How to Configure a TLS Inspection Policy for Outbound TLS Inspection

https://campus.barracuda.com/doc/96026322/

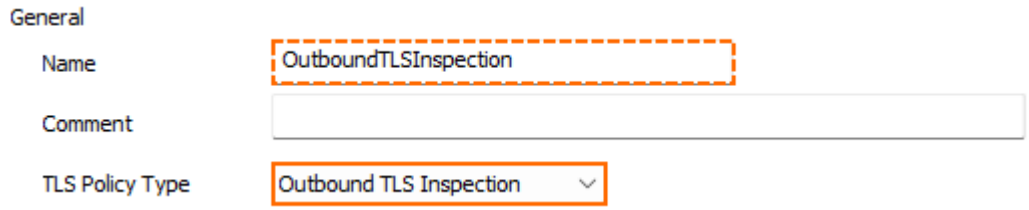
The TLS Inspection policy contains the information needed for the firewall to be able to accept and initiate TLS connections when intercepting TLS connections of clients protected by the firewall. The policy object defines the behavior when encountering validation errors or revocation check failures.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

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 TLS Inspection Policies.

Create TLS Inspection Policy Object

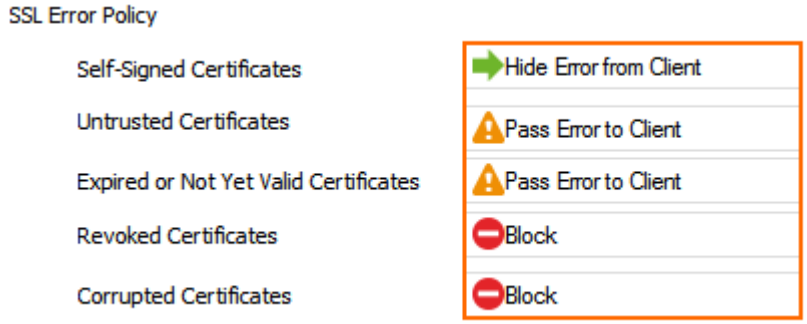
Create a TLS Inspection policy object for outbound TLS Inspection.

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 Inspection Policy**. The **Edit TLS Inspection** window opens.
5. Enter the **Name**.
6. From the **TLS Policy Type** drop-down list, select **Outbound TLS Inspection** and, if required, select **Download Intermediate CA Certificates automatically** to automatically complete and import missing intermediate certificates.

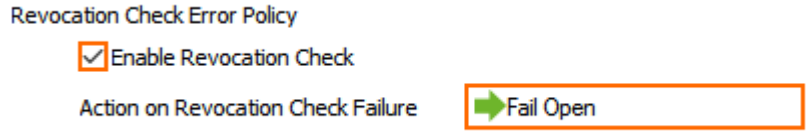


7. Configure the **TLS Validation Policy** settings. For more information on TLS Error Policies, see TLS Inspection in the Firewall.
   - **Self-Signed Certificates** – Select **Pass Error to Client**, **Hide Error from Client**, or

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**.

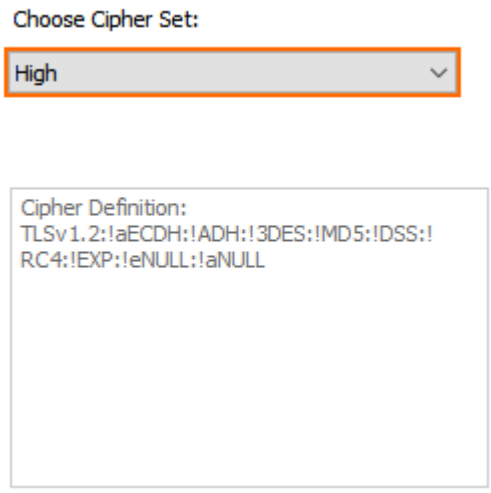


8. Select the **Enable Revocation Check** check box to check the revocation status of the certificate via OCSP stapling, OCSP, or CRL.
9. Configure the **Action on Revocation Check Error**:
   - **Fail Open** – If the revocation check fails due to operational errors, the connection is allowed.
   - **Fail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



10. (optional) Configure **Cryptographic Attributes**:
    - **Minimum 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.
11. (optional) Click **Configure** to customize the cipher set.



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

Next Steps

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

Figures

1. outbound_tls_policy_01.png
2. outbound_ssl_policy_02.png
3. outbound_ssl_policy_03.png
4. sslPolicy06.png