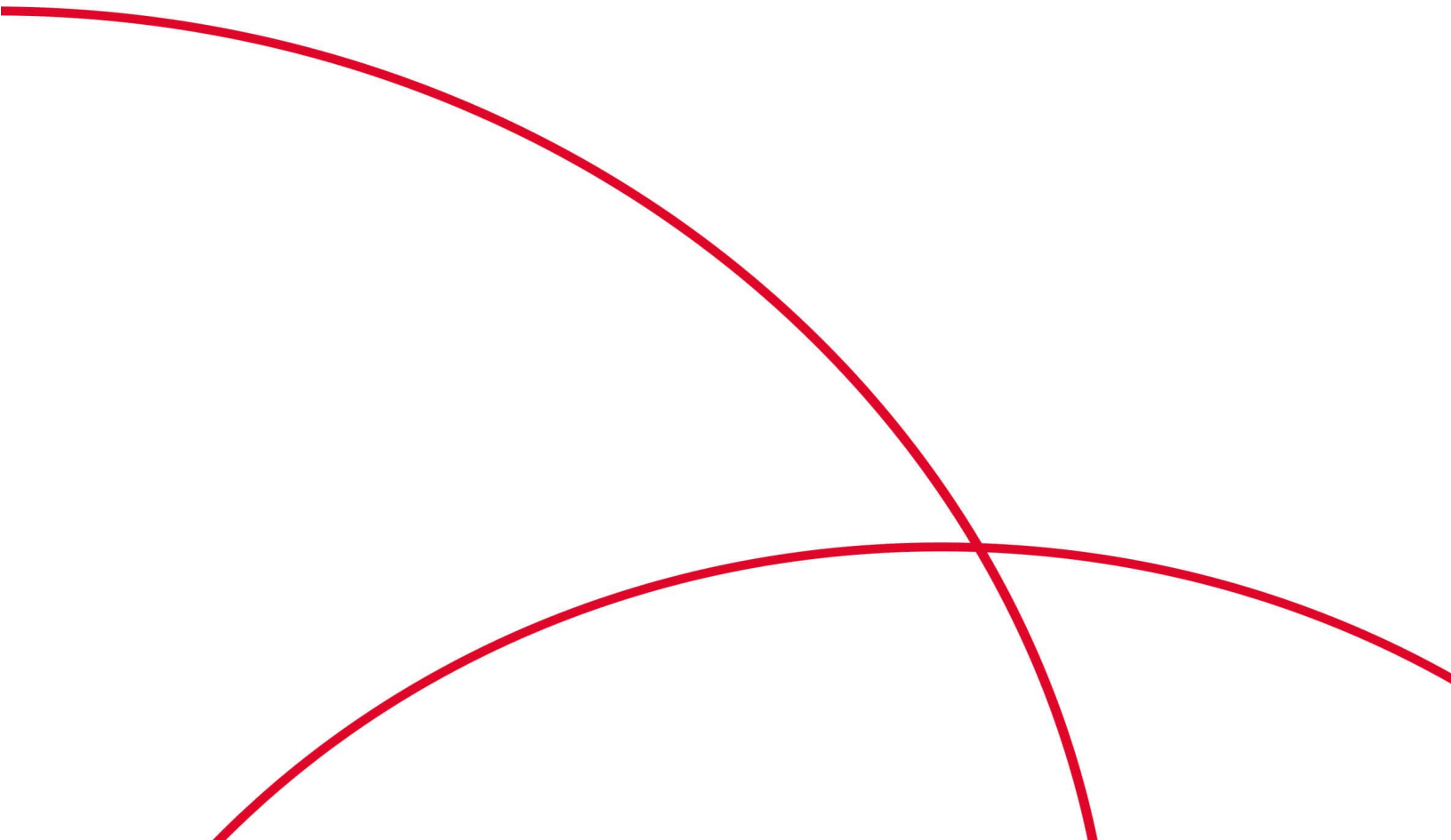
云防火墙（原生版）

N100 用户使用指南



目 录

手册约定

为方便用户阅读与理解，本手册遵循以下约定。在熟知通用控件操作方法的情况下，用户可完成大多数的功能配置。

> 注意: 如无特殊说明，WebUI 的选项配置请使用 UTF-8 编码格式。

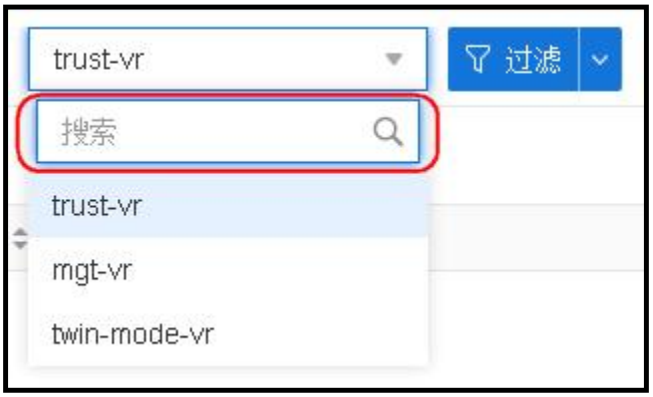
以下是通用控件和操作效果：

在功能大类之间切换：点击相应的标签页（位于页面顶端）。

在具体功能之间切换：在二级导航栏中点击相应功能。

展开功能列表：在左侧导航栏点击“ ”按钮；
合并功能列表，在左侧导航栏点击“ ”按钮。

部分下拉列表支持搜索功能，在“搜索”行内输入搜索关键字即可。



显示指定列：点击 按钮，在下拉列表中选择“列”，勾选需要显示的列。列表支持状态记忆功能，用户在登录设备时，将显示上次设置的列表状态。

锁定列：点击 按钮，在下拉列表中选择“锁定列”，将指定列固定在列表的左侧，左右滚动时始终显示锁定的列。

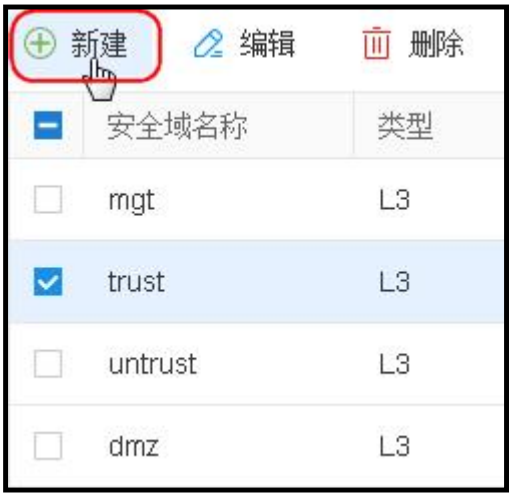
解除锁定：点击 按钮，在下拉列表中选择“解除锁定”，解除指定列的锁定。

需要恢复列表的初始状态，双击列表表头，在弹出的对话框中点击“确定”，清除该列表的个性化配置。

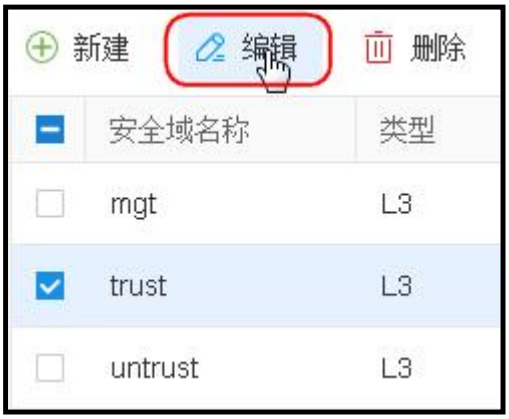
需要恢复所有列表的初始状态：点击页面右上角的用户名 按钮，点击“清除个性化”，在弹出的对话框中点击“确定”，清除所有列表的个性化配置并重新登录。

查看指定过滤条件的条目：点击 过滤 按钮，在下拉菜单中选择需要添加的过滤条件，并指定过滤条件内容。如需删除某个过滤条件，可将鼠标悬浮在此过滤框后，然后点击×图标。如需删除所有过滤条件，可在此状态栏的尾端点击 ×清空 图标。

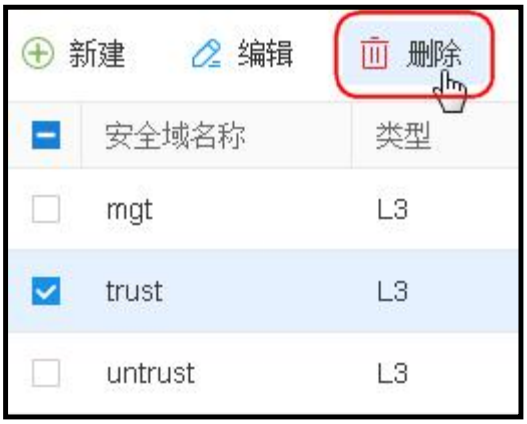
需要新建一个条目，点击“新建”按钮。



需要修改一个条目，选中该条目前的复选框，点击“编辑”按钮。



需要删除一个或多个条目，选中该条目前面的复选框，点击“删除”按钮。



需要复制一个条目，选中该条目前的复选框，点击“复制”按钮。

需要粘贴复制的条目，复制后，点击“粘贴”按钮。

需要显示隐藏的操作控件，点击“⋮”按钮。

需要更新当前页面上显示的数据，点击“刷新”按钮。

需要按照单个条件搜索相关内容时，点击“过滤”，在下拉菜单中选择条件，并输入关键字。按“回车键”开始搜索。

需要按照多个条件组合搜索相关内容，继续点击“过滤”，在下拉菜单中选择条件，并输入关键字。按“回车键”开始搜索。

需要保存组合过滤条件，点击⋮，在下拉菜单中点击“保存过滤条件”，并输入名称。点击“保存”，可保存该组合过滤条件。

在对话框中，点击右上角的“X”按钮，关闭该对话框。

在对话框中，点击“确定”按钮，保存所填配置。

在对话框中，点击“取消”按钮，放弃当前操作。

点击“确定”按钮，可使修改生效。

点击翻页键，跳转到上一页，下一页，首页或最后一页。输入页码数字，跳转到相应页面。

浏览器兼容性

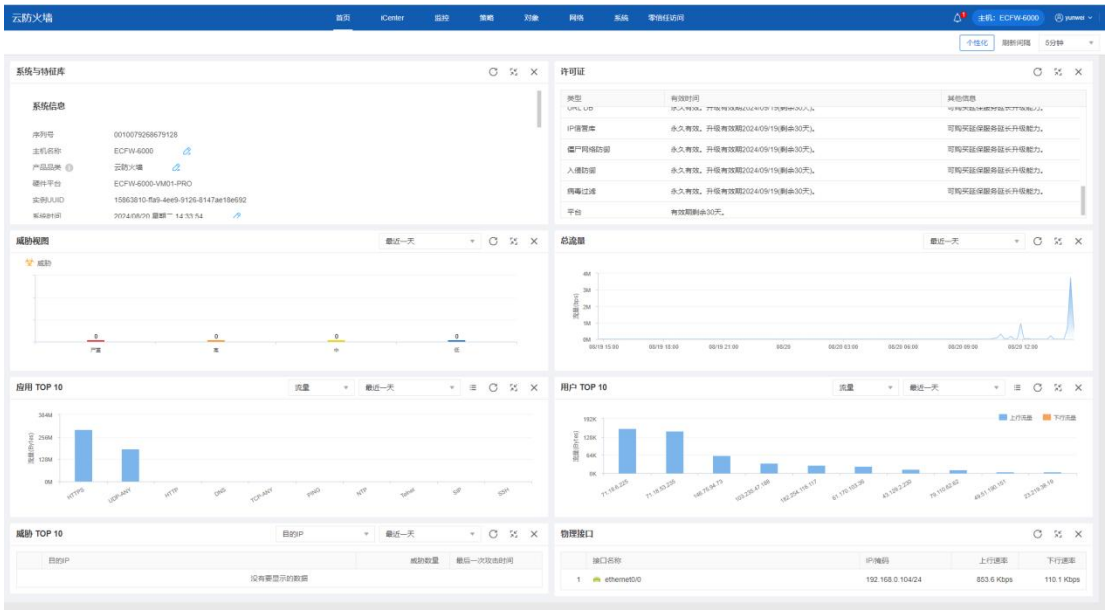
使用以下浏览器，能够获得最佳 Web 界面支持。

IE11

Chrome

第 1 章 首页

首页显示系统和威胁的各项信息。首页窗口具体布局，请参考下图：



个性化配置

用户可以根据需要，定制首页所显示的功能或修改功能区域位置。

定制首页显示功能，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. 在展开的列表中，勾选需要显示在首页的功能复选框。

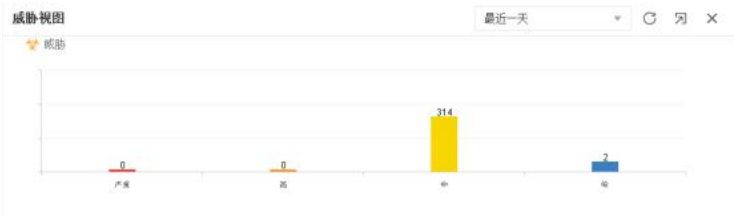
修改功能区域位置，请按照以下步骤进行操作：

1. 鼠标悬停在功能区标题部分。
2. 当出现  时，鼠标按住功能区域，拖动到需要显示的区域位置即可。

在列表中，将光标悬浮在需要查看威胁情报的对象上方，右侧出现 ⋮ 按钮。点击该按钮，选择“查看威胁情报”，跳转到云瞻威胁情报中心查看该情报的相关信息。威胁情报显示信息的含义，请参见 iCenter 的威胁部分。

威胁视图

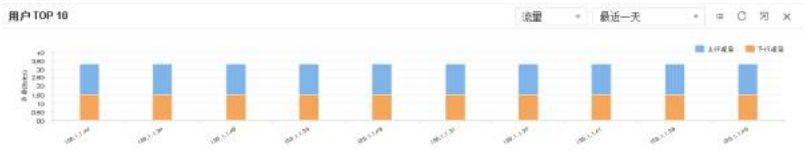
威胁视图部分以柱状图方式显示指定统计周期内的设备攻击统计信息。



点击柱状图跳转到 iCenter 页面，并且按照对应的威胁级别筛选出指定威胁条目。

用户信息

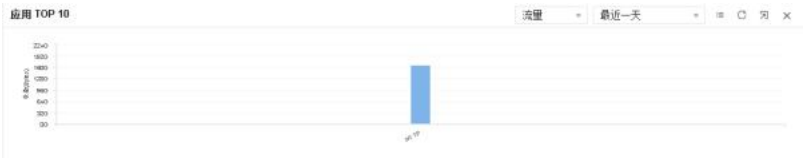
显示指定统计周期内的前 10 的用户流量。



用户可以在此区域执行以下操作：

应用信息

显示指定统计周期内的前 10 的应用流量。



用户可以在此区域执行以下操作：

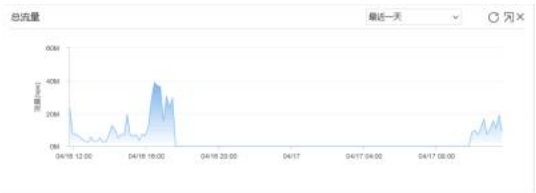
下拉菜单用于指定显示的应用排序类型：流量或并发连接数。

区域右上角、按钮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值或并发连接数，点击“详细信息”跳转到对应详细页面。

总流量

显示设备指定统计周期的整机总流量。



接口列表

显示设备所有物理接口的统计信息，包括接口名称、主 IP、上行速率、下行速率以及总速率。

实例 UUID：显示云防火墙实例的 UUID（通用唯一识别码）。

立即检查：点击“立即检查”按钮，更新并显示特征库的最新版本号。说明：显示特征库最新版本号需在已激活特征库许可证并已有特征库版本的情况下。

许可证

显示设备已安装的许可证的主要信息。

类型：显示许可证的类型。

有效时间：显示许可证的有效时间。

其他信息：显示许可证的其他备注信息。

统计周期

用户可以通过各项统计信息右上角的统计周期下拉菜单（ 

）指定统计周期：

实时: 显示实时流量信息（bps）。

最近 1 小时: 显示最近 1 小时的统计信息。

最近 1 天: 显示最近 1 天的统计信息。

最近 1 月: 显示最近 1 月的统计信息。

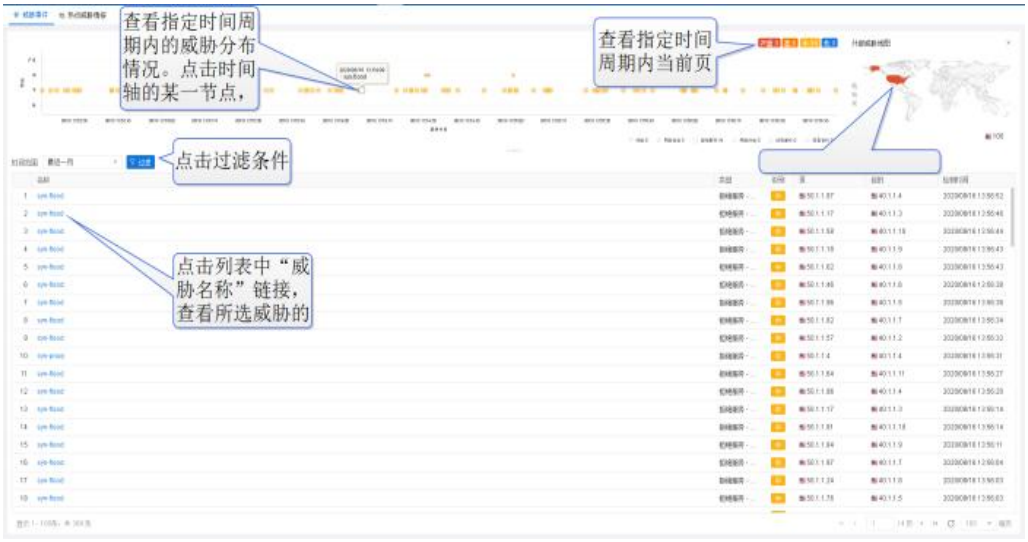
用户可以通过页面右上角的刷新间隔设置显示数据的刷新间隔。另外不同模块统计周期略有差异，比如威胁统计周期支持 5 分钟、1 周等统计周期。以实际界面看到为准。

第 2 章 iCenter

iCenter 即智能风险监控中心，针对设备管理的全网范围内受到的所有攻击，提供多维度、深层次的结果展现。

威胁事件

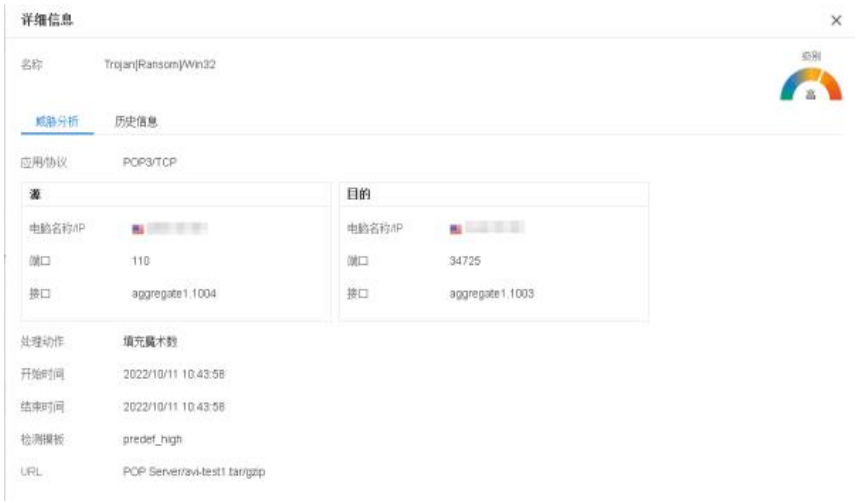
<威胁事件>统计并展示全网的所有威胁详细信息。点击“iCenter”。



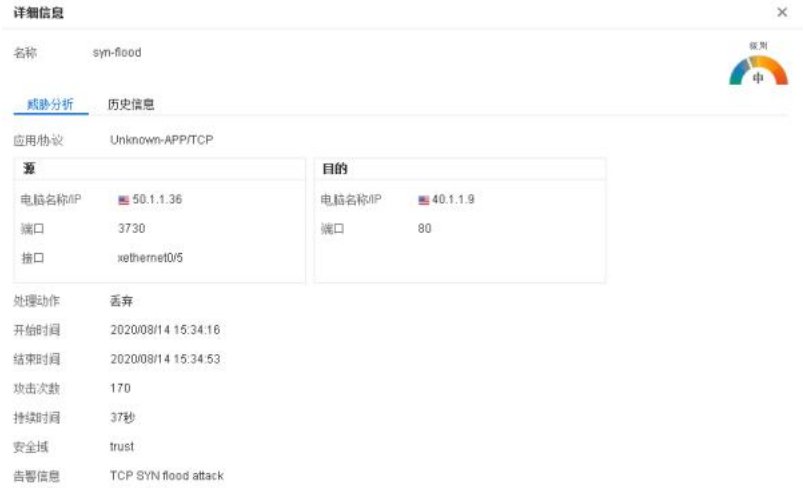
点击列表中“威胁名称”链接，查看所选威胁的分析结果、源/目的、知识库以及相关的历史信息。

威胁分析：根据不同检测引擎检测的攻击，威胁分析标签页内容也不同。

病毒过滤/入侵防御：显示指定威胁的详细分析信息。



攻击防护：显示指定威胁的详细分析信息。



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。

接口组：系统支持将多个物理接口的状态相互绑定，组成一个接口组，形成接口间的联动功能。

DNS：域名系统。

DHCP：动态主机配置协议。

DDNS：动态域名服务。

PPPoE：点对点协议。

Virtual-Wire：实现子网间的直接二层通信。

虚拟路由器：虚拟路由器具有路由器功能，不同虚拟路由器拥有各自独立的路由表。

虚拟交换机：虚拟交换机（VSwitch）具有交换机功能。VSwitch 工作在二层，将二层安全域绑定到 VSwitch 上后，绑定到安全域的接口也被绑定到该 VSwitch 上。流量可以通过 VSwitch 接口，实现二层与三层之间的转发。

链路负载均衡：通过动态链路探测技术将流量合理分发到不同链路，从而达到充分利用各条链路资源的目的。

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：

接口绑定到域，二层域绑定到 VSwitch，三层域绑定到 VRouter。因此，二层域所在的 VSwitch 决定了该域中接口的 VSwitch，三层域所在的 VRouter 决定了该域中接口的 VRouter。

二层和三层域决定其接口工作在二层模式或是三层模式。

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 8 个安全域，分别是：trust、untrust、dmz、L2-trust、L2-untrust、L2-dmz、vpnhub（VPN 功能域）以及 ha（HA 功能域）。用户也可以自定义域。事实上，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，打开<安全域配置>页面，如下图所示。

3. 指定安全域名称。在“安全域名称”文本框输入需要的名称。长度为 1-31 个字符。
4. 根据需要，在“描述”文本框中输入描述信息。长度为 0-63 个字符。
5. 指定安全域类型。如选择“二层安全域”，在其后的“虚拟交换机”下拉菜单选择安全域所属的 VSwitch；如选择“三层安全域”，在其后的“虚拟路由器”下拉菜单选择安全域所属的 VRouter；如选择“TAP”，既指定所创建的域为 Tap 域，Tap 域为旁路模式功能域。
6. 在“虚拟路由器”下拉菜单选择该安全域所属 VR。
7. 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。
8. 如需要，点击“应用识别”后的“启用”按钮，开启安全域的应用识别功能。
9. 如需要，点击“WAN 安全域”后的“启用”按钮，将安全域设置为 WAN 安全域，保证以 IP 为数据组织方式的统计集的统计数据的准确性。
10. 如需要，点击“NBT 缓存”后的“启用”按钮，开启安全域的 NetBIOS 主机名查询功能。
11. 点击“确定”，完成安全域的配置。

注意:

预定义安全域不可以被删除。

改变域所属的 VSwitch 时，必须保证域中没有绑定的接口。

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。

安全网关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：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，例如 ethernet0/0 或 ethernet0/1。

逻辑接口：系统中的逻辑接口包括子接口、VSwitch 接口、回环接口、隧道接口、集聚接口、冗余接口、PPPoE 接口以及 Virtual Forward 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：属于二层域或者 VLAN 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。
VSwitch 接口	VSwitch 接口是三层接口。它代表了 VSwitch 上所有接口的集合。VSwtich 接口相当于实际交换机的上连口，能够实现数据包在二层与三层之间的转发。
回环接口	回环接口是逻辑接口，并且只要回环接口所在的设备处于工作状态，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。
隧道接口	隧道接口充当 VPN 通道的入口。流量通过隧道接口进出 VPN 通道。隧道接口只能是三层接口。
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。
PPPoE 接口	使用 PPPoE 协议连接 PPPoE 服务器的逻辑接口，基于以太网口创建。
Virtual Forward 接口	在 HA 环境中，Virtual Forward 接口为 HA 组的接口，用于传输流量。

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。

目前系统支持配置接口地址为 IPv4 地址或 IPv6 地址。

新建 PPPoE 接口

新建 PPPoE 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“PPPoE 接口”，打开<PPPoE 接口>页面。

在此页面，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 0-63 个字符。
绑定安全域	如选择“三层安全域”，则继续从“安全域”下拉菜单选择安全域的名称。 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。
HA 同步	点击“启用”按钮，开启 HA 同步，即关闭 HA Local 属性，接口使用虚 MAC，此时主设备和备用设备信息同步；不选该选项复选框关闭 HA 同步，即开启 HA Local 属性，接口保持原有 MAC 地址，

选项	说明
	此时主设备和备用设备信息不再同步。
IP 配置	
用户	指定 PPPoE 用户名称。长度为 1-31 个字符。
密码	指定 PPPoE 用户相应的密码。长度为 1-31 个字符。
确认密码	再次输入密码进行确认。
修改密码	编辑 PPPoE 接口配置时，可以看到修改密码功能。开启后，将展示密码输入框。如需修改，输入新的密码后保存配置即可。
挂断前空闲间隔	当 PPPoE 接口的空闲（无流量）时间到达一定的时间，即指定的空闲间隔，系统会断开与因特网的连接；当产生上网需求时，系统会自动连接到因特网。该选项指定空闲间隔时间，单位为分钟。范围是 0 到 10000 秒，默认值是 0。
重拨间隔	该选项指定重拨间隔时间（系统在断开连接后自动重拨的时间间隔），单位为秒。范围是 0 到 10000 秒。默认值是 10，表示不进行自动重拨。
PPPoE 服务器提供的网管信息设置为默认网关路由	选中该选项复选框，系统会将 PPPoE 服务器提供的网关信息设置为默认网关路由。
高级选项	点击“高级选项”按钮，打开<高级选项>页面，用户可对 PPPoE 相关的高级选项进行配置，包括： 访问集中器：指定访问集中器的名称。 长度为 1-31 个字符。 认证：设备与 PPPoE 服务器建立连接时，需要通过 PPPoE 认证。设备支持的验证方式有 CHAP、PAP 和 any（系统默认方式，表示 CHAP 或者 PAP 的任意一种）。选中需要的认证方式的单选按钮。 网络掩码：为 PPPoE 方式获得的 IP 地址指定网络掩码。 静态 IP：用户可以指定一个静态的 IP 地址，并协商使用该静态 IP 地址。这样可以避免 IP 地址变化。该选项指定静态 IP 地址。在文本框中输入静态 IP 地址。 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。 服务：指定允许的服务。此处指定的服务必须与 PPPoE 服务器端提供的服务相同。如果不指定服务，设备自动接受服

选项	说明
	务器返回的任何服务。 长度为 1-31 个字符。
DDNS	点击“DDNS”按钮，打开<DDNS 配置>页面为接口进行 DDNS 配置。 说明：该功能仅在编辑接口时可用，新建接口时不可用。
管理方式	选中该接口需要的管理方式的复选框。包括 Telnet、SSH、Ping、HTTP、HTTPS 、SNMP、NETCONF 和 TRACEROUTE。
WebAuth	
认证服务	根据需要选择启用、关闭或者使用全局默认。 启用：开启指定接口的 Web 认证功能。 关闭：关闭指定接口的 Web 认证功能。 使用全局默认：指定接口 Web 认证功能使用全局默认配置。
主动认证	点击“启用”按钮，开启 Web 主动认证功能，并从下拉菜单中选择 AAA 服务器。 开启后，用户可通过访问 Web 认证地址主动发起认证请求，然后在认证登录页面填写正确的用户名和密码即可进行认证。Web 认证地址为该接口的 IP 地址+认证服务器的 HTTP 或 HTTPS 的端口号，如接口的 IP 地址为 192.168.3.1，认证服务器 HTTP 和 HTTPS 的端口号被分别配置为 8182、44434，则认证服务器配置为 HTTP 模式时 Web 认证地址为：http:// 192.168.3.1:8182；认证服务器配置为 HTTPS 模式时，Web 认证地址为 https:// 192.168.3.1:44434。
WebAuth 域名	指定接口对应的 Web 认证域名，取值范围是 1 到 255 个字符。为 Web 认证地址配置域名后，访问服务时弹出的 Web 认证页面（被动认证）的 URL 将显示为域名形式。配置该功能前，需先开启 Web 认证功能。

点击“接口属性”，展开接口属性配置项，配置接口的属性信息。

选项	说明
参数	
ARP 学习	点击“启用”按钮，开启接口的 ARP 学习功能。
ARP 学习限制	当一个接口接入的某个用户主机发起 ARP 攻击时，可能会出现耗尽 ARP 表项资源的情况，导致其他接口无法进行 ARP 学习。为避免上述问题，系统支持开启 ARP 学习限制功能，并指定该接口允许学习的最大数量。指定后，如果一个接口达到了允许学习的最大数量，将不再允许该接口继续进行 ARP 学习。

选项	说明
	点击“启用”按钮，开启接口的 ARP 学习限制功能，并在文本框中输入接口允许学习的最大数量。范围是 1 到 Capacity。
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	在文本框中输入指定的 MAC 地址，将其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。
上行带宽	指定接口上行带宽的最大值。
下行带宽	指定接口下行带宽的最大值。

点击“高级配置”，展开高级配置项，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
NetFlow 配置	从下拉菜单中选择已配置好的 NetFlow 规则。
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。
立即关闭	系统支持接口关闭功能，用户不仅可以根据需要手动强制关闭特定接口，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“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，也可以点击 新建时间表或监控对象。
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，也可以点击 新建时间表或监控对象。 2. 选择控制方式：

选项	说明
	监控接口，使路由失效：当到达时间表指定时间内或者指定的监控对象状态异常时，接口将自动切换到监控状态，同时相关的路由也将失效，不再进行流量转发。超出时间表或监控对象恢复后，接口也将自动恢复到原先的正常状态，同时原先的相关路由也将自动恢复正常，常用于日常的运维和故障的定位与恢复。 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，单位为分钟。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）。

选择“网络 > 路由 > RIP”，点击“接口配置”，打开<接口配置>页面，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。
被动模式	用户可以将一些接口配置为只接收更新但是不发送，这种只接收更新的接口就是被动接口。点击“启用”按钮，开启该接口为被动接口。

选择“网络 > 路由 > OSPF”，点击“接口配置”，打开<接口配置>页面，配置接口的 OSPF 功能。

选项	说明
接口定时器	接口的定时器有以下四个：接口发送 Hello 包的时间间隔、接口相

选项	说明
	邻路由器的失效时间、接口重传 LSA 的时间间隔以及接口更新包的延迟时间。 Hello 发送间隔：指定接口发送 Hello 包的时间间隔，单位为秒。默认值是 10 秒。范围是 1 到 65535 秒。 失效时间：指定接口的相邻路由失效时间，单位为秒。默认值是 40 秒（发送 Hello 包时间间隔的 4 倍）。范围是 1 到 65535 秒。 如果接口在一定的时间内都没有收到对方的 Hello 报文，则认为对端路由器失效，这个一定的时间就是相邻路由器间的失效时间。 LSA 重传间隔：指定接口重传 LSA（链路状态通告）的时间间隔，单位为秒。默认值是 5 秒。范围是 3 到 65535 秒。 LSU 传输时间：指定发送链路状态更新报文的延迟时间，单位为秒。默认值是 1 秒。范围是 1 到 65535 秒。
优先级	指定接口路由器的优先级。默认值是 1。范围是 0 到 255。优先级为 0 的路由器不会被选中作为指定路由器（用来接收网络中所有其他路由器的链路信息，并将收到的链路信息广播出去）。当同一个网络的两个路由器都可作为指定路由器时，优先级高的路由器会被选中；如果优先级也相同，Router ID 高的会被选中。
网络类型	指定接口的网络类型，包括广播、点到点（Point-to-point）以及点到多点（Point-to-multipoint）网络类型。默认情况下，接口的网络类型为广播类型。
链路开销	点击“启用”按钮，开启链路开销功能。指定接口的链路开销值，取值范围是 1 到 65535。默认情况下，“HA 同步”复选框是开启的，该接口的链路开销将会同步到备设备；取消勾选该复选框，该接口的链路开销将不会同步到备设备。

选择“网络 > 路由 > OSPFv3”，点击“接口配置”，打开<接口配置>页面，展开配置接口的 OSPFv3 功能。

选项	说明
区域 ID	指定接口所属区域的 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。
实例 ID	指定接口所属的实例 ID。取值范围是 0 到 255。默认值是 0。

选项	说明
接口定时器	接口的定时器有以下四个：接口发送 Hello 包的时间间隔、接口相邻路由器的失效时间、接口重传 LSA 的时间间隔以及接口更新包的延迟时间。 Hello 发送间隔：指定接口发送 Hello 包的时间间隔，单位为秒。默认值是 10 秒。范围是 1 到 65535 秒。 失效时间：指定接口的相邻路由失效时间，单位为秒。默认值是 40 秒（发送 Hello 包时间间隔的 4 倍）。范围是 1 到 65535 秒。 如果接口在一定的时间内都没有收到对方的 Hello 报文，则认为对端路由器失效，这个一定的时间就是相邻路由器间的失效时间。 LSA 重传间隔：指定接口重传 LSA（链路状态通告）的时间间隔，单位为秒。默认值是 5 秒。范围是 3 到 65535 秒。 LSU 传输时间：指定发送链路状态更新报文的延迟时间，单位为秒。默认值是 1 秒。范围是 1 到 65535 秒。
优先级	指定接口路由器的优先级。默认值是 1。范围是 0 到 255。优先级为 0 的路由器不会被选中作为指定路由器（用来接收网络中所有其他路由器的链路信息，并将收到的链路信息广播出去）。当同一个网络的两个路由器都可作为指定路由器时，优先级高的路由器会被选中；如果优先级也相同，Router ID 高的会被选中。
链路开销	指定接口的链路开销值，取值范围是 1 到 65535。
被动	用户可以将一些接口配置为只接收更新但是不发送，这种只接收更新的接口就是被动接口。点击“启用”按钮，开启该接口为被动接口。
忽略 MTU	OSPFv3 通过 DBD 报文检查邻居间的接口 MTU 设置是否匹配。如果相邻的 OSPFv3 路由器接口之间的 MTU 不匹配，则他们之间不能建立邻接关系。用户可通过修改接口的 MTU 来解决此问题。但是，有些接口无法修改 MTU，这时候用户可选中“启用”复选框，使 OSPFv3 忽略对 MTU 匹配的检查。

点击“IPv6 配置”后的“启用”按钮，展开 IPv6 配置项，配置接口的 IPv6 信息。

选项	说明

选项	说明
启用	点击“启用”按钮，开启接口的 IPv6 功能。
IPv6 地址	为接口指定 IPv6 地址前缀。
前缀长度	指定 IPv6 地址的前缀长度。
无状态地址自动配置	选中该复选框，开启无状态地址自动配置模式。在该模式下，接口先接收 RA 报文中的地址前缀，然后结合接口标识得到一个全球地址。如果为该接口指定了缺省路由器(即启用默认路由)，指定该参数将产生一条缺省路由器的缺省路由。
启用 DNS 代理	选中该选项复选框开启接口的 IPv6 域名代理功能。
DHCP	用户可以将设备的接口配置成 DHCP 客户端，并从 DHCP 服务器获得 IPv6 地址。选中 DHCP 复选框开启接口的 DHCP 客户端功能。若勾选“rapid-commit”复选框，系统将与服务器进行快速交互以获取 IPv6 地址。仅当客户端的 rapid-commit 与服务器的 rapid-commit 功能都启用时，该功能生效。 设备的接口还可以作为 DHCP 服务器和 DHCP 中继代理。启用 IPv6 后，点击 DHCP 下拉菜单，选中“DHCPv6 服务器”配置 DHCP 服务器的 IPv6 功能。点击 DHCP 下拉菜单，选中“DHCPv6 中继代理”配置 DHCP 中继代理的 IPv6 功能。
IPv6 高级选项	
静态地址	点击“新建”按钮，添加多个 IPv6 地址。目前支持最多添加 5 个。点击“删除”按钮，删除选中的 IPv6 地址。
动态地址	该列表显示所有自动学习得到的 IPv6 地址。
Link-local	指定链路本地地址。链路本地地址（link-local 地址）用于同一链路的相邻节点间通信，例如单条链路上没有路由器时主机间的通信。默认情况下，开启接口的 IPv6 功能后， 系统会自动为接口生成一个链路本地地址，用户也可以根据需要为接口指定，指定的链路本地地址将取代系统自动生成的链路本地地址。
MTU	指定接口 IPv6 最大传输单元的值。当设备通过接口发送 RA 报文时，用户可以指定是否在 RA 报文中包含 MTU 值告知其他路由器。默认情况下将通告 MTU 值。单位为字节，默认值为 1500。取值范围是 1280 到 1800/2000（不同型号的设备支持的 MTU 最大值不同）。如果开启巨帧报文（Jumbo Frame）转发功能，该最大传输单元的取值范围变为 1280 到 9300，默认值为 1500。
地址冲突检测	指定接口发送 NS（邻居请求，Neighbor Solicitation） 报文的次数。取值为 0 表示接口不启用地址冲突检测功能。系统支持地址冲突检测功能，其作用为验证 IPv6 地址的唯一性。该功能是通过发

选项	说明
	送 NS 报文实现的。NS 报文发出后，如果链路上有其他主机发现发送 NS 请求方的地址与自己的重复，它就会发送 NA（邻居通告，Neighbor Advertisment）报文告知对方这个地址已经有人在用，然后发送 NS 请求方会把这 个地址标记为“Duplicate”状态，这个地址就是一个无效的 IPv6 地址。取值范围为 0-20。
邻居发现学习	点击“启用”按钮，开启接口的邻居发现学习功能。 接口通过邻居发现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的邻居发现表中。默认情况下，接口的邻居发现学习功能是开启的，接口会持续进行邻居发现学习，并将学到的 IP-MAC 绑定信息添加到系统的邻居发现表中。关闭该功能后，只有已经在邻居发现表中的 IP 地址才可以通过接口转发报文。
邻居发现学习限制	当一个接口接入的某个用户主机发起邻居发现攻击时，可能会出现耗尽邻居发现表项资源的情况，导致其他接口无法进行邻居发现学习。为避免上述问题，系统支持开启邻居发现学习限制功能，并指定该接口允许学习的最大数量。指定后，如果一个接口达到了允许学习的最大数量，将不再允许该接口继续进行邻居发现学习。 点击“启用”按钮，开启接口的邻居发现学习限制功能，并在文本框中输入接口允许学习的最大数量。范围是 1 到 Capacity。
邻居消息发送间隔	指定接口发送 NS 报文的时间间隔，单位为毫秒。取值范围为 1000-3600000。
邻居消息超时时间	指接口在发送 NS 报文后，在得到邻居可达性确认后，认为邻居可达的时间。取值范围为 0-3600000。
发包跳数	指定接口发出的 IPv6 报文的最大跳数或者 RA 报文中的最大跳数。取值范围为 0-255。
禁用 RA 报文	点击“启用”按钮，系统将禁用 RA 报文。默认情况下，配置了 IPv6 单播路由的 FDDI 接口会自动发送 RA 报文，其他类型的接口不发送 RA 报文。
管理 IP/MASK	设置接口的管理 IP。

新建隧道接口

新建隧道接口，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“隧道接口”，打开<隧道接口>页面。

在此页面，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。不同平台的取值范围不同，请以实际为准
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”或者“三层安全域”，则继续从“安全域”下拉菜单选择安全域的名称。 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。
HA 同步	点击“启用”按钮，开启 HA 同步，即关闭 HA Local 属性，接口使用虚 MAC，此时主设备和备用设备信息同步；不选该选项复选框关闭 HA 同步，即开启 HA Local 属性，接口保持原有 MAC 地址，此时主设备和备用设备信息不再同步。
IP 配置	
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。
	配置为 Local IP：两台设备形成 HA 组网时，配置该选项，接口的 IP 配置将不会同步到 HA 对端。
	高级选项：

选项	说明
	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 10 个二级 IP 地址。 注意: 配置的接口的二级 IP 地址与接口当前 IP 地址必须在不同网段。
	DHCP：点击“DHCP”按钮，打开<DHCP 配置>页面为接口进行 DHCP 配置。
	DDNS：点击“DDNS”按钮，打开<DDNS 配置>页面为接口进行 DDNS 配置。 说明：该功能仅在编辑已新建接口时有效，新建接口时无效。
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 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。 无类别静态路由：开启无类别静态路由选项功能。启用后，DHCP 客户端将会向服务器端发送带有 Option121（即无类别静态路由选项）的请求报文，服务器端收到请求后将发送无类别静态路由信息给客户端。最终，客户端将收到的无类别静态路由信息添加到路由表中。

选项	说明
	DDNS：点击“DDNS”按钮，打开<DDNS 配置>页面为接口进行 DDNS 配置。 说明：该功能仅在编辑已新建接口时有效，新建接口时无效。
管理方式	选中该接口需要的管理方式的复选框。包括 SSH、Ping、HTTPS 、SNMP、NETCONF、TRACEROUTE、HTTP 和 Telnet。
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。
上行带宽	指定接口上行带宽的最大值。
下行带宽	指定接口下行带宽的最大值。
隧道绑定配置：绑定隧道接口到 VPN 隧道和 ZTNA 实例。一个隧道接口可以绑定多个 IPsec VPN 隧道，但仅可以绑定一个 SCVPN 隧道。	
新建	点击“新建”按钮，弹出可编辑行，指定类型/名称/网关。
类型	指定绑定到隧道接口的 VPN 隧道和 ZTNA 实例的名称。
名称	指定绑定到接口的 VPN 隧道和 ZTNA 实例的名称。
域名	为 L2TP 隧道绑定域名。绑定域名后，如果登陆 用户的用户名不存在域名，拨号将失败。如果没有为 L2TP 实例绑定域名，LNS 进行认证时将忽略 登录用户的域名。
IPv4 网关/IPv6 网关	添加隧道的下一跳 IP 地址，可以为对端隧道接口的 IP 地址或者对端出接口的 IP 地址。可以选择配置 IPv4 类型地址或 IPv6 类型地址，仅当绑定 GRE VPN 隧道时，可以同时配置 IPv4 类型地址或 IPv6 类型地址。

3. **点击“接口属性”，展开接口属性配置项，配置接口的属性信息。**

选项	说明
参数	
MTU	指定接口的最大传输单元，单位为字节。范围是 1280 到 1800/2000

选项	说明
	字节之间（不同型号的设备支持的 MTU 最大值不同），默认值是 1500 字节。
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	在文本框中输入指定的 MAC 地址，将其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。
上行带宽	指定接口上行带宽的最大值。
下行带宽	指定接口下行带宽的最大值。

4. **点击“IPv6 配置”后的“启用”按钮，展开 IPv6 配置项，配置接口的 IPv6 信息。**

选项	说明
启用	点击“启用”按钮，开启接口的 IPv6 功能。
IPv6 地址	为接口指定 IPv6 地址前缀。
前缀长度	指定 IPv6 地址的前缀长度。
无状态地址自动配置	选中该复选框，开启无状态地址自动配置模式。在该模式下，接口先接收 RA 报文中的地址前缀，然后结合接口标识得到一个全球地址。如果为该接口指定了缺省路由器(即启用默认路由)，指定该参数将产生一条缺省路由器的缺省路由。
启用 DNS 代理	选中该选项复选框开启接口的 IPv6 域名代理功能。
DHCP	用户可以将设备的接口配置成 DHCP 客户端，并从 DHCP 服务器获得 IPv6 地址。选中 DHCP 复选框开启接口的 DHCP 客户端功能。若勾选“rapid-commit”复选框，系统将与服务器进行快速交互以获取 IPv6 地址。仅当客户端的 rapid-commit 与服务器的 rapid-commit 功能都启用时，该功能生效。 设备的接口还可以作为 DHCP 服务器和 DHCP 中继代理。启用 IPv6 后，点击 DHCP 下拉菜单，选中“DHCPv6 服务器”配置 DHCP 服务器的 IPv6 功能。点击 DHCP 下拉菜单，选中“DHCPv6 中继代理”配置 DHCP 中继代理的 IPv6 功能。
IPv6 高级选项	
静态地址	点击“新建”按钮，添加多个 IPv6 地址。目前支持最多添加 5 个。点击“删除”按钮，删除选中的 IPv6 地址。
动态地址	该列表显示所有自动学习得到的 IPv6 地址。
Link-local	指定链路本地地址。链路本地地址（link-local 地址）用于同一链路的相邻节点间通信，例如单条链路上没有路由器时主机间的通信。

选项	说明
	默认情况下，开启接口的 IPv6 功能后， 系统会自动为接口生成一个链路本地地址，用户也可以根据需要为接口指定，指定的链路本地地址将取代系统自动生成的链路本地地址。
MTU	指定接口 IPv6 最大传输单元的值。当设备通过接口发送 RA 报文时，用户可以指定是否在 RA 报文中包含 MTU 值告知其他路由器。默认情况下将通告 MTU 值。单位为字节，默认值为 1500。取值范围是 1280 到 1800/2000（不同型号的设备支持的 MTU 最大值不同）。
地址冲突检测	指定接口发送 NS（邻居请求，Neighbor Solicitation） 报文的次数。取值为 0 表示接口不启用地址冲突检测功能。系统支持地址冲突检测功能，其作用为验证 IPv6 地址的唯一性。该功能是通过发送 NS 报文实现的。NS 报文发出后，如果链路上有其他主机发现发送 NS 请求方的地址与自己的重复，它就会发送 NA（邻居通告，Neighbor Advertisment）报文告知对方这个地址已经有人在用，然后发送 NS 请求方会把这 个地址标记为“Duplicate”状态，这个地址就是一个无效的 IPv6 地址。取值范围为 0-20。
邻居消息发送间隔	指定接口发送 NS 报文的时间间隔，单位为毫秒。取值范围为 1000-3600000。
邻居消息超时时间	指接口在发送 NS 报文后，在得到邻居可达性确认后，认为邻居可达的时间。取值范围为 0-3600000。
发包跳数	指定接口发出的 IPv6 报文的最大跳数或者 RA 报文中的最大跳数。取值范围为 0-255。
禁用 RA 报文	点击“启用”按钮，系统将禁用 RA 报文。默认情况下，配置了 IPv6 单播路由的 FDDI 接口会自动发送 RA 报文，其他类型的接口不发送 RA 报文。
管理 IP/MASK	设置接口的管理 IP。

5. 点击“确定”，完成配置。

新建 Virtual Forward 接口

新建 Virtual Forward 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“Virtual Forward 接口”，打开<Virtual Forward 接口>页面。

在此页面，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 0-63 个字符。
绑定安全域	如选择“二层安全域”或者“三层安全域”，则继续从“安全域”下拉菜单选择安全域的名称。 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。
IP 配置：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。
	配置为 Local IP：两台设备形成 HA 组网时，配置该选项，接口的 IP 配置将不会同步到 HA 对端。
	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。

选项	说明
	二级 IP：为接口指定二级 IP。最多可以指定 10 个二级 IP 地址。
	DHCP：点击“DHCP”按钮，打开<DHCP 配置>页面为接口进行 DHCP 配置。
	DDNS：点击“DDNS”按钮，打开<DDNS 配置>页面为接口进行 DDNS 配置。 说明：该功能仅在编辑已新建接口时有效，新建接口时无效。
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，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 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。 无类别静态路由：开启无类别静态路由选项功能。启用后，DHCP 客户端将会向服务器端发送带有 Option121（即无类别静态路由选项）的请求报文，服务器端收到请求后将发送无类别静态路由信息给客户端。最终，客户端将收到的无类别静态路由信息添加到路由表中。
	DDNS：点击“DDNS”按钮，打开<DDNS 配置>选项为接口进行 DDNS 配置。 说明：该功能仅在编辑已新建接口时有效，新建接口时无效。
管理方式	选中该接口需要的管理方式的复选框。包括 SSH、Ping、HTTPS 、SNMP、NETCONF、TRACEROUTE、HTTP 和 Telnet。
隧道绑定配置：绑定隧道接口到 VPN 隧道。一个隧道接口可以绑定多个 IPsec VPN 隧道，但仅可以绑定一个 SCVPN 隧道。	
新建	点击“新建”按钮，弹出可编辑行，指定类型/VPN 名称/网关。
类型	指定绑定到隧道接口的 IPsec VPN 隧道的名称。当需要为隧道接口绑定多个 IPsec VPN 隧道时，此配置参数有效。系统默认值为 0.0.0.0。

选项	说明
VPN 名称	指定绑定到接口的 SSL VPN 隧道的名称。
网关	添加隧道的下一跳 IP 地址，可以为对端隧道接口的 IP 地址或者对端出接口的 IP 地址。
WebAuth	
认证服务	根据需要选择启用、关闭或者使用全局默认。 启用：开启指定接口的 Web 认证功能。 关闭：关闭指定接口的 Web 认证功能。 使用全局默认：指定接口 Web 认证功能使用全局默认配置。
主动认证	点击“启用”按钮，开启 Web 主动认证功能，并从下拉菜单中选择 AAA 服务器。 开启后，用户可通过访问 Web 认证地址主动发起认证请求，然后在认证登录页面填写正确的用户名和密码即可进行认证。Web 认证地址为该接口的 IP 地址+认证服务器的 HTTP 或 HTTPS 的端口号，如接口的 IP 地址为 192.168.3.1，认证服务器 HTTP 和 HTTPS 的端口号被分别配置为 8182、44434，则认证服务器配置为 HTTP 模式时 Web 认证地址为：http:// 192.168.3.1:8182；认证服务器配置为 HTTPS 模式时，Web 认证地址为 https:// 192.168.3.1:44434。
WebAuth 域名	指定接口对应的 Web 认证域名，取值范围是 1 到 255 个字符。为 Web 认证地址配置域名后，访问服务时弹出的 Web 认证页面（被动认证）的 URL 将显示为域名形式。配置该功能前，需先开启 Web 认证功能。

3. 点击“确定”，完成配置。

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”，打开<回环接口>页面。

在此页面，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 0-63 个字符。
绑定安全域	如选择“三层安全域”，则继续从“安全域”下拉菜单选择安全域的名称。 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。
HA 同步	点击“启用”按钮，开启 HA 同步，即关闭 HA Local 属性，接口使用虚 MAC，此时主设备和备用设备信息同步；不选该选项复选框关闭 HA 同步，即开启 HA Local 属性，接口保持原有 MAC 地址，此时主设备和备用设备信息不再同步。
IP 配置：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。
	配置为 Local IP：两台设备形成 HA 组网时，配置该选项，接口的 IP 配置将不会同步到 HA 对端。

选项	说明
	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 10 个二级 IP 地址。
	DHCP：打开<DHCP 配置>页面为接口进行 DHCP 配置。
	DDNS：点击“DDNS”按钮，打开<DDNS 配置>页面为接口进行 DDNS 配置。 说明：该功能仅在编辑已新建接口时有效，新建接口时无效。
自动获取	DHCP 服务器提供的网关信息设置为默认网关路由：选择此选项，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 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。 无类别静态路由：开启无类别静态路由选项功能。启用后，DHCP 客户端将会向服务器端发送带有 Option121（即无类别静态路由选项）的请求报文，服务器端收到请求后将发送无类别静态路由信息给客户端。最终，客户端将收到的无类别静态路由信息添加到路由表中。
	DDNS：点击“DDNS”按钮，打开<DDNS 配置>页面为接口进行 DDNS 配置。 说明：该功能仅在编辑已新建接口时有效，新建接口时无效。
管理方式	选中该接口需要的管理方式的复选框。包括 SSH、Ping、HTTPS 、SNMP、NETCONF、TRACEROUTE、HTTP 和 Telnet。

3. 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”，打开<集聚接口>页面。

3. **在此页面，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 0-63 个字符。
绑定安全域	指定安全域类型。 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 IPv4 或者 IPv6 内网地址，使设备能够辨别内网流量，并在监控中进行展示。同时，可在下方“防火墙联动配置”中指定防火墙信息（防火墙 IPv4 或者 IPv6 地址，SSH 协议的端口号，登录用户名和密码），与防火墙联动。当设备工作在旁路模式且此接口作为镜像流量接口时，如果进行了以下一种或者几种配置，设备会将命中的流量信息发送给联动防火墙进行阻断：

<table>
<tr><th>选项</th><th>说明</th></tr>
<tr><td></td><td>源安全域和目的安全域为此 TAP 域的安全策略，且绑定到此安全策略的 IPS 规则的动作为“阻断 IP”或“阻断服务”；
源安全域为此 TAP 域的共享接入规则，且规则中指定的超限动作为“阻断”；
源安全域和目的安全域为此 TAP 域的安全策略，且绑定到此安全策略的终端防护规则的防护动作为“阻断”；
安全域为此 TAP 域的边界流量过滤功能，且指定的处理动作为“阻断 IP”。
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：</td></tr>
<tr><td></td><td><table><tr><td>属于</td><td>说明</td></tr><tr><td>集聚接口</td><td>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。</td></tr><tr><td>冗余接口</td><td>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。</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>HA 同步</td><td>点击“启用”按钮，开启 HA 同步，即关闭 HA Local 属性，接口使用虚 MAC，此时主设备和备用设备信息同步；点击禁用按钮，关闭 HA 同步，即开启 HA Local 属性，接口保持原有 MAC 地址，此时主设备和备用设备信息不再同步。</td></tr>
<tr><td colspan="2">IP 配置：根据 IP 类型不同进行如下的配置，包括静态 IP、自动获取和 PPPoE 方式获取。</td></tr>
<tr><td>静态 IP</td><td>IP 地址：为接口指定 IP 地址。</td></tr>
<tr><td></td><td>网络掩码：为接口指定网络掩码。</td></tr>
<tr><td></td><td>配置为 Local IP：两台设备形成 HA 组网时，配置该选项，接口的 IP 配置将不会同步到 HA 对端。</td></tr>
<tr><td></td><td>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 10 个二级 IP 地址。</td></tr>
<tr><td></td><td>DHCP：打开<DHCP 配置>页面为接口进行 DHCP 配置。</td></tr>
<tr><td></td><td>DDNS：点击“DDNS”按钮，打开<DDNS 配置>页面为接口进行</td></tr>
</table>

选项	说明
	DDNS 配置。 说明：该功能仅在编辑已新建接口时有效，新建接口时无效。
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 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。 无类别静态路由：开启无类别静态路由选项功能。启用后，DHCP 客户端将会向服务器端发送带有 Option121（即无类别静态路由选项）的请求报文，服务器端收到请求后将发送无类别静态路由信息给客户端。最终，客户端将收到的无类别静态路由信息添加到路由表中。
	DDNS：点击“DDNS”按钮，打开<DDNS 配置>页面为接口进行 DDNS 配置。 说明：该功能仅在编辑已新建接口时有效，新建接口时无效。
PPPoE	通过 PPPoE 方式获取 IP 地址。选取该方式后，配置如下选项： 用户：指定 PPPoE 用户名称。 密码：指定 PPPoE 用户相应的密码。 确认密码：再次输入密码进行确认。 挂断前空闲间隔：当 PPPoE 接口的空闲（无流量）时间到达一定的时间，即指定的空闲间隔，系统会断开与因特网的连接；当产生上网需求时，系统会自动连接到因特网。该选项指定空闲间隔时间，单位为分钟。范围是 0 到 10000 秒，默认值是 30。 重拨间隔：指定重拨间隔时间（系统在断开连接后自动重拨的时间间隔），单位为秒。范围是 0 到 10000 秒。默认值是 0，表示不进行自动 重拨

选项	说明
	PPPoE 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 PPPoE 服务器提供的网关信息设置为默认网关路由。
管理方式	选中该接口需要的管理方式的复选框。 包括 SSH、Ping、HTTPS 、SNMP、NETCONF、TRACEROUTE、HTTP 和 Telnet。
绑定端口	
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。
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。
TAP 配置	控制接口：指定旁路的控制接口，旁路控制接口用于发送控制报文（目前可以发送 TCP RST 控制报文）。在旁路设备中配置 IPS、病毒过滤或者网络行为控制的阻断功能后，如果设备检测到攻击、病毒或者访问受限网站的行为，就会通过旁路控制接口向干路设备发送 TCP RST 控制报文，重置 TCP 连接，从而对流量进行阻断。默认情况下，旁路控制接口为旁路接口本身。而对于隧道接口，若使用本身接口作为控制接口，其发送的控制报文对端可能无法正确处理。因此建议旁路的隧道接口配置其他接口作为控制接口。配置时，须保证该控制接口可以正常发送报文到干路设备上。 内网地址：指定内网地址范围，系统仅对源 IP 在指定内网地址范围的数据包进行统计和检测。
防火墙联动配置	指定联动防火墙的信息（防火墙 IP 地址、端口号、用户名和密码），与防火墙联动。若设备检测到攻击流量，会将攻击源的 IP 以黑名单的形式下发到联动的防火墙，联动防火墙将对攻击源 IP 的流量进行阻断。 IP：指定联动的防火墙的 IP 地址。 端口：指定联动的防火墙的 SSH 协议的端口号。 用户：指定登录联动的防火墙的用户名。 密码：指定登录联动的防火墙的密码。 修改密码：编辑 TAP 配置时，可以看到修改密码功能。开启后，将展示密码输入框。如需修改，输入新的密码后保存配置即可。
WebAuth	

选项	说明
认证服务	根据需要选择启用、关闭或者使用全局默认。 启用：开启指定接口的 Web 认证功能。 关闭：关闭指定接口的 Web 认证功能。 使用全局默认：指定接口 Web 认证功能使用全局默认配置。
主动认证	点击“启用”按钮，开启 Web 主动认证功能，并从下拉菜单中选择 AAA 服务器。开启后，用户可通过访问 Web 认证地址主动发起认证请求，然后在认证登录页面填写正确的用户名和密码即可进行认证。Web 认证地址为该接口的 IP 地址+认证服务器的 HTTP 或 HTTPS 的端口号，如接口的 IP 地址为 192.168.3.1，认证服务器 HTTP 和 HTTPS 的端口号被分别配置为 8182、44434，则认证服务器配置为 HTTP 模式时 Web 认证地址为：http:// 192.168.3.1:8182；认证服务器配置为 HTTPS 模式时，Web 认证地址为 https:// 192.168.3.1:44434。
WebAuth 域名	指定接口对应的 Web 认证域名，取值范围是 1 到 255 个字符。为 Web 认证地址配置域名后，访问服务时弹出的 Web 认证页面（被动认证）的 URL 将显示为域名形式。配置该功能前，需先开启 Web 认证功能。

4. 点击“负载均衡”，展开负载均衡配置项，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。

5. 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”，打开<冗余接口>页面。

3. 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”，打开相应接口页面。
3. **在此页面，配置接口的基本配置信息。**

选项	说明

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 0-63 个字符。
绑定安全域	如选择“二层安全域”或者“三层安全域”，则继续从“安全域”下拉菜单选择安全域的名称。 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。
HA 同步	点击“启用”按钮，开启 HA 同步，即关闭 HA Local 属性，接口使用虚 MAC，此时主设备和备用设备信息同步；不选该选项复选框关闭 HA 同步，即开启 HA Local 属性，接口保持原有 MAC 地址，此时主设备和备用设备信息不再同步。
IP 配置：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。
	配置为 Local IP：两台设备形成 HA 组网时，配置该选项，接口的 IP 配置将不会同步到 HA 对端。
	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 10 个二级 IP 地址。
	DHCP：打开<DHCP 配置>页面为接口进行 DHCP 配置。
	DDNS：点击“DDNS”按钮，打开<DDNS 配置>页面为接口进行 DDNS 配置。 说明：该功能仅在编辑已新建接口时有效，新建接口时无效。
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，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 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

选项	说明
	先级越高。静态配置的 DNS 服务器的优先级是 20。 无类别静态路由：开启无类别静态路由选项功能。启用后，DHCP 客户端将会向服务器端发送带有 Option121（即无类别静态路由选项）的请求报文，服务器端收到请求后将发送无类别静态路由信息给客户端。最终，客户端将收到的无类别静态路由信息添加到路由表中。
	DDNS：点击“DDNS”按钮，打开<DDNS 配置>页面为接口进行 DDNS 配置。 说明：该功能仅在编辑已新建接口时有效，新建接口时无效。
PPPoE	通过 PPPoE 方式获取 IP 地址。此选项仅创建集聚子接口时有效。选取该方式后，配置如下选项： 用户：指定 PPPoE 用户名称。 密码：指定 PPPoE 用户相应的密码。 确认密码：再次输入密码进行确认。 挂断前空闲间隔：当 PPPoE 接口的空闲（无流量）时间到达一定的时间，即指定的空闲间隔，系统会断开与因特网的连接；当产生上网需求时，系统会自动连接到因特网。该选项指定空闲间隔时间，单位为分钟。范围是 0 到 10000 秒，默认值是 30。 重拨间隔：指定重拨间隔时间（系统在断开连接后自动重拨的时间间隔），单位为秒。范围是 0 到 10000 秒。默认值是 0，表示不进行自动重拨 PPPoE 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 PPPoE 服务器提供的网关信息设置为默认网关路由。
管理方式	选中该接口需要的管理方式的复选框。包括 SSH、Ping、HTTPS 、SNMP、NETCONF、TRACEROUTE、HTTP 和 Telnet。
WebAuth	
认证服务	根据需要选择启用、关闭或者使用全局默认。 启用：开启指定接口的 Web 认证功能。 关闭：关闭指定接口的 Web 认证功能。 使用全局默认：指定接口 Web 认证功能使用全局默认配置。

选项	说明
主动认证	点击“启用”按钮，开启 Web 主动认证功能，并从下拉菜单中选择 AAA 服务器。开启后，用户可通过访问 Web 认证地址主动发起认证请求，然后在认证登录页面填写正确的用户名和密码即可进行认证。Web 认证地址为该接口的 IP 地址+认证服务器的 HTTP 或 HTTPS 的端口号，如接口的 IP 地址为 192.168.3.1，认证服务器 HTTP 和 HTTPS 的端口号被分别配置为 8182、44434，则认证服务器配置为 HTTP 模式时 Web 认证地址为：http:// 192.168.3.1:8182；认证服务器配置为 HTTPS 模式时，Web 认证地址为 https:// 192.168.3.1:44434。
WebAuth 域名	指定接口对应的 Web 认证域名，取值范围是 1 到 255 个字符。为 Web 认证地址配置域名后，访问服务时弹出的 Web 认证页面（被动认证）的 URL 将显示为域名形式。配置该功能前，需先开启 Web 认证功能。

4. 点击“确定”，完成配置。

新建 VSwitch 接口

新建 VSwitch 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“VSwitch 接口”，打开<VSwitch 接口>页面。

3. 点击“确定”，完成配置。

编辑以太网接口/HA 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/HA 接口，然后点击列表右上方的“编辑”按钮，打开<Ethernet 配置>/<HA 接口配置>页面。
3. **在此页面，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“二层安全域”、“三层安全域”或者“TAP”（HA 接口不支持“TAP”选项），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 IPv4 或者 IPv6 内网地址，使设备

<table>
<tr><th>选项</th><th>说明</th></tr>
<tr><td></td><td>能够辨别内网流量，并在监控中进行展示。同时，可在下方“防火墙联动配置”中指定防火墙信息（防火墙 IPv4 或者 IPv6 地址，SSH 协议的端口号，登录用户名和密码），与防火墙联动。当设备工作在旁路模式且此接口作为镜像流量接口时，如果进行了以下一种或者几种配置，设备会将命中的流量信息发送给联动防火墙进行阻断：
源安全域和目的安全域为此 TAP 域的安全策略，且绑定到此安全策略的 IPS 规则的动作为“阻断 IP”或“阻断服务”；
源安全域为此 TAP 域的共享接入规则，且规则中指定的超限动作为“阻断”；
源安全域和目的安全域为此 TAP 域的安全策略，且绑定到此安全策略的终端防护规则的防护动作为“阻断”；
安全域为此 TAP 域的边界流量过滤功能，且指定的处理动作为“阻断 IP”。
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：</td></tr>
<tr><td></td><td>
<table>
<tr><th>属于</th><th>说明</th></tr>
<tr><td>集聚接口</td><td>指定接口属于某集聚接口。
接口：从下拉菜单中选择所属的集聚接口。
端口 LACP 优先级：指定端口的 LACP 优先级。接口 LACP 优先级用于区分聚合组各成员接口变成 Selected 状态的优先程度，优先级高的成员接口将被优先选作 Selected 接口。数值越小，优先级越高。成员接口 LACP 优先级和 LACP 系统优先级通常配合使用，决定聚合组内的哪些链路将被成功聚合。
端口超时模式：指定 LACP 超时模式。LACP 超时模式有“快速（1 秒）”和“慢速（30 秒）”两种取值。即成员接口等待接收 LACPDU 的超时时间。在三倍 LACP 超时时间之后，如果本端成员接口仍未收到来自对端的 LACPDU，则认为对端成员接口已失效，接口会从 Active 状态切换到 Selected 状态，停止流量转发。</td></tr>
<tr><td>冗余接口</td><td>指定接口属于某冗余接口。从“接口”下拉菜单中选择所属的冗余接口。</td></tr>
</table>
</td></tr>
</table>

选项	说明
	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。
IP 配置：根据 IP 类型不同进行如下的配置，包括静态 IP、自动获取和 PPPoE	
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。
	配置为 Local IP：两台设备形成 HA 组网时，配置该选项，接口的 IP 配置将不会同步到 HA 对端。
	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 10 个二级 IP 地址。
	DHCP：打开<DHCP 配置>页面为接口进行 DHCP 配置。
	DDNS：点击“DDNS”按钮，打开<DDNS 配置>页面为接口进行 DDNS 配置。 说明：该功能仅在编辑已新建接口时有效，新建接口时无效。
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，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 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。 无类别静态路由：开启无类别静态路由选项功能。启用后，DHCP 客户端将会向服务器端发送带有 Option121（即无类别静态路由选项）的请求报文，服务器端收到请求后将发送无类别静态路由信息给客户端。最终，客户端将收到的无类别静态路由信息添加到路由表中。
	DDNS：点击“DDNS”按钮，打开<DDNS 配置>页面为接口进行 DDNS 配置。 说明：该功能仅在编辑已新建接口时有效，新建接口时无效。

选项	说明
PPPoE	用户名：指定 PPPoE 用户名称。 密码：指定 PPPoE 用户相应的密码。 确认密码：再次输入密码进行确认。 挂断前空闲间隔：当 PPPoE 接口的空闲（无流量）时间到达一定的时间，即指定的空闲间隔，系统会断开与因特网的连接；当产生上网需求时，系统会自动连接到因特网。该选项指定空闲间隔时间，单位为分钟。范围是 0 到 10000 秒，默认值是 30。 重拨间隔：该选项指定重拨间隔时间（系统在断开连接后自动重拨的时间间隔），单位为秒。范围是 0 到 10000 秒。默认值是 0，表示不进行自动重拨。 PPPoE 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 PPPoE 服务器提供的网关信息设置为默认网关路由。 高级选项 访问集中器：指定访问集中器的名称。 认证：设备与 PPPoE 服务器建立连接时，需要通过 PPPoE 认证。设备支持的验证方式有 CHAP、PAP 和任意（系统默认方式，表示 CHAP 或者 PAP 的任意一种）。选中需要的认证方式的单选按钮。 网络掩码：为 PPPoE 方式获得的 IP 地址指定网络掩码。 静态 IP：用户可以指定一个静态的 IP 地址，并协商使用该静态 IP 地址。这样可以避免 IP 地址变化。该选项指定静态 IP 地址。在文本框中输入静态 IP 地址。 服务：指定允许的服务。此处指定的服务必须与 PPPoE 服务器端提供的服务相同。如果不指定服务，设备自动接受服务器返回的任何服务。 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。 PPPoE 服务器提供的网管信息设置为默认网关路由：选中该选项，系统会将 PPPoE 服务器提供的网关信息设置为默认网关路由。
管理方式	选中该接口需要的管理方式的复选框。包括 SSH、Ping、HTTPS 、SNMP、NETCONF、TRACEROUTE、HTTP 和 Telnet。
WebAuth	
认证服务	根据需要选择启用、关闭或者使用全局默认。 启用：开启指定接口的 Web 认证功能。 关闭：关闭指定接口的 Web 认证功能。 使用全局默认：指定接口 Web 认证功能使用全局默认配置。

选项	说明
主动认证	点击“启用”按钮，开启 Web 主动认证功能，并从下拉菜单中选择 AAA 服务器。 开启后，用户可通过访问 Web 认证地址主动发起认证请求，然后在认证登录页面填写正确的用户名和密码即可进行认证。Web 认证地址为该接口的 IP 地址+认证服务器的 HTTP 或 HTTPS 的端口号，如接口的 IP 地址为 192.168.3.1，认证服务器 HTTP 和 HTTPS 的端口号被分别配置为 8182、44434，则认证服务器配置为 HTTP 模式时 Web 认证地址为：http:// 192.168.3.1:8182；认证服务器配置为 HTTPS 模式时，Web 认证地址为 https:// 192.168.3.1:44434。
WebAuth 域名	指定接口对应的 Web 认证域名，取值范围是 1 到 255 个字符。为 Web 认证地址配置域名后，访问服务时弹出的 Web 认证页面（被动认证）的 URL 将显示为域名形式。配置该功能前，需先开启 Web 认证功能。

4. **点击“接口属性”，展开接口属性配置项，配置接口的属性信息。**

选项	说明
参数	
MTU	指定接口的最大传输单元，单位为字节。取值范围是 1280 到 1800/2000（不同型号的设备支持的 MTU 最大值不同），默认值是 1500 字节。如果开启巨帧报文（Jumbo Frame）转发功能，该最大传输单元的取值范围变为 1280 到 9300，默认值为 1500。关于巨帧报文转发功能详细信息，请参阅配置全局网络参数。
ARP 学习	点击“启用”按钮，开启接口的 ARP 学习功能。
ARP 学习限制	为避免同一个接口进行 ARP 学习时，将 IP-MAC 绑定信息占满系统 ARP 表，导致其他接口无法进行 ARP 学习，可以开启 ARP 学习限制功能，并指定该接口允许学习的最大数量。 指定后，如果一个接口达到了允许学习的最大数量，将不再允许该接口继续进行 ARP 学习。 点击“启用”按钮，开启接口的 ARP 学习限制功能，并在文本框中输入接口允许学习的最大数量。范围是 1 到 Capacity。
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	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，恢复以太网子接口的缺省 MAC 地址。
上行带宽	指定接口上行带宽的最大值。
下行带宽	指定接口下行带宽的最大值。

5. 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。

删除 VSwitch 接口的同时，相应的 VSwitch 也会一并被删除。

HA 接口无法绑定监测对象。

查看接口状态

选择“网络 > 接口”，用户可以在接口列表“接口状态”列中查看接口的状态信息，其中状态指示灯分别表示为：

物理状态：显示接口的物理状态， 表示为“已连接”； 表示为“HA 保持运行”； 表示为连接“已断开”或者“LACP 已断开”。

管理状态：显示接口的管理状态， 表示为“已连接”； 表示为连接“已断开”或者“LACP 已断开”。

链路状态：显示接口的链路状态， 表示为“已连接”； 表示为“HA 保持运行”； 表示为连接“已断开”或者“LACP 已断开”。

IPv4 协议状态（IPv4 版本中仅展示“协议状态”）：显示接口的 IPv4 协议状态， 表示为“已连接”； 表示为“HA 保持运行”； 表示为连接“已断开”或者“LACP 已断开”。

IPv6 协议状态（仅在 IPv6 版本中展示该内容）：显示接口的 IPv6 协议状态， 表示为“已连接”； 表示为“HA 保持运行”； 表示为连接“已断开”或者“LACP 已断开”。

接口列表显示如下：

新建 编辑 删除

接口名称	接口状态				上行速率	下行速率	获取类型	IP/掩码	MAC
	物理状态	管理状态	链路状态	IPv4协议状态					
vswitchif1					0 bps	0 bps	静态	0.0.0.0/0	001c.544c.271e
ethernet0/0					97.67 Kbps	99.35 Kbps	静态	192.168.0.104/24	fa16.3e76.ce36
tunnel1					0 bps	0 bps	静态	172.10.101.254/24	001c.544c.274d
tunnel2					29.89 Kbps	61.1 Kbps	静态	172.31.199.254/24	001c.544c.274e

接口组

系统支持将多个物理接口的状态相互绑定，组成一个接口组，形成接口间的联动功能。如果接口组内任何一个接口发生故障，组内其他接口状态会被设置为 Down；只有当接口组内所有接口恢复正常后，接口组内接口状态才能被设置为 Up。

新建接口组

新建接口组，请按照以下步骤进行操作：

1. 选择“网络 > 接口组”，进入接口组配置页面。
2. 点击“新建”，打开<接口组配置>页面。

3. 在“名称”文本框输入接口组的名称，该名称不能重复。名称长度可以是 1-31 个字符。
4. 在“成员”下拉菜单中，选择需要添加至接口组的接口。可添加最多 8 个接口。
   说明：接口组的成员不能与其他接口组中的成员冲突。
5. 点击“确定”，完成配置。
   用户可以点击“编辑”和“删除”按钮，编辑指定接口组的成员或删除指定接口组。

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。

代理：设备作为 DNS 代理服务器，可根据用户设定的 DNS 代理规则，对 DNS 请求进行过滤，对于符合条件的 DNS 请求，系统将转发给指定的 DNS 域名服务器。

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。

NBT 缓存：显示 NBT 缓存信息。

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>DNS 服务器”，进入 DNS 服务器配置页面。
2. 点击“新建”按钮，打开<DNS 服务器配置>页面。

3. 在“IP 类型”部分指定 DNS 服务器 IP 地址的类型，可以为 IPv4 或者 IPv6。
4. 在“虚拟路由器”下拉菜单选择 VR，默认为缺省 VR，即 trust-vr。
5. 在“服务器 IP”文本框输入 DNS 服务器的 IP 地址。
6. 点击“确定”按钮。

配置 DNS 代理

DNS 代理功能通过 DNS 代理规则来实现。DNS 代理规则分为过滤条件和行为两部分。入接口、源地址、目的地址及 DNS 域名构成 DNS 代理规则的过滤条件。DNS 代理规则的行为包括代理、放行及阻断共三种。当代理规则的行为被指定为代理时，用户需同时配置 DNS 代理服务器，这样满足条件的 DNS 请求将通过指定的 DNS 代理服务器进行地址解析。

配置 DNS 代理规则

新建 DNS 代理规则，请按照以下步骤进行操作：

1. 选择“网络 > DNS>DNS 代理”，进入 DNS 代理配置页面。

2. 点击“新建”按钮，打开<DNS 代理规则配置>页面。

在<DNS 代理规则配置>页面内进行配置：

选项	说明
类型	指定 DNS 代理规则类型，IPv4 或者 IPv6。
入接口	指定需匹配的 DNS 请求的入接口，对 DNS 请求报文进行过滤。用户可指定多个入接口。指定后，系统将按照规则设定的行为，对该入接口流量进行处理。
源地址	指定 DNS 代理规则需匹配的 DNS 请求的源地址，对 DNS 请求报文进行过滤。用户可指定多条源地址类目。点击"类型"下拉菜单，选择地址类型，然后在下方选择或输入需要的地址，然后选中所输入的域名，将其添加到左侧列表中。添加完成后，点击页面空白区域，即可完成源地址的选择。 用户还可执行如下操作： 选择地址簿类型时，可点击 ⊕ 按钮创建新的地址簿。 选择地址簿类型时，点击搜索框中的 ▼ 按钮，可以按地址簿名称和地址成员的 IP 进行模糊搜索，名称和地址是与的关系。地址支持多种输入方式，例如：输入“地址”为 10.10.10.10/32，可能匹配到包含地址成员是 10.10.10.10/24 的地址簿；输入“地址”为段掩码 9.9.9.9/24，可能匹配到包含地址成员是 9.9.0.0/16 的地址簿；输入“地址”为 10.10.10.10，可能匹配到地址成员的 IP 范围为 10.10.10.0-

选项	说明
	10.10.10.255 的地址簿；输入“地址”为 10.23，可能匹配到包含地址成员是 1.10.23.10/24 的地址簿；输入“地址”为 aa，可能匹配到地址成员的“主机名称”为 aaa 的地址簿。 选择“IPv4”类型时，系统默认 IPv4 地址配置为 any。如需恢复为 any，选择 **any** 复选框。 选择“IPv6”类型时，系统默认 IPv6 地址配置为 IPv6-any。如需恢复为 IPv6-any，选择 **IPv6-any** 复选框。
目的地址	指定 DNS 代理规则需匹配的 DNS 请求的目的地址，对 DNS 请求报文进行过滤。用户可指定多条目的地址类目。点击"类型"下拉菜单，择地址类型，然后在下方选择或输入需要的地址，然后选中所输入的域名，将其添加到左侧列表中。添加完成后，点击页面空白区域，即可完成目的地址的选择。 用户还可执行如下操作： 选择地址簿类型时，可点击 ⊕ 按钮创建新的地址簿。 选择地址簿类型时，点击搜索框中的 ▼ 按钮，可以按地址簿名称和地址成员的 IP 进行模糊搜索，名称和地址是与的关系。地址支持多种输入方式，例如：输入“地址”为 10.10.10.10/32，可能匹配到包含地址成员是 10.10.10.10/24 的地址簿；输入“地址”为段掩码 9.9.9.9/24，可能匹配到包含地址成员是 9.9.0.0/16 的地址簿；输入“地址”为 10.10.10.10，可能匹配到地址成员的 IP 范围为 10.10.10.0-10.10.10.255 的地址簿；输入“地址”为 10.23，可能匹配到包含地址成员是 1.10.23.10/24 的地址簿；输入“地址”为 aa，可能匹配到地址成员的“主机名称”为 aaa 的地址簿。 选择“IPv4”类型时，系统默认 IPv4 地址配置为 any。如需恢复为 any，选择 **any** 复选框。 选择“IPv6”类型时，系统默认 IPv6 地址配置为 IPv6-any。如需恢复为 IPv6-any，选择 **IPv6-any** 复选框。
域名	指定 DNS 代理规则需匹配的 DNS 域名，用来匹配 DNS 请求中的域名，对 DNS 请求报文进行过滤。用户可指定多条域名过滤条件。点击"类型"下拉菜单，选择域名类型，然后在下方选择或输入需要的域名，然后选中所输入的域名添加到左侧列表中。添加完成后，点击页面空白区域，即可完成域名的选择。 用户还可执行如下操作：

选项	说明
	选择域名簿类型时，可点击  按钮创建新的域名簿。 系统默认域名配置为 any。如需恢复为 any，选择 **any** 复选框。
动作	指定 DNS 代理规则的处理动作。对于符合过滤条件的 DNS 请求，系统可对其进行代理、放行和阻断流量共 3 种动作。 代理：指定 DNS 代理规则的动作为代理，即 DNS 请求将通过代理服务器进行 DNS 解析。 放行：指定 DNS 代理规则的动作为放行，即 DNS 请求将被放行并转发给原始报文的 DNS 服务器。 阻断：指定 DNS 代理规则的动作为阻断，即 DNS 请求将被并丢弃。
DNS 代理失败时	指定 DNS 代理失败后，系统对 DNS 请求报文的处理动作：阻断或放行。
日志	点击“启用”按钮，启用 DNS 代理日志功能。启用该功能后，当 DNS 请求流量匹配 DNS 代理规则时，系统会记录日志信息。
DNS 服务器	指定 DNS 代理规则的 DNS 服务器。当用户将 DNS 代理规则的行为指定为代理时，需继续指定 DNS 代理服务器。每条 DNS 规则最多可指定 6 个 DNS 代理服务器。用户可按需为 DNS 服务器绑定出接口和首选代理属性。当用户配置多个 DNS 服务器时，将首先选择首选 DNS 服务器进行域名解析。若没有指定首选服务器，系统将查询是否有指定出接口的 DNS 服务器；若有，则轮询选择出接口 DNS 服务器；若无出接口 DNS 服务器，即只有普通的 DNS 服务器，则轮询选择此类普通的 DNS 服务器。 在 DNS 服务器列表下方，点击“新建”按钮，列表将新增一条表项，输入服务器的 IP 地址（IPv4 或 IPv6 地址）及所属虚拟路由器等参数即可。
DNS64	DNS64 用于当 IPv6 客户端主机收到 DNS 查询时，先解析 DNS 查询信息中的 AAAA 记录（IPv6 地址），如果解析成功，则直接将 IPv6 地址返回给客户端；如果解析失败，那么 DNS64 将会解析 DNS 查询信息中的 A 记录（IPv4 地址），并将 A 记录（IPv4 地址）合成 AAAA 记录（IPv6 地址）返回给客户端。 点击“启用”按钮，开启设备的 DNS64 功能。默认情况下，该功能是关闭的。
DNS64 服务器	DNS64 服务器用于解析 DNS 查询信息中的 A 记录（IPv4 地址）。当用户启用 DNS64 功能后，需继续指定 DNS64 服务器。每条 IPv6 DNS 代理规则最多可以指定 6 个 DNS64 服务器。

选项	说明
	DNS64 前缀：指定 DNS64 前缀地址和前缀长度。DNS64 前缀用于将 A 记录（IPv4 地址）合成 AAAA 记录（IPv6 地址），合成的 IPv6 地址为“DNS64 前缀+IPv4 地址”形式。默认情况下，DNS64 前缀为“64:ff9b:: /96”。 在 DNS64 服务器列表下方，点击“新建”按钮，列表将新增一条表项，输入服务器的 IP 地址（IPv4 地址）及所属虚拟路由器参数即可。
描述	配置 DNS 代理规则的描述信息，如规则的作用。取值范围是 0 到 127 个字符。

3. 配置完成点击“确定”按钮。

启用/禁用规则

默认情况下，配置完成的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/禁用策略规则，请按照以下步骤进行操作：

1. 选择“网络 > DNS>DNS 代理”，进入 DNS 代理配置页面。
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。启用和禁用的规则可通过状态栏的状态按钮查看。

调整优先级

DNS 代理规则通过 ID 进行唯一标识。DNS 请求到达设备后，设备对 DNS 代理规则由上到下进行查找匹配，然后按照查找到的相匹配的第一条规则对 DNS 请求进行处理。但是，DNS 代理规则 ID 的大小顺序并不是规则的优先级。默认情况下，新创建的 DNS 代理规则会被放到所有规则的末尾，即优先级最低。用户可以修改 DNS 代理规则的排列顺序来调整其优先级。DNS 代理规则的排列位置可以是绝对位置，即处在首位（Top）或者处在末位（Bottom），也可以是相对位置，即位于某个 ID 之前或之后。

调整 DNS 代理规则的优先级，请按照以下步骤进行操作：

1. 选择“网络 > DNS>DNS 代理”，进入 DNS 代理配置页面。
2. 从 DNS 代理规则列表中选中需要调整优先级的规则对应的复选框，然后点击列表上方的“优先级”按钮。
3. 在打开的<调整优先级>页面中，选择需排列的位置：列表最前、列表最后、该 ID 之前、该 ID 之后。选择“该 ID 之前、该 ID 之后”时，需在文本框中输入 ID 号。设置完成后被选中的代理规则将被移动至指定规则之前或之后。

DNS 代理全局配置

DNS 代理全局配置，请按照以下步骤进行操作：

1. 选择“网络 > DNS>DNS 代理”，进入 DNS 代理配置页面。
2. 点击代理规则列表右上角的“DNS 代理全局配置”按钮，打开<DNS 代理全局配置>页面。

在<DNS 代理全局配置>页面内进行配置：

选项	说明
生存时间	启用 DNS 域名解析记录在 DNS 客户端上的保存功能，并设置解析记录的生存时间。如果超过生存时间，系统将清除 DNS 客户端上缓存的域名解析记录。取值范围是 30 到 600s。默认值是 60s。
服务器探测	启用 DNS 代理对服务器的探测功能并指定探测间隔。取值范围为 3 至 60s，默认值为 10s。DNS 代理解析探测功能即对 DNS 代理服务器的可达性进行检测。配置该功能后，系统将按照指定的探测间隔周期性地对 DNS 代理服务器进行探测，并且及时将不可达的服务器 IP 地址从 DNS 解析列表中删除，待链路恢复后再重新加入到轮询解析列表。默认情况下，DNS 服务器探测功能是开启的。
UDP 检验和	启用 DNS 代理的 UDP 报文校验和功能，默认情况下，该功能是开启的，即 UDP 报文头部经过更改后设备会重新计算 UDP 校验和。用户如果希望提高设备的性能，可以关闭 DNS 代理 UDP 报文校验和功能，设备将不再进行 UDP 校验和的计算。

3. 点击“确定”，完成配置。

DNS 代理命中分析

该功能能够对系统中 DNS 请求流量与 DNS 代理规则的匹配次数进行统计，即每当进入系统的 DNS 请求流量与某条 DNS 代理规则相匹配时，该规则的命中次数会自动加 1，并对每条 DNS 代理规则命中数与系统全局 DNS 请求数的比例进行统计，直观显示 DNS 代理规则在用户网络中的使用效率。

查看 DNS 代理规则统计信息，按照以下步骤进行操作：

1. 选择“网络 > DNS>DNS 代理”，进入 DNS 代理配置页面。
2. 点击代理规则列表右上角的“DNS 代理命中分析”按钮，打开<DNS 代理命中分析>页面。

在<DNS 代理命中分析>页面查看统计信息：

选项	说明
时间	在下拉菜单中选择统计 DNS 代理规则命中次数以及该命中次数在系统全局 DNS 请求数占比的统计周期，包括： 最近一小时：显示最近一小时的统计信息。

选项	说明
	最近一天：显示最近一天的统计信息。 最近一周：显示最近一周的统计信息。 最近一月：显示最近一月的统计信息。 所有时间：显示历史累计统计信息。
统计清零	点击该按钮，清除所有统计结果。
ID	显示 DNS 代理规则的 ID。
命中数	显示在指定时间范围内，某 DNS 代理规则的命中次数。
命中百分比	显示在指定时间范围内，某 DNS 代理规则命中数与系统全局 DNS 请求数的比例。

3. 点击“关闭”，关闭<DNS 代理命中分析>页面。

解析配置

配置 DNS 请求重试次数和 DNS 请求响应超时时间，请按照以下步骤进行操作：

1. 选择“网络 > DNS > 解析配置”，进入解析配置页面。
2. 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. 在“TTL”处指定 DNS 主动解析缓存（包括动态域名缓存和注册域名缓存）在设备上的保存时间，可以为 DNS 服务器返回值（默认值）或者自定义时间（取值范围为 60 至 600 秒）。如果 DNS 主动解析缓存超过指定的 TTL 值无响应，系统将清除设备上缓存的域名解析记录。
5. 配置完成点击“应用”按钮将配置应用到系统中。

DNS 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 等，定义的 DNS 主机。

为了方便管理，DNS 静态缓存支持群组功能，即用户将具有相同 IP 地址、虚拟路由的多个域名主机组成一个 DNS 静态缓存组。

添加静态 DNS 映射组到缓存，请按照以下步骤进行操作：

1. 选择“网络 > DNS>缓存”，进入缓存页面。
2. 点击“新建”按钮，打开<DNS 缓存配置>页面。

选项	说明
虚拟路由器	在下拉菜单选择 DNS 缓存组所属的虚拟路由器。
主机名称	指定对应 DNS 缓存组的主机名称，可以点击“新建”按钮添加、“删除”按钮删除对应主机名称。根据需要最多可以配置 128 个域名主机，且每个主机名称最长为 255 个字符。
IP	指定对应 DNS 缓存组的主机 IPv4 地址，可以点击“新建”按钮添加、“删除”按钮删除对应主机 IP。根据需要最多可以为主机指定 8 个 IP 地址，优先匹配先配置的 IP。

3. 点击“确定”按钮，完成配置。

注意:

仅支持对 DNS 静态缓存组的新建、编辑和删除操作，无法对动态缓存和系统注册缓存进行以上操作。

用户可以通过命令清除 DNS 动态缓存条目，或者等待生存时间清零后清除。

用户只能通过删除功能模块定义的主机清除系统注册缓存。

DNS 静态缓存优先级高于动态和注册缓存，即添加静态缓存会覆盖已存在的相同的动态或注册缓存。

NBT 缓存

系统支持 NetBIOS 名字解析功能。开启该功能后，系统将自动获取设备所管理网络的所有主机注册的 NetBIOS 主机名，并将其记录在设备缓存中，用于为设备其它功能模块提供 IP 地址到 NetBIOS 主机名的查询服务。

开启 NetBIOS 名字解析功能是 NAT 日志中主机名称显示的前提条件。

开启安全域的 NetBIOS 功能，新建或者编辑安全域时，点击“NBT 缓存”后的“启用”按钮。开启 NetBIOS 功能的安全域不能为连接 WAN 网的安全域。开启该功能后，NetBIOS 查询过程可能会持续一段时间，查询结果将添加到 NetBIOS 缓存表中。系统每隔一段时间会重新进行一次查询并更新查询结果。

> 注意: 只有开启了 NetBIOS 设置的 PC 才可以被查询到其主机名称。请参阅 PC 操作系统的详细说明来获得开启 NetBIOS 功能的方法。

清除 NBT 缓存，请按照以下步骤进行操作：

1. 选择“网络 > DNS>NBT 缓存”，进入 NBT 缓存配置页面。
2. 在“虚拟路由器”下拉菜单选择 VR，系统显示该 VR 中的 NBT 缓存信息。
3. 选中需要清除的 NBT 缓存表项，然后点击列表左上方的“删除”按钮。

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。

系统支持通过 DHCP 实现动态分配 IPv4 和 IPv6 地址。启用 IPv6 功能后，用户可以将设备的接口配置成 DHCP 客户端，并从 DHCP 服务器获取 IPv6 地址。

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 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。

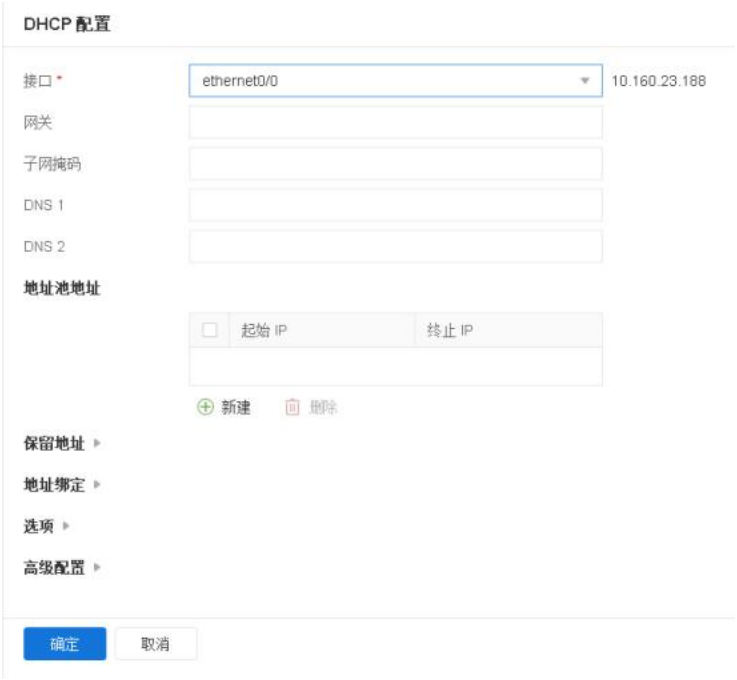
DHCP 中继代理：设备的接口可以设置成 DHCP 中继代理，中继代理从 DHCP 服务器获得 DHCP 信息，然后将获得信息传递到与接口相连的主机。

虽然设备同时具有以上三种 DHCP 功能，但是在为设备配置 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”，打开<DHCP 配置>页面。



3. 在该页面对 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。
子网掩码	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. 点击“新建”按钮，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。 重复以上步骤添加更多 IP 范围。 2. 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. 点击“保留地址”，展开保留地址配置项，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. 点击“地址绑定”，展开地址绑定配置项，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. **点击“选项”，展开选项配置项，对 DHCP 服务器支持的选项进行配置。**

选项	说明
43	Option 43 用于 DHCP 客户端与 DHCP 服务器交换特定的 VSI（Vendor Specific Information）。DHCP 服务器使用 Option 43 来下发 AC（Access Controller）地址，无线 AP（Access Point，即 DHCP 客户端）通过解析 Option43 字段获取 AC 地址来查找并连接 AC。 1. 点击“新建”按钮。 2. 在“选项”下拉菜单中，选择 **43**。 3. 在“格式”下拉菜单中选择使用 ASCII 格式或者 HEX 格式。ASCII 使用 ASCII 类型的 VCI。如果包含空格，需要用双引号包括此属性值。HEX 使用十六进制类型的 VSI。 4. 在“标识”文本框内，输入 VSI。 5. 点击“回车”或点击页面任意空白处，完成添加。 注意：如果系统已经配置了 VCI 验证字符串，那么首先需要验证客户端 Option 60 字段携带的 VCI。通过验证后，下发 IP 地址、Option 43 等相关信息；如果验证不通过，DHCP 服务器丢弃相关报文，不进行回复。
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. 点击“新建”按钮。 2. 在“选项”下拉菜单中，选择 **49**。 3. 在“成员”文本框中输入运行 X window System Display Manager 的系统的 IP 地址。 4. 点击“回车”或点击页面任意空白处，完成添加。 5. 重复以上步骤添加多条 IP 地址。如果需要删除 IP 地址，从

选项	说明
	列表中选中需要删除的 IP 地址，然后点击“删除”按钮。
60	Option 60 是由设备在形成 DHCP 报文时写入的，用以标识设备的类型或配置。设置 DHCP 服务器 Option 60 字段携带的 VCI 后，DHCP 服务器所发送的报文将携带此选项及 VCI。 1. 点击“新建”按钮。 2. 在“选项”下拉菜单中，选择 **60**。 3. 在“格式”下拉菜单中选择使用 ASCII 格式或者 HEX 格式。ASCII 使用 ASCII 类型的 VCI。如果包含空格，需要用双引号包括此属性值。HEX 使用十六进制类型的 VCI。 4. 在“标识”文本框内，输入 VCI。 5. 点击“回车”或点击页面任意空白处，完成添加。
66	Option 66 用来配置 TFTP 服务器名选项。通过配置 Option 66，DHCP 客户端可以获取 TFTP 服务器的域名或者 IP 地址。用户可以在该 TFTP 服务器中下载 Option67 中指定的启动文件。 1. 点击“新建”按钮。 2. 在“选项”下拉菜单中，选择 **66**。 3. 在“格式”下拉菜单中选择使用 ASCII 格式或者 HEX 格式。ASCII 使用 ASCII 类型的 TFTP 服务器的域名或者 IP 地址。名称长度可以是 1 到 255 个字符，但是在两个句点（.）之间，最多可以有 63 个字符。HEX 使用十六进制类型的 TFTP 服务器的域名或者 IP 地址。 4. 在“标识”文本框内，输入 TFTP 服务器的域名或者 IP 地址。 5. 点击“回车”或点击页面任意空白处，完成添加。
67	Option 67 用来配置 TFTP 服务器的启动文件名称选项。通过配置 Option67， DHCP 客户端可以获取启动文件名称。 1. 点击“新建”按钮。 2. 在“选项”下拉菜单中，选择 **67**。 3. 在“格式”下拉菜单中选择使用 ASCII 格式或者 HEX 格式。ASCII 使用 ASCII 类型的启动文件名。名称长度可以是 1 到

选项	说明
	255 个字符。 4. 在“标识”文本框内，输入启动文件名。 5. 点击“回车”或点击页面任意空白处，完成添加。
138	DHCP 服务器使用 Option 138 下发 CAPWAP AC (Access Control)的列表给 WTP（Wireless Terminal Point）。此列表包含一个或多个可用的 CAPWAP AC 的 IP 地址。WTP 通过获取 Option 138 字段中的 AC 地址来查找并连接 AC。 1. 点击“新建”按钮。 2. 在“选项”下拉菜单中，选择 **138**。 3. 在“成员”文本框中输入 AC 的 IP 地址 4. 点击“回车”或点击页面任意空白处，完成添加。用户可配置最多 4 个 AC。 若 DHCP 服务器端未设置 Option 138 或 DHCP 客户端未进行请求，DHCP 服务器端将不下发 Option 138 的信息。
150	Option 150 用来配置 TFTP 服务器的地址选项。通过配置 Option 150， DHCP 客户端可以获取 TFTP 服务器的地址。 1. 点击“新建”按钮。 2. 在“选项”下拉菜单中，选择 **150**。 3. 在“成员”文本框中输入 TFTP 服务器的 IP 地址 4. 点击“回车”或点击页面任意空白处，完成添加。用户可配置最多 8 个 TFTP 服务器。
242	Option 242 是 IP 电话专用的 DHCP 私有选项。通过配置 Option 242，DHCP 服务器和 DHCP 客户端之间可以交换 IP 电话相关的特定参数信息，如呼叫服务器地址（MCIPADD）、呼叫服务器端口（MCPORT）、TLS 服务器地址（TLSSRVR）、HTTP 服务器地址（HTTPSRVR）以及 HTTP 服务器端口（HTTPPORT）等。 1. 点击“新建”按钮。 2. 在“选项”下拉菜单中，选择 **242**。 3. 在“格式”下拉菜单中选择使用 ASCII 格式或者 HEX 格式。

选项	说明
	ASCII 使用 ASCII 类型的 IP 电话相关的特定参数。名称长度可以是 1 到 255 个字符。 4. 在“标识”文本框内，输入 IP 电话相关的特定参数。 5. 点击“回车”或点击页面任意空白处，完成添加。

7. **点击“高级配置”，展开高级配置项，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。域名长度可以是 1-255 个字符。
租约	指定租约时间，单位为秒，范围是 300 到 1048575 秒。默认是 3600 秒。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。
服务器	
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。	
IP/掩码	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。
VCI 验证字符串	用户可在 DHCP 服务器端验证客户端 DHCP 报文的 Option 60 字段携带的 VCI。当 DHCP 报文的 VCI 与 DHCP 服务器指定的 VCI 验

选项	说明
	证字符串相同时，DHCP 服务器下发 IP 地址等配置信息；不相同时，DHCP 服务器丢弃相关报文，不进行回复。当 DHCP 服务器不设置 VCI 验证字符串时，DHCP 服务器将忽略客户端 Option 60 的属性值。 1. 在下拉菜单中选择 ASCII 或 HEX。选择 ASCII 使用 ASCII 类型的 VCI 验证字符串。如果包含空格，需要用双引号包括此标示符。选择 HEX 使用十六进制类型的 VCI 验证字符串。 2. 在文本框中输入属性值。

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”，打开<DHCP 中继代理>页面。
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”按钮并返回 DHCP 列表。

注意: 为了保证客户端能正常获取到 IP 地址，必须配置从 DHCP 服务器到客户端方向的 DHCP 中继放通策略。

配置 DHCPv6 服务器

系统支持通过 DHCP 实现动态分配 IPv4 和 IPv6 地址。DHCPv6 服务器配置，即将设备作为 DHCP 服务器的 IPv6 配置。通过配置的地址池，向与该接口相连的主机分配 IPv6 地址。

配置 DHCPv6 服务器，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“DHCPv6 服务器”，打开<DHCPv6 配置>页面。

DHCPv6 服务器配置如下：

选项	说明
接口	配置开启 DHCPv6 服务器功能的接口，使该接口作为 DHCP 服务器为子网中 DHCP 客户端设备分配 IPv6 地址。
rapid-commit	点击“启用”按钮，启用 rapid-commit 功能。启用后，系统将与服务器进行快速交互以获取 IPv6 地址。仅当客户端的 rapid-commit 与服务器的 rapid-commit 功能都启用时，该功能生效。
优先权	指定 DHCP 服务器的优先级，取值范围为 0 至 255。数值越大，表示优先级越高。
DNS1	为 DHCP 客户端配置主 DNS 服务器。在文本框中输入主 DNS 服务器的 IPv6 地址。
DNS2	为 DHCP 客户端配置备 DNS 服务器。在文本框中输入备用 DNS 服务器的 IPv6 地址。
域名	指定 DHCP 服务器给客户端分配的域名。名称长度可以是 1-252 个字符。
地址池地址：配置 DHCP 服务器地址池。设备可作为 DHCP 服务器为子网中 DHCP 客户端设备分配 IPv6 地址，用户需要指定地址池的地址范围用来对外分配。	
IP	指定地址池的 IPv6 地址的通用前缀和前缀长度。
合法生命周期	指定 IPv6 地址的有效生存时间，即地址在该时间之前生效。
首选生命周期	指定 IPv6 地址的首选生存时间，该时间必须小于或者等于有效生存时间。

3. 点击“确定“完成配置。

配置 DHCPv6 中继代理

DHCP 中继代理支持 IPv6。配置 DHCPv6 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“DHCPv6 中继代理”，打开<DHCPv6 中继代理>页面。
3. 从“接口”下拉菜单选择应用 DHCPv6 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 IPv6 地址。
5. 若配置的 DHCP 服务器为本地链路地址，根据需要，在“出接口 1/出接口 2/出接口 3”文本框中选择对应的出接口名称。
6. 点击“确定”按钮并返回 DHCP 列表。

DDNS

DDNS 是动态域名服务（Dynamic Domain Name Server）的缩写，可以实现固定域名到动态 IP 地址之间的解析。通常情况下，用户每次连接因特网时都会从 ISP 得到一个动态 IP 地址，即用户每次连接因特网得到的 IP 地址都不同。动态域名解析功能可以将域名绑定到用户的动态 IP 地址，每次当用户连接到因特网时，它都会自动更新自己的动态 IP 与域名的绑定。

在使用 DDNS 功能之前，用户需要在 DDNS 服务的提供商那里进行注册，以获取动态域名。设备支持以下五个动态域名服务提供商，请访问相应的主页进行注册：

dyndns.org：http://dyndns.com/dns

3322.org：http://www.pubyun.com

no-ip.com：http://www.noip.com

Huagai.net：http://www.ddns.com.cn

ZoneEdit.com：http://www.zoneedit.com

配置 DDNS

配置 DDNS 功能，请按照以下步骤进行操作：

1. 选择“网络 > DDNS”，进入 DDNS 配置页面。

2. 点击“新建”按钮，打开<DDNS 配置>页面。

3. 在该页面，配置 DDNS 选项。

选项	说明
DDNS 名称	指定所需创建的 DDNS 服务名称。名称长度可以是 1-31 个字符。
接口	指定设备应用 DDNS 服务的接口。
主机名称	指定在相应 DDNS 提供商处申请得到的域名。名称长度可以是 1-127 个字符。
服务商配置	
服务商	指定 DDNS 服务器的提供商。从下拉菜单中选择需要的提供者。
服务器名称	指定所配置 DDNS 服务器相应的服务器名称。名称长度可以是 1-255 个字符。
服务器端口	指定所配置 DDNS 服务器相应的服务器端口号。范围是 1 到 65535，默认值为 80。
用户	
用户名	指定在 DDNS 服务提供商处注册的用户名称。名称长度可以是 1-49 个字符。

选项	说明
密码	指定与用户名称相对应的密码。密码长度可以是 1-31 个字符。
确认密码	再次输入密码进行确认。
修改密码	编辑 DDNS 配置时，可以看到修改密码功能。开启后，将展示密码输入框。如需修改，输入新的密码后保存配置即可。
更新间隔	
最小更新时间间隔	启用 DDNS 功能的接口的 IP 地址发生变化后，设备需要向 DDNS 服务器发送更新请求。如果发送的请求没有响应，设备会根据此处配置的最小更新间隔再次发送请求。例如，设置最小更新间隔为 5 分钟，当第一次失败后，设备会在 5 分钟后发出第二次请求，如果再次失败，将会在 10（5x2）分钟后再次发出请求，再次失败，则在 20（10x2）分钟后发出请求，以此类推，直到时间为 120 分钟后，不再增加时间，即以固定的每隔 120 分钟发出一次请求。在文本框中输入最小更新间隔时间，单位为分钟。默认值为 5 分钟。取值范围为 5 到 120 分钟。
最大更新时间间隔	最大更新间隔为在无 IP 地址变化的情况下，设备在多长时间后向 DDNS 服务器发出一次更新请求。在文本框中输入最大更新间隔时间，单位为小时。默认值为 24 小时。取值范围为 24 到 8760 小时。

4. 点击“确定”按钮，完成配置。

注意: 配置选项中的的“服务器名称”和“服务器端口”必须为 DDNS 服务器相对应的名称和端口号。如果不知道确切信息，请勿配置。与 DDNS 服务器连接成功后，服务器会自动将服务器名称和端口号信息一并返回。

PPPoE

PPPoE 是以太网上点对点协议（Point-to-Point Protocol over Ethernet）的缩写。PPPoE 结合 PPP 协议和以太网，在分配 IP 地址的同时，可以对客户端进行接入控制、验证以及计费等。

PPPoE 协议的实现包括两个阶段：发现阶段和 PPP 会话阶段。

发现阶段：在发现阶段，客户端确定一个 PPPoE 访问集中器（Access Concentrator），获得其以太网 MAC 地址并建立起一个 PPPoE 会话标识符 Session ID。

PPP 会话阶段：客户端与在发现阶段确定的访问集中器进行 PPP 协商。这个协商过程与标准的 PPP 协商相同。

设备的接口可以配置成 PPPoE 客户端，进行 PPPoE 连接。

配置 PPPoE

新建 PPPoE 实例，请按照以下步骤进行操作：

1. 选择“网络 > PPPoE”，进入 PPPoE 配置页面。
2. 点击“新建”按钮，打开<PPPoE 配置>页面。

3. 在此页面，配置 PPPoE 选项。

选项	说明
PPPoE 名称	指定 PPPoE 实例的名称。名称长度可以是 1-31 个字符。
接口	从下拉菜单选择以太网接口。
用户名	指定 PPPoE 用户名称。 名称长度可以是 1-31 个字符。
密码	指定 PPPoE 用户相应的密码。密码长度为 1-31 个字符。
确认密码	再次输入密码进行确认。
修改密码	编辑 PPPoE 配置时，可以看到修改密码功能。开启后，将展示密码

选项	说明
	输入框。如需修改，输入新的密码后保存配置即可。
挂断前空闲间隔	即自动连接方式，使用该方式，当 PPPoE 接口的空闲（无流量）时间到达一定的时间，即指定的空闲间隔，系统会断开与因特网的连接；当产生上网需求时，系统会自动连接到因特网。该选项指定空闲间隔时间，单位为分钟。范围是 0 到 10000 分钟，默认值为 0。
重拨间隔	使用该方式，当 PPPoE 连接由于某些原因断开，且断开时间到达一定的时间，即为用户指定的自动连接时间，系统会自动重拨。该选项指定自动连接的时间，单位为秒。范围是 0 到 10000 秒。默认值是 10 秒，表示关闭自动连接功能。
访问集中器	指定访问集中器的名称。名称长度为 1-31 个字符。
认证	设备与 PPPoE 服务器建立连接时，需要通过 PPPoE 认证。设备支持的验证方式有 CHAP、PAP 和任意（系统默认方式，表示 CHAP 或者 PAP 的任意一种）。该选项指定 PPPoE 认证方式。选中需要的认证方式的单选按钮。此处配置的认证方式必须与 PPPoE 服务器端的认证方式相同。
子网掩码	为 PPPoE 方式获得的 IP 地址指定网络掩码。
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。
服务	指定允许的服务。此处指定的服务必须与 PPPoE 服务器端提供的服务相同。如果不指定服务，设备自动接受服务器返回的任何服务。名称长度可以是 1-31 个字符。
静态 IP	用户可以指定一个静态的 IP 地址，并协商使用该静态 IP 地址。这样可以避免 IP 地址变化。该选项指定静态 IP 地址。在文本框中输入静态 IP 地址。

4. 点击“确定”，完成配置。

Virtual Wire

设备支持基于 VSwitch 的 Virtual Wire 功能。开启该功能并配置 Virtual Wire 接口对后，两个 Virtual Wire 接口对形成一条虚拟线路，将连接到设备 Virtual Wire 接口对的两个子网连接到一起，被连接的两个子网可以直接进行二层通信，不需要通过其它子网的转发。并且，使用 Virtual Wire 功能的同时，还可以使用策略规则等功能进行控制。

Virtual Wire 功能有两种模式，分别是 Strict 和 Non-Strict，具体描述如下：

Strict Virtual Wire 模式：在该模式下，设备不需要进行 MAC 地址学习，数据包只可以在 Virtual Wire 接口对之间传输，并且 VSwitch 不可以工作在混合模式下。连接到 Virtual Wire 接口的 PC 不可以通过该接口管理设备也不可以通过该接口访问 Internet。

Non-Strict Virtual Wire 模式：在该模式下，设备可以进行 MAC 地址学习，数据包除可以在 Virtual Wire 接口对之间传输外，VSwtich 还支持混合模式的数据转发，即该模式仅将二层数据包限制在 Virtual Wire 接口对之间传输，并不影响三层数据包的转发。

下表列出 Strict Virtual Wire 模式与 Non-Strict Virtual Wire 模式下数据包的传输情况。用户可以根据需要配置不同的 Virtual Wire 模式。

数据包	Strict	Non-strict
出接口和入接口分别为同一个 Vritual Wire 接口对的接口	允许	允许
入接口不是 Virtual Wire 接口	拒绝	拒绝
出接口和入接口分别为不同 Virtual Wire 接口对的接口	拒绝	拒绝
到设备本身的数据包的入接口为 Virtual Wire 接口	拒绝	允许
入接口为 Virtual Wire 接口，出接口为三层接口	拒绝	允许

配置 Virtual Wire

新建 Virtual Wire 配置，请按照以下步骤进行操作：

1. 选择“网络 > Virtual Wire”，进入 Virtual Wire 配置页面。
2. 点击“新建”按钮，打开<Virtual Wire 配置>页面。
3. 在“虚拟交换机”下拉菜单指定配置 Virtual Wire 的虚拟交换机名称。
4. 在“接口 1”下拉菜单指定 Virtual Wire 接口对的一个接口。同一个 Virtual Wire 接口对中的两个接口不可以相同，同一个接口不可以同时属于两个 Virtual Wire 接口对。
5. 在“接口 2”下拉菜单指定 Virtual Wire 接口对的一个接口。同一个 Virtual Wire 接口对中的两个接口不可以相同，同一个接口不可以同时属于两个 Virtual Wire 接口对。
6. 点击“确定”按钮，完成配置。

配置 Virtual Wire 模式

指定 Virtual Wire 模式，请按照以下步骤进行操作：

1. 选择“网络 > Virtual Wire”，进入 Virtual Wire 配置页面。
2. 点击“Virtual Wire 模式”，打开<Virtual Wire 模式配置>页面。
3. 在“虚拟交换机”下拉菜单指定配置 Virtual Wire 的虚拟交换机名称。

4. 指定 Virtual Wire 模式。

严格：在该模式下，数据包只可以在 Virtual Wire 接口对之间传输，并且 VSwitch 不可以工作在混合模式下。连接到 Virtual Wire 接口的 PC 不可以通过该接口管理设备也不可以通过该接口访问 Internet。

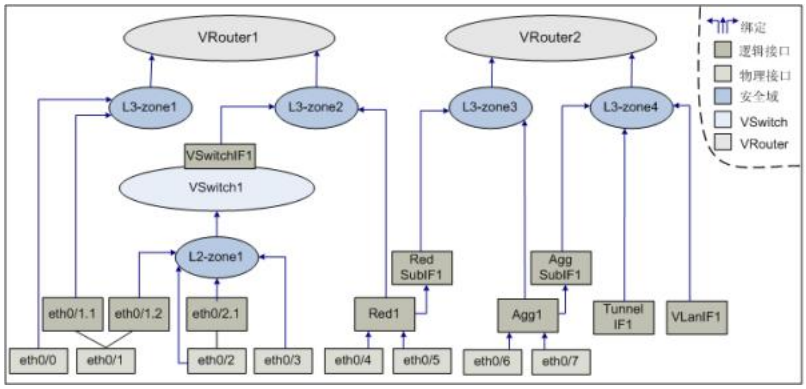
不严格：在该模式下，数据包除可以在 Virtual Wire 接口对之间传输外，VSwtich 还支持混合模式的数据转发，即该模式仅将二层数据包限制在 Virtual Wire 接口对之间传输，并不影响三层数据包的转发。

未启用：不开启 Virtual Wire 功能。

5. 点击“确定”按钮，完成配置。

虚拟路由器

虚拟路由器即 Virtual Router（VRouter），在系统中简称为 VR。VR 具有路由器功能，不同 VR 拥有各自独立的路由表。系统中有一个默认 VR，名为 trust-vr，默认情况下，所有三层安全域都将会自动绑定到 trust-vr 上。系统支持多 VR 功能且不同硬件平台支持的最大 VR 数不同。多 VR 将设备划分成多个虚拟路由器，每个虚拟路由器使用和维护各自完全独立的路由表，此时一台设备可以充当多台路由器使用。多 VR 使设备能够实现不同路由域的地址隔离与不同 VR 间的地址重叠，同时能够在一定程度上避免路由泄露，增加网络的路由安全。下图描述了接口、安全域、VSwitch 和 VRouter 之间的关系：



如上图所示，接口、安全域、VSwitch 和 VRouter 之间的绑定关系如下：

接口绑定到安全域。绑定到二层安全域的接口为二层接口，绑定到三层安全域的接口为三层接口。一个接口只能绑定到一个安全域。主接口与子接口可以分别属于不同的安全域。

安全域绑定到 VSwitch 或者 VRouter。二层安全域绑定到 VSwitch（预定义二层安全域默认绑定到系统缺省 VSwitch——VSwitch1），三层安全域绑定到 VRouter（预定义三层安全域默认绑定到系统缺省 VR——trust-vr）。由此，也实现了接口与 VSwitch 或者 VR 的绑定。一个安全域只能绑定到一个 VSwtich 或者 VR。

新建虚拟路由器

新建虚拟路由器，请按照以下步骤操作：

1. 选择“网络 > 虚拟路由器 > 虚拟路由”。
2. 点击“新建”按钮，打开<虚拟路由器配置>页面。
3. 在"虚拟路由"文本框输入虚拟路由器的名称。名称长度可以是 1-31 个字符。
4. 点击“确定”按钮，完成配置。

虚拟交换机

由于实际应用的需要，设备会让部分接口之间的数据包在二层转发域中做二层转发（称作透明应用模式），部分接口之间的数据包做三层转发（称作路由应用模式）。为了使用户能够灵活地配置这种二、三层混合应用模式，系统引入了虚拟交换机即 Virtual Switch（VSwitch）的概念。默认情况下，系统有一个 VSwitch，称作 VSwitch1。用户每新建一个 VSwitch，系统都会为 VSwitch 自动生成一个 VSwitch 接口（VSwitchIF）。通过把接口绑定到安全域，再把安全域绑定到 VSwitch，用户可以把接口绑定到 VSwitch。

一个 VSwitch 就是一个二层转发域，每个 VSwitch 都有自己独立的 MAC 地址表，因此 VSwitch 中的接口之间的数据包会被按照二层转发规则进行转发。在 VSwtich 中，用户可以方便地配置策略规则。VSwitch 接口相当于实际交换机的上连口，通过 VSwitch 接口，数据包可以实现二层与三层之间的转发。

新建虚拟交换机

新建虚拟交换机，请按照以下步骤进行操作：

1. 选择“网络 > 虚拟交换机”，进入虚拟交换机配置页面。
2. 点击“新建”按钮，打开<虚拟交换机配置>页面。

选项说明如下：

选项	说明
虚拟交换机名称	指定虚拟交换机名称。名称长度可以是 2-4094 个字符。
Vsys 共享	点击“启用”按钮，在不同 Vsys 中共享该虚拟交换机。
Virtual-Wire 模式	为虚拟交换机指定 Virtual-Wire 模式，包括以下几种： 严格：在该模式下，数据包只可以在 Virtual Wire 接口对之间传输，并且 VSwitch 不可以工作在混合模式下。连接到 Virtual Wire 接口的 PC 不可以通过该接口管理设备也不可以通过该接口访问 Internet。 不严格：在该模式下，数据包除可以在 Virtual Wire 接

选项	说明
	口对之间传输外，VSwtich 还支持混合模式的数据转发，即该模式仅将二层数据包限制在 Virtual Wire 接口对之间传输，并不影响三层数据包的转发。 未启用：不开启 Virtual-Wire 功能。
IGMP snooping	点击“启用”按钮，开启虚拟交换机的 IGMP snooping 功能。
转发标记包	点击“启用”按钮，开启 VLAN 透传功能使设备能够透传 VLAN 标记数据包，即带有 VLAN ID 的数据包在通过设备后仍保留原有 ID。
转发双标记包	点击“启用”按钮，开启 VLAN 透传功能使设备能够透传 VLAN 双标记数据包，即带有 VLAN ID 的数据包在通过设备后仍保留原有 ID。
丢弃未知多播包	点击“启用”按钮，丢弃发往未知组播组的报文，从而节省带宽。

3. 点击“确定”按钮，完成配置。

出站负载均衡

在出站方向，系统通过实时监控各链路的时延、抖动、丢包率和带宽利用率，实现智能选路、动态调整各链路的流量负载。用户可以配置灵活的 LLB 模板，并通过配置 LLB 规则将 LLB 模板绑定到路由上（目前系统仅支持目的路由和策略路由），以实现对出站链路流量的控制及负载均衡。

配置 LLB 模板

LLB 模板包含负载均衡算法中的各项参数供用户灵活配置，如带宽利用率阈值、探测开关、探测模式、均衡方向等。请按照以下步骤进行操作：

1. 选择“网络 > 出站负载均衡 > 模板”，进入模板列表界面。

2. 在页面左上角点击“新建 ”按钮，打开<LLB 模板配置>页面。

在该对话框中进行配置。

选项	说明
模板名称	配置 LLB 模板的名称，长度为 1-95 字符。
类型	配置 LLB 模板的类型，可指定为 IPv4 类型和 IPv6 类型，默认为 IPv4 类型。
带宽利用率	指定带宽利用率阈值。当接口的带宽利用率没有超过阈值时,系统将只分析链路的时延、抖动、丢包状况来动态调整选路的方法；当接口的带宽利用率超过阈值时，系统将同时分析各链路上“带宽利用率”这一参数来调整选路方法。Value 的取值范围为 0-100（0%-100%），默认为 60%。
均衡模式	均衡模式有两种：高性能和高兼容。 高性能 - 此模式下系统会根据链路实时的时延、抖动、丢包情况，迅速调整以最大限度的保持链路均衡。 高兼容 - 配置负载均衡模式为高兼容模式。当链路负载变动时，系统不会频繁地切换链路，而是优先保证业务尽量在先前链路上。此模式多适用于对链路切换比较敏感的业务，如银行业务。
描述	配置模板的详细信息。长度为 0-255 个字符。

3. 点击“确定”按钮将新模板添加到模板列表。

注意: 在编辑 LLB Profile 时不允许更改 IP 类型。

配置 LLB 规则

LLB 模板与路由绑定形成 LLB 规则，才能够真正生效，目前支持绑定有目的路由（DBR）和策略路由(PBR)。请按照以下步骤进行操作：

1. 选择“网络 > 出站负载均衡 > 规则”，进入规则列表界面。
2. 在页面左上角点击“新建 ”按钮，打开<LLB 策略配置>页面。

在该页面内进行配置。

选项	说明
规则名称	配置 LLB 规则的名称，长度为 1-95 字符。
类型	配置 LLB 规则的类型，可指定为 IPv4 类型和 IPv6 类型，默认为 IPv4 类型。
LLB 模板	选择需要绑定的模板。当 LLB 规则指定为 IPv4 类型时，只能绑定 IPv4 类型的模板。当 LLB 规则指定为 IPv6 类型时，只能绑定 IPv6 类型的模板。此项为必填项。
绑定路由	指定规则中需绑定的路由，包含以下选项： 目的路由 - 选择此选项时，需指定目的路由的虚拟路由器和目的地址。 策略路由 - 选择此选项时，需指定策略路由的名称和 id。需根据 LLB 规则配置的 IP 类型选择同类型的策略路由规则。
虚拟路由器	在下拉菜单中指定虚拟路由器的名称。默认为缺省 VR，即 trust-vr。
目的地址	指定虚拟路由器的目的地址。当 LLB 规则配置为 IPv6 类型时，使用 *X:X:X:X::X/M*方式指定 IPv6 目的地址。当 LLB 规则配置为 IPv4

选项	说明
	类型时，设备支持使用两种方式指定 IPv4 目的地址，*A.B.C.D/M* 或者 *A.B.C.D A.B.C.D*，例如 1.1.1.0/24 或者 1.1.1.0 255.255.255.0。
绑定域名簿	绑定目的路由时，需要选择绑定的域名簿。

3. 点击“确定”按钮将新规则添加到规则列表。

入站负载均衡

对入站流量启用负载均衡功能后，系统可以根据 DNS 请求的来源将域名解析成不同的 IP 地址，并将不同的 ISP 所对应的 IP 地址返回给相应的请求用户，从而达到减少跨 ISP 访问的目的。这种解析方式被称为智能域名解析（SmartDNS）。

用户可通过以下步骤启用入站负载均衡功能：

1. 启用 SmartDNS。启用该功能是实现入站负载均衡的前提条件。默认情况下，SmartDNS 功能为启用状态。
2. 配置 SmartDNS 规则表。系统根据 SmartDNS 规则表的匹配规则对源自不同链路的 DNS 请求返回不同的 IP 地址。

新建 SmartDNS 规则表

新建 SmartDNS 规则表，请按照以下步骤进行操作：

1. 选择“网络 > 入站负载均衡”，进入入站负载均衡页面。
2. 在页面左上角点击“新建 ”按钮，打开<新建 SmartDNS 规则>页面。

3. 在“名称”文本框中指定域名表的名称。名称长度可以是 1-31 个字符。
4. 点击“域名”下的“新建”按钮，指定需要被智能解析的域名。重复以上步骤添加更多域名。每个规则表最多支持 64 个不同的域名（不区分大小写）。
5. **点击“SmartDNS 规则”下的“新建”按钮，进行相关配置。**

选项	说明

选项	说明
ISP 静态地址簿	指定请求源地址需要匹配的 ISP 名称。当请求源地址匹配该 ISP 中的地址条目，系统返回指定的 IP 地址。 从下拉框选择系统中预定义或用户自定义的 ISP 名称。
返回地址	指定返回的 IP 地址。用户可以为一个域名最多配置 64 个 IP 地址。
权重	指定返回 IP 地址的权重。 取值范围是 1 到 100，默认值为 1。SmartDNS 规则表中一个域名可能对应多个 IP 地址，系统会根据权重值对 IP 地址进行排序后返回给用户。
入站接口	为返回 IP 地址指定 ISP 链路的入站接口。系统将根据入站接口的监测结果或入站接口协议状态来判断返回 IP 地址是否有效，系统只返回有效的 IP 地址给请求源。 从下拉框选择 ISP 链路的入站接口。
监测对象	为 ISP 链路的入站接口指定监测对象。当入站接口上配置了监测对象，若监测成功，则返回 IP 地址有效；否则 IP 地址无效。当入站接口没有配置监测对象，若该接口的协议状态为 UP，则返回 IP 地址有效；否则 IP 地址无效。若用户不配置入站接口，返回 IP 地址始终有效。 从下拉框选择 ISP 链路的入站接口的监测对象。如果监测对象状态为失败，则该返回 IP 地址失效。

6. 点击“确定”按钮将 SmartDNS 规则添加到规则列表。

> 注意：用户无法删除正在被 SmartDNS 规则表引用的 ISP 路由。

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。

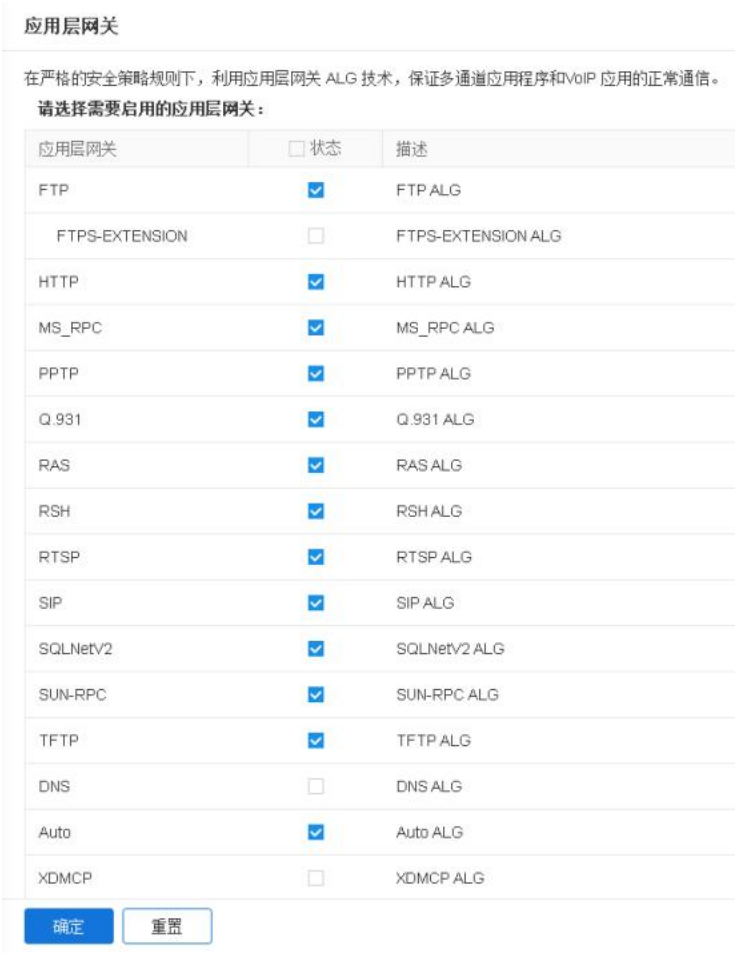
保证 VoIP 应用，在 NAT 模式下的正常工作，并能够根据安全策略要求，进行监控和过滤。

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、MSRPC、PPTP、Q.931、RAS、RSH、RTSP、SIP、SQLNetV2、SUNRPC、TFTP、DNS、Auto 和 XDMCP。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。取值范围为 60-1800 秒。
4. 点击“确定”完成配置。

注意: 在 FTP ALG 开启的情况下，支持开启显示 FTPS 的 ALG 功能。

全局网络参数

全局网络参数是对整个系统的数据流的设定，所有流经系统的数据包（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

配置全局网络参数，请按照以下步骤进行操作：

1. 点击“网络 > 全局网络参数 > 全局网络参数”，进入全局网络参数的主窗口。
2. **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 60 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 MSS VPN	为 IPsec VPN 的 TCP SYN 包指定最大数据分段值。
MSS 最大值	设定 IPSEC VPN 的 TCP 包的最大数据分段值，范围是 64 到 65535，默认 MSS 值为 1380。
TCP 包序列号检查	点击“启用”按钮，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 TCP 三次握手的检查功能。点击“启用”按钮开启该功能，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

IP 分片	
	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>复选框开启该功能并指定对 TCP 非 SYN 包的处理动作。在建立 TCP 连接时，设备将对收到的数据包进行检查。当收到的包为 TCP SYN 包时，建立 TCP 连接。当收到的包为 TCP 非 SYN 包时，按照指定动作对数据包进行处理。 丢弃：当收到的包为 TCP 非 SYN 包时，丢弃数据包。 发送 RST：当收到的包为 TCP 非 SYN 包时，丢弃数据包并向对方设备发送 RST 报文。
DHCP	
DHCP 中继报文源 IP 使用中继接口 IP	点击启用按钮开启该功能。开启后，当设备作为 DHCP 中继代理时，DHCP 中继报文的源 IP 将使用中继接口的 IP 报文源端口变为 67，主要用于某些严格安全策略的配置场景。默认情况下，该功能为关闭状态，关闭时 DHCP 中继报文的源 IP 为出接口的 IP，报文源端口为 68。
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。
Jumbo Frame	开启/关闭巨帧报文（Jumbo Frame）转发功能。该功能默认为关闭状态。 开启该功能后，对小于等于 9216 字节的报文，系统可以进行如下转发处理： 对于小于出接口 MTU 值的 IPv4/IPv6 报文，直接转发； 对于大于出接口 MTU 值的 IPv4 报文，分片转发； 对于大于出接口 MTU 值的 IPv6 报文，向发送报文的源节点发送“ICMPv6 Packet Too Big”错误信息，并促使发送端缩短报文的长度。 **注意：** 开启巨帧报文转发功能后，接口的 MTU 值配置范围会发生改变。

3. 点击“确定”。

配置防护模式

配置防护模式，请按照以下步骤进行操作：

1. 点击“网络 > 全局网络参数 > 防护模式”。
2. 选择系统中所有流量的统一处理模式。在默认模式下，“记录日志”功能和“防护”功能均被启用，设备的所有功能正常工作；若只启用“记录日志”功能，则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，请务必同时启用“记录日志”功能和“防护”功能，在该模式下，设备的安全功能正常生效；若只启用“记录日志”功能，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、QoS 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，同时系统支持多 VRouter（多 VR）功能。

设备支持目的路由、ISP 路由、源路由（Source-Based Routing，简称 SBR）、源接口路由（Source-Interface-Based Routing，简称 SIBR）、目的接口路由（Destination-Interface-Based Routing，简称 DIBR）、策略路由（Policy-Based Routing，简称 PBR）、动态路由（包括 RIP、OSPF 和 BGP）和等价多径路由（Equal Cost MultiPath Routing，简称 ECMP）。

目的路由：手工定义的路由条目，根据目的地址指定下一跳。

目的接口路由：根据数据包的目的 IP 地址和入接口，选择路由，进行转发。

源路由：根据数据包的源 IP 地址，选择路由，进行转发。

源接口路由（SIBR）：根据数据包的源 IP 地址和入接口，选择路由，进行转发。

ISP 信息：添加 ISP 相关信息。

ISP 路由：根据不同的 ISP 确定下一跳。

策略路由（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。

动态路由：设备按照动态路由协议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 > 目的接口路由 > 目的路由/ISP 路由/动态路由。

路由功能支持 IPv4 和 IPv6 地址。如接口开启了 IPv6 功能，用户可根据需要配置 IPv6 地址的路由条目。

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. 选择<IPv4>或<IPv6>标签页，在对应页面新建 IPv4 目的路由或 IPv6 目的路由。该步骤仅适用于 IPv6 版本。
3. **点击“新建”按钮，打开<目的路由配置>页面。**

选项	说明
所属虚拟路由器	从下拉菜单选择一个虚拟路由器，新建的路由将属于该虚拟路由器，默认为“trust-vr”。
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”、“当前系统虚拟路由器”、“接口”或“其他系统虚拟路由器”选项。 网关：在“网关”文本框中输入网关 IP 地址。 当前系统虚拟路由器：在“虚拟路由器”下拉菜单选择虚拟路由器名称。 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。 其他系统虚拟路由器：在“虚拟系统”下拉菜单选择虚拟系统名称。在“虚拟路由器”下拉菜单选择虚拟路由器名称。
时间表	指定时间表名称。在“时间表”下拉菜单中选择需要的时间表。该条路由将会在时间表指定的时间范围内生效。
监测对象	从下拉菜单中选择一个已创建的监测对象。选择后，若针对该监测对象的监测失败，则该路由无效。
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。
Tag 值	指定目的路由的标记值。在 OSPF 引入路由时，如果此处配置的路由标记值匹配到路由映射表中的规则，那么将会引入该路由，从而实现对引入路由信息的过滤。取值范围是 1 到 4294967295。
描述	输入所需的目的路由描述信息。长度为 1-63 个字符。

4. 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。

配置目的接口路由

目的接口路由根据数据包的目的 IP 地址和入接口，选择路由，进行转发。

新建目的接口路由

新建目的接口路由，请按照以下步骤进行操作：

1. 选择“网络 > 路由 > 目的接口路由”。
2. 选择<IPv4>或<IPv6>标签页，在对应页面新建 IPv4 目的接口路由或 IPv6 目的接口路由。该步骤仅适用于 IPv6 版本。
3. **点击“新建”按钮，打开<目的接口路由配置>页面。**

选项	说明
所属虚拟路由器	从下拉菜单选择一个虚拟路由器，新建的路由将属于该虚拟路由器，默认为“trust-vr”。
入接口	从下拉菜单中选择目的接口路由条目的入接口。
目的 IP	在文本框中输入目的接口路由条目的目的 IP 地址。
子网掩码	在文本框中输入目的接口路由条目的目的 IP 对应的子网掩码。
下一跳	指定下一跳类型，选择“网关”、“当前系统虚拟路由器”、“接口”或“其他系统虚拟路由器”选项。 网关：在“网关”文本框中输入网关 IP 地址。 当前系统虚拟路由器：在“虚拟路由器”下拉菜单选择虚拟路由器名称。 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。

选项	说明
	其他系统虚拟路由器：在“虚拟系统”下拉菜单选择虚拟系统名称。在“虚拟路由器”下拉菜单选择虚拟路由器名称。
时间表	指定时间表名称。在“时间表”下拉菜单中选择需要的时间表。该条路由将会在时间表指定的时间范围内生效。
监测对象	从下拉菜单中选择一个已创建的监测对象。选择后，若针对该监测对象的监测失败，则该路由无效。
优先权	在文本框中指定目的接口路由的优先级。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接口路由的路由权值。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	输入所需的目的接口路由描述信息。长度为 1-63 个字符。

4. 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接口路由列表中。

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. 选择<IPv4>或<IPv6>标签页，在对应页面新建 IPv4 源路由或 IPv6 源路由。该步骤仅适用于 IPv6 版本。
3. **点击“新建”按钮，打开<源路由配置>页面。**

选项	说明
所属虚拟路由器	从下拉菜单选择一个虚拟路由器，新建的路由将属于该虚拟路由器，默认为“trust-vr”。
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”、“当前系统虚拟路由器”、“接口”或“其他系统虚拟路由器”选项。 网关：在“网关”文本框中输入网关 IP 地址。 当前系统虚拟路由器：在“虚拟路由器”下拉菜单选择虚拟路由器名称。 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。 其他系统虚拟路由器：在“虚拟系统”下拉菜单选择虚拟系统名称。在“虚拟路由器”下拉菜单选择虚拟路由器名称。
时间表	指定时间表名称。在“时间表”下拉菜单中选择需要的时间表。该条路由将会在时间表指定的时间范围内生效。
监测对象	从下拉菜单中选择一个已创建的监测对象。选择后，若针对该监测对象的监测失败，则该路由无效。
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

选项	说明
	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。长度为 1-63 个字符。

4. 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. 选择<IPv4>或<IPv6>标签页，在对应页面新建 IPv4 源接口路由或 IPv6 源接口路由。该步骤仅适用于 IPv6 版本。
3. **点击“新建”按钮，打开<源接口路由配置>页面。**

选项	说明
所属虚拟路由器	从下拉菜单选择一个虚拟路由器，新建的路由将属于该虚拟路由器，默认为“trust-vr”。
入接口	从下拉菜单中选择源接口路由条目的入接口。

选项	说明
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”、“当前系统虚拟路由器”、“接口”或“其他系统虚拟路由器”选项。 网关：在“网关”文本框中输入网关 IP 地址。 当前系统虚拟路由器：在“虚拟路由器”下拉菜单选择虚拟路由器名称。 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。 其他系统虚拟路由器：在“虚拟系统”下拉菜单选择虚拟系统名称。在“虚拟路由器”下拉菜单选择虚拟路由器名称。
时间表	指定时间表名称。在“时间表”下拉菜单中选择需要的时间表。该条路由将会在时间表指定的时间范围内生效。
监测对象	从下拉菜单中选择一个已创建的监测对象。选择后，若针对该监测对象的监测失败，则该路由无效。
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。长度为 0-63 个字符。

4. 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 ISP 信息

配置 ISP 路由，用户首先需要将子网条目添加到一个 ISP，然后才可以配置以 ISP 名称为目的地的 ISP 路由。用户可以自定义 ISP 信息，也可以上传和下载 ISP 包含不同 ISP 信息的自定义配置文件。同时系统提供预定义 IPv4 ISP 配置文件包含四个 ISP，分别是中国电信（China-telecom）、中国联通（China-netcom）、中国移动（China-mobile）和教育网（CERNET）；预定义 IPv6 ISP 配置文件包含四个 ISP，分别是中国电信（China-telecom-v6）、中国联通（China-netcom-v6）、中国移动（China-mobile-v6）和教育网（CERNET-v6）。预定义 ISP 配置文件可通过 ISP 信息库实现远程或本地升级。

新建 ISP 信息配置文件

新建 ISP 信息配置文件，请按照以下步骤进行操作：

1. 选择“网络 > 路由 > ISP 信息”。
2. 选择“IPv4”或“IPv6”标签页，仅当该版本为 IPv6 版本时可配。
3. **点击“新建”按钮，打开<ISP 配置>页面。**

选项	说明
ISP 名称	在文本框中输入新建的 ISP 信息配置文件的名称。名称长度为 1-31 个字符。
ISP 子网列表	
成员	指定 ISP 信息成员类型，包括子网成员条目和 ISP 信息条目。 当创建“IPv4”类型 的 ISP 信息时： 添加子网条目：在下拉菜单中选择“IP/掩码”，然后在右侧的文本框中输入子网的 IPv4 地址和子网掩码。 添加 IPv4 ISP 信息条目：添加其他已配置的 IPv4 ISP 信息（预定义 IPv4 ISP 信息或自定义 IPv4 ISP 信息），在下拉菜单中选择“ISP 信息”然后在右侧的下拉菜单中选择指定 IPv4 ISP 名称。 当创建“IPv6”类型 的 ISP 信息时： 添加子网条目：在下拉菜单中选择“IPv6/前缀长度”，然后在右侧的文本框中输入子网的 IPv6 地址和前缀长度。 添加 IPv6 ISP 信息条目：添加其他已配置的 IPv6 ISP 信息（预定义 IPv6 ISP 信息或自定义 IPv6 ISP 信息），在下拉菜单中选择“ISP 信息”然后在右侧的下拉菜单中选择指定 IPv6 ISP 名称。

选项	说明
新建	点击此按钮添加新的 ISP 信息成员条目，并且显示在页面下方的列表中。重复以上步骤添加更多 ISP 成员条目。
删除	如果需要删除 ISP 信息成员条目，从列表中选中需要删除的 ISP 信息成员条目，然后点击右侧的“删除”按钮。

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

上传自定义 ISP 信息配置文件

上传 ISP 信息配置文件，请按照以下步骤进行操作：

1. 选择“网络 > 路由 > ISP 信息”。
2. 选择“IPv4”或“IPv6”标签页，仅当该版本为 IPv6 版本时可配。
3. 点击“上传”按钮，弹出<上传自定义 ISP 配置文件>对话框。

4. 点击“浏览”按钮，弹出<打开>对话框，用户在<打开>对话框中找到本地保存的自定义 ISP 配置文件。
5. 点击“上传”按钮上传所选择的自定义 ISP 配置文件至设备。

下载自定义 ISP 信息配置文件

下载用户自定义的 ISP 信息配置文件到本地，请按照以下步骤进行操作：

1. 选择“网络 > 路由 > ISP 信息”。
2. 选择“IPv4”或“IPv6”标签页，仅当该版本为 IPv6 版本时可配。
3. 点击“下载”按钮，打开<下载自定义 ISP 配置文件>页面。
4. 在“ISP 名称”下拉菜单中选择需要保存的 ISP 的名称。
5. 点击“确定”按钮，保存相应的 ISP 配置文件到电脑的指定位置。

删除自定义 ISP 信息配置文件

删除自定义 ISP 信息配置文件，请按照以下步骤进行操作：

1. 选择“网络 > 路由 > ISP 信息”。
2. 选择“IPv4”或“IPv6”标签页，仅当该版本为 IPv6 版本时可配。

3. 勾选列表中需要删除的 ISP 配置文件条目，点击“删除”按钮。

配置 ISP 路由

很多用户通常会申请多条线路进行流量负载均衡。然而，一般的均衡是不会根据流量的流向做均衡的，如果网通的服务器通过电信访问，网速就会很慢。设备针对该问题，提供 ISP 路由功能，使不同 ISP 流量走专有路由，从而提高网络访问速度。

配置 ISP 路由，用户首先需要将子网条目添加到一个 ISP，然后才可以配置以 ISP 名称为目的地的 ISP 路由。用户可以自定义 ISP 信息，也可以上传和下载 ISP 包含不同 ISP 信息的自定义配置文件。同时系统提供预定义 IPv4 ISP 配置文件包含四个 ISP，分别是中国电信（China-telecom）、中国联通（China-netcom）、中国移动（China-mobile）和教育网（CERNET）；预定义 IPv6 ISP 配置文件包含四个 ISP，分别是中国电信（China-telecom-v6）、中国联通（China-netcom-v6）、中国移动（China-mobile-v6）和教育网（CERNET-v6）。预定义 ISP 配置文件可通过 ISP 信息库实现远程或本地升级。

新建 ISP 路由

新建 ISP 路由，请按照以下步骤进行操作：

1. 选择“网络 > 路由 > ISP 路由”。
2. 选择“IPv4”或“IPv6”标签页，仅当该版本为 IPv6 版本时可配。
3. **点击“新建”按钮，打开<ISP 路由配置>页面。**

选项	说明

选项	说明
ISP 名称	从下拉菜单中选择已创建的 ISP 信息配置文件的名称。
所属虚拟路由器	从下拉菜单选择一个虚拟路由器，新建的策略路由将属于该虚拟路由器，默认为“trust-vr”。
下一跳	指定下一跳类型，选择“网关”、“当前系统虚拟路由器”、“接口”或“其他系统虚拟路由器”选项。 网关：在“网关”文本框中输入网关 IP 地址。 当前系统虚拟路由器：在“虚拟路由器”下拉菜单选择虚拟路由器名称。 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。 其他系统虚拟路由器：在“虚拟系统”下拉菜单选择虚拟系统名称。在“虚拟路由器”下拉菜单选择虚拟路由器名称。
时间表	指定时间表名称。在“时间表”下拉菜单中选择需要的时间表。该条路由将会在时间表指定的时间范围内生效。
优先权	在文本框中指定 ISP 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 10。当优先级为 255 时，该路由无效。
路由权值	在文本框中指定 ISP 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 ISP 路由描述信息。长度为 0-63 个字符。

4. 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 ISP 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，打开<策略路由绑定>页面。**

选项	说明
策略路由名称	在文本框中输入策略路由的名称。长度为 1-31 个字符。
所属虚拟路由器	从下拉菜单选择一个虚拟路由器，新建的策略路由将属于该虚拟路由器，默认为“trust-vr”。
类型	指定绑定该策略路由的类型，选择“安全域”、“虚拟路由器”、“接口”或者“无绑定”选项。 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。 虚拟路由器：选中“虚拟路由器”选项，在“绑定到”右侧显示绑定该策略路由的虚拟路由器名称，即为该策略路由所属的虚拟路由器。 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，点击“确定”。 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，打开<策略路由配置>页面。

在<策略路由配置>页面，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。长度为 0-255 个字符。
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”按钮将所选择的地址添加到左侧列表中。

选项	说明
	4. 添加完成后，点击“关闭”。 用户还可执行如下操作： 选择地址簿类型时，可点击 ⊕ 按钮创建新的地址簿。 选择地址簿类型时，点击搜索框中的 ▼ 按钮，可以按地址簿名称和地址成员的 IP 进行模糊搜索，名称和地址是与的关系。地址支持多种输入方式，例如：输入“地址”为 10.10.10.10/32，可能匹配到包含地址成员是 10.10.10.10/24 的地址簿；输入“地址”为段掩码 9.9.9.9/24，可能匹配到包含地址成员是 9.9.0.0/16 的地址簿；输入“地址”为 10.10.10.10，可能匹配到地址成员的 IP 范围为 10.10.10.0-10.10.10.255 的地址簿；输入“地址”为 10.23，可能匹配到包含地址成员是 1.10.23.10/24 的地址簿；输入“地址”为 aa，可能匹配到地址成员的“主机名称”为 aaa 的地址簿。 系统默认地址配置为 any。如需恢复为 any，选择 **any** 复选框。
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，选择用户或用户组所在的 AAA 服务器。如需指定角色，则在“AAA 服务器”下拉菜单中选择 **Role**。 2. 根据 AAA 服务器类型不同，用户可执行以下一个或多个操作：搜索指定用户/用户组/角色、展开用户/用户组列表、输入指定用户/用户组。 3. 选择指定用户/用户组/角色后，点击所选择的用户/用户组/角色将其添加到左侧列表中。 4. 添加完成后，点击“关闭”。
目的	
地址	指定策略路由规则的目的地址。 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 “添加按钮”将所选择的地址添加到左侧列表中。 4. 添加完成后，点击“关闭”。

选项	说明
	用户还可执行如下操作： 选择地址簿类型时，可点击 ⊕ 按钮创建新的地址簿。 选择地址簿类型时，点击搜索框中的 ▼ 按钮，可以按地址簿名称和地址成员的 IP 进行模糊搜索，名称和地址是与的关系。地址支持多种输入方式，例如：输入“地址”为 10.10.10.10/32，可能匹配到包含地址成员是 10.10.10.10/24 的地址簿；输入“地址”为段掩码 9.9.9.9/24，可能匹配到包含地址成员是 9.9.0.0/16 的地址簿；输入“地址”为 10.10.10.10，可能匹配到地址成员的 IP 范围为 10.10.10.0-10.10.10.255 的地址簿；输入“地址”为 10.23，可能匹配到包含地址成员是 1.10.23.10/24 的地址簿；输入“地址”为 aa，可能匹配到地址成员的“主机名称”为 aaa 的地址簿。 系统默认地址配置为 any。如需恢复为 any，选择 **any** 复选框。
其他信息	
服务	指定策略路由规则的服务/服务组。 1. 在“服务”下拉菜单中选择类型：服务，服务组。 2. 用户可搜索指定服务/服务组，展开服务/服务组列表。 3. 选择指定服务/服务组后，点击所选择的对象将其添加到左侧列表中。 4. 添加完成后，点击“关闭”。 用户还可执行如下操作： 如需添加新的服务/服务组，可在“预定义”下拉菜单中选择“自定义”，然后点击 ⊕ 按钮。 系统默认服务配置为 any。如需恢复为 any，选择 **any** 复选框。
应用	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，点击所选择的对象将其添加到左侧列表中。

选项	说明
	3. 添加完成后，点击“关闭”。 如需新建应用组或应用过滤组，点击 ⊕ 按钮即可新建。
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。选择完成后，点击对话框空白区域，即可完成时间表的选择。如需新建时间表，点击 ⊕ 按钮即可新建。

点击“下一跳”，展开下一跳配置项，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”、“当前系统虚拟路由器”、“接口”或“其他系统虚拟路由器”选项。 IP 地址：选择指定“IP 地址”类型的下一跳，并在“IP 地址”文本框中输入 IP 地址。 当前系统虚拟路由器：选择指定“当前系统虚拟路由器”类型的下一跳，并在“虚拟路由器”下拉菜单中选择虚拟路由器。 接口：选择指定“接口”类型的下一跳，并在“接口”下拉菜单中选择出接口。 其他系统虚拟路由器：选择指定“其他系统虚拟路由器”类型的下一跳，在“虚拟系统”下拉菜单中选择虚拟系统，在“虚拟路由器”下拉菜单中选择虚拟路由器。
监测对象	从下拉框中指定监测对象或点击 ⊕ 新建监测对象。
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。取值范围为 1-255。
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，打开<调整优先级>页面。**

选项	说明
移到首位	选中该选项，将策略路由规则移动到所有规则的顶部。
移到末尾	选中该选项，将策略路由规则移动到所有规则的底部。
该 ID 之前	选中该选项，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	选中该选项，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、虚拟路由器或者安全域来实现 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，打开<策略路由绑定>页面。**

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。
所属虚拟路由器	指定该策略路由所属的虚拟路由器。
类型	指定绑定该策略路由的类型，选择“安全域”、“虚拟路由器”、“接口”或者“无绑定”。 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。 虚拟路由器：在“绑定到”右侧显示绑定该策略路由的虚拟路由器名称，即为该策略路由所属的虚拟路由器。 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，请参阅设置 DNS 域名服务器一节。目前，DNS 重定向主要应用于视频引流。通过和 PBR 策略结合，系统可将 Web 视频网站的流量引流到指定的链路上，进而提升用户访问视频的体验。

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。

设置全局匹配顺序

如果用户绑定了 PBR 策略到接口、虚拟路由器或者安全域，默认情况下，流量的匹配顺序为：接口->安全域->虚拟路由器。用户可以根据需要自行设置 PBR 策略的全局匹配顺序。

设置全局匹配顺序，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“设置全局匹配顺序”按钮，打开<设置全局匹配顺序>页面。

3. 选中需要调整顺序的条目，点击或者调整顺序。
4. 如果需要恢复系统的默认配置，点击“恢复缺省”按钮。
5. 点击“确定”按钮保存所做配置。

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”，进入<RIP 配置>页面。

2. 从“虚拟路由器”下拉菜单选择一个 VR，新建的路由将属于该 VR。

点击“配置”，在<配置>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。
网络	
网络(IP/掩码)	在文本框中输入网络的 IP 地址和掩码。
新建	点击“新建”按钮，添加已配置的网络，被新添加的网络将显示在上方的列表中。重复以上步骤添加更多网络。
删除	如果需要删除网络，从列表中选中需要删除的网络，然后点击下方的“删除”按钮。

点击“高级配置”，展开高级配置项，对 RIP 进行高级配置。

选项	说明
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“启用”按钮，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。
引入路由	
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、静态、OSPF、IS-IS 或 BGP。
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。
新建	点击“新建”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上方的再发布路由列表中。重复以上步骤添加更多引入路由条目。
删除	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，然后点击下方的“删除”按钮。
邻居	
邻居 IP	在文本框中输入邻居的 IP 地址。
新建	点击“新建”按钮，添加已配置的邻居 IP，被添加的邻居 IP 将显示

选项	说明
	在上方的列表中。重复以上步骤添加更多邻居。
删除	如果需要删除邻居 IP，从列表中选中需要删除的邻居 IP，然后点击下方的“删除”按钮。
距离	
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。
新建	点击“新建”按钮，添加已配置的网络距离，被添加的网络距离将显示在上方的列表中。重复以上步骤添加更多网络距离。
删除	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，然后点击下方的“删除”按钮。

点击“数据库”，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。

点击页面右上角的“接口配置”，打开<接口>页面，对 RIP 进行被动接口配置。

选项	说明
编辑	勾选所需接口前的复选框，点击“编辑”，打开<接口配置>页面，对该接口进行详细配置。

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 OSPF

OSPF 是开放式最短路径优先协议（Open Shortest Path First）的缩写。它是 IETF 组织开发的一个基于链路状态的内部网关协议。当前的 OSPF 版本为版本 2（RFC2328）。OSPF 适应各种规模的网络，快速收敛特性能够在网络拓扑结构发生变化后立即发送更新报文，并且其算法本身决定了不会生成路由环路。OSPF 还具有以下特性：

• 区域划分：将自治系统的网络划分成区域来管理，从而减少了协议对 CPU 和内存的占用，提高性能。

• 无类路由：无类路由特性允许可变长子网掩码的使用。

• 等价路由：支持等价路由，提高多条路由的利用率。

• 组播发送：支持组播地址发送，减少对非 OSPF 设备的影响。

• 支持验证：支持基于接口的报文验证以保证路由计算的安全性。

说明：“自治系统”是处于一个管理机构控制之下的路由器和网络群组。一个自治系统中的所有路由器必须运行相同的路由协议。

新建 OSPF

新建 OSPF 进程，请按照以下步骤进行操作：

1. 选择“网络 > 路由 > OSPF”。
2. 从“虚拟路由器”下拉菜单选择一个 VR，新建的路由将属于该 VR。
3. 点击“新建”按钮，打开<OSPF 配置>页面。

在<OSPF 配置>页面，对 OSPF 进行基本配置。

选项	说明
进程 ID	输入 OSPF 的进程 ID。默认值是 1，取值范围是 1 到 65535。每个 OSPF 进程相互独立，有各自的链路状态数据库和对应的 OSPF 路由表信息。每一个 VRouter 支持最多 4 个 OSPF 进程，多个进程共同维护一个 VRouter 的路由表。 在指定 OSPF 进程 ID 时，注意如下事项： 每个 OSPF 进程中运行 OSPF 协议的接口网络不能重叠。

选项	说明
	当多个 OSPF 进程中存在相同前缀的路由条目时，首先比较各个路由条目的管理距离，管理距离低的将被优先加入到 VRouter 的路由表中；管理距离相同时，优先发现的的路由条目将被加入到 VRouter 的路由表中。 当其他路由协议引入 OSPF 路由时，将默认引入进程 ID 为 1 的 OSPF 路由信息。如果此进程不存在，将无法引入 OSPF 路由。
路由 ID	输入 OSPF 的路由 ID。每一台运行 OSPF 协议的路由器都必须拥有一个路由 ID。路由 ID 是每个路由器在整个 OSPF 域中唯一标识，使用 IP 地址的形式表示。
HA 同步	点击“启用”按钮，开启 HA 同步，主设备和备用设备的 OSPF 信息同步。
网络	配置运行 OSPF 协议的接口网络并且将网络配置到指定的区域中。点击”新建“按钮，弹出可编辑行，输入网络地址、网络掩码和区域 ID。 网络地址：输入运行 OSPF 协议的接口网络的 IP 地址。 子网掩码：输入 IP 地址的网络掩码。 区域 ID：输入网络的区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。
引入路由	
静态路由	点击“启用”按钮，将静态路由协议引入 OSPF 路由协议并对外发布。
直连路由	点击“启用”按钮，将直连路由协议引入 OSPF 路由协议并对外发布。
RIP	点击“启用”按钮，将 RIP 路由协议引入 OSPF 路由协议并对外发布。
OSPF	点击“启用”按钮，指定进程 ID，将其他 OSPF 进程引入该进程并对外发布。
ISIS	点击“启用”按钮，将 ISIS 路由协议引入 OSPF 路由协议并对外发布。
BGP	点击“启用”按钮，将 BGP 路由协议引入 OSPF 路由协议，并对外发布。
VPN	点击“启用”按钮，将 VPN 路由引入 OSPF 路由协议，并对外发布。

选项	说明
DOMAIN	点击“启用”按钮，将域名路由引入 OSPF 路由协议，并对外发布。

4. 点击“确定”按钮保存所做的配置。新创建的 OSPF 进程将会显示在 OSPF 路由列表中。

> 注意: OSPF 功能在设备接口上的配置包括：接口定时器、优先级、网络类型和链路开销。

查看邻居信息

查看指定 OSPF 进程的邻居信息，请按照以下步骤进行操作：

1. 选择“网络 > 路由 > OSPF”。
2. 选择需要查看邻居信息的进程 ID 前的“+”，邻居信息显示在进程列表中。

邻居路由器 ID：显示 OSPF 邻居的路由器 ID。

优先级：显示邻居路由器的优先级。路由器的优先级用来决定使用哪个路由器作为指定路由器。指定路由器用来接收网络中所有其它路由器的链路信息，并将收到的链路信息广播出去。

邻居状态：显示 OSPF 邻居状态。邻居状态包括以下 8 种：Down、Attempt、Init、2-Way、Exstart、Exchange、Loading 和 Full。其中，Full 状态包括 Full/DR（指定路由器）和 Full/BDR（备份指定路由器）。

超时时间：显示邻居超时时间。超时时间为失效时间与 Hello 发送间隔之差，单位为秒。如果在超时时间内没有收到邻居发送的 Hello 报文，则邻居关系无法继续建立。

邻居 IP：显示邻居路由器的 IP 地址。

本地接口：显示发送 Hello 报文到邻居路由器的接口。

配置 OSPFv3

OSPFv3 是 OSPF（Open Shortest Path First，开放式最短路径优先）的第 3 个版本，主要提供对 IPv6 的支持。在配置 OSPFv3 功能前，用户需首先在“网络 > 接口 > 新建”处开启 IPv6 配置，并配置 OSPFv3 接口。OSPFv3 接口配置包括：接口定时器、优先级、链路开销、被动接口和忽略 MTU。

OSPFv3 和 OSPFv2 在很多方面是相同的：

Router ID、Area ID 仍然是 32 位的。

相同类型的报文：Hello 报文，DD（Database Description，数据库描述）报文，LSR（Link State Request，链路状态请求）报文，LSU（Link State Update，链路状态更新）报文和 LSAck（Link State Acknowledgment，链路状态确认）报文。

相同的邻居发现机制和邻接形成机制。

相同的 LSA 扩散机制和老化机制。

OSPFv3 和 OSPFv2 的不同主要有：

OSPFv3 是基于链路（Link）运行，OSPFv2 是基于网段（Network）运行。

OSPFv3 在同一条链路上可以运行多个实例。

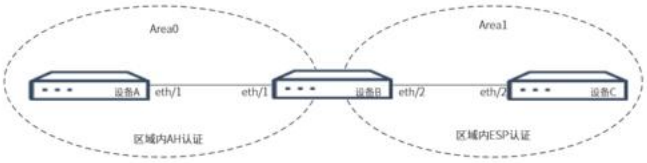
OSPFv3 是通过 Router ID 来标识邻接的邻居。OSPFv2 则是通过 IP 地址来标识邻接的邻居。

用户可以为不同的 VRouter 分别配置 OSPFv3 协议。

OSPFv3 支持基于 IPsec 的 AH（Authentication Header，认证头协议）或 ESP（Encapsulating Security Payload，封装安全负载协议）认证方式为设备邻居之间提供加密认证。OSPFv3 支持在区域内和接口下开启加密认证功能。

当需要保护同一区域内的所有 OSPFv3 协议报文时，可以在区域下开启加密认证，此时区域内所有设备需要配置相同的加密认证策略，包括相同的认证方式、SIP 值、认证算法、认证密钥等。

当需要保护区域内指定接口的 OSPFv3 协议报文时，可以在接口下开启加密认证，此时直连设备邻居的接口需要配置相同的加密认证策略，包括相同的认证方式、SIP 值、认证算法、认证密钥等。



新建 OSPFv3

新建 OSPFv3 进程，请按照以下步骤进行操作：

1. 选择“网络 > 路由 > OSPFv3”。
2. 从“虚拟路由器”下拉菜单选择一个 VR，新建的路由将属于该 VR。

3. 点击“新建”按钮，打开<OSPFv3 配置>页面。

在<OSPFv3 配置>页面，对 OSPFv3 进行基本配置。

选项	说明
进程 ID	输入 OSPFv3 的进程 ID。默认值是 1，取值范围是 1 到 65535。每个 OSPFv3 进程相互独立，有各自的链路状态数据库和对应的 OSPFv3 路由表信息。每一个 VRouter 支持最多 4 个 OSPFv3 进程，多个进程共同维护一个 VRouter 的路由表。 在指定 OSPFv3 进程 ID 时，注意如下事项： 每个 OSPFv3 进程中运行 OSPFv3 协议的接口网络不能重叠。 当多个 OSPFv3 进程中存在相同前缀的路由条目时，首先比较各个路由条目的管理距离，管理距离低的将被优先加入到 VRouter 的路由表中；管理距离相同时，优先发现的的路由条目将被加入到 VRouter 的路由表中。 当其他路由协议引入 OSPFv3 路由时，将默认引入进程 ID 为 1 的 OSPFv3 路由信息。如果此进程不存在，将无法引入 OSPFv3 路由。
路由 ID	输入 OSPFv3 的路由 ID。每一台运行 OSPFv3 协议的路由器都必须拥有一个路由 ID。路由 ID 是每个路由器在整个 OSPFv3 域中唯一标识，使用 IP 地址的形式表示。
HA 同步	点击“启用”按钮，开启 HA 同步，主设备和备用设备的 OSPFv3 信息同步。

选项	说明
引入 IPv6 路由	
静态路由	点击“启用”按钮，将静态路由协议引入 OSPFv3 路由协议并对外发布。
直连路由	点击“启用”按钮，将直连路由协议引入 OSPFv3 路由协议并对外发布。
RIPng	点击“启用”按钮，将 RIPng 路由协议引入 OSPFv3 路由协议并对外发布。
OSPFv3	点击“启用”按钮，指定进程 ID，将其他 OSPFv3 进程引入该进程并对外发布。
ISISv6	点击“启用”按钮，将 ISISv6 路由协议引入 OSPFv3 路由协议并对外发布。
BGP+	点击“启用”按钮，将 BGP+路由协议引入 OSPFv3 路由协议并对外发布。
加密认证：点击列表下方的“新建”按钮，开启 OSPFv3 的区域内加密认证功能。	
区域 ID	输入 OSPFv3 的区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。
认证方式	从下拉菜单中选择 OSPFv3 区域的认证方式，可以为 AH 认证或 ESP 认证。 注意：AH 认证不支持数据加密，即不支持配置“加密算法”和“加密密钥”。
安全参数序列	输入 SPI（Security Parameter Index，安全参数索引）值，范围是 256-4294967295。接收方接收报文时通过 SPI 值进行认证。
认证算法	从下拉菜单中选择 OSPFv3 区域内认证的认证算法，可以为基于 MD5 或 SHA1 算法的认证。
认证密钥	输入 OSPFv3 区域内认证的认证密钥。认证密钥为 16 进制字符。
加密算法	当选择认证方式为“ESP”时，需要指定加密算法。 可以为“-”、“DES”、“3DES”、“AES-128”、“AES-192”或“AES-256”。“-”即不指定加密算法，ESP 只提供认证功能。
加密密钥	当配置完“加密算法”后，需要输入相应的加密密钥。认证密钥为 16 进制字符。 **说明：**加密算法配置为“-”时，不需要配置加密密钥。
虚拟链路	
区域 ID	非骨干区域之间的路由信息必须通过骨干区域来转发。用

选项	说明
	户可以通过配置 OSPF 虚拟链路（Virtual Link）实现非骨干区域与骨干区域的连通，以及骨干区域自身的连通。指定虚拟链路穿过的区域 ID，区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。
虚拟链路对端 ABR 路由器 ID	虚链路总是建立在两台区域边界路由器(ABR)之间，且必须在两端同时配置才能生效。其中至少一台 ABR 属于骨干区域。指定虚拟链路对端 ABR 的路由器 ID，使用 IP 地址的形式表示。

4. 点击“确定”按钮保存所做的配置。新创建的 OSPFv3 进程将会显示在 OSPFv3 路由列表中。

5. **点击页面右上角的“接口配置”，打开<接口>页面，对 OSPFv3 进行接口配置。**

选项	说明
编辑	勾选所需接口前的复选框，点击“编辑”，打开<接口配置>页面，对该接口进行详细配置。
接口区域配置	配置接口所属的 OSPFv3 区域及实例。 **接口**：指定运行 OSPFv3 协议的接口。 **区域 ID**：指定接口所属区域的 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。 **实例 ID**：指定接口所属的实例 ID。建立邻居关系的接口必须属于相同的实例。取值范围是 0 到 255。默认值是 0。 **接口定时器**：接口的定时器有以下四个：接口发送 Hello 包的时间间隔、接口相邻路由器的失效时间、接口重传 LSA 的时间间隔以及接口更新包的延迟时间。 Hello 发送间隔：指定接口发送 Hello 包的时间间隔，单位为秒。默认值是 10 秒（若 OSPFv3 接口选择点到多点的网络类型，则默认值是 30 秒）。范围是 1 到 65535 秒。 失效时间：指定接口的相邻路由失效时间，单位为秒。默认值是 40 秒（发送 Hello 包时间间隔的 4 倍）。若 OSPFv3 接口选择点到多点的网络类型，则默认值是 120 秒。范围是 1 到 65535 秒。 如果接口在一定的时间内都没有收到对方的 Hello 报文，则认为对端路由器失效，这个一定的时间就是相邻路由器间的失效时间。

选项	说明
	LSA 重传间隔：指定接口重传 LSA（链路状态通告）的时间间隔，单位为秒。默认值是 5 秒。范围是 3 到 65535 秒。 LSU 传输时间：指定发送链路状态更新报文的延迟时间，单位为秒。默认值是 1 秒。范围是 1 到 65535 秒。 **优先级**：指定接口路由器的优先级。默认值是 1。范围是 0 到 255。优先级为 0 的路由器不会被选中作为指定路由器（用来接收网络中所有其他路由器的链路信息，并将收到的链路信息广播出去）。当同一个网络的两个路由器都可作为指定路由器时，优先级高的路由器会被选中；如果优先级也相同，Router ID 高的会被选中。 **网络类型**：指定接口的网络类型，包括广播、点到点（Point-to-point）以及点到多点（Point-to-multipoint）网络类型。默认情况下，接口的网络类型为广播类型。 **链路开销**：指定接口的链路开销值，取值范围是 1 到 65535。 **被动**：用户可以将一些接口配置为只接收更新但是不发送，这种只接收更新的接口就是被动接口。点击“启用”按钮，开启该接口为被动接口。 **忽略 MTU**：OSPFv3 通过 DBD 报文检查邻居间的接口 MTU 设置是否匹配。如果相邻的 OSPFv3 路由器接口之间的 MTU 不匹配，则他们之间不能建立邻接关系。用户可通过修改接口的 MTU 来解决此问题。但是，有些接口无法修改 MTU，这时用户可点击“启用”按钮，使 OSPFv3 忽略对 MTU 匹配的检查。 **加密认证**：点击“启用”按钮，开启 OSPFv3 的接口下加密认证功能。该功能默认是关闭状态。 认证方式：指定 OSPFv3 接口的认证方式，可以为 AH 认证、ESP 认证、AH NULL 或 ESP NULL。AH NULL 表示接口不开启 AH 认证，ESP NULL 表示接口不开启 ESP 加密认证。 安全参数序列：指定 SPI（Security Parameter Index）值，范围是 256-4294967295。接收方接收报

选项	说明
	文时通过 SPI 值进行认证。 认证算法：从下拉菜单中选择 OSPFv3 接口下认证的认证算法，可以为基于 MD5 或 SHA1 算法的认证。 认证密钥：输入 OSPFv3 接口下认证的认证密钥。认证密钥为 16 进制字符。 加密算法：当选择认证方式为“ESP”时，需要指定加密算法。可以为“-”、“DES”、“3DES”、“AES-128”、“AES-192”或“AES-256”。“-”即不指定加密算法，ESP 只提供认证功能。 加密密钥：当配置完“加密算法”后，需要输入相应的加密密钥。认证密钥为 16 进制字符。 **说明：**加密算法配置为“-”时，不需要配置加密密钥。

注意:

对于 OSPFv3 路由的加密认证功能：

当区域开启了加密认证，且区域内的所有接口未单独开启加密认证，则该区域内的所有接口使用区域的加密认证策略。

当接口和接口所属区域均开启了加密认证，且接口的认证方式非 AH NULL 或 ESP NULL，则接口下的加密认证策略优先生效。

当接口所属区域开启了加密认证，接口的认证类型不一致且配置为 NULL，则该接口使用区域的加密认证策略。例如：接口所属区域配置 AH 认证，接口配置 ESP NULL，则该接口使用区域的加密认证策略。

当接口所属区域开启了加密认证，接口的认证类型一致但配置为 NULL，则该接口下的报文不进行认证加密。例如：接口所属区域配置 ESP 认证，接口配置 ESP NULL，则该接口下的报文不进行加密认证。

接口和接口所属区域只能配置一种认证方式。

查看邻居信息

查看已创建的 OSPFv3 进程的邻居信息，请按照以下步骤进行操作：

1. 选择“网络 > 路由 > OSPFv3”。

2. 选中已创建的 OSPFv3 进程，邻居信息显示在页面列表中。

邻居路由器 ID：显示 OSPFv3 邻居的路由器 ID。

优先级：显示邻居路由器的优先级。路由器的优先级用来决定使用哪个路由器作为指定路由器。指定路由器用来接收网络中所有其它路由器的链路信息，并将收到的链路信息广播出去。

链路本地地址：显示邻居路由器接口的链路本地地址（Link-local）。

邻居状态：显示 OSPFv3 邻居状态。邻居状态包括以下 8 种：Down、Attempt、Init、2-Way、Exstart、Exchange、Loading 和 Full。其中，Full 状态包括 Full/DR（指定路由器）和 Full/BDR（备份指定路由器）。

超时时间：显示邻居超时时间。超时时间为失效时间与 Hello 发送间隔之差，单位为秒。如果在超时时间内没有收到邻居发送的 Hello 报文，则邻居关系无法继续建立。

本地接口：显示发送 Hello 报文到邻居路由器的接口。

配置 BGP

BGP 是边界网关协议（Border Gateway Protocol）的缩写。自治系统（Autonomous System）是处于一个管理机构控制之下的路器和网络群组。BGP 是在自治系统之间或在一个自治系统之内动态交换路由信息的路由协议，在同一自治系统间运行 BPG 路由协议形成的邻居关系，称为 IBGP（Internal Border Gateway Protocol）邻居关系；在不同自治系统间运行 BGP 路由协议形成的邻居关系，称为 EBGP（External Border Gateway Protocol）邻居关系。

BGP GR

GR（Graceful Restart）即平滑重启，也被称作 NSF（Non-Stop Forwarding）。

BGP GR 技术可以保证设备在主备切换或者设备重启时转发层面能够继续数据的转发，且控制层面邻居关系的重建及路由计算不会影响转发层面的功能，从而减少单点故障以及主备切换时路由震荡对网络的影响，提升整网的可靠性，避免流量中断对用户重要业务的影响。

BGP GR 基础概念：

End-of-RIB 标记：End-of-RIB 标记实际上是一个特殊的 BGP Update message。它没有可达的 NLRI（网络可达层信息，Network Layer Reachability Information），同时撤回 NLRI 也为空。其主要作用是当前设备从对等体收到 End-of-RIB 标记之后，表明该对等体所有需要通告的更新已经发送完毕。

Graceful Restart Capability：为支持 GR 功能，BGP 协议新增了一个 BGP Capability，即 Graceful Restart Capability。它在 BGP 连接建立时，随着 Open message 进行发布。它可以声明当前设备在 BGP 重启时依然能够维持转发能力，还可以声明当前设备在初始的 update 发送完毕后能产生 End-of-RIB 标记。

GR Restarter：指发生主备切换或者 BGP 协议重启时，以 GR 方式重启的设备。

GR Helper：GR Restarter 的邻居，具有 GR 能力，协助 GR Restarter 进行 GR 的设备。

一台设备既可以作为 GR Restarter，也可以作为 GR Helper，其角色确定由该设备在 BGP GR 过程中的实际作用决定。

以设备 HA 为例，BGP GR 的工作过程如下：

1. 在 HA 切换后，新主设备作为 GR Restarter 与 GR Helper 重新建立 BGP 连接。
2. GR Helper 断开与旧主设备的 BGP 邻居，将从旧主设备学习的 BGP 路由标记为 stale 状态（失效路由），但仍按照这些路由转发数据报文，并启动对等体陈旧路由保持时间（通过 **graceful-restart stale-path-time** *time* 配置）。
3. GR Restarter 如果在通告的 GR 等待重建时间（通过 **graceful-restart restart-path-time** *time* 配置）内与 GR Helper 成功建立 BGP 会话，则二者建立 BGP 邻居关系并进行路由信息交互。如果在通告的 GR 等待重建时间内未与 GR Helper 建立 BGP 邻居关系，GR Helper 将立即删除与 GR Restarter 相关的路由。
4. GR Helper 与 GR Restarter 建立邻居关系后，发送本地更新，并在更新完成后通告 End-of-RIB 标记，表示更新发送完毕。 即便 GR Helper 本地没有需要通告的更新，也必须发送 End-of-RIB 标记。
5. GR Restarter 在收到所有对等体发送的 End-of-RIB 标记后开始选择最佳路径。如果一直没收到必须的全部 End-of-RIB 标记， GR Restarter 会在所配置的 GR 等待 End-of-Rib 标记时间（通过 **graceful-restart wait-for-rib-time** *time* 配置）结束后开始选择最佳路径。
6. 最佳路径选择完毕后， GR Restarter 更新 RIB 路由表，产生 BGP 路由更新并发送给 BGP 邻居，无论是否有更新，都需通告 End-of-RIB 标记。
7. GR Helper 收到路由更新后，将相关路由的 stale 标记移除；在收到 GR Restarter 发送的 End-of-RIB 标记后，移除仍有 stale 标记的路由。
8. 如果在对等体陈旧路由保持时间内一直未完成路由信息的交互，则 GR Restarter 会强制退出 GR 过程，根据已经学习到的 BGP 路由信息更新 RIB 表项，删除老化的 RIB 表项。

基本配置

配置 BGP 进程的基本配置，请按照以下步骤进行操作：

1. 选择“网络 > 路由 > BGP”。
2. 从“虚拟路由器”下拉菜单选择需要创建 BGP 的虚拟路由器，默认虚拟路由器为 trust-vr。

3. 在<BGP>页面，填写 BGP 的基本信息。

配置 BGP 基本配置

选项	说明
AS	指定自治系统（Autonomous System）的编号，范围是 1 到 4294967295。
路由器 ID	指定运行 BGP 协议的路由器 ID。路由 ID 是每个路由器在整个 BGP 域中的唯一标识，使用 IP 地址的形式表示。
启用 GR	点击“启用”按钮，开启 BGP GR 功能。 GR 等待重建时间：指定对端等待重建 BGP 会话的最大时间。取值范围为 1 到 3600 秒。默认值为 120 秒。 GR 陈旧路由保持时间：指定保持重新启动对等体的陈旧路由的最大时间。取值范围为 1 到 3600 秒。默认值为 360 秒。 GR 等待 End-of-Rib 标记时间：指定 GR Restarter 等待邻居 End-of-RIB 标记的最大时间。取值范围为 1 到 3600 秒。默认值为 180 秒。
HA 同步	点击“启用”按钮，开启 HA 同步，主设备和备用设备的 BGP 信息同步。
启用 IPv6	点击“启用”按钮，启用 IPv6 地址。启用后，BGP 支持 IPv6 地址格式。
IPv4	
网络	用户可添加本地路由表中指定网段的路由至 BGP 路由表，也可从列表中删除指定网段。指定后，邻居路由器可学习到该网段的路由信息。

选项	说明
	新建：点击“新建”按钮，指定 IPv4 地址和子网掩码。当 IPv6 启用后，可以指定 IPv6 地址和前缀长度。 删除：如果需要删除指定网段的路由，从列表中选中需要删除的网段，然后点击下方的“删除”按钮。
邻居	用户可添加与指定路由器 ID 交换 BGP 路由信息的邻居路由器，也可从列表中删除指定的邻居路由器。用户最多可以添加 8 条邻居路由器。 新建：点击“新建”按钮，指定 BGP 邻居的信息。 **IP**：指定邻居路由器的 IP 地址。 **AS**：指定邻居路由器所在的自治系统编号，范围是 1 到 4294967295。 **下一跳为自身**：对于 EBGP 的邻居路由器，如果下一跳地址对于该邻居路由器的 IBGP 为不可达，需要设置下一跳为自身。 **EBGP 多跳**：对于运行在自治系统之间的 BGP（即 EBGP），如果当前路由器与邻居路由器建立的连接不是直连，需要指定最大下一跳数，取值范围是 0-255。 **激活**：激活已配置的邻居路由器与当前设备的 BGP 连接。默认情况下，“激活”功能是开启的。 **关闭**：将邻居 BGP 移出列表。关闭后，与被关闭邻居路由器的所有会话会被中断、所有相关的路由信息也会被删除。默认情况下，“关闭”功能是关闭的。 删除：如果需要删除指定的邻居路由器，从列表中选中该邻居路由器，然后点击下方的“删除”按钮。
引入路由	当支持的地址是 IPv4 格式的地址，指定引入的其他路由协议的路由信息。 **静态路由**：选中复选框，将静态路由协议引入 BGP 路由协议并对外发布。 **直连路由**：选中复选框，将直连路由协议引入 BGP 路由协议并对外发布。

选项	说明
	OSPF：选中复选框，将 OSPF 路由协议引入 BGP 路由协议并对外发布。 **RIP**：选中复选框，将 RIP 路由协议引入 BGP 路由协议并对外发布。 **IS-IS**：选中复选框，将 IS-IS 路由协议引入 BGP 路由协议并对外发布。 当支持的地址是 IPv6 格式的地址，指定引入的其他路由协议的路由信息。 **静态路由**：选中复选框，将静态路由协议引入 BGP 路由协议并对外发布。 **直连路由**：选中复选框，将直连路由协议引入 BGP 路由协议并对外发布。 **OSPFv3**：选中复选框，将 OSPFv3 路由协议引入 BGP 路由协议并对外发布。 **RIPng**：选中复选框，将 RIPng 路由协议引入 BGP 路由协议并对外发布。 **ISISv6**：选中复选框，将 ISISv6 路由协议引入 BGP 路由协议并对外发布。

4. 点击“确定”按钮保存所做的配置。新创建的邻居路由器将会显示在邻居列表中。

邻居列表

查看已创建的邻居路由器，请按照以下步骤进行操作：

1. 选择“网络 > 路由 > BGP”。
2. 点击“邻居列表”，打开“邻居列表”页面，查看邻居信息。

邻居 IP：显示邻居路由器的 IP 地址。

AS：显示邻居路由器的所在的自治系统编号。

远程路由器 ID：当邻居路由器与当前路由器的连接激活时，显示对端路由器 ID。

BGP 类型：显示 BGP 的运行方式。当 BGP 运行在自治系统之间时，为 EBGP；当 BGP 运行在自治系统之内时，为 IBGP。

状态：显示邻居路由器与当前路由器的连接状态，包括 Idle（空闲）、Connect（连接）、Active（活跃）、OpenSent（打开消息已发送）、OpenConfirm（打开消息确认）、Established（连接已建立）。

删除 BGP

删除 BGP 进程，请按照以下步骤进行操作：

1. 选择“网络 > 路由 > BGP”。
2. 点击“删除 BGP”按钮，即可删除所有的 BGP 配置。

第 5 章 用户认证

对用户和主机进行识别，即为“认证”，认证是产品的一个重要功能。开启了认证功能的网络能够允许或拒绝用户和主机对网络进行访问。从用户的角度出发，认证可以分为：

位于企业内网的用户通过认证访问互联网。该方式下的认证支持以下几种：

"Web 认证"

"单点登录"

"802.1x 认证"

"PKI"

位于互联网的用户访问内网的资源（通常使用 VPN）

"SSL VPN"

"IPSec VPN" （IPSec VPN （radius 服务器）+Xauth）

"L2TP VPN"（L2TP over IPsec VPN）

用户认证流程

用户通过终端与防火墙建立连接，防火墙基于存储在 AAA 服务器上的用户信息来认证用户。

认证用户（User）：认证请求者。用户发起认证给认证系统，并输入用户名和口令。

认证系统（Firewall）：接收用户名和密码，并向认证服务器发送认证请求。认证系统在认证用户和认证服务器之间充当代理角色。

认证服务器（AAA Server）：判断认证请求。该服务器可以存储用户的相关信息，如用户名称、用户口令等。它收到合法请求后，判断用户是否有权使用网络资源，并向认证系统返回认证结果。认证服务器分为以下五种：

本地服务器

Radius 服务器

LDAP 服务器

AD 服务器

TACACS+服务器

Web 认证

Web 认证功能用来对通过设备访问 Internet 的用户进行身份认证。配置 Web 认证功能后，打开浏览器访问互联网页面会被重定向到 Web 认证登录页面，根据认证方式的不同，用户需要在该页面提供正确的认证信息；Web 认证成功后，系统会按照策略配置给 IP 地址分配角色，从而实现设备对不同用户的访问控制。

Web 认证是指通过打开认证界面进行认证的方式。包括多种认证方式：口令认证、短信认证、NTLM 认证。

口令认证：通过用户名和密码的方式实现 Web 认证。

短信认证：通过短信认证的方式实现 Web 认证。用户需要在登录页面输入用于接收验证码的手机号码，然后再输入收到的手机短信验证码，才可以通过认证。

NTLM 认证：认证过程为安全设备自动获取用户本地 PC 端的登录用户信息，验证用户身份。

> 注意: NTLM 认证模式仅支持 Windows server 2008 之前版本的 Active-Directory 服务器。

启用 Web 认证

启用 Web 认证功能，请按照以下步骤进行操作：

1. 点击“网络>Web 认证>Web 认证”，进入 Web 认证主窗口。
2. 点击 Web 认证页面的“启用”按钮。

配置 Web 认证的基本参数

Web 认证的基本参数是对所有使用 Web 认证的策略生效的通用参数。

配置 Web 认证基本参数，请按照以下步骤进行操作：

1. 点击“网络 >Web 认证>Web 认证”，进入 Web 认证主窗口，点击“启用”按钮。

2. 在<基本配置>页面对 Web 认证功能进行详细设定。

基本配置	
Web 认证	点击“启用”按钮。
HTTP	“协议”选择 HTTP 认证模式。 端口：指定认证服务器的 HTTP 端口号。取值范围是 1 到 65535。默认值是 8181。
HTTPS	“协议”选择 HTTPS 认证模式。HTTPS 为加密协议，可以防止用户信息被窃取。 端口：指定认证服务器的 HTTPS 端口号。取值范围是 1 到 65535。默认值是 44433。 信任域：指定 HTTPS 信任域的名称。此 PKI 信任域已经建立，并且已经导入从国际 CA 认证中心购买的证书。
所有接口	指定所有接口 Web 认证功能的全局默认配置，包括默认开启认证服务和默认关闭认证服务。配置指定接口的 Web 认证功能，参见"配置接口" 在第 15 页。
代理端口	指定 HTTP、HTTPS 或 SSO 代理服务器用来代理相应请求的端口号。取值范围是 1 到 65535。

用户登录	
地址类型	指定认证用户地址类型为 IP 或 MAC。默认情况下，认证用户地址类型为 IP。 说明：指定认证用户地址类型为 MAC 时，设备需与客户端部署在同一个二层网络环境中，否则系统获取客户端的 MAC 地址时失败或者获取到的 MAC 地址错误。
多客户端登录	配置是否允许同一用户帐户在多个客户端同时登录。 如果不允许多客户端同时登录，可选择踢出已经登录的用户，或者禁止同名用户再次登录。 如果允许多客户端同时登录，那么可以限制同时登录的客户端个数。
认证模式	
口令认证：指定认证模式为口令认证方式。	
空闲超时时间	指认证成功页面在无流量状态下能够保持连接状态的最长时间，超出空闲超时时间后，将会断开连接。 点击“空闲超时时间”后的“启用”按钮，开启空闲超时时间功能，并在文本框中输入空闲超时时间。点击禁用按钮，关闭空闲超时时间功能。
强制超时时间	系统可强制用户在登录超过设定时间后，必须重新登录。 点击“强制超时时间”后的“启用”按钮，开启强制超时时间功能，并在文本框中输入强制用户重新登录时间间隔。点击禁用按钮取消勾选该复选框，关闭强制超时时间功能。
重认证时间间隔	当用户认证成功并访问网络后，系统可以对用户进行重认证。 点击“重认证时间间隔”后的“启用”按钮，开启重认证时间间隔功能，并在文本框中输入用户重认证的时间间隔。点击禁用按钮，关闭重认证时间间隔功能。
心跳超时时间	认证成功后，系统会在超时时间结束前对认证成功页面进行自动刷新，确认登录信息。 点击“客户端心跳超时”后的“启用”按钮，并在文本框中输入客户端超时时间。点击禁用按钮，关闭客户端心跳超时功能。
重定向 URL	重定向 URL 是指当客户端发送 HTTP 网页访问请求后，系统自动将该请求重新定向到指定的页面。 **注意：** 系统可以通过在 URL 地址中指定用户名和密码，当用户指定的重定向 URL 页面为内网中需认证的应用系统页面时，无需再次认证便可以正常访问应用系统。 对应的关键字为$USER,$PWD 或$HASHPWD 参数(通常$PWD 和$HASHPWD 参数二选一即可)。例如: example.com/oa/login.do?username=$USER&password=$HASHPWD 。
短信认证：指定认证模式为短信认证方式。	
认证方式	选择发送认证短信的方式，短信猫或者短信网关。

短信认证码有效时长	用户使用短信认证时，需要使用手机收到的短信验证码，验证码在超时时间结束前生效。在超过超时时间后，如果验证码没有使用，用户需要重新获取新的短信验证码。 指定验证码超时时间，单位为分钟。取值范围是 1 到 10 分钟。默认为 1 分钟。
发送方名称	指定短信发送方名称以显示在短信内容中。取值范围是 1 到 63 字符。 **注意**：由于 UMS 企业信息平台限制，当使用短信网关发送认证短信时，发送方名称将会显示在 UMS 企业信息平台注册的名称。
签名	当短信网关的协议类型为 ALIYUNSMS 时，用户需要输入阿里云短信服务中申请的短信签名，以显示在短信内容中。取值范围是 1 到 63 字符。该参数需与在阿里云短信服务中申请的签名保持一致。
认证码长度	指定短信认证码的长度。取值范围为 4 至 8 个字符。默认为 6 个字符。
模板 CODE	当短信网关名称指定为阿里云服务商名称时，用户需要输入阿里云短信服务中申请的短信内容模板对应的 CODE（代码）。取值范围为 1 至 30 个字符。该参数需与在阿里云短信服务中申请的模板 CODE 保持一致。
空闲超时时间	认证成功页面在无流量状态下能够保持连接状态的最长时间，超出空闲超时时间后，将会断开连接。 点击“空闲超时时间”后的“启用”按钮，开启空闲超时时间功能，并在文本框中输入空闲超时时间。点击禁用按钮，关闭空闲超时时间功能。
强制超时时间	系统可强制用户在登录超过设定时间后，必须重新登录。 点击“强制超时时间”后的“启用”按钮，开启强制超时时间功能，并在文本框中输入强制用户重新登录时间间隔。点击禁用按钮，关闭强制超时时间功能。
NTLM：指定认证模式为 NTLM 认证方式。	
空闲超时时间	认证成功页面在无流量状态下能够保持连接状态的最长时间，超出空闲超时时间后，将会断开连接。 点击“空闲超时时间”后的“启用”按钮，开启空闲超时时间功能，并在文本框中输入空闲超时时间。点击禁用按钮，关闭空闲超时时间功能。
强制超时时间	系统可强制用户在一段时间后重新登录。 点击“强制超时时间”后的“启用”按钮，开启强制超时时间功能，并在文本框中输入强制用户重新登录时间间隔。点击禁用按钮，关闭强制超时时间功能。
认证失败时	设定如果 NTLM 认证登录失败，用户的下一步操作。 选择“无动作”，则定义为认证失败，且不采取任何措施。 选择“口令认证”，那么用户通过密码认证方式继续认证。
口令认证/短信认证：指定认证模式为口令认证或者短信认证。	
口令认证	选择<口令认证>标签页，填写口令认证相关参数，具体说明参阅“口令认证”部分。
短信认证	选择<短信认证>标签页，填写短信认证相关参数，具体说明参阅“短信认证”部分。

短信认证：指定认证模式为短信认证。	
短信认证	选择<短信认证>标签页，填写短信认证相关参数，具体说明参阅“短信认证”部分。

3. 点击“确定”，使配置生效。

注意:

关闭认证成功页面后，不仅可以等待超出空闲超时时间后断开连接，还可以访问认证状态页面退出登录，认证状态页面中显示在线用户名称、在线时间和退出按钮。访问方法为“http(https)://IP-Address: Port-Number”。其中，“IP-Address”和“Port-Number”分别为认证接口地址和认证服务器端口号，默认情况下，HTTP 端口号为 8181，HTTPS 端口号为 44433。如果当前客户端无在线用户或者设备未开启 Web 认证，则该功能不生效。

为了使 Web 认证功能生效，请在完成“基本配置”后，进入"安全策略" 进行策略配置。配置安全策略时，Web 认证的两条策略优先级需最高，且需按照策略模板配置。策略模板如下图所示：

配置 Web 认证后，符合认证策略规则的用户若想访问网络，需要提供正确的用户名和密码（该用户应是 AAA 服务器中已有的用户）。通过认证后，出现认证成功页面，并可访问网络资源。为了防止非法用户通过暴力方法获取用户名和密码，系统支持防暴力破解，即在 2 分钟内，若用户使用同一主机连续 3 次输入错误的用户名和密码，该主机将会被锁定 2 分钟。

若希望通过 HTTPS 流量触发 Web 认证，需将设备证书导入到客户端的浏览器中。通过 HTTPS 流量触发 Web 认证功能依赖 SSL 代理功能，若系统不支持 SSL 代理功能，请通过 HTTP 流量来触发 Web 认证。

主动认证只支持口令认证和短信认证模式， 若系统已配置为 NTLM 认证模式，则主动认证将以口令认证的方式生效。

定制 Web 认证登录页面

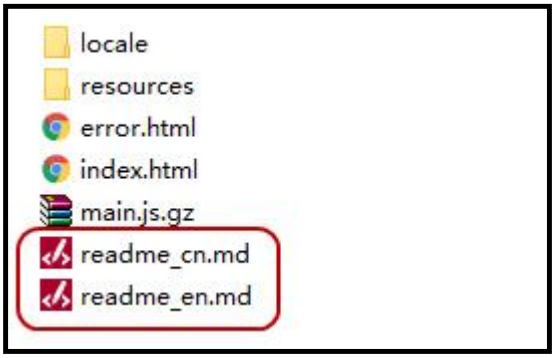
认证界面是 PC 端打开网页时被重定向的界面。默认页面中只要求用户输入用户名和密码，也可以选择短信认证模式。

系统有默认的认证界面，也支持用户自定义该界面。自定义认证界面，按照以下步骤进行操作：

1. 点击“网络>Web 认证>Web 认证"，进入 Web 认证主窗口。

2. 选择<登录页面定制>标签页，点击“下载模板”按钮下载系统默认认证界面的文件压缩包“webauth.zip"，并将该压缩包解压缩。

3. 打开源文件，根据需求进行修改，包括样式、图片等。修改方法请参阅“readme_cn.md”或“readme_en.md”文件，该文件可以通过记事本打开。



4. 将修改后的文件夹压缩，并点击“上传”按钮，将压缩包导入到系统。

注意:

上传的自定义页面的压缩包需要符合以下要求：上传文件格式为 zip；文件数量不能超过 50 个；压缩包最大为 1M；源文件中必须包含“index.html”文件。

系统仅保留一份默认模板页面和一份自定义页面文件，成功上传新的自定义页面后会覆盖之前的文件，建议管理员先进行本地调试并备份之前的文件。

NTLM 认证

NTLM 认证需要终端的用户打开浏览器，通过浏览器去触发认证，浏览器将用户 PC 的登录信息作为认证信息发给 AD 服务器，实现认证。

NTLM 认证需要配置以下两个步骤。

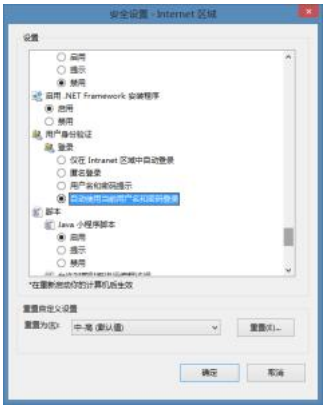
步骤一：在系统上进行配置

1. 点击“网络 >Web 认证>Web 认证”，进入 Web 认证主窗口。
2. 选择“NTLM”认证模式，基本参数请参阅配置 Web 认证的基本参数。
3. 点击“应用”确认。

步骤二：在用户 PC 上进行配置

1. 在用户的 PC 端，打开浏览器（以 IE 为例）。
2. 在菜单栏，点击“工具 > Internet 选项”。
3. 在弹出的对话框点击“安全”标签页，然后点击“自定义级别.”。

4. 在弹出的对话框找到“用户身份验证”，然后选择“自动使用当前用户名和密码登录”。



5. 点击“确定”。

单点登录

单点登录（SSO，Single Sign-On）指用户通过一次认证之后，系统通过某种方式获取其认证信息，之后该用户不需要再次在设备上进行认证，即用户可以实现“免认证”上网。

单点登录有多种实现方式，互相独立，均可实现“免输入”（不输入用户名、密码）认证。实现方式如下表所示：

实现方式	安装软件或脚本	描述
SSO Radius	---	启用 SSO Radius 功能后，系统可接收基于 Radius 标准协议的计费报文，并根据报文内容获取用户认证信息、更新在线用户信息以及对用户进行上下线操作。

实现方式	安装软件或脚本	描述
AD Scripting	脚本文件 Logonscript.exe	在 AD 服务器上安装脚本文件“Logonscript.exe”，通过脚本文件将上线用户发送给 StoneOS 系统。
Radius Snooping	---	Radius 为远程认证拨入用户服务， 是用于 NAS 和 AAA 服务器间通信的一种协议。 Radius Snooping 通过 解析镜像到设备上的 Radius 报文， 系统将自动获取认证用户的用户名和 IP 地址对应关系， 用于为设备 日志功能模块提供对认证用户的审计功能。
Agile Controller	---	启用 Agile Controller 功能后，系统可接收 Agile Controller 服务器发送的用户上下线报文和用户信息更新报文，根据报文内容获取用户认证信息，并进行在线用户上下线及在线用户信息更新操作。
AD Polling	---	启用 AD Polling 功能后，StoneOS 系统定时查询并获取 AD 服务器上的上线用户信息，并定时探测在线用户是否下线。
SSO Monitor	---	启用 SSO Monitor 功能后，StoneOS 系统通过 SSO-Monitor 协议与第三方认证服务器建立连接并获取用户在线状态及所属用户组信息，并实时更新用户名和 IP 的映射关系。
TS Agent	软件 Terminal Service Agent	在 Windows 服务器上安装并运行 Terminal Service Agent 软件。启用 TS Agent 功能后，当用户通过远程桌面服务登录 Windows 服务器时， Terminal Service Agent 为用户分配端口段，并将端口段和用户信息发送给设备，设备创建基于流量 IP、端口段和用户的映射信息，实现用户的“免登录”。

开启 SSO Radius 实现单点登录

启用 SSO Radius 功能后，系统可接收基于 Radius 标准协议的计费报文，并根据报文内容获取用户认证信息、更新在线用户信息以及对用户进行上下线操作。

配置 SSO Radius 功能，按照以下步骤进行操作：

1. 点击“对象>SSO Server>SSO Radius"，进入 SSO Radius 页面。默认情况下，SSO Radius 为关闭状态。
   注意：执行开启操作后，必须间隔 20 秒以上才能执行关闭操作，反过来也一样。
2. 点击“启用”按钮，开启 SSO Radius 功能。

3. 指定 StoneOS 接收 Radius 报文的端口号（不可在非根 VSYS 中配置端口）。取值范围为 1024 到 65535，默认端口号为 1813。

4. 指定用户所属的 AAA 服务器。系统支持选择已配置的 Local、AD 或者 LDAP 类型的服务器。选择 AAA 服务器后，系统可以在引用的 AAA 服务器上查询在线用户的用户名对应的用户组和角色信息，从而实现基于用户组和角色的策略控制。

5. 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。

6. 指定允许接入的 SSO Radius 客户端的 IP 地址、共享密钥和空闲超时时间。最多可以配置 8 个客户端。

   IP 地址：指定 SSO Radius 客户端的 IPv4 地址或 IPv6 地址（仅当系统版本为 IPv6 版本时可指定 IPv6 地址）。当 IP 地址输入“any”时，表示系统接受任意 SSO Radius 客户端发送的报文。

   共享密钥：指定 SSO Radius 客户端的共享密钥。取值范围为 1 到 31 个字符。设备使用共享密钥校验报文，校验成功后，才会对报文进行解析，否则丢弃报文。SSO Radius 客户端需要配置与设备相同的共享密钥，或者 SSO Radius 客户端和设备都不配置共享密钥，报文才能通过校验。如需修改共享密钥，点击共享密钥输入框，开启修改功能，然后在输入框中输入新的密钥保存即可。

   心跳超时时间（分钟）：心跳超时时间用来设置 Radius 报文中的用户认证信息在设备中的存活时间。如果在心跳超时时间内未收到此用户相关更新或删除报文，设备将删除用户认证信息。默认值为 30。如果设置为 0，则代表永不超时。如果同时配置了空闲超时时间和心跳超时时间， 用户会在两者中的最小时间点下线。

   空闲超时时间（分钟）：空闲超时时间指认证用户在无流量状态下保持认证状态的最长时间，超出空闲超时时间后，设备删除用户认证信息。取值范围是 0-1440，默认值为 0。如果设置为 0，则认证用户在无流量状态下永不超时。

   强制超时时间（分钟）：当用户在线时长超过配置的强制超时时间后，系统会提出用户，强制用户下线。取值范围是 0-1440，默认值为 0。如果设置为 0，则关闭该功能。

7. 点击“应用”按钮保存所做配置。

通过 AD Scripting 实现单点登录

在 Active Directory 服务器已经搭建完成的情况下，在 AD 服务器上安装脚本程序进行单点登录，按照以下步骤操作：

步骤一：在 AD 服务器上配置脚本程序

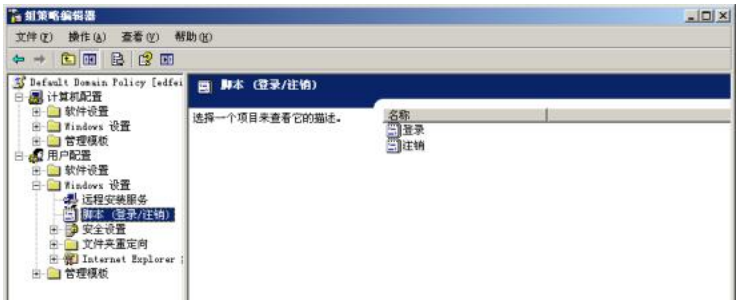
在 AD 服务器上配置脚本程序方法如下：

1. 打开 AD Agent 软件。在<AD Scripting>标签页，点击“获取 AD Scripting”获取脚本程序“Logonscript.exe”，然后将该脚本存放在域成员均有权限访问的路径下。

2. 在 AD 服务器上，进入“开始”菜单，选择“管理工具 > Active Directory 用户与计算机”，弹出<Active Directory 用户与计算机>对话框。

3. 右键点击要应用单点登录的域，选择“属性”，然后点击<组策略>标签页。

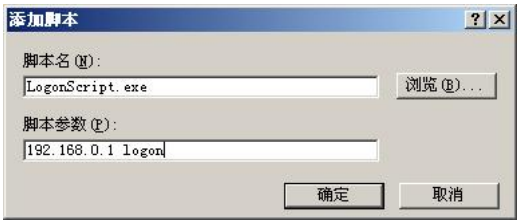
4. 在策略列表中，双击要应用单点登录的组策略，然后在弹出的<组策略编辑器>窗口中，点击“用户配置 > Windows 设置 > 脚本（登录/注销）”。



5. 双击右侧窗口的“登录”，在弹出的<登录属性>对话框中，点击“添加”。

6. 在弹出的<添加脚本>对话框中，点击“浏览”选择脚本程序（logonscript.exe），然后在“脚本参数”处输入 StoneOS 系统的认证接口地址 IP 和“Logon”字样（以空格隔开）。然后，点击“确定”

按钮。



7. 同样的，设置注销时启动的脚本程序。方法同步骤 5-6，注意输入“脚本参数”时，命令为“Logoff”。

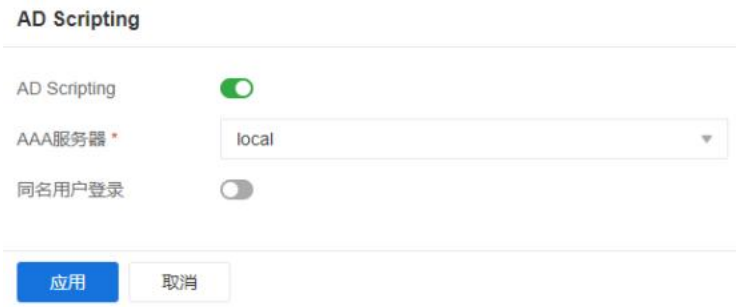
注意: 存储脚本程序的目录必须保证所有域用户均具有访问权限，否则脚本程序不能被触发。

步骤二：在系统上配置 AD Scripting 功能

AD Scripting 功能使用户通过认证服务器认证的同时，即可自动通过设备认证。目前只支持 Active-Directory 服务器的 AD Scripting 功能。

配置 AD Scripting 功能，请按照以下步骤进行操作：

1. 点击“对象> SSO Server>AD Scripting”，进入 AD Scripting 配置页面。 默认情况下，AD Scripting 为关闭状态。
2. 点击“启用”按钮，开启 AD Scripting 功能。



3. 指定用户所属的 AAA 服务器。系统支持选择已配置的 Local、AD 或者 LDAP 类型的服务器。选择 AAA 服务器后，系统可以在引用的 AAA 服务器上查询在线用户的用户名对应的用户组和角色信息，从而实现基于用户组和角色的策略控制。
4. 指定空闲超时时间。空闲超时时间指认证用户在无流量状态下保持认证状态的最长时间，超出空闲超时时间后，设备删除用户认证状态。范围是 0 到 1440 分钟，默认值为 0，即在无流量状态下认证用户永不超时。

5. 用户可以根据需要，允许同名用户在多处登录或者只允许一个同名用户登录。

   允许同名用户同时多处登录：允许相同名字的用户同时多处终端登录。

   只允许一个同名用户登录, 另一同名用户被踢出：系统仅允许一个同名用户登录，后登录的用户会将已登录的用户踢出，强迫已登录用户下线。

6. 点击“应用”按钮保存所做配置。

完成以上两个步骤后，能够实时传送用户信息给 StoneOS 系统。当用户上下线时，登录和注销的行为会触发该脚本程序，脚本程序发送信息给 StoneOS 系统，完成“免输入”认证，且记录该用户的上下线行为。

Radius Snooping

Radius 为远程认证拨入用户服务， 是用于 NAS 和 AAA 服务器间通信的一种协议。 Radius Snooping 通过解析镜像到设备上的 Radius 报文，系统将自动获取认证用户的用户名和 IP 地址对应关系，生成对应的用户认证信息并加入认证用户表，用于用户流量的控制和审计。

配置 Radius Snooping 功能，按照以下步骤进行操作：

1. 点击“对象>SSO Server>Radius Snooping"，进入 Radius Snooping 页面。 默认情况下，Radius Snooping 为关闭状态。

2. 点击“启用”按钮，开启 Radius Snooping 功能。

3. 指定用户所属的 AAA 服务器。系统支持选择已配置的 Local、AD 或者 LDAP 类型的服务器。选择 AAA 服务器后，系统可以在引用的 AAA 服务器上查询在线用户的用户名对应的用户组和角色信息，从而实现基于用户组和角色的策略控制。

4. 指定空闲超时时间。空闲超时时间指认证用户在无流量状态下保持认证状态的最长时间， 超出空闲超时时间后， 设备仍未收到镜像 RADIUS 报文设备， 则会删除设备记录的用户名和 IP 地址对应关系。范围是 0 到 1440 分钟，默认值为 0，即在无流量状态下认证用户永不超时。

5. 指定强制超时时间。 当用户在线时长超过配置的强制超时时间后， 系统会踢出用户， 强制用户下线。 取值范围是 0 到 1440 分钟， 默认为 600 分钟。

6. 指定心跳超时时间。认证成功后， 系统会在心跳超时时间结束前重新确认登录信息。 如果同时配置了空闲超时时间和心跳超时时间， 用户会在两者中的最小时间点下线。取值范围是 3 到 1440 分钟。 默认为 5 分钟。

7. 配置用户名过滤。“不结束于”表示在生成认证用户时，过滤掉用户名以指定字符串结尾的用户，只有没被过滤掉的用户名，才会生成认证用户信息。字符串的取值范围是 1 到 15 个字符。

8. 点击“应用”按钮保存所做配置。

通过 Agile Controller 实现单点登录

启用 Agile Controller 功能后，系统可接收 Agile Controller 服务器发送的用户上下线报文和用户信息更新报文，根据报文内容获取用户认证信息，并进行在线用户上下线及在线用户信息更新操作，实现单点登录。

配置 Agile Controller 功能，按照以下步骤进行操作：

1. 点击“对象>SSO Server>Agile Controller"，进入 Agile Controller 页面。默认情况下，Agile Controller 为关闭状态。

2. 点击“启用”按钮，开启 Agile Controller 功能。

填写配置信息。

选项	说明
端口	指定 StoneOS 接收 Agile Controller 服务器报文的端口号（不可在非根 VSYS 中配置端口）。取值范围为 1024 到 65535，默认端口号为 8001。
强制超时时间	指定强制下线时间。当用户在线时长超过配置的强制超时时间后，系统会踢出用户，强制用户下线。取值范围是 5 到 1440 分钟，默认为 600 分钟。
AAA 服务器	在下拉列表中选择用户所属的 AAA 服务器。系统支持选择已配置的 Local、AD 或者 LDAP 类型的服务器，配置方法参见"AAA 服务器" 在第 318 页。 选择 AAA 服务器后，系统可以在引用的 AAA 服务器上查询在线用户的用户名对应的用户组和角色信息，从而实现基于用户组和角色的策略控制。
查询速率	指定系统主动向 Agile Controller 服务器查询源 IP 对应的在线用户信息时，发送查询报文的速率。取值范围为 5 到 40 次/秒，默认值为

选项	说明
	20 次/秒。
每个 IP 查询间隔时间	指定系统主动向 Agile Controller 服务器查询源 IP 对应的在线用户信息时，每个源 IP 地址的查询时间间隔。取值范围为 1 到 100 秒，默认为 20 秒。
每次最多查询 IP 数	指定系统主动向 Agile Controller 服务器查询在线用户信息时，每个查询报文中最多包含的源 IP 地址数量。范围是 1 到 50 个，默认为 50 个。
查询地址范围	指定系统主动向 Agile Controller 服务器查询源 IP 对应的在线用户信息时，需要查询的源 IP 的地址范围。在下拉菜单中，用户可搜索并选定指定的地址条目。点击 ⊕ 按钮，可新建地址条目。
客户端	点击“新建”按钮，配置 Agile Controller 客户端。最多可以配置 24 个客户端。 名称：指定 Agile Controller 服务器的名称。 IP 地址：指定 Agile Controller 服务器的 IP 地址。 虚拟路由器：指定 Agile Controller 服务器所属虚拟路由器。 共享密钥：设备使用共享密钥校验与 Agile Controller 服务器之间的加密通信报文，校验成功后，才会对报文进行解析，否则丢弃报文。Agile Controller 客户端需要配置与 Agile Controller 服务器相同的共享密钥，报文才能通过校验。取值范围为 1-31 个字符。 加密算法：指定系统与 Agile Controller 服务器通信时的加密算法，可以为 3DES 或者 AES128。如不指定，默认采用 AES128 加密算法。 启用主动查询：勾选复选框，系统将主动向 Agile Controller 服务器查询用户在线信息。

3. 点击“确定”按钮，完成 Agile Controller 配置。

通过 AD Polling 实现单点登录

当域用户从 AD 服务器登录时，AD 服务器上会产生登录日志。开启 AD Polling 功能后，系统会定时查询并获取 AD 服务器上的用户登录信息，并定时探测在线用户是否下线，获取正确的认证用户信息，从而实现单点登录。

在 AD 服务器已经搭建完成的情况下，通过 AD Polling 实现单点登录，按照以下步骤进行操作：

1. 点击“对象>SSO Client>AD Polling"，进入 AD Polling 页面。

2. 点击“新建”按钮，打开<AD Polling配置>页面。

在<AD Polling配置>页面进行配置。

选项	说明
名称	输入新建的 AD Polling 的名称。范围是 1 到 31 个字符。
状态	点击“启用”按钮，开启 AD Polling 功能。启用后，系统会定时查询 AD 服务器的在线用户信息，并定时探测在线用户是否下线。初次查询时，会获取 AD 服务器之前 8 小时内的用户上线信息， 如果获取失败，系统直接获取后续上线的用户信息。
虚拟路由器	在下拉菜单中选择 AD 服务器所属的虚拟路由器。
外部服务器地址	输入域内认证 AD 服务器的地址 。此处仅支持 AD 服务器。指定认证 AD 服务器后，当域用户从该 AD 服务器登录时，AD 服务器会产生登录日志。 范围是 1 到 31 个字符。
账户	输入一个域用户的用户名，用于登录 AD 服务器。格式为 domain\username，范围是 1 到 63 个字符。 要求该用户具有读取 AD 服务器上的安全日志的权限，例如 AD 服务器上权限是 Domain Admins 的 Administrator 用户。
密钥	与域用户名对应的密码。范围是 1 到 31 个字符。
修改密钥	编辑服务器配置时，可以看到修改密钥功能。开启后，将展示密钥输入框。如需修改，输入新的密钥后保存配置即可。
AAA 服务器	在下拉列表中选择引用的 AAA 服务器。系统支持选择已配置的 Local、AD 或者 LDAP 类型的服务器。建议用户直接选择配置的认证 AD 服务器。 选择 AAA 服务器后，系统可以在引用的 AAA 服务器上查询在线用户的用户名对应的用户组和角色信息，从而实现基于用户组和角色的策略控制。

选项	说明
AD Polling 间隔	配置 AD Polling 定时探测的时间间隔。系统每隔时间间隔去 AD 服务器查询上线用户信息。取值范围为 1 到 3600 秒，默认为 2 秒。为保证获取的用户上线信息的实时性，建议配置 2 到 5 秒。
客户端探测间隔	配置客户端定时探测间隔。系统每隔时间间隔会通过 WMI 探测已上线用户是否在线，如果探测不到，则踢出用户。取值范围为 0 到 1440 分钟，默认为 0 分钟，即关闭该功能。如果对用户下线要求不高，建议配置较大探测间隔，节省系统性能。
强制超时时间	配置强制下线时间。当用户在线时长超过配置的强制超时时间后，系统会踢出用户，强制用户下线。取值范围是 0（关闭该功能）到 144000 分钟，默认为 600 分钟。

3. 点击“确定”按钮，完成 AD Polling 配置。

注意:

当系统重启或者 AD Polling 配置（除账户、密钥和强制超时时间）修改后，系统会清空已有的用户信息，并根据新配置重新获取用户信息。

要实现 AD Polling 功能，需要 AD 服务器所在 PC 和终端 PC 开启 WMI 功能。WMI 功能默认是开启的。开启 WMI 功能，进入“控制面板 > 管理工具 > 服务”，将 WMI performance adapter 状态修改为手动或自动。

要使 WMI 能够对 AD 服务器所在 PC 和终端 PC 进行探测查询，AD 服务器所在 PC 和终端 PC 必须开启 RPC 服务以及远程管理。RPC 服务和远程管理默认是开启的。开启 RPC 服务，进入“控制面板-管理工具-服务”，开启 Remote Procedure Call 和 Remote Procedure Call Locator；开启远程管理，以管理员身份运行命令提示符窗口（cmd），输入命令 netsh firewall set service RemoteAdmin。

要使 WMI 能够对 AD 服务器所在 PC 和终端 PC 进行探测查询，需要允许 WMI 功能通过 Windows 防火墙。选择“控制面板 > 系统和安全 > Windows 防火墙> 允许应用通过 Windows 防火墙”，在允许的应用和功能列表中，勾选 Windows Management Instrumentation (WMI)功能的域选项对应的复选框。

要使用下线功能，请确保 AD 服务器所在 PC 和终端 PC 的时间一致，需要开启二者 PC 的“与 Internet 时间服务器同步”功能。选择“控制面板 > 时钟、语言和区域>日期和时间”，弹出<日期和时间>对话框，点击“Internet 时间”标签页，勾选“与 Internet 时间服务器同步”。

通过 SSO Monitor 实现单点登录

SSO Monitor 单点登录可以将外部服务器上保存的用户在线状态通过 SSO Monitor 协议报文发送到防火墙，在防火墙上生成认证用户，并实时更新在线用户的用户名与 IP 绑定关系，而且支持提取报文中的用户所属用户组信息，使得用户可以免于二次登录。

StoneOS 并不限制外部服务器形式和类型，只要它能在 SSO Monitor 协议中充当 TCP 连接的服务端，向防火墙同步用户信息，即可将其视作可以对接的外部服务器，例如 AD Agent 软件。

> 注意: 在 StoneOS 5.5R10 之前的版本上，在需要使用 AD Agent 软件获取用户信息时，可以通过 SSO Monitor 对接 AD Agent 软件，也可以通过在 Active Directory 服务器页面配置 AD 服务监控功能。从 StoneOS 5.5R10 版本开始，系统不再支持配置 AD 服务监控功能。在版本升级到 StoneOS 5.5R10 后，系统中已配置的 AD 服务监控功能会自动转换成 SSO Monitor 功能对接 AD Agent 软件配置。可进入“对象 > SSO Client > SSO Monitor”页面查看配置，转换后的 SSO Monitor 名称与 AD 服务器名称相同。

通过 SSO Monitor 实现单点登录，按照以下步骤进行操作：

1. 点击“对象>SSO Client>SSO Monitor"，进入 SSO Monitor 页面。
2. 点击“新建”按钮，打开<SSO Monitor 配置>页面。

在<SSO Monitor 配置>页面进行配置。

选项	说明
名称	输入新建的 SSO Monitor 的名称。范围是 1 到 31 个字符。
状态	点击“启用”按钮，开启 SSO Monitor 功能。启用后，系统通过 SSO-Monitor 协议与外部服务器建立连接并获取用户在线状态及所属用户组信息，设备根据认证信息生成认证用户。
虚拟路由器 1	在下拉菜单中选择防火墙与外部服务器地址 1 的通信接口所属的

选项	说明
	虚拟路由器。
外部服务器地址 1	输入外部服务器的域名或 IP 地址。范围是 1 到 31 个字符。外部服务器需要支持将用户在线状态通过 SSO-Monitor 协议报文发送到防火墙。用户需配置至少一个外部服务器地址 1、2 或 3，当配置超过 1 个时，其他的地址会用于冗余备份。当某一个地址无法连接时，系统将尝试连接下一个地址。建议按照 1、2、3 的顺序配置。
虚拟路由器 2	在下拉菜单中选择防火墙与备份的外部服务器地址 2 的通信接口所属的虚拟路由器。
外部服务器地址 2	输入备份的外部服务器的地址。
虚拟路由器 3	在下拉菜单中选择防火墙与备份的外部服务器地址 3 的通信接口所属的虚拟路由器。
外部服务器地址 3	输入备份的外部服务器的地址。
端口	指定外部服务器的端口号，系统通过该端口号获取认证用户信息。默认为 6666，取值范围为 1024 到 65535。
AAA 服务器	在下拉列表中选择关联的 AAA 服务器。系统支持选择已配置的 Local、AD 或者 LDAP 类型的服务器，配置方法参见"AAA 服务器" 在第 318 页。在防火墙的认证用户架构中，所有认证用户及其用户组不能独立存在，必须关联于一个 AAA 服务器。SSO Monitor 用户是从外部服务器同步而来的。通过在防火墙上指定 AAA 服务器，可以将 SSO Monitor 用户与其关联。
组织源	选择系统查找用户所属组的方式： 消息：使用 SSO Monitor 协议报文中的用户组作为用户所属组，该用户组也将关联到所配置的 AAA 服务器上；默认的组织源为“消息”。 AAA 服务器：使用 AAA 服务器中的用户组织结构作为用户所属组，一般用于用户组织结构保存在关联的 AAA 服务器的场景。 注意： 当 SSO Monitor 对接的外部服务器是 AD Agent 时，组织源需设置为“AAA 服务器”。 在使用 AD Agent 软件获取用户信息的应用场景，如果配置了 AD 服务监控功能，那么当版本升级到 StoneOS 5.5R10 后，系统中已配置的 AD 服务监控功能会自动转换成 SSO Monitor 功能对接 AD Agent 软件配置。转换后的组

选项	说明
	织同步模式为 AAA 服务器。可进入“对象 > SSO Client > SSO Monitor”页面查看配置，转换后的 SSO Monitor 名称与 AD 服务器名称相同。
重连超时时间	设置连接超时时间。StoneOS 和外部服务器超时断开后，系统等待连接超时时间，如果超时时间内仍然连接失败，则删除在线用户。范围是 0 到 14400 秒，默认值为 300。0 表示用户认证信息永不超时。
强制超时时间	指定 SSO Monitor 强制超时时间，用于控制认证用户的在线时长。注意：当 SSO Monitor 对接的外部服务器是 AD Agent 软件时，该参数不建议与 AD Agent 软件上的用户在线时长参数同时配置。

3. 点击“确定”按钮，完成 SSO Monitor 配置。

SSO Monitor 对接 AD Agent 实现单点登录配置举例

AD Agent 软件能够将 AD 域内的用户在线状态通过 SSO Monitor 协议报文发送到防火墙，因此可以作为 SSO Monitor 单点登录功能对接的外部服务器。此处以 AD Agent 软件为例说明如何通过 SSO Monitor 与 AD Agent 对接实现单点登录。

在 Active-Directory 服务器或域内任一 PC 上安装 AD Agent 软件，当域用户从 Active-Directory 服务器登录时，AD Agent 软件会记录该用户的用户名、IP 地址、上线时间等信息，并将用户名和 IP 地址对应关系信息发送到 StoneOS，使得用户可以免于二次登录，在防火墙上生成认证用户。利用所获取的用户名和 IP 地址对应关系信息，系统还可以实现基于用户的安全统计、日志记录、上网行为审计等。

使用 SSO Monitor 对接 AD Agent 实现单点登录，按照以下步骤进行配置：

步骤一：在 PC 或服务器上安装并运行 AD Agent

AD Agent 可以安装在 AD 服务器或者域内任一 PC 上。推荐在 Windows Server 2008 /2012/2016/2019、Windows 7/10 中安装。

通信过程中默认使用的协议和端口号见下表：

通信方向	配置值
AD Agent→AD 服务器	协议：TCP 端口： StoneOS：--- AD Agent：1935、1984 AD 服务器：445

通信方向	配置值
AD Agent→StoneOS	协议：TCP 端口： StoneOS：6666 AD Agent：6666 AD 服务器：---

安装在 AD 服务器或者域内其他 PC 上，按照以下步骤操作：

1. 点击链接 http://swupdate.ctyunom:1337/sslvpn/download?os=windows-adagent 下载 AD Agent 安装程序。下载完成后，将其拷贝到域内的一台 PC 机或服务器上。
2. 双击 AD Agent 安装程序 ADAgentSetup.exe，按照安装向导提示逐步安装直至完成。
3. 使用以下两种方法启动 AD Agent 软件：

   双击桌面的 AD Agent Configuration Tool 快捷方式，系统弹出<AD Agent 设置工具>对话框。

   点击“开始菜单”中的“所有程序 > AD Agent > AD Agent Configuration Tool”，系统弹出<AD Agent 设置工具>对话框。

4. 点击<设置>标签页。

在<设置>标签页，配置基础选项。

选项	说明
端口号	输入监听端口号。AD Agent 通过该端口与 StoneOS 建立通信连接。取值范围为 1025 到 65535。系统默认为 6666。该端口号需和 SSO Monitor 单点登录中配置的端口号一致，否则无法通信。
域用户名	输入一个域用户的用户名，用于登录 AD 服务器。如果 AD Agent 运行在域内其他 PC 上，要求该用户具有较高的权限， 能够远程访问 AD 服务器上的事件日志，例如 AD 服务器上权限是 Domain Admins 的 Administrator 用户。
密码	与域用户名对应的密码。若 AD Agent 运行在 AD 服务器所在设备上，则可以不填写域用户名和密码。
服务器查询	
启用事件日志查询	选择该选项，开启日志查询功能，能够查看 AD 服务器的事件日志。默认每隔 5 秒查询一次。要实现 AD Agent 查询用户的功能，必须开启此开关。
查询间隔	设定轮询查找不同 AD 服务器的事件日志的间隔时间。取值范围为 1 到 99 秒，默认值为 5 秒。每当查找完成一个 AD 服务器，AD Agent 会将更新的用户信息发送给系统。
用户在线时长	设置用户单点登录成功后的在线时长，到期后用户将被下线。取值范围是 1 到 99 小时，默认是 8 小时。
客户端探测	
启用 WMI 探测	选中复选框，开启 WMI 协议查询。 要使 WMI 能够对终端 PC 进行探测查询，终端 PC 必须开启 RPC 服务以及远程管理。开启 RPC 服务，进入“控制面板 > 管理工具 > 服务”，开启 Remote Procedure Call 和 Remote Procedure Call Locator；开启远程管理，以管理员身份运行命令提示符窗口（cmd），输入命令 **netsh firewall set service RemoteAdmin**。 WMI 协议辅助事件日志查询，定期查找用户列表中的所有 IP。当发现终端 PC 的域用户名与已存储名称不符时，将更新为探测到的域用户名。
探测间隔	设定主动发起 WMI 探测的间隔时间。取值范围为 1 到 99 分钟，默认值是 20 分钟。

5. 在<查询到的服务器>标签页，点击“自动获取”按钮，自动搜索域内的认证 AD 服务器。也可以点击“添加”按钮，手动输入服务器 IP 地址，将其添加到服务器列表中。对于多个 AD 服务器的情况，按照列表中的顺序，由上到下进行事件日志查询。

6. 在<过滤的用户>标签页，在“过滤的用户名”文本框中输入用户名，点击“添加”按钮，该用户会显示在“过滤的用户”列表中。最多可以配置 100 个过滤用户，且不区分大小写。

7. 点击<查询到的用户>标签页，查看已经探测到的域用户名称和用户地址的对应关系。
   说明：已经添加到“过滤的用户”列表中的用户不会显示在该列表中。

8. 点击页面右上角“提交”按钮，提交所有设置并启动 AD Agent 服务。

> 注意: 提交后，AD Agent 的服务将一直在后台运行。如果您需要修改设置，仅需要在<AD Agent 设置工具>对话框中编辑后点击“提交”，AD Agent 服务立刻采用新的配置。

步骤二：在系统上配置 AD 服务器

按照以下步骤配置 AD 服务器：

1. 点击“对象 > AAA 服务器”，进入 AAA 服务器页面。
2. 根据情况选择以下两种方法之一，进入 Active Directory 服务器配置页面：

   点击页面左上角 新建 按钮，在下拉列表中选择“Active Directory 服务器”。

   选择已配置的 AD 服务器，点击页面左上角 编辑 按钮。

3. 点击“确定”按钮，完成 StoneOS 上 AD 服务器相关配置。

步骤三：启用并配置 SSO Monitor 功能。

为了实现 SSO Monitor 功能与 AD Agent 对接，按照以下步骤配置 SSO Monitor 功能：

1. 点击“对象 > SSO Client > SSO Monitor”。
2. 点击“新建”按钮，进入 SSO Monitor 配置页面。配置时，请注意以下事项：
   a. 外部服务器地址：需设置为 AD Agent 软件所在设备的 IP 地址；
   b. 端口：需和 AD Agent 软件中设置的端口号一致。
   c. AAA 服务器：需设置为步骤二中配置的 AD 服务器。
   d. 组织源：需设置为“AAA 服务器”。强制超时时间：不建议与 AD Agent 上的强制超时时间同时配置。
3. 点击“确定”按钮，完成 SSO Monitor 功能配置。

完成以上步骤后，当域用户从 Active-Directory 服务器登录时，AD Agent 会记录该用户的用户名、IP 地址、上线时间等信息发送到 StoneOS，并在防火墙上生成认证用户。

使用 TS Agent 实现单点登录

使用 TS Agent 实现单点登录，包含以下两个配置步骤：

TS Agent 服务器端配置，即在 Windows 服务器上安装并运行 Terminal Service Agent。

TS Agent 客户端配置，即在 StoneOS 上配置 TS Agent 功能。

步骤一：在 Windows 服务器上安装并运行 Terminal Service Agent

1. 点击链接 http://swupdate.ctyunom:1337/sslvpn/download?os=windows-tsagent 下载 Terminal Service Agent 安装程序。下载完成后，将其拷贝到 Windows 服务器上。

4. 点击<监听配置>标签页。

在<监听配置>标签页进行配置。

选项	说明
Agent 状态	显示 Terminal Service Agent 的运行状态。
监听地址 IPv4	指定要监听的 IPv4 地址。默认为“0.0.0.0"，即监听所有 IPv4 地址。
监听地址 IPv6	指定要监听的 IPv6 地址。默认为“::"，即监听所有 IPv6 地址。
监听端口	指定监听端口号。取值范围为 1025 到 65534，默认值是 5019。该端口号必须和 StoneOS 中设置的 TS Agent 服务器的端口号一致，否则 TS Agent 服务器端与客户端无法通信。
心跳时间间隔	指定 TS Agent 客户端向 TS Agent 服务器发送心跳的时间间隔。取值范围为 1 到 30 秒，默认值是 5 秒。
心跳超时时间	TS Agent 客户端在心跳超时时间结束前未收到 TS Agent 服务器的心跳响应，则会断开与 TS Agent 服务器的连接。取值范围为 10 到 300 秒，默认值是 60 秒。
SSL 证书	TS Agent 客户端与 TS Agent 服务器通过建立 SSL 连接同步信息。TS

选项	说明
	Agent 服务器支持内部默认 SSL 证书以及导入外部 SSL 证书。
导入外部 SSL 证书	点击该按钮，在<导入外部 SSL 证书>对话框导入新的证书。导入证书的加密标准为 PKCS12，后缀为.pfx。导入外部 SSL 证书，需要在 StoneOS 上新建 PKI 信任域，并导入对应的 CA 证书。 导入外部 SSL 证书后，需要重启 Terminal Service Agent，新的证书才能生效。重启 Terminal Service Agent，在菜单栏点击“系统>重启代理服务器"。
删除外部 SSL 证书	点击该按钮，删除外部 SSL 证书。删除后需要重启 Terminal Service Agent，内部默认证书才会生效。重启 Terminal Service Agent，在菜单栏点击“系统>重启代理服务器"。

5. 点击<访问控制配置>标签页。

在<访问控制配置>标签页进行配置。

选项	说明
开启访问控制列表	勾选复选框，检查新接入的 StoneOS IP 是否在下方的 IPv4 Address/IPv6 Address 列表中，如果不存在则拒绝接入。该功能默认关闭。
IPv4 Address	开启访问控制列表功能后，不在该列表中的 IPv4 地址会被拒绝接入。
IPv6 Address	开启访问控制列表功能后，不在该列表中的 IPv6 地址会被拒绝接入。
新增	在“新增”按钮上方的文本框中输入 IP 地址，点击该按钮，将 IP 地址添加到 IPv4 Address/IPv6 Address 列表中。
删除	在 IPv4 Address/IPv6 Address 列表中选中要删除的 IP 地址，点击该按钮，将 IP 地址从列表中删除。
修改	在 IPv4 Address/IPv6 Address 列表中选中要修改的 IP 地址，在下方文本框中修改该 IP 地址，点击该按钮，添加修改后的 IP 地址。

6. 点击<端口配置>标签页。

在<端口配置>标签页进行配置。

选项	说明
系统保留端口范围	系统保留的端口范围，从系统注册表中读取，不能修改。
系统动态分配端口范围	系统用于为用户动态分配的端口范围，从系统注册表中读取，不能修改。
用户分配端口范围	可用于分配给用户的总端口范围。取值范围为 1025 到 65534，默认值为 20000 到 39999。只能配置 1 个范围，最小范围大小为已配置的用户端口段大小，最大范围大小为 40960。
用户保留端口范围	用户自定义的预留端口范围。取值范围为 1025 到 65534，默认值为空。可配置多个范围，以英文逗号隔开，例如：2000-3000,3500,4000-4200。
用户端口段大小	每次为用户分配端口段的端口数量。取值范围为 20 到 2000，默认值为 200。
每用户最多端口段	为每位用户分配端口段的最大数。取值范围为 1 到 256，默认值为 1。
用户端口耗尽时允许系统分配端口	勾选复选框，当“用户分配端口范围”中的端口耗尽后，系统将从“系统动态分配端口范围”中为用户分配端口。 默认勾选。

7. 点击<用户信息>标签页。

在<用户信息>标签页查看用户相关信息。

选项	说明
用户信息列表	显示登录用户信息，包括 ID、UID、用户名、端口段数量及登录时间。当用户通过远程桌面登录 TS Agent 服务器时，Terminal Service Agent 检测到用户登录后，将用户信息记录在用户信息列表中。最多可以记录 2000 条用户信息。
过滤用户名	在文本框中输入用户名，点击“刷新”按钮，查找的用户信息将显示在用户信息列表中。用户名的输入区分大小写。
全局可用端口	可以为用户分配的剩余端口数量。
已分配端口范围	已经为登录用户分配的端口段范围。用户注销后，系统回收为该用户分配的所有端口段。
已分配端口合计	为登录用户分配的端口总数。
已使用 TCP/UDP/TCP6/UDP6 端口	用户已经使用的端口数量。用户的上网连接断开后，系统回收该用户已使用的端口。
可用 TCP/UDP/TCP6/UDP6 端口	用户新建连接时可用的端口数量。
自动刷新	勾选复选框，每 5 秒刷新一次端口统计信息。

8. 点击<防火墙信息>标签页。

在<防火墙信息>标签页查看 StoneOS 设备相关信息。

选项	说明
接入防火墙列表	显示当前连接到 TS Agent 服务器的 StoneOS 设备信息，包括 ID、设备 SN 号、连接状态、连接 IP、端口及连接时间。
自动刷新	勾选复选框，每 5 秒刷新一次接入的 StoneOS 设备信息。

9. 通过菜单栏进行相关功能配置及信息查看。

菜单栏选项说明。

系统	
重启代理服务器	点击该选项，重启 Terminal Service Agent。重启时，<监听配置>标签页的“Agent 状态”显示“Terminal Service Agent 停止运行；重启完成后，<监听配置>标签页的“Agent 状态”显示“Terminal Service Agent 正在运行。
信息	
打开日志信息	点击该选项，弹出<Log 信息>对话框，用户可以在该对话框进行如下操作： 在“显示信息选择”部分，勾选一个或者多个日志信息类型复选框，该类型日志信息会显示在日志信息列表中。 选中日志信息列表中的某条日志信息，该日志信息的完整信息将显示在左下角文本框中。 在“过滤”文本框中输入需要过滤的字符串，点击“刷新”按钮，包含该字符串的日志信息将显示在日志信息列表中。 在日志信息列表中勾选一条或者多条日志信息，点击“删

	除”按钮，删除日志信息。 点击“导出为文本”按钮，将日志信息导出为文本文件。 点击并拖动右下角水平滚动条，实现日志信息翻页功能。滚动条下方的文本框中显示日志信息总条数、日志信息总页数以及当前页。
日志信息使能设置	点击该选项，勾选或者取消勾选日志信息类型，系统会记录或者取消记录相应类型的日志信息。默认勾选并记录事件、告警及配置三类日志信息。
打开调试信息	点击该选项，弹出<Debug 信息>对话框，显示 SMP（Service Process Module）调试信息以及 KM（Kernel Module）调试信息记录文件。用户可以在该对话框进行如下操作： 双击 SMP 调试信息或者 KM 调试信息文件名称，打开相应的信息文件。 选中 SMP 调试信息或者 KM 调试信息文件名称，按下电脑键盘上的“Delete”键，删除文件。
SPM 调试信息级别设置	点击该选项，勾选 SMP 调试信息级别，系统会记录该级别及高于该级别的 SMP 调试信息。默认勾选级别为“事件”。用户可以在“打开调试信息”对话框中查看记录的 SMP 调试信息。“严重错误”和“错误”级别的 SMP 调试信息显示在“SPM error”里，其他级别的 SMP 调试信息保存在“SPM info”里。
KM 调试信息级别设置	点击该选项，勾选 KM 调试信息级别，系统会记录该级别及高于该级别的 KM 调试信息。默认勾选级别为“严重错误”。用户可以在“打开调试信息”对话框中查看记录的 KM 调试信息。“严重错误”和“错误”级别的 KM 调试信息显示在“KM error”里，其他级别的 KM 调试信息保存在“KM info”里。
关于	
关于	点击查看 Terminal Service Agent 的版本信息。

步骤二：在 StoneOS 上配置 TS Agent

配置 TS Agent 功能，请按照以下步骤进行操作：

1. 点击“对象>SSO Client>TS Agent"，进入 TS Agent 页面。

2. 点击“新建”按钮，打开<TS Agent 配置>页面。

在<TS Agent 配置>页面进行配置。

选项	说明
名称	指定新建的 TS Agent 的名称。范围是 1 到 31 个字符。
启用	点击“启用”按钮，开启 TS Agent 功能。
状态	启用 TS Agent 功能后，StoneOS 与 TS Agent 服务器建立 SSL 连接并获取用户及端口段信息，并实时更新在线用户的流量 IP、端口段和用户名的映射信息。
主机	指定 TS Agent 服务器的管理地址，支持 IPv4 地址、IPv6 地址以及域名。
虚拟路由器	在下拉菜单中选择 TS Agent 服务器所属的虚拟路由器。
端口	指定 TS Agent 服务器的端口号。取值范围为 1025 到 65534，默认值为 5019。该端口号必须和 Terminal Service Agent 中设置的监听端口一致，否则 TS Agent 服务器端与客户端无法通信。
AAA 服务器	在下拉菜单中选择引用的 AAA 服务器，支持选择已配置的 Local、AD 或者 LDAP 类型的服务器。选择 AAA 服务器后，系统可以在引用的 AAA 服务器上查询在线用户的用户名对应的用户组和角色信息，从而实现基于用户组和角色的策略控制。
断开超时时间	当 StoneOS 和 TS Agent 服务器的连接断开时，如果在指定的断开超时时间内仍然连接失败，则删除在线用户信息。范围是 0 到 1800 秒，默认值为 300。0 表示立即删除在线用户信息。
流量 IP	指定流量 IP 地址，即 TS Agent 服务器网络接口（网卡）的 IP 地址。支持 IPv4 地址和 IPv6 地址，最多可以指定 4 个 IP 地址。点击“新建”按钮，在文本框中输入 IP 地址。勾选 IP 列表中的 IP 地址，点击“删除”按钮，删除选中的 IP 地址。

3. 点击“确定”按钮，完成 TS Agent 配置。

完成以上两个步骤后，当用户通过远程桌面服务登录 TS Agent 服务器时，Terminal Service Agent 为用户分配端口段，并将端口段和用户信息发送给设备，设备创建基于流量 IP、端口段和用户的映射信息。

802.1x 认证

仅有部分平台支持该功能，请参阅您产品的功能列表。

802.1X 是 IEEE 为解决基于端口的接入控制（Port-Based Network Access Control）而定义的一个标准。它采用基于二层的认证方式，对局域网用户的接入的合法性进行认证。认证所使用的协议是 EAPOL（Extensible Authentication Protocol over LAN），该协议不基于网络层，而是基于二层的认证方式，也就是说，防火墙可以对基于二层安全域启用 802.1x 认证，只要指定的 MAC 地址或端口通过认证，通过该接口的所有数据均可以通过。

支持 802.1x 的认证服务器是本地认证服务器（Local）和 Radius 认证服务器，其他认证服务器（AD 或 LDAP）不支持。

配置 802.1x 认证

完整的配置 802.1x 认证功能的前提和步骤要点如下：

前期准备：开始配置 802.1x 认证之前，防火墙已经添加了有用户信息的认证服务器（本地或 Radius 认证服务器）。

配置步骤要点：

1. 创建 802.1x profile。
2. 配置允许访问的策略规则。

修改 PC 端网卡的属性：通过 802.1x 端口上网的 PC 需要在本地的网卡上开启认证（右键点击 LAN 网口，选择“属性”，在认证标签页选择“MD5-Challenge”，确定后，状态栏弹出提醒气泡，输入用户名和密码即可通过认证，实现上网。）

> 注意: 配置 PC 端的网卡时，早期的 Windows 系统默认支持 802.1x 认证方式。但 Windows 7 和 Windows 8 系统并非缺省支持，请 PC 用户搜寻解决方案，修改网卡配置。

创建 802.1x profile

1. 点击“网络 > 802.1x > 802.1x”。

2. 在页面点击“新建”，打开<802.1x 配置>页面。

3. **在<基本配置>标签页填写基本信息。**

基本信息	
802.1x 名称	指定 802.1x profile 的名称。
接口	指定 802.1X 认证的接入接口，接口应是二层接口。
AAA 服务器	指定 802.1X 认证服务器，支持本地认证服务器和 RADIUS 认证服务器。
接入模式	指定 802.1X 认证接口的接入模式。选择“MAC 模式”时，802.1X 认证的接入接口下连接的所有客户端都必须通过认证，才能访问网络资源。选择“端口模式”时，802.1X 认证的接入接口下连接的所有客户端，只要有一个客户端通过认证，即可访问网络资源。

4. **在<高级配置>标签页填写高级信息。**

高级配置	
端口授权状态	若选择“自动”，认证系统将依据 802.1X 协议认证的结果决定客户端是否可以接入网络；若选择“强制不授权”，系统认为接口始终为未授权模式，任何客户端都无法与之建立连接。
重认证周期	输入认证系统进行重认证的时间间隔。客户端认证成功并接入网络后，认证系统在该时间后对客户端进行重认证。取值范围为 0 至 65535 秒，默认值为 3600 秒。如果取值为 0，则关闭重认证功能。
静默周期	输入认证系统处于静默状态的秒数。如果认证失败，认证系统需要静默该时间段后再重新处理同一客户端的请求。取值范围为 0 至 65535 秒，默认值为 60 秒。如果取值为 0，认证系统将一直处理同一客户端的请求。

高级配置	
重传次数	认证系统向客户端发送认证请求帧并收到客户端响应的数据后，会将数据发送给认证服务器并等待认证服务器应答。如果未收到应答，则再次向客户端发送认证请求帧，直到收到认证服务器应答或达到允许的重复发送次数后放弃尝试。取值范围为 1 至 10 次，默认值为 2 次。
服务器超时	认证系统向客户端发送认证请求帧并收到客户端响应的数据后，会将数据发送给认证服务器并等待认证服务器应答。如果在指定的认证服务器应答超时时间结束时，认证系统仍未收到认证服务器的应答，则会重新发送请求帧到客户端。取值范围为 1 至 65535 秒，默认值为 30 秒。
客户端超时	当认证系统向客户端发送请求报文，请求客户端上传用户名后，客户端需要在指定时间内向认证系统发送应答报文。如果未在指定的客户端超时时间内完成发送，则认证系统将重发认证请求报文到客户端。取值范围为 1 至 65535 秒，默认值为 30 秒。

5. 点击“确定”。

802.1x 的全局配置

全局参数对所有的 802.1x profile 生效。

1. 点击“网络 > 802.1x >全局配置”。

在打开的<全局配置>页面中，设定所有 802.1x profile 都遵守的参数。

选项	说明
最大用户数	系统端口允许同时接入客户端数量最大值。
同名用户登录	点击“启用”按钮开启该项功能后，系统将允许同一账户从不同的远端登陆。 同时，若选择“无限制”，系统将不对同一用户名的登录次数做限制；若选择“允许登录数”并赋值，系统将限制最大同时登录客户端数量。 点击禁用按钮禁用该项功能后，系统将禁止同一用户在多个客户端登录。

选项	说明
	同时，若选择“踢出已登录用户”，同一用户再次登录时，系统自动断开已登录的连接；若选择“拒绝再次登录”，系统将禁止已登录用户的再次登录。
重新认证时间	配置已通过 802.1X 认证的客户端的认证超时时间。若客户端在此时间内没有回应认证系统，则需要再次申请认证。取值范围为 180 至 86400，默认值为 300，单位为秒。

2. 点击“确定”。

查看在线用户

1. 点击“网络 > 802.1x> 在线用户”。
2. 主窗口即显示在线用户；设置过滤条件后，点击“搜索”即可显示满足条件的用户。

PKI

PKI（Public Key Infrastructure）即公钥基础设施，是提供公钥加密和数字签名服务的系统，目的是为了自动管理密钥和证书，保证网上数据信息传输的机密性、真实性、完整性和不可否认性。PKI 采用证书进行公钥管理，通过第三方的可信任机构，把用户的公钥和用户的其它标识信息捆绑在一起，从而在网上验证用户的身份。一个 PKI 系统由公钥密码技术（Public Key Cryptography）、证书认证机构（CA）、注册机构（RA）、数字证书（Digital Certificate）和相应的 PKI 存储库组成。

以下介绍几个 PKI 相关的术语：

公钥密码技术：用户使用公钥密码技术产生密钥对，分别为公钥（public key）和私钥（private key），公钥向外界公开，私钥则自己保留。公钥与私钥互为补充，被一个密钥加密的数据，只可以用相匹配的另外一个密钥解密。

认证机构（CA）：是一个向个人、计算机或任何其它实体颁发证书的可信实体。CA 受理证书服务申请，根据证书管理策略验证申请方的信息，然后用其私钥对证书进行签名，并颁发该证书给申请方。

注册机构（RA）：RA 是 CA 的延伸，RA 向 CA 转发证书服务申请，也向目录服务器转发 CA 颁发的数字证书和证书撤消列表，以提供目录浏览和查询服务。

证书撤销列表（CRL）：证书具有一定的使用期限，但是由于密钥被泄露、业务终止等原因，CA 可通过撤销证书缩短证书的使用期限。一个证书一旦被撤销，证书中心就要公布 CRL 来声明该证书是无效的，并列出不能再使用的证书的序列号。

系统在以下功能模块中可以使用 PKI 认证方式：

IKE VPN：建立 IKE VPN 时，支持 PKI 认证。

HTTPS/SSH：使用 HTTPS 或者 SSH 方式访问设备时，支持 PKI 认证。

创建 PKI 密钥

1. 点击“系统 > PKI > 密钥”。
2. 点击“新建”按钮，打开<PKI 密钥配置>页面。

在该页面中配置参数。

选项	说明
标签	密钥对的名称，该名称在系统中应该是唯一的。
密钥配置方式	配置密钥的产生方式。系统可以通过生成和导入两种方式来产生密钥。
生成	
密钥对类型	密钥对的类型，包括 RSA、ECC 和 DSA。
模长	密钥对的模长，单位为比特。RSA 和 DSA 的模长可选项为 1024（系统默认值）、2048、512 和 768。
椭圆曲线组	若密钥类型为 ECC，用户需指定椭圆曲线组，包含 P-256、P-384、P-521 椭圆曲线。若未指定，系统默认为 P-256 椭圆曲线。
导入	
类型	密钥的类型，包括密钥对。 密钥对 - 若选择该选项，在密钥对类型中指定导入 RSA 或 DSA 类型的密钥到 PKI。
导入密钥	从本地导入密钥文件。

3. 点击“确定”。

创建信任域

1. 点击“系统 > PKI > 信任域”。

2. 点击“新建”，打开<信任域配置>页面。

在<信任域配置>页面填写信任域的参数。

基本	
信任域	输入信任域的名称。
证书获取方式	即 CA 中心的证书信息，根据 CA 中心的不同，可选择以下两种方式之一： 若选择外部的 CA 认证中心，选择“手动输入”。然后点击“导入 CA 证书”后面的“浏览”按钮，在打开的对话框中找到 CA 证书所在路径，点击“导入”按钮，将 CA 证书导入到系统中； 若使用当前防火墙作为 CA 认证中心，选择“自签名证书”。
密钥对	为信任域指定密钥对。
主题	
名称	指定被认证的单位名称。可选配置。
国家（地区）	指定国家（地区）名称。国家名称只能包含两个字符，如 CN。可选配置。
位置	指定所在位置。可选配置。
州/省	指定州或者省的名称。可选配置。

基本	
机构	指定机构名称。可选配置。
机构单元	指定机构单元名称。可选配置。
使用者可选名称	
IP 地址	点击“新建”按钮，指定需要添加到使用者可选名称列表里的 IP 地址。支持 IPv4 和 IPv6。
DNS 名称	点击“新建”按钮，指定需要添加到使用者可选名称列表里的 DNS 名称。取值范围是 1 到 255 个字符。

3. 点击“申请证书”链接，系统将生成一串代码。

4. 复制这串代码，发送给 CA 认证中心。

5. 取回 CA 认证中心发回的证书，点击<本地证书>处的“浏览”按钮找到将该证书的路径，然后点击“导入”按钮将该证书导入。

6. **（可选）在<证书吊销列表>页面配置与 CRL 有关的参数。**

证书吊销列表（CRL）	
检查	不检查 - 设备不检查 CRL。该选项为默认选项。 可选 - 即使 CRL 不可用，设备仍然可以接受对端的认证。

证书吊销列表（CRL）	
	强制 - 只有 CRL 可用时，才可以接收对端认证。
URL 1 URL 2 URL 3	指定获得 CRL 信息的 URL。系统最多支持 3 个 URL，最先使用 URL1，依次为 URL2、URL3。 选择“http://”，指定通过 HTTP 方式获得 CRL 信息； 选择“ldap://”，指定通过 LDAP 方式获得 CRL 信息。 如果通过 LDAP 方式获得 CRL 信息，请输入 LDAP 服务器的登录 DN（通常为 LDAP 服务器预设的具有查询权限的用户账号）和登录 DN 的密码。若不配置该选项，默认通过匿名方式获得 CRL。
自动更新	CRL 列表的自动刷新频率。
手动更新	通过手动点击“获取 CRL”的方式更新 CRL 列表。

7. 点击“确定”按钮。

导入导出信任域的信息

为简化配置，用户可以将 PKI 信任域的证书（CA 证书和本地证书）以及本地证书对应的私钥信息以 PKSC12 格式从一台设备上导出，然后再导入到另外一台设备。

导出 PKI 信任域信息，按照以下步骤进行：

1. 选择“系统 > PKI > 信任域证书”。
2. 从“信任域”下拉菜单选择要导出的信任域。
3. 选择要导出的证书类型，然后选择“导出”。

若导出的对象是加密标准，需要设定密码。

4. 点击“确定”按钮后，下载对话框将出现，选择保存路径即可下载相应信息。

将已经导出的信任域信息导入到另一台设备中，按照以下步骤操作：

1. 选择“系统 > PKI > 信任域证书”。
2. 从“信任域”下拉菜单选择要被导入的信任域。
3. 选择要导入的对象类型，然后选择“导入”。

若导入的对象是加密标准，需要输入导出时为文件设定的密码。

4. 点击“浏览”按钮后，找到文件路径，选中要导入的文件。
5. 点击“确定”按钮完成导入。

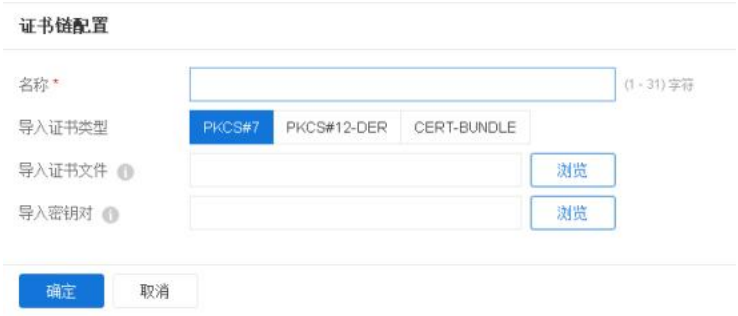
配置证书链

证书链是一个由根 CA 证书、中间证书和用户证书组成的一条完整证书信任链。只有当整个证书信任链上的各个证书都有效时，浏览器才会认定当前用户的证书是有效和受信任的。根 CA 证书是信任链的起点，是受信 CA 证书机构颁发给自己的证书。中间证书是根 CA 证书机构颁发给中间 CA 证书机构的证书，作用是保护根证书不被泄露，可以有多级。

创建证书链

创建证书链，按以下步骤操作：

1. 点击“系统 > PKI > 证书链”。
2. 点击“新建”，打开<证书链配置>页面。



在<证书链配置>页面填写相关参数。

名称	指定证书链的名称，范围是 1 到 31 个字符。
导入证书类型	指定证书链文件的格式，即 PKCS#7、PKCS#12 或 CERT-BUNDLE

	格式。CERT-BUNDLE 是 PEM 编码的证书链文件。
密码	对于 PKCS#12 格式的证书链，需要指定解密证书链文件的密码。
导入证书文件	点击“浏览”按钮，在打开的对话框中找到证书链所在路径，选择需要导入的文件。证书链中支持包含最多 6 个证书，链式必须连续，但不限制排列顺序。
导入密钥对	当证书类型为“PKCS#7”或“CERT-BUNDLE”时，可以导入最后一级证书的私钥用于加解密。点击“浏览”按钮，在打开的对话框中找到私钥所在路径，选择需要导入的文件。

3. 点击“确定”。

导出证书链

导出证书链到本地，按以下步骤操作：

1. 点击“系统 > PKI > 证书链”。
2. 在列表中选择一条证书链。
3. 点击“导出证书”按钮。如需导出 PKCS#12 格式的证书链，需输入密码。

配置证书有效性检查

默认情况下，开启证书有效期检查后，在证书到期前一周开始，系统会每天告警一次。当证书过期时，系统会记录 Critical 级别的事件日志。

配置证书有效期检查，按以下步骤操作：

1. 点击“系统 > PKI > 有效性检测”。

在<有效性检测>页面填写参数。

有效性检测	点击“开启”按钮，开启证书有效期检查。默认为开启状态。
检查间隔时间	指定证书有效期检查的间隔时间，取值范围是 1 到 100 小时，默认为 24。
告警提前时间	指定证书到期的提前告警时间，取值是 1 到 1000 小时，默认为 168。

2. 点击“确定”。

在线用户

查看认证相关在线用户，按照以下步骤进行操作：

1. 点击“网络 >Web 认证 > 在线用户”，进入在线用户主窗口。

2. 设置过滤条件后，即可显示满足条件的在线用户。

用户名：显示在线用户名称。

IP/MAC：显示在线用户的 IP 或者 MAC 地址。

接口：显示在线用户通过 Web 认证的接口。

在线时长：显示在线用户的在线时长。

认证类型：显示在线用户的认证类型。

操作：点击“踢出”强制断开该上线用户与认证系统的连接。

第 6 章 VPN

系统支持如下 VPN 功能：

IPSec VPN：IPSec 是 IETF 制定的三层隧道加密协议，它为互联网上传输的数据提供了高质量的、基于密码学的安全保证，是一种传统的实现三层 VPN 的安全技术。IPSec 通过在特定通信方之间（例如两个安全设备之间）建立“通道”，来保护通信方之间传输的用户数据，该通道通常称为 IPSec 隧道。

SSL VPN：SSL VPN 是以 HTTPS 为基础的 VPN 技术，充分利用了 SSL 协议提供的基于证书的身份认证、数据加密和消息完整性验证机制，可以为通信建立安全连接。

L2TP VPN：L2TP 是 VPDN（Virtual Private Dial-up Network，虚拟私有拨号网）隧道协议的一种。VPDN 是指利用公共网络的拨号功能接入公共网络，实现虚拟专用网，从而为企业、小型 ISP、移动办公人员等提供接入服务。即，VPDN 为远端用户与私有企业网之间提供了一种经济而有效的点到点连接方式。

VXLAN：VXLAN 是采用 MAC in UDP（User Datagram Protocol）封装方式，是 NVO3（Network Virtualization over Layer3）中的一种大二层虚拟网络扩展的隧道封装技术。VXLAN 引入了类似 VLAN ID 的用户标识，称为 VXLAN 网络标识 VNI（VXLAN Network ID），由 24 比特组成，可划分多达 16M 的 VXLAN 段，从而满足了大量的用户标识。通过 VXLAN 构建大二层网络，保证了在虚拟迁移时虚拟机的 IP 地址、MAC 地址等参数保持不变。

GRE VPN：GRE（Generic Routing Encapsulation）是通用封装路由，是定义了在任意一种网络层协议上封装任意一个其它网络层协议的协议。系统支持 GRE over IPSec 功能，实现路由协议信息的安全传输。

IPSec VPN

IPSec 是为实现 VPN 功能而使用的协议。IPSec 给出了应用于 IP 层上网络数据安全的一整套体系结构。该体系结构包括认证头协议（Authentication Header，简称为 AH）、封装安全负载协议（Encapsulating Security Payload，简称为 ESP）、密钥管理协议（Internet Key Exchange，简称为 IKE）和用于网络认证及加密的一些算法等。IPSec 规定了如何在对等体之间选择安全协议、确定安全算法和密钥交换，向上提供了访问控制、数据源认证、数据加密等网络安全服务。

IPSec VPN 基础概念

安全联盟

封装方式

协商方式

引用 IPSec VPN

安全联盟

IPSec 在两个端点之间提供安全通信，两个端点被称为 IPSec ISAKMP 网关。安全联盟（Security Association, 简称为 SA）是 IPSec 的基础，也是 IPSec 的本质。SA 是通信对等体间对某些要素的约定，例如使用哪种协议、协议的操作模式、加密算法（DES、3DES、AES-128、AES-192 和 AES-256）、特定流中保护数据的共享密钥以及 SA 的生存周期等。

安全联盟是单向的，在两个对等体之间的双向通信，最少需要两个安全联盟来分别对两个方向的数据流进行安全保护。

建立安全联盟的方式有两种，一种是手工方式（Manual），一种是 IKE 自动协商（ISAKMP）方式。

封装方式

IPSec 有如下两种工作模式：

隧道（tunnel）模式：用户的整个 IP 数据包被用来计算 AH 或 ESP 头，AH 或 ESP 头以及 ESP 加密的用户数据被封装在一个新的 IP 数据包中。通常，隧道模式应用在两台设备之间的通讯。

传输（transport）模式：只是传输层数据被用来计算 AH 或 ESP 头，AH 或 ESP 头以及 ESP 加密的用户数据被放置在原 IP 包头后面。通常，传输模式应用在两台主机之间的通讯，或一台主机和一台设备之间的通讯。

协商方式

手工方式配置比较复杂，创建安全联盟所需的全部信息都必须手工配置，而且 IPSec 的一些高级特性（例如定时更新密钥）不能被支持，但优点是可以不依赖 IKE 而单独实现 IPSec 功能。该方式适用于当与之进行通信的对等体设备数量较少的情况，或是 IP 地址相对固定的环境中。

IKE 自动协商方式相对比较简单，只需要配置好 IKE 协商安全策略的信息，由 IKE 自动协商来创建和维护安全联盟。该方式适用于中、大型的动态网络环境中。该方式建立 SA 的过程分两个阶段。第一阶段，协商创建一个通信信道（ISAKMP SA），并对该信道进行认证，为双方进一步的 IKE 通信提供机密性、数据完整性以及数据源认证服务；第二阶段，使用已建立的 ISAKMP SA 建立 IPSec SA。分两个阶段来完成这些服务有助于提高密钥交换的速度。

引用 IPSec VPN

设备通过“基于策略的 VPN”和“基于路由的 VPN”两种方式把配置好的 VPN 隧道调用到设备上，实现流量的加密解密安全传输。

基于策略的 VPN：将配置成功的 VPN 隧道名称引用到策略规则中，使符合条件的流量通过指定的 VPN 隧道进行传输。

基于路由的 VPN：将配置成功的 VPN 隧道与隧道接口绑定；配置静态路由时，将隧道接口指定为下一跳路由。

配置 IPSec VPN

IKE 自动协商方式相对比较简单，只需要配置好 IKE 协商安全策略的信息，由 IKE 自动协商来创建和维护安全联盟。该方式适用于中、大型的动态网络环境中。该方式建立 SA 的过程分两个阶段。第一阶段，协商创建一个通信信道（ISAKMP SA），并对该信道进行认证，为双方进一步的 IKE 通信提供机密性、数据完整性以及数据源认证服务；第二阶段，使用已建立的 ISAKMP SA 建立 IPSec SA。分两个阶段来完成这些服务有助于提高密钥交换的速度。

配置 IIPSec VPN，需要确认第一阶段提议，第二阶段提议，以及 VPN 对端信息。确认这三部分内容后，可继续完成 IKE VPN 的配置。

配置 IPSec VPN

配置 IPSec VPN，按照以下步骤进行操作：

1. 点击“网络 > VPN > IPSec VPN”，进入 IPSec VPN 页面。
2. 选择<IPSec VPN>页签。
3. 点击“新建”按钮，打开<IPSec VPN 配置>页面。

在<对端>区域，填写如下信息。

对端	
对端选项	在“对端选项”下拉列表中选择 ISAKMP 网关的名称。配置对端，请参考配置 VPN 对端。

在<隧道>区域，填写基本信息。

隧道	
名称	指定“隧道”的名称。
封装模式	指定封装模式。当前版本支持隧道模式和传输模式。默认为隧道模式。
P2 提议	为隧道指定 P2 提议。配置 P2 提议，请参考配置 P2 提议。
代理 ID	当用户需对 IPSec VPN 流量进行分流与限流时，需指定 IKE 第二阶段 ID（即 IKE 第二阶段 ID，后文简称为第二阶段 ID）。第二阶段 ID 由本地网段、远程网段和服务类型组成。配置时，需在本端和对端设备上对应配置，然后本端和对端将进行协商，最终创建 1 条 IKE IPSec 隧道。用户可指定 1 个或多个第二阶段 ID，即创建 1 条或多条 IKE IPSec 隧道。系统将根据每个隧道的第二阶段 ID 对隧道中的流量进行分流与限流。为隧道指定第二阶段 ID，可采用如下两种方法： 自动 - 自动指定第二阶段 ID。 手工 - 手动指定第二阶段 ID。需配置选项包括： 本地 IP/掩码：指定第二阶段的本地网段的 IP/掩码。 远程 IP/掩码：指定第二阶段的远程网段的 IP/掩码。 服务：指定第二阶段 IKE IPSec 隧道可传输的流量的服务或协议名称。 若不需对 IPSec VPN 流量分流与限流，可不配置。 **注意**：默认情况下，IKE IPSec 隧道本端与对端的第二阶段 ID 需对应配置，若没有对应配置，将导致协商失败。若响应方设备开启接受对端任意 ID 时，也可实现协商成功。

在<高级配置>标签页，填写高级配置选项。

选项	说明
Commit 位	点击“启用”按钮使相应方设置 Commit 位，用来防止丢包和出现时间差。但是，设置 Commit 位可能会使响

选项	说明
	应速度变慢。
自动连接	配置自动连接功能。默认情况下，该功能是关闭的，点击“启用”按钮开启该功能。设备提供两种触发建立 SA 的方式：自动方式和流量触发方式。自动方式时，设备每 60 秒检查一次 SA 的状态，如果 SA 未建立则自动发起协商请求；流量触发方式时，当有数据流量需要通过隧道进行传输时，该隧道才发起协商请求。默认情况下，系统使用流量触发方式。
接受对端任意代理 ID	该功能需在 IKE 隧道协商的响应方设备上进行配置。开启后，响应方设备将接受对端（协商发起方）配置第二阶段 ID，同时设置自身的第二阶段 ID 与对端保持对应，从而使 IKE 隧道两端能协商成功。常用于响应方设备对发起方的第二阶段 ID 无法感知或者不感兴趣的场景。 **注意**：当响应方设备上配置了多个第二阶段 ID（即配置多条 IKE 隧道时），需关闭该功能，否则只能协商出一条隧道。
启用空闲时间	配置空闲时间功能。默认情况下，该功能是关闭的，点击“启用”按钮开启该功能。启用该功能后，隧道在无流量状态下能够保持连接状态的最长时间，超出空闲时间后，SA 将会被清除。
DF 位	指定是否允许转发设备将包进行分片处理。选项包括： 拷贝 – 直接从发包端拷贝 IP 包的 DF 选项。该选项为系统默认选项。 清除 – 允许转发设备对包做分片处理。 设置 – 不允许转发设备对包做分片处理。
防重放	防重放指防止恶意用户通过重复发送捕获到的数据包所进行的攻击，即接收方会拒绝旧的或重复的数据包。默认情况下，防重放功能是关闭的。 关闭- 关闭防重放功能。该选项为系统的默认值。 32 – 指定防重放的窗口为 32。 64 – 指定防重放的窗口为 64。 128 – 指定防重放的窗口为 128。

选项	说明
	256 – 指定防重放的窗口为 256。 512 – 指定防重放的窗口为 512。
UDP 校验和	启用 UDP 报文校验和功能，即 UDP 报文头部经过更改后设备会重新计算 UDP 校验和。默认情况下，该功能是关闭的。
检查 ID	默认情况下，该功能是关闭的。检查 ID 功能用于对 IPSec VPN 流量进行分流与限流。开启前，需确保已配置第二阶段 ID 且 IKE 隧道第二阶段协商成功。开启后，设备将根据第二阶段 ID 的配置，对进出 IKE 隧道的流量进行过滤，然后分流、限流；未匹配到第二阶段 ID 的流量将被丢弃。具体如下： 分流：设备根据第二阶段 ID 的配置，在 IKE 隧道入口对进入 IKE 隧道的流量进行分流。如果流量的源 IP 地址、目的 IP 地址、以及流量的类型(service)匹配某一个第二阶段 ID 的配置，则该流量进入相应的 IKE 隧道进行封装发送。如果没有匹配的第二阶段 ID，则该流量被丢弃。 限流：设备根据第二阶段 ID 的配置，在 IKE 隧道出口对解封装后的流量进行限流。如果解封装后流量的源 IP 地址、目的 IP 地址、以及流量的类型(service)匹配某一个第二阶段 ID 的配置，则该流量被接收设备继续处理；如果流量无法匹配任何一个第二阶段 ID 的配置，则该流量被丢弃。
通知 VPN 隧道状态	点击“启用”按钮启用 VPN 隧道状态通知功能。启用该功能后，如果是基于路由的 VPN，系统一旦监测到中断的 VPN 隧道，会立即通知路由模块中断的 VPN 隧道信息并进行隧道路由的更新处理；如果是基于策略的 VPN，系统一旦监测到中断的 VPN 隧道，会立即通知策略模块中断的 VPN 隧道信息并进行隧道策略的更新处理。
VPN 隧道监测	点击“启用”按钮启用 VPN 隧道监测功能。设备能够监测指定的 VPN 隧道是否连通，并且能够实现两条或者多条 VPN 隧道的备份或者分流。该功能仅对基于路由的 VPN 以及基于策略的 VPN 均有效。选项包括：

选项	说明
	检测间隔时间 – 指定发送 Ping 监测报文的时间间隔。 连续失败次数 – 指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，即目标隧道中断。 源地址 – 指定发送 Ping 监测报文的源 IP 地址。 目的地址 – 指定监测目标的 IP 地址。
智能选路	在“智能选路”下拉列表里选择智能选路规则。智能选路与 VPN 隧道监测不能同时配置。 **说明：**仅当对端选项类型为静态 IP 时支持配置该功能。
DNS1	为 PnPVPN 服务器指定下发给用户端的主 DNS 服务器 IP 地址。
DNS2	为 PnPVPN 服务器指定下发给用户端的备 DNS 服务器 IP 地址。
DNS3	为 PnPVPN 服务器指定下发给用户端的备 DNS 服务器 IP 地址。
DNS4	为 PnPVPN 服务器指定下发给用户端的备 DNS 服务器 IP 地址。
WINS1	为 PnPVPN 服务器指定下发给用户端的主 WINS 服务器 IP 地址。
WINS2	为 PnPVPN 服务器指定下发给用户端的备 WINS 服务器 IP 地址。
隧道路由	该选项需要在 IKE VPN 配置完成后进行修改。点击“编辑”按钮，弹出<隧道路由配置>对话框。在该对话框添加一条或多条隧道路由。系统允许最多设置 128 条隧道路由。
描述	在文本框中为所创建隧道输入描述内容。

4. 点击“确定”完成配置。

配置 VPN 对端

配置 VPN 对端参数，按照以下步骤进行操作：

1. 点击“网络 > VPN > IPSec VPN”，进入 IPSec VPN 页面。
2. 选择<IPSec VPN>页签。

3. 点击“新建“按钮，打开<IPSec VPN>页面。

4. 点击“对端选项”下拉列表，点击 ⊕ 按钮，打开<VPN 对端配置>页面。

在<VPN 对端配置>页面，填写相关配置信息。

基本配置	
名称	指定 ISAKMP 网关的名称。
接口	指定 ISAKMP 网关的绑定接口。
接口类型	指定接口类型，包括 IPv4 和 IPv6。
协议标准	指定协商协议标准为国际标准（IKEv1）。 **注意：**如指定版本号 v1.0 或 v1.1，进行协商的两端设备必须是相同的版本号才能协商成功，否则协商失败。
接口类型	指定接口类型，包括 IPV4 和 IPV6。该选项仅适用于 IPv6 版本。
协商模式	指定 IKE 协商模式。IKE 的协商模式有两种：主模式和野蛮模式。主模式为系统的默认模式。IKE 野蛮模式不提供身份保护，以下情况只能用野蛮模式：中心设备的 IP 地址为固定分配的地址，而客户端设备的 IP 地址为动态获取的地址。
类型	指定对端 IP 地址的类型。 如果对端 IP 地址类型为静态，选择“静态 IP”按钮，并在之后的<对端 IP 地址>本框中输入对端的 IP 地址； 如果对端 IP 地址类型为用户组，选择“用户组”按钮，并从之后的<选择 AAA 服务器>下拉菜单中选中需要的认证服务器名称。 如果对端 IP 地址为动态 IP 地址，选择“动态 IP”按钮。
本地 ID	指定本地 ID。系统支持 FQDN、U-FQDN、ASD1-DN（仅用于使用证书的情况）、KEY-ID 和 IP 类型的 ID。选中所需 ID 类型的单选按钮，然后在其后的<本地 ID 值>或<本地 IP>文本框中输入 ID 或 IP 的具体内容。
对端 ID	指定对端 ID。系统支持 FQDN、U-FQDN、ASD1-DN（仅用于使用证书的情况）、KEY-ID 和 IP 类型的 ID。选中所需 ID 类型的单选按钮，然后在其后的<对端 ID 值>或<本地 IP>文本框中输入 ID 或 IP 的具体内容，如果使用 Radius 服务器进行认证，则需要选中<通配符>复选框。
提议 1	为 ISAKMP 网关指定 P1 提议。用户最多可指定 4 个提议。 配置 P1 提议，请参考配置 P1 提议。
提议 2	为 ISAKMP 网关指定 P1 提议。用户最多可指定 4 个提议。
提议 3	为 ISAKMP 网关指定 P1 提议。用户最多可指定 4 个提议。
提议 4	为 ISAKMP 网关指定 P1 提议。用户最多可指定 4 个提议。

基本配置	
预共享密钥	如果使用预共享密钥认证方式，通过该选项指定预共享密钥。
修改预共享密钥	编辑 VPN 对端配置时，可以看到预共享密钥功能。开启后，将展示预共享密钥输入框。如需修改，输入新的预共享密钥后保存配置即可。
签名信任域	如果使用 DSA Signature 或 RSA Signature 方式，通过该选项指定信任域。
高级配置	
连接类型	指定 ISAKMP 网关的连接类型。选择合适的类型即可。 双向 – 指定该 ISAKMP 网关既是发起端也是响应端。该选项为系统的默认选项。 发起者 – 指定该 ISAKMP 网关仅是发起端。 响应者 – 指定该 ISAKMP 网关仅是响应端。
NAT 穿越	在 IPSec 或者 IKE 组建的 VPN 隧道中，若存在 NAT 网关设备，且 NAT 网关设备对 VPN 数据进行了 NAT 转换，则必须开启 IPSec 或者 IKE 的 NAT 穿越功能。默认情况下，NAT 穿越功能是关闭的。
接受对端任意 ID	使所创建的 ISAKMP 网关接受任意的对端 ID，不对对端进行 ID 检查。
产生路由	配置自动生成路由功能。默认情况下，该功能是关闭的。该功能允许设备自动添加从中心设备到分支机构的路由条目，从而避免了手工配置路由所带来的问题。
对端存活检测	配置 DPD（安全隧道对端状态探测）功能。默认情况下，该功能是关闭的，点击“启用”按钮开启该功能。该功能开启后，系统将按照指定的时间间隔，周期性的向对端发送请求报文，对 ISAKMP 网关是否存在进行检测。 DPD 模式 – 指定 DPD 探测模式，分为 periodic 和 on-demand 两种： **periodic：**启用该模式后，系统将按照指定的时间间隔，持续向对端发送 DPD 探测报文。若在一个 DPD 周期内，未收到对端响应报文，则判定对端失活。计算方式：DPD 探测周期=DPD 间隔时间 *DPD 重试次数。 **on-demand：**启用该模式后，系统将根据设备是否收到 IPSec 流量来判断是否向对端发送 DPD 探测报文。若设备未收到 IPSec 流量，不发送 DPD 探测报文；若设备收到 IPSec 流量，需转发 IPSec 流量时，系统查询当前距离上一次收到对端 IPSec 报文的时间

基本配置	
	间隔，并与 DPD 探测周期进行比较：①当前距离上一次收到对端 IPSec 报文的时间间隔小于 DPD 探测周期，说明在 DPD 探测周期内收到了对端报文，表明对端 ISAKMP 网关存在，设备不发送 DPD 探测报文；②当前距离上一次收到对端 IPSec 报文的时间间隔超过 DPD 探测周期，则表明不确定对端 ISAKMP 网关是否存在，设备发送 DPD 探测报文对对端 ISAKMP 进行检测。若在一个 DPD 探测周期内均未收到对端报文，则判定对端 ISAKMP 网关已经失效。系统将老化第一阶段和第二阶段的 SA 信息，重新发起新的 IPSec 协商。 DPD 间隔 – 指定向对端发送 DPD 查询请求的时间间隔，单位为秒。取值范围是 1 到 10 秒，默认值是 10 秒。 DPD 重试 – 指定向对端发送 DPD 查询请求的次数。向对端发送查询请求后，如果本端在指定的时间间隔内收不到对端的报文，系统会在再次发送查询请求，如此反复，直到完成该参数指定的次数。在指定次数查询完成后如果仍然收不到对端的报文，则判断对端 ISAKMP 网关已经死掉。查询请求的次数范围是 1 到 10 次，默认是 3 次。
描述	在文本框中为所创建 ISAKMP 网关输入描述内容。
XAUTH 服务器	选中“启用”按钮，在设备上启用 XAUTH 服务器。启用 XAUTH 服务器后，设备可以结合已配置的认证服务器（RADIUS 和本地 AAA 服务器）对试图访问 IPSec VPN 网络的用户进行身份认证。用户可以在“地址池”下拉菜单中选择系统中已配置的 IPSec-XAUTH 地址池，该选项为可选配置。当客户端成功连接 XAUTH 服务端后，设备会从地址池里取出一个 IP 地址与其它相关参数（如 DNS 服务器地址与 WINS 服务器地址等）一起分配给用户。有关 IPSec-XAUTH 地址池的更多信息，请参考“VPN > IPSec VPN > 配置 IPSec-XAUTH 地址池”。

5. 点击“确定”完成配置。

编辑 VPN 对端

编辑 VPN 对端，按照以下步骤进行操作：

1. 点击“网络 > VPN > IPSec VPN”，进入 IPSec VPN 页面。
2. 选择<IPSec VPN>页签。
3. 点击“新建“按钮，打开<IPSec VPN>界面。

4. 点击“对端选项”下拉列表，点击 按钮，打开<VPN 对端配置>界面对 VPN 对端进行编辑。

删除 VPN 对端

删除 VPN 对端，按照以下步骤进行操作：

1. 点击“网络 > VPN > IPSec VPN”，进入 IPSec VPN 页面。
2. 选择<IPSec VPN>页签。
3. 点击“新建“按钮，打开<IPSec VPN>界面。
4. 点击“对端选项”下拉列表，点击 按钮，删除 IPSec VPN。

复制 VPN 对端

用户可以通过复制已配置的 VPN 对端更方便快捷地创建与之类似的 VPN 对端。

复制 VPN 对端，按照以下步骤进行操作：

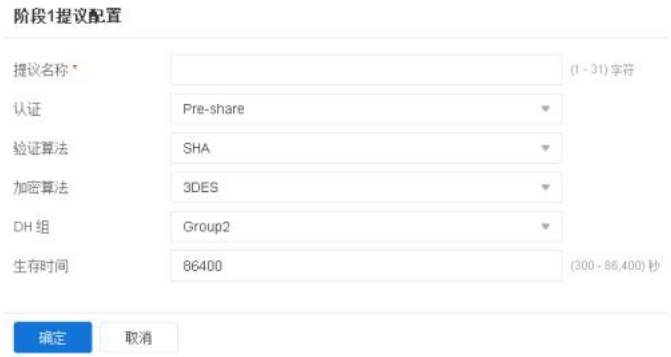
1. 点击“网络 > VPN > IPSec VPN”，进入 IPSec VPN 页面。
2. 选择<IPSec VPN>页签。
3. 点击“新建“按钮，打开<IPSec VPN>界面。
4. 点击“对端选项”下拉列表，点击 按钮，打开<VPN 对端配置>界面。可以根据需要编辑配置项，其中名称不能与已有的相同。
5. 点击“确定”创建一个新的 VPN 对端。

配置 P1 提议

P1 提议用来协商 IKE SA。配置 P1 协议，按照以下步骤进行操作：

1. 在<IPSec VPN>页签，点击“对端选项”下拉列表，点击 按钮，打开<VPN 对端配置>页面。

2. 点击“提议 1”下拉列表，点击 ⊕ 按钮，打开<阶段 1 提议配置>页面。



在<阶段 1 提议配置>页面，填写相关配置信息。

选项	说明
提议名称	指定 P1 提议的名称。
认证	指定 IKE 身份认证的方式。身份认证用来确认通信双方的身份。方式有三种：预共享密钥认证（Pre-Shared key）、RSA Signature 和 DSA Signature，系统默认为预共享密钥认证。对于预共享密钥认证方式，认证字用来作为一个输入产生密钥，认证字不同是不可能在双方产生相同的密钥的。
验证算法	为 P1 提议指定验证算法。在下拉列表中选择所需的验证算法。 MD5 – 指定使用 MD5 验证算法。摘要为 128 比特。 SHA – 指定使用 SHA 验证算法。摘要为 160 比特。该算法为系统的默认算法。 SHA-256 – 指定使用 SHA-256 验证算法。摘要为 256 比特。 SHA-384 – 指定使用 SHA-384 验证算法。摘要为 384 比特。 SHA-512 – 指定使用 SHA-512 验证算法。摘要为 512 比特。
加密算法	P1 提议指定加密算法。 3DES - 指定使用 3DES 加密方法。密钥长度为 192 比特。该方法为系统默认方法。 DES – 指定使用 DES 加密方法。密钥长度为 64 比特。 AES – 指定使用 AES 加密方法。密钥长度为 128 比特。 AES-192 – 指定使用 192bit AES 加密方法。密钥长度为 192 比特。

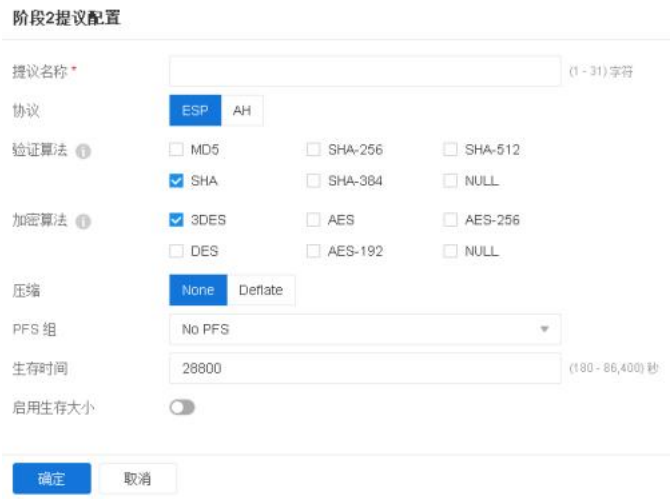
选项	说明
	AES-256 – 指定使用 256bit AES 加密方法。密钥长度为 256 比特。
DH 组	P1 提议选择 DH 组。 Group1 – 选择 DH 组 1。密钥的长度为 768 比特（MODP Group）。 Group2 – 选择 DH 组 2。密钥的长度为 1024 比特（MODP Group）。2 为系统默认值。 Group5 – 选择 DH 组 5。密钥的长度为 1536 比特（MODP Group）。 Group14 – 选择 DH 组 14。密钥的长度为 2048 比特（MODP Group）。 Group15 – 选择 DH 组 15。密钥的长度为 3072 比特（MODP Group）。 Group16 - 选择 DH 组 16。密钥的长度为 4096 比特（MODP Group）。 Group18 - 选择 DH 组 18。密钥的长度为 8192 比特（MODP Group）。 Group19 - 选择 DH 组 19。密钥的长度为 256 比特（ECP Group）。 Group20 - 选择 DH 组 20。密钥的长度为 384 比特（ECP Group）。 Group21 - 选择 DH 组 21。密钥的长度为 521 比特（ECP Group）。 Group24 - 选择 DH 组 24。密钥的长度为 2048 比特（MODP Group with 256-bit Prime Order Subgroup）。
生存时间	指定 SA 第一阶段的生命周期长度，单位为秒。默认 86400 秒。范围是 300 到 86400 秒。在文本框中输入生命周期的时间值。如果 SA 生命期时间到，要向对方发送第一阶段 SA 删除消息，通知对方第一阶段 SA 已经过期。之后需要重新进行 SA 协商。

3. 点击“确定”完成配置。

配置 P2 提议

P2 提议用来协商 IPSec SA。配置 P2 协议，按照以下步骤进行操作：

1. 点击“网络 > VPN > IPSec VPN”，进入 IPSec VPN 页面。
2. 选择<IPSec VPN>页签。
3. 点击“新建“按钮，打开<IPSec VPN>页面。
4. 点击“P2 提议”下拉列表，点击 ⊕ 按钮，打开<阶段 2 提议配置>页面。



在<阶段 2 提议配置>页面，填写相关配置信息。

选项	说明
提议名称	指定或者显示 P2 提议的名称。
协议	为 P2 提议指定协议类型。可以为 ESP 或者 AH，系统默认为 ESP。
验证算法	为 P2 提议指定第一验证算法。用户最多可以为 P2 提议指定 3 种验证算法。 MD5 – 指定使用 MD5 验证算法。摘要为 128 比特。 SHA – 指定使用 SHA 验证算法。摘要为 160 比特。该算法为系统的默认算法。 SHA-256 – 指定使用 SHA-256 验证算法。摘要为 256 比特。 SHA-384 – 指定使用 SHA-384 验证算法。摘要为 384 比特。 SHA-512 – 指定使用 SHA-512 验证算法。摘要为 512 比特。

选项	说明
	NULL - 不使用验证功能。
加密算法	为 P2 提议指定第一加密算法。用户最多可以为 P2 提议指定 4 种加密算法。 3DES - 指定使用 3DES 加密方法。密钥长度为 192 比特。该方法为系统默认方法。 DES – 指定使用 DES 加密方法。密钥长度为 64 比特。 AES – 指定使用 AES 加密方法。密钥长度为 128 比特。 AES-192 – 指定使用 192bit AES 加密方法。密钥长度为 192 比特。 AES-256 – 指定使用 256bit AES 加密方法。密钥长度为 256 比特。 AES-GCM-128 – 指定使用 128bit AES-GCM 加密方法。密钥长度为 128 比特。 AES-GCM-192 – 指定使用 192bit AES-GCM 加密方法。密钥长度为 192 比特。 AES-GCM-256 – 指定使用 256bit AES-GCM 加密方法。密钥长度为 256 比特。 NULL - 不使用加密功能。
压缩	为 P2 提议指定压缩算法。默认情况下，无任何压缩算法。
PFS 组	为 P2 提议配置 PFS 功能。PFS 功能是由 DH 算法做保障的。 Group1 – 选择 DH 组 1。密钥的长度为 768 比特（MODP Group）。 Group2 – 选择 DH 组 2。密钥的长度为 1024 比特（MODP Group）。2 为系统默认值。 Group5 – 选择 DH 组 5。密钥的长度为 1536 比特（MODP Group）。 Group14 – 选择 DH 组 14。密钥的长度为 2048 比特（MODP Group）。 Group15 – 选择 DH 组 15。密钥的长度为 3072 比特（MODP Group）。 Group16 - 选择 DH 组 16。密钥的长度为 4096 比特（MODP

选项	说明
	Group）。 Group18 - 选择 DH 组 18。密钥的长度为 8192 比特（MODP Group）。 Group19 - 选择 DH 组 19。密钥的长度为 256 比特（ECP Group）。 Group20 - 选择 DH 组 20。密钥的长度为 384 比特（ECP Group）。 Group21 - 选择 DH 组 21。密钥的长度为 521 比特（ECP Group）。 Group24 - 选择 DH 组 24。密钥的长度为 2048 比特（MODP Group with 256-bit Prime Order Subgroup）。 No PFS - 不使用 PFS 功能。该值为系统的默认值。
生存时间	设备有两种衡量生命周期的方法，分别是按时间和按流量。该选项指定 P2 提议时间类型生命周期的时间长度，单位为秒。默认 28800 秒。范围是 180 到 86400 秒。
启用生存大小	点击“启用”按钮，开启 P2 提议流量类型生命周期。默认情况下，该功能是关闭的。 生存大小 - 指定流量类型生命周期的流量值，单位为 KB，默认 1800KB。范围是 1800 到 4194303KB。在文本框中输入周期流量值。

5. 点击“确定”完成配置。

配置智能选路

当分支机构与数据中心之间有多条可通信的链路时，可以在分支机构防火墙上配置智能选路功能实现多条 IPSec 链路之间的动态切换。智能选路功能按照链路排列顺序选择链路协商 IPSec 隧道，每条链路都有唯一一个 ID 号，排列顺序可以在“网络 > VPN > IPSec VPN”页面查看和调整。在初始状态下，系统会选择排序在最顶部的链路协商 IPSec 隧道，在 IPSec 隧道建立后，系统会发送探测报文探测当前隧道的链路质量。当链路丢包率或时延高于配置的阈值时，按照链路排序切换到下一条链路重新建立 IPSec 隧道。

配置智能选路，按照以下步骤进行操作：

1. 点击“网络 > VPN > IPSec VPN”，进入 IPSec VPN 页面。
2. 选择<IPSec VPN>页签。
3. 点击“新建“按钮，打开<IPSec VPN>页面。

4. 点击“智能选路”下拉列表，点击“+”按钮，打开<智能选路配置>页面。

在<智能选路配置>区域，填写如下信息。

智能选路配置	
名称	指定智能选路规则的名称，取值是 1 到 31 个字符。
协商链路	点击“新建”按钮，选择链路本端接口并设置链路对端接口的 IP 地址，可以一次创建一条链路。点击“批量新建”按钮，在<批量新建链路>对话框可以一次添加多条链路。一个智能选路规则里可以配置最多 3 个本端接口和 10 个对端 IP，共 30 条链路。协商链路支持 IPv4 和 IPv6，一个智能选路规则里不能同时配置 IPv4 和 IPv6 链路。新建链路会按照配置顺序由上到下排列。
链路探测	点击“开启”按钮启用智能链路探测和切换功能，默认为开启。
源地址	指定链路探测报文的源 IP 地址，不指定时使用 IPSec 隧道本端接口的 IP 地址作为探测报文的源 IP 地址。默认为空。
目的地址	指定链路探测报文的目的 IP 地址，不指定时使用 IPSec 隧道对端接口的 IP 地址作为探测报文的目的 IP 地址。默认为空。
探测间隔	指定发送探测报文的时间间隔，取值范围是 1 到 5 秒，默认值为 3。
探测报文总数	指定一个探测周期内发送的探测报文总数。取值范围是 1 到 30，默认值为 10。
链路质量参数	选择链路质量参数，并配置相应的阈值。当完成一个周期的探测后，系统会将计算出的链路时延和丢包率和链路质量阈值进行比较，当时延或丢包率的任意一项高于配置的阈值时，就会触发链路的切换。链路时延阈值的取值范围是 100 到 3000 毫秒，建议值为 500。链路丢包率阈值的取值范围是 1 到 100，单位为百分比，建议值是 30。
循环切换次数	指定链路循环切换次数阈值，取值范围是 0 到 5，默认值是 5。0 表示不限制循环切换次数。所有链路依次完成一轮切换即为循环切换一次。当循环切换次数超出配置的阈值后，系统会停止链路探测和切换，并切换到质量最优的链路上。
切换静默时间	指定链路循环切换次数超出阈值时的静默时间。在链路循环切换的次数超出阈值时，系统会停止链路探测和切换，默认的静默时间是 600 秒。在静默时间到期后，系统会重新开始探测当前处于 Active 状态的链路质量。取值范围是 600 到 1800 秒。

管理 IPsec 链路，请按照以下步骤操作：

1. 点击“网络 > VPN > IPSec VPN”，进入 IPSec VPN 页面。

2. 选择<IPSec VPN>页签。

3. 展开选定的 IPSec VPN 条目，可以看到所有已配置的 IPSec 链路，以及当前处于 Active 状态的链路和各个链路的时延、丢包率统计值。

4. 在“操作”栏，点击向上箭头、向下箭头可以调整链路的排序。点击“激活”可以激活指定的链路立刻协商 IPSec 隧道。

编辑 IPSec VPN

编辑 IPSec VPN，按照以下步骤进行操作：

1. 点击“网络 > VPN > IPSec VPN”，进入 IPSec VPN 页面。

2. 选择<IPSec VPN>页签，勾选 IPSec VPN 列表需要编辑的 IPSec VPN 条目的复选框，点击列表上方的“编辑”按钮，打开<IPSec VPN 配置>界面对 IPSec VPN 进行编辑。

删除 IPSec VPN

删除 IPSec VPN，按照以下步骤进行操作：

1. 点击“网络 > VPN > IPSec VPN”，进入 IPSec VPN 页面。

2. 选择<IPSec VPN>页签，勾选 IPSec VPN 列表需要删除的一条或者多条 IPSec VPN 的复选框，点击列表上方的“删除”按钮，删除 IPSec VPN。

当需要删除的 IPSec VPN 存在隧道接口、安全策略、GRE VPN 或 L2VPN 关联项时，需要先解绑/删除关联项才能删除 IPSec VPN。用户可以去对应的各个模块解绑/删除关联项，也可以在<IPSec VPN>页面直接解绑/删除：

1. 选择需要删除的 IPSec VPN 后，点击“删除”按钮。

2. 系统弹出提示，询问是否解绑/删除 IPSec VPN 的所有关联项，点击“确定”直接解绑/删除所有关联项和选择的 IPSec VPN；点击“取消”，返回<IPSec VPN>页面；点击“查看详情”，系统将弹出<关联项>页面。

3. 在<关联项>页面，点击“对象”栏里安全策略 ID、隧道接口名称、GRE VPN 名称或 L2TP VPN 名称，可以查看各个关联项的具体配置信息；点击“操作”栏“解绑”或“删除”按钮，可以分别解绑/删除各个关联项。

注意:

当选中的 IPSec VPN 存在关联项时，不支持批量删除 IPSec VPN。

删除存在关联项的 IPSec VPN 时，支持一次解绑/删除最多 5000 条关联项。如果关联项超过 5000 条，需再次执行该手工密钥 VPN 的删除操作。

启用或禁用 IPSec VPN

启用或者禁用 IPSec VPN，按照以下步骤进行操作：

1. 点击“网络 > VPN > IPSec VPN”，进入 IPSec VPN 页面。
2. 选择<IPSec VPN>页签，勾选 IPSec VPN 列表中一条或者多条 IPSec VPN 条目的复选框，点击列表上方的“启用”或者“禁用”按钮，启用或者禁用 IPSec VPN。启用后，该 IPSec VPN 条目在 IPSec VPN 列表中的“状态”显示为 。

复制 IPSec VPN

用户可以通过复制已配置的 IPSec VPN 更方便快捷地创建与之类似的 IPSec VPN。

复制 IPSec VPN，按照以下步骤进行操作：

1. 点击“网络 > VPN > IPSec VPN"，进入 IPSec VPN 页面。
2. 选择<IPSec VPN>页签。
3. 选择一条 VPN 条目，点击“复制”按钮，打开<IPSec VPN 配置>界面。可以根据需要编辑配置项，其中名称不能与已有的相同。
4. 点击“确定”创建一条新的 IPSec VPN。

查看 IPSec VPN 条目

查看指定过滤条件下的 IPSec VPN 条目，按照以下步骤进行操作：

1. 点击“网络 > VPN > IPSec VPN"，进入 IPSec VPN 页面。
2. 选择<IPSec VPN>页签。
3. 在工具栏上方的“名称”、“对端名称”文本框中输入 IPSec VPN 条目的名称或对端名称，查看指定条件下的 IPSec VPN 条目。
4. 点击“关联项”栏数值，查看 IPSec VPN 条目的关联项详情。

配置手工密钥 VPN

使用手工密钥 VPN 完成 IPSec SA 的手动协商。配置手工密钥 VPN, 按照以下步骤进行操作：

1. 点击“网络 > VPN > IPSec VPN”，进入 IPSec VPN 页面。

2. 选择<手工密钥 VPN 配置>页签，点击“新建”按钮，打开<手工密钥 VPN 配置>页面。

在<手工密钥 VPN 配置>页面，填写相关配置信息。

基本配置	
隧道名称	指定或者显示所创建手工密钥 VPN 的名称。
封装模式	指定 IPSec 协议的封装模式。选中需要的模式：隧道模式或传输模式。隧道模式为系统默认模式。
对端 IP 地址	指定对端的 IP 地址。
本地 SPI	在文本框中输入本端的 SPI 值。SPI 是为唯一标识 SA 而生成的一个 32 比特的数值，它在 AH 和 ESP 头中传输。SPI 的作用是查找对应的 VPN 隧道进行解密。
远程 SPI	在文本框中输入对端的 SPI 值。 **注意：**在为系统配置安全联盟时，必须分别设置进和出两个方向的安全联盟的参数。并且在隧道的两端设置的安全联盟参数必须完全匹配。本端入方向安全联盟的 SPI 必须和对端出方向安全联盟的 SPI 一样；本端的出方向安全联盟的 SPI 必须和对端入方向安全联盟的 SPI 一样。
接口	为所创建手工密钥 VPN 指定出接口。从下拉菜单中选中需要的接口，点击“确认”。
接口类型	指定接口类型，包括 IPv4 和 IPv6。该选项仅适用于 IPv6 版本。
协议	指定 IPSec 协议类型。ESP 协议为系统默认协议类型。

基本配置	
加密算法	指定加密算法。3DES 为系统默认算法。
入方向加密密钥	指定进方向加密密钥。用户需要为安全隧道两端均配置协议的加密密钥，且本端进方向加密密钥必须与对端出方向的加密密钥相同，而本端出方向的加密密钥必须与对端进方向的加密密钥相同。
修改入方向加密密钥	编辑配置时，可以看到修改入方向加密密钥功能。开启后，将展示密钥输入框。如需修改，输入新的密钥后保存配置即可。
出方向加密密钥	指定出方向加密密钥。
修改出方向加密密钥	编辑配置时，可以看到修改出方向加密密钥功能。开启后，将展示密钥输入框。如需修改，输入新的密钥后保存配置即可。
验证算法	指定验证算法。SHA-1 为系统默认验证算法。
入方向验证密钥	指定进方向验证密钥。用户需要为安全隧道两端均配置协议的验证密钥，且本端进方向验证密钥必须与对端出方向的验证密钥相同，而本端出方向的验证密钥必须与对端进方向的验证密钥相同。
修改入方向验证密钥	编辑配置时，可以看到修改入方向验证密钥功能。开启后，将展示密钥输入框。如需修改，输入新的密钥后保存配置即可。
出方向验证密钥	指定出方向验证密钥。
修改出方向验证密钥	编辑配置时，可以看到修改出方向验证密钥功能。开启后，将展示密钥输入框。如需修改，输入新的密钥后保存配置即可。
压缩	指定压缩算法。默认情况下，无任何压缩算法。
描述	在文本框中为所创建手工密钥 VPN 输入描述内容。

3. 点击“确定”完成配置。

删除手工密钥 VPN

删除手工密钥 VPN，按照以下步骤进行操作：

1. 点击“网络 > VPN > IPSec VPN”，进入 IPSec VPN 页面。
2. 选择<手工密钥 VPN 配置>页签，勾选一条或者多条手工密钥 VPN 的复选框，点击列表上方的“删除”按钮，删除手工密钥 VPN。

当需要删除的手工密钥 VPN 存在隧道接口、安全策略、GRE VPN 或 L2VPN 关联项时，需要先解绑/删除关联项才能删除 VPN。用户可以去对应的各个模块解绑/删除关联项，也可以在<手工密钥 VPN 配置>页面直接解绑/删除：

1. 选择需要删除的手工密钥 VPN 后，点击“删除”按钮。
2. 系统弹出提示，询问是否解绑/删除手工密钥 VPN 的所有关联项，点击“确定”将解绑/删除所有关联项和选择的手工密钥 VPN；点击“取消”，返回<手工密钥 VPN 配置>页面；点击“查看详情”，系统将弹出<关联项>页面。

3. 在<关联项>页面，点击“对象”栏里的安全策略 ID、隧道接口名称、GRE VPN 名称或 L2TP VPN 名称，可以查看各个关联项的具体配置信息；点击“操作”栏“解绑”或“删除”按钮，可以分别解绑/删除各个关联项。

注意:

当选中的手工密钥 VPN 存在关联项时，不支持批量删除手工密钥 VPN。

删除存在关联项的手工密钥 VPN 时，支持一次解绑/删除最多 5000 条关联项。如果关联项超过 5000 条，需再次执行该手工密钥 VPN 的删除操作。

查看手工密钥 VPN

查看指定过滤条件下的手工密钥 VPN 条目，按照以下步骤进行操作：

1. 点击“网络 > VPN > IPSec VPN"，进入 IPSec VPN 页面。
2. 选择<手工密钥 VPN 配置>页签。
3. 在“名称”文本框中输入手工密钥 VPN 的名称，查看指定条件下的手工密钥 VPN 条目。
4. 点击“关联项”栏数值，查看手工密钥 VPN 条目的关联项详情。

查看 IPSec VPN 监控信息

IPSec VPN 监控主要通过 ISAKMP SA 列表、IPSec SA 列表和拨号用户列表分别列出 IPSec VPN 第 1 阶段 SA 协商结果、第 2 阶段 SA 协商结果和拨号端用户的统计信息。

查看 VPN 监控结果，请按照以下步骤进行操作：

1. 点击“网络 > VPN > IPSec VPN”，进入 IPSec VPN 页面。
2. 在页面右上方点击“ “IPSec VPN 监控”。用户可在<ISAKMP SA>，<IPSec SA>及<拨号用户>三个页面查看 IPSec VPN 监控信息。在<ISAKMP SA>页面，用户可以在“对端名称”下拉菜单中指定对端名称，按照对端名称过滤监控信息；在<IPSec SA>页面，用户可以在“VPN 名称”下拉菜单中指定 VPN 名称，按照 VPN 名称过滤监控信息。

各监控页面具体选项说明如下：

ISAKMP SA 列表

选项	说明
对端名称	显示对端名称，即 ISAKMP 网关的名称。
Cookie	显示协商建立的 Cookies，用于匹配第一阶段 SA。
状态	显示第一阶段 SA 的状态。

选项	说明
对端	显示对端 IP 地址。
端口	显示建立第一阶段 SA 使用的端口号。500 表示第一阶段 SA 建立过程中未检测到 NAT 转换，4500 表示检测到了 NAT 转换。
算法	显示第一阶段 SA 协商时使用的算法，包括认证方式、加密算法和验证算法。
生存时间	显示第一阶段 SA 的生存时间，单位是秒。

IPSec SA 列表

选项	说明
ID	显示系统为所创建的隧道自动分配的编号。
VPN 名称	显示 VPN 的名称。
方向	显示 VPN 的方向。
对端	显示对端 IP 地址。
端口	显示第二阶段 SA 协商使用的端口号。
算法	显示隧道使用的算法。包括协议类型、加密算法、验证算法和压缩算法。
SPI	显示本地 SPI 和对端 SPI。inbound 方向对应本地 SPI，outbound 方向对应对端 SPI。
CPI	显示第二阶段 SA 协商使用的压缩参数索引。
时间生存期	显示第二阶段 SA 的生存期，以秒为单位进行度量，即经过 X 秒后第二阶段 SA 将重新协商密钥。
流量生存期	显示第二阶段 SA 的生存期，以 KB 为单位进行度量，即经过 X 字节的流量后第二阶段 SA 将重新协商密钥。
状态	显示第二阶段 SA 的状态。
流量统计	显示隧道的收发流量累计值。
保护网段	显示隧道保护的网段。
持续时间（秒）	显示第二阶段 SA 最近一次协商成功到当前时间为止经历的时长，以秒为单位进行度量。
发送/接收速率（KB/s)	显示隧道发送/接收报文的实时速率，outbound 方向对应发送速率，inbound 方向对应接收速率。以 KB/s 为单位进行度量。
最近一次建立时间	显示第二阶段 SA 最近一次协商成功的时间。
最近一次断开时间	显示第二阶段 SA 最近一次断开的时间。
断开原因	显示第二阶段 SA 最近一次断开的原因。断开原因包括: 收到对端断开请求：a disconnection request is received from

选项	说明
	the peer 空闲时间超时：an idle connection timeout occurred 配置变更：configuration changed 用户执行 clear：VPN is manually cleared DPD 超时：a DPD timeout occurred VPN track 失败：VPN track failed SPI 不一致：an SPI inconsistency error occurred 生存时间超时：a lifetime timeout occurred
当日断开次数	显示从当日 0 点到当前时间为止，第二阶段 SA 断开的次数。最多统计从当日 0 点到次日 0 点之间的断开次数，次日 0 点之后已统计的次数清 0。

拨号用户列表

选项	说明
用户	显示用户 IKE ID。
IP	显示相应的 IP 地址。
加密包数	显示通过隧道传输的加密包数。
加密字节数	显示通过隧道传输的加密字节数。
解密包数	显示通过隧道传输的解密包数。
解密字节数	显示通过隧道传输的解密字节数

配置 PnPVPN

IPSec VPN 配置复杂，维护成本高，对网管人员技术要求高，针对该问题，为企业用户提供了一种简单易用的 VPN 技术——PnPVPN，即即插即用 VPN。PnPVPN 由两部分组成，分别是 PnPVPN Server 和 PnPVPN Client，各自功能描述如下：

PnPVPN Server：通常放置于企业总部，由总部 IT 工程师负责维护，客户端的大多数配置由服务器下发。PnPVPN Server 通常由设备充当，一台设备可充当多个 PnPVPN Server。

PnPVPN Client：通常放置于企业分支机构（如办事处），可由总部工程师远程维护，只需要做简单配置（如客户端 ID、密码和服务器端 IP 地址），和 Server 端协商成功后即可从 Server 端获取配置信息（如 DNS、WINS、DHCP 地址池等）。

设备既可以充当 PnPVPN Server，又可以充当 PnPVPN Client。当充当 Server 时，不同平台支持的 VPN 实例数和每个实例所支持的客户端数有所不同。

PnPVPN 工作流程

PnPVPN 的工作流程如下：

1. 客户端发起连接请求，并传送自己的 ID 以及密码到服务器端。
2. 服务器端收到请求后，验证客户端传送的 ID 和密码，验证通过即下发预配置的 DHCP 地址池、DHCP 掩码、DHCP 网关、WINS、DNS 和隧道路由等信息到客户端。
3. 客户端把收到的信息下发到相应的功能模块。
4. 客户端 PC 自动获取 IP 地址、IP 地址掩码和网关地址等网络参数，并正常接入 VPN 网络。

PnPVPN 链路冗余

PnPVPN 服务器端支持一个 PnPVPN 客户端拨入两条 VPN 链路并自动生成到客户端的路由、为客户端配置 VPN 监控。服务器端需要配置两个 ISAKMP 网关和两个隧道接口，两个 VPN 隧道分别引用不同的 ISAKMP 网关，并绑定到两个不同的隧道接口。

客户端支持通过 VPN 双链路拨入服务器端、VPN 监控和冗余选路。PnP 客户端的两个 VPN 隧道在和服务器端协商时，会根据服务器端的隧道路由配置分别生成不同优先级的路由， 优先级高的隧道作为主链路，优先级低的隧道作为备份链路，从而实现冗余选路。主 VPN 隧道会首先处于 active 状态，如果客户端监测到该主隧道中断，客户端设备会通过备份隧道重新传输数据；当监测到主隧道恢复正常后，客户端设备会重新启用主隧道传输数据。

配置 PnPVPN

配置 PnPVPN，按照以下步骤进行操作：

1. 点击“网络 > VPN > IPSec VPN”，进入 IPSec VPN 页面。
2. 选择<IKE VPN 配置>页签，在右上方的“相关配置”下拉列表中选择“PnPVPN 客户端”，打开<PnPVPN 配置>页面。

在<PnPVPN 配置>页面，填写相关配置信息。

选项	说明
服务器地址 1	指定服务器端 IP 地址。 PnPVPN 客户端支持多链路拨入服务器端。该选项为必选项。
服务器地址 2	指定服务器端 IP 地址。 服务器地址 1 和服务器地址 2 可以相同，也可以不同。该选项为可选项。
ID	指定服务器端分配给用户端的 IKE ID。
密码	指定服务器端分配给用户端的密码。
确认密码	再次输入密码以确认。
修改密码	编辑 PnPVPN 配置时，可以看到修改密码功能。开启后，将展示密码输入框。如需修改，输入新的密码后保存配置即可。
自动保存	选中“启用”复选框，系统自动保存连接建立后 PnPVPN 服务器端下发给客户端的 DHCP 和 WINS 信息。
VPN 出接口 1	VPN 出接口 1 是接入 Internet 的接口，从下拉菜单中选择需要的接口名称。该选项为必选项。
VPN 出接口 2	VPN 出接口 2 是接入 Internet 的接口，从下拉菜单中选择需要的接口名称。出接口 1 和出接口 2 可以相同，也可以不同。该选项为可选项。
VPN 入接口	VPN 入接口是内部 PC 或应用服务器在 PnPVPN 客户端上的接入口。

3. 点击“确定”完成配置。

配置 IPSec-XAUTH 地址池

XAUTH 通过地址池给用户分配 IP 地址。当客户端连接 XAUTH 服务端成功后，设备会从地址池里取出一个 IP 地址与其它相关参数（如 DNS 服务器地址与 WINS 服务器地址等）一起分配给用户。

XAUTH 服务器通过创建和执行 IP 地址绑定规则来满足客户端的固定 IP 地址需求。IP 地址绑定规则包括 IP 用户绑定规则和 IP 角色绑定规则。IP 用户绑定规则将客户端用户与已配置地址池中的某个固定 IP 地址绑定，当客户端连接成功后，设备端会将绑定的 IP 地址分配给客户端；IP 角色绑定规则是将角色与已配置地址池中的某一 IP 地址范围绑定，当此客户端连接成功后，设备端会从绑定的地址范围中取出一个 IP 地址分配给客户端。

当 XAUTH 通过地址池给客户端分配 IP 地址时，系统会按照一定的顺序对客户端的 IP 地址绑定规则进行检查，决定如何为客户端分配 IP 地址：

1. 检查是否已为客户端用户配置 IP 用户绑定规则，如果是，则将绑定的 IP 地址分配给客户端；否则，需要进一步检查。注意，如果此 IP 用户绑定规则中的 IP 地址已被占用，则该用户无法登录。

2. 检查是否已为客户端用户配置 IP 角色绑定规则，如果是，则从绑定的地址范围中取出一个 IP 地址分配给客户端；否则，该用户无法登录。

> 注意: IP 用户绑定规则中的 IP 地址和 IP 角色绑定规则中的 IP 地址不能重叠。

配置 IPSec-XAUTH 地址池，按照以下步骤进行操作：

1. 点击“网络 > VPN > IPSec VPN”，进入 IPSec VPN 页面。
2. 选择<IKE VPN 配置>页签，在右上方的“相关配置”下拉列表中选择“IPSec-XAUTH 地址池”，打开<地址池>页面。
3. 点击“新建”，打开<地址池配置>页面。

基本配置.

选项	说明
地址池名称	指定地址池名称。
起始 IP	指定地址池的起始 IP 地址。
终止 IP	指定地址池的终止 IP 地址。
保留起始 IP	指定保留地址池的起始 IP 地址。
保留终止 IP	指定保留地址池的终止 IP 地址。
子网掩码	指定上述 IP 地址的网络掩码。

选项	说明
DNS1	指定地址池的 DNS 服务器 IP 地址。此项为可选项，即地址池可以不指定 DNS 服务器。用户最多可以为每个地址池指定 2 个 DNS 服务器。
DNS2	指定地址池的 DNS 服务器 IP 地址。此项为可选项，即地址池可以不指定 DNS 服务器。用户最多可以为每个地址池指定 2 个 DNS 服务器。
WINS1	指定地址池的 WINS 服务器 IP 地址。此项为可选项，即地址池可以不指定 WINS 服务器。用户最多可以为每个地址池指定 2 个 WINS 服务器。
WINS2	指定地址池的 WINS 服务器 IP 地址。此项为可选项，即地址池可以不指定 WINS 服务器。用户最多可以为每个地址池指定 2 个 WINS 服务器。

配置 IP 用户绑定信息。

选项	说明
新建	将用户与 IP 地址的绑定条目添加到列表中。
用户	输入用户名称。
IP	输入 IP 地址。

配置 IP 角色绑定信息。

选项	说明
新建	将角色与 IP 地址的绑定条目添加到列表中。
角色	输入用户名称。
起始 IP	输入起始 IP 地址。
终止 IP	输入终止 IP 地址。
上移/下移/移到最前/移到最后	点击“上移/下移/移到最前/移到最后”等按钮移动已有的角色-IP 地址绑定规则从而改变规则的排列顺序。对于绑定到多个角色且多个角色有相应的角色-IP 地址绑定规则的用户，系统会对角色-IP 地址绑定规则进行顺序查找，然后按照查找到的相匹配的第一条规则为用户分配地址。

4. 点击“确定”完成配置。

SSL VPN

为解决远程用户安全访问私网数据的问题，设备提供基于 SSL 的远程登录解决方案。SSL VPN 功能可以通过简单易用的方法实现信息的远程连通。

设备的 SSL VPN 功能包含设备端和客户端两部分。配置了 SSL VPN 功能的设备作为设备端，具有以下功能：

接受客户端连接；

为客户端分配 IP 地址、DNS 服务器地址和 WINS 服务器地址；

进行客户端用户的认证与授权；

进行客户端主机的安全检测；

解密来自客户端的加密报文并转发。

不同型号的设备默认情况下支持的同时在线最大 VPN 客户端数不同，如果想增加支持的客户端数，请向代理商购买相应的许可证。

SSL VPN 客户端成功连接设备端后，用户就可以通过 SSL VPN 功能安全的传输数据信息。SSL VPN 客户端分为以下版本： Windows、Android、、iOS、、macOS

配置 SSL VPN

配置 SSL VPN 功能，按照以下步骤进行操作：

1. 点击“网络 > VPN > SSL VPN”，进入 SSL VPN 页面。
2. 点击 SSL VPN 列表左上角的“新建”，打开<SSL VPN 配置>页面。

点击“名称/接入用户”，填写相关信息。

选项	说明
SSL VPN 名称	输入此 SSL VPN 实例的名称。取值范围为 1 到 31 个字符。
类型	指定 SSL VPN 实例的服务类型，可选择 IPv4 或 IPv6。IPv6 选项仅当该版本为 IPv6 版本时可配。
接入用户（最多 10 条）	
AAA 服务器	在下拉菜单中选择需要的服务器名称。
域名	输入服务器对应的域名。
用户域名验证	启用用户域名验证后，将对用户名及对应的域名进行验证。

点击“接入接口/隧道接口”，填写相关配置信息。

选项	说明
出接口	指定客户端所访问的设备端接口。点击“+”按钮，在下拉菜单中选择需要的设备端接口。最多可添加 8 个接口。
服务端口	指定客户端所访问的设备端 SSL VPN 服务端口号。
隧道接口	在下拉菜单中选择系统中已配置的隧道接口；或者，选中下拉菜单中的“新建”选项，在弹出的<隧道接口>对话框中新建隧道接口；还可以在下拉菜单中选中系统中已配置的隧道接口，然后点击“编辑”按钮，在弹出的<隧道接口>对话框中编辑该隧道接口。
地址池	指定 SSL VPN 的接入地址池。在下拉菜单中选择系统中已配置的地址池；或者，选中下拉菜单中的“新建”选项，在弹出的<接入地址池配置>对话框中新建地址池；还可以在下拉菜单中选中系统中已配置的地址池，然后点击“编辑”按钮，在弹出的<接入地址池配置>对话框中编辑该地址池。配置地址池，请参阅“配置地址池”。 当配置 IPv6 类型的 SSL VPN 时，该选项指定 IPv6 SSL VPN 地址池。

点击“隧道路由配置”，指定通过 SSL VPN 隧道能到达的网段或域名。

隧道路由	
SSL VPN 客户端接收到指定网段后，生成到达指定网段的路由条目。	
新建	点击“新建”按钮，配置隧道路由条目的相关信息并添加到列表中
IP	输入目的 IP 地址。
子网掩码	输入目的 IP 地址的网络掩码。
度量值	输入路由的度量值。
删除	点击此按钮删除选中的隧道路由。
启用域名下发功能	
点击“启用”按钮，系统下发指定的域名。SSL VPN 客户端接收到指定域名后，根据域名解析结果，生成到达域名所在地址的路由条目。	
设置路由上限	指定客户端可以根据域名解析后生成的最大路由条目数。取值范围是 1 到 10000。
新建	点击“新建”按钮，配置域名并添加到列表中。系统支持最多 64 个域名。
域名	指定域名。每次可添加一个。每个域名的字符串长度不得超过 63 个字符。域名末尾不能为“.”，不支持通配符，且不支持过于宽泛的 URL，比如：“.com”、“com”。
删除	点击此按钮删除选中的域名。

点击“绑定资源”，配置用户组/角色和资源的绑定关系。

绑定资源	
新建	点击“新建”按钮，将创建好的资源与用户组/角色进行绑定。
条目名称	指定创建好的资源名称。范围是 1 到 63 个字符。
类型	在下拉菜单中指定绑定类型，可以为用户组或者角色
用户组/角色	在下拉菜单中指定与上述资源名称相绑定的用户组/角色。点击  按钮，可新建用户组/角色。 在“AAA 服务器”下拉菜单中，选择用户组所在的 AAA 服务器。目前仅支持本地认证服务器和 RADIUS 认证服务器。 **说明：** 一个用户组/角色可以绑定多个资源，一个资源也可以绑定多个用户组/角色。 一个 SSL VPN 实例中最多可以配置 256 个绑定条目。
AAA 服务器	在下拉菜单中，选择用户组所在的 AAA 服务器。目前仅支持本地认证服务器和 RADIUS 认证服务器。
删除	点击此按钮，可以删除选中的绑定条目。

3. 用户可对 SSL VPN 功能进行高级配置。点击当前对话框左下角的“高级配置”按钮，对 SSL VPN 功能进行高级配置。

点击“参数配置”，填写相关配置信息。

安全套件	
SSL 版本	指定 SSL 协议类型。默认为 TLSv1.2。<any>表示 TLSv1、TLSv1.1、TLSv1.2 协议中的任何一种。 如果设备端指定的 SSL 协议类型为 tlsv1.2 或者 any，在 SSL VPN 客户端进行数字证书认证前，需要用户将要导入到浏览器中的软证书或者 USB Key 中的.pfx 格式证书进行处理，使得证书能够支持 tlsv1.2 协议，以便用户在使用“用户名/密码+数字证书”或者“数字证书”认证方式进行认证时，能够连接成功。处理证书前，请先准备一台安装了 OpenSSL1.0.1 版本及以上的 PC（Windows 或 Linux 系统均可）。以文件名称为 oldcert.pfx 的证书为例，处理步骤如下： 1. 在 OpenSSL 软件界面中，输入以下命令将.pfx 格式的证书转换为.pem 格式的证书。 **openssl pkcs12 –in oldcert.pfx –out cert.pem** 2. 继续输入下面的命令将.pem 格式的证书转换为支持 tlsv1.2 的.pfx 格式证书。 **openssl pkcs12 –export –in cert.pem –out newcert.pfx –CSP**

	“Microsoft Enhanced RSA and AES Cryptographic Provider” 3. 将新生成的.pfx 格式证书导入到浏览器或者 USB Key。 上述操作完成后，请使用 1.4.6.1239 及以上版本的 SSL VPN 客户端进行登录。
信任域	指定 PKI 信任域。当选用国密 SSL 标准，此处指定的 PKI 信任域需要包含用于国密 SSL 协商的 SM2 签名证书及其私钥。
加密信任域	当选用国密 SSL 标准，此项配置为必选项，此处指定的加密 PKI 信任域需要包含用于国密 SSL 协商的 SM2 加密证书及其私钥。
加密算法	为 SSL VPN 隧道指定加密算法。<NULL>表示不使用加密功能。当使用国密 GMSSLv1.0 协议时，加密算法建议优先选择 SM4。默认值为 AES。
Hash 算法	为 SSL VPN 隧道指定验证算法。<NULL>表示不使用验证功能。当使用国密 GMSSLv1.0 协议时，hash 算法建议优先选择 SM3。默认值为 MD5。
压缩算法	为 SSL VPN 隧道指定压缩算法。默认无任何压缩算法。
客户端连接	
允许浏览器下载客户端	浏览器下载功能指通过浏览器 Web 页面的方式下载 SSL VPN 客户端，默认情况下，该功能为开启状态。 说明：通过浏览器下载 SSL VPN 客户端的方法为： "https://IP-Address:Port-Number" ，其中 "IP-Address" 为“接入接口”处配置的出接口 IP 地址，"Port-Number" 为“接入接口”处配置的服务端口号。
空闲时间	空闲时间指客户端与设备端在无流量状态下能够保持连接状态的最长时间，超出空闲时间后，设备端将断开与客户端的连接。单位为分钟，取值范围为 1 到 1500，默认值为 30。
允许同名登录	设备允许同一个用户在多个地点同时登录认证。选中“启用”开启该功能。
同名登录数	输入允许同名登录的个数，取值范围为 0 到 99999999，其中 0 表示不限制个数。
高级参数	
防重放	防重放功能是指防止恶意用户通过重复发送捕获到的数据包所进行的攻击，即接收方会拒绝旧的或重复的数据包。默认值为 32。
DF 位	DF 位：指定是否允许转发数据包的设备对数据包进行分片。包括： 设置 - 不允许转发设备对数据包分片。 拷贝 - 直接从发包端拷贝 IP 包的 DF 选项。该选项为系统默认选项。 清除 - 允许转发设备对包做分片处理。

数据端口（UDP）	SSL VPN 连接建立后数据通讯的 UDP 端口号。取值范围为 1 到 65535。
数据端口（TCP）	SSL VPN 连接建立后数据通讯的 TCP 端口号。取值范围为 1 到 65535。

点击“客户端”，填写相关配置信息。

客户端配置	
修改密码 URL	配置 URL 地址，用户可以从客户端跳转到指定 URL 页面修改密码，取值范围 0-255 字符。
忘记密码 URL	配置 URL 地址，用户可以从客户端跳转到指定 URL 页面重新设置密码，取值范围 0-255 字符。
重新定向 URL	重定向 URL：URL 重定向功能是指在 SSL VPN 设备端配置重定向的 URL，客户端认证成功后将自动跳转到指定 URL 的页面。在文本框中输入重定向的 URL 字符串，取值范围为 0 到 255 字符。系统支持 HTTP（http://）和 HTTPS（https://）两种类型的 URL。根据重定向页面类型的不同，系统支持内容符合下列格式的 URL 输入，以 HTTP 类型 URL 为例： UTF-8 编码格式的页面 - 输入“URL”+“username=$USER&password=$PWD”。比如，http://www.abc.com/oa/login.do?usernam-e=$GBUSER&password=$PWD GB2312 编码格式的页面 - 输入“URL”+“username=$GBUSER&password=$PWD”。比如，http://www.abc.com/oa/login.do?usernam-e=$GBUSER&password=$PWD 其它页面 - 直接输入 URL。比如，http://www.abc.com
标题	指定重定向 URL 的描述，范围为 0 到 31 字符。该名称会在客户端菜单项中显示。
断开时清除隐私数据	启用该功能后，系统会在客户端断开时清除相关的隐私数据。
客户端证书认证	
证书认证	点击此按钮开启客户端证书认证功能。该功能支持“用户名/密码 + 数字证书”和“只用数字证书”两种认证方式。数字证书可以是软证书或 USB Key 证书。选中所需认证方式单选按钮。 当认证方式为“只用数字证书”时： 系统可以根据数字证书中的证书名称（证书 CN 字段）或者组织机构（证书 OU 字段）为认证成功的用户映射相应的角

客户端配置	
	色。 系统不支持允许本地用户修改密码功能。 系统不支持配置短信口令认证功能。 如果使用 USB-Key 证书的用户移除了 UKey，客户端不会自动重连。
USB KEY 下载网址	当使用 USB Key 证书认证功能时，用户可以通过该地址，下载 UKey 对应的驱动程序。取值范围为 0 到 63 个字符。
信任域 主题名字检查 CN 匹配 OU 匹配	信任域和主题名字检查功能配置方法如下： 1. 在“信任域”下拉菜单中选中用户 CA（Certification Authority）证书所在的 PKI 信任域。客户端所提交的证书匹配到其中任意一个信任域的 CA 证书，都会认证成功。 2. 如需要，选中“主题名字检查”对应的<启用>复选框，启用主题名字检查功能。启用后，当用户通过数字证书认证功能登录时，设备端会检查客户端证书的主题名称（subject commonName）是否和登录用户的用户名一致。用户可另外指定是否匹配 CN 字段和 OU 字段。 3. 点击“添加”按钮，添加已配置的信任域和主题名字检查条目，被添加的信任域和主题名字检查条目将显示在下方的列表中。 4. 如需要，按照步骤 1 至 3 添加其它信任域和主题名字检查条目。如需要删除信任域和主题名字检查条目，从列表中选中需要删除的信任域和主题名字检查条目复选框，点击“删除”按钮。

点击“二次认证”，填写相关配置信息。

选项	说明
二次认证	点击“启用”按钮，当 SSL VPN 用户使用用户名/密码或用户名/密码+数字证书方式登录时，收到登录请求的设备通过短信口令、令牌口令或者邮件口令的方式进行二次认证，用户输入收到的认证码后，才可以通过认证，进而访问内网资源。
类型	指定二次认证的类型，包括“短信口令认证”、“令牌口令认证”和“邮件口令认证”。 选择“短信口令认证”时，点击“短信猫”或“短信网关”单选按钮，指定认证方式并根据需要在下方配置选项中进行相关配置。 选择“令牌口令认证”时，根据需要输入提示信息，取值

选项	说明
	范围为 0 到 255 个字符。 选择“邮件口令认证”时，根据需要在下方配置选项中进行相关配置。
短信口令认证	
短信认证类型	指定短信口令认证的类型，包括“短信猫”和“短信网关”。
短信网关名称	在下拉菜单选择已创建的短信网关名称。
短信认证码有效时长	输入或者选择短信认证码有效时间。取值范围是 1 到 10 分钟。默认值为 10。如果用户在有效时间内没有输入短信认证码也没有重新申请认证码，SSL VPN 设备端将自动断开连接。
发送方名称	指定短信发送方名称以显示在短信内容中。取值范围是 0 至 63 个字符。 注意: 由于 UMS 企业信息平台限制，当使用短信网关认证时，发送方名称将会显示在 UMS 企业信息平台注册的名称。
发送方自动添加尖括号	当短信网关名称指定为 SGIP 或 UMS 协议的服务商名称时，系统支持为发送方名称自动添加尖括号。点击“启用”按钮，当用户配置了发送方名称且使用默认短信模板时，验证短信中的发送方名称将自动添加尖括号。默认为启用状态。
认证码长度	指定短信认证码的长度。取值范围为 4 至 8。默认为 8。
短信模板	指定认证码短信的验证内容，内容必须包含“$VRFYCODE”（用于获取认证码）。可以包含“$USERNAME”和“$EXPIRATION”（“$USERNAME”用于获取用户名；“$EXPIRATION”用于获取认证码有效期）。短信模板长度的取值范围为 9 至 500 个字符。若未配置短信模板，将使用默认短信模板，默认短信模板的内容为“Your *num* sms authing message is *vrfycode*”(*num* 为认证次数，*vrfycode* 为认证码。) **说明：** 配置短信模板后，“发送方名称自动添加尖括号”功能将不再生效。如需要，用户可以在配置短信模板时，直接在短信模板内容末尾处手动添加带尖括号的发送方名称。 仅 ACC、XUANWU、CAS 和 HTTP(S)协议的短信网关支持配置短信模板。
签名	当短信网关名称指定为阿里云服务商名称时，用户需要输入阿里云短信服务中申请的短信签名，以显示在短信内容中。取值范围是 1 到 63 字符。该参数需与在阿里云短信服务中申请的签名保持一致。
模板 CODE	当短信网关名称指定为阿里云服务商名称时，用户需要输入阿里云短信服务中申请的短信内容模板对应的 CODE（代码）。取值范围

选项	说明
	为 1 至 30 个字符。该参数需与在阿里云短信服务中申请的模板 CODE 保持一致。
邮件口令认证	
邮件服务器	指定邮件服务器，该服务器上配有用于发送认证码的邮箱地址，且为系统中已配置的邮件服务器。取值范围为 1 至 31 个字符。
邮件认证码有效时间	指定邮件认证码的有效时间。取值范围为 1 至 10 分钟。默认为 10 分钟。每个邮件认证码都有一个有效时间，如果用户在有效时间内没有输入认证码也没有重新申请认证码，SSL VPN 设备端将自动断开连接。
发送方名称	指定认证码的发送方名称以显示在邮件内容中。取值范围为 0 至 63 个字符。为防止认证码邮件被认定为垃圾邮件，建议用户进行认证码邮件发送方名称的配置。
认证码长度	指定邮件认证码长度。取值范围为 4 至 8。默认为 8。
邮件验证内容	指定认证码邮件的验证内容，内容必须包含“$USERNAME”和“$VRFYCODE”（“$USERNAME”用于获取用户名；“$VRFYCODE”用于获取认证码）。取值范围为 18 至 128 个字符。默认内容为“SCVPN user < $USERNAME> email verification code: $VRFYCODE. Do not reveal to anyone! If you did not request this, please ignore it.”。

在<主机检测/绑定>标签页，填写相关配置信息。

主机检测	
进行此部分配置前，请先在主机检测页面配置主机检测规则。	
角色	在“角色”下拉菜单选中所需的用户初级角色名称，主机检测功能对该角色有效。“缺省”表示对多个用户均有效。
主机检测名称	在“主机检测名称”下拉菜单中选中已配置的主机检测规则名称。
异常处理方法	指定异常处理方法。 访客角色：选中“访客角色”单选按钮，然后在下拉菜单中选中所需的用户次级角色名称，当客户端的主机检测失败时，用户将获得该次级角色拥有的访问权限；“——”表示当客户端的主机检测失败时，系统将断开该客户端连接。 跳转 URL：选中“跳转 URL”单选按钮，然后在文本框中输入重定向 URL。当客户端的主机安全检测失败时，将会自动打开浏览器并跳转到指定的 URL，引导用户下载主机安全检测需要安装的软件并断开客户端连接；如果不配置该选项，系统将断开该客户端连接。
周期检测	在“周期检测”文本框中指定用户的自动检测周期。单位为分钟，取值范围为 5 到 1440 分钟，默认值为 30 分钟。指定该参数后，系

主机检测	
	统可以周期性地进行安全检查，比如可以定时地检查客户端主机的防病毒软件是否开启，如果用户在使用过程中关闭了防病毒软件，系统可能会因此在用户的访问过程中改变该用户所属的角色，重新为该用户分配相应的权限。
添加	点击“添加”按钮，添加已配置的主机检测策略，被添加的主机检测策略将显示在下方的列表中。
主机绑定	
启用主机绑定，还需要在主机绑定验证页面配置主机绑定功能。	
启用主机绑定	点击此按钮=开启主机绑定功能。默认情况下，系统仅允许一个用户通过一台主机登录，即用户名和主机一一对应。用户可以通过选择以下选项改变主机名与用户的绑定关系： 允许一个用户通过多台主机登录。 允许多个用户通过一台主机登录。 用户首次登录时自动把用户名和主机 ID 的应用关系加入绑定表。

点击“最优路径检测”，填写相关配置信息。最优路径检测功能够使不同 ISP 线路接入的客户端自动选择最快线路连接到 SSL VPN 设备端，从而提供访问总部资源时的速度。（仅 IPv4 类型的 SSL VPN 支持）

选项	说明
不检测	不进行最优路径检测。
客户端	客户端通过发送 UDP 探测包自动判断最优链路，并选择连接的最优路径。
设备端	当 SSL VPN 客户端直接访问设备端出接口地址时，选择该项，设备端通过客户端的源接入地址判断其 ISP 类型，根据判断，将所有的 SSL VPN 出接口 IP 地址按照优先级重新排序并下发给客户端，由客户端选择连接的最优路径；当 SSL VPN 客户端通过 NAT 设备访问 SSL VPN 设备端时，如果选择该项，设备端会通过客户端的源接入地址判断其 ISP 类型，根据判断，将所有的 NAT 外网接口 IP 地址按照优先级重新排序并下发给客户端，由客户端选择连接的最优路径。
NAT 映射地址及端口	如需要，在<NAT 映射地址及端口>部分指定 NAT 设备上 DNAT 规则映射到 SSL VPN 服务器的外网 IP 及端口。当 SSL VPN 客户端通过 NAT 设备访问 SSL VPN 设备端时，该 NAT 设备会将客户端的访问地址映射到 SSL VPN 设备端的出接口地址。分别在<服务器 IP>和<端口>文本框中输入 NAT 设备外网端口 IP 地址及 HTTPS 端口号（为避免与 WebUI 使用的 HTTPS 端口号相冲突，建议用户不要把 HTTPS 端口号设置为 443）。系统允许最多配置四个 IP 地址。

4. 点击“完成”，保存所做的配置。

查看 SSL VPN 所有在线客户端，请按照以下步骤进行操作：

1. 点击“网络 > VPN > SSL VPN”，进入 SSL VPN 页面。
2. 选择 SSL VPN 实例。
3. 在页面下方的在线用户列表中查看该实例所有在线客户端的详细信息。用户还可以点击 过滤 按钮添加过滤条件（在线用户、用户组、主机绑定 ID），查看符合过滤条件的在线客户端的详细信息

配置资源列表

资源列表是指系统中配置的用户可便捷访问的资源，其中每个资源又包含多个资源条目。资源条目的展现形式为“资源名称+对应的 URL“。SSL VPN 用户登录认证通过后，认证服务器将该用户所属的用户组信息发送给 SSL VPN 服务器，然后服务器会根据配置的 SSL VPN 实例中用户组和资源的绑定关系，把该用户可访问的内网资源列表发送给 SSL VPN 客户端，客户端对接收到的资源列表信息进行分析并展示在用户系统自带的 IE 浏览器弹出的页面中，用户可以通过点击“资源条目”名称直接访问内网资源。需要注意的是，该资源列表页面只在认证通过后显示一次。如果登录的用户不属于任何用户组，认证成功后浏览器不会弹出资源列表页面。

配置 SSL VPN 资源列表，按照以下步骤进行操作：

1. 点击“网络 > VPN > SSL VPN”，进入 SSL VPN 页面。
2. 点击 SSL VPN 页面右上方的“相关配置”，选择“资源列表”。
3. 点击“新建”按钮，打开<资源配置> 页面。

在对话框中填写资源配置信息。

选项	说明
资源名称	输入新建资源的名称。范围是 1 到 63 个字符。
添加	点击“新建”按钮，将条目名称与 URL 的绑定条目添加到列表中。 **说明：**可配置的资源条目数目最大值根据平台不同可分为 200、500、1000 三类，请以实际情况为准。

选项	说明
条目名称	输入新资源条目的名称。每个资源中的资源条目名称不能重复。范围是 1 到 95 个字符。
URL	输入新资源条目所对应的 URL。
删除	点击“删除”按钮，删除选中的绑定条目。
上移/下移/移到最前/移到最后	移动已有的资源条目从而改变其在浏览器页面中的展示顺序。

4. 点击“确定”按钮，该资源的配置信息将会被显示在资源列表中。
   每个资源最多显示 3 个资源条目，其他的条目将以“…”显示。用户可以点击“编辑”和“删除”按钮，对选中的资源进行编辑和删除。

注意:

系统最多允许配置 256 个资源列表。

不同平台可配置的资源条目数目最大值不同，请以实际情况为准。

支持资源列表功能的 SSL VPN 客户端版本：SSL VPN Windows 客户端 v1.4.6.1238 及之后版本、iOS v2.0.6 及之后版本、Android v4.6 及之后版本。

配置接入地址池

设备端通过地址池给客户端分配 IP 地址。当客户端连接设备端成功后，设备端会从地址池里取出一个 IP 地址与其它相关参数（如 DNS 服务器地址与 WINS 服务器地址等）一起分配给客户端。

设备端通过创建和执行 IP 地址绑定规则来满足客户端的固定 IP 地址需求。IP 地址绑定规则包括 IP 用户绑定规则和 IP 角色绑定规则。IP 用户绑定规则将客户端用户与已配置地址池中的某个固定 IP 地址绑定，当客户端连接成功后，设备端会将绑定的 IP 地址分配给客户端；IP 角色绑定规则是将角色与已配置地址池中的某一 IP 地址范围绑定，当此客户端连接成功后，设备端会从绑定的地址范围中取出一个 IP 地址分配给客户端。

当设备端通过地址池给客户端分配 IP 地址时，系统会按照一定的顺序对客户端的 IP 地址绑定规则进行检查，决定如何为客户端分配 IP 地址。

检查是否已为客户端用户配置 IP 用户绑定规则，如果是，则将绑定的 IP 地址分配给客户端；否则，从非绑定地址范围中取出一个未被占用的 IP 分配给客户端。

检查是否已为客户端用户配置 IP 角色绑定规则，如果是，则从绑定的地址范围中取出一个 IP 地址分配给客户端；否则，从非绑定地址范围中取出一个未被占用的 IP 分配给客户端。

注意: IP 用户绑定规则中的 IP 地址和 IP 角色绑定规则中的 IP 地址不能重叠。

配置接入地址池，按照以下步骤进行操作：

1. 点击“对象 > 接入地址池”，进入接入地址池页面。
2. 选择“IPv4”或“IPv6”标签页，仅当该版本为 IPv6 版本时可配。
3. 点击“新建”按钮，打开<接入地址池配置> 页面。

在<接入地址池配置>标签页，填写配置信息。

基本配置	
接入地址池名称	指定地址池名称。
起始 IP	指定地址池的起始 IP 地址。
终止 IP	指定地址池的终止 IP 地址。
保留起始 IP	指定保留地址池的起始 IP 地址。
保留终止 IP	指定保留地址池的终止 IP 地址。
子网掩码	当创建的地址池类型为 IPv4 时，指定网络掩码。
前缀长度	当创建的地址池类型为 IPv6 时，指定 IPv6 地址前缀长

基本配置	
	度。取值范围是 111 到 128。该选项仅当该版本为 IPv6 版本时可配。
DNS1/DNS2/DNS3/DNS4	指定地址池的 DNS 服务器 IP 地址。此项为可选项，即地址池可以不指定 DNS 服务器。用户最多可以为每个地址池指定 4 个 DNS 服务器。
WINS1/WINS2	指定地址池的 WINS 服务器 IP 地址。此项为可选项，即地址池可以不指定 WINS 服务器。用户最多可以为每个地址池指定 2 个 WINS 服务器。仅在创建的地址池类型为 IPv4 时可配。
IP 用户绑定	
新建	点击“新建”按钮，将用户与 IP 地址的绑定条目添加到列表中。
用户	输入用户名称。
IP	输入 IP 地址。
删除	点击“删除”按钮删除选中的绑定条目。
IP 角色绑定	
新建	点击“新建”按钮，将角色与 IP 地址的绑定条目添加到列表中。
角色	输入角色名称。
起始 IP 地址	输入起始 IP 地址。
终止 IP 地址	输入终止 IP 地址。
删除	点击“删除”按钮删除选中的绑定条目。
上移/下移/移到最前/移到最后	移动已有的角色-IP 地址绑定规则从而改变规则的排列顺序。对于绑定到多个角色且多个角色有相应的角色-IP 地址绑定规则的用户，系统会对角色-IP 地址绑定规则进行顺序查找，然后按照查找到的相匹配的第一条规则为用户分配地址。

4. 点击“确定”按钮，保存所做的配置。

Secure Connect 客户端管理

终端用户可以通过以下地址下载 Secure Connect 客户端：

MAC OS：https://vpn.obs.cn-gdgz1.ctyun.cn/MACOS/rw.eCloudSecurityCloud1.2.0.852_20230921003440.dmg

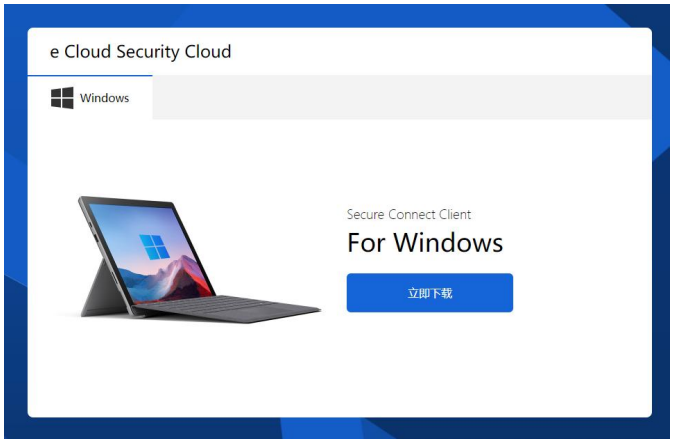
安卓：https://vpn.obs.cn-gdgz1.ctyun.cn/Android/app-eCloud-release.apk

IOS：https://vpn.obs.cn-gdgz1.ctyun.cn/IOS/IOS.txt 或 iOS 应用商店搜索 e Cloud Security 进行下载

Windows：https://vpn.obs.cn-gdgz1.ctyun.cn/Windows/scvpn.exe

自定义客户端下载页面

对于设备端提供的客户端下载地址，设备支持自行定制下载页面的背景图片及页面标题。默认情况下，下载页面无标题，背景图如下所示：



定制下载页面的背景图片和标题，按照以下步骤进行操作：

1. 点击“系统 > Secure Connect 客户端管理”。
2. 在“客户端下载页面配置”区域，点击“上传背景图片”按钮，选中需要的图片。图片需是 PNG 格式，建议分辨率为 1920px*1080px，大小不超过 2MB。
3. 点击“上传”按钮，将背景图片上载到系统。上传成功后，背景图片即完成修改。
4. 在“下载页面标题”文本框中，输入新的页面标题，长度为 1 到 63 个字符。
5. 点击“确定”保存设置。点击“取消”按钮，将只影响下载页面标题的设置。如不输入标题并保存配置，下载页面将不显示任何标题。
6. 点击“恢复缺省背景”，恢复默认下载页面的背景图。

自定义客户端下载源

管理员可以自行导入客户端到系统内，覆盖设备端的默认下载源，支持导入的客户端类型包括 Windows、macOS 和 Linux 类型客户端。

导入客户端，按照以下步骤操作：

1. 点击“系统 > Secure Connect 客户端管理”。
2. 在“客户端列表”区域，找到需要上传的客户端类型，点击“上传”按钮。

3. 在“上传 Windows/macOS/Linux 客户端”对话框，点击“浏览”按钮，选择需要上传的客户端文件，点击“上传””。

4. 上传后，“客户端列表”中相应客户端的下载源将由“官网”变为“本地”。

5. 点击“下载”按钮，检查下载的客户端是否是导入的客户端。

6. 点击“删除”按钮，删除导入的客户端。删除后，客户端下载源将恢复为默认下载源“官网”。

主机绑定

主机绑定也即主机验证。主机验证功能是指 SSL VPN 对运行 SSL VPN 客户端的主机进行验证。用户在 PC 上通过 SSL VPN 客户端登录时，客户端先收集主机的主板序列号、硬盘序列号、CPU ID 和 BIOS 序列号，然后客户端对这些信息进行 MD5 运算，生成一个 32 位的字符串，即主机 ID。之后，客户端将主机 ID 以及用户名密码信息发送到 SSL VPN 设备端进行验证。SSL VPN 设备端根据未绑定主机列表和已绑定主机列表中记录表项以及主机验证配置进行验证。未绑定主机列表和已绑定主机列表描述如下：

未绑定主机列表：客户端首次登录时，SSL VPN 设备端会记录用户名与主机 ID 的对应关系，并加入未绑定主机列表中。

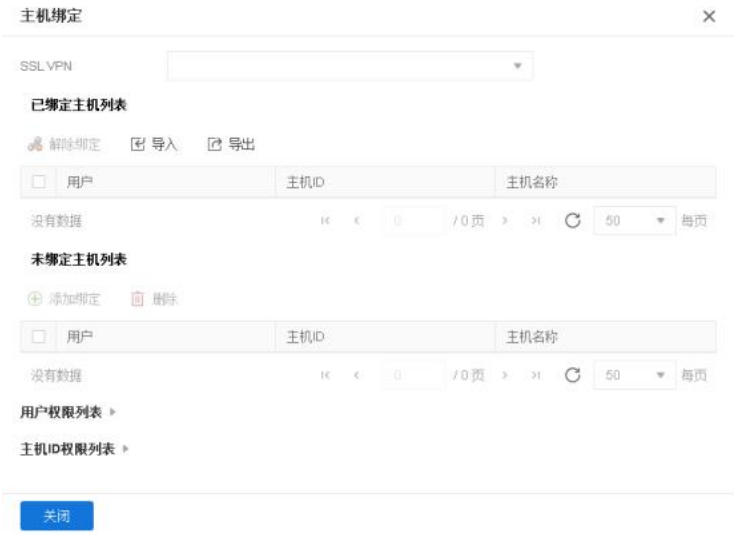
已绑定主机列表：已绑定主机列表中包含允许验证通过的主机 ID 与用户名对应关系的表项。用户可以通过手工操作或首次登录自动批准方式把候选表中的表项移入已绑定主机列表中。客户端登录时，SSL VPN 设备端会先检查已绑定主机列表中是否有该主机 ID 与用户名的对应关系表项，如果有，则通过主机验证，继续进行用户名密码验证；如果没有，则直接中断 SSL 通讯过程。

注意：对于虚拟化平台上部署的主机，由于主机 ID 无法保证唯一性，不同的虚拟机可能显示相同的主机 ID。

配置主机绑定

主机绑定配置包括主机绑定与解除绑定、超级用户，共享主机以及主机绑定导入/导出配置。

配置主机绑定与解除绑定



添加绑定表项，按照以下步骤进行操作：

1. 点击“网络 > VPN > SSL VPN”，进入 SSL VPN 页面。
2. 在 SSL VPN 页面右上方的“相关配置”下拉列表中选择“主机绑定”，打开<主机绑定>页面。
3. 在“未绑定主机列表”下方列表中，选中需要添加的主机 ID 与用户名对应关系表项复选框。 可以点击 过滤 按钮添加过滤条件（用户、主机 ID），搜索符合过滤条件的对应关系表项。
4. 点击“添加绑定”按钮将列表中相应的对应关系表项移到<已绑定主机列表>中。

解除绑定表项，按照以下步骤进行操作：

1. 点击“网络 > VPN > SSL VPN”，进入 SSL VPN 页面。
2. 在 SSL VPN 页面右上方的“相关配置”下拉列表中选择“主机绑定”，打开<主机绑定>页面。
3. 在“已绑定主机列表”下方列表中，选中需要解除绑定的表项复选框。 可以点击 过滤 按钮添加过滤条件（用户、主机 ID），搜索符合过滤条件的表项。
4. 点击“解除绑定”按钮删除列表中相应的表项。

配置超级用户

超级用户不受主机绑定功能限制，可以通过任意主机登录。配置超级用户，按照以下步骤进行操作：

1. 点击“网络 > VPN > SSL VPN”，进入 SSL VPN 页面。
2. 在 SSL VPN 页面右上方的“相关配置”下拉列表中选择“主机绑定”，打开<主机绑定>页面。

3. 点击“用户权限列表”后展开按钮，点击“新建”，打开<用户配置>页面。

在<用户配置>页面，填写相关信息。

选项	说明
用户	输入用户名称。
超级用户	点击“启用”按钮，将用户设置为超级用户，取值范围是 1 到 95 个字符。
预批准数	输入预批准数值。当允许一个用户通过多台主机登录且设置了用户首次登录自动批准用户名和主机 ID 的绑定关系时，默认情况下，仅自动批准用户和首次登录主机 ID 的绑定关系表项，即仅批准一个主机 ID，以后登录的主机 ID 进入候选表。该选项为用户设定预批准主机数，使数量范围限制内的主机 ID 都进入绑定表。

4. 点击“确定”按钮保存当前所做配置。

配置共享主机

通过共享主机登录的用户不受主机验证功能限制。配置共享主机，按照以下步骤进行操作：

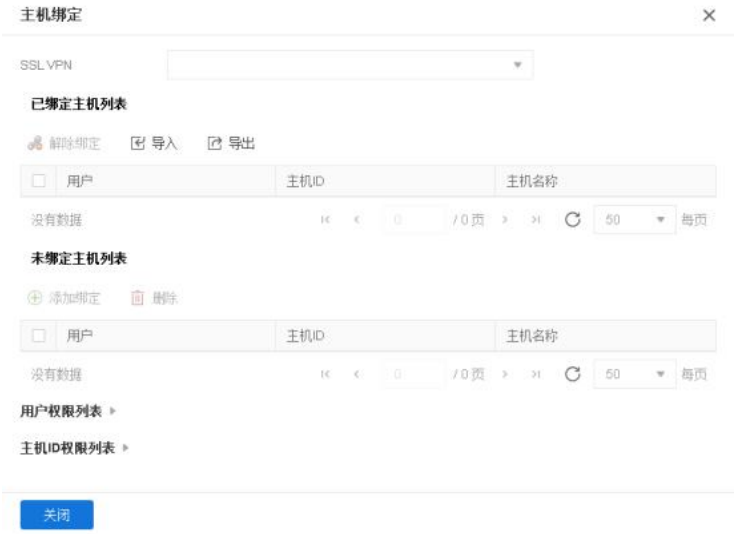
1. 点击“网络 > VPN > SSL VPN”，进入 SSL VPN 页面。
2. 在 SSL VPN 页面右上方的“相关配置”下拉列表中选择“主机绑定”，打开<主机绑定>页面。
3. 点击“主机 ID 权限列表”后展开按钮，点击“新建”，打开<主机配置>页面。

在<主机配置>页面，填写相关信息。

选项	说明
主机 ID	输入主机 ID。

4. 点击“确定”按钮保存当前所做配置。

导入/导出已绑定主机列表



导入已绑定主机列表，按照以下步骤进行操作：

1. 点击“网络 > VPN > SSL VPN”，进入 SSL VPN 页面。
2. 在 SSL VPN 页面右上方的“相关配置”下拉列表中选择“主机绑定”，打开<主机绑定>页面。
3. 在已绑定主机列表部分，点击“导入”按钮，进入<主机绑定导入设置>页面。
4. 点击“浏览”按钮，选择已绑定主机列表文件，然后点击“确定”按钮，系统将把选中的已绑定主机列表文件导入到设备。

导出已绑定主机列表，按照以下步骤进行操作：

1. 点击“网络 > VPN > SSL VPN”，进入 SSL VPN 页面。
2. 在 SSL VPN 页面右上方的“相关配置”下拉列表中选择“主机绑定”，打开<主机绑定>页面。
3. 在已绑定主机列表部分，选中列表中某项，点击“导出”按钮，导出列表文件。

主机检测

主机检测功能是指 SSL VPN 设备端对运行 SSL VPN 客户端主机的安全状况进行检测，通过检查客户端主机的操作系统、IE 版本以及特定软件的安装情况等因素来评估客户端主机的安全级别，并根据不同安全级别为客户端分配不同的资源访问权限，保证 SSL VPN 接入的安全性。

主机检测功能对客户端主机的详细检查内容，请参阅下表：

检查项目	详细描述
操作系统配置	操作系统版本（如 Windows 2000、Windows 2003、Windows XP、Windows Vista、Windows 7、Windows 8 等）

检查项目	详细描述
	操作系统补丁包版本（如 Service Pack 1 等） Windows 特定补丁包是否安装（如 KB958215 等）
	Windows 安全中心和自动升级是否打开 防病毒软件是否必须安装，实时监控和病毒库在线升级是否打开 防间谍软件是否必须安装，实时监控和特征库在线升级是否打开 个人防火墙是否必须安装和实时保护是否打开
	IE 版本和安全级别是否达到指定标准
其他配置	指定进程是否正在运行
	指定服务是否已经安装
	指定服务是否正在运行
	指定注册表键值是否存在
	指定文件是否存在于操作系统中

基于角色的访问控制和主机检测流程

基于角色的访问控制是指用户的权限不是由用户名而是由用户在系统中的角色决定的，一个登录于某系统的用户，可以通过它所对应角色的权限来决定其可以访问的系统资源。在权限管理中，角色作为中间桥梁把用户和权限联系起来。

SSL VPN 在主机检测流程中实现了基于角色的访问控制，在主机检测策略规则中引入初级角色和次级角色的概念。初级角色主要用于用户从设备端获取对应的主机检测规则信息（包含主机检测的内容以及安全级别）；次级角色决定检测失败用户的实际访问权限。

主机检测流程如下：

1. 客户端发起连接请求并成功认证。
2. 设备端下发主机检测规则到客户端。
3. 客户端根据主机检测规则对主机系统进行相应的安全检测。如果检测失败，则弹出检测结果进行提示。
4. 客户端将最终检测结果返回给设备端。
5. 设备端根据配置的主机检测策略规则断开检测失败客户端的连接或者根据其相应的次级角色授予实际访问权限。

另外，主机检测功能还支持动态的访问权限控制。一方面，当设备端的安全状况发生变化时，设备端会主动下发主机检测规则给客户端，并要求客户端重新进行安全检测；另一方面，客户端可以周期性地进行安全检查，比如可以定时地检查客户端主机的防病毒软件是否开启，如果用户在使用过程中关闭了防病毒软件，系统可能会因此在用户的访问过程中改变该用户所属的角色，重新为该用户分配相应的权限。

配置主机检测规则

配置主机检测规则，按照如下步骤进行操作：

1. 点击“网络 > VPN > SSL VPN”，进入 SSL VPN 页面。
2. 在右上方的“相关配置”下拉列表中选择“主机检测”，打开<主机检测>页面。
3. 点击<主机检测>的“新建”按钮，打开<主机检测配置>页面。

在<基本配置>页面，填写基本配置信息。

选项	说明
主机检测名称	指定主机安全检测规则名称。
OS 版本	指定是否检测客户端主机的操作系统版本。从下拉菜单中选择合适的检测类型，包括： 不检测：不对客户端主机操作系统版本进行检测。 必须匹配：客户端主机操作系统版本必须和指定操作系统版本一致。分别在后面的下拉菜单中选择操作系统版本和操作系统补丁包版本。 至少：客户端主机操作系统版本必须高于指定操作系统版本或者和指定操作系统版本一致。分别在后面的下拉菜单中选择操作系统版本和操作系统补丁包版本。
补丁包 1/2/3/4/5	指定客户端主机必须安装的特定 Windows 补丁包，在文本框中输入补丁包名称。用户最多可以为每条主机检测规则指定 5 个补丁包。

选项	说明
最低 IE 版本	指定检测客户端主机 Internet zone 的 IE 版本是否达到指定标准。当选择特定 IE 版本时，用户还可以在后面“最低 IE 安全级别”部分指定检测的 IE 安全级别。
最低 IE 安全级别	指定检测客户端主机的 IE 安全级别是否达到指定标准。

在<高级配置>页面，填写相关配置信息。

选项	说明
安全中心	指定检测客户端主机的 Windows 安全中心是否开启。点击“启用”按钮指定客户端主机必须开启 Windows 安全中心。
自动更新	指定检测客户端主机的 Windows 自动更新功能是否开启。点击“启用”按钮指定客户端主机必须开启 Windows 自动更新功能。
防病毒软件	安装软件：指定客户端主机必须安装防病毒软件。 实时监控：指定客户端主机必须开启防病毒软件实时监控功能。 病毒库更新：指定客户端主机必须开启防病毒软件病毒库在线升级功能
防间谍软件	安装软件：指定客户端主机必须安装防间谍软件。 实时监控：指定客户端主机必须开启防间谍软件实时监控功能。 特征库更新：指定客户端主机必须开启防间谍软件特征库在线升级功能。
防火墙	安装软件：指定客户端主机必须安装个人防火墙。 实时监控：指定客户端主机必须开启个人防火墙实时监控功能。
注册表键值	指定检测客户端主机的特定注册表键值是否存在。用户最多可以为每条主机检测规则指定 5 个注册表键值。在展开的列表中选择合适的检测类型，包括： 不检测：不检测特定注册表键值是否存在。 存在：客户端主机中包含指定注册表键值。在文本框中输入注册表键值名称，填写内容为“路径+表项名”，以下图为例，填写内容为 HKEY_LOCAL_MACHINE\SOFTWARE\Tencent\WeDrive\UpdateStatus。

选项	说明
	 不存在：指定注册表键值在客户端主机中不存在。在文本框中输入注册表键值名称，填写方法请见上图。
文件路径名称	指定检测客户端主机的特定文件是否存在。用户最多可以为每条主机检测规则指定 5 个文件名称。在展开的列表中选择合适的检测类型，包括： 不检测：不检测特定文件是否存在。 存在：客户端主机操作系统中包含指定文件。在文本框中输入文件名称。 不存在：指定文件在客户端主机操作系统中不存在。在文本框中输入文件名称。
运行进程名称	指定检测客户端主机的特定进程是否正在运行。用户最多可以为每条主机检测规则指定 5 个进程名称。在展开的列表中选择合适的检测类型，包括： 不检测：不对特定进程的运行情况进行检测。 存在：指定进程在客户端主机中正在运行。在文本框中输入进程名称。 不存在：指定进程在客户端主机中没有运行。在文本框中输入进程名称。
安装服务名称	指定检测客户端主机的特定服务是否已经安装。用户最多可以为每条主机检测规则指定 5 个服务名称。在展开的列表中选择合适的检测类型，包括： 不检测：不对特定服务的安装情况进行检测。 存在：指定服务在客户端主机中已经安装。在文本框中输入服务名称。 不存在：指定服务在客户端主机中没有安装。在文本框中输入服务名称。
运行服务名称	指定检测客户端主机的特定服务是否正在运行。用户最多可以为每条主机检测规则指定 5 个服务名称。在展开的列表中选择合适的检测类型，包括：

选项	说明
	不检测：不对特定服务的运行情况进行检测。 存在：指定服务在客户端主机中正在运行。在文本框中输入服务名称。 不存在：指定服务在客户端主机中没有运行。在文本框中输入服务名称。

4. 点击“确定”按钮，保存所做的配置。

Secure Connect 客户端 for Windows

支持 Windows 系统的 SSL VPN/ZTNA 客户端工具为 Secure Connect，建议在以下操作系统中运行：

Windows7、Windows8.1、Windows10、Windows11

Windows server 2008 R2、Windows server 2012、Windows server 2012 R2、Windows server 2016、Windows server 2019、Windows server 2022

通过客户端与设备端的连接，即可实现数据的加密通信。该客户端的主要作用包括：

从所在 PC 获得接口和路由信息；

显示与连接状态、数据流统计数据以及接口和路由信息；

显示应用程序日志信息；

调用客户端更新程序进行客户端更新；

解析从服务器端接收到的资源列表信息；

采集和上报终端状态信息。

本节主要介绍 Secure Connect Windows 客户端的下载、安装和启动。设备端对客户端支持以下三种认证方式：

用户名/密码

用户名/密码 + 数字证书（包括 USB Key 证书和软证书）

只用数字证书（包括 USB Key 证书和软证书）

系统支持 IPv4 和 IPv6 类型的 Secure Connect Windows 客户端。

下载与安装

可以通过以下方法下载 Secure Connect Windows 客户端：

https://vpn.obs.cn-gdgz1.ctyun.cn/Windows/scvpn.exe

在浏览器的地址栏输入以下 URL 访问设备端下载和安装：https://IP-Address:Port-Number。其中“IP-Address”和“Port-Number”分别为设备端 SSL VPN 或 ZTNA 实例中指定的接口的 IP 地址和 HTTPS 端口号。

成功安装 Secure Connect Windows 客户端后，将有一个虚拟网卡安装到 PC 上。该虚拟网卡用来实现客户端与设备端信息的安全加密传输。

启动与连接

客户端安装成功后，按照以下步骤启动和登录客户端：

1. 双击桌面的 Secure Connect Windows 客户端快捷方式，或者点击“开始菜单”中的“所有程序 > Secure Connect > Secure Connect”，系统弹出客户端页面。
2. 点击“添加连接”按钮，系统弹出下图所示对话框。

输入连接信息。

选项	说明
TLS/SSL	选择该页签，表示使用 TLS/SSL 加密协议。
国密 SSL	选择该页签，表示使用国密 SSL 协议。
连接名称	填写连接名称。
服务器	填写 SSL VPN 或 ZTNA 设备端的服务 IP 地址。
端口	填写 SSL VPN 或 ZTNA 设备端的 HTTPS 端口号。
认证类型	选择认证类型，支持“用户名/密码”、“用户名/密码+数字证书”和“仅数字证书”认证方式。数字证书认证支持软证书和 USB Key 证书。
用户名	当认证类型包含“用户名/密码”时，需填写客户端用户名和密码。
密码	填写与用户名相对应的密码。如果设备端采用本地认证服务器进行用户认证，此处的用户名和密码为设备中配置的用户及其相应

选项	说明
	的密码。
记住密码	勾选后，客户端在下一次建立连接时，无需用户再次输入密码。
数字证书	当认证类型设置为“用户名/密码+数字证书”或“仅数字证书”时，点击此项进入“选择证书”对话框选择认证所用的证书。
选择证书	当加密协议为 TLS/SSL 时，“选择数字证书”对话框各选项说明如下： 默认系统证书：选中该单选按钮时，设备采用 UKey 证书作为默认系统证书。该选项为系统默认选项。 USB Key 证书：选中该单选按钮，并在“证书列表”中选择 USB Key 证书，需提前将 USB Key 插入 PC 的 USB 接口。用户可以通过 USB Key 批量部署工具将第三方 USB Key 证书设置为默认系统证书。 软证书：选中该单选按钮，并在“证书列表”中选择软证书，需提前将软证书导入系统。 证书列表：显示系统中已有的证书。点击“刷新”图标刷新证书列表。
选择证书	当加密协议为国密 SSL 时，“选择数字证书”对话框各选项说明如下： 设备名称：在下拉菜单中选择当前 USB Token 设备名称。需提前将 USB Token 插入 PC 的 USB 接口。 应用名称：应用是包含容器、设备认证密钥以及文件的一种结构。在下拉菜单选择指定的应用名称。 容器名称：容器是 USB Token 设备中用于保存密钥所划分的唯一性存储空间。用来存储加密密钥对、与加密密钥对所对应的加密证书、签名密钥对、与签名密钥对所对应的签名证书。在下拉菜单选择指定的容器名称。 签名证书：显示指定容器内的 SM2 签名证书名称。 加密证书：显示指定容器内的 SM2 加密证书名称。
PIN 码	当认证类型设置为“用户名/密码+数字证书”或“仅数字证书”时，需填写数字证书对应的 PIN 码。
记住 PIN 码	勾选后，客户端在下一次建立连接时，无需用户再次输入 PIN 码。

选项	说明
最优通道	设置是否开启最优路径检测功能。该功能用于 SSL VPN 访问场景。默认为关闭。
网关探测	设置是否开启网关探测功能。该功能用于 ZTNA 访问场景。当 ZTNA 设备端配置了备选网关时，ZTNA 客户端可以开启网关探测功能。用户登录时，ZTNA 客户端会先获取备选网关列表，探测每个备选网关的链路质量，并选择链路质量最优的网关建立 ZTNA 连接。建立连接后，客户端会每隔 30 分钟更新一次备选网关的链路质量。如果发生连接中断或用户登录失败，客户端会自动切换到链路质量最优的备选网关重新建立连接。默认为开启。
最优网关	开启网关探测后，ZTNA 客户端会在用户登录时获取到备选网关列表，此时用户可以手动选择最优网关。最优网关默认不指定。如果指定了最优网关，用户再次登录时，ZTNA 客户端将优先向最优网关地址发起连接请求，若连接失败，则自动切换到链路质量最优的备选网关重新建立连接。
单包授权	设置是否开启单包授权（SPA）功能。该功能用于 ZTNA 访问场景。如果 ZTNA 设备端开启了 SPA 并配置了隐藏 IP 和端口，ZTNA 客户端也需要开启 SPA。用户通过 ZTNA 客户端登录时，需要先通过 SPA 敲门认证后才能建立到 ZTNA 服务的连接。当 ZTNA 设备端关闭 SPA 或开启了 SPA 但未配置隐藏 IP 和端口时，无论客户端是否开启 SPA，设备端都不会对客户端进行 SPA 认证。 开：开启时，客户端需要手动指定 SPA 的敲门端口。 关：客户端登录时不会敲门。 自动：无论 ZTNA 设备端是否开启 SPA 功能，客户端均认为服务器已开启 SPA 功能，并通过默认端口敲门。该选项为默认设置。
通信稳定性优化	设置是否使用 TCP 协议传输数据，该功能用于 SSL VPN 访问场景，默认为关闭。 启用该功能时需要设备端配置 TCP 端口。
验证服务器证书	点击“启用”按钮，在建立连接时，对服务器进行证书验证。

3. 连接信息填写完成后，点击“确定”按钮，系统将添加一条登录信息条目。如需要，可重复以上步骤添加多个登录信息条目。

4. 在客户端页面，客户端已将填写的连接信息保存为一条登录信息条目。点击“连接”按钮，客户端将建立到设备端的连接。

5. 如果设备端开启短信口令认证功能，客户端会弹出短信口令认证对话框（如下图所示）。输入短信认证码，并点击“验证”按钮。如果用户在 1 分钟内没收到认证码短信，可以重新申请认证码。

6. 如果设备端开启令牌口令认证功能，客户端将转到令牌口令认证对话框，用户需通过令牌口令认证

7. 如果设备端开启邮件口令认证功能，客户端会弹出邮件口令认证对话框，用户需通过邮件口令认证。

   通过用户名和密码验证后，用户最多可以输入 3 次认证码。如果连续 3 次输入错误，设备端将自动断开连接。

   用户最多能重新申请 3 次认证码，重新申请认证码的时间间隔为 1 分钟。重新申请认证码后，旧认证码信息失效，用户必须输入最新认证码才能认证成功。

8. 连接成功后，在系统任务栏的通知区域将会显示绿色的图标。

编辑和删除登录信息条目

当连接为断开状态时，将光标指向登录信息条目，点击  图标编辑登录信息条目；点击  图标删除登录信息条目。

查看连接和统计信息

在客户端页面，点击“统计”页签，查看连接和统计信息。

地址信息:显示 IP 地址信息。	
服务器	显示客户端连接到的设备端的 IP 地址。
客户端	显示当前客户端的 IP 地址。
加密信息:显示设备端使用的加密与验证算法以及 SSL 版本信息。	
密码套件	依次显示设备端使用的加密算法和验证算法。

地址信息:显示 IP 地址信息。	
密码版本	显示设备端使用的 SSL 协议版本。
连接状态:	
状态	显示客户端与设备端的当前连接状态。
IP 压缩	
算法	显示客户端所使用的数据压缩算法。
隧道包统计	
发送	显示通过隧道发送的数据包数。
接收	显示通过隧道接收的数据包数。
隧道字节统计	
发送	显示通过隧道发送的数据字节数。
接收	显示通过隧道接收的数据字节数。
连接时长	
持续	显示客户端与设备端保持连接的时间。
压缩率	
发送	显示通过压缩算法处理后的发送数据长度百分比。
接收	显示通过压缩算法处理后的接收数据长度百分比。

查看接口和路由信息

在客户端页面，点击“接口”页签，查看接口信息。在客户端页面，点击“路由”页签，查看路由信息。

选项	说明
接口名称	显示客户端传送加密信息的接口的名称。
接口类型	显示客户端传送加密信息的接口的类型。
接口状态	显示客户端传送加密信息的接口的状态。
IP 地址类型	显示客户端传送加密信息的接口 IP 地址的类型。
IP 地址	显示客户端传送加密信息的接口的 IP 地址（由设备端自动分配）。
子网掩码	显示客户端传送加密信息的接口的网络掩码。
默认网关	显示客户端传送加密信息的接口的默认网关地址。
DNS 服务器地址	显示客户端使用的 DNS 服务器地址。
WINS 地址	显示客户端使用的 WINS 服务器地址。

查看日志

在客户端页面，点击“日志”页签，查看日志信息。点击“导出”，导出日志信息到本地文件。点击“清除”，清除客户端日志。

点击 ，选择“日志级别”，设置需要显示的日志的级别。

USB Key 批量部署

设备采用 UKey 证书作为默认系统证书。使用默认系统证书进行认证时，Secure Connect Windows 客户端会自动选择默认系统证书传送至设备端，设备端对收到的数字证书进行认证，整个认证过程对用户来说是透明的，不需要用户手动进行证书选择。针对用户使用第三方 USB Key 进行 Secure Connect Windows 客户端认证的情况，提供 USB Key 批量部署工具 SelectUSBKey。通过 SelectUSBKey，用户能够将第三方 USB Key 证书设置为默认系统证书，从而简化认证时的操作过程。

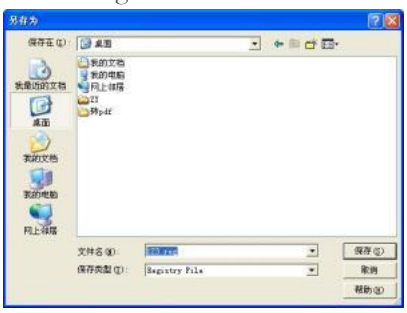
通过 SelectUSBKey 将第三方 USB Key 证书设置为默认系统证书，用户首先要将 USB Key 的 CSP Name 信息以注册表文件的格式导出，然后将文件中的信息添加进客户端 PC 注册表。

请按照以下步骤导出 USB Key 的 CSP Name 信息：

1. 在 PC 中安装第三方 USB Key 驱动程序。
2. 插入第三方 USB Key。
3. 双击 SelectUSBKey.exe，系统弹出<Select Default Certificate>对话框。如下图所示：

Export： 将 USB Key 的 CSP Name 以注册表文件（.reg）格式导出到本地目录。
Update： 刷新证书列表。
Close： 关闭对话框。

4. 在<Certificate List>中选中所需证书，点击『Export』按钮，将 USB Key 的 CSP Name 信息以注册表文件（.reg）格式导出到本地目录。如下图所示:



导出 USB Key 的 CSP Name 信息后，用户将信息文件存放在客户端 PC 目录中并双击该文件，将文件中的信息添加进客户端 PC 注册表。添加完成后，当用户通过该 USB Key 进行 SSL VPN 客户端认证时，客户端会自动选择 USB Key 中的数字证书传送至设备端，不需要用户手动选择证书。

客户端菜单

右键单击系统任务栏通知区域的 Secure Connect Windows 客户端的绿色图标，系统弹出客户端菜单，菜单项的作用如下：

修改密码：弹出<修改密码>对话框输入密码信息。

重定向 URL：设备端配置重定向 URL 时，点击此菜单可以快速跳转至该地址。

资源列表：当用户访问 SCVPN 服务时，连接成功后点击此菜单项将弹出浏览器页面，用户可以点击页面里的资源条目访问内网资源。

应用资源列表：当用户使用 Secure Connect Windows 客户端访问 ZTNA 服务时，连接成功后可以看到此菜单项。用户登录成功后弹出的 Portal 页面关闭后，可以点击该菜单打开最新的 Portal 页面查看应用资源的访问权限。Portal 页面上展示用户有权限和无权限访问的应用资源。对于无权限访问的应用资源，用户在调整终端配置后，可以获得访问权限。禁止访问的应用资源不在 Portal 页面上展示，如果用户被禁止访问任何应用资源，Portal 页面将展示“无可用的 Web 服务资源”。

显示主页面：当客户端界面处于最小化状态时，点击此项可以显示客户端主页面。

退出：退出 Secure Connect Windows 客户端程序。

通用设置

在客户端页面，点击“设置”。

开机自动运行：开启后，客户端将在 PC 系统启动时自动启动。

自动重连：开启后，客户端将在连接中断时进行自动重连。

自动登录：开启后，客户端将在启动时使用指定的用户名自动登录。从下拉菜单中选择自动登录用户名称。

连接最小化：开启后，客户端将在连接成功后自动缩小到托盘。

导入服务端可信证书：在建立连接时开启“验证服务器证书”功能后，点击按钮，在<可信证书>页面点击“导入”按钮，导入对服务器进行认证的证书。点击“删除”按钮，删除列表中的可信证书。

客户端的卸载

从 PC 上卸载 Secure Connect Windows 客户端，从“开始菜单”点击“所有程序 > Secure Connect > Secure Connect”，右键点击“Secure Connect”，在菜单中选择“卸载”。

Secure Connect 客户端 for Android

支持 Android 系统的 SSL VPN/ZTNA 客户端工具为 Secure Connect，可在 Android 8.x/Android 9.x/Android 10.x/Android 11.x/Android 12.x/Android 13.x 及鸿蒙 2.0 系统环境中运行。Secure Connect 主要作用包括：

从所在 Android 系统中获得接口信息；

显示与设备端连接状态、数据流统计以及接口和路由信息；

显示应用程序日志信息。

收集和上报终端状态信息。

下载与安装

下载和安装 Secure Connect Android 客户端，参照如下步骤：

1. 访问 https://vpn.obs.cn-gdgz1.ctyun.cn/Android/app-eCloud-release.apk 进行下载。
2. 下载完成后，在手机存储器中找到该安装文件。
3. 点击该安装文件。弹出程序安装界面。
4. 阅读权限需求。
5. 点击“安装”按钮。

安装成功后会在 Android 系统中出现程序图标。

启动与连接

客户端安装成功后，按照以下步骤启动和登录客户端：

1. 点击 Android 系统桌面上的 Secure Connect 图标，进入客户端界面。

2. 在“首页”页签，点击“+”，进入“添加连接”页面。

输入连接信息。

选项	说明
认证方式	选择认证方式，包括“用户名/密码”，“用户名/密码+数字证书”和“数字证书”。
连接名称	填写连接名称。
服务器地址	填写 SSL VPN 或 ZTNA 设备端的服务 IP 地址。
端口	填写 SSL VPN 或 ZTNA 设备端的 HTTPS 端口号。
用户名	当认证类型包含“用户名/密码”时，需填写客户端用户名和密码。
密码	填写与用户名相对应的密码。如果设备端采用本地认证服务器进行用户认证，此处的用户名和密码为设备中配置的用户及其相应的密码。
PIN 码	当认证类型设置为“用户名/密码+数字证书”或“数字证书”时，需填写数字证书对应的 PIN 码。
密码标准	选择使用哪种加密协议建立连接。 TLS/SSL：表示使用 TLS/SSL 协议。 国密 SSL：表示使用国密 SSL 协议。
选择证书	当认证类型设置为“用户名/密码+数字证书”或“数字证书”时，点击此项选择 TLS/SSL 证书或国密证书，需提前将证书导入 Android 系统。客户端会将证书传送到设备端进行认证。

选项	说明
网关探测	设置是否开启网关探测。该功能用于 ZTNA 访问场景。当 ZTNA 设备端配置了备选网关时，ZTNA 客户端可以开启网关探测功能。用户登录时，ZTNA 客户端会先获取备选网关列表，探测每个备选网关的链路质量，并选择链路质量最优的网关建立 ZTNA 连接。建立连接后，客户端会每隔 30 分钟更新一次备选网关的链路质量。如果发生连接中断或用户登录失败，客户端会自动切换到链路质量最优的备选网关重新建立连接。
最优网关	开启网关探测后，ZTNA 客户端会在用户登录时获取到备选网关列表，此时用户可以手动选择最优网关。最优网关默认不指定。如果指定了最优网关，用户再次登录时，ZTNA 客户端将优先向最优网关地址发起连接请求，若连接失败，则自动切换到链路质量最优的备选网关重新建立连接。
单包授权	设置是否开启单包授权（SPA）功能。该功能用于 ZTNA 访问场景。如果 ZTNA 设备端开启了 SPA 并配置了隐藏 IP 和端口，ZTNA 客户端也需要开启 SPA。用户通过 ZTNA 客户端登录时，需要先通过 SPA 敲门认证后才能建立到 ZTNA 服务的连接。当 ZTNA 设备端关闭 SPA 或开启了 SPA 但未配置隐藏 IP 和端口时，无论客户端是否开启 SPA，设备端都不会对客户端进行 SPA 认证。 开启：开启时，客户端需要手动指定 SPA 的敲门端口。默认为开启。 关闭：客户端登录时不会敲门。 AUTO：无论 ZTNA 设备端是否开启 SPA 功能，客户端均认为服务器已开启 SPA 功能，并通过默认端口敲门。该选项为默认设置。

3. 连接信息填写完成后，点击“确定”按钮，系统将添加一条登录信息条目。如需要，可重复以上步骤添加多个登录信息条目。
4. 返回客户端主界面，选择刚刚添加的登录信息条目，打开“连接状态”开关。
5. 如果设备端开启短信口令、令牌口令或邮件口令认证功能，需输入相应的认证码完成认证。
6. 连接成功后，此时就可以实现客户端与设备端之间的加密通信。

编辑和删除登录信息条目

点击需要编辑的登录信息条目，点击  图标，可以编辑登录信息条目。

按住需要删除的登录信息条目，向右拖拽，可以删除登录信息条目。

查看连接信息

点击客户端界面下方的“连接信息”页签，可查看连接统计、接口和路由信息。

连接统计信息：

选项	说明
服务器地址	显示当前连接的设备端 IP 地址或域名。
端口	显示当前连接的服务器端口号。
用户名	显示当前连接的登录用户名。
连接时长	显示客户端与设备端保持连接的时间。
接收字节	显示通过加密隧道接收的数据字节数。
发送字节	显示通过加密隧道发送的数据字节数。
接收数据包	显示通过加密隧道接收的数据包个数。
发送数据包	显示通过加密隧道发送的数据包个数。
接收压缩率	显示通过压缩算法处理后的接收数据长度百分比。
发送压缩率	显示通过压缩算法处理后的发送数据长度百分比。

接口统计信息：

选项	说明
接口名称	显示客户端传送加密信息的接口的名称。
接口类型	显示客户端传送加密信息的接口的类型。
接口状态	显示客户端传送加密信息的接口的状态。
物理地址	显示客户端传送加密信息的接口的 MAC 地址。
IP 地址类型	显示客户端传送加密信息的接口 IP 地址的类型。
网络地址	显示客户端传送加密信息的接口的 IP 地址（由设备端自动分配）。
子网掩码	显示客户端传送加密信息的接口的网络掩码。
默认网关	显示客户端传送加密信息的接口的默认网关地址。
DNS 服务器地址	显示客户端使用的 DNS 服务器地址。

Secure Connect 客户端 for iOS

支持 iOS 系统的 SSL VPN/ZTNA 客户端工具为 Secure Client，可在 iOS 12.x/iOS 13.x/iOS 14.x/iOS 15.x/iOS 16.x 系统环境中运行。iOS 客户端的主要作用包括：

简化与设备端建立隧道的过程；

显示与设备端连接状态；

显示日志信息。

采集和上报终端状态信息。

下载与安装

可以通过以下方法下载 Secure Connect iOS 客户端：

从 App Store 搜索应用 e Cloud Security 进行下载下载和安装。

启动与连接

客户端安装成功后，如果是首次登录，需要按照以下步骤启动和登录客户端：

1. 点击 iOS 系统桌面上的 HSAccess 图标，进入客户端界面。
2. 点击“+”，进入“添加连接”页面。

输入连接信息。

选项	说明
连接名称	填写连接名称。
服务器地址	填写 SSL VPN 或 ZTNA 设备端的服务 IP 地址。
端口	填写 SSL VPN 或 ZTNA 设备端的 HTTPS 端口号。
用户名	填写客户端用户名。
密码	填写与用户名相对应的密码。如果设备端采用本地认证服务器进行

选项	说明
	用户认证，此处的用户名和密码为设备中配置的用户及其相应的密码。
密码标准	选择加密连接的密码标准。 TLS/SSL：表示使用 TLS 加密。 国密 SSL：表示使用国密 SSL 加密。
网关探测	设置是否开启网关探测。该功能用于 ZTNA 访问场景。当 ZTNA 设备端配置了备选网关时，ZTNA 客户端可以开启网关探测功能。用户登录时，ZTNA 客户端会先获取备选网关列表，探测每个备选网关的链路质量，并选择链路质量最优的网关建立 ZTNA 连接。建立连接后，客户端会每隔 30 分钟更新一次备选网关的链路质量。如果发生连接中断或用户登录失败，客户端会自动切换到链路质量最优的备选网关重新建立连接。
最优网关	开启网关探测后，ZTNA 客户端会在用户登录时获取到备选网关列表，此时用户可以手动选择最优网关。最优网关默认不指定。如果指定了最优网关，用户再次登录时，ZTNA 客户端将优先向最优网关地址发起连接请求，若连接失败，则自动切换到链路质量最优的备选网关重新建立连接。
单包授权	设置是否开启单包授权（SPA）功能。该功能用于 ZTNA 访问场景。如果 ZTNA 设备端开启了 SPA 并配置了隐藏 IP 和端口，ZTNA 客户端也需要开启 SPA。用户通过 ZTNA 客户端登录时，需要先通过 SPA 敲门认证后才能建立到 ZTNA 服务的连接。当 ZTNA 设备端关闭 SPA 或开启了 SPA 但未配置隐藏 IP 和端口时，无论客户端是否开启 SPA，设备端都不会对客户端进行 SPA 认证。 开启：开启时，客户端需要手动指定 SPA 的敲门端口。默认为开启。 关闭：客户端登录时不会敲门。 AUTO：无论 ZTNA 设备端是否开启 SPA 功能，客户端均认为服务器已开启 SPA 功能，并通过默认端口敲门。该选项为默认设置。

3. 连接信息填写完成后，点击“确定”按钮，系统将添加一条登录信息条目。如需要，可重复以上步骤添加多个登录信息条目。
4. 返回客户端主界面，选择刚刚添加的登录信息条目，打开“连接状态”开关。
5. 如果设备端开启短信口令、令牌口令或邮件认证功能，需输入相应的认证码。
6. 登录成功后，客户端与设备端成功建立连接。
7. 在<允许安装 VPN 配置文件>对话框中，点击“允许”按钮。

8. 在<输入密码>页面中，输入 iOS 锁屏密码。密码输入正确后，iOS 开始下发 VPN 配置文件。
9. 下发完成后，打开 iOS 设备的设置功能，点击“通用>VPN”。在<选择配置>列表中，选中需要连接的 VPN 名称，即在 VPN 配置中设置的连接名称。
10. 打开 VPN 开关。iOS 设备进行 VPN 连接。
11. 连接成功后，就可以实现客户端与设备端之间的加密通信。

注意: 如果不是首次登录，将不会进行 VPN 配置文件的安装。只需要登录客户端与设备端进行连接，并在 iOS 系统中完成 VPN 的连接，即可对客户端与设备端之间传输的数据进行加密。

编辑和删除登录信息条目

点击需要编辑的登录信息条目，点击  图标，可以编辑登录信息条目。

按住需要删除的登录信息条目，向右拖拽，可以删除登录信息条目。

查看连接信息

点击客户端界面下方的“连接信息”页签，可查看连接统计、接口和路由信息。

连接统计信息：

选项	说明
服务器地址	显示当前连接的设备端 IP 地址或域名。
端口	显示当前连接的服务器端口号。
用户名	显示当前连接的登录用户名。
连接时长	显示客户端与设备端保持连接的时间。
接收字节	显示通过加密隧道接收的数据字节数。
发送字节	显示通过加密隧道发送的数据字节数。
接收数据包	显示通过加密隧道接收的数据包个数。
发送数据包	显示通过加密隧道发送的数据包个数。
接收压缩率	显示通过压缩算法处理后的接收数据长度百分比。
发送压缩率	显示通过压缩算法处理后的发送数据长度百分比。

接口统计信息：

选项	说明
接口名称	显示客户端传送加密信息的接口的名称。
接口类型	显示客户端传送加密信息的接口的类型。
接口状态	显示客户端传送加密信息的接口的状态。
物理地址	显示客户端传送加密信息的接口的 MAC 地址。

选项	说明
IP 地址类型	显示客户端传送加密信息的接口 IP 地址的类型。
网络地址	显示客户端传送加密信息的接口的 IP 地址（由设备端自动分配）。
子网掩码	显示客户端传送加密信息的接口的网络掩码。
默认网关	显示客户端传送加密信息的接口的默认网关地址。
DNS 服务器地址	显示客户端使用的 DNS 服务器地址。

Secure Connect 客户端 for macOS

支持 macOS 系统的 SSL VPN/ZTNA 客户端工具为 Secure Connect，建议在 macOS 10.13、macOS 10.14、macOS 10.15、macOS 11、macOS 12、macOS 13 系统环境中运行。

通过客户端与设备端的连接，即可实现数据的加密通信。客户端的主要作用包括：

与设备端建立安全连接；

显示与设备端的连接状态、数据流统计数据以及路由信息；

显示应用程序日志信息；

采集和上报终端状态信息。

下载与安装

下载和安装 Secure Connect macOS 客户端，参照如下步骤：

1. 访问 https://vpn.obs.cn-gdgz1.ctyun.cn/MACOS/rw.eCloudSecurityCloud1.2.0.852_20230921003440.dmg 进行下载。
2. 下载完成后，双击安装程序，在弹出窗口中将 Secure Connect macOS 客户端拖拽到 Applications 中即可完成安装。

启动与连接

客户端安装成功后，按照以下步骤启动和登录客户端：

1. 在 macOS Launchpad 中单击 Secure Connect 图标，启动客户端。

2. 点击“添加连接”按钮，系统弹出下图所示对话框。

输入连接信息。

选项	说明
TLS/SSL	选择该页签，表示使用 TLS/SSL 加密协议。
国密 SSL	选择该页签，表示使用国密 SSL 协议。
连接名称	填写连接名称。
服务器	填写 SSL VPN 或 ZTNA 设备端的服务 IP 地址。
端口	填写 SSL VPN 或 ZTNA 设备端的 HTTPS 端口号。
认证类型	Linux 客户端的认证类型为“用户名/密码”。
用户名	填写客户端用户名。
密码	填写与用户名相对应的密码。如果设备端采用本地认证服务器进行用户认证，此处的用户名和密码为设备中配置的用户及其相应的密码。
记住密码	勾选后，客户端在下一次建立连接时，无需用户再次输入密码。
网关探测	设置是否开启网关探测功能。该功能用于 ZTNA 访问场景。当 ZTNA 设备端配置了备选网关时，ZTNA 客户端可以开启网关探测功能。用户登录时，ZTNA 客户端会先获取备选网关列表，探测每个备选网关的链路质量，并选择链路质量最优的网关建立 ZTNA 连接。建立连接后，客户端会每隔 30 分钟更新一次备选网关的链路质量。如果发生连接中断或用户登录失败，客户端会自动切换到链路质量最优的备选网关重新建立连接。默认为开启。
最优网关	开启网关探测后，ZTNA 客户端会在用户登录时获取到备选网关列表，此时用户可以手动选择最优网关。最优网关默认不指定。如果指定了最优网关，用户再次登录时，ZTNA 客户端将优先向最优网关地址发起连接请求，若连接失败，则自动切换到链路质量最优的备选网关重新建立连接。

选项	说明
单包授权	设置是否开启单包授权（SPA）功能。该功能用于 ZTNA 访问场景。如果 ZTNA 设备端开启了 SPA 并配置了隐藏 IP 和端口，ZTNA 客户端也需要开启 SPA。用户通过 ZTNA 客户端登录时，需要先通过 SPA 敲门认证后才能建立到 ZTNA 服务的连接。当 ZTNA 设备端关闭 SPA 或开启了 SPA 但未配置隐藏 IP 和端口时，无论客户端是否开启 SPA，设备端都不会对客户端进行 SPA 认证。 开：开启时，客户端需要手动指定 SPA 的敲门端口。 关：客户端登录时不会敲门。 自动：无论 ZTNA 设备端是否开启 SPA 功能，客户端均认为服务器已开启 SPA 功能，并通过默认端口敲门。该选项为默认设置。
通信稳定性优化	设置是否使用 TCP 协议传输数据，该功能用于 SSL VPN 访问场景，默认为关闭。 启用该功能时需要设备端配置 TCP 端口。
验证服务器证书	点击“启用”按钮，在建立连接时，对服务器进行证书验证。

3. 连接信息填写完成后，点击“确定”按钮，系统将添加一条登录信息条目。如需要，可重复以上步骤添加多个登录信息条目。
4. 在客户端页面，客户端已将填写的连接信息保存为一条登录信息条目，用户可以编辑和删除登录信息。点击“连接”按钮，客户端将建立到设备端的连接。
5. 如果设备端开启短信口令、令牌口令或邮件口令认证功能，需输入相应的认证码完成认证。
6. 连接成功后，就可以实现客户端与设备端之间的加密通信。

编辑和删除登录信息条目

当连接为断开状态时，将光标指向登录信息条目，点击  图标编辑登录信息条目；点击  图标删除登录信息条目。

查看连接和统计信息

在客户端页面，点击“统计”页签，查看连接和统计信息。

地址信息:显示 IP 地址信息。	
服务器	显示客户端连接到的设备端的 IP 地址。
客户端	显示当前客户端的 IP 地址。
加密信息:显示设备端使用的加密与验证算法以及 SSL 版本信息。	
密码套件	依次显示设备端使用的加密算法和验证算法。
密码版本	显示设备端使用的 SSL 协议版本。
连接状态:	
状态	显示客户端与设备端的当前连接状态。
IP 压缩	
算法	显示客户端所使用的数据压缩算法。
隧道包统计	
发送	显示通过隧道发送的数据包数。
接收	显示通过隧道接收的数据包数。
隧道字节统计	
发送	显示通过隧道发送的数据字节数。
接收	显示通过隧道接收的数据字节数。
连接时长	
持续	显示客户端与设备端保持连接的时间。
压缩率	
发送	显示通过压缩算法处理后的发送数据长度百分比。
接收	显示通过压缩算法处理后的接收数据长度百分比。

查看接口和路由信息

在客户端页面，点击“接口”页签，查看接口信息。在客户端页面，点击“路由”页签，查看路由信息。

选项	说明
接口名称	显示客户端传送加密信息的接口的名称。
接口类型	显示客户端传送加密信息的接口的类型。
接口状态	显示客户端传送加密信息的接口的状态。
IP 地址类型	显示客户端传送加密信息的接口 IP 地址的类型。
IP 地址	显示客户端传送加密信息的接口的 IP 地址（由设备端自动分配）。
子网掩码	显示客户端传送加密信息的接口的网络掩码。
默认网关	显示客户端传送加密信息的接口的默认网关地址。
DNS 服务器地址	显示客户端使用的 DNS 服务器地址。
WINS 地址	显示客户端使用的 WINS 服务器地址。

查看日志

在客户端页面，点击“日志”页签，查看日志信息。点击“导出日志”，导出日志信息到本地文件。点击“清除日志”，清除客户端日志。

点击，选择“日志级别”，设置需要显示的日志的级别。

通用设置

在客户端页面，点击“设置”。

自动重连：开启后，客户端将在连接中断时进行自动重连。

自动登录：开启后，客户端将在启动时使用指定的用户名自动登录。从下拉菜单中选择自动登录用户名称。

连接最小化：开启后，客户端将在连接成功后自动缩小到托盘。

导入服务端可信证书：在建立连接时开启“验证服务器证书”功能后，点击按钮，在<可信证书>页面点击“导入”按钮，导入对服务器进行认证的证书。点击“删除”按钮，删除列表中的可信证书。

客户端菜单

右键单击系统任务栏通知区域的 Secure Connect macOS 客户端的绿色图标，系统弹出客户端菜单，菜单项的作用如下：

重定向 URL：设备端配置重定向 URL 时，点击此菜单可以快速跳转至该地址。

资源列表：当用户访问 SCVPN 服务时，连接成功后点击此菜单项将弹出浏览器页面，用户可以点击页面里的资源条目访问内网资源。

应用资源列表：当用户使用 Secure Connect macOS 客户端访问 ZTNA 服务时，连接成功后可以看到此菜单项。用户登录成功后弹出的 Portal 页面关闭后，可以点击该菜单打开最新的 Portal 页面查看应用资源的访问权限。Portal 页面上展示用户有权限和无权限访问的应用资源。对于无权限访问的应用资源，用户在调整终端配置后，可以获得访问权限。禁止访问的应用资源不在 Portal 页面上展示，如果用户被禁止访问任何应用资源，Portal 页面将展示“无可用的 Web 服务资源”。

显示主页面：当客户端界面处于最小化状态时，点击此项可以显示客户端主页面。

退出：退出 Secure Connect macOS 客户端程序。

卸载客户端

卸载客户端，右击客户端图标，从下拉菜单中选择“移到废纸篓”。

L2TP VPN

L2TP（Layer Two Tunneling Protocol，第二层隧道协议）是虚拟专用拨号网络（VPDN）技术的一种。L2TP 可以让拨号用户从 L2TP 客户端或者 L2TP 访问集中器端（LAC）发起 VPN 连接，通过点对点协议（PPP）连接到 L2TP 网络服务器（LNS）。连接成功后，LNS 会向合法用户分配 IP 地址，并允许其访问私网。

设备在 L2TP 协议隧道组网中可以充当 LNS 的角色，也可以充当 L2TP 客户端的角色。当作为 LNS 的角色时，它接受来自 L2TP 客户端或 LAC 的连接，进行用户认证与授权，为合法用户分配 IP 地址、DNS 服务

器地址和 WINS 服务器地址。当作为 L2TP 客户端的角色时，它主动发起 PPP 协商和认证，隧道建立完成过后，流量通过 L2TP VPN 隧道传输到对端。

L2TP 协议不对隧道传输中的数据进行加密，因此在传输过程中无法保证数据的安全。用户可以将 L2TP 协议和 IPSec 协议结合使用，利用 IPSec 协议对数据进行加密的优势，保证 L2TP 隧道传输中的数据安全。

配置设备作为 LNS

配置 L2TP VPN

新建 L2TP VPN，按照以下步骤进行操作：

1. 点击“网络 > VPN > L2TP VPN”，进入 L2TP VPN 页面。
2. 点击左上角的“新建”，打开<L2TP VPN 配置>页面。输入 L2TP VPN 名称并开始进行相关配置。

配置 L2TP VPN 信息。

接入用户	
L2TP VPN 名称	配置 L2TP VPN 名称。
接入用户	点击“新建”按钮，添加的 AAA 服务器。 AAA 服务器：在下拉菜单中选择需要的服务器名称。 域名：在文本框中输入服务器对应的域名。 用户域名验证：启用用户域名验证后，将对用户名及对应的域名进行验证。
出接口	指定客户端所访问的设备端接口。在下拉菜单中选择需要的设备端接口。
隧道接口	指定绑定 L2TP VPN 隧道的隧道接口，流量通过隧道接口进出 L2TP VPN 通道。在下拉菜单中选择系统中已配置的隧道接口；或者，点击下拉菜单中的“新建”按钮，在打开的<隧道接口>页面中新建隧道接口。
用户域名验证	启用用户域名验证后，将对用户名及对应的域名进行验证。

信息展示	显示隧道接口相关信息。
地址池	指定 L2TP VPN 地址池。在下拉菜单中选择系统中已配置的地址池；或者，点击下拉菜单中的“新建”按钮，在打开的<地址池配置>页面中新建地址池。
引用 IPSec 隧道	从下拉菜单选择引用的 IPSec 隧道。L2TP 协议不对隧道传输中的数据进行加密，因此在传输过程中无法保证数据的安全。用户可以将 L2TP 协议和 IPSec 协议结合使用，利用 IPSec 协议对数据进行加密的优势，保证 L2TP 隧道传输中的数据安全。

3. 如需要，点击“高级配置”后展开按钮，进行相应配置。

配置高级配置相关信息。

安全配置	
隧道认证	点击“启用”按钮启用隧道认证，保证连接的安全。隧道认证可由 LNS 或 LAC 任何一端发起，只有两端均通过隧道认证，即隧道密码一致时，方可建立隧道。
AVP 数据隐含	点击“启用”按钮启用 AVP 数据隐含。L2TP 协议使用 AVP（attribute value pair，属性值对）来传递和协商 L2TP 的一些参数、属性等。在默认情况下，AVP 是采用明文形式传输的。为了保证数据安全，用户可以通过隧道密码加解密这些数据，将这些 AVP 隐藏起来传输。
隧道密码	指定 LNS 端隧道认证的密码。
修改隧道密码	编辑配置时，可以看到修改隧道密码功能。开启后，将展示密码输入框。如需修改，输入新的密码后保存配置即可。
对端名称	指定 LAC 端设备的主机名称。如果多个 LAC 与 LNS 建立连接，用户可通过配置该项参数为不同的 LAC 端设备指定不同的隧道密码。点击“添加”按钮将配置的隧道密码和对端名称组合添加到列表。点击“删除”按钮删除选中的组合。
客户端连接	
允许客户端指定	点击“启用”按钮允许用户指定 IP 地址。默认情况下，客户端的 IP 地址由 LNS 从地址池中取出并自动分配。启用该功能后，用户可以指定 IP 地址，但该 IP 地址必须属于已指定的地址池范围之内且与用户的用户名和角色一致。如果指定的 IP 地址已被占用，则系统禁止该用户登录。
允许同名登录	点击“启用”按钮允许同一个用户在多个地点同时登录认证。
Hello 报文间隔	指定发送 Hello 报文的时间间隔。LNS 定时向 L2TP 客户端或 LAC 发送 Hello 报文检测隧道是否连通，若在一段时间内未收到应答，该隧道连接将被断开。
LNS 名称	指定本端隧道的名称。
隧道数据窗口大小	指定隧道传输数据的窗口大小。

安全配置	
控制报文重传次数	指定控制报文重传次数。如果在指定的重传次数内未收到对端的响应，则系统认为隧道连接已经断开。
PPP 配置	
LCP-echo	指定 PPP 协商过程中 LNS 发送 LCP Echo 报文的相关参数，包括： 发送间隔 - 指定发送 LCP Echo 报文的间隔时间。 重传次数 - 指定发送 LCP Echo 报文的重传次数。如果 LNS 在发送次数达到设置的重传次数后未收到响应，会判断连接已经断开。
PPP 认证	指定 PPP 认证的协议，包括： PAP - 指定 PPP 认证方式为密码认证协议 PAP。 CHAP - 指定 PPP 认证方式为质询握手认证协议 CHAP。此选项为默认选项。 any - 指定该参数后，系统首选认证方式为 CHAP，如果认证不支持 CHAP 协议时，则使用 PAP 协议进行认证。

4. 点击“确定”按钮，保存所做配置。

配置 L2TP VPN 地址池

LNS 通过地址池给用户分配 IP 地址。当用户连接 LNS 成功后，LNS 会从地址池里取出一个 IP 地址与其它相关参数（如 DNS 服务器地址与 WINS 服务器地址等）一起分配给用户。

L2TP 通过创建和执行 IP 地址绑定规则来满足客户端的固定 IP 地址需求。IP 地址绑定规则包括静态 IP 地址绑定规则和角色-IP 地址绑定规则。

静态 IP 地址绑定规则将客户端用户与已配置地址池中的某个固定 IP 地址绑定，当客户端连接成功后，系统会将绑定的 IP 地址分配给客户端；

角色-IP 地址绑定规则是将角色与已配置地址池中的某一 IP 地址范围绑定，当此客户端连接成功后，系统会从绑定的地址范围中取出一个 IP 地址分配给客户端。

> 注意: 静态 IP 地址绑定规则中的 IP 地址和角色-IP 地址绑定规则中的 IP 地址不能重叠。

新建 L2TP VPN 地址池，按照以下步骤进行操作：

1. 点击“网络 > VPN > L2TP VPN”，进入 L2TP VPN 页面。
2. 点击页面右上角的“L2TP VPN 地址池”，打开<地址池>页面。

3. 点击“新建”，打开<地址池配置>页面。

配置基本信息。

选项	说明
地址池名称	指定地址池名称。
起始 IP	指定地址池的起始 IP 地址。
终止 IP	指定地址池的终止 IP 地址。
保留起始 IP	指定保留地址池的起始 IP 地址。
保留终止 IP	指定保留地址池的终止 IP 地址。
DNS1/2	指定地址池的 DNS 服务器 IP 地址。此项为可选项，即地址池可以不指定 DNS 服务器。用户最多可以为每个地址池指定 2 个 DNS 服务器。
WINS1/2	指定地址池的 WINS 服务器 IP 地址。此项为可选项，即地址池可以不指定 WINS 服务器。用户最多可以为每个地址池指定 2 个 WINS 服务器。

配置 IP 用户绑定信息。

选项	说明
用户	输入用户名称。
IP	输入 IP 地址。
新建	将用户与 IP 地址的绑定条目添加到列表中。
删除	删除选中的绑定条目。

在<IP 角色绑定>标签页，填写相关信息。

选项	说明
角色	输入角色名称。
起始 IP	输入起始 IP 地址。
终止 IP	输入终止 IP 地址。
新建	将角色与 IP 地址的绑定条目添加到列表中。
删除	删除选中的绑定条目。
上移/下移/移到最前/移到最后	移动已有的角色-IP 地址绑定规则从而改变规则的排列顺序。对于绑定到多个角色且多个角色有相应的角色-IP 地址绑定规则的用户，系统会对角色-IP 地址绑定规则进行顺序查找，然后按照查找到的相匹配的第一条规则为用户分配地址。

4. 点击“确定”按钮，完成配置。

查看在线用户

查看 L2TP VPN 所有在线客户端，按照以下步骤进行操作：

1. 点击“网络 > VPN > L2TP VPN”，进入 L2TP VPN 页面。
2. 选择 L2TP VPN 实例。
3. 在页面下方的在线用户列表中查看该 L2TP VPN 实例所有在线客户端的详细信息。

选项	说明
名称	显示 L2TP VPN 名称。
登录时间	显示在线用户的登录时间。
公网 IP	显示在线用户的公网 IP 地址。
私有 IP	显示 L2TP VPN 分配给在线用户的 IP 地址。
操作	显示在线用户的可执行操作。

配置设备作为 L2TP 客户端

配置 L2TP VPN 客户端

新建 L2TP VPN 客户端，按照以下步骤进行操作：

1. 点击“网络 > VPN > L2TP VPN”，进入 L2TP VPN 页面。
2. 点击页面右上角的“L2TP VPN 客户端”，打开<L2TP 客户端>页面。

3. 点击“新建”按钮，打开<L2TP 客户端配置>页面。

配置 L2TP 客户端信息。

选项	说明
客户端名称	配置 L2TP 客户端的名称。
隧道接口	指定绑定 L2TP 客户端的隧道接口，流量通过隧道接口进出 L2TP 客户端。在下拉菜单中选择系统中已配置的隧道接口；或者，点击下拉菜单中的“新建”按钮，在打开的<隧道接口>页面中新建隧道接口。
出接口	指定 LNS 端所访问的设备端接口。在下拉菜单中选择需要的设备端接口。
服务器 IP 地址	指定 LNS 服务器的 IP 地址。
隧道保活时间	LNS 和 L2TP 客户端之间的隧道建立后，为保证双方的正常通信，L2TP 客户端会定期发送 Hello 报文确认 LNS 是否可以正常连接。“保活时间”即连续两次发送 hello 报文之间的时间间隔，取值越小则设备对于可能存在的网络故障感知越快，取值越大则 hello 报文占用网络带宽越小。
控制报文重传次数	指定控制报文重传次数。如果在指定的重传次数内未收到对端的响应，则系统认为隧道连接已经断开。
用户名	指定 L2TP 客户端的用户名，L2TP 客户端使用此用户名向 LNS 端发起 L2TP 隧道建立请求，LNS 端对拨入用户认证通过后，建立 L2TP 隧道和会话。
密码	指定 L2TP 客户端的用户密码。
修改密码	编辑配置时，可以看到修改密码功能。开启后，将展示密码输入框。如需修改，输入新的密码后保存配置即可。
PPP 配置	

选项	说明
LCP-echo 发送间隔	指定 PPP 协商过程中发送 LCP Echo 报文的间隔时间，取值范围是 0-1000 秒。
重传次数	指定发送 LCP Echo 报文的重传次数。如果 L2TP 客户端在发送次数达到设置的重传次数后未收到响应，会判断连接已经断开。
PPP 认证	指定 PPP 认证的协议，包括： PAP - 指定 PPP 认证方式为密码认证协议 PAP。 CHAP - 指定 PPP 认证方式为质询握手认证协议 CHAP。此选项为默认选项。 any - 指定该参数后，系统首选认证方式为 CHAP，如果认证不支持 CHAP 协议时，则使用 PAP 协议进行认证。
自动连接	开启 L2TP 客户端自动拨号功能。开启此功能后，L2TP 客户端与 LNS 之间可以自主建立隧道，用户不用 PPP 拨号即可访问 LNS 内网。

4. 点击“确定”按钮，保存所做配置。

VXLAN

VXLAN 是采用 MAC in UDP（User Datagram Protocol）封装方式，是 NVO3（Network Virtualization over Layer3）中的一种大二层虚拟网络扩展的隧道封装技术。VXLAN 引入了类似 VLAN ID 的用户标识，称为 VXLAN 网络标识 VNI（VXLAN Network ID），由 24 比特组成，可划分多达 16M 的 VXLAN 段，从而满足了大量的用户标识。通过 VXLAN 构建大二层网络，保证了在虚拟迁移时虚拟机的 IP 地址、MAC 地址等参数保持不变。

VXLAN 使用 VTEP（VXLAN Tunnel Endpoint）设备对 VXLAN 报文进行封装与解封装，包括 ARP 请求报文和正常的 VXLAN 数据报文。VTEP 将原始以太网帧通过 VXLAN 封装后发送至对端 VTEP 设备，对端 VTEP 设备接收到 VXLAN 报文后解封装，然后根据原始 MAC 进行转发，VTEP 可以是物理交换机、物理服务器或者其他支持 VXLAN 的硬件设备或软件来实现。

配置 VXLAN 静态隧道

配置 VXLAN 静态隧道，按照以下步骤进行操作：

1. 点击“网络 > VPN > VXLAN”，进入 VXLAN 页面。

2. 点击“新建”，打开<VXLAN 配置>页面。输入 VXLAN 名称并开始进行相关配置。

配置 VXLAN 信息。

选项	说明
名称	配置 VXLAN 隧道的名称。
VNI	配置 VXLAN ID，作为 VXLAN 网络的全局标识，取值范围是 1-16777215。
出接口	在下拉列表中选择 VXLAN 网络的出接口。配置二层安全域请参考隧道接口。
对端 IP	配置目的 VTEP 的 IP 地址。

3. 点击“确定”按钮，保存所做配置。

GRE VPN

GRE（Generic Routing Encapsulation）是通用封装路由，是定义了在任意一种网络层协议上封装任意一个其它网络层协议的协议。系统支持 GRE over IPSec 功能，实现路由协议信息的安全传输。

配置 GRE VPN

新建 GRE VPN，按照以下步骤进行操作：

1. 点击“网络 > VPN > GRE VPN”，进入 GRE VPN 页面。

2. 点击左上角的“新建”，打开<GRE VPN 配置>页面。输入 GRE VPN 名称并开始进行相关配置。

配置 GRE VPN 信息。

选项	说明
GRE VPN 名称	配置 GRE VPN 名称。
源地址类型	指定源地址类型，可以是源接口或源 IP 地址。
源接口/源 IP	为 GRE 隧道指定源地址，可以是接口名称或源 IP 地址。
目的 IP 地址	为 GRE 隧道指定目的地址。
出接口	为 GRE 隧道指定出接口。在下拉菜单中选择需要的设备端接口。
验证秘钥	指定验证秘钥。当数据包携带的秘钥与接收端配置的验证秘钥相同时，数据包将会被解密。如果不相同，数据包将会被丢弃。
引用 IPSec 隧道	从下拉菜单选择或新建引用的 IPSec 隧道。GRE 协议不对隧道传输中的数据进行加密，因此在传输过程中无法保证数据的安全。用户可以将 GRE 协议和 IPSec 协议结合使用，利用 IPSec 协议对数据进行加密的优势，保证 GRE 隧道传输中的数据安全。
隧道接口	指定绑定 GRE VPN 隧道的隧道接口。 在下拉列表中选择隧道接口。点击 按钮，编辑所选接口。 点击 按钮，新建接口。
隧道接口 IPv4/IPv6 网关	指定 GRE 隧道的下一跳 IP 地址，为对端隧道接口的 IP 地址。当配置多个隧道到隧道接口时，需要配置该参数。可以同时配置 IPv4 和 IPv6 类型的地址或仅配置其中一个。

3. 点击“确定”按钮，保存所做配置。

第 7 章 零信任网络访问(ZTNA)

介绍

相比于传统的 VPN 接入方式允许接入内网的终端访问任意资源，零信任网络访问（简称为 ZTNA），是以不信任企业边界内部和外部的任何实体为核心思想而提出的一种安全网络连接概念。只有对访问用户的身份、使用的设备以及访问时间等其他环境属性进行验证后，ZTNA 才会授予用户最小范围内的最可控的访问权限，用户可以从任何地点、通过任何设备安全地访问云上和数据中心的私有应用。

ZTNA 解决方案支持基于用户身份、终端设备的状态、访问时间等维度对访问流量进行管控，通过细粒度控制策略使之只能访问特定的授权应用，并持续监控终端状态变化，灵活调整用户可访问的授权应用范围。ZTNA 用户的登录流程如下：

1. ZTNA 用户在客户端输入服务器地址、端口、用户名、密码，请求验证。如果配置了二次认证，则需要完成二次认证。
2. 认证通过后，设备端为客户端分配私网 IP，并下发终端信息收集脚本。
3. 客户端执行脚本，收集主机信息，例如操作系统版本、是否安装防火墙、防病毒软件、IE 浏览器安全级别、是否运行某些进程等等，并上报给设备端。
4. 设备端解析主机信息，获取终端标签，将用户名和终端标签发送给认证模块，请求创建认证用户。
5. 认证模块创建认证用户，关联终端标签，获取用户组信息。
6. 设备端根据用户名、用户组和终端标签等信息匹配 ZTNA 策略，确定允许客户端访问的应用资源列表。
7. ZTNA 客户端弹出 Portal 页面，展示用户有权限和无权限访问的应用资源，并展示应用资源名称和 URL 地址。

ZTNA 需要安装许可证使用，设备默认提供 8 个 ZTNA 并发用户授权。不同性能的设备支持的最大 ZTNA 并发用户数不同，具体可与工程师沟通。

ZTNA 与 SSL VPN 共用 Secure Connect 客户端，如需访问 ZTNA 服务，请下载和安装最新版本的客户端，升级后的客户端支持 ZTNA 接入，也支持 SSL VPN 接入。ZTNA 解决方案支持 Windows、macOS、iOS 和 Android 终端接入，接入时需登录相应的客户端。

配置 ZTNA

配置 ZTNA 功能，按照以下步骤进行操作：

1. 点击“零信任访问 > 网关”，进入<ZTNA 服务配置>页面。

点击“名称/接入用户”，填写相关信息。

选项	说明
服务名称	输入 ZTNA 实例的名称。取值范围为 1 到 31 个字符。
类型	指定 ZTNA 实例的服务类型，可选择 IPv4 或 IPv6。IPv6 选项仅当该版本为 IPv6 版本时可配。
接入用户（最多配置 10 条）	
AAA 服务器	点击“新建”按钮，在下拉菜单中选择需要的服务器名称；或者，点击下拉菜单中的“+”按钮，新建一个 AAA 服务器。
域名	输入服务器对应的域名，用于区分不同的 AAA 服务器。取值范围为 1 到 31 个字符。
用户域名验证	启用用户域名验证后，将对用户名及对应的域名进行验证。

点击“接入接口/隧道接口”，填写相关信息。

选项	说明
出接口	指定客户端所访问的设备端接口。在下拉菜单中选择系统已配置的接口；或者，点击下拉菜单中的“+”按钮，按新建一个接口。最多可添加 8 个接口。
服务端口	指定客户端所访问的设备端 ZTNA 服务的端口号。取值范围为 1 至 65535。
隧道接口	指定 ZTNA 实例绑定的隧道接口。在下拉菜单中选择系统中已配置的隧道接口；或者，在下拉菜单中点击“+”按钮，新建隧道接口。
地址池	指定 ZTNA 的接入地址池。在下拉菜单中选择系统中已配置的地址池；或者，点击“+”按钮，在弹出的<接入地址池配置>对话框中新建地址池。关于接入地址池的配置说明，请参阅配置接入地址池。当配置 IPv6 类型的 ZTNA 时，该选项指定 IPv6 ZTNA 地址池。

点击“隧道路由配置”，指定通过 ZTNA 隧道能到达的网段或域名。

隧道路由
ZTNA 客户端接收到指定网段后，生成到达指定网段的路由条目。一个 ZTNA 实例

隧道路由	
可以配置 128 个基于网段的隧道路由。	
新建	点击“新建”按钮，配置隧道路由条目的相关信息并添加到列表中。
IP	输入目的 IP 地址。
子网掩码	输入目的 IP 地址的网络掩码。
度量值	输入路由的度量值。取值范围为 1 到 9999。
删除	点击此按钮删除选中的隧道路由。
添加默认路由	点击此按钮添加 IP 和掩码分别为全 0 的默认路由。
启用域名下发功能	
点击“启用”按钮，系统下发指定的域名。ZTNA 客户端接收到指定域名后，根据域名解析结果，生成到达域名所在地址的路由条目。	
设置路由上限	指定客户端可以根据域名解析后生成的最大路由条目数。取值范围是 1 到 10000。默认值为 1000。
新建	点击“新建”按钮，配置域名并添加到列表中。系统支持最多 64 个域名。
域名	指定域名。每次可添加一个。每个域名的字符串长度不得超过 63 个字符。域名末尾不能为“.”，不支持通配符，且不支持过于宽泛的 URL，比如：“.com”、“com”。
删除	点击此按钮删除选中的域名。

点击“参数配置”，填写相关配置信息。

安全套件	
SSL 版本	指定 SSL 协议类型。默认为 TLSv1.2。<any>表示 TLSv1、TLSv1.1、TLSv1.2 协议中的任何一种。 如果设备端指定的 SSL 协议类型为<TLSv1.2>或者<any>，在 ZTNA 客户端进行数字证书认证前，需要用户将要导入到浏览器中的软证书或者 USB Key 中的.pfx 格式证书进行处理，使得证书能够支持 TLSv1.2 协议，以便用户在使用“用户名/密码+数字证书”或者“数字证书”认证方式进行认证时，能够连接成功。处理证书前，请先准备一台安装了 OpenSSL1.0.1 版本及以上的 PC（Windows 或 Linux 系统均可）。以文件名称为 oldcert.pfx 的证书为例，处理步骤如下： 1. 在 OpenSSL 软件界面中，输入以下命令将.pfx 格式的证书转换为.pem 格式的证书。 **openssl pkcs12 –in oldcert.pfx –out cert.pem** 2. 继续输入下面的命令将.pem 格式的证书转换为支持 tlsv1.2 的.pfx 格式证书。 **openssl pkcs12 –export –in cert.pem –out newcert.pfx –CSP**

	“Microsoft Enhanced RSA and AES Cryptographic Provider” 3. 将新生成的.pfx 格式证书导入到浏览器或者 USB Key。
信任域	指定 PKI 信任域。当选用国密 SSL 标准，此处指定的 PKI 信任域需要包含用于国密 SSL 协商的 SM2 签名证书及其私钥。默认值为 trust_domain_default。
加密信任域	当选用国密 SSL 标准，此项配置为必选项，此处指定的加密 PKI 信任域需要包含用于国密 SSL 协商的 SM2 加密证书及其私钥。
加密算法	指定 ZTNA 隧道加密算法。<NULL>表示不使用加密功能。当使用国密 GMSSLv1.0 协议时，加密算法建议优先选择 SM4。默认值为 AES。
Hash 算法	指定 ZTNA 隧道验证算法。<NULL>表示不使用验证功能。当使用国密 GMSSLv1.0 协议时，hash 算法建议优先选择 SM3。默认值为 MD5。
压缩算法	指定 ZTNA 隧道压缩算法。默认无任何压缩算法。
客户端连接	
允许浏览器下载客户端	开启浏览器下载功能后，用户可以通过浏览器 Web 页面的方式下载 Secure Connect 客户端，默认情况下，该功能为开启状态。 说明：通过浏览器下载客户端的方法为：“https://IP-Address:Port-Number”，其中“IP-Address”为接入接口/隧道接口处配置的出接口的 IP 地址，“Port-Number”为此处配置的服务端口。
空闲时间	空闲时间指客户端与设备端在无流量状态下能够保持连接状态的最长时间，超出空闲时间后，设备端将断开与客户端的连接。单位为分钟，取值范围为 1 到 1500，默认值为 30。
允许同名登录	设备允许同一个用户在多个地点同时登录认证。选中“启用”按钮开启该功能。
同名登录数	输入允许同一个用户同时登录的个数，取值范围为 0 到 99999999，其中 0 表示不限制个数。默认值为 0。
高级参数	
防重放	防重放功能是指防止恶意用户通过重复发送捕获到的数据包所进行的攻击，即接收方会拒绝旧的或重复的数据包。默认值为 32。
DF 位	指定是否允许转发数据包的设备对数据包进行分片。包括： 设置 - 不允许转发设备对数据包分片。 拷贝 - 直接从发包端拷贝 IP 包的 DF 选项。该选项为系统默认选项。 清除 - 允许转发设备对包做分片处理。
数据端口（UDP）	ZTNA 连接建立后数据通讯的 UDP 端口号。取值范围为 1 到 65535。
数据端口（TCP）	ZTNA 连接建立后数据通讯的 TCP 端口号。取值范围为 1 到 65535。

点击“客户端”，填写相关配置信息。

客户端配置	
修改密码 URL	配置 URL 地址，用户可以从客户端跳转到指定 URL 页面修改密码，取值范围为 0 到 255 个字符。
忘记密码 URL	配置 URL 地址，用户可以从客户端跳转到指定 URL 页面重新设置密码，取值范围为 0 到 255 个字符。
重新定向 URL	URL 重定向功能是指在 ZTNA 设备端配置重定向的 URL，客户端认证成功后将自动跳转到指定 URL 的页面。在文本框中输入重定向的 URL 字符串，取值范围为 0 到 255 个字符。系统支持 HTTP（http://）和 HTTPS（https://）两种类型的 URL。根据重定向页面类型的不同，系统支持内容符合下列格式的 URL 输入，以 HTTP 类型 URL 为例： UTF-8 编码格式的页面 - 输入“URL”+“username=$USER&password=$PWD”。比如，http://www.abc.com/oa/login.do?usernam-e=$GBUSER&password=$PWD GB2312 编码格式的页面 - 输入“URL”+“username=$GBUSER&password=$PWD”。比如，http://www.abc.com/oa/login.do?usernam-e=$GBUSER&password=$PWD 其它页面 - 直接输入 URL。比如，http://www.abc.com
标题	指定重定向 URL 的描述，取值范围为 0 到 31 个字符。该名称会在客户端菜单项中显示。
客户端证书认证	
证书认证	点击“启用”按钮开启客户端证书认证功能。该功能支持“用户名/密码 + 数字证书”和“只用数字证书”两种认证方式。数字证书可以是软证书或 USB Key 证书。 当认证方式为“只用数字证书”时： 系统可以根据数字证书中的证书名称（证书 CN 字段）或者组织机构（证书 OU 字段）为认证成功的用户映射相应的角色。 系统不支持允许本地用户修改密码功能。 系统不支持配置短信口令认证功能。 如果使用 USB-Key 证书的用户移除了 UKey，客户端不会自动重连。
USB KEY 下载网址	当使用 USB Key 证书认证功能时，用户可以通过该地址，下载 UKey 对应的驱动程序。取值范围为 0 到 63 个字符。
信任域 主题名字检查 CN 匹配	信任域和主题名字检查功能配置方法如下： 1. 点击“新建”按钮，在“信任域”下拉菜单中选中用户 CA

客户端配置	
OU 匹配 USB KEY Download URL	（Certification Authority）证书所在的 PKI 信任域。客户端所提交的证书匹配到其中任意一个信任域的 CA 证书，都会认证成功。 2. 如需要，选中“主题名字检查”对应的<启用>复选框，启用主题名字检查功能。启用后，当用户通过数字证书认证功能登录时，设备端会检查客户端证书的主题名称（subject commonName）是否和登录用户的用户名一致。用户可另外指定是否匹配 CN 字段和 OU 字段。 3. 如需要，按照步骤 1 至 2 添加其它信任域和主题名字检查条目。如需要删除信任域和主题名字检查条目，从列表中选中需要删除的信任域和主题名字检查条目复选框，点击“删除”按钮。

点击“二次认证”，填写相关配置信息。

选项	说明
二次认证	点击“启用”按钮，当 ZTNA 用户使用用户名/密码或用户名/密码+数字证书方式登录时，收到登录请求的通过短信口令、令牌口令或者邮件口令的方式进行二次认证，用户输入收到的认证码后，才可以通过认证，进而访问内网资源。
类型	指定二次认证的类型，包括“短信口令认证”、“令牌口令认证”和“邮件口令认证”。 选择“短信口令认证”时，指定“短信猫”或“短信网关”并根据需要在下方配置选项中进行相关配置。 选择“令牌口令认证”时，根据需要输入提示信息，取值范围是 0 到 255 个字符。 选择“邮件口令认证”时，根据需要在下方配置选项中进行相关配置。
短信口令认证	
短信认证类型	指定短信口令认证的类型，包括“短信猫”和“短信网关”。
短信网关名称	在下拉菜单选择已创建的短信网关名称。
短信认证码有效时间	输入短信认证码有效时间，单位为分钟。取值范围是 1 到 10。默认值为 10。如果用户在有效时间内没有输入短信认证码也没有重新申请认证码，ZTNA 设备端将自动断开连接。
发送方名称	指定短信发送方名称以显示在短信内容中。取值范围是 0 到 63 字符。 注意: 由于 UMS 企业信息平台限制，当使用短信网关认证时，发送方名称将会显示在 UMS 企业信息平台注册的名称。
认证码长度	指定短信认证码的长度。取值范围为 4 至 8。默认为 8。
短信模板	指定认证码短信的验证内容，内容必须包含“$VRFYCODE”（用

选项	说明
	于获取认证码），“$USERNAME”和“EXPIRATION”为可选关键字。取值范围为 9 至 500 个字符。
签名	当短信网关名称指定为阿里云服务商名称时，用户需要输入阿里云短信服务中申请的短信签名，以显示在短信内容中。取值范围是 1 到 63 字符。该参数需与在阿里云短信服务中申请的签名保持一致。
模板 CODE	当短信网关名称指定为阿里云服务商名称时，用户需要输入阿里云短信服务中申请的短信内容模板对应的 CODE（代码）。取值范围为 1 至 30 个字符。该参数需与在阿里云短信服务中申请的模板 CODE 保持一致。
邮件口令认证	
邮件服务器	在下拉菜单中选择系统中已配置的邮件服务器；或者，点击“+”按钮，新建邮件服务器。关于邮件服务器的配置详情，请见配置邮件服务器。
邮件认证码有效时间	指定邮件认证码的有效时间，单位为分钟。取值范围为 1 至 10。默认为 10。每个邮件认证码都有一个有效时间，如果用户在有效时间内没有输入认证码也没有重新申请认证码，ZTNA 设备端将自动断开连接。
发送方名称	指定认证码的发送方名称以显示在邮件内容中。取值范围为 0 至 63 个字符。为防止认证码邮件被认定为垃圾邮件，建议用户进行认证码邮件发送方名称的配置。
认证码长度	指定邮件认证码长度。取值范围为 4 至 8。默认为 8。
邮件验证内容	指定认证码邮件的验证内容，内容必须包含“$USERNAME”和“$VRFYCODE”（“$USERNAME”用于获取用户名；“$VRFYCODE”用于获取认证码）。取值范围为 18 至 128 个字符。默认内容为“ZTNA user < $USERNAME> email verification code: $VRFYCODE. Do not reveal to anyone! If you did not request this, please ignore it.”。

点击“多网关地址配置”，填写相关配置信息。

选项	说明
当网络中有多台设备开启了 ZTNA 服务时，用户可以将这些设备的服务地址（出接口地址或域名）添加至网关地址列表中。当客户端与设备端建立 ZTNA 连接时，可以从列表中选择链路质量最优的地址建立连接。设备端配置了网关地址列表时，客户端可以开启网关探测功能选择需要连接的 ZTNA 网关。	
名称	点击“新建”按钮，在网关地址列表中添加一条网关地址配置。输入网关的名称，取值范围是 1 到 31 个字符。最多支持添加 24 个网关。当配置了多网关时，多网关上的 ZTNA 配置需和主网关上保持一致。
网关地址	指定多网关的 IPv4 地址或域名。域名的取值范围是 1 到 255 个字符，但是在两个句点（.）之间，最多可以有 63 个字符。

2. 点击“确定”，保存所做的配置。

管理终端信息项

终端信息项管理实现终端信息采集配置、终端信息收集脚本的生成和下发，以及终端状态的持续性监控。在客户端登录成功后和访问应用资源期间，设备端会持续监控终端状态，根据终端信息的变化更新终端标签和允许访问的应用资源，流程如下：

1. 客户端根据终端信息收集脚本，定期收集终端信息，并上报给设备端。客户端默认每 60 分钟收集和上报一次终端信息，该上报周期可以通过 **ztna-endpoint-information-monitor** 命令调整。
2. 设备端解析终端信息，若发生了变化，则重新获取终端标签，更新认证用户的终端标签，重新匹配 ZTNA 策略，更新认证用户可访问的应用资源，并根据 **session-rematch** 命令的配置对该用户的已有会话进行处理。

终端信息项包括预定义和自定义项。预定义项是系统默认收集的项目，不支持编辑。自定义项允许用户添加需要收集的项目，每种可以添加最多 5 条。通过配置自定义终端信息项，ZTNA 可以获取到更多的终端信息，实现更加精细的权限控制。

系统支持以下操作系统的终端信息管理

Windows 终端信息管理

macOS 终端信息管理

Linux 终端信息管理

iOS 终端信息管理

Android 终端信息管理

Windows 终端信息管理

管理 Windows 终端信息项，请按照以下步骤进行操作：

1. 点击“零信任访问 > 终端 > 终端信息 > Windows”。

2. 查看系统支持的预定义 Windows 终端信息项和配置自定义的 Windows 终端信息项。

Windows 终端信息项-预定义项

选项	说明
OS 版本	检查 Windows 终端的操作系统版本。点击“OS 版本”，显示系统支持检查的 Windows 版本信息，包括： Windows 7/8.1/10/11 Windows server 2008 R2/2012/2012 R2/2016/2019/2022
IE	检查 Windows 终端的 IE 版本和 IE 安全级别信息。点击“IE”，显示系统支持检查的 IE 版本和 IE 安全级别信息： IE 版本：IE7 ~ IE11 IE 安全级别：custom define、low、medium low、medium、medium high、high
安全中心	检查 Windows 终端的系统安全性。点击“安全中心”，显示系统支持检查的安全检查项： 防间谍软件是否安装、开启、更新 防病毒软件是否安装、开启、更新 防火墙是否安装、开启 windows 更新是否开启

Windows 终端信息项-自定义项

选项	说明
热补丁	检查 Windows 终端是否安装了指定的热补丁包。点击“热补丁”，在热补丁页面点击“新建”，输入需要收集的热补丁信息，点击“确定”保存配置。可以自定义最多 5 条需要收集的已安装热补丁包信息。 别名：指定热补丁包的别名，范围是 1 至 31 个字符。 热补丁：指定热补丁包的实际名称，范围是 1 至 255 个字符。
注册表项	检查 Windows 终端内是否存在指定的注册表项。点击“注册表项”，在注册表项页面点击“新建”，输入需要收集的注册表项信息，点击“确定”保存配置。可以自定义最多 5 条需要收集的注册表项信息。 别名：指定注册表项的别名，范围是 1 至 31 个字符。

选项	说明
	键值：指定注册表项的名称，范围是 1 至 255 个字符。填写内容为“路径+表项名”，以下图为例，键值填写内容为 HKEY_LOCAL_MACHINE\SOFTWARE\Tencent\WeDrive\UpdateStatus。 
文件	检查 Windows 终端内是否存在指定的文件。点击“文件”，在文件页面点击“新建”，输入需要收集的文件信息，点击“确定”保存配置。可以自定义最多 5 条需要收集的文件信息。 别名：指定文件的别名，范围是 1 至 31 个字符。 文件路径：指定文件的绝对路径，范围是 1 至 255 个字符。
运行进程	检查 Windows 终端是否正在运行指定的进程。点击“运行进程”，在运行进程页面点击“新建”，输入需要收集的进程信息，点击“确定”保存配置。可以自定义最多 5 条需要收集的运行进程信息。 别名：指定进程的别名，范围是 1 至 31 个字符。 运行进程：指定进程的实际名称，范围是 1 至 255 个字符。
安装服务	检查 Windows 终端是否安装了指定的服务。点击“安装服务”，在安装服务页面点击“新建”，输入需要收集的服务信息，点击“确定”保存配置。 可以自定义最多 5 条需要收集的安装服务信息。 别名：指定服务的别名，范围是 1 至 31 个字符。 安装服务：指定服务的实际名称，范围是 1 至 255 个字符。
运行服务	检查 Windows 终端是否正在运行指定的服务。点击“运行服务”，在运行服务页面点击“新建”，输入需要收集的服务信息，点击“确定”保存配置。可以自定义最多 5 条需要收集的运行服务信息。 别名：指定服务的别名，范围是 1 至 31 个字符。 运行服务：指定服务的实际名称，范围是 1 至 255 个字符。

macOS 终端信息管理

管理 macOS 终端信息项，请按照以下步骤进行操作：

1. 点击“零信任访问 > 终端 > 终端信息 > macOS”。

2. 查看系统支持的预定义 macOS 终端信息项和配置自定义的 macOS 终端信息项。

macOS 终端信息项-预定义项

选项	说明
OS 版本	检查 macOS 终端的操作系统版本。点击“OS 版本”，显示系统支持收集的 macOS 版本信息，包括： macOS High Sierra 10.13 macOS Mojave 10.14 macOS Catalina 10.15 macOS Big Sur 11 macOS Monterey 12 macOS Ventura 13
安全中心	检查 Windows 终端的系统安全性。点击“安全中心”，显示系统支持检查的安全检查项，即 FileVault 功能是否开启。

macOS 终端信息项-自定义项

选项	说明
AD 域	检查 macOS 终端的 AD 域名。点击“AD 域”，在 AD 域页面点击“新建”，输入需要收集的 AD 域信息，点击“确定”保存配置。 可以自定义最多 1 条需要收集的 AD 域名信息。 别名：指定 AD 域名的别名，范围是 1 至 31 个字符。 AD 域：指定 AD 域名，范围是 1 至 255 个字符。
文件	检查 macOS 系统内是否存在指定的文件。点击“文件”，在文件页面点击“新建”，输入需要收集的文件信息，点击“确定”保存配置。 可以自定义最多 5 条需要收集的文件信息。

选项	说明
	别名：指定文件的别名，范围是 1 至 31 个字符。 文件路径：指定文件的绝对路径，范围是 1 至 255 个字符。
运行进程	检查 macOS 系统是否正在运行指定的进程。点击“运行进程”，在运行进程页面点击“新建”，输入需要收集的正在运行进程信息，点击“确定”保存配置。 可以自定义最多 5 条需要收集的运行进程信息。 别名：指定进程的别名，范围是 1 至 31 个字符。 运行进程：指定进程的实际名称，范围是 1 至 255 个字符。
安装服务	检查 macOS 系统是否安装了指定的服务。点击“安装服务”，在安装服务页面点击“新建”，输入需要收集的已安装服务的信息，点击“确定”保存配置。 可以自定义最多 5 条需要收集的已安装服务信息。 别名：指定服务的别名，范围是 1 至 31 个字符。 安装服务：指定服务的实际名称，范围是 1 至 255 个字符。
运行服务	检查 macOS 系统是否正在运行指定的服务。点击“运行服务”，在运行服务页面点击“新建”，输入需要收集的正在运行服务的信息，点击“确定”保存配置。 可以自定义最多 5 条需要收集的运行服务信息。 别名：指定服务的别名，范围是 1 至 31 个字符。 运行服务：指定服务的实际名称，范围是 1 至 255 个字符。

Linux 终端信息管理

管理 Linux 终端信息项，请按照以下步骤进行操作：

1. 点击“零信任访问 > 终端 > 终端信息 > Linux”。

2. 查看系统支持的预定义 Linux 终端信息项和配置自定义的 Linux 终端信息项。

Linux 终端信息项-预定义项

选项	说明
OS 版本	收集 Linux 操作系统的版本信息。点击“OS 版本”，显示系统支持收集的 Linux 版本信息，包括： CentOS 7.6/7.7/7.8/7.9/8.0/8.1/8.2/8.3/8.4/8.5 Ubuntu 18.04/18.10/19.04/19.10/20.04/20.10/21.04 Ubuntu Kylin 18.04/20.04

Linux 终端信息项-自定义项

选项	说明
文件	检查 Linux 系统内是否存在指定的文件。点击“文件”，在文件页面点击“新建”，输入需要收集的文件信息，点击“确定”保存配置。 可以自定义最多 5 条需要收集的文件信息。 别名：指定文件的别名，范围是 1 至 31 个字符。 文件路径：指定文件的绝对路径，范围是 1 至 255 个字符。
运行进程	检查 Linux 系统是否正在运行指定的进程。点击“运行进程”，在运行进程页面点击“新建”，输入需要收集的正在运行进程信息，点击“确定”保存配置。 可以自定义最多 5 条需要收集的运行进程信息。 别名：指定进程的别名，范围是 1 至 31 个字符。 运行进程：指定进程的实际名称，范围是 1 至 255 个字符。
安装服务	检查 Linux 系统是否安装了指定的服务。点击“安装服务”，在安装服务页面点击“新建”，输入需要收集的已安装服务的信息，点击“确定”保存配置。 可以自定义最多 5 条需要收集的已安装服务信息。 别名：指定服务的别名，范围是 1 至 31 个字符。 安装服务：指定服务的实际名称，范围是 1 至 255 个字符。
运行服务	检查 Linux 系统是否正在运行指定的服务。点击“运行服务”，在运行服务页面点击“新建”，输入需要收集的正在运

选项	说明
	行服务的信息，点击“确定”保存配置。 可以自定义最多 5 条需要收集的运行服务信息。 别名：指定服务的别名，范围是 1 至 31 个字符。 运行服务：指定服务的实际名称，范围是 1 至 255 个字符。

iOS 终端信息管理

管理 iOS 终端信息项，请按照以下步骤进行操作：

1. 点击“零信任访问 > 终端 > 终端信息 > iOS”。

2. 查看系统支持的预定义 iOS 终端信息项和配置自定义的 iOS 终端信息项。

iOS 终端信息项-预定义项

选项	说明
OS 版本	收集 iOS 操作系统的版本信息。点击“OS 版本”，显示系统支持收集的 iOS 版本信息，包括 iOS 12/13/14/15/16。

iOS 终端信息项-自定义项

选项	说明
设备型号	收集 iOS 终端设备的型号。点击“设备型号”，在设备型号页面点击“新建”，输入需要收集的设备型号信息，点击“确定”保存配置。 可以自定义最多 5 条需要收集的 iOS 终端设备型号信息。 别名：指定 iOS 终端设备型号的别名，范围是 1 至 31 个字符。 设备型号：指定 iOS 终端设备型号，范围是 1 至 255 个字符。
连接的 WiFi	收集 iOS 终端所连接的 WiFi SSID。点击“连接的 WiFi”，在连接的 WiFi 页面点击“新建”，输入需要收集的 WiFi SSID 信息，点击“确定”保存配置。 可以自定义最多 5 条需要收集的 WiFi SSID 信息。

选项	说明
	别名：指定 WiFi SSID 的别名，范围是 1 至 31 个字符。 连接的 WiFi：指定 WiFi SSID，范围是 1 至 255 个字符。
客户端版本	收集 iOS 终端使用的客户端版本。点击“客户端版本”，在客户端版本页面点击“新建”，输入需要收集的客户端版本信息，点击“确定”保存配置。 可以自定义最多 5 条需要收集的客户端版本信息。 别名：指定客户端版本的别名，范围是 1 至 31 个字符。 客户端版本：指定客户端版本，范围是 1 至 255 个字符。

Android 终端信息管理

管理 Android 终端信息项，请按照以下步骤进行操作：

1. 点击“零信任访问 > 终端 > 终端信息 > Android”。

2. 查看系统支持的预定义 Android 终端信息项和配置自定义的 Android 终端信息项。

Android 终端信息项-预定义项

选项	说明
OS 版本	收集 Android 操作系统的版本信息。点击“OS 版本”，显示系统支持收集的 Android 版本信息，包括 Android 8/9/10/11/12/13。

Android 终端信息项-自定义项

选项	说明
设备型号	收集 Android 终端设备的型号。点击“设备型号”，在设备型号页面点击“新建”，输入需要收集的设备型号信息，点击“确定”保存配置。 可以自定义最多 5 条需要收集的 Android

选项	说明
	终端设备型号信息。 别名：指定 Android 终端设备型号的别名，范围是 1 至 31 个字符。 设备型号：指定 Android 终端设备型号，范围是 1 至 255 个字符。
连接的 WiFi	收集 Android 终端所连接的 WiFi SSID。点击“连接的 WiFi”，在连接的 WiFi 页面点击“新建”，输入需要收集的 WiFi SSID 信息，点击“确定”保存配置。 可以自定义最多 5 条需要收集的 WiFi SSID 信息。 别名：指定 WiFi SSID 的别名，范围是 1 至 31 个字符。 连接的 WiFi：指定 WiFi SSID，范围是 1 至 255 个字符。
客户端版本	收集 Android 终端使用的客户端版本。点击“客户端版本”，在客户端版本页面点击“新建”，输入需要收集的客户端版本信息，点击“确定”保存配置。 可以自定义最多 5 条需要收集的客户端版本信息。 别名：指定客户端版本的别名，范围是 1 至 31 个字符。 客户端版本：指定客户端版本，范围是 1 至 255 个字符。

配置终端标签

终端标签用于标识用户的终端状态信息，系统会根据用户携带的终端信息为其打上相应的终端标签，这些标签会被用作 ZTNA 策略的匹配条件。带有特定标签的用户只能获取指定资源的访问权限，从而实现对用户访问权限的检查和控制。

终端标签由一个或多个条件组构成，条件组由一个或多个条件构成。系统支持配置最多 1024 个终端标签。

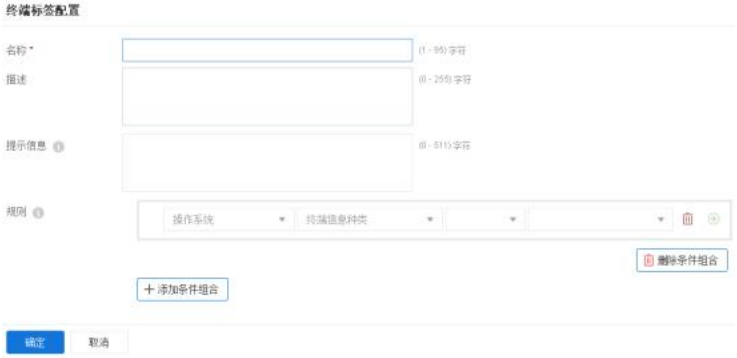
条件组之间是逻辑“或”关系，用户携带的终端标签匹配终端标签中的任意一个条件组，即认为是匹配了这条终端标签。

每个条件组内的各个条件之间是逻辑“与”关系，用户携带的终端标签同时匹配了某一条件组中的所有条件，才认为是匹配了这个条件组。

配置 ZTNA 终端标签，按照以下 步骤进行操作：

1. 点击“零信任访问 > 终端 > 终端标签”，进入终端标签页面。

2. 点击“新建”按钮，打开<终端标签配置>页面。



在<终端标签配置>页面填写终端标签配置信息。

选项	说明
名称	输入终端标签的名称。范围是 1 到 95 个字符。
描述	输入终端标签的描述信息。范围是 0 到 255 个字符。
提示信息	指定在 ZTNA Portal 页面上展示的提示信息。取值范围是 0 到 511 个字符。对于因为不匹配终端标签而无权限访问的应用资源，配置提示信息可以使终端用户了解不能访问的原因，从而通过更新自己的终端配置来获得访问应用资源的权限。提示信息中支持包含 URL 地址，展示在 ZTNA Portal 上时将显示为超链接。默认的提示信息是“无法访问！请联系 IT 管理员！”。当一条 ZTNA 策略绑定多个终端标签时： 如果用户匹配任意一个终端标签且具有应用资源的访问权限，ZTNA Portal 上对应应用资源将不展示任何提示信息。 如果用户因为不匹配任意一个终端标签而无法访问应用资源，ZTNA Portal 上对应应用资源将汇总展示所有终端标签的提示信息。如果所有终端标签都未配置提示信息，则展示默认提示信息。
规则	指定终端标签的条件组和条件，每个终端标签可以添加最多 16 个条件组和 16 个条件。
添加条件组合	点击“添加条件组合”按钮，为终端标签添加一个条件组，并配置组内包含的条件。如需要，可点击该按钮添加更多条件组。
操作系统	指定操作系统类型，支持 windows、macOS、Linux、iOS 和 Android。
终端信息种类	指定终端信息项名称，此处包括系统支持的所有预定义和自定义终端信息项。选择终端信息项之后，指定关系运算符和取值。

选项	说明
	自定义终端信息项的取值需要通过“零信任访问 > 终端 > 终端信息”提前配置或点击下拉菜单中的添加按钮新建。如需要，点击“+”按钮可以新建多个条件；点击“删除”按钮，可以删除选定的条件；点击“删除条件组合”按钮，可以删除一个条件组。

3. 点击“确定”，保存配置。

4. 在标签页面，可以查看到所有标签的配置信息和被 ZTNA 策略引用的次数。点击被引用数，在弹出的对话框中，可以查看终端标签被哪些 ZTNA 策略引用。点击策略 ID，可以查看 ZTNA 策略的详细配置信息。

在<标签>页面，对标签进行管理。

选项	说明
过滤	从下拉菜单中选择过滤条件，输入过滤条件，标签列表将展示匹配指定条件的标签。
编辑	点击此按钮修改选中的标签的配置。
删除	点击此按钮删除选定的标签。

配置应用资源/应用资源组

应用资源用于定义用户需要访问的应用、内容、服务等资源，用户需要通过配置地址、协议、端口等来指定一个应用资源条目。应用资源组用于定义一组应用资源。系统支持配置最多 256 个应用资源，64 个应用资源组。

系统支持以下方式配置应用资源条目：

基于 IP 地址、协议、端口

基于 IP 范围、协议、端口

基于域名、协议、端口

配置应用资源，按照以下步骤进行操作：

1. 点击“对象 > 应用资源簿 > 应用资源”，或点击“零信任访问 > 应用资源簿 > 应用资源”，进入应用资源页面。

2. 点击“新建”按钮，打开<应用资源配置>页面。

在<应用资源配置>页面填写应用资源基本信息。

选项	说明
名称	输入应用资源的名称。范围是 1 到 95 个字符。
超链接	输入应用资源的 URL 地址，范围是 0 到 2047 个字符。在用户登录后展示的 ZTNA Portal 页面上，配置了超链接的应用资源，用户可以复制链接到浏览器访问，也可以直接点击图标实现快速访问（需确保链接有效）。不配置超链接的应用资源不会展示在 Portal 页面上。如果超链接中未指定协议类型，默认使用 HTTP 协议。关闭 Portal 页面后，用户可以通过客户端菜单的“应用资源列表”选项重新打开最新的 Portal 页面查看应用资源的访问权限。Portal 页面上展示用户有权限和无权限访问的应用资源。对于无权限访问的应用资源，用户在调整终端配置后，可以获得访问权限。禁止访问的应用资源不在 Portal 页面上展示，如果用户被禁止访问任何应用资源，Portal 页面将展示“无可用的 Web 服务资源”。
规则描述	点击“新建”按钮为应用资源添加一个条目。每个应用资源可以添加最多 16 个条目。在“应用资源规则配置”页面，指定条目信息。 类型：指定应用资源条目的类型，包括 IPv4/掩码、IPv6/前缀长度、IPv4 范围、IPv6 范围、域名。 地址：指定应用资源条目的 IP 地址或 IP 地址范围。 域名：指定应用资源条目的域名，取值范围是 1 到 255 个字符，且在两个点号（.）之间最多可以有 63 个字符。支持设置精确域名和以“*”作为第一个字符的通配域名。 协议：指定应用资源条目的协议类型。基于 IP 地址定义应用资源条目时，协议类型支持 TCP 和 UDP；基于域名定义应用资源条目时，协议类型支持 HTTP 或 HTTPS。 端口：指定应用资源条目的端口号。范围为 1 至 65535。 超时：指定应用资源条目的超时时间，单位为可以为秒或天。单位为秒时，取值范围是 1 到 65535。单位为天时，取

选项	说明
	值范围是 1 到 1000。协议类型为 TCP/HTTP/HTTPS 时，默认是 1800 秒，协议类型为 UDP 时，默认是 60 秒。
描述	指定应用资源的描述信息。范围为 0 至 255 个字符。

3. 点击“确定”，保存配置。

4. 在应用资源页面，点击列表里的“+”展开一个应用资源，可以查看到该应用资源的更多信息，包括所属的应用资源组、引用的 ZTNA 策略。

在应用资源页面，对应用资源进行管理。

选项	说明
过滤	从下拉菜单中选择过滤条件，应用资源列表将展示匹配指定条件的应用资源。
编辑	点击此按钮修改选中的应用资源的的配置。
删除	点击此按钮删除选定的应用资源。

配置应用资源组，按照以下步骤进行操作：

1. 点击“对象 > 应用资源簿 > 应用资源组”或点击“零信任访问 > 应用资源簿 > 应用资源组”，进入应用资源组页面。

2. 点击“新建”按钮，打开<应用资源组>配置页面。

在<应用资源组配置>页面填写应用资源组基本信息。

选项	说明
名称	输入应用资源组的名称。范围是 1 到 95 个字符。
应用资源	选择系统已配置的应用资源。或者，点击“+”按钮，在弹出的<应用资源配置>对话框里新建一个应用资源。最多可以添加 16 个应用资源。
描述	指定应用资源的描述信息。范围为 0 至 255 个字符。

3. 点击“确定”，保存配置。

4. 在应用资源组页面，点击列表里的“+”展开一个应用资源组，可以查看到该应用资源组的更多信息，包括引用的 ZTNA 策略 ID。

在<应用资源组>页面，对应用资源组进行管理。

选项	说明
名称	输入应用资源组名称，列表将展示匹配指定名称的应用资源组，支持部分匹配和全部匹配。
编辑	点击此按钮修改选中的应用资源组的配置。
删除	点击此按钮删除选定的应用资源组。

配置 ZTNA 策略

ZTNA 通过配置策略对用户的访问进行控制。策略中需要指定匹配条件和控制动作，策略支持以下维度作为匹配条件：

用户/用户组：当用户的用户名/用户组和 ZTNA 策略中绑定的用户名/用户组匹配时，即命中了该维度。

终端标签：当用户携带的终端标签和 ZTNA 策略中绑定的终端标签匹配时，即命中了该维度。

应用资源/应用资源组：当用户请求访问的应用资源/应用资源组和 ZTNA 策略中绑定的应用资源匹配时，即命中了该维度。

时间表：当用户的访问时间和 ZTNA 策略中绑定的时间表匹配时，即命中了该维度。

在一条 ZTNA 策略中，可以配置一个或多个上述维度作为匹配条件。当配置多个维度时，需要同时匹配所有维度，才会命中策略并按照策略规定的控制动作处理流量。当某个维度未配置时，表示该维度可以匹配任意对象。策略的控制动作包括两种（必须配置一种）：

permit：当流量匹配指定的 ZTNA 策略时，允许访问策略中绑定的应用资源。

deny：当流量匹配指定的 ZTNA 策略时，拒绝访问策略中绑定的应用资源。

如果流量未匹配到任何 ZTNA 策略，会命中 ZTNA 默认策略，按照默认策略里配置的控制动作处理。

配置 ZTNA 策略，按照以下步骤进行操作：

1. 点击“零信任访问 > 策略”，进入策略页面。

2. 点击“新建”按钮，打开<策略配置>页面。

在<策略配置>页面填写策略基本信息。

选项	说明
名称	输入策略的名称。范围是 1 到 95 个字符。
用户	指定需要绑定的用户/用户组。 AAA 服务器名称：指定用户/用户组所属的 AAA 服务器。在下拉列表中选择系统已配置的 AAA 服务器；或者，点击“+”按钮，选择认证服务器类型后，在弹出的对话框中新建一个认证服务器。 选择用户/选择用户组：选择系统中已配置的用户和用户组；或者点击“+”按钮，在弹出的<用户配置>或<用户组配置>对话框中新建用户或用户组。 输入用户/输入用户组：输入用户名或用户组名，然后点击“添加”按钮。 用户名的范围为 1 至 63 个字符；用户组名范围为 1 至 127 个字符。最多可以添加 8 个用户和 8 个用户组。 多个用户/用户组之间是逻辑“或”的关系，其中的任何一个用户访问时，即认为匹配了该条策略的用户/用户组维度。当策略中不绑定用户/用户组时，表示所有用户/用户组都可以匹配。
终端标签	指定需要绑定的终端标签。在下拉列表中选择系统已配置的终端标签；或者点击“+”按钮，在弹出的<终端标签配置>对话框里新建一个终端标签。每个策略支持绑定最多 10 个终端标签。多个终端标签之间是逻辑“或”的关系，用户匹配其中的任何一个终端标签，即认为命中了该条策略的终端标签维度。当策略中不绑定任何终端标签时，表示所有终端标签都可以匹配。

选项	说明
应用资源	指定需要绑定的应用资源/应用资源组名称。在下拉列表中选择系统已配置的应用资源或应用资源组；或者，点击“+”按钮，在弹出的<应用资源配置>或<应用资源组配置>对话框里新建一个应用资源或应用资源组。每个策略支持绑定最多 10 个应用资源和 10 个应用资源组。策略中绑定的多个应用资源或应用资源组之间是逻辑“或”关系，用户访问其中的任何一个应用资源，即认为命中了这条策略的应用资源维度。当策略中不绑定应用资源时，可以匹配所有应用资源。
动作	指定对匹配策略的用户流量执行指定的控制动作，即允许或拒绝访问策略中绑定的应用资源。

点击“防护状态”，可以为策略添加威胁防护配置。

选项	说明
病毒过滤	当系统安装了病毒过滤许可证时，点击启用病毒过滤功能，为 ZTNA 策略绑定病毒过滤规则，对匹配 ZTNA 策略的流量实现多种病毒威胁的探测，并根据病毒过滤规则的配置对发现的病毒进行处理。
入侵防御	当系统安装了入侵防御许可证时，点击启用入侵防御功能，为 ZTNA 策略绑定入侵防御规则，对匹配 ZTNA 策略的流量实现多种网络攻击的探测，并根据入侵防御规则的配置对网络攻击执行阻断等操作。
沙箱防护	当系统安装了沙箱防护许可证时，点击启用沙箱防护功能，为 ZTNA 策略绑定沙箱防护规则，对匹配 ZTNA 策略的流量实现沙箱防护检查。通过云 · 影或智影，对可疑文件进行分析，搜集可疑文件的动态行为，判断文件合法性，将分析结果反馈给系统，并根据沙箱防护规则的配置对恶意文件进行处理。

点击“数据安全”，可以为策略添加数据安全配置。

选项	说明
文件过滤	点击启用文件过滤功能，为 ZTNA 策略绑定文件过滤规则，对匹配 ZTNA 策略的流量实现文件检测，并根据文件过滤规则的配置对符合过滤条件的文件进行控制。
文件内容过滤	点击启用文件内容过滤功能，为 ZTNA 策略绑定文件内容过滤规则，对匹配 ZTNA 策略的流量实现文件内容检测，并根据文件内容过滤规则的配置执行记录日志或者阻断动作。

点击“选项”，可以对策略进行高级配置。

选项	说明
时间表	指定需要匹配的时间表；在下拉列表选择系统已配置的时间表；或者，点击“+”按钮，在弹出的<时间表配置>对话框里新建一个时

选项	说明
	间表。每个策略支持添加最多 10 个时间表。多个时间表之间是逻辑“或”关系，匹配其中的任何一个时间表，即认为命中了该条策略的时间表维度。策略中不绑定任何时间表时，表示所有时间都匹配。
记录日志	用户可以根据需要，通过系统日志信息记录 ZTNA 流量对策略的匹配情况，可多选： 策略拒绝：勾选“策略拒绝”复选框，开启记录 ZTNA 会话拒绝日志信息。 会话开始：勾选“会话开始”复选框，开启记录 ZTNA 会话建立日志信息。 会话结束：勾选“会话结束”复选框，开启记录 ZTNA 会话结束日志信息。
列表位置	选择 ZTNA 策略在所有策略中的位置。每一条 ZTNA 策略规则都有唯一的 ID 号。ZTNA 流量进入设备时，设备对 ZTNA 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， 策略页面上的显示顺序才是 ZTNA 策略的查找顺序。ZTNA 策略的排列位置可以是绝对位置，即列表最前或者列表最后，也可以是相对位置，即位于某个 ID 或名称之前或之后。默认位置为列表最后。
描述	指定策略描述信息。范围是 0 到 255 个字符。

1. 点击“确定”，保存配置。
2. 在策略页面，可以查看到所有策略的配置信息，对策略进行管理。

在<策略>页面，对策略进行管理。

选项	说明
过滤	从下拉菜单中选择过滤条件，策略列表将展示匹配指定条件的策略。
编辑	点击此按钮修改选中的策略的配置。
删除	点击此按钮删除选定的策略。
复制、粘贴	选择策略，点击“复制”，然后点击“粘贴”，从下拉列表选择位置，可以增加一条具有同样配置的策略，并将新增的策略置于指定的位置。
移动	选择策略，点击“移动”，从下拉列表选择位置，可以修改策略位置。

点击“┆”，选择相关配置。

选项	说明
启用	选择处于禁用状态的策略后，选择“启用”可以启用策略。
禁用	选择处于启用状态的策略后，选择“禁用”可以禁用策略。
策略默认动作	指定对不匹配任何 ZTNA 策略的流量执行的控制动作。选择该选项后，在弹出的对话框中，可以查看到默认策略的统计信息，并配置控制动作和日志功能。 默认动作：允许或拒绝。 日志：点击此按钮可以开启默认策略的日志功能。
命中数清零	选择该选项后，在弹出的对话框中，可以选择对所有策略、默认策略、指定 ID、指定名称的策略相关统计信息清零。

配置接入地址池

设备端通过地址池给客户端分配 IP 地址。当客户端连接设备端成功后，设备端会从地址池里取出一个 IP 地址与其它相关参数（如 DNS 服务器地址与 WINS 服务器地址等）一起分配给客户端。

设备端通过创建和执行 IP 地址绑定规则来满足客户端的固定 IP 地址需求。IP 地址绑定规则包括 IP 用户绑定规则和 IP 角色绑定规则。IP 用户绑定规则将客户端用户与已配置地址池中的某个固定 IP 地址绑定，当客户端连接成功后，设备端会将绑定的 IP 地址分配给客户端；IP 角色绑定规则是将角色与已配置地址池中的某一 IP 地址范围绑定，当此客户端连接成功后，设备端会从绑定的地址范围中取出一个 IP 地址分配给客户端。

当设备端通过地址池给客户端分配 IP 地址时，系统会按照一定的顺序对客户端的 IP 地址绑定规则进行检查，决定如何为客户端分配 IP 地址。

检查是否已为客户端用户配置 IP 用户绑定规则，如果是，则将绑定的 IP 地址分配给客户端；否则，从非绑定地址范围中取出一个未被占用的 IP 分配给客户端。

检查是否已为客户端用户配置 IP 角色绑定规则，如果是，则从绑定的地址范围中取出一个 IP 地址分配给客户端；否则，从非绑定地址范围中取出一个未被占用的 IP 分配给客户端。

> 注意: IP 用户绑定规则中的 IP 地址和 IP 角色绑定规则中的 IP 地址不能重叠。

配置接入地址池，按照以下步骤进行操作：

1. 点击“对象 > 接入地址池”，进入接入地址池页面。
2. 选择“IPv4”或“IPv6”标签页，仅当该版本为 IPv6 版本时可配。

3. 点击“新建”按钮，打开<接入地址池配置> 页面。

在<接入地址池配置>标签页，填写配置信息。

基本配置	
接入地址池名称	指定地址池名称。
起始 IP	指定地址池的起始 IP 地址。
终止 IP	指定地址池的终止 IP 地址。
保留起始 IP	指定保留地址池的起始 IP 地址。
保留终止 IP	指定保留地址池的终止 IP 地址。
子网掩码	当创建的地址池类型为 IPv4 时，指定网络掩码。
前缀长度	当创建的地址池类型为 IPv6 时，指定 IPv6 地址前缀长度。取值范围是 111 到 128。该选项仅当该版本为 IPv6 版本时可配。
DNS1/DNS2/DNS3/DNS4	指定地址池的 DNS 服务器 IP 地址。此项为可选项，即地址池可以不指定 DNS 服务器。用户最多可以为每个地址池指定 4 个 DNS 服务器。
WINS1/WINS2	指定地址池的 WINS 服务器 IP 地址。此项为可选项，即地址池可以不指定 WINS 服务器。用户最多可以为每个地址池指定 2 个 WINS 服务器。仅在创建的地址

基本配置	
	池类型为 IPv4 时可配。
IP 用户绑定	
新建	点击“新建”按钮，将用户与 IP 地址的绑定条目添加到列表中。
用户	输入用户名称。
IP	输入 IP 地址。
删除	点击“删除”按钮删除选中的绑定条目。
IP 角色绑定	
新建	点击“新建”按钮，将角色与 IP 地址的绑定条目添加到列表中。
角色	输入角色名称。
起始 IP 地址	输入起始 IP 地址。
终止 IP 地址	输入终止 IP 地址。
删除	点击“删除”按钮删除选中的绑定条目。

4. 点击“确定”按钮，保存所做的配置。

对于绑定到多个角色且多个角色有相应的角色-IP 地址绑定规则的用户，系统会对角色-IP 地址绑定规则进行顺序查找，然后按照查找到的相匹配的第一条规则为用户分配地址。如需改变已有的角色-IP 地址绑定规则的排列顺序，在<接入地址池>页面，选择一个地址池后，点击“IP 角色调序”。在 IP 角色调序对话框里，选择需要调整的角色名称，点击“上移/下移/移到最前/移到最后”。

配置单包授权（SPA）

SPA（Single Packet Authorization，单包授权）是一种通用的访问技术理念，主要目的是将主机端口隐藏，因此也隐藏了主机上运行的服务。只有携带正确信息的报文，系统才会对其开放端口，否则不做回应。

ZTNA 设备端支持开启 SPA 并将 ZTNA 服务 IP 和端口隐藏，访问 ZTNA 服务的客户端也需要开启 SPA，通过单包授权。配置 SPA 后，ZTNA 用户通过客户端登录时的 SPA 流程如下：

1. 客户端向 ZTNA 设备端发送敲门报文，目的端口为敲门端口。
2. ZTNA 设备端检查敲门报文的目的 IP，如果目的 IP 不是隐藏 IP 会丢弃报文。如果是隐藏 IP 会对校验通过的敲门报文生成包含目的 IP、目的端口和源 IP 的放行表项。
3. 客户端发送 ZTNA 连接请求。
4. ZTNA 设备端检查连接请求的 IP 和端口是隐藏 IP 和端口。如果是隐藏 IP 和端口，则查询是否存在匹配的放行表项。如果存在，则允许建立 ZTNA 连接。如果不存在会丢弃报文。

为 ZTNA 配置 SPA，请按照以下步骤操作：

1. 点击“零信任访问 > SPA > SPA 配置”。

在<SPA 配置>页面填写以下信息。

选项	说明
启用	点击启用 SPA 功能。SPA 功能默认为关闭状态。在开启 SPA 功能时，需配置隐藏的 IP 和端口，SPA 功能才会生效。当设备端关闭 SPA 或开启了 SPA 但未配置隐藏 IP 和端口时，无论客户端是否开启 SPA，设备端都不会对客户端进行 SPA 校验。
端口	指定 ZTNA 设备端接收敲门报文的端口号。取值范围是 1025 到 65535，默认值是 60001。
隐藏地址	点击“新建”按钮创建隐藏地址。 IP：指定需要隐藏的 IPv4 地址，即在接入接口/隧道接口中配置的出接口的 IPv4 地址。 端口：指定需要隐藏的端口，即在接入接口/隧道接口中配置的服务端口。取值范围是 1 到 65535。 虚拟路由器：指定隐藏 IP 所在接口所属的虚拟路由器名称。 描述：指定隐藏地址的说明信息。取值范围是 0 到 63 个字符。

2. 点击“确定”，保存配置。

查看 ZTNA 设备端生成的 SPA 放行表项，点击“零信任访问 > SPA > SPA 列表”：

客户端 IP：表示客户端的源 IP 地址。

服务 IP：表示需要隐藏的 IP 地址，也是客户端访问的目的 IP。

虚拟路由器：表示隐藏 IP 所在接口所属的虚拟路由器名称。

端口：表示需要隐藏的端口，也是客户端访问的目的端口。

生存时间（秒）：表示放行表项的超时时间。超时时间到期后，放行表项会被删除。

ZTNA Portal

ZTNA 用户登录成功后，用户终端会通过默认浏览器弹出 ZTNA Portal 页面，展示用户有权限和无权限访问的应用资源。

有权限访问：当用户的认证信息和终端标签匹配动作类型为 Permit 的 ZTNA 策略时，用户有权限访问策略中绑定的应用资源。

无权限访问：当用户的认证信息匹配 ZTNA 策略，但终端标签不匹配 ZTNA 策略时，用户无权限访问策略中绑定的应用资源。

对于有权限访问的应用资源，用户可以通过点击应用资源图标跳转到相应的 URL 地址，或者复制 URL 地址到浏览器访问。对于无权限访问的应用资源，用户可以查看提示信息了解无权限访问的原因。

ZTNA Portal 页面不展示以下应用资源：

禁止用户访问的应用资源

允许用户访问，但未指定超链接的应用资源

在 ZTNA Portal 页面关闭后，用户可以通过 ZTNA 客户端的“应用资源列表”菜单重新获取 ZTNA Portal 页面。

监控

点击“零信任访问 > 监控 > 概览”页面，进入 ZTNA 监控页面。

ZTNA 授权使用情况

点击刷新图标获取实时的 ZTNA 授权统计。

在根 VSYS 下，用户可以查看到整机的 ZTNA 授权总数、使用量和剩余可用数量。使用量即为所有 VSYS 的使用量总和，包含 SCVPN 和 ZTNA 用户所使用的 ZTNA 授权数量。

在非根 VSYS 下，用户可以查看到所有 VSYS 可以共享的 ZTNA 授权总数以及所有 VSYS 已使用的 ZTNA 授权总数。

在线终端总数

ZTNA 用户上线后，系统会定时采集用户终端信息，通过匹配终端标签规则生成用户的终端标签。一个用户终端可能会命中 0 个或多个终端标签。在线终端总数实时统计，包含有终端标签的终端数和无终端标签的终端数的统计。

点击刷新图标获取实时的在线终端数统计。

终端标签命中数 Top 10

一个终端标签可能会被命中 0 次或多次。终端标签命中数 Top10 显示自系统运行以来命中数排名前 10 的终端标签名称，并按命中数从高到低排列。

点击刷新图标获取实时排名。

用户流量 Top 10

用户流量是指 ZTNA 用户访问应用资源后产生的数据交互，包含总流量、上行流量和下行流量。查看用户流量统计，需开启“零信任访问监控”开关。

用户可以查看到实时的用户流量统计以及最近一小时、最近一天、最近一月内流量排名前 10 的用户。

点击“上行流量”、“下行流量”。当“上行流量”图标变成灰色时，可以查看下行流量排名前 10 的用户。当“下行流量”图标变成灰色时，可以查看上行流量排名前 10 的用户。默认按照总流量排名。

点击刷新图标获取实时排名。

注意：该功能依赖于监控统计集的配置。若需查看用户流量 Top10，请确保在“监控 > 监控配置”页面已开启“用户监控”功能并勾选“带宽”统计项。

在线用户查看和管理

查看和管理 ZTNA 在线用户的状态，请按照以下步骤进行操作：

1. 点击“零信任访问 > 监控 > 用户状态”。
    a. 登录时间：表示在线用户的登录时间。
    b. 用户名：表示在线用户的用户名。
    c. AAA 服务器：表示在线用户所属的 AAA 服务器名称。
    d. ZTNA 服务：表示在线用户访问的 ZTNA 服务名称。
    e. 用户 IP：表示 ZTNA 设备端分配给在线用户的私网 IP 地址。
    f. 终端名称：表示访问终端的名称。
    g. 终端 IP：表示访问终端的 IP 地址，即用户的公网 IP 地址。
    h. 操作系统：表示访问终端的操作系统。
    i. 终端标签：表示在线用户关联的终端标签。
    j. 允许访问的应用资源：表示允许在线用户访问的应用资源。
    k. 禁止访问的应用资源：表示禁止在线用户访问的应用资源。
    l. 上行速率：表示在线用户的上传速率。
    m. 下行速率：表示在线用户的下载速率。
2. 点击 

按钮添加过滤条件，查看符合过滤条件的在线用户信息。
3. 选择一个或多个用户，点击“强制下线”，强制断开用户与 ZTNA 设备的连接。

注意：查看“上行速率”和“下行速率”统计，需开启“零信任访问监控”开关。

终端标签日志

系统支持配置终端标签日志功能对终端标签日志单独管理。配置和管理终端标签日志功能，请按照以下步骤操作：

1. 点击“监控 > 日志 > 终端标签日志”或点击“零信任访问 > 终端标签日志”。
    时间：表示终端标签日志的生成时间。

类型：表示终端标签日志的类型，包括登录、登出、异常登出、强制下线、终端标签更新、应用资源更新。

用户名：表示用户名。

用户 IP：表示用户 IP 地址。

AAA 服务器：表示用户所属的 AAA 服务器名称。

终端名称：表示访问终端的名称。

终端 IP：表示访问终端的 IP 地址。

操作系统：表示访问终端的操作系统。

终端标签：表示用户关联的终端标签。

ZTNA 服务：表示用户访问的 ZTNA 服务名称。

允许访问的应用资源：表示允许用户访问的应用资源。

禁止访问的应用资源：表示禁止用户访问的应用资源。

2. 点击“配置”按钮，打开<终端标签日志>页面。

在<终端标签日志>页面配置相关参数

选项	说明
启用	点击开启系统的终端标签日志功能，并设置终端标签日志的输出目的地，可以设置多个目的地。终端标签日志功能默认为开启，日志输出目的地为缓存内存。
缓存	选中该复选框将终端标签日志信息输出到内存缓存。
最大缓存大小	设置了输出终端标签日志到内存缓存时，用户可以自定义最大缓存大小，取值范围是 4096 到 2097152，单位是字节。默认的缓存大小是 2097152。
日志服务器	选中该复选框将终端标签日志输出到系统日志服务器，输出的日志类型为明文，需先配置好日志服务器。点击“查看日志服务器”链接查看所有已配置的系统日志服务器。

3. 点击“过滤”按钮，查看符合过滤条件的终端标签日志。

4. 点击“清除”按钮，将所有终端标签日志清除。（注意：对于支持将日志信息存储到本地数据库的设备，不支持该选项）

5. 点击“导出”按钮，将所有终端标签日志导出到本地文件。

第 8 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：包含地址信息，可被多个功能模块引用，例如策略规则、NAT 规则、QoS、会话限制等。

域名簿：包含域名信息，可被多个功能模块引用，例如 DNS 代理、LLB 规则。

服务簿：包含应用信息，可被多个功能模块引用，例如策略规则、NAT 规则、QoS 等。

应用簿：应用簿储存和管理应用和应用组。

SSL 代理： 设备提供 SSL 代理功能，能够解密 HTTPS 流量。

SLB 服务器池：介绍设备的 SLB 服务器配置。

时间表：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，例如策略规则、主机黑名单、PPPoE 接口与 Internet 的连接等。

AAA 服务器：介绍设备的 AAA 服务器配置。

Radius 动态授权：介绍 Radius 动态授权功能配置。

用户：包含使用设备提供的功能、服务、被设备认证以及管理的用户信息。

角色：包含将用户和权限联系起来的角色信息。功能配置中，为不同的角色指定不同的服务，由此，角色对应的用户即可拥有其角色的服务。

监测对象：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，可用于 HA 以及接口监控。

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。

设备拥有一个全局地址簿。用户需要为全局地址簿定义地址条目。在定义地址条目时，DNS 名称可以直接用来代替 IP 地址范围。已经配置好 IP 地址的接口也会作为地址条目自动添加到地址簿中，方便用户做 NAT 时使用。地址条目还具有以下特点：

地址簿中包含预定义条目“Any”，“IPv6-any”（仅 IPv6 版本支持）和“private_network"。“Any”对应的 IP 地址是 0.0.0.0/0，代表所有 IPv4 地址。“IPv6-any”对应的 IP 地址是::/0，代表所有 IPv6 地址。“private_network"对应的 IP 地址成员有 10.0.0.0/8、172.16.0.0/12、192.168.0.0/16，

代表所有私网地址。
“Any”和“IPv6-any”不可以编辑也不可以被删除。“private_network" 可以编辑或删除。

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。

系统支持 IPv4 和 IPv6 地址簿。如接口开启了 IPv6 功能，用户可根据需要配置 IPv6 格式的 IPv6/前缀长度、IP 地址范围或 IP 地址条目。

新建地址簿条目

新建地址簿条目，请按照以下步骤进行操作：

1. 点击“对象 > 地址簿”，进入<地址簿>页面。
2. 点击“新建”按钮。

在<配置地址簿>页面,配置地址簿信息。

基本配置	
名称	输入地址簿的名称。
类型	指定 IP 的地址类型，可选择 IPv4 或 IPv6。IPv6 选项仅当该版本支持 IPv6 时可配。
描述	输入该地址簿的描述信息。
地址成员	
成员	点击“新建”，配置地址条目成员。 IP 地址类型为 IPv4 时，点击“新建”按钮后，可以根据需要在“类型”列的下拉菜单中选择“IP/掩码”、“IP 范围”、“主机名称”、“地址簿”、“IP/通配符掩码”或“国家/地区”，然后在“成员”列的文本框中输入或者选

基本配置	
	择相应的配置。 IP 地址类型为 IPv6 时，点击“新建”按钮后，可以根据需要在“类型”列的下拉菜单中选择“IPv6/前缀长度”、“IPv6 范围”、“主机名称”、“地址簿”或者“IPv6/通配符”，然后在“成员”列的文本框中输入或者选择相应的配置。 说明： 添加“IP/通配符掩码”成员的地址簿时，通配符掩码中的 1 代表精确匹配，0 代表模糊匹配，不支持配置子网掩码格式。同时该地址簿不支持被 QoS 规则引用。 添加了“国家/地区”成员的地址簿，仅可以被策略规则和策略路由规则引用。 添加了“国家/地区”成员的地址簿，不支持排除地址成员配置。 当地址条目成员类型为“IPv6/通配符掩码”时，128 位的通配符掩码必须由连续的 8 个（或者 8 的整数倍个）0 或者 1 组成，比如 FF00::FFFF。 每条地址簿条目中最多允许配置 8 个“IP/反掩码”或者“IPv6/通配符掩码”类型的地址成员。 包含“IPv6/通配符掩码”类型的地址成员的地址簿，仅可以被其它 IPv6 地址簿或者策略规则引用。
删除	将选中的地址成员从地址条目成员列表中删除。
排除地址成员	
成员	点击“新建”，配置地址条目排除成员。 IP 地址类型为 IPv4 时，点击“新建”按钮后，可以根据需要在“类型”列的下拉菜单中选择“IP/掩码”或“IP 范围”，然后在“成员”列的文本框中输入相应的配置。 IP 地址类型为 IPv6 时，点击“新建”按钮后，可以根据需要在“类型”列的下拉菜单中选择“IPv6/前缀长度”或“IPv6 范围”，然后在“成员”列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。
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。新创建的地址簿名称将会显示在地址簿列表中。

查看地址簿条目详情

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、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“对象 > 地址簿”。
2. **在地址条目列表中点击需要查看详情的地址簿条目名称前的“+”，在地址簿条目下方区域查看详情。**

详情	
名称	查看地址簿的名称。
类型	查看 IP 地址的类型。
成员	查看地址簿中的地址条目成员。
排除成员	查看地址簿中的地址条目排除成员。
被引用次数	查看地址簿被引用的次数。
描述	查看地址簿的描述信息。
关联项	
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。点击策略规则名称，查看关联项详情。
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。
DNS 改写	被 DNS 改写规则引用的信息。
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。
Qos	被 QoS 规则引用的信息。
DNS 代理	被 DNS 代理规则引用的信息。
共享接入	被共享接入规则引用的信息。

过滤地址簿条目

用户可使用过滤器搜索符合过滤条件的地址条目，过滤条件包括地址条目名称、成员 IP 地址、描述和是否被其他功能模块引用。

1. 点击“对象 > 地址簿”。
2. 在页面右上方点击“过滤”。出现新行进行过滤条件的设置。
3. 点击“+过滤条件”后，从下拉菜单中选择一个过滤条件，并输入值。

4. 输入完成后，符合过滤条件的服务条目显示在下方的服务条目列表中。
5. 重复以上两步添加更多过滤条件。各个过滤条件之间的关系为“与”。
6. 如需删除某个过滤条件，可将鼠标悬浮在此过滤条件上，然后点击过滤条件上的叉图标。如需删除所有过滤条件，可在此行的尾端点击叉图标。

用户可保存已搜索的过滤条件：

1. 添加过滤条件后，点击“+过滤条件”后的下箭头，在下拉菜单中点击“+保存过滤条件”。
2. 指定要保存的过滤条件名称，每个过滤条件名称最长为 32 个英文字符，且名称仅支持中英文字符和下划线组成。
3. 点击文本框右侧“保存”按钮。
4. 如需使用已保存的过滤条件，双击过滤条件名称。
5. 如需删除已保存的过滤条件，点击过滤条件右侧 × 按钮。

注意:

根据需要最多可以保存 20 个过滤条件。

设备升级后，已保存的过滤条件将会被清除。

域名簿

用户可以将一个域名或多个域名的集合指定一个名称，在配置时，只需引用该名称。域名簿(Host book)就是系统中用来存储域名集合与其名称的对应关系的数据库。域名簿中的域名与名称的对应关系条目被称作域名条目（Host entry）。

需要注意的是：

域名条目个数的最大值为地址条目个数最大值的四分之一。

新建域名条目

新建域名条目，请按照以下步骤进行操作：

1. 选择“对象 > 域名簿”，进入域名簿页面。
2. **点击“新建”按钮，打开<配置域名簿>页面。**

选项	说明
名称	输入域名簿的名称。
添加方式	指定域名条目成员的添加方式。 手动输入：通过手动输入 IP 地址或者域名的方式，将域名成员添加至域名簿。 文件导入：通过导入文件的方式批量导入域名成员至域名簿。
域名组	当选择“手动输入”的添加方式后，在“域名组”文本框中输入单个或多个域名成员的 IP 地址或者域名。 **注意：**如需要添加多个域名成员，请在域名成员之间用回车键换行。
文件名称	当选择“文件导入”的添加方式后，点击“浏览”按钮选择本地的域名文件。 **注意：**目前仅支持导入 UTF-8 的编码文件（*.txt 或 *.csv）。
描述	输入所需的域名条目描述信息。

3. 点击“确定”按钮保存所做的配置。新创建的域名条目将会显示在域名簿列表中。

编辑域名条目

修改域名条目配置，请按照以下步骤进行操作：

1. 选择“对象 > 域名簿”，进入域名簿页面。
2. 在域名簿列表中，勾选需要编辑的域名条目复选框，然后点击“编辑”按钮。
3. 在打开的<配置域名簿>页面中，修改域名条目配置信息。

注意: 如果在编辑域名条目时，选择“文件导入”方式添加域名成员，通过文件导入的域名将会覆盖原来域名条目中的所有域名成员。

删除域名条目

删除域名条目，请按照以下步骤进行操作：

1. 选择“对象 > 域名簿”，进入域名簿页面。
2. 在域名簿列表中，勾选需要删除的域名条目复选框，然后点击“删除”按钮。

查看域名条目详情

查看域名条目详情，请按照以下步骤进行操作：

1. 点击“对象 > 域名簿”。
2. **在域名条目列表中点击需要查看详情的域名簿条目名称前的“+”，在域名条目下方区域查看详情。**

详情	
名称	查看域名簿的名称。
成员	查看域名簿中的域名条目成员。
描述	查看域名簿的描述信息。
关联项	
DNS 代理	被 DNS 代理规则引用的信息。
出站负载均衡规则	被出站负载均衡规则引用的信息。
DNS 改写	被 DNS 改写规则引用的信息。

服务簿

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应用类型。不同平台支持的预定义服务不同。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，用户还可以很容易地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

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。

配置服务簿

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“对象 > 服务簿 > 服务”，进入服务页面。
2. **点击“新建”按钮，打开<服务配置>页面**

选项	说明	
服务名称	输入服务簿的名称。	
规则描述	指定所创建自定义服务的协议类型，点击“新建”按钮，打开<服务规则配置>页面，可选择的协议类型有 TCP、UDP、ICMP、ICMPv6 以及全部。 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。 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”。 目的端口的“最小”为必填项，其他选项均为选填项。 当不配置“最大”时，系统将使用“最小端口”作为端口号。 超时：用户可以配置服务簿的超时时间及单位，范围是 1 到 65535 秒或 1 到 1000 天。如不配置，默认为 0。
	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。 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”。

选项	说明	
		当不配置“最大”时，系统将使用“最小端口”作为端口号。 目的端口的“最小”为必填项，其他选项均为选填项。 超时：用户可以配置服务簿的超时时间及单位，范围是 1 到 65535 秒或 1 到 1000 天。如不配置，默认为 0。
	ICMP	类型：指定服务条目的 ICMP type 值。通过下拉菜单可以选择 0（Echp-Reply）、3（Destination-Unreachable）、4（Source Quench）、5（Redirect）、8（Echo）、11（Time Exceeded）、12（Parameter Problem）、13（Timestamp）、14（Timestamp Reply）、15（Information Request）、16（Information Reply）、17（Address Mask Request）、18（Address Mask Reply）、30（Traceroute）、31（Datagram Conversion Error）、32（Mobile Host Redirect）、33（IPv6 Where-Are-You）、34（IPv6 I-Am-Here）、35（Mobile Registration Request）、36（Mobile Registration Reply）。 代码：指定自定义服务的 ICMP code 最小值和最大值。范围是 0-15。 **注意：** “最小值”不能大于“最大值”。 如果不配置“最大值”，系统将使用“最小值”作为单一代码值。 超时：用户可以配置服务簿的超时时间及单位，范围是 1 到 65535 秒或 1 到 1000 天。如不配置，默认为 0。
	ICMPv6	类型：指定服务条目的 ICMPv6 type 值。通过下拉菜单可以选择 1（Dest-Unreachable）、2（Packet Too Big）、3（Time Exceeded）、4（Parameter Problem）、5-99（Unallocated Error message）、100（Private experimentation）、101（Private experimentation）、102-126

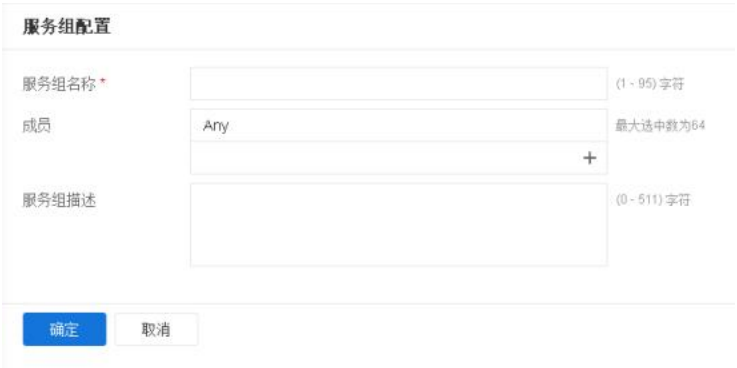
选项	说明	
		（Unallocated Error message）、127（Reserved for expansion of ICMPv6 error message）、128（Echo Request）、129（Echo Reply）、130（Multicast Listener Query）、131（Multicast Listener Report）、132（Multicast Listener Done）、133（Router Solicitation）、134（Router Advertisement）、135（Neighbor Solicitation）、136（Neighbor Advertisement）、137（Redirect Message）、138（Router Renumbering）、139（ICMP Node Information Query）、140（ICMP Node Information Response）、141（Inverse Neighbor Discovery Solicitation Message）、142（Inverse Neighbor Discovery Advertisement Message）、143（Version 2 Multicast Listener Report）、144（Home Agent Address Discovery Request Massage）、145（Home Agent Address Discovery Reply Massage）、146（Mobile Prefix Solicitation）、147（Mobile Prefix Advertisement ）、148（Certification Path Solicitation Message）、149（Certification Path Advertisement Message）、150（ICMP message utilized by experimental mobility protocols such as Seamoby）、151（Multicast Router Advertisement）、152（Multicast Router Solicitation ）、153（Multicast Router Termination）、154（FMIPv6 Messages）、200（Private experimentation）、201（Private experimentation）和 255（Reserved for expansion of ICMPv6 informational）。 代码：指定服务条目的 ICMP code 最小值和最大值。范围是 0-255。 **注意：** “最小值”不能大于“最大值”。 如果不配置“最大值”，系统将使用“最小值”作为单一代码值。 选择全部时：指定服务条目的协议号。范围是 1 到 255。

选项	说明	
	全部	指定服务条目的协议号。范围是 1 到 255。
描述	添加服务的描述信息。	

3. 点击“确定”按钮保存所做的配置。新创建的服务簿将会显示在服务簿列表中。

配置自定义服务组

1. 选择“对象 > 服务簿 > 服务组”，进入服务组页面。
2. **点击“新建”按钮，打开<服务组配置>页面**



选项	说明
服务组名称	输入自定义服务组的名称。
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。点击“+”按钮后，从右侧列表中选择需要的服务或服务组，点击“关闭”按钮将其添加到左侧成员列表，可添加多个成员。
服务组描述	输入所需的自定义服务组描述信息。

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。

查看服务条目详情

用户可以查看服务的详细信息，包括服务条目名称、协议、端口以及关联项。

查看服务条目详情，请按照以下步骤进行操作：

1. 点击“对象 > 服务簿> 服务”。
2. **在服务条目列表中点击需要查看详情的服务条目名称前的“+”，在服务条目下方区域查看详情。**

详情	
描述	查看应用的详细描述信息。
关联项	

详情	
服务组	被服务组引用的信息。
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。
策略	被策略规则引用的信息。点击策略规则名称，查看关联项详情。
策略路由	被策略路由规则引用的信息。

过滤服务条目

用户可使用过滤器搜索符合过滤条件的服务条目，过滤条件包括服务类型、名称、协议、目的端口、源端口和是否被其他功能模块引用。

1. 点击“对象 > 服务簿> 服务名称”。
2. 在页面右上方点击“过滤”。出现新行进行过滤条件的设置。
3. 点击“+过滤条件”后，从下拉菜单中选择一个过滤条件，并输入值。
4. 输入完成后，符合过滤条件的服务条目显示在下方的服务条目列表中。
5. 重复以上两步添加更多过滤条件。各个过滤条件之间的关系为“与”。
6. 如需删除某个过滤条件，可将鼠标悬浮在此过滤条件上，然后点击过滤条件上的叉图标。如需删除所有过滤条件，可在此行的尾端点击叉图标。

用户可保存已搜索的过滤条件：

1. 添加过滤条件后，点击“+过滤条件”后的下箭头，在下拉菜单中点击“+保存过滤条件”。
2. 指定要保存的过滤条件名称，每个过滤条件名称最长为 32 个英文字符，且名称仅支持中英文字符和下划线组成。
3. 点击文本框右侧“保存”按钮。
4. 如需使用已保存的过滤条件，双击过滤条件名称。
5. 如需删除已保存的过滤条件，点击过滤右侧 × 按钮。

过滤服务组

用户可使用过滤器搜索符合过滤条件的服务组，过滤条件包括服务组名称和是否被其他功能模块引用。

1. 点击“对象 > 服务簿> 服务组”。

2. 在页面左上方点击“过滤”，进行过滤条件的设置。
3. 点击“过滤”后，从下拉菜单中选择一个过滤条件，并输入值。
4. 输入完成后，符合过滤条件的服务条目显示在下方的服务条目列表中。
5. 重复以上两步添加更多过滤条件。各个过滤条件之间的关系为“与”。
6. 如需删除某个过滤条件，可将鼠标悬浮在此过滤条件上，然后点击过滤条件上的叉图标。如需删除所有过滤条件，可在此行的尾端点击叉图标。

用户可保存已搜索的过滤条件：

1. 添加过滤条件后，点击“过滤”后的下箭头，在下拉菜单中点击“保存过滤条件”。
2. 指定要保存的过滤条件名称，每个过滤条件名称最长为 32 个英文字符，且名称仅支持中英文字符和下划线组成。
3. 点击文本框右侧“保存“按钮。
4. 如需使用已保存的过滤条件，双击过滤条件名称。
5. 如需删除已保存的过滤条件，点击过滤条件右侧 × 按钮。

> 注意:
>
> 根据需要最多可以保存 20 个过滤条件。
>
> 设备升级后，已保存的过滤条件将会被清除。

应用簿

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，同时用户也可以根据自己的需要自定义应用和应用组。系统用应用簿来储存和管理这些应用和应用组。

如设备开启 IPv6，系统支持识别 IPv6 地址。

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等配置，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“对象 > 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、特征规则等配置。

新建自定义应用

用户可以根据需要创建自定义应用，并可以通过配置静态特征规则，对进入设备的流量进行识别控制，从而识别出应用。

新建自定义应用，请按照以下步骤进行操作：

1. 选择“对象 > 应用簿 > 应用”。
2. **点击“新建”按钮，打开<应用配置>页面。**

选项	说明
名称	输入自定义应用的名称。
超时	用户可以配置应用的超时时间，如果不指定超时时间，系统会使用协议的默认值。
类别	指定自定义应用所属的类别。应用所属的类别和子类别是由应用特征库维护的，类别对应特征库中的 1 级应用组，子类别对应 1 级应用组下的 2 级应用组。用户可以为自定义应用配置一个类别。默认为空。
子类别	指定自定义应用所属的子类别，只支持配置一种。默认为空。
所用技术	指定自定义应用所用的技术。应用所用的技术是由应用特征库维护的，只支持配置一种。默认为空。
特征	指定自定义应用的特征。应用的特征是由应用特征库维护的，支持配置一种或多种。默认为空。

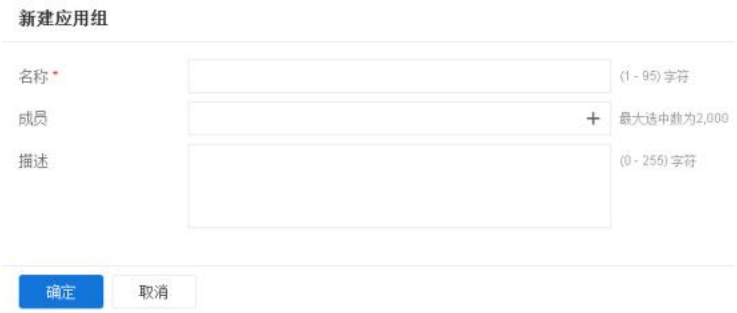
选项	说明
特征规则	点击“+”按钮，在右边滑出的<特征规则>对话框中选择用于识别该条应用的特征规则。
描述	输入自定义应用的描述信息。

3. 点击“确定”按钮，完成配置。

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“对象 > 应用簿 > 应用组”。
2. **点击“新建”按钮，打开<新建应用组>页面。**



选项	说明
名称	输入自定义用户组的名称。
成员	在“成员”列表中选择需要添加到应用组的应用、应用组和应用过滤组，选择时可以使用搜索和过滤功能筛选需要添加的成员。如需删除已添加的应用，点击“X”按钮。
描述	输入所需的自定义应用组描述信息。

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，系统支持自定义应用过滤组，即用户可设置一定的过滤条件，将过滤出的应用重新建组。当配置功能时需选择应用时，可快速引用该过滤组中的应用。

用户可根据应用的类别、子类别、所用技术、风险等级、特征等条件来定义应用过滤组。

新建应用过滤组，请按照以下步骤进行操作：

1. 选择“对象 > 应用簿 > 应用过滤组”。
2. 点击“新建”按钮，打开<应用过滤组配置>页面。
3. 在“名称”文本框中输入该应用过滤组的名字。

4. 点击“过滤”按钮，选择所需创建的应用过滤组的过滤条件，可选择过滤条件为“类别”、“子类别”、“所用技术”、“风险等级”、“特征”，然后选择具体的过滤条件，选定后，点击“过滤”即可。用户可根据需要，同时添加多条过滤条件。

5. 点击“确定”按钮，完成配置。

新建静态特征规则

系统通过配置静态特征规则，对进入设备的流量进行识别控制，当流量满足静态特征规则中的所有条件，才会认定为命中了该条静态特征规则，从而识别出对应的应用类型。

如设备开启 IPv6，系统支持对 IPv6 地址的流量进行识别。

新建静态特征规则：

1. 选择“对象 > 应用簿 > 静态特征规则”。

2. 点击“新建”按钮，打开<特征规则配置>页面。

在打开的页面中进行配置。

选项	说明
应用	选择配置的特征规则所适用的应用名称（包括预定义和自定义的应用）。配置后，满足下方特征规则所有条件的流量将被识别为该应用。
类型	选择流量的 IP 地址类型。如设备开启 IPv6，系统支持对 IPv6 地址

选项	说明
	的流量进行识别。
源信息	
安全域	指定特征规则的源安全域。
地址	指定特征规则的源地址，可以是地址簿条目类型源地址或 IP 成员类型源地址。 用户还可执行如下操作： 选择地址簿类型时，点击搜索框中的 按钮，可以按地址簿名称和地址成员的 IP 进行模糊搜索，名称和地址是与的关系。地址支持多种输入方式，例如：输入“地址”为 10.10.10.10/32，可能匹配到包含地址成员是 10.10.10.10/24 的地址簿；输入“地址”为段掩码 9.9.9.9/24，可能匹配到包含地址成员是 9.9.0.0/16 的地址簿；输入“地址”为 10.10.10.10，可能匹配到地址成员的 IP 范围为 10.10.10.0-10.10.10.255 的地址簿；输入“地址”为 10.23，可能匹配到包含地址成员是 1.10.23.10/24 的地址簿；输入“地址”为 aa，可能匹配到地址成员的“主机名称”为 aaa 的地址簿。
目的	
地址	指定特征规则的目的地址，可以是地址簿条目类型源地址或 IP 成员类型源地址。 用户还可执行如下操作： 选择地址簿类型时，点击搜索框中的 按钮，可以按地址簿名称和地址成员的 IP 进行模糊搜索，名称和地址是与的关系。地址支持多种输入方式，例如：输入“地址”为 10.10.10.10/32，可能匹配到包含地址成员是 10.10.10.10/24 的地址簿；输入“地址”为段掩码 9.9.9.9/24，可能匹配到包含地址成员是 9.9.0.0/16 的地址簿；输入“地址”为 10.10.10.10，可能匹配到地址成员的 IP 范围为 10.10.10.0-10.10.10.255 的地址簿；输入“地址”为 10.23，可能匹配到包含地址成员是 1.10.23.10/24 的地址簿；输入“地址”为 aa，可能匹配到地址成员的“主机名称”为 aaa 的地址簿。
协议	
类型	选择“TCP”和“UDP”类型时， 目的端口：指定静态特征规则的目的端口号。如果目的端口号为一个范围，在“最小”文本框中填写最小目的端口号，在“最大”文本框中填写为最大目的端口号。目的端口号的范围是 0 到 65535，并且目的端口号不能为单一的

选项	说明
	0，例如，目的端口号可以是 0 到 20，但是不能仅为 0。 源端口：指定静态特征规则的源端口号。如果源端口号为一个范围，在“最小”文本框填写最小源端口号，在“最大”文本框填写最大源端口号。源端口号的范围是 0 到 65535。 选择“ICMP”或“ICMPv6”类型时， IP 地址类型为 IPv4 时，选择“ICMP”： 类型：指定自定义应用特征的 ICMP type 值。范围是 0（Echp-Reply）、3（Destination-Unreachable）、4（Source Quench）、5（Redirect）、8（Echo）、11（Time Exceeded）、12（Parameter Problem）、13（Timestamp）、14（Timestamp Reply）、15（Information Request）、16（Information Reply）、17（Address Mask Request）、18（Address Mask Reply）、30（Traceroute）、31（Datagram Conversion Error）、32（Mobile Host Redirect）、33（IPv6 Where-Are-You）、34（IPv6 I-Am-Here）、35（Mobile Registration Request）、36（Mobile Registration Reply）。 代码最小值：指定静态特征规则的 ICMP code 值。范围是 0 到 15。默认值是 0。 IP 地址类型为 IPv6 时，选择“ICMPv6”： 类型：指定自定义应用特征的 ICMPv6 type 值。范围是 1（Dest-Unreachable）、2（Packet Too Big）、3（Time Exceeded）、4（Parameter Problem）、5-99（Unallocated Error message）、100（Private experimentation）、101（Private experimentation）、102-126（Unallocated Error message）、127（Reserved for expansion of ICMPv6 error message）、128（Echo Request）、129（Echo Reply）、130（Multicast Listener Query）、131（Multicast Listener Report）、132（Multicast Listener Done）、133（Router Solicitation）、134（Router Advertisement）、135（Neighbor Solicitation）、136（Neighbor Advertisement）、137（Redirect Message）、138（Router Renumbering）、139（ICMP Node Information Query）、140（ICMP Node Information Response）、141（Inverse Neighbor

选项	说明
	Discovery Solicitation Message）、142（Inverse Neighbor Discovery Advertisement Message）、143（Version 2 Multicast Listener Report）、144（Home Agent Address Discovery Request Massage）、145（Home Agent Address Discovery Reply Massage）、146（Mobile Prefix Solicitation）、147（Mobile Prefix Advertisement ）、148（Certification Path Solicitation Message）、149（Certification Path Advertisement Message）、150（ICMP message utilized by experimental mobility protocols such as Seamoby）、151（Multicast Router Advertisement）、152（Multicast Router Solicitation ）、153（Multicast Router Termination）、154（FMIPv6 Messages）、200（Private experimentation）、201（Private experimentation）和 255（Reserved for expansion of ICMPv6 informational）。 代码最小值：指定静态特征规则的 ICMPv6 code 值。范围是 0 到 255。默认值是 0。 选择“其它”时， 协议号：指定静态特征规则的协议号。范围是 1 到 255。
动作	
应用特征规则	点击“启用”按钮，配置完成的特征规则生效。否则，特征规则不生效。
继续动态识别	点击“启用”按钮，如果流量命中静态特征规则，识别出对应的应用名称后，系统将继续进行动态识别。用户可以要求系统在命中静态特征规则后仍继续进行动态识别，以实现更精细的控制。否则，将不继续进行动态识别。

3. 点击“确定”按钮，完成配置。

查看应用条目详情

用户可以查看应用的详细信息，包括应用条目名称、类别、子类别、风险等级、所用技术以及关联项。

查看应用条目详情，请按照以下步骤进行操作：

1. 点击“对象 > 应用簿> 应用”。
2. **在应用条目列表中点击需要查看详情的应用条目名称前的“+”，在应用条目下方区域查看详情。**

详情

详情	
描述	查看应用的详细描述信息。
参考	查看应用的参考实例。
常规端口	查看应用使用的常规端口号。
易逃逸	查看该应用是否属于易逃逸。
大量消耗带宽	查看该应用是否大量消耗带宽。
易被滥用	查看该应用是否容易被滥用。
能够传输文件	查看该应用是否能够传输文件。
被其他应用使用	查看该应用是否被其他应用使用。
被恶意软件利用	查看该应用是否被恶意软件利用。
存在已知漏洞	查看该应用是否存在已知漏洞。
已被大规模使用	查看该应用是否已被大规模使用。
关联项	
应用组	被应用组引用的信息。
应用过滤组	被应用过滤组引用的信息。
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。
策略	被策略规则引用的信息。点击策略规则名称，查看关联项详情。

配置应用资源/应用资源组

应用资源用于定义用户需要访问的应用、内容、服务等资源，用户需要通过配置地址、协议、端口等来指定一个应用资源条目。应用资源组用于定义一组应用资源。系统支持配置最多 256 个应用资源，64 个应用资源组。

系统支持以下方式配置应用资源条目：

基于 IP 地址、协议、端口

基于 IP 范围、协议、端口

基于域名、协议、端口

配置应用资源，按照以下步骤进行操作：

1. 点击“对象 > 应用资源簿 > 应用资源”，或点击“零信任访问 > 应用资源簿 > 应用资源”，进入应用资源页面。

2. 点击“新建”按钮，打开<应用资源配置>页面。

在<应用资源配置>页面填写应用资源基本信息。

选项	说明
名称	输入应用资源的名称。范围是 1 到 95 个字符。
超链接	输入应用资源的 URL 地址，范围是 0 到 2047 个字符。在用户登录后展示的 ZTNA Portal 页面上，配置了超链接的应用资源，用户可以复制链接到浏览器访问，也可以直接点击图标实现快速访问（需确保链接有效）。不配置超链接的应用资源不会展示在 Portal 页面上。如果超链接中未指定协议类型，默认使用 HTTP 协议。关闭 Portal 页面后，用户可以通过客户端菜单的“应用资源列表”选项重新打开最新的 Portal 页面查看应用资源的访问权限。Portal 页面上展示用户有权限和无权限访问的应用资源。对于无权限访问的应用资源，用户在调整终端配置后，可以获得访问权限。禁止访问的应用资源不在 Portal 页面上展示，如果用户被禁止访问任何应用资源，Portal 页面将展示“无可用的 Web 服务资源”。
规则描述	点击“新建”按钮为应用资源添加一个条目。每个应用资源可以添加最多 16 个条目。在“应用资源规则配置”页面，指定条目信息。 类型：指定应用资源条目的类型，包括 IPv4/掩码、IPv6/前缀长度、IPv4 范围、IPv6 范围、域名。 地址：指定应用资源条目的 IP 地址或 IP 地址范围。 域名：指定应用资源条目的域名，取值范围是 1 到 255 个字符，且在两个点号（.）之间最多可以有 63 个字符。支持设置精确域名和以“*”作为第一个字符的通配域名。 协议：指定应用资源条目的协议类型。基于 IP 地址定义应用资源条目时，协议类型支持 TCP 和 UDP；基于域名定义应用资源条目时，协议类型支持 HTTP 或 HTTPS。 端口：指定应用资源条目的端口号。范围为 1 至 65535。 超时：指定应用资源条目的超时时间，单位为可以为秒或天。单位为秒时，取值范围是 1 到 65535。单位为天时，取

选项	说明
	值范围是 1 到 1000。协议类型为 TCP/HTTP/HTTPS 时，默认是 1800 秒，协议类型为 UDP 时，默认是 60 秒。
描述	指定应用资源的描述信息。范围为 0 至 255 个字符。

3. 点击“确定”，保存配置。

4. 在应用资源页面，点击列表里的“+”展开一个应用资源，可以查看到该应用资源的更多信息，包括所属的应用资源组、引用的 ZTNA 策略。

在应用资源页面，对应用资源进行管理。

选项	说明
过滤	从下拉菜单中选择过滤条件，应用资源列表将展示匹配指定条件的应用资源。
编辑	点击此按钮修改选中的应用资源的的配置。
删除	点击此按钮删除选定的应用资源。

配置应用资源组，按照以下步骤进行操作：

1. 点击“对象 > 应用资源簿 > 应用资源组”或点击“零信任访问 > 应用资源簿 > 应用资源组”，进入应用资源组页面。

2. 点击“新建”按钮，打开<应用资源组>配置页面。

在<应用资源组配置>页面填写应用资源组基本信息。

选项	说明
名称	输入应用资源组的名称。范围是 1 到 95 个字符。
应用资源	选择系统已配置的应用资源。或者，点击“+”按钮，在弹出的<应用资源配置>对话框里新建一个应用资源。最多可以添加 16 个应用资源。
描述	指定应用资源的描述信息。范围为 0 至 255 个字符。

3. 点击“确定”，保存配置。

4. 在应用资源组页面，点击列表里的“+”展开一个应用资源组，可以查看到该应用资源组的更多信息，包括引用的 ZTNA 策略 ID。

在<应用资源组>页面，对应用资源组进行管理。

选项	说明
名称	输入应用资源组名称，列表将展示匹配指定名称的应用资源组，支持部分匹配和全部匹配。
编辑	点击此按钮修改选中的应用资源组的配置。
删除	点击此按钮删除选定的应用资源组。

配置接入地址池

设备端通过地址池给客户端分配 IP 地址。当客户端连接设备端成功后，设备端会从地址池里取出一个 IP 地址与其它相关参数（如 DNS 服务器地址与 WINS 服务器地址等）一起分配给客户端。

设备端通过创建和执行 IP 地址绑定规则来满足客户端的固定 IP 地址需求。IP 地址绑定规则包括 IP 用户绑定规则和 IP 角色绑定规则。IP 用户绑定规则将客户端用户与已配置地址池中的某个固定 IP 地址绑定，当客户端连接成功后，设备端会将绑定的 IP 地址分配给客户端；IP 角色绑定规则是将角色与已配置地址池中的某一 IP 地址范围绑定，当此客户端连接成功后，设备端会从绑定的地址范围中取出一个 IP 地址分配给客户端。

当设备端通过地址池给客户端分配 IP 地址时，系统会按照一定的顺序对客户端的 IP 地址绑定规则进行检查，决定如何为客户端分配 IP 地址。

检查是否已为客户端用户配置 IP 用户绑定规则，如果是，则将绑定的 IP 地址分配给客户端；否则，从非绑定地址范围中取出一个未被占用的 IP 分配给客户端。

检查是否已为客户端用户配置 IP 角色绑定规则，如果是，则从绑定的地址范围中取出一个 IP 地址分配给客户端；否则，从非绑定地址范围中取出一个未被占用的 IP 分配给客户端。

> 注意: IP 用户绑定规则中的 IP 地址和 IP 角色绑定规则中的 IP 地址不能重叠。

配置接入地址池，按照以下步骤进行操作：

1. 点击“对象 > 接入地址池”，进入接入地址池页面。
2. 选择“IPv4”或“IPv6”标签页，仅当该版本为 IPv6 版本时可配。

3. 点击“新建”按钮，打开<接入地址池配置> 页面。

在<接入地址池配置>标签页，填写配置信息。

基本配置	
接入地址池名称	指定地址池名称。
起始 IP	指定地址池的起始 IP 地址。
终止 IP	指定地址池的终止 IP 地址。
保留起始 IP	指定保留地址池的起始 IP 地址。
保留终止 IP	指定保留地址池的终止 IP 地址。
子网掩码	当创建的地址池类型为 IPv4 时，指定网络掩码。
前缀长度	当创建的地址池类型为 IPv6 时，指定 IPv6 地址前缀长度。取值范围是 111 到 128。该选项仅当该版本为 IPv6 版本时可配。
DNS1/DNS2/DNS3/DNS4	指定地址池的 DNS 服务器 IP 地址。此项为可选项，即地址池可以不指定 DNS 服务器。用户最多可以为每个地址池指定 4 个 DNS 服务器。
WINS1/WINS2	指定地址池的 WINS 服务器 IP 地址。此项为可选项，即地址池可以不指定 WINS 服务器。用户最多可以为每个地址池指定 2 个 WINS 服务器。仅在创建的地址池类

基本配置	
	型为 IPv4 时可配。
IP 用户绑定	
新建	点击“新建”按钮，将用户与 IP 地址的绑定条目添加到列表中。
用户	输入用户名称。
IP	输入 IP 地址。
删除	点击“删除”按钮删除选中的绑定条目。
IP 角色绑定	
新建	点击“新建”按钮，将角色与 IP 地址的绑定条目添加到列表中。
角色	输入角色名称。
起始 IP 地址	输入起始 IP 地址。
终止 IP 地址	输入终止 IP 地址。
删除	点击“删除”按钮删除选中的绑定条目。

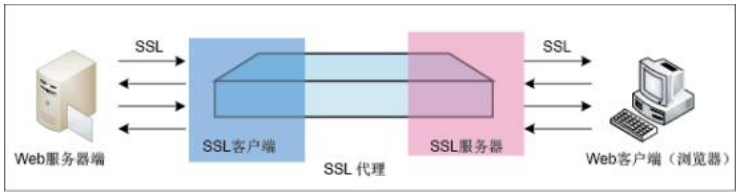
4. 点击“确定”按钮，保存所做的配置。

对于绑定到多个角色且多个角色有相应的角色-IP 地址绑定规则的用户，系统会对角色-IP 地址绑定规则进行顺序查找，然后按照查找到的相匹配的第一条规则为用户分配地址。如需改变已有的角色-IP 地址绑定规则的排列顺序，在<接入地址池>页面，选择一个地址池后，点击“IP 角色调序”。在 IP 角色调序对话框里，选择需要调整的角色名称，点击“上移/下移/移到最前/移到最后”。

SSL 代理

为了保护敏感数据在互联网传送中的安全性，越来越多的网站都采用 SSL 加密形式发布。设备提供 SSL 代理功能，能够解密 HTTPS、POP3S、SMTPS、IMAPS、RDPS 和 FTPS 流量。SSL 代理功能可工作在如下两种场景：

第一种场景，当设备作为 Web 客户端一侧的网关时，SSL 代理功能利用 SSL 代理证书替换加密 Web 网站的数字证书，并将 SSL 代理证书发送到客户端的 Web 浏览器，在此过程中，设备分别作为 SSL 客户端和 SSL 服务器与 Web 服务器和 Web 浏览器建立 SSL 连接，从而获得加密通信的明文内容。SSL 代理证书是使用设备本身的证书对 Web 服务器证书重新签发而成的证书。过程如下图所示：



第二种场景，当设备作为 Web 服务器一侧的网关时，开启 SSL 代理功能的设备可充当 SSL 服务器，使用 Web 服务器的证书与客户端建立 SSL 连接，并将解密后的流量以明文的方式发送到内网的 Web 服务器。

工作模式

根据如上两种使用场景，SSL 代理可工作在两种模式下。对于第一种场景，可工作在“客户端流量检查-代理模式”下；对于第二种场景，可工作在“服务器流量检查-卸载模式”和“服务器流量检查-代理模式”下。

工作在“客户端流量检查-代理模式”时，可对指定的网站进行 SSL 代理。对于不需要进行 SSL 代理的网站，设备将网站 IP 地址和端口号动态添加到放行名单，其流量被放行；对于需要进行 SSL 代理的网站，设备将会对 SSL 协商过程中的参数进行检查。对于符合检查条件的 SSL 协商参数，用户可对其 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量进行阻断或者放行。

设置为阻断行为的 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量，设备将会对其进行阻断；

设置为放行行为的 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量，设备不会对其进行解密。同时，设备将此网站 IP 地址和端口号动态地添加到放行名单，则其 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量被放行。

对于既没有被阻断，也没有被放行的 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量，设备将会对其解密。

工作在“服务器流量检查-卸载模式”时，设备将对来自 Web 客户端发起的 SSL 连接进行代理，解密数据，并将数据以明文的方式发送给 Web 服务器。

工作在“服务器流量检查-代理模式”时，设备将对来自 Web 客户端发起的 SSL 连接进行代理，解密数据，并将数据重新加密后发送给 Web 服务器。

SSL 代理功能可与如下功能模块结合使用：

与应用识别结合使用，设备能够对使用 SSL 加密通讯的应用所产生的 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量进行解密与识别。识别应用后，可针对应用进行策略控制、流量控制、会话限制、配置策略路由等。

与 Web 认证结合使用，支持单边 SSL 代理。在客户端进行认证时启动 SSL 连接，认证通过后，SSL 代理不再工作，客户端与服务器之间直接交互。

与 AV、IPS、URL、文件过滤、内容过滤结合使用，设备能够对 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量进行 AV 防护、IPS 防护、文件过滤、URL 过滤、文件内容过滤；对 HTTPS 流量进行网页关键字过滤、Web 外发信息过滤以及应用行为控制；对 POP3S/SMTPS/IMAPS 流量进行邮件过滤。

当设备作为 Web 客户端一侧的网关时

通过策略规则与 SSL 代理 Profile 相结合的方式可实现 SSL 代理。将 SSL 代理 Profile 绑定到策略规则后，系统将会对与策略规则相匹配的网络流量根据 SSL 代理 Profile 配置进行处理。请按照以下步骤进行操作：

1. 配置 SSL 代理相关参数，包括指定设备证书的 PKI 信任域、获取网站证书 Subject 字段的 CN 值以及导入设备证书到客户端 Web 浏览器。
2. 定义 SSL 代理 Profile，在 Profile 中设置工作模式，对符合检查条件的 SSL 协商设置行为、启用警告提示功能等。
3. 将 SSL 代理 Profile 绑定到适当的策略规则，对符合策略规则且没有被阻断与放行的 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量进行解密。

配置 SSL 代理相关参数

SSL 代理相关参数的配置包括：

指定设备证书的 PKI 信任域

获取网站证书的 CN 值

导入设备证书到客户端 Web 浏览器

指定设备证书的 PKI 信任域

默认情况下，设备会使用缺省 PKI 信任域 trust_domain_ssl_proxy_2048 中的证书对 Web 服务器证书重新签发，生成 SSL 代理证书。用户也可以将系统中其它 PKI 信任域指定为设备证书信任域，该 PKI 信任域必须配有 CA 证书、本地证书以及本地证书对应的私钥。指定设备证书的 PKI 信任域，按照以下步骤进行操作：

1. 点击“对象 > SSL 代理”，进入相应功能页面。
2. 在页面右上角，点击“信任域设置”，并在打开的页面中选择需要使用的信任域。

   trust_domain_ssl_proxy 使用 RSA 算法，模长 1024 位。

   trust_domain_ssl_proxy_2048 使用 RSA 算法，模长 2048 位。
3. 点击“确定”按钮，保存所做配置并返回上一级页面。

获取网站证书的 CN 值

获取网站证书 Subject 字段的 CN 值，按照以下步骤进行操作（以需要获得 https://mail.qq.com/网站证书 Subject 字段的 CN 值为例）：

1. 打开 IE 浏览器，访问此 URL。

2. 在浏览器地址栏单击“锁”状图标。

3. 在弹出菜单中选择“查看证书”链接。

4. 打开“详细信息”标签页。

5. 在“使用者”字段查看对应的 CN 值。

导入设备证书到客户端 Web 浏览器

进行 SSL 代理时，设备会用 SSL 代理证书替换 SSL Web 站点的证书，并发送到客户端 Web 浏览器。由于客户端浏览器不拥有 SSL 代理证书的根证书，从而导致用户不能正常访问代理站点。为了解决这个问题，需要在客户端浏览器中导入 SSL 代理证书的根证书，也即设备证书。导入设备证书到客户端 PC 浏览器，请按照以下步骤进行操作：

1. 导出设备证书。点击“系统 > PKI >信任域证书”，进入信任域证书页面。

2. 在该页面，做如下配置：

   信任域： trust_domain_ssl_proxy 或者 trust_domain_ssl_proxy_2048

   内容：CA 证书

   行为：导出

3. 点击“确定”按钮并选择导出路径。证书将会输出到指定路径。

导入证书到客户端 PC 浏览器。在客户端 Web 浏览器（以 Internet Explorer 为例）选择“工具>Internet 选项>内容>证书>受信任的根证书颁发机构”。点击列表下方的“导入”按钮，弹出<证书导入向导>对话框，按照向导提示将导出证书导入到浏览器。参见下图：

配置 SSL 代理 Profile

SSL 代理 Profile 中可以配置会话复用功能，设置 SSL 代理工作模式，设置需要进行 SSL 代理的网站名单(通过网站证书的 Subject 字段的 CN 值进行指定)，对符合检查条件的 SSL 协商设置相应的行为，配置设备根证书下载提示，以及配置描述信息等。系统支持最多 32 个 SSL 代理 Profile。配置 SSL 代理 Profile，请按照以下步骤进行操作：

1. 点击“对象 > SSL 代理 > SSL 代理”，进入相应功能页面。

2. 点击列表上方的“新建”按钮，新建 SSL 代理 Profile。

在该页面，配置相关参数。

<table>
<tr><th>选项</th><th>说明</th></tr>
<tr><td>名称</td><td>指定所创建的 SSL 代理 Profile 的名称。</td></tr>
<tr><td>描述</td><td>添加 SSL 代理 Profile 的描述信息。</td></tr>
<tr><td>会话复用方式</td><td>配置会话复用功能后，当客户端向服务器端发起 SSL 连接请求时，服务器端会判断该请求连接是否已经创建过，如果是，则恢复之前的 SSL 连接，无需再进行完整的 TLS 握手协商过程，从而减少了 TLS 握手过程中的时间耗费。系统支持以下两种会话复用方式：

Ticket：勾选该复选框，指定 Session Ticket 会话复用方式。该方式下，客户端与 Web 服务器端完成第一次 SSL 连接后，服务器端将本次 TLS 握手中生成的对称密钥及其他状态信息加密并生成 Session Ticket，然后将 Session Ticket 发送给客户端，缓存在客户端。当客户端再次向服务器端发起 SSL 连接请求（或者断开连接后再次发起连接请求）时，会首先将 Session Ticket 发送给服务器端，如果服务器端解密校验成功，则恢复第一次的 SSL 连接，进行会话复用；

ID：勾选该复选框，指定 Session ID 会话复用方式。该方式下，客户端与 Web 服务器端完成第一次 SSL 连接后，客户端和服务器端将本次 TLS 握手中生成的 Session ID、对称密钥及其他状态信息缓存在本端。当客户端再次向服务器端发起 SSL 连接请求（或者断开连接后再次发起连接请求）时，服务器将新请求中的 Session ID 与已缓存的 Session ID 进行对比，如果一致，则恢复第一次的 SSL 连接，进行会话复用。</td></tr>
<tr><td>会话缓存数量</td><td>指定系统保存 Session ID 会话复用方式下的会话缓存数量或者 Session Ticket 会话复用方式下的会话缓存数量。取值范围及默认值请参考下表：
<table><tr><th>产品型号</th><th>取值范围（单位：条）</th><th>默认值（单位：条）</th></tr></table></td></tr>
<tr><td>会话超时时间</td><td>指定系统保存 Session ID 会话复用方式下的会话缓存或者 Session Ticket 会话复用方式下的会话缓存的时间，超过该指定时间后，系统将删除会话缓存，当客户端与服务器端建立 SSL 连接时，需要重新进行完整的 TLS 握手协商过程。取值范围为 1800 秒至 72000 秒，默认取值为 3600 秒。</td></tr>
<tr><td>模式</td><td>选择客户端流量检查模式。当设备作为 Web 客户端一侧的网关时，设备对来自服务器端的 SSL 连接进行代理，解密数据并做检查。</td></tr>
<tr><td>检查应用</td><td>选择 SSL 代理将检查的应用类型。目前系统支持对默认端口的 HTTPS、POP3S、SMTPS 和 IMAPS/RDPS/FTPS 流量进行 SSL 代</td></tr>
</table>

选项	说明
	理。默认情况下，系统仅对 HTTPS 流量进行 SSL 代理，用户可根据需要同时选择多种应用类型。用户可在“对象>应用簿>静态特征规则”页面，配置上述应用的自定义端口，实现系统对自定义端口的 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 应用进行 SSL 代理。 **注意：**只有系统在“对象>应用簿>应用”创建好的预定义应用，才可进行 SSL 代理。
根证书推送	点击“启用”按钮，启用根证书推送功能。当用户的 HTTPS 访问行为被监控时，即，HTTPS 流量被解密，系统将为客户端 Web 浏览器推送设备根证书下载页面。在根证书下载页面，用户可根据需要选择“下载证书”和“已安装，忽略”。 下载证书：点击该按钮，下载根证书文件并保存到本地。将本地根证书导入客户端浏览器具体步骤可参照“导入设备证书到客户端 Web 浏览器”。 已安装，忽略：点击该按钮，系统将不再推送根证书下载页面，并且为客户端 Web 浏览器跳转至目标访问页面。 **注意：** 系统为客户端 Web 浏览器推送根证书下载页面时，必须点击“下载证书”或“已安装，忽略”按钮。若用户未点击或者直接关闭浏览器，则在该浏览器下次申请 HTTPS 访问时，系统仍为其推送根证书下载页面。 请用户务必安装设备根证书。若用户未安装设备根证书，系统将提示用户访问不安全，可能会出现访问页面加载不全的现象。 点击“禁用”按钮，关闭根证书推送功能。关闭后，当客户端发起 HTTPS 访问时： 若客户端 Web 浏览器已安装设备根证书，系统将自动为用户跳转至目标访问页面。 若客户端 Web 浏览器未安装设备根证书，系统将提示用户该访问不安全。

配置解密配置。系统完成对 SSL 协商的检查后，既没有被阻断也没有被放行的访问申请，其 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量将会被解密。当 SSL 协商的参数符合多个检查条件且用户对不同的检查条件设置不同的行为，即，阻断行为和放行行为，则阻断行为生效，相应流量会被阻断。

加密模式检查	
不支持的版本	检查服务器使用的 SSL 协议版本。

	当系统不支持 SSL 服务器使用的 SSL 协议时，可选择“阻断”阻断其 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量，或者选择“放行”使用 BYPASS 模式放行 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量。默认为“放行”。 当系统支持 SSL 服务器使用的 SSL 协议时，将继续检查后续项目。
不支持的加密算法	检查服务器使用的加密算法。 当系统不支持 SSL 服务器使用的加密算法时，可选择“阻断”阻断其 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量，或者选择“放行”使用 BYPASS 模式放行 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量。默认为“放行”。 当系统支持 SSL 服务器使用的加密算法时，将继续检查后续项目。
未知错误	检查是否有未知错误。 当 SSL 握手失败而又无法确认失败的原因时，可选择“阻断”阻断其 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量，或者选择“放行”使用 BYPASS 模式放行 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量。默认为“放行”。 当系统不需要检查是否有未知错误时，将继续检查后续项。
最低支持版本	指定系统支持的 SSL 协议的最低版本。当 SSL 连接使用的 SSL 协议版本符合条件时，系统可代理其 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量。
最高支持版本	指定系统支持的 SSL 协议的最高版本。当 SSL 连接使用的 SSL 协议版本符合条件时，系统可代理其 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量。
服务器证书检查	
过期证书	检查服务器使用的证书。当 SSL 服务器的证书过期时，可选择“阻断”阻断其 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量，或者选择“放行”使用 BYPASS 模式放行 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量，或者选择“解密”对 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量进行解密。默认为“解密”。
客户端认证	检查服务器是否需要验证客户端证书。

	当服务器需要验证客户端证书时，可选择“阻断”阻断其 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量，或者选择“放行”使用 BYPASS 模式放行 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量。默认为“放行”。 当服务器不需要验证客户端证书时，将继续检查后续项目。
失败验证	验证服务器使用的证书。当设备对服务器证书验证失败时，用户可根据需要配置系统对其 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量的防护行为。 默认为“解密”。 解密：对验证失败的 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量进行解密，并选择是否使用设备自签名证书。 使用自签名证书：点击“启用”按钮，系统将返回设备自签名证书与客户端浏览器进行 SSL 协商，此时客户端浏览器会产生告警提示。 不使用自签名证书：点击“禁用”按钮，系统将返回可信证书“SG6000”与客户端浏览器进行 SSL 协商，在用户已经安装“SG6000”根证书的情况下，浏览器将不会产生告警提示。 阻断：阻断验证失败的 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量。 放行：放行验证失败的 HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS 流量。

3. 点击“确定”按钮，保存所做配置并返回上一级页面。

当设备作为 Web 服务器一侧的网关时

通过策略规则与 SSL 代理 Profile 相结合的方式可实现 SSL 代理。将 SSL 代理 Profile 绑定到策略规则后，系统将会对与策略规则相匹配的网络流量根据 SSL 代理 Profile 配置进行处理。请按照以下步骤进行操作：

1. 定义 SSL 代理 Profile，在 Profile 中设置工作模式，指定 Web 服务器证书的信任域及端口号。
2. 将 SSL 代理 Profile 绑定到适当的策略规则，对符合策略规则的 HTTPS 流量进行代理。

配置 SSL 代理 Profile

SSL 代理 Profile 中可以配置会话复用功能，设置 SSL 代理工作模式，指定 Web 服务器证书的信任域及端口号。配置 SSL 代理 Profile，请按照以下步骤进行操作：

1. 点击“对象 > SSL 代理 > SSL 代理”，进入相应功能页面。

2. 点击列表上方的“新建”按钮，新建 SSL 代理 Profile。

在“基本配置”标签页配置基本配置。

选项	说明
名称	指定所创建的 SSL 代理 Profile 的名称。
描述	添加 SSL 代理 Profile 的描述信息。
会话复用方式	配置会话复用功能后，当客户端向服务器端发起 SSL 连接请求时，服务器端会判断该请求连接是否已经创建过，如果是，则恢复之前的 SSL 连接，无需再进行完整的 TLS 握手协商过程，从而减少了 TLS 握手过程中的时间耗费。系统支持以下两种会话复用方式： Ticket：勾选该复选框，指定 Session Ticket 会话复用方式。该方式下，客户端与 Web 服务器端完成第一次 SSL 连接后，服务器端将本次 TLS 握手中生成的对称密钥及其他状态信息加密并生成 Session Ticket，然后将 Session Ticket 发送给客户端，由客户端保存。当客户端再次向服务器端发起 SSL 连接请求（或者断开连接后再次发起连接请求）时，会将

<table>
<tr><th>选项</th><th>说明</th></tr>
<tr><td></td><td>Session Ticket 同时发送给服务器端，如果服务器端解密校验成功，则恢复第一次的 SSL 连接，进行会话复用；

ID：勾选该复选框，指定 Session ID 会话复用方式。该方式下，客户端与 Web 服务器端完成第一次 SSL 连接后，客户端和服务器端将本次 TLS 握手中生成的 Session ID、对称密钥及其他状态信息缓存在本端。当客户端再次向服务器端发起 SSL 连接请求（或者断开连接后再次发起连接请求）时，服务器将新请求中的 Session ID 与已缓存的 Session ID 进行对比，如果一致，则恢复第一次的 SSL 连接，进行会话复用。</td></tr>
<tr><td>会话缓存数量</td><td>指定系统保存 Session ID 会话复用方式下的会话缓存数量或者 Session Ticket 会话复用方式下的会话缓存数量。取值范围及默认值请参考下表：<table><tr><th>产品型号</th><th>取值范围（单位：条）</th><th>默认值（单位：条）</th></tr></table></td></tr>
<tr><td>会话超时时间</td><td>指定系统保存 Session ID 会话复用方式下的会话缓存或者 Session Ticket 会话复用方式下的会话缓存的时间，超过该指定时间后，系统将删除会话缓存，当客户端与服务器端建立 SSL 连接时，需要重新进行完整的 TLS 握手协商过程。取值范围为 1800 秒至 72000 秒，默认取值为 3600 秒。</td></tr>
<tr><td>模式</td><td>选择服务端流量检查模式。当设备作为 Web 服务器一侧的网关时，SSL 代理可工作在服务端流量检查-代理模式或服务端流量检查-卸载模式下。

在服务端流量检查-代理模式：设备将对来自 Web 客户端发起的 SSL 连接进行代理，解密数据，并将数据重新加密，以密文的方式发送给 Web 服务器。

在服务端流量检查-卸载模式：设备将对来自 Web 客户端发起的 SSL 连接进行代理，解密数据，并将数据以明文的方式发送给 Web 服务器。</td></tr>
<tr><td>服务端口</td><td>当设备工作在服务端流量检查模式下时，需要指定设备所代理得 Web 服务器的 HTTP 服务的端口号。</td></tr>
<tr><td>服务器信任域</td><td>由于设备代理 Web 服务器与 Web 客户端建立 SSL 连接，所以，需要将 Web 服务器的证书和秘钥对导入到设备中。如何导入证书和秘钥对，可选择“系统 > PKI”并查看相关文档进行操作。导入证书后和秘钥对后，需要在设备中指定此服务端流量检查模式对应的信任域，即，存储此证书和秘钥对的容器。</td></tr>
</table>

绑定 SSL 代理 Profile 到策略规则

将 SSL 代理 Profile 绑定到策略规则后，系统将会对与策略规则相匹配的流量根据 Profile 配置进行处理。

配置域名白名单

对于不需要或无法进行 SSL 代理的网站，可以将其加入域名白名单。系统提供预定义域名白名单，用于保存目前无法进行 SSL 代理的站点，例如需要进行客户端证书认证或网站证书固定的情况。用户也可以根据需要将站点加入网站白名单。预定义的域名白名单条目不允许进行编辑和删除。

新建自定义域名白名单

用户出于业务、隐私或其他自愿原因选择不解密指定站点时，可以将该站点加入域名白名单，设备将不会对白名单内的网站进行 SSL 代理。新建自定义域名白名单，请按照以下步骤进行操作：

1. 点击“对象 > SSL 代理 > 域名白名单”，打开<域名白名单>页面。
2. 点击“新建”，打开<白名单配置>页面。

在<白名单配置>页面，配置相关参数。

选项	说明
域名	指定自定义域名白名单的域名。取值范围为 1-63 个字符。域名注意区分大小写。支持含有通配符“*”的域名，但仅支持一个通配符且必须在域名的起始位置，如“*.net.com”。
描述	添加自定义域名白名单的描述信息。取值范围为 1-63 个字符。
免代理	选择“启用”/“禁用”按钮，可启用/禁用该域名白名单条目。

3. 点击“确定”，完成配置。

编辑自定义域名白名单

编辑自定义域名白名单，请按照以下步骤进行操作：

1. 点击“对象 > SSL 代理 > 域名白名单”，打开<域名白名单>页面。
2. 在域名白名单列表中，勾选需要编辑的自定义域名白名单条目的复选框，点击“编辑”按钮。
3. 在打开的<白名单配置>页面中，修改该域名白名单条目的描述信息以及免代理状态。

4. 编辑完毕，点击页面下方的“确认”按钮保存配置。

删除自定义域名白名单

删除自定义域名白名单，请按照以下步骤进行操作：

1. 点击“对象 > SSL 代理 > 域名白名单”，打开<域名白名单>页面。
2. 在域名白名单列表中，勾选需要删除的自定义域名白名单条目的复选框，点击“删除”按钮，弹出提示框对删除操作进行确认。
3. 点击提示框下方的“确认”按钮，删除此自定义域名白名单条目。

导出域名白名单

系统导出的域名白名单列表文件为.csv 格式，内容为系统当前保存的域名白名单。

从设备导出域名白名单列表到本地，请按照以下步骤进行操作：

1. 点击“对象 > SSL 代理 > 域名白名单”，打开<域名白名单>页面。
2. 点击“导出”按钮。
3. 导出完成后，本地将有下载文件生成。

配置 IP 白名单

配置 IP 白名单后，系统不会对 IP 白名单中的流量进行 SSL 代理。对于不需要或无法进行 SSL 代理的流量，可以将其加入 IP 白名单。IP 白名单列表中包括动态 IP 白名单和静态 IP 白名单。

配置动态 IP 白名单

当设备作为客户端一侧的网关时，出现系统无法对流量进行代理的情况且 SSL Profile 中配置了放行动作时，系统会自动将该流量的 IP 地址加入动态 IP 白名单中，后续不会再对 IP 白名单列表中的流量进行 SSL 代理。由于设备无法代理而被加入动态 IP 白名单的流量超过有效时长后会被重新代理，配置动态 IP 白名单的有效时长可以自动删除当前存在的动态 IP 白名单。系统每 1 小时检查一次动态 IP 白名单，将超过有效时长的条目删除。

配置动态 IP 白名单有效时长

配置动态 IP 白名单有效时长，请按照以下步骤进行操作：

1. 点击“对象 > SSL 代理 > IP 白名单”，打开<IP 白名单>页面。

2. 点击页面上方的“有效时长配置”按钮，打开<有效时长配置>页面。

在<有效时长配置>页面，配置相关参数。

选项	说明
有效时长	配置动态 IP 白名单条目的有效时长，默认为 15 天。取值范围为 1 至 30 天。

3. 点击“确定”，完成配置。

配置动态 IP 白名单永不过期

若要使指定的动态 IP 白名单条目不被系统自动删除，可以配置该动态 IP 白名单条目永不过期。配置动态 IP 白名单永不过期，请按照以下步骤进行操作：

1. 点击“对象 > SSL 代理 > IP 白名单”，打开<IP 白名单>页面。

2. 在 IP 白名单列表中，勾选需要设置为永不过期的动态 IP 白名单条目前的复选框，点击页面上方的“设置 IP 永不过期”按钮。

3. 点击“确定”，完成配置。

配置静态 IP 白名单

系统不会对 IP 白名单中的流量进行 SSL 代理，用户可以根据需要自定义静态 IP 白名单，静态 IP 白名单永不过期。新建静态 IP 白名单，请按照以下步骤进行操作：

1. 点击“对象 > SSL 代理 > IP 白名单”，打开<IP 白名单>页面。

2. 点击“新建”，打开<IP 白名单配置>页面。

在<IP 白名单配置>页面，配置相关参数。

选项	说明
类型	指定静态 IP 白名单条目的 IP 类型为 IPv4 或 IPv6。
IP	配置静态 IP 白名单条目的 IP 地址。
TCP 端口	配置静态 IP 白名单条目的 TCP 端口。系统提供了 4 个预定义端口，分别为 443、465、993 和 995。用户可以根据需要在下拉框中选择，或者点击 ⊕ ，打开<TCP 端口配置>页面，在文本框中输入端口号。

3. 点击“确定”，完成配置。

删除 IP 白名单

删除 IP 白名单，请按照以下步骤进行操作：

1. 点击“对象 > SSL 代理 > IP 白名单”，打开<IP 白名单>页面。
2. 在 IP 白名单列表中，勾选需要删除的白名单条目的复选框，点击“删除”按钮，弹出提示框对删除操作进行确认。
3. 点击提示框下方的“删除”按钮，删除此 IP 白名单条目。

> 注意: 不同平台支持 IP 白名单总数不同，当存在的 IP 白名单数目超过限制个数时，系统会生成事件日志提醒用户清理。

SLB 服务器池

服务器负载均衡功能（SLB）均衡流量，充分利用各内网服务器，提高业务处理能力。可通过如下方式进行服务器负载均衡：

均衡流量到不同的内网服务器的指定端口，适用于不同内网服务器在各自指定端口分别且同时提供同一个应用服务的场景。

均衡流量到同一内网服务器的不同端口，适用于同一服务器在多个端口运行多个进程来提供同一个应用服务的场景。

结合以上两种方式进行流量均衡。

配置 SLB 服务器池条目和监测规则

新建 SLB 服务器池条目和监测规则，按照以下步骤进行操作：

1. 点击“对象 > SLB 服务器池”，进入 SLB 服务器池页面。

2. 点击“新建”，打开<配置 SLB 服务器池>页面。

在<配置 SLB 服务器池>页面中，填写绑定信息。

选项	说明
名称	输入 SLB 服务器池名称。
算法	选择使用的服务器负载均衡算法。
成员	
成员	指定 SLB 服务器池条目成员。 当类型指定为 IPv4 时，根据需要配置 IP/掩码成员或 IP 范围成员，例如：10.100.2.0/24 或 10.100.2.3 – 10.100.2.100； 当类型指定为 IPv6 时，根据需要配置 IPv6 地址/前缀长度或 IPv6 范围成员，例如：2000::2/127 或 2000::2 - 2000::5。
端口	输入服务器端口号。
最大连接数	输入服务器最大连接数。范围是 1 到 1000000000，默认值是 0，表示无最大连接数限制。
权重	输入负载均衡中流量转发的权重，范围是 1 到 255。
添加	将配置的 SLB 服务器池成员添加到 SLB 服务器池条目成员列表中。最多可添加 256 个成员。
探测：点击“添加”按钮，打开“探测”页面。配置完成后，点击“确定”按钮，将配置的监测规则添加到监测规则条目列表中。	
监测类型	选择协议类型。
监测端口	输入监测规则端口号，范围是 1 到 65535。 当 SLB 服务器池中的成员具有同一 IP 地址和不同端口号时，配置监测规则不需要指定端口号。系统将对地址池中的 IP 地址及其端口号进行监测。

选项	说明
	当 SLB 服务器池中的成员只配置了 IP 地址，没有配置端口号时，配置监测规则必须指定端口号。系统将对地址池中的 IP 地址的指定端口号进行监测。 当 SLB 服务器池中的成员都配置了 IP 地址和端口号且这些 IP 地址没有重复的时候，配置监测规则可选择是否指定端口号。如果指定端口号，系统将对地址池中的 IP 地址的指定端口号进行监测。如果不指定端口号，系统将对地址池中成员的 IP 地址及其端口号进行监测。
源接口	指定监测规则源接口。指定后，系统将使用该接口的 IP 地址发送 Ping/TCP/UDP 报文。
发送报文间隔	输入发送 Ping/TCP/UDP 报文的时间间隔，单位为秒。范围是 1 到 255 秒。
重试次数	输入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 3 到 255。
权重	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。
警戒值	输入监测警戒值。范围是 1 到 255。当失败监测规则的权重之和高于设置的监测警戒值后，则认为该服务器不可用。
描述	输入所需的 SLB 服务器池条目描述信息。

3. 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 SLB 服务器池条目详情

用户可以查看 SLB 服务器池条目的详细信息，包括 SLB 服务器池条目的监测规则信息、服务器对应关系以及关联项。查看 SLB 服务器池条目详情，按照以下步骤进行操作：

1. 点击“对象 > SLB 服务器池”，进入 SLB 服务器池页面。
2. 选中 SLB 服务器池条目列表中的 SLB 服务器池条目复选框前的"+"，在 SLB 服务器池条目下方区域查看详情。
3. 在“服务器列表”标签页查看 SLB 服务器池条目与服务器对应关系。
4. 在“监控”标签页查看监测规则的监测类型、监测端口、发送报文间隔、重试次数和权重。
5. 在“关联项”标签页，查看 SLB 服务器池被目的 NAT 规则引用的信息。

时间表

设备支持时间表（Schedule）功能。时间表功能可以使策略规则、NAT 规则在指定的时间生效，也可以控制 PPPoE 接口与因特网的连接时间。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 9：00：30 到 18：00：20。

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 9：00：15 到 13：30：45。

每周一段时间：一周中的一个连续时间段。例如从周一早上 9：30：30 到周三下午 15：00：05。

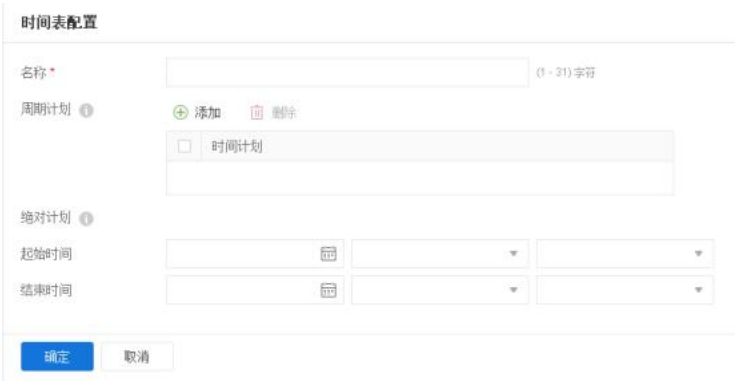
绝对计划

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“对象 > 时间表”。
2. 点击“新建”，打开<时间表配置>页面。



在<时间表配置>页面，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	添加周期计划。

<table>
<tr><th colspan="3">角色映射配置</th></tr>
<tr><td></td><td colspan="2"><table>
<tr><td>类型</td><td>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。

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。</td></tr>
<tr><td>预览</td><td>如需要，点击“预览” 按钮，在<预览>部分预览周期计划详情。</td></tr>
<tr><td>确定</td><td>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。</td></tr>
</table>
每天计划任务。
<table>
<tr><td>起始时间</td><td>指定每天计划的起始时间。</td></tr>
<tr><td>结束时间</td><td>指定每天计划的结束时间。</td></tr>
</table></td></tr>
<tr><td>删除</td><td colspan="2">将选中的周期条目从周期条目列表中删除。</td></tr>
<tr><th colspan="3">绝对计划</th></tr>
<tr><td>起始时间</td><td colspan="2">指定绝对计划的起始日期和时间。</td></tr>
<tr><td>结束时间</td><td colspan="2">指定绝对计划的结束日期和时间。</td></tr>
</table>

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。

注意: 在周期计划和绝对计划中，时间表的开始时间和结束时间的时间间隔不能小于 1 分钟。

AAA 服务器

AAA 服务器是认证服务器，存储用户信息（包括用户名称、密码和各种属性），在用户请求访问网络时，提供认证功能。

AAA 服务器包括以下五种：

本地服务器：Local 服务器即设备本身。将用户信息存储在防火墙上。本地认证速度快，可以降低运营成本，但是存储信息量受设备硬件条件的限制。

外部服务器，包括：

Radius 服务器

LDAP 服务器

Active-Directory 服务器

TACACS+服务器

根据认证类型的不同，选择不同的 AAA 服务器。

802.1x 认证：只能选择 Local 和 Radius 服务器。

IPSec-XAUTH 地址池：可选择 Local、Radius、LDAP、AD、Tacacs+服务器。

配置本地 AAA 服务器

1. 点击“对象 > AAA 服务器”。
2. 点击“新建 > 本地服务器”，打开<本地服务器配置>页面。

在<本地服务器配置>页面进行配置。

选项	说明
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。
密码控制	为防止因管理员长期不修改密码而出现安全问题，可以配置密码控制功能。 允许修改密码：点击“启用”按钮，开启允许本地用户修改登录密码功能。当本地用户通过 Web 认证/SSL VPN 认证后，在认证登录成功页面/客户端修改自己的用户密码。 首次登录修改密码：点击“启用”按钮，开启首次登录修改密码功能。使用该功能前，需先开启允许修改密码功能。开启首次登录修改密码功能后，当用户首次登录进行 Web 认证时，系统将会提示用户“首次登录，请修改密码”强制用户按照已配置的密码复杂度进行修改密码。当用户首次登录建立 SSL VPN 连接时，支持两种模式： 兼容模式：①若 SSL VPN 客户端版本不支持该功能，用户首次登录 SSL VPN 客户端时，无需修改密码，可立即使用；②若 SSL VPN 客户端版本支持该功能，用户首次登录 SSL VPN 客户端时，需立即修改登录密码后才可使用。 强制模式：首次登录 SSL VPN 客户端时，需立即修改登录密码才可使用。 注意: 配置强制模式后，若 SSL VPN 客户端不支持该功能，客户端将无法正常使用。建议升级客户端版本或切换至兼容模式。 支持首次登录修改密码的 SSL VPN 客户端版本：SSL VPN Windows 客户端 1.4.9.1274 及之后版本、Linux 1.4.0 及之后版本、Android 4.5 及之后版本、iOS2.0.6 及之后版本。 SSL VPN Windows 客户端（非管理员）1.5.x 版本不支持首次登录修改密码。 历史密码检查：为保证密码的安全性，系统支持历史密码检查功能。开启历史密码检查功能后，用户在修改密码时，系统将对新密码与历史密码进行重复校验，即新密码不能与最近使用的历史密码重复。若用户的新密码与历史密码重复，系统将会提示“新密码不能与历史密码重复”，提醒用户重新输入新密码。点击“历史密码检查”后的“启用”按

选项	说明
	钮，启用历史密码检查功能，并指定历史密码的个数。范围是 1 到 5 个，默认值是 3，即新密码不能与最近使用的 3 个历史密码重复。 密码有效期检查：点击“启用”按钮，开启密码有效期检查功能，并且配置密码的过期时间。 密码到期提醒：点击“启用”按钮，开启密码到期提醒功能，并且配置在密码到期多少天前提醒用户密码即将到期，取值范围是 1-30 天，例如在密码到期前 10 天提醒用户密码即将到期，默认值是 7。 密码复杂度：密码的复杂度越低，其被破解的可能性就越大，比如包含用户名、密码长度短等。出于安全性的考虑，用户可以开启密码复杂度的配置功能并配置密码复杂度的要求，以确保用户的密码具有较高的复杂度。点击“启用”按钮，开启密码复杂度配置功能。 密码最小长度：指定密码最小长度，范围是 1-16，默认值是 1。 大写字母最小长度：指定密码包含的大写字母的最小长度，范围是 0-16，默认值是 0。 小写字母最小长度：指定密码包含的小写字母的最小长度，范围是 0-16，默认值是 0。 数字最小长度：指定密码包含的数字的最小长度，范围是 0-16，默认值是 0。 特殊字符最小长度：指定密码包含特殊字符（即非数字的字符）的最小长度，范围是 0-16，默认值是 0。 密码不能包含用户名：点击“启用”按钮，不允许密码包含用户名。
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。备份认证服务器可以为系统中已配置的本地、Active-Directory、Radius 或者 LDAP 服务器。
提取用户名格式	
认证	指定认证用户名格式。用户认证时，系统会根据配置的认证用户名格式，对用户名进行提取（不满足格式时，使用原始用户名）。最终使用提取后的用户名进行认证。支持配置的格式包括“domain\username”和“username@domain”。
查找用户组	指定在本地存储中查找用户所属的用户组时支持的用户名格式。在

选项	说明
	基于用户/用户组进行策略控制时，系统会根据配置的格式在本地存储的组织机构中查找用户名所属的用户组。支持配置的格式包括“domain\username”和“username@domain”。
防暴力破解	为了防止非法用户通过暴力方法获取用户名和密码，可以配置基于用户锁定或基于 IP 锁定的防暴力破解功能。 勾选“用户锁定”复选框，开启基于用户的防暴力破解功能。在指定时间（1-180 秒）内，用户连续输错指定次数（1-32 次）的用户名和密码，系统将会按照指定的锁定时间（30-1800 秒）锁定该用户。默认情况下，在 60 秒内，用户连续输错 5 次用户名和密码，将被锁定 600 秒。 勾选“IP 锁定”复选框，开启基于 IP 地址的防暴力破解功能。在指定时间（1-180 秒）内，用户连续输错指定次数（1-2048 次）的用户名和密码，系统将会按照指定的锁定时间（30-1800 秒）锁定该 IP 地址。默认情况下，在 60 秒内，用户连续输错 64 次用户名和密码，将被锁定 60 秒。

3. 点击“确定”。

配置 Radius 服务器

1. 点击“对象 > AAA 服务器”。
2. 点击“新建 > Radius 服务器”，打开<Radius 服务器配置>页面。

在<Radius 服务器配置>页面填写服务器信息。

基本配置	
名称	输入 Radius 认证服务器的名称。
服务器地址	指定认证服务器的 IP 地址（IPv4 地址或 IPv6 地址）或者域名。
虚拟路由器	指定认证服务器所属的虚拟路由器（VRouter）。

基本配置	
端口	指定 Radius 服务器的端口号。默认值是 1812，范围是 1024 到 65535。
密钥	指定 Radius 服务器的密钥。
修改密钥	编辑服务器配置时，可以看到修改密钥功能。开启后，将展示密钥输入框。如需修改，输入新的密钥后保存配置即可。
可选配置	
授权策略	用户通过 Radius 服务器认证时，当用户认证成功后，Radius 服务器会为认证用户创建一条包含目的网段、目的端口、协议以及行为的安全策略，该策略被称为授权策略。用户可以启用授权策略功能，使系统能够从 Radius 服务器获取该授权策略，并加入到系统的策略列表中，使其生效。当认证用户断开连接后，授权策略将会被自动删除。 默认情况下，授权策略为禁用状态。点击“授权策略”后的“启用”按钮，启用授权策略。 启用 Radius 服务器的授权策略后，用户可以指定将获取到的授权策略添加到系统已创建的聚合策略中，作为聚合策略成员排列在聚合策略的末尾，更便于用户统一管理授权策略。如果未添加到聚合策略，授权策略将会默认加入到系统策略列表的末尾。 点击下拉菜单，选择已创建好的聚合策略名称。
提取用户名格式	
认证	指定认证用户名格式。用户认证时，系统会根据配置的认证用户名格式，对用户名进行提取（不满足格式时，使用原始用户名）。最终使用提取后的用户名进行认证。支持配置的格式包括“domain\username”和“username@domain”。
查找用户组	指定在本地存储中查找用户所属的用户组时支持的用户名格式。在基于用户/用户组进行策略控制时，系统会根据配置的格式在本地存储的组织机构中查找用户名所属的用户组。支持配置的格式包括“domain\username”和“username@domain”。
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。
备份服务器 1（或 2）	一台用于备份的 Radius 服务器，与主服务器互为备份。
虚拟路由器 1（或 2）	备份服务器所属的虚拟路由器（VRouter）。
重拨次数	指定 AAA 服务器（认证报文）的重传次数。取值范围为 1 到 10 次，默认为 3 次。
应答超时时间	指定服务器的应答超时时间。取值范围为 1 到 30 秒，默认为 3

<table>
<tr><th colspan="3">基本配置</th></tr>
<tr><td></td><td colspan="2">秒。</td></tr>
<tr><td>备份认证服务器</td><td colspan="2">指定备份认证服务器。为 Radius 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。备份认证服务器可以为系统中已配置的本地、Active-Directory、Radius 或者 LDAP 服务器。</td></tr>
<tr><td>Local NAS IP</td><td colspan="2">指定 LOCAL NAS（Network Access Server） IP 地址。指定后，RADIUS 认证、计费报文中的源地址以及认证报文中的“nas-ip-address”都将变更为该指定地址，从而保证复杂网络环境下，RADIUS 服务器返回的报文能被当前设备正常接收到。指定时，需保证 LACAL NAS IP 需为本设备上的接口 IP，否则可能无法正常发送 RADIUS 认证或计费报文。
注意：
在 HA 环境下，LACAL NAS IP 的配置不会被同步到备设备上，请用户需在主、备设备上进行分别配置。
需保证 RADIUS 服务器上与当前设备是路由可达的。</td></tr>
<tr><td>启用计费功能</td><td colspan="2">点击“启用”按钮，启用 Radius 服务器的计费功能，然后在展开区域配置服务器的计费功能。
<table>
<tr><td>服务器地址</td><td>指定计费服务器的 IP 地址或者域名。</td></tr>
<tr><td>虚拟路由器</td><td>计费服务器所属的虚拟路由器。</td></tr>
<tr><td>端口</td><td>指定计费服务器的端口号。默认值是 1813。取值范围是 1024 到 65535。</td></tr>
<tr><td>密钥</td><td>指定 Radius 服务器的密钥。</td></tr>
<tr><td>修改密钥</td><td>编辑服务器配置时，可以看到修改密钥功能。开启后，将展示密钥输入框。如需修改，输入新的密钥后保存配置即可。</td></tr>
<tr><td>备份服务器 1（或 2）</td><td>指定备份服务器 1 的 IP 地址或者域名。</td></tr>
<tr><td>虚拟路由器 1（或 2）</td><td>备份服务器所属的虚拟路由器（VRouter）。</td></tr>
</table></td></tr>
<tr><td>防暴力破解</td><td colspan="2">为了防止非法用户通过暴力方法获取用户名和密码，可以配置基于用户锁定或基于 IP 锁定的防暴力破解功能。
勾选“用户锁定”复选框，开启基于用户的防暴力破解功</td></tr>
</table>

基本配置	
	能。在指定时间（1-180 秒）内，用户连续输错指定次数（1-32 次）的用户名和密码，系统将会按照指定的锁定时间（30-1800 秒）锁定该用户。默认情况下，在 60 秒内，用户连续输错 5 次用户名和密码，将被锁定 600 秒。 勾选“IP 锁定”复选框，开启基于 IP 地址的防暴力破解功能。在指定时间（1-180 秒）内，用户连续输错指定次数（1-2048 次）的用户名和密码，系统将会按照指定的锁定时间（30-1800 秒）锁定该 IP 地址。默认情况下，在 60 秒内，用户连续输错 64 次用户名和密码，将被锁定 60 秒。
扩展配置	
扩展密码加密算法	点击下拉菜单，在列表中选择 SM4 扩展密码加密算法。配置后，Radius 服务器将使用 SM4 国密加密算法对密码进行加密存储以及加密传输。

3. 点击“确定”。

配置 Active Directory 服务器

1. 点击“对象 > AAA 服务器”。
2. 点击“新建 >Active Directory 服务器”，打开<Active Directory 服务器配置>页面。

点击“基础配置”，填写相关信息。

选项	说明
名称	输入 Active Directory 认证服务器的名称。
服务器地址	指定认证服务器的 IP 地址（IPv4 地址或 IPv6 地址）或者域名。如果要实现单点登录，此处 IP 需与安装 AD Agent 客户端的设备 IP 地址一致。

选项	说明
虚拟路由器	指定认证服务器所属的虚拟路由器（VRouter）。
端口	指定 Active Directory 服务器的端口号。默认值是 389，范围是 1 到 65535。
Base-dn	Base-dn 是指当前 AD 服务器搜索的路径起始点。以服务器域名为 abc.xyz.com 为例，Base-dn 的输入格式是“dc=abc,dc=xyz,dc=com"。
Login-dn	DN 意为可辨别名称（distinguished name）。 当认证方式指定为明文时，需要配置 Login-dn 的属性值，即有权限读取用户信息的 AD 服务器的用户名。 输入格式是“cn=xxx, DC=xxx,...”，举例说明：服务器的域名为 abc.xyz.com, AD 服务器的管理员名为 administrator，该管理员名位于“Users”路径下， 那么 login-dn 应写为“cn=administrator,cn=users,dc=abc,dc=xyz,dc=com”。
sAMAccountName	当认证方式指定为 MD5 时，需要配置 sAMAccountName 的属性值，即有权限读取用户信息的 AD 服务器的用户名。输入格式是“xxx”,举例说明：AD 服务器的管理员名为 administrator，那么 sAMAccountName 应写为“administrator”。
认证方式	指定用户认证或用户同步方法，明文或 MD5 摘要。默认为 MD5 摘要。 指定使用 MD5 摘要方法后需要配置 sAMAccountName 属性值，如果没有配置，那么从服务器同步用户的过程中将使用明文方法，认证用户的过程中将使用 MD5 摘要方法。
密码	指定登录 AD 服务器的用户名所对应的密码。
SSL 加密连接	点击“启用”按钮，开启 SSL 加密连接功能。开启该功能后，系统通过 SSL 加密方式连接 Active Directory 认证服务器。
修改密钥	编辑服务器配置时，可以看到修改密钥功能。开启后，将展示密钥输入框。如需修改，输入新的密钥后保存配置即可。
可选配置	
提取用户名格式	
认证	指定认证用户名格式。用户认证时，系统会根据配置的认证用户名格式，对用户名进行提取（不满足格式时，使用原始用户名）。最终使用提取后的用户名进行认证。支持配置的格式包括“domain\username”和“username@domain”。
查找用户组	指定在本地存储中查找用户所属的用户组时支持的用户名格式。在基于用户/用户组进行策略控制时，系统会根据配置的格式在本地存储的组织机构中查找用户名所属的用户组。支持配置的格式包括“domain\username”和“username@domain”。
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。

选项	说明
备份服务器 1（或 2）	一台用于备份的 AD 服务器，与主服务器互为备份。
虚拟路由器 1（或 2）	备份服务器所属的虚拟路由器（VRouter）。
认证 Base-dn	指定认证 Base-DN 的具体内容。该 Base-DN 路径下的所有用户（包括用户组中的直属用户）将允许通过认证。DN 的格式为 "OU=xxx, DC=xxx,…".
备份认证服务器	指定备份认证服务器。为 AD 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。备份认证服务器可以为系统中已配置的本地、Active-Directory、Radius 或者 LDAP 服务器。
防暴力破解	为了防止非法用户通过暴力方法获取用户名和密码，可以配置基于用户锁定或基于 IP 锁定的防暴力破解功能。 勾选“用户锁定”复选框，开启基于用户的防暴力破解功能。在指定时间（1-180 秒）内，用户连续输错指定次数（1-32 次）的用户名和密码，系统将会按照指定的锁定时间（30-1800 秒）锁定该用户。默认情况下，在 60 秒内，用户连续输错 5 次用户名和密码，将被锁定 600 秒。 勾选“IP 锁定”复选框，开启基于 IP 地址的防暴力破解功能。在指定时间（1-180 秒）内，用户连续输错指定次数（1-2048 次）的用户名和密码， 系统将会按照指定的锁定时间（30-1800 秒）锁定该 IP 地址。默认情况下，在 60 秒内，用户连续输错 64 次用户名和密码，将被锁定 60 秒。

点击“同步配置”，会收到是否下发配置的提示。点击“确定”下发基础配置后，才可以开始同步配置。

选项	说明
同步	点击“启用”按钮，开启同步功能。开启后，可以指定自动同步方式；禁用后，系统停止同步并清除原有同步信息，且无法指定自动同步方式。默认情况下，系统每隔 30 分钟将认证服务器上的用户信息同步到本地一次。
自动同步	单击选择自动同步方式：按时间间隔同步、每天同步和一次性同步。 按时间间隔同步　指定为按时间间隔同步，并配置自动同步的间隔时间。取值范围为 15 到 1440，单位为分钟， 默认值为 30。 每天同步　指定为每天同步，并配置每天执行自动同步的时间点。格式为 HH:MM，HH 和 MM 分别代表小时和分钟。

选项	说明
	一次性同步　指定为一次性同步，当 AD 服务器配置信息有更改时，系统将会自动同步。首次配置该命令后，系统会执行一次同步。
同步工作模式	指定同步用户的模式，包括按组同步和按 OU（OrganizationUnit）同步。默认情况下，系统会按组同步用户信息到本地。
同步对象	筛选同步到本地的信息，并保留指定对象的信息。可选择用户和用户组，默认情况下均勾选。
OU 最大深度	指定同步的 OU 的最大深度。取值范围为 1 到 12，默认值为 12。超过最大深度的 OU 组织结构不会被同步，但是超过最大深度的所有用户会被同步，并且被同步到其所属最大限制深度的 OU 中。需要注意的是，如果各层级 OU 的名称总长度（包括“OU=”和标点符号）大于 128 个字符，那么超过此长度的 OU 信息将不会被同步。
用户过滤条件	指定过滤条件后，系统只同步或认证符合过滤条件的用户。长度为 0 到 120 个字符的字符串。常用的操作符如下：=（等于）、&（条件与）、|（条件或）、！（条件非）、*（通配符，代替 0 个或多个字符）、～=（类似，用于模糊查询）、>=（字典序大于等于）、<=（字典序小于等于）。例如，只同步或认证 DN 为“CN=Admin,DC=test,DC=com”的用户组中的用户，用户过滤条件应设置为“memberOf=CN=Admin,DC=test,DC=com”。其中，memberOf 指 AD 服务器中用户组属性（不能更改），“CN=Admin,DC=test,DC=com”代表需要同步或认证的用户组的 DN。
同步 Base-dn	同步 Base-DN 是指系统从 Active Directory 服务器同步用户和用户组时的路径起点。点击输入框，在“服务器路径”页面选择需要同步的路径，选择的路径下所有的用户和用户组将同步到本地。可以选择最多 32 条路径，DN 的格式为"OU=xxx, DC=xxx,…".

3. 点击“确定”。

配置 LDAP 服务器

1. 点击“对象 > AAA 服务器”。

2. 点击“新建 > LDAP 服务器”，打开<LDAP 服务器配置>页面。

点击“基础配置”，填写相关信息

选项	说明
名称	输入 LDAP 认证服务器的名称
服务器地址	指定认证服务器的 IP 地址（IPv4 地址或 IPv6 地址）或者域名。
虚拟路由器	指定认证服务器所属的虚拟路由器（VRouter）。
端口	指定 LDAP 服务器的端口号。默认值是 389，范围是 1 到 65535。
Base-dn	Base-DN 是指当 LDAP 服务器收到一个认证请求时，目录查询的起始点。该选项用于指定 Base-dn 的具体内容。
Login-dn	指定登录 DN（通常为 LDAP 服务器预设的具有查询权限的用户账号）的具体内容。
Authid	指定 Authid 的值，为 1 到 63 个字符的字符串，区分大小写。
认证方式	指定用户认证或用户同步方法，明文或 MD5 摘要。默认为 MD5 摘要。 指定使用 MD5 摘要方法后需要配置 Authid 属性值，如果没有配置，那么从服务器同步用户的过程中将使用明文方法，认证用户的过程中将使用 MD5 摘要方法。
密码	指定 login-dn 所对应的密码，为管理员 DN 所对应的密码。
SSL 加密连接	点击“启用”按钮，开启 SSL 加密连接功能。开启该功能后，系统通过 SSL 加密方式连接 LDAP 认证服务器。
修改密码	编辑服务器配置时，可以看到修改密码功能。开启后，将展示密码输入框。如需修改，输入新的密码后保存配置即可。
可选配置	
提取用户名格式	
认证	指定认证用户名格式。用户认证时，系统会根据配置的认证用户名格式，对用户名进行提取（不满足格式时，使用原始用户名）。最终使用提取后的用户名进行认证。支持配置的格式包括“domain\username”和“username@domain”。

选项	说明
查找用户组	指定在本地存储中查找用户所属的用户组时支持的用户名格式。在基于用户/用户组进行策略控制时，系统会根据配置的格式在本地存储的组织机构中查找用户名所属的用户组。支持配置的格式包括“domain\username”和“username@domain”。
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。
备份服务器 1（或 2）	一台用于备份的 LDAP 服务器，与主服务器互为备份。
虚拟路由器 1（或 2）	备份服务器所属的虚拟路由器（VRouter）。
认证 Base-dn	指定认证 Base-DN 的具体内容。该 Base-DN 路径下的所有用户（包括用户组中的直属用户）将允许通过认证。DN 的格式为 "OU=xxx, DC=xxx,…".
备份认证服务器	指定备份认证服务器。为 LDAP 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。备份认证服务器可以为系统中已配置的本地、Active-Directory、RADIUS 或者 LDAP 服务器。
防暴力破解	为了防止非法用户通过暴力方法获取用户名和密码，可以配置基于用户锁定或基于 IP 锁定的防暴力破解功能。 勾选“用户锁定”复选框，开启基于用户的防暴力破解功能。在指定时间（1-180 秒）内，用户连续输错指定次数（1-32 次）的用户名和密码，系统将会按照指定的锁定时间（30-1800 秒）锁定该用户。默认情况下，在 60 秒内，用户连续输错 5 次用户名和密码，将被锁定 600 秒。 勾选“IP 锁定”复选框，开启基于 IP 地址的防暴力破解功能。在指定时间（1-180 秒）内，用户连续输错指定次数（1-2048 次）的用户名和密码，系统将会按照指定的锁定时间（30-1800 秒）锁定该 IP 地址。默认情况下，在 60 秒内，用户连续输错 64 次用户名和密码，将被锁定 60 秒。

点击“同步配置”，填写相关信息（添加同步配置前需先下发基础配置）。

选项	说明
同步	点击“启用”按钮，开启同步功能。开启后，可以指定自动同步方式；禁用后，系统停止同步并清除原有同步信息，且无法指定自动同步方式。默认情况下，系统每隔 30 分钟将认证服务器上的用户信息同步到本地一次。
自动同步	单击选择自动同步方式：按时间间隔同步、每天同步和一次性同步。

选项	说明
	按时间间隔同步　指定为按时间间隔同步，并配置自动同步的间隔时间。取值范围为 15 到 1440，单位为分钟， 默认值为 30。 每天同步　指定为每天同步，并配置每天执行自动同步的时间点。格式为 HH:MM，HH 和 MM 分别代表小时和分钟。 一次性同步　指定为一次性同步，当 LDAP 服务器配置信息有更改时，系统将会自动同步。首次配置该命令后，系统会执行一次同步。
同步工作模式	指定同步用户的模式，包括按组同步和按 OU（OrganizationUnit）同步。默认情况下，系统会按组同步用户信息到本地。
同步对象	筛选获取的同步信息，并保留指定对象的信息。可选择用户和用户组，默认情况下均勾选。
OU 最大深度	指定同步的 OU 的最大深度。取值范围为 1 到 12，默认值为 12。超过最大深度的 OU 组织结构不会被同步，但是超过最大深度的所有用户会被同步，并且被同步到其所属最大限制深度的 OU 中。 需要注意的是，如果各层级 OU 的名称总长度（包括“OU=”和标点符号）大于 128 个字符，那么超过此长度的 OU 信息将不会被同步。
用户过滤条件	指定过滤条件后，系统只同步或认证符合过滤条件的用户。长度为 0 到 120 个字符的字符串。例如，用户过滤条件设置为“（|（objectclass=inetOrgperson）（objectclass=person））”，表明只同步或认证所有被定义为 inetOrgperson 或者 person 的用户。常用的操作符如下：=（等于）、&（条件与）、|（条件或）、！（条件非）、*（通配符，代替 0 个或多个字符）、～=（类似，用于模糊查询）、>=（字典序大于等于）、<=（字典序小于等于）。
用户名属性	用户名属性是指 LDAP 服务器上唯一标识名称的字符串。 该字符串通常为 uid（User ID）或 cn（Common Name），默认值为 uid。
用户组属性	用户组属性是指 LDAP 服务器上唯一标识用户组名称的字符串。该字符串通常为 uid（User ID）或 cn（Common Name），默认值为 uid。
成员属性	指定 LDAP 服务器的成员属性名称。默认为 uniqueMember。
组类别	指定组对象 objectClass 的值。默认为 groupOfUniqueNames。
同步 Base-dn	同步 Base-DN 是指系统从 LDAP 服务器同步用户和用户组时的路径起点。点击输入框，在“服务器路径”页面选择需要同步的路径，选择的路径下所有的用户和用户组将同步到本地。可以选择最多 32 条路径，DN 的格式为"OU=xxx, DC=xxx,…".

3. 点击“确定”。

配置 TACACS+服务器

1. 点击“对象 > AAA 服务器”。
2. 点击“新建 > TACACS+服务器”，打开<TACACS+服务器配置>页面。

在<TACACS+服务器配置>页面填写服务器信息。

基本配置	
名称	输入 TACACS+认证服务器的名称。
服务器地址	指定认证服务器的 IP 地址或者域名。
虚拟路由器	指定认证服务器所属的虚拟路由器（VRouter）。
端口	指定 TACACS+服务器的端口号。默认值是 49，范围是 1 到 65535。
密钥	指定 TACACS+服务器的密钥。
修改密钥	编辑服务器配置时，可以看到修改密钥功能。开启后，将展示密钥输入框。如需修改，输入新的密钥后保存配置即可。
可选配置	
提取用户名格式	
认证	指定认证用户名格式。用户认证时，系统会根据配置的认证用户名格式，对用户名进行提取（不满足格式时，使用原始用户名）。最终使用提取后的用户名进行认证。支持配置的格式包括“domain\username”和“username@domain”。
查找用户组	指定在本地存储中查找用户所属的用户组时支持的用户名格式。在基于用户/用户组进行策略控制时，系统会根据配置的格式在本地存储的组织机构中查找用户名所属的用户组。支持配置的格式包括“domain\username”和“username@domain”。
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。
备份服务器 1（或 2）	一台用于备份的 TACACS+服务器，与主服务器互为备份。

基本配置	
虚拟路由器 1（或 2）	备份服务器所属的虚拟路由器（VRouter）。
防暴力破解	为了防止非法用户通过暴力方法获取用户名和密码，可以配置基于用户锁定或基于 IP 锁定的防暴力破解功能。 勾选“用户锁定”复选框，开启基于用户的防暴力破解功能。在指定时间（1-180 秒）内，用户连续输错指定次数（1-32 次）的用户名和密码，系统将会按照指定的锁定时间（30-1800 秒）锁定该用户。默认情况下，在 60 秒内，用户连续输错 5 次用户名和密码，将被锁定 600 秒。 勾选“IP 锁定”复选框，开启基于 IP 地址的防暴力破解功能。在指定时间（1-180 秒）内，用户连续输错指定次数（1-2048 次）的用户名和密码，系统将会按照指定的锁定时间（30-1800 秒）锁定该 IP 地址。 默认情况下，在 60 秒内，用户连续输错 64 次用户名和密码，将被锁定 60 秒。

连通性测试

配置完成 AAA 服务器的参数后，可以立即测试一下参数是否正确，服务器是否能够连通。

执行连通性测试，按照以下步骤进行：

1. 在“对象 > AAA 服务器”，点击“新建”。
2. 根据实际认证服务器，选择服务器类型，可以是 Radius、AD、LDAP 或 TACACS+服务器。本地服务器无需进行连通性测试。
3. 按照上面的参数说明填写完成后，点击“连通测试”。
4. 如果服务器为 Radius 或 TACACS+类型，在系统打开的<连通测试>页面中，输入一个可用的用户名和密码。如果服务器为 AD 或 LDAP 服务器，该测试直接使用 login-dn 和密钥的值进行测试。

5. 出现“连通测试成功”提示信息时，标明 AAA 服务器配置正确。

如果出现错误提醒信息，可能是如下原因：

连接 AAA 服务器超时：可能配置了错误的地址、端口号或虚拟 VR。

AAA 服务器配置错误：表示密钥错误。

用户名或密码错误：表示测试所使用的用户名或密码错误。

配置 Radius 动态授权

Radius 动态授权功能，包含以下两点内容：

当用户认证成功后，Radius 服务器可以发送 Radius CoA（Change of Authorization）请求消息将认证用户的权限下发到设备，设备自动生成该用户的安全策略规则，当该用户下线时，设备将会自动删除该用户的安全策略规则。

当 SCVPN 用户认证成功后，Radius 服务器可以发送 Radius DM（Disconnect Messages）请求消息，将该计费用户信息（包括用户名称、用户 IP 地址、用户计费 ID 等）下发到设备，设备能够断开指定 SCVPN 认证用户的连接并结束计费。

配置 Radius 动态授权功能，请按照以下步骤进行操作：

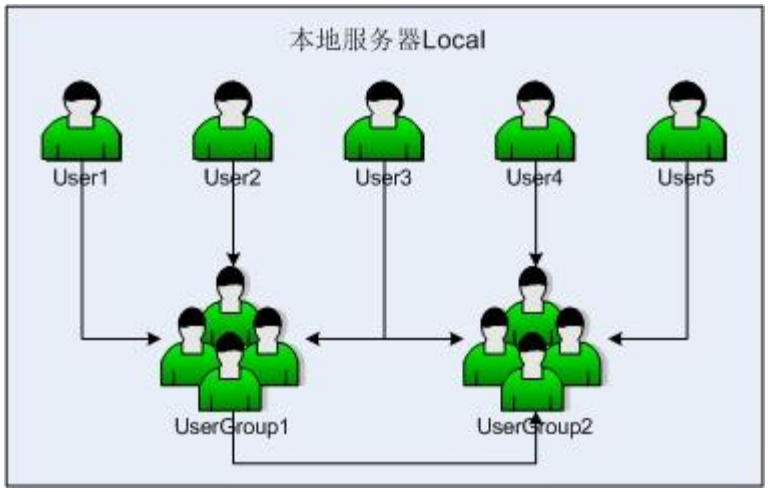
1. 选择“对象>Radius 动态授权”，打开 Radius 动态授权配置页面。

2. 点击“Radius 动态授权”后的“启用”按钮，开启 Radius 动态授权功能。
3. 在“端口”文本框中输入动态授权的端口号，默认值是 3799，取值范围是 1024 到 65535。
4. 在“授权服务器”处，点击 “新建”按钮，然后在表格中指定授权服务器 IP 地址、授权请求的目的 IP 地址以及共享密钥。
5. 如需删除授权服务器，在列表中勾选授权服务器复选框，然后点击“删除”按钮。
6. 点击“应用”按钮，完成配置。
7. 如需修改共享密钥，点击共享密钥输入框，开启修改功能，然后在输入框中输入新的密钥保存即可。

注意: 如果需要使用 Radius 授权功能，请先开启并配置 Radius 服务器的计费功能。

用户

系统中的用户（User）是指使用设备提供的功能、服务、被设备认证、管理的用户。被设备认证的用户有本地和外部两种。本地用户（Local User）由系统管理员创建，分属于不同的本地认证服务器，储存在系统的配置文件中；外部用户（External User）储存在外部服务器上，例如 AD 服务器、LDAP 服务器。为方便管理用户，系统支持用户组功能，属于同一本地认证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，属于同一个本地认证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。

本地用户

本节主要介绍本地用户和用户组的配置。

选择“对象 > 用户 > 本地用户”或者“零信任访问 > 用户 > 本地用户”，打开本地用户页面，在该页面可以查看以下内容：

用户点击页面左上角的“本地服务器”下拉框，切换本地用户服务器。

提供红 已过期 、橙 一周内过期 、黄 一月内过期 三种颜色对列表中的已过期、一周内过期、一月内过期的用户进行标识，便于管理与维护。

在列表中可以查看本地用户信息，包括用户的“用户”，“用户组”，“账户到期日”，“手机号码”和“描述”。

新建用户

新建用户，请按照以下步骤进行操作：

1. 选择“对象 > 用户 > 本地用户”或者“零信任访问 > 用户 > 本地用户”。
2. 点击“新建 > 用户”，打开<用户配置>页面。

在<用户配置>页面，对本地用户进行基本配置。

选项	说明
名称	输入用户的名称。
密码加密方式	指定用户密码的加密方式，即指定用户密码是否采用可逆加密算法或不可逆加密算法。 可逆：表示系统将使用 AES 可逆加密算法对用户密码进行加密，在某些认证场景，系统可对密码进行解密后使用。 不可逆：表示系统将使用 SHA 不可逆加密算法对用户密码进行加密，密码将无法被解密。此时该用户通过 CHAP（挑战握手认证协议，L2TP VPN 和 802.1X 中使用该协议）方式将无法认证通过。
密码	输入用户的密码。
确认密码	再次输入密码以确认。
修改密码	编辑用户配置时，可以看到修改密码功能。开启后，将展示密码输入框。如需修改，输入新的密码后保存配置即可。
手机号码	配置用户的手机号码，在用户登录 SCVPN 时，设备将验证码发送到该手机号码上。
邮箱	输入用户的邮箱地址。取值范围为 1 至 127 个字符。如果启用了邮件口令认证功能，用户会通过此邮箱接收包含认证码信息的邮件。关于邮件口令认证功能的详细信息，请见配置 SSL VPN。
描述	输入用户描述信息。

选项	说明
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。注意：当一个用户加入的用户组个数超过 256 时，按照加入的顺序，只有前 256 个生效。该原则适用于外部认证服务器上配置的用户组。
账户到期日	点击“启用”按钮，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。

点击“VPN 配置”，展开 VPN 配置项，为拨号 VPN 指定 IKE ID 和为 PnPVPN 客户端用户配置网络参数信息。

选项	说明
IKE ID	为拨号 VPN 用户指定 IKE 标识类型，选中所需类型即可。当选择 FQDN、ASN1DN 或 KEY-ID 时还需在后面的文本框内指定标识内容。
PnPVPN	
DHCP 起始地址	DHCP 地址池的起始 IP 地址。
DHCP 结束地址	DHCP 地址池的终止 IP 地址。
DHCP 网络掩码	DHCP 地址池的网络掩码。
DHCP 网关	DHCP 地址池的网关地址。该地址用来作为 PnPVPN 客户端内网接口的 IP 地址，并被设置为 PC 的网关地址，PC 的 IP 地址由以上设置的 DHCP 地址池的网段以及网络掩码确定，所以网关地址应该和 DHCP 地址池在同一个网段。
DNS1	指定 DNS 服务器的 IP 地址。可同时指定 1 个主 DNS 服务器（DNS1）和最多 3 个备份服务器。
DNS2	
DNS3	
DNS4	
WINS1	指定 WINS 服务器的 IP 地址，可同时指定一个主 WINS 服务器和一个备份 WINS 服务器。
WINS2	
隧道 IP1	指定 PnPVPN 客户端主隧道接口的 IP 地址。选择“启用源 NAT”复选框，开启 SNAT 功能。
隧道 IP2	指定 PnPVPN 客户端备隧道接口的 IP 地址。

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“对象 > 用户 > 本地用户”。

   点击“新建 > 用户组”，打开<用户组配置>页面。

选项	说明
名称	输入用户组的名称。
用户	指定用户组所包含的用户组成员。 点击文本框，在弹出的用户列表中选中需要指定的用户或者用户组，即可将其添加到“用户”的文本框中。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。 点击“用户”文本框”中已选用户或用户组最右侧“×”按钮，即可移除指定的用户或用户组。

2. 点击“确定”按钮，完成配置。

导出用户列表

系统导出的用户列表文件为.csv 格式，内容为系统当前保存的用户列表信息。

从设备导出用户列表到本地，请按照以下步骤进行操作：

1. 选择“对象 > 用户 > 本地用户”或者“零信任访问 > 用户 > 本地用户”。
2. 点击“导出用户列表”按钮，弹出导出进度条。
3. 导出完成后，本地将有下载文件生成。

导入用户列表

系统支持导入 GBK 编码、UTF-8 编码格式的.csv 格式的用户列表文件。导入时，系统将会对整个文件进行合法性和用户密码复杂度检查，检查成功后完成导入，若检查失败，则导入失败。

下图为.csv 格式的用户列表文件及参数描述示例：

	servername	username	password	group	description	phone	expire
2	local	test	testadfdgfadg	group1;group2;group3;group4	desc1	112356	2/2/2020 12:12
3	local	test1	testadfdgfadg	group	desc1	112356	2/2/2020 12:12
4	local	test2		group	desc1	112356	2/2/2020 12:12
5	local	test3	testadfdgfadg		desc1	112356	2/2/2020 12:12
6	local	test5	testadfdgfadg	group		112356	2/2/2020 12:12
7	local	test6	testadfdgfadg	group	desc1		17/1/2020 12:12
8	local	test7	testadfdgfadg	group	desc1	112356	
9	local	test8	testadfdgfadg	group	desc1	112356	1/1/2020 12:12
10							
11	本地AAA服务器名称	用户名称	用户密码	用户组名称	描述	手机号码	账户到期日
12							
13							
14							
15							

注意: 在导入用户列表文件前，请仔细阅读上图中的批注文字，并且将用户信息按照格式要求填写。

导入用户列表到设备，请按照以下步骤进行操作：

1. 选择“对象 > 用户 > 本地用户”或者“零信任访问 > 用户 > 本地用户”。
2. 点击“导入用户列表”按钮，打开<导入用户列表>页面。
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。

注意:

导入\导出文件中的用户密码均为明文。若导入时输入的字符串匹配 AES 加密格式，则按密文处理。

导入的文件内容格式请尽量与导出文件保持一致。

导入时，若相同服务器下存在相同用户名，则会覆盖原有的用户列表信息。

导入时，若当前系统里不存在该用户，系统自动创建新用户。

导入的用户列表文件中，“用户名称”参数不能包含斜线、逗号、双引号、问号、“@”；“用户组名称”参数不能包含逗号、双引号、问号。

导入的用户列表文件中，“账号到期日”参数需符合 DD/MM/YYYY HH:SS 格式。

LDAP 用户

本节主要介绍 LDAP 用户相关配置。用户点击页面左上角的“LDAP 服务器”下拉框，切换 LDAP 用户服务器。

同步用户

用户可以将 LDAP 服务器中的用户同步到设备中。同步 LDAP 用户，首先要配置需要获取用户和认证的 LDAP 服务器。同步用户，按照以下步骤进行操作：

1. 选择“对象 > 用户 > LDAP 用户”或者“零信任访问 > 用户 > LDAP 用户”，进入 LDAP 用户配置页面。
2. 点击“同步用户 ”按钮，进行同步用户操作。

注意: 系统默认支持自动同步功能。当配置 LDAP 服务器后，系统会自动同步 LDAP 服务器中的用户，之后每隔 30 分钟同步一次。

Active Directory 用户

本节主要介绍 Active Directory（AD）用户相关配置。用户点击页面左上角的“Active Directory”下拉框，切换 AD 用户服务器。

同步用户

用户可以将 AD 服务器中的用户同步到设备中。同步 AD 用户，首先要配置需要获取用户和认证的 AD 服务器。同步用户，请按照以下步骤进行操作：

1. 选择“对象 > 用户 > Active Directory 用户”或者“零信任访问 > 用户 > Active Directory 用户”，进入 AD 用户配置页面。
2. 点击“同步用户 ”按钮，进行同步用户操作。

注意: 系统默认支持自动同步功能。当配置 AD 服务器后，系统会自动同步 AD 服务器中的用户，之后每隔 30 分钟同步一次。

用户绑定

本节主要介绍用户绑定相关配置。

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“对象 > 用户 > 用户绑定”或者“零信任访问 > 用户 > 用户绑定”。
2. **点击“添加用户绑定”按钮，打开<IP MAC 绑定>页面。**

用户	
用户	指定需要绑定的用户名称。 在下拉菜单中选择指定用户，点击“确定”。点击“清除”，可清除已选定的用户。
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，支持 IPv4 地址和 IPv6 地址。 MAC：需要在“MAC”文本框中输入 MAC 地址。
虚拟路由器	在“虚拟路由器”下拉菜单选择所属的虚拟路由器。
只用于 Web 认证“IP-用户	选中该复选框，则该 IP-用户绑定关系只用于 Web 认证时 IP 和用户的对应关系检查。

3. 点击“确定”按钮，完成配置。

导入用户绑定列表

导入用户列表绑定到设备，请按照以下步骤进行操作：

1. 选择“对象 > 用户 > 用户绑定”或者“零信任访问 > 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本地，请按照以下步骤进行操作：

1. 选择“对象 > 用户 > 用户绑定”或者“零信任访问 > 用户 > 用户绑定”。
2. 在“导出”下拉菜单中选择要导出用户的类别（包含本地用户、LDAP 用户、Active Directory 用户、全部共四种类别），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者某角色可以独享一定带宽等。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。功能配置中，为不同的角色指定不同的服务，由此，角色对应的用户即可拥有其角色的服务。

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 QoS：实现不同用户的带宽控制。

基于角色的统计集：统计不同用户的带宽、会话以及新建会话数。

基于角色的会话限制：实现对特定用户的会话数限制。

SCVPN 基于角色的主机安全检测：实现不同用户对特定资源的访问控制。

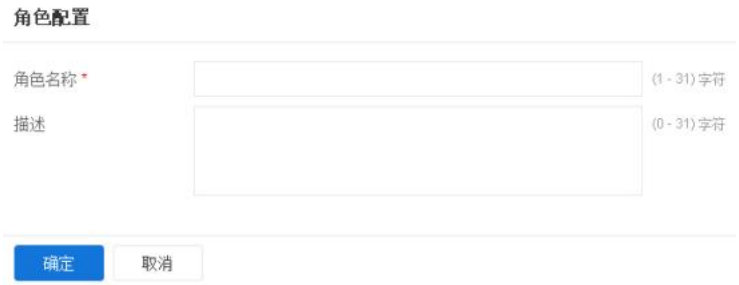
基于角色的策略路由：实现根据不同源用户选择路由。

配置角色

新建角色

新建角色，请按照以下步骤进行操作：

1. 选择“对象 > 角色 > 角色”，进入角色页面。
2. **点击“新建”按钮，打开<角色配置>页面。**



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。

关联到角色映射

用户可以通过该功能或新建角色映射，将角色关联到用户、用户组、证书名称、组织机构、用户属性或者证书 DN。新建角色映射规则后，用户可点击“关联到映射”，将所选角色重新关联。

重新关联角色，请按照以下步骤进行操作：

1. 选择“对象 > 角色 > 角色”。
2. 在角色列表中，勾选需要重新关联的角色，点击“关联到映射”按钮，打开配置页面。

3. 点击“新建”按钮，将指定名称的角色映射条目添加到上方的角色映射条目列表中。在“映射名称”的第一个下拉列表中选择已创建的角色映射规则名称；在第二个下拉列表中指定用户、用户组、证书名称（USB Key 证书 CN 字段）、组织机构（USB Key 证书 OU 字段）、用户属性、证书 DN 或者 any。如果选中“用户”、“用户组”、“证书名称”、“组织机构”、“用户属性”或者“证书 DN”，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、证书名称、组织机构、用户属性或者证书 DN。
4. 如需要，可再添加其它角色映射条目。
5. 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。
6. 点击“确定”按钮，完成配置。新添加的角色映射规则同步显示在角色列表和角色映射列表中。

新建角色映射

新建角色映射规则，请按照以下步骤进行操作：

1. 选择“对象 > 角色 > 角色映射”。
2. 点击“新建”按钮，打开<角色映射配置>页面。

3. 在“映射名称”文本框输入角色映射规则名称。
4. 在“角色映射规则”部分，点击“新建”按钮，将角色映射条目添加到上方的角色映射条目列表中。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、证书名称（USB

Key 证书 CN 字段）、组织机构（USB Key 证书 OU 字段）、用户属性、证书 DN 或者 any。如果选中“用户”、“用户组”、“证书名称”、“组织机构”、“用户属性”或者“证书 DN”，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、证书名称、组织机构、用户属性或者证书 DN。

5. 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。新添加的角色映射规则同步显示在角色映射列表和角色列表中。

配置用户属性实例

配置用户属性实例，请按照以下步骤进行操作：

1. 选择“对象 > 角色 > 角色映射”。
2. 在页面右上角，点击“相关配置”，在弹出菜单中选择“用户属性”，打开<用户属性>页面。
3. 点击“新建”按钮，打开<用户属性配置>页面。

在<用户属性配置>页面，填写如下配置信息。

选项	说明
名称	指定用户属性实例的名称。
类型	指定协议类型，可以是 RADIUS 或者 AD/LDAP。
规则命中方式	指定该用户属性实例命中角色映射规则的方式，包括： 任意一个条件满足，则命中当前规则：如果用户满足用户属性实例中的任意一条过滤条件，该用户就会匹配到用户属性实例映射到的角色； 所有条件满足，则命中当前规则：仅当用户满足用户属性实例中的全部过滤条件，该用户才会匹配到用户属性实例映射到的角色。
当前过滤条件	指定该用户属性实例的过滤条件。点击“新建”按钮，在“属性”文本框中输入用户属性名称或者从下拉菜单中选择常用用户属性；在“操

选项	说明
	作”下拉菜单中选择映射条件，可以是 equal-to（等于）、greater-than（大于）、less-than（小于）、contain（包含）、start-with（起始于）、end-with（终止于）、或者 same-as（一致）；在“值”文本框中输入用户属性的映射值。注意: 每个用户属性实例中最多允许配置 8 条过滤条件； 当协议类型为 RADIUS 时，字符串类型的用户属性对应的映射条件只能为 contain（包含）、start-with（起始于）、end-with（终止于）或者 same-as（一致）；数字类型的用户属性对应的映射条件只能为 equal-to（等于）、greater-than（大于）或者 less-than（小于）； 当映射条件为 contain（包含）、start-with（起始于）、end-with（终止于）、或者 same-as（一致）时，映射值可以为字符串或者数字；当映射条件为 equal-to（等于）、greater-than（大于）或者 less-than（小于）时，映射值只能为数字。

4. 点击“确定”按钮，完成配置。新添加的用户属性实例会显示在用户属性实例列表中。
5. 如需要，可再添加其它用户属性实例。
6. 如需删除用户属性实例，选中用户属性实例列表中的用户属性实例复选框，点击“删除”按钮，删除相应的用户属性实例。

注意: 系统最多允许配置 64 个用户属性实例。

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“对象 > 监测对象”。
2. 点击“新建”按钮，打开<监测对象配置>页面。

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	选择监测对象的类型。可以是“接口”、“HTTP/ICMP/ICMPv6/ARP/NDP/DNS/TCP”或者“链路质量探测”。一个监测对象中可以配置多种监测类型的监测条目。 选择“接口”。 点击“添加”按钮，添加接口类型的监测成员。 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/ICMP/ICMPv6/ARP/NDP/DNS/TCP”。 点击“添加”按钮，添加HTTP/ICMP/ICMPv6/ARP/NDP/DNS/TCP 类型的监测成员 。 IP 类型：通过 HTTP/DNS/TCP 报文对目标进行监测时，该选项用于指定监测目标地址类型，IPv4 或者 IPv6。 IP/主机：通过 HTTP/ICMP/ICMPv6/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/NDP 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

选项	说明
	255。 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/ICMP/ICMPv6/ARP/NDP/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/ICMP/ICMPv6/ARP/NDP/DNS/TCP 检测报文的出接口。 接收报文接口：指定 HTTP/ICMP/ICMPv6/ARP/DNS/TCP 检测报文的源接口。 选择“链路质量探测”单选按钮。 点击“添加”按钮，添加链路质量探测类型的监测成员 。 IP 类型：指定链路质量探测类型的监测成员的地址类型，包括 IPv4 和 IPv6。当指定“IPv4”时，只对被监测接口的 IPv4 类型的流量进行监测；当指定“IPv6”时，只对被监测接口的 IPv6 类型的流量进行监测。 探测接口：指定被监测接口的名称。 探测时间：指定每个监测周期的持续时间，单位为秒。取值范围是 1 到 255 秒。默认值是 3 秒。每个监测周期结束后，系统会重置探测到的新建会话相关数值。 重试次数：指定判断监测失败的警戒值。如果系统连续检测到参数指定次数的监测失败情况，就判断该条监测失败。取值范围是 1 到 255。默认值是 3。 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。 失败界定阈值：指定新建会话成功率的失败界定阈值。取值范围是 0 到 100。默认值为 30。在某个监测周期内，当系统检测到新建会话成功率小于指定的失败界定阈值时，判断为监测失败。 成功界定阈值：指定新建会话成功率的成功界定阈值。取值范围是 0 到 100。默认值为 50。在某个监测周期内，当系统检测到新建会话成功率大于指定的成功界定阈值时，判断为监测成功。 **说明**：在某个监测周期内，当系统检测到新建会话成功率大于等

选项	说明
	于失败界定阈值且小于等于成功界定阈值时，系统保持原来的监测状态。
HA 同步	点击该选项“启用”按钮开启 HA 同步，主设备和备用设备信息同步。
Ping 报文动态 ID	选中该选项复选框开启 Ping 报文动态 ID 功能。开启后，同一个监测对象发送的 ICMP 报文的 ID 为动态随机值。该功能默认为关闭状态，即通过 ICMP 报文对目标进行监测时，同一个监测对象发送的 ICMP 报文的 ID 为固定值。

3. 点击“确定”按钮，完成配置。新建监测对象显示在监测对象列表中。

监测对象列表

监测对象列表中显示系统中已配置的监测对象的信息，包括“状态”、“名称”、“警戒值”、“类型”和“关联项”。“关联项”列显示监测对象绑定的功能模块名称，可以为接口、HA、策略路由或者 vsys-track-status（非根 VSYS），点击功能模块名称，查看该模块的详细信息。解除绑定或未绑定监测对象，“关联项”列显示“没有关联项”。

注意:

一个监测对象只能被一个模块绑定。

进入非根 VSYS，非根 VSYS 绑定监测对象前需要先创建监测对象，绑定完在监测对象列表的“关联项”列显示“vsys-track-status”，不支持查看 vsys-track-status 的详细信息。

在非根 VSYS 中，监测对象可以被接口、策略路由绑定，不能被 HA 绑定，绑定完支持在监测对象列表中查看关联项详细信息。

关于接口、HA、策略路由以及非根 VSYS 如何绑定监测对象，请参阅：

接口：接口绑定监测对象

HA：HA Peer Active-Active（A/A）模式下绑定监测对象/HA Active-Passive（A/P）模式下绑定监测对象

策略路由：策略路由绑定监测对象

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。URL 过滤支持配置 IPv4 和 IPv6 地址的 URL 和关键字（keyword）。

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。

控制用户对某个网站的访问。比如，对用户访问某网站的行为进行日志记录。

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

配置 URL 过滤功能包含两部分:

1. 新建 URL 过滤规则
2. 绑定 URL 过滤规则到策略规则或安全域

新建 URL 过滤规则

1. 点击“对象 > URL 过滤>模板”，进入 URL 过滤页面。

2. 点击“新建”按钮，打开<URL 过滤配置>页面。

在<URL 过滤配置>页面中填写 URL 过滤规则的配置信息。

选项	说明
名称	输入规则名称。不同的 VSYS 中可以配置相同名称的 URL 过滤规则。
安全搜索	许多搜索引擎都包含“安全搜索”设置项，该设置用来过滤搜索结果中的成人内容，搜索引擎会根据该设置项的设置返回不同级别的搜索结果。 点击“启用”按钮，开启安全搜索功能，来检测搜索引擎“安全搜索”的设置以及相应的控制动作。 注意: 安全搜索功能目前仅支持以下搜索引擎：Google、Bing、Yahoo!、Yandex、Youtube。 由于搜索引擎使用 HTTPS 协议，因此安全搜索功能与 SSL 代理功能结合才可使用，需要为已开启安全搜索过滤功能的 URL 过滤 Profile 绑定到的策略规则启用 SSL 代理功能。 为了保证 Google 搜索引擎安全搜索功能的有效性，需要配置策略规则阻断 UDP 80 和 UDP 443 端口号。
安全搜索动作	指定安全搜索控制动作。

选项	说明
	阻断：指定动作为阻断，即当检测出搜索引擎“安全搜索”未设置时，阻止用户访问搜索页面并显示警告提示页面，提供 “安全搜索”设置链接提示用户前往设置。 执行：指定动作为执行，即当检测出搜索引擎“安全搜索”未设置时，系统强制将搜索引擎的“安全搜索”设置为最严格级别。
URL 单条配置	点击“新建”按钮，填写单条 URL 信息，勾选“阻断”或“记录日志”复选框，指定访问该 URL 时系统将执行的动作。
URL 类别	新建：点击该按钮，打开<URL 类别>配置页面。 编辑：点击该按钮，编辑相应的预定义或者自定义 URL 类别。 阻断：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。
SSL 检测	点击“启用”按钮，开启 SSL 协商报文检测功能。对于 HTTPS 流量，通过开启此功能，系统可以从 SSL 协商报文中获取用户要访问的站点的域名，从而进行 URL 过滤。如果同时配置了 SSL 代理功能，系统会优先使用 SSL 协商报文检测方式进行 URL 过滤。
URL 关键字类别	新建：点击该按钮新建关键字类别。系统支持预定义关键字类别和自定义关键字类别。 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。 关键字类别：显示系统中已有的关键字类别。 阻断：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。 列表外的所有关键字：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。

3. 点击“确定”完成配置。

> 注意: 同一个 URL 过滤规则的控制类型可以同时配置 URL 类别和 URL 关键字类别。

绑定 URL 过滤规则到安全域/策略规则

系统支持基于安全域和基于策略的 URL 过滤配置方式：

为安全域配置 URL 过滤规则后，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 URL 过滤规则配置进行过滤。

为策略规则配置 URL 过滤规则后，系统将会对与策略规则相匹配的流量根据 URL 过滤规则配置进行过滤。

若安全域和策略中均配置了 URL 过滤规则，策略中的配置项将有更高的优先权；在安全域配置中，目的安全域的优先权将高于源安全域。

基于安全域的配置方式，请按照以下步骤进行操作：

1. 创建安全域。
2. 在<安全域配置>对话框中，选择<威胁防护>标签页。
3. 勾选“URL 过滤”后的“启用”复选框；并可根据自身需要，点击“模板”下拉菜单选择已配置好的 URL 过滤规则或默认规则；也可点击“模板”下拉菜单中“新建配置”按钮，新建 URL 过滤规则。
4. 点击“确定”完成配置。

基于策略的 URL 过滤配置方式，请按照以下步骤进行操作：

1. 配置策略。
2. 在<策略配置>对话框中，选择<防护状态>标签页。
3. 勾选“URL 过滤”后的“启用”复选框；并可根据自身需要，点击“模板”下拉菜单选择已配置好的 URL 过滤规则；也可点击“模板”下拉菜单中“新建配置”按钮，新建 URL 过滤规则。
4. 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 查询和页面提示功能。

功能	介绍
预定义 URL 库	预定义的 URL 库，包含数十个类别，多达上千万条 URL，用于 URL 类别的指定。
自定义 URL 库	自定义的 URL 库。用于 URL 类别的指定。

功能	介绍
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	用户可以根据需要使用预定义关键字类别或者自定义关键字类别。用于 URL 关键字的指定。
页面提示	用户可以根据需要启用或禁用告警页面提示功能。 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

注意:

被绑定的 URL 过滤规则只有在解除绑定后，才可以进行删除。

为确保配置时引用最新 URL 类别，建议首先进行 URL 库更新。

用户可以指定将日志信息输出到特定目的地。

克隆 URL 过滤规则

系统支持将某一 URL 过滤规则快速克隆，用户只要将克隆的 URL 过滤规则的部分参数进行修改，即可生成一条新的 URL 过滤规则。

克隆 URL 过滤规则，请按照以下步骤进行操作：

1. 选择“对象 > URL 过滤”。
2. 选中列表中的一条 URL 过滤规则。
3. 点击列表上方的“克隆”按钮，按钮下方将出现“名称”配置框，输入新克隆的 URL 过滤规则名称。
4. 列表中将生成一条克隆的 URL 过滤规则。

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 访问部分。

在查看 URL 访问统计之前，用户需要在监控配置中开启 **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 日志部分。在查看上网日志记录之前，用户需要在日志配置中启用 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	预定义的 URL 库，包含数十个类别，多达上千万条 URL，用于 URL 类别的指定。
自定义 URL 库	自定义的 URL 库。用于 URL 类别的指定。
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	用户可以根据需要使用预定义关键字类别或者自定义关键字类别。用于 URL 关键字的指定。
页面提示	用户可以根据需要启用或禁用告警页面提示功能。 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提示页面。 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提示页面。

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。系统支持在线更新和本地更新两种方式供用户进行选择。

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>标签页，点击“确定并在线升级”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>标签页，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。

系统提供 3 个预定义的 URL 类别，分别是 custom1，custom2，custom3；用户可将自定义的 URL 列表导入其中。

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“对象 > URL 过滤>模板”，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”，打开<自定义 URL 库>页面。

3. 点击“新建”按钮，打开<URL 类别>页面。

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. 点击“新建”按钮，在文本框中输入 URL。

6. 如需要，按照以上步骤添加其它 URL。

7. 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(s)://”文本框中对 URL 进行编辑，然后点击文本框后的“添加”按钮。

8. 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。

9. 点击“确定”按钮，保存所做配置并返回上一级对话框/页面。

导入 URL 列表

用户可批量导入 URL 到预定义的自定义 URL 类别中。

导入用户自定义的 URL，按照以下步骤进行操作：

1. 点击“对象 > URL 过滤>模板”，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. 选中系统预定义的 URL 类别名称（custom1/custom2/custom3），然后再点击“导入”按钮。

4. 在弹出的<批量导入 URL>对话框中，点击“浏览”选择用户本地的 URL 文件。该文件大小应不超过 1M，且最多仅支持 1000 条 URL。文件中支持使用通配符，但仅支持一个通配符且必须在 URL 的起始位置。

5. 点击“确定”。

清除 URL 列表

在预定义 URL 类别中，清除用户自定义的 URL，按照以下步骤进行操作：

1. 点击“对象 > URL 过滤>模板”，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. 选中想要清除的 URL 类别名称（custom1/custom2/custom3），然后再点击“清除”按钮。

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“对象 > URL 过滤>模板”，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”，打开<URL 查询>页面。

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。

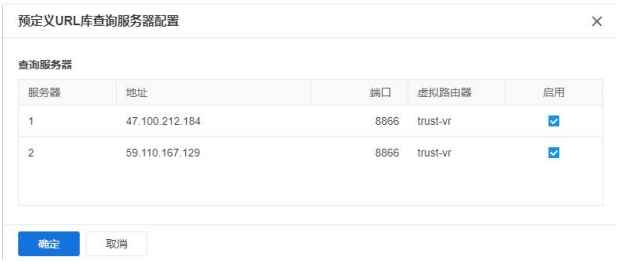
配置 URL 查询服务器

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。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“对象 > URL 过滤>模板”，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”，打开<预定义 URL 库>页面。

3. 在页面中，点击“查询服务器配置”按钮，打开<预定义 URL 库查询服务器配置>页面。



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. 双击指定服务器对应的“虚拟路由器”栏单元格，指定查询服务所使用的虚拟路由器。

7. 选择指定服务器的“启用”复选框，启用此服务器。

8. 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

关键字类别包括预定义关键字类别和自定义关键字类别，用于“URL 过滤/文件内容过滤/网页关键字/Web 外发信息/邮件过滤/应用行为控制”中关键字的指定。用户可以根据需要使用预定义关键字类别或者自定义关键字类别。系统默认提供四种预定义关键字类别，分别是 predef_bank_card（银行卡号关键字）、predef_email_address（邮箱账号关键字）、predef_cellphone_number（手机号关键字）和 predef_mainland_id_card（身份证号关键字），不可被编辑和删除。

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=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“对象 > URL 过滤>模板”，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”，打开<关键字类别>页面。
3. 在页面中关键字类别列表中展示预定义关键字类别和已创建的自定义关键字类别。
4. 点击“新建”按钮，打开<关键字类别配置>页面。

5. 在“类别名称”文本框中输入关键字类别名称。
6. 点击“新建”按钮，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）。
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“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

页面提示功能指通过告警页面提示用户被阻断警告信息或提示用户被监控警告信息，用户可以根据需要启用或禁用告警页面提示功能。

告警页面包括预定义告警页面和自定义告警页面。

预定义告警页面：显示系统预定义的警告信息内容，包括提示信息以及警告原因。

自定义告警页面：用户可以通过自定义警告信息和插入自定义图片，来自定义符合自己实际需求的告警页面。

启用/禁用用户被阻断警告提示

默认情况下，用户被阻断警告提示是开启的。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。用户被阻断警告页面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，并显示引起阻断的原因。主要包括以下两种情况：

当用户对某类 URL 的访问行为被 URL 过滤规则阻断时，用户的 Web 浏览器中会显示如下图所示的阻断提示信息。下图所示为预定义告警页面内容。

当用户对网址中含有关键字类别的网页的访问行为被 URL 过滤规则阻断时，用户的 Web 浏览器会显示如下图所示的阻断提示信息。下图所示为预定义告警页面内容。

启用/禁用用户被阻断警告提示，按照以下步骤进行操作：

1. 点击“对象 > URL 过滤>模板”，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”，打开<页面提示>页面。

3. 点击“用户被阻断警告”对应的“启用”按钮。如需禁用该功能，点击“禁用”按钮。
4. **指定用户被阻断警告信息内容。**

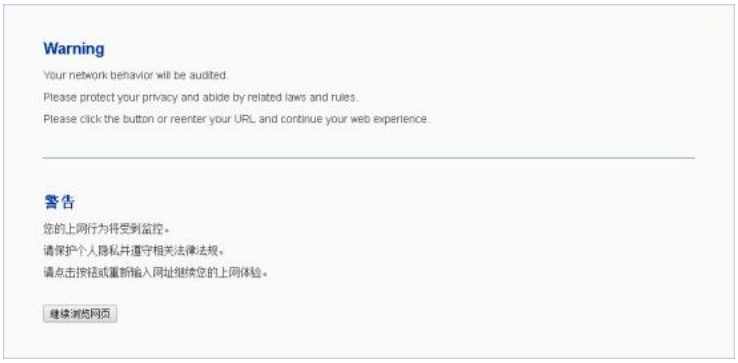
选项	说明
默认配置	选择“默认配置”后： 如果未配置自定义告警页面，将会使用预定义告警页面。

选项	说明
	如果已配置并启用自定义告警页面，将会使用自定义告警页面。
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。

5. 点击“确定”按钮保存所做配置并返回上一级对话框/页面。

启用/禁用用户被监控警告提示

默认情况下，用户被监控警告提示功能是关闭的。当用户启用该功能后，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，并且用户被监控警告提示功能是启用的，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。预定义告警页面内容如图所示：



启用/禁用用户被监控警告提示，按照以下步骤进行操作：

1. 点击“对象 > URL 过滤>模板”，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。如需禁用该功能，取消勾选“启用”复选框。

   如果未配置自定义告警页面，将会使用预定义告警页面；

   如果已配置并启用自定义告警页面，将会使用自定义告警页面。
4. 点击“确定”按钮保存所做配置并返回上一级对话框/页面。

未分类 URL 首次访问

对于用户首次访问的未分类 URL，即该 URL 并未包含在系统的预定义 URL 库或自定义 URL 库中，系统将会在云端继续查询该 URL 的类别，由于查询结果返回可能会出现时延，在查询结果返回之前，对于该未分类的 URL 系统不能及时执行类别相对应的处理动作。

为解决上述问题，针对首次访问的未分类 URL，用户可以指定其查询等待时间并启用等待超时阻断动作，超过查询等待时间后，系统将会对该未分类 URL 的访问进行阻断。

配置未分类 URL 首次访问相关内容，请按照以下步骤进行操作：

1. 点击“对象 > URL 过滤 > 模板”，进入模板页面。
2. 在页面右上角，点击“相关配置”，并在下拉菜单中选择“未分类 URL 首次访问”，打开<未分类 URL 首次访问>页面。

3. 在“查询等待时间”文本框输入查询等待时长，范围是 0 到 5000 毫秒，默认值为 0，表示没有等待时间的限制。
4. 勾选“等待超时阻断”后的“启用”复选框，启用阻断动作，在超过查询等待时间后，对未分类 URL 的首次访问进行阻断。取消勾选“启用”复选框后，在超过查询等待时间后，将会继续按照 URL 过滤规则配置进行 URL 过滤。
5. 点击“确定”按钮保存所做配置。

配置 URL 黑白名单

用户可以通过配置 URL 黑白名单来进一步控制对某些指定网站的访问。

在配置 URL 黑名单后，当用户向黑名单中指定的 URL 发出访问请求时，系统将对该请求进行阻断。

在配置 URL 白名单后，当用户向白名单中指定的 URL 发出访问请求时，系统将不对该访问请求通过 URL 过滤规则过滤，并且对该访问请求放行处理。

若 URL 黑名单、URL 白名单、URL 过滤规则中均配置了 URL 类别，系统对 URL 类别过滤的匹配优先级为：URL 黑名单>URL 白名单>URL 过滤规则。

配置 URL 黑名单

配置 URL 黑名单，按照以下步骤进行操作：

1. 点击“对象 > URL 过滤 > 黑白名单分类”。
2. 选择<URL 黑名单>标签页，打开 URL 黑名单页面，该页面展示已加入 URL 黑名单中的所有 URL 类别。

3. 点击“+”按钮，在<URL 类别>列表中， 选择需要添加到 URL 黑名单的 URL 类别。

4. “URL 类别”列表包含可以引用的所有 URL 类别（预定义 URL 库和自定义 URL 库），用户还可以点击 ⊕ 按钮，新建 URL 类别，具体步骤请参阅配置自定义 URL 库。

5. 如果需要删除 URL 黑名单中的 URL 类别条目，在“URL 黑名单”列表中，点击该条目后的 × 按钮。

6. 点击“确定”按钮，完成 URL 黑名单的配置。

配置 URL 白名单

配置 URL 白名单，按照以下步骤进行操作：

1. 点击“对象 > URL 过滤 > 黑白名单分类”。

2. 选择<URL 白名单>标签页，打开 URL 白名单页面，该页面展示已加入 URL 白名单中的所有 URL 类别。

3. 点击“+”按钮，在<URL 类别>列表中， 选择需要添加到 URL 白名单的 URL 类别。

4. “URL 类别”列表中包含可以引用的所有 URL 类别（预定义 URL 库和自定义 URL 库），用户还可以点击 ⊕ 按钮，新建 URL 类别，具体步骤请参阅配置自定义 URL 库。

5. 如果需要删除 URL 白名单中的 URL 类别条目，在“URL 白名单”列表中，点击该条目后的 × 按钮。

6. 点击“确定”按钮，完成 URL 白名单的配置。

数据安全

系统提供数据安全功能，可以根据需要针对不同用户、不同上网行为、不同时间进行灵活的控制，对用户的上网行为进行全面的行为控制和行为审计（记录行为日志）。通过对用户的网络访问行为、敏感数据进行控制和审计，有效解决因接入互联网而可能引发的各种问题，防止数据信息泄露，优化对互联网资源的应用。

数据安全功能主要包括以下几个方面：

功能	说明
文件过滤	对使用 HTTP(S)、FTP、SMTP(S)、IMAP(S)、POP3(S)以及 SMB 协议传输的文件进行检测，对符合过滤条件的文件进行控制。
内容过滤	文件内容过滤：对指定协议类型、文件类型的文件内容中携带的敏感关键字进行检测，并且可以对其进行日志记录或者阻断。

功能	说明
	网页关键字：对用户访问含有某关键字的网页进行行为控制和行为审计。 Web 外发信息：对用户在某网站发布含有某关键字信息进行行为控制和行为审计。 邮件过滤：对用户使用 SMTP(S)协议、POP3(S)协议、IMAP(S)协议外发邮件进行控制。 应用行为控制：对 FTP、HTTP(S)、TELNET 应用程序行为进行控制和审计。
上网行为审计	对 IM 应用程序行为进行审计，并能对上网行为进行日志记录

对象配置

对象是指用户在配置内容过滤规则时，需要引用的一些配置项。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“网页关键字/Web 外发信息”中 URL 类别及控制范围的指定。
自定义 URL 库	自定义的 URL 库。用于“网页关键字/Web 外发信息”中 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	用户可以根据需要使用预定义关键字类别或者自定义关键字类别。用于“文件内容过滤/网页关键字/Web 外发信息/邮件过滤/应用行为控制”中关键字的指定。关于关键字类别的详细信息，请参阅数据安全中的关键字类别。
页面提示	用户可以根据需要启用或禁用告警页面提示功能。 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提示页面。 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提示页面。
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。

预定义 URL 库

系统内置预定义 URL 库。

预定义 URL 库能够为网页关键字过滤功能和 Web 外发信息控制功能提供 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。系统支持在线更新和本地更新两种方式供用户进行选择。

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>标签页，点击“确定并在线升级”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>标签页，选择“本地升级”，点击“浏览”按钮，选中本地 URL 库特征文件并选择“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 库能够为网页关键字过滤功能和 Web 外发信息控制功能提供 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。

系统提供 3 个预定义的 URL 类别，分别是 custom1，custom2，custom3；用户可将自定义的 URL 列表导入其中。

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“对象 > 数据安全> 内容过滤”。
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”，打开<自定义 URL 库>页面。
3. 点击“新建”按钮，打开<URL 类别>页面。

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。

导入 URL 列表

用户可批量导入 URL 到预定义的 URL 类别中。

导入用户自定义的 URL，按照以下步骤进行操作：

1. 点击“对象 > URL 过滤>模板”，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”，打开<自定义 URL 库>页面。
3. 选中系统预定义的 URL 类别名称（custom1/custom2/custom3），然后再点击“导入”按钮。
4. 在打开的<批量导入 URL>页面中，点击“浏览”选择用户本地的 URL 文件。该文件大小应不超过 1M，且最多仅支持 1000 条 URL。文件中支持使用通配符，但仅支持一个通配符且必须在 URL 的起始位置。
5. 点击“关闭”。

清除 URL 列表

在预定义 URL 类别中，清除用户自定义的 URL，按照以下步骤进行操作：

1. 点击“对象 > URL 过滤>模板”，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”，打开<自定义 URL 库>页面。
3. 选中想要清除的 URL 类别名称（custom1/custom2/custom3），然后再点击“清除”按钮。

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“对象 > 数据安全> 内容过滤”。
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”，打开<URL 查询>页面。

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。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“对象 > 数据安全> 内容过滤”。

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”，打开<预定义 URL 库>页面。

3. 在页面中，点击“查询服务器配置”按钮，打开<预定义 URL 库查询服务器配置>页面。

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. 双击指定服务器对应的“虚拟路由器”栏单元格，指定查询服务所使用的虚拟路由器。

7. 选择指定服务器的“启用”复选框，启用此服务器。

8. 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

关键字类别包括预定义关键字类别和自定义关键字类别，用于“URL 过滤/文件内容过滤/网页关键字/Web 外发信息/邮件过滤/应用行为控制”中关键字的指定。用户可以根据需要使用预定义关键字类别或者自定义关键字类别。系统默认提供四种预定义关键字类别，分别是 predef_bank_card（银行卡号关键字）、predef_email_address（邮箱账号关键字）、predef_cellphone_number（手机号关键字）和 predef_mainland_id_card（身份证号关键字），不可被编辑和删除。

配置关键字相关的上网行为控制规则后，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：某网页关键字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。

假设扫描某网页，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。

假设扫描某网页，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=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。

建议通过关键字组合的方式实现关键字相关的上网行为控制功能。例如，配置网页关键字功能阻止用户访问网游相关网站，如果只指定过滤关键字“网游”，则可能阻止很多无关网站；但如果指定过滤关键字“网游”、“经验值”、“装备”和“外挂”，并恰当设置每个关键字的信任值，这样就能大大提高控制的准确性。更为高级的使用方式是将网游相关的术语都收集起来，按照可能性给每个关键字分配信任值，这样可以较为全面和准确的达到控制目的。

配置关键字类别

配置关键字类别，按照以下步骤进行操作：

1. 点击“对象 > 数据安全> 内容过滤”。
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”，打开<关键字类别>页面。
3. 在页面中关键字类别列表中展示预定义关键字类别和已创建的自定义关键字类别。
4. 点击“新建”按钮，打开<关键字类别配置>页面创建自定义关键字类别。

5. 在“类别名称”文本框中输入关键字类别名称。
6. 点击“新建”按钮，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）。
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“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

页面提示功能指通过告警页面提示用户被阻断警告信息或提示用户被监控警告信息，用户可以根据需要启用或禁用告警页面提示功能。

告警页面包括预定义告警页面和自定义告警页面。

预定义告警页面：显示系统预定义的警告信息内容，包括提示信息以及警告原因。

自定义告警页面：用户可以通过自定义警告信息和插入自定义图片，来自定义符合自己实际需求的告警页面。

启用/禁用用户被阻断警告提示

默认情况下，用户被阻断警告提示是开启的。当用户的上网行为被上网行为控制功能（网页关键字过滤、Web 外发信息控制、邮件过滤和应用行为控制）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。下图所示为默认预定义告警页面：

启用用户被阻断警告提示功能后，当用户的下列上网行为被上网行为控制规则阻断时，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

对内容中含有某关键字类别的网页的访问行为

对在某网站发布信息或者发布含有特定关键字信息的行为

对 HTTP 的 Connect、Get、Put、Head、Options、Post、Trace 行为

启用/禁用用户被阻断警告提示，按照以下步骤进行操作：

1. 点击“对象 > 数据安全> 内容过滤”。

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”，打开<页面提示>页面。

3. 选中“用户被阻断警告”对应的“启用”复选框。如需禁用该功能，取消勾选“启用”复选框。

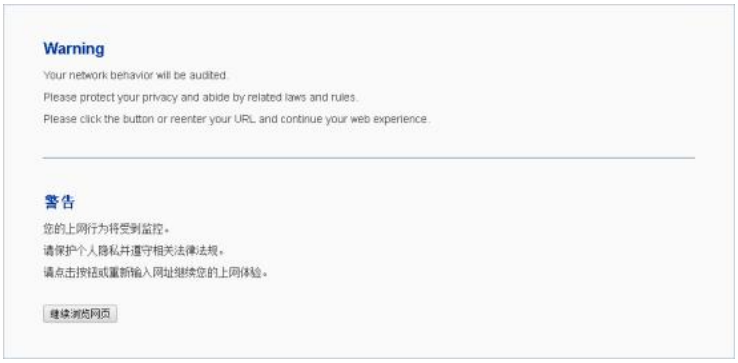
   如果未配置自定义告警页面，将会使用预定义告警页面；

   如果已配置并启用自定义告警页面，将会使用自定义告警页面。

4. 点击“确定”按钮保存所做配置并返回上一级对话框/页面。

启用/禁用用户被监控警告提示

默认情况下，用户被监控警告提示功能是关闭的。当用户启用该功能后，如果用户的上网行为与系统中已配置的上网行为控制功能（网页关键字过滤、Web 外发信息控制、邮件过滤和应用行为控制）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，如果创建网页关键字规则对用户浏览某网页的行为进行监控，并且用户被监控警告提示功能是启用的，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。预定义告警页面内容如图所示：



启用/禁用用户被监控警告提示，按照以下步骤进行操作：

1. 点击“对象 > 数据安全> 内容过滤”。
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”，打开<页面提示>页面。
3. 选中“用户被阻断警告”对应的“启用”复选框。如需禁用该功能，取消勾选“启用”复选框。

   如果未配置自定义告警页面，将会使用预定义告警页面；

   如果已配置并启用自定义告警页面，将会使用自定义告警页面。

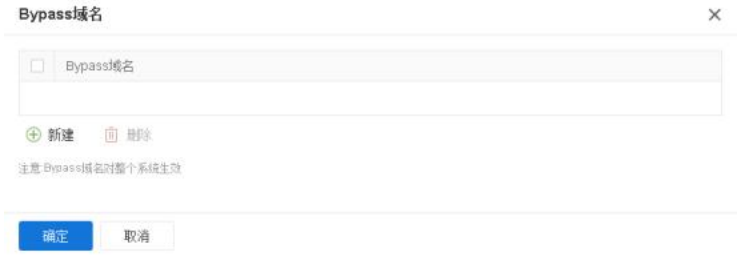
4. 点击“确定”按钮保存所做配置并返回上一级对话框/页面。

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，不受上网行为控制功能（网页关键字过滤、Web 外发信息控制、邮件过滤和应用行为控制）的控制。

配置 Bypass 域名，按照以下步骤进行操作：

1. 点击“对象 > 数据安全> 内容过滤”。
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”，打开<Bypass 域名>页面。



3. 在文本框中输入所需域名。
4. 点击“新建”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

免监控用户将不受上网行为控制功能（网页关键字过滤、Web 外发信息控制、邮件过滤、网络聊天控制和应用行为控制）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“对象 > 数据安全> 内容过滤”。
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”，打开<免监控用户>页面。

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。

文件过滤

文件过滤功能是对通过 HTTP(S）、FTP、SMTP(S)、IMAP(S)、POP3(S)以及 SMB 协议传输的文件进行检测，对符合过滤条件的文件进行控制。

支持通过 HTTP(S) GET/POST 方法、FTP、SMTP(S)、IMAP(S)、POP3(S)、SMB 传输的文件进行检测和控制。对于 SMB 协议，系统还支持断点续传场景下的文件检测和控制。

支持对文件类型设置过滤条件。

可对符合过滤条件的文件进行阻断传输、记录日志、允许访问等控制动作。

文件过滤功能需要通过策略规则与文件过滤规则相结合的方式实现。将文件过滤规则绑定到策略规则后，系统将会对与策略规则相匹配的网络流量根据文件过滤规则配置进行处理。系统还支持绑定文件过滤规则到 ZTNA 策略，对与 ZTNA 策略相匹配的流量进行文件检测和处理。

配置文件过滤规则

文件过滤规则用来指定需要进行检测的协议、过滤条件、以及控制动作。

文件必须符合任意一个过滤规则中所有过滤条件，系统才会执行响应的控制动作。

新建文件过滤规则，按照以下步骤进行操作：

1. 点击“对象 > 数据安全 > 文件过滤”，进入文件过滤页面。
2. 点击“新建”按钮，打开<文件过滤配置>页面。

在对话框中填写文件过滤规则的配置信息。

选项	说明
名称	输入文件过滤规则的名称。
描述	输入文件过滤规则的描述信息。范围是 1 到 255 个字符。
过滤规则	

选项	说明
ID	文件过滤规则条目的编号。每个文件过滤规则中最多可包含 8 个条目。点击“+”按钮，添加文件过滤规则条目。 如果任意一个过滤条目的控制动作为阻断且文件符合此过滤规则条目，则系统直接阻断当前上传或下载。
最小文件大小	当传输的文件大小达到指定的值时，触发控制动作。取值范围为 1 到 512000，单位 KB。
文件类型	指定文件类型。鼠标左键点击此列的单元格，从下拉菜单中进行选择，可以指定一个或多个文件类型。对系统无法识别的文件进行控制，可指定 UNKNOWN 文件类型。 当系统检测到传输的文件类型是指定的类型时，将触发控制动作。 文件过滤功能支持对如下文件类型进行识别： 7Z, AI, APK, ASF, AVI, BAT, BMP, CAB, CATPART, CDR, CIN, CLASS, CMD, CPL, DLL, DOC, DOCX, DPX, DSN, DWF, DWG, DXF, EDIT, EMF, EPS, EPUB, EXE, EXR, FLA, FLV, GDS, GIF, GZ, HLP, HTA, HTML, IFF, ISO, JAR, JPG, KEY, LNK, LZH, MA, MB, MDB, MDI, MIF, MKV, MOV, MP3, MP4, MPEG, MPKG, MSI, NUMBERS, OCX, PAGES, PBM, PCL, PDF, PGP, PIF, PL, PNG, PPT, PPTX, PSD, RAR, REG, RLA, RMVB, RPF, RTF, SGI, SH, SHK, STP, SVG, SWF, TAR, TDB, TIF, TORRENT, TXT, VBE, WAV, WEBM, WMA, WMF, WMV, WRI, WSF, XLS, XLSX, XML, XPM, ZIP, BZ2, UNKNOWN
协议	指定检测的协议。http-get 表示对 HTTP 协议的 GET 请求进行检测；http-post 表示对 HTTP 协议的 POST 请求进行检测；ftp 表示对 FTP 协议进行检测；smtp 表示对 SMTP 协议进行检测；imap 表示对 IMAP 协议进行检测；pop3 表示对 POP3 协议进行检测。可以指定一个或多个协议类型。该选项为必填项。
动作	对符合文件过滤规则的文件进行处理。可以选择阻断或者记录日志。该选项为必填项。

3. 点击“确定”按钮完成配置。

配置解压控制功能

配置解压控制功能后，系统会对传输的压缩文件进行解压，并能对超出最大压缩层数的文件以及加密压缩文件按照指定的动作进行处理。支持解压缩的文件格式包括 RAR、ZIP、TAR、GZIP 及 BZIP2。

配置解压控制功能，请按照以下步骤进行操作：

1. 点击“对象 > 数据安全 > 文件过滤”，进入文件过滤功能页面。

2. 在页面右上角，点击“解压控制”，打开<解压控制>页面。

在<解压控制>页面进行配置。

选项	说明
解压缩	点击“启用/禁用”按钮，开启/关闭解压缩功能。
最大压缩层	默认情况下，系统可以对最多 5 层压缩嵌套的文件进行检测（含 5 层），用户可以通过该选项对可检测压缩层数进行配置。从下拉菜单中选择需要的层数。范围是 1-5 层。
超出行为	指定对超出最大压缩层限制的压缩文件的处理动作。用户可以根据需要进行选择，可以是： 只记录日志 - 只生成相关日志信息。该行为是系统默认行为。 重置连接 - 重置压缩文件连接。
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处理。根据文件过滤规则配置，系统可能会继续对加密压缩文件进行过滤检测和控制。 只记录日志 - 只生成相关日志信息，不对加密压缩文件进行过滤检测和控制。 重置连接 - 重置加密压缩文件连接。

3. 配置完成，点击“确定”按钮。

注意：对于包含 docx、pptx，xlsx、jar、apk 格式的压缩文件，当“超出行为”被指定为重置连接时，用户需要将最大压缩层数增加 1 层，以避免无法下载该压缩文件的问题。

查看文件过滤日志

查看文件过滤日志，参阅监控模块中的**文件过滤日志**部分。

内容过滤

内容过滤功能主要包括以下几个方面：

文件内容过滤：对指定传输协议类型、文件类型的文件内容中携带的敏感关键字进行检测以及行为控制。

网页关键字：对用户访问含有某关键字的网页进行行为控制和行为审计：比如，禁止访问含“赌博”词汇的网页，并记录访问行为日志。

Web 外发信息：对用户在某网站发布信息或者发布含有某关键字信息进行行为控制和行为审计：比如，禁止在社区论坛上发布含“色情”词汇的信息，并记录发布行为日志。

邮件过滤：对用户使用 SMTP(S)/POP3(S)/IMAP(S)协议及 Webmail 外发邮件进行控制：

对所有邮件外发行为进行行为控制和行为审计。

对发送包含特定收件人、发件人、关键字内容的行为进行行为控制和行为审计。

应用行为控制：对 FTP、HTTP(S)和 TELNET 应用程序行为进行控制和审计：

对 FTP 的 Login、Get、Put 行为进行行为控制和行为审计。

对 HTTP(S)的 Connect、Get、Put、Head、Options、Post、Trace、Delete 行为进行行为控制和行为审计。

对 TELNET 客户端向服务器发起的请求内容进行行为控制和行为审计。

文件内容过滤

文件内容过滤功能可以对指定协议类型、文件类型的文件内容中携带的敏感关键字进行检测，并且可以对其进行日志记录或者阻断。比如，通过 HTTP(S)协议下载的 doc 类型的文件内容进行检测，对于包含手机号关键字内容的文件，进行记录日志信息。

网络管理员可以针对不同协议传输的不同类型文件制定适合的文件内容过滤规则，系统将会对与规则相匹配的网络流量根据配置进行处理。

配置文件内容过滤

配置文件内容过滤功能包含两部分:

1. 配置文件内容过滤规则。
2. 绑定文件内容过滤规则到策略规则或安全域。系统还支持绑定文件内容过滤规则到 ZTNA 策略，对与 ZTNA 策略相匹配的流量进行文件内容检测和处理。

配置文件内容过滤规则

1. 点击“对象 > 数据安全>内容过滤”，选择“文件内容过滤”标签页。

2. 点击“新建”按钮，打开<文件内容过滤配置>页面。

在页面中填写文件内容过滤规则的配置信息。

选项	说明
名称	输入规则名称。
文件类型	指定文件类型。点击  按钮，在打开的<文件类型>页面选择文件类型，可以指定一个或多个文件类型。 目前支持的文件类型有：txt，doc，docx，ppt，pptx，xls，xlsx。
协议类型	指定检测的文件传输协议和方向。点击指 定协议类型后的“启用”按钮，并且在下拉菜单中选择检测的方向。HTTP(S)、FTP、SMB 协议支持选择的方向为下载、上传、双向；SMTP(S)协议仅支持选择上传；POP3(S)、IMAP(S)协议仅支持下载。
指定的关键字	指定过滤的关键字类别并指定动作。 1. 在该部分列表中展示所有预定义关键字类别和自定义关键字类别。 2. 在“动作”下拉菜单选择控制动作，包括无、只记录日志以及阻断（阻断并记录日志）。 3. 点击“新建”按钮，弹出<关键字类别配置>页面，在该页面配置需要进行控制的关键字。

3. 点击“确定”按钮，保存所做配置并返回上一级对话框/页面。

绑定文件内容过滤规则到安全域/策略规则

系统支持基于安全域和基于策略的文件内容过滤配置方式：

为安全域配置文件内容过滤规则后，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文件内容过滤规则配置进行过滤。

为策略规则配置文件内容过滤规则后，系统将会对与策略规则相匹配的流量根据文件内容过滤规则配置进行过滤。

若安全域和策略中均配置了文件内容过滤规则，策略中的配置项将有更高的优先权；在安全域配置中，目的安全域的优先权将高于源安全域。

基于安全域的配置方式，请按照以下步骤进行操作：

1. 创建安全域。
2. 在<安全域配置>对话框中，点击“数据安全”展开配置项。
3. 点击“文件内容过滤”后的“启用”按钮；并可根据自身需要，点击“模板”下拉菜单选择已配置好的文件内容过滤规则或默认规则；也可点击“模板”下拉菜单中 ⊕ 按钮，新建文件内容过滤规则。关于配置文件内容过滤规则，请参阅配置文件内容过滤。
4. 点击“确定”完成配置。

基于策略的文件内容过滤配置方式，请按照以下步骤进行操作：

1. 配置策略。
2. 在<策略配置>对话框中，点击“数据安全”展开配置项。
3. 点击“文件内容过滤”后的“启用”按钮；并可根据自身需要，点击“模板”下拉菜单选择已配置好的文件内容过滤规则或默认规则；也可点击“模板”下拉菜单中 ⊕ 按钮，新建文件内容过滤规则。
4. 点击“确定”完成配置。

查看文件内容关键字阻断统计

配置文件内容过滤功能后，用户可查看文件内容关键字阻断统计结果。

点击“监控 > 关键字阻断 > 文件内容”，进入文件内容关键字阻断结果的统计页面，该页面显示文件内容关键字阻断的统计信息。

查看文件内容关键字日志

查看文件内容关键字日志，参阅监控模块中的内容过滤日志部分。

网页关键字

网页关键字功能可以对用户访问含有特定关键字内容的网站的行为进行控制，并能对访问行为进行日志记录。比如，阻止用户访问含“赌博”词汇的网站，并记录访问行为日志。网络管理员可以针对不同上网行为制定适合的网页关键字规则，系统将会对与规则相匹配的网络流量根据配置进行处理。

配置网页关键字

配置网页关键字功能包含两部分:

1. 配置网页关键字规则。
2. 绑定网页关键字规则到策略规则或安全域。

配置网页关键字规则

1. 点击“对象 > 数据安全>内容过滤 ”，选择“网页关键字”页签。
2. 点击“新建”按钮，打开<网页关键字规则配置>页面。

在对话框中填写网页关键字规则的配置信息。

选项	说明
名称	输入规则名称。
指定的关键字	指定关键字控制范围。默认情况下，系统会对所有网站进行关键字控制。 1. 在该标签页中选中需要进行关键字控制的网站类别对应的复选框。

选项	说明
	2. 点击“确定”按钮，保存所做配置并返回上一级对话框/页面。
控制范围	控制对网页内容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。 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。 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，指定阻止访问网页中含有相应关键字的网站。 记录日志：选中复选框，指定对访问网页中含有相应关键字的网站的行为进行日志记录。

3. 点击“确定”按钮完成配置。

绑定网页关键字规则到安全域/策略规则

系统支持基于安全域和基于策略的网页关键字配置方式：

为安全域配置网页关键字规则后，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网页关键字规则配置进行过滤。

为策略规则配置网页关键字规则后，系统将会对与策略规则相匹配的流量根据网页关键字规则配置进行过滤。

若安全域和策略中均配置了网页关键字规则，策略中的配置项将有更高的优先权；在安全域配置中，目的安全域的优先权将高于源安全域。

基于安全域的配置方式，请按照以下步骤进行操作：

1. 创建安全域。
2. 在<安全域配置>页面中，点击“数据安全”展开配置项。
3. 点击“网页关键字”后的“启用”按钮；并可根据自身需要，点击“模板”下拉菜单选择已配置好的网页关键字规则或默认规则；也可点击“模板”下拉菜单中 ⊕ 按钮，新建网页关键字规则。
4. 点击“确定”完成配置。

基于策略的网页关键字配置方式，请按照以下步骤进行操作：

1. 配置策略。
2. 在<策略配置>页面中，点击“数据安全”展开配置项。

3. 点击“网页关键字”后的“启用”按钮；并可根据自身需要，点击“模板”下拉菜单选择已配置好的网页关键字规则；也可点击“模板”下拉菜单中 ⊕ 按钮，新建网页关键字规则。

4. 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、自定义 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。
自定义 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。

查看网页内容关键字阻断统计

配置网页关键字功能后，用户可查看网页内容关键字阻断统计结果。

点击“监控 > 关键字阻断 > 网页关键字”，进入网页内容关键字阻断结果的统计页面，该页面显示网页内容关键字阻断的统计信息。

查看网页内容关键字日志

查看网页关键字日志，参阅监控模块中的内容过滤日志部分。

Web 外发信息

Web 外发信息功能可以对用户在某网站发布信息或者发布含有特定关键字信息的行为进行控制，并能对发布行为进行日志记录。例如，阻止用户在社区论坛类网站发布含有关键字“舆论”的信息，并记录发布行为日志。网络管理员可以针对不同信息发布行为制定适合的 Web 外发信息规则，系统将会对与规则相匹配的网络流量根据配置进行处理。

配置 Web 外发信息

配置 Web 外发信息功能包含两部分:

1. 配置 Web 外发信息规则。
2. 绑定 Web 外发信息规则到策略规则或安全域。

新建 Web 外发信息规则

1. 点击“对象 > 数据安全>内容过滤 ”，选择“Web 外发信息”页签。
2. 点击“新建”按钮，打开<Web 外发信息规则配置>页面。

在页面中填写 Web 外发信息规则的配置信息。

选项	说明
名称	输入规则名称。
所有 Web 外发信息	阻止外发：选中复选框，指定阻止所有信息发布行为。 记录日志：选中复选框，指定对所有信息发布行为进行日志记录。
指定的关键字	对含有特定关键字的 Web 外发信息进行控制。具体配置选项包括： 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，参阅对象配置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。 阻止外发：选中复选框，指定阻止发布含有特定关键字的信息。 记录日志：选中复选框，指定对发布含有特定关键字信息的行为进行日志记录。
控制范围	指定控制范围。默认情况下，系统会对所有网站进行 Web 外发信息控制。 1. 在该标签页中选中需要进行 Web 外发信息控制的网站类别对应的复选框。 2. 点击“确定”按钮，保存所做配置并返回上一级对话框。

3. 点击“确定”完成配置。

绑定 Web 外发信息规则到安全域/策略规则

系统支持基于安全域和基于策略的 Web 外发信息配置方式：

为安全域配置 Web 外发信息规则后，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 Web 外发信息规则配置进行过滤。

为策略规则配置 Web 外发信息规则后，系统将会对与策略规则相匹配的流量根据 Web 外发信息规则配置进行过滤。

若安全域和策略中均配置了 Web 外发信息规则，策略中的配置项将有更高的优先权；在安全域配置中，目的安全域的优先权将高于源安全域。

基于安全域的配置方式，请按照以下步骤进行操作：

1. 创建安全域。
2. 在<安全域配置>页面中，点击“数据安全”展开配置项。
3. 点击“Web 外发信息”后的“启用”按钮；并可根据自身需要，点击“模板”下拉菜单选择已配置好的 Web 外发信息规则或默认规则；也可点击“模板”下拉菜单中 ⊕ 按钮，新建 Web 外发信息规则。
4. 点击“确定”完成配置。

基于策略的 Web 外发信息配置方式，请按照以下步骤进行操作：

1. 配置策略。
2. 在<策略配置>页面中，点击“数据安全”展开配置项。

3. 点击“Web 外发信息”后的“启用”按钮；并可根据自身需要，点击“模板”下拉菜单选择已配置好的 Web 外发信息规则；也可点击“模板”下拉菜单中 ⊕ 按钮，新建 Web 外发信息规则。

4. 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、自定义 URL 库、URL 查询、SSL 代理、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 Web 外发信息规则的控制范围。
自定义 URL 库	通过维护相应的 URL 库，指定 Web 外发信息规则的控制范围。
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。

查看 Web 外发信息关键字阻断统计

配置 Web 外发信息关键字功能后，用户可查看 Web 外发信息关键字阻断统计结果。

点击“监控 > 关键字阻断 > Web 外发信息”，进入 Web 外发关键字阻断结果的统计页面，该页面显示 Web 外发信息关键字阻断的统计信息。

查看 Web 外发信息关键字日志

查看 Web 外发信息关键字日志，参阅监控模块中的内容过滤日志部分。

邮件过滤

邮件过滤功能主要用于当用户通过 SMTP(S)、POP(S)、IMAP(S)发送邮件时，根据邮件的发件人、收件人和内容对邮件的发送行为进行控制，并能记录发送行为日志。网络管理员可以针对不同邮件发送行为制定适合的邮件过滤规则，系统将会对与规则相匹配的网络流量根据配置进行处理。

配置邮件过滤

配置邮件过滤功能包含两部分:

1. 配置邮件过滤规则。

2. 绑定邮件过滤规则到策略规则或安全域。

配置邮件过滤规则

1. 点击“对象 > 数据安全>内容过滤”，选择“邮件过滤”页签。
2. 点击“新建”按钮，打开<邮件过滤规则配置>页面。

在页面中填写邮件过滤规则的配置信息。

选项	说明
名称	输入规则名称。
控制类型	指定控制类型。 所有邮件 - 对所有外发邮件进行控制。用户需要在“控制动作”部分选择“记录日志”按钮对所有外发邮件行为进行日志记录。 指定邮件 - 对指定条件下的外发邮件进行控制。用户需要在“控制动作”部分指定相应的动作。
指定邮件	
阻断/审计发件人	选中复选框，指定对外发邮件的发件人进行控制。配置方法如下： 1. 点击“发件人”链接，弹出<发件人>对话框。 2. 在“发件人”文本框输入需要控制的发件人邮箱帐号。 3. 点击“添加”按钮，将发件人邮箱帐号添加进下方的发件人列表中。 4. 在发件人列表中选中需要进行控制的邮箱帐号对应的控制动作复选框，包括“阻止发送”和“记录日志”。如需要删除发件人，单击选中发件人邮箱帐号，点击“删除”按钮将发件人从列表中删除。

选项	说明
	5. 点击“确定”按钮，保存所做配置并返回上一级对话框/页面。
阻断/审计收件人	选中复选框，指定对外发邮件的收件人进行控制。配置方法如下： 1. 点击“收件人”链接，弹出<收件人>对话框。 2. 在“收件人”文本框输入需要控制的收件人邮箱帐号。 3. 点击“添加”按钮，将收件人邮箱帐号添加进下方的收件人列表中。 4. 在收件人列表中选中需要进行控制的邮箱帐号对应的控制动作复选框，包括“阻止发送”和“记录日志”。如需要删除收件人，单击选中收件人邮箱帐号，点击“删除”按钮将收件人从列表中删除。 5. 点击“确定”按钮，保存所做配置并返回上一级对话框/页面。
阻断/审计邮件内容	选中复选框，指定对外发邮件的内容关键字进行控制。配置方法如下： 1. 点击“邮件内容”链接，弹出<邮件内容>对话框。 2. 点击“新建”按钮，弹出<关键字类别>对话框，在该对话框配置需要进行控制的邮件内容关键字。 3. 在关键字类别列表中选中需要进行控制的关键字对应的控制动作复选框，包括“阻止发送”和“记录日志”。 4. 点击“确定”按钮，保存所做配置并返回上一级对话框/页面。
上述配置外邮件	对上述配置不包含的邮件，指定控制动作，包括“阻止发送”和“记录日志”。

3. 如需要，可以配置例外邮箱帐号，指定不受邮件过滤规则控制的邮箱帐号。
4. 点击“新建”按钮，在“例外”文本框中输入不受邮件过滤规则控制的邮箱帐号，可以为发件人帐号或者收件人帐号。
5. 在例外帐号列表中选中需要进行编辑/删除的帐号，点击“编辑”/“删除”按钮，编辑/删除相应的帐号。
6. 点击“确定”按钮，保存所做配置并返回上一级对话框/页面。

绑定邮件过滤规则到安全域/策略规则

系统支持基于安全域和基于策略的邮件过滤配置方式：

为安全域配置邮件过滤规则后，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邮件过滤规则配置进行过滤。

为策略规则配置邮件过滤规则后，系统将会对与策略规则相匹配的流量根据邮件过滤规则配置进行过滤。

若安全域和策略中均配置了邮件过滤规则，策略中的配置项将有更高的优先权；在安全域配置中，目的安全域的优先权将高于源安全域。

基于安全域的配置方式，请按照以下步骤进行操作：

1. 创建安全域。
2. 在<安全域配置>页面中，点击“数据安全”展开配置项。
3. 点击“邮件过滤”后的“启用”按钮；并可根据自身需要，点击“模板”下拉菜单选择已配置好的邮件过滤规则或默认规则；也可点击“模板”下拉菜单中 ⊕ 按钮，新建邮件过滤规则。
4. 点击“确定”完成配置。

基于策略的邮件过滤配置方式，请按照以下步骤进行操作：

1. 配置策略。
2. 在<策略配置>页面中，点击“数据安全”展开配置项。
3. 点击“邮件过滤”后的“启用”启用；并可根据自身需要，点击“模板”下拉菜单选择已配置好的邮件过滤规则；也可点击“模板”下拉菜单中 ⊕ 按钮，新建邮件过滤规则。
4. 点击“确定”完成配置。

查看邮件内容关键字阻断统计

配置邮件过滤功能后，用户可查看邮件内容关键字阻断统计结果。

点击“监控 > 关键字阻断 > 邮件内容”，进入邮件内容关键字阻断结果的统计页面，该页面显示邮件内容关键字阻断的统计信息。

查看邮件过滤关键字日志

查看邮件内容关键字日志，参阅监控模块中的内容过滤日志部分。

应用行为控制

应用行为控制功能可以对 FTP、HTTP(S)和 TELNET 应用程序行为进行控制和审计（记录日志），包括：

对 FTP 协议传输的内容，以及 FTP 的 Login、Get、Put 行为进行行为控制和行为审计；

对 HTTP(S)的 Connect、Get、Put、Head、Options、Post、Trace、Delete 行为进行行为控制和行为审计；

对 TELNET 客户端向服务器发起的请求内容进行行为控制和行为审计。

网络管理员可以针对不同用户、不同时间、不同应用程序行为制定适合的应用行为控制规则，系统将会对与规则相匹配的网络流量根据配置进行处理。

配置应用行为控制规则

配置应用行为控制功能包含两部分:

1. 配置应用行为控制规则。
2. 绑定应用行为控制规则到策略规则或安全域。

配置应用行为控制规则

1. 点击“对象 > 数据安全>内容过滤”，选择“应用行为控制”页签。
2. 点击“新建”按钮，打开<应用行为控制规则配置>页面。

在页面中填写应用行为控制规则的配置信息。

选项	说明
名称	输入规则名称。
控制	
FTP 控制	内容控制：对 FTP 协议的传输内容进行控制，如果传输内容匹配了指定的关键字类别，将执行指定的动作（阻断或记录日志）。点击“内容控制”，在展开区域进行如下配置： 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，参阅配置数据安全对象中的关键字类别部分。

选项	说明
	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。 关键字类别：显示系统中已有的关键字类别。 阻断：选中复选框，对传输内容包含相应关键字类别的行为进行阻断。 记录日志：选中复选框，对传输内容中包含相应关键字类别的行为进行日志记录。 命令控制：对 FTP 的 Login、Get、Put 行为进行控制。点击“命令控制”，在展开区域进行如下配置： 1. 在第一个下拉菜单中指定需要控制的 FTP 应用程序行为，包括 GET、PUT 和 Login。 2. 在文本框中输入相应的文件名（应用程序行为为 GET 或者 PUT 时）或者用户名（应用程序行为为 Login 时）。 3. 在第二个下拉菜单中指定控制动作，包括阻止和允许。 4. 在第三个下拉菜单中指定日志记录类型，包括不记录和记录日志。 5. 点击“添加”按钮，将控制配置条目添加进下方的列表。 6. 如需要，按照步骤 1 和 5 添加其它控制配置条目。如需要编辑/删除控制配置，单击选中列表中的控制配置条目，点击列表右侧的“编辑”/“删除”按钮，编辑/删除相应的控制配置条目。
HTTP 控制	命令控制：对 HTTP(S)的 Connect、Get、Put、Head、Options、Post、Trace、Delete 行为进行控制。点击“命令控制”，在展开区域进行如下配置： 1. 在第一个下拉菜单中指定需要控制的 HTTP(S)应用程序行为，包括 Connect、GET、PUT、Head、Options、Post、Trace 和 Delete。 2. 在文本框中输入相应的域名。 3. 在第二个下拉菜单中指定控制动作，包括阻止和允许。 4. 在第三个下拉菜单中指定日志记录类型，包括不记录和记录日志。 5. 点击“添加”按钮，将控制配置条目添加进下方的列表。 6. 如需要，按照步骤 1 和 5 添加其它控制配置条目。如需要

选项	说明
	编辑/删除控制配置，单击选中列表中的控制配置条目，点击列表右侧的“编辑”/“删除”按钮，编辑/删除相应的控制配置条目。
TELNET 控制	内容控制：对 TELNET 客户端向服务器发起的请求内容进行控制，如果请求内容匹配了指定的关键字类别，将执行指定的动作（阻断或记录日志）。点击"内容控制"，在展开区域进行如下配置： 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，参阅配置数据安全对象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。 关键字类别：显示系统中已有的关键字类别。 阻断：选中复选框，对请求内容中包含相应关键字类别的行为进行阻断。 记录日志：选中复选框，对请求内容中包含相应关键字类别的行为进行日志记录。

4. 点击“确定”按钮，保存所做配置并返回上一级对话框/页面。

绑定应用行为控制规则到安全域/策略规则

系统支持基于安全域和基于策略的应用行为控制配置方式：

为安全域配置应用行为控制规则后，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应用行为控制规则配置进行过滤。

为策略规则配置应用行为控制规则后，系统将会对与策略规则相匹配的流量根据应用行为控制规则配置进行过滤。

若安全域和策略中均配置了应用行为控制规则，策略中的配置项将有更高的优先权；在安全域配置中，目的安全域的优先权将高于源安全域。

基于安全域的配置方式，请按照以下步骤进行操作：

1. 创建安全域。
2. 在<安全域配置>页面中，点击“数据安全”展开配置项。
3. 点击“应用行为控制”后的“启用”按钮；并可根据自身需要，点击“模板”下拉菜单选择已配置好的应用行为控制规则或默认规则；也可点击“模板”下拉菜单中 ⊕ 按钮，新建应用行为控制规则。
4. 点击“确定”完成配置。

基于策略的应用行为控制配置方式，请按照以下步骤进行操作：

1. 配置策略。
2. 在<策略配置>页面中，点击“数据安全”展开配置项。
3. 点击“应用行为控制”后的“启用”按钮；并可根据自身需要，点击“模板”下拉菜单选择已配置好的应用行为控制规则；也可点击“模板”下拉菜单中 ⊕ 按钮，新建应用行为控制规则。
4. 点击“确定”完成配置。

如果需要，用户还可以配置相关的页面提示、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	预定义的 URL 库，包含数十个类别，多达上千万条 URL，用于 URL 类别的指定。
自定义 URL 库	自定义的 URL 库。用于 URL 类别的指定。
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。

查看应用行为控制日志

查看应用行为控制日志，参阅监控模块中的**内容过滤日志**部分。

上网行为审计

上网行为审计功能可以对 IM 应用程序行为进行审计，并能对访问行为进行日志记录，包括：

对 QQ、微信和微博的行为审计；

指定上网日志记录控制动作。

配置上网行为审计

配置上网行为审计功能包含两部分:

1. 配置上网行为审计规则。
2. 绑定上网行为审计规则到策略规则或安全域。

配置上网行为审计规则

1. 点击“对象 > 数据安全> 上网行为审计”，进入上网行为审计页面。
2. 点击“新建”按钮，打开<上网行为审计配置>页面。

在对话框中填写上网行为审计规则的配置信息。

选项	说明
名称	输入规则名称。
IM 种类	
QQ	对使用 QQ 聊天进行审计。 1. 点击“QQ”的“启用”按钮。 2. 超时：输入超时时间。单位为分钟，取值范围为 5 到 20，默认值为 10。在超时时间内，相同 QQ 用户的流量不会触发新的日志。超过超时时间后，QQ 用户的流量会触发新的日志。
微信	对微信进行审计。 1. 点击“微信”的“启用”按钮。 2. 超时：输入超时时间。单位为分钟，取值范围为 5 到 20，默认值为 20。在超时时间内，相同微信用户的流量不会触发新的日志。超过超时时间后，微信用户的流量会触发新的日志。
新浪微博	对新浪微博进行审计。 1. 点击“新浪微博”的“启用”按钮。

选项	说明
	2. 超时：输入超时时间。单位为分钟，取值范围为 5 到 20，默认值为 20。在超时时间内，相同新浪微博用户的流量不会触发新的日志。超过超时时间后，微信用户的流量会触发新的日志。
上网日志记录	
记录上网方式	上网日志记录对 HTTP 的 GET 及 POST 方法进行日志记录： Get：记录 GET 方法的上网日志信息。 Post：记录 POST 方法的上网日志信息。
记录日志内容	当使用 POST 方法记录日志时，可以指定记录日志内容： Post 内容：记录 POST 内容。

3. 点击“确定”按钮，保存所做配置并返回上一级对话框/页面。

绑定上网行为审计规则到安全域/策略规则

系统支持基于安全域和基于策略的上网行为审计配置方式：

为安全域配置上网行为审计规则后，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上网行为审计规则配置进行过滤。

为策略规则配置上网行为审计规则后，系统将会对与策略规则相匹配的流量根据上网行为审计规则配置进行过滤。

若安全域和策略中均配置了上网行为审计规则，策略中的配置项将有更高的优先权；在安全域配置中，目的安全域的优先权将高于源安全域。

基于安全域的配置方式，请按照以下步骤进行操作：

1. 创建安全域。
2. 在<安全域配置>对话框中，选择<数据安全>标签页。
3. 勾选“上网行为审计”后的“启用”复选框；并可根据自身需要，点击“模板”下拉菜单选择已配置好的上网行为审计规则或默认规则；也可点击“模板”下拉菜单中“新建配置”按钮，新建上网行为审计规则。
4. 配置 IM 审计功能后，需要开启安全域的应用识别功能。在<安全域配置>对话框中，选中“应用识别”复选框。
5. 点击“确定”完成配置。

基于策略的上网行为审计配置方式，请按照以下步骤进行操作：

1. 配置策略。
2. 在<策略配置>对话框中，选择<数据安全>标签页。
3. 勾选“上网行为审计”后的“启用”复选框；并可根据自身需要，点击“模板”下拉菜单选择已配置好的上网行为审计规则；也可点击“模板”下拉菜单中“新建配置”按钮，新建上网行为审计规则。
4. 点击“确定”完成配置。

查看上网行为审计日志

查看上网行为审计日志，参阅监控模块中的上网行为审计日志部分。

NetFlow

NetFlow 是一种数据交换方式，统计记录网络中数据包的源\目的地址、端口号等信息，是网络流量统计和分析的一种重要手段。

系统的 NetFlow 功能，支持 NetFlow V9，能够根据配置的 NetFlow 模板规则采集用户的入接口流量信息，并发送到带有 NetFlow 数据分析工具的服务器，通过服务器对流量的分析，实现对网络流量的检测、监控以及流量计费等。

配置 NetFlow

系统支持基于接口的 NetFlow 配置方式。

基于接口的 NetFlow 配置，请按照以下步骤进行操作：

1. 点击“对象 > NetFlow > 配置”，点击“开启 NetFlow”的“启用”按钮，开启全局 NetFlow 功能。
2. 点击“对象 > NetFlow > 模板”，配置 NetFlow。
3. 将已创建的 NetFlow 规则，绑定到接口上。点击“网络 > 接口”，创建或编辑接口。在<接口配置>对话框中，选择<高级配置>标签页。在“NetFlow 配置”下拉菜单中选择已配置好的 NetFlow 规则。

配置 NetFlow 规则

配置 NetFlow 规则，请按照以下步骤进行操作：

1. 点击“对象>NetFlow>模板”。
2. 点击“新建”按钮创建新的 NetFlow 规则。如需编辑已存在的 NetFlow 规则，勾选其复选框，并点击“编辑”。

在<NetFlow 配置>页面，填写 NetFlow 规则配置信息

选项	说明
名称	指定 NetFlow 规则名称。
服务器	配置用于 NetFlow 数据分析的服务器。配置方法如下： 1. 点击“新建”按钮，分别在“服务器名称”、“IP”和“端口”文本框中输入服务器名称、IP 地址以及端口号。 2. 重复以上步骤添加更多服务器，系统最多允许配置 2 个服务器。如果需要删除服务器，从列表中选中需要删除的服务器的复选框，然后点击“删除”按钮。
主动超时时间	指定发送 NetFlow 流量信息的频率时间。在主动超时时间结束后，设备将发送一次采集的 NetFlow 流量信息到指定服务器。范围是 1 到 60 分钟，默认值是 5 分钟。
源接口	在下拉菜单中选择发送 NetFlow 流量信息的源接口。
源 IP 地址	在指定源接口后，系统会自动获取并在下拉菜单中显示该源接口的管理 IP 地址或者接口二级 IP 地址。
模板刷新率	时间：指定 NetFlow 规则模板按照时间的刷新率。范围是 1 到 3600 分钟，默认值是 30 分钟。 数据包：指定数据包个数，即当 NetFlow 数据包个数达到指定值后，该 NetFlow 规则模板刷新一次。范围是 1 到 600 个，默认值是 20 个。 企业字段：点击“启用”按钮，采集的 NetFlow 流量信息

选项	说明
	中将包含企业字段信息。

3. 点击“保存”完成配置。

配置 NetFlow 全局参数

配置 NetFlow 全局参数，请按照以下步骤进行：

1. 点击“对象 > NetFlow > 配置”。
2. 点击“开启 NetFlow”后“启用”按钮，开启 NetFlow 功能。清除该复选框，禁用 NetFlow 功能。配置后，需要重启设备以使其生效。

访问控制

系统支持基于 MAC 地址的访问控制策略，用户可以创建访问控制模板并将其引用到安全策略上，实现对特定的 MAC 地址的访问控制。通过安全策略与访问控制模板规则相结合，能够使设备完成细粒度的访问控制。

访问控制模板

访问控制模板是由一条或多条访问控制规则组成。在访问规则中，用户可以通过指定源 MAC 地址和目的 MAC 地址，从而对流经设备的报文进行过滤，同时对符合条件的报文设置访问控制动作（通过或丢弃）。配置完成的访问控制模板只有被安全策略引用时，才会真正生效。

新建访问控制模板，请按照以下步骤进行操作：

1. 选择“对象 > 访问控制 > 模板”；
2. 点击“新建”按钮，打开<配置访问控制模板>页面。

在<配置访问控制模板>页面，填写如下配置信息：

选项	描述

选项	描述
名称	指定访问控制模板的名称。
默认控制动作	指定访问控制的默认动作，对于命中下方访问控制规则列表中的报文，则优先按照访问控制规则中动作进行处理；对于未命中访问控制规则列表中的报文，系统将按照此处的默认动作进行处理。默认控制动作包括： 通过：系统默认允许报文通过访问控制策略检测，但仍需继续进行其他安全检测（如 IPS，AV 病毒检测等）。 丢弃：系统默认将直接丢弃报文，报文将无法通过设备。
规则序列	点击“新建”按钮。 访问控制优先级：指定访问控制规则的优先级。取值范围为 1~32。系统会对报文按照优先级数值从小到大的顺序依次匹配。 动作： 指定访问控制策略的动作。 通过： 对符合条件的报文，系统将允许其通过访问控制策略检测，但仍需继续进行其他安全检测（如 IPS，AV 病毒检测等）。 丢弃：对符合条件的报文，系统将直接丢弃，该报文将无法通过设备。 流量方向 ：指定访问控制规则匹配和生效的流量方向。“正向流量”表示发起会话方向的流量。“反向流量”表示会话响应方向的流量。“双向”表示会话发起和响应的方向。默认情况下，系统匹配双向的流量。 源 MAC 地址 ：指定访问控制规则所匹配报文的源 MAC 地址。 目的 MAC 地址 ：指定访问控制规则所匹配报文的目的 MAC 地址。 DSCP：指定 DSCP 的值，取值范围是 0-63。 限制类型：指定访问控制规则所匹配 IPv6 报文的扩展头的限制类型，包括总扩展头数、单扩展头数和扩展头顺序。 总扩展头数：需继续指定报文的总扩展头数及对比方式，系统将对 IPv6 报文中的扩展头的总数进行统计和限制，若符合限制要求，系统将按照该规则的动作进行处理。 单扩展头头数：需继续指定单扩展头名称、头数及对比方式，系统将对 IPv6 报文中的单个扩展头的数

选项	描述
	量进行统计和限制，若符合限制要求，系统将按照该规则的动作进行处理。 扩展头顺序：需继续指定 IPv6 报文扩展头的排列顺序：顺序或乱序。“顺序”表示扩展头需按照顺序进行排列；“乱序”表示扩展头为非顺序排列，即乱序。若符合限制要求，系统将按照该规则的动作进行处理。 日志：开启后，系统将对匹配该访问控制规则的报文进行日志信息记录。 编辑/删除指定的规则，勾选指定规则前的复选框，然后点击“编辑”/“删除”按钮。

3. 点击“确定”，完成配置。

第 9 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 将 IP 数据包包头中的 IP 地址转换为另一个 IP 地址。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。

iQoS：iQoS 为特定流量提供更高优先服务的同时控制抖动和延迟的能力，并且能够降低数据传输丢包率。当网络过载或拥塞时，系统能够确保重要业务流量的正常传输。

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。

共享接入：即多个用户终端通过同一个 IP 地址接入到网络。系统的共享接入功能可以防范未知设备的接入，消除潜在的安全风险，并能够帮助用户合理分配带宽，限制多用户共享带宽，保证用户的上网体验。

ARP 防护：ARP 防护功能保护网络免受各种 ARP 攻击。

边界流量过滤：通过对基于已知的 IP 地址黑白名单对流量进行过滤，并对命中黑名单的恶意流量采取阻断措施进行处理。

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，网络安全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决定从一个安全域到另一个安全域，以及从一个地址段到另一个地址段的哪些流量该被允许，哪些流量该被拒绝。

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

流量的服务类型

设备在遇到指定类型流量时所做的行为，包括允许（Permit）、拒绝（Deny）、隧道（Tunnel）、是否来自隧道（Fromtunnel）、Web 认证以及 Portal 服务器六个行为

一般来讲，策略规则分为两部分：过滤条件和行为。安全域间流量的源安全域/源地址、目的安全域/目的地址、服务类型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，同时用户也可以按自己的需求为策略规则指定 ID。整个系统的所有策略规则有特定的排列顺序。在流量进入系统时，系统会对流量按照找到的第一条与过滤条件相匹配的策略规则进行处理。

不同设备平台支持的全局最大策略规则数不同。

安全策略支持指定 IPv4 和 IPv6 格式的地址条目。如接口开启了 IPv6 功能，用户可根据需要配置 IPv6 地址的策略规则。

本章节包含以下内容：

配置策略规则

管理策略规则：启用/禁用策略规则，复制策略规则，调整优先级，设置策略默认动作，查看及清零策略命中数，规则冗余检查，命中数检测，时间表有效性检测，显示禁用策略，导入/导出策略规则、命中查询、配置策略审计功能。

配置聚合策略

配置策略组

配置微型策略

查看及过滤策略规则/策略组/微型策略

配置策略助手

配置策略规则

配置策略规则，请按照如下步骤进行操作：

1. 点击“策略 > 安全策略 > 策略”。

2. 点击左上角的“新建”按钮，点击“策略”，打开<策略配置>页面。

在<策略配置>页面，填写基本配置信息。

选项	说明
名称	输入安全策略的名称。长度为 0-95 字符。
类型	指定 IP 的地址类型，可选择 IPv4 或 IPv6。类型指定仅当该版本支持 IPv6 时可配；选择后，系统仅支持配置 IPv6 格式的 IPv6/前缀长度、IP 地址范围或 IP 地址条目。
源安全域	指定策略规则的源安全域。该选项会保存上次新建策略规则所选安全域。 单安全域模式下，点击“源安全域”，在下拉菜单中选择需要的安全域。若开启了**多安全域模式**，请按照以下步骤进行操作： 1. 点击“源安全域”，弹出的对话框将展示系统中可供选择的安全域。 2. 选中需要的安全域，将其添加到左侧列表中。最多可选择 16 个。 3. 添加完成后，点击“关闭”。 用户还可执行如下操作： 选择安全域时，可点击 ⊕ 按钮创建新的安全域。 系统默认安全域配置为 Any。如需恢复为 Any，点击

选项	说明
	“Any“启用按钮。
源地址	指定策略规则的源地址。 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左侧列表中。 4. 添加完成后，点击“关闭”。 用户还可执行如下操作： 选择地址簿类型时，可点击  按钮创建新的地址簿。 选择地址簿类型时，点击搜索框中的  按钮，可以按地址簿名称和地址成员的 IP 进行模糊搜索，名称和地址是与的关系。地址支持多种输入方式，例如：输入“地址”为 10.10.10.10/32，可能匹配到包含地址成员是 10.10.10.10/24 的地址簿；输入“地址”为段掩码 9.9.9.9/24，可能匹配到包含地址成员是 9.9.0.0/16 的地址簿；输入“地址”为 10.10.10.10，可能匹配到地址成员的 IP 范围为 10.10.10.0-10.10.10.255 的地址簿；输入“地址”为 10.23，可能匹配到包含地址成员是 1.10.23.10/24 的地址簿；输入“地址”为 aa，可能匹配到地址成员的“主机名称”为 aaa 的地址簿。 系统默认地址配置为 any。如需恢复为 any，选择 **any** 复选框。
源用户	指定策略规则的角色、用户和用户组。 1. 在“用户/用户组”下拉菜单中，选择用户或用户组所在的 AAA 服务器。如需指定角色，则在“AAA 服务器/角色”下拉菜单中选择 **Role**。 2. 根据 AAA 服务器类型不同，用户可执行以下一个或多个操作：搜索指定用户/用户组/角色、展开用户/用户组列表、输入指定用户/用户组。 3. 点击所选择的用户/用户组/角色，将其添加到左侧列表中。 4. 添加完成后，点击“关闭”。
目的安全域	指定策略规则的目的安全域。该选项会保存上次新建策略规则所选

选项	说明
	安全域。 单安全域模式下，点击“目的安全域”，在下拉菜单中选择需要的安全域。 若开启了多安全域模式，请按照以下步骤进行操作： 1. 点击“目的安全域”，弹出的对话框将展示系统中可供选择的安全域。 2. 选中需要的安全域，将其添加到左侧列表中。最多可选择16个。 3. 添加完成后，点击“关闭”。 用户还可执行如下操作： 选择安全域时，可点击⊕按钮创建新的安全域。 系统默认安全域配置为 Any。如需恢复为 Any，点击“Any“启用按钮。
目的地址	指定策略规则的目的地址。 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左侧列表中。 4. 添加完成后，点击“关闭”。 用户还可执行如下操作： 选择地址簿类型时，可点击⊕按钮创建新的地址簿。 选择地址簿类型时，点击搜索框中的▼按钮，可以按地址簿名称和地址成员的 IP 进行模糊搜索，名称和地址是与的关系。地址支持多种输入方式，例如：输入“地址”为10.10.10.10/32，可能匹配到包含地址成员是 10.10.10.10/24的地址簿；输入“地址”为段掩码 9.9.9.9/24，可能匹配到包含地址成员是 9.9.0.0/16 的地址簿；输入“地址”为10.10.10.10，可能匹配到地址成员的 IP 范围为 10.10.10.0-10.10.10.255 的地址簿；输入“地址”为 10.23，可能匹配到包含地址成员是 1.10.23.10/24 的地址簿；输入“地址”为 aa，可能匹配到地址成员的“主机名称”为 aaa 的地址簿。

选项	说明
	系统默认地址配置为 any。如需恢复为 any，选择 **any** 复选框。
服务	指定策略规则的服务/服务组。 1. 在“服务”下拉菜单中选择类型：服务，服务组。 2. 用户可搜索指定服务/服务组，展开服务/服务组列表。 3. 选择指定服务/服务组，将其添加到左侧列表中。 4. 添加完成后，点击“关闭”。 用户还可执行如下操作： 如需添加新的服务/服务组，在“预定义”下拉菜单中选择“自定义”，再点击 ⊕ 按钮。 系统默认服务配置为 any。如需恢复为 any，选择 **any** 复选框。 指定策略规则的服务规则。当所需要的服务在服务簿中不存在时，可以通过配置服务规则，直接指定服务的协议类型以及端口号等信息，从而简化策略的配置步骤。 1. 在“服务”下拉菜单中选择类型：服务规则。 2. 在“协议类型”下拉菜单中选择协议类型：TCP、UDP、SCTP、ICMP、ICMPv6 以及全部。 不同类型的具体参数的配置描述如下： **TCP/UDP/SCTP**： 目的端口：“最小端口”指定服务规则的最小目的端口号；“最大端口”指定服务规则的最大目的端口号。端口号范围是 0 到 65535。 源端口：“最小端口”指定服务规则的最小源端口号；“最大端口”指定服务规则的最大源端口号。范围是 0 到 65535。 **注意：** “最小端口号”不能大于“最大端口号”。 目的端口的“最小端口”为必填项，其他选项均为选填项。 当不配置“最大端口”时，系统将使用“最小端口”作

选项	说明
	为端口号。 **ICMP：** 类型：指定服务规则的 ICMP type 值。通过下拉菜单可以选择 0（Echp-Reply）、3（Destination-Unreachable）、4（Source Quench）、5（Redirect）、8（Echo）、11（Time Exceeded）、12（Parameter Problem）、13（Timestamp）、14（Timestamp Reply）、15（Information Request）、16（Information Reply）、17（Address Mask Request）、18（Address Mask Reply）、30（Traceroute）、31（Datagram Conversion Error）、32（Mobile Host Redirect）、33（IPv6 Where-Are-You）、34（IPv6 I-Am-Here）、35（Mobile Registration Request）、36（Mobile Registration Reply）。 代码：指定服务规则的 ICMP code 最小值和最大值。范围是 0-15，默认值最小值为 0、最大值为 15。 **ICMPv6：** 类型：指定服务规则的 ICMPv6 type 值。通过下拉菜单可以选择 1（Dest-Unreachable）、2（Packet Too Big）、3（Time Exceeded）、4（Parameter Problem）、5-99（Unallocated Error message）、100（Private experimentation）、101（Private experimentation）、102-126（Unallocated Error message）、127（Reserved for expansion of ICMPv6 error message）、128（Echo Request）、129（Echo Reply）、130（Multicast Listener Query）、131（Multicast Listener Report）、132（Multicast Listener Done）、133（Router Solicitation）、134（Router Advertisement）、135（Neighbor Solicitation）、136（Neighbor Advertisement）、137（Redirect Message）、138（Router Renumbering）、139（ICMP Node Information Query）、140（ICMP Node Information Response）、141（Inverse Neighbor Discovery Solicitation Message）、142（Inverse

选项	说明
	Neighbor Discovery Advertisement Message）、143（Version 2 Multicast Listener Report）、144（Home Agent Address Discovery Request Massage）、145（Home Agent Address Discovery Reply Massage）、146（Mobile Prefix Solicitation）、147（Mobile Prefix Advertisement ）、148（Certification Path Solicitation Message）、149（Certification Path Advertisement Message）、150（ICMP message utilized by experimental mobility protocols such as Seamoby）、151（Multicast Router Advertisement）、152（Multicast Router Solicitation ）、153（Multicast Router Termination）、154（FMIPv6 Messages）、200（Private experimentation）、201（Private experimentation）和 255（Reserved for expansion of ICMPv6 informational）。 代码：指定服务规则的 ICMPv6 code 最小值和最大值。范围是 0-255。默认值最小值为 0、最大值为 255。 **注意：** “最小值”不能大于“最大值”。 如果不配置“最大值”，系统将使用“最小值”作为单一代码值。 **全部：** 在下拉菜单选择服务规则的协议名称。如果是非知名协议，可以直接输入对应的协议号。 3. 点击“添加”按钮将配置的服务规则添加到左侧列表中。 4. 添加完成后，点击“关闭”。
应用	指定策略规则的应用/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，将其添加到左侧列表中。 3. 添加完成后，点击“关闭”。 如需新建应用组或应用过滤组，在“应用”下拉菜单中选择应用组或

选项	说明
	应用过滤组，然后点击  按钮。
VLAN ID	指定策略规则需要匹配的 VLAN ID，取值范围为 1 到 4094。当需要配置多个 VLAN ID 时，使用分号分隔。每条策略规则可以配置最多 32 个 VLAN ID。
动作	指定对匹配策略规则的流量所采取的行为，包括： 允许： 允许流量通过。选择“允许”。 拒绝：拒绝流量通过。选择“拒绝”。 Web 认证：对符合条件的流量进行 Web 认证。选择“安全连接”，在下拉菜单中选择“Web 认证”，并在其后的下拉菜单中选择认证服务器的名称。 来自隧道（VPN）： 当流量为从对端到本地时，如果使用该行为，系统将会首先判断流量是否来自隧道，只有来自隧道的流量才会被允许通过。选择“安全连接”，在下拉菜单中选择“来自隧道（VPN）”，并在其后的下拉菜单中选择隧道名称。 隧道（VPN）：当流量为从本地到对端时，使用该行为使流量通过 VPN 隧道。选择“安全连接”，在下拉菜单中选择“隧道（VPN）”，并在其后的下拉菜单中选择隧道名称。如同时需要允许来自该指定 VPN 隧道的流量，勾选“双向 VPN 策略”复选框，当策略规则创建完成时，会同时自动创建另一条“来自隧道（VPN）”为该 VPN 隧道的策略规则。 **注意**：仅在新建策略规则时支持配置“双向 VPN 策略”功能。 Portal 服务器：对符合条件的流量进行 Portal 认证。选择“安全连接”，在下拉菜单中选择“Portal 服务器”，并在其后的文本框中输入 Portal 认证服务器地址。
启用 Web 重定向	Web 重定向是指当客户端发送 HTTP 网页访问请求后，系统自动将该请求重新定向到指定的通知页面。配置该功能后，当用户使用 HTTP 访问网络时，页面会先跳转到指定的通知页面。 1. 点击“启用 Web 重定向”后的“启用”按钮。 2. 输入通知页面的网址。 使用 Web 重定向功能时，需要同时配置 Web 认证。

选项	说明
审计注释	在启用“配置审计”功能后，当新建、修改策略配置时，该选项为必填项，用户必须在该文本框中添加策略审计注释内容。范围是 1 到 255 个字符。该功能详细操作，请参阅配置策略审计功能。 当未启用“配置审计”功能时，该选项为非必填项，范围是 0 到 255 个字符。 关于启用/禁用“配置审计”功能，请在<设置及操作>页面中配置（“系统>设备管理>设置及操作”），可参阅设置及操作中的配置审计部分。

点击“防护状态”，展开防护状态配置项，填写配置信息。

选项	说明
URL 过滤	启用 URL 过滤功能并指定 URL 过滤规则。通过安全策略与 URL 过滤规则相结合，能够使设备完成细粒度的应用层安全策略控制。选择“启用”并在下拉菜单中选择已创建的规则。

点击“数据安全”，展开数据安全配置项，填写配置信息。

选项	说明
文件过滤	启用文件过滤功能并指定文件过滤规则。通过安全策略与文件过滤规则相结合，能够使设备完成细粒度的文件过滤。选择“启用”按钮并在下拉菜单中选择已创建的规则。若要新建新规则，点击 ⊕ 按钮。
文件内容过滤	启用文件内容过滤功能并指定文件内容过滤规则。通过安全策略与文件内容过滤规则相结合，能够使设备完成细粒度的文件内容过滤。选择“启用”按钮并在下拉菜单中选择已创建的规则。若要新建新规则，点击 ⊕ 按钮。
网页关键字	启用网页关键字过滤功能并指定网页关键字规则。通过安全策略与网页关键字规则相结合，能够使设备完成细粒度的网页关键字过滤。选择“启用”按钮并在下拉菜单中选择已创建的规则。若要新建新规则，点击 ⊕ 按钮。
Web 外发信息	启用 Web 外发信息功能并指定 Web 外发信息规则。通过安全策略与 Web 外发信息规则相结合，能够使设备完成细粒度的 Web 外发信息审计。选择“启用”按钮并在下拉菜单中选择已创建的规则。若要新建新规则，点击 ⊕ 按钮。
邮件过滤	启用邮件过滤功能并指定邮件过滤规则。通过安全策略与邮件过滤规则相结合，能够使设备完成细粒度的邮件过滤。选择“启用”按钮并在下拉菜单中选择已创建的规则。若要新建新规则，点击 ⊕

选项	说明
	按钮。
应用行为控制	启用应用行为控制功能并指定应用行为控制规则。通过安全策略与应用行为控制规则相结合，能够使设备完成细粒度的应用行为控制。选择“启用”按钮并在下拉菜单中选择已创建的规则。若要新建新规则，点击  按钮。
上网行为审计	启用上网行为审计并指定上网行为审计规则。通过安全策略与上网行为审计规则相结合，能够使设备完成细粒度的上网行为审计控制。选择“启用”按钮，并在下拉菜单中选择已创建的规则。若要新建新规则，点击  按钮。

点击“选项”，展开选项配置项，填写配置信息。

选项	说明
时间表	指定策略规则的时间表。在“时间表”下拉菜单中选择需要的时间表，同时支持模糊搜索。选择完成后，点击对话框空白区域，即可完成时间表的选择。如需新建时间表，点击  按钮。
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。选中“记录日志”后相应的复选框开启相应的日志记录功能。 策略拒绝：对于拒绝类型的策略规则，记录符合策略规则的流量被拒绝时生成日志信息。 会话开始：对于允许类型的策略规则，记录符合策略规则的流量建立会话时生成日志信息。 会话结束：对于允许类型的策略规则，记录符合策略规则的流量结束会话时生成日志信息。
SSL 代理	指定 SSL 代理规则。通过策略与 SSL 代理规则相结合，能够使设备控制并解密 HTTPS 流量。点击“启用”按钮并在下拉菜单中选择已创建的规则。
策略助手	点击“启用”按钮，开启策略助手功能。开启策略助手功能后，用户可以在“策略助手”页面指定该策略 ID 为流量命中的策略 ID。系统能够提取命中指定策略 ID 的流量作为流量数据分析源，并根据用户设置的聚合规则聚合流量数据列表，最后生成符合用户期望的安全策略规则。如何使用策略助手功能，参见配置策略助手。
访问控制	启用访问控制功能并指定访问控制模板。通过安全策略和访问控制规则相结合，能够使设备完成细粒度的访问控制。点击“启用”按钮，并在下拉菜单中选择已创建的访问控制模板。
所属聚合策略	点击“所属聚合策略”下拉菜单，选择需要加入的聚合策略。

选项	说明
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的 ID 号或名称。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，即列表最前或者列表最后，也可以是相对位置，即位于该 ID 之前或之后，该名称之前或之后。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。长度为 0-255 字符。

3. 点击“确定”完成配置。

管理策略规则

对策略规则进行管理，包括启用/禁用策略规则，复制策略规则，调整优先级，设置策略默认动作，查看及清零策略命中数，规则冗余检查，命中数检测，时间表有效性检测、显示禁用策略和导入/导出策略规则。

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，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 策略”。
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 ⋮ 按钮，选择“启用”或“禁用”按钮。

策略规则禁用后，不再显示列表中。查看禁用的策略规则，在 ⋮ 按钮中选择“显示禁用策略”。

复制/粘贴策略规则

当系统中存在大量的策略规则时，为使用户更方便快捷地创建与已配置策略规则类似的策略规则，可以复制策略规则并且粘贴在指定位置。

复制/粘贴策略规则，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 策略”。
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。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，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 策略”。
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 号或者名称，并点击“之前”或“之后”按钮。被选中的安全策略规则将被移动至指定 ID 或者名称规则之前或之后。点击“最前”或“最后”按钮，被选中的安全策略规则将被移动至列表最前或最后。

设置策略规则默认动作

用户可以对未匹配到任何已配置策略规则的流量指定默认行为，系统将按照指定的默认行为对此类流量进行处理。默认情况下，系统会拒绝未匹配到任何已配置策略规则的流量通过。

指定策略的默认行为，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 策略”。
2. 点击 ⋮ 按钮，并在弹出菜单中选择“策略默认动作”。打开<策略默认动作>页面。

在<策略默认动作>页面，填写如下配置信息。

选项	说明
默认动作	指定未匹配到任何已配置策略规则的流量的默认行为。 允许：系统将允许未匹配到任何已配置的策略规则的流量通过。 拒绝：系统将拒绝未匹配到任何已配置的策略规则的流量通过。
日志	系统对于未匹配到策略规则的流量，可以指定是否为其生成日志信息。默认情况下，系统不为此类流量生成日志信息。选中“启用”复

选项	说明
	选框，开启日志功能，系统将对未匹配到策略规则的流量生成日志信息。

3. 点击“确定”完成配置。

策略全局配置

在策略全局配置中可以实现多安全域模式和单安全域模式的切换。单安全域模式下，一条策略仅支持配置一个源安全域和一个目的安全域；多安全域模式下，一条策略支持同时配置多个安全域，以减少系统中所需配置的策略数量，方便用户对策略进行管理。默认情况下，系统使用单安全域模式。

切换多/单安全域，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 策略”。
2. 点击 ⋮ 按钮，并在弹出菜单中选择“策略全局配置”。打开<策略全局配置>页面。
3. 点击多安全域后的“启用”按钮，开启多安全域模式；取消点击多安全域后的“启用”按钮，开启单安全域模式。
4. 点击“确定”完成配置。

时间表有效性检测

为保证基于时间的策略的有效性，系统可对规则进行时间表有效性检测。检测完成后，失效的基于时间的策略规则会被黄色高亮显示。

进行时间表有效性检测，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 策略”。
2. 点击 ⋮ 按钮，并在弹出菜单中选择“时间表有效性检测”。系统检测完成后，失效的基于时间的策略规则将被黄色高亮显示在策略列表中。另外，用户还可以在显示的“有效性”一列查看有效性状态。

显示禁用策略

为了更清晰的显示禁用的策略规则，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 策略”。

2. 点击 ⋮ 按钮，并在弹出菜单中勾选“显示禁用策略”复选框。禁用的策略规则将被灰色高亮显示在策略列表中。

导入策略规则

用户可以将本地策略规则配置文件导入到设备中，从而减少手动创建策略规则的工作量。目前仅支持导入 DAT 格式的文件。

导入策略规则配置文件，请按照以下步骤进行操作：

1. 点击“策略>安全策略>策略”。
2. 点击“导入”按钮，打开<导入>页面。

3. 点击“浏览”按钮，并选中需上传的本地策略规则配置文件。
4. 点击“确定”按钮，导入的策略规则将显示在策略页面中。

导出策略规则

用户可以将设备中当前的策略规则以 HTML 或 DAT 格式导出到本地，从而方便导入到其他设备中。同时，系统还支持将所有地址簿、服务簿、应用簿（自定义应用条目）等对象全部导出。

导出策略规则，请按照以下步骤进行操作：

1. 点击“策略>安全策略>策略”。
2. 点击“导出”按钮，打开<导出>页面。

在<导出>页面，填写如下配置信息。

选项	说明
范围	指定策略规则的导出范围。

选项	说明
	所有策略：选中“所有策略”，导出设备中当前的所有策略规则。 选中策略：在策略列表中，勾选需要导出的策略规则复选框，然后在该对话框中，选中“选中策略”，导出所选策略规则。 页码范围：选中“页码范围”，然后在文本框中输入页码或页码范围，导出指定页内的所有策略规则。 注意：页码之间须用分号隔开，例如：如需导出第 3 页以及第 5-8 页的策略规则，输入“3；5-8”。
导出地址条目、服务、应用	勾选该复选框，将所有地址簿、服务簿、应用簿等策略规则引用的对象全部导出，生成以“book+导出时间”命名的 ZIP 压缩文件。
导出 DAT 格式所有策略	勾选该复选框，以 DAT 格式导出所有策略规则配置文件。

3. 点击“确定”按钮，开始下载导出文件。导出文件包括 4 种：policyExport.html（安全策略展示页）、policy+导出时间.zip（策略规则配置文件）、book+导出时间.zip（对象配置文件）以及 DAT 格式策略规则配置文件。

4. 双击已下载的安全策略展示页“policyExport.html”，点击“选择文件”按钮，选择已下载的策略规则配置文件“policy+导出时间.zip”，即可查看已导出的策略规则表格。

5. 双击已下载的安全策略展示页“policyExport.html”，点击“选择文件”按钮，选择已下载的对象配置文件“book+导出时间.zip”，即可查看已导出的对象配置文件表格。

命中查询

用户可以通过五元组（源 IP 地址、目的 IP 地址、协议、源端口、目的端口）查询策略规则。请按照以下步骤进行操作：

1. 点击“策略>安全策略>策略”。

2. 点击“命中查询”按钮，展开配置页面。

配置如下信息。

选项	说明
源安全域	点击下拉菜单选择指定的源安全域，查询符合指定源安全域的策略规则。
源地址	在文本框中输入源地址，查询符合指定源地址的策略规则。该源地址支持模糊匹配，可以查询包含输入地址的策略规则。
目的安全域	点击下拉菜单选择指定的目的安全域，查询符合指定目的安全域的策略规则。
目的地址	在文本框中输入目的地址，查询符合指定目的地址的策略规则。该目的地址支持模糊匹配，可以查询包含输入地址的策略规则。
协议	在“协议”下拉菜单中选择协议类型，查询符合指定协议的策略规则。 当协议指定为 TCP、 UDP 时，可以指定源/目的端口范围，取值范围是 0-65535，如果指定相同的最小、最大源/目的端口号，系统将使用该端口号作为单一源/目的端口号。 当协议指定为 ICMP 时，可以指定类型、代码范围。如果指定相同的最小、最大代码值，系统将使用该代码值作为单一代码值。代码的取值范围是 0-15。 当协议指定为 ICMPv6 时，可以指定类型、代码范围。如果指定相同的最小、最大代码值，系统将使用该代码值作为单一代码值。代码的取值范围是 0-255。 当协议指定为其他协议类型时，则不支持配置端口范围或代码范围。 **注意：**如果指定端口范围或代码范围，那么最大端口号/代码值和最小端口号/代码值必须同时配置。

3. 点击“确定”按钮后，策略列表将显示查询结果。

4. 如需清除命中查询配置，显示所有策略规则，点击“清除命中查询”按钮。

注意: 命中查询功能与通过过滤条件查询策略规则功能为互斥的，二者不能同时配置，当已配置命中查询功能时，过滤条件配置将会被清空，反之同理。

配置策略审计功能

系统支持策略审计功能，当用户新建、修改策略规则/聚合策略配置时，需要使用该功能，为策略规则/聚合策略添加策略审计注释内容，来说明策略规则/聚合策略的创建/修改原因，以便用户了解策略规则/聚合策略配置的变更理由、变更历史记录。

开启配置审计功能

默认情况下，配置审计功能为关闭状态。开启配置审计功能，请按照以下步骤进行操作：

1. 选择“系统 > 设备管理 > 设置及操作”，进入设置及操作页面。
2. 在系统设置标签页，点击“配置审计”后的“启用”按钮，点击“确定”按钮。

添加审计注释

当用户新建或修改策略规则/聚合策略配置时，为策略规则/聚合策略添加策略审计注释内容，请按照以下步骤进行操作：

1. 选择“策略>安全策略>策略”。
2. 点击左上角的“新建”下拉菜单，选择“策略”或“聚合策略”，或者在列表中选中需要编辑的策略规则/聚合策略，点击上方“编辑”按钮。
3. 在<策略配置>页面的“审计注释”文本框中，输入注释内容。
4. 点击“确定”保存配置。

在删除、粘贴、移动、启用、禁用策略规则/聚合策略、添加到聚合策略、移出聚合策略后，均会弹出<审计注释>对话框，用户需在该对话框中填写注释内容。

注意: 在新建、修改、删除、粘贴、移动、启用、策略规则/聚合策略、添加到聚合策略、移出聚合策略时，审计注释均为必配项。

查看审计历史

在<策略配置>页面的“审计注释”文本框下方，点击“审计历史”按钮，打开<策略审计>页面，查看策略规则/聚合策略的审计历史。

“版本变化情况”列表中，展示了所选策略规则/聚合策略的版本号、修改日期、修改人名称以及审计注释内容。其中，“版本号”为系统自动分配，在恢复出厂设置后将会重新从 1 开始叠加。

点击版本号，打开<策略及审计注释详情>页面，查看策略的详细配置信息内容。

勾选需要对比查看的两个条目，点击“对比”按钮，下方“版本变化对比”页面中展示两个版本的策略配置信息内容，并以黄色高亮显示出不同的内容。

勾选指定条目，点击“导出”按钮，在<审计导出>页面中指定导出文件的名称、导出文件格式类型（TXT 或 CSV），然后点击“确定”后浏览器启动默认的下载工具，下载导出文件压缩包。

注意: 仅系统管理员（admin）支持配置审计历史文件的导出功能。

配置聚合策略

用户可以根据场景需要，创建聚合策略并且将一些具有相同作用或者相同属性的策略规则加入聚合策略，管理员调整聚合策略的优先级后，所有聚合策略成员的优先级将会一起调整，实现对策略规则的批量管理。

配置聚合策略包括新建聚合策略、添加聚合策略成员、移出聚合策略成员、删除聚合策略、调整聚合策略优先级、启用/禁用聚合策略。

新建聚合策略

新建聚合策略，请按照如下步骤进行操作：

1. 点击“策略 > 安全策略 > 策略”。
2. 点击左上角的“新建”下拉菜单，选择“聚合策略”，打开<聚合策略配置>页面。

在<聚合策略配置>页面，填写基本配置信息。

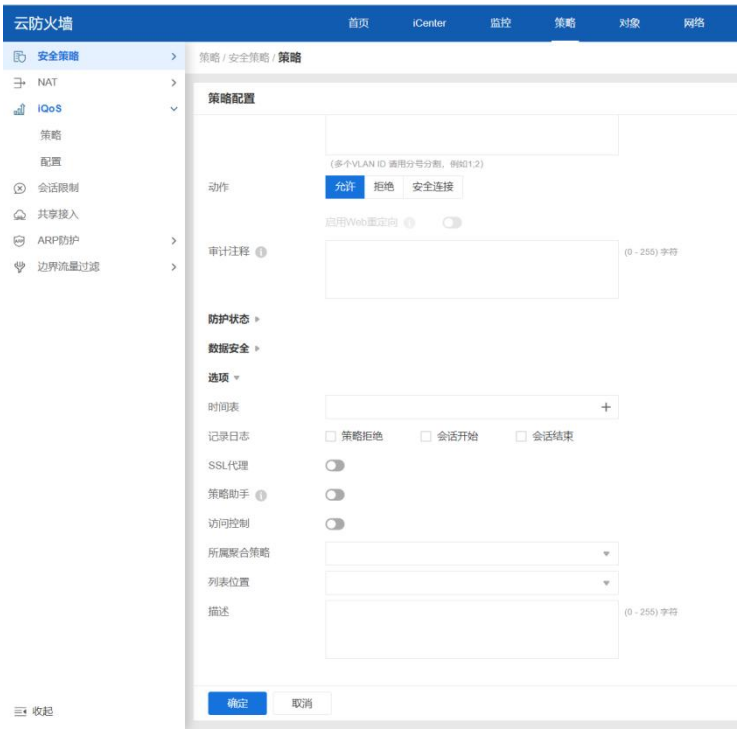
选项	说明
名称	指定聚合策略的名称。范围是 1 到 95 个字符。
列表位置	聚合策略的排列位置可以是绝对位置，即列表最前或者列表最后，也可以是相对位置，即位于该 ID 之前或之后，该名称之前或之后。 在“列表位置”下拉菜单中选择该聚合策略的位置。
描述	添加聚合策略的描述信息。
审计注释	在启用“配置审计”功能后，当新建、修改聚合策略配置时，该选项为必填项，用户必须在该文本框中添加策略审计注释内容。范围是 1 到 255 个字符。该功能详细操作，请参阅配置策略审计功能。 当未启用“配置审计”功能时，该选项为非必填项，范围是 0 到 255 个字符。 关于启用/禁用“配置审计”功能，请在<设置及操作>页面中配置（“系统>设备管理>设置及操作”），可参阅设置及操作中的配置审计部分。

3. 点击“确定”按钮，完成配置。

添加聚合策略成员

当聚合策略创建完成后，管理员可以将策略规则添加到聚合策略中成为聚合策略成员。管理员可以通过以下 2 种方式，将策略规则添加到聚合策略中。

通过编辑策略规则配置信息的方式：



如上图所示，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 策略”。
2. 在列表中选中一个需要添加到聚合策略的策略规则复选框。
3. 点击上方“编辑”按钮，打开<策略配置>页面。
4. 点击“选项”展开相关配置项。
5. 点击“所属聚合策略”下拉菜单，选择需要加入的聚合策略。
6. 点击“确定”完成添加。

通过勾选策略规则直接添加的方式：

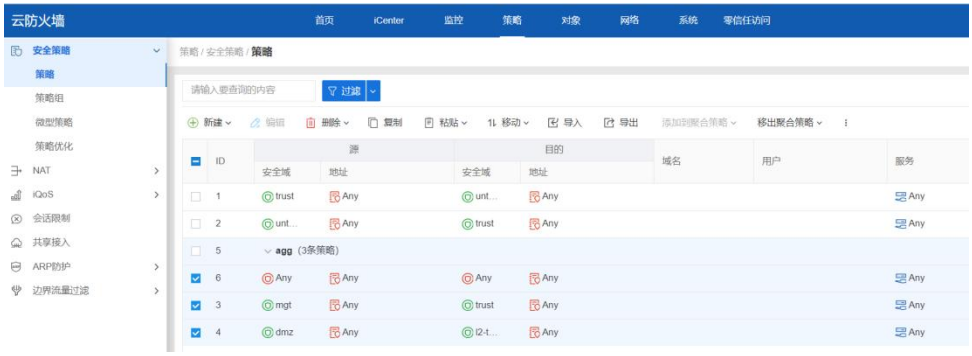
如上图所示，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 策略”。
2. 在列表中选中需要添加到聚合策略的策略规则复选框，可多选。

3. 点击上方“添加到聚合策略”下拉菜单，选择需要加入的聚合策略。

移出聚合策略成员

从聚合策略中移出聚合策略成员，请按照以下步骤进行操作：



1. 点击“策略 > 安全策略 > 策略”。
2. 在列表中，点击聚合策略前的箭头，展开聚合策略。
3. 选中需要移出的聚合策略成员复选框，可多选。
4. 点击上方“移出聚合策略”按钮。

注意:

当最前位置的聚合策略成员被移出聚合策略后，将会被排列到该聚合策略之前。

当非最前位置的聚合策略成员被移出聚合策略后，将会被排列到该聚合策略之后。

当移出多个连续且包含最前位置的聚合策略成员后，将会一同被排列到该聚合策略之前。

删除聚合策略

删除聚合策略，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 策略”。
2. 在列表中勾选需要删除的聚合策略复选框。
3. 点击上方“删除”按钮。

4. 在展开的下拉菜单中选择删除方式。

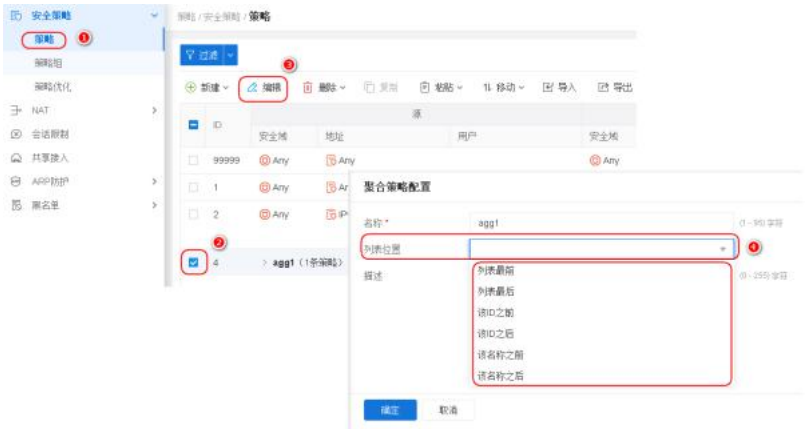
删除聚合策略及其成员：删除聚合策略的同时，将其中的聚合策略成员一并删除。

删除聚合策略并解绑成员：删除聚合策略的同时，将其中的聚合策略成员全部移出。

调整聚合策略优先级

管理员可以通过以下 2 种方式，调整聚合策略的优先级，调整后，所有聚合策略成员的优先级将会一起被调整。

通过编辑聚合策略配置信息的方式：



如上图所示，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 策略”。
2. 在列表中勾选需要调整优先级的聚合策略复选框。

3. 点击上方“编辑”按钮，打开<聚合策略配置>页面。

4. 点击“列表位置”下拉菜单，选择该聚合策略需要调整的位置。

通过在策略列表中直接调整的方式：

如上图所示，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 策略”。

2. 从策略列表中选中需要调整优先级的聚合策略对应的复选框。

3. 点击列表上方的“移动”按钮。

4. 在弹出下拉菜单中点击“最前”、“最后”或者在“到 ID”、“到名称”文本框中，输入 ID 号或者名称，并点击“之前”或“之后”按钮。被选中的聚合策略将被移动至策略列表最前、最后、或指定 ID/名称规则之前/之后。

注意:

聚合策略中的成员优先级的调整方式，与上述聚合策略优先级调整方式一致。

聚合策略成员的优先级调整只能在所属聚合策略中进行。

不支持通过调整策略规则的优先级实现添加到聚合策略或者从聚合策略中移出。

启用/禁用聚合策略

默认情况下，配置好的聚合策略会在系统中立即生效。管理员可以通过配置禁用某个聚合策略，使其不对流量进行控制。

启用/禁用聚合策略，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 策略”。

2. 选中列表中需要启用/禁用的聚合策略对应的复选框。

3. 点击 ⋮ 按钮，选择“启用”或“禁用”按钮。

聚合策略禁用后，不再显示列表中。查看禁用的聚合策略，在“ ⋮ ”下拉菜单中选择“显示禁用策略”。

注意:

禁用聚合策略后，聚合策略中的成员同时被禁用。

启用聚合策略后，聚合策略中的成员状态将会保持原有启用/禁用状态。例如，某个聚合策略成员原有状态为禁用，那么当启用其所属的聚合策略后，该聚合策略成员状态依旧保持禁用状态。

配置策略组

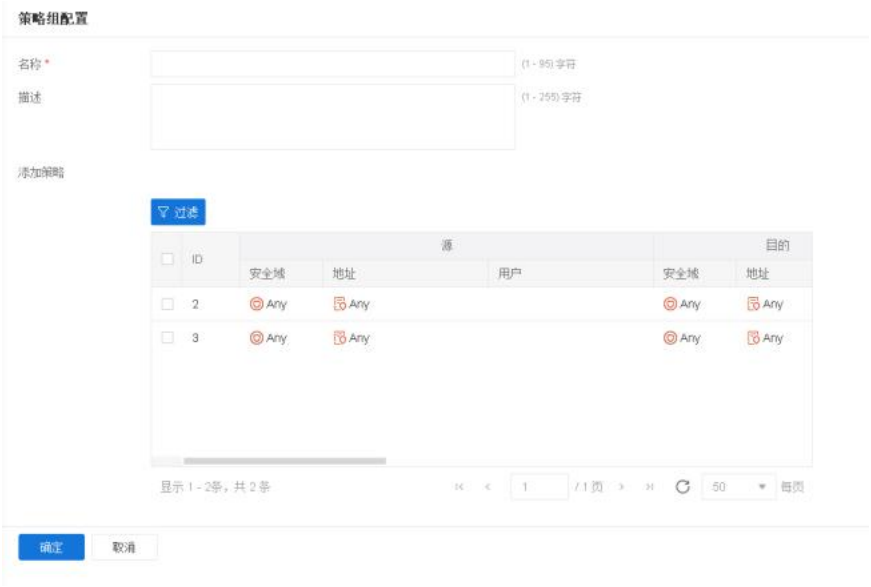
用户可以将一些策略规则组织到一起组成策略组。用户可以直接对策略组进行配置，以简化管理。

配置策略组，包括新建策略组、删除策略组、启用/禁用策略组、添加/删除策略规则成员、编辑策略组和显示禁用策略组。

新建策略组

新建策略组，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 策略组”。
2. 点击“新建策略组”按钮，打开<策略组配置>页面。



在<策略组配置>页面，填写策略组基本配置信息。

选项	说明
名称	指定策略组名称。范围是 1 到 95 个字符。
描述	指定策略组的描述信息。范围是 1 到 255 字符。
添加策略	在策略列表中，勾选策略规则复选框，为策略组添加策略规则成员。

3. 点击“确定”完成配置。

删除策略组

删除策略组，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 策略组”。
2. 勾选需要删除的策略组复选框，点击“删除策略组”按钮。

启用/禁用策略组

默认情况下，配置好的策略组会在系统中立即生效。用户可以通过配置禁用某个策略组。

启用/禁用策略组，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 策略组”。
2. 从策略组列表中选中启用/禁用的策略组对应的复选框，然后点击列表“状态”栏的“启用”按钮。启用状态显示为  ，禁用状态显示为  。

添加/删除策略规则成员

为策略组添加策略规则成员，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 策略组”。
2. 在策略组列表中点击策略组条目前的“+”，展开该策略组的成员列表。
3. 点击“添加成员”按钮，打开<策略组-添加成员>页面，该对话框显示未添加到策略组的策略规则成员列表。
4. 勾选策略规则复选框，为该策略组添加策略规则成员。
5. 点击“确定”按钮，保存配置。

> 注意: 一条策略规则只能添加到一个策略组中。

为策略组删除策略规则成员，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 策略组”。
2. 在策略组列表中点击策略组条目前的“+”，展开该策略组的成员列表。
3. 勾选需要删除的策略规则成员复选框，点击“删除成员”按钮。

编辑策略组

修改策略组名称或者描述信息，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 策略组”。
2. 从策略组列表中选中编辑的策略组对应的复选框，然后点击“编辑”按钮。
3. 在打开的<策略组配置>页面中，修改策略组名称或者描述信息。

显示禁用策略组

为了更清晰的显示禁用的策略组，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 策略组”。
2. 勾选列表上方“显示禁用策略组”复选框。禁用的策略组将显示在策略组列表中，否则策略组列表仅显示启用的策略组。

微型策略

微型策略（mini policy）是一种仅使用源/目的地址、协议、目的端口、源/目的安全域作为流量的过滤条件、允许（Permit）或拒绝（Deny）作为处理行为的精简化的策略规则。同时，系统支持配置大规模数量的微型策略，因此，可满足更多的策略存储需求。

不同设备平台支持的最大微型策略规则数不同，请以实际设备限制（Capacity）为准。

> 注意:
>
> 微型策略不支持调整优先级。
>
> 策略的匹配优先级为：微型策略>策略规则>策略规则默认动作，即系统的流量会优先匹配微型策略，再匹配策略规则，当为未匹配到任何已配置的微型策略或策略规则时，将会按照指定的策略规则默认动作对流量进行处理。

配置微型策略

微型策略配置包括：

新建微型策略

删除微型策略

编辑微型策略

启用/禁用微型策略

新建微型策略

新建微型策略，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 微型策略”。
2. 点击“新建”，打开<微型策略配置>页面。

在<微型策略配置>页面，填写微型策略基本配置信息。

选项	说明
类型	指定 IP 的地址类型，可选择 IPv4 或 IPv6。类型指定仅当该版本支持 IPv6 时可配；选择后，系统仅支持配置 IPv6 格式的 IPv6/前缀长度、IP 地址范围或 IP 地址条目。
源安全域	指定微型策略的源安全域。点击下拉菜单，选择已创建的安全域，可点击 ⊕ 按钮创建新的安全域。如不指定，则默认为“Any”。
源地址（必填项）	指定微型策略的源地址。在文本框中输入源地址，可指定为 IPv4 地址或 IPv6 地址。
目的安全域	指定微型策略的目的安全域。点击下拉菜单，选择已创建的安全域，可点击 ⊕ 按钮创建新的安全域。如不指定，则默认为“Any”。
目的地址（必填项）	指定微型策略的目的地址。在文本框中输入目的地址，可指定为 IPv4 地址或 IPv6 地址。

选项	说明
协议类型（必填项）	在“协议类型”下拉菜单中选择协议类型。
目的端口	当协议类型指定为 TCP、 UDP 时，则必须指定目的端口号，取值范围是 1-65535，其他协议类型时则不支持配置。
动作（必填项）	指定对匹配微型策略的流量所采取的行为，包括： 允许： 允许流量通过。选择“允许”。 拒绝：拒绝流量通过。选择“拒绝”。
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，可多选： 策略拒绝：勾选“策略拒绝”复选框，开启记录会话拒绝日志信息。 会话开始：勾选“会话开始”复选框，开启记录会话建立日志信息。 会话结束：勾选“会话结束”复选框，开启记录会话结束日志信息。
描述	指定微型策略的描述信息。长度为 0-31 个字符。

3. 点击“确定”完成配置。

删除微型策略

删除微型策略，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 微型策略”。
2. 勾选需要删除的微型策略复选框，点击“删除”按钮。

编辑微型策略

修改微型策略配置信息，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 微型策略”。
2. 从微型策略列表中选中编辑的微型策略对应的复选框，然后点击“编辑”按钮。
3. 在打开的<微型策略配置>页面中，修改微型策略配置信息。

> 注意: 微型策略地址类型不可进行修改。

启用/禁用微型策略

默认情况下，配置好的微型策略会在系统中立即生效。管理员可以通过配置禁用某个微型策略，使其不对流量进行控制。

启用/禁用微型策略，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 微型策略”。
2. 选中列表中需要启用/禁用的微型策略对应的复选框。
3. 点击⋮按钮，选择“启用”或“禁用”按钮。

微型策略禁用后，不再显示列表中。查看禁用的微型策略，在“⋮”下拉菜单中选择“显示禁用微型策略”。

查看及过滤策略规则/策略组/微型策略

用户可在策略规则/策略组/微型策略列表中查看及过滤策略规则/策略组/微型策略的信息。

查看策略规则/策略组/微型策略

策略规则页面显示如下：

每一列显示对应的配置。

点击“会话详情”一列的按钮，打开<会话详情>页面。在该页面，用户可查看当前策略的会话状态，用户还可以点击过滤按钮添加过滤条件并搜索符合过滤条件的会话状态信息。

将鼠标悬停在不同列的配置上时，根据配置类型不同，出现⋮图标，或直接显示配置信息。

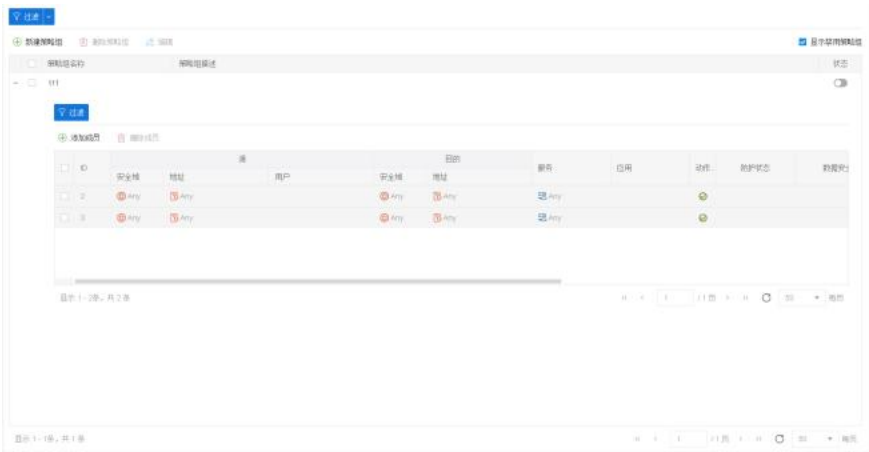
直接显示配置信息时，可进行查看。

出现⋮图标时，点击此图标后，根据配置类型的不同，可出现“详情”或“添加过滤条件”。

点击“详情”，查看配置的详细信息。然后在详情页面点击“条目详情”可以查看地址/服务条目详情。

点击“添加过滤条件”，系统在列表上方添加相应行与列的过滤条件，且根据过滤条件进行规则过滤。

策略组页面显示如下：



每一列显示对应的配置。

在列表“状态”栏中，用户可查看当前策略组的状态，启用状态显示为，禁用状态显示为。

微型策略页面显示如下：

每一列显示对应的配置。

“ID”列显示系统为微型策略自动分配的 ID。规则 ID 在整个系统中必须是唯一的。

过滤策略规则/策略组/微型策略

用户可使用过滤器搜索符合过滤条件的策略规则/策略组/微型策略。

1. 点击“策略 > 安全策略 > 策略”、“策略 > 安全策略 > 策略组”或“策略 > 安全策略 > 微型策略”。
2. 在策略规则/策略组/微型策略页面左上方点击 过滤 按钮，然后从下拉菜单中选择一个过滤条件，并输入值。
3. 输入完成后，按回车键即可搜索符合过滤条件的策略规则/策略组/微型策略。
4. 重复以上两步添加更多过滤条件。各个过滤条件之间的关系为“与”。
5. 如需删除某个过滤条件，可将鼠标悬浮在此过滤条件上，然后点击过滤条件上的叉图标。如需删除所有过滤条件，可在此状态栏的尾端点击叉图标。

用户可保存已搜索的过滤条件：

1. 添加过滤条件后，点击 过滤 后的 按钮，在下拉菜单中点击 保存过滤条件 按钮。
2. 指定要保存的过滤条件名称，每个过滤条件名称最长为 32 个英文字符，且名称仅支持中英文字符和下划线组成。
3. 点击文本框右侧“保存”按钮。
4. 如需使用已保存的过滤条件，双击过滤条件名称。
5. 如需删除已保存的过滤条件，点击过滤条件右侧 × 按钮。

注意:

根据需要最多可以保存 20 个过滤条件。

设备升级后，已保存的过滤条件将会被清除。

配置策略优化

当设备上有大量的策略规则堆积，不能确定是否需要删除，增加了用户的维护难度。系统支持策略优化功能，包括策略命中分析、冗余检测以及策略助手。

策略命中分析

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，并对策略首次命中时间、最后一次命中时间及最近未命中天数（最近一次命中时间距离现在的天数）进行统计，帮助用户识别长期未被命中的策略规则。用户可以通过设置过滤条件，查看符合过滤条件的策略规则的命中情况。

查看策略规则的命中情况，按照以下步骤进行操作：

1. 选择“策略 > 安全策略 > 策略优化”，然后选择<策略命中分析>标签页。
2. 从 过滤 下拉菜单中选择需要添加的过滤条件，并指定过滤条件内容。

过滤条件说明如下。

选项	说明
首次命中距现在天数大于	显示首次命中时间距现在天数大于指定天数的策略规则。
最近未命中天数大于	显示最近一次命中时间距现在天数大于指定天数的策略规则。
创建距现在天数大于	显示创建时间距现在天数大于指定天数的策略规则。

3. 点击回车键或点击页面任意空白处，查看最新的命中分析结果。

4. 点击“导出”按钮，将符合过滤条件的策略规则的命中情况分析结果以 CSV 格式导出。

5. 点击策略 ID 前的 + 按钮，查看策略规则的详情。

6. 点击 过滤 右侧的 ⋮ 按钮，可以保存当前选中的过滤条件。点击“保存过滤条件”， 在文本框中为当前组合过滤条件指定名称，点击“保存”。保存后，该组合过滤条件可以直接从 过滤 下拉列表中进行选择。

7. 如需删除某个过滤条件， 可将鼠标悬浮在此过滤条件上，然后点击过滤条件上的×图标。如需删除所有过滤条件，可在此状态栏的尾端点击 ×清空 图标。

清除策略规则命中数统计信息，按照以下步骤进行操作：

1. 选择“策略 > 安全策略 > 策略优化”，然后选择<策略命中分析>标签页。

2. 点击“统计清零”，打开<统计清零>页面。

选项说明如下。

选项	说明
所有策略	清除所有规则的命中数统计信息。
默认策略	清除策略规则的默认动作命中数统计信息。
策略 ID	清除指定策略 ID 的命中数统计信息。在文本框中输入策略规则的 ID。
名称	清除指定策略名称的命中数统计信息。在文本框中输入策略规则的名称。

3. 点击“确定”，完成配置。

用户还可执行如下操作：

点击策略规则后的 按钮，删除该策略规则。

点击策略规则后的 按钮，禁用该策略规则。

规则冗余检测

为保证策略中规则的有效性，系统可对规则进行冗余检测，即检查规则的覆盖情况，帮助用户排除由于规则覆盖导致的匹配问题。检测完成后，无用策略规则会被显示在策略列表中。

进行规则冗余检测，请按照以下步骤进行操作：

1. 点击“策略 > 安全策略 > 策略优化”，然后选择<冗余检测>标签页。
2. 点击“冗余检测”按钮。系统开始检测，可能会消耗较长时间，请耐心等待。完成后，无用的策略规则将被显示在策略列表中。用户可在“覆盖此策略的策略 ID”一列查看被覆盖的策略规则的 ID。

> 注意: 当规则冗余检测开始后，策略列表左下方将显示检测状态条。检测期间，不建议配置或编辑策略规则。用户可根据需求，点击 ✖ 手动停止检测。点击后，系统将弹出提示框确认是否终止规则冗余检测，点击“确定”停止检测。

配置策略助手

为了辅助管理员更快速、更准确和更完整的配置安全策略，系统提供策略助手功能。策略助手能够提取命中指定策略 ID 的流量作为流量数据分析源，根据管理员设置的替换规则、聚合规则优化流量数据，根据需要对流量数据的源 IP 或目的 IP 生成地址簿以及对流量数据的服务生成服务簿，最后自动生成符合管理员期望的安全策略规则。

点击“策略>安全策略 > 策略优化”，然后选择“策略助手”标签页，在“策略助手”页面中，根据策略助手的配置向导，逐步完成策略助手的以下配置：

流量展示 ->替换 ->聚合 ->地址簿生成 ->服务簿生成-> 策略生成

开启策略助手功能

在配置策略助手之前，需要先在指定策略配置中开启策略助手功能，请按照以下步骤进行操作：

1. 选择“策略 > 安全策略 > 策略”。
2. 选中需要开启策略助手功能的策略规则复选框，点击“编辑”按钮，打开<策略配置>页面。或者点击“新建”按钮，创建新的策略规则。

3. 点击“选项”，展开配置选项，点击策略助手后的“启用”按钮开启策略助手功能。

流量展示

流量展示页面中，以源安全域、源 IP、目的安全域、目的 IP、服务类型、应用类型的形式展示命中指定策略 ID 的所有流量数据。

配置流量展示，请按照以下步骤进行操作：

1. 点击“策略>安全策略 > 策略优化”，然后选择<策略助手>标签页。
2. 在<策略助手>页面上方的配置向导中，点击“流量展示”。

在<流量展示>页面，配置如下信息。

选项	说明
流量获取	在“策略 ID”下拉菜单中选择已经开启策略助手功能的策略规则 ID，点击“获取”按钮，命中该策略 ID 的流量数据将会被显示在下方的流量列表中。 **说明：** 流量数据列表最多支持显示 1000 条流量数据。 如果修改策略、关闭策略助手或重启设备，之前获取的命中该策略的流量会被清空。

选项	说明
流量筛选	根据源 IP、目的 IP 和协议设置过滤条件，对获取到的流量数据进行筛选过滤。
隐藏说明/显示说明	点击右上角“隐藏说明”或“显示说明”按钮，可以查看/隐藏策略助手功能的步骤说明。
统计清零	点击“统计清零”，清空列表中已获取到的所有流量数据。 **注意**：请确保已获取的流量数据已经分析完成后再进行“统计清零”操作。

3. 点击“下一步”按钮，进入到下一配置步骤。

替换

在替换页面中，可以指定源 IP、目的 IP、服务的范围作为策略替换条件，对策略条目的对应项进行进一步替换，当列表中策略规则条目的对应项满足指定的替换条件，那么将会被替换条件的内容替换，从而能够生成更精确的策略规则。

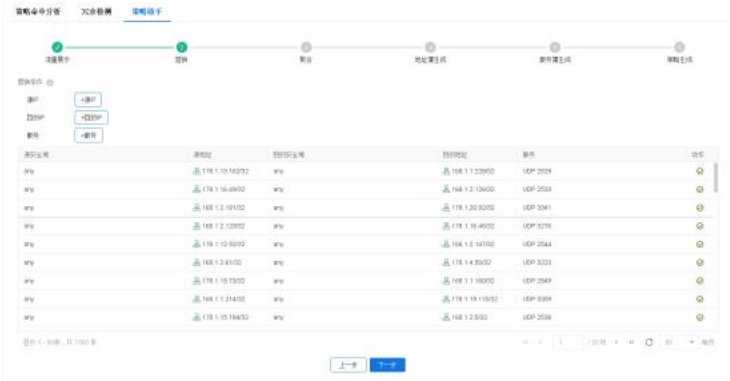
应用场景举例

例如：当管理员获取某一源 IP 为 172.16.1.10 访问正常服务的流量数据，在分析该数据流量后，确认该源 IP 为正常访问源，同时也分析出所有在 172.16.1.0/24 网段内的所有源 IP 都应该作为正常访问源。为了满足上述需求，可使用“策略替换”步骤配置策略替换条件，将策略规则条目的源 IP 在 172.16.1.0/24 范围内的源 IP 地址全部替换为 172.16.1.0/24，在最终生成策略规则后以实现该网段内所有源 IP 成为正常访问源。

配置策略替换条件

配置替换条件，请按照以下步骤进行操作：

1. 在“策略助手”页面上方的配置向导中，点击“替换”。



在“替换”页面，配置如下信息。

选项	说明
源 IP	添加源 IP 替换条件。如需要，可添加多个源 IP 替换条件，系统最多允许添加 3 个源 IP 替换条件。 1. 点击“+源 IP”按钮。 2. 在下拉菜单中选择地址类型“IP/掩码”或“IP 范围”，然后在右侧的文本框输入相应的配置。
目的 IP	添加目的 IP 替换条件。如需要，可添加多个目的 IP 替换条件，最多允许添加 3 个目的 IP 替换条件。 1. 点击“+目的 IP”按钮。 2. 在下拉菜单中选择地址类型“IP/掩码”或“IP 范围”，然后在右侧的文本框输入相应的配置。
服务	添加服务替换条件。如需要，可添加多个服务替换条件，最多允许添加 3 个服务替换条件。 1. 点击“+服务”按钮。 2. 在下拉菜单中选择服务协议类型，然后在右侧的文本框输入相应的协议端口号范围配置。

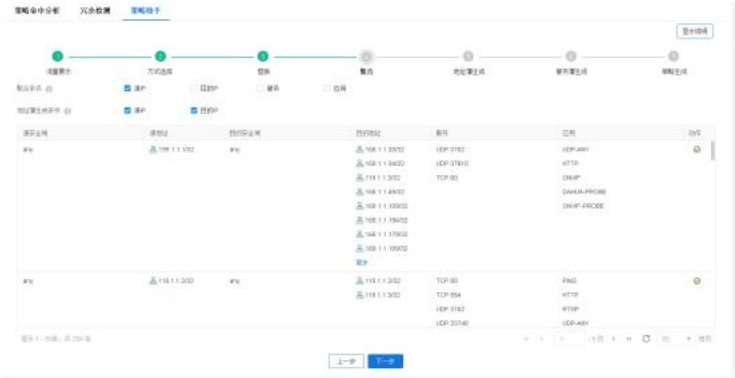
2. 点击“下一步”按钮，进入到下一配置步骤。

聚合

聚合是指将符合聚合条件（源 IP 相同、目的 IP 相同、服务相同）的策略规则条目聚合成为一条策略规则，从而减少策略规则的数量。

配置聚合条件，请按照以下步骤进行操作：

1. 在“策略助手”页面上方的配置向导中，点击“聚合”。



2. 勾选指定的聚合条件（源 IP、目的 IP 或服务），开启聚合功能，列表中的策略规则条目将会按照条件聚合展示。

3. 勾选地址簿生成条件（源 IP、目的 IP），开启生成地址簿功能，并且在“地址簿生成”步骤中将会按照指定生成条件列出对应的地址簿条目。默认情况下，勾选所有地址簿生成条件。若未勾选，关闭生成地址簿功能，配置向导中将不包含“地址簿生成”步骤页面，最终将会根据 IP 地址生成策略。

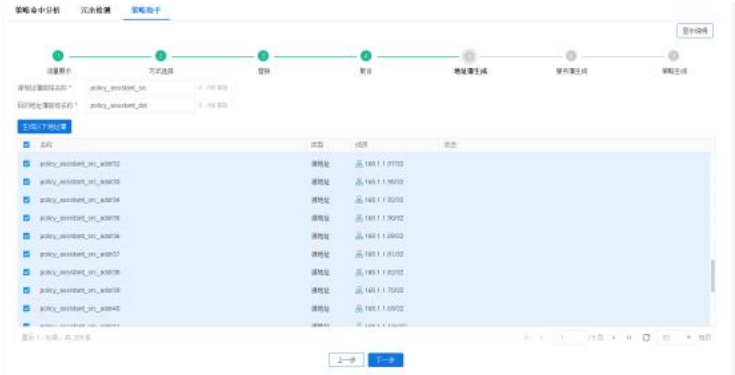
4. 点击“下一步”按钮，进入到下一配置步骤。

地址簿生成

设备获取到的命中指定策略 ID 的流量数据中，能够展示出策略配置中的源 IP 和目的 IP。经过替换和聚合步骤优化之后，如果用户在“聚合”页面中已指定地址簿生成条件，地址簿生成页面列表中展示了根据生成条件可生成的地址簿条目，用户可以根据需求，指定生成对应的地址簿并加入到系统地址簿中。
若不生成地址簿，则直接点击“下一步”按钮，进入下一个步骤。

生成地址簿，请按照以下步骤进行操作：

1. 在“策略助手”页面上方的配置向导中，点击“地址簿生成”。



2. 在文本框中输入生成的源地址簿前缀名称，范围是 1 到 80 个字符，默认前缀名称为“policy_assistant_src”。当指定源地址簿前缀名称后，下方列表中源地址簿名称将会按照“指定的源地址簿前缀名称_addr+序号”的命名方式进行修改。

3. 在文本框中输入生成的目的地址簿前缀名称，范围是 1 到 80 个字符，默认前缀名称为“policy_assistant_dst”。当指定目的地址簿前缀名称后，下方列表中目的地址簿名称将会按照“指定的目的地址簿前缀名称_addr+序号”的命名方式进行修改。

4. 在列表中勾选需要生成地址簿的条目，点击“地址簿生成”按钮，即可生成对应的地址簿（可点击“对象>地址簿”进行查看）。生成地址簿后，在该列表“状态”栏中将显示“已生成”；若生成失败，则在该列表“状态”栏中将显示“生成失败+错误信息”。

5. 点击“下一步”按钮，进入到下一配置步骤。

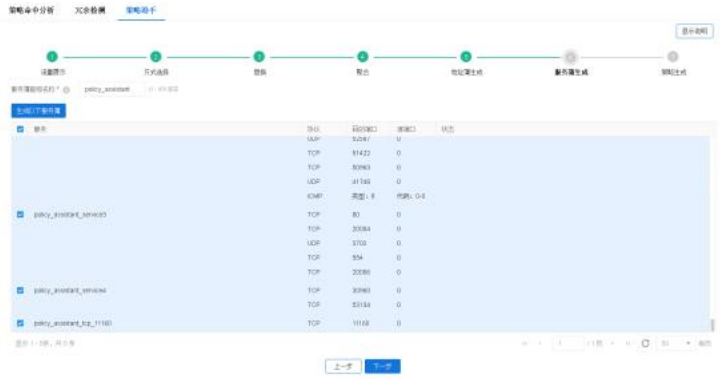
服务簿生成

设备获取到的命中指定策略 ID 的流量数据中，能够展示出策略配置中服务的协议以及端口号信息。经过替换、聚合、地址簿生成步骤优化之后，服务簿生成页面中展示了根据服务协议和端口号信息可以生成的

服务簿条目，用户可以根据需求，指定生成对应的服务簿并加入到系统服务簿中。
若不生成服务簿，则直接点击“下一步”按钮，进入下一个步骤。

生成服务，请按照以下步骤进行操作：

1. 在“策略助手”页面上方的配置向导中，点击“服务簿生成”。



2. 在文本框中输入生成的服务簿前缀名称，范围是 1 到 95 个字符，默认前缀名称为“policy_assistant”。当指定服务簿前缀名称后，下方列表中服务簿名称将会按照“指定的服务簿前缀名称+协议配置”的方式进行修改。

3. 在列表中勾选需要生成服务簿的条目，点击“服务簿生成”按钮，即可生成对应的服务簿（可点击“对象>服务簿>服务”进行查看）。生成服务簿后，在该列表“状态”栏中将显示“已生成”；若生成失败，则在该列表“状态”栏中将显示“生成失败+错误信息”。

4. 点击“下一步”按钮，进入到下一配置步骤。

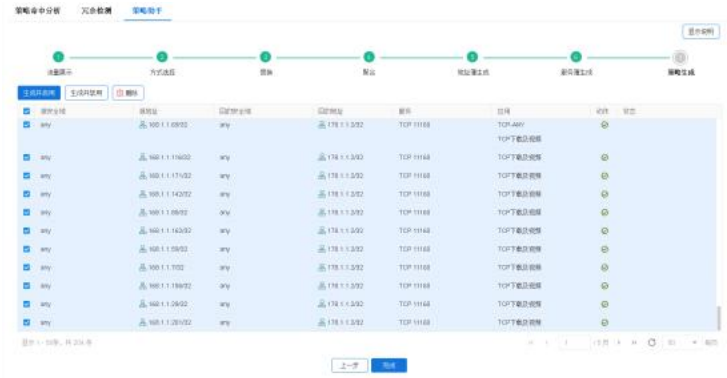
策略生成

策略生成页面列表中展示已经过替换、聚合、地址簿生成及服务簿生成步骤优化之后的所有策略规则。根据需要，在该页面选择符合要求的策略规则条目生成新的策略规则，并添加到安全策略页面中。

说明：对于生成的安全策略，源 IP、目的 IP 和服务取决于配置的策略聚合条件；源安全域、目的安全域和动作继承自原有的策略规则。

生成策略规则，请按照以下步骤进行操作：

1. 在“策略助手”页面上方的配置向导中，点击“策略生成”。



在“策略生成”页面，配置如下信息。

选项	说明
生成并启用	根据需求勾选列表中策略条目的复选框，点击“生成并启用”按钮，该安全策略规则会被启用并添加到安全策略页面中，且位于原有的安全策略规则之前。
生成并禁用	根据需求勾选列表中策略条目的复选框，点击“生成并禁用”按钮，该安全策略规则会被禁用并添加到安全策略页面中，且位于原有的安全策略规则之前。
删除	根据需求勾选列表中策略条目的复选框，点击“删除”按钮，对列表中该策略规则条目进行删除。

2. 点击“完成”按钮，完成策略助手的所有配置。

用户上线通知

系统提供基于策略的用户上线通知功能。用户上线通知功能结合 Web 认证和 Web Redirect 功能。

配置该功能后，当客户端发送 HTTP 网页访问请求后，页面会首先跳转到提示页面（如下图所示），点击该页面上的“继续浏览网页”按钮，系统会将网页重定向到通知页面。用户若想访问第一次输入的 URL 地址，需要重新在 Web 浏览器中输入该地址。

在启用用户上线功能前，需要配置 Web 认证功能。配置 Web 认证功能，参阅 Web 认证部分内容。

配置用户上线通知功能

配置用户上线通知功能，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. 根据用户策略配置，选择需要启用用户上线通知功能的策略。一般情况下，选择 Web 认证策略下面的且对上网流量（服务类型为 HTTP）进行放行动作的策略配置用户上线通知功能。
3. 点击“编辑”按钮对选择的策略进行编辑。
4. 在<策略配置>页面，选择“启用 Web 重定向”后的“启用”按钮。
5. 在“通知页面网址”文本框中的填写通知页面的 URL。
6. 点击“确定”按钮保存所做配置。

配置用户上线通知功能参数

用户上线通知功能参数包括：

空闲时间：指网络在无流量状态下保持连接状态的最长时间。超出空闲时间后，如果用户再次打开浏览器请求浏览网页，网页将会重新定向到指定的通知页面。

上线通知页面背景：用户可以自定义转到通知页面前的提示页面的背景图片。

配置用户上线通知功能参数，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 ⋮ 按钮，并在弹出菜单中选择“Web Redirect 页面配置”，打开<Web Redirect 页面配置>页面。
3. 在“空闲时间”文本框输入空闲时间。默认是 30 分钟，范围是 0 到 1440 分钟。
4. 更换提示页面的图片。点击“浏览”按钮，选中新图片，然后点击“上传”。背景图片要求如下：文件需压缩成 ZIP 文件后上传；名称必须为 logo.jpg；图片大小应小于 100KB，建议为 120 像素*40 像素。

查看上线通知用户

配置用户上线通知功能后，用户可以通过上线通知用户页面查看相关信息。

1. 点击“策略 > 安全策略”，进入安全策略页面。
2. 点击 ⋮ 按钮，并在弹出菜单中选择“Web Redirect IP 列表”，打开<Web Redirect IP 列表>页面。该页面显示上线通知用户的相关信息，如下：

   IP 地址：显示上线用户的 IP 地址。

   会话数：显示上线用户的会话数。

   接口：显示上线用户的源接口。

   存活时间：显示上线用户的在线时长。

   过期时间：显示上线用户的空闲时间。

iQoS

系统提供 iQoS（智能流量管理）功能，能够管理和优化网络带宽，提高用户的网络体验和带宽资源利用率。

iQoS 为特定流量提供更高优先服务的同时控制抖动和延迟的能力，并且能够降低数据传输丢包率。当网络过载或拥塞时，系统能够确保重要业务流量的正常传输。iQoS 功能受许可证控制，安装许可证后，iQoS 功能才可使用。

实现机制

数据包进入系统后，首先会被分类和标记。对于分类标记后的流量，系统会通过整形机制使流量平滑的转发或管制机制丢弃。若选择整形机制转发流量，系统则会通过拥塞管理机制和拥塞避免机制对数据包进行管理，为数据包排列优先次序并且在发生拥塞时保证高优先级数据包优先调度。

通常来讲，实现流量管理的工具包括：

分类和标记工具：分类和标记的过程就是识别出需进行不同处理（优先或者区分）的流量的过程。分类和标记是执行 iQoS 的第一步。

管制和整形工具：识别流量违约并做出响应。管制和整形使用同样的算法识别流量违约，但是做出的响应不同。管制工具对流量违约进行即时检查，发现违约后立即采取设定的动作进行处理。整形工具是一个与排队机制一起工作的流量平滑工具，整形的目的是控制流量永远不超出指定的速率，使流量平滑地转发。

拥塞管理工具：即排队工具，应用在产生拥塞处。由于网络之间的速率不匹配，在广域网或者局域网中都有可能出现拥塞。只有当发生拥塞时，排队工具才会被启用。

拥塞避免工具：拥塞避免工具是排队算法的补充，它的目的是为了处理基于 TCP 的数据流。

管道与流控层级

系统支持两层流控，即第一层流控和第二层流控。在每层流控中，流量的具体控制通过管道来实现。

管道

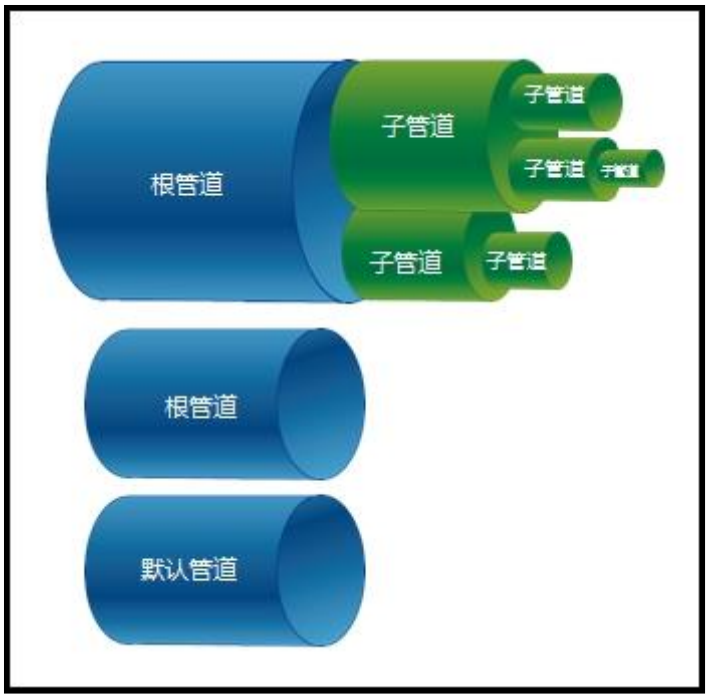
设备通过配置管道来实现 iQoS。管道，即带宽通道，是一个虚拟概念。系统以管道为单位对流量进行划分，并根据管道配置的流控动作对管道内的流量进行管控。所有流经设备的流量，都将按照设置的匹配条件进入虚拟管道。未匹配到的流量将进入系统预定义的默认管道。

管道（除默认管道）必须包含两部分，分别是流量匹配条件和流量管理动作。

流量匹配条件：定义设备需要匹配的流量，从而设备可以将流量进行区分。流经设备的流量会根据用户设置的条件分类，划入对应的管道。系统为匹配到匹配条件的流量提供带宽控制。一个管道可以有多个流量匹配条件，各个匹配条件之间为“或”的关系。流量只要匹配到其中一个匹配条件，就会进入该管道。

流量管理动作：对已被划分到管道中的流量所做的动作。流控分为正向控制和反向控制。正向控制即对从源到目的方向的流量进行控制；反向控制即对从目的到源方向的流量进行控制。

为了给用户提供灵活和方便的配置，系统支持多级管道。配置多级管道，可将不同用户的不同应用分别限制在一定带宽之内，从而能优先保障重要用户或重要应用的带宽。管道最多支持四级嵌套，默认管道不可嵌套子管道。管道逻辑关系如下图所示：



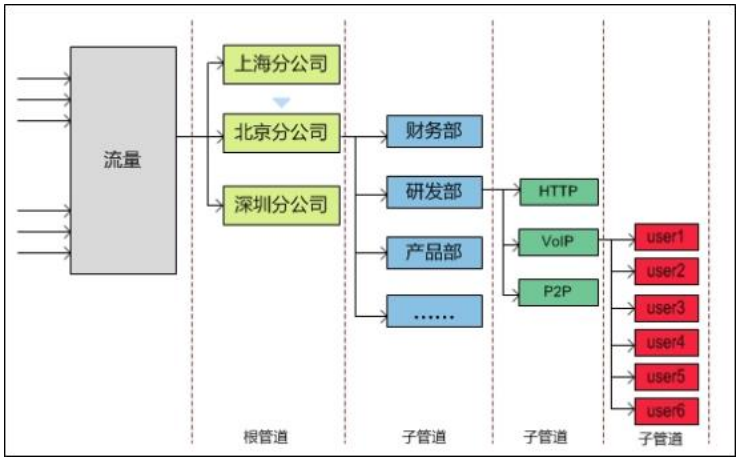
用户可创建多个根管道，各个根管道之间是彼此独立的。每个根管道下均可嵌套三级子管道。

子管道的最小带宽之和不能大于其上一级管道的最小带宽，最大带宽也不能大于其上一级管道的最大带宽

用户若在根管道上配置了正向或反向的流量管理动作后，该根管道下的所有子管道都必须继承根管道设定的流量方向。

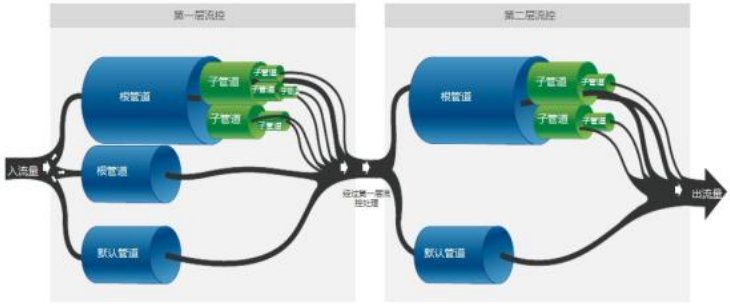
仅配置了反向流量管理动作的管道不可用。

以某企业的应用场景为例说明如何嵌套多级管道。如下图所示，管理员可创建一个根管道，限制该企业北京分公司的流量。创建一个子管道，限制其研发部门的流量。再创建子管道对研发部应用进行划分，限制不同应用拥有不同的带宽。最后为某种应用的每用户设置子管道，限制该应用的每位用户的流量。



流控层级

系统支持两层流控，即第一层流控和第二层流控。在每层流控中，流量的具体控制通过管道来实现。经过第一层流控处理过的流量进入第二层流控，系统再根据第二层流控的管道设置对流量进行进一步管控。流量进入设备后，iQoS 处理流程如下图所示：



根据上图所示，系统的流控处理流程描述如下：

1. 流量首先进入第一层流控，系统根据第一层流控中管道的匹配条件设置划分流量到不同的管道中。不匹配任何管道的流量进入默认管道。如果存在相同匹配条件的根管道，流量优先匹配位置靠前的根管道。流量进入根管道后，再根据子管道的匹配条件逐层匹配。
2. 系统根据管道配置的流控动作对匹配到的流量进行管控。
3. 经过第一层流控处理的流量进入第二层流控进行再次管控。系统在第二层流控中的管道匹配以及流量管控原理与第一层流控相同。
4. 流控处理结束。

开启 iQoS

开启 iQoS：

1. 选择“策略 > iQoS > 配置”。
2. 点击“开启 iQoS”后的“启用”按钮，出现以下界面。

3. 点击“开启阈值告警”后的“启用”按钮，并在“告警阈值”文本框中指定管道使用率的告警阈值。取值范围为 50-100。默认值为 80。在开启该功能并指定告警阈值后，当管道使用率达到或超过指定的告警阈值时，系统会记录警告级别的事件日志。对于同一个管道，系统记录事件日志的时间间隔为 10 秒钟，即每 10 秒记录一次事件日志。

4. 如果用户在“第一层流控”或“第二层流控”点击了“启用 NAT IP 匹配”后的“启用”按钮，系统将使用源 NAT 后和目的 NAT 前的 IP 地址作为匹配项。如果匹配成功，系统将会对这些 IP 地址进行限速。

> 注意: 在启用 NAT IP 匹配功能之前，必须配置 NAT 规则。否则，该配置不生效。

5. 点击“应用”，保存配置。

管道

系统通过管道来实现 iQoS，进而管理和优化网络带宽。管道可属于不同的流控层级，不同流控层级的管道在各自阶段对流量进行管理。

配置管道，包括：

1. 创建流量匹配条件，系统对匹配到匹配条件的流量进行控制。若为管道配置多个匹配条件，各匹配条件之间为“或”的关系。
2. 根据需求创建流量白名单。目前仅根管道和默认管道支持配置白名单。配置后，系统将不对白名单中指定的流量做 iQoS。
3. 指定流量管理动作，即对已被划分到管道中的流量指定动作。
4. 指定时间表，管道将在指定的时间周期内生效。

基本操作

选择“策略 > iQoS > 策略”打开策略页面。

在此页面，可以实现以下操作：

禁用二层流控：点击“禁用二级流控”将禁用第二层流控。被禁用的第二层流控及其管道将不参与 iQoS。页面将不显示“第二层流控”标签页。

查看管道配置：在管道列表中可查看管道的名称、模式、流控动作、时间表、匹配条件、白名单、子管道以及描述。

 表示根管道为可用状态，  表示根管道为不可用状态，  表示子管道为可用状态，  表示子管道为不可用状态。  灰色名称表示管道为禁用状态。

新建根管道：选中“第一层流控”或“第二层流控”标签页，然后点击“新建”，在打开的页面内创建根管道。

新建子管道：点击根管道或子管道的  图标，在打开的页面内创建相应的子管道。

编辑管道：点击“编辑”按钮，编辑所选的管道。

启用管道：点击“启用”按钮，启用所选的管道。管道创建后将被系统默认启用。

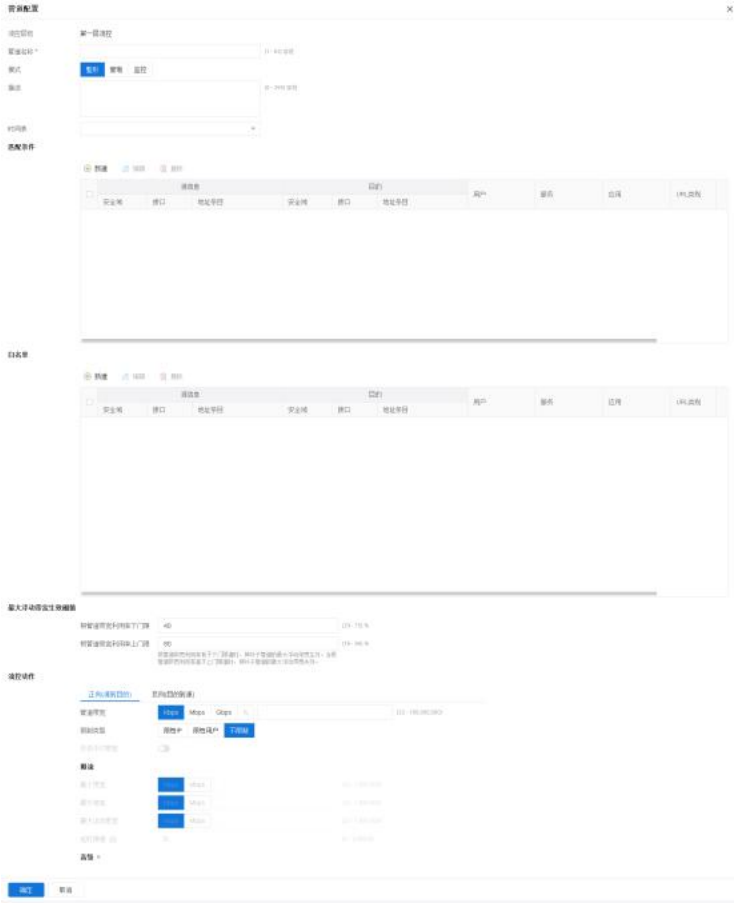
禁用管道：点击“禁用”按钮，禁用所选的管道。管道被禁用后，将不参与流控处理。

删除管道：点击“删除”按钮，删除所选的管道。默认管道无法删除。

配置管道

按照以下步骤配置管道：

1. 根据基本配置中介绍的根管道及子管道的创建方法，创建一个管道，打开<管道配置>页面。



2. **在该页面，填写管道的基础信息。**

选项	说明
父管道/流控层级	显示该管道所属的流控层级名称或父管道名称。
管道名称	输入将要创建的管道的名称。长度为 1-63 个字符。
模式	整形，管制，或监控： 整形模式能够限制数据传输速率，使流量平滑地转发。根

选项	说明
	管道范围内流量将支持带宽借用和优先级调度。 管制模式对超出带宽限制的流量进行丢弃。该模式不支持带宽借用和优先级调度，且不做最小带宽保障。 监控模式仅对匹配到的流量进行监控和统计，不对流量进行任何控制。 带宽借用：同一根管道内的所有子管道，在确保自身管道流量正常转发的情况下，可将空闲流量分配给带宽不足的管道。 优先级调度：在流量拥塞时，超出带宽限制的流量将进入等待队列，用户可设置优先级以确保某些应用优先调度。
描述	输入此管道的描述信息。长度为 0-255 个字符。
时间表	在下拉菜单中指定时间表。管道将在时间表所指定的时间周期内生效。如需新建时间表，点击  按钮。

3. **点击“匹配条件”下的“新建”按钮，打开“匹配条件配置”页面，配置匹配条件**

选项	说明
类型	指定 IP 的地址类型，可选择 IPv4 或 IPv6。IPv6 选项仅当该版本支持 IPv6 时可配；选择后，系统仅支持选择 IPv6 格式的 IP、掩码、IP 地址范围或 IP 地址条目。
源信息	
安全域	指定流量的源安全域。在下拉菜单中选中所需的流量源安全域名称。
接口	指定流量的源接口。在下拉菜单中选中所需的流量源接口名称。点击  按钮，可删除已选定的接口。
地址条目	指定流量的源地址。 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左侧列表中。 4. 添加完成后，点击“关闭”。 用户还可执行如下操作： 选择地址簿类型时，可点击  按钮创建新的地址簿。

选项	说明
	选择地址簿类型时，点击搜索框中的 按钮，可以按地址簿名称和地址成员的 IP 进行模糊搜索，名称和地址是与的关系。地址支持多种输入方式，例如：输入“地址”为 10.10.10.10/32，可能匹配到包含地址成员是 10.10.10.10/24 的地址簿；输入“地址”为段掩码 9.9.9.9/24，可能匹配到包含地址成员是 9.9.0.0/16 的地址簿；输入“地址”为 10.10.10.10，可能匹配到地址成员的 IP 范围为 10.10.10.0-10.10.10.255 的地址簿；输入“地址”为 10.23，可能匹配到包含地址成员是 1.10.23.10/24 的地址簿；输入“地址”为 aa，可能匹配到地址成员的“主机名称”为 aaa 的地址簿。 系统默认地址配置为 any。如需恢复为 any，选择 **any** 复选框。
目的信息	
安全域	指定流量的目的全域。在下拉菜单中选中所需的流量目的安全域名称。
接口	指定流量的目的接口。在下拉菜单中选中所需的流量目的接口名称。点击 × 按钮，可删除已选定的接口。
地址条目	指定流量的目的地址。 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左侧列表中。 4. 添加完成后，点击“关闭”。 用户还可执行如下操作： 选择地址簿类型时，可点击 ⊕ 按钮创建新的地址簿。 选择地址簿类型时，点击搜索框中的 按钮，可以按地址簿名称和地址成员的 IP 进行模糊搜索，名称和地址是与的关系。地址支持多种输入方式，例如：输入“地址”为 10.10.10.10/32，可能匹配到包含地址成员是 10.10.10.10/24 的地址簿；输入“地址”为段掩码 9.9.9.9/24，可能匹配到包含地址成员是

选项	说明
	9.9.0.0/16 的地址簿；输入“地址”为 10.10.10.10，可能匹配到地址成员的 IP 范围为 10.10.10.0-10.10.10.255 的地址簿；输入“地址”为 10.23，可能匹配到包含地址成员是 1.10.23.10/24 的地址簿；输入“地址”为 aa，可能匹配到地址成员的“主机名称”为 aaa 的地址簿。 系统默认地址配置为 any。如需恢复为 any，选择 **any** 复选框。
用户信息	指定流量所属的用户/用户组。 1. 在“用户信息”下拉菜单中，选择用户或用户组所在的 AAA 服务器。 2. 根据 AAA 服务器类型不同，用户可执行以下一个或多个操作：搜索指定用户/用户组/角色、展开用户/用户组列表、输入指定用户/用户组。 3. 选择指定用户/用户组/角色后，点击所选择的用户/用户组/角色将其添加到左侧列表中。 4. 添加完成后，点击“关闭”。
服务	指定流量所属的服务/服务组。 1. 在“服务”下拉菜单中选择类型：服务，服务组。 2. 用户可搜索指定服务/服务组，展开服务/服务组列表。 3. 选择指定服务/服务组后，点击所选择的对象将其添加到左侧列表中。 4. 添加完成后，点击“关闭”。 用户还可执行如下操作： 如需添加新的服务/服务组，可在“预定义”下拉菜单中选择“自定义”，然后点击 ⊕ 按钮。 系统默认服务配置为 any。如需恢复为 any，选择 **any** 复选框。
应用	指定流量所属的应用/应用组/应用过滤组。

选项	说明
	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，点击所选择的对象将其添加到左侧列表中。 3. 添加完成后，点击“关闭”。 如需新建应用组或应用过滤组，点击 ⊕ 按钮即可。
URL 类别	指定流量所属的 URL 类别。用户指定 URL 类别后，系统将按照指定类别对流量进行匹配过滤。 1. 在“URL 类别”下拉菜单中，用户可点击一个或多个 URL 类别以选择，最多选择 8 个类别。 2. 选择完成后，点击“关闭”。 如需新建 URL 类别，点击 ⊕ 按钮，打开“URL 类别”页面。在该页面内，用户可配置类别名称和 URL。 类别名称：指定 URL 类别的名称，长度取值范围为 1-31 个字符。 URL：配置 URL 地址，长度取值范围为 1-255 个字符。填写正确的 URLI 地址后，点击“添加”按钮，将配置的 URL 成员添加到下方的成员列表中。如需要，可以为 URL 类别添加多个 URL 成员。
高级	

选项	说明
TOS	输入流量对应的 ToS 字段；或点击“设置”按钮，打开<ToS 配置>页面，指定流量 IP 头部的 ToS 字段。 优先级：指定先行位。 延迟：指定最小延迟。 吞吐量：指定最大吞吐量。 可靠度：指定最高可靠性。 花费：指定最小通信成本。 保留：指定普通服务。
TrafficClass	当选择 IPv6 地址类型时，输入流量对应的 TrafficClass 字段。

4. 当配置根管道时，用户可指定白名单。白名单配置过程，参照匹配条件配置过程。

5. **配置最大浮动带宽生效阈值。**

选项	说明
根管道带宽利用率下门限	指定根管道内实际流量占最大带宽的比值的下门限。当低于该门限值时，其叶子管道的最大浮动带宽生效。下门限取值范围为 20%-75%，默认为 40%。
根管道带宽利用率上门限	指定根管道内实际流量占最大带宽的比值的上门限。当高于该门限值时，其叶子管道的最大浮动带宽失效。上门限取值范围为 76%-90%，默认为 80%。

6. **配置流控动作，对匹配流量设置控制动作。**

正向(源到目的)	
正向，即从源到目的方向流量的控制。系统将对命中匹配条件的正向流量指定流控动作。	
管道带宽	当配置根管道时，指定根管道的带宽。当配置子管道时，指定管道的最小带宽和最大带宽： 最小带宽：输入管道的最小带宽值。当配置子管道最小带宽时，选择“开启预留带宽”为此子管道预留最小带宽。此预留最小带宽不可以被借用。 最大带宽：在文本框中输入管道的最大带宽值。
限制类型	为每个 IP 或每个用户指定最小带宽或最大带宽： 类型：选择带宽限制的类型，可以是“限每 IP”或“限每用户”或“不限制”。

	“不限制”表示不为每 IP 或每用户限制带宽。 “限每 IP”表示针对每个 IP 地址进行限制。选择后，继续在**限流**配置中选择“源 IP”单选按钮指定为该管道的每个源 IP 限制最小带宽和最大带宽；或选择“目的 IP”单选按钮指定为该管道的每个目的 IP 限制最小带宽和最大带宽。 “限每用户”表示针对每个用户进行限制。选择后，继续在**限流**配置中指定为该管道的每个用户限制最小带宽和最大带宽。 当配置根管道时，可点击“开启平均带宽”后的“启用”按钮，为此根管道中的源 IP，目的 IP，或用户平均分配带宽。
限流	当限制类型为“限每用户”或者“限每 IP”时，继续指定每用户或者每 IP 的最小带宽和最大带宽。 最小带宽：在文本框中输入最小带宽值。 最大带宽：在文本框中输入最大带宽值。 最大浮动带宽：需要配置最大带宽后，才能在文本框中输入最大浮动带宽值。 延时限速：指定延时限速时间。取值范围为 1 秒到 3600 秒。指定该参数后，系统将开启延时限速功能，并且在指定的延时时间范围内，对每 IP/用户的最大带宽限制不生效。
优先级	在“高级”配置中指定管道的优先级。从下拉菜单中选中数值，范围为 0 到 7。数值越小，表示该管道的优先级越高。优先级较高的管道，系统将优先调度，并优先借用其他管道的空闲带宽。默认管道的优先级是 7。
TOS	在“高级”配置中输入流量对应的 ToS 字段；或点击“设置”按钮，打开<ToS 配置>页面，指定流量 IP 头部的 ToS 字段。 优先级：指定先行位。 延时：指定最小延迟。 吞吐量：指定最大吞吐量。 可靠度：指定最高可靠性。

	花费：指定最小通信成本。 保留：指定普通服务。
TrafficClass	在“高级”配置中输入对应的 IPv6 流量 TrafficClass 字段的数值。系统会将匹配成功的 IPv6 流量的 TrafficClass 字段值设置为该指定的数值。
对端发送抑制	在“高级”配置中开启对端发送抑制功能。默认情况下，该功能为关闭状态。对端抑制功能可根据用户分配的带宽， 使到达设备的流量尽可能与分配带宽相符，以减少设备上的丢包。开启对端抑制功能后，默认抑制强度为 1，抑制强度取值范围为 1-8。数值越大，抑制强度越大，丢包越少。注： 对端抑制功能只能在正反流控的一个方向开启。只有最末端管道支持配置对端抑制功能。
反向(目的到源)	
反向，即从目的到源方向流量的控制。系统将对命中匹配条件的反向流量指定流控动作。	
管道带宽	当配置根管道时，指定根管道的带宽。 当配置指定管道的最小带宽和最大带宽： 最小带宽：输入管道的最小带宽值。当配置子管道最小带宽时，选择“开启预留带宽”为此子管道预留最小带宽。此预留最小带宽不可以被借用。 最大带宽：在文本框中输入管道的最大带宽值。
限制类型	为每个 IP 或每个用户指定最小带宽或最大带宽： 类型：选择带宽限制的类型，可以是“限每 IP”或“限每用户”或“不限制”。 “不限制”表示不为每 IP 或每用户限制带宽。 “限每 IP”表示针对每个 IP 地址进行限制。选择后，继续在**限流**配置中选择“源 IP”单选按钮指定为该管道的每个源 IP 限制最小带宽和最大带宽；或选择“目的 IP”单选按钮指定为该管道的每个目的 IP 限制最小带宽和最大带宽。 “限每用户”表示针对每个用户进行限制。选择后，继续在**限流**配置中指定为该管道的每个用户限制最小带宽和最大带宽。 当配置根管道时，可点击“开启平均带宽”后的“启用”按钮为此根管道中的源 IP，目的 IP，或用户平均分配

	带宽。
限流	当限制类型为“限每用户”或者“限每 IP”时，继续指定每用户或者每 IP 的最小带宽和最大带宽。 最小带宽：在文本框中输入最小带宽值。 最大带宽：在文本框中输入最大带宽值。 最大浮动带宽：配置最大带宽后，在文本框中输入最大浮动带宽值。 延时限速：指定延时限速时间。取值范围为 1 秒到 3600 秒。指定该参数后，系统将开启延时限速功能，并且在指定的延时时间范围内，对每 IP/用户的最大带宽限制不生效。
优先级	在“高级”配置中指定管道的优先级。从下拉菜单中选中数值，范围为 0 到 7。数值越小，表示该管道的优先级越高。优先级较高的管道，系统将优先调度，并优先借用其他管道的空闲带宽。默认管道的优先级是 7。
ToS	在“高级”配置中输入流量对应的 ToS 字段；或点击“设置”按钮，打开<ToS 配置>页面，指定流量 IP 头部的 ToS 字段。 优先级：指定先行位。 延时：指定最小延迟。 吞吐量：指定最大吞吐量。 可靠度：指定最高可靠性。 花费：指定最小通信成本。 保留：指定普通服务。
对端发送抑制	在“高级”配置中开启对端发送抑制功能。默认情况下，该功能为关闭状态。对端抑制功能可根据用户分配的带宽， 使到达设备的流量尽可能与分配带宽相符，以减少设备上的丢包。开启对端抑制功能后，默认抑制强度为 1，抑制强度取值范围为 1-8。数值越大，抑制强度越大，丢包越少。注： 对端抑制功能只能在正反流控的一个方向开启。只有最末端管道支持配置对端抑制功能。

7. 点击“确定”按钮完成配置。

过滤 iQoS 策略

用户可使用过滤器搜索符合过滤条件的 iQoS 策略。

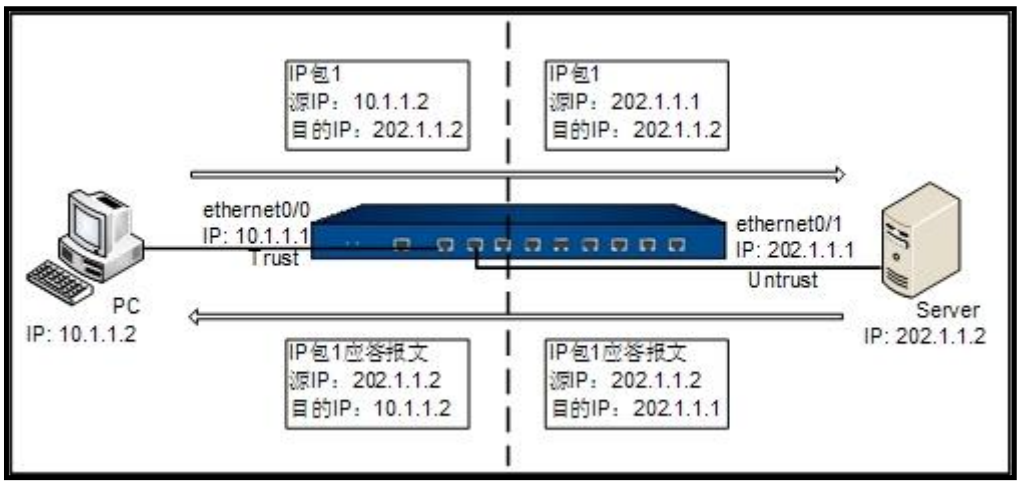
1. 点击“策略 >iQOS > 策略”，在 iQOS 策略列表页面左上方，点击 过滤 按钮。
2. 然后从下拉菜单中选择一个过滤条件，并输入对应的数值。
3. 输入完成后，按回车键即可搜索符合过滤条件的 iQOS 策略。
4. 重复以上两步添加更多过滤条件。各个过滤条件之间的关系为“与”。
5. 如需删除某个过滤条件，可将鼠标悬浮在此过滤条件上，然后点击过滤条件上的“X”图标。如需删除所有过滤条件，可在此状态栏的尾端点击“X 清空”图标。

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。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：

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

在<源 NAT 配置>页面，填写相关信息。

当 IP 地址符合以下条件时	
虚拟路由器	指定源 NAT 规则所在的虚拟路由器。
类型	指定源 NAT 规则的类型，可以为 IPv4、NAT46、NAT64 或者 IPv6。

当 IP 地址符合以下条件时	
源安全域	指定源 NAT 规则中流量入接口所属的安全域，默认为 Any。配置了源安全域之后，只有从绑定了该安全域的接口进入的流量才会继续匹配这条 SNAT 规则。 **注意：**源安全域需要属于指定的虚拟路由器。
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，用户可搜索并选定指定的地址条目。点击 ⊕ 按钮，可新建地址簿。 IP 地址： 在文本框中直接输入 IP 地址。当源 NAT 规则类型为 IPv4 或者 NAT46 时，输入 IPv4 地址；当源 NAT 规则类型为 NAT64 或者 IPv6 时，输入 IPv6 地址。 IP/掩码：在文本框中输入 IPv4 地址及掩码。当源 NAT 规则类型为 IPv4 或者 NAT46 时，可以配置该选项。 IPv6/前缀长度：在文本框中输入 IPv6 地址及前缀长度。当源 NAT 规则类型为 NAT64 或者 IPv6 时，可以配置该选项。
目的安全域	指定源 NAT 规则中流量出接口所属的安全域，默认为 Any。配置了目的安全域之后，只有从绑定了该安全域的接口出去的流量才会继续匹配这条 SNAT 规则。 **注意：**目的安全域需要属于指定的虚拟路由器。
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，用户可搜索并选定指定的地址条目。点击 ⊕ 按钮，可新建地址簿。 IP 地址：在文本框中直接输入 IP 地址。当源 NAT 规则类型为 IPv4 或者 NAT46 时，输入 IPv4 地址；当源 NAT 规则类型为 NAT64 或者 IPv6 时，输入 IPv6 地址。 IP/掩码：在文本框中输入 IPv4 地址及掩码。当源 NAT 规则类型为 IPv4 或者 NAT46 时，可以配置该选项。 IPv6/前缀长度：在文本框中输入 IPv6 地址及前缀长度。当源 NAT 规则类型为 NAT64 或者 IPv6 时，可以配置该选项。
入流量	指定源 NAT 规则的入流量。默认为所有流量。 所有流量：指定源 NAT 规则中入流量为所有流量。 从任意

当 IP 地址符合以下条件时	
	接口进入的流量都会继续匹配该源 NAT 规则。 入接口：指定源 NAT 规则中流量的入接口，从下拉菜单中选择接口名称。配置了入接口之后，只有从该接口进入的流量才会继续匹配这条源 NAT 规则，其他接口进入的流量不匹配。
出流量	指定源 NAT 规则的出流量。默认为所有流量。 所有流量：指定源 NAT 规则中出流量为所有流量。从任意接口出去的流量都会继续匹配该源 NAT 规则。 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。配置了出接口之后，只有从该接口出去的流量才会继续匹配这条源 NAT 规则，其他接口出去的流量不匹配。 下一跳虚拟路由器：指定源 NAT 规则中出流量的下一跳虚拟路由器，从下拉菜单中选择虚拟路由器的名称。
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，在“预定义”下拉菜单中选择“自定义”，然后点击 ⊕ 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（IPv6/前缀长度）”，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： 静态： 选中并使用静态转换模式。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：选中并使用动态转换模式。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。

当 IP 地址符合以下条件时	
	动态端口：选中并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 后的“启用”按钮。 如果启用了 Round-robin 功能，每一个源 IP 产生的会话将以轮询的方式进行 IP 地址映射。启用 Round-robin 功能，选中 Round-robin 后“启用”按钮。 如果不启用 Sticky 功能和 Round-robin 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 Track 功能，系统将对 NAT 转换后的公网地址是否有效进行监测，即以其作为源地址来监测到目标网站或主机的访问是否正常。可配置的监测对象包括 Ping 报文监测对象、HTTP 报文监测对象、TCP 报文监测对象。该功能仅支持 IPv4 或者 NAT64 类型的源 NAT 规则，NAT 转换后的地址必须为 IP 地址或者地址簿中的地址，且转换模式为动态端口模式。系统优先使用监测成功的转换地址，当某个转换地址对目标网站或主机监测失败时，该地址被临时禁用，直至再次监测成功。当监测对象失败时，系统将在下个监测周期内禁用此地址并生成日志信息，不再转换私网地址为该公网地址，直到该地址被判定为可达。若 SNAT 规则的公网地址簿中地址全部被判定为不可达，系统将不禁用任何转换地址并发出日志信息。选中 Track 后的“启用”按钮启用该功能，并从下拉菜单选择监测对象。 **注意**：Sticky 功能和 Round-robin 功能是互斥的，二者不能同时配置。

点击“更多配置”，展开更多配置项，填写相关信息。

选项	说明
HA 组	指定源 NAT 规则所属的 HA 组。默认属于 HA 组 0。
时间表	指定源 NAT 规则的时间表。在“时间表”下拉菜单中选择需要的时间表，同时支持模糊搜索。如需新建时间表，点击 ⊕ 按钮。

选项	说明
NAT 日志	点击“启用”按钮，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，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。
描述	为此条源 NAT 规则输入描述信息。长度为 0-63 个字符。

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。

查看及过滤源 NAT 规则

用户可在源 NAT 列表中查看及过滤源 NAT 规则的信息。

源 NAT 规则页面显示如下：

每一列显示对应的配置。“时间表”一列显示源 NAT 规则的时间表名称和生效状态，还未生效或已失效的源 NAT 规则显示为“失效”。

点击“会话详情”一列的 按钮，打开<会话详情>页面。在该页面，用户可查看命中该源 NAT 规则的会话状态，用户还可以点击 过滤 按钮添加过滤条件并搜索符合过滤条件的会话状态信息。支持对“会话 id”、“源地址”、“源端口”、“目的地址”、“目的端口”、“协议”、“应用”、“flow0”、“flow1”进行过滤。可同时添加多个过滤条件，各个过滤条件之间的关系为“与”。

将鼠标悬停在不同列的配置上时，根据配置类型不同，出现 图标，或直接显示配置信息。

直接显示配置信息时，可进行查看。

出现 图标时，点击此图标后，根据配置类型的不同，可出现“过滤器”或“添加过滤条件”或“详情”。

点击“过滤器”或“添加过滤条件”，系统在列表上方添加相应行与列的过滤条件，且根据过滤条件进行规则过滤。

点击“详情”，查看配置的详细信息。然后在详情页面点击“条目详情”可以查看地址/服务条目详情。

复制/粘贴源 NAT 规则

当系统中存在大量的 NAT 规则时，为使用户更方便快捷地创建与已配置 NAT 规则类似的 NAT 规则，可以复制 NAT 规则并且粘贴在指定位置。

复制/粘贴源 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. 选中列表中需要复制的源 NAT 规则对应的复选框，然后点击“复制”按钮。
3. 点击“粘贴”按钮。从弹出下拉菜单中选择指定位置。该源 NAT 规则将被粘贴到指定的位置。

选项	说明

选项	说明
列表最前	将复制的源 NAT 规则粘贴至所有源 NAT 规则的首位。
列表最后	将复制的源 NAT 规则粘贴至所有源 NAT 规则的末位。
所选规则前	将复制的源 NAT 规则粘贴至所勾选的源 NAT 规则的前一位。
所选规则后	将复制的源 NAT 规则粘贴至所勾选的源 NAT 规则的后一位。

注意: 在粘贴源 NAT 规则时，如果粘贴位置选择多条源 NAT 规则或者未勾选任何规则，“所选规则前”和“所选规则后”选项不可用。

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，打开<调整优先级>页面。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。

导入源 NAT 规则

用户可以将本地源 NAT 规则配置文件导入到设备中，从而减少手动创建源 NAT 规则的工作量。目前仅支持导入 DAT 格式的文件。

导入源 NAT 规则配置文件，请按照以下步骤进行操作：

1. 点击“策略 > NAT > 源 NAT”。

2. 点击“导入”按钮，打开<导入>页面。

3. 点击“浏览”按钮，并选中需上传的本地源 NAT 规则配置文件。
4. 点击“确定”按钮，导入的源 NAT 规则将显示在 SNAT 页面中。

注意:

在导入源 NAT 规则配置文件时，需尽量使用导出的原文件，不要随意修改文件内容，否则可能造成格式错误而无法导入。

在导入源 NAT 规则配置文件时，如果出现报错，系统将自动停止导入，并且已导入的源 NAT 规则将被回滚删除。

导入的源 NAT 规则将会列在当前 SNAT 列表的最后。

若导入的源 NAT 的 ID 已存在，系统将覆盖掉原有的 NAT 规则的配置。

导出源 NAT 规则

用户可以将设备中当前的源 NAT 规则以 HTML、DAT 或 CSV 格式导出到本地，从而方便导入到其他设备中。同时，系统还支持将所有地址簿和服务簿（自定义条目）导出。

导出源 NAT 规则，请按照以下步骤进行操作：

1. 点击“策略 > NAT > 源 NAT”。
2. 点击“导出”按钮，打开<导出>页面。

在<导出>页面，填写如下配置信息。

选项	说明
范围	指定源 NAT 规则的导出范围。

选项	说明
	所有 SNAT：选中“所有 SNAT”，导出设备中当前的所有源 NAT 规则。 选中 SNAT：在 SNAT 列表中，勾选需要导出的源 NAT 规则复选框，然后在该对话框中，选中“选中 SNAT”，导出所选源 NAT 规则。 页码范围：选中“页码范围”，然后在文本框中输入页码或页码范围，导出指定页内的所有源 NAT 规则。 **注意**：页码之间须用分号隔开，例如：如需导出第 3 页以及第 5-8 页的源 NAT 规则，输入“3；5-8”。
导出地址条目和服务	勾选该复选框，系统会将所有地址簿和服务簿（自定义条目）导出。
导出 DAT 格式所有 SNAT	勾选该复选框，以 DAT 格式导出所有源 NAT 规则配置文件。

3. 点击“确定”按钮，开始下载导出文件。导出文件包括 4 种：natExport.html（NAT 展示页）、snat+导出时间.zip（源 NAT 规则配置文件）、snat rule+导出时间.csv 以及 DAT 格式目的 NAT 规则配置文件 vrrouter_snat+导出时间.DAT。
4. 双击已下载的 NAT 展示页“natExport.html”，点击“选择文件”按钮，选择已下载的目的 NAT 规则配置文件“snat+导出时间.zip”，即可查看已导出的目的 NAT 规则表格。

导出 NAT444 静态端口块映射表

用户可以将 NAT444 静态端口块映射表以文件形式导出，导出的映射表文件中包含 SNAT 规则 ID、源地址、转换后地址、起始端口号、结束端口号和协议信息。

导出静态端口块映射表，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“导出 NAT444 静态映射”按钮，将映射表导出并保存到适当位置。
3. 导出的映射表文件为 CSV 格式，建议用户通过管理接口导出映射表文件。

配置源 NAT 优化

当设备上有大量的 NAT 规则堆积，不能确定是否需要删除，增加了用户的维护难度。系统支持源 NAT 优化功能，包括源 NAT 命中分析以及冗余检测。

命中数

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

查看源 NAT 规则的命中数，进入源 NAT 页面。在源 NAT 规则列表的“命中数”一列，查看相应源 NAT 规则的命中数统计。

命中数清零

清除源 NAT 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 > NAT > 源 NAT 优化”，进入源 NAT 优化页面。
2. 选择<命中分析>标签页，在“虚拟路由器”下拉菜单中选择指定的虚拟路由器，点击页面右上角的“统计清零”按钮，打开<命中数清零>页面。
3. 根据需要，清除源 NAT 规则匹配次数统计信息。具体选项说明如下：

   所有 NAT：清除所有源 NAT 规则的匹配次数统计信息。

   NAT 的 ID：清除指定 ID 规则的匹配次数统计信息。在文本框中输入源 NAT 规则的 ID。
4. 点击“确定”按钮完成配置。

命中数检测

系统支持检测源 NAT 规则的命中数。命中数为 0 的源 NAT 规则即为未使用的源 NAT。

检测源 NAT 规则的命中数，按照以下步骤进行操作：

1. 点击“策略 > NAT > 源 NAT 优化”，进入源 NAT 优化页面。
2. 选择<命中分析>标签页，在“虚拟路由器”下拉菜单中选择指定的虚拟路由器，点击页面右上角的“命中分析”按钮，系统将开始检测源 NAT 规则的命中数。

冗余检测

为保证源 NAT 规则的有效性，系统可对源 NAT 规则进行冗余检测，即检查源 NAT 规则的覆盖情况，帮助用户排除由于源 NAT 规则覆盖导致有些源 NAT 规则无法被命中的问题。检测完成后，冗余源 NAT 规则会被显示在冗余检测列表中。

进行源 NAT 规则冗余检测，请按照以下步骤进行操作：

1. 点击“策略 > NAT > 源 NAT 优化”，进入源 NAT 优化页面，选择<冗余检测>标签页。

2. 在“虚拟路由器”下拉菜单中选择指定的虚拟路由器，点击“冗余检测”按钮。系统开始检测当前所有源 NAT 规则，可能会消耗较长时间，请耐心等待。完成后，冗余的源 NAT 规则将被显示在列表中。

用户可在“ID”一列查看被覆盖的 SNAT 规则的 ID，在“覆盖此 SNAT 规则的规则 ID”一列查看覆盖本条 SNAT 规则的所有规则 ID。

点击被覆盖的 SNAT 规则“操作”列的 按钮，删除本条冗余 SNAT 规则。

点击被覆盖的 SNAT 规则“操作”列的 按钮，禁用本条冗余 SNAT 规则。禁用后若不修改该 SNAT 规则的状态，之后将不参与冗余检测。如需恢复启用状态，在“策略 > NAT > 源 NAT”页面，选中禁用的 SNAT 规则，点击页面上方的“启用”按钮即可恢复。

点击“+”按钮，页面下方将展示被覆盖的 SNAT 规则详情。

注意: 当冗余检测开始后，SNAT 规则列表左下方将显示检测状态条。检测期间，不建议配置或编辑 SNAT 规则。用户可根据需求，点击 手动停止检测。点击后，系统将弹出提示框确认是否终止冗余检测，点击“确定”停止检测。

配置目的 NAT

DNAT 转换目的 IP 地址，通常是将受安全网关保护的内部服务器（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”，打开<IP 映射配置>页面。

在<IP 映射配置>页面，填写相关信息。

当 IP 地址符合以下条件时	
虚拟路由器	指定目的 NAT 规则所在的虚拟路由器。
类型	指定目的 NAT 规则的类型，可以为 IPv4、NAT46、NAT64 或者 IPv6。
目的地址	指定流量的目的 IP 地址或接口。包括： 地址条目：在下拉菜单中，用户可搜索并选定指定的地址条目。点击 ⊕ 按钮，可新建地址簿。 IP 地址：在文本框中直接输入 IP 地址。当目的 NAT 规则类型为 IPv4 或者 NAT46 时，输入 IPv4 地址；当目的 NAT 规则类型为 NAT64 或者 IPv6 时，输入 IPv6 地址。 IP/掩码：在文本框中输入 IPv4 地址及掩码。当目的 NAT 规则类型为 IPv4 或者 NAT46 时，可以配置该选项。 IPv6/前缀长度：在文本框中输入 IPv6 地址及前缀长度。当目的 NAT 规则类型为 NAT64 或者 IPv6 时，可以配置该选项。 动态 IP（物理接口）：在下拉列表中，用户可搜索并选定通过 DHCP、PPPoE 等协议动态获取 IP 的接口，点击“确

当 IP 地址符合以下条件时	
	定”。当目的 NAT 规则类型为 IPv4 或者 NAT46 时，可以配置该选项。
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（IPv6/前缀长度）。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	
HA 组	指定目的 NAT 规则所属的 HA 组。默认属于 HA 组 0。
描述	为此条目的 NAT 规则输入描述信息。长度为 0-63 个字符。

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”，打开<端口映射配置>页面。

在<端口映射配置>页面，填写相关信息。

当 IP 地址符合以下条件时	
虚拟路由器	指定目的 NAT 规则所在的虚拟路由器。
类型	指定目的 NAT 规则的类型，可以为 IPv4、NAT46、NAT64 或者

当 IP 地址符合以下条件时	
	IPv6。
目的地址	指定流量的目的 IP 地址或接口。包括： 地址条目：在下拉菜单中，用户可搜索并选定指定的地址条目。点击 ⊕ 按钮，可新建地址簿。 IP 地址：在文本框中直接输入 IP 地址。当目的 NAT 规则类型为 IPv4 或者 NAT46 时，输入 IPv4 地址；当目的 NAT 规则类型为 NAT64 或者 IPv6 时，输入 IPv6 地址。 IP/掩码：在文本框中输入 IPv4 地址及掩码。当目的 NAT 规则类型为 IPv4 或者 NAT46 时，可以配置该选项。 IPv6/前缀长度 ： 在文本框中输入 IPv6 地址及前缀长度。当目的 NAT 规则类型为 NAT64 或者 IPv6 时，可以配置该选项 。 动态 IP（物理接口）：在下拉列表中，用户可搜索并选定通过 DHCP、PPPoE 等协议动态获取 IP 的接口，点击“确定”。当目的 NAT 规则类型为 IPv4 或者 NAT46 时，可以配置该选项。
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（IPv6/前缀长度）。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	
HA 组	指定目的 NAT 规则所属的 HA 组。默认属于 HA 组 0。
描述	为此条目的 NAT 规则输入描述信息。长度为 0-63 个字符。

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”，打开<目的 NAT 配置>页面；对已经存在的 NAT 规则，选中此条规则，并点击“编辑”按钮，打开<目的 NAT 配置>页面。

在<目的 NAT 配置>页面，填写相关信息。

当 IP 地址符合以下条件时	
虚拟路由器	指定目的 NAT 规则所在的虚拟路由器。
类型	指定目的 NAT 规则的类型，可以为 IPv4、NAT46、NAT64 或者 IPv6。
源安全域	指定目的 NAT 规则中流量入接口所属的安全域，默认为 Any。配置了源安全域之后，只有从绑定了该安全域的接口进入的流量才会继续匹配这条 DNAT 规则。 **注意：**源安全域需要属于指定的虚拟路由器。
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，用户可搜索并选定指定的地址条目。点击 ⊕ 按钮，可新建地址簿。 IP 地址：在文本框中直接输入 IP 地址。当目的 NAT 规则类型为 IPv4 或者 NAT46 时，输入 IPv4 地址；当目的 NAT 规则类型为 NAT64 或者 IPv6 时，输入 IPv6 地址。 IP/掩码：在文本框中输入 IPv4 地址及掩码。当目的 NAT 规则类型为 IPv4 或者 NAT46 时，可以配置该选项。 IPv6/前缀长度：在文本框中输入 IPv6 地址及前缀长度。当目的 NAT 规则类型为 NAT64 或者 IPv6 时，可以配置该选项。

当 IP 地址符合以下条件时	
目的地址	指定流量的目的 IP 地址或接口。包括： 地址条目：在下拉菜单中，用户可搜索并选定指定的地址条目。点击 ⊕ 按钮，可新建地址簿。 IP 地址：在文本框中直接输入 IP 地址。当目的 NAT 规则类型为 IPv4 或者 NAT46 时，输入 IPv4 地址；当目的 NAT 规则类型为 NAT64 或者 IPv6 时，输入 IPv6 地址。 IP/掩码：在文本框中输入 IPv4 地址及掩码。当目的 NAT 规则类型为 IPv4 或者 NAT46 时，可以配置该选项。 IPv6/前缀长度：在文本框中输入 IPv6 地址及前缀长度。当目的 NAT 规则类型为 NAT64 或者 IPv6 时，可以配置该选项。 动态 IP（物理接口）：在下拉列表中，用户可搜索并选定通过 DHCP、PPPoE 等协议动态获取 IP 的接口，点击“确定”。当目的 NAT 规则类型为 NAT64 或者 IPv6 时，可以配置该选项。
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。 V4-MAPPED：对符合条件的流量做地址转换，且直接从报文的目的 IPv6 地址中抽取目的 IPv4 地址。当目的 NAT 规则的类型为 NAT64 时，可以配置该选项。
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（IPv6/前缀长度）”、或者“SLB 服务器池”。选择类型后，指定相应的取值。SLB 服务器池类型仅支持 IPv4 类型或者 NAT64 类型的目的 NAT 规则。关于 SLB 服务器地址池配置，参阅"SLB 服务器池" 在第 314 页。
将服务端口转换为	
转换端口	点击“启用”按钮，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	点击“启用”按钮，开启负载均衡功能。开启负载均衡功能后，流量

当 IP 地址符合以下条件时	
	将会均衡到不同的内网服务器。
重定向	点击“启用”按钮，开启重定向功能。 如果“转换为 IP”地址个数如果与“目的地址”的个数不相同或者流量目的 IP 地址指定为 any 时，则需要为该条 DNAT 规则开启重定向功能。

点击“更多配置”，展开更多配置项，填写相关信息。

服务器跟踪	
HA 组	指定目的 NAT 规则所属的 HA 组。默认属于 HA 组 0。
源转换	点击“启用”按钮，开启目的 NAT 规则的源地址转换功能，即双向 NAT。开启双向 NAT 后，设备会根据目的 NAT 规则对经过设备的数据的目的地址和源地址都进行转换。
源转换为 IP	在启用“源转换”后，指定 NAT 转换地址的类型，可以为“地址条目”、“IP 地址”、“IP/掩码（IPv6/前缀长度）”。
模式	指定源地址转换的模式，包括： 动态端口：选中并使用动态端口转换模式，同一个源 IP 将被转换为同一个转换地址。当转换失败时，随机选择一个转换地址。 指定 IP：选中并使用静态转换模式，即一对一转换，该模式要求源 IP 地址和转换 IP 地址的数量相同。
时间表	指定目的 NAT 规则的时间表。在“时间表”下拉菜单中选择需要的时间表，同时支持模糊搜索。如需新建时间表，点击 ⊕ 按钮。
Ping 跟踪	点击“启用”按钮，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。
TCP 跟踪	点击“启用”按钮，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。
NAT 日志	点击“启用”按钮，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：

服务器跟踪	
	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，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。
描述	为此条目的 NAT 规则输入描述信息。长度为 0-63 个字符。

3. 点击“确定”完成配置。

注意: 目的 NAT 规则绑定非“Any”的源安全域后，该安全域不能删除。

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。

查看及过滤目的 NAT 规则

用户可在目的 NAT 列表中查看及过滤目的 NAT 规则的信息。

目的 NAT 规则页面显示如下：

每一列显示对应的配置。“时间表”一列显示目的 NAT 规则的时间表名称和生效状态，还未生效或已失效的目的 NAT 规则显示为“失效”。

点击“会话详情”一列的 按钮，打开<会话详情>页面。在该页面，用户可查看命中该目的 NAT 规则的会话状态，用户还可以点击 过滤 按钮添加过滤条件并搜索符合过滤条件的会话状态信息。
支持对“会话 id”、“源地址”、“源端口”、“目的地址”、“目的端口”、“协议”、“应用”、“flow0”、“flow1”进行过滤。可同时添加多个过滤条件，各个过滤条件之间的关系为“与”。

将鼠标悬停在不同列的配置上时，根据配置类型不同，出现 图标，或直接显示配置信息。

直接显示配置信息时，可进行查看。

出现 图标时，点击此图标后，根据配置类型的不同，可出现“过滤器”或“添加过滤条件”或“详情”。

点击“过滤器”或“添加过滤条件”，系统在列表上方添加相应行与列的过滤条件，且根据过滤条件进行规则过滤。

点击“详情”，查看配置的详细信息。然后在详情页面点击“条目详情”可以查看地址/服务条目详情。

复制/粘贴目的 NAT 规则

当系统中存在大量的 NAT 规则时，为使用户更方便快捷地创建与已配置 NAT 规则类似的 NAT 规则，可以复制 NAT 规则并且粘贴在指定位置。

复制/粘贴目的 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. 选中列表中需要复制的目的 NAT 规则对应的复选框，然后点击“复制”按钮。
3. 点击“粘贴”按钮。从弹出下拉菜单中选择指定位置。该目的 NAT 规则将被粘贴到指定的位置。

选项	说明
列表最前	将复制的目的 NAT 规则粘贴至所有目的 NAT 规则的首位。
列表最后	将复制的目的 NAT 规则粘贴至所有目的 NAT 规则的末位。
所选规则前	将复制的目的 NAT 规则粘贴至所勾选的目的 NAT 规则的前一位。

选项	说明
所选规则后	将复制的目的 NAT 规则粘贴至所勾选的目的 NAT 规则的后一位。

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，然后点击列表上方的“优先级”按钮，打开<调整优先级>页面。选择“列表最前”、“列表最后”、“该 ID 之前”或“该 ID 之后”，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。
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。

导入目的 NAT 规则

用户可以将本地目的 NAT 规则配置文件导入到设备中，从而减少手动创建目的 NAT 规则的工作量。目前仅支持导入 DAT 格式的文件。

导入目的 NAT 规则配置文件，请按照以下步骤进行操作：

1. 点击“策略 > NAT > 目的 NAT”。
2. 点击“导入”按钮，打开<导入>页面。

3. 点击“浏览”按钮，并选中需上传的本地目的 NAT 规则配置文件。

4. 点击“确定”按钮，导入的目的 NAT 规则将显示在 DNAT 页面中。

注意:

在导入目的 NAT 规则配置文件时，需尽量使用导出的原文件，不要随意修改文件内容，否则可能造成格式错误而无法导入。

如果出现格式或其他异常的报错，系统将自动停止导入，并且已导入的目的 NAT 规则将被回滚删除。

导入的目的 NAT 规则将会列在当前 DNAT 列表的最后。

若导入的目的 NAT 的 ID 已存在，系统将覆盖掉原有的 NAT 规则的配置。

导出目的 NAT 规则

用户可以将设备中当前的目的 NAT 规则以 HTML、DAT 或 CSV 格式导出到本地，从而方便导入到其他设备中。同时，系统还支持将所有地址簿、服务簿（自定义条目）和 SLB 服务器池（自定义条目）等对象导出。

导出目的 NAT 规则，请按照以下步骤进行操作：

1. 点击“策略 > NAT > 目的 NAT”。

2. 点击“导出”按钮，打开<导出>页面。

在<导出>页面，填写如下配置信息。

选项	说明
范围	指定目的 NAT 规则的导出范围。 所有 DNAT：选中“所有 DNAT”，导出设备中当前的所有目的 NAT 规则。 选中 DNAT：在 DNAT 列表中，勾选需要导出的目的 NAT 规则复选框，然后在该对话框中，选中“选中 DNAT”，导出所选目的 NAT 规则。

选项	说明
	页码范围：选中“页码范围”，然后在文本框中输入页码或页码范围，导出指定页内的所有目的 NAT 规则。 **注意**：页码之间须用分号隔开，例如：如需导出第 3 页以及第 5-8 页的目的 NAT 规则，输入“3；5-8”。
导出地址条目、服务和 SLB 服务器池	勾选该复选框，将所有地址簿、服务簿（自定义条目）、SLB 服务器（自定义条目）池等目的 NAT 规则引用的对象全部导出。
导出 DAT 格式所有 DNAT	勾选该复选框，以 DAT 格式导出所有目的 NAT 规则配置文件。

3. 点击“确定”按钮，开始下载导出文件。导出文件包括 4 种：natExport.html（NAT 展示页）、dnat+导出时间.zip（目的 NAT 规则配置文件）、dnat rule+导出时间.csv 以及 DAT 格式目的 NAT 规则配置文件 vr vrouter_dnat+导出时间.dat。

4. 双击已下载的 NAT 展示页“natExport.html”，点击“选择文件”按钮，选择已下载的目的 NAT 规则配置文件“dnat+导出时间.zip”，即可查看已导出的目的 NAT 规则表格。

配置目的 NAT 优化

当设备上有大量的 NAT 规则堆积，不能确定是否需要删除，增加了用户的维护难度。系统支持目的 NAT 优化功能，包括目的 NAT 命中分析以及冗余检测。

命中数

设备支持目的 NAT 规则匹配次数统计功能。该功能能够对系统流量与目的 NAT 规则的匹配次数进行统计，即每当进入系统的流量与某条目的 NAT 规则相匹配时，该目的 NAT 规则的匹配次数会自动加 1。

查看目的 NAT 规则的命中数，进入目的 NAT 页面。在目的 NAT 规则列表的“命中数”一列，查看相应目的 NAT 规则的命中数统计。

命中数清零

清除目的 NAT 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 > NAT > 目的 NAT 优化”，进入目的 NAT 优化页面。

2. 点击“统计清零”按钮，打开<命中数清零>页面。

3. 根据需要，清除目的 NAT 规则匹配次数统计信息。具体选项说明如下：

   所有 NAT：清除所有目的 NAT 规则的匹配次数统计信息。

   NAT 的 ID：清除指定 ID 规则的匹配次数统计信息。在文本框中输入目的 NAT 规则的 ID。

4. 点击“确定”按钮完成配置。

命中数检测

系统支持检测目的 NAT 规则的命中数。命中数为 0 的目的 NAT 规则即为未使用的目的 NAT。

检测目的 NAT 规则的命中数，按照以下步骤进行操作：

1. 点击“策略 > NAT > 目的 NAT 优化”，进入目的 NAT 优化页面。
2. 点击“命中分析”按钮，系统将开始检测目的 NAT 规则的命中数。

冗余检测

为保证目的 NAT 规则的有效性，系统可对目的 NAT 规则进行冗余检测，即检查目的 NAT 规则的覆盖情况，帮助用户排除由于目的 NAT 规则覆盖导致有些目的 NAT 规则无法被命中的问题。检测完成后，冗余目的 NAT 规则会被显示在冗余检测列表中。

进行目的 NAT 规则冗余检测，请按照以下步骤进行操作：

1. 点击“策略 > NAT > 目的 NAT 优化”，进入目的 NAT 优化页面，选择<冗余检测>标签页。
2. 在“虚拟路由器”下拉菜单中选择指定的虚拟路由器，点击“冗余检测”按钮。系统开始检测当前所有目的 NAT 规则，可能会消耗较长时间，请耐心等待。完成后，冗余的 DNAT 规则将被显示在列表中。

用户可在“ID”一列查看被覆盖的 DNAT 规则的 ID，在“覆盖此 DNAT 规则的规则 ID”一列查看覆盖本条 DNAT 规则的所有规则 ID。

点击被覆盖的 DNAT 规则“操作”列的 按钮，删除本条冗余 DNAT 规则。

点击被覆盖的 DNAT 规则“操作”列的 按钮，禁用本条冗余 DNAT 规则。禁用后若不修改该 DNAT 规则的状态，之后将不参与冗余检测。如需恢复启用状态，在“策略 > NAT > 目的 NAT”页面，选中禁用的 DNAT 规则，点击页面上方的“启用”按钮即可恢复。

点击“+”按钮，页面下方将展示被覆盖的 DNAT 规则详情。

注意: 当冗余检测开始后，DNAT 规则列表左下方将显示检测状态条。检测期间，不建议配置或编辑 DNAT 规则。用户可根据需求，点击 ✖ 手动停止检测。点击后，系统将弹出提示框确认是否终止冗余检测，点击“确定”停止检测。

配置 DNS 改写

DNS 改写功能，也称为 DNS Rewrite 功能。当客户端经过防火墙向公网的 DNS 服务器发起 DNS 解析请求时，系统支持基于 DNS 改写规则对 DNS 服务器返回的响应报文中的 IP 地址进行改写，将其改为私网 IP 地址以保护和隐藏组网环境中的网络配置。

在匹配 DNS 改写规则时，系统会按照 DNS 改写规则的排序从上到下依次匹配，然后按照第一条匹配的规则改写响应。用户可以通过“策略 > NAT > DNS 改写”进入 DNS 改写页面查看 DNS 改写规则的排序。

注意: 开启 DNS ALG 功能后，DNS 改写功能才会生效。

配置 DNS 改写规则

配置 DNS 改写规则，按照以下步骤进行操作：

1. 点击“策略 > NAT > DNS 改写”，进入 DNS 改写页面。
2. 点击“新建”按钮，打开<DNS 改写配置>页面。

3.

选项	说明
虚拟路由器	指定 DNS 改写规则所在的虚拟路由器。
类型	指定 DNS 改写规则的 IP 协议类型，支持 IPv4 和 IPv6。

选项	说明
响应地址	指定需要被改写的地址，可以为地址条目名称、IP 地址、IP/掩码或域名簿名称。当指定地址条目或域名簿时，支持选择一个已配置的地址条目或域名簿，也支持新建。
改写地址	指定改写后的地址，可以为 IP 地址、IP/掩码或地址条目名称。当指定地址条目时，支持选择一个已配置的地址条目，也支持新建。
列表位置	指定 DNS 改写规则的位置，可以位于某个 ID 之前或者之后，也可以是位于所有规则的首位或者末尾。默认情况下，新创建的规则会被放到所有规则的末尾。
ID	指定 DNS 改写规则的 ID。每一条规则都有一个唯一的 ID。可以选择由系统自动分配一个 ID，或者手动指定一个 ID。取值范围是 1 到 16。
描述	指定 DNS 改写规则的描述信息。取值范围是 0 到 63 个字符。

4. 点击“确定”完成配置。

管理 DNS 改写规则

用户可以通过“策略 > NAT > DNS 改写”进入 DNS 改写页面查看已配置的 DNS 改写规则。

选择一条 DNS 改写规则后，点击“编辑”，可以修改规则。

选择一条或多条 DNS 改写规则后，点击“删除”，可以删除规则。

选择一条 DNS 改写规则后，点击“优先级”，可以调整该规则在所有规则中的排列位置。

点击“过滤”按钮，从下拉菜单中选择过滤项目，在输入框输入过滤条件可以筛选出符合过滤条件的 DNS 改写规则。

查看 DNS 改写动态映射表

DNS 动态映射表里保存了响应地址和改写地址之间的动态映射关系。收到 DNS 响应后时，系统会获取响应中的域名和 IP 地址，并查找 DNS 动态映射表。

如果存在匹配的动态映射条目，则直接改写 DNS 响应，并更新动态映射条目的生存时间。

如果找不到匹配的动态映射条目，则按照 DNS 改写规则的排序依次匹配规则。当查找到匹配的 DNS 改写规则时，系统会生成一条动态映射条目，并改写 DNS 响应。当没有 DNS 改写规则命中时，系统会直接转发响应。

收到客户端的业务访问请求时，系统也会在动态映射表中查找匹配的表项，并基于命中的表项做地址转换。

点击“策略 > NAT > DNS 改写动态映射”，可以进入 DNS 改写动态映射页面查看系统内保存的 DNS 动态映射表。点击“过滤”按钮，可以选择和设置过滤条件筛选 DNS 动态映射条目。

查看负载均衡服务器及地址池状态

查看服务器状态：如果在 SLB 服务器池中启用探测功能（Ping 探测、TCP 探测或 UDP 探测），系统列出 Ping 报文、TCP 报文或 UDP 报文探测的内网服务器的状态信息，包括服务器 IP 地址、类型、端口、所属 HA 组、状态、当前连接数以及该服务器被哪些目的 NAT 规则引用。

查看服务器池状态：启用服务器负载均衡功能后，系统将列出监测的内网服务器的状态信息，包括服务器名称、类型、负载均衡算法、引用 SLB 服务器池的目的 NAT 规则、异常服务器数以及当前会话数。

查看服务器状态

查看服务器状态信息，按照以下步骤进行操作：

1. 点击“策略 > NAT > SLB 服务器状态”，进入 SLB 服务器状态页面。
2. 用户可根据虚拟路由器，SLB 服务器池，以及服务器地址设置过滤条件，查看符合过滤条件的信息。

查看 SLB 服务器状态页面显示相关的信息。

选项	说明
服务器	显示服务器的 IP 地址。
类型	显示服务器的类型，包括 IPv4、IPv6。
端口	显示服务器的端口号。
状态	显示服务器的状态。
当前连接数	显示与服务器建立会话的连接数。
目的 NAT	显示服务器被哪些目的 NAT 规则引用。
HA 组	显示服务器所属的 HA 组。

查看 SLB 服务器地址池状态

查看服务器池状态信息，按照以下步骤进行操作：

1. 点击“策略 > NAT > SLB 服务器池状态”，进入 SLB 服务器池状态页面。
2. 用户可根据虚拟路由器、算法、以及名称设置过滤条件，查看符合过滤条件的信息。

查看 SLB 服务器地址池状态页面显示的信息

选项	说明
名称	显示 SLB 服务器池的名称。
类型	显示 SLB 服务器池的类型，包括 IPv4、IPv6。
算法	显示负载均衡算法。
目的 NAT	显示服务器被哪些目的 NAT 规则引用。

选项	说明
异常/服务器总数	显示异常服务器数和服务器总数。
当前会话数	显示当前会话数。

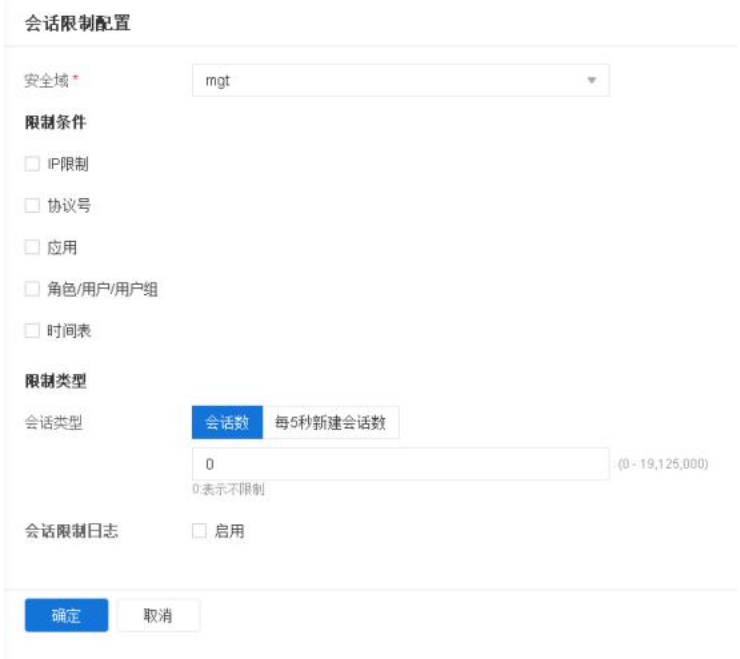
会话限制

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，打开<会话限制配置>页面。



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。限制条件可以是 IP 限制、应用限制、角色/用户/用户组限制、时间表。**

限制条件
勾选“IP 限制”复选框，设置 IP 限制条件。

限制条件	
IP	选择该选项，并选择地址条目，然后限制安全域中某个 IP 地址段的会话数。在地址下拉菜单中，当鼠标悬停在某地址条目上时，右侧会出现  按钮，点击可对所选地址条目进行编辑。
源 IP-->目的 IP	选择该选项，并选择源 IP 的地址条目和目的 IP 的地址条目。在地址下拉菜单中，当鼠标悬停在某地址条目上时，右侧会出现  按钮，点击可对所选地址条目进行编辑。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：
协议号	勾选“协议号”复选框，在文本框中输入协议号的数值。
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。
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。
限制类型	
会话数	选择该选项，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	选择该选项，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。

5. 勾选“会话限制日志”复选框，开启记录会话限制日志功能。

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。用户可根据需要清除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. 选择需要清除统计信息的会话限制条目。

3. 点击“清除”按钮，清除特定会话限制规则中被丢弃会话数的统计信息。

共享接入

共享接入，即多个用户终端通过同一个 IP 地址接入到网络。系统的共享接入功能可以防范未知设备的接入，消除潜在的安全风险，并能够帮助用户合理分配带宽，限制多用户共享带宽，保证用户的上网体验。

配置共享接入规则

新建共享接入规则，按照以下步骤进行操作：

1. 点击“策略 > 共享接入”，进入共享接入页面。
2. 点击共享接入列表左上方的“新建”按钮，打开<共享接入配置>页面。

选项	说明
名称	指定共享接入规则的名称。长度为 1-63 个字符。
类型	指定共享接入规则的地址类型，包括 IPv4 和 IPv6。IPv6 选项仅当该版本支持 IPv6 时可配。
源安全域	指定共享接入规则的源安全域。
源地址	指定共享接入规则的源地址。用户可指定多条源地址类目。 1. 点击 +，打开“地址”页面。 2. 在“ 地址”页面中选择地址类型。 3. 根据地址类型的不同，选择或输入需要的地址。 4. 点击“ 添加” 按钮将所选择的地址添加到左侧列表中。 5. 添加完成后，点击“ 关闭” 。 用户还可执行如下操作：

选项	说明
	选择地址簿类型时，可点击 + 按钮创建新的地址簿。 选择地址簿类型时，点击搜索框中的 ▼ 按钮，可以按地址簿名称和地址成员的 IP 进行模糊搜索，名称和地址是与的关系。地址支持多种输入方式，例如：输入“地址”为 10.10.10.10/32，可能匹配到包含地址成员是 10.10.10.10/24 的地址簿；输入“地址”为段掩码 9.9.9.9/24，可能匹配到包含地址成员是 9.9.0.0/16 的地址簿；输入“地址”为 10.10.10.10，可能匹配到地址成员的 IP 范围为 10.10.10.0-10.10.10.255 的地址簿；输入“地址”为 10.23，可能匹配到包含地址成员是 1.10.23.10/24 的地址簿；输入“地址”为 aa，可能匹配到地址成员的“主机名称”为 aaa 的地址簿。 当共享接入规则的类型选择“ IPv4” 类型时，系统默认 IPv4 地址配置为 any。 如需恢复为 any，选择 any 复选框。 当共享接入规则的类型选择“ IPv6” 类型时，系统默认 IPv6 地址配置为 IPv6- any。如需恢复为 IPv6-any，选择 IPv6-any 复选框。
时间表	指定时间表。共享接入规则将在时间表所指定的时间周期内生效。如果不配置，那么共享接入检测规则会一直生效。
最大终端数	指定系统允许接入的最大终端数。取值范围是 1-15，默认值为 2。
超限动作	当共享接入同一个 IP 地址的终端数超出系统允许共享接入的最大终端数后，将按指定的动作处理该超限终端的 IP 地址。 只记录日志：指定该超限动作，当共享接入终端数超出最大终端数后，系统将对超限终端的 IP 仅进行记录日志信息，而不影响接入终端的正常上网。 警告：指定该超限动作，当共享接入终端数超出最大终端数后，系统将在指定的持续时间内，对超限终端发送警告信息页面并记录日志信息。 持续时间：指定警告的持续时间，取值范围是 60-3600 秒，默认值为 60 秒。持续时间结束后，系统将会重新检测该 IP 地址下接入终端数是否超限。 警告信息：指定警告信息页面的自定义告警内容，取值范围是 0 到 255 个字符。 阻断：指定该超限动作，当共享接入终端数超出最大终端数后，系统在指定的持续时间内将对超限终端的 IP 地址进行阻断并记录日志信息。

选项	说明
	持续时间：指定阻断的持续时间，取值范围是 60-3600s，默认值为 60s。持续时间结束后，系统将会重新检测该 IP 地址下接入终端数是否超限。
终端超时时间	指定终端的超时时间，当超出该时间后，终端未再使用该 IP 访问网络时，清除终端信息。取值范围是 300-86400 秒，默认值为 600 秒。

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 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 > ARP 绑定”。
2. 点击“新建”按钮。打开<IP-MAC 绑定配置>页面。

在<IP-MAC 绑定配置>页面内填写绑定信息。

选项	说明
MAC	指定 MAC 地址。
IP	在文本框中输入需要绑定的 IP 地址。
端口	在下拉菜单选择需要绑定的端口。
虚拟路由器	从下拉菜单选择静态 IP-MAC 绑定条目所属的虚拟路由器，默认属于缺省虚拟路由器（trust-vr）。
MAC 描述	为 IP-MAC 绑定条目添加描述信息。

3. 配置完成，点击“确定”按钮保存所做配置并返回 ARP 绑定页面。

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 > ARP 绑定”。

2. 点击 ⋮ 按钮，选择“ARP-MAC 学习配置”，打开<ARP/MAC 学习配置>页面。

3. 选中需要开启 ARP 学习/MAC 学习的接口。

4. 点击“启用”按钮并在下拉菜单中选择“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 绑定页面。

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 > ARP 绑定”，进入 ARP 绑定页面。

2. 点击“绑定配置”按钮并在下拉菜单中选择“扫描添加 IP-MAC 绑定”，打开<IP MAC 扫描>页面。

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> ARP 绑定”。

2. 点击“绑定配置”按钮并在下拉菜单中选择“绑定所有配置”，打开出<绑定所有配置>页面。

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 > ARP 绑定”。

2. 点击“绑定配置”按钮并在下拉菜单中选择“解除绑定配置”，打开<解除绑定配置>页面。

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> ARP 绑定”。

2. 点击 ⋮ 按钮，选择“导入 IP-MAC 绑定”，打开<导入>页面。

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> ARP 绑定”。

2. 点击 ⋮ 按钮，选择“导出 IP-MAC 绑定”，打开<导出>页面。

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 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> ARP 检查”。
2. 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，打开<接口配置>页面。

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. 点击接口名称前的“+”按钮，展开该 VSwitch 接口的端口信息，包括端口名称、所属接口、检查状态及 ARP 速率。若需要对信息进行编辑，点击左上方的“编辑”按钮，打开<编辑 ARP 速率>页面，用户可进行以下操作。

   勾选“检查状态”部分的“不检查”/“检查”选项，设置不需要/需要进行 ARP 检查。

   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。

7. 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。

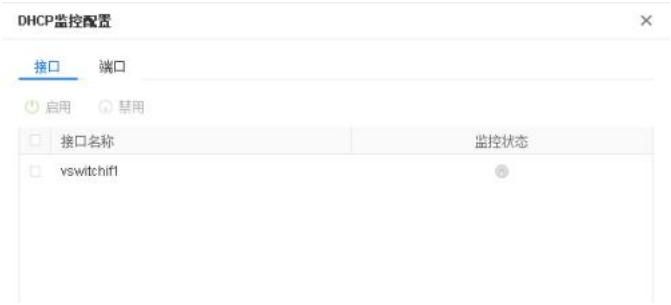
由于 DHCP 服务的客户端是以广播的方式寻找服务器，并且只接收第一个到达的服务器提供的网络配置参数，因此，如果网络中存在非授权的 DHCP 服务器，就有可能引发 DHCP 服务器欺骗。设备可以通过在相应端口上设置丢弃 DHCP 响应报文来防止 DHCP 服务器欺骗。

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 > DHCP 监控”。
2. 点击“DHCP 监控设置”按钮。打开<DHCP 监控配置>页面。



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、VLAN 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 >主机防御”。
2. 点击“新建”按钮。打开<主机防御>页面。

在<主机防御>页面内填写绑定信息。

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	

发送设置	
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。

边界流量过滤

边界流量过滤（Perimeter Traffic Filtering）功能是基于已知的风险 IP、MAC 或服务等对流量进行过滤，并对命中风险 IP、MAC 或服务的恶意流量采取阻断、记录日志等措施进行处理。

黑白名单配置包括以下内容：

IP 黑名单：系统支持静态 IP 黑名单、黑名单库、动态 IP 黑名单、真实 IP 黑名单及命中统计。

Service 黑名单：将服务添加到黑名单后，系统将对黑名单中的服务执行阻断操作，直到阻断时间结束。

MAC 黑名单：将主机的 MAC 添加到黑名单中，通过绑定时间表来控制添加到黑名单中的主机在某一时间段不能上网。

IP 信誉：通过更新系统的 IP 信誉特征库，从云端同步符合僵尸主机、垃圾邮件、Tor 节点、失陷主机、暴力破解等特征的 IP 信誉风险 IP 地址。

IP 白名单：将 IP 地址添加至全局白名单列表，配置后，系统将不对白名单中 IP 地址做阻断限制。

全局检索：查看指定 IP 地址的静态 IP 黑名单、黑名单库详情、动态 IP 黑名单、例外白名单、Service 黑名单及 IP 信誉过滤条目。

配置：黑名单全局配置，包括黑名单日志、会话重匹配及 IP 黑名单 TCP 重置。

注意:

使用 IP 信誉功能前，请先安装 IP 信誉库许可证，然后重启设备。设备成功重启后，升级 IP 信誉库功能才可使用。

配置 IP 黑名单

静态 IP 黑名单

静态 IP 黑名单对指定 IP 的恶意流量进行过滤阻断或控制添加到黑名单中的主机在某一时间段不能上网。

配置静态 IP 黑名单，请按照以下步骤进行操作：

1. 点击“策略 > 边界流量过滤 > IP 黑名单”，进入 IP 黑名单页面。
2. 在“静态 IP 黑名单”页签中点击“新建”按钮，打开<静态 IP 黑名单>页面。

在<静态 IP 黑名单>页面中填写配置信息。

选项	说明
IP 类型	选择 IP 地址的类型，包含 IPv4 和 IPv6 以及用户名。当指定为“用户名”时，表示对指定用户的恶意流量进行过滤阻断或控制。
条目类型	选择地址条目类型，包括 IP 地址、IP 范围和地址簿。并在文本框中输入相应的 IP 地址范围或选择指定的地址簿。
用户名	当 IP 类型指定为“用户名”时，点击下拉菜单，在展开页面中指定用户类型和名称： 指定用户：点击“AAA 服务器/角色”，选择用户所属 AAA 服务器，然后点击“选择用户”下拉菜单后选择已配置的用户名称。 指定用户组：点击“AAA 服务器/角色”，选择用户组所属 AAA 服务器，然后点击“选择用户组”下拉菜单后选择已配置的用户组名称。 指定角色：点击“AAA 服务器/角色”，选择角色后搜索或选择已配置的角色名称。 注意: 在配置前，请先完成如下配置：创建用户/用户组并绑定 IP 地址、创建角色并映射到用户、在 AAA 服务器中指定角色映射规则。

选项	说明
作用域	指定黑名单生效于全局、指定安全域或指定虚拟路由器。当选择“安全域”或“虚拟路由器”时，在相应的下拉列表中选择需要的条目。
时间表	在“时间表”下拉菜单中选择需要的时间表。该条黑名单将会在时间表指定的时间范围内生效。
状态	指定静态 IP 黑名单的开启状态。

3. 点击“确定”按钮保存所做配置。

冗余检测

系统可对黑名单条目进行冗余检测，即检查 IP 地址的覆盖情况，帮助用户排除由于 IP 地址覆盖导致的匹配问题。

配置冗余检测，请按照以下步骤进行操作：

1. 点击“策略>边界流量过滤>IP 黑名单”，进入 IP 黑名单页面。
2. 在“静态 IP 黑名单”页签中点击“冗余检测”按钮，在弹出的提示对话框中点击“确定”按钮，系统开始检测，可能会消耗较长时间，请耐心等待。

3. 完成后，在“冗余检测”页面查看结果，包括黑名单条目的 IP、作用域、时间表、状态、被覆盖 ID 及 IP 个数。

4. 如果需要删除，从列表中勾选需要删除的条目，点击“删除”按钮。

黑名单库

系统支持导入/导出黑名单库或从指定服务器更新黑名单库文件，并指定黑名单库的策略。

配置黑名单库策略，请按照以下步骤进行操作：

1. 点击“策略>边界流量过滤>IP 黑名单”，进入 IP 黑名单页面。
2. 在“黑名单库策略”页签中点击“新建”按钮，打开<黑名单库策略>页面。

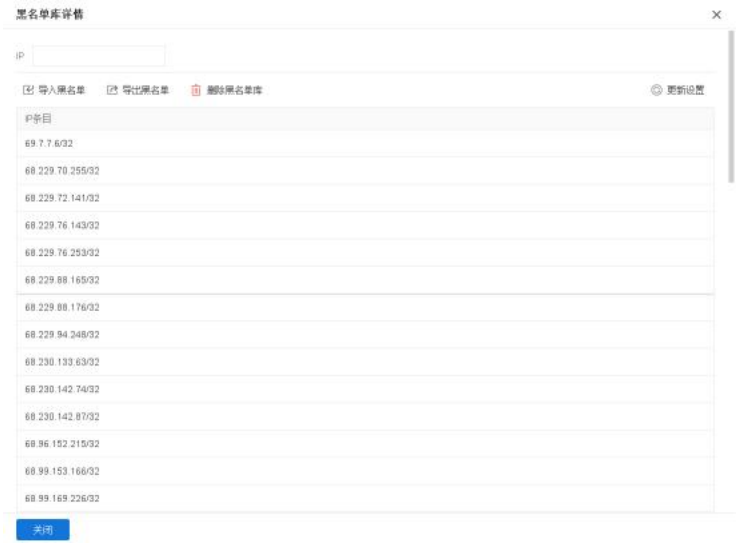
在<黑名单库策略>页面中填写配置信息。

选项	说明
作用域	指定黑名单库生效于全局、指定安全域或指定虚拟路由器。当选择“安全域”或“虚拟路由器”时，在相应的下拉列表中选择需要的条目。
状态	指定黑名单库策略的开启状态。

3. 点击“确定”按钮保存所做配置。

黑名单库详情

1. 点击“策略 > 边界流量过滤 > IP 黑名单”，进入 IP 黑名单页面。
2. 点击“黑名单库详情”按钮，打开黑名单库详情页面。



导入黑名单文件，请按照以下步骤进行操作：

1. 在黑名单库详情页面，点击“导入黑名单”按钮，打开<导入>页面。
2. 选择“增量导入”或”覆盖导入”，指定导入黑名单的模式。

   增量导入：在原有文件的基础上继续导入黑名单库文件。

   覆盖导入：覆盖原有黑名单库文件。
3. 在“文件名”处，点击“浏览”按钮，选择需要导入的本地文件。
4. 点击“确定”按钮，完成配置。

配置自动更新，请按照以下步骤进行操作：

1. 在黑名单库详情页面，点击“更新设置”按钮，打开<更新设置>页面。
2. 开启“自动更新” 按钮， 从指定服务器自动更新黑名单库文件。

在<更新设置>页面中配置如下信息。

选项	说明
类型	指定自动更新的时间间隔，在每天的指定时间或一周中指定天的指定时间进行自动更新。
服务器类型	指定服务器类型，包括 FTP、TFTP、HTTP 或 HTTPS。
IP 地址	当选择 FTP 或 TFTP 类型服务器时，需输入服务器的 IP 地址。
URL（必填）	当选择 HTTP 或 HTTPS 类型服务器时，需要在“URL”文本框中输入服务器对应的 URL 地址。范围是 1-255 个字符。 注意：HTTP 服务器 URL 必须以“http://”开头，HTTPS 服务器 URL 必须以“https://”开头。
虚拟路由器（必填）	从下拉列表中选择服务器所属的虚拟路由器。
用户名	当选择 FTP 服务器时，输入登录 FTP 服务器的用户名。
密码	当选择 FTP 服务器时，输入登录 FTP 服务器的用户名对应的密码。
修改密码	编辑更新配置时，可以看到修改密码功能。开启后，将展示密码输入框。如需修改，输入新的密码后保存配置即可。
导入模式	指定黑名单导入模式，包括增量导入或覆盖导入。
文件名（必填）	当选择 FTP 或 TFTP 类型服务器时，在文本框中输入需要导入的文件名称。

3. 点击“确定”按钮保存所做配置。
4. 还可点击“确定并立即更新”按钮，保存配置的同时将会立即更新黑名单库。

注意:

导入或自动更新的黑名单库文件仅支持 TXT 和 CSV 格式（仅对 FTP 或 TFTP 类型服务器生效）。

导入或自动更新的黑名单文件大小不能大于 20M。

导入或自动更新的黑名单库文件时会按导入先后顺序进行冗余检测，后导入的条目若被先导入的条目完全覆盖则导入失败。

用户可以进行如下操作:

导出黑名单库：点击“导出黑名单”按钮，将当前黑名单文件导出到本地。

删除黑名单库：点击“删除黑名单库”按钮，删除当前黑名单文件。

动态 IP 黑名单

将 IP 添加到黑名单后，系统将对黑名单中的 IP 执行阻断操作，直到阻断时间结束。

配置动态 IP 黑名单，请按照以下步骤进行操作：

1. 点击“策略 > 边界流量过滤 > IP 黑名单”，进入 IP 黑名单页面。
2. 在“动态 IP 黑名单”页签中点击“新建”按钮，打开<动态 IP 黑名单>页面。

在<动态 IP 黑名单>页面中填写配置信息。

选项	说明
IP 类型	选择 IP 地址的类型，包含 IPv4 和 IPv6 以及用户名。当指定为“用户名”时，表示对指定用户的恶意流量进行过滤阻断或控制。
IP	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。
用户名	当 IP 类型指定为“用户名”时，点击下拉菜单，在展开页面中指定用户类型和名称： 指定用户：点击“AAA 服务器/角色”，选择用户所属 AAA 服务器，然后点击“选择用户”下拉菜单后选择已配

选项	说明
	置的用户名称。 指定用户组：点击“AAA 服务器/角色”，选择用户组所属 AAA 服务器，然后点击“选择用户组”下拉菜单后选择已配置的用户组名称。 指定角色：点击“AAA 服务器/角色”，选择角色后搜索或选择已配置的角色名称。 注意: 在配置前，请先完成如下配置：创建用户/用户组并绑定 IP 地址、创建角色并映射到用户、在 AAA 服务器中指定角色映射规则。
虚拟路由器	在下拉菜单中选择被阻断 IP 所属的虚拟路由器。
阻断类型	指定黑名单的阻断类型，包括“永久阻断”和“阻断时长”。默认为“永久阻断”。当选择“阻断时长”时，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 1296000 秒。

3. 点击“确定”按钮保存所做配置。

真实 IP 黑名单

一般情况下用户可以通过查看 HTTP 数据包判断客户端 IP 地址，如果客户端进行了代理设置，HTTP 数据包中查看到的源 IP 地址将会是代理服务器的 IP 地址，不是真实的客户端 IP 地址。系统发现攻击后，进行阻断时将会阻断代理服务器的 IP 地址，导致所有业务不可用。为了解决上述问题，用户可通过解析 HTTP 数据包中的 X-Forwarded-For 字段和 X-Real-IP 字段来判断真实的客户端 IP 地址。其中，X-Forwarded-For 字段用于记录真实客户端 IP 地址和每一级代理服务器的地址，X-Real-IP 字段仅用于记录真实客户端 IP 地址。

将解析出的真实客户端 IP 地址加入真实 IP 黑名单后，系统将对黑名单中的 IP 执行阻断操作，直到阻断时间结束。

配置真实 IP 黑名单，请按照以下步骤进行操作：

1. 点击“策略 > 边界流量过滤 > IP 黑名单”，进入 IP 黑名单页面。

2. 在“真实 IP 黑名单”页签中点击“新建”按钮，打开<动态 IP 黑名单>页面。

在<真实 IP 黑名单>页面中填写配置信息。

选项	说明
IP 类型	选择 IP 地址的类型，包含 IPv4 和 IPv6。
IP	在文本框中输入需要被阻断的 IP。此 IP 地址为 HTTP 协议中的 X-Forwarded-For 字段和 X-Real-IP 字段解析出的真实客户端 IP 地址。
虚拟路由器	在下拉菜单中选择被阻断 IP 所属的虚拟路由器。
阻断类型	指定黑名单的阻断类型，包括“永久阻断”和“阻断时长”。默认为“永久阻断”。当选择“阻断时长”时，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 1296000 秒。

3. 点击“确定”按钮保存所做配置。

命中统计

系统支持对黑名单命中情况进行统计，当系统有大量黑名单条目，可以通过命中统计页面查看所有命中条目及 TOP100 的黑名单条目，包括 IP 地址、作用域、首次命中时间、最后一次命中时间及命中数。

查看命中统计，请按照如下步骤进行操作：

1. 点击“策略>边界流量过滤>IP 黑名单”，进入 IP 黑名单页面。
2. 点击“命中统计”页签中查看所有命中统计的黑名单条目。

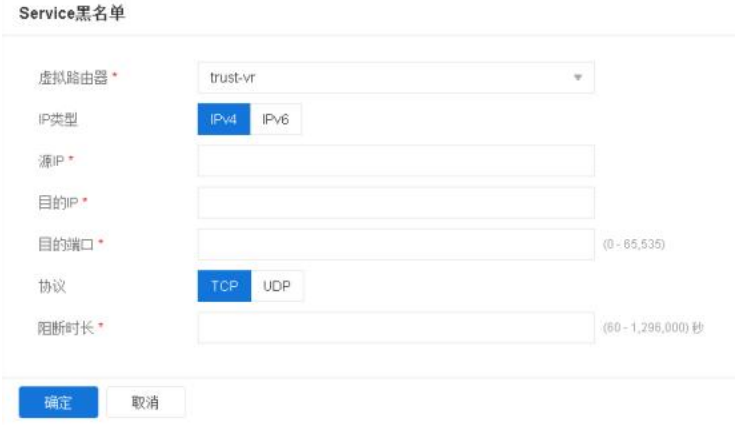
3. 点击“TOP100”按钮，在“命中数统计”页面查看命中数 TOP100 的黑名单条目。
4. 勾选需要清除的条目，点击“清空所选命中”按钮，清除指定 IP 的命中统计。点击“全部删除”按钮，清除所有命中统计。

注意：删除 IP 黑名单条目后，相应的命中统计也会清除。

Service 黑名单

配置 Service 黑名单，请按照以下步骤进行操作：

1. 点击“策略>边界流量过滤>Service 黑名单”，进入 Service 黑名单页面。
2. 点击“新建”按钮，打开<Service 黑名单>页面。



在<Service 黑名单>页面中填写配置信息。

选项	说明
虚拟路由器	在下拉菜单中选择被阻断 IP 所属的虚拟路由器。
类型	选择 IP 地址的类型，包含 IPv4 和 IPv6。
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 1296000 秒。

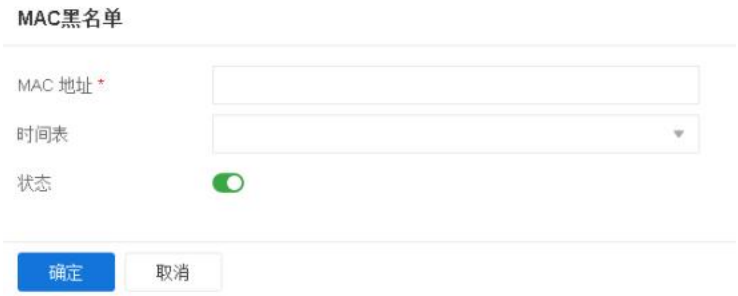
3. 点击“确定”按钮，保存所做配置并返回上一级页面。

MAC 黑名单

配置 MAC 黑名单功能，请按照以下步骤进行操作：

1. 点击“策略>边界流量过滤>MAC 黑名单”，进入 MAC 黑名单页面。

2. 点击列表上方“新建”按钮，打开<MAC 黑名单>页面。



在<MAC 黑名单>页面中填写配置信息。

选项	说明
MAC 地址	在文本框中输入需要添加到黑名单的主机的 MAC 地址。
时间表	在“时间表”下拉菜单中选择需要的时间表。该条黑名单将会在时间表指定的时间范围内生效。
状态	指定 MAC 黑名单的开启状态。

3. 点击“确定”按钮完成配置。

注意: 不支持配置组播 MAC 地址。

IP 信誉过滤

配置 IP 信誉过滤功能，请按照以下步骤进行操作：

1. 点击“策略>边界流量过滤>IP 信誉过滤”，进入 IP 信誉过滤页面。

2. 点击列表上方“新建”按钮，打开<IP 信誉过滤>页面。

在<IP 信誉过滤>页面中填写配置信息。

选项	说明
作用域	指定 IP 信誉过滤作用于全局、指定安全域或指定虚拟路由器。当选择“安全域”或“虚拟路由器”时，在相应的下拉列表中选择需要的条目。
分类	在分类中勾选需要开启的风险 IP 类型：僵尸主机、垃圾邮件、Tor 节点、失陷主机、代理服务、扫描、暴力破解、DDos 攻击者，对相应的 IP 进行阻断。

3. 点击“确定”按钮完成配置。

配置 IP 白名单

系统支持全局白名单和边界流量过滤白名单。全局白名单作用于全局，对于在全局白名单中的 IP 地址，系统不进行安全检测，直接放行。边界流量过滤白名单作用于边界流量过滤功能，对于在边界流量过滤白名单中的 IP 地址，系统不做边界流量过滤检测，不进行阻断。

> 注意:
>
> NAT 转换和流量配额功能不受全局白名单影响。
>
> 配置 NAT 转换后，由于系统在 NAT 转换前后各进行一次边界流量过滤检测，若转换前后的 IP 地址并未都设置为全局白名单，则流量可能被黑名单拦截。

配置 IP 白名单，请按照以下步骤进行操作：

1. 点击“策略 > 边界流量过滤 > IP 白名单”，进入 IP 白名单页面。
2. 点击列表上方“新建”按钮，进入<IP 白名单> 页面。

在<IP 白名单>页面中填写配置信息。

选项	说明
IP 类型	选择 IP 地址的类型，包含 IPv4 和 IPv6。
IP 掩码	在文本框中输入需要添加到白名单的 IP 地址及网络掩码。
全局白名单	启用后，白名单将在全局生效。
边界流量过滤白名单	指定白名单生效于全域、指定安全域或指定虚拟路由器。 当选择“全域”时，白名单将在所有的安全域或虚拟路由器中（即在边界流量过滤模块）生效；当选择“安全域”或“虚拟路由器”时，须在相应下拉列表中指定一个“安全域”或“虚拟路由器”。指定后，白名单将在指定的安全域或虚拟路由器中生效。

3. 点击“确定”按钮保存所做配置。

全局检索

查看指定 IP 地址的黑白名单条目，请按照以下步骤进行操作：

1. 点击“策略>边界流量过滤>全局检索”，进入全局检索页面。
2. 在 IP 地址文本框中输入需要查询的 IP 地址，点击“搜索”按钮，跳转到相应的黑名单页签中查看对应的条目。

配置

配置黑名单全局配置，请按照以下步骤进行操作：

1. 点击“策略>边界流量过滤>配置”，进入黑名单全局配置页面。
2. 点击黑名单日志的“启用”按钮，开启黑名单的日志功能，可在威胁日志页面进行查看。
3. 点击会话重匹配的“启用”按钮，当用户添加、修改或者删除黑名单时，会话会重新匹配黑名单。
4. 点击 IP 黑名单 TCP 重置的“启用”按钮，系统会向命中黑名单的 TCP 流量 IP 地址发送 TCP-RST 报文，从而阻断该 IP 地址。

第 10 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，设备可防御外部攻击，减少对内网安全造成的损失。

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（HTTP、SMTP、POP3、IMAP4、FTP、以及 SMB）并对其进行病毒防护。可扫描文件类型包括存档文件（包含压缩存档文件，支持压缩类型有 GZIP、BZIP2、TAR、ZIP 和 RAR）、PE、HTML、MAIL、RIFF、ELF、PDF、MS OFFICE、Raw Data 和 Others。其中 Other 表示对除页面可选择的文件类型以外的其他类型文件进行病毒扫描，主要包括 GIF，BMP， PNG， JPEG， FWS， CWS， RTF， MPEG，Ogg， MP3，wma， WMV， ASF， RM 等。

入侵防御：可检测并防护针对主流应用层协议（DNS、FTP、HTTP、POP3、SMTP、TELNET、MYSQL、MSSQL、ORACLE、NETBIOS 等）的入侵攻击、基于 Web 的攻击行为以及常见的木马攻击。

攻击防护：可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。

加密流量检测：对加密流量的特征数据进行提取和检测，以及时识别威胁流量。

设备支持基于安全域和基于策略的威胁防护方式。

为安全域配置威胁防护后，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威胁防护配置进行检查并做相应的动作响应。

为策略配置威胁防护后，系统将会对与策略规则相匹配的流量根据威胁防护配置进行检查和响应。

若安全域和策略中均配置了威胁防护，策略中的配置项将有更高的优先权；在安全域配置中，目的安全域的优先权将高于源安全域。

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、边界流量过滤特征库。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。用户可以根据需要更改特征库更新配置。

特征根据严重程度分为三个级别（安全级别），分别为严重（Critical）、警告（Warning）和信息（Informational），各级别说明如下。 用户可根据特征严重程度，设置系统对该特征攻击所将采取的行为。

严重（Critical）：严重的攻击事件，例如缓冲区溢出。

警告（Warning）：具有一定攻击性的事件，例如超长的 URL。

信息（Informational）：一般事件，例如登录失败。

病毒过滤

系统的病毒过滤功能能够为用户提供高速、高性能以及低延迟的病毒过滤解决方案。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（HTTP、FTPSMTP、POP3、IMAP4 以及 SMB）并对其进行病毒防护。对于 SMB 协议，系统还支持断点续传场景下的病毒文件过滤和阻断。可扫描文件类型包括存档文件（包含压缩存档文件，支持压缩类型有 GZIP、BZIP2、TAR、ZIP 和 RAR）、PE、HTML、MAIL、RIFF、ELF、PDF、MS OFFICE、Raw Data 和 Others。其中 Other 表示对除页面可选择的文件类型以外的其他类型文件进行病毒扫描，主要包括 GIF，BMP， PNG， JPEG， FWS， CWS，RTF， MPEG，Ogg， MP3， wma， WMV， ASF， RM 等。

如设备开启了 IPv6，病毒过滤功能支持扫描 IPv6 地址的病毒。

系统的病毒过滤特征库包含百万余种以上病毒特征，支持病毒过滤特征库的默认每日自动升级，也可以手动实时升级。

配置病毒过滤

本章节包括如下内容：

病毒过滤配置准备工作

配置病毒过滤功能

配置病毒过滤全局参数

配置病毒过滤功能

系统支持基于安全域和基于策略的病毒过滤配置方式：

为安全域配置病毒过滤规则后，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病毒过滤规则配置进行病毒过滤检查。

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规则配置进行病毒过滤检查。

若安全域和策略中均配置了病毒过滤规则，策略中的配置项将有更高的优先权；在安全域配置中，目的安全域的优先权将高于源安全域。

系统还支持绑定病毒过滤规则到 ZTNA 策略，对与 ZTNA 策略相匹配的流量进行病毒检测和处理。

基于安全域的配置方式，请按照以下步骤进行操作：

1. 创建安全域。

2. 在<安全域配置>页面中，点击“威胁防护”，展开威胁防护配置项。
3. 点击“病毒过滤”后的“启用”按钮；并可根据自身需要，点击“模板”下拉菜单选择已配置好的病毒过滤规则或默认规则；也可点击“模板”下拉菜单中 ⊕ 按钮，新建病毒过滤规则。关于配置病毒过滤规则，请参阅 配置病毒过滤规则。
4. 点击“确定”完成配置。

基于策略的病毒过滤配置方式，请按照以下步骤进行操作：

1. 创建策略。
2. 在<策略配置>页面中，点击“防护状态”，展开防护状态配置项。
3. 勾选“病毒过滤”后的“启用”按钮；并可根据自身需要，点击“模板”下拉菜单选择已配置好的病毒过滤规则或默认规则；也可点击“模板”下拉菜单中 ⊕ 按钮，新建病毒过滤规则。关于配置病毒过滤规则，请参阅 配置病毒过滤规则。
4. 点击“确定”完成配置。

配置病毒过滤规则

配置病毒过滤规则，请按照以下步骤进行操作：

1. 点击“对象 > 病毒过滤 > 模板”。
2. 点击“新建”按钮。

在<病毒过滤规则配置>页面，填写病毒过滤规则配置信息。

选项	说明
名称	指定病毒过滤规则名称。长度为 1-31 个字符。
扫描文件类型	指定系统将扫描的文件类型，可以是 GZIP、JPEG、MAIL、RAR、HTML 等。其中 Other 表示对除页面可选择的文件类型以外的其他类型文件进行病毒扫描，主要包括 GIF，BMP， PNG，JPEG， FWS， CWS， RTF， MPEG，Ogg， MP3， wma，WMV， ASF， RM 等。
扫描协议类型	指定系统将扫描的协议类型（HTTP、SMTP、POP3、IMAP4、FTP、SMB）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。
恶意网站访问控制	点击“启用”按钮，开启策略或安全域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，根据病毒过滤的防护级别，系统自带三条默认病毒过滤规则：predef_low、predef_middle、predef_high，默认规则不允许执行编辑或删除操作。

predef_low 扫描最常见的文件类型，防护级别最低；predef_middle 扫描中等数量的文件类型，防护级别中等；predef_high 扫描全部文件类型，防护级别最高。

根据协议特点，邮件传输类协议推荐防护动作为填充魔术字，其他类推荐防护动作为重置连接。

克隆病毒过滤规则

系统支持将某一病毒过滤规则快速克隆，用户只要将克隆的病毒过滤规则的部分参数进行修改，即可生成一条新的病毒过滤规则。

克隆病毒过滤规则，请按照以下步骤进行操作：

1. 选择“对象 > 病毒过滤 > 模板”。
2. 选中列表中的一条病毒过滤规则。
3. 点击列表上方的“克隆”按钮，按钮下方将出现“名称”文本框，输入新克隆的病毒过滤规则名称。
4. 列表中将生成一条克隆的病毒过滤规则。

配置病毒过滤全局参数

病毒过滤全局参数配置包含开启/关闭病毒过滤功能以及配置解压控制功能。

开启/关闭病毒过滤功能

开启/关闭病毒过滤功能，请按照以下步骤进行操作：

1. 点击“对象 > 病毒过滤 > 配置”。
2. 选中/取消选中“启用”按钮，开启/关闭设备的病毒过滤功能。
3. 在“日志聚合类型”选项后，选择病毒过滤日志聚合的类型。

   选择“不聚合”，系统将对每一条病毒过滤日志分别存入数据库，不进行日志聚合。

   选择“源 IP,目的 IP”并指定日志聚合的时间粒度，系统将对同源且同目的的病毒过滤日志，按照指定的时间粒度进行聚合，然后存入数据库一次，不再重复存入多次，聚合的日志数量将展示在“攻击次数”中。
4. 配置完成，点击“确定”按钮。

注意: 病毒过滤功能的开启与关闭需要重启设备生效，日志聚合的配置不需要重启。

配置解压控制功能

配置解压控制功能后，系统会对传输的压缩文件进行解压，并能对超出最大压缩层数的文件以及加密压缩文件按照指定的动作进行处理。支持解压缩的文件格式包括 RAR、ZIP、TAR、GZIP 及 BZIP2。配置解压控制功能，请按照以下步骤进行操作：

1. 点击“对象 > 病毒过滤 > 配置”。
2. 点击“压缩文件处理”后的“配置”按钮，打开<解压控制>页面。

在<解压控制>页面进行配置。

选项	说明
解压缩	点击/不点击“启用”按钮，开启/关闭解压缩功能。
最大压缩层	默认情况下，系统可以对最多 5 层压缩嵌套的文件进行扫描（含 5 层），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	指定对超出最大压缩层限制的压缩文件的处理动作。可选择： 只记录日志 - 只生成相关日志信息。该行为是系统默认行为。 重置连接 - 重置压缩文件连接。
加密压缩文件	指定对加密压缩文件的处理方式，可选择： 无动作 - 不对加密压缩文件进行病毒过滤特殊处理，根据病毒过滤规则配置，系统可能会继续对加密压缩文件进行扫描。 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。

3. 配置完成，点击“确定”按钮。

注意: 对于包含 docx、pptx，xlsx、jar、apk 格式的压缩文件，当“超出行为”被指定为重置连接时，用户需要将最大压缩层数增加 1 层，以避免无法下载该压缩文件的问题。

入侵防御

入侵防御系统（Intrusion Prevention System）简称 IPS，能够实时监控多种网络攻击并根据配置对网络攻击进行阻断等操作。

系统的入侵防御功能能够实现完整的基于状态的检查，从而极大降低误报率。当设备开启多项应用层数据检测功能时，启用入侵防御功能不会导致设备性能的明显下降。另外，系统默认每天通过特征服务器自动更新特征库，保证特征的完整性和正确性。

> 如接口开启了 IPv6 功能，IPS 支持对 IPv6 地址进行扫描。

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：

> 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。
>
> 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。

特征介绍

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。

配置入侵防御

配置入侵防御功能

系统支持基于安全域和基于策略的入侵防御配置方式。

系统还支持绑定入侵防御规则到 ZTNA 策略，对与 ZTNA 策略相匹配的流量进行入侵防御检测和处理。

基于安全域的入侵防御配置，请按照以下步骤进行操作：

1. 创建或编辑安全域。
2. 在<安全域配置>页面内，点击“威胁防护”，展开威胁防护配置项。
3. 点击“入侵防御”后的“启用”按钮；并可根据自身需要，点击“模板”下拉菜单选择已配置好的入侵防御规则或默认规则；也可点击下拉菜单中的 ⊕ 按钮，新建入侵防御规则。关于配置入侵防御规则，请参阅配置入侵防御规则。
4. 在配置基于安全域的入侵防御功能时，可以在“防护方向”中选择方向（流入、流出或者双向），使入侵防御规则对指定安全域指定方向的流量生效。
5. 点击“确定”完成配置。

基于策略的入侵防御配置，请按照以下步骤进行操作：

1. 创建或编辑策略。
2. 在<策略配置>页面内，点击“防护状态”，展开防护状态配置项。
3. 点击“入侵防御”后的“启用”按钮；并可根据自身需要，点击“模板”下拉菜单选择已配置好的入侵防御规则或默认规则；也可点击下拉菜单中的 ⊕ 按钮，新建入侵防御规则。关于配置入侵防御规则，请参阅配置入侵防御规则。
4. 点击“确定”完成配置。

配置入侵防御规则

用户可使用系统默认的入侵防御规则，也可自行创建规则。系统提供三个默认的入侵防御规则，分别为 predef_default、predef_loose 和 predef_critical。默认入侵防御规则不可被删除和编辑。

predef_default 规则包含可信度为中和高的所有 IPS 特征，对威胁进行检测，且处理行为默认为各 IPS 特征的默认动作；

predef_loose 规则包含所有类型的 IPS 特征，对威胁进行检测且处理行为默认为只记录日志；

predef_critical 规则包含最新时段高危类型的攻击检测，对检测效果要求严格，且处理行为默认为重置。

系统支持创建最多 64 个自定义入侵防御规则，每个非根 VSYS 下可以创建最多 4 个自定义入侵防御规则。

配置入侵防御规则，请按照以下步骤进行：

1. 点击“对象 > 入侵防御 > 模板”。
2. 点击“新建”按钮创建新的入侵防御规则。如需编辑已存在的入侵防御规则，勾选其复选框，并点击“编辑”。如需查看某条规则的配置，可单击此条规则的名称。

3. 在“名称”文本框输入新建规则的名称。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. 根据需要，点击“全局抓包”后的“启用”按钮，将该规则下的所有协议都启用抓包。
5. 根据需要，填写改规则的描述信息。
6. 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。新建特征集规则时，可按需选择过滤特征集和选择特征集两种方式，对特征库进行筛选与检索，从而选择出需要使用的特征集。

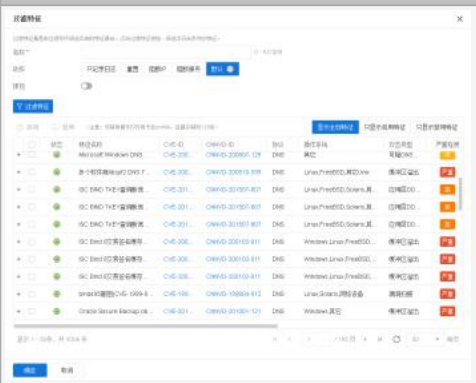
   过滤特征集：由过滤条件筛选出来的特征集合。点击过滤特征按钮，筛选出符合条件的特征，用户可以通过该方式快速选择出系统已分类的特征。

   选择特征集：在特征库中一一选择出来的特征集合，用户可以通过该方式快速选择某个特定的特征。

7. **新建特征集规则，点击“新建”按钮**，并选择“过滤特征”或“选择特征”。

选项	说明
名称	指定特征集的名称。
动作	指定对匹配特征集的异常流量采取的动作。 只记录日志：系统发现攻击后仅记录日志信息。

选项	说明
	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：阻断攻击者的 IP 地址并设置阻断时间。 阻断时间：默认值为 60，取值范围为 60 到 3600，单位为秒。若需设置更长的阻断时间，可选择更大的时间单位（“小时”或者“天”）并指定数值，也可选择“永久”对攻击者 IP 进行永久阻断。 阻断服务：阻断攻击者的服务并设置阻断时间。 阻断时间：默认值为 60，取值范围为 60 到 3600，单位为秒。若需设置更长的阻断时间，可选择更大的时间单位（“小时”或者“天”）并指定数值，也可选择“永久”对协议/源 IP/目的 IP/目的端口进行永久阻断。 默认：发现攻击后，系统将按照特征规则中的默认动作进行处理。新建特征集时，系统推荐的处理动作为“默认”。
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。
过滤特征	当选择新建时，选择“过滤特征”的方式时：在新页面中，点击“过滤特征”按钮，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，可信度，发布年份，影响软件，公告板。用户可继续选择各分类中的子类从而筛选出相关联的特征。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 200211 的规则，在操作系统这个维度上，同时属于 Linux, FreeBSD, 其他 Linux。 用户可点击特征 ID 查看特征详细信息，同时用户可选择某一条或多条特征，点击“禁用”按钮，来禁用特征规则；点击“启用”按钮，可重新启用特征规则。**注意**：此处的启用/禁用状态只作用于当前模板，全局状态不受影响。

选项	说明
	 选择类别及其子类别时，注意如下事项： 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。
选择特征	当选择新建时，选择“选择特征”的方式时：在新页面中，在“关键词”搜索框中，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，特征将加入<已选特征>标签页中，代表此特征集规则包含的特征。 检索出特征后，用户也可勾选特征，然后点击“启用”、“禁用”按钮，来禁用或重新启用特征。此处的启用/禁用状态只作用于该模板，全局状态不受影响。
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	

选项	说明
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 > 默认。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。 由于新建特征集时系统默认的处理动作为“默认”，其严格程度是最低的，所以只要用户重新选择了其他动作（阻断 IP 、 阻断服务 、 重置 、 只记录日志 ），系统处理攻击时，总是会优先处理用户重新设置的动作。例如：特征集 A 采用默认动作，而某一特征的默认动作为“重置”，而另一特征集 B 的动作被用户设置为了“只记录日志”，那么最终对匹配该特征的攻击的处理方式为用户设置的“只记录日志”。 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。 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。	

8. 点击“确认”完成特征集配置。用户可创建多个特征集配置。

9. 在“禁用特征”部分，查看该模板中禁用的特征集列表。在列表中，勾选一条或多条特征，然后点击“启用”按钮可重新启用该特征。

10. 在“口令防护”配置部分，点击“弱口令检测”后的启用按钮，系统将对该模板下的 FTP/Telnet/POP3/IMAP/SMTP 协议的明文密码进行密码强度检测，符合弱口令检测条件的密码将被视为弱密码，系统发出报警日志，可防止弱密码所引起的安全隐患。点击“设置”，可对弱口令检测参数进行配置。

设置弱口令检测参数

选项	说明
密码长度	指定系统所检测的密码长度，小于该长度的密码将被检测为弱密码。默认值为 6，取值范围为 6-50。
密码字符种类	指定系统所检测的密码字符种类数。字符种类包括：数字、大写字母、小写字母和符号，少于设定字符种类数的密码将被检测为弱密码。默认值为 2，取值范围为 1-4。
其他情形	弱密码检测的其他情形包括：账号与密码相同、连续字符和 FTP 匿名登录。 账号与密码相同：点击启用按钮后，与账号相同的密码将被检测为弱密码。 连续字符检测：点击启用按钮后，密码长度小于 10 位且连续相同或顺序字符位数大于等于 8 位的密码将被检测为弱密

选项	说明
	码，如 1aaaaaaaa，1abcdefgh，a87654321。 FTP 匿名登录：点击启用按钮后，当用户使用 FTP 匿名登录时，系统将检测其为弱密码。
指定弱密码	用户可自行指定弱密码。当系统检测到的密码与指定弱密码相匹配时，则认定该密码为弱密码。最多可指定 100 条弱密码。

11. 在“口令防护”配置部分，可对 FTP/MSRPC/POP3/SMTP/SUNRPC/Telnet/IMAP/SSH/LDAP/SMB/VNC/RDP 协议下的暴力破解攻击进行阻断设置。

点击“设置”，在协议后点击启用按钮，进行配置

选项	说明
FTP/MSRPC/POP3/SMTP/SUNRPC/Telnet/IMAP/SSH/LDAP/SMB/VNC/RDP	**在暴力破解下阻断配置**：如果 5 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 5 分钟登录上限值**：指定每 5 分钟内允许认证/登录失败的次数的最大值。 **动作**：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。 **阻断时间**：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。默认值为 60，取值范围为 60 到 3600，默认单位为秒。 **阻断时间单位**：若需设置更长的阻断时间，可选择更大的时间单位（“小时”或者“天”）并指定数值，也可选择“永久”对攻击者 IP 或者协议/源 IP/目的 IP/目的端口进行永久阻断。

12. **在“反弹 shell 检测”部分，点击 ▶ 展开页面，反弹 shell 检测功能进行配置。**

选项	说明
反弹 shell 检测	点击启用按钮，系统将对反弹 shell 攻击进行检测和防护，若发现攻击行为，系统将按照用户所设置的动作进行防护。
动作	指定系统对反弹 shell 攻击的防护动作。 只记录日志 - 系统发现反弹 shell 攻击后仅记录日志信息； 重置 - 发现反弹 shell 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；

选项	说明
	阻断 IP - 阻断反弹 shell 攻击者的 IP 地址并设置阻断时间； 阻断时间：默认值为 60，取值范围为 60 到 3600，单位为秒。若需设置更长的阻断时间，可选择更大的时间单位（“小时”或者“天”）并指定数值，也可选择“永久”对攻击者 IP 进行永久阻断。
模式	指定系统对反弹 shell 攻击的检测和防护模式。 低误报：系统对反弹 shell 攻击的关键词进行扫描检测时，若关键词被命中的次数超过 4 次才进行日志上报，可用于系统性能要求比较高的场景。 高检测：系统对反弹 shell 攻击的关键词进行扫描检测时，若关键词被命中的次数超过 2 次就进行日志上报，可用于对攻击检测要求较高的场景。

13. 点击“协议配置”，展开协议配置项。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。

点击“HTTP”，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，可进行如下处理： 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。 动作：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，可进行如下处理： 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。

选项	说明
	动作：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，配置<WebServer>部分。

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。每个入侵防御规则最多配置 32 个 Web 服务器防护规则，不包括 default 规则。

在<Web 服务器配置>页面中新建 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”，打开<域名设置>页面，在该页面中点击“新建”，弹出可编辑行，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。
高频访问限制	点击“启用”按钮，开启 Web 服务器高频访问限制功能。启用该功能后，系统会对频繁访问某 URL 路径的源 IP 进行限制，当其访问频率超过设定的阈值时，阻断该请求的源 IP，该 IP 将无法访问 Web 服务器。 阈值：指定单个源 IP 每分钟访问 URL 路径的最大次数。当某源 IP 的访问的频率超过此阈值，系统将会对此 IP 进行阻断。其取值范围为 1-65535 次/分钟。 URL 路径：点击“URL 路径”链接，打开<URL 路径设置>页面。在对话框中输入 URL 路径，进行添加或删除。配置后，包含该路径名称的所有路径也将被统计。系统会对访问这些路径的 HTTP 请求进行访问频率检查。若 HTTP 请求的访问频率超过阈值，会阻断该请求的源 IP，该 IP 将无法访问 Web 服务器。例如：配置/home/ab，系统将对访问 /home/ab/login 与/home/abc/login 的 HTTP 请求进行频率检查。URL 路径不支持带主机名或域名的路径格式，例如：不能配置 www.baidu.com/home/login.html，应该配置

选项	说明
	/home/login.html，而 www.baidu.com 应该配置在对应的 Web 服务器的域名设置里。系统最多允许配置 32 条 URL 路径，每条路径长度取值范围为 1-255 字符。
敏感目录扫描	选中“启用”开启 Web 服务器敏感目录扫描检测功能。 敏感目录扫描是一种针对 Web 服务器的常见攻击手段，攻击者使用目录扫描工具对 Web 服务器内的站点进行遍历，以获取 Web 服务器的目录结构、后台文件、备份文件等敏感信息。 若攻击者试图对 Web 服务器进行敏感目录扫描，Web 服务器将返回大量状态码为 404 的响应报文。此时系统将对每分钟 Web 服务器返回的“404”响应报文进行计数：①若该数目大于 10 次，系统则对所有的 HTTP 请求报文中的 URL 进行解析，并将解析后的 URL 路径与内置的敏感文件字典进行匹配。若解析后的 URL 路径命中敏感文件字典的次数超出指定的阈值，系统将按照用户指定的防护动作进行处理（只记录日志/重置/阻断 IP/阻断服务）；②若该数目大于等于 100 次，系统直接判定该行为是敏感目录扫描攻击，并按照指定的防护动作进行处理（只记录日志/重置/阻断 IP/阻断服务）。 阈值：指定系统防护敏感目录扫描攻击的阈值。指定后，当每分钟 URL 路径命中敏感文件字典的次数超过该阈值时，系统将按照用户指定的动作进行防护。 默认值为 10，取值范围为 10-100 次/分钟。 动作：指定系统对敏感目录扫描攻击的防护动作。 只记录日志 - 系统发现敏感目录扫描后，只记录日志。 重置- 系统发现敏感目录扫描后重置连接（TCP）或者发送目标不可达包（UDP）并且记录日志信息。 阻断 IP - 阻断攻击者的 IP 地址并设置阻断时间。默认阻断时间为 60 秒，取值范围为 60 到 3600，单位为秒。若需设置更长的阻断时间，可选择更大的时间单位（“小时”或者“天”）并指定数值，也可选择“永久”对攻击者 IP 进行永久阻断。 阻断服务 - 阻断攻击者的服务并设置阻断时间。默认阻断时间为 60 秒，取值范围为 60 到 3600，单位为秒。若需设置更长的阻断时间，可选择更大的时间单位（“小时”或者“天”）并指定数值，也可选择“永久”对协议/源 IP/目的 IP/目的端口进行永久阻断。
SQL 注入检查	点击“启用”按钮，开启 Web 服务器 SQL 注入检查功能。

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。 动作：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。 检查点：为 SQL 注入检查指定检查点，可以为 URI、Cookie、Referer 或者 Post 。
XSS 注入检查	点击“启用”按钮，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。 动作：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。 检查点：为 Web 服务器 XSS 注入检查指定检查点，可以为 URI、Cookie、Referer 或者 Post 。
外链检查	点击“启用”按钮，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，打开<外链特例配置>页面，在该页面配置的 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。 动作：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。
盗链检查	点击“启用”按钮，开启盗链检查功能。系统通过对 HTTP 报文的首部进行检查，获知 HTTP 请求的来源站点。如果来源站点在“盗链例外”列表中，则放行；否则进行日志记录或重置连接。从而控制 Web 站点不被其他站点盗链和防止 CSRF(Cross Site Request

选项	说明
	Forgery 跨网站请求欺骗)攻击发生。 盗链例外：点击“ 盗链例外”链接，打开< 盗链例外配置>页面，在该页面配置的 URL 是可以引用 Web 站点的。每个 Web 服务器防护规则最多可配置 32 个 URL。 动作：为发生盗链行为的 HTTP 请求指定相应的动作，可以为“仅记录日志”或者“重置”。“仅记录日志”对发生盗链行为的 HTTP 请求仅记录日志信息。“重置”对发现发生盗链行为的 HTTP 请求进行重置连接（TCP）或者发送目标不可达包（UDP）并且记录日志信息。
Iframe 检查	点击“启用”按钮，开启 iframe 检查功能。开启 iframe 检查后，系统会根据限定的 iframe 高度和宽度来检查 HTML 页面中的 iframe，当高度和宽度中任意一项小于或等于限定值，系统将会识别为隐藏的 iframe 攻击发生，从而进行记录日志或重置连接。 高度：指定 iframe 的限定的高度值，取值范围为 0-4096px。 宽度：指定 iframe 的限定的宽度值，取值范围为 0-4096px。 动作：为隐藏 iframe 行为的 HTTP 请求指定相应的动作，可以为“仅记录日志”或者“重置”。“仅记录日志”指定发生隐藏 iframe 行为的 HTML 页面仅记录日志信息。“重置”指定隐藏 iframe 行为的 HTTP 请求进行重置连接（TCP）或者发送目标不可达包（UDP）并且记录日志信息。
访问控制	点击“启用”按钮，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，打开<访问控制配置>页面，在该页面配置 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。 动作：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

选项	说明
	（UDP）并且记录日志信息。
CC 防护	点击“启用”按钮，开启 CC 防护功能，保护 Web 服务器免受 HTTP Request Flood 攻击。CC 防护支持 IPv6 流量的地址统计。 请求阈值：设置请求阈值。对于被保护的域名，如果连续 20s 之内，系统收到的单个源 IP 的 HTTP 请求每秒都超过请求阈值，则系统判定 CC 攻击发生。 系统支持 HTTP 请求的源 IP、x-forwarded-for、x-real-ip 字段来作为统计对象统计，当每秒被访问次数超过阈值且持续 20s 时，系统判定 CC 攻击发生。 x-forwarded-for：选择“无”，不对 x-forwarded-for 字段的值进行统计，即按照 HTTP 请求的源 IP 进行统计。选择“第一个”，统计对象为 x-forwarded-for 字段的第一个值，选择“最后一个”，统计对象为 x-forwarded-for 字段的最后一个值，选择“全部”，统计对象为 x-forwarded-for 字段中全部的值。 x-real-ip：选择是否对 x-real-ip 字段的值进行统计。 判定发生攻击后，用户可采取如下措施： 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：不认证，即系统对发起 HTTP 请求的源 IP 不进行认证；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：点击“启用”按钮，不对爬虫进行认证。 访问限速：点击“启用”按钮，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。若需设置更长的阻断时间，可选择更大的时间单位（“小时”或者“天”）并指定数值，也可选择

选项	说明
	“永久”对攻击者 IP 进行永久阻断。“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：点击“启用”按钮，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。若需设置更长的阻断时间，可选择更大的时间单位（“小时”或者“天”）并指定数值，也可选择“永久”对攻击者 IP 进行永久阻断。“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。

点击“DNS”，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，可以进行如下处理： 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。 动作：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。

点击“FTP”，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，可以进行如下处理： 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。

选项	说明
	动作：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**：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，可以进行如下处理： 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。 动作：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，可以进行如下处理： 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。 动作：只记录日志；重置 ；阻断 IP；阻断服务。

点击“MSRPC”，对 MSRPC 协议进行配置。

选项	说明
MSRPC	**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，可以进行如下处理： 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。 动作：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。 **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，可以进行如下处理： 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。

选项	说明
	动作：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，可以进行如下处理： 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。 动作：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。

点击“POP3”，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，可以进行如下处理： 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。 动作：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，可以进行如下处理： 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。 动作：只记录日志；重置 ；阻断 IP；阻断服务。

选项	说明
	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，可以进行如下处理： 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。 动作：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，可以进行如下处理： 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。 动作：只记录日志；重置 ；阻断 IP；阻断服务。

点击“SMTP”，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，可以进行如下处理： 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。 动作：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，可以进行如下处理： 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。 动作：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，可以进行如下处理：

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。 动作：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，可以进行如下处理： 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。 动作：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，可以进行如下处理： 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。 动作：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，可以进行如下处理： 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。 动作：只记录日志；重置；阻断 IP；阻断服务。 **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，可以进行如下处理： 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。 动作：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，可以进行如下处理： 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。 动作：只记录日志；重置；阻断 IP；阻断服务。

点击“SUNRPC”，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。

选项	说明
	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，可以进行如下处理： 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。 动作：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。

点击“Telnet”，对 Telnet 协议进行配置。

选项	说明
Telnet	**扫描最大长度**：对 Telnet 协议报文进行扫描时，扫描的最大长度。 **协议异常检查**：对 Telent 协议报文进行分析，查看协议是否存在异常。 对于异常报文，可以进行如下处理： 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。 动作：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。 **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，可以进行如下处理： 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。 动作：只记录日志；重置 ；阻断 IP；阻断服务。

14. 点击“保存”完成协议配置。
15. 点击“确定”完成入侵防御规则配置。

克隆入侵防御规则

系统支持将某一入侵防御规则快速克隆，用户只要将克隆的入侵防御规则的部分参数进行修改，即可生成一条新的入侵防御规则。

克隆入侵防御规则，请按照以下步骤进行操作：

1. 选择“对象 > 入侵防御 > 模板”。
2. 选中列表中的一条入侵防御规则。
3. 点击列表上方的“克隆”按钮，按钮下方将出现“名称”配置框，输入新克隆的入侵防御规则名称。
4. 列表中将生成一条克隆的入侵防御规则。

配置入侵防御全局参数

入侵防御全局参数配置包括：

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

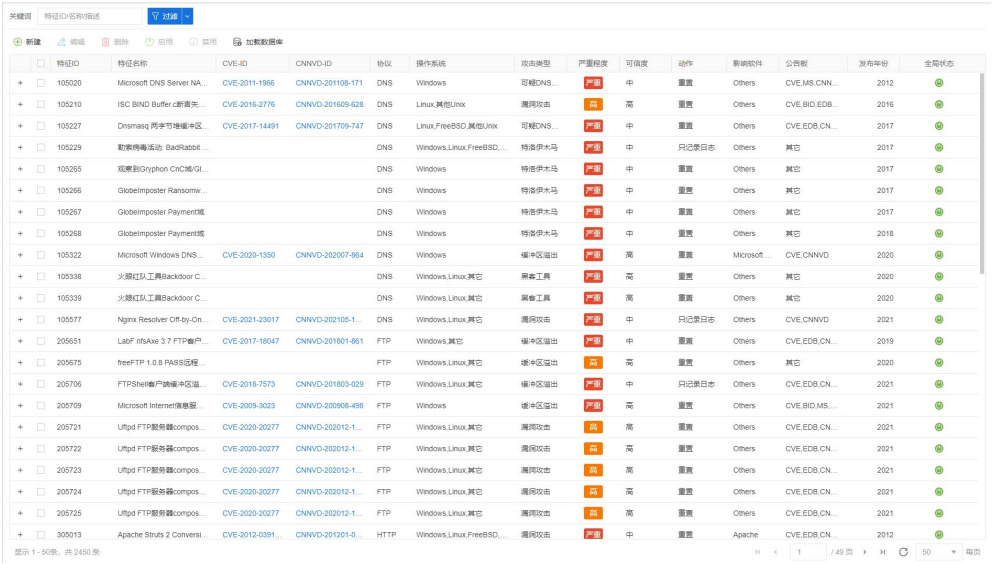
点击“对象 > 入侵防御 > 配置”进行入侵防御全局配置。配置完成后，点击“确定”按钮。

选项	说明
入侵防御	点击/不点击“启用”按钮开启/关闭设备的入侵防御防护功能。 配置后，需要重启设备。
日志聚合类型	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“日志聚合类型”下拉菜单中选择聚合类型： 不聚合 - 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。
日志聚合时间粒度	指定入侵防御同类型（上面指定的聚合类型）的威胁日志存入数据库的时间粒度。指定后，系统将对同一时间粒度内、同一类型的日志只存入数据库一次，不再重复存入多次。取值范围为 10-600 秒。
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

选项	说明
	攻击做重置和阻断操作。

管理特征规则

打开“对象 > 入侵防御 > 特征列表”，显示特征列表页。



支持使用过滤条件检索特征，对特征列表的操作，包括：查看/新建/编辑/删除/启用/禁用特征。

检索特征

点击特征库列表上方 过滤 添加过滤条件，并在过滤条件的搜索框中输入搜索内容，可对特征规则进行检索查询。过滤条件包括：当前状态、操作系统、严重程度、可信度、特征类型、影响软件、公告板、发布年份、关键词以及 CVE 和 CNNVD 编号。

说明：系统支持 CNNVD 和 CVE 两种标准漏洞库中的漏洞信息检索并支持快速链接到公共信息漏洞库。系统每周将会从 CNNVD/CVE 官方网站获取漏洞信息，并保存到特征库，然后每周发布更新一次特征库版本，及时与公共标准漏洞库保持同步。

> CNNVD：（China National Vulnerability Database of Information Security,简称“CNNVD”）国家信息安全漏洞库，是中国信息安全测评中心为切实履行漏洞分析和风险评估的职能，负责建设运维的国家信息安全漏洞库，为中国信息安全保障提供基础服务。CNNVD 兼容性服务是 CNNVD 面向国内外信息安全从业单位，对其产品/服务等涉及的漏洞信息进行规范性评估与认证的服务。通过 CNNVD 兼容性服务的信息安全产品/服务，可实现其漏洞信息拥有统一的规范性命名与标准化描述，从而提高和加强国内信息安全行业漏洞信息资源的共享与服务能力。系统通过使用 CNNVD 标识，实现了安全平台与漏洞信息的交叉引用，提高了产品的安全服务能力。

CVE：(Common Vulnerabilities & Exposures）,公共漏洞和暴露。CVE 类似一张字典表，包含大多数广泛认同的信息安全漏洞或者已经暴露出来的弱点。CVE 为每个漏洞和暴露确定了唯一的名称和一个标准化的描述。用户可以通过在 CVE 漏洞库中查到相应修补的信息，解决安全漏洞问题。

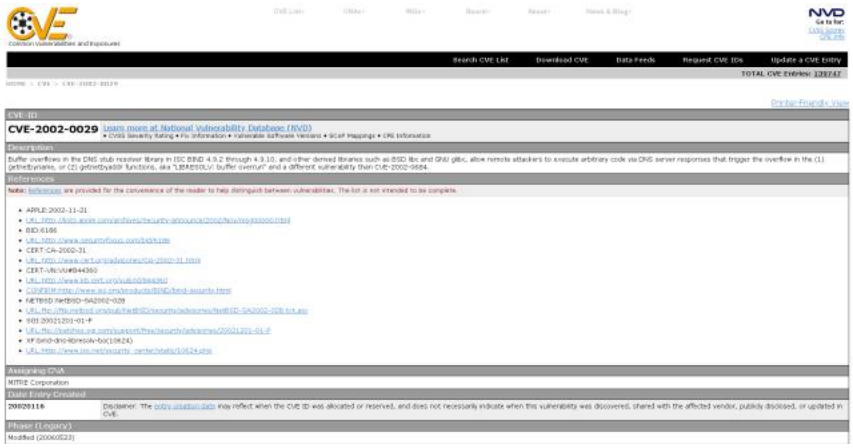
进行特征检索时，用户可点击特征库列表上方 

，添加 CNNVN ID 或 CVE ID 过滤条件，然后在其搜索框中输直接输入 ID 编号，即可搜索出漏洞所对应的的特征规则。

例如：检索 CVE 编号为 2002-0029 的漏洞信息。在“CVE-ID”后的搜索框中输入“2002-0029”，可搜索出该漏洞对应的特征规则。

点击特征 ID 前的“+”，可展开特征规则的详细信息。

点击 CVE ID 链接 "CVE-2002-0029"，页面将直接跳转到 CVE 官网的漏洞详情界面，方便用户直接查看。



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”按钮。

在<自定义特征>页面，进行如下配置：

选项	说明
名称	指定特征的名称。长度为 1-255 个字符。
描述	指定特征的描述信息。长度为 0-255 个字符。
协议	指定受影响的协议。
匹配方向	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； any - 具有特征的报文可以是任意方向的。
攻击方向	指定系统用来判断攻击的流量方向，该选项通常与检测“方向”配合使用。系统通常情况下会将流量的源地址判断为攻击者。例如：若检测“方向”设置为“客户端到服务器”， 当“攻击方向”设置为“源到目的”，那么攻击发生时，系统将判定攻击源来自客户端；当设置为“目的到源”，则判定攻击源来自服务器。
源端口	指定该特征的源端口号。 any - 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。 any - 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。

选项	说明
公告板	指定公告板。
发布年份	指定发布年份。
动作	指定特征规则的默认动作：只记录动作或重置。选择“只记录日志”时，系统发现攻击后仅记录日志信息。选择“重置”，系统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。
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	点击“新建”按钮，打开<新增内容>页面，指定新增特征的内容。 普通字符串：表示新增特征内容为普通字符串。勾选“十六进制”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。 正则表达式：表示新增特征内容为正则表达式。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。点击“正则表达式测试”按钮，在<正则表达式测试>页面输入正则表达式和期望匹配的内容，点击“匹配”按钮，测试正则表达式是否正确。
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。

选项	说明
	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。

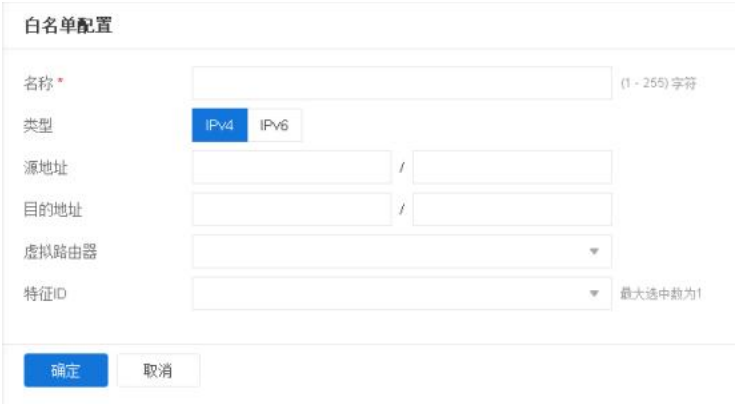
启用/禁用特征：选中特征后，点击启用/禁用。

配置入侵防御白名单

系统实时对网路中的流量进行检测，当遇到威胁时，设备会产生告警或者阻断威胁。随着网络环境的复杂，威胁的增多使设备产生的告警也会越来越多，过多的威胁告警使得用户无从下手，而且很多都存在误报的问题。系统通过提供入侵防御白名单功能，对匹配到白名单的威胁不再上报告警或阻断，从而降低威胁的误报率。入侵防御白名单由源地址、目的地址和特征 ID 组成，用户至少选择一项进行配置，当配置多条匹配条件时，只有所有都匹配成功的威胁，系统才会放行，并且不再上报告警或阻断流量。

配置入侵防御白名单，请按照以下步骤进行：

1. 点击“对象 > 入侵防御> 白名单“。
2. 点击“新建”按钮，打开<白名单配置>页面。



入侵防御白名单配置界面参数说明

选项	说明
名称	指定入侵防御白名单名称，取值范围为 1-255 字符。
类型	指定地址类型，IPv4 或者 IPv6。
源地址	指定白名单的源 IP 地址。指定后，系统将对流经设备的所有流量

选项	说明
	的源 IP 地址进行匹配过滤。
目的地址	指定白名单的目的 IP 地址。指定后，系统将对流经设备的所有流量的目的 IP 地址进行匹配过滤。
虚拟路由器	从下拉菜单中选择所需的虚拟路由器名称。
特征 ID	从下拉单中选择白名单的特征 ID。一个白名单最多允许配置一个特征 ID，不配置时表示特征 ID 可以任意，只根据源地址或目的地址来进行过滤，当源地址和目的地址匹配成功，就对报文进行放行；若配置了特征 ID，则须同时源地址、目的地址和特征 ID 都匹配成功，才能对报文进行放行。

3. 点击“确定”完成白名单的配置。

点击右上角“过滤”按钮，指定入侵防御白名单的过滤条件。指定后，系统自动显示符合过滤条件的白名单。

沙箱防护

沙箱在虚拟环境中执行可疑文件，收集可疑文件的动态行为，对这些动态行为进行分析，并根据分析结果判断文件合法性。

系统的沙箱防护功能使用云沙箱和本地沙箱技术，将可疑文件上传到云影（云沙箱）或者智影（本地沙箱）。云影或者智影对可疑文件分析，搜集可疑文件的动态行为，判断文件合法性，将分析结果反馈给系统，并根据系统设置的动作对恶意文件进行处理。

沙箱防护功能包括如下内容：

收集及上传可疑文件：沙箱防护功能对设备流量进行解析，提取出流量里的可疑文件。

如果此可疑文件在本地数据库中暂无分析结果，则将其上传到云平台或者智影，并由云平台将可疑文件上传到云影进行检测或者由智影进行检测。

如果此文件已经在本地数据库中标记为恶意文件，系统可根据设置的动作对恶意文件进行处理。

此外，用户需要配置沙箱防护规则，指定可疑文件标准。

检查分析结果并采取响应措施：沙箱防护功能从云影或者智影接收到可疑文件的分析结果后，检查分析结果，判断文件合法性，保存分析结果到本地数据库。若分析结果判定可疑文件为恶意文件，根据系统设置的动作（即重置连接或报告日志）对恶意文件进行处理。如云影或者智影第一次发现恶意文件，系统将记录威胁日志和云沙箱日志，不能阻断该恶意链接。当恶意文件命中本地设备缓存的威胁信息，重置连接方可生效。

维护本地数据库：标识上传的文件，记录文件上传时间，保存其分析结果。此部分工作由沙箱防护功能自动完成，无需相关配置。

注意: 云沙箱功能受许可证控制，当用户安装云沙箱许可证后，可以使用完整的沙箱检测功能，即可分析多种类型文件；

配置沙箱防护功能

本章节包括如下内容：

沙箱防护配置准备工作

使用沙箱防护功能前，必须完成以下准备工作：

1. 当前设备已经连接到云平台。
2. 安装云沙箱防护许可证，然后重启设备。设备成功重启后，云影功能才可使用。

配置沙箱防护功能

系统支持基于安全域和基于策略的沙箱防护配置方式：

为安全域配置沙箱防护规则后，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沙箱防护规则配置进行沙箱防护检查。

为策略配置沙箱防护规则后，系统将会对与策略规则相匹配的流量根据沙箱防护规则配置进行沙箱防护检查。

若安全域和策略中均配置了沙箱防护规则，策略中的配置项将有更高的优先权；在安全域配置中，目的安全域的优先权将高于源安全域。

系统还支持绑定沙箱防护规则到 ZTNA 策略，对与 ZTNA 策略相匹配的流量进行沙箱防护检测和处理。

基于安全域的沙箱防护配置，请按照以下步骤进行操作：

1. 创建安全域。
2. 在<安全域配置>页面中，选择<威胁防护>配置项。
3. 勾选“沙箱防护”后的“启用”复选框；并可根据自身需要，点击“模板”下拉菜单选择已配置好的沙箱防护规则或默认规则；也可点击“模板”下拉菜单中“+”按钮，新建沙箱防护规则。关于配置沙箱防护规则，请参阅配置沙箱防护规则。
4. 点击“确定”完成配置。

基于策略的沙箱防护配置，请按照以下步骤进行操作：

1. 点击“对象 > 沙箱防护 > 配置”，点击“云影”或者“智影”后的“启用”按钮，开启沙箱防护功能。当没有安装云沙箱防护许可证时，可以开启免费云影试用功能。免费云影功能仅支持 PE 文件的检测。
2. 点击“对象 > 沙箱防护 > 模板”，创建沙箱防护规则。
3. 将已创建的沙箱防护规则，绑定到策略上。点击“策略 > 安全策略”，在<策略配置>页面中，点击“防护状态”，展开防护状态配置项，点击“沙箱防护”后的“启用”按钮；并可根据自身需要，点击“模板”下拉菜单选择已配置好的沙箱防护规则或默认规则；也可点击下拉菜单中的 ⊕ 按钮，配置沙箱防护规则。

配置沙箱防护规则

沙箱防护规则用于指定进行检测的文件或协议类型、指定域名白名单、配置可疑文件识别标准、指定系统对恶意文件所执行的动作。

文件类型：沙箱支持对 PE、APK、JAR、MS-Office、PDF、SWF、RAR、ZIP、ELF、Script 及其他文件类型进行检测。其中，“其他”表示除页面可选择的文件类型以外的其他所有类型文件。

协议类型：沙箱支持对 HTTP、FTP、POP3、SMTP、IMAP4 及 SMB 协议类型进行检测。对于 SMB 协议，系统还支持断点续传场景下的文件过滤和阻断。

域名白名单：域名白名单中包含安全域名，当文件的来源是域名白名单中的域名时，此文件被认为是合法文件，不会被上传到云影或者智影进行检测。

可疑文件识别标准：将符合标准的文件判断为可疑文件，并上传到云影或者智影进行检测。可疑文件的检查结果决定文件是合法文件或是非法文件。

动作：当可疑文件命中本地沙箱的威胁条目时，系统将按指定的动作处理恶意文件。

用户可使用系统默认的沙箱防护规则，也可自行创建规则。系统提供 5 个默认的沙箱防护规则 predef_low、predef_middle、predef_high、no_sandbox 和 predef_pe：

predef_low：宽松的沙箱检测策略。此规则开启域名白名单、可信证书验证，扫描 HTTP/FTP/POP3/SMTP/IMAP4/SMB 协议流量，将 PE 类型文件作为检测对象。

predef_middle：中等的沙箱检测策略。此规则开启域名白名单、可信证书验证，扫描 HTTP/FTP/POP3/SMTP/IMAP4/SMB 协议流量，将 PE、APK、JAR、MS-Office、PDF 类型文件作为检测对象。

predef_high：严格的沙箱检测策略。此规则扫描 HTTP/FTP/POP3/SMTP/IMAP4/SMB 协议流量，将所有文件类型（PE、APK、JAR、MS-Office、PDF、SWF、RAR、ZIP、Script 及其他）作为检测对象。

predef_pe：仅支持 PE 文件检测的沙箱检测策略。此规则扫描 HTTP/FTP/POP3/SMTP/IMAP4 协议流量，将 PE 类型文件作为检测对象。

no_sandbox：此规则不进行任何沙箱检测。

注意: 当开启 SSL 代理功能时，系统将支持对 HTTPS/POP3S/SMTPS/IMAPS 流量进行沙箱检测。

配置沙箱防护规则，请按照以下步骤进行：

1. 点击“对象 > 沙箱防护 > 模板”。
2. 点击“新建”按钮创建新的沙箱防护规则。如需编辑已存在的沙箱防护规则，勾选其复选框，并点击“编辑”。

在<沙箱防护配置>页面，配置相关参数。

选项	说明
名称	输入沙箱防护规则的名称。长度为 1-31 个字符。
动作	当可疑文件命中本地沙箱的威胁条目时，系统将按指定的动作处理恶意文件。动作包含： 只记录日志 - 系统发现恶意文件后，对流量放行，仅记录日志信息（威胁日志和云沙箱日志）。

选项	说明
	重置 - 系统发现恶意文件后，重置恶意链接连接，并记录威胁日志和云沙箱日志。
域名白名单	点击“启用”按钮，开启域名白名单功能。域名白名单中预定义安全域名，当文件的来源是域名白名单中的域名时，此文件被认为是合法文件，不会被上传到云影或者智影进行检测。域名白名单可手动或自动更新。更多信息，请选择**系统 > 升级管理 > 特征库升级**，查看沙箱白名单升级管理。
可信证书验证	系统支持对 PE 文件进行可信证书白名单验证，即如文件的签名证书是可信的，系统将不对其进行检测。点击“启用”按钮开启可信证书验证功能。
文件上传	系统在认定文件为可疑文件后，默认情况下，会上传该可疑文件文件到云影或者智影进行检测。用户可以根据需求禁用可疑文件上传，即该可疑文件将不会被上传到云影或者智影。点击“禁用”按钮，禁用可疑文件上传。
文件过滤：将符合标准的文件判断为可疑文件，并上传到云影或者智影进行检测。可疑文件的检查结果决定文件是合法文件或是非法文件。如下标准的逻辑关系为与。	
文件类型	将指定类型的文件识别为可疑文件。点击文件类型名称后的“启用”按钮，选择“使用云影检测”或者“使用智影检测”，指定将可疑文件上传至云影或者智影进行检测。支持识别 PE（.exe）、APK、JAR、MS-Office、PDF、SWF、ELF、RAR、ZIP、Script 及其他（除上述类型之外的其他所有文件类型）类型的文件作为检测对象。其中，“其他”类型的文件仅支持上传到智影进行检测，不支持上传到云影进行检测。不指定类型表示沙箱防护功能不将任何文件作为检测对象。
协议类型	扫描指定类型的协议报文。支持扫描 HTTP、FTP、POP3、SMTP、IMAP4 及 SMB 协议类型报文。不指定协议类型表示沙箱防护功能不扫描任何协议的报文。指定协议类型后，在其后的下拉菜单中，选择检测该协议可疑流方向，包含上传、下载、双向。 上传 -- 流量方向为从客户端到服务器。 下载 -- 流量方向为从服务器到客户端。 双向 -- 包含上传和下载双向。

3. 点击“确定”完成配置。

沙箱全局配置

配置沙箱全局配置，请按照以下步骤进行：

1. 点击“对象 > 沙箱防护 > 配置”。

2. 点击“免费云影使用”后的“启用”按钮，开启云沙箱防护功能。当没有安装云沙箱防护许可证时，可以开启免费云影试用功能。 免费云影功能仅支持 PE 文件的检测。

3. 点击“智影”后的“启用”按钮，开启本地沙箱防护功能。开启后，分别在“智影地址”和“智影虚拟路由器”配置项中指定智影的 IP 地址和所属虚拟路由器。

4. 配置沙箱检测的文件大小限制。系统将小于指定大小的文件识别为可疑文件。

5. 点击“报告良性文件日志”后的“启用”按钮，系统在认定该文件为良性文件时，即上报该文件相关的沙箱日志。默认情况下，系统不对良性文件结果记录日志。

6. 点击“报告灰文件日志”后的“启用”按钮，系统在认定该文件为灰文件（灰文件指无法断定其是良性文件或恶意文件的所有其他文件）时，将上报该文件相关的沙箱日志。默认情况下，系统不对灰文件结果记录日志。

7. 点击“确定”完成配置。

威胁列表

威胁列表中的威胁条目的来源有以下 3 种方式：

设备收集可疑流量上传至云影或者智影。当云影或者智影确认其为恶意文件后，向设备返回结果及威胁 MD5 值，该威胁条目将显示在威胁列表中。

设备发现可疑文件并在云影或者智影中查询到威胁 MD5 值，该威胁条目将显示在威胁列表中。

设备获取到云平台同步的威胁 MD5 信息后，当本地命中该威胁时，系统威胁列表中显示该威胁条目。

用户可在沙箱威胁列表页面，通过指定 MD5 或者病毒名称，过滤查看威胁条目。或将选中的威胁条目，加入到信任列表中，请按以下步骤进行操作：

1. 点击“对象 > 沙箱防护 > 威胁列表”。
2. 选中需要加入到可信列表的威胁条目，并点击“添加信任”按钮。添加后，该威胁条目一旦被匹配，其对应的流量将被放行。

信任列表

用户可查看设备上检测到的所有沙箱威胁信息，并选择将其添加到信任列表中。信任列表中的条目一旦被匹配，对应的流量将被无条件放行，不受沙箱防护规则中动作的控制。

在信任列表中移除威胁条目，请按照以下步骤进行操作：

1. 点击“对象 > 沙箱防护 >信任列表”。
2. 在信任列表中，选中需要移除的威胁条目名称，然后点击“移除信任”按钮。该威胁条目将被从信任列表中移除。

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。作为网络安全设备的安全网关，必须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。

ICMP Flood 和 UDP Flood 攻击

这种攻击在短时间内向被攻击目标发送大量的 ICMP 消息（如 ping）和 UDP 报文，请求回应，致使被攻击目标负担过重而不能完成正常的传输任务。

ARP 欺骗攻击

局域网的网络流通根据 MAC 地址进行传输。ARP 欺骗攻击是通过填写错误的发送端 MAC 地址和 IP 地址，使目标主机的 ARP 缓存表中 IP 地址和 MAC 地址对应关系错误。导致目标主机后续将 IP 数据报文发给错误主机，目标网络不通且报文资源被窃取。

SYN Flood 攻击

由于资源的限制，服务器只能允许有限个 TCP 连接。而 SYN Flood 攻击正是利用这一点，它伪造一个 SYN 报文，将其源地址设置成伪造的或者不存在的地址，然后向服务器发起连接。服务器在收到报文后用 SYN-ACK 应答，而此应答发出去后，不会收到 ACK 报文，从而造成半连接。如果攻击者发送大量这样的报文，会在被攻击主机上出现大量的半连接，直到半连接超时，从而消耗尽其资源，使正常的用户无法访问。在连接不受限制的环境里，SYN Flood 会消耗掉系统的内存等资源。

SIP Flood 攻击

SIP(Session Initiation Protocol)是一个应用层的信令控制协议，它被用来发起、修改和终止交互式多媒体会话，例如多媒体会议或者 IP 电话。SIP Flood 攻击由攻击者在短时间内向被攻击 SIP 服务器发送大量的 INVITE 请求，导致 SIP 服务器资源耗尽，无法响应合法用户的呼叫请求。

WinNuke 攻击

WinNuke 攻击通常向装有 Windows 系统的特定目标的 NetBIOS 端口（139）发送 OOB（out-of-band）数据包，引起一个 NetBIOS 片断重叠，致使被攻击主机崩溃。还有一种是 IGMP 分片报文。一般情况下，IGMP 报文是不会分片的，所以，不少系统对 IGMP 分片报文的处理有问题。如果收到 IGMP 分片报文，则基本可判定受到了攻击。

IP 地址欺骗（IP Spoofing）攻击

IP 地址欺骗攻击是一种获取对计算机未经许可的访问的技术，即攻击者通过伪 IP 地址向计算机发送报文，并显示该报文来自于真实主机。对于基于 IP 地址进行验证的应用，此攻击方法能够使未被授权的用户访问被攻击系统。即使响应报文不能到达攻击者，被攻击系统也会遭到破坏。

ICMP 重定向攻击

ICMP 重定向报文属于 ICMP 控制报文的一种，它用于提示主机改变路由从而使路由路径最优化。ICMP 重定向攻击是指攻击者通过向被攻击者发送虚假 ICMP 重定向报文，以改变被攻击者的主机路由表，从而达到干扰主机正常 IP 报文发送的目的。

地址扫描与端口扫描攻击

这种攻击运用扫描工具探测目标地址和端口，对此作出响应的表示其存在，从而确定哪些目标系统确实存活着并且连接在目标网络上，这些主机使用哪些端口提供服务。

Ping of Death 攻击

Ping of Death 就是利用一些尺寸超大的 ICMP 报文对系统进行的一种攻击。IP 报文的字段长度为 16 位，这表明一个 IP 报文的最大长度为 65535 字节。对于 ICMP 回应请求报文，如果数据长度大于 65507 字节，就会使 ICMP 数据、IP 头长度（20 字节）和 ICMP 头长度（8 字节）的总合大于 65535 字节。一些路由器或系统在接收到这样一个报文后会由于处理不当，造成系统崩溃、死机或重启。

Teardrop 攻击防护

Teardrop 攻击是一种拒绝服务攻击。是基于 UDP 的病态分片数据包的攻击方法，其工作原理是向被攻击者发送多个分片的 IP 包（IP 分片数据包中包括该分片数据包属于哪个数据包以及在数据包中的位置等信息），某些操作系统收到含有重叠偏移的伪造分片数据包时将会出现系统崩溃、重启等现象。

Smurf 攻击

Smurf 攻击分简单和高级两种。简单 Smurf 攻击用来攻击一个网络。方法是将 ICMP 应答请求包的目标地址设置为被攻击网络的广播地址，这样该网络的所有主机都会对此 ICMP 应答请求作出答复，从而导致网络阻塞。高级 Smurf 攻击主要用来攻击目标主机。方法是将 ICMP 应答请求包的源地址更改为被攻击主机的地址，最终导致被攻击主机崩溃。理论上讲，网络的主机越多，攻击的效果越明显。

Fraggle 攻击

Fraggle 攻击与 Smurf 攻击为同种类型攻击。不同之处在于 Fraggle 攻击使用 UDP 包形成攻击。

Land 攻击

在 Land 攻击中，攻击者将一个特别打造的数据包的源地址和目标地址都设置成被攻击服务器地址。这样被攻击服务器向它自己的地址发送消息，结果这个地址又发回消息并创建一个空连接，每一个这样的连接都将保留直到超时。在这种 Land 攻击下，许多服务器将崩溃。

IP Fragment 攻击

攻击者通过向目标主机发送分片偏移小于 5 的分片报文，导致主机对分片报文进行重组时发生错误而造成系统崩溃。

IP Option 攻击

攻击者利用 IP 报文中的异常选项的设置，达到探测网络结构的目的，也可由于系统缺乏对错误报文的处理而造成系统崩溃。

Huge ICMP 包攻击

某些主机或设备收到超大的报文，会引起内存分配错误而导致协议栈崩溃。攻击者通过发送超大 ICMP 报文，让目标主机崩溃，达到攻击目的。

TCP Flag 异常攻击

不同操作系统对于非常规的 TCP 标志位有不同的处理。攻击者通过发送带有非常规 TCP 标志的报文探测目标主机的操作系统类型，若操作系统对这类报文处理不当，攻击者便可达到使目标主机系统崩溃的目的。

DNS Query Flood 攻击

DNS 服务器收到任何 DNS Query 报文时都会试图进行域名解析并且回复该 DNS 报文。攻击者通过构造并向 DNS 服务器发送大量虚假 DNS Query 报文，占用 DNS 服务器的带宽或计算资源，使得正常的 DNS Query 得不到处理。

DNS Reply Flood 攻击

DNS 服务器收到任何 DNS Reply 报文时都会对其进行处理。攻击者通过构造并向 DNS 服务器发送大量 DNS Reply 报文，导致 DNS 缓存服务器因处理这些 DNS Reply 报文而资源耗尽，影响正常业务。

TCP Split Handshake 攻击

客户端与恶意 TCP 服务器建立 TCP 连接时，恶意服务器伪造 SYN 包及其内容，向客户端发起 TCP 连接。建立 TCP 连接后，恶意 TCP 服务器反转角色变成了发起 TCP 连接的“客户端”，使得恶意流量进入内网。

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. 创建安全域。
2. 在<安全域配置>页面内，点击“威胁防护”，展开威胁防护配置项。

3. 点击“攻击防护”后的“启用”按钮，点击“设置”打开<攻击防护>页面。

在<攻击防护>页面，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”，打开<配置白名单>页面, 并点击“新建”按钮。在"类型"下拉框中选择白名单类型，分为源白名单和目的白名单，然后指定添加到白名单中的 IP 地址： IP/掩码 - 指定添加到白名单中的 IP 地址和网络掩码。 IPv6/前缀长度 - 指定添加到白名单中的 IPv6 地址和前缀长度，范围为 120 至 128。 地址条目 - 指定添加到白名单中的地址条目。
Flood 防护阈值学习	合理的攻击检测阈值是配置攻击防护功能的关键。Flood 防护阈值学习是指通过对正常网络环境下所通过流量的最大速率进行统计，为攻击检测阈值提供合理参考数值。SYN flood 攻击、DNS Query flood 攻击、DNS Recursive Query flood 攻击、DNS Reply flood 攻击、UDP flood 攻击、ICMP flood 攻击和 SIP flood 攻击均支持 Flood 防护阈值学习功能。
全选	**全部启用**：选中该“启用”按钮，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。

选项	说明
Flood 防护	点击 按钮，展开所有 Flood 防护信息。选中“Flood 防护”复选框，开启所有 Flood 防护功能。
	ICMP 洪水攻击防护：点击该“启用”按钮，开启 ICMP 洪水攻击防护功能。 警戒值 - 指定设备收到的 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：点击该“启用”按钮，开启 UDP 洪水攻击防护功能。 源警戒值 - 指定设备发送的 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。 会话状态检查 - 点击该“启用”按钮，开启会话状态检查功能。开启后，系统将对识别到会话的 UDP 报文的回包流量不做 UDP 洪水攻击防护的检查。
	DNS 查询洪水防护：点击该“启用”按钮，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 查询洪水攻击，从而采取

选项	说明
	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：点击该“启用”按钮，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。 **DNS 响应洪水防护：**点击该“启用”按钮，开启 DNS 响应洪水防护功能。 源警戒值 - 指定设备收到的源 IP 地址相同的 DNS 响应报文的警戒值。即如果一秒钟内同一个源 IP 地址发送的 DNS 响应报文个数超过该警戒值，设备就判断为受到 DNS 响应洪水攻击，从而采取相应的处理措施。 目的警戒值 - 指定设备收到的目的地址相同的 DNS 响应报文的个数的警戒值。即如果一秒钟内设备收到的到达同一个目的 IP 地址的 DNS 响应报文个数超过该警戒值，设备就判断为受到 DNS 响应洪水攻击，从而采取相应的处理措施。

选项	说明
	行为 - 指定设备对 DNS 响应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 响应报文通过，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 响应洪水攻击后发出警报但是允许 DNS 查询报文通过。
	SYN 洪水攻击防护：点击该“启用”按钮，开启 SYN 洪水攻击防护功能。 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

选项	说明
	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。 **SIP 洪水攻击防护**：点击该“启用”按钮，开启 SIP 洪水攻击防护功能。 目的警戒值- 指定设备收到的目的地址相同的 SIP INVITE 报文的个数的警戒值。即如果一秒钟内设备收到的到达同一个目的 IP 地址的 SIP INVITE 报文个数超过该警戒值，设备就判断为受到 SIP 洪水攻击，从而采取相应的处理措施。 行为- 系统将在检测到发生攻击的下一秒内，检查后续源 IP 地址主机是否存在真实 SIP 客户端，如果存在，则允许该源 IP 之后发送的 SIP INVITE 报文通过；如果不存在，则攻击发生后 3 秒内对该源 IP 发送的 SIP INVITE 报文按照配置行为处理，包括丢弃 INVITE 报文（选择默认行为“丢弃”）或者发出警报但允许 INVITE 报文通过（选择“告警”）。
ARP 欺骗攻击防护	点击 ▼ 按钮，展开 ARP 欺骗攻击防护信息。选中“ARP 欺骗攻击防护”复选框，开启 ARP 欺骗攻击防护所有功能。
	每个 MAC 最大 IP 数：点击该“启用”按钮，开启检查每个 MAC 最大 IP 数功能。 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：点击该“启用”按钮，开启检查免费 ARP 包发送速率的功能。 指定设备是否发出免费 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：点击该“启用”按钮，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。

选项	说明
ND 欺骗攻击防护	点击 按钮，展开 ND 欺骗攻击防护信息。选中“ND 欺骗攻击防护”复选框，开启 ND 欺骗攻击防护所有功能。该功能仅支持 IPv6 版本。 **每个 MAC 最大 IP 数**：点击该“启用”按钮，开启检查每个 MAC 最大 IP 数功能。 指定是否检查 ND 表中一个 MAC 地址对应的 IP 地址数，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 1 到 1024。 **ND 通告速率**：点击该“启用”按钮，开启检查 ND 通告速率的功能。 指定设备每秒钟发出 ND 通告包的个数的值。该参数的取值范围是 1 到 10。 **反向查询**：点击该“启用”按钮，开启 ND 反向查询功能。 当设备收到 NS/NA 报文后，会记录 IP 地址并且发送反向查询报文，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 NS/NA 包的 MAC 地址是否相同。
MS-Windows 防护	点击 按钮，展开 MS-Windows 防护信息。选中“MS-Windows 防护”复选框，开启 MWinNuke 攻击防护功能。
	WinNuke 攻击防护：点击该“启用”按钮，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	点击 按钮，展开所有扫描/欺骗防护信息。选中“扫描/欺骗防护”复选框，开启所有扫描/欺骗防护功能。
	IP 地址欺骗攻击防护：点击该“启用”按钮，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。
	ICMP 重定向攻击防护：点击该“启用”按钮，开启 ICMP 重定向攻击防护功能。 行为- 指定受到 ICMP 重定向攻击而进行的处理行为。如果选择默认行为“丢弃”，系统将丢弃 ICMP 重定向报文，并且发出警报。如果选择行为“告警”，系统将允许 ICMP 重

选项	说明
	定向报文通过，并且发出警报。
	IP 地址扫描攻击防护：点击该“启用”按钮，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/TCP 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 2，单位是毫秒，取值范围是 1 到 1800000 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/TCP 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。 **IP 协议扫描攻击防护**：点击该“启用”按钮，开启 IP 协议扫描攻击防护功能。 警戒值 - 指定 IP 协议扫描的时间警戒值。如果设备探测到在该指定时间内同一个源 IP 地址发送 10 种以上不同 IP 协议的数据包到同一台主机，设备就认为是受到 IP 协议扫描攻击。默认值是 10，单位是毫秒，取值范围是 1 到 1800000 毫秒。 行为 - 指定受到 IP 协议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），同一个源 IP 地址仅允许 10 种 IP 协议发往同一主机通过，多出的 IP 协议报文，系统将会丢弃并发出告警。
	TCP 端口扫描防护：点击该“启用”按钮，开启 TCP 端口扫描攻击防护功能。 警戒值- 指定 TCP 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 TCP 端口扫描攻击。默认值是 5，单位是毫秒，取值范围是 1 到 1800000 毫秒。 行为- 指定受到 TCP 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。 **UDP 端口扫描防护**：点击该“启用”按钮，开启 UDP 端口扫描攻击防护功能。

选项	说明
	警戒值 - 指定 UDP 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 UDP 包（源 IP 相同）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 5，单位是毫秒，取值范围是 1 到 1800000 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 UDP 包（源 IP 相同）通过，其它同类包将会被丢弃，同时系统将发出告警。
拒绝服务防护	点击 ▼ 按钮，展开所有拒绝服务防护信息。选中“拒绝服务防护”复选框，开启所有拒绝服务防护功能。
	Ping of Death 攻击防护：点击该“启用”按钮，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。
	Teardrop 攻击防护：点击该“启用”按钮，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：点击该“启用”按钮，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：点击该“启用”按钮，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：点击该“启用”按钮，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：点击该“启用”按钮，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：点击该“启用”按钮，开启 ICMP 大包攻击防护功能。

选项	说明
	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	点击 ▼ 按钮，展开所有代理信息。选中“代理”复选框，开启所有代理功能。
	SYN 代理：点击该“启用”按钮，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（点击“Cookie”后的“启用”按钮）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 - 点击该“启用”按钮，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（点击“Cookie”后的“启用”按钮）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	点击 ▼ 按钮，展开所有协议异常报告信息。选中“协议异常报告”复选

选项	说明
	框，开启所有协议异常报告功能。
	TCP 异常：点击该“启用”按钮，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”。 **TCP 分离握手攻击防护（TCP Split Handshake Attack）**：点击该“启用”按钮，开启 TCP 分离握手攻击防护。 行为 - 指定受到 TCP 分离握手攻击而进行的处理行为。默认为“丢弃”。

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

配置 Flood 防护阈值学习功能

配置 Flood 防护阈值学习参数

配置 Flood 防护阈值学习参数，请按照以下步骤进行操作：

1. 创建安全域。
2. 在<安全域配置>页面内，点击“威胁防护”，展开威胁防护配置项。
3. 点击“攻击防护”后的“启用”按钮，点击“设置”打开<攻击防护>页面。
4. 点击“Flood 防护阈值学习”后的“设置”按钮，打开<Flood 防护阈值学习配置>页面。

在<Flood 防护阈值学习配置>页面，配置各项参数信息。

选项	说明
学习类型	指定 Flood 防护阈值学习的学习类型，可选择单次学习或周期学习。默认是单次学习。 单次学习：只进行一次学习任务，结束后自动停止学习任务。 周期学习：按照指定周期进行循环学习，需要手动停止学习任务。

选项	说明
	当指定学习类型为周期学习时，还需指定周期学习间隔。 周期间隔：周期间隔是指从上次学习结束到下次学习开始开始之间的间隔时间。在文本框中指定时间，并在下拉框中选择时间单位，单位可以是“天”、“小时”和“分钟”。 当所选单位为“天”时，可指定的周期间隔范围是1到365天，默认是7天。 当所选单位为“小时”时，可指定的周期间隔范围是1到8760小时，默认是1小时。 当所选单位为“分钟”时，可指定的周期间隔范围是10到525600分钟，即周期间隔不能小于10分钟，默认是1440分钟。
学习时间	指定Flood防护阈值学习的学习时间，在文本框中指定时间，并在下拉框中选择时间单位，单位可以是“天”、“小时”和“分钟”。 当所选单位为“天”时，可指定的学习时间范围是1到365天，默认是1天。 当所选单位为“小时”时，可指定的学习时间范围是1到8760小时，默认是1小时。 当所选单位为“分钟”时，可指定的学习时间范围是10-525600分钟，即学习时间不能小于10分钟，默认是1440分钟。
阈值系数	最终的阈值学习结果=学习时间内的最大流量速率*阈值系数。指定Flood防护阈值学习的阈值系数，其单位为百分比，可选择“默认”、“宽松”、“严格”和“自定义”四种类型的阈值系数。默认的学习系数是200。 默认：学习系数为200。 宽松：学习系数为4000。 严格：学习系数为100。 自定义：学习系数为100到4000。
应用模式	指定Flood防护阈值学习结果的应用模式，可选择“手动应用”或

选项	说明
	者“自动应用”。默认是手动应用。 手动应用：选择该模式，根据需要将阈值学习结果应用至相应的 Flood 攻击防护项的警戒值配置中。 自动应用：选择该模式，所有已开启的 Flood 攻击防护项的警戒值将自动配置学习完成后的阈值结果并进行下发。

5. 点击“确定”按钮保存所做配置。

开启 Flood 防护阈值学习

完成 Flood 防护阈值学习参数的配置之后，可以进行 Flood 防护阈值学习。开启 Flood 防护阈值学习，请按照以下步骤进行操作：

1. 选择“网络 > 安全域 ”，进入安全域列表页面。
2. 在已开启攻击防护功能的安全域条目中，点击“AD 智能学习”列下的“状态”按钮，打开<Flood 防护阈值学习状态>页面。点击“开始学习”按钮开启 Flood 防护阈值学习。

3. 开始 Flood 防护阈值学习后，可以在该页面查看已学时间、剩余时间以及学习结果等详细信息，还可以点击“停止学习”按钮停止 Flood 防护阈值学习。

查看及应用 Flood 防护阈值学习结果

完成 Flood 防护阈值学习之后，可以查看并应用该学习结果。查看及应用 Flood 防护阈值学习结果，请按照以下步骤进行操作：

1. 创建安全域。
2. 在<安全域配置>页面内，点击“威胁防护”，展开威胁防护配置项。

3. 点击“攻击防护”后的“启用”按钮，点击“设置”打开<攻击防护>页面。

4. 点击“Flood 防护阈值学习”后的“查看结果”按钮，打开<Flood 防护阈值学习结果>页面，可以查看相应 Flood 攻击类型的阈值学习结果，包括最终完成时结果与临时结果，临时结果需人为记录并手动下发配置。

5. 勾选需要应用该阈值学习结果的 Flood 攻击类型前的复选框，点击“应用”按钮，将相应的 Flood 攻击防护项的阈值配置为此次阈值学习结果。

注意:

Flood 防护阈值学习功能生效的前提是开启攻击防护及相应 Flood 攻击防护项。

Flood 防护阈值学习期间不可以更改阈值学习参数配置。

实际的 Flood 防护阈值学习结果最小值为 1500，最大值为该 Flood 攻击防护项可配置的最大值。

HA 状态下，只有主设备可以进行 Flood 防护阈值学习。主设备开始阈值学习后，学习结果不会同步至备设备，仅当主设备下发学习结果后，阈值配置信息会同步至备设备。若发生主备切换，阈值学习将会自动停止。

若设备重启，需重新开始 Flood 防护阈值学习。

僵尸网络防御

僵尸网络，是指采用一种或多种传播手段，使大量主机感染僵尸程序，从而在控制者和被感染主机之间所形成的一个可一对多控制的网络，对用户的网络安全以及数据安全造成很大的威胁隐患。

系统的僵尸网络防御功能能够根据特征库中的地址及时发现用户内网的僵尸主机，并且根据配置对发现的僵尸主机进行处理，从而避免发生进一步的威胁攻击。

系统支持基于安全域和基于策略的僵尸网络防御配置方式。为安全域配置僵尸网络防御规则后，系统将会对以绑定安全域为目的安全域的流量根据僵尸网络防御规则配置进行僵尸网络检查。将僵尸网络防御规则绑定到策略规则后，系统将会对与策略规则相匹配的流量根据规则配置进行僵尸网络检查。

注意: 僵尸网络防御功能受许可证控制，因此，为支持僵尸网络防御功能的设备安装僵尸网络防御许可证后，僵尸网络防御功能才可使用。

配置僵尸网络防御

本章节包括如下内容：

僵尸网络防御配置准备工作

使用僵尸网络防御功能前，必须完成以下准备工作：

1. 安装僵尸网络防御许可证，然后重启设备。设备成功重启后，僵尸网络防御功能即处于开启状态。

注意: 初次使用僵尸网络防御功能，需要首先更新僵尸网络防御特征库。

配置僵尸网络防御功能

系统支持基于安全域和基于策略的僵尸网络防御配置方式。

基于安全域的僵尸网络防御配置，请按照以下步骤进行操作：

1. 创建或编辑安全域。
2. 在<安全域配置>页面中，点击“威胁防护”展开其配置项。
3. 点击“僵尸网络防御”后的“启用”按钮；并可根据自身需要，点击“模板”下拉菜单选择已配置好的僵尸网络防御规则或默认规则；也可点击下拉菜单中 ⊕ 按钮，新建僵尸网络防御规则。关于配置僵尸网络防御规则，请参阅**配置僵尸网络防御规则**。
4. 点击“确定”完成配置。

基于策略的僵尸网络防御配置，请按照以下步骤进行操作：

1. 创建或编辑策略。
2. 在<策略配置>页面中，点击“防护状态”展开其配置项。
3. 点击“僵尸网络防御”后的“启用”按钮；并可根据自身需要，点击“模板”下拉菜单选择已配置好的僵尸网络防御规则或默认规则；也可点击下拉菜单中 ⊕ 按钮，新建僵尸网络防御规则。关于配置僵尸网络防御规则，请参阅**配置僵尸网络防御规则**。

4. 点击“确定”完成配置。

配置僵尸网络防御规则

用户可使用系统默认的僵尸网络防御规则，也可自行创建规则。

配置僵尸网络防御规则，请按照以下步骤进行：

1. 点击“对象 > 僵尸网络防御 > 模板”。
2. 点击“新建”按钮。

在<僵尸网络防御规则配置>页面，填写僵尸网络防御规则配置信息。

选项	说明
规则名称	指定僵尸网络防御规则名称。
扫描协议类型	指定系统将扫描的协议类型（TCP、HTTP、DNS）以及发现僵尸主机后的处理动作。 只记录日志 - 系统发现僵尸主机后仅记录日志信息。 重置连接 - 发现僵尸主机后，重置连接。 Sinkhole 地址替换 - 当协议类型为 DNS，可以指定处理动作为“Sinkhole 地址替换”。指定后，若发现威胁后，系统会将 DNS 应答报文中的 IP 地址替换为 Sinkhole IP 地址。

3. 点击“确定”按钮保存所做配置并返回僵尸网络防御规则页面。

管理地址库

僵尸网络防御地址库包括预定义地址库和自定义地址库，每种地址库又包含阻断名单和例外名单，描述如下：

预定义例外名单：通过僵尸网络防御特征库自动获取。当流量匹配到例外名单中的域名时，系统将不会对该流量进行僵尸网络防御功能控制。

自定义例外名单：用户手动添加的 IP 地址、域名和 URL。当流量匹配到例外名单中的 IP 地址、域名或 URL 时，系统将不会对该流量进行僵尸网络防御功能控制。

预定义阻断名单：通过僵尸网络防御特征库自动获取。当流量匹配到阻断名单中的 IP 地址、域名和 URL 时，系统会对该流量进行僵尸网络防御功能控制。

自定义阻断名单：用户手动添加的 IP 地址、域名和 URL。当流量匹配到阻断名单中的 IP 地址、域名或 URL 时，系统会对该流量进行僵尸网络防御功能控制。

系统对流量进行僵尸网络防御功能控制的匹配顺序为：自定义例外名单 > 自定义阻断名单 > 预定义例外名单 > 预定义阻断名单。

例外名单配置

新建自定义例外名单

新建自定义例外名单特征条目，请按照以下步骤进行操作：

1. 点击“对象 > 僵尸网络防御 > 地址库”。
2. 在“例外名单”标签页点击“新建”按钮，打开<例外名单配置>页面。
3. 点击“类型”后的“IP”、“域名”或“URL”按钮，指定 IP（或 IP 地址和端口号）、域名或 URL 类型的例外名单特征条目。

   IP：如果选择 IP 选项，需要在“IP”文本框中输入 IP 地址或 IP 地址和端口号。不输入端口号，默认为任意端口。

   域名：如果选择域名选项，需要在“域名”文本框中输入域名。还可以点击“包含子域名”后的开启按钮，指定域名为通配符域名。

   URL：如果选择 URL 选项，需要在“URL”下拉列表中选择 http 或 https 类型并在文本框中输入 URL 地址。
4. 点击“确定”按钮，保存所做配置。

删除自定义例外名单

删除自定义例外名单特征条目，请按照以下步骤进行操作：

1. 点击“对象 > 僵尸网络防御 > 地址库”。
2. 选中“例外名单”标签，在例外名单列表中勾选例外名单特征条目，点击“删除”按钮删除例外名单特征条目。

过滤例外名单特征条目

用户可以过滤并查看预定义和自定义地址库的例外名单特征条目。过滤例外名单特征条目，请按照以下步骤进行操作：

1. 点击“对象 > 僵尸网络防御 > 地址库”。

2. 选中“例外名单”标签，点击“过滤”按钮并在弹出的下拉菜单中选择“IP/域名/URL”，在“IP/域名/URL”文本框中输入 IP 地址、域名或 URL 地址并回车，符合过滤条件的特征条目将显示在列表中。

阻断名单配置

新建自定义阻断名单

新建自定义阻断名单特征条目，请按照以下步骤进行操作：

1. 点击“对象 > 僵尸网络防御 > 地址库”。
2. 在“阻断名单”标签页点击“新建”按钮，打开<阻断名单配置>页面。
3. 点击“类型”后的“IP”、“域名”或“URL”按钮，指定 IP（或 IP 地址和端口号）、域名或 URL 类型的阻断名单特征条目。

   IP：如果选择 IP 选项，需要在“IP”文本框中输入 IP 地址或 IP 地址和端口号。不输入端口号，默认为任意端口。

   域名：如果选择域名选项，需要在“域名”文本框中输入域名。还可以点击“包含子域名”后的“开启”按钮，指定域名为通配符域名。

   URL：如果选择 URL 选项，需要在“URL”下拉列表中选择 http 或 https 类型并在文本框中输入 URL 地址。
4. 点击“确定”按钮，保存所做配置。

删除自定义阻断名单

删除自定义阻断名单特征条目，请按照以下步骤进行操作：

1. 点击“对象 > 僵尸网络防御 > 地址库”。
2. 选中“阻断名单”标签，在阻断名单列表中勾选阻断名单特征条目，点击“删除”按钮删除阻断名单特征条目。

过滤阻断名单特征条目

用户可以过滤并查看预定义和自定义地址库的阻断名单特征条目。过滤阻断名单特征条目，请按照以下步骤进行操作：

1. 点击“对象 > 僵尸网络防御 > 地址库”。
2. 选中“阻断名单”标签，点击“过滤”按钮并在弹出的下拉菜单中选择“IP/域名/URL”，在“IP/域名/URL”文本框中输入 IP 地址、域名或 URL 地址并回车，符合过滤条件的特征条目将显示在列表中。

加入例外名单

将自定义地址库的阻断名单特征条目加入到例外名单，请按照以下步骤进行操作：

1. 点击“对象 > 僵尸网络防御 > 地址库”。
2. 选中“阻断名单”标签，点击阻断名单列表操作列的“加入例外”将阻断名单特征条目加入例外名单。

配置僵尸网络防御全局参数

配置僵尸网络防御全局参数，请按照以下步骤进行操作：

1. 点击“对象 > 僵尸网络防御 > 配置”。

2. 在“僵尸网络防御”处，点击“启用”按钮开启/关闭设备的僵尸网络防御功能。 配置后，需要重启设备。
3. 在“日志聚合类型”选项后，选择僵尸网络防御日志聚合的类型。除选择“不聚合”选项外，系统将按照指定的日志聚合类型和时间粒度进行聚合，从而减少日志数量，避免日志服务器接受冗余的日志信息。
   选项说明如下：

选项	说明
不聚合	将每一条僵尸网络防御日志分别存入数据库，不进行日志聚合。
源 IP	将相同源 IP 的僵尸网络防御日志，按照指定的时间粒度进行聚合。
目的 IP	将相同目的 IP 的僵尸网络防御日志，按照指定的时间粒度进行聚合。
源 IP，目的 IP	将相同源 IP 且相同目的 IP 的僵尸网络防御日志，按照指定的时间粒度进行聚合。
源 IP，IOC	将相同源 IP 且相同 IOC 的僵尸网络防御日志，按照指定的时间粒度进行聚合。其中，IOC 表示威胁情报，即僵尸网络防御功能检测出的恶意域名、IP 地址或 URL。
目的 IP，IOC	将相同目的 IP 且相同 IOC 的僵尸网络防御日志，按照指定的时间粒度进行聚合。 其中，IOC 表示威胁情报，即僵尸网络防御功能检测出的恶意域名、IP 地址或 URL。
源 IP，目的 IP，IOC	将相同源 IP、相同目的 IP 且相同 IOC 的僵尸网络防御日志，按照指定的时间粒度进行聚合。 其中，IOC 表示威胁情报，即僵尸网络

选项	说明
	防御功能检测出的恶意域名、IP 地址或 URL。

4. 在“日志聚合时间粒度” 处， 指定日志聚合的时间间隔。指定后，系统将对同一时间间隔内，同一聚合类型的日志只存入数据库一次，不再重复存入多次。 取值范围为 10 到 600 秒，默认值为 10 秒。

5. 在“DNS Sinkhole 配置”处，指定替换 DNS 应答报文中 IP 地址的 Sinkhole IP 地址。用户可以选择系统预定义的 Sinkhole IP 地址或指定自定义的 Sinkhole IP 地址。选择“自定义 Sinkhole”后，指定自定义的 IPv4 地址及 IPv6 地址。如果仅配置了 IPv4 地址而没有配置 IPv6 地址，当 DNS 服务器使用 IPv6 协议通信时，系统会自动则将配置的 IPv4 地址映射为相应的 IPv6 地址。

6. 点击“确定”完成配置。

第 11 章 监控

系统监控部分包含如下功能：

监控：对设备数据进行统计，并以柱状图、折线图、表格等方式呈现出来，帮助用户通过统计数据掌握设备状况，排查问题。

报表：通过对设备流量信息、流量管理情况、威胁防护情况、设备监控情况以及设备资源使用情况的相关数据的统计和综合分析，为用户提供全方位、多角度的统计报告。

日志：记录并输出设备的各种日志信息，分别是设备系统、威胁、会话、NAT、NBC 以及 URL。

监控

系统提供以下多种监控方式。

如设备开启 IPv6 功能，系统支持同时统计 IPv4 地址和 IPv6 地址的带宽、会话数、AD、URL 和应用。支持 IPv6 统计的监控包含：用户监控、应用监控、云应用监控、设备监控、URL 访问、应用阻断、自定义监控。

用户监控：展现指定时间周期内（实时、最近 1 小时、最近 1 天、最近 1 月）不同用户的各类统计信息，包括用户带宽流量和用户并发连接个数。

应用监控：展现指定时间周期内（实时、最近 1 小时、最近 1 天、最近 1 月）不同应用、应用的类别、应用的子分类、应用的风险等级、应用技术、应用特征的各类统计信息，包括应用带宽流量和应用并发连接个数。

云应用监控：展现指定时间内不同云应用的使用统计信息，包括流量排名、并发连接。

共享接入监控：展现指定过滤条件（虚拟路由器、IP、接入数量）下接入终端的统计信息，包括用户的操作系统、在线时间、上线时间和最后在线时间。

终端安全状态：展示与终端安全控制中心同步的终端数据信息列表。

设备监控：展现指定时间周期内（实时、最近 1 小时、最近 1 天、最近 1 月）的包括整机流量、接口流量、安全域流量、在线 IP 数、CPU/内存状态、会话以及硬件状态统计信息。

URL 访问：系统配置 URL 过滤功能后，展现用户/IP、URL 访问以及 URL 类别统计信息。

链路状态监控：链路状态监控是通过统计链路中特定接口的采样流量信息，包括延迟、丢包率、抖动、带宽利用率，从而实现链路整体状态的监控和展示。

应用阻断：系统配置安全策略阻断应用功能后，展现被阻断的应用以及用户/IP 统计信息。

关键字阻断：系统配置上网行为控制的文件内容过滤、网页关键字、邮件过滤、Web 外发信息功能后，展现文件内容关键字、网页关键字、邮件内容关键字、 Web 外发信息关键字阻断次数统计信息以及用户/IP 统计信息。

认证用户：系统配置 Web 认证、单点登录、802.1x 认证、SSL VPN、L2TP VPN 等功能后，统计认证登录的用户信息。

监控配置：开启或者关闭指定监控项目。

自定义监控：配置自定义监控统计集为用户提供更加灵活的统计信息查看方法。

用户监控

用户监控页面展现指定时间周期内（实时、最近 1 小时、最近 1 天、最近 1 月）不同用户的各类统计信息，包括用户带宽流量和用户并发连接个数。

如设备开启 IPv6 功能，系统支持 IPv4 和 IPv6 地址的统计。

概览

概览页面为用户展示指定时间周期内的如下内容：

前 10 用户流量排名。

前 10 用户并发连接排名。

点击“监控>用户监控>概览”。

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。

“”图标用于立即刷新该页面监控数据。

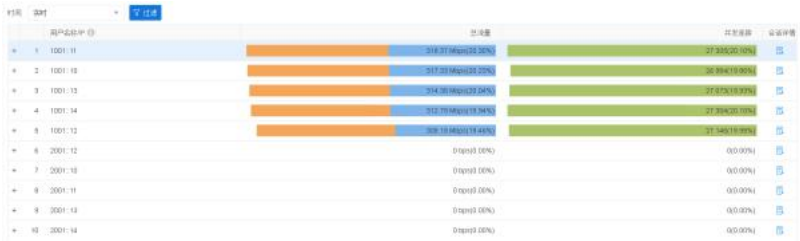
“”图标用于收起当前框图。

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、总流量值或者并发连接总个数。

当显示用户用户流量统计结果时，“上行”、“下行”选项用于指定柱状图的流量统计对象。

用户详情

点击“监控>用户监控>用户详情”，进一步查看所有用户的详细统计信息。



点击上方 过滤 添加过滤条件，符合条件的信息将显示在用户统计信息列表中。

在用户列表中选定某一用户条目，点击条目前“+”，可以进一步查看该用户的详细统计信息。

应用（实时）：点击<应用（实时）>标签页，显示所选用户使用的各应用的上行、下行、总流量统计详细信息。点击列表中”详情“列的“ ”按钮，查看指定统计周期对应的趋势图。

云应用（实时）：点击<云应用（实时）>标签页，显示所选用户的云应用信息。

URL（实时）：点击<URL（实时）>标签页，显示所选用户的 URL 访问次数等详细信息。

URL 类别（实时）：点击<URL 类别（实时）>标签页，显示所选用户的 URL 类别访问次数信息。

流量：点击列表下方<流量>标签页，显示所选用户的流量趋势图。

并发连接：点击列表下方<并发>标签页，显示所选用户的并发连接统计趋势图。

鼠标框选趋势图中某一区域，可以放大显示的时间段范围，点击趋势图右上角 重置缩放 按钮，恢复趋势图默认大小。

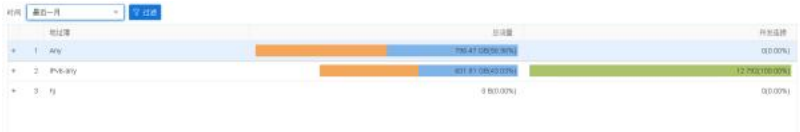
在用户列表中选定某一用户条目，点击条目所对应的“会话详情”列的“”按钮，打开<会话详情>页面，查看该用户的所有会话详情。

点击上方 过滤 添加过滤条件，符合条件的会话将显示在会话详情列表中。

在用户列表中，光标悬浮在想要添加入黑名单的某一用户条目上方，右侧出现“”按钮，点击该按钮，选择“添加到黑名单”。

地址簿详情

点击“监控>用户监控>地址簿详情”，进一步查看需要统计的监控地址簿的详细统计信息。



点击上方 过滤 添加过滤条件，符合条件的信息将显示在地址簿统计信息列表中。

在用户列表中选定某一地址簿条目，点击条目前“+”，可以进一步查看该地址簿的详细统计信息。

应用（实时）：点击<应用（实时）>标签页，显示所选地址簿使用的各应用的总流量、统计详细信息。点击列表中“详情”，查看对应的趋势图。

云应用（实时）：点击<云应用>标签页，显示所选地址簿的云应用信息。

用户（实时）：点击<用户（实时）>标签页，显示所选地址簿使用的各用户的总流量、统计详细信息。点击列表中“详情”，查看对应的趋势图。

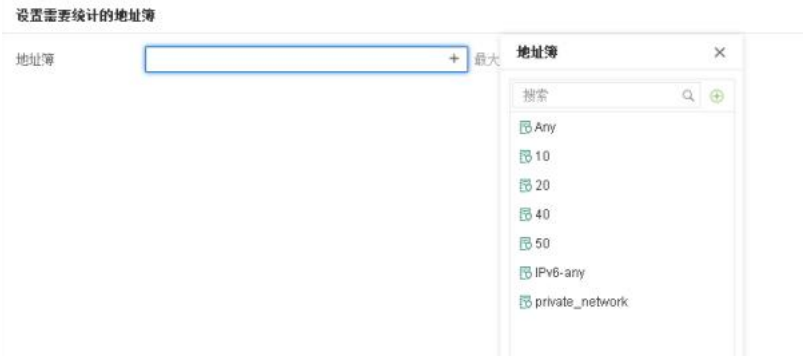
流量：点击<流量>标签页，显示所选地址簿的流量趋势图。

并发连接：点击<并发>标签页，显示所选地址簿的并发统计趋势图。

监控地址簿

此监控地址簿用来储存需要统计的用户地址条目，即在全局地址簿中选择需要统计的地址条目。

点击“监控>用户监控>设置需要统计的地址簿”。



在<设置需要统计的地址簿>页面，可以实现以下操作：

在右侧地址簿中，点击需要统计的地址条目，将地址条目添加到左侧列表中。点击搜索框中的按钮，可以按地址簿名称和地址成员的 IP 进行模糊搜索，名称和地址是与的关系。

在左侧列表中，点击需要移出的地址条目将其移出，此地址条目将不会被统计。

注意: 地址支持多种输入方式，例如：输入“地址”为 10.10.10.10/32，可能匹配到包含地址成员是 10.10.10.10/24 的地址簿；输入“地址”为段掩码 9.9.9.9/24，可能匹配到包含地址成员是 9.9.0.0/16 的地址簿；输入“地址”为 10.10.10.10，可能匹配到地址成员的 IP 范围为 10.10.10.0-10.10.10.255 的地址簿；输入“地址”为 10.23，可能匹配到包含地址成员是 1.10.23.10/24 的地址簿；输入“地址”为 aa，可能匹配到地址成员的“主机名称”为 aaa 的地址簿。

统计周期

系统支持预定义统计周期。用户可以通过监控页面右上角的统计周期下拉菜单（ 

）指定统计周期：

实时: 显示当前的统计信息。

最近 1 小时: 显示最近 1 小时的统计信息。

最近 1 天: 显示最近 1 天的统计信息。

最近 1 月: 显示最近 1 月的统计信息。

应用监控

应用监控页面展现指定时间周期内（实时、最近 1 小时、最近 1 天、最近 1 月）不同应用、应用的类别、应用的子分类、应用的风险等级、应用技术、应用特征的各类统计信息，包括应用带宽流量和应用并发连接个数。

如设备开启 IPv6 功能，系统支持 IPv4 和 IPv6 地址的统计。

概览

概览页面为用户展示指定时间周期内的如下内容：

前 10 热门高风险应用的并发连接数。

前 10 应用的带宽流量/并发连接数。

前 10 应用分类的带宽流量/并发连接数。

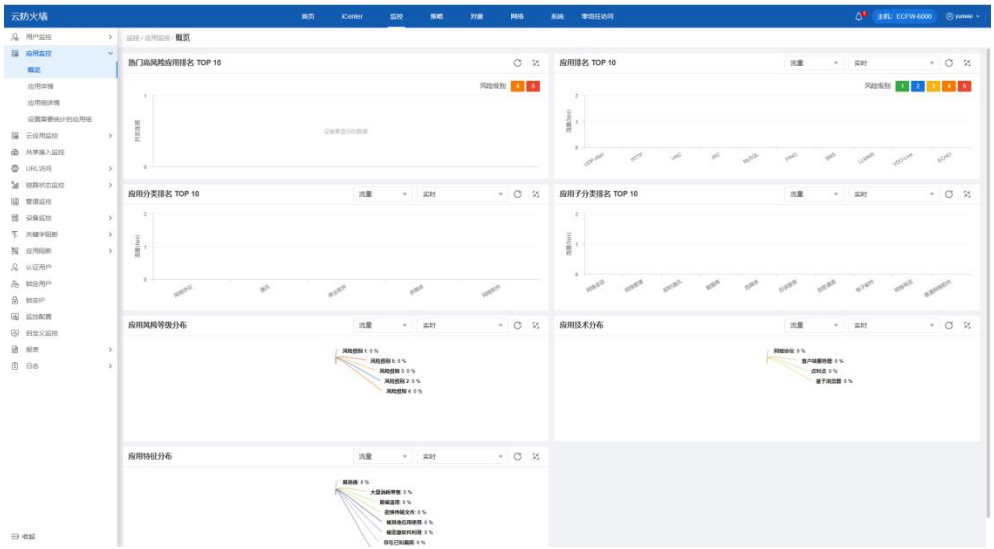
前 10 应用子分类的带宽流量/并发连接数。

应用风险等级的带宽流量/并发连接数分布。

应用技术的带宽流量/并发连接数分布。

应用特征的带宽流量/并发连接数分布。

点击“监控>应用监控>概览”。



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。

通过选择下拉菜单中的流量或并发连接，可以指定统计的内容类型。

“”图标用于立即刷新页面监控数据。

“”图标用于收起当前框图。

鼠标悬停在柱状图或饼状图上，查看具体的总流量值或者并发连接数。

应用详情

点击“监控>应用监控>应用详情”，进一步查看所有应用的详细统计信息。

点击“时间”下拉菜单，可以选择不同的**统计周期**，查看不同时间范围内的应用统计信息。

点击 过滤 按钮，选择下拉菜单中的“应用名称”，在增加的“应用名称”文本框中输入需要搜索的应用。

在应用列表中选定某一应用条目，点击条目前“+”，可以进一步查看该应用的详细统计信息。

用户（实时）：点击<用户（实时）>标签页，查看使用此应用的用户列表详情。点击“详情”列的 图标，显示使用所选应用的用户的上行、下行、总流量统计趋势图。

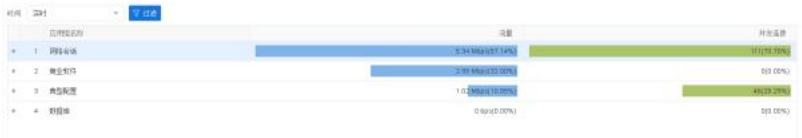
流量：点击<流量>标签页，显示所选应用的流量趋势图。

并发连接：点击<并发连接>标签页，显示所选应用的并发统计趋势图。

描述：点击<描述>标签页，显示所选应用的描述详细信息。

应用组详情

点击“监控>应用监控>应用组详情”，进一步查看所有应用组的详细统计信息 。



点击“时间”下拉菜单，可以选择不同的**统计周期**，查看不同时间范围内的应用组统计信息。

点击 过滤 按钮，选择下拉菜单中的“应用组名称”，在增加的“应用组名称”文本框中输入需要搜索的应用组。

在应用组列表中选定某一应用组条目，点击条目前“+”，可以进一步查看该应用组的详细统计信息。

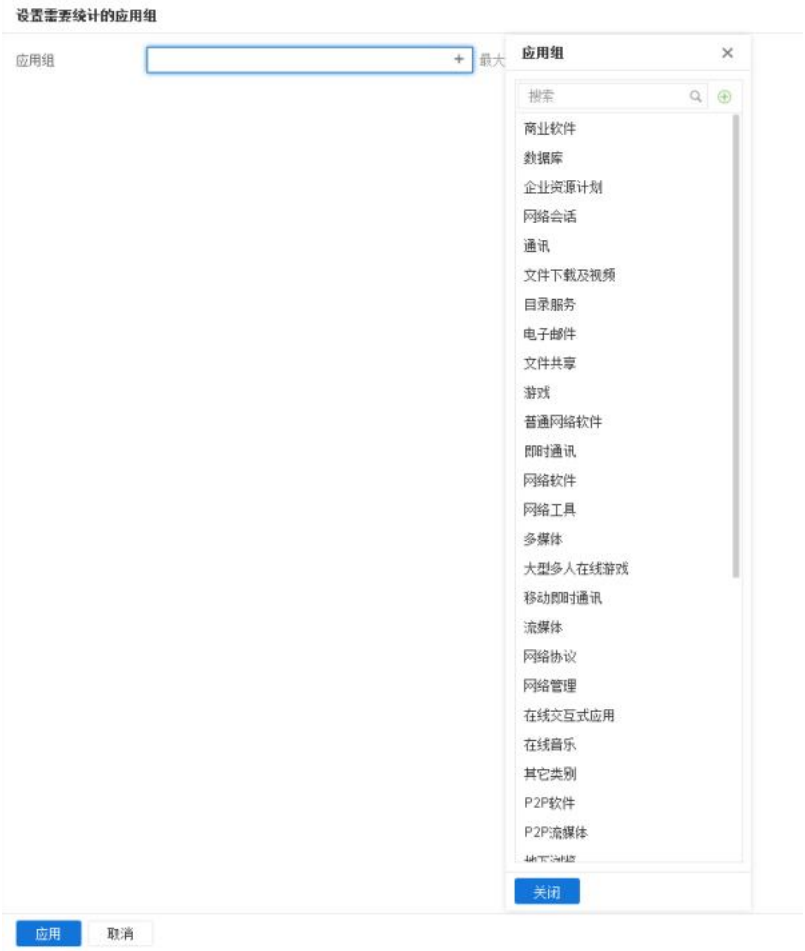
用户（实时）：点击<用户（实时）>标签页，查看使用此应用组的用户列表详情。点击“详情”列的 图标，显示使用所选应用组的用户的上行、下行、总流量的统计趋势图。

流量：点击<流量>标签页，显示所选应用组的流量趋势图。

并发连接：点击<并发>标签页，显示所选应用组的并发连接统计趋势图。

设置需要统计的应用组

点击“监控>应用监控>设置需要统计的应用组”，在页面中对需要统计的应用组进行配置。



在此页面，可以实现以下操作：

在右侧全局应用组中，点击需要统计的应用组条目，将应用组条目添加到左侧列表中。

在左侧列表中，点击需要移出的应用组条目将其移出，此应用组条目将不会被统计。

统计周期

系统支持预定义统计周期。用户可以通过监控页面右上角的统计周期下拉菜单（ 最近一天 ）指定统计周期：

实时: 显示当前的统计信息。

最近一小时: 显示最近 1 小时的统计信息。

最近一天: 显示最近 1 天的统计信息。

最近一月: 显示最近 1 月的统计信息。

云应用监控

云应用是指在云端使用的应用程序。云应用完全架构在远程服务器，通过互联网提供服务。

云应用监控页面展现指定时间周期内（实时、最近 1 小时、最近 1 天、最近 1 月）不同云应用和其用户的各类统计信息，包括应用流量、用户数量。

如设备开启 IPv6 功能，系统支持 IPv4 和 IPv6 地址的统计。

概览

概览页面为用户展示指定时间周期内的如下内容：

前 10 云应用在指定时间范围内的带宽流量/并发连接数排名，统计时间包括实时、最近 1 小时、最近 1 天、最近 1 月。

前 10 云应用用户排名，统计时间包括实时。

点击“监控>云应用监控>概览”。

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。

通过选择下拉菜单中的流量或并发连接，可以指定统计的内容类型。

图标用于立即刷新页面监控数据。

鼠标悬停在柱状图或饼状图上，查看具体的数据，点击悬停框中的“详细信息”，可以跳转到“云应用详情”页面。

云应用详情

点击“监控>云应用监控>云应用详情”，进一步查看所有应用的详细统计信息。

点击“时间”下拉菜单，可以选择不同的统计周期，查看不同时间范围内的应用统计信息。

点击 过滤 按钮，选择下拉菜单中的“应用名称”，在增加的“应用名称”文本框中输入需要搜索的应用。

在应用列表中选定某一应用条目，点击 + 按钮，可以进一步查看该应用的详细统计信息。

用户（实时）：点击列表下方<用户（实时）>标签页，查看使用此应用的用户列表详情。

点击“详情”列的 图标，显示使用所选应用的用户的上行、下行、总流量统计趋势图。

流量：点击列表下方<流量>标签页，显示所选应用的流量趋势图。

并发连接：点击列表下方<并发连接>标签页，显示所选应用的并发统计趋势图。

描述：点击列表下方<描述>标签页，显示所选应用的描述详细信息。

统计周期

系统支持预定义统计周期。用户可以通过监控页面右上角的统计周期下拉菜单（ 最近一天 ）指定统计周期：

实时: 显示当前的统计信息。

最近一小时: 显示最近 1 小时的统计信息。

最近一天: 显示最近 1 天的统计信息。

最近一月: 显示最近 1 月的统计信息。

共享接入监控

共享接入监控是一种基于应用特征的终端识别方法，即基于 HTTP 报文 User-agent 字段识别网络接入终端，对网络中用户私接设备共享上网的行为进行识别和控制。共享接入监控页面可以展现指定过滤条件（源 IP、源安全域、规则名称、状态和接入数量）下共享接入监控的统计信息。

点击“监控>共享接入监控”，查看共享接入监控的统计信息。如下图所示：

点击 过滤 按钮，在下拉菜单中选择过滤条件，符合条件的信息将显示在列表中。过滤条件如下：

源 IP：显示指定 IP 地址（IPv4 或 IPv6）下的终端监控信息。

规则名称：显示指定 IP 地址下的终端监控信息。

源安全域：显示指定安全域下的终端统计信息。

状态：显示 IP 地址为指定状态下的终端监控信息，包括正常状态、记录日志状态、告警状态和阻断状态。

接入数量：显示 IP 地址下终端数量为指定条件的终端监控信息。

配置完成过滤条件后，下方列表会显示指定过滤条件的终端接入监控信息。

点击“+”按钮，查看指定列的具体接入的终端型号和上线时间的详情列表，如下图所示：

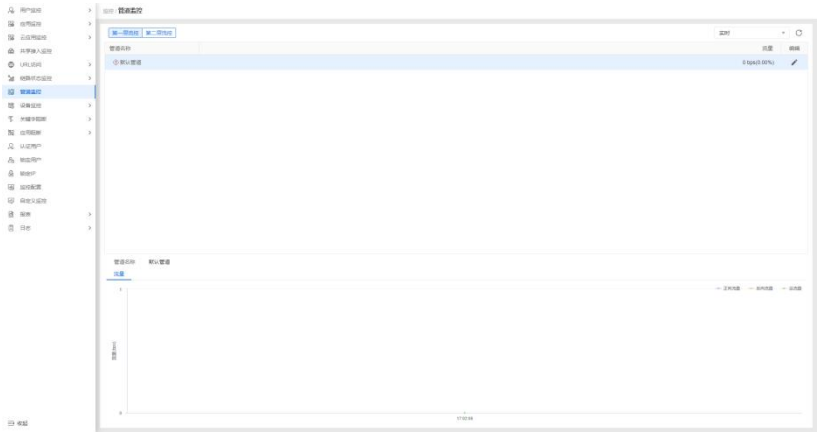
管道监控

系统配置 iQOS 策略且 iQOS 功能启用后，管道监控页面将展示第一层流控和第二层流控的根管道及子管道的实时及历史流量信息。

> 注意: 管道监控功能受许可证控制，即设备安装 iQOS 许可证后，功能才可使用。

管道监控详情

点击“监控>管道监控”，进入管道监控页面。



该页面上方以列表方式列出管道的名称、流量（正向流量、反向流量）。

点击 第一层流控 或 第二层流控，显示该层流控下的管道信息。

在 实时 下拉菜单中选择“最近一小时”、“最近一天”、“最近一周”、“最近一月”，系统将显示指定时间内的管道流量详情信息。用户最远可以指定从当前时间起往前 30 天的时间周期。

点击 图标，可展开管道，查看其子管道。

点击“编辑”按钮，编辑所选的管道。

鼠标悬停在“流量”列的色条上，可查看管道的正向流量和反向流量。

该页面下方显示上方选中管道的流量详细信息，系统提供流量、子管道叠加（正向）和子管道叠加（反向）共三种方式展示流量的详情。

流量：展示管道实时正向流量、反向流量、总流量的趋势图以及历史趋势图。鼠标悬停在折线图上，可查看具体某一时刻的正向流量、反向流量、总流量；点击右上角的"正向流量"、"反向流量"、”总流量“文字，文字将置灰同时趋势图中将隐藏对应的流量折线，再次点击可重新显示。

子管道叠加（正向）：展示某管道下所有子管道的正向流量的历史趋势叠加图。鼠标悬停在折线图上，可查看具体某一时刻的排名前五的管道流量和其他（除去 Top5 以外的所有管道流量）流量。点击右上角的子管道名称，该名称将置灰同时趋势图中将隐藏对应的流量折线，再次点击可重新显示。

子管道叠加（反向）：展示某管道下所有子管道的反向流量的历史趋势叠加图。鼠标悬停在折线图上，可查看具体某一时刻的排名前五的管道流量和其他（除去 Top5 以外的所有管道流量）流量。点击右上角的子管道名称，该名称将置灰同时趋势图中将隐藏对应的流量折线，再次点击可重新显示。

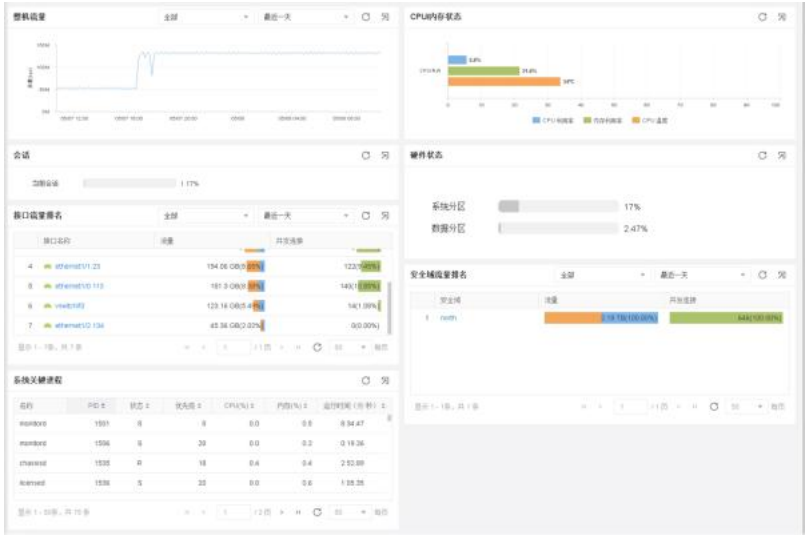
设备监控

设备监控页面展现指定时间周期内包括整机流量、接口流量、安全域流量、CPU/内存状态、会话、硬件状态以及在线 IP 数统计信息。

如设备开启 IPv6 功能，系统支持 IPv4 和 IPv6 地址的统计。

概览

概览页面为用户展示最近 1 天的设备统计信息。点击“监控>设备监控>概览”。



整机流量：显示设备在指定统计周期内的整机流量历史趋势。

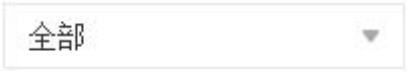
鼠标悬停在曲线图上，查看对应时刻的整机流量信息。

在 

下拉菜单中，通过选择不同的地址类型，可以分别查看整机的 IPv4 流量、IPv6 流量或者全部流量。

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。

接口流量排名：按照排名显示设备所使用的接口在指定统计周期内的总流量信息、上下行流量信息、并发连接数以及各自使用率。系统按照总流量大小显示接口流量排名。

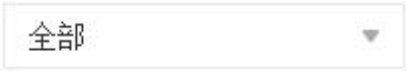
在 

下拉菜单中，通过选择不同的地址类型，可以分别查看接口的 IPv4 流量、IPv6 流量或者全部流量。

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。

点击接口名称，可以进入详细信息页面，进一步查看该接口的详细统计信息。

安全域流量排名：按照排名显示设备各安全域在指定统计周期内的总流量信息、上下行流量信息、并发连接数以及各自使用率。系统按照总流量大小显示安全域流量排名。

在 

下拉菜单中，通过选择不同的地址类型，可以分别查看安全域的 IPv4 流量、IPv6 流量或者全部流量。

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。

点击安全域名称，可以进入详细信息页面，进一步查看该安全域的详细统计信息。

硬件状态：显示设备虚拟硬盘的实时使用状态，包括系统分区和数据分区的使用状态。其中系统分区用于存储系统文件，数据分区用于存储日志和报表。

系统分区：显示虚拟硬盘的系统盘使用百分比。

鼠标悬停在百分比上，可以查看当前系统盘使用量以及总量。

数据分区：显示虚拟硬盘的数据盘使用百分比。

鼠标悬停在百分比上，可以查看当前数据盘使用量以及总量。

会话：显示设备的当前会话使用率。

CPU/内存状态：显示设备当前 CPU 利用率、内存利用率和 CPU 温度统计信息。

点击“CPU 利用率“、”内存利用率“或者”CPU 温度”图例，可指定柱状图的统计对象，默认是所有对象。

系统关键进程：显示设备关键进程的信息，包括进程名称、PID、状态、优先级、CPU 占用率。

统计周期

系统支持预定义统计周期。 用户可以通过监控页面右上角的统计周期下拉菜单（ 

）指定统计周期：

实时: 显示当前的统计信息。

最近 1 小时: 显示最近 1 小时的统计信息。

最近 1 天: 显示最近 1 天的统计信息。

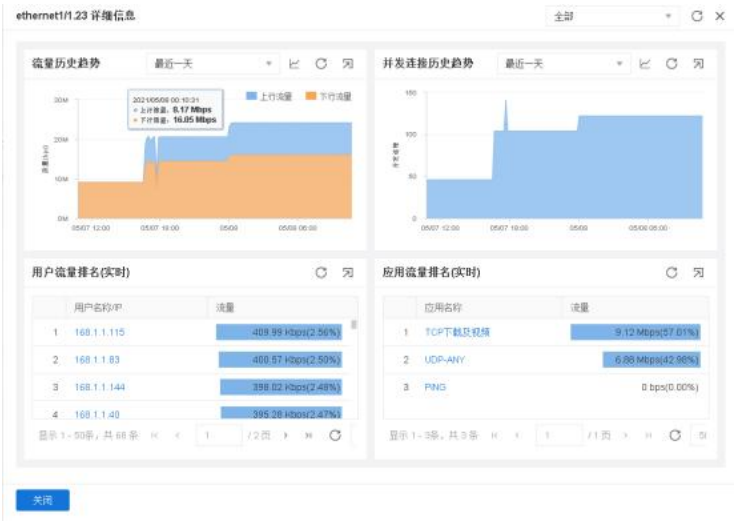
最近 1 月: 显示最近 1 月的统计信息。

用户可以通过页面右上角的刷新间隔设置显示数据的刷新间隔。

详细信息页面

在详细信息页面可以进一步查看某对象的详细统计信息。另外，在详细信息页面中，鼠标悬停在某统计对象对应的曲线图上，可以查看该统计对象对应时刻的统计信息。

例如，单击接口流量排名列表中接口 ethernet1/1.23， 进入 ethernet1/1.23 对应的详细信息页面。



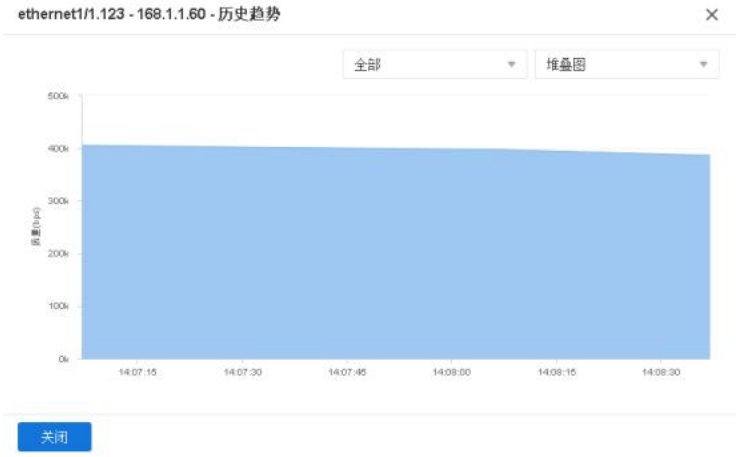
页面右上角下拉菜单（ 

）用于指定接口流量的统计类型，包括全部、IPv4、IPv6。

页面右上角图标用于将统计图在趋势图和堆叠图之间切换，分别展现接口 ethernet1/1.23 的流量、并发连接历史趋势统计信息；

在流量历史趋势图部分，点击“上行流量“或者”下行流量”图例，可指定接口流量曲线图的统计对象，默认是总流量。

在用户流量或者应用流量排名部分，单击用户名称/IP 或者应用名称，系统会弹出窗口显示该用户或应用的实时流量趋势。以用户流量为例，如下图所示。



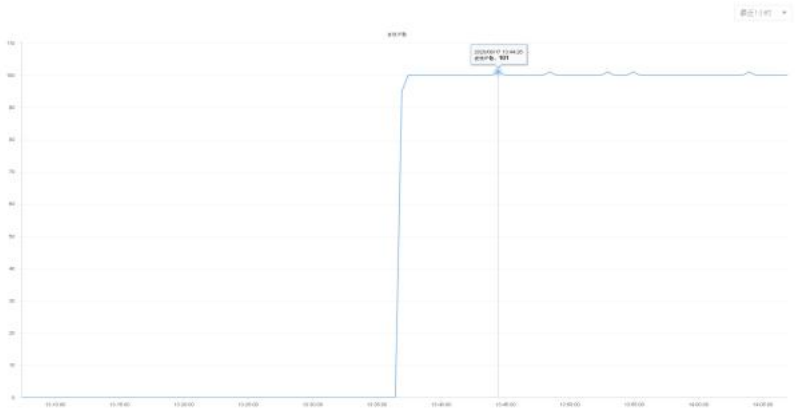
通过页面右上角下拉菜单（ 全部 ）指定用户流量的类型，包括全部、IPv4、IPv6。

通过页面右上角下拉菜单（ 堆叠图 ）指定趋势图或者堆叠图。

鼠标悬停在该用户的实时流量曲线图上，查看对应时刻的流量信息。

在线 IP 数

点击“监控>设备监控>在线 IP 数”。用户可在该页面查看指定时间周期内（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。

URL 访问

系统配置 URL 过滤功能且在策略规则中启用后，URL 访问页面展现用户/IP、URL 访问以及 URL 类别统计信息。

如设备开启 IPv6 功能，系统支持 IPv4 和 IPv6 地址的统计。

概览

概览页面为用户展示指定时间周期内前 10 用户/IP、前 10URL 以及前 10URL 类统计信息。点击“监控>URL 访问>概览”。

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。

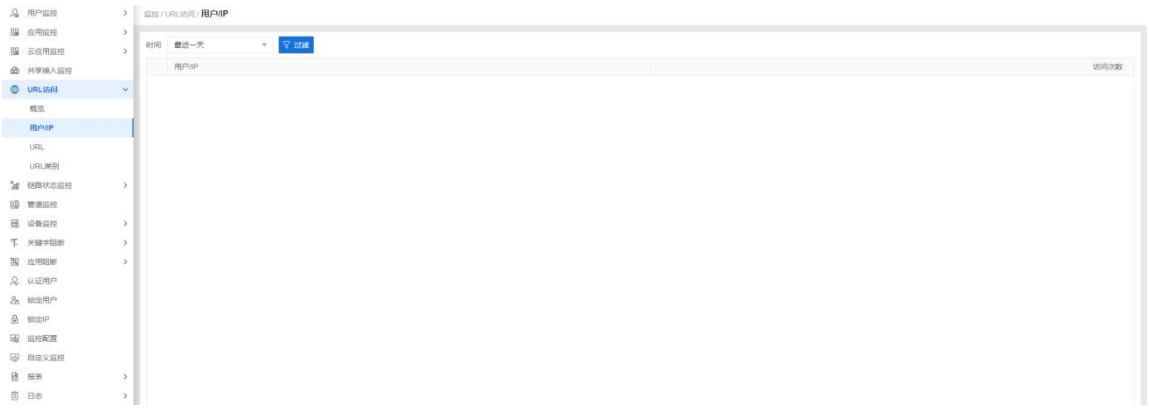
鼠标悬停在某用户/IP、URL 或 URL 类别对应的柱状图上，查看该用户/IP、URL 或 URL 类别的访问次数。

点击各图表右上角图标，进入对应的详情页面。

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 详情统计页面。



该页面上方以列表方式列出用户/IP 的以及具体访问次数数据。

点击条目前“+”，查看相应的用户/IP 的访问次数趋势图以及 URL 详情列表。

趋势图：点击“趋势图”标签页，查看所选用户/IP 的趋势图。包括即时趋势、一小时趋势、24 小时、一个月趋势。

URL(实时)：点击“URL(实时)"标签页，查看访问所选用户/IP 的 URL 的详细统计信息。从列表中点击选中 URL，系统将跳转到对应的 URL 详情统计页面。点击列表详情栏中“详情”，显示所选 URL 的用户/IP 访问趋势图。

URL 类别(实时)：点击“URL 类别(实时)"标签页，查看用户/IP 所访问的 URL 类别的详细统计信息。从列表中点击选中 URL 类别，系统将跳转到对应的 URL 类别详情统计页面。点击列表详情栏中“详情”，显示所选 URL 类别的用户/IP 访问趋势图。

在页面右上方点击 过滤 按钮，然后在页面左上方点击“过滤条件”，选择下拉菜单中的“用户/IP”，在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。

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 访问统计页面。

该页面上方以列表方式列出 URL 的名称、对应的 URL 类别以及具体访问次数数据。

点击条目前“+”，查看相应的 URL 访问次数统计信息趋势图以及对应的用户/IP。

趋势图：点击“趋势图”标签页，查看所选 URL 的趋势图。包括即时趋势、1 小时趋势、24 小时、一个月趋势。

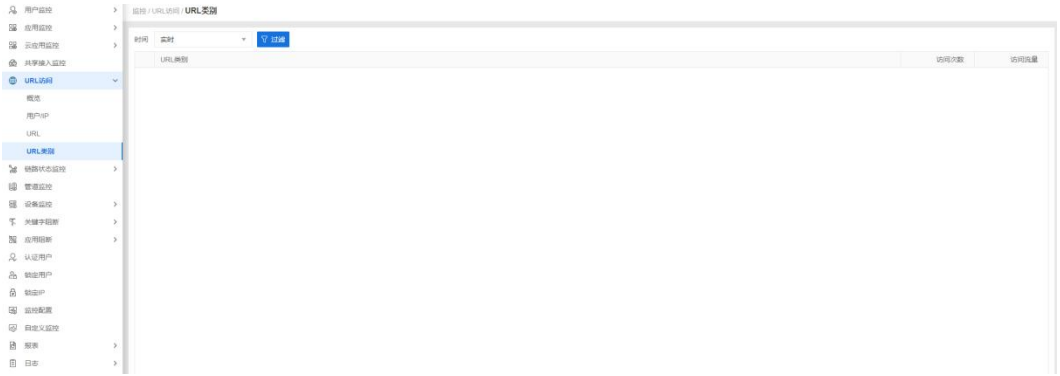
用户/IP(实时)：点击“用户/IP(实时)"标签页，查看访问所选 URL 的用户/IP 的详细统计信息。从列表中点击选中用户/IP，系统将跳转到对应的用户/IP 详情统计页面。点击列表详情栏中“详情”，显示所选用户/IP 的 URL 访问趋势图。

在页面右上方点击 过滤 按钮，然后在页面左上方点击“过滤条件”，选择下拉菜单中的“URL”，在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。

点击列表下方的刷新按钮实时刷新列表信息。

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 类别的名称、访问次数、以及访问流量。

点击条目前“+”，查看相应的 URL 类别访问次数趋势图、实时访问的 URL、以及实时访问的用户/IP。

趋势图：点击“趋势图”标签页，查看所选 URL 类别的访问次数趋势图。包括即时趋势、最近一小时趋势、最近一天趋势、最近一月趋势。

URL(实时)：点击“URL(实时)”标签页，查看所选 URL 类别所包含的 URL 的实时访问信息。

用户/IP(实时)：点击“用户/IP(实时)"标签页，查看实时访问所选 URL 类别的用户/IP 的信息。

点击列表下方的刷新按钮实时刷新列表信息。

统计周期

系统支持预定义统计周期。用户可以通过统计周期下拉菜单（ 

）指定统计周期：

实时: 显示当前的统计信息。

最近一小时: 显示最近 1 小时的统计信息。

最近一天: 显示最近 1 天的统计信息。

最近一月: 显示最近 1 月的统计信息。

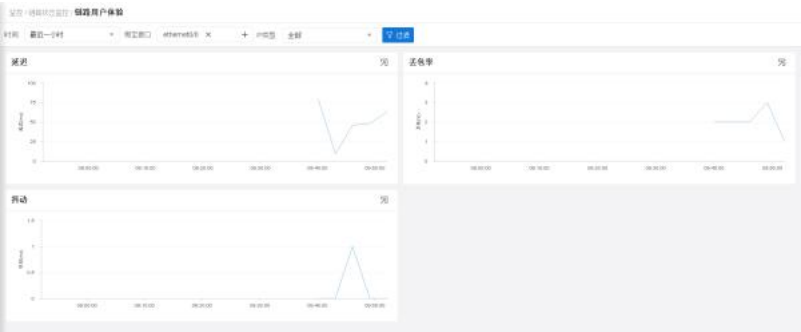
链路状态监控

链路状态监控可以通过统计链路中特定接口的采样流量信息，包括延迟、丢包率、抖动，从而实现链路整体状态的监控和展示。系统也可以对特定目的 IP 进行链路探测，统计指定链路的流量信息，包括延迟和抖动。

链路用户体验

链路用户体验页面展现指定时间周期内（实时、最近 1 小时、最近 1 天、最近 1 月）已绑定的接口的流量统计信息，包括延迟、丢包率、抖动。

点击“监控>链路状态监控>链路用户体验”。



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“绑定接口”下拉菜单，选择已绑定的接口，显示该接口的链路状态监控统计信息，可选择多个绑定接口。

点击“IP 类型”下拉菜单，选择需要查看链路状态的地址类型，包括 IPv4、IPv6 或者全部。

点击 

按钮，在下拉菜单中选择“应用”，然后在增加的“应用”下拉菜单中选择 TOP10 或者应用/应用组名称，按照指定应用显示链路状态监控统计信息。

注意:

过滤条件中“时间”、“绑定接口”和“IP 类型”均为必选项，其中“IP 类型”默认为“全部”。

如果链路配置中未开启指定接口的应用维度，则不能添加“应用”过滤条件。

统计周期

系统支持预定义统计周期。用户可以通过监控页面左上角的统计周期下拉菜单（ 

）指定统计周期：

实时: 显示当前的统计信息。

最近一小时: 显示最近 1 小时的统计信息。

最近一天: 显示最近 1 天的统计信息。

最近一月: 显示最近 1 月的统计信息。

链路探测

链路探测页面展现指定探测目的 IP 到链路、链路到探测目的 IP 的实时流量统计信息，包括延迟和抖动。

配置实时链路探测，请按照如下步骤进行操作：

1. 点击“监控>链路状态监控>链路探测”，进入链路探测（实时）页面。

2. 在“链路”下拉菜单中选择需要监控链路状态的接口，最多可选择 8 个接口。点击“新建”，添加需要监控链路状态的接口，最多可添加 16 个接口。

3. 在“探测目的”下拉菜单中选择需要监控链路状态的探测目的 IP 地址，最多可选择 8 个探测目标。点击“新建”，添加需要监控链路状态的探测目的 IP，最多可添加 32 个探测目的 IP。

4. 点击“开始探测”，在页面下方区域展示实时链路探测的数据。选择“探测目的 IP->链路”或“链路->探测目的 IP”页签，查看链路实时延迟和丢包趋势图。“趋势图”及“列表”按钮用于将探测信息在趋势图和列表之间切换。

5. 点击“结束探测”，结束实时链路探测。

链路配置

在链路配置页面配置需要监控链路状态的接口，并且可以根据需要开启应用维度、链路用户体验。

链路配置，请按照以下步骤进行操作：

1. 点击“监控>链路状态监控>链路配置”，进入链路配置页面。

2. 点击“新建”按钮，打开<链路配置>页面。

在<链路配置>页面填写配置信息

选项	说明
绑定接口	在下拉菜单中选择需要统计流量的接口。
接口描述	在文本框中指定接口的描述信息。
应用	点击“应用”后的“启用”按钮，开启接口的应用维度。开启后，可以在“链路用户体验”页面查看该接口下具体应用的信息，包括延迟、丢包率、抖动。

选项	说明
监控	点击“监控”后的“启用”按钮，开启接口的链路用户体验监控。开启后，可以在“链路用户体验”页面查看该接口的流量统计信息，包括延迟、丢包率、抖动。

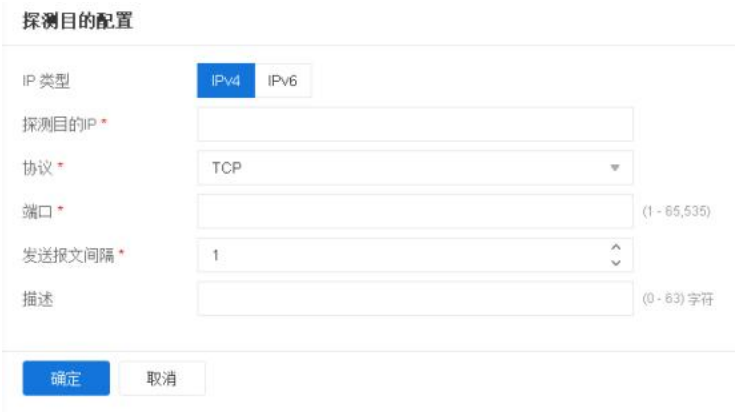
3. 点击“确定”按钮，保存链路配置信息。

探测目的

在探测目的页面配置需要监控链路状态的探测目的 IP。

探测目的 IP 配置，请按照以下步骤进行操作：

1. 点击“监控>链路状态监控>探测目的”，进入探测目的页面。
2. 点击“新建”按钮，打开<探测目的配置>页面。



在<探测目的配置>页面填写配置信息

选项	说明
IP 类型	指定探测目的的 IP 地址类型，IPv4 或者 IPv6。
探测目的 IP	指定探测目的的 IP 地址。
协议	指定探测目的的协议类型，TCP 或者 ICMP。
端口	指定探测目的的端口号。
发送报文间隔	指定探测报文的间隔时间，取值范围是 1 到 5 秒，默认值是 1。
描述	指定探测目的的描述信息。

3. 点击“确定”按钮，保存探测目的配置信息。

应用阻断

系统配置安全策略阻断应用功能后，应用阻断页面展现被阻断的应用以及用户/IP 统计信息。如设备开启 IPv6 功能，系统支持 IPv4 和 IPv6 地址的统计。

概览

概览页面为用户展示指定时间周期内被阻断次数最多的前 10 应用以及前 10 用户/IP 统计信息。点击“监控>应用阻断>概览”。

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。

鼠标悬停在某应用或用户/IP 对应的柱状图上，查看该应用或用户/IP 的被阻断次数。

点击各图表右上角图标，将统计图在柱状图和饼状图之间切换。

点击各图表右上角图标，收起图表。

点击各图表右上角图标，进入对应的详情页面。

应用

点击“监控>应用阻断>应用”或者点击概览页面“前 10 应用”图表右上角图标。

该页面以列表方式列出应用的名称以及具体阻断数据。

通过选中列表中不同的应用，点击条目前“+”，可查看相应的应用阻断统计信息趋势图以及对应的用户/IP。

趋势图：点击“趋势图”标签页，查看所选应用的趋势图。包括即时趋势、1 小时趋势、24 小时趋势以及 30 天趋势。

用户/IP：点击“用户/IP",标签页，查看所选应用被阻断的用户/IP 的详细统计信息。从列表中点击选中用户/IP，系统将打开<应用阻断详情>页面，显示所选用户/IP 的实时阻断趋势图。点击列表“操作”栏中，跳转到对应的用户/IP 页面。

点击上方 过滤 添加过滤条件，列表将显示对应的应用阻断信息。

点击列表下方的刷新按钮实时刷新列表信息。

用户/IP

点击“监控>应用阻断>用户/IP”或者点击概览页面“前 10 用户/IP 访问情况”图表右上角图标。

该页面以列表方式列出用户/IP 的以及具体阻断数据。

通过选中列表中不同的用户/IP，点击条目前“+”，可查看相应的用户/IP 的阻断统计信息趋势图以及应用阻断详情列表。点击列表“操作”栏中，跳转到对应的详情页面。

点击上方 过滤 添加过滤条件，列表将显示对应的用户/IP 的以及具体阻断数据。

统计周期

系统支持预定义统计周期。用户可以通过统计周期下拉菜单（ 最近一天 ）指定统计周期：

实时: 显示当前的统计信息。

最近 1 小时: 显示最近 1 小时的统计信息。

最近 1 天: 显示最近 1 天的统计信息。

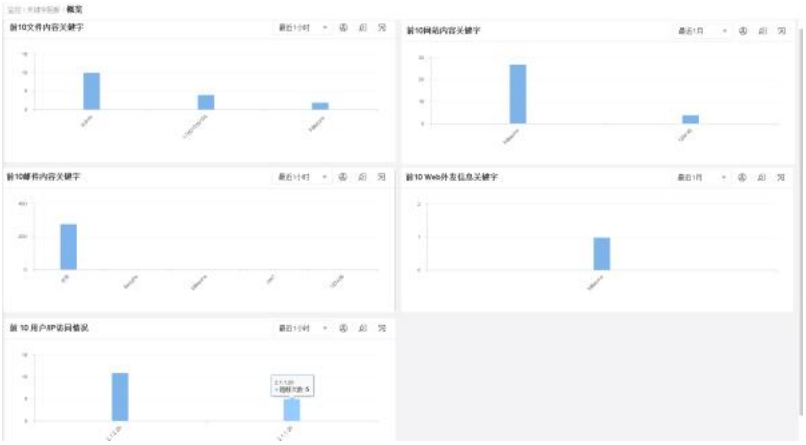
最近 1 月: 显示最近 1 月的统计信息。

关键字阻断

系统配置上网行为控制的文件内容过滤、网页关键字、"邮件过滤、Web 外发信息功能后，关键字阻断页面展现文件内容关键字、网页关键字、邮件内容关键字、 Web 外发信息关键字阻断次数统计信息以及用户/IP 统计信息。

概览

概览页面为用户展示指定时间周期内被阻断次数最多的前 10 文件内容关键字、前 10 网站内容关键字、前 10 邮件内容关键字、前 10 Web 外发信息关键字以及前 10 用户/IP 访问情况统计信息。点击“监控>关键字阻断>概览”。



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。

鼠标悬停在某关键字对应的柱状图上，查看该关键字的被阻断次数。

点击各图表右上角图标，进入对应的详情页面。

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。

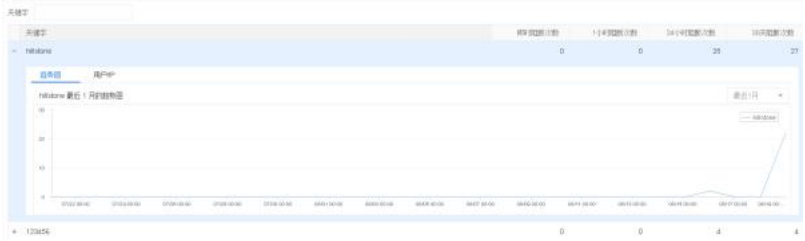
文件内容

点击“监控>关键字阻断>文件内容”或者点击概览页面“前 10 文件内容关键字”图表右上角图标，进入网页关键字统计页面。

页面说明见网页关键字说明。

网页关键字

点击“监控>关键字阻断>网页关键字”或者点击概览页面“前 10 网站内容关键字”图表右上角图标，进入网页关键字统计页面。



该页面上方以列表方式列出网站关键字的名称以及具体阻断数据。

点击不同的网页关键字前的“+”，可在条目下方查看相应的关键字阻断统计信息趋势图以及对应的用户/IP。

趋势图：点击“趋势图”标签页，查看所选关键字的趋势图。包括即时趋势、1 小时趋势、24 小时趋势以及 30 天趋势。

用户/IP：点击“用户/IP",标签页，查看所选关键字被阻断的用户/IP 的详细统计信息。从列表中点击选中用户/IP，系统将打开<关键字阻断详情>对话框，显示所选用户/IP 的实时阻断趋势图。点击列表“操作”栏中，跳转到对应的用户/IP 页面。

点击 过滤 添加过滤条件，列表将显示对应的关键字信息。

点击列表下方的刷新按钮实时刷新列表信息。

邮件内容

点击“监控>关键字阻断>邮件内容”或者点击概览页面“前 10 邮件内容关键字”图表右上角图标，进入邮件内容统计页面。

页面说明见网页关键字说明。

Web 外发信息

点击“监控>关键字阻断>Web 外发信息”或者点击概览页面“前 10Web 外发信息关键字”图表右上角图标，进入 Web 外发信息统计页面。

页面说明见网页关键字说明。

用户/IP

点击“监控>关键字阻断>用户/IP”或者点击概览页面“前 10 用户/IP 访问情况”图表右上角图标，进入用户/IP 详情统计页面。

该页面上方以列表方式列出用户的以及具体阻断数据。

点击不同的用户/IP 前的“+”，可在页面下方查看相应的用户/IP 的阻断统计信息趋势图、网站内容阻断详情列表、邮件内容阻断详情列表以及 Web 外发信息阻断详情。点击列表”操作“栏中，跳转到对应的详情页面。

点击上方 过滤 添加过滤条件，列表将显示对应的用户/IP 详情信息。

统计周期

系统支持预定义统计周期。用户可以通过统计周期下拉菜单（ 最近一天 ）指定统计周期：

实时: 显示当前的统计信息。

最近 1 小时: 显示最近 1 小时的统计信息。

最近 1 天: 显示最近 1 天的统计信息。

最近 1 月: 显示最近 1 月的统计信息。

认证用户

系统配置 Web 认证、单点登录、802.1x 认证、SSL VPN、L2TP VPN 等功能后，认证用户页面统计认证登录的用户信息。仅当系统版本为 IPv6 版本时，“IP/MAC”列表可显示认证用户的 IPv6 地址。

点击“监控>认证用户”，进入<认证用户>页面。

点击 过滤 添加过滤条件，符合条件的信息将显示在用户信息列表中，过滤条件包括用户名/用户组、AAA 服务器、IP/IP 段以及认证类型，可同时选择多个过滤条件。

在列表中“操作”栏点击“踢出”可以把对应的用户踢出系统。

点击列表下方的刷新按钮实时刷新列表信息。

锁定用户

系统配置防暴力破解功能后，锁定用户页面统计所有被锁定的用户信息，包括被锁定用户的名称、锁定时间、锁定时长以及可以执行的操作。

点击“监控>锁定用户”，打开锁定用户页面。

点击“AAA 服务器”下拉菜单，选择 AAA 服务器名称，对应所选 AAA 服务器的锁定用户信息将显示在列表中；

点击 过滤 添加过滤条件，符合条件的信息将显示在锁定用户信息列表中；

在列表中“操作”栏点击“删除”解除对应用户的锁定并且在锁定列表中删除。

点击“删除所有锁定用户”，解除所有用户的锁定并且在锁定列表中删除。

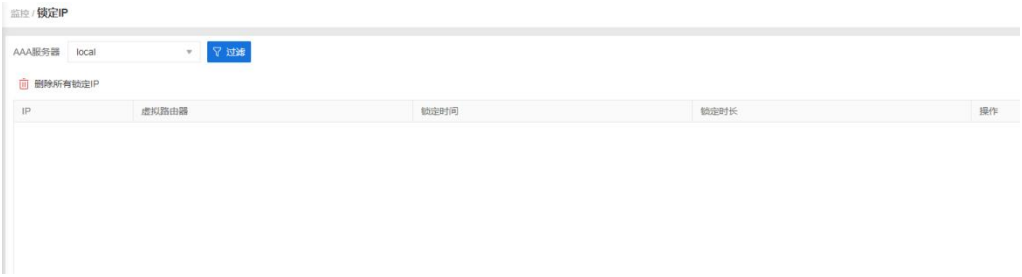
注意:

锁定用户列表最多允许包含 2000 个锁定 IP 信息，当锁定用户超过 2000 个时，将会解除对最早锁定用户的锁定。

锁定 IP

系统配置防暴力破解功能后，锁定 IP 页面统计所有被锁定的 IP 信息，包括被锁定 IP 地址、锁定时间、锁定时长以及可以执行的操作。

点击“监控>锁定 IP”，打开锁定 IP 页面。



点击“AAA 服务器”下拉菜单，选择 AAA 服务器名称，对应所选 AAA 服务器的锁定 IP 信息将显示在列表中；

点击 

添加过滤条件，符合条件的信息将显示在锁定 IP 信息列表中；

在列表中“操作”栏点击“删除”解除对应 IP 地址的锁定并且在锁定列表中删除。

点击“删除所有锁定用户”，解除所有 IP 的锁定并且在锁定列表中删除。

监控配置

用户可以根据需要开启或者关闭部分监控项目。认证用户监控项目会根据配置自动开启。

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. 点击监控项目对应的“启用”按钮开启对应的监控项目；点击监控项目的“禁用”按钮关闭对应的监控项目。

3. 在“IPv4 内网监控地址簿”及“IPv6 内网监控地址簿”下拉列表下，指定内网监控地址簿，系统会根据该地址簿对外网到内网中的流量进行匹配，并将匹配到的流量统计到内网 IP 侧。点击搜索框中的 ▼ 按钮，可以按地址簿名称和地址成员的 IP 进行模糊搜索，名称和地址是与的关系。

4. 配置完成，点击“确定”按钮保存所做配置。

注意:

地址支持多种输入方式，例如：输入“地址”为 10.10.10.10/32，可能匹配到包含地址成员是 10.10.10.10/24 的地址簿；输入“地址”为段掩码 9.9.9.9/24，可能匹配到包含地址成员是 9.9.0.0/16 的地址簿；输入“地址”为 10.10.10.10，可能匹配到地址成员的 IP 范围为 10.10.10.0-10.10.10.255 的地址簿；输入“地址”为 10.23，可能匹配到包含地址成员是 1.10.23.10/24 的地址簿；输入“地址”为 aa，可能匹配到地址成员的“主机名称”为 aaa 的地址簿。

自定义监控

自定义监控统计集为用户提供更加灵活的统计信息查看方法，用户可以根据需要查看相关的统计信息。根据所选数据类型的不同，可统计的数据信息也不同。如设备开启 IPv6 功能，系统支持 IPv4 和 IPv6 地址的统计。

基于 IP 数据类型的统计数据信息表

方式	条件	统计数据类型					
		流量	会话	新建会话速率	URL 访问次数	关键字阻断次数	应用阻断次数
无方向	发起者 (initiator)	统计发起会话 IP 的流量	统计发起会话 IP 的会话个数	统计发起会话 IP 的新建会话速率	统计 IP 的 URL 命中次数	统计 IP 的关键字阻断次数	统计 IP 的应用阻断次数
	回应者 (responder)	统计接收会话 IP 的流量	统计接收会话 IP 的会话个数	统计接收会话 IP 的新建会话速率			
	属于安全域 (belong to zone)	统计属于某安全域的 IP 的流量	统计属于某安全域的 IP 的会话数	统计属于某安全域的 IP 的新建会话速率			
	不属于安全域 (not belong to zone)	统计不属于某安全域的 IP 的流量	统计不属于某安全域的 IP 的会话数	统计不属于某安全域的 IP 的新建会话速率			
	属于接口 (belong to interface)	统计属于某接口的 IP 的流量	统计属于某接口的 IP 的会话数	统计属于某接口的 IP 的新建会话速率			
	不属于接口 (not belong to interface)	统计不属于某接口的 IP 的流量	统计不属于某接口的 IP 的会话数	统计不属于某接口的 IP 的新建会话速率			
双向	发起者 (initiator)	统计发起会话 IP 的上行和下行流量	统计发起会话 IP 的接收和发送会话个数	统计发起会话 IP 的接收和发送新建会话速率			
	回应者	统计接收	统计接收	统计接收			

方式	条件	统计数据类型					
		流量	会话	新建会话速率	URL 访问次数	关键字阻断次数	应用阻断次数
	(responder)	会话 IP 的上行和下行流量	会话 IP 的接收和发送会话个数	会话 IP 的接收和发送新建会话速率			
	属于安全域 (belong to zone)	统计属于某安全域的 IP 的上行和下行流量	统计属于某安全域的 IP 的接收和发送会话个数	统计属于某安全域的 IP 的接收和发送新建会话速率			
	不属于安全域 (not belong to zone)	统计不属于某安全域的 IP 的上行和下行流量	统计不属于某安全域的 IP 的接收和发送会话个数	统计不属于某安全域的 IP 的接收和发送新建会话速率			
	属于接口 (belong to interface)	统计属于某接口的 IP 的上行和下行流量	统计属于某接口的 IP 的接收和发送会话个数	统计属于某接口的 IP 的接收和发送新建会话速率			
	不属于接口 (not belong to interface)	统计不属于某接口的 IP 的上行和下行流量	统计不属于某接口的 IP 的接收和发送会话个数	统计不属于某接口的 IP 的接收和发送新建会话速率			

基于安全域、接口、用户、应用、URL、URL 类别、VSYS 的统计数据信息表

组织方式	方式	统计数据类型					
		流量	会话	新建会话速率	URL 命中次数	关键字阻断	应用阻断次数
安全域	无方向	统计安全域的流量	统计安全域的会话个数	统计安全域的新建会话速率	统计安全域的 URL 命中次数	N/A	N/A
	双向	统计安全域的上行和下行流量	统计安全域的接收和发送会话个数	统计安全域的接收和发送新建会话速			

组织方式	方式	统计数据类型					
		流量	会话	新建会话速率	URL 命中次数	关键字阻断	应用阻断次数
				率			
接口	无方向	统计接口的流量	统计接口的会话个数	统计接口的新建会话速率	统计接口的 URL 命中次数	N/A	N/A
	双向	统计接口的上行和下行流量	统计接口的接收和发送会话个数	统计接口的接收和发送新建会话速率			
应用	N/A	统计应用的流量	统计应用的会话个数	统计应用的新建会话速率	N/A	N/A	统计应用的应用阻断次数
用户	无方向	统计用户的流量	统计用户的会话个数	统计用户的新建会话速率	统计用户的 URL 命中次数	统计用户的关键字阻断次数	统计用户的应用阻断次数
	双向	统计用户的上行和下行流量					
URL	N/A	N/A	N/A	N/A	统计 URL 命中次数	N/A	N/A
URL 类别	N/A	N/A	N/A	N/A	统计 URL 类别命中次数	N/A	N/A
VSYS	N/A	统计 VSYS 的带宽	统计 VSYS 的会话个数	统计 VSYS 的新建会话速率	统计 VSYS 的 URL 命中次数	N/A	N/A

用户可以为统计集配置过滤条件，以统计特定条件下的数据信息，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。系统最多允许每个统计集配置 32 个过滤条件，其中用户名称、用户组和用户角色每种最多可以配置 8 个过滤条件。如果为同一个统计集配置的多个过滤条件属于同一类型，那么这些过滤条件之间为逻辑“或”（or）的关系；如果分属不同类型，那么这些过滤条件之间为逻辑“与”（and）的关系。

自定义监控功能的所有过滤条件类型表

类型	描述
安全域（filter zone）	以安全域为条件进行过滤
安全域-流入（filter zone zone-name	以入安全域为条件进行过滤

类型	描述
ingress）	
安全域-流出（filter zone zone-name egress）	以出安全域为条件进行过滤
接口（filter interface）	以接口为条件进行过滤
接口-流入（filter interface if-name ingress）	以入接口为条件进行过滤
接口-流出（filter interface if-name egress）	以出接口为条件进行过滤
应用（filter application）	以应用为条件进行过滤
地址条目（filter ip）	以地址条目为条件进行过滤
地址条目-源（filter ip add-entry source）	以源地址（地址条目）为条件进行过滤
地址条目-目的（filter ip add-entry destination）	以目的地址（地址条目）为条件进行过滤
IP/掩码（filter ip A.B.C.D/M）	以 IP 为条件进行过滤
IP/掩码-源（filter ip A.B.C.D/M source）	以源 IP 为条件进行过滤
IP/掩码-目的（filter ip A.B.C.D/M destination）	以目的 IP 为条件进行过滤
用户（filter user）	以用户名称为条件进行过滤
用户组（filter user-group）	以用户组名称为条件进行过滤
用户角色（filter role）	以用户角色名称为条件进行过滤
服务（filter service）	以服务名称为条件进行过滤

自定义监控页面展现所有监控统计集的状态、统计数据类型以及数据组织方式。点击“监控 > 自定义监控”。

点击”新建“按钮，在<自定义监控配置>页面新建监控统计集。

点击列表中监控统计集名称链接，查看监控统计集信息。

新建监控统计集

新建监控统计集，请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>页面填写规则的基本信息。

选项	说明
监控统计集名称	指定将要创建的统计集的名称。长度为 1-31 个字符。
统计数据类型	在下拉菜单中选择统计数据类型。
数据组织方式	在下拉菜单中选择数据组织方式。
只统计根虚拟系统	如仅需对根 VSYS 做数据统计，点击“只统计根虚拟系统”后的“启用”按钮。此选项仅当统计数据类型为流量统计、会话统计、新建会话统计、URL 访问次数统计时有效。指定数据组织方式为 VSYS 后，该选项不可用。
高级配置	如果需要配置过滤条件，点击“高级配置”，展开高级配置项，添加过滤条件。过滤条件的具体说明请参考以上“自定义监控功能的所有过滤条件类型表”。

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

注意: 配置统计集时：

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。

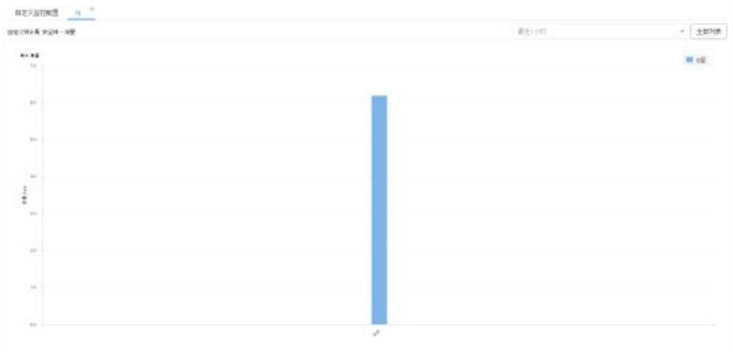
如果统计数据类型为流量、会话、新建会话速率或者 URL 访问次数，则相应的过滤条件不能为攻击类型。

如果统计数据类型为 URL 访问次数，则相应的过滤条件不能为服务。

进行配置时，系统会根据选择的选项自动屏蔽不可用选项。

查看监控统计集信息

查看监控统计集的统计信息，在自定义监控页面统计集列表中点击某个统计集的名称，将打开对应的标签页，显示所选监控统计集的统计结果。



通过柱状图查看前十统计集数据的统计结果。

通过统计周期下拉菜单指定统计周期，从而选择查看历史统计信息。

点击“全部列表”，以列表方式查看该监控统计集的所有统计信息，下方查看统计趋势图；点击“前十数据”返回柱状图显示页面。

报表

系统为用户提供直观、丰富的统计报表，通过对网络风险、网络访问、设备信息等方面进行综合分析，为用户呈现全方位、多角度的统计报告。

用户可通过报表模板和报表任务制定报表任务，生成对应的报表，在报表汇总中查看或者下载生成的报表文件。

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“监控>报表>报表汇总”，打开报表汇总页面。

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。

报表模板

报表模板是报表文件的基础，要生成报表文件，需要首先配置报表模板，报表模板规定报表文件的统计内容。

报表模板分为预定义报表模板和自定义报表模板，提供多种预分类的报表项内容。

预定义报表模板：系统内置报表模板，已根据类别默认选择对应的报表项内容，不可编辑或删除。包括如下预定义报表模板：

类别	说明
全局网络及风险评估报表	统计分析全局网络及风险状况，涵盖整体概览、网络及应用流量、网络威胁、主机详情等相关信息。
网络及应用流量报表	统计分析当前网络访问的基本情况，涵盖网络流量、应用流量访问、URL 访问等相关信息。
网络威胁报表	统计分析当前网络中存在的网络威胁，涵盖威胁趋势、外部攻击区域、威胁类型统计等信息。

自定义报表模板：用户按照需求创建的报表模板，勾选需要的报表项内容。最多可以创建 32 个自定义报表模板。

新建自定义报表模板

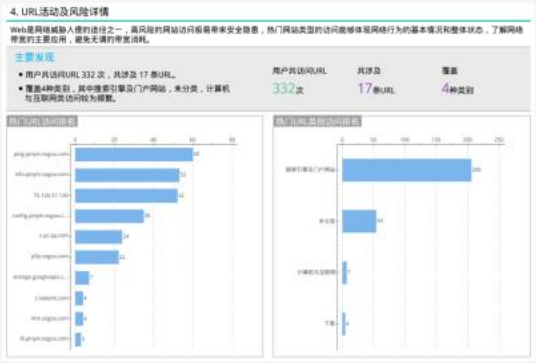
新建自定义报表模板，请按照以下步骤进行操作：

1. 点击“监控>报表>模板”。
2. 点击“新建”按钮，打开<报表模板配置>页面。

在<报表模板配置>页面，填写自定义报表模板配置信息。

选项	说明
名称	指定自定义报表模板的名称。范围是 1 到 128 个字符。
描述	指定自定义报表模板的描述信息。范围是 0 到 255 个字符。
内容	勾选需要统计的报表项内容复选框，使报表只统计特定的内容。默

选项	说明
	认情况下，勾选所有报表项内容。报表项内容说明如下： 网络及安全风险概况：针对全网的健康状态和安全风险程度，进行综合整体的评估以及概览统计。  网络流量详情：反映网络使用的整体情况，通过统计相关流量，了解链路带宽的利用情况。  应用统计及风险详情：统计设备的所有应用的流量，掌握内网的主要业务应用使用情况。点击“TOP”下拉菜单，指定需要统计流量的应用排名数量，包括 TOP5、TOP10、TOP20 以及 TOP50。  URL 活动及风险详情：统计设备的 URL 访问趋势以及排名情况。

选项	说明
	 网络风险威胁详情：统计设备检测到的威胁事件、外部攻击分布等，从而了解当前网络中存在的网络威胁、风险程度。  威胁说明：威胁的详细描述说明，帮助用户了解威胁信息。 

3. 点击“确定”按钮完成配置。

编辑自定义报表模板

编辑自定义报表模板，请按照以下步骤进行操作：

1. 点击“监控>报表>模板”。

2. 在模板列表中，勾选需要编辑的自定义报表模板条目。
3. 点击列表上方的“编辑”按钮，打开<报表模板配置>页面，对所选模板进行编辑。
4. 编辑完成后，点击“确定”按钮完成配置。

删除自定义报表模板

删除自定义报表模板，请按照以下步骤进行操作：

1. 点击“监控>报表>模板”。
2. 在模板列表中，勾选需要删除的自定义报表模板条目。
3. 点击列表上方的“删除”按钮完成删除。

克隆报表模板

系统支持将某一报表模板快速克隆，用户只要将克隆的报表模板的部分参数进行修改，即可生成一个新的报表模板。

克隆报表模板，请按照以下步骤进行操作：

1. 选择“监控>报表>模板”。
2. 在模板列表中，勾选需要克隆的一个报表模板条目。
3. 点击列表上方的“克隆”按钮，在打开的<报表模板配置>页面的“名称”文本框，输入新克隆的报表模板名称。
4. 列表中将生成一个克隆的报表模板。

报表任务

报表任务是与报表生成有关的时间计划，它规定报表文件使用的报表模板、威胁数据范围、生成周期和生成时间，以及输出方式。

用户可以在设备上按照需求配置报表任务，生成报表文件。

新建报表任务

新建报表任务，请按照以下步骤进行操作：

1. 点击“监控>报表>报表任务”。

2. 点击“新建”按钮，打开<报表任务配置>页面。

填写报表任务配置信息。

选项	说明
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。

点击“报表模板选择”展开配置项，选择报表任务需要使用的报表模板。

选项	说明
报表模板选择	指定报表任务需要使用的报表模板： 1. 从左侧的“报表模板”列表中选中报表模板（预定义报表模板或已创建的自定义报表模板）。 2. 选中报表模板后，右侧“已选报表模板”列表展示该模板的描述和报表项详细内容。 用户还可以在左侧“报表模板”列表中，点击“新建”或“编辑”按钮，快速打开<报表模板配置>页面，新建或编辑自定义报表模板。

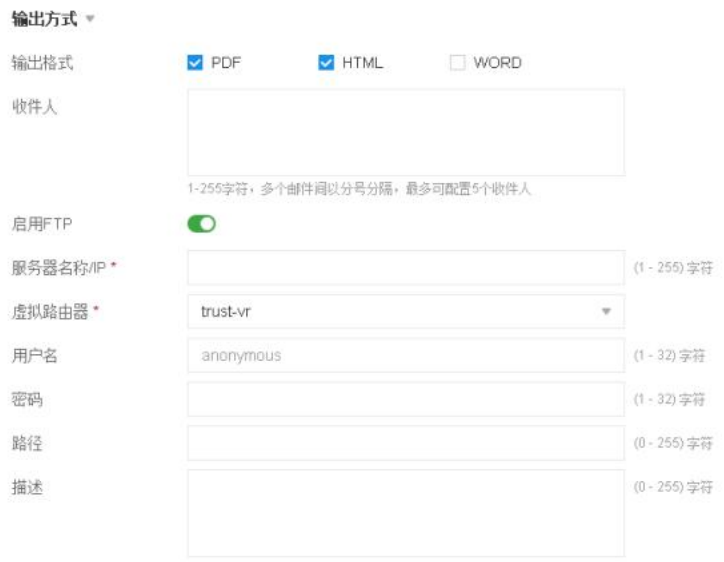
点击“威胁数据范围”展开配置项，配置威胁数据范围。

选项	说明
威胁类型	指定生成报表统计数据的威胁类型，包括扫描、网络攻击、拒绝服务、网络钓鱼、垃圾邮件和恶意软件六类威胁。
威胁级别	指定生成报表统计数据的威胁级别，包括“严重”、“高”、“中”、“低”四种级别。
安全域	指定生成报表统计数据的安全域。 1. 点击“安全域”下拉菜单的“+”。 2. 在右侧弹出的下拉列表中指定安全域。 如需编辑安全域的配置信息，可将鼠标悬浮在该安全域条目上，然后点击按钮进入安全域配置页面进行修改。 如需创建新的安全域，在右侧弹出的下拉列表中点击按钮进入安全域配置页面进行创建。
接口	指定生成报表统计数据的接口。 1. 点击“接口”下拉菜单的“+”。 2. 在右侧弹出的下拉列表中指定接口。 如需编辑接口的配置信息，可将鼠标悬浮在该接口条目上，然后点击按钮进入指定的接口配置页面进行修改。 如需创建新的接口，在右侧弹出的下拉列表中点击按钮进入指定的接口配置页面进行创建。
IP	指定生成报表统计数据的 IP 地址范围。IP 统计范围包含源 IP 和目的 IP。 1. 点击“IP”下拉菜单中的“+”。 2. 在弹出页面中的下拉菜单中选择 IP 地址类型，包括 IP/掩

选项	说明
	码、IPv4 范围、IPv6/前缀长度和 IPv6 范围。 3. 根据地址类型的不同，输入需要的地址。 4. 点击 “添加”按钮将所选择的地址添加到该页面右侧列表中。 5. 如果需要删除添加的地址，在右侧列表中需要删除的地址右侧点击×按钮。

点击“生成计划”展开配置项，填写报表任务的生成时间配置信息。

选项	说明
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：指定生成报表文件的时间。 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。该周期时间可指定到具体时刻，但结束时刻与开始时刻的间隔不应小于 24 小时，且不能超过 1 年。



点击“输出方式”展开配置项，填写报表的输出方式信息。

选项	说明
输出格式	指定报表文件的输出格式，包括 PDF 格式、HTML 格式以及 WORD 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，邮件地址之间以分号“;”隔开，最多可以配置 5 个收件人）。
启用 FTP	点击“启用 FTP”处启用按钮，将生成的报表文件发送到指定 FTP 服务器上。 发送报表文件到 FTP 服务器的配置参数说明如下： 服务器名称/IP：输入 FTP 服务器的名称或 IP 地址。 虚拟路由器：从下拉菜单选择 FTP 服务器所属的虚拟路由器。 如需创建新的虚拟路由器，点击下拉菜单，在弹出的下拉列表中点击 ⊕ 按钮进入虚拟路由器配置页面进行创建。 用户名：输入登录 FTP 服务器的用户名。 密码：输入用户名对应的密码。 修改密码：编辑报表任务配置时，可以看到修改密码功能。开启后，将展示密码输入框。如需修改，输入新的密码后保存配置即可。 匿名用户：选中“匿名用户”复选框，则不需要使用用户名和密码就可登录 FTP 服务器（适用于允许匿名登录的 FTP 服务器）。

选项	说明
	路径：输入要保存报表文件的文件夹路径。 描述：输入描述信息。

3. 点击“确定”按钮完成配置。

编辑报表任务

编辑报表任务，请按照以下步骤进行操作：

1. 点击“监控>报表>报表任务”。
2. 在报表任务列表中，勾选需要编辑的报表任务条目。
3. 点击列表上方的“编辑”按钮，打开<报表任务配置>页面，对所选报表任务进行编辑。
4. 编辑完成后，点击“确定”按钮完成配置。

删除报表任务

删除报表任务，请按照以下步骤进行操作：

1. 点击“监控>报表>报表任务”。
2. 在报表任务列表中，勾选需要删除的报表任务条目。
3. 点击列表上方的“删除”按钮完成删除。

启用/禁用报表任务

启用或禁用报表任务,请按照以下步骤进行操作：

1. 点击“监控>报表>报表任务”。
2. 选中列表中报表任务条目，点击列表上方“启用”或“禁用”按钮，系统将启用或禁用该报表任务。
   报表任务默认为启用状态。

报表状态

报表的生成可能需要消耗较长的时间，用户可以在报表状态页面查看报表任务的运行状态。实时报表任务在用户创建后就可以查看到，周期性报表任务在到达指定的执行时间后可以查看到。

点击“日志报表 > 报表 > 报表状态”，选择“进行中”查看当前报表任务的状态。

时间：表示执行报表任务执行已花费的时间。

报表任务名称：表示报表任务的名称。

状态：报表任务的运行状态，包含“等待中”、“运行中”、“已完成”。

停止任务：选择一个报表任务后，点击“停止任务”按钮可以停止报表任务。

自动刷新：点击“自动刷新”后的启用按钮，系统每隔 5 秒自动刷新“进行中”的报表任务。

点击“日志报表 > 报表 > 报表状态”，选择“已失败”查看已执行失败的报表任务。

时间：表示报表任务执行结束的时间。

报表任务名称：表示报表任务的名称。

状态：报表任务的运行状态，运行失败的任务状态会显示为“已失败”。

失败原因：报表任务执行失败的原因。

自动刷新：点击“自动刷新”后的启用按钮，系统每隔 5 秒自动刷新“已失败”的报表任务。

> 注意: 当关闭自动刷新功能时，将同时关闭“进行中”和“已失败”两个页面的自动刷新功能。

日志

设备支持日志管理功能。记录并输出设备的各种日志信息，分别是设备系统、威胁、云沙箱、会话、NAT、文件过滤、内容过滤、上网行为审计、共享接入以及 URL。

设备系统日志 - 包含事件日志信息、网络日志信息以及配置日志信息。

事件日志 - 包括错误、警告、通告、信息、调试、紧急、警报和严重 8 个级别的系统事件信息。

网络日志 - 与网络服务操作相关的日志信息，例如 PPPoE 以及 DDNS 等。

配置日志 - 与 CLI 配置相关的日志信息，例如接口配置等。

威胁日志 - 与系统威胁相关的日志信息，例如攻击防护和应用安全等。

会话日志 - 与会话相关的日志信息，例如会话的协议、源/目的 IP 地址、源/目的端口等。

NAT 日志 - 与 NAT 行为相关的日志信息，例如 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信息，例如用户的上网时间和网页访问情况、URL 过滤等。

EPP 日志 - 与终端防护相关的日志信息。

PBR 日志 - 策略路由日志信息，与策略路由相关日志信息。

文件过滤日志 - 与文件过滤相关的日志信息。

内容过滤日志 - 与内容过滤相关的日志信息，例如网页关键字过滤、Web 外发信息、邮件过滤或者应用程序控制。

上网行为审计日志 - 与上网行为相关的日志信息，例如 QQ 用户、微信用户、微博用户的使用情况等。

云沙箱日志 - 与沙箱检测相关的日志信息。

共享接入日志 - 与多终端共享接入相关的日志信息。

系统的多种日志信息能够有效的记录设备的运行情况，从而为用户分析网络情况和防护网络攻击提供依据。

日志的严重等级

系统的事件日志信息根据日志信息的严重程度区分的。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	日志定义
紧急（Emergencies）	0	系统不可用信息。	LOG_EMERG
警报（Alerts）	1	需要立即处理的信息，如设备受到攻击等。	LOG_ALERT
严重（Critical）	2	危急信息，如硬件出错。	LOG_CRIT
错误（Errors）	3	错误信息。	LOG_ERR
警告（Warnings）	4	报警信息。	LOG_WARNING
通告（Notifications）	5	非错误信息，但需要特殊处理。	LOG_NOTICE
信息（Informational）	6	通知信息。	LOG_INFO
调试（Debugging）	7	调试信息，包括正常的使用信息。	LOG_DEBUG

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。

本地数据库（Localdb）- 将日志信息发送到本地数据库。本地数据库存在于硬盘卡中。

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：**<设备号*8+日志严重等级> 时间设备序列号（VSYS 名称） 日志 ID Networks#日志类型 @模块：日志描述**请参阅以下示例：

<188>Mar 8 17:26:44 5821838205000143(root) 4424363e Networks#Traffic@FLOW:

SESSION: 2.1.1.200:53262(ethernet0/1)->3.1.1.200:21(ethernet0/0), Protocol TCP, vr trust-vr, policy 11, user -@-, host -, mac 0000.0000.0000, zone from trust to trust, session start

事件日志

用户可以在设备系统日志页面查看、搜索或导出事件日志。

点击“监控>日志>事件日志”，打开事件日志页面。

点击上方 

添加过滤条件，符合条件的信息将显示在日志列表中。

配置：点击该按钮，进入日志管理相关页面对事件日志信息进行配置。

导出：点击该按钮，以 TXT 或 CSV 格式导出全部或部分日志条目，并可以根据需要为导出的文件添加加密口令，添加后，用户需要输入指定的口令才能查看文件。

网络日志

用户可以在设备系统日志页面查看、搜索或导出网络日志。

点击“监控>日志>网络日志”，打开网络日志页面。

点击上方 

添加过滤条件，符合条件的信息将显示在日志列表中。

配置：点击该按钮，进入日志管理相关页面对网络日志信息进行配置。

导出：点击该按钮，以 TXT 或 CSV 格式导出全部或部分日志条目，，并可以根据需要为导出的文件添加加密口令，添加后，用户需要输入指定的口令才能查看文件。

配置日志

用户可以在设备系统日志页面查看、搜索或导出配置日志。

点击“监控>日志>配置日志”，打开配置日志页面。

点击上方  添加过滤条件，符合条件的信息将显示在日志列表中

配置：点击该按钮，进入日志管理相关页面对配置日志信息进行配置。

导出：点击该按钮，以 TXT 或 CSV 格式导出全部或部分日志条目，并可以根据需要为导出的文件添加加密口令，添加后，用户需要输入指定的口令才能查看文件。

共享接入日志

用户可以在设备系统日志页面查看、搜索或导出共享接入日志。

点击“监控>日志>共享接入日志”，打开共享接入日志页面。

点击  按钮添加过滤条件，符合条件的信息将显示在日志列表中。

配置：点击该按钮，进入日志管理相关页面对共享接入日志信息进行配置。

清除：点击该按钮，清除所有系统存储的共享接入日志信息。

导出：点击该按钮，以 TXT 或 CSV 格式导出全部或部分日志条目，并可以根据需要为导出的文件添加加密口令，添加后，用户需要输入指定的口令才能查看文件。

威胁日志

威胁日志信息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配置。

已经配置、入侵防御、攻击防护功能。具体功能请参阅相关页面。

点击“监控>日志>威胁日志信息”，打开威胁日志页面。

点击上方  添加过滤条件，符合条件的信息将显示在日志列表中。过滤条件如下：

查询时间 - 显示指定时间段的威胁日志信息。

类型 - 显示指定威胁类型的威胁日志信息。

级别 - 显示指定威胁级别的威胁日志信息。

源 - 显示指定攻击主机的威胁日志信息。支持 IPv4 和 IPv6 地址查询。

目的 - 显示指定受害主机的威胁日志信息。支持 IPv4 和 IPv6 地址查询。

检测引擎 - 显示指定检测引擎的威胁日志信息。检测引擎包括入侵防御、攻击防护、边界流量过滤、沙箱威胁检测、黑名单、加密流量检测。

源接口 - 显示指定源接口的威胁日志信息。

目的接口 - 显示指定目的接口的威胁日志信息。

源用户 - 显示指定源用户的威胁日志信息。

目的用户 - 显示指定目的用户的威胁日志信息。

CVE ID - 显示指定 CVE 编号的威胁日志信息。

CNNVD ID - 显示指定 CNNVD 编号的威胁日志信息。

处理动作 - 显示指定处理动作的威胁日志信息。

策略类型 - 显示指定策略类型的威胁日志信息。

策略 ID - 显示指定策略 ID 的威胁日志信息。

聚合类型：在下拉菜单选择列表所显示的内容的聚合类型，包括不聚合、威胁名称、源 IP 以及目的 IP。

配置：点击该按钮，进入日志管理相关页面对网络日志信息进行配置。导出：导出所有系统存储的威胁日志日志信息或者搜索结果信息（先进行搜索后再导出），并可以根据需要为导出的文件添加加密口令，添加后，用户需要输入指定的口令才能查看文件。

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。在详细信息页面，可以进行如下操作：

查看威胁的级别、应用协议、源/目的端口、威胁开始时间、结束时间及其他威胁相关的信息（如明文形式的 SQL 语句，URI 的明文路径等）。

点击“查看报文”链接可以查看该威胁对应的报文情况，也可点击“下载”,将报文下载到本地进行查看。系统支持抓取 IPv6 和 IPv4 协议类型的报文，供用户进行查看。

点击“特征 ID”选项后的“ID 号”、“加入白名单”、“禁用特征”执行相应的操作，可快速链接到相关界面，具体功能请参阅对应页面。

对于检测引擎为入侵防御的威胁日志，若用户开启了抓取完整的威胁数据功能，可点击“威胁数据”选项后的“下载”链接，将完整的威胁数据下载到本地进行查看。用户可通过“威胁数据”分析威胁发生的全过程。“威胁数据”是一个后缀名为*.buffer 的二进制文件，需使用二进制文件查看器进行查看。若未开启该功能，威胁日志详情页面将不显示“威胁数据” 选项。

对于检测引擎为入侵防御和病毒过滤的威胁日志，可点击“加入黑名单”将攻击源的 IP 地址加入系统的黑名单进行阻断。在打开的<静态 IP 黑名单>页面中，配置黑名单 IP，具体配置方法可参考静态 IP 黑名单。

在列表中，将光标悬浮在需要查看威胁情报的对象上方，右侧出现 ⋮ 按钮。点击该按钮，选择“查看威胁情报”，在云瞻威胁情报中心查看该情报的相关信息。威胁情报显示信息的含义，请参见 ICenter 的威胁事件部分。

会话日志

会话日志信息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。

已经为策略规则开启日志记录功能。

点击“监控>日志>会话日志”，打开会话日志页面。

点击上方 过滤 添加过滤条件，符合条件的信息将显示在日志列表中。会话日志过滤条件如下：

时间 - 显示指定时间范围（开始时间、结束时间）的会话日志信息。

策略 ID - 显示指定 ID 策略规则的会话日志信息。

源 IP - 显示指定源 IP 地址的会话日志信息。

源端口 - 显示指定源端口的会话日志信息。

目的 IP - 显示指定目的 IP 的会话日志信息。

目的端口 - 显示指定目的端口的会话日志信息。

协议 - 显示指定协议的会话日志信息。

行为 - 显示指定行为的会话日志信息。

会话结束原因 - 显示指定会话结束原因的会话日志信息。

配置：点击该按钮，进入**日志配置**相关页面对会话日志信息进行配置。

导出：以.txt 或.csv 格式导出所有系统存储的会话日志信息或者搜索结果信息（先进行搜索后再导出），并可以根据需要为导出的文件添加加密口令，添加后，用户需要输入指定的口令才能查看文件。

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。

PBR 日志

PBR 日志信息的产生需要满足以下两个条件：

已经开启设备的 PBR 日志功能。

已经为策略路由规则开启日志记录功能。

点击“监控>日志>PBR 日志”，打开 PBR 日志页面。

点击上方 过滤 添加过滤条件，符合条件的信息将显示在日志列表中。PBR 日志过滤条件如下：

时间 - 显示指定时间范围（开始时间、结束时间）的 PBR 日志信息。

PBR 名称/规则 ID - 在第一个文本框中输入 PRB 名称，在第二个文本框中输入策略路由规则 ID，显示指定 PBR 中的 ID 规则的 PBR 日志信息。

源 IP - 显示指定源 IP 地址的 PBR 日志信息。

源端口 - 显示指定源端口的 PBR 日志信息。

目的 IP - 显示指定目的 IP 的 PBR 日志信息。

目的端口 - 显示指定目的端口的 PBR 日志信息。

协议 - 显示指定协议的 PBR 日志信息。

应用 - 显示指定应用的 PBR 日志信息。

出接口 - 显示指定出接口的 PBR 日志信息。

配置：点击该按钮，进入日志配置相关页面对 PBR 日志信息进行配置。

导出：导出所有系统存储的 PBR 日志信息或者搜索结果信息（先进行搜索后再导出），并可以根据需要为导出的文件添加加密口令，添加后，用户需要输入指定的口令才能查看文件。

NAT 日志

NAT 日志信息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。

已经为 NAT 规则开启 NAT 日志功能。

点击“监控>日志>NAT 日志信息”，打开 NAT 日志页面。

点击上方 过滤 添加过滤条件，符合条件的信息将显示在日志列表中。NAT 日志过滤条件如下：

时间 - 显示指定时间范围（开始时间、结束时间）的 NAT 日志信息。

NAT 类型 - 显示指定类型（源 NAT、目的 NAT）的 NAT 日志信息。

规则 ID - 显示指定 ID 的 NAT 日志信息。

源 IP - 显示指定源 IP 地址的 NAT 日志信息。

源端口 - 显示指定源端口的 NAT 日志信息。

目的 IP - 显示指定目的 IP 的 NAT 日志信息。

目的端口 - 显示指定目的端口的 NAT 日志信息。

转换后 IP - 显示指定转换后 IP 地址的 NAT 日志信息。

转换后端口 - 显示指定转换后端口号的 NAT 日志信息。

协议 - 显示指定协议的 NAT 日志信息。

配置：点击该按钮，进入**日志配置相**关页面对 NAT 日志信息进行配置。

导出：导出所有系统存储的 NAT 日志信息或者搜索结果信息（先进行搜索后再导出），并可以根据需要为导出的文件添加加密口令，添加后，用户需要输入指定的口令才能查看文件。

URL 日志

URL 日志信息的产生需要满足以下条件：

已经开启设备的 URL 日志功能。

已经为 URL 过滤规则开启日志记录功能。

点击“监控>日志>URL 日志”，打开 URL 日志页面。

点击上方 过滤 添加过滤条件，符合条件的信息将显示在日志列表中。URL 日志过滤条件如下：

消息 - 显示包含指定消息的 URL 日志信息，可输入消息中的关键字进行过滤。

配置：点击该按钮，进入日志配置相关页面对 URL 日志信息进行配置。

清除：点击该按钮，清除所有系统存储 URL 日志信息。

导出：点击“导出”按钮，指定分隔符后，导出所有系统存储的 URL 日志信息或者搜索结果信息（先进行搜索后再导出），并可以根据需要为导出的文件添加加密口令，添加后，用户需要输入指定的口令才能查看文件。

文件过滤日志

文件过滤日志信息的产生需要满足以下两个条件：

已经开启设备的文件过滤日志功能。

系统配置了文件过滤功能。

点击“监控>日志>文件过滤日志”，打开文件过滤日志页面。

点击上方 过滤 添加过滤条件，符合条件的信息将显示在日志列表中。

配置：点击该按钮，进入日志配置相关页面对文件过滤日志信息进行配置。

清除：点击该按钮，清除所有系统存储文件过滤日志信息。

导出：点击“导出”按钮，指定分隔符后，导出所有系统存储的文件过滤日志信息或者搜索结果信息（先进行搜索后再导出），并可以根据需要为导出的文件添加加密口令，添加后，用户需要输入指定的口令才能查看文件。

内容过滤日志

内容过滤日志信息的产生需要满足以下两个条件：

已经开启设备的内容过滤日志功能。

系统配置了文件内容过滤、网页关键字、Web 外发信息、邮件过滤或者应用行为控制功能。具体功能请参阅相关页面。

点击“监控>日志>内容过滤日志”，打开内容过滤日志页面。

点击上方 过滤 添加过滤条件，符合条件的信息将显示在日志列表中。

配置：点击该按钮，进入日志配置相关页面对内容过滤日志信息进行配置。

清除：点击该按钮，清除所有系统存储内容过滤日志信息。

导出：点击“导出”按钮，指定分隔符后，导出所有系统存储的内容过滤日志信息或者搜索结果信息（先进行搜索后再导出），并可以根据需要为导出的文件添加加密口令，添加后，用户需要输入指定的口令才能查看文件。

上网行为审计日志

上网行为审计日志信息的产生需要满足以下两个条件：

已经开启设备的内容过滤日志功能。

系统配置了上网行为审计功能。具体功能请参阅相关页面。

点击“监控>日志>上网行为审计日志信息”，打开上网行为审计日志页面。

点击上方 

添加过滤条件，符合条件的信息将显示在日志列表中。

配置：点击该按钮，进入日志配置相关页面对上网行为审计日志信息进行配置。

清除：点击该按钮，清除所有系统存储上网行为审计日志信息。

导出：点击“导出”按钮，指定分隔符后，导出所有系统存储的上网行为审计日志信息或者搜索结果信息（先进行搜索后再导出），并可以根据需要为导出的文件添加加密口令，添加后，用户需要输入指定的口令才能查看文件。

云沙箱日志

用户可以在云沙箱日志页面查看、配置或导出云沙箱日志。

点击“监控>日志>云沙箱日志”，打开云沙箱日志页面。

点击上方 

添加过滤条件，符合条件的信息将显示在日志列表中。其中，过滤条件中的源和目的地址支持 IPv4 和 IPv6。

配置：点击该按钮，进入日志管理相关页面对网络日志信息进行配置。

导出：点击该按钮，以 TXT 或 CSV 格式导出全部或部分日志条目，并可以根据需要为导出的文件添加加密口令，添加后，用户需要输入指定的口令才能查看文件。

终端标签日志

系统支持配置终端标签日志功能对终端标签日志单独管理。配置和管理终端标签日志功能，请按照以下步骤操作：

1. 点击“监控 > 日志 > 终端标签日志”或点击“零信任访问 > 终端标签日志”。

时间：表示终端标签日志的生成时间。

类型：表示终端标签日志的类型，包括登录、登出、异常登出、强制下线、终端标签更新、应用资源更新。

用户名：表示用户名。

用户 IP：表示用户 IP 地址。

AAA 服务器：表示用户所属的 AAA 服务器名称。

终端名称：表示访问终端的名称。

终端 IP：表示访问终端的 IP 地址。

操作系统：表示访问终端的操作系统。

终端标签：表示用户关联的终端标签。

ZTNA 服务：表示用户访问的 ZTNA 服务名称。

允许访问的应用资源：表示允许用户访问的应用资源。

禁止访问的应用资源：表示禁止用户访问的应用资源。

2. 点击“配置”按钮，打开<终端标签日志>页面。

在<终端标签日志>页面配置相关参数

选项	说明
启用	点击开启系统的终端标签日志功能，并设置终端标签日志的输出目的地，可以设置多个目的地。终端标签日志功能默认为开启，日志输出目的地为缓存内存。
缓存	选中该复选框将终端标签日志信息输出到内存缓存。
最大缓存大小	设置了输出终端标签日志到内存缓存时，用户可以自定义最大缓存大小，取值范围是 4096 到 2097152，单位是字节。默认的缓存大小是 2097152。
日志服务器	选中该复选框将终端标签日志输出到系统日志服务器，输出的日志类型为明文，需先配置好日志服务器。点击“查看日志服务器”链接查看所有已配置的系统日志服务器。关于日志服务器的配置说明，请参阅日志服务器配置。

3. 点击“过滤”按钮，查看符合过滤条件的终端标签日志。

4. 点击“清除”按钮，将所有终端标签日志清除。

5. 点击“导出”按钮，将所有终端标签日志导出到本地文件。

日志管理

用户可以在日志管理界面配置各种类型日志的相关选项。

配置日志信息

配置各类型日志信息，请按照以下步骤进行操作：

1. 点击“监控>日志>日志管理”，打开日志管理页面。
2. 根据需要，点击<事件日志>/<网络日志>/<配置日志>/<共享接入日志>/<会话日志>/<NAT 日志>/<URL 日志>/<文件过滤日志>/<内容过滤日志>/<上网行为审计日志>/<威胁日志>/<云沙箱日志>/<终端标签日志>后的“启用”按钮，开启系统的相应日志功能；点击 按钮，配置相应的日志选项。不同类型日志配置选项不同。具体请参阅日志配置选项说明一节。
3. 配置完成后点击“确定”按钮。

日志配置选项说明

该节介绍不同类型日志的配置选项。

事件日志

选项	说明
启用	点击“启用”按钮，开启系统的事件日志功能。
Console	选中该复选框将事件日志信息输出到 Console。 最小日志级别 - 指定输出事件日志信息的最小日志级别。
终端	选中该复选框将事件日志信息输出到终端。 最小日志级别 - 指定输出事件日志信息的最小日志级别。
缓存	选中该复选框将事件日志信息输出到缓存。 最小日志级别 - 指定输出事件日志信息的最小日志级别。 最大缓存大小 - 指定输出事件日志信息的最大缓存大小。
本地数据库	选中该复选框将事件日志信息输出到本地硬盘卡。 最小日志级别 - 指定输出事件日志信息的最小日志级别。
文件	选中该复选框将事件日志信息输出到文件。 最小日志级别 - 指定输出事件日志信息的最小日志级别。

选项	说明
	最大文件大小 - 指定日志信息文件的最大值。范围是 4096 到 1048576 字节。默认是 1048576 字节。
日志服务器	选中该复选框将事件日志信息输出到日志服务器。 查看日志服务器 - 点击该链接查看所有已配置的系统日志服务器。 最小日志级别 - 指定输出事件日志信息的最小日志级别。
Email 地址	选中该复选框将事件日志信息输出到 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 - 指定输出事件日志信息的最小日志级别。
手机短信	选中该复选框将事件日志信息输出到手机短信。 最小日志级别 - 指定输出事件日志信息的最小日志级别。

网络日志

选项	说明
启用	点击“启用”按钮，开启系统的网络日志功能。
缓存	选中该复选框将网络日志信息输出到缓存。 最大缓存大小 - 指定输出网络日志信息的最大缓存大小。
文件	选中该复选框将网络日志信息输出到文件。 最大文件大小 - 指定日志信息文件的最大值。范围是 4096 到 1048576 字节。默认是 1048576 字节。
日志服务器	选中该复选框将网络日志信息输出到日志服务器。 查看日志服务器 - 点击该链接查看所有已配置的系统日志服务器。

配置日志

选项	说明
启用	点击“启用”按钮，开启系统的配置日志功能。
缓存	选中该复选框将配置日志信息输出到缓存。

选项	说明
	最大缓存大小 - 指定输出配置日志信息的最大缓存大小。
日志服务器	选中该复选框将配置日志信息输出到日志服务器。 查看日志服务器 - 点击该链接查看所有已配置的系统日志服务器。
日志限速	选中该复选框指定配置日志信息输出最大速率。 最大速率 - 指定输出配置日志信息的最大速率。

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信息输出到缓存。 最大缓存大小 - 指定输出会话日志信息的最大缓存大小。
日志服务器	选中该复选框将会话日志信息输出到日志服务器。 查看日志服务器 - 点击该链接查看所有已配置的系统日志服务器。 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 - 将会话日志信息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	点击“启用”按钮，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 日志信息输出到缓存。

选项	说明
	最大缓存大小 - 指定输出 NAT 日志信息的最大缓存大小。
日志服务器	选中该复选框将 NAT 日志信息输出到日志服务器。 查看日志服务器 - 点击该链接查看所有已配置的系统日志服务器。 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 日志信息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	点击“启用”按钮，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 日志信息输出到缓存。 最大缓存大小 - 指定输出 URL 日志信息的最大缓存大小。
日志服务器	选中该复选框将 URL 日志信息输出到日志服务器。 查看日志服务器 - 点击该链接查看所有已配置的系统日志服务器。 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 - 将会话日志信息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

文件过滤日志

选项	说明
启用	点击“启用”按钮，开启系统的文件过滤日志功能。
缓存	选中该复选框将文件过滤日志信息输出到缓存。

选项	说明
	最大缓存大小 - 指定输出文件过滤日志信息的最大缓存大小。
日志服务器	选中该复选框将文件过滤日志信息输出到日志服务器。 查看日志服务器 - 点击该链接查看所有已配置的系统日志服务器。 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 - 将会话日志信息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

内容过滤日志

选项	说明
启用	点击“启用”按钮，开启系统的内容过滤日志功能。
缓存	选中该复选框将内容过滤日志信息输出到缓存。 最大缓存大小 - 指定输出内容过滤日志信息的最大缓存大小。
日志服务器	选中该复选框将内容过滤日志信息输出到日志服务器。 查看日志服务器 - 点击该链接查看所有已配置的系统日志服务器。 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 - 将会话日志信息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

上网行为审计日志

选项	说明
启用	点击“启用”按钮，开启系统的上网行为审计日志功能。
缓存	选中该复选框将上网行为审计日志信息输出到缓存。 最大缓存大小 - 指定输出上网行为审计日志信息的最大缓存

选项	说明
	大小。
日志服务器	选中该复选框将上网行为审计日志信息输出到日志服务器。 查看日志服务器 - 点击该链接查看所有已配置的系统日志服务器。 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 - 将会话日志信息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

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。 记录用户名：在威胁日志中显示用户名称。
记录用户信息	点击“启用”按钮，开启威胁日志记录认证用户信息功能。开启该功能后，威胁日志中会记录认证用户信息，包括 AAA 服务器、用户名称、主机名称。
终端	选中该复选框将威胁日志选项输出到终端。
缓存	选中该复选框将威胁日志信息输出到缓存。 最大缓存大小 - 指定输出威胁日志信息的最大缓存大小。 最小日志级别 - 指定输出威胁日志信息的最小日志级别。
本地数据库	选中该复选框将威胁日志信息输出到本地硬盘卡。 最小日志级别 - 指定输出威胁日志信息的最小日志级别。
文件	选中该复选框将威胁日志信息输出到文件。 最小日志级别 - 指定输出威胁日志信息的最小日志级别。 最大文件大小 - 指定威胁日志信息文件的最大值。范围是 4096 到 1048576 字节。默认是 1048576 字节。
日志服务器	选中该复选框将威胁日志信息输出到日志服务器。

选项	说明
	查看日志服务器 - 点击该链接查看所有已配置的系统日志服务器。 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 - 将会话日志信息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。
Email 地址	选中该复选框将威胁日志信息输出到 Email 地址。 查看 Email 地址：点击该链接查看所有已配置的 Email 地址。

云沙箱日志

选项	说明
启用	点击“启用”按钮，开启系统的云沙箱日志功能。
缓存	选中该复选框将云沙箱日志信息输出到缓存。 最大缓存大小 - 指定输出云沙箱日志信息的最大缓存大小。
文件	选中该复选框将云沙箱日志信息输出到文件。
日志服务器	选中该复选框将云沙箱日志信息输出到日志服务器。 查看日志服务器 - 点击该链接查看所有已配置的系统日志服务器。

共享接入日志

选项	说明
启用	点击“启用”按钮，开启系统的共享接入日志功能。 记录主机名：在共享接入日志中显示主机名称。
Console	选中该复选框将共享接入日志信息输出到 Console。
缓存	选中该复选框将共享接入日志信息输出到缓存。 最大缓存大小 - 指定输出共享接入日志信息的最大缓存大小。

选项	说明
日志服务器	选中该复选框将共享接入日志信息输出到日志服务器。 查看日志服务器 - 点击该链接查看所有已配置的系统日志服务器。

终端标签日志

选项	说明
启用	点击开启系统的终端标签日志功能，并设置终端标签日志的输出目的地，可以设置多个目的地。终端标签日志功能默认为开启，日志输出目的地为缓存。
缓存	选中该复选框将终端标签日志信息输出到缓存。
最大缓存大小	设置了输出终端标签日志到缓存时，用户可以自定义最大缓存大小，单位是字节，取值范围是 4096 到 2097152。默认的缓存大小是 2097152。
本地数据库	选中该复选框将终端标签日志信息输出到本地硬盘卡。
日志服务器	选中该复选框将终端标签日志输出到系统日志服务器，输出的日志类型为明文，需先配置好日志服务器。点击“查看日志服务器”链接查看所有已配置的系统日志服务器。关于日志服务器的配置说明，请参阅日志服务器配置。

日志配置

用户可以在日志配置界面配置日志服务器、Web 邮件以及设备名称的相关选项。

日志服务器配置

用户可以在<日志服务器配置>页面新建、编辑或删除用于接收日志信息的日志服务器，同时可以进行发送源端口和日志编码的设置。

新建日志服务器

新建日志服务器，请按照以下步骤进行操作：

1. 点击“监控>日志>日志配置"，选择“日志服务器配置”标签页。

2. 点击“新建”按钮，打开<日志服务器配置>页面。

在<日志服务器配置>页面，配日志服务器相关信息。

选项	说明
主机名称	指定日志服务器的主机名称。
日志格式	指定日志服务器的日志格式，包括 Default，S5000 和 S6000，请根据对应的日志服务器类型进行选择。 Default - 表示该日志服务器仅可接收安全设备的日志格式。 S5000 - 表示该日志服务器仅可接收 SGCC-S5000 格式的日志，如国家电网日志服务器。 S6000 - 表示该日志服务器仅可接收 SGCC-S6000 格式的日志，如国家电网网监设备。
绑定方式	用户可以通过选择虚拟路由器或源接口，指定日志服务器接收日志信息的源 IP 地址： 虚拟路由器：在<虚拟路由器>下拉菜单中选择日志服务器所属的虚拟路由器。 源接口：在<源接口>下拉菜单选择设备发送日志信息的源接口。设备会以指定接口的 IP 地址为源 IP，向日志服务器发送日志信息。如果该接口配有管理 IP 地址，优先使用管理 IP 地址。
协议	选择系统日志服务器的协议类型。若选择“Secure-TCP”协议，用户可根据需要勾选“不验证服务器证书”复选框，系统将与

选项	说明
	日志服务器不需验证证书即可正常传输日志。
端口	输入系统日志服务器的协议端口号。
Hostname Standard	默认情况下，输出到 Syslog Server 的日志信息不显示年份、主机名称和日志严重等级，输出格式为：**<设备号*8+日志严重等级> 时间设备序列号（VSYS 名称） 日志 ID Networks#日志类型 @模块：日志描述**。选中该选项后，输出的日志信息显示主机名称，不显示设备序列号，输出格式为：**<设备号*8+日志严重等级> 时间主机名称 日志 ID Networks#日志类型 @模块：日志描述**。
日志类型	选择该系统日志服务器接收的日志信息的类型。

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。

设置发送源端口

系统支持指定向日志服务器发送日志信息时使用的源端口号。指定后，将日志信息输出到日志服务器时，系统将会使用该源端口。若不指定，系统将默认使用随机源端口将日志信息输出到日志服务器。

设置发送源端口，请按照以下步骤进行操作：

1. 点击“监控>日志>日志配置"，选择“日志服务器配置”标签页。
2. 点击右上角“发送源端口设置”按钮，进入<发送源端口设置>页面。

3. 输入指定的源端口号，范围是 1024 到 65535。若要取消对当前源端口号的配置，则删除当前源端口号的值。
4. 点击“确定”按钮，保存当前配置。

注意:

对于发送到日志服务器的二进制日志，将不受发送源端口配置的影响，通过 UDP 协议使用端口 5566 进行发送。

当启用 SNAT 功能时，系统会根据 NAT 转换后的网络地址端口资源随机选择端口作为发送源端口。

设置日志编码

输出到日志服务器的日志信息默认的编码格式为 UTF-8,用户可根据需要开启 GBK 编码。开启 GBK 编码格式后，输出到日志服务器的日志编码格式将变为 GBK 编码。设置日志编码格式，请按照以下步骤进行操作：

1. 点击“监控>日志>日志配置"，选择“日志服务器配置”标签页。
2. 点击右上角“日志编码设置”按钮，打开<日志编码配置>页面。
3. 点击“启用”按钮，启用日志 GBK 编码。
4. 点击“确定”按钮，保存当前配置。

Web 邮件配置

Web 邮件配置用于指定接收日志信息邮件的 Email 地址。

Web 邮件配置，请按照以下步骤进行操作：

1. 点击“监控 >日志 > 日志配置"，选择“Web 邮件配置”标签页。

2. 点击“新建”，弹出可编辑行，在<Email 地址>文本框中输入用于接收日志信息邮件的 Email 地址。
3. 如果需要删除，点击“删除”。

注意: 用户最多允许配置 3 个 Email 地址。

设备名称配置

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

设备名称配置，请按照以下步骤进行操作：

1. 点击“监控>日志>日志配置"，选择“设备名称配置”标签页。

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

手机短信配置

用于指定接收短信的手机号码。改选项适用于将日志信息以短信的形式发送到某个手机上。

手机短信配置，请按照以下步骤进行操作：

1. 点击“监控>日志>日志配置"，选择“手机短信配置”。
2. 点击“新建”，弹出可编辑行，在<手机号码>文本框中输入用于接收日志信息短信的手机号码。
3. 如果需要删除，点击“删除”。

> 注意: 用户最多允许配置 3 个手机号码。

日志参数配置

系统支持修改事件日志、网络日志、配置日志的参数，包括日志的描述信息、级别及开启/关闭日志输出。用户可以通过相应的日志页面修改指定日志的参数，并通过日志参数配置页面进行查看，也可以在日志参数配置页面编辑或删除日志条目。

编辑日志参数，请按照以下步骤进行操作：

1. 点击“监控>日志>日志配置"，选择“日志参数配置”。

2. 选择需要编辑日志参数的条目，点击“编辑”，在<日志参数配置>页面，编辑日志的描述信息、级别及开启/关闭生成日志。

3. 点击“确定”。

第 12 章 分析诊断

在线抓包工具：实时抓取系统中的数据包，并能够将抓取到的数据包导出到本地硬盘，然后通过第三方抓包工具查看数据包内容。

测试工具：设备支持域名检查，支持使用网络连接测试工具 Ping 和 Traceroute。当网络出现问题时，用户可以用这些工具对网络进行测试，查找故障原因。

在线抓包工具

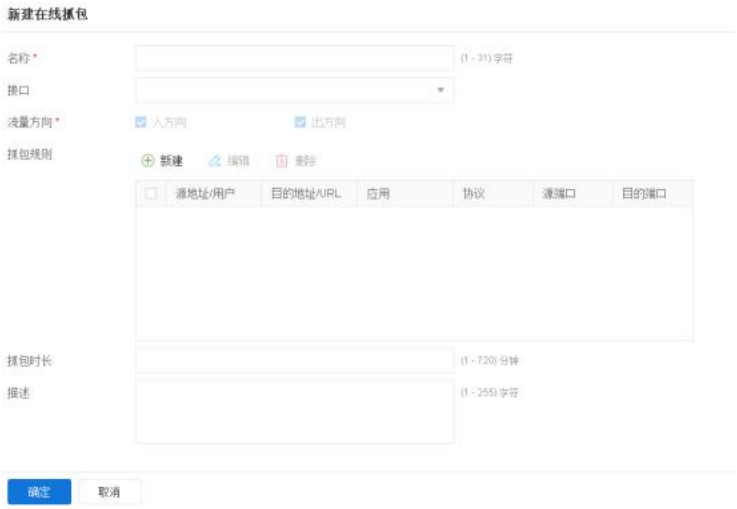
在线抓包工具支持创建抓包任务进行抓包，用户可在抓包任务中设置流量出入接口，以及添加一条或多条抓包规则，实时抓取多种条件的数据包，同时可随时查看当前抓包及丢包的情况。抓取到的数据包可被下载或导出到本地硬盘，然后用户可以通过第三方抓包工具查看数据包内容。

配置在线抓包任务

配置在线抓包任务，请按照以下步骤进行操作：

1. 选择“系统 > 诊断中心 > 在线抓包工具”，进入在线抓包工具配置页面。

2. 点击“新建”按钮，打开<新建在线抓包>页面。



在<新建在线抓包>页面中配置在线抓包任务

选项	说明
名称	指定在线抓包任务的名称。
接口	在下拉菜单中指定在线抓包任务的接口。
流量方向	指定接口的流量方向，入方向或出方向。默认是同时设置入方向和出方向。 入方向：在线抓包任务抓取入接口的报文。如果没有抓取到，该报文可能已被防火墙防护或没有进入防火墙。若没有进入防火墙，如有需要可以进一步排查上行链路或上行设备的情况。 出方向：在线抓包任务抓取出接口的报文。如果抓取到，如有需要可以进一步排查下行链路或下行设备的情况。 入方向+出方向：用户可以同时设置入方向和出方向，根据抓取的数据包可判断该接口实际的流量方向。
抓包规则	点击“新建”按钮，在打开的<抓包规则>页面配置抓包规则。 勾选列表中抓包规则复选框，点击“编辑”按钮，可以重新编辑抓包规则的配置信息。 勾选列表中抓包规则复选框，点击“删除”按钮，删除所选抓包规则。
抓包时长	指定抓包任务的生效时长，范围是 1 到 720 分钟，默认值为 30 分钟。
描述	指定抓包任务的描述信息。范围是 1 到 255 个字符。

3. 点击“确定”按钮完成创建。配置完成后，在线抓包任务将自动添加到下方列表。

4. 点击列表中任一在线抓包任务对应的“开始抓包”按钮，开始执行抓包任务，“开始抓包”按钮将变为“抓包中”。点击"状态"按钮，打开<抓包状态>页面，可查看当前抓包大小/数量。

5. 点击在线抓包任务对应的“抓包中”按钮，停止抓包。

6. 抓包停止或者抓包完成后，抓取到的报文文件将在页面下方的<报文文件列表>中显示，点击“报文下载”处的下载按钮进行下载。

7. 可选中一条或多条抓包文件条目，点击列表右上角的“导出”按钮，导出抓包文件，导出的抓包文件为压缩文件。

8. 若需清除抓包数据，可选中一条在线抓包任务，点击“清除数据”按钮，该任务下抓取的报文文件都将被清除。

注意:

系统最多允许创建 5 条在线抓包任务。

在线抓包任务无法基于隧道接口抓取数据包。

导出抓包文件时，如果抓包文件过大可能会导致文件因导出超时而失败，建议单次抓包的文件不大于 500M。

新建抓包规则

新建抓包规则，请按照以下步骤进行操作：

1. 选择“系统 > 诊断中心 > 在线抓包工具”，进入在线抓包工具配置页面。

2. 点击“新建”按钮，打开<新建在线抓包>页面。

3. 点击“抓包规则”处的“新建”按钮，打开<抓包规则>页面。

在<抓包规则>页面中配置抓包规则。

选项	说明
源类型	点击下拉菜单，选择需要抓取数据包的源地址类型。

选项	说明
	IP/掩码：在文本框中输入 IPv4 类型的源地址及掩码，不输入表示 any。 IP 范围：在文本框中输入 IPv4 类型的源地址范围，不输入表示 any。 IPv6/前缀长度：在文本框中输入 IPv6 类型的源地址及前缀长度，不输入表示 any。 IPv6 范围：在文本框中输入 IPv6 类型的源地址范围，不输入表示 any。 用户/用户组：在下拉菜单中指定 AAA 服务器并选择用户/用户组，或者直接添加用户/用户组。不选择表示 any。
目的类型	点击下拉菜单，选择需要抓取数据包的目的地址类型。 IP/掩码：在文本框中输入 IPv4 类型的目的地址及掩码，不输入表示 any。 IP 范围：在文本框中输入 IPv4 类型的目的地址范围，不输入表示 any。 IPv6/前缀长度：在文本框中输入 IPv6 类型的目的地址及前缀长度，不输入表示 any。 IPv6 范围：在文本框中输入 IPv6 类型的目的地址范围，不输入表示 any。 目的 URL：在文本框中输入目的 URL，不输入表示 any
应用	在下拉菜单中选中需要抓取数据包的应用类型，不选择表示 any。
协议	在下拉菜单中选中需要抓取数据包的协议类型或者协议号，不选择表示 any。

4. 点击“确定”按钮完成创建。

注意: 同一个抓包任务中最多允许创建 8 个抓包规则。

抓包全局配置

抓包全局配置项根据设备的类型不同而不同：

对于带硬盘的设备，用户可以配置抓包文件占硬盘总大小的百分比。

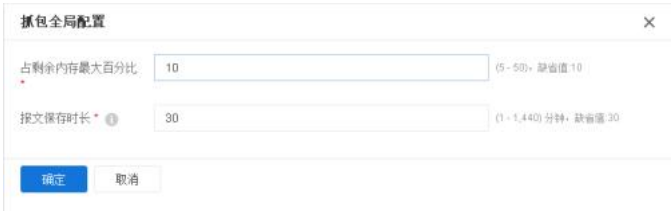
对于无硬盘的设备，用户可以配置抓包文件占剩余内存最大百分比和报文保存时长。

配置抓包全局配置项，请按照以下步骤进行操作：

1. 选择“系统 > 诊断中心 > 在线抓包工具”，进入在线抓包工具配置页面。
2. 点击页面右上角“全局配置”按钮，打开<抓包全局配置>页面。
3. 带硬盘的设备<抓包全局配置>页面如下：

选项	说明
硬盘百分比	在文本框中输入抓包文件占硬盘总大小的百分比，范围是 5%-50%，默认值是 10%。

4. 无硬盘的设备<抓包全局配置>页面如下：



选项	说明
占剩余内存最大百分比	在文本框中输入抓包文件允许占用剩余内存的最大百分比，范围是 5%-50%，默认值是 10%。
报文保存时长	在文本框中输入抓包文件保存的时长，单位为分钟，范围是 1-1440 分钟，默认值是 30 分钟。

5. 点击“确定”按钮完成配置。

测试工具

设备支持域名检查，支持使用网络连接测试工具 Ping 和 Traceroute。当网络出现问题时，用户可以用这些工具对网络进行测试，查找故障原因。

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 > 诊断中心 > 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 > 诊断中心 > 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。系统支持对 IPv4 和 IPv6 的对端地址进行测试。

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 > 诊断中心 > 测试工具”，进入测试工具页面。
2. 在“虚拟路由器”下拉列表中选择 VR。
3. 选择“IPv4”或“IPv6”，指定对端 IP 地址的类型。
4. 在“Traceroute”文本框中输入网络对端的 IP 地址。
5. 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 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。实现 HA 功能，用户需要配置两台采用完全相同型号的硬件平台、固件版本，VSYS 特性及相同的 VR 特性组成 HA 簇。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。

在云上支持支持 HA 的 1 种工作模式：Active-Passive（A/P）模式：

> Active-Passive（A/P）模式：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。如果网络中存在多对 HA 设备，用户需要为它们配置不同的 HA 簇 ID，否则可能出现 MAC 地址冲突现象。

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。在 Peer A/A 模式中，目前的版本支持用户创建 2 个 HA 组，组 0 和组 1。

HA Node

为区分 HA 簇中的 HA 设备，用户可使用 HA Node（节点）值来标识设备。目前的版本仅支持 Node 值为 0 和 1。

在 HA Peer 模式下，系统可通过标识 HA Node 值来决定哪个设备处于主动状态，哪个处于禁用状态。在 HA 组 0 中，HA Node 值为 0 的设备处于主动状态， Node 值为 1 的设备处于禁用状态。在 HA 组 1 中，Node 值为 1 的设备处于主动状态， Node 值为 0 的设备处于禁用状态。

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。HA 簇中不同 HA 组之间不互相转发数据。VMAC 地址由 HA 虚拟基 MAC、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、隧道会话、Deny Session、ICMP 会话以及 tentative 会话）

IPsec VPN 信息

SCVPN 信息

DNS 缓存映射条目

ARP 表

PKI 信息

DHCP 信息

MAC 表

Web 认证信息

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 Active-Passive（A/P）模式

HA Active-Passive（A/P）模式的主要配置步骤包括：

1. 配置 HA 组的接口。
2. 指定 HA 工作模式为 Active-Passive（A/P）模式。

3. 配置 HA 连接，包括 HA 连接接口和 HA 链路 IP 的配置，用于传输 HA 控制协商报文以及数据同步。

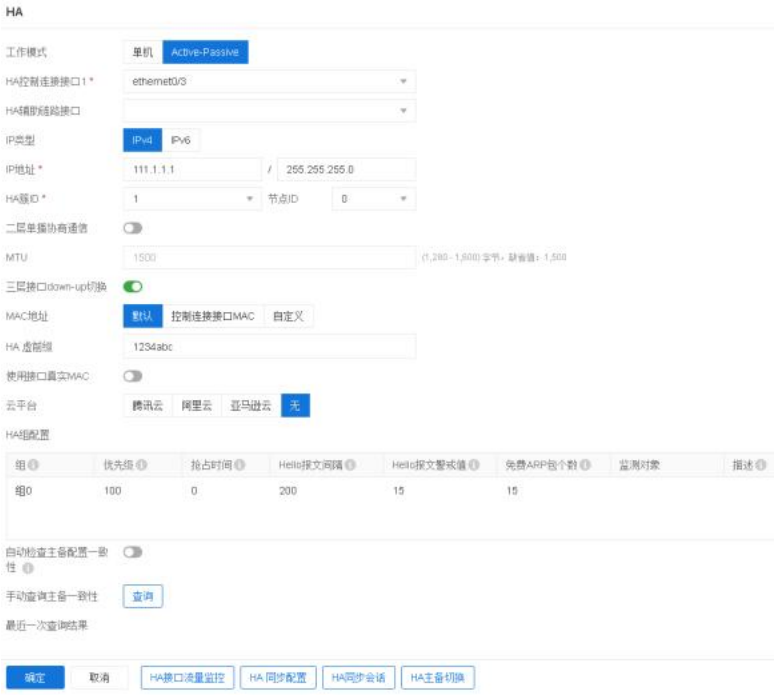
4. 配置 HA 簇。为设备指定 HA 虚前缀（可选）、HA 簇 ID 和节点 ID，并且开启设备的 HA 功能。

5. 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 Active-Passive（A/P）模式，请按照以下步骤进行操作：

1. 选择“系统 > HA”，进入 HA 配置页面。

2. 指定工作模式为“Active-Passive”，表示 HA 簇中的两台设备分别工作在主动模式和备份模式。



进行 HA Active-Passive（A/P）模式选项配置。

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。控制连接同步两台设备间的所有数据。
HA 辅助链路接口	指定 HA 辅助链路接口的名称。为了避免当 HA 连接发生故障时 HA 设备的主备状态出现异常，用户可以指定 HA 辅助链路接口，通过配置的 HA 辅助链路接收和发送心跳报文（Hello 报文），以确保 HA 设备维持正常的主备状态。 **说明：** 在 HA 连接恢复正常之前，HA 辅助链路只能接收和发送心跳报文，不能同步数据报文信息，因此建议用户不要修改当前设备配置信息，在 HA 连接恢复后，进行手动同步会话信息。

选项	说明
	HA 辅助链路接口必须使用除 HA 连接接口以外的接口，并且已绑定到安全域。 HA 主备设备需将相同的接口指定为 HA 辅助链路接口，并确保两端设备的该接口属于同一个 VLAN。
IP 类型	指定 HA 链路的 IP 地址类型，可选择 IPv4 或 IPv6。该配置项仅当当前版本为 IPv6 版本时显示并且可配。
IP 地址/IPv6 地址	指定 HA 链路的 IP 地址，系统通过该地址进行 HA 控制协商与数据同步。 当 IP 类型选择“IPv4”或者当前版本为 IPv4 版本时，指定 IPv4 类型的 IP 地址及网络掩码，输入格式为 A.B.C.D/M。M 可以为 1 到 32 之间的数字，也可以是点分十进制格式； 当 IP 类型选择“IPv6”时，指定 IPv6 类型的 IP 地址和前缀长度，输入格式为 X.X.X.X::X/M。“X.X.X.X::X”为 IPv6 地址前缀，“M”为前缀长度，取值范围为 1 到 128。
HA 簇 ID	选择 HA 簇 ID。配置 HA 簇 ID 并保存即表示启用 HA 功能，删除 HA 簇 ID 配置并保存将关闭 HA 功能。如果网络中存在多对 HA 设备，用户需要为它们配置不同的 HA 簇 ID，否则可能出现 MAC 地址冲突现象。当 HA 虚前缀设置为七位时，取值范围为 1~128；当 HA 虚前缀设置为八位或者不设置时，取值范围为 1~8。
节点 ID	指定节点 ID，两台设备需指定不同的节点 ID。范围是 0 到 1。 某些设备型号支持自动协商节点 ID，建议手动指定。
二层单播协商通信	启用该功能，设备采用二层单播的方式进行 HA 协商通信。开启该功能后，需配置 HA 对端 IP 地址，或者同时配置对端 IP 地址和 MAC 地址，HA 对端 IP 地址类型和 HA 链路的 IP 地址类型相同。该功能默认为关闭。
HA 对端 IP 地址/HA 对端 IPv6 地址	指定 HA 对端的 IP 地址，设备将通过该地址进行 HA 控制协商与数据同步： 当 HA 链路的 IP 类型选择“IPv4”或者当前版本为 IPv4 版本时，指定 IPv4 类型的 HA 对端 IP 地址； 当 HA 链路的 IP 类型选择“IPv6”时，指定 IPv6 类型的 HA 对端 IP 地址。
HA 对端 MAC 地址	输入对端 HA 设备的 MAC 址，即心跳口的 MAC 地址。
MTU	指定 HA 连接接口的最大传输单元的数值。当报文大小超过配置的 HA 接口 MTU 值时，发送端会将报文进行分片发送，接收端收到后会将报文进行重组，然后再进行后续处理。取值范围是 1280 到

选项	说明
	1600 字节，默认为 1500。
三层接口 down-up 切换	该功能默认开启。关闭该功能后，当设备进行 HA 切换由主设备切换为备份设备时，以下类型的物理接口不进行 down-up 操作。 已绑定三层安全域的物理接口。 属于冗余接口的物理接口，且该冗余接口已绑定三层安全域。 属于集聚接口的物理接口，且该集聚接口已绑定三层安全域。
MAC 地址	指定 HA 设备向 HA 组中的其它设备发送心跳（Hello 报文）时所使用的源 MAC 地址： 默认：使用默认的 MAC 地址发送心跳报文。 控制连接接口 MAC：指定使用控制连接接口的 MAC 地址作为 HA 心跳口的 MAC 地址。当用户配置多个控制连接接口时，系统将使用第一个控制连接接口的 MAC 作为 HA 心跳口的 MAC 地址。 自定义：指定使用自定义的 MAC 地址作为 HA 心跳口的 MAC 地址。选择该选项时，需要在下方“MAC”文本框中输入自定义 MAC 地址。
HA 虚前缀	指定 HA 虚拟基 MAC 的前缀，格式为十六进制，且只能配置为七位或者八位。当同一网段内需要配置 8 个以上的 HA 簇时， 为了防止系统生成的 HA 虚 MAC 地址重复，用户可以配置 HA 虚拟基 MAC 的前缀，即 HA 虚 MAC 前缀。默认情况下，HA 虚 MAC 的前缀为 0x001C54FF。 需要注意的是，全 0、全 F 或者组播地址（即第二个十六进制数为奇数的 MAC 地址）前缀是无效的。重启后配置才能生效。 **说明**：开启 HA 功能后，如需修改 HA 虚 MAC 前缀，请先关闭 HA 功能。
使用接口真实 MAC	启用该功能后，设备将使用接口的真实的 MAC（除 HA 连接接口和配置了 Local 属性的接口）。默认情况下，设备接口使用系统分配的虚拟 MAC 进行正常的数据流量转发。配置该功能后，设备将使用云平台分配给接口的真实 MAC 进行业务通信。
云平台	选择当前云防火墙所属的云平台：腾讯云、阿里云、亚马逊云，并根据部署方式配置相应的选项。非上述平台选择“无”即可。
部署方式	选择在云平台上部署 HA 的方式，系统支持两种 HA 部署方式：HAVIP 和访问密钥的方式。配置“访问密钥”方式时，需配置访问密钥 ID 和密码。

选项	说明
	访问密钥：指在云防火墙通过访问密钥（AccessKey）认证方式访问控制云平台，然后借助辅助 IP 等来部署云防火墙 HA 场景。 HAVIP：指在云平台上通过配置高可用虚拟 IP（HAVIP），来部署云防火墙 HA 场景。
访问密钥 ID	输入在云平台上已经申请的 AccessKey 或 APPID。
访问密钥密码	输入 AccessKey 或 APPID 对应的访问密码。
修改访问密钥密码	编辑 HA 配置时，可以看到修改密钥密码功能。开启后，将展示密码输入框。如需修改，输入新的密钥密码后保存配置即可。
连通测试	点击“连通测试”，可测试系统与云平台 API 是否连通。
校验访问 ID 和密码	点击“校验访问 ID 和密码”，可校验访问密钥 ID 及对应的密码是否填写正确。
HA 组配置	HA 组配置包含以下项目： 组：指定 HA 工作模式后，组 ID 会自动生成，且不可修改。在 HA A/P 模式下，设备仅具有组 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。取值范围是 1 到 254。 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。取值范围是 0 到 600。 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。取值范围是 50 到 10000 毫秒。 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。取值范围是 3 到 255。 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。取值范围是 10 到 180。 监测对象：指定已配置的监测对象的名称或点击 ⊕ 新建监测对象。系统利用监测对象监控设备的工作状态。一旦发现

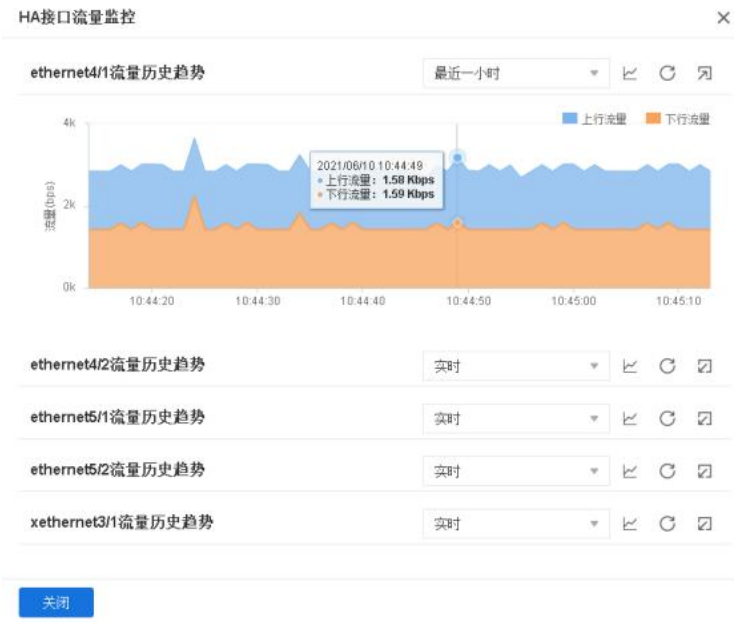
选项	说明
	设备不能正常工作，立即采取相应措施。 描述：指定该 HA 组的描述信息。
自动检查主备配置一致性	开启该功能后，系统会立刻查询一次主设备和备份设备的配置是否一致，之后每小时自动执行一次查询。每次执行后，会在“最近一次查询结果”项里刷新显示。如果配置不一致，会同时记录日志。如果需要查看具体存在哪些不一致的配置，可以通过手动查询再执行一次查询。该功能默认为关闭。**注意**：请在 HA 协商成功后，在主设备上开启“自动检查主备配置一致性”功能。开启“自动检查主备配置一致性”功能后，备份设备会同步该配置。
手动查询主备一致性	点击“查询”，系统会立刻查询一次主设备和备份设备的配置是否一致。执行后，“最近一次查询结果”会自动刷新。如果配置不一致，会弹出页面显示详情。**说明**：在支持 VSYS 功能且安装了 VSYS 许可证的设备上，可以点击弹出页面上 VSYS 对应的“Details”信息，查看主备配置不一致详情。其他情况下，会直接显示详情。**注意**：请在 HA 协商成功后，在主设备上进行“手动查询主备一致性”操作。
最近一次查询结果	显示配置一致性的查询结果、查询时间和查询类型。

3. 点击“确定”按钮，完成配置。

HA 接口流量监控

HA 接口流量监控功能能够统计指定时间周期内 HA 接口的历史流量趋势。

选择“系统 > HA”，在 HA 配置页面下方点击“HA 接口流量监控”按钮，打开 HA 接口流量监控页面，查看 HA 接口流量历史趋势统计信息。



在“实时”下拉菜单中选择“最近一小时”、“最近一天”、“最近一月”，系统将显示指定时间内的 HA 接口流量历史趋势统计信息。

点击右上角图标，将统计图在曲线图和面积图之间切换。

点击右上角按钮，实时刷新统计信息。

点击右上角图标，收起或者展开统计图。

鼠标悬停在流量统计图上，可查看 HA 接口的上行流量、下行流量或者总流量详情。

点击“上行流量“、”下行流量”或者“总流量”图例，可指定流量曲线图或者面积图的统计对象。

HA 配置同步

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。选择“系统 > HA”，在 HA 配置页面下方点击“HA 同步配置”按钮，完成主备间的配置信息同步。

HA 会话同步

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 sync rdo session disable”命令关闭 HA 会话自动同步功能，以确保设备的稳定性。

关闭 HA 会话自动同步后，用户可以选择“系统 > HA”，在 HA 配置页面下方点击“HA 同步会话”按钮，手动同步 HA 会话。

HA 主备切换

选择“系统 > HA”，在 HA 配置页面下方点击“HA 主备切换”按钮，手动切换 HA 设备的主备状态。

查看设备的 HA 部署状态

在 HA 环境下，可在系统主页面右上角“设备名称”处，的查看当前设备的 HA 部署状态。

主：表示当前设备为 HA 组的主设备。

备：表示当前设备为 HA 组的备份设备。

第 14 章 系统管理

设备的系统维护与管理主要包括但不限于以下各项：系统信息 、管理设备、管理配置文件、告警页面管理、设置 SNMP 、升级管理、许可证、配置邮件服务器、测试工具等

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 > 系统与特征库”，系统相关信息如下：

系统信息	
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。
实例 UUID	显示实例 的 UUID（通用唯一识别码）。
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。

系统信息	
	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。 Disabled：不可用状态，表示 HA 组下的接口均不工作。仅 Peer Active-Active 模式有该状态。
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的版本名称及其编译时间。
API 版本	获取 RESTful API 用户手册。
特征库信息	
立即检查	点击“立即检查”按钮，更新并显示特征库的最新版本号。 说明：显示特征库最新版本号需在已激活特征库许可证并已有特征库版本的情况下。
应用特征库	显示设备的应用特征库当前版本号、发布日期、最新版本号，以及升级特征库。
URL 分类库	显示设备的 URL 特征库当前版本号、发布日期、最新版本号，以及升级特征库。
沙箱白名单	显示设备的沙箱白名单当前版本号、发布日期、最新版本号，以及升级特征库。
IP 信誉特征库	显示设备的 IP 信誉特征库当前版本号、发布日期、最新版本号，以及升级特征库。
病毒过滤特征库	显示设备的病毒特征库当前版本号、发布日期、最新版本号，以及升级特征库。
入侵防御特征库	显示设备的入侵防御特征库当前版本号、发布日期、最新版本号，以及升级特征库。
僵尸网络防御特征库	显示设备的僵尸网络防御特征库当前版本号、发布日期、最新版本号，以及升级特征库。
ISP 信息库	显示设备的 ISP 特征库当前版本号、发布日期、最新版本号，以及升级特征库。

注意: 除 ISP 信息库外，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。

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 密钥和设置及操作。

API Token

开启短信或邮箱二次认证后，当管理员通过 RESTful API 登录设备时，只能使用 API Token 的认证方式。支持创建指定管理员的 API Token，对 API Token 进行更新、续期、清除以及启用等操作。

创建 API Token

创建 API Token，请按照以下步骤进行操作：

1. 选择“系统 > 设备管理 > API Token”，进入到 API Token 页面。
2. 选中指定的管理员，点击“创建”按钮，打开<创建 API Token>页面。

3. **配置如下信息。**

选项	说明
管理员	显示需要创建 API Token 的管理员名称。
有效期	指定 API Token 的有效期。包括：10 天、30 天、60 天、180 天、360 天、长期有效以及自定义有效期。 默认是 60 天。
自定义有效期	当“有效期”选择为“自定义”时，需要配置此参数。范围是 0-365 天。

4. 点击“确定”按钮保存所做的配置。新创建的 API Token 将会显示在 API Token 列表中。默认是“已启用”状态。

在 API Token 列表中，选中指定管理员的 API Token，用户还可以进行如下操作：

点击“更新”按钮， 可以更新 API Token 及有效期。更新之后， 生成新的 API Token。

点击“续期”按钮， 可以对启用状态和过期状态的 API Token 进行续期操作。续期之后， API Token 的值不发生改变。 例如：管理员“test”的 API Token 有效期为 10 天，当前时间为 2022 年 11 月 17 日，到期时间为 2022 年 11 月 25 日，点击“续期”，到期时间变更为 2022 年 11 月 27 日。

点击“清除”按钮， 可以删除指定管理员的 API Token。当删除指定管理员时，系统将自动删除管理员的 API Token。

点击“启用” 按钮，可以对状态为“未启用”的 API Token 进行启用。启用时重新计算有效期，例如，API Token 有效期原本设置为 30 天，重新启用后，有效期重新变为 30 天。

点击“禁用”按钮， 可以对状态为“已启用”的 API Token 进行禁用。

点击“操作”列的 按钮，可以复制指定管理员的“API Token”用于 RESTful API 登录。

可信主机

设备使用可信主机来进一步保证系统安全。管理员可以通过指定 IP 地址/IP 地址范围，或同时指定 IP 地址/IP 地址范围和 MAC 地址/MAC 范围来匹配可信主机，即在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。

注意:

如果远程主机不能访问设备，可能是可信主机配置问题，请进行相关检查。

系统最多允许配置 128 条可信主机。

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 > 可信主机”，进入到可信主机配置页面。
2. 点击“新建”按钮，打开<可信主机配置>页面。

配置如下信息。

选项	说明
当系统版本为 IPv4 版本时，配置以下选项：	
匹配地址类型	选择匹配可信主机的地址类型：“IPv4”或“IPv4&MAC"。 选择“IPv4”时，需指定 IP 地址/IP 地址范围，只有符合指定 IP 地址的主机或在指定 IP 范围内的主机可以为可信主机 选择“IPv4&MAC"时，需指定 IP 地址/IP 地址范围和 MAC 地址/MAC 范围，只有同时符合指定条件的主机可以为可信主机。

选项	说明
IP 类型	指定可信主机的 IP 地址/IP 地址范围： IP 地址和掩码：在文本框中分别输入可信主机的 IP 地址和子网掩码。 IP 地址范围：在文本框中分别输入可信主机的起始 IP 地址和终止 IP 地址。
MAC 类型	指定可信主机的 MAC 地址/MAC 范围： MAC 地址：在文本框中分别输入可信主机的 MAC 地址。 MAC 范围：在文本框中分别输入可信主机的起始 MAC 地址和终止 MAC 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、 HTTPS、NETCONF 的方式登录。
当系统版本为 IPv6 版本时，配置以下选项：	
类型	选择匹配可信主机的地址类型：“IPv4”或“IPv6"。
主机类型	用户可以配置 IPv4 类型的可信主机或 IPv6 类型的可信主机。 当类型选择“IPv4”时，指定 IPv4 类型可信主机的 IP 地址/IP 地址范围： IP 地址和掩码：在文本框中分别输入可信主机的 IPv4 地址和子网掩码。 IP 地址范围：在文本框中分别输入可信主机的起始 IPv4 地址和终止 IPv4 地址。 当类型选择“IPv6”时，指定 IPv6 类型可信主机的 IP 地址/IP 地址范围： IPv6/前缀长度：在文本框中分别输入可信主机的 IPv6 地址和子网前缀长度。 IPv6 范围：在文本框中分别输入可信主机的起始 IPv6 地址和终止 IPv6 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、 HTTPS、NETCONF 的方式登录。

3. 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、HTTPS 的 PKI 信任域以及证书认证信任域。 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 > 管理接口”。
2. **配置如下信息。**

选项	说明
Console	配置使用 Console 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。 单点登录：选中该复选框，开启允许第三方单点登录云防火墙的功能。该功能默认为关闭状态，用户可按需开启。开启该功能并配置第三方平台对应的单点登录方案后，用户可在登录第三方平台后，直接访问云防火墙而无需输入用户名和密码。系统支持三种单点登录方案： CAS_QIMING： 指定单点登录方案为启明 CAS 服务器单点登录。指定后，用户可在启明星辰云安全资源池平台单点登录到云防火墙。

选项	说明
	Service Ticket 校验地址： 指定 CAS 服务器校验 Service Ticket 的 URL 地址。 虚拟路由器：指定 CAS 服务器所在的虚拟路由器。 CTYUN：指定单点登录方案为天翼云单点登录。指定后，用户可在天翼云平台单点登录到云防火墙。 360_YUNZHEN：指定单点登陆方案为 360 云阵单点登录。指定后，用户可在 360 云阵云安全管理平台单点登录到云防火墙。 允许相同账号同时登录：选中该复选框，开启允许相同账号同时登录功能。开启该功能后，当使用 Web 方式登录设备时，用户可以使用同一账号在多处同时登录设备。默认情况下，该功能为关闭状态，即当使用同一账号再次登录时，已登录的用户将会被踢出。 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。 HTTPS 信任域：从下拉菜单中选择 HTTPS 登录的 PKI 信任域。当使用 HTTPS 方式登录设备时，系统会使用指定 PKI 信任域中的证书。 证书认证：选中该复选框，开启证书认证登录功能。其中证书包括两种：客户端数字证书和由根 CA 签名的二级 CA 证书。证书认证属于双因素认证的一种。双因素认证是指除了对用户名和密码进行认证外，还需要进行其他方式的认证，例如证书和指纹等等。 证书绑定信任域：开启证书认证登录功能后，当使用 HTTPS 方式登录设备时，系统会使用此 PKI 信任域中的证书进行认证。此信任域必须导入 CA 根证书。 CN 检查：开启 CN 检查后，用户登录时会对 CA 根证书的主题名称进行检查校验，只有证书与用户对应一致才能登录成功。

3. 点击“确定”。

注意: 当改变 HTTP 端口、HTTPS 端口、HTTPS 信任域时，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，包括配置系统时间和通过 NTP 服务器同步系统时间。

设置系统时间

配置系统时间，请按照以下步骤进行操作：

1. 选择“系统 > 设备管理 > 系统时间”。
2. **在“系统时间配置”处进行设置。**

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。
-	配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”按钮保存所做配置。

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 > 系统时间”。
2. **在“启用 NTP”部分进行配置。**

选项	说明
启用	点击“启用”按钮，开启 NTP 功能。默认情况下，系统的 NTP 功能是关闭的。

选项	说明
认证	点击“启用”复选框，开启 NTP 身份验证。
NTP 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。 虚拟路由器：指定进行 NTP 通信的接口所属的 VR。 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 > NTP 密钥”, 进入到 NTP 密钥配置页面。
2. **点击“新建”按钮，打开<NTP 密钥配置>页面。**

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。
修改密钥	编辑 NTP 密钥配置时，可以看到修改密钥功能。开启后，将展示密钥输入框。如需修改，输入新的密钥后保存配置即可。

3. 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、重启设备和导出系统调试信息。

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 > 设置及操作”。
2. **进入到系统设置页面。**

系统设置	
主机名称	在文本框中输入设备的主机名称。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。
域名	在文本框中输入设备的域名。
页签标题模式	设置通过 WebUI 登录设备时的浏览器页签标题，可以设置为主机名称、设备型号和管理地址。支持选择多项，不限制顺序。实际的页签标题在显示时，各项的排列顺序与配置的顺序一致。配置保存后即生效。默认标题为“Networks”。
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。
授权模式	选择授权模式，包括两种： 本地授权：配置“本地授权”后，需要在设备上配置管理员及认证信息。 服务器授权：配置“服务器授权”后，不需要在设备上配置管理员及认证信息。
认证服务器	当“授权模式”选择为“服务器授权”，需要选择已有的认证服务器，或者点击 ⊕ 新建认证服务器。配置认证服务器，请参考配置 AAA 服务器。支持选择以下两种服务器： Radious 服务器 TACACS+服务器
本地密码重试	启用本功能后，服务器返回密码错误时，会尝试本地密码校验。当服务器不可达时，Stone OS 默认会开启本地密码重试，无需开启此配置。默认是开启状态。
最大登录尝试数	在文本框中输入最大尝试次数，取值范围为 1 至 5，默认值为 3。登录设备时，密码被输入错误的次数超过最大登录尝试次数时，系统将会锁定，在锁定时间内禁止使用该用户账号登录设备。
锁定时间	在文本框中输入被锁定账号禁止登录设备的时长。取值范围为 1 至 65535 分钟，默认值为 2 分钟。
密码最小长度	在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”单选按钮不对密码复杂度进行检测，或者选择“设置密码复杂度“，来自定义密码复杂度： 大写字母最小长度：取值范围为 0 到 16，默认值为 2。 小写字母最小长度： 取值范围为 0 到 16，默认值为 2。

系统设置	
	数字最小长度： 取值范围为 0 到 16，默认值为 2。 特殊字符长度： 取值范围为 0 到 16，默认值为 2。 密码有效期：单位为天， 取值范围为 0 到 365，默认值为 0，表示不对有效期进行限制。
历史密码检查	为保证密码的安全性，系统支持历史密码检查功能。开启历史密码检查功能后，用户在修改密码时，系统将对新密码与历史密码进行重复校验，即新密码不能与最近使用的历史密码重复。若用户的新密码与历史密码重复，系统将会提示“新密码不能与历史密码重复”，提醒用户重新输入新密码。 点击“历史密码检查”后的“启用”按钮，启用历史密码检查功能，并指定历史密码的个数。范围是 3 到 8 个，默认值是 5，即新密码不能与最近使用的 5 个历史密码重复。

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 > 设置及操作"。
2. 在“系统操作”标签页，点击“重启设备”。
3. 系统将重新启动。

系统调试

设备具有调试功能，供用户查阅与分析。

故障反馈

开启故障反馈功能，请按照以下步骤进行操作：

1. 选择“系统 >设备管理>设备及操作”。
2. 在“系统设置”标签页，点击“故障反馈”后的“启用”按钮。系统将自动发送技术支持文件到厂商。

系统调试信息

系统调试功能可以帮助用户根据导出的设备故障文件对错误进行诊断和定位。

导出系统调试信息，请按照以下步骤进行操作：

1. 选择“系统 >设备管理>设备及操作”。
2. 在“系统操作”标签页，点击系统调试信息后的“导出”按钮，系统会将/etc/local/core 目录下的文件打包，并提示保存“tech-support”文件，选择保存位置并点击“确认”后，即可成功导出。

应用层安全 Bypass

系统支持对应用层的功能一键 Bypass，包括入侵防御、病毒过滤、URL 过滤、数据安全、沙箱防护、僵尸网络、IP 信誉过滤。

开启应用层安全 Bypass 功能，请按照以下步骤进行操作：

1. 选择“系统 > 设备管理 > 设置及操作”，进入设置及操作页面。
2. 在系统设置标签页，点击“应用层安全 Bypass”后的“启用”按钮，点击“确定”按钮。

安全认证管理

启用安全认证管理功能，通过短信或邮箱二次认证的方式登录设备。

开启安全认证管理功能，请按照以下步骤进行操作：

1. 选择“系统 > 设备管理 > 安全认证管理”。
2. **进入到安全认证管理页面。**

选项	说明
禁用	选择“禁用”，关闭安全认证功能。默认是关闭状态。
短信	选择“短信”，开启短信认证功能。开启短信认证后，未配置手机号码的管理员将无法登录设备。 短信认证：指定短信认证的方式，包括短信猫和短信网关。当选择短信网关时，在“短信网关”下拉菜单选择指定的短信网关。配置短信发送参数，请参考 短信发送参数。 验证码有效时间：指定短信认证码的有效时间，取值范围是 1 到 30 分钟。默认是 5 分钟。如果用户在有效时间内没有输入短信认证码，将无法登录设备。 发送者名称：指定短信发送者名称以显示在短信内容中。取值范围是 1 到 64 字符。
邮箱	选择“邮箱”，开启邮箱认证功能。开启邮箱认证后，未配

选项	说明
	置邮箱地址的管理员将无法登录设备。 邮箱服务器：在下拉菜单中选择邮箱服务器。配置邮箱服务器，请参考 配置邮件服务器内容。 验证码有效时间：指定邮箱认证码的有效时间，取值范围是 1 到 30 分钟。默认是 5 分钟。如果用户在有效时间内没有输入邮箱认证码，将无法登录设备。 发送者名称：指定邮件发送者名称以显示在邮件中。取值范围是 1 到 64 字符。

3. 点击“确定”按钮保存所做配置。

注意: 短信/邮箱认证和“系统 > 设备管理 > 管理接口”页面的单点登录功能无法同时开启。

存储管理

存储管理功能通过限制各个功能占用磁盘空间的大小来管理系统存储空间。配置存储管理功能，请按照以下步骤进行操作：

1. 选择“系统 > 设备管理 > 存储管理”。

2. 配置如下选项：

选项	说明
阈值	当系统存储比例或存储空间达到指定的阈值时，系统将执行指定的动作，从而控制系统存储。存储比例取值范围为0.01%~90%。
阈值告警	当系统存储比例或存储空间达到指定的阈值时，系统会向用户发送日志进行提示。
日志超过存储阈值	该选项仅对日志存储空间有效。当日志达到指定的存储阈值时，系统将执行指定的动作，包括覆盖最早的数据和停止记录。 覆盖最早的数据：系统将删除较早的日志。 停止记录：系统将停止存储新的日志。
自定义存储空间	
查看当前存储状况	显示存储空间总量、已分配空间及占比。点击“查看当前存储状况”按钮，在“当前存储状况”页面查看各类日志及报表文件的最大存储空间及已占用存储百分比。
报表空间设置	指定报表文件的磁盘空间大小。系统为报表文件分配了默认的磁盘空间大小，用户可以根据需要为报表文件自定义配置磁盘空间大小。当存储空间达到指定的阈值时，系统将删除较早的统计数据。（仅安装有硬盘的设备支持该选项）
日志空间设置	点击“启用”按钮，指定每个模块日志的磁盘空间大小。系统为每个模块的日志分配了默认的磁盘空间大小，用户可以根据需要为日志自定义配置磁盘空间大小。（仅安装有硬盘的设备支持该选项）

3. 点击“确定”按钮，保存所做配置。

密码重置管理

通过密保问题重置管理员密码功能可以让用户修改密码时无需知道旧密码，从而更加便捷地重置密码。若配置并启用了该功能，当管理员用户通过 console 口登录时，在输入正确的用户名，且连续三次输入错误密码的情况下，系统会提示用户可以通过密保修改密码。配置密码重置功能，请按照以下步骤进行操作：

1. 选择“系统 > 设备管理 > 密码重置管理”。

2. **点击“启用”按钮，开启密码重置功能，并配置如下选项：**

选项	说明
密码重置	点击“启用”按钮，开启密码重置功能。
密保问题类型	指定密保问题的类型为自定义或预定义。
密保问题	配置密保问题。当密保问题类型为自定义时，在文本框中输入自定义的密保问题。当密保问题类型为预定义时，在下拉框中选择系统预定义的密保问题。取值范围为 1-256 字符，只支持英文字母、数字、英文特殊字符（"除外），不支持中文字符。
密保答案	配置密保问题的答案。取值范围为 1-256 字符，只支持英文字母、数字、英文特殊字符（"除外），不支持中文字符。
确认密保答案	在文本框中再次输入密保问题的答案，须和密保答案文本框中的内容保持一致。

3. 点击“确认”，完成配置。

开局安装向导

在通过 WebUI 首次登录防火墙，并完成修改密码后，系统会弹出防火墙安装向导欢迎页面。用户可以按照安装向导指引的步骤，完成防火墙设备的初始配置，包括主机名称、时间时区、许可证等基本配置、路由模式的部署以及安全策略相关配置，也可以跳过安装向导自行配置。

注意:

在以下任一情况下，管理员登录 WebUI 时，不会弹出安装向导欢迎页面：

防火墙部署在 HA 模式；

登录的地址非 WebUI 首页，例如“http://x.x.x.x/#icenter”；

在 HSM 设备上登录防火墙的 WebUI；

通过云平台单点登录防火墙的 WebUI。

跳过安装向导

跳过安装向导，按照以下步骤操作：

1. 在防火墙开局向导的任何页面，点击“跳过”。
2. 在弹出的“您是否确定跳过配置向导？”询问页面，用户可以选择“下次登录不再显示”。如不选择，再次登录时，系统仍会弹出安装向导页面。
3. 点击“确定”，关闭安装向导页面。

开启安装向导

跳过安装向导后，用户可以再次开启安装向导：

1. 点击“系统 > 设备管理 > 安装向导”。
2. 在<安装向导>页面，根据需要选择是否恢复出厂配置：
   a. 点击开启“恢复出厂配置”，系统会在开启安装向导后清空设备的所有配置。
   b. 如不开启“恢复出厂配置”，安装向导中创建的策略将具有高优先级，其他新增配置将在已有配置的基础上进行修改。“恢复出厂配置”功能默认为关闭。
3. 点击“开启”按钮，打开安装向导页面。
4. 点击“开始向导”按钮开启安装向导，进入<系统时间配置>页面。

配置主机名称和系统时间

选项	说明
主机名称	输入主机名称，取值范围是 1 到 63 个字符。默认是 SG-6000。 点击“下一步”下发配置。
系统时间	设置系统时间，支持两种方式： 点击“同步时间”按钮，在弹出的页面将会显示当前时区，点击“确定”按钮下发配置。 点击“编辑时间”按钮，在弹出的页面手动设置时区、日期和时间后，点击“确定”按钮下发配置。

5. 点击“下一步”，进入<导入许可信息>页面。

导入许可证

选项	说明
导入类型	导入后，页面下方将展示导入的许可证列表。注意：部分许可证导入后，需重启系统才能生效，请在完成全部向导配置后重启系统。

选项	说明
	系统支持两种方式导入许可证： 上传许可证文件：点击“浏览”按钮，选择需要导入的许可证文件后，点击“导入”按钮。 手动输入：在“许可证”文本框中输入许可证内容后，点击“导入”按钮。

6. 点击“下一步”，进入<网络配置>页面。网络配置会在安装向导完成后下发。在网络配置部分，除了向导中用户可以手动添加的配置外，系统还会自动配置一条启用 Sticky 功能的源 NAT 规则，用于将内网 IP 转换为出接口 IP。

选择内网口和外网口

选项	说明
外网口（untrust）	选择外网接口。选择的外网接口将被加入 untrust 安全域。
内网口（trust）	选择内网接口。选择的内网接口将被加入 trust 安全域。

7. 点击“下一步”，对外网接口进行配置。

配置外网接口

选项	说明
IP 获取方式	选择外网接口的 IP 获取方式。
静态 IP	选择静态 IP 方式时需指定接口的 IP 地址和子网掩码。
自动获取	选择自动获取方式时，接口将通过 DHCP 方式自动获取 IP 地址。
PPPoE	选择 PPPoE 方式需设置： 用户：指定 PPPoE 用户名称，取值范围是 1 到 31 个字符。 密码：指定 PPPoE 用户的密码，取值范围是 1 到 31 个字符。

选项	说明
	确认密码：再次输入密码进行确认。 挂断前空闲间隔：指定空闲间隔时间，单位为分钟，取值范围是 0 到 10000 分钟。当 PPPoE 接口的空闲时间达到指定的空闲间隔时间时，系统会断开网络连接。默认值是 0，表示不会断开网络连接。 重拨间隔：指定系统在断开连接后自动重拨前的时间间隔，单位为秒，取值范围是 1 到 10000 秒。默认值是 10。
管理方式	选择接口管理方式，包括 Telnet、SSH、Ping、HTTP、HTTPS、SNMP、NETCONF 和 TRACEROUTE。
默认网关	指定默认网关地址。
DNS 服务器	指定 DNS 服务器地址。

8. 点击“下一步”，对内网接口进行配置。

配置内网接口

选项	说明
IP 地址/子网掩码	指定接口的 IP 地址和子网掩码。
管理方式	选择接口管理方式，包括 Telnet、SSH、Ping、HTTP、HTTPS、SNMP、NETCONF 和 TRACEROUTE。
开启 DHCP 服务	开启 DHCP 服务后，接口将被设置成 DHCP 服务器。
DHCP lease range	指定地址池 IP 范围。将接口设置成 DHCP 服务器后，系统将通过配置的地址池，为与该接口相连的主机分配 IP 地址。

9. 点击“下一步”，进入<安全策略>页面。安全策略配置会在安装向导完成后下发。

配置安全策略

选项	说明
允许内网访问互联网	选择该复选框将配置一条从源安全域（trust）到目的安全域（untrust）的安全策略，允许内网用户访问外网。若不勾选，则不创建策略。
威胁防护	选择了“允许内网访问互联网”后，根据需要开启威胁防护功能。只有安装了有效的许可证后，才能开启相应的威胁防护功能。开启的威胁防护功能使用默认的防护规则，用户在完成安装向导后可以到相应的功能模块做进一步的配置。注意：部分威胁防护功能在安装许可证后，需重启设备才能生效。

10. 点击“下一步”，进入<配置信息>页面，可以看到之前通过配置向导添加的所有配置信息。

11. 确认配置信息正确后，点击“确定”，下发网络配置及安全策略配置。

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。系统记录最近十次保存的配置信息，最近一次保存的配置信息会记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。

> 注意: 如果已回退到已保存的指定的起始配置信息，那么该配置信息将会以“startup”作为标记。

导出/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 > 配置文件列表”，进入配置文件列表页面。

2. 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。可以选择导出 DAT 或 ZIP 类型的配置文件。选择 ZIP 类型时，可以根据需要设置压缩密码。

   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。

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。支持导入 DAT 和 ZIP 类型的配置文件。如果 ZIP 文件是加密的，需输入压缩密码。 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。

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。

查看当前系统配置

查看系统当前的配置文件，请按照以下步骤进行操作：

1. 选择“系统 > 配置文件管理 > 当前系统配置”，可以查看系统当前的配置文件。
2. 如果需要导出当前配置文件，点击页面下方的“导出”按钮。

导入/导出 VSYS 配置文件

用户可以导出当前所有 VSYS 的配置文件，也可以导入已保存的 VSYS 配置文件。

导出当前所有 VSYS 的配置文件，请按照以下步骤进行操作：

1. 选择“系统 > 配置文件管理 > 配置文件列表”，进入配置文件列表页面。
2. 点击“导出所有 VSYS 配置”，导出当前所有 VSYS 的配置文件至本地。

导入已保存的 VSYS 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 > 配置文件列表”，进入配置文件列表页面。
2. 点击“导入所有 VSYS 配置”，打开<导入配置文件>页面。
3. 点击“浏览”，选择需要导入的 VSYS 配置文件。支持导入的文件类型为 GZ 和 ZIP。
4. 导入配置文件后，需重启设备才能生效。勾选“立即重启，使新配置生效”复选框，可立即重启设备。
5. 点击“确定”按钮。

告警页面管理

告警页面管理包括自定义告警页面的图片管理以及页面管理。

图片管理

用户根据需求，可以上传所需要的图片，并且可以在自定义告警页面中引用已上传的自定义图片。在图片管理页面中，将会以列表方式展示所有上传的自定义图片名称、图像预览以及最近一次修改时间。

上传图片

上传自定义图片，请通过以下步骤进行操作：

1. 选择“系统>告警页面管理>图片管理”。
2. 点击“新建”按钮，打开<上传图片>配置页面。

3. 在“名称”文本框中输入自定义图片的名称。
4. 点击“上传图片”按钮，选择本地需要上传的图片文件。
5. 上传完成后，图片将预览显示在该对话框中。
6. 点击“确定”按钮，保存配置。

注意: 仅支持上传的图片类型：jpeg、jpg、png、gif、jfif；上传图片大小限制为 24KB；系统最多允许上传 32 个图片文件。

编辑图片

替换修改已上传的图片，请按照以下步骤进行操作：

1. 选择“系统>告警页面管理>图片管理”。
2. 在列表中勾选需要编辑的图片复选框，点击“编辑”按钮。
3. 在<上传图片>页面中，点击“上传图片”按钮，上传图片文件。
4. 点击“确定”按钮，保存配置。

删除图片

删除已上传的图片，请按照以下步骤进行操作：

1. 选择“系统>告警页面管理>图片管理”。
2. 在列表中勾选需要删除的图片复选框，点击“删除”按钮。
3. 在确认删除对话框中，点击“是”按钮，完成删除。

注意: 删除图片之前，请先确保图片未被自定义告警页面引用，否则无法被删除。

页面管理

系统支持 6 种自定义告警页面，并且页面中已包含默认显示的引用串和警告信息内容。用户可以根据实际需求自定义告警页面，通过使用 html 编码方式添加或修改引用串，来自定义告警页面的警告信息文字、图片等内容。

URL 过滤监控用户通知：通知 URL 过滤功能将扫描用户流量。

URL 过滤阻断用户通知：通知用户流量被 URL 过滤阻断。

病毒过滤发现恶意软件：病毒过滤扫描网络流量，发现恶意软件后显示告警页面。

病毒过滤发现恶意站点：病毒过滤扫描网络流量，发现恶意软件后显示告警页面。

内容过滤监控用户通知：通知内容过滤功能将扫描用户流量。

内容过滤阻断用户通知：通知用户流量被内容过滤阻断。

配置自定义告警页面，请按照以下步骤进行操作：

1. 选择“系统>告警页面管理>页面管理”，打开页面管理页。

在“页面管理”页，查看自定义告警页面详细信息。

页面上方列表展示系统支持的 6 种自定义告警页面名称、描述、最近一次修改时间、以及自定义页面启用状态。

页面下方左侧部分，展示所选自定义告警页面的页面预览。

页面下方右侧部分，展示自定义告警页面的默认 html 编码，用户可以在该部分使用 html 编码方式自定义页面内容。

2. 在上方列表中，勾选需要自定义的告警页面复选框。

3. 在下方 html 编码页面中，修改警告信息内容，或者输入“%%”选择需要添加的引用串，引用对应的内容或图片。

自定义告警页面可包含如下引用串。

引用串	含义
%%AUDIT_BUTTON%%	用于在页面显示按钮，用户点击该按钮可以开始上网。 **注意：**在“URL 过滤监控用户通知”和“内容过滤监控用户通知”页面中该引用串为必配项，请勿删除或者修改该关键字。
%%IGNORE_WARNING%%	用于在页面显示按钮，用户点击该按钮可以忽略提示并继续浏览。

引用串	含义
	注意：该引用串为页面默认显示的引用串，修改后可能导致忽略提示和按钮无法正常显示。
%%IMAGE_NAME%%	图片前缀，用于引用“图片管理”中已上传的图片，在告警页面输出图片。
%%URLFILTER_REASON%%	用于在“URL 过滤阻断用户通知”页面中显示 URL 过滤阻断的原因。 **注意**：该引用串为此页面默认显示的引用串，修改后可能导致阻断原因无法正常显示。
%%VIRUS_NAME%%	用于在“病毒过滤发现恶意软件”页面中显示扫描到的病毒名称。 **注意**：该引用串为此页面默认显示的引用串，修改后可能导致病毒名称无法正常显示。
%%CONTENTFILTER_REASON%%	用于在“内容过滤阻断用户通知”页面中显示内容过滤阻断的原因。 **注意**：该引用串为此页面默认显示的引用串，修改后可能导致阻断原因无法正常显示。

4. html 编码修改完成后，点击“保存”按钮，保存自定义告警页面配置。同时，该自定义告警页面将会被启用，并且在上方列表“自定义”栏中显示 。

5. 如果需要恢复自定义告警页面默认内容，点击“恢复默认”按钮。

设置 SNMP

系统的 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系统的相应信息。

系统支持 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系统信息。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。

系统支持 RFC-1213 中定义的管理信息库组相关 MIB（Management Information Base for Network Management of TCP/IP-based Internets: MIB-II）、RFC-2233 中定义的使用 SMIv2 的接口组 MIB（The Interfaces Group MIB using SMIv2：IF-MIB）、RFC-2574 中定义的 SNMPv3 安全模块相关 MIB（User-based Security Model：USM）以及 RFC-2575 中定义的 SNMPv3 用户访问控制模块相关 MIB（View-based Access Control Model：VACM）。此外，系统提供一个私有 MIB 库，MIB 库中包含系统的系统信息、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

系统拥有一个 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系统的运行情况。

配置 SNMP 代理，请按照以下步骤进行操作：

1. 选择“系统 > SNMP > SNMP 代理”。
2. **点击“启用”按钮，进行 SNMP 代理的配置。**

选项	说明
SNMP 代理	点击“启用”按钮，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	在文本框中输入系统 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，内容为网关相关人员的标识及联系方法。用户可以通过配置此参数，将重要信息存储在网关中，以便出现紧急问题时查询使用。
系统位置	在文本框中输入系统的位置。
主机端口	在文本框中输入 SNMP 代理系统的端口号。
虚拟路由器	从下拉菜单中选择所需的虚拟路由器名称。
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 > SNMP 主机”，进行 SNMP 主机的配置。
2. **点击“新建”按钮，打开<SNMP 主机配置>页面。**

选项	说明
类型	选择 SNMP 主机的类型。选择“IP 地址”、“IP 地址范围”或“IP/掩码”。 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	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。
修改团体字	编辑 SNMP 主机配置时，可以看到修改团体字功能。开启后，将展示团体字输入框。如需修改，输入新的团体字后保存配置即可。
权限	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。

3. 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 >Trap 主机”，进行 Trap 主机的配置。
2. **点击“新建”按钮，打开<Trap 主机配置>页面。**

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	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。

3. 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。
4. 编辑 Trap 主机配置时，可以看到修改团体字功能。开启后，将展示团体字输入框。如需修改，输入新的团体字后保存配置即可。

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 > V3 用户组”，进行 V3 用户组的配置。
2. **点击“新建”按钮，打开<V3 组配置>页面。**

选项	说明

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	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。 V3 用户组的安全级别包括不认证（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	选择该用户组的可读 MIB 视图名，包括： 全部：能够对所有 MIB 进行读操作； MIB2：能够对 RFC-1213 以及 RFC-2233 中定义的公有 MIB（MIB-II）进行读操作； Private MIB：能够对设备的私有 MIB 库进行读操作； VACM MIB：能够对 RFC-2575 中定义的 SNMPv3 用户访问控制模块相关 MIB（VACM）进行读操作； USM MIB：能够对 RFC-2574 中定义的 SNMPv3 安全模块相关 MIB（USM）进行读操作。
写视图	选择该用户组的可写 MIB 视图名，包括： 全部：能够对所有 MIB（USM）进行写操作； USM MIB:能够对 RFC-2574 中定义的 SNMPv3 安全模块相关 MIB（USM）进行写操作。

3. 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 > V3 用户”，进行 V3 用户的配置。
2. **点击“新建”按钮，打开<V3 用户配置>页面。**

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	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。
确认密码	在文本框中再次输入认证密码进行确认。
修改密码	编辑 V3 用户配置时，可以看到修改密码功能。开启后，将展示密码输入框。如需修改，输入新的密码后保存配置即可。
加密算法	指定用户加密协议。
加密密码	在文本框中指定加密密码。
确认密码	在文本框中再次输入加密密码进行确认。

3. 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。

SNMP 服务器

用户可以配置 SNMP 服务器，从而通过 SNMP 协议来获取相关的 ARP 信息。

新建 SNMP 服务器

新建 SNMP 服务器，请按照以下步骤进行操作：

1. 选择“系统 > SNMP>SNMP 服务器”。

2. 点击“新建”按钮，打开<SNMP 服务器配置>页面。

在<SNMP 服务器配置>页面中配置相关信息

选项	说明
服务器 IP	在文本框中输入 SNMP 服务器的 IP 地址。
端口	在文本框中输入 SNMP 服务器的端口号。范围为 1 到 65535。默认值为 161。
团体字	在文本框中输入 SNMPv1 或者 SNMPv2C 的团体字。
修改团体字	编辑 SNMP 服务器配置时，可以看到修改团体字功能。开启后，将展示团体字输入框。如需修改，输入新的团体字后保存配置即可。
虚拟路由器	从下拉菜单中选择所需的虚拟路由器名称。
源接口	从下拉菜单中选择 SNMP 服务器上用来接收 ARP 信息的源接口名称。
间隔时间	在文本框中输入 SNMP 服务器上接收 ARP 信息的时间间隔，单位为秒，范围是 5 到 1800 秒，默认值是 60 秒

3. 点击“确定”按钮保存所做的配置。新创建的 SNMP 服务器将会显示在 SNMP 服务器列表中。

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，可以指定共享接入特征库、应用特征库、URL 特征库、入侵防御特征库、沙箱白名单、IP 信誉特征库、风险减缓规则特征库、异常行为模型库、恶意软件行为模型库、僵尸网络防御特征库、ISP 信息库的升级配置，也可以对数据库中的日志、监控和报表等旧版本数据进行格式升级或删除，还可以配置可信根证书库的升级信息。

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 > 版本升级”。

2. 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。
备份版本	显示设备中的备份软件版本。
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。
选择下次启动版本	
当前版本	显示当前软件的版本号。
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。

升级数据库数据

当用户对系统版本进行升级后，系统的新旧版本数据同时存在于数据库中，例如日志、报表文件、监控数据等，由于新旧版本数据格式不一致，导致系统页面可能无法正常显示旧版本数据信息。为保证系统功能的正常显示与使用，用户需及时将数据库中的旧版本数据升级至符合当前版本的数据格式，若用户不需要旧版本数据也可以选择将旧版本数据删除。

> 注意： 系统仅支持手动升级数据库数据。

当系统存在旧版本数据时，用户登录设备后，系统将弹出<数据库数据升级提醒>对话框，提醒用户进行数据升级，升级完成前将无法查看旧版本数据。

勾选“不再提醒”复选框，关闭升级提醒弹窗提示。后续若想重新查看升级提醒弹窗提示，可将鼠标指针移动到系统右上角的通知图标上，在下拉框中点击“数据库数据升级提醒”，系统将弹出<数据库数据升级提醒>对话框。

点击“前往查看”按钮，跳转至数据库数据升级页面，可在此页面进行数据库数据的升级和删除操作。

升级数据库数据，请按照以下步骤进行操作：

1. 选择“系统 > 升级管理 > 数据库数据升级”。
2. 进入到数据库数据升级页面。

选项	说明
数据库操作	对于系统数据库中存在的旧版本数据，可选择升级或删除。 升级旧版本数据：点击“升级旧版本数据”按钮，可以将与系统当前版本数据格式不一致的旧版本数据升级至当前符合系统版本的数据格式。 删除旧版本数据：点击“删除旧版本数据”按钮，可以将与系统当前版本数据格式不一致的旧版本数据删除，此操作不会影响数据库中其他符合当前版本数据格式的数据。 说明：若系统版本降级后，当数据状态处于“待升级”时，可以通过点击“升级旧版本数据”按钮，将数据库的数据降级至符合当前版本的数据格式。
数据库数据升级状态	展示系统数据库中数据的升级状态。 待升级：当系统中存在与当前版本数据格式不一致的旧版

选项	说明
	本数据时，状态显示为“待升级”。 升级中：当系统中存在与当前版本数据格式不一致的旧版本数据时，用户通过点击“升级旧版本数据”按钮，将旧版本数据升级成符合当前版本的数据格式，此时状态显示为“升级中”，同时显示升级进度和已耗时间。 已是最新，无需升级：当升级旧版本数据或删除旧版本数据后，数据库中的数据均符合当前版本的数据格式，此时状态显示为“已是最新，无需升级”。

升级特征库

用户可以直接在设备上查看到 ISP 信息库，其他特征库只能通过安装许可证才能查看。系统可以安装的特征库包括加密流量检测库、共享接入特征库、应用特征库、URL 特征库、沙箱白名单、入侵防御特征库、IP 信誉特征库、风险减缓规则特征库、异常行为模型库、恶意软件行为模型库、僵尸网络防御特征库、ISP 信息库。系统支持两种特征库升级方式：一是通过 HTTP 和 HTTPS 协议的方式实现远程升级；二是通过默认特征库更新服务器下载升级包进行本地升级。

系统支持通过 IPv6 协议下载各特征库。

各个特征库的升级操作相同，请按照以下步骤进行操作：

1. 选择“系统 > 升级管理 > 特征库升级”。
2. **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。
最新版本	显示最新特征库的版本号。 **说明：**ISP 信息库显示最新版本号需要在已有特征库版本的情况下，其他特征库显示特征库最新版本号需在已激活特征库许可证并已有特征库版本的情况下。
远程升级	系统支持通过 HTTP 和 HTTPS 协议的方式实现远程升级。 在加密流量检测库、共享接入特征库、应用特征库、URL 特征库、沙箱白名单、病毒过滤特征库、入侵防御特征库、IP 信誉特征库、僵尸网络防御特征库、ISP 信息库相应模块配置对应特征库远程升级参数。 协议：选择特征库的更新方式，包括 HTTP 和 HTTPS。点击“恢复缺省”按钮，恢复默认 HTTPS 传输方式。 升级服务器：设备提供两个默认特征库更新服务器。用户也可根据需要自定义升级服务器：在“升级服务器”模块，指定

选项	说明
	需要的服务器的 IP 地址或者域名，并在下拉菜单中指定虚拟路由器。升级服务器均支持双栈协议，可配置 IPv4 和 IPv6 地址。 升级代理服务器：当设备需要通过 HTTP 代理服务器访问互联网时，为确保特征库能够正常升级，需要在设备上指定代理服务器的 IP 地址和端口号。在“升级代理服务器”模块，输入主代理服务器和备代理服务器的 IP 地址和端口。升级服务器均支持双栈协议，可配置 IPv4 和 IPv6 地址。 自动升级配置：点击“启用”按钮并设置自动升级时间，点击“确定”按钮，系统将按照设置的时间自动升级特征库。 确定并在线升级：点击该按钮，立即升级特征库。
本地升级	系统支持通过默认特征更新服务器下载升级包进行本地升级。 通过特征库服务器路径下载加密流量检测库、应用特征库、URL 特征库、病毒过滤特征库、入侵防御特征库、IP 信誉特征库、僵尸网络防御特征库、ISP 信息库对应的升级包。 在各特征库升级模块，点击“本地升级”，在“升级包路径”处上传升级文件：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。

升级可信根证书

为保证设备本地存储的服务器根证书足够全且最新，减少验证服务器证书时出现问题，用户需及时升级更新可信根证书库，可选择远程升级或本地升级方式。系统升级可信根证书库时，将删除已被吊销证书、过期证书和添加新的根证书等。

升级可信根证书库，请按照以下步骤进行操作：

1. 选择“系统>升级管理>可信根证书升级”。
2. **进入“可信根证书升级”页面。**

选项	说明
当前版本	显示当前可信根证书库的版本号。
远程升级	点击“远程升级”按钮，配置可信根证书库远程升级参数。 升级服务器：设备提供两个默认可信根证书库更新服务器。用户也可根据需要自定义升级服务器：在“升级服务器”模块，指定需要的服务器的 IP 地址或者域名，并在下拉菜单中

选项	说明
	指定虚拟路由器。 升级代理服务器：当设备需要通过 HTTP 代理服务器访问互联网时，为确保可信根证书库能够正常升级，需要在设备上指定代理服务器的 IP 地址和端口号。在“升级代理服务器”模块，输入主代理服务器和备代理服务器的 IP 地址和端口。 自动升级配置：点击“启用”按钮并设置自动升级时间，点击“确定”按钮，系统将按照设置的时间自动升级可信根证书库。 确定并在线升级：点击该按钮，立即升级可信根证书库。
本地升级	系统支持通过默认特征更新服务器下载升级包进行本地升级。 通过特征库服务器路径下载可信根证书库升级包。 点击“本地升级”按钮，并上传本地升级文件：点击“浏览”按钮，选中本地根证书库文件，点击“上传”按钮，系统开始上传可信根证书库信息。

许可证

不同档次的设备性能，由许可证的控制。只有购买并安装了相应的许可证，才能使产品达到其标称的数值。购买之后默认会安装基础 license 及入侵防御、病毒过滤、URL 功能 license，其余 license 需要单独扩展。

许可证展示

选择“系统 > 许可证”，进入许可证页面。许可证列表部分显示当前系统支持的所有许可证，包括已授权的和未授权的两种。

如果许可证即将过期（有效时间剩余 30 天内）或者已经过期：

登录设备后，系统将会弹出<许可证过期>对话框，提示即将过期或者已经过期的许可证。您可以勾选“当天不再提醒“复选框关闭提示。点击“前往更新”按钮，系统将跳转到许可证页面。

系统右上角的通知图标会显示通知数量，将鼠标指针移动到图标上，点击<许可证过期>后的“详情”，系统弹出<许可证过期>对话框。

许可证校验

此步骤开通默认完成

安装许可证后，需连接到 LMS（许可证管理系统），进行合法性校验，以防止许可证被克隆。

若防火墙到 LMS 进行校验，设备将会每隔 30 天进行重启。

使用过程中不可随意改动该项配置。

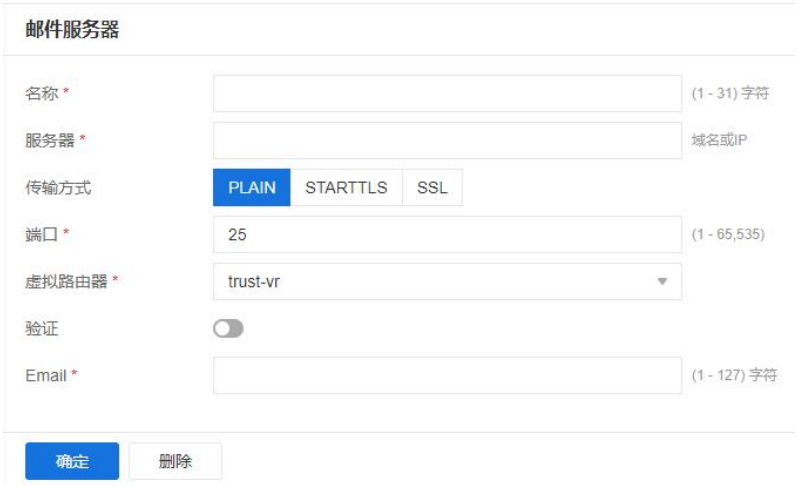
配置邮件服务器

用户可以在邮件服务器配置页面配置邮件服务器，系统将会通过配置好的邮件服务器将日志信息、报表文件或者告警信息以邮件形式发送到指定的邮箱。

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”。**



选项	说明
名称	在文本框输入邮件服务器的名称。

选项	说明
服务器	在文本框输入邮件服务器的域名或者 IP 地址。
传输方式	指定邮件的传输方式。 PLAIN：指定邮件使用明文且非加密的方式传输。该方式为默认传输方式。 STARTTLS：STARTTLS 是对纯文本通信协议的扩展，它将纯文本连接升级为加密连接。指定为该方式，邮件将使用加密方式传输。 SSL：SSL 协议是为网络通信提供安全及数据完整性的一种安全协议。指定为该方式，邮件将使用加密方式传输。
端口	在文本框中指定邮件服务器的端口号。范围是 1 到 65535。不同传输方式下的默认端口号不同，PLAIN：25，STARTTLS：25，SSL：465。
虚拟路由器	从下拉菜单中选择邮件服务器的 VR。
验证	用户可根据需要，点击“启用”按钮开启验证功能，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。编辑邮件服务器配置时，可以看到修改密码功能。开启后，将展示密码输入框。如需修改，输入新的密码后保存配置即可。
Email	在文本框中指定 Email 地址，系统将通过该 Email 地址发送邮件。

2. 点击“应用”按钮，保存当前页面所做配置。

短信网关

本节主要介绍短信网关的配置。

配置短信网关

配置短信网关，按照以下步骤进行操作：

1. 选择“系统 > 短信发送参数 > 短信网关”，进入短信网关页面。

2. 点击列表上方的“新建”，打开<短信网关配置>页面。

在<短信网关配置>页面，配置短信网关相关信息。

选项	描述
协议类型	指定短信网关协议。SGIP 表示联通的 SGIP 协议，UMS 表示使用联通企业信息平台，ACC 表示电信的 ACC 协议，ALIYUNSMS 表示使用阿里云短信服务平台，XUANWU 表示使用玄武科技短信服务平台，CAS 表示使用 12302 短信服务平台，BEIKE 表示贝壳的短信网关，HTTP(S)表示 HTTP/HTTPS 协议。
服务商名称	指定服务商名称。取值范围是 1 至 31 个字符。
发送方式	当协议类型指定为 HTTP(S)时，指定系统向短信网关发送 HTTP 请求时使用的方法。默认为 POST 方式。
内容类型	当协议类型指定为 HTTP(S)时，指定系统向短信网关发送 HTTP Post 请求报文的内容类型（Content-type），默认为 URL-ENCODE。 URL-ENCODE - 指定 HTTP POST 请求报文的内容类型为 application/x-www-from-urlencode。 JSON - 指定 HTTP POST 请求报文的内容类型为 application/json。
编码格式	当协议类型指定为 HTTP(S)时，指定对认证短信内容进行编码的格式。默认为 UTF-8 编码格式。
UMS 协议	当协议类型指定为“UMS”时，用户可以指定 UMS 协议

选项	描述
	类型。默认情况下，使用 HTTPS。
协议	当协议类型指定为“ACC”、“ALIYUNSMS”、“CAS”或者“BEIKE”时，用户可以指定协议类型。当协议类型指定为“CAS”或者“BEIKE”时，默认协议为 HTTPS；当协议类型指定为“ACC”或者“ALIYUNSMS”时，默认协议为 HTTP。
虚拟路由器	指定短信网关所属的 VRouter。系统有一个默认 VRouter，即 trust-vr，同时系统支持多 VR。
url 地址	当协议类型指定为 HTTP(S)时，指定短信网关的 URL 地址，需要输入完整的访问路径，例如“http(s)://1.1.1.1:80/SendSms”。系统根据指定的 URL 地址向短信网关请求通信。取值范围为 1 至 255 个字符。
成功标识	当协议类型指定为 HTTP(S)时，成功标识用于判断短信网关短信是否发送成功。配置成功标识需要参考不同短信网关使用手册中给出的成功发送短信时返回的状态码。例如：某短信网关成功发送短信时返回的状态码为“OK:325689”，发送短信失败时返回的状态码为“ERROR:eUser”，此时用户可以将成功标识设置为“OK”。取值范围为 1 至 50 字符。
属性	当协议类型指定为 HTTP(S)时，指定短信网关属性的参数名称和参数值，系统通过配置的属性参数和短信网关进行交互。 手机号码字段：指定手机号码的参数名称，此项为默认属性，必须配置。取值范围为 1 至 20 个字符。 短信内容字段：指定短信内容的参数名称，此项为默认属性，必须配置。取值范围为 1 至 20 个字符。 密码字段：指定登录短信网关的用户密码参数名称和参数值，参数名称和参数值必须同时存在或为空。此项为可选属性。参数名的取值范围我 1 至 20 个字符，参数值的取值范围为 1 至 255 个字符。 点击新建可以配置登录短信网关的用户名参数名称、参数值和参数类型。参数名的取值范围为 1 至 20 个字符，参数值的取值范围为 1 至 255 个字符。参数类型可配置为 HTTP DATA 或 HTTP HEADER。当配置为 HTTP DATA 时表示该属性选项将作为 HTTP 的数据内容部分；当配置为

选项	描述
	HTTP HEADER 时表示该属性选项将被加入 HTTP 的头部。 用户可根据需要新建属性，最多同时存在 32 条。勾选属性条目前的复选框，点击删除，可以删除用户新建的属性。
网关主机	指定短信网关主机的名称和 IP 地址。
短信网关端口	指定短信网关的端口号。当协议类型指定为“SGIP”时，默认端口号为 8801；当协议类型指定为“UMS”时，默认端口号为 9600；当协议类型指定为“XUANWU”或“CAS”时，默认端口号为 8080；当协议类型制定为“ACC”时，默认端口号为 80；当协议类型指定为“BEIKE”时，默认端口号为 8086。
设备编码	当协议类型指定为“SGIP”时，用户可以指定设备编码。在配置短信网关前，用户需向运营商索取允许发送短信的设备 ID。取值范围为 1 至 4294967295。
来源号码	当协议类型指定为“SGIP”时，用户可以指定来源号码。开启短信口令认证功能后，系统会向已指定的来源号码发送认证码短信。取值范围为 1 至 21 个字符。
企业编码	当协议类型指定为“UMS”时，用户可以指定在 UMS 平台上注册的企业编码。取值范围为 1 至 31 位数字。
用户名	指定登录短信网关的用户名称。当协议类型指定为“SGIP”、“UMS”或“CAS”时，取值范围是 1 至 31 个字符；当协议类型指定为“XUANWU”时，取值范围是 1 至 6 个字符。
密码	指定登录短信网关的用户名称对应的密码。当协议类型指定为“SGIP”、“UMS”或“CAS”时，取值范围是 1 至 31 个字符；当协议类型指定为“XUANWU”时，取值范围是 1 至 6 个字符。
重新输入密码	在文本框中再次输入认证密码进行确认。
模板名	指定贝壳短信网关的模板参数。
修改密码	编辑短信网关配置时，可以看到修改密码功能。开启后，将展示密码输入框。如需修改，输入新的密码后保存配置即可。
每小时最多发送条数	配置短信网关每小时最多发送的短信数量，点击“每小时最多发送条数”对应的“启用”按钮，然后在后面的文本框中输入或者选择短信数量。
每天最多发送条数	配置短信网关每天最多发送的短信数量，点击“每天最多发送条数”对应的“启用”按钮，然后在后面的文本

选项	描述
	框中输入或者选择短信数量。
AccessKeyId	阿里云短信服务中申请的 AccessKeyId，作为设备和阿里云短信网关之间相互认证时的用户名。该参数需与在阿里云短信服务中申请的模板 AccessKeyId 保持一致。
AccessKeySecret	阿里云短信服务中申请的 AccessKeySecret，作为设备和阿里云短信网关之间相互认证时的密码。该参数需与在阿里云短信服务中申请的模板 AccessKeySecret 保持一致。
确认 AccessKeySecret	在文本框中再次输入 AccessKeySecret 进行确认。
修改 AccessKeySecret	编辑阿里云短信服务配置时，可以看到修改 AccessKeySecret 功能。开启后，将展示 AccessKeySecret 输入框。如需修改，输入新的 AccessKeySecret 后保存配置即可。
交易码	当协议类型指定为“XUANWU”时，用户须向 12302 短信服务平台索取交易码，然后进行指定。取值范围是 1 至 7 个字符。
渠道码	当协议类型指定为“XUANWU”时，用户须向 12302 短信服务平台索取渠道码，然后进行指定。取值范围是 a 至 z。
请求类型	当协议类型指定为“CAS”时，用户可以向 12302 短信服务平台索取请求类型，然后进行指定。取值范围是 1 至 6 个字符。
机构子码	当协议类型指定为“CAS”时，用户可以向玄武科技短信服务平台索取机构子码，然后进行指定。取值范围是 1 至 31 个字符。
短信业务类型	当协议类型指定为“CAS”时，用户可以向玄武科技短信服务平台索取短信业务类型，然后进行指定。取值范围是 1 至 31 个字符。
发送校验码	当协议类型指定为“ACC”时，选中“启用”复选框，开启发送校验码功能。开启该功能后，ACC 短信网关向 ACC 服务器发送请求时会增加校验码字段，从而防止短信内容被篡改。

短信测试

为验证指定服务商能否正常发送短信，管理员可以向指定手机号码发送测试短信。

向指定手机号码通过指定服务商发送测试短信，请按照以下方式进行：

1. 选择“系统 > 短信发送参数>短信网关”，进入配置短信网关页面。
2. 在短信网关列表的“短信测试”栏，点击“短信测试”链接，弹出的<短信测试>对话框。

3. 在“请输入手机号”文本框输入接收测试短信的手机号码。
4. 在“请输入测试短信内容”文本框输入向指定手机号发送的测试短信的内容，默认情况下为“这是一条测试短信，请不要回复！”。
5. 点击“发送”按钮。如果发送成功，指定手机号码会收到系统发送的测试短信；如果发送失败，系统会记录日志并描述失败原因。

测试工具

设备支持域名检查，支持使用网络连接测试工具 Ping 和 Traceroute。当网络出现问题时，用户可以用这些工具对网络进行测试，查找故障原因。

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 > 诊断中心 > 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 > 诊断中心 > 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。系统支持对 IPv4 和 IPv6 的对端地址进行测试。

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 > 诊断中心 > 测试工具”，进入测试工具页面。
2. 在“虚拟路由器”下拉列表中选择 VR。
3. 选择“IPv4”或“IPv6”，指定对端 IP 地址的类型。
4. 在“Traceroute”文本框中输入网络对端的 IP 地址。
5. 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。

Secure Connect 客户端管理

终端用户可以通过以下地址下载 Secure Connect 客户端：

访问设备端提供的客户端下载地址 https://IP-Address:Port-Number。其中“IP-Address”和“Port-Number”分别为 SSL VPN 或 ZTNA 实例中指定的接口的 IP 地址和 HTTPS 端口号。

访问官方提供的客户端下载地址

MAC OS：https://vpn.obs.cn-gdgz1.ctyun.cn/MACOS/rw.eCloudSecurityCloud1.2.0.852_20230921003440.dmg

安卓：https://vpn.obs.cn-gdgz1.ctyun.cn/Android/app-eCloud-release.apk

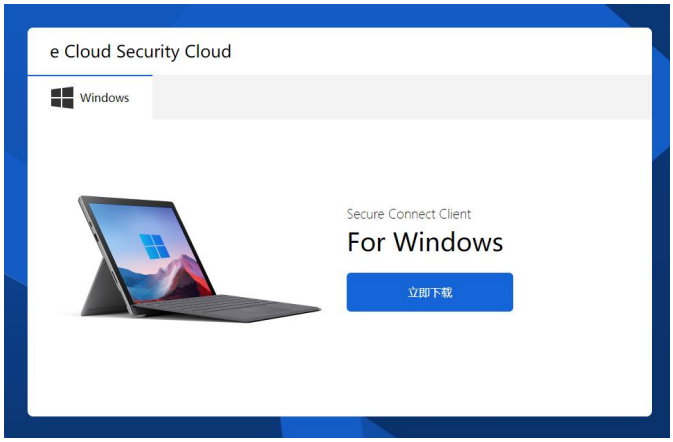
IOS：https://vpn.obs.cn-gdgz1.ctyun.cn/IOS/IOS.txt

Windows：https://vpn.obs.cn-gdgz1.ctyun.cn/Windows/scvpn.exe

默认情况下，两个地址的客户端下载源相同，下载到的 Secure Connect 客户端也是相同的。

自定义客户端下载页面

对于设备端提供的客户端下载地址，设备支持自行定制下载页面的背景图片及页面标题。默认情况下，下载页面无标题，背景图如下所示：



定制下载页面的背景图片和标题，按照以下步骤进行操作：

1. 点击“系统 > Secure Connect 客户端管理”。
2. 在“客户端下载页面配置”区域，点击“上传背景图片”按钮，选中需要的图片。图片需是 PNG 格式，建议分辨率为 1920px*1080px，大小不超过 2MB。
3. 点击“上传”按钮，将背景图片上载到系统。上传成功后，背景图片即完成修改。
4. 在“下载页面标题”文本框中，输入新的页面标题，长度为 1 到 63 个字符。
5. 点击“确定”保存设置。点击“取消”按钮，将只影响下载页面标题的设置。如不输入标题并保存配置，下载页面将不显示任何标题。
6. 点击“恢复缺省背景”，恢复默认下载页面的背景图。

自定义客户端下载源

默认情况下，设备端提供的客户端下载源与官方提供的客户端下载源相同。在需要终端用户下载和使用特定客户端时，例如特定版本客户端或定制客户端，管理员可以自行导入客户端到系统内，覆盖设备端的默认下载源，支持导入的客户端类型包括 Windows、macOS 和 Linux（测试中）客户端。

导入客户端，按照以下步骤操作：

1. 点击“系统 > Secure Connect 客户端管理”。
2. 在“客户端列表”区域，找到需要上传的客户端类型，点击“上传”按钮。
3. 在“上传 Windows/macOS/Linux 客户端”对话框，点击“浏览”按钮，选择需要上传的客户端文件，点击“上传”。
4. 上传后，“客户端列表”中相应客户端的下载源将由“官网”变为“本地”。
5. 点击“下载”按钮，检查下载的客户端是否是导入的客户端。

6. 点击“删除”按钮，删除导入的客户端。删除后，客户端下载源将恢复为默认下载源“官网”。