|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **采购清单** | | | | | |
| **序号** | **名称** | **品牌** | **规格型号** | **参数要求** | **数量** |
| 43 | AP | 锐捷 | RG-AP720-L | 1.名称： 无线AP 2.规格：按设计 3.其他：其他：满足设计施工图、《泸县监管中心安全技术防范系统项目设计方案（修订稿）》及现行技术、质量验收规范 | 20 |
| 172 | 防火墙 | 锐捷 | RG-WALL 1600-M5100 | 1.整机吞吐量≥5Gbps，应用层吞吐量≥700Mbps，并发连接数≥1,800,000，每秒新建连接数≥50,000CPS 2.机架式硬件设备，本次配置：≥6个千兆电口； 3.支持802.1Q VLAN Trunk、access接口，VLAN三层接口，子接口，支持链路聚合功能；  4.支持静态路由，ECMP等价路由，支持RIPv1/v2，OSPFv2/v3，BGP等动态路由协议； 5.访问控制规则支持数据模拟匹配，输入源目的IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试； 6.支持根据国家/地区来进行地域访问控制； 7.支持IPv4／v6 NAT地址转换，支持源目的地址转换，目的地址转换和双向地址转换，支持针对源IP、目的IP和双向IP连接数控制； 8.支持针对SMTP、POP3、IMAP邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件账号撞库攻击检测等，支持根据邮件附件类型进行文件过滤； 9.支持对信任区域主机外发的异常流量进行检测，如ICMP，UPD，SYN，DNS Flood等DDoS攻击行为； 10.可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则； 11.支持针对网站的漏洞扫描进行防护，能够拦截漏洞扫描设备或软件对网站漏洞的扫描探测； 12.支持Web漏洞扫描功能，可扫描检测网站是否存在SQL注入、XSS、跨站脚本、目录遍历、文件包含、命令执行等脚本漏洞； 13.其他：满足设计施工图、《泸县监管中心安全技术防范系统项目设计方案（修订稿）》及现行技术、质量验收规范 | 1 |
| 173 | 公安网核心交换机 | 锐捷 | S7808C | 1、模块化核心路由交换机，整机主控引擎插槽≥2个，业务插槽≥6个； 2、提供交换容量≥40T，包转发性能≥14000Mpps； 3、具有整机ARP表项≥130K，整机MAC表项≥500K； 4、支持虚拟化功能，实现资源池化，提供权威第三方测试报告； 5、支持DHCP SERVER；支持BGP4/4+、ISISv4/v6、OSPFv2/v3、VRRPv2/v3、支持BFD与RIP/OSPF/BGP联动；支持GR for RIP/OSPF/BGP/ISIS等，支持MPLS PE； 6、支持基础安全保护策略 ，提供交换机防攻击功能，在受攻击情况下，保护系统各种服务的正常运行，以及保持较低的CPU负载，从而保障整个网络的稳定运行； 7、配置单引擎、1+1电源、千兆光口≥48个，万兆光口≥8个，千兆电口≥36个。 8、其他：满足设计施工图、《泸县监管中心安全技术防范系统项目设计方案（修订稿）》及现行技术、质量验收规范 | 1 |
| 174 | 互联网核心交换机 | 锐捷 | RG-S5750C-28SFP4XS-H | 1、硬件规格：三层交换机，配置≥24个千兆SFP接口，≥8个10/100/1000M Base-T(RJ45) 端口；≥2个多业务扩展槽；配置USB接口≥1个；配置一个电源，支持冗余电源； 2、性能要求：交换容量≥2.5Tbps、包转发率≥210Mpps 3、功能要求：支持QinQ、Super Vlan、链路聚合、端口镜像；支持DHCP Server；支持RIPng、OSPF，OSPF v3、BGP，BGP4+、等价路由（ECMP）、等价路由、IGMP v1,v2和v3 Snooping；支持虚拟化技术，将多台交换机虚拟成1台使用；支持G.8032国际标准环网技术；支持BFD与RIP/OSPF/BGP联动；支持GR for RIP/OSPF/BGP/ISIS；支持MPLS VPN、支持PE和MCE功能； 4、扩展要求：支持MAC扩展ACL、专家级ACL（可同时基于VLAN号、以太网类型、MAC地址、IP地址、TCP/UDP端口号、协议类型等灵活组合的硬件ACL）和输出ACL；支持802.1p/DSCP/IP Precedence流量分类和输出QoS；配置支持源/目的IPv6地址、源/目的端口的硬件IPv6 ACL ；支持IPV6+MAC绑定； 5、认证要求：支持802.1x和WEB认证功能，且交换机端口802.1x和WEB认证可以同时开启，不会相互冲突制约； 6、安全要求：支持限制非法报文对CPU的攻击，保护交换机稳定工作；能禁止非法ARP欺骗，防止合法用户的数据被窃取；支持ARP网关欺骗防御功能，能够防止非法用户针对网关的欺骗；支持DHCP抗攻击、ICMP抗攻击、防IP扫描攻击、DoS Protection抗攻击等防御功能；支持防源IP地址欺骗功能 7、其他：满足设计施工图、《泸县监管中心安全技术防范系统项目设计方案（修订稿）》及现行技术、质量验收规范 | 1 |
| 176 | 千兆单模光模块 | 锐捷 | GE-LX-SM1310 | 1.名称：千兆单模光模块 2.规格：千兆 3.类型：模块 4.其他：满足设计施工图、《泸县监管中心安全技术防范系统项目设计方案（修订稿）》及现行技术、质量验收规范 | 68 |
| 177 | 应用安防系统接入交换机 | 锐捷 | RG-S2928G-E V3 | 1、硬件规格：配置≥24口10/100/1000M自适应端口，≥4个100/1000M SFP光口（非复用）；USB接口≥1； 2、性能要求：交换容量≥250G，包转发率≥90Mpps； ★3、功能要求： 满足4K 802.1Q 、protocol VLAN、QINQ、IGMP Snooping v1/v2/v3、堆叠、端口镜像； 4、扩展要求：满足MAC扩展ACL、专家级ACL （可同时基于VLAN号、以太网类型、MAC地址、IP地址、TCP/UDP端口号、协议类型、时间等灵活组合）等；配置满足基于源/目的IPv6地址、源/目的端口的IPv6 ACL ；满足IPV6+MAC绑定； ★5、认证要求：满足802.1x和WEB认证功能，且交换机端口802.1x和WEB认证可以同时开启，不会相互冲突制约； ★6、安全要求：满足限制非法报文对CPU的攻击，保护交换机稳定工作；能禁止非法ARP欺骗，防止合法用户的数据被窃取；满足ARP网关欺骗防御功能，能够防止非法用户针对网关的欺骗；满足DHCP抗攻击、ICMP抗攻击、防IP扫描攻击、DoS Protection抗攻击等防御功能；满足防源IP地址欺骗功能；  ★7、满足基础网络保护策略（NFPP，Network Foundation Protection Policy）技术； ★8、满足满足SNMP V1/V2/V3、RMON、Syslog、USB备份日志及配置等特性来进行网络的日常诊断及维护； 9、其他：满足设计施工图、《泸县监管中心安全技术防范系统项目设计方案（修订稿）》及现行技术、质量验收规范 | 68 |
| 178 | 路由器 | 锐捷 | RSR30-X-SPU10 | 1、硬件规格：业务端口模块插槽数≥2，业务插槽满足扩展接口类型至少包括：E1/CE1、同/异步串口、百兆以太网、FXS/FXO等；配置≥2个千兆以太网三层路由端口，固化千兆和百兆以太端口数≥10个，1个Console口；配置SDRAM≥512M；为便于设备管理，要求路由器面板提供多功能复原键 ，便于紧急情况的设备状态恢复； 2、性能要求：包转发速率≥600Kpps， ★3、功能要求：满足静态路由；满足RIPv1/v2、OSPFv2、BGPv4等路由协议；满足丰富的组播功能；满足ACL、QoS；满足IPSec、GRE、L2TP/PPTP等VPN功能；满足MPLS VPN功能；配置流量分析功能； ★4、链路备份：为了方便路由器进行网络接入，实现在有线网络不易部署的环境下仍能实现网络接入，要求投标产品满足3G功能，并满足3G功能接口模块； 5、其他：满足设计施工图、《泸县监管中心安全技术防范系统项目设计方案（修订稿）》及现行技术、质量验收规范 | 1 |
| 182 | 智能数据分析接入交换机 | 锐捷 | RG-S2910-24GT4XS-E | 1、交换容量：≥336Gbps 2、包转发：≥108Mpps；≥24 个10/100/1000BASE-T 3、以太网端口，≥4 个10G BASE-X SFP+万兆端口 4、其他：满足设计施工图、《泸县监管中心安全技术防范系统项目设计方案（修订稿）》及现行技术、质量验收规范 | 4 |
| 188 | 虚拟应用防火墙 | 锐捷 | RG-WG 1000E-A | ★1、满足DDoS攻击防护、Web应用安全防护、入侵防护功能、满足URL过滤和文件过滤功能、僵尸主机检测、病毒防护、网页篡改防护等功能，保障业务的高安全性 ★2、具备独立的Web应用防护规则库，Web应用防护规则总数在3000条以上 ★3、具备独立的僵尸主机识别特征库，恶意软件识别特征总数在50万条以上 ★4、满足对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能，全面保障业务的安全 ★5、满足对被防护网站是否被挂黑链进行检测； 6、具备对常见网络协议（SSH、FTP、RDP、VNC、Netbios）和数据库（MySQL、Oracle、MSSQL）的弱密码扫描功能，全面保障业务的安全 ★7、可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后满足一键生成防护规则，能够及时的进行安全防护，全面保障业务的安全 ★满足B/S服务漏洞扫描功能，可扫描WEB网站是否存在SQL注入、XSS、跨站脚本、目录遍历、文件包含、命令执行等脚本漏洞，全面保障业务的安全 9、提供安全报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，可以查看到有效攻击行为次数和攻击趋势 10、其他：满足设计施工图、《泸县监管中心安全技术防范系统项目设计方案（修订稿）》及现行技术、质量验收规范 | 1 |