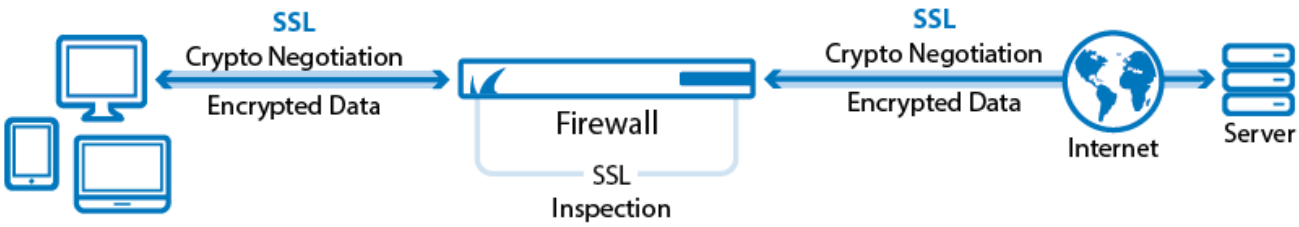
How to Configure Outbound SSL Inspection

https://campus.barracuda.com/doc/73719893/

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



Before You Begin

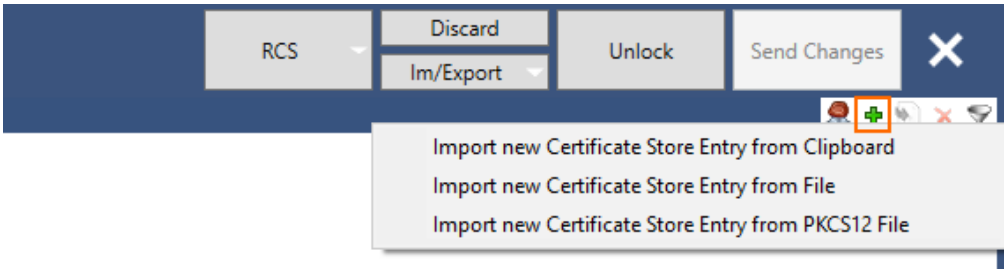
- Verify that the **Firewall Feature** level is set to **7.2** or higher.
- Create an SSL Inspection policy for outbound SSL Inspection. For more information, see How to Configure an SSL Inspection Policy for Outbound SSL Inspection.

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-left corner, click **+** and select **Import new Certificate Store Entry from File** or **Import new Certificate Store Entry from PKCS12**.

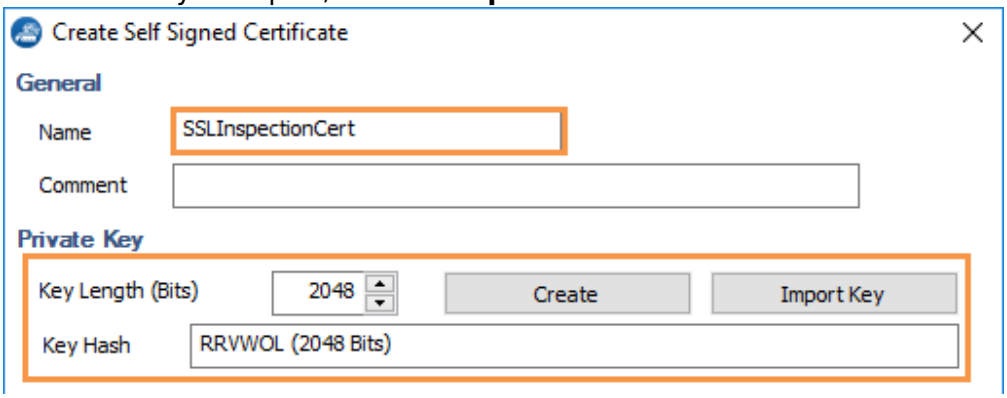


4. Select the certificate file and click **Open**.
5. (optional) Enter the **Password** and click **OK**.
6. Enter a **Name** and click **OK**.
7. (optional) If needed right-click the certificate and select **Assign Key to Certificate Store Entry**.
    1. Select the certificate key file and click **Open.**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

Generate Self-Signed Certificates on the Firewall

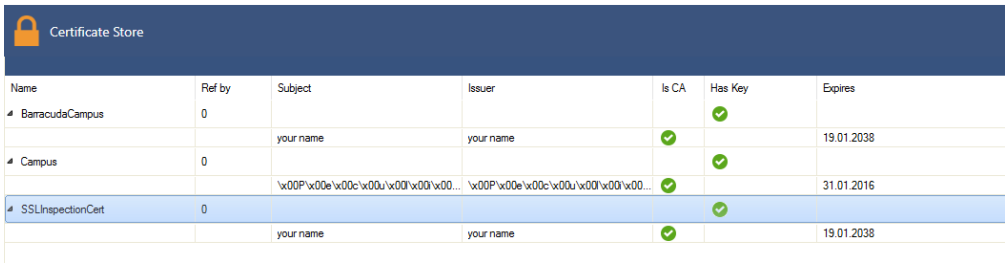
1. Go to the **Certificate store**. On a standalone firewall the certificate store is in the **Advanced Configuration**, on the Control Center in the **Global Settings**, **Range Settings** or **Cluster Settings**.
2. Click **Lock**.
3. Right-click in the table and select **Create Self Signed Certificate** or use the respective button 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**.



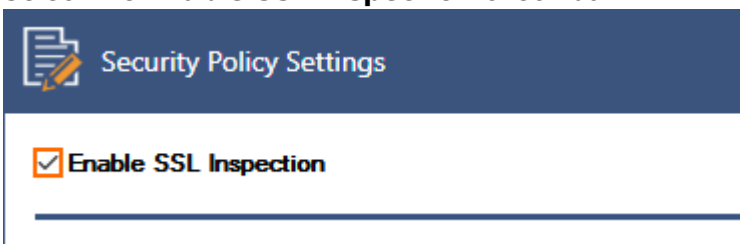
9. In the **Subject - Issuer** section, will in the required certificate information.
10. Click **OK**.

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

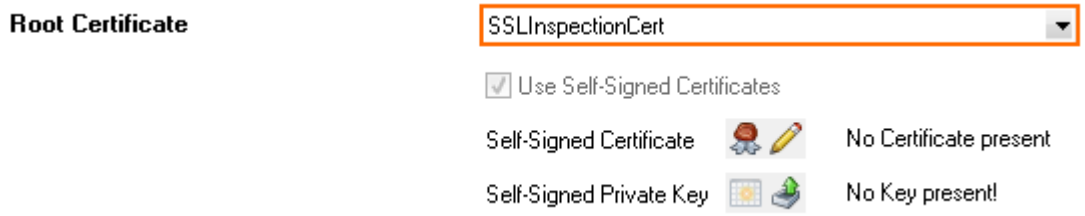


Step 2. Enable SSL Inspection

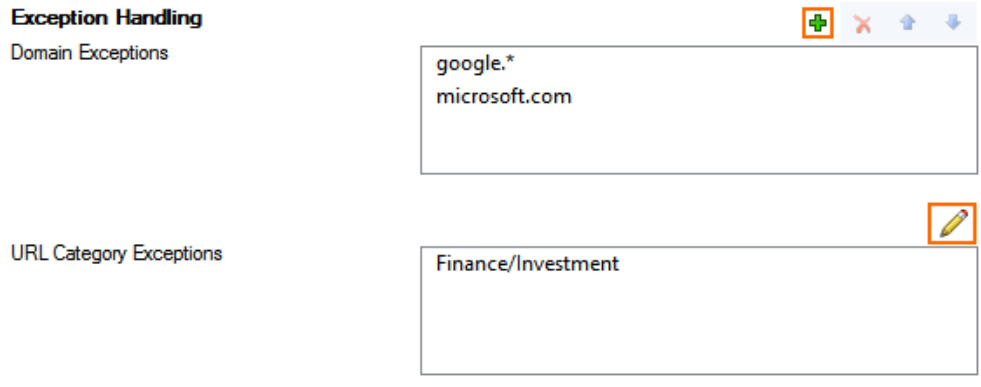
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server*** **> Assigned Services > Firewall > Security Policy** .
2. Click **Lock**.
3. Select the **Enable SSL Inspection** check box.



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



5. Configure SSL Inspection **Exception Handling**:
   - **Domain Exceptions** – Enter the domain names that are exempt from SSL Inspection. Subdomains are automatically included. Using * wildcards is allowed.
   - **URL Category Exceptions** – Select URL Filter categories excluded from SSL Inspection.

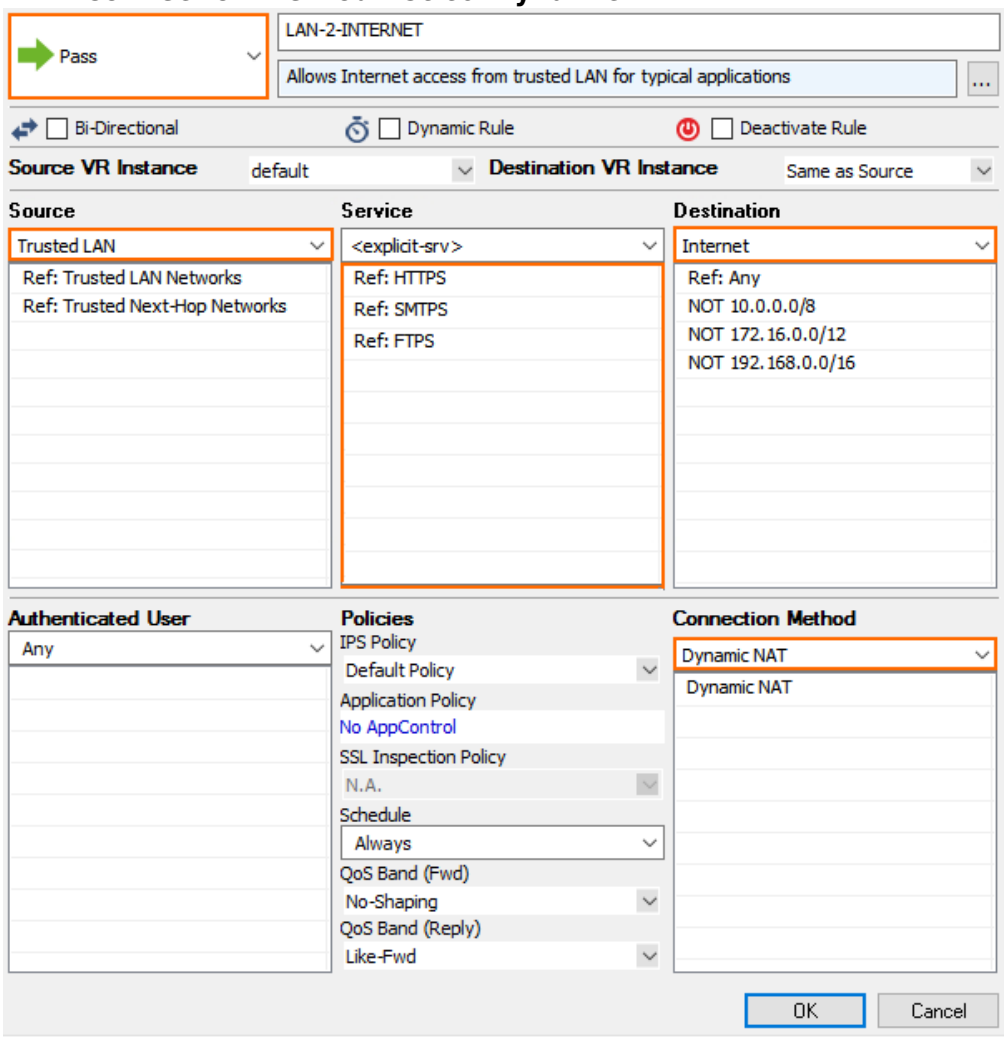


6. Click **Send Changes** and **Activate**.

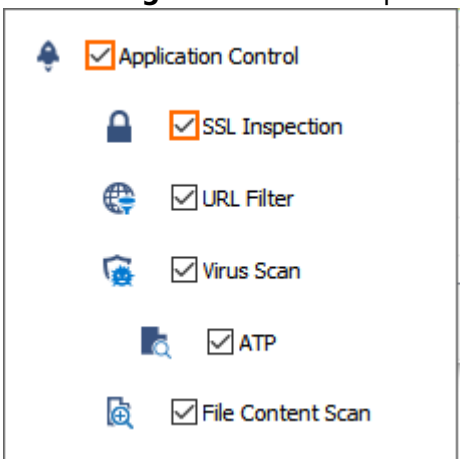
Step 3. Create Access Rule for Outbound SSL Inspection

Enable SSL Inspection on the access rule handling outbound traffic.

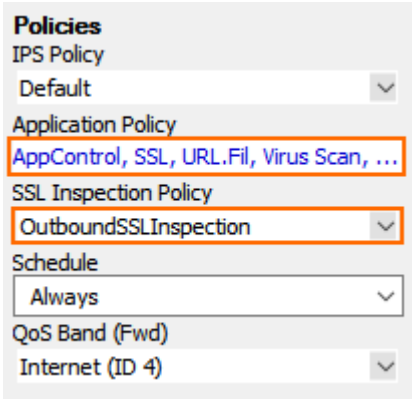
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**
3. Either click the plus icon (**+**) in the top right of the ruleset, or right-click the ruleset and select **New > Rule**.
4. Select **Pass** 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 an SSL Inspection policy for outbound SSL inspection. For more information, see How to Create an SSL Inspection Policy for Inbound SSL Inspection.

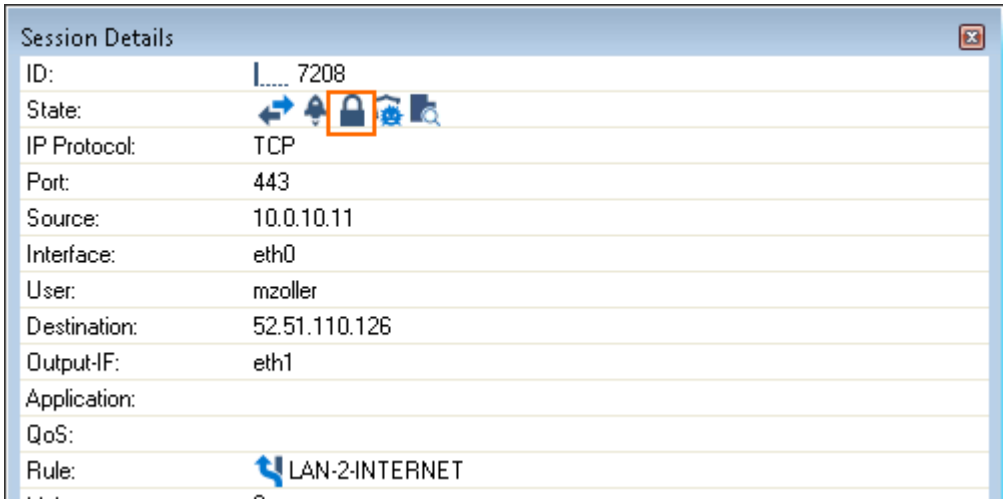


9. Click **OK**.
10. Click **Send Changes** and **Activate**.

Outbound SSL or TLS connections are now inspected by the firewall.

Monitoring and Troubleshooting

SSL Inspection error message are written the Firewall/SSL.log file. On the **FIREWALL > Live** page the **State** column show the padlock (🔒) icon for SSL inspected connections.



Next Steps

Outbound SSL 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 Safe Search in the Firewall
- How to Configure Google Accounts Filtering in the Firewall

Figures

1. ssl_inspection_outbound.png
2. cert_import.png
3. cert_create1.png
4. cert_create2.png
5. outbound_SSL_Inpection_00b.png
6. outbound_SSL_Inspection_01.png
7. outbound_SSL_Inspection_02.png
8. outbound_SSL_Inspection_04.png
9. outbound_SSL_Inspection_05.png
10. outbound_SSL_Inspection_06.png
11. outbound_SSL_Inspection_07.png
12. padlock.png
13. firewall_live_outbound.png