How to Configure an SSL Inspection Policy for Outbound SSL Inspection

https://campus.barracuda.com/doc/79463052/

The SSL Inspection policy contains the information needed for the firewall to be able to accept and initiate SSL or TLS connections for when intercepting SSL or TLS connections of clients protected by the firewall. The policy object defines the behavior when encountering validation errors or revocation check failures. SSL connections that do not meet these requirements are blocked. The SSL Inspection policy also defines the minimum SSL or TLS version as well as the allowed ciphers. The connection will be terminated if these minimum requirements are not met.

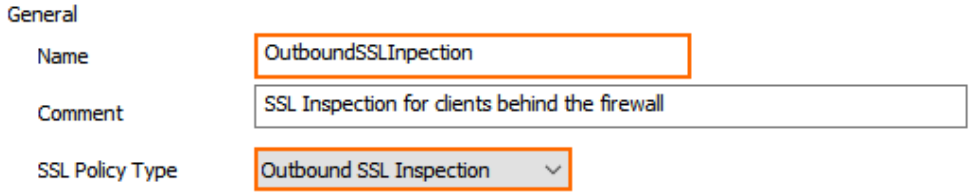
Before You Begin

Verify that the **Feature Level** of the Forwarding Firewall is set to 7.2 or higher.

Create SSL Inspection Policy Object

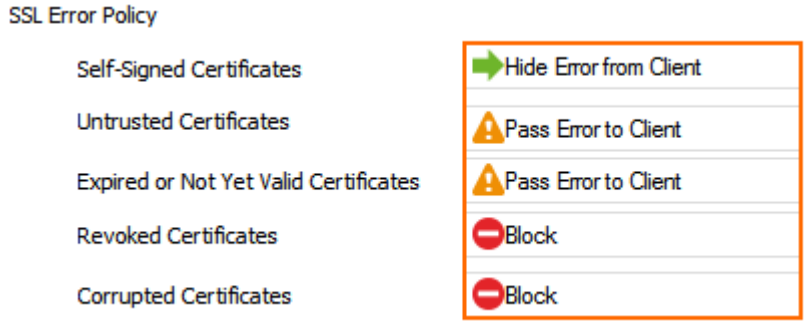
Create an SSL Inspection policy object for outbound SSL Inspection.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. In the left menu, click **SSL Inspection**.
4. Right-click the table and select **New Inspection Policy**. The **Edit SSL Inspection** window opens.
5. Enter the **Name**.
6. From the **SSL Policy Type** drop-down list, select **Outbound SSL Inspection** and, if required, select **Download Intermediate CA Certificates automatically** to automatically complete and import missing intermediate certificates.

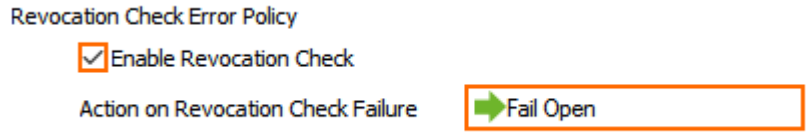


7. Configure the **SSL Validation Policy** settings. For more information on SSL Error Policies, see SSL Inspection in the Firewall.
   - **Self-Signed Certificates** – Select **Pass Error to Client**, **Hide Error from Client**, or **Block**.
   - **Untrusted Certificates** – Select **Pass Error to Client**, **Hide Error from Client**, or

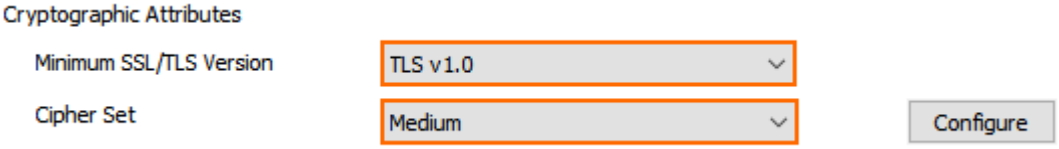
Block.
- **Expired of Not Yet Valid Certificates** – Select **Pass Error to Client**, **Hide Error from Client**, or **Block**.
- **Revoked Certificates** – Select **Hide Error from Client**, or **Block**.
- **Corrupted Certificates** – Select **Pass Error to Client**, **Hide Error from Client**, or **Block**.



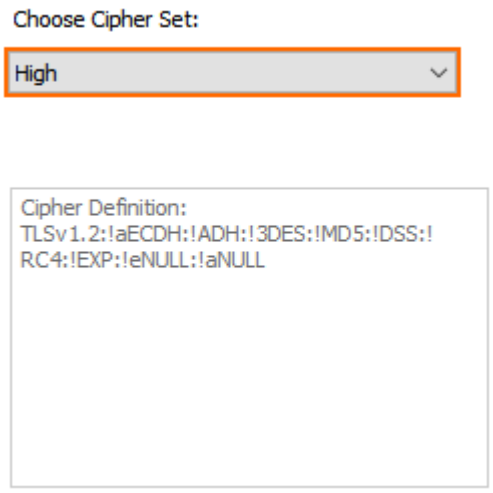
8. Select the **Enable Revocation Check** check box to check the revocation status of the certificate via OCSP stapling, OCSP, or CRL.
9. Configure the **Action on Revocation Check Error**:
   - **Fail Open** – If the revocation check fails due to operational errors, the connection is allowed.
   - **Fail Close** – If the revocation check fails due to operational errors, the connection is blocked.



10. (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.



11. (optional) Click **Configure** to customize cipher set.



12. Click **OK**
13. Click **Send Changes** and **Activate**.

Next Steps

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

Figures

1. outbound_ssl_policy_01.png
2. outbound_ssl_policy_02.png
3. outbound_ssl_policy_03.png
4. sslPolicy05.png
5. sslPolicy06.png