**青岛特殊钢铁有限公司**

**信息安全提升项目**

**技术协议**

甲方：青岛特殊钢铁有限公司

乙方：

2023年12月

**目 录**

[1、总则 - 3 -](#_Toc632754785)

[2、现状分析 - 3 -](#_Toc370651551)

[3、 项目建设内容、设备清单和建设要求 - 4 -](#_Toc1838041357)

[4、技术资料及交付进度 - 12 -](#_Toc408825004)

[5、性能保证值考核 - 13 -](#_Toc1321655475)

[6、双方人员派遣 - 13 -](#_Toc1640207404)

[7、技术支持和售后服务 - 14 -](#_Toc1865746136)

[8、双方当事人的权利和义务 - 14 -](#_Toc39094258)

[9、解决争议的方法 - 15 -](#_Toc2074681871)

[10、其他 - 15 -](#_Toc486229558)

甲乙双方就青岛特殊钢铁有限公司信息安全提升项目所涉及的技术问题进行了充分协商，达成共识，形成以下条款：

# 1、总则

1.1本协议的使用范围，仅限于青岛特殊钢铁有限公司信息安全基础设备实施项目的实施及售后服务等方面。

1.2本协议提出的是最低限度的技术要求，并未对一切技术细节做出规定，也未充分引述有关标准和规范条文，乙方应保证提供符合本技术协议和有关最新工业标准的优质产品及服务。

1.3在签订合同后，甲方保留对本技术协议提出补充要求和修改的权利，乙方应予以配合。

1.4所有系统软件采用最新成熟版本，应用软件开放、不加密，所有系统、软件、程序及相关数据库至少提供不低于30年的授权或永久授权，供甲方免费试用，且软件为正版，软硬件及程序无加密，除本技术协议另有规定外，不再有其它包括第三方授权、服务费、年费等任何形式的费用，甲方无需另行向乙方支付其他任何费用。项目涉及到的与运行相关的工艺技术、源代码不涉及到乙方独有的核心知识产权的，都应该给甲方并进行专业知识培训，硬件、自动化运维、软件的画面及程序修改、编写要开放给甲方，保证甲方后期检维修、数据修改及增减，以及数据的上传和下载，并将软件、画面及程序备份至甲方存储设备上，确保甲方能独立自主维护。

1.5项目实施必须基于甲方现有施工现场、网络及软硬件平台环境，项目的实施不得影响甲方目前现场与信息化的各类应用。若因前期准备不充分导致对甲方现有环境或项目本身产生不利影响，一切后果皆由乙方负全部责任，甲方有权对遭受的损失向乙方提出索赔。

1.6由乙方根据本项目具体计划及策略，按时实施。本项目为交钥匙工程(项目)，除规定范围的内容，其余一切软硬件、人工、运输等为完成工程(项目)所必需的物资及相关工作均由乙方负责甲方不再负担任何费用、物资。

# 2、现状分析

青岛特殊钢铁有限公司目前已有VPN设备使用多年，设备故障率高，而且每年VPN设备自身都会有0day漏洞出现，容易成为被入侵的突破口；

新建的DMZ区域没有对应的入侵防御设备和Web层防护设备对其敏感业务进行安全防护；

目前DMZ业务和核心业务运行的服务器平台暂未采取有效隔离策略，DMZ区域需要单独隔离的超融合平台承载区域的敏感业务，避免与核心业务之间直接互通，造成业务互扰。同时需要配置DMZ区域的汇聚交换机配套使用。

# 项目建设内容、设备清单和建设要求

**3.1 建设内容**

3.1.1升级现有2套VPN为分离式架构的零信任设备，作为业务安全访问控制系统，将公司外业务访问权限跟用户身份和使用终端对应起来；

3.1.2新增DMZ区域的入侵防御设备和Web防火墙设备，提供针对DMZ区域敏感业务的L2-L7层的安全防护能力;

3.1.3新增3台超融合设备，作为DMZ区域的业务承载平台；

3.1.4新增2台汇聚交换机，为DMZ区域提供交换互联。

**3.2配置要求：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 名称 | 数量 | 单位 | 功能及性能要求 |
| 1 | 零信任安全  体系 | 2 | 套 | 1、每套提供一台零信任控制中心硬件设备，内存≥16G，冗余电源，≥6个千兆电口，≥4个千兆光口SFP。  2、每套配置550个零信任并发授权。  3、为方便维护人员管理应用权限，支持直接在应用授权界面为单一应用或某个应用分类分配用户授权，授权方式支持直接授权给用户所在的组织架构、用户关联的角色或用户本身，并展示应用直接授权的组织架构、授权角色或用户数量。  4、支持配置是否允许用户自助申请应用访问权限，启用后，管理员可以在控制台根据审批状态查看应用申请详情，包括但不限于：申请时间、用户名、所属组织架构、角色、应用名称、应用访问地址、申请理由、申请有效期等。  5、PC和移动端的零信任客户端均支持由用户自主切换客户端语言为中文或英文。  6、要求无缝替换现有的SSL VPN设备，包含但不限于账号信息、用户权限、客户端软件等，应实现用户在打开现有VPN客户端时直接升级成零信任客户端来登录访问业务，管理员可以自行通过配置决定升级完成后是否卸载原VPN客户端。  7、要求实现终端All in one功能，通过现有PC版EDR客户端推送零信任客户端，安装完成后两个客户端合为一个客户端，减少用户桌面客户端数量。  8、支持不同平台的终端同时在线，管理员可分别设置可同时在线的PC或移动终端个数，配置范围不小于0-1000，当超过终端个数时，可以注销最早登录的终端，且被注销的终端有对应的注销提醒。  9、为方便统一管理用户的终端，支持为接入系统的终端设置标签，支持通过终端标签来配置特殊的上线准入策略及应用访问策略。终端标签应至少内置内网终端、外网终端、开发终端、办公网终端等标签，且支持管理员自定义新增标签。  10、为了保障单位员工认证安全与便捷性的平衡，需支持设置授信终端绑定，支持配置绑定授信终端的可信网络区域、增强认证条件；并可限定用户可绑定的授信终端数量。  11、为强化系统认证安全性，可配置在触发异常环境的条件时，用户需完成增强认证才可登录。可配置的异常环境包括但不限于：帐号首次登录、帐号在该终端首次登录、账号在该地点首次登录、账号在新地点登录、账号在非常用地点登录、闲置帐号登录、弱密码登录、异常时间登录等。  12、为满足组织灵活的管理要求，支持配置动态上线准入规则和动态访问规则，可配置化的ACL规则引擎，可以灵活地将终端环境、用户身份、处置动作等进行配置。控制策略支持“与”、“或”条件嵌套，实现终端EDR的检测评分作为策略条件的功能。  13、为了最大程度缩小网络、业务暴露面，零信任平台需提供单包授权能力（SPA），支持UDP+TCP组合的单包授权技术，未授权用户无法连接零信任设备，无法扫描到服务端口，不会出现敲门放大漏洞。支持一人一码。  14、为了满足单位有序平滑、推广零信任接入，需支持零信任客户端的按需灰度升级。  15、支持替换用户登录页面的主题包，对登录页、产品logo、应用中心背景图进行替换。  16、每套提供一台零信任代理网关，最大理论加密流量≥300Mbps，最大并发用户数（个）≥3000。内存≥16G，≥6千兆电口，≥2千兆光口SFP。  17、支持将用户访问零信任系统的WEB资源访问流量解密后镜像给现有态势感知设备，以完善系统的用户行为审计溯源能力，提升设备自身的安全性。 18、要求零信任控制中心硬件设备、零信任代理网关设备均实现双机热备部署模式，单台设备故障不影响用户接入、业务访问等，并且零信任并发授权不受单台控制中心设备故障影响，可由任意一台设备承载。 |
| 2 | DMZ区WAF防火墙 | 2 | 台 | 1、性能参数：网络层吞吐量≥40Gbps，全威胁吞吐量≥2Gbps；（提供第三方检测机构出具的检测报告，并加盖中国合格评定国家认可委员会CNAS章或中国信息安全测评中心盖章）  2、硬件参数：X86架构，内存≥16G，硬盘≥480GB SSD，≥8个千兆电口（支持Bypass功能），≥2个万兆SFP+光口（满配光模块），提供三年规则库更新和质保服务。  3、并支持用户自定义URL保护范围和保护阈值。  4、支持防护SQL注入、XSS攻击、网页木马、网站扫描、Webshell、跨站请求伪造（CSRF）、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web漏洞攻击等。  5、支持语义引擎用于检测Web攻击，能针对不同类型的Web攻击如命令注入攻击防护等，单独选择开启或关闭语义引擎检测。  6、支持自定义Web应用防护规则，通过基于正则表达式自定义规则匹配方向、动作、字符串、危险等级、动作、攻击影响、描述等。  7、要求接入现有态势感知平台，实现平台展示报警信息和WAF防火墙封锁黑客攻击的信息。 |
| 3 | DMZ区入侵防御 | 2 | 台 | 1、性能参数：网络层吞吐量≥40Gbps，IPS吞吐量≥3.5Gbps；（提供第三方检测机构出具的检测报告，并加盖中国合格评定国家认可委员会CNAS章或中国信息安全测评中心盖章）  2、硬件参数：X86架构，内存≥16G，硬盘≥480GB SSD，≥16个千兆电口（支持Bypass功能），≥4个万兆SFP+光口（满配光模块），提供三年规则库更新和质保服务；  3、产品支持IPv4/IPv6双栈工作模式，以适应IPv6发展趋势；；  4、支持链路聚合功能，可将多条物理链路聚合成一条带宽更高的逻辑链路使用；  5、当上行/下行端口链路出现故障时，对应的另一端下行/上行端口自动切断链路；  6、设备具备独立的入侵防护漏洞规则特征库，特征总数在7000条以上；  7、支持对服务器和客户端的漏洞攻击防护，支持XSS攻击、SQL注入等WEB攻击行为进行有效防护；  8、可以针对检测到的攻击源IP进行联动封锁，支持自定义封锁时间；  9、支持根据国家/地区来进行地域访问控制，保障业务访问安全性；  10、支持细致的服务器敏感数据识别，识别维度包含服务器IP、业务重要性、识别方式、开放的服务与端口、敏感数据页面数以及更新时间等，并且可以进行详细的页面URL以及页面信息举证；  11、支持木马远控类、恶意链接类、移动安全类、异常流量类僵尸网络行为的检测；  12、要求接入现有态势感知平台，实现平台展示报警信息和入侵防御封锁黑客攻击的信息。 |
| 4 | DMZ区超融合 | 3 | 台 | 1、单台硬件配置要求  规格：2U  CPU≥ 2颗Intel Xeon Gold 63\*\* （16C）  内存≥ 512GB DDR4  系统盘≥ 2\*240GB SSD  缓存盘≥ 4\*1.92T SSD  数据盘≥ 8\*10T 机械硬盘  电源：冗余  千兆电口≥6个；万兆光口 ≥ 6个（满配模块）  服务器生产厂家仅限于联想、超聚变、浪潮  相应的超融合云管软件、计算虚拟化、存储虚拟化、网络虚拟化等永久授权  2、计算虚拟化  通过虚拟化技术将物理服务器虚拟化为一个逻辑计算资源池，开通后具备对虚拟机全生命周期管理的能力。  在超融合管理平台界面上提供虚拟机删除、开关机、挂起与恢复、重启、关闭、关闭电源、克隆、迁移、备份、模板导出、快照、标签管理等功能，并支持批量操作。  每个虚拟机都可以安装独立的操作系统，应支持Windows、 Linux，并且支持国产操作系统。  当某台物理节点发生意外故障，在其上运行的虚拟机能够自动漂移到其他正常的物理节点上并自动启动。  集群动态资源调度DRS，系统自动评估物理主机的负载情况，当物理主机负载过高时，自动将该物理主机上的虚拟机迁移到其他负载较低的主机上，确保业务持续稳定和集群主机负载均衡。  提供热添加CPU、内存、磁盘、网卡的功能，无需中断或停机即可实现虚拟资源的在线添加。  当云资源、虚拟机被删除后，将移入回收站，提供恢复和确认销毁。用户可自定义回收站云资源、虚拟机彻底删除时延。可恢复30天内已删除的云资源、虚拟机，30天以后自己删除，也可手动删除。  3、存储虚拟化功能要求  采用分布式的软件定义存储架构，在通用服务器部署，将所有服务器硬盘组织成一个虚拟存储资源池以提高资源利用率，无需独立的元数据及控制器节点，通过新增物理服务器可以实现存储容量和性能的横向扩展（Scale-Out架构），扩容过程保证业务零中断。  同一存储资源池混插磁盘，统一存储资源池异构服务器。  多种硬盘状态检测监控及告警，包括“健康”状态、“亚健康”状态、“故障”状态，不同状态的硬盘在UI上呈现不同的特征或告警，方便用户能够区分处理。  数据重建智能保护业务性能，可以对数据重建速度进行智能限速，避免数据重建过程中IO性能占用导致对业务的性能造成影响。  需支持云主机在线快照，用户能够在不影响现有业务的情况下，对云主机或单块云盘创建快照，以便业务发生故障时可以快速回滚覆盖原虚拟机或者生成全新虚拟机，进而恢复至业务健康状态。  坏道扫描及修复功能，发现坏道后，主动修复坏道区域的数据，及时恢复数据副本的冗余性；当硬盘的坏道数过多，系统能自动将该盘的数据迁移至其他健康的硬盘上，保障数据的安全。  多副本数据保护，跨节点跨机柜的副本保护机制，容忍跨节点机柜的宕机而业务数据不丢失。允许用户设置副本数量，可设副本数不少于2，最多支持副本数不少于3，动态调整副本数。  4、网络虚拟化功能要求  利用统一的管理平台对虚拟网络设备分布式虚拟交换机、虚拟路由器、虚拟应用防火墙、虚拟应用负载均衡）进行管理和配置，实现虚拟化平台与现有网络的兼容。  管理网、业务网、数据通信网（VXLAN）可复用相同物理网口，网口复用后，对不同网络平面进行流量控制和VLAN隔离。  提供网络可视化组件，可在图形化界面上观察到所有虚拟机的流量走向与访问关系，包括源IP、目的IP、访问次数、服务类型等。  虚拟机可使用IPv4、IPv6或双栈类型的网络，并可使用多种网络服务。  5、统一管理要求  要求能够被现有的云管平台统一管理，包含CPU、内存、网卡、硬盘、存储等，便于及时发现问题并提供相应建议。  支持设置告警类型（紧急和普通）、告警内容（集群、主机、虚拟机、CPU、内存、存储），针对告警信息平台可自动给出告警处理建议，同时支持将告警信息以短信和邮件方式发送给管理员。  6、质保及升级服务  软、硬件质保3年；云平台等相关模块软件3年免费升级，且提供原厂工程师现场升级服务保障，支持跨大版本升级，升级过程不影响云主机业务。影响应用或信息安全的bug、漏洞等，不受年限限制免费升级或修补。   1. 配件：IBMstorwizeV7000硬盘/2.4TB 10K 12Gb SAS\*2块; HPproliant d1580 gen10硬盘/900G 15K SAS DS \*2块； |
| 5 | DMZ区汇聚交换机 | 2 | 台 | 1、24个万兆光口，24个千兆电口，2个40GE QSFP+光口，包转发率≥1000Mpps，配置冗余电源。  2、配置一条40G的堆叠线缆，12个万兆多模光模块，12根多模光纤线。  3、硬件质保3年，软件更新3年。 |

备注：以上产品所有授权，均注明授权给“青岛特殊钢铁有限公司”，设备的生产日期须在2023年11月之后。

**3.3建设要求：**

3.3.1 应用标准和设计原则

《中华人民共和国网络安全法》

《信息系统安全等级保护基本要求》（GB/T 22239-2008）；

3.3.2 实施内容要求

1. 所有设备需配套提供相关连接线缆，网关设备连接不低于万兆；
2. 所有设备按照要求安装到指定位置，完成设备加电运行、测试等；
3. 设备调试前，须对原有环境进行专业的梳理，提供配置现状、配置规划、割接规划等完整的实施方案，经甲方确认后方可进行配置；
4. 配置完成后，须进行试运行，验证配置、性能、功能等是否满足实际需求，为后续正式割接提供基础保障；
5. 正式割接前，须经甲方同意，在割接窗口时间内完成设备割接，不得影响日常生产办公业务；
6. 割接完成后，须按照甲方要求完成设备标签标识、线缆标签标识等，并对线缆进行标准化的困扎整理；
7. 项目验收前，须对每台设备的配置、管理、维护等进行专业的培训，培训内容、时间、范围由甲方指定；
8. 须提供完整准确的项目竣工资料，作为验收的依据。

**3.3设备清单**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 信息安全提升项目清单 | | | | | |
| 序号 | 名称 | 数量 | 单位 | 基本配置 | 建议品牌 |
| 1 | 零信任安全体系 | 2 | 套 | 详见3.2配置要求中的零信任安全体系 | 深信服 |
| 2 | DMZ区WAF防火墙 | 2 | 台 | 详见3.2配置要求中的DMZ区WAF防火墙 | 深信服、天融信、网御星云 |
| 3 | DMZ区入侵防御 | 2 | 台 | 详见3.2配置要求中的DMZ区入侵防御 | 深信服、天融信、网御星云 |
| 4 | DMZ区超融合 | 3 | 台 | 详见3.2配置要求中的DMZ区超融合 | 青云、星辰天合、深信服 |
| 5 | DMZ区汇聚交换机 | 2 | 台 | 详见3.2配置要求中的DMZ区汇聚交换机 | 华为 、锐捷、信锐、H3C |

# 4、技术资料及交付进度

4.1电子文档以WORD、EXCEL、PDF格式提供；

4.2每次交付的资料附资料清单；

4.3项目交付的资料包括但不限于：

* 设备到货前

《施工现场情况登记表》

* 设备到货后

《货物签收单》

* 安装部署中

《单项安装测试记录表》

《安装测试报告》

* 项目验收前

《试运行方案》

《试运行记录》

《验收方案》

* 项目验收后

《设备硬件安装规范》

《设备技术手册》

《设备安装手册》

《设备维护操作手册》

《设备测试与验收手册》

《设备培训手册》

4.4.设备随机资料

提供的设备随机资料，主要包括（但不限于）：

1）装箱清单；

2）产品合格证、质量检验证书；

3）装配图纸、原理图、接线图、系统图等（若有）；

4）安装使用说明书、操作和维修手册；

4.5交付进度

项目实施过程中各阶段提供。

# 5、性能保证值考核

所供设备须提供第三方检测机构出具的检测报告，加盖中国合格评定国家认可委员会CNAS章，包含但不限于以下内容：

1. 零信任网关

最大理论加密流量≥300Mbps

最大并发用户数（个）≥3000。

1. WAF防火墙

网络吞吐量≥40Gbps（1518字节转发理论最大性能）

全威胁吞吐量≥2Gbps

并发连接数≥400万（使用connection方式，选用http协议，爬坡时间<延迟时间<释放时间）

新建连接数≥18万（使用connection方式，选用http协议，使用rst结束）

1. 入侵防御

网络吞吐量≥40Gbps（1518字节转发理论最大性能）

IPS吞吐量≥3.5Gbps

并发连接数≥400万（使用connection方式，选用http协议，爬坡时间<延迟时间<释放时间）

新建连接数≥15万（使用connection方式，选用http协议，使用rst结束）

# 6、双方人员派遣

6.1项目实施团队拟派遣项目经理需有类似项目的实施经验，且须承诺全职参与；

6.2项目实施团队中须有专业服务工程师，且工作年限不少于3年；

6.3项目经理及项目核心人员不得随意更换。如需更换应征得青岛特钢同意并更换同等或更高资历人员；如在青岛特钢不同意的情况下更换项目经理及项目组核心人员，青岛特钢有权解除合同，并赔偿青岛特钢因此带来的一切损失；

6.4甲方将向乙方派出技术人员参与项目的实施。

# 7、技术支持和售后服务

7.1技术支持内容、范围

在项目实施过程中，乙方应提供相应技术服务，起内容包含以下几个方面：

①向甲方提供与本项目相关的技术咨询；

②向甲方提供项目实施的技术诀窍、实施经验、注意事项；

③向甲方提供相关的标准、规范；

④向甲方提供项目实施过程中的其他技术服务。

7.2知识转移服务

通过培训、指导、文档资料等多种形式将项目的各种知识转移给青岛特钢。

7.3质保服务

本项目建设内容的质量标准均满足本技术要求及国家现行的相关标准和规范，并遵守国家关于质量质保及赔偿的相关规定。

①接受和配合甲方对项目建设质量、安全及工期的监督；

②在项目的实施过程及质保期内出现质量问题，乙方将无偿进行更换、维护，若出现重大损失将根据合同规定进行赔偿；

③对项目使用过程中出现的问题或甲方在原需求设计整体不变的情况下提出的局部修改意见，在质保期内由乙方负责完善，超过质保期的，由双方协商解决；

④在质保期内指定专人7\*24小时（每周七天，每天24小时）反馈解决甲方的技术支持及系统问题，需要解决的问题，技术人员应在半小时内电话响应，远程响应无法解决的24小时内到达现场解决；

⑤系统在运行阶段给予配合及支持。

# 8、双方当事人的权利和义务

8.1甲乙双方对对方提供的资料都有保密责任，未经对方同意，不得转让或许可第三方使用；

8.2乙方负责甲方相关人员的培训，做好知识转移工作；

8.3在合同执行期间，如果供方提供的所有设备/备件有缺陷，供方应立即无偿赔付与缺陷设备/备件数量相同的设备/备件，赔偿期限应不迟于证实属供方责任之日起的 15 天内。供方应承担由此给需方造成相应损失的赔偿责任；

8.4项目实施过程中，乙方自行负责住宿和餐饮，甲方只提供办公场所。

8.5**所有硬件设备的整体使用寿命均不得少于5年，配件使用寿命不少于3年，使用寿命期间出现问题需乙方免费解决。**

# 9、解决争议的方法

未尽事宜，应由双方友好协商解决，若存在争议，15日协商不成，按商务合同通过法律途径解决。

# 10、其他

10.1本技术协议书一式肆份,甲方三份、乙方一份，均具有相同的法律效力。

10.2本技术协议是商务合同不可分割的一部分，与商务合同具有同等的法律效力。甲乙双方代表签字后与商务合同同时生效。

10.3根据甲乙双方的具体要求，未尽事宜友好协商解决，并可签订书面补充协议。

（以下无正文）

甲 方：青岛特殊钢铁有限公司 乙 方：

代表签字： 代表签字：

日期： 日期：