DPI-SSL

Document Scope

This document describes the DPI-SSL feature available in SonicOS 5.6. This document contains the following sections:

DPI-SSL Overview

Deep Packet Inspection of Secure Socket Layer (DPI-SSL) extends SonicWALL's Deep Packet Inspection technology to allow for the inspection of encrypted HTTPS traffic and other SSL-based traffic. The SSL traffic is decrypted transparently, scanned for threats and then re-encrypted and sent along to its destination if no threats or vulnerabilities are found. DPI-SSL provides additional security, application control, and data leakage prevention for analyzing encrypted HTTPS and other SSL-based traffic.

The following security services and features are capable of utilizing DPI-SSL:

- Gateway Anti-Virus
- Gateway Anti-Spyware
- Intrusion Prevention
- Content Filtering
- Application Firewall
- Packet Capture
- Packet Mirror

DPI-SSL has two main deployment scenarios:

- Client DPI-SSL: Used to inspect HTTPS traffic when clients on the SonicWALL security appliance's LAN access content located on the WAN.
- Server DPI-SSL: Used to inspect HTTPS traffic when remote clients connect over the WAN to access content located on the SonicWALL security appliance's LAN.

Platforms

The DPI-SSL feature is available in SonicOS Enhanced 5.6. The following table shows which platforms support DPI-SSL and the maximum number of concurrent connections on which the appliance can perform DPI-SSL inspection.

Hardware Model	Max Concurrent DPI-SSL inspected connections
NSA 3500	250
NSA 4500	350
NSA 5000	1000
NSA E5500	2000
NSA E6500	3000
NSA E7500	8000

Using DPI-SSL

DPI-SSL has two main deployment scenarios:

- Client DPI-SSL: Used to inspect HTTPS traffic when clients on the SonicWALL security appliance's LAN access content located on the WAN.
- Server DPI-SSL: Used to inspect HTTPS traffic when remote clients connect over the WAN to access content located on the SonicWALL security appliance's LAN.

This section contains the following subsections:

- "Client DPI-SSL" on page 2
- "Server DPI-SSL" on page 6

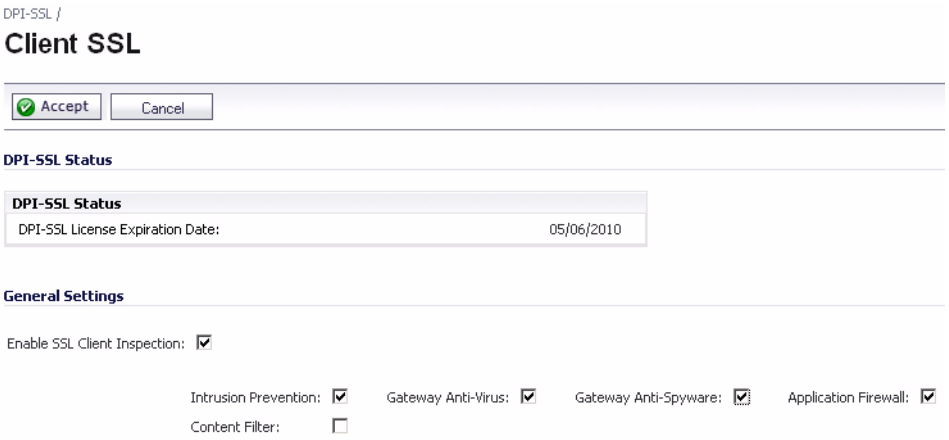
Client DPI-SSL

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 the Client DPI-SSL scenario, the SonicWALL UTM appliance typically does not own the certificates and private keys for the content it is inspecting. After the appliance performs DPI-SSL inspection, it 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 SonicWALL certificate authority (CA) certificate, or 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.

The following sections describe how to configure Client DPI-SSL:

- "Configuring General Client DPI-SSL Settings" on page 3
- "Configuring the Inclusion/Exclusion List" on page 3
- "Selecting the Re-Signing Certificate Authority" on page 4
- "Content Filtering" on page 5

Configuring General Client DPI-SSL Settings



To enable Client DPI-SSL inspection, perform the following steps:

1. Navigate to the **DPI-SSL > Client SSL** page.
2. Select the **Enable SSL Inspection** checkbox.
3. Select which of the following services to perform inspection with: **Intrusion Prevent**, **Gateway Anti-Virus**, **Gateway Anti-Spyware**, **Application Firewall**, and **Content Filter**.
4. Click **Accept**.

Configuring the Inclusion/Exclusion List

By default, the DPI-SSL applies to all traffic on the appliance when it is enabled. You can configure an Inclusion/Exclusion list to customize which traffic DPI-SSL inspection will apply to. The Inclusion/Exclusion list provides the ability to specify certain objects, groups, or hostnames. In deployments that are processing a large amount of traffic, it can be useful to exclude trusted sources in order to reduce the CPU impact of DPI-SSL and to prevent the appliance from reaching the maximum number of concurrent DPI-SSL inspected connections.

The **Inclusion/Exclusion** section of the **Client SSL** page contains four options for specifying the inclusion list:

- On the **Address Object/Group** line, select an address object or group from the **Exclude** pulldown menu to exempt it from DPI-SSL inspection.
- On the **Service Object/Group** line, select a service object or group from the **Exclude** pulldown menu to exempt it from DPI-SSL inspection.

- On the **User Object/Group** line, select a user object or group from the **Exclude** pulldown menu to exempt it from DPI-SSL inspection.

Tip

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

- The **Common Name Exclusions** section is used to add domain names to the exclusion list. To add a domain name, type it in the text box and click **Add**.
- Click **Apply** at the top of the page to confirm the configuration.

Selecting the Re-Signing Certificate Authority

By default, DPI-SSL uses the **Default SonicWALL DPI-SSL CA Certificate** to re-sign traffic that has been inspected. Optionally, users can specify that another certificate will be used. To use a custom certificate, you must first import the certificate to the SonicWALL UTM appliance:

1. Navigate to the **System > Certificates** page.
2. Click **Import Certificate**.
3. Select the **Import a local end-user certificate with private key from a PKCS#12 (.p12 or .pfx) encoded file** option.
4. Choose **password** and click **Import**.

After the certificate has been imported, you must configure it on the Client DPI-SSL page:

1. Navigate to the **DPI-SSL > Client SSL** page.
2. Scroll down to the **Certificate Re-Signing Authority** section and select the certificate from the pulldown menu.
3. Click **Apply**.

For help with creating PKCS-12 formatted files, see "Creating PKCS-12 Formatted Certificate File" on page 4.

Adding Trust to the Browser

In the previous section we described how to configure a re-signing certificate authority. In order for re-signing certificate authority to successfully re-sign certificates browsers would have to trust this certificate authority. Such trust can be established by having re-signing certificate imported into the browser's trusted CA list.

- Internet Explorer: Go to **Tools > Internet Options**, click the **Content** tab and click **Certificates**. Click the **Trusted Root Certification Authorities** tab and click **Import**. The **Certificate Import Wizard** will guide you through importing the certificate.
- Firefox: Go to **Tools > Options**, click the **Advanced** tab and then the **Encryption** tab. Click **View Certificates**, select the **Authorities** tab, and click **Import**. Select the certificate file, make sure the **Trust this CA to identify websites** check box is selected, and click **OK**.
- Mac: Double-click the certificate file, select **Keychain menu**, click **X509 Anchors**, and then click **OK**. Enter the system username and password and click **OK**.

Creating PKCS-12 Formatted Certificate File

PKCS12 formatted certificate file can be created using Linux system with OpenSSL. In order to create a PKCS-12 formatted certificate file, one needs to have two main components of the certificate:

- Private key (typically a file with .key extension or the word key in the filename)
- Certificate with a public key (typically a file with .crt extension or the word cert as part of filename).

For example, Apache HTTP server on Linux has its private key and certificate in the following locations:

- /etc/httpd/conf/ssl.key/server.key
- /etc/httpd/conf/ssl.crt/server.crt

With these two files available, run the following command:

```
openssl pkcs12 -export -out out.p12 -inkey server.key -in server.crt
```

In this example **out.p12** will become the PKCS-12 formatted certificate file and **server.key** and **server.crt** are the PEM formatted private key and the certificate file respectively.

After the above command, one would be prompted for the password to protect/encrypted the file. After the password is chosen, the creation of PKCS-12 formatted certificate file is complete and it can be imported into the UTM appliance.

Client DPI-SSL Examples

The following sections

- "Content Filtering" on page 5
- "Application Firewall" on page 5

Content Filtering

To perform SonicWALL Content Filtering on HTTPS and SSL-based traffic using DPI-SSL, perform the following steps:

1. Navigate to the **DPI-SSL > Client SSL** page
2. Select the **Enable SSL Inspection** checkbox and the **Content Filter** checkbox.
3. Click **Apply**.
4. Navigate to the **Security Services > Content Filter** page and click the **Configure** button.
5. Uncheck the **Enable IP based HTTPS Content Filtering** checkbox.
6. Select the appropriate categories to be blocked.
7. Click **Apply**.
8. 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 result in a blank page being displayed. If the page is refreshed, the user will see the SonicWALL block page.

Application Firewall

Enable Application Firewall checkbox on the Client DPI-SSL screen and enable Application Firewall on the Application Firewall >Policies screen.

1. Navigate to the **DPI-SSL > Client SSL** page
2. Select the **Enable SSL Inspection** checkbox and the **Application Firewall** checkbox.
3. Click **Apply**.
4. Navigate to the **Application Firewall > Policies** page.
5. Enable **Application Firewall**.

6. Configure an **HTTP Client policy** to block Microsoft Internet Explorer browser.
7. Select **block page** as an action for the policy. Click **Apply**.
8. Access any website using the HTTPS protocol with Internet Explorer and verify that it is blocked.

DPI-SSL also supports Application Level Bandwidth Management over SSL tunnels. Application Firewall HTTP bandwidth management policies also applies to content that is accessed over HTTPS when DPI-SSL is enabled for Application Firewall.

Server DPI-SSL

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 SonicWALL security appliance's LAN. Server DPI-SSL allows the user 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.

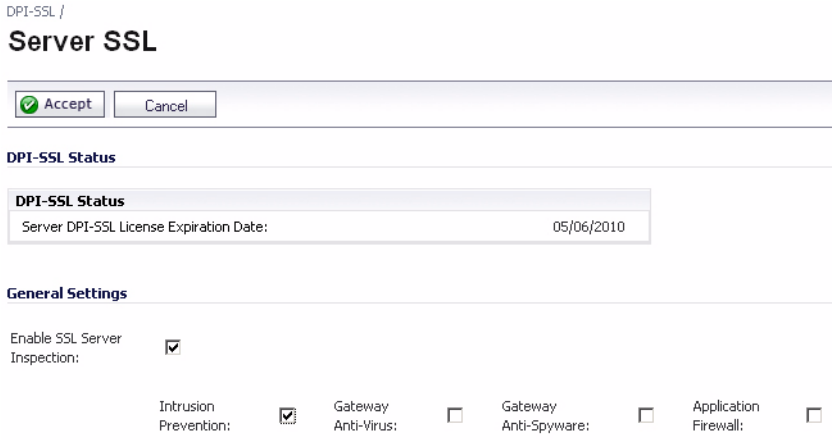
Afterward, if the pairing defines the server to be 'cleartext' then a standard TCP connection is made to the server on the original (post NAT remapping) port. If the pairing is not defined to be cleartext, then an SSL connection to the server is negotiated. This allows for end-to-end encryption of the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

In this deployment scenario the owner of the SonicWALL UTM owns the certificates and private keys of the origin content servers. Administrator would have to import server's original certificate onto the UTM appliance and create appropriate server IP address to server certificate mappings in the Server DPI-SSL UI.

The following sections describe how to configure Server DPI-SSL:

- "Configuring General Server DPI-SSL Settings" on page 6
- "Configuring the Exclusion List" on page 7
- "Configuring Server-to-Certificate Pairings" on page 7
- "SSL Offloading" on page 8

Configuring General Server DPI-SSL Settings



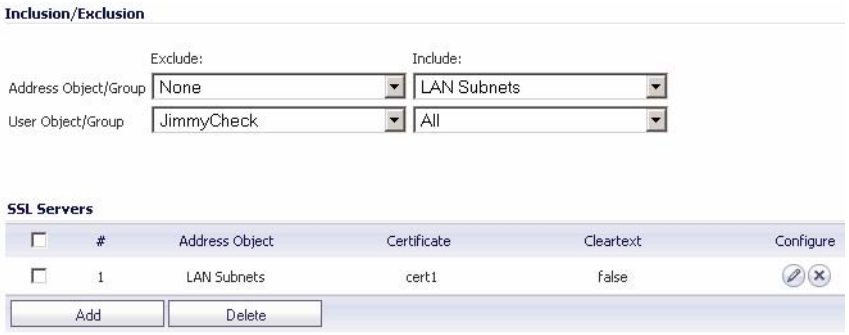
To enable Server DPI-SSL inspection, perform the following steps:

1. Navigate to the **DPI-SSL > Server SSL** page.
2. Select the **Enable SSL Inspection** checkbox.
3. Select which of the following services to perform inspection with: **Intrusion Prevent**, **Gateway Anti-Virus**, **Gateway Anti-Spyware**, and **Application Firewall**.

4. Click **Apply**.
5. Scroll down to the **SSL Servers** section to configure the server or servers to which DPI-SSL inspection will be applied. See "Configuring Server-to-Certificate Pairings" on page 7.

Configuring the Exclusion List

By default, the DPI-SSL applies to all traffic on the appliance when it is enabled. You can configure an Inclusion/Exclusion list to customize which traffic DPI-SSL inspection will apply to. The Inclusion/Exclusion list provides the ability to specify certain objects, groups, or hostnames. In deployments that are processing a large amount of traffic, it can be useful to exclude trusted sources in order to reduce the CPU impact of DPI-SSL and to prevent the appliance from reaching the maximum number of concurrent DPI-SSL inspected connections.



The **Inclusion/Exclusion** section of the **Server SSL** page contains two options for specifying the inclusion list:

- On the **Address Object/Group** line, select an address object or group from the **Exclude** pulldown menu to exempt it from DPI-SSL inspection.
- On the **User Object/Group** line, select a user object or group from the **Exclude** pulldown menu to exempt it from DPI-SSL inspection.

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

Configuring Server-to-Certificate Pairings

Server DPI-SSL inspection requires that you specify which certificate will be used to sign traffic for each server that will have DPI-SSL inspection performed on its traffic. To configure a server-to-certificate pairing, perform the following steps:

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

2. Click the **Add** button.

3. In the **Address Object/Group** pulldown menu, select the address object or group for the server or servers that you want to apply DPI-SSL inspection to.
4. In the **SSL Certificate** pulldown menu, select the certificate that will be used to sign the traffic for the server. For more information on importing a new certificate to the appliance, see "Selecting the Re-Signing Certificate Authority" on page 4 For information on creating a certificate, see "Creating PKCS-12 Formatted Certificate File" on page 4.
5. Select the **Cleartext** checkbox to enable SSL offloading. See "SSL Offloading" on page 8 for more information.
6. Click **Add**.

SSL Offloading

When adding server-to-certificate pairs, a **cleartext** option is available. This option indicates that the portion of the TCP connection between the UTM appliance and the local server will be in the clear without SSL layer, thus allowing SSL processing to be offloaded from the server by the appliance.

Please note that in order for such configuration to work properly, a NAT policy needs to be created on the **Network > NAT Policies** page to map traffic destined for the offload server from an SSL port to a non-SSL port. For example, in case of HTTPS traffic being used with SSL offloading, an inbound NAT policy remapping traffic from port 443 to another port needs to be created in order for things to work properly. A port other than port 80 should be used, because port 80 is used for clear text data inbound to the server.

Document Version History

Version Number	Date	Notes
1	1/8/2010	This document was created.