UNIS SDOP安全管理平台

产品概述

UNIS SDOP 安全业务管理平台是一个负责网络安全业务的独立平台。SDOP 能够对网络中的防火墙、入侵防御安全设备进行统一管理，它能够适应各种网络规模需求，为部署于各关键位置的安全设备提供集中的安全策略管理与控制，并能直观的为实时事件监控和综合分析攻击等各种安全事件提供丰富的统计报告，方便用户随时了解网络安全状况。提供实时监控、综合分析、策略下发以及威胁日志审计等功能。并且能对全网范围内的安全事件进行集中的统计分析。

UNIS SDOP

产品特点

◆ 统一运维管理

- 安全策略统一管理
- 设备性能统一监控
- 安全特征库统一升级

SDOP 平台将设备同步至平台的全局资源；可以进行安全策略手动新增/修改/删除，并批量下发至设备功能；支持设备 IPS、AV、ARP 特征库信息查看/同步/升级/回滚功能；支持特征库文件上传/查询/推送/删除功能；支持特征库文件推送任务管理，包括

推送任务状态、运行结果等信息展示；对被管理设备的性能值 CPU、内存利用率、系统流量统计、接口流量详情、系统并发会话、系统新建会话做统一展示。

◆ 日志审计告警

- IPS/FW 设备安全事件威胁日志收集分析；多条件日志查询
- IPS/FW 安全事件日志范式化处理；支持按照开始时间和结束时间、源 IP、目的 IP、源端口、源安全域、目的安全域、产生日志设备名称、动作、协议、事件级别等条件进行日志梳理
- 支持自定义日志聚合进行事件告警

SDOP 通过收集设备日志直观了解安全事件的来源、目的地等的行为状况，详细记录攻击事件，帮助管理员了解到网络攻击、异常流量状况，并对用户操作进行跟踪，便于事后审计和追踪。同时，SDOP 提供强有力的搜索查询能力，能够从海量的历史数据中，基于设备、时间、事件级别、协议、动作、源/目的 IP、等多维度定义进行快速查询。

◆ **报表管理**

- 平台预定义多种报表
- 支持报表自定义，可以基于日、周、月进行报告输出，支持时间自定义输出

SDOP 平台预定义了 IPS 阻断事件、IPS 攻击事件、IPS 攻击目的端口、IPS 攻击源 ip、IPS 攻击目的 ip 五个报表模板；并且支持自定义报表；支持基于不同时间区域、报表模板，自定义报告输出。

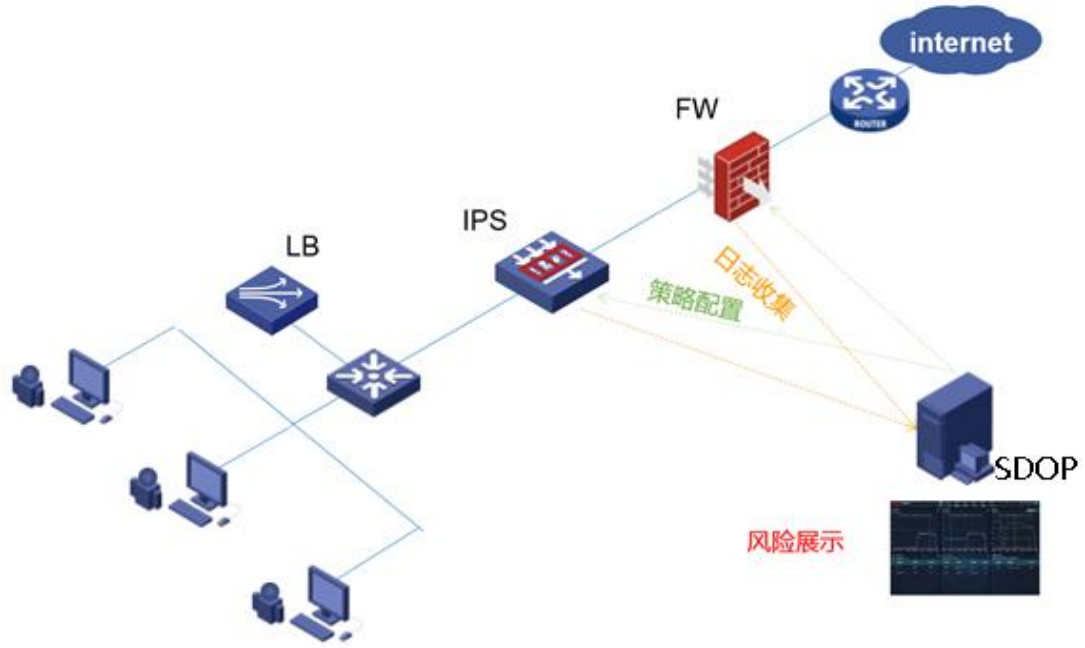
产品规格

项目	描述
首页管理	展示设备性能状况，安全事件状况；根据不同时间统计TOPN排名
安全分析	通过安全日志，对网内攻击、漏洞、阻断事件数趋势进行展示
报表管理	提供丰富的报表模板，具有定时生成报表以及根据模板自定义生成报表
日志审计	FW/IPS威胁日志收集归类；基于多条件查询功能；查看日志详情；支持日志的查询导出等功能
安全事件	支持安全事件的展示以及自定义关联规则，并根据告警规则生成告警事件；页面弹框生成告警，支持处理/批量处理安全事件
运维管理	支持区域管理、资产管理、安全业务管理、特征库管理
系统管理	数据清理设置、系统参数配置、角色管理、个性化定制标题LOGO等

产品性能

项目	描述
管理数量	最大支持管理千兆防火墙、万兆防火墙等安防设备数量1000 台（根据授权节点数量决定）
日志处理	安全日志接收处理性能达8.6亿条/天（平均1万条/秒）

典型组网



紫光恒越技术有限公司

北京基地
北京市海淀区中关村东路 1 号院 2 号楼 402 室
邮编：100084
电话：010-82054431
传真：010-82054401

www.unisyue.com

客户服务热线
400-910-9998