奇安信
新一代网络安全领军者

奇安信Web安全网关

Web安全网关（SWG，Secure Web Gateway），是奇安信集团为满足企业用户针对互联网边界安全管控需求研发的一款专业Web访问代理产品。SWG提供了URL过滤，恶意代码检测和过滤，应用控制，数据泄漏等防护能力。可从用户发起的Web流量中过滤掉存在风险的流量和恶意软件，并强制执行公司相关策略。有效帮助用户免受基于Web的威胁。

核心功能 CORE FUNCTION

代理上网
- 支持HTTP、HTTPS、DNS、FTP、Socks代理
- 正向、反向、多级代理

安全检测
- 本地病毒扫描、恶意URL检测
- 第三方安全设备联动

代理认证
- 基于BASIC协议的AD认证
- NTLM集成域认证等

SSL解密
- 针对指定分类、未分类的HTTPS站点进行解密扫描；对无法解密扫描的HTTPS访问进行控制及日志记录

代理控制
- 针对HTTP、HTTPS协议进行方法控制及过滤HTTP Header内容修改
- 针对不同用户/组、源IP、目的IP/域名/URL分类/端口策略使用不同的访问控制

高可用性
- 自主集群方案。在不依赖第三方负载均衡设备的情况下，通过部署两个以上的设备，实现设备冗余和负载均衡

产品特性 PRODUCT FEATURE

基于全代理架构的安全检测及控制	采用全代理工作方式，可实现用户内外网的完全隔离 完全终结用户的互联网请求后，执行100%全流量安全检查和控制
主流协议代理	支持针对HTTP、HTTPS、Socks等主流应用的代理 支持灵活的端口配置和基于源/目的地址的代理策略配置 支持多级代理和反向代理，满足不同业务场景的需要
安全可靠的代理认证能力	支持基于源IP的用户身份认证 支持基于Session的代理认证，提供更高安全性的互联网访问控制能力

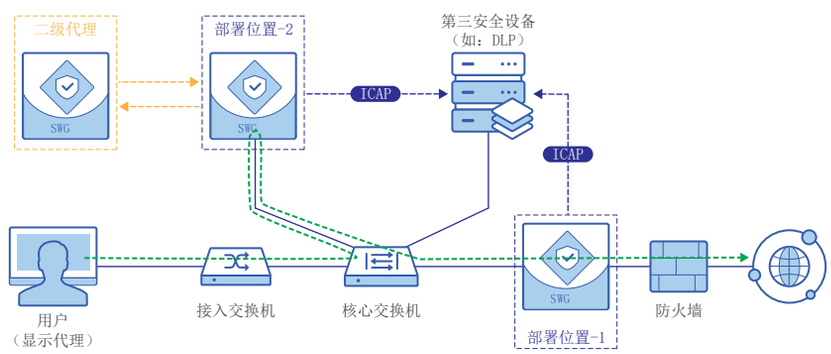
奇安信
新 一 代 网 络 安 全 领 军 者

高效的安全检测引擎	自主研发高效安全引擎，可对用户Web流量进行全方位的安全检测，如病毒扫描、URL过滤、威胁检测等 兼顾检测能力与检测速度，不引入额外时延，不降低用户体验
多层次的访问控制能力	支持基于传统五元组（源目的IP、源目的端口及协议）的协议层访问控制 支持基于应用及其细分功能（子应用）的访问控制 支持基于Web页面内容、上传下载内容的检查及过滤
强大的URL过滤能力	具备99%以上的网址分类覆盖度
丰富的安全扩展支持	支持基于应用的原始流量镜像 支持解密后明文外发 支持通过ICAP协议与其他第三方安全设备联动
灵活的部署方式	提供多种硬件规格，且支持多种虚拟化平台

典型应用 CLASSICAL PRACTICE

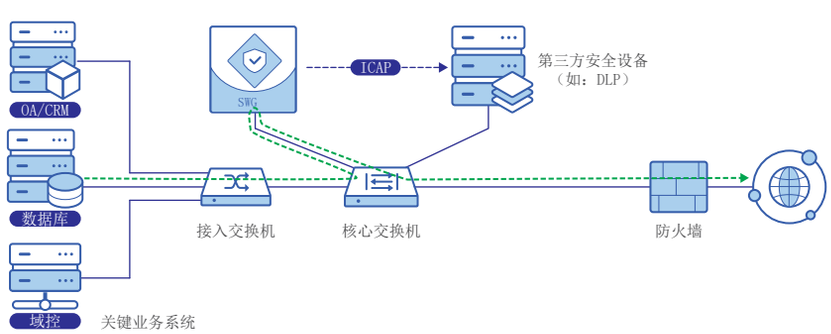
互联网出口管控

- SWG串行部署于互联网出口或旁路部署于内网；所有用户必须通过SWG代理上网
- 从用户发起的Web流量中过滤掉存在风险的流量和恶意软件；有效保护用户免受基于Web的威胁



关键业务系统代理访问互联网

- 关键业务系统配置显式代理，当其进行升级或特征更新时需通过代理访问互联网



内部业务系统安全访问

- SWG部署于内部业务系统前，内网用户通过“反向代理”访问业务系统
- 实现对业务系统真实信息的隐藏和保护，及对访问流量的全方位安全检测与控