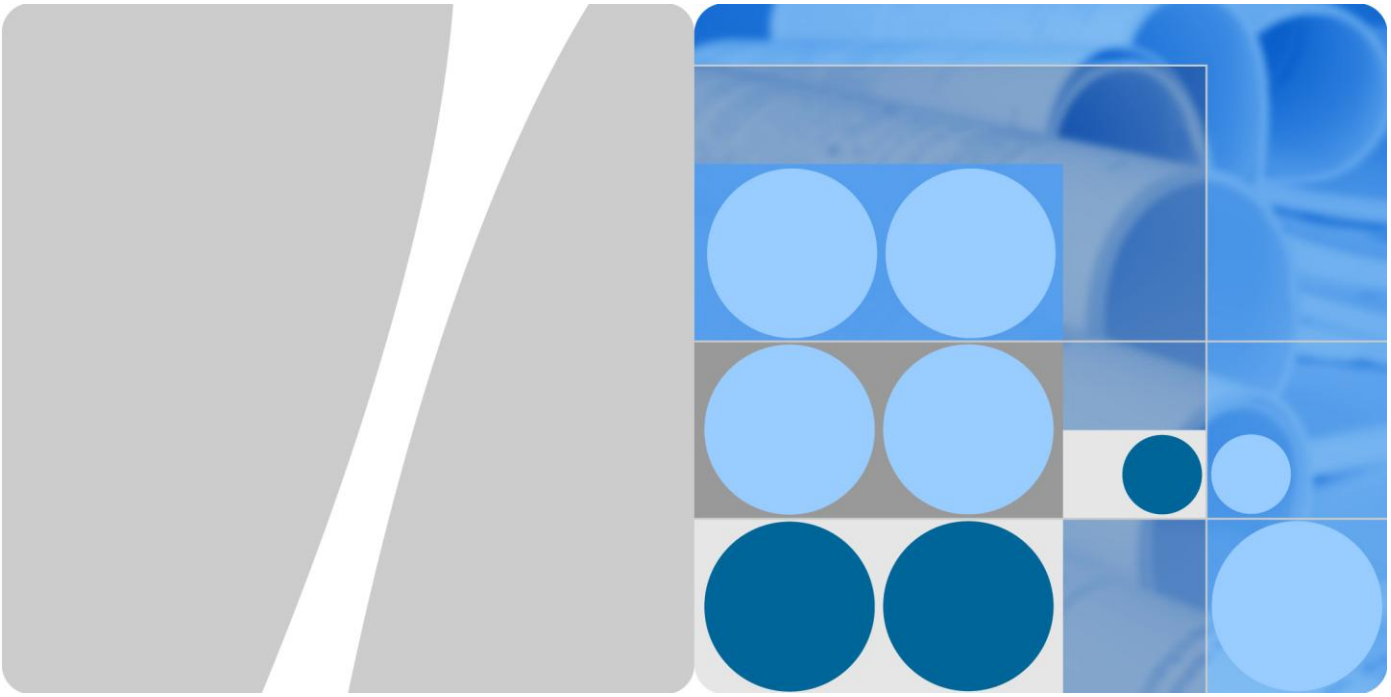


华为 eSight

产品描述

文档版本 01

发布日期 2014-07-25

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://enterprise.huawei.com

前言

概述

本文档介绍了 eSight 的网络地位、产品架构、组网应用和功能特性。同时提供了 eSight 的配置要求和技术指标。

本文档指导用户了解 eSight 的功能特性。

读者对象

本文档主要适用于以下工程师：

- 网络规划工程师
- 数据配置工程师
- 系统维护工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
	用于警示紧急的危险情形，若不避免，将会导致人员死亡或严重的人身伤害。
	用于警示潜在的危险情形，若不避免，可能会导致人员死亡或严重的人身伤害。
	用于警示潜在的危险情形，若不避免，可能会导致中度或轻微的人身伤害。
	用于传递设备或环境安全警示信息，若不避免，可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “注意”不涉及人身伤害。
	用于突出重要/关键信息、最佳实践和小窍门等。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害。

修订记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 01 (2014-07-25)

第一次正式发布。

目 录

1 产品定位和特点

1.1 产品定位

eSight（eSight V200R005C00）系统是华为公司研制的新一代面向企业敏捷网络园区、企业分支的运维管理系统，实现对企业资源、业务、用户的统一管理以及智能联动。

eSight 支持对多厂商设备进行统一管理，支持对 WLAN 无线网络进行监控和配置管理，支持对 MPLS VPN 网络进行监控和配置管理，通过 IPCA、SLA、网络流量分析功能对网络质量进行监视和分析。同时，eSight 提供灵活的开放平台，为企业量身打造自己的智能管理系统提供基础。

1.2 产品特点

多厂商设备管理能力

eSight 能够统一管理华为、H3C、CISCO、ZTE 等厂商的网络设备。eSight 预置对 H3C、CISCO、ZTE 等厂商主流设备的管理能力，同时提供灵活的自定义能力。

- 对于支持标准 MIB（RFC1213-MIB，Entity-MIB，SNMPv2-MIB，IF-MIB）的非华为设备，eSight 通过自定义设置就能达到与预置的非华为设备同样的管理能力；
- 对于不支持标准 MIB 的非华为设备，可以通过打网元适配包的方式进行适配。

支持多种操作系统

eSight 支持 Windows、SuSE Linux 操作系统，支持 Oracle 、MySQL、SQL Server 数据库。

差异化的版本

eSight 提供精简版、标准版和专业版三种版本，标准版和专业版可以根据业务发展的需要灵活增加新的业务组件。

版本类型	功能	使用场景

版本类型	功能	使用场景
精简版	告警管理、性能管理、拓扑管理、配置文件管理、网元管理、链路管理、VLAN 管理、日志管理、物理资源、电子标签、IP 拓扑、智能配置工具、自定义设备管理、安全管理、终端资源管理、MIB 管理、设备软件管理。系统监控工具、数据库备份/恢复工具、故障采集工具。	满足小规模的网络监控场景。
标准版	精简版功能、智能报表组件、SNMP 告警北向接口、SLA 管理组件、WLAN 管理组件、NTA 网流分析管理组件、MPLS VPN 管理组件、MPLS Tunnel 管理组件、Secure Center 安全策略管理组件、LogCenter 日志管理组件、IPSec VPN 管理组件。	满足大部分的网络管理场景，提供全方位的网络业务管理。
专业版	标准版功能、下级网管、双机热备。	提供对大规模网络的管理能力，管理规模可达 2 万网元。

多业务管理组件

WLAN 管理组件：对园区无线网络的无线资源（AC/AP）进行资源管理、配置管理，提供无线网络从用户侧到网络侧的故障诊断，提供有线无线一体化 TOPO 展示。

MPLS VPN 管理组件：提供图形化界面实现对 VPN 业务端到端配置，能自动发现网络中 MPLS VPN 配置，通过 TOPO 直观展示设备间的 VPN 网络逻辑结构，并提供对 VPN 的业务状态监控、业务质量监控、流量统计的能力。

MPLS Tunnel 管理组件：提供对 MPLS TE 隧道和 LDP 隧道的监控能力，包括查看隧道的运行状态、备份状态、隧道拓扑、隧道告警以及与隧道相关的 VPN 业务。

SLA 管理组件：通过两种方式相结合实现整网质量的可视化监控：包括基于仿真流和基于真实业务流的网络质量检测。网络仿真流的网络质量监测，与设备 NQA 特性配合，支持 7*24 小时主动诊断、度量网络设备间链路的性能。网络真实业务流的质量感知测试，基于网络包守恒算法，通过增强的分区域包守恒监控，不但实现了无连接网络的质量监控，同时也提供了精确故障定位能力，实现了质量监控+精确故障定位。

网流分析管理组件：基于报文来源/目的、协议、应用对网络流量报文进行分析，协助用户了解网络流量分布。

终端资源管理组件：提供接入网络中终端的 MAC、IP 以及接入设备的端口等信息，协助网络管理员进行故障定位。并能够根据用户设定的合法的 IP 和 MAC 地址范围，检测接入终端的合法性，帮助用户构筑安全的终端接入环境。

LogCenter 日志管理组件：eSight LogCenter 日志管理系统是华为面向运营商与行业用户推出的统一安全业务管理系统，是基于华为 B/S 的安全管理平台，实现对华为安全产品的全面网元管理、全方位安全业务分析和安全审计等功能，具有高集成度、高可靠性等特点。

SecureCenter 安全管理组件：能有效管理大规模华为防火墙/UTM 部署环境中设备的安全策略。包括：安全策略集中批量配置、公共对象配置、内容安全策略配置、安全策略发现、策略部署/拆除

2 产品架构

2.1 Web 化架构

eSight 系统采用 B/S 架构，拥有 B/S 架构的先天优势，通过客户端的浏览器即可访问 eSight 系统，当系统升级或维护时只需更新服务器端软件，减轻了客户端电脑载荷，简化了系统维护与升级操作，降低了用户的总体成本（TCO）。

另外，B/S 架构还具有如下优点：

- 具有分布性特点，可以随时随地进行查询、浏览等操作。
- 免客户端，新业务发布时只需要更新服务端。

2.2 独立的网元适配

eSight 采用扩展点机制实现了功能的增量开发与网元版本适配包的增量开发，达到不用修改原有发布包代码即可增加新的功能或新的网元适配包。基于 OSGI 平台的模块化框架使得各业务组件都可做到独立升级、打补丁。

当需要支持新的功能时，可以开发新的功能插件包部署到系统中；当需要适配新的设备时只需要增加新的网元适配包即可。功能插件包及网元适配包都以 Bundle（可理解为插件）的形态部署到 eSight 的 OSGI 容器中。

2.3 安全防护

eSight 针对网络安全问题，针对企业运维特点，提供全面的安全防护方案。

- 平台安全：包括系统加固、安全补丁、防病毒三类防护手段，通过提升操作系统、数据库的安全级别为 eSight 提供安全可靠的平台。
- 应用安全：包括传输安全、用户管理、会话管理、日志管理等方案。

2.4 北向接口

通过 eSight 北向接口可以灵活的将 eSight 集成到不同的 OSS 管理系统中，满足不同的 OSS 系统集成的需求。目前 eSight 仅支持 SNMP 的告警北向接口。

2.5 南向接口

eSight 南向接口实现 eSight 与设备之间的对接，完成 eSight 对设备的管理功能。

eSight 支持的南向接口类型，包括 SNMP、Telnet/STelnet、FTP/SFTP/FTPS/TFTP。

SNMP 接口

eSight 支持标准的 SNMP V1/V2C/V3 接口，通过 SNMP 接口可以实现 eSight 同网络设备的链接。用于发现网络设备，实现业务配置数据同步、故障管理和性能管理等基本管理功能。 SNMP 是基于 TCP/IP 的应用层网络管理协议，它使用 UDP 协议作为传输层协议，能管理支持代理进程的网络设备。

Telnet/STelnet 接口

Telnet 接口和 STelnet（SSH Telnet）接口是管理网络设备的基本接口之一，用于远程登录和管理设备。通过 Telnet/Stelnet 接口能够弥补通过 SNMP 接口管理的不足，并增加部分管理功能。eSight 通过 Telnet/STelnet 接口，可以与网络设备连接。

- Telnet 用于从 eSight 智能配置工具或网管启动命令窗口访问网元，直接使用 CLI 命令行对网元进行维护配置操作。Telnet 是基于 TCP/IP 的应用层网络管理协议，它使用 TCP 协议作为传输层协议，给网络通信提供服务。但 Telnet 采用明文传输通信数据，存在安全隐患。

说明

Telnet **采用明文传输通信数据，存在安全隐患，建议和** SSH **等安全协议配合使用。**

- SSH（Secure Shell）是一种类似于 Telnet 的工具。但是 SSH 在数据传输的过程中使用加密的数据。通过提供认证、加密和鉴别来保证网络通信的安全性，支持 password 和 RSA 认证，而且 SSH 传输的数据是经过压缩的，可以加快传输的速度。SSH 也是 TCP/IP 的应用层网络管理协议，在传输层使用 TCP 协议，但在应用层对数据进行了加密。

TFTP/FTP/SFTP/FTPS 接口

- Telnet 参数设置-修改网元的 Telnet/STelnet 参数。

FTP/SFTP/FTPS 接口用于备份设备数据。FTP/SFTP/FTPS 是基于 TCP/IP 的应用层网络管理协议。

- FTP（File Transfer Protocol）是用于在网络上进行文件传输的一套标准协议。密码和文件内容都使用明文传输。

说明

FTP **协议本身有安全风险，建议使用** SFTP **和** FTPS **等安全协议。**

- SFTP（SSH FTP）通过 SSH 协议提供安全的文件传输和处理功能。使用 SFTP 方式备份时，指令与数据在传输过程中都是经过加密的。
- FTPS（FTP over SSL）为 FTP 及数据通道增加了 SSL 安全功能，是一个在客户机和具有 SSL 功能的服务器之间的安全连接中数据进行加密与解密的协议。
- TFTP（Trivial File Transfer Protocol，简单文件传输协议）是 TCP/IP 协议族中的一个用来在客户机与服务器之间进行简单文件传输的协议，提供不复杂、开销不大的文件传输服务。

3 产品和应用场景

3.1 eSight 组网方式

eSight 包括单服务器、分布式和分级部署三种组网模式。

3.1.1 单服务器模式

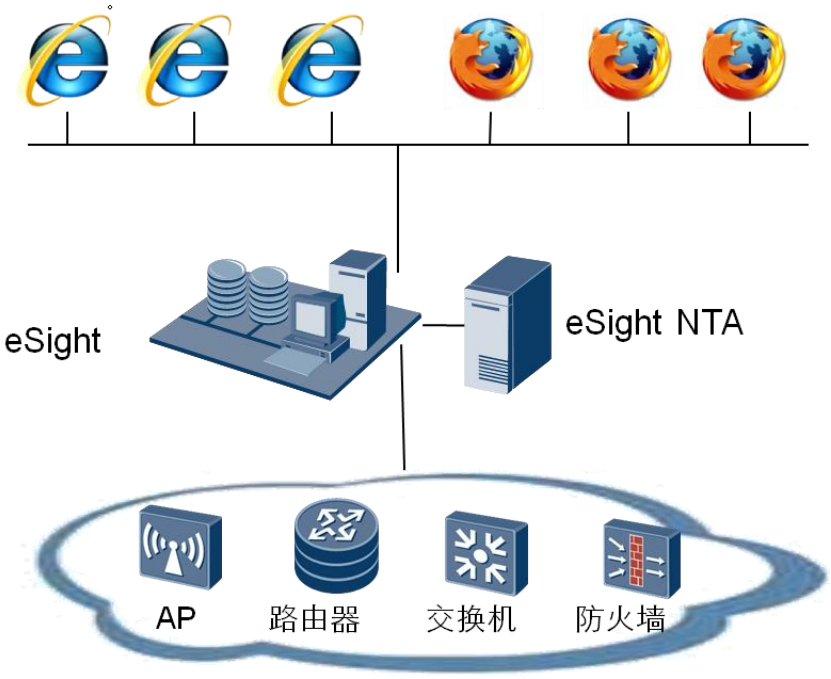
eSight 是 B/S 模式，支持多浏览器同时接入。

图3-1 单服务器部署模式

3.1.2 分布式模式

网流分析组件在大规模网络管理场景下，存在大量的系统资源消耗，eSight 支持将网流分析组件部署在另一台机器上，与 eSight 基础组件形成分布式部署模式。

图3-2 分布式部署模式

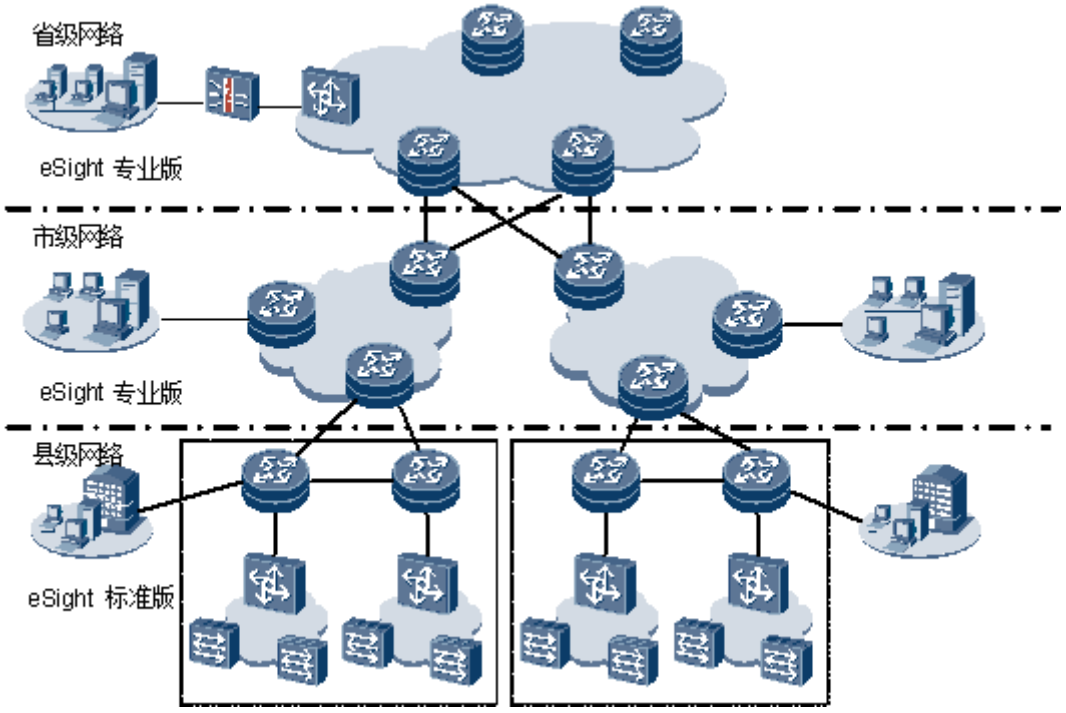


3.1.3 分级模式

eSight 支持分级管理，以满足企业总部监管各地区网络的需求。

在分级部署模式下，上级网管可以把下级网管加入到系统中，并提供打开下级网管界面的链接。当用户单击下级网管链接时，将会弹出一个新的浏览器窗口，在新的浏览器窗口中打开下级网管的登录界面。

图3-3 分级部署模式



3.2 eSight 与网元组网方式

eSight 可管理华为自研设备和非华为设备，如表 3-1 所示。

表3-1 eSight 管理的设备

领域	设备
交换机	S 系列交换机，CE 系列交换机
路由器	NE 系列路由器、AR 系列路由器
安全系列设备	安全设备 USG 系列、安全设备 SRG 系列、安全设备 SVN 系列
非华为设备	预集成的非华为设备：H3C、Cisco 等设备

华为设备：eSight 主要通过 SNMP 方式管理华为设备，支持网元管理、性能、告警、配置文件管理、终端资源等基础管理能力，支持 MPLS L3VPN、NTA 网流分析、SLA 管理、WLAN 业务管理、安全策略管理、日志管理等业务；

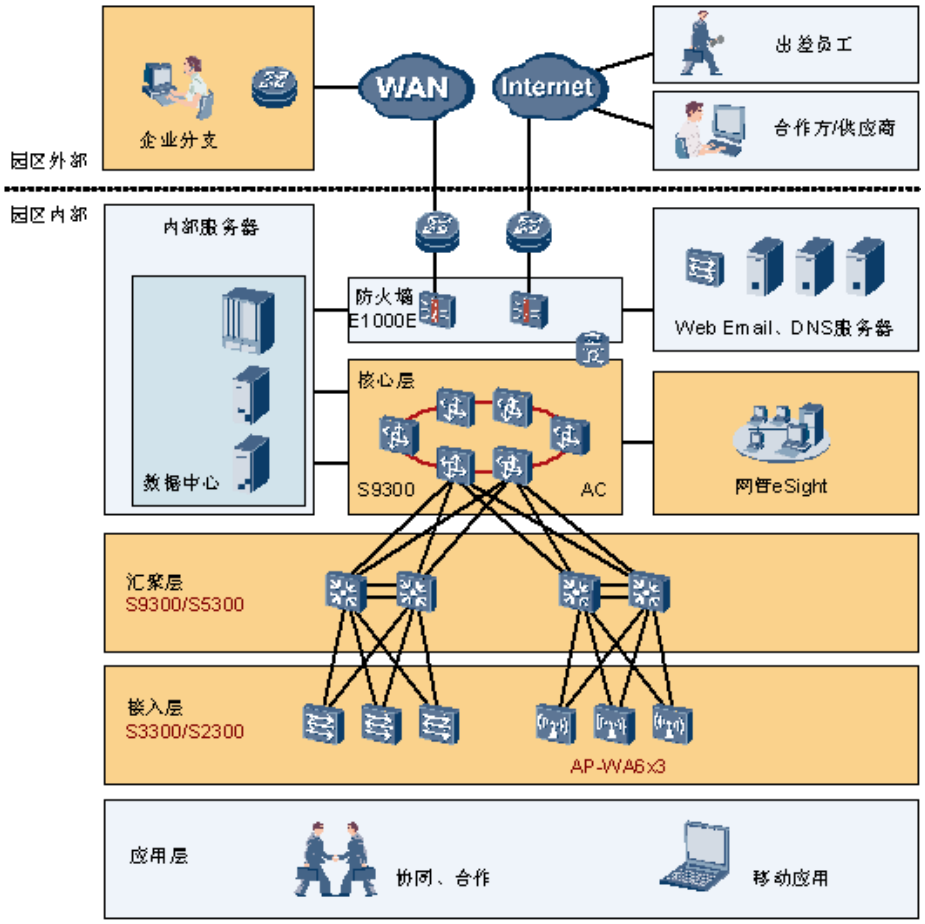
预集成的非华为设备：eSight 主要通过 SNMP 方式管理预集成的非华为设备，支持网元管理、终端资源等基础管理能力，支持部分设备的 MPLS L3VPN、NTA 网流分析、SLA 管理、日志管理等业务；

说明

详细的管理设备信息请参见《eSight 规格清单》。

企业园区需要实现分支、Internet 移动办公、无线用户等业务接入企业园区网络，通过 eSight 实现多系统集成管理和 IT 与 IP 的统一管理。eSight 与网元配合解决方案的场景如图 3-4 所示。

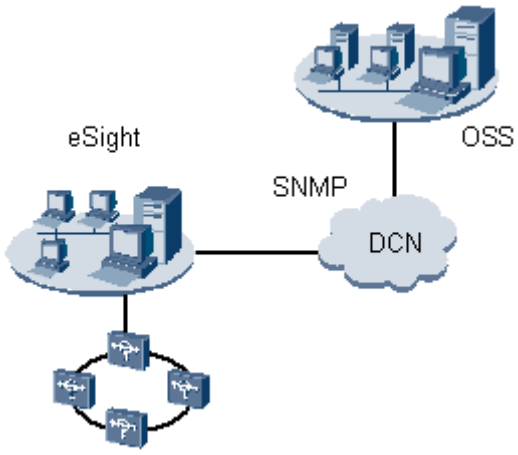
图3-4 eSight 与网元配合解决方案示意图



3.3 eSight 与 OSS 系统组网方式

eSight 系统通过北向接口接入到上层 OSS 网管系统。eSight 系统缺省提供了 SNMP 协议与上层综合网管进行告警北向对接。

图3-5 eSight 与 OSS 系统组网方式图



4 功能特性

4.1 系统 Portal 首页

eSight 提供 Portal 首页视图监控网络，缺省提供总览首页，可以设置展示在首页的内容。

用户可以设置展示在首页的内容，并选择 Portal 首页的布局方式。

基础网管 Portal 首页

- TopN 平均 CPU 利用率

显示近 1 小时、近 24 小时、近 7 天平均 CPU 使用率 TopN（默认 5 个）的设备。

- TopN 平均内存利用率

显示近 1 小时、近 24 小时、近 7 天平均内存占用率 TopN（默认 5 个）的设备。

- TopN 平均接口流入带宽利用率

显示近 1 小时、近 24 小时、近 7 天平均流入带宽利用率 TopN（默认 5 个）的接口。

- TopN 平均接口流出带宽利用率

显示近 1 小时、近 24 小时、近 7 天平均流出带宽利用率 TopN（默认 5 个）的接口。

- 网元 TopN 告警

以设备维度统计 TopN(默认 10 台)设备的紧急、重要、次要、提示告警的数目。

终端管理

- 终端在线趋势

  展示最近一段时间内，在线终端数的变化趋势。

WLAN Portal 首页

- 全网无线资源统计

  展示当前网络 AC 数（在线数、离线数、总数）、Fit AP 数（在线数、离线数、总数）和 Fat AP 数（在线数、离线数、总数）。

- TopN AP 上行端口流量与信道利用率
  展示当前网络的 Top N 上行端口流量与信道使用情况。
- TopN AP 接口流量统计
  展示当前网络的 Top N AP 接口的流量统计情况（仅支持 WLAN V2R5 之后版本的 AP）。
- TopN AP 用户关联失败率
  展示 TopN 的 AP 用户关联失败率。
- TopN SSID 用户统计
  展示全网 SSID TopN 的接入用户数统计。
- TopN WLAN 平均 CPU 利用率
  展示 TopN 的 AC/AP 的平均 CPU 利用率。
- TopN WLAN 平均内存利用率
  展示 TopN 的 AC/AP 的平均内存利用率。
- TopN 区域统计
  展示 TopN 的区域位置信息（AP 数、AP 用户接入数、用户数等）。
- WLAN 信道利用率
  展示一段时间 WLAN 信道利用率趋势。
- WLAN 全网在线用户统计
  展示一定时间范围内 Wlan 全网在线用户趋势。
- 客户端射频类型用户统计
  展示 2.4G、5G 用户数信息。
- 非法设备与非法客户端统计
  展示当前无线网络中存在的非法设备和非法客户端的数量。
- 干扰源统计
  展示当前对无线网络有影响的干扰源种类以及每种干扰源的数量。

SLA Portal 首页

- SLA 符合度
  展示最近一段时间 SLA 符合度最低的任务。
- TopN SLA ICMP 指标
  展示最近一段时间 SLA ICMP 指标的情况。
- TopN SLA ICMP JITTER 指标
  展示最近一段时间 SLA ICMP JITTER 指标的情况。
- TopN SLA UDP 指标
  展示最近一段时间 SLA UDP 指标的情况。
- TopN SLA UDP JITTER 指标
  展示最近一段时间 SLA UDP JITTER 指标的情况。
- TopN SLA TCP 指标

展示最近一段时间 SLA TCP 指标的情况。

- TopN SLA SNMP 指标
  展示最近一段时间 SLA SNMP 指标的情况。
- TopN SLA HTTP 指标
  展示最近一段时间 SLA HTTP 指标的情况。
- TopN SLA DNS 指标
  展示最近一段时间 SLA DNS 指标的情况。
- TopN SLA DHCP 指标
  展示最近一段时间 SLA DHCP 指标的情况。
- TopN SLA FTP 指标
  展示最近一段时间 SLA FTP 指标的情况。
- TopN SLA LSP PING 指标
  展示最近一段时间 SLA LSP PING 指标的情况。
- TopN SLA LSP JITTER 指标
  展示最近一段时间 SLA LSP JITTER 指标的情况。
- SLA 任务状态
  显示最近的任务运行状态。
- 最近智能策略任务

显示最近触发智能策略的任务。

QoS Portal 首页

- TopN 尾部丢包数
  展示最近一段时间尾部丢包数情况。
- TopN 最大丢弃速率

展示最近一段时间丢弃速率的情况。

- TopN 最大匹配速率

展示最近一段时间匹配速率的情况。

- TopN 最大流分类带宽利用率

展示最近一段时间流分类带宽利用率的情况。

- TopN 最大超出承诺带宽速率

展示最近一段时间超出承诺带宽速率的情况。

- TopN 最大通过速率

展示最近一段时间通过速率的情况。

- TopN 随机丢包数

展示最近一段时间随机丢包数的情况。

网络流量管理 Portal 首页

- TopN 接口流量
  展示最近一段时间接口流量 TopN（默认 5 个）的接口。
- TopN 接口利用率
  展示最近一段时间接口利用率 TopN（默认 5 个）的接口。
- TopN 设备流量
  展示最近一段时间设备流量 TopN（默认 5 个）的设备。
- TopN 应用流量
  展示最近一段时间应用流量 TopN（默认 5 个）的应用。
- TopN DSCP 流量
  展示最近一段时间 DSCP 流量 TopN（默认 5 个）的 DSCP。
- TopN 主机流量
  展示最近一段时间主机流量 TopN（默认 5 个）的主机。
- TopN 会话流量
  展示最近一段时间会话流量 TopN（默认 5 个）的会话。
- TopN 接口组流量
  展示最近一段时间接口组流量 TopN（默认 5 个）的接口组。
- TopN 接口组利用率
  展示最近一段时间接口组利用率 TopN（默认 5 个）的接口组。
- TopN IP 组流量
  展示最近一段时间 IP 组流量 TopN（默认 5 个）的 IP 组。
- TopN 应用组流量
  展示最近一段时间应用组流量 TopN（默认 5 个）的应用组。
- TopN DSCP 组流量
  展示最近一段时间 DSCP 组流量 TopN（默认 5 个）的 DSCP 组。

4.2 拓扑管理

拓扑管理以拓扑图的方式直观显示被管网元及其之间的连接关系和状态，用户可以通过浏览拓扑视图把握全网设备的层次结构和运行状态。

表4-1 拓扑管理基本概念

术语	说明
网元	拓扑管理的核心单位，用来标识被管理的设备。在拓扑视图中，不同的图标代表各种网元类型。
子网	按照某种原则（如按地域或按设备类型划分）将一个比较大的网络结构分解为几个相对较小的网络结构，以便网络管理。

术语	说明
链路	标识通信设备之间的物理或者逻辑连接。

浏览拓扑图

- 拓扑界面上分成左树右图的方式，对拓扑对象通过子网进行分层展示。
- 提供全屏、自适应屏幕等拓扑图整体、局部观测的能力。
- 显示网元、链路的告警状态。
- 富媒体 Tips 展现效果。
- 提供链路标签展现接口流量等性能采集数据的能力。
- 提供对 MP-Group 捆绑链路的父子关系展示、链路状态监控能力。

拓扑图操作

- 支持拓扑图的缩放、图片导出、图片打印、设置背景图、全屏、自适应屏幕、返回上一层等基本操作。
- 支持在拓扑上接入物理设备、查看设备管理信息、编辑网元基本属性及维保信息、设置协议参数、同步设备数据、节点移动、删除、保存位置等网元基本操作。
- 提供完善的右键菜单操作入口，支持在拓扑空白处右键弹出菜单、单设备及链路右键弹出菜单、多设备及链路右键弹出菜单等操作。
- 提供功能丰富的链路展现统一设置入口，支持链路两端接口流量、带宽利用率等性能监控数据的设置及展现、提供链路按类型及状态过滤的定制能力、链路颜色根据接口带宽利用率自适应调整、提供链路名称及链路 Tips 的定制能力。提供跨层链路标记及查询展现能力，跨层链路计算及标记、跨层链路详细信息表格展现、跨层链路详细信息查询。
- 提供灵活的设备图标大小及样式、链路线条粗细及样式的定制能力，用户可以根据实际的运维场景简单快捷地自定义设备图标或链路样式，支持批量操作。
- 提供丰富的拓扑自动布局设置，支持环形布局、对称布局、星形布局、上下树形布局等多种布局操作。
- 提供拓扑对象模糊查找能力，支持按名称和类型模糊搜索并快速定位到所关注的设备、链路、子网等拓扑对象。
- 对部分常用功能提供快捷键操作：

表4-2 拓扑快捷键清单

编号	快捷键	功能描述
1	Ctrl+A	全选拓扑资源，包括设备、子网、链路等
2	Ctrl+X	剪切选中资源，包括设备、子网
3	Ctrl+V	粘贴被剪切资源

编号	快捷键	功能描述
4	Ctrl+S	保存拓扑图
5	Ctrl+R	刷新拓扑，恢复拓扑为上一次保存状态
6	ESC	关闭当前弹出的模态窗口（拓扑图例、拓扑编辑的属性设置等非模态窗口不支持此操作）
7	Alt+鼠标滚轮	拓扑图放大、缩小

- 支持双击设备图标跳转到网元管理器快捷操作。

拓扑编辑

拓扑可编辑是拓扑操作能力的一个重要组成部分，辅助用户根据实际的运维场景和需求在拓扑上进行网络可视化的系统组织、描述、标记。

当前拓扑编辑支持用户在拓扑上任意位置绘制方框、圆、椭圆等常用图形，也支持用户在任意位置上编辑文字。用户可以通过点击工具栏的保存拓扑图按钮，保存自定义的图形或文字。同时也支持对已添加的图形、文字的属性进行编辑，支持剪切、删除、图层切换等常用操作的菜单项。

告警级别显示

拓扑节点的颜色直观地反映该节点相应的最高告警级别。用户可以根据图标动态刷新的颜色实时了解到全网设备的告警情况，如有紧急告警，可在第一时间确认和处理。

偏好设置

提供拓扑偏好设置的基础能力，用户可以根据需要设置拓扑背景图颜色、节点标签样式设置字体大小、颜色等、设备标签内容设置、子网默认展开样式；默认设备图标大小、链路标签字体大小、颜色、两设备间存在多链路时，链路间的间距、默认链路粗细。

网元管理集中入口

- 支持在拓扑上直接接入物理设备、创建子网、创建链路。
- 用户可以通过双击拓扑节点或者点击右键菜单的网元管理，快速进入到该设备的单网元管理界面。
- 支持单个及多个设备的 SNMP、Telnet 协议参数设置。
- 支持单个及多个设备的同步、状态刷新、剪切、粘贴、删除操作。
- 支持用户修改设备的基本信息、维保信息。
- 支持用户自定义设备图标的样式、调整设备图标的大小。

浏览网元的性能

用户可以通过拓扑视图中网元的 Tips 来查看网元的 CPU 利用率、内存利用率、响应时间、当日不可达比率。

浏览链路历史性能

用户可以通过拓扑视图中链路历史性能菜单查看链路接收速率和发送速率历史性能。

4.3 IP 拓扑管理

用户可以通过 IP 拓扑的菜单，进入 IP 拓扑界面，查看路由设备和二层设备及其之间链路连接。

表4-3 IP 拓扑管理基本概念

术语	说明
网元	拓扑管理的核心单位，用来标识被管理的设备。在拓扑视图中，不同的图标代表各种网元类型。
IP 子网	根据 IP 地址和子网掩码划分出的 IP 地址段。
链路	标识通信设备之间的物理或者逻辑连接。
路由设备	具备路由能力，可以连接多个网络或网段的网络设备。
二层设备	工作在 OSI/RM 网络体系结构中数据链路层的网络设备。

浏览拓扑图

- 拓扑界面上分成左树右图的方式，对拓扑对象按所属 IP 子网进行分层展示。
- 提供鸟瞰、全屏进行拓扑图整体、局部观测能力。
- 显示网元、链路的告警状态及 Tips 信息。

拓扑图操作

- 支持拓扑图的缩放操作。
- 支持拓扑图图片导出、图片打印、设置背景图。
- 支持拓扑图节点的移动，并保存设置。
- 提供其他功能的快捷操作入口。

告警级别显示

拓扑节点的颜色直观的反映该节点相应的最高告警级别，且是动态更新显示的。用户可以根据图标颜色了解到全网设备的告警情况，如有紧急告警，可以第一时间确认和处理。

网元管理集中入口

用户可以通过拓扑视图中网元的快捷菜单，快速进入到该设备的单网元管理界面。

接口 IP 地址变更显示

- 显示全网/单个网元接口 IP 地址的变更情况。

4.4 故障管理

告警管理包含以下功能：

- 告警管理提供全网告警监控、远程告警通知等方式第一时间通知维护人员，保证故障处理的实时有效性。
- 告警管理提供告警屏蔽、告警过滤、级别重定义等个性化定制功能，满足不同场景下的个性化需求。

告警基本概念

- 告警级别：根据影响业务的严重性，告警级别分为紧急、重要、次要和提示，如表 4-4 所示。根据不同的告警级别可以采取对应的处理策略。

表4-4 告警级别

告警级别	说明
紧急	已经影响业务，需要立即采取纠正措施的告警。
重要	已经影响业务，如果不及时处理会产生较为严重后果的告警。
次要	目前对业务没有影响，但需要采取纠正措施，以防止产生严重故障的告警。
提示	检测到潜在的或即将发生的影响业务的故障，但是目前对业务还没有影响的告警。

- 告警状态：根据告警是否被确认以及清除，告警可分为不同的状态。其中，告警确认表示有用户已经对此告警进行了跟踪或处理。告警清楚表示当告警产生的条件消除，设备恢复正常。告警状态的分类如表 4-5 所示。

表4-5 告警状态分类

告警类别	告警状态
当前告警	未确认未清除
	已确认未清除
	未确认已清除

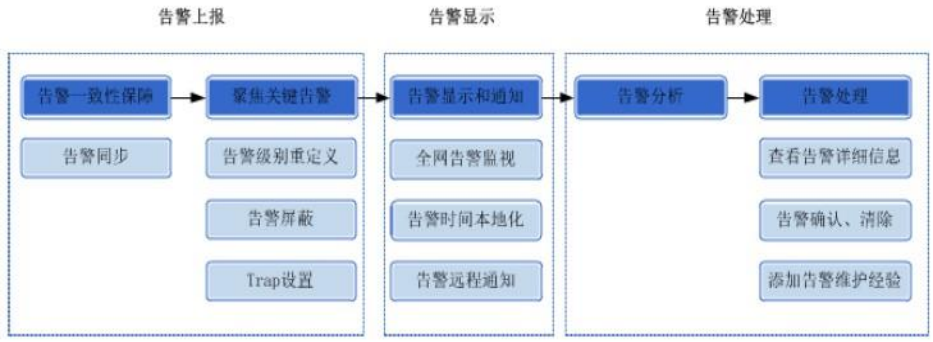
告警类别	告警状态
历史告警	已确认已清除

- 告警状态转换：告警状态转换分类的说明如表 4-6 所示。

表4-6 告警状态转换分类

告警状态转换类别	说明
清除状态转换	当告警产生的条件消除，设备恢复正常，此时设备将上报对应的清除告警，告警由未清除状态变成清除状态。
确认状态转换	对告警进行确认表示告警即将或已经被处理。告警被确认后，由未确认状态变成已确认状态。 如果要重新关注已确认的告警，可以对该告警进行反确认操作。告警被反确认后，由已确认状态变成未确认状态。

- 故障和告警：告警是系统检测到故障而产生的通知。并不是系统中所有故障都会产生告警，只有系统能够检测到的故障才会产生告警，对于不能检测到的故障，不会产生告警，但是该故障依然存在。
- 告警和事件：告警是指 eSight 检测到故障而产生的通知。事件是指被管对象除故障外发生变化的统称。告警发生时，用户必须进行排障处理，否则会导致由于 eSight 或设备异常而引起业务的异常。事件的发生只是告诉用户被管对象发生了变化，不一定会引起业务的异常。
- eSight 告警上报和处理流程：



全网告警监视

- 告警板：按照级别显示被管理对象的当前告警总数，简要的提供系统的故障状况，可作为监视面板。
- 告警声音：支持为不同级别的告警指定告警提示声音。当告警发生时，主机上的音箱会发出对应的声音。

- 当前告警界面：同屏滚动查询全部全网活动告警。通过设置过滤条件和搜索关键字查找搜索告警。并根据需要将常用的查询条件设置为告警查询过滤模板。详细功能如下：

表4-7 当前告警浏览页面功能说明

编号	功能说明
1	全局操作按钮，对选中的多条告警生效。 • 滚动锁定/滚动解锁 滚动锁定状态下，新上报的告警不会更新到当前列表中。锁定状态下确认且清除的告警不会列入到历史告警列表，解锁后才会更新到历史列表中。 • 确认：标识该告警已有用户处理，其他用户不需要关注。 • 清除：手工清除告警：当告警无法自动清除或已确认网元上不存在该告警的时候，可以单击按钮进行手工清除。 • 备注：供用户备注一些自己想记录的注意事项等信息，如告警处理进度及状态。 • 反确认：将告警从确认状态变为未确认状态。 • 组合排序：可以自由选择三列进行排序。 • 导出：将告警信息导出，方便其他用户定位故障和备份数据。
2	选择或设置过滤条件，浏览当前告警。系统预置告警过滤模板： • 未确认的紧急告警 • 未确认的重要告警 • 未清除的紧急告警 • 未清除的重要告警 • 最新一天的告警 如果预置的告警过滤模板不满足过滤要求，用户可以选择基于：级别、确认状态、清除状态、首次发生时间创建过滤条件过滤当前告警，并可以保存为新的模板复用。上述条件如果无法满足过滤要求，可以基于“更多选项”：告警类型、告警源类型、告警源、名称、定位信息创建告警过滤条件。
3	选择告警级别、确认状态、清除状态、首次发生时间、事件类型、告警源类型、名称、告警源、定位信息搜索告警。 单击“清空”可以清除已选的条件。 单击“过滤”可以按已选的条件进行搜索。
4	定制告警列表显示列。
5	针对该告警的操作按钮，eSight 从左到右提供了 4 个按钮： • 定位到拓扑，将告警定位到拓扑视图中产生告警的对象。 • 告警确认，标识该告警已有用户处理，其他用户不需要关注。 • 告警清除，当告警无法自动清除或已确认网元上不存在该告警的时候，可以单击按钮进行手工清除。

编号	功能说明
	• 提供告警屏蔽规则、告警级别重定义快捷操作。

告警屏蔽

- 通过设置屏蔽规则（属性包含日期、时段、告警源、具体告警）可以对某些不重要的告警进行屏蔽，使其不在当前告警列表中显示，避免大量的冗余信息。
- 网元在维修、测试或者开局期间，网元上报的告警会特别多，但此时不需要关心上报的告警，因此对处于这种状态的网元上报的告警信息要予以屏蔽，既不显示，也不保存。
- 屏蔽规则中告警源支持所有告警源和自定义告警源，支持选择设备、接口、子网、设备分组、接口分组做为自定义告警源。

告警级别重定义

eSight 提供对网元侧的告警进行级别重定义功能，用户可以根据实际需要重新设置某些告警的级别，提高或者降低告警的关注度。

告警远程通知

通过设置告警/事件远程通知规则，选择告警源，支持所有告警源和自定义告警源。支持选择设备、接口、子网、设备分组、接口分组做为自定义告警源。在产生符合通知规则的告警/事件时，eSight 通过短消息、邮件方式将告警/事件信息发送给指定人员，便于不在现场的维护人员及时了解到设备告警情况从而采取相应措施。

远程通知支持自定义通知内容模板和通知用户组（通知用户组为系统设置，对整个系统生效，供所有具有远程通知功能模块使用）。

自动确认规则

通过设置自动确认规则，eSight 通过将处于清除状态的当前告警，按照指定的规则进行自动确认，以简化用户操作。

系统支持对已清除未确认的“紧急、重要、次要、提示”级别告警进行自动确认。启用实时确认前已清除的告警不受影响。

告警时间本地化

上报告警的网元可能和用户使用的网管不在同一时区，为了方便用户准确的了解告警发生的时间，eSight 会自动将告警的时间（网元时间）转换为网管的本地时间。

eSight 支持所有告警的产生、确认、清除，上报到网管时间均显示为网管本地时间。

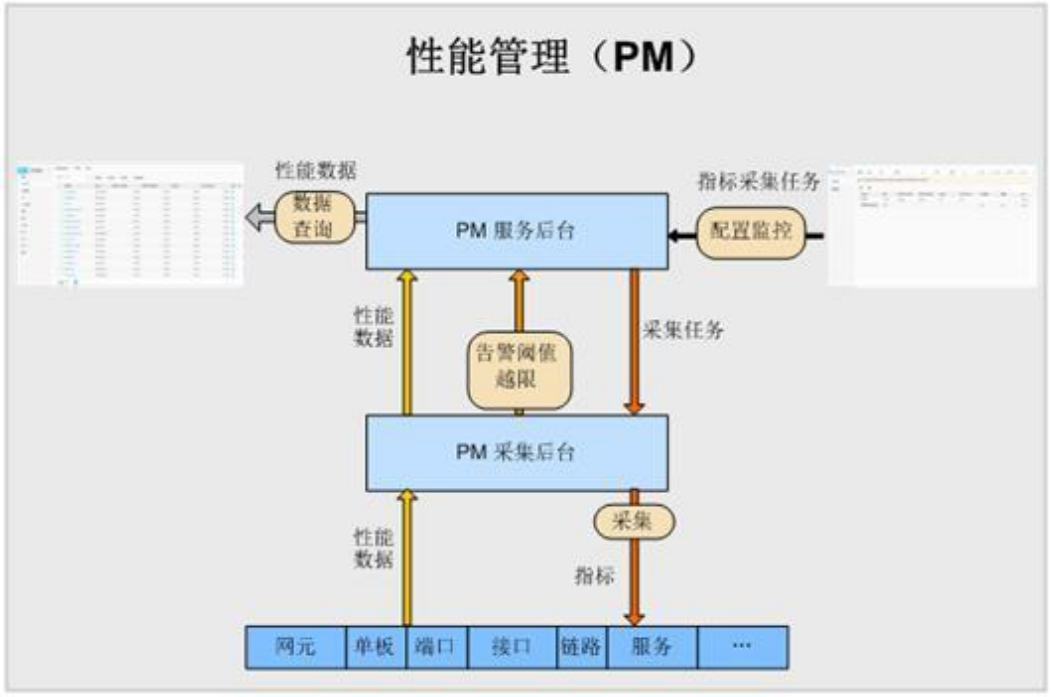
4.5 性能管理

网络在正常运行过程中，内部与外部的原因可能会影响网络性能的下降，引发网络故障。为保证当前网络在低成本下的性能足够，并为网络性能未来需求作准备，需要规划、监控与衡量网络效率，如通断率、利用率等。通过性能管理可以提前发现这种劣化的趋势，并在故障发生前解决掉这些隐患，规避网络故障风险。

性能管理

eSight 通过可视化的操作界面对网络的关键性能指标进行监控，并对采集到的性能数据进行统计，方便用户对网络性能进行管理。如图 4-1 所示。

图4-1 统一性能处理过程



eSight 性能管理提供了指标模板管理、采集任务管理、历史性能查询、实时性能查询、性能指标采集状态监控等功能。如下是对性能管理各模块功能的大体介绍。

监控模板

同一类型的设备具有相同的指标属性，将这些指标设置为一个指标模板，创建性能采集任务时直接加载，可以快速设置指定设备的采集指标。

eSight 监控模板管理支持：

- 增加、修改、删除指标模板。
- 在监控模板中设置指标，即收集网络资源的哪些性能数据。

- 在监控模板中设置性能指标的阈值。同时，可设置连续次数，即如果指标连续多次满足阈值条件，网管才会产生告警。用户通过告警，可以监控指定资源的性能。

  阈值包括上限触发值、下限触发值、上限清除值、下限清除值。相应的阈值告警分为上限阈值告警和下限阈值告警。

监控设置

eSight 以任务形式统一管理性能数据采集。采集任务定义了对哪些设备的哪些指标进行采集。设备的指标被采集后，就能查看到该设备的此项历史性能数据。

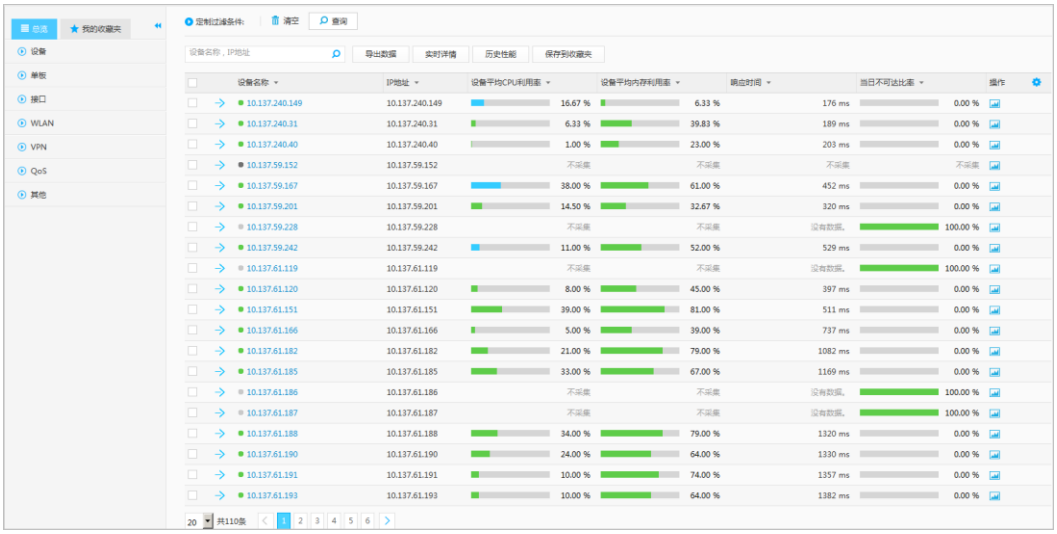
eSight 监控设置包括以下功能：

- 支持增加、删除、启动、停止、修改性能采集任务。
- 支持查看性能指标的采集状态、阈值设置等。
- 修改采集周期。
- 查看各设备的指标采集状态是否正常。
- 直观地展示任务的指标采集情况，同时支持直接在表格中调整指标的采集与否，以及阈值设置。

性能数据

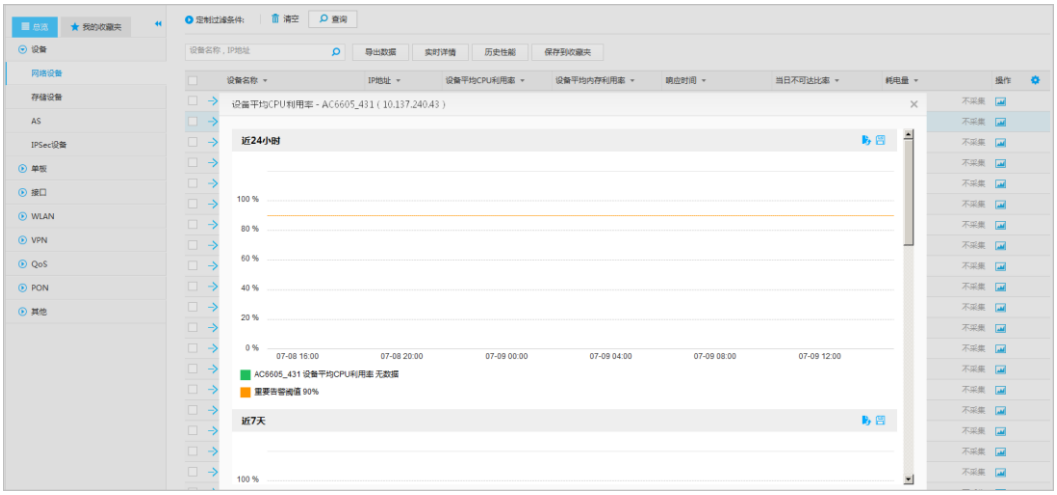
用户可通过性能数据总览界面，对各种资源的当前性能数据进行浏览和排序。同时提供了丰富的过滤条件，支持用户对自己关心的资源进行过滤，并将过滤的结果保存到收藏夹中，以便下次直接打开，如图 1-2 所示。

图 1-2 性能数据



当用户发现某个对象的某个指标值过高时，可以单击表格中该指标对应的单元格，直接打开这个指标的历史曲线图进行查看。界面中同时展现了近 1 天、近 1 周、近 1 月、近 3 月的历史曲线，方便用户对历史情况进行分析，确认当前指标值是否异常，如图 1-3 所示。

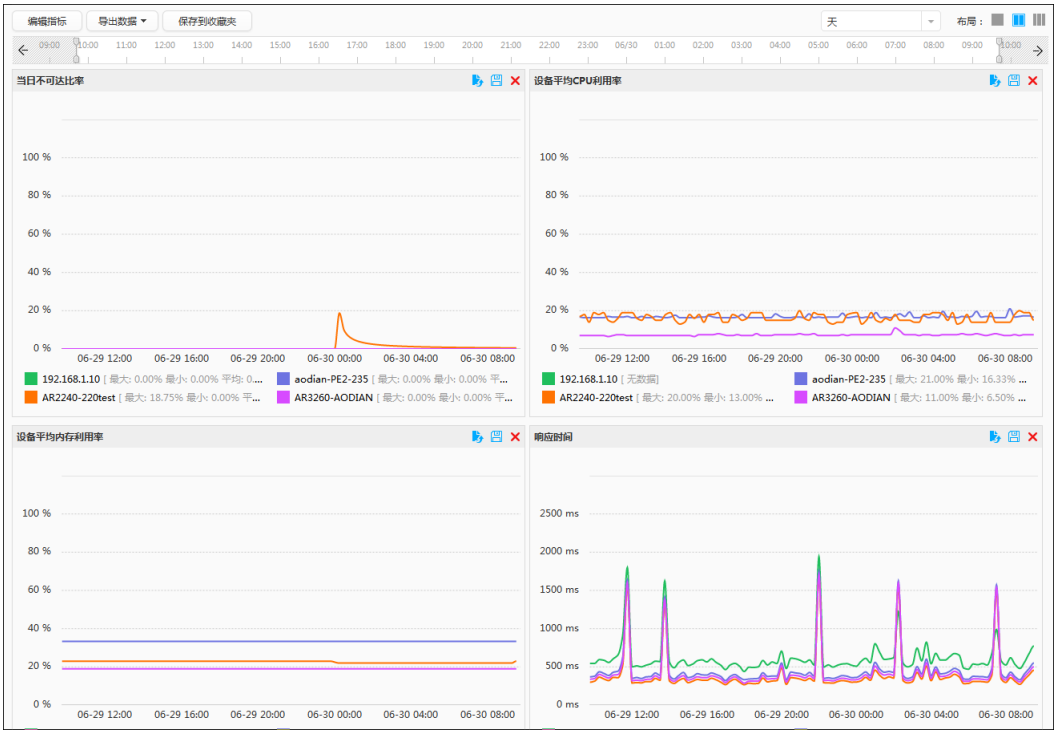
图 1-3 历史曲线图



用户在性能数据总览界面中，可以查询实时和历史性能数据，具体见下文。

历史性能数据

eSight 通过性能采集任务采集设备性能数据后，用户可以通 eSight 客户端指定指标、资源来查看历史性能数据，以了解设备历史性能趋势并预防故障发生。



用户可以在历史数据界面中，编辑要查看的指标。用户可拖动通过图表上方的时间划块来改变图中的曲线的时间范围。同时，用户可以改变页面的布局，设置页面显示是 1 列、2 列、3 列。

用户对指标、布局的编辑结果，可以保存到收藏夹中，用户下次打开后，就能直接显示这些对象的这些指标的历史曲线，无须再通过数据总览界面进入。

实时性能数据

通过监控设备实时性能，可以了解设备的当前运行状态，以便确认设备当前是否异常并及时采取措施。例如，当有阈值告警（如 CPU 占用率高）上报后，通过查看实时性能，可以确认设备当前是否存在对应问题。

eSight 提供数据曲线图实时查看性能数据。

- 支持设置查询条件查看实时性能数据。
- 支持导出查询结果到“.csv”文件。
- 通过网元管理器中的性能 KPI，及时了解网元关键性能指标的当前值。
- 支持保存到收藏夹，用户下次可以直接打开进行实时监控。

我的收藏夹

我的收藏夹，支持用户可按照自己的管理方式，组织自己关心的数据。总览数据、历史性能、实时性能均可保存到收藏夹中。

4.6 资源管理

网管对设备的管理，包括提供子网的管理方式，用户可以根据实际设备的物理位置，划分不同的子网对设备进行区域管理。提供自定义分组的管理方式，用户可以将多台设备划入一个分组，以简化后续对这些设备的批量操作。

同时针对企业网用户提供用户对设备的配置、查询功能，提供用户对设备机框、单板、子卡及端口的查询功能。

添加设备

说明

支持 SNMP 接入和 ICMP 接入两种方式。如果用户只需要监控设备的连通状态，则可以通过 ICMP 接入方式将设备添加到网管，此时不需要设定设备的 SNMP 参数。

添加设备作为网管管理的基础，用户可通过多种方式完成网管添加设备的过程。支持三种方式的设备添加方式：自动发现设备、手工创建单个设备、手工批量导入设备。

- 自动发现设备

立即发现：通过设备自动发现功能，可以根据指定的 SNMP 协议信息在指定 IP 网段中搜索设备，并把发现的设备增加到网管中。

定时发现：用户可以设置定时发现周期，网管根据指定的周期定时执行立即发现。

- 手工创建单个设备

  用户可以手动输入设备 IP 地址，设定设备的 SNMP 参数，实现将单个设备添加到网管。

- 手工批量导入设备

  用户可以以文件方式导入设备 IP 地址、SNMP 参数信息，实现批量添加设备功能。

设备/子网管理

设备/子网管理包括以下功能：

- 查询设备/子网

  支持设置查询条件查询所关注的设备/子网。

- 创建/修改/删除子网
  - 通过创建子网，可以将设备添加到创建的子网进行分类管理。
  - 当子网信息变更时，可以修改子网的属性。
  - 当网络结构调整，不再需要 eSight 管理某些子网，可以删除这些子网。
- 查看子网信息

  支持查看子网的基本信息。

- 查看设备信息

  支持查看设备的基本信息和协议信息。

- 调整设备所属子网或者子网所属子网

  当网络结构发生变动时，可以根据实际情况，调整设备/子网，以便正确的体现设备、子网之间的关系。

分组管理

1. **设备分组：**

基于不同的监控运维场景需要，用户可以使用设备分组管理功能将需要维护监控的设备放入一个分组当中。

场景 1：

路由器设备和交换机设备，都要采集 cpu 内存信息，路由器做为骨干设备为及时发现设备异常，需要将路由器设备的性能采集周期设置相对交换机短一些，这个时候可以使用预置的路由器和交换机分组，基于分组做监控设置；

场景 2：

某块接入园区网正在做割接，可以根据设备名称（设备命名按照规范命名）建立分组，将该区域设备放入一个分组，在割接的时间段内，屏蔽该区域上报的告警；

系统预置设备类别分组：如路由器、交换机等；

支持按照设备名称、类型、所属子网、厂商、IP 地址、类别、备注、资产管理人，自定义设备分组；

设备增加完成后能够按照预置和自定义设备分组自动分组；

2. **接口分组**

基于不同的监控运维场景需要，用户可以使用接口分组管理功能将需要维护监控的设备接口放入一个分组当中。

场景 1：

网络中设备接口很多，重点需要关注影响网络运维的接口，可以使用预置的有链路接口分组，只对有链路的接口做流量性能数据采集；

场景 2：

某片网络区域用户大面积反馈上网慢经常掉线，可以针对这个区域网络出接口，接口别名或描述建立接口分组，对这个部分接口做重点的监控，采集数据做针对性分析；

系统预置有链路接口分组；

支持按照设备类型、设备类别、设备 IP、设备别名、设备名称、设备备注、资产管理人、接口速率、有链路、接口别名、接口名称，自定义接口分组；

设备接口同步完成后能够按照预置和自定义接口分组自动分组；

设备资源

- 提供用户浏览、查询设备名称、IP 地址、类型、软件版本、厂商、同步完成时间、维保时间、投入使用时间、维保到期时间、创建网元时间、时区、资产管理人、资产编号、购买日期、备注、设备所属分组等信息。
- 提供导入、导出设备资源、导入设备信息、设置/恢复网元不管理功能；
- 提供用户批量配置 SNMP 参数、Telnet 参数、NetConf 参数等功能，批量同步设备的功能，批量设置时区功能，批量移动设备到子网的功能；
- 提供用户修改和批量修改设备备注、维保字段等信息的功能；
- 提供查询设备实体数据功能；
- 提供定位到拓扑管理查看该设备的功能。

机框资源

提供用户对设备机框资源的查询、导出功能，及对机框备注进行修改功能。

单板资源

提供用户对设备单板资源的查询、导出功能，及对单板备注进行修改的功能。

子卡资源

提供用户对设备子卡资源的查询、导出功能，及对子卡备注进行修改的功能。

端口资源

提供用户对设备端口资源的查询、导出功能，及对端口备注进行修改的功能。

4.7 链路管理

链路管理通过自动发现、手动创建设备间链路连接关系，直观在拓扑视图上展示。并通过监控链路的状态，便于用户根据拓扑了解现网中的网络拓扑结构和监控网络变化。

链路发现

当前 eSight 主要支持 LLDP 协议，MAC 转发表，接口 IP 地址进行链路的自动发现算法，并支持用户手动调整链路。

显示规则

用户可以在“显示规则”的弹出窗口中，选择新的链路名称规则和 Tips 规则所需的字段，其中 Tips 在拓扑中的链路上展示。

链路删除

链路删除功能主要应用场景有两个：（1）物理拓扑上存在用户不想显示的某条链路，用户想将其隐藏起来，并且在自动发现或者手动发现时，都不显示；（2）拓扑中可能会存在发现错误的链路，此时需要将错误的链路隐藏不显示。

链路删除功能使用：如果用户不想显示某条链路，可以在物理拓扑或者链路管理中将其“删除”，则在网管中就不会对用户展现此链路；如果用户想恢复展现此链路，可以在链路管理的“查看删除链路”中进行链路恢复操作。

4.8 单网元特性管理

单网元特性管理功能列表

查看

- 基本信息-显示网元的概览信息，包括基本信息、性能 KPI、TOPN 告警和接口流量。
- 设备面板-以图形化方式显示该网元。
- 告警列表-显示当前网元的当前告警。
- 性能状态-显示当前网元的性能指标数据。

配置

- WEB 网管-打开该网元内嵌的 WEB 管理界面。
- 业务配置-打开智能配置工具对该网元进行配置。

- 接口管理-查看当前网元的接口列表，可以对接口进行启用、禁用、告警屏蔽、告警去屏蔽。
- IP 地址管理-查看当前网元的 IP 地址列表。
- 配置文件-查看、备份当前网元的配置文件。

协议参数

- Telnet 参数设置-修改网元的 Telnet/STelnet 参数。
- SNMP 参数设置-修改网元的 SNMP 参数。
- NetConf 参数设置-修改网元的 NetConf 参数(部分设备支持)。

4.9 终端资源

终端资源提供对网络中接入终端的统一管控手段。通过浏览终端接入历史、可疑终端日志、非法接入管理、远程通知等手段，便于网络管理员及时掌握终端的接入情况。

用户可通过两种方式进行终端资源的发现：用户手工触发的立即发现、系统周期执行的自动发现。

终端发现配置

- 支持设定是否解析终端名称
- 支持设定是否启用终端自动发现
- 支持设定终端自动发现的周期
- 支持设定需要发现接入终端的设备范围，该范围同时适用于立即发现和自动发现

白名单

用户将合法的 IP 地址和 MAC 地址在白名单中进行配置后，网管就会在发现终端的过程中，依据配置生效后的白名单，检测接入终端是否合法，并记录所有非法接入终端的详细信息，为用户审计非法接入情况提供依据。

接入绑定规则

用户可以配置 PORT-IP 或 PORT-MAC 规则以限制设备端口下准许接入的终端，可以配置 IP-MAC 规则以限制 IP 地址与 MAC 地址的对应关系，网管会将违反这些规则的终端识别为非法终端，并记录下详细的接入信息。

终端接入记录

- 查看终端接入详细信息和接入历史
- 查看终端的非法接入日志
- 跳转至物理拓扑中定位终端的接入设备
- 接入接口跳转到接口管理
- 跳转至设备面板中查看终端的接入端口
- 配置终端的备注信息

可疑终端日志

- 查看端口多 MAC 地址，识别端口下私接设备
- 查看重复 MAC 地址，识别 MAC 地址盗用
- 查看重复 IP 地址，识别 IP 地址盗用

非法接入管理

网管根据用户设定的 IP/MAC 地址白名单，自动识别出所有非法的接入终端。

- 查看非法接入终端的详细信息和非法日志
- 导出非法接入终端的详细信息
- 确认非法终端的处理状态

远程通知

用户通过配置远程通知，在系统发现非法接入终端的时候，发送邮件通知，帮助用户及时掌握非法接入情况。

4.10 VLAN 管理

VLAN 管理模块是对 eSight 网管内的 VLAN 资源进行统一管理配置的应用。主要包括管理全网 VLAN 资源；向各设备的端口下发 VLAN 配置（对于 Access 类型的端口，仅下发 PVID，对于 Trunk 类型的端口，下发 PVID 和允许通过的 VLAN；对于 Hybrid 类型的端口，下发 PVID，Tagged VLAN 和 Untagged VLAN 示设备和链路的 VLAN 拓扑 ）； 同时提供单设备下 VLAN 管理的功能。

VLAN 资源管理

提供统一查询模式，可以通过 VLANID 和是否存在 VLANIF 接口等条件查询当前存在的所有 VLAN 资源。

通过创建 VLAN，可以在全网范围内选择多个设备，将创建的 VLAN 资源直接下发到设备；支持一次批量创建多个 VLAN 资源。

通过删除 VLAN，可以在全网范围内将此 VLAN 删除；如果该 VLAN 在某个端口上已经被设置为 PVID，则可以将这个端口的 PVID 重新设置为另外一个 VLAN，默认重设值为 1。

VLAN 设备管理

提供统一查询模式，可以通过子网、设备类型、设备名称、设备 IP 地址等条件过滤查询符合条件的设备。

通过配置端口 VLAN，可以在全网范围内选择多个设备的多个端口，并将 VLAN 参数统一下发到这些端口上。

可以跳转到设备管理器中进行单设备 VLAN 的管理。

VLAN 拓扑

提供全网 VLAN 资源相关的设备和链路的统一拓扑视图。

可以在拓扑上查看某一条链路两端的设备接口类型以及接口 VLAN 详细信息；同时查看该链路上现在允许通过的 VLAN 报文信息。

提供按照 VLAN ID 过滤相关的设备和链路的功能；可以通过不同的 VLAN 查看哪些设备和链路允许该 VLAN 通过。

可以在拓扑上直接将某一个设备加入或者从某个 VLAN 中去除。

单设备 VLAN 管理

单设备 VLAN 管理在设备管理器中提供对该设备上 VLAN 资源的管理能力。

可以在该设备上创建和删除 VLAN。

删除 VLAN 时，如果该 VLAN 已经被某个端口设为 PVID，则用户可以将这个端口的 PVID 重新设置为另外一个 VLAN，默认重设值为 1。

提供批量修改该设备下多个端口的 VLAN 参数的功能；可以统一修改一批端口的类型和 VLAN 参数。

可以在该设备上新建/删除 VLAN IF。

提供对该设备上的语音 VLAN 进行管理的功能；包括设置设备上的语音 VLAN 的通信参数，包括生命周期以及协议优先级（802.1P/DSCP）；语音流源 MAC 地址和掩码；接收语音流的端口参数。

4.11 智能配置工具

智能配置工具用于对设备进行业务配置，支持配置模板和规划表对设备批量下发业务配置。

模板主要用于对多个网元进行相同业务配置的批量下发；规划表主要用于对多个网元进行相似业务配置的批量下发。 对于定时的下发任务，可以通过邮件通知执行结果。

模板下发

通过配置系统预定义模版、导入模版与自定义模板，以向导方式下发，对设备实现批量配置，并且可进行命令校验。

模板规划表下发

通过模板规划表方式对华为设备实现批量配置下发，用户在导出模板的规划表中填写业务配置参数，导入智能配置工具后以向导方式下发设备。

命令规划表下发

通过命令规划表方式对华为以及第三方设备实现批量配置下发，用户下载命令规划表模版，填写业务配置命令行，导入智能配置工具后以向导方式下发设备。

4.12 配置文件管理

配置文件管理指对设备的配置信息进行管理，提供对设备配置文件的导入、备份、恢复、比较、基线化管理。当网络出现问题时，可以根据之前备份的网络可运行时的配置文件与当前设备正在运行的配置进行比较，帮助您快速定位并恢复当前出现的故障。同时还支持配置变更管理，配置文件备份后会自动进行差异比较，获取配置变更，支持告警与邮件通知配置变更，帮助你即时了解网络的配置变更情况。

设备配置管理

- 备份任务

  按日、周、月为周期，按设定时间对任务所包含设备的运行配置文件进行备份。支持设置设备配置变更告警触发备份配置文件。备份任务可以按照定制的时间进行定时备份，也可以对备份任务进行立即备份操作，同时支持设备变更告警触发备份。备份的执行结果支持 Email 远程通知，备份任务的执行结果以邮件的方式通知用户，邮件当中以附件的方式告知用户执行备份失败的设备列表。

- 配置文件

  对指定设备的运行配置/启动配置进行备份，将选定的设备的配置文件恢复成设备的运行配置/启动配置，对选定的配置文件进行基线化，对选定的设备更改 FTP 操作类型(第三方设备不支持)，同时能够方便地查看设备上面已经备份到网管服务器的运行配置文件和启动配置文件，还支持以 Excel 形式导出配置变更统计报告。

- 配置文件

  对于已经备份到本地的配置文件，可以进行配置文件在线查看并进行比较配置文件差异和配置文件下载、导入配置文件以及配置文件删除操作。文件比较功能当前提供了已经备份到网管服务器的配置文件之间的比较。

- 配置变更

  对配置文件备份后网管会自动进行差异比较获取配置变更，配置变更界面可以方便地查询出配置变更的差异，快速地查看一个配置的增、删、改信息。通过查看详情弹出文件比较页面 了解配置变更的具体情况。

系统参数管理

- 备份参数

  配置每一台设备在网管服务器上保存的配置文件的数量的上限，该上限应用于网管服务器所管理的所有设备。对设备配置变更是否触发配置文件备份进行配置。

- 邮件通知

  创建配置文件备份任务执行结果提醒以及设备配置文件变更提醒。 支持选择收件人（选择范围为：系统 > 系统设置 > 通知用户设置 > 用户组 中增加的用户组、用户信息），配置文件变更提醒支持邮件主题及发送时间的设置。

4.13 MIB 管理

eSight 网管中提供 MIB 工具可以读取一个 MIB(.mib)文件进行编译，产生的目标文件将自动被放到 MIB 工具要使用的目录下供 MIB 工具使用。 支持 SNMP 协议版本

V1/V2c/V3 协议的查询操作，通过它可以有效、安全地对 MIB 数据进行读取和监控，从而实现对网络的有效管理。

MIB 编译

支持选择一个 MIB 文件执行编译操作，编译完成后可以选择结果文件的保存目录，具体 MIB 文件的编译结果显示在编译结果界面上。

MIB 加载

MIB 节点管理，支持 MIB 节点的上传、编译、加载、卸载、新建文件目录、删除操作。

MIB 操作

在设备 IP 框当中输入设备 IP 后，使用 SNMP 设备，设备连通后可以通过工具对设备做 Get/GetNext/Walk/TableView 等操作，操作过程当中如果用户想终止操作可以点击 Stop 操作按钮停止数据获取。

4.14 设备软件管理

设备软件管理是 eSight 网管对于管理设备的软件版本进行升级操作的功能模块，当前版本支持通过 AC 来升级瘦 AP 的软件版本，包括任务监控、升级向导和版本管理三个子功能。任务监控管理当前网管中所有的设备升级任务，实时反映升级状态；升级向导通过向导式创建设备升级任务；版本管理按照设备类型粒度统一管理设备软件映像文件。

任务监控

统一管理所有的设备升级任务，实时反馈升级状态。如图 4-2 所示。

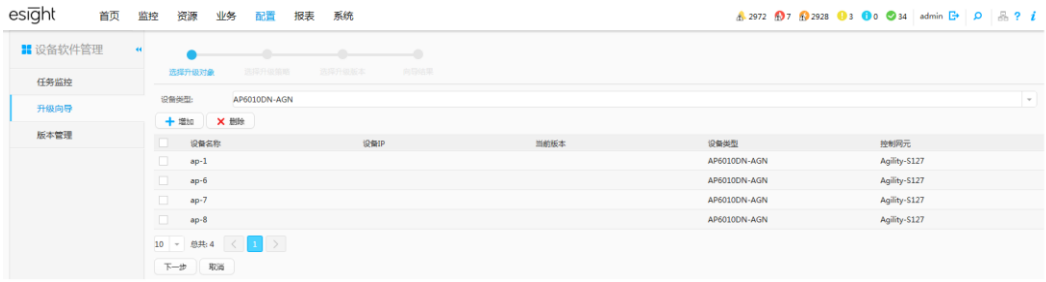
图4-2 任务监控示意图

- 目前版本支持瘦 AP 的软件升级，主菜单加鉴权处理，在 WLAN 业务组件安装的情况下展示。
- 瘦 AP 的升级支持单个与批量任务，若选取的瘦 AP 为 AC 下某种类型的全量 AP 则生成一条批量任务，提升效率并降低设备 telnet 连接通道负担。
- 升级任务当前进展有更新时实时刷新页面，对于失败的任务可进行重试操作。

升级向导

通过向导式创建升级任务。如图 4-3 所示。

图4-3 升级向导示意图



- 三步向导式创建升级任务并汇总任务详情。
- 可重置继续创建任务，亦可跳转至监控主界面查看任务执行实时情况。
- 选择升级版本步骤中增加版本管理创建链接，增加操作易用性。

版本管理

统一管理设备的软件映像文件。如图 4-4 所示。

图4-4 版本管理示意图

4.15 分级网管管理

eSight 支持用户建立分级分层的网络管理方案。在上级网管统一维护下级网管列表，通过链接可以直接打开下级网管的界面。从而实现查看下级网管告警、拓扑、性能和报表等功能。

分级网管提供如下管理下级网管的方式：

- 通过分级网管管理界面，完成下级网管的增加、删除、修改和手工连通性检测功能
- 通过下级网管 Portal 首页，可以实时监控各下级网管的连通性，并且可以单击各下级网管的链接，直接打开下级网管的界面

4.16 系统管理

轮询参数设置

- 提供轮询参数设置界面，可以设置定时同步时间、接口状态轮询、IP 地址轮询时间间隔。
- 设备定时同步：设备定时同步会同步设备上接口、实体、IP 地址等特性数据（不同设备可能存在差异），定时同步属于比较耗费系统资源的操作，一般将设备定时同步放在系统闲时执行。
- 接口状态轮询：轮询设备接口状态，不依赖设备 Trap 上报能产生“link up/down”告警，拓扑管理、IP 拓扑管理界面上对应的设备和链路状态根据告警刷新。
- IP 地址轮询：轮询设备接口 IP，主动感知设备接口 IP 地址变更，并刷新 IP 拓扑管理界面上对应设备，生成 IP 地址变更标记。

FTP 参数配置

支持 FTP、SFTP、TFTP 之间的切换。配置当前网管服务器所使用的 FTP/SFTP/TFTP 服务，可以对 FTP/SFTP 服务的用户名、密码以及 FTP/SFTP/TFTP 服务根目录进行设置，与此同时可以直观的看到 FTP/SFTP/TFTP 服务器当前的运行状态。

4.17 License 管理

License 是 eSight 管理容量、客户端接入数和使用时间等方面的许可。License 管理包括查询 License 信息、获取 ESN、设置 License 失效和导入 License 等。

License 管理所包含的主要功能有：

查询 License 信息

通过 eSight 客户端可以方便地查询 eSight 的 License 授权和消耗情况。

获取 ESN

通过 eSight 客户端获取 ESN，在申请新 License 时，需要提供 ESN。

设置当前 License 失效

当 ESN 变更或者网络调整时，可以设置当前 License 失效，并可以使用生成的失效码申请新的 License 文件。

导入 License

通过 eSight 客户端可以方便地将新申请的 License 更新应用到 eSight 服务器上。

说明

只有具备“更新 License”操作权限的用户才能导入 License 文件。

4.18 数据库数据溢出转储

为了避免数据库表空间不足而影响业务运行，eSight 提供了数据溢出自动转储功能。系统对于存在大数据量的模块每日定时检测数据库容量，在超出时系统自动将数据转储到指定的路径下。

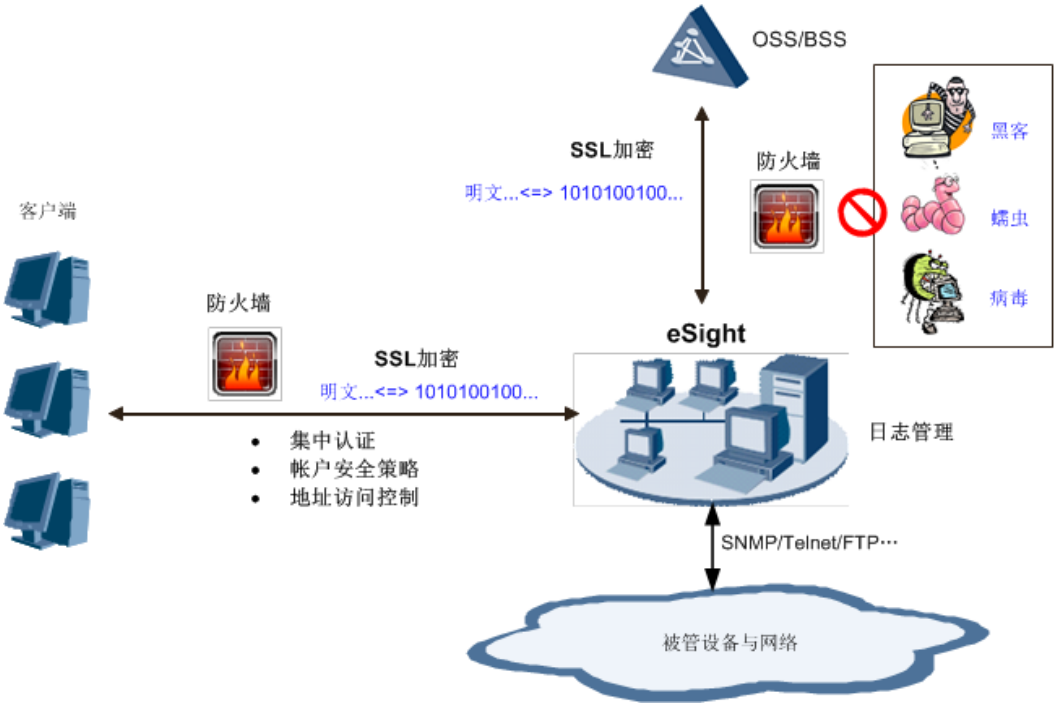
数据溢出转储包括日志数据库溢出转储、告警数据库溢出转储、性能数据库溢出转储、终端资源数据库溢出转储、网络流量数据库溢出转储、SLA 数据库溢出转储、配置文件数据库溢出转储。

4.19 安全管理

安全管理实现对 eSight 系统本身的安全控制，通过对用户管理、角色管理（授权管理——分权分域）、用户登录管理和一系列其他的安全策略，来保证 eSight 的安全。同时，eSight 支持对用户登录、操作和 eSight 运行过程中的日志进行管理，支持数据库备份，进一步完善安全解决方案。

安全管理的实现机制如图 4-5 所示。

图4-5 安全管理实现机制



说明

本节主要描述网管用户安全相关内容。

- 关于日志管理的安全方案，请参见 4.20 日志管理。
- 关于数据库备份和恢复，请参见 4.22 维护工具一节的备份恢复。

用户管理

用户需拥有合法的用户帐号和密码，才能成功登录 eSight 客户端并进行维护管理操作。eSight 通过用户名及其密码唯一确定了网管用户的登录和操作权限。

eSight 用户密码使用不可逆算法 SHA256 加密，并存储在数据库中。eSight 安装完成后，只提供一个缺省用户：admin 用户。admin 用户拥有所有的操作权限和管理权限。其他用户都是直接或间接地由 admin 用户创建的。

用户属性包含用户名、密码、所属角色、描述和访问控制。用户从其“所属角色”继承了对应的操作和管理权限。“访问控制”属性限定了用户只能在特定时间段、从特定 IP 地址登录 eSight，以确保 eSight 访问安全性。

用户管理包括以下功能：

- 创建用户：eSight 支持创建单个用户和批量创建用户两种创建方式。
- 删除用户
- 查看、修改用户属性
- 修改用户密码
  - 重置密码

当用户登录 eSight 客户端忘记密码时，可联系拥有用户管理权限的管理员重置密码。密码重置后，用户可以使用新密码登录 eSight 客户端。

说明

admin 用户的密码不能被重置。

- 修改当前用户密码

  用户可以在 eSight 客户端修改自己的密码。周期性的修改密码，可提高用户信息的安全性。

- 停用、启用用户

  帐号长时间未使用且达到帐号策略设置的帐号连续未使用天数时，帐号会被自动停用。暂时不使用某用户时，也可手工停用该用户。

  若需重新使用该用户时，可启用被停用的用户。

角色管理（权限管理）

角色是权限的集合，用于对用户进行授权。通过角色来对用户进行授权，可以使权限管理更有条理，避免权限管理的混乱。规划了网管用户后，需要给用户设置角色，使其具有对应角色的权限来管理设备。

eSight 角色管理支持创建、修改、删除角色及查看角色属性。

eSight 提供了一个缺省角色：Administrators。“Administrators”是管理员角色，拥有所有管理对象的所有操作权限，且不可修改。

角色属性包含角色名、包含用户、管理对象、操作和描述等。

- 管理对象：指角色可以管理的对象及其配置数据范围。如果 A 角色不可管理 C 设备和 D 对象组，则在拓扑视图上，C 设备和属于 D 对象组的设备对于只属于 A 角色的用户都是不可见的。对象组是多个设备的集合，eSight 支持创建、修改和删除对象组。
- 操作：指角色可以执行的具体操作。将一个设备的多个操作分配给不同的角色，可以达到各角色对同一设备拥有不同的操作权限。

通过设置角色的“管理对象”和“操作”属性，eSight 支持分权分域管理，即只允许用户将权限范围内的操作下发到网元。只有 Administrators 角色下的用户或者拥有“用户管理”权限的用户具备为其它用户分权分域的操作权限。

- 分域是指将网络中的管理对象分配给不同的角色，使每个角色拥有的管理对象范围不尽相同。通过分域，可以实现不同运维部门的人员管理不同范围内的网络对象。
- 分权是指将对管理对象的操作分配给不同的角色，使每个角色拥有的操作权限不尽相同。通过分域基础上的分权，可以实现同一区域不同职责（岗位/运维部门）的管理人员，对区域内管理对象可执行的操作权限不同。

eSight 的分权分域管理实现了网络设备和功能的统一管理，基于设备为单位实现分域管理，基于设备上的功能进行分配权限。

网管用户鉴权管理

eSight 的用户鉴权管理包含 3 种方案：本地认证方式、RADIUS 认证、LDAP 认证。

- 本地认证：网管用户管理、登录鉴权、安全策略完全由 eSight 服务器来集中独立完成。该方式是默认的网管用户登录鉴权管理方式，详细参见基于本地认证的网管用户鉴权。
- RADIUS 认证：用户登录时，eSight 通过 RADIUS 服务器对用户的登录请求进行校验和认证；并根据 RADIUS 服务器上用户所属用户组，映射到 eSight 系统中该用户的所属角色为登录用户授权。详细参见基于 RADIUS 认证的网管用户鉴权。
- LDAP 认证：用户登录时，eSight 通过 LDAP 服务器对用户的登录请求进行校验和认证；并根据 LDAP 服务器上用户所属用户组，映射到 eSight 系统中该用户的所属角色来为登录用户授权。基于 LDAP 的认证方式同基于 RADIUS 的认证方式类似，只是基于的认证协议不同，参见基于 LDAP 认证的网管用户鉴权。

基于本地认证的网管用户鉴权

在本地认证方式下，用户安全管理包括本地用户管理、权限管理、密码策略、帐户策略、登录控制等，从多方面保障 eSight 系统的安全运行。其中，账户策略和密码策略设置后对 eSight 所有的帐户生效。

- 密码策略
  - 密码最小字符个数（系统默认为 8 字符）。
  - 密码不能与历史密码重复次数（系统默认为 3 次）。
  - 密码中允许同一字符出现的次数（系统默认为 3 次）。
  - 密码修改最短时间间隔（系统默认为 5 分钟）。
  - 是否限制密码中至少包含一个特殊字符（系统默认为不限制）。
  - 密码的时效性：包含密码有效天数（系统默认为 90 天）和密码到期提前提醒用户修改的天数（系统默认为 7 天）。
- 帐号策略
  - 帐号名最小字符个数（系统默认为 6 字符）。
  - 帐号停用策略：连续多天（系统默认为 60 天）未使用停用帐号。
  - 帐号锁定策略：限定时间段内连续登录多次失败时，自动锁定帐号一段时间（系统默认为：10 分钟内连续登录 5 次失败后，锁定帐号 30 分钟）。
- 登录控制：登录控制包括用户登录时间段控制和用户登录 IP 地址控制。
  - 用户登录时间段的控制指如果当前时间不在登录时间段内时，用户将不能登录 eSight。
  - 登录 IP 地址的控制是指用户只能从特定 IP 地址的客户端登录 eSight 服务器。这样即使在某些情况下用户 ID 与密码被盗，盗号者也无法登录到 eSight 服务器上，从而进一步提高了 eSight 安全性。
- 客户端自动注销

  为了防止其他人员在用户离开时进行非法操作，eSight 提供设置客户端自动注销的功能。如果在指定时间段内不做任何操作，客户端将被自动注销。

基于 RADIUS 认证的网管用户鉴权

eSight 采用 RADIUS 模式对用户认证时，eSight 用户帐号不再需要管理员预先在 eSight 中创建。登录 eSight 的用户帐号是复用企业已有的、可以被 RADIUS 服务器认证通过的帐号信息。

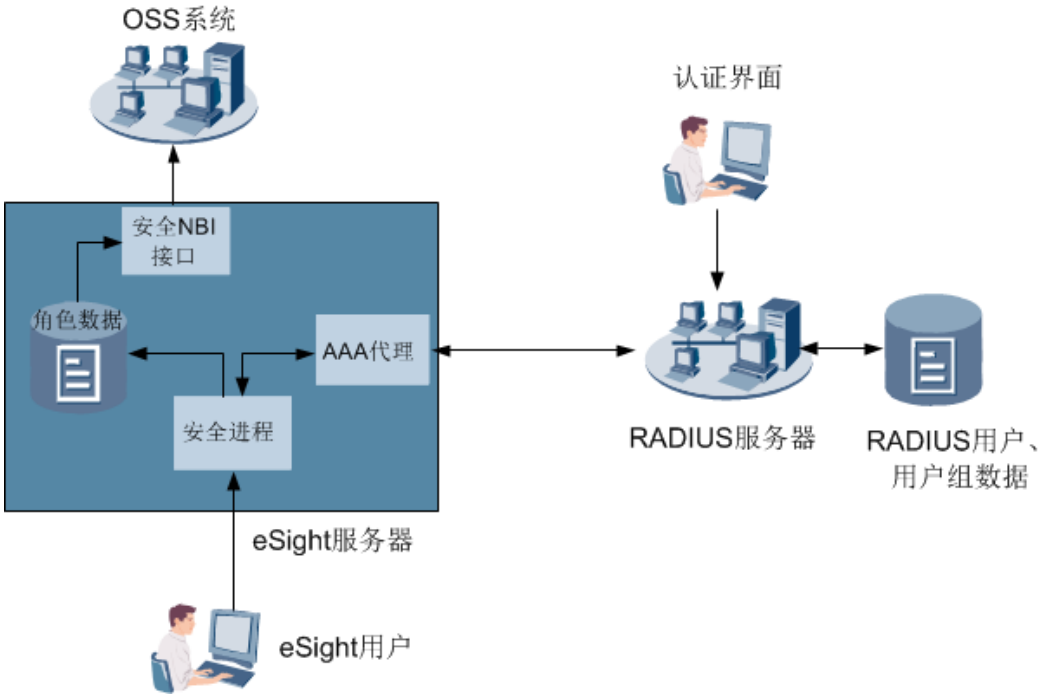
当用户输入用户名、密码登录时，eSight 服务器的安全进程将用户名、密码发送给 RADIUS 服务器。对于通过 RADIUS 认证的用户，eSight 安全进程将会从 RADIUS 服务器上获知用户所属的用户组，并映射到本地角色，实现用户授权。

说明

集成 RADIUS 的认证模式之前，必须保证 eSight 定义的角色名称与 RADIUS 服务器的用户帐号数据库的用户组名称一致，并保证将被授权登录 eSight 的帐号已经划定到了隶属的角色。

基于 RADIUS 认证的用户鉴权流程可以参见图 4-6。

图4-6 RADIUS 用户鉴权



基于 LDAP 认证的网管用户鉴权

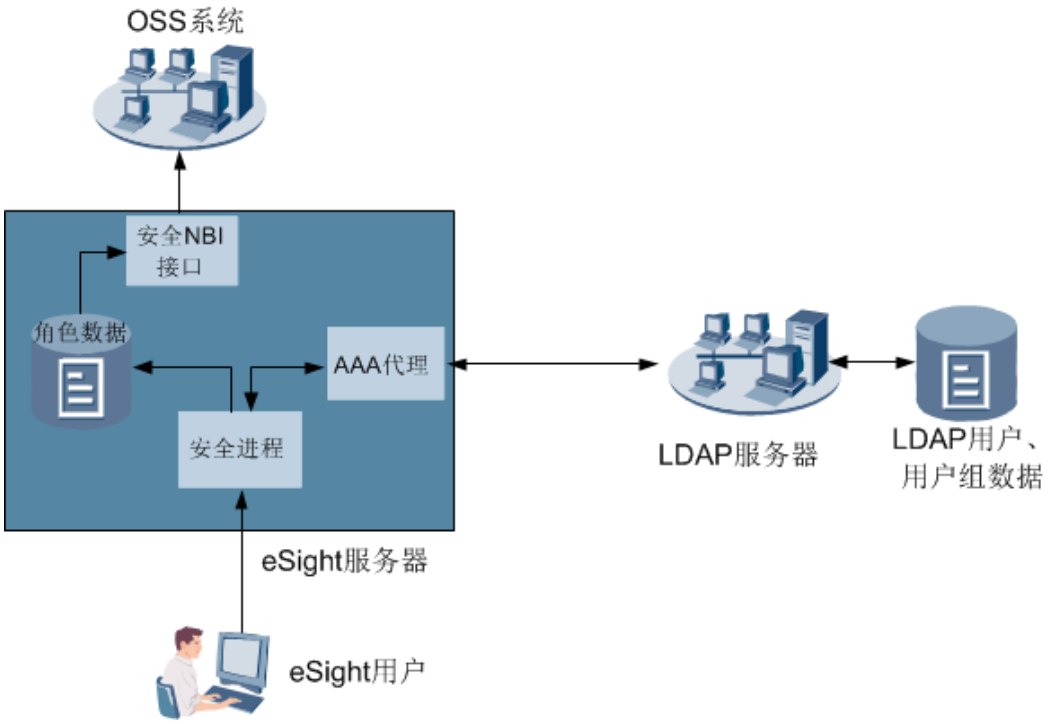
LDAP 在 VPN 和 WAN 中被广泛使用来控制用户连接的各个方面，是一个分布式客户端/服务器系统协议，可以防止未授权的用户访问网络。

基于 LDAP 的认证方式与基于 RADIUS 的认证方式类似，只是基于的认证协议不同。相对于 RADIUS 认证，LDAP 认证支持：

- eSight 和 LDAP 服务器之间的通信支持普通方式（不带加密）、SSL 方式和 TLS 方式。
- 支持多个 LDAP 认证服务器。

基于 LDAP 认证的用户鉴权流程可以参见图 4-7。

图4-7 LDAP 用户鉴权



会话管理

- 查看在线用户

  通过查看在线用户，能了解当前登录用户以及登录时间、登录 IP 等信息。
- 强制注销用户

  查看在线用户时，若发现一些危险操作或非法会话，可以强制将产生会话的用户帐号注销。
- 用户登录模式切换

用户登录模式指是否允许多用户同时登录 eSight，一般情况下 eSight 运行在多用户模式下，但如果需要对 eSight 服务器进行特别操作时，可以将 eSight 设置为单用户模式，防止其他用户的操作造成干扰。

- 进入单用户模式后，eSight 只允许当前用户登录 eSight 客户端，其他所有的在线用户会被强制注销。
- 退出单用户模式后，其他用户可重新登录 eSight 客户端。

4.20 日志管理

eSight 日志信息记录了用户进行的一些重要操作，用户可以查询日志列表并查看日志的详细信息，还可以导出操作日志、安全日志和系统日志。eSight 提供提示、一般和危险三种级别的日志信息

安全日志

安全日志记录用户在 eSight 客户端上进行的影响 eSight 安全的操作，如登录服务器、修改密码、创建用户和退出服务器等。

可以通过查询安全日志了解涉及 eSight 安全操作的相关信息，及时发现潜在的安全隐患并进行处理。

系统日志

记录 eSight 发生的事件，如 eSight 运行异常、网络故障、eSight 受到攻击等，有利于分析 eSight 运行状态，排除故障。

可以通过查询系统日志了解涉及 eSight 系统操作的相关信息。

操作日志

记录用户触发的各种修改网管数据的操作，如新增监视图、修改资源管理器等。

可以通过查询操作日志了解涉及用户执行操作的相关信息。

4.21 自定义设备管理

针对企业网用户需要管理的多种厂商的设备类型，eSight 提供了自定义管理功能。用户通过自定义管理模块，完成对设备类型、性能指标、告警参数、Telnet 定制、配置文件管理、网元面板定制，增强对设备基本能力的管理。

厂商基本信息定制

厂商基本信息定制，完成对设备厂商的基本信息的定制功能，包括增加、删除以及修改功能。

- 厂商名称：当前要定制的厂商的名称。
- 厂商描述：记录用户关注的厂商信息。（可选择是否定制）
- 厂商电话：厂商的服务电话。（可选择是否定制）
- 厂商联系人：一般是厂商设备的维护人员。（可选择是否定制）
- 定义类型：区分当前厂商基本信息是由网管开发人员定制还是由用户定制，分为预定义和自定义两种类型，前者标识厂商基本信息在网管发布之前由开发人员定制，后者标识该厂商基本信息由用户定制的。

设备类型信息定制

提供对设备类型的定制功能。设备在加载到网管之前，如果系统中没有预定义信息，在网管显示此设备为 unknown 设备，网管只提供对当前设备基本信息的查看能力，不具备对设备告警、性能等的管理能力，用户通过自定义设备管理定制完设备类型信息之后，网管界面显示此设备的真实的类型信息，并能够对设备的标准告警、性能进行监控。

- 设备 OID：用于区分设备类型的标识。
- 设备类别：用于区分当前设备的特性，目前区分为交换机、路由器、服务器、打印机、安全设备等几种类别。
- WEB 网管链接：部分设备提供了 web 网管的功能，用户定制 web 网管链接之后，通过网元管理器提供的访问接口，自动链接到设备的 web 网管。
- 设备图标：可标识当前设备类型的图标，用户可任意定制。
- 定义类型：同厂商基本信息定制。

告警参数定制

提供按照 SNMP v1 和 SNMP v2c/v3 两种不同的 SNMP 版本定制告警参数的功能，包括增加、删除、修改功能。用户可通过此功能定制关注的告警信息。对于没有预定义的告警，在定制之前，网管丢弃设备上报的告警，用户定制之后，告警模块解析并上报此告警。

用户删除定制的告警参数，网管不会删除对应告警的历史告警信息，但是在删除之后，告警模块不再处理设备上报的此告警信息。

提供修改告警级别、事件类型、告警原因、修复建议、详细信息、告警定位参数的功能。

- 厂商名称：由于各个厂商的设备的告警参数不一致，告警信息的定制按厂商进行区分。
- 告警名称：告警信息的名称。
- 告警级别：告警的紧急级别，与告警模块一致，分为紧急、重要、次要、提示四个级别。
- 通知类型：设备上报的告警的通知类型，分为告警、恢复告警和事件三种类型。
- 事件类型：分为通信告警、设备告警、处理出错告警、业务质量告警、环境告警、完整性告警、操作告警、物理资源告警、安全告警以及时间域告警。
- SNMP 版本：根据设备支持的 SNMP 版本的不同，提供 SNMPv1 和 SNMP v2c/v3 两种不同的 SNMP 版本告警的定制功能。
- generic、specific、企业 ID：用户定位一条 SNMP v1 告警的关键参数。
- 告警 OID：用于定位一条 SNMP v2c/v3 版本告警信息的参数，对应告警数据包的 Trap oid 值。
- 告警原因：当前告警产生的可能原因。
- 修复建议：修复当前告警的可能的途径和方法。
- 详细信息：告警的详细信息。
- 定位参数：解析一条告警所需要的定位参数信息。

性能指标定制

提供定制用户关注的指标的功能，包括增加、删除以及修改指标的能力。用户定制指标之后在性能管理模块定制此指标的监控实例，性能模块在下一个采集周期采集定制的指标的数据。

- 指标名称：标识当前指标采集内容的指标名称。
- 指标组：根据指标采集对象的不同，分为不同的指标组。例如：用户自定义设备指标组、用户自定义机框指标组、用户自定义单板指标组、用户自定义接口指标组等。如果用户定制采集接口某个性能的指标，需要选择“用户自定义接口指标组”。
- 设备类型：当前定制的指标可用于采集的设备类型。
- 指标单位：指标显示的度量单位。
- 指标公式：是用户要监视的 MIB 节点及其运算的一个表达式。

网元面板定制

对于用户自定义的设备类型，网管提供默认的设备面板显示功能。用户可通过网元面板定制功能，实现使用设备照片或者高仿真图对设备面板的定制，包括机框、面板、子卡以及端口的定制功能。定制完毕，用户打开属于当前设备类型的设备面板之后，设备面板显示的就是定制后的高仿真设备面板。

Telnet 定制

Telnet 定制提供不同设备类型的 Telnet 参数定制功能。Telnet 参数定制可以定制设备 Telnet 基本信息：包括登录用户名提示符、登录密码提示符、登录失败提示符、下发命令提示符、退出命令、备注信息。以及 Telnet 的特权模式信息：包括特权命令、特权密码提示符、More 提示符、回显控制命令、交互式选择提示符、交互式选择命令、失败提示、排除失败。

用户通过完成 Telnet 参数定制，可以对设备进行 Telnet 连通性检测。通过读取定制的 Telnet 参数完成配置文件管理对设备进行配置文件的备份，完成智能配置工具对设备下发配置命令。

配置文件定制

配置文件定制提供对设备的配置文件管理的命令的定制功能，包括备份配置文件命令、恢复设备配置文件命令以及重启设备命令。用户完成配置文件定制之后，在设备配置文件管理模块定制属于当前设备类型的设备的备份任务，网管就可以对设备的配置文件进行备份管理。

- 设备类型：要定制的配置文件命令的设备类型。
- 备份命令：备份设备配置文件的命令。
- 恢复命令：恢复设备配置文件的命令。
- 重启命令：重启设备的命令。

4.22 维护工具

维护工具提供 eSight 的维护功能，包括服务器管理、进程管理、网元包安装和升级、eSight 配置文件和数据库备份恢复等。

系统监控

对服务器的内存、CPU 等基本信息进行查看功能。

数据库密码管理

通过维护工具，可以修改数据库的超级用户和普通用户密码。

操作日志

通过维护工具查询操作日志，可以了解维护工具的用户 sys 在日常操作中所执行操作的相关信息。

修改密码

通过维护工具，周期性地修改维护工具用户 sys 的密码，可提高用户信息的安全性。

启停网管

通过维护工具，可以快速启动和停止网管 eSight 网管。提供本地和远程的管理进程的启动和停止功能，并实现进程的守护，在异常终止的情况下可以自动拉起。

服务器管理

通过维护工具，建立网管服务器对网流服务器的管理关系。

备份恢复

提供备份策略定制、手工备份和手工恢复的功能，备份内容包括系统运行时的配置文件和数据库数据

通过维护工具的备份策略设置，提供定时备份功能。

通过手工恢复，将网管恢复到备份前的状态，保证使用网管的安全性。

4.23 报表管理

eSight 通过执行报表任务生成报表，支持周期执行报表任务、手工执行报表任务；生成的报表支持导出为 PDF、Excel、Word 等常见文件格式。eSight 预集成了丰富的报表模板，可以满足常见的网络运维报表需求。

报表任务管理

报表任务分为周期报表任务和手工报表任务两种。用户可以在任务中设置 Email 转发相关信息，在任务执行成功后，eSight 会将生成的报表通过 Email 发送给指定的收件人。

- 周期报表任务

  周期报表任务，系统会按照用户指定的运行周期定时执行。报表任务执行成功后，会将生成的报表保存下来，用户可以查看和管理某个周期任务生成的所有报表。用户也可以将所生成的报表导出成文件、通过 E-Mail 发送。

- 手工报表任务

  手工报表任务，用户手工执行后即时生成报表。任务执行成功后，用户单击“查看”，即打开生成的报表。用户在查看生成的报表时，可以将报表以指定的格式导出。

4.24 双机系统

eSight 高可用系统提供双机热备和倒换的全新功能。主、备站点服务器的软硬件配置要求完全一致，通过 Veritas 远程热备份技术，实现主、备站点数据实时同步，并动态监视 eSight 的运行状态。当主服务器发生硬件故障、操作系统故障、网管关键应用故障或心跳线路故障时，系统会自动倒换到备份服务器，倒换时间不超过 15 分钟。

双机部署

双机部署包括磁盘的 RAID 划分工具、Linux 操作系统、Veritas 软件、Oracle 数据库以及 eSight 软件的安装。为了降低安装难度，提高安装效率，其中 RAID 划分工具、Linux 操作系统定制成一键式安装，Veritas 和 Oracle 集成安装。

双机主备关联

主备关联功能用于将完成安装部署的两台机器建立主备关联关系。

双机主备断连

主备断连功能用于将两台已经建立了主备关联关系的机器拆分。

4.25 WLAN 业务管理

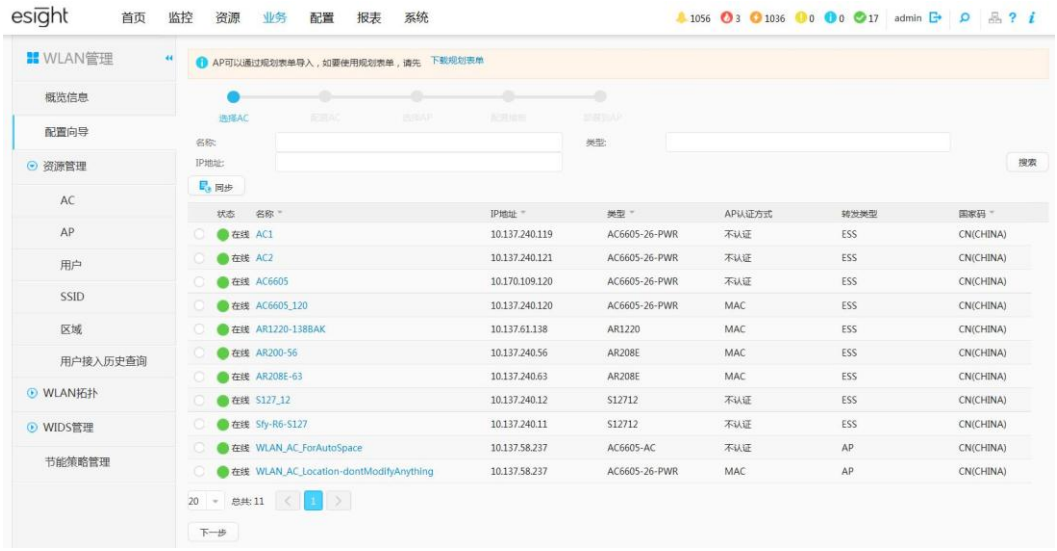
WLAN 管理提供了有线无线一体化的解决方案，实现了有线网络和无线网络的融合管理

- 向导式业务批量部署：批量 AP 统一下发无线业务配置
- 无线资源统一管理：AC、AP、无线用户、区域统一管理
- 用户故障诊断：诊断用户接入网络故障与用户接入后的健康度诊断

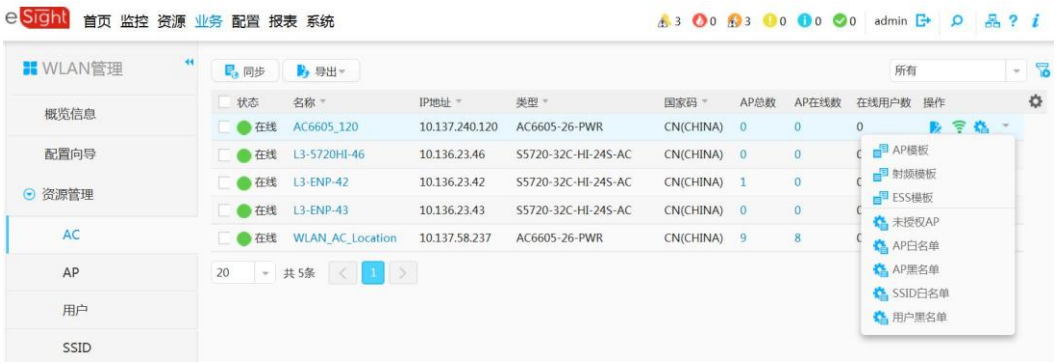
- 无线网络安全检测：WIDS 统一监控入侵网络设备与非 WIFI 干扰源，并提供频谱分析能力
- 无线网络拓扑可视化管理：基于区域对 AP 物理布放位置可视化呈现，并展现 AP 的热图覆盖

业务管理

提供向导式的业务配置，基于 AP 规划表单，端到端实现 AP 业务的统一下发与部署，大幅提升部署效率（相比手工部署效率提升约 90%）。



配置管理



WLAN 管理，提供 WLAN 设备配置，通过在线确认（未授权 AP 上线）、离线部署（添加部署离线 AP）、自动上线（符合白名单的 AP 自动上线）三种形式，方便、快捷完成 AP 与 AC 互通配置。

- AC 基本信息

  无线控制器对无线局域网中的所有 AP 进行控制和管理。AC 管理提供源接口、AP 认证方式、转发类型、国家码等业务配置。

- AP

AP 提供无线终端到局域网的桥接功能，进行无线到有线和有线到无线的帧转换。AP 管理提供 AP 基本信息配置、射频配置、模板绑定；支持预定义表单批量导入 AP、批量绑定模板；支持对 AP 重启、恢复出厂配置、替换、配置反制。

- AP 白名单

  网络管理员通过配置 AP 白名单确认合法 AP，完成 AP 上线。AP 白名单为合法 AP 的 MAC 或 SN 的列表。若 AC 的认证方式设置为 MAC 或 SN， 则当 AP 的 MAC 或 SN 在白名单中时，AP 自动上线。

- 未授权 AP

  当 AC 自动发现的 AP 对应的 MAC 或 SN 不在白名单中时，用户可在未授权 AP 列表界面查看当前 AC 自动发现的未授权 AP；同时，可通过批量方式在线确认，将 AP 加入白名单，实现 AP 上线。

- AP 域

  为了尽量减少 AP 参数调整的持续时间和影响范围，将 AP 划分成若干个域，将影响范围限定有这个域，减轻调整算法的开销。AP 域展示 ID、名称、布放类型、别名信息，并提供指定默认域操作。

- AP 白名单

  网络管理员通过配置 AP MAC 加入 AP 白名单，允许在白名单中的 AP 正常上线，不在白名单中的 AP 无法正常上线。

- AP 黑名单

  网络管理员通过配置 MAC 地址抑制 AP 上线。MAC 地址在 AP 黑名单中的 AP 无法上线。

- 用户黑名单

  网络管理员通过配置 MAC 地址抑制无线用户接入。MAC 地址在用户黑名单中的用户无法关联 AP。同时，可将非法用户添加至用户黑名单并配置 AP 的反制模式为用户黑名单，发起对用户黑名单中设备的反制操作。

- SSID 白名单

  网络管理员通过配置 SSID 白名单过滤对非法设备的探测。将无线网络周围一直存在、对网络环境无影响的 SSID 信号添加至白名单以后，则不会被识别为非法设备。

模板管理，提供网元级的预定义模板配置。

- AP 模板

  通过 AP 模板指定 AP 上行太网接口最大传输单元及日志备份相关设置。

- 射频模板

  通过射频模板配置无线传输数据过程中需要抢占信道、射频类型、速率、功率等相关参数。

- ESS 模板

  服务集是一个业务参数集合（SSID 名称、业务 VLAN、数据转发 ESS 接口、接入最大用户数、WLAN 用户接入安全管理等）。当它被绑定到指定 AP 的指定射频上时，即将它所有的业务参数应用到无线业务功能实体 VAP（Virtual Access Point）上。

网络监控

提供全网物理资源、统计数据、性能数据、用户接入历史、频谱分析等相关信息查看。

- 物理资源

  AC：包括状态、名称、IP 地址、类型、AP 认证方式、转发类型、国家码、区域位置信息、AP 总数、在线 AP 数、在线用户数等

  AP：包括状态、名称、别名、类别、类型、SN、MAC、IP 地址、反制开关、射频工作模式、接入 AC 名称、所属域、布放位置、定位开关、区域位置信息、在线用户数等

  用户：包括 MAC、IP 地址、用户名、接入 AC 名称、AP 名称、AP IP、认证方式、射频、SSID、区域位置信息

  SSID：包括 SSID、接入 AC 名称、接入 Fat AP 名称、ESS 模板名称信息

  用户接入历史：包括接入用户名、MAC 地址、接入 AP、接入 AC、接入结果、接入结果详细信息

  区域位置：包括区域名称、AP 总数、AP 在线总数、在线用户数总数。

说明

在支持定位的场景下，还显示区域的定位状态、启用定位的 AP 数

- 统计数据

  全网概览：包括用户在线趋势统计、Top 接入 SSID 用户统计、无线资源统计等，详细列表参见 WLAN Portal 首页；

- 性能数据

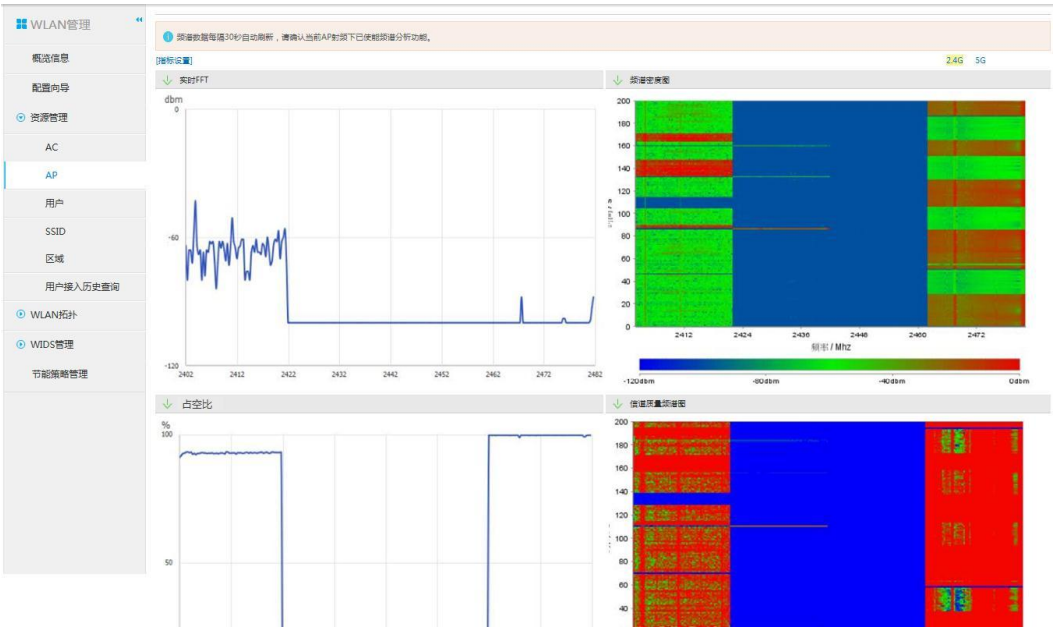
  AP 关联终端、AP 物理资源、AP 流量、射频流量、用户流量、WIDS 攻击数量实时性能统计；

- 用户接入历史

  记录用户接入历史信息。

- 频谱分析

在设备上使能 AP 射频的频谱功能后，在网管上可以查看 AP 周围的信号干扰情况，用户可从频谱图中识别信道质量以及周边环境的干扰源。频谱图包括信号实时图、深度图、信道质量图、信道质量趋势图、设备占空比。

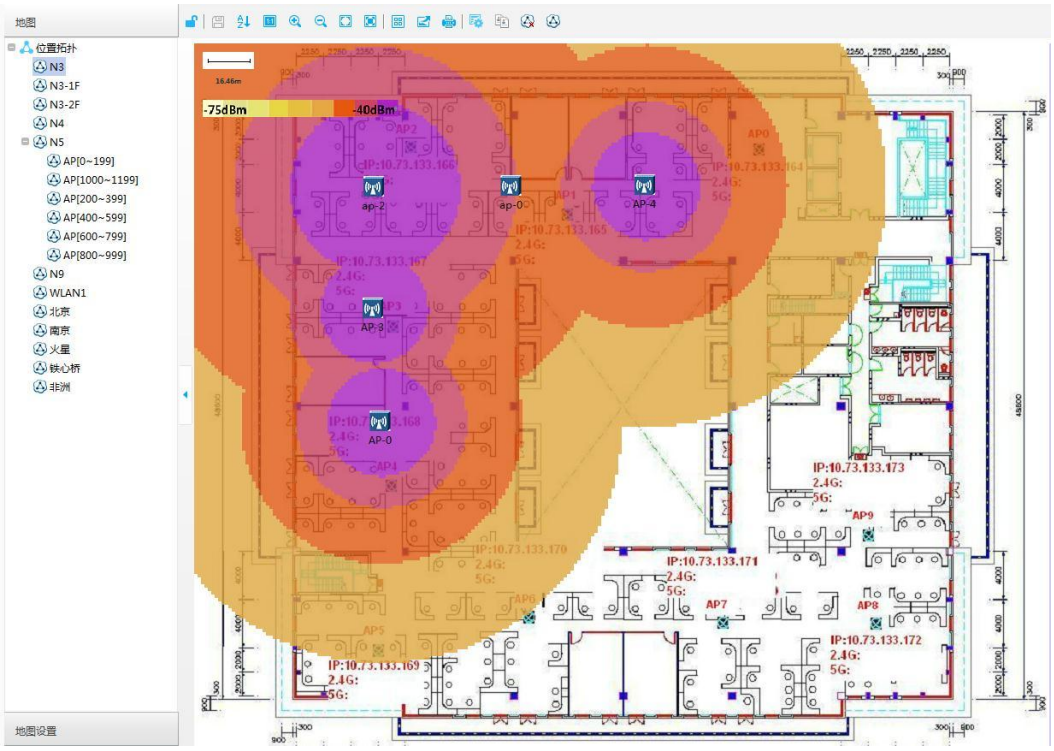


位置拓扑

位置拓扑支持依据物理位置按区域进行 AP 布放，热图覆盖可视化展现，帮助运维人员及时发现信号覆盖盲点与信道冲突域。对于具有定位 License 并使能定位的区域，拓扑刷新定位节点（非法设备和非 WIFI 干扰源）的位置。

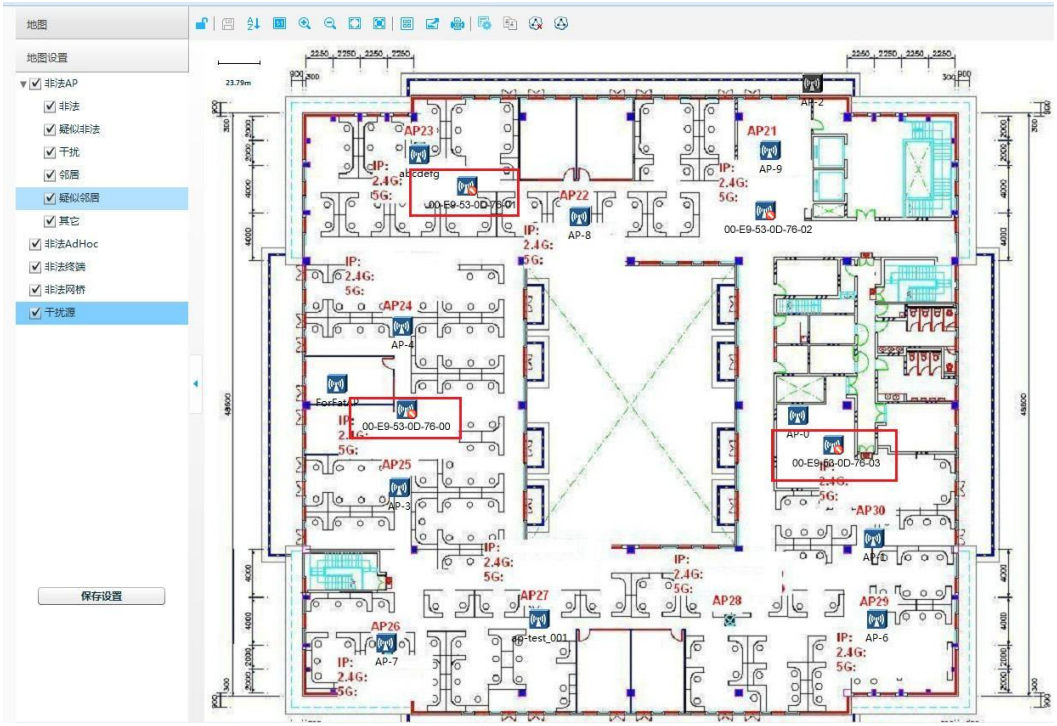
1、通过位置拓扑查看当前热点位置及射频信号覆盖范围，并标识冲突域。

2、添加预部署 AP，查看模拟的射频覆盖范围；AP 部署上线后切换真实 AP，显示 AP 的真实覆盖范围。



3、地图设置：便于运维人员控制区域内节点的隐藏与显示。过滤项包括非法 AP、非法 Adhoc、非法网桥、干扰源；其中非法 AP 支持更细粒度的按照规则分类控制显示。

4、拓扑图中的非法设备位置、干扰源位置在具备 AP 定位 license，并且该区域使能定位后，定位并刷新节点的最新坐标。



WIDS 管理

无线入侵检测（WIDS）管理，监控网络中存在的非法设备、非法客户端、干扰源、攻击信息，支持用户通过定义规则分类识别、远程告警通知并提供对入侵的保护措施。

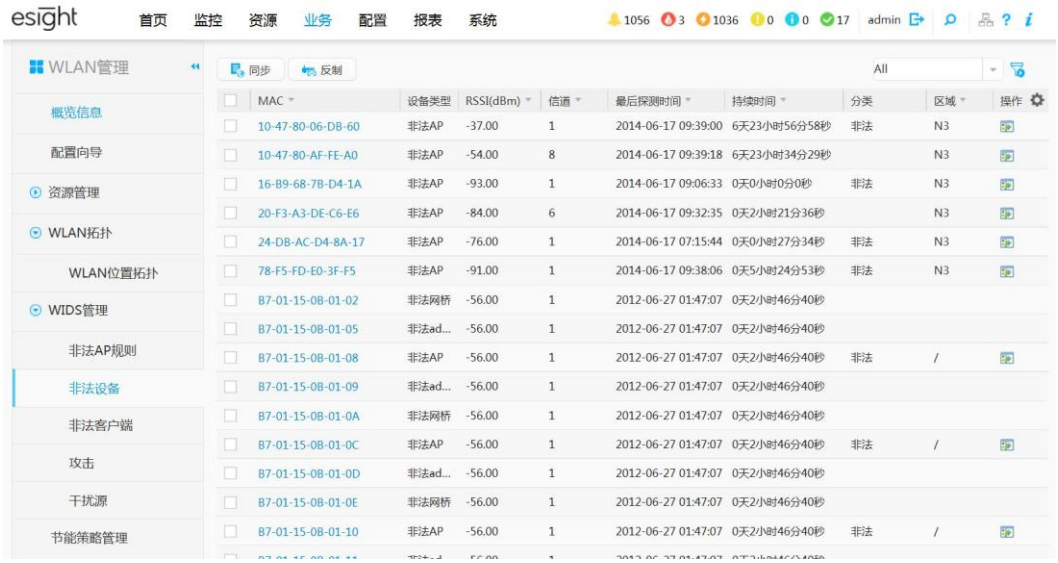
1、支持非法设备的统计、展示和反制

2、支持非法客户端的展示、反制和抑制接入保护

3、支持非 WIFI 干扰源的统计和展示

4、支持攻击信息的统计、展示和保护

5、支持用户通过定义规则对非法 AP 进行分类，类别分为非法、疑似非法、邻居、疑似邻居、干扰。支持的规则匹配指标为：邻频同频干扰 、信号强度、 SSID（模糊匹配/正则表达式匹配）、探测 AP 数量、是否攻击



故障诊断

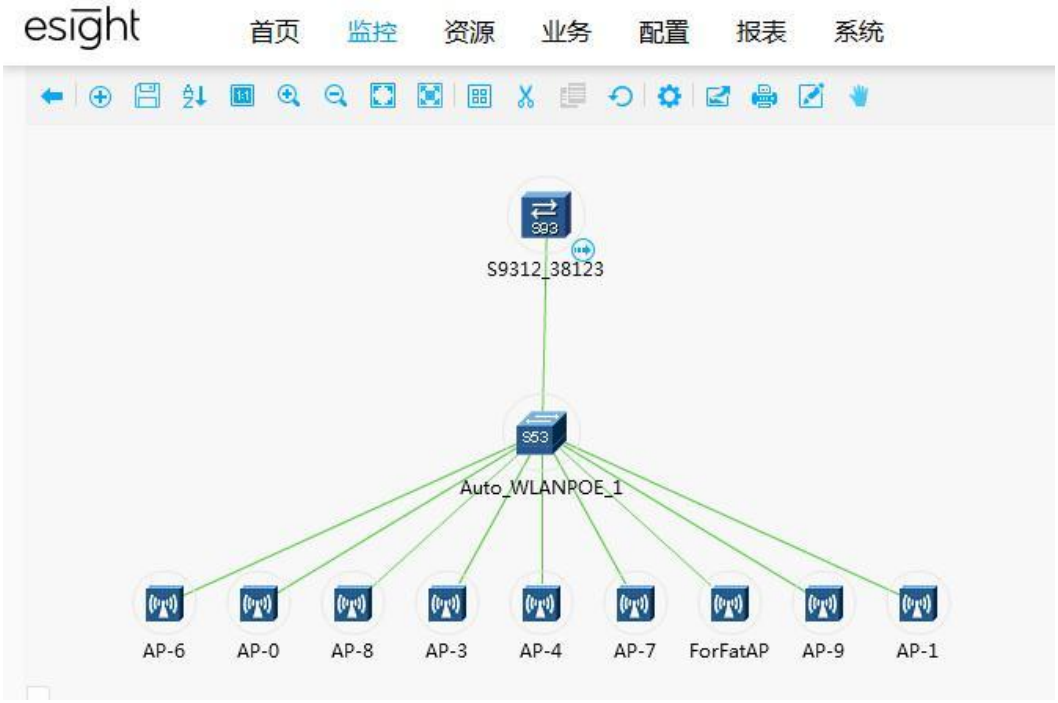
1、WLAN 用户故障诊断：从用户、SSID、AP、AC 四个无线组网层面对在线用户的网络质量进行诊断。对于诊断出的异常问题，给出可能引发的问题与修复建议，指导用户排查故障。

2、提供通讯、环境、非法设备、非 WIFI 干扰源、攻击等相关故障告警帮助用户故障点定位、解决。

3、提供对 WLAN 网络设备和资源的监控，方便用户了解当前网络和设备状态。

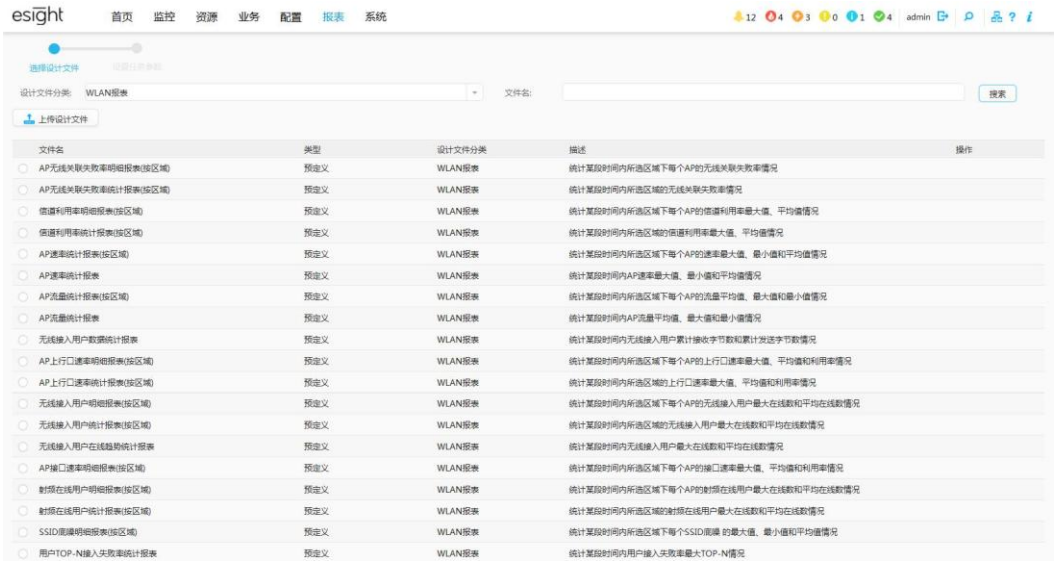
有线无线一体化管理

在使能 AP 的 LLDP 链路发现后，用户在物理拓扑中，可以查看有线侧 POE 交换机与无线侧 AP 之间的链路，实现有线无线统一管理。



业务报表

提供 AP 上行口流量、信道利用率、射频在线用户数、无线在线用户、TopN 用户接入失败率和 TopN 用户接入总次数等预定义报表，以及 AP 关联统计、AP 流量统计、AP 速率统计的快速报表，支持预定义报表。



节能管理

提供 AP、射频、SSID 维度的节能策略定制。支持节能任务管理，方便用户立即、周期性开启、关闭无线信号。

4.26 SLA 业务管理

SLA 管理提供网络性能度量与诊断功能，用户通过创建 SLA 任务可周期性监控网络的时延、丢包、抖动情况，并根据 SLA 服务中提供的服务来计算出当前网络的符合度情况。

SLA 服务默认提供了 24 种服务，用户也可以根据需求自定义服务。Dashboard 提供了全局监控 SLA 任务的能力，可通过 Dashboard 快速了解所有业务的全网的质量总体情

况，也可以查看某一地区或者是某一种业务的全网质量。SLA 视图界面可以将多个任务建立一个视图，对任务数据进行对比。快速诊断用于临时发起源宿设备间的链路及其承载的业务的诊断，可快速定位网络故障。

Dashboard

通过 SLA Dashboard 全局监控 SLA 任务情况，可以监控最近触发智能策略的任务、SLA 测试例指标以及 SLA 任务最低符合度的情况。Dashboard 支持添加、删除功能，并可设置过滤条件，对展现在 Dashboard 中的 SLA 任务进行过滤。

SLA 服务管理

SLA 服务管理提供对业务的服务质量定义，提供常用业务如语音、视频、数据等二十四种预定义模板，同时支持用户自定义，可根据用户运维需求和网络状况定制符合度和各种网络质量指标阈值。

SLA 任务管理

SLA 任务可周期性监控网络的时延、抖动、丢包率各项指标。SLA 任务管理界面提供 SLA 任务的管理功能，实现对任务的创建、复制创建、删除、启动、停止等操作。提供查看历史数据、告警、快速诊断的快捷操作入口。SLA 任务的采集周期支持智能调节，可以在网络质量发生劣化时，自动调高采集频率，使用户了解质量劣化的详细信息。

SLA 视图管理

提供对 SLA 任务进行分组管理的功能，方便用户进行多任务历史数据查看。

快速诊断

在无需创建任务的条件下，提供快速进行 SLA 服务质量检测的能力。

历史数据

提供业务质量数据图表，支持总体符合度、单网络指标的数据展示。 在SLA 任务界面点击 SLA 任务名称即可跳转到历史数据页面。

多任务历史数据查看可以同时展现多个任务的历史数据。

SLA 业务报表

提供 SLA 业务质量统计报表、SLA 任务指标统计报表和 TopN SLA 符合度报表。

业务诊断

业务诊断实现了对网络质量的检测，将采集到的时延、抖动、丢包率、DSCP 值分段展现出来，帮助用户完成对业务质量的评估，同时基于采集到的数据，定位出现质量问题的网络位置，帮助用户排除故障，保障业务的畅通性。

- 模板管理

系统提供缺省的网络业务质量（时延、抖动、丢包率等网络性能指标）评估标准，用户可根据需求自定义模板，默认提供两个预定义的模板：

（1）智真诊断的预置模板，用于评估智真系统的网络质量；

（2）桌面云诊断的预置模板，用于评估桌面云的网络质量；

- 业务诊断

  对业务质量进行诊断，快速有效地支撑用户对网络故障的定位及质量评估。进行业务诊断之前首先要选择对应的模板。

  诊断结果以分段的形式进行展示。表格中的每一条数据表示从源设备到目的设备之间的网络状况。

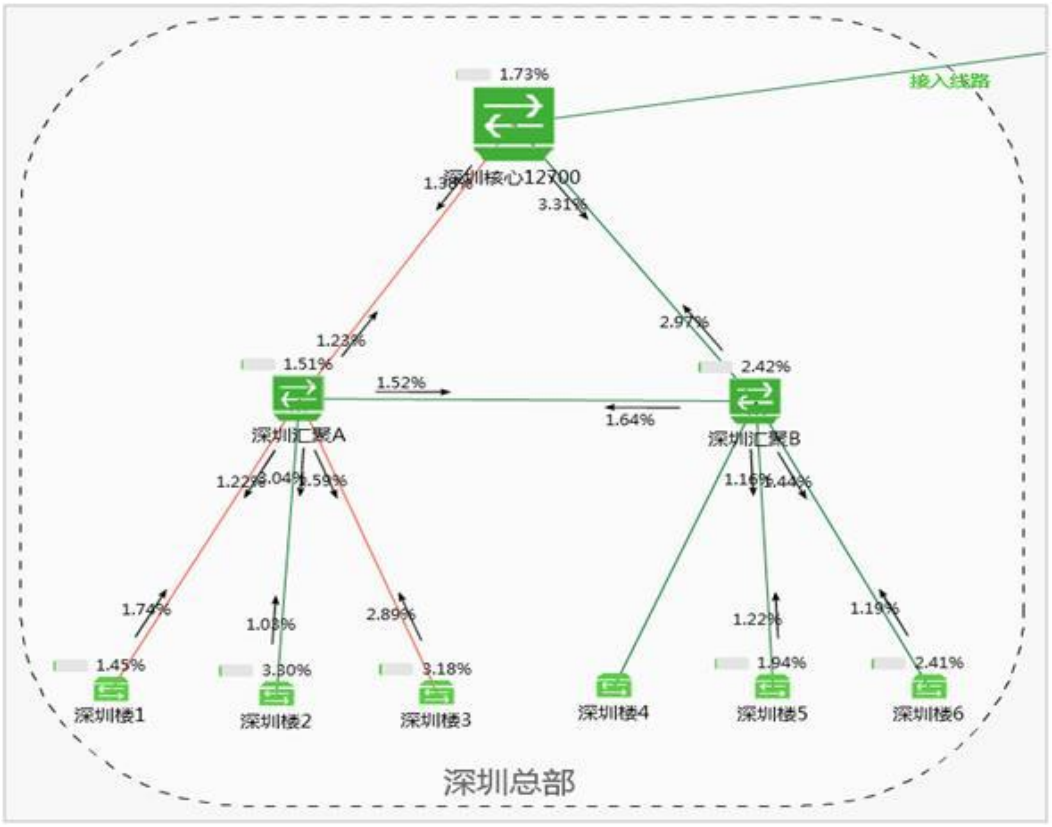
4.27 iPCA 管理

企业 IP 网络承载的业务越来越复杂、多样，并且网络应用与企业正常的运营紧密关联；质量感知（iPCA）基于企业园区网络特点提供了设备级、网络级、业务流丢包检测，通过对网络中的真实 IP 业务报文进行检测，在不增加用户数据网络负担的前提下，让网络管理员简单、快捷地监控网络质量，快速定位。

设备级监测

企业园区部署了支持 iPCA 的设备， 可以对园区内的支持 iPCA 的设备以及设备之间二层直连链路创建 iPCA 检测，通过网络拓扑实时监控该区域单播 IP 业务是否存在丢包，如果出现丢包，能够直观看出在哪个设备节点丢包，具体的丢包率和丢包数。

1. 网络拓扑直观显示设备、链路最近一次的丢包检测结果。
2. 设备、链路检测结果高于阈值，将上报告警通知用户。



网络级监测

企业园区分支之间通过租用运营商线路进行互联，分支出口设备作为 CE 接入运营商网络；如何评估运营商提供的网络是否满足质量要求，业务出现质量问题，是否是运营商网络存在丢包。iPCA 通过在园区出口设备之间创建网络级检测，实时监控业务在运营商网络质量状态。

单播 IP 业务流丢包检测

企业关键业务出现质量不稳定，首先需要判断是应用服务器、终端的问题，还是网络质量问题，如果是网络存在丢包，需要快速定位在网络的哪个节点、线路出现丢包。以下以智真业务为例，检测和快速定位业务在网络中的丢包。

1. 通过智真终端、智真服务器连接的两端交换机端口创建网络级检测，查看网络是否存在丢包。如果网络不丢包，可以确定问题出在智真终端，进一步检查终端。

2. 如果智真服务器与智真终端之间的网络存在丢包， 则需要进一步定位是网络中哪个节点或者线路存在丢包。

3. 对业务路径进行检测，显示设备、设备之间线路的丢包检测结果，帮助用户快速找到故障节点。

4.28 QoS 管理

eSight QoS 管理提供了基于 QoS 流量的监控工具，对于配置了流策略的接口，提供匹配速率、丢弃速率、超出承诺带宽速率、带宽利用率等网络性能指标的度量。

Dashboard

QoS 的 Dashboard 展示了 QoS 性能指标 TopN 任务，可以帮助网络运维人员快速发现有可能出现 QoS 流量异常的区域。

QoS 配置信息

查看设备的 QoS 配置信息。

历史数据

QoS 流量历史数据可以展现 QoS 流量的历史趋势情况，帮助网络运维人员了解 QoS 流量的历史情况。

4.29 网络流量分析

eSight NTA 组件提供了一种便捷、经济的网络流量分析方法，能深入分析网络中的流量数据并提供详细的流量分析报告。用户利用 NTA 能实时监控全网应用流量分布，能及时发现网络中异常流量，根据长期的流量分布做好网络规划，做到流量可视、故障可查、规划可依的网络透明化管理。

设备接口 NetStream 使能

通过智能配置工具向设备下发 NetStream 命令，用户不再需要手工登录一个个设备进行 Netstream 配置，从而实现快速部署。

流量配置

网流配置提供设备配置、接口配置、协议配置、应用配置、DSCP 配置、IP 组配置、应用组配置、接口组配置以及 DSCP 组配置能力。

- 设备配置

  展示全网有流量上报的设备，用户可选择性地对设备进行监控。

- 接口配置

  展示全网有流量的接口，用户可对接口流入速率、流出速率和采样比进行配置，保证网流流量数据的正确性；其中，采样率的配置值要与设备端采样率保持一致，以还原设备的真实流量。

- 协议配置

  用户根据实际需要，选择性地对协议进行监控。

- 应用配置

  列举常用的 543 个网络应用，分为四层应用、七层应用、协议应用和用户自定义应用，用户可自定义重要应用。

  - 四层应用：由一组（或多组）固定的网络协议和通讯端口的组合进行标识的网络应用。
  - 七层应用：端口不固定的应用，该类应用通过报文应用层数据的特征进行识别。
  - 协议应用：不区分端口，直接根据协议来标识的应用。
  - 用户自定义应用：用户添加的应用，根据指定的协议(UDP/TCP)、端口范围和 IP 范围来定义应用。

- DSCP 配置

  列举常见的 22 种 DSCP，并且用户可自定义 DSCP 名称。

- IP 组配置

  用户可将有关联的一组 IP 地址分为一组，如一个部门或一个楼层，方便查看该 IP 组的流量信息。

- 应用组配置

  用户可将按照自己关注的点进行应用分类，如邮件类应用组，便于查看该应用组的流量信息。

- DSCP 组配置

  用户可将有关联的服务类型进行分组，如语音类，便于查看该 DSCP 类的流量信息。

- 接口组配置

  用户可将相关联的接口定义成一个接口组，方便查看接口组流量信息。

- 告警配置

用户可以指定某个应用、主机、DSCP 速率超过指定的阈值就触发告警，并指定告警的恢复条件。

- 采集器配置

  用户可以查看当前采集器的 IP 地址和状态，设置采集接口的会话 TOPN 数，系统默认为 TOP30；启用流量取证功能将采集器原始流文件上传到分析器。

流量概览

提供全网流量概览，多维度、实时展现全网流量动态，用户可快速的查看到各维度的流量信息。

- 界面包括接口流量排行、接口利用率排行、设备流量排行、应用流量排行、主机流量排行、DSCP 流量排行、会话流量排行等内容；
- 展现形式、展现内容、内容排版可自定制，支持自定义“窗件”操作， 窗件支持 Tooltips，超链接，最小化/最大化等操作。

流量分析

提供钻取式流量分析能力，用户可通过逐步选择查看条件，查看需要关注的流量信息。系统提供了设备流量、接口流量、应用流量、DSCP 流量、主机流量、会话流量、接口组流量、IP 组流量、应用组流量等维度详细的流量分析能力。

用户可通过设备、应用、DSCP 等不同的维度查看全网流量信息，以应用流量为例，可看到全网的应用流量分布。

用户可通过进一步的下钻，查看某一具体对象的流量信息，以接口流量分析为例，可选择某一具体接口，查看该接口详细的流量信息。

另外，提供了强大的数据下钻能力，用户可通过设置不同的过滤条件，层层下钻，最终定位查看详细的会话信息；

网流报表

提供向导式的自定义报表能力，用户灵活定制所关注的流量报表。提供报表的导出和邮件发送能力，用户可通过报表，及时地了解网络中的流量分布信息。

- 支持多种报表数据展示方式：饼图、表格、折线图、区域图。
- 支持多种汇总类型：应用、会话、DSCP、主机、接口汇总。
- 支持多个过滤条件：源地址、目的地址、应用、DSCP。
- 支持即时任务和周期任务：
  - 即时任务

    即时任务，需要用户手工执行，反映的是即时的统计结果。任务执行成功后，界面上会有状态提示，打开报表会展示详细的数据和图形供用户查看。
  - 周期任务

    周期任务，系统会按照用户指定的运行周期执行，反映的是一个周期内的统计结果。
- 支持单个和批量导出报表。
- 支持报表的邮件发送功能

流量取证

发现网络中存在异常流量，需要进一步进行定位时，系统提供获取流量原始数据的能力，协助定位网络故障。

取证结果以七元组的维度分组审计数据，清晰直观的展现任务的流量信息；如：用户可通过比对协议、端口及包速率，查看是否存在病毒威胁；通过 TCP 标志位，确认是否存在协议攻击威胁。

- 支持按照时间范围进行原始报文获取；
- 支持多个过滤条件：源地址、目的地址、入接口、出接口、源端口、目的端口、协议、应用、DSCP、TCP 标志；
- 支持设置查询结果保存期限，最多可保存 30 天；
- 支持查询结果导出，可选择分页或全部导出。

流量告警

支持对应用、服务器、会话等七种类型的流量创建阈值告警，当流量在规定的时间内超过阈值次数满足条件时，会自动生成告警，当流量在规定时间内满足恢复条件时，告警自动清除。触发告警和清除告警均可发送邮件通知用户。

流量阈值告警配置界面提供了阈值告警的管理能力，实现了创建、复制创建、删除、启用、禁用等操作，用户可选择需要监控的对象，参照历史流量数据设定告警级别、阈值、重复次数等基本信息。

当前告警页面可以查看网流告警信息，并且支持从当前告警跳转至流量分析页面查看告警生成时间段的详细流量信息。

4.30 IPSec VPN 管理

IPSec VPN 管理组件提供对 IPSec VPN 业务的全方位监控与诊断能力，包括业务的激活状态与告警状态监控、业务拓扑、性能监控、业务诊断以及历史隧道信息查看等功能。

概览信息

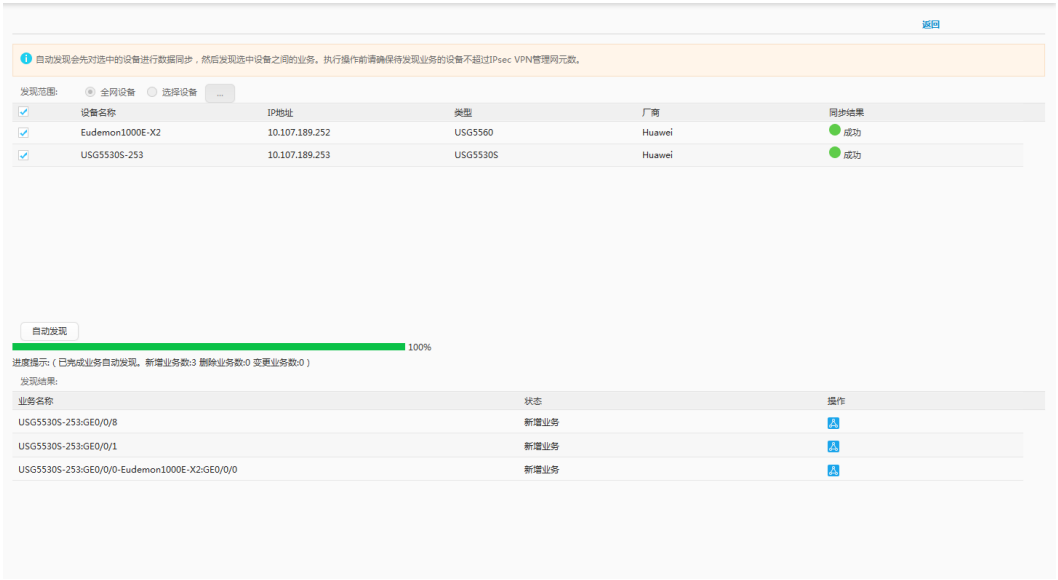
通过 IPSecVPN 概览信息可以全局监控 IPSecVPN 业务的整体情况，包括：IPSec 隧道总数、设备全局与 IPSec 隧道的接收与发送包速率/报文速率/丢包率、IPSec 隧道远程接入用户数、业务告警列表等监控信息。概览信息如图 1 所示。

图4-8 IPSec VPN 概览信息

业务发现

自动发现网络中全部或者部分设备的 IPSec VPN 业务，支持 Hub-Spoke、Site-to-Site 类型组网的业务发现，发现过程中会自动根据组网对业务进行分组。业务发现如图 2 所示。

图4-9 IPSecVPN 业务发现



业务组管理

IPSec VPN 通过业务组对业务进行管理，提供业务组的搜索、删除、移动等基本管理功能。通过业务组列表可以直观了解每个业务组中的业务数量、告警状态，并提供到告警列表的跳转。

另外，可以基于业务组对业务进行快速诊断与业务配置修改，其中业务配置修改目前主要是修改业务的预共享密钥信息。

业务组管理列表如图 3 所示。

图4-10 IPSecVPN 业务组管理列表

修改预共享密钥如图 4 所示。

图4-11 修改业务的预共享密钥

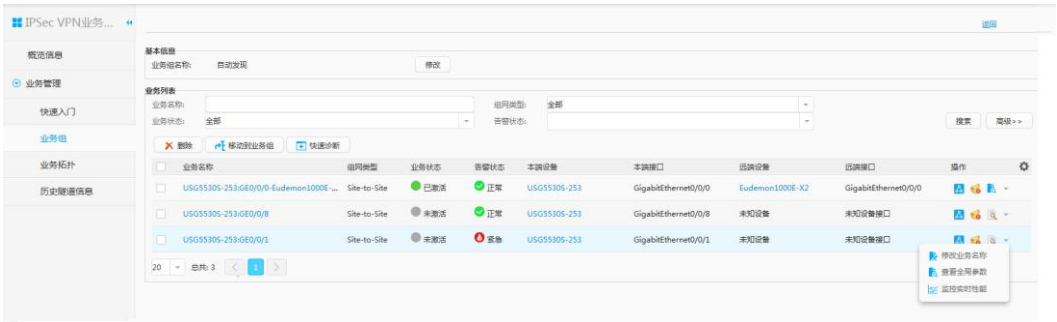
业务列表管理

可以通过业务组列表中的链接进入业务列表。

业务列表中除了提供修改当前业务组名称的功能外，主要提供了基于业务的各种操作，包括条件搜索、删除、移动、快速诊断、修改业务名称、查看全局参数、监控实时性能、查看隧道信息、拓扑跳转、告警跳转等。

业务列表如图 5 所示。

图4-12 IPSecVPN 业务列表



- 条件搜索

  支持通过业务名称进行模糊搜索，支持根据组网类型、业务状态、告警状态、本端/远端设备、本端/远端接口来搜索过滤符合指定条件的业务。

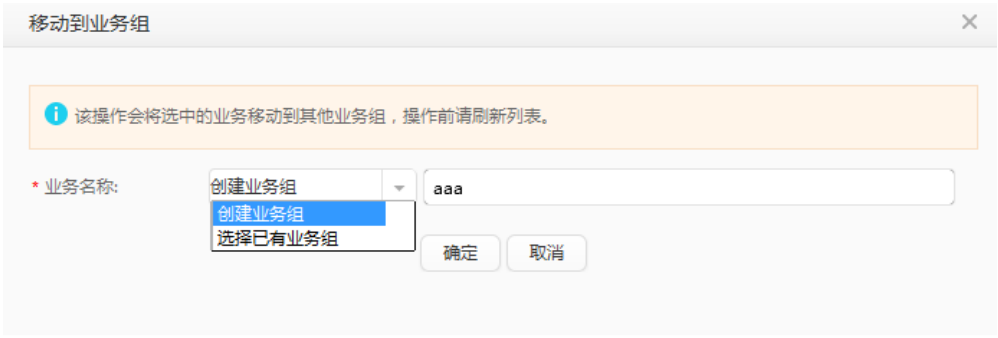
- 业务删除

  把选定的业务从网管中删除，注意该删除操作不会把设备上的业务删除。删除后可以通过发现功能把业务重新发现到网管。

- 业务移动

  把选定的业务移动到其它组中，可以移动到新业务组，也可以移动到已有的业务组。业务移动如图 6 所示：

图4-13 IPSecVPN 业务移动界面



- 快速诊断

  当用户发现业务产生故障后，可以对业务进行快速诊断，以协助定位业务故障产生的原因。

- 修改业务名称

  业务名称在发现过程中由系统自动生成，用户可以对业务名称进行修改。业务名称修改成功后，会通知拓扑更新业务链路名称。业务名称修改界面如图 7 所示：

图4-14 IPSecVPN 业务名称修改

- 查看全局参数

  可以查看业务两端设备的 IPSecVPN 全局配置参数，包括两端设备的名称、类型、IP 地址、IKE 协商名称、发送 Keepalive 报文时间间隔、等待 Keepalive 报文超时时间间隔、NAT Keepalive 更新报文时间间隔等配置。如图 8 所示：

图4-15 IPSecVPN 业务全局参数

配置项	本端	远端
设备名称	USG5530S-253	Eudemon1000E-X2
设备类型	USG5530S	USG5560
IP地址	10.107.189.253	10.107.189.252
IKE协商本端名称	253	Eudemon1000E-X2
发送Keepalive报文的时间间隔(秒)		
等待Keepalive报文的超时时间间隔(秒)		
NAT Keepalive更新报文的时间间隔(秒)	20	20
流量模式时间间隔(秒)		
轮询模式时间间隔(秒)		
超时重传时间(秒)	5	5
基于时间的安全联盟生命周期(秒)	3600	3600
基于流量的安全联盟生命周期(KB)	1843200	1843200
IPSec前反查	启用	启用
IPSec后反查	启用	启用

- 监控实时性能

  监控业务的实时性能，包括 IPSec 隧道远程接入用户数、IPSec 隧道接收/发送包速率、报文速率与丢包率等。

- 查看隧道信息

  当业务的状态为“未激活”时，查看隧道信息图标置灰不可用；当业务为“已激活”时，可以通过此图标查看隧道的详细信息，包括连接号、持续时间、本端/远端设备、本端/远端接口、本端/远端 IP 地址、报文封装模式、密钥协商类型以及 SA 列表。如图 9 所示：

图4-16 IPSecVPN 业务隧道详细信息查看

- 拓扑跳转

  通过业务可以跳转到 IPSecVPN 业务拓扑界面，同时定位到选中的业务链路。

- 告警跳转

  当业务的告警状态为非正常状态时，可以通过告警跳转链接打开当前告警列表，告警列表中列出业务两端设备的告警信息。

业务拓扑

通过业务拓扑可以直观的对 IPSecVPN 业务进行监控管理。IPSec VPN 业务拓扑展现支持如下场景：

- Hub-Spoke、Site-to-Site 组网
- 第三方设备对接场景
- 支持双机热备场景及主备倒换

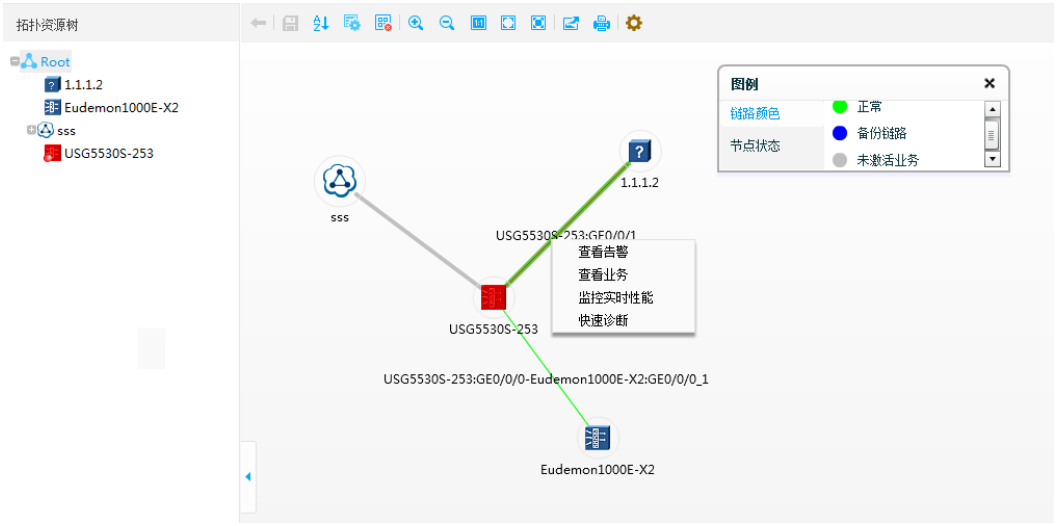
拓扑中提供丰富的跳转功能，包括到业务发现、告警列表、业务列表、业务诊断、实时性能、设备管理的跳转，另外支持设备的全局参数查看功能。

提供完整的 Tooltip 信息，设备节点、业务链路、子网、备份链路分别在各自的 Tooltip 中显示对应的信息，包括基本信息、最近历史性能数据等。

支持子网管理，通过子网对网络设备进行层次划分，避免拓扑臃肿，方便用户管理与查看拓扑。子网管理包括导入物理子网、新建、修改、删除、移动到子网、添加设备到子网等功能。

业务拓扑如图 10 所示。

图4-17 IPSecVPN 业务拓扑



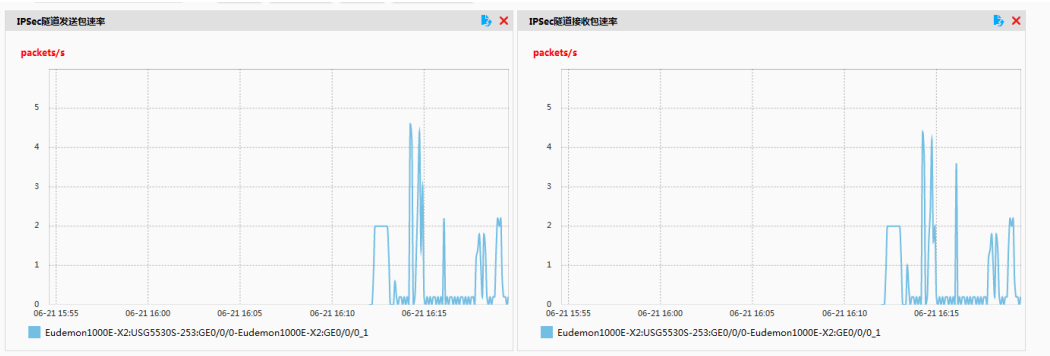
告警监控

通过业务组与业务列表中的告警状态实时反应业务故障的产生与恢复情况，拓扑中的业务链路也能通过颜色即时展现告警状态。当用户发现业务有告警后，可以跳转到告警列表，查看告警详细信息，了解故障产生原因。

性能监控

提供基于设备全局和 IPSecVPN 业务的性能监控功能，让用户了解网络设备与业务的流量等情况，包括包速率、报文速率、丢包率、隧道总数与远程用户接入数等。业务实时性能监控如图 11 所示。

图4-18 IPSecVPN 业务性能监控



快速诊断

在无需创建任务的条件下，提供快速对业务进行故障检测的能力。

业务诊断内容包括两端的接口状态、IPSec 策略是否应用到接口、接口是否应用能发起 IPSec 协商的策略、IPSec 策略配置完整性、IKE 协商结果、IPSec 协商结果等。

诊断结果可以导出到 Excel 表格。

业务诊断如图 12 所示。

图4-19 IPSecVPN 业务快速诊断

历史隧道查看

通过历史隧道列表可以查看在一段时间范围内全网隧道连通和断开的情况，用户可以通过此功能发现隧道连通和断开的规律，以协助定位业务故障的原因。

历史隧道列表如图 13、图 14 所示。

图4-20 IPSecVPN 历史隧道列表

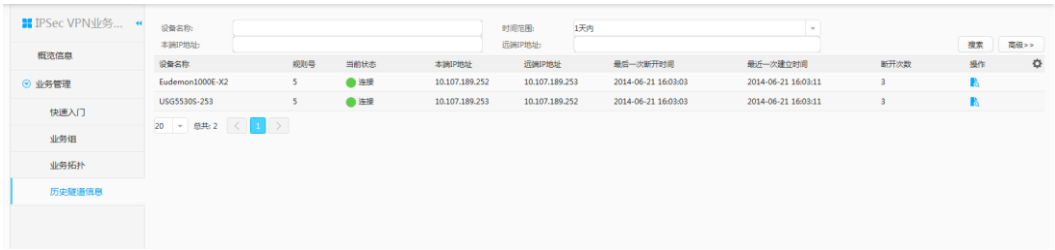


图4-21 IPSecVPN 历史隧道详细信息

4.31 BGP/MPLS VPN 业务管理

BGP/MPLS VPN 管理组件提供对 VPN 业务的部署、监控和故障诊断端到端解决方案。

- 向导式业务批量部署：批量部署 PE、CE 设备 VRF、接口、路由等业务数据
- 方便快捷自动发现：无需指定设备角色，自动发现网络中已部署的 VPN 业务
- 可视化业务拓扑：直观展示业务 PE-PE、PE-CE 业务逻辑结构，并实时显示业务告警
- 多维度业务监控：从告警、性能、业务链路 SLA 等多个方面监控业务的运行状况

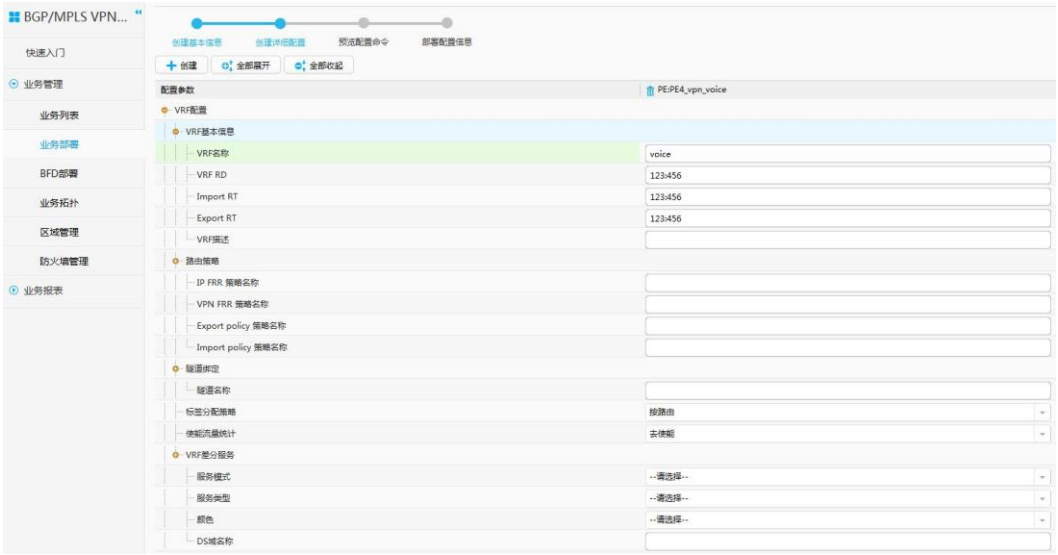
- 一键式故障诊断：分段分层多手段诊断 VPN 业务故障

业务部署

提供图形化、向导式、端到端的业务部署能力，帮助用户简单快速开通新 VPN 业务、增加新的 VPN 接入点以及调整已有的 VPN 业务，提升用户业务维护的效率。支持对 Full-mesh、Hub-Sopke、MCE、自定义组网类型的业务开通，支持在 PE-CE 间部署 OSPF、ISIS、静态以及 EBGP 路由协议。如图 4-22，图 4-23 所示。

图4-22 MPLS VPN 业务部署

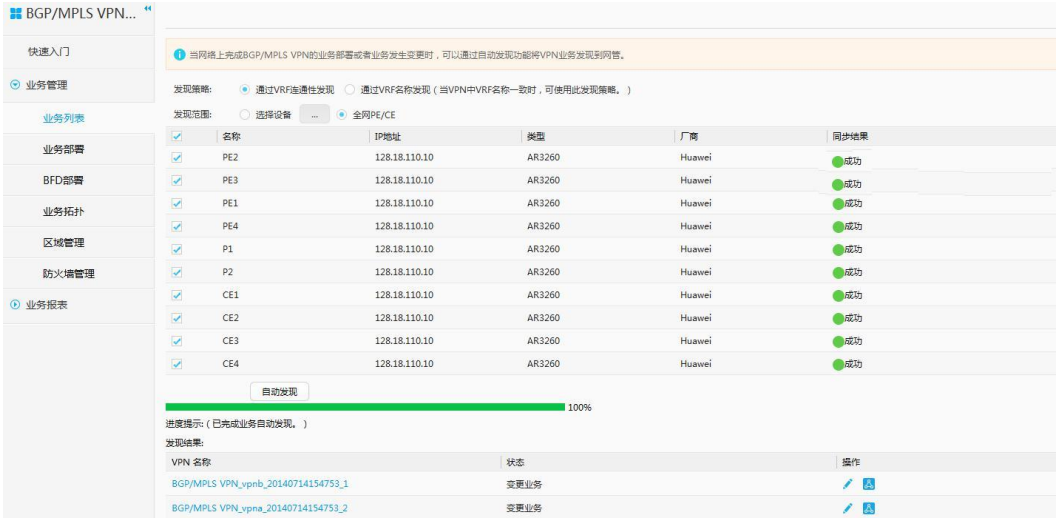
图4-23 创建详细配置



自动发现

自动发现网络中已部署的 MPLS VPN 业务，支持 Full-Mesh、Hub-Spoke、MCE、HoVPN、跨域 OptionA、跨域 OptionB 组网类型的业务自动发现。在进行自动发现的时候，用户无需指定 PE 和 CE 设备，系统能够根据业务配置信息自动识别设备角色并发现 PE-PE、PE-CE 之间的业务逻辑关系。自动发现如图 4-24 所示。

图4-24 MPLS VPN 自动发现



业务监控

- 提供 MPLS VPN 业务监控能力，查看 MPLS VPN 业务配置信息，包括 PE-PE 链路、PE-CE 链路、VRF 实例、路由配置信息。
- 提供 MPLS VPN 性能监控，支持 TopN 流入/流出流量性能统计、PE-CE 流量性能统计、VRF 流量性能统计、VRF 路由性能统计。通过与网流组件联动，用户能够查看哪些应用和终端消耗了当前接口的流量，实现对 VPN 流量的精细化管理。
- 提供 MPLS VPN 业务质量监控。通过和 SLA 组件联动，监控 VPN 业务的 PE-PE、PE-CE、CE-CE 等各段链路的传输质量，一旦有业务链路出现质量问题，能即时预警。

业务拓扑

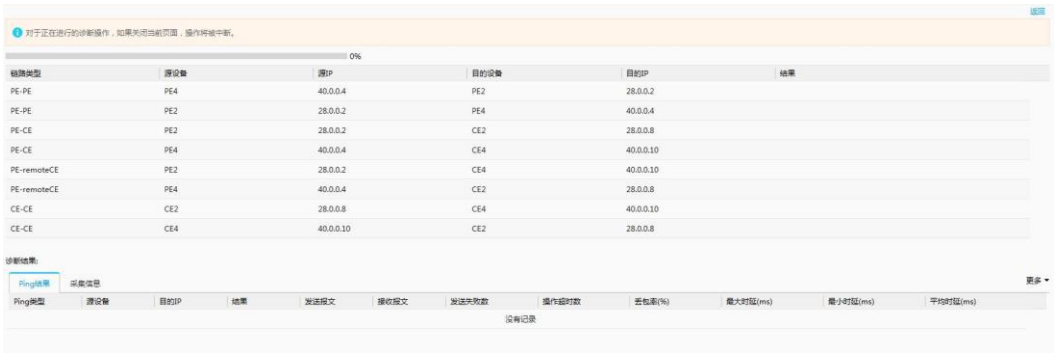
通过 MPLS VPN 业务拓扑可直观展示 VPN 网络逻辑结构。提供自定义区域管理。如图 4-25 所示。

图4-25 MPLS VPN 业务拓扑

快速诊断

提供一键式故障诊断，分段对 PE-PE、PE-CE、CE-CE、PE-remoteCE 链路从三层路由和 MPLS 转发层通过 ping、trace、路由信息采集等多种手段进行故障诊断，诊断结束之后系统给出具体的失败原因，帮助用户快速定位故障点和故障原因。如图 4-26 所示。

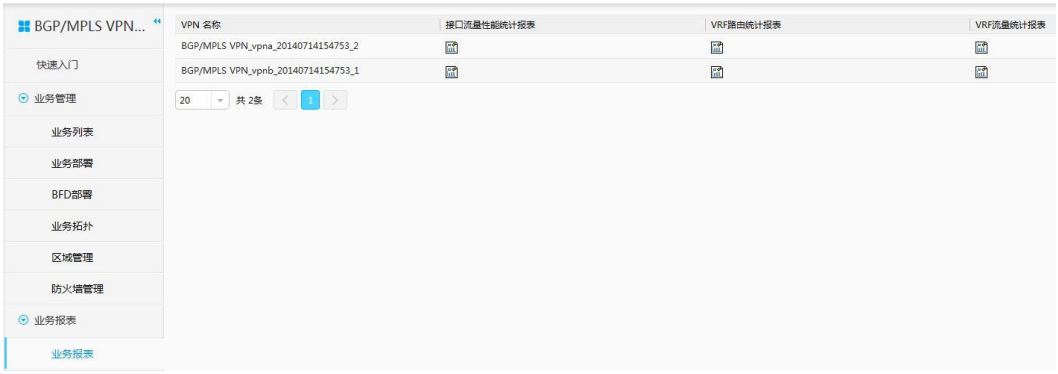
图4-26 MPLS VPN 快速诊断



业务报表

提供接口流量性能统计表、VRF 流量统计报表、VRF 路由统计报。用户通过查看接口流量统计报表，能够了解当前 VPN 业务所有接入接口的历史数据走势，通过查看 VRF 流量统计报表能够了解 VPN 流量在每个 PE 设备上的分布，通过查看 VRF 路由统计报表能够了解当前 VPN 业务 CE 接入的路由变化。上述三个报表从流量和路由的角度给用户扩容等操作提供数据依据。如图 4-27 所示。

图4-27 MPLS VPN 业务报表



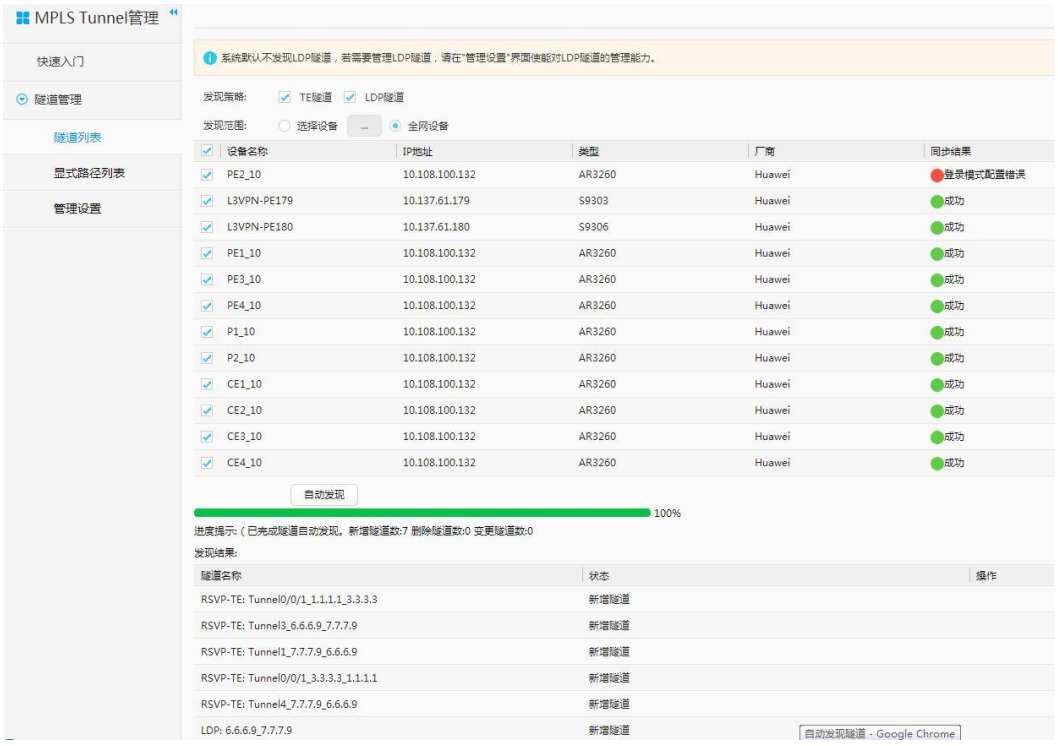
4.32 BGP/MPLS Tunnel 管理

MPLS Tunnel 管理组件提供对 MPLS TE 隧道和 LDP 隧道的监控能力，包括隧道的运行状态、备份状态、隧道拓扑、隧道告警、故障诊断以及查看与隧道相关的 VPN 业务。

自动发现

自动发现网络中的 MPLS 隧道，支持 MPLS TE 隧道及 MPLS LDP 虚隧道的自动发现。如图 4-28 所示。

图4-28 MPLS Tunnel 自动发现



隧道监控

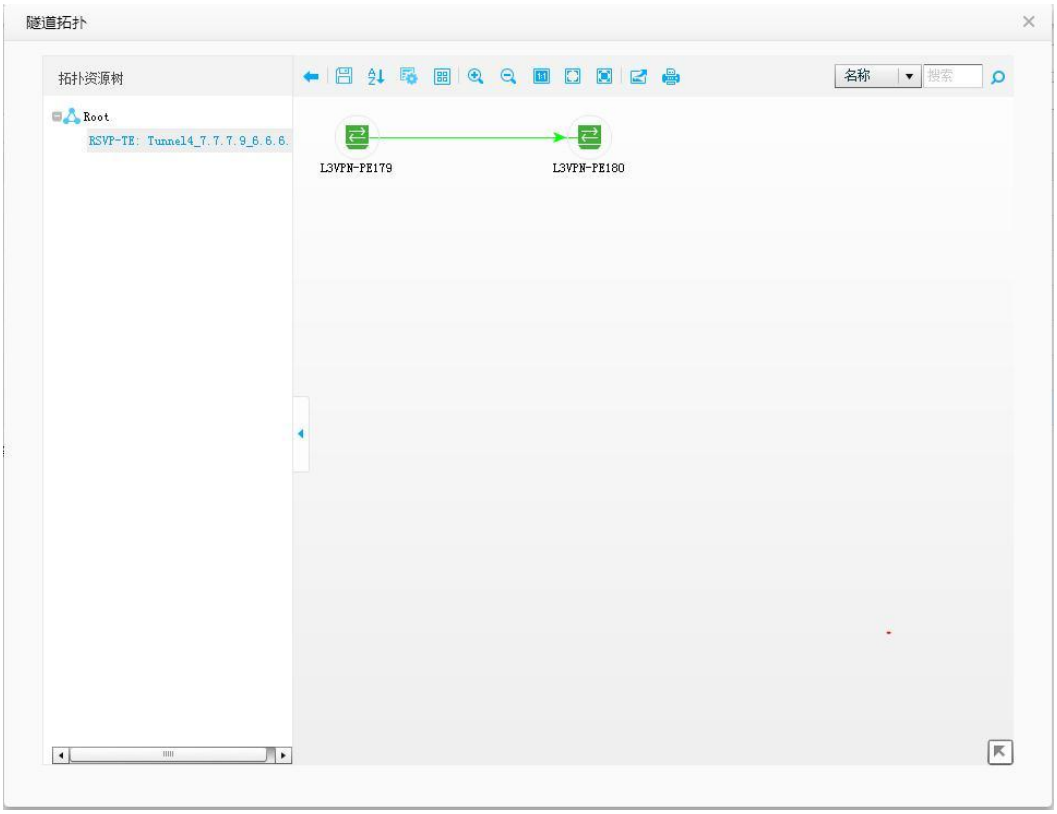
提供 MPLS 隧道监控能力，支持 MPLS TE 动态隧道主备保护和旁路保护、MPLS TE Static-CR 隧道的监控，包括隧道的备份状态、运行状态、隧道告警。

提供 MPLS 隧道与 L3VPN 的联动能力，支持查看 TE 隧道承载的 VPN 业务。

隧道拓扑

通过隧道拓扑能可视化监控隧道状态、链路状态、节点状态等关键状态信息，并能够查看和设备相关的 MPLS 信息。如图 4-29 所示。

图4-29 隧道拓扑



- 支持对 MPLS TE 隧道设备 MPLS 能力、接口 MPLS 能力、DS-TE 信息、链路带宽信息查看。
- 支持对 MPLS LDP 虚隧道设备 MPLS 能力、接口 MPLS 能力信息查看。

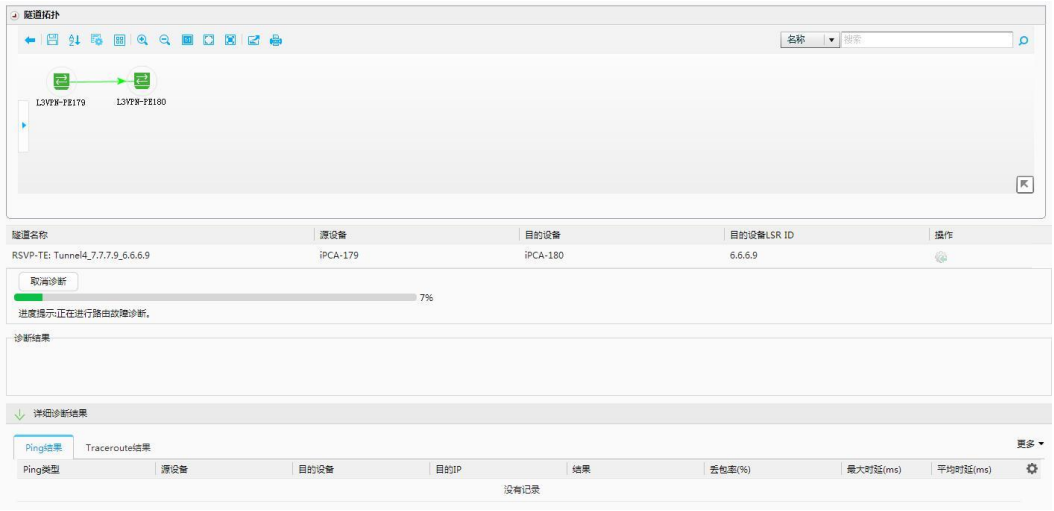
显式路径

提供显式路径查看，支持显式路径列表以及显式路径每一条详细信息的查看。

快速诊断

提供 MPLS 隧道诊断功能。eSight 可诊断隧道中沿途各节点路由转发是否正常，标签转发是否正常，各节点隧道相关配置是否正确。如隧道存在故障，eSight 可精确定位发生故障的节点和原因，并给出详细的诊断结果。 如图 4-30 所示。

图4-30 隧道诊断



4.33 Secure Center 安全策略管理组件

Secure Center 安全策略管理组件

Secure Center 能有效管理大规模华为防火墙、交换机和路由器部署环境中设备的安全策略，主要功能包括：

1. 安全策略分析
   - 支持对防火墙的安全策略进行冗余分析、风险分析、命中分析和综合分析
   - 支持对 NGFW 的安全策略进行冗余分析、风险分析、命中分析和综合分析
2. 防火墙安全策略管理
   - 支持防火墙安全策略、入侵防御策略和反病毒策略的批量配置和部署
   - 支持集中配置地址集、时间段、服务等公共对象
   - 支持虚拟防火墙的管理和基于虚拟防火墙的安全策略配置
3. NGFW 安全策略管理
   - 支持 NGFW 安全策略、入侵防御策略的批量配置和部署
   - 支持集中配置地址集、时间段、服务等公共对象
   - 支持虚拟防火墙的管理和基于虚拟防火墙的安全策略配置
4. 交换机策略管理
   - 支持交换机接入认证策略批量配置和部署

- 支持集中配置用户组、Radius 服务器组和接入策略模板
- 支持接入认证策略的一致性审计

5. AR 策略管理
   - 支持域间安全策略的集中配置和批量部署
6. ACL 管理
   - 支持基本和高级 ACL 的集中配置

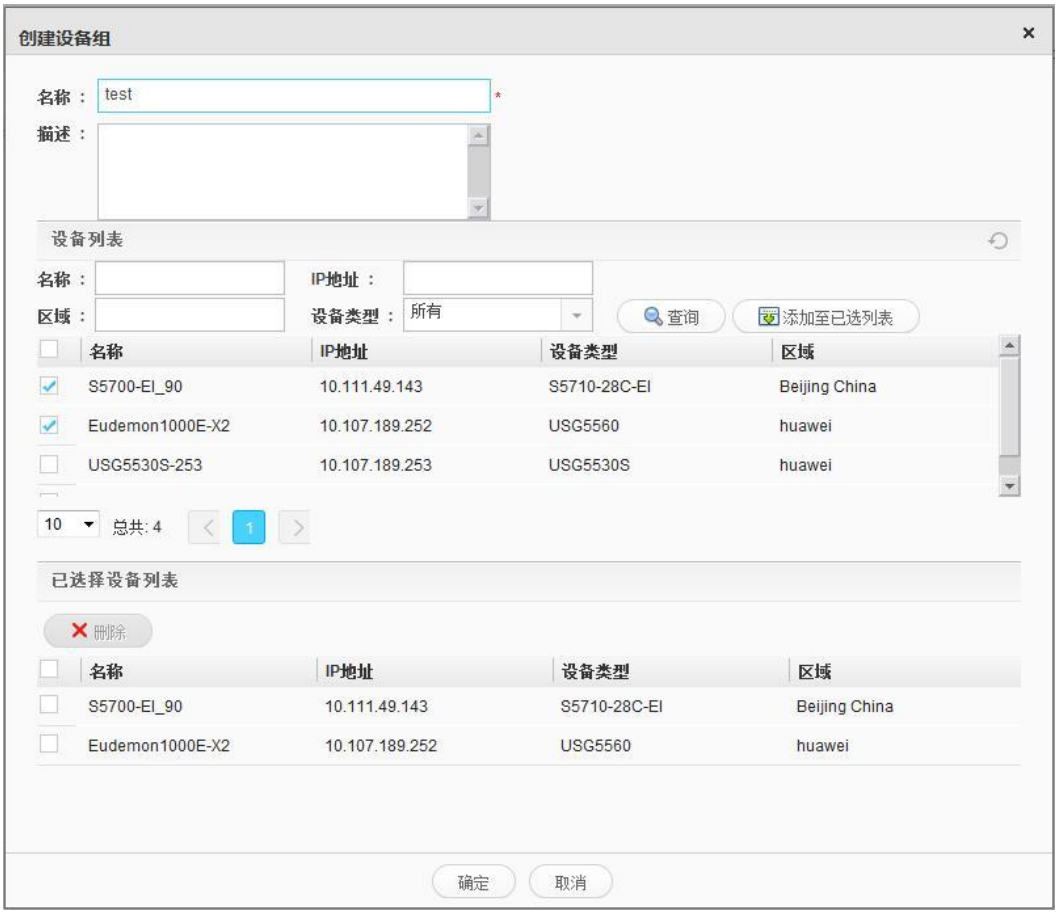
基础配置

- 支持对安全设备的策略授权管理，可以查看目前已经 license 授权管理的设备。

图4-31 安全策略授权管理

- 支持设备组的创建、删除、修改和查询。

图4-32 创建设备组



- 支持虚拟防火墙的创建、删除和查询

图4-33 创建虚拟防火墙

安全策略分析

- 策略冗余分析

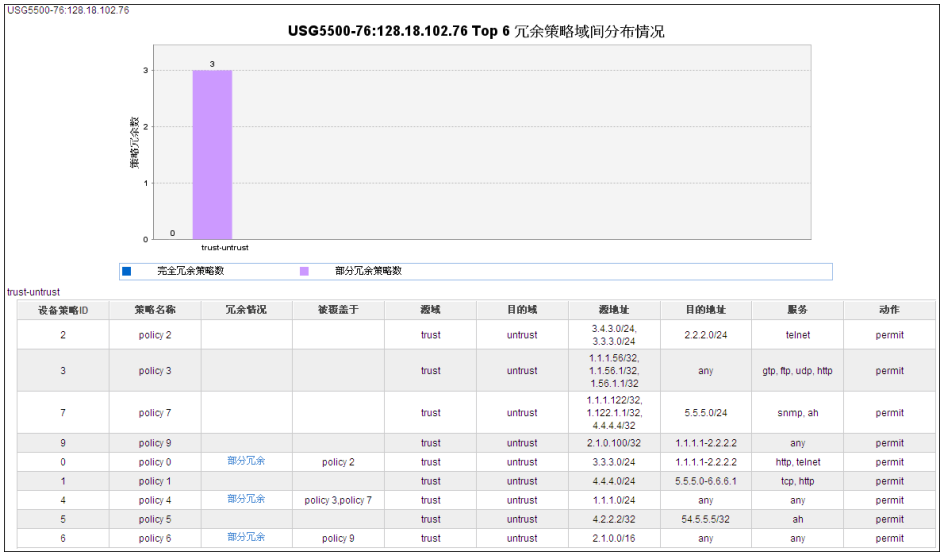
  提供分析网管中配置的安全策略是否存在冗余的能力；还可以直接分析防火墙设备上当前配置的安全策略是否存在冗余，利用高效的冗余分析算法，分析出策略完全冗余数、部分冗余数，正常策略数。最大可支持一次选中 20 台设备进行分析，分析结果会采用分组柱状图的形式展示 Top5 设备的完全、部分、正常策略数。

  设备策略冗余数据详情以两种形式展示

  1．用户设定定时任务得到执行结果，此结果采用 PDF 文档形式展示。任务分析生成的 PDF 文档会把所有的设备域间策略冗余分配情况全部列出，并采用表格的形式按照域间分组展示出域间策略，并提示是否是 “完全冗余”或“部分冗余”策略。如果某条策略是冗余策略，则会给出当前策略被哪些策略所覆盖的信息。

2．用户立即执行某个任务，采用网页形式展现分析报表结果。该方式提供一种互动查看某个设备策略冗余情况的能力，用户可以根据自己的需求，选择某个设备来查看策略配置冗余情况。还可以根据需求查看某个策略的详细的冗余情况。

图4-34 策略冗余分析结果



trust-untrust

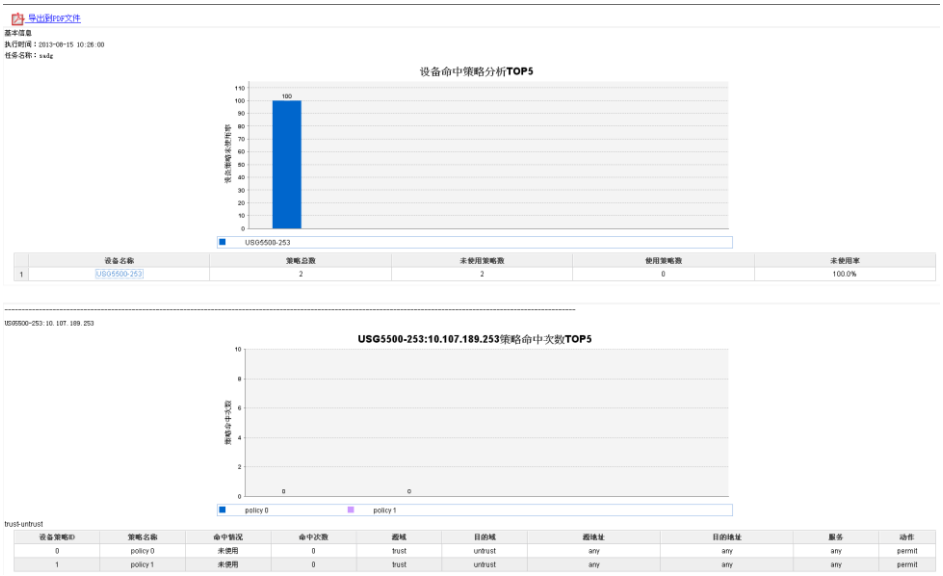
设备策略ID	策略名称	冗余情况	被覆盖于	源域	目的域	源地址	目的地址	服务	动作
2	policy 2			trust	untrust	3.4.3.0/24, 3.3.3.0/24	2.2.2.0/24	telnet	permit
3	policy 3			trust	untrust	1.1.1.56/32, 1.1.56.1/32, 1.56.1.1/32	any	gtp, ftp, udp, http	permit
7	policy 7			trust	untrust	1.1.1.122/32, 1.122.1.1/32, 4.4.4.4/32	5.5.5.0/24	snmp, ah	permit
9	policy 9			trust	untrust	2.1.0.100/32	1.1.1.1-2.2.2.2	any	permit
0	policy 0	部分冗余	policy 2	trust	untrust	3.3.3.0/24	1.1.1.1-2.2.2.2	http, telnet	permit
1	policy 1			trust	untrust	4.4.4.0/24	5.5.5.0-6.6.6.1	tcp, http	permit
4	policy 4	部分冗余	policy 3,policy 7	trust	untrust	1.1.1.0/24	any	any	permit
5	policy 5			trust	untrust	4.2.2.2/32	54.5.5.5/32	ah	permit
6	policy 6	部分冗余	policy 9	trust	untrust	2.1.0.0/16	any	any	permit

- 策略命中分析

命中分析只支持直接读取设备策略命中数据进行分析的功能，最大可支持一次选中 20 台设备进行安全策略命中情况分析。按照域间分组展示设备上的策略命中情况，给出命中次数以及策略所配置的公共对象内容详情。

命中分析提供两种展示方法：PDF 文档展示和网页形式展示的功能。网页形式执行提供给用户更多的交互功能，用户可以根据自己的需求选择某个设备查看设备策略命中情况。

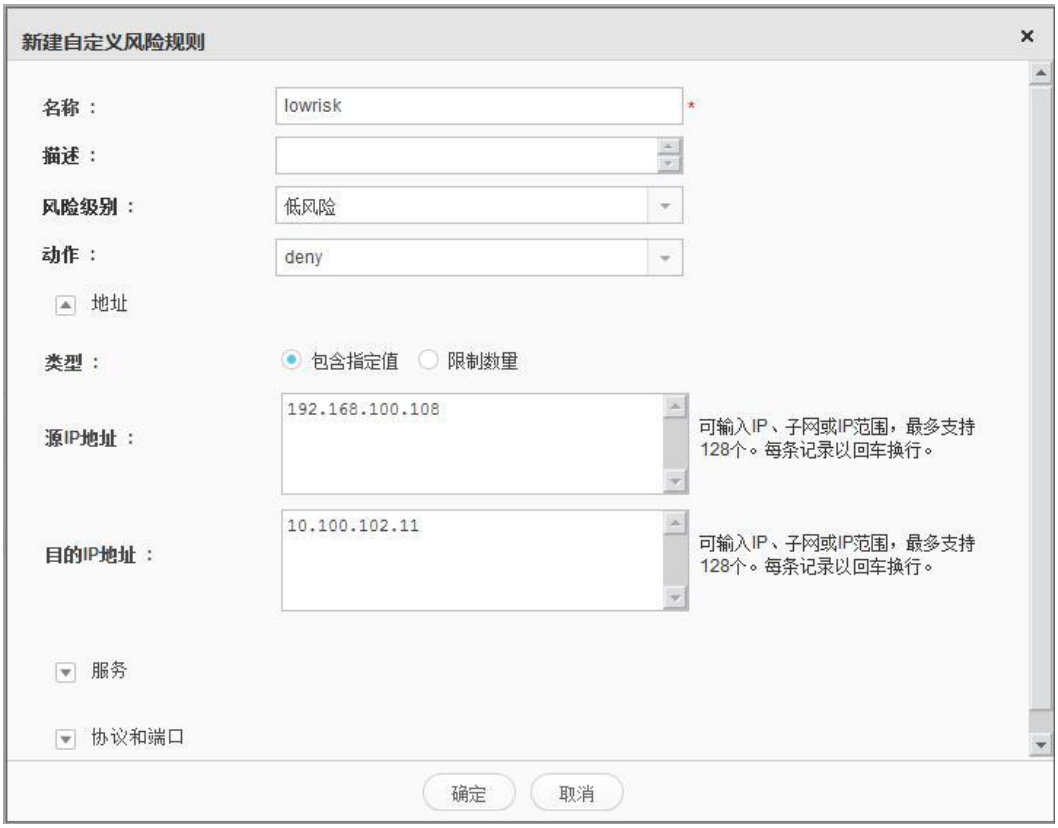
图4-35 策略命中分析结果



- 策略风险分析

  提供分析网管中配置的安全策略是否存在风险的能力；还可以通过选中“任务执行前同步设备数据”的方法直接分析防火墙设备上当前配置的安全策略是否存在风险，利用风险分析算法，根据用户选择的风险规则分析出设备的高、中、低风险策略数。除了系统提供的默认自定义风险规则外，还支持用户创建自定义风险规则。最大可支持一次选中 20 台设备进行分析，分析结果会采用分组柱状图的形式展示 Top5 设备的高、中、低风险策略数，同时用表格形式展示出创建分析任务时所有被选中设备的高、中、低风险策略数。

图4-36 自定义风险规则

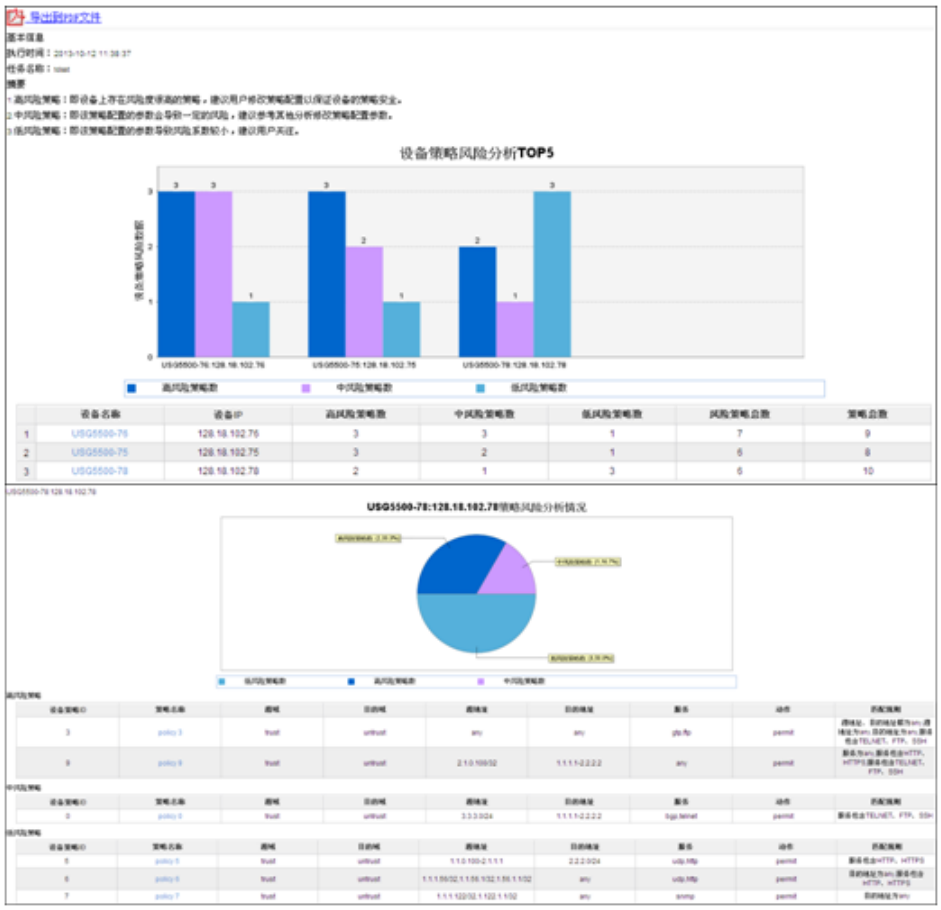


设备策略风险数据详情采用两种形式展示：

1．用户设定定时任务得到执行结果，此结果采用 PDF 文档形式展示。任务执行结果会把创建分析任务时所选设备的高风险策略、中风险策略、低风险策略全部在 PDF 文档中展示出来。

2．用户立即执行某个任务，采用网页形式展现分析报表结果。用户可以根据自己的需求查看某个设备的高、中、低风险策略情况。还可以查看某个策略产生风险所匹配的风险规则。

图4-37 策略风险分析结果



- 策略综合分析

  提供对防火墙安全策略进行综合分析的能力，系统可以根据防火墙策略综合分析的结果（冗余策略数、风险策略数和未命中策略数），利用健康度算法对防火墙设备策略给出一个直观的分值，帮助管理员了解防火墙策略的整体运维情况。

  支持手工或定时执行综合分析，综合分析结果以列表和饼图的方式展示，可以查看设备策略全貌和设备健康度历史曲线，并能将分析结果导出 PDF 报表。

图4-38 策略综合分析结果

防火墙策略管理

- 公共对象配置

支持集中配置地址集、时间段、服务等公共对象的新建、删除、修改等操作。

图4-39 创建地址集

图4-40 创建自定义服务

- 访问控制策略配置

  提供网络访问控制功能配置，可以通过源地址、目的地址、服务、时间段配置访问数据流的动作为放行或阻断。

  支持策略的创建、删除、修改、复制等功能，可以对多个设备或设备组的安全策略进行配置。

图4-41 创建防火墙安全策略

- 内容安全策略配置

提供 IPS、AV 策略的配置，实现对于不同安全区域的内容安全控制，避免黑客入侵和病毒传播，保证企业网络的安全。

图4-42 创建内容安全策略

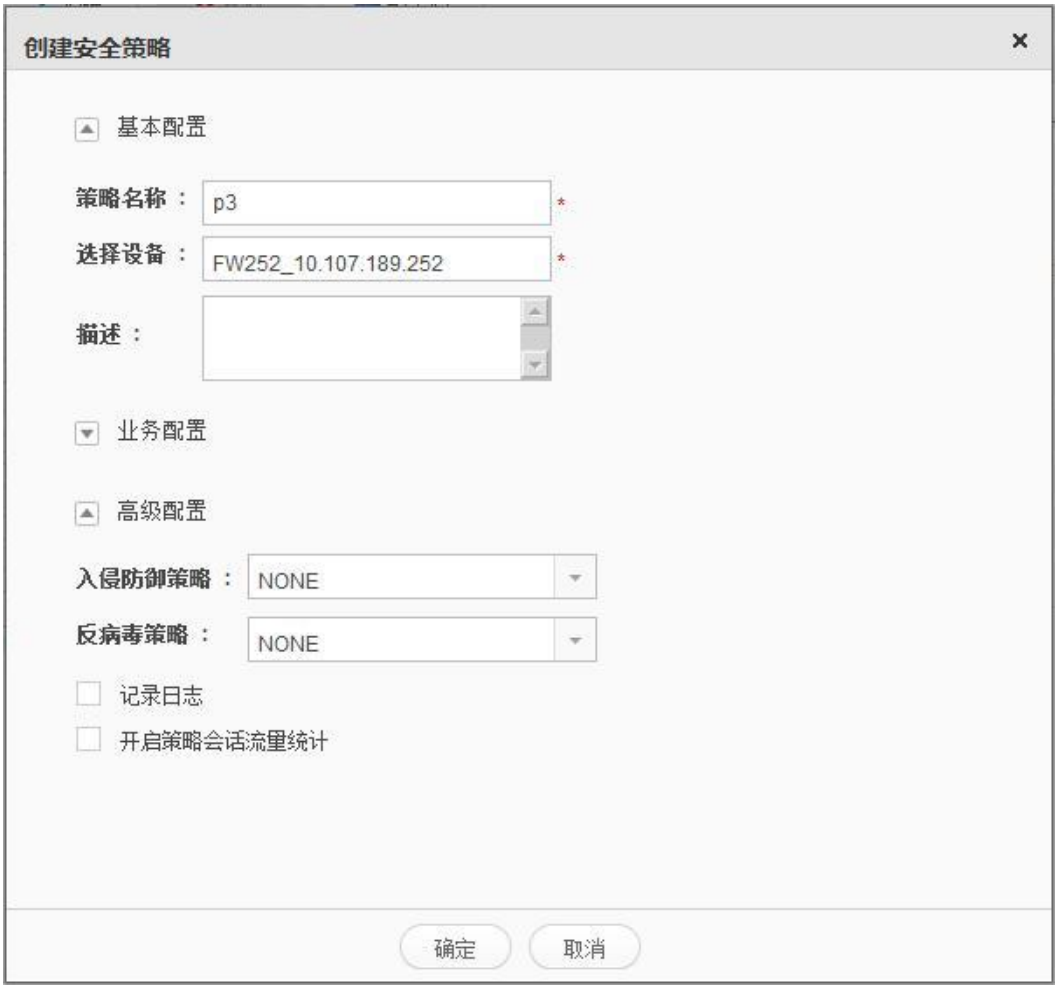


图4-43 入侵防御策略模板

对于入侵防御策略，提供默认的策略模板，并支持自定义签名，为客户提供了更加方便和灵活的管理方式。

图4-44 反病毒策略配置

- 策略查看

策略总览界面，可以查看策略的部署状态，策略的上下文环境，即域间策略的优先级，排在前面的安全年策略优先被命中。

图4-45 策略查看界面

- 策略部署

提供策略的集中、批量式部署操作，用户完成策略集中配置后，点击“部署”按钮，选择需要部署的物理防火墙或虚拟防火墙，一键式批量下发安全策略，大大节省运维人员的维护时间和操作成本。

图4-46 安全策略部署

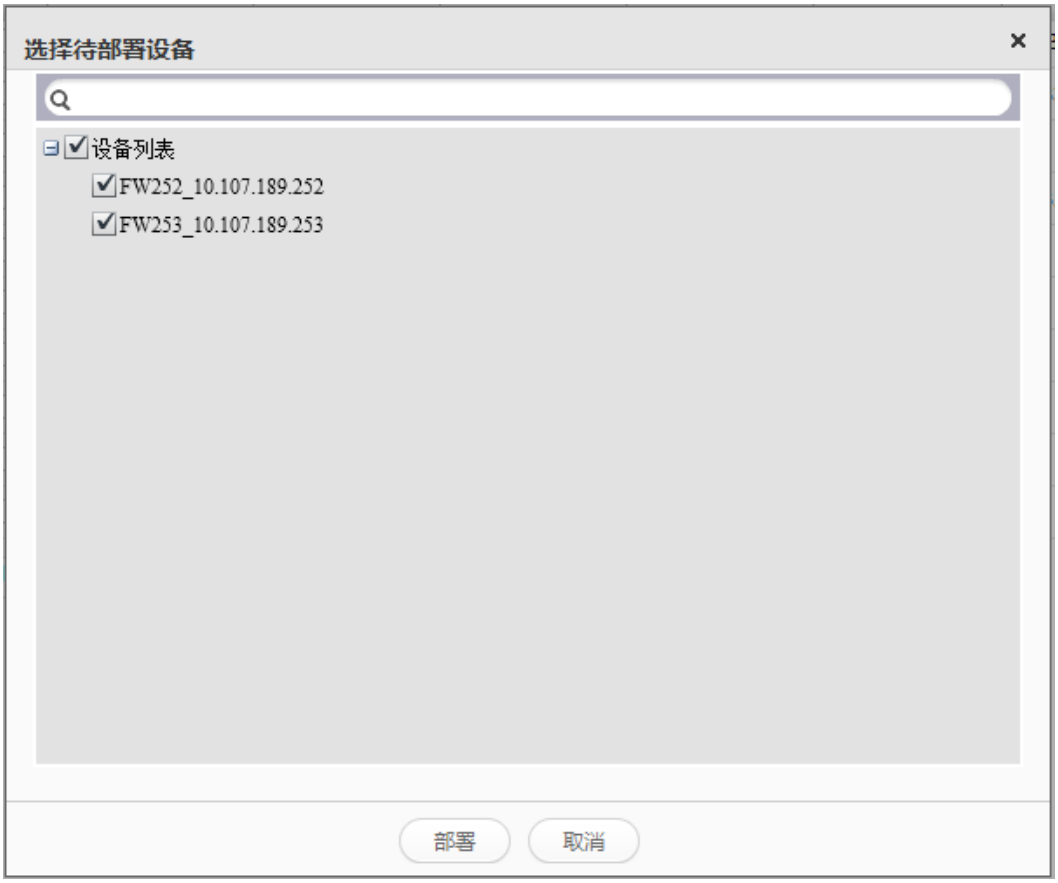
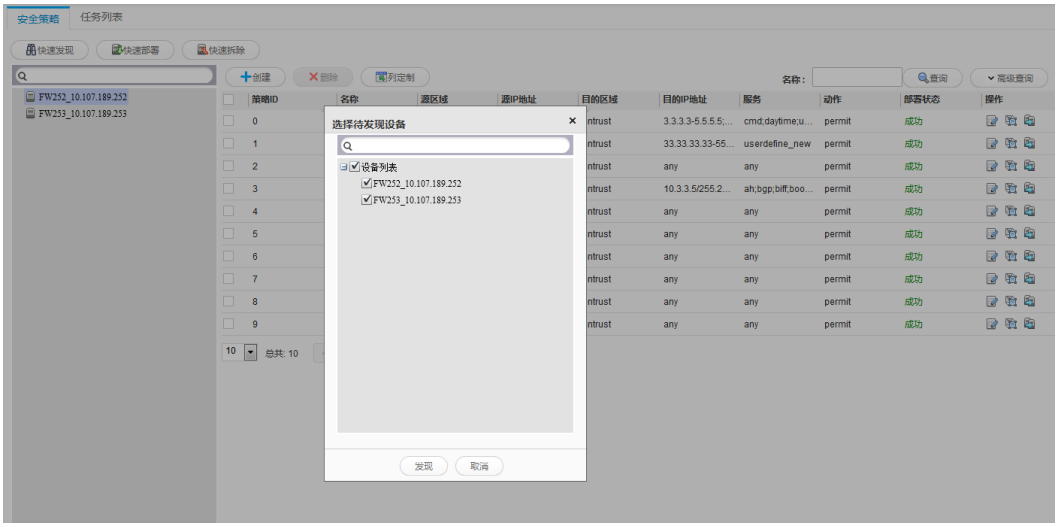


图4-47 策略部署结果

- 策略发现

提供策略的集中、批量式发现操作，将现网设备上的策略同步到网管中集中管理。

图4-48 批量设备策略发现



- 策略拆除

提供策略的集中、批量式拆除操作，用户网络整改或搬迁时，对于不再需要的配置，可以通过拆除操作，一键式清理安全策略配置，保证企业信息安全。

图4-49 批量设备策略拆除

NGFW 策略管理

- 公共对象配置

支持集中配置地址集、时间段、服务等公共对象的新建、删除、修改等操作。

图4-50 创建地址集

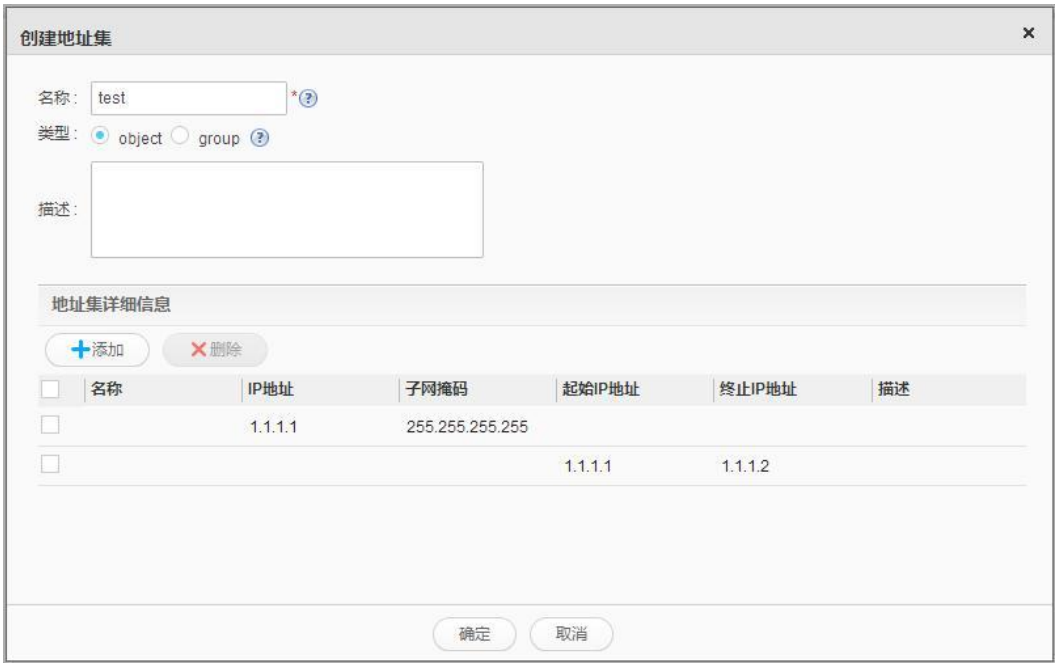


图4-51 创建时间段

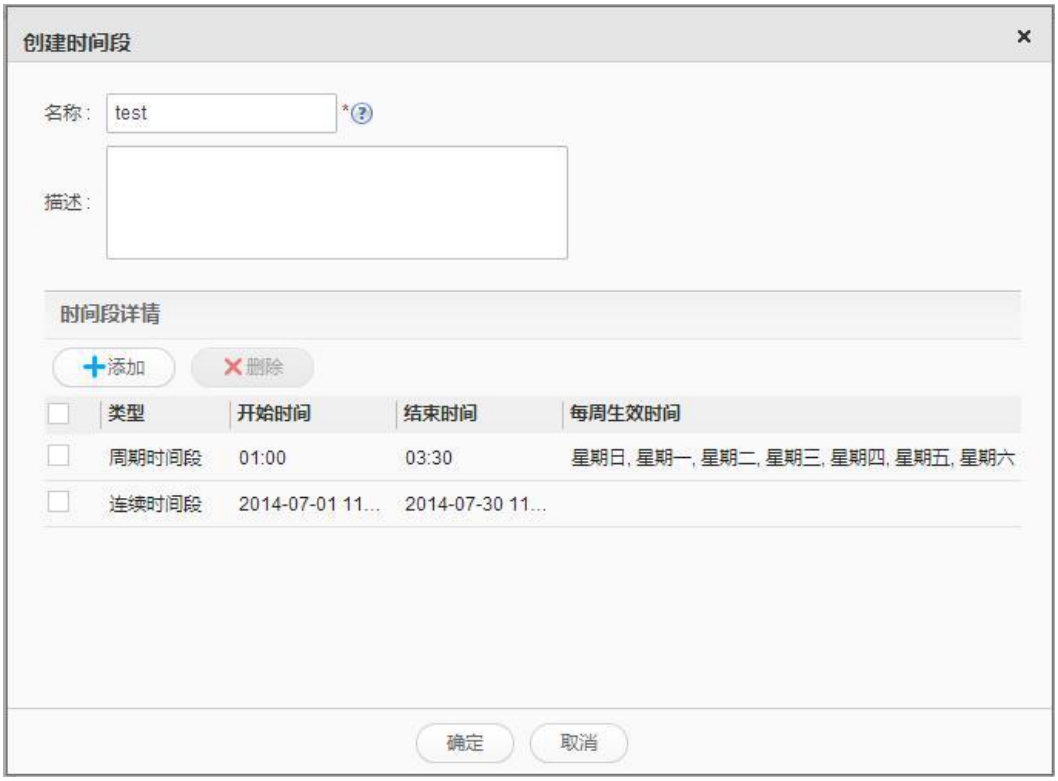


图4-52 创建自定义服务

图4-53 创建服务集

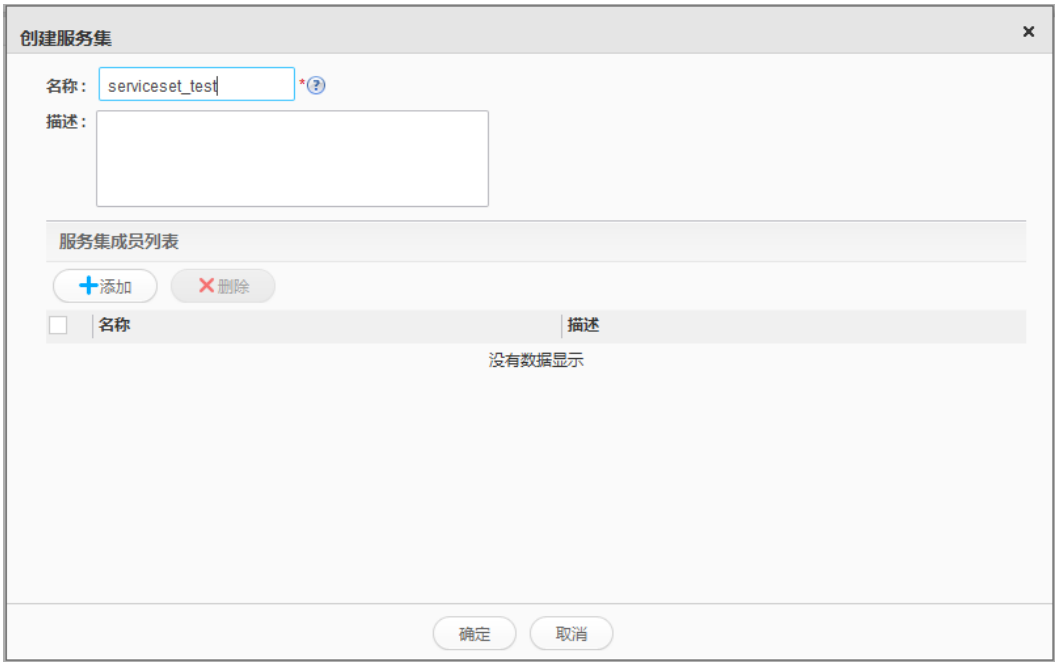


图4-54 创建上网用户

图4-55 创建上网用户组

图4-56 创建自定义应用

图4-57 创建应用组

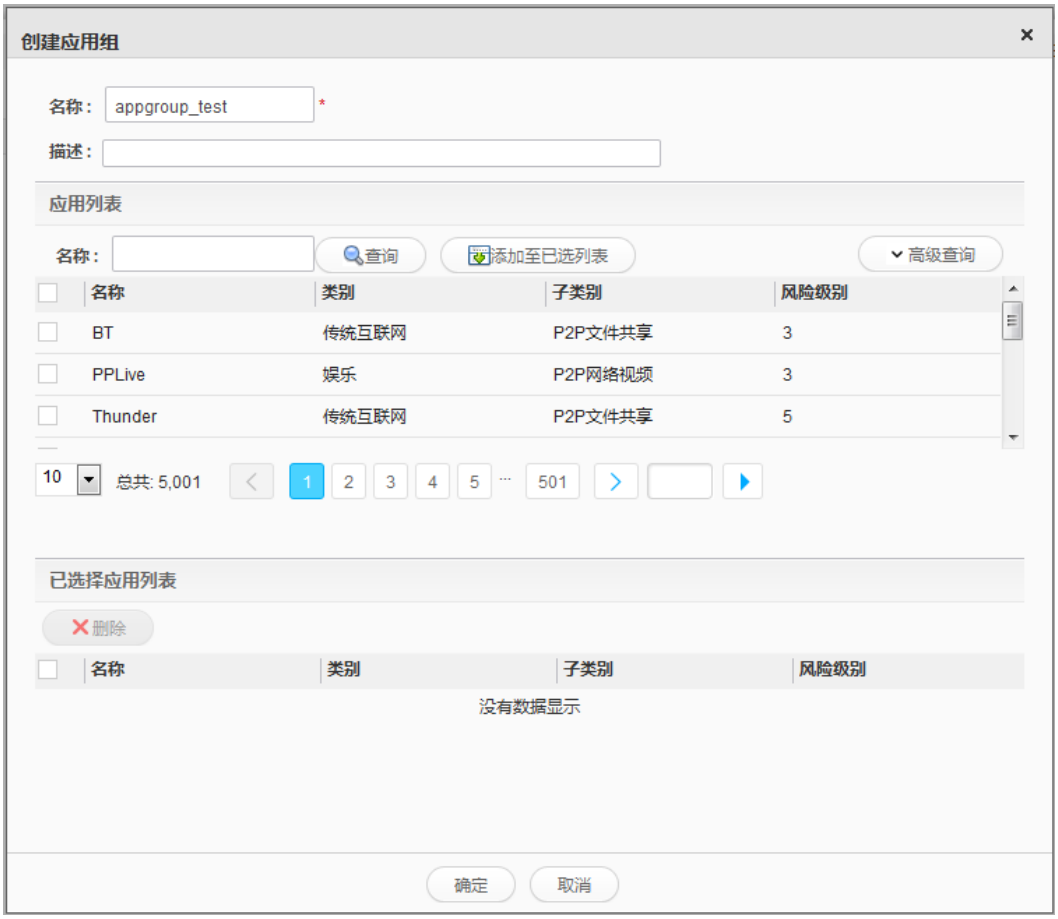
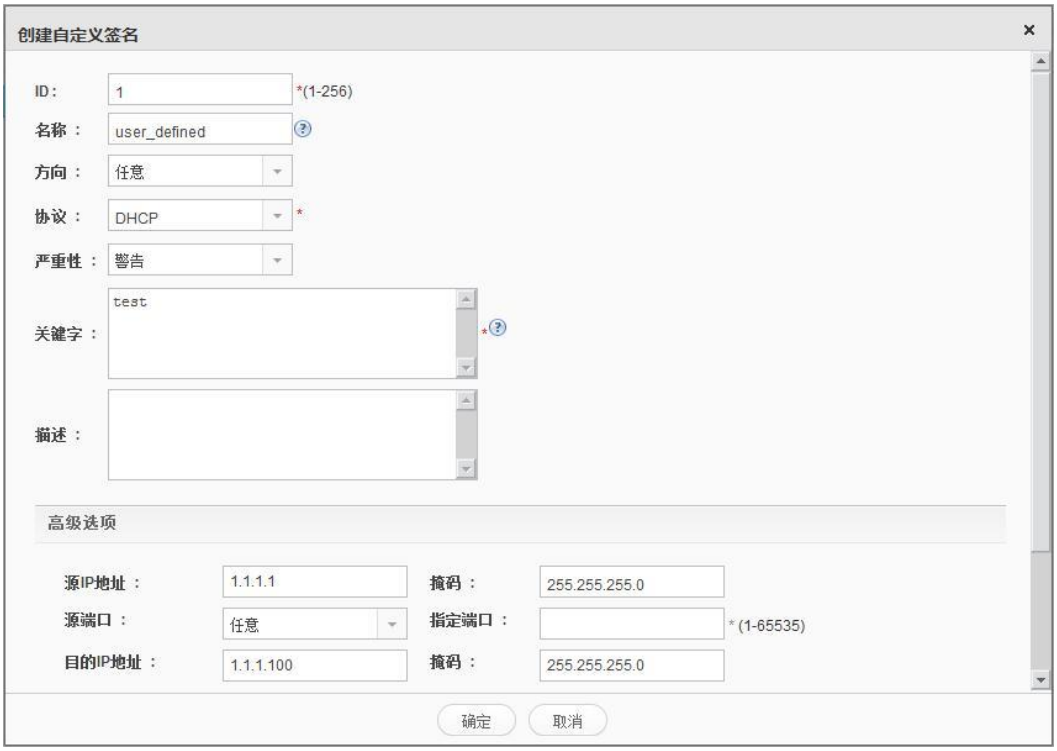


图4-58 创建自定义签名



- 访问控制策略配置

  提供网络访问控制功能配置，可以通过源地址、目的地址、服务、时间段配置访问数据流的动作为放行或阻断。

  支持策略的创建、删除、修改、复制等功能，可以对多个设备或设备组的安全策略进行配置。

图4-59 创建 NGFW 安全策略

- 安全配置文件配置

提供 IPS 入侵防御策略的配置，实现对于不同安全区域的内容安全控制，避免黑客入侵，保证企业网络的安全。

图4-60 创建可配置 IPS 内容安全的安全策略

图4-61 创建入侵防御策略

提供入侵防御策略的管理，提供预定义签名，并支持自定义签名，为客户提供了更加方便和灵活的管理方式。

- 策略查看

策略总览界面，可以查看策略的部署状态，策略的上下文环境，即域间策略的优先级，排在前面的安全年策略优先被命中。

图4-62 策略查看界面

- 策略部署

提供策略的集中、批量式部署操作，用户完成策略集中配置后，点击“快速部署”按钮，选择需要部署的物理防火墙或虚拟防火墙，一键式批量下发安全策略，大大节省运维人员的维护时间和操作成本。

图4-63 安全策略部署

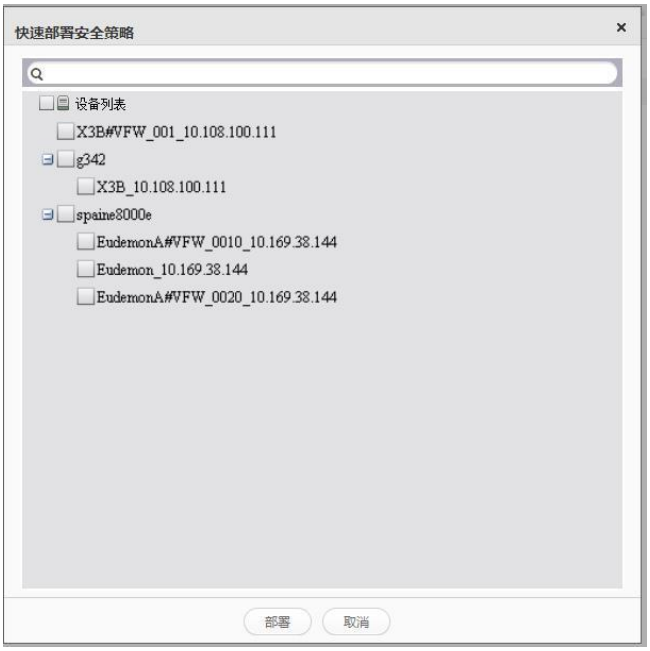


图4-64 策略部署结果

交换机策略管理

- 接入认证策略配置

  提供对华为交换机接入认证策略的集中配置和批量部署。

图4-65 创建接入认证策略

在创建接入认证策略时，需要选择 AAA 模板、用户权限模板和 802.1x 模板，同时需要选择绑定的设备或设备组。

图4-66 绑定设备或设备组

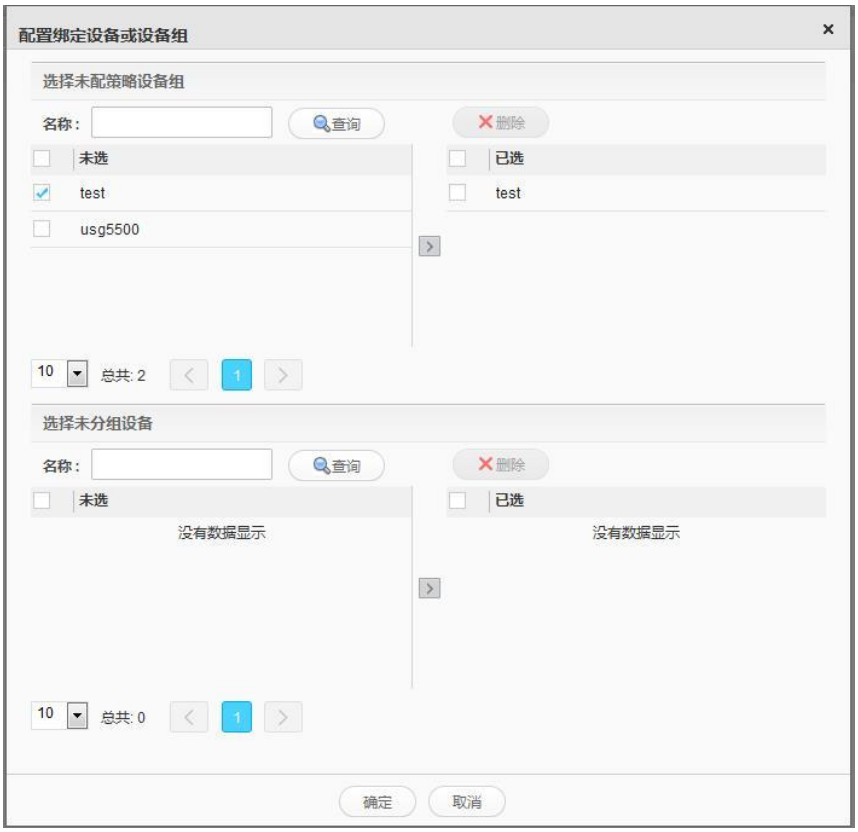


图4-67 创建 AAA 模板

图4-68 创建用户权限模板

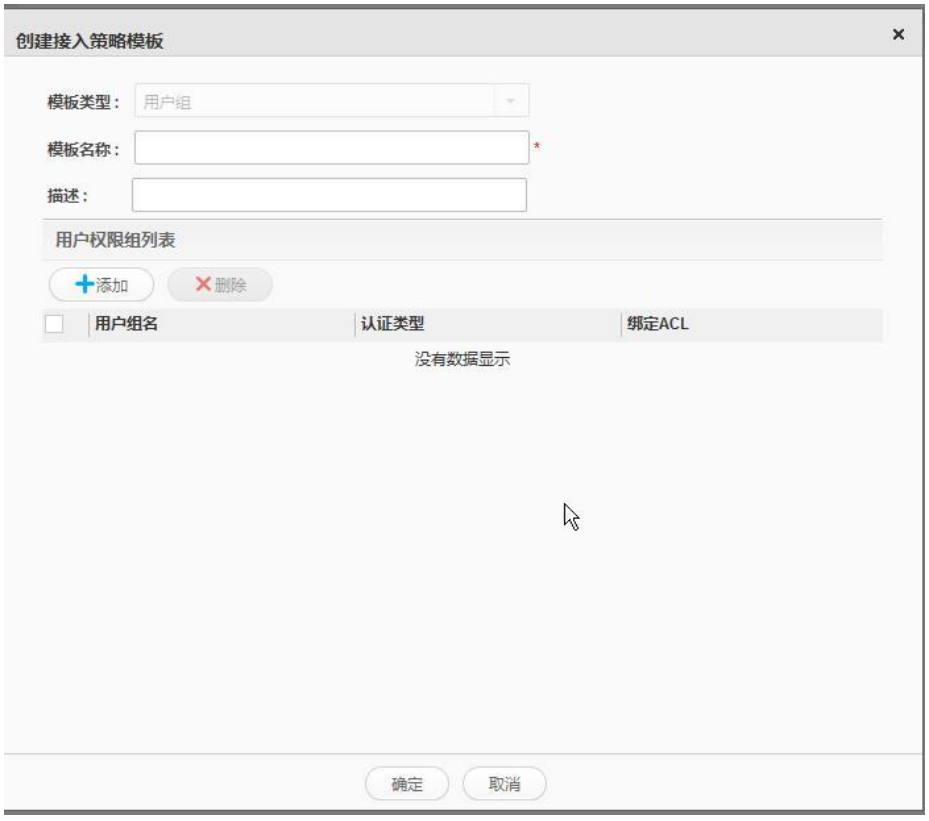


图4-69 创建 802.1x 模板

- 接入认证策略一致性审计

  支持手工和定时对交换机设备的接入认证策略进行一致性审计，审计结果支持导出报表，并可以查看一致性比较详细结果。

图4-70 策略一致性审计

AR 策略管理

- AR 安全策略配置

  提供对华为 AR 路由安全策略的集中配置和批量部署。

  图4-71 快速新建域间策略

在创建域间策略时，可以使用快速创建的方式将新建的域间策略直接部署到多个 AR 设备上，也可以在创建策略后选择策略进行批量策略部署。

图4-72 快速部署 AR 域间策略

ACL 管理

- 基本 ACL 配置
  提供对基本 ACL 的创建、删除、复制和修改。

图4-73 创建基本 ACL 规则

- 高级 ACL 配置

  提供对高级 ACL 的创建、删除、复制和修改，并支持从文本文件导入。

图4-74 创建高级 ACL 及规则

4.34 LogCenter 日志管理组件

eSight LogCenter 日志管理系统是华为面向行业用户推出的统一日志管理系统，实现对华为安全产品的全面日志分析和安全审计等功能，具有高集成度、高可靠性等特点。

日志统一管理和分析

企业内部部署了大量的路由器、交换机、防火墙等网元，由于存在网元日志格式不统一、可读性差、海量日志存储困难、日志难于统一管理等问题，网管很难及时从日志中发现重大安全隐患。

logCenter 日志管理系统能够实现日志统一管理，支持 SYSLOG、SESSION、SFTP、FTP 静态文件、FTP 动态文件、WMI（仅在 Windows 操作系统中安装 logCenter 日志管理系统时支持）多种日志采集方式。logCenter 日志管理系统能够采集、分类、过滤、归并、分析、存储和监控应用系统或网元上报的日志，帮助管理员对海量日志进行管理，使管理员能及时了解安全网元和网络网元的运行情况，跟踪网络用户行为，迅速识别并消除安全威胁。

logCenter 日志管理系统在日志管理的基础上，提供日志的实时告警响应功能，能够对日志进行实时的分析，并实时产生告警。

上网 NAT 溯源

在该应用场景下，logCenter 日志管理系统对 MA5200G、NE40E/80E、USG 防火墙等网络网元和安全网元的会话日志进行采集和分析，获取 NAT 信息（包括目的 IP 地址、目的端口、NAT 前源 IP 地址和协议等），结合用户数据源（如 AAA 服务器），从而追踪 NAT 用户的上网行为。

上网行为管理

在上网行为管理的应用场景下，logCenter 日志管理系统对 USG 防火墙等网络网元的会话日志和安全日志进行采集和分析，从而追踪上网行为（如使用 P2P、email、HTTP、MSN、QQ 等业务）；并可以按用户的上网流量、上网时长、上网关键字、Web 访问、邮件收发、上网应用、网络威胁、文件外发等查询和分析用户上网行为，从而根据分析结果对用户上网行为进行管理。

5 配置要求

5.1 软硬件配置要求

eSight 不同版本采用不同的软硬件配置，不同的硬件平台对管理能力不可避免地有所影响。

eSight 各版本软硬件配置信息如下所示。

表5-1 AppBase 服务器配置说明表

版本	管理规模	最低硬件配置	推荐服务器	系统配置
精简版	精简版：40（固定值）	CPU：1*双核 2G 以上 内存：4G 硬盘空间：40G	无	Windows 7（32 位）（中文简体或英文版本）+ MySql 5.5
标准版	0-200	CPU：1*双核 2G 以上 内存：4G 硬盘空间：40G 说明：请选用 PC Server	**IBM**：X3650M4-1*E5-2640 6c2.5GHz 或以上-8G(2*4G)-2*300G(双 6Gbps SAS 端口) **Huawei**：Tecal RH2288H V2-1*E5-2630 V2 CPU,2*4GB 内存,2*300GB	配置 1：Windows Server 2008 R2 标准版（64 位）（中文简体或英文版本）/Windows Server 2012 R1 标准版（64 位）（中文简体或英文版本）+ MySql 5.5（标准版网管软件包中自带）/Microsoft SQL Server 2008 R2-标准版 配置 2：Novell SuSE LINUX Enterprise Server-多国语言版本-企业版
	200-500	CPU：2*双核 2G 以上 内存：4G 硬盘空间：60G 说明：请选用 PC Server		
	500-2000 WLAN	CPU：2*四核 2G 以上	**IBM**：X3650 M4-2*Xeon 6C E5-2640 2.5G	

版本	管理规模	最低硬件配置	推荐服务器	系统配置
	定位 AP：0-50	内存：8G 硬盘空间：120G 说明：请选用 PC Server	或以上-32G(4*8G)-3*300G(双 6Gbps SAS 端口) **Huawei：** Tecal RH2288H V2-2*E5-2630 V2 CPU,4*8GB 内存,3*300GB	-11.0 SP3 （中文简体或英文版本）+ Oracle Database Standard Edition 11g R2
	2000-5000 WLAN 定位 AP：50-500	CPU：2*四核 2G 以上 内存：16G 硬盘空间：250G 说明：请选用 PC Server		
专业版	0-200	CPU：1*双核 2G 以上 内存：4G 硬盘空间：40G 说明：请选用 PC Server	**IBM：** X3650M4-1*E5-2640 6c2.5GHz 或以上-8G(2*4G)-2*300G(双 6Gbps SAS 端口) **Huawei：** Tecal RH2288H V2-1*E5-2630 V2 CPU,2*4GB 内存,2*300GB	配置 1：Windows Server 2008 R2 标准版（64 位）（中文简体或英文版本）/Windows Server 2012 R1 标准版（64 位）（中文简体或英文版本）+ MySql 5.5（标准版网管软件包中自带）/Microsoft SQL Server 2008 R2-标准版 配置 2：Novell SuSE LINUX Enterprise Server-多国语言版本-企业版-11.0 SP3 （中文简体或英文版本）+ Oracle Database Standard Edition 11g R2
	200-500	CPU：2*双核 2G 以上 内存：4G 硬盘空间：60G 说明：请选用 PC Server		
	500-2000 WLAN 定位 AP：0-50	CPU：2*四核 2G 以上 内存：8G 硬盘空间：120G 说明： 请选用 PC Server	**IBM：** X3650 M4-2*Xeon 6C E5-2640 2.5G 或以上-32G(4*8G)-3*300G(双 6Gbps SAS 端口) **Huawei：** Tecal RH2288H V2-2*E5-2630 V2 CPU,4*8GB 内存,3*300GB	
	2000-5000 WLAN 定位 AP：50-500	CPU：2*四核 2G 以上 内存：16G 硬盘空间：250G 说明：请选用		

版本	管理规模	最低硬件配置	推荐服务器	系统配置
		PC Server		
	5000-20000 WLAN 定位 AP : 500-1000	CPU：4*四核 2G 以上 内存：32G 硬盘空间：320G 说明：请选用 PC Server	**IBM**：X3850 X5-4*Xeon 8C E7-4820 2.0G 或以上-64G(8*8G)-8*300G **Huawei**：Tecal RH5885H V3-4*E7-4820 V2 CPU,8*8GB 内存,8*300GB	配置 1：Novell SuSE LINUX Enterprise Server-多国语言版本-企业版-11.0 SP3 （中文简体或英文版本）+ Oracle Database Standard Edition 11g R2

表5-2 eSight NTA 与服务器的配套说明

版本	管理节点	硬件器配置	推荐服务器	系统配置
同机部署 （AppBase+NTA）	APPBASE：0-500 NTA： 0-10	CPU：2*四核 2G 以上 内存：8GB 硬盘空间：120GB 说明：请选用 PC Server。	**IBM**：X3650 M4-2*Xeon 6C E5-2640 2.5G 或以上-32G-3*300G **Huawei**：Tecal RH2288H V2-2*E5-2630 V2 CPU,4*8GB 内存,3*300GB	Windows Server 2008 R2 标准版（64 位）（中文简体或英文版本）/Windows Server 2012 R1 标准版（64 位）（中文简体或英文版本）+ MySql 5.5（标准版网管软件包中自带）/ Microsoft SQL Server 2008 R2-标准版
	AppBase：500-2000 WLAN 定位 AP : 0-50 NTA： 0~10	CPU：2*四核 2G 以上 内存：16GB 硬盘空间：250GB 说明：请选用 PC Server。	**IBM**：X3650 M4-2*Xeon 6C E5-2640 2.5G 或以上-32G-3*300G **Huawei**：Tecal RH2288H V2-2*E5-2630 V2 CPU,4*8GB 内存,3*300GB	
	AppBase： 2000~5000 WLAN 定位 AP : 50-500 NTA： 0~10	CPU：4*四核 2G 以上 内存：32GB 硬盘空间：320GB 说明：请选用 PC Server。	**IBM**：X3850 X5-4*Xeon 8C E7-4820 2.0G 或以上-64G-8*300G **Huawei**：Tecal RH5885H V3-4*E7-4820 V2 CPU,8*8GB 内存,8*300GB	
分机部署	0-100	CPU：1*四核 2G 以上	**IBM**：X3650M4-1*E5-2640 6c2.5GHz 或以上-8G-2*300G	网流分机部署，不需要安装数据库，操作系统要求与

版本	管理节点	硬件器配置	推荐服务器	系统配置
		内存：4GB 硬盘空间：120GB 说明：请选用 PC Server。	**Huawei：** Tecal RH2288H V2-1*E5-2630 V2 CPU,2*4GB 内存,2*300GB	eSight AppBase 保持一致。
	100-350	CPU：2*四核 2G 以上 内存：16GB 硬盘空间：250GB 说明：请选用 PC Server。	**IBM：** X3650 M4-2*Xeon 6C E5-2640 2.5G 或以上-32G-3*300G **Huawei：** Tecal RH2288H V2-2*E5-2630 V2 CPU,4*8GB 内存,3*300GB	

表5-3 eSight LogCenter 服务器的配套说明

版本	管理规模	硬件配置	推荐服务器	系统配置
同机部署（AppBase+LogCenter）	AppBase： 0-500 LogCenter： Syslog 0 ~ 2000EPS 或者 NAT 溯源 0 ~ 10000EPS；	CPU：2 * 6 核 2.5G 以上 内存：12G 硬盘空间：8*300G 或者 2*300G+磁盘阵列。 说明：请选用 PC Server。	**IBM：** X3650 M4-2*Xeon 6C E5-2640 2.5G 或以上-32G(4*8G)-3*300G **Huawei：** Tecal RH2288H V2-2*E5-2630 V2 CPU,4*8GB 内存,3*300GB	Windows Server 2008 R2 标准版（64 位）（中文简体或英文版本）/Windows Server 2012 R1 标准版（64 位）（中文简体或英文版本）+ MySql 5.5（标准版网管软件包中自带）/Microsoft SQL Server 2008 R2-标准版
	AppBase： 500-2000 WLAN 定位 AP : 0-50 LogCenter： Syslog 0 ~ 2000EPS 或者 NAT 溯源 0 ~ 10000EPS；	CPU：2 * 6 核 2.5G 以上 内存：16G 硬盘空间：8*300G 或者 2*300G+磁盘阵列。 说明：请选用 PC Server。	**IBM：** X3650 M4-2*Xeon 6C E5-2640 2.5G 或以上-32G(4*8G)-3*300G **Huawei：** Tecal RH2288H V2-2*E5-2630 V2 CPU,4*8GB 内存,3*300GB	
	AppBase： 2000-5000 WLAN 定位	CPU：2 * 6 核 2.5G 以上 内存：24G 硬盘空间：8*300G 或者	**IBM：** X3850 X5-4*Xeon 8C E7-4820 2.0G 或以上-	

版本	管理规模	硬件配置	推荐服务器	系统配置
	AP：50-500 LogCenter： Syslog 0 ~ 2000EPS 或者 NAT 溯源 0 ~ 10000EPS；	2*300G+磁盘阵列。 说明：请选用 PC Server。	64G(8*8G)-8*300G **Huawei：**Tecal RH5885H V3-4*E7-4820 V2 CPU,8*8GB 内存,8*300GB	
采集器独立部署	每采集器： 会话日志（针对上网行为分析）150000EPS（不带磁盘柜）；或 会话日志（传统防火墙）160000EPS；或文本日志 7000EPS；或二进制 Dataflow 日志 20000EPS；	CPU：2*四核 2G 以上内存：8G 硬盘空间：8*300G 说明：请选用 PC Server	**IBM：**X3650M4-1*E5-2640 6c2.5GHz 或以上-8G(2*4G) **Huawei：**Tecal RH2288H V2-1*E5-2630 V2 CPU,2*4GB 内存,2*300GB	1、采集器不需要安装数据库； 2、操作系统要求：Windows Server 2008 R2 标准版（64 位）

表5-4 eSight 全组件同机部署服务器的配套说明

版本	管理节点	硬件器配置	推荐服务器	系统配置
eSight 全组件同机部署 （支持 AppBase 与组件的任意组合）	AppBase：0-200 网流：0-10 节点 LogCenter：Syslog 0 ~ 1000EPS 或者 NAT 溯源 0 ~ 5000EPS	CPU：2 * 四核 2G 以上 内存：16G 硬盘空间：500G（可用硬盘空间推荐 1TB） 说明：请选用 PC Server	**IBM：**X3650 M4-2*Xeon 6C E5-2640 2.5G 或以上-32G-3*300G **Huawei：**Tecal RH2288H V2-2*E5-2630 V2 CPU,4*8GB 内存,3*300GB	Windows Server 2008 R2 标准版（64 位）（中文简体或英文版本）/Windows Server 2012 R1 标准版（64 位）（中文简体或英文版本）+ Microsoft SQL Server 2008 R2-标准版

注意

客户端对操作系统没有特殊要求，要求浏览器版本以及内存满足以下条件：

- 浏览器版本：Internet Explorer 9.0/10.0、Mozilla Firefox 27.0/30.0、Chrome 29。
- 系统可用内存：至少 1G 以上。

6 技术指标

介绍 eSight 系统的技术指标。

eSight 系统最多可管理 20000 个网元。

表6-1 技术指标

指标项	指标值
当前告警存储容量(条)	2 万
历史告警存储容量(条)	1500 万
事件告警存储容量 (条)	200 万
审计日志存储容量(条)	300 万
告警处理能力(条/秒)	100
单个子网支持拓扑对象个数(个)	500
拓扑管理支持的拓扑对象最大层数(层)	11

7 遵从的标准和协议

介绍 eSight 系统遵从的标准和协议。

- 与设备的接口遵从 SNMP、MIBII 标准
  - RFC1155 基于 TCP/IP 的互联网管理信息的结构和标识。
  - RFC1157 基于简单网络管理协议 SNMP。
  - RFC1213 基于 TCP/IP 的互联网的网络管理信息库 MIB-II。
- XML 1.0
- ITU-T X.733 故障管理规范

A 术语

术语	解释
B	
NBI	NorthBound Interface：北向接口。连接上级网管系统和设备的接口，用于实现发放业务、上报告警、上报性能指标数据等功能。
C	
CLI	Command Line Interface：命令行接口，以命令行的方式对云存储系统进行管理。
E	
ESN	Equipment Serial Number：设备序列号。
F	
FTP	File Transfer Protocol：文件传输协议。
I	
iPCA	Packet Conservation Algorithm for Internet：网络包守恒算法。
O	
OSS	Operating Support System：运营支撑系统。
R	
RSA	Revist-Shamir-Adleman Algorithm：RSA 加密算法。
S	
SFTP	Secure File Transfer Protocol：安全文件传输协议。
SNMP	Simple Network Management Protocol：简单网络管理协议。
SOAP	Simple Object Access Protocol：简单对象访问协议。
T	
TCP	Transmission Control Protocol：传输控制协议。
U	

术语	解释
UDP	User Datagram Protocol：用户数据报协议。
V	
VMM	Virtual Machine Manager：虚拟资源的集中管理软件，eSight 通过 VMM 管理所有的虚拟资源。
X	
XML	eXtensible Markup Language：可扩展标记语言。