HTTPS加速 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

Content 目录

网宿 HTTPS 加速产品，致力于解决数据传输安全问题和加速数据访问，多年来不断自我优化和革新，深耕业务场景，为客户提供给卓越的 HTTPS 加速服务。

1. 行业挑战

HTTPS（全称：Hyper Text Transfer Protocol over Secure Socket Layer），安全的超文本传输协议，是以安全为目标的 HTTP 通道，俗称：HTTP 的安全版。HTTPS 协议利用证书的信任机制建立双方信任通道，数据的交互采用 SSL 加密，不仅能够有效的加强数据传输的安全性，同时也让用户访问数据的可靠性得到保障。

在数据安全日益重要的今天，HTTPS 完美的契合了企业数据安全的需求。同时，在谷歌、苹果等科技巨头的对 HTTPS 的大力扶持下，全网普及 HTTPS 的时代正在铺展开来。

- **HTTPS 的性能消耗远高于 HTTP**

HTTPS 在保障数据安全的同时，也对网站的服务性能产生了巨大的冲击，在未经过加速的情况下，使用 HTTPS 比使用 HTTP 的对于的服务器性能消耗增加 20%。同时，HTTPS 的请求时延是 HTTP 的 200%。在互联网用户体验为先的时代里，这样的性能消耗对于企业发展来讲无疑是致命的打击。

- **流量劫持已成为行业难题**

在当前的互联网环境中，流量劫持成为一种随处可见的现象。流量劫持的危害有：在用户界面上植入弹窗或广告，影响用户体验，导致用户流失；流量劫持原有广告被替换成其他信息，直接给企业带来经济损失；互联网公司每年都会投入大笔资金资源去获取流量，但由于劫持，用户正常流量被伪装成了渠道流量，导致投入的资金都被嫁接到做劫持的渠道中。

- **IPv4 资源即将消耗殆尽**

早在 2011 年，全球 IPv4 的地址资源已经分配完毕，资源消耗步入倒计时阶段。传统的 HTTPS 加速服务，需要把证书与 IP 地址一一绑定，加快了 IPv4 的资源消耗。然而对于中小运营商而言，它们所拥有的 IP 地址资源少，可对外提供的 IP 地址有限，最终导致在加速服务的资源覆盖上，覆盖较差，加速效果无法达到最佳的预期。

◆ **证书安全**

证书是使用 HTTPS 加密传输的核心基础，证书包括私钥与公钥，公钥是对外公开的，私钥是不对外公开的，具有唯一性。因此，私钥的存放是否安全，直接关系着互联网数据传输的安全性。在加速服务和证书安全的选择上，企业往往采用舍弃用户体验的方式来确保证书的安全。

2 产品介绍

2.1 产品简介

使用 HTTPS 加密后，数据在传输的过程中，从源站服务器的性能、证书加密位数、互联网链路状况等因素都会直接或间接影响到终端用户的访问体验。HTTPS 加速产品通过优化其加解密机制，采用全平台硬件加速策略，多方位提升数据传输效率，针对动态数据实现全网加速、静态数据边缘响应获取、动静混合数据智能分离加速，提升终端用户的访问体验，为企业业务创收提供全面加速服务。

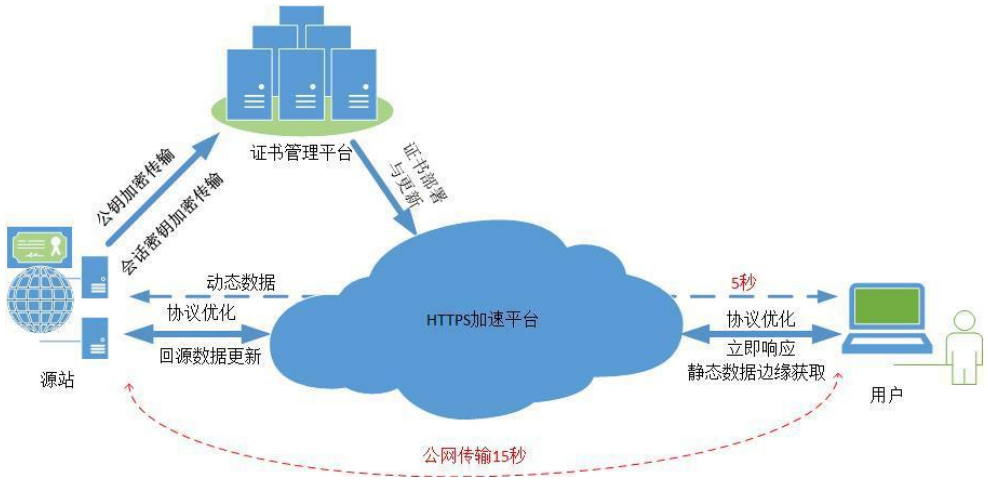

图 2-1-1 HTTPS 加速原理图

2.2 目标行业

网宿 HTTPS 加速服务适用于当前市面上可使用 HTTPS 的网站，主要应用于电商、政府网站、金融网站等行业，包含但不局限于 3-2 表的内容。

行业	电子商务	企业信息化	网络游戏	信息交流	金融网站	网络服务	企业政府
适用场景	机票酒店	ERP	在线游戏	SNS	网上银行	网页邮箱	政府网站
	网站预订	SAP	网页游戏	论坛	金融门户	网络招聘	外企门户
	网络购物	CRM	休闲游戏	虚拟社区	基金证券	网络教育	传媒网站
	团购网站	OA	对战平台	微客微博	网络炒股	信息查询	

表 3-2：HTTPS 应用行业细分

3 产品功能

3.1 HTTPS 动态加速

DAA(Dynamic Application Accelerate)动态应用加速技术。创新性的对动态资源进行加速，借助路由优化、私有传输协议两项核心动态加速技术对动态回源访问进行加速，并辅以页面优化、数据库传输优化等多项高级技术，显著提高互联网站的动态服务质量。

3.1.1 智能路由，实时调度

针对公网默认路由存在偶发故障、低连通、高延时等问题，网宿自主研发的智能路由技术，结合人工智能算法获取性能最优的访问路径，有效避开网络拥塞、实现平滑跨网，保证数据传输的最佳效果，提升用户体验。

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%。

3.1.3 压缩传输，提高效率

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 HTTPS 静态加速

3.2.1 层级收敛，冗余备份

HTTPS 静态加速，采用层级收敛方式。访问热度较高的静态资源一般会缓存在边缘节点，而对于访问热度较低的冷资源，传统加速方案是回到源站获取，无法最大化降低源站的负载压力。针对不同区域，不同运营商，资源的访问热度也不同，造成节点缓存的资源差异较大，节点静态资源缓存的差异性，导致用户的访问体验存在巨大的差异。同时也会因冷文件回源获取的数量增加而导致源站负载过大。

3.2.2 个性操作，定制缓存

互联网应用对资源的定义日趋多样化，以传统的方式去定义静态资源，已经无法满足当前互联网业务的个性化发展。HTTPS 加速产品提供了定制化的缓存服务。 HTTPS 加速产品根据对资源更新需求的不同，提供两种不同的更新模式：

主动更新：对于文件更新频繁的客户，可使用网宿提供的 API 接口或通过内容管理界面对缓存在全国各地节点服务器上的文件或目录进行快速强制更新，迅速将内容更新到全网，以避免更新后大量回源导致流量暴增问题。

被动更新：被动更新由用户请求触发，当用户请求的文件在节点上已经缓存过期，此时节点与源站进行更新判断，若文件未更新，节点直接响应用户请求，同时刷新缓存时间；若文件更新，则请求回源，节点响应用户同时缓存到本地，以保证用户能及时的访问到最新内容。

3.3 HTTPS 全站加速

互联网应用中，有一些应用资源是采用动静态资源混合的方式，传统的加速服务会要求把动静态混合资源进行域名拆分加速，无法实现在单域名全站加速。

HTTPS 加速产品将动静态内容自动分离，针对动态资源采用智能路由、冗余压缩等方式进行全网加速。静态资源采用边缘响应获取、层级收敛等方式，达到最佳的缓存效果。源站无需做任何的拆分域名，即可实现全站 HTTPS 加速。

3.4 HTTPS 加速保障技术

HTTPS 加速产品在提升用户访问体验的同时，结合多项服务技术，不仅从技术、资源、安全、源站稳定等多方面保障客户的服务效果，而且多方位、多角度地保障业务正常运行，为企业提升行业竞争力提供强有力的保障。

3.4.1 应对突发，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阀值，如果所有源站负载均已达到上限、回源请求超出阀值，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。

3.4.2 共享 IP 服务，突破瓶颈

传统 HTTPS 加速方案里一套证书智能单独绑定一套 IP，导致 HTTPS 加速时，覆盖的资源节点会因为 IP 地址的问题而受到限制。网宿提供的 HTTPS 加速产品支持 SNI 方案，该方案能够有效的解决因 IP 地址匮乏而导致节点运营商覆盖不全面的问题。

SNI(Server Name Indication)，它允许客户端在服务器端向其发送证书之前发送域名给服务器，这使得服务器可以在 SSL 握手阶段就知道域名。实现多个 HTTPS 客户可以共享同一个 IP 地址，解决了资源匮乏而导致覆盖不全的问题，最大化的提升了资源覆盖率。

3.5 HTTPS 优化特性支持

3.5.1 TLS 会话复用

TLS 会话复用，CDN 可以通过特定的标识记录用户对域名的访问情况，在指定的时间里(可配置)，当用户再次访问同一域名时，即可通过标识直接与服务器建联，省去了重复的 TLS 握手过程。极大程度提升用户的访问速度。

3.5.2 False Start

传统的 HTTPS，客户端必须等待 TLS 握手完全完成后，才能向服务端发送 HTTP 请求报文，这样的串行方式，增加了 HTTPS 的请求时延。False Start 优化了原有的形式，在 TLS 握手未完全完成时，就异步发送 HTTP 请求报文，节省了约 25%的 TLS 握手时延。

3.5.3 HSTS 强制 HTTPS 请求

在传统 HTTPS 请求过程中，当在浏览器输入网址时，一般情况下浏览器默认发起的是 HTTP 请求，需要经历由 HTTP 请求 302 跳转至 HTTPS 请求的过程，由于跳转过程中信息都是明文的，存在被攻击的风险。HSTS 优化要求用户访问指定域名时，浏览器强制发起 HTTPS 请求，避免了被攻击的风险，且节省了 302 跳转时间。

3.5.4 OCSP Stapling

在 TLS 我握手过程中，证书会携带用于通信对象校验该证书合法性的 URL， 每一次 TLS 握手都要向 OCSP 的服务器发起一次校验请求。OCSP Stapling 方式，由服务器预先将证书的合法性的校验结果缓存在服务器上，当客户端发起 HTTPS 请求时，将检验结果连同证书一起发送给服务端。避免了大量不必要的性能消耗和请求时延。

4 产品方案

4.1 HTTPS 无缝加速，源站无需改动

HTTPS 无缝加速方案，全程采用加密传输部署，从证书的获取到平台的部署，只有用户平台管理员才能够直接接触到私钥，部署人员只能通过部署平台，通过下发策略的方式来实现 HTTPS 加速服务部署。其中部署人员无法直接接触证书，避免因第三方人员接触而造成私钥泄漏的潜在风险。

4.2 回源 HTTP 安全加速，全网加密访问

如何实现在不改变源站继续使用 HTTP 协议服务模式的前提下，又能实现用户访问数据加密传输。回源 HTTP 安全加速方案，通过在 CDN 平台部署 HTTPS 加速方案，终端用户通过访问边缘节点，建

立 HTTPS 链接，进行加密传输。CDN 节点与源站采用双方协商的特殊机制回源，确保数据来源的可靠性。

4.3 一键证书申请，高效自动化部署

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。

4.4 HTTPS 双向认证，安全保障无隐患

HTTPS 双向认证，不仅客户端能验证服务器的身份，而且服务器也能验证客户端的身份，业务安全保障性更强。HTTPS 双向认证分为“用户和 CDN 的双向认证”和“CDN 和源站的双向认证”：

用户和 CDN 双向认证：当前绝大多数 HTTPS 为单向认证，即用户可以验证服务器的身份，服务器无法验证浏览器的身份。然而，在某些特定的场景，服务器需要验证用户的身份，以确定该用户是否为服务器所要服务的目标对象。如：某公司提供给合作商使用的系统网站，如果不是目标用户则无法访问该网站，确保网站的业务安全性；

CDN 和源站双向认证：源站验证 CDN 的身份，不是来自 CDN 的请求则拒绝访问，有效提高源站的安全性。

4.5 HTTPS 无私钥驻留加速，私钥源站唯一持有

对于监管要求十分严格的客户来说，对外是无法提供私钥的。如何能够在不对外提供私钥的前提下，实现加速服务。HTTPS 无私钥驻留加速方案，客户无需提供私钥，在源站唯一持有的情况下，只需在源站中部署安全加速模块，即可实现业务的加速服务。 HTTPS 无私钥驻留加速具有如下特点：

- 客户对私钥具有绝对掌控权，保障私钥安全；
- 融合了网宿多项尖端加速技术：智能路由选路、私有协议优化、全路径支持 HTTPS2.0 等，保障了 HTTPS 请求性能最优；
- 在安全层面，配备了抗 DDos 服务、HTTPS 双向认证，保障业务安全更上一层楼。

4.6 HTTPS 证书优选，访问速度更上一层楼

网宿证书优选方案，在 CDN 上分别部署 ECC 和 RSA 证书，根据客户端对证书的支持情况，优先匹配 ECC 证书，以达到更优秀的服务效果。

随着浏览器的不断更新及对 ECC 证书的支持，ECC 证书作为一种使用性能相对优秀的证书，开始受到广泛的关注，2014 年 ECC 证书在国外被普遍开始使用，2015 年国内开始接受 ECC 证书。在客户端支持 ECC 证书情况下，优选 ECC 证书具有如下优势：

(1) 安全性高：256 位的 ECC 和 3072 位的 RSA 具有相 同的加密强度。

(2) 访问速度快：有 ECC 证书的 HTTPS 请求速度提升 50%+。

(3) CPU 占有率小：使用 ECC 的 CPU 占有率相比使用 RSA 降低 30%~60%。

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。