CLOUDFLARE

白皮書

最大程度地發揮 TLS 的作用 — 同時儘可能減少您的開銷

目錄

TLS 概觀

我們為什麼需要 TLS？

謹慎處理網際網路上的個人資料已變得越來越重要。在某些司法轄區，資料隱私權被視為一項基本人權，且全球正在實施越來越多的資料保護法規。而除此之外，確保網際網路流量私密且安全只是一件需要做的正確的事。

Transport Layer Security (TLS) 是隱私權與資料安全的通訊骨幹。它讓使用者能夠私密地瀏覽網際網路，而不會暴露自己的信用卡資訊或其他個人和敏感性資訊。Cloudflare 的使命是協助構建更好的網際網路，利用 TLS 等通訊協定保護網際網路使用者的隱私權也是該使命的一部分。

如果未能擁有適當的 TLS，會發生什麼？

TLS 憑證會驗證網站或應用程式是否完成了三個主要動作：

- **加密：**隱藏從第三方傳輸的資料
- **驗證：**確保交換資訊的各方是他們所聲稱的身分
- **完整性：**驗證資料未被偽造或篡改

當 TLS 憑證過期後，保護上的漏洞可能會造成肉眼可見的後果。例如：

- **負面 SEO 影響：**Google 和其他搜尋引擎會在搜尋結果中將具有 TLS/SSL 憑證 (https://) 的網站優先置於更高的位置。如果您僅執行 HTTP，則更難以與 HTTPS 網站競爭。
- **阻止訪客進入的警告：**當使用者嘗試存取沒有有效 TLS 憑證的網站時，瀏覽器會向使用者發出警告。如果看到瀏覽器警告，許多使用者會理所應當地關心隱私權風險，從而不再造訪您的網站。更少的流量意味著更少的轉換，進而對品牌知名度和收入產生影響。
- **洩露和罰款：**擁有過期的 TLS 憑證也會增加資料外洩的風險。如今，在全球不同地區有數不勝數的法規來管理資料隱私權，這些法規通常都要求或暗示需要進行加密。如果一家組織發生資料外洩且在當時並沒有採取適當的加密措施，則可能會面臨罰款或其他法規影響。

所有這些可能的後果都表明了 TLS 對應用程式效能與收益的重要性。

當 TLS 失效時，通常會影響終端使用者、客戶、合作夥伴和其他利害關係人的信任。好消息是可以輕鬆避免這些後果，本指南將詳細說明如何避免。

您知道嗎？

憑證在一開始擁有 398 天的生命週期，而隨著網際網路的發展，憑證越來越傾向於具有 90 天的生命週期。這意味著您續訂憑證的頻率要比之前快了大約 3.5 倍！ [1]

當今的四大 TLS 挑戰

1) 簡化 TLS 管理

在 Cloudflare，當我們與客戶談論 TLS 憑證生命週期管理時，他們經常告訴我們這是一個手動的艱難過程。他們的組織追蹤續訂的過程可能就是在頻繁續訂的試算表中記錄續訂，單調而乏味。如果沒有利用工具和自動化的方法來解決 TLS 憑證續訂問題，安全專業人員或團隊可能需要手動續訂憑證，這個過程會讓他們感到挫敗。

2) 確保合規性

正如之前所提及的，加密是保持應用程式私密且合規的基本組成部分。當我們在 IT 世界中設法保持應用程式的安全時，憑證簽發要求變得更加嚴格。隨著我們越來越多地瞭解到如何加強密碼，密碼最佳做法（例如推薦金鑰長度或雜湊演算法）也在不斷演進。

許多 Zero Trust 架構（如適用於私營部門的 NIST SP 800-207 和適用於公共部門的 NIST SP 800-53）直接呼籲將加密作為全面 Zero Trust 策略的關鍵部分。儘管大部分資料隱私權法規並不直接要求將加密作為一個必需項，但仍使用「適當的安全措施」等語句來暗示其必要性。

然而，團隊很難在第一時間瞭解到維護資料安全與隱私權的最新標準。

3) 管理團隊工作量

IT 團隊的負擔已經過重。始終掌握憑證續訂截止日期，看上去就像一個永遠不會結束的任務。隨著續訂期間變得越來越短，保持追蹤憑證續訂截止日期變得越來越耗時。

4) 讓網站和應用程式始終出現在客戶面前

錯過憑證續訂截止日期，可能會降低網站的搜尋引擎排名，或者當使用者從另一個來源前往您的網站時，他們可能會在看到瀏覽器安全警告後停止造訪。要確保組織的 Web 應用程式出現在客戶與使用者面前，保持憑證續訂是一個重要的方法。

Cloudflare 如何解決主要 TLS 挑戰

在下面的章節中，您將瞭解客戶利用 Cloudflare，透過 TLS 加密其資料和流量的一些主要使用案例：

- 常見使用案例：
  - 保護邊緣連線
  - 利用 mutual TLS (mTLS) 保護源站連線
- mTLS 的新興使用案例：
  - 驗證用戶端和裝置
  - 增強 Zero Trust 存取
  - 保護 API
  - 保護 IoT 流量

以下是您在進行自己的內容傳遞網路 (CDN) 部署 (包括 Cloudflare 部署) 時可能遇到的一些常見情境。

保護邊緣連線

保護網站訪客/用戶端裝置之間的連線，可以在使用者瀏覽時保護其隱私權，因此這是 Cloudflare 使命的基礎。

當您為網域訪客實施保護時，請考慮以下選項來保護與 Cloudflare TLS 的邊緣連線。

利用 Cloudflare 減少憑證管理開銷

使用基本 TLS 憑證並讓 Cloudflare 管理簽發和續訂
Cloudflare 為網際網路上的數百萬網域提供免費憑證。在 Cloudflare 代理後方佈設的所有網域都可使用此 Universal SSL 服務，該服務作為「通用」解決方案提供，個人網站和《財富》500 強企業都可以使用。

對於想要減少管理開銷的組織而言，這是一個完美的免費選項。我們的可擴展基礎架構能夠處理超過 5000 萬個憑證 (截至 2023 年 5 月)，而且我們可從每一個資料中心提供 TLS 憑證，因此您可以選擇更靠近使用者的資料中心，從而減少延遲。Cloudflare 還可以代表您處理網域控制驗證以及簽發和續訂憑證。當您的網域佈設至 Cloudflare 後，Cloudflare 會自動處理憑證驗證、簽發和續訂，您無需採取任何額外動作。

如果您符合以下情況，則 Cloudflare 的 Universal SSL 是您的最佳選擇：

- 需要一個免費方案來減少憑證生命週期管理開銷（尤其是當您擁有有限的員工、預算或時間時）；以及
- 沒有對自訂憑證的獨特需求，或不需要選擇要接受哪個憑證授權單位 (CA)。

在減少管理開銷的同時自訂 TLS 部署
Cloudflare 代理後方的許多組織發現他們很喜歡 Universal SSL 提供的生命週期管理。然而，對於那些因為組織或法規要求而需要更多自訂，但仍然想要減少管理開支的組織，Cloudflare 提供了 Advanced Certificates Manager。

如果您符合以下情況，則 Advanced Certificate Manager 是您的完美之選：

- 對於需要顯示在憑證上的主機名稱有具體要求；
- 想要比預設的 90 天有效期更短的有效期間（例如，一些組織有更高的安全需求，希望其憑證僅在 2 週內有效）；及/或
- 對想要使用的 CA 需要更多的靈活性。（參閱此處以獲取當前的 Cloudflare CA 合作夥伴清單。）

自動為新主機名稱簽發 TLS 憑證
隨著組織的成長，他們極有可能需要新的主機名稱和新的 Web 內容，例如新的產品線或網站的當地語係化版本。當您使用進階憑證時，您始終需要告知我們需要出現在憑證上的主機名稱。但有時您可能想要告訴 Cloudflare，「我想要為我放置在 Cloudflare 代理後方的每一個新主機名稱都簽發 TLS 憑證。」在這種情況下，對於快速成長的組織而言，利用我們稱為 Total TLS 的服務自動為任何新主機名稱簽發 TLS 憑證是一個更有效的選項。

利用 Total TLS 為每個新主機名稱自動簽發，意味著您的新建網域不會出現安全和隱私權漏洞。除了無需再考慮與佈設新子網域相關的一切事情外，您還可以省去與簽發新 TLS 憑證相關的管理開銷。

Cloudflare 將利用針對單個主機名稱的憑證，為您的每個主機名稱簽發憑證，您也可以選擇為所有憑證簽發 CA。隨著您建立更多的子網域，Cloudflare 將始終以您的名義簽發憑證，並在其有效期即將到期時進行續訂。與其他 Cloudflare 管理的憑證模式一樣，我們將按照您的安全規範以及您偏好的 CA 和有效期，以您的名義續訂您的憑證。

如果您符合以下情況，則 Total TLS 是您的絕佳選擇：

- 正在為一家快速成長的組織管理網站/應用程式；
- 多項 Web 內容都需要 TLS 憑證，例如新產品線、服務或網站的當地語係化 (已翻譯) 版本的託管資訊；
- 除了上線新子網域外，沒有內部資源來管理與簽發 TLS 憑證相關的開銷；及/或
- 想要確保新建的網域不會出現安全或隱私權漏洞。

自動備份憑證

除了選擇正確的解決方案來減少憑證管理開銷外，**確保 TLS 憑證的安全備援**也十分關鍵。一場金鑰洩露或 CA 撤銷之類的事件就可能導致需要立即重新簽發憑證——假設您當前的憑證將被洩露。例如，2021 年，最受歡迎的一家 CA 經歷了一次撤銷，在此期間，這家 CA 撤銷了幾千個憑證。或者，像 2014 年的 Heartbleed CVE 事件中一樣，憑證可能因漏洞或其他安全問題而被洩露。

一旦 CA 撤銷開始，在所有憑證被標記為「已撤銷」之前，組織和個人只有 24 小時的時間來簽發和部署替換憑證。在 Cloudflare，我們管理數千萬個憑證。如果我們支援的一家 CA 經歷撤銷，或者他們的憑證被洩露，我們將需要一次重新簽發數千萬個憑證。儘管 Cloudflare 的管線能夠處理這種需求激增，但我們仍需要與 CA 合作以重新簽發憑證，除此之外，依據客戶管理其 TLS 憑證的方式，客戶可能需要手動將網域控制驗證記錄上傳到 Cloudflare。

為撤銷或漏洞之類的災難場景制定應急方案至關重要。如果 CA 撤銷再一次發生，擁有備份憑證意味著您可以立即切換至有效憑證，從而防止在 TLS 保護方面出現漏洞的可能性。這會減少網站停機時間，確保您的網站保持安全，並為終端使用者提供連續性。

為此，我們建議**利用 Cloudflare 自動備份憑證**（預設啟用），Cloudflare 利用單獨的加密金鑰和與主要憑證不同的 CA 來簽發備份憑證。一旦發生金鑰洩露或 CA 撤銷，即可快速切換。與 Cloudflare 管理的其他憑證一樣，我們將為您管理簽發和續訂。

您知道嗎？

Google 上來自美國的 Web 流量中，大約 91% 是加密的 [2]。在 Google 的前十大流量來源國當中，另外九個國家擁有更高的百分比，這些國家包括：

- 英國 - 93%
- 德國 - 94%
- 巴西 - 95%
- 墨西哥 - 96%
- 日本 - 96%
- 印尼 - 96%
- 荷蘭 - 96%
- 印度 - 97%
- 比利時 - 99%

自行管理憑證

使用自己的憑證

組織可能出於一些原因而想要使用自己選擇的 CA 簽發的自訂憑證。例如，如果您想要使用延伸驗證 (EV) 或組織驗證 (OV)，您可以從您選擇的 CA 處獲得憑證，並將憑證和私密金鑰上傳到 Cloudflare。擁有偏好 CA 或已經與不在我們生態系統中的 CA 建立關係的使用者會想要選擇此選項，因為這種部署模式可讓您在外部 CA 處獲取憑證並將其上傳到 Cloudflare，然後您可以獲得在邊緣提供憑證的所有好處。

在 Cloudflare 保留您的私密金鑰的情況下處理續訂

如果您想要使用自訂憑證，您可以從心儀的 CA 處獲得憑證，並要求 Cloudflare 控制私密金鑰。在這種情況下，您只需負責公用憑證部分。您可以使用憑證簽署要求 (CSR) 進行憑證續訂，自行處理憑證續訂並重複使用 CSR 進行憑證續訂。

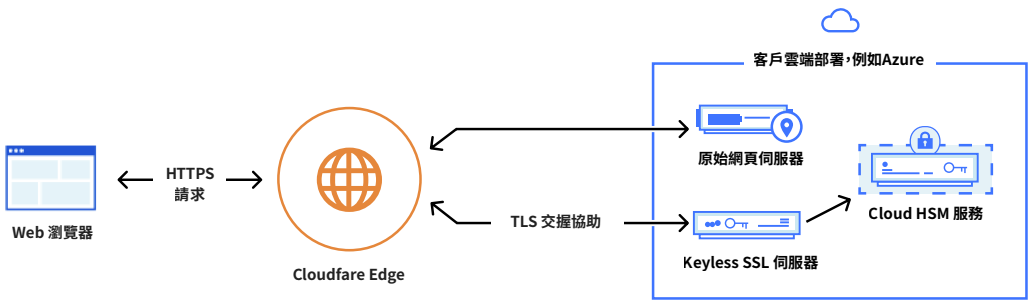
對於需要親自進行憑證管理或有特殊的憑證簽發要求的組織來說，自己處理續訂並讓 Cloudflare 保留私密金鑰是一個有用的方案。在這兩種情況下，您都要完全負責續訂事宜；不過，我們將會傳送憑證續訂提醒電子郵件，協助您掌握有關截止日期的資訊。

安全團隊需要獨立續訂憑證，並在續訂憑證後將其重新上傳到 Cloudflare。當您變更憑證時，建議您在我們的暫存網路上暫存您的轉換。暫存可以幫助安全團隊在部署到生產環境之前發現任何問題。在將憑證部署到生產環境後，Cloudflare 提供輕鬆復原憑證的功能。儘管在這種情況下我們不管理續訂管線，但我們會為您提供工具，確保您能夠安全可靠地管理續訂。

在硬體安全性模組 (HSM) 上保管私密金鑰

處於高度監管產業的許多組織（如政府、處理醫療健康記錄的組織和金融服務）不能與外部組織分享私密金鑰。利用無金鑰 SSL，這些公司可以在將私密金鑰安全儲存在自有硬體安全性模組 (HSM) 中的同時，仍然使用 TLS 和雲端服務。某些客戶需要將其金鑰儲存在 HSM 中（包括雲端 HSM），且可能已經將金鑰儲存在這些伺服器中。如果您的組織也屬於這種情況，您可以在保持內部監管私密金鑰的同時，仍然使用 Cloudflare 安全性、效能和可靠性服務。

利用無金鑰設定，您可以將私密金鑰保留在自己的基礎架構中，同時讓 Cloudflare 提供公用憑證，並允許使用工作階段金鑰終止 TLS。為此，您需要在您自己的基礎架構中執行 Cloudflare 無金鑰 SSL 精靈，可閱讀我們的產品文件瞭解相關資訊。



TLS 安全狀態的整體考量

建議組織僅允許來自支援 TLS 1.3 的流量的連線，這是最新、最快速且更安全的 TLS 通訊協定版本。利用 Cloudflare，您僅需最少的 TLS 設定即可設定 TLS 1.3。

NIST SP 800-52（選擇、設定和使用 Transport Layer Security 實施的指南）將從 2024 年 1 月 1 日起要求使用 TLS 1.3。PCI DSS v4.0 合規性要求支付卡處理商使用 TLS 1.2 或 1.3。

用戶端可能支援各種密碼套件，其中一些在這些年中被發現並不安全。建議您限制舊版密碼套件，僅允許來自支援更安全的密碼套件之用戶端的連線，例如使用完美前向保密 (PFS) 或驗證加密的用戶端。選擇此選項可為您的組織提供最佳的安全性和效能，並僅與具有最現代化、最安全的裝置和瀏覽器的用戶端建立連線。

就像個人識別資訊 (PII) 一樣，密碼編譯金鑰也通常會受法規的約束。部分法規要求將金鑰保持在特定的地理位置，其中最常見的就是歐盟和 GDPR 要求。不過，全球範圍內的私密金鑰法規正在持續激增。

Cloudflare Data Localization Suite 可讓組織輕鬆滿足將資料和金鑰儲存在特定地理位置的要求。使用 Data Localization Suite 這類工具不僅可以確保安全儲存您的金鑰，還可以保證其不會離開法律規定的地區。隨著越來越多的地區新增類似於 GDPR 的規則（實際上，越來越多的國家和地區將 GDPR 用作資料隱私權法的模型），對基於地理位置的儲存要求也將增加。

Geo Key Manager 讓您可以將私密金鑰的位置限制為所允許地區內的資料中心，也可以透過基於規則的地理限制，建立排除項。例如，您可以進行設定，允許將金鑰儲存在歐盟和美國，但將法國排除在外。

此功能可以用於儲存私密金鑰以及其他受隱私權法律影響的資料。

您知道嗎？

超過 50% 的 Web 伺服器仍然支援 TLS 1.0 和 TLS 1.1，儘管這兩個通訊協定版本早已在 2021 年被 IETF 正式棄用。[3]

保護源站連線

保護源站連線的最佳做法
保護源站連線的最佳做法是要求 Cloudflare 使用 HTTPS 連線至您的源站，同時使用 mutual TLS（mTLS，也稱為雙向 TLS）。

當 Cloudflare 透過 HTTPS 連線來連線至您的源站時，我們會檢查源站是否提供了伺服器憑證。我們會驗證憑證：

- 有效且未過期；
- 包含目標主機名稱的通用名稱（上面具有正確的主機名稱）；以及
- 公開受信任，或者您已將 CA 列入我們的 trust store 中，以告訴我們可以信任它。

當我們連線至您的源站時，這有助於保護 Cloudflare 代理，就像當您的用戶端連線至 Cloudflare 時，您知道自己可以信任我們的網路一樣。

當您的組織允許 Cloudflare 連線至您的源站時，理論上，世界上的其他用戶端也可以連線至您的源站。為緩解潛在的安全問題，此處的最佳做法是限制該連線，並僅允許來自 Cloudflare（或透過 Cloudflare 代理）的流量。

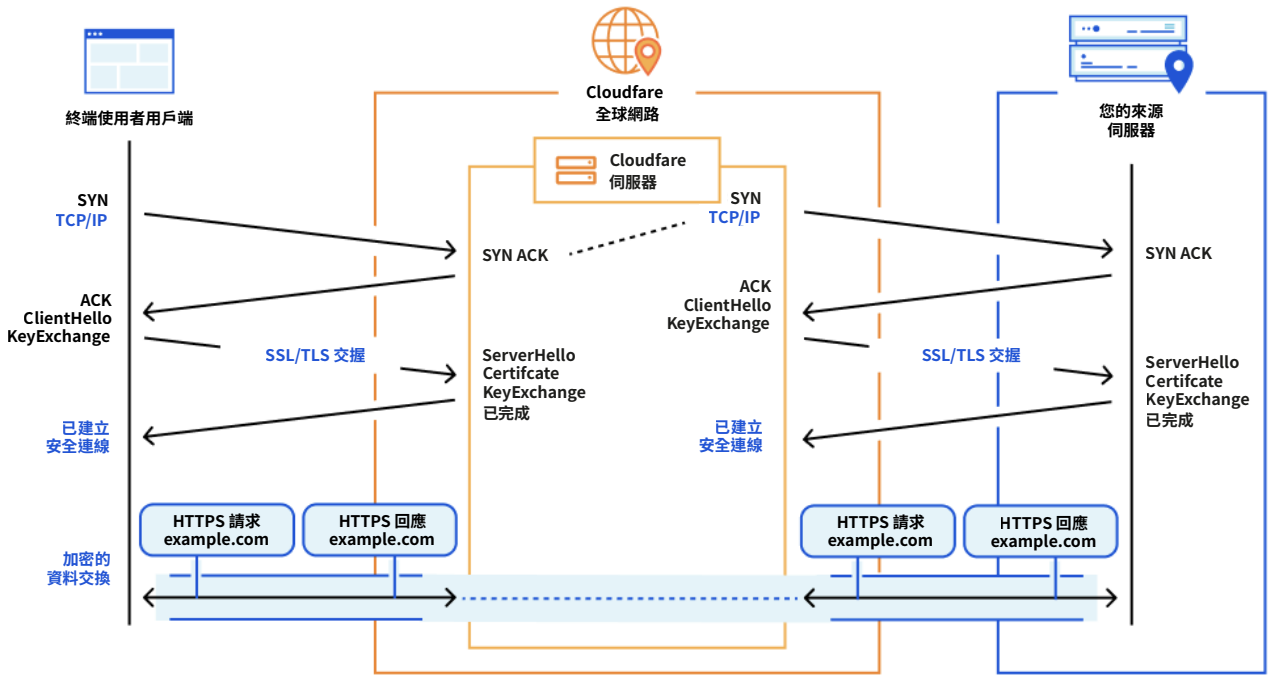
未授權的連線可能耗用寶貴的 CPU，因此，最好的情況是根本不處理這些不需要的請求。

與此相似，利用 mTLS 保護您的源站會對您整體的阻斷服務 (DoS) 緩解策略有所幫助。使用 mTLS，Cloudflare 將始終為請求提供用戶端憑證。而在源站端，您可以驗證該用戶端憑證，確保流量來自受信任的來源——Cloudflare。

如果您看到用戶端憑證與 Cloudflare 相符，則可以允許該請求通過。如果用戶端憑證無效，您可以捨棄該請求，從而阻止來自不受信任的未知第三方的攻擊。

利用 mTLS，安全團隊可以確保流量來自 Cloudflare，而不是第三方伺服器。若要進行此設定，請在您的整個網域或特定主機名稱上設定 Authenticated Origin Pulls。按之前章節中所述的方式，使用 Cloudflare 管理的憑證或上傳您自己的用戶端憑證。

實現安全 SSL/TLS 連線

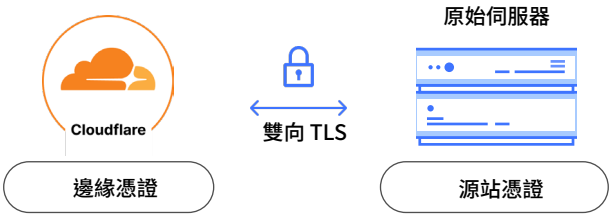


新興 TLS 使用案例

驗證用戶端和裝置

在傳統的單向 TLS 中，裝置將檢查伺服器的憑證，以確保可以安全連線。與此不同的是，mTLS 是雙向連線，可同時保護用戶端和伺服器，因為二者都需要出示有效的憑證，以證明它們是所聲稱的身分。

mTLS 是一個基本的工具，用於確保只有授權的用戶端和裝置向您的應用程式發出請求。下面詳細討論了 Cloudflare 客戶如何使用 mTLS 的一些範例。



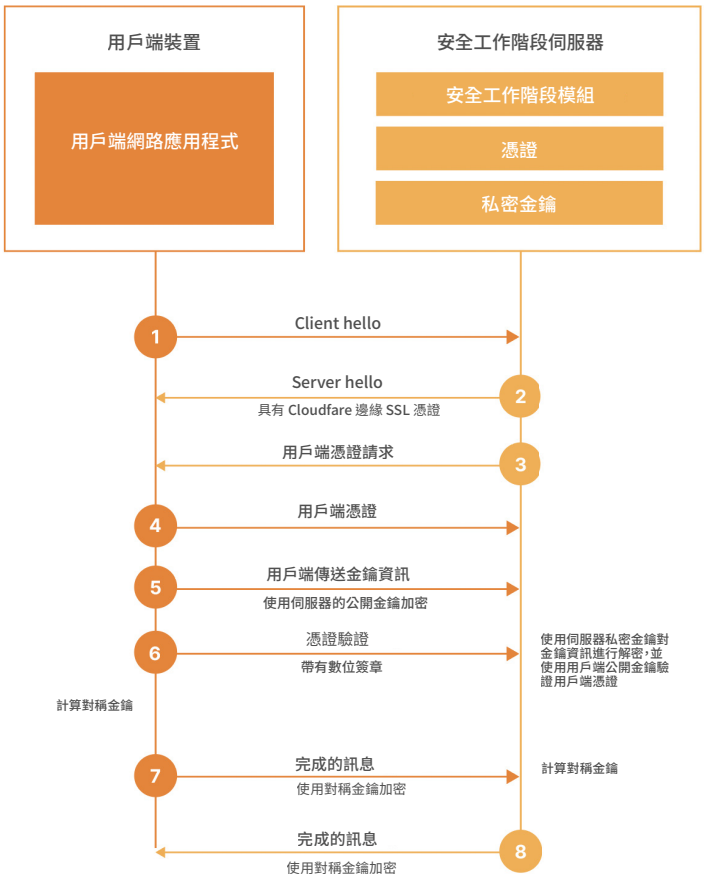
增強 Zero Trust 存取

當您聽到 Zero Trust 時，您可能會想起預設拒絕之類的概念：除了明確允許的連線和請求外，拒絕其他所有連線和存取請求。可以將 mTLS 視為另一個 Zero Trust 安全層，它非常強大，可以確保僅允許所需的連線。

mTLS 與驗證相似：裝置將出示一個用戶端憑證作為額外的安全層，源站可以驗證該用戶端憑證以允許該連線繼續。如果傳送的請求包含不正確的用戶端憑證，源站會注意到該憑證無效，組織可以進行安全性設定，以自動阻止此類請求通過。這可以作為身分和存取管理等其他安全層的補充。

在公司網路中，組織通常會指定敏感的內部資源，員工只能從公司裝置存取這些資源，而不能從個人裝置存取。mTLS 是一款適用於此案例的強大工具：安全團隊可以向經核准的工作裝置授予用戶端憑證，組織也可以建立原則，阻止缺乏有效憑證的裝置進行存取。

用戶端驗證的 TLS 交握



保護 API

管理和保護 API 是 Cloudflare 的首要任務。事實上，我們在全球網路上看到的大部分動態流量都與 API 相關。隨著越來越多的大型企業將 API 用於業務關鍵型運作，安全性領導者和團隊對 API 安全的責任也越來越大。

除了 Cloudflare API Gateway 功能外，對於採用積極網路安全模型，或者我們之前討論的「預設拒絕」安全狀態的組織來說，也可以將 mTLS 納入 API 安全策略之中。這意味著封鎖所允許連線之外的所有連線，例如，允許來自受信任業務合作夥伴或受信任開發人員的連線，以及僅允許授權使用者和裝置進行 API 呼叫。與其他使用案例一樣，在這裡，mTLS 也可以用作驗證和授權工具，僅允許出示正確憑證的主機真正進行 API 呼叫。

這種 mTLS 使用案例在金融服務和金融科技公司中尤為常見，但許多組織擁有的 API 端點僅應透過有效的用戶端憑證進行安全存取。舉例來說，mTLS 讓組織可以驗證向資料庫發出寫入請求的 API 來自經核准的來源。隨著 API 安全需求的擴展，mTLS 在積極網路安全模型中扮演著重要角色。

保護 IoT 流量

IoT 裝置之類的無頭裝置是 mTLS 的另一個新使用案例。儘管這些裝置上缺少 GUI，組織仍然可以識別和驗證它們。就像公司網路中的工作筆記型電腦安裝了用戶端憑證一樣，您也可以在攝影機系統、咖啡機、智慧鎖、辦公室讀卡器等裝置上安裝用戶端憑證。

當這些裝置向伺服器發出請求時，伺服器應當可以驗證請求來自哪個裝置，以及檢查是否已授權該裝置發出請求。組織可以封鎖來自未經授權裝置的請求。因此，如果有人嘗試駭入您的應用程式，他們將無法對 Web 伺服器發出請求，除非他們使用通過驗證且已識別身分的 IoT 裝置。除了 mTLS 之外，採取機器人緩解等額外的安全措施，也有助於識別惡意流量是否源自遭到入侵但通過驗證的裝置。

保護無伺服器開發

越來越多的客戶使用我們的無伺服器運算平台 Cloudflare Workers 來開發他們自己的應用程式，而無伺服器運算有其自己獨特的安全需求。

確保您的開發人員向受信任的來源傳送資料
當在 Workers 上構建時，您通常會指示單個 Cloudflare Service Workers（處理 HTTP 流量的 Workers）向資料庫、服務、雲端提供者等發出輸出請求。您可能在 Workers 上執行多項服務，且需要能夠識別特定的 Workers，以知曉其是否有權向特定資源發出特定請求。

透過使用 mTLS 要求 Worker 識別伺服器，以及要求伺服器識別請求來自哪個 Worker，您可以更好地保護來源伺服器免遭資料外洩和其他攻擊。

利用 mTLS 進一步保護伺服器與 Worker 之間的連線，可以阻止未經授權的 Worker 接收敏感性資訊。利用 mTLS，開發人員可以確保他們正在向受信任的已知來源傳送資料。

允許 Worker 和源站互相驗證身分可減少二者之間攻擊的可能性。mTLS 可以防止憑證填充、中間人攻擊、欺詐、網路釣魚等攻擊。

如之前所提及的，mTLS 遵循 Zero Trust 的原則——在驗證彼此的身分之前，Worker 和伺服器都不會被視為「可信」。

透過驗證獲得更精細的存取控制
由於有多項 Workers 服務向同一資料庫寫入，您可能會希望能夠區分它們。如果，在某一時刻，您需要移除某個 Worker 的「寫入」權限，該怎麼辦？或者，如果僅應允許 Worker「A」和「B」發出寫入請求，並僅允許 Worker「C」發出讀取請求，該怎麼辦？Cloudflare 提供兩個選項：

- 您可以利用我們的 Zero Trust 網路存取 (ZTNA) 服務 Cloudflare Access，並透過使用預先共用的金鑰和設定 Worker，來設定權杖驗證，進而基於標頭中的預先共用金鑰來允許或拒絕存取。
- 或者，如果您不想暴露用戶端的身分或需要兩個服務透過 HTTP 進行通話，則可以針對 Workers 使用 mTLS 驗證。Workers 上的 mTLS 支援是在 Workers 上構建的開發人員管理驗證和身分的一種簡單方式。

這兩種方法都允許您在 Worker 層級甚至請求層級鎖定驗證，以進行更精細的驗證和識別。

實際客戶體驗

DHL

DHL 是一間大型全球貨運和物流公司，其利用 Cloudflare 來加密所有客戶通訊，以維持遵守資料隱私權法律。數位與業務流程最佳化副總裁 Jan De Groot 說道：「我們對安全洩露零容忍。我們保護客戶資料，並確保與客戶的所有通訊都是安全的。」

利用 Cloudflare TLS，DHL Parcel 可以將強加密延伸到其消費者以及企業對企業客戶通訊上，而不用考慮他們使用什麼 Web 瀏覽器。

即使攻擊數量增加，DHL Parcel 也可以簡化客戶面向應用程式的合規性要求，這些應用程式需要遵守歐盟的一般資料保護要求 (GDPR) 以及德國更嚴格的資料保護法規。

de Groot 說道：「Cloudflare 幫助 DHL Parcel 保護我們的客戶資料和客戶溝通，簡化了對 GDPR 等資料隱私權法規的遵循。」

挑戰：確保強安全性和合規性

「我們對安全洩露零容忍。我們保護客戶資料，並確保與客戶的所有通訊都是安全的。」

使用 Cloudflare 後的結果：

- 利用 Cloudflare TLS，DHL Parcel 可以將強加密延伸到其消費者以及企業對企業客戶通訊上，而不用考慮他們使用什麼 Web 瀏覽器。
- 從惡意瀏覽器外掛程式，到最新的應用程式和網路威脅，Cloudflare 可幫助 DHL Parcel 保護其業務和客戶免受資料外洩和業務中斷。
- 即使攻擊數量增加，DHL Parcel 也可以簡化客戶面向應用程式的合規性要求，這些應用程式需要遵守歐盟的一般資料保護要求 (GDPR) 以及德國更嚴格的資料保護法規。

「Cloudflare 幫助 DHL Parcel 保護我們的客戶資料和客戶溝通，簡化了對 GDPR 等資料隱私權法規的遵循。」

Jan De Groot，

數位與商務程序最佳化副總裁

閱讀完整案例研究 >

SHOPYY

SHOPYY 是一個電子商務平台，其與 Cloudflare 合作以獲取 SSL for SaaS 功能，該功能可以自動化 SSL 憑證管理，涵蓋私密金鑰建立、保護、網域驗證、簽發，以及進行續訂以重新簽發的整個過程。最初，SHOPYY 使用免費的憑證管理工具，產生了不可靠的憑證以及很短的有效期。這款免費工具也需要大量的時間和人力，需要 SHOPYY 雇用額外的員工來監管憑證管理程序。

使用 Cloudflare SSL for SaaS，SHOPYY 將所有憑證管理工作委託給 Cloudflare，只需一名員工即可維護整個流程。「使用 Cloudflare 產品後，僅在營運和維護方面，我們的員工成本就降低了 60%，」創辦人暨技術長 Yuanming Chen 說道。「作為 Cloudflare 的客戶，我們獲得了效率與成本效益，同時又能夠將同樣的優質服務提供給我們自己的客戶。」

挑戰：從自製平台升級到成熟的雲端產品——該平台包含可靠的全方面憑證代管

使用 Cloudflare 後的結果：

- 使用可自動化 SSL 憑證管理的 Cloudflare SSL for SaaS 後，SHOPYY 現在能夠將憑證管理完全委託給 Cloudflare，無需擔憂 SSL 憑證生命週期的任何部分。
- Cloudflare 管理從私密金鑰建立和保護到網域驗證、簽發、續訂和重新簽發的整個過程。
- 因此，SHOPYY 現在只需要一個員工來維持整個營運和維護結構，將員工成本減少了大約 60%。

SHOPYY

「使用 Cloudflare 產品後，僅在營運和維護方面，我們的員工成本就降低了 60%……作為 Cloudflare 的客戶，我們獲得了效率與成本效益，同時又能夠將同樣的優質服務提供給我們自己的客戶。」

Yuanming Chen，

創辦人兼技術長

閱讀完整案例研究 >

OneTrust

OneTrust 是一款熱門的隱私權與合規性服務。全球有超過 7,500 家企業利用 OneTrust 的 SaaS 解決方案來管理隱私權、安全性和治理，以遵守 CCPA、GDPR、LGPD、PDPA 和 ISO27001 等法規。OneTrust 在約 33 個頂級網域和約 16,000 個子網域中使用 Cloudflare 產品，公司每月透過 Cloudflare 處理的流量剛剛超過 2PB。得益於 Cloudflare SSL for SaaS，所有 OneTrust 客戶都可以選擇部署一個自訂網域。

該公司也使用 Cloudflare 來保護他們自己的網域。OneTrust 的資訊安全主管 Colin Henderson 說道：「Advanced Certificates Manager 簡化了我們在眾多網域中管理憑證的方式，同時讓我們能夠滿足嚴格的安全性要求。管理密碼套件以及在我們的參數內自動續訂的功能，創造了一個可用且安全的環境。」

挑戰：部署高效、可擴展且具成本效益的效能和安全解決方案，以此來支援巨大的增長

使用 Cloudflare 後的結果：

- OneTrust 在約 33 個頂級網域和約 16,000 個子網域中使用 Cloudflare 產品，公司每月透過 Cloudflare CDN 服務的流量已超過 2PB。得益於適用於 SaaS 的 Cloudflare SSL，所有 OneTrust 客戶都可以選擇部署一個自訂網域。
- 該公司也使用 Cloudflare 來保護他們自己的網域。管理密碼套件以及在其參數內自動續訂的功能，創造了一個可用且安全的環境。

onetrust

Advanced Certificates Manager 簡化了我們在眾多網域中管理憑證的方式，同時讓我們能夠滿足嚴格的安全性要求。」

Colin Henderson

資訊安全主管

閱讀完整案例研究 >

Cloudflare 的 SSL/TLS 產品

Cloudflare 提供免費和企業級的 SSL/TLS 憑證管理和簽發，為您的終端使用者和資料提供隱私權保護，並提供大量自訂選項：

- Universal SSL - 免費的 SSL/TLS 憑證，由 Cloudflare 管理簽發和續訂
- Advanced Certificates Manager - 自動執行憑證簽發和續訂，並提供強大的自訂選項
- SSL for SaaS - 讓 SaaS 提供者能夠代表其客戶簽發和續訂憑證

探索我們的 SSL/TLS 產品可如何滿足您的安全性目標

請求示範

或連絡我們！ + 886 8 0185 7030

+ 886 8 0185 7030 | enterprise@cloudflare.com | Cloudflare.com

REV:BDES-4636.2023JUL19