



安州安全策略管理系统

1. 产品概述

随着信息化在各行业不断的普及和推进,对信息安全要求越来越高。安全策略是信息安全管理的重要组成部分,安全策略的精细化控制是安州安全策略管理的核心。能够完成从过去的人工单点分析策略,到现在的全网安全拓扑可视化;能够完成安全策略梳理优化,减少被攻击面,保障全网业务可靠性。

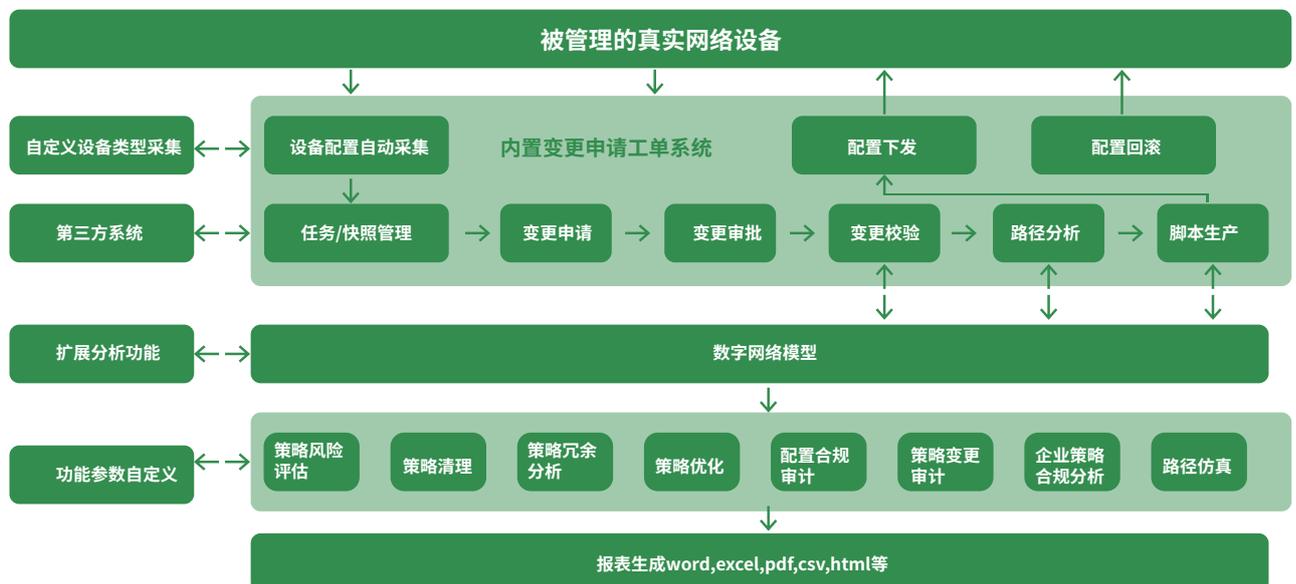
安全策略在事前可对全网风险评估,对各区域间的安全配置进行合规性审计,分析出风险配置,实现全网安全策略可视化。

安全策略在事中可快速分析攻击路径,自动生成策略,阻断攻击路径。

安全策略在事后可建立全网配置基线和安全核查基线,定期自动生成网络安全指数,跟踪全网安全策略变化。

通过综合数据网业务安全保障及业务可视化分析与优化服务,用自动化智能方式代替人工方式,全面高效精确分析业务流量运行数据,实现业务可视化分析。通过收紧业务安全访问的颗粒度,精确细化业务可访问的白名单规则,降低业务受非法入侵的概率,进而提升业务系统的安全性。同时,在服务期间,定期对业务进行梳理及安全优化。包括无效、冗余、冲突等业务关系的梳理,提升业务访问性能。减少业务攻击面,从而减轻业务层面受到的安全威胁。另外,在护网等重要时刻,能够更加高效的保障业务系统安全。

2. 产品部署



实现本项目需求需要的核心技术包括:任务/快照管理、自动配置采集、网络建模、策略风险评估、策略清理、策略冗余分析、策略优化、配置合规审计、策略变更审计、企业策略合规分析、路径仿真、报表生成、策略变更工单系统(包括:变更申请、审批、校验、路径分析、脚本生成、配置下发、回滚)。除了上述功能,本系统还支持自定义设置类型采集,与第三方系统接口,扩展分析功能,以及对现有分析功能的自定义。

平台部署

安全策略可视化梳理平台可在linux系统上安装

支持国产化虚拟机平台

提供基于web页面的平台服务

推荐使用Centos7.5系统

至强 8核CPU

16G内存

100G硬盘空间以上

3.产品优势

一、等保2.0要求

2019年发布GB/T 22239-2019 信息安全技术网络安全等级保护基本要求(简称 等保2.0)中,对于等保二级三级四级网络的边界防护、访问控制、集中管控都提出了明确要求。“对分布在网络中的安全设备或安全组件进行管控,应能够建立一条安全的信息传输路径,对网络中的安全设备或安全组件进行管理;应对网络链路、安全设备、网络设备和服务器的运行状况进行集中监测;应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理。”

二、全网安全策略可视化

安全策略可视化梳理优化平台,全面支持国内外各厂商的二三层防火墙、交换机、路由器、负载均衡设备等。支持品牌包括华为、华三、中兴、锐捷、深信服、思科、瞻博、天融信、网神、启明星辰、联想、山石网科、飞塔、迈普、网康、迪普等主流品牌,支持管理的设备可以是防火墙、交换机、路由器任何一种或者组合。

1.态势可视化

在监控面板上可以看到,被监控的网络安全设备列表,Top10设备的策略数,Top10设备的安全配置审计问题数,需要清理的策略分类柱状图,以及设备的实时变更信息。

2.策略可视化

展示多厂商的设备基本信息、策略、接口、NAT、路由、访问关系等信息,对策略进行冗余、遮盖、合并分析、优化策略,减少安全漏洞,提高设备性能。以策略最小化为原则,自动分析海量防火墙日志,发现网段地址中的单个ip真实使用情况,帮助用户进行策略收紧。

3.拓扑可视化

基于采集的网络设备的CDP、LLDP配置信息,以及网络数据包在设备上留下的ARP、MAC等信息痕迹,检查设备间的逻辑关系,自动推导还原出和真实网络拓扑结构一致的虚拟数字化二三层网络拓扑结构,包括云平台内的虚拟机设备节点。可以准确了解当前生产网络逻辑结构,找出网络边界。并提供详细的设备信息查询功能。

4.攻击面可视化

交叉比对全网防火墙策略,给出全网暴露风险统计,top10 危险端口,top10 危险服务器。

5.搜索可视化

网络策略安全与配置核查管理系统根据当前流行的搜索引擎模式,对全网的网络安全设备配置进行大数据分析和索引,创造性地构建了类似搜索引擎的模式。

三、减少被攻击面

攻击面是攻击者可能危害企业设备或网络的总位置数。减少攻击面意味着攻击者更少地执行攻击。网络策略安全与配置核查管理系统通过风险分析、企业合规矩阵分析、路径可视化、配置合规分析、策略梳理优化五个方面对全网安全策略进行分析,减少潜在的被攻击面。

四、自动化配置变更

为安全管理人员提供全网安全可视化平台,用于管理安全策略,自动化管理系统替代传统人工分析,可以避免人为错误,减少运维人员投入,降低企业IT成本。

电话:010-60606994 售后热线:400-188-5118
网址:<http://www.anzhou.net.cn> 邮编:100193
地址:北京市海淀区西北旺东路10号院东区4号楼科锐大厦206房间

