政企安全解决方案（GESS） 白皮书V2.0

网世界 心归宿

网宿科技 全球领先的互联网基础设施平台

关注公众号，及时了解网宿产品与服务动态

400-010-0617 | www.wangsu.com

Content 目录

网宿科技“政企安全解决方案（Government & Enterprise Security Solution，简称 GESS）”是隶属“网宿网盾”品牌旗下的一款专为政企行业打造的集安全防护和加速为一体的一站式安全解决方案。政府单位和企业单位可以一站式地享受 DDoS 攻击防御、WEB 应用攻击防御、防篡改、防盗链、加速等各项服务。

“网宿网盾”是网宿科技发布的云安全全新品牌，其业务全景主要覆盖网络安全、业务安全、内容安全、DNS 安全、源站可用性、传输安全、安全管理和安全评估等八大领域，“网宿网盾”依托高容量节点和自主研发的安全技术，构建出一套云端智能安全体系。

1. 行业现状和挑战

随着互联网、大数据和云计算时代的到来，政府部门以及金融、教育、商务等各行业的企事业单位将业务逐渐转移至线上，云计算、大数据等新兴技术在政企网站得到了落地和应用。在发展前景呈现一片欣欣向荣的同时，随之而来的安全问题也日益突出。在互联网时代，信息更容易被整合和采集，由此带来的安全问题更加需要重视，否则后果不堪设想。

政府部门、企事业单位在信息化进程中主要面临以下问题和挑战：

- **合规性要求**

政府部门的网站作为国家重要的信息发布系统，因此国家对政府网站的安全性非常重视。《关于进一步加强政府网站管理工作的通知》（国办函〔2011〕40 号）、《关于大力推进信息化发展和切实保障信息安全的若干意见》（国发〔2012〕23 号）均指出要切实严格检查和提高重要信息系统防攻击、防篡改、防病毒、防瘫痪、防窃密能力。同时，《中华人民共和国网络安全法》指出网络运营者应当采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施，保障网络免受干扰、破

坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改；网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。

- **网页被植入非法信息，损害政企形象**

2016 年 CNCERT 监测发现，2016 年我国境内 16758 个网站被篡改，其中被篡改政府网站有 467 个，在被篡改的政府网站中，超过 85%的网页被植入暗链（由于搜索引擎给政府类网站的 PR 值和网页级别都很高，因此博彩、私服、色情等非法行业，通过向政府网站植入暗链提高网络搜索排名），成为黑客地下产业链牟利方式之一。境内进 82072 万个网站被植入后门，其中政府网站有 2361 个，此类篡改行为既违反了国家禁止赌博等相关法律，又严重损害了被篡改网站的声誉和公信力，也影响了网站正常业务的运行。

- **网站被拖库，信息泄露事件频发，影响业务安全**

政企网站日趋向便民服务网点转型，随着越来越多的业务搬迁至网上，政府机构、互联网金融、电子商务等网络平台承载了大量有价值的数据信息（如身份证、社保信息、电话号码、住址、政府机构涉密文件、银行卡等），因此广泛被攻击者关注。在大数据时代，信息更容易被采集和整合，信息的泄露将会损害政府机构的声誉和公信力，影响人民财产安全，甚至危及到国家安全。

- **DDoS 攻击事件愈演愈烈，业务中断**

近年来，DDoS 攻击的方式和手段不断发生变化，增加了攻击防御和溯源的难度。而几乎不需要技术基础即可使用的 DDoS 攻击服务在互联网上公开明码标价叫卖，极大降低了 DDoS 攻击技术门槛，使攻击者可以轻易发起大流量攻击。根据 CNCERT《2016 年中国互联网网络安全报告》显示，2016 年 1Gbps 以上 DDoS 攻击事件日均 452 起，且大流量攻击事件数量全年持续增加，10Gbps 以上攻击事件数量第四季度日均攻全年日均达 133 次，占日均攻击事件的 29.4%。

- **网站访问响应慢，影响公众体验和办公效率**

政企网站包括大量的新闻信息，同时以文字、图片和视频等形式展现，同时随着越来越多政企将其业务迁移至线上，公众对政企网站的关注度大大提高，进而导致政府、企事业单位网站的访问并发越来越高，同时，跨运营商、跨区域访问频繁，容易出现网站响应速度慢等现象，影响公众的访问体验、网站应用服务开展的质量以及办公效率。

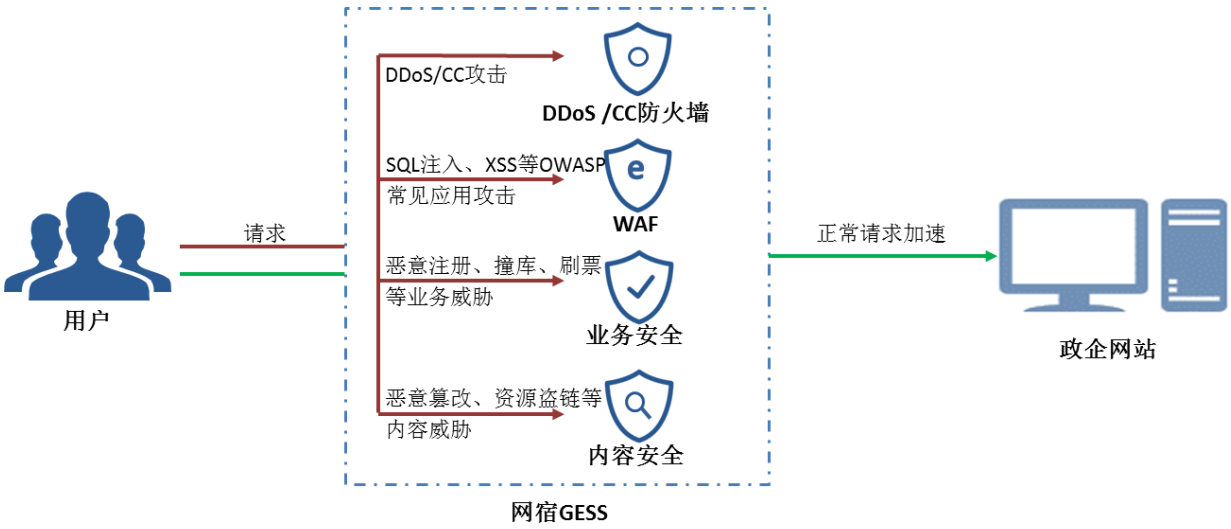
2. 解决方案介绍

2.1. 解决方案简介

网宿“政企安全解决方案”依托网宿 CDN 资源优势，结合大数据分析，自主研发防护算法，实时检测并过滤各种异常访问，为政企用户提供集安全和加速为一体的服务。GESS 可有效防御各类网络层和应用层攻击，防止网站被篡改、敏感信息泄露等，保障网站稳定安全运行，保障网站业务和内容安全，并提升网站服务质量。

2.2. 解决方案架构

网宿政企安全解决方案架构图如下：



2.3. 适用行业与场景

网宿 GESS 致力于为政企提供集安全防护与加速为一体的服务，保障政企业务安全的同时，提高网站可用性和访问速度。

GESS 的应用场景包括但不限于：

1. 门户网站

门户网站作为政府、企业和学校等机构提供给互联网用户获取信息服务的重要渠道，将面临网站篡改、网页挂马、SQL 注入攻击等多种安全问题，同时也面临上级单位和测评机构的安全检测的压力。一旦发生安全事件，将严重影响其形象和公信力。

2. 网上办事平台

网上办事一般由政府或企业为公众用户提供的便民服务，让用户可以足不出户完成业务的办理，如考试报名系统、政府在线申报系统、医院网上预约挂号系统等。以考试报名系统为例，在考试报名、查询成绩等期间均会出现流量井喷现象，其系统要求可靠性高、实时性强，如果黑客恶意发起大量 DDOS/CC 攻击会造成系统中断，对网上办事用户造成严重影响，且网上办事系统承载着大量用户隐私信息，将面临数据泄露等众多 Web 安全问题。同时，由于该类系统具有并发量大等特点，极易出现网页访问速度慢的情况，严重影响用户体验。

3. 大型活动/发布会等

各类大型活动主办方都会筹办活动官网，作为活动宣传、展示活动信息、业务开展的入口。由于大型活动自身备受关注、影响力巨大等特点，其相关网站更是成为黑客炫技、敲诈勒索、不当竞争最爱的攻击目标之一。一旦遭受攻击，导致其业务服务质量下降，甚至服务中断，影响业务正常开展，严重损害活动主办方的社会形象和公信力。

4. 金融行业

近年来，在线理财、彩票、基金、P2P 等互联网金融发展得风起云涌，金融行业向来是黑客觊觎的“钱袋子”。而该类业务平台对业务可用性要求非常高，而一旦发生安全问题，如网站无法正常登录——哪怕是短暂的，也可能会引发投资人恐慌，造成金融界最恐惧的挤兑事件。同时，该类业务对实时性要求也非常高，如出现网站响应缓慢，影响业务操作等情况，将会影响平台信誉度和用户体验。

5. 电子商务

越来越多的企业开展电商业务来迎合用户网购需求。黑客通过爬虫手段独占电商平台提供的优惠、返现等资源以牟利，导致企业投入的资源无法帮助其扩展自身业务且消耗大量带宽等支出。同时电商平台也面临着恶意竞争等因素引起的 DDoS 攻击而导致业务中断等问题。且电商平台具有并发量大、跨区域跨运营商访问频繁等特点，极易出现网页访问速度慢的情况，进而影响业务的实时性和网购体验。

6. 旅游服务行业

旅游服务行业包含旅游、交通、住宿、餐饮等一系列服务，其中诸多环节已成为黑客觊觎的对象，如在交通方面，航空售票、铁路售票等互联网售票平台频繁遭受恶意刷单、占座、恶意查询等；在住宿方面，酒店订单系统频受攻击，导致敏感歇息泄露（姓名、电话、信用卡、入住/退房时间等）；景区网上订票系统，一些“黄牛党”大量囤票后，借机把价格炒高数倍获利；旅游高峰期，同行通过 DDoS/CC 攻击，致使竞争对手网站中断服务。这些行为不仅危害了旅客的个人利益，也给各平台造成了经济损失。

3. 解决方案功能

网宿 GESS 提供监控报警、DDoS 防护、Web 应用攻击防护、漏洞补丁修复、内容安全保障、Bot 管理、加速、源站高可用性保障等一站式服务，保障用户网站安全稳定运行。

3.1. 监控报警

网宿 GESS 能够为用户提供多维度、全方位的监控报警服务，包括网站弱点检测、攻击监控报警、网站可用性监控等，帮助网站相关人员更加及时有效了解站点是否存在安全隐患、是否在遭受攻击、可用性情况等，同时采用多种告警通知方式，协助客户运维人员快速发现问题、定位问题、解决问题。

网站弱点检测：网宿安全团队通过自主挖掘与行业共享相结合的方式搜集漏洞信息并更新漏洞库，通过扫描等手段对网站的脆弱性进行检测，提供 SQL 注入、XSS、CSRF 等各类 Web 漏洞和第三方开源程序漏洞扫描服务，以及弱口令检测、安全配置错误检测，敏感信息检测等，挖掘 Web 应用中可能影响业务正常运行、敏感信息泄露等的漏洞，并对漏洞风险进行评级，输出网站弱点检测报告。

3.2. 访问控制策略

访问控制策略主要包括 IP/URL 黑白名单、单 IP 访问控制、单 URL 访问控制、域名整体访问控制等。

- **黑/白名单**

黑/白名单包括 IP 黑白名单和 URL 黑/白名单。

IP 黑白名单可以设定 IP 访问白名单和黑名单。如将源站办公环境的出口 IP 设置为白名单，加入白名单后的 IP，将不受防护策略限制。

URL 黑/白名单可以设定 URL 访问白名单和黑名单。有些攻击者使用非法 URL 进行攻击，导致大量回源，可将此类 URL 设置为黑名单，拒绝其访问。

- **单 IP 访问控制**

通过设定某 IP 的访问频率阈值，超出阈值则拦截或进行人机校验，GESS 的阈值设置能够根据自学习引擎的学习结果动态自动调整。

- **单 URL 访问控制**

通过设定某 URL 的连接数阈值，超出阈值则返回 403，避免过高的连接数导致网页无法访问，GESS 的阈值设置能够根据自学习引擎的学习结果动态自动调整。

- **域名整体访问控制**

有些攻击 IP 很庞大，单 IP 请求量不大，但总请求量比较大。针对此类的攻击，启用域名整体访问控制，当域名的回源总数超过一定的次数时，则触发防御策略，控制总体防问次数，保护源站。

3.3. 攻击防御

GESS 提供网络层/应用层 DDoS 攻击防护、Web 应用攻击防护、内容安全保障、业务安全保障服务。

3.4. 网络层/应用层 DDoS 攻击防护

针对网络层 DDoS 攻击，通过在 GESS 服务节点上部署智能防火墙，实现对数据报文的实时检测和分析，在不影响正常数据报文访问的前提下，实时高效阻断攻击报文。GESS 单机防护性能可达 40Gbps，平台总体防护能力达 1Tbps+。目前可有效防御 SYN Flood、UDP Flood、ICMP Flood、NTP 反射攻击、SSDP 反射攻击、DNS 反射攻击等各类网络层 DDoS 攻击。

针对应用层 DDoS 攻击，网宿 GESS 通过威胁情报库、访问控制、日志自学习、人机校验等方式实现对请求包实时检测和分析，在不影响正常访问的前提下，实时高效阻断恶意请求，单机防护性能达 500 万 QPS，平台总体防护能力达 10 亿 QPS。目前可防御 CC、HTTP Flood、慢攻击、POST Flood 等各类常见的应用层 DDoS 攻击。

3.4.1. Web 应用攻击防护

通过攻击特征库+自学习防护引擎相结合的防御机制，能够防御 SQL 注入、XSS 跨站脚本、目录遍历、木马上传、第三方开源软件漏洞、非授权核心资源访问等 OWASP 常见 Web 应用攻击，避免政企网站资产数据泄露，保障网站的业务安全。

攻击特征库：基于大数据分析技术提取历史攻击事件的攻击特征并入库，当请求命中攻击特征时能够快速有效拦截攻击。

自学习防护引擎：通过自学习网站正常访问的特征（如数据类型、数据边界、数据取值等）和业务访问逻辑，构建出被防护网站的应用程序结构、正常用户访问的流量数据模型，进而更加精准有效地应对 0day 漏洞。

3.4.2. 内容安全保障

网宿 GESS 基于大数据分析等技术，提供全链路防篡改（包括云端阻断篡改行为、传输防篡改和源站防篡改）、双向防敏感信息泄露（检测并阻断可能引起敏感信息泄露的恶意请求；检测响应内容是否存在服务器敏感信息、个人隐私信息等）、全程防劫持（包括防域名劫持、防传输劫持、清除广告植入）、防资源盗链、智能图片鉴黄等服务，为政企网站提供全方位的内容安全保障。避免网站内容被篡改、敏感信息泄露、页面被劫持、资源被盗链、页面被上传黄色图片等现象，维护政企对外形象。

3.5. Bot 管理

Bot 程序是指按照一定的规则自动的抓取互联网信息的程序或者脚本，已被广泛应用于互联网领域。

网宿 GESS 实时检测网站访问流量，并基于大数据分析、客户端指纹采集、布设爬虫陷阱、行为特征分析等技术，识别真实用户流量及各类 Bot 流量，并针对 Bot 流量进行合理的智能分类与管理。

GESS 将 Bot 流量分为善意 Bot 和恶意 Bot。善意 Bot（如搜索引擎类 Bot、图片搜索引擎类 Bot 等）有助于网站的优化和推广。恶意 Bot（如注册 Bot、登录 Bot、营销活动 Bot、购票 Bot 等），常

见于网站的注册（如机器人注册、垃圾注册、注册短信攻击等）、登录（如撞库、暴力破解等）、活动促销（如刷红包、抢优惠券、薅羊毛等）、订票（“黄牛”抢票、抢号、占座）等业务环节，将给客户带来经济和形象损失。同时，频繁的爬取行为将导致网站服务器负载高，进而影响源站响应速度甚至宕机。

针对识别出来的 Bot 流量，GESS 可以根据客户需求，提供告警、拦截、限速、伪造响应、重定向等 Bot 管理策略。

3.6. 源站高可用性保障

网宿 GESS 能够提供多源负载均衡、无损限流等方式保障客户网站业务突增时稳定运行。同时，如客户网站由于不可抗拒外力因素不能正常对外响应，能够提供主备源无缝切换、离线模式、源站被篡改后应急响应等多项紧急服务，保障访问者依然能够获取相关服务，将客户意外损失降到最低，维护对外形象。

3.7. 加速服务

GESS 由分布在全国各地的运营商节点组成，可以将网页中静态内容通过智能缓存技术分发至全网服务节点，并通过智能调度将网站访问者的请求调度到最近服务节点上，由节点直接向网站访问者提供相应的内容，缓解源站压力，加快访问速度，提高用户体验。针对网页中的动态内容，GESS 可通过网宿自主研发的智能路由、内容压缩等技术提升访问速度。

3.8. 支持 HTTPS 业务

为了应对数据传输安全性问题，越来越多的网站采用 SSL 加密传输，网宿提供无缝部署、无证书部署和 SNI 部署三种 HTTPS 业务部署方案。

◆ **无缝部署**

无缝部署是指用户证书和私钥全程加密传输部署，无人工介入，保障加密证书文件与内容服务的安全性，并且采用调度中心智能审核验证证书内容，确保证书准确性，缩短部署时间。

◆ **无证书部署**

针对数据保护要求较高而不能提供私钥的客户（如银行证券机构），网宿支持无证书部署方案，客户无需提供证书，只需要在源站配合安装一个网宿提供的私钥服务器软件进行私钥解密工作，使节点服务器在不持有私钥的情况下，也可与客户端建立正常的 SSL 连接，客户无需担心私钥泄露风险又可以提升访问速度。

◆ **SNI 证书部署**

网宿通过服务器名称指示技术（SNI）能够在一个 IP 上部署多个证书，使多个 HTTPS 客户可以共享一套服务 IP,用户能够获得更丰富的节点资源，实现按需扩展，提升加速效果和访问体验。

3.9. 可视化报表

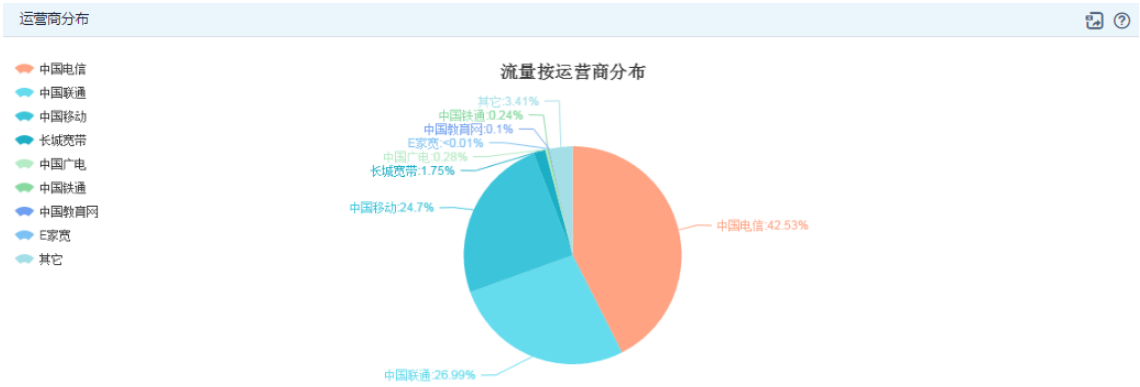
网宿 GESS 实时展示业务情况及防护信息，用户可以实时查看防护效果，并根据攻击趋势了解网站的安全状态。

◆ **业务访问情况**

提供业务访问数据分析，如访客分布、PV、访问来源等指标展示，帮助运营人员全面了解线上业务的运营情况。

➢ 访客按区域（按省/按地区）分布情况：

➢ 访客按运营商情况分布情况：



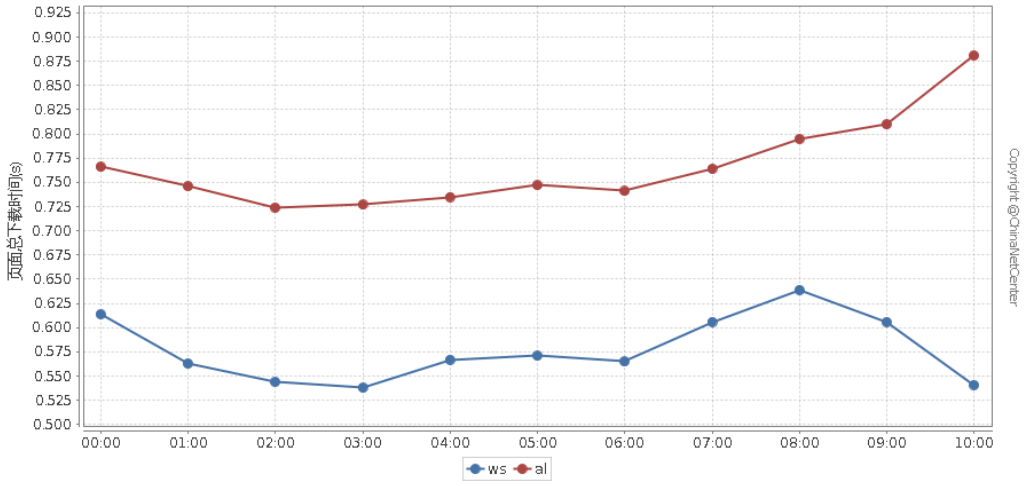
访客运营商分布情况

➢ PV 按省份/地区排行：

PV 排行

◆ **加速效果监控**

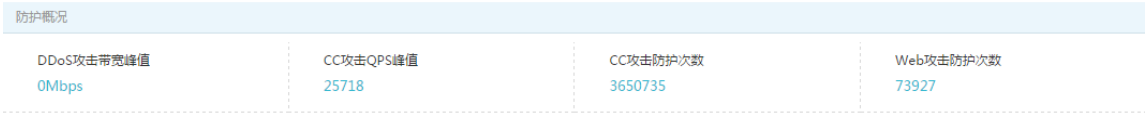
直观展示网站加速前与加速后的加速效果对比，使运维人员了解使用服务后的价值：



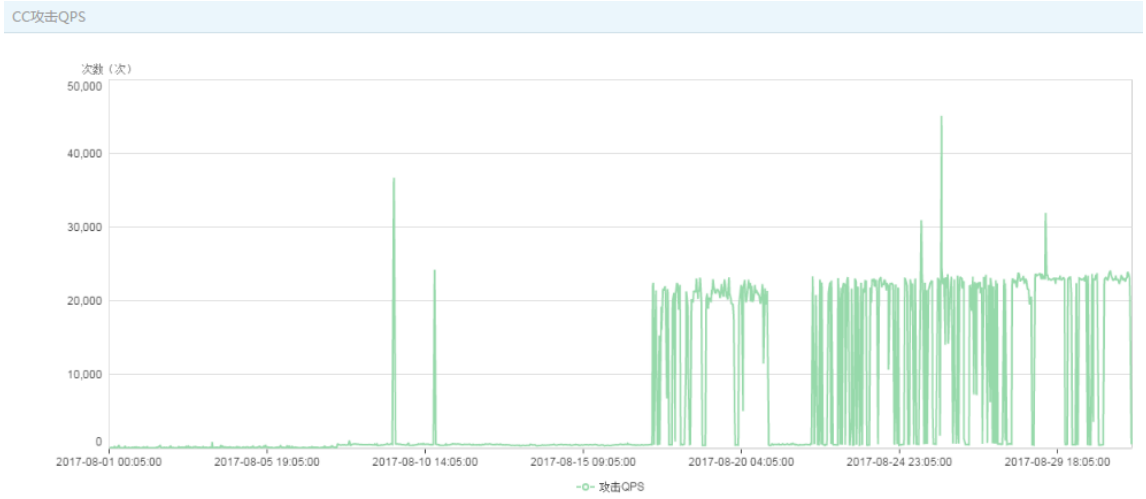
◆ **攻击数据展示**

（1）展示网站 DDoS/CC 防护、Web 攻击防护概况，方便客户了解网站安全情况。包括某段时间内 DDoS 攻击带宽峰值、清洗流量类型、CC 攻击 QPS、Web 攻击次数等。

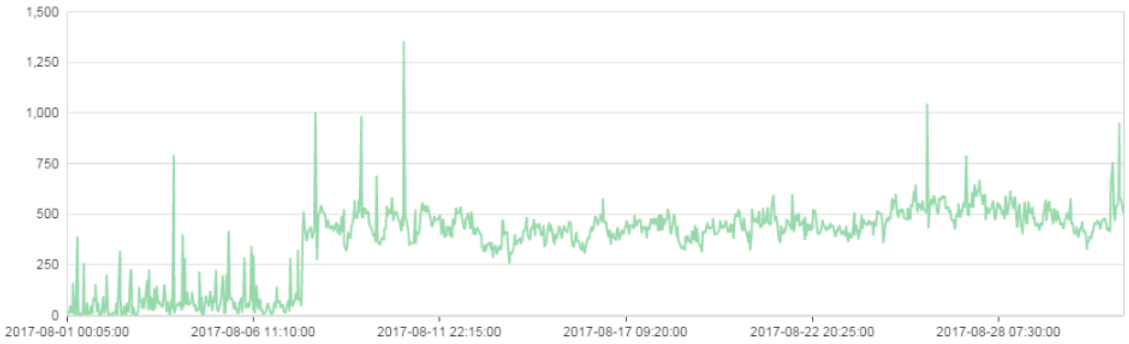
i. 防护概况展示：



ii. CC 攻击防护展示：



iii. Web 应用攻击防护展示：



（2）以攻击事件形式展示攻击 IP、所属区域、攻击时间、攻击域名等。

防护动态

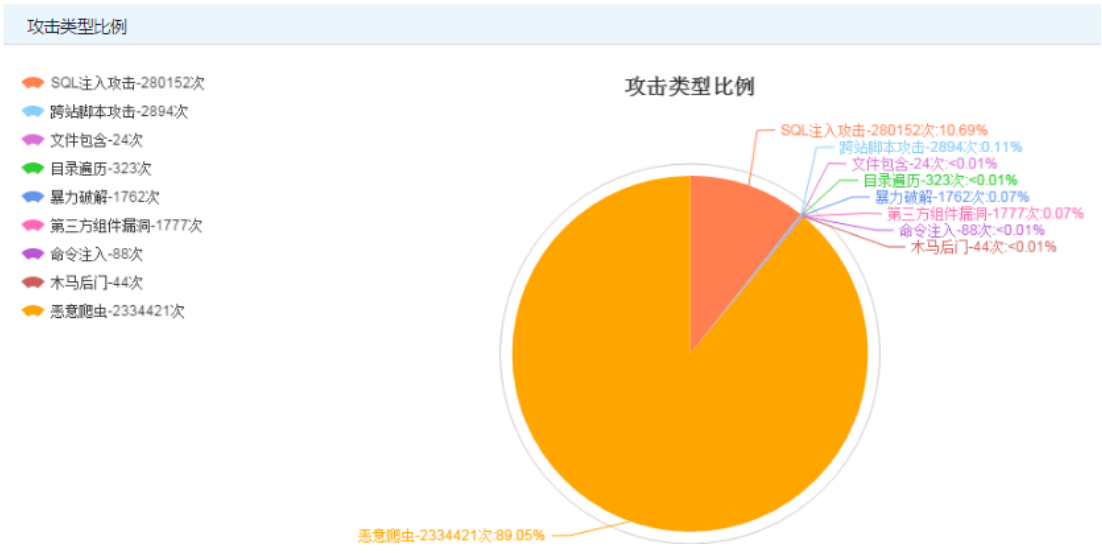
序号	攻击IP	所属区域	攻击时间	攻击域名	处理动作
1		娄底/loudi/CN	2017-09-15 15:17:00	www	拦截
2		邵阳/shaoyang/CN	2017-09-15 15:17:00	www	拦截
3		娄底/loudi/CN	2017-09-15 15:16:00	www	拦截
4		邵阳/shaoyang/CN	2017-09-15 15:16:00	www	拦截
5		娄底/loudi/CN	2017-09-15 15:15:00	www	拦截
6		邵阳/shaoyang/CN	2017-09-15 15:15:00	www	拦截
7		娄底/loudi/CN	2017-09-15 15:14:00	www	拦截
8		邵阳/shaoyang/CN	2017-09-15 15:14:00	www	拦截
9		娄底/loudi/CN	2017-09-15 15:13:00	www	拦截
10		邵阳/shaoyang/CN	2017-09-15 15:13:00	www	拦截
11		娄底/loudi/CN	2017-09-15 15:12:00	www	拦截
12		邵阳/shaoyang/CN	2017-09-15 15:12:00	www	拦截
13		娄底/loudi/CN	2017-09-15 15:11:00	www	拦截
14		邵阳/shaoyang/CN	2017-09-15 15:11:00	www	拦截
15		娄底/loudi/CN	2017-09-15 15:10:00	www	拦截

（3）提供被拦截的 IP 详细信息，包括 IP 所在地、攻击类型、攻击次数等，以利于客户对后续对攻击者的处理。

攻击IP详情

序号	攻击IP	所属区域	总访问次数	攻击类型	攻击次数
1	[redacted]	中国大陆	2,091	非法下载	900
2	[redacted]	美国	1,266	跨站脚本攻击 SQL注入攻击 非法下载	516 221 28
3	[redacted]	美国	22,811	跨站脚本攻击 SQL注入攻击 非法下载	433 219 7
4	[redacted]	香港	1,122	跨站脚本攻击 SQL注入攻击 非法下载	391 217 34
5	[redacted]	香港	1,108	跨站脚本攻击 SQL注入攻击 非法下载 第三方组件漏洞	348 198 30 14
6	[redacted]	中国大陆	1,405	跨站脚本攻击 SQL注入攻击 非法下载 第三方组件漏洞 木马后门	327 143 30 16 1
7	[redacted]	台湾	861	跨站脚本攻击 SQL注入攻击 命令注入 非法下载	243 160 47 25
8	[redacted]	中国大陆	2,782	非法下载	414
9	[redacted]	香港	474	跨站脚本攻击 SQL注入攻击 非法下载	231 127 20

（4）饼图形式展示攻击类型分布：



4. 解决方案价值

4.1. 零部署、零维护，轻松享受一站式服务

使用网宿 GESS，用户无需改变网站现有拓扑架构，不需添加任何硬件，只需简单地做一层 CNAME，即可享受专业的集安全防御和网页加速为一体的服务。有效防御各类网络层和应用层攻击，防止网站被篡改、敏感信息泄露等，保障网站稳定安全运行，保障网站业务和内容安全，并提升网站服务质量。

4.2. 全方位监控报警，实时掌控网站情况

网宿 GESS 提供 7*24 小时全方位的自动化监控报警服务，包括网站弱点检测、可用性监控、攻击监控等。发现问题可立即告警，并生成告警报告及可视化图表，使相关人员对网站的安全状态一目了然，并协助相关人员评估网站安全状况。

4.3. 数据驱动安全，保障业务不中断

网宿 GESS 依托大数据分析平台和丰富的威胁情报库，能够在云端进行攻击事件特征分析及关联分析，内置的威胁评估模型自动预测攻击趋势及风险，对于高风险攻击事件能够全网快速部署防御策略，防患于未然，保障用户业务不中断。

4.4. 全链路防篡改，维护政企形象

政企网站的页面如果被恶意篡改，植入赌博、黄色等非法信息，将严重影响其对公形象和公信力。网宿 GESS 提供全链路防篡改体系，包括云端阻断 SQL 注入、XSS 等可能导致篡改的行为、传输防篡改和源站防篡改服务，从而避免政企页面被篡改，维护政企形象。

4.5. 双向检测机制，避免敏感信息泄露

网宿 GESS 采用双向敏感信息检测机制，一方面实时检测并阻断可能引起敏感信息泄露的恶意请求（如 SQL 注入、XSS 等 Web 应用攻击），另一方面检测源站响应内容是否存在敏感信息（如是否存在服务器敏感信息、非法敏感词汇等），并采取相应措施，避免敏感信息泄露。

4.6. 高效应急响应能力

网宿 GESS 提供专属安全服务团队为用提供 7*24 小时一对一的贴身服务，遇到突发事件时能够保障及时响应，提供各项应急预案，保障用户的业务不受影响。

关于网宿

网宿科技 始创于 2000 年 1 月，主要提供互联网内容分发与加速（CDN）、云计算、云安全、全球分布式数据中心(IDC) 等服务。

2009 年 10 月，网宿科技在深交所上市，股票代码 300017。

网宿科技拥有遍布全球的 1000+ CDN 加速节点，在北京、上海、广州、深圳等地设有分公司，在美国、香港、印度、爱尔兰、马来西亚、济南、南京、杭州等地建有多家全资子公司，并在厦门及美国硅谷设立了研发中心。现有员工 3000 多名，研发以及技术人员占总人数 60% 左右。客户群覆盖各类互联网门户网站、视音频网站、网络游戏公司、电子商务网站、政府网站、企业网站以及运营商等，公司服务的客户超过 3000 家，是市场同类公司中拥有客户数量较多、行业覆盖面较广的公司。