质疑函

一、质疑供应商基本信息：

质疑供应商：柳州市友方科技发展有限责任公司

地址：柳州市三中路 117 号　　邮编：545001

联系人：杨柳萍　　联系电话：130[redacted]

授权代表：杨柳萍

联系电话：130[redacted]

地址：柳州市三中路 117 号　　邮编：545001

二、质疑项目基本情况：

质疑项目的名称：购买网络安全防护设备

质疑项目的编号：LZZC2022-J1-990752-GXJD

采购人名称：柳州市公安局交通警察支队

质疑事项：

□采购文件　　采购文件获取日期：2022 年 11 月 21 日

□采购过程

√成交结果

三、质疑事项具体内容

质疑事项 1：招标文件第三章采购需求 01 分标：堡垒机，11.用户登录堡垒机支持多种认证方式，包括本地静态密码认证、LDAP 认证、RADIUS 认证、证书认证、USBKEY 认证、短信认证、手机 APP 动态密码认证等身份认证方式；支持可知因素和不可知因素的双因素认证；其中证书认证支持国密算法。（提供相关证明材料，包括但不限于彩页、产品功能截图等）；14.支持自动发现运维人员运维过程中创建的后门账号行为，并以列表方式向设备管理员展示托管设备中所有的后门账号信息。18.支持按部门、设备类型、业务类型、设备组等多

种方式备份托管设备的设备账号和密码，密码备份文件支持 excel 和 html 方式加密保存；24.支持基于访问权限定义高危操作。支持基于时间、IP/IP 段、用户/用户组、设备/设备组、设备账号、命令关键字、命令关键字正则表达式、危险级别等组合条件设置告警规则 ，当用户越权执行某些特定命令或者使用特权的时候进行告警、记录及阻断。中标公司“北京启明星辰信息安全技术有限公司”投标并中标的产品“启明星辰 OSM-7800-CFT”无法满足招标参数。

事实依据：中标供应商北京启明星辰信息安全技术有限公司官方网站上无法体现该公司产品具备“11.支持可知因素和不可知因素的双因素认证”、“14.支持自动发现运维人员运维过程中创建的后门账号行为，并以列表方式向设备管理员展示托管设备中所有的后门账号信息”、“18.支持按部门、设备类型、业务类型、设备组等多种方式备份托管设备的设备账号和密码，密码备份文件支持 excel 和 html 方式加密保存”、“24.支持基于访问权限定义高危操作。支持基于时间、IP/IP 段、用户/用户组、设备/设备组、设备账号、命令关键字、命令关键字正则表达式、危险级别等组合条件设置告警规则，当用户越权执行某些特定命令或者使用特权的时候进行告警、记录及阻断”的产品功能，无法满足招标参数。

1、启明星辰官网查询链接：https://www.venustech.com.cn/new_type/blj/

2、官网功能截图（附件一）

法律依据：违反了《中华人民共和国政府采购法》中

第三条 政府采购应当遵循公开透明原则、公平竞争原则、公正原则和诚实信用原则。

第三十八条中(五)确定成交供应商。谈判结束后，谈判小组应当要求所有参加谈判的供应商在规定时间内进行最后报价，采购人从谈判小组提出的成交候选人中根据符合采购需求、质量和服务相等且报价最低的原则确定成交供应商，并将结果通知所有参加谈判的未成交的供应商。

第七十七条 供应商有下列情形之一的，处以采购金额千分之五以上千分之十以下的罚款，列入不良行为记录名单，在一至三年内禁止参加政府采购活动，有违法所得的，并处没收违法所得，情节严重的，由工商行政管理机关吊销营业执照;构成犯罪的，依法追究刑事责任:(一)提供虚假材料谋取中标、成交的。

质疑事项 2： 招标文件第三章采购需求 02 分标：**防火墙、服务器区入侵检测，项号 3 服务器区入侵检测，第 2.▲吞吐量≥15Gbps，并发连接≥600 万，新建≥12 万；业务接口：千兆电口≥5 个，万兆光口≥2 个，双电源，配置硬盘≥1T；中标公司“北京启明星辰信息安全技术有限公司”投标并中标的产品“启明星辰 NGIPS8000-ZX(万兆)”无法满足招标参数。**

事实依据：北京启明星辰信息安全技术有限公司 ，型号：启明星辰 NGIPS8000-ZX(万兆)官网参数为“吞吐量 14Gbps，并发连接 1000 万”不符合招标参数实质性参数“▲吞吐量≥15Gbps”。

1、公开官网 https://www.venustech.com.cn/new_type/rqfyIPS1/

2、官网功能截图（附件二）

法律依据：违反了《中华人民共和国政府采购法》中

第三条 政府采购应当遵循公开透明原则、公平竞争原则、公正原则和诚实信用原则。

第三十八条中(五)确定成交供应商。谈判结束后，谈判小组应当要求所有参加谈判的供应商在规定时间内进行最后报价，采购人从谈判小组提出的成交候选人中根据符合采购需求、质量和服务相等且报价最低的原则确定成交供应商，并将结果通知所有参加谈判的未成交的供应商。

第七十七条 供应商有下列情形之一的，处以采购金额千分之五以上千分之十以下的罚款，列入不良行为记录名单，在一至三年内禁止参加政府采购活动，有违法所得的，并处没收违法所得，情节严重的，由工商行政管理机关吊销营业执照;构成犯罪的，依法追究刑事责任:(一)提供虚假材料谋取中标、成交的。

招标文件第三章采购需求 七）“采购需求”中带”▲”号的为关键性参数及要求，竞标产品必须满足，否则竞标无效。

四、与质疑事项相关的质疑请求：

请求：要求中标单位提供的投标产品进行功能及性能验证测试，若技术检测不通过或检测结果与投标文件不符的即为虚假应标，重新审查中标公司的投标文件，作废中标结果

签字（签章）：杨柳萍

公章：柳州市友方科技发展有限责任公司

日期：2022 年 12 月 14 日

附件一

堡垒机

需求分析

随着企业信息化进程不断深入，企业的IT系统变得日益复杂，不同背景的运维人员违规操作导致的安全问题变得日益突出起来，主要表现在：内部人员操作的安全隐患、第三方维护人员安全隐患、高权限账号滥用风险、系统共享账号安全隐患、违规行为无法控制的风险。

运维操作过程是导致安全事件频发的主要环节，所以对运维操作过程的安全管控就显得极为重要。而防火墙、防病毒、入侵检测系统等常规的安全产品可以解决一部分安全问题，但对于运维人员的违规操作却无能为力。如何转换运维安全管控模式，降低人为安全风险，满足企业要求，是当下所面临的迫切需求。

产品简介

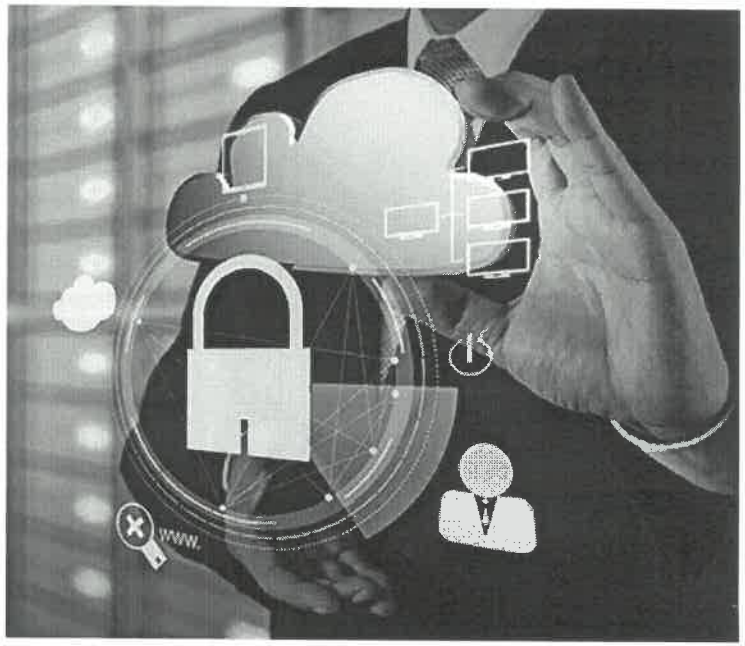
天玥运维安全网关，俗称堡垒机，能够对运维人员维护过程进行全面跟踪、控制、记录、回放；支持细粒度配置运维人员的访问权限，实时阻断违规、越权的访问行为，同时提供维护人员操作的全过程的记录与报告；系统支持对加密与图形协议进行审计，消除了传统行为审计系统中的审计盲点，是IT系统内部控制最有力的支撑平台。运维过程三个阶段进行严格管控：

事前预防：建立“自然人-资源-资源账号”关系，实现统一认证和授权

事中控制：建立“自然人-操作-资源”关系，实现操作审计和控制

事后审计：建立“自然人-资源-审计日志”关系，实现事后溯源和责任界定

功能特点



部署方式灵活性： 天玥运维安全网关支持单机、双机、分布式部署多种部署方式，并支持NAT和网口聚合方式，适应多变业务场景。

操作使用便捷性： 天玥运维安全网关提供多种运维方式、C/S运维客户端、资源批量登录、命令批量执行、设备自动改密等多种功能以保证运维过程的自动和快捷性。

管控方式严格性： 天玥运维安全网关提供命令限制与复核、应用发布防跳转、运维账号IP、MAC限制等。严格的管控方式以保证运维过程的规范性。

审计效果精细化： 数据库协议深度解析、数据库返回行数记录、Oracle数据库变量绑定解析。

认证方式多样性： 天玥运维安全网关包括多样认证方式，支持对不同用户设置不同认证方式组合的双因素认证，更具灵活性。

运维协议全面性： 天玥运维安全网关支持多种运维访问协议，能够充分满足日常运维需要。

技术优势

堡垒机分身

虚化出多台堡垒机，适用于分权分域的用户管理场景。

虚拟化部署

支持VMware、VirtualBox、KVM和Xen（HVM）虚拟化环境部署。

运维操作防跳转

防止通过应用发布服务器进行跳转登录未授权资源。web页面防跳转功能，进行http/https访问过程时运维人员仅允许访问授权地址。

双重审计

实现数据库协议、字符协议、文件传输协议命令和录像的双重审计。实现命令审计和录像审计的关联检索和回放。

命令限制与复核

对于高危命令实现实时告警或阻断。对于特别重要的命令实现多人审核。

数据库深度解析

数据库协议级审计。数据库返回行数记录。Oracle数据库变量绑定解析。

敏感数据管控

运维人员拥有高权限系统账号，会接触到重要敏感数据。对运维人员上传、下载、流转重要敏感数据进行控制和记录。

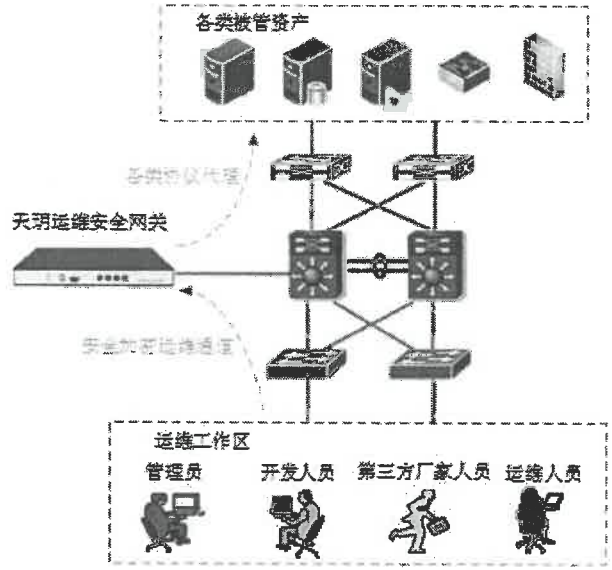
典型应用

单双机部署：

天玥运维安全网关旁路方式部署于网络中，无需对网络结构进行任何调整。

运维人员直接访问天玥运维安全网关的对应端口，建立安全加密的数据通道，然后发起到服务器对应服务的访问，无需直接访问服务器，从而进一步加强内部服务器的安全性。

支持HA双机热备部署，以避免单点故障隐患，最大程度满足运维的可靠性和连续性。



分布式部署：

支持添加多台堡垒机作为协议代理服务器，分担主堡垒机性能压力，扩展运维能力。

多协议代理服务器节点可访问相同资源时实现自动负载均衡。

主堡垒机集中管理配置和日志信息。

大规模应用

某省电信网管中心部署堡垒机集群32台，接入资源7000多个，发布运维工具60多个、编辑工具6个、专用工具9个。

运维用户同时在线5520人，并发7800多个会话的压力下，用户体验依然良好。

云合作模式

与某电子政务云服务商合作，由云服务商以增值服务的方式向他们的租户推广我们的云堡垒机。

我们为云服务商提供云堡垒机软件和授权，并且按照授权中云资产管理数量每年向云服务商收取相应的授权费用。

发展历程

性能参数

系列名称	产品形态	并发会话数	网络接口
OSM-2600 系列	1U 机架式软硬一体设备，单电源	字符并发≥ 400 个或图形并发≥ 100 个	默认自带 6 个千兆电口，1 个扩展插槽
OSM-4600 系列	1U 机架式软硬一体设备，液晶屏，单电源	字符并发≥ 800 个或图形并发≥ 200 个	默认自带 6 个千兆电口，2 个扩展插槽
OSM-6600 系列	1U 机架式软硬一体设备，液晶屏，双电源	字符并发≥ 1200 个或图形并发≥ 400 个	默认自带 6 个千兆电口，4 个千兆光口，2 个扩展插槽
OSM-8600 系列	2U 机架式软硬一体设备，液晶屏，双电源	字符并发≥ 2400 个或图形并发≥ 800 个	默认自带 6 个千兆电口，2 个扩展插槽

产品简介

天玥运维安全网关，俗称堡垒机，能够对运维人员维护过程进行全面跟踪、控制、记录、回放；
支持细粒度配置运维人员的访问权限，实时阻断违规、越权的访问行为，
同时提供维护人员操作的全过程的记录与报告；
系统支持对加密与图形协议进行审计，消除了传统行为审计系统中的审计盲点，
是IT系统内部控制最有力的支撑平台。

产品优势

产品型号覆盖全应用场景：IPv6、BM、国产化

高易用性
独有的CS客户端，
无需安装任何控件

自动化运维
账号自动巡检、
网络设备配置自动备份、
命令自动执行等

深度协议解析
数据库命令级权限控制、
自动改密、
变量和下行行效审计

强安全性
应用发布防跳转、
SSH强加密、
RDP安全层SSL加密

客户收益

满足合规性要求
顺利通过IT审计

有效减少核心信息资产
的破坏和泄露风险

有效控制运维风险
有利于事后原因追查
和界定责任

实现独立审计与三权分立
完善IT内控机制

权威认证

销量排名第一
CCID《中国运维安全审计产品市场研究报告（2017）》

销量排名第一
CCID《中国运维安全审计与防护产品市场研究报告（2018）》

销量排名第一
CCID《中国运维安全审计与防护产品市场研究报告（2019）》

销量排名第一
FROST & SULLIVAN
堡垒机中国地区市场调研报告（2019）

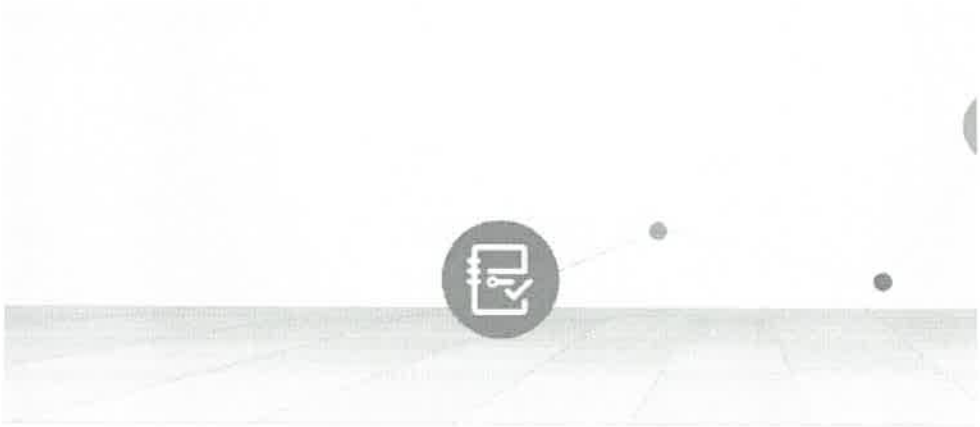
销量排名第一
IDC《中国运维安全管理硬件产品市场份额》报告（2020）

用户价值

天玥运维安全网关（堡垒机）：

完善内控内审，满足合规要求：目前，越来越多的单位面临一种或者几种合规性要求。堡垒机提供的完备审计方案，可以完善组织的IT内控与审计体系，从而满足各种合规性要求，并且使组织能够顺利通过IT审计。

简化运维管理，提高运维效率：堡垒机对账号和资产进行统一管理，规范简化运维流程。提供多种运维操作方式以满足各种不同使用习惯。自动便捷的使用体验提供整体运维效率。



附件二

入侵防御IPS

天清入侵防御系统

需求分析

入侵攻击的检测及防御，是用户保障信息系统安全的核心需求之一，然而，有限的安全预算下如何防御日益更新的多样化攻击，对用户来说是个艰巨的挑战。入侵防御（IPS）正是解决该问题的最佳解决方案：在线部署的入侵防御系统不但能发现攻击，而且能自动化、实时的执行防御策略，有效保障信息系统安全。由此可见，对于入侵攻击识别的准确性、及时性、全面性以及高效性，是优秀入侵防御产品必备条件。

产品简介

天清入侵防御系统（Intrusion Prevention System，以下简称“天清NGIPS”）是启明星辰自主研发的网络型入侵防御产品，围绕深层防御、精确阻断的核心理念，通过对网络流量的深层次分析，可及时准确发现各类入侵攻击行为，并执行实时精确阻断，主动而高效的保护用户网络安全。

天清入侵防御系统融合了启明星辰在攻防技术领域的先进技术及研究成果，使其在精确阻断方面达到国际领先水平，可以对漏洞攻击、蠕虫病毒、间谍软件、木马后门、溢出攻击、数据库攻击、高级威胁攻击、暴力破解等多种深层攻击行为进行防御，有效弥补网络层防护产品深层防御效果的不足。

型号概述：天清入侵防御系统 NGIPS8000-ZX（万兆）
（1）2U机架式设备，标配1个独立管理口，1个HA口，1个console口，配置8个万兆端口（含4个SPF+万兆多模光模块，传输距离>=300M），8个千兆光口（不含光模块），8个千兆电口；内置8T硬盘，双电源（单个电源能支持设备满负荷运行）；尺寸（深宽高）:500*440*88 mm；
（2）实际网络环境处理能力（混合包、混合流）：14Gbps（应用层吞吐量），并发连接数：1000万。

技术优势

采用高性能专用硬件

搭配启明星辰自主研发的安全操作系统，稳定安全高效

领先的威胁防御能力

ADlab和VenusEye两大团队保障，及时应对最新攻击和高级威胁

双引擎高效病毒防护

内置知名第三方防病毒引擎，高效查杀

全面的内容过滤功能

实时监控敏感信息通过邮件、Web外发

完善的应用控制能力

支持上千种应用识别能力，防止网络资源滥用

保障业务的高可靠性

软硬件BYPASS、HA优先保障业务畅通

方便的集中管理功能

多设备统一管理、升级、监控并生成报表，省时省力

典型应用

启明星辰入侵防御产品已广泛应用于政府、金融、能源、电信等各行业领域，并积极拓展国际市场。根据CCID报告，启明星辰IDS/IPS产品已连续18年（至2019年）国内市场占有率第一；根据IDC报告，启明星辰IDS/IPS产品已连续6年（至2020年）排名市场第一；启明星辰在2016、2017连续2年成功入围Gartner IDPS魔力象限，成为少数入围Gartner魔力象限的国内厂商之一。
天清入侵防御系统V6.0典型应用如下：

- 透明部署于企业内联网、互联网网络边界：不改变原有网络拓扑，执行流量的深层次分析和攻击防御，保护子网终端及服务器的安全。

- 分布式部署统一管理：分布式部署于各个子网边界的入侵防御设备，可通过天清集中管理与数据分析中心软件统一管理起来，进行统一安全策略的配置、特征库升级、日志收集存储及集中监控。
- 与天阗APT联动，构建高级威胁防御方案

1.天清NGIPS对边界流量进行深层分析及防御，还原协议中包含的文件
2.天清NGIPS对文件执行恶意代码静态检测，同时将文件提交给天阗APT引擎
3.天清NGIPS从天阗APT引擎获取文件的准确检测结果及Callback特征
4.天清NGIPS针对Callback特征生成防护策略，执行自动防护

用户价值

天清入侵防御系统（IPS）以其领先的攻击防御能力，在确保业务可用性的同时，可准确、及时、全面、高效的帮助用户抵御多样化的入侵攻击，尽可能的降低用户在攻击事件处理上的人力和资金投入，获得最佳的投资收益。