1. 详细需求

1需求清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序 号 | 品 名 | 规格型号 | 描 述 | 数 量 | 单 位 |
| 1 | 防火墙入侵防御授权许可 | 天融信NGFW4000-UF | 入侵防御模块及三年攻击规则特征库升级授权许可。 | 1 | 套 |
| 2 | 办公网安全管理系统授权许可 | 网御星云Leadsec-ISM | 100点内网桌面终端运维客户端组建授权许可，提供DMS桌面管理模块（增补）。 | 1 | 套 |

2安全管理系统详细参数

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| **内网终端接入管理** | 终端准入 | 1. 支持基于802.1x协议的网络准入控制。基于802.1x网络准入控制需要同时支持有线网络和无线网络接入。
2. 有线和无线的网络准入控制，至少支持用户，客户端安装，安全状态等多因素绑定认证。
3. 支持Radius Bypass功能
4. 支持安卓、iOS等移动平台无线、支持windows或linux系统自带第三方802.1X准入认证。
5. 支持基于MAC地址的设备免认证。
 |
| 指定关键业务系统和服务器以及网关联动准入 | 1. 能够对尝试访问应用系统和服务器的终端执行应用准入控制，对终端进行身份认证和安全状态检查，保证只有合法的和安全的终端才能访问指定关键业务系统和服务器，对未安装客户端的终端可自定义提示页。
2. 具备专用的准入控制硬件设备，能够实现对于通过局域网和通过广域网、城域网接入的终端，或者访问关键业务系统或服务器的终端，执行基于硬件的准入控制，并实现阻断其接入。支持透明接入和旁路接入。
3. 支持个性化提示信息,可设置管理员姓名、电话以及邮箱；支持提示页面重定向。
 |
| **非法外联** | 多网卡限制与网络非法外联控制 | 1. 能够自动检测和识别存在多网卡的终端，自动选择网卡，禁用其他网卡，并可以对VPN、PPPoE等虚拟网卡例外。
2. 支持探测方式进行非法外联监控，并可以检测到外联时提示用户、断网和告警。
3. 操作系统开机即时进行非法外联检测，防止终端利用系统未启动进行外联传输数据。
 |
| **终端安全基线管理** | windows帐号策略 | 1. 支持对windows帐号策略进行设置，包括禁用禁用、启用管理员帐号，取消帐户锁定，为用户分配所属用户组，禁用或删除无用帐户等。
 |
| Windows服务管理 | 1. 具备Windows服务管理功能。能够禁用或启用终端指定软件服务。有且不限于SNMP服务、ICS服务等。
 |
| Ip协议安全 | 1. 可对终端SYN泛洪水攻击进行保护。可根据SYN洪水攻击的特点进行TCP连接数及连接请求阀值的设置，保证终端不受泛洪攻击。
 |
| 软件安装策略 | 1. 支持软件红名单，要求终端至少安装一个红名单策略里的软件。
2. 支持软件黑名单，禁止终端安装黑名单策略里面的任何软件，针对已安装的终端可进行“提示“、”仅记录“以及“拦截与卸载”三种动作。
3. 支持软件白名单，要求终端安装的软件必须是在白名单策略设置的范围之内，对于非白名单软件可进行“提示”、“仅记录”、“拦截与卸载”三种动作。
 |
| **移动存储管理** | 移动存储设备认证和授权 | 1. 支持对终端接入的移动存储设备提供认证、授权和审计，确保终端使用认证通过的移动储存设备，对数据进行授权共享，彻底杜绝通过移动存储设备的数据非法外泄。
2. 对移动存储认证模式至少要支持专用目录加密和全盘加密二种认证模式，以适应不同使用需求的用户和部门。
3. 支持移动存储设备分散认证，集中授权。
 |
| 移动存储认证例外 | 1. 能够对指定移动存储设备只授权不加密。
2. 能够对指定移动存储进行挂失处理。
 |
| **数据防泄密** | 敏感信息定义 | 1. 可定义涉密文档关键字，当检测到终端内文档中包含有大量涉密关键字时可将其视为涉密文件。
2. 可定义正则表达式，对文件内的银行帐号，电话号码等进行检查，如发现有大量涉密帐号、电话号码等可将其视为涉密文件。
3. 可定义文件指纹，对文件进行涉密评估，当某文档被视为涉密文件后，即使修改其部分内容，也可立即识别出来，避免因为检测md5码而出现涉密漏洞。
4. 可定义文件MD5码，计算出样本文件MD5码，判定终端具有相同MD5码的文件为涉密文件。
5. 可定义文件类型，指定某一种或几种类型的文件为涉密文件。
6. 可定义文件大小，计算样本文件的大小，判定终端具有相同大小的文档为涉密文件。
7. 可定义自动分级分类，对多个样本文件自动进行聚类，提取涉密信息，实现了对某些特定文件的涉密信息的快速定义。
 |
| DLP | 1. 终端DLP，支持基于客户端的数据防泄密功能，支持敏感文件扫描、文件拷贝、剪切板、QQ、邮件、WEB、FTP以及自定义应用程序等方式外发的管控与审计。
2. 网络DLP，联动物理DLP网关，对内部终端通过邮件、QQ、WEB等方式外发的信息进行管控与审计。
3. 存储DLP，支持对linux以及windows server版服务器等不能安装客户端的操作系统进敏感文件扫描。
 |
| **防病毒** | 防病毒 | 1. 支持快速扫描、全屏扫描以及移动设备接入扫描，可自定义扫描工作时间范围。
2. 支持清除、隔离两种病毒处理方式，保证误删除的文件可以被还原。
3. 支持目录与文件的白名单设置来对一些特定的对象进行放开。
4. 提供自动更新和手动更新两种病毒库更新方式，可自定义自动更新病毒库的时间周期。
 |
| **系统体系架构** | 一体化终端安全 | 1. 一体化管理管理服务器：服务器同时支持桌面管理、准入控制、数据防泄漏、终端防病毒等功能模块统一运维管理、策略管控、报表查询等。各功能模块可根据授权信息启用或停用，无需新增或重新部署安装服务器程序
2. 一体化客户端：客户端同时集成桌面管理、准入控制、数据防泄漏、终端防病毒等功能实现。各功能受服务器策略控制可随时启用或或停用，无需新增或重新部署安装客户端程序。
 |
| 客户端端部署与升级 | 1. 客户端部署简单，不依赖传统客户端部署方式，能够通过浏览器在线提示并引导终端用户自助完成客户端安装。
2. 支持客户端升级支持智能升级框架，无需借助单独的升级程序，即可以实现新版本的整体升级，也可以实现同一版本的个别模块单独升级，使软件升级更容易。
3. 支持多个服务器版本和多个客户端版本共存，在大型用户环境下，方便分网段分阶段逐步部署和升级。支持对NAT环境下的终端管理，在NAT环境下的客户端能正常获取策略并执行策略，且能正确上报数据报表。
 |
| 服务器端部署与升级 | 1. 服务器部署简单方便，可以自动检测服务器安装时需要的系统环境组件，并可以通过快速安装方式，一键安装所需要的所有系统服务器组件和数据库，并自动生成客户端安装包。
2. 支持对安装系统的服务器性能状况进行实时监控，可以监控和显示服务器的CPU使用率、内存使用率、系统所在硬盘分区使用率和数据库可用磁盘空间的状况。
3. 可以对数据库所在硬盘空间低于设定的数据库所在硬盘最小剩余空间时，提供告警。
 |
| 平台支持 | 1. 服务器支持在Windows 2008/2012 64位平台上安装。
2. 服务器支持在linux系统上安装。
3. 支持的数据库为MySQL。
4. 客户端支持XP/Windows 7/Win8/Win10的32位操作系统和Windows XP/Windows 7/Win8/Win10的64位操作系统。
 |
| **性能和稳定性要求** | 资源占用 | 系统在计算机运行后，资源占用小，Agent占用的CPU利用率应< 1％，Memory占用大小应<50M。网络性能影响要求：系统运行后，对网络性能基本无影响。 |
| 软件可靠性 | 要求系统产品成熟、稳定和可靠，支持多层服务器架构，支持数据库冗余备份。 |
| 系统自身安全 | 1. 系统具有功能强大的身份认证系统和良好的自身安全性，没有预留的后门，客户端与服务器的通讯需要进行验证，客户端软件卸载需要提供卸载密码。
2. 客户端与服务端通讯，包括日志汇总要求使用加密通道进行通讯。
3. 涉及需要用到到web管理中心，要求使用https协议。
 |
| **资质与案例** | 产品资质 | 1. 计算机信息系统安全专用产品销售许可证，证书显示产品类别应为 “非授权外联监测”产品和“网络版防病毒” 产品。
2. 涉密信息系统产品检测证书，
3. 计算机软件著作权登记证书，
4. 信息技术产品安全评测证书EAL2级
5. 具备公安部计算机信息系统安全产品质量监督检验中心认可的数据防泄密功能(截图证明)；
6. 具备国家计算机病毒应急处理中心计算机病毒防治产品检验实验室认定的合格产品证书
 |