. 点击“确定”，完成配置。

新建冗余接口

新建冗余接口，请按照以下步骤进行操作：

1. 选择“网络 > 接口”，进入接口配置页面。
2. 点击“新建”下拉菜单，并选择“冗余接口”，弹出<冗余接口>对话框。

在<基本配置>标签页，配置接口的基本配置信息。

选项	说明
接口名称	指定接口名称。
描述	用户可根据需要指定接口描述信息，范围是0到63个字符。
绑定安全域	如选择“二层安全域”、“三层安全域”或者“TAP”，则继续从“安全域”下拉菜单选择安全域的名称。如选择TAP安全域，可继续指定内网地址，使设备能够辨别内网流量，并在监控中进行展示。如选择“无绑定”，该接口将不绑定到任何安全域上。
安全域	从下拉菜单中选择安全域。
类型	根据IP类型不同进行如下的配置，包括静态IP和自动获取。
静态IP	IP地址：为接口指定IP地址。 网络掩码：为接口指定网络掩码。 高级选项： » 管理IP：为接口指定管理IP。在文本框中输入IP地址。 » 二级IP：为接口指定二级IP。最多可以指定6个二级IP地址。 DHCP：点击倒三角，选择“DHCP服务器”或“DHCP中继代理”进行相关配置。具体说明参见"DHCP" 在第45页。
自动获取	DHCP服务器提供的网关信息设置为默认网关路由：选中该选项复选框，系统会将DHCP服务器提供的网关信息设置为默认网关路由。 高级选项 ： » 路由距离：指定路由距离。范围是1到255，默认值是1。 » 路由权值：指定路由权值。范围是1到255，默认值是1。 » 管理优先级：指定DNS服务器的优先级。除了静态配置的DNS服务器，系统还可以通过DHCP学到DNS服务器，因此，需要配置这些DNS服务器的优先级，当系统做DNS解析时，会按照优先级从高到底的顺序使用DNS服务器。优先级用1到255的数字表示，数字越大，优先级越高。静态配置的DNS服务器的优先级是20。
管理方式	选中该接口需要的管理方式的复选框。
逆向路由	根据需要启用或关闭逆向路由。 » 启用：强制使用逆向路由。如果找不到逆向路由，则丢弃数据包。默认情况下，接口强制使用逆向路由。

选项	说明
	» 关闭：不使用逆向路由。反向数据流到达接口后不进行逆向路由检查，原路返回（即从初始化数据包的入接口发送反向数据包）。 » 自动：优先使用逆向路由。如果能够找到逆向路由就使用逆向路由发送数据包；如果找不到逆向路由以初始化数据包的入接口作为发送反向数据包的出接口。

3. "在<属性>标签页，配置接口的属性信息。" 在第33页
4. "在<高级>标签页，配置接口的高级选项，包括接口关闭和接口监控与备份。" 在第34页
5. "在<RIP>标签页，配置接口的RIP功能。" 在第34页
6. 点击“确定”完成配置。

新建以太网子接口/集聚子接口/冗余子接口

新建太网子接口/集聚子接口/冗余子接口，请按照以下步骤进行操作：

1. 选择“网络 > 接口”，进入接口配置页面。
2. 点击“新建”下拉菜单，并选择“以太网子接口/集聚子接口/冗余子接口”，弹出相应接口对话框。

在<基本配置>标签页，配置接口的基本配置信息。

选项	说明
接口名称	指定接口名称。
描述	用户可根据需要指定接口描述信息，范围是0到63个字符。
绑定安全域	指定安全域类型。如果选择“三层安全域”、“二层安全域”或者”TAP“，则继续从“安全域”下拉菜单选择安全域的名称。如选择TAP安全域，可继续指定内网地址，使设备能够辨别内网流量，并在监控中进行展示。如选择“无绑定”，该接口将不绑定到任何安全域上。
安全域	从下拉菜单中选择安全域。
类型	根据IP类型不同进行如下的配置，包括静态IP和自动获取。
静态IP	IP地址：为接口指定IP地址。
	网络掩码：为接口指定网络掩码。
	启用DNS代理：选中该选项复选框开启接口的DNS代理功能。 » 使用DNS普通代理时，客户端收到的DNS应答来自其配置的DNS服务器，只有客户端的DNS服务器地址为设备的接口地址时，设备才承担DNS服务器功能； » 使用DNS透明代理时，不管客户端的DNS服务器地址是否为设备接口地址，其收到的DNS应答均来自设备。在DNS透明代理模式下，用户无需逐个修改客户端的DNS参数，只要通过设备的DNS配置即可控制所管理网络上的DNS服务。
	高级选项： » 管理IP：为接口指定管理IP。在文本框中输入IP地址。 » 二级IP：为接口指定二级IP。最多可以指定6个二级IP地址。
	DHCP：点击倒三角，选择“DHCP服务器”或“DHCP中继代理”进行相关配置。具体说明参见"DHCP" 在第45页。
自动获取	DHCP服务器提供的网关信息设置为默认网关路由：选中该选项复选框，系统会将DHCP服务器提供的网关信息设置为默认网关路由。
	高级选项 ：

选项	说明
	» 路由距离：指定路由距离。范围是1到255，默认值是1。 » 路由权值：指定路由权值。范围是1到255，默认值是1。 » 管理优先级：指定DNS服务器的优先级。除了静态配置的DNS服务器，系统还可以通过DHCP学到DNS服务器，因此，需要配置这些DNS服务器的优先级，当系统做DNS解析时，会按照优先级从高到底的顺序使用DNS服务器。优先级用1到255的数字表示，数字越大，优先级越高。静态配置的DNS服务器的优先级是20。
管理方式	选中该接口需要的管理方式的复选框。
逆向路由	根据需要启用或关闭逆向路由。 » 启用：强制使用逆向路由。如果找不到逆向路由，则丢弃数据包。默认情况下，接口强制使用逆向路由。 » 关闭：不使用逆向路由。反向数据流到达接口后不进行逆向路由检查，原路返回（即从初始化数据包的入接口发送反向数据包）。 » 自动：优先使用逆向路由。如果能够找到逆向路由就使用逆向路由发送数据包；如果找不到逆向路由以初始化数据包的入接口作为发送反向数据包的出接口。

3. "在<属性>标签页，配置接口的属性信息。" 在第33页
4. "在<高级>标签页，配置接口的高级选项，包括接口关闭和接口监控与备份。" 在第34页
5. "在<RIP>标签页，配置接口的RIP功能。" 在第34页
6. 点击“确定”完成配置。

编辑以太接口

编辑以太接口，请按照以下步骤进行操作：

1. 选择“网络 > 接口”，进入接口配置页面。
2. 从接口列表中选中需要编辑的以太接口，然后点击列表右上方的“编辑”按钮，弹出<Ethernet配置>对话框。

在<基本配置>标签页，配置接口的基本配置信息。

选项	说明
接口名称	指定接口名称。
描述	用户可根据需要指定接口描述信息，范围是0到63个字符。
绑定安全域	指定安全域类型。 如选择“三层安全域”、“二层安全域”或者”TAP“，则继续从“安全域”下拉菜单选择安全域的名称。如选择TAP安全域，可继续指定内网地址，使设备能够辨别内网流量，并在监控中进行展示。如选择“无绑定”，可继续为接口选择所属的集聚接口或者冗余接口：

属于	说明
集聚接口	指定接口属于某集聚接口。从“接口组”下拉菜单中选择接口所属的集聚接口。
冗余接口	指定接口属于某冗余接口。从“接口组”下拉菜单中选择接口所属的冗余接口。
无	指定接口不属于任何对象。

安全域	从下拉菜单中选择安全域。

选项	说明
类型	根据IP类型不同进行如下的配置，包括静态IP和自动获取。
静态IP	IP地址：为接口指定IP地址。 网络掩码：为接口指定网络掩码。 高级选项： » 管理IP：为接口指定管理IP。在文本框中输入IP地址。 » 二级IP：为接口指定二级IP。最多可以指定6个二级IP地址。 DHCP：点击倒三角，选择“DHCP服务器”或“DHCP中继代理”进行相关配置。具体说明参见"DHCP" 在第45页。
自动获取	DHCP服务器提供的网关信息设置为默认网关路由：选中该选项复选框，系统会将DHCP服务器提供的网关信息设置为默认网关路由。 高级选项 ： » 路由距离：指定路由距离。范围是1到255，默认值是1。 » 路由权值：指定路由权值。范围是1到255，默认值是1。 » 管理优先级：指定DNS服务器的优先级。除了静态配置的DNS服务器，系统还可以通过DHCP学到DNS服务器，因此，需要配置这些DNS服务器的优先级，当系统做DNS解析时，会按照优先级从高到底的顺序使用DNS服务器。优先级用1到255的数字表示，数字越大，优先级越高。静态配置的DNS服务器的优先级是20。
管理方式	选中该接口需要的管理方式的复选框。
逆向路由	根据需要启用或关闭逆向路由。 » 启用：强制使用逆向路由。如果找不到逆向路由，则丢弃数据包。默认情况下，接口强制使用逆向路由。 » 关闭：不使用逆向路由。反向数据流到达接口后不进行逆向路由检查，原路返回（即从初始化数据包的入接口发送反向数据包）。 » 自动：优先使用逆向路由。如果能够找到逆向路由就使用逆向路由发送数据包；如果找不到逆向路由以初始化数据包的入接口作为发送反向数据包的出接口。

3. "在<属性>标签页，配置接口的属性信息。" 在第33页
4. "在<高级>标签页，配置接口的高级选项，包括接口关闭和接口监控与备份。" 在第34页
5. "在<RIP>标签页，配置接口的RIP功能。" 在第34页
6. 点击“确定”完成配置。

注意:

» 删除集聚/冗余接口之前，必须取消其它接口与集聚/冗余接口的绑定、集聚/冗余子接口的配置、接口的IP地址配置以及接口与安全域的绑定。

» 以太网接口只可以编辑，不可以删除。

DNS

DNS为域名系统（Domain Name System）的缩写。DNS是一种组织成域层次结构的计算机和网络服务命名系统，用于TCP/IP网络，主要用来寻找Internet域名（如www.xxxx.com）并转化为IP地址（如“10.1.1.1”）以定位相应的计算机和相应服务。

系统的DNS功能如下：

- 服务器：为设备配置DNS服务器。
- 解析：为设备的DNS功能设置重试次数和响应超时时间。
- 缓存：将DNS映射项储存在缓存中，用以提高查找速度。DNS映射项可新建、编辑以及删除。

配置DNS服务器

配置DNS服务器，即配置为设备进行DNS解析时使用的服务器。指定DNS服务器，请按照以下步骤进行操作：

1. 选择“网络 > DNS”。
2. 在<DNS服务器>标签页，点击“新建”按钮，弹出<DNS服务器配置>对话框。
3. 在“服务器IP”文本框输入DNS服务器的IP地址。
4. 在“出接口”下拉菜单选择接口名称。该参数主要用于多出口DNS代理。如果仅用于设备进行DNS解析，可不选择出接口，保持默认“------”。
5. 点击“确定”按钮。

解析配置

配置DNS请求重试次数和DNS请求响应时间，请按照以下步骤进行操作：

1. 选择“网络 > DNS”，进入DNS配置页面。
2. 在<解析配置>标签页，在“重试”处指定DNS请求重试次数。当设备发送DNS请求时，如果在超时时间内得不到对方的DNS响应，设备会再次发出DNS请求。如果在指定的重试次数内（即为DNS请求重试次数）仍得不到响应，设备会向下一个DNS服务器发送DNS请求。
3. 在“超时”处指定DNS请求响应超时时间。设备向DNS服务器发送DNS请求后，会等待DNS服务器的DNS响应，如果一定时间内，仍没有响应，设备会再次发送请求。这一等待时间即为DNS请求响应超时时间。
4. 配置完成点击“应用”按钮将配置应用到系统中。

缓存

在使用DNS功能过程中，系统可以将DNS映射条目储存到缓存中以提高查找速度。系统有以下三种获得DNS映射条目的方法：

- 动态获得：来自DNS响应。
- 静态获得：手动添加DNS映射条目到缓存。
- 注册获得：设备的一些功能模块，例如NTP、AAA和地址簿等，定义的DNS主机。

用户可以通过命令添加静态DNS映射条目到缓存、查看系统的DNS映射条目以及清除DNS动态映射条目。

添加静态DNS映射条目到缓存，请按照以下步骤进行操作：

1. 选择“网络 > DNS”，进入DNS配置页面。
2. 选中<缓存>标签，点击“新建”按钮，弹出<DNS缓存配置>对话框。

选项	说明
主机名称	指定主机名称。
主IP地址	指定主机的IP地址。用户最多可为主机指定8个IP地址，如果有需要，分别将IP地址输入到下边的“第二/三/四/五/六/七/八IP地址”文本框中。

3. 点击“确定”按钮，完成配置。

DHCP

DHCP为动态主机配置协议（Dynamic Host Configuration Protocol）的缩写。DHCP能够自动为子网分配适当的IP地址以及相关网络参数，从而减少网络管理需求。同时，DHCP能够保证不会出现地址冲突，能够重新分配闲置资源。

系统支持DHCP客户端功能、DHCP服务器功能和DHCP中继代理功能。

- DHCP客户端：设备的接口可以设置成DHCP客户端，从DHCP服务器动态获得IP地址及网络参数配置。DHCP客户端配置参见"配置接口" 在第33页。
- DHCP服务器：设备的接口可以设置成DHCP服务器，通过配置的地址池，向与该接口相连的主机分配IP地址及网络参数。
- DHCP中继代理：设备的接口可以设置成DHCP中继代理，中继代理从DHCP服务器获得DHCP信息，然后将获得信息传递到与接口相连的主机。

虽然安全设备同时具有以上三种DHCP功能，但是在为安全设备配置DHCP功能时，一个接口只能配置一种功能。

配置DHCP服务器

DHCP服务器功能即设备作为DHCP服务器为子网中DHCP客户端设备分配IP地址及网络参数。配置DHCP服务器功能，请按照以下步骤进行操作：

1. 选择“网络 > DHCP”，进入DHCP配置页面。
2. 点击“新建”下拉菜单，并选择“DHCP服务器”，弹出<DHCP配置>对话框。

3. **在<基本配置>标签页对DHCP的基本属性进行配置。**

选项	说明
接口	配置开启DHCP服务器功能的接口。
网关	为客户端配置网关IP。
网络掩码	为客户端配置网络掩码。
DNS1	为客户端配置主DNS服务器。在文本框中输入服务器的IP地址。
DNS2	为客户端配置备DNS服务器。在文本框中输入服务器的IP地址。
地址池地址	配置地址池IP范围用于对外分配IP地址。配置方法如下： 1. 分别在“起始IP”和“终止IP”文本框中输入IP范围的起始IP和终止IP。 2. 点击“添加”按钮，将IP范围添加进系统并显示在下方的列表中。

选项	说明
	3. 重复以上步骤添加更多IP范围。如果需要删除IP范围，从列表中选中需要删除的IP范围的复选框，然后点击“删除”按钮。

4. 在<保留地址>标签页，配置保留地址池（保留地址池中的IP地址为地址池中的部分IP地址，作为DHCP服务器保留使用，不进行分配）。

5. 在<地址绑定>标签页，配置地址绑定。手动将IP与MAC地址绑定后，绑定的IP地址只能分配给指定的MAC地址。

6. **在<选项>标签页，对DHCP Server支持的选项进行配置。**

选项	说明
49	通过配置选项49，DHCP客户端可以获取到运行X window System Display Manager的系统的IP地址列表。 1. 在“选项”下拉菜单中，选择**49**。 2. 在“IP地址”文本框中输入运行X window System Display Manager的系统的IP地址。 3. 点击“添加”按钮。 4. 重复以上步骤添加多条IP地址。如果需要删除IP地址，从列表中选中需要删除的IP地址，然后点击“删除”按钮。

7. **在<高级配置>标签页，对DHCP服务器高级选项进行配置。**

选项	说明
域名	为DHCP客户端配置域名。
租约	指定租约时间。租约为客户端从获得IP地址开始，能够使用该IP地址的时间，租约到期后，客户端需要重新向DHCP服务器申请IP地址。客户端会在租约到达50%时向原DHCP服务器发送续租请求；客户端会在租约到达87.5%时进行广播尝试重新申请IP地址。
自动配置	配置自动配置功能。从下拉菜单中选择同一设备上开启了DHCP客户端功能的接口名称。“----”表示不使用自动配置功能。 自动配置功能在以下条件下能够起效：配置了DHCP服务器功能的设备上有另外一个接口启用了DHCP客户端功能。此时，配置了自动配置功能后，DHCP服务器（设备）如果没有配置DNS、WINS和域名，DHCP客户端（设备）会把从与自己相连的DHCP服务器上获取的DNS、WINS和域名信息下发给通过DHCP服务器（设备）获得信息的主机。但是，手工配置的DNS、WINS和域名具有高优先级。
WINS1	为客户端配主WINS服务器。在文本框中输入服务器的IP地址。
WINS2	为客户端配备WINS服务器。在文本框中输入服务器的IP地址。
SMTP服务器	为客户端配置SMTP服务器。在文本框中输入服务器的IP地址。
POP3服务器	为客户端配置POP3服务器。在文本框中输入服务器的IP地址。
新闻服务器	为客户端配置新闻服务器。在文本框中输入服务器的IP地址。
中继代理	当配有DHCP服务器功能的设备（设备1）与另一台配有DHCP中继代理功能的设备（设备2）相连，且PC需要通过设备2获得设备1的DHCP信息时，用户必须在设备1上配置中继代理IP地址和掩码，才能够成功传输DHCP信息到PC。 配置中继代理功能，在文本框中输入中继代理的IP地址和掩码，即设备2上启用中继代理功能的接口的IP地址和掩码。

8. 点击“确定”按钮，完成配置。

配置DHCP中继代理

设备可以作为DHCP中继代理，接受DHCP客户端请求，并且将请求发送到DHCP服务器，然后将从DHCP服务器获得DHCP信息再返回给DHCP客户端。

配置DHCP中继代理功能，请按照以下步骤进行操作：

1. 选择“网络 > DHCP”，进入DHCP配置页面。
2. 点击“新建”下拉菜单，并选择“DHCP中继代理”，弹出<DHCP中继代理>对话框。
3. 从“接口”下拉菜单选择应用DHCP中继代理功能的接口。
4. 在“服务器1/服务器2/服务器3”文本框中输入DHCP服务器的IP地址。
5. 配置完成，点击“确定”按钮关闭对话框并返回DHCP列表。

应用层网关

一些应用程序采用多通道数据传送，如常见的FTP，其控制通道和数据通道是分开的。在严格安全策略控制条件下的设备，就有可能对每种数据通道进行严格限制，例如只允许从内网到外网的FTP数据在知名的TCP 21号端口上进行传输，一旦FTP主动模式下，在公网上的FTP服务器试图主动连接内网主机的随机端口，设备就会进行拦截，此时FTP无法正常工作。这就要求设备足够智能以正确处理严格安全策略下合法应用的随机性。在FTP的实例中，设备通过分析FTP控制通道上传送的信息，得知服务器与客户端达成一致，服务器将主动连接客户端的某端口，设备就能临时的打开一条通道，使FTP正常工作。

系统采用最严格的NAT模式。一些VoIP应用在进行NAT穿越时，由于IP地址和端口号的改变可能导致VoIP无法正常工作，ALG技术在此时将保证NAT地址转换后，VoIP应用能够正常通信。因此，应用层网关提供以下功能：

- 在严格的安全策略规则下，利用应用层网关ALG技术，保证多通道应用程序正常的通信。
- 保证VoIP应用，在NAT模式下的正常工作，并能够根据安全策略要求，进行监控和过滤。

开启应用层网关

系统可根据每种应用分别开启ALG（应用层网关）控制功能。设备可配置以下应用的ALG控制功能： FTP、HTTP、MS-RPC、PPTP、Q.931、RAS、RSH、RTSP、SIP、SQLNetV2、SUN-RPC、TFTP、DNS和Auto。用户可以开启或者关闭应用的ALG功能，也可以指定H323协议的超时时间。

开启应用的ALG功能，按照以下步骤进行操作：

1. 点击“网络 > 应用层网关”，进入相关页面。
2. 选中需要开启ALG功能的应用所对应的复选框。

3. 如果需要修改H323的超时时间，在“H.323会话超时”文本框中输入新的超时时间。
4. 点击“确定”完成配置。

全局网络参数

全局网络参数是对整个StoneOS系统的数据流的设定，所有流经StoneOS系统的数据包（TCP和IP报文）都遵守全局网络参数的限制。

配置全局网络参数：

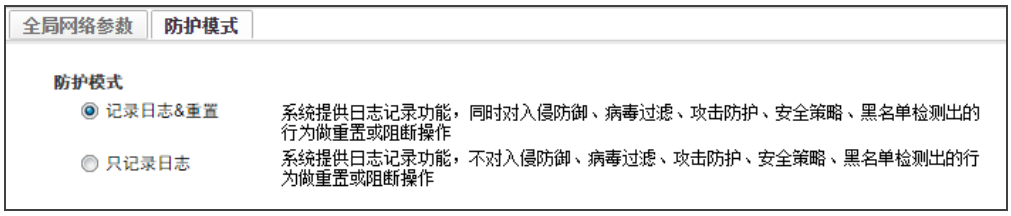
1. 点击“网络 > 全局网络参数”，进入全局网络参数的主窗口。

在主窗口设置参数。

IP分片	
最大分片数	指定系统允许的每个IP包的最大分片数（超过该分片数值的IP数据包将会被丢弃），默认值为48。取值范围是1到1024。
超时	指定分片重组超时时间（如果在指定的超时时间结束时设备仍未收到所有的分片包，数据包将会被丢弃），默认值为2秒。取值范围是1到30秒。
长效会话	指定是否启用长效会话功能。如果开启该功能，在<长效会话百分比>文本框中指定长效会话百分比，即长效会话占设备总会话数的百分比。默认值是10%。
TCP	
TCP MSS	为所有TCP SYN/ACK包指定每次传输时的最大数据分段值（MSS, Maximum Segment Size）。
MSS最大值	设定TCP包的最大数据分段值，范围是64到65535，默认MSS值为1448。
TCP包序列号检查	开启检查功能后，如果TCP序列号超出TCP窗口，该TCP包将会被丢弃。
TCP三次握手	配置是否检查TCP三次握手超时时间。选中该选项的<启用>复选框开启该功能，并在其后的<超时>文本框中指定三次握手的超时时间（如果在超时时间内，未完成三次握手，则断掉该连接），单位为秒。范围是1到1800秒，默认值是20.
TCP SYN包检查	配置TCP SYN包的检查功能。选中该选项的<启用>复选框开启该功能，此时只有检查收到的包为TCP SYN包后，才建立连接。
其他	
非IP包且非ARP包	指定系统对非IP非ARP包的处理方式，可选择丢弃或转发该数据包。

2. 点击“确定”。

3. 点击主窗口的<防护模式>标签页，选择系统中所有流量的统一处理模式。“记录日志&重置”是默认模式，该模式下，设备的所有功能正常工作；“只记录日志”模式下，设备主要用于监控和统计，不阻断任何流量。



注意: 通常情况下，请务必选择“记录日志&重置”模式，在该模式下，设备的安全功能正常生效；若选择“只记录日志”模式，系统只记录日志，对所有流量均作放行，系统中的任何阻断流量的功能全部失效，包括安全策略、IPS、AV等。

第4章 高级路由功能

路由是将数据包从一个网络转发到另一个网络中的目的地址的过程。路由器是处在两个网络之间转发数据包的设备。路由器根据路由表中储存的各种传输路径传输数据包，每一个传输路径即为一个路由条目。

设备具有三层路由功能，通过VRouter，进行路由配置，对不同的数据包进行转发。系统有一个默认VRouter，即trust-vr。

设备支持目的路由、源路由（Source-Based Routing，简称SBR）、源接口路由（Source-Interface-Based Routing，简称SIBR）、策略路由（Policy-Based Routing，简称PBR）、RIP、和等价多径路由（Equal Cost MultiPath Routing，简称ECMP）。

- "配置目的路由" 在第52页：手工定义的路由条目，根据目的地址指定下一跳。
- "配置源路由" 在第53页：根据数据包的源IP地址，选择路由，进行转发。
- "配置源接口路由" 在第54页（SIBR）：根据数据包的源IP地址和入接口，选择路由，进行转发。
- "配置策略路由" 在第55页（PBR）：根据数据包的源IP地址、目的IP地址以及服务类型，选择路由，进行转发。
- "配置RIP" 在第59页：根据RIP自动生成的动态路由表项对数据包进行路由选择并转发。
- 等价多径路由（ECMP）：到达相同目的IP地址或网段的数据流量在多条相同管理距离的路径上进行负载均衡。

当设备对进入的数据包进行转发时，按照这样的顺序选路：策略路由 > 源接口路由 > 源路由 > 目的路由/RIP。

配置目的路由

目的路由是手工定义的路由条目，根据目的地址指定下一跳。对外连接较少或者内网连接相对比较稳定的网络通常使用目的路由。用户可以根据需要确定是否添加默认路由条目。

新建目的路由

新建目的路由，请按照以下步骤进行操作：

1. 选择“网络 > 路由 > 目的路由”。
2. **点击“新建”按钮，弹出<目的路由配置>对话框。**

选项	说明
目的地	在文本框中输入路由条目的IP地址。
子网掩码	在文本框中输入路由条目的目的IP地址对应的子网掩码。
下一跳	指定下一跳类型，选择“网关”或“接口”单选按钮。 » 网关：在“网关”文本框中输入网关IP地址。 » 接口：需要在“接口”下拉菜单中选择接口名称。在“网关”文本框中输入网关IP地址。
优先权	在文本框中指定目的路由的优先级。该参数取值越小，优先级越高，而在多条路由选择的时候，优先级高的路由会被优先使用。取值范围是1到255，默认值为1。当优先级为255时，该路由无效。
路由权值	在文本框中指定目的路由的路由权值。路由权值决定负载均衡中流量转发的比重。范围是1到255，默认值是1。
描述	输入所需的目的路由描述信息。

3. 点击“确定”按钮保存所做的配置。新创建的路由条目将会显示在目的路由列表中。

配置源路由

源路由根据数据包的源IP地址，选择路由，进行转发。

新建源路由

新建源路由，请按照以下步骤进行操作：

1. 选择“网络 > 路由 > 源路由”。
2. **点击“新建”按钮，弹出<源路由配置>对话框。**

选项	说明
源IP	在文本框中输入路由条源IP地址。
子网掩码	在文本框中输入路由条目的源IP地址对应的子网掩码。
下一跳	指定下一跳类型，选择“网关”或“接口”单选按钮。 » 网关：在“网关”文本框中输入网关IP地址。 » 接口：需要在“接口”下拉菜单中选择接口名称。在“网关”文本框中输入网关IP地址。如果选中Tunnel接口时，需要在可选栏输入Tunnel对端的网关地址。
优先权	在文本框中指定目的路由的优先级。该参数取值越小，优先级越高，而在多条路由选择的时候，优先级高的路由会被优先使用。取值范围是1到255，默认值为1。当优先级为255时，该路由无效。
路由权值	在文本框中指定目的路由的路由权值。路由权值决定负载均衡中流量转发的比重。范围是1到255，默认值是1。
描述	输入所需的源路由描述信息。

3. 点击“确定”按钮保存所做的配置。新创建的路由条目将会显示在源路由列表中。

配置源接口路由

源接口路由根据数据包的源IP地址和入接口，选择路由，进行转发。

新建源接口路由

新建源接口路由，请按照以下步骤进行操作：

1. 选择“网络 > 路由 > 源接口路由”。
2. **点击“新建”按钮，弹出<源接口路由配置>对话框。**

选项	说明
入接口	从下拉菜单中选择源接口路由条目的入接口。
源IP	在文本框中输入源接口路由条目的源IP地址。
子网掩码	在文本框中输入源接口路由条目的源IP对应的子网掩码。
下一跳	指定下一跳类型，选择“网关”或“接口”单选按钮。 » 网关：在“网关”文本框中输入网关IP地址。 » 接口：需要在“接口”下拉菜单中选择接口名称。在“网关”文本框中输入网关IP地址。如果选中Tunnel接口时，需要在可选栏输入Tunnel对端的网关地址。
优先权	在文本框中指定目的路由的优先级。该参数取值越小，优先级越高，而在多条路由选择的时候，优先级高的路由会被优先使用。取值范围是1到255，默认值为1。当优先级为255时，该路由无效。
路由权值	在文本框中指定目的路由的路由权值。路由权值决定负载均衡中流量转发的比重。范围是1到255，默认值是1。
描述	输入所需的源接口路由描述信息。

3. 点击“确定”按钮保存所做的配置。新创建的路由条目将会显示在源接口路由列表中。

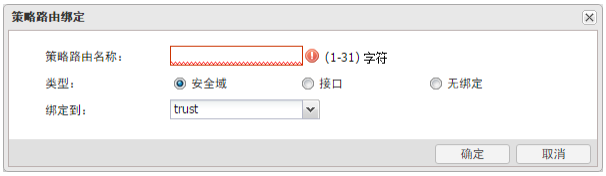
配置策略路由

用户可以配置策略路由（PBR），根据数据包的源地址、源用户、目的地址和服务选择路由并进行转发。

新建策略路由

新建策略路由，请按照以下步骤进行操作：

1. 选择“网络 > 路由 > 策略路由”。
2. **点击“新建”按钮，在下拉菜单选择“策略路由”并点击，弹出<策略路由绑定>对话框。**



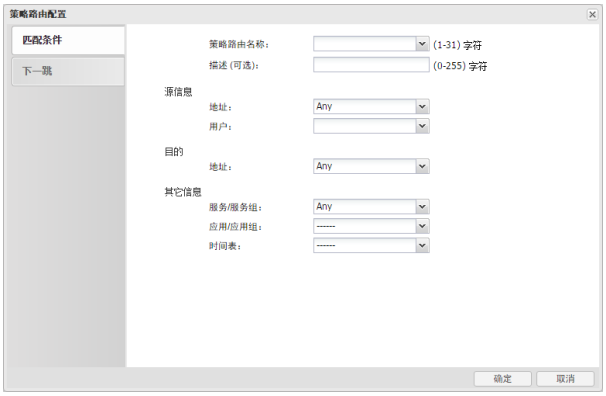
选项	说明
策略路由名称	在文本框中输入策略路由的名称。
类型	指定绑定该策略路由的类型，选择“安全域”、“接口”或者“无绑定”单选按钮。 » 安全域：在“绑定到”下拉菜单选择需要绑定该策略路由的安全域名称。 » 接口：在“绑定到”下拉菜单选择需要绑定该策略路由的接口名称。 » 无绑定：该策略路由没有被绑定。

3. 点击“确定”按钮保存所做的配置。新创建的路由条目将会显示在策略路由列表中。

新建策略路由规则

新建策略路由规则，请按照以下步骤进行操作：

1. 选择“网络 > 路由 > 策略路由”。
2. 点击“新建”按钮，在下拉菜单选择“规则”并点击，弹出<策略路由配置>对话框。



在<匹配条件>标签页，进行策略路由规则的基本配置。

选项	说明
策略路由名称	指定策略路由规则名称。
描述（可选）	指定策略路由规则的描述信息。
源信息	
地址	指定策略路由规则的源地址。 1. 在“地址”下拉菜单中选择地址类型。 2. 根据地址类型的不同，选择或输入需要的地址。 3. 点击“添加”将所选择的地址添加到列表中。 4. 添加完成后，点击<策略路由配置>对话框空白区域，即可完成源地址的选择。
用户	指定策略路由规则的角色、用户和用户组。 1. 在“用户”下拉菜单中选择类型：角色、用户组、用户。 2. 根据类型的不同，选择需要的角色/用户/用户组。 3. 点击“添加”将所选择的角色/用户/用户组添加到列表中。 4. 添加完成后，点击<策略配置>对话框空白区域，完成用户配置。
目的	
地址	指定策略路由规则的源地址。 1. 在“地址”下拉菜单中选择地址类型。 2. 根据地址类型的不同，选择或输入需要的地址。 3. 点击“添加”将所选择的地址添加到列表中。 4. 添加完成后，点击<策略路由配置>对话框空白区域，即可完成目的地址的选择。
其他信息	
服务/服务组	指定策略路由规则的服务/服务组。 1. 在“服务”下拉菜单中，用户可搜索指定服务/服务组，展开服务/服务组列表。 2. 选择指定服务/服务组后，点击 将所选择的对象添加到右侧列表中。 3. 添加完成后，点击<策略路由配置>对话框空白区域，完成配置。 如需添加新的服务/服务组，可点击“新建服务”或“新建服务组”按钮。
应用/应用组	指定策略路由规则的应用/应用组/应用过滤组。 1. 在“应用”下拉菜单中，用户可搜索指定的应用/应用组/应用过滤组，展开应用/应用组/应用过滤组列表。 2. 选择指定应用/应用组/应用过滤组组后，点击 将所选择的对象添加到右侧列表中。 3. 添加完成后，点击<策略路由配置>对话框空白区域，完成配置。 如需新建应用组或应用过滤组，点击“新建应用组”或“新建应用过滤组”按钮。
时间表	指定策略路由规则的时间表。在“时间表”下拉菜单中选择需要的时间表。

选项	说明
	如需新建时间表，点击“新建时间表”按钮。

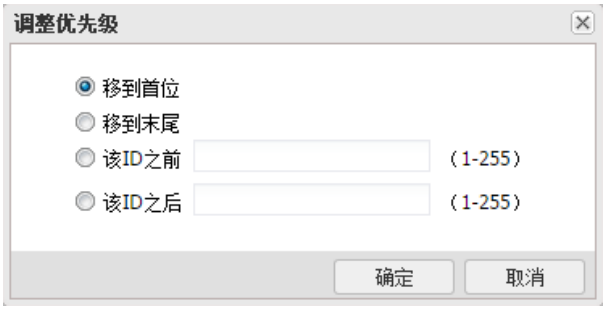
在<下一跳>标签页，进行策略路由规则的下一跳配置。

选项	说明
设置下一跳	指定下一跳类型，选择“IP地址”或“接口”单选按钮。 » IP地址：选中单选按钮指定“IP地址”类型的下一跳，并在“IP地址”文本框中输入IP地址。 » 接口：选中单选按钮指定“接口”类型的下一跳，并在“接口”下拉菜单中选择出接口。
监测对象	从下拉框中指定监控对象。详情请参见“"监测对象" 在第78页”。
路由权值	在文本框中输入下一跳的权重。如果一条策略路由匹配多个下一跳，系统会按照权重值比例分配流量。
添加	点击该按钮将配置的下一跳地址条目添加到系统。已添加的下一跳地址条目会显示在下方的列表中。
删除	选中列表中需要删除的下一跳地址条目对应的复选框，点击该按钮删除相应的下一跳地址条目。

配置策略路由规则优先级

配置策略路由规则优先级，请按照以下步骤进行操作：

1. 选择“网络 > 路由 > 策略路由”。
2. **在策略路由规则列表部分，选中需要配置优先级的路由规则对应的复选框，点击“优先级”按钮，弹出<调整优先级>对话框。**



选项	说明
移到首位	选中该单选按钮，将策略路由规则移动到所有规则的顶部。
移到末尾	选中该单选按钮，将策略路由规则移动到所有规则的底部。
该ID之前	选中该单选按钮，并在其后的文本框中输入ID，将策略路由规则移动到该ID规则之前。
该ID之后	选中该单选按钮，并在其后的文本框中输入ID，将策略路由规则移动到该ID规则之后。

注意: PBR策略中的规则通过ID进行唯一标识。流量进入设备时，设备对PBR策略规则进行顺序查找，然后按照查找到的相匹配的第一条规则对流量进行处理。但是，PBR策略规则ID的大小顺序并不是规则查找

时的匹配顺序。用户可根据需要，移动策略路由规则的位置进而调整规则的匹配顺序，使其处在首位或者处在末位，也可以位于某个ID之前或之后。

应用策略路由

可以通过绑定PBR策略到接口或者安全域来实现PBR策略的应用。

应用策略路由，请按照以下步骤进行操作：

1. 选择“网络 > 路由 > 策略路由”。
2. **点击“策略绑定”按钮，弹出<策略路由绑定>对话框。**

选项	说明
策略路由名称	从下拉菜单中选择需要绑定的策略路由条目名称。
类型	指定绑定该策略路由的类型，选择“安全域”、“接口”或者“无绑定”单选按钮。 » 安全域：在“绑定到”下拉菜单选择需要绑定该策略路由的安全域名称。 » 接口：在“绑定到”下拉菜单选择需要绑定该策略路由的接口名称。 » 无绑定：该策略路由没有被绑定。

3. 点击“确定”按钮保存所做的配置。

DNS重定向

在用户向DNS服务器发出域名请求时，系统将DNS请求重定向到指定的DNS服务器地址。如何指定DNS服务器的IP地址，请参阅"配置DNS服务器" 在第43页。

开启DNS重定向，请按照以下步骤进行操作：

1. 选择“网络 > 路由 > 策略路由”。
2. 点击“启用DNS重定向”按钮，开启该功能。

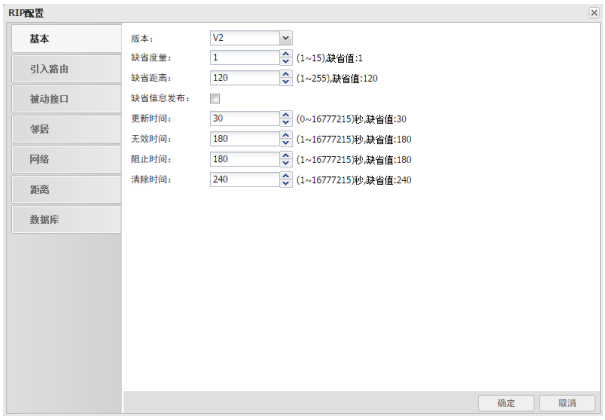
配置RIP

RIP（Routing Information Protocol）是路由信息协议。它是一种在路由器之间交换路由信息的内部网关路由协议。设备支持RIP-1和RIP-2两个版本。 对RIP协议的配置包括基本配置、引入路由、被动接口、邻居、网络和距离。另外，RIP参数配置完成后，用户还需要在不同的接口上配置RIP参数，包括指定接口接收和发送更新的RIP版本号、水平分割以及接口的RIP认证。

新建RIP

新建RIP，请按照以下步骤进行操作：

1. 选择“网络 > 路由 > RIP”。
2. 点击“新建”按钮，弹出<RIP配置>对话框。



在<基本>标签页，对RIP进行基本配置。

选项	说明
版本	指定RIP版本号。设备支持RIP-1和RIP-2两个版本，RIP-1以广播方式传输报文，而RIP-2使用组播方式。从下拉菜单中选择合适的版本号。默认为RIP-2。
缺省度量	指定缺省度量。范围是1到15，默认值是1。RIP协议使用跳数来衡量到达目的网络的距离，称为度量。路由器到与它直接相连网络的度量为1，通过一个路由器可达的网络的度量为2，依此类推，度量的最大值可以到15，度量大于15的网络为不可达网络。缺省度量在引入路由时生效。
缺省距离	指定缺省距离。范围是1到255，默认值是120。
缺省信息发布	指定是否将默认路由发布到其它使用RIP协议的路由器。默认情况下，RIP协议不发送默认路由。选中该复选框，发送默认路由。
更新时间	指定每次向所有邻居发送全部RIP路由所间隔的时间。该选项用来指定更新时间间隔值，单位为秒。默认是30秒。范围是0到16777215秒。
无效时间	如果一条路由在失效时间内一直没有被更新，该路由的度量就会被标记为16，表示为不可达路由。该选项用来指定失效时间值，单位为秒。默认的失效时间是180秒。范围是1到16777215秒。
阻止时间	如果一条更新后的路由的度量变大，例如，从2更新到4，该路由会被赋予一个阻止时间，路由在阻止时间内，不接受任何更新。该选项用来指定阻止时间值，单位为秒。默认的阻止时间是180秒。范围是1到16777215秒。
清除时间	度量被标记为16的不可达路由会一直被发布到其它RIP协议路由，直到清除时间结束；如果该路由仍没有被更新，清除时间结束后，将会被从RIP路由信息数据库中删除。该选项用来指定清除时间值，单位为秒。默认的清除时间是240秒。范围是1到16777215秒。

在<引入路由>标签页，对RIP进行引入路由配置。

选项	说明
协议	从下拉菜单中选择被引入路由的协议类型，可以是直连或静态。
度量	在文本框中输入引入路由的度量值。如果不指定该数值，系统会使用RIP实例基本配置中指定的缺省度量。
添加	点击“添加”按钮，添加已配置的引入路由条目，被添加的引入路由条目将显示在下方的再发布路由列表中。
删除	重复以上步骤添加更多引入路由条目。如果需要删除引入路由条目，从列表中选中需要删除的引入路由条目，然后点击右侧的“删除”按钮。

在<被动接口>标签页，对RIP进行被动接口配置。

选项	说明
接口	从下拉菜单中选择需要的被动接口。
添加	点击“添加”按钮，添加已配置的被动接口，被添加的被动接口将显示在下方的列表中。
删除	重复以上步骤添加更多被动接口。如果需要删除被动接口，从列表中选中需要删除的被动接口，然后点击右侧的“删除”按钮。

在<邻居>标签页，对RIP进行邻居配置。

选项	说明
邻居IP	在文本框中输入邻居的IP地址。
添加	点击“添加”按钮，添加已配置的邻居IP，被添加的邻居IP将显示在下方的列表中。
删除	重复以上步骤添加更多邻居。如果需要删除邻居IP，从列表中选中需要删除的邻居IP，然后点击右侧的“删除”按钮。

在<网络>标签页，对RIP进行网络配置。

选项	说明
网络(IP/掩码)	在文本框中输入网络的IP地址和掩码。
添加	点击“添加”按钮，添加已配置的网络，被添加的网络将显示在下方的列表中。
删除	重复以上步骤添加更多网络。如果需要删除网络，从列表中选中需要删除的网络，然后点击右侧的“删除”按钮。

在<距离>标签页，对RIP进行距离配置。

选项	说明
距离	指定网络距离，范围是1到255。该处指定的距离优先级高于RIP实例基本配置中的缺省距离。
网络(IP/掩码)	在文本框中输入网络的IP地址和掩码。
添加	点击“添加”按钮，添加已配置的网络距离，被添加的网络距离将显示在下方的列表中。
删除	重复以上步骤添加更多网络距离。如果需要删除网络距离，从列表中选中需要删除的网络距离，然后点击右侧的“删除”按钮。

在<数据库>标签页，查看RIP路由数据库。

该数据库中储存了所有可达目的网络的路由条目。

3. 点击“确定”按钮保存所做的配置。新创建的RIP路由条目将会显示在RIP路由列表中。

注意: RIP功能在设备接口上的配置包括：认证方式、发送和接收的RIP版本号以及水平分割功能。配置接口的RIP功能，请参阅"配置接口" 在第33页。

第5章 对象

本章介绍系统中需要被其它功能模块引用的对象用户的概念以及配置，包括：

- "地址簿" 在第63页：用来管理地址条目。地址条目用来配置IP地址，可被多个功能模块引用。
- "服务薄" 在第65页：用来管理服务/服务组。服务/服务组用来指定特定的服务，可被多个功能模块引用。
- "应用薄" 在第68页：用来管理应用/应用组/应用过滤组。应用/应用组/应用过滤组用来指定特定的应用，可被多个功能模块引用。
- "时间表" 在第70页：指定时间段或者时间周期，使引用时间表的功能在时间表指定时间内生效。
- "AAA服务器" 在第72页：配置设备的AAA服务器。
- "用户" 在第73页：用来管理用户。用户是指使用设备提供的功能、处于设备管理下的人或机器。
- "角色" 在第76页：用来管理角色。角色将用户和权限进行联系。
- "监测对象" 在第78页：监测指定的目标（IP地址或者主机）是否可达或者接口的链路是否连通。

地址簿

IP地址是多个功能模块配置的重要组成元素，例如策略规则、网络地址转换规则以及会话数限制等。因此，为方便引用IP地址，实现灵活配置，设备支持地址簿功能。用户可以给一个IP地址范围指定一个名称，在配置时，只需引用该名称。而地址簿就是系统中用来储存IP地址范围与其名称的对应关系的数据库。地址簿中的IP地址与名称的对应关系条目被称作地址条目。

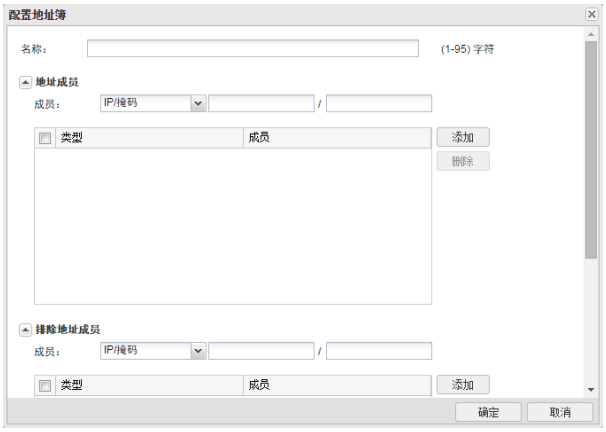
地址条目还具有以下特点：

- 地址簿中有一条默认地址条目“Any”。“Any”对应的IP地址是0.0.0.0/0，也就是代表所有IP地址。“Any”不可以编辑也不可以被删除。
- 一条地址条目中可以包含地址簿中另外的地址条目。
- 如果地址条目的IP地址范围发生了变化，系统会自动更新其它引用了该地址条目的模块。

新建地址条目

新建地址条目，请按照以下步骤进行操作：

1. 点击“策略 > 地址簿”，进入<配置地址簿>对话框。
2. 点击“新建”按钮。



在<配置地址簿>对话框，填写配置信息。

基本配置	
名称	输入地址条目的名称。
地址成员	
成员	指定地址条目成员。 可以根据需要在下拉菜单中选择“IP/掩码”、“IP范围”、“主机名称”、“地址条目”或“IP反掩码”，然后在右侧的文本框中输入相应的配置。
添加	将配置的地址成员添加到下方的地址条目成员列表中。如需要，可以多次点击“添加”按钮为地址条目添加多个地址成员。
删除	将选中的地址成员从下方的地址条目成员列表中删除。
排除地址成员	
成员	指定地址条目排除成员。 可以根据需要在下拉菜单中选择“IP/掩码”或“IP范围”，然后在右侧的文本框中输入相应的配置。 **注意：**排除地址成员需要配置在地址成员范围内，否则无法完成配置。
添加	将配置的地址条目排除成员添加到下方的地址条目排除成员列表中。如需要，可以多次点击“添加”按钮为地址条目添加多个地址条目排除成员。
删除	将选中的地址条目排除成员从下方的地址条目排除成员列表中删除。

3. 点击“确定”按钮保存所做的配置。新创建的地址条目将会显示在地址簿列表中。

查看地址条目详情

用户可以查看地址条目的详细信息，包括地址条目名称、成员、排除成员、描述以及关联项。

查看地址条目详情，请按照以下步骤进行操作：

1. 点击“策略 > 地址簿”。
2. **在地址条目列表中点击需要查看详情的地址条目名称，在地址条目列表下方区域查看详情。**

详情	
名称	查看地址条目的名称。
成员	查看地址条目中的成员。
排除成员	查看地址条目中的排除成员。
描述	查看地址条目的描述信息。
关联性	
地址	被其它地址条目引用的信息。
策略	被策略规则引用的信息。
源NAT	被源NAT规则引用的信息。
目的NAT	被目的NAT规则引用的信息。
会话限制	被会话限制规则引用的信息。
策略路由	被策略路由规则引用的信息。

服务薄

服务（Service）是具有协议标准的信息流。服务具有一定的特征，例如相应的协议、端口号等，举例来讲，FTP服务使用TCP传输协议，其目的端口号是21。服务是多个功能模块配置的重要组成元素，例如策略规则、网络地址转换规则等。

设备提供多种预定义服务、预定义服务组，同时用户也可以根据自己的需要自定义服务、自定义服务组。设备用服务簿来储存和管理这些服务和服务组。

预定义服务及预定义服务组

设备提供多种标准预定义服务，系统会根据服务的端口直接识别对应的服务类型。预定义服务组中包含相关的预定义服务，可方便用户配置。

自定义服务

除了使用系统提供的预定义服务以外，用户还可以创建自己的自定义服务。用户需指定的自定义服务条目的参数包括：

- 名称
- 传输协议
- TCP或UDP类型服务的源和目标端口号或者ICMP类型服务的type和code值
- 超时时间
- 应用类型

自定义服务组

用户将一些服务组织到一起便组成了服务组。用户可以直接将服务组应用到设备策略中，这样便简化了管理。服务组有以下特征：

- 服务簿中的每一条服务都可以被一个或多个服务组引用。
- 每个服务组中既可以包含预定义服务，也可以包含用户自定义服务。
- 服务组可以包含服务组。服务组支持8层嵌套。

服务组还有以下限制：

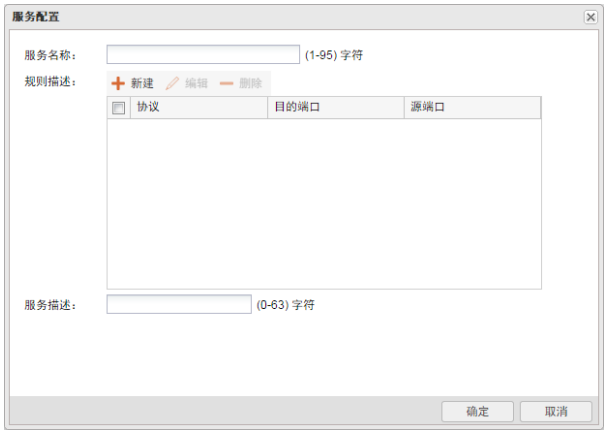
- 服务组名称与服务名称不能相同。
- 被策略引用的服务组不能被删除。如果要删除一个服务组，必须首先从其它模块中删除对该服务组的引用。
- 如果用户从服务簿中删除了一条用户自定义服务，该条服务也将会从所有引用它的服务组中被删除。

配置服务薄

本节主要介绍自定义服务和自定义服务组配置。

配置自定义服务

1. 选择“策略 > 服务簿 > 服务名称”。
2. **点击“新建”按钮，弹出<服务配置>对话框**



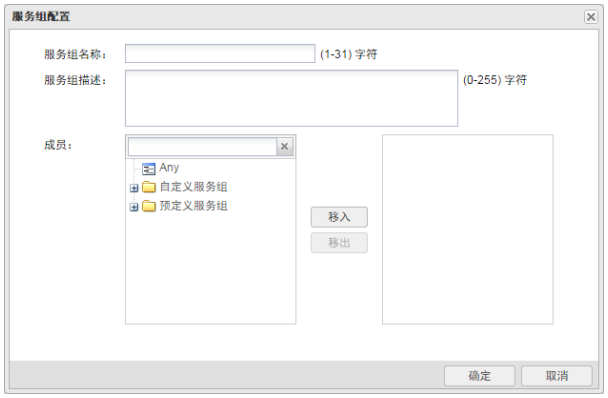
选项	说明
服务名称	输入服务的名称。
规则描述	指定所创建自定义服务的特征。点击“新建”按钮，弹出<服务规则配置>对话框，可选择的协议类型有TCP、UDP、ICMP以及其它。如需要，可添加多条服务条目。 不同类型的具体参数的配置描述如下： TCP：目的端口：“最小”指定服务条目的最小目的端口号；“最大”指定服务条目的最大目的端口号。端口号范围是0到65535，但是目的端口号不能是单一的“0” 源端口：“最小”指定服务条目的最小源端口号；“最大”指定服务条目的最大源端口号。范围是0到65535。 注意：最小端口号不能大于最大端口号。 UDP：目的端口：“最小”指定服务条目的最小目的端口号；“最大”指定服务条目的最大目的端口号。端口号范围是0到65535，但是目的端口号不能是单一的“0” 源端口：“最小”指定服务条目的最小源端口号；“最大”指定服务条目的最大源端口号。范围是0到65535。 注意：最小端口号不能大于最大端口号。 ICMP：类型：指定服务条目的ICMP type值。通过下拉菜单可以选择： » 3（Destination-Unreachable） » 4（Source Quench） » 5（Redirect） » 8（Echo）

选项	说明	
		11（Time Exceeded）
		12（Parameter Problem）
		13（Timestamp）
		15（Information）
		最小码：指定自定义服务的ICMP code最小值。范围是0-5。
		最大码：指定自定义服务的ICMP code最大值。范围是0-5。
		注意：最小端口号不能大于最大端口号。
	其他	指定服务条目的协议号。范围是1到255
服务描述	输入所需的自定义服务描述信息。	

3. 点击“确定”按钮保存所做的配置。新创建的服务将会显示在服务簿列表中。

配置自定义服务组

1. 选择“策略 > 服务簿 > 服务组”，进入服务组页面。
2. **点击“新建”按钮，弹出<服务组配置>对话框**



选项	说明
服务组名称	输入自定义服务组的名称。
服务组描述	输入所需的自定义服务组描述信息。
成员	指定服务组的成员，成员可以是自定义服务、自定义服务组、预定义服务或预定义服务组。从左侧列表中选择需要的服务或服务组，点击“移入”按钮将其添加到右侧列表，可添加多个成员。

3. 点击“确定”按钮保存所做的配置。新创建的服务组将会显示在自定义服务组列表中。

应用薄

应用具有一定的特征，例如相应的协议、端口号、应用类型等，应用是系统中多个功能模块配置的重要组成元素，例如策略规则、网络地址转换规则等。

设备提供多种预定义应用以及预定义应用组。用户也可以根据自己的需要自定义应用组。系统用应用簿来储存和管理这些应用和应用组。

编辑预定义应用

用户可以查看和使用当前版本支持的所有预定义应用并且修改预定义应用超时时间，但是不能删除预定义应用。

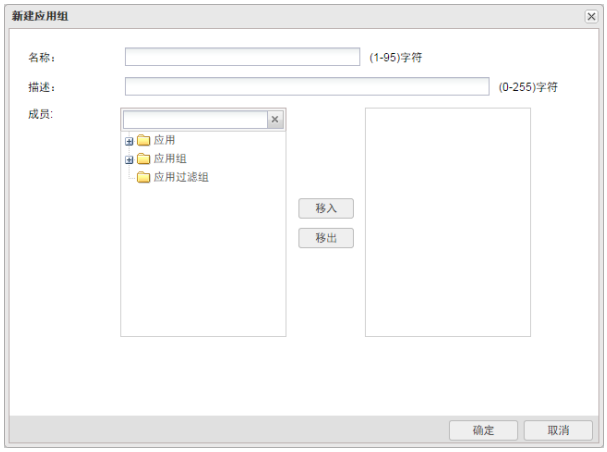
编辑预定义应用，请按照以下步骤进行操作：

1. 选择“策略 > 应用簿 > 应用”。
2. 在列表中选中需要的预定义应用复选框，点击“编辑”按钮，在弹出的“编辑应用”对话框中编辑相应的预定义应用的超时时间。

新建自定义应用组

新建自定义应用组，请按照以下步骤进行操作：

1. 选择“策略 > 应用簿 > 应用组”。
2. **点击“新建”按钮，弹出<新建应用组>对话框。**



选项	说明
名称	输入自定义用户组的名称。
描述	输入所需的自定义应用组描述信息。
成员	在“可选应用”列表选中需要的预定义应用、自定义应用组或者常用软件，点击“移入”按钮，将选中项目添加到“已选应用”列表。如需删除已选应用，选中“已选应用”列表中的应用，点击“移出”按钮，删除相应的应用。

3. 点击“确定”按钮，完成配置。

新建应用过滤组

为了细分应用种类以及简化用户重复的搜索，系统支持定义应用过滤组。用户可根据应用的类别、子类别、所用技术、风险等级、特征等条件定义应用过滤组。

新建应用过滤组，请按照以下步骤进行操作：

1. 选择“策略 > 应用簿 > 应用过滤组”。
2. 点击“新建”按钮，弹出<应用过滤组配置>对话框。

3. 在“名称”文本框中输入该应用过滤组的名字。
4. 依次在“类别”、“子类别”、“所用技术”、“风险等级”、“特征”下方对应的列表中选择所需创建的应用过滤组的过滤条件。用户可根据需要，点击“清除过滤”按钮清除所选的过滤条件。
5. 点击“确定”按钮，完成配置。

时间表

设备支持时间表（Schedule）功能。时间表功能可以使多种配置在指定的时间生效。时间表包含绝对计划和周期计划。周期计划通过周期条目指定时间表的时间点或者时间段；而绝对计划决定周期计划的生效时间。

周期计划

周期计划的时间是该周期计划中周期条目的总和。一个周期计划中最多可以添加16个条周期条目。用户可以配置三种类型的周期条目：

- 每天：每天的指定时间。例如每天的9：00到18：00。
- 每周的某几天：一周中指定天的指定时间。例如每周一、周二和周六的9：00到13：30。
- 每周一段时间：一周中的一个连续时间段。例如从周一早上9：30到周三下午15：00。

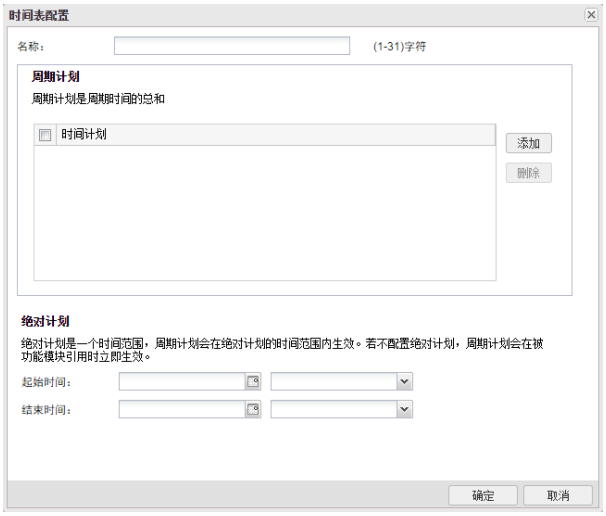
绝对计划

绝对计划是一个时间范围，指定的周期计划会在绝对计划的时间范围内生效。同时，用户也可以不启用绝对计划功能，此时周期计划会在被应用到系统中某项功能上时，立即生效。

创建时间表

新建时间表，请按照以下步骤进行操作：

1. 选择“策略> 时间表”。
2. 点击“新建”按钮，弹出<时间表配置>对话框。



在<时间表配置>对话框，配置如下信息。

角色映射配置	
名称	输入时间表的名称
周期计划	
添加	添加周期条目。
	类型：指定周期条目类型，可以为每天、每周的某几天或者每周一段时间。 - 每天：每天的指定时间。选中该单选按钮并在“每天计划任务”部分指定每天的起始时间和结束时间。

角色映射配置		
		» 每周的某几天：一周中指定天的指定时间。选中该单选按钮，在“每周计划任务”部分选择星期，在“起始时间”下拉菜单选中起始时间，在“结束时间”下拉菜单选中结束时间。 » 每周一段时间：一周中的一个连续时间段。选中该单选按钮，在“每周一段时间的计划任务”部分指定时间段的起始日期和时间以及结束日期和时间。
	预览	如需要，点击“预览” 按钮，在<预览>部分预览周期计划详情。
	确定	保存所做配置，新创建的周期条目将会显示在周期条目列表中。
删除	将选中的周期条目从周期条目列表中删除。	
绝对计划		
起始时间	指定绝对计划的起始日期和时间。	
结束时间	指定绝对计划的结束日期和时间。	

3. 点击“确定”按钮保存所做的配置。新创建的时间表将会显示在时间表列表中。

AAA服务器

AAA服务器是用来存储用户信息（包括用户名称、密码和各种属性）。设备支持本地服务器（LOCAL服务器）。本地服务器位于设备上。

配置本地AAA服务器

1. 点击“策略 > AAA服务器”。
2. 点击“新建 > 本地服务器”，弹出<本地服务器配置>对话框。

在<本地服务器配置>对话框进行配置。

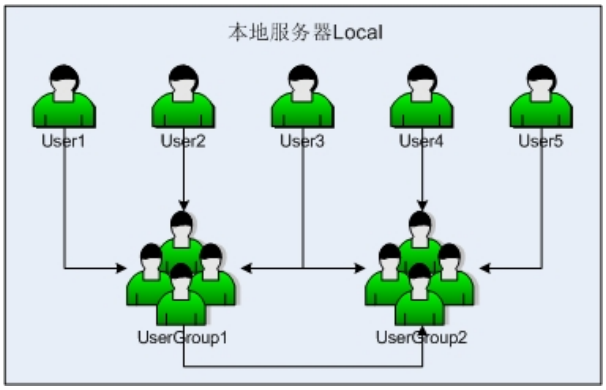
选项	说明
服务器名称	输入本地认证服务器的名称
角色映射规则	如果需要为服务器指定角色映射规则，从“角色映射规则”下拉菜单选择映射规则。指定角色映射规则后，系统将会为通过该服务器认证的用户按照指定角色映射规则分配角色。
允许用户修改密码	选中“启用”复选框允许用户自行修改密码。
备份认证服务器	为本地服务器配置备份认证服务器后，当主服务器出现问题或者用户在主服务器认证失败时，备份认证服务器发挥身份认证的作用。

3. 点击“确定”。

用户

用户（User）是指使用设备提供的功能、处于设备管理下的人或机器。用户是多个功能模块配置的重要组成元素，例如策略规则、会话数限制等。因此，为方便引用用户，实现灵活配置，设备支持用户功能。

为方便管理用户，系统支持用户组功能，属于同一本地AAA服务器的用户可以划分到不同的用户组中，并且同一个用户可以同时属于不同的用户组，属于同一个本地AAA服务器的用户组可以划分到不同的用户组中，并且同一个用户组可以同时属于不同的用户组。下图以缺省本地AAA认证服务器“Local”的用户配置说明用户以及用户组关系：



如上图所示，用户User1、User2和User3均属于用户组UserGroup1，而User3又同时属于用户组UserGroup2，UserGroup2中还包含User4、User5以及用户组UserGroup1。

新建用户

新建用户，请按照以下步骤进行操作：

1. 选择“策略> 用户 > 本地用户”。
2. 点击“新建 > 用户”，弹出<用户配置>对话框。

在<基本配置>标签页，对本地用户进行基本配置。

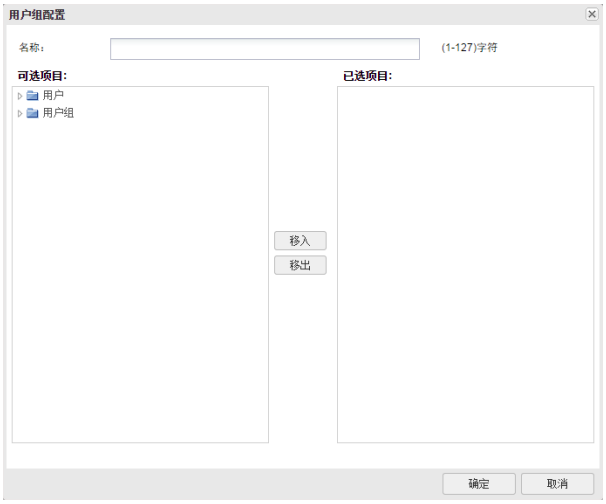
选项	说明
名称	输入用户的名称。
密码	输入用户的密码。
重新输入密码	再次输入密码以确认。
描述	输入用户描述信息。
组	把当前用户加入一个或多个用户组。点击“选择”按钮，弹出<选择用户组>对话框，从“可选项目”中选择已创建的用户组名称，点击“移入”按钮。
账户到期日	选中“启用”复选框，开启用户的有效期限制功能，并选择日期和时间。超过有效期的用户不可以通过设备的认证，因此不可以在系统中继续使用。默认情况下，用户没有有效期限制。

3. 点击“确定”按钮保存所做的配置。新创建的用户将会显示在用户列表中。

新建用户组

新建用户组，请按照以下步骤进行操作：

1. 选择“策略> 用户 > 本地用户”。
2. **点击“新建 > 用户组”，弹出<用户组配置>对话框。**



选项	说明
名称	输入用户组的名称。
移入	指定用户组所包含的用户组成员。 在“可选项目”列表中选中需要指定的用户或者用户组，点击“移入”将其添加到“已选项目”列表中。一个用户组可包含多个用户或者用户组，但是系统支持的用户组的嵌套层数最多为12层，并且不支持回环嵌套，用户组不可以再嵌套它所属的用户组。
移出	移除已指定的用户或者用户组。 在“可选项目”列表中选择用户或者用户组，点击“移出”将其从“已选项目”列表中移除。

3. 点击“确定”按钮，完成配置。

配置用户绑定

本节主要介绍添加用户绑定，导入/导出用户绑定。配置用户绑定后，设备可通过IP地址或MAC地址识别用户。

添加用户绑定

绑定IP地址或MAC地址到用户，请按照以下步骤进行操作：

1. 选择“策略> 用户 > 用户绑定”。
2. **点击“添加用户绑定”按钮，弹出<IP MAC 绑定>对话框。**

用户	
AAA服务器	指定AAA服务器名称。
用户	指定需要绑定的用户名称。
绑定类型	
绑定类型	指定所需的绑定类型，可以为IP类型或者MAC类型。 » IP：需要在“IP”文本框中输入IP地址。 » MAC：需要在“MAC”文本框中输入MAC地址。

3. 点击“确定”按钮，完成配置。

导入用户绑定列表

导入用户绑列表定到设备，请按照以下步骤进行操作：

1. 选择“策略> 用户 > 用户绑定”。
2. 点击“导入”按钮，弹出<导入用户绑定列表>对话框。
3. 点击“浏览”按钮，选择所需导入的文件。
4. 点击“确定”按钮，完成导入。

导出用户绑定列表

从设备导出用户绑列表定到设备，请按照以下步骤进行操作：

1. 选择“策略> 用户 > 用户绑定”。
2. 点击“导出”按钮，弹出导出对话框。选择保存的位置将文件保存到本地。
3. 点击“确定”按钮，完成导出。

角色

角色拥有某些特定的权限，例如某角色可以访问某指定网络资源或受到会话限制等。

在系统中，用户与权限并不直接关联，而是需要通过角色把二者联系起来。角色映射规则定义角色和用户的对应关系。在系统多个功能的配置中，可以为不同的角色指定不同的权限，由此，角色对应的用户即可受到相同权限的约束。

设备支持角色组合，即通过对角色进行“与”、“或”逻辑运算，将角色进行组合。被不同功能模块引用的角色对应的用户将是经过运算后的角色对应的用户。

设备支持以下基于角色的功能：

- 基于角色的策略规则：实现不同用户的访问控制。
- 基于角色的统计集：统计不同用户的带宽、会话。
- 基于角色的会话限制：实现对特定用户的会话数限制。
- 基于角色的策略路由：实现根据不同源用户选择路由。

新建角色

新建角色，请按照以下步骤进行操作：

1. 选择“策略> 角色 > 角色”，进入角色页面。
2. **点击“新建”按钮，弹出<角色配置>对话框**

选项	说明
角色名称	输入角色的名称。
描述	输入角色描述信息。

3. 点击“确定”按钮保存所做的配置。新创建的角色名称将会显示在角色列表中。

创建角色映射

新建角色映射规则，请按照以下步骤进行操作：

1. 选择“策略 > 角色 > 角色映射”。
2. 点击“新建”按钮，弹出<角色映射配置>对话框。

3. 在“映射名称”文本框输入角色映射规则名称。
4. 在“成员”部分的第一个下拉菜单中指定角色名称；在第二个下拉菜单中指定用户、用户组、或任意。如果选中“用户”或“用户组”，还需在后面的文本框中分别指定相应的用户名称、用户组名称。
5. 点击“添加”按钮，将角色映射条目添加到下方的角色映射条目列表中。如需要，可再添加其它角色映射条目。
6. 如需删除角色映射条目，选中角色映射条目列表中的角色映射条目复选框，点击“删除”按钮，删除相应的角色映射条目。
7. 点击“确定”按钮，完成配置。

新建角色组合

新建角色组合，请按照以下步骤进行操作：

1. 选择“策略> 角色 > 角色组合”。
2. 点击“新建”按钮，弹出<角色组合配置>对话框。

配置角色组合。

选项	说明
前缀一	选择“无前缀”或者“非”单选按钮，指定角色正则表达式中第一个角色的前缀。
角色一	从下拉菜单中选择需要的角色名称，指定角色表正则达式中第一个角色的名称。
操作符	选择“无操作符”、“与”或者“或”单选按钮，指定角色正则表达式的操作符。
前缀二	如果操作符选择“与”或者“或”单选按钮时，该选项选择“无前缀”或者“非”单选按钮，指定角色正则表达式中第二个角色的前缀。
角色二	如果操作符选择“与”或者“或”单选按钮时，该选项从下拉菜单中选择需要的角色名称，指定角色正则表达式中第二个角色的名称。
最终角色	从下拉菜单中选择需要的角色名称，指定角色正则表达式的最终角色名称。

3. 点击“确定”按钮，完成配置。

监测对象

设备的监测功能能够监测指定的目标（IP地址或者主机）是否可达或者接口的链路是否连通。监测功能用于HA以及接口监控等。

新建监测对象

新建监测对象，请按照以下步骤进行操作：

1. 选择“策略> 监测对象”。
2. 点击“新建”按钮，弹出<监测对象配置>对话框。

配置监测对象。

选项	说明
名称	指定监测对象的名称。
警戒值	指定监测对象的警戒值。
监测类型	选择检测对象的类型。可以是“接口”或者“HTTP Ping ARP DNS TCP”。一个监测对象中只能配置一种监测类型的监测条目。 选择“接口”单选按钮。 » 点击“添加”按钮，添加接口对象。 » 接口：指定被监测接口的名称。 » 权值：指定接口的权值，即该条监测失败对整个监测对象失败贡献的权重值。 选择“HTTP Ping ARP DNS TCP”单选按钮。 » 点击“添加”按钮，添加HTTP/Ping/ARP/DNS/TCP对象。 » IP/主机：通过HTTP/Ping/TCP报文对目标进行监测时，该选项用于指定监测目标的IP地址或者主机名称。 IP：通过ARP报文对目标进行监测时，该选项用于指定监测目标的IP地址。 DNS：通过DNS报文对目标进行监测时，该选项用于指定监测目标的域名。 » 权值：指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是1到255。默认值是255。

选项	说明
	» 重试次数：定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是1到255。默认值是3。 » 发送报文间隔：指定发送HTTP/Ping/ARP/DNS/TCP报文的时间间隔，单位为秒。范围是1到255秒。默认值是3秒。 » 发送报文接口：指定发送HTTP/Ping/ARP/DNS/TCP检测报文的出接口。 » 接收报文接口：指定HTTP/Ping/ARP/DNS/TCP检测报文的源接口。
HA同步	选中该选项复选框开启HA同步，主设备和备用设备信息同步。

3. 点击“确定”按钮，完成配置。

第6章 策略

策略模块提供如下功能：

- 安全策略：安全策略是网络安全设备的基本功能，控制安全域间/不同地址段间的流量转发。默认情况下，设备会拒绝所有安全域/地址段之间的信息传输。
- NAT：NAT是将IP数据包包头中的IP地址转换为另一个IP地址的协议。当IP数据包通过设备时，设备会把IP数据包的源IP地址和/或者目的IP地址进行转换。
- 会话限制：用户可以对安全域内的源IP地址、目的IP地址、指定的IP地址、服务或角色/用户/用户组进行会话数量或者建立会话速率控制，从而保护连接表不被DoS攻击填满，并且能够在一定程度上限制一些应用的带宽。
- ARP防护：ARP防护功能保护网络免受各种ARP攻击。
- URL过滤：URL过滤功能可以控制用户对某些网站的访问，并能对访问行为进行日志记录。
- 黑名单：将IP或者服务添加到黑名单后，系统将对黑名单中的IP或者服务执行阻断操作，直到阻断时间结束。

安全策略

安全策略是设备的基本功能，控制安全域间/不同地址段间的流量转发。默认情况下，设备会拒绝设备上所有安全域/地址段之间的信息传输。而安全策略则通过策略规则允许从一个（多个）安全域到另一个（多个）安全域/从一个地址段到另一个地址段的流量。

策略规则的基本元素包括：

- 流量的源安全域/源地址
- 流量的目的安全域/目的地址
- 流量的服务、应用
- 流量的用户

安全域间流量的源安全域/源地址、目的安全域/目的地址、服务、应用以及用户构成策略规则的过滤条件。策略规则都有其独有的ID号。策略规则ID会在定义规则时自动生成。所有策略规则在WebUI上按照用户设定的优先级高低从上往下排列。在流量进入系统时，系统从上到下匹配策略规则。如果匹配到规则，则根据规则进行处理。如果没有匹配到规则，则拒绝流量转发。

系统预定义多条策略规则，便于用户进行快速配置。可在安全策略页面进行进行查看。

配置策略规则

配置策略规则，按照如下步骤进行操作：

1. 点击“策略 > 安全策略”，进入安全策略页面。
2. 点击列表左上角的“添加”按钮，弹出<策略配置>对话框。

在<基本配置>标签页，填写基本配置信息。

选项	说明
名称	输入此条策略规则的名称。
源信息	
安全域	指定策略规则的源安全域。
源地址	指定策略规则的源地址。在“配置类型”选择地址类型，然后在下方选择或输入需要的地址，然后点击“添加”按钮将所选择的地址添加到下方列表中。 添加完成后，点击对话框空白区域，即可完成源地址的选择。
用户	指定策略规则的角色、用户和用户组。在“用户”下拉菜单中，选择配置类型。

选项	说明
	» 角色： 选择“角色”单选按钮，并在“角色”后的下拉菜单中选择角色名称，然后点击“添加”按钮将该角色添加到列表中。用户可根据自身需要添加多个角色，也可点击“删除”按钮将选中的角色从列表中删除。点击对话框空白区域完成为策略规则指定角色。 » 用户：选择“用户”单选按钮，并在“AAA服务器”后的下拉菜单中选择已创建的服务器、在“用户”下拉菜单中选择已创建的用户，然后点击“添加”按钮将该用户添加到列表中。可根据需要添加多个用户，也可点击“删除”按钮将选中的用户从列表中删除。点击对话框空白区域按钮完成为策略规则指定用户。 » 用户组：选择“用户组”单选按钮，并在“AAA服务器”后的下拉菜单中选择已创建的服务器、在“用户组”下拉菜单中选择已创建的用户组，然后点击“添加”按钮将该用户组添加到列表中。可根据需要添加多个用户组，也可点击“删除”按钮将选中的用户组从列表中删除。点击对话框空白区域按钮完成为策略规则指定用户组。
目的信息	
安全域	指定策略规则的目的安全域。
地址	指定策略规则的目的地址。在“配置类型”选择地址类型，然后在下方选择或输入需要的地址，然后点击“添加”按钮将所选择的地址添加到下方列表中。 添加完成后，点击对话框空白区域，即可完成目的地址的选择。
其他信息	
服务/服务组	指定策略规则的服务/服务组。在“服务/服务组”下拉菜单中选择需要的服务/服务组，然后点击  按钮将所选择的服务/服务组添加到右侧列表中。添加完成后，点击对话框空白区域，即可完成服务/服务组的选择。 如需新建服务/服务组，点击“新建服务”或“新建服务组”按钮。
应用/应用组	指定策略规则的应用/应用组/应用过滤组。在“应用/应用组”下拉菜单中选择需要的应用/应用组/应用过滤组，然后点击  按钮将所选择的项目添加到右侧列表中。添加完成后，点击对话框空白区域，即可完成应用/应用组/应用过滤组的选择。 如需新建应用组/应用过滤组，点击“新建应用组”/“新建应用过滤组”按钮。
操作	
记录日志	用户可以根据需要，通过系统日志信息记录流量对策略规则的匹配情况： » 对于允许类型的策略规则，可以记录两种情况，分别是符合策略规则的流量建立会话时生成日志信息和结束会话时生成日志信息； 选中“记录日志”后相应的复选框开启相应的日志记录功能。
列表位置	修改策略规则排列顺序。每一条策略规则都有唯一一个ID号。流量进入设备时，设备对策略规则进行顺序查找，然后按照查找到的相匹配的第一条规则对流量进行处理。但是，策略规则ID的大小顺序并不是规则查找时的匹配顺序。WebUI页面上的显示顺序才是系统策略规则的查找顺序。策略规则的排列位置可以是绝对位置，即处在首位或者处在末位，也可以是相对位置，即位于某个ID之前或之后。在“列表位置”下拉菜单中选择该策略规则的位置。
描述	添加策略的描述信息。

在<威胁防护>标签页，填写基本配置信息。

选项	说明
病毒过滤	指定病毒过滤规则。病毒过滤功能可检测最易携带病毒的文件类型和常用的协

选项	说明
	议类型并对其进行病毒防护。选择“启用”按钮并在下拉菜单中选择已创建的规则。 关于配置病毒过滤规则，请参阅"病毒过滤" 在第131页。
入侵防御	指定入侵防御规则。入侵防御功能能够实时监控和应对多种网络攻击。选择“启用按钮”并在下拉菜单中选择已创建的规则。 关于配置入侵防御规则，请参阅"入侵防御" 在第116页。

3. 点击“确定”完成配置。

启用/禁用策略规则

默认情况下，配置好的策略规则会在系统中立即生效。用户可以通过配置禁用某条策略规则，使其不对流量进行控制。

启用/禁用策略规则，按照以下步骤进行操作：

1. 点击“策略 > 安全策略”，进入安全策略页面。
2. 选中列表中需要启用/禁用的策略规则对应的复选框。
3. 点击“启用”或“禁用”按钮。

复制策略规则

复制策略规则，按照以下步骤进行操作：

1. 点击“策略 > 安全策略”，进入安全策略页面。
2. 选中列表中需要复制的策略规则对应的复选框，然后点击“复制”按钮。
3. 点击“粘贴”按钮。该策略规则将被粘贴到策略规则列表的末位。粘贴此策略规则到指定位置，点击与“粘贴”按钮相邻的倒三角，并从弹出菜单中选择指定位置。该策略规则将被粘贴到指定的位置。

调整优先级

调整策略规则的优先级，按照以下步骤进行操作：

1. 点击“策略 > 安全策略”，进入安全策略页面。
2. 从安全策略列表中选中需要调整优先级的安全策略规则对应的复选框，然后点击列表上方的“移动”按钮。
3. 在弹出下拉菜单的“移动到”文本框中，输入ID号，并点击“之前”/“之后”按钮。被选中安全策略规则将被移动至指定ID规则的前/后。

查看及清零策略命中数

设备支持策略规则匹配次数统计功能。该功能能够对系统流量与策略规则的匹配次数进行统计，即每当进入系统的流量与某条策略规则相匹配时，该策略规则的匹配次数会自动加1。

查看策略规则的命中数，进入安全策略页面。在策略规则列表的“命中数”一列，查看相应策略规则的命中数统计。

清除策略规则匹配次数统计信息，按照以下步骤进行操作：

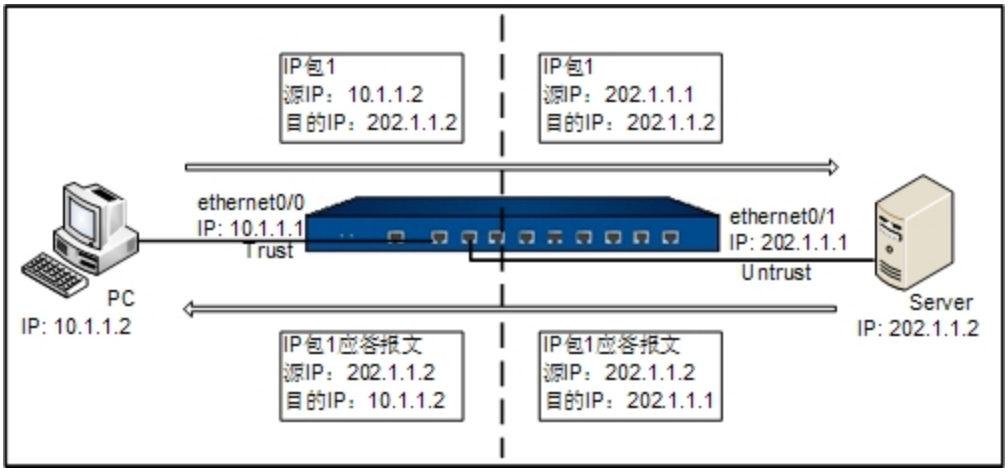
1. 点击“策略 > 安全策略”，进入安全策略页面。
2. 点击“命中数清零”按钮。系统弹出<策略命中数清零>对话框。
3. 根据需要，清除策略规则匹配次数统计信息。具体选项说明如下：
   - 所有策略：清除所有规则的匹配次数统计信息。
   - 策略ID：清除指定ID规则的匹配次数统计信息。在文本框中输入策略规则的ID。
4. 点击“确定”按钮完成配置。

NAT

网络地址转换（Network Address Translation）简称为NAT，是将IP数据包包头中的IP地址转换为另一个IP地址的协议。当IP数据包通过设备时，设备会把IP数据包的源IP地址和/或者目的IP地址进行转换。在实际应用中，NAT主要用于私有网络访问外部网络或外部网络访问私有网络的情况。

NAT的基本转换过程

设备执行NAT功能时，处于公有网络和私有网络的连接处。下图描述了NAT的基本转换过程：



如上图所示，设备处于私有网络和公有网络的连接处。当内部PC（10.1.1.2）向外部服务器（202.1.1.2）发送一个IP包时，IP包将通过设备。设备查看包头内容，发现该IP包是发向公有网络的，然后它将IP包1的源地址10.1.1.2换成一个可以在Internet上选路的公有地址202.1.1.1，并将该IP包发送到外部服务器，与此同时，设备还在网络地址转换表中记录这一映射。外部服务器给内部PC发送IP包1的应答报文（其初始目的地址为202.1.1.1），到达设备后，设备再次查看包头内容，然后查找当前网络地址转换表的记录，用内部PC的私有地址10.1.1.2替换目的地址。这个过程中，设备对PC和Server来说是透明的。对外部服务器来说，它认为内部PC的地址就是202.1.1.1，并不知道10.1.1.2这个地址。因此，NAT“隐藏”了企业的私有网络。

设备的NAT功能

设备的NAT功能将内部网络主机的IP地址和端口替换为设备外部网络的地址和端口，以及将设备的外部网络地址和端口转换为内部网络主机的IP地址和端口。也就是“私有地址+端口”与“公有地址+端口”之间的转换。

设备通过创建并执行NAT规则来实现NAT功能。NAT规则有两类，分别为源NAT规则（SNAT Rule）和目的NAT规则（DNAT Rule）。SNAT转换源IP地址，从而隐藏内部IP地址或者分享有限的IP地址；DNAT转换目的IP地址，通常是将受设备保护的内部服务器（如WWW服务器或者SMTP服务器）的IP地址转换成公网IP地址。

配置源NAT

新建源NAT规则，按照以下步骤进行操作：

1. 点击“策略 > NAT > 源NAT”，进入源NAT页面。
2. 点击“新建”按钮，弹出<源NAT配置>对话框。

在<基本配置>标签页，填写相关信息。

当IP地址符合以下条件时	
源地址	指定源NAT规则中流量的源IP地址。可选地址包括： » 地址条目：在下拉菜单中选择已配置的地址条目。 » IP地址： 在文本框中直接输入IP地址。 » IP/掩码：在文本框中输入IP地址及掩码。
目的地址	指定源NAT规则中流量的目的IP地址。可选地址包括： » 地址条目：在下拉菜单中选择已配置的地址条目。 » IP地址 - 在文本框中直接输入IP地址。 » IP/掩码 - 在文本框中输入IP地址及掩码。
出流量	指定源NAT规则的出流量。包括： » 所有流量：指定源NAT规则中出流量为所有流量。 » 出接口：指定源NAT规则中出流量的出接口，从下拉菜单中选择接口名称。
服务	指定流量的服务类型。从下拉菜单中选择服务类型。 如需新建服务/服务组，点击“新建服务”或“新建服务组”按钮。
将地址转换为	
转换为	指定将符合条件的流量转为出接口IP、指定IP或不做流量转换。 » 出接口IP：将符合条件的流量转为出接口IP地址。 » 指定IP：将符合条件的流量转为指定的IP地址。选择此选项后，在“地址”下拉菜单中选择“地址条目”，“IP地址”，或者“IP/掩码”，并指定相应的取值。 » 不转换：对符合条件的流量不做NAT转换。
模式	指定地址转换的模式。包括：

当IP地址符合以下条件时	
	» 静态： 选中该单选按钮使用静态转换模式。静态源NAT转换即一对一的转换。该模式要求被转换到的地址条目包含的IP地址数与流量的源地址的地址条目包含的IP地址数相同。 » 动态：选中该单选按钮使用动态转换模式。动态源NAT转换即多对一的转换。该模式将源地址转换到指定的IP地址。每一个源地址会被映射到一个唯一的IP地址做转换，直到指定地址全部被占用。 » 动态端口：选中该单选按钮使用动态端口转换模式。该模式即为PAT。多个源地址将被转换成指定IP地址条目中的一个地址。如果不启用Sticky功能，地址条目中的第一个地址将会首先被使用，当第一个地址的端口资源被用尽，第二个地址将会被使用。如果启用了Sticky功能，每一个源IP产生的所有会话将被映射到同一个固定的IP地址。启用Sticky功能，选中Sticky对应的“启用”复选框。选中Track对应的“启用”复选框启用该功能，并从下拉菜单选择监测对象。
其他	
描述	为此条源NAT规则输入描述信息。

在<更多配置>标签页，填写相关信息。

选项	说明
NAT日志	选中“启用”复选框开启该源NAT规则的日志功能。当有流量匹配该地址转换规则时产生日志信息。
列表位置	指定规则所在的位置。每一条源NAT规则都有唯一一个ID号。流量进入设备时，设备对源NAT规则进行顺序查找，然后按照查找到的相匹配的第一条规则对流量的源IP做NAT转换。但是，ID的大小顺序并不是规则匹配顺序。在源NAT列表中显示的顺序才是规则的匹配顺序。从下拉菜单中选择该源NAT规则在源NAT列表中所处的位置，包括： » 列表最后：配置的源NAT规则将处于所有源NAT规则的末尾。默认情况下，系统会将新创建的源NAT规则放到所有源NAT规则的末尾。 » 列表最前：配置的源NAT规则将处于所有源NAT规则的首位。 » 该ID之前：选择此选项，并在其后的文本框中输入需要的源NAT规则ID，配置的源NAT将处于指定ID源NAT规则的前一位。 » 该ID之后：选择此选项，并且在其后的文本框中输入需要的源NAT规则ID，配置的源NAT将处于指定ID源NAT规则的后一位。
ID	指定规则获得ID的方式。每一条源NAT规则都有一个唯一的ID。选中合适方式的单选按钮，可以为“自动分配ID”（系统默认）或者“手工分配ID”。当选择“手工分配ID”时，还需在后面的文本框中输入ID。

3. 点击“确定”完成配置。

启用/禁用NAT规则

默认情况下，配置好的NAT规则会在系统中立即生效。用户可以通过配置禁用某条NAT规则，使其不对流量进行控制。

启用/禁用NAT规则，按照以下步骤进行操作：

1. 点击“策略 > NAT > 源NAT”，进入源NAT页面。
2. 选中列表中需要启用/禁用的NAT规则对应的复选框。
3. 点击“启用”或“禁用”按钮。

调整优先级

每一条源NAT规则都有唯一一个ID号。流量进入设备时，设备对源NAT规则进行顺序查找，然后按照查找到的相匹配的第一条规则对流量的源IP做NAT转换。但是，ID的大小顺序并不是规则匹配顺序。在源NAT列表中显示的顺序才是规则的匹配顺序。

调整源NAT规则的优先级，按照以下步骤进行操作：

1. 点击“策略 > NAT > 源NAT”，进入源NAT页面。
2. 从源NAT列表中选中需要调整优先级的源NAT规则对应的复选框，然后点击列表上方的“优先级”按钮，弹出<调整优先级>对话框。选择相应的单选按钮，调整源NAT规则的在列表中的顺序。

选项	说明
列表最前	将该源NAT规则移至所有源NAT规则的首位。
列表最后	将该源NAT规则移至所有源NAT规则的末位。
该ID之前	将源NAT规则移至指定ID源NAT规则的前一位。在文本框中输入ID号。
该ID之后	将源NAT规则移至指定ID源NAT规则的后一位。在文本框中输入ID号。

3. 点击“确定”完成配置。

配置目的NAT

DNAT转换目的IP地址，通常是将受设备保护的内部服务器（如WWW服务器或者SMTP服务器）的IP地址转换成公网IP地址。

配置IP映射类型的目的NAT

新建IP映射类型的目的NAT，按照以下步骤进行操作：

1. 点击“策略 > NAT > 目的NAT”，进入目的NAT页面。
2. 点击“新建”按钮，并在弹出的下拉菜单中选择“IP映射”，弹出<IP映射配置>对话框。

在<IP映射配置>标签页，填写相关信息。

当IP地址符合以下条件时	
目的地址	指定流量的目的IP地址。可选地址包括： » 地址条目：在下拉菜单中选择已配置的地址条目。 » IP地址：在文本框中直接输入IP地址。 » IP/掩码：在文本框中输入IP地址及掩码。
映射	
映射到地址	指定NAT转换地址。可选择地址条目、IP地址、或IP/掩码。此处指定的NAT转换地址个数必须与流量目的IP地址的个数相同。
其他	
描述	为此条目的NAT规则输入描述信息。

3. 点击“确定”完成配置。

配置端口映射类型的目的NAT

新建端口映射类型的目的NAT规则，按照以下步骤进行操作：

1. 点击“策略 > NAT > 目的NAT”，进入目的NAT页面。

2. 点击“新建”按钮，并在弹出的下拉菜单中选择“端口映射”，弹出<端口映射配置>对话框。

在<端口映射配置>对话框，填写相关信息。

当IP地址符合以下条件时	
目的地址	指定流量的目的IP地址。可选地址包括： » 地址条目：在下拉菜单中选择已配置的地址条目。 » IP地址：在文本框中直接输入IP地址。 » IP/掩码：在文本框中输入IP地址及掩码。
服务	指定流量的服务类型。用户可搜索指定的服务，或创建新的服务或服务组。
映射	
映射到地址	指定NAT转换地址。可选择地址条目、IP地址、或IP/掩码。此处指定的NAT转换地址个数必须与流量目的IP地址的个数相同。
端口映射	在文本框中输入NAT转换的内网服务器端口号。取值范围为1到65535。
其他	
描述	为此条目的NAT规则输入描述信息。

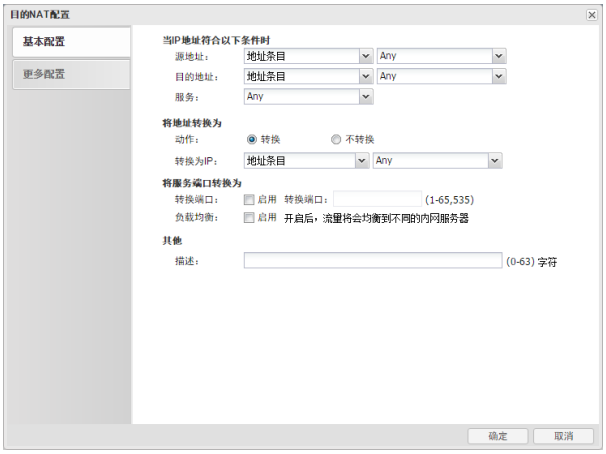
3. 点击“确定”完成配置。

配置NAT规则的高级配置

用户可新建一条NAT规则并进行相应的高级配置，也可以对已经存在的NAT规则进行高级配置。

新建目的NAT规则并进行高级配置，按照以下步骤进行操作：

1. 点击“策略 > NAT > 目的NAT”，进入目的NAT页面。
2. 点击“新建”按钮，并在弹出的下拉菜单中选择“高级配置”，弹出<目的NAT配置>对话框；对已经存在的NAT规则，选中此条规则，并点击“编辑”按钮，弹出<目的NAT配置>对话框。



在<基本配置>标签页，填写相关信息。

当IP地址符合以下条件时	
源地址	指定目的NAT规则中流量的源IP地址。可选地址包括： » 地址条目：在下拉菜单中选择已配置的地址条目。 » IP地址：在文本框中直接输入IP地址。 » IP/掩码：在文本框中输入IP地址及掩码。
目的地址	指定流量的目的IP地址。可选地址包括： » 地址条目：在下拉菜单中选择已配置的地址条目。 » IP地址：在文本框中直接输入IP地址。 » IP/掩码：在文本框中输入IP地址及掩码。
服务	指定流量的服务类型。用户可搜索指定的服务，或创建新的服务或服务组。
将地址转换为	
动作	指定对符合条件的流量所做的行为。包括： » 转换：对符合条件的流量做地址转换。 » 不转换：对符合条件的流量不做NAT转换。
转换为IP	当选择“转换”动作后，指定NAT转换地址的类型，可以为“地址条目”、“IP地址”、“IP/掩码”、或者“SLB服务器池”。选择类型后，指定相应的取值。关于SLB服务器地址池配置，参阅。
将服务端口转换为	
转换端口	选中“启用”复选框，并在“转换端口”后的文本框中输入转换后的端口号，取值范围为1到65535。
负载均衡	选中“启用”复选框开启负载均衡功能。开启负载均衡功能后，流量将会均衡到不同的内网服务器。
其他	
描述	为此条目的NAT规则输入描述信息。

在<更多配置>标签页，填写相关信息。

服务器跟踪	
Ping跟踪	选中“启用”开启Ping跟踪功能，以使设备发送Ping报文监测内网服务器是否可达。

服务器跟踪	
TCP跟踪	选中“启用”开启TCP跟踪功能，以使设备发送TCP报文监测内网服务器的TCP端口是否可达。
TCP端口	输入内网服务器端口号，
其他	
NAT日志	选中“启用”开启该目的NAT规则的日志功能（当有流量匹配该地址转换规则时产生日志信息）。
列表位置	指定规则所在的位置。每一条目的NAT规则都有唯一一个ID号。流量进入设备时，设备对目的NAT规则进行顺序查找，然后按照查找到的相匹配的第一条规则对流量的目的IP做NAT转换。但是，ID的大小顺序并不是规则匹配顺序。在目的NAT列表中显示的顺序才是规则的匹配顺序。从下拉菜单中选择该目的NAT规则在目的NAT列表中所处的位置，包括： » 列表最后：配置的目的NAT规则将处于所有目的NAT规则的末尾。默认情况下，系统会将新创建的目的NAT规则放到所有目的NAT规则的末尾。 » 列表最前：配置的目的NAT规则将处于所有目的NAT规则的首位。 » 该ID之前：从下拉菜单中选择“该ID之前”，并且在其后的文本框中输入需要的目的NAT规则ID，配置的目的NAT将处于指定ID目的NAT规则的前一位。 » 该ID之后：从下拉菜单中选择“该ID之后”，并且在其后的文本框中输入需要的目的NAT规则ID，配置的目的NAT将处于指定ID目的NAT规则的后一位。
ID	指定规则获得ID的方式。每一条目的NAT规则都有一个唯一的ID。选中合适方式的单选按钮，可以为“自动分配ID”（系统默认）或者“手工分配ID”。当选择“手工分配ID”时，还需在后面的文本框中输入ID。

3. 点击“确定”完成配置。

启用/禁用NAT规则

默认情况下，配置好的NAT规则会在系统中立即生效。用户可以通过配置禁用某条NAT规则，使其不对流量进行控制。

启用/禁用NAT规则，按照以下步骤进行操作：

1. 点击“策略 > NAT > 目的NAT”，进入目的NAT页面。
2. 选中列表中需要启用/禁用的NAT规则对应的复选框。
3. 点击“启用”或“禁用”按钮。

调整优先级

每一条目的NAT规则都有唯一一个ID号。流量进入设备时，设备对目的NAT规则进行顺序查找，然后按照查找到的相匹配的第一条规则对流量的目的IP做NAT转换。但是，ID的大小顺序并不是规则匹配顺序。在目的NAT列表中显示的顺序才是规则的匹配顺序。

调整目的NAT规则的优先级，按照以下步骤进行操作：

1. 点击“策略 > NAT > 目的NAT”，进入目的NAT页面。
2. 从目的NAT列表中选中需要调整优先级的目的NAT规则对应的复选框，然后点击列表左上方的“优先级”按钮，弹出<调整优先级>对话框。选择“列表最前”、“列表最后”、“该ID之前”或“该ID之后”单选按钮，调整目的NAT规则的在列表中的顺序。

选项	说明
列表最前	将该目的NAT规则移至所有目的NAT规则的首位。
列表最后	将该目的NAT规则移至所有目的NAT规则的末位。
该ID之前	将目的NAT规则移至指定ID目的NAT规则的前一位。在文本框中输入ID号。

选项	说明
该ID之后	将目的NAT规则移至指定ID目的NAT规则的后一位。在文本框中输入ID号。

3. 点击“确定”完成配置。

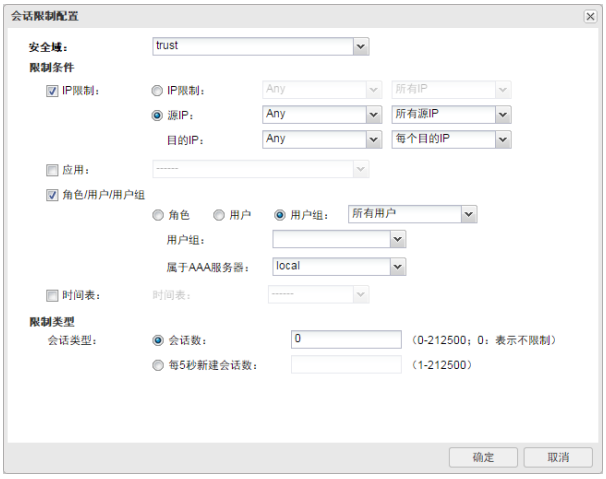
会话限制

设备支持基于安全域的会话限制功能。用户可以对安全域内的源IP地址、目的IP地址、指定的IP地址、应用或角色/用户/用户组进行会话数量或者建立会话速率控制，从而保护连接表不被DoS攻击填满，并且能够在一定程度上限制一些应用的带宽，如IM或者P2P等。

配置会话限制规则

新建会话限制规则，按照以下步骤进行操作：

1. 点击“策略 > 会话限制”，进入会话限制页面。
2. 点击会话限制列表左上方的“新建”按钮，弹出<会话限制配置>对话框。



3. 在“安全域”下拉菜单中选择配置会话限制功能的安全域。
4. **配置限制条件和时间表。限制条件可以是IP限制、应用限制、角色/用户/用户组限制。**

IP限制	
勾选“IP限制”复选框，设置IP限制条件。	
IP限制	选中该单选按钮，并选择地址条目，限制安全域中某个IP地址段的会话数。 » 在下拉菜单中选中“所有IP”，表示限制所有IP地址的最大会话数或每5秒新建会话数； » 在下拉菜单中选中“每个IP”，表示限制每个IP地址的最大会话数。
源IP	选中该单选按钮，并选择源IP的地址条目和目的IP的地址条目。当会话的源目IP地址处在地址条目的限定范围内时，系统将根据如下配置限制会话数/新建会话数： » 当在源IP对应的下拉菜单中选中“每个源IP”时，表示限制每个源IP地址的最大会话数或每5秒新建会话数； » 当在目的IP对应的下拉菜单中选中“每个目的IP”时，表示限制每个目的IP地址的最大会话数或每5秒新建会话数。
应用	
应用	勾选“应用”复选框，设置应用限制条件。在下拉菜单中选择需要限制会话的应用类型。
角色/用户/用户组	
勾选“角色/用户/用户组”复选框，设置相关限制条件。	

IP限制	
角色	选中该单选按钮，并从下拉菜单中选择角色名称，限制指定角色的会话数。
用户	选中该单选按钮，并从“用户”下拉菜单中选择用户名称，从“属于AAA服务器”下拉菜单中选择该用户所属的AAA服务器的名称，限制指定用户的会话数。
用户组	选中该单选按钮，并从“用户组”下拉菜单中选择用户组名称，从“属于AAA服务器”下拉菜单中选择该用户组所属的AAA服务器的名称，限制指定用户组会话数。 » 从下拉菜单中选中“所有用户”按钮，表示限制该用户组对应的所有用户的最大会话数或每5秒新建会话数； » 从下拉菜单中选中“每个用户”按钮，表示限制该用户组对应的每个用户的最大会话数。
时间表	
时间表	勾选“时间表”复选框，设置时间表限制条件。在下拉菜单中选择需要使用的时间表。

5. **配置限制类型，可以是会话数和每5秒新建会话数。**

会话限制	
会话数	选中该单选按钮，并在文本框中输入数值，指定最大会话数。0表示无会话数限制。
每5秒新建会话数	选中该单选按钮，指定每5秒钟可建立的最大会话数。在文本框中输入允许建立的最大会话数。

6. 点击“确定”完成配置。
7. 点击会话限制列表左上方“匹配模式配置”，选择一种匹配模式：在“同类限制取最小值”模式下，如果一个IP地址符合多条会话限制规则，那么该IP地址的最大会话数为规则中的最小值；在“同类限制取最大值”模式下，如果一个IP地址符合多条会话限制规则，那么该IP地址的最大会话数为规则中的最大值。

清除统计信息

配置会话限制功能后，超出最大会话数限制的会话将被丢弃。用户可根据需要清楚特定会话限制规则中被丢弃会话数的统计信息。

清除会话限制规则中被丢弃会话数的统计信息，按照以下步骤进行操作：

1. 点击“策略 > 会话限制”，进入会话限制页面。
2. 选择需要清楚统计信息的会话限制条目。
3. 点击“清楚”按钮，清除特定会话限制规则中被丢弃会话数的统计信息。

ARP防护

系统提供一系列功能进行ARP防护，保护网络免受各种ARP攻击。这些ARP防护功能包括：

- ARP学习：设备通过ARP学习过程获得内网中的IP-MAC的绑定信息，并将绑定信息添加到系统ARP表中。默认情况下，设备的ARP学习功能是开启的，设备会一直进行ARP学习，并将学到的IP-MAC绑定信息添加到系统ARP表中。在ARP学习过程中，如果IP或者MAC地址发生变化，设备会将更新的IP-MAC绑定信息添加到系统ARP表中。关闭ARP学习功能，只有已经在系统ARP表中的IP地址可以访问Internet。
- MAC学习：设备通过MAC学习过程获得内网中的MAC-端口绑定信息，并将其添加到系统MAC表中。默认情况下，设备的MAC学习功能是开启的，设备会一直进行MAC学习，并将学到的MAC-端口绑定信息添加到系统MAC表中。在MAC学习过程中，如果MAC地址或者端口发生变化，设备会将更新的MAC-端口绑定信息添加到MAC表中。
- IP-MAC-端口绑定：IP-MAC、MAC-端口以及IP-MAC-端口绑定后，与绑定列表中不一致的数据包将会被丢弃，保证系统免受ARP欺骗攻击或者MAC地址表攻击。结合ARP/MAC学习功能，实现“实时扫描+静态绑定”，使防护配置更加简单有效。
- ARP认证：保护客户端免受ARP欺骗攻击。
- ARP检查：系统会对通过接口的所有ARP包进行检查，将ARP包的IP地址与系统ARP表中的静态表项以及DHCP监控列表中的IP-MAC绑定表项进行对比。
- DHCP监控：DHCP监控通过分析DHCP客户端与DHCP服务器之间的DHCP报文建立DHCP客户端的MAC地址和被分配的IP地址的对应关系。
- 主机防御：设备代替不同主机发送免费ARP包，保护被代理主机免受ARP攻击。

配置ARP防护

配置ARP绑定

为加强网络安全控制，设备支持IP-MAC地址绑定、MAC-端口绑定以及IP-MAC-端口绑定。这些绑定信息分为静态和动态两种。通过ARP学习功能、ARP扫描功能以及MAC学习功能获得的绑定信息为动态绑定信息；而手工配置的绑定信息为静态信息。

配置静态绑定

添加静态IP-MAC绑定条目，按照以下步骤进行操作：

1. 点击“策略 > ARP防护”，进入ARP防护页面。
2. 在<ARP绑定>标签页，点击“新建”按钮。弹出<IP-MAC绑定配置>对话框。

在<IP-MAC绑定配置>对话框中填写绑定信息。

选项	说明
MAC	指定MAC地址。
IP	选中“启用”复选框开启IP绑定，并在后边的文本框中输入需要绑定的IP地址。
端口	选中“启用”复选框开启端口绑定，并从后边的下拉菜单选择需要绑定的端口。
MAC描述	为IP-MAC绑定条目添加描述信息。
ARP认证	选中“启用”复选框开启ARP认证功能。

3. 配置完成，点击“确定”按钮保存所做配置并返回ARP防护页面。

获取动态绑定信息

设备可以通过以下两种方式获得动态IP-MAC-端口绑定信息：

- ARP-MAC学习功能
- ARP扫描功能

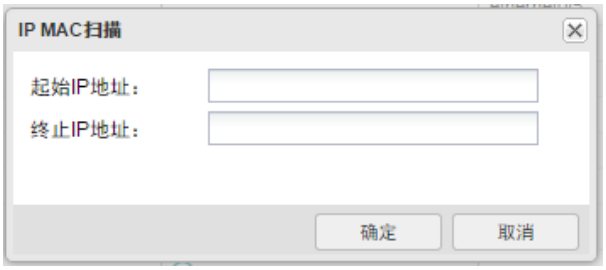
配置ARP-MAC学习功能，按照以下步骤进行操作：

1. 点击“策略 > ARP防护”，进入ARP防护页面。
2. 在<ARP绑定>标签页，点击“其他操作”按钮并在弹出菜单中选择“ARP-MAC学习配置”。弹出<ARP/MAC学习配置>对话框。

3. 选中需要开启ARP学习/MAC学习的接口。
4. 点击“启用”按钮并在弹出菜单中选择“启用ARP学习”或“启用MAC学习”。系统将开启相应接口的功能。
5. 配置完成后，关闭此对话框并返回ARP防护页面。

配置ARP扫描功能，按照以下步骤进行操作：

1. 点击“策略 > ARP防护”，进入ARP防护页面。
2. 在<ARP绑定>标签页，点击“绑定配置”按钮并在弹出菜单中选择“扫描添加IP-MAC绑定”。弹出<IP MAC扫描>对话框。



3. 分别在“起始IP地址”和“终止IP地址”文本框中输入需要扫描的IP地址范围的起始IP地址和终止IP地址。
4. 点击“确定”按钮系统开始扫描指定的IP范围，扫描结果将显示在ARP防护页面的绑定列表中。

强制绑定IP-MAC-端口绑定信息

强制绑定IP-MAC-端口绑定信息，按照以下步骤进行操作：

1. 点击“策略 > ARP防护”，进入ARP防护页面。
2. 在<ARP绑定>标签页，点击“绑定配置”按钮并在弹出菜单中选择“绑定所有配置”。弹出<绑定所有配置>对话框。
3. 选择需要绑定的信息类型。
4. 点击“确定”按钮完成配置。

解除IP-MAC-端口的强制绑定，按照以下步骤进行操作：

1. 点击“策略 > ARP防护”，进入ARP防护页面。
2. 在<ARP绑定>标签页，点击“绑定配置”按钮并在弹出菜单中选择“解除绑定配置”。弹出<解除绑定配置>对话框。

3. 选择需要解除绑定的信息类型。
4. 点击“确定”按钮完成配置。

导入/导出绑定信息

导入绑定信息，按照以下步骤进行操作：

1. 点击“策略 > ARP防护”，进入ARP防护页面。
2. 在<ARP绑定>标签页，点击“其他操作”按钮并在弹出菜单中选择“导入IP-MAC绑定”。弹出<导入>对话框。
3. 点击“浏览”按钮选择绑定信息文件（当前版本仅支持UTF-8编码文件的导入）。

导出绑定信息，按照以下步骤进行操作：

1. 点击“策略 > ARP防护”，进入ARP防护页面。
2. 在<ARP绑定>标签页，点击“其他操作”按钮并在弹出菜单中选择“导出IP-MAC绑定”。弹出<导出>对话框。
3. 选择导出信息的类型。
4. 点击“确定”按钮导出绑定信息文件。

配置ARP认证

设备提供ARP认证功能，保护客户端免受ARP欺骗攻击。ARP认证功能通过ARP客户端Hillstone Secure Defender来实现。安装Hillstone Secure Defender的PC在通过设备开启ARP认证功能的接口访问网络时，会与设备进行ARP认证，保证与PC相连的设备的MAC地址是可信的。同时，该ARP客户端还具有强大的反伪造和防重放机制，为系统防御各种ARP攻击。

注意: 由于Loopback接口不具有ARP学习功能，所以Loopback接口不支持ARP认证。

配置ARP认证功能需要在设备上开启ARP认证功能，并在PC上安装Hillstone Secure Defender程序。

在设备上开启ARP认证功能并完成相关配置，按照以下步骤进行操作：

1. 点击“策略 > ARP防护”，进入ARP防护页面。
2. 在<ARP认证>标签页，选中需要开启ARP认证的接口的复选框。
3. 点击“启用”按钮，然后在弹出菜单中选择“ARP强制认证”，开启ARP认证功能。
4. 选中需要开启强制安装客户端功能的接口的复选框。点击“启用”按钮，然后在弹出菜单中选择“强制安装客户端”。
   - 根据情况选择是否开启强制安装客户端功能。如果开启强制安装客户端，所有通过该接口访问网络的PC都需要安装ARP认证客户端Hillstone Secure Defender，否则设备将拒绝其访问网络；如果不开启强制安装客户端，ARP认证功能只对安装了客户端的PC起效。
5. 指定显示在客户端下载页面的ARP认证描述。点击“ARP认证客户端下载页”链接并在弹出对话框中输入相应的描述信息。

在PC上安装Hillstone Secure Defender，按照以下步骤进行操作：

1. 开启接口的ARP认证功能并且配置强制安装客户端。
2. PC通过该接口访问网络时，PC端会弹出Hillstone Secure Defneder的下载页面。根据提示下载客户端程序HillstoneSecureDefender.exe。
3. 下载完毕，双击HillstoneSecureDefender.exe，按照安装向导安装客户端。

配置ARP检查

设备支持接口的ARP检查功能。开启该功能后，系统会对通过接口的所有ARP包进行检查，将ARP包的IP地址与系统ARP表中的静态表项以及DHCP监控列表中的IP-MAC绑定表项进行对比：

- 如果IP地址在ARP表中，并且与表中记录的MAC地址相同，则继续转发该ARP包；
- 如果IP地址在ARP表中，但是与表中记录的MAC地址不一致，系统将丢弃该ARP包；
- 如果IP地址不在ARP表中，则继续检查该IP地址是否在DHCP监控列表中；
- 如果IP地址在DHCP监控列表中，并且与表中记录的MAC地址相同，则继续转发该ARP包；
- 如果IP地址在DHCP监控列表中，但是与表中记录的MAC地址不一致，系统将丢弃该ARP包；
- 如果IP地址不在DHCP监控列表中，则根据配置进行丢弃或者转发。

系统支持对VSwitch接口进行ARP检查功能。默认情况下，该功能是关闭的。

配置VSwitch接口的ARP检查功能，按照以下步骤进行操作：

1. 点击“策略 > ARP防护”，进入ARP防护页面。
2. 在<ARP检查>标签页，系统自动列出已经存在的VSwitch接口。
3. 双击该接口所属的条目，弹出<接口配置>对话框。

4. 在对话框中，选择<启用>复选框。
5. 选择丢弃或者转发IP地址不在ARP表中的ARP包。
6. 对于属于VSwitch的接口，如果不需要/需要进行ARP检查，则需要在<ARP检查>标签页下方的“高级配置”部分双击接口所属的条目，并在弹出的<编辑ARP速率>对话框中勾选“检查状态”部分的“不检查”/“检查”选项。
7. 如果有需要，在<编辑ARP速率>对话框中可以设置接口每秒接受ARP包的个数。当每秒钟接收ARP包的个数超过该指定值时，系统将丢弃超出的ARP包。ARP包速率取值范围是0到10000。默认值是0，即无速率限制。
8. 点击“确定”完成配置。

配置DHCP监控

DHCP为动态主机配置协议（Dynamic Host Configuration Protocol），它能够自动为子网分配适当的IP地址以及其它网络参数。DHCP监控通过分析DHCP客户端与DHCP服务器之间的DHCP报文建立DHCP客户端的MAC地址和被分配的IP地址的对应关系。在启动ARP检查功能后，将检查经过设备的ARP包是否与该表的内容匹配，如果不匹配则丢弃该ARP包。在用DHCP获取地址的网络中，可以通过启用ARP检查和DHCP监控功能来防止ARP欺骗。

由于DHCP服务的客户端是以广播的方式寻找服务器，并且只接收第一个到达的服务器提供的网络配置参数，因此，如果网络中存在非授权的DHCP服务器，就有可能引发DHCP服务器欺骗。设备可以通过在相应端口上设置丢弃DHCP响应报文来防止DHCP服务器欺骗。

另外，一些恶意攻击者通过伪造不同的MAC地址不断地向DHCP服务器发送DHCP请求，从而耗尽服务器的IP地址资源，最终导致合法用户不能获得IP地址。这种攻击也即网络上常见的DHCP Starvation Attack。设备可以通过在相应端口上设置丢弃请求报文、设置DHCP包速率限制或者打开合法性检查功能来防止该类攻击。

系统的VSwitch接口支持DHCP监控功能。默认情况下，该功能是关闭的。

配置DHCP监控功能，按照以下步骤进行操作：

1. 点击“策略 > ARP防护”，进入ARP防护页面。
2. 在<DHCP监控配置>标签页，点击“DHCP监控设置”按钮。弹出<DHCP监控配置>对话框。

3. 在<接口>标签页，选中需要开启DHCP监控功能的接口相应的复选框。
4. 点击“启用”按钮，开启接口的DHCP监控功能。
5. 在<端口>标签页，对DHCP监控参数进行配置。
   - DHCP有效性检查：检查DHCP包的客户端MAC地址与以太网包的源MAC地址是否一致，如不一致，则丢弃。选中端口后，点击“启用”按钮开启检查功能。
   - 速率：指定接口每秒钟接收DHCP包的个数。当每秒钟接收DHCP包的个数超过该指定值时，系统将丢弃超出的DHCP包。选中端口后，点击“编辑”按钮对速率限制进行限制。默认值是0，即无速率限制。
   - 丢弃：配置是否丢弃端口的指定类型数据包。选中端口后，点击“编辑”按钮进行指定。选中“DHCP请求”，系统将丢弃从客户端发送到服务器端的所有请求报文；选中“DHCP应答”，系统将丢弃从服务器端到客户端的所有响应报文。
6. 配置完成后，点击“确定”按钮保存配置。

查看DHCP监控列表

启用DHCP监控功能后，系统会对通过接口的所有DHCP包进行检查，并在此过程中建立并维护一个包含IP-MAC绑定信息的DHCP监控列表。另外，当系统的VSwitch接口以及其它三层物理接口配置为DHCP服务器时，不用开启DHCP监控功能，系统也会自动建立IP-MAC绑定信息并将它们添加到DHCP监控列表中。列表中的绑定条目包含合法用户的MAC 地址、所获IP地址、接口、端口、租约期限等信息。

打开<DHCP监控>标签页即可查看到DHCP监控列表。

配置主机防御

主机防御功能即设备代替不同主机发送免费ARP包，保护被代理主机免受ARP攻击。本节介绍主机防御功能的配置。

配置主机防御，按照以下步骤进行操作：

1. 点击“策略 > ARP防护”，进入ARP防护页面。
2. 在<主机防御>标签页，点击“新建”按钮。弹出<主机防御>对话框。

在<主机防御>对话框中填写绑定信息。

发送设置	
接口	指定发送ARP广播包的接口。
排除接口	指定排除接口，即不发送免费ARP包的接口。通常为连接被代理主机的接口。
被代理主机	
IP	指定被代理主机的IP地址。
MAC	指定被代理主机的MAC地址。
发送速率	指定设备发送免费ARP包的速率。单位为个/每秒。默认值为1个。取值范围是1到10个。

3. 配置完成点击“确定”按钮保存所做配置并返回主机防御页面。
4. 重复2到3步配置为代理更多主机发送免费ARP包。设备最多可代理16台主机发送免费ARP包。

URL过滤

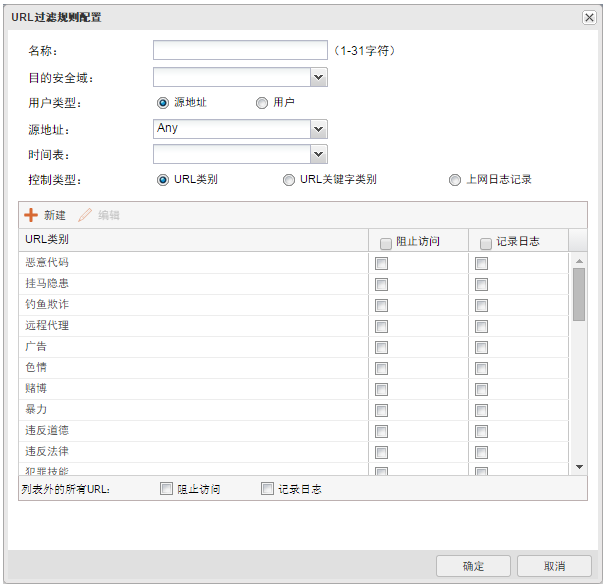
URL过滤功能可以控制用户对某些网站的访问，并能对访问行为进行日志记录。通过配置URL过滤功能，可以实现：

- 控制用户对某类网站的访问。比如，阻止用户访问赌博、色情类网站。
- 分时段控制用户对某类网站的访问。比如，阻止用户在上班时间访问在线聊天类网站，下班后则允许访问。
- 控制用户对网址中含有特定关键字的网站的访问。比如，阻止用户访问网址中含有关键字“游戏”的网站。

配置URL过滤

新建URL过滤规则，按照以下步骤进行操作：

1. 点击“策略 > URL过滤”，进入URL过滤页面。
2. 点击“新建”按钮，弹出<URL过滤规则配置>对话框。



在对话框中填写URL过滤规则的配置信息。

选项	说明
名称	输入规则名称。
目的安全域	指定规则的目的安全域。URL过滤规则将对进入此安全域的流量生效。
用户类型	指定规则的用户类型。URL过滤规则将对此类用户类型的流量生效。用户类型包括“源地址”和“用户”两类。 - “源地址”类型包括地址簿、IP/掩码、IP范围、主机名称。 - “用户”类型包括角色、用户组、用户。 系统默认使用地址簿条目Any，从而对任意IP地址生效。用户可根据需求进行调整。
源地址	“源地址”类型包括地址簿、IP/掩码、IP范围和主机名称之间的任意组合。在“配置类型”中选中需要的类型。

选项	说明
	» 如果选中“地址簿”，需要在“地址簿”下拉菜单中选中需要的地址条目； » 如果选中“IP/掩码”，需要在文本框输入IP地址和网络掩码； » 如果选中“IP范围”，需要在文本框中输入范围的起始IP； » 如果选中“主机名称”，需要在文本框中输入主机名称。输入完成后，点击“添加”按钮。
用户	“用户”类型包括角色、用户和用户组之间的任意组合。在“配置类型”中选中需要的类型。 » 如果选中“角色”，需要在“角色”下拉菜单选中需要的角色； » 如果选中“用户组”，需要在“AAA服务器”下拉菜单选中服务器并在“用户组”下拉菜单中选中用户组； » 如果选中“用户”，需要在“AAA服务器”下拉菜单选中服务器并在“用户”下拉菜单中选中用户。
时间表	指定规则的时间表，控制规则在指定时间内生效。系统默认无时间表配置，即任意时间都有效。在下拉菜单中选择所需要的时间表，或者在下拉菜单中点击“新建时间表”按钮新建时间表。
控制类型	控制类型包括URL类别、URL关键字类别、以及上网日志记录。 URL类别控制对某类网站的访问： » 新建：点击该按钮新建URL类别。关于新建URL类别的详细信息，请参阅"自定义URL库" 在第106页中的自定义URL库部分。 » 编辑：单击选中URL类别列表中的URL类别，点击该按钮，编辑相应的预定义或者自定义URL类别。 » URL类别：显示系统预定义URL类别以及用户自定义的URL类别。 » 阻止访问：选中复选框，指定阻止访问相应的URL类别。 » 记录日志：选中复选框，指定对用户的URL访问行为进行日志记录。 » 列表外的所有URL：指定对URL类别列表以外的URL进行的控制动作，包括“阻止访问”和“记录日志”。选中复选框进行指定。 URL关键字类别控制对网址中含有特定关键字的网站的访问： » 新建：点击该按钮新建关键字类别。关于新建关键字类别的详细信息，请参阅"关键字类别" 在第108页中的关键字类别部分。 » 编辑：单击选中关键字类别列表中的关键字，点击该按钮，编辑相应的关键字类别。

选项	说明
	» 关键字类别：显示系统中已有的关键字类别。 » 阻止访问：选中复选框，阻止访问网址中含有相应关键字的网站。 » 记录日志：选中复选框，对访问网址中含有相应关键字的网站的行为进行日志记录。 » 列表外的所有URL：对不包含关键字类别的网址进行的控制动作，包括“阻止访问”和“记录日志”。选中复选框进行指定。 上网日志记录对HTTP的GET及POST操作进行日志记录 » GET：记录GET方式的上网日志信息。 » POST：记录POST方式的上网日志信息。 » POST内容：记录POST内容。

3. 点击“确定”完成配置。

如果需要，用户还可以配置相关的预定义URL库、URL查询、页面提示、Bypass域名和免监控用户功能。相关功能介绍如下：

功能	介绍
预定义URL库	通过维护相应的URL库，指定关键字规则的控制范围。
URL查询	通过URL查询功能查看特定URL的具体信息，包括该URL所属的URL类别以及所属URL库的类型。
页面提示	» 用户被阻断警告：当用户的上网行为被阻断时，在用户的Web浏览器中显示访问被拒绝的警告信息。 » 用户被监控警告：当用户的上网行为被监控时，在用户的Web浏览器中显示行为被监控的警告信息
Bypass域名	设置不受上网行为控制规则控制的特殊域名。
免监控用户	设置不受上网行为控制规则控制的特殊用户。

注意:

» 为确保配置时引用最新URL类别，建议首先进行URL库更新。关于更新URL库的详细信息，请参阅"在线升级URL库" 在第106页中的在线升级URL库部分。

» 用户可以指定将日志信息输出到特定目的地。关于日志信息输出配置的详细信息，请参阅"日志管理" 在第174页。

» URL过滤规则配置后会立即生效。

启用/禁用规则

默认情况下，配置好的规则会在系统中立即生效。用户可以通过配置禁用某条规则，使其不对流量进行控制。

启用/禁用规则，按照以下步骤进行操作：

1. 点击“策略 > URL过滤”，进入URL过滤页面。
2. 选中列表中需要启用/禁用的规则对应的复选框，然后点击“启用”或“禁用”按钮。

调整优先级

流量进入设备时，设备对规则进行顺序查找，然后按照查找到的相匹配的第一条规则对流量进行处理。用户可根据需要，移动规则的位置进而调整规则的优先级，使其处在首位或者处在末位，也可以位于某个规则之前或之后。

调整URL过滤规则的优先级，按照以下步骤进行操作：

1. 点击“策略 > URL过滤”，进入URL过滤页面。
2. 点击规则列表上方的“优先级”按钮，弹出<优先级>对话框。
3. 单击选中需要移动的规则名称，点击右侧的按钮移动相应的规则。
4. 点击“确定”按钮，保存所做配置并返回上一级对话框/页面。

查看URL访问统计

URL访问统计包括以下内容：

- 概述：展示指定时间周期内前10位用户/IP访问情况、前10位URL访问情况、以及前10位URL类统计信息。
- 用户/IP：展示用户/IP以及访问次数数据。
- URL：展示URL的名称以及访问次数数据。
- URL类别：展示URL类别的名称、访问次数、以及访问流量等数据。

查看URL访问统计，参阅监控模块中的"URL访问" 在第147页部分。

- 在查看URL访问统计之前，用户需要在"监控配置" 在第155页中开启**URL访问**。
- 在查看URL类别的访问流量前，用户需要在"监控配置" 在第155页中开启**URL访问**和**URL类别流量**复选框。

查看上网日志记录

查看上网日志记录，参阅监控模块中的"URL日志" 在第173页部分。在查看上网日志记录之前，用户需要在"日志管理" 在第174页中启用URL日志。

配置URL过滤对象

对象是URL过滤功能中配置项的集合，可以供用户在配置URL过滤规则时使用。包括：

对象	说明
预定义URL库	包含数十个类别，多达上千万条URL，用于URL类别及控制范围的指定。
自定义URL库	自定义的URL库。用于URL类别及控制范围的指定。
URL查询	通过URL查询功能查看特定URL的具体信息，包括该URL所属的URL类别以及所属URL库的类型。
关键字类别	用户可以根据需要自定义关键字类别。用于URL关键字的指定。
页面提示	用户被阻断警告：当用户访问的URL被阻断时，在用户的Web浏览器中显示访问被拒绝的警告信息。 用户被监控警告：当用户被访问的URL被监控时，在用户的Web浏览器中显示行为被监控的警告信息
Bypass域名	设置不受URL过滤规则控制的特殊域名。
免监控用户	设置不受URL过滤规则控制的特殊用户。

预定义URL库

系统内置预定义URL库。

注意: 预定义URL库受许可证控制，安装许可证后，预定义URL库才可使用。

预定义URL库能够为URL过滤功能提供URL类别。预定义URL库中的URL按照中国的文化背景、伦理道德、法律法规、应用领域、上网习惯等进行分类。目前，系统预定义URL库共提供数十个类别，包含多达上千万条的URL。

对于URL类别的匹配顺序，优先匹配自定义URL库，其次匹配预定义URL库。

更改预定义URL库更新配置

默认情况下，系统会每日自动更新预定义URL库，用户可以根据需要更改数据库更新配置。目前提供两个默认数据库更新服务器，分别是update1.hillstonenet.com和update2.hillstonenet.com。系统支持在线更新和本地更新两种方式供用户进行选择。更改预定义URL库更新配置，按照以下步骤进行操作：

1. 点击“系统 > 升级管理 > 特征库升级”，进入特征库升级页面。
2. 在<URL分类库升级>部分，可查看当前分类库版本，执行远程升级，配置远程升级，以及执行本地升级。

3. 选中“启动自动更新”开启URL库自动更新功能，并配置自动更新的间隔和时间。配置完成后，点击“保存”按钮保存所做配置。
4. 点击“配置升级服务器”按钮对升级服务器进行配置。在弹出的<升级服务器设置>对话框，配置升级服务器的IP地址或者域名。如需恢复缺省设置，点击“恢复缺省”按钮。
5. 点击“确定”按钮，保存所做配置并返回上一级对话框/页面。

在线升级URL库

在线更新预定义URL数据库，按照以下步骤进行操作：

1. 点击“系统 > 升级管理 > 特征库升级”，进入特征库升级页面。
2. 在<URL分类库升级>部分，点击“立即在线升级”按钮升级URL数据库。

本地升级URL库

本地升级URL数据库，按照以下步骤进行操作：

1. 点击“系统 > 升级管理 > 特征库升级”，进入特征库升级页面。
2. 在<URL分类库升级>部分，点击“浏览”按钮，选中本地URL库分类文件并选择“打开”。
3. 点击“上传”按钮进行升级。

自定义URL库

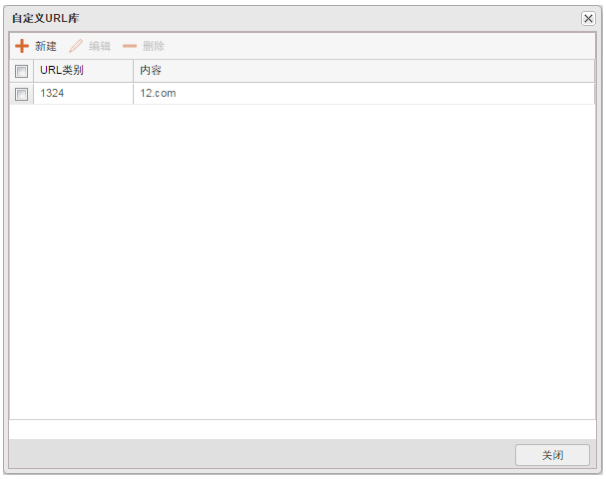
用户可以根据需要自定义URL类别。与预定义URL类别相同，自定义URL库能够为URL过滤功能提供URL类别。对于URL类别的匹配顺序，优先匹配自定义URL库，其次匹配预定义URL库。

配置自定义URL库

新建URL类别，按照以下步骤进行操作：

1. 点击“策略 > URL过滤”，进入URL过滤功能页面。
2. 在页面右上角，点击“相关配置”，并在弹出菜单中选择“自定义URL库”，弹出<自定义URL库>对话框。

3. 点击“新建”按钮，弹出<URL类别>对话框。



4. 在“类别名称”文本框中输入类别名称。URL类别名称不能只为连字符“-”且系统最多支持16个自定义URL类别。
5. 在“URL http://”文本框中输入URL。
6. 点击“添加”将URL添加进URL列表框中。
7. 如需要，按照以上步骤添加其它URL。
8. 如需要编辑已添加进URL列表框中的URL，选中该URL对应的复选框，点击“编辑”按钮，在“URL http://”文本框中对URL进行编辑，然后点击文本框后的“添加”按钮。
9. 如需要删除已添加进URL列表框中的URL，选中该URL对应的复选框，点击“删除”按钮。
10. 点击“确定”按钮，保存所做配置并返回上一级对话框/页面。

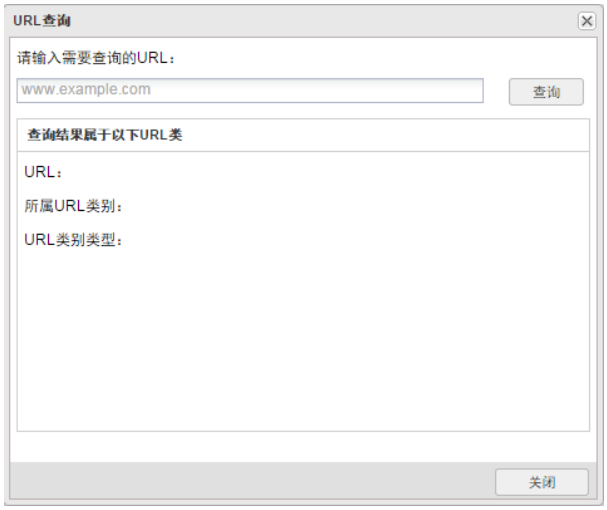
URL查询

通过URL查询功能查看特定URL的具体信息，包括该URL所属的URL类别以及所属URL库的类型。

查询URL信息

用户可以通过URL查询功能查看特定URL的具体信息，包括该URL所属的URL类别以及所属URL库的类型。查看URL信息，按照以下步骤进行操作：

1. 点击“策略 > URL过滤”，进入URL过滤功能页面。
2. 在页面右上角，点击“相关配置”，并在弹出菜单中选择“URL查询”，弹出<URL查询>对话框。



3. 在“请输入需要查询的URL”文本框输入需要查询的URL。
4. 点击“查询”按钮，查询结果会显示在下方的“查询结果属于以下URL类”部分。

配置URL查询服务器

URL查询服务器可以将网站访问过程中出现的未分类URL地址（预定义及自定义URL库中不包含的URL地址）进行分类，并在以后的URL数据库升级中更新到数据库。目前提供两个默认URL查询服务器，分别是url1.hillstonenet.com和url2.hillstonenet.com。默认情况下，URL查询服务器处于启用状态。

配置查询服务器，按照以下步骤进行操作：

1. 点击“策略 > URL过滤”，进入URL过滤功能页面。
2. 在页面右上角，点击“相关配置”，并在弹出菜单中选择“预定义URL库”，弹出<预定义URL库>对话框。
3. 在对话框中，点击“查询服务器配置”按钮，弹出<预定义URL库查询服务器配置>对话框。

4. 在“查询服务器”部分，双击指定服务器对应的“地址”栏单元格，输入需要的服务器的IP地址或者域名。
5. 双击指定服务器对应的“端口”栏单元格，输入需要的服务器的端口号。
6. 选择指定服务器的“启用”复选框，启用此服务器。
7. 点击“确定”按钮，保存所做配置并返回上一级对话框/页面。

关键字类别

用户可以根据需要自定义关键字类别。用于URL过滤中关键字的指定。

配置URL过滤规则后，系统会按照关键字对流量进行扫描，并将扫描到的关键字按照关键字类别进行信任值的统计计算，计算方法为：将扫描到的所有属于该类别的关键字按照“次数 * 关键字信任值”进行累加计算，然后用此计算值与关键字类别的警戒值进行比较（关键字类别的警戒值为100）。根据比较结果进行如下处理：

- 如果计算值大于或者等于该类别的警戒值，则触发该类别所对应的控制动作；
- 如果多个关键字类别的计算值大于或者等于警戒值，且对应控制动作有阻止的，则按照阻止进行处理；
- 如果多个关键字类别的计算值大于或者等于警戒值，且对应控制动作都为允许，则按照允许进行处理。

例如：某URL过滤规则配有两个关键字类别C1和C2，C1对应控制动作为阻止，C2对应控制动作为允许。类别C1中包含两个关键字K1和K2，K1的信任值为20，K2的信任值为40。类别C2中包含两个关键字K1和K2，K1的信任值为30，K2的信任值为80。

假设访问某URL，发现K1和K2各出现一次。对C1信任值计算：20*1+40*1=60<100；对C2信任值计算：30*1+80*1=110>100。所以触发C2对应的控制动作，即允许访问该网页。

假设访问某URL，发现K1出现三次，K2出现一次。对C1信任值计算：20*3+40*1=100；对C2信任值计算：30*3+80*1-1=170>100。C1和C2都满足触发条件，所以触发C1对应的阻止控制动作，即禁止访问该网页。

配置关键字类别

新建关键字类别，按照以下步骤进行操作：

1. 点击“策略 > URL过滤”，进入URL过滤功能页面。
2. 在页面右上角，点击“相关配置”，并在弹出菜单中选择“关键字类别”，弹出<关键字类别>对话框。
3. 在对话框中，点击“新建”按钮，弹出<关键字类别配置>对话框。

4. 在“类别名称”文本框中输入关键字类别名称。
5. 点击“新建”按钮，在滑出区域指定关键字名称、关键字类型（完全匹配/正则匹配）和信任值（默认值100）。
6. 点击“添加”按钮，将关键字添加进关键字列表。
7. 如需要，按照步骤3至6添加其它关键字。
8. 如需要删除已添加进关键字列表中的关键字，选中该关键字对应的复选框，点击列表上方的“删除”按钮。
9. 点击“确定”按钮保存所做配置并返回上一级对话框/页面。

页面提示

页面提示功能包括提示用户被阻断警告信息和提示用户被监控警告信息。

配置用户被阻断警告信息

当用户的上网行为被URL过滤功能阻断时，访问连接将无法建立。若此时用户使用Web浏览器访问网页，浏览器中将显示“无法显示页面”的错误提示信息。用户被阻断警告功能能够在用户的上网行为被阻断时，反馈给用户适当的提示信息。下图所示为默认配置：

开启用户被阻断警告功能后，当用户的下列上网行为被URL过滤规则阻断时，用户的Web浏览器中会显示阻断提示信息：

- 对某类URL的访问行为
- 对网址中含有某关键字类别的网页的访问行为

默认情况下，用户被阻断警告功能是关闭的。配置用户被阻断警告功能，按照以下步骤进行操作：

1. 点击“策略 > URL过滤”，进入URL过滤功能页面。
2. 在页面右上角，点击“相关配置”，并在弹出菜单中选择“页面提示”，弹出<页面提示>对话框。

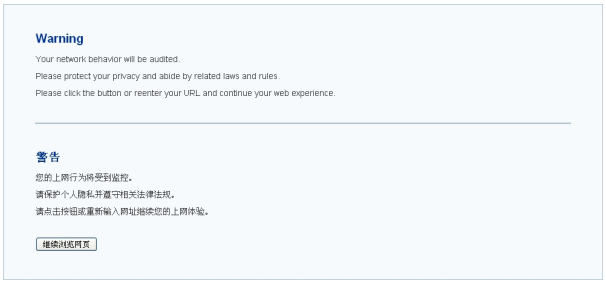
3. 选中“用户被阻断警告”对应的“启用”复选框。
4. **指定用户被阻断警告信息内容。**

选项	说明
默认配置	使用默认阻断警告信息。
重定向页面	重定向到指定的URL。在“URL”文本框中输入指定的URL。取值范围是1到255个字符。设置后，可点击“检测”测试URL的有效性。
自定义内容	需在“标题”文本框中输入自定义阻断警告信息标题，取值范围是1到31个字符；在“详细内容”文本框中输入自定义阻断警告信息详细内容，取值范围是1到255个字符。设置后，可点击“预览”按钮预览用户被阻断警告信息的显示效果。

5. 点击“确定”按钮保存所做配置并返回上一级对话框/页面。

配置用户被监控警告信息

开启用户被监控警告功能后，如果用户的上网行为与系统中已配置的URL过滤规则相匹配，则该用户的HTTP网页访问请求会被重定向到用户被监控警告提示页面，提示其上网行为将受到监控，注意保护个人隐私并遵守相关法律法规。例如，如果创建URL过滤规则对用户浏览某网页的行为进行监控，并开启用户被监控警告功能，当用户浏览该网页时，用户PC的Web浏览器将显示用户被监控警告提示页面。如图所示：



默认情况下，用户被监控警告功能是关闭的。配置用户被监控警告功能，按照以下步骤进行操作：

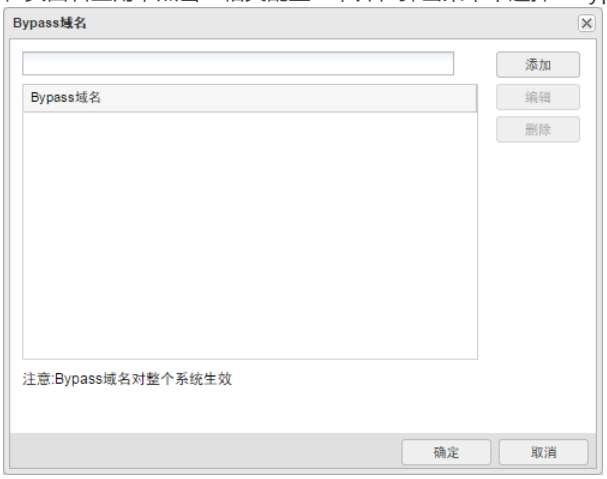
1. 点击“策略 > URL过滤”，进入URL过滤功能页面。
2. 在页面右上角，点击“相关配置”，并在弹出菜单中选择“页面提示”，弹出<页面提示>对话框。
3. 选中“用户被监控警告”对应的“启用”复选框。
4. 点击“确定”按钮保存所做配置并返回上一级对话框/页面。

Bypass域名

设置Bypass域名后，系统将无条件允许用户对Bypass域名的访问，不受URL过滤功能的控制。

配置Bypass域名，按照以下步骤进行操作：

1. 点击“策略 > URL过滤”，进入URL过滤功能页面。
2. 在页面右上角，点击“相关配置”，并在弹出菜单中选择“Bypass域名”，弹出<Bypass域名>对话框。



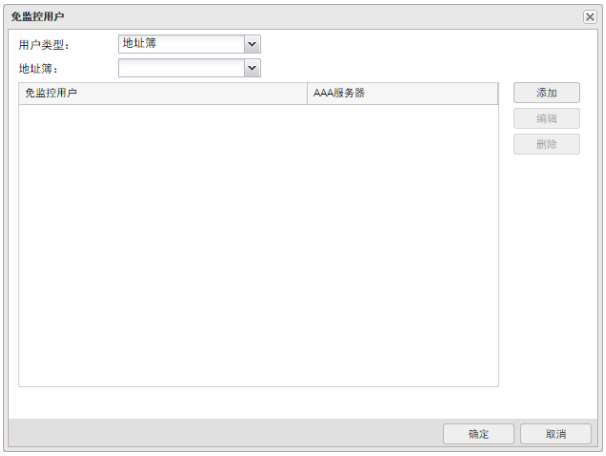
3. 在文本框中输入所需域名。
4. 点击“添加”按钮将域名添加进系统。被添加的域名将显示在下方的Bypass域名列表中。
5. 点击“确定”按钮，保存所做配置并返回上一级对话框/页面。

免监控用户

免监控用户将不受URL过滤功能的控制，比如，可以将公司领导层或者某些特殊部门设置为免监控用户。系统支持地址簿、IP地址、IP范围、用户、用户组和角色类型的免监控用户。

配置免监控用户，按照以下步骤进行操作：

1. 点击“策略 > URL过滤”，进入URL过滤功能页面。
2. 在页面右上角，点击“相关配置”，并在弹出菜单中选择“免监控用户”，弹出<免监控用户>对话框。



3. 在“用户类型”下拉菜单中选择免监控用户类型。系统支持地址簿、IP地址、IP范围、角色、用户和用户组类型的免监控用户。用户可根据需要指定，并完成相应参数的配置。
4. 点击“添加”按钮将用户添加进系统。被添加的免监控用户将显示在下方的免监控用户列表中。
5. 点击“确定”按钮，保存所做配置并返回上一级对话框/页面。

黑名单

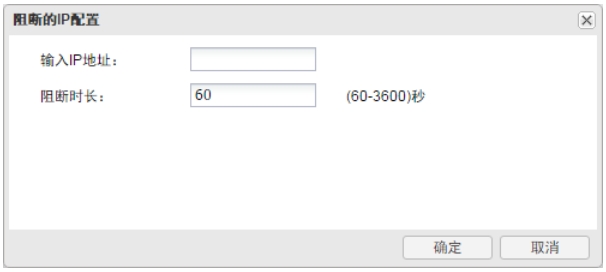
将IP或者服务添加到黑名单后，系统将对黑名单中的IP或者服务执行阻断操作，直到阻断时间结束。加入到黑名单的IP或者服务分两种，即用户手动加入和系统自动加入。系统自动加入指在功能模块（例如IPS）中配置了IP或者服务阻断的动作后，IP或者服务匹配到相关策略后被阻断，系统将自动把被阻断的IP或者服务添加到黑名单中。

黑名单配置包括IP阻断配置以及服务阻断配置。

配置IP阻断

配置IP阻断，按照以下步骤进行操作：

1. 点击“策略 > 黑名单”，进入黑名单页面。
2. 在<IP阻断>标签页，点击“新建”按钮，弹出<阻断的IP配置>对话框。



在对话框中填写配置信息。

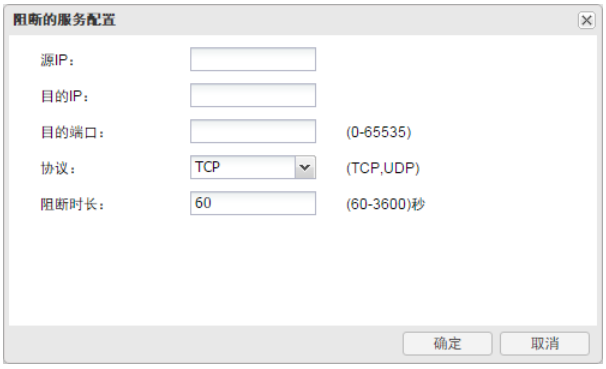
选项	说明
输入IP地址	在文本框中输入需要被阻断的IP。此IP地址既可以为发起访问的源IP地址，也可以为被访问的目的IP地址。
阻断时长	在文本框中输入IP地址将被阻断的时长，单位为秒，范围是60到3600秒。默认为60秒。

3. 点击“确定”按钮，保存所做配置并返回上一级对话框/页面。

配置服务阻断

配置服务阻断，按照以下步骤进行操作：

1. 点击“策略 > 黑名单”，进入黑名单页面。
2. 在<服务阻断>标签页，点击“新建”按钮，弹出<阻断的服务配置>对话框。



在对话框中填写配置信息。

选项	说明
源IP	指定被阻断服务的源IP。服务阻断功能将阻止从源IP访问目的IP的服务。
目的IP	指定被阻断服务的目的IP。
目的端口	指定被阻断服务的目的端口。
协议	指定被阻断服务的协议。
阻断时长	在文本框中输入IP地址将被阻断的时长，单位为秒，范围是60到3600秒。默认为60秒。

3. 点击“确定”按钮，保存所做配置并返回上一级对话框/页面。

第7章 威胁防护

威胁防护，即设备可检测并阻断网络威胁的发生。通过配置威胁防护功能，设备可防御外部威胁，减少对内网安全造成的损害。

威胁防护包括：

- 病毒过滤：可检测最易携带病毒的文件类型和常用的协议类型，并采取相应的措施处理攻击流量，保护内部网络免受攻击。
- 入侵防御：可检测针对主流应用层协议的入侵攻击、基于Web的攻击行为以及常见的木马攻击等， 并采取相应的措施处理攻击流量，保护内部网络免受攻击。
- 攻击防护：可检测多种类型的网络攻击，并采取相应的措施处理攻击流量，保护内部网络免受攻击。

设备支持基于安全域和基于策略的威胁防护配置方式。

- 攻击防护支持基于安全域的配置。安全域配置攻击防护后，系统将会对以绑定安全域为目的安全域/源安全域的流量根据配置进行检查和响应。
- 病毒过滤和入侵防御支持基于策略的配置。策略配置病毒过滤和入侵防御后，系统将会对与策略规则相匹配的流量根据配置进行检查和响应。

注意： 病毒过滤和入侵防御功能受许可证控制。安装许可证后，功能才可使用。

威胁防护特征库

威胁防护特征库包括病毒过滤特征库、入侵防御特征库。默认情况下，设备会每日自动更新威胁防护特征库，目前支持在线更新和本地更新两种方式。Hillstone提供两个默认特征库更新服务器，分别是update1.hillstonenet.com和update2.hillstonenet.com。用户可以根据需要更改特征库更新配置。

入侵防御

入侵防御功能能够实时检测多种网络攻击，可以对如下攻击类型进行防护：

- 扫描
- 网络攻击
- 拒绝服务
- 网络钓鱼
- 垃圾邮件
- 恶意软件

入侵防御功能对流量的检测包括两部分，分别是特征匹配和协议解析：

- 特征匹配：提取流量的元素，对其进行特征匹配，发现其与特征库中特征相匹配后，系统会根据配置处理流量（记录日志、重置、阻断）。此种检测在入侵防御规则的特征集部分进行配置。
- 协议解析：对流量所在协议进行分析，发现流量不符合协议的规定后，系统会根据配置处理流量（记录日志、重置、阻断）。此种检测在入侵防御规则的协议部分进行配置。

入侵防御功能的配置包括如下两部分：

- 入侵防御规则配置
- 入侵防御全局配置

入侵防御全局配置

入侵防御全局配置包括：

- 启用入侵防御功能
- 配置日志聚合类型
- 指定入侵防御工作模式

点击“策略 > 入侵防御 > 参数”进行入侵防御全局配置。配置完成后，点击“确定”按钮。

选项	说明
入侵防御	选中/取消选中“启用”复选框开启/关闭设备的入侵防御防护功能。 配置后，需要重启设备。
聚合类型	系统可将符合聚合规则（协议ID相同、特征规则ID相同、日志信息ID相同、聚合类型相同）的日志信息进行聚合，从而减少日志数量，避免日志服务器接受冗余的日志信息。系统仅支持聚合由IPS功能所产生的日志信息。该功能默认为关闭状态。在“聚合类型”下拉菜单中选择聚合类型： - ---- - 不聚合日志。 - 源IP - 将相同源IP并符合其他聚合规则的日志进行聚合。 - 目的IP - 将相同目的IP并符合其他聚合规则的日志进行聚合。 - 源IP, 目的IP - 将相同源IP、相同目的IP并符合其他聚合规则的日志进行聚合。
模式	指定系统的入侵防御工作模式，可以是： - 入侵防御 - 在该模式下，系统提供IPS日志功能，可对检出攻击做重置和阻断操作。该模式为系统默认模式。 - 只记录日志 - 在该模式下，系统提供IPS日志功能，不对检出攻击做重置和阻断操作。

配置入侵防御规则

配置入侵防御规则并将其绑定到某安全策略上，系统将对符合此安全策略的流量执行入侵防御功能。

系统预定义多个入侵防御规则，绑定到不同的预定义策略。用户可查看其具体配置，根据自身网络环境进行调整。

用户也可自行配置入侵防御规则。配置包含如下两部分：

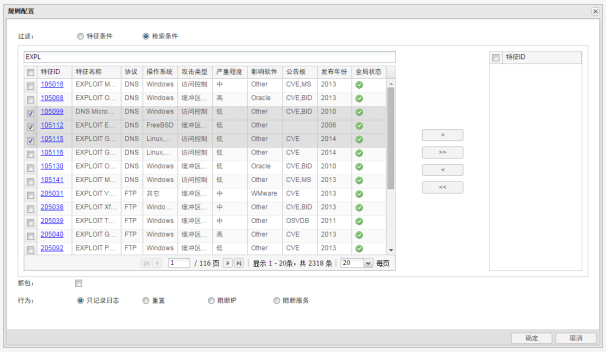
- 特征集配置
- 协议配置

配置入侵防御规则，请按照以下步骤进行：

1. 点击“策略 > 入侵防御 > 入侵防御 “。
2. 点击“新建”按钮。
3. 在“名称”文本框输入新建入侵防御规则的名称。如果只是输入名称，但是没有对特征集和协议进行配置，则该规则不生效。
4. 在“特征集”配置区域，对特征集规则进行管理，包括新建，编辑，和删除。对于存在的特征集规则，将在表格中展示特征集规则的信息。

新建特征集规则，点击“新建”按钮。

选项	说明
新建特征集规则包含如下部分: » 过滤：选择出需要使用的特征集。可通过“特征条件”和“检索条件”两种方式对特征库进行筛选与检索，从而选择出需要使用的特征集； » 抓包：对异常数据包进行抓包；对符合特征的数据包抓取后，可在威胁日志中查看。 » 行为：指定对匹配特征集的异常流量采取的行为。	
过滤	
特征条件	系统对特征从如下维度进行分类：操作系统，攻击类型，协议，严重程度，发布年份，影响软件，公告板。同一规则在某个维度上，可能属于此分类下的多个子类。比如，特征ID为105001的规则，在操作系统这个维度上，同时属于Linux, FreeBSD, Solaris, 其他Linux。  选择“特征条件”单选按钮后，系统展示如上分类，用户可通过选择各分类中的子类从而选中相关联的特征。如下图所示，在“攻击类型”分类中选择“Web攻击”子类别后，将选中与Web攻击相关联的特征。用户可点击特征ID查看特征详细信息。  选择类别及其子类别时，注意如下事项：

选项	说明
	» 同一个类别支持选择多个子类别，之间的关系为“或”。 » 不同类别之间的关系为“与”。 » 示例：在操作系统类别中选择“Windows”和“Linux”，在严重程度类别中选择“高”，则会在特征库中筛选出：既可以在Window系统中被利用也可以在Linux系统中被利用的，且严重程度为高的特征。
检索条件	用户可输入特征的信息进行检索。系统将在如下字段中进行模糊检索：特征ID，特征名称，描述信息。  检索出特征后，勾选特征，并点击 > 按钮，将特征加入右侧栏。右侧栏中添加的特征，代表此特征集规则包含的特征。 如需将左侧栏当前页中的全部规则加入右侧栏，点击 >> 按钮。 使用 < 或 << 按钮，部分取消或全部取消右侧栏的特征。
抓包	
抓包	对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。
行为	
只记录日志	系统发现攻击后仅记录日志信息。
重置	发现攻击后重置连接（TCP）或者发送目标不可达包（UDP）并且记录日志信息。
阻断IP	屏蔽攻击者的IP地址并设置屏蔽时间。取值范围为60至3600秒，默认值60秒。
阻断服务	屏蔽攻击者的服务并设置屏蔽时间。取值范围为60至3600秒，默认值60秒。
注意：用户创建多个特征集规则且这些特征集规则中包含同一个特征时，如果不同特征集规则指定的行为不一致，那么，当发现某个攻击的特征符合多个特征集规则中的同一个特征时： » 总是采取更严格的行为对攻击进行处理。哪个特征集规则设置的行为更严格，则使用哪个特征集规则设置的行为对攻击进行处理。严格程度：阻断IP > 阻断服务 > 重置 > 只记录日志。对于阻断IP和阻断服务，如果在一个特征集规则中的配置为阻断IP15s，另外一个特征集规则中的配置为阻断服务30s，则，采取的行为时阻断IP30s。 » 只要一个特征集规则中配置了抓包，就会对异常数据包进行抓包。	

选项	说明
»	通过检索条件创建的特征集规则所配置的行为，优先级高于通过特征条件创建的特征集规则所配置的行为。

5. 在“协议配置”部分，点击 进行配置。协议配置用来指定流量所在协议需要满足的规定，当流量不符合协议的规定后，系统会根据配置对流量进行处理。支持对HTTP， DNS，FTP， MSRPC， POP3，SMTP，SUNRPC，和Telnet进行配置。

在HTTP标签页，选择<协议>标签，对HTTP协议进行配置。

选项	说明
HTTP	**扫描最大长度**：对HTTP协议报文进行扫描时，扫描的最大长度。 **协议异常检查**：对HTTP协议报文进行分析，查看协议是否存在异常。对于异常报文，可以进行抓包，并指定动作进行处理： » 抓包：对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 行为：只记录日志 - 系统发现攻击后仅记录日志信息；重置 - 发现攻击后重置连接（TCP）或者发送目标不可达包（UDP）并且记录日志信息；阻断IP - 屏蔽攻击者的IP地址并设置屏蔽时间；阻断服务 - 屏蔽攻击者的服务并设置屏蔽时间。 **Banner防护**：开启HTTP服务器banner信息保护功能。 » Banner信息：开启Banner防护功能后，在该文本框中输入新信息替换原有服务器banner信息。 **URI最大长度**：指定允许的HTTP协议URI的最大长度。 对超出限定范围的报文，可以进行抓包，并指定动作进行处理： » 抓包：对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 行为：只记录日志；重置 ；阻断IP；阻断服务。 **允许HTTP方法**：指定允许的HTTP方法。

如果需要对Web服务器进行防护，在HTTP标签页，选择<WebServer>标签。

防护Web服务器包括对如下攻击行为的检测与防护：SQL注入攻击、XSS注入攻击、外链攻击、访问控制、CC攻击。系统预定义一个名称为“default”的默认Web服务器防护规则，默认Web服务器防护规则缺省为开启状态，且不能被禁用和删除。

在<Web服务器配置>对话框中新建Web服务器防护规则并对其进行防护配置。

选项	说明
Web服务器名称	输入规则名称。
域名设置	指定防护规则保护的域名。 点击“域名设置”链接，弹出<域名设置>对话框，在该对话框中输入域名。最多允许配置5个域名。访问这些域名的流量将会通过Web服务器防护规则的检查。 Web服务器域名遵循从后往前的最长匹配原则，例如，配置Web服务器防护规则rule1和防护规则rule2，且rule1中域名设置为abc.com，rule2中域名设置为email.abc.com。完成配置后，访问news.abc.com的流量将匹配rule1；访问www.email.abc.com的流量将匹配rule2；访问www.abc.com.cn的流量将匹配默认防护规则default。
SQL注入检查	选中“启用”复选框开启Web服务器SQL注入检查功能。 » 抓包： 对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。

选项	说明
	» 行为：只记录日志 - 系统发现攻击后仅记录日志信息；重置 - 发现攻击后重置连接（TCP）或者发送目标不可达包（UDP）并且记录日志信息；阻断IP - 屏蔽攻击者的IP地址并设置屏蔽时间；阻断服务 - 屏蔽攻击者的服务并设置屏蔽时间。 » 敏感度：为SQL注入检查指定检测敏感度，可以为“高”、“中”或者“低”。敏感度越高，漏报率越低。 » 检查点：为SQL注入检查指定检查点，可以为URI、Cookie、 Cookie2、Referer或者 Post 。
XSS注入检查	选中“启用”复选框开启XSS注入检查功能。 » 抓包 ： 对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 行为：只记录日志 - 系统发现攻击后仅记录日志信息；重置 - 发现攻击后重置连接（TCP）或者发送目标不可达包（UDP）并且记录日志信息；阻断IP - 屏蔽攻击者的IP地址并设置屏蔽时间；阻断服务 - 屏蔽攻击者的服务并设置屏蔽时间。 » 敏感度：为Web服务器XSS注入检查指定检测敏感度，可以为“高”、“中”或者“低”。敏感度越高，漏报率越低。 » 检查点：为Web服务器XSS注入检查指定检查点，可以为URI、Cookie、Cookie2、Referer或者 Post 。
外链检查	选中“启用”复选框开启Web站点外链检查功能，控制Web站点对其它站点资源的引用。 » 抓包 ： 对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 外链特例：点击“外链特例”链接，弹出<外链特例配置>对话框，在该对话框配置的URL都可以被Web站点引用（被外链）。每个Web服务器防护规则最多可配置32个URL。 » 行为：为Web站点外链行为指定相应的动作，可以为“仅记录日志”或者“重置”。“仅记录日志”指定发现Web站点进行不合规外链行为后仅记录日志信息。“重置”指定发现Web站点不合规外链行为后重置连接（TCP）或者发送目标不可达包（UDP）并且记录日志信息。
访问控制	选中“启用”复选框开启访问控制功能，即对Web站点进行上传路径检查，防止攻击者利用上传漏洞向Web站点上传恶意代码。 » 访问控制路径：点击“访问控制路径”链接，弹出<访问控制配置>对话框，在该对话框配置Web站点路径并指定其属性，该路径为Web站点的相对路径。“静态”属性表示Web站点路径下的资源只能按照静态资源（图片和普通文本）进行访问，否则，将按照控制行为设置（仅记录日志/重置）进行处理；“禁止”属性表示Web站点路径下的资源不允许访问。 » 行为：为Web站点上传行为指定相应的动作，可以为“仅记录日志”或者“重置”。“仅记录日志”指定发现Web站点上传行为后仅记录日志信息。“重置”指定发现Web站点上传行为后重置连接（TCP）或者发送目标不可达包（UDP）并且记录日志信息。
CC防护	选中“启用”复选框开启CC防护功能，保护Web服务器免受HTTP Request Flood攻击。 » 请求阈值：设置请求阈值。如果20秒钟之内，系统收到的HTTP请求每秒都超过请求阈值，则系统判定CC攻击发生。 判定发生攻击后，用户可采取如下措施：

选项	说明
	» 认证方法：为CC防护功能配置认证方法。系统通过认证判断HTTP请求的源IP是否合法，从而识别攻击流量并进行防护。如果某个源IP认证失败，系统将阻断该源IP发起的本次HTTP请求。认证方法包括：自动（JS Cookie），该认证方法由浏览器自动完成认证交互；自动（重定向），该认证方法由浏览器自动完成认证交互；手动（访问确认），该认证方法需要HTTP请求发起者点击返回提示框上的“确认”按钮进行认证；手动（验证码），该认证方法需要请求发起者输入验证码进行认证。 » 爬虫友好：选中复选框，不对爬虫进行认证。 » 访问限速：选中“启用”复选框，为CC防护功能配置访问限速。配置访问限速后，系统会根据配置对每个源IP进行请求速率限制。在“阈值”文本框中指定访问速率阈值，如果收到的请求速率超过该指定值且CC防护功能已开启，系统会对超出的请求数做相应的限制操作，可以为“阻断IP”或者“重置”。“阻断IP”对超出的请求速率的源IP进行阻断，并在“时长”文本框中指定阻断时长，单位为秒，范围是60到3600秒。“重置”指定重置超出的请求数的请求连接；选中“记录日志”复选框，指定记录日志信息。 » 代理限速：选中“启用”复选框，为CC防护功能配置代理限速。配置代理限速后，系统会检查每个源IP是否属于代理服务器，若属于，则根据配置进行请求速率限制。在“阈值”文本框中指定请求速率阈值，如果收到的请求速率超过该指定值且CC防护功能已开启，系统会对超出的请求数做相应的限制操作，可以为“阻断IP”或者“重置”。“阻断IP”指定对攻超出的请求数的源IP进行阻断，并在“时长”文本框中指定阻断时长，单位为秒，范围是60到3600秒。“重置”指定重置超出的请求数的请求连接；选中“记录日志”复选框，指定记录日志信息。 » 白名单：对白名单中的地址不做CC防护。

在DNS标签页，对DNS协议进行配置。

选项	说明
DNS	**扫描最大长度**：对DNS协议报文进行扫描时，扫描的最大长度。 **协议异常检查**：对DNS协议报文进行分析，查看协议是否存在异常。 对于异常报文，可以进行抓包，并指定动作进行处理： » 抓包：对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 行为：只记录日志 - 系统发现攻击后仅记录日志信息；重置 - 发现攻击后重置连接（TCP）或者发送目标不可达包（UDP）并且记录日志信息；阻断IP - 屏蔽攻击者的IP地址并设置屏蔽时间；阻断服务 - 屏蔽攻击者的服务并设置屏蔽时间。

在FTP标签页，对FTP协议进行配置。

选项	说明
FTP	**扫描最大长度**：对FTP协议报文进行扫描时，扫描的最大长度。 **协议异常检查**：对FTP协议报文进行分析，查看协议是否存在异常。 对于异常报文，可以进行抓包，并指定动作进行处理： » 抓包：对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 行为：只记录日志 - 系统发现攻击后仅记录日志信息；重置 - 发现攻击后重置连接（TCP）或者发送目标不可达包（UDP）并且记录日志信息；阻断IP - 屏蔽攻击者的IP地址并设置屏蔽时间；阻断服务 - 屏蔽攻击者的服

选项	说明
	务并设置屏蔽时间。 **Banner防护**：FTP服务器banner信息保护功能。 » Banner信息：开启banner防护功能后，在该文本框中输入新信息替换原有服务器banner信息。 **命令行最大长度：**指定FTP命令行的最大长度（包含回车换行）。对超出限定范围的报文，可以进行抓包，并指定动作进行处理： » 抓包：对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 行为：只记录日志；重置 ；阻断IP；阻断服务。 **响应行最大长度**：指定FTP最大响应长度。 对超出限定范围的报文，可以进行抓包，并指定动作进行处理： » 抓包：对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 行为：只记录日志；重置 ；阻断IP；阻断服务。 **在暴力破解下阻断配置**：如果一分钟内指定次数尝试登录均失败，系统会判定为攻击，并根据配置做出相应处理。 » 每分钟登录上限值：指定允许的一分钟内认证/登录失败的次数。 » 屏蔽对象：指定对超出限定认证/登录失败频率的攻击者的IP地址或者协议/源IP/目的IP/目的端口进行阻断。 » 屏蔽时间：指定对攻击者IP或者协议/源IP/目的IP/目的端口进行阻断的时长。

在MSRPC标签页，对MSRPC协议进行配置。

选项	说明
	扫描最大长度：对MSRPC协议报文进行扫描时，扫描的最大长度。 **协议异常检查**：对MSRPC协议报文进行分析，查看协议是否存在异常。 对于异常报文，可以进行抓包，并指定动作进行处理： » 抓包：对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 行为：只记录日志 - 系统发现攻击后仅记录日志信息；重置 - 发现攻击后重置连接（TCP）或者发送目标不可达包（UDP）并且记录日志信息；阻断IP - 屏蔽攻击者的IP地址并设置屏蔽时间；阻断服务 - 屏蔽攻击者的服务并设置屏蔽时间。
MSRPC	**Bind最大长度**：指定系统允许的MSRPC协议绑定报文的最大长度。对超出限定范围的报文，可以进行抓包，并指定动作进行处理： » 抓包：对异常数据包进行抓包。 » 行为：只记录日志；重置 ；阻断IP；阻断服务。 **Request最大长度**：指定系统允许的MSRCP协议请求报文的最大长度。 对超出限定范围的报文，可以进行抓包，并指定动作进行处理： » 抓包：对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 行为：只记录日志；重置 ；阻断IP；阻断服务。

选项	说明
	在暴力破解下阻断配置：如果一分钟内指定次数尝试登录均失败，系统会判定为攻击，并根据配置做出相应处理。 » 每分钟登录上限值：指定允许的一分钟内登录失败的次数。 » 屏蔽对象：指定对攻击者的IP地址或者协议/源IP/目的IP/目的端口进行阻断。 » 屏蔽时间：指定对攻击者IP或者协议/源IP/目的IP/目的端口进行阻断的时长。

在POP3标签页，对POP3协议进行配置。

选项	说明
POP3	**扫描最大长度**：对POP3协议报文进行扫描时，扫描的最大长度。 **协议异常检查**：对POP3协议报文进行分析，查看协议是否存在异常。 对于异常报文，可以进行抓包，并指定动作进行处理： » 抓包：对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 行为：只记录日志 - 系统发现攻击后仅记录日志信息；重置 - 发现攻击后重置连接（TCP）或者发送目标不可达包（UDP）并且记录日志信息；阻断IP - 屏蔽攻击者的IP地址并设置屏蔽时间；阻断服务 - 屏蔽攻击者的服务并设置屏蔽时间。 **Banner防护**：POP3服务器banner信息保护功能。 » Banner信息：开启banner防护功能后，在该文本框中输入新信息替换原有服务器banner信息。 **命令行最大长度**：指定POP3命令行的最大长度（包含回车换行）。 对超出限定范围的报文，可以进行抓包，并指定动作进行处理： » 抓包：对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 行为：只记录日志；重置 ；阻断IP；阻断服务。 **参数最大长度**：指定POP3客户端命令参数的最大长度。对超出限定范围的报文，可以进行抓包，并指定动作进行处理： » 抓包：对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 行为：只记录日志；重置 ；阻断IP；阻断服务。 **失败最大次数**：指定系统允许的POP3服务器返回错误的最大次数（同一个POP3会话中）。对超出限定范围的报文，可以进行抓包，并指定动作进行处理： » 抓包：对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 行为：只记录日志；重置 ；阻断IP；阻断服务。 **在暴力破解下阻断配置**：如果一分钟内指定次数尝试登录均失败，系统会判定为攻击，并根据配置做出相应处理。 » 每分钟登录上限值：指定允许的一分钟内登录失败的次数。 » 屏蔽对象：指定对攻击者的IP地址或者协议/源IP/目的IP/目的端口进行阻断。

选项	说明
	» 屏蔽时间：指定对攻击者IP或者协议/源IP/目的IP/目的端口进行阻断的时长。

在SMTP标签页，对SMTP协议进行配置。

选项	说明
SMTP	**扫描最大长度**：对SMTP协议报文进行扫描时，扫描的最大长度。 **协议异常检查**：对SMTP协议报文进行分析，查看协议是否存在异常。 对于异常报文，可以进行抓包，并指定动作进行处理： » 抓包：对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 行为：只记录日志 - 系统发现攻击后仅记录日志信息；重置 - 发现攻击后重置连接（TCP）或者发送目标不可达包（UDP）并且记录日志信息；阻断IP - 屏蔽攻击者的IP地址并设置屏蔽时间；阻断服务 - 屏蔽攻击者的服务并设置屏蔽时间。 **Banner防护**：SMTP服务器banner信息保护功能。 » Banner信息：开启banner防护功能后，在该文本框中输入新信息替换原有服务器banner信息。 **命令行最大长度**：指定SMTP命令行的最大长度（包含回车换行）。对超出限定范围的报文，可以进行抓包，并指定动作进行处理： » 抓包：对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 行为：只记录日志；重置 ；阻断IP；阻断服务。 **路径最大长度**：指定系统允许的SMTP客户端命令中reverse-path和forward-path的最大长度。对超出限定范围的报文，可以进行抓包，并指定动作进行处理： » 抓包：对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 行为：只记录日志；重置 ；阻断IP；阻断服务。 **回复行最大长度**：指定系统允许的SMTP服务器端响应的最大长度。对超出限定范围的报文，可以进行抓包，并指定动作进行处理： » 抓包：对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 行为：只记录日志；重置 ；阻断IP；阻断服务。 **文本行最大长度**：指定系统允许的SMTP客户端邮件文本的最大长度。对超出限定范围的报文，可以进行抓包，并指定动作进行处理： » 抓包：对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 行为：只记录日志；重置 ；阻断IP；阻断服务。 **内容类型最大长度**：指定SMTP协议Content-Type值的最大长度。对超出限定范围的报文，可以进行抓包，并指定动作进行处理： » 抓包：对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 行为：只记录日志；重置 ；阻断IP；阻断服务。

选项	说明
	内容文件名最大长度：指定SMTP协议邮件附件名称的最大长度。对超出限定范围的报文，可以进行抓包，并指定动作进行处理： » 抓包：对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 行为：只记录日志；重置 ；阻断IP；阻断服务。 **失败最大次数**：指定系统允许的SMTP服务器返回错误的最大次数（同一个SMTP会话中）。对超出限定范围的报文，可以进行抓包，并指定动作进行处理： » 抓包：对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 行为：只记录日志；重置 ；阻断IP；阻断服务。 **在暴力破解下阻断配置**：如果一分钟内指定次数尝试登录均失败，系统会判定为攻击，并根据配置做出相应处理。 » 每分钟登录上限值：指定允许的一分钟内登录失败的次数。 » 屏蔽对象：指定对攻击者的IP地址或者协议/源IP/目的IP/目的端口进行阻断。 » 屏蔽时间：指定对攻击者IP或者协议/源IP/目的IP/目的端口进行阻断的时长。

在SUNRPC标签页，对SUNRPC协议进行配置。

选项	说明
SUNRPC	**扫描最大长度**：对SUNRPC协议报文进行扫描时，扫描的最大长度。 **协议异常检查**：对SUNRPC协议报文进行分析，查看协议是否存在异常。 对于异常报文，可以进行抓包，并指定动作进行处理： » 抓包：对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 行为：只记录日志 - 系统发现攻击后仅记录日志信息；重置 - 发现攻击后重置连接（TCP）或者发送目标不可达包（UDP）并且记录日志信息；阻断IP - 屏蔽攻击者的IP地址并设置屏蔽时间；阻断服务 - 屏蔽攻击者的服务并设置屏蔽时间。 **在暴力破解下阻断配置**：如果一分钟内指定次数尝试登录均失败，系统会判定为攻击，并根据配置做出相应处理。 » 每分钟登录上限值：指定允许的一分钟内登录失败的次数。 » 屏蔽对象：指定对攻击者的IP地址或者协议/源IP/目的IP/目的端口进行阻断。 » 屏蔽时间：指定对攻击者IP或者协议/源IP/目的IP/目的端口进行阻断的时长。

在Telnet标签页，对Telnet协议进行配置。

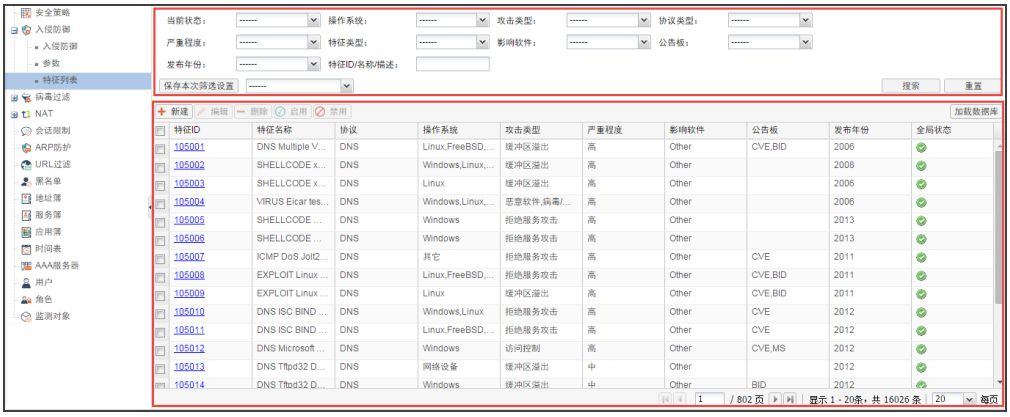
选项	说明
Telnet	**扫描最大长度**：对SUNRPC协议报文进行扫描时，扫描的最大长度。 **协议异常检查**：对SUNRPC协议报文进行分析，查看协议是否存在异常。 对于异常报文，可以进行抓包，并指定动作进行处理：

选项	说明
	» 抓包：对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 行为：只记录日志 - 系统发现攻击后仅记录日志信息；重置 - 发现攻击后重置连接（TCP）或者发送目标不可达包（UDP）并且记录日志信息；阻断IP - 屏蔽攻击者的IP地址并设置屏蔽时间；阻断服务 - 屏蔽攻击者的服务并设置屏蔽时间。 **在暴力破解下阻断配置**：如果一分钟内指定次数尝试登录均失败，系统会判定为攻击，并根据配置做出相应处理。 » 每分钟登录上限值：指定允许的一分钟内登录失败的次数。 » 屏蔽对象：指定对攻击者的IP地址或者协议/源IP/目的IP/目的端口进行阻断。 » 屏蔽时间：指定对攻击者IP或者协议/源IP/目的IP/目的端口进行阻断的时长。 **用户名/密码最大长度**：指定Telnet用户名和密码的最大长度。对超出限定范围的报文，可以进行抓包，并指定动作进行处理： » 抓包：对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。 » 行为：只记录日志；重置 ；阻断IP；阻断服务。

6. 点击“保存”完成配置。

特征列表

打开“策略 > 入侵防御 > 特征列表”，显示特征列表页。



特征列表页上部分是检索栏，用来检索特征，下部分是特征列表，用于管理特征，包括：查看/新建/编辑/删除/启用/禁用特征。

检索特征

用户可在搜索栏设置检索条件，查看符合需求的特征。点击“搜索”按键搜索特定的特征条目。点击“重置”按键重置所有过滤条件。点击“保存此次筛选配置”将检索条件保存。

管理特征

在特征列表部分，对特征进行管理。

- 查看特征：在特征列表中点击特征ID，查看特征详情。
- 新建特征，点击“新建”。

在<基本配置>标签页，进行如下配置：

选项	说明
名称	指定特征的名称。
描述	指定特征的描述信息。
协议	指定受影响的协议。
方向	指定该特征的匹配方向。 » 客户端到服务器 - 具有特征的报文是客户端发给服务器的； » 服务器到客户端 - 具有特征的报文是服务器发给客户端的； » 任意 - 具有特征的报文可以是任意方向的。
源端口	指定该特征的源端口号。 » 任意 - 任意端口。 » 包含 - 特征的源端口需包含该端口号；可以是一个，多个，或者是一个范围。在其后的文本框中输入端口号，用“，”隔开。 » 不包含 - 排除指定的端口；可以是一个，多个，或者是一个范围。在其后的文本框中输入端口号，用“，”隔开。
目的端口	指定该特征的目的端口号。 » 任意 - 任意端口。 » 包含 - 特征的目的端口需包含该端口号；可以是一个，多个，或者是一个

选项	说明
	范围。在其后的文本框中输入端口号，用“，”隔开。 » 不包含 - 排除指定的端口；可以是一个，多个，或者是一个范围。在其后的文本框中输入端口号，用“，”隔开。
包净荷尺寸值	指定报文数据（payload）包的大小。从下拉框中选择“>”、“<”或“=”，并在其后的文本框中输入数值大小。“----”表示不指定该参数。
严重程度	指定攻击的严重程度。
攻击类型	指定攻击的类型。
影响软件	指定受影响的软件。“----”表示所有软件。
操作系统	指定受影响操作系统的名称。“----”表示所有操作系统。
公告板	指定公告板。
发布年份	指定发布年份。
检测过滤	指定特征规则发生的频率。 » 跟踪 - 从下拉菜单中选择跟踪的类型，可以是源IP，也可以是目的IP。指定后，系统将依据源IP或目的IP的统计，匹配当前规则的攻击。 » 次数 - 指定在规定时间内，该规则发生的最大次数。攻击若超过指定次数，系统就会触发规则并按指定的动作进行操作。 » 秒数 - 指定该特征规则发生的时间间隔。

<内容>标签页：点击“新建”按钮，弹出<新增内容>对话框，创建特征的内容。

选项	说明
<内容>标签页：点击“新建”按钮，弹出<新增内容>对话框，创建特征的内容。	
内容	指定新增特征的内容。勾选“HEX”表示该内容为十六进制；勾选“忽略大小写”表示该内容输入时可忽略字母大小写；勾选“URI”表示内容需要匹配HTTP请求中的URI字段。
相对位置	指定该内容的位置。 » 如选择“头部”，表示在应用层报文头部的位置开始搜索。 » 绝对偏移：系统将在应用层报文头偏移指定字节之后开始搜索。 » 绝对深度：指定应用层报文头偏移后的扫描长度。 » 如选择“前一个内容”，表示在前一个内容结束位置开始搜索。 » 相对偏移：系统将在前一个内容结束位置偏移指定字节之后开始搜索。 » 相对深度：指定在前一个内容结束位置偏移指定字节之后的扫描长度。

» 加载数据库：新建特征后，需点击“加载数据库”，才能将新建特征生效。

» 编辑特征：选中特征后，点击编辑。只可编辑自定义特征。编辑特征后，需点击“加载数据库”，才能使编辑后的特征生效。

» 删除特征：选中特征后，点击删除。只可删除自定义特征。删除特征后，需点击“加载数据库”，才能使删除后的特征失效。

» 启用/禁用特征：选中特征后，点击启用/禁用。

特征ID作为特征的唯一标识， 根据协议进行分类。特征ID由两部分构成，分别为协议ID（第1位或者第1和第2位）和攻击特征ID（后5位），例如ID“605001”中，“6”表示Telnet协议，“05001”表示攻击特征ID。攻击特征ID的第1位是“6”的为协议异常特征，其余为攻击特征。协议ID与协议的对应关系下表所示：

协议ID	协议	协议ID	协议	协议ID	协议	协议ID	协议
1	DNS	7	Other-TCP	13	TFTP	19	NetBIOS
2	FTP	8	Other-UDP	14	SNMP	20	DHCP
3	HTTP	9	IMAP	15	MySQL	21	LDAP
4	POP3	10	Finger	16	MSSQL	22	VoIP
5	SMTP	11	SUNRPC	17	Oracle	-	-
6	Telnet	12	NNTP	18	MSRPC	-	-

上表中，“Other-TCP”表示除表中已列出的标准TCP协议以外的其他TCP协议；“Other-UDP”表示除表中已列出的标准UDP协议以外的其他UDP协议。

病毒过滤

配置病毒过滤功能后，设备能够探测各种病毒威胁，例如恶意软件、恶意网站等，并且根据配置对发现的病毒进行处理。

病毒过滤功能可检测最易携带病毒的文件类型和常用的协议类型并对其进行病毒防护。

- 可扫描文件类型：GZIP、BZIP2、TAR、ZIP、RAR、PE、HTML、MAIL、RIFF、以及JPEG。
- 可扫描协议类型：POP3、HTTP、SMTP、IMAP4、以及FTP

系统的病毒过滤特征库包含万余种病毒特征，支持病毒过滤特征库的每日自动升级，也可以手动实时升级，请参阅"升级管理" 在第197页的升级特征库部分。

注意:

- 病毒过滤功能受许可证控制。为设备安装病毒过滤（AV）许可证，功能才可使用。
- 开启病毒过滤功能后，系统的最大并发连接数将会减半。

配置病毒过滤

配置病毒过滤包括如下内容：

- 病毒过滤配置准备工作
- 配置病毒过滤功能
- 病毒过滤全局配置

病毒过滤配置准备工作

使用病毒过滤功能前，必须完成以下准备工作：

- 安装病毒过滤（AV）许可证，然后重启设备。设备成功重启后，病毒过滤功能即处于开启状态。
- 初次使用病毒过滤功能，需要首先更新病毒过滤特征库。为保证能够正常连接到默认更新服务器，请在更新前为设备配置DNS服务器。

配置病毒过滤功能

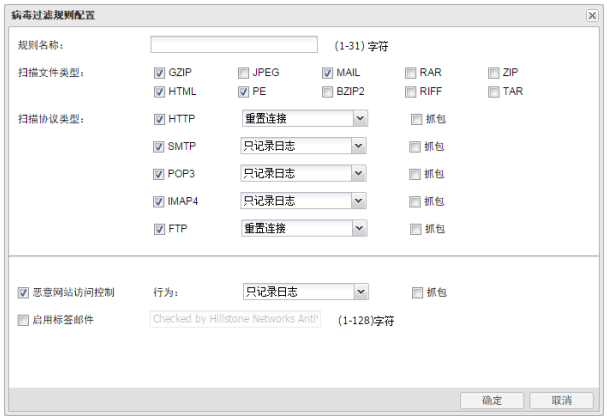
系统支持基于策略的病毒过滤配置方式。为策略配置病毒过滤规则后，系统将会对与策略规则相匹配的流量根据病毒过滤规则进行病毒过滤检查。

配置病毒过滤功能包含两部分:

1. 配置病毒过滤规则。
2. 绑定病毒过滤规则到策略规则。详细信息，请参阅"安全策略" 在第81页。

配置病毒过滤规则，请按照以下步骤进行操作：

1. 点击“策略 > 病毒过滤 > 病毒过滤 “。
2. 点击“新建”按钮。



在<病毒过滤规则配置>对话框，填写病毒过滤规则配置信息。

选项	说明
规则名称	指定病毒过滤规则名称。
扫描文件类型	指定系统将扫描的文件类型。
扫描协议类型	指定系统将扫描的协议类型（HTTP、SMTP、POP3、IMAP4、FTP）以及发现病毒后的处理动作。 » 填充魔术数 - 使用文件填充的方式处理病毒文件，即从文件中被病毒感染部分的起始位置起使用魔术字（Virus is found, cleaned）进行填充，一直到被感染部分结束。 » 只记录日志 - 系统发现病毒后仅记录日志信息。 » 警告 - 弹出警告提示页面，提示用户发现病毒。用户可在警告提示页面点击“忽略此警告”链接，跳过该页面，继续访问。跳过警告提示页面后，若用户一小时之内再次访问该网站，将不会收到警告提示。该选项只对通过HTTP协议传输的信息进行病毒扫描时有效。 » 重置连接 - 发现病毒后，重置病毒连接。
抓包	勾选“抓包”复选框对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。
恶意网站访问控制	勾选复选框，开启策略的恶意网站访问控制功能。
行为	指定系统发现恶意链接后的处理动作： » 只记录日志 - 系统发现恶意链接后仅记录日志信息。 » 重置连接 - 发现恶意链接后，重置恶意链接连接。 » 返回告警页面 - 弹出警告提示页面，提示用户发现恶意网站。点击“忽略此警告”链接，跳过警告提示页面继续访问。跳过警告提示页面后，若用户一小时之内再次访问该网站，将不会收到警告提示。
启用标签邮件	如果选择对通过SMTP协议传输的邮件进行病毒扫描，则用户可以对发出的电子邮件开启标签邮件功能，即系统对邮件及其附件进行扫描，扫描病毒的结果会包含在邮件的主体中，随邮件一起发送。如果没有发现病毒，则提示“No virus found”；如发现病毒，则显示邮件中病毒相关信息，包括系统扫描文件的名称、扫描结果以及对该病毒的执行动作。 在文本框内指定邮件结尾内容， 范围是1-128个字符。

3. 点击“确定”按钮保存所做配置并返回病毒过滤规则页面。

注意： 默认情况下，系统预定义多条默认病毒过滤规则。用户可查看规则配置，根据情况直接使用。

病毒过滤全局配置

配置病毒过滤全局配置选项，请按照以下步骤进行操作：

1. 点击“策略 > 病毒过滤 > 参数”。

在“病毒过滤全局配置”部分配置全局配置信息。

选项	说明
病毒过滤	选中/取消选中“启用”复选框开启/关闭设备的病毒过滤功能。

选项	说明
最大压缩层	针对压缩嵌套的文件，用户可以通过该选项对可扫描压缩层数进行配置。从下拉菜单中选择需要的层数。范围是1-5层。
超出行为	指定对超出限制的压缩文件的处理动作。从下拉菜单中进行选择，可以是： » 只记录日志 - 只生成相关日志信息。 » 重置连接 - 发现病毒后，重置病毒连接。
加密压缩文件	指定对加密压缩文件的处理方式，可以是： » ------ - 不对加密压缩文件进行病毒过滤特殊处理，根据配置，系统可能会继续扫描。 » 只记录日志 - 只生成相关日志信息，不对加密压缩文件进行扫描。 » 重置连接 - 重置加密压缩文件连接。

2. 配置完成，点击“确定”按钮。

攻击防护

网络中存在多种防不胜防的攻击，如侵入或破坏网络上的服务器、盗取服务器的敏感数据、破坏服务器对外提供的服务，或者直接破坏网络设备导致网络服务异常甚至中断。设备具备攻击防护功能来检测各种类型的网络攻击，从而采取相应的措施保护内部网络免受恶意攻击，以保证内部网络及系统正常运行。

系统提供基于安全域的攻击防护功能，能够对网络攻击进行合理处理从而保证用户网络系统的安全。

配置攻击防护

配置基于安全域的攻击防护功能，请按照以下步骤进行操作：

1. 点击“网络 > 安全域”。
2. 双击需要配置攻击防护的安全域。
3. 在<安全域配置>对话框中，选择“攻击防护”对应的“启用”按钮。
4. 点击“设置”打开<攻击防护>对话框进行设置。

在<攻击防护>对话框，配置各功能的参数信息。

选项	说明
白名单	白名单中的地址或地址段不受攻击防护功能的检查。 点击“设置”，弹出<白名单配置>对话框。 » IP/掩码 - 指定添加到白名单中的IP地址和网络掩码。 » 地址条目 - 指定添加到白名单中的地址条目。
全选	**全部启用**：选中该复选框开启所有的攻击防护功能。 **行为**：为所有的攻击防护功能指定默认操作，即受到攻击后设备的防护措施： » 丢弃 - 系统的默认行为。丢弃攻击包。 » 告警 - 发出警报但是允许包通过。 » --- - 不指定全局行为。
Flood防护	**ICMP洪水攻击防护**：选中该复选框开启ICMP洪水攻击防护功能。 » 警戒值 - 指定安全设备收到的ICMP包个数的警戒值。如果同一个目的IP地址在一秒钟内收到的ICMP包的个数超过该警戒值，设备就判断为受到ICMP洪水攻击，从而采取相应的处理。默认值是1500个，取值范围是1到50000。 » 行为 - 指定受到ICMP洪水攻击而进行的处理行为。如果选择默认行为“丢弃”，系统将在发生攻击的当前秒和下一秒这段时间内，仅允许指定个数（警戒值）的ICMP包通过，并且发出警报，在这段时间内的其它同类包将会被丢弃。
	UDP洪水攻击防护：选中该复选框开启UDP洪水攻击防护功能。 » 源警戒值 - 指定安全设备发送的UDP包个数的警戒值。如果同一个源IP地址在一秒钟内发送的UDP包的个数超过该警戒值，设备就判断为受到UDP洪水攻击，从而采取相应的处理。默认值是1500个，取值范围是1到50000。 » 目的警戒值 - 指定设备收到的UDP包个数的警戒值。如果同一个目的IP地址的同一个端口号在一秒钟内收到的UDP包的个数超过该警戒值，设备就判断为受到UDP洪水攻击，从而采取相应的处理。默认值是1500个，取值范围是1到50000。 » 行为 - 指定受到UDP洪水攻击而进行的处理行为。如果选择默认行为“丢弃”，系统将在发生攻击的当前秒和下一秒这段时间内，仅允许指定个数（警戒值）的UDP包通过，并且发出警报，在这段时间内的其它同类包将会被丢弃。
	ARP欺骗攻击防护：选中该复选框开启ARP欺骗攻击防护功能。 » 每个MAC最大IP数 - 指定是否检查ARP表中一个MAC地址对应的IP地址数。如果该选项值为0，则不检查；如果非0，则进行检查，并且如果每个MAC地址对应的IP地址数多于该参数的值，系统将按照“行为”选项的配置进行处理。该参数值的范围是0到1024。 » 免费ARP包发送速率 - 指定安全设备是否发出免费ARP包。如果该参数值是0，则不发送免费ARP包（参数的默认值）；如果非0，则发出，并且每秒钟发出包的个数为该参数的值。该参数的取值范围是0到10。 » 反向查询 - 选中该复选框开启ARP反向查询功能。当设备收到ARP请求后，会记录IP地址并且发送ARP请求，检查是否会收到不同MAC地址的返回包或者返回包的MAC地址与ARP请求包的MAC地址是否相同。
	SYN洪水攻击防护：选中该复选框开启SYN洪水攻击防护功能。

选项	说明
	» 源警戒值 - 指定一秒钟内从一个源IP地址发出的SYN包的个数，无论目标IP地址和端口号是什么。如果安全设备探测到一秒钟内从同一个源IP地址发出的SYN包多于该指定数，就判断为受到了SYN洪水攻击。默认值是1500个。取值范围是0到50000个。0表示不对源警戒值进行检测。 » 目的警戒值 - 指定一秒钟内基于IP或基于端口的收SYN包个数。 » 基于IP - 选中“基于IP”单选按钮并在对应文本框中输入需要的数值，指定一秒钟内同一个目的IP地址收到的SYN包个数。如果设备探测到一秒钟同一个目的IP地址收到的SYN包多于该指定数，就认为是受到了SYN洪水攻击。默认值是1500个。取值范围是0到50000个。0表示不对目的警戒值进行检测。 » 基于端口 - 选中“基于端口”单选按钮并在对应文本框中输入需要的数值，指定一秒钟内同一目的IP的同一个目的端口收到的SYN包个数。如果设备探测到一秒钟同一目的IP的同一个目的端口收到的SYN包多于该指定数，就认为是受到了SYN洪水攻击。默认值是1500个。取值范围是0到50000个。0表示不对目的警戒值进行检测。选中“基于端口”单选按钮并在“目的地址”组合框中输入或选中“IP地址”或者“地址条目”，指定开启特定网段的基于目的端口的SYN洪水攻击防护功能，其它网段做基于目的IP地址的SYN洪水攻击防护。目的IP地址掩码取值范围是24到32。 » 行为 - 指定受到SYN洪水攻击而进行的处理行为。如果选择默认行为“丢弃”，系统将在发生攻击的当前秒和下一秒这段时间内，仅允许指定个数（源警戒值或者目的警戒值）的SYN包通过，并且发出警报，在这段时间内的其它同类包将会被丢弃；如果同时配置了源和目的警戒值，系统会先检查其是否为目的SYN洪水攻击，如果是，则丢弃并报警，如果不是，再检查其是否为源SYN洪水攻击，是则丢弃并报警。
MS-Windows防护	**WinNuke攻击防护**：选中该复选框开启WinNuke攻击防护功能。当设备发现受到WinNuke攻击后，会丢弃攻击包并且发出警报通知。
扫描/欺骗防护	**IP地址欺骗攻击防护**：选中该复选框开启IP地址欺骗攻击防护功能。当设备发现受到IP地址欺骗攻击后，会丢弃攻击包并且发出警报通知。 **IP地址扫描攻击防护**：选中该复选框开启IP地址扫描攻击防护功能。 » 警戒值 - 指定地址扫描的时间警戒值。如果设备探测到在该指定时间内有10个以上来自同一个源IP地址的ICMP包发往不同的主机，设备就认为是受到IP地址扫描攻击。默认值是1，单位是毫秒，取值范围是1到5000毫秒。 » 行为 - 指定受到IP地址扫描攻击而进行的处理行为。如果选择默认行为“丢弃”，系统在指定时间内（警戒值），仅允许10个来自同一个源IP地址的发往不同主机的ICMP包通过，并且发出警报，指定时间内的其它同类包将会被丢弃。 **端口扫描防护**：选中该复选框开启端口扫描攻击防护功能。 » 警戒值 - 指定端口扫描的时间警戒值。如果设备探测到在该指定时间内有10个以上TCP SYN包发往同一目标的不同端口，设备就认为是受到了端口扫描攻击。默认值是1，单位是毫秒，取值范围是1到5000毫秒。 » 行为：指定受到端口扫描攻击而进行的处理行为。如果选择默认行为“丢弃”，系统在指定时间内（警戒值），仅允许10个发往同一目标的不同端口的TCP SYN包通过，并且发出警报，指定时间内的其它同类包将会被丢弃。
拒绝服务防护	**Ping of Death攻击防护**：选中其复选框开启Ping of Death攻击防护功能。当设备发现受到Ping of Death攻击后，会丢弃攻击包并且发出警报通知。

选项	说明
	Teardrop攻击防护：选中其复选框开启Teardrop攻击防护功能。当设备发现受到Teardrop攻击后，会丢弃攻击包并且发出警报通知。
	IP分片防护：选中其复选框开启IP分片攻击防护功能。 » 行为 - 指定受到IP分片攻击而进行的处理行为。默认为“丢弃”。
	IP选项：选中其复选框开启IP选项攻击防护功能。系统会对以下IP选项类型进行防护：Security、Loose Source Route、Record Route、Stream ID、Strict Source Route和Timestamp。 » 行为 - 指定受到IP选项攻击而进行的处理行为。默认为“丢弃”。
	Smurf或者Fraggle攻击防护：选中其复选框开启Smurf或者Fraggle攻击防护功能。 » 行为 - 指定受到Smurf或者Fraggle攻击而进行的处理行为。默认为“丢弃”。
	Land攻击防护：选中其复选框开启Land攻击防护功能。 » 行为 - 指定受到Land攻击而进行的处理行为。默认为“丢弃”。
	ICMP大包攻击防护：选中其复选框开启ICMP大包攻击防护功能。 » 警戒值 - 指定ICMP包的大小的警戒值。如果收到的ICMP包的大小大于该指定值，系统就判断为受到大ICMP包攻击，从而采取相应的处理措施。默认值是1024字节，取值范围是1到50000字节。 » 行为：指定受到ICMP大包攻击而进行的处理行为。默认为“丢弃”。
代理	**SYN代理**：选中其复选框开启SYN代理功能。SYN代理功能配合SYN洪水攻击防护功能来共同防护SYN洪水攻击。当SYN洪水攻击防护功能和SYN代理功能都开启时，SYN代理功能对已经通过SYN洪水攻击防护功能检测的数据包起效。 » 最小代理速率 - 指定激活SYN代理机制或者SYN-Cookie机制（选中“Cookie”复选框）的最小SYN包个数值。如果一个目的IP地址的同一个端口在一秒钟内收到的SYN包个数多于该选项的指定值，就会激活SYN代理机制或者SYN-Cookie机制。默认值是1000个每秒，取值范围是0到50000。 » Cookie - 选中该复选框开启SYN-Cookie功能。SYN-Cookie是一种无状态的SYN代理机制。该功能开启后，能够在功能上扩大设备处理多个SYN包的能力，因此用户可以适当的增大“最小代理速率”和“最大代理速率”两个选项之间的范围。 » 最大代理速率 - 指定SYN代理机制或者SYN-Cookie机制（选中“Cookie”复选框）在指定时间内允许通过的最大SYN包个数。如果一个目的IP地址的同一个端口在一秒钟内收到的SYN包个数多于该参数的指定值，系统会在当前秒和下一秒内仅允许该指定数值的SYN包通过，其它同类包将会被丢弃。默认值是3000个每秒，取值范围是1到1500000。 » 代理超时 - 指定半连接的超时时间值，单位为秒。半连接达到该超时值后会被丢弃。默认值是30秒。取值范围是1到180秒。
协议异常报告	**TCP异常**：选中其复选框开启TCP异常攻击防护功能。 » 行为 - 指定受到TCP异常攻击而进行的处理行为。默认为“丢弃”。
DNS查询洪水防护	**DNS查询洪水防护**：选中其复选框开启DNS查询洪水防护功能。 » 源警戒值 - 指定设备发送的DNS查询报文的警戒值。如果一秒钟内同一个源IP地址发送的DNS查询报文个数超过该警戒值，设备就判断为受到DNS

选项	说明
	查询洪水攻击，从而采取相应的处理措施。 » 目的警戒值 - 指定设备收到的DNS查询报文的个数的警戒值。如果一秒钟内设备收到的到达同一个目的IP地址且相同端口号的DNS查询报文个数超过该警戒值，设备就判断为受到DNS查询洪水攻击，从而采取相应的处理措施。 » 行为 - 指定设备对DNS查询洪水攻击采取的行为。如果选择默认行为“丢弃”，在发生攻击的当前秒和下一秒这段时间内，设备仅允许指定个数（警戒值）的DNS查询报文通过，并且发出警报，在这段时间内的其它同类包将会被丢弃；如果选择“告警”，系统将在发现DNS查询洪水攻击后发出警报但是允许DNS查询报文通过。
	DNS递归查询洪水攻击防护：选中其复选框开启安全域的DNS递归查询洪水防护功能。 » 源警戒值 - 指定设备发送的DNS递归查询报文的警戒值。如果一秒钟内同一个源IP地址发送的DNS查询报文个数超过该警戒值，设备就判断为受到DNS查询洪水攻击，从而采取相应的处理措施。 » 目的警戒值 - 指定设备收到的DNS递归查询报文的个数的警戒值。如果一秒钟内设备收到的到达同一个目的IP地址且相同端口号的DNS查询报文个数超过该警戒值，设备就判断为受到DNS查询洪水攻击，从而采取相应的处理措施。 » 行为 - 指定设备对DNS递归查询洪水攻击采取的行为。如果选择默认行为“丢弃”，在发生攻击的当前秒和下一秒这段时间内，设备仅允许指定个数（警戒值）的DNS递归查询报文通过，并且发出警报，在这段时间内的其它同类包将会被丢弃；如果选择“告警”，系统将在发现DNS递归查询洪水攻击后发出警报但是允许DNS查询报文通过。

5. 如果需要恢复系统的默认配置，点击“恢复缺省”按钮。
6. 点击“确定”按钮保存所做配置。

第8章 监控

监控模块对通过设备的流量进行统计分析。将统计分析的结果以多维度多样式进行展示。

系统提供多种监控项目，包括：

- **用户监控**：展示指定时间周期内（实时、最近1小时、最近1天、最近1月）每用户的统计信息，包括使用的应用、产生的流量、以及并发连接个数。
- **应用监控**：展示指定时间周期内（实时、最近1小时、最近1天、最近1月）每应用的统计信息，包括使用的用户、产生的流量、以及并发连接个数。
- **URL访问**：展示指定时间周期内（实时、最近1小时、最近1天、最近1月）用户/IP访问URL的统计信息，以及被访问URL的统计信息。
- **设备监控**：展示指定时间周期内（实时、最近1小时、最近1天、最近1月）整机流量、接口流量、安全域、硬件状态、以及在线IP数的统计信息。
- **认证用户**：展示通过"用户" 在第73页中用户绑定认证的用户及其信息。

用户可对监控项目进行开启或关闭，也可自定义监控项目：

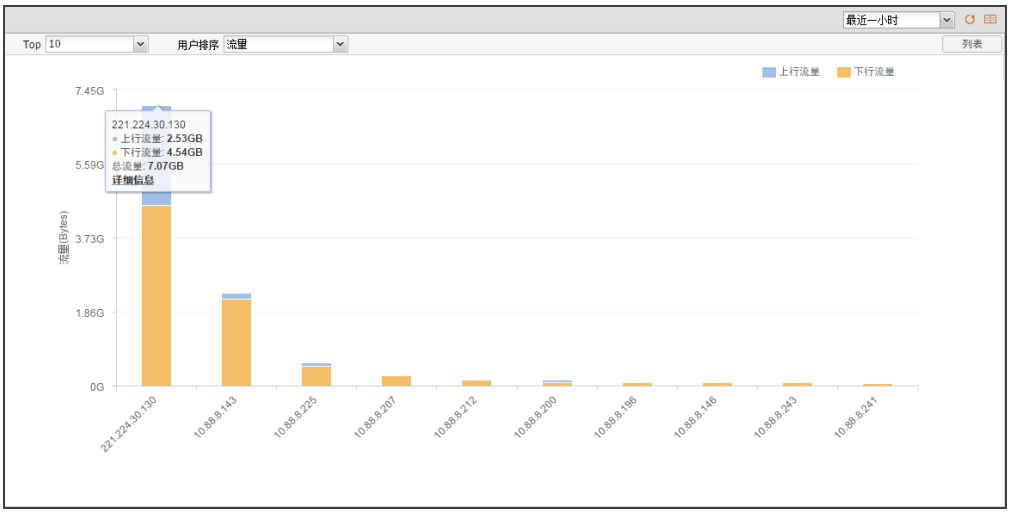
- **监控配置**：开启或者关闭指定监控项目。
- **自定义监控**：用户可自行定义监控项目并查看统计信息。

用户监控

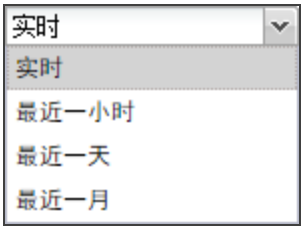
用户监控展示指定时间周期内（实时、最近1小时、最近1天、最近1月）每用户的统计信息，包括使用的应用、产生的流量、以及并发连接个数。

概览

点击“监控 > 用户监控 > 概览”，此页面展示用户的统计信息的概览。



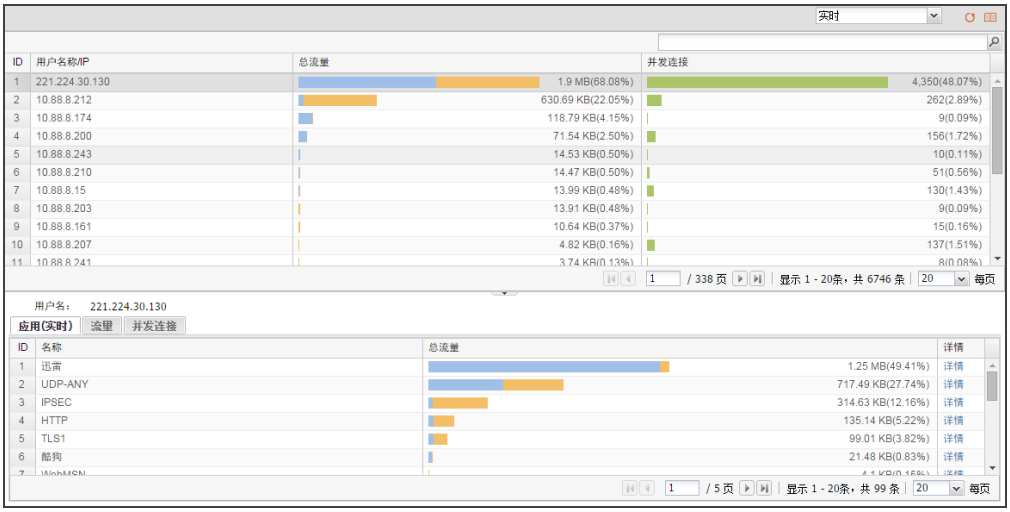
- 点击“TOP”下拉菜单，选择参与排序的用户的个数。
- 点击“用户排序”下拉菜单，选择排序的依据。
- 通过选择不同的统计周期，可以查看不同时间范围内的统计信息。



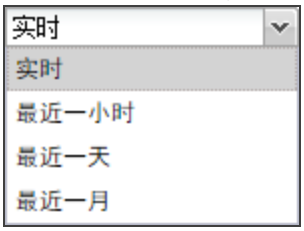
- 点击  刷新页面监控数据。
- 点击  将统计信息切换到列表展示。
- 用户排序方式为“流量”时，鼠标悬停在某用户对应的柱状图上，查看该用户的上行流量、下行流量、以及总流量。点击“详细信息”跳转到用户详情页面。
- 用户排序方式为“并发连接”时，鼠标悬停在某用户对应的柱状图上，查看该用户的实时并发连接。点击“详细信息”跳转到用户详情页面。

用户详情

点击“监控 > 用户监控 > 用户详情 “，此页面展示所有用户的详细统计信息。



- 通过选择不同的统计周期，可以查看不同时间范围内的统计信息。



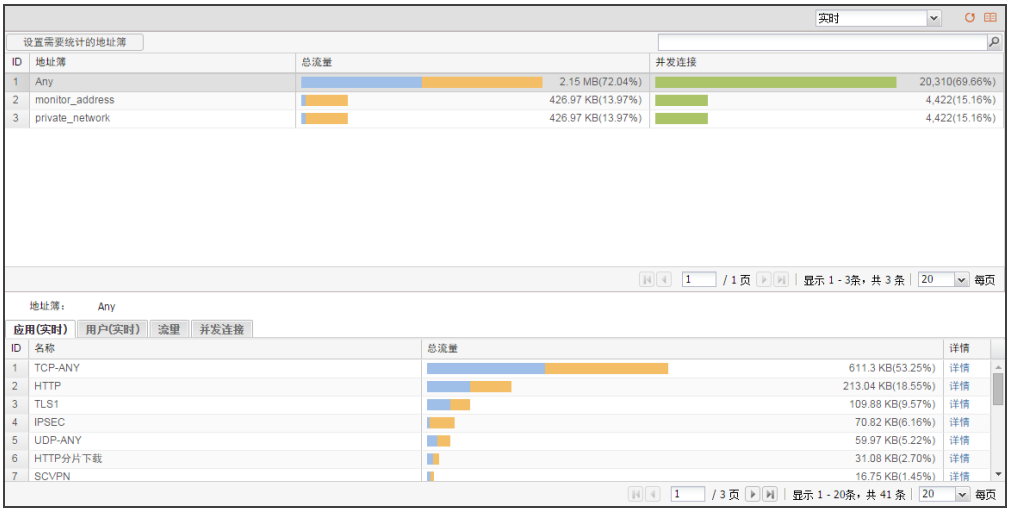
- 点击  刷新页面监控数据。

- 在列表右上方文本框中输入用户名称或IP地址，然后点击  ，系统将显示指定用户的详细统计信息。

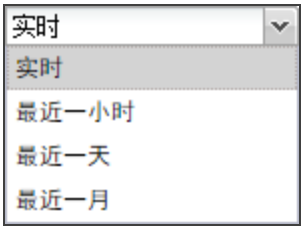
- 在用户列表中选定某一用户条目，列表下方显示所选用户名称，并且可以进一步查看该用户的详细统计信息。
  - 点击<应用(实时)> 标签页，显示所选用户使用的各应用的上行流量、下行流量、总流量。点击“详情”，查看此应用的采样周期（30s）内平均速率趋势图。
  - 点击<流量> 标签页，显示所选用户的采样周期（30s）内平均速率趋势图。
  - 点击<并发连接> 标签页，显示所选用户的并发连接趋势图。

地址簿详情

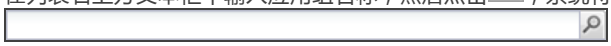
点击”监控 > 用户监控 > 地址簿详情 “，此页面展示所选地址簿的详细统计信息。



- 点击“设置需要统计的地址簿”按钮，打开配置对话框将需要统计的地址簿移入右侧列表并点击“确定”。
- 通过选择不同的统计周期，可以查看不同时间范围内的统计信息。



- 点击  刷新页面监控数据。
- 在列表右上方文本框中输入应用组名称，然后点击  ，系统将显示被搜索的地址簿统计信息。



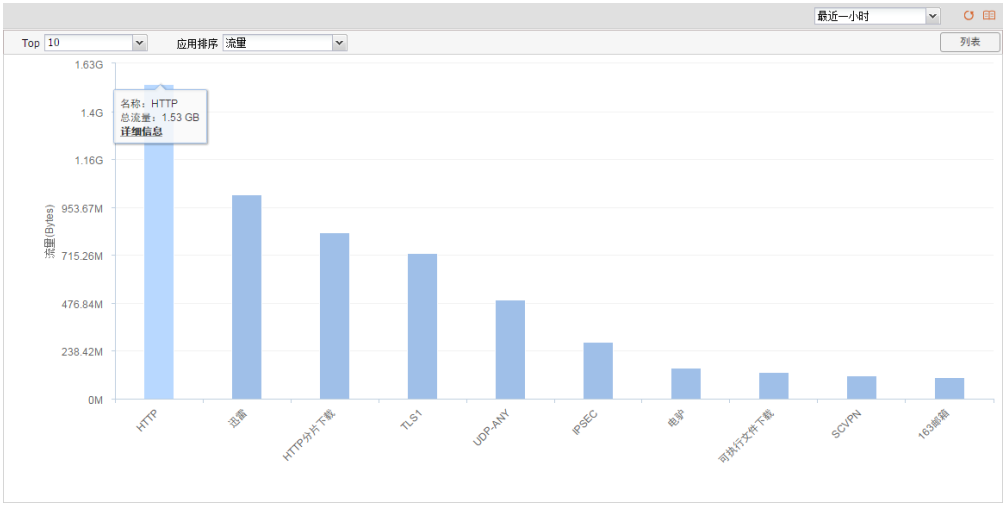
- 在地址簿列表中选定某一地址簿条目，列表下方显示所选地址簿名称，并且可以进一步查看该地址簿的详细统计信息。
  - 点击<应用(实时)> 标签页，显示所选地址簿使用的各应用的上行流量、下行流量、以及总流量。点击“详情”，查看此应用的采样周期（30s）内平均速率趋势图。
  - 点击<用户(实时)> 标签页，显示所选地址簿中各用户的上行流量、下行流量、以及总流量。点击“详情”，查看此用户的采样周期（30s）内平均速率趋势图。
  - 点击<流量> 标签页，显示所选地址簿的采样周期（30s）内平均速率趋势图。
  - 点击<并发连接> 标签页，显示所选地址簿的并发连接趋势图。

应用监控

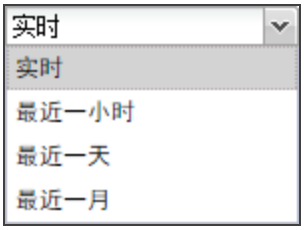
应用监控展示指定时间周期内（实时、最近1小时、最近1天、最近1月）每应用的统计信息，包括使用的用户、产生的流量、以及并发连接个数。

概览

点击“监控 > 应用监控 > 概览”，此页面展示应用的统计信息的概览。



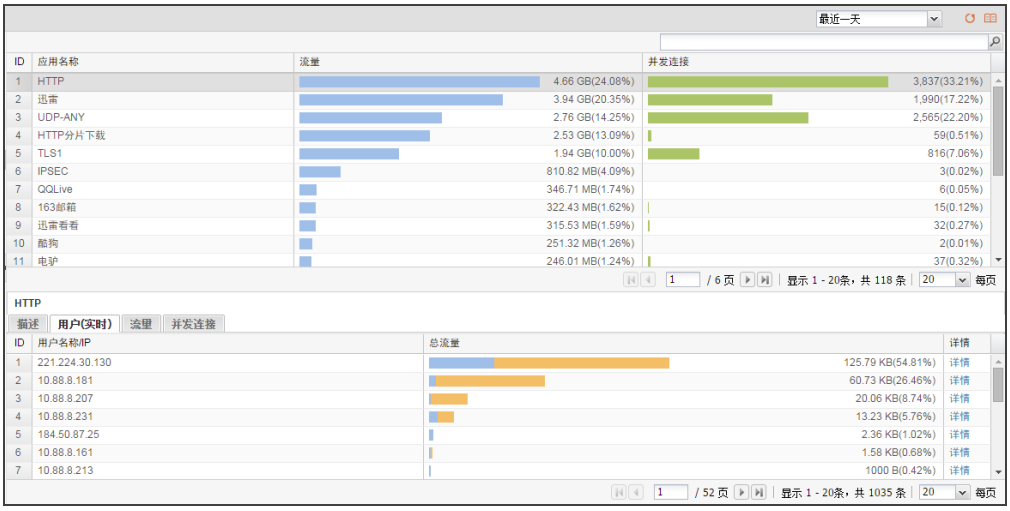
- 点击“TOP”下拉菜单，选择参与排序的应用的个数。
- 点击“应用排序”下拉菜单，选择排序的依据。
- 通过选择不同的统计周期，可以查看不同时间范围内的统计信息。



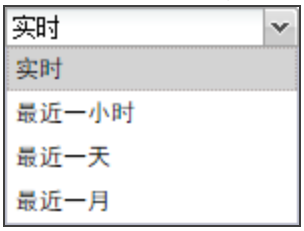
- 点击  刷新页面监控数据。
- 点击  将统计信息切换到列表展示。
- 应用排序方式为“流量”时，鼠标悬停在某应用对应的柱状图上，查看该应用的总流量。点击“详细信息”跳转到应用详情页面。
- 应用排序方式为“并发连接”时，鼠标悬停在某应用对应的柱状图上，查看该应用的总流量。点击“详细信息”跳转到应用详情页面。

应用详情

点击”监控 > 应用监控 > 应用详情 “，此页面展示所有应用的详细统计信息。



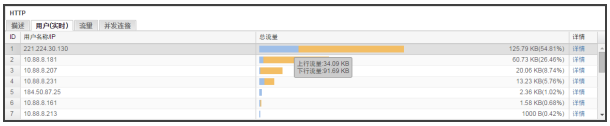
- 通过选择不同的统计周期，可以查看不同时间范围内的统计信息。



- 点击  刷新页面监控数据。

- 在列表右上方文本框中输入应用名称，然后点击  ，系统将显示指定应用的详细统计信息。

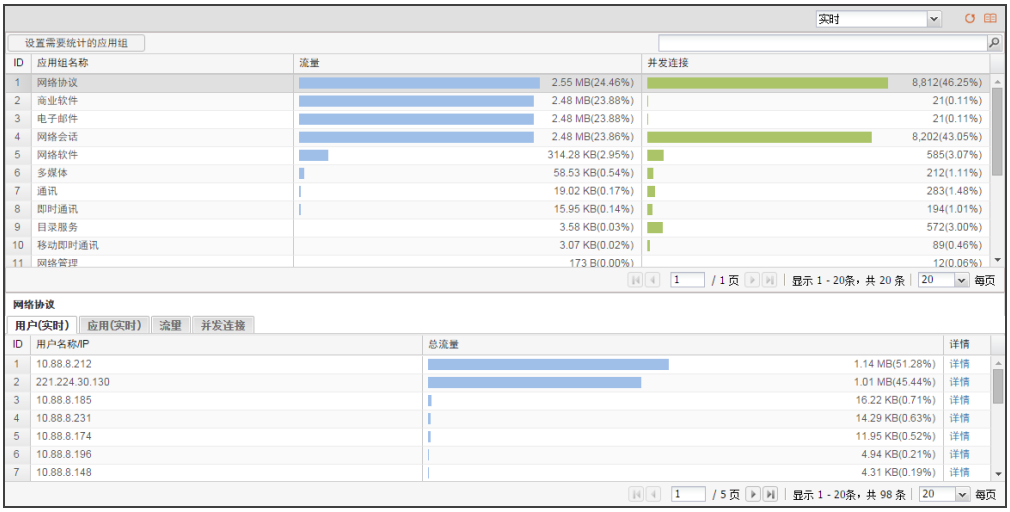
- 在应用列表中选定某一应用条目，列表下方显示所选应用名称，并且可以进一步查看该应用的详细统计信息。
  - 点击<描述>标签页，显示所选应用的描述详细信息。
  - 点击<用户(实时)>标签页，显示使用所选应用的每用户的上行流量、下行流量、以及总流量。点击“详情”，查看此用户的采样周期（30s）内平均速率趋势图。



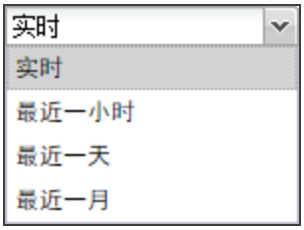
  - 点击<流量>标签页，显示所选应用的采样周期（30s）内平均速率趋势图。。
  - 点击<并发连接>标签页，显示所选应用的并发连接趋势图。

应用组详情

点击”监控 > 应用监控 > 应用组详情 “，此页面展示所选应用组的详细统计信息 。



- 点击“设置需要统计的应用组”按钮，打开配置对话框将需要统计的应用组移入右侧列表并点击“确定”。
- 通过选择不同的统计周期，可以查看不同时间范围内的统计信息。



- 点击  刷新页面监控数据。
- 在列表右上方文本框中输入应用组名称，然后点击  ，系统将显示被搜索的应用组统计信息。

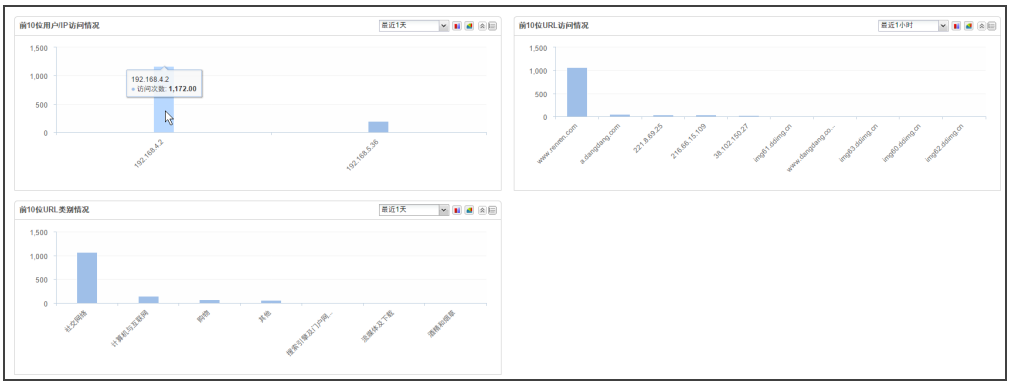
- 在应用组列表中选定某一应用组条目，列表下方显示所选应用组名称，并且可以进一步查看该应用组的详细统计信息。
  - 点击<用户(实时)>标签页，显示使用所选应用组的用户的上行流量、下行流量、总流量。点击“详情”，查看此用户的采样周期（30s）内平均速率趋势图。
  - 点击<应用(实时)>标签页，显示应用组内各应用的总流量。点击“详情”，查看此应用的采样周期（30s）内平均速率趋势图。
  - 点击<流量>标签页，显示所选应用组的采样周期（30s）内平均速率趋势图。
  - 点击<并发>标签页，显示所选应用组的并发连接趋势图。

URL访问

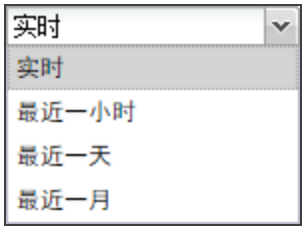
系统配置"URL过滤" 在第102页功能后，URL访问展示指定时间周期内（实时、最近1小时、最近1天、最近1月）用户/IP访问URL的统计信息，以及被访问URL的统计信息。

概览

点击“监控 > URL访问 > 概览”，此页面展示前10位用户/IP访问情况、前10位URL访问情况、以及前10位URL类别访问情况。



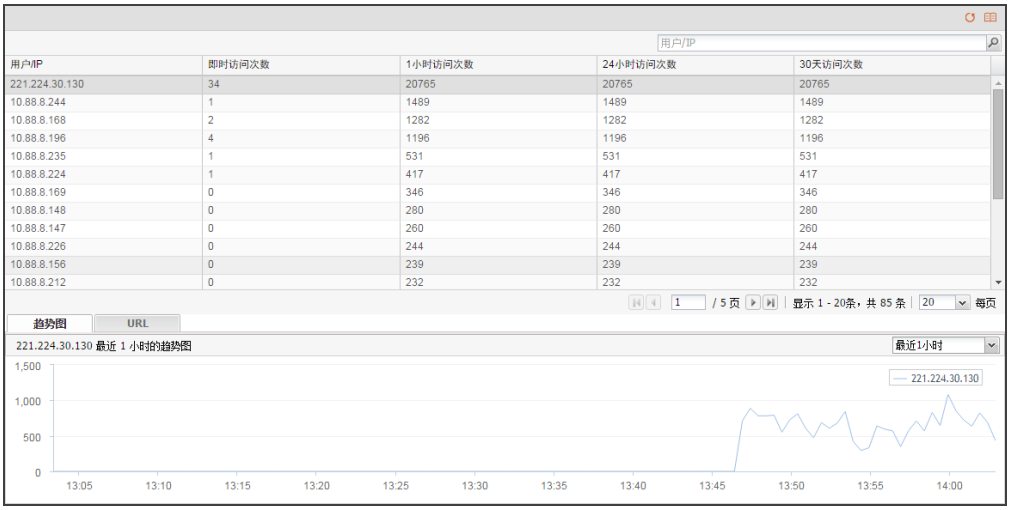
- 通过选择不同的统计周期，可以查看不同时间范围内的统计信息。



- 鼠标悬停在某用户/IP、URL或URL类别对应的柱状图上，查看该用户/IP、URL或URL类别的访问次数。
- 点击各图表右上角图标，进入对应的详情页面。
- 点击各图表右上角 图标用于将统计图在柱状图和饼状图之间切换。

用户/IP

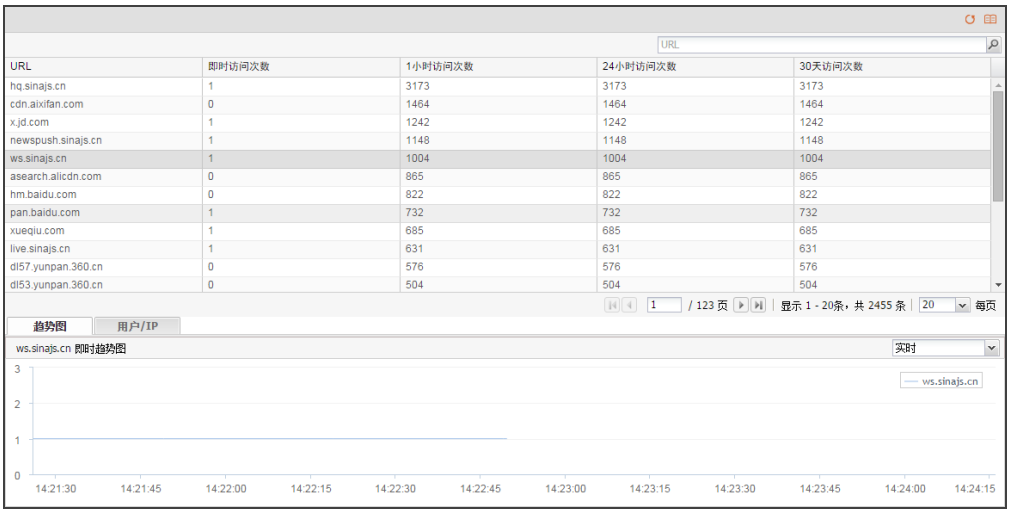
点击“监控 > URL访问 > 用户/IP”或者点击概览页面“前10位用户/IP访问情况”图表右上角图标，进入用户/IP统计页面。



- 该页面上方以列表方式列出用户/IP在不同时间段内访问URL的统计数据。
- 在页面右上方“用户/IP”文本框中输入需要搜索的用户/IP，列表将显示对应用户/IP的访问次数数据。
- 点击  刷新页面监控数据。
- 在列表中选择某一用户/IP，列表下方显示此用户/IP的URL访问次数趋势图以及访问的URL。在<URL>标签页，点击某一条目对应的  ，查看对应的访问次数趋势变化。

URL

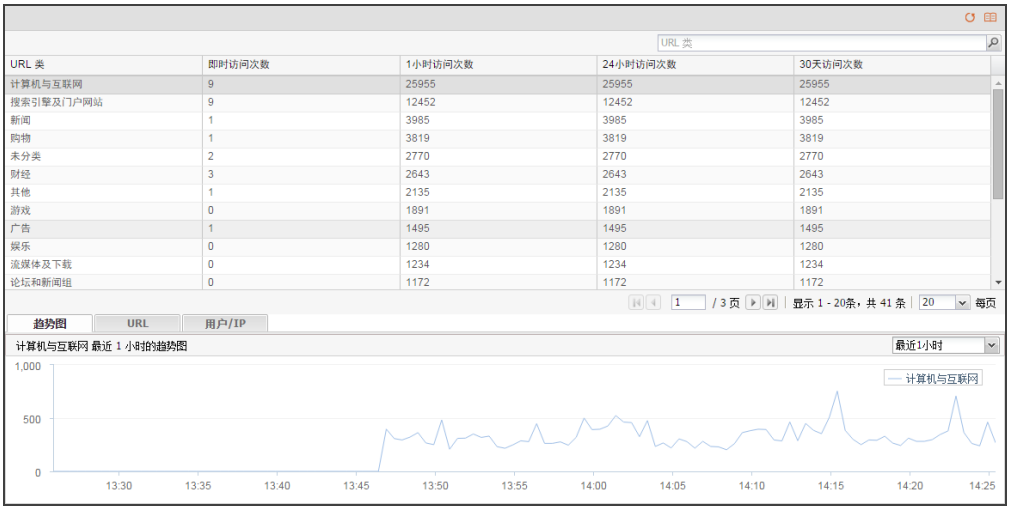
点击“监控 > URL访问 > URL”或者点击概览页面“前10位URL访问情况”图表右上角  图标，进入URL统计页面。



- 该页面上方以列表方式列出URL在不同时间段内被访问次数的统计数据。
- 在页面右上方“URL”文本框中输入需要搜索的URL，列表将显示对应的URL访问次数信息。
- 点击  刷新页面监控数据。
- 在列表中选择某一URL，列表下方显示此URL被访问次数趋势图以及访问此URL的用户/IP。在<用户/IP>标签页，点击某一条目对应的  ，查看对应的访问次数趋势变化。

URL类别

点击“监控 > URL访问 > URL类别”或者点击概览页面“前10位URL类别情况”图表右上角  图标，进入URL类别统计页面。



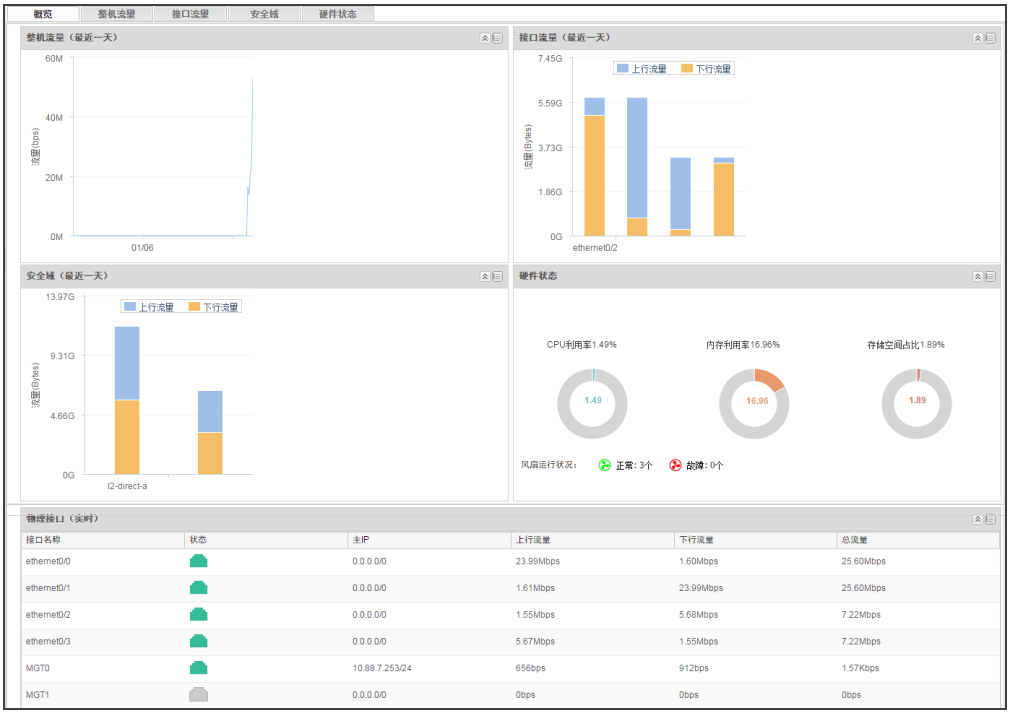
- 该页面上方以列表方式列出URL类别在不同时间段内被访问次数的统计数据。
- 在页面右上方“URL类”文本框中输入需要搜索的URL类别，列表将显示对应的URL类别访问次数信息。
- 点击  刷新页面监控数据。
- 在列表中选择某一URL类别，列表下方显示此URL类别被访问次数趋势图、此类别中的URL的即时访问次数、以及访问此URL类别的用户/IP的即时访问次数。在<用户/IP>和<URL>标签页，点击某一条目对应的  ，查看对应的访问次数趋势变化。

设备监控

设备监控展示指定时间周期内（实时、最近1小时、最近1天、最近1月）整机流量、接口流量、安全域、硬件状态、以及在线IP数的统计信息。

概览

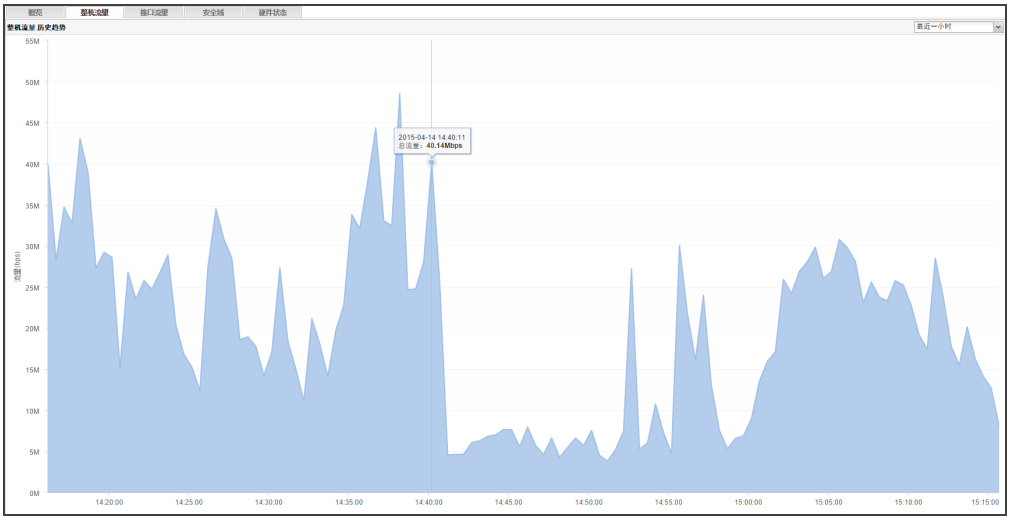
点击“监控 > 设备监控 > 概览”，展示最近1天的整机流量、接口流量、安全域、硬件状态的统计信息，以及实时的物理接口的状态、IP、流量统计信息。



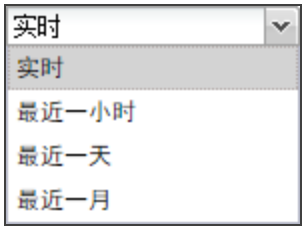
- 整机流量：显示设备最近1天内的10分钟内速率平均值的趋势图。鼠标悬停在曲线图上，查看对应时刻的10分钟内速率平均值。
- 接口流量：显示设备所使用的接口最近1天内的上行、下行以及总流量信息。鼠标悬停在某一柱形图上，查看对应接口的流量统计信息。
- 安全域：显示设备各安全域最近1天内的上行、下行以及总流量信息。鼠标悬停在某一柱形图上，查看对应安全域的流量统计信息。
- 硬件状态：显示设备的实时硬件状态，包括CPU利用率、内存利用率、存储空间利用率、和风扇状态。
- 物理接口（实时）：显示设备所有接口的统计信息，包括接口状态、主IP、实时上行速率、实时下行速率、以及实时总速率。
- 点击各图表右上角图标，进入对应的详情页面。

整机流量

点击<整机流量>标签页或者点击概览页面整机流量图表右上角图标，进入整机流量页面。该页面通过曲线图展示指定时间周期内的整机速率平均值的趋势图。

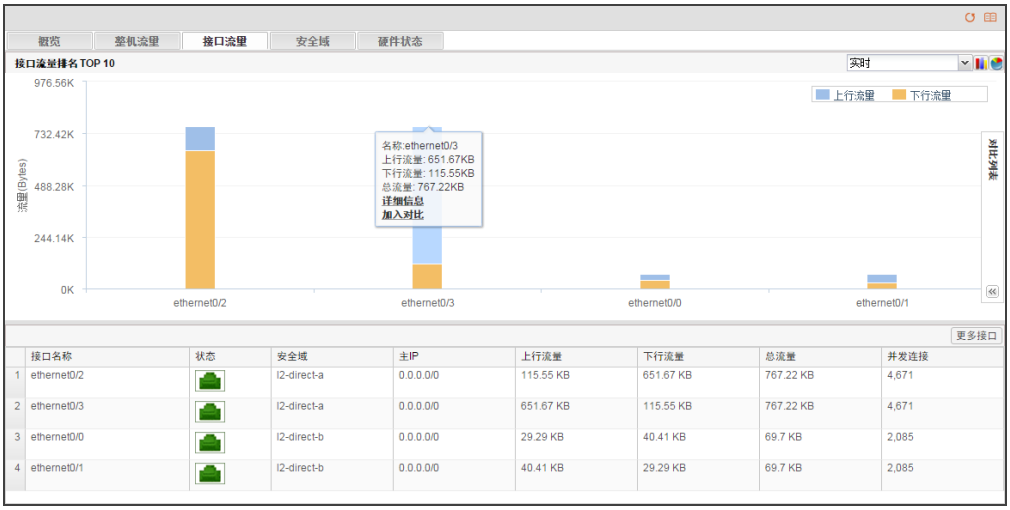


- 鼠标悬停在曲线图上，查看对应时刻的整机速率平均值。
- 通过选择不同的统计周期，可以查看不同时间范围内的统计信息。

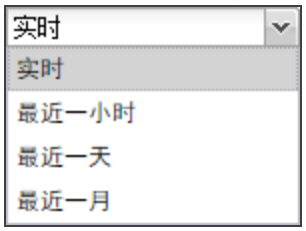


接口流量

点击<接口流量>标签页或者点击概览页面接口流量图表右上角图标，进入接口流量页面。该页面上方通过柱状图显示接口流量排名前10位的接口及其流量信息，页面下方以列表方式列出接口的状态、所属安全域、主IP、上行流量、下行流量、流量及并发连接。



- 通过选择不同的统计周期，可以查看不同时间范围内的统计信息。

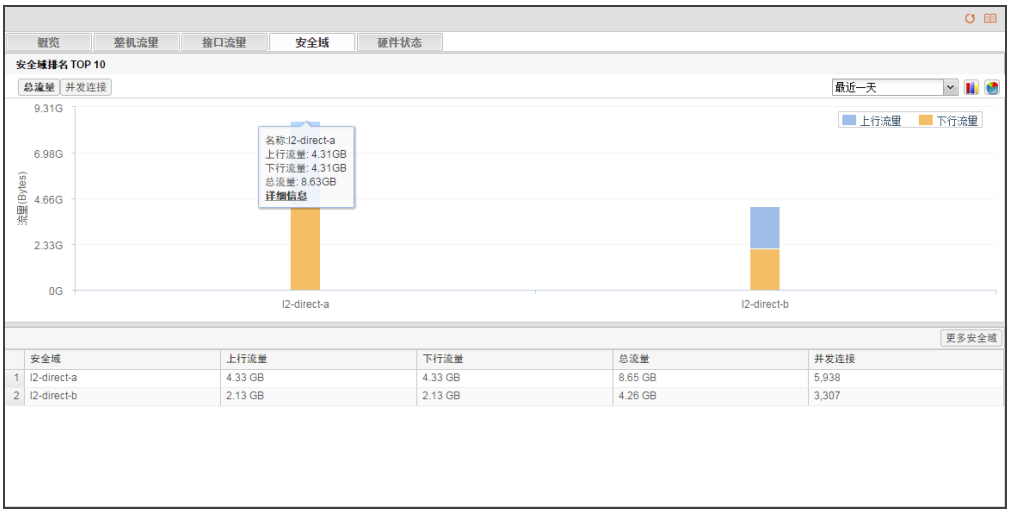


- 页面右上角  图标用于将统计图在柱状图和饼状图之间切换。
- 在图例中点击“上行流量”或“下行流量”，展示接口上行流量或下行流量的统计数据。

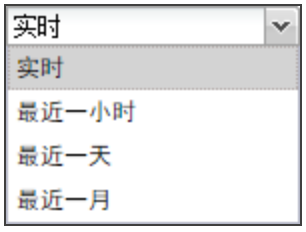
- 点击页面下方接口列表右上角的“更多接口”，进入全部接口信息页面，查看所有接口的统计信息。
- 鼠标悬停在某接口对应的柱状图上，查看该接口的流量信息。
  - 点击“详细信息”，进入此接口的详细信息页面，查看该接口的流量历史趋势、并发连接历史趋势、用户流量排名及指定用户流量历史趋势、应用流量排名及指定应用流量历史趋势。
  - 点击“加入对比”，将此接口加入到右侧对比列表中。在对比列表中点击“进入对比”，即可在弹出的趋势对比窗口中查看各个接口的流量历史趋势和并发连接历史趋势的比较。

安全域

点击<安全域>标签页或者点击概览页面安全域流量图表右上角  图标，进入安全域流量页面。该页面上方通过柱状图显示安全域流量排名前10位的安全域及其流量信息。页面下方以列表方式列出安全域流量及并发连接相关信息。



- 通过选择不同的统计周期，可以查看不同时间范围内的统计信息。

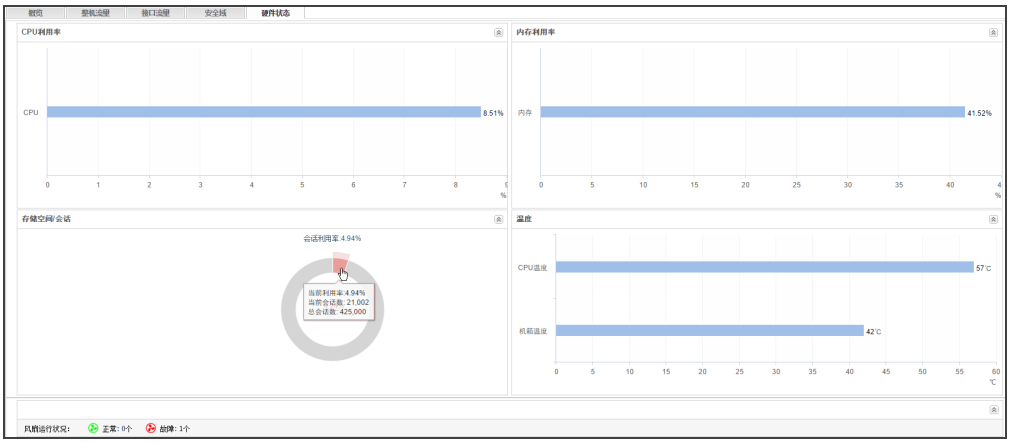


- 页面右上角  图标用于将统计图在柱状图和饼状图之间切换。
- 在图例中点击“上行流量”或“下行流量”，展示安全域上行流量或下行流量的统计数据。

- 页面左上角“总流量”和“并发连接”按钮用于切换统计图表显示的统计数据。
- 点击页面下方安全域列表右上角的“更多安全域”，进入全部安全域信息页面，查看所有安全域的统计信息。
- 鼠标悬停在某安全域对应的柱状图上，查看该安全域的流量或并发连接信息。点击“详细信息”，进入此安全域的详细信息页面，查看该安全域的流量历史趋势、并发连接历史趋势、用户流量排名及指定用户流量历史趋势、应用流量排名指定应用流量历史趋势。

硬件状态

点击<硬件状态>标签页或者点击概览页面硬件状态图表右上角  图标，进入硬件状态页面。该页面通过柱状图显示CPU利用率和内存利用率，通过饼图显示存储空间占比、会话利用率，通过列表显示风扇运行情况。将鼠标悬停在对应的图表上，查看相应的详细信息。



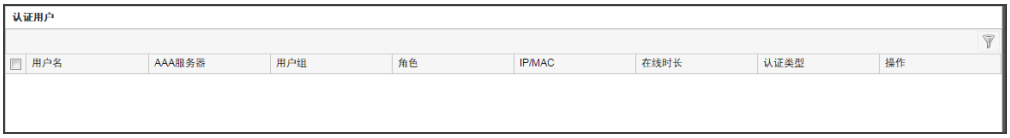
在线IP数

点击“监控 > 设备监控 > 在线IP数”，此页面展示指定时间周期内（最近1小时、最近1天、最近1月）的在线用户数的历史趋势统计信息。鼠标悬停在曲线图上，查看对应时刻的在线用户IP数信息。

认证用户

系统配置"用户" 在第73页中的用户绑定后，认证用户展示通过用户绑定认证的用户及其信息。

点击“监控>认证用户”，此页面显示通过用户绑定认证的用户及其信息



- 点击 ，指定搜索条件：选择AAA服务器，或输入用户名。点击 进行搜索。点击 清楚搜索条件。点击 关闭搜索。

- 在列表中“操作”栏点击“踢出”可使对应的用户掉线。

监控配置

用户可以根据需要开启或者关闭部分监控项目。

开启或者关闭监控项目，请按照以下步骤进行操作：

1. 点击“监控>监控配置”。

2. 选中监控项目对应的复选框开启对应的监控项目；取消选中监控项目的复选框关闭对应的监控项目。认证用户项目在配置用户绑定后自动开启。

3. 配置完成，点击“确定”按钮保存所做配置。

注意：“设备监控、用户监控、应用监控”默认开启。由于报表模块中网络数据来源于监控模块，如果关闭某项将导致关闭时间段内报表中该项也会没有对应记录。

自定义监控

通过自定义监控，用户可自行定义监控项目并查看统计信息。

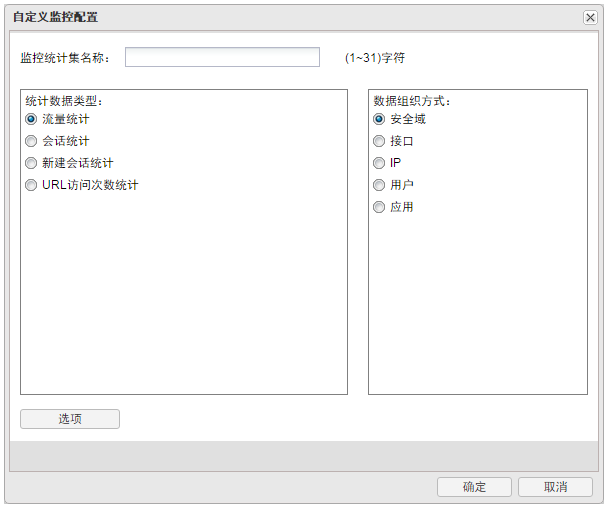
点击“监控>自定义监控”，此页面展示所有监控的名称、状态、统计数据类型以及数据组织方式。

- 点击“新建”按钮，新建自定义监控。
- 点击“名称”列中的链接，查看自定义监控的统计信息。

新建自定义监控

新建自定义监控，按照以下步骤进行操作：

1. 点击”监控>自定义监控“。
2. 点击“新建”按钮。



在<自定义监控配置>对话框中进行配置。

选项	说明
监控统计集名称	指定将要创建的自定义监控的名称。
统计数据类型	选择监控的数据类型。
数据组织方式	选择数据的组织方式。此自定义监控将根据选择的组织方式对数据进行组织与展示。 当统计数据类型为流量统计、会话统计、或者新建会话统计时，选择**IP**组织方式时后，点击“高级”进行高级配置。
选项	用户可以为自定义监控配置过滤条件，以统计符合特定条件的数据，比如统计某个特定安全域的会话数、统计某个特定目的IP的流量等。配置过滤条件，点

统计范围	描述
不限制	不进行限制。
发起者	根据监控的数据类型，统计发起会话的IP的数据。
回应者	根据监控的数据类型，统计接收会话的IP的数据。
属于安全域	根据监控的数据类型，统计属于某安全域的IP的数据。
不属于安全域	根据监控的数据类型，统计不属于某安全域的IP的数据。
属于接口	根据监控的数据类型，统计属于某接口的IP的数据。
不属于接口	根据监控的数据类型，统计不属于某接口的IP的数据。

<table>
<tr><th>选项</th><th>说明</th></tr>
<tr><td></td><td>击“选项”按钮，弹出<高级配置>对话框，在该对话框添加过滤条件。
<table><tr><th>类型</th><th>描述</th></tr><tr><td>安全域</td><td>以安全域为条件进行过滤</td></tr><tr><td>安全域-流入</td><td>以入安全域为条件进行过滤</td></tr><tr><td>安全域-流出</td><td>以出安全域为条件进行过滤</td></tr><tr><td>接口</td><td>以接口为条件进行过滤</td></tr><tr><td>接口-流入</td><td>以入接口为条件进行过滤</td></tr><tr><td>接口-流出</td><td>以出接口为条件进行过滤</td></tr><tr><td>服务</td><td>以应用为条件进行过滤</td></tr><tr><td>地址条目</td><td>以地址条目为条件进行过滤</td></tr><tr><td>地址簿-源</td><td>以源地址（地址条目）为条件进行过滤</td></tr><tr><td>地址簿-目的</td><td>以目的地址（地址条目）为条件进行过滤</td></tr><tr><td>IP/掩码</td><td>以IP为条件进行过滤</td></tr><tr><td>IP/掩码-源</td><td>以源IP为条件进行过滤</td></tr><tr><td>IP/掩码-目的</td><td>以目的IP为条件进行过滤</td></tr><tr><td>角色</td><td>以角色名称为条件进行过滤</td></tr><tr><td>用户</td><td>以用户名称为条件进行过滤</td></tr><tr><td>用户组</td><td>以用户组名称为条件进行过滤</td></tr></table></td></tr>
</table>

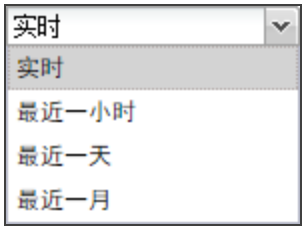
3. 配置完成，点击“确定”按钮。系统将返回自定义监控页面。配置的自定义监控将显示在列表中。

注意: 自定义统计集时，URL访问次数统计数据类型仅对安装有URL许可证的用户可用。

查看自定义监控的统计信息

在自定义监控页面的列表中点击某个自定义监控的名称，将打开对应的标签页，显示相应的统计信息。

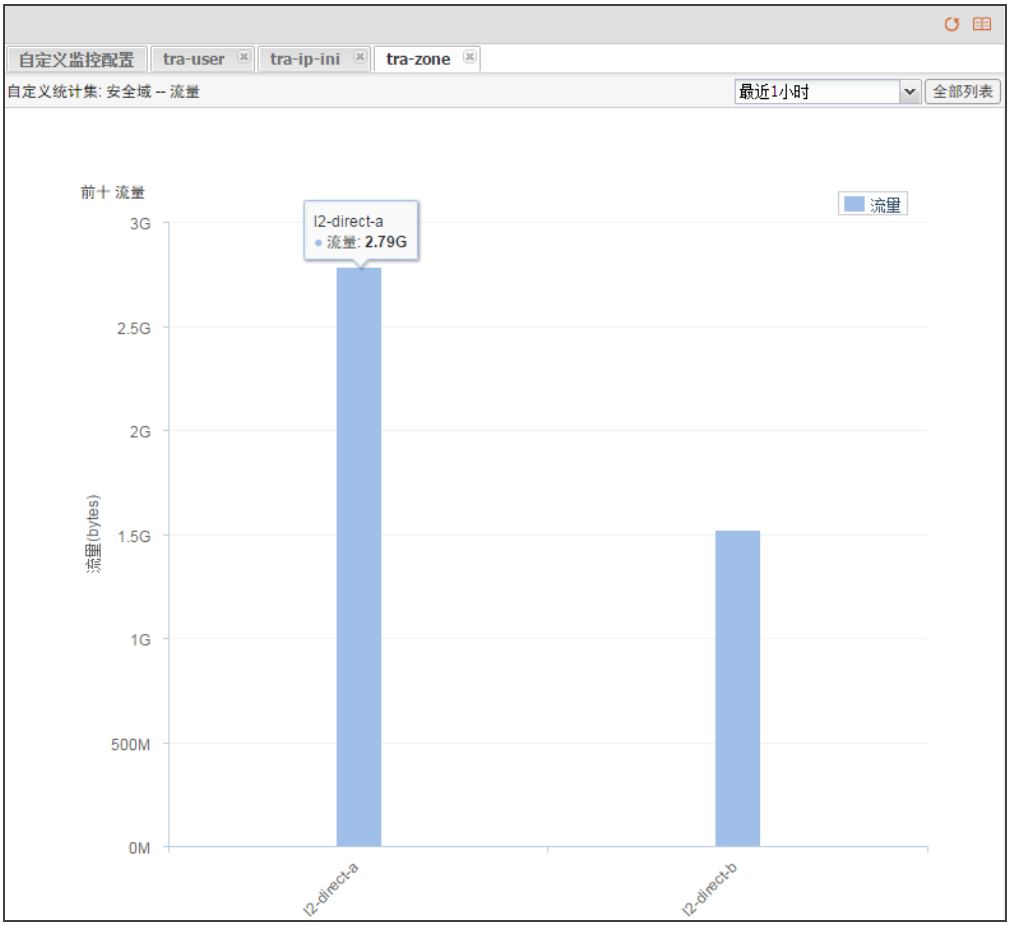
- 通过柱状图查看排名前十的统计信息。
- 通过选择不同的统计周期，可以查看不同时间范围内的统计信息。



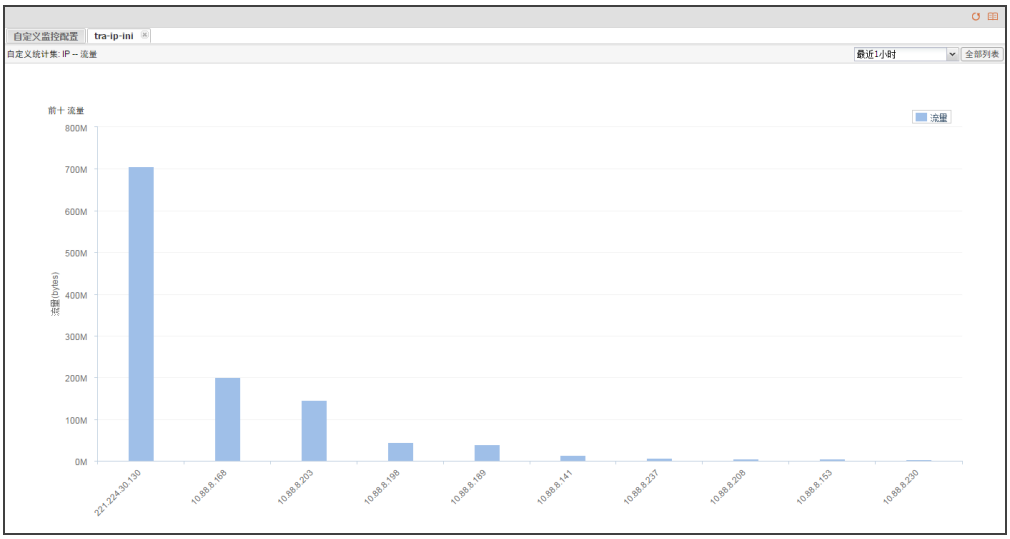
- 点击“全部列表”，以列表方式展示全部统计信息。此列表下方展示趋势图；点击“前十数据”查看柱状图。。

自定义监控配置示例及结果展示：

统计数据类型为**流量统计**，数据组织方式为**安全域**。监控结果为：流量排名前十的安全域的统计信息：



统计数据类型为**流量统计**，数据组织方式为**IP**，并在“高级”设置中选择“发起者”。监控结果为：在发起会话的IP中流量排名前十的IP的统计信息：



第9章 报表

报表模块对如下报表项的相关数据进行统计和分析，为用户提供全方位、多角度的统计报告：

报表项	说明
安全风险概览	帮助用户快速全面的了解业务、用户及风险的整体状况。
安全风险详情	详细说明业务和用户的受攻击、威胁情况。
威胁类型汇总	详细说明本设备检测到的威胁情况、影响范围，并给出相应的解决方案。
网络流量分析	分析展示用户、应用、接口、安全域的流量和并发情况。
系统运行状况	列举本设备的CPU、内存、硬盘等资源使用情况。

用户可通过"自定义任务" 在第161页和"快捷任务" 在第163页制定报表任务，通过"业务系统" 在第165页划分内网区域，在"报表汇总" 在第160页中查看生成的报表。

注意: 在监控配置中，“设备监控、用户监控、应用监控”默认开启。由于报表模块中网络数据来源于监控模块，如果关闭某项将导致关闭时间段内报表中该项也会没有对应记录。

报表汇总

用户可以在报表汇总页面查看已生成的报表文件。点击“报表 > 报表汇总”，打开报表汇总页面。

- 点击文件类型列中的 图标，预览PDF格式的报表。
- 点击“标记为已读”按钮，修改选中的报表文件状态为已读。
- 点击“删除”按钮，删除所选的报表文件。

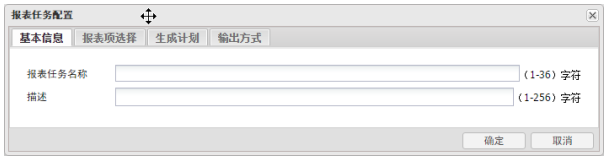
自定义任务

用户可以在设备上按照需求配置自定义任务。自定义任务可包含任意报表项。

新建自定义任务

新建报表自定义任务，请按照以下步骤进行操作：

1. 点击“报表 > 自定义任务”。
2. 点击“新建“按钮，弹出<报表任务配置>对话框。



在<报表任务配置>对话框，填写自定义任务配置信息。

基本信息	
报表任务名称	指定报表任务的名称。
描述	指定报表任务的描述信息。
报表项选择	
报表项选择	指定报表的内容： 1. 从左侧的“所有类别”列表中选中报表类别。 2. 点击“添加”按钮。添加选中报表类别到“已选择的报表项”列表中。
生成计划	
生成计划	指定报表任务的生成时间。可按周期生成，也可立即生成。 周期计划：按计划生成报表。 » 周期类型：根据指定周期内的数据生成报表。可根据最近一天、最近一周、最近一月、最近一季、最近半年、以及最近一年的数据生成报表。 » 生成时间：根据周期类型不同，可选择每天生成一次、每周生成一次、每月生成一次、每季生成一次、每半年生成一次、以及每年生成一次。 立即生成：立即生成报表。 » 在时间文本框中指定数据的采集周期。
输出方式	
报表格式	报表文件的格式为PDF格式。
收件人	使用邮件发送报表文件。添加报表文件收件人邮件地址，可以直接在“收件人”文本框中输入邮件地址（若有多个收件人，邮件之间以分号“;”隔开）。

3. 点击“完成”按钮完成配置。

查看报表文件

查看报表文件，请点击“报表 > 报表汇总”。

注意: 如果浏览器设置了禁止弹出窗口，将不能弹出生成的报表。请开启“一直允许弹窗”功能，或者在浏览器的阻断窗口记录中查看生成的报表文件。

快捷任务

快捷任务是设备预定义报表任务，每一个报表任务都根据一个报表项的名称进行命名，且只提供该报表项对应的报表。

快捷任务包括如下报表任务：

- 安全风险概览
- 安全风险详情
- 威胁类型汇总
- 网络流量分析
- 系统运行状况

报表名称	描述	动作
安全风险概览	帮助用户快速全面的了解业务、用户及风险的整体状况。	
安全风险详情	详细说明业务和用户的受攻击、威胁情况。	
威胁类型汇总	详细说明本设备检测到的威胁情况、影响范围，并给出相应的解决方案。	
网络流量分析	分析展示用户、应用、接口、安全域的流量、并发情况。	
系统运行状况	列举本设备的CPU、内存、硬盘等资源使用情况。	

配置快捷任务

配置快捷任务，请按照以下步骤进行操作：

1. 点击“报表 > 快捷任务”。
2. 在某个报表名称对应的“动作”列中，点击 按钮，弹出<报表任务配置>对话框。

   在<报表任务配置>对话框，填写自定义任务配置信息。

基本信息	
报表任务名称	显示报表任务的名称。
描述	显示报表任务的描述信息。 用户可自行修改。
生成计划	
生成计划	指定报表任务的生成时间。可按周期生成，也可立即生成。 周期计划：按计划生成报表。 » 周期类型：根据指定周期内的数据生成报表。可根据最近一天、最近一周、最近一月、最近一季、最近半年、以及最近一年的数据生成报表。 » 生成时间：根据周期类型不同，可选择每天生成一次、每周生成一次、每月生成一次、每季生成一次、每半年生成一次、以及每年生成一次。 立即生成：立即生成报表。 » 在时间文本框中指定数据的采集周期。
输出方式	
报表格式	报表文件的格式为PDF格式。
收件人	使用邮件发送报表文件。添加报表文件收件人邮件地址，可以直接在“收件人”文本框中输入邮件地址（若有多个收件人，邮件之间以分号“;”隔开）。

3. 点击“完成”按钮完成配置。

查看报表文件

查看报表文件，请点击“报表 > 报表汇总”。

注意: 如果浏览器设置了禁止弹出窗口，将不能弹出生成的报表。请开启“一直允许弹窗”功能，或者在浏览器的阻断窗口记录中查看生成的报表文件。

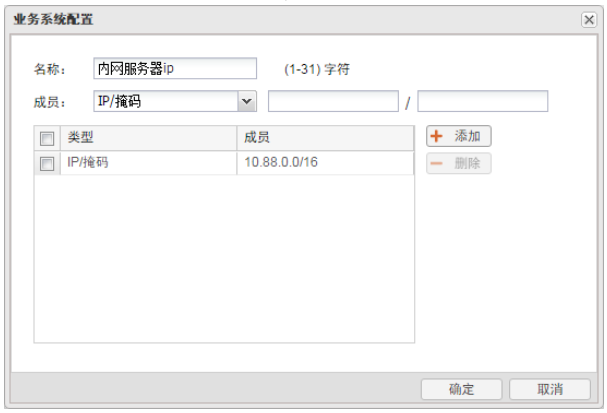
业务系统

通过指定业务系统的名称及其IP地址，可对内网区域进行标识和逻辑划分。在安全风险概览和安全风险详情报表项中，将对配置的业务系统的安全风险进行展示。

配置业务系统

配置业务系统，请按照以下步骤进行操作：

1. 点击“报表 > 业务系统”。
2. 点击“新建”按钮，弹出<业务系统配置>对话框。



在<业务系统配置>对话框，填写自定义任务配置信息。

选项	说明
名称	输入业务系统名称。
成员	指定业务系统成员的IP地址。
添加	点击“添加”按钮，添加此成员。

3. 点击“确定”完成配置。

在报表中查看业务系统的安全风险

业务系统的安全风险在报表中的展示示例（业务系统名称为“内网服务器ip”）：

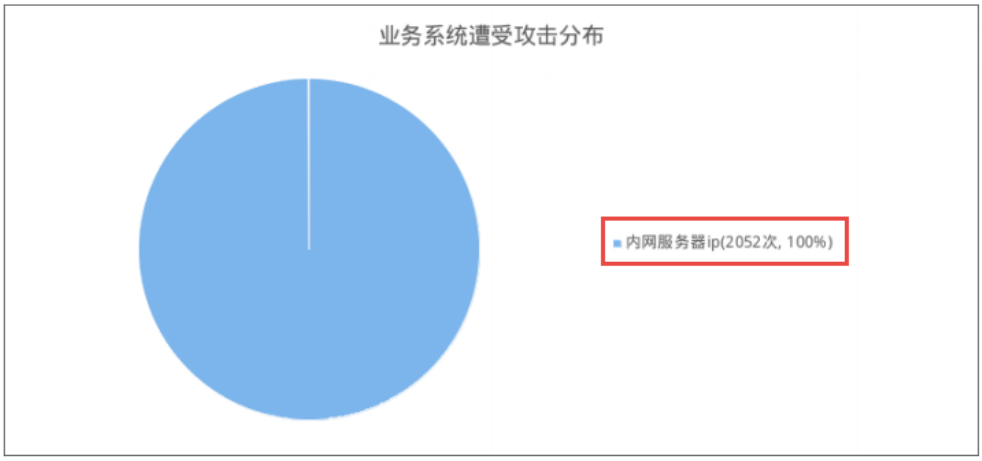
» 在安全风险概览报表项中查看业务系统的安全风险：

1. 安全风险概览

2016-01-10至2016-01-11期间，共发生威胁攻击2052次，平均每天发生2052次，其中致命等级攻击41次，危险等级攻击219次，轻微等级攻击1792次，主要涉及内网服务器ip等业务系统。主要的攻击类型包括访问控制攻击，WEB攻击，网络钓鱼等。业务系统和用户面临较高的攻击频率，需要进行紧急安全防护和漏洞修补。

1.1. 业务安全概览

统计期间，业务系统共遭受攻击2052次，其中内网服务器ip占比100%。具体的分布图如下：



遭受攻击最多的业务系统详情如下：

#	业务系统 (IP)	攻击类型(次)	次	百分比
1	内网服务器ip	访问控制攻击(1401), WEB攻击(639), 网络钓鱼(8), 扫描攻击(3), 恶意软件(1)	2052	100%

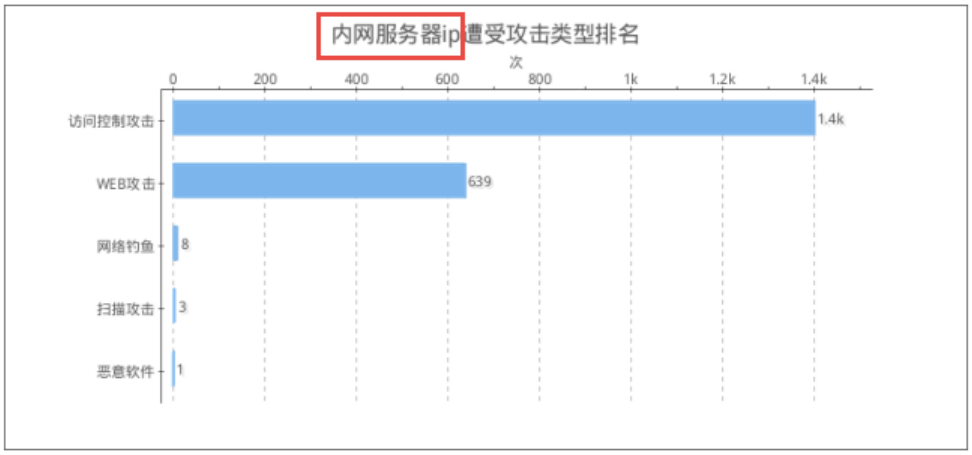
» 在安全风险详细报表项中查看业务系统的安全风险：

2. 安全风险详情

2.1. 业务安全分析

2.1.1. 内网服务器ip受攻击分析

统计期间，内网服务器ip共遭受攻击2052次，其中访问控制攻击占比68.27%，WEB攻击占比31.14%，网络钓鱼占比0.39%。具体的排名如下：



对内网服务器ip发起攻击的IP地址详情如下

#	攻击源	攻击类型(次)	次	百分比
1	163.177.83.187	访问控制攻击(501)	501	24.42%
2	221.224.30.130	WEB攻击(265), 访问控制攻击(2)	267	13.01%
3	10.88.8.247	访问控制攻击(185)	185	9.02%
4	10.88.8.250	WEB攻击(161)	161	7.85%

第10章 日志

日志模块记录并展示如下日志信息：

- 威胁日志 - 与威胁防护相关的日志信息，包括病毒过滤日志、入侵防御日志、以及攻击防护日志。
- 设备系统日志 - 包含事件日志、网络日志以及配置日志。
  - 事件 - 与系统本身相关的日志，例如登录日志、ARP日志。
  - 网络 - 与网络服务相关的日志，例如DHCP日志、路由日志。
  - 配置 - 与配置相关的日志，例如接口配置日志。
- 会话日志 - 与会话相关的日志，记录会话的协议、源/目的IP地址、源/目的端口等。
- NAT日志 -与NAT行为相关的日志，记录NAT类型、源/目的IP地址、源/目的端口等。
- URL日志 - 与上网行为相关的日志，记录用户的上网时间和网页访问情况、URL过滤等。

日志的严重等级

系统日志的严重等级可分为8级，关于各级的具体信息，请参阅下表：

级别	级别号	描述
紧急（Emergencies）	0	系统不可用信息。
警报（Alerts）	1	需要立即处理的信息，如设备受到攻击等。
严重（Critical）	2	危急信息，如硬件出错。
错误（Errors）	3	错误信息。
警告（Warnings）	4	报警信息。
通告（Notifications）	5	非错误信息，但需要特殊处理。
信息（Informational）	6	通知信息。
调试（Debugging）	7	调试信息，包括正常的使用信息。

日志信息输出目的地

日志信息可以输出到不同的目的地，设备支持以下7种日志信息输出目的地，用户可以根据自己的需要指定：

- Console - 日志信息的默认输出目的地。用户可以通过命令关闭此输出.
- 终端（Remote）- 包括Telnet和SSH两种终端。
- 内存缓存（Buffer）- 内存缓存。
- 文件（File）- 默认情况下，系统会生成一个文件记录日志信息，用户可以指定将信息输出到USB口的文件中。
- 系统日志服务器（Syslog Server）- 系统可以将日志信息发往 UNIX 或 Windows Syslog Server。
- Email地址 - 将日志信息发送到某个邮件地址。

日志信息格式

为方便用户查阅和分析系统日志信息，系统按照固定的格式输出日志信息。该格式为：**时间，级别@模块：日志描述**。请参阅以下示例：

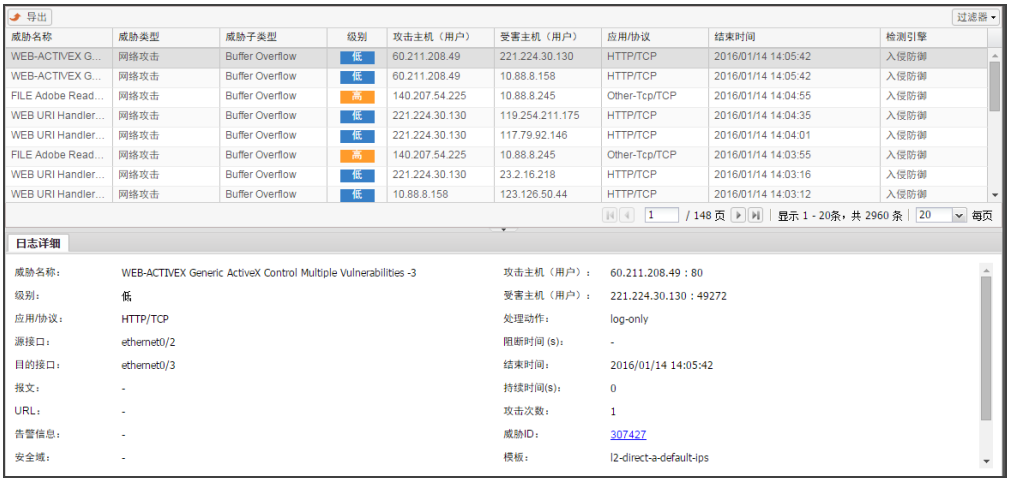
2013-02-05 01:51:21, WARNING@LOGIN: Admin user "admin" logged in through console from localhost.

威胁日志

威胁日志的产生需要满足以下条件：

- 已经开启设备的威胁日志功能。具体配置请参阅"日志管理" 在第174页。
- 已经配置"病毒过滤" 在第131页、"入侵防御" 在第116页、"攻击防护" 在第135页或功能。具体功能请参阅相关页面。

点击“日志 > 威胁日志”，打开威胁日志页面。

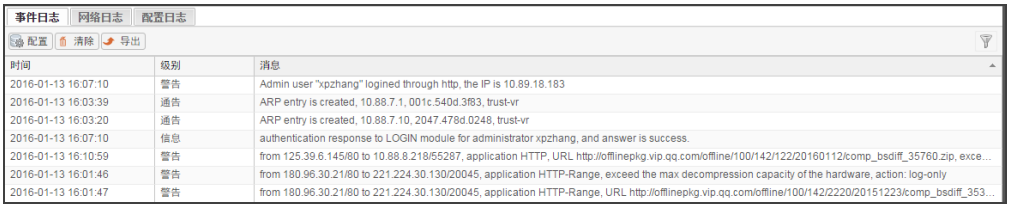


- 点击右上角“过滤器”下拉菜单，指定威胁日志过滤条件。点击“查询”按键搜索特定的日志条目。点击“重置”按键重置所有过滤条件。过滤条件如下：
  - 查询时间 - 显示指定时间段的威胁日志。
  - 威胁类型 - 显示指定威胁类型的威胁日志。
  - 级别 - 显示指定威胁级别的威胁日志。
  - 攻击主机（用户） - 显示指定攻击主机的威胁日志。
  - 受害主机（用户） - 显示指定受害主机的威胁日志。
  - 检测引擎 - 显示指定检测引擎的威胁日志。检测引擎包括入侵防御、攻击防护、以及病毒过滤。
  - 源接口 - 显示指定源接口的威胁日志。
  - 目的接口 - 显示指定目的接口的威胁日志。
  - 处理动作 - 显示指定处理动作的威胁日志。
- 导出：导出所有系统存储的威胁日志或者搜索结果（先进行搜索后再导出）。导出过程中设置的分隔符主要用于将导出的日志导入其他审计系统。
- 选中列表中的日志条目，在列表下方<日志详细>标签页中查看该日志的详细信息。

设备系统日志

用户可以在设备系统日志页面查看事件日志、网络日志和配置日志。

点击“日志 > 设备系统日志”，打开设备系统日志页面。



- 点击<事件日志>、<网络日志>或<配置日志>标签，在日志列表中查看相应的日志。
- 配置：点击该按钮，进入日志管理相关页面对日志进行配置。
- 清除：点击该按钮，清除所有日志。
- 导出：点击该按钮，导出所有系统存储的设备系统日志或者搜索结果（先进行搜索后再导出）。导出过程中设置的分隔符主要用于将导出的日志导入其他审计系统。
- 在<事件日志>标签页，点击 设置过滤条件。在“级别”下拉菜单中指定级别，点击 搜索指定级别的日志。点击 取消搜索结果。
- 在<配置日志>标签页，在右上角文本框中输入需要查询的管理员名称，点击 搜索指定管理员的日志。

会话日志

会话日志的产生需要满足以下两个条件：

- 已经开启设备的会话日志功能。具体配置请参阅"日志管理" 在第174页。
- 已经为策略规则开启日志记录功能。具体配置请参阅"安全策略" 在第81页页面。

点击“日志 > 会话日志”，打开会话日志页面。

- 点击右上角  设置过滤条件，在下列下拉菜单中指定过滤条件。指定过滤条件后，点击  搜索指定级别的日志。点击  取消搜索结果。
  - 时间 - 显示指定时间范围（开始时间、结束时间）的会话日志。
  - 策略ID - 显示指定ID策略规则的会话日志。
  - 源IP - 显示指定源IP地址的会话日志。
  - 源端口 - 显示指定源端口的会话日志。
  - 目的IP - 显示指定目的IP的会话日志。
  - 目的端口 - 显示指定目的端口的会话日志。
  - 协议 - 显示指定协议的会话日志。
  - 行为 - 显示指定行为的会话日志。
- 配置：点击该按钮，进入"日志管理" 在第174页相关页面对会话日志进行配置。
- 清除：点击该按钮，清除所有系统存储会话日志。
- 导出：点击该按钮，导出所有系统存储的会话日志或者搜索结果（先进行搜索后再导出）。导出过程中设置的分隔符主要用于将导出的日志导入其他审计系统。

注意:

- 对于ICMP会话，系统会在日志中记录ICMP报文的类型和代码值（ICMP type-value,code-value）。ICMP 3、4、5、11和12类型报文是由其他通讯触发的，并未创建完整的ICMP会话，因此会话日志不会记录这类ICMP报文。
- 对于TCP和UDP会话，设备首先会检查TCP和UDP报文的长度。如果报文长度为20字节（即，只有IP报头但无负载），设备会判断为畸形报文并直接丢弃；如果报文长度大于20字节，设备会检查报文中的校验和字段并直接丢弃校验和错误的报文。因此，会话日志不会记录上述类型的畸形TCP和UDP报文。

NAT日志

NAT日志的产生需要满足以下两个条件：

- 已经开启设备的NAT日志功能。具体配置请参阅"日志管理" 在第174页。
- 已经为NAT规则开启NAT日志功能。具体配置请参阅"配置源NAT" 在第85页以及"配置目的NAT" 在第88页。

点击“日志 > NAT日志信息”，打开NAT日志页面。

- 点击右上角设置过滤条件，在下列下拉菜单中指定过滤条件。指定过滤条件后，点击搜索指定级别的日志。点击取消搜索结果。
  - 时间 - 显示指定时间范围（开始时间、结束时间）的NAT日志。
  - NAT类型 - 显示指定类型（源NAT、目的NAT）的NAT日志。
  - 规则ID - 显示指定ID的NAT日志。
  - 源IP - 显示指定源IP地址的NAT日志。
  - 源端口 - 显示指定源端口的NAT日志。
  - 目的IP - 显示指定目的IP的NAT日志。
  - 目的端口 - 显示指定目的端口的NAT日志。
  - 转换后IP - 显示指定转换后IP地址的NAT日志。
  - 转换后端口 - 显示指定转换后端口号的NAT日志。
  - 协议 - 显示指定协议的NAT日志。
- 配置：点击该按钮，进入日志管理相关页面对NAT日志进行配置。
- 清除：点击该按钮，清除所有系统存储NAT日志。
- 导出：点击该按钮，导出所有系统存储的NAT日志或者搜索结果（先进行搜索后再导出）。导出过程中设置的分隔符主要用于将导出的日志导入其他审计系统。

URL日志

URL日志的产生需要满足以下条件：

- 已经开启设备的URL日志功能。具体配置请参阅"日志管理" 在第174页。
- 已经为URL过滤规则开启日志记录功能。具体配置请参阅"URL过滤" 在第102页。

点击“日志 > URL日志”，打开URL日志页面。

- 在右上角设置过滤条件。设置后，点击 搜索符合过滤条件的日志。
  - 源IP - 显示指定源IP地址的URL日志。
  - 关键字 - 显示包含指定关键字的URL日志。
- 配置：点击该按钮，进入日志管理相关页面对URL日志进行配置。
- 清除：点击该按钮，清除所有系统存储URL日志。
- 导出：点击该按钮，导出所有系统存储的URL日志或者搜索结果（先进行搜索后再导出）。导出过程中设置的分隔符主要用于将导出的日志导入其他审计系统。

日志管理

用户可以在日志管理界面配置各种类型日志、日志服务器、Web邮件以及设备名称的相关选项。

配置日志选项

配置各类型日志的选项，请按照以下步骤进行操作：

1. 点击“日志 > 日志管理”，打开日志管理页面。
2. 根据需要，选择<威胁日志>/<事件日志>/<网络日志>/<配置日志>/<会话日志>/<NAT日志>/<URL日志>标签页，配置相应的日志选项。

威胁日志

选项	说明
启用	选中该复选框，开启系统的威胁日志功能。
终端	选中该复选框将威胁日志选项输出到终端。 » 最小日志级别 - 指定输出威胁日志的最小日志级别。
缓存	选中该复选框将威胁日志输出到缓存。 » 最小日志级别 - 指定输出威胁日志的最小日志级别。 » 最大缓存大小 - 指定输出威胁日志的最大缓存大小。
文件	选中该复选框将威胁日志输出到文件。 » 最小日志级别 - 指定输出威胁日志的最小日志级别。 » 最大文件大小 - 指定输出威胁日志文件的最大值。 » 储存日志到USB - 选中该复选框将日志文件保存到U盘。从下拉菜单中选择U盘，在“文件名”文本框输入威胁日志的文件名称。
日志服务器	选中该复选框将威胁日志输出到日志服务器。 » 最小日志级别 - 指定输出威胁日志的最小日志级别。 » 日志分发方式 - 日志以明文方式进行发送。 » 使用分布式日志 - 将威胁日志分布式发送到多个日志服务器，缓解单台日志服务器的压力。系统通过指定的算法选定日志服务器，可选择算法有“轮询方式外发”和“按源IP Hash方式外发。 » 查看日志服务器 - 点击该链接查看所有已配置的日志服务器。
Email地址	选中该复选框将威胁日志输出到Email地址。 » 最小日志级别 - 指定输出威胁日志的最小日志级别。 » 查看Email地址：点击该链接查看所有已配置的Email地址。

事件日志

选项	说明
启用	选中该复选框，开启系统的事件日志功能。
Console	选中该复选框将事件日志输出到Console。 » 最小日志级别 - 指定输出事件日志的最小日志级别。
终端	选中该复选框将事件日志输出到终端。

选项	说明
	» 最小日志级别 - 指定输出事件日志的最小日志级别。
缓存	选中该复选框将事件日志输出到缓存。 » 最小日志级别 - 指定输出事件日志的最小日志级别。 » 最大缓存大小 - 指定输出事件日志的最大缓存大小。
文件	选中该复选框将事件日志输出到文件。 » 最小日志级别 - 指定输出事件日志的最小日志级别。 » 最大文件大小 - 指定事件日志文件的最大值。 » 储存日志到USB - 选中该复选框将日志文件保存到U盘。从下拉菜单中选择U盘，在“文件名”文本框输入事件日志的文件名称。
日志服务器	选中该复选框将事件日志输出到日志服务器。 » 查看日志服务器 - 点击该链接查看所有已配置的日志服务器。 » 最小日志级别 - 指定输出事件日志的最小日志级别。
Email地址	选中该复选框将事件日志输出到Email地址。 » 查看Email地址：点击该链接查看所有已配置的Email地址。 » 最小日志级别 - 指定输出事件日志的最小日志级别。

网络日志

选项	说明
启用	选中该复选框，开启系统的网络日志功能。
缓存	选中该复选框将网络日志输出到缓存。 » 最大缓存大小 - 指定输出网络日志的最大缓存大小。
文件	选中该复选框将网络日志输出到文件。 » 最大文件大小 - 指定网络日志文件的最大值。 » 储存日志到USB - 选中该复选框将日志文件保存到U盘。从下拉菜单中选择U盘，在“文件名”文本框输入网络日志的文件名称。
日志服务器	选中该复选框将网络日志输出到日志服务器。 » 查看日志服务器 - 点击该链接查看所有已配置的日志服务器。

配置日志

选项	说明
启用	选中该复选框，开启系统的配置日志功能。
缓存	选中该复选框将配置日志输出到缓存。 » 最大缓存大小 - 指定输出配置日志的最大缓存大小。
日志服务器	选中该复选框将配置日志输出到日志服务器。 » 查看日志服务器 - 点击该链接查看所有已配置的日志服务器。
日志限速	选中该复选框指定配置日志输出最大速率。 » 最大速率 - 指定输出配置日志的最大速率。

会话日志

选项	说明
启用	选中该复选框，开启系统的会话日志功能。 » 记录用户名：在会话日志中显示用户名称。 » 记录主机名：在会话日志中显示主机名称。
缓存	选中该复选框将会话日志输出到缓存。 » 最大缓存大小 - 指定输出会话日志的最大缓存大小。
日志服务器	选中该复选框将会话日志输出到日志服务器。 » 查看日志服务器 - 点击该链接查看所有已配置的日志服务器。 » 日志分发方式 - 选择发送的日志类型，包括明文日志和二进制日志。 » 使用分布式日志 - 将会话日志分布式发送到多个日志服务器，缓解单台日志服务器的压力。系统通过指定的算法选定日志服务器，可选择算法有“轮询方式外发”和“按源IP Hash方式外发

NAT日志

选项	说明
启用	选中该复选框，开启系统的NAT日志功能。 » 记录主机名：在NAT日志中显示主机名称。
缓存	选中该复选框将NAT日志输出到缓存。 » 最大缓存大小 - 指定输出NAT日志的最大缓存大小。
日志服务器	选中该复选框将NAT日志输出到日志服务器。 » 查看日志服务器 - 点击该链接查看所有已配置的日志服务器。 » 日志分发方式 - 选择发送的日志类型，包括明文日志和二进制日志。 » 使用分布式日志 - 将NAT日志分布式发送到多个日志服务器，缓解单台日志服务器的压力。系统通过指定的算法选定日志服务器，可选择算法有“轮询方式外发”和“按源IP Hash方式外发

URL日志

选项	说明
启用	选中该复选框，开启系统的URL日志功能。 » 记录主机名：在URL日志中显示主机名称。
缓存	选中该复选框将URL日志输出到缓存。 » 最大缓存大小 - 指定输出URL日志的最大缓存大小。
日志服务器	选中该复选框将URL日志输出到日志服务器。 » 查看日志服务器 - 点击该链接查看所有已配置的日志服务器。 » 日志分发方式 - 选择发送的日志类型，包括明文日志和二进制日志。 » 使用分布式日志 - 将URL日志分布式发送到多个日志服务器，缓解单台日志服务器的压力。系统通过指定的算法选定日志服务器，可选择算法有“轮询方式外发”和“按源IP Hash方式外发

3. 配置完成后点击“确定”按钮。

配置日志服务器

用户可以在<日志服务器配置>对话框新建、编辑或删除用于接收日志的日志服务器。

新建日志服务器，请按照以下步骤进行操作：

1. 在日志管理页面右上角点击“配置”菜单选择“日志服务器配置”，打开<日志服务器配置>对话框。
2. 点击“新建”按钮，打开<日志服务器配置>对话框。

在<日志服务器配置>对话框，配日志服务器相关信息。

选项	说明
主机名称	指定日志服务器的IP地址或域名。
绑定方式	指定发送日志的源IP地址。 » 源接口：选择发送日志的源接口，设备会以指定接口的IP地址为发送日志的源IP地址。如果该接口配有管理IP地址，优先使用管理IP地址。请确保存在相关的路由条目使日志可以从源接口转发到日志服务器。
协议	选择与日志服务器通讯的协议，包括TCP、UDP、以及Secure-TCP。 当选择“Secure-TCP”协议时，设备将与日志服务器通过SSL加密日志。设备在与日志服务器建立SSL连接时，客户可选择是否验证服务器证书。 » 如需验证服务器证书，需要将第三方日志服务器的CA证书导入到设备的trust_domain_default信任域。如果日志服务器为HSM（Hillstone Security Management），设备已经在trust_domain_default中预置CA证书，因此不需要手工导入CA证书。 » 如果不需要验证服务器证书，选择“不验证服务器证书”复选框。
端口	输入日志服务器的端口号。
日志类型	选择该日志服务器接收的日志的类型。

3. 点击“确定”按钮，保存当前页面所做配置。

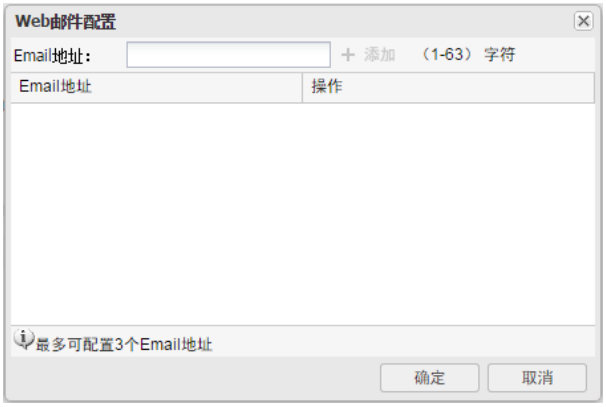
注意: 用户最多允许配置15台日志服务器。

配置Web邮件

Web邮件配置用于指定接收日志邮件的Email地址。

Web邮件配置，请按照以下步骤进行操作：

1. 在日志管理页面右上角点击“配置”菜单选择“Web邮件配置”，打开<Web邮件配置>对话框。



2. 在<Email地址>文本框中输入用于接收日志邮件的Email地址，点击“添加”按钮，将Email地址添加到列表中。
3. 如果需要删除，在Email列表对应Email条目的“操作”栏中点击“删除”按钮。
4. 点击“确定”按钮，保存当前页面所做配置。

注意: 用户最多允许配置3台Email地址。

配置设备名称

用于指定UNIX日志服务器的名称。该选项仅适用于将日志输出到UNIX日志服务器。

设备名称配置，请按照以下步骤进行操作：

1. 在日志管理页面右上角点击"配置"菜单选择“设备名称配置”，打开<设备名称配置>对话框。

2. 选中指定设备名称单选按钮，日志将输出到该UNIX日志服务器。
3. 点击“确定”按钮，保存当前页面所做配置。

第11章 高可靠性

高可靠性（High Availability），简称为HA，能够在通信线路或设备产生故障时提供备用方案，从而保证数据通信的畅通，有效增强网络的可靠性。当一台设备不可用或者不能处理来自客户端的请求时，该请求会及时转到另外的可用设备来处理，这样就保证了网络通信的不间断进行，极大地提高了通信的可靠性。

实现HA功能，用户需要两台设备组成HA簇，这两台设备需要采用完全相同的硬件平台，安装相同的R版本固件，安装相同的可证、安装相同的板卡。

设备支持Active-Passive（A/P）模式进行HA组网。使用Active-Passive（A/P）模式时，在HA簇中配置两台设备组成一个HA组，组内只有一台主设备。主设备处于活动状态，转发报文，同时将其所有网络和配置信息以及当前会话信息传递给备份设备。当主设备出现故障时，备份设备接替主设备工作，转发报文。这种A/P模式具有较强冗余性，而且其网络结构简单，便于维护管理。

HA基础概念

HA簇

HA簇是实现HA功能的设备的组合。对于外部网络设备而言，一个HA簇是一个单一的设备，处理网络流量和提供安全服务。HA簇通过簇ID进行标识。为设备指定HA簇ID后，设备进入HA状态，执行HA功能。

HA组

系统会对HA簇中相同HA组ID的设备，按照HCMP协议，根据设备的HA配置，进行主备选举。主设备处于活动状态处理网络流量，而当主设备出现故障时，其它设备代替主设备继续工作。当为设备设置簇ID时，组ID为0的HA组会自动创建。在Active-Passive（A/P）模式中，设备仅具有HA组0。

HA组接口和虚拟MAC

在HA环境中，每个HA组都具有接口，流量通过接口进行传输。每个HA组的主设备维护对应接口的虚拟MAC（VMAC）地址，流量通过这些具有VMAC地址的接口进行转发。VMAC地址由簇ID、HA组ID以及物理接口索引确定。

HA选举

HA簇中，拥有同样HA组ID的具有高优先级的设备会被选举为HA组的主设备。

HA同步

为保证备份设备能够在主设备失效时代替主设备工作，主设备需要与备用设备进行同步。同步的信息类型有三种：配置信息、文件以及RDO（Runtime Dynamic Object）。RDO的具体内容主要包括：

- 会话信息（以下类型会话信息不会同步：到设备本身的会话、Deny Session、ICMP会话以及tentative会话）
- DNS缓存映射条目
- ARP表
- DHCP信息
- MAC表

系统使用两种方法进行同步，分别是实时同步和批量同步。当主设备刚刚选举成功时，系统会使用批量同步方法，将主设备信息全部同步到备份设备；当配置发生变化时，系统将使用实时同步的方法将变化的信息同步到备份设备。除HA相关配置和本地配置（例如，主机名称配置），其它的配置都会被同步。

配置HA

使用HA功能，用户需要按照以下步骤进行配置：

1. 选择HA组的控制连接接口和数据连接接口。
2. 配置HA组控制连接接口的IP。
3. 配置HA簇。为设备指定HA簇ID，并且开启设备的HA功能。
4. 配置HA组。HA组的配置包括指定设备优先级（选举使用）以及设备HA报文相关参数等。

配置HA，请按照以下步骤进行操作：

1. 选择“系统 > HA”，进入HA配置页面。

在该页面配置HA。

选项	说明
HA控制连接接口1	指定HA控制连接接口1的名称。HA控制连接接口同步两台设备间的所有数据。 » S2060/S2560/S3560/S3860：系统默认将MGT1接口绑定到HA域，便于用户进行HA控制连接接口的选择。用户可选择其他绑定到HA域或无绑定的接口作为HA控制连接接口。 » S1060/S1560：系统默认将ethernet0/1接口绑定到HA域，便于用户进行HA控制连接接口的选择。用户可选择其他绑定到HA域或无绑定的接口作为HA控制连接接口。
HA控制连接接口2	指定HA控制连接接口2的名称。 HA控制连接接口2可以作为HA控制连接接口1的备份接口工作。当HA控制连接接口1断开连接，HA控制连接接口2会继续工作。
HA数据连接接口	指定HA数据连接接口的名称。数据连接仅同步数据报文信息，如会话信息。用户可根据需求选择是否配置数据连接。若配置数据连接，设备间的Hello报文等将通过控制连接完成，数据同步等信息将通过数据连接完成。若不配置数据连接，设备间所有的同步信息将通过控制连接接口完成。
IP地址	指定HA控制连接接口的IP地址及网络掩码。
HA簇ID	指定HA簇ID。取值范围为1至8。当选择HA簇ID为无时表示关闭设备的HA功

选项	说明
	能。
HA同步配置	在某些特殊情况下，可能出现主备配置信息不同步现象。此时，需要用户手动同步主备设备的配置信息。点击“HA同步配置”按钮，完成配置信息同步。
HA同步会话	默认情况下，HA设备之间会自动同步会话信息。同步会话会产生一定流量，在高负载情况下可能会对设备性能造成影响。用户可以根据设备负载情况使用HA会话自动同步功能，以确保设备的稳定性。点击“HA同步会话”按钮，启用HA会话自动同步功能。
组0	
优先级	指定当前设备在HA组中的优先级。优先级高（数字小）的会被选举为主设备。
抢占时间	指定当前设备是否开启抢占模式以及抢占延迟时间。如果将设备配置为抢占模式，一旦设备发现自己的优先级高于主设备，就会将自己升级为主设备，而原先的主设备将变为备份设备。如果输入0，则表示不开启抢占模式；即使设备的优先级高于主设备，它也只能在主设备故障时代替主设备工作。
Hello报文间隔	输入HA设备向HA组中的其它设备发送Hello报文的时间间隔。同一个HA组的设备的Hello报文间隔时间必须相同。
Hello报文警戒值	输入HA组对应的Hello报文的警戒值，即如果设备没有收到对方设备的该命令指定个数的Hello报文，就判断对方无心跳。
免费ARP包个数	指定当前设备选举为主设备后，发送ARP请求包的个数。当备份设备升级为主设备时，新主设备需要向网络中发送ARP请求包，通知相关网络设备更新其ARP表。
监测对象	指定已配置的监测对象的名称。系统利用监测对象监控设备的工作状态。一旦发现设备不能正常工作，立即采取相应措施。
描述	指定该HA组的描述信息。

2. 点击“发送”按钮，完成配置。

第12章 系统管理

设备的系统维护与管理主要包括以下各项：

系统信息

用户可以在系统信息页面查看基本系统信息，包括设备序列号、主机名称、硬件平台、系统时间及运行时间、HA状态、软件版本、启动文件、特征库版本等。

查看系统信息

查看系统信息，选择“系统 > 系统信息”，系统相关信息如下：

选项	说明
序列号	显示该设备的序列号。
主机名称	显示该设备的名称。
硬件平台	显示设备的硬件平台型号。
系统时间	显示该设备的系统日期和时间。
系统运行时间	显示系统已运行时长。
HA状态	显示设备的高可用性工作状态。包括以下六种状态： » Standalone：非HA模式，表示设备没有开启HA功能。 » Init：HA初始状态。 » Hello：HA协商状态，表示设备在协商HA的主备关系。 » Master：HA主状态，表示当前设备为HA组的主设备。 » Backup：HA备状态，表示当前设备为HA组的备份设备。 » Failed：故障状态，表示当前设备故障。
软件版本	显示设备当前的软件版本。
启动文件	显示设备当前的启动文件，以及启动文件的生成时间。
病毒过滤特征库	显示设备的病毒特征库当前版本，以及特征库发布时间。
入侵防御特征库	显示设备的入侵防御特征库当前版本，以及特征库发布时间。
URL分类库	显示设备的URL特征库当前版本，以及分类库发布时间。
应用特征库	显示设备的应用特征库当前版本，以及特征库发布时间。

注意: 仅当系统安装了某个特征库的许可证，系统信息才会显示该特征库的信息。安装特征库的许可证，请参阅"安装许可证" 在第198页。

管理设备

介绍管理员、管理员角色、可信主机、管理接口、系统时间、NTP密钥和系统设置。

管理员

设备的管理员根据角色的不同，对系统可执行的管理和配置权限不同。

系统默认预定义如下四类管理员角色，这四类管理员角色不可被删除和编辑：

- 系统管理员（admin）：拥有读、执行和写权限，可以在任何模式下对设备所有功能模块进行配置，可查看当前或者历史配置信息。
- 系统操作员（Operator）：可以修改除管理员配置以外的其他功能模块配置，但是不能查看日志信息。
- 系统审计员（Auditor）：只可以对日志信息进行操作，包括查看、导出和清除。
- 系统管理员（只读）（Administrator-read-only）：拥有读和执行权限，可查看当前或者历史配置信息。

注意:

- 设备拥有一个默认系统管理员”hillstone“，用户可以对系统管理员”hillstone“进行编辑（只可编辑密码和访问方式），但是不能删除该管理员。
- 除了系统管理员，其他角色的管理员不能进行管理员配置，只能修改自身密码。
- 系统审计员可以管理一种或多种日志信息，管理日志类型需要系统管理员配置。

新建管理员

新建管理员，请按照以下步骤进行操作：

1. 选择“系统 > 设备管理”。
2. 点击<管理员>标签，进入到管理员配置页面。
3. 点击“新建”按钮，弹出<管理员配置>对话框。

配置如下信息。

选项	说明
管理员	在“管理员”文本框中输入管理员的名称。
管理员角色	从下拉菜单选择管理员的角色。不同的管理员角色拥有不同的权限。 » 系统管理员：拥有读、执行和写权限，可以对设备所有功能模块进行配置。 » 系统操作员：可以修改除管理员配置以外的其他功能模块配置，但是不能查看日志信息。 » 系统审计员：只可以对日志信息进行操作，包括查看、导出和清除。 » 系统管理员（只读）：拥有读和执行权限，可查看当前或者历史配置信息。
密码	在“密码”文本框中输入管理员的登陆密码。密码的设定需符合系统密码策略规则。
重新输入密码	在“重新输入密码”文本框中再次输入管理员密码进行确认。
登录类型	选择管理员的登录类型复选框。管理员可以采用Console、Telnet、SSH、HTTP和HTTPS的方式登录，如果需要采用以上所有方式登录，可选择“全选”复选框。
描述	用户可根据需要指定管理员的描述信息。

4. 点击“确定”按钮保存所做的配置。新创建的管理员名称将会显示在管理员列表中。

可信主机

设备使用可信主机来进一步保证系统安全。管理员可以指定一个IP地址范围，在该指定范围内的主机为可信主机。只有可信主机才可以对设备进行管理。

新建可信主机

新建可信主机，请按照以下步骤进行操作：

1. 选择“系统 > 设备管理”。
2. 点击<可信主机>标签，进入到可信主机配置页面。
3. 点击“新建”按钮，弹出<可信主机配置>对话框。

配置如下信息。

选项	说明
类型	指定可信主机地址类型，选择“IP地址和掩码”或“IP地址范围”单选按钮。 » IP地址和掩码：在“IP”文本框中分别输入可信主机的IP地址和子网掩码。0.0.0.0/0表示任意主机都为可信主机。 » IP地址范围：在“IP”文本框中分别输入可信主机的起始IP地址和终止IP地址。
登录类型	选择可信主机的登录类型复选框。可信主机可以采用Telnet、SSH、HTTP和HTTPS的方式登录

4. 点击“确定”按钮保存所做的配置。新创建的可信主机名称将会显示在可信主机列表中。

管理接口

设备支持Console、Telnet、SSH以及Web方式的访问。用户可以配置各种访问方式的超时时间、端口号。 使用Telnet、SSH、HTTP或者HTTPS方式登录设备时，如果在一分钟内连续三次登录失败，系统会将登录失败的IP地址锁定两分钟。被锁定的IP地址在两分钟内不能建立与设备的连接。

配置Console、Telnet、SSH以及Web方式访问的相关参数，请按照以下步骤进行操作：

1. 选择“系统 > 设备管理”。
2. **点击“管理接口”标签，进入到管理接口配置页面。**

选项	说明
Console	配置使用Consoe管理口登录的参数信息。 » 超时：输入Console登录的超时时间。单位为分钟，取值范围为0到60，默认值为10。若取值为0，表示Console方式访问无时间限制。系统若发现用户在超时时间内未通过Console口进行任何配置，将断开此次Console连接。
Telnet	配置Telnet登录的参数信息。 » 超时：输入Telnet登录的超时时间。单位为分钟，取值范围为1到60，默认值为10。 » 端口：输入Telnet登录使用的TCP端口号，取值范围为1到65535，默认值为23。
SSH	配置SSH登录的参数信息。 » 超时：输入SSH登录的超时时间。单位为分钟，取值范围为1到60，默认值为10。 » 端口：输入SSH登录使用的TCP端口号，取值范围为1到65535，默认值为22。
Web	配置WebUI登录的参数信息。 » 超时：输入WebUI登录的超时时间。单位为分钟，取值范围为1到1440，默认值为10。 » HTTP端口：输入HTTP登录使用的TCP端口号，取值范围为1到65535，默认值为80。 » HTTPS端口：输入HTTPS登录使用的TCP端口号，取值范围为1到65535，默认值为443。

3. 点击“确定”。

注意: 当改变HTTP端口、HTTPS端口时，Web服务器需要重启，这可能会导致浏览器无法得到回应。当这种情况发生时，请重新登录。

系统时间

介绍系统时间的配置，包括设置系统时间和通过NTP服务器同步系统时间。

设置系统时间

设置系统时间，请按照以下步骤进行操作：

1. 选择“系统 > 设备管理”。

2. **点击<系统时间>标签，在“设置系统时间”处进行配置。**

选项	说明
与本地时间同步	选择需要同步本地时间的方式，选择“仅同步时间”或“同步时区与时间”按钮。 » 仅同步时间：使系统时间与本地电脑时间同步。 » 同步时区与时间：使系统时区和时间与本地电脑的时区和时间同步。
指定系统时间	设置系统时间的参数信息。 » 时区：指定系统所在时区。 » 日期：指定系统的日期。 » 时间：指定系统的时间。

3. 点击“确定”按钮保存所做设置。

设置NTP

设备的系统时间影响到VPN隧道的建立和时间表的时间，因此系统时间的精确性十分重要。为保证设备系统能够一直保持精确时间，设备允许用户通过NTP来使系统时间与网络上的NTP服务器同步。

配置NTP，请按照以下步骤进行操作：

1. 选择“系统 > 设备管理”。

2. **点击<系统时间>标签，在“设置NTP”处进行配置。**

选项	说明
启用	选中“启用”复选框，开启NTP功能。默认情况下，系统的NTP功能是关闭的。
认证	选中“认证”复选框，开启NTP身份验证。
服务器	指定设备需要同步的NTP服务器，用户最多可以指定3个NTP服务器。 » IP：在文本框中输入服务器的IP地址。 » 密钥：指定可以通过该服务器验证的密钥。如果要在配置的时钟服务器上使用NTP身份验证功能，用户必须指定密钥参数值。 » 源接口：指定设备上发送和接收NTP包的接口。 » 设置为首选服务器：点击“设置为首选服务器”按钮将对应的服务器设置为首选服务器。设备首先与首选服务器进行时间同步。
同步间隔	在“同步间隔”文本框中输入同步间隔的时间。设备每隔一个同步间隔就与服务器做一次同步，以保证设备系统时间的准确。
最大调整时间	在“最大调整时间”文本框中输入最大调整时间的值。如果设备和NTP时钟服务器的时间差在最大调整时间之内，就能成功进行时间同步，否则同步不成功。

3. 点击“确定”按钮保存所做配置。

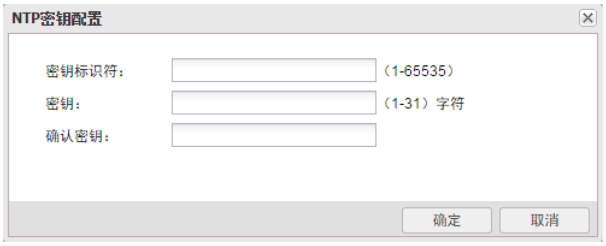
NTP密钥

启用NTP身份验证功能，用户需要配置MD5身份验证密钥ID和密钥。启动该功能后，设备只会与通过验证的服务器进行同步。

新建NTP密钥

新建NTP密钥,请按照以下步骤进行操作：

1. 选择“系统 > 设备管理”。
2. 点击<NTP密钥>标签，进入到NTP密钥配置页面。
3. **点击“新建”按钮，弹出<NTP密钥配置>对话框。**



选项	说明
密钥标识符	在“密钥标识符”文本框中输入密钥ID，取值范围是从1到65535。
密钥	在“密钥”文本框中输入MD5验证密钥，取值范围是1到31个字符。
确认密钥	在“确认密钥”文本框中再次输入验证密钥，需要与“密钥”指定的字符相一致。

4. 点击“确定”按钮保存所做配置。系统将此条NTP密钥信息添加到NTP密钥列表中。

设置及操作

介绍系统相关设置，包括设置系统语言、配置管理员认证服务器、配置主机名称、设置密码策略和重启设备。

更改系统设置，请按照以下步骤进行操作：

1. 选择“系统 > 设备管理”。
2. **点击<设置及操作>标签，进入到系统设置页面。**

设置	说明
系统维护	配置系统信息语言和管理员认证服务器。 » 系统信息语言：选择系统提示（如日志、错误提示）所使用的语言，可选中文或者英文。 » 管理员认证服务器：在“管理员认证服务器”下拉菜单中选择系统管理员认证服务器。
主机配置	某些情况下，用户的网络环境中会配有一台以上设备，为区分这些设备，就需要为每一台设备指定不同的名称。设备的默认名称是其平台名称。 » 主机名称：在“主机名称”文本框中输入设备的主机名称 » 域名：在“域名”文本框中输入设备的域名。
密码策略	配置设备登录密码的长度和复杂度。 » 密码最小长度：在“密码最小长度”文本框中输入密码的最小长度，取值范围为4至16，默认值为4。 » 密码复杂度：用户可以选择“无限制”单选按钮对密码复杂度不进行限制，或者选择限制密码必须包括至少两个大写字母，两个小写字母，两个数字和两个其它字符。

3. 点击“确定”按钮保存所做配置。

重启系统

安装许可证、系统升级等操作需要设备重启才能生效。

重启设备，请按照以下步骤进行操作：

1. 选择“系统 > 设备管理”。
2. 点击<设置及操作>标签页。
3. 点击“重启设备”，然后在提示对话框点击“确定”。
4. 系统将重新启动。

管理配置文件

设备的配置信息都被保存在系统的配置文件中。配置文件以命令行的格式保存配置信息，并且也以这种格式显示配置信息。配置文件中保存的用来初始化设备的配置信息称作起始配置信息，设备通过读取起始配置信息进行启动时的初始化工作；如果找不到起始配置信息，则使用设备的缺省参数初始化。与起始配置信息相对应，设备运行过程中正在生效的配置称为当前配置信息。

系统起始配置信息包括系统的当前起始配置信息（系统启动时使用的配置信息）和系统的备份起始信息。系统纪录最近十次保存的配置信息，最近一次保存的配置信息会纪录为系统的当前起始配置信息，当前系统配置信息以“Startup”作为标记。前九次的配置信息按照保存时间的先后以数字0到8作为标记。

用户可以导出、删除已创建的系统配置文件，也可以导出当前的系统配置。

备份/恢复配置文件

管理配置文件，请按照以下步骤进行操作：

1. 选择“系统 > 配置文件管理”，进入配置文件管理页面。
2. 选择<配置文件列表>标签页，用户可根据需要，做如下配置：
   - 导出：选中需要导出的配置文件前的复选框，然后点击列表上方的“导出”按钮。
   - 删除：选中需要删除的配置文件前的复选框，然后点击列表上方的“删除”按钮。
   - 配置备份/恢复：将系统配置恢复到已保存的配置文件或出厂配置，也可以备份当前的系统配置信息。

配置信息如下。

选项	说明
备份当前配置	在“配置描述”文本框中为备份的系统配置文件添加描述信息。点击“开始备份”按钮进行备份。
恢复配置	恢复到已备份配置： » 选择备份配置文件：点击“选择备份配置文件”按钮，从已备份配置文件列表中选择需要的系统配置文件。点击“确定”按钮。 » 本地上传配置文件：点击“本地上传配置文件”按钮，在<导入配置文件>对话框中，点击“浏览”按钮，并选中需上传的本地配置文件。如需要使配置立即生效，选中复选框，点击“确定”按钮。 恢复出厂配置： » 点击“恢复”按钮，弹出“恢复出厂配置”对话框，点击“确定”按钮，设备自动重启。所有配置将被删除，包括已备份的系统配置文件。数据库内容不清除。 » 如需清除数据库内容，包括威胁日志、报表、抓包等，请参阅"第13章 CLI" 在第203页。

3. 选择<当前系统配置>标签页，可以查看系统当前的配置文件。

注意: 设备在恢复出厂配置后，所有配置将被删除，包括已备份的系统配置文件。请谨慎操作。

设置SNMP

设备的SNMP代理功能，能够接受网络管理平台的操作请求并反馈网络和设备的相应信息。

设备支持SNMPv1协议、SNMPv2协议和SNMPv3协议。SNMPv1和SNMPv2c都使用了团体字的认证方式，可以限制网络管理平台获取设备信息。SNMPv3引入了基于用户的安全模型用于保证消息安全及基于视图的访问控制模型用于访问控制。

设备支持RFC-1213中定义的所有相关的管理信息库组和RFC-2233中定义的使用SMIv2的接口组MIB（The Interfaces Group MIB using SMIv2：IF-MIB）。此外，系统提供一个私有MIB库，MIB库中包含设备的系统信息、IPSec VPN信息以及系统统计信息。用户可以将其导入到管理主机的MIB浏览器，进行使用。

配置SNMP代理

设备拥有一个SNMP代理，该SNMP代理提供网络管理，通过统计数据和接收重要系统事件通知监控网络和设备的运行情况。

配置SNMP代理，请按照以下步骤进行操作：

1. 选择“系统 > SNMP”，进入SNMP页面。
2. **选择“SNMP代理”标签页，进行SNMP代理的配置。**

选项	说明
SNMP代理	选中“启用”复选框，开启SNMP代理功能。
对象ID	显示系统的SNMP对象ID。此ID为系统专有，用户不能修改。
系统联络	在文本框中输入设备SNMP系统联系信息。系统联络，是MIB II中系统组的一个管理变量，内容为设备相关人员的标识及联系方法。用户可以通过配置此参数，将重要信息存储在设备中，以便出现紧急问题时查询使用。
系统位置	在文本框中输入设备的位置。
主机端口	在文本框中输入SNMP代理设备的端口号。
本地引擎ID	在文本框中输入SNMP引擎ID号。

3. 配置完成后，点击“应用”按钮。

注意: SNMP引擎ID唯一标识一个引擎。SNMP引擎是SNMP实体（网络管理平台或者被管理网络设备）的重要组成部分，完成SNMP消息的收发、验证、提取PDU、组装消息与SNMP应用程序通信等功能。

新建SNMP主机

新建SNMP主机，请按照以下步骤进行操作：

1. 选择“系统 > SNMP”，进入SNMP页面。
2. 选择“SNMP主机”标签页，进行SNMP主机的配置。
3. **点击“新建”按钮，弹出<SNMP主机配置>对话框。**

选项	说明
类型	从下拉菜单中选择SNMP主机的类型。选择“IP地址”、“IP地址范围”、“IP/掩码”或“主机”。 » IP地址：在“主机”文本框中输入主机的IP地址。 » IP范围：在“主机”文本框中分别输入起始IP地址和终止IP地址。 » IP/掩码：在“主机”文本框中分别输入主机的IP地址和网络掩码。
SNMP版本	从下拉菜单中选择SNMP版本。
团体字	在文本框中输入SNMP主机的团体字。团体字是管理进程和代理进程之间的口令，是明文格式。此选项仅当版本为SNMP V1和SNMP V2C时有效。
权限	从下拉菜单中选择该团体字的读写权限为“只读”或“可写”，此选项仅当版本为SNMP V1和SNMP V2C时有效。 » 只读：表示此类团体字只可读取MIB中的信息。 » 可写：表示此类团体字不仅可以读取MIB中的信息，还可以对信息进行修改。

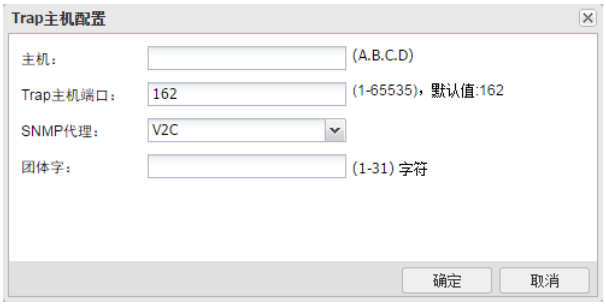
4. 点击“确定”按钮保存所做的配置。新创建的SNMP主机将会显示在SNMP主机列表中。

Trap主机

用户可以配置SNMP Trap主机，用于接收SNMP Trap报文。

新建Trap主机，请按照以下步骤进行操作：

1. 选择“系统 > SNMP”，进入SNMP页面。
2. 选择“Trap主机”标签页，进行Trap主机的配置。
3. **点击“新建”按钮，弹出<Trap主机配置>对话框。**



选项	说明
主机	在文本框中输入Trap主机的IP地址。
Trap主机端口	在文本框中输入Trap主机的端口号。
SNMP代理	从下拉菜单中选择SNMP版本为V1、V2C或V3。 » V1或者V2C：选择版本为V1或V2C时，在“团体字”文本框中输入SNMP主机的团体字。 » V3：选择版本为V3时，在“V3用户”下拉菜单中选择V3用户名称，在“引擎ID”文本框中输入Trap主机的引擎ID号。

4. 点击“确定”按钮保存所做的配置。新创建的Trap主机将会显示在Trap主机列表中。

V3用户组

SNMP V3建议的安全模型是基于用户的安全模型。当选择SNMP版本为SNMP V3时，用户需要为SNMP主机创建SNMP V3用户组。

新建V3用户组，请按照以下步骤进行操作：

1. 选择“系统 > SNMP”，进入SNMP页面。
2. 选择“V3用户组”标签页，进行V3用户组的配置。
3. **点击“新建”按钮，弹出<V3组配置>对话框。**

选项	说明
名称	在文本框中输入SNMP V3用户组名称。
安全模式	显示了SNMP V3用户组的安全模式。
安全级别	在下拉菜单中选择用户组的安全级别。安全级别决定了在处理一个SNMP数据包时所采用的安全机制。

选项	说明
	V3用户组的安全级别包括无（无认证和加密）、认证（提供基于MD5或SHA算法的认证）或者认证&加密（提供基于MD5或SHA算法的认证和基于AES和DES的报文加密）。
可读视图	在下拉菜单中选择该用户组的只读MIB视图名。如不指定该参数，系统默认为空。
写视图	在下拉菜单中选择该用户组的可写MIB视图名。如不指定该参数，系统默认为空。

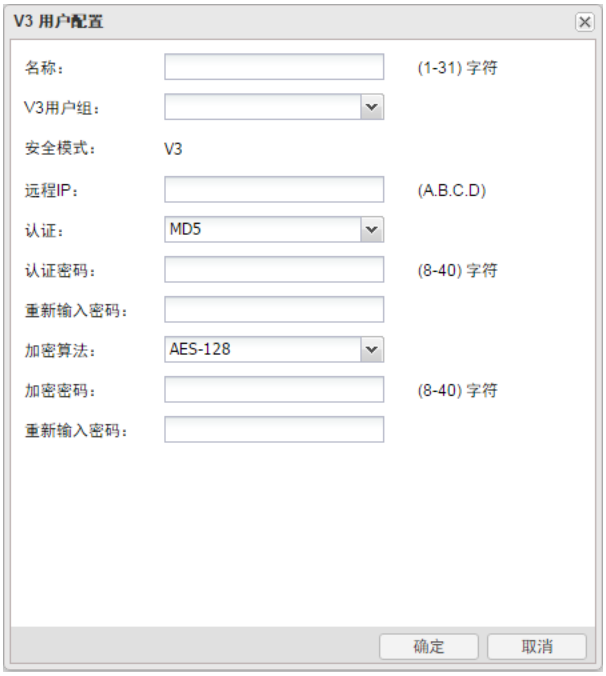
4. 点击“确定”按钮保存所做的配置。新创建的V3用户组将会显示在V3用户组列表中。

V3用户

如果使用的SNMP版本为SNMP V3，用户需要为SNMP主机创建SNMP V3用户组，之后可以向用户组添加用户。

新建V3用户，请按照以下步骤进行操作：

1. 选择“系统 > SNMP”，进入SNMP页面。
2. 选择“V3用户”标签页，进行V3用户的配置。
3. **点击“新建”按钮，弹出<V3用户配置>对话框。**



选项	说明
名称	在文本框中输入SNMP V3用户名称。
V3用户组	在下拉菜单中为所创建的用户选择已经配置好的用户组。
安全模式	显示了SNMP V3用户的安全模式。
远程IP	文本框中输入远程管理主机的IP地址。
认证	在下拉菜单中为用户指定认证协议。默认情况下，该参数值为空，即无认证，无加密模式。
认证密码	在文本框中指定认证密码。

选项	说明
重新输入密码	在文本框中再次输入认证密码进行确认。
加密算法	在下拉菜单中指定用户加密协议。
加密密码	在文本框中指定加密密码。
重新输入密码	在文本框中再次输入加密密码进行确认。

4. 点击“确定”按钮保存所做的配置。新创建的V3用户将会显示在V3用户列表中。

升级管理

用户可以在版本升级配置页面将系统升级或降级到指定版本，也可以指定应用特征库、URL分类库、病毒过滤特征库、入侵防御特征库的升级配置。

升级版本

升级软件版本，请按照以下步骤进行操作：

1. 选择“系统 > 升级管理”，进入升级管理页面。
2. **点击“版本升级”标签页，进入到版本升级页面。**

升级版本	
备份配置文件	在升级版本前，建议先备份配置文件，点击“备份配置文件”按钮为当前的软件版本做为备份，完成备份后，系统会自动跳转到“配置文件管理”页面，在配置文件列表中显示已备份的文件。
当前版本	显示当前软件的版本号。
上传版本文件	点击“浏览”按钮在本地计算机选择软件版本文件。
重启设备	选中“立即重启，使新版本生效”复选框并点击“应用”按钮立即重启系统并进入新版本，或直接点击“应用”保存配置。新版本将在下次重启时生效。
选择下次启动版本	
选择下次启动的版本	从下拉菜单选择下次启动时生效的软件版本。
重启设备	选中“立即重启，使新版本生效”复选框并点击“应用”按钮立即重启系统并进入新版本，或直接点击“应用”保存配置。新版本将在下次重启时生效。

升级特征库

只能查看到已安装的许可证的特征库。系统可以安装的特征库包括应用特征库、URL分类库、病毒过滤特征库、入侵防御特征库。

各个特征库的升级操作相同，请参考以下步骤：

1. 选择“系统 > 升级管理”，进入升级管理页面。
2. **点击“特征库升级”标签页，进入到特征库升级页面。**

选项	**说明**
当前版本	显示当前特征库的版本号。
远程升级	配置应用特征库、URL特征库、病毒过滤特征库、入侵防御特征库或IP信誉特征库远程升级参数。 » 立即升级升级：点击“立即在线升级”按钮，立即升级特征库。 » 自动升级配置：选中“启用自动升级”复选框并设置自动升级时间，点击“保存”按钮，系统将按照设置的时间自动升级特征库。 » 升级服务器设置：设备提供两个默认特征库更新服务器，分别是update1.hillstonenet.com和update2.hillstonenet.com。用户也可根据需要自定义升级服务器：点击“配置升级服务器”按钮，在弹出的<升级服务器设置>对话框中，指定需要的服务器的IP地址或者域名。
本地升级	上传本地升级文件。点击“浏览”按钮，选中本地特征库文件，点击“上传”按钮，系统开始上传特征库信息。

安装许可证

许可证（license）用来授权用户使用一些功能和服务。对于基于许可证的功能和服务来说，如果没有购买和安装相应的许可证，该功能和服务就无法使用。

许可证的分类和规则如下：

平台许可证	说明	许可证过期
平台试用许可证	平台许可证是其他许可证运行的基础，如果平台许可证无效，其他许可证均不生效。 设备出厂时已预装15天的试用许可证，支持功能同正式许可证。	到期后， 已有的配置不能修改，若设备重启，系统恢复出厂配置。
平台正式许可证	平台许可证是其他许可证运行的基础，如果平台许可证无效，其他许可证均不生效。 设备正式销售后，可以安装平台正式许可证。该许可证提供基础功能。	到期后，设备仍可正常使用，但不能升级到期后的OS版本。
服务许可证	**说明**	**许可证过期**
病毒过滤许可证	提供病毒过滤功能和病毒特征库的升级。	过期后，不能升级病毒特征库，病毒过滤功能正常使用。
入侵防御许可证	提供入侵防御功能和IPS特征库升级。	过期后，不能升级IPS特征库，入侵防御功能正常使用。
URL许可证	支持URL过滤功能使用URL分类库和URL的在线查询功能。	过期后，不能升级URL分类库，不能提供URL的在线查询功能，自定义URL和URL过滤功能仍正常使用。
应用特征库许可证	提供应用特征库升级功能。应用特征库许可证不需要单独申请，随平台许可证一同发放，有效期也同平台许可证。	过期后，不能升级应用特征库。

申请许可证

申请许可证之前，用户需要先申请许可证请求，请按照以下步骤进行操作：

1. 选择“系统 > 许可证”，进入许可证页面。
2. 在“许可证申请”中，填写生成许可证请求所需要的信息。

3. 点击“生成”，出现一串代码。
4. 将生成的代码发送给销售人员，由其获取许可证再返回给您。

安装许可证

获得许可证后，用户需要将其装载到设备上使其生效。安装许可证，请按照以下步骤进行操作：

1. 选择“系统 > 许可证”，进入许可证页面。
2. **在“许可证申请”中，用户可根据需要，以下以下两种方式中的一种导入许可证**
   - 上传许可证文件：选中“上传许可证文件”单选按钮，点击“浏览”按钮，并且选中许可证文件（许可证为纯文本.txt文件）。
   - 手动输入：选中“手动输入”单选按钮，然后将许可证字符串内容粘贴到文本框中。
3. 点击“确定”按钮保存所做配置。
4. 选择“系统 > 设备管理”，然后点击<设置及操作>标签页。
5. 点击“重启设备”，然后在提示对话框点击“确定”。
6. 等待系统重启。启动后，许可证将生效。

配置邮件服务器

用户可以在邮件服务器配置页面配置SMTP服务器，将系统日志等信息发送到指定的邮箱。

新建邮件服务器

新建邮件服务器，请按照以下步骤进行操作：

1. **选择“系统 > 邮件服务器”，进入“SMTP 服务器配置”页面。**

选项	说明
名称	在文本框输入SMTP服务器的名称。
服务器	在文本框输入SMTP服务器的域名或者IP地址。
验证	用户可根据需要，选中“启用”复选框开启验证功能，并在之后的“用户名”、“密码”和“重新输入密码”文本框中输入发送日志信息的用户名以及对应的密码。
Email	在文本框中指定发送日志信息的Email地址。

2. 点击“应用”按钮，保存当前页面所做配置。

系统调试

故障反馈

开启故障反馈功能后，当系统发生异常时，将自动发送异常相关信息到厂商。

开启故障反馈功能，请按照以下步骤进行操作：

1. 选择“系统 > 系统调试”。

2. 选中“故障反馈”后的“启用”复选框。
3. 点击“确认”按钮。

系统调试信息

当系统发生异常时，将产生异常相关信息供诊断问题。

导出系统调试信息，请按照以下步骤进行操作：

1. 选择“系统 > 系统调试”。
2. 点击“导出”按钮。

3. 将调试文件保存并发送给厂商进行诊断。

测试工具

设备支持域名查询，支持使用网络连接测试工具Ping和Traceroute。

DNS查询

检查设备的DNS功能是否工作正常，请按照以下步骤进行操作：

1. 选择“系统 > 诊断工具 > 测试工具”，进入测试工具页面。
2. 在“DNS查询”文本框中输入需要查询的域名。
3. 点击“DNS查询”对应的“测试”按钮，检测结果会显示在下方的文本框中。

Ping

使用工具Ping进行网络连通测试，请按照以下步骤进行操作：

1. 选择“系统 > 诊断工具 > 测试工具”，进入测试工具页面。
2. 在“Ping”文本框中输入网络对端的IP地址。
3. 点击“Ping”对应的“测试”按钮，检测结果会显示在下方的文本框中。
4. 检测结果包含以下两部分：
   - 对每个Ping报文的响应情况。如果在超时时间到后仍没有收到响应报文，则输出Destination Host Not Responsed等，否则显示响应报文中报文序号、TTL和响应时间。
   - 最后的统计信息，包括发送报文数、接收报文数、未响应报文百分比和响应时间的最小、平均和最大值。

Traceroute

Traceroute用于测试数据包从发送主机到目的地所经过的网关。它主要用于检查网络连接是否可达，以及分析网络什么地方发生了故障。Traceroute通常的执行过程是：首先发送一个TTL为1的数据包，因此第一跳发送回一个ICMP错误消息以指明此数据包不能被发送（因为TTL超时），之后此数据包被重新发送，TTL为2，同样第二跳返回TTL超时，这个过程不断进行，直到到达目的地。执行这些过程的目的是记录每一个ICMP TTL超时消息的源地址，以提供一个IP数据包到达目的地所经历的路径。

使用Traceroute命令测试数据包经过的网关，请按照以下步骤进行操作：

1. 选择“系统 > 诊断工具 > 测试工具”，进入测试工具页面。
2. 在“Traceroute”文本框中输入网络对端的IP地址。
3. 点击“Traceroute”对应的“测试”按钮，检测结果会显示在下方的文本框中。

第13章 CLI

在CLI中对设备进行基础网络配置，包括对ethernet0/0或MGT0接口的配置以及路由配置。还可对设备恢复出厂配置。

登录设备

通过Console口，Telnet，或SSH与设备建立连接。在设备CLI登录界面，提供如下参数：

login：hillstone

password：hillstone

验证后，登录设备。登录后，用户位于全局视图中。

配置接口的安全域，IP和管理方式

对于S1060和S1560，用户可对ethernet0/0接口进行配置。此接口绑定到trust安全域，其默认IP地址为192.168.1.1

对于S2060、S2560、S3560、和S3860，用户可对MGT0接口进行配置。此接口绑定到mgt安全域，其默认IP地址为192.168.1.1。

在全局视图中，使用如下命令进入接口的配置模式：

interface ethernet0/0

或

interface mgt0

在接口配置模式下，使用如下命令将接口绑定到已定义的二层或三层域。使用该命令no的形式取消配置。

zone *zone-name*

在接口配置模式下，使用如下命令为接口设置IP地址。使用该命令no的形式取消配置。

ip address *ip-address/mask*

在接口配置模式下，使用如下命令为接口开启相应的管理功能。使用该命令no的形式取消配置。

manage {ssh | telnet | ping | snmp | http | https }

配置路由

在全局视图中，使用如下命令，添加静态路由条目：

ip route { *A.B.C.D/M* | *A.B.C.D A.B.C.D*} *A.B.C.D*

- *A.B.C.D/M | A.B.C.D A.B.C.D* – 指定目的地址。
- *A.B.C.D* – 指定下一跳地址。

恢复出厂配置

在全局视图中，使用如下命令，恢复出厂配置：

unset all

- a - 输入a并按回车删除所有配置，包括已备份的系统配置文件。数据库内容不清除。
- b - 输入b并按回车删除所有配置，包括已备份的系统配置文件。且清除数据库内容，包括威胁日志、报表、抓包等。
- c - 输入c并按回车取消恢复出厂配置。