

How to Create an SSL Inspection Policy for Inbound SSL Inspection

<https://campus.barracuda.com/doc/73703655/>

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

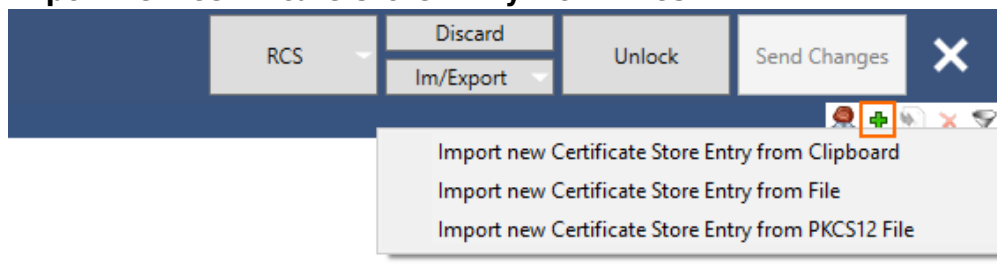
Before You Begin

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

Step 1. Upload the Certificate to Certificate Store

Upload the server certificate used to terminate incoming SSL 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**.

Certificate Store						
Name	Ref by	Subject	Issuer	Is CA	Has...	Expires
WebServerCertificate	0				✓	
		www.sj1net.com	subCA2.sj1net.com			03.04.2022
		subCA2.sj1net.com	subCA1.sj1net.com	✓		02.04.2027
		subCA1.sj1net.com	rootCA.sj1net.com	✓		02.04.2027
		rootCA.sj1net.com	rootCA.sj1net.com	✓		03.04.2020

Step 2. Create an SSL Inspection Policy Object

Create an SSL Inspection policy object for inbound SSL Inspection.

- Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Firewall > Forwarding Rules**.
- Click **Lock**.
- In the left menu, click **SSL Inspection**.
- Right-click the table and select **New SSL Inspection Policy**. The **Edit SSL Inspection** window opens.
- Enter the **Name**.
- From the **SSL Policy Type** drop-down list, select **Inbound SSL Inspection**.

General

Name	<input type="text" value="WebServerInbound"/>
Comment	<input type="text" value="SSL Inspection for Web Server protected by firewall"/>
SSL Policy Type	<input type="text" value="Inbound SSL Inspection"/>

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

Inbound SSL Inspection Certificate

<input type="text" value="WebServerCertificate"/>

- (optional) Configure **Cryptographic Attributes**:

- **Minimum SSL/TLS Version** – Select the minimum SSL or TLS version.
- **Cipher Set** – Select a preset cipher set, or click **Configure** to customize the cipher set.

Cryptographic Attributes

Minimum SSL/TLS Version	<input type="text" value="TLS v1.0"/>	
Cipher Set	<input type="text" value="Medium"/>	<input type="button" value="Configure"/>

- (optional) Click **Configure** to customize cipher set and/or click **Show Cipher String** to view a list of support ciphers of the set.

Choose Cipher Set:

```
Cipher Definition:  
TLSv1.2:!aECDH:!ADH:!3DES:!MD5:!DSS!  
RC4:!EXP:!eNULL:!aNULL
```

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

Next Steps

Configure outbound SSL Inspection. For more information, see [How to Configure Outbound SSL Inspection](#).

Figures

1. cert_import.png
2. sslPolicy02.png
3. sslPolicy03.png
4. sslPolicy04.png
5. sslPolicy05.png
6. sslPolicy06.png

© Barracuda Networks Inc., 2020 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.