SecFox-SGM
安全设备集中管理系统

SecFox-SGM（SecGateManager）安全设备集中管理系统的目标定位于网御神州科技（北京）有限公司一系列安全设备的集中策略管理，统一升级，以及集中的日志分析与审计。

需求分析

为了不断应对来自内部和外部的安全挑战，企业和组织先后部署了大量的安全网关，包括防火墙、VPN、UTM等设备。针对这些大量的分布式部署的安全设备，管理人员耗费了很多精力在设备的配置和维护上，费时费力，十分不方便。尤其是下发VPN策略的时候，需要分别在不同的安全网关上进行设置，十分容易出错。因此，企业和组织迫切需要一个针对这些安全设备的集中管理解决方案。

产品特点

设备监控与管理

SecFox-SGM采用集中管理的方式，对网神防火墙、VPN、UTM设备进行集中策略配置。

安全设备日志分析与审计

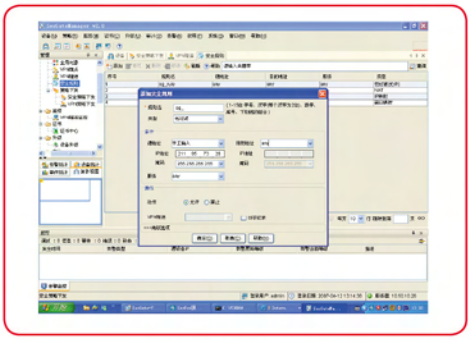
SecFox-SGM能够采集多种信息源的安全事件信息并提供实时告警及图形化分析。

防火墙/VPN集中策略管理

SecFox-SGM能够集中地对防火墙/VPN进行策略定义和可视化发布。

安全设备升级

SecFox-SGM能够实现防火墙/VPN设备的批量升级。



全网统一策略下发

在SecGateManager中激活SecGate防火墙管理界面

功能列表

功能点	说明	
产品形态	软件，有多个模块可选	
网络拓扑管理	提供用户一个企业计算环境的总体概况，直观地给出了整个网络中网络设备、主机设备、安全设备的分布和连接情况。用户可以进行手动拓扑发现，用户可以通过拓扑图进行设备监控、配置管理和策略管理，通过拓扑图可以直观的反映设备的实际运行状态	
设备监控	通过一个控制台，用户就能够监控整个计算环境中所有安全设备的运行状态和性能分析，并实时获得告警，便于采取应急响应行动	
策略管理	通过统一的界面，对全网的安全设备进行安全策略的编辑和下发。策略管理的内容包括设备对象定义、VPN端点（IKE）管理、VPN隧道（IPSec）管理、安全规则管理、安全策略下发和VPN隧道监控（该功能针对企业版）	
设备升级管理	用户可以通过本系统上传升级包，对安全设备进行批量升级操作。包括升级包管理、查看设备当前版本、下发升级包等功能（该功能针对企业版）	
安全审计	安全审计的主要功能是日志查询、日志分析规则设置、安全审计报表。系统能够收集来自防火墙、网络设备、主机和应用的日志信息	
告警与响应管理	将所有的告警记录按发生时间、告警状态、事件类型、事件等级、源设备IP、源设备类型等信息列表显示，对告警信息进行分析和统计。产生的告警信息能够通过电话响铃、邮件、短信、电脑语音、控制台弹出窗口、SNMP trap、防火墙/交换机设备联动告警的方式通知管理人员	
报表管理	提供丰富的报表管理功能；根据时间、数据类型等生成报表，提供打印、导出以及邮件送达等服务；直观地为管理员提供决策和分析的数据基础，帮助管理员掌握网络及业务系统的状况。报表可以保存为HTML、Excel、文本、PDF等多种格式	
权限管理	通过一个控制台，用户就能够监控整个计算环境中所有设备的运行状态和性能分析，并实时获得告警，便于采取应急响应行动	
系统配置	完成对系统自身的各项配置工作	
性能	节点规模	1000个
	事件处理性能	8000EPS（事件数每秒）
	事件存储性能	事件存储量仅取决于系统所用存储空间大小
	控制台并发连接数	50个（即同一时刻可以有50个用户使用本系统）