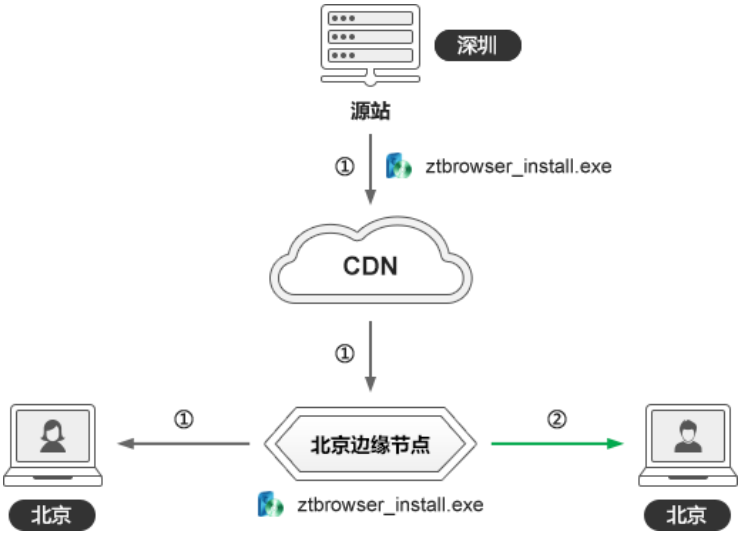
一文讲清 HTTP 回源和 HTTPS 回源

无论是 CDN 服务还是 WAF 防护服务，以及零信网关提供的 HTTPS 加密自动化服务都是采用反向代理技术实现，都涉及到回源这个概念，本文讲清回源的原理和如何正确配置回源参数，以便 CDN 用户、WAF 用户和零信网关用户能正确设置回源方式和回源参数，确保全链路的 HTTPS 加密的实现，切实保障数据流通的全程传输安全。

一、 什么是回源？

要回答这个问题，则先讲一件什么是 CDN。CDN 是内容分发网络(Content Delivery Network)的英文缩写，由位于不同区域的边缘服务器组成的分布式内容分发网络，将源站资源缓存到各地的边缘服务器上，供网站访问者就近获取，降低源站压力和快速为用户提供源站内容。最适合于 CDN 的内容是各种下载文件、音乐文件和视频文件等静态文件，当然，现在的 DCDN 已经支持动态请求，为各种资源提供动静态加速和防护。

回源就是指 CDN 节点从源站获取网站访问者的请求数据后返回给网站访问者的过程。CDN 会按照设定的时间缓存这个数据，下一个访问者希望获取同一资源时就不再去源站获取，可以直接从边缘节点给用户所需的资源，以达到用户可以就近快速获取数据的目的。简单来说，就是当用户请求的数据在本地 CDN 节点服务器上没有或者需要更新时，节点服务器会回到原始的数据源去获取数据，这就是回源。如下图所示，第一个下载零信浏览器的北京用户需要 CDN 北京节点从深圳源站去获取后再返回给用户，下载速度会慢些，而第二个北京用户就直接从 CDN 北京边缘节点获取，下载速度就很快了。



二、 什么是回源协议？HTTP 回源和 HTTPS 回源有什么不同？

回源协议指 CDN 节点向源站请求资源时使用的协议，常用的协议就是网站访问的 HTTP 协议和 HTTPS 协议，同时可以指定回源端口，如 HTTP 协议默认端口为 80 端口，HTTPS 协议默认端口为 443 端口。CDN 节点会根据用户设定协议和端口回源到源站请求资源。

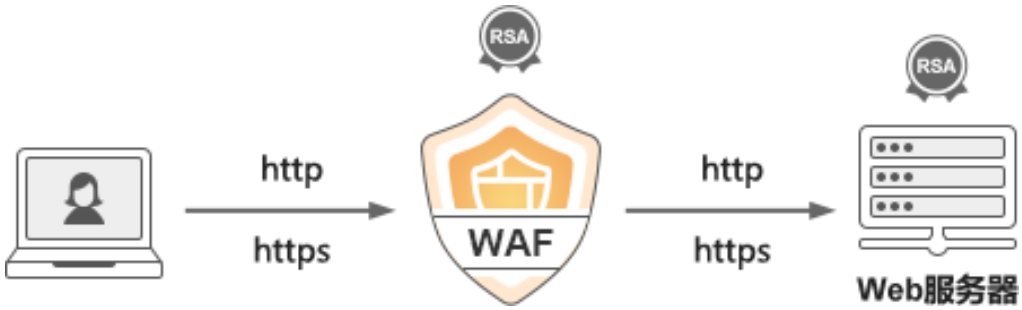
如下图所示，如果使用 HTTP 协议去回源源站资源，则称之为 HTTP 回源。这是全程明文传输方式回源和用户访问，机密数据非常容易在传输过程中被非法窃取和非法篡改，无法保障数据在传输过程的安全。所以，所有浏览器都会显示为“不安全”。但是，现在仍然有大量政府网站都在使用 HTTP 方式的 CDN 服务和 WAF 服务，这是非常不安全的方式，也是不符合等保和密评要求的保障网络传输安全的方式。四部委发布并于 7 月 1 日施行的《互联网政务应用安全管理规定》就明确要求政府网站和政务服务系统都必须采用 HTTPS 加密方式实现安全连接和使用 HTTPS 加密方式的 CDN 服务。

而如果使用 HTTPS 加密协议回源源站资源，则称之为 HTTPS 回源。HTTPS 回源需要源站也支持 HTTPS 协议，也就是源站必须配置了 SSL 证书，能用 HTTPS 方式访问。当然，从用户端到 CDN 节点也必须采用 HTTPS 协议，也就是 CDN 边缘服务器上也必须部署 SSL 证书，只有这样才能实现全程 HTTPS 加密方式传输网站机密数据，全程保障网站数据安全。

由于 HTTPS 回源要求源站必须部署 SSL 证书，这就要求用户向 CA 申请 SSL 证书，不仅必须配置 SSL 证书到源 Web 服务器上，同时要求用户上传 SSL 证书到 CDN 系统中，这个过程非常麻烦。所以，大量的网站都是采用 HTTP 回源方式回源，虽然用户访问时浏览器会显示

加密锁标识，但是从 CDN 节点服务器到源站之间仍然时 HTTP 明文传输，仍然不安全，机密数据仍然有可能被非法窃取和非法篡改。

对于 WAF 防护，也是采用 CDN 一样的反向代理转发技术，也有 HTTP 回源和 HTTPS 回源之分，也有用户是 http 方式还是 https 方式访问网站之分，如果 WAF 设备或 WAF 云服务不支持 HTTPS 加密，则是不安全的 HTTP 明文方式访问网站。而如果 WAF 设备或云 WAF 服务支持 HTTPS 加密，则必须在 WAF 设备或云 WAF 服务上部署 SSL 证书，如果同时必须支持 HTTPS 方式转发，则要求 Web 服务器也必须部署 SSL 证书，支持 HTTPS 加密。为了保障网站机密信息传输安全，所有 WAF 设备或云 WAF 服务都必须支持 HTTPS 加密。而依据相关法律和文件规定，必须支持商密算法 HTTPS 加密。



三、 零信网关支持哪些回源方式？有何特别之处？

通过上一部分对 CDN 服务和 WAF 服务的了解，我们知道，必须实现全程 HTTPS 加密才能保障网站机密数据的全程传输安全，也就是 CDN 节点服务器和源站 Web 服务器都必须部署 SSL 证书，要求 WAF 设备和 Web 服务器都必须部署 SSL 证书。但是，申请和部署 SSL 证书是一件非常困难的事情，特别是必须部署国密 SSL 证书就更难了。

零信网关，包括国密 HTTPS 加密自动化网关和国密 WAF 自动化网关，也是采用 CDN/WAF

服务器一样的反向代理转发技术实现，也需要回源到源 Web 服务器，不同的是支持自动化配置双算法 SSL 证书实现 HTTPS 加密，双算法自适应加密。

所以，零信网关在设置时也需要设置回源信息，也需要设置回源协议和回源 HOST。其中回源 HOST 就是网关发起回源请求时携带的 HOST 请求头默认为 HTTPS 交付网站的域名，以便源 Web 服务器可以根据 HOST 来正确回源源站内容，这对于一台 Web 服务器设置了多个站点是必须的，否则可能无法回源到正确的源站点。零信网关支持域名回源和 IP 地址回源，如果是 HTTPS 交付网站域名同源站域名不一致，则可能需要关闭回源 HOST。如果采用 IP 地址回源，并且此 IP 上有多个网站，则必须启用回源 HOST，以便源 Web 服务器能正确识别用户要访问哪个网站而实现正确回源。

无论是 CDN 还是 WAF 都需要支持 HTTPS 加密(用户访问或者回源)，都要求用户向 CA 申请 SSL 证书上传到 CDN 系统或 WAF 系统中，同时还需要部署在源 Web 服务器中，并且是每年必须处理一次，每个网站都必须处理一次，这对于有成百上千个、甚至上万个网站系统需要部署 CDN/WAF 服务的大型机构，是一个非常大的工程，需要投入大量的人力成本，而不仅仅是 SSL 证书费用。而零信网关的最大创新在于自动化为网关配置双 SSL 证书实现 HTTPS 加密自动化和 WAF 防护自动化，并且是一站一密钥的方式，而不是各个网站常用的通配证书共享同一密钥的不安全方式，用户无需向 CA 购买和申请 SSL 证书，无需人工手动部署 SSL 证书，也无需安装 ACME 客户端软件，最多支持 255 个网站 5 年不间断的自动化配置双算法 SSL 证书(国际 SSL 证书和国密 SSL 证书)。

对于 HTTPS 回源，如果原网站已经实现 HTTPS 加密，则可以直接使用这张 SSL 证书实现 HTTPS 回源，而这张 SSL 证书可以一直用于回源而不再需要更新，即使这张 SSL 证书已经过期也没有问题。对于原网站没有 SSL 证书的情况，如果 Web 服务器是直接连接到网关的内网网卡(共 4 个千兆电口和 4 个万兆光口可用)，则可以采用 HTTP 回源，原 Web 服务器无需安

装 SSL 证书。而对于 Web 服务器无法物理连接网关内网网口，则可以通过内部网络或者通过互联网来实现 Web 服务器的回源，强烈推荐采用 HTTPS 回源，但用户仍然无需向 CA 申请 SSL 证书，网关免费提供 5 年有效期的回源专用 SSL 证书，在设置 HTTPS 交付网站域名后就可以下载回源专用证书，部署在源 Web 服务器中，可以长期专用于 HTTPS 回源，以保障网站机密信息传输的全程加密安全。

一样的回源转发技术，不一样的是 HTTPS 回源和 HTTPS 访问的 SSL 证书自动化，零信网关这个创新特点不仅实现了 HTTPS 加密自动化，也同时实现了 WAF 防护的 SSL 卸载自动化，不仅支持国际算法 HTTPS 加密，而且同时支持商密算法 HTTPS 加密，这才是用户所需的网站安全服务，让用户尽享 HTTPS 加密和 WAF 防护的自动化带来的业务系统的安全可靠性和安全敏捷性的大幅提升，彻底解放宝贵的工程师人力资源，大大提升生产力和核心竞争力，切实保障核心数据资产的流通传输安全。

王高华

2024 年 7 月 15 日于深圳

欢迎关注零信技术公众号，实时推送每篇精彩 CEO 博客文章。
已累计发表中文 172 篇(共 47 万 3 千多字)和英文 68 篇(8 万 4 千多单词)。。