绿盟业务安全网关

产品白皮书

【绿盟科技】

■ **文档编号**	NSF-TR-RPM-081	■ **密级**	完全公开
■ **版本编号**	V2.0	■ **日期**	2019 年 5 月 16 日
■ **撰 写 人**		■ **批准人**	

■ **版本变更记录**

时间	版本	说明	修改人
2019.5.13	V1.0	初始化、添加市场情况	揭淼
2019.5.15	V2.0	补充技术能力	刘书浩
2019.5.16		内容修订、总结	詹圣君

目录

一. 引言

1.1 市场趋势

在大力发展信息化战略、积极开展互联网+业务的背景下，各个企业机构的信息化系统和互联网系统快速增长，为用户提供更加灵活便捷的服务体验、更短的上市时间、更低的成本费用，以及出色的工作效率。

在信息化的过程中也催生了网络灰产的发展，据 Distil Networks 统计自动化攻击流量已占到全网流量的 42.4%，据南都大数据研究院等机构发布的《2018 网络黑灰产治理研究报告》估算，2017 年我国每年业务安全领域的直接经济损失已达近千亿元规模；全年因垃圾短信、诈骗信息、个人信息泄露等造成的经济损失估算达 915 亿元。自动化攻击近些年一直保持高增长的态势，给信息系统业务安全带来严峻挑战。

传统安全产品在自动化攻击手段面前已显无力。自动化攻击往往都是模拟的合规的操作请求，一般情况下这些网络请求在 URL、网络带宽、服务资源消耗、数据库读写上并无明显异常，只有通过访问用户的交互行为、设备特征、IP 信息、访问日志等数据来判断一个用户是否是机器发起的自动化请求，且网络攻击具有分散性、低频持续性攻击无明显攻击特征、随机性等特点。对于传统被动式的网络安全产品很难在数据有限的情况下被动应对，只能通过采集更多的客户端数据来对此进行应对。

1.2 客户痛点

面对自动化攻击请求，带来的危害也是方方面面的，其中主要包括：

- 爬虫攻击：通过内容爬虫肆意侵犯版权，窃取者获得极大利益的同时损害了自身利益。通过价格爬虫进行非法商业竞争，使用商业爬虫窃取竞争对手产品定价数据导致恶性价格竞争。
- 隐私泄露：通过爬虫等自动化工具暴力撞库、调用关键接口骚扰用户，暴力破解查询接口获取用户隐私信息等，损害公司和公户利益，影响公司形象，乃至危害社会公共安全。
- 网络层攻击：网络资产扫描获取可攻击接口，导致重要网络资产接口泄露，为攻击者下一步行动提供便利。

- 内容风险：通过篡改网站内容、批量式的机器发布政治敏感、垃圾内容，给企业带来巨大涉政风险，给国家和社会带来巨大不安定因素。
- 客户端数据篡改：用户通过随意修改客户端数据，非法请求网络资源，给网站带来巨大的经济损失和数据泄露风险。
- 黄牛：抢购特价商品、恶意抢拍等行为影响公司营销效果、严重妨碍平台公平性。
- 薅羊毛：通过机器批量注册、自动化领取优惠券，大批量低价购买平台商品和资源，导致企业承受巨大经济损失。

1.3 市场现状

在过去，防御自动化攻击的手段主要使用图片验证码，但图片验证码已经不再安全，随着图像识别技术发展验证码的识别准确率已经接近 100%，且传统验证码不能有效感知攻击存在，无法主动进行全网防御 。

二. 绿盟科技业务安全网关产品

2.1 产品概述

绿盟业务安全网关设备聚焦于业务安全市场，主要来弥补传统 WAF 设备无法解决的业务安全防护能力。目前常见的业务安全漏洞主要由自动化工具发起，请求流量不携带攻击特征，这使得传统基于流量特征进行检测的 WAF 无法进行有效检测。同时权威认证机构 Gartner 在进行产品能力划分时，将自动化工具识别单独划分一个产品，部署在 WAF 前面，将自动化工具流量进行过滤，让 WAF 进行有效的特征匹配。同时随着网络安全攻击行为逐渐向业务安全发生转换，也极大的推动了绿盟业务安全网关设备的诞生，绿盟业务安全网关设备在自动化工具识别能力上进行了创新，同时实行了主动防御模式，提升攻击者的攻击难度，致力于业务安全的精准防护。

绿盟业务安全网关设备主要包含以下功能：

1、识别爬虫等自动化工具及机器流量缓解

2、主动出击对网页代码进行混淆的混沌防御

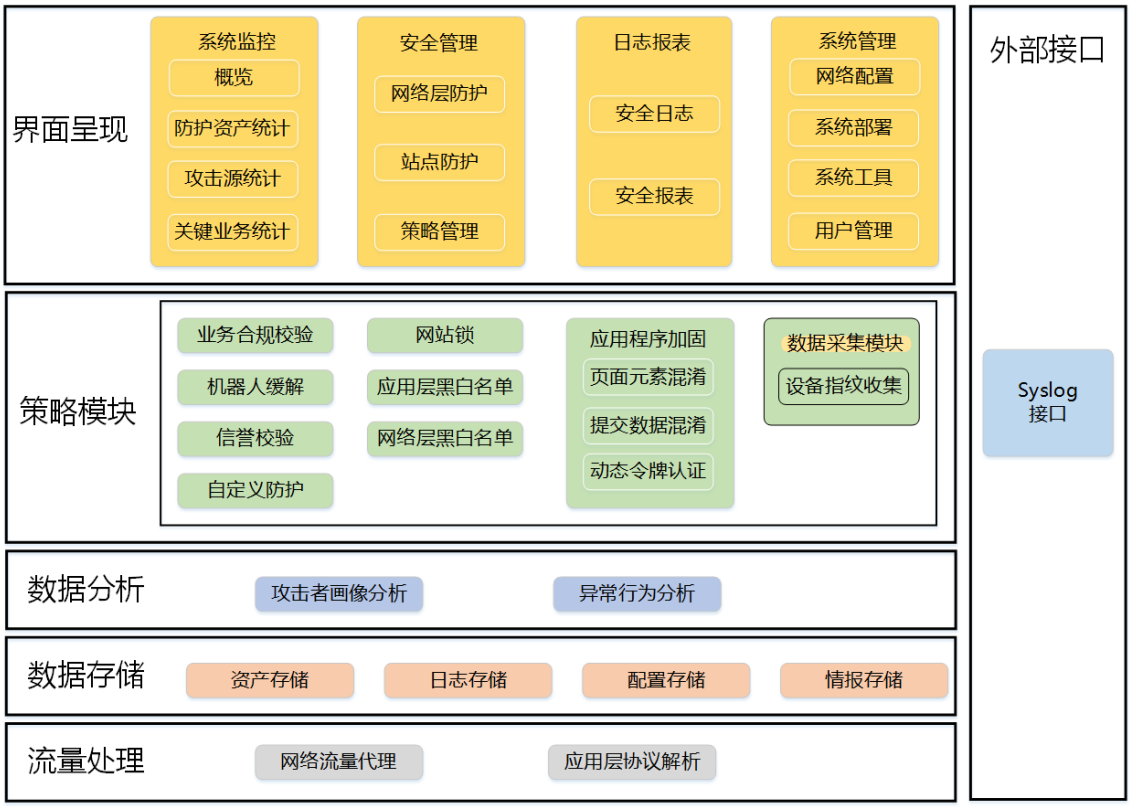
3、精准客户端识别的设备指纹提取

4、特殊时间段锁定网站的网站锁

5、防护能力补充的自定义防护

2.2 产品架构

整体架构分为五层，分别为流量处理层、数据处理层、安全策略层、关联分析层以及界面呈现层，系统配置和站点配置属于界面呈现层子模块，同时提供外部接口能力。架构图如下：



各层主要功能说明如下：

1) 流量处理层：主要功能包括网络流量代理以及应用层协议解析。网络流量代理功能通过相关网络配置实现网络流量牵引，识别防护流量将非防护流量直接进行转发，并将防护流量转发至设备引擎；应用层协议解析功能主要将识别到的防护流量进行 HTTP 以及 HTTPS 应用层协议解析，并将解析出来的数据（包括请求头部信息，请求参数信息，请求路径信息等）进行存储，供后续模块使用；

2) 数据处理层：请求流量经过系统产生的相关日志及网络、系统等配置数据进行分类存储，并支持导入外部威胁情报数据，包括端口与服务、反查域名、自治域信息、Whois 信息以及威胁历史等；

3) 安全策略层：可以通过数据采集模块进行设备指纹以及用户会话信息收集，精准定位客户端设备以及识别请求中的客户身份，为后续的关联分析提供基础数据；同时结合业务合规校验、网络层黑白名单、应用层黑白名单、网站锁、API 防护、机器人缓解、信誉检验、应用程序加固等功能进行主动防御，实现对网站攻击入口的隐藏以及提供业务安全防护能力，达到过滤自动化工具流量以及阻断相关业务安全攻击事件，同时提供自定义防护功能，能够及时补充现有防护能力；

4) 关联分析层：将相关日志结合设备指纹、用户会话等信息通过威胁关联模型进行深度关联，实现攻击行为关联分析，输出攻击者画像、异常行为分析等报表；

5) 界面呈现层：提供用户可视化界面，实现系统监控、安全管理、日志报表、系统管理四大功能。其中系统监控将各类威胁事件结合防护资产进行统计分析，并实现可视化呈现，方便用户了解网站运行状态；安全管理提供站点配置、策略管理等功能，通过界面进行策略调整以及动态修改防护站点相关配置；日志报表提供查询告警日志以及访问日志和各类报表的查询；系统管理主要包括设备基础配置、网络配置、用户管理等功能，并提供可视化界面对其进行配置；

6) 外部接口：设备提供 Syslog 日志外发接口。

2.3 产品优势（技术优势&特色）

创新的机器人识别技术

绿盟业务安全网关聚焦于目前常见的自动化工具识别技术，提出了创新的机器人检测技术，并基于此技术推出了层次递进校验的策略，根据脚本执行环境检测、客户端浏览器环境检测、客户操作特征检测以及机器学习建模分析来进行机器人检测，能有效的防护基于自动化工具发起的攻击行为，保障客户业务的正常运行。

主动出击、漏洞隐藏

传统的安全防护策略都是被动根据漏洞特征进行规则编写来进行防御的，此种方式不能防护未知漏洞，且规则维护成本较高，绿盟业务安全网关在防护策略上进行升级，提出了混沌防御的策略，混沌防御下设备会主动对网站代码进行混淆处理，让攻击者无法有效分析网站漏洞，提升攻击者攻击的门槛。

客户端精准识别

在网络发展迅速的信息化时代，攻击者也在不断提升自己的攻击能力。随着越来越多的代理 IP 工具的出现，导致代理 IP 获取的成本日益降低，攻击者也开始大量使用代理 IP 进行攻击。同时随着企业的需求，越来越多的采用 CDN，NAT 等技术，导致客户端 IP 的标识能力越来越低，仅仅通过 IP 无法追踪到真实的客户端。绿盟业务安全网关基于客户端浏览器信

息、客户端操作系统信息的收集，使用设备指纹技术来进行客户端识别，通过设备指纹技术将使用代理 IP 的相同客户端联系起来，实现客户端精准识别。

特殊时段网站锁定

绿盟业务安全网关为了应对目前重保期间，保障网站不被篡改的需求，推出了网站锁功能。支持在特殊时间段一键锁定网站，保障网站不被篡改，同时支持基于用户名和设备指纹的锁定，从不同的角度来防止恶意用户在特殊时间段对网站进行攻击，保障网站的安全稳定运行。

机器学习智能检测

绿盟业务安全网关加入了机器学习能力，让设备更加智能化，能够自动学习请求流量建立网站基线，形成白名单特征，防止恶意用户的访问。同时，还能基于机器学习能力对日志进行分析处理，寻找到攻击者的关联以及特征应用到策略中， 达到智能检测的效果。

2.4 主要功能

业务合规校验

绿盟业务安全网关设备支持基础业务安全校验功能，包含：协议合规、请求合规、文件合规等功能，来对业务系统进行防护。

1、协议合规：依据 RFC 协议规范来对请求流量进行规范校验，支持：HTTP 协议版本、HTTP 头部字段、是否允许特殊字符等配置。

2、请求合规：定义站点的请求是否满足合规性要求，包括：HTTP 请求方法、HTTP 请求长度、URL 关键字和 URL 后缀名。

3、文件合规：定义站点文件上传下载是否满足合规性要求，包括：文件后缀名校验、文件大小校验、文件 MIME 头部校验等。

机器人缓解

绿盟业务安全网关设备能对访问应用系统的客户端行为进行甄别，鉴别客户端的访问行为是否来自一个真实的人类，是否通过业务系统合法的访问路径与流程进行的访问，是否具有人工访问的正常轨迹。能从以下几个方面进行识别：脚本运行环境检测、浏览器环境检测、生物特征识别等。

1、脚本运行环境检测：能判断客户端是否有执行脚本的能力，并每次判断时随机选取判断标准，防止客户端进行绕过；

2、浏览器环境检测：能判断客户端是否具有浏览器的特征，并每次判断随机选取判断标准，防止客户端进行伪装；

3、生物特征识别：能针对用户的操作行为进行检测和分析，包括检测鼠标的点击、鼠标的移动、触摸屏点击、按键行为等特征。

4、能识别 PhantomJS 和 Webdriver 在内的所有流行自动化工具。并能支持防护撞库、暴力破解、应用 Dos、业务欺诈等通过自动化工具发起的攻击。

自定义防护

1.支持细粒度防护，能对整个站点、部分页面以及单个 url 路径进行防护。

2.支持基于客户端特征与攻击行为的拦截，支持多源低频和单源多频攻击的拦截。

3.支持添加新的策略规则防护，拦截规则策略要能针对用户特征的拦截和攻击行为的拦截。

混沌防御

支持对响应的页面内容中关键信息进行混淆，客户端提交的敏感数据进行加密以及通过生成动态的令牌来进行验证请求是否合法等功能来进行主动防御。

1、页面元素混淆：支持对响应页面中的 Form 表单、URL 链接等关键信息的混淆，并保证不干扰正常业务的运行以及不能影响页面的正常呈现效果。策略配置提供配置混淆的元素，支持多选；支持配置例外 URL，不对其进行混淆操作。并能够防止恶意扫描工具扫描出被防护站点的各类漏洞，对应用目录结构进行有效防护；能够防止攻击者通过爬虫工具，爬取网站的信息。

2、提交数据混淆：支持设置数据的提交方式、防护的 URL 路径和请求的来源 URL，支持 GET 和 POST 两种请求方式；自动识别数据提交动作，并针对提交的数据使用加密算法进行加密处理，同时保证加密算法不唯一，防止攻击者逆向分析。支持防护中间人攻击。

3、动态令牌认证策略：针对响应页面中的 URL，为其生成一个唯一短期有效的令牌，同时支持配置 URL 白名单用来取消令牌认证功能，支持配置校验 URL（默认为自动识别）、令牌过期时间等参数，进行更加细化的防护。能支持防护重放攻击。

攻击者画像

绿盟业务安全网关支持攻击者信息关联。根据请求流量、告警日志、设备指纹、用户会话信息分析特定攻击者使用过的代理 IP、网站用户以及所有的事件活动，检测分析近期攻击过程及受影响资产范围和数量。

攻击者定位：从告警日志结合设备指纹将多个 IP 的攻击事件关联分析得到攻击者。

攻击者信息补齐：补全攻击者的背景信息，如归属地、使用过的代理 IP、使用过的账户、使用过的攻击工具等等信息。

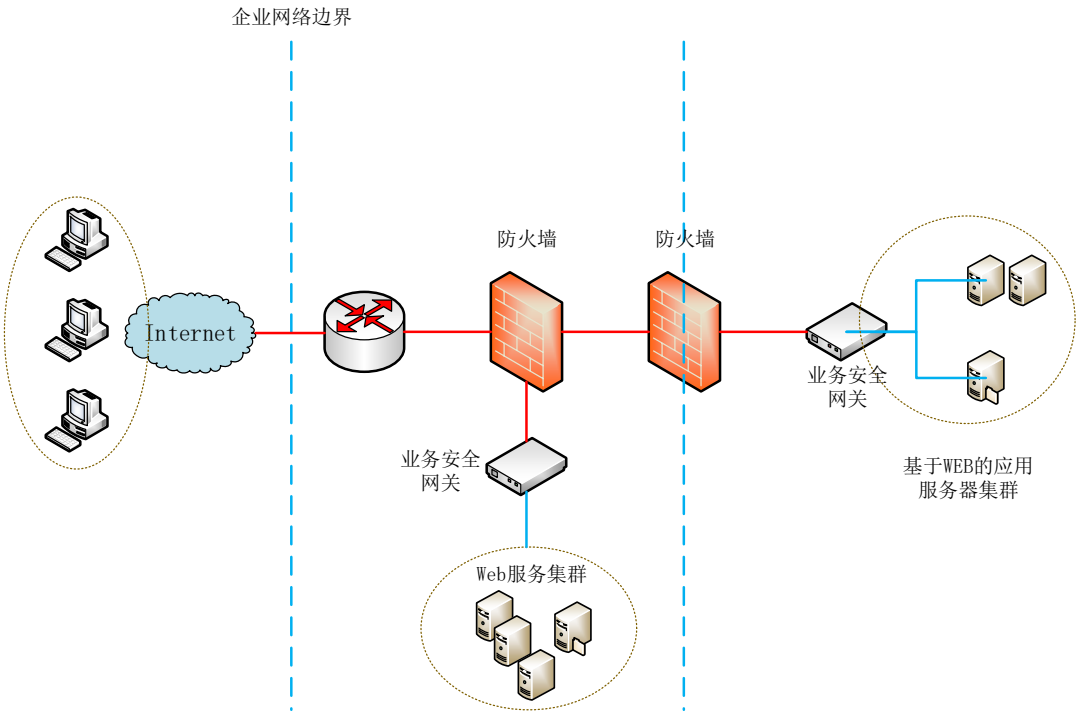
攻击者关联分析：支持将单台设备上的攻击者行为数据上报到云端，通过更多的攻击信息进行更加深入的分析攻击者的目标、意图、关联出攻击者的攻击路径图。

2.5 典型部署

绿盟业务安全网关提供多种灵活的部署方式，包括透明部署模式、反向代理模式和旁路模式。

串联部署模式下，绿盟业务安全网关在内核模块实现基于 TCP/IP 协议栈的透明代理，极大地提高网络适应能力、确保产品在网络中即插即用而无需修改网络及服务器配置，降低了部署、维护开销。而反向代理模式，需要改动服务器 IP 地址以及 DNS 解析。

在部署了多业务网段服务器的网络环境中，业务安全网关设备也可以采用旁路方式部署，提供一种逻辑在线防护能力。该种部署灵活性较好，可以实现业务分流，对核心系统影响较小。旁路方式部署的技术原理如下：



1. **流量牵引：**通过路由方式，将原来去往目标网站 IP 的流量牵引至业务安全网关设备。被牵引的流量为攻击流量与正常流量混杂的请求流量；
2. **流量检测和过滤：**业务安全网关设备通过多层的攻击流量识别与净化功能，将攻击流量从混合流量中过滤；
3. **流量分发：**业务安全网关设备过滤完攻击流量之后，根据建立好的站点映射表将不同的请求分发到指定的后端服务器中；
4. **流量注入：**经过业务安全网关分发之后的合法流量被重新注入回网络，最终到达目的网站。
5. **对返回流量检测：**网站响应的 HTTP 流量在返回给客户端之前，仍然需要流经业务安全网关设备，业务安全网关可提供安全检测，经业务安全网关检测后的流量最终返回给客户端。

三. 客户利益

◆ **防止爬虫爬取网站信息**

绿盟业务安全网关设备通过混沌防御对网页关键信息进行混淆，如：URL 链接、Form 表单等，让爬虫无法解析页面内容，无法从页面中提取到有效信息，从而导致爬虫无法爬取到网站的目录结构。在人机识别、动态令牌、扫描器请求识别的几大功能组合下能够有效防护资源类爬虫、商业爬虫、恶意爬虫、模拟器爬虫以及失控类爬虫，达到有效防护客户数据资产，保障客户数据安全的目的。

◆ **降低自动化工具窃取数据风险**

目前通过自动化工具及枚举类爬虫等进行隐私数据窃取的事件常有发生，绿盟业务安全网关设备通过机器人缓解、API 防护等功能，对请求流量进行识别，过滤出自动化工具的请求流量，同时针对关键 API 进行监控，防止其请求流量异常，来防止攻击者通过 API 资源滥用获取到隐私数据，保障网站的数据安全和完整性。

◆ **防止恶意漏洞扫描**

绿盟业务安全网关设备通过混沌防御、机器人缓解功能，来对网站可能出现的漏洞信息进行隐藏，加大漏洞挖掘难度，传统的扫描器无法通过扫描获取到漏洞信息；针对高级渗透

工具，通过机器人缓解的四层校验可以有效的分辨出来，从各个方位阻止了对网站进行漏洞扫描的攻击行为。

- **防黄牛、薅羊毛等**

绿盟业务安全网关设备通过机器人缓解、API 防护功能，能够有效甄别出通过自动化工具发起的黄牛党刷票以及针对活动期间的薅羊毛事件，通过四层递进校验结合机器学习建模分析，能够准确的区分攻击者和真实客户，保障客户不遭受经济损失。

- **分析攻击行为，降低运维成本**

绿盟业务安全网关设备通过机器学习建模，结合设备指纹、攻击日志、访问日志等信息，进行离线日志分析，通过关联算法和设备指纹信息能够有效的对攻击者的攻击行为进行分析，得出完整的攻击者行为画像，并进行可视化呈现，方便客户进行追踪溯源以及事后复盘，大大的降低了客户运维成本。

四. 总结

业务安全市场一直处于传统网络安全市场之外， 随着近几年技术发展，越来越多的调研机构、投资机构都在倾斜对业务的关注，同时利用传统安全漏洞发动攻击的难度不断提升，攻击者的重心开始从传统的系统与应用漏洞转向无明显攻击特征的业务安全攻击（如：撞库/拖库、账户盗用、刷单/薅羊毛、漏洞探测、0day 攻击等），攻击的方式也从单一人工的方式转向以工具为主辅助人工的形式。

绿盟业务安全网关产品结合了机器人缓解、业务基线、混沌防御等功能，对业务进行主动防御，有效识别和过滤自动化工具流量，使客户不再陷入薅羊毛、拖库、篡改、监管扫描等业务困境，全方位的保障客户网站的业务安全。