什么是 TLS（Transport Layer Security）？

TLS 是一种安全协议，可为互联网通信提供私密性和数据完整性。实施 TLS 是构建安全 Web 应用的一个标准实践。

学习目标

阅读本文后，您将能够：

- 定义 Transport Layer Security (TLS)
- 说明 TLS 的工作方式
- 区分 TLS 和 SSL
- 了解 TLS 如何影响性能
- 概述如何实施 TLS

相关内容

复制文章链接

什么是 Transport Layer Security（TLS）？

Transport Layer Security (TLS) 是一种广泛采用的安全性协议，旨在促进互联网通信的私密性和数据安全性。TLS 的主要用例是对 Web 应用和服务器之间的通信（例如，Web 浏览器加载网站）进行加密。TLS 还可以用于加密其他通信，如电子邮件、消息传递和 IP 语音 (VoIP) 等。在本文中，我们将重点介绍 TLS 在 Web 应用安全中发挥的作用。

TLS 由互联网工程任务组（Internet Engineering Task Force, IETF）提出，协议的第一个版本于 1999 年发布。最新版本是 TLS 1.3，发布于 2018 年。

TLS 和 SSL 之间有什么区别?

Netscape 开发了名为安全套接字层（Secure Socket Layer，SSL）的上一代加密协议，TLS 由此演变而来。TLS 1.0 版实际上最初作为 SSL 3.1 版开发，但在发布前更改了名称，以表明它不再与 Netscape 关联。由于这个历史原因，TLS 和 SSL 这两个术语有时会互换使用。

TLS 和 HTTPS 有什么区别?

HTTPS 是在 HTTP 协议基础上实施 TLS 加密，所有网站以及其他部分 Web 服务都使用该协议。因此，任何使用 HTTPS 的网站都使用 TLS 加密。

为什么企业和 Web 应用应该使用 TLS 协议?

TLS 加密可以帮助保护 Web 应用免受数据泄露和其他攻击。如今，受 TLS 保护的 HTTPS 是网站的标准做法。Google Chrome 浏览器逐渐对非 HTTPS 网站进行打击，其他浏览器也纷纷效仿。日常互联网用户对没有 HTTPS 挂锁图标的网站更加警惕。

TLS 有什么作用?

TLS 协议实现的功能有三个主要组成部分：加密、认证和完整性。

- **加密：**隐藏从第三方传输的数据。
- **身份验证：**确保交换信息的各方是他们所声称的身份。
- **完整性：**验证数据未被伪造或篡改。

什么是 TLS 证书?

网站或应用要使用 TLS，必须在其源服务器上安装 TLS 证书（由于上述命名混淆，该证书也被称为 SSL 证书）。TLS 证书由证书权威机构颁发给拥有域的个人或企业。该证书包含有关域所有者的重要信息以及服务器的公钥，两者对验证服务器身份都很重要。

TLS 如何工作?

TLS 连接是通过一个称为 TLS 握手的流程启动的。当用户导航到一个使用 TLS 的网站时，用户设备（也称为*客户端*设备）和 Web 服务器之间开始 TLS 握手。

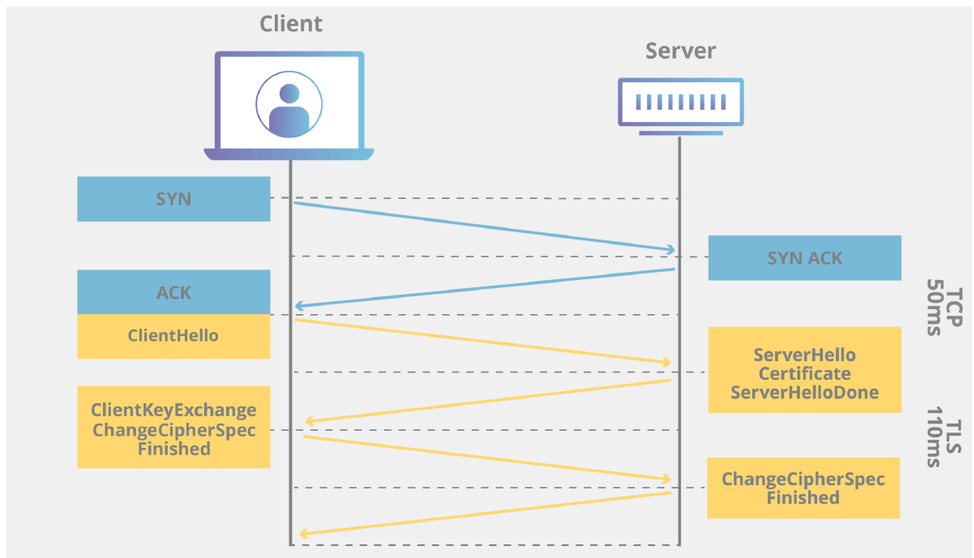
在 TLS 过程中，用户设备和 Web 服务器：

- 指定将要使用的 TLS 版本（TLS 1.0、1.2、1.3 等）
- 决定将要使用哪些密码套件（见下文）
- 使用服务器的 TLS 证书验证服务器的身份
- 握手完成后，生成会话密钥用于加密两者之间的消息

TLS 握手为每个通信会话建立一个密码套件密码套件是一组算法，其中指定了一些细节，例如哪些共享加密密钥（即会话密钥）将用于该特定会话。TLS 也能在一个未加密的通道上设置匹配的会话密钥，这要归功于一种称为公钥加密的技术。

握手还处理身份验证，其中通常包括服务器向客户端证明其身份。这是通过使用公钥来完成的。公钥是使用单向加密的加密密钥，即任何拥有公钥的人都可以解读使用服务器私钥加密的数据，以确保其真实性，但只有源发送方才可以使用私钥加密数据。服务器的公钥是其 TLS 证书的一部分。

数据完成加密和验明身份后，使用消息身份验证码（MAC）进行签名。接收方然后可以验证 MAC 来确保数据的完整性。这有点像阿司匹林药瓶上的防篡改铝箔；消费者知道没人篡改过他们的药品，因为购买时铝箔完好无损。



TLS 如何影响 Web 应用性能?

TLS 的最新版本对 Web 应用的性能几乎没有任何影响。

由于建立 TLS 连接涉及到的复杂过程，因此必须花费一些加载时间和计算能力。在传输任何数据之前，客户端和服务器必须来回通信几次，这将占用 Web 应用宝贵的几毫秒加载时间，以及客户端和服务器的一些内存。

然而，目前已有技术帮助缓解 TLS 握手造成的延迟。其一是 TLS 虚假启动（False Start），让服务器和客户端在 TLS 握手完成前开始传输数据。另一种加速 TLS 的技术是 TLS 会话恢复，允许之前通信过的客户端和服务器简化握手过程。

这些改良帮助 TLS 成为一种非常快速的协议，不会明显影响加载时间。至于与 TLS 相关的计算成本，以今天的标准来看几乎可以忽略不计。

2018 年发布的 TLS 1.3 进一步提高了 TLS 的速度。TLS 1.3 中的 TLS 握手仅需要一次往返（即来回通信），而不是以前的两次，将握手过程所需时间缩短了几毫秒。如果用户以前已连接过网站，TLS 握手的往返次数为零，从而进一步加快了速度。

如何开始在网站上实施 TLS?

Cloudflare 向所有用户提供免费的 TLS/SSL 证书。任何没有使用 Cloudflare 的用户将必须向一家证书机构获取 SSL 证书，而且往往需要付费，然后在其源服务器上安装证书。

要进一步了解 TLS/SSL 证书的工作原理，请参阅什么是 SSL 证书?