GOODWAF 功能说明

全面了解产品

1.网站安全痛点分析

1、风险敞口大

网站在公网上，攻击者通过域名即可获取到服务器的真实 ip 地址，随即可以对 ip 地址进行扫描、嗅探、爆破、流量攻击等，直接威胁网站安全。

2、应急资源不足

本地没有机房、没有云安全组件，多数用户只有一台服务器甚至是虚拟空间，安全服务人员严重不足，一旦碰到恶意攻击，不能及时应对。

3、合规改造需求

网络安全法对于信息系统安全要求更高，等保合规要求也逐步增加。政府、事业单位等要求系统 https、ipv6 等，传统改造花费较高，借助云安全平台能够实现一键改造。

4、配置操作复杂

传统硬件设备部署困难，设备调试难度也较大，对于运维人员要求较高。

5、数据分析困难

本地安全设备记录攻击日志复杂，多数都是内网 ip，不容易区分系统。同时无法用态势感知方式呈现攻击情况，影响结果分析。

2.云安全平台

云安全防护平台基于大数据安全分析技术，通过搜集来自多种数据源的信息安全数据，深入分析挖掘有价值的信息，主动获取威胁信息，实时动态联动升级安全规则库，对未知安全威胁做到提前响应，主动应对威胁。平台构建的是一套集威胁预警、攻击防护、黑客溯源于一体的“自动化安全运营闭环体系”既可检测风险威胁预警，又能用户提供安全防护，同时实现黑客攻击溯源，三位一体构成系统的安全防护矩阵。颠覆传统单点、被动、孤岛防护，降低风险，实现最佳的安全防护。

通过完善覆盖的网络架构，将原本孤立的威胁信息预警、网络安全防护、黑客攻击溯源串连起来，协同工作，分布式感知与控制管理网络流量,集中分析与处理安全事件，形成完善的网络安全事件管理与解决方案。

平台能够监测、防御如 SQL 注入、CC 入侵、暴力破解、网站篡改等网络攻击，且具有独特的多重身份认证方式、态势感知、情报威胁系统，构建了以安全产品为基础，覆盖安全方案、安全服务、安全运营的业务生态。

2.1 云端全面防护

一个管理中心： “云防护”平台采用 SAAS 服务模式，为网站实现全量 Web 化服务体验。用户仅需要登录 Web 操作界面即可享受云防护为您提供的八大优势服务。

八大优势服务：云 WAF 服务、CDN 加速服务、监测告警服务、技术支持服务、IPV6 升级改造服务、业务安全服务、态势感知服务、零部署服务。

云安全平台能够实时检测拦截多种攻击，并在 web 层面上实现 Web 攻击防护、异常过滤、协议漏洞威胁防护、扫描窥探威胁防护、传输层威胁防护、应用型威胁防护等多种威胁防护。

威胁防御类型	
Web 攻击防护	注入攻击、跨站脚本攻击（XSS）、防系统命令执行、防远程代码执行、防文件包含攻击
异常过滤	黑名单/基于 HTTP 协议字段的过滤/TCP/UDP/other 协议负载特征过滤
协议漏洞威胁防护	IP Spoofing；LAND 攻击；Fraggle 攻击；Smurf 攻击；Winnuke 攻击；Ping of Death 攻击；Tear Drop 攻击； IP Option 控制攻击；IP 分片控制报文攻击；TCP 标记合法性检查攻击；超大 ICMP 控制报文攻击；ICMP 重定向控制报文攻击； ICMP 不可达控制报 文攻击
扫描窥探威胁防护	端口扫描攻击； 地址扫描攻击； TRACERT 控制报文攻击； IP 源站选路选项攻击； IP 时间戳选项攻击； IP 路由记录选项攻击等
传输层威胁防护	SYN flood 攻击；ACK flood 攻击；SYN-ACK flood 攻击；FIN/RST flood 攻击；TCP fragment flood 攻击；UDP flood 攻击；UDP fragment flood 攻击； ICMP flood 等
应用型威胁防护	虚假源 DNS query flood 攻击；真实源 DNS query flood 攻击；DNS reply flood 攻击； DNS 缓存投毒攻击； DNS 协议漏洞攻击； HTTP get /post flood 攻击； HTTP slow header/post 攻击； HTTPS flood 攻击； TCP 连接耗尽攻击； Sockstress 攻击； TCP 重传攻击； TCP 空连接攻击； SIP flood 等

2.2 应用安全防护

云端对网站所有公网数据进行安全加固，打造成云端防护+本地安全形成"护城河"纵深体系。**强化合规建设手段**。

- 替换原始应用头部敏感信息，防止 WEB 应用程序类型、版本信息、网站源码泄露问题。
- 针对常见的建站程序可能出现的 ASP 木马、JSP 木马、PHP 木马、一句话木马等多种形式的 WEB Shell 后门木马漏洞攻击、木马文件上传防护。
- 防止系统命令注入、目录遍历、恶意扫描行为，避免被黑客进行系统命令执行，文件提权等操作
- 畸形报文过滤、HTTP 标准 RFC 检查，有效防止报文头缺失、请求方法限制、协议违规等访问行为导致的应用程序崩溃等问题。

2.3 业务安全防护

云防护不仅可以针对 web 应用程序自身的漏洞攻击进行防护，还对所有访问行为进行多维度分解。**确保网站程序安全性和最终用户权益不受侵害**。

- 防盗链避免网站被盗链导致的用户流量流失，机构权威信誉度下降。
- 识别和阻断 SQL 注入攻击、Cookie 注入攻击、命令注入、会话劫持、跨站脚本攻击、文件包含攻击、LDAP 注入、XPATH 注入、爬虫攻击、Struts2 命令执行攻击等常见的 WEB 攻击。
- 登录接口设置访问频次，减小、阻断密码爆破行为发生。
- 拦截恶意爬虫，防止数据泄露，减轻网站性能压力。

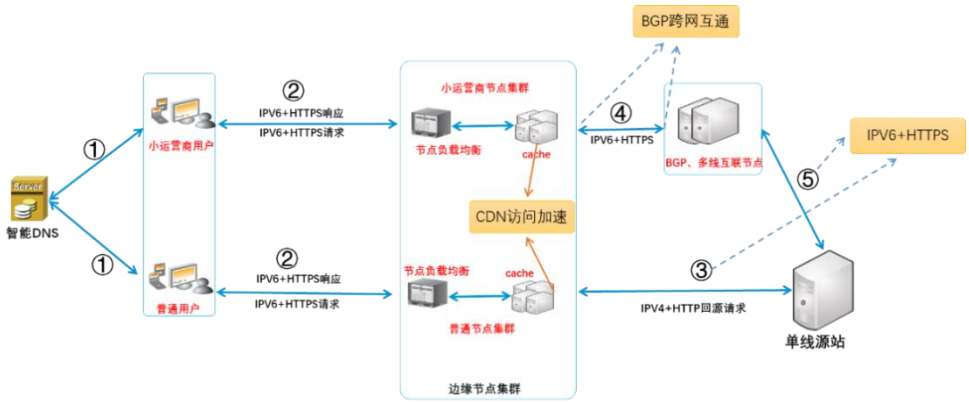
2.4 CDN 加速

智能 DNS 服务优化用户访问链路，加速网络传输，**提高用户访问体验，增强权威性**。

- 静态资源缓存到云节点，提高网站下发速度，减轻源站压力。
- 多线、BGP 节点，解决跨运营商、跨地区用户体验差现象。网站访问更

快、服务更稳定。

- TCP 协议优化、智能压缩技术，加速传输速度，提升网站访问速度。
- IPV4/IPV6 双协议栈、https 和 http 转换功能，满足网站合规建设需求。



2.5 联动防御

一体化管理中心，采集、分析六大防护体系数据，AI 攻防大脑针对威胁情报、态感预警进行智能分析处置，生成安全规则下发给云安全平台。**降低运维难度，减少本地运维工作量**。

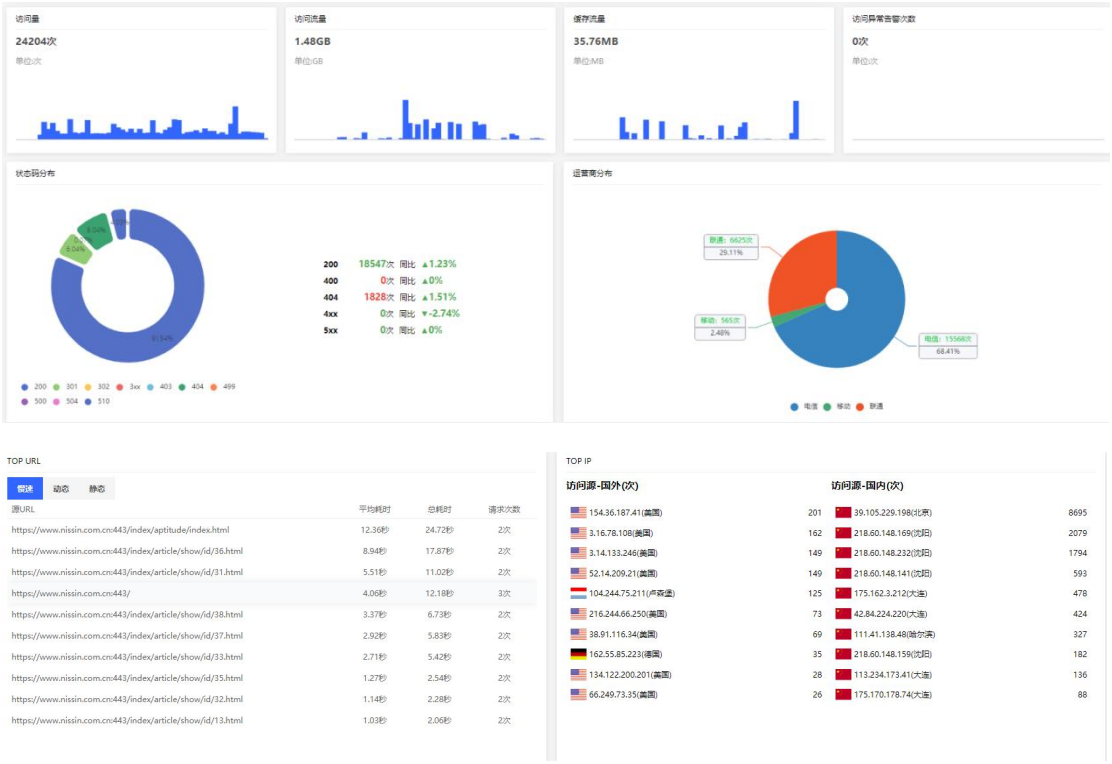
2.6 态势感知

可视化实时攻防态势图，发现网站威胁，进行邮箱、微信多维度告警推送。可用性、攻击次数统计分析告警推送，随时追踪网站攻击情况。**弥补本地设备无法有效进行溯源分析痛点**。

专业的周报、月报，提供运营分析数据、Web 攻击防护报表以及网站运行业务质量的监控。

2.7 完善的报表机制

针对平台系统网站防护情况，可以为客户提供分析访问量和攻击情况等日常运行情况。为用户提供 Web 攻击防护报表以及网站运行业务质量的监控，让用户全面了解网站运营情况。



3.产品优势

1、精准的网站防护功能

从基础资源到安全智能 DNS，到网站云服务，到网站监控，到大数据威胁分析，到专家服务再到黑客追溯。形成完整的防护闭环。层层防护，拒绝漏防。

2、实时的监控告警系统

云防护的云监控可以为用户轻松搞定网站注入攻击、恶意代码、敏感信息、宕机、漏洞、DNS 劫持、服务器宕机等等各种问题的监控需求。

3、攻击溯源分析

依托威胁情报中心的大数据处理能力以及专家团队人工分析，为攻击取证提供强力保障，让攻击者无处可藏。

4、防护接入零改造

接入云平台为 saas 化服务，按需定制、零部署、零维护，保障您的线上业务永续运行。无需安装任何软硬件，通过配置智能 DNS 实现云防护；为满足用户数据私有化的需求，可提供专用节点实现独立部署。接入系统平台后，用户只需要关注业务系统本身状态即可。

5、业务调整操作简单

客户可登录云防护服务系统进行查询和管理。登录系统后，可自助查看网站安全情况、访问以及监控情况。网站安全运维工作简单明了，前期完成一次性配置后，后期查看防护报表即可。

6、多年安全技术储备

云防护专门针对政企网站防护需求特点，量身定制的防护产品。数十位安全技术人员，整合旗下漏洞库、恶意代码库、社工库等等完美的防护资源倾情打造。

7、顶尖的运营团队

云防护拥有行业内最顶尖的产品设计团队，不断挖掘用户需求，始终致力于为用户提供更丰富、易用、高效的防护产品。同时 7x8 小时的运维服务团队，提供管家式的服务。技术人员均通过专业培训，由专业成熟的安全运营团队做支撑，有效保障了接入网站的安全运行状况。以及依赖多年来我司在网络安全上积累，直接将丰富的安全能力为接入网站保驾护航。产品和运维团队采用三层架构：

第一层，产品支持，问题发现与解决团队，为用户解决使用配置过程中的常见疑难问题。

第二层，技术支持团队，时刻为企业用户在使用过程中所遇到的问题进行相关的技术支持。

第三层，专家团队，为用户端做详细的分析，提供分析结果，进行专业安全加速评估，协助用户实施具体有效的解决方案。

4.应用场景

4.1 云 WAF 主要针对哪些用户？

云WAF致力于解决WEB应用安全问题，适用于“政府、企业、银行、金融、游戏、教育、互联网”等所有涉及WEB应用的各个行业。

4.2 WAF 支持域名形式的哪些网站协议

云WAF支持基于域名访问，并且是http和https的网站协议防护。（http(s)://aaa.bbb.com形式可申请防护，http(s)://1.2.3.4形式不能防护），具体要提供的内容参考《WAF接入申请表》。

备注：https需要提供https证书

4.3 WAF 支持域名和 IP 形式的网站吗？

由于WAF需要通过域名的cname进行引流，所以云WAF只支持以域名形式的网站防护，不支持IP形式的网站防护。示例：http(s)://1.1.1.1形式不支持，http(s)://www.abc.com/形式支持。

4.4 云 WAF 的（部署方式）是怎样的？

客户只需要提供互联网网站域名、IP地址、协议和对应端口，并通过CNAME引流方式将流量引入WAF防护系统，即可实现对客户网站的安全防护，无需对客户网站部署做任何调整。

4.5 接入云 WAF 的流程是怎样的？

首先，用户在goodwaf网站进行注册。

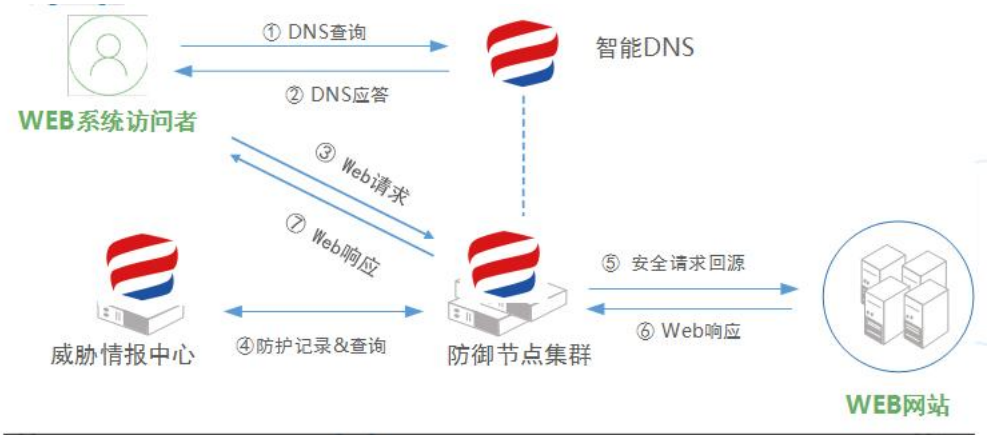
其次，添加域名、ip、端口等信息，等待审核。

最后，将域名的DNS记录修改为cname解析。

注意：请您严格按照流程执行相关步骤操作，如出现已经备案域名提示未备案，请联系客服添加机房白名单。。

5.交付方式

Web系统访问者发起的请求通过智能DNS解析后到达就近的云服务节点，该节点对流量进行安全检测，清洗异常流量、阻断网络攻击后，把正常请求流量回源，从源站返回的响应流量再经过防护节点后响应客户请求，以完成正常的访问过程。



5.1 网站迁移工作

用户变更DNS解析记录，修改CNAME记录：用户需要在域名服务商对应域名的CNAME记录进行修改，将待接入云安全防护防护平台的域名修改为平台指定的CNAME记录值，这样客户的域名就可以解析到平台响应防护节点上了。

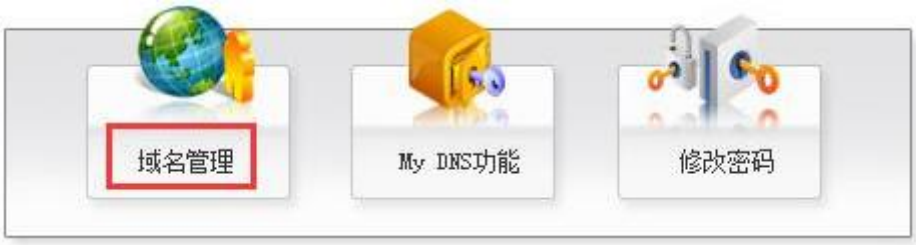
5.2 各主流平台DNS修改方式

（1）新网互联注册商域名修改DNS地址

- 登录http://www.xinnet.com 会员中心，点击页面上方的【进入我的账户】。
- 依次点击会员专区上侧导航栏中的【我的产品】。

• 在域名管理页面找到要修改DNS的域名，点击【管理】。

• 打开页面后，点击【域名管理】



• 进入修改 DNS 页面，域名服务器选择为【填写具体信息】，域名服务器名字1和域名服务器名字2分别修改为云安全防护防护系统提供的NS记录。

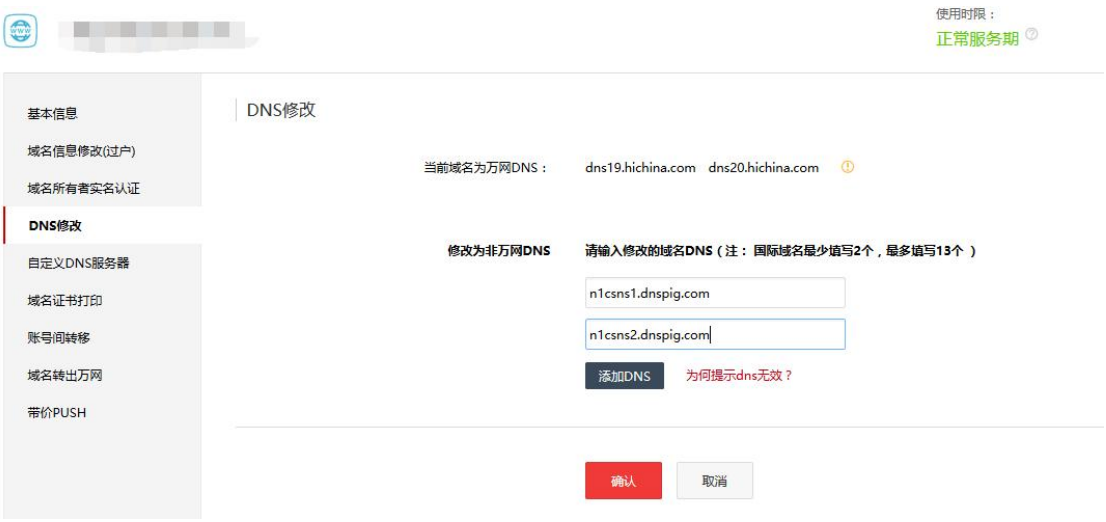
- 设置完成，请耐心等待 DNS 生效。

（2）万注册商域名修改DNS地址

- 使用万网域名管理账号登录，点击【域名】。

- 选择域名，点击【修改 DNS】 。

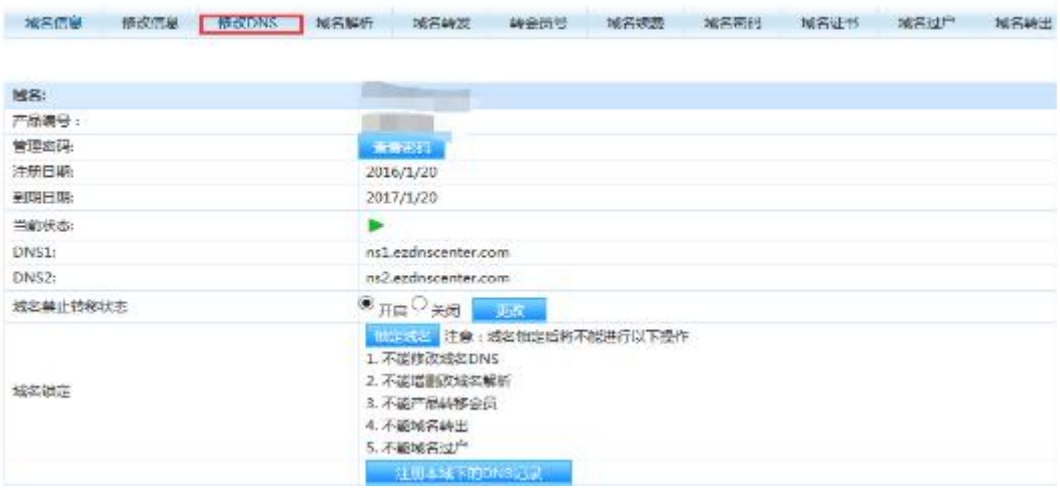
- 将 DNS 修改为云安全防护系统提供的 NS 记录。



（3）美橙互联注册商域名修改DNS地址

- 登陆域名管理账号，点击域名 。

• 点击修改 DNS。



• 把 DNS1 和 DNS2 修改成云安全防护系统提供的 NS 记录。

注意：因修改 dns 的 NS 记录刷新时间较长，建议晚间修改。因为部分域名注册商每天支持修改 dns 的次数有限，请尽量一次修改成功。

6.产品价值

云防护提供以 SaaS 方式的云清洗服务模式，用户按需动态购买、扩容安全服务能力，无需用户在本地投入物理资源进行建设和维护。

云防护聚焦用户安全防护能力的提升，提供威胁情报预警、防护能力升级和攻击实时分析、检测、阻断等能力，将云防护作为网站云防护系统平台支撑，其安全能力更贴近客户业务，更好的将安全能力输送到最前沿。

●防 OWASP 攻击：注入、SXX、篡改、拖库、挂马、黑链、漏洞、Webshell、恶意扫描等各种黑客攻击。

● CDN 加速：静态缓存减轻源站压力同时，加速用户访问速度；多线、BGP 节点提高跨网跨运营商访问质量。

●随时监控掌握网站情况，网站服务可用性、网站攻击次数统计分析以及告警推送。

●可视化的实时攻防态势图，可用随时追踪网站攻击情况。并且具有专业的周报、月报，以及专家级网站运营分析报告。