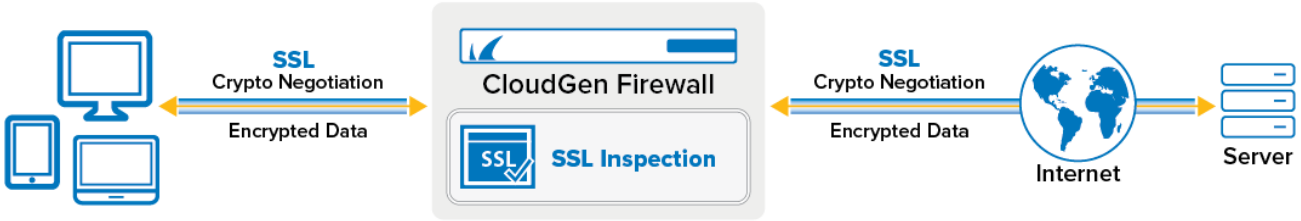
How to Configure Outbound TLS Inspection

https://campus.barracuda.com/doc/96026323/

Outbound SSL Inspection allows the firewall to inspect TLS traffic when clients behind the firewall access SSL-encrypted services on the Internet. Depending on the settings in the TLS Inspection policy used, various TLS errors are handled directly on the firewall, without allowing the user to override this decision. For example, it is possible to block users from accepting self-signed certificates.

With Barracuda CloudGen Firewall version 8.3.0, a new feature 'Policy Profiles' has been implemented. Policy profiles are centrally managed, (pre-)defined rules for handling network traffic and applications. Instead of configuring outbound TLS Inspection, you can also switch from the application ruleset to the Policy Profiles view and configure TLS Inspection policies. For more information, see Policy Profiles and How to Configure a TLS Inspection Policy for Outbound TLS Inspection.



Before You Begin

- Create a TLS Inspection policy for outbound TLS Inspection. For more information, see How to Configure a TLS Inspection Policy for Outbound TLS Inspection.

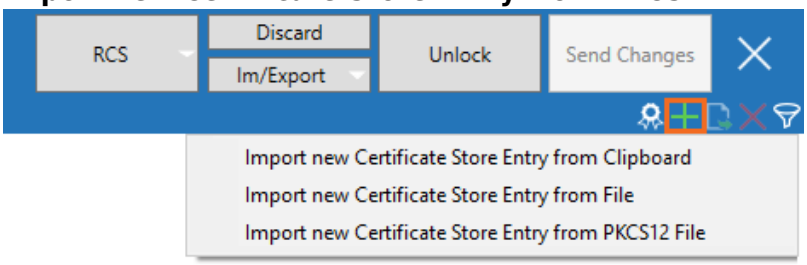
Step 1. Upload the SSL Certificate and Key to the Certificate Store

External Certificates

Upload the certificate and optionally key to the certificate store.

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

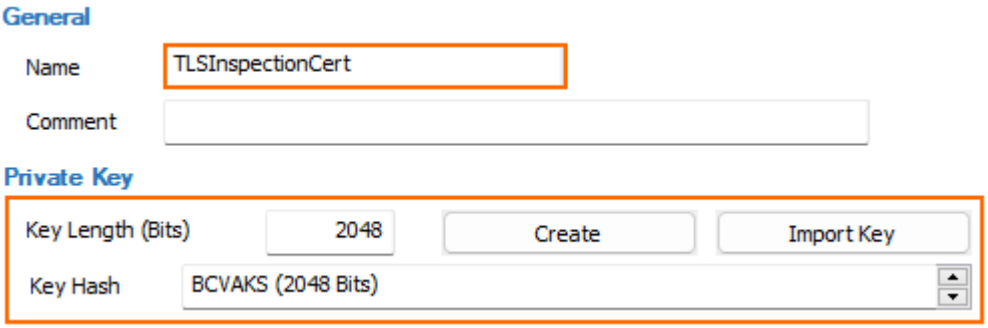
Import new Certificate Store Entry from PKCS12.



4. Select the certificate file and click **Open**.
5. (optional) Enter the **Password** and click **OK**.
6. Enter a **Name** and click **OK**.
7. (optional) If needed right-click the certificate and select **Assign Key to Certificate Store Entry**.
    1. Select the certificate key file and click **Open.**
    2. Enter a **Name** and click **OK**.
8. Click **Send Changes** and **Activate**.

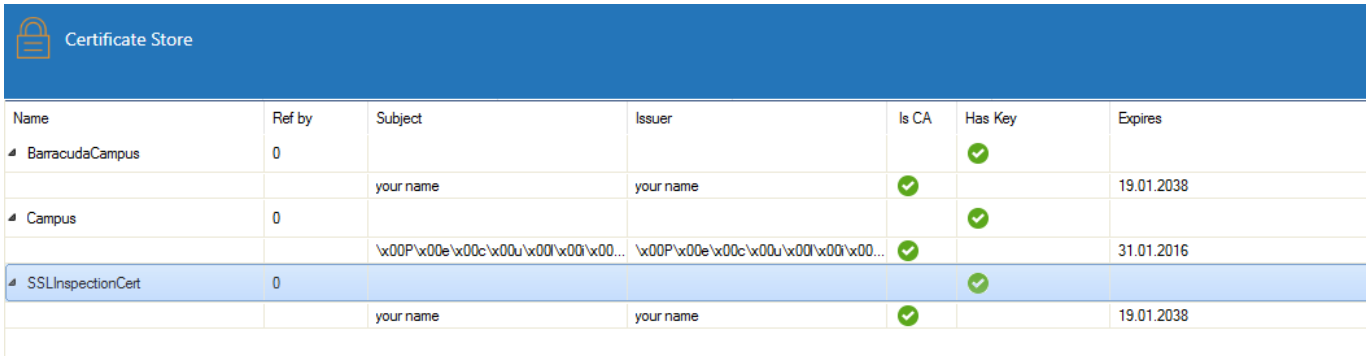
Generate Self-Signed Certificates on the Firewall

1. Go to the **Certificate store**. On a standalone firewall, the certificate store is in the **Advanced Configuration**, on the Control Center in the **Global Settings**, **Range Settings**, or **Cluster Settings**.
2. Click **Lock**.
3. Right-click in the table and select **Create Self Signed Certificate** or click the respective icon at the top right of the window ( ).
4. Select **Create Self Signed Certificate**. The **Create Self Signed Certificate** window opens.
5. Enter a **Name** for the certificate.
6. (optional) Enter the **Key Length**.
7. Click **Create** to create a key,
8. Select the key to import, and click **Open**.



9. In the **Subject - Issuer** section, will in the required certificate information.
10. Click **OK**.

The certificate used for outbound SSL Inspection is now listed in the certificate store.



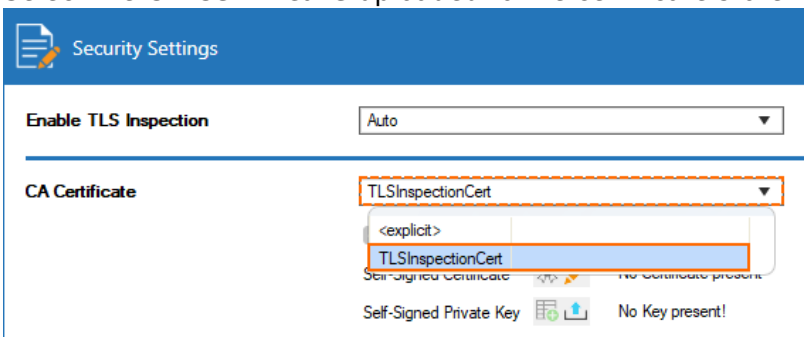
Step 2. Enable SSL Inspection

Make sure that SSL is enabled in the **Security Policy Settings**.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Security Policy**.
2. Click **Lock**.
3. Expand the **Enable SSL Inspection** drop-down list and enable SSL Inspection.

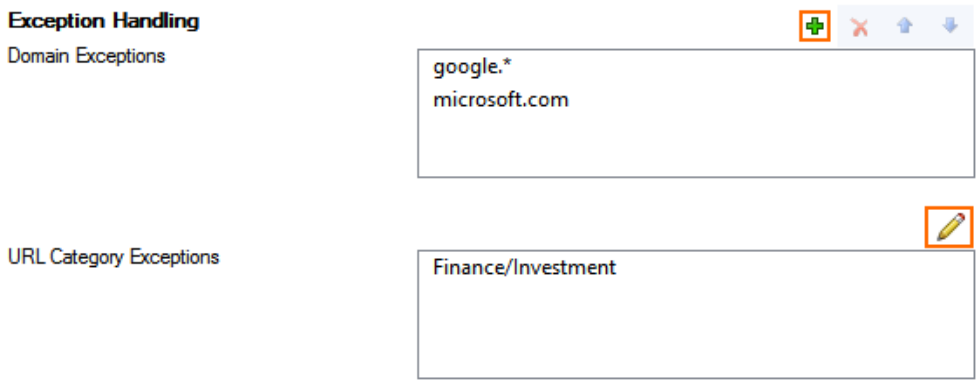
When set to **Auto**, the CloudGen Firewall will check for certificates and automatically enable SSL Inspection as soon as a valid license is detected.

4. Select the **CA Certificate** uploaded to the certificate store in Step 1 from the drop-down list.



5. Configure TLS Inspection **Exception Handling**. (This setting is only available when using the application ruleset instead of firewall policy profiles. For information on how to configure policies, see Policy Profiles and How to Create TLS Inspection Policies.
   - **Domain Exceptions** – Enter the domain names that are exempt from TLS Inspection. Subdomains are automatically included. Using * wildcards is allowed.

- **URL Category Exceptions** – Select URL Filter categories excluded from TLS Inspection.

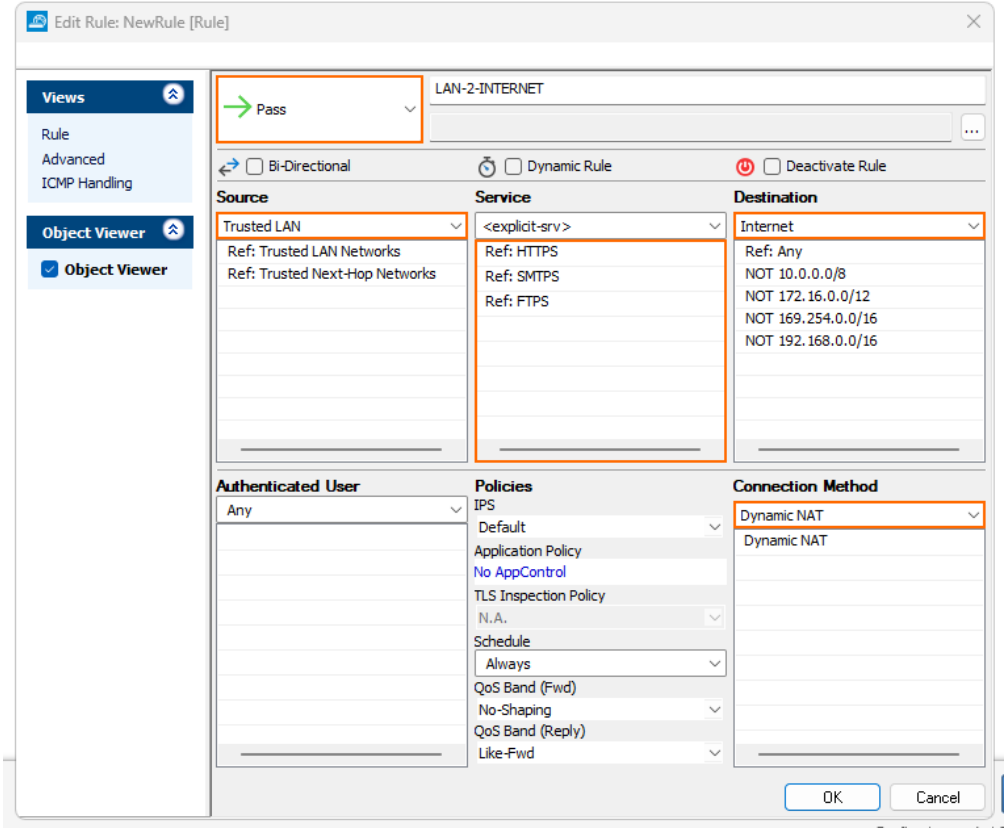


6. Click **Send Changes** and **Activate**.

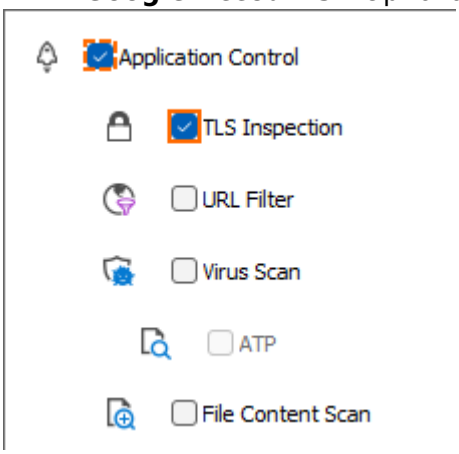
Step 3. Create an Access Rule for Outbound TLS Inspection

Enable TLS Inspection on the access rule handling outbound traffic.

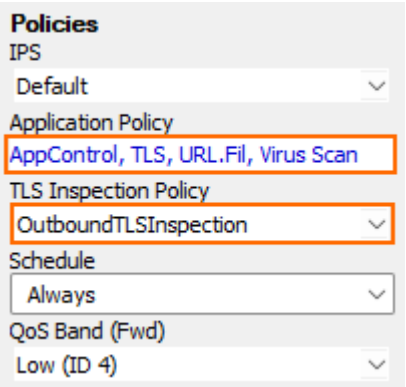
1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**
3. Either click the plus icon (**+**) in the top right of the ruleset or right-click the ruleset and select **New > Rule**.
4. Select **Pass** as the action.
5. Enter a **Name** for the rule.
6. Specify the following settings that must be matched by the traffic to be handled by the access rule:
   - **Source** – Select the internal network.
   - **Destination** – Select **Internet**.
   - **Service** – Select the services. E.g., HTTPS, FTPS, SMTPS,...
   - **Connection Method** – Select **Dynamic NAT.**



7. Click the **Application Policy** link and select**:**
   - **Application Control** – Required.
   - **SSL Inspection** – Required.
   - **Virus Scan** – Optional.
   - **ATP** – Optional.
   - **File Content Scan** – Optional.
   - **Safe Search** – Optional.
   - **Google Accounts** – Optional.



8. From the **SSL Inspection Policy** drop-down list, select a TLS Inspection policy for outbound TLS inspection. For more information, see [How to Create a TLS Inspection Policy for Inbound TLS Inspection](#).

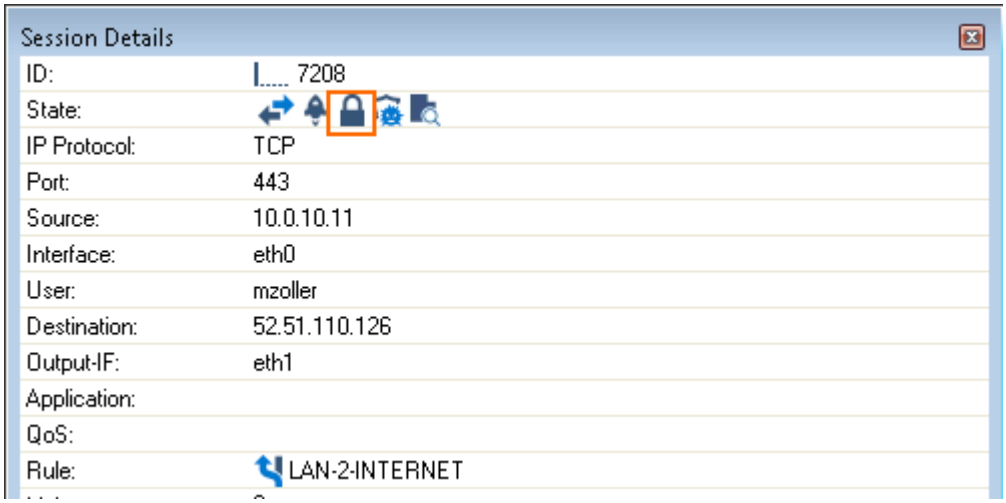


9. Click **OK**.
10. Click **Send Changes** and **Activate**.

Outbound TLS connections are now inspected by the firewall.

Monitoring and Troubleshooting

SSL Inspection error messages are written in the Firewall/SSL.log file. On the **FIREWALL > Live** page, the **State** column shows the padlock (🔒) icon for TLS-inspected connections.



Next Steps

Outbound TLS Inspection can be combined with the following features:

- Virus Scanning and ATP in the Firewall
- URL Filtering in the Firewall
- File Content Filtering in the Firewall

- User Agent Filtering in the Firewall
- How to Enforce SafeSearch in the Firewall
- How to Configure Google Accounts Filtering in the Firewall

Figures