SonicWall® Global Management System DPI-SSL

Administration

Contents

Configuring Client DPI-SSL Settings 2

Configuring General Settings 2

Selecting the Re-Signing Certificate Authority 4

Configuring Exclusions and Inclusions 5

Excluding/Including Objects/Groups 6

Excluding/Including by Common Name 7

Specifying CFS Category-based Exclusions/Inclusions 9

Client DPI-SSL Examples 10

Content Filtering 10

App Rules 12

Configuring Server DPI-SSL Settings 13

Configuring General Server DPI-SSL Settings 14

Configuring Exclusions and Inclusions 14

SonicWall Support 18

About This Document 19

Configuring Client DPI-SSL Settings

The Client DPI-SSL deployment scenario typically is used to inspect HTTPS traffic when clients on the LAN browse content located on the WAN. In this scenario, the firewall typically does not own the certificates and private keys for the content it is inspecting. After performing DPI-SSL inspection, the appliance re-writes the certificate sent by the remote server and signs this newly generated certificate with the certificate specified in the Client DPI-SSL configuration. By default, this is the firewall certificate authority (CA) certificate, but a different certificate can be specified. Users should be instructed to add the certificate to their browser's trusted list to avoid certificate trust errors.

Topics:

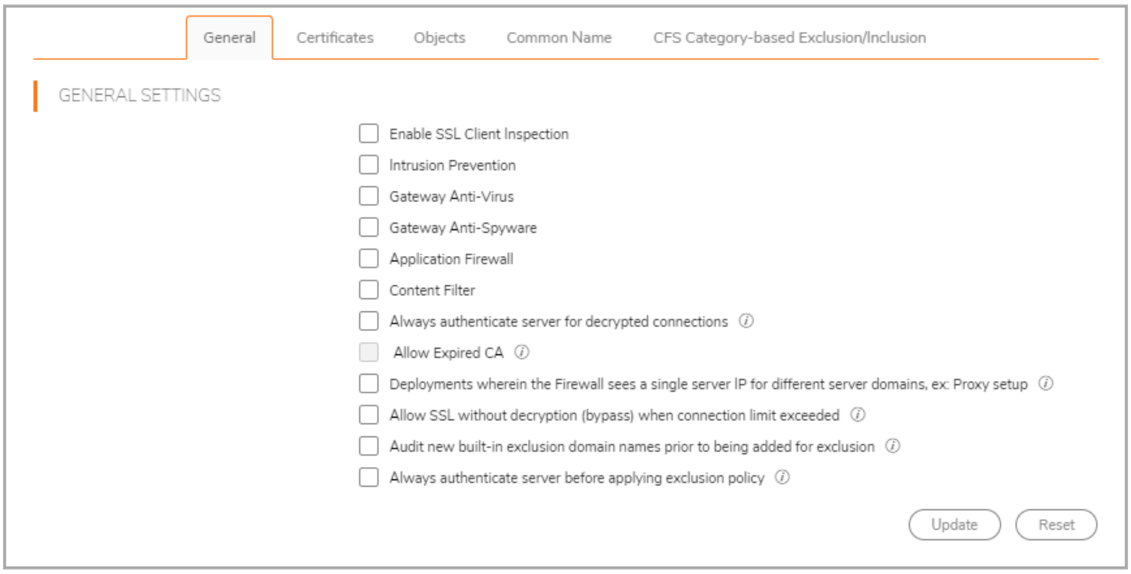
- Configuring General Settings
- Selecting the Re-Signing Certificate Authority
- Configuring Exclusions and Inclusions
- Client DPI-SSL Examples

Configuring General Settings

To enable Client DPI-SSL inspection:

1 Navigate to the **DPI-SSL > Client SSL | General** page.

2 In the **General Settings** section,



□ Enable SSL Client Inspection
□ Intrusion Prevention
□ Gateway Anti-Virus
□ Gateway Anti-Spyware
□ Application Firewall
□ Content Filter
□ Always authenticate server for decrypted connections
□ Allow Expired CA
□ Deployments wherein the Firewall sees a single server IP for different server domains, ex: Proxy setup
□ Allow SSL without decryption (bypass) when connection limit exceeded
□ Audit new built-in exclusion domain names prior to being added for exclusion
□ Always authenticate server before applying exclusion policy

3 Select **Enable SSL Client Inspection**. By default, this checkbox is not enabled.

4 Select one or more of the following services with which to perform inspection; none are selected by default:

- **Intrusion Prevention**
- **Gateway Anti-Virus**
- **Gateway Anti-Spyware**
- **Application Firewall**
- **Content Filter**

5 To authenticate servers for decrypted/intercepted connections, select **Always authenticate server for decrypted connections**. When enabled, DPI-SSL blocks those connections:

- To sites with untrusted certificates.
- If the domain name in the Client Hello cannot be validated against the Server Certificate for the connection.

By default, this checkbox is not enabled.

ⓘ **IMPORTANT:** Only enable this option if you need a high level of security. Blocked connections show up in the connection failures list, as described in Specifying CFS Category-based Exclusions/Inclusions.

ⓘ **TIP:** If you enable this option, use the **Skip CFS Category-based Exclusion** option (see Excluding/Including Common Names) to exclude a particular domain or domains from this global authenticate option. This is useful to override any server authentication-related failures of trusted sites.

6 To disable use of the server IP address-based dynamic cache for exclusion, select **Deployments wherein the Firewall sees a single server IP for different server domains, ex: Proxy setup**. By default, this checkbox is not enabled.

This option is useful for proxy deployments, where all client browsers redirect to a proxy server, including if appliance is between the client browsers and the proxy server. All DPI-SSL features are supported, including domain exclusions when the domain is part of a virtual hosting server, as part of a server farm fronted with a load balancer, or in some cloud deployments, wherein the same server IP can be used by multiple domains.

In such deployments, all server IPs as seen by the appliance are the proxy server's IP. It is, therefore, imperative that in proxy deployments, IP-based exclusion cache is disabled. Enabling this option does not affect the capability of the GMS to perform exclusions.

7 By default, new connections over the DPI-SSL connection limit are bypassed. To allow new connections to bypass decryption instead of being dropped when the connection limit is exceeded, select **Allow SSL without decryption (bypass) when connection limit exceeded**. This option is not enabled by default.

To ensure new connections over the DPI-SSL connection limit are dropped, deselect/disable this checkbox.

8 To audit new, built-in exclusion domain names before they are added for exclusion, select **Audit new built-in exclusion domain names prior to being added for exclusion**. By default, this checkbox is not enabled.

When this option is enabled, whenever changes to the built-in exclusion list occur, for example, an upgrade to a new firmware image or other system-related actions, a notification pop-up dialog displays over the **Client SSL** page with the changes. You can inspect/audit the new changes and accept or reject any, some, or all of the new changes to the built-in exclusion list. At this point, the run-time exclusion list is updated to reflect the new changes.

If this option is disabled, the GMS accepts all new changes to the built-in exclusion list and adds them automatically.

9 To always authenticate a server before applying a common-name or category exclusion policy, select **Always authenticate server before applying exclusion policy**. When enabled, DPI-SSL blocks excluded connections:

- To sites with untrusted certificates.
- If the domain name in the Client Hello cannot be validated against the Server Certificate for the connection.

This is a useful feature to authenticate the server connection before applying exclusion policies. Enabling this option ensures that the appliance does not blindly apply exclusion on connections and thereby create a security hole for exclusion sites or sites belonging to excluded categories. This is especially relevant when banking sites, as a category, are excluded.

By validating both the server certificate and the domain name in the Client Hello before applying an exclusion policy, the GMS can reject untrusted sites and potentially block a type of zero-day attack from taking place. The GMS implementation takes the “trust-but-verify” approach to ensure that a domain name that matches the exclusion policy criteria is validated first, thus preventing an unsuspecting client from phishing or URL-redirect-related attacks.

By default, this checkbox is not enabled.

ⓘ **IMPORTANT:** If you are excluding alternate domains in the Subject-Alternate-Name extension, it is recommended that you enable this option.

ⓘ **TIP:** If you enable this option, use the **Skip CFS Category-based Exclusion** option (see Excluding/Including Common Names) to exclude a particular domain or domains from this global authenticate option. This is useful to override any server authentication-related failures of trusted sites.

10 Click **Update**.

Selecting the Re-Signing Certificate Authority

The re-signing certificate replaces the original certificate signing authority only if that authority certificate is trusted by the firewall. If the authority is not trusted, then the certificate is self-signed. To avoid certificate errors, choose a certificate that is trusted by devices protected by DPI-SSL.

ⓘ **NOTE:** For information about requesting/creating a DPI SSL Certificate Authority (CA) certificate, see the Knowledge Base article, *How to request/create DPI-SSL Certificate Authority (CA) certificates for the purpose of DPI-SSL certificate resigning* (SW14090).

To select a re-signing certificate:

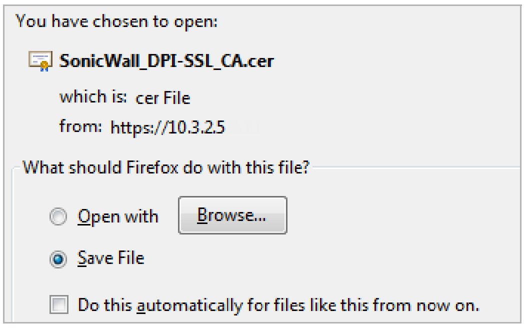
1 Navigate to the **DPI-SSL > Client SSL | Certificates** page.

2 Scroll to the **Certification Re-signing Authority** section.

3 Select the certificate to use from the **Certificate** drop-down menu. By default, DPI-SSL uses the **Default SonicWall DPI-SSL CA certificate** to re-sign traffic that has been inspected.

4 To download the selected certificate to the firewall, click the **(download)** link. The **Opening *filename*** dialog appears.

> **TIP:** To view available certificates, click on the **(Manage Certificates)** link to display the **System > Certificates** page.



You have chosen to open:

SonicWall_DPI-SSL_CA.cer

which is: cer File

from: https://10.3.2.5

What should Firefox do with this file?

○ Open with

● Save File

□ Do this automatically for files like this from now on.

a Ensure the **Save File** radio button is selected.

b Click **OK**.

The file is downloaded.

5 Click **Update**.

Adding Trust to the Browser

For a re-signing certificate authority to successfully re-sign certificates, browsers have to trust the certificate authority. Such trust can be established by having the re-signing certificate imported into the browser's trusted CA list. Follow your browser’s instructions for importing re-signing certificates.

Configuring Exclusions and Inclusions

By default, when DPI-SSL is enabled, it applies to all traffic on the appliance. You can customize to which traffic DPI-SSL inspection applies:

- **Exclusion/Inclusion** lists exclude/include specified objects and groups
- **Common Name** exclusions excludes specified host names
- **CFS Category-based Exclusion/Inclusion** excludes or includes specified categories based on CFS categories

This customization allows individual exclusion/inclusion of alternate names for a domain that is part of a list of domains supported by the same server (certificate). In deployments that process a large amount of traffic, to reduce the CPU impact of DPI-SSL and to prevent the appliance from reaching the maximum number of concurrent DPI-SSL inspected connections, it can be useful to exclude trusted sources.

ⓘ **NOTE:** If DPI-SSL is enabled on the firewall when using Google Drive, Apple iTunes, or any other application with pinned certificates, the application may fail to connect to the server. To allow the application to connect, exclude the associated domains from DPI-SSL; for example, to allow Google Drive to work, exclude:

- `.google.com`
- `.googleapis.com`
- `.gstatic.com`

As Google uses one certificate for all its applications, excluding these domains allows Google applications to bypass DPI-SSL.

Alternatively, exclude the client machines from DPI-SSL.

Topics:

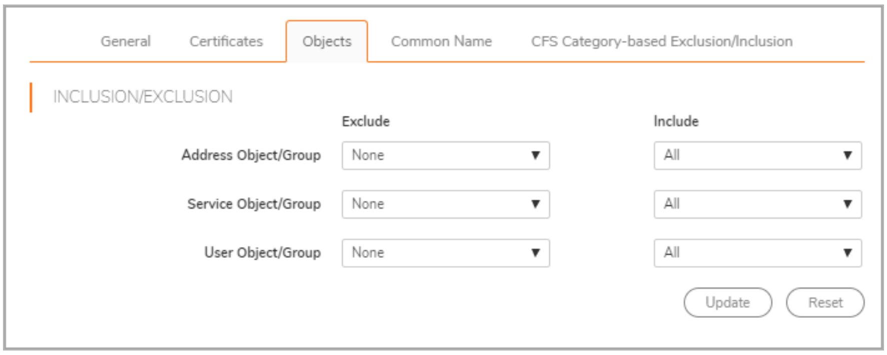
- Excluding/Including Objects/Groups
- Excluding/Including by Common Name
- Specifying CFS Category-based Exclusions/Inclusions
- Content Filtering
- App Rules

Excluding/Including Objects/Groups

To customize DPI-SSL client inspection:

1 Navigate to the **DPI-SSL > Client SSL** page.

2 Scroll down to the **Inclusion/Exclusion** section.



	Exclude	Include
Address Object/Group	None	All
Service Object/Group	None	All
User Object/Group	None	All

3 From the **Address Object/Group Exclude** and **Include** drop-down menus, select an address object or group to exclude or include from DPI-SSL inspection. By default, **Exclude** is set to **None** and **Include** is set to **All**.

ⓘ **TIP:** The **Include** drop-down menu can be used to fine tune the specified exclusion list. For example, by selecting the **Remote-office-California** address object in the **Exclude** drop-down menu and the **Remote-office-Oakland** address object in the **Include** drop-down menu.

4 From the **Service Object/Group Exclude** and **Include** drop-down menus, select an address object or group to exclude or include from DPI-SSL inspection. By default, **Exclude** is set to **None** and **Include** is set to **All**.

5 From the **User Object/Group Exclude** and **Include** drop-down menus, select an address object or group to exclude or include from DPI-SSL inspection. By default, **Exclude** is set to **None** and **Include** is set to **All**.

6 Click **Accept**.

Excluding/Including by Common Name

You can add trusted domain names to the exclusion list. Adding trusted domains to the Built-in exclusion database reduces the CPU effect of DPI-SSL and prevents he appliance from reaching the maximum number of concurrent DPI-SSL inspected connections.

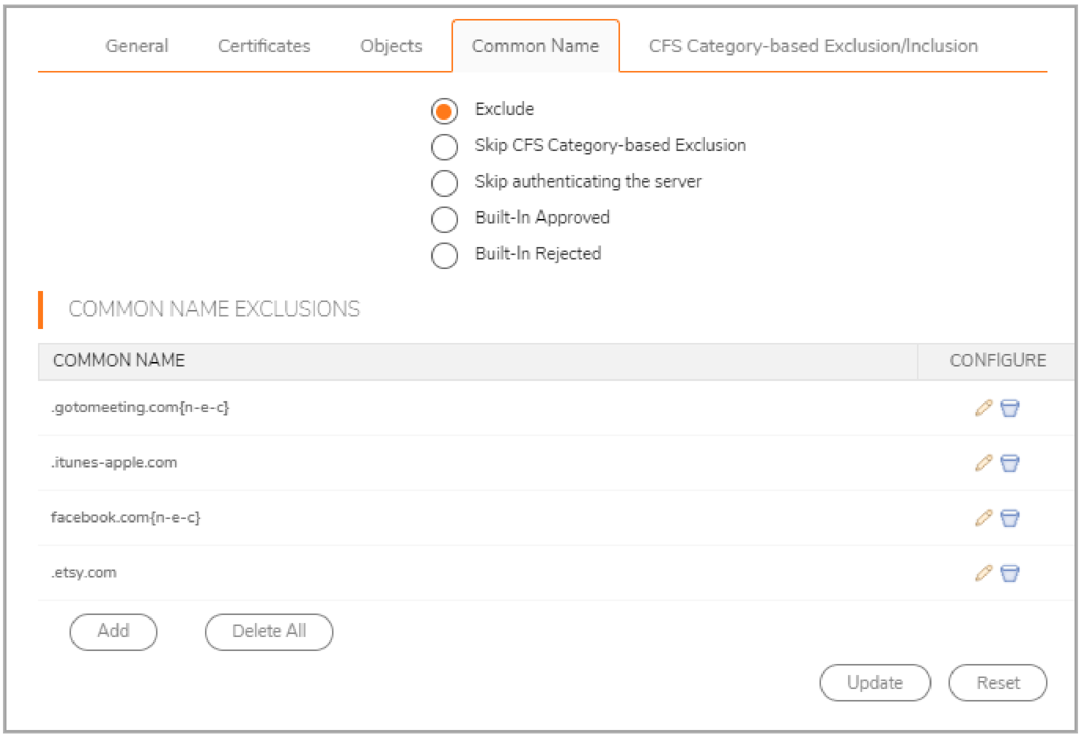
Topics:

- Excluding/Including Common Names
- Deleting Custom Common Names
- Specifying CFS Category-based Exclusions/Inclusions

Excluding/Including Common Names

To exclude/include entities by common name:

1 Navigate to the **DPI-SSL > Client SSL | Common Name** page.



● Exclude
○ Skip CFS Category-based Exclusion
○ Skip authenticating the server
○ Built-In Approved
○ Built-In Rejected

COMMON NAME EXCLUSIONS

COMMON NAME	CONFIGURE
.gotomeeting.com{n-e-c}	
.itunes-apple.com	
facebook.com{n-e-c}	
.etsy.com	

2 You can control the display of the common names by selecting the following options:

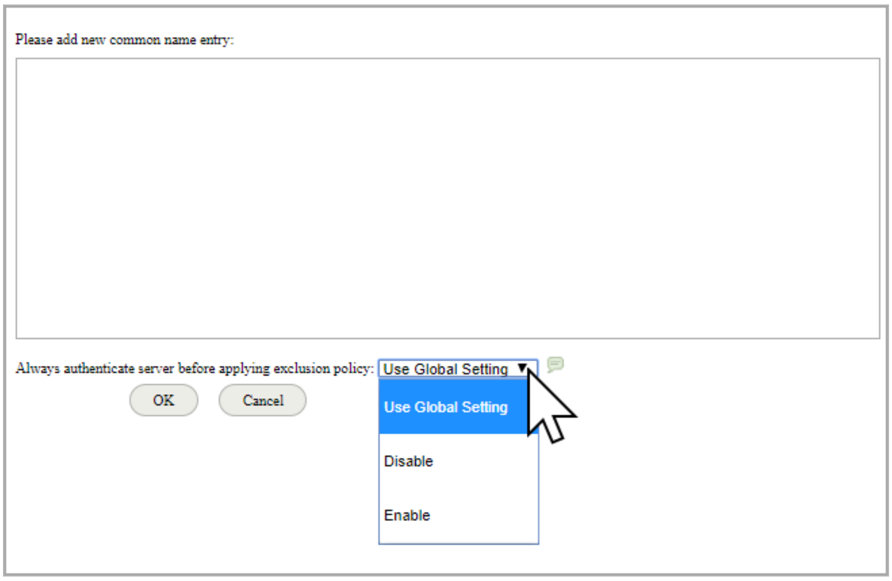
- **Action** options:
  - **Exclude** – Displays only excluded common names.
  - **Skip CFS Category-based Exclusion** – Displays only custom common names that have the override CFS category-based exclusion option selected.

ⓘ **NOTE:** Use the **Skip CFS Category-based Exclusion** option to exclude a particular domain from the global inclusion options, **Always authenticate server for decrypted connections** and **Always authenticate server before applying exclusion policy**.

  - **Skip authenticating the server** – Allow skipping all server authentication.
  - **Built-In Approval** – Approval automatically built-in.
  - **Built-In Rejected** – Rejection built-in.

  c Click **OK**.

3 To add a custom common name, click the **Add** button below the **Common Name Exclusions** table. The **Add Common Names** dialog displays.



Please add new common name entry:

Always authenticate server before applying exclusion policy: Use Global Setting

  a Add one or more common names in the field. Separate multiple entries with commas or newline characters.

  b Click **OK**.

  The **Common Name Exclusions/Inclusions** table is updated, with **Custom** in the **Built-in** column. If the **Always authenticate server before applying exclusion policy** option has been selected an **Information** icon displays next to **Custom** in the **Built-in** column.

4 You can search for common names by specifying a filter.

  a In the **Filter** field, enter a name by specifying the name in this syntax: `name:mycommonname`.

  b Click **Filter**.

5 Click **OK**.

Deleting Custom Common Names

To delete custom common names:

1 Navigate to the **DPI-SSL > Client SSL** page.

2 Scroll down to the **Common Name Exclusions** section.

3 Do one of the following:

  - Clicking a custom common name's **Delete** icon in the **Configure** column.
  - Clicking the **Delete All** checkbox to delete all custom common names. A confirmation message displays. Click **OK**.

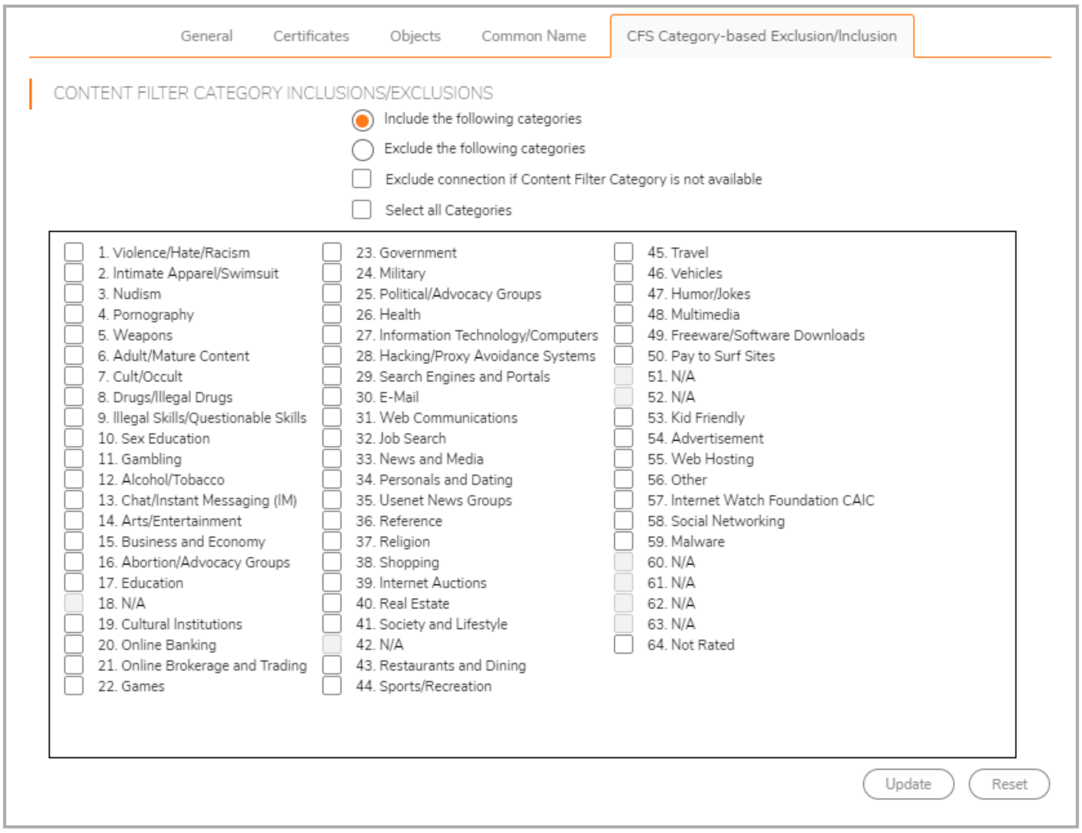
4 Click **Update**.

Specifying CFS Category-based Exclusions/Inclusions

You can exclude/include entities by content filter categories.

To specify CFS category-based exclusions/inclusions:

1 Navigate to the **DPI-SSL > Client SSL** | **CFS Category-based Exclusions/Inclusions**.



CONTENT FILTER CATEGORY INCLUSIONS/EXCLUSIONS

● Include the following categories

○ Exclude the following categories

□ Exclude connection if Content Filter Category is not available

□ Select all Categories

□ 1. Violence/Hate/Racism
□ 2. Intimate Apparel/Swimsuit
□ 3. Nudism
□ 4. Pornography
□ 5. Weapons
□ 6. Adult/Mature Content
□ 7. Cult/Occult
□ 8. Drugs/Illegal Drugs
□ 9. Illegal Skills/Questionable Skills
□ 10. Sex Education
□ 11. Gambling
□ 12. Alcohol/Tobacco
□ 13. Chat/Instant Messaging (IM)
□ 14. Arts/Entertainment
□ 15. Business and Economy
□ 16. Abortion/Advocacy Groups
□ 17. Education
□ 18. N/A
□ 19. Cultural Institutions
□ 20. Online Banking
□ 21. Online Brokerage and Trading
□ 22. Games
□ 23. Government
□ 24. Military
□ 25. Political/Advocacy Groups
□ 26. Health
□ 27. Information Technology/Computers
□ 28. Hacking/Proxy Avoidance Systems
□ 29. Search Engines and Portals
□ 30. E-Mail
□ 31. Web Communications
□ 32. Job Search
□ 33. News and Media
□ 34. Personals and Dating
□ 35. Usenet News Groups
□ 36. Reference
□ 37. Religion
□ 38. Shopping
□ 39. Internet Auctions
□ 40. Real Estate
□ 41. Society and Lifestyle
□ 42. N/A
□ 43. Restaurants and Dining
□ 44. Sports/Recreation
□ 45. Travel
□ 46. Vehicles
□ 47. Humor/Jokes
□ 48. Multimedia
□ 49. Freeware/Software Downloads
□ 50. Pay to Surf Sites
□ 51. N/A
□ 52. N/A
□ 53. Kid Friendly
□ 54. Advertisement
□ 55. Web Hosting
□ 56. Other
□ 57. Internet Watch Foundation CAIC
□ 58. Social Networking
□ 59. Malware
□ 60. N/A
□ 61. N/A
□ 62. N/A
□ 63. N/A
□ 64. Not Rated

2 Select whether you want to include or exclude the selected categories by clicking either the **Include the following categories** (default) or **Exclude the following categories** radio button. By default, all categories are unselected.

3 Select the categories to be included/excluded. To select all categories, click **Select all Categories**.

4 Optionally, repeat Step 2 and Step 3 to create the opposite list.

5 Optionally, to exclude a connection if the content filter category information for a domain is not available to DPI-SSL, select **Exclude connection if Content Filter Category is not available**. This option is not selected by default.

In most cases, category information for a HTTPS domain is available locally in the firewall cache. When the category information is not locally available, DPI-SSL obtains the category information from the cloud without blocking the client or server communication. In rare cases, the category information is not available for DPI-SSL to make a decision. By default, such sites are inspected in DPI-SSL.

6 Click **Update**.

Client DPI-SSL Examples

Topics:

- Content Filtering
- App Rules

Content Filtering

To perform SonicWall Content Filtering on HTTPS and SSL-based traffic using DPI-SSL:

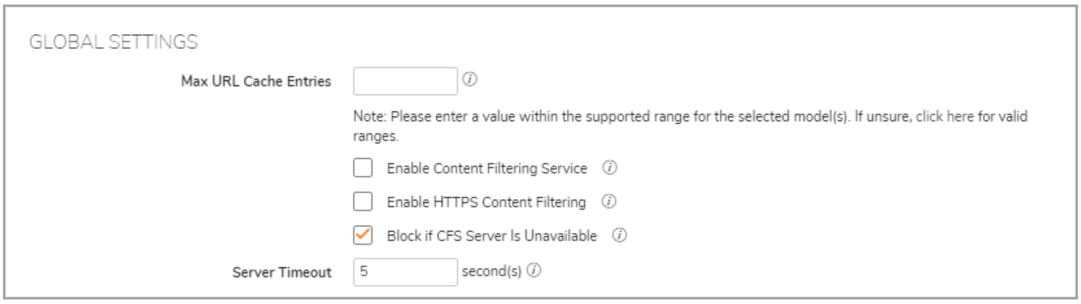
1 Navigate to the **Security Services > Content Filter** page.

1 Scroll down to the **Global Settings** section.

2 Select **Enable Content Filter Service**.

3 Clear the **Enable HTTPS Content Filtering** checkbox.

> ⓘ **NOTE:** HTTPS content filtering is IP and hostname based. While HTTP content filtering can perform redirects to enforce authentication or provide a block page, HTTPS-filtered pages are silently blocked.



GLOBAL SETTINGS

Max URL Cache Entries

Note: Please enter a value within the supported range for the selected model(s). If unsure, click here for valid ranges.

□ Enable Content Filtering Service

□ Enable HTTPS Content Filtering

☑ Block if CFS Server Is Unavailable

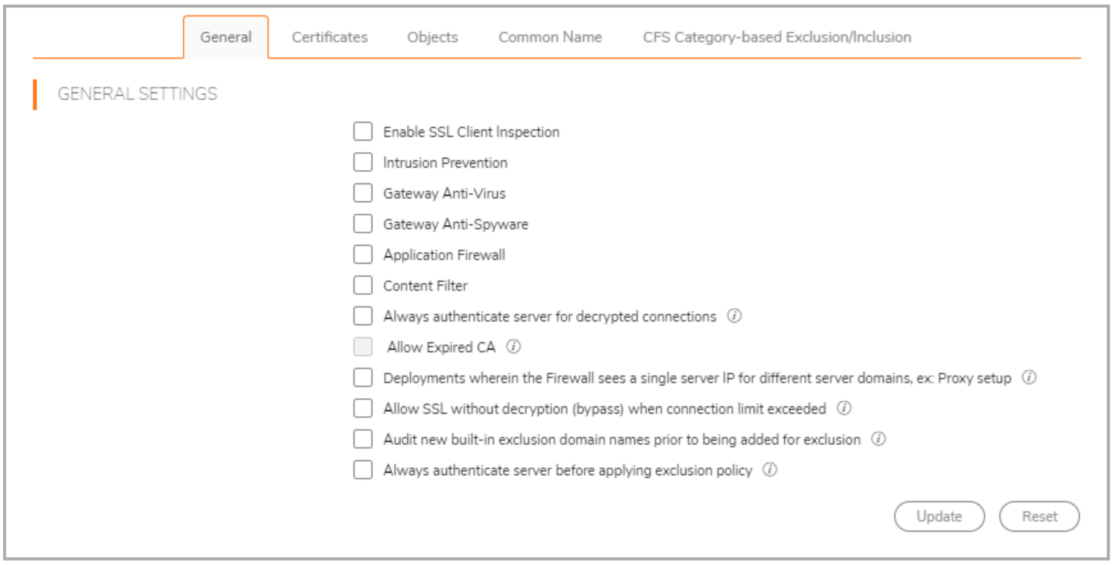
Server Timeout 5 second(s)

4 Ensure **SonicWall CFS** is selected for the **Content Filter Type** from the drop-down menu.

5 Click **Update**.

6 Navigate to the **DPI-SSL > Client SSL** page.

7 Click **General**.



GENERAL SETTINGS

□ Enable SSL Client Inspection

□ Intrusion Prevention

□ Gateway Anti-Virus

□ Gateway Anti-Spyware

□ Application Firewall

□ Content Filter

□ Always authenticate server for decrypted connections ⓘ

□ Allow Expired CA ⓘ

□ Deployments wherein the Firewall sees a single server IP for different server domains, ex: Proxy setup ⓘ

□ Allow SSL without decryption (bypass) when connection limit exceeded ⓘ

□ Audit new built-in exclusion domain names prior to being added for exclusion ⓘ

□ Always authenticate server before applying exclusion policy ⓘ

8 Select **Enable SSL Inspection**.

9 Select **Content Filter**.

10 Click **Update**.

11 For information about configuring the content filters, see Configuring Content Filtering Service.

12 Navigate to a blocked site using the HTTPS protocol to verify that it is properly blocked.

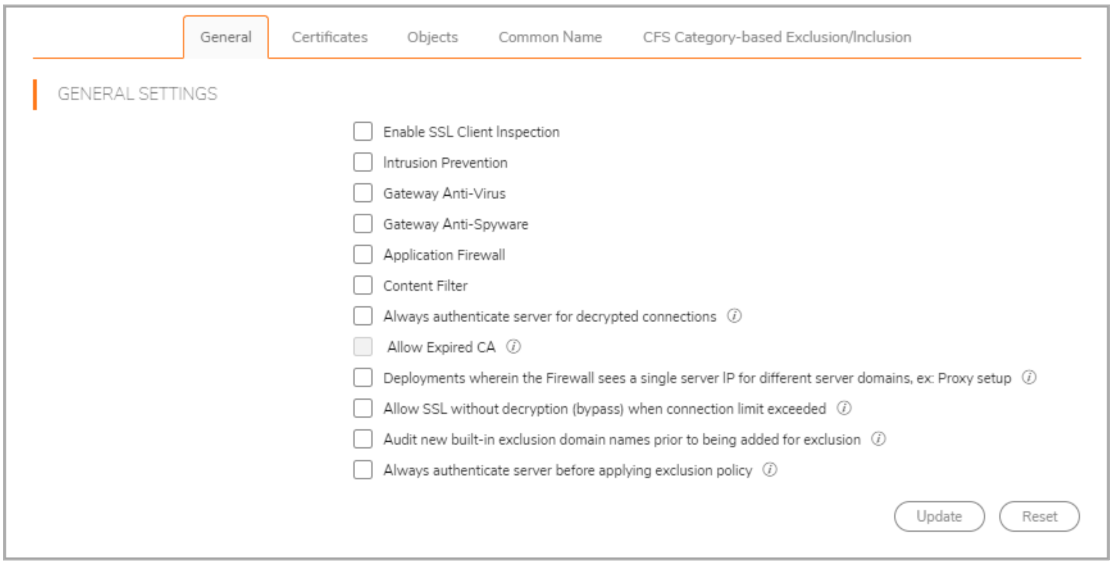
ⓘ **NOTE:** For content filtering over DPI-SSL, the first time HTTPS access is blocked results in a blank page being displayed. If the page is refreshed, the user sees the firewall block page.

App Rules

To filter by application firewall rules, you need to enable them on both the **Security | DPI-SSL > Client SSL** page and the **Firewall > Advanced Application Control** page.

1 Navigate to the **DPI-SSL > Client SSL** page.

2 Scroll down to the **General Settings** section.



GENERAL SETTINGS

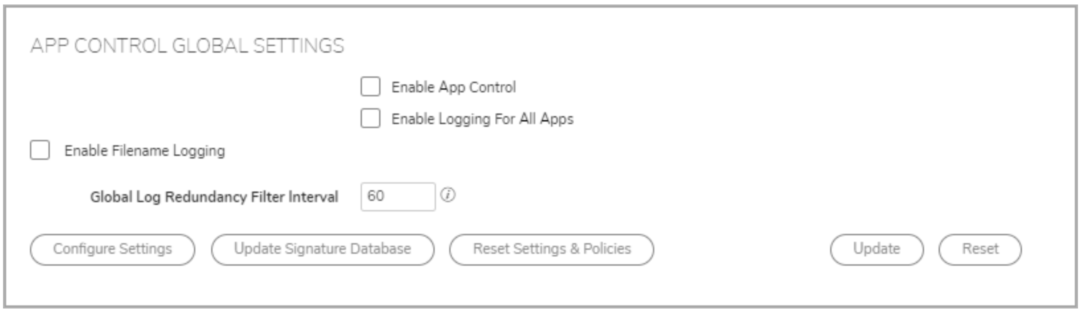
□ Enable SSL Client Inspection
□ Intrusion Prevention
□ Gateway Anti-Virus
□ Gateway Anti-Spyware
□ Application Firewall
□ Content Filter
□ Always authenticate server for decrypted connections
□ Allow Expired CA
□ Deployments wherein the Firewall sees a single server IP for different server domains, ex: Proxy setup
□ Allow SSL without decryption (bypass) when connection limit exceeded
□ Audit new built-in exclusion domain names prior to being added for exclusion
□ Always authenticate server before applying exclusion policy

3 Select **Enable SSL Client Inspection**.

4 Select **Application Firewall**.

5 Click **Update**.

6 Navigate to the **App Rules Global Settings** section of the **Firewall > App Control Advanced** page.



APP CONTROL GLOBAL SETTINGS

□ Enable App Control
□ Enable Logging For All Apps
□ Enable Filename Logging

Global Log Redundancy Filter Interval: 60

7 Select the **Enable App Control**.

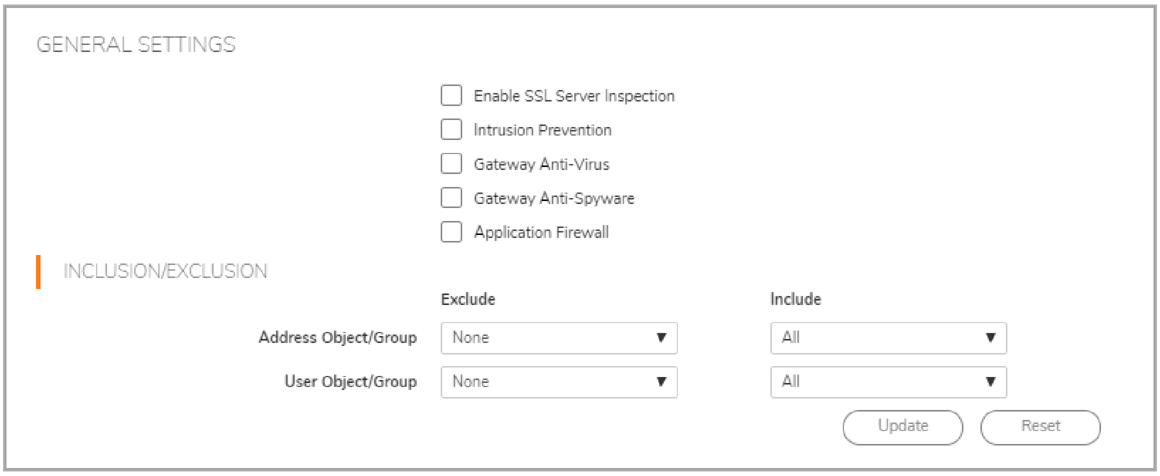
8 Configure an HTTP Client policy to block Microsoft Internet Explorer browser with **block page** as an action for the policy. For how to configure an App Rule, see *SonicWall SonicOS Policies*.

9 Click **Update**.

10 Access any website using the HTTPS protocol with your web browser to verify it is blocked.

2

Configuring Server DPI-SSL Settings



GENERAL SETTINGS

□ Enable SSL Server Inspection

□ Intrusion Prevention

□ Gateway Anti-Virus

□ Gateway Anti-Spyware

□ Application Firewall

INCLUSION/EXCLUSION

	Exclude	Include
Address Object/Group	None	All
User Object/Group	None	All

The Server DPI-SSL deployment scenario is typically used to inspect HTTPS traffic when remote clients connect over the WAN to access content located on the firewall’s LAN. Server DPI-SSL allows you to configure pairings of an address object and certificate. When the appliance detects SSL connections to the address object, it presents the paired certificate and negotiates SSL with the connecting client.

Afterward, if the pairing defines the server to be cleartext, then a standard TCP connection is made to the server on the original (post NAT remapping) port. If the pairing is not defined to be cleartext, then an SSL connection to the server is negotiated. This allows for end-to-end encryption of the connection.

ⓘ **NOTE:** In this deployment scenario, the owner of the firewall owns the certificates and private keys of the origin content servers. You would have to import the server's original certificate onto the appliance and create an appropriate server IP address to server certificate mappings in the Server DPI-SSL UI.

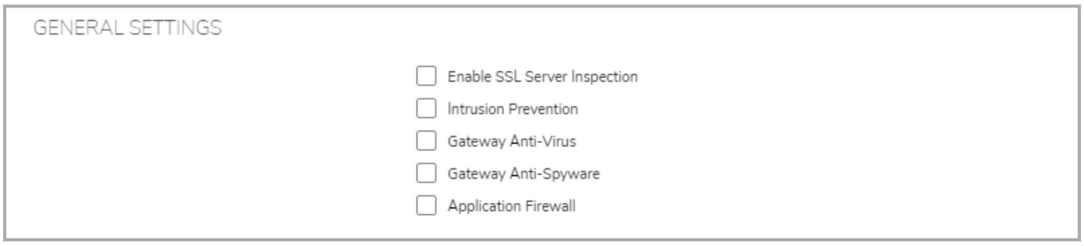
Topics:

- Configuring General Server DPI-SSL Settings
- Configuring Exclusions and Inclusions

Configuring General Server DPI-SSL Settings

To enable Server DPI-SSL inspection:

1 Navigate to the **DPI-SSL > Server SSL | General** page.



GENERAL SETTINGS

□ Enable SSL Server Inspection
□ Intrusion Prevention
□ Gateway Anti-Virus
□ Gateway Anti-Spyware
□ Application Firewall

2 Select the **Enable SSL Server Inspection** checkbox.

3 Select the services with which to perform inspection:

- **Intrusion Prevention**
- **Gateway Anti-Virus**
- **Gateway Anti-Spyware**
- **Application Firewall**

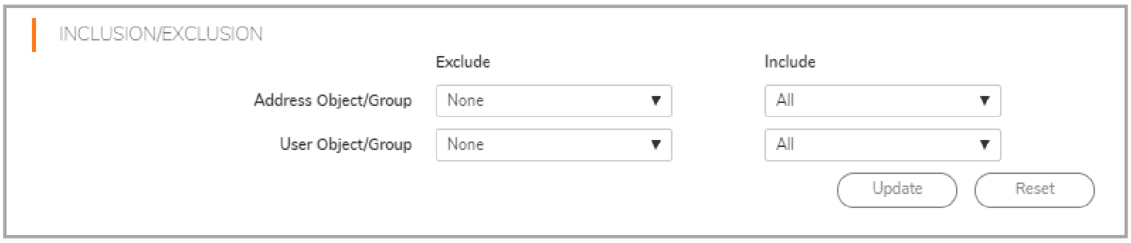
4 Click **Update**.

Configuring Exclusions and Inclusions

By default, the DPI-SSL applies to all traffic on the appliance when it is enabled. You can configure inclusion/exclusion lists to customize to which traffic DPI-SSL inspection applies. The **Inclusion/Exclusion** lists provide the ability to specify certain objects or groups. In deployments that process a large amount of traffic, to reduce the CPU impact of DPI-SSL and to prevent the appliance from reaching the maximum number of concurrent DPI-SSL inspected connections, it can be useful to exclude trusted sources.

To customize DPI-SSL server inspection:

1 Navigate to the **DPI-SSL > Server SSL** page and scroll down to the **Inclusion/Exclusion** section.



INCLUSION/EXCLUSION

	Exclude	Include
Address Object/Group	None ▼	All ▼
User Object/Group	None ▼	All ▼

2 From the **Address Object/Group** section **Exclude** and **Include** drop-down menus, select an address object or group to exclude or include from DPI-SSL inspection. By default, **Exclude** is set to **None** and **Include** is set to **All**.

> ⓘ **TIP:** The **Include** drop-down menu can be used to fine tune the specified exclusion list. For example, by selecting the **Remote-office-California** address object in the **Exclude** drop-down menu and the **Remote-office-Oakland** address object in the **Include** drop-down menu.

3 From the **User Object/Group** section **Exclude** and **Include** drop-down menus, select an address object or group to exclude or include from DPI-SSL inspection. By default, **Exclude** is set to **None** and **Include** is set to **All**.

4 Click **Update**.

3

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

About This Document

Legend

ⓘ **NOTE:** A NOTE icon indicates supporting information.

ⓘ **IMPORTANT:** An IMPORTANT icon indicates supporting information that may need a little extra attention.

ⓘ **TIP:** A TIP indicates helpful information.

△ **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

⚠ **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

Global Management System DPI-SSL Administration
Updated - November 2020
Software Version - 9.3
232-005138-00 RevB

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/en-us/legal/license-agreements.

Open Source Code

SonicWall is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
SonicWall Inc. Attn: Jennifer Anderson
1033 McCarthy Blvd

Milpitas, CA 95035