安全云加速（WSS） 产品白皮书V3.0

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

网宿安全云加速（WSS）为“网宿网盾”品牌旗下一款将“DDoS 攻击防御”和“网络加速”结合而设计的产品，在保障网站高性能访问的同时，在云端阻断各类 DDoS 攻击，实现“平时加速、攻时防御”，形成真正意义上的“一站式安全加速服务”，使网站访问环境更为安全、稳定、高效。

“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+”的高速发展，网络安全问题也日益突出，其中分布式拒绝服务攻击（DDoS）以其简单粗暴、攻击效果显著、难以抵御和追踪的特点成为黑客进行网络攻击的首选。互联网行业主要面临以下挑战：

◆ **DDoS 攻击事件频发，影响企业正常运营**

目前地下黑色产业市场已形成一条成熟的产业链，发动 DDoS 攻击的服务和工具已公然在网上叫卖，因此，其发动门槛极低，而由于利益驱动（如敲诈勒索、恶意竞争等）等因素，DDoS 攻击越来越多。根据 CNCERT 发布的《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击次数较第一季度增长 1.1 倍，全年日均达 133 次，占日均攻击事件的 29.4%。

DDoS 攻击将导致平台服务中断，进而导致用户流失、交易量下降、品牌形象损失等，甚至有些黑客还利用 DDoS 攻击对企业进行敲诈勒索，这些都给企业的正常运营带来极大的影响。

◆ **传统防护方式存在瓶颈**

企业可能会选择购买抗 D 硬件设备来抵御 DDoS 攻击。这种方法虽然能一定程度上缓解攻击，但是存在以下瓶颈：

1. 受限于带宽和设备性能，无法有效应对突发大流量攻击

目前市场上黑客攻击成本和门槛都很低，已经形成了产业链，同时黑客攻击手段捉摸不定，数百 G 的突发大规模攻击已是司空见惯。而传统抗 D 硬件设备的可扩展性受限于带宽和设备性能，因此当黑客骤然提高攻击流量后，传统防御方式往往失效，所以不能从根本上防护 DDoS 攻击。

2. 部署复杂，运维难度高

硬件设备一般采用串联或旁路方式部署，需要对源站的网络拓扑做变更，部署过程中存在系统和业务风险，并且加大运维难度，当设备出现问题时，难以及时解决。

3. 数据分析能力有限，存在误杀

硬件设备受限于数据来源和数据采集分析能力，无法很好整合数据资源，且具有封闭性，防御算法更新慢，难以形成联动防御，因此应用层 DDoS 攻击（尤其是 CC）识别能力较弱，进而影响到防御效果。

◆ **网站访问响应慢，影响用户体验**

随着企业业务的扩展，其业务网站的访问并发越来越高，同时，跨运营商、跨区域访问频繁，而运营商针对跨网传输的内容都做了流量限制（如电信与联通之间有着数万毫秒的网络延时），将导致跨网访问的时延过高，而国内还存在一百多家小运营商，运营商互联互通问题瓶颈愈加凸显，各类问题都导致网站容易出现网站响应速度慢等现象，影响用户体验和办公效率。在各行各业竞争激烈的大背景下，一个体验不好的网站将流失大量用户，直接影响企业的收入与形象。

2. 产品介绍

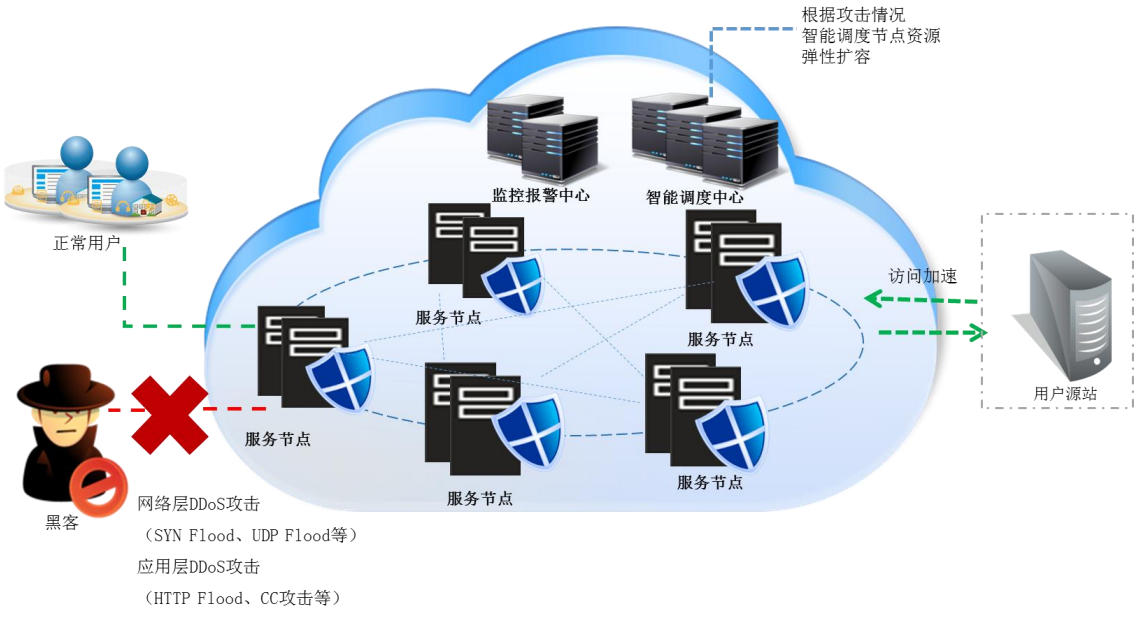
2.1. 产品简介

网宿安全云加速产品（WSS） 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 DDoS 攻击（如 SYN Flood、ACK Flood、UDP Flood、CC 等），同时为正常访问者提供加速服务，提升网站访问体验。

2.2. 产品技术架构

网宿 WSS 依托全球部署的云安全节点联接形成云安全网络，并配以专有的攻击监控报警中心和智能调度中心，结合云端大数据分析平台，实时检测分析请求包，如发现异常请求则拦截，并根据攻击情况实时动态调整防护策略，有效保障客户网站安全；对于正常访问提供加速服务，提升用户访问体验。

网宿 WSS 产品架构如下图所示：



2.3. 产品适用行业与场景

网宿 WSS 致力于为企业提供集 DDoS 防护与加速为一体的服务，保障客户网站业务可用性的同时，提高网站的访问速度。

WSS 的应用场景包括但不限于：

1. 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。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。

2. 互联网金融

近年来，在线理财、彩票、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”，且同行竞争也非常激烈。而该类网站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。

3. 在线教育

在线教育平台能够让学生通过视音频、互动白板等形式在网上接受名师的 VIP 辅导。由于同行恶意竞争等因素，极易遭受 DDoS 攻击，导致其网站访问缓慢难以登录，影响用户在线学习体验。

3. 产品功能

网宿 WSS 提供监控报警、攻击防护（包括网络层 DDoS 防护、应用层 DDoS 防护）、防护数据可视化、网页加速等功能，保障网站服务实时稳定在线。

3.1. 监控报警

能够为用户提供多维度全方位的监控报警服务，包括攻击监控报警、网站可用性监控、安全预警和节点服务质量监控，保障用户能够第一时间掌握网站各种异常情况。

◆ **攻击监控报警**

网宿 WSS 提供全方位的 DDoS 攻击监控报警功能：

➢ 网络层 DDoS 监控报警

网宿 WSS 为每个客户提供一组独立 IP 服务，因此能够以客户为粒度实时采集并统计客户对应服务 IP 的网络层攻击带宽，当网络层攻击到达客户设置的攻击带宽阈值时，将通过邮件/短信形式向客户报警，报警信息包括攻击时间、攻击峰值等。

➢ 应用层 DDoS 监控报警

网宿 WSS 各安全节点通过动态学习客户的历史访问日志（如客户每个资源的访问量、行为特征等），建立动态访问基线，当检测到异常访问时，根据报警规则（如 QPS 设置的阈值）通过邮件/短信形式向客户发送相应攻击报警。

◆ **网站可用性监控报警**

包括 HTTP/HTTPS 监控、PING 监控。

➢ HTTP/HTTPS 监控

通过周期性模拟访客请求访问被监控站点，通过分布在全球各地的监控节点实时获取站点的响应状态和请求详情，如发现网站出现响应异常情况，将通过邮件、短信等渠道告知站点相关人员，帮助站点人员第一时间察觉网站异常。

➢ PING 监控

通过周期性探测被监控的主机或者站点连通性，获取站点/服务器的连通状态、丢包率、RTT 响应时间等信息，并结合实时报警模块，通过邮件、短信等渠道将链路异常信息告知客户相关人员。

◆ **安全预警**

网宿 WSS 通过大数据分析平台对云端攻击数据进行分析，提取其攻击特征（如 IP、UA、Refer 等），并可查看采用同类型攻击手法的多网站数据及行业数据，进行安全事件关联分析，进而全网下发防护策略，联动防御，并对可能遭受攻击的行业提前配置安全防御体系，防患于未然。

◆ **节点服务质量监控**

网宿 WSS 提供 7*24 小时全网节点监控，能够基于服务质量（如根据各节点的负载、流量等）智能调度服务节点，保障服务实时稳定可用。

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，WSS 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，WSS 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，控制总体访问次数，保护源站。

3.3. 攻击防御

3.3.1. 网络层 DDoS 防御

网络层 DDoS 攻击是攻击者通过伪造大量 IP 地址向目标服务器发起大量数据包，耗尽网络带宽资源进而导致目标服务器无法响应正常的请求。常见的网络层 DDoS 攻击包括 SYN Flood、ACK Flood、ICMP Flood、UDP Flood、各类反射攻击（如 NTP 反射、DNS 反射、SSDP 反射）等。

网宿 WSS 通过部署智能防火墙，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。WSS 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。各攻击类型简介及防护方法如下：

- **SYN Flood**

  - 攻击简介

攻击者利用工具或者操纵僵尸主机，向目标服务器发起大量的 TCP SYN 报文，当服务器回应 SYN-ACK 报文时，攻击者不再继续回应 ACK 报文，导致服务器上存在大量的 TCP 半连接，服务器的资源会被这些半连接耗尽，无法响应正常的请求。

  - 防护原理

采用异构防护架构，利用国内独创的专利技术实时检测过滤畸形包（如长度值异常等）和不符合规则的报文，同时通过 SYN Cookie 校验、重传验证等方式完成客户端的协议行为验证，从而在不影响正常客户端连接的情况下阻断攻击。

- **ACK Flood**

  - 攻击简介

攻击者利用工具或者操纵僵尸主机，向目标服务器发送大量的 ACK 报文，服务器忙于回复这些凭空出现的第三次握手报文，导致资源耗尽，无法响应正常的请求。

➢ 防护原理

网宿智能防火墙实时存储连接表信息，通过对接收到的 ACK 报文进行智能校验，判断其是否为合法报文，如不合法，则直接丢弃，进而高效阻断攻击报文，不会对正常访问造成影响。

◆ **ICMP Flood**

➢ 攻击简介

攻击者通过对目标发送大量超大数据包（例如：超过 65535 字节的数据包），给服务器带来较大的负载，影响服务器的正常服务，进而令目标主机瘫痪。

➢ 防护原理

智能防火墙实时统计到达目的 IP 的流量，超过设定阈值则直接丢包。

◆ **UDP Flood**

➢ 攻击简介

由于 UDP 协议都是无连接的协议，不提供可靠性和完整性校验，因此数据传输速率很快，成为攻击者理想的利用对象。UDP Flood 的常见情况是攻击者向目标地址发送大量伪造源 IP 地址的 UDP 报文，消耗网络带宽资源，造成链路拥堵，进而网站服务器拒绝服务。

➢ 防护原理

针对没有 UDP 业务的客户，网宿智能防火墙丢弃所有 UDP 包。对于有 UDP 业务的客户，网宿智能防火墙通过速率限制、UDP 报文匹配等方式防御 UDP Flood。

◆ **反射型 DDoS 攻击**

➢ 攻击简介

反射攻击是基于 UDP 报文的一种 DDoS 攻击形式。攻击者不是直接发起对攻击目标的攻击，而是利用互联网的某些服务开放的服务器（如 NTP 服务器、DNS 服务器），通过伪造被攻击者的地址、向该服务器发送基于 UDP 服务的特殊请求报文，数倍于请求报文的回复的数据被发送到被攻击 IP，从而对后者间接形成 DDoS 攻击。

➢ 防护原理

网宿智能防火墙直接过滤来自常用的反射端口（如 NTP、DNS、SSDP 等）的报文防御反射型 DDoS 攻击。

3.3.2. 应用层 DDoS 防御

网宿 WSS 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。各攻击类型简介及防护方法如下：

◆ **CC、HTTP Flood 攻击**

➢ 攻击简介

CC 攻击是指攻击者借助代理服务器模拟真实用户，不断向目标网站发送大量请求，如频繁请求某个动态 URL 或某个不存在的 URL，致使源站大量回源，耗尽网站服务器性能，进而致使目标网站拒绝服务。

HTTP Flood 是指攻击者借助代理服务器模拟真实用户，不断向目标网站发送大量请求，如频繁请求某个静态 URL，耗尽网站服务器性能，进而致使目标网站拒绝服务。

➢ 防护原理

1. 威胁情报库：WSS 通过大数据分析平台，实时汇总分析攻击事件的日志，提取攻击特征（如 IP、URL、User-Agent、Refer 等），并对这些特征进行威胁等级评估，形成威胁情报库，对于高风险性的 IP、UA、URL、Refer 等会自动下发到全网防护节点中，一旦后续请求命中威胁情报库中的高风险性特征，则直接拦截，最大限度地提高防御效率，避免 CC 攻击对网站的影响。
2. 个性化策略配置：如请求没有命中威胁情报库中的高风险特征，则通过个性化策略配置（如 IP 黑白名单、IP 访问频率控制）防御攻击；
3. 日志自学习：WSS 实时动态学习客户网站的访问特征（如客户每个资源的访问量、行为特征等），建立网站的正常访问基线。
4. 人机校验：当请求与网站正常访问基线不一致时，启动人机校验（如 JS 验证、META 验证等）方式进行验证，避免误杀正常访问，校验通过则放行该请求，如不通过，则拦截并实时将该请求的攻击特征同步至威胁情报库。

WSS 提供 JS 验证、META 验证、302 跳转、验证码等多种人机校验方式，有效拦截攻击的同时，保障正常用户的访问体验。

✓ JS 验证

通过返回 200+JS（内容为原先访问的 URL+验证 key）验证客户端是否合法，正常用户的客户端能够自动解析 JS 代码，带上验证 key 重新请求 URL，继续正常访问。而恶意访问无法解析 JS，则 WSS 拦截该请求。

✓ META 验证跳转

通过在 meta 标签加入验证参数验证客户端是否合法，正常用户的客户端能够自动解析节点返回的 meta 标签，并携带上验证参数重新发起请求，继续正常访问。而恶意访问无法解析，则 WSS 拦截该请求。

◆ **慢连接攻击**

➢ 攻击简介

攻击者利用 HTTP 协议的正常交互机制，先与目标服务器建立一个连接，然后长时间保持该连接不释放。如果攻击者持续与目标服务器建立大量这样的连接，就会使目标服务器上的可用资源耗尽，无法提供正常服务。HTTP 慢速攻击主要包括 Slow Headers 攻击和 Slow POST 攻击。

Slow Headers 攻击：攻击者使用 GET 或 POST 请求方法与目标服务器建立连接，然后持续发送不包含结束符的 HTTP 头部报文，目标服务器会一直等待请求头部中的结束符而导致连接始终被占用。当攻击者大量发起这类请求，将会导致服务器资源耗尽，无法正常提供服务。

Slow POST 攻击：攻击者向目标服务器发送 POST 请求报文提交数据，数据的长度设置为一个很大的数值，但是在随后的数据发送中，每次只发送很小的报文，导致目标服务器一直等待攻击者发送数据。当攻击者大量发起这类请求，将会导致服务器资源耗尽，无法正常提供服务。

➢ 防护原理

对 Slow Headers 攻击，WSS 通过检测请求头超时时间、最大包数量阈值（即请求报文的报文头中一段时间内没有结束符“\r\n”）进行防护。

对 Slow Post 攻击，WSS 通过检测请求小包数量阈值（即 POST 请求报文的长度设置的很大，但是实际报文的数据部分长度都很小）进行防护。

◆ **POST Flood**

➢ 攻击简介

攻击者利用攻击工具或者操纵僵尸主机，向目标服务器发起大量的 HTTP POST 报文，消耗服务器资源，使服务器无法响应正常请求。

➢ 防护原理

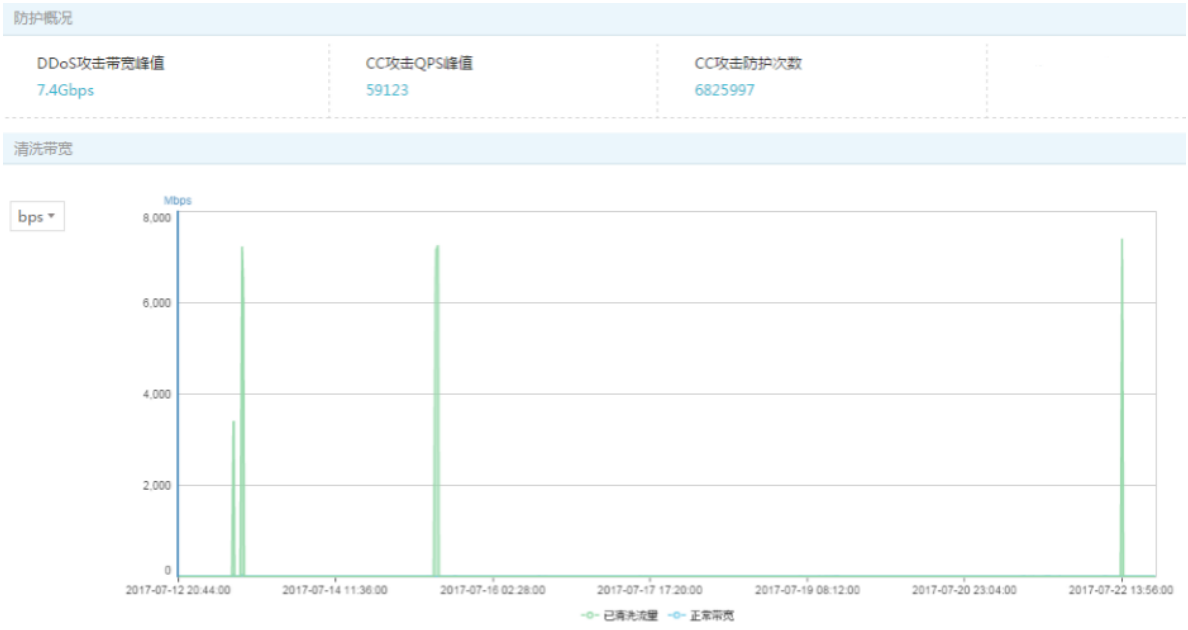
WSS 通过访问控制策略（如 IP 黑白名单、IP 访问速率等）、Cookie 校验等方式检测并拦截 POST Flood 攻击。

3.4. 防护数据可视化

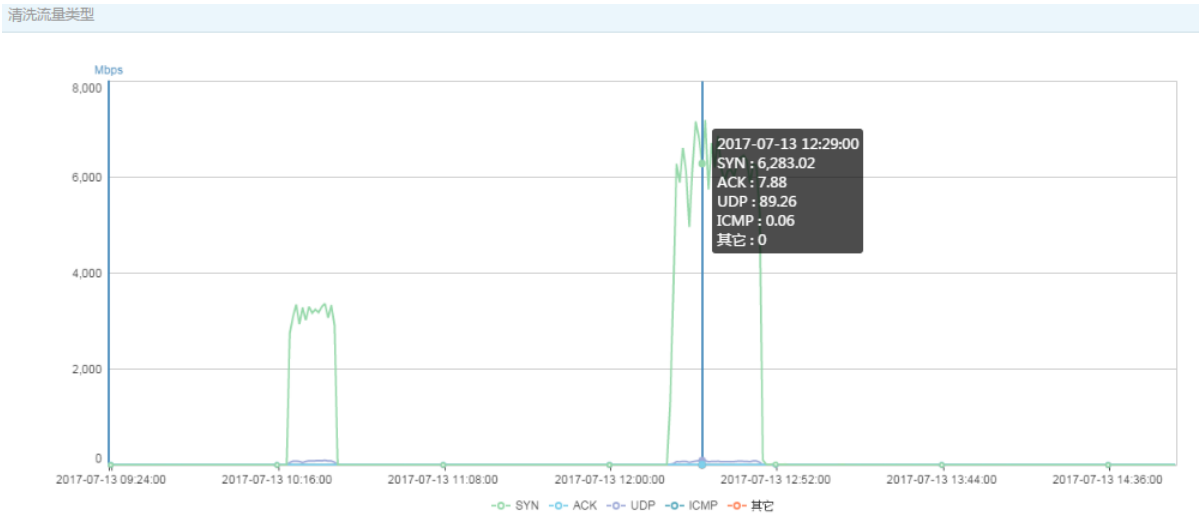
网宿 WSS 实时展示各类 DDoS 攻击的防护信息，客户可以实时查看防护效果，并根据攻击趋势了解网站的安全状态。

（1）展示网站防护概况，方便客户了解网站安全情况。

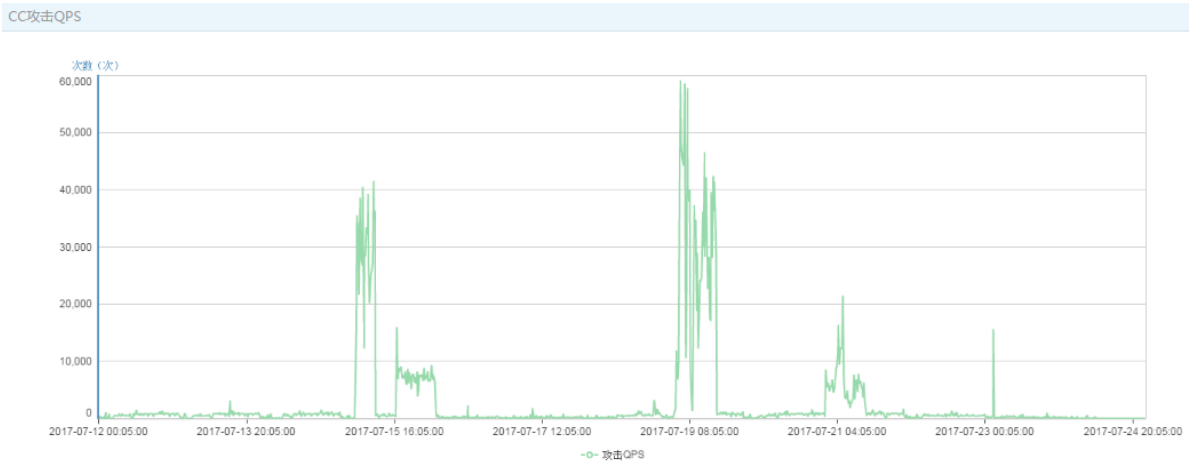
i. 某段时间内 DDoS 攻击带宽峰值，并实时展示清洗带宽和正常带宽。



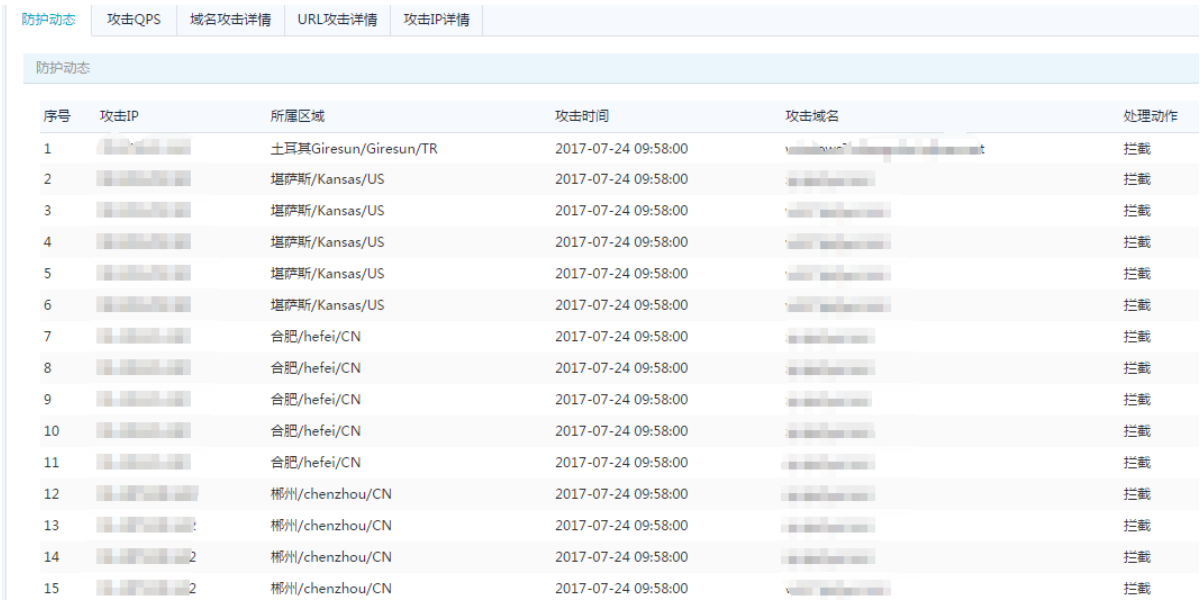
ii. 展示清洗流量类型



iii. 曲线图形式展示 CC 攻击 QPS。



（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 | 攻击QPS | 域名攻击详情 | URL攻击详情 | 攻击IP详情

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		土耳其Giresun/Giresun/TR	2017-07-24 09:58:00		拦截
2		堪萨斯/Kansas/US	2017-07-24 09:58:00		拦截
3		堪萨斯/Kansas/US	2017-07-24 09:58:00		拦截
4		堪萨斯/Kansas/US	2017-07-24 09:58:00		拦截
5		堪萨斯/Kansas/US	2017-07-24 09:58:00		拦截
6		堪萨斯/Kansas/US	2017-07-24 09:58:00		拦截
7		合肥/hefei/CN	2017-07-24 09:58:00		拦截
8		合肥/hefei/CN	2017-07-24 09:58:00		拦截
9		合肥/hefei/CN	2017-07-24 09:58:00		拦截
10		合肥/hefei/CN	2017-07-24 09:58:00		拦截
11		合肥/hefei/CN	2017-07-24 09:58:00		拦截
12		郴州/chenzhou/CN	2017-07-24 09:58:00		拦截
13		郴州/chenzhou/CN	2017-07-24 09:58:00		拦截
14		郴州/chenzhou/CN	2017-07-24 09:58:00		拦截
15		郴州/chenzhou/CN	2017-07-24 09:58:00		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

攻击IP	所属区域	总访问次数	攻击类型	攻击次数
	中国大陆	2,903,277	CC	2,903,277
	中国大陆	1,861,101	CC	1,869,069
	中国大陆	1,506,897	CC	1,506,897
	中国大陆	1,443,708	CC	1,443,708
	中国大陆	1,273,377	CC	1,272,811
	中国大陆	1,268,493	CC	1,253,935
	中国大陆	1,238,316	CC	1,237,685
	中国大陆	1,166,932	CC	1,161,099
	中国大陆	1,230,232	CC	1,158,568
	中国大陆	1,143,267	CC	1,143,267
	中国大陆	1,071,142	CC	1,055,668
	中国大陆	1,061,660	CC	1,053,160
	中国大陆	1,048,737	CC	1,041,812
	中国大陆	1,030,447	CC	1,021,088
	中国大陆	1,030,074	CC	1,020,881

3.5. 网页加速

WSS 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，缓存机制可以按客户需求进行针对性定制，如根据目录或扩展名等，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，WSS 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。具体如下：

- **智能路由**

公网默认传输路径存在偶发故障、低连通、高延时问题，这些问题严重影响请求的响应速度，用户请求的服务质量不能得到很好的保证。网宿自主研发的路由最优选择技术，能有效提升请求的响应速度。WSS 通过对网络情况进行全局探测，实时智能加权计算传输路径，避开公网故障或目前正在拥塞的路径，自动选择节点到用户网站总耗时最短、稳定性最好的路径回源。同时传输路径可实时根据网络情况自动切换，保证数据的最佳传输效果，解决传输路径过长、网络质量不稳定的问题。

- **内容压缩**

在相同的网络传输速度下，传输的字节数越少，则传输时间越短。WSS 通过网宿自主研发的传输内容压缩技术对网络中传输的数据进行压缩，可以有效减少网络传输的数据量，缩短传输时间，并在数据出口进行数据解压缩处理，保障请求数据的完整重现。例如网站服务器在北京，而福建用户发起请求，网站返回的数据是 100K，则经 WSS 中转节点将内容压缩到 30K 后进行传输，待数据传输到福建边缘节点时，将数据解压成 100K 后响应给用户。

3.6. 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。

4. 产品价值

4.1. 零部署、零维护，快速享受专业安全防护服务

使用网宿 WSS，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。并且由专业的安全专家一对一 7*24 提供服务，真正做到快速响应、深入了解、优质服务。

4.2. 数据驱动安全，保障业务不中断

网宿 WSS 依托大数据分析平台和丰富的安全威胁情报库，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。

4.3. 高效应急响应能力

网宿 WSS 提供专属安全服务团队为用户一对一的贴身服务，突发大规模攻击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。

4.4. 智能加速，提升网站用户访问体验

网宿 WSS 依托一张分布全球的智能加速网络，能够帮助终端用户更快地接入最佳服务节点，从而达到提升访问速度的效果，并可避免大量用户从同一服务器接入造成的拥塞，使服务质量得到保障。同时，WSS 还能有效解决跨地区跨运营商的瓶颈，解决了网络波动造成的访问不稳定问题。

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。