**一、AF-1000-B1810-P9**

1、性能配置

网络层吞吐量：12G，应用层吞吐量：4.4G，防病毒吞吐量：1G，IPS吞吐量：800M，全威胁吞吐量：650M，并发连接数：200万，HTTP新建连接数：8万， SSL VPN最大用户数：130，SSL VPN最大理论加密流量：300M，IPSec最大隧道数：1000，IPSec VPN吞吐量：250M。

硬件参数：规格：1U，内存大小：8G，硬盘容量：64G minisata SSD，电源：单电源，接口：6千兆电口+2千兆光口SFP+4个万兆光口。

2、功能模块

本次采购的下一代防火墙，为保障我单位核心资产，设备需提供L2-L7层各类威胁的检测和防护，产品需能够有效应对传统网络攻击和未知威胁攻击的网络安全产品。

产品需提供：ACL控制、应用识别与流控、入侵防御、僵尸网络检测等功能模块；

产品需提供：WEB应用防护识别库、IPS特征库、僵尸网络与病毒防护库、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。

3、设备维保

提供3年技术支持服务、产品质保服务、软件升级服务。包括：设备的400-远程技术服务、设备的返厂寄修服务、设备的软件升级授权等。

4、核心功能

（1）产品需支持基于地区维度设置流控策略，实现多区域流量批量快速管控功能。所投产品必须提供具备CMA认证的第三方权威机构关于“国家/地区的流量管理”功能项的产品检测报告；

（2）产品需支持勒索病毒检测与防御功能，为保障勒索病毒的防御效果，所投产品必须提供具备CMA认证的第三方权威机构关于“勒索软件通信防护”功能项的产品检测报告；

（3）产品需支持主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危IP。需提供产品功能截图证明，并提供公安部计算机信息系统安全产品质量监督检验中心、中国信息安全测评中心、中华人民共和国国家版权局、公安部信息安全产品检测中心之中任意一家检测机构出具关于“云蜜罐”的证书或检测报告证明功能有效性。

（4）产品需支持与本次采购态势感知功能联动，可通过态势感知自动下发安全策略到防火墙上，对攻击源的联动阻断和一键病毒查杀（需提供截图证明）

**二、NIPS-1000-B1810-P9**

1、性能配置

网络层吞吐量：12Gbps，IPS吞吐量：800M，并发连接数：200万，新建连接数：8万。

硬件参数：规格：1U，内存大小：8G，硬盘容量：64GB minisata SSD，电源：单电源，接口：6千兆电口+2千兆光口SFP+4个万兆光口。

2、功能模块

本次采购入侵防御系统为下一代入侵防御系统，需围绕我单位精确检测，有效防御的核心理念，通过对网络流量的深度解析，可及时准确发现各类非法入侵攻击行为，并执行实时精确阻断，主动而高效的保护我单位的网络安全。产品需要具备全面的恶意软件检测功能。

3、设备维保

提供3年技术支持服务、产品质保服务、软件升级服务。包括：设备的400-远程技术服务、设备的返厂寄修服务、设备的软件升级授权等。

4、核心功能

（1）产品需支持安全策略一体化配置，通过一条策略快速实现不同安全功能的配置，简化策略配置工作；（需提供相关功能截图证明）

（2）产品需支持与本次采购安全态势感知产品实现联动，NIPS支持以标准syslog形式上传到态势感知平台，供态势感知系统进行深度关联分析并对恶意威胁实现联动封锁；（提供截图证明文件）

**三、STA-100-B2100-P9**

1、性能配置

吞吐性能：1Gbps。

硬件参数：规格：1U，内存大小：8G，硬盘容量：64G minisata SSD，电源：单电源，接口：6千兆电口+2千兆光口SFP。

2、功能模块

本次采购的流量探针设备，是我单位建设全网态势感知系统的核心组件，负责对网络流量进行采集和分析，将分析后的数据上传给安全感知系统。

探针需识别应用类型超过1100种，应用识别规则总数超过3000条，具备亿万级别URL识别能力。漏洞利用规则特征库数量在4000条以上；

流量探针需具备：产发现、基础检测功能、元数据采集、监测识别规则库、异常会话检测

深度监测能力、Web应用安全检测能力、元数据采集、僵尸主机检测、违规访问检测、流量记录、抓包分析等功能

3、设备维保

提供3年技术支持服务、产品质保服务、软件升级服务。包括：设备的400-远程技术服务、设备的返厂寄修服务、设备的软件升级授权等。

4、核心功能

（1）探针需支持敏感数据泄密功能检测能力，可自定义敏感信息，支持根据文件类型和敏感关键字进行信息过滤（需提供截图证明）。

（2）探针需支持5种类型日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求（需提供截图证明）。

（3）探针内置URL库、IPS漏洞特征识别库、应用识别库、WEB应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、恶意链接库、白名单库（需提供截图证明）

**四、SIP-1000-F600-P9**

1、性能配置

存储容量：14.4T，在带宽性能1Gbps时存储时长：900天/1Gbps。

硬件参数：内存：4\*16GB，系统盘：1\*240GB，缓存盘：无缓存盘，数据盘：4\*4TB，标配盘位数：8，电源：单电源，接口：4千兆电口。

2、功能模块

本次采购的安全态势感知，定位为全网安全大脑，是一个集检测、可视、响应处置于一体的大数据安全分析平台，可让我单位安全可感知、易运营。采购的设备需以大数据分析为核心，提供威胁情报、UEBA、机器学习、失陷主机检测、大数据关联分析、NTA流量分析、可视化等技术模块，对全网安全进行可视，

设备核心能力：1、海量多源异构的数据分析2、全网资产与脆弱性精细管控3、AI精细发现高级威胁4、全过程溯源分析举证5、事件自动化闭环处置6、安全态势全方位感知7、量化安全运营工作绩效

3、设备维保

提供3年技术支持服务、产品质保服务、软件升级服务。包括：设备的400-远程技术服务、设备的返厂寄修服务、设备的软件升级授权等。

4、核心功能

（1）设备需支持等保合规自检功能，支持已合规基线管控业务安全，实时监测等保差距项和高风险项，避免策略变更导致不合规，有效应对网监不定期抽查和复测场景。（需提供截图证明）

（2）设备需支持利用EBA技术进行资产的行为分析，对这些对象进行持续的学习和行为画像构建，以基线画像的形式检测异于基线的异常行为作为入口点，结合以降维、聚类、决策树为主的计算处理模型发现异常用户/资产行为。共含有不少于27种异常行为学习模型；并支持用户对EBA基线进行自定义调整，优化模型。（需提供截图证明）

（3）设备需支持内置挖矿安全知识库，对常见的挖矿如：Bluehero挖矿蠕虫变种、虚拟货币挖矿、EnMiner挖矿病毒、DDG挖矿病毒、Docker挖矿、DDG挖矿变种、Linux 挖矿木马、ZombieBoy挖矿木马等提供详细的背景介绍、感染现象、详细分析、相关IOC（MD5、C2、URL）、解决方案。（需提供截图证明）

（4）设备需支持与本次采购防火墙、负载均衡联动封锁、访问控制，安全事件支持与终端安全响应系统联动一键查杀、进程取证，支持关闭服务器上的中毒虚拟主机，支持对服务器上中毒的虚拟主机进行快照。

**五、AD-1000-B2200-P9**

1、性能配置

MAD虚拟个数 （MAD一虚多授权）-7.0.21版本：不支持，4层吞吐量（默认网口）：20Gbps，四层并发连接数：8000000，4层新建连接数 CPS：210000，7层新建连接数 RPS：350000。

硬件参数：规格：1U，内存大小：8G，硬盘容量：128G minisata SSD，电源：冗余电源，接口：6千兆电口+4个万兆光口。

2、功能模块

本次招标的负载均衡设备，需具备多数据中心负载均衡、多链路负载均衡、服务器负载均衡的等全方位功能。不仅实现对我单位数据中心、链路以及服务器状态的实时监控，同时根据预设规则，将我单位的访问请求分配给相应的数据中心、链路以及服务器，进而实现数据流的合理分配，使所有的数据中心、链路和服务器都得到充分的利用。同事负载均衡需具备支持IPv6改造能力，需有效协助单位解决“天窗”等问题。

3、设备维保

提供3年技术支持服务、产品质保服务、软件升级服务。包括：设备的400-远程技术服务、设备的返厂寄修服务、设备的软件升级授权等。

4、核心功能

（1）设备需支持链路负载投屏展示，能够分别基于链路监测、应用选路和ISP流量进行投屏展示分析。链路监测展示链路的健康状态、上下行带宽、总带宽、新建连接数、并发连接数和吞吐量；应用选路展示基于应用分类选择相应链路的示意图；ISP展示基于运营商分类选择链路的示意图；（提供设备操作界面截图证明材料）

（2）设备需支持IPv6改造功能，设备能够解决天窗问题，支持一条策略匹配多个外链网站，同时外链和网站子链发生修改时支持自动识别并做主动修改，不允许通过人工解析配置的方式解决天窗问题；

（3）设备需支持基于URL的链路调度功能，内置不少于10万条的国外URL网址库，无需手动导入并支持自动更新，管理员可查看。可根据URL将访问国外网站的请求调度到指定线路；（提供设备操作界面截图证明材料）

**六、AC-1000-B1400-P9**

1、性能配置

网络层吞吐量（大包）：4.8Gb，应用层吞吐量：600Mb，带宽性能：400Mb，IPSEC VPN加密性能（最高性能）：120Mb，支持用户数：3000，准入终端数（默认客户端授权数）：1500，包转发率：72Kpps，每秒新建连接数：8000，最大并发连接数：400000。

硬件参数：规格：1U，内存大小：4G，硬盘容量：64G SSD+960G SSD，电源：单电源，接口：4千兆电口+4千兆光口SFP。

2、功能模块

本次采购的准入设备，需提供包含终端安全检查、非法外联、外设管控、802.1x客户端认证、U盘审计、客户端portal认证、客户端分时访问等功能。

3、设备维保

提供3年技术支持服务、产品质保服务、软件升级服务。包括：设备的400-远程技术服务、设备的返厂寄修服务、设备的软件升级授权等。

4、核心功能

（1）设备需支持与浙江钉同步组织结构，支持对接浙政钉进行身份验证，实现第三方账号授权认证（提供产品界面截图）

（2）设备需支持对于已安装浙政钉2.0的办公PC，通过手机钉钉扫码登录验证，已安装浙政钉2.0的移动终端，通过页面跳转拉起钉钉认证验证（提供产品认证过程截图）

（3）设备需支持20款以上主流杀毒软件的运行情况、软件版本、病毒库更新时间检查，对不满足检查要求的终端可重定向页面修复、弹窗提示、限制权限、禁止上网；

（4）设备需支持非法外联检查，支持自动检查终端是否能PING通互联网地址，对不满足检查要求的终端强制断网，支持向管理员告警，并弹窗提示用户（提供产品功能界面截图）

（5）设备需支持与本次采购的防火墙系统实现认证联动，同时部署产品后，可以实现认证同步机制，实现单点登录；（提供截图证明文件）

**七、NAP-5530-X**

1、性能配置

2.4G最大传输速率≥0.5Gbps，5G最大传输速率≥6Gbps，整机最大传输速率≥6.5Gbps

3.千兆以太网口≥1个，2.5G上行电口1个；并需提供1个RJ-45 Console管理口；USB接口≥1个,可拓展物联网模块使用，可外接U盘

4.单射频接入人数≥512，整机最大接入人数≥1500；

2、功能模块

1.802.11ax 协议，兼容802.11a/b/g/n/ac协议，支持2.4G和5G同时工作；

2.内置智能天线，支持2.4G频段 2\*2条流及 5G(1) 2\*2条流,5G(2) 4\*4条流；

3、设备维保

提供3年技术支持服务、产品质保服务、软件升级服务。包括：设备的400-远程技术服务、设备的返厂寄修服务、设备的软件升级授权等。

4、核心功能

（1）.支持Fat和Fit 两种工作模式，根据网络规划的需要，可以灵活地在Fat和Fit两种工作模式中切换，同时可以根据应用需求，选择工作模式。

（2）.无线AP支持联动安全策略，通过安全策略可以实现对疑似感染病毒或已感染病毒的无线客户端进行识别、监控与隔离等多种方式的处理，提供功能截图证明。

（3）.通过基于特征和协议的射频优化，有效提升无线部署中高密度接入、流媒体传输等场景中的应用加速能力和质量保障效果。其中包含：多用户时间公平调度、混合接入公平、干扰过滤、终端速率管控、频谱导航、组播增强、广播优化、逐包功率控制和智能带宽保障等。

（4）.为保证兼容性与统一管理，要求该无线AP和现有无线控制器兼容，可被现有无线控制器上线管理。

**八、EDR终端检测与响应平台**

1、性能配置

提供500个PC主机授权，产品控制中心最大支持管控客户端数量2000点以上。

2、功能模块

周密防护：系统漏洞扫描，补丁修复管理，终端基线检查，资产盘点，资产主动发现； 全面防护：文件实时监控，勒索诱饵防护，勒索病毒立体防护，勒索攻击对抗； 灵敏检测：恶意文件检测，僵尸网络检测，暴力破解检测； 快速响应：文件急速隔离，终端一键隔离，感染文件修复，病毒处置响应； 简便运维：外设管控，违规外联检测，远程桌面，广告弹窗拦截。MAC系统病毒防护。

3、设备维保

提供3年技术支持服务、产品质保服务、软件升级服务。包括：设备的400-远程技术服务、设备的返厂寄修服务、设备的软件升级授权等。

4、核心功能

（1）支持一键式操作对指定终端/终端组进行合规性检查，包括身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范，对不合规的检查项提供设置建议，并可视化展示终端的基线合规检查结果（提供产品界面截图）

（2）提供基于可信鉴定方式的进程防护方式，通过人工智能自学习机制，自动建立信任进程名单，阻断非可信进程的运行并提供配置指引，同时支持通过模板和手动的方式添加信任进程（提供产品界面截图）

（3）支持与本次采购的上网行为管理联动，管理员在上网行为管理平台界面下发推送指令，对指定网段的终端重定向推送客户端软件，支持自定义重定向的地址；（提供产品界面截图）

**九、WAF-1000-B1810-P9**

1、性能配置

网络层吞吐量：12G，HTTP应用层吞吐量：1Gbps，HTTP新建连接数：80000，HTTP并发连接数：2000000。

硬件参数：规格：1U，内存大小：8G，硬盘容量：64G minisata SSD，电源：单电源，接口：6千兆电口+2千兆光口SFP+4个万兆光口。

2、功能模块

本次采购的WAF，是基于Bot防护、威胁情报、语义分析技术进行漏斗化高效检测Web攻击，满足 OWASP TOP 10 防护需求和符合监管要求。提供贴合业务的多重手段，帮助我单位建设适用业务需求的安全防线，并通过多种智能分析技术和联动组件持续对抗各类新型攻击。实现Web业务应用安全与可靠保障。

3、设备维保

提供3年技术支持服务、产品质保服务、软件升级服务。包括：设备的400-远程技术服务、设备的返厂寄修服务、设备的软件升级授权等。

4、核心功能

（1）产品需原生支持BOT防护功能，可过滤机器人自动化流量，非联动其他组件或产品，并支持用户自定义保护阈值。（需提供产品功能截图证明）

（2）产品需支持自定义BOT防护排除功能，支持通过IP地址白名单、User-Agent、URL前缀的方式排除。（需提供产品功能截图证明）

（3）产品支持超过4900种Web应用防护规则，和超过1200种Web漏洞攻击特征识别规则。（需提供产品功能截图证明）

**十、AC-1000-B2100-P9**

1、性能配置

网络层吞吐量（大包）：10Gb，应用层吞吐量：1.5Gb，带宽性能：1Gb，IPSEC VPN加密性能（最高性能）：200Mb，支持用户数：6000，准入终端数（默认客户端授权数）：1500，包转发率：132Kpps，每秒新建连接数：14000，最大并发连接数：600000。

硬件参数：规格：1U，内存大小：8G，硬盘容量：64G SSD+960G SSD，电源：单电源，接口：6千兆电口+2万兆光口SFP+。

2、功能模块

本次采购的准入设备，需提供包含终端安全检查、非法外联、外设管控、802.1x客户端认证、U盘审计、客户端portal认证、客户端分时访问等功能。

3、设备维保

提供3年技术支持服务、产品质保服务、软件升级服务。包括：设备的400-远程技术服务、设备的返厂寄修服务、设备的软件升级授权等。

4、核心功能

（1）设备需支持与浙江钉同步组织结构，支持对接浙政钉进行身份验证，实现第三方账号授权认证（提供产品界面截图）

（2）设备需支持对于已安装浙政钉2.0的办公PC，通过手机钉钉扫码登录验证，已安装浙政钉2.0的移动终端，通过页面跳转拉起钉钉认证验证（提供产品认证过程截图）

（3）设备需支持20款以上主流杀毒软件的运行情况、软件版本、病毒库更新时间检查，对不满足检查要求的终端可重定向页面修复、弹窗提示、限制权限、禁止上网；

（4）设备需支持非法外联检查，支持自动检查终端是否能PING通互联网地址，对不满足检查要求的终端强制断网，支持向管理员告警，并弹窗提示用户（提供产品功能界面截图）

（5）设备需支持与本次采购的防火墙系统实现认证联动，同时部署产品后，可以实现认证同步机制，实现单点登录；（提供截图证明文件）