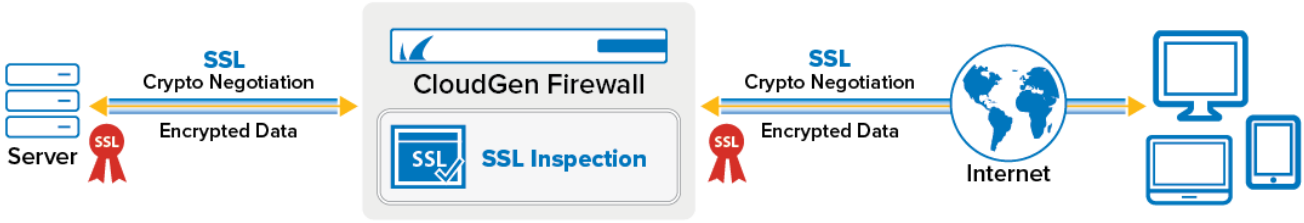
How to Create a TLS Inspection Policy for Inbound TLS Inspection

https://campus.barracuda.com/doc/96026321/

For inbound TLS Inspection, the firewall uses the same TLS certificate that is installed on the internal server.



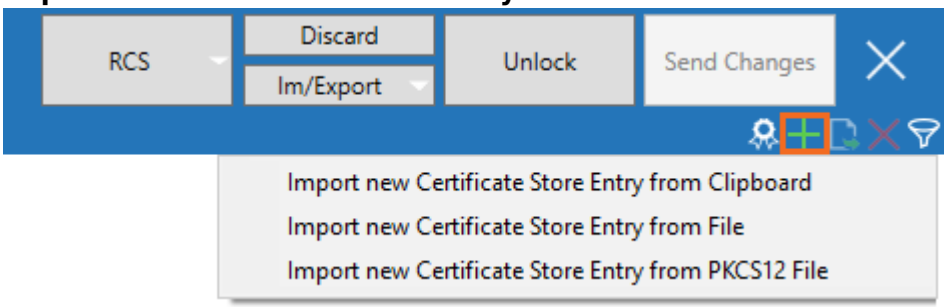
Before You Begin

- Create or purchase the server certificate to be used for TLS Inspection.
- Verify that the **Feature Level** of the Forwarding Firewall is set to 7.2 or higher.

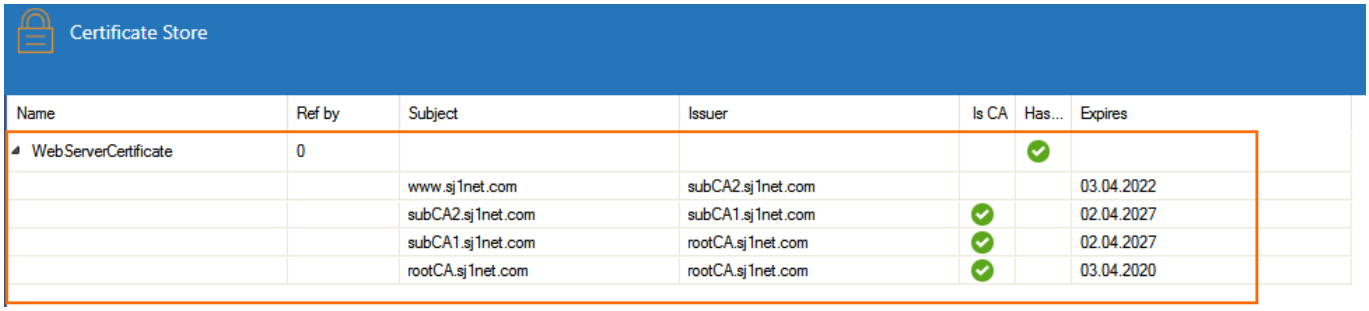
Step 1. Upload the Certificate to the Certificate Store

Upload the server certificate used to terminate incoming TLS connections on the firewall.

1. Go to the **Certificate Store**. On the CloudGen Firewall, the certificate store is located under **Advanced Configuration**, on the Control Center in the **Global Settings**, **Range Settings**, or **Cluster Settings**.
2. Click **Lock**.
3. In the upper-left corner, click **+** and select **Import new Certificate Store Entry from File** or **Import new Certificate Store Entry from PKCS12**.



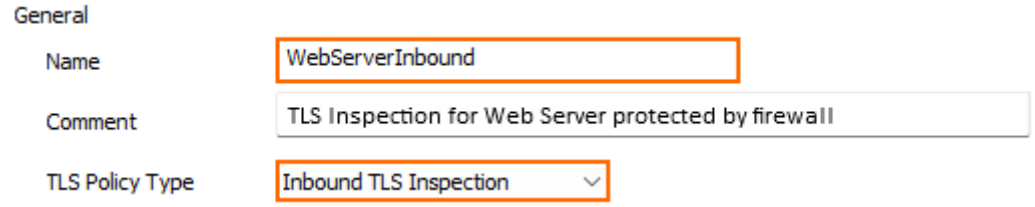
4. Select the certificate file and click **Open**.
5. (optional) Enter the **Password** and click **OK**.
6. Enter a **Name** and click **OK**.
7. Click **Send Changes** and **Activate**.



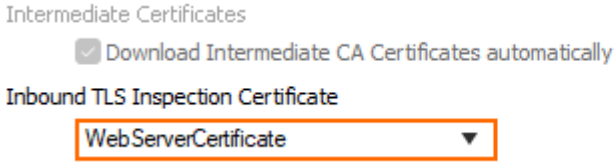
Step 2. Create a TLS Inspection Policy Object

Create a TLS Inspection policy object for inbound TLS Inspection.

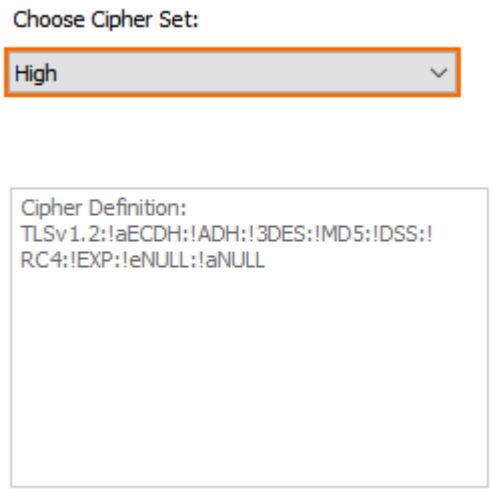
1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. In the left menu, click **TLS Inspection**.
4. Right-click the table and select **New TLS Inspection Policy**. The **Edit TLS Inspection** window opens.
5. Enter the **Name**.
6. From the **TLS Policy Type** drop-down list, select **Inbound TLS Inspection**.



7. From the **Inbound TLS Inspection Certificate** drop-down list, select the server certificate you uploaded to the certificate store in Step 1.



8. (optional) Configure **Cryptographic Attributes**:
   - **Minimum TLS Version** – Select the minimum TLS version.
     Since most servers currently support only TLS version 1.2, do not set this parameter to a higher value. Setting the minimum TLS version to 1.3 enforces TLS 1.3, which can cause connections to fail.
   - **Cipher Set** – Select a preset cipher set, or click **Configure** to customize the cipher set.
9. (optional) Click **Configure** to customize the cipher set and/or click **Show Cipher String** to view a list of support ciphers of the set.



10. Click **OK**
11. Click **Send Changes** and **Activate**.

Next Steps

Configure outbound TLS Inspection. For more information, see How to Configure Outbound TLS Inspection.

Figures

1. ssl_inspection_in.png
2. cert_import01.png
3. ssl_policy02.png
4. inbound_TLS_policy_webserver.png
5. inbound_TLS_webserver_certificate.png
6. sslPolicy06.png