三亚市公安局信息系统安全建设

招标文件

项目编号：HNXHZB2018-046

信华招标

采　购　人：三亚市公安局

招标代理机构：海南信华招标代理有限公司

二〇一八年十月

三亚市公安局信息系统安全建设

招标文件

项目编号：HNXHZB2018-046

信华招标

采　　购　　人：三亚市公安局

招标代理机构：海南信华招标代理有限公司

二〇一八年十月

目　　录

第一章 投标邀请函

海南信华招标代理有限公司受三亚市公安局委托，对三亚市公安局信息系统安全建设进行公开招标 ，现邀请国内合格的供应或制造商来参加密封投标。

1、招标编号： HNXHZB2018-046

2、招标项目及范围：三亚市公安局信息系统安全建设（2 个包）。

1、项目名称：三亚市公安局信息系统安全建设

包号：A 包：软硬件设备及材料采购

B 包：等级保护测评及信息安全服务

2、项目编号：HNXHZB2018-046

3、用途：三亚市公安局工作需要

4、技术要求：见“用户需求书”

5、本项目预算为：A 包：¥3,122,856.00 元、B 包：¥560,000.00 元，超过采购预算金额的投标文件按无效投标处理。（A 包：¥3,122,856.00 元、B 包：¥560,000.00 元为最高限价）

3、供应商资格要求

A 包：

1、在中华人民共和国注册，具有独立承担民事责任能力的法人（需提供营业执照、税务登记证、组织机构代码证复印件，或者三证合一复印件）；

2、具有良好的商业信誉和健全的财务会计制度（需提供近一年内任意三个月的纳税证明或者会计师事务所出具的近一个年度财务审计报告）；

3、有依法缴纳社会保障资金的良好记录（需提供近一年内任意三个月的社保缴费记录复印件）；

4、参加政府采购活动前三年内，在经营活动中没有重大违法记录（提供声明函）；

5、购买本项目招标文件并缴纳投标保证金。

6、本包不接受联合体投标。

B 包：

1、在中华人民共和国注册，具有独立承担民事责任能力的法人（需提供营业执照、税务登记证、组织机构代码证复印件，或者三证合一复印件）；

2、具有良好的商业信誉和健全的财务会计制度（需提供近一年内任意三个月的纳税证明或者会计师事务所出具的近一个年度财务审计报告）；

3、有依法缴纳社会保障资金的良好记录（需提供近一年内任意三个月的社保缴费记录复印件）；

4、参加政府采购活动前三年内，在经营活动中没有重大违法记录（提供声明函）；

5、购买本项目招标文件并缴纳投标保证金。

6、本包不接受联合体投标。

4、招标文件的获取

4.1、发售标书时间：2018-12-24　　00:00:00— 2018-12-29　　00:00:00。

4.2、下载标书地址：http://zw.hainan.gov.cn/htms/login!register.do 。

4.3、标书售价

• 项目自身： 招标文件每套售价 200.00 元/包； 投标保证金的金额：A 包 30000.00 元;B 包 5000.00 元。

4.4、投标人提问截止时间：2019-1-7　　17:00:00（北京时间）。

5、投标文件和保证金的递交

5.1、投标文件递交截止时间：2019-1-16　　15:30:00（北京时间）。

5.2、投标文件递交地点(地址)为：三亚市政务中心公共资源交易大厅第 1 开标室 。

5.3、开标时间： 报名成功后于系统的项目信息中查看。

5.4、开标地点： 报名成功后于系统的项目信息中查看。

5.5、保证金到账截止日期： 2019-1-16　15:30:00（北京时间）， 投标保证金的形式：网上支付， 支付地址为：http://zw.hainan.gov.cn/htms/login!register.do。

5.6、公告发布媒介：中国海南政府采购网:http://www.ccgp-hainan.gov.cn、全国公共资源交易平台（海南省）• 三亚市：http://zw.hainan.gov.cn/ggzy/syggzy/、

全国公共资源交易平台（海南省）：http://zw.hainan.gov.cn/ggzy/、中国政府采购网:http://www.ccgp.gov.cn。

6、其他

1、必须在海南省人民政府政务服务中心企业信息管理系统（http://zw.hainan.gov.cn/ggzy）中注册并备案通过，然后登陆电子招投标系统（http://zw.hainan.gov.cn/htms/login!register.do）下载、购买电子版的招标文件；

2、非电子标（标书后缀名不是.GZBS）：必须使用电子签章工具（在http://zw.hainan.gov.cn/ggzy/下载签章工具）对 PDF 格式的电子投标文件进行盖章(使用 WinRAR 对 PDF 格式的标书加密压缩)；

3、投标截止日期前，必须在网上上传电子投标书——（电子标：投标书为 GTBS 格式；非电子标：投标书需上传 PDF 加密压缩的 rar 格式）；

4、开标现场按招标文件要求提交纸质版投标文件，同时提供 wrod 和 PDF 格式电子版投标文件各一份（其中 PDF 格式需加盖公章或电子公章，光盘或 U 盘均可），投标时报价一览表须再单独用信封密封一份，否则将拒收报价文件。

5、公告期限：2018 年 12 月 24 日 00:00:00 至 2018 年 12 月 29 日 00:00:00

6、招标文件每套售价 200 元/包(现场缴纳)；

7、招标代理机构联系方式

1、代理机构：海南信华招标代理有限公司

2、地址：海口市龙昆南路汇隆广场 1 单元 1106 室

3、邮政编码:572000

4、项目联系人：张大为

5、联系电话：15248942316

8、采购人联系方式

1、采购人：三亚市公安局

2、地址：三亚市迎宾路 362 号

3、联系人：吴奇聪

4、联系电话：13876386547

海南信华招标代理有限公司

第二章 投标人须知

一、总则

1. 名词解释

1.1 项目名称：三亚市公安局信息系统安全建设

1.2 采购人：三亚市公安局

1.3 招标代理机构：海南信华招标代理有限公司

1.4 投标人：已从海南信华招标代理有限公司购买招标文件并向海南信华招标代理有限公司提交投标文件的投标人。

2. 适用范围

本招标文件仅适用于海南信华招标代理有限公司组织的本次投标活动。

3. 合格的投标人

3.1 凡有能力按照本招标文件规定的要求交付货物和服务的投标单位均为合格的投标人。

3.2 投标人参加本次招标活动应当符合《中华人民共和国政府采购法》第二十二条的规定，并具备本招标文件第一章的“投标人资格要求”规定的条件。

3.3 本项目如为信息系统采购项目，供应商不得为该整体项目或其中分项目前期工作提供过设计、编制、管理等服务的法人及附属单位。

3.4 单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。除单一来源采购项目外，为项目提供整体设计、规范编制或者项目管理，监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。

3.5 投标人在本项目招标公告前三年内被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单，以及存在其他不符合《中华人民共和国政府采购法》第二十二条规定条件的情况的投标人不得参与投标。

两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购活动的，联合体任意成员存在不良信用记录的，视同联合体存在不良信用记录。

3.6　本章 3.5 款的信用记录以“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）、信用三亚（http://xysy.sanya.gov.cn/）上公布的信用记录为准。

4.联合体投标

4.1 联合投标时，联合体各方之间应当签订共同投标协议，明确约定联合体各方承担的工作和相应的责任，并将共同投标协议连同投标文件一并提交。联合体各方签订共同投标协议后，不得再以自己名义单独在同一项目中投标，也不得组成新的联合体参加同一项目投标。联合体中至少有一方完全满足投标人资格要求的特定条件。

4.2 本项目不接受联合体投标。

5．投标费用和解释权

5.1 无论招标投标过程中的做法和结果如何，投标人均自行承担所有与参加投标有关的全部费用。

5.1 本招标文件由海南信华招标代理有限公司负责解释。

二、招标文件

6．招标文件的组成

6.1 招标文件由六部分组成，包括：

第一章　投标邀请书

第二章　投标人须知

第三章　用户需求书

第四章　评审方法

第五章　合同条款

第六章　投标文件内容和格式

请仔细检查招标文件是否齐全，如有缺漏，请立即与招标代理机构联系解决。

6.2 投标人必须详阅招标文件的所有条款、文件及表格格式。投标人若未按招标文件的要求和规范编制、提交招标文件，将有可能导致招标文件被拒绝接受，所造成的负面后果由投标人负责。

7．招标文件的澄清、修改或补充

7.1 投标人在收到招标文件后，若有疑问需要澄清，应及时以书面形式向海南信华招标代理有限公司提出，海南信华招标代理有限公司将以书面形式进行答复，同时海南信华招标代理有限公司有权将答复内容分发给所有购买了此招标文件的投标人。

7.2 海南信华招标代理有限公司可以指定媒体上公告的方式修改/补充招标文件。修改/补充通知作为招标文件的组成部分，对投标人起同等约束作用。

7.3 当招标文件与修改/补充公告的内容相互矛盾时，以海南信华招标代理有限公司最后发出的修改/补充公告为准。

7.4 为使投标人有足够的时间按招标文件的修改/补充要求修正投标文件，海南信华招标代理有限公司有权决定推迟投标截止日期和开标时间。

三、投标文件

8．投标文件的组成

8.1 投标文件应按“第六章 投标文件内容和格式”要求编制。

8.2 若投标人未按招标文件的要求提供资料，或未对招标文件做出实质性响应，将可能导致投标文件被视为无效。

9．投标报价

9.1 报价均须以人民币为计算单位。

9.2 报价应包括全部货物、服务的价格及相关税费、运输到指定地点的装运费用（如有）、安装调试（如有）、培训（如有）、售后服务等其它有关的所有费用。

9.3 投标人应按开标一览表的要求报价，不能提供有选择的报价。

9.4 中标候选人的报价如超过预算且采购人不能支付的，采购人有权拒绝而递选下一个顺位的候选人。

10．投标保证金

10.1 投标保证金是参加本项目投标的必要条件，保证金支付要求见第一章。为避免资金在途不能及时到账造成投标无效，建议投标人提前在投标截止时间一个工作日前办理保证金支付手续。

10.2 若投标人不按规定提交投标保证金，其投标文件将被拒绝接受。

10.3 投标保证金的退还

10.3.1 中标人的投标保证金在其与采购人签订了合同后五个工作日内无息退还。

10.3.2 落标的投标人的投标保证金将在海南信华招标代理有限公司发出中标通知书五个工作日内无息退还。

10.3.3 如投标保证金为海南信华招标代理有限公司收取，则中标结果公告期满后，投标人应把投标保证金退还申请函（必须注明项目名称、金额以及退还的银行账户）传真到 0898-65783734，以便办理投标保证金退还手续。

1）如投标保证金为海南省公共资源交易服务中心、三沙市公共资源交易服务中心、儋州市公共资源交易服务中心收取，未中标方的投标保证金待中标结果公示期满后由代理机构工作人员办理退款，中标方的投标保证金待和采购单位签订合同并送达代理机构提交电子招投标系统后由代理机构工作人员操作办理退款。

如投标保证金已缴纳但未在电子招投标系统中提交关联，则和投标保证金收取单位联系办理退款手续，退款时请提供如下材料（加盖公章）：(1)退款申请书；(2)法人代表及经办人身份证（复印件）；(3)授权委托书；(4)电汇单（复印件）；(5)开户许可证（复印件）。

2）三亚市人民政府政务服务中心收取，未成交的供应商，保证金将在成交通知书发出之日起 5 个工作日内，由招标代理机构在全国公共资源交易平台（海南省）·三亚市系统中操作退还保证金。成交的供应商，保证金将在采购合同签署后 5 个工作日内，由招标代理机构在全国公共资源交易平台（海南省）·三亚市系统中操作退还保证金。

如投标保证金已缴纳但未在电子招投标系统中提交关联，则和投标保证金收取单位联系办理退款手续，退款时请提供如下材料（加盖公章）：(1)退款申请书；(2)法人代表及经办人身份证（复印件）；(3)授权委托书；(4)电汇单（复印件）；(5)开户许可证（复印件）。

3）如投标保证金为海口市公共资源交易中心收取，未中标方的投标保证金待中标通知书发放后由海口市公共资源交易中心相关工作人员操作办理退款。中标方的投标保证金待合同原件及电子版合同送达海口市公共资源交易中心后由海口市公共资源交易中心相关工作人员操作办理退款。

联系电话：

海南省公共资源交易服务中心：0898-66529867

三沙市公共资源交易服务中心：0898-66860296

儋州市公共资源交易服务中心：0898-23335693

三亚市人民政府政务服务中心：0898-38860835

海口市公共资源交易服务中心：0898-65250512

10.4 发生下列情况之一，投标保证金将不予退还：

（1）投标人在投标有效期内撤回其投标文件的；

（2）投标人不按本章规定签订合同；

（3）投标人提供虚假材料谋取中标、成交的；

（4）与采购人、其它投标人或者招标代理机构恶意串通的；

（5）向采购人、招标代理机构、评标委员会成员行贿或者提供其他不正当利益的；

11．投标有效期

11.1 投标有效期：60 日历天。

11.2 在特殊情况下，海南信华招标代理有限公司可于投标有效期满之前，征得投标人同意延长投标有效期，要求与答复均应以书面形式进行。投标人可以拒绝接受这一要求而放弃投标，投标保证金将尽快无息退还。同意这一要求的投标人，无需也不允许修改其投标文件，但须相应延长投标保证金的有效期。受投标有效期制约的所有权利和义务均应延长至新的有效期。

12．投标文件的数量、签署及形式

12.1 投标文件数量：**正本壹份，副本肆份**。投标文件须固定装订。

12.2 投标文件须按投标文件的要求执行，每份投标文件均须在封面上清楚标明“正本”或“副本”字样，“正本”和“副本”具有同等的法律效力；“正本”和“副本”之间如有差异，以正本为准。

12.3 投标文件正本中，文字材料需打印或用不褪色墨水书写。投标文件的正本须经法人代表或授权代表签署和加盖投标人公章。

12.4 投标文件不得涂改和增删，如要修改错漏处，修改处必须由法人代表或授权代表签名、或盖公章。

四、投标文件的递交

13．投标文件的密封及标记

13.1 投标人应将投标文件正本和所有副本分别密封在两个报价专用袋（箱）中（正本一包，副本一包），并在报价专用袋（箱）上标明“正本”、“副本”字样，封口处应加盖骑缝章。封皮上均应写明：

致：海南信华招标代理有限公司

项目名称：三亚市公安局信息系统安全建设

项目编号：HNXHZB2018-046（如分包则注明包号）

注明：“请勿在开标时间之前启封”

投标单位名称、联系人姓名和电话

13.2 投标文件未按上述规定书写标记和密封者，海南信华招标代理有限公司不对投标文件被错放或先期启封负责。

14. 投标截止时间

14.1 投标人须在投标截止时间前将投标文件送达招标代理机构规定的地点。

14.2 若招标代理机构推迟了投标截止时间，应以公告的形式通知所有投标人。在这种情况下，招标代理机构、采购人和投标人的权利和义务均应以新的截止时间为准。

14.3 在投标截止时间后递交的投标文件，海南信华招标代理有限公司将拒绝接受。

14.4 在规定时间内提交投标文件的投标人不足 3 家，不得开标，本次招标失败。

五、开标及评标

15. 开标

15.1 海南信华招标代理有限公司按投标文件第一章规定的时间和地点进行开标，采购人代表、招标代理机构有关工作人员参加。投标人可以委派授权代表参加开标活动，参加开标的代表须持本人身份证件签名报到以证明其出席，评标委员会成员（包括采购人委派的用户评委）不能参加开标活动。

投标人未参加开标的，视同认可开标结果。

15.2 开标时，投标人代表将查验投标文件密封情况，确认无误后拆封唱标，公布每份投标文件中“开标一览表”的内容，以及海南信华招标代理有限公司认为合适的其他内容，海南信华招标代理有限公司将作开标记录。

15.3 若投标文件未密封，海南信华招标代理有限公司将拒绝接受该投标人的投标文件。

16. 评标委员会

评标委员会由技术、经济等方面的专家和用户代表组成，其中技术、经济等方面的专家随机抽取，且人数不得少于总数的 2/3。该评标委员会独立工作，负责评审所有投标文件并确定中标侯选人。

17.关于政策性加分

17.1 所投分包(如不分包则指本项目)的所有投标产品进入当期节能清单的，其评标价=投标报价*（2%）；投标人所投产品满足此规定的，必须提供声明函并提供相关证明文件。

17.2 所投分包(如不分包则指本项目)的所有投标产品进入当期环保清单的，其评标价=投标报价*（1%）；投标人所投产品满足此规定的，必须提供声明函并提供相关证明文件。

17.3 投标人为小型和微型企业（含联合体）的情况：

17.3.1 中小企业的认定标准：

1）提供本企业制造的货物、承担的工程或者服务，或者提供其他中小企业制造的货物，不包括提供或使用大型企业注册商标的货物；

2）本规定所称中小企业划分标准，是指国务院有关部门根据企业从业人员、营业收入、资产总额等指标制定的中小企业划型标准（工信部联企业〔2011〕300 号）；

3）小型、微型企业提供有中型企业制造的货物的，视同为中型企业；小型、微型、中型企业提供有大型企业制造的货物的，视同为大型企业。

4）监狱企业视同为小型、微型企业。

（投标人为小型、微型企业，同时所投产品为小型、微型企业生产的才能享受政策性优惠）

17.3.2 具体评审价说明：

1）投标人为小型或微型企业，其评审价=投标报价*（6%）；

2）投标人为联合体投标，联合体中有小型或微型企业且联合协议中约定小型、微型企业的协议合同金额占到联合体协议合同总金额 30％以上的，其评审价=投标报价*（2%）。

17.3.3 投标人为工信部联企业〔2011〕300 号文规定的小型和微型企业（含联合体）的，必须如实填写“中小企业声明函”（内容、格式见财库〔2011〕181 号），并提供营业收入、人员等相关证明材料，否则无效。**如有虚假骗取政策性加分，将依法承担相应责任。**

18.评标

18.1 除采购人代表、评标现场组织人员外，采购人的其他工作人员以及与评标工作无关的人员不得进入评标现场。

18.2 见“第四章 评审方法和程序”。

六、授标及签约

19. 定标原则

19.1 评标委员会将严格按照投标文件的要求和条件进行评标,根据评标办法推荐排名前三的投标人为中标候选人，其中排名第一的投标人为第一中标候选人。采购人将确定排名第一的中标候选人为中标人并向其授予合同。排名第一的中标候选人因不可抗力或者自身原因不能履行合同，或者本文件规定应当提交履约保证金而在规定期限未能提交的，或者是评标委员会出现评标错误，被他人质疑后证实确有其事的，采购人将把合同授予排名第二的中标候选人或重新组织招标。如此类推。

19.2 海南信华招标代理有限公司将在指定的网站上公告投标结果。

20. 质疑处理

20.1 投标人如认为招标文件、招标过程和中标结果使自己的权益受到损害的，应在知道或应知道其权益受到损害之日起七个工作日内以书面形式向海南信华招标代理有限公司提出质疑，并附相关证明材料。匿名、非书面形式、七个工作日之外的质疑均不予受理。

21. 中标通知

21.1 定标后,海南信华招标代理有限公司应将定标结果通知所有的投标人。

21.2 中标人收到中标通知后，应在规定时间内到海南信华招标代理有限公司处领取中标通知书，并办理相关手续。

21.3 中标通知书将是合同的一个组成部分。

22. 签订合同

22.1 中标人应按中标通知书规定的时间、地点与采购人签订中标合同,否则投标保证金将不予退还，给采购人和招标代理机构造成损失的，投标人还应承担赔偿责任。

22.2 投标文件、中标人的投标文件及评标过程中有关澄清文件均应作为合同附件。

23. 招标代理服务费

根据项目预算按计价格[2002]1980 号文相关规定向中标人收取招标代理服务费。

24.本项目不召开答疑会。

第三章 用户需求书

第一部分 A 包需求书

一、项目名称

软硬件设备及材料采购

二、采购清单

主要采购的软硬件设备包括：防火墙、WEB 防火墙、防毒墙、准入控制、运维审计、数据库审计、日志审计及网管平台等，具体清单如下：

序号	名　称	单位	数量	备注
一、公安网				
1	上联边界防火墙	台	1	
2	服务器区域边界防火墙	台	1	
3	上联边界防毒墙	台	1	
4	终端准入控制系统	台	1	
5	运维审计系统	套	1	
6	数据审计系统	套	1	
7	日志审计系统	套	1	
8	网络管理平台	套	1	
9	网络管理平台服务器	台	1	
二、视频专网				
1	边界防火墙	台	1	
2	终端准入控制系统	台	1	
3	运维审计系统	套	1	
4	日志审计系统	台	1	
5	网络管理平台	套	1	
6	网络管理平台服务器	台	1	
7	服务器接入交换机	台	2	
三、互联网				
1	边界防火墙	台	1	
2	边界 WEB 防火墙	台	1	
3	终端准入控制系统	台	1	
4	服务器接入交换机	台	1	

三、详细技术参数及技术要求

注：以下参数中带▲的参数为重要参数，如不满足则将在评分中加重扣分。

1、 公安网

（1）上联边界防火墙

序号	指标项	指标参数

1	▲基本配置	标准 2U 设备,双冗余电源；≥6 个 10/100/1000M Base-TX 接口，≥4 个 SFP 接口；
		最大并发连接数≥300 万，最大吞吐量≥10Gbps，每秒新建连接数≥8 万；
		配置 IPS 模块，三年质保
2	网络适应性	支持静态路由，动态路由（OSPF、RIP、BGP、ISIS 等），VLAN 间路由，单臂路由，组播路由等。
		支持基于应用的策略路由，可实现为不同的应用类型智能选择相应的链路。
		支持基于文件类型的策略路由，可实现将预定义或者自定义的文件按照不同的分类进行智能选路。
		支持多出口路由情况下的默认路由备份、负载均衡。
		支持 ISP 路由，支持联通、电信、教育网、移动等 ISP 服务商地址列表，列表可导出及导入，可通过 Web 界面选择不同的 ISP 服务商实现快速切换。
3	网络管理	支持 DHCP Client、DHCP Relay、DHCP Server。
		各种工作模式下均支持 H.323（H.323 GK）、SIP、FTP、MMS、RTSP、XDMCP、TNS 等多种动态协议。
		支持对虚拟环境的数据流进行全策略控制。
		支持链路聚合功能，支持 802.3ad 和静态轮询、热备等多种模式，MAC、MAC&IP、IP&Port 多种聚合负载算法。
4	网络访问控制	支持一体化安全策略配置，可以通过一条策略实现用户认证、IPS、AV、URL 过滤、协议控制、流量控制、并发限制、新建限制、垃圾邮件过滤、审计等功能,简化用户管理。
		支持将源 MAC 作为独立的访问控制条件，防止非法设备接入。
		支持基于数据包的安全域、地址、用户及用户组、MAC、端口号、服务、域名等进行安全策略控制 。
		支持以组的方式管理安全策略，支持安全策略组的增、删、改操作，简化安全策略管理。
		支持针对策略中的源、目的地址进行并发限制，可以针对单 IP(或地址范围)进行并发控制。
		支持针对策略中的源、目的地址进行新建限制，可以针对单 IP(或地址范围)进行新建控制。
		支持策略命中数显示，并支持通过安全策略命中数范围查询。
		支持根据 IP 地址进行策略查询、支持根据服务端口进行策略查询。
		支持根据规则序号、规则名、源地址、目的地址、入侵防护策略、服务、认证用户、认证用户组、所属策略组、备注进行规则查询。
		支持查看资源被访问控制策略引用情况。
		支持查看访问控制策略引用地址、服务、时间资源情况。
5	服务器负载均衡	至少支持两种方法主动探测服务器的存活状态
6	入侵防护	支持基于策略的入侵检测与防护，可针对不同的源目 IP 地址、源 MAC 地址、服务、时间、安全域、用户等，采用不同的入侵防护策略。
		入侵防御特征库库至少应包括信息窃取、木马后门、间谍软件、可疑行为、网络设备攻击、安全漏洞及网络数据库攻击等的特征事件。
		支持细粒度的自定义 IPS 特征功能，支持 DNS\HTTP\FTP\TFTP\TELNET\SNMP\POP3\SMTP\IMAP\等 17 大类应用层协议的自定义，可以精准设置各个协议字段内容，例如字符内容、偏移、长度等细粒度的参数。
		支持对网络扫描行为的检测和过滤，可实现基于端口的扫描防护和基于主

		机的扫描防护。
		支持 IP/MAC 地址绑定的方式防止 ARP 欺骗，可采用手动建立或自动探测的方式生成 IP/MAC 对。
		支持多接口的攻击行为监听检测方式，可并行旁路检测多个网段内的网络攻击行为，用于高可靠性要求的旁路应用环境。
		至少支持丢弃封包、切断会话、攻击重定向、记录日志、邮件报警、声音报警 7 种响应方式。
		支持实时的入侵防护事件分级报警列表，可按事件的源 IP、目的 IP、协议、时间等显示；通过不同的入侵防护事件实时阻断入侵源 IP，阻断时间可控，提供入侵防护事件分级列表界面和实时阻断界面。
7	抗拒绝服务攻击	支持主流 ICMPFLOOD\SYNFLOOD\ACKFLOOD\SYNACKFLOOD\UDPFLOOD 攻击防护，采用专业高效的攻击防护算法，非采用简单的阈值进行攻击防护
		以上主流的功能，支持基于源 IP 限速、基于特征过滤系数、聚类限速系数、重传检测、自学习白名单等多种防御机制。
		支持专业的 DNSflood 攻击防护，具有高级的基于聚类限速、聚类分析、重传检测等多种高级防护算法。
		支持专业的 HTTP Flood 攻击防护；可以实现 get 和 post 的攻击防护，且 get 防护算法支持 4 类；支持独立 url 处理动作；以上防护功能均可以基于聚类分析、可信度、回探等多种防御机制。
		支持抗地址欺骗攻击、抗源路由攻击、抗 Smurf 攻击、抗 LAND 攻击、抗 Winnuke 攻击、抗 Queso 扫描、抗 SYN/FIN 扫描、抗 NULL 扫描、抗圣诞树攻击、抗 FIN 扫描、抗 Fraggle 攻击。
		支持自定义攻击日志的生成频率以及每时间段所需要记录的告警日志数目，攻击日志能够准确记录时间、攻击源目的、攻击类型、攻击次数等信息。
		支持攻击流量统计、攻击事件统计、攻击流量排行、攻击事件排行。
		支持 web 界面下对攻击流量进行抓包分析，支持自定义抓包参数，至少包括数据报文长度、报文数量、抓包时间及采样频率等基本参数；支持根据协议、源目的 IP、端口等参数进行数据报文过滤。
		支持对本地抓包文件的管理，包括下载、删除等操作，同时支持 FTP 方式将抓包文件上传至指定的 FTP 服务器中。
8	统一认证管理	支持多人使用同一帐号登录。
		支持在用户认证失败的情况下仍提供基本的网络访问权限。
		支持对 WEB 认证、LDAP 认证、RADIUS 认证、邮件账号认证、IP 识别用户的强制下线。
		支持用户的 AD 域、POP3、BJCA 单点登录，支持自定义单点登录监听端口。
		支持设置认证服务器组。
		支持用户口令复杂度设置。
		支持显示详细的用户在线信息，包括用户名称、真实姓名、所属组、认证源、接入方式、认证方式、登录 IP/MAC、在线时间、登录时间和可对其进行相关操作。
9	主动防御	支持 IPv4 和 IPv6 双栈协议下的主动防御。
		要求支持主动防御功能，对服务器、主机进行后门、服务探测、文件共享、系统补丁、IE 漏洞等主动式扫描。
10	安全日志	支持至少 2 个 Syslog 服务器，发送流量、系统或默认 2 类型日志到不同服务器。
		支持日志中文化，可显示配置命令日志的操作人。

		支持在三权分立模式下，对日志文件的加密导出/导入
11	高可用性	支持端口联动，支持上下行端口组的联动，可以实现单端口决定同组中的任意接口失效启动链路切换。
		自动同步、心跳接口多级（≥2 级）物理备份。
		可在热备和集群工作模式下支持多台防火墙的会话、配置的实时同步、手动同步。
		支持多重冗余协议(MRP)，实现链路备份、端口冗余、双机热备份、集群备份等。
		支持基于 VRRP 技术的热备和负载均衡。
		在 NAT、路由、透明模式下支持 A-A,A-S 模式，且切换时间小于 1 秒 。
12	▲保修	三年原厂硬件质保

（2）服务器区域边界防火墙

序号	指标项	指标参数
1	▲基本配置	标准 2U 设备,双冗余电源；≥6 个 10/100/1000M Base-TX 接口，≥4 个 SFP 接口；
		最大并发连接数 300 万，最大吞吐量 8Gbps，每秒新建连接数 6 万；
		配置 IPS 模块，AV 模块，三年质保
2	网络适应性	支持静态路由，动态路由（OSPF、RIP、BGP、ISIS 等），VLAN 间路由，单臂路由，组播路由等。
		支持基于应用的策略路由，可实现为不同的应用类型智能选择相应的链路。
		支持基于文件类型的策略路由，可实现将预定义或者自定义的文件按照不同的分类进行智能选路。
		支持多出口路由情况下的默认路由备份、负载均衡。
		支持 ISP 路由，支持联通、电信、教育网、移动等 ISP 服务商地址列表，列表可导出及导入，可通过 Web 界面选择不同的 ISP 服务商实现快速切换。
3	网络管理	支持 DHCP Client、DHCP Relay、DHCP Server。
		各种工作模式下均支持 H.323（H.323 GK）、SIP、FTP、MMS、RTSP、XDMCP、TNS 等多种动态协议。
		支持对虚拟环境的数据流进行全策略控制。
		支持链路聚合功能，支持 802.3ad 和静态轮询、热备等多种模式，MAC、MAC&IP、IP&Port 多种聚合负载算法。
4	网络访问控制	支持一体化安全策略配置，可以通过一条策略实现用户认证、IPS、AV、URL 过滤、协议控制、流量控制、并发限制、新建限制、垃圾邮件过滤、审计等功能,简化用户管理。
		支持将源 MAC 作为独立的访问控制条件，防止非法设备接入。
		支持基于数据包的安全域、地址、用户及用户组、MAC、端口号、服务、域名等进行安全策略控制 。
		支持以组的方式管理安全策略，支持安全策略组的增、删、改操作，简化安全策略管理。
		支持针对策略中的源、目的地址进行并发限制，可以针对单 IP(或地址范围)进行并发控制。
		支持针对策略中的源、目的地址进行新建限制，可以针对单 IP(或地址范围)进行新建控制。
		支持策略命中数显示，并支持通过安全策略命中数范围查询。
		支持根据 IP 地址进行策略查询、支持根据服务端口进行策略查询。

		支持根据规则序号、规则名、源地址、目的地址、入侵防护策略、服务、认证用户、认证用户组、所属策略组、备注进行规则查询。
		支持查看资源被访问控制策略引用情况。
		支持查看访问控制策略引用地址、服务、时间资源情况。
5	服务器负载均衡	至少支持两种方法主动探测服务器的存活状态
6	入侵防护	支持基于策略的入侵检测与防护，可针对不同的源目 IP 地址、源 MAC 地址、服务、时间、安全域、用户等，采用不同的入侵防护策略。
		入侵防御特征库库至少应包括信息窃取、木马后门、间谍软件、可疑行为、网络设备攻击、安全漏洞及网络数据库攻击等的特征事件。
		支持细粒度的自定义 IPS 特征功能，支持 DNS\HTTP\FTP\TFTP\TELNET\SNMP\POP3\SMTP\IMAP\等 17 大类应用层协议的自定义，可以精准设置各个协议字段内容，例如字符内容、偏移、长度等细粒度的参数。
		支持对网络扫描行为的检测和过滤，可实现基于端口的扫描防护和基于主机的扫描防护。
		支持 IP/MAC 地址绑定的方式防止 ARP 欺骗，可采用手动建立或自动探测的方式生成 IP/MAC 对。
		支持多接口的攻击行为监听检测方式，可并行旁路检测多个网段内的网络攻击行为，用于高可靠性要求的旁路应用环境。
		至少支持丢弃封包、切断会话、攻击重定向、记录日志、邮件报警、声音报警 7 种响应方式。
		支持实时的入侵防护事件分级报警列表，可按事件的源 IP、目的 IP、协议、时间等显示；通过不同的入侵防护事件实时阻断入侵源 IP，阻断时间可控，提供入侵防护事件分级列表界面和实时阻断界面。
7	恶意代码防护	支持基于策略的病毒扫描与防护，可针对不同的源目 IP 地址、源 MAC 地址、服务、时间、安全域、用户等，采用不同的病毒防护策略。
		支持应用协议自识别，可以实现 HTTP,SMTP,FTP,POP3,IMAP,FTP,WEBMAIL 多种应用协议下的病毒防护，支持自定义非标准端口下应用协议的病毒防护。
		支持常见 WEB 邮件系统的病毒防护。
		支持路由、透明、混合等各种工作模式下的网络病毒检测
		支持多接口可旁路的病毒文件传输监听检测方式，可并行监听并检测多个接口、多个网段内的病毒传输行为，用于高可靠性要求的旁路应用环境。
		支持隔离病毒源地址，防止病毒源主机访问内部网络，提高网络整体安全性。
		支持病毒文件隔离，用于后续分析取证。
		支持基于病毒防护规则，可以实现病毒隔离、阻断、声音告警、记录日志，发送告警邮件等 5 种响应方式。
		系统内置多种病毒防护模板，支持自定义病毒防护模板。
		支持 gzip、rar、zip 等压缩格式的病毒扫描。
		支持针对 FTP 断点续传环境下的病毒检查。
		支持过滤邮件病毒、文件病毒、恶意网页代码、木马后门、蠕虫等多种类型的病毒。
		支持 AV 云防护功能，可将检测出的病毒文件备份至云端进行分析。

8	抗拒绝服务攻击	支持主流 ICMPFLOOD\SYNFLOOD\ACKFLOOD\SYNACKFLOOD\UDPFLOOD 攻击防护，采用专业高效的攻击防护算法，非采用简单的阈值进行攻击防护
		以上主流的功能，支持基于源 IP 限速、基于特征过滤系数、聚类限速系数、重传检测、自学习白名单等多种防御机制。
		支持专业的 DNSflood 攻击防护，具有高级的基于聚类限速、聚类分析、重传检测等多种高级防护算法。
		支持专业的 HTTP Flood 攻击防护；可以实现 get 和 post 的攻击防护，且 get 防护算法支持 4 类；支持独立 url 处理动作；以上防护功能均可以基于聚类分析、可信度、回探等多种防御机制。
		支持抗地址欺骗攻击、抗源路由攻击、抗 Smurf 攻击、抗 LAND 攻击、抗 Winnuke 攻击、抗 Queso 扫描、抗 SYN/FIN 扫描、抗 NULL 扫描、抗圣诞树攻击、抗 FIN 扫描、抗 Fraggle 攻击。
		支持自定义攻击日志的生成频率以及每时间段所需要记录的告警日志数目，攻击日志能够准确记录时间、攻击源目的、攻击类型、攻击次数等信息。
		支持攻击流量统计、攻击事件统计、攻击流量排行、攻击事件排行。
		支持 web 界面下对攻击流量进行抓包分析，支持自定义抓包参数，至少包括数据报文长度、报文数量、抓包时间及采样频率等基本参数；支持根据协议、源目的 IP、端口等参数进行数据报文过滤。
		支持对本地抓包文件的管理，包括下载、删除等操作，同时支持 FTP 方式将抓包文件上传至指定的 FTP 服务器中。
9	统一认证管理	支持多人使用同一帐号登录。
		支持在用户认证失败的情况下仍提供基本的网络访问权限。
		支持对 WEB 认证、LDAP 认证、RADIUS 认证、邮件账号认证、IP 识别用户的强制下线。
		支持用户的 AD 域、POP3、BJCA 单点登录，支持自定义单点登录监听端口。
		支持设置认证服务器组。
		支持用户口令复杂度设置。
		支持显示详细的用户在线信息，包括用户名称、真实姓名、所属组、认证源、接入方式、认证方式、登录 IP/MAC、在线时间、登录时间和可对其进行相关操作。
10	主动防御	支持 IPv4 和 IPv6 双栈协议下的主动防御。
		要求支持主动防御功能，对服务器、主机进行后门、服务探测、文件共享、系统补丁、IE 漏洞等主动式扫描。
11	安全日志	支持至少 2 个 Syslog 服务器，发送流量、系统或默认 2 类型日志到不同服务器。
		支持日志中文化，可显示配置命令日志的操作人。
		支持在三权分立模式下，对日志文件的加密导出/导入
12	高可用性	支持端口联动，支持上下行端口组的联动，可以实现单端口决定同组中的任意接口失效启动链路切换。
		自动同步、心跳接口多级（≥2 级）物理备份。
		可在热备和集群工作模式下支持多台防火墙的会话、配置的实时同步、手动同步。
		支持多重冗余协议(MRP)，实现链路备份、端口冗余、双机热备份、集群备份等。
		支持基于 VRRP 技术的热备和负载均衡。
		在 NAT、路由、透明模式下支持 A-A,A-S 模式，且切换时间小于 1 秒 。

13	▲保修	三年原厂硬件质保

（3）上联边界防毒墙

序号	指标项	指标参数
1	产品形态及资质要求	产品需为软硬件一体化的专业防毒墙，非病毒扫描功能建立在防火墙基础上的设备。
		产品对通过文件、邮件附件、网页浏览等方式传播的木马、病毒、后门、蠕虫、间谍软件等恶意软件实时扫描并拦截，同时可分析网内各种应用协议使用情况，以及防御 SQL 注入、XSS 跨站脚本等针对 WEB 服务器的攻击。
2	▲硬件要求	要求设备至少应支持 2 路硬件 Bypass
		至少具备 4 个 10/100/1000MBase-T 端口，4 个 SFP 端口，
3	▲性能要求	最大并发连接数≥300 万，最大吞吐量≥10Gbps，每秒新建连接数≥8 万；
4	功能要求	支持对 HTTP/HTTPS/FTP/SMTP/POP3 五种协议实现木马、病毒、后门、间谍软件、蠕虫等恶意软件的扫描和过滤。
		设备支持基于端口的 VLAN 和基于 802.1Q 的 VLAN。
		支持僵尸网络的防护。
		支持 HTTP POST 和 Get 的双向实时检测，HTTPS POST 的单向检测，并允许用户自定义检测规则。
		设备能加载的特征库大于 1000 万
		支持通过分析软件的行为和特征判定是否为恶意软件的启发式扫描技术。
		支持恶意网页和 URL 过滤功能，并支持自定义黑白名单。
		需支持应用程序控制功能，支持对常见的视频、股票、IM 和游戏等应用程序进行管控。
		设备支持直连病毒预防模式或旁路病毒预警部署模式，要求部署时无需改变现有 DNS 配置和网络结构。
		支持对 IP、IP 范围、用户、用户组、时间段、物理端口、应用以及上述的组合设置带宽策略，满足关键应用及用户带宽需要。
		支持 365 天不间断更新，要求支持 80 端口加密升级，每天不少于 1 次，并无需改变防火墙等网络设备的访问控制策略。
		支持详细的病毒防护日志记录，要求必须记录日期、病毒名、文件名、源 IP 地址、目的 IP 地址、采取的动作等内容。
		支持详细的 Web 防护日志记录，要求必须记录日期、源 IP 地址、目的 IP 地址、访问方法、攻击 URL、攻击名称、采取的动作等内容。
		支持即时、定期报表生成功能，要求体现病毒威胁变化、各类应用与各 IP 地址带宽利用率、当前会话数、系统运行状态信息等，并根据报警信息的特征可同时设置多个报警显示界面。
		支持简体中文操作界面和多级管理员权限分配，要求必须但不少于读写帐号、只读帐号及审计帐号。
		支持带内、带外管理，要求可通过 SSL 加密的 WEB 、SSH 命令行、Console 方式管理。
5	▲保修	三年原厂硬件质保

（4）终端准入控制系统

序号	指标项		指标参数
1	基本要求	▲系统要求	具有独立自主知识产权，须为标准机架式硬件产品，除自身硬件设备外，产品功能的实现无需额外增加服务器等设备。
		▲性能要求	配置 6 个千兆电口；每秒事务数（TPS）：≥3500（次/秒），最大吞吐量：≥1.5Gbps，最大并发链接数：3000（条）；1500 用户许可；
		▲高可用性	1. 准入设备必须具备HA模式，HA须支持主备机心跳IP检测及虚地址管理模式，支持vrrp管理模式。 2. 提供第三方监控平台，在出现重大异常情况时能及时通知网络设备放开网络。
		语言支持	支持终端客户端、web 显示的中英文双语切换
		终端部署	1. 准入设备应至少提供安全客户端（Agent）、安全控件、无客户端等多种可供自定义部署、管理模式。 2. 安全客户端模式部署时，客户端程序应支持功能定制，以降低系统资源耗用，提升客户端兼容性。
2	准入架构	终端发现	1、 能够实时监测并发现接入内网的PC、平板电脑、智能手机、IP设备等终端，能够在第一时间隔离阻断并通知管理员。 2、 对自动发现的终端能够按照类别自动归类，以方便网络终端的统计管理（提供截图证明，加盖原厂商章）。
		准入技术	1. 准入设备须原生支持802.1x标准协议，无需第三方RADIUS服务器支持。 2. ▲准入设备支持基于多厂商Virtual Gateway的VLAN隔离技术，实现无客户端环境下端口级准入控制（提供截图证明，加盖原厂商章）。 3. 准入设备支持基于策略路由技术的准入控制模式，入网设备在访问网内关键资源时，将被强制隔离、引导至认证管理页面，同时支持交换机接口动态VLAN下发、端口隔离模式的网络边界管理。 4. 单台准入设备可支持至少2个核心交换机进行策略路由准入控制。 5. 准入设备可支持端口镜像准入技术，通过对交换机镜像数据的实时分析，能够及时发现并阻断非授权终端的接入。 6. 支持使用802.1x MAC认证时，记录详细的认证信息，包括:认证的时间、认证类型、认证的MAC、认证是否成功等，并支持报表记录。
		定向引导	1. 支持终端入网IE重定向引导，当用户访问网页时能够自动转向到指定的页面或地址，并支持http代理及多重重定向引导。 2. 可根据用户的实际环境自定义非80端口的Web服务端口号及用户重定向引导。 3. 能通过浏览器完成身份认证、控件安装、设备注册、安全检查、检查结果展现等全流程引导管理。 4. ▲具有Mac OS、Linux、iOS、Android等系统专属客户端，支持认证引导和准入管理（提供截图证明，加盖原厂商章）。

3	违规外联	▲违规外联	1. 能够针对3G拨号、双网卡、随身WIFI、代理等多种违规联网行为做实时检测，不接受间歇性ping外网地址的探测方式。 2. 能够针对违规外联终端进行即时断网，断网方式应支持断开链接、关闭连接进程、断网后重启恢复、重启计算机等多级模式，并能够实时通知管理员。 3. 准入设备能够支持按照用户角色定义、限制员工的内网访问范围，防止其越权访问操作。 4. SSID白名单，可对连接到白名单之外的无线网络行为进行阻断（提供截图证明，加盖原厂商章）。
4	边界管理	IP/MAC 绑定	具有入网设备自动学习功能，支持 IP/MAC/端口三者强制绑定，以及违规终端 VLAN 隔离机制，防止终端仿冒 IP 接入网络或移动设备位置。
		主机防火墙	1. 终端在准入通过后访问域严格收管理员策略控制 2. 同网段终端无法互相访问，做到精确到端口的高安全性控制
5	设备特征指纹	设备特征指纹	1. 具有非智能IP终端信息库，能够精准识别网络打印机、网络摄像头、IP电话等设备，并根据设备特征进行自动匹配和归类。 2. 通过伪造合法IP或MAC地址的非法设备和行为，能够被即时发现并阻断。
6	设备私接管理	NAT 设备	1. ▲具有NAT识别和检测机制能够及时发现网内私接的小路由器、无线AP、随身WIFI等NAT设备，帮助清查通过网中网隐藏的真实网络终端（提供截图证明，加盖原厂商章）。 2. 对通过NAT入网的计算机可以实现准入控制、安全评估和修复等流程化管理（提供截图证明，加盖原厂商章）
		Hub 管理	1. 能够发现内网私接的Hub、傻瓜交换机等非网管设备，当多台计算机通过Hub接入网络时，能够及时产生告警通知管理员（提供截图证明，加盖原厂商章）。 2. 准入设备能够采用VLAN隔离、逻辑关闭端口等方式禁止Hub下联计算机接入网络。 3. 支持Hub下多个终端需分别认证才能入网和只需一台认证即可全部入网两种认证机制。
7	网络管理	设备识别	1. 支持自动识别网络设备类型，包括：交换机、路由器、防火墙等，并按照类别自动进行归类。 2. 支持设备管理模板的定义功能，能够通过SNMP、SSH、TELNET等方式自动、批量添加网络设备。
		▲终端网络拓扑	1. 准入设备支持交换机到终端计算机的网络拓扑管理功能，能够自动绘制出网络拓扑图（提供截图证明，加盖原厂商章）。 2. 能够在拓扑图上选取设备查看其基本状态信息、设备型号、所处位置、子节点、路由表、ARP 表等信息（提供截图证明，加盖原厂商章）。 3. 支持在界面上提供对该网络设备进行TELNET、SSH等管理。
		交换机状态展现	1. 支持可网管型交换机面板图形化展现各接口状态（up、down、trunk等），以及各接口下联的终端详细信息（IP、地址、MAC地址等）（提供截图证明，加盖原厂商章）。 2. 能够支持自上而下逐级查找终端的具体位置、安全状态、认证用户、上下线时间等信息。

		AP 联动管理	能够与主流的 AP 设备深度联动，支持 AP 控制器面板的图形展现，包括 AP 连接状态、下联终端信息（IP 地址、MAC 地址等）等。
		DHCP 中继	1. 能提供稳定的DHCP服务，并可以通过DHCP二次地址分配机制实现安全准入管理，支持交换机中继认证方式。 2. 能够根据用户、IP/MAC绑定信息等条件，为指定终端设备分配特定的IP地址。 3. 支持DHCP服务器筛选，防止非法DHCP服务器分发错误地址
		DHCP 地址释放	支持 DHCP 通过管理服务器手动操作，主动进行某台主机的 IP 地址释放。实现 IP 地址充分利用。
8	移动终端管理	终端识别	支持当前主流智能终端设备的安全准入控制，能够自动识别主流手机、智能终端等设备，并自动进行分类。
		移动终端入网	1. 提供独立的智能终端入网引导界面的自主定制功能，至少包括界面标题、界面 LOGO、界面说明文字等。 2. 能够提供移动终端入网的设备注册功能。
9	认证管理	联动认证	能够全面结合用户已有的认证或业务系统，可以与 RADIUS、LDAP、STMP/POP 等采用标准协议的系统做深度联动认证。
		AD 域单点登录	1. 能够与用户现有的AD域相结合，当用户登录到AD域后，无需二次认证即可入网，避免多次认证的繁琐流程。 2. 当用户未登录到AD域时，该终端将一直被隔离，该状态下只有通过IE页面进行认证才能够入网。
		证书认证	支持至少 2 个以上的根证书。终端用户认证时，自动进行认证证书的根证书匹配
		短信认证	支持短信认证模式，用户在登记入网手机号码后，能够在手机上接收到入网的短信验证码，并在 IE 页面上利用短信验证码认证入网。
		微信认证	通过关注微信公众号放行移动终端入网
		接入审核	能够针对不同的角色或设备类别有选择的开启入网审核功能，待审核的用户或设备必须经过管理员审批才能入网。
		认证控制	支持对认证时间段、IP 段控制限制某类（角色）账户只能在指定的时间段、IP 段认证。
		自助账号申请	支持用户在认证页面自行进行账号的申请。用户可自行提交用户名、密码、姓名、电话、部门、E-Mail 等信息。管理员审核通过后，用户即可使用该账号进行认证。有效解决用户账号和密码创建和分发的困难。
10	来宾管理	来宾角色	能够提供来宾角色选择，能够设定来宾设备的访问权限和入网时长
		来宾码认证	提供临时入网码，支持来宾设备与受访人员进行一对一绑定功能
		二维码认证	通过扫描二维码进行来宾入网管理（提供截图证明，加盖原厂商章）
		来宾使用报表	生成来宾分配、来宾入网等动态审计报表

11	终端安全管理	安全检查库	准入设备须提供系统安全配置、用户行为规范等类别检查项，至少提供 24 种以上安全检查项。
		系统补丁	▲准入设备具有完整的补丁管理子系统，无需第三方补丁服务器支持，自身即可以提供完整的流程化补丁管理，包括同步更新、补丁分类、补丁分发、补丁报表等功能（提供截图证明，加盖原厂商章）。能够在 IE 页面进行入网终端的补丁检查，补丁均划分为严重、重要、中等的类别，能够在 IE 页面显示出检查结果（提供截图证明，加盖原厂商章）。
		防病毒软件	能够在 IE 页面检查出终端的杀毒软件情况，支持主流的 20 种以上的杀毒软件检查，包括微软 MSE、可牛、Avast 等，支持杀毒软件版本、病毒库和运行情况的检查，能够在 IE 页面显示出检查结果（提供截图证明，加盖原厂商章）。
		Windows 组策略检测	windows 密码策略、屏保、共享目录、弱口令、防火墙、网卡配置等系统策略进行检查和修复
		计算机健康性检测	对终端的磁盘使用率、垃圾文件、IE 主页、网络监听端口等安全性配置进行检查和修复
		自定义安全检查	通过检测终端文件路径、指定文件版本、大小、MD5，注册表的项、注册表值，进程，服务名称、服务状态，进行检查。通过安装包运行、访问站点、开关服务、关闭进程、执行文件、删除文件、修改注册表进行修复。可以灵活的全访问的对终端进行安全检查和修复（提供截图证明，加盖原厂商章）。
		终端安全加固	能够通过傻瓜式的漏洞修复模式为用户提供简单、形象的漏洞自我修复功能，完全不需要管理员的介入即可完成终端安全风险项修补。
		桌管系统联动	能够在 IE 页面检查出主流的桌面管理系统（包括 Landesk、北信源、威盾、盈高、圣博润等）客户端是否安装并正常运行，能够在 IE 页面显示出检查结果。
12	移动存储设备管理	移动存储设备管理	1. 管理员可以通过对存储介质统一注册、授权的方式来加强管理存储介质的使用范围和权限，并支持存储介质分区加密，未经标识的存储介质将不能在企业内正常使用。 2. 针对不同注册状态的存储介质制定不同的控制策略，能够对存储介质进行只读、禁用、放行、脱机生效以及时间范围等做精细控制。
		移动存储设备审计	1. 支持查询存储介质的类型、设备名称、设备插入时间、设备拔出时间、设备使用 IP 地址、类型代码、设备容量、厂家名称、产品名称、该存储介质使用人、操作系统用户名、备注信息。 2. 支持使用存储介质的终端信息显示，包括：设备名称、IP 地址信息、所在部门、所在位置、联系人、联系电话、E-Mail 地址、设备状态（开机、关机）、最后在线时间等。

13	资产管理	资产管理	1. 能够对全网计算机上安装的软件进行统计，可以按照部门、名称提供精确查询以及软件资产报表的导出。 2. 能够对终端硬件初始记录、最新记录和变动记录形成报表，并且能够查询变动的历史。
		资产变动	准入设备能够针对软硬件资产变动、资产异常情况提供了丰富多样的报警方式，便于管理员及时迅速了解资产信息。
		变动确认	支持管理员对每一条软硬件变动进行确认操作，已确认的条目显示已确认，并显示进行确认操作的确认人。对变动和变动确认可进行报表统计；
14	资源管理	软件检查	1. 通过安全检查检测终端软件安装、使用状态 2. 自动强制为终端安装软件 3. 软件产品授权，支持进行windows、office、WPS的产品授权信息进行检查
		IP 地址管理	1. 提供IP地址分配表，能够通过图示直观的查看各网段中未分配、开机、关机的数量和分布情况。 2. 能够直接、快捷的查看全网终端历史上线、下线、在线时长等详细的IP使用情况。
		能耗管理	提供未关机终端自动统计功能，并能够按照部门、时间段等条件生成统计报表。
15	运维管理	移动终端管理	移动端管理平台可实现设备快速定位、设备审核、实时报警监控、小助手确认码生成、准入控制器管理、平台基本信息、关机与重启
		管理角色控制	准入设备须采用系统管理员、安全管理员、审计员三权分立机制，防止单个角色管理者权限滥用。
		网络诊断工具	支持通过 Web 管理界面提供 ping、抓包、traceroute、nslookup 等功能，并可以设置命令参数进行相关调试。
		消息群发	能够支持在指定的一台或者多台终端计算机上产生桌面消息通知，该消息会立即弹出在用户桌面上，对用户进行提醒。
		软件分发	1. 准入设备应具有软件分发和部署功能，管理员可以预定义软件分发的路径、运行参数、是否执行等任务策略，以提升软件部署效率。 2. 能够自动判断并统计软件分发、部署的成功率，支持进程、注册表、安装路径等多种参数的组合判断。
16	报警报表管理	虚拟监控台	为了方便管理员从整体上把握网络安全态势，系统提供虚拟监控台功能。通过集中的仪表、数值显示快速进行安全态势的把握，主要包括：报警、安全风险等级、全网终端数、清理终端数、安检和规律、安检项状态分布。
		安全管理报表	1. 准入设备后台能够按周、月、年统计安全状况走势图。 2. 准入设备后台提供每日入网报告、每周入网报告、每月入网报告。

		报警信息	1. 可以提供紧急、重要、次要、提示等多个级别自定义报警模式。 2. 支持系统报警、网络报警、终端报警等类别，超过20种以上自定义报警类型。 3. 支持Syslog报警信息的定向输出。
		报警提醒	准入设备能够以邮件、手机短信、页面消息等多种报警方式提醒管理员各种安全异常状态。
17	▲第三方产品联动		1. 支持与主流上网行为管理系统深度联动，构建内网准入、准出的全面安全管理体系。 2. 能够与主流动态口令认证系统相结合，提供动态密码联动认证机制。 3. 支持与国内外主流U-Key联动认证。
18	资质要求		1. 公安部《计算机信息系统安全专用产品销售许可证》（提供证明文件，加盖原厂商章）； 2. 国家保密局《涉密信息系统产品检测证书（网络访问控制产品）》（提供证明文件，加盖原厂商章）； 3. 国家版权局《计算机软件著作权登记证书》（提供证明文件，加盖原厂商章）；
19	▲保修		三年原厂硬件质保
20	▲其他		提供原厂商授权函及售后服务承诺函（加盖原厂商章）

（5）运维审计系统

序号	指标项		技术参数及技术要求
1	▲硬件指标		标准机架式设备，软硬一体化；单电源；10/100/1000M Base-TX 接口≥6 个，存储容量≥1TB
			支持 700 路字符会话或 200 路图形会话并发
			包含 100 个点的被管资源数
			支持旁路部署
2	主要功能		通过安全产品将人与目标设备进行分离，建立以“人->用户账号->授权->目标设备账号->目标设备”为管理模式，通过基于唯一身份标识的集中管理账号与权限、授权的控制策略，与各服务器、网络设备等无缝连接，实现集中精细化运维操作管控与审计。使 IT 安全运维从被动响应的模式转变为主动的运维安全管控模式，降低人为安全风险，满足合规和内部管理要求。
3	统一身份及认证管理	完善的身份管理和认证	1)支持账号分属组织的管理模式；组织管理能力，支持纵向七级、横向 255 个的组织划分能力，能够实现更完善的分权管理和分权审计；
			2)支持运维用户和管理员采用同一个账号；
			3)支持管理员、运维用户的静态口令、数字证书、动态口令、LDAP、AD 域、Radius 等认证方式；
			4)支持 AD 域、LDAP 账号的自动同步；

序号	指标项		技术参数及技术要求
			5)支持密码强度、密码有效期（按天设置）、口令尝试死锁、用户激活、备注、访问白名单等安全管理功能；
			6)支持用户分组管理，并且单个用户可以属于多个用户组；
			7)支持用户信息导入导出，方便批量处理；
			8)支持系统管理员、运维管理员、设备账号管理员、会话审计员、管理审计员等管理员角色；
			9)审计员分权管理，分为会话审计员、管理审计员，其中会话审计员只能审计会话信息，管理审计员只能审计 HAC 自身操作信息。
		后台账号口令集中管理	系统支持对后台各类资源（主机、服务器、网络设备、数据库等）的账号口令进行统一管理，即后台资源的账号口令由系统托管，用户登录系统后，系统根据用户权限分配后台资源的使用权。
			托管账号支持一站式关联用户、关联用户组。
		SSO 单点登录	管理员将后台资源账号及口令配置到堡垒机中；
			根据管理员配置，实现运维用户与后台资源账号对应，限制账号的越权使用；
			运维用户通过堡垒机认证和授权后，堡垒机根据分配的账号实现自动登录后台资源。
			支持的 SSO 账号类型包括： 支持 Windows、Linux、Unix 等服务器账号自动登录； 支持 CISCO(包括特权账号)、H3C 等网络设备账号自动登录； 支持 FTP、VNC、SFTP 等账号自动登录； 支持 PLSQL、SQLPLUS 等数据库工具账号自动登录；
		后台设备自动改密	根据口令安全策略，堡垒机定期自动修改后台资源帐户口令；
			支持密码更新周期自定义，可以按天设置；
			根据管理员配置，实现运维用户与后台资源账号对应，限制账号的越权使用
			运维用户通过堡垒机认证和授权后，堡垒机根据分配的账号实现自动登录后台资源
		电子口令保管箱	对于托管的后台设备口令，除支持以文件导出、邮件等的方式进行备份外，还支持把该托管口令备份到专用的口令安全存储设备上，防止口令丢失的风险。对于该口令安全存储设备的访问，支持指纹方式认证
4	访问控制及授权	灵活、细粒度的授权	系统提供基于授权规则名的授权设置，每个授权规则名下可以绑定多个用户、用户组、设备、设备组、访问规则（年、月、日、周、时间、会话时长、运维客户端 IP、协议类型）。
			每条授权规则可以设置相应的备注、启用/禁用设置。
		命令级授权	对于字符型协议，如 Telnet、SSH、FTP、SFTP 等，能够实现命令级别的授权控制。系统提供基于告警规则名的授权设置，每个告警规则名下可以绑定多个用户、用户组、设备、设备组、命令规则。每条授权规则可以设置为启用或禁用。
			可以通过命令规则进行规则匹配，支持黑、白名单功能；
			支持预订义和自定义的匹配命令设置，匹配命令支持多条命令，支持正则表达式；
			告警规则可以设置为阻断或只告警；
			告警规则支持告警级别设置，支持普通、严重、紧急等级别；
			告警规则可以按照帐号级别进行绑定，可以设置为只有指定安全级别的帐号才能触发告警规则，针对不同用户实施不同的规则，从而提供更细粒度的操作控制。

序号	指标项		技术参数及技术要求
		应用发布	运维操作全程可控，可做到授权后应用只能访问指定服务，最大降低对后台目标服务集群的可能安全风险。
			可对整个运维操作过程进行完整记录，实现详尽的会话审计和回放。
			可依据用户要求快速实现新应用的发布和审计。
			可支持对数据库维护工具、pcAnywhere、DameWare 等不同工具的运维操作进行监控和审计。
5	运维事件事中控制	实时监控及阻断	监控正在运维的会话，信息包括运维用户、运维客户端地址、资源地址、协议、开始时间等；
			监控后台资源被访问情况；
			提供在线运维操作的实时监控功能。针对命令协议和图形协议可以图像方式实时监控正在运维的各种操作，其信息与运维客户端所见完全一致；
			管理员可以关闭在线会话。
		违规操作实时告警与阻断	违反告警规则的各种事件，根据告警规则自动处理；告警事件可实时查看，并通过审计平台的声音、闪烁提示；
			对于设置为阻断的命令，运维用户无法执行，系统提示相关阻断信息；
			告警事件以邮件、短信通知。
		可支持ITSM	可与 ITSM 相结合，为其优化变更管理流程，加强对变更管理中的风险控制；
			支持对现有运维变更管理系统快速集成。
		可支持双人复核操作	支持 Telnet/SSH 的强制登录复核；
			支持运维过程的高危命令复核，例如对某阻断命令，可以设置必须由其它人进行复核；复核人复核通过后，运维人员才可以执行该阻断命令；
			支持会话日志记录双人复核操作审批人、时间、操作符合命令；
			支持设置复核级别，可设置由任意高级别的用户进行复核，也可以设置专门的高级别用户进行复核。
6	运维事件事后审计	完整记录网络会话过程	系统提供运维协议 Telnet、FTP、SSH、SFTP、RDP(Windows Terminal)、Xwindows、VNC、Http、Https 以及应用发布等网络会话的完整会话记录，完全满足内容审计中信息百分百不丢失的要求；
			会话信息包括运维用户、运维地址、后台资源地址、资源名、协议、起始时间、终止时间、流量大小信息；
			会话信息包括运维过程中所有进出后台资源的数据。
		详尽的会话审计与回放	运维操作审计以会话为单位，提供当日和条件查询定位。条件查询支持按运维用户、运维地址、后台资源地址、协议、起始时间、结束时间和操作内容中关键字等组合方式；
			针对命令交互方式的协议，提供逐条命令及相关操作结果的显示；
			提供图像形式的回放，真实、直观、可视地重现当时的操作过程；
			回放提供快放、慢放、拖拉等方式，方便快速定位和查看；
			针对命令交互方式的协议，提供按命令进行定位回放；
			针对 RDP、Xwindows、VNC 协议，提供按时间进行定位回放。
			对于 RDP 协议除记录视频格式外，对于各种键盘鼠标的操作进行记录，具体包括键盘信息、屏幕文本信息、文件读写信息等。
		自审计功能	管理员、审计员、运维人员在系统中关键操作行为记录，并可通过报表展现；
			可记录主帐号访问审计设备时间、终端 IP 记录；
			可记录主帐号访问目标设备、从帐号记录。

序号	指标项		技术参数及技术要求
		事件通知	事件通知功能可以将发生的事件以邮件或短信（需定制）的方式通知任何管理员。事件分为系统访问事件、配置管理事件、运维操作事件、运维审计事件、系统维护事件等 5 大类。
		完备的审计报表功能	提供日常报表，包括今日会话、今日自审计、用户信息、资源信息、权限信息、规则信息、管理员角色信息等报表；
			提供会话报表，可根据用户选定时间、用户、资源形成会话报表；
			自审计操作报表，可根据用户选定时间、管理员、模块形成自审计报表；
			告警报表，可根据告警类别、级别、资源、运维用户、协议、时间等条件形成报表；
			综合统计报表，可根据时间、资源、用户等条件形成综合统计报表，报表中包括概要信息、每个用户操作信息、每个资源被操作信息等；
			报表导出，支持 PDF、Excel、Word 等格式。
7	兼容性、可扩展性		运维审计作为 IT 运维流程中的一个部分，能够遵循 ITIL 满足稽核与审计的要求，系统能够通过定制开发与现有 ITSM、SOC、网管平台进行集成，满足大型网络系统的管理要求。
			能够与 KVM 系统进行整合，解决 KVM 系统本身审计功能薄弱的问题。
			能够与专业的数据库审计系统进行整合，审计日志信息既满足直观、方面查看的目的，又可以记录详细的数据库操作记录，便于故障分析。
8	▲保修		三年原厂硬件质保

（6）数据审计系统

序号	指标项	指标要求
1	硬件指标	系统：审计产品采用专用工控机硬件架构，非普通 PC 服务器， MTBF(平均故障间隔时间)≥65000 小时； ▲系统启动采用 CF 卡加硬盘方式，保证稳定可靠不可篡改（提供产品图片，加盖原厂商章）。
		处理器：采用当前主流 Intel 酷睿第四代 I7 系列 CPU,主频至少 3.4G，至少 4 核 8 线程
		内存：≥16GB DDR3 1600Mhz；
		电源模块：具备冗余热插拔双电源；冗余热插拔风扇；
		硬盘可用容量：≥2TB，支持 RAID0， RAID5 阵列，最大支持扩展到 4T*4。
		网络端口：支持监听接口扩展；配备 2 个千兆电口管理口； 支持千兆网络环境下的监听能力，配备至少 2 个千兆业务电口，至少 2 个千兆业务光口；
		支持硬件扩展第三方 FC SAN 存储 HBA 卡，速率 4Gbs 以上， Qlogic 2460 以上型号
		审计性能：能够稳定、流畅地同时支持 16 个数据库数审计能力，不会产生漏审；
2	部署方式	旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计
		支持在目标数据库安装 agent 解决云环境、虚拟化环境内部流量无法镜像场景下数据库的审计（提供公安部三所或国家保密科技测评中心测评报告，加盖原厂商章）
		支持分布式部署，管理中心可实现统一配置、统一报表生成、统一查询；
		管理中心和探测器都可存储审计数据，实现大数据环境下磁盘空间的有效利用和扩展；

		管理中心和探测器直接的数据传输速率、时间、端口都可自定义（提供截图证明，加盖原厂商章）；
		▲支持大数据平台部署，具有成熟的大数据 hadoop 平台处理，支持后期无缝扩展大数据版本，支持审计数据外送至大数据平台，检索性能高达 100 亿数据仅需 6-8 秒，存储数据量高达 3000 亿以上，并具有至少提供一个 100 万以上大数据处理合同案例（提供大数据合同关键页面复印件，加盖原厂商章）
3	处理能力	吞吐能力：≥3000M
		▲峰值处理能力：≥3 万条/秒（提供公安部三所或国家保密科技测评中心检测报告，加盖原厂商章）
		审计日志检索能力：≥3000 万条/秒；
4	协议支持	支持 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL 等六种主流数据库审计；
		支持 PostgreSQL、Teradata、Cache、人大金仓、达梦、南大通用等数据库审计（提供截图证明，加盖原厂商章）；
		支持主流业务协议 HTTP、Telnet、FTP、SMTP、POP3、DCOM；
		支持对各种协议自动识别编码及在 web 界面手工配置特定编码（提供截图证明，加盖原厂商章）
5	审计功能	支持数据库操作类、表、视图、索引、存储过程等各种对象的所有 SQL 操作审计；
		支持对操作时间、SQL 语句、执行结果、返回结果集、影响行数、执行时长、数据库用户名、实例名、源/目的 IP、源/目的端口、源/目的 MAC、客户端主机名、客户端程序名称、客户端操作系统用户名、业务主机群、SQL 模板、会话 ID、事件唯一 ID 等至少 21 个条件进行审计；
		▲支持数据库请求和返回的双向审计，特别是返回字段和结果集、执行状态、返回行数、执行时长等内容，支持通过返回行数和内容大小控制返回结果集大小（提供截图证明，加盖原厂商章；并提供公安部三所或国家保密科技测评中心检测报告，加盖原厂商章）；
		支持跨语句、跨多包的绑定变量名及绑定变量值的审计（提供截图证明，加盖原厂商章）
		▲支持在 IPV6 环境中部署，且支持所有数据库 IPV6 协议的审计（提供截图证明，加盖原厂商章）
		支持导入审计关联的账号信息，支持通过 IP 和账号关联到具体 SQL 是哪个自然人操作。
		应对数据库中所有初始化参数的状态进行审计，至少将数据库自身审计的启用和禁用、日志恢复的启动和禁用等信息记入审计日志
6	智能发现	自动识别流量中存在的数据库，也可通过扫描发现网络中的数据库
		▲支持定期自动扫描数据库漏洞和不安全配置，提供漏洞扫描报告（提供截图证明，加盖原厂商章；并提供公安部三所或国家保密科技测评中心检测报告，加盖原厂商章）
7	应用关联(三层关联)	支持 B/S 业务系统三层关联审计（需提供功能截图，并提供国家权威检测机构（公安部三所或国家保密科技测评中心）检测报告，加盖原厂商章）
		支持 C/S、B/S 三层架构下的真实用户名关联配置
		支持通过部署 agent 实现 java web 环境 100%准确关联（提供截图证明，加盖原厂商章）
		支持旁路自动学习三层审计关联功能（提供截图证明，加盖原厂商章）；
8	运维审计	支持与堡垒主机自动关联审计通过 ssh、rdp 等加密协议操作数据库行为（提供截

		图证明，加盖原厂商章；并提供公安部三所或国家保密科技测评中心检测报告，加盖原厂商章）
9	安全审计	支持审计记录中敏感数据的模糊化处理，内置常见敏感数据掩码规则，支持自定义敏感数据掩码规则（提供截图证明，加盖原厂商章）
		内置安全特征库规则不少于 300 条，支持对数据库安全进行检查，如 SQL 注入，缓冲区溢出，数据库漏洞、弱口令等（提供截图证明，加盖原厂商章）；
10	审计策略	内置审计规则库不少于 200 条。支持事件类型和策略分组，同时支持黑白名单方式策略
		告警分析应支持根据 SQL 模板排行分析，便于告警处理。
		告警查询应支持根据登陆用户、客户端工具名、客户端 IP、规则进行归并分析，能详细展示每类告警占总告警数量百分比，便于告警分析处理（提供截图证明，加盖原厂商章）
11	统计报表	系统提供内置多种报表模板库，内置的报表不少于 35 种（提供截图证明，加盖原厂商章）
		支持根据单个数据库或逻辑数据库组生成报表（提供截图证明，加盖原厂商章）
		报表支持严格按照塞班斯（SOX）法案、等级保护标准要求生成多维度综合报告；
		支持按照源 IP 地址、客户端工具、帐号、告警数等源信息生成报表；
		支持定期自动生成审计报表且以电子邮件方式自动进行发送（提供截图证明，加盖原厂商章）；
		支持报表自定义，自定义的条件不少于 20 个（提供截图证明，加盖原厂商章）
12	模型分析	▲支持对数据库自动建模及智能对异常行为告警功能（提供截图证明，加盖原厂商章；并提供公安部三所或国家保密科技测评中心检测报告，加盖原厂商章）；
		可通过行为轨迹图方式展示数据库访问行为（提供截图证明，加盖原厂商章）
		可基于账号、IP 地址、访问权限、客户端工具等维度对行为模型做钻取分析、变更分析，对学习的安全基线以外的行为自动智能的进行告警（提供截图证明，加盖原厂商章）
		可以自动对比不同时期的行为模型，以区分其审计日志数趋势、用户、IP 地址、工具、访问权限的差异情况（提供截图证明，加盖原厂商章）；
		提供审计策略和系统配置信息的单独导入、导出功能；
13	实时监视	提供用户界面告警、Syslog 告警、SNMP 告警、邮件告警、短信告警、ftp 告警等六种方式
		支持本地和数据中心查看 CPU、内存、磁盘、网口、运行状态等信息
14	系统管理	采用 B/S 架构管理，支持中英文两种管理界面（提供截图证明，加盖原厂商章）
		支持离线手工自动升级，升级数据和配置均需保留
		支持三权分立，系统默认设定系统管理员、规则配置员、审计查看员、操作日志查看员等角色
15	故障排错	系统内置独立的故障排错系统，可以支持一键导出加密的系统调试日志，支持一键检测服务、许可证、流量等大部分常见常见故障的检测（提供截图证明，加盖原厂商章）
		支持流量分析功能，包括抓包、包内容查看、自动探测 sql 语句等（提供截图证明，加盖原厂商章）；
16	产品资质	所有资质必须为数据库审计产品专有的资质，不能是网络审计产品或者综合审计的产品资质： 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》，数据库安全审计国标-增强级（提供复印件，加盖原厂商章）； 要求内置的数据库扫描系统也通过国家相关部门的认证和检测，并获得独立的销

		售许可、涉密资质（提供复印件，加盖原厂商章）
17	▲保修	三年原厂硬件质保
18	▲其他	提供原厂商授权函及售后服务承诺函（加盖原厂商章）

（7）日志审计系统

序号	技术指标	技术要求
1	工作模式	独立完成审计日志采集，不依赖于设备或系统自身的日志系统； 审计工作不影响被审计对象的性能、稳定性或日常管理流程； 审计结果存储于独立存储空间； 自身用户管理与设备或主机的管理、使用、权限无关联； 提供全中文 WEB 管理界面，无需安装任意客户端软件或插件
2	功能扩展	采用解决方案包上传对产品进行功能扩展，无需要代码开发。
3	日志收集	支持 Syslog、SNMP Trap、OPSec、FTP 协议日志收集； 支持使用代理(Agent)方式提取日志并收集； 支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等； 设备厂家包括但不限于：Cisco(思科)，Juniper，联想网御/网御神州，F5，华为，H3C，微软，绿盟，飞塔(fortinet)，Foundry，天融信，启明星辰，天网，趋势，东软，Nokia，CheckPoint，Hillstone(山石)，安恒，珠海伟思，BEA，中国电信，安氏，帕拉迪，apc，arbor，clam，戴尔（dell），digium，东方电子，EMC，中国电力科学研究院，Eudora，google，冠群金辰，linksys，Mcafee，netapp，NAS（美国国家安全局），永达，sonicwall，vigor，天存，西岭，Symantec（赛门铁克），Hardened-PHP，foundertech(方正)，三零盛安，allot，蓝盾，IBM，金诺网安，网威，nortel(北电)，citrix(思杰)，watchguard，中兴，阿帕奇，WINDOWS 系统日志，Linux/UNIX syslog、IIS、Apache 等； 支持常见的虚拟机环境日志收集，包括 Xen、VMWare、Hyper-V 等
4	性能监控	▲能够通过在目标主机上按章 agent 程序，支持监测目标主机的 CPU 利用率、内存使用率、磁盘使用情况、流量等信息、监测结果正确并支持设置报警阈值（提供公安部计算机信息系统安全产品质量监督检验中心检验报告，加盖原厂商章）。
5	产品要求	产品获得公安部计算机信息系统安全产品销售许可证（提供证书复印件，加盖原厂商章）； 所提供的产品检验报告须符合《信息安全技术日志分析产品检验规范》（提供完整检测报告（行标三级）复印件，加盖原厂商章）； 获得中国信息安全认证中心颁发的《IT 产品信息安全认证证书》（提供证书复印件，加盖原厂商章）； 检测标准符合 ISCCC-TR-056-2016《日志采集与分析产品安全技术要求》（提供完整检测报告，加盖原厂商章）。
6	硬件性能	软硬一体化设备，日志解析处理能力：≥8000EPS，网络流量：≥800Mb；日志容量：≥1.5 亿条；支持审计 100 个以上日志源；
7	日志备份	可设置日志存储备份策略，包括系统日志保存期（180 天）、磁盘使用率百分比；支持日志备份自动传送到远程服务器；
8	关联分析	产品维护一个安全知识库和包含资产信息的弱点库，当接受到针对制定资产并且匹配到弱点库中指定漏洞攻击时会触发与安全知识库、弱点库的关联。
9	日志查询	支持 B/S 模式管理，支持 SSL 加密模式访问；

		支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、技术方式、技术动作、技术效果、攻击类型、地理城市等参数进行过滤查询； 支持用任意关键字对所有事件进行高性能全文检索； 支持可指定多个查询条件进行组合查询； 支持将查询的条件存储为查询模版，方便再次使用； 极高的日志高查询性能，支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果。
10	弱点管理	▲支持导入安恒应用弱点扫描器、绿盟极光扫描器等扫描报告，可进行统一检索、并支持计算威胁等级（提供公安部计算机信息系统安全产品质量监督检验中心检验报告，加盖原厂商章）。
11	告警功能	可预设置安全告警策略； 支持数据阀值设置，超过阀值将产生告警; 可以通过邮件、短信和屏幕显示进行告警；支持自动防止报警信息在短时间内大量发送(告警抑制)；具备报警合并和在一个时间段内抑制报警次数的能力。
12	综合查询及报表管理	内置合规性报表 1000+种； 内置 SOX、ISO27001、WEB 安全等解决方案包 内置完善的等级保护合规报表（提供截图证明，加盖原厂商章）。 内置综合性自动化审计报告；支持用户自定义报表；自定义的报表支持多个统计维度的数据集合；支持报表导出为 PDF 和 Word 格式文件。
13	用户管理	根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，审计员只负责查看相关的审计结果及告警内容；日志员只负责完成对系统本身的用户操作日志管理。 系统自带自身管理日志 ▲注册用户资产时，提供自动发现识别能力，提供一键式故障排除功能。提供自助式的升级接口，支持对产品升级、规则升级（提供截图证明，加盖原厂商章）。
14	部署方式	支持分布式部署；支持集中式管理和升级模式； 支持分级管理模式； 采用 B/S 架构操作方式，无需客户端安装。 支持监控设备自身 CPU、内存、磁盘等工作运行状况
15	▲保修	三年原厂硬件质保
16	▲其他	提供原厂商授权函及售后服务承诺函（加盖原厂商章）

（8）网络管理平台

序号	功能指标	参数要求
1	稳定可靠	1、原厂商有通过 CMMi-4 级或以上的软件质量证书认证（提供证书复印件，加盖原厂商章）。 2、原厂商产品具备有效的公安部安全管理平台测试和认证（提供证书复印件，加盖原厂商章）。 3、原厂商具备 3 个以上省内公安行业用户的案例（提供合同关键页复印件，加盖原厂商章）。
2	系统平台	1、必须基于 Java 的开放式平台开发。 2、可以部署在目前流行的操作系统之上例如 Windows 和 linux 平台上。 3、系统可以运行在各种流行的关系型数据库系统之上。 4、采用 B/S（Browser/Server）模式。

		5、支持多采集器分布式部署，减少服务器数据采集压力。
3	网元数量	1、至少能同时管理网络设备、服务器、数据库、中间件、业务系统,共计 200 个网元。
4	网络管理	1、系统能够对符合 SNMP 标准协议的交换机、路由器、防火墙、均衡负载等网络设备进行监控。 2、系统能够自动发现网络设备间的链路和网络设备与计算机间的链路，手动添加单体资源（设备）可自动生成链路，能监测链路的上行、下行带宽利用率和速率、上行和下行的丢包率、错包率；链路连通状况。 3、能够对设备进行手动刷新，重新计算链路与刷新物理信息；能手动对全网链路计算与发现，计算发现过程为自动。 4、可在原有拓扑情况不变的情况下手动发现指定的两台设备之间的链路，并自动计算链路两端接口。
5	服务器管理	1、系统能够支持监控多种主流操作系统，包括 Windows 2000/2003/2008 的 32 位/64 位等各版本、RedHat Linux AS、AIX、Solaris、HP-UX 等。 2、服务器操作系统各种详细信息，如文件系统信息、系统日志信息、系统版本信息。 3、服务器运行指标包括多个 CPU 中每个 CPU 的实时负载情况；物理内存、虚拟内存及页面文件的实时使用率；磁盘每个逻辑分区的分区容量；进程运行状态等；CPU 温度、网卡实时连接及流量、网络端口的丢包率、利用率、发送速率等指标；安装软件的情况等自定义指标项。 4、服务硬件管理监控，CPU、内存、磁盘等硬件状态。 5、系统能够支持通过自定义 SNMP OID 脚本，采集特殊的服务器特殊指标项。 6、系统支持单设备手动刷新；系统能够对设备进行手动刷新，重新计算链路与刷新物理信息。
6	数据库管理	1、支持的数据库类型 sqlserver2005,sqlserver2008,sqlserver2012,oracle、mysql 等。 2、系统能对核心业务系统的数据库进行有效的监控和管理。 3、数据库管理的功能包括：对数据库的表空间进行容量规划，并能够对表空间的使用情况进行定期分析和预警；实时监控当前数据库连接、监听器的管理并能够在连接数据库出现问题时告警；对数据库的碎片情况进行监测；对 SQL 的执行效率进行分析。 4、数据库的监控包括配置的连接监控、语句的执行情况监控、数据库的性能及其阀值的监控。 5、数据库监视器实例对数据库连接失败、执行语句失败、性能阀值越界产生报警事件。
7	中间件管理	1、支持的中间件类型 tomcat ,DB2,IIS,apache,tuxedo, jboss, weblogic, websphere 等。 2、对中间件的管理是通过模拟监视和性能指标两种方式进行：实时监控当前中间件的连接响应时间、监听器的管理模式，能够在连接中间件出现问题时告警检测。监控中间件的响应时间、请求数、传输速度、内存总数、连接数等等诸多指标，并可直观了解所在服务器的性能和使用情况。
8	资产管理	1、提供整合的资源监控和管理模块。把大量信息，按用户的的管理思路和管理目标整合在一起，方便用户查看和管理。资源列表提供管理一览和实时一览，并提供自定义排序 。 2、本模块可以融监控、CMDB、报表、快照、知识库、体验化于一体。 方便用户从各个方面来监控和管理系统的软硬件资源。结合资源监控和 CMDB，并在监控和 CMDB 中，均提供模板的功能，方便用户快速部署和调整多个资源监控和 CMDB 的各个子窗口都支持展开收缩，方便用户关注最重要的信息。 3、CMDB 可以管理设备的保修和服务信息，并及时提醒用户续保，；并可以展

		现设备的图片信息和物理信息（如高度、功率等），帮助用户进行管理。 4、CMDB 支持二维码扫码查看功能，扫码即可查看设备的详细情况，并且在巡检时扫二维码即可查看信息，方便巡检。 5、提供快照功能，用户可以把网络异常瞬间的各个设备和资源的情况生成快照，以便后续对指标和关联性逐项分析。
9	▲模板管理	1、提供通过“模板”来设置指标轮询周期、阈值和异常等级、告警方法、异常过滤和告警过滤。对于很多规则相同的设备或资源，直接运用模板即可，改变上述设置，也只要更换模板即可。 2、用户可以通过模板设置通断指标、性能指标、扩展指标、安全指标、自定义指标、复合指标和配置指标等等。也可以直接启动或停止不同类型的指标，可以批量将模板适配到不同设备。 3、系统提供各种内建模板，至少包括 SNMP 网络设备模板、Windows2003 模板、Windows2008 模板、LinuxAS4 模板、LinuxAS5 模板、HP-UX 基本模板、HP-UX 告警模板、AIX 基本模板、AIX 高级模板、防火墙模板、Oracle 数据库模板、SQLserver 数据库模板、各中间件模板等等。 4、用户可以通过设备选择不同模板，实时改变设备的监控策略而无需重新启动系统，也可以把模板批量应用于各设备。通过模板，可以很方便地引导用户设置指标，达到化繁为简，协助和帮助用户人员进行管理的目标。 5、分时模板可根据用户在高峰期或闲置期，根据使用情况调整多个关键指标的阈值大小，根据不同时间段的需求，灵活设置对应的阈值规则。
10	▲拓扑展示	1、全 BS Flex 拓扑图，拓扑图功能完全通过浏览器操作。 2、拓扑图管理提供高效的展示模式与自定义布局功能，用户可以在展示模式中根据网元数量等迅速找到适合自身网络环境的图元拓扑，在自定义布局模式中有各种视图表现形式、各种链路类型和各种图元类型，布局至少包括（径向类、树状、坐标类、蜗牛状等）类型，图片布局至少包括（图片类、图片鱼眼、小圆点类、小圆点鱼眼等）类型，链路样式至少包括（默认、方向箭头、方向气球、正交、流模式、贝塞尔曲线、磁线）等类型。 拓扑图展示层数和链路连线长短可以方便自定义。用户选择不同效果后界面能自动动态重新排列，效果美观。 3、拓扑支持分层分级展现，用户可以选择不同层数来控制大规模的拓扑图的展现。用户双击图元可以自动实现图元居中重排。运行状态和指标能实时展现在拓扑图上，并可以有鼠标位置展现和常展现两种不同状态。 4、拓扑图中可以提供搜索和整体概况，整体概况提供各种 Flex 的动态统计展现效果，能让用户不离开视图模块就能了解本视图的整体运行情况（如本视图上设备的统计、性能、异常等等），将视图功能拓展到视图代表的整体管理概念。 5、用户可以选择视图的实时镜像，可以在“我的”的模块中，和其他展现项（如指标、设备情况、性能曲线等），在一个页面中并列展现。 6、用户可以根据自己的需求选择不同的刷新模式，分为系统页面刷新时间和实时数据刷新 7、用户可以创建业务拓扑图，实时了解业务的结构与状态。 8、用户可以创建机柜拓扑图，自动化排列模拟用户现场 3D 机柜拓扑图场景，自动匹配体验化背板图片，打造设备图元真实性。 9、拓扑图支持上传图元背景功能，更好的美化拓扑图，便于展示。 10、用户添加 2 个设备间链路时，软件自动发现链路并计算出设备接口关系，方便准确。
11	整体管理	1、能在一个页面上提供系统总览、异常一览、报表一览、我的关注。把系统的各个方面的情况及时反映。 2、能把多个重要的网络设备、服务器、应用、防火墙、业务、网站等等设为我的关注，能显示这些设备的实时运行情况和历史运行情况。

		3、能按类型、等级、是否确认、是否恢复、时间等来筛选展现当前和当天异常，能展现异常发生到现在的时间（MTBR），并能直接通过远程消息将异常信息通知设备的管理人，用户也可以在这个界面直接确认异常。 4、此页面能展示当前生成的报表。 5、此页面有“我的秘书”组件，能实时展现在线用户和不在线用户，能给用户发短信、邮件、远程消息。也能查看我收到的消息记录。 6、能通过图形方式，实时展现网络设备、服务器、链路、服务、业务和应用的不同状态数量（健康、亚健康、可用、不可用），并能通过鼠标点击后，实时查看哪些设备亚健康或哪些设备不可用，实时进行管理。
12	我的界面定制	1、提供“我的”界面。 能让用户在一个页面上配置多个组件，支持第三方界面直接嵌入。 2、组件类型包含“指标分析”“单个资源一览”“指标一览”“TopN”“拓扑图”“我的异常”“IPMAC 异常”“收藏夹”等等。 3、用户可以根据不同的情况，定制不同的展示组合。将上述的组件灵活搭配。同样的组件在一个页面也可以部署多个。为了适应用户的不同需要，本页面支持一列排列、两列排列、三列排列。在使用过程中，用户也可以随时切换而不需要重启服务。 4、所有组件支持拖拽的方式实时调整位置和排列。 5、系统所有界面都提供换肤功能，至少提供三种不同的界面风格（如正规色系，炫酷色系，节庆色系、灰色经典）等等，适合不同场景（如评审、会议、领导视察、日常管理、屏幕投射）等等场景。
13	告警方式	1、系统支持多种告警方式，包括拓扑图图标颜色变化告警，异常列表告警，消息框告警，声音告警，短信告警，微信告警，邮件告警，关闭网络端口告警、运维告警等方式。 2、用户可以自行灵活组合，生成新的告警方式。 3、后期采购硬件后可以支持语音电话告警、声光告警。 4、微信告警，及时的微信报警推送，方便用户有网情况下，随时随地了解到故障详情，节省短信使用成本。
14	异常处理	1、系统能够对各监测指标偶然产生的波动，可自动进行判断，避免误报事件，告警敏感度的设置可以精确到每个不同的指标。 2、系统能够分时对不同的异常和告警生成过滤条件并进行过滤，可以精确到每天的不同时间以及不同的异常判断和不同的告警判断。 3、系统在一段时间内对连续性的同一故障只报一次警，避免告警风暴。时间可以灵活设置。 4、支持故障智能依赖树配置，找出故障真正的来源，系统能够通过异常依赖树智能分析各个异常间的逻辑关联关系，提供根本原因分析,快速发现故障根源，缩短恢复时间，防止告警泛滥。
15	报表和订阅	1、报表系统支持自定义和内建报表模板，模板可以分为内建、公共、个人、共享模板； 2、报表支持订阅、退订。 3、报表种类有日周月年报表和快照报表和一日内不同时段报表。 4、运行周期有一次性报表和周期性报表。 5、报表有类型时段报表、快照报表和单设备详细报表。
16	分析和统计	1、报表系统支持高效灵活的类 Mrtg 的性能分析。可以实时统计分析每次轮询数据、30 分钟统计、2 小时统计、日统计等多种实时统计和数据保存。 2、用户可以在一个屏幕上，同时展现各指标（如接口速率）的每次轮询、30 分钟统计、2 小时统计、日统计数据，并可以分成日曲线、周曲线、月曲线、年曲线进行图形趋势分析。 3、用户还可以自定义时间段来分析各个指标的历史情况。 4、支持多设备多指标分析，用户可以对多个设备的多个指标在指定的同一个

		时间段内进行对比分析，给用户提供多角度数据分析参考，并可将分析数据导出到 Excel。
17	故障分析	1、系统可以方便用户实时查看系统中的不同异常类型（当前、今天、昨天、本周、本月），并能筛选出（已确认、未确认、已恢复、未恢复、手动恢复不同异常等级、不同异常来源类型）等不同状态。 2、在查看和筛选时，同一屏幕上，可以通过立体饼图和立体柱状图动态展现不同等级和不同种类异常的各项分类数据和总数。用户可以操作和点击图形来减少分类类型，图表能实时动态重构。 3、用户也可以在异常列表上实时进行确认、恢复、手动恢复、删除等各项操作，手动恢复可将不重要的故障进行手工恢复。 4、故障信息支持与运维管理软件相关联，故障产生后可快速生成故障工单，严格按照标准 ITIL 流程理念进行处理和结果跟进。
18	个性化订制	1、用户可以通过个性化设置，简单在界面上定制用户的单位名称、系统名称，体现最佳客户满意度。
19	整体轮换	1、系统可以自动在多个界面自动轮换。包括但不仅限于（整体页面、我的页面、故障页面、分析页面）。 2、同时用户能够自行选择和定义要参与轮换的页面信息。 3、为适合不同用户，用户可以自行定义页面轮换间隔时间（如 15 秒、30 秒、40 秒、1 分钟、2 分钟、3 分钟、5 分钟）。 4、对于轮换可进行暂停与开启的模式， 自动轮换的客户端只需要标准的 B/S 浏览器，不需安装任何客户端。
20	地域和权限管理	1、系统可以把不同资源分为不同管理域，对不同的网管功能，给不同的角色分配不同的权限； 同时给不同用户分配不同的角色以及不同的地域。 2、通过立体化多维化的地域和权限管理，构建智能化的权限和视图管理，并保证高效管理和严密权限相结合。 3、同时，系统建立独立的用户中心，方便和运维系统等等其他系统的用户密码统一管理。
21	面板展现	1、能直观的看出每个设备的真实背板情况及设备接口的连接信息。 2、通过真实的设备背板图可以对设备的各个端口进行实时查看、打开和关闭等操作，能及时查看各个端口的基本信息,接口列表可监控指标当前值，如健康度、接口输出或输入速率以及接口状态等信息。 3、当某个交换机出现异常速率或者异常流量时，能够提醒及时把相对应的端口宕掉。
22	带宽管理	1、带宽管理能够获得广域网各线路的带宽与实际利用的带宽情况，管理者就可以第一时间的掌握网络设备的连接情况，并根据具体的连接情况做相应的处理和记录。
23	指标系统	1、系统提供高度灵活性的指标系统，包括通断指标、性能指标、扩展指标、安全指标、自定义指标、复合指标、配置指标等等。 2、可以灵活设置不同类型指标的轮询周期、阈值、异常策略、告警方法、异常过滤方法和告警过滤方法。 3、 支持设置多阈值策略，可设置交集或并集阈值策略，以适应多种设置场景以避免遗漏特殊告警。 4、用户可以自定义 SNMP 采集器、SQL 采集器、Tcp 采集器来采集各种系统的各个实时指标，并在拓扑图、实时运行情况等等界面展现。 并能提供实时健康度和可用率等等服务水平相关指标。 5、 系统管理来自系统主动定时轮询的轮询指标以及设备即时上报的 Trap/Syslog 信息生成的指标。 6、 为了能避免重复告警，能智能分析根源，轮询指标和 Syslog/Trap 指标必须在统一的处理渠道中合并处理。 7、 对于同一指标的高峰时段和非高峰时段，可以设置不同的阈值和不同的异

		常规则。 8、支持指标轮询周期、阈值和异常等级、告警方法、异常过滤和告警过滤。可自定义 ssh、telnet、SNMP、tcp、SQL、ping 取值，SSH 取值和 TELNET 取值在同一模块中，提供 SSH 和 telnet 取值模版和方式不低于 15 个模版，snmp、sql 模版不低于 5 个。
24	智能巡检	1、支持按不同巡检内容和设备制定周期性的定点智能巡检,自定义添加检测点,构建巡检规则。 2、以模板规范标准值为依据,根据预设的要求进行数据采集,进行自主分析判断,进行定期巡检 。 3、以报表的形式直观反映巡检结果,将巡检异常状态以告警灯形式展现,快速反映本次巡检的异常, 越界次数、标准值和当前值的差异性,系统会定期生成并主动发送运维人员 。 4、支持对系统监控巡查的整体进行评价和备注说明,导出多种格式向领导汇报,避 免传统的签到纸张的损坏、备注信息不全。 5、工作核查繁琐未如期巡查、巡检报表 乱写等问题。
25	工具模块	1、集成常用网络诊断和分析工具：Ping 、TraceRoute、NetBios、NetSend、链路延时、SNMP 连接 测试、TCP 端口扫描、实时表查询、Telnet&ssh、Mibbrowser（测试 OID 节点）。
26	日志管理	1、网管支持系统操作日志的记录，记录设备管理用户登录登录设备成功或失败信息，包括登录名、登录结果（失败原因），登陆时间，日志类型等，日志可以导出到 Excel 表格中。
27	系统备份恢复与数据维护	1、支持检测和查看数据类型的范围和容量。 2、支持一键备份与定时备份功能。 3、支持数据备份结束以客户端和消息进行通知。。 4、支持下载数据到任何终端 5、支持一键恢复和上传数据恢复。 6、通过核心数据存储设置，自定义保留用户最为关心的数据指标。 7、对系统性能数据、异常数据、报表数据、日志数据进行当前容量的检测，并可设置超过阈值告警方式，执行立即清理功能，为系统数据做瘦身。
28	资源管理	1、系统可以提供 IP 地址/信息点/VLAN 管理功能，方便用户输入和管理 IP 地址/信息点/VLAN 管理的信息，并将设备、IP 地址、信息点、物理位置/布线系统、VLAN 等等信息集中管理和保存，也可以方便查询。避免这部分管理信息遗失或散乱。 2、IP 地址管理，统一规划分配 IP 地址给每台终端机器，并建立 IP 地址分配基准表通过自动扫描，快速的查找网络中正在使用的 IP 地址，也可以手工设置要分配的 IP 地址，直观的了解和掌握整个网络的 IP 地址资源使用情况同时 IP 地址管理将与 IPMAC 绑定实时联动，各类状态：正常、占用 IP 且 PING 不通、非法使用 IP，每个地址是否在用，当前是否在线，计算机的名称，子网掩码 MAC 地址等的数据实时显示，当指定的 IP 地址或地址空间出现变更时立即获取告警通知，同时支持恢复基准分配地址。
29	配置管理	1、配置管理支持自定义 telnet 命令获取配置信息，以适应各类型的网络设备。 2、支持对各种网络设备如交换机、三层交换机、路由器、防火墙、负载均衡等配置信息的查询、查看、保存、对比、备份。 3、通过对配置文件与基准文件的对比，系统以状态灯（图元）形式表示配置变更的状态，红色表示配置产生变化，绿色则表示配置未变化。直接点击红色类态灯，即可对配置文件进行查看，并可以自动对配置文件进行实时比较。 4、另外，当配置发生变更或产生异常时，系统则会根据设定的相告警方式进行告警。 5、系统的对比检测，可以实时维护网络设备配置。

30	IPMAC 管理	1、系统可以动态实时做到终端准入控制的功能。 2、对交换机网络下，系统支持 IP-MAC-PORT 3 者之间的绑定，并可以查看 3 者之间的绑定关系，如 IP 地址与 MAC 地址的关系，MAC 地域与交换机端口的关系，同时还能由 IP 地址查找到该 IP 的 MAC 地址及该 IP 所连接的交换机端口。 3、通过 IP-MAC-PORT3 者的绑定，可以查看基准表信息、实时表信息、实时表与基准表信息比较后的差异信息、差异处理信息等。。 4、支持以实时图形化的方式查看接口利用率、速率、流量等 TOPN 运行数据情况。 5、支持自动生成快照轮询策略，定时进行 IP 使用情况进行巡检记录，并可以通过差异告警配置，对网络环境中出现的 IP 变更、新增终端及终端变更等异常进行告警.有助于用户及时掌握网络环境动态。 6、对未经许可上网的终端，可以采取告警，自动断网等等多项措施。 7、用户可对已知的 ip、mac 地址变动信息进行手动确认，确认后软件会在基准表中添加最新信息，避免频繁重复告警，提高工作效率。
31	多屏大屏幕展示	1、大屏幕数据实时采集，采用炫酷的动态图形展示，将概览统计，核心资源监控、趋势分析、TOPN、拓扑图、业务系统运行情况（繁忙度和响应时间，下属状态），服务器运行状况、中间件数据库运行状况、网络运行状况、机房运行状况、安全告警状况等等，以动态方式在展示中心多个或单个大屏幕上全屏集中展现。 2、灵活部署和多屏展示，支持不同分辨率，可根据多屏或单屏自定义配置多个界面，灵活部署在各类拼接屏或单屏轮换进行展示。 3、内建数据展示模板智能匹配，根据不同的行业满足用户业务、IT 资源、网络结构等各场景的展示需求。 4、多种类型组件数据支持、图形化编辑界面，通过简单拖拽即可配置灵活易用的自定义组件，轻松部署各视角核心数据展现。
32	▲保修	三年软件升级、原厂质保
33	▲其他	提供原厂商授权函及售后服务承诺函（加盖原厂商章）

（9）网络管理平台服务器

序号	指标项	技术参数及技术要求
1	处理器	单颗处理器核数≥6 核，主频≥1.6GHz，缓存≥15MB；本次配置处理器数量≥1
2	内存	≥24GB DDR4
3	硬盘	≥2*300GB 2.5 寸热插拔 SAS 硬盘
4	RAID 卡	支持 RAID 0/1，缓存≥2GB
5	网卡	≥4 个千兆电口
6	电源	1 个热插拔电源
7	其他	集成阵列卡(支持 Raid0/1)，DVD 光驱
8	▲保修	三年原厂硬件质保

2、视频专网

（1）边界防火墙

序号	指标项	指标参数
1	▲基本配置	标准 2U 设备,双冗余电源；≥6 个 10/100/1000M Base-TX 接口，≥4 个 SFP 接口；
		最大并发连接数 320 万，最大吞吐量 12Gbps，每秒新建连接数 10 万

		配置 IPS 模块，三年质保
2	网络适应性	支持静态路由，动态路由（OSPF、RIP、BGP、ISIS 等），VLAN 间路由，单臂路由，组播路由等。
		支持基于应用的策略路由，可实现为不同的应用类型智能选择相应的链路。
		支持基于文件类型的策略路由，可实现将预定义或者自定义的文件按照不同的分类进行智能选路。
		支持多出口路由情况下的默认路由备份、负载均衡。
		支持 ISP 路由，支持联通、电信、教育网、移动等 ISP 服务商地址列表，列表可导出及导入，可通过 Web 界面选择不同的 ISP 服务商实现快速切换。
3	网络管理	支持 DHCP Client、DHCP Relay、DHCP Server。
		各种工作模式下均支持 H.323（H.323 GK）、SIP、FTP、MMS、RTSP、XDMCP、TNS 等多种动态协议。
		支持对虚拟环境的数据流进行全策略控制。
		支持链路聚合功能，支持 802.3ad 和静态轮询、热备等多种模式，MAC、MAC&IP、IP&Port 多种聚合负载算法。
4	网络访问控制	支持一体化安全策略配置，可以通过一条策略实现用户认证、IPS、AV、URL 过滤、协议控制、流量控制、并发限制、新建限制、垃圾邮件过滤、审计等功能,简化用户管理。
		支持将源 MAC 作为独立的访问控制条件，防止非法设备接入。
		支持基于数据包的安全域、地址、用户及用户组、MAC、端口号、服务、域名等进行安全策略控制 。
		支持以组的方式管理安全策略，支持安全策略组的增、删、改操作，简化安全策略管理。
		支持针对策略中的源、目的地址进行并发限制，可以针对单 IP(或地址范围)进行并发控制。
		支持针对策略中的源、目的地址进行新建限制，可以针对单 IP(或地址范围)进行新建控制。
		支持策略命中数显示，并支持通过安全策略命中数范围查询。
		支持根据 IP 地址进行策略查询、支持根据服务端口进行策略查询。
		支持根据规则序号、规则名、源地址、目的地址、入侵防护策略、服务、认证用户、认证用户组、所属策略组、备注进行规则查询。
		支持查看资源被访问控制策略引用情况。
		支持查看访问控制策略引用地址、服务、时间资源情况。
5	服务器负载均衡	至少支持两种方法主动探测服务器的存活状态
6	入侵防护	支持基于策略的入侵检测与防护，可针对不同的源目 IP 地址、源 MAC 地址、服务、时间、安全域、用户等，采用不同的入侵防护策略。
		入侵防御特征库库至少应包括信息窃取、木马后门、间谍软件、可疑行为、网络设备攻击、安全漏洞及网络数据库攻击等的特征事件。
		支持细粒度的自定义 IPS 特征功能，支持 DNS\HTTP\FTP\TFTP\TELNET\SNMP\POP3\SMTP\IMAP\等 17 大类应用层协议的自定义，可以精准设置各个协议字段内容，例如字符内容、偏移、长度等细粒度的参数。
		支持对网络扫描行为的检测和过滤，可实现基于端口的扫描防护和基于主机的扫描防护。
		支持 IP/MAC 地址绑定的方式防止 ARP 欺骗，可采用手动建立或自动探测的方式生成 IP/MAC 对。

		支持多接口的攻击行为监听检测方式，可并行旁路检测多个网段内的网络攻击行为，用于高可靠性要求的旁路应用环境。
		至少支持丢弃封包、切断会话、攻击重定向、记录日志、邮件报警、声音报警 7 种响应方式。
		支持实时的入侵防护事件分级报警列表，可按事件的源 IP、目的 IP、协议、时间等显示；通过不同的入侵防护事件实时阻断入侵源 IP，阻断时间可控，提供入侵防护事件分级列表界面和实时阻断界面。
7	抗拒绝服务攻击	支持主流 ICMPFLOOD\SYNFLOOD\ACKFLOOD\SYNACKFLOOD\UDPFLOOD 攻击防护，采用专业高效的攻击防护算法，非采用简单的阈值进行攻击防护
		以上主流的功能，支持基于源 IP 限速、基于特征过滤系数、聚类限速系数、重传检测、自学习白名单等多种防御机制。
		支持专业的 DNSflood 攻击防护，具有高级的基于聚类限速、聚类分析、重传检测等多种高级防护算法。
		支持专业的 HTTP Flood 攻击防护；可以实现 get 和 post 的攻击防护，且 get 防护算法支持 4 类；支持独立 url 处理动作；以上防护功能均可以基于聚类分析、可信度、回探等多种防御机制。
		支持抗地址欺骗攻击、抗源路由攻击、抗 Smurf 攻击、抗 LAND 攻击、抗 Winnuke 攻击、抗 Queso 扫描、抗 SYN/FIN 扫描、抗 NULL 扫描、抗圣诞树攻击、抗 FIN 扫描、抗 Fraggle 攻击。
		支持自定义攻击日志的生成频率以及每时间段所需要记录的告警日志数目，攻击日志能够准确记录时间、攻击源目的、攻击类型、攻击次数等信息。
		支持攻击流量统计、攻击事件统计、攻击流量排行、攻击事件排行。
		支持 web 界面下对攻击流量进行抓包分析，支持自定义抓包参数，至少包括数据报文长度、报文数量、抓包时间及采样频率等基本参数；支持根据协议、源目的 IP、端口等参数进行数据报文过滤。
		支持对本地抓包文件的管理，包括下载、删除等操作，同时支持 FTP 方式将抓包文件上传至指定的 FTP 服务器中。
8	统一认证管理	支持多人使用同一帐号登录。
		支持在用户认证失败的情况下仍提供基本的网络访问权限。
		支持对 WEB 认证、LDAP 认证、RADIUS 认证、邮件账号认证、IP 识别用户的强制下线。
		支持用户的 AD 域、POP3、BJCA 单点登录，支持自定义单点登录监听端口。
		支持设置认证服务器组。
		支持用户口令复杂度设置。
		支持显示详细的用户在线信息，包括用户名称、真实姓名、所属组、认证源、接入方式、认证方式、登录 IP/MAC、在线时间、登录时间和可对其进行相关操作。
9	主动防御	支持 IPv4 和 IPv6 双栈协议下的主动防御。
		要求支持主动防御功能，对服务器、主机进行后门、服务探测、文件共享、系统补丁、IE 漏洞等主动式扫描。
10	安全日志	支持至少 2 个 Syslog 服务器，发送流量、系统或默认 2 类型日志到不同服务器。
		支持日志中文化，可显示配置命令日志的操作人。
		支持在三权分立模式下，对日志文件的加密导出/导入
11	高可用性	支持端口联动，支持上下行端口组的联动，可以实现单端口决定同组中的任意接口失效启动链路切换。

		自动同步、心跳接口多级（≥2 级）物理备份。
		可在热备和集群工作模式下支持多台防火墙的会话、配置的实时同步、手动同步。
		支持多重冗余协议(MRP)，实现链路备份、端口冗余、双机热备份、集群备份等。
		支持基于 VRRP 技术的热备和负载均衡。
		在 NAT、路由、透明模式下支持 A-A,A-S 模式，且切换时间小于 1 秒 。
12	▲保修	三年原厂硬件质保

（2）终端准入控制系统

序号	指标项		指标参数
1	基本要求	▲系统要求	具有独立自主知识产权，须为标准机架式硬件产品，除自身硬件设备外，产品功能的实现无需额外增加服务器等设备。
		▲性能要求	配置 6 个千兆电口；每秒事务数（TPS)：≥6000（次/秒），最大吞吐量：≥2.3Gbps，最大并发连接数：5000（条）；2500 用户许可；配置设备指纹识别模块。
		▲高可用性	1. 准入设备必须具备HA模式，HA须支持主备机心跳IP检测及虚地址管理模式，支持vrrp管理模式。 2. 提供第三方监控平台，在出现重大异常情况时能及时通知网络设备放开网络。
		语言支持	支持终端客户端、web 显示的中英文双语切换
		终端部署	1. 准入设备应至少提供安全客户端（Agent）、安全控件、无客户端等多种可供自定义部署、管理模式。 2. 安全客户端模式部署时，客户端程序应支持功能定制，以降低系统资源耗用，提升客户端兼容性。
2	准入架构	终端发现	1、 能够实时监测并发现接入内网的PC、平板电脑、智能手机、IP设备等终端，能够在第一时间隔离阻断并通知管理员。 2、 对自动发现的终端能够按照类别自动归类，以方便网络终端的统计管理（提供截图证明，加盖原厂商章）。
		准入技术	1. 准入设备须原生支持802.1x标准协议，无需第三方RADIUS服务器支持。 2. ▲准入设备支持基于多厂商Virtual Gateway的VLAN隔离技术，实现无客户端环境下端口级准入控制（提供截图证明，加盖原厂商章）。 3. 准入设备支持基于策略路由技术的准入控制模式，入网设备在访问网内关键资源时，将被强制隔离、引导至认证管理页面，同时支持交换机接口动态VLAN下发、端口隔离模式的网络边界管理。 4. 单台准入设备可支持至少2个核心交换机进行策略路由准入控制。 5. 准入设备可支持端口镜像准入技术，通过对交换机镜像数据的实时分析，能够及时发现并阻断非授权终端的接入。 6. 支持使用802.1x MAC认证时，记录详细的认证信息，包括:认证的时间、认证类型、认证的MAC、认证是否成功等，并支持报表记录。

		定向引导	1. 支持终端入网IE重定向引导，当用户访问网页时能够自动转向到指定的页面或地址，并支持http代理及多重重定向引导。 2. 可根据用户的实际环境自定义非80端口的Web服务端口号及用户重定向引导。 3. 能通过浏览器完成身份认证、控件安装、设备注册、安全检查、检查结果展现等全流程引导管理。 4. ▲具有Mac OS、Linux、iOS、Android等系统专属客户端，支持认证引导和准入管理（提供截图证明，加盖原厂商章）。
3	违规外联	▲违规外联	1. 能够针对3G拨号、双网卡、随身WIFI、代理等多种违规联网行为做实时检测，不接受间歇性ping外网地址的探测方式。 2. 能够针对违规外联终端进行即时断网，断网方式应支持断开链接、关闭连接进程、断网后重启恢复、重启计算机等多级模式，并能够实时通知管理员。 3. 准入设备能够支持按照用户角色定义、限制员工的内网访问范围，防止其越权访问操作。 4. SSID白名单，可对连接到白名单之外的无线网络行为进行阻断（提供截图证明，加盖原厂商章）。
4	边界管理	IP/MAC 绑定	具有入网设备自动学习功能，支持 IP/MAC/端口三者强制绑定，以及违规终端 VLAN 隔离机制，防止终端仿冒 IP 接入网络或移动设备位置。
		主机防火墙	1. 终端在准入通过后访问域严格收管理员策略控制 2. 同网段终端无法互相访问，做到精确到端口的高安全性控制
5	设备特征指纹	设备特征指纹	1. 具有非智能IP终端信息库，能够精准识别网络打印机、网络摄像头、IP电话等设备，并根据设备特征进行自动匹配和归类。 2. 通过伪造合法IP或MAC地址的非法设备和行为，能够被即时发现并阻断。
6	设备私接管理	NAT 设备	1. ▲具有NAT识别和检测机制能够及时发现网内私接的小路由器、无线AP、随身WIFI等NAT设备，帮助清查通过网中网隐藏的真实网络终端（提供截图证明，加盖原厂商章）。 2. 对通过NAT入网的计算机可以实现准入控制、安全评估和修复等流程化管理（提供截图证明，加盖原厂商章）
		Hub 管理	1. 能够发现内网私接的Hub、傻瓜交换机等非网管设备，当多台计算机通过Hub接入网络时，能够及时产生告警通知管理员（提供截图证明，加盖原厂商章）。 2. 准入设备能够采用VLAN隔离、逻辑关闭端口等方式禁止Hub下联计算机接入网络。 3. 支持Hub下多个终端需分别认证才能入网和只需一台认证即可全部入网两种认证机制。
7	网络管理	设备识别	1. 支持自动识别网络设备类型，包括：交换机、路由器、防火墙等，并按照类别自动进行归类。 2. 支持设备管理模板的定义功能，能够通过SNMP、SSH、TELNET等方式自动、批量添加网络设备。

		▲终端网络拓扑	1. 准入设备支持交换机到终端计算机的网络拓扑管理功能，能够自动绘制出网络拓扑图（提供截图证明，加盖原厂商章）。 2. 能够在拓扑图上选取设备查看其基本状态信息、设备型号、所处位置、子节点、路由表、ARP表等信息（提供截图证明，加盖原厂商章）。 3. 支持在界面上提供对该网络设备进行TELNET、SSH等管理。
		交换机状态展现	1. 支持可网管型交换机面板图形化展现各接口状态（up、down、trunk等），以及各接口下联的终端详细信息（IP、地址、MAC地址等）（提供截图证明，加盖原厂商章）。 2. 能够支持自上而下逐级查找终端的具体位置、安全状态、认证用户、上下线时间等信息。
		AP 联动管理	能够与主流的 AP 设备深度联动，支持 AP 控制器面板的图形展现，包括 AP 连接状态、下联终端信息（IP 地址、MAC 地址等）等。
		DHCP 中继	1. 能提供稳定的DHCP服务，并可以通过DHCP二次地址分配机制实现安全准入管理，支持交换机中继认证方式。 2. 能够根据用户、IP/MAC绑定信息等条件，为指定终端设备分配特定的IP地址。 3. 支持DHCP服务器筛选，防止非法DHCP服务器分发错误地址
		DHCP 地址释放	支持 DHCP 通过管理服务器手动操作，主动进行某台主机的 IP 地址释放。实现 IP 地址充分利用。
8	移动终端管理	终端识别	支持当前主流智能终端设备的安全准入控制，能够自动识别主流手机、智能终端等设备，并自动进行分类。
		移动终端入网	1. 提供独立的智能终端入网引导界面的自主定制功能，至少包括界面标题、界面 LOGO、界面说明文字等。 2. 能够提供移动终端入网的设备注册功能。
9	认证管理	联动认证	能够全面结合用户已有的认证或业务系统，可以与 RADIUS、LDAP、STMP/POP 等采用标准协议的系统做深度联动认证。
		AD 域单点登录	1. 能够与用户现有的AD域相结合，当用户登录到AD域后，无需二次认证即可入网，避免多次认证的繁琐流程。 2. 当用户未登录到AD域时，该终端将一直被隔离，该状态下只有通过IE页面进行认证才能够入网。
		证书认证	支持至少 2 个以上的根证书。终端用户认证时，自动进行认证证书的根证书匹配
		短信认证	支持短信认证模式，用户在登记入网手机号码后，能够在手机上接收到入网的短信验证码，并在 IE 页面上利用短信验证码认证入网。
		微信认证	通过关注微信公众号放行移动终端入网
		接入审核	能够针对不同的角色或设备类别有选择的开启入网审核功能，待审核的用户或设备必须经过管理员审批才能入网。

		认证控制	支持对认证时间段、IP 段控制限制某类（角色）账户只能在指定的时间段、IP 段认证。
		自助账号申请	支持用户在认证页面自行进行账号的申请。用户可自行提交用户名、密码、姓名、电话、部门、E-Mail 等信息。管理员审核通过后，用户即可使用该账号进行认证。有效解决用户账号和密码创建和分发的困难。
10	来宾管理	来宾角色	能够提供来宾角色选择，能够设定来宾设备的访问权限和入网时长
		来宾码认证	提供临时入网码，支持来宾设备与受访人员进行一对一绑定功能
		二维码认证	通过扫描二维码进行来宾入网管理（提供截图证明，加盖原厂商章）
		来宾使用报表	生成来宾分配、来宾入网等动态审计报表
11	终端安全管理	安全检查库	准入设备须提供系统安全配置、用户行为规范等类别检查项，至少提供 24 种以上安全检查项。
		系统补丁	▲准入设备具有完整的补丁管理子系统，无需第三方补丁服务器支持，自身即可以提供完整的流程化补丁管理，包括同步更新、补丁分类、补丁分发、补丁报表等功能（提供截图证明，加盖原厂商章）。能够在 IE 页面进行入网终端的补丁检查，补丁均划分为严重、重要、中等的类别，能够在 IE 页面显示出检查结果（提供截图证明，加盖原厂商章）。
		防病毒软件	能够在 IE 页面检查出终端的杀毒软件情况，支持主流的 20 种以上的杀毒软件检查，包括微软 MSE、可牛、Avast 等，支持杀毒软件版本、病毒库和运行情况的检查，能够在 IE 页面显示出检查结果（提供截图证明，加盖原厂商章）。
		Windows 组策略检测	windows 密码策略、屏保、共享目录、弱口令、防火墙、网卡配置等系统策略进行检查和修复
		计算机健康性检测	对终端的磁盘使用率、垃圾文件、IE 主页、网络监听端口等安全性配置进行检查和修复
		自定义安全检查	通过检测终端文件路径、指定文件版本、大小、MD5，注册表的项、注册表值，进程，服务名称、服务状态，进行检查。通过安装包运行、访问站点、开关服务、关闭进程、执行文件、删除文件、修改注册表进行修复。可以灵活的全访问的对终端进行安全检查和修复（提供截图证明，加盖原厂商章）。
		终端安全加固	能够通过傻瓜式的漏洞修复模式为用户提供简单、形象的漏洞自我修复功能，完全不需要管理员的介入即可完成终端安全风险项修补。
		桌管系统联动	能够在 IE 页面检查出主流的桌面管理系统（包括 Landesk、北信源、威盾、盈高、圣博润等）客户端是否安装并正常运行，能够在 IE 页面显示出检查结果。
12	移动存储设备管理	移动存储设备管理	1. 管理员可以通过对存储介质统一注册、授权的方式来加强管理存储介质的使用范围和权限，并支持存储介质分区加密，未经标识的存储介质将不能在企业内正常使用。 2. 针对不同注册状态的存储介质制定不同的控制策略，能够对存储介质进行只读、禁用、放行、脱机生效以及时间范围等做精

			细控制。
		移动存储设备审计	1. 支持查询存储介质的类型、设备名称、设备插入时间、设备拔出时间、设备使用 IP 地址、类型代码、设备容量、厂家名称、产品名称、该存储介质使用人、操作系统用户名、备注信息。 2. 支持使用存储介质的终端信息显示，包括：设备名称、IP 地址信息、所在部门、所在位置、联系人、联系电话、E-Mail 地址、设备状态（开机、关机）、最后在线时间等。
13	资产管理	资产管理	1. 能够对全网计算机上安装的软件进行统计，可以按照部门、名称提供精确查询以及软件资产报表的导出。 2. 能够对终端硬件初始记录、最新记录和变动记录形成报表，并且能够查询变动的历史。
		资产变动	准入设备能够针对软硬件资产变动、资产异常情况提供了丰富多样的报警方式，便于管理员及时迅速了解资产信息。
		变动确认	支持管理员对每一条软硬件变动进行确认操作，已确认的条目显示已确认，并显示进行确认操作的确认人。对变动和变动确认可进行报表统计；
14	资源管理	软件检查	1. 通过安全检查检测终端软件安装、使用状态 2. 自动强制为终端安装软件 3. 软件产品授权，支持进行windows、office、WPS的产品授权信息进行检查
		IP 地址管理	1. 提供IP地址分配表，能够通过图示直观的查看各网段中未分配、开机、关机的数量和分布情况。 2. 能够直接、快捷的查看全网终端历史上线、下线、在线时长等详细的IP使用情况。
		能耗管理	提供未关机终端自动统计功能，并能够按照部门、时间段等条件生成统计报表。
15	运维管理	移动终端管理	移动端管理平台可实现设备快速定位、设备审核、实时报警监控、小助手确认码生成、准入控制器管理、平台基本信息、关机与重启
		管理角色控制	准入设备须采用系统管理员、安全管理员、审计员三权分立机制，防止单个角色管理者权限滥用。
		网络诊断工具	支持通过 Web 管理界面提供 ping、抓包、traceroute、nslookup 等功能，并可以设置命令参数进行相关调试。
		消息群发	能够支持在指定的一台或者多台终端计算机上产生桌面消息通知，该消息会立即弹出在用户桌面上，对用户进行提醒。
		软件分发	1. 准入设备应具有软件分发和部署功能，管理员可以预定义软件分发的路径、运行参数、是否执行等任务策略，以提升软件部署效率。 2. 能够自动判断并统计软件分发、部署的成功率，支持进程、注册表、安装路径等多种参数的组合判断。
16	报警报表	虚拟监控台	为了方便管理员从整体上把握网络安全态势，系统提供虚拟监控台功能。通过集中的仪表、数值显示快速进行安全态势的把握，主要

	管理		包括：报警、安全风险等级、全网终端数、清理终端数、安检和规律、安检项状态分布。
		安全管理报表	1. 准入设备后台能够按周、月、年统计安全状况走势图。 2. 准入设备后台提供每日入网报告、每周入网报告、每月入网报告。
		报警信息	1. 可以提供紧急、重要、次要、提示等多个级别自定义报警模式。 2. 支持系统报警、网络报警、终端报警等类别，超过20种以上自定义报警类型。 3. 支持Syslog报警信息的定向输出。
		报警提醒	准入设备能够以邮件、手机短信、页面消息等多种报警方式提醒管理员各种安全异常状态。
17	▲第三方产品联动		1. 支持与主流上网行为管理系统深度联动，构建内网准入、准出的全面安全管理体系。 2. 能够与主流动态口令认证系统相结合，提供动态密码联动认证机制。 3. 支持与国内外主流U-Key联动认证。
18	资质要求		1. 公安部《计算机信息系统安全专用产品销售许可证》（提供证明文件，加盖原厂商章）； 2. 国家保密局《涉密信息系统产品检测证书（网络访问控制产品）》（提供证明文件，加盖原厂商章）； 3. 国家版权局《计算机软件著作权登记证书》（提供证明文件，加盖原厂商章）；
19	▲保修		三年原厂硬件质保
20	▲其他		提供原厂商授权函及售后服务承诺函（加盖原厂商章）

（3）运维审计系统

序号	指标项		技术参数及技术要求
1	▲硬件指标		标准机架式设备，软硬一体化；单电源；10/100/1000M Base-TX 接口≥6 个，存储容量≥1TB
			支持 700 路字符会话或 200 路图形会话并发
			包含 100 个点的被管资源数
			支持旁路部署
2	主要功能		通过安全产品将人与目标设备进行分离，建立以“人->用户账号->授权->目标设备账号->目标设备”为管理模式，通过基于唯一身份标识的集中管理账号与权限、授权的控制策略，与各服务器、网络设备等无缝连接，实现集中精细化运维操作管控与审计。使 IT 安全运维从被动响应的模式转变为主动的运维安全管控模式，降低人为安全风险，满足合规和内部管理要求。
3	统一身份及认证管理	完善的身份管理和认证	1)支持账号分属组织的管理模式；组织管理能力，支持纵向七级、横向 255 个的组织划分能力，能够实现更完善的分权管理和分权审计；
			2)支持运维用户和管理员采用同一个账号；
			3)支持管理员、运维用户的静态口令、数字证书、动态口令、LDAP、

序号	指标项		技术参数及技术要求
			AD 域、Radius 等认证方式；
			4)支持 AD 域、LDAP 账号的自动同步；
			5)支持密码强度、密码有效期（按天设置）、口令尝试死锁、用户激活、备注、访问白名单等安全管理功能；
			6)支持用户分组管理，并且单个用户可以属于多个用户组；
			7)支持用户信息导入导出，方便批量处理；
			8)支持系统管理员、运维管理员、设备账号管理员、会话审计员、管理审计员等管理员角色；
			9)审计员分权管理，分为会话审计员、管理审计员，其中会话审计员只能审计会话信息，管理审计员只能审计 HAC 自身操作信息。
		后台账号口令集中管理	系统支持对后台各类资源（主机、服务器、网络设备、数据库等）的账号口令进行统一管理，即后台资源的账号口令由系统托管，用户登录系统后，系统根据用户权限分配后台资源的使用权。
			托管账号支持一站式关联用户、关联用户组。
		SSO 单点登录	管理员将后台资源账号及口令配置到堡垒机中；
			根据管理员配置，实现运维用户与后台资源账号对应，限制账号的越权使用；
			运维用户通过堡垒机认证和授权后，堡垒机根据分配的账号实现自动登录后台资源。
			支持的 SSO 账号类型包括： 支持 Windows、Linux、Unix 等服务器账号自动登录； 支持 CISCO(包括特权账号)、H3C 等网络设备账号自动登录； 支持 FTP、VNC、SFTP 等账号自动登录； 支持 PLSQL、SQLPLUS 等数据库工具账号自动登录；
		后台设备自动改密	根据口令安全策略，堡垒机定期自动修改后台资源帐户口令；
			支持密码更新周期自定义，可以按天设置；
			根据管理员配置，实现运维用户与后台资源账号对应，限制账号的越权使用
			运维用户通过堡垒机认证和授权后，堡垒机根据分配的账号实现自动登录后台资源
		电子口令保管箱	对于托管的后台设备口令，除支持以文件导出、邮件等的方式进行备份外，还支持把该托管口令备份到专用的口令安全存储设备上，防止口令丢失的风险。对于该口令安全存储设备的访问，支持指纹方式认证
4	访问控制及授权	灵活、细粒度的授权	系统提供基于授权规则名的授权设置，每个授权规则名下可以绑定多个用户、用户组、设备、设备组、访问规则（年、月、日、周、时间、会话时长、运维客户端 IP、协议类型）。
			每条授权规则可以设置相应的备注、启用/禁用设置。
		命令级授权	对于字符型协议，如 Telnet、SSH、FTP、SFTP 等，能够实现命令级别的授权控制。系统提供基于告警规则名的授权设置，每个告警规则名下可以绑定多个用户、用户组、设备、设备组、命令规则。每条授权规则可以设置为启用或禁用。
			可以通过命令规则进行规则匹配，支持黑、白名单功能；
			支持预订义和自定义的匹配命令设置，匹配命令支持多条命令，支持正则表达式；
			告警规则可以设置为阻断或只告警；
			告警规则支持告警级别设置，支持普通、严重、紧急等级别；
			告警规则可以按照帐号级别进行绑定，可以设置为只有指定安全级

序号	指标项		技术参数及技术要求
			别的帐号才能触发告警规则，针对不同用户实施不同的规则，从而提供更细粒度的操作控制。
		应用发布	运维操作全程可控，可做到授权后应用只能访问指定服务，最大降低对后台目标服务集群的可能安全风险。
			可对整个运维操作过程进行完整记录，实现详尽的会话审计和回放。
			可依据用户要求快速实现新应用的发布和审计。
			可支持对数据库维护工具、pcAnywhere、DameWare 等不同工具的运维操作进行监控和审计。
5	运维事件事中控制	实时监控及阻断	监控正在运维的会话，信息包括运维用户、运维客户端地址、资源地址、协议、开始时间等；
			监控后台资源被访问情况；
			提供在线运维操作的实时监控功能。针对命令协议和图形协议可以图像方式实时监控正在运维的各种操作，其信息与运维客户端所见完全一致；
			管理员可以关闭在线会话。
		违规操作实时告警与阻断	违反告警规则的各种事件，根据告警规则自动处理；告警事件可实时查看，并通过审计平台的声音、闪烁提示；
			对于设置为阻断的命令，运维用户无法执行，系统提示相关阻断信息；
			告警事件以邮件、短信通知。
		可支持ITSM	可与 ITSM 相结合，为其优化变更管理流程，加强对变更管理中的风险控制；
			支持对现有运维变更管理系统快速集成。
		可支持双人复核操作	支持 Telnet/SSH 的强制登录复核；
			支持运维过程的高危命令复核，例如对某阻断命令，可以设置必须由其它人进行复核；复核人复核通过后，运维人员才可以执行该阻断命令；
			支持会话日志记录双人复核操作审批人、时间、操作符合命令；
			支持设置复核级别，可设置由任意高级别的用户进行复核，也可以设置专门的高级别用户进行复核。
6	运维事件事后审计	完整记录网络会话过程	系统提供运维协议 Telnet、FTP、SSH、SFTP、RDP(Windows Terminal)、Xwindows、VNC、Http、Https 以及应用发布等网络会话的完整会话记录，完全满足内容审计中信息百分百不丢失的要求；
			会话信息包括运维用户、运维地址、后台资源地址、资源名、协议、起始时间、终止时间、流量大小信息；
			会话信息包括运维过程中所有进出后台资源的数据。
		详尽的会话审计与回放	运维操作审计以会话为单位，提供当日和条件查询定位。条件查询支持按运维用户、运维地址、后台资源地址、协议、起始时间、结束时间和操作内容中关键字等组合方式；
			针对命令交互方式的协议，提供逐条命令及相关操作结果的显示；
			提供图像形式的回放，真实、直观、可视地重现当时的操作过程；
			回放提供快放、慢放、拖拉等方式，方便快速定位和查看；
			针对命令交互方式的协议，提供按命令进行定位回放；
			针对 RDP、Xwindows、VNC 协议，提供按时间进行定位回放。
			对于 RDP 协议除记录视频格式外，对于各种键盘鼠标的操作进行记录，具体包括键盘信息、屏幕文本信息、文件读写信息等。
		自审计功能	管理员、审计员、运维人员在系统中关键操作行为记录，并可通过报表展现；

序号	指标项		技术参数及技术要求
			可记录主帐号访问审计设备时间、终端 IP 记录；
			可记录主帐号访问目标设备、从帐号记录。
		事件通知	事件通知功能可以将发生的事件以邮件或短信（需定制）的方式通知任何管理员。事件分为系统访问事件、配置管理事件、运维操作事件、运维审计事件、系统维护事件等 5 大类。
		完备的审计报表功能	提供日常报表，包括今日会话、今日自审计、用户信息、资源信息、权限信息、规则信息、管理员角色信息等报表；
			提供会话报表，可根据用户选定时间、用户、资源形成会话报表；
			自审计操作报表，可根据用户选定时间、管理员、模块形成自审计报表；
			告警报表，可根据告警类别、级别、资源、运维用户、协议、时间等条件形成报表；
			综合统计报表，可根据时间、资源、用户等条件形成综合统计报表，报表中包括概要信息、每个用户操作信息、每个资源被操作信息等；
			报表导出，支持 PDF、Excel、Word 等格式。
7	兼容性、可扩展性		运维审计作为 IT 运维流程中的一个部分，能够遵循 ITIL 满足稽核与审计的要求，系统能够通过定制开发与现有 ITSM、SOC、网管平台进行集成，满足大型网络系统的管理要求。
			能够与 KVM 系统进行整合，解决 KVM 系统本身审计功能薄弱的问题。
			能够与专业的数据库审计系统进行整合，审计日志信息既满足直观、方面查看的目的，又可以记录详细的数据库操作记录，便于故障分析。
8	▲保修		三年原厂硬件质保

（4）日志审计系统

序号	技术指标	技术要求
1	工作模式	独立完成审计日志采集，不依赖于设备或系统自身的日志系统； 审计工作不影响被审计对象的性能、稳定性或日常管理流程； 审计结果存储于独立存储空间； 自身用户管理与设备或主机的管理、使用、权限无关联； 提供全中文 WEB 管理界面，无需安装任意客户端软件或插件
2	功能扩展	采用解决方案包上传对产品进行功能扩展，无需要代码开发。
3	日志收集	支持 Syslog、SNMP Trap、OPSec、FTP 协议日志收集； 支持使用代理(Agent)方式提取日志并收集； 支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等； 设备厂家包括但不限于：Cisco(思科)，Juniper，联想网御/网御神州，F5，华为，H3C，微软，绿盟，飞塔(fortinet)，Foundry，天融信，启明星辰，天网，趋势，东软，Nokia，CheckPoint，Hillstone(山石)，安恒，珠海伟思，BEA，中国电信，安氏，帕拉迪，apc，arbor，clam，戴尔（dell），digium，东方电子，EMC，中国电力科学研究院，Eudora，google，冠群金辰，linksys，Mcafee，netapp，NAS（美国国家安全局），永达，sonicwall，vigor，天存，西岭，Symantec（赛门铁克），Hardened-PHP，foundertech(方正)，三零盛安，allot，蓝盾，IBM，金诺网安，网威，nortel(北电)，citrix(思杰)，watchguard，中兴，阿帕奇，WINDOWS 系统日志，Linux/UNIX syslog、IIS、Apache 等；

		支持常见的虚拟机环境日志收集，包括 Xen、VMWare、Hyper-V 等
4	性能监控	▲能够通过在目标主机上按章 agent 程序，支持监测目标主机的 CPU 利用率、内存使用率、磁盘使用情况、流量等信息、监测结果正确并支持设置报警阈值（提供公安部计算机信息系统安全产品质量监督检验中心检验报告，加盖原厂商章）。
5	产品要求	产品获得公安部计算机信息系统安全产品销售许可证（提供证书复印件，加盖原厂商章）； 所提供的产品检验报告须符合《信息安全技术日志分析产品检验规范》（提供完整检测报告（行标三级）复印件，加盖原厂商章）； 获得中国信息安全认证中心颁发的《IT 产品信息安全认证证书》（提供证书复印件，加盖原厂商章）； 检测标准符合 ISCCC-TR-056-2016《日志采集与分析产品安全技术要求》（提供完整检测报告，加盖原厂商章）。
6	硬件性能	软硬一体化设备，日志解析处理能力：≥8000EPS，网络流量：≥800Mb；日志容量：≥1.5 亿条；支持审计 100 个以上日志源；
7	日志备份	可设置日志存储备份策略，包括系统日志保存期（180 天）、磁盘使用率百分比；支持日志备份自动传送到远程服务器；
8	关联分析	产品维护一个安全知识库和包含资产信息的弱点库，当接受到针对制定资产并且匹配到弱点库中指定漏洞攻击时会触发与安全知识库、弱点库的关联。
9	日志查询	支持 B/S 模式管理，支持 SSL 加密模式访问； 支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、技术方式、技术动作、技术效果、攻击类型、地理城市等参数进行过滤查询； 支持用任意关键字对所有事件进行高性能全文检索； 支持可指定多个查询条件进行组合查询； 支持将查询的条件存储为查询模版，方便再次使用； 极高的日志高查询性能，支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果。
10	弱点管理	▲支持导入安恒应用弱点扫描器、绿盟极光扫描器等扫描报告，可进行统一检索、并支持计算威胁等级（提供公安部计算机信息系统安全产品质量监督检验中心检验报告，加盖原厂商章）。
11	告警功能	可预设置安全告警策略； 支持数据阀值设置，超过阀值将产生告警; 可以通过邮件、短信和屏幕显示进行告警；支持自动防止报警信息在短时间内大量发送(告警抑制)；具备报警合并和在一个时间段内抑制报警次数的能力。
12	综合查询及报表管理	内置合规性报表 1000+种； 内置 SOX、ISO27001、WEB 安全等解决方案包 内置完善的等级保护合规报表（提供截图证明，加盖原厂商章）。 内置综合性自动化审计报告；支持用户自定义报表；自定义的报表支持多个统计维度的数据集合；支持报表导出为 PDF 和 Word 格式文件。
13	用户管理	根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，审计员只负责查看相关的审计结果及告警内容；日志员只负责完成对系统本身的用户操作日志管理。 系统自带自身管理日志 ▲注册用户资产时，提供自动发现识别能力，提供一键式故障排除功能。提供自助式的升级接口，支持对产品升级、规则升级（提供截图证明，加盖原厂商章）。
14	部署方式	支持分布式部署；支持集中式管理和升级模式；

		支持分级管理模式； 采用 B/S 架构操作方式，无需客户端安装。 支持监控设备自身 CPU、内存、磁盘等工作运行状况
15	▲保修	三年原厂硬件质保
16	▲其他	提供原厂商授权函及售后服务承诺函（加盖原厂商章）

（5）网络管理平台

序号	功能指标	参数要求
1	稳定可靠	1、原厂商有通过 CMMi-4 级或以上的软件质量证书认证（提供证书复印件，加盖原厂商章）。 2、原厂商产品具备有效的公安部安全管理平台测试和认证（提供证书复印件，加盖原厂商章）。 3、原厂商具备 3 个以上省内公安行业用户的案例（提供合同关键页复印件，加盖原厂商章）。
2	系统平台	1、必须基于 Java 的开放式平台开发。 2、可以部署在目前流行的操作系统之上例如 Windows 和 linux 平台上。 3、系统可以运行在各种流行的关系型数据库系统之上。 4、采用 B/S（Browser/Server）模式。 5、支持多采集器分布式部署，减少服务器数据采集压力。
3	网元数量	1、至少能同时管理网络设备、服务器、数据库、中间件、业务系统,共计 200 个网元。
4	网络管理	1、系统能够对符合 SNMP 标准协议的交换机、路由器、防火墙、均衡负载等网络设备进行监控。 2、系统能够自动发现网络设备间的链路和网络设备与计算机间的链路，手动添加单体资源（设备）可自动生成链路，能监测链路的上行、下行带宽利用率和速率、上行和下行的丢包率、错包率；链路连通状况。 3、能够对设备进行手动刷新，重新计算链路与刷新物理信息；能手动对全网链路计算与发现，计算发现过程为自动。 4、可在原有拓扑情况不变的情况下手动发现指定的两台设备之间的链路，并自动计算链路两端接口。
5	服务器管理	1、系统能够支持监控多种主流操作系统，包括 Windows 2000/2003/2008 的 32 位/64 位等各版本、RedHat Linux AS、AIX、Solaris、HP-UX 等。 2、服务器操作系统各种详细信息，如文件系统信息、系统日志信息、系统版本信息。 3、服务器运行指标包括多个 CPU 中每个 CPU 的实时负载情况；物理内存、虚拟内存及页面文件的实时使用率；磁盘每个逻辑分区的分区容量；进程运行状态等；CPU 温度、网卡实时连接及流量、网络端口的丢包率、利用率、发送速率等指标；安装软件的情况等自定义指标项。 4、服务硬件管理监控，CPU、内存、磁盘等硬件状态。 5、系统能够支持通过自定义 SNMP OID 脚本，采集特殊的服务器特殊指标项。 6、系统支持单设备手动刷新；系统能够对设备进行手动刷新，重新计算链路与刷新物理信息。
6	数据库管理	1、支持的数据库类型 sqlserver2005,sqlserver2008,sqlserver2012,oracle、mysql 等。 2、系统能对核心业务系统的数据库进行有效的监控和管理。 3、数据库管理的功能包括：对数据库的表空间进行容量规划，并能够对表空间的使用情况进行定期分析和预警；实时监控当前数据库连接、监听器的管理

		并能够在连接数据库出现问题时告警；对数据库的碎片情况进行监测；对 SQL 的执行效率进行分析。 4、数据库的监控包括配置的连接监控、语句的执行情况监控、数据库的性能及其阀值的监控。 5、数据库监视器实例对数据库连接失败、执行语句失败、性能阀值越界产生报警事件。
7	中间件管理	1、支持的中间件类型 tomcat ,DB2,IIS,apache,tuxedo, jboss, weblogic, websphere 等。 2、对中间件的管理是通过模拟监视和性能指标两种方式进行：实时监控当前中间件的连接响应时间、监听器的管理模式，能够在连接中间件出现问题时告警检测。监控中间件的响应时间、请求数、传输速度、内存总数、连接数等等诸多指标，并可直观了解所在服务器的性能和使用情况。
8	资产管理	1、提供整合的资源监控和管理模块。把大量信息，按用户的的管理思路和管理目标整合在一起，方便用户查看和管理。资源列表提供管理一览和实时一览，并提供自定义排序 。 2、本模块可以融监控、CMDB、报表、快照、知识库、体验化于一体。 方便用户从各个方面来监控和管理系统的软硬件资源。结合资源监控和 CMDB，并在监控和 CMDB 中，均提供模板的功能，方便用户快速部署和调整多个资源监控和 CMDB 的各个子窗口都支持展开收缩，方便用户关注最重要的信息。 3、CMDB 可以管理设备的保修和服务信息，并及时提醒用户续保，；并可以展现设备的图片信息和物理信息（如高度、功率等），帮助用户进行管理。 4、CMDB 支持二维码扫码查看功能，扫码即可查看设备的详细情况，并且在巡检时扫二维码即可查看信息，方便巡检。 5、提供快照功能，用户可以把网络异常瞬间的各个设备和资源的情况生成快照，以便后续对指标和关联性逐项分析。
9	▲模板管理	1、提供通过“模板”来设置指标轮询周期、阈值和异常等级、告警方法、异常过滤和告警过滤。对于很多规则相同的设备或资源，直接运用模板即可，改变上述设置，也只要更换模板即可。 2、用户可以通过模板设置通断指标、性能指标、扩展指标、安全指标、自定义指标、复合指标和配置指标等等。也可以直接启动或停止不同类型的指标，可以批量将模板适配到不同设备。 3、系统提供各种内建模板，至少包括 SNMP 网络设备模板、Windows2003 模板、Windows2008 模板、LinuxAS4 模板、LinuxAS5 模板、HP-UX 基本模板、HP-UX 告警模板、AIX 基本模板、AIX 高级模板、防火墙模板、Oracle 数据库模板、SQLserver 数据库模板、各中间件模板等等。 4、用户可以通过设备选择不同模板，实时改变设备的监控策略而无需重新启动系统，也可以把模板批量应用于各设备。通过模板，可以很方便地引导用户设置指标，达到化繁为简，协助和帮助用户人员进行管理的目标。 5、分时模板可根据用户在高峰期或闲置期，根据使用情况调整多个关键指标的阈值大小，根据不同时间段的需求，灵活设置对应的阈值规则。
10	▲拓扑展示	1、全 BS Flex 拓扑图，拓扑图功能完全通过浏览器操作。 2、拓扑图管理提供高效的展示模式与自定义布局功能，用户可以在展示模式中根据网元数量等迅速找到适合自身网络环境的图元拓扑，在自定义布局模式中有各种视图表现形式、各种链路类型和各种图元类型，布局至少包括（径向类、树状、坐标类、蜗牛状等）类型，图片布局至少包括（图片类、图片鱼眼、小圆点类、小圆点鱼眼等）类型，链路样式至少包括（默认、方向箭头、方向气球、正交、流模式、贝塞尔曲线、磁线）等类型。 拓扑图展示层数和链路连线长短可以方便自定义。用户选择不同效果后界面能自动动态重新排列，效果美观。 3、拓扑支持分层分级展现，用户可以选择不同层数来控制大规模的拓扑图的

		展现。用户双击图元可以自动实现图元居中重排。运行状态和指标能实时展现在拓扑图上，并可以有鼠标位置展现和常展现两种不同状态。 4、拓扑图中可以提供搜索和整体概况，整体概况提供各种 Flex 的动态统计展现效果，能让用户不离开视图模块就能了解本视图的整体运行情况（如本视图上设备的统计、性能、异常等等），将视图功能拓展到视图代表的整体管理概念。 5、用户可以选择视图的实时镜像，可以在“我的”的模块中，和其他展现项（如指标、设备情况、性能曲线等），在一个页面中并列展现。 6、用户可以根据自己的需求选择不同的刷新模式，分为系统页面刷新时间和实时数据刷新 7、用户可以创建业务拓扑图，实时了解业务的结构与状态。 8、用户可以创建机柜拓扑图，自动化排列模拟用户现场 3D 机柜拓扑图场景，自动匹配体验化背板图片，打造设备图元真实性。 9、拓扑图支持上传图元背景功能，更好的美化拓扑图，便于展示。 10、用户添加 2 个设备间链路时，软件自动发现链路并计算出设备接口关系，方便准确。
11	整体管理	1、能在一个页面上提供系统总览、异常一览、报表一览、我的关注。把系统的各个方面的情况及时反映。 2、能把多个重要的网络设备、服务器、应用、防火墙、业务、网站等等设为我的关注，能显示这些设备的实时运行情况和历史运行情况。 3、能按类型、等级、是否确认、是否恢复、时间等来筛选展现当前和当天异常，能展现异常发生到现在的时间（MTBR），并能直接通过远程消息将异常信息通知设备的管理人，用户也可以在这个界面直接确认异常。 4、此页面能展示当前生成的报表。 5、此页面有“我的秘书”组件，能实时展现在线用户和不在线用户，能给用户发短信、邮件、远程消息。也能查看我收到的消息记录。 6、能通过图形方式，实时展现网络设备、服务器、链路、服务、业务和应用的不同状态数量（健康、亚健康、可用、不可用），并能通过鼠标点击后，实时查看哪些设备亚健康或哪些设备不可用，实时进行管理。
12	我的界面定制	1、提供“我的”界面。 能让用户在一个页面上配置多个组件，支持第三方界面直接嵌入。 2、组件类型包含“指标分析”“单个资源一览”“指标一览”“TopN”“拓扑图”“我的异常”“IPMAC 异常”“收藏夹”等等。 3、用户可以根据不同的情况，定制不同的展示组合。将上述的组件灵活搭配。同样的组件在一个页面也可以部署多个。为了适应用户的不同需要，本页面支持一列排列、两列排列、三列排列。在使用过程中，用户也可以随时切换而不需要重启服务。 4、所有组件支持拖拽的方式实时调整位置和排列。 5、系统所有界面都提供换肤功能，至少提供三种不同的界面风格（如正规色系，炫酷色系，节庆色系、灰色经典）等等，适合不同场景（如评审、会议、领导视察、日常管理、屏幕投射）等等场景。
13	告警方式	1、系统支持多种告警方式，包括拓扑图图标颜色变化告警，异常列表告警，消息框告警，声音告警，短信告警，微信告警，邮件告警，关闭网络端口告警、运维告警等方式。 2、用户可以自行灵活组合，生成新的告警方式。 3、后期采购硬件后可以支持语音电话告警、声光告警。 4、微信告警，及时的微信报警推送，方便用户有网情况下，随时随地了解到故障详情，节省短信使用成本。
14	异常处理	1、系统能够对各监测指标偶然产生的波动，可自动进行判断，避免误报事件，告警敏感度的设置可以精确到每个不同的指标。

		2、系统能够分时对不同的异常和告警生成过滤条件并进行过滤，可以精确到每天的不同时间以及不同的异常判断和不同的告警判断。 3、系统在一段时间内对连续性的同一故障只报一次警，避免告警风暴。时间可以灵活设置。 4、支持故障智能依赖树配置，找出故障真正的来源，系统能够通过异常依赖树智能分析各个异常间的逻辑关联关系，提供根本原因分析,快速发现故障根源，缩短恢复时间，防止告警泛滥。
15	报表和订阅	1、报表系统支持自定义和内建报表模板，模板可以分为内建、公共、个人、共享模板； 2、报表支持订阅、退订。 3、报表种类有日周月年报表和快照报表和一日内不同时段报表。 4、运行周期有一次性报表和周期性报表。 5、报表有类型时段报表、快照报表和单设备详细报表。
16	分析和统计	1、报表系统支持高效灵活的类 Mrtg 的性能分析。可以实时统计分析每次轮询数据、30 分钟统计、2 小时统计、日统计等多种实时统计和数据保存。 2、用户可以在一个屏幕上，同时展现各指标（如接口速率）的每次轮询、30 分钟统计、2 小时统计、日统计数据，并可以分成日曲线、周曲线、月曲线、年曲线进行图形趋势分析。 3、用户还可以自定义时间段来分析各个指标的历史情况。 4、支持多设备多指标分析，用户可以对多个设备的多个指标在指定的同一个时间段内进行对比分析，给用户提供多角度数据分析参考，并可将分析数据导出到 Excel。
17	故障分析	1、系统可以方便用户实时查看系统中的不同异常类型（当前、今天、昨天、本周、本月），并能筛选出（已确认、未确认、已恢复、未恢复、手动恢复不同异常等级、不同异常来源类型）等不同状态。 2、在查看和筛选时，同一屏幕上，可以通过立体饼图和立体柱状图动态展现不同等级和不同种类异常的各项分类数据和总数。用户可以操作和点击图形来减少分类类型，图表能实时动态重构。 3、用户也可以在异常列表上实时进行确认、恢复、手动恢复、删除等各项操作，手动恢复可将不重要的故障进行手工恢复。 4、故障信息支持与运维管理软件相关联，故障产生后可快速生成故障工单，严格按照标准 ITIL 流程理念进行处理和结果跟进。
18	个性化订制	1、用户可以通过个性化设置，简单在界面上定制用户的单位名称、系统名称，体现最佳客户满意度。
19	整体轮换	1、系统可以自动在多个界面自动轮换。包括但不仅限于（整体页面、我的页面、故障页面、分析页面）。 2、同时用户能够自行选择和定义要参与轮换的页面信息。 3、为适合不同用户，用户可以自行定义页面轮换间隔时间（如 15 秒、30 秒、40 秒、1 分钟、2 分钟、3 分钟、5 分钟）。 4、对于轮换可进行暂停与开启的模式， 自动轮换的客户端只需要标准的 B/S 浏览器，不需安装任何客户端。
20	地域和权限管理	1、系统可以把不同资源分为不同管理域，对不同的网管功能，给不同的角色分配不同的权限； 同时给不同用户分配不同的角色以及不同的地域。 2、通过立体化多维化的地域和权限管理，构建智能化的权限和视图管理，并保证高效管理和严密权限相结合。 3、同时，系统建立独立的用户中心，方便和运维系统等等其他系统的用户密码统一管理。
21	面板展现	1、能直观的看出每个设备的真实背板情况及设备接口的连接信息。 2、通过真实的设备背板图可以对设备的各个端口进行实时查看、打开和关闭等操作，能及时查看各个端口的基本信息,接口列表可监控指标当前值，如健

		康度、接口输出或输入速率以及接口状态等信息。 3、当某个交换机出现异常速率或者异常流量时，能够提醒及时把相对应的端口宕掉。
22	带宽管理	1、带宽管理能够获得广域网各线路的带宽与实际利用的带宽情况，管理者就可以第一时间的掌握网络设备的连接情况，并根据具体的连接情况做相应的处理和记录。
23	指标系统	1、系统提供高度灵活性的指标系统，包括通断指标、性能指标、扩展指标、安全指标、自定义指标、复合指标、配置指标等等。 2、可以灵活设置不同类型指标的轮询周期、阈值、异常策略、告警方法、异常过滤方法和告警过滤方法。 3、 支持设置多阈值策略，可设置交集或并集阈值策略，以适应多种设置场景以避免遗漏特殊告警。 4、用户可以自定义 SNMP 采集器、SQL 采集器、Tcp 采集器来采集各种系统的各个实时指标，并在拓扑图、实时运行情况等等界面展现。 并能提供实时健康度和可用率等等服务水平相关指标。 5、 系统管理来自系统主动定时轮询的轮询指标以及设备即时上报的 Trap/Syslog 信息生成的指标。 6、 为了能避免重复告警，能智能分析根源，轮询指标和 Syslog/Trap 指标必须在统一的处理渠道中合并处理。 7、 对于同一指标的高峰时段和非高峰时段，可以设置不同的阈值和不同的异常规则。 8、支持指标轮询周期、阈值和异常等级、告警方法、异常过滤和告警过滤。可自定义 ssh、telnet、SNMP、tcp、SQL、ping 取值，SSH 取值和 TELNET 取值在同一模块中，提供 SSH 和 telnet 取值模版和方式不低于 15 个模版，snmp、sql 模版不低于 5 个。
24	智能巡检	1、支持按不同巡检内容和设备制定周期性的定点智能巡检,自定义添加检测点,构建巡检规则。 2、以模板规范标准值为依据,根据预设的要求进行数据采集,进行自主分析判断,进行定期巡检 。 3、以报表的形式直观反映巡检结果,将巡检异常状态以告警灯形式展现,快速反映本次巡检的异常, 越界次数、标准值和当前值的差异性,系统会定期生成并主动发送运维人员 。 4、支持对系统监控巡查的整体进行评价和备注说明,导出多种格式向领导汇报,避 免传统的签到纸张的损坏、备注信息不全。 5、工作核查繁琐未如期巡查、巡检报表 乱写等问题。
25	工具模块	1、集成常用网络诊断和分析工具：Ping 、TraceRoute、NetBios、NetSend、链路延时、SNMP 连接 测试、TCP 端口扫描、实时表查询、Telnet&ssh、Mibbrowser（测试 OID 节点）。
26	日志管理	1、网管支持系统操作日志的记录，记录设备管理用户登录登录设备成功或失败信息，包括登录名、登录结果（失败原因），登陆时间，日志类型等，日志可以导出到 Excel 表格中。
27	系统备份恢复与数据维护	1、支持检测和查看数据类型的范围和容量。 2、支持一键备份与定时备份功能。 3、支持数据备份结束以客户端和消息进行通知。。 4、支持下载数据到任何终端 5、支持一键恢复和上传数据恢复。 6、通过核心数据存储设置，自定义保留用户最为关心的数据指标。 7、对系统性能数据、异常数据、报表数据、日志数据进行当前容量的检测，并可设置超过阈值告警方式，执行立即清理功能，为系统数据做瘦身。

28	资源管理	1、系统可以提供 IP 地址/信息点/VLAN 管理功能，方便用户输入和管理 IP 地址/信息点/VLAN 管理的信息，并将设备、IP 地址、信息点、物理位置/布线系统、VLAN 等等信息集中管理和保存，也可以方便查询。避免这部分管理信息遗失或散乱。 2、IP 地址管理，统一规划分配 IP 地址给每台终端机器，并建立 IP 地址分配基准表通过自动扫描，快速的查找网络中正在使用的 IP 地址，也可以手工设置要分配的 IP 地址，直观的了解和掌握整个网络的 IP 地址资源使用情况同时 IP 地址管理将与 IPMAC 绑定实时联动，各类状态：正常、占用 IP 且 PING 不通、非法使用 IP，每个地址是否在用，当前是否在线，计算机的名称，子网掩码 MAC 地址等的数据实时显示，当指定的 IP 地址或地址空间出现变更时立即获取告警通知，同时支持恢复基准分配地址。
29	配置管理	1、配置管理支持自定义 telnet 命令获取配置信息，以适应各类型的网络设备。 2、支持对各种网络设备如交换机、三层交换机、路由器、防火墙、负载均衡等配置信息的查询、查看、保存、对比、备份。 3、通过对配置文件与基准文件的对比，系统以状态灯（图元）形式表示配置变更的状态，红色表示配置产生变化，绿色则表示配置未变化。直接点击红色类态灯，即可对配置文件进行查看，并可以自动对配置文件进行实时比较。 4、另外，当配置发生变更或产生异常时，系统则会根据设定的相告警方式进行告警。 5、系统的对比检测，可以实时维护网络设备配置。
30	IPMAC 管理	1、系统可以动态实时做到终端准入控制的功能。 2、对交换机网络下，系统支持 IP-MAC-PORT 3 者之间的绑定，并可以查看 3 者之间的绑定关系，如 IP 地址与 MAC 地址的关系，MAC 地域与交换机端口的关系，同时还能由 IP 地址查找到该 IP 的 MAC 地址及该 IP 所连接的交换机端口。 3、通过 IP-MAC-PORT3 者的绑定，可以查看基准表信息、实时表信息、实时表与基准表信息比较后的差异信息、差异处理信息等。。 4、支持以实时图形化的方式查看接口利用率、速率、流量等 TOPN 运行数据情况。 5、支持自动生成快照轮询策略，定时进行 IP 使用情况进行巡检记录，并可以通过差异告警配置，对网络环境中出现的 IP 变更、新增终端及终端变更等异常进行告警.有助于用户及时掌握网络环境动态。 6、对未经许可上网的终端，可以采取告警，自动断网等等多项措施。 7、用户可对已知的 ip、mac 地址变动信息进行手动确认，确认后软件会在基准表中添加最新信息，避免频繁重复告警，提高工作效率。
31	多屏大屏幕展示	1、大屏幕数据实时采集，采用炫酷的动态图形展示，将概览统计，核心资源监控、趋势分析、TOPN、拓扑图、业务系统运行情况（繁忙度和响应时间，下属状态），服务器运行状况、中间件数据库运行状况、网络运行状况、机房运行状况、安全告警状况等等，以动态方式在展示中心多个或单个大屏幕上全屏集中展现。 2、灵活部署和多屏展示，支持不同分辨率，可根据多屏或单屏自定义配置多个界面，灵活部署在各类拼接屏或单屏轮换进行展示。 3、内建数据展示模板智能匹配，根据不同的行业满足用户业务、IT 资源、网络结构等各场景的展示需求。 4、多种类型组件数据支持、图形化编辑界面，通过简单拖拽即可配置灵活易用的自定义组件，轻松部署各视角核心数据展现。
32	▲保修	三年软件升级、原厂质保
33	▲其他	提供原厂商授权函及售后服务承诺函（加盖原厂商章）

（6）网络管理平台服务器

序号	指标项	技术参数及技术要求
1	处理器	单颗处理器核数≥6 核，主频≥1.6GHz，缓存≥15MB；本次配置处理器数量≥1
2	内存	≥24GB DDR4
3	硬盘	≥2*300GB 2.5 寸热插拔 SAS 硬盘
4	RAID 卡	支持 RAID 0/1，缓存≥2GB
5	网卡	≥4 个千兆电口
6	电源	1 个热插拔电源
7	其他	集成阵列卡(支持 Raid0/1)，DVD 光驱
8	▲保修	三年原厂硬件质保

（7）服务器接入交换机

序号	指标项	技术参数及技术要求
1	基本配置	10/100/1000Base-T 以太网端口≥48 个，其中 4 个复用的 1000Base-X 千兆 SFP 端口
2	性能	交换容量≥200Gbps，包转发率≥90Mpps
3	IP 路由	支持静态路由，支持 RIPv1/v2，支持 OSPFv1/v2
4	管理与维护	支持命令行接口（CLI）、Telnet、Console 口进行配置，支持 SNMPv1/v2/v3
5	▲保修	三年原厂硬件质保

3、互联网

（1）边界防火墙

序号	指标项	指标参数
1	▲基本配置	标准 2U 设备,双冗余电源；≥4 个 10/100/1000M Base-TX 接口，≥2 个 SFP 接口。
		最大并发连接数 300 万，最大吞吐量 8Gbps，每秒新建连接数 6 万；支持扩展插槽；
		配置 IPS 模块、防病毒模块，三年质保
2	网络适应性	支持静态路由，动态路由（OSPF、RIP、BGP、ISIS 等），VLAN 间路由，单臂路由，组播路由等。
		支持基于应用的策略路由，可实现为不同的应用类型智能选择相应的链路。
		支持基于文件类型的策略路由，可实现将预定义或者自定义的文件按照不同的分类进行智能选路。
		支持多出口路由情况下的默认路由备份、负载均衡。
		支持 ISP 路由，支持联通、电信、教育网、移动等 ISP 服务商地址列表，列表可导出及导入，可通过 Web 界面选择不同的 ISP 服务商实现快速切换。
3	网络管理	支持 DHCP Client、DHCP Relay、DHCP Server。
		各种工作模式下均支持 H.323（H.323 GK）、SIP、FTP、MMS、RTSP、XDMCP、TNS 等多种动态协议。
		支持对虚拟环境的数据流进行全策略控制。
		支持链路聚合功能，支持 802.3ad 和静态轮询、热备等多种模式，MAC、MAC&IP、IP&Port 多种聚合负载算法。

4	网络访问控制	支持一体化安全策略配置，可以通过一条策略实现用户认证、IPS、AV、URL 过滤、协议控制、流量控制、并发限制、新建限制、垃圾邮件过滤、审计等功能,简化用户管理。
		支持将源 MAC 作为独立的访问控制条件，防止非法设备接入。
		支持基于数据包的安全域、地址、用户及用户组、MAC、端口号、服务、域名等进行安全策略控制 。
		支持以组的方式管理安全策略，支持安全策略组的增、删、改操作，简化安全策略管理。
		支持针对策略中的源、目的地址进行并发限制，可以针对单 IP(或地址范围)进行并发控制。
		支持针对策略中的源、目的地址进行新建限制，可以针对单 IP(或地址范围)进行新建控制。
		支持策略命中数显示，并支持通过安全策略命中数范围查询。
		支持根据 IP 地址进行策略查询、支持根据服务端口进行策略查询。
		支持根据规则序号、规则名、源地址、目的地址、入侵防护策略、服务、认证用户、认证用户组、所属策略组、备注进行规则查询。
		支持查看资源被访问控制策略引用情况。
		支持查看访问控制策略引用地址、服务、时间资源情况。
5	服务器负载均衡	至少支持两种方法主动探测服务器的存活状态
6	入侵防护	支持基于策略的入侵检测与防护，可针对不同的源目 IP 地址、源 MAC 地址、服务、时间、安全域、用户等，采用不同的入侵防护策略。
		入侵防御特征库库至少应包括信息窃取、木马后门、间谍软件、可疑行为、网络设备攻击、安全漏洞及网络数据库攻击等的特征事件。
		支持细粒度的自定义 IPS 特征功能，支持 DNS\HTTP\FTP\TFTP\TELNET\SNMP\POP3\SMTP\IMAP\等 17 大类应用层协议的自定义，可以精准设置各个协议字段内容，例如字符内容、偏移、长度等细粒度的参数。
		支持对网络扫描行为的检测和过滤，可实现基于端口的扫描防护和基于主机的扫描防护。
		支持 IP/MAC 地址绑定的方式防止 ARP 欺骗，可采用手动建立或自动探测的方式生成 IP/MAC 对。
		支持多接口的攻击行为监听检测方式，可并行旁路检测多个网段内的网络攻击行为，用于高可靠性要求的旁路应用环境。
		至少支持丢弃封包、切断会话、攻击重定向、记录日志、邮件报警、声音报警 7 种响应方式。
		支持实时的入侵防护事件分级报警列表，可按事件的源 IP、目的 IP、协议、时间等显示；通过不同的入侵防护事件实时阻断入侵源 IP，阻断时间可控，提供入侵防护事件分级列表界面和实时阻断界面。
7	抗拒绝服务攻击	支持主流 ICMPFLOOD\SYNFLOOD\ACKFLOOD\SYNACKFLOOD\UDPFLOOD 攻击防护，采用专业高效的攻击防护算法，非采用简单的阈值进行攻击防护
		以上主流的功能，支持基于源 IP 限速、基于特征过滤系数、聚类限速系数、重传检测、自学习白名单等多种防御机制。
		支持专业的 DNSflood 攻击防护，具有高级的基于聚类限速、聚类分析、重传检测等多种高级防护算法。
		支持专业的 HTTP Flood 攻击防护；可以实现 get 和 post 的攻击防护，且 get 防护算法支持 4 类；支持独立 url 处理动作；以上防护功能均可以基于聚类分析、可信度、回探等多种防御机制。

		支持抗地址欺骗攻击、抗源路由攻击、抗 Smurf 攻击、抗 LAND 攻击、抗 Winnuke 攻击、抗 Queso 扫描、抗 SYN/FIN 扫描、抗 NULL 扫描、抗圣诞树攻击、抗 FIN 扫描、抗 Fraggle 攻击。
		支持自定义攻击日志的生成频率以及每时间段所需要记录的告警日志数目，攻击日志能够准确记录时间、攻击源目的、攻击类型、攻击次数等信息。
		支持攻击流量统计、攻击事件统计、攻击流量排行、攻击事件排行。
		支持 web 界面下对攻击流量进行抓包分析，支持自定义抓包参数，至少包括数据报文长度、报文数量、抓包时间及采样频率等基本参数；支持根据协议、源目的 IP、端口等参数进行数据报文过滤。
		支持对本地抓包文件的管理，包括下载、删除等操作，同时支持 FTP 方式将抓包文件上传至指定的 FTP 服务器中。
8	统一认证管理	支持多人使用同一帐号登录。
		支持在用户认证失败的情况下仍提供基本的网络访问权限。
		支持对 WEB 认证、LDAP 认证、RADIUS 认证、邮件账号认证、IP 识别用户的强制下线。
		支持用户的 AD 域、POP3、BJCA 单点登录，支持自定义单点登录监听端口。
		支持设置认证服务器组。
		支持用户口令复杂度设置。
		支持显示详细的用户在线信息，包括用户名称、真实姓名、所属组、认证源、接入方式、认证方式、登录 IP/MAC、在线时间、登录时间和可对其进行相关操作。
9	主动防御	支持 IPv4 和 IPv6 双栈协议下的主动防御。
		要求支持主动防御功能，对服务器、主机进行后门、服务探测、文件共享、系统补丁、IE 漏洞等主动式扫描。
10	安全日志	支持至少 2 个 Syslog 服务器，发送流量、系统或默认 2 类型日志到不同服务器。
		支持日志中文化，可显示配置命令日志的操作人。
		支持在三权分立模式下，对日志文件的加密导出/导入
11	高可用性	支持端口联动，支持上下行端口组的联动，可以实现单端口决定同组中的任意接口失效启动链路切换。
		自动同步、心跳接口多级（≥2 级）物理备份。
		可在热备和集群工作模式下支持多台防火墙的会话、配置的实时同步、手动同步。
		支持多重冗余协议(MRP)，实现链路备份、端口冗余、双机热备份、集群备份等。
		支持基于 VRRP 技术的热备和负载均衡。
		在 NAT、路由、透明模式下支持 A-A,A-S 模式，且切换时间小于 1 秒 。
12	▲保修	三年原厂硬件质保

（2）边界 WEB 防火墙

序号	指标项	详细说明
1	基本参数	4 个 10/100/1000 Base-T 接口（支持 bypass），整机吞吐量 4G，应用吞吐量 1G；
2	防护功能	支持 HTTP 0.9/1.0/1.1。

	要求	支持扩展 WEB 漏洞扫描功能，支持对 SQL 注入漏洞、XSS 漏洞等 WEB 脆弱性的扫描。
		支持扫描防护。
		支持 SQL 注入、XSS 防护，支持使 HTTP 头域中的 Cookie、Referer、User-Agent，Except 字段过防护策略。
		支持 CSRF（跨站请求伪造）防护。
		支持防护：蠕虫、缓冲区溢出、CGI 信息扫描、目录遍历等攻击。
		支持 Cookie 安全机制，包括加密和签名的防护方法，支持 Cookie 自学习。
		支持对服务器状态码进行过滤和伪装的安全策略。
		可以根据文件大小、MIME 类型、及文件扩展名，灵活定义下载限制策略，限制用户非法获取网站的关键数据（比如数据库文件，配置文件等）。
		支持 100 种以上爬虫防护；支持盗链防护，可采用 Referer 和 Cookie 算法。
		支持自动监测页面被篡改情况的功能，支持视觉恢复功能，即发生网页篡改后，对外仍显示被篡改前的正常页面，支持时间管理功能，可以在不同的时间段设定不同的网页篡改防护策略，支持恶意代码过滤功能，支持敏感关键字自定义功能。
		支持各类 DDOS 防护，包括 TCP Flood、HTTP Flood 防护，并说明 HTTP Flood 防护的检测算法。
		支持 HTTP 协议解码并对相关字段进行检查，包括 URI、HTTP 版本、请求方法、响应状态码、HTTP 头部各字段和其他 HTTP 元素。
		防护策略模型由基于静态规则的反向（黑名单）安全模式及基于智能用户行为识别的动态防护机制（正向安全模式，即白名单）构建。
		支持对 SSL（HTTPS）加密会话进行分析。
3	管理功能要求	支持标准 SNMP trap 和 Syslog 接口；支持 WEB 界面管理及 Console 及 SSH 管理。
		系统各组件通过强加密的 SSL 安全通道进行通讯，防止窃听，确保了整个系统的安全性和抗毁性；能对账户进行安全策略配置，包括口令最小长度和口令生存期；可以限制远程管理的登录 IP。
4	▲保修	三年原厂硬件质保

（3）终端准入控制系统

序号	指标项		指标参数
1	基本要求	▲系统要求	具有独立自主知识产权，须为标准机架式硬件产品，除自身硬件设备外，产品功能的实现无需额外增加服务器等设备。
		▲性能要求	配置 6 个千兆电口；每秒事务数（TPS）：≥1500（次/秒），最大吞吐量：≥800Mbps，最大并发链接数：1600（条）；800 用户许可；
		▲高可用性	1. 准入设备必须具备HA模式，HA须支持主备机心跳IP检测及虚地址管理模式，支持vrrp管理模式。 2. 提供第三方监控平台，在出现重大异常情况时能及时通知网络设备放开网络。
		语言支持	支持终端客户端、web 显示的中英文双语切换

		终端部署	1. 准入设备应至少提供安全客户端（Agent）、安全控件、无客户端等多种可供自定义部署、管理模式。 2. 安全客户端模式部署时，客户端程序应支持功能定制，以降低系统资源耗用，提升客户端兼容性。
2	准入架构	终端发现	1、 能够实时监测并发现接入内网的PC、平板电脑、智能手机、IP设备等终端，能够在第一时间隔离阻断并通知管理员。 2、 对自动发现的终端能够按照类别自动归类，以方便网络终端的统计管理（提供截图证明，加盖原厂商章）。
		准入技术	1. 准入设备须原生支持802.1x标准协议，无需第三方RADIUS服务器支持。 2. ▲准入设备支持基于多厂商Virtual Gateway的VLAN隔离技术，实现无客户端环境下端口级准入控制（提供截图证明，加盖原厂商章）。 3. 准入设备支持基于策略路由技术的准入控制模式，入网设备在访问网内关键资源时，将被强制隔离、引导至认证管理页面，同时支持交换机接口动态VLAN下发、端口隔离模式的网络边界管理。 4. 单台准入设备可支持至少2个核心交换机进行策略路由准入控制。 5. 准入设备可支持端口镜像准入技术，通过对交换机镜像数据的实时分析，能够及时发现并阻断非授权终端的接入。 6. 支持使用802.1x MAC认证时，记录详细的认证信息，包括:认证的时间、认证类型、认证的MAC、认证是否成功等，并支持报表记录。
		定向引导	1. 支持终端入网IE重定向引导，当用户访问网页时能够自动转向到指定的页面或地址，并支持http代理及多重重定向引导。 2. 可根据用户的实际环境自定义非80端口的Web服务端口号及用户重定向引导。 3. 能通过浏览器完成身份认证、控件安装、设备注册、安全检查、检查结果展现等全流程引导管理。 4. ▲具有Mac OS、Linux、iOS、Android等系统专属客户端，支持认证引导和准入管理（提供截图证明，加盖原厂商章）。
3	违规外联	▲违规外联	1. 能够针对3G拨号、双网卡、随身WIFI、代理等多种违规联网行为做实时检测，不接受间歇性ping外网地址的探测方式。 2. 能够针对违规外联终端进行即时断网，断网方式应支持断开链接、关闭连接进程、断网后重启恢复、重启计算机等多级模式，并能够实时通知管理员。 3. 准入设备能够支持按照用户角色定义、限制员工的内网访问范围，防止其越权访问操作。 4. SSID白名单，可对连接到白名单之外的无线网络行为进行阻断（提供截图证明，加盖原厂商章）。
4	边界管理	IP/MAC 绑定	具有入网设备自动学习功能，支持 IP/MAC/端口三者强制绑定，以及违规终端 VLAN 隔离机制，防止终端仿冒 IP 接入网络或移动设备位置。
		主机防火墙	1. 终端在准入通过后访问域严格收管理员策略控制 2. 同网段终端无法互相访问，做到精确到端口的高安全性控制

5	设备特征指纹	设备特征指纹	3. 具有非智能IP终端信息库，能够精准识别网络打印机、网络摄像头、IP电话等设备，并根据设备特征进行自动匹配和归类。 4. 通过伪造合法IP或MAC地址的非法设备和行为，能够被即时发现并阻断。
6	设备私接管理	NAT 设备	1. ▲具有NAT识别和检测机制能够及时发现网内私接的小路由器、无线AP、随身WIFI等NAT设备，帮助清查通过网中网隐藏的真实网络终端（提供截图证明，加盖原厂商章）。 2. 对通过NAT入网的计算机可以实现准入控制、安全评估和修复等流程化管理（提供截图证明，加盖原厂商章）
		Hub 管理	1. 能够发现内网私接的Hub、傻瓜交换机等非网管设备，当多台计算机通过Hub接入网络时，能够及时产生告警通知管理员（提供截图证明，加盖原厂商章）。 2. 准入设备能够采用VLAN隔离、逻辑关闭端口等方式禁止Hub下联计算机接入网络。 3. 支持Hub下多个终端需分别认证才能入网和只需一台认证即可全部入网两种认证机制。
7	网络管理	设备识别	1. 支持自动识别网络设备类型，包括：交换机、路由器、防火墙等，并按照类别自动进行归类。 2. 支持设备管理模板的定义功能，能够通过SNMP、SSH、TELNET等方式自动、批量添加网络设备。
		▲终端网络拓扑	1. 准入设备支持交换机到终端计算机的网络拓扑管理功能，能够自动绘制出网络拓扑图（提供截图证明，加盖原厂商章）。 2. 能够在拓扑图上选取设备查看其基本状态信息、设备型号、所处位置、子节点、路由表、ARP表等信息（提供截图证明，加盖原厂商章）。 3. 支持在界面上提供对该网络设备进行TELNET、SSH等管理。
		交换机状态展现	1. 支持可网管型交换机面板图形化展现各接口状态（up、down、trunk等），以及各接口下联的终端详细信息（IP、地址、MAC地址等）（提供截图证明，加盖原厂商章）。 2. 能够支持自上而下逐级查找终端的具体位置、安全状态、认证用户、上下线时间等信息。
		AP 联动管理	能够与主流的 AP 设备深度联动，支持 AP 控制器面板的图形展现，包括 AP 连接状态、下联终端信息（IP 地址、MAC 地址等）等。
		DHCP 中继	1. 能提供稳定的DHCP服务，并可以通过DHCP二次地址分配机制实现安全准入管理，支持交换机中继认证方式。 2. 能够根据用户、IP/MAC绑定信息等条件，为指定终端设备分配特定的IP地址。 3. 支持DHCP服务器筛选，防止非法DHCP服务器分发错误地址
		DHCP 地址释放	支持 DHCP 通过管理服务器手动操作，主动进行某台主机的 IP 地址释放。实现 IP 地址充分利用。
8	移动终端	终端识别	支持当前主流智能终端设备的安全准入控制，能够自动识别主流手机、智能终端等设备，并自动进行分类。

	管理	移动终端入网	1. 提供独立的智能终端入网引导界面的自主定制功能，至少包括界面标题、界面 LOGO、界面说明文字等。 2. 能够提供移动终端入网的设备注册功能。
9	认证管理	联动认证	能够全面结合用户已有的认证或业务系统，可以与 RADIUS、LDAP、STMP/POP 等采用标准协议的系统做深度联动认证。
		AD 域单点登录	1. 能够与用户现有的AD域相结合，当用户登录到AD域后，无需二次认证即可入网，避免多次认证的繁琐流程。 2. 当用户未登录到AD域时，该终端将一直被隔离，该状态下只有通过IE页面进行认证才能够入网。
		证书认证	支持至少 2 个以上的根证书。终端用户认证时，自动进行认证证书的根证书匹配
		短信认证	支持短信认证模式，用户在登记入网手机号码后，能够在手机上接收到入网的短信验证码，并在 IE 页面上利用短信验证码认证入网。
		微信认证	通过关注微信公众号放行移动终端入网
		接入审核	能够针对不同的角色或设备类别有选择的开启入网审核功能，待审核的用户或设备必须经过管理员审批才能入网。
		认证控制	支持对认证时间段、IP 段控制限制某类（角色）账户只能在指定的时间段、IP 段认证。
		自助账号申请	支持用户在认证页面自行进行账号的申请。用户可自行提交用户名、密码、姓名、电话、部门、E-Mail 等信息。管理员审核通过后，用户即可使用该账号进行认证。有效解决用户账号和密码创建和分发的困难。
10	来宾管理	来宾角色	能够提供来宾角色选择，能够设定来宾设备的访问权限和入网时长
		来宾码认证	提供临时入网码，支持来宾设备与受访人员进行一对一绑定功能
		二维码认证	通过扫描二维码进行来宾入网管理（提供截图证明，加盖原厂商章）
		来宾使用报表	生成来宾分配、来宾入网等动态审计报表
11	终端安全管理	安全检查库	准入设备须提供系统安全配置、用户行为规范等类别检查项，至少提供 24 种以上安全检查项。
		系统补丁	▲准入设备具有完整的补丁管理子系统，无需第三方补丁服务器支持，自身即可以提供完整的流程化补丁管理，包括同步更新、补丁分类、补丁分发、补丁报表等功能（提供截图证明，加盖原厂商章）。能够在 IE 页面进行入网终端的补丁检查，补丁均划分为严重、重要、中等的类别，能够在 IE 页面显示出检查结果（提供截图证明，加盖原厂商章）。
		防病毒软件	能够在 IE 页面检查出终端的杀毒软件情况，支持主流的 20 种以上的杀毒软件检查，包括微软 MSE、可牛、Avast 等，支持杀毒软件版本、病毒库和运行情况的检查，能够在 IE 页面显示出检查结果（提供截图证明，加盖原厂商章）。

		Windows 组策略检测	windows 密码策略、屏保、共享目录、弱口令、防火墙、网卡配置等系统策略进行检查和修复
		计算机健康性检测	对终端的磁盘使用率、垃圾文件、IE 主页、网络监听端口等安全性配置进行检查和修复
		自定义安全检查	通过检测终端文件路径、指定文件版本、大小、MD5，注册表的项、注册表值，进程，服务名称、服务状态，进行检查。通过安装包运行、访问站点、开关服务、关闭进程、执行文件、删除文件、修改注册表进行修复。可以灵活的全访问的对终端进行安全检查和修复（提供截图证明，加盖原厂商章）。
		终端安全加固	能够通过傻瓜式的漏洞修复模式为用户提供简单、形象的漏洞自我修复功能，完全不需要管理员的介入即可完成终端安全风险项修补。
		桌管系统联动	能够在 IE 页面检查出主流的桌面管理系统（包括 Landesk、北信源、威盾、盈高、圣博润等）客户端是否安装并正常运行，能够在 IE 页面显示出检查结果。
12	移动存储设备管理	移动存储设备管理	1. 管理员可以通过对存储介质统一注册、授权的方式来加强管理存储介质的使用范围和权限，并支持存储介质分区加密，未经标识的存储介质将不能在企业内正常使用。 2. 针对不同注册状态的存储介质制定不同的控制策略，能够对存储介质进行只读、禁用、放行、脱机生效以及时间范围等做精细控制。
		移动存储设备审计	1. 支持查询存储介质的类型、设备名称、设备插入时间、设备拔出时间、设备使用 IP 地址、类型代码、设备容量、厂家名称、产品名称、该存储介质使用人、操作系统用户名、备注信息。 2. 支持使用存储介质的终端信息显示，包括：设备名称、IP 地址信息、所在部门、所在位置、联系人、联系电话、E-Mail 地址、设备状态（开机、关机）、最后在线时间等。
13	资产管理	资产管理	1. 能够对全网计算机上安装的软件进行统计，可以按照部门、名称提供精确查询以及软件资产报表的导出。 2. 能够对终端硬件初始记录、最新记录和变动记录形成报表，并且能够查询变动的历史。
		资产变动	准入设备能够针对软硬件资产变动、资产异常情况提供了丰富多样的报警方式，便于管理员及时迅速了解资产信息。
		变动确认	支持管理员对每一条软硬件变动进行确认操作，已确认的条目显示已确认，并显示进行确认操作的确认人。对变动和变动确认可进行报表统计；
14	资源管理	软件检查	1. 通过安全检查检测终端软件安装、使用状态 2. 自动强制为终端安装软件 3. 软件产品授权，支持进行windows、office、WPS的产品授权信息进行检查
		IP 地址管理	1. 提供IP地址分配表，能够通过图示直观的查看各网段中未分配、开机、关机的数量和分布情况。 2. 能够直接、快捷的查看全网终端历史上线、下线、在线时长等详细的IP使用情况。
		能耗管理	提供未关机终端自动统计功能，并能够按照部门、时间段等条件生成统计报表。

15	运维管理	移动终端管理	移动端管理平台可实现设备快速定位、设备审核、实时报警监控、小助手确认码生成、准入控制器管理、平台基本信息、关机与重启
		管理角色控制	准入设备须采用系统管理员、安全管理员、审计员三权分立机制，防止单个角色管理者权限滥用。
		网络诊断工具	支持通过 Web 管理界面提供 ping、抓包、traceroute、nslookup 等功能，并可以设置命令参数进行相关调试。
		消息群发	能够支持在指定的一台或者多台终端计算机上产生桌面消息通知，该消息会立即弹出在用户桌面上，对用户进行提醒。
		软件分发	1. 准入设备应具有软件分发和部署功能，管理员可以预定义软件分发的路径、运行参数、是否执行等任务策略，以提升软件部署效率。 2. 能够自动判断并统计软件分发、部署的成功率，支持进程、注册表、安装路径等多种参数的组合判断。
16	报警报表管理	虚拟监控台	为了方便管理员从整体上把握网络安全态势，系统提供虚拟监控台功能。通过集中的仪表、数值显示快速进行安全态势的把握，主要包括：报警、安全风险等级、全网终端数、清理终端数、安检和规律、安检项状态分布。
		安全管理报表	1. 准入设备后台能够按周、月、年统计安全状况走势图。 2. 准入设备后台提供每日入网报告、每周入网报告、每月入网报告。
		报警信息	1. 可以提供紧急、重要、次要、提示等多个级别自定义报警模式。 2. 支持系统报警、网络报警、终端报警等类别，超过20种以上自定义报警类型。 3. 支持Syslog报警信息的定向输出。
		报警提醒	准入设备能够以邮件、手机短信、页面消息等多种报警方式提醒管理员各种安全异常状态。
17	▲第三方产品联动		1. 支持与主流上网行为管理系统深度联动，构建内网准入、准出的全面安全管理体系。 2. 能够与主流动态口令认证系统相结合，提供动态密码联动认证机制。 3. 支持与国内外主流U-Key联动认证。
18	资质要求		1. 公安部《计算机信息系统安全专用产品销售许可证》（提供证明文件，加盖原厂商章）； 2. 国家保密局《涉密信息系统产品检测证书（网络访问控制产品）》（提供证明文件，加盖原厂商章）； 3. 国家版权局《计算机软件著作权登记证书》（提供证明文件，加盖原厂商章）；
19	▲保修		三年原厂硬件质保
20	▲其他		提供原厂商授权函及售后服务承诺函（加盖原厂商章）

（4）服务器接入交换机

序号	指标项	技术参数及技术要求

序号	指标项	技术参数及技术要求
6	基本配置	10/100/1000Base-T 以太网端口≥24 个，其中 4 个复用的 1000Base-X 千兆 SFP 端口
7	性能	交换容量≥200Gbps，包转发率≥90Mpps
8	IP 路由	支持静态路由，支持 RIPv1/v2，支持 OSPFv1/v2
9	管理与维护	支持命令行接口（CLI）、Telnet、Console 口进行配置，支持 SNMPv1/v2/v3
10	▲保修	三年原厂硬件质保

四、其他相关要求

1、工　　期：合同签订后 60 天内。

2、交付地点：用户指定地点。

3、采购资金的支付方式、时间、条件：

完成全部设备的供货，经甲方确认后，支付合同总金额的 30%，项目完成安装调试，经甲方验收合格后，支付合同总金额的 65%，剩余合同总金额的 5%转为质保金，质保期为 1 年，质保期结束后无息返还。

4、验收要求：按标书技术参数和国家行业标准进行验收。

5、售后服务要求：

(1)整体工程提供不少于三年的免费维护，设备按原厂商标准提供维护。

(2) 投标人或生产厂家须在国内设立服务机构，提供每周 7×24 小时技术支持和服务，针对使用过程中出现的故障问题，可以通过电话、网络方式先提供服务，2 小时内作出实质性响应，对重大问题提供现场技术支持，如果解决不了的情况下需要及时赶赴现场提供服务，8 小时内到达指定现场。

(3) 软硬件免费保修期，自验收合格之日起算。

(4) 保修期内非采购方人为因素而出现的质量问题，生产厂家负责保修、包换或者包退，并承担修理、调换或退货的实际费用。

(5) 投标人承诺提供的每一台设备均是全新的，厂家提供终身有偿维修、保养服务，保修范围外有偿维修，只收成本费。

(6) 投标人或生产厂家负责产品安装系统调试。

(7) 投标人或生产厂家负责长期提供技术资料和技术支持。

(8) 生产厂家保修期外需提供终身维护，设备故障维修只收取零配件费用。

(9) 投标人或生产厂家须对招标方使用人员及设备维修人员进行培训，使用人员能够熟练掌握设备的各项功能和操作，使维修人员能对设备进行日常维护和一般性故障的查找及故障的排除。

6、由于项目实施过程会涉及招标方敏感信息，中标人必须提交保密承诺函。

7、投标人必须根据所投产品的技术参数、资质资料编写投标文件。在中标结果公示期间，采购人有权对中标候选人所投产品的资质证书等进行核查，如发现与其投标文件中的描述不一，代理机构将报政府采购主管部门严肃处理。

8、投标人不能低于成本价恶意报价，如中标人的报价过低（低于预算金额的80%），明显有违市场合理价格的，则采购人有权要求中标人提供预算金额的8%作为履约保证金和预付款调整为0%。如中标人在实施过程中偷工减料、不按工期完成项目，则采购人有权终止合同，没收履约保证金，并报主管部门严肃处理。

第二部分　B包需求书

一、项目名称

等级保护测评及信息安全服务

二、项目背景

通过委托专业的信息安全等级保护测评服务机构，对用户的信息系统安全保护等级进行需求分析，并协助用户完成等保备案相关事宜。依据《信息系统安全等级保护基本要求》，对信息系统的物理机房、网络结构、应用系统、主机、网络及安全设备等进行合规性检查，分析信息系统与安全保护等级要求之间的差距，出具《信息系统安全等级保护测评报告》，提出具有针对性的整改意见，并根据信息系统及安全防护措施的现状，提供渗透测试、安全管理体系建设服务、安全加固技术咨询服务、应急预案编制服务、应急演练服务及、网站云监测和云防护服务，确保信息系统的安全运行。

三、项目工期和地点

项目实施工期：采购人下达测评通知书后60个日历天内交付测评报告；

交付地点：用户指定地点。

四、等级保护测评服务需求

1、测评内容

（1）对用户的信息系统进行摸底、分析和梳理，提出详细的测评方案及完成系统备案工作。

（2）逐一对信息系统进行安全等级保护测评，测评的内容包括但不限于以下内容：

1）安全技术测评：包括物理安全、网络安全、主机系统安全、应用安全和数据备份及恢复等五个方面的安全测评；

2）安全管理测评：安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等五个方面的安全测评。

（3）完成测评工作后，提出整改方案；最后出具符合等保要求的网络安全保护等级测评报告，并协助用户完成网络安全保护等级备案工作。

2、 项目输出(包括但不限于以下内容)

（1）信息系统定级相关文件和报告；

（2）信息系统测评报告及整改建议；

（3）网络安全整改设计方案。

3、 测评对象描述

序号	被测系统名称	安全等级	被测系统描述
1	三亚市公安局门户网站	三级	三亚市公安局门户网站的功能包括信息展示、警务公开、便民服务、警民互动、赏金猎手、新闻发布、视频专栏、社区警务室等，业务办理模块包含交通管理办理、户政办理、出入境服务、治安管理业务、消防管理等。
2	三亚市公安局内网	三级	三亚市公安局内网是三亚公安业务的核心网络，该内网系统有两个专网出口，一个电信100M，一个移动100M，出口处做了边界路由冗余，防火墙串联边界路由做访问控制，再下连IPS入侵防御，接入核心交换机，各楼层内网业务交换机通过汇聚交换机接入内网核心区，组成整个网络。
3	三亚市公安局视频监控系统	三级	三亚市公安局视频监控系统为适应社会经济、治安形势的发展，不断加强监控点、监控网络、监控中心、监控管理平台和监控机制建设，逐步建成一个覆盖各大型聚集场所、治安复杂区域和要害部位的社会面治安监控系统，全面提高公安机关掌握和控制社会面治安局势的能力。它可实现事故发生后的现场搜索、图像记录，以及疑犯跟踪等，更重要的是，它对犯罪份子起到了威慑的作用。与其他领域的监控系统相比，城市治安监控系统要求设备具有24小时连续工作的能力、稳定可靠性高，

4、测评服务步骤

信息系统等级保护测评过程需按照《信息系统安全等级保护测评过程指南》开展工作，等级测评过程分为四个基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析及报告编制活动。测评双方之间的沟通与洽谈应贯穿整个等级测评过程。

（1）测评准备活动

测评准备工作包括编制项目启动、信息收集和分析、工具和表单准备。

详细要求见下表：

项目内容	工作内容	成果输出
项目启动	1.组建测评项目组	向用户提交 《项目计划书》《提供资料清单》
	2.编制《项目计划书》	
	3.确定测评委托单位应提供的资料	
信息收集分析	定级报告及整改方案分析	《系统基本情况分析报告》
	1.整理调查表单	

	2.发放调查表单给测评委托单位	
	3.协助测评委托单位填写调查表	
	4.收回调查结果	
	5.分析调查	
工具和表单准备	1.调试测评工具	确定测评工具（测评工具清单）《现场测评授权书》 《测评结果记录表》 《文档交接单》
	2.模拟被测系统搭建测评环境	
	3.模拟测评	
	4.准备打印表单	

（2）方案编制活动

方案编制活动包括测评对象确定、测评指标确定、测试工具接入点确定、测评内容确定、测评指导书开发及测评方案编制等六项主要任务。

详细要求见下表：

工作内容	工作详细任务	输出成果
一、测评对象确认	识别被测系统等级 识别被测系统的整体结构 识别被测系统的边界 识别被测系统的网络区域 识别被测系统的重要节点和业务应用 确定测评对象	《测评方案》的测评对象部分
二、测评指标确定	识别被测系统业务信息和系统服务安全保护等级	《测评方案》的测评指标部分
	选择对应等级的安全要求作为测评指标	
	就高原则调整多个定级对象共用的某些物理安全或管理安全测评指标	
三、工具测试点确定	确定工具测试的测评对象 选择测试路径 确定测试工具的接入点	《测评方案》的测试工具接入点部分
四、测试内容确定	识别每个测评对象的测评指标	《测评方案》的单项测评实施和系统测评实施部分
	识别每个测评对象对应的每个测试指标的测试方法	
五、测评指导书开发	从已有的测评指导书中选择与测评对象对应的手册	《测评方案》的测评实施手册部分
	针对没有现成测评指导书的测评对象，开发新的测评指导书	
六、测评方案编制	描述测评项目基本情况和工作依据	向用户提交 《测评方案》
	描述被测系统的整体结构、边界和网络区域	
	描述被测系统的重要节点和业务应用	
	描述测评指标	
	描述测评对象	
	描述测评内容和方法	

（3）现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调，为现场测评的顺利开展打下良好基础，然后依据测评方案实施现场测评工作，将测评方案和测评工具等具体落实到现场测评活动中。现场测评工作应取得分析与报告编制活动所需的、足够的证据和资料。

现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

详细要求见下表：

工作内容	工作详细任务	输出
1.现场测评准备	现场测评授权书签署	会议记录、确认的授权委托书、更新后的测评计划和测评方案
	召开现场测评启动会	
	双方确认测评方案	
	双方确认配合人员、环境等资源	
	确认信息系统已经备份	
	测评方案、结构记录表格等资料更新	
2.现场测评和结构记录	依据测评指导书实施测评	访谈结果：技术安全和管理安全测评的测评结果记录或录音 文档审查结果： 管理安全测评的测评结果记录 配置检查结果： 技术安全测评的网络、主机、应用测评结果记录表格 工具测试结果： 技术安全测评的网络、主机、应用测评结果记录，工具测试完成后的电子输出记录，备份的测试结果文件 实地察看结果： 技术安全测评的物理安全和管理安全测评结果记录 测评结果确认： 现场核查中发现的问题汇总、证据和证据源记录、被测单位的书面认可文件
	记录测评获取的证据、资料等信息	
	汇总测评记录，如果需要，实施补充测评	
3.结果确认和资料归还	召开现场测评结束会	
	测评委托单位确认测评过程中获取的证据和资料的正确性，并签字认可	
	测评人员归还借阅的各种资料	

（4）报告分析及编制活动

在现场测评工作结束后，应对现场测评获得的测评结果（或称测评证据）进行汇总分析，形成等级测评结论，并编制测评报告。

测评人员在初步判定单元测评结果后，还需进行整体测评，经过整体测评后，有的单元测评结果可能会有所变化，需进一步修订单元测评结果，而后进行风险分析和评价，形成等级测评结论。分析与报告编制活动包括单项测评结果判定、单元测评结果判定、整体测评、风险分析、等级测评结论形成及测评报告编制六项主要任务。

详细要求见下表：

工作内容	工作详细任务	工作依据（模版）
1.单项测评结果判定	分析测评项所对抗威胁的存在情况	等级测评报告的单项测评结果部分
	分析单个测评项是否有多方面的要求内容，依据“优势证据”法选择优势证据，并将优势证据与预期测评结果相比较	
	综合判定单个测评项的测评结果	
2.单元测评结果判定	汇总每个测评对象在每个测评单元的单项测评结果	等级测评报告的单项测评结果汇总分析部分
	判定每个测评对象的单元测评结果	
3.整体测评	分析不符合和部分符合的测评项与其他测评项（包括单元内、层面间、区域间）之间	等级测评报告的系统整体测评分析部分

	的关联关系及对结果的影响情况	
	分析被测系统整体结构的安全性对结果的影响情况	
4.风险分析	整体测评后的单项测评结果再次汇总	等级测评报告的风险分析部分
	分析部分符合项或不符合项所产生的安全问题被威胁利用的可能性	
	分析威胁利用安全问题后造成的影响程度	
	为被测系统面临的风险进行赋值	
	评价风险分析结果	
5.等级测评结论形成	统计再次汇总后的单项测评结果为部分符合和不符合项的项数	等级测评报告的等级测评结论部分
	形成等级测评结论	
6.测评报告编制	概述测评项目情况	等级测评报告 提交用户
	描述被测系统情况	
	描述测评范围和方法	
	描述整体测评情况	
	汇总测评结果	
	描述风险情况	
	给出等级测评结论和整改建议	

五、渗透测试服务需求

借鉴黑客攻击的手法和技巧，在可控的范围内分别对公安网、视频监控网络、门户网站或整个内网进行模拟测试，全面挖掘漏洞，提供渗透测试报告。

渗透测试方法包括但不限于信息收集、端口扫描、口令猜测、远程溢出、本地溢出、脚步测试、权限获取等。

渗透测试是专业技术人员利用多种专业漏洞扫描工具对网络、操作系统、数据库、WEB 系统等进行交叉扫描验证，专业技术人员在对结果进行分析并人工对可能存在的漏洞点进行检查和模拟黑客攻击，帮助用户及时掌握信息系统安全状况，发现存在的主要问题和薄弱环节，并对发现的安全隐患提供改善建议，以及时帮助客户堵塞安全漏洞，协助指导客户落实和完善安全措施，以帮助客户建立信息安全保障机制，减少安全风险，提高应急处置能力，从而促进信息系统持续安全稳定运行。

六、安全管理体系建设服务需求

根据《BG-T22239-2008 信息系统安全等级保护基本要求》中的三级要求，结合单位的实际管理需求，调整原有信息安全管理模式和信息安全管理策略，对安全管理制度和规范流程进行梳理、调整和编制，构建满足信息安全等级保护的安全管理体系,制度至少包含以下内容：安全策略和管理制度、岗位设置、人员配备、授权审批、沟通合作、审查和检查、人员录用、人员离岗、安全意识教育和培训、外部人员访问管理、定级和备案、方案设计、产品采购和使用、软件开发管理、工程实施、测试验收、系统交付、

等级测评、供应商选择、环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份和恢复管理、安全事件处置、应急预案管理、外包运维管理。

服务结果输出

《安全管理制度汇编》,汇编中至少包含以下制度：

1. 《信息安全组织机构》
2. 《信息安全组织建设规定》
3. 《用户密码管理制度》
4. 《信息化安全建设目标及组织机构管理办法》
5. 《人员安全管理》
6. 《岗位职责管理规定》
7. 《办公环境管理制度》
8. 《管理评审制度》
9. 《保密协议》
10. 《产品选型指导办法》
11. 《系统安全管理制度》
12. 《信息系统变更控制管理制度》
13. 《口令使用规定》
14. 《介质管理制度》
15. 《文件控制制度》
16. 《项目验收检查流程》
17. 《信息类设备标识管理办法》
18. 《信息安全奖惩管理规定》
19. 《信息资产管理制度》
20. 《信息系统管理维护制度》
21. 《信息系统建设管理制度》
22. 《机房管理制度》
23. 《防病毒管理制度》
24. 《日志审计管理办法》

25.《设备管理制度》

26.《网络安全管理制度》

27.《网络设备安全配置管理规定》

28.《信息系统开发与维护管理制度》

29.《信息系统外包管理制度》

30.《资产备份恢复管理制度》

31.《基础设施故障处理流程》

32.《安全事件管理制度》

33.《突发事件应急制度》

34.《网络故障应急处理流程》

编制后的制度必须符合最新的等级保护规范中的三级要求。

七、安全加固技术咨询服务

依据《信息系统安全等级保护基本要求》并结合三亚市公安局信息安全现状、测评过程中发现的问题，从物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复等方面提供安全加固技术咨询服务，服务内容包括漏洞修复、策略优化、结构调整、配置加固、规划设计等，旨在从软技术上加强三亚市公安局网络与信息系统安全防护水平，能够抵御网络入侵和攻击，防止信息网络瘫痪、应用系统被破坏、业务数据丢失、数据泄露、终端病毒感染、有害信息传播，确保信息系统安全稳定运行，确保业务数据安全。

八、应急预案编制及应急演练服务

应急预案及应急演练服务将根据《中华人民共和国突发事件应对法》、《突发事件应急预案管理办法》、国家信息安全等级保护标准《信息安全等级保护基本要求》（GB/T22239--2008）、《中华人民共和国网络安全法》、《海南省信息化条例》和《关于印发海南省党政机关、事业单位和国有企业互联网网站安全专项整治行动方案的通知》等文件对“信息安全事件应急响应、应急预案和应急演练”的相关规定，结合用户信息系统的实际情况，指导用户建立健全信息与网络安全事件应急响应工作机制，并对信息系统相关人员进行应急预案、应急技巧及对典型的信息安全事件进行预防等方面的培训。

信息安全事件应急预案包括以下安全事件：

有害程序事件：计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件和其它有害程序事件；

网络攻击事件：拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件；

信息破坏事件：信息篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件和其它信息破坏事件；

信息内容安全事件：违反宪法和法律、行政法规的信息安全事件；针对社会事项进行讨论、评论形成网上敏感的舆论热点,出现一定规模炒作的信息安全事件；组织串连、煽动集会游行的信息安全事件；其他信息内容安全事件；

设备设施故障：软硬件自身故障、外围保障设施故障、人为破坏事故、和其它设备设施故障。

信息安全事件应急预案演练主要对运行环境安全、网络结构安全、设备运行安全、系统可用性、外界风险因素等各方面进行全面演练，主要覆盖重要信息系统、数据中心、灾备中心等重要基础设施，重要服务商应急保障能力，外部应急协调机制等。

做到全面演练和专项演练相结合。应急演练应贴合信息系统的实际情况，主要的演练方式为模拟演练及桌面演练。

演练场景以可能出现的通讯故障、系统故障、系统安全等为重点，结合用户实际情况和关键风险点，设计以下应急场景进行演练：

通讯故障：演练在用户量激增、网络设备故障、通信线路被破坏、网络受到攻击等原因导致通讯中断和拥塞时的应急预案以及与公安、电信部门的应急协调与保障机制。

系统安全：演练因病毒爆发、网络入侵攻击、篡改网站等情形下的系统应急预案以及与公安、电信部门的应急协调机制。

系统故障：主要演练主要信息系统出现应用故障、数据库故障、存储设备故障、主机硬件故障等的应急预案以及外联单位、系统重要服务商的应急协调与保障能力；检验外联单位相关系统的应急保障能力。

九、网站云监测和云防护服务

针对三亚市公安局门户网站，提供 1 年的 7X24 小时云安全防护及监测服务。服务内容包括： Web 攻击防护、抗 DDOS 攻击（10Gbps）防护、抗 CC 攻击（10000Q/S）防护、

可用性监测、漏洞监测、网页篡改监测、网页挂马监测、内容变更监测、黑词监测、黑链监测、敏感词监测、可用性云监测、提供报表和通报功能。

十、项目服务要求

1、项目实施要求

项目实施过程中，投标人应遵循国家标准、行业标准。

在项目实施中投标放须做到：

（1）本项目的项目经理必须具有 1 年以上的等保测评服务项目管理经验；其中，本项目成员中至少有 2 人具备信息安全等级保护中级测评师资格；

（2）提供完整的系统实施方案和项目实施管理办法；

（3）提供详细的项目实施方案和计划进度说明书；

（4）项目实施完成后提供可靠的后期技术服务工作；

（5）严格按照双方确定的计划进度保质保量完成工作；

（6）规范项目实施过程中的文档管理。

2、项目验收要求

中标方必须提供给业主详细的项目验收方案。

（1） 验收组织

成立由招标方、中标方以及其他有关人员组成的验收小组，负责对项目进行全面的验收。

（2）验收标准

1）标准化：项目验收最关键的指标，应确保测评过程符合国家标准规范；

2）系统稳定性：在测评过程中应确保软硬件环境的稳定性、运行正常；

3）系统文档：验收文档是否齐全、规范、准确、详细；

4）系统可操作性：交付成果清晰、通俗易懂。

（3）售后服务要求

对于评估中发现的应用系统、主机和网络设备漏洞，中标方应提供项目验收后一年内的跟踪服务，对本次评估范围内的问题提供远程或现场技术咨询，对于漏洞的修补、问题的排除给出建议和指导。

第四章　评审办法和程序

一、评审办法和步骤

1、评标办法采用综合评分法。

2、评标步骤：先进行资格审查，然后由评标委员会进行符合性审查以及技术、商务的详细评审。只有通过资格审查、符合性审查的投标人才能进入详细评审。

二、资格审查

1. 根据财政部第 87 号令第四十四条的规定，采购人、招标代理机构对投标人的资格进行审查。

2.采购人、海南信华招标代理有限公司根据“资格审查表”（附表 1）对投标人的资格性进行评审，只有对“资格评审表”（附表 1）所列各项作出实质性响应的投标文件才能通过资格评审。有以下情况的将不能通过初步评审：

- 投标人未能满足投标人资格要求的；
- 投标人未按招标文件要求的金额提交投标保证金的；
- 投标有效期不足的；
- 不符合招标文件规定的其它条件。

3. 判断投标文件的响应与否只根据投标文件本身，而不寻求外部证据。

4.通过资格审查的投标人不足三家，则本次招标失败。

三、符合性审查

1.评标委员会根据“符合性审查表”（附表 2）对通过资格审查的投标文件的符合性进行评审，只有对“符合性审查表”所列各项作出实质性响应的投标文件才能通过符合性审查。对是否实质性响应招标文件的要求有争议的投标内容，评标委员会将以记名方式表决，得票超过半数的投标人有资格进入下一阶段的评审，否则将被淘汰。

2. 判断投标文件的响应与否只根据投标文件本身，而不寻求外部证据。

3. 评标委员会在符合性审查中，对算术错误的修正原则如下：

（1）开标一览表内容与投标文件中明细表内容不一致的，以开标一览表为准

（2）投标文件的大写金额和小写金额不一致的，以大写金额为准；

（3）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准；

（4）单价金额小数点有明显错位的，以总价为准并修改单价。

（5）若投标人不同意以上修正，投标文件将视为无效。

4.评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，将要求其在评标现场接到通知后 20 分钟内提供书面说明，必要时提交相关证明材料。投标人不能证明其报价合理性的，评标委员会将其作为无效投标处理。

5.通过符合性审查的投标人不足三家，则本次招标失败。

四、详细评审

1. 评标委员会根据评审办法对通过初步评审的投标文件进行详细评审，并进行技术和商务的评审打分。

2. 技术、商务评分：具体评审的内容详见（附表 3）；

3. 价格分统一采用低价优先法计算，将通过初步评审的所有投标人最低的投标价格，即满足招标文件要求且价格最低的投标价为基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算：

价格分=(基准价 / 投标报价)×价格权值×100

4. 如投标人满足第二章第 17 条“关于政策性加分”规定的，应按该条规定对投标人的评标价进行调整。

5.技术、商务及价格权重分配

包号	评估因素	技术、商务	价格
A 包	权重	70%	30%
B 包	权重	90%	10%

6. 综合评分及其统计：按照评标程序、评分标准以及分值分配的规定，评标委员会成员分别就各个投标人的技术、商务状况，其对招标文件要求的响应情况进行评议和比较，评出各投标人的得分，得分与投标报价分相加得出综合得分。综合得分最高的投标人为第一中标候选投标人，综合得分次高的投标人为第二中标候选投标人，以此类推。综合得分相同的，按投标报价由低到高顺序排列。综合得分和投标报价均相同的，按技术指标由优至劣顺序排列。

附表 1

资格审查表

项目名称：三亚市公安局信息系统安全建设　　包号：　　包

项目编号：HNXHZB2018-046

序号	审查项目	评议内容（无效投标认定条件）	投标人 1	投标人 2	投标人 3
1	投标有效期	是否满足招标文件要求			
2	投标报价	是否超过最高限价或预算金额			
3	投标人的资格	是否符合投标人资格要求			
4	保证金	是否提交保证金的			
结　　论					

1、表中只需填写“√/通过”或“×/不通过”。

2、在结论中按“一项否决”的原则，只有全部是√/通过的，填写“合格”；只要其中有一项是×/不通过的，填写“不合格”。

3、结论是合格的，才能进入下一轮；不合格的被淘汰。

采购人代表：　　海南信华招标代理有限公司代表：

海南信华招标代理有限公司

年　　月　　日

附表 2

符合性审查表

项目名称：三亚市公安局信息系统安全建设　　包号：　包

项目编号：HNXHZB2018-046

序号	审查项目	评议内容（无效投标认定条件）	投标人 1	投标人 2	投标人 3
1	投标文件的有效性、完整性	是否符合招标文件的式样和签署要求			
2	报价项目完整性	是否对本项目内所有的内容进行投标，漏报其投标将被拒绝			
3	投标报价	投标价是否固定价且投标价是唯一的			
4	工期或交货期	是否满足招标文件要求			
5	其它	无其它无效投标认定条件			
6	结　　论				

1、表中只需填写“√/通过”或“×/不通过”。

2、在结论中按“一项否决”的原则，只有全部是√/通过的，填写“合格”；只要其中有一项是×/不通过的，填写“不合格”。

3、结论是合格的，才能进入下一轮；不合格的被淘汰。

评　委：

海南信华招标代理有限公司

年　　月　　日

附表 3

技术、商务评分表（A 包）

项目名称：三亚市公安局信息系统安全建设

项目编号：HNXHZB2018-046

序号	评比项目			满分
1	技术部分（45 分）	技术方案与招标需求的吻合程度	方案整体设计合理性、技术先进、成熟、可扩展性，方案完整性、前后一致性；方案以可研报告为基础，逐项需求细化，具有前瞻性。 优：5 分；良好 3-4 分；一般 1-2 分；不合格 0 分	5
			实施方案完整，实施工作安排及售后服务合理。 优：5 分；良好 3-4 分；一般 1-2 分；不合格 0 分	5
		需求指标响应情况	投标人对需求指标响应情况，完全满足为满分，带▲的重要条款，有一项不满足要求扣 2 分；其他不满足要求扣 1 分，扣完为止	35
2	商务部分（25 分）	投标人实力部分	投标人持有效中国信息安全认证中心颁发的信息系统安全集成服务资质：壹级得 3 分，贰级得 2 分，叁级得 1 分，无得 0 分。（需提供资质证书复印件并加盖公章，原件备查）	3
			投标人持有效信息技术服务运行维护标准符合成熟度贰级（含）以上证书得 3 分，叁级证书得 2 分，肆级证书得 1 分，否则得 0 分。（需提供证书复印件并加盖公章，原件备查）	3
			投标人持有效国家信息安全漏洞库（CNNVD）技术支撑单位等级证书壹级得 2 分，贰级（含）以下得 1 分，无得 0 分。（需提供资质证书复印件并加盖公章，原件备查）	2
			投标人持有效中国信息安全认证中心颁发的信息系统应急处理服务资质：二级（含）或以上得 2 分，三级得 1 分，无得 0 分。（需提供证书复印件并加盖公章，原件备查）	2
			投标人持有效中国信息安全认证中心颁发的信息安全风险评估服务资质：二级（含）或以上得 2 分，三级得 1 分，无得 0 分。（需提供证书复印件并加盖公章，原件备查）	2
			投标人项目团队成员具有中国电子信息行业联合会或工业和信息化部认证的项目经理 3 人（含）及以上，得 2 分；1 至 2 人，得 1 分；否则得 0 分。（提供相关人员证书复印件和最近 3 个月社保缴纳证明，社保缴纳单位必须与投标单位名称一致，加盖公章）	2
			1. 投标人具有 ISO9001 质量管理体系认证证书； 2. 投标人具有 ISO/IEC 20000-1:2011 信息技术服务管理体系认证证书； 3. 投标人具有 ISO/IEC 27001:2013 信息安全管理活	3

			动体系认证； 具备三个得 3 分，具有二个得 2 分，具有一个得 1 分，没有得 0 分（需提供证书复印件并加盖公章，原件备查）	
		技术服务支持	投标人具有可靠的技术服务支持 技术服务队伍人数≥15 人，得 5 分 技术服务队伍人数≥10 人，得 3 分 技术服务队伍人数≥6 人，得 1 分 （提供技术服务团队近期 3 个月社保缴纳记录复印件，原件备查）。	5
		类似项目经验	2015 年以来投标人完成 200 万以上（含 200 万）同类项目案例，每个合同案例得 1 分，最高得 3 分。（需提供相合同复印件并加盖公章，原件备查）	3
3	价格部分（30 分）	价格项得分=（评标基准价 / 投标报价）×价格权值×100		30
4	评比总得分（100 分）			100

评委：

技术、商务评分表（B 包）

项目名称：三亚市公安局信息系统安全建设

项目编号：HNXHZB2018-046

序号	评标细项	评 分 细 则	分值
1	公司资质（20 分）	投标单位具有 ISO9001 质量管理体系认证，有得 5 分，无得 0 分；（提供证书复印件，原件备查）	5
2		投标单位近期三年内参与中国合格评定国家认可委员会组织的等级保护测评能力验证活动，结果为 2 次满意的得 5 分，1 次满意的得 3 分，没有得 0 分；（提供证明材料复印件，原件备查）	5
3		具有省级或以上网络与信息安全通报中心颁发技术支撑单位证书，有得 5 分，无得 0 分；（提供证书复印件，原件备查）	5
4		投标单位近两年获得过国家网络安全等级保护工作协调小组办公室颁发的全国网络安全等级保护测评机构先进单位的得 5 分，无得 0 分；（提供证书复印件，原件备查）	5
5	人员资质（25 分）	为保障项目进度，在项目实施中投标人应安排足够的测评师参与本项目，其中承诺安排等保测评师数量≥6 人，得 5 分，3-5 人，得 3 分，3 人以下得 1 分，没有不得分。（须提供等保测评师证书及社保证明复印件，且社保缴纳单位必须与投标单位名称一致，原件备查）	5
6		实施人员中有注册信息安全专业人员（CISP），有得 5 分，无得 0 分；	5
7		实施人员中有项目经理资格证书，有得 5 分，无得 0 分；	5
8		实施人员中有通过国内安全厂商工程师级别认证证书，有得 5 分，无得 0 分；	5
9		实施人员中有通过网络排错专家级别认证，有得 5 分，无得 0 分；	5
10	技术方案（20 分）	技术方案应含如下重点内容：被测信息系统的详细描述及分析；测评对象与指标；测评方法与工具；测评相关工作的实施计划； 重点评价方案编写的质量，包括方案是否符合采购单位的实际现状，并对方案的客观性、准确性、公正性、符合性等进行评价。 优秀得 9-10 分，良好得 5-8 分，一般得 1-4 分，差为 0 分。	10
11		具有较完整的风险说明及风险规避处置措施。 优秀得 9-10 分，良好得 5-8 分，一般得 1-4 分，差为 0 分。	10

序号	评标细项	评 分 细 则	分值
12	**项目管理（10 分）**	投标人按招标人要求有明确的建设质量目标，质量保证措施，并具有详细可行的实施内容等。 优秀得 9-10 分，良好得 5-8 分，一般得 1-4 分，差为 0 分。	10
13	**案例（5 分）**	投标人近三年内具有同类项目的合同案例，每个得 1 分，最高得 5 分，无得 0 分；	5
14	**整改咨询（5 分）**	测评完成之后，投标人承诺提供整改咨询服务，且所提供的整改建议科学、合理、有效、并承诺及时跟进。 优秀得 4-5 分，良好得 2-3 分，一般得 1 分，差为 0 分。	5
15	**售后服务（5 分）**	售后服务措施得当，内容完整，可操作性和针对性强。 优秀得 4-5 分，良好得 2-3 分，一般得 1 分，差为 0 分。	5
16	**报价评分（10 分）**	满足招标文件要求且投标价格最低的投标报价为评标基准价，报价得分统一按照下列公式计算： 投标报价得分=（评标基准价/投标报价）×价格权重	10
	合计		100

评委：

第五章 合同条款

甲方：_____

乙方：_____

甲乙双方根据____年____月____日三亚市公安局信息系统安全建设（项目编号:HNXHZB2018-046）公开招标结果及招标文件的要求,经协商一致,同意以下专用条款作为本项目合同条款的补充。当合同条款与专用条款不一致时，以专用条款为准。

一、合同标的及金额等(详见附件清单)

序号	产品名称	品牌型号、规格、参数	单价（元）	数量	单位	合计（元）	备注
1							
2							
合同总额		（小写）：¥ 元					
		（大写）： 元整					

二、交货期：合同签订后 天内。

三、合同通用条款

（双方友好协商）

四、付款方式

A 包：

1、合同签订后，甲方凭乙方开具的正式有效发票向乙方支付合同金额的 30%作为项目预付款；

2、主要设备到货并经甲方验收后 10 个工作日内，甲方凭乙方开具的正式有效发票向乙方支付合同金额的 20%；

3、项目安装、调试并通过验收后 10 个工作日内，甲方凭乙方开具的正式有效发票向乙方支付合同金额的 45%；

4、项目验收通过后一年后无质量问题，甲方凭乙方开具的正式有效发票向乙方支付合同剩余 5%款项（质保金）。

B 包：

（双方友好协商）

五、违约赔偿

1. 除下一条规定的不可抗力外，如果乙方没有按照合同规定的时间交货和提供服务，甲方可从合同款中扣除违约赔偿费，每延迟一个工作日迟交货物（含软件及相关服务）或未提供服务或提供产品及服务不满足项目需求，按合同金额的 1%/天计扣违约赔偿费。但违约赔偿费的最高限额为合同金额的 10%。如果乙方延迟交货时间超过一个月，甲方有权终止合同，并按合同约定及法律规定追究乙方的违约责任。

2. 如果双方中任何一方由于战争、严重火灾、水灾、台风和地震以及其它经双方同意属于不可抗力的事故，致使合同履行受阻时，履行合同的期限应予以延长，延长的期限应相当于事故所影响的时间。

六、合同纠纷处理

本合同履行过程中发生纠纷，应协商解决，协商不成，可向人民法院提起诉讼解决。

七、合同生效

本合同由甲乙双方签字盖章后生效。

八、合同鉴证

招标代理机构应当在本合同上签章，以证明本合同条款与招标文件、投标文件的相关要求相符并且未对采购内容和技术参数进行实质性修改。

九、本合同的组成文件

1. 合同通用条款和专用条款；

2. 招标文件、乙方的投标文件和评标时的澄清函（如有）；

3. 中标通知书；

4. 甲乙双方商定的其他必要文件。

上述合同文件内容互为补充，如有不明确，由甲方负责解释。

十、合同备案

本合同一式陆份，中文书写。甲方、乙方各执两份，招标代理机构各执一份，另外一份由招标代理机构报政府采购主管部门备案。

甲方：_____**（盖章）**　　**乙方：**_____**（盖章）**

地址：_____　　地址：_____

法定（或授权）代表人：_____　　法定（或授权）代表人：_____

开户行：_____　　开户行：_____

户名：_____　　户名：_____

帐号：_____　　帐号：_____

_____年___月____日　　_____年___月____日

招标代理机构声明：本合同标的经海南信华招标代理有限公司依法定程序采购，合同主要条款内容与招投标文件的内容一致。

招标代理机构：海南信华招标代理有限公司（盖章）

经办人：_____

_____年___月____日

第六章 投标文件内容和格式

请投标人根据本招标文件要求，按以下格式、内容制作投标文件，并按以下顺序编制目录及页码：

1、投标函（表 1）

2、开标一览表（表 2）**（注：须单独密封一份，否则将拒收投标文件）**

3、技术及资质要求响应表（表 3）

4、投标人简介

5、营业执照副本、税务登记证、组织机构代码证复印件（或者三证合一复印件），投标人资格要求中的所有材料复印件

6、保证金缴纳证明复印件

7、企业纳税证明或者会计师事务所出具的财务审计报告

8、社会保障缴费记录复印件

9、授权委托书（表 4，报价文件正本原件，副本复印件）

10、法人代表、授权代表身份证复印件

11、参加政府采购活动前三年内，在经营活动中没有重大违法记录的声明函（表 5，注：同时提供“信用中国”、“中国政府采购网”和“信用三亚”网站信用查询页面截图。）

12、同类项目业绩表（表 6）

13、技术部分（包括设计方案、实施方案、所投产品彩页、技术资料、售后服务、培训等）

14、投标人认为需要的其它材料

为了便于评委对报价文件内容的审核，投标人可针对招标文件第六章中“技术、商务评分表”编写响应页码索引表，即投标文件中关于该评分项目内容的页码。

注：以上复印件均需要加盖公章或投标专用章

表 1、投标函

致：海南信华招标代理有限公司

根据贵单位 三亚市公安局信息系统安全建设 （项目编号为：HNXHZB2018-046）的投标邀请函，正式授权下述签字人_____（姓名和职务）代表投标人_____（投标单位名称）提交投标文件。

根据此函，我们宣布同意如下：

1、我方接受招标文件的所有的条款和规定。

2、我方同意按照招标文件第二章“投标人须知”的规定，本投标文件的有效期为从投标截止日期起计算的 60 天，在此期间，本投标文件将始终对我方具有约束力，并可随时被接受。

3、我们同意提供贵单位要求的有关本次投标的所有资料或证据，并保证资料、证据的真实有效性。

4、我方完全理解贵方不一定要接受最低投标价的投标，即**最低投标价不是中标的保证**。

5、如果我方中标，我们将根据招标文件的规定严格履行自己的责任和义务。

6、如果我方中标，我方将按规定支付本次招标的服务费。

投标人名称：_____（公章）

地址：_____邮编：_____

电话：_____传真：_____

授权代表：（签字或私章）_____ 职务：_____

日期：_____

表 2、开标一览表（A 包）

项目名称：三亚市公安局信息系统安全建设

项目编号： HNXHZB2018-046

工　　期：合同签订后_____天内。

序号	产品名称	品牌型号、规格配置	单位	数量	单价	小计
1						
2						
3						
4						
5						
…						
投标总额		（小写）				
		（大写）				

投标人全称：（盖章）　　授权代表：（签名或私章）

注：1、投标总金额包括本包招标书中要求的所有货物、运输、服务、人工、税等费用；

2、开标一览表格式不得自行改动。

开标一览表（B 包）

项目名称：三亚市公安局信息系统安全建设

项目编号： HNXHZB2018-046

工　　期：采购人下达测评通知书后_____个日历天内交付测评报告。

序号	项目名称	报价	备注
1			
	…….		
投标总额		（小写）	
		（大写）	

投标人全称：（盖章）　　授权代表：（签名或私章）

注：1、投标总价包括本招标书中要求的所有服务的费用。

2、开标一览表格式不得自行改动。

表 3、技术及资质响应表

说明：投标人必须仔细阅读招标文件中所有技术规范条款和相关功能要求，并对所有技术规范、功能条目及资质要求列入下表，未列入下表的视作投标人不响应。带▲或★的指标列入下表时，必须在指标前面保留▲或★。**投标人必须根据所投产品的实际情况（技术资料）如实填写，评标委员会如发现有虚假描述的，该投标文件无效，该投标人列入黑名单，并报政府采购主管部门严肃处理。**

序号	设备/项目	招标文件技术参数/功能要求	投标人技术参数/功能响应描述	偏离情况	页码索引
1					
2					
3					
4					
5					
	…				

投标人全称：（公章）　　授权代表：（签字或私章）

注：1、此表为表样，行数可自行添加，但表式不变。

2、**此表后面按响应顺序附上第三章中要求的各产品资质文件、检测报告等复印件（如有），否则视为不满足。**

3、投标人在“投标人技术参数/功能描述” 中填写所投设备/项目的详细技术参数或功能描述情况，投标人必须如实填写。

4、偏离情况说明分正偏离、完全响应、负偏离，分别表示优于要求、满足要求、不满足要求。**评委评标时不能只根据投标人填写的偏离情况说明来判断是否响应**，而应认真查阅“投标文件技术参数/功能响应”内容以及相关的技术资料判断是否满足要求。

5、“页码索引”指“投标人技术参数/功能描述”所对应证明材料在投标人投标文件中的页码。

表 4、授权委托书

致 海南信华招标代理有限公司：

本授权书声明：

委托人：_____

地　址：_____ 法定代表人：_____

受托人：姓名_____ 性别：____ 出生日期：____年__月__日

所在单位：_____职务：_____

身 份 证：_____联系方式:_____

兹委托受托人_____代表我方参加海南信华招标代理有限公司组织的三亚市公安局信息系统安全建设（项目编号为：HNXHZB2018-046 ）的招标活动，并授权其全权办理以下事宜：

1、参加投标活动；

2、出席开标评标会议；

3、签订与中标事宜有关的合同；

4、负责合同的履行、服务以及在合同履行过程中有关事宜的洽谈和处理。

受托人在办理上述事宜过程中以其自己的名义所签署的所有文件我方均予以承认。受托人无转委托权。

委托期限：至上述事宜处理完毕止。

委托单位：（公章）

法定代表人：（签名或私章）

受托人：（签名或私章）

_____年_____月_____日

表 5、参加政府采购活动前三年内，在经营活动中没有重大违法记录的声明函

致：海南信华招标代理有限公司

为响应贵公司组织的三亚市公安局信息系统安全建设（项目编号：HNXHZB2018-046）货物及服务的招标采购活动，我司声明如下：

本项目招标公告前三年内，我司在经营活动中没有被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单等重大违法记录。

如有虚假，我司愿意接受相关处罚。

特此声明。

注：同时提供“信用中国”、“中国政府采购网”和“信用三亚”网站信用查询页面截图。

投标人名称：_____（公章）

地址：_____邮编：_____

电话：_____传真：_____

授权代表：_____（签字或私章）_____ 职务：_____

日期：_____

表 6、投标人项目业绩表

项目名称：三亚市公安局信息系统安全建设　　项目编号：HNXHZB2018-046

序号	项目名称	项目内容	合同金额	签约时间	业主联系人电话	备注

投标人全称（公章）：　　授权代表（签名或私章）：

注：1、在此表后面按顺序附上各项目的合同复印件。

表 7、生产厂商授权书

海南信华招标代理有限公司：

作为设在_____（制造厂家地址）的制造/生产_____（货物名称）的 _____（制造厂家名称）在此以制造厂的名义授权_____（投标人名称和地址）用我厂制造的上述货物参加海南信华招标代理有限公司组织的采购项目编号为 HNXHZB2018-046 的三亚市公安局信息系统安全建设的投标活动及后续的合同谈判和签署合同。

我们在此保证以合作人来约束自己，并为上述投标人就此次招标而提交的货物承担全部质量保证责任及按招标文件要求提供售后服务。

（可增加其它服务承诺内容）

我方于_____年____月____日签署本文，以此为证。

投标人名称：_____

出具授权书的制造厂家名称：_____

姓　　名：_____（制造厂授权代表签名或私章）

职　　务：_____　　联系电话：_____

公　　章：_____　　日　　期：_____

注：1、如投标人所投产品为国外品牌产品，生产厂家在国内有注册分支机构的由注册分支机构出具授权，否则由国内的总代理出具授权（总代理需附上代理证明）。所投产品为国内品牌产品的，由生产厂家或负责该区域的分公司或注册机构出具授权。

2、授权出具单位如有内部格式授权书，可以按其格式出具，但必须包含上述格式文件的意思表达。

3、制造厂盖章可以为公章或授权专用章。

4、制造厂商参与投标则无需提供此授权书。