高防云清洗（DMS） 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

网宿高防云清洗（DMS）为“网宿网盾”品牌旗下一款高性能云端流量清洗产品。依托网宿强大的 CDN 平台，采用领先的攻击防御技术，平台抗攻击能力达 10 Tbps 级别，可对 SYN Flood、UDP Flood、ICMP Flood、CC 等主流 DDoS 攻击进行有效防御。

“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。目前 DDoS 攻击主要呈现以下趋势：

◆ **攻击频率越来越高，峰值越来越高**

随着 DDoS 攻击工具的泛滥及地下黑色产业市场的发展，DDoS 攻击门槛越来越低，且物联网设备的大力发展（但物联网设备厂商的安全意识普遍不高，其设备往往存在漏洞，极易被黑客利用成为 DDoS 攻击的工具），DDoS 攻击事件越来越频繁。根据 CNCERT 发布的《2016 年中国互联网网络安全报告》显示，2016 年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%，且数百 G 的攻击带宽已司空见惯。

◆ **攻击造成的损失越来越大**

DDoS 攻击将导致平台服务中断，服务中断导致的用户流失、交易量下降、网站恢复的代价、品牌形象损失等等，都应该计算到其经济损失内，甚至目前有些黑客还利用 DDoS 攻击对网站进行敲诈勒索，这些都给网站的正常运营带来极大的影响，DDoS 攻击造成的损失呈几何式增长。在网络攻击猖獗的大环境下，互联网企业频繁遭遇窘况，无法专注于业务开展和推广，形式及其严峻。

◆ **传统防护方式存在瓶颈**

为了抵御各类 DDoS 攻击，企业可能会选择购买抗 D 硬件设备或高防机房的方式来提高系统抗 DDoS 攻击的能力。这种方法虽然能一定程度上缓解攻击，但是这两种方法存在以下不足：

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，影响正常业务开展

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。高防机房，一般是单运营商路线防护，并且，一般是在骨干网做防御，如果攻击影响了出口带宽就直接封 IP，极易造成误杀，影响企业的正常运营。

4. 安全防御成本高

硬件设备单台的价格在 5-30 万不等，平均生命周期 3 年左右，大大提高了安全防御的成本。此外，遇到攻击，需要专业安全团队进行设备监控、策略调整和升级维护，需要企业设置专业的安全运维岗位，增加了人力成本。

2. 产品介绍

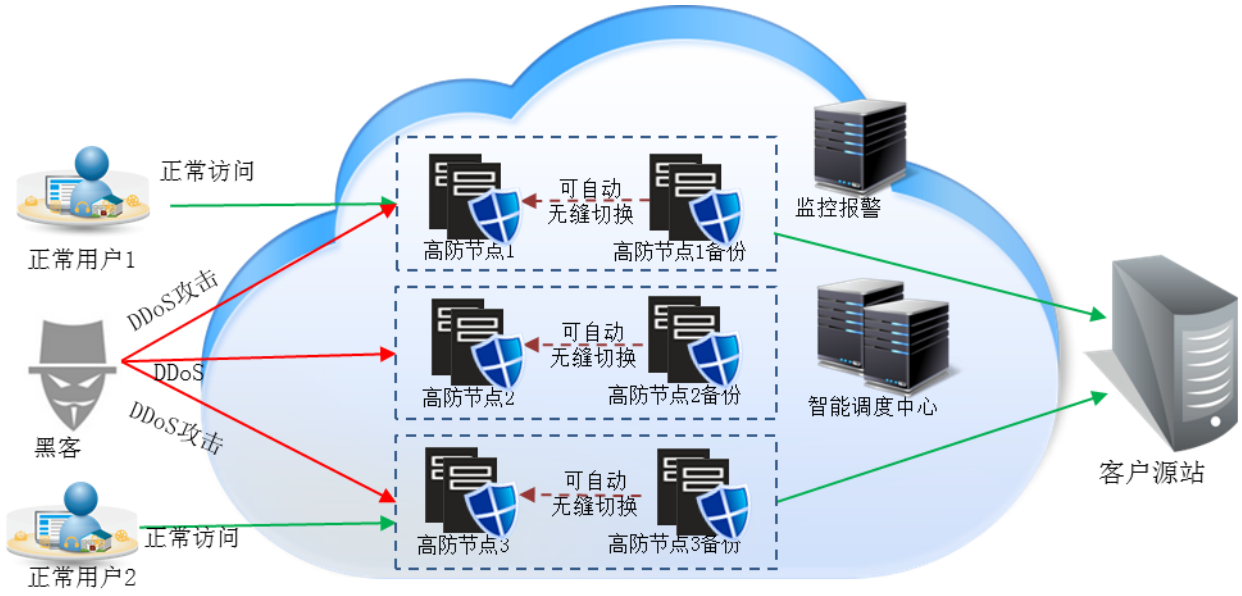
2.1. 产品简介

网宿高防云清洗（DDoS Mitigation Service，简称 DMS），依托 CDN 资源优势，结合大数据分析，自主研发防护算法，实时检测并清洗各类 DDoS 攻击（如 SYN Flood、UDP Flood、CC 等），保障基于 HTTP/HTTPS 的用户业务在遭遇大流量 DDoS 攻击时仍然能够稳定在线。

目前 DMS 单节点抗攻击能力可达 600Gbps，同时 DMS 的智能调度中心能够根据攻击情况智能调度全网资源，总体抗攻击能力达到 10Tbps+。

2.2. 产品技术架构

网宿 DMS 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，有效保障用户平台安全。网宿 DMS 产品架构如图所示：



2.3. 产品适用行业与场景

DMS 面向的行业及使用场景包括但不限于：

1. 游戏行业

游戏行业作为高产值、高利润、竞争激烈的行业，一直是黑客发起 DDoS 攻击的高发地，同时也是动辄数百 G 大流量攻击的多发行业。对于游戏行业来说，保证业务的可用性和连续性是留住玩家的前提，而 DDoS 攻击恰恰是对可用性和连续性的最大威胁。

2. 金融行业

金融行业（证券、基金、股票等）向来是黑客觊觎的“钱袋子”，且同行竞争也非常激烈。该类业务系统对业务可用性要求非常高，而一旦发生业务中断，如系统无法正常登录——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。

3. 直播行业

随着直播行业的大火，鉴于黑客向来是哪里热闹往哪凑，因此直播行业成为黑客发动 DDoS 攻击的新目标。直播行业竞争激烈，其对业务的连续性要求非常高，如果发生 DDoS 攻击导致业务中断，将会导致大量用户流失，损失巨大。

3. 产品功能

网宿 DMS 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 DMS 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 DMS 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 DMS 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 DMS 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 DMS 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，DMS 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，DMS 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 DMS 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。DMS 单节点防护容量达 600Gbps，平台总体防护能力达 2Tbps+。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 DMS 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 1000 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：DMS 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：DMS 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。

DMS 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 DMS 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 DMS 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，DMS 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，DMS 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

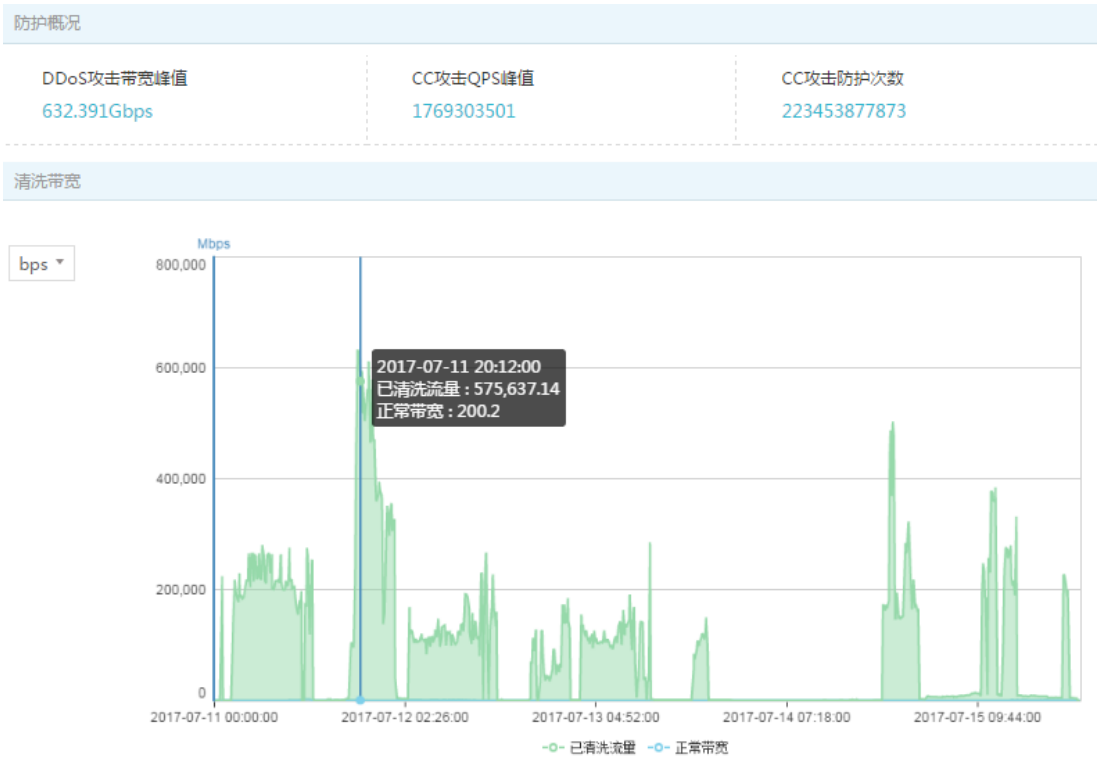
DMS 通过访问控制策略（如 IP 黑白名单、IP 访问速率等）、Cookie 校验等方式检测并拦截 POST Flood 攻击。

3.4. 防护数据可视化

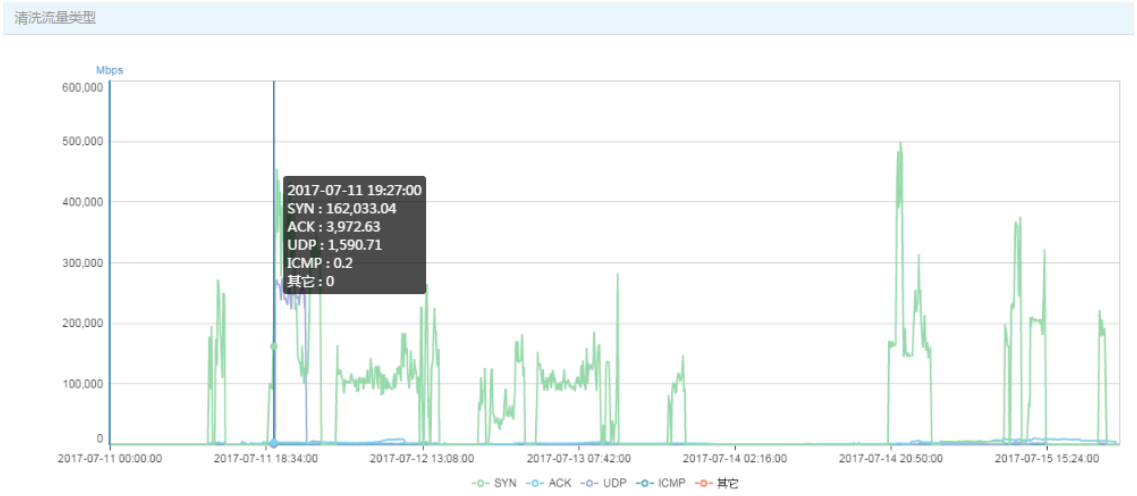
网宿 DMS 实时展示各类 DDoS 攻击的防护信息，客户可以实时查看防护效果，并根据攻击趋势了解网站的安全状态。

（1）展示网站防护概况，方便客户了解网站安全情况。

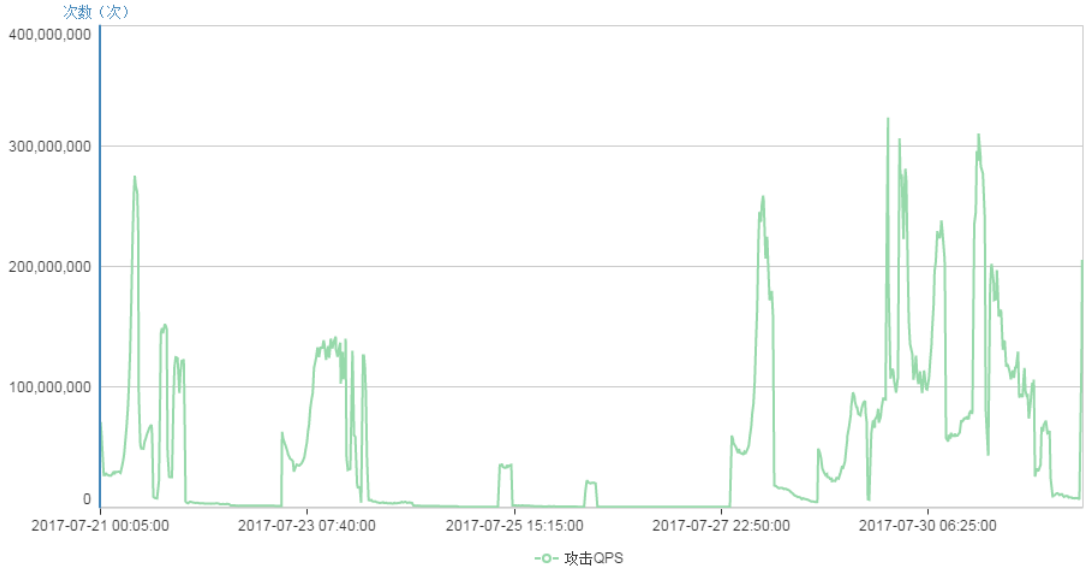
i. 某段时间内 DDoS 攻击带宽峰值，并实时展示清洗带宽和正常带宽。



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	[redacted]	土耳其Giresun/Giresun/TR	2017-07-24 09:58:00	[redacted]	拦截
2	[redacted]	堪萨斯/Kansas/US	2017-07-24 09:58:00	[redacted]	拦截
3	[redacted]	堪萨斯/Kansas/US	2017-07-24 09:58:00	[redacted]	拦截
4	[redacted]	堪萨斯/Kansas/US	2017-07-24 09:58:00	[redacted]	拦截
5	[redacted]	堪萨斯/Kansas/US	2017-07-24 09:58:00	[redacted]	拦截
6	[redacted]	堪萨斯/Kansas/US	2017-07-24 09:58:00	[redacted]	拦截
7	[redacted]	合肥/hefei/CN	2017-07-24 09:58:00	[redacted]	拦截
8	[redacted]	合肥/hefei/CN	2017-07-24 09:58:00	[redacted]	拦截
9	[redacted]	合肥/hefei/CN	2017-07-24 09:58:00	[redacted]	拦截
10	[redacted]	合肥/hefei/CN	2017-07-24 09:58:00	[redacted]	拦截
11	[redacted]	合肥/hefei/CN	2017-07-24 09:58:00	[redacted]	拦截
12	[redacted]	郴州/chenzhou/CN	2017-07-24 09:58:00	[redacted]	拦截
13	[redacted]	郴州/chenzhou/CN	2017-07-24 09:58:00	[redacted]	拦截
14	[redacted]	郴州/chenzhou/CN	2017-07-24 09:58:00	[redacted]	拦截
15	[redacted]	郴州/chenzhou/CN	2017-07-24 09:58:00	[redacted]	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
[illegible]	中国大陆	2,903,277	CC	2,903,277
[illegible]	中国大陆	1,861,101	CC	1,869,069
[illegible]	中国大陆	1,506,897	CC	1,506,897
[illegible]	中国大陆	1,443,708	CC	1,443,708
[illegible]	中国大陆	1,273,377	CC	1,272,811
[illegible]	中国大陆	1,268,493	CC	1,253,935
[illegible]	中国大陆	1,238,316	CC	1,237,685
[illegible]	中国大陆	1,166,932	CC	1,161,099
[illegible]	中国大陆	1,230,232	CC	1,158,568
[illegible]	中国大陆	1,143,267	CC	1,143,267
[illegible]	中国大陆	1,071,142	CC	1,055,668
[illegible]	中国大陆	1,061,660	CC	1,053,160
[illegible]	中国大陆	1,048,737	CC	1,041,812
[illegible]	中国大陆	1,030,447	CC	1,021,088
[illegible]	中国大陆	1,030,074	CC	1,020,881

4. 产品价值

4.1. 零部署、零维护

使用 DMS，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，即可享受专业的流量清洗服务。同时，DMS 能够基于服务质量智能调度服务节点，保证平台服务的质量和稳定性，真正做到零部署、零维护。

4.2. 弹性扩容，无谓突发大流量 DDoS 攻击

网宿 DMS 拥有多个大容量节点，目前单节点抗攻击能力可达 600Gbps，同时 DMS 的智能调度中心能够根据攻击情况智能调度全网资源，总体抗攻击能力达到 10Tbps+，当突发大流量攻击时，DMS 可以全力保障用户的业务不中断。

4.3. 最佳备份节点自动无缝切换，保证用户访问体验

网宿 DMS 为客户提供多组节点资源，一旦某个节点出现故障或被攻击到防护上限等情况，能够自动将该节点上的服务调度到最佳备份节点（尽可能同运营商同地区），不影响用户业务的访问体验。

4.4. 按需防护，降低企业成本

网宿 DMS 能够根据 DDoS 攻击情况按需提供服务，如突发大流量攻击则智能调度全网带宽资源为用户抵御攻击，攻击结束后能够智能调度走多余资源，可以有效避免传统硬件设备“买少了防不住，买多了闲置”的情况。同时也减少了购买安全设备（一台安全设备花费需 5-30 万，平均生命周期 3 年左右）与网络带宽（目前国内二线城市机房 10G 带宽大概是 150 万/年）的费用支出，以及减少了聘请专业安全运维团队的人力成本，大幅度降低了企业安全防御的成本。

4.5. 高效应急响应能力

网宿 DMS 提供专属安全服务团队为用户一对一的贴身服务，在突发大规模攻击时能够及时响应，并提供各项应急预案，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。