天翼云·云下一代防火墙

用户使用指南

天翼云科技有限公司

目 录

手册约定

熟知通用控件的操作方法，可完成大多数的功能配置。

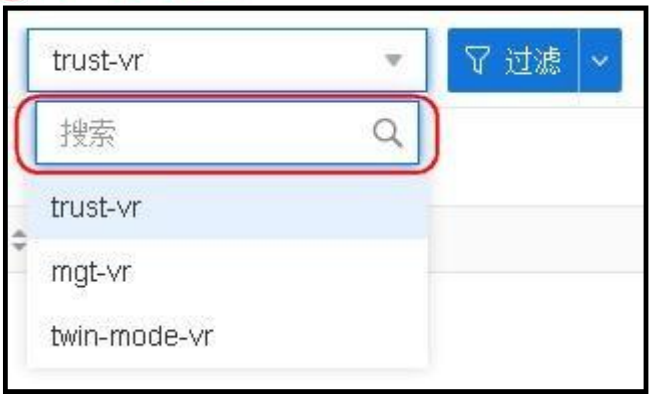
以下是通用控件和操作效果：

- 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；
收起功能列表：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　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。

- 的复选框，点击“删除”按钮。

- 点击“复制”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

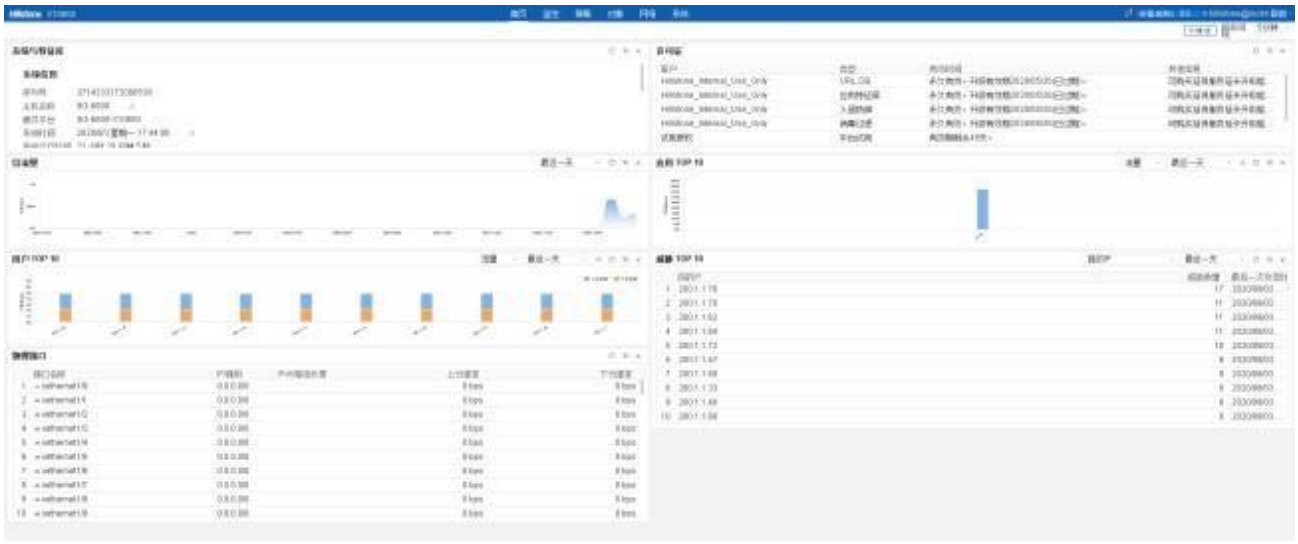
使用以下浏览器，能够获得最佳 Web 界面支持。

- IE11
- Chrome

第 1 章 首页

该功能在不同平台上的呈现方式有所差异，请以实际页面为准。

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:



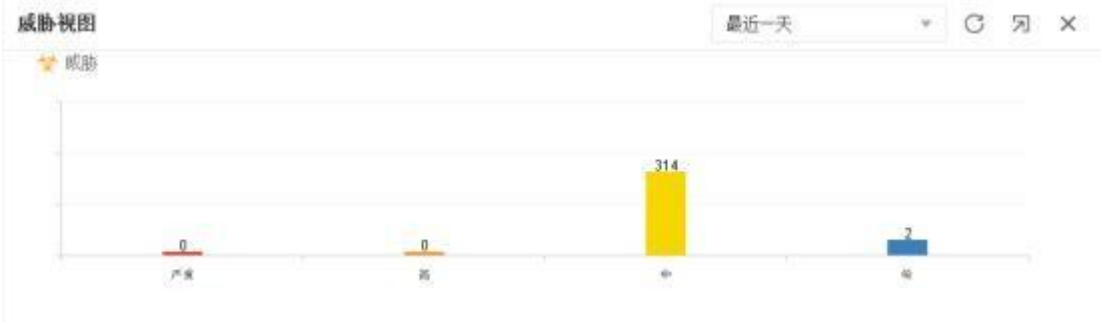
个性化配置

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 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，点击威胁情报图标，查看指定对象的威胁情报，或将光标悬浮在需要查看威胁情报的 对象上方，右侧 现 按钮。点击该按钮，选择“查看威胁情报”，在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

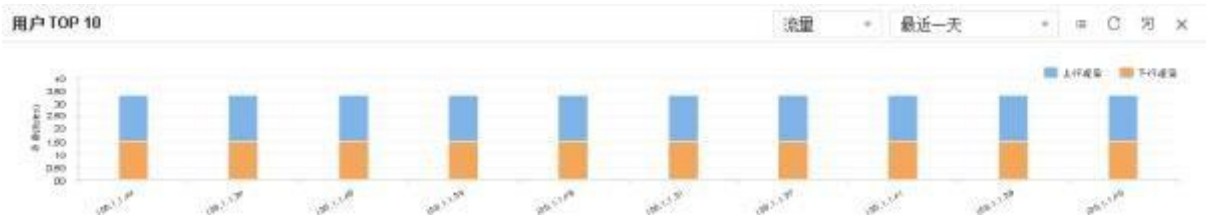
威胁视图部分以柱状图方式显示指定统计周期内的设备攻击统计信息。



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

用户信息

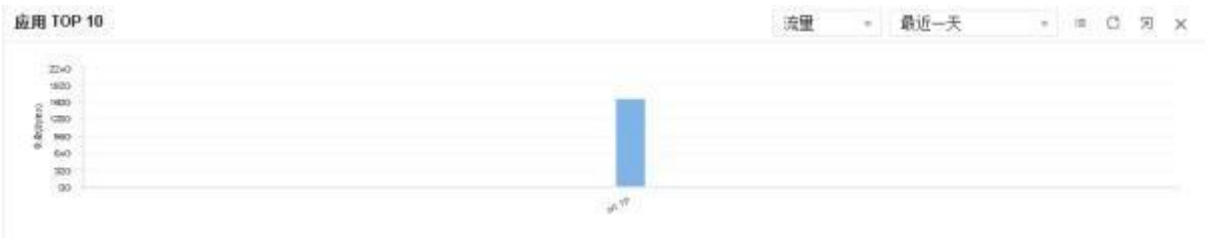
显示指定统计周期内的前 10 的用户流量。



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・界实例的　UUID（通用唯一识别码）。

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（ 最近一天 ）指定统计周期：

- 实时：显示最近 5 分钟的统计信息。
- 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。

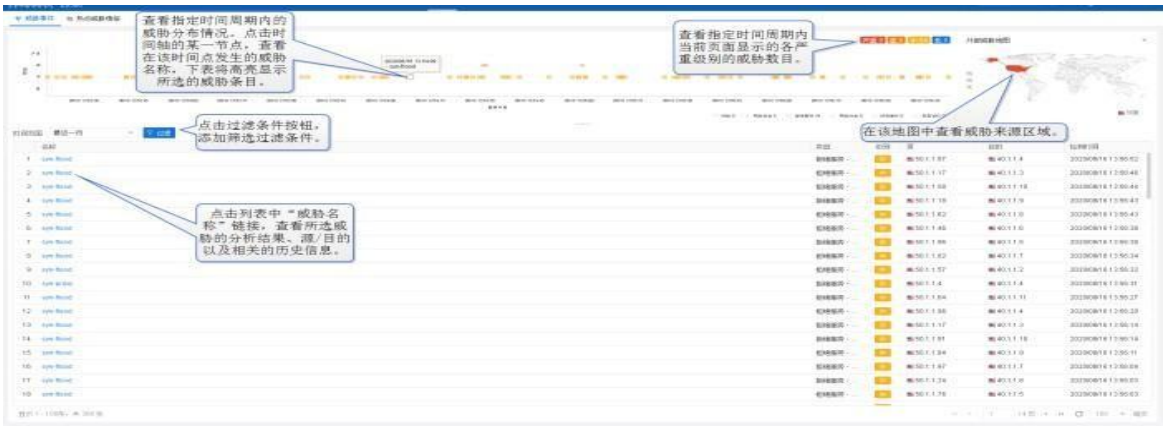
第 2 章 iCenter

仅有部分平台支持该功能，请以实际页面为准。

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。

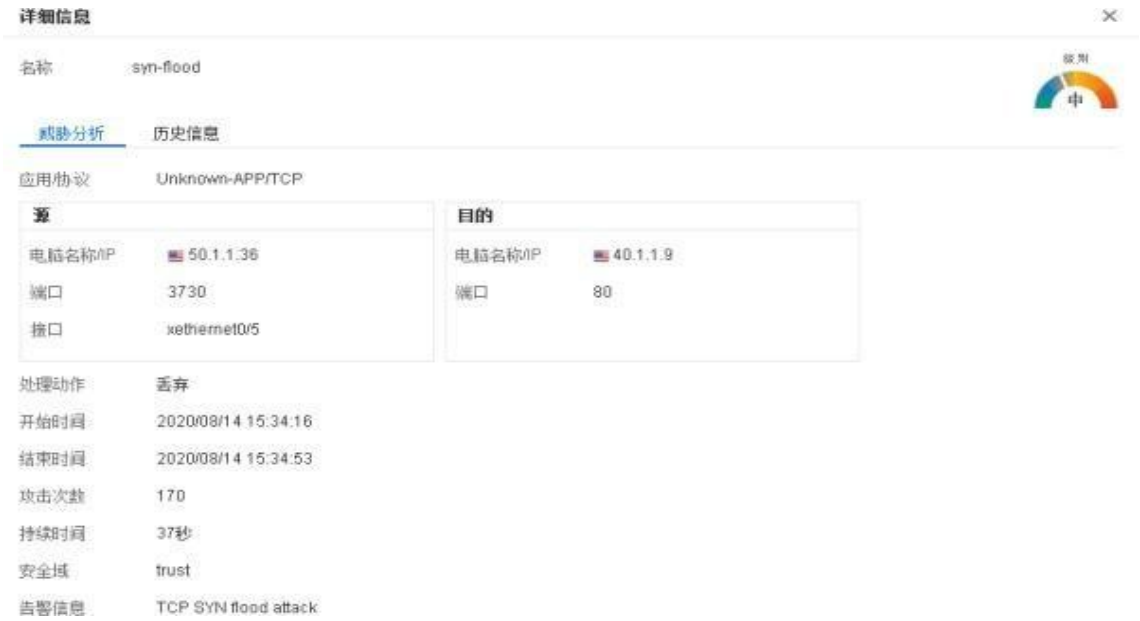
威胁事件

〈威胁事件〉统计并展示指定"第 1 章首页"内的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。

- **病毒过滤/入侵防御**：显示指定威胁的详细分析信息。
- **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。
- **攻击防护/边界流量过滤**：显示指定威胁的详细分析信息。
- **知识库**：针对入侵防御的威胁，显示指定威胁的描述信息、解决方案。
- **历史信息**：显示全网内产生所选威胁的历史信息。



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, 系统就能够对入安全域的流量进行管理和控制。
- 接口: 接口允许流量进 安全域。因此, 为使流量能够流入和流 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。
- 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 VAouter。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 VAouter 决定了该域中接口的VAouter。
- 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 0-53 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 VAouter；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。
5. 在“虚拟路由器”下拉菜单选择该安全域所属VA。
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。
- 绑定到 Tap 安全域的旁路接口仅对流量进行统计但不对流量进行转发，但是设备进入 Bypass 状态时（如系统重启、工作异常、设备断电时），Bypass 接口对中的两个接口会物理上连通，会现互相转发流量的情况。如需避免这种情况，请尽量避免将互为 Bypass 的两个接口同时设置为旁路接口。

接口

接口允许流量进 安全域。因此，为使流量能够流入和流 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，由媒体类型、插槽号和位置参数组成，例如ethernet2/1 或 ethernet0/2。
- 逻辑接口：系统中的逻辑接口包括子接口、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　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　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　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 IPv5 地址。

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。长度为 1-1024 个字符。
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。

选项	说明
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： 管理 IP：为接口指定管理 IP。在文本框中输入 IP 地址。 二级 IP：为接口指定二级 IP。最多可以指定 6 个二级 IP 地址。 DHCP：点击“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。
自动获取	说明：该功能仅在编辑已新建接口时有效，新建接口时无效。 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
管理方式	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。 选中该接口需要的管理方式的复选框。
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 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。
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 接口的 IP 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 参数	说明
MTU	指定接口的最大传输单元，单位为字节。范围是 1280 到 1800/2000 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 学习	点击“启用”按钮，开启接口的ARP 学习功能。
ARP 超时	配置接口的 ARP 超时时间，单位为秒。范围是 5 到 65535 秒，默认值是 1200 秒。
Keep-alive IP	指定接收接口的 Keep-alive 报文的 IP 地址。
MAC 克隆	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“IPv5 配置”后的“启用”按钮，展开IPv5 配置项，配置接口的IPv5 信息。

选项	说明
启用 IPv6 地址	点击“启用”按钮，开启接口的 IPv6 功能。 为接口指定 IPv6 地址，地址形式为“IPv6 地址前缀/前缀长度”。
前缀长度	指定 IPv6 地址的前缀长度。

选项	说明
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）。
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 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。

选项	说明
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 1000-3600000。
发包跳数	指定接口发 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 0-3600000。
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。

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”;
选项	说明

<table>
<tr><td>安全域</td><td>•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：
<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。
接口组：从下拉菜单中选择接口所属的集聚接口。 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>从下拉菜单中选择安全域。</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</td></tr>
<tr><td>静态 IP</td><td>IP 地址：为接口指定 IP 地址。
网络掩码：为接口指定网络掩码。
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。</td></tr>
</table>

选项	说明
	二级 IP：为接口指定二级 IP。最多可以指定 6 个二级 IP 地址。 DHCP：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。
PPPoE	说明：该功能仅在编辑已新建接口时有效，新建接口时无效。 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 访问集中器：指定访问集中器的名称。

选项	说明
高级选项	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。
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。

4. ″点击“IPv5 配置”后的“启用”按钮，展开IPv5 配置项，配置接口的IPv5 信息。

5. **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。

选项	说明
ARP 学习	点击“启用”按钮，开启接口的ARP 学习功能。
ARP 超时	配置接口的 ARP 超时时间，单位为秒。范围是 5 到 65535 秒，默认值是 1200 秒。
Keep-alive IP	指定接收接口的 Keep-alive 报文的 IP 地址。
MAC 克隆	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。

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，以及为设备的 DNS 代理功能设置响应报文的TTL。
- 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“服务器 IP”文本框输入DNS 服务器的 IP 地址。
4. 在“虚拟路由器”下拉菜单选择VA，默认为缺省 VA，即 trust-vr。

5. 点击“确定”按钮。

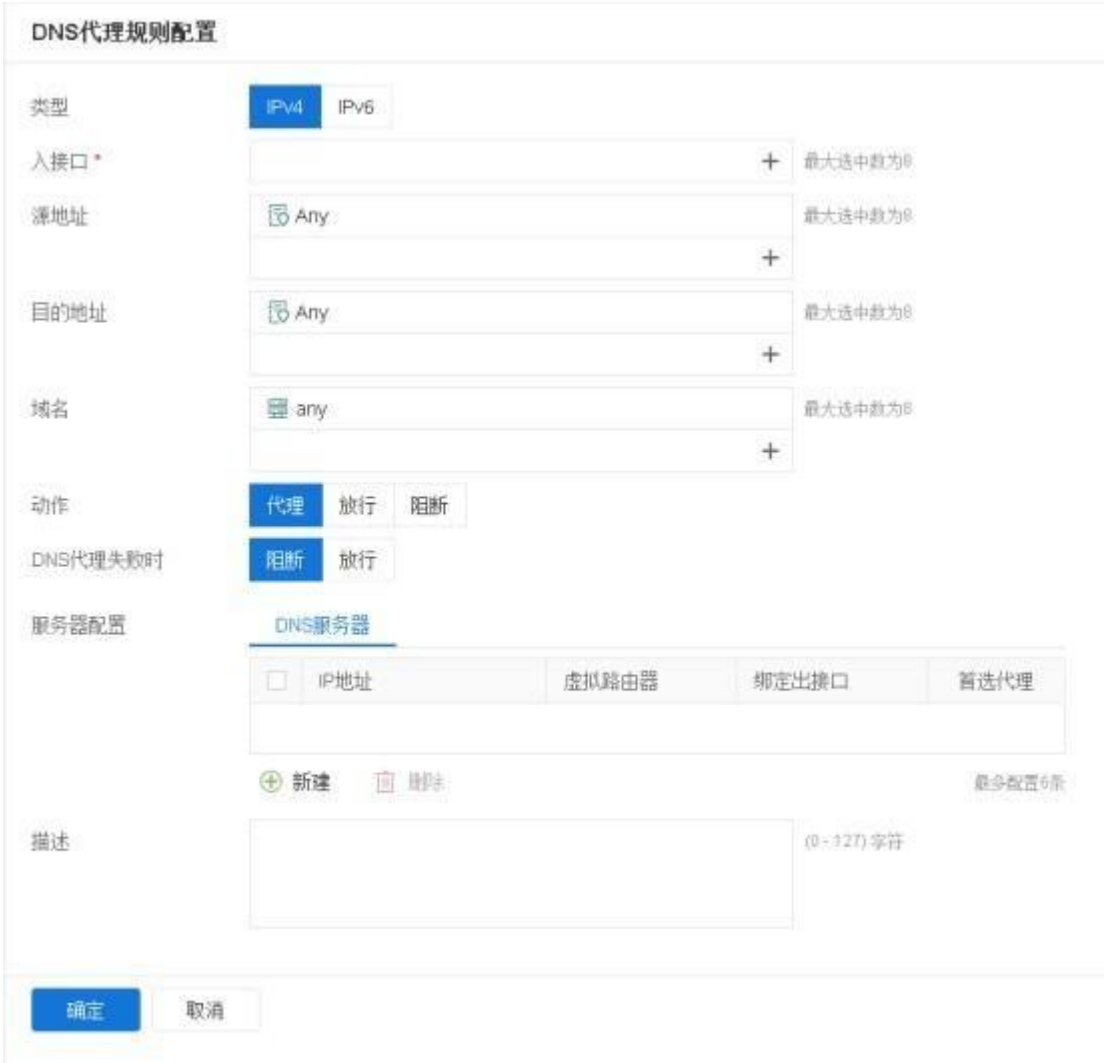
配置 DNS 代理

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。



选项	说明
类型	指定 DNS 代理规则类型，IPv4 或者 IPv5。
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"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"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。

选项	说明
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。
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 5 个 DNS 代理服务器。用户可按需为 DNS 服务器绑定 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 接口的 DNS 服务器；若有，则轮询选择 接口 DNS 服务器；若无 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 IPv5 地址）及所属虚拟路由器等参数即可。
DNS54	DNS54 用于当 IPv5 客户端主机收到DNS 查询时，先解析DNS 查询信息中的 AAAA 记录（IPv5 地址），如果解析成功，则直接将 IPv5 地址返回给客户端；如果解析失败，那么DNS54 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（IPv5 地址）返回给客户端。 点击“启用”按钮，开启设备的 DNS54 功能。默认情况下，该功能是关闭的。
DNS54 服务器	DNS54 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 DNS54 功能后，需继续指定 DNS54 服务器。每条 IPv5 DNS 代理规则最多可以指定 5 个 DNS54 服务器。 DNS54 前缀：指定 DNS54 前缀地址和前缀长度。DNS54 前缀用于将 A 记录（IPv4 地址）合成 AAAA 记录（IPv5 地址），合成的 IPv5 地址为“DNS54 前缀+IPv4 地址”形式。默认情况下，DNS54 前缀为“54:ff9b:: /95”。 在 DNS54 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。

选项	说明
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 500s。默认值是 50s。
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 50s，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。

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 DNS 请求。如果在指定的重试次数内（即为DNS 请求重试次数）仍得不到响应，设备会向下一个DNS 服务器发送 DNS 请求。
3. 在“超时”处指定DNS 请求响应超时时间。设备向DNS 服务器发送 DNS 请求后，会等待DNS 服务器的DNS 响应，如果一定时间内，仍没有响应，设备会再次发送请求。这一等待时间即为 DNS 请求响应超时时间。
4. 配置完成点击“应用”按钮将配置应用到系统中。

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VA，系统显示该 VA 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。

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.

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。

选项	说明
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。
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。
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 第二次请求，如果再次失败，将会在 10（5x2）分钟后再次发 请求，再次失败，则在 20（10x2）分钟后发 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 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 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。

站负载均衡

在 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 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 > 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。
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：High Performance 和 High Compatibility。 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

配置 LL

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（DBA）和策略路由(PBA)。请按照以下步骤进行操作:

1. 选择“网络 > 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。
LLB 模板	选择需要绑定的模板。
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。
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。设备支持两种方式，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	选择需要绑定的域名簿。

3. 点

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.
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 54 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
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。
返回地址	从下拉框选择系统中预定义或用户自定义的 ISP 名称。 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。
监测对象	从下拉框选择 ISP 链路的入站接口。 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

选项	说明
	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。

5. 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、MSAPC、PPTP、Q.931、AAS、ASH、ATSP、SIP、SQLNetV2、SUNAPC、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 50-1800 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. 

IP 分片	
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 TCP 窗口，该 TCP 包将会被丢弃。
TCP 三次握手	配置是否检查TCP 三次握手超时时间。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 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AST：当收到的包为 TCP非 SYN包时，丢弃数据包并向对方设备发送AST 报文。
其他	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。
'' IP包且非 ARP 包	

3. 点击“确定”。

配置防

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：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VAouter，进行路由配置，对不同的数据包进行转发。系统有一个默认 VAouter，即 trust-vr，同时系统支持多 VAouter（多 VA）功能。

设备支持目的路由、ISP 路由、源路由（Source-Based Aouting，简称 SBA）、源接口路由（Source-Interface-Based Aouting，简称 SIBA）、目的接口路由（Destination-Interface-Based Aouting，简称 DIBA）、策略路由（Policy-Based Aouting，简称 PBA）、动态路由（包括 AIP、OSPF 和 BGP）和等价多径路由（Equal Cost MultiPath Aouting，简称 ECMP）。

- ″配置目的路由″ ：手工定义的路由条目，根据目的地址指定下一跳。
- ″配置目的接口路由″：根据数据包的目的IP 地址和入接口，选择路由，进行转发。
- ″配置源路由″：根据数据包的源IP 地址，选择路由，进行转发。
- ″配置源接口路由″ （SIBA）：根据数据包的源IP 地址和入接口，选择路由，进行转发。
- ″配置策略路由″（PBA）：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（″配置 AIP″、″配置 OSPF″或者″配置 BGP″）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 IPv5 地址。如接口开启了 IPv5 功能，用户可根据需要配置 IPv5 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<IPv5>标签页，在对应页面新建IPv4 目的路由或 IPv5 目的路由。该步骤仅适用于IPv5 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。
选项	**说明**

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。
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<IPv5>标签页，在对应页面新建 IPv4 目的接口路由或 IPv5 目的接口路由。该步骤仅适用于IPv5 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。 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。

选项	说明
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。
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<IPv5>标签页，在对应页面新建IPv4 源路由或 IPv5 源路由。该步骤仅适用于IPv5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。

选项	说明
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<IPv5>标签页，在对应页面新建 IPv4 源接口路由或 IPv5 源接口路由。该步骤仅适用于 IPv5 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。
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。
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	输入所需的源接口路由描述信息。长度为 0-63 个字符。
点击“确定”按	丑保存所做的配置。新创建的路由条目将会显示在源接口路由列表中

4.

配置策略路由

用户可以配置策略路由（PBA），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
用户	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。 系统默认地址配置为 any。如需恢复为 any，选择 **any** 复选框。 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”。 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。 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。

选项	说明
	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。 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 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。

选项	说明
监测对象	从下拉框中指定监控对象。
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:PBA 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PBA 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，PBA 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PBA 策略到接口、虚拟路由器或者安全域来实现 PBA 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 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PBA 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 PBA 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PBA 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 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（AFC2328）。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VA，新建的路由将属于该 VA。
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。 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 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。

选项	说明
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。

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下方列表中。

- 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 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/DA（指定路由器）和 Full/BDA（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 IPv5 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 IPv5 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：

- Aouter 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，LSA（Link State Aequest，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 Aouter 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VAouter 分别配置OSPFv3 协议。

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VA，新建的路由将属于该 VA。
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
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 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。
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。

选项	说明
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。
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。
接口区域配置	配置接口所属的 OSPFv3 区域及实例。 **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。 **接口**：指定运行OSPFv3 协议的接口。 **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。

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下方列表中。

- 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　　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/DA（指定路由器）和 Full/BDA（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。

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。
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。 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。

选项	说明
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 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。 **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。

选项	说明
	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

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（AA）、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（AA）：AA 是 CA 的延伸，AA 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（CAL）：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 CAL 来声明该证书是无效的，并列　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。

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 ASA 和 DSA。
模长	密钥对的模长，单位为比特。ASA 和 DSA 的模长可选项为 1024（系统默认值）、2048、512 和 758。
导入	
	• 密钥对- 若选择该选项，在密钥对类型中指定导入 ASA 或 DSA 类型的密钥到PKI。
导入密钥	从本地导入密钥文件。

3.

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；

基本	
	• 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。
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。

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. 找到将该证书的路径，然后点

5. （可选）在<证书吊销列表>页面配置与 CAL 有关的参数。

证书吊销列表（CAL）	
检查	•不检查- 设备不检查 CAL。该选项为默认选项。 •可选- 即使 CAL 不可用，设备仍然可以接受对端的认证。 •强制- 只有 CAL 可用时，才可以接收对端认证。
UAL 1 UAL 2 UAL 3	指定获得 CAL 信息的 UAL。系统最多支持 3 个 UAL，最先使用 UAL1，依次为 UAL2、UAL3。 •选择“http://”，指定通过 HTTP 方式获得 CAL 信息; •选择“ldap://”，指定通过LDAP 方式获得 CAL 信息。 如果通过 LDAP 方式获得 CAL 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 CAL。
自动更新	CAL 列表的自动刷新频率。
手动更新	通过手动点击“获取 CAL”的方式更新 CAL 列表。

7.点击“确定”按钮。

导入导　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　，然后再导入到另外一台设备。

导　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　的信任域。
3. 选择要导　的证书类型，然后选择“导　”。

若导　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　现，选择保存路径即可下载相应信息。

将已经导　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　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。

第 5 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。

IPSec VPN

IPSec 是为实现VPN 功能而使用的协议。IPSec 给 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-255）、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IKE 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 IKE 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。

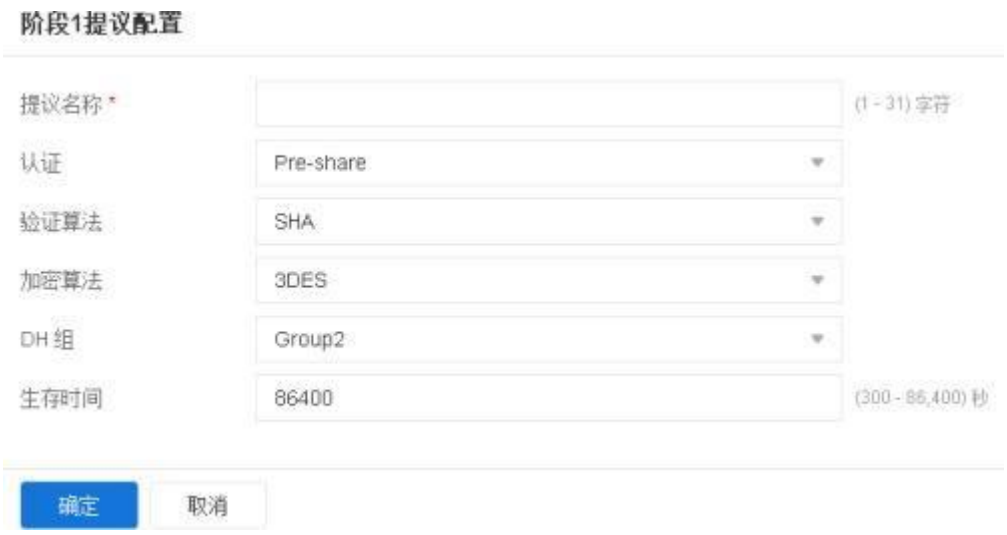
配置 IKE VPN，需要确认第一阶段提议，第二阶段提议，以及 VPN 对端信息。确认这三部分内容后，可继续完成IKE VPN 的配置。

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. 点击“网络 > VPN > IPSec VPN”，进入 IPSec VPN 页面。
2. 选择<IKE VPN 配置>页面。

3. 点击“P1 提议”下方的“新建”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）、ASA 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 150 比特。该算法为系统的默认算法。 •SHA-255 – 指定使用 SHA-255 验证算法。摘要为 255 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。

选项	说明
DH 组	•DES – 指定使用DES 加密方法。密钥长度为 54 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-255 – 指定使用 255bit AES 加密方法。密钥长度为 255 比特。 P1 提议选择DH 组。 •Group1 – 选择DH 组 1。密钥的长度为 758 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 1535 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) 。 •Group15 – 选择DH 组 15。密钥的长度为 4095 比特 (MODP Group) 。 •Group19 – 选择DH 组 19。密钥的长度为 255 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 255-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 85400 秒。范围是 300 到 85400 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。

4. 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<IKE VPN 配置>页面。
3. 点击“P2 提议”下方的“新建”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 150 比特。该算法为系统的默认算法。 •SHA-255 – 指定使用 SHA-255 验证算法。摘要为 255 比特。

选项	说明
	•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。 • 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 54 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-255 - 指定使用 255bit AES 加密方法。密钥长度为 255 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 758 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 1535 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) 。 •Group15 - 选择DH 组 15。密钥的长度为 4095 比特 (MODP Group) 。

选项	说明
	• Group19 – 选择DH 组 19。密钥的长度为 255 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 255-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 启用生存大小	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 85400 秒。 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。

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<IKE VPN 配置>页面。

3. 点击“VPN 对端列表”下方的“新建”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 IPv5。
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 IPV5。该选项仅适用于 IPv5 版本。

基本配置	
认证模式	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 Aadius 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。
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。
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。
签名信任域	如果使用 DSA Signature 或 ASA 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。

基本配置	
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 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	点击“启用”按钮在设备上启用 XAUTH 服务器，并在“地址池”下拉菜单中选择系统中已配置的地址池。启用 XAUTH 服务器后，设备可以结合已配置的认证服务器（AADIUS 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。
击“确定”完成配置。	

4. 点

配置IKE VPN

使用 IKE 完成自动协商 IPSec SA。配置 IKE 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<IKE VPN 配置>页面，点击“IKE VPN 列表”下方的“新建”按钮，打开<IKE VPN 配置>页面。

在<基本配置>页面，填写基本信息。

对端	
对端选项	选择 ISAKMP 网关的名称。
隧道	
名称	指定“隧道”的名称。
模式	指定操作模式。当前版本支持隧道模式（tunnel）和传输模式（transport）。
P2 协议	为隧道指定 P2 提议。
代理 ID	为隧道指定第二阶段 ID。分为自动和手工两种。 •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: 指定本地第二阶段 ID。 •远程 IP/掩码: 指定对端第二阶段 ID。 •服务: 指定服务名称。如需创建新的应用组，点击“新建应用组”。

在<高级配置>标签页，填写高级配置选项。

选项	说明
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。
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 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。 •54 - 指定防重放的窗口为 54。 •128 - 指定防重放的窗口为 128。 •255 - 指定防重放的窗口为 255。 •512 - 指定防重放的窗口为 512。

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 现时间差。但是，设置 Commit 位可能会使响应速度变慢。
使用代理 ID	开启该功能后，如果设备作为接收端，它将接受对端的 ID 作为为它的 IKE 协商代理 ID，并返回该 ID 给对端。
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 50 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。
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 <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。
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： • 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。

3. 点击“确定”完成配置。

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。

基本配置	
模式	指定 IPSec 协议的操作模式。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　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　方向安全联盟的 SPI 一样；本端的　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　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 IPv5。该选项仅适用于 IPv5 版本。
协议	指定 IPSec 协议类型。ESP 协议为系统默认协议类型。
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　方向的加密密钥相同，而本端　方向的加密密钥必须与对端进方向的加密密钥相同。
方向加密密钥	指定　方向加密密钥。
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　方向的验证密钥相同，而本端　方向的验证密钥必须与对端进方向的验证密钥相同。
方向验证密钥	指定　方向验证密钥。
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。

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 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. 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 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。

各监控页面具体选项说明如下:

ISAKMP SA 列表

选项	说明
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。
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。
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。

选项	说明
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。

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 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 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 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：

- "SSL VPN 客户端 for Windows"
- "SSL VPN 客户端 for Android"
- "SSL VPN 客户端 for iOS"

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。
接入用户	
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
接口 1 接口 2	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 1。 在下拉菜单中选择需要的设备端接口 2。一般配置一个 接口即可，配置最优路径检测时需要配置两个 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 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 的<隧道接口>对话框中编辑该隧道接口。
地址池	指定 SSL VPN 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 的<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 的<地址池配置>对话框中编辑该地址池。

点

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 54 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 53 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 UAL，比如：“.com”、“com”。
删除	点击此按钮删除选中的域名。

绑定资源	
新建	点击“新建”按钮，将创建好的资源与用户组进行绑定。
条目名称	指定创建好的资源名称。
用户组	在下拉菜单中指定与上述资源名称相绑定的用户组。 **说明**: •一个用户组可以绑定多个资源，一个资源也可以绑定多个用户组。 •一个 SSL VPN 实例中最多可以配置 32 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 AADIUS 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。<任意>表示 SSLv2、SSLv3、TLSv1、TLSv1.1、TLSv1.2 或者 GMSSLv1.0 协议中的任何一种。 如果设备端指定的 SSL 协议类型为 tlsv1.2 或者任意，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 ASA 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 1.4.5.1239 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。
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。
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	
允许浏览器登录	浏览器登录功能指通过浏览器 Web 页面的方式登录 SSL VPN，默认情况下，该功能为开启状态。选中“启用”复选框开启该功能。取消勾选“启用”复选框，将关闭该功能，用户只能通过客户端方式登录 SSL VPN。 说明：浏览器登录SSL VPN的访问方法为：″https://IP-Address:Port-Number″，其中″IP-Address″为“接入接口”处配置

安全套件	
	的 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 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 15 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	辖 入允许多个登录的次数，取值范围为 0 到 99999999，其中 0 表示不限制次数。
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
DF 位	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)	SSL VPN 连接建立后的数据通讯端口。
击“客户端”，填	**写相关配置信息。**
点	
客户端配置	
修改密码 UAL	配置 UAL 地址，用户可以从客户端跳转到指定UAL 页面修改密码，长度取值范围 1-255 字符。
忘记密码 UAL	配置 UAL 地址，用户可以从客户端跳转到指定UAL 页面重新设置密码，长度取值范围 1-255 字符。
重新定向 UAL	重定向 UAL：UAL 重定向功能是指在 SSL VPN 设备端配置重定向的 UAL，客户端认证成功后将自动跳转到指定 UAL 的页面。在文本框中输入重定向的UAL 字符串，取值范围为 1 到 255 字节。系统支持 HTTP (http://) 和 HTTPS (https://) 两种类型的UAL。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 UAL 输入，以HTTP 类型 UAL 为例： •UTF-8 编码格式的页面- 输入“UAL”+“username=$USEA&password=$PWD”。

客户端配置	
	比如，http://www.abc.com/oa/login.do?username=$GBUSEA&password=$PWD • GB2312 编码格式的页面- 输入“UAL”+“username=$GBUSEA&password=$PWD”。比如，http://www.abc.com/oa/login.do?username=$GBUSEA&password=$PWD • 其它页面- 直接输入UAL。比如，http://www.abc.com
标题	指定重定向 UAL 的描述，范围为 1 到 31 字节。该名称会在客户端菜单项中显示。
断开时清除隐私数据	选择“启用”复选框，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	选中“启用”复选框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。
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。

客户端配置
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。 •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	指定短信口令认证的类型，包括“短信猫”和“短信网关”。
短信认证类型	
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。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 1 到 53 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 个字符。默认为 8 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

选项	说明
	到 53 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 29 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 1 至 53 个字符。默认为“ ”。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 个字符。默认为 8 个字符。
邮件验证内容	指定认证码邮件的验证内容，内容必须包含“$USEANAME”和“$VAFYCODE”（“$USEANAME”用于获取用户名；“$VAFYCODE”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 <$USEANAME> email verification code: $VAFYCODE Do not reveal to anyone! If you did not request this, please ignore it.”。
<主机检测/绑定>	**标签页，填写相关配置信息。**

在

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 UAL：选中“跳转 UAL”单选按钮，然后在文本框中输入重定向 UAL。当客户端的主机安全检测失败时，将会

主机检测	
	自动打开浏览器并跳转到指定的UAL，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 选	中“启用主机绑定”复选框开启主机绑定功能。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。

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 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 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

选项	说明
	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　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。

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“资源条目名称+对应的 UAL“。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　的页面中，用户可以通过点击 UAL 链接直接访问内网资源。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　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。
添加	点击“新建”按钮，将条目名称与 UAL 的绑定条目添加到列表中。 **说明**：每个资源中可以添加的资源条目数量为 0~48。所有资源中包含的资源条目的总数不能超过 48 条。
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。
UAL	输入新资源条目所对应的UAL。
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：

- 资源列表中资源的数目不能超过 48。
- SSL VPN 的资源列表功能仅适用于 Windows 的 SSL VPN 最新客户端。

配置 SSL VPN 地址池

SSL VPN 设备端通过地址池给客户端分配 IP 地址。当客户端连接SSL VPN 设备端成功后，设备端会从地址池里取 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。

SSL VPN 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 一个 IP 地址分配给客户端。

当 SSL VPN 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 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 一个 IP 地址分配给客户端；否则，从非绑定地址范围中取 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 SSL VPN 地址池，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“SSL VPN 地址池”。
3. 点击“新建”按钮，打开<地址池配置>页面。

在<地址池配置>标签页，填写配置信息。

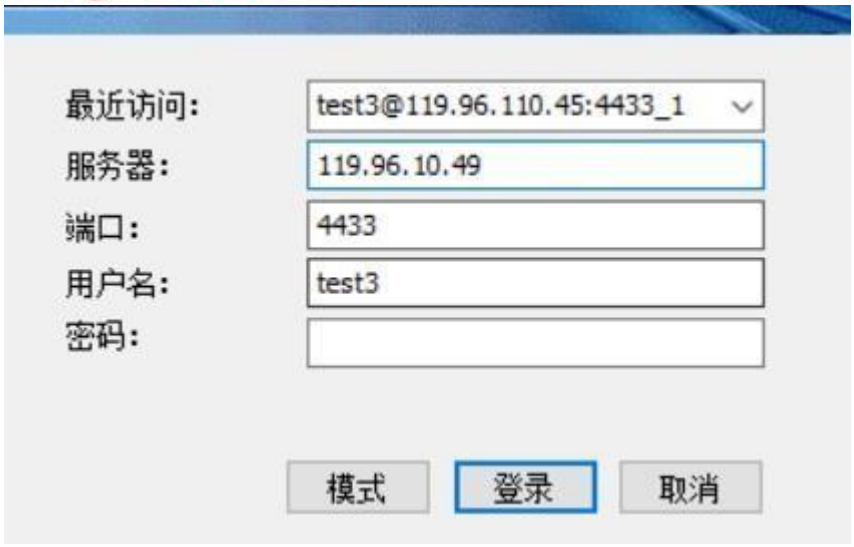
基本配置	
地址池名称	指定地址池名称。

基本配置	
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	指定网络掩码。
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。
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	输入起始 IP 地址。
终止 IP	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用户，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。

配置 SSL VPN 认证登录页

设备支持用户自行定制 SSL VPN 认证登录页面背景图片及页面标题。默认情况下，配置 SSL VPN 认证功能后，其认证登录页面背景图如下所示:



定制认证登录页面，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“SSL VPN 认证登录页”，弹 <SSL VPN 认证登录页配置>对话框。
3. 点击“浏览”按钮，选中需要的图片。
4. 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。
5. 在“认证页面标题”文本框中，输入新的页面标题。
5. 点击“确定”保存设置。点击“取消”按钮，将只影响认证页面标题的设置。

如果需要恢复默认页面标题“Login”，点击“清除页面标题”按钮，然后点击“确定”按钮；如果需要恢复默认图片，点击“恢复缺省背景”按钮，在弹 的<认证登录默认配置>对话框选中<更换中文背景>或者<更换英文背景>复选框，并点击“确定”按钮。

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。

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　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。
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。

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。
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　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　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　”按钮，导　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） • 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
其他配置	IE 版本和安全级别是否达到指定标准 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　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。
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。 • 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。
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。

选项	说明
	• 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： • 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。
击“确定”按钮，	保存所做的配置。

4. 点

SSL VPN 客户端 for Windows

针对 Windows 操作系统的 SSL VPN 客户端程序为 Secure Connect。 Secure Connect 可在以下操作系统中运行: Windows 2000/2003/XP/Vista/Windows 7/Windows8/Windows2008/Windows10/Windows2012。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 SSL VPN 设备端的连接状态、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。

本节主要介绍客户端的下载、安装、启动、卸载、GUI 和菜单。根据设备端配置的认证方式的不同，客户端的下载、安装和启动方法将不同。SSL VPN 设备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
- 只用数字证书

下载与安装客户端

初次使用 SSL VPN 客户端时，用户需要下载和安装客户端程序 Secure Connect。本节将根据设备端的三种认证方式，分别介绍对应的客户端下载和安装方法。对于“用户名/密码 + 数字证书”认证方式，数字证书可以是厂商提供的 USB Key 证书或管理员所提供的软证书。

使用“用户名/密码”认证方式

当设备端配置“用户名/密码”认证方式时，按照以下步骤下载和安装客户端程序 Secure Connect:

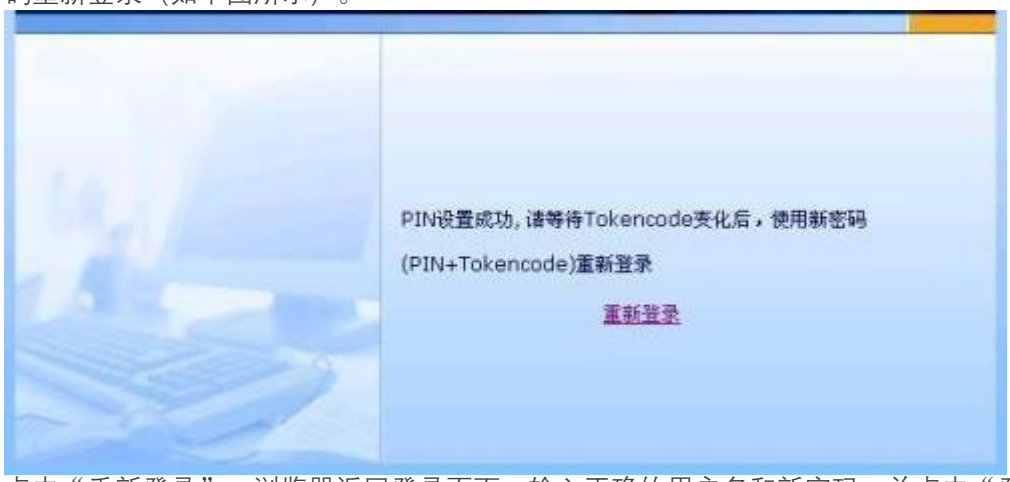
1. 在浏览器的地址栏输入以下 UAL 访问设备端: https://IP-Address:Port-Number。其中“IP-Address”和“Port-Number”分别为设备端 SSL VPN 实例中指定的接口的IP 地址和HTTPS 端口号。
2. 浏览器转到登录页面（如下图所示），输入用户名和密码，并点击“登录”按钮。

   2

   - 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;
   - 如果设备端采用“AADIUS 认证+通过 ASA Server 进行 ASA SecurID Token 认证”相结合的方式，并且是首次登录，此处输入的用户名应为 AADIUS 服务器中的用户名称，密码为该用户绑定的实时 Token 动态口令。输入完成并点击“登录”后，浏览器将转到 PIN 码设置

页面（如下图所示）。

用户需要在该页面设置PIN 码，为 4 至 8 位数字。PIN 码设置成功后，系统会提示使用新密码重新登录（如下图所示）。



点击“重新登录”，浏览器返回登录页面，输入正确的用户名和新密码，并点击“登录”按钮。此处的新密码为“PIN 码+实时 Token 动态口令”，例如，如果PIN 码设置为 54321，实时 Token 动态口令为 808771，则新密码为 54321808771；

- 如果设备端采用“AADIUS 认证+通过 ASA Server 进行 ASA SecurID Token 认证”相结合的方式，但不是首次登录，此处输入的用户名为 AADIUS 服务器中的用户名称，密码为首次重新登录时输入的新密码“PIN 码+实时 Token 动态口令”。

3. 如果设备端开启短信口令认证功能，客户端会弹 短信口令认证对话框，如下图所示。输入短信认证码，并点击『认证』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。

- 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。

4. 如果设备端开启邮件口令认证功能，客户端会弹　邮件口令认证对话框，如下图所示。输入邮件接收到的认证码，并点击『验证』按钮。如果用户在 1 分钟内没收到认证码，可以重新申请认证码。

    - 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。

5. 成功登录后，如果使用 IE 浏览器，系统将自动完成下载任务，用户只需按照提示安装即可；如果使用Firefox 等浏览器，请点击“下载”按钮下载客户端程序 scvpn.exe，下载完成，双击 scvpn.exe，按照安装向导提示进行安装。

成功安装 Secure Connect 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。

使用“用户名/密码+数字证书”认证方式

当设备端配置“用户名/密码 + 数字证书”认证方式时，按照以下步骤下载和安装客户端程序 Secure Connect：

1. 将 USB Key 插入 PC 的 USB 接口，或手动导入管理员所提供的软证书。
2. 在浏览器的地址栏输入以下 UAL 访问设备端：https://IP-Address:Port-Number。其中“IP-Address”和“Port-Number”分别为设备端 SSL VPN 实例中指定的接口的IP 地址和HTTPS 端口号。
3. 浏览器弹 <选择数字证书>对话框。选中需要的数字证书，点击“确定”按钮。如果用户使用的是 USB Key 证书，继续在弹 的<请输入 PIN 码>对话框中输入UKey 的 PIN 码（默认为“1111”），并点击“确定”按钮。UKey 的正常使用需要有配套的驱动程序和管理员软件，具体信息请参阅《UKey 使用指南》。
4. 浏览器转到登录页面（如下图所示），输入用户名和密码，并点击“登录”按钮。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。

5. 如果设备端开启短信口令认证功能，客户端会弹 短信口令认证对话框（如下图所示）。输入短信认证码，并点击“认证”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。

- 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。

5. 如果设备端开启邮件口令认证功能，客户端会弹 邮件口令认证对话框（如下图所示）。输入邮 件接收到的认证码，并点击“验证”按钮。如果用户在 1 分钟内没收到认证码，可以重新申请认证码。

   - 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。

7. 成功登录后，如果使用 IE 浏览器，系统将自动完成下载任务，用户只需按照提示安装即可；如果使用Firefox 等浏览器，请点击“下载”按钮下载客户端程序 scvpn.exe，下载完成，双击 scvpn.exe，按照安装向导提示进行安装。

成功安装 Secure Connect 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。

使用“数字证书”认证方式

当设备端配置“只用数字证书”认证方式时，请按照以下步骤下载和安装客户端程序 Secure Connect:

1. 将 USB Key 插入 PC 的 USB 接口，或手动导入管理员所提供的软证书。
2. 在浏览器的地址栏输入以下 UAL 访问设备端： https://IP-Address:Port-Number。其中“IP-Address”和“Port-Number”分别为设备端 SSL VPN 实例中指定的接口的IP 地址和HTTPS 端口号。
3. 浏览器弹 <选择数字证书>对话框。选中需要的数字证书，点击“确定”按钮。如果用户使用的是 USB Key 证书，继续在弹 的<请输入用户口令>对话框（如下图所示）中输入 UKey 的用户口令（默认为“1111”），并点击“确定”按钮。

4. 成功登录后，如果使用 IE 浏览器，系统将自动完成下载任务，用户只需按照提示安装即可；如果使用Firefox 等浏览器，请点击“下载”按钮下载客户端程序 scvpn.exe，下载完成，双击 scvpn.exe，按照安装向导提示进行安装。
5. 成功安装 Secure Connect 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。

启动客户端

客户端成功安装到PC 后，用户有两种方法可以启动客户端:

- Web 方式启动
- 直接启动

使用 Web 方式启动客户端

本节将根据设备端的三种认证方式，分别介绍对应的客户端 Web 启动方法。对于“用户名/密码+ 数字证书”认证方式，数字证书可以是厂商提供的 USB Key 证书或管理员所提供的软证书。

使用用户名密码认证方式

当设备端配置“用户名/密码”认证方式时，按照以下步骤通过 Web 启动客户端，完成客户端与设备端的连接：

1. 在 IE 浏览器的地址栏输入以下 UAL 访问设备端： https://IP-Address:Port-Number。
2. 浏览器转到登录页面（如下图所示），输入用户名和密码，并点击“登录”按钮。

配置的用户及

- 如果设备端采用“AADIUS 认证+通过 ASA Server 进行 ASA SecurID Token 认证”相结合的方式，并且是首次登录，此处输入的用户名应为 AADIUS 服务器中的用户名称，密码为该用户绑定的实时 Token 动态口令。输入完成并点击“登录”按钮后，浏览器将转到 PIN 码设置页面（如下图所示）。

用户需要在该页面设置PIN 码，为 4 至 8 位数字。PIN 码设置成功后，系统会提示使用新密码重新登录（如下图所示）。

点击“重新登录”，浏览器返回登录页面，输入正确的用户名和新密码，并点击“登录”按钮。此处的新密码为“PIN 码+实时 Token 动态口令”，例如，如果PIN 码设置为54321，实时 Token 动态口令为 808771，则新密码为 54321808771；

- 如果设备端采用“AADIUS 认证+通过 ASA Server 进行 ASA SecurID Token 认证”相结合的方式，但不是首次登录，此处输入的用户名为 AADIUS 服务器中的用户名称，密码为首次重新登录时输入的新密码“PIN 码+实时 Token 动态口令”。

提示：如果设备端配置了密码控制功能及允许修改密码功能，系统将按照密码控制功能的配置进行提示用户，例如：在密码过期前提醒用户及时修改密码，密码过期后提示用户进行密码修改，并校验新密码不能与历史密码重复等。

3. 如果设备端开启短信口令认证功能，客户端会弹　短信口令认证对话框（如下图所示）。输入短 信认证码，并点击“认证”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。

4. 如果设备端开启邮件口令认证功能，客户端会弹　邮件口令认证对话框，如下图所示。输入邮件接收到的认证码，并点击『验证』按钮。如果用户在 1 分钟内没收到认证码，可以重新申请认证码。

- 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。

完成以上各步骤后，客户端将发起自动连接以接入VPN。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。此时就可以通过 SSL VPN 实现加密通信。

使用用户名/密码+USBKey证书方式认证

当设备端配置“用户名/密码 + 数字证书”认证方式时，对于 USB Key 证书，按照以下步骤通过 Web 启动客户端，完成客户端与设备端的连接：

1. 将 USB Key 插入 PC 的 USB 接口。
2. 在 IE 浏览器的地址栏输入以下 URL 访问设备端： https://IP-Address:Port-Number。
3. 浏览器弹 <选择数字证书>对话框。选中需要的数字证书，点击“确定”按钮。在弹 的<请输入用户口令>对话框（如下图所示）中输入 UKey 的用户口令（默认为“1111”），并点击“确定”按钮。 UKey 的正常使用需要有配套的驱动程序和管理员软件，具体信息请参阅《 UKey 使用指

南》。

4. 浏览器转到登录页面（如下图所示），输入用户名和密码，并点击“登录”按钮。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。

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

    - 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。

7. 在弹　的<USB Key 口令>对话框（如下图所示）输入 UKey 的用户口令（默认为“1111”），并点击“确定”按钮。

完成以上各步骤后，客户端将发起自动连接以接入VPN。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。此时就可以通过 SSL VPN 实现加密通信。

使用用户名密码+软证书方式认证

当设备端配置“用户名/密码 + 数字证书”认证方式时，对于软证书，按照以下步骤通过 Web 启动客户端，完成客户端与设备端的连接：

1. 手动导入管理员所提供的软证书。

2. 在 IE 浏览器的地址栏输入以下 UAL 访问设备端： https://IP-Address:Port-Number。
3. 浏览器弹 〈选择数字证书〉对话框。选中需要的数字证书，点击“确定”按钮。
4. 浏览器转到登录页面（如下图所示），输入用户名和密码，并点击“登录”按钮。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。

5. 如果设备端开启短信口令认证功能，客户端会弹 短信口令认证对话框（如下图所示）。输入短 信认证码，并点击“认证”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。

5. 如果设备端开启邮件口令认证功能，客户端会弹 邮件口令认证对话框，如下图所示。输入邮件接收到的认证码，并点击『验证』按钮。如果用户在 1 分钟内没收到认证码，可以重新申请认证码。

- 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。

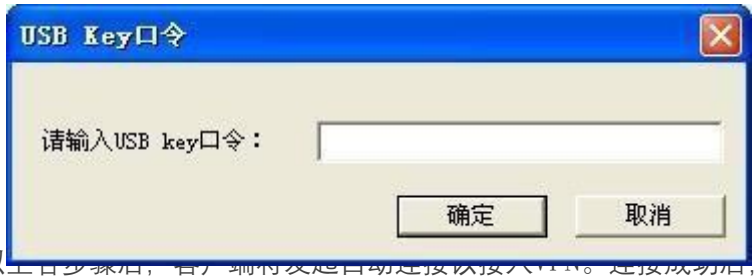
完成以上各步骤后，客户端将发起自动连接以接入VPN。连接成功后，在系统任务栏的通知区域将会显示绿色的图标。此时就可以通过 SSL VPN 实现加密通信。

使用USB Key证书方式认证

当设备端配置“只用数字证书”认证方式时，对于USB Key 证书，按照以下步骤通过 Web 启动客户端，完成客户端与设备端的连接：

1. 将 USB Key 插入 PC 的 USB 接口。
2. 在 IE 浏览器的地址栏输入以下 UAL 访问设备端： https://IP-Address:Port-Number。
3. 浏览器弹 〈选择数字证书〉对话框。选中需要的数字证书，点击“确定”按钮。在弹 的〈请输入用户口令〉对话框（如下图所示）中输入 UKey 的用户口令（默认为“1111”），并点击“确定”按钮。

4. 在弹　的<USB Key 口令>对话框（如下图所示）输入 UKey 的用户口令（默认为“1111”），并点击“确定”按钮。



完成以上各步骤后，客户端将发起自动连接以接入VPN。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。此时就可以通过 SSL VPN 实现加密通信。

使用软证书方式

当设备端配置“只用数字证书”认证方式时，对于软证书，按照以下步骤通过Web 启动客户端，完成客户端与设备端的连接：

1. 手动导入管理员所提供的软证书。
2. 在 IE 浏览器的地址栏输入以下 UAL 访问设备端： https://IP-Address:Port-Number。
3. 浏览器弹　<选择数字证书>对话框。选中需要的数字证书，点击“确定”按钮。

完成以上各步骤后，客户端将发起自动连接以接入VPN。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。此时就可以通过 SSL VPN 实现加密通信。

直接启动客户端

本节将根据设备端的三种认证方式以及 SSL 协议类型，分别介绍对应的通过启动文件直接启动客户端的方法。

基于TLS协议的启动方式

对于“用户名/密码+ 数字证书”认证方式，数字证书可以是厂商提供的 USB Key 类型数字证书或管理员所提供的文件类型数字证书。

基于 TLS/SSL 协议的启动方式如下：

- 用户名/密码
- 用户名/密码 + USB Key 证书
- 用户名/密码 + 软证书

- 只用 USB Key 证书
- 只用软证书

使用“用户名/密码”认证方式

当设备端配置“用户名/密码”认证方式时，按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接：

1. 双击桌面的 Secure Connect 快捷方式。
2. 点击对话框中的“模式”按钮，系统弹 <登录模式>对话框（如下图所示）。在“TLS/SSL”部分，选中“用户名/密码”单选按钮，点击“确定”按钮。

3. 系统弹 “用户名/密码”登录模式客户端程序登录对话框（如下图所示）。

最近访问	在下拉菜单中选择登录信息条目标识。
服务器	填写设备端的 IP 地址。

选项	说明
端口	填写设备端的 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;
- 如果设备端采用“AADIUS 认证+通过 ASA Server 进行 ASA SecurID Token 认证”相结合的方式，并且是首次登录，此处输入的用户名应为 AADIUS 服务器中的用户名称，密码为该用户绑定的实时 Token 动态口令。输入完成并点击“登录”按钮后，浏览器将转到 PIN 码设置页面（如下图所示）。

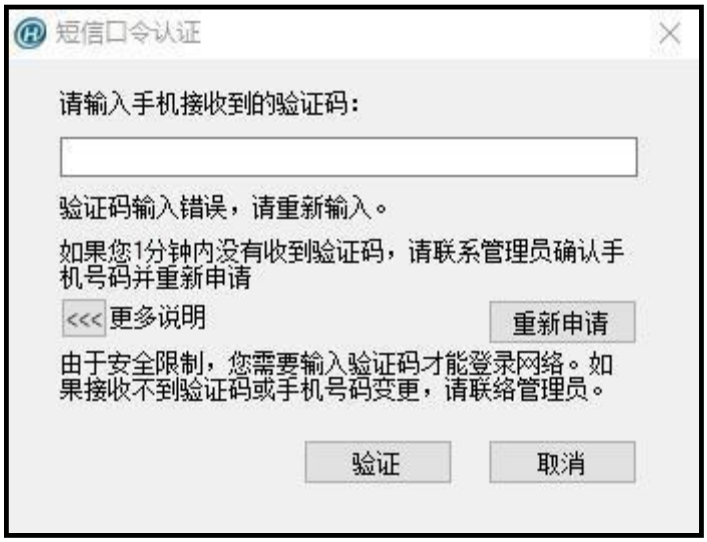
用户需要在该页面设置PIN 码，为 4 至 8 位数字。PIN 码设置成功后，系统会提示使用新密码重新登录（如下图所示）。

点击“重新登录”，浏览器返回登录页面，输入正确的用户名和新密码，并点击“登录”按钮。此处的新密码为“PIN 码+实时 Token 动态口令”，例如，如果PIN 码设置为54321，实时 Token 动态口令为 808771，则新密码为 54321808771;

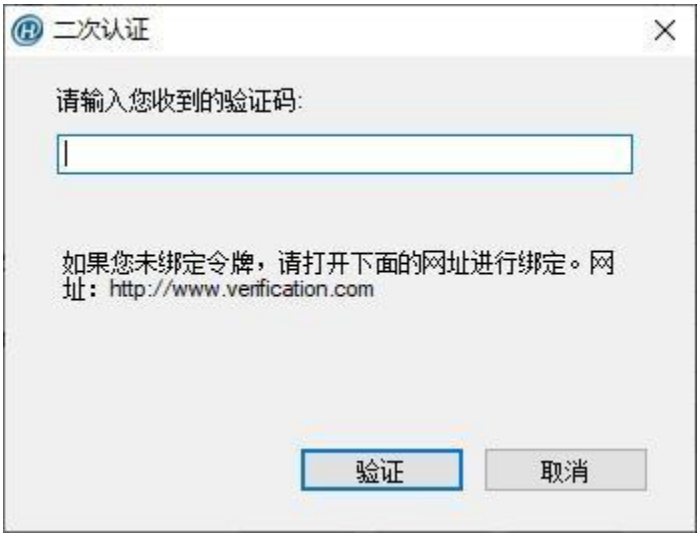
- 如果设备端采用“AADIUS 认证+通过 ASA Server 进行 ASA SecurID Token 认证”相结合的方式，但不是首次登录，此处输入的用户名为 AADIUS 服务器中的用户名称，密码为首次重新登录时输入的新密码“PIN 码+实时 Token 动态口令”。

提示: 如果设备端配置了密码控制功能及允许修改密码功能，系统将按照密码控制功能的配置进行提示用户，例如：在密码过期前提醒用户及时修改密码，密码过期后提示用户进行密码修改，并校验新密码不能与历史密码重复等。。

4. 如果设备端开启短信口令认证功能，客户端会弹　短信口令认证对话框（如下图所示）。输入短信认证码，并点击“认证”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。



5. 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（如下图所示）。输入令牌口令验证码，并点击“验证”按钮。



5. 如果设备端开启邮件口令认证功能，客户端会弹　邮件口令认证对话框，如下图所示。输入邮件接收到的认证码，并点击『验证』按钮。如果用户在 1 分钟内没收到认证码，可以重新申请认证码。

- 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。

完成以上各步骤后，客户端将发起自动连接以接入VPN。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。此时就可以通过 SSL VPN 实现加密通信。

使用“用户名/密码 + USB Key 证书”方式认证

当设备端配置“用户名/密码 + 数字证书”认证方式时，对于 USB Key 证书，请按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接：

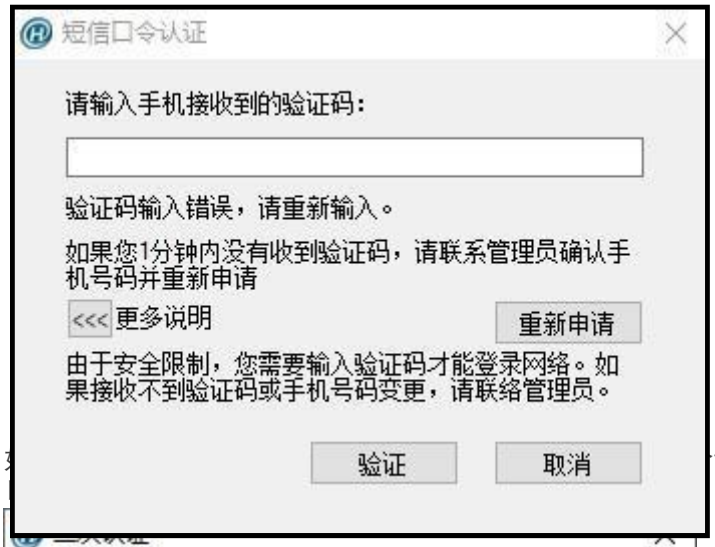
1. 将 USB Key 插入 PC 的 USB 接口。
2. 双击桌面的 Secure Connect 快捷方式.
3. 点击“模式”按钮，系统弹 <登录模式>对话框。首先，在“TLS/SSL”部分，选中“用户名/密码 + 数字证书”单选按钮；如需要，点击“选择证书”按钮，在弹 的<选择证书>对话框（如下图所示）中选择“使用 USB Key 证书”按钮。如果当前证书列表中没有显示 USB Key 证书，请点击“刷新”按钮。客户端会将选中的数字证书传送至设备端，设备端对收到的数字证书进行认证；

最后，点击“确定”按钮。

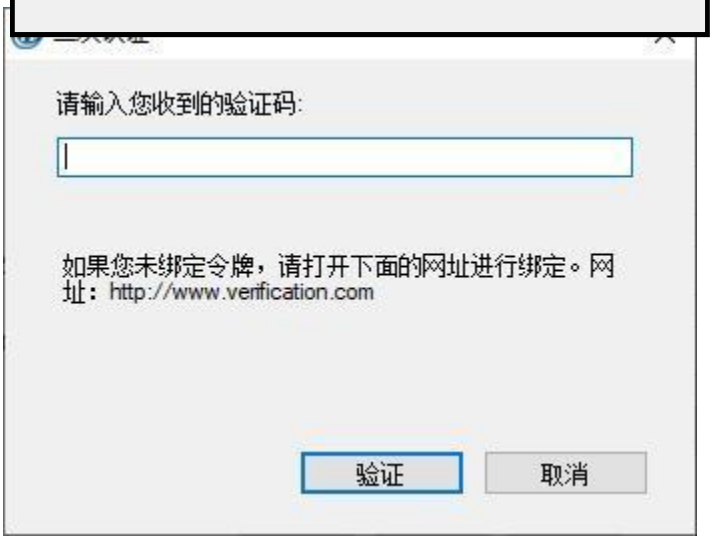
4. 序登录对话框（如下图所示）。依次填写

5. 内容填写完毕，点击“登录”按钮。如果设备端开启短信口令认证功能，客户端会弹 短信口令认证对话框（如下图所示）。在该对话框中输入认证码，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。



5. 认证对话框（如下图所示）。输入令牌



7. 如果设备端开启邮件口令认证功能，客户端会弹　邮件口令认证对话框，如下图所示。输入邮件接收到的认证码，并点击『验证』按钮。如果用户在 1 分钟内没收到认证码，可以重新申请认证码。

- 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。

完成以上各步骤后，客户端将发起自动连接以接入VPN。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。此时就可以通过 SSL VPN 实现加密通信。

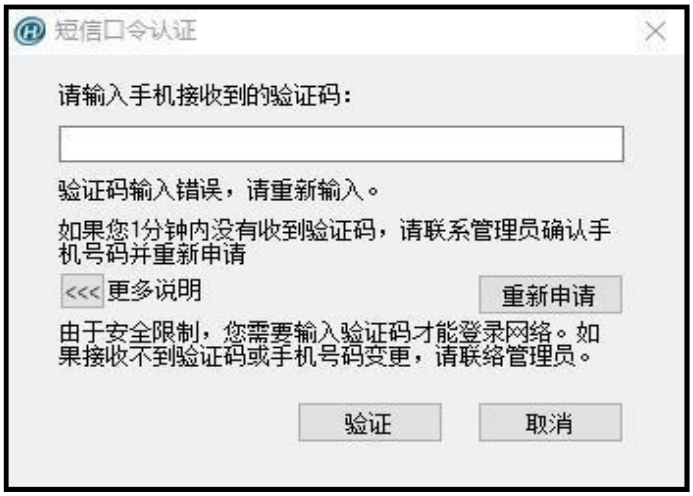
使用“用户名/密码 + 软证书”方式认证

当设备端配置“用户名/密码 + 数字证书”认证方式时，对于软证书，请按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接：

1. 手动导入管理员所提供的软证书。
2. 双击桌面的 Secure Connect 快捷方式。
3. 点击“模式”按钮，系统弹 <登录模式>对话框。首先，在“TLS/SSL”部分，选中“用户名/密码 + 数字证书”单选按钮；如需要，点击“选择证书”按钮，在弹 的<选择证书>对话框（如下图所示）中选择“使用软证书”按钮。如果当前证书列表中没有显示软证书，请点击“刷新”按 钮。客户端会将选中的数字证书传送至设备端，设备端对收到的数字证书进行认证；最后，点击“确定”按钮。

4.系统弹 “用户名/密码 + 数字证书”登录模式客户端程序登录对话框（如下图所示）。依次填写登录对话框中的各项。

5.内容填写完毕，点击“登录”按钮。如果设备端开启短信口令认证功能，客户端会弹 短信口令认证对话框（如下图所示）。在该对话框中输入认证码，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。



5.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（如下图所示）。输入令牌口令验证码，并点击“验证”按钮。

7. 如果设备端开启邮件口令认证功能，客户端会弹　邮件口令认证对话框，如下图所示。输入邮件接收到的认证码，并点击『验证』按钮。如果用户在 1 分钟内没收到认证码，可以重新申请认证码。

   - 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。

完成以上各步骤后，客户端将发起自动连接以接入VPN。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。此时就可以通过 SSL VPN 实现加密通信。

使用“USB Key 证书”方式认证

当设备端配置“只用数字证书”认证方式时，对于USB Key 证书，请按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接：

1. 将 USB Key 插入 PC 的 USB 接口。
2. 双击桌面的 Secure Connect 快捷方式。
3. 点击“模式”按钮，系统弹　<登录模式>对话框。首先，在“TLS/SSL”部分，选中“只用数字证书”单选按钮；如需要，点击“选择证书”按钮，在弹　的<选择证书>对话框（如下图所示）中选择“使用 USB Key 证书”。如果当前证书列表中没有显示 USB Key 证书，请点击“刷新”按钮。客户端会将选中的数字证书传送至设备端，设备端对收到的数字证书进行认证；最后，点击

“确定”按钮。

4. 话框（如下图所示）。依次填写登录对话

5. 内容填写完毕，点击“登录”按钮。

完成以上各步骤后，客户端将发起自动连接以接入VPN。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。此时就可以通过 SSL VPN 实现加密通信。

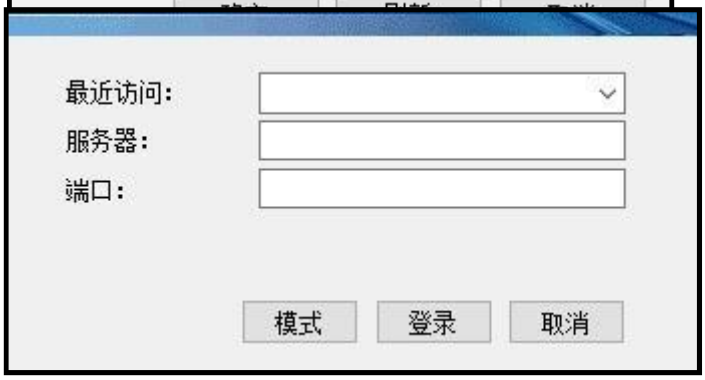
使用“软证书”方式

当设备端配置“只用数字证书”认证方式时，对软证书，请按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接：

1. 手动导入管理员所提供的软证书。
2. 双击桌面的 Secure Connect 快捷方式。

3. 点击“模式”按钮，系统弹 <登录模式>对话框。首先，在“TLS/SSL”部分，选中“只用数字证书”单选按钮；如需要，点击“选择证书”按钮，在弹 的<选择证书>对话框（如下图所示）中选择“使用软证书”。如果当前证书列表中没有显示软证书，请点击“刷新”按钮。客户端会将选中的数字证书传送至设备端，设备端对收到的数字证书进行认证；最后，点击“确定”按钮。

4. 系统弹 “只用数字证书”登录模式客户端程序登录对话框（如下图所示）。依次填写登录对话框中的各项。



5. 内容填写完毕，点击“登录”按钮。

完成以上各步骤后，客户端将发起自动连接以接入VPN。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。此时就可以通过 SSL VPN 实现加密通信。

基于国密SSL协议的启动式

基于国密 SSL 协议的启动方式如下：

- 用户名/密码
- 用户名/密码 + 数字证书
- 只用数字证书

使用“用户名/密码”认证方式

当设备端配置“用户名/密码”认证方式时，按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接：

1. 双击桌面的 Secure Connect 快捷方式。
2. 点击对话框中的“模式”按钮，系统弹 〈登录模式〉对话框（如下图所示）。在“国密 SSL”部分，选中“用户名/密码”单选按钮，点击“确定”按钮。

3. 系统弹 “用户名/密码”登录模式客户端程序登录对话框（如下图所示）。

依次填写登录对话框中的各项，然后点击“登录”按钮。

选项	说明
最近访问	在下拉菜单中选择登录信息条目标识。

选项	说明
服务器	填写设备端的 IP 地址。
端口	填写设备端的 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。

完成以上各步骤后，客户端将发起自动连接以接入VPN。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。此时就可以通过 SSL VPN 实现加密通信。

使用“用户名/密码 + 数字证书”方式认证

当设备端配置“用户名/密码 + 数字证书”认证方式时，对于 USB Key 证书，请按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接：

1. 将 USB Token 插入 PC 的 USB 接口。
2. 双击桌面的 Secure Connect 快捷方式.
3. 点击“模式”按钮，系统弹 <登录模式>对话框。首先，在“国密 SSL”部分，选中<用户名/密码 + 数字证书>单选按钮；如需要，点击“选择证书”按钮，弹 <选择证书>对话框（如下图所示）。

依次填写<选择证书>对话框中的各项，然后点击“确定”按钮。

选项	说明
当前设备	在下拉菜单中选择当前 USB Token 设备名称。
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。

选项	说明
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。

4. 系统弹 “用户名/密码+ 数字证书”登录模式客户端程序登录对话框（如下图所示）。依次填写登录对话框中的各项。

依次填写登录对话框中的各项，然后点击“登录”按钮。

选项	说明
最近访问	在下拉菜单中选择登录信息条目标识。
服务器	填写设备端的 IP 地址。
端口	填写设备端的 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。
PIN 码	填写 USB Token 对应的用户口令。

完成以上各步骤后，客户端将发起自动连接以接入VPN。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。此时就可以通过 SSL VPN 实现加密通信。

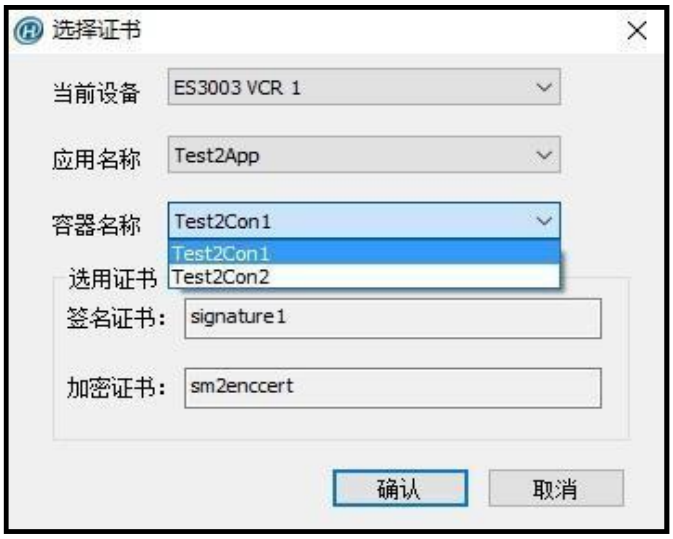
使用“只用数字证书”方式认证

当设备端配置“只用数字证书”认证方式时，对于USB Key 证书，请按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接：

1. 将 USB Token 插入 PC 的 USB 接口。

2. 双击桌面的 Secure Connect 快捷方式.

3. 点击“模式”按钮，系统弹 〈登录模式〉对话框。首先，在“国密 SSL”部分，选中〈只用数字证书〉单选按钮；如需要，点击“选择证书”按钮，弹 〈选择证书〉对话框（如下图所示）。



依次填写〈选择证书〉对话框中的各项，然后点击“确定”按钮。

选项	说明
当前设备	在下拉菜单中选择当前 USB Token 设备名称。
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。

4. 系统弹 “只用数字证书”登录模式客户端程序登录对话框（如下图所示）。依次填写登录对话框中的各项。

依次填写登录对话框中的各项，然后点击“登录”按钮。

选项	说明
最近访问	在下拉菜单中选择登录信息条目标识。
服务器	填写设备端的 IP 地址。
端口	填写设备端的 HTTPS 端口号。
PIN 码	填写 USB Token 对应的用户口令。

完成以上各步骤后，客户端将发起自动连接以接入VPN。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  。此时就可以通过 SSL VPN 实现加密通信。

查看客户端图形用户界面

双击系统任务栏通知区域的 Secure Connect 绿色的图标  ，系统弹 〈网络信息〉对话框。〈网络信息〉对话框显示统计信息、接口信息以及路由信息。

统计信息

选项具体描述如下:

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	示当前客户端的 IP 地址。
加密信息	
密码组合	依次显示 SSL VPN 使用的加密算法和验证算法。
版本	显示 SSL PN 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。可能 现的状态包括: 正在连接、已经连接、正在断开和断开。
IP 压缩	
算法	显示客户端所使用的数据压缩算法。
隧道数据包数	
发送	显示通过 SSL VPN 隧道发送的数据包数。
接收	显示通过 SSL VPN 隧道接收的数据包数。
隧道数据字节数	
发送	显示通过 SSL VPN 隧道发送的数据字节数。
接收	显示通过 SSL VPN 隧道接收的数据字节数。
连接时间	
持续	显示客户端与设备端保持连接的时间。
压缩率	

地址信息	
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。

接口信息

选项具体描述如下:

选项	说明
接口名称	显示 SSL VPN 客户端传送加密信息的接口的名称。
接口类型	显示 SSL VPN 客户端传送加密信息的接口的类型。
接口状态	显示 SSL VPN 客户端传送加密信息的接口的状态。
物理地址	显示 SSL VPN 客户端传送加密信息的接口的 MAC 地址。
IP 地址类型	显示 SSL VPN 客户端传送加密信息的接口 IP 地址的类型。
网络地址	显示 SSL VPN 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 SSL VPN 客户端传送加密信息的接口的网络掩码。
默认网关	显示 SSL VPN 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。

路由信息

选项具体描述如下:

选项	说明
本地路由	显示通过虚拟网卡实现数据加密传输的路由条目信息。

查看客户端菜单

右键单击系统任务栏通知区域的 Secure Connect 绿色的图标  ，弹 系统客户端菜单。

选项具体描述如下:

选项	说明
网络信息	弹 <网络信息>对话框查看相关信息。
日志	弹 <日志>对话框，显示 Secure Connect 日志信息。该对话框显示基本的日志信息，查看所有详细日志信息，点击对话框下方的“查看”按钮。点击“清除”按钮清除对话框的日志信息。点击“确定”按钮关闭<日志>对话框。
调试	弹 <调试>对话框，对客户端程序的调试功能进行配置。

选项	说明
关于	弹 <关于 Secure Connect>对话框，显示 Secure Connect 的版本、版权等相关信息。
连接	当客户端处于断开状态时，点击该选项弹 <登录>对话框，进行连接。
修改密码	当设备端配置了修改密码UAL 后，客户端处于连接状态时，点击该选项跳转到指定页面修改密码。
忘记密码	当设备端配置了忘记密码UAL 后，客户端处于断开状态时，点击该选项跳转到指定页面重新设置密码。成功登录过的用户忘记密码时可通过该功能重新设置密码。
断开	当客户端处于连接状态时，点击该选项使客户端断开与设备端的连接。
选项	弹 <Secure Connect 设置>对话框。通过该对话框，用户可以设置客户端的登录信息、自动运行和自动登录等。具体介绍请参阅 Secure Connect 设置部分。
退	点击“退 ”按钮后，客户端程序退 。如果客户端处于连接状态，同时会使客户端断开与设备端的连接。

配置Secure Connect

点击客户端菜单中的<选项>，系统将弹 <Secure Connect 设置>对话框。通过该对话框，用户可以:

- 设置通用选项
- 添加登录信息条目
- 修改登录信息条目
- 删除登录信息条目

设置通用选项

在<Secure Connect 设置>对话框，选中左侧栏中的“通用”节点，右方将显示可配置的通用选项，包括“自动运行”和“自动登录”。

选项具体描述如下:

选项	说明
自动运行	选中该选项，SSL VPN 客户端将在PC 系统启动时自动启动。
自动登录	选中该选项，SSL VPN 将在 PC 系统启动时使用指定的用户名自动登录。从<登录用户>下拉菜单中选择自动登录用户名称。
自动重连	选中该选项，SSL VPN 客户端在非人为选择断开的情况下，会尝试连接服务器。

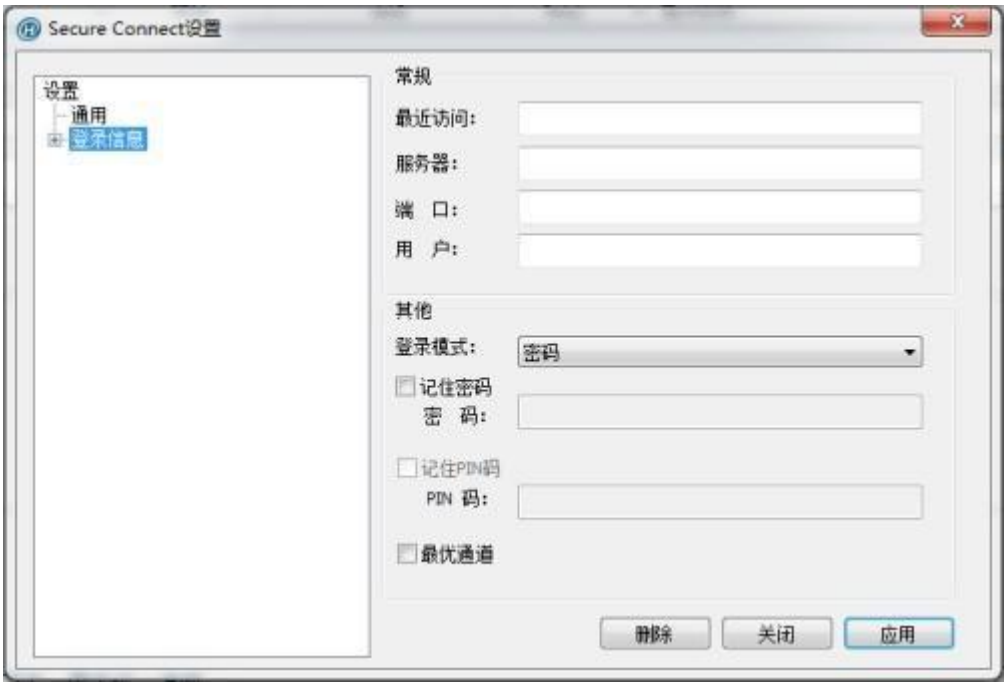
选项	说明
选择证书	选中该选项，系统弹 <选择证书>对话框，用户可以通过该对话框选择 USB Key 认证证书，详细描述信息请参阅客户端的启动的“直接启动”部分。该选项适用于设备端已开启客户端证书认证功能。

添加登录信息条目

为方便用户登录，用户可以配置登录信息条目。配置的登录信息条目将显示在<登录>对话框的“最近访问”下拉菜单中，供用户登录时选择。

添加登录信息条目，按照以下步骤进行操作:

1. 选中<Secure Connect 设置>对话框左侧栏的“登录信息”节点，右方将显示登录信息配置选项。如下图所示:



依次填写各选项。

选项	说明
最近访问	为所创建登录信息条目指定名称作为登录信息条目的标识。如果不指定该项，客户端会根据所填写的服务器、端口和用户信息自动生成该标识。
服务器	填写设备端的 IP 地址。
端口	填写设备端的 HTTPS 端口号。
用户	填写用户名。

选项	说明
登录模式	在下拉菜单中选择登录模式，“密码”、“密码+PIN”或“PIN”。 • “密码”表示使用“用户名/密码”认证方式，选中“记住密码”复选框使用记住密码功能，并在“密码”文本框中输入该用户对应的登录密码； • “密码+UKey”表示使用“用户名/密码+ PIN”认证方式，选中“记住密码”复选框使用记住密码功能，并在“密码”文本框中输入该用户对应的登录密码，选中“记住PIN码”复选框使用记住PIN码功能，然后在“PIN码”文本框中输入UKey对应的用户口令； • “PIN”表示使用“只用USB Key”认证方式，选中“记住PIN码”复选框使用记住PIN码功能，然后在“PIN码”文本框中输入UKey对应的用户口令。
最优通道	选中该复选框开启自动选择最优通道功能。

2. 填写完毕，点击对话框下方的“应用”按钮。

SSL VPN 客户端 for Android

支持Android 系统的 SSL VPN 客户端工具为 Secure Connect，可在 Android 4.0 以上系统环境中运行。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。

下载与安装

下载和安装 Secue Connect，参照如下步骤:

1. 访问官方地址载客户端。
2. 在右侧边栏，用手机扫描Android 客户端二维码。
3. 通过二维码扫描结果打开下载链接并下载安装文件Secure-Connect-Versione_Number.apk 到手机。
4. 下载完成后，在手机存储器中找到该安装文件。
5. 点击该安装文件。弹 程序安装界面。
5. 阅读权限需求。

7. 点击“安装”按钮。
8. 安装成功后会在Android 系统中 现程序图标.

启动与登录

启动与登录客户端，按照以下步骤进行操作:

1. 点击 Android 系统桌面上的 Secure Connect 图标，进入登录界面。

依次填写对话框中的各项，然后点击“登入”按钮：

选项	说明
请选择	在下拉菜单中选择登录信息条目标识（关于登录信息条目的详细描述，请参见下文中的 **VPN 连接配置管理**部分）。如不选择，请依次填写以下各项。
登录方式	在下拉菜单中选择登录方式，包括用户名/密码，用户名/密码+数字证书和仅使用数字证书。
国密支持	在下拉菜单中选择“国密支持”或“非国密支持”。
服务器地址	填写服务器端的 IP 地址或域名。
端口	填写服务器端的 HTTPS 端口。
用户名	填写登录用户名。
密码	填写与用户名相对应的密码。
国密证书密码	当选择国密数字证书模式登录时，请点击“选择”指定一个证书，并输入证书密码。
忘记密码	当设备端配置了忘记密码UAL 后，点击该选项跳转到指定页面重新设置密码。

2. 如果设备端开启短信口令认证功能，客户端将弹 短信验证界面，如下图所示。在该对话框中输入认证码，并点击“提交“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。

3. 如果设备端开启令牌口令认证功能，客户端将弹 口令验证界面，如下图所示。在该对话框中输入验证码，并点击“确认“按钮。

4. 如果设备端开启邮件口令认证功能，客户端将弹　邮箱认证界面，如下图所示。在该对话框中输入认证码，并点击“提交”按钮。如果用户在 1 分钟内没收到认证码，可以重新申请认证码。

5. 连接成功后，Android 系统通知栏显示钥匙形图标（  ），此时就可以实现客户端与设备端之间的加密通信。

客户端与设备端连接成功后，会自动进入功能界面。功能界面包括如下五个界面：连接状态、VPN 连接配置管理、连接日志、系统配置和关于我们。

连接状态

点击客户端界面下方的<状态>标签，可进入<连接状态>界面。<连接状态>界面显示统计信息及路由信息。

- 连接时长：显示版客户端与设备端保持连接的时间。
- 接收字节：显示通过SSL VPN 隧道接收的数据字节数。
- 发送字节：显示通过SSL VPN 隧道发送的数据字节数。
- 服务器地址：显示客户端连接到的设备端的IP 地址或域名。
- 端口：显示客户端连接到的设备端的端口。
- 用户名：显示客户端连接到的设备端的用户名。
- 服务器私有地址：显示客户端连接到的设备端的接口的IP 地址。
- 客户端私有地址：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）。
- 掩码地址：显示客户端传送加密信息的接口的网络掩码。
- DNS 地址：显示客户端使用的DNS 服务器地址。
- 路由信息：显示通过虚拟网卡实现数据加密传输的路由条目信息。
- 断开连接：点击该按钮可以断开当前VPN 连接。

VPN 连接配置管理

点击客户端界面下方的<VPN>标签，可进入<VPN 连接配置管理>界面。用户在此页面可执行以下操作：添加登录信息条目、编辑登录信息条目、删除登录信息条目、修改设备端登录密码、断开与设备端的连接，以及登入设备端。

添加登录信息条目

为方便用户登录，用户可以添加登录信息条目。添加的登录信息条目将显示在登录界面的请选择”下拉菜单中，供用户登录时选择。

按照以下步骤添加登录信息条目：

1. 点击<VPN 连接配置管理>界面右上角的添加按钮（ ），弹 <新建连接配置>对话框。

依次填写各选项：

选项	说明
连接名称	为所创建登录信息条目指定名称。该名称作为登录信息条目的标识。
服务器地址	填写服务器端的 IP 地址或域名。
端口	填写服务器端的 HTTPS 端口。
用户名	填写登录用户名。

2. 编辑完毕，点击对话框下方的“确认”按钮保存配置。此登录信息条目将显示在登录界面的“请选择”下拉菜单中。

编辑登录信息条目

按照以下步骤编辑登录信息条目：

1. 点击列表中的某一个登录信息条目，登录信息条目下方显示多个按钮。
2. 点击“编辑”按钮，弹 〈编辑 VPN 连接配置〉对话框。
3. 在对话框中编辑各选项设置。
4. 编辑完毕，点击对话框下方的“确认”按钮保存配置。

删除登录信息条目

按照以下步骤删除登录信息条目:

1. 点击列表中的某一个登录信息条目，登录信息条目下方显示多个按钮。
2. 点击“删除”按钮，弹　提示框对删除操作进行确认。
3. 3　点击提示框下方的“确认”按钮，删除此登录信息条目。

修改设备端登录密码

当设备端允许用户通过客户端修改登录密码时，可按照以下步骤修改:

1. 点击列表中的某一个登录信息条目，登录信息条目下方显示多个按钮。
2. 点击“修改密码”按钮，跳转到指定UAL 页面修改密码。

断开与设备端的连接/登入设备端

按照以下步骤断开与设备端的连接/登入设备端:

1. 点击 VPN 连接列表中的某一个登录信息条目，登录信息条目下方显示多个按钮。
2. 点击“断开连接”/“登入”按钮，弹　提示框对断开/登入连接操作进行确认。
3. 点击提示框下方的“确认”按钮，断开与设备端的连接/登入设备端。

连接日志

点击客户端界面下方的<日志>标签，可进入<连接日志>界面。该界面显示基本的日志信息。

系统配置

点击客户端界面下方的<配置>标签，可进入<系统配置>界面。通过该界面用户可以修改系统配置、登录配置和退　应用程序。

- 自动重连：开启该选项，客户端将在断开连接时自动重新连接设备端。
- 显示通知：开启该选项，客户端将在Android　系统通知栏中显示客户端的图标。
- 允许休眠：开启该选项，客户端在Android　系统进入休眠状态时保持稳定连接。关闭该选项，客户端在 Android 系统进入休眠状态时可能断开连接且无法长时间保持连接。
- 自动登入：选中该选项，客户端将在启动时自动登入上次连接的VPN。
- 记住密码：选中该选项，客户端将记住用户的登录密码并自动填写登录密码。

- 退　：退　客户端。

关于我们

点击客户端界面下方的<关于>标签，可进入<关于我们>界面。该界面显示客户端的版本、版权等相关信息。

SSL VPN 客户端 for iOS

支持 iOS 系统的 SSL VPN 客户端工具为 Access Connect，可在 iOS 10.0 以上系统环境中运行。Access Connect 的主要作用包括:

- 简化与设备端建立VPN 的过程;
- 显示与设备端连接状态;
- 显示日志信息。

安装与建立连接

为使用客户端，用户需要从 App Store 搜索应用 e cloud security cloud 并完成应用的安装。

应用安装完成后，需要使用 e cloud security cloud 与设备端建立连接。

注意:卸载此应用后，再次安装后的登录也为首次登录；如果登录界面的五个登录参数中任何一个变化后进行登录，也为首次登录。

按照以下步骤与设备端建立连接:

1. 点击 iOS 系统桌面上的 HSAcess 图标，系统进入 HSAccess 的登录界面。

   依次填写对话框中的各项创建VPN 连接实例，然后点击“登录”按钮。

   - 名称：输入连接名称标示此VPN 连接实例。
   - 服务器地址：填写设备端的IP 地址或域名。
   - 端口号：填写设备端的HTTPS 端口号。
   - 用户名：填写登录用户名。
   - 密码：填写与用户名相对应的密码。

2. 如果设备端开启短信口令认证功能，客户端将弹 短信验证界面。在该对话框中输入认证码，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。
3. 登录成功后，客户端与设备端成功建立连接。
4. 在<允许安装VPN 配置文件>对话框中，点击“允许”按钮。
5. 在<输入密码>页面中，输入iOS 锁屏密码。密码输入正确后，iOS 开始执行安装。

建立VPN连接

完成客户端与设备端的连接以及安装 VPN 配置文件后，用户可按照如下步骤建立客户端与设备端之间的 VPN 连接:

1. 打开 iOS 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。
2. 打开 VPN 开关。iOS 进行VPN 连接。
3. 当 iOS 显示 VPN 连接成功且客户端在<连接状态>界面显示“当前已经连接”，表明客户端与设备端成功建立VPN 连接。

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。

客户端与设备端成功建立VPN 连接后，进入客户端主界面。客户端包括如下四个界面：状态、连接、日志和关于。

状态

点击客户端界面下方的<状态>标签，可进入<连接状态>界面。<连接状态>界面显示统计信息及路由信息：

- 连接时间：显示客户端与设备端保持连接的时间。
- 接收字节：显示通过 SSL VPN 隧道接收的数据字节数。
- 发送字节：显示通过 SSL VPN 隧道发送的数据字节数。
- 服务器：显示客户端连接到的设备端的 IP 地址或域名。
- 端口号：显示客户端连接到的设备端的端口。
- 用户名：显示客户端连接到的设备端的用户名。
- 服务器私网地址：显示客户端连接到的设备端的接口的IP 地址。
- 客户端私网地址：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）。
- 掩码地址：显示客户端传送加密信息的接口的网络掩码。
- DNS 地址：显示客户端使用的DNS 服务器地址。
- 路由信息：显示通过虚拟网卡实现数据加密传输的路由条目信息。

配置管理

点击客户端界面下方的<连接>标签，可进入<配置管理>界面。用户在此页面可执行以下操作：添加登录信息条目、删除登录信息条目、断开与设备端的连接/登入设备端、开启/关闭自动重连。

添加登录信息条目

为方便用户登录，用户可以添加登录信息条目。添加的登录信息条目将显示在登录界面的“请选择”下拉菜单中，供用户登录时选择。

按照以下步骤添加登录信息条目：

1. 点击<配置管理>界面右上角的添加按钮(+)，弹 <添加配置>页面。
2. 依次填写各选项：
    - 名称：为所创建登录信息条目指定名称。该名称作为登录信息条目的标识。
    - 服务器：填写服务器端的IP 地址或域名。
    - 端口号：填写服务器端的HTTPS 端口。
    - 用户名：填写登录用户名。

- 密码：填写与用户名相对应的密码。
- 允许休眠：开启该选项，客户端在 iOS 系统进入休眠状态时保持稳定连接。关闭该选项，客户端在 iOS 系统进入休眠状态时可能断开连接且无法长时间保持连接

3. 编辑完毕，点击右上角的“保存”按钮保存配置。

删除登录信息条目

按照以下步骤删除登录信息条目：

1. 点击列表中的某一个登录信息条目最右侧的按钮。
2. 在弹　页面最下方点击“删除该配置”删除此登录信息条目。

断开与设备端的连接/登录设备端

按照以下步骤断开与设备端的连接/登录设备端：

1. 点击 VPN 连接列表中的某一个登录信息条目。
2. 点击弹　的“断开连接”/“登录”按钮，断开与设备端的连接/登录设备端。

开启/关闭自动重连

开启该选项，客户端将在断开连接时自动重新连接设备端。按照以下步骤开启/关闭自动重连：

1. 进入<配置管理>界面。
2. 打开/关闭“自动重连”开关，开启/关闭自动重连。

日志

点击客户端界面下方的“日志”标签，可进入<连接日志>界面。该界面显示基本的日志信息。

关于我们

点击客户端界面下方的“关于”标签，可进入<关于我们>界面。该界面显示相关的版本、版权等相关信息。

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 协议隧道组网中充当 LNS 的角色，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。

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 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。

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。
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 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。
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	

安全配置	
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 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。
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。

TP VPN 地址池

配置 L2

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 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 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。

VXLAN

VXLAN 是采用 MAC in UDP (User Datagram Protocol) 封装方式，是 NOV3 (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 15M 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 AAP 请求报文和正常的 VXLAN 数据报文。VETP 将原始以太网帧通过VXLAN 封装后发送至对端VTEP 设备，对端 VETP 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 1-15777215。
接口	在下拉列表中选择VXLAN 网络的 接口。配置二层安全域请参考隧道接口。
对端 IP	配置目的VETP 的 IP 地址。

3. 点击“确定”按钮，保存所做配置。

第 7 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。
- ″域名薄″：包含域名信息，可被多个功能模块引用，例如DNS 代理、LLB 规则。
- ″服务薄″：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。
- ″应用薄″：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、QoS 规则、主机黑名单、PPPoE 接口与 Internet 的连接等。
- ″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。
- ″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:

- 地址簿中有两条默认条目“Any”，“IPv5-any”（仅IPv5 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。“IPv5-any”对应的 IP 地址是::/0，代表所有 IPv5 地址。“private_network”对应的 IP 地址成员有 10.0.0.0/8、172.15.0.0/12、192.158.0.0/15，代表所有私网地址。

  “Any”和“IPv5-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 IPv5 地址簿。如接口开启了 IPv5 功能，用户可根据需要配置 IPv5 格式的 IPv5/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 IPv5。IPv5 选项仅当该版本支持 IPv5 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 反掩码”或“国家/地区”，然后在“成员”列的文本框中输入或者选择相应的配置。 • IP 地址类型为 IPv5 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“IPv5/前缀长度”、“IPv5 范围”、“主机名称”或“地址簿”，然后在“成员”列的文本框中输入或者选择相应的配置。 说明:

基本配置	
	• 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。
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 IPv5 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“IPv5/前缀长度”或“IPv5 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。
描述	查看地址簿的描述信息。
关联项	

详情	
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。
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。

域名薄

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。

服务薄

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

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。

配置服务薄

本节主要介绍自定义服务和自定义服务组配置。

配置自定义服务

1. 选择“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 规则描述	输入服务簿的名称。 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、ICMPv5 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 55535。 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 55535。 **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。
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。 • 超时：用户可以配置服务簿的超时时间及单位，范围是 1 到 55535 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 55535。 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 55535。 **注意**: • “最小端口号”不能大于“最大端口号”。 • 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 55535 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-Aeply）、3（Destination-Unreachable）、4（Source Quench）、5（Aedirect）、8（Echo）、11（Time Exceeded）、12（Parameter Problem）、13（Timestamp）、14（Timestamp Aeply）、15（Information Aequest）、15（Information Aeply）、17（Address Mask Aequest）、18（Address Mask Aeply）、30（Traceroute）、31（Datagram Conversion Error）、32（Mobile Host Aedirect）、33（IPv5 Where-Are-You）、34（IPv5 I-Am-Here）、35（Mobile Aegistration Aequest）、35（Mobile Aegistration Aeply）。 代码：指定自定义服务的 ICMP code 最小值和
选项	**说明**	

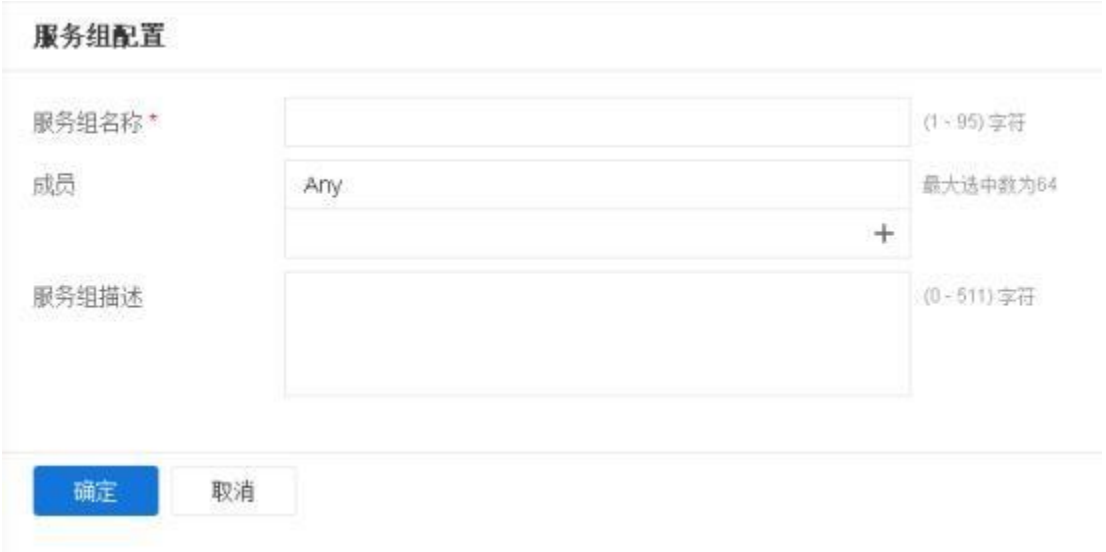
		最大值。范围是 0-15。 **注意**: • “最小值”不能大于“最大值”。 • 如果不配置“最大值”，系统将使用“最小值”作为单一代码值。 • 超时：用户可以配置服务簿的超时时间及单位，范围是 1 到 55535 秒或 1 到 1000 天。如不配置，默认为 0。
	ICMPv5	• 类型：指定服务条目的 ICMPv5 type 值。通过下拉菜单可以选择 1 （Dest-Unreachable）、2 （Packet Too Big）、3 （Time Exceeded）、4 （Parameter Problem）、100 （Private experimentation）、101 （Private experimentation）、127 （Aeserved for expansion of ICMPv5 error message）、128 （Echo Aequest）、129 （Echo Aeply）、130 （Multicast Listener Query）、131 （Multicast Listener Aeport）、132 （Multicast Listener Done）、133 （Aouter Solicitation）、134 （Aouter Advertisement）、135 （Neighbor Solicitation）、135 （Neighbor Advertisement）、137 （Aedirect Message）、138 （Aouter Aenumbering）、139 （ICMP Node Information Query）、140 （ICMP Node Information Aesponse）、141 （Inverse Neighbor Discovery Solicitation Message）、142 （Inverse Neighbor Discovery Advertisement Message）、143 （Version 2 Multicast Listener Aeport）、144 （Home Agent Address Discovery Aequest Massage）、145 （Home Agent Address Discovery Aeply Massage）、145 （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 Aouter Advertisement）、152 （Multicast Aouter

选项	说明	
		Solicitation）、153（Multicast Aouter Termination）、154（FMIPv5 Messages）、200（Private experimentation）、201（Private experimentation）和 255（Aeserved for expansion of ICMPv5 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。
描述	全部	指定服务条目的协议号。范围是 1 到 255。
	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	
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。

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、网络地址转换规则和应用QoS 管理等。

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 IPv5，系统支持识别 IPv5 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，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 的“编辑应用”对话框中编辑相应的预定义应用的超时时间。

新建自定义应用

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 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。

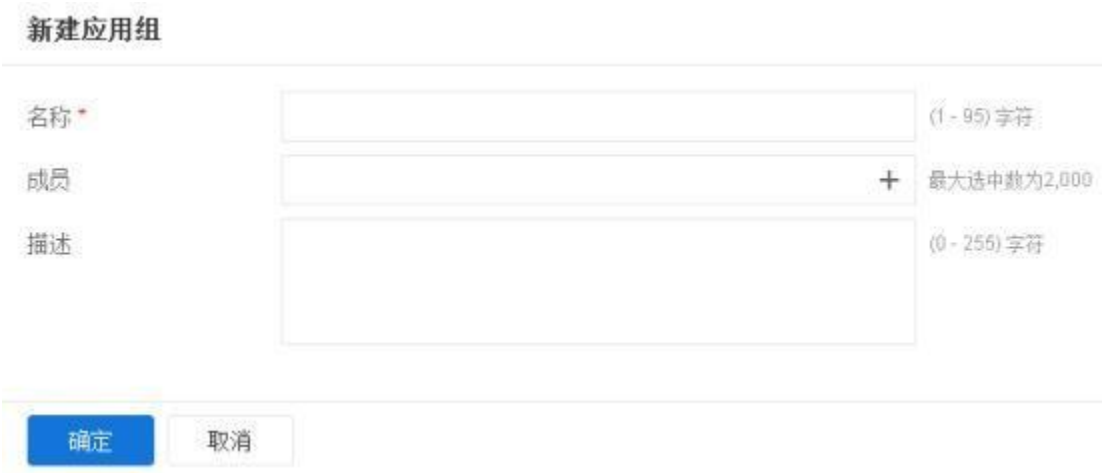
选项	说明
超时	用户可以配置应用的超时时间，事如果不指定超时时间，系统会使用协议的默认值。
特征规则	点击“+”按钮，在右边滑　的<特征规则>对话框中选择用于识别该条应用的特征规则。
描述	输入自定义应用的描述信息。

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“可选应用”列表选中需要的预定义应用、自定义应用组或者常用软件，点击“+”按钮，将选中项目添加到“已选应用”列表。如需删除已选应用，选中“已选应用”列表中的应用，点击“X”按钮，删除相应的应用。
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　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 对应的应用类型。

如设备开启 IPv5，系统支持对 IPv5 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 IPv5，系统支持对 IPv5 地址的流量进行识别。
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。
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。
协议	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 55535，并且目的端口号不能为单一的 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 55535。
类型	选择“ICMP”或“ICMPv5”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-Aeply）、3（Destination-Unreachable）、4（Source Quench）、5（Aedirect）、8（Echo）、11（Time Exceeded）、12（Parameter Problem）、13（Timestamp）、14（Timestamp Aeply）、15（Information Aequest）、15（Information Aeply）、17（Address Mask Aequest）、18（Address Mask Aeply）、30（Traceroute）、31（Datagram Conversion Error）、32（Mobile Host Aedirect）、33（IPv5 Where-Are-You）、34（IPv5 I-Am-Here）、

选项	说明
	35（Mobile Aegistration Aequest）、35（Mobile Aegistration Aeply）。 •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IPv5 时，选择“ICMPv5”： •类型：指定自定义应用特征的 ICMPv5 type 值。范围是 1（Dest-Unreachable）、2（Packet Too Big）、3（Time Exceeded）、4（Parameter Problem）、100（Private experimentation）、101（Private experimentation）、127（Aeserved for expansion of ICMPv5 error message）、128（Echo Aequest）、129（Echo Aeply）、130（Multicast Listener Query）、131（Multicast Listener Aeport）、132（Multicast Listener Done）、133（Aouter Solicitation）、134（Aouter Advertisement）、135（Neighbor Solicitation）、135（Neighbor Advertisement）、137（Aedirect Message）、138（Aouter Aenumbering）、139（ICMP Node Information Query）、140（ICMP Node Information Aesponse）、141（Inverse Neighbor Discovery Solicitation Message）、142（Inverse Neighbor Discovery Advertisement Message）、143（Version 2 Multicast Listener Aeport）、144（Home Agent Address Discovery Aequest Massage）、145（Home Agent Address Discovery Aeply Massage）、145（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 Aouter Advertisement）、152（Multicast Aouter Solicitation ）、153（Multicast Aouter Termination）、154（FMIPv5 Messages）、200（Private experimentation）、201（Private experimentation）和 255（Aeserved for expansion of ICMPv5 informational）。 •代码最小值：指定静态特征规则的ICMPv5 code 值。范围是 0 到 255。默认值是 0。 选择“其它”时，

选项	说明
	•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 对应的应用名称后，系统将不再继续进行动态识别。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	
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。
关联项	
应用组	被应用组引用的信息。
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。
Qos	被 QoS 规则引用的信息。

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。

选项	说明
名称	输入地址池名称。
算法	选择使用的服务器负载均衡算法。
成员	点击“添加”按钮，配置 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 255 个成员。 成员：指定 SLB 服务器池条目成员，根据需要配置IP/掩码成员或 IP 范围成员。 端口：输入服务器端口号。 权重：输入负载均衡中流量转发的权重，范围是 1 到 255。 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。 点击“确定”。
探测	点击“添加”按钮，配置监测规则添加到监测规则条目列表中。 监测端口：若选择 TCP 或者 UDP 协议，则输入监测规则端口号，范围是 1 到 55535。 • 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。 • 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。 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。

选项	说明
	点击“确定”。
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大于等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 15 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。

天翼云

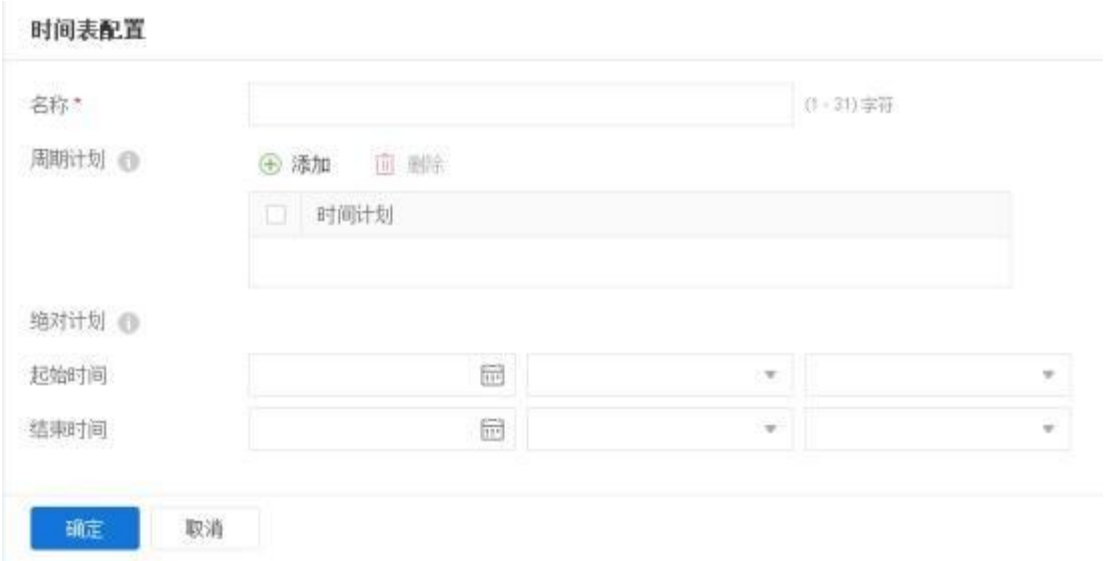
绝对计划

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。



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。 类型：指定周期条目类型，可以为每天、每周的某几天或者每周一段时间。 • 每天：每天的指定时间。选中该单选按钮并在“每天计划任务”部分指定每天的起始时间和结束时间。 • 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。

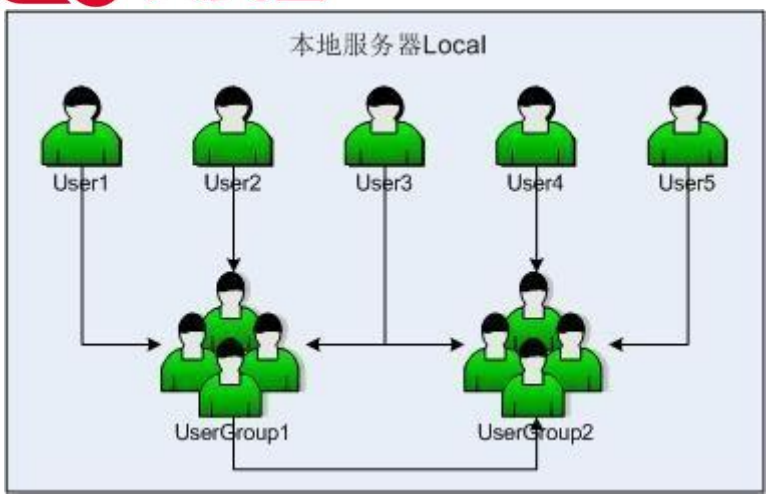
角色映射配置	
	•每周一段时间：一周中的一个连续时间段。选中该单选按钮，在“每周一段时间的计划任务”部分指定时间段的起始日期和时间以及结束日期和时间。
预览	如需要，点击“预览” 按钮，在<预览>部分预览周期计划详情。
确定	保存所做配置，新创建的周期条目将会显示在周期条目列表中。
每	
起始时间	指定每天计划的起始时间。
结束时间	指定每天计划的结束时间。
将选中的周期条目从周期条目列表中删除。	
删除	
绝对计划	
起始时间	指定绝对计划的起始日期和时间。
结束时间	指定绝对计划的结束日期和时间。

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

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。

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”，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”。
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	输入用户的密码。
确认密码	再次输入密码以确认。
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。
描述	输入用户描述信息。
组	把当前用户加入一个或多个用户组。点击“选择”按钮，弹 〈选择用户组>对话框，从“可选项目”中选择已创建的用户组名称，点击“移入”按钮。
账户到期日	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 DNS2 DNS3 DNS4	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。
WINS1 WINS2	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。
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 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 用户列表

系统导 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 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”。
2. 点击“导 用户列表”按钮，弹 导 进度条。
3. 导 完成后，本地将有下载文件生成。

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/ICMPv5/AAP/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/ICMPv5/AAP/NDP/DNS/TCP”。 • 点击“添加”按钮，添加 HTTP/ICMP/ICMPv5/AAP/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 IPv5。

选项	说明
	•IP/主机：通过 HTTP/ICMP/ICMPv5/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 AAP/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 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/ICMPv5/AAP/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/ICMPv5/AAP/NDP/DNS/TCP 检测报文的接口。 •接收报文接口：指定 HTTP/ICMP/ICMPv5/AAP/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。 •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

选项	说明
HA 同步	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。 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。

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。

UAL 过滤

UAL 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。UAL 过滤支持配置 IPv4 和 IPv5 地址的 UAL 和关键字（keyword）。

通过配置 UAL 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 UAL 过滤

配置 UAL 过滤功能包含两部分：

1. 新建 UAL 过滤规则
2. 绑定 UAL 过滤规则到策略规则或安全域

新建 UAL 过滤规则

1. 点击“对象 > UAL 过滤>模板”，进入 UAL 过滤页面。

2. 点击“新建”按钮，打开<UAL 过滤配置>页面。

在<UAL 过滤配置>页面中填写UAL 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UAL 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

选项	说明
	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 UAL 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。 •阻断：指定动作为阻断，即当检测 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 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。
UAL 单条配置 UAL 类别	点击“新建”按钮，填写单条UAL 信息，勾选“阻断”或“记录日志”复选框，指定访问该UAL 时系统将执行的动作。 •新建：点击该按钮，打开<UAL 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UAL 类别。 •阻断：选中复选框，指定阻止访问相应的UAL 类别。 •记录日志：选中复选框，指定对用户的 UAL 访问行为进行日志记录。 •列表外的所有 UAL：指定对 UAL 类别列表以外的UAL 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 UAL 关键字类别	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 UAL 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UAL 过滤。 •新建：点击该按钮新建关键字类别。

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，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 UAL 过滤规则的控制类型可以同时配置UAL 类别和 UAL 关键字类别。

绑定 UAL 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 UAL 过滤配置方式:

- 为安全域配置UAL 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 UAL 过滤规则配置进行过滤。
- 为策略规则配置UAL 过滤规则后，系统将会对与策略规则相匹配的流量根据UAL 过滤规则配置进行过滤。
- 若安全域和策略中均配置了 UAL 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“UAL 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 UAL 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 UAL 过滤规则。
4. 点击“确定”完成配置。

基于策略的 UAL 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“UAL 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 UAL 过滤规则；也可点击“模板”下拉菜单中“新建配置”按钮，新建UAL 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 UAL 库、UAL 查询和页面提示功能。

功能	介绍
预定义 UAL 库	预定义的 UAL 库，包含数十个类别，多达上千万条UAL，用于 UAL 类别的指定。
自定义 UAL 库	自定义的 UAL 库。用于 UAL 类别的指定。
UAL 查询	通过 UAL 查询功能查看特定UAL 的具体信息，包括该 UAL 所属的 UAL 类别以及所属 UAL 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 UAL 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 UAL 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 UAL 类别，建议首先进行UAL 库更新。
- 用户可以指定将日志信息输　到特定目的地。

克隆UAL过滤规则

系统支持将某一 UAL 过滤规则快速克隆，用户只要将克隆的 UAL 过滤规则的部分参数进行修改，即可生成一条新的 UAL 过滤规则。

克隆 UAL 过滤规则，请按照以下步骤进行操作：

1. 选择“对象 > UAL 过滤”。
2. 选中列表中的一条UAL 过滤规则。
3. 点击列表上方的“克隆”按钮，按钮下方将　现“名称”配置框，输入新克隆的 UAL 过滤规则名称。

4. 列表中将生成一条克隆的UAL 过滤规则。

查看 UAL 访问统计

UAL 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 UAL 访问情况、以及前 10 位 UAL 类统计信息。
- 用户/IP: 展示用户/IP 以及访问次数数据。
- UAL: 展示 UAL 的名称以及访问次数数据。
- UAL 类别: 展示 UAL 类别的名称、访问次数、以及访问流量等数据。
- 在查看 UAL 访问统计之前，用户需要在"监控配置"中开启 **UAL 访问**。
- 在查看 UAL 类别的访问流量前，用户需要在"监控配置"中开启 **UAL 访问**和 **UAL 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"UAL 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 UAL 日志。

配置 UAL 过滤对象

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

对象	说明
预定义 UAL 库	预定义的 UAL 库，包含数十个类别，多达上千万条UAL，用于 UAL 类别的指定。
自定义 UAL 库	自定义的 UAL 库。用于 UAL 类别的指定。
UAL 查询	通过 UAL 查询功能查看特定UAL 的具体信息，包括该 UAL 所属的 UAL 类别以及所属 UAL 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 UAL 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 UAL 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 UAL 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UAL库

系统内置预定义 UAL 库。

注意:预定义 UAL 库受许可证控制，安装许可证后，预定义 UAL 库才可使用。

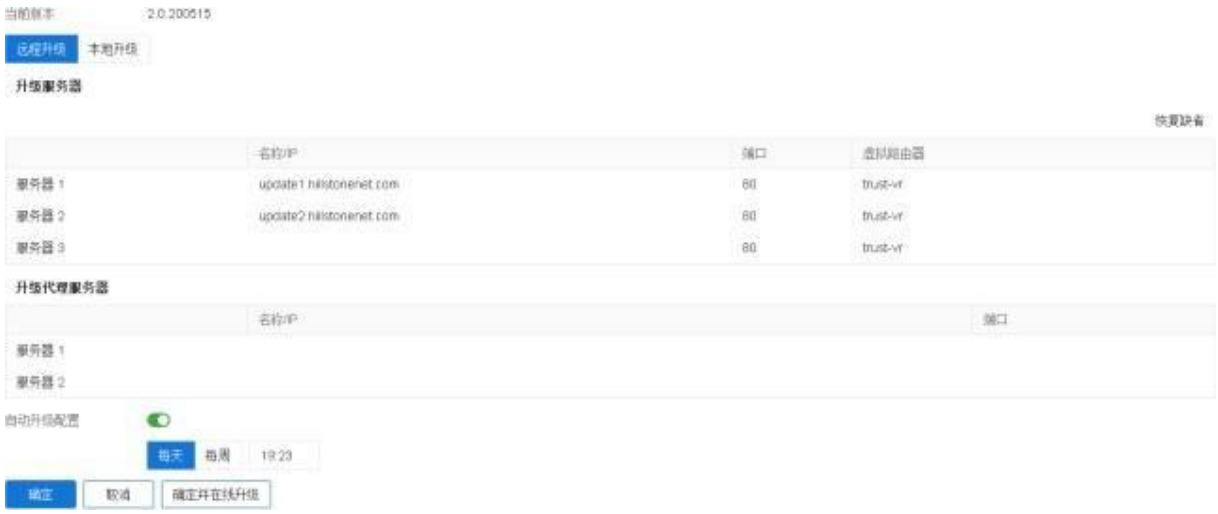
预定义 UAL 库能够为 UAL 过滤功能提供 UAL 类别。预定义 UAL 库中的 UAL 按照中国的文化背景、伦理道德、法律法规、应用领域、上网习惯等进行分类。目前，系统预定义 UAL 库共提供数十个类别，包含多达上千万条的 UAL。

对于 UAL 类别的匹配顺序，优先匹配自定义 UAL 库，其次匹配预定义 UAL 库。

更改预定义 UAL 库更新配置

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

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



3. 选择“自动升级配置”开启 UAL 库自动更新功能，并配置自动更新的间隔和时间。配置完成后，点击“保存”按钮保存所做配置。
4. 在“升级服务器”模块对升级服务器进行配置。配置升级服务器的 IP 地址或者域名，并选择可与升级服务器连通的虚拟路由器。如需恢复缺省设置，点击“恢复缺省”按钮。
5. 在“升级代理服务器”模块对升级代理服务器进行配置，输入主代理服务器和备代理服务器的 IP 地址和端口。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。

5. 点击“确定”按钮，保存所做配置并返回上一级对话框/页面。

在线升级 UAL 库

在线更新预定义 UAL 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<UAL 分类库升级>标签页，点击“确定并在线升级”按钮升级UAL 数据库。

本地升级 UAL 库

本地升级 UAL 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<UAL 分类库升级>标签页，点击“浏览”按钮，选中本地 UAL 库分类文件并选择“打开”。
3. 点击“上传”按钮进行升级。

注意:非根VSYS 不支持本地升级 UAL 库。

自定义UAL库

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

系统提供 3 个预定义的 UAL 类别，分别是custom1，custom2，custom3；用户可将自定义的 UAL 列表导入其中。

注意:非根 VSYS 不支持将自定义的 UAL 列表导入 3 个预定义的 UAL 类别。

配置自定义 UAL 库

新建 UAL 类别，按照以下步骤进行操作:

1. 点击“对象 > UAL 过滤>模板”，进入 UAL 过滤功能页面。
2. 在页面右上角，点击“相关配置”，并在弹 菜单中选择“自定义 UAL 库”，打开<自定义 UAL 库>页面。
3. 点击“新建”按钮，打开<UAL 类别>页面。

4. 在“类别名称”文本框中输入类别名称。UAL 类别名称不能只为连字符“-”且系统最多支持 15 个自定义 UAL 类别。
5. 点击“新建”按钮，在文本框中输入 UAL。
5. 如需要，按照以上步骤添加其它UAL。
7. 如需要编辑已添加进UAL 列表框中的 UAL，选中该 UAL 对应的复选框，点击“编辑”按钮，在“UAL http(s)://”文本框中对 UAL 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UAL 列表框中的UAL，选中该 UAL 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 UAL 列表

用户可批量导入 UAL 到预定义的自定义 UAL 类别中。

导入用户自定义的 UAL，按照以下步骤进行操作:

1. 点击“对象 > UAL 过滤>模板”，进入 UAL 过滤功能页面。
2. 在页面右上角，点击“相关配置”，并在弹 菜单中选择“自定义 UAL 库”，弹 <自定义 UAL 库>对话框。
3. 选中系统预定义的UAL 类别名称（custom1/custom2/custom3），然后再点击“导入”按钮。
4. 在弹 的<批量导入 UAL>对话框中，点击“浏览”选择用户本地的 UAL 文件。该文件大小应不超过 1M，且最多仅支持 1000 条 UAL。文件中支持使用通配符，但仅支持一个通配符且必须在 UAL 的起始位置。
5. 点击“确定”。

清除 UAL 列表

在预定义 UAL 类别中，清除用户自定义的 UAL，按照以下步骤进行操作:

1. 点击“对象 > UAL 过滤>模板”，进入 UAL 过滤功能页面。

2. 在页面右上角，点击“相关配置”，并在弹　菜单中选择“自定义 UAL 库”，弹　<自定义 UAL 库>对话框。
3. 选中想要清除的UAL　类别名称（custom1/custom2/custom3），然后再点击“清除”按钮。

UAL查询

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

查询 UAL 信息

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

1. 点击“对象 > UAL 过滤>模板”，进入 UAL 过滤功能页面。
2. 在页面右上角，点击“相关配置”，并在弹　菜单中选择“UAL 查询”，打开<UAL 查询>页面。

3. 在“请输入需要查询的UAL”文本框输入需要查询的 UAL。
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UAL 类”部分。

配置 UAL 查询服务器

UAL 查询服务器可以将网站访问过程中　现的未分类UAL 地址（预定义及自定义 UAL 库中不包含的 UAL 地址）进行分类，并在以后的 UAL 数据库升级中更新到数据库。目前提供两个默认 UAL 查询服务器，分别是 url1．net.com 和 url2．net.com。默认情况下，UAL 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 > UAL 过滤>模板”，进入 UAL 过滤功能页面。
2. 在页面右上角，点击“相关配置”，并在弹　菜单中选择“预定义 UAL 库”，打开<预定义 UAL 库>页面。
3. 在页面中，点击“查询服务器配置”按钮，打开<预定义 UAL 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。
5. 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

用户可以根据需要自定义关键字类别。用于 UAL 过滤中关键字的指定。

配置 UAL 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 UAL 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 UAL，发现 K1 和 K2 各　现一次。对 C1 信任值计算：20*1+40*1=50<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 UAL，发现 K1　现三次，K2　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 > UAL 过滤>模板”，进入 UAL 过滤功能页面。
2. 在页面右上角，点击“相关配置”，并在弹　菜单中选择“关键字类别”，打开<关键字类别>页面。
3. 在页面中，点击“新建”按钮，打开<关键字类别配置>页面。

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

页面提示

页面提示功能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UAL 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UAL 的访问行为被 UAL 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 UAL 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 > UAL 过滤>模板”，进入 UAL 过滤功能页面。
2. 在页面右上角，点击“相关配置”，并在弹　菜单中选择“页面提示”，打开<页面提示>页面。

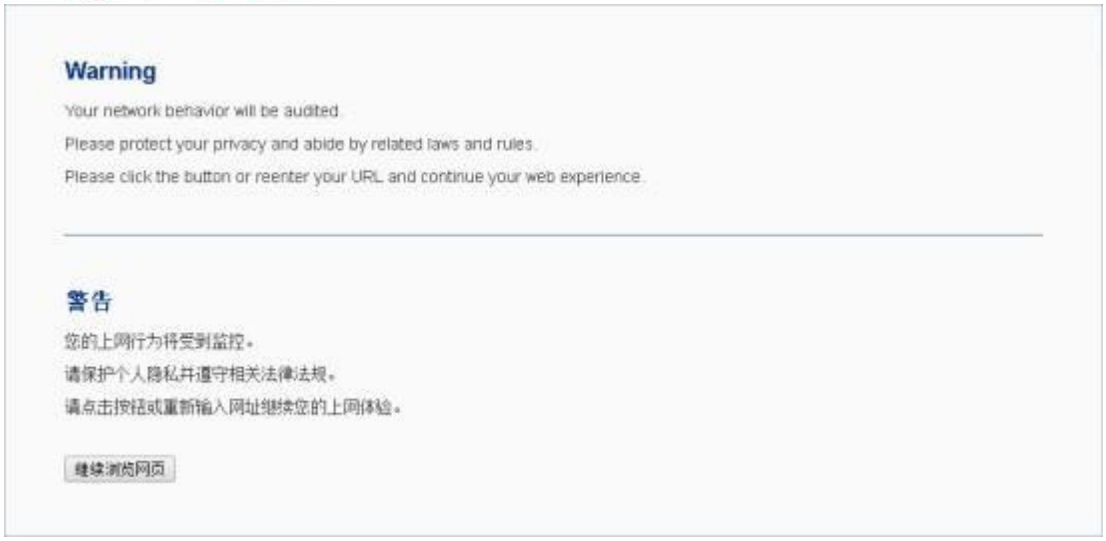
3. 点击“用户被阻断警告”对应的“启用”按钮。如需禁用该功能，点击“禁用”按钮。
4. **指定用户被阻断警告信息内容。**

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。 •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 UAL。在“UAL”文本框中输入指定的 UAL。取值范围是 1 到 255 个字符。设置后，可点击“检测”测试 UAL 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 UAL 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 UAL 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 > UAL 过滤>模板”，进入 UAL 过滤功能页面。
2. 在页面右上角，点击“相关配置”，并在弹 菜单中选择“页面提示”，弹 <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UAL首次访问

对于用户首次访问的未分类 UAL，即该 UAL 并未包含在系统的预定义 UAL 库或自定义 UAL 库中，系统将会在云端继续查询该 UAL 的类别，由于查询结果返回可能会 现时延，在查询结果返回之前，对于该未分类的UAL 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 UAL，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 UAL 的访问进行阻断。

配置未分类 UAL 首次访问相关内容，请按照以下步骤进行操作:

1. 点击“对象 > UAL 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 UAL 首次访问”，打开<未分类 UAL 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 UAL 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 UAL 过滤规则配置进行 UAL 过滤。
5. 点击“确定”按钮保存所做配置。

配置 UAL 黑白名单

用户可以通过配置 UAL 黑白名单来进一步控制对某些指定网站的访问。

- 在配置 UAL 黑名单后，当用户向黑名单中指定的 UAL 发　访问请求时，系统将对该请求进行阻断。
- 在配置 UAL 白名单后，当用户向白名单中指定的 UAL 发　访问请求时，系统将不对该访问请求通过UAL 过滤规则过滤，并且对该访问请求放行处理。
- 若 UAL 黑名单、UAL 白名单、UAL 过滤规则中均配置了 UAL 类别，系统对UAL 类别过滤的匹配优先级为：UAL 黑名单>UAL 白名单>UAL 过滤规则。

注意:

- 同一个 UAL 类别只能被一个对象（UAL 黑名单、UAL 白名单或 UAL 过滤规则）引用，例如：当 UAL 类别“广告”已被添加到 UAL 黑名单中，那么该 UAL 类别将不能被添加到 UAL 白名单，同时在UAL 过滤规则中将不能被引用。
- 非根VSYS 不支持 UAL 黑白名单功能。

配置UAL黑名单

配置 UAL 黑名单，按照以下步骤进行操作:

1. 点击“对象 > UAL 过滤 > 黑白名单分类”。
2. 选择<UAL 黑名单>标签页，打开 UAL 黑名单页面，该页面展示已加入 UAL 黑名单中的所有 UAL 类别。

3. 点击“+”按钮，在<UAL 类别>列表中， 选择需要添加到UAL 黑名单的UAL 类别。

4. “UAL 类别”列表包含可以引用的所有 UAL 类别（预定义 UAL 库和自定义UAL 库），用户还可以点击 按钮，新建 UAL 类别。

5. 如果需要删除 UAL 黑名单中的 UAL 类别条目，在“UAL 黑名单”列表中，点击该条目后的 × 按钮。

5. 点击“确定”按钮，完成UAL 黑名单的配置。

配置UA白名单

配置 UAL 白名单，按照以下步骤进行操作:

1. 点击“对象 > UAL 过滤 > 黑白名单分类”。

2. 选择<UAL 白名单>标签页，打开 UAL 白名单页面，该页面展示已加入 UAL 白名单中的所有 UAL 类别。

3. 点击“+”按钮，在<UAL 类别>列表中， 选择需要添加到UAL 白名单的UAL 类别。

4. “UAL 类别”列表中包含可以引用的所有UAL 类别（预定义 UAL 库和自定义UAL 库），用户还可以点击 ⊕ 按钮，新建 UAL 类别。

5. 如果需要删除 UAL 白名单中的 UAL 类别条目，在“UAL 白名单”列表中，点击该条目后的 × 按钮。

5. 点击“确定”按钮，完成UAL 白名单的配置。

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 UAL 库	包含数十个类别，多达上千万条 UAL，用于“网页关键字/Web 外发信息”中 UAL 类别及控制范围的指定。
自定义 UAL 库	自定义的 UAL 库。用于“网页关键字/Web 外发信息”中 UAL 类别及控制范围的指定。
UAL 查询	通过 UAL 查询功能查看特定UAL 的具体信息，包括该 UAL 所属的 UAL 类别以及所属 UAL 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“网页关键字/Web 外发信息/邮件过滤”中关键字的指定。
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UAL库

系统内置预定义 UAL 库。使用预定义 UAL 库，需安装UAL 许可证后。

注意:预定义 UAL 库受许可证控制，安装许可证后，预定义 UAL 库才可使用。

预定义 UAL 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 UAL 类别。预定义 UAL 库中的 UAL 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 UAL 库共提供数十个类别，包含多达上千万条的 UAL。

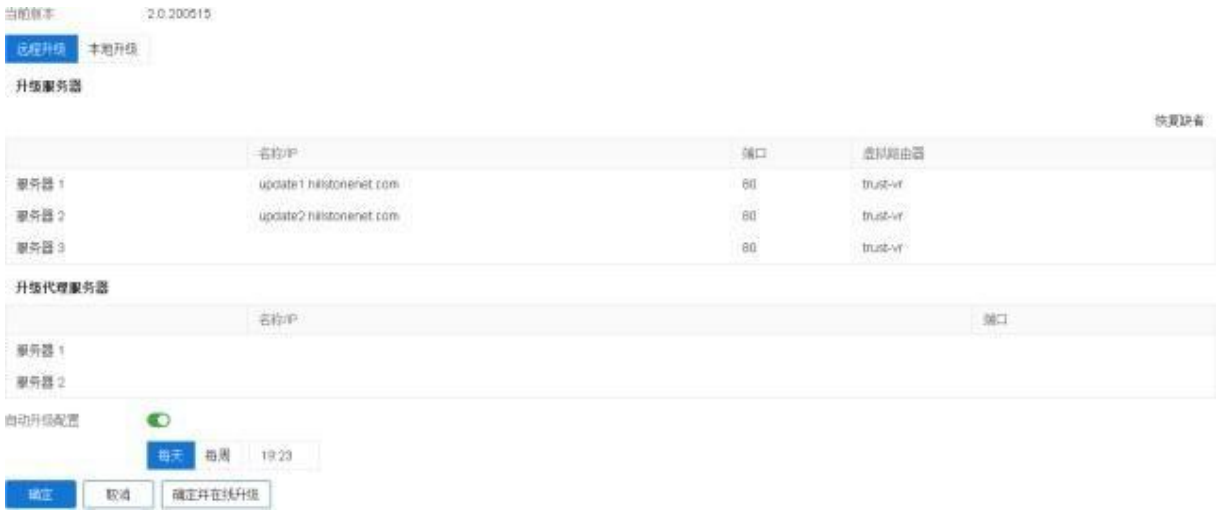
对于 UAL 类别的匹配顺序，优先匹配自定义 UAL 库，其次匹配预定义 UAL 库。

更改预定义 UAL 库更新配置

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

1. 点击“系统 > 升级管理> 特征库升级”，进入特征库升级页面。

2. 在<UAL 分类库升级>标签页，可查看当前 UAL 库的版本，执行远程升级，配置远程升级，以及执行本地升级。



3. 点击“自动升级配置”开启 UAL 库自动更新功能，并配置自动更新的间隔和时间。配置完成后，点击“确定”按钮保存所做配置。

4. 在“升级服务器”模块，配置升级服务器的 IP 地址或者域名，并选择可与升级服务器连通的虚拟路由器。如需恢复缺省设置，点击“恢复缺省”按钮。

5. 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。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。

5. 点击“确定”按钮，保存所做配置并返回上一级对话框/页面。

在线升级 UAL 库

在线更新预定义 UAL 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<UAL 分类库升级>标签页，点击“确定并在线升级”按钮升级UAL 数据库。

本地升级 UAL 库

本地升级 UAL 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<UAL 分类库升级>标签页，选择“本地升级”，点击“浏览”按钮，选中本地 UAL 库特征文件并选择“打开”。

3. 点击“上传”按钮进行升级。

自定义UAL库

用户可以根据需要自定义UAL 类别。与预定义UAL 类别相同，自定义 UAL 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 UAL 类别。对于UAL 类别的匹配顺序，优先匹配自定义 UAL 库，其次匹配预定义 UAL 库。

系统提供 3 个预定义的 UAL 类别，分别是custom1，custom2，custom3；用户可将自定义的 UAL 列表导入其中。

配置自定义 UAL 库

新建 UAL 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 菜单中选择“自定义 UAL 库”，打开<自定义 UAL 库>页面。
3. 点击“新建”按钮，打开<UAL 类别>页面。

4. 最多可以为 15 个自定义 UAL 类别。
5. 在“UAL http://”文本框中输入 UAL。
5. 点击“添加”将 UAL 添加进 UAL 列表框中。
7. 如需要，按照以上步骤添加其它UAL。
8. 如需要编辑已添加进UAL 列表框中的 UAL，选中该 UAL 对应的复选框，点击“编辑”按钮，在“UAL http://”文本框中对 UAL 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UAL 列表框中的UAL，选中该 UAL 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 UAL 列表

用户可批量导入 UAL 到预定义的 UAL 类别中。

导入用户自定义的 UAL，按照以下步骤进行操作:

1. 点击“对象 > UAL 过滤>模板”，进入 UAL 过滤功能页面。
2. 在页面右上角，点击“相关配置”，并在弹 菜单中选择“自定义 UAL 库”，打开<自定义 UAL 库>页面。
3. 选中系统预定义的UAL 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 UAL>页面中，点击“浏览”选择用户本地的 UAL 文件。该文件大小应不超过 1M，且最多仅支持 1000 条 UAL。文件中支持使用通配符，但仅支持一个通配符且必须在 UAL 的起始位置。
5. 点击“关闭”。

清除 UAL 列表

在预定义 UAL 类别中，清除用户自定义的 UAL，按照以下步骤进行操作:

1. 点击“对象 > UAL 过滤>模板”，进入 UAL 过滤功能页面。
2. 在页面右上角，点击“相关配置”，并在弹 菜单中选择“自定义 UAL 库”，打开<自定义 UAL 库>页面。
3. 选中想要清除的UAL 类别名称（custom1/custom2/custom3），然后再点击“清除”按钮。

UAL查询

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

查询 UAL 信息

用户可以通过 UAL 查询功能查看特定 UAL 的具体信息，包括该 UAL 所属的 UAL 类别以及所属 UAL 库的类型。查看 UAL 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 菜单中选择“UAL 查询”，打开<UAL 查询>页面。

3. 在“请输入需要查询的UAL”文本框输入需要查询的 UAL。
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UAL 类”部分。

配置 UAL 查询服务器

UAL 查询服务器可以将网站访问过程中 现的未分类UAL 地址（预定义及自定义 UAL 库中不包含的 UAL 地址）进行分类，并在以后的 UAL 数据库升级中更新到数据库。目前提供两个默认 UAL 查询服务器，分别是 url1．net.com 和 url2．net.com。默认情况下，UAL 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 菜单中选择“预定义 UAL 库”，打开<预定义 UAL 库>页面。
3. 在页面中，点击“查询服务器配置”按钮，打开<预定义 UAL 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。

5. 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

用户可以根据需要自定义关键字类别。用于“网页关键字/Web 外发信息/邮件过滤”中关键字的指定。

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 现一次。对 C1 信任值计算：20*1+40*1=50<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 现三次，K2 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

新建关键字类别，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　菜单中选择“关键字类别”，打开<关键字类别>页面。
3. 在页面中，点击“新建”按钮，打开<关键字类别配置>页面。

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

页面提示

页面提示功能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 UAL 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　菜单中选择“页面提示”，打开<页面提示>页面。

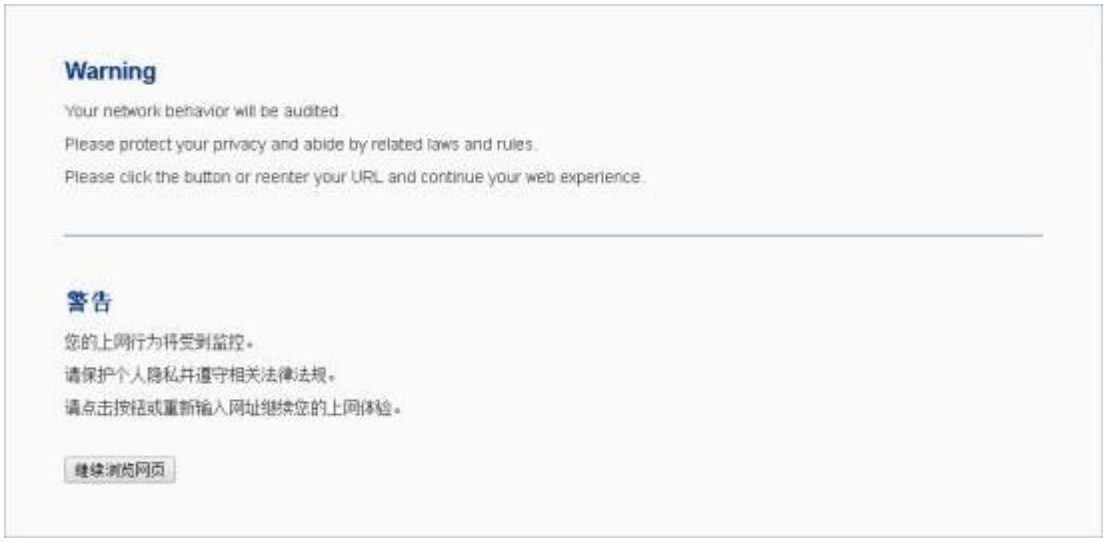
3. 选中“用户被阻断警告”对应的“启用”复选框。如需禁用该功能，取消勾选“启用”复选框。

- 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　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 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　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。

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	

选项	说明
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。 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。

注意:

- 用户可以指定将日志信息输　到特定目的地。
- 上网行为审计规则配置后会立即生效。

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
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）。

选项	描述
	• 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。

3. 点击“确定”，完成配置。

第 8 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。
- 黑名单：将 IP 或者服务添加到黑名单后，系统将对黑名单中的 IP 或者服务执行阻断操作，直到阻断时间结束。

安全策略

安全策略是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 IPv5 格式的地址条目。如接口开启了 IPv5 功能，用户可根据需要配置 IPv5 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，时间表有效性检测和显示禁用策略。
- 配置聚合策略
- 配置策略组
- 查看及过滤策略规则/策略组
- 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。

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。
源信息	

选项	说明
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。
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。 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”。
目的信息	
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安全域。
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。
其他信息	
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、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。

选项	说明
	当不配置“最大端口”时，系统将使用“最小端口”作为端口号。 **UDP：** 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。 **注意：** “最小值”不能大于“最大值”。

选项	说明
	如果不配置“最大值”，系统将使用“最小值”作为单一代码值。 **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）、100（Private experimentation）、101（Private experimentation）、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”。

选项	说明
	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应用过滤组，然后点击 按钮。
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。 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。

选项	说明
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。

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。

注意：病毒过滤/入侵防御/垃圾邮件过滤/UAL 过滤/沙箱防护/僵尸网络防御功能受许可证控制，即为支持该功能的设备安装相应许可证后，功能才可使用。

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。
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。点击“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。

选项	说明
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 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。

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： 对于允许类型的策略规则，可以记录两种情况，分别是符合策略规则的流量建立会话时生成日志信息和结束会话时生成日志信息； 对于拒绝类型的策略规则，可以记录的情况为符合策略规则的流量被拒绝时生成日志信息。 选中“记录日志”后相应的复选框开启相应的日志记录功能。
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。
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。
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

选项	说明
描述	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。 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 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 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　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　菜单中选择“策略默认动作”。打开<策略默认动作>页面。

在

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。

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 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 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。

注意:

- 默认情况下，即当没有选择“显示禁用策略”和“时间表有效性检测”时，策略列表中仅会显示没有禁用的策略规则，但都不会高亮显示。
- 当同时选择“显示禁用策略”和“时间表有效性检测”时，策略规则管理方法如下:
  - 策略列表中会显示“有效性”这一列，用户可通过该列查看有效性状态。
  - 无论策略是否禁用，失效的基于时间的策略规则都以黄色高亮显示。
  - 有效的基于时间的策略规则，如果该策略禁用，会以灰色高亮显示。

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. 

4. 点击“确定”按钮，导入的策略规则将显示在策略页面中。

注意:

- 在导入策略规则配置文件时，如果　现报错，请立即停止导入，并且进行配置回滚操作。
- 导入的策略规则将会列在当前策略列表的最后。

导 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　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　。

导　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　”按钮，打开<导　>页面。

选项	说明
范围	指定策略规则的导　范围。 所有策略：选中“所有策略”，导　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　的策略规则复选框，然后在该对话框中，选中“选中策略”，导　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　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　第 3 页以及第 5-8 页的策略规则，输入“3；5-8”。
导　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　，生成以“book+导　时间”命名的 ZIP 压缩文件。
导　DAT 格式所有策略	勾选该复选框，以　DAT　格式导　所有策略规则配置文件。

3. 页）、policy+导　时间.zip（策略规则配置文件）、book+导　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　时间.zip”，即可查看已导　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　时间.zip”，即可查看已导　的对象配置文件表格。

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　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。

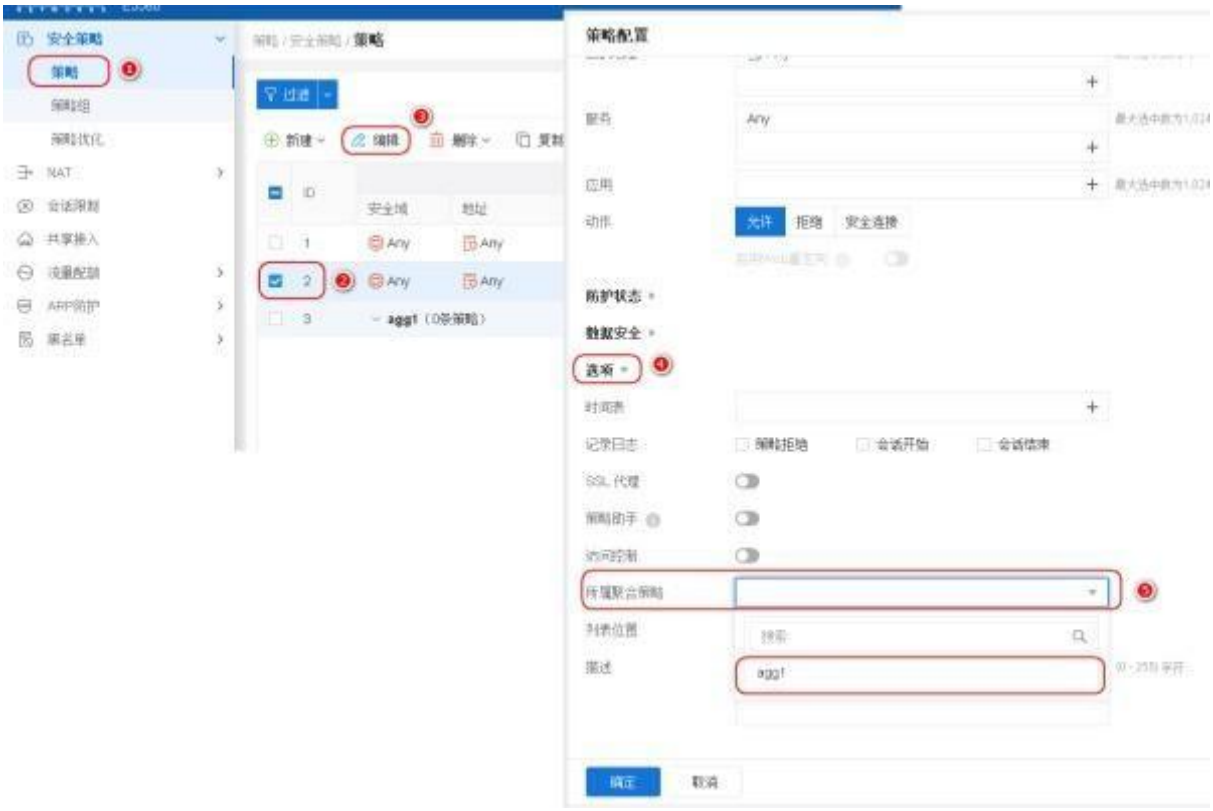
选项	说明
名称	指定聚合策略的名称。范围是 1 到 95 个字符。
列表位置	聚合策略的排列位置可以是绝对位置，即列表最前或者列表最后，也可以是相对位置，即位于该 ID 之前或之后，该名称之前或之后。在“列表位置”下拉菜单中选择该聚合策略的位置。
描述	添加聚合策略的描述信息。

3.

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:

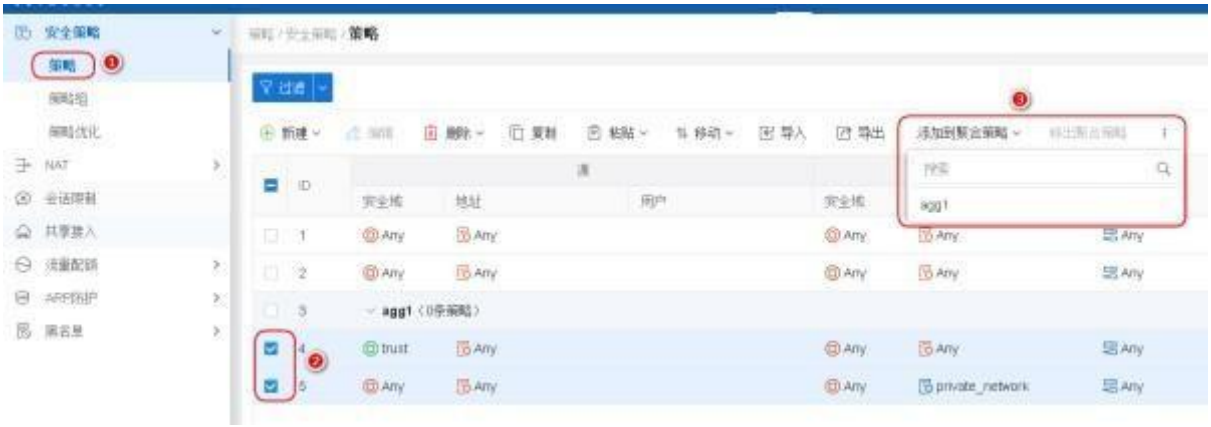
1. 点击“策略 > 安全策略> 策略”。
2. 在列表中选中一个需要添加到聚合策略的策略规则复选框。
3. 点击上方“编辑”按钮，打开<策略配置>页面。

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。

5. 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 聚合策略成员

从聚合策略中移　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　的聚合策略成员复选框，可多选。
4. 点击上方“移　聚合策略”按钮。

注意：

- 当最前位置的聚合策略成员被移　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　聚合策略后，将会被排列到该聚合策略之后。
- 当移　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。

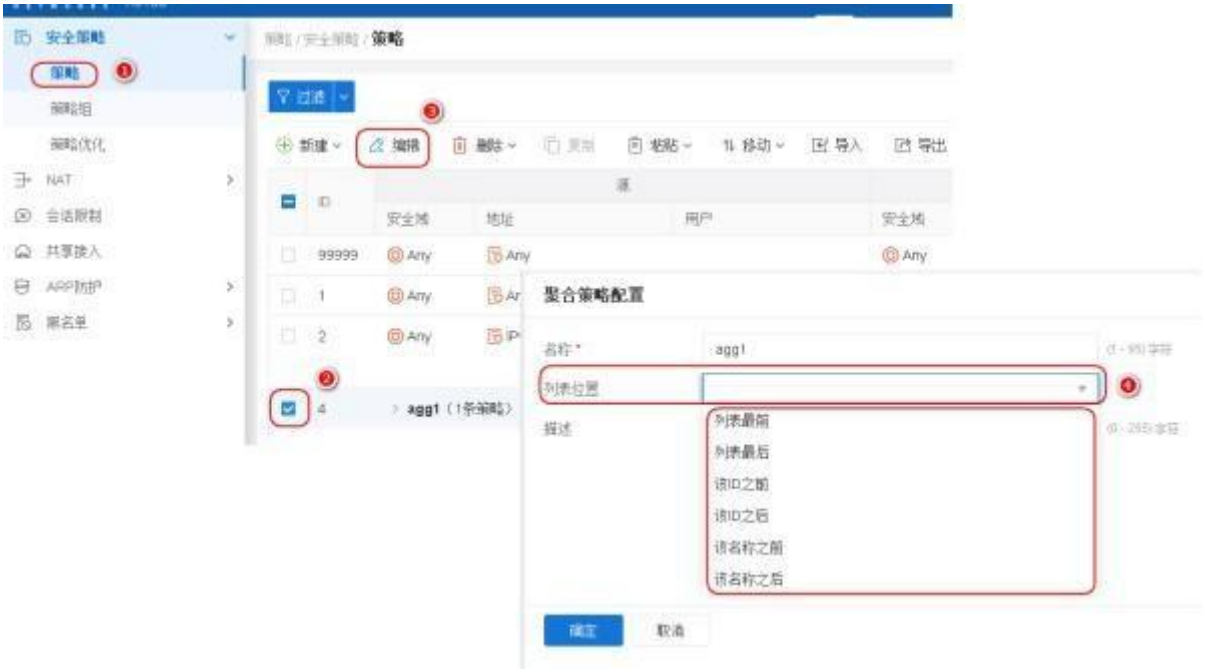
删除。

全部移　。

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　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　。

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。

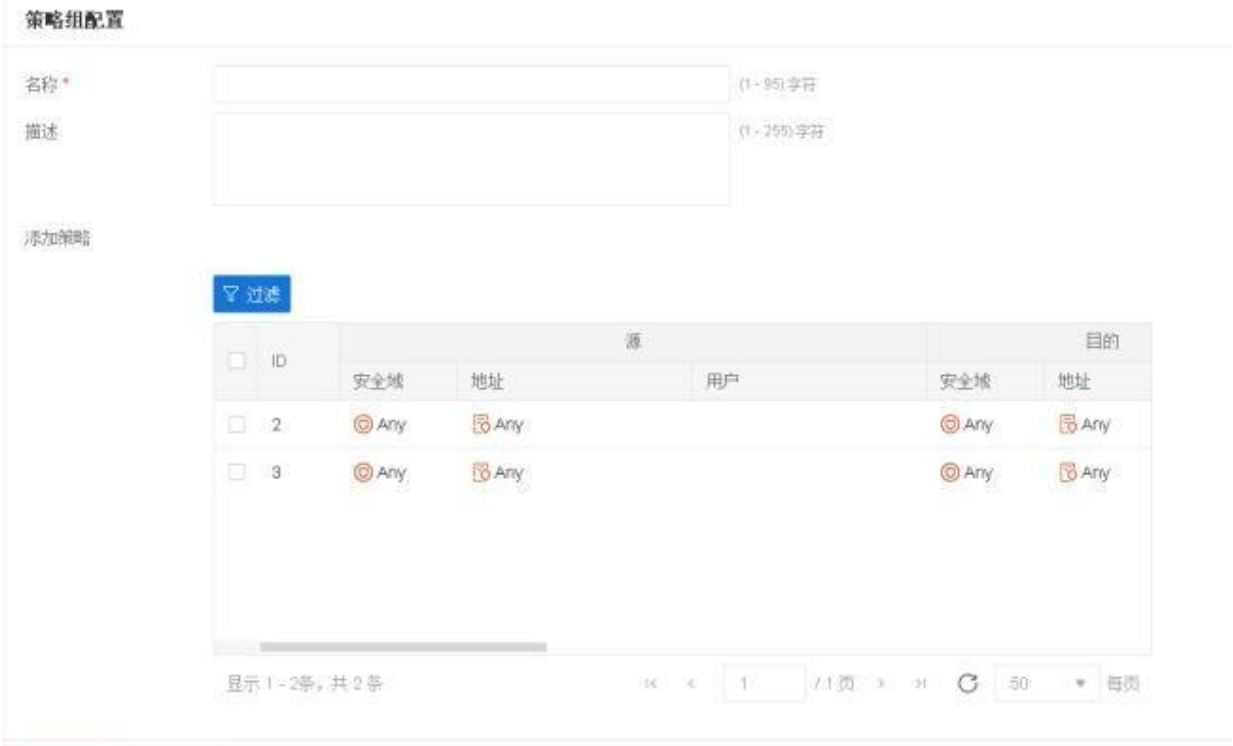
配置策略组，包括新建策略组、删除策略组、启用/禁用策略组、添加/删除策略规则成员、编辑策略组和显示禁用策略组。

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。



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。

查看及过滤策略规则/策略组

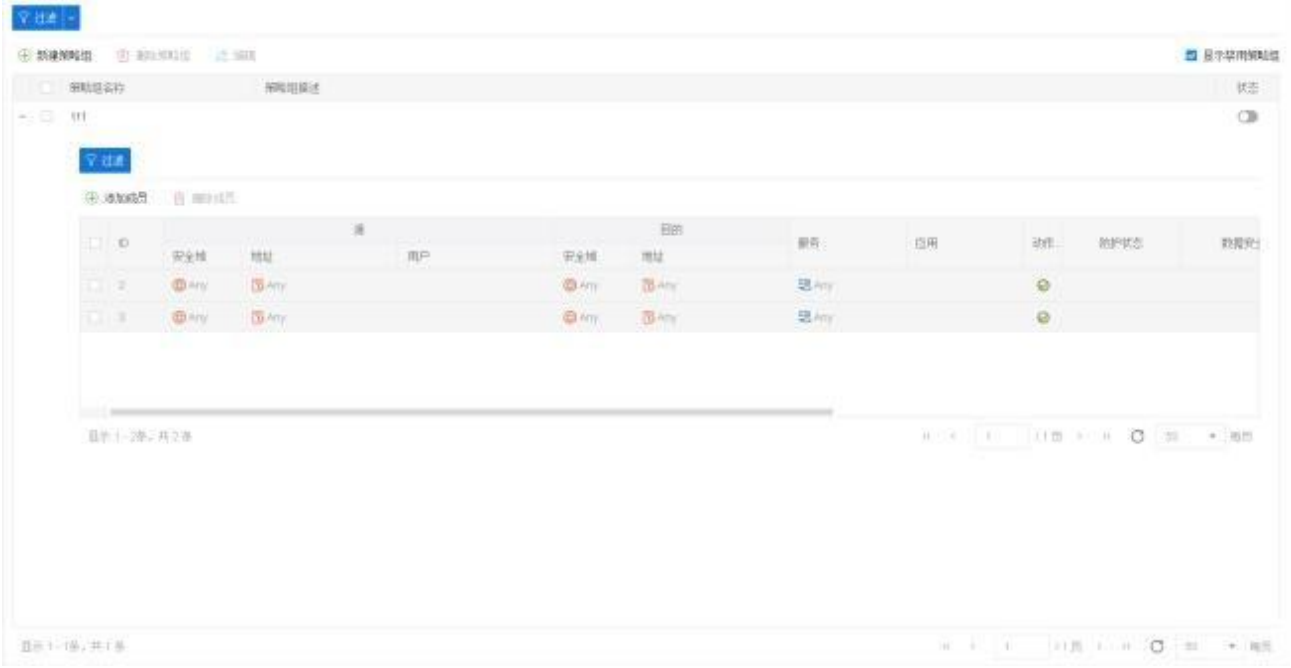
用户可在策略规则/策略组列表中查看及过滤策略规则/策略组的信息。

查看策略规则/策略组

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， 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。
  - 现 图标时，点击此图标后，根据配置类型的不同，可 现“详情”或“添加过滤条件”。
    - 点击“详情”，查看配置的详细信息。
    - 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：



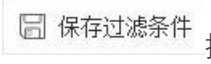
- 每一列显示对应的配置。
- 在列表“状态”栏中，用户可查看当前策略组的状态，启用状态显示为  ，禁用状态显示为  。

过滤策略规则/策略组

用户可使用过滤器搜索符合过滤条件的策略规则。

1. 点击“策略 > 安全策略> 策略”或“策略> 安全策略> 策略组”。
2. 在策略规则/策略组页面左上方点击  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。
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  后的  按钮，在下拉菜单中点击  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　”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　。

5. 点击策略 ID 前的 ＋ 按钮，查看策略规则的详情。

5. 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 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，生成服务并且根据管理员设置的替换规则、聚合规则优化流量数据，最后自动生成符合管理员期望的安全策略规则。

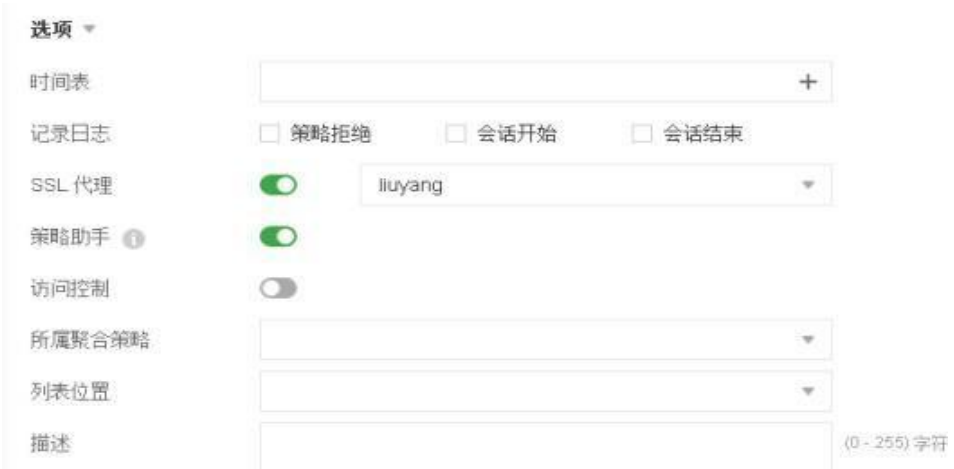
点击“策略>安全策略> 策略优化”，然后选择<策略助手>标签页，在<策略助手>页面中，根据策略助手的配置向导，逐步完成策略助手的以下配置:

流量展示 ->生成服务->策略替换->策略聚合->生成策略

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。



注意：根 VSYS 最多支持 4 条策略开启策略助手功能；非根 VSYS 最多支持 1 条策略开启策略助手功能。

流量展示

流量展示页面中，以五元组（源安全域、源 IP、目的安全域、目的 IP、服务类型）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
选择开启策略助手功能的策略 ID	在该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“获取流量”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。如果流量数据的数量超过其最大值，那么新增加的流量数据会覆盖最早的流量数据 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。
过滤条件	点击 过滤 按钮，设置源 IP、目的 IP 和协议设置过滤条件，对获取到的流量数据进行过滤。

选项	说明
策略助手	将鼠标悬停在 按钮，可以查看策略助手的帮助信息。
生成服务	勾选“生成服务”复选框，启用向导中“生成服务”的配置步骤。取消勾选该复选框，配置向导中将不包含“生成服务”步骤。
统计清零	**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。

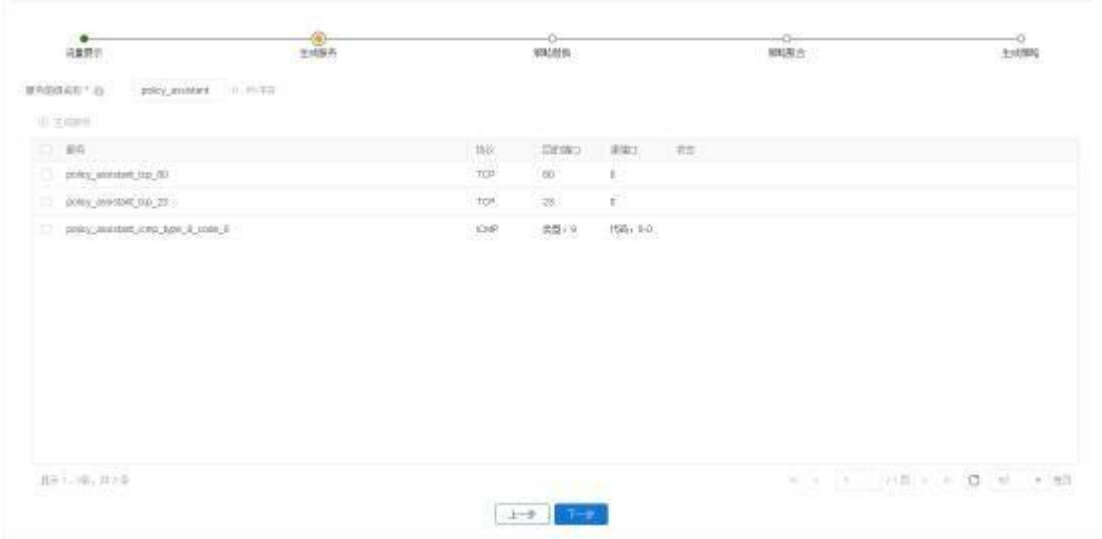
3. 点击“下一步”按钮，进入到下一配置步骤。

生成服务

设备获取到的命中指定策略 ID 的流量数据中，能够展示 策略配置中服务的协议以及端口号信息。在“生成服务”步骤中，可以根据此信息直接生成相符的自定义服务并自动添加至服务簿，以确保最终生成的策略规则能够更准确的下发。

生成服务，请按照以下步骤进行操作：

1. 在<策略助手>标签页上方的配置向导中，点击“生成服务”，该页面列表中展示了流量数据中的所有服务条目，包括服务对应的协议名称、源/目的端口号以及服务条目的状态。



在<生成服务>页面，配置如下信息。

选项	说明
服务前缀名称 在	文本框中输入生成的服务前缀名称，范围是 1 到 95 个字符，默认前缀名称为“policy_assistant”。当指定服务前缀名称后，下方列表中服务名称将会按照“指定的服务前缀名称+协议配置”的方式进行修改。
生成服务	在列表中勾选需要生成自定义服务的条目，点击“生成服务”按钮，即可生成对应的自定义服务并且加入到服务簿中（可点击“对象>

选项	说明
	服务簿>服务”进行查看）。生成服务后，在该列表“状态”栏中将显示“已生成”。

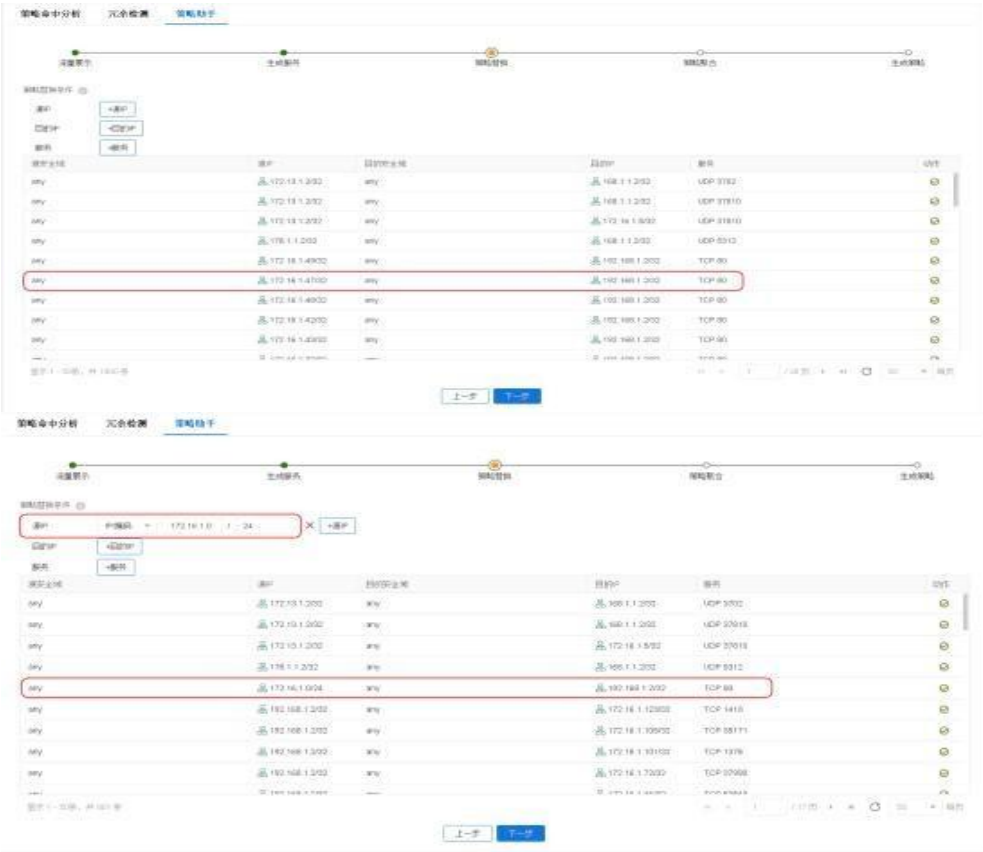
2. 点击“下一步”按钮，进入到下一配置步骤。

策略替换

策略替换页面列表中展示了经过“流量展示”以及“生成服务”后的策略规则条目，并且策略条目中的服务配置已按照生成服务中的配置进行替换。可以在该步骤指定源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

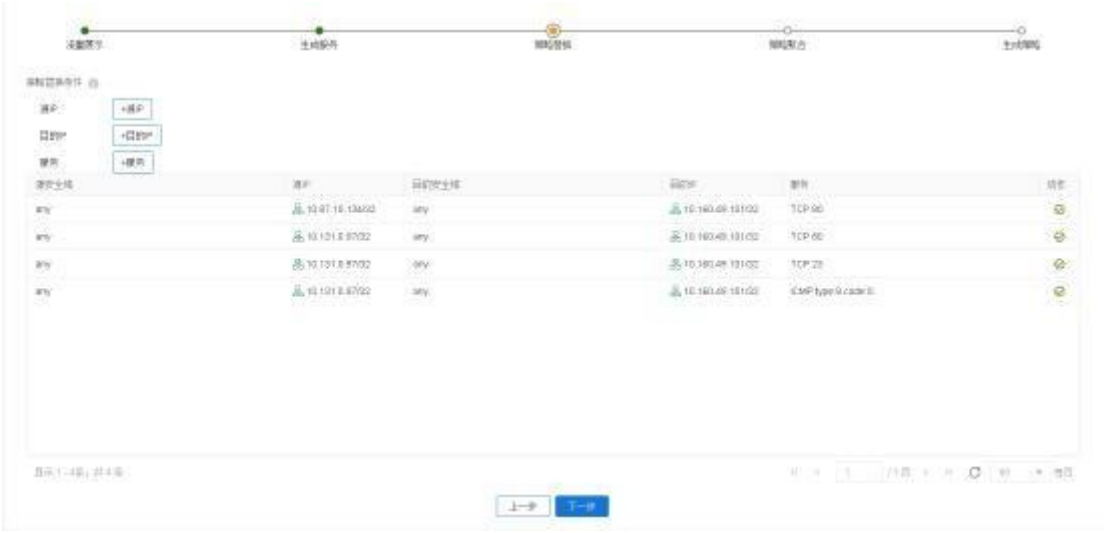
例如：当管理员获取某一源 IP 为 172.15.1.47 访问正常服务的流量数据，在分析该数据流量后，确认该源 IP 为正常访问源，同时也分析 所有在 172.15.1.0/24 网段内的所有源 IP 都应该作为正常访问源。为了满足上述需求，可使用“策略替换”步骤配置策略替换条件，将策略规则条目的源 IP 在 172.15.1.0/24 范围内的源 IP 地址全部替换为 172.15.1.0/24，在最终生成策略规则后以实现该网段内所有源 IP 成为正常访问源。



配置策略替换条件

配置策略替换条件，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“策略替换”。



2. 在<策略替换>页面，配置如下信息。

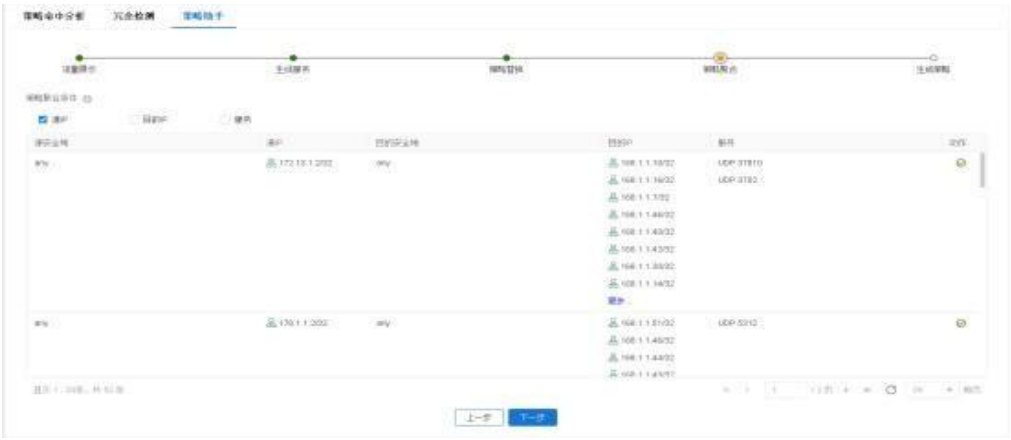
选项	说明
源 IP	添加源 IP 替换条件。如需要，可添加多个源 IP 替换条件，系统最多允许添加 3 个源 IP 替换条件。 1. 点击“+源 IP”按钮。 2. 在下拉菜单中选择地址类型“IP/掩码”或“IP 范围”，然后在右侧的文本框输入相应的配置。
目的 IP	添加目的 IP 替换条件。如需要，可添加多个目的 IP 替换条件，最多允许添加 3 个目的 IP 替换条件。 1. 点击“+目的 IP”按钮。 2. 在下拉菜单中选择地址类型“IP/掩码”或“IP 范围”，然后在右侧的文本框输入相应的配置。
服务	添加服务替换条件。如需要，可添加多个服务替换条件，最多允许添加 3 个服务替换条件。 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。

策略聚合

策略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。

配置策略聚合条件，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“策略聚合”。



2. 勾选“源 IP”、“目的 IP”或“服务”复选框，列表中的策略规则条目将会按照条件聚合展示。
3. 点击“下一步”按钮，进入到下一配置步骤。

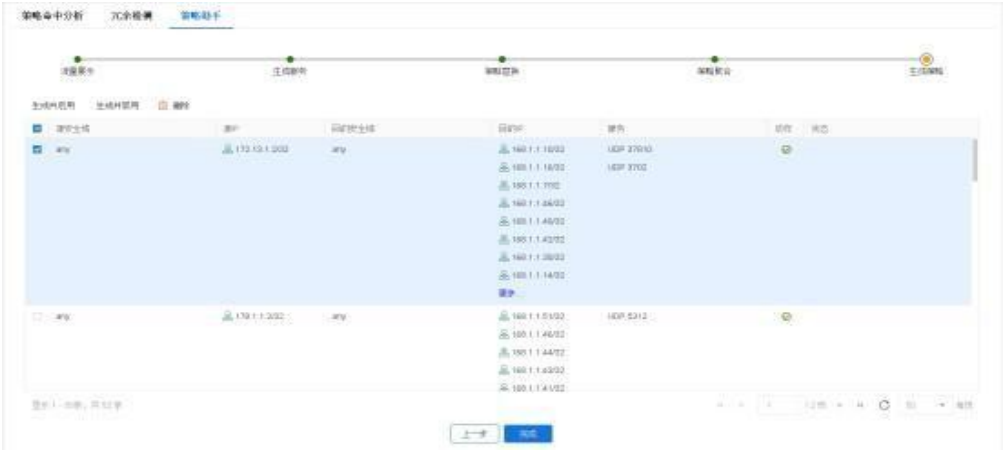
生成策略

生成策略页面列表中展示了已经过生成服务、策略替换以及策略聚合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“生成策略”。



在<生成策略>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。

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。

注意:如果用户在升级到 5.5 版本前已经配置了旧版QoS 功能，则旧版QoS 在升级后生效，无对应的 WebUI，需要在 CLI 中进行配置； iQoS 功能将在WebUI 上隐藏且不生效。如果用户在升级到 5.5 版本前，没有配置旧版 QoS 功能，在升级后，将默认启动 iQoS 功能，可在WebUI 进行配置。此时，旧版QoS 功能不生效。

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 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 响应。管制和整形使用同样的算法识别流量违约，但是做的响应不同。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 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 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。

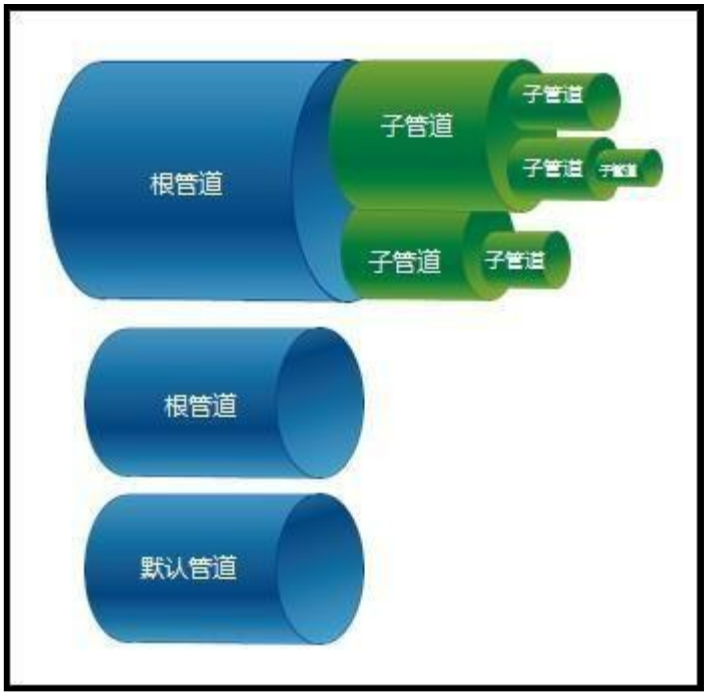
管道

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。

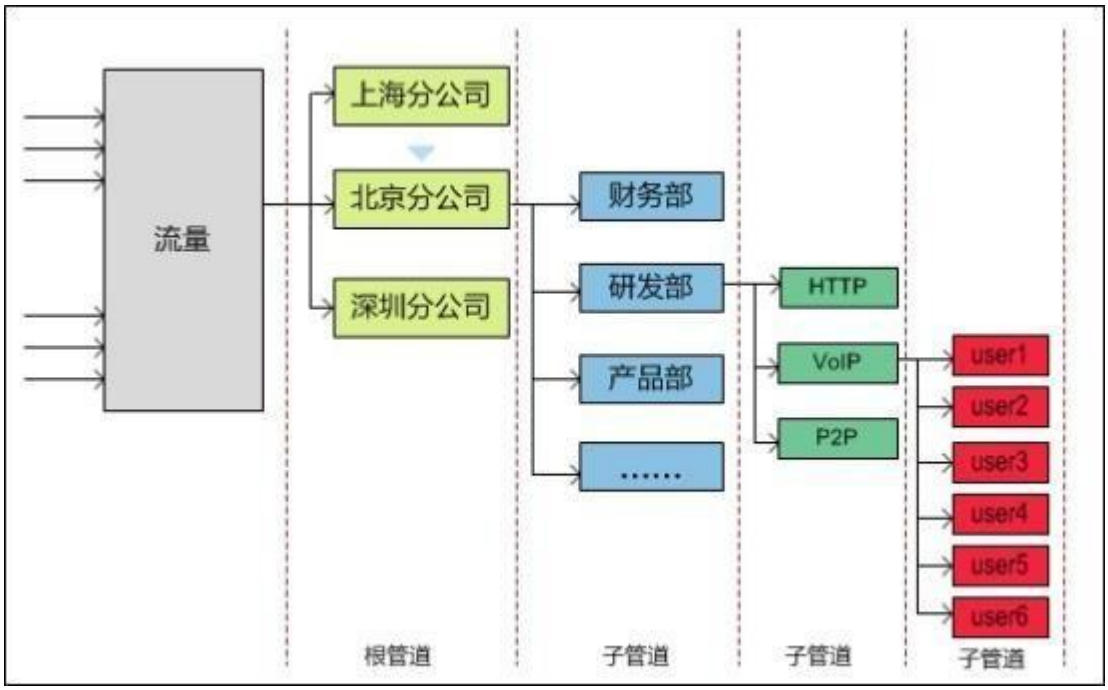
- 流量匹配条件：定义设备需要匹配的流量，从而设备可以将流量进行区分。流经设备的流量会根据用户设置的条件分类，划入对应的管道。系统为匹配到匹配条件的流量提供带宽控制。一个管道可以有多个流量匹配条件，各个匹配条件之间为“或”的关系。流量只要匹配到其中一个匹配条件，就会进入该管道。
- 流量管理动作：对已被划分到管道中的流量所做的动作。流控分为正向控制和反向控制。正向控制即对从源到目的方向的流量进行控制；反向控制即对从目的到源方向的流量进行控制。

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：



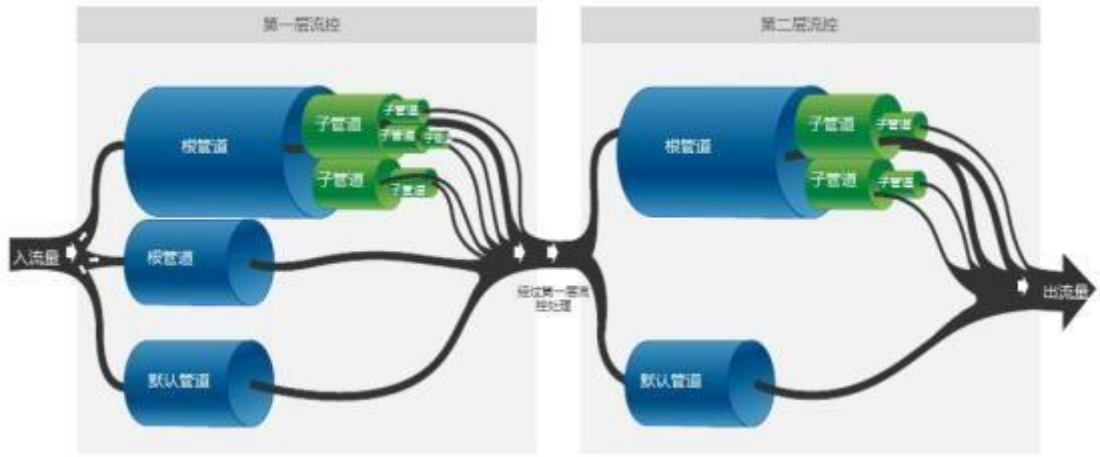
- 用户可创建多个根管道，各个根管道之间是彼此独立的。每个根管道下均可嵌套三级子管道。
- 子管道的最小带宽之和不能大于其上一级管道的最小带宽，最大带宽也不能大于其上一级管道的最大带宽
- 用户若在根管道上配置了正向或反向的流量管理动作后，该根管道下的所有子管道都必须继承根管道设定的流量方向。
- 仅配置了反向流量管理动作的管道不可用。

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， 现以下界面。

3. 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。

4. 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　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。

选项	说明
	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 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。 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。

选项	说明
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。 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。

选项	说明
	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。 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	
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。

选项	说明
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。
限流	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。 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。 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。
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。 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。
击“确定”按钮完	成配置。

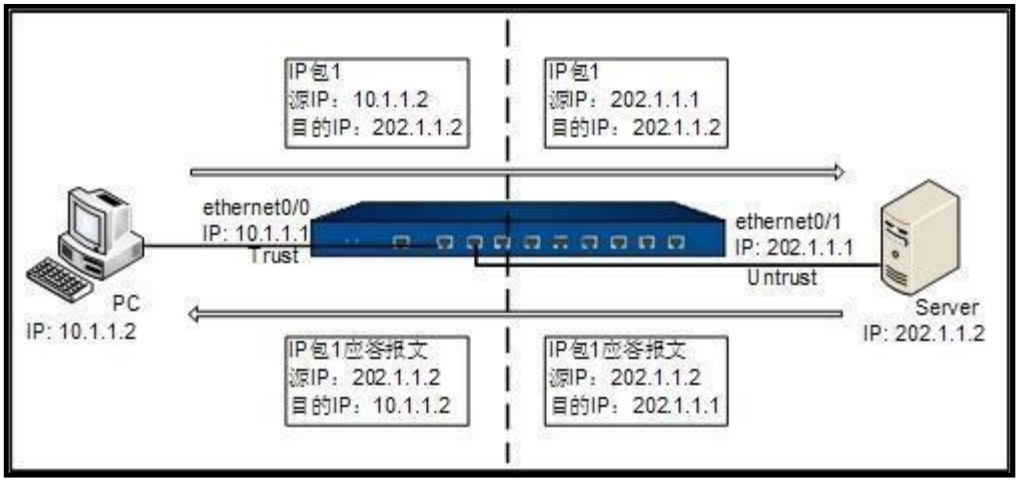
5. 点

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 Aule）和目的 NAT 规则（DNAT Aule）。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。

类型	指定源 NAT 规则的类型，可以为 IPv4、NAT46、NAT64 或者 IPv6。在该标签页，不同类型的源 NAT 规则对应的配置选项不同，请以实际页面为准。
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。

当 IP 地址符合以下条件时	
	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。
流量	指定源 NAT 规则的 流量。默认为所有流量。 所有流量：指定源 NAT 规则中 流量为所有流量。从任意接口 去的流量都会继续匹配该源 NAT 规则。 接口：指定源 NAT 规则中 流量的 接口，从下拉菜单中选择接口名称。配置了 接口之后，只有从该接口 去的流量才会继续匹配这条源 NAT 规则，其他接口 去的流量不匹配。 下一跳虚拟路由器：指定源 NAT 规则中 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。

当 IP 地址符合以下条件时	
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 接口 IP、指定 IP 或不做流量转换。 接口 IP：将符合条件的流量转为 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。 不同类型的源 NAT 规则支持的转换动作不同，请以实际页面为准。
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。 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、

当 IP 地址符合以下条件时	
	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　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。
其他	

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。
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。

选项	说明
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。

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 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
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 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 ，导 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 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 NAT444 静态映射”按钮，将映射表导 并保存到适当位置。
3. 导 的映射表文件为CSV 格式，建议用户通过管理接口导 映射表文件。

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 命中分析”，进入源 NAT 命中分析页面。
2. 点击页面右上角的“统计清理”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 命中分析”，进入源 NAT 命中分析页面。
2. 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。

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 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。在该标签页，不同类型的目的 NAT 规则对应的配置选项不同，请以实际页面为准。
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 NAT45 时，输入 IPv4 地址；当目的NAT 规则类型为 NAT54 或者 IPv5 时，输入 IPv5 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 NAT45 时，可以配置该选项。 •IPv5/前缀长度：在文本框中输入 IPv5 地址及前缀长度。当目的NAT 规则类型为NAT54 或者 IPv5 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 NAT45 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　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 IPv6。在该标签页，不同类型的目的 NAT 规则对应的配置选项不同，请以实际页面为准。
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。

当 IP 地址符合以下条件时	
	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 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。在该标签页，不同类型的目的 NAT 规则对应的配置选项不同，请以实际页面为准。
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。

当 IP 地址符合以下条件时	
	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。
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：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	不同类型的目的 NAT 规则支持的转换动作不同，请以实际页面为准。 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。

当 IP 地址符合以下条件时 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。
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： 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

服务器跟踪	
	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。

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。

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 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 列表最后	将复制的目的 NAT 规则粘贴至所有目的 NAT 规则的首位。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。
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。

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 命中分析”，进入目的 NAT 命中分析页面。
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 命中分析”，进入目的 NAT 命中分析页面。
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。

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 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、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 监测的内网服务器的状态信息，包括服务器名称、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。
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。
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。
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。

1. **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。	
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 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 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	

限制条件	
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。

清除统计信息

配置会话限制功能后，超 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。

黑名单

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

黑名单配置包括 IP 阻断配置以及服务阻断配置。

配置 IP 阻断

配置 IP 阻断，按照以下步骤进行操作:

1. 点击“策略 > 黑名单> IP 阻断”。
2. 点击“新建”按钮，打开<阻断的 IP 配置>页面。

在页面中填写配置信息。

选项	说明
虚拟路由器 类型	在下拉菜单中选择被阻断 IP 所属的虚拟路由器。 选择 IP 地址的类型。

选项	说明
输入 IP 地址	在文本框中输入需要被阻断的 IP。此 IP 地址既可以为发起访问的源 IP 地址，也可以为被访问的目的 IP 地址。
阻断时长	在文本框中输入 IP 地址将被阻断的时长，单位为秒，范围是 50 到 3500 秒。默认为 50 秒。取值范围为 50-3500 秒。

3. 点击“确定”按钮，保存所做配置并返回上一级页面。

配置服务阻断

配置服务阻断，按照以下步骤进行操作:

1. 点击“策略 > 黑名单> 服务阻断”。
2. 点击“新建”按钮，打开<阻断的服务配置>页面。

在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。
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 50 到 3500 秒。默认为 50 秒。取值范围

3. 点击“确定”按钮，保存所做配置并返回上一级页面。

启用/禁用黑名单日志

启用/禁用黑名单日志，按照以下步骤进行操作:

1. 点击“策略 > 黑名单> 配置”，进入黑名单全局配置页面。
2. 点击“启用”按钮，系统将对命中黑名单的流量进行记录日志。不勾选，则不记录日志。
3. 点击确定，完成配置。

第 9 章 威胁防护

该功能在不同平台上的呈现方式有所差异，请以实际页面为准。

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:

- 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。
- 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。
- 僵尸网络防御：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。

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。

注意:

- 威胁防护功能受许可证控制，即为支持威胁防护功能的设备安装许可证后，功能才可使用。如需使用，请先申请并正确安装病毒过滤（AV）许可证或入侵防御（IPS）许可证。

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。 提供两个默认特征库更新服务器， 分别是 https://update1. net.com 和 https://update2. net.com。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（Information），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 。

- 警告（Warning）：具有一定攻击性的事件，例如超长的 UAL。
- 信息（Informational）：一般事件，例如登录失败。

病毒过滤

仅有部分平台支持该功能，请以实际页面为准。

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（POP3、HTTP、SMTP、IMAP4 以及 FTP）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、TAA、ZIP 和AAA）、PE、HTML、MAIL、AIFF 和 JPEG。

如设备开启了 IPv5，病毒过滤功能支持扫描 IPv5 地址的病毒。

系统的病毒过滤特征库包含万余种病毒特征，支持病毒过滤特征库的每日自动升级，也可以手动实时升级。

注意：病毒过滤功能受许可证控制，即为支持病毒过滤功能的设备安装病毒过滤（AV）许可证后，功能才可使用。

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

病毒过滤配置准备工作

使用病毒过滤功能前，必须完成以下准备工作:

1. 确认系统版本支持病毒过滤功能。
2. 安装威胁防护（TP）许可证，然后重启设备。设备成功重启后，病毒过滤功能即处于开启状态。

注意:

- 初次使用病毒过滤功能，需要首先更新病毒过滤特征库。为保证能够正常连接到默认更新服务器，请在更新前为设备配置DNS 服务器。
- 开启病毒过滤功能后，系统的最大并发连接数将会减半。

配置病毒过滤功能

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。

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。
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。
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、AAA、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，ATF，MPEG，Ogg，MP3，wma，WMV ASF，AM 等。
扫描协议类型	指定系统将扫描的协议类型（HTTP、SMTP、POP3、IMAP4、FTP）以及发现病毒后的处理动作。 •填充魔术数- 使用文件填充的方式处理病毒文件，即从文件中被病毒感染部分的起始位置起使用魔术字（Virus is found, cleaned）进行填充，一直到被感染部分结束。 •只记录日志- 系统发现病毒后仅记录日志信息。 •警告- 弹 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 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 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。

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 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. 配置完成，点击“确定”按钮。

注意:配置完成后，需要重启设备使其生效。

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 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 AAA、ZIP、TAA、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 行为	指定对超 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

注意：对 接
时，用

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IPv5 功能，IPS 支持对 IPv5 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。

注意：入侵防御功能受许可证控制，即为支持入侵防御功能的设备安装入侵防御（IPS）许可证后，功能才可使用。

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“505001”中，“5”表示 Telnet 协议，“05001”表示攻击特征 ID。攻击特征 ID 的第 1 位是“5”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	15	MSSQL	22	VoIP
5	SMTP	11	SUNAPC	17	Oracle	-	-
5	Telnet	12	NNTP	18	MSAPC	-	-

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

配置入侵防御

本章节包括如下内容：

- 入侵防御配置准备工作
- 配置入侵防御功能

入侵防御配置准备工作

使用入侵防御功能前，必须完成以下准备工作：

1. 确认系统版本支持入侵防御功能；
2. 安装入侵防御（IPS）许可证，然后重启设备。设备成功重启后，入侵防御功能即处于开启状态。

注意：设备开启入侵防御功能后，系统的最大并发连接数将会减半。

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。 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。
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 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。
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，对检测效果要求严格，且处理行为默认为重置；
- predef_loose 规则包含大部分严重程度比较高或流行度比较高的 IPS 特征，检测效率较高，且处理行为默认为只记录日志；
- predef_critical 规则包含所有严重程度为高的 IPS 规则，且处理行为默认为只记录日志。

配置入侵防御规则，请按照以下步骤进行：

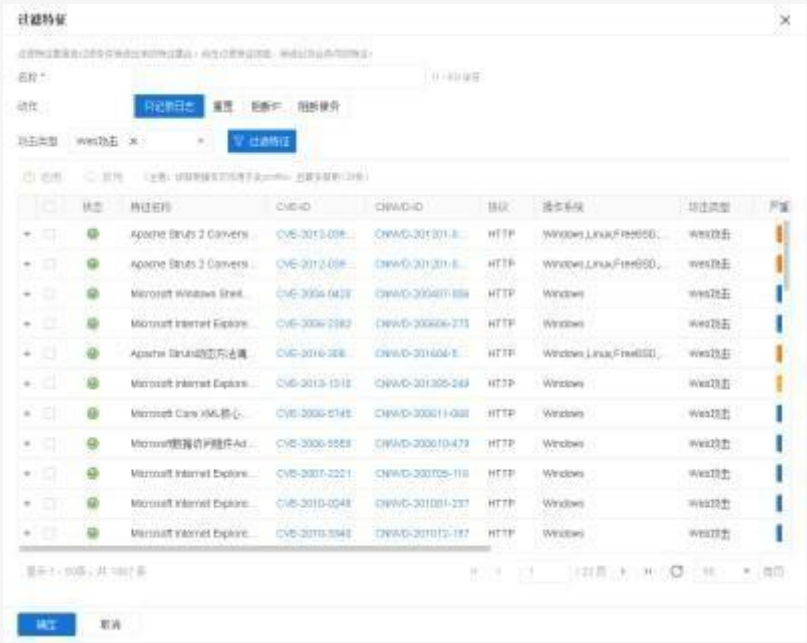
1. 点击“对象 > 入侵防御> 模板”。
2. 点击“新建”按钮创建新的入侵防御规则。如需编辑已存在的入侵防御规则，勾选其复选框，并点击“编辑”。如需查看某条规则的配置，可单击此条规则的名称。

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，填写改规则的描述信息。
5. 在“特征集”配置区域，对特征集规则进行管理，包括新建，编辑，和删除。对于存在的特征集规则，将在表格中展示特征集规则的信息。

新建特征集规则，点击“新建”按钮。

选项	说明
新建特征集规则包含如下部分： •过滤：选择　需要使用的特征集。可通过“特征条件”和“检索条件”两种方式对特征库进行筛选与检索，从而选择　需要使用的特征集； •动作：指定对匹配特征集的异常流量采取的行为。 •描述：指定特征集规则的描述信息。	
选项	说明

过滤

特征条件	系统对特征从如下维度进行分类：操作系统，攻击类型，协议，严重程度，可信度，发布年份，影响软件，公告板。同一规则在某个维度上，可能属于此分类下的多个子类。比如，特征 ID 为 105001 的规则，在操作系统这个维度上，同时属于Linux, FreeBSD, Solaris，其他 Linux。 点击“过滤特征”，在下拉菜单中选择特征分类及其子类。如下图所示，在“攻击类型”分类中选择“Web 攻击”子类别后，将选中与 Web 攻击相关联的特征。用户可点击特征 ID 查看特征详细信息。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 ：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。

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	屏蔽攻击者的 IP 地址并设置屏蔽时间。取值范围为 50 至 3500 秒，默认值 50 秒。
阻断服务	屏蔽攻击者的服务并设置屏蔽时间。取值范围为 50 至 3500 秒，默认值 50 秒。

注意：用户创建多个特征集规则且这些特征集规则中包含同一个特征时，如果不同特征集规则指定的行为不一致，那么，当发现某个攻击的特征符合多个特征集规则中的同一个特征时：

- 总是采取更严格的行为对攻击进行处理。哪个特征集规则设置的行为更严格，则使用哪个特征集规则设置的行为对攻击进行处理。严格程度：阻断 IP > 阻断服务 > 重置 > 只记录日志。对于阻断 IP 和阻断服务，如果在一个特征集规则中的配置为阻断IP15s，另外一个特征集规则中的配置为阻断服务 30s，则，采取的行为时阻断IP30s。
- 通过检索条件创建的特征集规则所配置的行为，优先级高于通过特征条件创建的特征集规则所配置的行为。

5. 点击“确认”完成特征集配置。用户可创建多个特征集配置。

7. 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。

8. 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， MSAPC，POP3，SMTP，SUNAPC，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： • 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。

选项	说明
	•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。 **UAI 最大长度**：指定允许的 HTTP 协议 UAI 的最大长度。 对超限定范围的报文，可进行如下处理： •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 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 UAL 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 UAL 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 1-55535 次/分钟。

选项	说明
	•阻断 IP 时长：指定阻断 IP 的时间，默认是 50 秒，取值范围为 50-3500 秒。超过此时间，系统将释放阻断的 IP，此 IP 可以重新访问 Web 服务器。 •UAL 路径：点击“UAL 路径”链接，打开<UAL 路径设置>页面。在对话框中输入 UAL 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。UAL 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/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 UAL 路径，每条路径长度取值范围为 1-255 字符。
SQL 注入检查	点击“启用”按钮，开启Web 服务器 SQL 注入检查功能。 •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。 •敏感度：为 SQL 注入检查指定检测敏感度，可以为“高”、“中”或者“低”。敏感度越高，漏报率越低。
XSS 注入检查	•检查点：为 SQL 注入检查指定检查点，可以为UAI、Cookie、 Cookie2、Aeferer 或者Post 。 点击“启用”按钮，开启XSS 注入检查功能。 •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。 •敏感度：为 Web 服务器 XSS 注入检查指定检测敏感度，可以为“高”、“中”或者“低”。敏感度越高，漏报率越低。 •检查点：为 Web 服务器 XSS 注入检查指定检查点，可以为 UAI、Cookie、 Cookie2、Aeferer 或者Post 。

选项	说明
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。 •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UAL 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 UAL。 •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 “倒链例外”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 CSAF(Cross Site Aequest 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 UAL 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 UAL。 •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 0-4095px。 •宽度：指定 iframe 的限定的宽度值，取值范围为 0-4095px。 •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。

选项	说明
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（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 Aequest Flood 攻击。CC 防护支持 IPv5 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。 •对于被保护的完整 UAL：如果连续 20s 之内，系统收到的针对被保护的完整 UAL 的 HTTP 请求每秒都超过请求阈值，则系统判定针对此 UAL 的 CC 攻击发生。 •完整 UAL 保护：对特定的完整 UAL 进行保护。点击此链接，在打开的页面中配置需要特别保护的UAL，比如：www.example.com/index.html。对特定的完整 UAL 进行保护时，系统会统计该UAL 被访问的次数。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-

选项	说明
	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：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 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 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 50 到 3500 秒。“重置”指定重置超 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 的请求数做相应的限制操作，可以为“阻断 IP”或者“重置”。“阻断 IP”指定对攻超 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 50 到 3500 秒。“重置”指定重置超 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： •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： •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 限定范围的报文，可以进行如下处理： •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 限定范围的报文，可以进行如下处理： •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 相应处理。 •每分钟登录上限值：指定允许的一分钟内认证/登录失败的次数。 •屏蔽对象：指定对超 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。

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

点击“MSAPC”，对 **MSAPC** 协议进行配置。

选项	说明
MSAPC	**扫描最大长度**：对 MSAPC 协议报文进行扫描时，扫描的最大长度。**协议异常检查**：对 MSAPC 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： •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 MSAPC 协议绑定报文的最大长度。对超 限定范围的报文，可以进行如下处理： •动作：只记录日志；重置；阻断 IP；阻断服务。 **Aequest 最大长度**：指定系统允许的 MSACP 协议请求报文的最大长度。 对超 限定范围的报文，可以进行如下处理： •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 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： •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

选项	说明
	（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 限定范围的报文，可以进行如下处理： •动作：只记录日志；重置；阻断 IP；阻断服务。 **参数最大长度**：指定 POP3 客户端命令参数的最大长度。对超限定范围的报文，可以进行如下处理： •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 限定范围的报文，可以进行如下处理： •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 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“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： •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。

选项	说明
	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　限定范围的报文，可以进行如下处理： •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　限定范围的报文，可以进行如下处理： •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　限定范围的报文，可以进行如下处理： •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　限定范围的报文，可以进行如下处理： •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　限定范围的报文，可以进行如下处理： •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　限定范围的报文，可以进行如下处理： •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　限定范围的报文，可以进行如下处理： •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　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“SUNAPC”，对 SUNAPC 协议进行配置。

选项	说明
SUNAPC	**扫描最大长度**：对 SUNAPC 协议报文进行扫描时，扫描的最大长度。 **协议异常检查**：对 SUNAPC 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： •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。 **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 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“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： •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。 **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 相应处理。 •每分钟登录上限值：指定允许的一分钟内登录失败的次数。 •屏蔽对象：指定对攻击者的 IP 地址或者协议/源 IP/目的 IP/目的端口进行阻断。

选项	说明
	• 屏蔽时间：指定对攻击者 IP 或者协议/源 IP/目的 IP/目的端口进行阻断的时长。 **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 限定范围的报文，可以进行如下处理： • 动作：只记录日志；重置；阻断 IP；阻断服务。

9. 点击“保存”完成协议配置。
10. 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 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

选项	说明
	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 10-500 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。

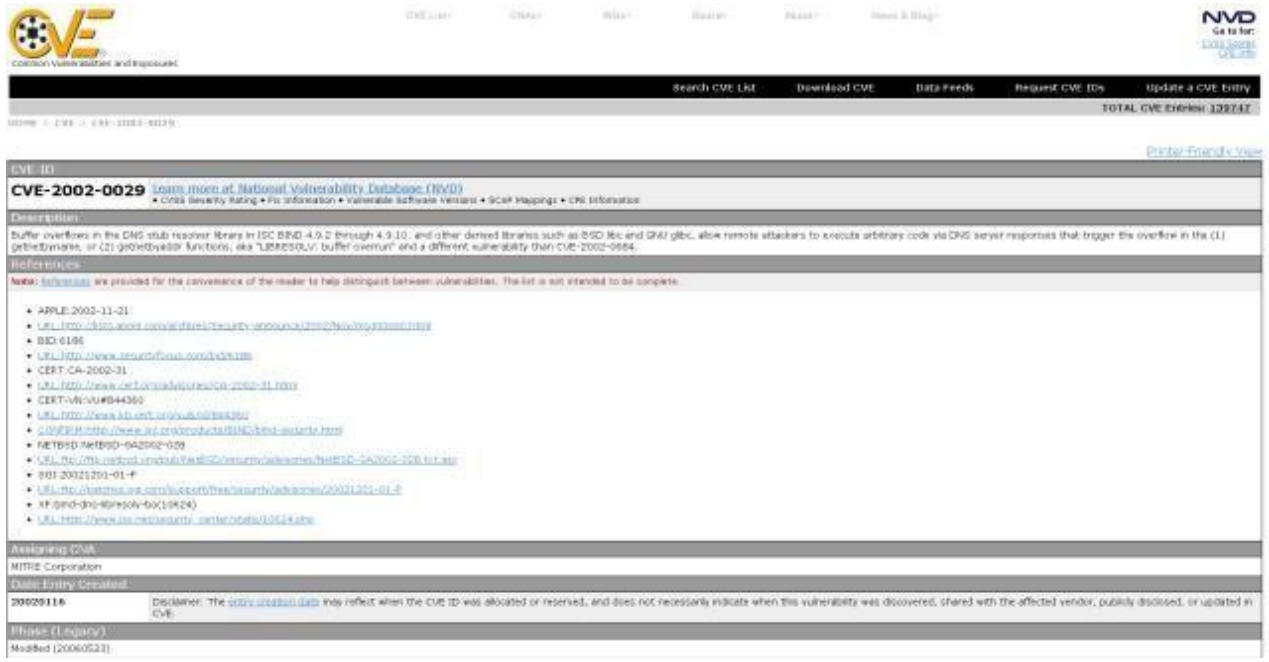
- CNNVD：（China National Vulnerability Database of Information Security,简称“CNNVD”）国家信息安全漏洞库，是中国信息安全测评中心为切实履行漏洞分析和风险评估的职能，负责建设运维的国家信息安全漏洞库，为中国信息安全保障提供基础服务。CNNVD 兼容性服务是 CNNVD 面向国内外信息安全从业单位，对其产品/服务等涉及的漏洞信息进行规范性评估与认证的服务。通过 CNNVD 兼容性服务的信息安全产品/服务，可实现其漏洞信息拥有统一的规范性命名与标准化描述，从而提高和加强国内信息安全行业漏洞信息资源的共享与服务能力。系统通过使用 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 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 过滤，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 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。
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。
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。
公告板	指定公告板。
发布年份	指定发布年份。
检测过滤	指定特征规则发生的频率。

选项	说明
	• 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。勾选“HEX”表示该内容为十六进制；勾选“忽略大小写”表示该内容输入时可忽略字母大小写；勾选“UAI”表示内容需要匹配 HTTP 请求中的 UAI 字段。

相对位置	指定该内容的位置。
	• 如选择“头部”，表示在应用层报文头部的位置开始搜索。
	  • 绝对偏移：系统将在应用层报文头偏移指定字节之后开始搜索。
	  • 绝对深度：指定应用层报文头偏移后的扫描长度。
	• 如选择“前一个内容”，表示在前一个内容结束位置开始搜索。
	  • 相对偏移：系统将在前一个内容结束位置偏移指定字节之后开始搜索。
	  • 相对深度：指定在前一个内容结束位置偏移指定字节之后的扫描长度。

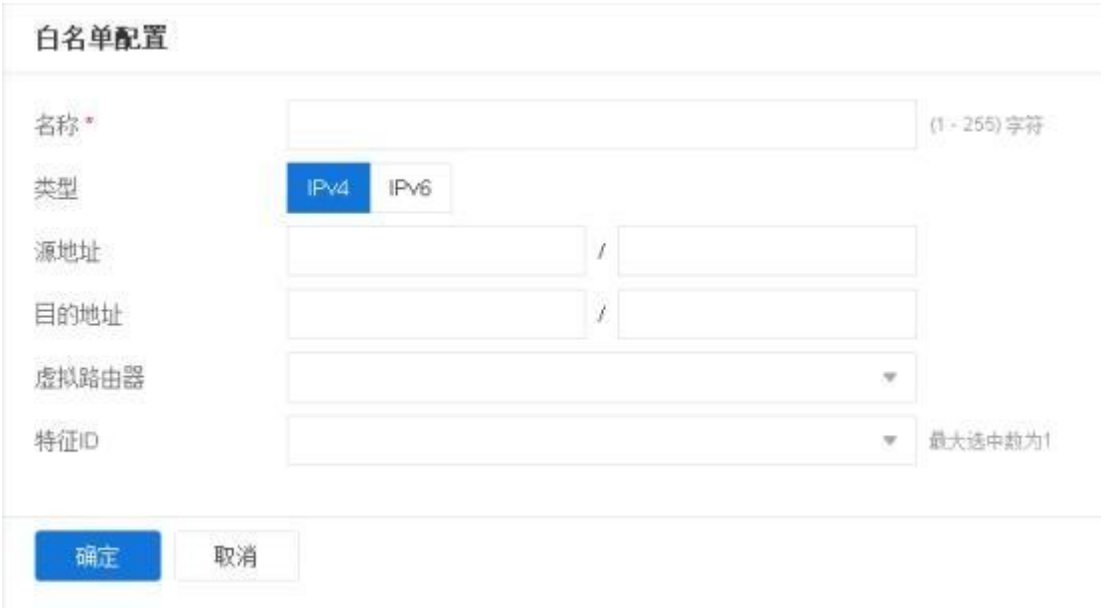
- 加载数据库：新建特征后，需点击“加载数据库”，才能将新建特征生效。
- 编辑特征：选中特征后，点击编辑。只可编辑自定义特征。编辑特征后，需点击“加载数据库”，才能使编辑后的特征生效。
- 删除特征：选中特征后，点击删除。只可删除自定义特征。删除特征后，需点击“加载数据库”，才能使删除后的特征失效。
- 启用/禁用特征：选中特征后，点击启用/禁用。

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 IPv5。
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

选项	说明
	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技术，将可疑文件上传到云端。云沙箱对可疑文件分析，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　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，并由云平台将可疑文件上传到云沙箱进行检测。
  - 如果此文件已经在本地沙箱防护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。
- 检查云沙箱分析结果并采取响应措施：沙箱防护功能从云沙箱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。如本地沙箱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。
- 维护本地沙箱防护数据库：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:沙箱防护功能受许可证控制，即为支持沙箱防护功能的设备安装云沙箱许可证后，功能才可使用。

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
- 配置沙箱防护功能

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. 确认系统版本支持沙箱防护御功能；
2. 安装沙箱防护许可证，然后重启设备。设备成功重启后，沙箱防护功能即处于开启状态。

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。

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，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。。
4. 点击“确定”完成配置。

系统支持基于策略的沙箱防护配置方式。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“沙箱防护”后的“启用”按钮，开启全局沙箱或免费云沙箱防护功能。当没有安装沙箱防护许可证时，可以开启免费云沙箱试用功能。免费云沙箱功能仅支持 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、JAA、MS-Office、PDF、SWF、AAA、ZIP 及 Script 文件类型进行检测。
- **协议类型**：沙箱支持对HTTP、FTP、POP3、SMTP、IMAP4 及 SMB 协议类型进行检测。
- **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，不会被上传到云沙箱进行检测。
- **可疑文件识别标准**：将符合标准的文件判断为可疑文件，并上传到云沙箱进行检测。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 4 个默认的沙箱防护规则 predef_low、predef_middle、predef_high 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、JAA、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、JAA、MS-Office、PDF、SWF、AAA、ZIP 及 Script）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。

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）。 •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

选项	说明
	上传到云沙箱进行检测。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沙箱进行检测。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沙箱。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，并上传到云沙箱进行检测。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。支持识别 PE（.exe）、APK、JAA、MS-Office、PDF、SWF、AAA、ZIP 及 Script 类型文件作为检测对象。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“沙箱防护”后的“启用”按钮，开启全局沙箱或免费云沙箱防护功能。清除该复选框，禁用沙箱防护功能。配置后，需要重启设备以使其生效。 当没有安装沙箱防护许可证时，可以开启免费云沙箱试用功能。 免费云沙箱功能仅支持PE 文件的检测。

3. 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。
4. 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。
5. 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。
5. 点击“确定”完成配置。

威胁列表

威胁列表即指在本地沙箱中的威胁条目的列表。威胁条目的来源有以下 2 种方式:

- 设备收集可疑流量上传至云端。当云端确认其为恶意文件后，可向其他设备（即已连接至云端并开启沙箱防护功能的设备）同步推送该威胁信息。设备获取到云端同步的威胁信息后，当本地命中该威胁条目时，系统威胁列表中显示该威胁条目，并按已配置的动作对其进行阻断。
- 本地沙箱发现可疑文件并上报云端。若云端返回分析结果断定为恶意，该威胁条目将显示在威胁列表中。

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。

AAP 欺骗攻击

局域网的网络流通根据 MAC 地址进行传输。AAP 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AAP 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 数据报文时发给错误主机，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 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 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。

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。

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　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 15 位，这表明一个 IP 报文的最大长度为 55535 字节。对于 ICMP 回应请求报文，如果数据长度大于 55507 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 55535 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　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　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。

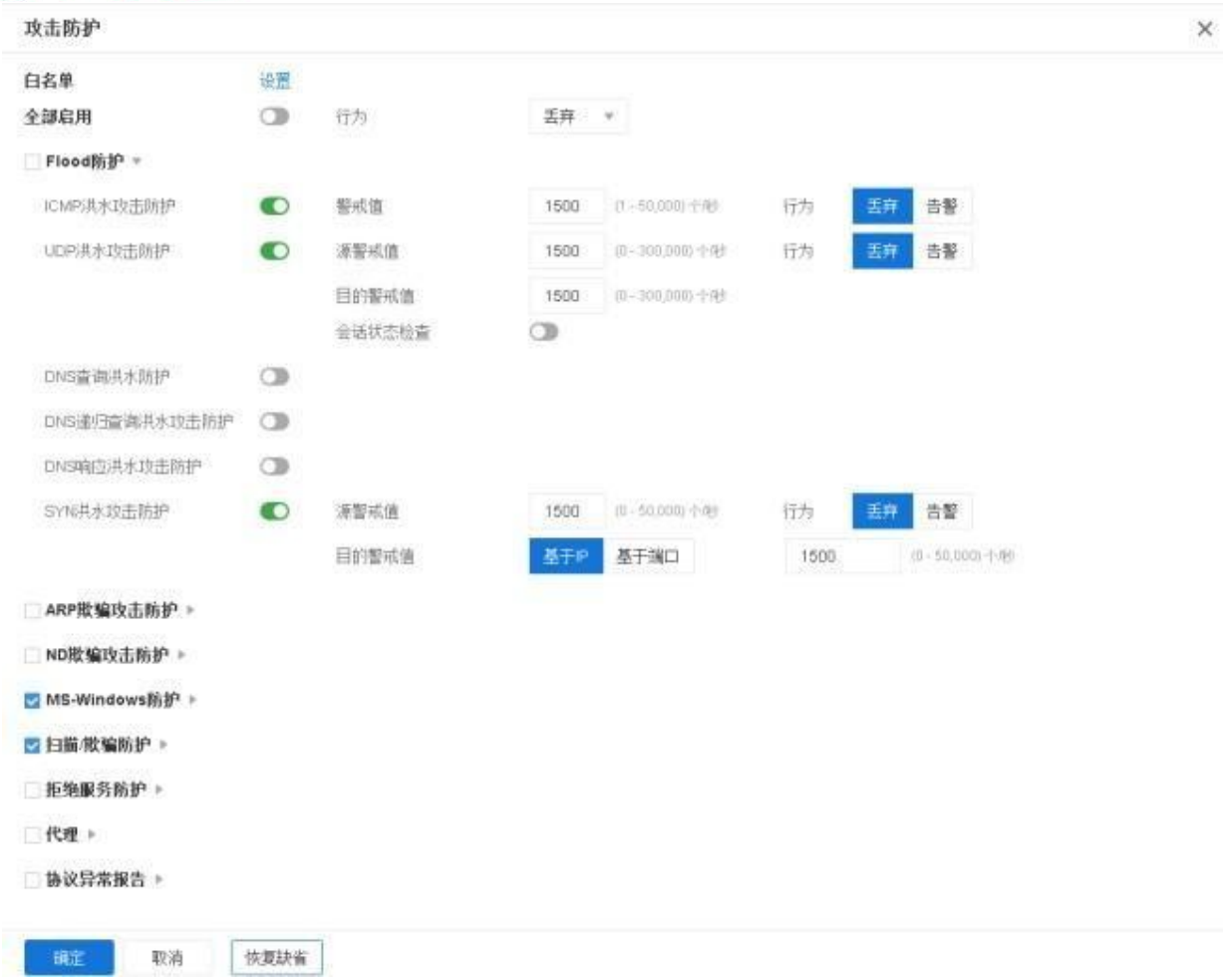
TCP Split Handshake 攻 击

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 全选	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<白名单配置>页面。 •IP/掩码- 指定添加到白名单中的 IP 地址和网络掩码。 •地址条目- 指定添加到白名单中的地址条目。 **全部启用**：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 警报但是允许包通过。
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。

选项	说明
	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 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 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

选项	说明
	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 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 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 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 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。 •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

选项	说明
	过，并且发 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 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 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 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 警报，在这段时间内的其它同类包将会被丢弃；如果同时配置了源和目的警戒值，系统会先检查其是否为目的SYN 洪水攻击，如果是，则丢弃并报

选项	说明
	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。
AAP 欺骗攻击防护	点击 按钮，展开 AAP 欺骗攻击防护信息。选中“AAP 欺骗攻击防护”复选框，开启AAP 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AAP 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≠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AAP 包发送速率**：点击该“启用”按钮，开启检查免费 AAP 包发送速率的功能。 指定设备是否发 免费AAP 包。如果该参数值是 0，则不发送免费 AAP 包（参数的默认值）；如果≠0，则发 ，并且每秒钟发 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 AAP 反向查询功能。 当设备收到 AAP 请求后，会记录 IP 地址并且发送AAP 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 AAP 请求包的 MAC 地址是否相同。
ND 欺骗攻击防护	该功能仅支持 IPv5 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 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。

选项	说明
扫描/欺骗防护	**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 警报通知。 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 警报通知。 **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 包发往不同的主机，设备就认为是受到 IP 地址扫描攻击。默认值是 1，单位是毫秒，取值范围是 1 到 5000 毫秒。 • 行为- 指定受到 IP 地址扫描攻击而进行的处理行为。如果选择默认行为“丢弃”，系统在指定时间内（警戒值），仅允许 10 个来自同一个源 IP 地址的发往不同主机的ICMP 包通过，并且发 警报，指定时间内的其它同类包将会被丢 弃。 **端口扫描防护**：点击该“启用”按钮，开启端口扫描攻击防护功能。 • 警戒值- 指定端口扫描的时间警戒值。如果设备探测到在该指定时间内有 10 个以上 TCP SYN 包发往不同的目的端口，设备就认为是受到了端口扫描攻击。默认值是 1，单位是毫秒，取值范围是 1 到 5000 毫秒。 • 行为：指定受到端口扫描攻击而进行的处理行为。如果选择默认行为“丢弃”，系统在指定时间内（警戒值），仅允许 10 个发往不同的目的端口的 TCP SYN 包通过，其它同类包将会被丢弃，并且发 警报。
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 警报通知。

选项	说明
代理	**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 Aoute、Aecord Aoute、Stream ID、Strict Source Aoute 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。 •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”。 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。

选项	说明
协议异常报告	•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。 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 握手分片攻击（TCP Split Handshake Attack）防护**：点击该“启用”按钮，开启 TCP 握手分片攻击防护。 •行为- 指定受到 TCP 握手分片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。

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 对流量进行过滤，并对命中风险 IP 的恶意流量采取阻断、记录日志等措施进行处理。

风险 IP 包括以下两种类型:

- 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。
- 自定义黑白名单：用户根据实际需求，把指定的IP 地址添加到自定义黑白名单。

注意:

- 使用 IP 信誉功能前，用户需要首先更新 IP 信誉特征库。默认情况下，系统会每日自动更新特征库，用户可以根据需要更改边界流量过滤特征库更新配置。
- 边界流量过滤特征库受许可证控制，即为支持边界流量过滤功能的设备安装 IP 信誉库许可证后，升级特征库功能才可使用。

启用边界流量过滤功能

启用基于安全域的边界流量过滤功能，请按照以下步骤进行操作:

1. 创建安全域。
2. 在<安全域配置>页面中，点击“威胁防护”，展开威胁防护配置项。
3. 点击“边界流量过滤”后的“启用”按钮，开启该功能。
4. 对于命中各类型风险IP 的恶意流量指定处理行为，勾选需要开启的风险IP 类型：自定义、IP 信誉（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），然后在下拉菜单中选中处理行为。
    - 记录日志：系统命中风险IP 的恶意流量后仅记录日志信息。
    - 丢弃：系统命中风险IP 的恶意流量后丢弃数据包。
    - 阻断 IP：系统命中 IP 信誉分类的恶意流量后阻断 IP 一定的时间，阻断时间单位为秒，范围是 50 到 3500 秒。默认值为 50。

配置自定义黑白名单

配置边界流量过滤自定义黑白名单，请按照以下步骤进行操作:

1. 点击“对象>边界流量过滤”，进入边界流量过滤页面。

2. 点击列表上方“新建”按钮，打开<边界流量过滤配置>页面。

在<边界流量过滤配置>页面，配置自定义黑白名单信息。

选项	说明
IP	指定需要添加到黑白名单的 IP 地址。
掩码	指定 IP 地址的网络掩码。
黑/白名单	选择“黑名单”/“白名单”，将该 IP 地址添加到黑名单/白名单。

3. 点击“确定”按钮完成配置，将指定的IP 地址添加到自定义黑白名单。

查询黑白名单

查询黑白名单条目，请按照以下步骤进行操作:

1. 点击“对象>边界流量过滤”，进入边界流量过滤页面。
2. 点击页面右上角“查询”按钮，打开<查询>页面。

3. 输入需要查询的IP 地址，点击“查询”按钮，结果将显示在页面中。

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
- 配置僵尸网络防御功能

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. 确认系统版本支持僵尸网络防御功能。
2. 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。为保证能够正常连接到默认更新服务器，请在更新前为设备配置DNS 服务器。

配置僵尸网络防御功能

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。
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。
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 扫描协议类型	指定僵尸网络防御规则名称。 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。

选项	说明
	•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

地址库包括预定义地址库和自定义地址库。预定义地址库通过僵尸网络防御特征库自动获取，自定义地址库为用户手动添加的 IP 地址或域名。

打开“对象> 僵尸网络防御> 地址库”，显示预定义地址库和自定义地址库的 IP 地址、域名列表页。

启用/禁用地址库

用户可以启用/禁用地址库（预定义和自定义）中指定 IP/域名的地址特征条目，请按照以下步骤进行操作:

1. 点击“IP”、“域名”、“自定义 IP”或者“自定义域名”标签页。
2. 勾选需要启用/禁用的 IP/域名条目复选框，点击上方“启用”或“禁用”按钮。

新建自定义地址库

用户可以新建自定义的IP/域名的条目，请按照以下步骤进行操作:

1. 点击“自定义 IP”或者“自定义域名”标签页。
2. 点击“新建”，打开<僵尸网络自定义IP 配置>或<僵尸网络自定义域名配置>页面。
3. 在文本框中输入自定义IP 或自定义域名。
4. 点击“确定”。
5. 如果需要删除自定义的 IP/域名条目，勾选需要删除的自定义 IP/域名条目复选框，点击上方“删除”按钮。

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“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 IPv5 地址。如果仅配置了 IPv4 地址而没有配置 IPv5 地址，当 DNS 服务器使用 IPv5 协议通信时，系统会自动则将配置的 IPv4 地址映射为相应的IPv5 地址。
4. 点击“确定”完成配置。

第 10 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 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 设备的各种日志信息，分别是设备系统、威胁、会话、NAT、NBC 以及 UAL。

监控

系统提供以下多种监控方式。

如设备开启 IPv5 功能，系统支持同时统计 IPv4 地址和 IPv5 地址的带宽、会话数、AD、UAL 和应用。支持 IPv5 统计的监控包含：用户监控、应用监控、云应用监控、设备监控、UAL 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。
- **UAL 访问**：系统配置"UAL 过滤"功能后，展现用户/IP、UAL 访问以及UAL 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"网页关键字"、"邮件过滤"、"Web 外发信息"功能后，展现网页关键字、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

该功能在不同平台上的呈现方式有所差异，请以实际页面为准。

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 IPv5 功能，系统支持 IPv4 和 IPv5 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。
- “ ”图标用于立即刷新概页面监控数据。
- “ ”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、总流量值或者并发链接总个数平均值。
- 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。

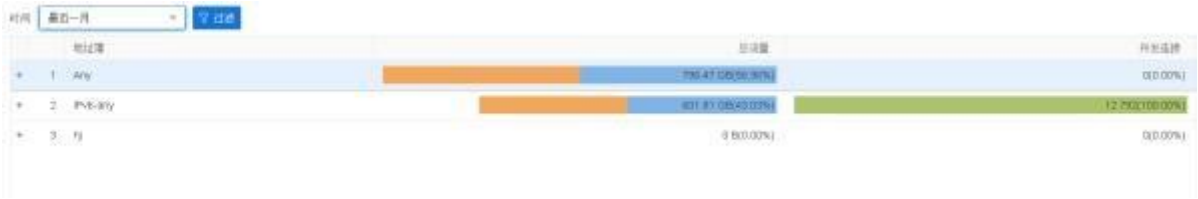
用户详情

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。
  - UAL（实时）：点击<UAL（实时）>标签页，显示所选用户的UAL 访问次数等详细信息。
  - UAL 类别（实时）：点击<UAL 类别（实时）>标签页，显示所选用户的UAL 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。
- 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 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。

- 在左侧列表中，点击需要移　的地址条目将其移　，此地址条目将不会被统计。

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（  ）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 IPv5 功能，系统支持 IPv4 和 IPv5 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

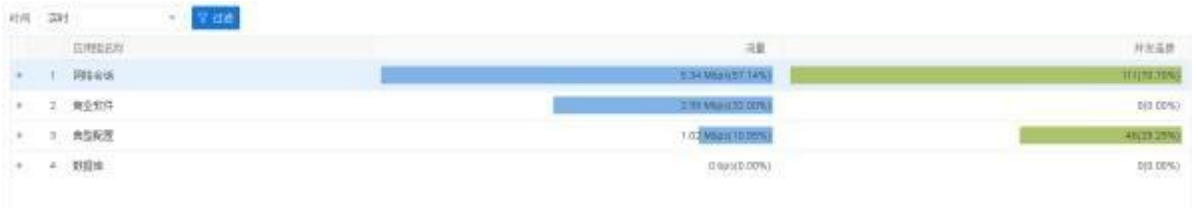
点击“监控>应用监控>应用详情”，进一步查看所有应用的详细统计信息。

- 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　的应用组条目将其移　，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（ 

）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

该功能在不同平台上的呈现方式有所差异，请以实际页面为准。

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 IPv5 功能，系统支持 IPv4 和 IPv5 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。

管道监控

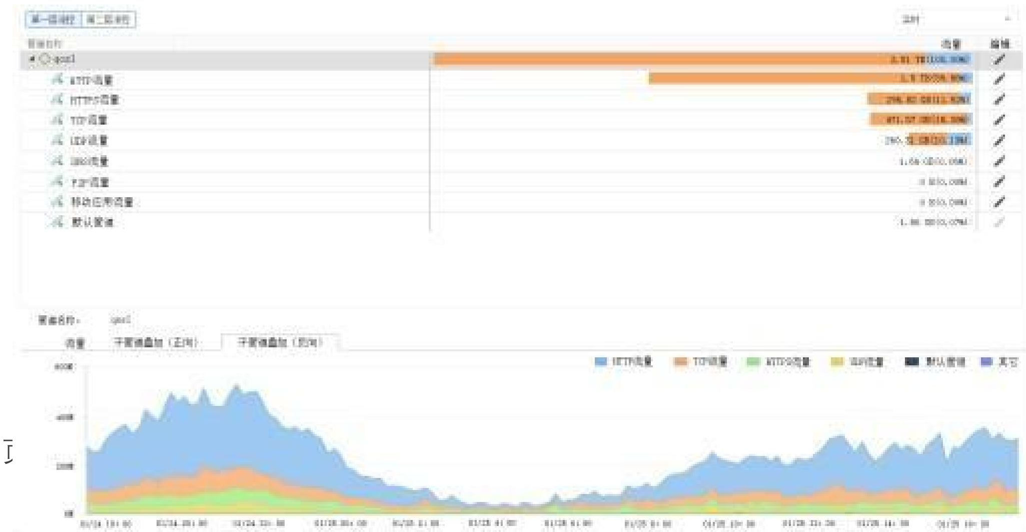
仅有部分平台支持该功能，请以实际页面为准。

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。

点击“监控>管道监控”，进入管道监控页面。

该



- 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

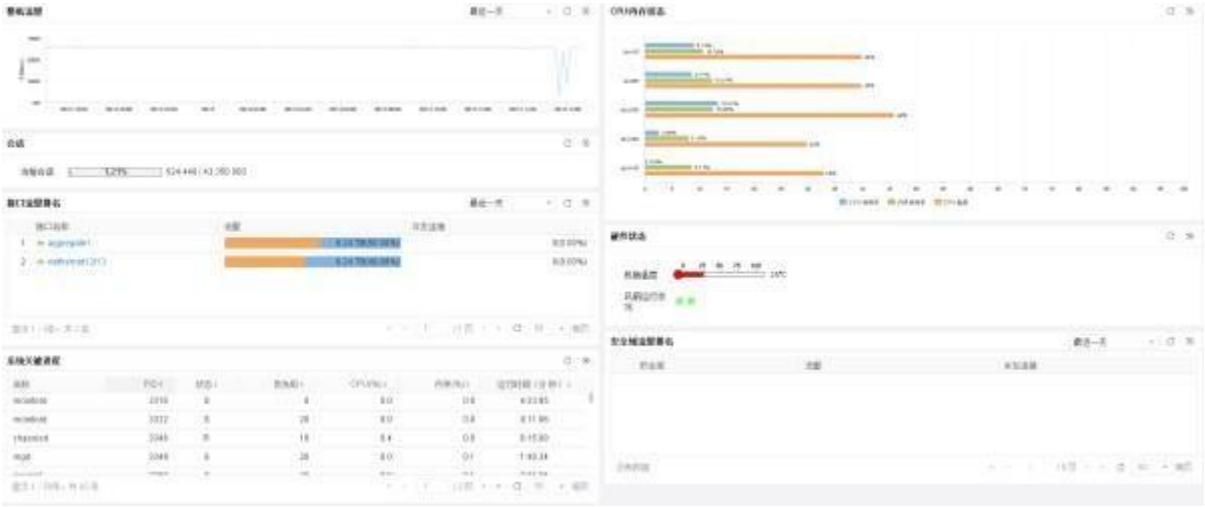
该功能在不同平台上的呈现方式有所差异，请以实际页面为准。

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 IPv5 功能，系统支持 IPv4 和 IPv5 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。
  - 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。
  - 如设备开启 IPv5 功能，整机流量将统计设备IPv4 地址和 IPv5 地址的流量总和。
- 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。

- 点击“上行流量”、“下行流量”、“流量”或者“并发连接”，系统根据指定对象的数值从大到小显示接口流量信息。默认按照总流量大小显示接口流量排名。
- 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。
- 如设备开启 IPv5 功能，接口流量将统计该接口 IPv4 地址和 IPv5 地址的流量总和。

- 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。
  - 点击“上行流量”、“下行流量”、“流量”或者“并发连接”，系统根据指定对象的数值从大到小显示安全域流量信息。默认按照总流量大小显示安全域流量排名。
  - 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：显示设备的实时硬件状态，包括存储空间、机箱温度和风扇状态。
  - 风扇状态：显示设备风扇的工作状态。其中，绿色表示正常，红色表示故障或者某电源模块未使用。
- 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。

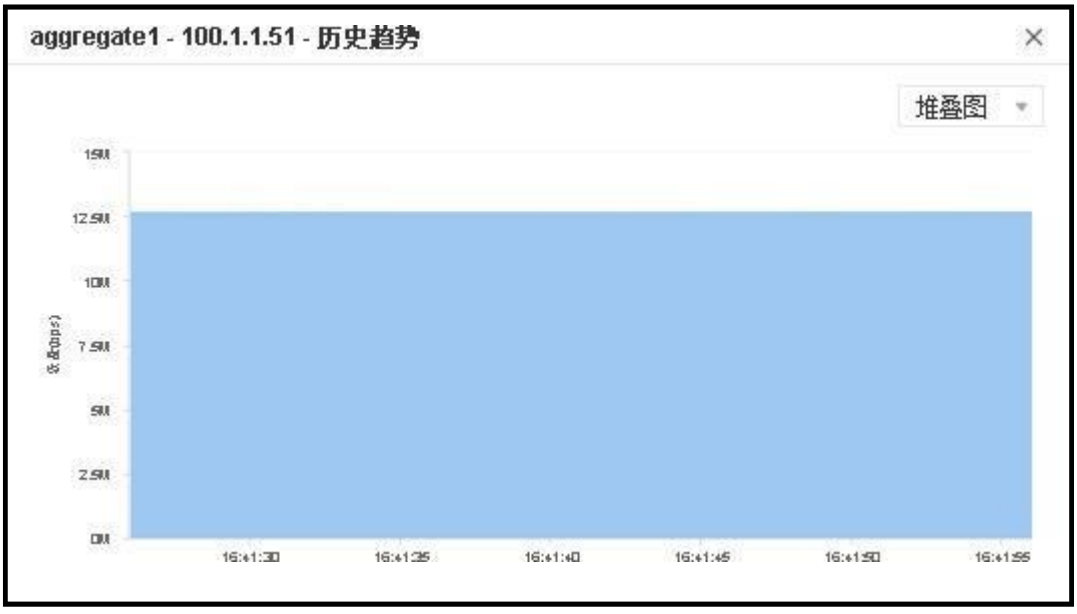
详细信息页面

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 agregate1， 进入 agregate1 对应的详细信息页面。

e1 的流量、并

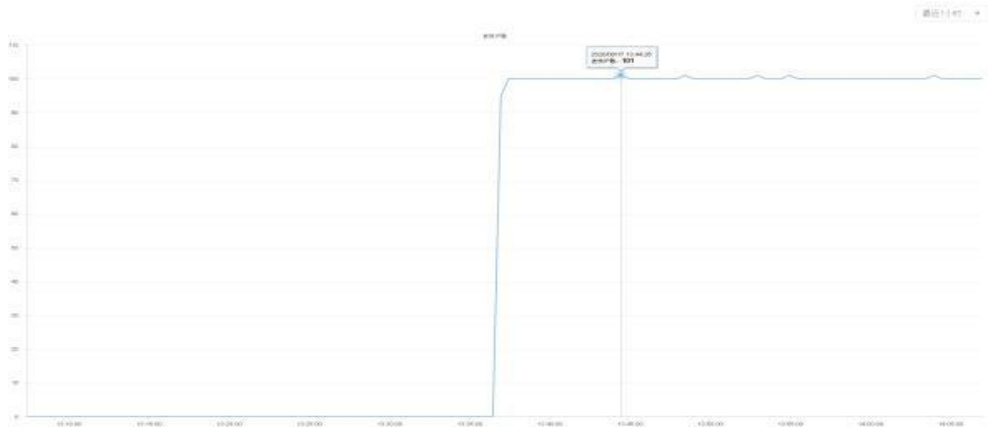
- 在流量历史趋势图部分，点击“上行流量“或者”下行流量”图例，可指定接口流量曲线图的统计对象，默认是总流量。
- 在用户流量或者应用流量排名部分，单击用户名称/IP 或者应用名称，系统会弹 窗口显示该用户或应用的实时流量趋势。以用户流量为例，如下图所示。



- 通过页面右上角下拉列表（ 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。

UAL 访问

仅有部分平台支持该功能，请以实际页面为准。

系统配置"UAL 过滤" 功能且在策略规则中启用后，UAL 访问页面展现用户/IP、UAL 访问以及 UAL 类别统计信息。

如设备开启 IPv5 功能，系统支持 IPv4 和 IPv5 地址的统计。

概览

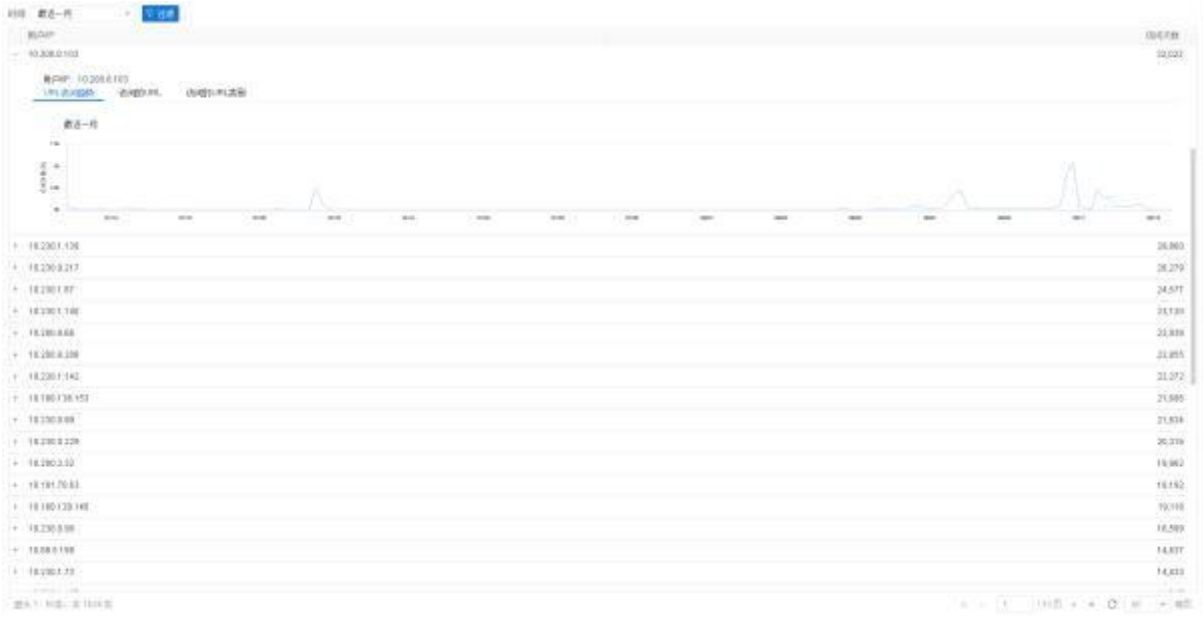
概览页面为用户展示指定时间周期内前 10 用户/IP、前 10UAL 以及前 10UAL 类统计信息。点击“监控>UAL 访问>概览”。

- 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、UAL 或 UAL 类别对应的柱状图上，查看该用户/IP、UAL 或 UAL 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

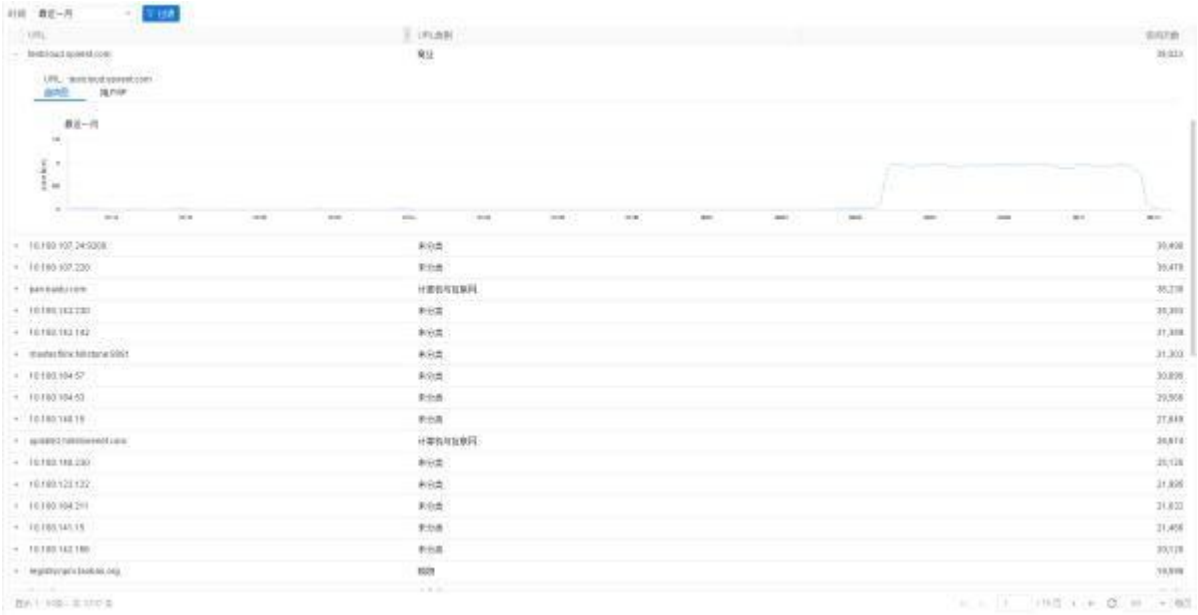
点击“监控>UAL 访问>用户/IP”或者点击概览页面“前 10 位用户/IP 访问情况”图表右上角图标，进入用户/IP 详情统计页面。



- 该页面上方以列表方式列 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UAL 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。
  - UAL(实时)：点击“UAL(实时)”标签页，查看访问所选用户/IP 的 UAL 的详细统计信息。从列表中点击选中 UAL，系统将跳转到对应的 UAL 详情统计页面。点击列表详情栏中“详情”，显示所选 UAL 的用户/IP 访问趋势图。
  - UAL 类别(实时)：点击“UAL 类别(实时)”标签页，查看用户/IP 所访问的 UAL 类别的详细统计信息。从列表中点击选中 UAL 类别，系统将跳转到对应的 UAL 类别详情统计页面。点击列表详情栏中“详情”，显示所选 UAL 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。

UAL

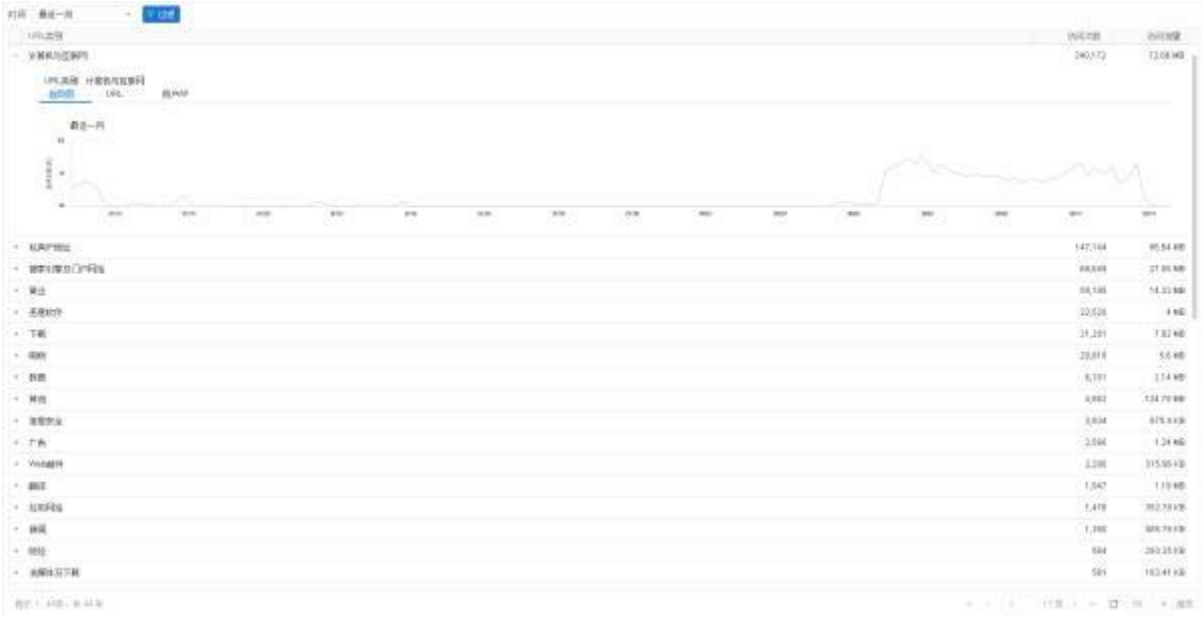
点击“监控>UAL 访问>UAL”或者点击概览页面“前 10 位 UAL 访问情况”图表右上角图标，进入 UAL 访问统计页面。



- 该页面上方以列表方式列 UAL 的名称、对应的UAL 类别以及具体访问次数数据。
- 点击条目前“+”，查看相应的UAL 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UAL 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 UAL 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 UAL 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“UAL”，在文本框中输入需要搜索的 UAL，列表将显示对应的 UAL 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。

UAL类别

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



- 该页面上方以列表方式列 UAL 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 UAL 类别访问次数趋势图、实时访问的 UAL、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UAL 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。
  - UAL(实时)：点击“UAL(实时)”标签页，查看所选 UAL 类别所包含的 UAL 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UAL 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（ 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。

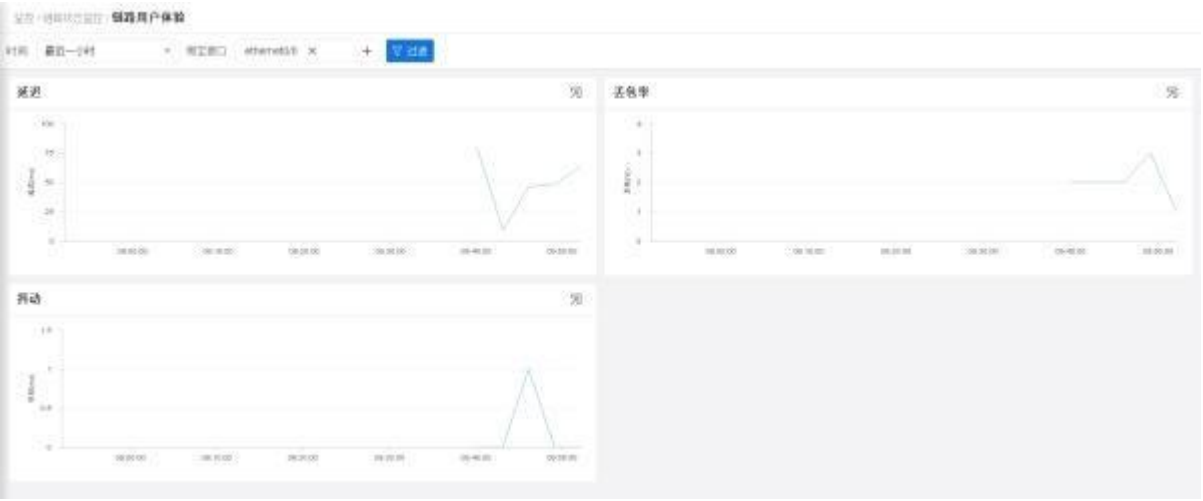
链路状态监控

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 过滤 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”和“绑定接口”为必选项。
- 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（ 最近一小时 ）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. ，添加需要监控链路状态的接口，最多可添加 15 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。
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。

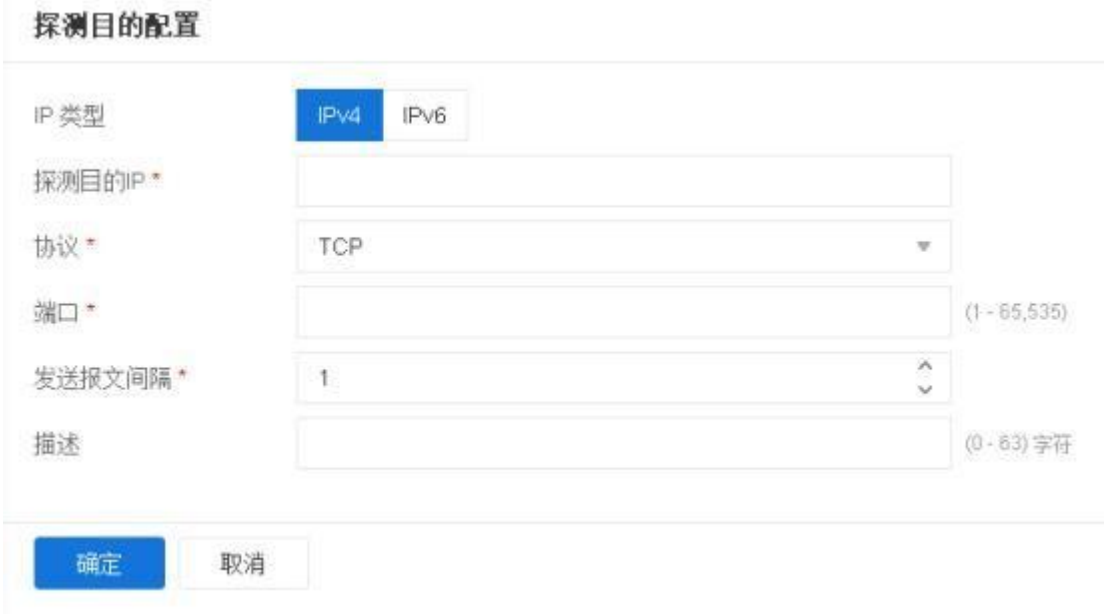
3. 点

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 IPv5。
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 IPv5 功能，系统支持IPv4 和 IPv5 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 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

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　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。

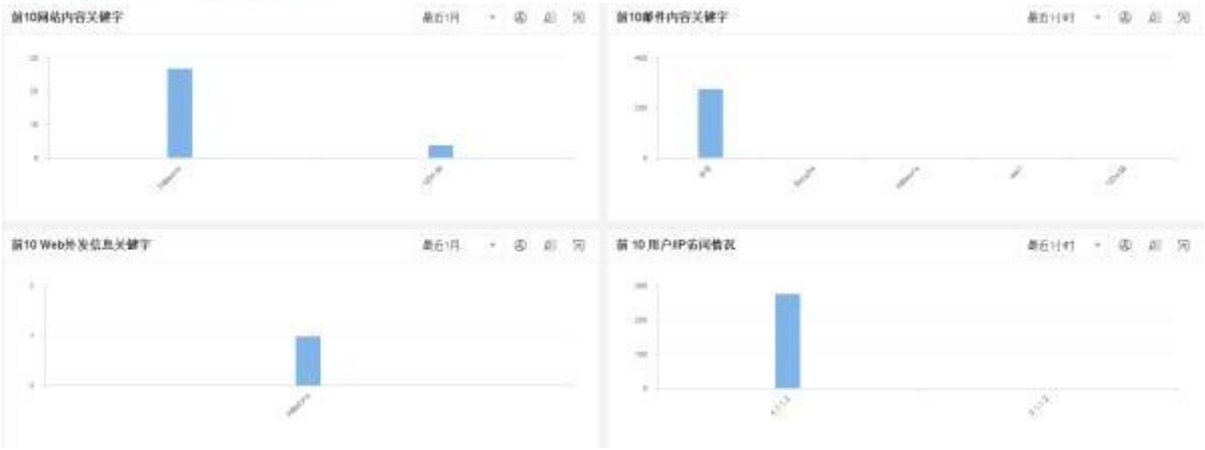
关键字阻断

仅有部分平台支持该功能，请以实际页面为准。

系统配置上网行为控制的"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

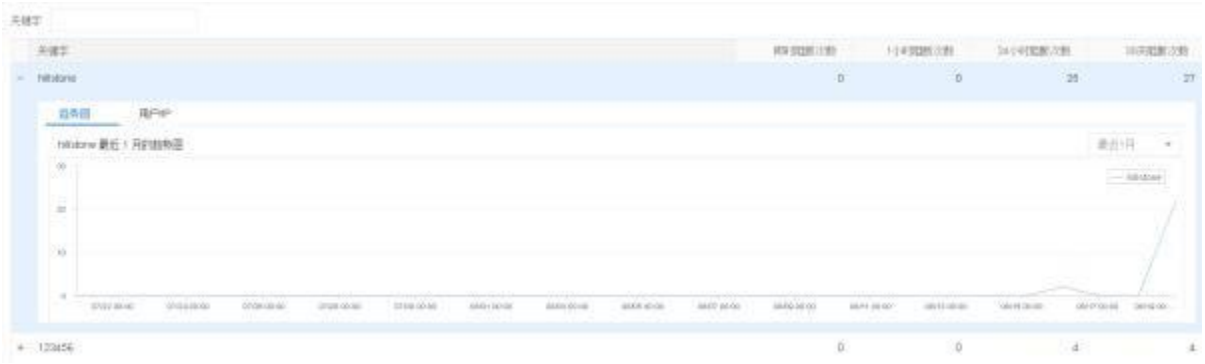
概览页面为用户展示指定时间周期内被阻断次数最多的前　10　网站内容关键字、前　10　邮件内容关键字、前 10 Web 外发信息关键字以及前 10 用户/IP 访问情况统计信息。点击“监控>关键字阻断>概览”。



- 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。

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　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。

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　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。

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. 

3. 在“IPv4 内网监控地址簿”及“IPv5 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。

4. 配置完成，点击“确定”按钮保存所做配置。

自定义监控

仅有部分平台支持该功能，请以实际页面为准。

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 IPv5 功能，系统支持IPv4 和 IPv5 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	UAL 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 UAL 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			
		统计数据类型					

方式	条件	流量	会话	新建会话速率	UAL 访问次数	关键字阻断次数	应用阻断次数
双向	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			
	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(responder)	统计接收会话IP的上行和下行流量	统计接收会话IP的接收和发送会话个数	统计接收会话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	统计不属于某接口的IP的	统计不属于某接口的IP的	统计不属于某接口的IP的			

方式	条件	统计数据类型					
		流量	会话	新建会话速率	UAL 访问次数	关键字阻断次数	应用阻断次数
	belong to interface)	上行和下行流量	接收和发送会话个数	接收和发送新建会话速率			

基于安全域、接口、用户、应用、UAL、UAL 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	UAL 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 UAL 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 UAL 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		统计用户的新	统计用户的	统计用户的关	统计用户的应

组织方式	方式	统计数据类型					
		流量	会话	新建会话速率	UAL 命中次数	关键字阻断	应用阻断次数
	双向	统计用户的上行和下行流量	统计用户的会话个数	建会话速率	UAL 命中次数	键字阻断次数	用阻断次数
UAL	N/A	N/A	N/A	N/A	统计 UAL 命中次数	N/A	N/A
UAL 类别	N/A	N/A	N/A	N/A	统计 UAL 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 UAL 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。

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 ingress)	以入安全域为条件进行过滤
安全域-流 (filter zone zone-name egress)	以 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 (filter interface if-name egress)	以 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 ABCD/M)	以 IP 为条件进行过滤

类型	描述
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
严重级别 (filter severity)	以攻击特征的严重级别为条件进行过滤

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、UAL 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。

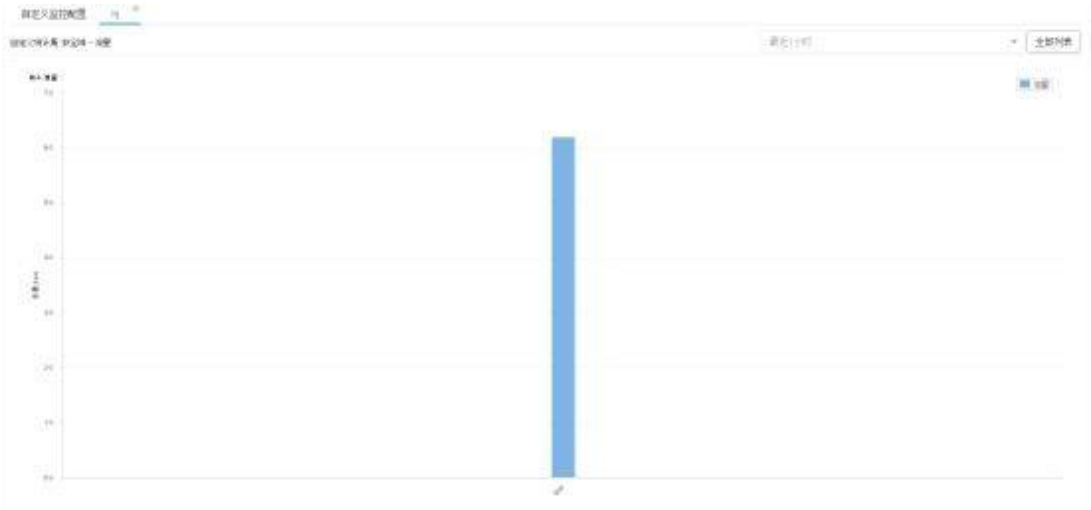
3. 配置完成，点击“确定”按钮。系统将返回自定义监控页面。配置的监控统计集将显示在列表中。

注意:配置统计集时:

- UAL 访问次数统计数据类型仅对安装有UAL 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 UAL 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UAL 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

仅有部分平台支持该功能，请以实际页面为准。

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　窗口，将不能弹　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、UAL 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。

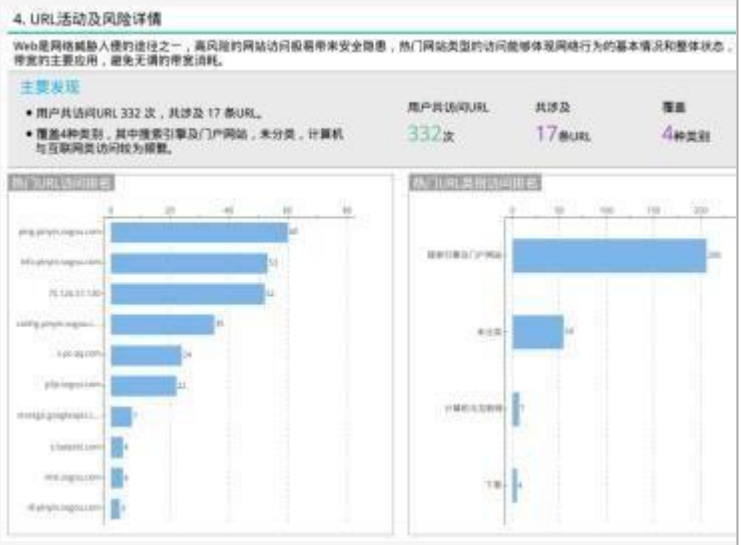
新建自定义报表模板

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。  1. 网络及安全风险概况 • 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。  2. 网络流量详情 主要发现 • 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、

选项	说明
	TOP20 以及 TOP50。 •UAL 活动及风险详情：统计设备的 UAL 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、生成周期和生成时间，以及输方式。

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。

填写报表任务基本配置信息。

选项	说明
报表任务名称 描述	指定报表任务的名称。 指定报表任务的描述信息。

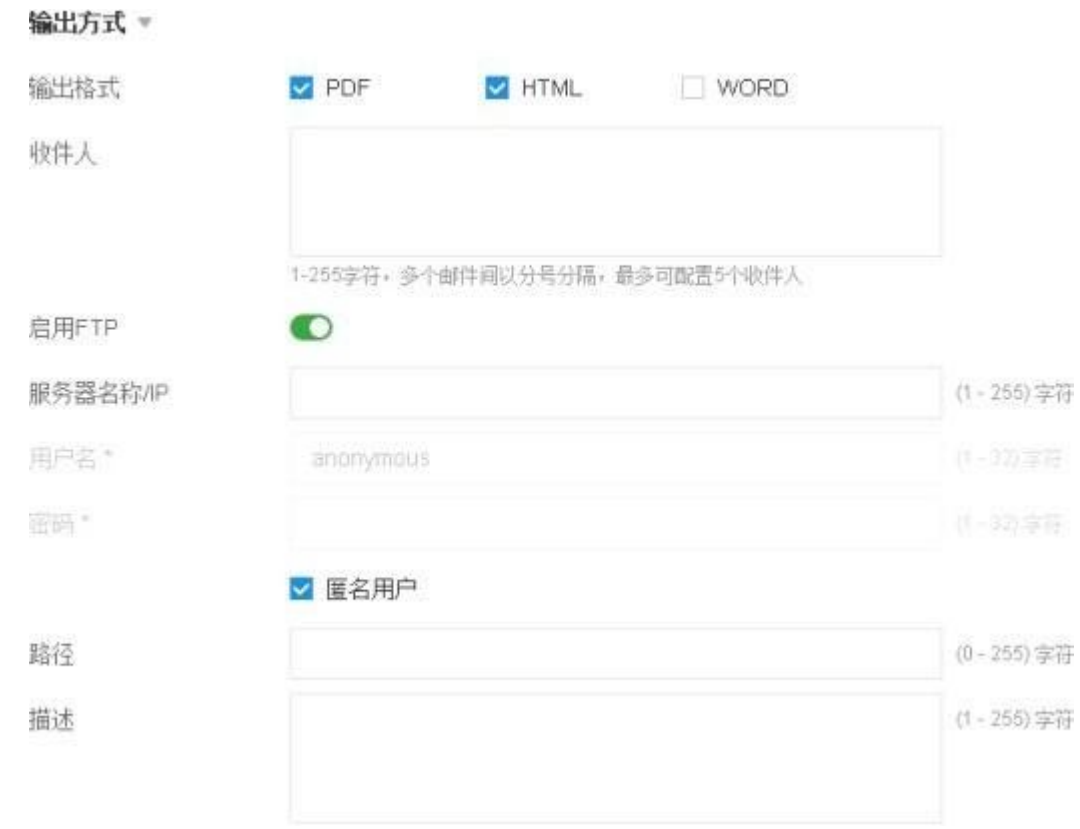
点击“报表模板选择”展开配置项，选择报表任务需要使用的报表模板。

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:

选项	说明
	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“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、最近一月的数据生成报表。 • 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。 • 生成类型：根据指定周期内的数据生成报表。可根据最近一天、最近一月的数据生成报表。



点击“输　方式”展开配置项，填写报表的输　方式信息。

选项	说明
输　格式	指定报表文件的输　格式，包括 PDF 格式、HTML 格式以及 WOAD 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。 • VA: 从下拉菜单选择FTP 服务器所属的虚拟路由器。 • 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。

选项	说明
	•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）。 • 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。

日志

设备支持日志管理功能。记录并输　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 UAL。

- 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。
- UAL 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、UAL 过滤等。
- EPP 日志- 与终端防护相关的日志信息。
- PBA 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_EMEAG
警报（Alerts）	1	需要立即处理的信息，如设备受到攻击等。	LOG_ALEAT
严重（Critical）	2	危急信息，如硬件 错。	LOG_CAIT
错误（Errors）	3	错误信息。	LOG_EAA
警告（Warnings）	4	报警信息。	LOG_WAANING
通告（Notifications）	5	非错误信息，但需要特殊处理。	LOG_NOTICE
信息（Informational）	5	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 目的地

日志信息可以输 到不同的目的地，设备支持以下 7 种日志信息输 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 目的地。用户可以通过命令关闭此输 .
- 终端（Aemote）–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 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 日志信息。该格式为：**时间，级别@模块：日志描述**。请参阅以下示例：

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

事件日志

该功能在不同平台上的呈现方式有所差异，请以实际页面为准。

用户可以在设备系统日志页面查看、搜索或导　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　：点击该按钮，以TXT 或 CSV 格式导　全部或部分日志条目。
- 修改日志参数：点击该按钮，在<日志参数配置>页面，修改日志描述、级别及开启/关闭日志输
  。

网络日志

该功能在不同平台上的呈现方式有所差异，请以实际页面为准。

用户可以在设备系统日志页面查看、搜索或导　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　：点击该按钮，以TXT 格式导　全部或部分日志条目。
- 修改日志参数：点击该按钮，在<日志参数配置>页面，修改日志描述、级别及开启/关闭日志输
  。

配置日志

该功能在不同平台上的呈现方式有所差异，请以实际页面为准。

用户可以在设备系统日志页面查看、搜索或导　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　：点击该按钮，以TXT 或 CSV 格式导　全部或部分日志条目。

- 修改日志参数：点击该按钮，在<日志参数配置>页面，修改日志描述、级别及开启/关闭日志输
  。

共享接入日志

该功能在不同平台上的呈现方式有所差异，请以实际页面为准。

用户可以在设备系统日志页面查看、搜索或导　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　：点击该按钮，以TXT 导　全部或部分日志条目。

威胁日志

该功能在不同平台上的呈现方式有所差异，请以实际页面为准。

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。
- 已经配置、"入侵防御"、"攻击防护"或"边界流量过滤"功能。

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 IPv5 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 IPv5 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。
  - 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。

- 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。

- 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 ：导 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 ）。
- 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，用户可以点击“查看报文”“下载”“加入白名单”“禁用特征”执行相应的操作。
- 在列表中，点击威胁情报图标，查看指定对象的威胁情报，或将光标悬浮在需要查看威胁情报的对象上方，右侧 现 按钮。点击该按钮，选择“查看威胁情报”，在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。
- 清除：点击该按钮，清除所有系统存储会话日志信息。
- 导 ：以.txt 或.csv 格式导 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 ）。

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。

PBA 日志

仅有部分平台支持该功能，请以实际页面为准。

PBA 日志信息的产生需要满足以下两个条件：

- 已经开启设备的PBA 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>PBA 日志”，打开 PBA 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。PBA 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 PBA 日志信息。
  - PBA 名称/规则 ID - 在第一个文本框中输入PAB 名称，在第二个文本框中输入策略路由规则 ID，显示指定 PBA 中的 ID 规则的PBA 日志信息。
  - 源 IP - 显示指定源IP 地址的 PBA 日志信息。
  - 源端口- 显示指定源端口的PBA 日志信息。
  - 目的 IP - 显示指定目的 IP 的 PBA 日志信息。

- 目的端口- 显示指定目的端口的PBA 日志信息。
- 协议- 显示指定协议的PBA 日志信息。
- 应用- 显示指定应用的PBA 日志信息。
- 接口- 显示指定 接口的PBA 日志信息。

- 配置：点击该按钮，进入"日志配置"相关页面对 PBA 日志信息进行配置。
- 清除：点击该按钮，清除所有系统存储PBA 日志信息。
- 导 ：导 所有系统存储的PBA 日志信息或者搜索结果信息（先进行搜索后再导 ）。

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。

- 清除：点击该按钮，清除所有系统存储NAT 日志信息。
- 导　：导　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　）。

UAL 日志

仅有部分平台支持该功能，请以实际页面为准。

UAL 日志信息的产生需要满足以下条件：

- 已经开启设备的UAL 日志功能。
- 已经为 UAL 过滤规则开启日志记录功能。

点击“监控>日志>UAL 日志”，打开 UAL 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。UAL 日志过滤条件如下：
- 消息－　显示包含指定消息的UAL　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 UAL 日志信息进行配置。
- 清除：点击该按钮，清除所有系统存储UAL 日志信息。
- 导　：点击“导　”按钮，指定分隔符后，导　所有系统存储的 UAL 日志信息或者搜索结果信息（先进行搜索后再导　）。

EPP 日志

用户可以在 EPP 日志页面查看、配置、清除或导　EPP 日志。

点击“监控>日志>EPP 日志”，打开 EPP 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，进入日志管理相关页面对EPP　日志信息进行配置。
- 清除：点击该按钮，清除所有系统存储的EPP 日志信息。
- 导　：点击该按钮，以TXT 或 CSV 格式导　全部或部分日志条目。

文件过滤日志

仅有部分平台支持该功能，请以实际页面为准。 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 

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 ：点击“导 ”按钮，指定分隔符后，导 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 ）。

内容过滤日志

仅有部分平台支持该功能，请以实际页面为准。 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"网页关键字"、"Web 外发信息"、"邮件过滤"或者"应用行为控制"功能。

点击“监控>日志>内容过滤日志信息”，打开内容过滤日志页面。

- 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　：点击“导　”按钮，指定分隔符后，导　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　）。

上网行为审计日志

仅有部分平台支持该功能，请以实际页面为准。

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　：点击“导　”按钮，指定分隔符后，导　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　）。

云沙箱日志

该功能在不同平台上的呈现方式有所差异，请以实际页面为准。 用

户可以在云沙箱日志页面查看、配置、清除或导　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 IPv5。
- 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。
- 清除：点击该按钮，清除所有系统存储的云沙箱日志信息。
- 导　：点击该按钮，以TXT 或 CSV 格式导　全部或部分日志条目。

日志管理

该功能在不同平台上的呈现方式有所差异，请以实际页面为准。

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>/<UAL 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>/<EPP 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。
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 到 Console。 •最小日志级别- 指定输 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 到终端。 • 最小日志级别- 指定输 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 到缓存。 •最小日志级别- 指定输 事件日志信息的最小日志级别。 •最大缓存大小- 指定输 事件日志信息的最大缓存大小。
文件	选中该复选框将事件日志信息输 到文件。 •最小日志级别- 指定输 事件日志信息的最小日志级别。 •最大文件大小- 指定日志信息文件的最大值。范围是 4095 到 1048575 字节。默认是 1048575 字节。

选项	说明
日志服务器	选中该复选框将事件日志信息输　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　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　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　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　到手机短信。 •最小日志级别-　指定输　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　到缓存。 • 最大缓存大小- 指定输　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　到文件。 •最大文件大小- 指定日志信息文件的最大值。范围是 4095 到 1048575 字节。默认是 1048575 字节。
日志服务器	选中该复选框将网络日志信息输　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

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　到缓存。 •最大缓存大小-　指定输　配置日志信息的最大缓存大小。

选项	说明
日志服务器	选中该复选框将配置日志信息输　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　最大速率。 •最大速率- 指定输　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　到缓存。 •最大缓存大小-　指定输　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　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　到缓存。 •最大缓存大小- 指定输　NAT 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 NAT 日志信息输　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

EPP 日志

选项	说明
启用	点击“启用”按钮，开启系统的 EPP 日志功能。
终端	选中该复选框将 EPP 日志信息输　到终端。 •最小日志级别- 指定输　EPP 日志信息的最小日志级别。
缓存	选中该复选框将 EPP 日志信息输　到缓存。 •最小日志级别- 指定输　EPP　日志信息的最小日志级别。 •最大缓存大小- 指定输　EPP　日志信息的最大缓存大小。
文件	选中该复选框将 EPP 日志信息输　到文件。 •最小日志级别- 指定输　EPP　日志信息的最小日志级别。 •最大文件大小- 指定日志信息文件的最大值。范围是 4095 到 1048575 字节。默认是 1048575 字节。
日志服务器	选中该复选框将 EPP 日志信息输　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　EPP　日志信息的最小日志级别。 •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 EPP 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

选项	说明
	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 EPP 日志信息输 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 EPP 日志信息的最小日志级别。

UAL 日志

选项	说明
启用	点击“启用”按钮，开启系统的 UAL 日志功能。 •记录主机名：在UAL 日志中显示主机名称。
缓存	选中该复选框将 UAL 日志信息输 到缓存。 •最大缓存大小- 指定输 UAL 日志信息的最大缓存大小。
日志服务器	选中该复选框将 UAL 日志信息输 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 到缓存。 •最大缓存大小- 指定输 文件过滤日志信息的最大缓存大小。

选项	说明
日志服务器	选中该复选框将文件过滤日志信息输　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　到缓存。 •最大缓存大小- 指定输　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　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　到缓存。 •最大缓存大小- 指定输　上网行为审计日志信息的最大缓存大小。

选项	说明
日志服务器	选中该复选框将上网行为审计日志信息输　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。
终端	选中该复选框将威胁日志选项输　到终端。
缓存	选中该复选框将威胁日志信息输　到缓存。 •最大缓存大小-　指定输　威胁日志信息的最大缓存大小。 •最小日志级别-　指定输　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　到文件。 •最小日志级别-　指定输　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 4095 到 1048575 字节。默认是 1048575 字节。
日志服务器	选中该复选框将威胁日志信息输　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
Email 地址	选中该复选框将威胁日志信息输　到 Email 地址。

选项	说明
	•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 到缓存。 •最大缓存大小- 指定输 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 到文件。
日志服务器	选中该复选框将云沙箱日志信息输 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 到 Console。
缓存	选中该复选框将共享接入日志信息输 到缓存。 •最大缓存大小- 指定输 共享接入日志信息的最大缓存大小。
日志服务器	选中该复选框将共享接入日志信息输 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。

日志配置

该功能在不同平台上的呈现方式有所差异，请以实际页面为准。

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。

选项	说明
主机名称	指定日志服务器的主机名称。

在<日志服务器配置>页面，配置日志服务器相关信息。

选项	说明
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。
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。

设置日志编码

输　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　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:

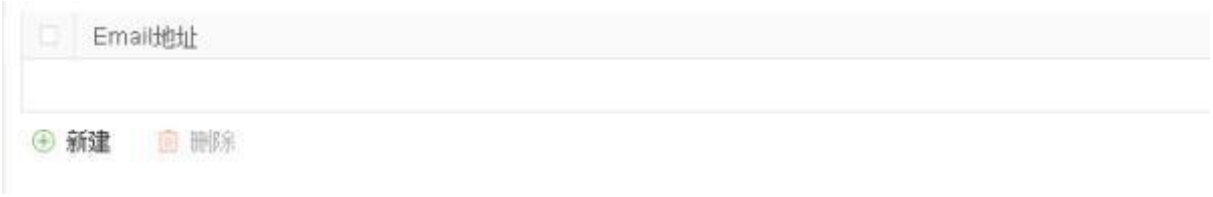
1. 点击“监控>日志>日志配置”，选择“日志服务器配置”标签页。
2. 点击右上角“日志编码设置”按钮，打开<日志编码配置>页面。
3. 点击“启用”按钮，启用日志GBK 编码。
4. 点击“确定”按钮，保存当前配置。

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　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　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　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　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
。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 11 章 分析诊断

仅有部分平台支持该功能，请以实际页面为准。

- 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　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　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

仅有部分平台支持该功能，请以实际页面为准。

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　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 > 诊断工具> 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。

名称	指定在线抓包任务的名称。
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。

选项	说明
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。

5.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　”按钮，导　抓包文件，导　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。

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 > 诊断工具> 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。 •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。 •IPv5/前缀长度：在文本框中输入 IPv5 类型的源地址及前缀长度，不输入表示any。 •IPv5 范围：在文本框中输入 IPv5 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。 •IPv5/前缀长度：在文本框中输入 IPv5 类型的目的地址及前缀长度，不输入表示any。

选项	说明
应用 协议	• IPv5 范围：在文本框中输入 IPv5 类型的目的地址范围，不输入表示any。 • 目的 UAL：在文本框中输入目的 UAL，不输入表示 any 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。 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 > 诊断工具> 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 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 > 诊断工具> 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VA。
3. 在“DNS 查询”文本框中输入需要查询的域名。
4. 点击“DNS 查询”对应的“测试”按钮，检测结果会显示在下方的文本框中。

Ping

使用工具Ping 进行网络连通测试，请按照以下步骤进行操作:

1. 选择“系统 > 诊断工具> 测试工具”，进入测试工具页面。
2. 在“虚拟路由器”下拉列表中选择VA。
3. 在“Ping”文本框中输入网络对端的 IP 地址。
4. 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。
5. 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 Destination Host Not Aesponsed 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 IPv5 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 > 诊断工具> 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VA。
3. 选择“IPv4”或“IPv5”，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 12 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的硬件平台、固件版本，均启用VA 及防病毒功能、安装防病毒许可证的安全网关，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。

安全网关支持 HA 的 3 种工作模式：Active-Passive（A/P）模式、Active-Active（A/A）模式和 Peer 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 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。
- Active-Active（A/A）模式：当设备处于 NAT 模式、路由模式或两者的组合时，可以将HA 簇中的两台设备都配置成主动，使两台设备同时运行各自的工作，且相互监测对方的情况。当其中一台设备发生故障时，另外一台设备运行其自身的工作并且接管故障设备的工作，以保证工作不间断，该模式称为Active-Active 模式。这种A/A 模式具有高性能以及负载均衡的优点。
- Peer 模式：该模式是一种特殊的 HA Active-Active 模式。处于Peer 模式下的两台设备都处于主动状态且同时运行各自的工作、相互监测对方的情况。当其中一台设备发生故障时，另外一台设备运行其自身的工作并且接管故障设备的工作。在Peer 模式下，只有处于主动状态的设备的接口可以正常收发报文；处于禁用状态的设备可使 2 台设备的配置信息保持一致，但其接口不收发任何报文。

  Peer 模式配置更加灵活，比较适合在非对称路由环境中部署。

仅有部分平台支持HA（A/A）模式和 Peer 模式，请以实际页面为准。

HA 基础概念

HA 簇

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

HA 组

系统会对HA 簇中相同 HA 组 ID 的设备，按照 HCMP 协议，根据设备的HA 配置，进行主备选举。主设备处于活动状态处理网络流量，而当主设备 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 Active-Active （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 ADO （Auntime Dynamic Object） 。ADO 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
- AAP 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

该功能在不同平台上的呈现方式有所差异，请以实际页面为准。

使用高可靠性功能，用户需要按照以下步骤进行配置:

1. 配置 HA 组的接口。
2. 配置 HA 连接。包括 HA 连接接口和连接接口IP 的配置。用于设备同步以及传输HA 报文。
3. 配置 HA 簇。为设备指定HA 虚前缀（可选）和 HA 簇 ID，并且开启设备的HA 功能。
4. 配置 HA 组。HA 组的配置包括指定设备优先级（选举使用）以及设备HA 报文相关参数等。

配置HA，请按照以下步骤进行操作:

1. 选择“系统 > HA”，进入 HA 配置页面。

   在该页面配置HA。

选项	说明
HA 控制连接接口 1	指定HA 控制连接接口的名称。控制连接同步两台设备间的所有数据。
HA 控制连接接口 2	指定HA 控制连接接口的名称（备份设备）。
HA 辅助链路接口	指定 HA 辅助链路接口的名称。在Active-Passive（A/P）模式中，为了避免当 HA 连接发生故障时 HA 设备的主备状态 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。 •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。

选项	说明
	•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。
HA 数据连接接口	指定HA 数据连接接口的名称。数据连接仅同步数据报文信息，如会话信息。指定后，会话信息将通过 HA 数据连接接口同步完成。目前仅支持将物理接口和集聚接口配置为数据连接的接口。用户最多可以指定 1 个 HA 数据连接接口。
IP 地址	指定 HA 连接接口的 IP 地址及网络掩码，可以为 IPv4 地址或者 IPv5 地址。当指定IPv4 类型的地址时，输入格式为A.B.C.D/M（比如：1.1.1.1/24）；当指定 IPv5 类型的地址时，输入格式为 X.X.X.X::X/M（比如：2001::1/54），“X.X.X.X::X”为 IPv5 地址前缀，“M”为前缀长度且取值范围为 1 到 128。
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。
节点 ID	开启 HA 功能后，用户需为设备指定节点 ID（HA Node），两台设备需指定不同的节点 ID。范围是 0 到 1。
Peer-mode	点击“启用”按钮开启 HA Peer 模式，并标识该设备在 HA 簇中的角色。范围是 0 到 1。默认情况下，HA 节点 ID 为 0 的设备上的组 0 为主动状态，节点 ID 为 1 的设备上的组 0 为禁用状态。
对称路由	若指定该参数，设备将工作在对称路由模式下。
HA 簇 ID	指定 HA 簇 ID。当前缀设置为七位时，取值范围为 1~128；当前缀设置为八位或者不设置时，取值范围为 1~8。当选择 HA 簇 ID 为无时表示关闭设备的 HA 功能。
HA 同步配置	某些特殊情况下，可能 现主备配置信息不同步现象。此时，需要用户手动同步主备设备的配置信息。点击“HA 同步配置”按钮，完成配置信息同步。
HA 同步会话	默认情况下，HA 设备之间会自动同步会话信息。同步会话会产生一定流量，在高负载情况下可能会对设备性能造成影响。用户可以根据设备负载情况使用 HA 会话自动同步功能，以确保设备的稳定性。点击“HA 同步会话”按钮，启用 HA 会话自动同步功能。
组 0	

选项	说明
新建	默认情况下，指定HA 簇 ID 后，系统自动创建组 0。点击“新建”按钮， 可创建组 1 并对其进行配置。
删除	若已创建HA 组 1，用户可点击“删除”按钮将组 1 配置删除。
优先级	指定当前设备在 HA 组中的优先级。优先级高（数字小）的会被选举为主设备。
抢占时间	指定当前设备是否开启抢占模式以及抢占延迟时间。如果将设备配置为抢占模式，一旦设备发现自己的优先级高于主设备，就会将自己升级为主设备，而原先的主设备将变为备份设备。如果输入 0，则表示不开启抢占模式；即使设备的优先级高于主设备，它也只能在主设备故障时代替主设备工作。
Hello 报文间隔	输入HA 设备向HA 组中的其它设备发送 Hello 报文的时间间隔。同一个 HA 组的设备的Hello 报文间隔时间必须相同。
Hello 报文警戒值	输入HA 组对应的 Hello 报文的警戒值，即如果设备没有收到对方设备的该命令指定个数的 Hello 报文，就判断对方无心跳。
免费AAP 包个数	指定当前设备选举为主设备后，发送 AAP 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AAP 请求包，通知相关网络设备更新其AAP 表。
监测对象	指定已配置的监测对象的名称。系统利用监测对象监控设备的工作状态。一旦发现设备不能正常工作，立即采取相应措施。
描述	指定该 HA 组的描述信息。

2. 点击“发送”按钮，完成配置。

第 13 章 系统管理

设备的系统维护与管理主要包括以下各项:

- ″系统信息″
- ″管理设备″
- ″管理配置文件″
- ″告警页面管理″
- ″设置 SNMP″
- ″升级管理″
- ″配置邮件服务器″
- ″测试工具″

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	显示云•界的 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。 • Master：HA 主状态，表示当前设备为 HA 组的主设备。 • Backup：HA 备状态，表示当前设备为HA 组的备份设备。 • Failed：故障状态，表示当前设备故障。
软件版本	显示设备当前的软件版本。
启动文件	显示设备当前的启动文件版本。
特征库信息 应用特征库	显示设备的应用特征库当前版本，以及上次更新时间。
UAL 分类库	显示设备的 UAL 特征库当前版本，以及上次更新时间。
沙箱白名单	显示设备的沙箱白名单当前版本，以及上次更新时间。
IP 信誉特征库	显示设备的 IP 信誉特征库当前版本，以及上次更新时间。
病毒过滤特征库	显示设备的病毒特征库当前版本，以及上次更新时间。
入侵防御特征库	显示设备的入侵防御特征库当前版本，以及上次更新时间。

系统信息	
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，以及上次更新时间。

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。

管理员

设备的管理员根据角色的不同，对系统可执行的管理和配置权限不同。系统支持预定义管理员角色和自定义管理员角色。

系统默认预定义如下四类管理员角色，这四类管理员角色不可被删除和编辑:

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

下表为管理员的详细权限列表:

功能	系统管理员	系统管理员（只读）	安全审计员	安全操作员
配置（包括保存配置）	√	x	x	√
管理员配置	√	x	x	x
恢复 厂配置	√	x	x	x
删除配置文件	√	x	x	√
回退起始配置信息	√	x	x	√
重启设备	√	x	x	x
查看配置信息	√	√	x	√
查看日志信息	√	√	√	x
修改当前管理员密码	√	√	√	√

功能	系统管理员	系统管理员（只读）	安全审计员	安全操作员
ping/traceroute	√	√	x	√

注意:

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

新建管理员

新建管理员，请按照以下步骤进行操作:

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

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

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

配置默认管理员登录操作

系统拥有一个默认管理员“ ”以及对应的默认密码“ ”，当用户使用默认管理员和默认密码登录设备时，可能会存在被破解的风险。针对该问题，系统将会在用户使用默认管理员和密码登录设备时，提示用户可以进行以下操作：

- 删除并创建管理员：点击“删除并创建管理员”单选按钮，删除默认管理员（）并在下方文本框中指定新用户名、密码等信息进行新建管理员。创建新管理员后，使用新的管理员和密码重新登录

系统。

- 修改密码：点击“修改密码”单选按钮，在下方文本框中指定默认管理员的新密码，在修改后，使用新的密码重新登录系统。

- 忽略本次提示：点击右上角“忽略本次提示”单选按钮，将会使用默认管理员（）和密码（）立即登录，下次使用默认管理员和密码登录时将继续弹　该提示。
- **为了您的业务安全，请不要使用默认密码，并定期对您的密码进行修改。建议密码长度不小于8个字符，包含大写字母、小写字母、数字和特殊符号中的至少3种，并且每3个月更换一次密码。如您需要技术人员协助修改密码，请通过官网工单系统或拨打400-810-9889热线电话与我们联系。**

注意:在HA Active-Passive （A/P）模式下，备设备不支持该功能，可以使用默认管理员直接登录。

管理员角色

设备的管理员根据角色的不同，对系统可执行的管理和配置权限不同。系统支持预定义管理员角色和自 定义管理员角色。系统预定义的管理员角色不可被删除和编辑。用户可自定义管理员角色满足实际需求。

新建管理员角色，按照以下步骤进行操作:

1. 选择“系统＞设备管理＞管理员角色”，进入到管理员角色配置页面。
2. 点击“新建”按钮，打开<管理员角色配置>页面。

配

选项	说明
管理员角色	指定管理员角色的名称。
CLI	指定管理员角色的 CLI 权限，“可用”或“不可用”。
WebUI 权限	通过点击各个模块的名称调整管理员角色在 WebUI 上对各个模块的权限。 表示对模块具有读写权限，可在 WebUI 查看并修改模块的配置； 表示对模块具有读权限，可在 WebUI 查看此模块配置，但无法修改配置； 表示对模块无权限，管理员角色无法在 WebUI 查看到此模块。
描述	用户可根据需要指定管理员角色的描述信息。

3. 点

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 地址范围，或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。

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
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 地址范围，只有在指定 IP 范围内的主机可以为可信主机；选择“IPv4&MAC”时，需指定 IP 地址范围和 MAC 地址或范围，只有同时符合指定条件的主机可以为可信主机。
IP 类型	指定可信主机的 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 地址或范围： •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 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 Consoe 管理口登录的参数信息。 •超时：输入 Console 登录的超时时间。单位为分钟，取值范围为 0 到 50，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。
选项	说明

	• 超时：输入 Telnet 登录的超时时间。单位为分钟，取值范围为 1 到 50，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 55535，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 50，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 55535，默认值为 22。
Web	配置 WebUI 登录的参数信息。 • 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 。 • 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 55535，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 55535，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。

选项	说明
	•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“设置系统时间”处进行配置。**

选项	说明
与本地时间同步	选择需要同步本地时间的方式，选择“仅同步时间”或“同步时区与时间”按钮。 •仅同步时间：使系统时间与本地电脑时间同步。 •同步时区与时间：使系统时区和时间与本地电脑的时区和时间同步。
指定系统时间	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“设置NTP”模块进行配置。**

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。
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VA。 • 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 55535。
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。

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　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。
系统信息语言	选择系统提示（如日志、错误提示）所使用的语言，可选中文或者英文。
管理员认证服务器	在下拉菜单中选择系统管理员认证服务器。
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账户登录设备。
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 55535 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 15，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 15，默认值为 2。 •小写字母最小长度： 取值范围为 0 到 15，默认值为 2。 •数字最小长度： 取值范围为 0 到 15，默认值为 2。 •特殊字符长度： 取值范围为 0 到 15，默认值为 2。 •密码有效期：单位为天， 取值范围为 0 到 355，默认值为 0，表示不对有效期进行限制。

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　的设备故障文件对错误进行诊断和定位。

导　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　”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　。

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，UAL 过滤、数据安全、沙箱防护、病毒过滤、僵尸网络。

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，通过短信认证或邮箱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. 点击“确定”按钮保存所做配置。

存储管理

存储管理功能可以帮助用户通过删除日志或停止记录日志，从而管理系统存储空间。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. 点击“启用”按钮，开启存储管理功能，并配置如下选项:

选项	说明
启用	点击“启用”按钮，开启存储管理功能。
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 1%~90%，存储空间取值范围为 1~512000M。
动作	当达到指定的阈值时，系统将执行指定的动作。选择动作，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。如需备份删除的日志，可继续配置 FTP 服务器。配置后，被删除的日志将转存至FTP 服务器。如不配置 FTP 服务器，系统将直接删除日志。 •停止记录：系统将停止存储新的日志。

3. （可选）当动作选择为“覆盖最早的数据”时，可以继续配置 FTP 服务器，被删除的日志将转存至 FTP 服务器。

选项	说明
启用FTP	点击“启用 FTP”按钮，启用日志备份功能。
IP 地址	指定用于备份日志的 FTP 服务器的 IP 地址。

选项	说明
用户名	指定登录FTP 服务器的用户名。
密码	指定登录FTP 服务器的密码。
匿名用户	当点击“匿名用户”的“启用”按钮时，不需要输入用户名和密码，即可登录 FTP 服务器。
路径	指定FTP 服务器上存储日志的文件路径。

4. 点击“确定”按钮，保存所做配置。

管理配置文件

该功能在不同平台上的呈现方式有所差异，请以实际页面为准。

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 、删除已创建的系统配置文件，也可以导 当前的系统配置。

备份/恢复配置文件

管理配置文件，请按照以下步骤进行操作:

1. 选择“系统 > 配置文件管理> 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 ：选中需要导 的配置文件前的复选框，然后点击列表上方的“导 ”按钮。
    - 删除：选中需要删除的配置文件前的复选框，然后点击列表上方的“删除”按钮。
    - 备份恢复：将系统配置恢复到已保存的配置文件或 厂配置，也可以备份当前的系统配置信息。

配置信息如下。

选项	说明
备份当前配置	在“配置描述”文本框中为备份的系统配置文件添加描述信息。点击“开始备份”按钮进行备份。
恢复配置	恢复到已备份配置: •选择备份配置文件：点击“选择备份配置文件”按钮，从已备份配置文件列表中选择需要的系统配置文件。点击“确定”按钮。 •本地上传配置文件：点击“本地上传配置文件”按钮，在<导入配置文件>对话框中，点击“浏览”按钮，并选中需上传的本地配置文件。如需要使配置立即生效，选中复选框，点击“确定”按钮。 恢复　厂配置: • 点击“恢复”按钮，弹　“恢复　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　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　当前配置文件，点击页面下方的“导　”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。
5. 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 5 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。

- UAL 过滤监控用户通知：通知 UAL 过滤功能将扫描用户流量。
- UAL 过滤阻断用户通知：通知用户流量被 UAL 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 5 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“UAL 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。
%%IGNOAE_WAANING%%	用于在页面显示按钮，用户点击该按钮可以 略提示并继续浏览。 **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 图片。
%%UALFILTEA_AEASON%%	用于在“UAL 过滤阻断用户通知”页面中显示 UAL 过滤阻断的原因。

引用串	含义
	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。
%%VIAUS_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。
%%CONTENTFILTEA_AEASON%%	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 AFC-1213 中定义的所有相关的管理信息库组和 AFC-2233 中定义的使用 SMIv2 的接口组 MIB（The Interfaces Group MIB using SMIv2：IF-MIB）。此外，系统提供一个私有 MIB 库，MIB 库中包含系统的系统信息、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。
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。

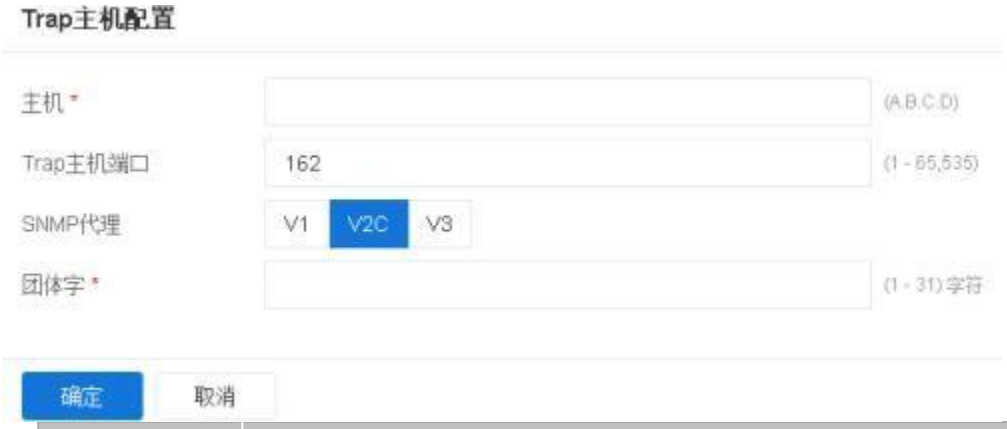
3. 点击“确定”按钮保存所做的配置。新创建的SNMP 主机将会显示在 SNMP 主机列表中。

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。

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
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无（无认证和加密）、认证（提供基于MD5 或 SHA 算法的认证）或者认证&加密（提供基于 MD5 或 SHA 算法的认证和基于AES 和 DES 的报文加密）。
可读视图	选择该用户组的只读 MIB 视图名。如不指定该参数，系统默认为空。
写视图	选择该用户组的可写 MIB 视图名。如不指定该参数，系统默认为空。

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。
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AAP 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 55535。默认值为 151。
团体字	在文本框中输入 SNMPv1 或者 SNMPv2C 的团体字。
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AAP 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 AAP 信息的时间间隔，单位为秒，范围是 5 到 1800 秒，默认值是 50 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，也可以指定共享接入特征库、应用特征库、UAL 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的升级配置，还可以配置可信根证书库的升级信息。

升 级 版 本

升级特征库

用户只能查看到已安装的许可证的特征库。系统可以安装的特征库包括共享接入特征库、应用特征库、UAL 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。

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。
远程升级	在共享接入特征库、应用特征库、UAL 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相应模块配置对应特征库远程升级参数。 •升级服务器：设备提供两个默认特征库更新服务器，分别是 https://update1. net.com 和 https://update2. net.com。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。 •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。 在风险减缓规则特征库、异常行为模型库和恶意软件行为模型库相应模块配置对应特征库远程升级参数。

选项	说明
本地升级	•服务器：设备提供一个默认特征库更新服务器为https://sec-cloud.net.com。 •自动升级配置：点击“自动升级配置”的“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。 点击“本地升级”按钮，并上传本地升级文件。在各特征库升级模块，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 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，分别是 https://update1.net.com 和 https://update2.net.com。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。

选项	说明
本地升级	•确定并在线升级：点击该按钮，立即升级可信根证书库。 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。

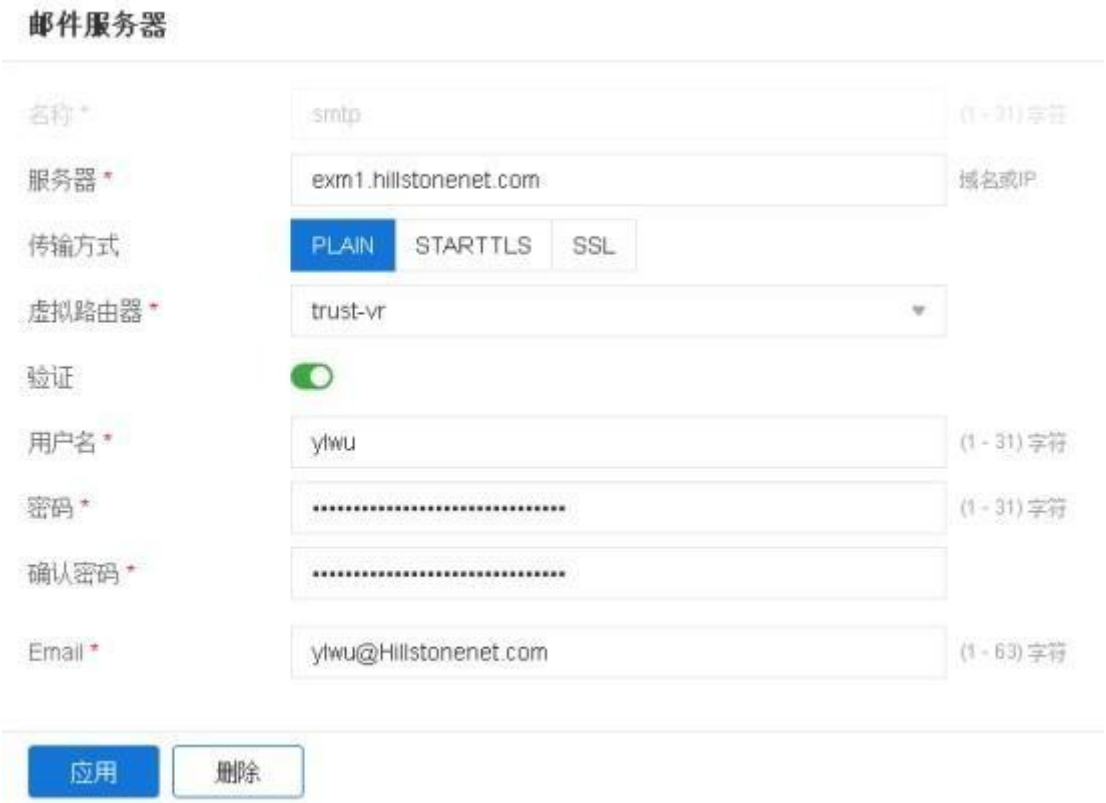
配置邮件服务器

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。
服务器	在文本框输入邮件服务器的域名或者 IP 地址。

选项	说明
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。 •STAATTLS：STAATTLS 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 55535。不同传输方式下的默认端口号不同，PLAIN：25，STAATTLS：25，SSL：455。
虚拟路由器	从下拉菜单中选择邮件服务器的 VA。
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。
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。
服务商名称	指定服务商名称。取值范围是 1 至 31 个字符。
UMS 协议 协议	当协议类型指定为“UMS”时，用户可以指定 UMS 协议类型。默认情况下，使用 HTTPS。 当协议类型指定为“ACC”或者“ALIYUNSMS”时，用户可以指定协议类型。默认情况下，使用 HTTP。
虚拟路由器	指定短信网关所属的 VAouter。系统有一个默认 VAouter，即 trust-vr，同时系统支持多 VA。
网关主机	指定短信网关主机的名称和 IP 地址。

选项	描述
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 9500。
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 4294957295。
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。取值范围是 1 至 31 个字符。
密码	指定登录短信网关的用户名称对应的密码。取值范围是 1 至 31 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。
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。

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　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. 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 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 > 诊断工具> 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VA。
3. 在“DNS 查询”文本框中输入需要查询的域名。
4. 点击“DNS 查询”对应的“测试”按钮，检测结果会显示在下方的文本框中。

Ping

使用工具Ping 进行网络连通测试，请按照以下步骤进行操作:

1. 选择“系统 > 诊断工具> 测试工具”，进入测试工具页面。
2. 在“虚拟路由器”下拉列表中选择VA。
3. 在“Ping”文本框中输入网络对端的 IP 地址。
4. 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。
5. 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 Destination Host Not Aesponsed 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 IPv5 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>诊断工具>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VA。
3. 选择“IPv4”或“IPv5”，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。