**绿盟产品技术参数**

## 网络安全审计系统

1. 2U机架式硬件设备，含交流冗余电源模块,至少提供1\*USB接口，1\*RJ45串口，1\*GE管理口，6个10/100/1000M电口，至少提供1个接口扩展插槽。支持外部存储设备。检测能力不低于1Gbps。
2. 系统为机架式独立的硬件设备，全内置封闭式结构，具有完全自主知识产权的专用安全操作系统，稳定可靠。需提供相关证明材料。
3. 支持透明串联和旁路部署；采用旁路部署方式对原有网络不造成影响，网络审计产品的故障不影响被审计系统的正常运行；支持透明串联部署时可对异常会话进行阻断。
4. 可支持通过授权扩展基于域名、关键字正则表达式等多种组合的主动内容审计功能，可扫描指定网站，分析网页页面是否含有非法敏感信息。要求提供专利证明。
5. 可支持通过授权扩展网站挂马扫描功能，通过扫描指定网站，分析检测网页是否被挂马，并实时告警响应记录。须提供界面截图。
6. 可支持通过授权扩展无线热点发现功能，能够实时、自动发现办公网络内的无线热点，记录无线热点访问网络时所使用的IP地址、认证用户等信息。需提供界面截图。
7. 可支持通过授权扩展Web安全功能：通过对互联网资源（域名、IP地址、URL等）进行威胁分析和信誉评级，将含有恶意代码的网站例入Web信誉库，达到阻止过滤含有恶意代码的高风险网站，实现对终端用户的安全保护。需提供界面截图。
8. 可支持通过授权扩展移动应用审计，能够识别通过移动热点所访问的移动类应用，例如IM类、社交类、网购类、影音类、资讯类等应用，并记录IP地址、应用名称、访问时间等信息；能够对主流的移动应用进行内容层面的详细审计，主要是对微博、网页言论、网页访问详细记录IP地址、URL地址、访问时间、访问或发布的具体内容等信息。需提供界面截图。
9. 可支持通过授权扩展流量审计功能：支持基于时间、协议、IP地址等组合流量审计策略。支持统计各种应用协议的总流量、上下行流量及TOP10排名；针对协议TOP10排名，可查看使用当前协议的IP及其流量。支持统计各IP的总流量、上下行流量及TOP10排名；针对IP TOP10排名，可查看当前IP使用的协议及其流量。需提供界面截图。
10. 支持审计ORACLE、SQL Server、MY SQL、DB2、Sybase、Informix、Postgresql等各类主流数据库系统；支持实时审计用户对数据库系统所有操作；需提供界面截图。
11. 支持HTTP网页浏览及关键字搜索审计：记录用户网站访问行为包括源IP地址、目的IP地址、访问时间、URL、网页浏览时间等，并提供网页还原功能。需提供界面截图。
12. 支持电子邮件审计：支持SMTP、POP3、WEBMAIL等协议，支持基于邮箱地址、邮件主题、邮件内容、附件名的关键字审计功能；可记录源IP地址、目的IP地址、时间、邮箱地址、邮件主题、邮件内容、邮件附件等信息；邮件附件格式支持DOC、PDF、ZIP、RAR、TXT等；也可以无条件完全记录所有邮件内容和附件。需提供界面截图。
13. 支持基于论坛主题、发帖内容的关键字审计功能；支持基于用户/用户组、时间、关键字等多种组合审计策略，可记录源IP地址、目的IP地址、发帖论坛、发帖人、主题、发帖时间、发帖内容等，并提供内容还原功能。需提供界面截图。
14. 支持文件传输审计：支持HTTP、FTP协议，支持基于用户/用户组、时间、关键字等多种组合审计策略，用户可自定义下载文件类型，对文件上传、下载类型进行审计，可记录日志包括源IP地址、目的IP地址、时间、传输文件名等。需提供界面截图。
15. 支持TELNET、FTP等业务操作进行命令级审计，支持基于IP地址、用户组、时间、关键字等组合审计策略。

TELNET：可记录源IP地址、目的IP地址、帐号、和命令等；FTP：可记录源IP地址、目的IP地址、帐号、命令及上传下载文件名等。需提供界面截图。

1. 支持即时聊天工具审计：可审计QQ、MSN Messenger、ICQ、雅虎通、新浪UC等，支持基于IP地址、用户/用户组、时间、关键字等组合审计策略，可记录日志包括即时通讯号码、上下线时间、文件传输名等。需提供界面截图。
2. 支持用户识别功能，可将终端IP地址与终端用户身份绑定，在审计日志中显示终端用户身份信息。需提供界面截图。
3. 支持用户身份信息智能关联技术，可将用户各种身份信息与其终端IP地址进行智能关联形成用户身份信息库，从而提高事件定位的精确度。需提供界面截图。
4. 支持与学院现有的网站防护系统（web应用防护设备（14-32-P-0165）和网页防篡改软件（13-51-003））、漏洞扫描（17-09-L-0005）设备共同接入一个安全管理平台进行统一管理及攻击告警日志分析，请说明接入方式并提供截图证明。
5. 产品具备公安部颁发的《计算机信息系统安全专用产品销售许可证》（国标增强级）；提供有效证书的复印件
6. 产品具备中国国家信息安全中心认颁发的《中国国家信息安全产品认证证书》（增强级）；提供有效证书的复印件
7. 产品具备中国信息安全测评中心颁发的《信息技术产品安全测评证书》（EAL3+级别），提供有效证书的复印件
8. 产品提供三年原厂软件更新服务、产品保修服务、远程支持服务。

## 安全运维审计系统

1. 2U机架式硬件设备，交流冗余电源，至少提供2\*USB接口，1\*RJ45串口，1\*RJ45管理口，6\*GE千兆电口，2T SATA硬盘，最大图形会话并发400个，最大字符会话并发600个，提供200台设备管理授权。
2. 系统管理采用B/S架构，采用HTTPS方式远程安全管理，无需安装客户端；支持添加静态路由信息，可部署于学校内部复杂的网络环境。须提供界面截图。
3. 具有用户多角色划分功能，如堡垒机系统管理员、运维主管、设备管理员、普通用户、审计管理员、审计员等，对各类角色需要进行细粒度的权限管理，进一步符合国家等保法规要求。须提供界面截图。
4. 支持SSH(V1、V2)、TELNET等字符型远程操作协议；支持RDP、VNC、X11等图形化远程操作协议；支持FTP、SFTP、SCP等文件传输协议；支持Oracle、MS SQL Server、IBM DB2、Sybase、IBM Informix Dynamic Server、PostgreSQL等数据库；支持HTTP、HTTPS操作审计，HTTP/HTTPS协议可以直接代理；
5. 支持主帐号关联：支持以首页中的主账号为基准，支持直接查询该主账号相关的运维信息；支持设备关联：支持以首页中的设备为基准，支持直接查询该设备相关运维信息；支持目标设备分组展示：用户登录堡垒机后可在首页分组显示该用户有权限管理的目标设备，设备分组可按最近访问、最常访问、访问策略、按照个性化配置中的分类等分组显示可登录的设备；并可按全部/工单相关来查询设备。方便学校运维人员快速有效管理自身运维设备情况。须提供界面截图。
6. 支持批量导入/导出/修改用户帐号及目标设备信息，提高学校运维人员运维效率。须提供界面截图。
7. 支持智能扫描方式自动发现网络中的设备，通过IP地址扫描，快速发现指定IP地址范围内的主机、服务器和网络设备，并自动识别启用服务和端口。方便学校管理员快速添加设备，提高工作效率。须提供界面截图。
8. 支持幽灵账号功能，支持主动对从账号进行关联分析，当发现攻击者植入的异常账号时，对相关管理员采取告警、记录及通知等操作；支持孤儿账号功能，能够提供对各从账号的运维使用率的分析功能，当发现使用率异常的从账号，对相关管理员采取告警、记录及通知等操作。有利于学校管理员全面掌握学校设备资产的账号使用情况。须提供界面截图。
9. 支持定期自动修改目标设备密码功能。须提供界面截图。
10. 支持特权密码代填：支持自动填写特权密码，从普通管理模式进入到特权模式。提高学校运维人员运维操作效率。须提供界面截图。
11. 支持设备访问授权：除身份认证之外，需要更高级管理员授权才能对设备进行运维操作；支持命令执行授权：对特定命令的执行需要更高级管理员授权才能执行。防止学校内部出现非授权访问操作事情。须提供界面截图。
12. 支持客户端访问方式访问设备：支持通过SecurCRT等常用的命令行客户端工具登录堡垒机并访问目标设备，并支持会话克隆；支持设备列表可导入到SecrueCRT 中，达到运维设备一键登录；
13. 支持灵活多样的设备登录方式：支持自动登录目标设备、支持半自动登录目标设备、支持手工登录目标设备、支撑密钥登录方式。须提供界面截图。
14. 支持配置向导模式：对配置操作能提供向导式配置界面，尤其是操作步骤比较多，前后有关联的数据库审计配置，方便学校管理员操作配置。须提供界面截图。
15. 可支持和同品牌防火墙联动，远程运维环境下通过防火墙VPN登录内网时只需在登VPN过程中输入堡垒机账号即可直接快速登录到堡垒机运维设备，无需输入VPN账号，再输入堡垒机账号才可运维，可有效提高运维人员运维效率，同时又确保了远程运维的安全性。须提供界面截图。
16. 支持工单系统，支撑运维工单流程，运维人员审批可提前申请工单，审批人员审批自由度大幅提高，不再受审批时间限制，解放运维人员和审批人员，提高工作效率；须提供界面截图。
17. 支持手机APP管理：支持手机APP上进行登录授权审批，金库授权审批，工单审批，方便客户随时随地进行审批工作；支持手机APP上进行运维监控，包括设备信息推送，系统告警监控等；须提供界面截图。
18. 支持与学院现有的网站防护系统（web应用防护设备（14-32-P-0165）和网页防篡改软件（13-51-003））、漏洞扫描（17-09-L-0005）设备共同接入一个安全管理平台进行统一管理及攻击告警日志分析，请说明接入方式并提供截图证明。
19. 产品具备公安部颁发的《计算机信息系统安全专用产品销售许可证》（国标增强级）；提供有效证书的复印件
20. 产品具备中国国家信息安全中心认颁发的《中国国家信息安全产品认证证书》（增强级）；提供有效证书的复印件
21. 产品具备中国信息安全测评中心颁发的《信息技术产品安全测评证书》（EAL3+级别），提供有效证书的复印件
22. 产品获得中国IT运维管理最佳产品奖，并提供证书复印件
23. 产品提供三年原厂软件更新服务、产品保修服务、远程支持服务。

## 网站安全监测系统

1. 2U机架式设备，含交流冗余电源模块，至少提供1个GE管理口，1个RJ45串口，6个100M/1000M自适应以太网电口,1个扩展插槽；可支持200个域名监控。
2. 使用专门的硬件，基于嵌入式安全操作系统，保证系统的工作效率和自身安全性。系统稳定可靠，无需额外存储设备即可运行，系统采用B/S设计架构，并采用SSL加密通信方式，用户可以通过浏览器远程方便的对产品进行管理，产品无需安装任何控制台和第三方数据库。
3. 支持网页挂马监测：可远程对监测的目标站点进行网页挂马监测，其监测频率可以自定义，引擎检测能力至少达到50万页面/每天，高端可达到100万页面/每天，能够将挂马网页以及攻击者最终所使用的恶意代码进行保存，并能够提供木马相关信息及修补意见，同时提供场景文件用于取证。须提供界面截图。
4. 支持暗链监测；须提供界面截图。
5. 支持网站敏感内容监测：可监测网页中出现的赌博、邪教、广告、反政治、反政府、化学、社会、黑客等敏感内容，能够实时告警，并提供场景文件用于取证。须提供界面截图。
6. 因金砖重保及学院招生宣传需要，额外提供针对www.fjmzw.com的7\*24小时远程事件值守服务，包含网站的平稳度监测、DNS解析监测、50页面内的挂马、黑链、篡改、敏感内容监测，需具备7\*24小时大规模网站安全监测服务能力的证明以及网站安全监测服务的案例，提供中标通告、相应网站中标通知网页截图或链接、中标通知书复印件、采购合同复印件。
7. 支持基于组织结构站点资源视图，允许用户从不同维度来关注资产的风险情况。总部可以根据资产树的根节点信息来查看整体风险情况，各单位可以根据自己的管理节点查看单位内各子部门的风险整体情况和各种风险的分布情况。产品提供各个维度的风险趋势数据。须提供界面截图。
8. 支持基于关键页面远程对目标站点进行监测，允许用户自定义设置监测的关键页面，可增、删、变更关键页面，根据设置的关键页面进行网页监测，提供详细功能截图
9. 产品应自带网络工具，支持相关的网络工具ping、traceroute、dig和curl，须提供界面截图。
10. 支持用户发现未知网站，可以通过ip＋端口方式进行查询，快速定位网络中的站点列表
11. 产品提供三年原厂软件更新服务、产品保修服务、远程支持服务。

## 四、集中管理平台-安全中心

1. 软件产品，部署安装在学院内部服务器上，对学院内部主要安全防护设备日志进行采集汇总分析及统一调节管控。可以有效提高学校信息中心运维人员运维工作效率。
2. 支持对学院现有的网站防护系统（web应用防护设备（14-32-P-0165）和网页防篡改软件（13-51-003））、漏洞扫描（17-09-L-0005）及本次采购的安全审计系统等主要安全设备进行统一集中管理维护。可支持安全设备的CPU使用率，内存使用率，磁盘剩余空间，接口流量等设备状态的展示；支持对CPU过载、内存空间不足、设备离线等设备异常的告警；支持对安全设备配置进行自动备份或恢复及手动备份或恢复；支持安全设备的自动升级和手动升级；支持安全设备的拓扑管理
3. 支持对学院现有的网站防护系统（WEB应用防护系统、网页防篡改软件）、远程安全评估系统及本次采购的安全审计系统等主要安全设备的安全日志进行采集分析及告警；具备实时的日志归并功能，可以根据用户需要，按照告警事件的源/目的IP/MAC地址、事件类型等信息，对告警日志执行任意粒度的归并，有效抵御告警风暴；提供基于告警设备、时间、IP地址、事件类型等等条件的日志检索功能，具备日志备份、清除和恢复功能；支持通过IP地址，端口，事件类型，处理动作，时间，危险程度，攻击手段，服务类型，名称，规则编号，关键字等多种方式进行日志查询。
4. 提供丰富的报表功能，支持TopN事件、TopN源地址、TopN目的地址、TopN服务、事件类型分布与趋势、危险程度分类统计与趋势、风险级别统计与趋势以及交叉报表等多种报表模板；为便于分析，还应支持用户自定义报表模版，能够按照用户需求生成各种风格的统计报表。
5. 提供定时自动发送报表功能，支持在指定的时间内将生成的报表以html、word、excel等通用格式通过FTP或邮件发送给指定的管理员，以减少日常维护工作量。
6. 提供智能提醒功能，通过设定提醒阈值，在报表上突出显示以提醒管理员快速发现问题。
7. 具备系统健康状态异常告警机制，能够实时监控系统CPU、内存等关键部件的状态，并在发现异常状况时通过声音、邮件、短信等多种方式及时通知管理员。
8. 产品提供三年原厂软件更新服务、产品保修服务、远程支持服务。