奇安信
新一代网络安全领军者

奇安信上网行为管理系统

上网行为管理系统是一款面向政企客户的软硬件一体化控制管理网关，可对企业内部员工的上网行为进行全方位有效管理，保护Web访问安全，降低企业互联网使用风险，避免企业机密信息泄露，提升员工工作效率，阻止、限制P2P等严重消耗带宽的应用，保障企业核心业务带宽。

核心功能特性 CORE FUNCTION

上网安全

借助奇安信云端大数据能力，对用户网络访问行为进行实时病毒云查杀、恶意URL云查，保障上网安全。通过威胁情报、应用行为特征等多种维度，有效发现内网失陷主机，保护上网安全。

网页过滤

通过网址预分类技术、标题关键字、URL关键字、网页正文关键字、搜索关键字过滤等方式管控网络访问行为，避免用户访问离风险、违法内容。

应用管控

利用应用识别技术和管控策略对各类应用进行封堵、时长限额、流量限额，实现对网络应用的人性化的管控，提高工作效率。

数据防泄漏

对外发途径（应用）、文件类型、大小、内容等进行管控，防止机密信息外泄。

业务防护

为业务系统提供入侵防护、病毒防护和沙箱检测。对业务系统访问进行双向扫描、识别并标识敏感信息、安全规则、行为接口、自定义接口等，对业务访问内容详情记录。

内容审计

对论坛、微博、邮件、IM等外发信息进行内容及审计及过滤，避免非法言论传播，审计留存用户上网日志，满足国家网络安全法要求。

冗余电源

支持带宽100M、200M、300M、500M、800M以及1G以上设备冗余电源。

支持型号有NBM3240、NBM3245、NBM5310、NBM5350等

用户认证

支持通过IP/MAC、用户名标识上网人员身份；可利用PortaI、微信、短信、二维码等本地认证方式完成用户真实身份的关联，同时支持与多种第三方系统联动以实现单点登录，为用户带来无感知的认证体

奇安信
新一代网络安全领军者

共享管控

基于应用层特征分析技术，秒级识别网络共享接入行为，快速定位私接网络用户，并对共享接入终端的数量进行控制，有效管理网络接入权限。

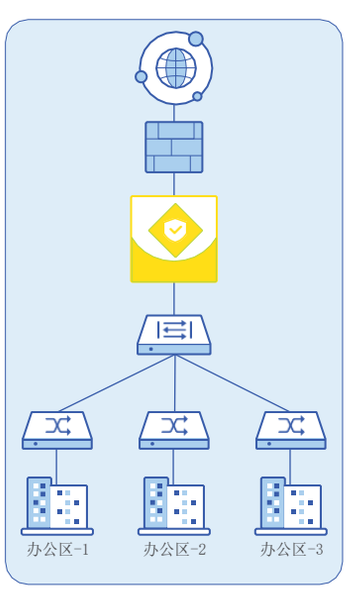
授权管理

支持5年特征库免费升级，支持本地和云杀毒服务、入侵检测服务、恶意URL云查服务。

产品特性 PRODUCT FEATURE

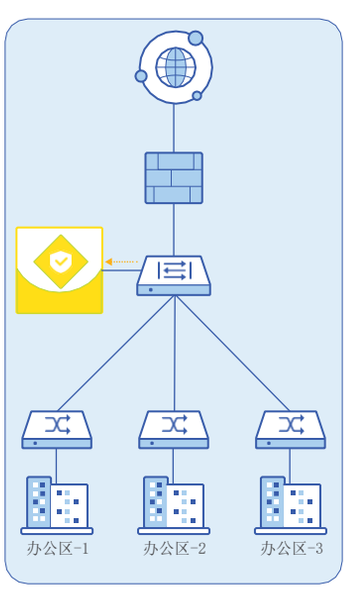
1 高效的的内容处理架构	高效的一体化内容处理架构，一次性解析协议和内容，一次性全功能匹配，从架构层面解决了由于产品功能增加造成的性能衰减问题
2 灵活的用户识别能力	具备30余种认证和识别方式，能够实现对用户身份的精准识别和验证 具备单机最高20万用户并发量的处理能力
3 全面的SSL解密能力	支持HTTPS/SMTPS/POP3S/IMAPS等主流应用解密 完善的解密协议算法适配，覆盖主流的所有协议和算法(包括tls1.3等) 支持加密网址分类库，应对海量加密网址管理
4 丰富的安全检测能力	集成了奇安信的威胁情报检测能力、云端病毒库和恶意URL库，具备多重丰富的安全检测能力 基于威胁情报和大数据能力构建了完整的三层安全防护体系
5 领先的网址分类库	领先的URL分类数据库，总规模超过2.8亿条 21个URL大类，134个小类，完整覆盖各种场景使用 自动化分类与人工审查结合，保证URL分类的分类率和有效性
6 精细全面的应用协议库	应用协议数据库包含12,000+种网络应用及其子应用 移动应用5000+，可有效满足移动互联网时代的管控要求 三级子应用分类，轻松实现细粒度的精细化管控（如允许QQ聊天与游戏，但禁止QQ文件传输）
7 完善的审计能力	覆盖主流webmail、论坛、搜索、网盘、文件服务器、IM等数千种应用 包含3000+论坛特征，3000+搜索特征，3000+虚拟身份等审计特征

典型应用 CLASSICAL PRACTICE



企业互联网出口管控

- 上网行为管理串行部署于互联网出口，所有流量通过上网行为管理转发；
- 根据规则对互联网访问进行管控，保护Web访问安全，避免企业机密信息泄露，提升员工工作效率。



企业互联网出口审计

- 上网行为管理旁路部署于互联网出口，所有流量镜像发送给上网行为管理；
- 根据规则对流量进行检测并记录日志，为管理提供依据。