深度解读美国《联邦零信任战略》(二)：DNS 安全

美国联邦政府在两年前发布了《联邦零信任战略》，笔者当时专门写了解读文章-深度解读美国《联邦零信任战略》(一)：网站安全，建议读者在读这篇文章之前先读一下第一个解读，重点解读了 HTTPS 加密。本篇为第二个解读：DNS 安全。

一、 解读《联邦零信任战略》中对 DNS 安全的要求

先看看《联邦零信任战略》是如何要求联邦政府机构加强 DNS 流量安全的-加密 DNS 流量：联邦政府机构使用的 DNS 服务必须采用加密 DNS 协议(DNS-over-HTTPS 或 DNS-over-TLS)，并且必须使用加密协议与上游 DNS 通信，政府机构必须启用加密 DNS 以支持各种应用软件(如浏览器、管理软件)、操作系统级的加密 DNS 应用。这项任务必须在 2024 年财年完成。

> **2. Encrypting DNS traffic**
>
> Agencies must resolve DNS queries using encrypted DNS wherever it is technically supported. This means that agency DNS resolvers must support standard encrypted DNS protocols (DNS-over-HTTPS or DNS-over-TLS), and must use them to communicate with upstream DNS resolvers. Agency endpoints must enable encrypted DNS in supporting applications (for example, web browsers) and at the operating system level wherever these features are available.

原文只有 315 个单词，笔者总结有以下四个方面的重点内容：

(1) 所有政府机构的 DNS 都必须加密(must)，这是明确适用范围，是强制要求。

(2) 必须采用 DoH 或 DoT 标准来加密 DNS，这是明确技术路线。请注意：不是采用 DNSSEC 技术。

(3) 各种软件包括浏览器必须支持加密 DNS，这是明确哪些软件必须支持加密 DNS。

(4) 必须在 2024 财年完成这项任务，这是明确完成时间。

相信大家看了这个要求，一定会感觉非常简单明了，一目了然，明明白白。那么，美国《联邦零信任战略》为何要出台这个强制政策呢？本文第二部分将详细讲解 DNS 和加密 DNS 的来

龙去脉。

二、 什么是 DNS？什么是加密 DNS？

什么是 DNS？浏览器在使用 HTTP 或 HTTPS 访问网站时首先必须访问一个 IP 地址查询服务获得网站域名的 IP 地址，才能正常从这个网站获取网站内容，这个 IP 地址查询服务就是 DNS 服务。也就是说：我们日常上网一刻也离不开 DNS 服务，所以 DNS 安全至关重要，DNS 是 IT 可靠运营的基础，DNS 数据必须保护以免遭遇非法窃取和篡改。但是传统的 DNS 安全一般指 DNS 服务器的攻击防护，并没有更多的考虑到 DNS 数据的传输安全。

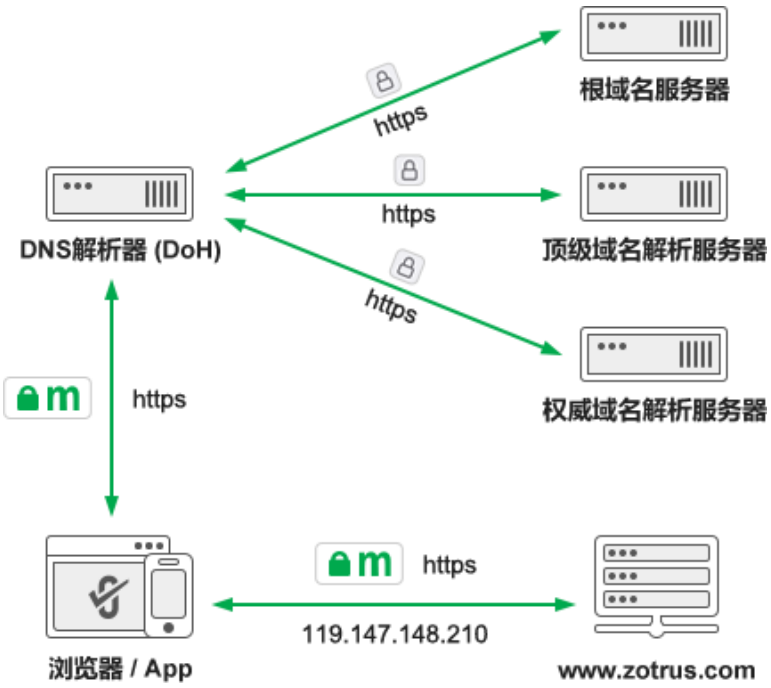
DNS 域名系统在 1983 年诞生时同后来诞生的 HTTP 服务一样都是明文传输协议，浏览器在查询 DNS 服务的 DNS 数据包是以明文方式在互联网上传输，任何人都可以查看甚至非常容易篡改这些域名解析数据(DNS 劫持)，这不仅仅影响到用户是否能访问正确的网站，而且非常容易泄露用户的互联网访问记录而泄露用户隐私。很遗憾的是，目前用户上网使用的 DNS 查询服务在 DNS 服务诞生 40 年后的今天仍然几乎 100%都是明文传输，而比 DNS 协议还要晚 6 年的 HTTP 协议已经实现了全球 90%以上流量的加密。那为何就没有实现 DNS 加密？

早在 1999 年就诞生了 DNS 加密技术-DNSSEC (Domain Name System Security Extension, 域名系统安全扩展)，但该技术的侧重点在于保证 DNS 响应的完整性（防止攻击者篡改响应内容），而非对 DNS 查询数据的传输进行加密。DNSSEC 虽然使用了数字签名技术来保证 DNS 数据的完整性，但是其缺陷是密钥管理太复杂，导致了这项技术并没有得到普及应用。DNSSEC 技术的缺陷可以简单地理解为其加密机制并没有利用完善的 PKI 体系，而是采用了很难管理的自签密钥实现 DNS 数据的数字签名。

随着 HTTPS 加密技术的普及应用，这个技术也就自然而然地用于保护 DNS 数据的传输安全，因为 HTTPS 是一个非常成熟的加密传输技术，可以高效地解决 DNS 数据的明文传输难题。这就是《联邦零信任战略》推荐的两个加密 DNS 技术：DNS-over-HTTPS (DoH) 和 DNS-over-TLS (DoT) 技术，这两个 DNS 加密技术都已经成为 RFC 国际标准，都是基于成熟的 PKI 密码体系的 SSL 证书实现 DNS 数据的传输加密。DoH 和 DoT 技术的不同点是前者基于非常成熟的 HTTPS 加密通道来加密 DNS 数据，而后者则采用了一个专用端口 853 和通过 UDP 协议实现 TLS/SSL 加密。

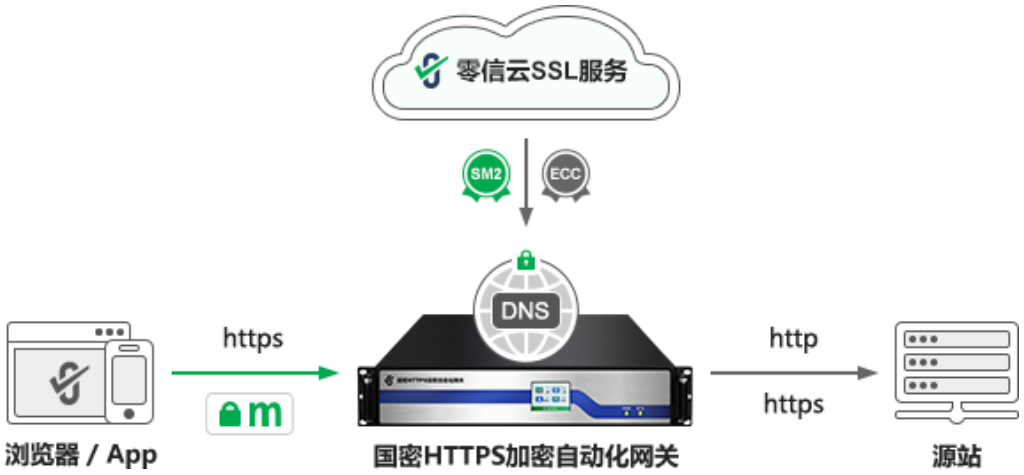
那么，DoH 和 DoT 两个加密 DNS 技术到底哪个更好呢？用户应该选择哪个技术来保护 DNS 安全？从网络安全的角度来看，DoT 技术由于使用了特定端口使得网络管理员能够监视和阻止 DNS 查询，这对于识别和阻止恶意流量非常重要。而 DoH 查询则隐藏在常规 HTTPS

流量中，这意味着，无法阻止恶意 DNS 流量。但是，从隐私保护角度来看，DoH 可以说是更好的技术。使用 DoH 时，DNS 查询隐藏在 HTTPS 流量，这虽然削弱了网络管理员的可见性，但增强了用户的隐私性。笔者倾向于使用 DoH 技术，因为它采用 HTTPS 加密技术，使得浏览器可以非常容易地集成 DoH 服务，也使得用于自动化证书管理 HTTPS 加密的各种解决方案都不用改造地支持加密 DNS 的自动化证书管理，这非常重要，特别是 SSL 证书的有效期即将缩短为 90 天后，自动化证书管理确保了加密 DNS 服务的持续不间断提供服务。



三、零信技术 DNS 加密解决方案

零信技术提供 HTTPS 加密自动化解决方案，而加密 DNS 是 HTTPS 加密上网的开始，只有先实现了 DNS 加密，再加上 HTTPS 加密，才真正实现了用户上网的全程加密安全，才能真正保护用户数据安全和保障互联网安全。DNS 加密和 HTTPS 加密缺一不可，这就是为何零信**国密 HTTPS 加密自动化网关**在最近的升级版本中集成了加密 DNS 服务，基于开源 Bind 9 DNS 服务系统，实现了自动化为 DoH 服务配置双算法 SSL 证书，同时自动化实现了国密 HTTPS 加密和国密 DNS 加密(SM2 DoH)，为用户提供一站式 HTTPS 加密和 DoH 加密 DNS 服务，这是零信技术 DNS 加密解决方案之一。



零信技术 DNS 加密解决方案之二就是零信浏览器支持 DoH/DoT 加密 DNS 服务，用户可以在“使用安全 DNS”菜单启用加密 DNS 服务，为用户上网浏览提供 DNS 加密服务，有力保障用户的上网隐私安全。零信浏览器今天发布了升级版本，在开源 Chromium 默认内置 4 个全球知名的加密 DNS 服务基础上增加了国内 4 个国内知名的加密 DNS 服务，推荐大家选用腾讯国密加密 DNS 服务-TencentDNS(SM2)，这是目前笔者发现的唯一一个采用国密算法实现的加密 DNS 服务(DoH)，选用此国密加密 DNS 服务后，零信浏览器会自动采用国密算法加密 DNS 信息，实现国密 DNS 加密和国密 HTTPS 加密的全程上网安全国密保护。

四、安全上网从使用加密 DNS 开始

从用户在浏览器地址栏输入网站域名开始，DNS 解析器就开始了从域名到 IP 地址的翻译工作，并把查到的 IP 地址通过 HTTPS 加密通道返回给浏览器，浏览器就可以访问网站获取网

站内容了。从这个加密 DNS 服务的工作原理可以看出：加密 DNS 服务实现了 DNS 数据查询的全程加密保护，这是保护用户上网隐私安全和信息安全的重要技术手段。而保障我国用户的上网安全，则必须采用国密算法来加密 DNS，采用国密 SSL 证书实现国密 DoH/DoT 加密 DNS 服务。

美国《联邦零信任战略》要求联邦政府机构使用的 DNS 服务必须采用加密 DNS 协议(DoH 或 DoT)，这就是对传统的明文 DNS 的零信任，只信任加密 DNS，这非常值得我国政府机构学习与借鉴。

我国《密码法》和《商用密码管理条例》要求所有关键信息基础设施必须采用商用密码来保障其网络安全，这就是要求采用国密 DoH 或国密 DoT 技术来保障我国关键信息基础设施系统的 DNS 安全，这非常值得我国所有关键信息基础设施单位高度重视和尽快普及应用国密加密 DNS。

零信浏览器不仅支持国密 HTTPS 加密，而且支持国密 DNS 加密服务，有效保障了用户的上网安全和隐私保护。零信国密 HTTPS 加密自动化网关集成了加密 DNS 服务模块，实现了加密 DNS 的自动化，为用户提供了一站式 DNS 加密和 HTTPS 加密自动化解决方案。欢迎免费体验零信浏览器和优先选用零信国密 HTTPS 加密自动化网关。

有诗为证：

美国战略可借鉴，域名解析必加密。

加密也需自动化，零信网关已做到。

上网解析需加密，国密加密保安全。

王高华

2024 年 1 月 29 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。
从 2021 年 12 月 9 日开始，已累计发表中文 150 篇(共 39 万多字)和英文 60 篇(7 万多单词)。