2023

智安网络

ZHIAN NETWORK

云保-等级保护建设系统

技术白皮书

AQ-CP-010 V1.2

市场指南

深圳市智安网络有限公司

www.zhiannet.com

智安网络
ZHIAN NETWORK

目录

1. 概述……1
2. 产品简介……1
   2.1 产品概述……1
   2.2 安全能力……2
   2.3 产品特点……3
3. 平台功能……4
   3.1 DDoS 防火墙……4
   3.2 云防火墙……4
   3.3 Web 应用防火墙……5
   3.4 漏洞扫描……7
   3.5 主机防护系统……8
   3.6 安全审计……9
   3.7 堡垒机……9
   3.8 数据备份……10
4. 交付方式……11
   4.1 云保（SaaS 服务）……11
   4.2 智安等保一体机（硬件一体机方案）……12
   4.3 私有化部署方案……15
5. 客户案例……16
   5.1 河北省某地级市政府……16
   5.2 四川省某投资集团……16
   5.3 北京市某网络科技公司……17
6. 关于我们……18

1. 概述

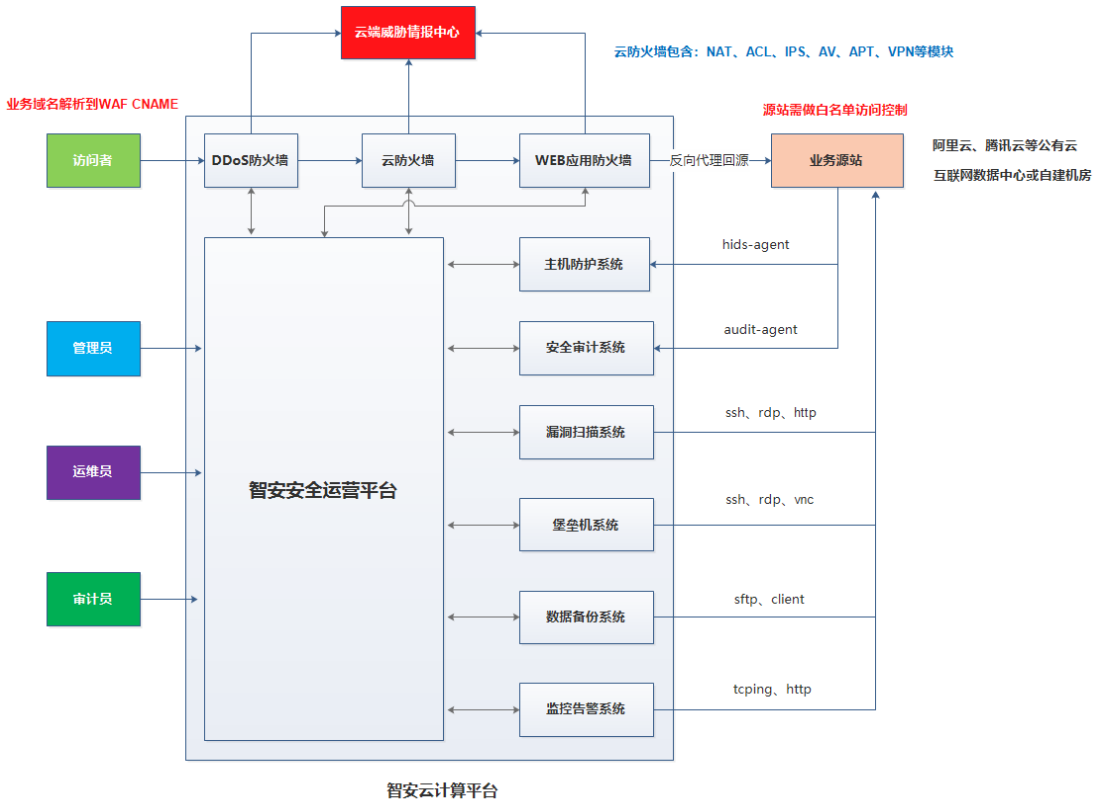
随着网络技术的不断发展和普及，网络安全问题也变得日益突出。网络安全涉及到保护网络系统、数据和用户免受各种威胁和攻击的问题。这些威胁包括黑客攻击、病毒和恶意软件、社会工程学攻击等，可能导致数据泄露、系统瘫痪、财务损失等严重后果。《网络安全法》和《数据安全安全法》的出台，国家对网络安全重视程度达到新高度。

为了应对这些威胁和满足客户对网络安全保护的需求，智安网络推出了基于智安网络云计算平台的云综合防御平台，并配备专业的入侵防御特征库、病毒库、应用协议库、URL 库，是目前业界领先的一站式安全合规平台。平台高可用性、高性能和高可靠性的特别，使得可以放心规模部署于数据中心、大型园区网等各种复杂场景；另外，功能丰富并可按需扩展的方案，也简化了网络的安全架构，并大大降低了企业网络总体拥有成本。

2. 产品简介

2.1 产品概述

智安云综合防御平台（等保云平台）是一套基于智安云计算平台构建的综合型安全运营平台，集成了 DDoS 防火墙、云防火墙、WEB 应用防火墙、主机防护系统、APT 防御系统、上网行为管理、SSL VPN、漏洞扫描、数据备份、数据库审计、日志审计、堡垒机、安全监测等安全组件，满足等保 2.0 相关标准和企业安全运营实战需求。



2.2 安全能力

安全要求	安全组件	功能介绍
安全通信网络	云防火墙	提供统一的互联网边界、内网 VPC 边界、主机边界流量管控防护，包括结合情报的实时入侵防护、全流量分析可见、智能化访问控制、日志溯源分析等能力。通过简单易用的方式交付，全面防护各类威胁，并具备多重智能模型和智能联动手段，可持续对抗不断出现的各类新风险。支持 ACL、流控、NAT、上网行为管理、SSL VPN 等服务。支持入侵防御和病毒防护。
安全区域边界	DDoS 防火墙	配置 DDoS 高防，将恶意攻击流量进行清洗过滤，为用户提供的抗 DDoS 服务。可抵御 SYN Flood、ICMP Flood 等各种常见的 DDoS 攻击，具有配置简单、公网 IP 不用换、防护能力强、防护对象能灵活更换等特点。
	WEB 应用防火墙	通过防御 SQL 注入、XSS 跨站脚本、常见 Web 服务器

		插件漏洞、非授权核心资源访问等恶意行为攻击，过滤海量恶意 CC 攻击，避免网站资产数据泄露，保障网站的安全与可用性。支持 WEB 应用防护、网页防篡改、防扫描、黑链、漏洞分析服务等
安全计算环境	堡垒机	实现对云上服务器的集中管控和运维审计等安全能力
	安全审计	提供虚拟化审计能力，提供数据库审计、主机审计、应用审计、设备审计。保障云上数据及资产的安全
	数据备份	提升主机整体安全性的服务，提供威胁情报、资产采集、合规基线、漏洞风险、安全监控、入侵威胁等服务,帮助企业降低主机安全风险
	漏洞扫描	漏洞扫描服务支持对企业外部网络、主机、系统、WEB 服务、中间件、应用等进行专业漏洞扫描；针对扫描结果形成专业漏洞扫描报告；支持对漏洞进行归类，并提供专家级修复建议，帮助客户更加精细化管理业务。精准的漏洞扫描及安全风险检测，漏洞扫描结合情报大数据、透测试实战经验和深度机器学习，提供全面资产威胁检测
安全管理中心	云综合防御平台	安全管理中心统一管理云平台安全组件上的能力，通过数据分析提供合理的资源调配，控制运维成本开支提升管理效率

2.3 产品特点

功能丰富，满足安全合规要求：针对等级保护“一个中心”,“三重防护”要求，提供全面的安全组件和服务快速过测评；

灵活部署，多业务场景支持：根据业务系统实际网络环境(公有云、IDC 托管、自建机房)， 支持 SaaS、私有化、一体机等方式部署；

统一运维，管理模式多元化：采用统一的安全服务平台，用户只需要一个平台即可统一管理各种安全功能，安全运维更简单；

弹性调度，业务安全有保障：CDN 节点遍布全国，形成一张巨大的调度网络，自动弹性调度，用户的请求将就近访问 CDN 节点，保证业务的安全可用。

3. 平台功能

3.1 DDoS 防火墙

DDoS 防火墙以智安云覆盖全球的 DDoS 防护网络为基础，结合智安云 AI 智能 DDoS 防护体系，提供 T 级别的 DDOS 攻击防护，打破了传统集中式高防架构的局限性，以布局全球的高防集群和数据中心资源为基础结合智能调度算法，实现全网分布式联动防御，有效抵御超大流量 DDoS、CC 攻击，保证业务的安全、快速、可持续交付；

- **策略配置：**随支持根据流量触发阈值和防御阈值来选择宽松、适中、严格、超级严格等防护策略；支持一键开启或关闭 DDoS 防护。
- **屏蔽列表：**支持对入侵 IP 进行自动屏蔽；支持对已屏蔽 IP 进行解除屏蔽；支持一键释放全部屏蔽 IP。
- **黑白名单：**支持对入侵 IP 进行自动加黑处理；支持手动添加黑名单和白名单数据；支持删除已有的黑名单或白名单。
- **流量分析：**支持查看每分、每时、每月、每年的流量数据；支持查看最大输入流量、最大输出流量、平均输入流量、平均输出流量。
- **连接分析：**支持查看每分、每时、每月、每年的连接数据；支持查看最大 TCP 连接次数、最大 UDP 连接次数、平均 TCP 连接次数、平均 UDP 连接次数。
- **攻击分析：**支持按攻击时间、攻击类型、攻击状态、攻击目标进行多条件查询；支持查看攻击的目的地址、目的端口、开始日期、开始日期、结束日期、攻击类型、高层协议、攻击状态、最大流量、攻击源地址。

3.2 云防火墙

平台基于“一个中心三重防护”的合规理念进行设计，结合控制转发与管理审计分离的设计思路，由云防火墙实现安全通信网络和安全区域边界的防护。云防火墙组件构成一体化全方位的防御体系能够基于传统防火墙的五元组进行安全策略配置，还可以基于应用、用户、时间等条件进行安全策略配置。提供一体化的策略，对于

所有策略条件进行融合，提供统一配置界面。此外，云防火墙由于采用商用高性能大规模防火墙，能有效抵御 DDOS 攻击外，基于智安网络全球范围内的有效应用进行识别，可对全球 URL 分类过滤，基于云端推送的威胁进行防御，结合第三方入侵防护，病毒过滤技术进行有效防护。

- **访问控制策略：**随着 WEB2.0 技术的蓬勃发展和动态端口的新应用层出不穷，使得传统网关产品采用五元组的访问控制方式早已变得力不从心，而云防火墙基于 7 元组以及时间的访问控制策略，能有效的控制自然人、应用的访问控制；

- **入侵防御：**在蠕虫、后门、木马、间谍软件、Web 攻击、拒绝服务等攻击的防御方面具备了完善的检测、阻断、限流、审计报警等防御手段，并随时关注业界最新发现的安全漏洞和接收全球用户反馈的攻击特征，并在第一时间做出响应和提供更新，实时完善攻击特征库，提供最及时、最全面的入侵防御。

- **病毒防护：**实时病毒连接阻断，病毒事件日志记录，提供超过 800W 条病毒特征数据。

- **APT 威胁检测：**支持对可疑域、可疑 IP、可疑文件、可疑 HTTP、恶意端口扫描、DNS 消耗等威胁进行实时监测与防护。

- **上网行为管理：**支持对指定网站、指定终端进行访问限制，支持对非法网站访问行为进行自动拦截，可展示详细的上网行为日志和分析信息。

- **SSL VPN：**提供基于 OpenSSL 库的应用层 VPN。

3.3 Web 应用防火墙

Web 应用防火墙，是一款集静态资源、缓存、代理、安全防护、日志、统计、监控于一体的智能 WEB 应用防火墙。可以对内部的业务访问进行访问控制和业务审计，防范来自内部的威胁。相比于传统的硬件 WAF，等保云的虚拟 WAF 更专注于 WEB 应用

自身的漏洞，并基于智安网络全国海量防御节点和资深的安全技术能力，结合智安网络态势感知平台、全球智能调度系统，提供无上限防护 DDoS 攻击服务，WEB 攻击防御，并且提供了 SSL 加速，应用负载均衡等 WEB 应用安全模块，为业务安全保驾护航。

- 常见 Web 应用攻击防护：

1） 防御 OWASP 常见威胁：支持防御以下常见威胁：SQL 注入、XSS 攻击、Webshell 上传、后门隔离保护、命令注入、非法 HTTP 协议请求、常见 Web 服务器漏洞攻击、核心文件非授权访问、路径穿越、扫描防护等。

2） 网站隐身：不对攻击者暴露站点地址、避免其绕过 Web 应用防火墙直接攻击。

3） 识别精准：内置语义分析+正则双引擎，黑白名单配置，误报率更低。支持防逃逸，自动还原常见编码，识别变形攻击能力更强。

4） 0day 补丁定期及时更新：防护规则及时更新最新漏洞补丁，第一时间全球同步下发最新补丁，对网站进行安全防护。

- CC 攻击防护：

1） 对单一源 IP 的访问频率进行控制，基于重定向跳转验证，人机识别等。

2） 针对海量慢速请求攻击，根据统计响应码及 URL 请求分布、异常 Referer 及 User-Agent 特征识别，结合网站精准防护规则进行综合防护。

- 精准访问控制

1） 支持 IP、Path、Referer、User-Agent 等 HTTP 常见字段的条件，配置强大的精准访问控制策略。

2） 与 Web 常见攻击防护、CC 防护等安全模块结和，搭建多层综合保护机制；依据需求，轻松识别可信与恶意流量。

3） 支持黑白名单、国家地区运营商封锁、SSL 管理，TCP/HTTP/WS 协议反向

代理，CDN 缓存加速。

- 高级 Web 应用安全防护

1） 支持多种端口：支持除 80 和 443 以外的非常用端口的防御需求。

2） 扫描器爬虫防护：自定义扫描器与爬虫规则，用于阻断非授权的网页爬取行为，添加定制的恶意爬虫、扫描器特征，使爬虫防护更精准。

3） 黑白名单设置：添加始终拦截与始终放行的黑白名单 IP，增加防御准确性。

4） 网页防篡改：对网站的静态网页进行缓存配置，当用户访问时返回给用户缓存的正常页面，并随机检测网页是否被篡改。

5） 网站反爬虫：动态分析网站业务模型，结合人机识别技术和数据风控手段，精准识别爬虫行为。

6） 误报屏蔽：针对特定请求忽略某些攻击检测规则，用于处理误报事件。

7） 隐私屏蔽：避免在防护事件日志中，出现用户名或者密码等敏感信息。

8） 防敏感信息泄露：防止在页面中泄露用户的敏感信息，例如：用户的身份证号码、手机号码、电子邮箱等。

3.4 漏洞扫描

智安网络等保云经过多年的安全研究沉淀和全球服务实践经验的基础上，研发的一款用于评估网络运行环境风险的产品，可以对各类服务器、网络设备、安全设备等操作系统环境、数据库环境、WEB 应用等进行综合漏洞扫描检测。该系统主要用于分析和指出存在的相关安全漏洞即被测系统的薄弱环节，给出详细的检测报告，在业务环境受到危害会签为安全管理员提供专业、有效的安全分析和修补建议。该系统从系统扫描、Web 扫描、数据库扫描、安全基线扫描和弱口令扫描五大类发现信息系统、网站页面、数据库安全漏洞，检查系统存在的弱口令，收集系统必要开放的账号、服务、端口，检查不合规的设备配置，形成整体安全风险报告，帮助安全管

理人员限于攻击者发现安全问题，及时进行自我修补。

- **系统扫描：**主要用于分析和指出有关网络的安全漏洞及被测系统的薄弱环节，给出详细的检测报告，并针对检测到的网络安全隐患给出相应的修补措施和安全建议。全方位检测信息系统存在的主机、软件的安全漏洞，安全配置问题，弱口令，不必要开放的账户、服务、端口，独创的端口识别技术，结合丰富的协议指纹库，能自动快速准确的识别出非标准开放端口和应用服务类型，准确扫描端口对应的服务漏洞，避免扫描过程中的漏报和误报；
- **Web 扫描：**全面支持 OWASP 检测，可以帮助用户充分了解 Web 应用存在的安全隐患，建立安全可靠的 Web 应用服务，改善并提升应用系统抗各类 Web 应用攻击的能力（如：注入攻击、跨站脚本、文件包含、钓鱼攻击、信息泄漏、恶意编码、表单绕过等），协助用户满足等级保护、PCI、内控审计等规范要求；

3.5 主机防护系统

适应公有云、私有云及混合云架构，采用自适应安全及端点检测及响应（EDR）的解决方案，提供云+端的云安全管理平台为用户解决公有云、私有云和混合云环境中可能遇到的安全及管理问题；独立的自助安装界面，支持自动生成下载和安装命令。

- **系统支持：**支持 Windows 2003、Windows 2008、Windows 2012、Windows 2016、Ubuntu、Centos、RedHat、Fedora、Suse、OpenSuse、Debian 等操作系统
- **主机体检：**支持采集已安装轻代理主机中的各类信息，支持采集主机内外网 IP、主机名、操作系统、安装时间、在线状态等信息；支持对主机进行一键体检。
- **文件事件：**支持检测暴力破解、账号异常登录、进程异常等安全事件
- **病毒查杀：**支持发现二进制病毒木马信息，包含病毒的 hash、路径、发现世界，并且提供对病毒的隔离。

- **合规基线：**提供常用的 linux 及 windows 系统基线模板，支持基线检查及异常项展示,并提出修复建议。
- **完整性监控：**监控文件和目录的完整性情况，包括文件被修改、删除和新增。

3.6 安全审计

提供数据库安全审计、主机安全审计、应用安全审计；以高性能日志采集能力与强大的分析功能，对大量分散数据库、主机及应用的日志进行统一管理、集中存储、统计分析、快速查询，为用户提供真正可信赖的事件追责依据和业务运行的深度安全。

- **数据库审计：**支持 MySQL、Oracle、SQL Server、MongoDB 等市面上大多数的数据库日志审计。多维度分析，识别并预警风险语句。
- **日志审计：**支持对 Windows、 Linux 等主机日志审计、支持 Nginx、IIS、Tomcat 等应用中间件日志审计、支持各种网络设备的日志审计。
- **报告订阅：**提供丰富的报告展示，可订阅日报、周报、月报。
- **安全告警：**支持自定义告警规则；支持按关键词、告警周期、目标资产进行指定告警规则；支持站内信、邮件、钉钉等方式告警。

3.7 堡垒机

提供的核心系统运维和安全审计的管控平台，可集中管理资产权限，全程管控操作行为，实时还原运维场景，保障运维行为身份可鉴别、权限可管控、操作可审计，解决众多资产难管理、运维职责权限不清晰以及运维事件难追溯等问题， 助力企业满足等保合规需求。

- **资源管理：**集中资源账户管理，资源账户全生命周期管理，实现单点登录资源，管理或运维无缝切换。支持 SSH、RDP、VNC、TELNET 等协议类型主机资源。

- **运维审计：**全程记录用户的运维操作，支持多种运维审计技术和审计形式，可随时审计用户操作行为，识别运维风险，为安全事件追溯和分析提供依据。

3.8 数据备份

为云内的云服务器、云硬盘进行备份，通过备份快速恢复数据，保证业务安全可靠。在数据误删除、云服务器宕机、黑客攻击或病毒入侵情况下都可以通过备份快速恢复数据，保证业务不受影响。

4. 交付方式

4.1 云保（SaaS 服务）

4.1.1【方案描述】

云保（SaaS 服务），以智安一站式等保云平台+安全合规专家的服务形式，为客户提供一站式等保咨询整改服务。产品完全云化部署，客户通过 IP 地址切换、DNS 域名切换等方式接入，无需对现有系统的软件、硬件做任何迁移或调整。不需要客户具备专业安全知识，安全专家全程指导操作。最快 10 分钟内可实现无缝快速接入；

4.1.2【适用场景】

客户待测评系统的源站是在互联网中可访问的（公有云、私有云、VPC、IDC 等场景均满足），特别适用于没有安全运维人员、没有特殊的数据私密要求、想省心过等保的企业客户。只需在等保平台上开通账号并配置待测评系统相关信息后，即可满足等保测评要求。

4.1.3【方案优势】

- **功能丰富：**多种安全组件满足用户在等保建设过程中所需的各类安全防护需求。
- **配置灵活：**安全组件能够持续更新和扩展，为用户持续提供全方位的防护。
- **管理统一：**安全组件通过内部网络通讯联动，出现安全事件时可快速做出响应。
- **部署快速：**采用 All In One 的设计理念，缩短安全服务的交付周期
- **一站式服务：**一站式合规检测服务，覆盖等保 2.0 检测、隐私合规检测、安全合规检测、等保过检加固。

4.1.4【接入流程】

登录智安一站式等保云平台，配置 WAF 回源规则，获得高防 CNAME 并更换业务域名解析为高防 CNAME，完成业务流量接入。

登录测评系统关联的服务器，安装和配置主机防护 agent、安全审计 agent，然后登录智安一站式等保云平台配置堡垒机和数据备份，完成管理流量接入。

4.1.5【计费方式】

- 计费方式：半年、包年计费；
- 根据客户实际等保评级（二级或三级）情况，按测评系统套数收费。

4.1.6【产品套餐】

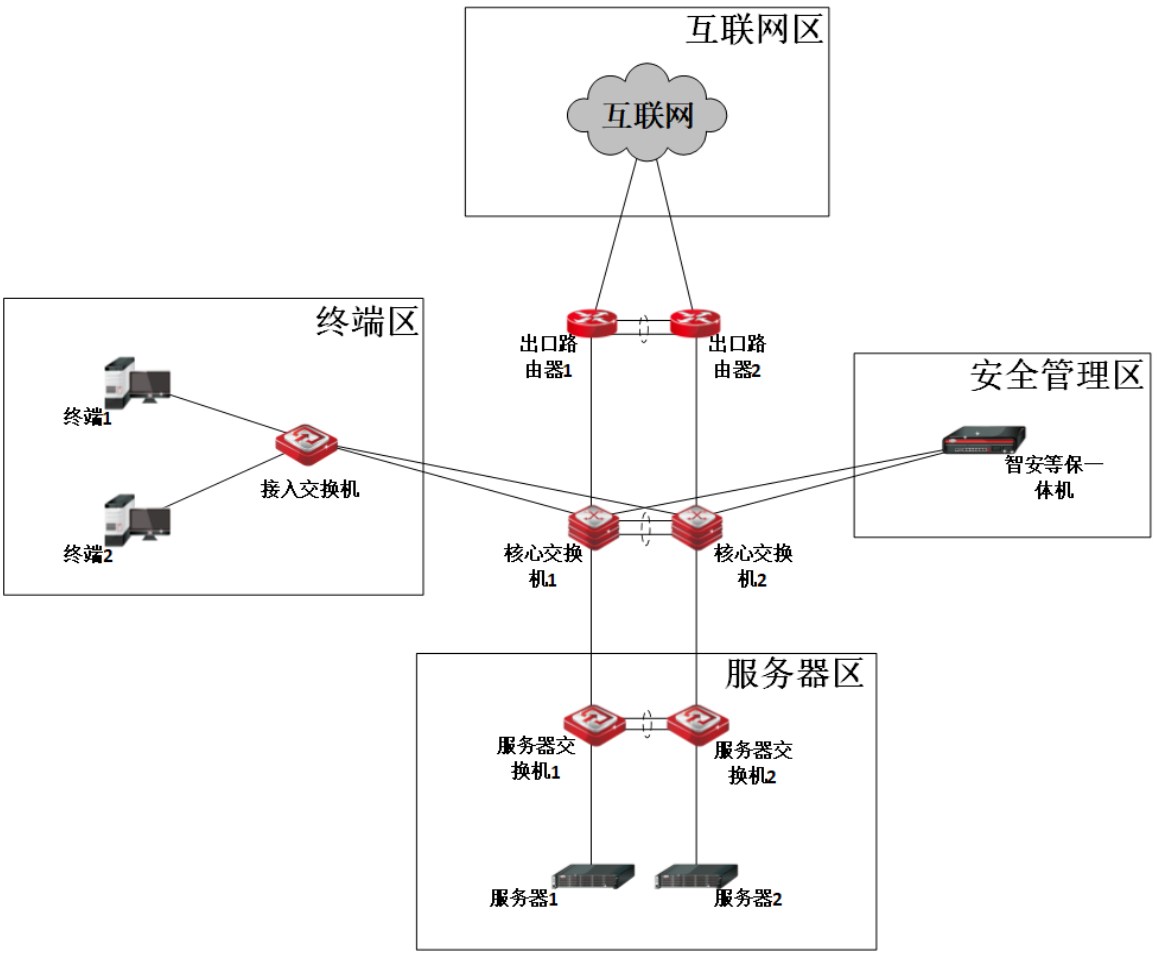
安全组件	等保二级	等保三级
DDoS 防火墙		√
云防火墙	√	√
WEB 应用防火墙	√	√
堡垒机		√
安全审计	√	√
主机安全	√	√
数据备份		√
漏洞扫描		√
管理中心	√	√

4.2 智安等保一体机（硬件一体机方案）

4.2.1【方案描述】

智安等保一体机是一款融合了智安自主研发的云综合防御平台的软硬一体机产品，适用于物理环境和虚拟化环境，为二、三级等保系统提供一站式等保合规整体解决方案。

智安等保一体机能够帮助用户顺利通过等级保护测评，从物理安全、网络安全、主机安全、应用安全、数据安全等多个层面进行体系化等保建设，提高安全运维效率。实现全网动态监测、精确感知、主动防护。



4.2.2【适用场景】

适用于有自建机房、对数据私密有要求的企业客户。只需将一体机旁挂到核心交换机上，并做相应的网络初始化配置。即可完成等保一体机接入。完成一体机接入后，在安全管理平台中配置测评系统相关信息，即可满足等保测评要求。

4.2.3【方案优势】

- **数据私密安全：**数据私有化隔离；容灾备份机制；算法、密钥双重保险，数据安全可靠；独享云资源，速度更快，性能更优。
- **企业自主掌控：**客户完全自主掌控，轻松实现成员管理、认证配置、身份源管理；用户信息和密钥信息本地存储。

4.2.4【产品配置】

产品名称	产品说明
硬件服务器	标准版（ZA-Scloud-A-100）： 配置：CPU：10 核 20 线程，内存：64GB，硬盘： 4T 规格：最大支持 20 台服务器 增强版（ZA-Scloud-A-200）： 配置：CPU：20 核 40 线程，内存：96GB，硬盘： 16T 规格：最大支持 80 台服务器
安全管理平台	统一提供底层基础硬件平台、安全虚拟化平台、安全资源池管理平台、安全模块。安全虚拟化平台实现计算资源、存储资源、网络资源、网络功能资源、安全功能等 IT 基础资源的虚拟化。集中管理安全功能
云防火墙	提供统一的互联网边界、内网 VPC 边界、主机边界流量管控防护，包括结合情报的实时入侵防护、全流量分析可见、智能化访问控制、日志溯源分析等能力。 通过简单易用的方式交付，全面防护各类威胁，并具备多重智能模型和智能联动手段，可持续对抗不断出现的各类新风险。支持实时入侵防护（IPS）、访问控制（ACL）、高级威胁持续监测（APT）、上网行为管理、SSL VPN 等功能
WEB 应用防火墙	提供网站入侵防护、业务访问风险、网址传播护航等安全服务
安全审计	提供数据库审计、主机审计、中间件审计、设备审计等合规审计服务
主机防护	提供资产管理、安全事件、病毒木马、合规基线、文件监控等安全服务
堡垒机	实现对服务器的操作运维审计等安全能力，可管理资产（服务器、网络设备），支持会话连接、会话监控、会话审计等安全服务；

4.2.5【接入流程】

客户需进行网络配置将流量引导到一体机

4.2.6【计费方式】

硬件质保 3 年+系统授权服务时间 1 年+第二年开始按 10%的费用收取作为维保费用

4.3 私有化部署方案

4.3.1【方案描述】

由客户出硬件资源和网络资源，由智安提供软件部署及运维服务。满足客户本地私有化、定制化需求。

4.3.2【适用场景】

1）客户业务系统在云上 VPC 等专有网络中，互联网无法直接访问的场景。

2）客户业务系统体量较大，一体机配置无法满足其需求的场景。

4.3.3【方案优势】

1）**数据私密安全：**数据私有化隔离；容灾备份机制；算法、密钥双重保险，数据安全可靠；独享云资源，速度更快，性能更优。

2）**企业自主掌控：**客户完全自主掌控，轻松实现成员管理、认证配置、身份源管理；用户信息和密钥信息本地存储。

3）**资源可扩展：** 随着后期业务的增长或变化，可动态调整资源配置。

4.3.4【计费方式】

私有化部署费+等保服务费+OEM 订制费（可选）。

5. 客户案例

5.1 河北省某地级市政府

项目背景：客户是河北省下辖的一个地级市，位于河北省东南部，客户需要对市人民政府、市司法局、市教育局等 37 个市级门户网站进行等保测评。

整改方案：客户通过购买我司【智云保（等保云）产品】，将需要测评的域名和源站 IP 配置到我司等保平台中，通过修改域名 DNS 解析后即可完成业务系统的流量接入，从而使用 DDoS 防护、云防火墙、WEB 应用防火墙等安全服务。

针对主机安全、日志审计和数据库审计等安全服务，则需客户在需要测评的服务器上安装我司提供的 agent，从而完成日志采集和安全防护。针对堡垒机和漏洞扫描等安全服务，客户只需在等保云平台上进行主机或 WEB 信息配置，即可完成资产的统一管理。

在我们安全专家的全程指导下，客户通过不到半天的时间，就完成了所有信息的配置和接入。最终通过等保三级测评，获得等级保护备案证明于等级保护测评报告。

客户价值：客户通过智安的一站式等保服务，省心省力的完成了所有的业务系统整改，满足了等级保护安全建设标准，同时也提升了客户各政务网站的安全防护能力，有效抵御各类网络攻击。

5.2 四川省某投资集团

项目背景：客户是四川省委省政府批准组建的大型旗舰型企业集团。该集团拥有 200 多家子公司，分子公司业务系统众多。集团自身的信息等保定级为三级，下属二级单位的部分业务系统，例如账单管理系统的等保定级为二级。总公司和每个子公司均有自己的机房，业务系统独立，信息化建设也各自进行。集团的信息中心负责集团的信息化建设，没有额外的安全团队进行进一步的信息安全专门管理工作。因此如何基于一套安全标准准则进行管理成为当前企业的需求。

解决方案：由于客户是自建机房，并且对数据私密性有一定要求，因此，通过采购我司【智安等保一体机】产品，并将等保一体机旁挂到客户的核心交换机上，从而完成设备的接入。客户只需将待测评系统信息配置到一体机的安全管理平台中，即可完成业务系统的整改接入，从而达到等保合规要求。在对客户业务系统的整改同时，我们的安全专家也对客户机房环境的等保整改输出了详细的方案，确保客户的安全物理环境也满足等保合规要求。

客户价值：客户的信息部门认为，通过独立信息安全设备【智安等保一体机】的综合部署，能够快速满足等保的需求， 并且不影响到已有设备的使用。同时，一体机的部分功能能够切实应用到日常信息安全工作中，例如日志审计模块，是进行系统审计的必备功能，这让一体机成为了非常高性价比的信息安全投入。

5.3 北京市某网络科技公司

项目背景：客户是北京一家网络科技有限公司，其业务系统是一款智能教学运营管理平台。旗下拥有业务系统多个均为线上直播形式，其核心信息系统部署于阿里云 VPC 网络中上。为保障业务系统全国稳定运行，还部署了若干应用服务。该企业要求通信网络不掉线，延迟不能高，并且基于云上合规安全，需要严格的防御措施，要防止非法用户进入网络,减少网络的安全风险。

解决方案：客户在其 VPC 网络提供资源，智安网络为客户私有化近源部署等保云平台，保障其业务安全性，满足等保合规要求。近源私有化部署满足客户网络不掉线、延迟低等需求。同时也满足数据加密存储，独享资源，更安全稳定，满足国家合规相关政策。

客户价值：数据私有化隔离，更安全可靠；独享云资源，速度更快，性能更优；企业可完全自主掌控，轻松实现成员管理、认证配置、身份源管理；支持高可用架构，支持横向扩容，可以基于客户的业务场景自主伸缩容量。

6. 关于我们

深圳市智安网络有限公司（简称：智安网络）是深圳市高新技术企业，下设成都智安云御网络有限公司（安全运营中心）和深圳市智安网络有限公司南京分公司（研发中心）两个子公司，成立于 2017 年 12 月 27 日，注册资本 2,000 万(元)。

作为安全运营中心，成都智安云御网络有限公司（简称：智安云御）成立于 2021 年 3 月，智安云御立足四川，放眼全球，坚持用户需求为导向，安全合规为目标，自主研发为宗旨，力争成为云安全领域领先者，在数字时代为用户的云安全及数据安全保驾护航。

智安云御基于企业安全能力模型 IPDRC（风险识别、安全防御、安全检测与响应、安全管控）构建安全 API 即服务的能力，搭建了智安安全中台。通过该中台，衍生了 6 条产品线路，形成“云 X 系列”的产品服务体系。

智安云御产品体系有：**云检**（流量检测--基于 snmp 与 flow 流量分析协议实现流量的采集、归类、威胁识别与告警）、**云测**（安全测试--提供可用性、漏洞、基线、权限、内容方面的风险测试和体检报告）、**云防**（攻击防御--提供主机/容器安全防护 cwpp 和网站/APP 安全防护 waap 能力）、**云控**（访问控制--基于零信任 SDP 与 IAM 理念实现下一代 VPN 技术）、**云保**（等保整改---一站式等保 2.0 建设服务平台）、**云密**（密码整改---一站式商用密码建设服务平台）