

动态加速 (DSA) 产品白皮书V1.0



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

网宿科技股份有限公司
版权所有 侵权必究

Content 目录

1. 产品&行业现状&挑战	4
2. 产品介绍	4
2.1. 产品简介	4
2.2. 产品技术架构.....	5
3. 产品功能	5
3.1. 动态传输加速.....	5
3.1.1.智能路由	5
3.1.2.私有传输协议	6
3.1.3.传输内容压缩	6
3.2. 可用性保障	6
3.2.1.多点覆盖	6
3.2.2.多源负载均衡	6
3.2.3.零时延切换	7
3.2.4.连接复用	7
3.2.5.有序回源	7
3.2.6.源站监控	7
3.3. HTTPS 优化	7
3.3.1.一键证书	7
3.3.2.无私钥驻留加速	8
3.3.3.双向认证	8
3.3.4.证书优选	8
3.4. 基础安全防护.....	8
3.4.1.数据传输安全	8
3.4.2.源站安全	9
3.5. 扩展功能更丰富.....	10
3.5.1.IPV6 与 IPV4 自适应	10
3.5.2.HTTP 2.0	10
3.5.3.Websocket	10

4. 产品价值	10
4.1. 显著提升访问体验.....	10
4.2. 基础有效的安全防护	11
4.3. 优质的服务保障.....	11

网宿 DSA (Dynamic Site Accelerator) 是由网宿科技自主研发, 针对动态交互网站的动态加速产品。通过动态路径优化、传输协议优化、数据库传输优化等私有尖端技术提升电子商务、SNS 社区、金融支付、游戏娱乐等含有较多动态内容的行业的网站业务。利用多项源站服务技术保障源站服务稳定, 在复杂拥堵的互联网环境下实现飞跃式的访问体验, 增加用户留存率。

1. 产品&行业现状&挑战



互联网经济最重要的特点是以用户为载体创造价值, 其最大的财富是用户规模和行为数据的积累。随着互联网带宽不断的提升以及 4G 的普及, 用户对网站的访问速度要求越来越高, 各行各业竞争激烈, 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。

相比于浏览图片和下载等传统业务, 动态交互数据需要与源站服务器频繁交互, 受限于骨干网传输、源站服务压力等诸多问题, 用户访问动态交互业务时更容易发生中断, 用户体验不佳, 容易打击用户信心, 直接影响业务收入。

然而在实际业务流程中, 网站受到极大的用户体验压力: 用户分布广、跨网传输延迟严重造成网站加载速度慢; 网络波动不能及时避免、突发访问、机器设备宕机问题带来服务稳定性压力; 恶意请求、网站劫持现象频发影响网站安全。在各行各业竞争激烈的前提下, 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 DSA (Dynamic Site Accelerator), 即网宿自主研发的动态网站加速产品, 本产品针对动态交互内容网站设计, 通过路由优化、传输优化、数据库优化等私有尖端技术大幅度提升访问速度, 利

用多项源站服务技术保障源站服务稳定，并支持 WAF、HTTPS 加密等全面的安全防护技术保障数据安全，实现用户体验飞跃提升，是全网、全球领先的高速、稳定和安全的动态交互内容加速解决方案。

2.2. 产品技术架构



DSA 基础架构

网宿 DSA 动态网站加速产品在全国部署专用的服务器组成加速平台，用户请求通过网宿全球负载均衡中心解析接入网宿 DSA 加速平台，通过网宿动态传输加速技术，快速实现与源站交互获取内容，提升用户访问体验。

3. 产品功能

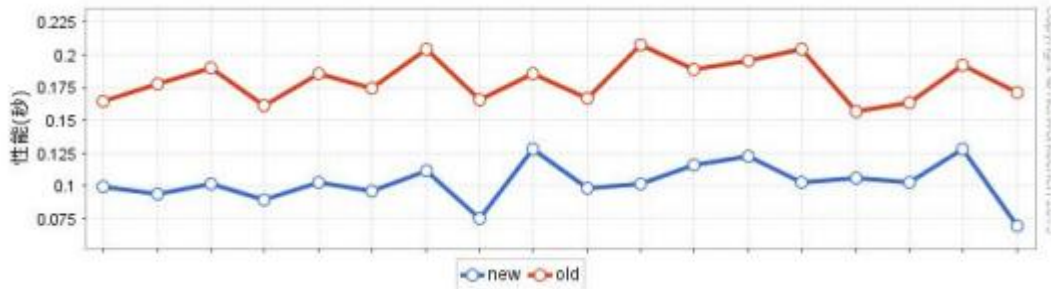
3.1. 动态传输加速

3.1.1. 智能路由

公网默认路由存在偶发故障、低连通、高延时的问题，严重影响请求的响应速度，使用户请求的服务质量不能得到很好的保证。网宿自主研发了智能路由技术，通过对互联网路由进行智能探测，实时掌握网络变化，结合人工智能算法智能地避开公网故障或目前正在拥堵的路径，自动选择节点到源站总耗时最短、稳定性最好的路径回源。有效解决运营商互联互通问题，实现平滑跨网，提升访问速度，保证数据的最佳传输效果，解决传输路径过长、网络质量不稳定问题。

3.1.2. 私有传输协议

网宿自主研发传输协议，该协议基于传统的 TCP 传输协议做改善，实现快速和稳定地传输数据，实际测试常规动态文件提升比例为 30% 至 130%。



私有传输协议加速效果图

3.1.3. 传输内容压缩

针对高并发小文件的动态应用场景，通过传输内容压缩技术对网络中传输的数据进行压缩，可以有效地减少网络传输的字节数，缩短传输时间，让应用数据更快地交付。

3.2. 可用性保障

3.2.1. 多点覆盖

DSA 平台会储备足够的冗余资源应对线上的突发情况，对每个区域使用多个节点进行覆盖，当所使用的节点发生异常不适合再继续服务时，系统会自动切换到其它可用的节点进行服务覆盖，保证服务的连续性，不影响用户访问。

3.2.2. 多源负载均衡

当企业有多个源时，DSA 节点可以按照各源的承受能力，按照一定比例到各源进行请求，当多个源分布在不同的地区，不同地区的节点可以回不同地区的源，如果有个别源站出现故障将自动剔除坏源。

3.2.3. 零时延切换

当企业个别源站出现问题无法提供服务时，将导致一部分用户无法访问，造成客户流失，不利于树立网站良好的品牌形象。零时延切换功能可以及时屏蔽故障源，自动切换到其他源来获取资源，切换无任何时延，平滑过渡，不会影响到终端用户访问。

3.2.4. 连接复用

利用 CDN 节点接收用户连接，再根据实际请求进行回源，例如 100 万个连接，实际连接数仅 10 万，减低源站 IO 消耗，缓解源站压力。

3.2.5. 有序回源

针对短时间内访问突增的情况，有序回源功能可对服务器回源请求的最高连接数设置阈值，如果所有源站负载均已达到上限、回源请求超出阈值，按发出请求时间先后有序排队等待回源。可以按用户优先级、区域优先级以及文件优先级排序，以避免源站宕机。

3.2.6. 源站监控

普通的源站监控：采用监控 URL 对源站服务状态进行监控。

高级源站监控：源监控可以实现 4 个层面的监控：客户的源站设备是否宕机进行监控、源站网络情况是否异常监控、源站 HTTP 服务是否异常进行监控、源站域名 DNS 解析过程是否异常进行监控，并可以灵活进行邮件及短信报警。

3.3. HTTPS 优化

3.3.1. 一键证书

网宿提供一键证书极速申请，申请下来的证书会自动部署到网宿的 CDN 节点上并生效，省去了人工申请证书及人工部署证书的的繁琐流程，企业客户可以极速体验和接入网宿的 HTTPS 加速服务。

3.3.2. 无私钥驻留加速

针对安全审核比较严格，不方便提供证书私钥给 CDN 厂商，但同时又有 https 加速需求。网宿科技支持无私钥驻留加速功能，将私钥解密的操作从 SSL 握手中分离出来，交由专门的私钥服务器来处理。客户拥有私钥服务器的管理权而无需将私钥交由 CDN 厂商。

3.3.3. 双向认证

网宿提供“用户-CDN 节点”和“CDN 节点-源站”两端双向认证功能，全方位保障业务和源站安全。

3.3.4. 证书优选

ECC 证书具有诸多优势：安全性高：256 位的 ECC 和 3072 位的 RSA 具有相同的加密强度；加解密速度快：HTTPS 请求速度提升 25%~35%；CPU 占有量少：使用 ECC 的占有率相比使用 RSA 降低 40%~60%。但是目前 ECC 证书的兼容性要差一些，下图是可以使用 ECC 证书的浏览器。

客户端环境		版本号	客户端环境		版本号
操作系统	Windows	Vista+	浏览器	IE	7+
	MacOS	10.6+		Firefox	2.0+
	IOS	7+		Chrome	1.0+
	Android	4.0+		Safari	4+

网宿提供证书优化功能，在 CDN 节点部署 RSA 和 ECC 两份证书，在 SSL 握手过程中，根据客户端对证书的支持情况，选择最适合的证书，以达到更好的服务效果。

3.4.基础安全防护

3.4.1. 数据传输安全

防盗链	Referer 防盗链：针对不想被引用的文件，可以设定只有特定的 Referer 才可以引用； Cookie 防盗链：设定请求中 Cookie 包含某个关键字才可以访问； 时间戳防盗链：基于请求中携带的时间戳进行过期验证； 回源验证：每个请求都回源进行验证访问合法性。
防篡改	基础防篡改：在 CDN 网络内部加密传输，节点间进行内容一致性验证工作；

	高级防篡改：除了内部加密传输，在源站和 CDN 之间的采用定制化验证和加密传输。
防劫持	<p>DNS 防劫持：对于有客户端的客户，采用 HTTP 的方式传递解析结果，避开 DNS 层面的拦截。</p> <p>内容防劫持：1. URL 加密（源站配合）：通过对 URL 进行一定形式的加密可以避免劫持的发生。 2. URL 高级加密（源站无需配合）：当源站无法配合并且非 APP 客户端访问的情况，由于源站和客户端无法根据协商的加密算法进行加解密，所以 CDN 单边加解密。 3. 请求加密（HTTPS 加速）：请求加密方案，即 HTTPS 加速解决方案。</p>
爬虫引导	<p>对于常规的搜索引擎爬虫，网宿通过智能 DNS 解析，在 DNS 层面去做判断，在 DNS 解析环节就分离了爬虫。目前网宿有精准的蜘蛛 IP 库，包含了各类蜘蛛库如百度、google、Bing、搜狗。</p> <p>对于搜索引擎的正常爬虫，网宿采用专门的节点进行覆盖，客户亦可以选择将爬虫请求回源处理，不经过 CDN。网宿还支持通过 IP 访问控制、智能黑白名单来屏蔽访问爬虫。</p>

3.4.2. 源站安全

源站隐藏	网宿提供高防 IP 节点，帮助企业隐藏源站，当黑客发起攻击，DSA 节点可快速启用安全策略，保障应用网站服务器安全。
IP 名单	IP 黑白名单可以有效防止恶意用户的行为对网站造成损失。可以设置限制允许或不允许某些 IP 段访问，或将 IP 放入黑名单中，并设定锁定的时间周期，在该周期内，IP 的访问都会被拦截。
URL 黑白名单	支持将特定的 URL 加入黑白名单，黑客常常会构造跟普通用户访问很相似的 URL 但又不完全一致，往往只有一个字符之差，DSA 可以根据这一特征，将指定的或者符合某类特征的 URL 加入访问黑名单。
整体带宽防护	针对客户的单个域名或者多个域名集合进行整体带宽的实时监控与防护，设定带宽报警阈值与防护阈值。当带宽值超过报警阈值时，进行邮件、短信报警，当带宽值超过防护阈值时，则根据事先设定的防护策略进行防护；
区域访问限制	黑客有时候有地域特征，比如黑客 IP 都来自某个国家或者地区，若网站的正常的访问用户很少来自该国家或者地区时，则可以针对这些国家或者地区进行限制访问。

3.5. 扩展功能更丰富

3.5.1. IPv6 与 IPv4 自适应

第二代互联网 IPv4 技术网络地址资源有限，IP 地址已于 2011 年 2 月分配完毕，于是 IPv6 应运而生。随着全世界 IP 需求加大，IPv6 地址越来越普遍，这就要求直接面向用户的服务器需要能同时应对 IPv4 与 IPv6。当客户端采取 IPv4 或 IPv6 方式访问，而源站不能同时支持时，网宿 DSA 可提供自适应协议转换方法，在无需源站提供额外支持的情况下，保证用户不论 IPv4 或 IPv6 方式的访问都能正常访问。

3.5.2. HTTP 2.0

网宿率先开发支持 HTTP2.0 协议，HTTP2.0 通过压缩头部减少传输内容，利用多路复用技术降低请求连接数和减少页面阻塞，降低服务器和网络的负载同时实现访问速度飞跃提升。

3.5.3. WebSocket

网宿 CDN 通过支持 WebSocket，使浏览器具备像 C/S 架构的实时通讯能力，服务器也能向浏览器推送数据。实时推送使股票行情、SNS 社区互动、游戏等更加快捷，提升用户访问体验。

4 产品价值

4.1. 显著提升访问体验

在目前国内众多的 CDN 加速厂商中，网宿 DSA 加速综合性能首屈一指，加速后网站的响应速度、成功率、源站资源使用都得到较大的优化。DSA 覆盖全国高性能节点，覆盖全国大小运营商，在大幅度提升用户体验增加用户黏性的同时，有效降低了客户源的负载，保障服务稳定性。

4.2. 基础有效的安全防护

网宿 DSA 动态网站加速支持访问控制、黑白名单、整体带宽防护、防篡改、防盗链等多种防护手段按需使用，保障网络数据安全，保证服务稳定进行，DSA 的 HTTPS 加密实现了证书部署无需人工介入、双向认证、证书优化等功能，大幅提升安全防护，确保了数据安全。

4.3. 优质的服务保障

网宿强大的运营保障体系，为网站提供 7*24 小时的售后监控服务。网宿专业的技术支持团队，提供优质售前售后服务，保证网站稳定运行。



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。