安全业务管理平台 Web 登录与简介

对浏览器的要求

推荐使用的浏览器及版本为：Chrome57 及以上版本，推荐分辨率为 1600*900。

首次登录安全业务管理平台

安全业务管理平台设置有缺省的 Web 登录信息 ,用户可以直接使用缺省登录信息通过 HTTPS 服务登录设备的 Web 界面。缺省的 Web 登录信息如下表所示。

用户名/密码	用户角色	用户权限
sysAdmin/sysAdmin	系统管理员	管理系统配置、区域、资产
buzAdmin/buzAdmin	业务管理员	管理各类安全业务
admin/admin@admin	超级管理员	所有权限
auditAdmin/auditAdmin	审计管理员	查看日志记录

在 Chrome 浏览器地址栏输入安全业务管理平台的 IP 地址，即可进入登录界面。首次登录建议使用超级管理员用户登录。

登录设备后，可以进入“系统配置 > 系统管理 > 角色及权限管理 > 用户管理”页面，修改用户的密码，以提高安全性；还可以创建新的用户，以方便对设备进行管理。

Web页面布局介绍

用户登录Web后，能够看到的页面导航内容、能够执行的操作与该用户的角色有关。

图-1 Web 页面布局

（1）标识和面板区	（2）导航栏	（3）执行区

如上图所示，Web 页面有以下几个功能区域：

- 标识和面板区：该区域用来显示公司 Logo、系统名称、功能面板、当前登录用户信息，并提供显示通知消息、退出登录、更改系统主题、全屏展示功能。
- 导航栏：以树的形式组织设备的 Web 功能菜单。用户在导航栏中可以方便的选择功能菜单，选择结果显示在执行区中。
- 执行区：进行配置操作、信息查看、操作结果显示的区域。

退出Web登录

为保证设备的安全性，用户在 Web 上完成操作后应及时退出登录。单击 Web 页面右上角用户名后的  按钮，选择注销，即可退出 Web。

首页

首页展示资产资源使用情况以及网络安全概况。包括 CPU 利用率、内存利用率、会话趋势图、IPS 攻击目的 IP 的 Top 50 事件、Top 50 的 IPS 攻击源 IP 和目的 IP、IPS 阻断 Top 50 事件、攻击事件趋势图和设备日志接收趋势图。

单击<参数设置>按钮，可通过设置资产名称、时间范围以及刷新时间，展示用户关心的数据。

安全分析

本功能可对主平台或子平台所管理的设备上报的漏洞攻击和病毒攻击日志进行汇总、分析，生成安全事件。并从攻击趋势、事件级别、事件类型等多个维度展示分析结果。

攻击趋势

攻击趋势页面用于展示统计时间段内，主平台或子平台上报的攻击事件的攻击趋势。

用户可通过单击列表中“全部事件数”或“阻断事件数”列下的统计值，跳转到详情界面，查看相应的日志详情。

参数说明：

- 时间：事件统计时间，例如，统计时间为 1 天，则每 15 分钟统计一次。
- 全部事件数：该统计时间段内发生的所有攻击事件数。
- 阻断事件数：该统计时间段内发生的阻断事件数。
- 阻断事件比例（%）：阻断事件在同时段全部事件中所占比例。

事件级别

事件级别页面用于展示统计时间段内，主平台或子平台上报的攻击事件的严重级别分布情况。

选择“安全分析 > 安全事件分析”页面，单击页面右上角<>按钮，在弹出的分析选项页面中，配置统计对象为事件级别，其他选项可根据需要进行配置。单击<确认>按钮，即可查看攻击事件的严重级别分布情况。

用户可通过单击列表中“严重”、“高危”、“中危”或“低危”列下的统计值，跳转到详情界面，查看相应的日志详情。

参数说明：

- 时间：事件统计时间，例如，统计时间为 1 天，则每 15 分钟统计一次。
- 严重：该统计时间段内所有严重级别的攻击事件数。
- 高危：该统计时间段内所有高危级别的攻击事件数。
- 中危：该统计时间段内所有中危级别的攻击事件数。
- 低危：该统计时间段内所有低危级别的攻击事件数。

目的端口

目的端口页面用于展示统计时间段内，主平台或子平台上报的端口被攻击的情况。

选择“安全分析 > 安全事件分析”，单击页面右上角<>按钮，在弹出的分析选项页面中，配置统计对象为“目的端口”，其他选项可根据需要配置。单击<确认>按钮，即可查看目的端口的统计信息。

用户可通过单击列表中“目的端口”和“事件数”列下的统计值，或者单击操作列下的<>按钮，跳转到详情界面，查看相应的日志详情。

参数说明：

- 目的端口：统计时间段内被攻击的端口。
- 事件数：统计时间段内端口发生的攻击事件数。
- 百分比（%）：统计时间段内该端口发生的攻击事件在所有端口攻击事件中所占比例。

事件类型

事件类型页面用于展示统计时间段内，主平台或子平台上报的攻击事件的类型分布情况。

选择“安全分析 > 安全事件分析”，单击页面右上角<>按钮，在弹出的分析选项页面中，配置统计对象为事件类型，其他选项可根据需要选择。单击<确认>按钮，即可查看攻击事件的类型分布情况。

用户可通过单击列表中“事件类型”和“事件数”列下的统计值，或者单击操作列下的<>按钮，跳转到详情界面，查看相应的日志详情。

参数说明：

- 事件类型：统计时间段内发生的攻击事件类型。
- 事件数：统计时间段内该类型事件发生次数。
- 百分比（%）：统计时间段内该类型事件在所有类型事件中所占比例。

事件协议

事件协议页面用于展示统计时间段内，主平台或子平台上报的攻击事件的协议分布情况。

选择“安全分析 > 安全事件分析”，单击页面右上角<>按钮，在弹出的分析选项页面中，配置统计对象为事件协议，其他选项可根据需要选择。单击<确认>按钮，即可查看攻击事件的协议分布情况。

用户可通过单击列表中“事件协议”和“事件数”列下的统计值，或者单击操作列下的<>按钮，跳转到详情界面，查看相应的日志详情。

参数说明：

- 事件协议：统计时间段内发生的攻击事件协议。
- 事件数：统计时间段内发生的基于该协议的攻击事件数。
- 百分比（%）：统计时间段内发生基于该协议的攻击事件在所有攻击事件中所占比例。

源 IP

源 IP 页面用于展示统计时间段内，主平台或子平台上报的攻击事件的源 IP 地址分布情况。

选择“安全分析 > 安全事件分析”，单击页面右上角<>按钮，在弹出的分析选项页面中，配置统计对象为源 IP ,其他选项可根据需要选择。单击<确认>按钮 ,即可查看攻击事件的源 IP 分布情况。

用户可通过单击列表中“源 IP”和“事件数”列下的统计值，或者单击操作列下的<>按钮，跳转到详情界面，查看相应的日志详情。

参数说明：

- 源 IP：统计时间段内发生的攻击事件的源 IP 地址。
- 事件数：统计时间段内该源 IP 地址发生的攻击事件数。
- 百分比：统计时间段内该源 IP 地址发生的攻击事件在所有攻击事件中所占比例。

目的 IP

目的 IP 页面用于展示统计时间段内，主平台或子平台上报的攻击事件的目的 IP 分布情况。

选择“安全分析 > 安全事件分析”，单击页面右上角<>按钮，在弹出的分析选项页面中，配置统计对象为目的 IP，其他选项可根据需要选择。单击<确认>按钮，即可查看攻击事件的目的 IP 分布情况。

用户可通过单击列表中“目的 IP”和“事件数”列下的统计值，或者单击操作列下的<  >按钮，跳转到详情界面，查看相应的日志详情。

参数说明：

- 目的 IP：统计时间段内发生的攻击事件的目的 IP 地址。
- 事件数：统计时间段内该目的 IP 地址发生的攻击事件数。
- 百分比（%）：统计时间段内该目的 IP 地址发生的攻击事件在所有攻击事件中所占比例。

特征命中次数

特征命中次数页面用于展示统计时间段内，主平台上报的漏洞攻击日志中的特征命中情况。

选择“安全分析 > 安全事件分析”，单击页面右上角<  >按钮，在弹出的分析选项页面中，配置统计对象为特征命中次数，其他选项可根据需要选择。单击<确认>按钮，即可查看特征命中的统计信息。

用户可通过单击列表中“命中次数”下的统计值，或者单击操作列下的<  >按钮，跳转到详情界面，查看相应的日志详情。

参数说明：

- 攻击 ID：统计时间段内主平台或子平台上报的漏洞攻击日志中的攻击 ID。
- 命中次数：统计时间段内，该攻击 ID 的命中次数。

- 命中次数占比（%）：统计时间段内，该攻击 ID 命中次数在同时段所有攻击 ID 命中次数中所占比例。

报表管理

报表模板

安全业务管理平台提供了 6 个预定义报表模板，不同模板可以生成不同内容的报表。报表模板功能用于展示报表模板信息，包括模板名称、模板类型及模板的创建人、创建时间及上一次修改模板的时间。不同报表模板功能如下：

- IPS 允许放通事件：选择该模板后，将统计所有允许放通事件名称及事件数，并按放通事件数排序。
- IPS 阻断事件：选择该模板后，将统计所有阻断事件名称及事件数，并按阻断事件数排序。
- IPS 攻击事件：选择该模板后，将统计所有攻击事件名称及攻击次数，并按攻击次数排序。
- IPS 攻击目的端口：选择该模板后，将统计所有攻击事件的目的端口及攻击次数，并按攻击次数排序。
- IPS 攻击源 IP：选择该模板后，将统计所有攻击事件的源 IP 地址及攻击次数，并按攻击次数排序。

- IPS 攻击目的 IP：选择该模板后，将统计所有攻击事件的目的 IP 地址及攻击次数，并按攻击次数排序。

不同模板可以生成不同的报表。报表模板功能用于展示报表模板信息，包括模板名称、模板类型及模板的创建人、创建时间及上一次修改模板的时间。

选择“报表管理 > 报表管理 > 报表模板”，进入报表模板页面，可查看模板信息。单击操作列的<  >按钮可预览报表模板内容。

报表任务

该功能用于管理报表任务，根据报表任务选择的报表模板可生成相应的报表文件。

报表任务分为两大类型：

- 周期性报表任务：包括日报、周报、月报，根据设置时间自动执行任务，生成周期报表。周期性报表统计数据的开始时间为统计周期前的 00:00:00，结束时间为执行日期的 00:00:00。
- 即时性报表任务：立即执行，可立即生成报表。即时性统计报表统计数据的时间范围为当前时刻到统计周期前的当前时刻。

新增报表任务

1. 选择“报表管理 > 报表管理 > 报表任务”，进入报表任务页面，单击<新增>按钮，新增报表任务，配置基本信息。

基本信息参数说明：

- 任务名称：报表任务名称。
- 任务类型：任务执行周期，可选择日报、周报、月报及立即执行，不同的任务类型需要配置的参数如下：
  - 选择日报，需要指定任务执行时间，例如，指定任务执行时间为 20:30:00，安全业务管理平台将会在每天 20:30:00 执行报表任务，并统计前一天的安全事件信息，生成报表。
  - 选择周报，需要指定任务执行时间和在每周周几执行，例如指定任务执行时间为 20:30:00、每周字段选择周一，安全业务管理平台将会在每周一的 20:30:00 执行报表任务，并统计最近 1 周（不包含当天）的安全事件信息，生成报表。
  - 选择月报，需要指定任务执行时间，例如，指定任务执行时间为 20:30:00，安全业务管理平台将会在每月 1 号 20:30:00 执行报表任务，并统计上个月的安全事件信息，生成报表。
  - 选择立即执行，需要指定统计类型，即选择统计周期（例如，最近 1 小时），配置完成后，任务将立即执行并按统计周期统计安全事件信息，生成报表。
- 报表格式：选择生成的报表文件的格式，目前仅支持生成 DOCX 文件。

2. 完成基本信息配置后，单击<下一步>按钮，选择报表模板。安全业务管理平台将根据选择的模板统计相应的事件信息生成报表文件。

3. 完成模板选择后，单击<下一步>按钮，配置统计条件。

统计条件参数说明：

- 事件列表 TOP N：统计排名 TOP N 的事件。
- 统计对象：统计指定的对象，目前仅支持设备组。
- 设备组：统计指定的设备组。

4. 配置完成后，可在报表任务列表中任务状态。

使用限制和注意事项

在启用或停用报表任务时，只能对周期性报表任务进行操作。

报表文件

该功能用于展示通过报表任务生成的报表文件，可查看报表文件名称、生该该报表文件的任务名称、任务类型等信息，用户可通过该页面检索、下载、删除报表文件。

用户可通过选择指定的报表文件，并单击<下载>按钮，或单击指定报表文件右侧的<>按钮，下载报表文件到本地，进行查看。

日志审计

该功能用于展示从设备采集的安全日志、流量日志和应用审计日志的分析结果。

页面默认 30s 自动刷新一次 ,仅刷新当前页面。用户可根据实际情况 ,通过单击左上角<配置>按钮，进入配置页面，设置自动刷新的时间间隔或关闭自动刷新功能。

用户可配置统计周期，或通过单击<更多条件>按钮，配置多种查询条件，筛选出关心的日志。界面将根据用户配置的查询条件显示相应的日志信息。

如需导出界面中的日志信息 ,可单击左上角的<导出>按钮 ,导出日志。并通过单击面板区右侧<  >按钮，查看日志导出进度。单击<  >按钮后，进入下载列表页面，可单击指定文件右侧操作列下的<下载>按钮，将导出的日志文件下载到浏览器中。也可以单击<删除>按钮，删除导出的文件。其中，下载的日志保存在 CSV 格式的文件中，每个 CSV 文件可保存 10 万条日志。CSV 文件将压缩为.TAR.GZ 的压缩文件。

单击<  >列定制按钮，可选择界面中需要展示的日志字段。

安全日志

该功能用于展示从设备采集的漏洞攻击日志、病毒攻击日志和安全策略日志的分析结果。

漏洞攻击日志

选择“日志审计 > 安全日志 > 漏洞攻击日志”，进入漏洞攻击日志页面，可查看设备上报的漏洞攻击日志信息。

参数说明：

- 时间：攻击日志产生时间。
- 源 IP：攻击源 IP 地址。
- 目的 IP：被攻击目标的 IP 地址。
- 攻击子分类：攻击子分类名称。
- 事件名称：攻击事件名称。
- 事件级别：攻击事件的严重级别。
- 真实源 IP：攻击源的真实 IP 地址。
- 设备名称：产生该日志的设备的名称。
- 源安全域：日志产生的源安全域。
- 目的安全域：日志产生的目的安全域。
- 动作：产生该日志的设备接收到攻击报文后执行的动作。
- 类型：用于标识报文匹配黑白灰名单的标记。
- 操作：单击操作列的<详情>按钮可查看详细的漏洞攻击详情。
- HOST 字段：攻击报文头域中获取到的主机名。
- URI：攻击报文首行中获取到的 URL。
- 抓包名称：抓包文件的名称。
- 攻击载荷：攻击报文的载荷内容。

- 协议：攻击报文的传输协议。

选择“日志审计 > 安全日志 > 漏洞攻击日志”，进入漏洞攻击日志页面，单击指定日志右侧的<  >按钮，进入新增 IPS 白名单页面，系统将自动提取该条日志的信息加入 IPS 白名单。详细参数说明请参见“入侵防御白名单配置”。

病毒攻击日志

选择“日志审计 > 安全日志 > 病毒攻击日志”，进入病毒攻击日志页面，可查看设备上报的病毒攻击日志信息。

参数说明：

- 时间：攻击日志产生时间。
- 源 IP：攻击源 IP 地址。
- 目的 IP：被攻击目标的 IP 地址。
- 事件名称：攻击事件名称。
- 事件级别：攻击事件的严重级别。
- 源端口：攻击报文的源端口。
- 源安全域：攻击报文的源安全域。
- 目的安全域：攻击报文的目的安全域。
- 协议：攻击报文的传输协议。

- 方向：攻击报文的方向，即请求报文和应答报文。
- 策略名称：攻击报文命中的策略名称。
- 动作：产生该日志的设备接收到攻击报文后执行的动作。
- 设备名称：产生该日志的设备的名称。
- 病毒 ID：攻击报文的病毒 ID。

安全策略日志

选择“日志审计 > 安全日志 > 安全策略日志”，进入安全策略日志页面，可查看设备上报的安全策略日志信息。

流量日志

流量日志中可查看设备上报的 NAT 会话日志、NAT444 端口块日志和 NAT444 会话日志。

- NAT 会话日志：NAT 会话日志是为了满足用户的安全审计需要，对 NAT 会话（报文经过设备时，源或目的信息被 NAT 进行过转换的连接）信息进行的记录，包括 IP 地址及端口的转换信息、用户的访问信息、会话开始和结束时间等信息。
- NAT444 端口块日志：NAT444 端口块日志是为了满足用户溯源的需要，在 NAT444 地址转换中，对每个用户的私网 IP 地址进行端口块分配或回收时，都会输出一条基于用户的日志，记

录私网 IP 地址和端口块的映射关系。在进行用户溯源时，只需根据报文的公网 IP 地址和端口找到对应的端口块分配日志信息，即可确定私网 IP 地址。

- NAT444 会话日志：NAT444 会话日志是为了满足用户的安全审计需要，对 NAT444 会话信息进行的记录，包括 IP 地址及端口的转换信息。

应用审计日志

应用审计日志用来查看用户的上网行为记录（例如 IM 聊天软件中的用户信息、搜索引擎的历史记录等），方便管理员根据用户上网的情况调整相关策略，规范用户的上网行为。

告警事件

告警事件列表

该功能用于展示平台记录的告警事件。可查看事件的生成时间、事件名称、源/目的 IP 地址、真实源 IP 等信息，并可查看生成该事件的原始日志信息。

告警规则设置

该功能用于配置生成告警事件需要满足的条件以及间隔时间。在间隔时间内，匹配相同告警条件的事件将被聚合输出为一个告警事件。

参数说明：

- 聚合条件：生成告警事件的聚合条件。系统会对符合条件的事件进行聚合，生成告警事件。包括：源 IP、目的 IP、真实源 IP、事件名称、动作。
- 时间窗：生成告警事件的间隔时间。系统仅会对时间窗内上报的事件进行聚合条件匹配。时间窗单位可选 10 秒、20 秒、30 秒、40 秒和 50 秒。

安全告警

本功能用于将告警事件以邮件的方式发送到指定的收件人。

告警策略

用于配置发送告警事件邮件的过滤条件以及邮件参数。

新建告警策略

选择“告警事件 > 安全告警 > 告警策略”，单击<新增>按钮，进入新增告警策略页面，可配置告警邮件的基本信息、触发条件和邮件参数。详细参数说明如下。

参数说明：

- 告警策略名称：告警策略的名称。
- 描述：告警策略的描述信息。
- 告警级别：告警事件的严重级别，包括严重、高危、中危、低危。
- 发送间隔：发送邮件的间隔时间。
- 阈值：告警事件中原始事件数的阈值。仅当原始事件数高于或等于阈值时，才发送告警事件邮件。
- 邮件标题：告警事件邮件的标题。
- 收件人：告警事件的收件人。其中，收件人仅支持选择已配置邮件的用户列表。
- 模板预览：预览邮件中的内容。

告警事件邮件中，仅显示按照原始事件数降序排行的 top50 个告警事件。

使用限制和注意事项

配置本功能前，需要完成以下配置：

- 选择“系统配置 > 全局配置 > 邮件服务器”，在邮件服务器配置页面中，配置邮件服务器参数。

- 选择“系统配置 > 全局配置 > 角色及权限管理”，在用户管理页面中，配置用户的邮箱。

告警记录

系统每发送一次告警事件邮件，则生成一条告警记录。

选择“告警事件 > 安全告警 > 告警记录”，可查看告警事件邮件的发送记录，包括发送时间、告警策略名、收件人等。

运维管理

区域管理

该功能用于对用户网络进行划分区域管理，用户可根据实际需要将网络划分为不同区域，并为区域配置子区域、资产及区域采集器。平台通过区域采集器与资产进行信息交互。

新增区域管理

选择“运维管理 > 区域管理”，进入区域管理页面，单击<新增>按钮，进入新增区域管理页面。

参数说明：

- 区域名称：区域的名称。
- 区域描述：区域的描述信息。
- 区域地理位置：区域所在的省市。
- 区域采集器：当前区域所部署的采集器 IP 地址。平台通过区域采集器与资产进行信息交互。
- 区域 IP 范围：当前区域包含的 IP 地址范围。单击<添加>按钮，进入添加 IP 界面，并配置如下参数。
    - 开始 IP：IP 地址范围的起始 IPv4 或 IPv6 地址。
    - 结束 IP：IP 地址范围的结束 IPv4 或 IPv6 地址，结束 IP 必须大于或等于起始 IP。
    - IP 类型：可选择配置 IPv4 或 IPv6。

添加子区域

在区域管理页面，单击指定区域右侧操作列的<>按钮，即可为该区域添加子区域。

设备组管理

该功能用于对用户资产进行分组管理，用户可根据实际需要将资产划分为不同组，方便管理员对属于同一组的多个资产进行安全分析、查询日志审计、生成报表等。

新增设备组

选择“运维管理 > 设备组管理”进入设备组管理页面，单击<新增>按钮进入新增设备组页面。配置如下参数后，单击<确认>完成操作。

参数说明：

- 设备组名称：设备组的名称。
- 资产设备：设备组中包含的资产。
- 设备组描述：设备组的描述信息，合理的设备组的描述信息有利于管理员快速了解和使用设备组。

删除设备组

在设备组管理页面，可通过如下方式删除设备组：

- 单击指定设备组后面的<删除>按钮，即可删除该设备组。
- 选中多个设备组，单击<删除>按钮可以批量删除设备组。

使用限制和指导

当设备组下面存在设备时，不能删除该设备组。

资产监控

该功能用于管理用户的资产，并实时监控资产运行信息。

模板参数管理

该功能用于管理参数模板，包括 SNMP 模板、SSH 模板和 SOAP 模板。

- SNMP 模板：可用于监控设备状态、获取 CPU 和内存使用率等信息。
- SSH 模板：可用于登录设备。
- SOAP 模板：可对设备进行配置和管理，例如特征库升级、回滚等。

通过配置参数模板，安全业务管理平台可监控设备状态、远程登录设备、下发配置到设备。

新增 SNMP 模板

在资产监控页面，单击页面右上角<模板参数管理>按钮，进入模板参数管理界面。选择 SNMP 模板页签，单击<新增>按钮，进入新增 SNMP 模板界面。配置如下参数，并在完成配置后，单击<确认>按钮，完成模板配置。

参数说明：

- 模板名称：模板的名称。

- SNMP 版本：支持 SNMP v1、v2 和 v3。其中 V3 支持多种加密认证方式，包括：无加密/无认证、无加密/MD5 认证、无加密/SHA 认证、DES 加密/MD5 认证、DES 加密/SHA 认证、AES128 加密/MD5 认证和 AES128 加密/SHA 认证。
- 只读团体字：若配置该参数，必须与设备上配置的只读团体名一致。
- 用户名：用于认证的用户名。
- 认证密码：用于认证的密码。
- 加密密码：用于加密的密码。
- SNMP 端口号：安全业务管理平台接收 SNMP 报文的本地端口号。
- 模板描述：模板的描述信息。

新增 SSH 模板

在资产监控页面，单击页面右上角<模板参数管理>按钮，进入模板参数管理界面。选择 SSH 模板页签，单击<新增>按钮，进入新增 SSH 模板页面。配置如下参数，并在完成配置后，单击<确认>按钮，完成模板配置。

参数说明：

- 模板名称：模板的名称。
- SSH 端口号：安全业务管理平台使用该端口号登录设备。
- 用户名：安全业务管理平台使用该用户名登录设备。
- 用户密码：安全业务管理平台使用该密码登录设备。

- 模板描述：模板的描述信息。

新增 SOAP 模板

在资产监控页面，单击页面右上角<模板参数管理>按钮，进入模板参数管理界面。选择 SOAP 模板页签，单击<新增>按钮，进入新增 SOAP 模板页面。配置如下参数，并在完成配置后，单击<确认>按钮，完成模板配置。

参数说明：

- 模板名称：模板的名称。
- 访问 URL 协议：选择开启基于 HTTPS 或 HTTP 的 NETCONF over SOAP 功能。
- 端口号：NETCONF over SOAP 功能使用的端口号。基于 HTTP 的 NETCONF over SOAP 功能使用的端口号为 80；基于 HTTPSNETCONF over SOAP 功能使用的端口号为 832。
- 用户名：安全业务管理平台使用该用户名登录设备。
- 密码：安全业务管理平台使用该密码登录设备。
- 模板描述：模板的描述信息。

设备管理

本功能用于管理和监控设备，并支持同步设备上的业务配置到平台进行管理以及向设备下发业务配置。其中，设备可由用户手动添加或批量导入。

查看资产系统信息

在设备管理页面可查看设备的基本信息（例如资产名称、所属区域、IP 地址等）以及 CPU 利用率和内存利用率等信息。

单击<详情>按钮，可查看设备的流量统计趋势、新建会话趋势、并发会话趋势、CPU/内存利用率趋势以及接口详情信息。

单击<打开设备>按钮，可跳转至设备的 Web 登录界面。

新增资产

新增资产的配置步骤如下：

1. 在设备管理页面，单击<新增>按钮，进入新增资产信息界面，配置如下参数。

   参数说明：

   - 资产名称：设备的名称，建议填写设备的实际名称。
   - 管理 IP：设备的管理 IP 地址。
   - 制造商：设备制造厂商。
   - 资产类型：入侵防御设备选择“安全设备-入侵防御”，防火墙设备选择“安全设备-防火墙”。
   - 资产描述：设备的描述信息
   - 所属区域：设备所在的区域。

- 资产 IP：在输入框中输入设备的 IP 地址，并单击右侧的<添加>按钮，可添加资产 IP 地址。管理员可打开资产 IP 列表，查看设备的 IP 信息。
- 所属设备组：设备所在的设备组。
- 日志编码格式：设备上报日志的编码格式。取值包括 GBK 和 UTF-8，默认为 GBK。

2. 配置设备引用的认证模板，可手工编辑或者选择已配置的模板。
   - 选择“认证模板”，配置 SNMP 参数，单击<设置>按钮进入设置 SNMP 参数页面，可选择手工编辑或者从已有模板选取。该页面参数说明请参见“新增 SNMP 模板”。
   - 选择“认证模板”，配置 SSH 参数，单击<设置>按钮进入设置 SSH 参数页面，可选择手工编辑或者从已有模板选取。该页面参数说明请参见“新增 SSH 模板”。
   - 选择“认证模板”，配置 SOAP 参数，单击<设置>按钮进入设置 SOAP 参数页面，可选择手工编辑或者从已有模板选取。该页面参数说明请参见“新增 SSH 模板”。
3. 配置扩展属性，可根据设备实际情况配置其各属性值，包括设备序列号、资产编号等。

批量导入资产

1. 在设备管理页面，单击<导入>按钮，选择资产批量导入模板下载。
2. 按照模板样式填写设备信息后，再次单击<导入>按钮，选择资产导入，选择已经填写设备信息的模板，即可批量导入设备。

完成以上操作后，可单击<导入>按钮，选择操作结果，查看资产导入结果。

同步资产配置

同步功能可将设备上已有的业务配置同步到本平台进行统一的管理。

选择一个或多个设备，单击<同步>按钮，可将选中设备上所有支持同步的业务配置同步至平台。可在“业务配置”列查看同步结果。

资产业务配置

业务配置用于管理单个设备上的业务配置信息，支持的配置包括安全策略、IP 地址组、服务组、应用、应用组、时间段、安全域、入侵防御、防病毒、入侵防御白名单、NAT 动态转换、NAT 地址组、带宽策略和带宽通道。用户可根据实际需求，对设备上的业务配置进行统一的管理。

设备同步成功后，选择指定的设备，单击“业务配置”列下的<  >按钮，进入业务配置页面。可向指定的设备下发业务配置。

需要注意，对设备的业务配置进行的新增、删除、修改移动等操作将立即下发至设备。

保存资产配置

本功能用于批量保存设备配置。单击<保存配置>按钮，所选设备的当前配置将保存到设备的配置文件中。可单击<操作结果>按钮，查看配置是否保存成功。

导入资产配置到平台

本功能主要用于将设备上的业务配置导入到平台，可实现安全策略等业务配置的快速迁移。单设备的配置资源可导入至本平台成为全局资源。管理员可将全局资源下发至多台设备，从而实现多设备间的配置复制下发。

设备同步成功后，单击“业务配置”列下的<  >按钮，进入业务配置页面。单击右上角的<导入配置>按钮，进入导入配置页面。该页面可查看设备下支持导入的资源和安全策略列表。

管理员可以根据实际需求，勾选状态为“可导入”的资源或安全策略，单击<导入>按钮，即可将设备的配置导入到本平台。

其中，有如下限制需要关注：

- 导入配置时，设备会对待导入的配置与“安全业务管理 > 全局资源“中的配置进行对比分析，如果待导入的配置与全局资源中的配置存在冲突，则不允许导入该配置。
- 导入资源时，该资源及其所引用的资源都会被导入到全局资源。
- 导入安全策略时，该策略及其引用的资源都会被导入到全局资源。

使用限制和指导

添加设备之前，需要先配置模板参数。安全业务管理平台配置的 SNMP 模板或 SOAP 模板参数必须与设备上配置的 SNMP 功能或 NETCONF over SOAP 功能相关参数一致，否则会导致信息交互失败。

虚拟设备管理

该功能用于对用户设备上的虚拟设备（即 Context）进行管理。

虚拟设备是通过虚拟化技术将一台物理设备划分成多台虚拟设备，每台虚拟设备就称为一个 Context。每个 Context 拥有自己专属的软硬件资源，独立运行。

对于用户来说，每个 Context 就是一台独立的设备，方便管理和维护；对于管理者来说，可以将一台物理设备虚拟成多台逻辑设备供不同的分支机构使用，可以保护现有投资，提高组网灵活性。

用户可以在该页面查看、删除、创建、停用、启用虚拟设备。

新增虚拟设备

新增虚拟设备的配置步骤如下：

1. 单击<新增>按钮，进入增加虚拟设备界面。

   参数说明：

   - 虚拟设备名称：用户设备中的 Context 的名称。
   - 描述：Context 的描述信息，合理编写描述信息便于管理员快速了解和识别 Context 的作用，有利于后期维护。
   - 物理设备名称：指定需要创建 Context 的物理设备。

   配置完成上述参数后，可勾选<资源设置>前的复选框，为 Context 分配资源。

   参数说明：

- CPU 资源限额：即 CPU 权重，当 CPU 无法满足所有 Context 的处理需求时，系统将按照 CPU 权重值为每个 Context 分配处理时间。通过调整权重，可以使指定的 Context 获得更多的 CPU 资源，保证关键业务的运行。
- 吞吐量值：为了防止一个 Context 的报文过多而导致其它 Context 的报文被丢弃，需要限制 Context 的吞吐量。当启用吞吐量限制时，系统优先处理协议报文，对于超过限制值的业务报文会被丢弃。
- SSL VPN 登录用户数：对 Context 的最大 SSL VPN 登录用户数进行限制后，当该 Context 的 SSL VPN 登录用户数达到最大数目时，该 Context 将不允许新的用户登录。如果设置的数值小于当前 Context 的 SSL VPN 登录用户总数，则配置可以成功，但不再允许新的用户登录，且已经登录的用户不会被删除。直到已登录的用户通过老化机制下线或用户主动下线，使得用户总数低于配置的最大值后，系统才允许新的用户登录。
- 会话并发数：设备能够同时维持的会话连接总数是有限制的，为防止一个 Context 创建过多的会话，而导致其它 Context 无法创建新的会话，需要限制 Context 的会话并发数。用户可以为每个 Context 配置最大的会话并发数。
- 会话新建速率：会话新建速率是指设备在单位时间内所能够完全处理的新会话请求数量。由于设备的处理能力有限，为防止一个 Context 的会话新建速率过高，而导致其它 Context 创建会话失败，需要限制 Context 的会话新建速率。用户可以为每个 Context 配置最大的会话新建速率。

2. 配置完成上述参数后，可单击<下一步>按钮，可继续为 Context 分配接口和 VLAN 资源。

VLAN 支持如下分配方式：

- 共享：该模式下的 VLAN 由管理员在缺省 Context 中创建，统一配置和管理。此方式适用于同一个 VLAN 由多个 Context 共同使用的场景。
- 独占：该模式下的 VLAN 由各 Context 的管理员登录各自的 Context 后，自行创建、配置和管理。该模式要求各 Context 的管理员来规划和配置 VLAN。此方式适用于 Context 需要各自管理和使用一个独立 VLAN 的场景。

3. 单击<新增>按钮，在接口列表中选择为 Context 分配的接口。

4. 单击<下一步>按钮，配置管理接口 IP 和接口信息。

参数说明：

- 管理接口：Context 的管理接口。
- 管理 IP/子网掩码/网关：Context 管理口的 IP 地址/子网掩码/网关地址。
- 网关路由（目的地址/掩码/下一跳）：设备到平台的路由。
- SNMP 参数模板：Context 绑定的 SNMP 模板。
- NETCONF 参数模板：Context 绑定的 SOAP 参数模板。
- 保存配置：勾选此项后，Context 的配置将保存在设备配置文件中。

5. 配置完成上述参数后，单击<确认>按钮，完成 Context 的创建。

用户可在虚拟设备管理界面查看 Context 的信息、启用状态以及资源使用情况。也可以根据实际需求，对 Context 进行删除、启用和停用的操作。

Context 创建成功后，将作为新增设备显示在设备管理页面中，管理员可在该页面中对其进行管理。

使用限制和指导

创建虚拟设备时需要确保物理设备在线，且 NETCONF 连接通畅。

分配 VLAN 时有如下注意事项：

- 共享 VLAN 必须是设备上存在的 VLAN。请先创建 VLAN，再指定共享 VLAN。
- VLAN 1 不能被共享。
- 端口的缺省 VLAN 不能被共享。
- 已经创建了 VLAN 接口的 VLAN 不能被共享。

分配接口时有如下注意事项：

- 逻辑接口（如子接口、聚合接口等）仅支持共享方式分配，物理接口支持独占和共享两种方式分配。
- 如果子接口已经被分配，则不能再分配其父接口；如果父接口已经被分配，则不能再分配其子接口。
- 如果接口已经被共享分配，则不能再独占分配。需将共享分配配置取消后，才能独占分配。
- 当设备运行在集群模式时，禁止将集群物理端口分配给 Context。
- 聚合接口的成员接口不能分配给 Context。
- 冗余口的成员接口不能分配给 Context，当冗余口的成员接口为子接口时，其子接口的主接口也不能分配给 Context。

安全业务管理

该功能用于管理设备的安全业务配置，包括全局资源（如 IP 地址组、服务管理、时间段管理等）和安全策略。全局资源可被安全策略引用并下发至一台或多台设备，以便管理员可通过本平台快速、批量管理和下发安全策略。

全局资源

IP 地址管理

该功能主要用于管理主机地址、范围地址、子网地址及 IP 地址组，包括查询、新增、删除及修改地址。

- 主机地址：该功能用于管理系统中所有的主机地址，包括查询、增加、删除、修改主机地址。主机地址名称不能与 IP 地址列表中的范围地址和子网地址的名称重复。
- 范围地址：该功能用于管理系统中所有的范围地址，包括查询、新增、删除、修改范围地址。范围 IP 地址分为 IPv4 和 IPv6 两种形式，其使用状态由该范围地址是否加入了 IP 地址组决定，若加入了 IP 地址组，则状态为已使用，否则状态为未使用。
- 子网地址：该功能用于管理系统中所有的子网地址，包括查询、增加、删除、修改子网地址。子网 IP 地址分为 IPv4 和 IPv6 两种形式，其使用状态由该地址是否加入了 IP 地址组决定，若加入了 IP 地址组，则状态为已使用，否则状态为未使用。

- IP 地址组 :该功能用于管理系统中所有的 IP 地址组 ,包括查询、增加、删除、修改 IP 地址组。IP 地址组分为 IPv4 和 IPv6 两种类型。

服务管理

服务组中包含服务对象，用于匹配报文中的协议类型以及协议的特性（如 TCP 或 UDP 的源端口/目的端口、ICMP 协议的消息类型/消息码等 ）。服务组包括预定义服务组和自定义服务组，管理员可以根据需要自定义服务组。自定义服务组支持查询、增加、修改、删除操作。

时间段管理

时间段定义了一个时间范围，用户通过创建一个时间段并在域间规则中将其引用，就可以使该规则在此时间段定义的时间范围内生效。时间段包括绝对时间段和周期时间段：

- 周期时间段：表示以一周为周期（如每周一的 8 至 12 点）循环生效的时间段。
- 绝对时间段：表示在指定时间范围内（如 2015 年 1 月 1 日 8 点至 2015 年 1 月 3 日 18 点）生效的时间段。

安全域管理

安全域（Security Zone），是一个逻辑概念，用于管理设备上安全需求相同的多个接口。管理员将安全需求相同的接口进行分类 ,并划分到不同的安全域 ,统一应用安全策略 ,简化配置 ,方便管理。

在安全域管理页面，单击<新增>按钮，进入增加安全域页面。配置安全域名称和描述，并添加设备接口。单击<选择接口>按钮，在选择接口页面中，选择下发安全域的设备，以及该设备中需要加入该安全域的接口。单击<确定>按钮，系统将对该设备下发新增安全域的操作。

使用限制和指导：

- 新增安全域时，需要选择目标设备和加入该安全域的接口。配置完成后，系统将下发该安全域配置到目标设备，下发配置需要一段时间。
- 为安全域选择接口时，已被加入到其它安全域的接口不能重复添加。

入侵防御

入侵防御是一种可以对应用层攻击进行检测并防御的安全防御技术。入侵防御通过分析流经设备的网络流量来实时检测入侵行为，并通过一定的响应动作来阻断入侵行为，实现保护企业信息系统和网络免遭攻击的目的。

新增入侵防御配置文件的配置步骤如下：

1. 在“入侵防御”页面单击<新增>按钮，进入“新增入侵防御”页面，配置配置文件的名称。
2. 在特征筛选条件区域，配置如下参数，筛选出配置文件中所需的入侵防御特征。

   参数说明：

   - 保护对象：特征的保护对象。
   - 攻击分类：特征所属的攻击分类。
   - 缺省动作：特征的预定义动作。包括如下取值：丢弃、允许、重置、黑名单。

- 严重级别：特征的严重级别，包括如下取值：严重、高、中、低。
- 缺省状态：特征的推荐使用状态，该状态值用于标识特征库中缺省是否推荐使用该特征匹配报文。取值包括使能和未使能。其中，使能表示该特征具有广泛的使用场景、具备普遍性，缺省推荐使用；未使能表示该特征仅适用于特殊场景、不具备普遍性，缺省不推荐使用。

入侵防御配置文件将筛选出匹配所有条件的特征，如果某个条件配置了多个参数，则特征至少需要匹配上其中一个参数，才表示匹配上该属性。

3. （可选）在统一配置区域，可选择配置如下参数。

参数说明：

- 策略匹配统计：开启此功能后，可以统计报文命中入侵防御配置文件的次数。
- 动作：特征统一执行的动作，动作类型包括：缺省、黑名单、丢弃、允许、重置和重定向。如果动作为缺省，则对筛选出的特征执行各自的缺省动作。
- 日志：对匹配特征的报文记录日志。
- 抓包：对匹配特征的报文进行抓包。

4. （可选）在筛选特征区域，可更改“生效特征列表”和“非生效特征列表”中特征的状态和执行的动作。选择指定的特征，单击<更改状态>按钮，可修改特征的状态；单击<编辑>按钮，可修改对匹配该特征报文执行的动作。

5. 单击<选择设备>按钮，选择需要下发该入侵防御配置文件的设备。单击<确认>按钮，完成设备的选择。

6. 单击<确认>按钮，完成入侵防御配置文件的配置，配置文件将下发至该设备。

7. 在安全策略的 IPS 策略中引用此配置文件。有关安全策略的详细配置介绍请参见“安全策略”。

入侵防御白名单

当发现入侵防御日志中存在误报的情况时，可通过开启白名单功能，将误报日志中提取到的威胁 ID（入侵防御特征 ID）、URL 或 IP 地址加入白名单。设备对匹配白名单的报文放行，可以减少误报。

新增入侵防御白名单的配置步骤如下：

1. 在“入侵防御白名单”页面，单击<新增>按钮，进入“新增入侵防御白名单”页面。配置如下参数。

   参数说明：

   - 名称：配置入侵防御白名单的名称。
   - 描述：配置入侵防御白名单的描述信息。
   - 威胁 ID：从误报的日志中提取到的入侵防御特征 ID。
   - URL：从误报的日志中提取到的 URL，由报文头域和报文首行组成，例如：111.15.93.166/wnm/get.j。
   - 匹配模式：URL 的匹配方式，取值包括精确匹配和字串匹配。其中，精确匹配要求报文中 URL 必须和配置的 URL 完全一致才能匹配成功；子串匹配要求报文中携带的 URL 只要包含配置的 URL 即可匹配成功。
   - IP 地址：从误报的日志中提取到的 IP 地址。

- IP 地址类型：IP 地址类型，取值包括 IPV4 和 IPv6。

2. 单击<选择设备>按钮，选择需要下发该入侵防御白名单的设备。单击<确认>按钮，完成设备选择。

3. 单击<确认>按钮，完成入侵防御白名单的配置，白名单将直接下发至该设备。

防病毒

防病毒功能是一种通过对报文应用层信息进行检测来识别和处理病毒报文的安全机制。防病毒功能凭借庞大且不断更新的病毒特征库可有效保护网络安全，防止病毒在网络中的传播。将具有防病毒功能的设备部署在企业网入口，可以将病毒隔离在企业网之外，为企业内网的数据安全提供坚固的防御。目前，该功能支持对基于以下应用层协议传输的报文进行防病毒检测：

HTTP（Hypertext Transfer Protocol，超文本传输协议）

FTP（File Transfer Protocol，文件传输协议）

SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）

IMAP（Internet Mail Access Protocol，Internet 邮件访问协议）

POP3（Post Office Protocol - Version 3，邮局协议版本 3）

新增防病毒配置文件的配置步骤如下：

1. 在“防病毒”页面单击<新增>按钮，进入“新增防病毒配置文件”页面，配置如下参数。

   参数说明：

   - 名称：防病毒配置文件的名称。

- 描述：通过合理编写描述信息，便于管理员快速理解和识别防病毒配置文件的作用，有利于后期维护。
- 上传：对 HTTP、FTP、SMTP 和 IMAP 协议上传方向的报文进行病毒检测。其中，SMTP 协议只支持上传方向。
- 下载：对 HTTP、FTP、POP3 和 IMAP 协议下载方向的报文进行病毒检测。其中，POP3 协议只支持下载方向。
- 动作：设备可根据报文的应用层协议类型和传输方向来对其进行病毒检测，如果检测到病毒，则对此报文执行此处指定的动作。动作包括：告警、阻断、重定向。IMAP 协议只支持告警动作。

2. （可选）缺省情况下，设备基于应用层协议的防病毒动作对符合病毒特征的报文进行处理，当需要对某应用层协议上的具体应用采取不同的动作时，可在应用例外区域中在下拉框中选择指定的应用，单击右侧的<添加>按钮，将指定的应用添加到应用例外列表中，可为应用配置动作。设备将对该匹配该应用的报文执行配置的动作。例如，对 HTTP 协议进行允许通过处理，但是需要对 HTTP 协议上承载的游戏类应用采取阻断动作，这时就可以把所有游戏类的应用设置为应用例外，并配置动作为阻断。
3. （可选）当发现某类检测出病毒的报文被误报时，可以把该报文对应的病毒特征设置为病毒例。当后续再有检测出包含此病毒特征的报文通过时，设备将对其执行允许动作。
4. 单击<选择设备>按钮，选择需要下发该防病毒配置文件的设备。单击<确认>按钮，完成设备选择。
5. 单击<确认>按钮，完成防病毒配置文件的配置。防病毒配置文件将立即下发到指定的设备。

6. 在安全策略的防病毒策略中引用此配置文件。有关安全策略的详细配置介绍请参见“安全策略”。

应用管理

APR（Application Recognition）即应用层协议识别。基于应用的业务在进行报文处理时需要知道报文所属的应用层协议，APR 可以为这样的业务提供应用识别服务，并能够对接口上接收或者发送的某个应用层协议的报文进行数目和速率统计。APR 为了更好地识别报文所属的应用层协议，提供了两种应用识别方法：基于端口的应用识别和基于内容特征的应用识别。

- PBAR（Port Based Application Recognition，基于端口的应用层协议识别）：根据定义的应用层协议端口与应用的映射关系识别报文所属的应用层协议。
- NBAR（Network Based Application Recognition，基于内容特征的应用层协议识别）：提取应用报文区别于其它应用报文的特征，通过将报文的内容与特征库中的特征项进行匹配来识别报文所属的应用层协议。

新增自定义应用的配置步骤如下：

1. 在“应用管理”页面选择应用服务页签。单击<新增>按钮，进入“新增自定义应用”页面。
2. 配置应用的名称。
3. 单击<新增>按钮，进入新增端口映射页面，配置如下参数。

   参数说明：

   - 端口号：表示指定与应用层协议映射的端口。

- 协议类型：表示指定应用层协议使用的传输层协议。取值包括 all、DCCP（Datagram Congestion Control Protocol，数据报拥塞控制协议）、SCTP（Stream Control Transmission Protocol，流控制传输协议）、TCP 协议、UDP 协议和 UDP-Lite 协议。其中，all 表示所有传输层协议的指定端口的报文均被识别为指定应用层协议的报文
- 匹配方式：端口映射的匹配方式，取值包括 all（通用端口映射）、基于 IPv4 地址的主机端口映射、基于 IPv4 网段的主机端口映射、基于 IPv4 ACL 的主机端口映射、基于 IPv6 地址的主机端口映射、基于 IPv6 网段的主机端口映射和基于 IPv6 ACL 的主机端口映射。其中，对于基于 IPv4 和 IPv6 ACL 的主机端口映射，平台仅支持使用设备上已有的 ACL。

4. 单击确认按钮，完成应用配置。
5. 单击<选择设备>按钮，选择需要下发应用的设备。单击<确认>按钮，完成设备的选择。
6. 单击<完成>按钮，应用将下发到指定的设备。

可以将具有相似特征或者相似限制要求的应用添加到一个应用组。设备最多可支持配置 1000 个应用组，每个应用组里最多可以包含 1000 个用户自定义应用，预定义应用无限制。

新增应用组的配置步骤如下：

1. 在“应用管理”页面选择自定义应用组页签。单击<新增>按钮，进入“新增自定义应用组”页面。
2. 配置应用组的名称和描述信息。
3. 在“类别”区域，筛选出指定类型的应用。筛选结果将显示在“可选应用”列表中。

4. 选择需要加入应用组的应用，单击右侧的<  >按钮，可将所选应用加入右侧的“已选应用”列表中；或者可以单击<  >按钮，将所有应用加入右侧的“已选应用”列表中。

5. 单击<选择设备>按钮，选择需要下发应用组的设备。单击<确认>按钮，完成设备的选择。

6. 单击<确认>按钮，应用组将下发到指定的设备。

安全策略

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

新增安全策略

新增安全策略的配置步骤如下：

1. 在“安全策略”界面下，单击<新增>按钮，进入新增安全策略界面。配置如下参数。

   参数说明：

   - 策略名称：表示安全策略的名称，同一类型安全策略的名称不能相同。
   - 源安全域：配置源安全域作为安全策略的过滤条件。
   - 目的安全域：配置目的安全域作为安全策略的过滤条件。
   - 动作：安全策略动作包括如下：

- 允许：表示对符合安全策略过滤条件的报文进行允许通过处理。
- 拒绝：表示对符合安全策略过滤条件的报文进行阻断处理。

- IP 类型：安全策略包括 IPv4 和 IPv6 两种类型。
- 源 IP 地址组：配置源 IP 地址组作为安全策略的过滤条件。
- 目的 IP 地址组：配置目的 IP 地址作为安全策略的过滤条件。
- 服务组：配置服务组作为安全策略的过滤条件。
- 应用：配置应用作为安全策略的过滤条件。
- 应用组：配置应用组作为安全策略的过滤条件。
- 时间段：配置安全策略生效的时间段。
- IPS 策略：在安全策略中引用入侵防御策略，设备将对符合安全策略过滤条件的报文进行入侵防御业务处理。
- 防病毒策略：在安全策略中引用防病毒策略，设备将对符合安全策略过滤条件的报文进行防病毒业务处理。
- 描述信息：通过配置描述信息，便于管理员快速理解和识别此安全策略的作用。
- 日志记录：开启日志记录功能后，对符合安全策略过滤条件的报文记录日志信息。
- 统计功能：开启开启策略匹配功能后，对符合安全策略过滤条件的报文进行数据统计。
- 启用策略：开启本功能后，安全策略开始生效。

2. 配置上述参数后，单击<确认>按钮，完成安全策略的创建。

管理员可对安全策略进行删除、编辑和复制的操作。

策略下发任务

该功能用于批量下发安全策略到多个设备并展示下发结果。

新增策略下发任务的配置步骤如下：

1. 在“策略下发”页面，单击<新增>按钮，进入新增策略下发任务页面。配置如下参数：

   参数说明：

   - 任务名称：策略下发任务名称，名称不可重复。
   - 任务描述：通过配置描述信息，便于管理员快速理解和识别此策略下发任务的作用。

2. 单击<选择设备>按钮，选择将安全策略下发到目标设备。单击<确认>按钮，完成设备的选择。
3. 单击<确认>按钮，完成策略下发任务的创建，并进入“策略详情”页面。
4. 在策略详情页面添加需要下发到目标设备上的安全策略。可通过新增和选择已有安全策略的方式添加安全策略。并可以对待下发的安全策略进行调序、移动、删除和冗余分析的操作。

使用限制和指导

下发配置前必须先在设备配置 NETCONF over SOAP，并将设备添加为资产，且指定设备所属区域和引用 SOAP 参数模板。

特征库管理

设备特征库

设备特征库页面可查看所有设备的特征库信息，并支持对设备进行特征库升级和回滚操作。

特征库升级

1. 在设备特征库页面，选择目标设备，单击<升级>按钮，选择特征库文件。单击<确认>按钮，设备将使用该文件进行特征库升级。
2. 升级成功后，选择目标设备，单击<同步>按钮，可显示该设备当前特征库版本升级结果。

特征库回滚

1. 在设备特征库页面，选中目标设备，单击<回滚>按钮，可选择将该设备上的 IPS 特征库（即入侵防御特征库）、AV 特征库（即防病毒特征库）、APR 特征库（即应用识别特征库）或 URL 特征库回滚到上一版本或出厂版本。
2. 回滚成功后，选择目标设备，单击<同步>按钮，可显示该设备当前特征库版本回滚结果。

特征库文件

该功能可管理特征库文件，包括上传特征库文件到平台、删除特征库文件，向子平台推送特征库文件。

上传特征库文件

在特征库文件页面，单击<文件上传>按钮，选择需要上传到平台的特征库文件，单击<上传>按钮。文件将被上传到平台。

即时推送特征库文件

1. 在特征库文件页面，选择需要推送的特征库文件，单击<文件推送>按钮，选择立即推送，选择推送的目标子级平台。单击<确认>按钮，系统会立即将特征库文件推送到子级平台。
2. 单击操作列的<详情>按钮，可查看推送结果。

定时推送特征库文件

1. 在特征库文件页面，选择需要推送特征库文件，单击<文件推送>按钮，选择定时推送，进入文件定时推送界面。
2. 选择推送的子级平台并设置定时推送的时间，单击<确认>按钮，系统将在指定时间将特征库文件推送到子级平台。

3. 选择“运维管理 > 特征库管理 > 推送任务管理”，可查看任务运行结果，也可停止或启用指定的推送任务。

使用限制和指导

使用特征库管理功能前必须确保设备已配置 NETCONF over SOAP 功能，且设备已被平台添加为资产并指定所属区域和引用 SOAP 参数。

系统配置

该功能用于管理系统相关的配置，如设置用户对本系统的操作权限、记录用户操作日志、系统名称及 Logo 定制、分级系统管理等。

系统管理

全局配置

系统参数

本功能用于设置用户登录相关的参数或恢复缺省设置。

参数说明：

- 用户闲置超时时长：用户在本参数设置的时间内一直没有操作 Web 界面，系统会强制断开该用户的 Web 连接，使该用户下线。
- 允许登录失败次数：允许连续登录失败次数。
- 登录失败锁定时长：达到允许连续登录失败次数后，需要等待本参数设置的时间后才能重新登录。
- 高级模式配置：本功能仅限农行局点使用，其他局点环境中，请关闭本功能。开启高级模式后，系统将会打开入侵防御易用性以及入侵防御白名单相关功能。

邮件服务器

本功能用于发送告警事件邮件的邮件服务器参数。

参数说明：

- 协议：支持 SMTP 和 ExChange。
- 开启 SSL：是否开启 SSL 加密功能。开启本功能后，邮件将使用 SSL 协议进行加密传输。
- 邮件服务器地址：邮件服务器的 IP 地址或主机名。
- 端口号：邮件服务器的端口号。
- 邮箱账号：系统向外发送邮件时使用的账号。
- 密码：邮箱的账号密码。
- 邮箱测试：勾选本功能后，可测试邮箱服务器是否可用。
- 接受者地址：用于邮箱测试的接受者邮箱地址。单击<发送邮件测试>按钮，系统将使用上述配置的参数进行邮件发送测试。

告警规则设置

系统告警规则：该功能用于设置系统 CPU、内存、磁盘（数据）、磁盘（系统）的告警阈值，当其中某项的利用率达到所设置的阈值，系统将发出告警提示信息。

系统告警规则的具体操作步骤如下：

1. 选择“系统配置 > 全局配置 > 告警规则设置 “，选择系统告警规则页签。
2. 单击指定告警规则右侧的<编辑>按钮，进入编辑告警规则页面，可修改规则参数。

   参数说明：

   - 规则名称：告警规则名称，包括 CPU、内存、磁盘（数据）、磁盘（系统）。

- 告警阈值：CPU、内存、磁盘（数据）、磁盘（系统）的使用率的上限值。
- 告警级别：告警信息的严重级别，取值包括严重、警告和通知。
- 告警描述：告警信息的描述信息，格式固定为“%主机名%XXX 利用率超过%阈值%“。其中，”%主机名%“表示触发告警的主机名；”XXX“表示告警规则的类型，取值包括 CPU、内存、数据盘或系统盘；”%阈值%“表示告警阈值。

3. 单击<确认>按钮，完成告警规则参数的配置。

设备告警规则：该功能用于设置设备离线和长时间无日志上报时是否开启弹窗提示，并可以配置提示弹窗的间隔时长以及无日志上报的间隔时长。

认证服务器配置

该功能用于配置对用户身份信息进行认证的 RADIUS 服务器。平台将用户信息传输到指定的 RADIUS 服务器，然后根据服务器返回的信息进行相应处理（如接受/拒绝用户接入）。

参数说明：

- 认证方式：表示服务器认证用户的方式，包括 CHAP 和 PAP。
- RADIUS 服务器 IP 地址：表示服务器的 IP 地址。
- 认证端口：表示服务器的端口号。
- 共享密钥：表示与服务器交互信息时使用的密钥。

数据清理设置

数据清理功能可自动周期性检查并清理系统中原始日志，当日志存储容量或存储时间达到阈值条件时会触发删除告警，系统将删除存储时间最早的原始日志，直到原始日志的存储空间或存储天数降到清理阈值以下。

参数说明：

- 日志存储空间阈值：日志存储量占系统总容量的百分比达到空间阈值后，系统将清理存储时间最早的日志，直到日志存储百分比小于空间阈值。
- 时间阈值设置：日志存储天数达到设置的保存天数后将删除存储时间最早的原始日志。可单击指定类型日志右侧的<编辑>按钮，修改保存天数。

日志备份与恢复

该功能用于备份与恢复平台产生的大量日志数据，为用户提供更加灵活的方式管理日志数据。

- 日志备份：自动备份系统中的日志。配置正确的 FTP 服务器连接参数并启用备份功能后，系统将于配置的开始时间，打包前一天的日志数据并将其转储至目标 FTP 服务器上。一次最多只能备份 50GB 日志数据包，超过 50GB 会备份失败。
- 日志恢复：可从目标 FTP 服务器上恢复指定时间区间内的日志数据。

日志备份的具体操作如下：

1. 选择“系统配置 > 系统管理 > 全局配置 > 日志备份与恢复”，选择“日志备份”页签。
2. 配置相关参数。

参数说明：

- FTP 路径：将系统中的日志转储到该 FTP 服务器的对应目录下。
- 用户名：FTP 的登录用户名，用于连接 FTP 服务器，上传备份的日志。
- 密码：FTP 的登录密码，用于连接 FTP 服务器，上传备份的日志。
- 开始时间：设置日志备份功能启用时间。

3. 单击<启用>按钮，开启日志备份功能。备份成功的日志记录将展示在下方的日志备份记录列表中。

如需停止日志备份功能，可单击<停用>按钮，停止备份日志。

日志恢复的具体操作如下：

1. 选择“系统配置 > 系统管理 > 全局配置 > 日志备份与恢复”，选择“日志恢复”页签。
2. 配置相关参数。

参数说明：

- FTP 路径：FTP 服务器用于存放备份日志文件的路径。
- 用户名：FTP 的登录用户名，用于连接 FTP 服务器。
- 密码：FTP 的登录密码，用于连接 FTP 服务器。
- 时间区间：在该时间段内的备份的日志将被恢复到本系统，最大恢复时间段为 7 天（包含开始时间和结束时间）。

3. 单击<开始恢复>按钮，系统将根据配置的参数恢复日志。恢复成功的日志记录将展示在下方的恢复任务记录列表中。

日志转发策略

该功能用于将本平台收集的日志转发到其他日志分析平台或日志接收系统。

新增日志转发策略的配置步骤如下：

1. 选择“系统配置 > 系统管理 > 全局配置 > 日志转发策略”，进入日志转发策略页面。
2. 单击<新增>按钮，进入新增日志转发策略页面。配置如下参数。

   参数说明：

   - 接收主机 IP：接收本平台转发的日志数据主机的 IPv4 或 IPv6 地址。
   - 接收端口：接收本平台转发的日志数据的目的端口。
   - 日志内容：选择需要转发的日志字段。
   - 级别：选择需要转发的日志级别。
3. 单击<确认>按钮，完成日志转发策略的配置。

告警事件转发策略

该功能用于将本平台收集的告警事件转发到其他日志分析平台或日志接收系统。

新增告警事件转发策略的配置步骤如下：

1. 选择“系统配置 > 系统管理 > 全局配置 > 告警事件转发策略”，进入告警事件转发策略页面。

2. 单击<新增>按钮，进入新增告警事件转发策略页面。配置如下参数。

   参数说明：

   - 接收主机 IP：接收本平台转发的告警事件主机的 IPv4 地址。
   - 接收端口：接收本平台转发的告警事件的目的端口。
   - 告警内容：选择需要转发的告警事件信息字段。
   - 级别：选择需要转发的告警事件级别。

3. 单击<确认>按钮，完成告警事件转发策略的配置。

黑白名单设置

该功能用于根据漏洞日志中提取的信息生成黑白名单，可快速阻断或放行报文。

新增黑白名单的配置步骤如下：

1. 选择“系统配置 > 系统管理 > 全局配置 > 黑白名单管理”，进入黑白名单管理页面。
2. 单击<新增>按钮，进入新增黑白名单页面。配置如下参数。

   参数说明：

   - 策略名称：黑/白名单的名称。
   - 描述：黑/白名单的描述信息。
   - 类型：标识名单类型，取值包括黑名单和白名单。如果为黑名单，则对匹配黑名单的报文进行阻断；如果为白名单，则对匹配白名单的报文执行放行动作。

- 源 IP：日志中提取出的报文源 IP 地址。
- 目的 IP：日志中提取出的报文目的 IP 地址。
- 目的端口：日志中提取出的报文目的端口。
- HOST 字段：日志中提取出的报文 HOST 字段信息。
- 真实源 IP：日志中提取出的报文真实源 IP 地址。
- 动作：日志中提取出的报文被执行的动作。
- 特征 ID：日志中提取出的报文匹配到的特征 ID。

3. 单击<确认>按钮，完成黑白名单的配置。

配置黑白名单功能后，当报文匹配到黑/白名单时，管理员可到日志审计页面进行查看。匹配黑白名单的报文日志中，将携带黑/白名单的类型。

系统监控

管理员可实时监控平台整体运行状态和资源消耗情况，包括平台 CPU 使用率、内存使用率、磁盘的系统区与数据区的使用率，还可以查看平台的核心服务与各服务器节点的运行状态。

参数说明：

- 平台整体运行状态
  - 整体运行状态：平台的整体运行状态由节点运行状态和核心服务状态共同决定，包括健康和故障：

- 平台中除 cyber2 外的任意节点离线，整体运行状态显示故障。
- 任意核心服务故障，整体运行状态显示为故障。

- CPU 使用率：集群 CPU 的总容量和当前使用百分比。
- 内存使用率：集群内存总容量合和当前使用百分比。
- 磁盘[系统区]使用率：集群中所有系统盘总容量和当前使用百分比。
- 磁盘[数据区]使用率：集群中所有数据盘总容量和当前使用百分比。

- 核心服务监控
  - 名称：核心服务的名称。
  - 状态：服务的运行状态，包括健康和故障：
    - 对于在线服务，若该服务包含的任意进程异常退出，则该服务状态为故障。
    - 对于离线服务，若在调度周期内启动失败，则该服务状态为故障。
  - CPU 使用率：服务包含的所有进程的 CPU 使用率总和。
  - 内存使用率：服务包含的所有进程的内存使用率总和。
- 节点监控
  - 名称：节点名称，组成安全业务管理平台的一台服务器为一个节点。
  - 状态：节点服务器的运行情况，包括健康和故障，若服务器离线则显示故障。
  - CPU 使用率：节点服务器的 CPU 使用百分比。
  - 内存使用率：节点服务器的内存使用百分比。

- 磁盘[系统区]使用率：节点服务器的系统盘使用百分比。
- 磁盘[数据区]使用率：节点服务器的数据盘的使用百分比。

角色及权限管理

安全业务管理平台预定义了 4 个缺省用户角色及 4 个相应角色的用户。其中，预定义角色不能修改或删除，包括业务管理员、系统管理员、审计管理员及超级管理员；预定义用户不能删除，但可以修改其用户全称、电话、邮箱、密码及登录认证方式。

不同角色的用户拥有不同的权限，为用户指定角色后可以实现用户权限管理。系统预定义角色、用户及其权限如下表所示。

表-1 系统预定义角色、用户及权限信息

用户名/密码	用户角色	用户权限
sysAdmin/sysAdmin	系统管理员	管理系统配置、区域、资产
buzAdmin/buzAdmin	业务管理员	管理各类安全业务
admin/admin@admin	超级管理员	所有权限
auditAdmin/auditAdmin	审计管理员	查看日志记录

用户可以根据实际需求自定义角色并赋予相应的权限，创建新用户。选择“系统配置 > 系统管理 > 角色及权限管理”即可对管理用户及角色信息。

用户管理

选择“系统配置 > 系统管理 > 角色及权限管理 > 用户管理”，进入用户管理页面，可查看、新增、修改或删除用户信息。

新增管理员的配置步骤如下：

1. 单击<新增>按钮，进入新增管理员页面。配置如下参数。

   参数说明：

   - 账号：登录用户名。
   - 用户全称：用户全称，可与账号相同。
   - 登录认证：用户身份认证方式，支持 RADIUS 认证和简单密码认证。
   - 密码：登录用户的密码。
   - 确认密码：再次输入登录用户的密码。
   - 电话：用户联系方式，11 位手机号。
   - 邮箱：用户邮箱，配置后可在告警策略中选为收件人，接收告警邮件。
   - 用户角色：选择用户所属角色。取值包括：超级管理员、业务管理员、系统管理员和审计管理员。
   - 登录状态：默认为正常，状态为锁定时不可登录。

2. 单击<确认>按钮，完成新增管理员的配置。

角色管理

选择“系统配置 > 系统管理 > 角色及权限管理 > 角色管理”进入角色管理页面，可查看、新增或删除角色信息。

新增角色的配置步骤如下：

1. 单击<新增>按钮，进入新增角色页面。配置如下参数。

   参数说明：

   - 角色名称：角色的名称。
   - 角色描述：配置有关此角色的描述信息。

2. 单击<确认>按钮，完成新增角色的配置。

系统支持为自定义角色赋予权限，管理员可选择指定的自定义角色，单击<权限>按钮，进入角色权限页面。可在界面导航中勾选指定界面前的复选框，为角色赋予该界面的操作权限。单击<确认>按钮，完成角色权限配置。

日志记录

本功能用于展示登录本系统的用户操作日志和系统日志。

操作日志：用于展示登录平台的操作人的用户名、IP 地址及其操作内容等信息，便于管理员对登录用户行为进行审计。

系统日志：用户展示平台的系统信息，便于管理员了解平台下设备的日志上报情况和在线状态等信息。

个性化定制

本功能用于用户自定义系统名称和系统的 Logo 图片。

系统信息

本功能用于展示系统信息，包括产品名称、型号及软件版本号。

License

该功能用于管理系统 license 文件，包括展示当前已安装的特性许可文件、获取授权信息及导入许可文件。

获取授权码

该功能用于获取主机信息文件（安全业务管理平台的设备硬件信息和用户信息加密后生成的.did 文件），使用主机信息文件、授权码及 SN 序列号即可登录官网申请 License 文件。

获取授权码的具体操作如下：

1. 选择“系统配置 > License 管理 “，进入 License 管理页面。
2. 单击<获取授权申请码>按钮，进入产品注册页面，填写获取主机信息文件的配置信息，如下：
    - 输入最终用户信息，包括用户姓名、国家/地区、省/市、公司/单位名称、地址、邮编、邮件地址及联系电话。
    - 输入申请人信息：包括申请人姓名、公司/单位名称、电子邮件地址及联系电话。
    - 单击<下一步>进入下载文件页面。
    - 单击<下载>按钮即可下载主机信息文件。

导入许可文件

该功能用于导入从官网申请的 License 文件。

导入 License 文件的具体操作步骤如下：

1. 选择“系统配置 > License 管理 “，进入 License 管理页面。
2. 单击<导入许可文件>按钮，进入产品注册页面，选择通过官网申请的激活后的 license 文件，单击上传完成操作。

3. 系统将解析并安装 license 文件。

分级管理

该功能用于监控本平台所拥有的子级平台或采集器状态。当需要将网络划分为不同的区域时，每个区域都需要通过安全业务管理平台平台进行管理，用户可根据实际情况选择一个安全业务管理平台作为父级平台 ,其他平台作为子级平台注册到父级平台下并每隔1分钟上报一次资源使用信息(CPU 负载、内存使用率、硬盘使用率等)，便可通过父级平台统一监控子级平台的状态。

父级平台下可以注册多个子级平台，子级平台下不能再注册子级平台。因此，只有父级平台的分级管理页面会显示子级平台信息。

注册父级平台和子级平台请参见安全业务管理平台安装指导，不支持通过 Web 界面新增或删除父级或子级平台。

参数说明：

- 名称：子级平台名称。
- 类型：子级运维系统
- IP：子级平台 IP 地址
- 描述：对子级平台或采集器的描述
- 注册状态：显示子级平台是否已经注册。
- 在线状态：子级平台状态，包括离线和在线两种状态。

- 最后一次信息上报时间：子级平台上一次上报资源使用情况的时间。
- 跳转到子平台：显示为  图标，单击可跳转到该子平台的登录页面。
- 状态监控：显示为图标，单击可查看子级平台资源使用情况。

  参数说明：

  - 最后一次信息上报时间：子平台最后一次信息上报时间。
  - 在线状态：展示子级平台系统是否在线。
  - 内存使用率：展示子级平台系统内存的使用情况。
  - 磁盘使用率：展示子级平台系统磁盘的使用情况。
  - CPU 利用率：展示子级平台的 CPU 使用情况。