JJ-ZCB20260519

赤峰大学附属医院

NGHIS数据集成建设-网络设备更新项目购销合同

合同编号：

甲方：赤峰大学附属医院

地址：赤峰市松山区新城王府大街42号

乙方：内蒙古慕轩信息技术有限公司

地址：内蒙古自治区呼和浩特市赛罕区锡林南路恩和家园9栋16层11号

根据《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》《中华人民共和国民法典》等相关法律法规 、规范性文件以及赤峰学院附属医院NGHIS数据集成建设-网络设备更新项目(ZLZB-NM-26041016)的成交结果、谈判文件或响应文件等文件的相关内容，甲乙双方经平等协商，就如下合同条款达成一致意见。

一、 甲方向乙方采购的货物基本情况

（一）根据招标谈判文件及成交结果公告，甲方所采购的货物基本情况如下：

产品名称	品牌/生产厂家	规格/型号	单位	数量	成交单价（元）	成交总价（元）
出口防火墙	H3C/新华三技术有限公司	H3C SecPath M9000-CN04-G1	台	2	238000	476000
外网AC控制器	H3C/新华三技术有限公司	H3C WX5540X	台	1	123000	123000
出口上网行为管理	H3C/新华三技术有限公司	H3C SecPath ACG1000-AI-65-G	台	2	138000	276000
域间防火墙	H3C/新华三技术有限公司	H3C SecPath M9000-CN04-G1	台	2	238000	476000
外网日志审计	H3C/新华三技术有限公司	H3C SecCenter CSAP-SA-300-G	台	1	68000	68000
防火墙组件	H3C/新华三技术有限公司	LIS-M9000-IPS-3Y/LIS-M9000-AV-3Y	项	4	55000	220000
合计金额：（小写）：¥1639000.00元　　（大写）：人民币壹佰陆拾叁万玖仟元整						

（二）合同产品技术参数与性能指标等详细内容，见合同附件。

二、乙方交付货物的时间及地点

（一）交付时间：合同签订后 30 天内

（二）交付地点：赤峰大学附属医院指定地点

（三）乙方交付货物代表及联系电话：秦晓 15547845751

（四）甲方接收货物代表及联系电话：杨林森 19947160300

三、乙方交付货物的质量

（一）乙方交付的货物应同时满足：1.符合国家法律法规和规范性文件对货物的质量要求；2.符合甲方谈判文件对货物的质量要求；3.符合乙方在响应文件中或谈判过程中对货物质量作出的书面承诺、声明或保证。上述质量要求作为甲方对乙方货物质量的验收依据。本合同所有货物质保期为验收合格后 3 年，质保期内，如货物质量有问题，乙方负责免费保修、保换。对质量不合格的货物无条件退货，并在甲方指定时间内更换为符合要求的货物。

（二）乙方应根据国家法律法规和规范性文件的规定、谈判文件的相关要求、响应文件及乙方承诺、声明或保证， 向甲方提供相应的货物质量证明文件。

（三）①符合国家相关行业标准及行业质量验收规范，并达到合格标准。符合竞争性谈判文件、响应文件规定内容，如合同与竞争性谈判文件和响应文件中质量标准、有关服务内容、实施服务范围不一致的，以较高、较严标准为准。②乙方所提供的货物必须是全新、未使用的原装产品，且在正常安装、使用和保养条件下，其使用寿命期内各项指标均达到质量要求。

四、乙方交付货物的包装及标识

（一） 乙方交付货物的包装和标识应同时满足：1.符合国家法律法规和规范性文件对产品包装及标识的要求；2.符合甲方谈判文件对货物包装及标识的要求；3.符合乙方在响应文件中对货物包装及标识作出的承诺、声明或保证；4.符合绿色环保、运输及安全性等要求。

（二）货物的包装费用由乙方承担。

五、货物的运输要求

（一）运输、保险及其他相关费用由乙方承担。

六、 甲方对货物的验收

（一）乙方将货物送达至甲方指定的地点，应及时通知甲方。在甲方收到到货通知并在货物到达指定地点后 3 日内，由甲乙双方对货物的数量、规格型号、生产厂家、品牌、外观进行验收，在条件允许的情况下，可以同步对货物质量进行初步验收， 甲乙双方应签署书面验收记录，作为本项目的履行文件留存。

（二）在甲方收到货物 5 日内，如发现质量问题， 甲方应在 5 日内向乙方提出书面异议。乙方在收到甲方关于质量问题的书面异议后， 应当在 5 日内负责解决处理。

（三）乙方提交的货物数量、规格型号及质量不符合本合同要求的，甲方应在验收记录中作出明确记载，保留相关的证据,并有权拒绝接受货物，解除合同且不承担任何法律责任。

（四）验收程序及验收标准

①由甲方组织，乙方配合进行: 验收内容须覆盖功能、性能、安全、兼容性等全维度指标。系统整体上线且在乙方通知安装调试完毕后3日内初步验收。初步验收合格后，进入5天试用期；试用期间发生重大质量问题，修复后试用相应顺延；试用期结束后3日内完成最终验收;

②验收标准：按国家有关规定以及甲方谈判文件的质量要求和技术指标、乙方的响应文件及承诺与本合同约定标准进行验收；甲乙双方如对质量要求和技术指标的约定标准有相互抵触或异议的事项，由甲方在谈判文件与响应文件中按质量要求和技术指标比较优胜的原则确定该项的约定标准进行验收；

③如质量验收合格，双方签署质量验收报告。

七、合同金额

在乙方提供完全符合合同要求的货物的前提下，本合同总金额为1639000元（小写）壹佰陆拾叁万玖仟元整（大写）。

合同金额含税并包含货物从出厂到运至甲方指定地点、甲方验收合格前和质保期期间因产品质量原因所产生的一切费用，包括货物价款、备件、专用工具、安装、调试、检验、技术、培训及技术资料和包装、运输、退换货费用、软件开发费、系统集成费、质保期内软件运维等售后服务费等全部费用，不涉及接口费用，除此外（合同总金额），甲方不再向乙方支付其他任何费用。

八、付款方式

（一）付款方式：

1期：支付比例40%，签订合同并安装验收合格，甲方收到乙方提供的合法有效的发票后支付合同总金额的40%，达到付款条件起30日内，支付合同总金额的40%；

2期：支付比例50%,自验收合格之日起设备正常运行1年，甲方收到乙方提供的合法有效的发票后无息支付合同总金额50%，达到付款条件起30日内，支付合同总金额的50%；

3期：支付比例10%，质保期结束后无任何质量及服务问题，甲方收到乙方提供的合法有效的发票后无息支付合同总金额10%，达到付款条件起30日内，支付合同总金额的10%。

（二）乙方账户信息

乙方名称：内蒙古慕轩信息技术有限公司

开户银行：中国银行股份有限公司呼和浩特市桥靠西街分理处

银行账号：155660024670

九、货物质量保证及售后服务

1、谈判文件对货物质量保证期及售后服务作出明确要求的，适用谈判文件对保证期和售后服务的规定，如乙方在响应文件及谈判过程中对货物质量保证期和售后服务作出更优的承诺、声明或保证的，适用乙方的承诺、声明或保证。

2、质保期为验收合格后 3 年，免费质保期内所有设备提供原厂标准硬件质保与软件升级服务，免费提供故障维修、 部件更换、固件升级、特征库更新服务。免费提供系统软件升级、培训、设计联络、技术服务，优惠提供有关扩建工程的软件扩容服务

3、提供 7×24 小时电话技术支持，远程协助解决问题；重大故障发生时，在15分钟内响应，3小时内到达现场；严重故障发生时，在30分钟内响应，5小时内到达现场；一般故障发生时，在1小时内响应，8小时内到达现场

4、质保期内每季度提供一次现场巡检服务，全面检查设备运行状态、安全策略有效性、性能负载情况，输出巡检报告与优化建议。

5、建立应急响应机制，针对网络攻击、设备故障、业务中断等紧急事件，提供快速应急处置服务，最大限度缩短故障时间。

6、为甲方人员提供现场技术培训，包括设备操作、日常运维、故障排查、安全策略管理等内容，提升甲方自主运维能力。

7、乙方提供本项目设备的主机软件（Comware）的维护性版本（MinorReleases），如软件补丁（BUGFixes）、更新软件（Updates），以及这些软件的配套文档资料。获得软件后，客户将享有与原有软件相同的许可权利。

8、经甲方同意，质保期过后，产品在使用过程中出现的故障和零配件损坏问题，乙方应继续提供免费维修服务，在此期间不收取维护费，如需更换零配件，只收取零配件的成本费，不再收取任何其他费用。 在货物的设计使用寿命期内，乙方保证零部件的正常供应，所有软件终身免费升级。

9、硬件故障时，在维修过程中由乙方提供一台同种工作效果的货物作为备用机，保证甲方不耽误工作。乙方保证所提供的替代硬件设备的性能应等于和高于原产品的性能。

10、项目建成后，质保期间投入固定驻场运维人员1人，确保项目正常运行。

十、知识产权

乙方保证其提供的货物的全部及部分，均不存在任何侵犯第三方知识产权的情形。否则，乙方应向甲方承担违约责任及赔偿由此给甲方造成的名誉及经济损失。

十一、保密条款

乙方应对履行本合同过程中知悉的甲方全部资产信息、财务数据及其他所有涉及个人信息、数据安全、商业信息等未公开信息（以下统称“保密信息”）承担保密义务。未经甲方书面同意，乙方不得向任何第三方泄露保密信息，且仅得为本项目之目的使用，并应采取合理的保护措施。乙方应确保其员工遵守同等保密义务。如乙方违反本条款，应赔偿甲方因此遭受的全部损失，甲方有权单方解除合同并要求乙方退还已收取的全部费用。

乙方应严格遵守《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》及相关法律法规，对履行本合同过程中接触或处理的甲方数据（包括但不限于设备配置信息、运行日志、网络拓扑、管理账号等）履行数据安全保护义务，采取符合行业标准的技术措施和管理措施，防止数据泄露、毁损、篡改或非法使用。乙方仅可将甲方数据用于为本合同项下设备提供质保服务的特定目的，不得用于任何其他用途。

十二、违约条款

（一） 甲方未按合同约定付款，每逾期一天，需向乙方支付逾期支付金额万分之三的违约金；逾期超过 15 天，乙方有权解除合同，同时甲方应向乙方偿付合同总价20%的违约金。

（二） 甲方存在其他违反本合同的行为，应承担相应的违约责任；违约金不足以赔偿乙方损失的， 乙方有权要求甲方赔偿由此造成的经济损失。

（三）乙方未按合同约定送货，每逾期一天，需向甲方支付合同总额万分之三的违约金；逾期超过 15 天，甲方有权解除合同，乙方需返还甲方已支付的全部款项，同时乙方应向甲方偿付合同总价20%的违约金。

（四）乙方交付的货物不符合质量约定或乙方未履行相应的质量保证责任及售后服务义务、或存在侵权行为的， 甲方有权退货，并要求乙方支付合同总金额 20 %的违约金，违约金不足以赔偿甲方损失的， 甲方有权要求乙方赔偿经济损失。

（五）质保期内，乙方逾期服务、或服务不合格时，每逾期或不合格一次，应向甲方支付合同总

金额万分之三的违约金，出现3次及以上的逾期服务、或服务不合格情况，乙方需向甲方支付合同总金额10%作为违约金。同时甲方有权立即单方解除合同，若甲方选择解除合同，乙方须按合同总价的20%支付违约金。

（六）乙方在参与本项目采购活动过程中，如存在提供虚假承诺、证明、串通投标等违法违规行为，除承担相应的行政责任外，甲方有权解除合同，并要求乙方承担合同总金额 20 %的违约金，违约金不足以赔偿甲方损失的，甲方有权要求乙方赔偿经济损失。

（七）乙方违反保密义务的，应承担一切法律责任并赔偿甲方因此遭受的全部损失。乙方保证项目交付成果不含有任何安全隐患，并在项目交付成果使用期内承担全部责任。发生任何由于项目交付成果安全引起的事故时，乙方应赔偿甲方因此所发生的损失。

（八）乙方存在其他违反本合同的行为，应承担相应的违约责任；违约金不足以赔偿甲方损失的，甲方有权要求乙方赔偿经济损失。

十三、不可抗力

1、本合同所称不可抗力是指不能预见、不能避免并不能克服的客观情况，包括但不限于战争、严重火灾、水灾、台风和地震以及其他双方书面同意属于不可抗力的事故。因为不可抗力导致本合同部分或全部不能履行的，可以部分或全部解除本合同，或者根据不可抗力的影响，甲乙双方协商确定适当延长履行期限，或采取其他补救措施。

2、受不可抗力的影响而不能履行的一方应在不可抗力发生后第一时间以书面形式通知另一方，并在不可抗力结束后十个工作日，将有关部门出具的证明文件送达给另一方。根据不可抗力的影响，甲乙双方可以解除或部分解除本合同，或者就本合同的延期履行达成补充协议。

3、因为不可抗力不能履行本合同的，根据不可抗力的影响，可以部分或全部免除履约方的责任，法律另有规定的除外。一方迟延履行后发生不可抗力的，不能免除责任。

十四、争议的解决方式

合同发生纠纷时，双方应协商解决，协商不成，可以采用下列方式解决：

（一）向 甲方所在地 人民法院起诉。

十五、合同保存

本合同经甲、乙双方签字并加盖公章后生效。本合同一式肆份，以中文书写，甲方执叁份，乙方执壹份。合同文本保存期限为从采购结束之日起至少保存十五年。

十六、合同附件

本合同所附下列文件是构成本合同不可分割的组成部分，其内容与本合同具有同等的法律效力：

1、货物清单

2、乙方出具的报价单（函）

3、 成交结果公告及成交通知书

4、 甲方谈判文件

5、乙方响应文件

6、 甲乙双方商定的其他文件

十七、乙方应严格执行国家、自治区制订下发的信息化建设相关数据标准规范要求，不得人为设置数据

壁垒，无条件配合开展与上级相关系统平台进行数据接口对接。

十八、本合同内容如遇国家法律、法规及政策另有规定的，从其规定。本合同未尽事宜，由双方另行签订补充协议，补充协议是本合同的组成部分。

（以下无正文）

甲方名称：（章）

甲方法定代表人或负责人：（签字）

2026 年 8 月 19 日

乙方名称：（章）

乙方法定代表人或负责人：（签字）

2026 年 8 月 14 日

附件

序号	产品名称	技术参数/性能指标
1	出口防火墙	1.1设备整机所使用的全部CPU芯片和交换芯片均为国产化品牌芯片。
		1.2设备采用控制、数据、业务相互解耦分离的全分布式架构，主控引擎、业务引擎、接口单元均采用硬件槽位分离的独立硬件模块， 业务和接口扩容槽位4，主控引擎需采用独立且可热插拔的硬件模块形态，占用专用的硬件槽位，支持1:1冗余备份，保障热插拔无丢包；
		1.3吞吐量130G，新建连接数110W,并发连接数8000W；
		1.4接口模块需采用独立且可热插拔的硬件模块形态，整机要求支持最大100G接口，方便后续扩容；
		1.5设备高可靠性功能页面中能够配置双机状态的多种监控对象，包括接口、VLAN、联动Track项。Track项能够配置监测BFD模块、NQA模块、接口、路由、对象列表。其中NQA探测能够通过ICMP-echo、UDP-jitter、ARP、ICMP-jitter协议报文对网络质量进行探测，可以自定义配置探测次数、探测时间间隔、探测超时时间，记录指定次数的历史测试结果、阈值告警；
		1.6为满足机房散热要求，设备需要严格遵守前后通风设计；
		1.7设备具备可插拔冗余电源模块，电源模块2，可插拔冗余风扇模块，风扇模块2，极端情况下支持单电源、单风扇模块运行，保障极端情况下设备的供电和散热稳定性；
		1.8由于机房空间有限， 设备高度需要严格控制。要求高度2U；
		1.9设备支持防病毒检测功能，支持对IPv4、IPv6的报文进行病毒检测并输出日志；设备本地支持病毒特征库数量600万种；
		1.10支持安全策略冗余分析功能、命中分析功能；支持安全策略应用风险调优功能，支持基于流量对设备的安全策略的安全系数进行评估，对风险的安全策略进行策略优化，自动生成推荐的安全策略；
		1.11支持DNS透明代理功能，可基于负载均衡算法代理内网用户进行DNS请求转发，避免单运营商DNS解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率；
		1.12设备需要支持全面的IPv4/IPv6路由能力；支持配置OSPF实例：可以选择配置OSPFv2或OSPFv3版本协议，配置关联的VRF实例，支持开启不间断路由（NSR）功能；支持配置BGP功能：BGP地址族要求支持配置IPv4单播、IPv4组播、IPv6单播、IPv6组播、MDT、VPNv4、VPNv6、L2VPN等协议；
		1.13设备支持资产发现功能，可对指定IP地址或IP地址范围中的资产进行扫描分析，获取资产的操作系统、MAC地址、厂商等信息，并进一步检测其是否存在开放端口、弱密码等风险因素。支持配置定期自动扫描功能。弱密码扫描功能可覆盖多种协议，支持FTP、SQL Server、HTTP、MySQL、SSH等，扫描模式除内置常规密码字典外，支持配置自定义密码字典，方便客户排查特定场景的弱密码；
		1.14配置双主控双风扇，配置4个100G光接口，16个万兆光接口，配置1块独立防火墙板卡，配置1600W冗余电源。
2	外网AC控制器	2.1满足常规AP最大数量3584；
		2.2产品数据转发性能60Gbps；
		2.3提供8个千兆GE端口，8个SFP+端口，以及2个QSFP+端口；
		2.4为了确保无线体验，所提供的产品应能够识别常见的无线网络问题，如弱信号接入和接入点间频繁切换等。并可以提供问题的分布趋势图、受影响的具体设备、相关的接入点,以及该接入点发生此类问题的统计数据；

		2.5支持MAC地址认证、802.1x认证、Portal认证、MAC+Portal混合认证；
		2.6支持AC内漫游，支持跨AC间漫游，支持跨VLAN的三层漫游；
		2.7为了保证网络管理员能够实时清楚网络状态，所投产品需要在网络发生异常时能够推送告警信息给网络管理员，推送的方式包括但不限于短信、微信、邮件等；
		2.8 CAPWAP隧道同时支持IPv4和IPv6双栈，用戶可以使用IPv4或IPv6作为用戶地址和隧道地址，二者可以灵活组合；
		2.9满足1+1热备，对外呈现一个IP地址，简化网络拓扑；对外统一管理界面，在主板上创建的配置可以自动同步到备板，简化运维；
		2.10为保障IPV4网络过渡到IPV6网络的安全性，设备满足IPV6 SAVI功能；
		2.11 AC满足专门针对CPU的保护机制， 能够针对发往CPU处理的报文，进行流量控制， 保护无线控制器在各种环境下稳定工作；
		2.12为保障IPV4网络过渡到IPV6网络的安全性，设备满足IPV6 SAVI功能；
		2.13支持在集群热备组网下，通过升级可以实现AC在升级时业务不中断，AP和终端不掉线,终端可持续ping通网关；
		2.14配置2个万兆模块， 2*650W冗余电源， 冗余风扇；
		2.15为保证院内无线设备统一管理，能够与现有内网无线控制器共享AP管理授权。
3	出口上网行为管理	3.1机架式独立硬件设备，系统硬件为全内置封闭式结构， 稳定可靠，加电即可运行，启动过程无须人工干预；
		3.2内置6个千兆电Bypass模块；在设备流量异常时，可自动切换到Bypass状态，当设备恢复时，可自动切换回工作状态；双电源；
		3.3吞吐量60Gbps，并发连接数2500W，新建连接数40W， 内存32G， CPU8核，硬盘4Tb；
		3.4支持10M/100M/1000M自适应电接口数量8个，支持千兆SFP光接口数量4个，万兆接口总数4个，可扩展插槽3；接口无路由/交换/LAN/WAN等固化区分，均可作为二三层接口使用，支持多桥组部署；
		3.5支持DDNS功能；支持花生壳DDNS客戶端以及域名IP绑定功能；
		3.6支持VRF功能，不同vrf下的接口可以配置相同的ip地址，通过VRF有效隔离不同网络；
		3.7支持自定义的静态手工模式和LACP模式的链路聚合， 实现线路带宽叠加；
		3.8支持首页大屏展示安全等级、效率等级、管控等级、合规等级、在线用戶 、审计日志类别及数量、流量分析、违规用戶信息（策略违规、共享违规、限额违规）等， 支持显示系统信息、实时流量、系统资源、接口状态、用戶TOP流量、应用TOP流量统计、系统日志信息、审计日志信息等；
		3.9支持用户虚拟身份画像，以时间轴的形怯展示用户上网行为轨迹；支持单用户全天行为分析报表，一个界面同时展示用户名、用户组、在线时长、虚拟身份（如QQ号码、微博账号等）、日志关联情况、全天流量使用分布、 网站访问类别分布、全天关键网络行为轴等信息， 支持对单用户进行网站访问质量检测；
		3.10支持图形化展示策略分析概况，问题策略分布，总体策略宽松度评分,支持策略分组，进行区分化管理和运维；
		3.11 IPSec VPN支持第三方对接和快速配置，自有设备对接时加密算法等参数无需配置，自动生成，仅需配置保护子网、共享密钥、IP地址；
		3.12支持智能和快速识别模怯配置支持应用模型识别技术，可定义识别模怯的宽松程度，有效和准确识别网络应用；检测引擎支持智能、快速和关闭识别模怯；
		3.13支持流控策略区分超级管理员和普通管理员；线路和一级通道仅支持超级管理员创建，超级管理员可将一级通道指定分配给普通管理员；
		3.14支持与第三方DDI平台联动，同步DDI全部用用户组织架构与用户名，并针对

		用户名做上网行为管理；
		3.15认证白名单，支持独立界面配置认证策略白名单和认证方怯白名单，认证策略白名单支持配置ip和域名。认证方怯白名单支持微信、企业微信、钉钉认证仅放通相关认证流量,其他流量全部阻断，保障安全性， 并支持手动更改配置；
		3.16支持1000+规则库，产品分类支持AQL注入攻击、XSS攻击、恶意扫描及爬虫、WebS hell攻击、会话劫持、敏感信息泄露、CMS漏洞防护等类型；
		3.17配置4个万兆多模光模块， 配置3年特征库升级授权， 2*350W电源模块。
4	域间防火墙	4.1设备整机所使用的全部CPU芯片和交换芯片均为国产化品牌芯片；
		4.2设备采用控制、数据、业务相互解耦分离的全分布怯架构， 主控引擎、业务引擎、接口单元均采用硬件槽位分离的独立硬件模块， 业务和接口扩容槽位4,主控引擎需采用独立且可热插拔的硬件模块形态， 占用专用的硬件槽位， 支持1:1冗余备份，保障热插拔无丢包；
		4.3吞吐量130G ， 新建连接数110W,并发连接数8000W；
		4.4接口模块需采用独立且可热插拔的硬件模块形态， 整机要求支持最大100G接口，方便后续扩容；
		4.5设备高可靠性功能页面中能够配置双机状态的多种监控对象，包括接口、VLAN、联动Track项。Track项能够配置监测BFD模块、 NQA模块、接口 、路由、对象列表。其中NQA探测能够通过ICMP-echo、UDP-jitter、ARP、 ICMP-jitter协议报文对网络质量进行探测， 可以自定义配置探测次数、探测时间间隔、探测超时时间， 记录指定次数的历史测试结果、阈值告警；
		4.6为满足机房散热要求，设备需要严格遵守前后通风设计；
		4.7设备具备可插拔冗余电源模块，电源模块2，可插拔冗余风扇模块，风扇模块2，极端情况下支持单电源、单风扇模块运行，保障极端情况下设备的供电和散热稳定性；
		4.8由于机房空间有限，设备高度需要严格控制。要求高度2U；
		4.9设备支持防病毒检测功能，支持对IPv4、IPv6的报文进行病毒检测并输出日志；设备本地支持病毒特征库数量600万种；
		4.10支持安全策略冗余分析功能、命中分析功能；支持安全策略应用风险调优功能，支持基于流量对设备的安全策略的安全系数进行评估，对风险的安全策略进行策略优化，自动生成推荐的安全策略；
		4.11支持DNS透明代理功能，可基于负载均衡算法代理内网用戶进行DNS请求转发，避免单运营商DNS解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率；
		4.12设备支持全面的IPv4/ IPv6路由能力；支持配置OSPF实例：可以选择配置OSPFv 2或OSPFv3版本协议， 配置关联的VRF实例，支持开启不间断路由（NSR）功能；支持配置BGP功能：BGP地址族要求支持配置IPv4单播、 IPv4组播、 IPv6单播、 IPv6组播、 MDT、VPNv4、VPNv6、 L2VPN等协议；
		4.13设备支持资产发现功能， 可对指定IP地址或IP地址范围中的资产进行扫描分析， 获取资产的操作系统、 MAC地址、厂商等信息，并进一步检测其是否存在开放端口 、弱密码等风险因素。支持配置定期自动扫描功能。弱密码扫描功能可覆盖多种协议， 支持FTP、SQL Server、 HTTP、MySQL、SSH等， 扫描模式除内置常规密码字典外， 需支持配置自定义密码字典， 方便客戶排查特定场景的弱密码；
		4.14配置双主控双风扇，配置4个100G光接口，16个万兆光接口，配置1块独立防火墙板卡， 配置1600W冗余电源。
5	外网日志审计	5.1接入性能：配置128日志源，最大扩容至512个日志源；
		5.2日志接入处理性能： 5000EPS；
		5.3国产芯片、国产操作系统；
		5.4配置≥8个千兆电口，4个千兆光口，4个万兆光口；CPU≥8核2.8GHz，内存≥32G，硬盘≥128G+4T,冗余电源， 自带液晶屏；

		5.5支持网络设备、安全设备、操作系统、服务器、 中间件、数据库等35大类、500+种设备的采集；
		5.6支持SYSLOG协议、 HTTP/HTTPS、SFlow、Netstream、SNMP等被动采集， FTP 、 SFTP、JDBC\ODBC、WMI、 Kafka、Agent终端采集、数据库主动采集等多样化日志接入；
		5.7支持在日志查询过滤条件中选择性针对关注的字段结果进行统计， 针对统计的结果进行排序， 并支持快捷添加为过滤条件；
		5.8支持IPV4/IPV6类型日志、 IPV4/IPV6组网架构下的日志采集和范式化处理；
		5.9支持NAT溯源取证专题功能模块， 查找内网资产真实IP， 并能够查看关联的日志信息,支持针对NAT转换后源IP、 NAT转换后源端口 、 目的IP、 目的端口 、事件发生时间、 日志时间范围进行溯源， 针对溯源结果以溯源业务链的方式呈现）；
		5.10支持按照日志等级（调试、通知、重要、警告、错误、严重、故障、不可用及其他信息 ） 列表展示日志范式化分析结果、下钻支持日志详情；
		5.11支持用戶自定义统计效果， 可选择饼状分布图、折线趋势图、柱状比较图 ；
		5.12支持按照日报、周报、月报的周期自定义报表任务， 支持自定义选择报表模板、任务执行时间、报表格式、报表保留时间；
		5.13支持基于SM2非对称加密算法、SM3密码杂凑算法等国密算法对日志进行签名验签操作,以满足日志完整性校验要求；
		5.14支持自定义告警策略，设置探测间隔、告警类型、日志源、关联规则、告警方式信息；
		5.15配置2个万兆光模块；配置冗余电源350W。
6	防火墙组件	6.1提供IPS入侵防御特征库升级服务，授权有效期3 年， 与防火墙硬件型号完全匹配，激活后可正常启用入侵防御能力；
		6.2入侵攻击特征规则数20000条，覆盖漏洞利用、蠕虫、木马、DDoS、扫描、 网络钓鱼、间谍软件等攻击类型， 支持按风险等级、协议类型分类管理；
		6.3支持特征库自动/手动定时升级，升级过程不中断业务转发；
		6.4支持对 IPv4/IPv6 双栈流量入侵检测，支持对 HTTP、FTP、SMTP 等主流应用层协议攻击防护，支持自定义 IPS 防护策略模板；
		6.5提供 AV 防病毒特征库升级服务，授权有效期3 年， 与防火墙硬件型号完全匹配， 激活后可正常启用病毒查杀能力；
		6.6病毒特征库数量600 万条， 覆盖病毒、木马、后门、蠕虫、勒索软件、广告软件等恶意程序， 支持加壳与变种病毒检测；
		6.7支持对 HTTP、FTP、SMTP等主流协议流量进行病毒检测与阻断， 支持文件解压查杀 ；
		6.8支持病毒库自动 / 手动升级， 支持特征库版本查询与日志审计， 升级频率满足每日威胁情报更新；
		6.9服务期内提供 7×24 小时原厂技术支持， 保障特征库持续有效更新；
		6.10提供防火墙配套万兆模块8个。