南通沪蔬通农业发展有限公司网络安全

提升建设方案

一、防火墙建设

（一）功能定位

企业网络的“AI安检门“

（二）核心需求

1.精准识别500余种变种病毒，包括伪装成文档的勒索程序 。

2.实时拦截网络攻击行为，如端口扫描、暴力破解等。

3.智能管理上网行为，阻止访问赌博、钓鱼等高风险网站。

（三）实现技术

1.云端威胁情报库每小时更新，自动识别最新攻击特征。

2.虚拟补丁技术可在厂商发布修复程序前防御漏洞攻击 。

3.可视化流量分析，直观展示网络攻击来源与类型。

（四）应用案例

当黑客试图通过伪造的采购合同文件传播病毒时，系统在0.3秒内识别异常代码特征，立即阻断文件传输并向管理员发送预警信息。

二、云端安全监测平台

包括WEB应用识别库、IPS特征库、热门威胁库、实时漏洞分析识别库和URL&应用识别库定期更新，保持设备具备检测防御最新威胁的能力。

三、硬件侧安全屏障——公司机房和各弱电间线路整理和VLAN划分

（一）提高安全性

没有划分VLAN前，交换机端口连接下的所有主机都处于一个LAN中，即一个广播域中，实现ARP中间人攻击太简单了。划分了VLAN之后，缩小了ARP攻击的范围。ARP报文是一个2.5层的报文，只能在同一个VLAN中传播。

（二）提高性能

不划分VLAN，整个交换机都处于一个广播域，随便一台PC发送的广播报文都能传送整个广域播，占用了很多带宽(引起广播风暴)。划分了VLAN，缩小的广播域的大小，缩小了广播报文能够到达的范围。

1. 项目内容

推荐品牌：深信服、锐捷、天融信

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 参数 | 数量 | 单位 |
| 1 | 下一代防火墙 | 性能参数：网络层吞吐量：≥4G，应用层吞吐量：≥2G，防病毒吞吐量：≥600M，IPS吞吐量：≥600M，全威胁吞吐量：≥450M，并发连接数：≥200万，HTTP新建连接数：≥6万，SSL VPN推荐用户数：≥20，SSL VPN最大用户数：≥60，SSL VPN最大理论加密流量：≥160M，IPSec VPN 最大接入数：≥300，IPSec VPN吞吐量：≥270M。 最低硬件参数：规格：1U，内存大小：4G，硬盘容量：128G SSD，电源：单电源，接口：8千兆电口+2千兆光口SFP。  其它：1套\* 防火墙软件基础级;  3套\* 配套网络安全订阅软件;  3年\* 维保服务; | 1 | 台 |
| 2 | 信息机房整理 | 机房整理、含理线架、配线架、网络跳线、光纤跳线、巡线、打标签、核心交换机配置、网络重新规划、防火墙配置、原配置导入、vlan划分等。 | 1 | 项 |

南通沪蔬通农业发展有限公司

2025年8月15日