Forcepoint

Web Security Gateway

v8.5.x

Content Gateway SSL Certificate Verification

Revision A

Contents

Introduction

Content Gateway, the Forcepoint™ Web Security proxy component, includes support for decrypting, analyzing, and re-encrypting HTTPS (TLS/SSL) traffic as it transits the proxy. The feature must be enabled in the Content Gateway manager, otherwise HTTPS traffic is subject to only URL policy enforcement.

This article describes the most effective use of Certificate Verification Engine (CVE), a sub-component of Content Gateway TLS/SSL support. The CVE enables you to configure certificate verification to comply with your organization's IT security requirements.

For general information on SSL support, see Working with Encrypted Data in the Technical Library. Several articles follow in a sequence.

This guide includes the below topics:

Related concepts

SSL support and the Certificate Verification Engine (CVE) on page 3
CVE Best Practices on page 4
Certificate Verification Failures and Remediation Options on page 7
Frequently Asked Questions on page 15
Additional Resources on page 19

Related reference

Troubleshooting Certificate Verification Failures on page 11

Related information

Glossary on page 19

SSL support and the Certificate Verification Engine (CVE)

SSL and TLS are the standard protocols used by HTTPS to establish secure connections and transmit secure data on the Internet.

A primary feature of SSL/TLS is the connection handshake. At the onset of establishing an HTTPS connection, the certificate verification process verifies that the Certificate Authority (CA) certificates offered by the origin servers are legitimate and meet the configured set of verification conditions. See *Common verification checks*.

When the handshake is successful, a secure connection is established and encrypted content is passed.

To configure the CVE in the Content Gateway manager, go to **Configure** > **SSL** > **Validation** > **General**.

Important

Acquiring a complete understanding of the behavior of each option is the best way to achieve your certificate verification objectives.

For more information on CVE options, see Validating certificates.

Related concepts
Common verification checks on page 3

Common verification checks

Common verification checks include:

1) The certificate must be issued by a trusted Certificate Authority (CA).
2) The fully qualified hostname in the HTTPS request URL and the certificate owner (“Issued to” name) must match.
3) The certificate must be current (within its “Valid from...to...” date range).
4) The certificate must not be on a revocation list (either CRL or OCSP).
5) Checks 1-4 are recursively applied to every certificate in the trust chain.
6) The certificate is not self-signed.

Note

In the above list, quoted field names (“ ”) are those used by Internet Explorer.

Below is a certificate as it appears in Internet Explorer 11. The numbers in red correspond to checks in the preceding list.

CVE Best Practices

Certificate verification is essential to HTTPS security. If mismanaged, HTTPS security and the security of your network can be compromised and significantly weakened.

Certificate verification is an investment.

- Certificate checks fail in expected and intended ways when browsing to sites with CAs not known to Content Gateway. That's security. Regular, proactive user education helps users recognize and assess legitimate failures. See *Frequently Asked Questions* for a summary of information for users.
- *Certificate checks may also fail in unexpected ways* that also require user education, as well as administrative effort in the form of investigation and remediation.

When using SSL certificate verification, therefore, you need to know:

- Your organization's certificate verification requirements as they pertain to your IT security policy.
- Your organization's ability and willingness to manage the administrative burden. When verification fails and there is no remediation in place, the connection request is dropped and users often call HelpDesk. Some failures will require administrator investigation and remediation.

To administer certificate verification, you need to:

- Know which failures legitimately protect your network
- Know how to investigate failures
- Determine which failures are undesirable and can be remediated (certificate replacement, verification bypass, other)
- Educate users about SSL connection failures, what they look like, and why they occur
- Anticipate more HelpDesk calls

Important

You should **not** use Content Gateway to proxy internal traffic.

However, if you do, before enabling the CVE, audit your internal HTTPS servers to ensure that their certificates are valid and trusted by Content Gateway.

If you plan to use the CVE, be sure to acquaint yourself with these topics:

- *Troubleshooting Certificate Verification Failures*
- *Certificate Verification Failures and Remediation Options*

Related concepts

Frequently Asked Questions on page 15
Certificate Verification Failures and Remediation Options on page 7

Related reference

Troubleshooting Certificate Verification Failures on page 11

CVE configurations

Before you begin

This section describes a phased approach to deploying certificate verification. It is recommended that in addition to the production environment, Content Gateway be installed in a controlled test environment in which phased configuration can be tested and monitored, and problems remediated and tested again. When the test environment is functioning as desired, the configuration can be rolled out to the production environment with continued monitoring and testing. The starting point assumes that Content Gateway is stable and SSL support is off.

The phases of SSL and CVE deployment include:

Steps

1) Enabling SSL support.
   This automatically enables the options for certificate verification engine (CVE), verification of the entire certificate chain, and denial of self-signed certificates.

2) Adding CVE checks to the configuration as needed.
   The entire certificate chain is validated for each CVE check enabled.

Enabling SSL support

Before enabling SSL support, verify that Content Gateway:

- Is installed in a supported environment that includes a network test segment
- Is passing explicit or transparent traffic as expected
- Is integrated and tested with Forcepoint Web Security
  - Policies are configured
  - Scanning (analytic) options are configured
  - HTTP requests are handled as expected
  - Policy is being enforced as expected
- Is stable:
  - Content Gateway performance monitoring graphs show a predictable ramp up in traffic with no unexplained traffic spikes
  - All mission critical websites and web-hosted applications have been validated to work properly through the proxy, or acceptable bypasses are in place

When the above conditions are met:

- Enable SSL support.
- Confirm that HTTPS traffic is passing through Content Gateway.
- Verify that clients are not receiving certificate errors in the browser. If they are, see these instructions on installing the Internal Root CA.
- Test by accessing several sites that are commonly used in your organization.
- Test by using HTTPS-based applications that are commonly used in your organization. See these articles for information about common problems.
  - Dropped HTTPS connections

  - Websites that have difficulty transiting Content Gateway
- Send a representative sample of traffic into the test environment with the objective of uncovering as many HTTPS traffic problems as possible.
- When the environment is stable, proceed to *Enabling the CVE*.

Related concepts
Enabling the CVE on page 6

Enabling the CVE

Now that SSL support is on and stable, with **Deny self-signed certificates** and **Verify entire certificate chain** enabled, enable the CVE with CRL checking enabled. The CRL check is an essential certificate verification check that rarely fails in error.

Repeat the testing performed after SSL was enabled.

Note

If a certificate fails because it is on a revocation list, a fast and easy way to confirm the revocation status is to use a web-hosted certificate verification tool. Using a browser and a common Search site, search for “SSL checker”.

Select a site that you trust and enter the exact URL of the site that failed.

At this stage, to minimize disruption to users, you may also want to enable Verification Bypass. See *CVE with Verification Bypass enabled*.

Related concepts
CVE with Verification Bypass enabled on page 7

Adding CVE checks to the configuration

When you are satisfied with certificate verification using **Deny self-signed certificates** and **Verify entire certificate chain** with the CRL check, you can start to enable additional verification options. Enable options one at a time and repeat the same testing procedures.

Note

If you are following the recommended steps, “Check certificate revocation by CRL” is already enabled.

For each option enabled, when there is a certificate verification failure, an incident is added to the Incident List. Begin troubleshooting by examining the Incident List. See *Troubleshooting Certificate Verification Failures*.

Important

To reduce administrative overhead, do not enable checks that aren’t required by your IT security policy.

For more information on CVE options, see Validating certificates.

Related reference
Troubleshooting Certificate Verification Failures on page 11

CVE with Verification Bypass enabled

In addition to the verification options, SSL support includes an option for Verification Bypass (**Configure > SSL > Validation > Verification Bypass**). This feature is turned on by default and means that when certificate verification fails, a dialog box warns the user that a failure has occurred and gives the user the option to go to the site anyway.

Advantages include:

- Certificate verification is performed and incidents are logged, but users aren't blocked. Users are allowed to make the decision about whether a site is safe.
- Administrators can see how the CVE affects the network before allowing it to impact users or require an administrator response.
- By monitoring the Incident List, administrators can put remediation measures in place before enforcing certificate verification and impacting users.
- Verification bypass provides a response to users that is much like the warning dialogs used by common browsers.

Disadvantages include:

- Security is compromised because the choice to drop the connection is given to the user.
- In cases where the HTTPS request is for an object embedded in the page or in another page, and its certificate verification fails, the bypass page may not render.

Certificate Verification Failures and Remediation Options

When certificate verification fails, an access denied message is displayed to the user and an incident is recorded in the SSL Incident List.

If the CVE blocks access to a site believed to be safe, the administrator should research the failure in the Incident List, and may want to research the status of the destination host.

Certificate verification failures occur for the following reasons:

Important

The failures you see at your site will depend, in part, on the CVE options you have enabled.

1) A certificate that was not issued by a CA in Content Gateway's trusted CA list; this is often a self-signed certificate

2) A certificate that was not issued by a CA that is trusted by the destination server

3) A revoked CA (on a CRL or OCSP list)

4) An expired or not yet valid certificate

5) An expired, not yet valid, or revoked certificate in the certificate chain

6) A self-signed certificate in the chain

7) A name mismatch between the hostname and URL, or similar (hostname and the Common Name, hostname and the Subject Alternative Name; hostname and use of a wildcard in the certificate)

8) Missing and/or optional fields in the certificate (no CRL or OCSP state; result in “Unknown revocation state” errors)

9) A problem in the logic of the CVE

List of common certificate verification error messages

See the *Troubleshooting Certificate Verification Failures* section for more information on each of these errors.

1) CA explicitly denied

2) Certificate has expired

3) Certificate is not yet valid

4) Certificate revoked

5) Client certificate requested

6) Common Name does not match URL

7) Invalid CA certificate

8) Self-signed certificate

9) Self-signed certificate in certificate chain

10) Unable to get local issuer certificate

11) Unable to verify the first certificate

12) Unknown revocation state

Related reference
Troubleshooting Certificate Verification Failures on page 11

Remediation

Certificate verification failures can be remediated in several ways.

Important

The SSL Incident List is the primary vehicle for investigating verification failures. To effectively use the CVE, administrators must become fluent with the Incident List facility. Help system information starts here.

The primary remediation options include:

1) Correcting the certificate problem. See *Troubleshooting Certificate Verification Failures* and *SSL trusted certificate store*.
2) Bypassing certificate verification via SSL Decryption bypass, the SSL Incident List, or another bypass option. See *Bypass options*.
3) Enabling or disabling CVE options.
4) Using the **CVE Verification Bypass** option to give users the ability to proceed to a site after certificate verification fails.

Related concepts
SSL trusted certificate store on page 9
Bypass options on page 10

Related reference
Troubleshooting Certificate Verification Failures on page 11

SSL trusted certificate store

When Content Gateway is installed, Certificate Authorities trusted by Mozilla Firefox and Microsoft Internet Explorer, and Apple Safari are included in the SSL trusted certificate store.

The list is accessed in the Content Gateway manager on the **Configure** > **SSL** > **Certificates** > **Certificate Authorities** tab.

Content Gateway trusts web servers that offer these certificates. Note that a lowercase “i” appears before the name of some certificates validated via CRL (certificate revocation lists) or OCSP (online certification status protocol). These certificates provide URLs where their revocation status can be verified. See Keeping revocation information up to date .

You can manually add, delete, or change the status of a certificate. Help system information on SSL certificate management starts here.

SSL transaction logging

SSL transaction logs are sent to the same systems logs as those used by HTTP. Content Gateway transaction logging is described here.

Bypass options

Bypass is the term used to describe several methods of specifically allowing a request to circumvent (bypass) all or select features of Content Gateway. Full proxy bypass is often called tunneling.

In this discussion take note of when bypass affects:

- Only certificate verification
- Certificate verification and SSL decryption
- Complete bypass of Content Gateway

These are the primary bypass methods:

- SSL decryption bypass (category, client IP addresses, and destination hostname/IP address); SSL decryption bypass is configured in the Web module of Forcepoint Security Manager
- The Content Gateway SSL Incident List
- Content Gateway ARM bypass (transparent proxy)
- Explicit proxy PAC file bypass
- Transparent proxy routing device ACL bypass
- Allow users to continue after verification failure (**Configure** > **SSL** > **Validation** > **Verification Bypass**)

SSL Decryption Category bypass and Hostname/IP address bypass

In the Web module of Forcepoint Security Manager you can specify categories, client IP addresses, or destination hostname/IP addresses of websites for which SSL decryption and inspection are not performed. See SSL Decryption Bypass.

The SSL Incident List

The SSL Incident List is the principal SSL decryption and certificate verification bypass mechanism in Content Gateway. In addition to automatically adding certificate verification failures (incidents) to the list, administrators can manually add destination URLs.

Administrators should set “Action:Allow” to bypass certificate verification (the check is made but has no effect). Administrators should use “Action:Tunnel” to bypass certificate verification and SSL decryption. See Managing Web HTTPS site access.

Content Gateway ARM bypass

See Interception bypass.

Explicit proxy PAC file bypass

See:

- How do I specify in a PAC file a URL that will bypass Content Gateway?
- PAC File Best Practices

Transparent proxy Access Control List (ACL) bypass

See the vendor documentation for your transparent routing device.

SSL Verification Bypass

See SSL Verification bypass.

Troubleshooting Certificate Verification Failures

This section describes how to use resources in Content Gateway and on your PC to troubleshoot certificate verification failures.

As new information becomes available, updated Troubleshooting information will be posted online to Troubleshooting for Certificate Verification.

Note

Several websites offer excellent online SSL checkers that diagnose problems with SSL certificates installed on web servers. To access one of those tools, in a browser go to a Search service and search for “SSL checker”.

When a failure occurs:

1) Note the incident ID and URL in the block page displayed to the user.

2) Log on to the Content Gateway manager and go to **Configure** > **SSL** > **Incidents** > **Incidents List**.

3) Search for the incident ID and verify the URL.

4) In the Message field, click the magnifying glass to view the complete details. It is important to note the “depth=” value as it indicates the location within the certificate chain where the error occurred.

If the message is:

Message	Description & Action
Certificate is not yet valid	The certificate's "Valid from" date is in the future. Verify the failure by accessing the same URL without Content Gateway and check the "Valid from ---- to " fields. The "Valid from" date should be a date in the future. If the **Verify entire certificate chain** option is enabled, the "Valid from" date of every certificate in the chain may have to be checked. Look for the "depth=" value in the error message for the level in the chain at which the error occurred. **Note:** Also check that the time and date are set correctly on the Content Gateway host system. To check the time in the Content Gateway manager, go to **Monitor** > **My Proxy** > **Alarms**.
Certificate has expired	The certificate's "Valid to" date is in the past. Verify the failure by accessing the same URL without Content Gateway and check the "Valid from ---- to " fields. The "Valid to" field should be a date in the past. If the **Verify entire certificate chain** option is enabled, the expiration date of every certificate in the chain may have to be checked. Look for the "depth=" value in the error message for the level in the chain at which the error occurred.
Self-signed certificate	The offered certificate is self-signed and the same certificate cannot be found in the list of trusted certificates. Verify the failure by accessing the same URL without Content Gateway. The browser should display the same error.

Message	Description & Action
Self-signed certificate in certificate chain	The certificate chain cannot be built up due to an untrusted self-signed certificate, or the root CA is not yet added to the CA tree. To verify if the failure is due to an untrusted self-signed certificate in the chain, access the URL without Content Gateway to produce the same error. When a certificate is signed by its own issuer, it is assumed to be the root CA. Verify if the root CA is listed on the CA tree by going to **Configure** > **SSL** > **Certificates**. This is a common error, especially with network equipment that includes HTTPS management interfaces. If the devices are internal to your network, you may want to bypass proxying altogether. To resolve the issue, you have to import a certificate from a trusted source.
Unable to get local issuer certificate	The issuer certificate of an untrusted certificate cannot be found. When this failure occurs, the error message displays “depth= 0”, which indicates that the problem is the peer or local issuer certificate. A trusted CA certificate (depth= 1) is required. Investigate the problem by accessing the site without Content Gateway and view the certificate in the browser. To identify the certificate from the Certification Path that does not appear in the CA tree, look up one level in the chain. Then, compare the identified certificate to the CA tree to verify the missing certificate (**Configure** > **SSL** > **Certificates**). Make a copy of the missing certificate and add it to the trusted certificate tree. See *How do I copy a certificate from my browser to the CA tree?* Remove the incident from the Incident List and then access the site again to confirm that the failure is cleared.
Unable to verify the first certificate	The certificate could not be verified because the Certification Path (certificate chain) contains only one certificate and it is not self- signed. To verify the failure, access the site without Content Gateway, examine the certificate, and verify that the Certification Path includes only 1 certificate and that it is not self-signed. The root CA that signed the certificate must be part of the chain to avert this error.

Message	Description & Action
Certificate revoked	The certificate has been revoked. This is a serious security alert. Content Gateway has learned via the CRL or OCSP that the Certificate Authority that signed the certificate has revoked the certificate. A Web search can lead to good information about why the certificate was revoked. To verify the failure, access the site without Content Gateway. The browser should encounter the same error. Also, submit the URL to a web-hosted SSL certificate checking tool.
Invalid CA certificate	The certificate is invalid. Either the certificate is not a CA or its extensions are not consistent with the supplied purpose.
Common Name does not match URL	The Common Name of the certificate does not match the specified URL. Due to the way that certificates are constructed and URLs specified, this can be a common error. To verify the failure, access the site without Content Gateway, open the certificate, and verify that the Common Name or Subject Alternative Name, if present, does not match the fully qualified hostname in the URL. If your IT security policy permits it, it may work best to configure Verification Bypass to allow your users to bypass the warning at their discretion. Forcepoint Web Security has additional protections to detect if websites are being impersonated. The SSL Verification Bypass feature only allows the user to continue to the site. Web protection features of Forcepoint Web Security are not bypassed by this feature.
Unknown revocation state	A common error when OCSP verification is enabled. To verify the failure, access the site with an OCSP-supported browser and without Content Gateway. The error should occur.

Message	Description & Action
CA explicitly denied	A new CA was added to the CA tree, but is explicitly denied by Content Gateway. To verify and remediate the condition, log on to the Content Gateway manager and go to **Configure** > **SSL** > **Certificates** > **Certificates Authorities**. The new CA should be listed with a red cross to the left. This CA was offered as part of the SSL handshake and added to the CA tree with the status: untrusted. After validating the CA with Content Gateway, set the allow or deny status. From the **Certificate Authorities** page, select the CA to view the deny and allow options. If you elect to allow the CA, delete the incident and go to the site to verify access.
Client certificate requested	The destination server requires a client certificate. To verify the failure, access the site without Content Gateway and confirm that the origin server is requesting a client certificate. **Note:** When a client certificate is required, there is an option to bypass the client certificate. The default bypass option is to create an incident by going to the **SSL** > **Client Certificates** > **General page**.

Related tasks

How do I copy a certificate from my browser to the CA tree? on page 18

Frequently Asked Questions

Related concepts

Why am I getting so many incidents? on page 16
How do I know which certificate verification failures are problems that need a response? on page 16
What are the best troubleshooting techniques for certificate verification failures? on page 16
How do I view a certificate in my browser? on page 16
Why do some HTTPS sites not load properly? on page 17
What do my users need to know about HTTPS certificate verification? on page 18

Related tasks

How can I make best use of the Incident List? on page 17
How do I copy a certificate from my browser to the CA tree? on page 18
How do I check and update a CRL link? on page 18

Why am I getting so many incidents?

The answer requires analysis of the SSL Incident List. See *Troubleshooting Certificate Verification Failures*. Take into consideration that strict verification configurations may generate a significant number of incidents.

Related reference
Troubleshooting Certificate Verification Failures on page 11

How do I know which certificate verification failures are problems that need a response?

You need to become familiar with all of the types of failures that can occur and their causes. See *Troubleshooting Certificate Verification Failures* to verify certificate verification failures. Should a failure be deemed an error, or the destination server be deemed safe or necessary, see *Certificate Verification Failures and Remediation Options* for a list of remediation alternatives.

Related concepts
Certificate Verification Failures and Remediation Options on page 7

Related reference
Troubleshooting Certificate Verification Failures on page 11

What are the best troubleshooting techniques for certificate verification failures?

See *Troubleshooting Certificate Verification Failures*.

Related reference
Troubleshooting Certificate Verification Failures on page 11

How do I view a certificate in my browser?

In Firefox, click the menu icon in the upper right corner and navigate to **Options** > **Advanced** > **Certificates**. Click **View Certificates**.

In Internet Explorer 11, click on the gear in the upper right and navigate to **Internet Options** > **Content** > **Certificates**.

How can I make best use of the Incident List?

Steps

1) Review the section in this paper titled *The SSL Incident List*. Follow the link to *Managing Web HTTPS site access* to review information for administrators in the Content Gateway Help system.

2) The number of incidents automatically created by certificate verification failures depends on the CVE options enabled and peculiarities of the sites your users visit. For more about CVE options, see Validating certificates.

3) If you have several individual sites on the Incident List and some of those sites have certificates signed by the same new root CA, you could trust the CA that they have in common and delete the individual site entries, thus keeping the Incident List as small as possible.

4) Do **not** add "*.*" as "Action:Tunnel". This has the effect of tunneling all HTTPS traffic, which subverts the purpose of SSL support and creates a lot of unnecessary overhead.

Related concepts
The SSL Incident List on page 10

Why do some HTTPS sites not load properly?

HTTPS pages can fail to load, or only partially load, for many reasons.

Here is a set of frequently accessed HTTP and HTTPS sites that often cause problems with Web proxy servers, including Content Gateway. Affected sites include:

- Microsoft Update
- Skype
- WebEx
- Real Networks Real Player
- Citrix collaboration products
- Firefox Update
- Yahoo! Messenger with Pidgin messaging client
- Logitech Messenger Agent and VirtualBox

Here are 2 Technical Library articles that discuss these problem sites:

- Dropped HTTPS connections
- Websites that have difficulty transiting Content Gateway

What do my users need to know about HTTPS certificate verification?

Explain to them that:

- HTTPS is designed to provide secure connections and transmission of data.
- HTTPS sites, connections, and transmission of data are vulnerable to attack and compromise.
- A key element of HTTPS security is the exchange of signed digital certificates.
- When an HTTPS connection is being established, certificate verification is performed to validate the authenticity of the responding website, which protects you and your network.
- Sometimes certificate verification checks fail, usually for valid reasons.
- Sometimes certificate verification checks fail in error, or for obscure reasons that your administrator will have to investigate.
- In most cases, certificate verification failure will block you from accessing the site.
- If your connection request fails due to a certificate verification failure, look carefully at the URL you are requesting to ensure that it does not have any typos.
- Ask a colleague if she or he is experiencing the same problem. If other colleagues are not, see if you can determine why not (what's different). If other colleagues are, report the problem to your HelpDesk.

How do I copy a certificate from my browser to the CA tree?

Steps

1) From the certificate window in your browser, select and open the desired certificate. Then, select the **Details** tab.

2) Select **Copy to File** to open the Certificate Export Wizard, then select **Next**.

3) Select **Base-64 encoded x.509 (.CER)**. Then, select **Next**.

4) Choose a file name and location to save the certificate. Then, select **Next**.

5) Select **Finish**.

6) Import the certificate to the CA tree from its save location by going to **Configure** > **SSL** > **Certificates** > **Add Root CA**.

How do I check and update a CRL link?

Steps

1) Go to the CA Tree (**Configure** > **SSL** > **Certificates** > **Certificate Authorities**).

2) Select the site to view or update the CRL link. To update the CRL link, click **Edit**.

3) Click **Submit** to save your changes.

Additional Resources

- HTTP Secure (Wikipedia)
- Transport Layer Security (Wikipedia)
- Digital Certificates (Microsoft)
- The First few Milliseconds of an HTTPS Connection

Below is a sample of online TLS/SSL certificate checking tools. For more, use an Internet Search tool and search for “SSL checker”.

- http://www.sslshopper.com/ssl- checker.html
- http://www.digicert.com/help/
- http://www.geocerts.com/ssl_checker

Glossary

Certificate Revocation List (CRL)

The Certificate Revocation List is used to check a certificate’s revocation state and includes a list of certificates that have been issued and subsequently revoked by a given Certification Authority (CA).

Certificate Verification Engine (CVE)

The Certificate Verification Engine verifies certificates and checks for revoked certificates within Content Gateway.

Common Name (CN)

A Common Name is composed of the host + domain name that is used to identify the location being accessed.

Explicit proxy

An explicit proxy is configured within the application and is visible to the client. The client is explicitly configured to use a proxy server in which the browser knows that all requests will go through the proxy. Unlike Transparent proxy, each desktop must be configured to run explicit proxy.

Online Certificate Status Protocol (OCSP)

The Online Certificate Status Protocol is used to check a certificate's revocation state and can be used separately or as a backup in conjunction with CRL. This allows the end host to query the OCSP server about a certificate's revocation state at the time the certificate is presented.

Secure Sockets Layer (SSL)

Secure Sockets Layer is the standard security technology for establishing an encrypted connection between a Web server and a browser. This connection ensures that all data passed between the Web server and browser remains private and protected.

Server Name Indication (SNI)

The Server Name Indication (SNI) indicates what hostname the client is attempting to connect to at the start of the handshaking process. SNI allows multiple secure sites to be served off of the same IP address without requiring those sites to use the same certificate.

Subject Alternative Name (SAN)

Subject Alternative Names protect multiple hostnames with a single certificate after specifying a list of hostnames to be protected.

Transparent proxy

A transparent proxy is not configured within the application and is not visible to the client. The client does not know the traffic is being processed by a proxy other than the origin server. Unlike Explicit proxy, a transparent proxy typically intercepts all of the traffic for all IP addresses on a specified port.

Transport Layer Security (TLS)

Transport Layer Security (TLS), successor to Secure Sockets Layer (SSL), is the protocol that provides secure HTTP (HTTPS) for Internet transactions between Web browsers and Web servers.

Uniform Resource Identifier (URI)

A Uniform Resource Identifier (URI) identifies points of content such as a page of text, a video, a sound clip, a still or animated image, or a program.

Uniform Resource Locator (URL)

Uniform Resource Locator is the unique address for a website or file that is accessible on the Internet.

Web Cache Communication Protocol (WCCP)

Web Cache Communication Protocol (WCCP) transparently redirects users to cache servers without having to configure proxy settings in their browsers.

Published 05 August 2024