CLOUDFLARE®

HTTPS is Fast and Hassle-free with Cloudflare

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

In the past, organizations had to choose between performance and security when encrypting their web traffic. Even if they were willing to trade increased latency for higher security, operational difficulties limited broad adoption.

This situation has changed. With recent developments in HTTPS technology, such as SPDY, sending requests over HTTPS can be faster than using regular HTTP. Also, the complicated operational issues associated with sending encrypted data can be handled by third parties like Cloudflare. It's time for enterprises to take another look at securing their web traffic.

What Exactly is HTTPS?

The Hypertext Transfer Protocol (HTTP) is the foundation for transferring data on the Internet, and HTTPS builds on this by adding Transport Layer Security (TLS), ensuring a reliable and secure way to send data over the Internet.

Every new HTTPS connection requires a TLS "handshake" in order to prove the identity of the server and establish shared encryption keys. A TLS handshake does four things:

- It agrees on connection protocols and parameters, such as cryptographic and signature algorithms
- It authenticates the server, so users can be sure they are communicating with the intended party
- It generates a master encryption key that will be used to encrypt and decrypt data
- It verifies that none of the previous steps were modified by a third party

Unfortunately, each of these steps requires that information be sent back and forth between the client and server, adding latency to HTTPS connections and noticeably slowing the initial page load. This degraded user experience is why many companies have steered away from using HTTPS for all of their website traffic.

Lightning-fast HTTPS

Cloudflare makes HTTPS connections lightning-fast by keeping up with the latest performance-enhancing features:

- **ELLIPTIC CURVE CRYPTOGRAPHY** Smaller certificates with smaller keys result in faster connection establishment.
- **SPDY PROTOCOL** SPDY enables faster-than-HTTP download speeds with multiplexing, and is on by default for all customers. SPDY is the inspiration for the new HTTP/2 standard, which Cloudflare will support in the coming year.
- **HTTPS SESSION RESUMPTION** Connections to sites you have already visited are jump-started making connection times faster.
- **OCSP STAPLING** Allows browsers to quickly check if a TLS certificate is valid.
- **GLOBALLY DISTRIBUTED NETWORK** Reduces connection latency by shortening the distance information has to travel via our CDN.

Elliptic Curves

The first part of the TLS handshake, authenticating servers and (optionally) clients, adds the most latency to an HTTPS connection of any steps.Typically, authentication is done using RSA keys. RSA keys were the standard for years, but they've run into some problems. As mathematicians have discovered new factoring techniques and computing power has continued to grow, cracking RSA keys has become easier and cheaper.

The response has been to create larger, more secure keys. While this did improve security, it also increased latency for TLS handshakes because larger keys means that more data must be sent back and forth to authenticate a connection.

Cloudflare is leading the industry in adopting the latest HTTPS key technology called Elliptic Curve Cryptography or ECC. ECC offers the same level of security as RSA, but with much smaller keys. The use of smaller ECC keys speeds up HTTPS in two ways:

- Smaller keys mean smaller certificates and less data to pass around to establish an HTTPS connection.
- Smaller keys have faster algorithms for generating signatures because the math involves smaller numbers.

The graph below shows that a highly secure RSA key uses 3,248 bits, while an Elliptic Curve key of the same strength only requires 256 bits:

Protection	RSA keys	ECC keys
Short-term protection (10 years)	1,776 bits	192 bits
Medium-term protection (20 years)	2,432 bits	224 bits
Long-term protection (30 years)	3,248 bits	256 bits

*From: http://www.ecrypt.eu.org/ecrypt2/documents/D.SPA.20.pdf (pp. 30-31)

SPDY

SPDY is a protocol developed by Google to speed up web traffic. SPDY requires HTTPS, and Cloudflare utilizes it to speed up encrypted traffic.

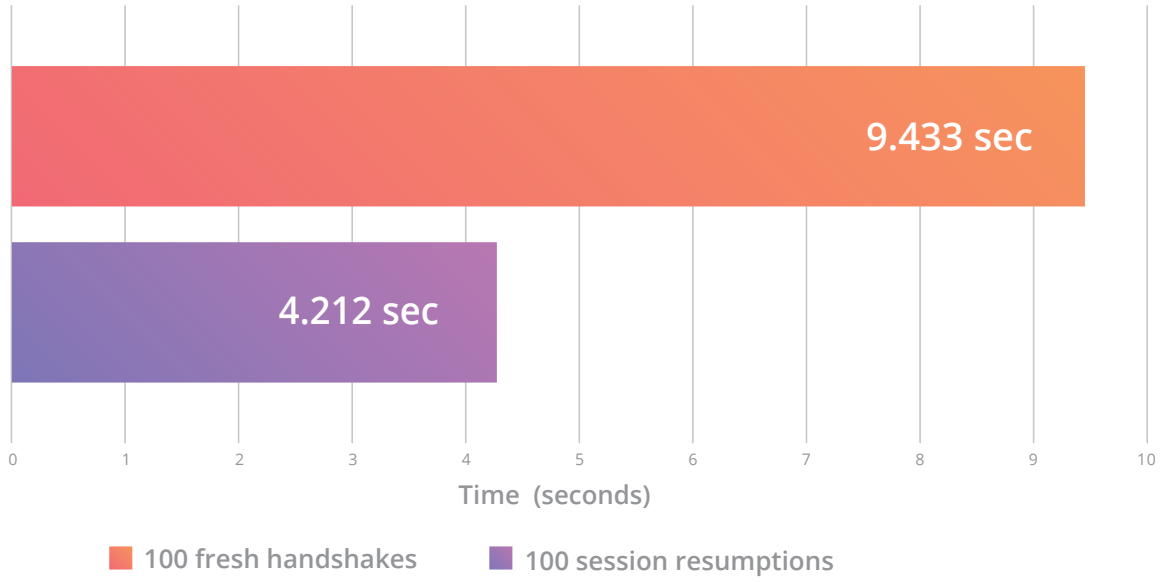
SPDY improves HTTPS performance through:

- **Multiplexing:** Standard HTTP requests need to make multiple TCP requests to retrieve all objects on a web page, and each new TCP connection adds latency to the request. With multiplexing, SPDY uses only one connection for all requests, greatly reducing latency.
- **Smart Download Order:** Objects are sent as they are ready, increasing performance by not holding up delivery because of one slow object. SPDY also allows servers to push data to browsers in anticipation of requests.
- **Header Compression:** By compressing request and response headers for HTTPS, common strings that appear in headers don't need to be sent across the network, and every byte not sent reduces bandwidth and increases performance.

Cloudflare's HTTPS Session Resumption

Another way Cloudflare is speeding up HTTPS is with session resumption. Session resumption reduces the number of trips a TLS handshake needs to make by resuming a previously established session with a server using an abbreviated handshake.

The performance gains of a reduced handshake can be seen in the following graph:



OCSP Stapling

One of the less frequently discussed but most significant performance hits to HTTPS is the OCSP/CRL check. To support secure connections over HTTPS, a website must have a TLS certificate. Unfortunately, these certificates can be stolen or compromised, and if that happens the Certificate Authority that issued the certificate can revoke it. To confirm that the certificate being used to set up an HTTPS connection is valid, browsers must check the status of that certificate with each new request using a Certificate Revocation List (CRL) or the Online Certificate Status Protocol (OCSP).

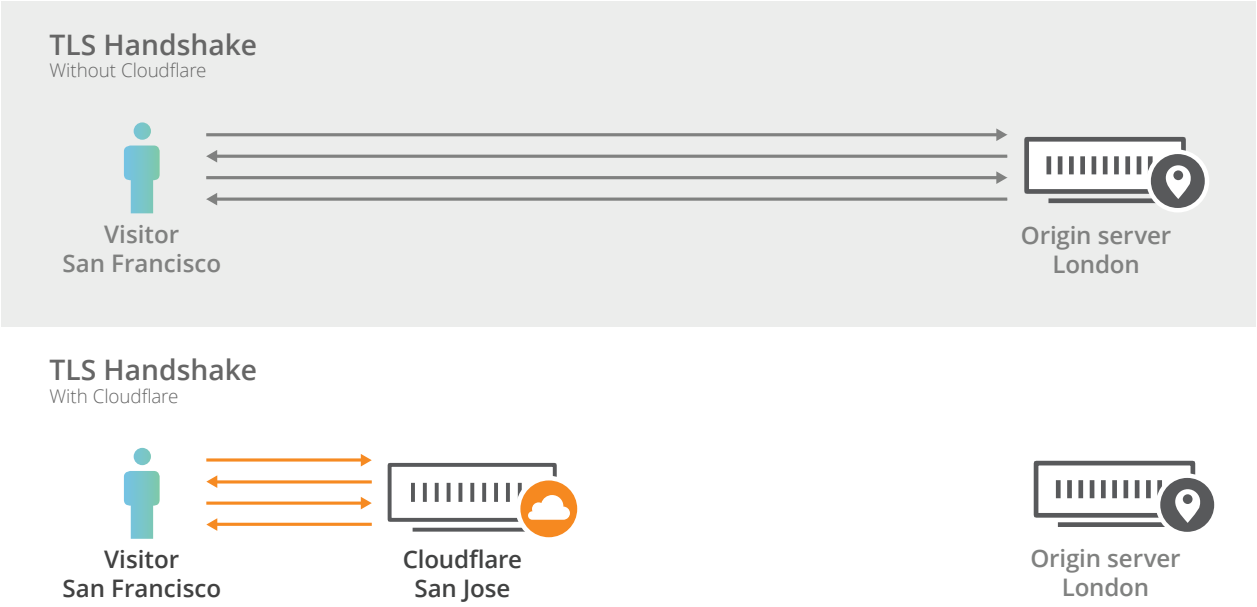
A CRL is a list of all revoked certificates. By requesting an updated list, a browser can verify that the certificate being used is valid. OCSP, on the other hand, only checks the validity of the certificate being used rather than the entire list. This method is preferable to CRL because less data needs to be sent and parsed by the browser.

Both of the CRL and OCSP security checks add latency to HTTPS request, but Cloudflare uses a technique called "OCSP stapling" to optimize this process. OCSP stapling reduces connection times by eliminating the need for browsers to check the revocation status of a certificate.

While OCSP Stapling is a great way to increase HTTPS performance, it's not widely supported by web servers. Part of the problem is that it often requires a significant technical investment by web administrators. While that investment may not make sense for many individual sites, Cloudflare is in a unique position to enable OCSP stapling for a large number of sites in one fell swoop.

Cloudflare's Globally Distributed Network

One of the easiest ways to reduce HTTPS latency is by moving servers closer to end users. Cloudflare's CDN ensures shorter distance between a web server and end users which speeds up the TLS handshake. For example, a TLS handshake taking place between a user in San Francisco and a server in London would have lots of latency because of the distance, but if the server is close to the visitor the latency is greatly reduced.



Cloudflare Handles HTTPS Operational Complexities

Along with making HTTPS fast using the latest technology, Cloudflare also makes HTTPS easy to implement by taking care of many of the operational complexities associated with TLS certificates.

One of the biggest hassles for companies wanting secure HTTPS traffic is dealing with TLS certificate and key management. Not only are TLS certificates expensive and time consuming to request, they can be difficult to install to secure traffic properly. With Cloudflare, you never have to worry about installing a certificate, and we take care of other issues as well:

- **Creating and storing keys** Once authentication and encryption keys are generated, they need to be safeguarded. If a server holding TLS keys is compromised and your keys are stolen, hackers could impersonate your site and decrypt your traffic giving them access to sensitive data like credit card numbers, medical information, and passwords. To protect against this vulnerability, Cloudflare holds TLS keys in an encrypted data store.
- **Multiple certificate and key management** If you have more than one website running on HTTPS, then you will be managing multiple certificates and multiple keys. This can get confusing, and any mixups will create browser errors that may give your users pause, or cause them to abandon your site entirely.
- **Certificate expiration** It's vital to keep track of when each TLS certificate expires. Expired certificate can cause system issues, and create a gap in security. Cloudflare keeps track of the certificates we have issued for our users and reissues them before they expire.

If you already have your own certificate, you can simply upload it to Cloudflare, and we'll take care of the rest. Otherwise, we will automatically issue you a new certificate.

Cloudflare's HTTPS is More Secure

By keeping up with up with industry best practices as they evolve, Cloudflare ensures the highest standard for HTTPS security.

When the POODLE vulnerability that targeted SSLv3 was announced, Cloudflare responded within an hour to disable SSLv3 by default across our entire network, keeping our customers protected from possible attacks.

Deprecating RC4

Most recently, we've deprecated RC4 and introduced the ChaCha/Poly1305 cipher suite. Cloudflare led the industry in doing away with RC4 and adopting the ChaCha/Poly to improve security and performance for mobile devices. To follow through with our mission to build a more secure web, we share our TLS configurations on GitHub and open-source our cryptographic contributions and cipher implementations.

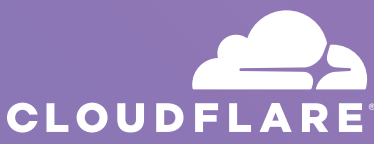
SHA-1 to SHA-2 migration

We plan to migrate SHA1 to SHA2 as our default signature algorithm in the fall of 2015. The leading browser providers—Google, Microsoft, and Mozilla—previously announced they would start sunsetting the SHA1 cryptographic signature algorithm because it no longer met their security requirements. In response to this announcement, Cloudflare will follow suit by serving the more secure SHA2 certificates when we detect visitors browsers can support this new standard. But when they can't, Cloudflare will instead "fall back" to SHA1 because we are committed to supporting HTTPS in all browsers, regardless of device or geographic location.

Extra Security with Keyless SSL

Cloudflare offers an added layer of security to HTTPS with our Keyless SSL technology. Keyless SSL allows TLS keys to be stored on machines administered by our customers, ensuring that if there are regulatory restrictions on sharing private keys, Cloudflares encryption technology is still an option.

The other customer benefit of Keyless SSL is that it lets sites use Cloudflare's HTTPS service while retaining on-premise custody of their private keys. This is a revolutionary solution for customers that have policies or technical obstacles preventing them from sharing their site's SSL key with Cloudflare.



1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com