Secure Content Delivery with Amazon CloudFront

Improve the Security and Performance of Your Applications, While Lowering Your Content Delivery Costs

November 2016

This paper has been archived.

For the latest technical content about secure content delivery with Amazon CloudFront, see https://docs-aws.amazon.com/whitepapers/latest/secure-content-delivery-amazon-cloudfront/secure-content-delivery-with-amazon-cloudfront.html

Archived

© 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Archived

Contents

Archived

Abstract

As companies respond to cybercrime, compliance requirements, and a commitment to securing customer data, their adoption of Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocols increases. This whitepaper explains how Amazon CloudFront improves the security and performance of your APIs and applications, while helping you lower your content delivery costs. It focuses on three specific benefits of using CloudFront: easy SSL adoption with AWS Certificate Manager (ACM) and Server Name Indication (SNI) Custom SSL support, improved SSL performance with SSL termination available at all CloudFront edge locations globally, and economical adoption of SSL, thanks to free custom SSL certificates with ACM and SNI support at no additional charge.

Archived

Introduction

The adoption of Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocols to encrypt Internet traffic has increased in response to more cybercrime, compliance requirements (PCI v3.2), and a commitment to secure customer data. A survey of the top 140,000 websites revealed that more than 40 percent were secured by SSL.[1]

As measured by Alexa (an amazon.com company), 32 percent of the top million URLs were encrypted using HTTPS (also called HTTP over TLS, HTTP over SSL, and HTTP Secure) in September 2016,[2] an increase of 45 percent from the same month in 2015. Amazon CloudFront is moving in this direction, with a rapidly increasing share of global content traffic on CloudFront delivered over SSL/TLS. CloudFront integrates with AWS Certificate Manager (ACM) for SSL/TLS-level support to ensure secure data transmission using the most modern ciphers and handshakes. Figure 1 shows how this secure content delivery works.

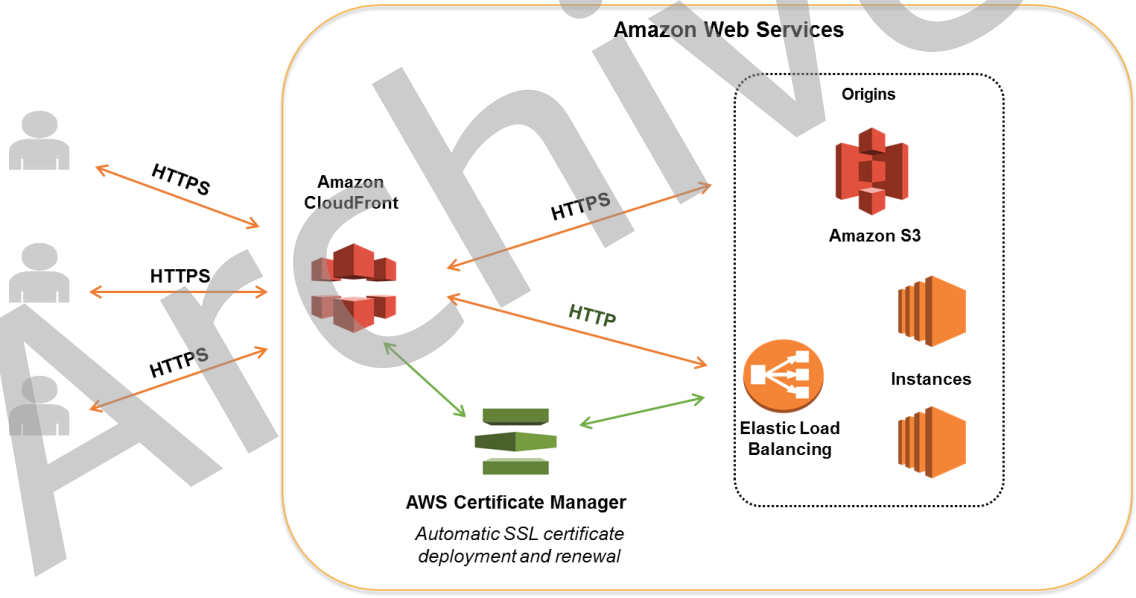

Figure 1: Secure content delivery with CloudFront and the AWS Certificate Manager

SSL/TLS on CloudFront offers these key benefits (summarized in Table 1):

- Ease of use
- Improved performance

Archived

- Lower costs

The integration of CloudFront with ACM reduces the time to set up and deploy SSL/TLS certificates, and translates to improved HTTPS availability and performance. Finally, certificates and encrypted data rates are offered at very low charge. These benefits are discussed in detail in the following sections.

Table 1: Summary of the key benefits of SSL/TLS on CloudFront

Ease of Use	Improved Performance	Lower Costs
Integrated with ACM • Procurement of new certificate directly from CloudFront console • Automatic certificate distribution globally • Automatic certificate renewal	SSL management in AWS environment	Free custom SSL/TLS certificate with ACM
	HTTPS capability at all global edge locations	SNI Custom SSL/TLS at no additional charge
Revocation management	SSL/TLS termination close to viewers	No setup fees, no hosting fees, and no extra charges for the HTTPS bytes transferred
SNI Custom SSL support	Latency reduction with Session Tickets and OCSP stapling	Standard (or discounted with a signed contract) CloudFront rates for data transfer and HTTPS requests
Support for standards (e.g., Apple iOS ATS and PCI)		

Archived

Enabling Easy SSL/TLS Adoption

All browsers have the capability to interact with secured web servers using the SSL/TLS protocol. However, both browser and server need an SSL certificate to establish a secure connection. Support for SSL certificate management requires working with a Certificate Authority (CA), which is a third-party that is trusted by both the subject of the certificate (e.g., the content owner) and the party that relies on the certificate (e.g., the content viewer). The entire manual process of purchasing, uploading, and renewing valid certificates through third-party CAs can be quite lengthy. AWS provides seamless integration between CloudFront and ACM to reduce the creation and deployment time of a new, free custom SSL certificate and make certificate management a simpler, more automatic process, as shown in Figure 2.

Custom SSL certificates allow you to deliver secure content using your own domain name (e.g., www.example.com). Although it typically takes a couple of minutes for a certificate to be issued after receiving approval, it could take longer.[3] Once a certificate is issued or imported into ACM, it is immediately available for use via the CloudFront console and automatically propagated to the global network of CloudFront edge locations when it is associated with distributions.

ACM automatically handles certificate renewal, which makes configuring and maintaining SSL/TLS for your secure website or application easier and less error prone than by using a manual process. In turn, this helps you avoid downtime due to misconfigured, revoked, or expired certificates. ACM-provided certificates are valid for 13 months and renewal starts 60 days prior to expiration. If a certificate is compromised, it can be revoked and replaced via ACM at no additional charge. AWS ensures that private keys are never exported, which removes the need to secure and track them.

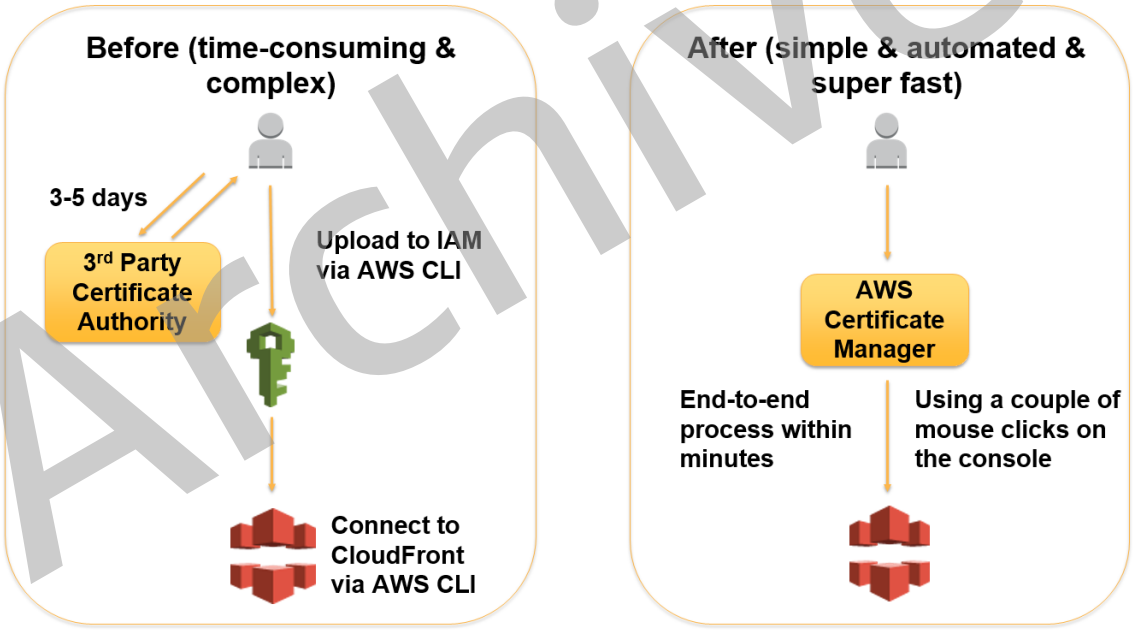

Figure 2: CloudFront integration with ACM

Using SSL Certificates with SNI Custom SSL

You can use your own SSL certificates with CloudFront at no additional charge with Server Name Indication (SNI) Custom SSL. SNI is an extension of the TLS protocol that provides an efficient way to deliver content over HTTPS using your

Archived

own domain and SSL certificate. SNI identifies the domain without the server having to examine the request body, so it can offer the correct certificate during the TLS handshake. SNI is supported by most modern browsers, including Chrome 6.0 and later, Safari 3.0 and later, Firefox 2.0 and later, and Internet Explorer 7 and later.[4] (If you need to support older browsers and operating systems, you can use the CloudFront dedicated IP-based custom SSL for an additional charge.)

Meeting Requirements for PCI Compliance and Industry Standard Apple iOS ATS

You can leverage the combination of ACM, SNI, and CloudFront security features to help meet the requirements of many compliance and regulatory standards, such as PCI. Additionally, CloudFront has "out-of-the-box" support for the industry standard Apple iOS App Transport Security (ATS). For more information on CloudFront security capabilities, see Table 2 and Table 3.

Table 2: Overview of CloudFront security capabilities

Vulnerability	CloudFront Security Capabilities
Cryptographic attacks	CloudFront frequently reviews the latest security standards and supports only viewer requests using SSL v3 and TLS v1.0, 1.1, and 1.2. When available, TLS v1.3 will also be supported. CloudFront supports the strongest ciphers (ECDHE, RSA-AES128, GCM-SHA256) and offers them to the client in preferential sequence. Export ciphers are not supported.
Patching	Dedicated teams are responsible for monitoring the threat landscape, handling security events, and patching software. Under the shared security model, AWS will take the necessary measures to remediate vulnerabilities with methods such as patching, deprecation, and revocation.
DDoS attacks	CloudFront has extensive mitigation techniques for standard flood-type attacks against SSL. To thwart SSL renegotiation-type attacks, CloudFront disables renegotiation.

Table 3: Amazon CloudFront support of Apple iOS ATS requirements

Apple iOS ATS Requirement	CloudFront Support
TLS/SSL version must be TLS 1.2	CloudFront supports TLS 1.2

Archived

Apple iOS ATS Requirement	CloudFront Support
TLS Cipher Suite must be from the following with Perfect Forward Secrecy:	CloudFront supports Perfect Forward Secrecy with the following ciphers:
ECDSA Certificates:	**RSA Certificates:**
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	
RSA Certificates:	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	
Leaf server certs must be signed with the following:	Server certificates signed with the following type of key:
Rivest-Shamir-Adleman (RSA) key with a length of at least 2048 bits	**Rivest-Shamir-Adleman (RSA) key** with a length of 2048 bits
Elliptic-Curve Cryptography (ECC) key with a size of at least 256 bits	

Archived

Improving Performance of SSL/TLS Connections

You may see a degradation in the performance of your API or application when clients connect directly to your origin servers using SSL. Setting up an SSL/TLS connection adds up to three round trips between the client and server, introducing additional latency in the connection setup. Once the connection is established, additional CPU resources are required to encrypt the data that is transmitted.

Terminating SSL Connections at the Edge

When you enable SSL with CloudFront, all global edge locations are used for handling your SSL traffic. Clients terminate SSL connections at a nearby CloudFront edge location, thus reducing network latency in setting up an SSL connection. In addition, moving the SSL termination to CloudFront helps you offload encryption to CloudFront servers that are specifically designed to be highly scalable and performance optimized.

These factors boost the performance of not only static content but also dynamic content. For example, Slack improved its performance when it migrated the delivery of its dynamic content to HTTPS with CloudFront. The worldwide average response time to slack.com dropped from 488 milliseconds to 199 milliseconds (see Figure 3). A large portion of these performance benefits came from the decreased SSL negotiation time, as the worldwide average for SSL connection times decreased from 215 milliseconds to 52 milliseconds.

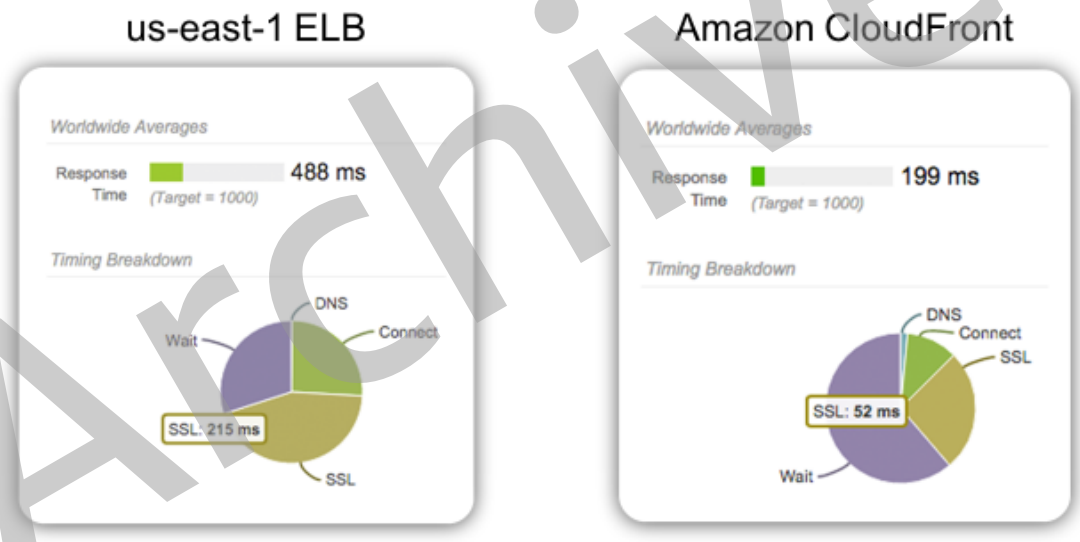

Figure 3: Slack improved its performance by delivering its dynamic content via HTTPS with CloudFront

Supporting Session Tickets and OCSP Stapling

CloudFront further improves the performance of SSL connections with the support of Session Tickets and Online Certificate Status Protocol (OCSP) stapling (see Figure 4). Session Tickets help decrease the time spent restarting or resuming an SSL session. CloudFront encrypts SSL session information and

Archived

stores it in a ticket that the client can use to resume a secure connection instead of repeating the SSL handshake process. OCSP stapling improves the time taken for individual SSL handshakes by moving the OSCP check (a call used to obtain the revocation status of an SSL certificate) from the client to a periodic, secure check by the CloudFront servers. With OCSP stapling, the CloudFront engineering team measured up to a 30 percent performance improvement in the initial connection between the client and the server.

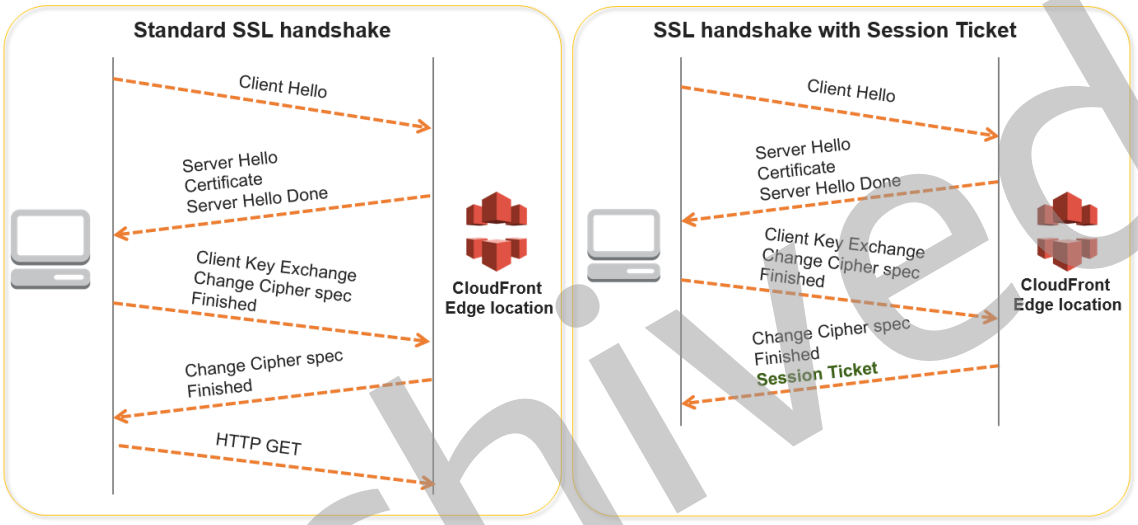

Figure 4: Session Tickets decrease the time spent restarting or resuming an SSL session

Balancing Security and Performance with Half Bridge and Full Bridge TLS Termination

With CloudFront, you can strike a balance between security and performance by choosing between half bridge and full bridge TLS termination (see Figure 5). By defining different cache behaviors in the same distribution, you can define which connections to the origin use HTTPS and which use HTTP. You can configure objects that need secure connections to the origin to use HTTPS (e.g., login pages, sensitive data), and configure objects that do not need secure connections to use HTTP (e.g., logos, images). Thus, everything can be securely transmitted to the client, and origin fetches can be optimized to use HTTP to reduce the overall latency of the transaction.

Archived

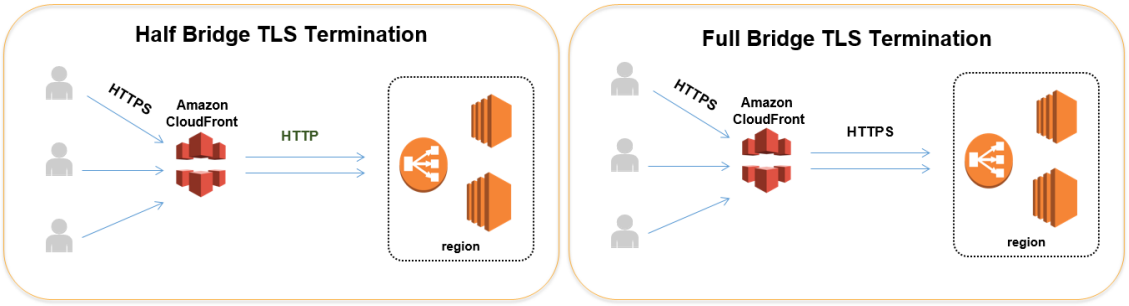

Figure 5: Balancing security and performance on the same distribution

For full secure delivery, you can configure CloudFront to require HTTPS for communication between viewers and CloudFront and, optionally, between CloudFront and your origin.[5] Also, you can configure CloudFront to require viewers to interact with your content over an HTTPS connection using the HTTP to HTTPS Redirect feature. When you enable HTTP to HTTPS Redirect, CloudFront will respond to an HTTP request with a 301 redirect response that requires the viewer to resend the request over HTTPS.

Ensuring Asset Availability

CloudFront puts significant focus on and dedication to maintaining the availability of your assets. Availability is calculated based on how often an attempt was made to download a single object and how often the download failed. As shown in Table 4, CloudFront SSL availability (as measured from real clients) across multiple regions is consistently high when compared to other top CDNs.[6]

Table 4: SSL/TLS traffic – availability by geography for July 2016 to August 2016

#	CDN	United States	Europe	Japan	Korea
1	CloudFront SSL	99.14	99.35	99.35	99.22
2	CDN A	98.70	97.53	98.64	98.98
3	CDA B	96.77	94.44	91.67	98.19

Making SSL/TLS Adoption Economical

CloudFront enables you to generate custom SSL/TLS certificates with ACM and support them with SNI at no additional charge. These features are offered with

Archived

no setup fees, no hosting fees, and no extra charges for the HTTPS bytes transferred. You simply pay standard (or discounted with a signed contract) CloudFront rates for data transfer and HTTPS requests. For more information, see the Amazon CloudFront pricing page.[7]

For dedicated IP custom SSL, there is an additional charge per month. This additional charge is associated with dedicating multiple IPv4 addresses (a finite resource) for each SSL certificate at each CloudFront edge location.

Conclusion

You can deliver your secure APIs or applications via SSL/TLS with Amazon CloudFront in an easy way, at no additional charge, and with improved SSL performance. You can create free custom SSL/TLS certificates with AWS ACM in minutes and immediately add them to your CloudFront distributions, at no additional charge, with automatic SNI support. You don't have to manage certificate renewal because ACM takes care of it automatically and, if any certificate is compromised, you can revoke it and replace it via ACM.

You can do all of this while benefiting from improved SSL/TLS performance because of SSL/TLS terminations near your end user, and CloudFront support of Session Tickets and OCSP stapling. This also applies if you want to deliver dynamic content, as CloudFront provides a way to increase performance and security at no additional charge.

Further Reading

There is a wealth of information available in the following whitepapers, blog posts, user guides, presentations, and slides to help customers get a deeper understanding of CloudFront, ACM, and how SSL is used.

Amazon CloudFront Custom SSL

- Amazon CloudFront Custom SSL
- List of browsers supported by SNI Custom SSL

AWS Certificate Manager

Archived

- Getting started
- Managed certificate renewal
- FAQs

Blogs

- Amazon CloudFront What's New
- HTTP and TLS v1.1 - v1.2 to the origin
- AWS Certificate Manager – Deploy SSL/TLS-Based Apps on AWS

Developers Guide

- Introduction to Amazon CloudFront
- Using an HTTPS Connection to Access Your Objects

Slack Performance Improvement with Amazon CloudFront

- Video
- Slides

re:Invent Presentations

- SSL with Amazon Web Services (SEC316) 11/2014
- Using Amazon CloudFront For Your Websites & Apps STG206 10/2015
- Secure Content delivery Using Amazon CloudFront STG205 10/2015

re:Invent Slides

- Secure Content Delivery Using Amazon CloudFront and AWS WAF

Archived

Notes

[1] https://www.trustworthyinternet.org/ssl-pulse/

[2] http://httparchive.org/trends.php#perHttps

[3] https://aws.amazon.com/certificate-manager/faqs/

[4] https://en.wikipedia.org/wiki/Server_Name_Indication

[5] http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/SecureConnections.html#SecureConnectionsHowToRequireCustomProcedure

[6] http://www.cedexis.com/get-the-data/country-report/?report=secure_object_delivery_response_time

[7] https://aws.amazon.com/cloudfront/pricing/

Archived