

TLS Inspection Policies

<https://campus.barracuda.com/doc/98210334/>

TLS Inspection decrypts TLS/SSL connections so the appliance can allow features, such as Malware Protection and IPS, to scan traffic that would otherwise not be visible to the service. You can use a default TLS Inspection policy profile for your access rules, or you can create an explicit profile to match individual requirements.

TLS Inspection Shared Policy Profiles

Name	Origin	Refer...	Description
0 GlobSSLInsp	Local	0	

GlobSSLInsp

TLS Inspection Policy Profile

References

Name	Description	Action	TLS Inspection ...	Source	Destination	Application	User	URL Filter Match
0 TlsDefault		Inspect	Default	Private 192.168.0.0/16	Internet 0.0.0.0/0, NOT 10.0.0.0/8, ...	Any	Any	Any

For information on how to customize default policy profiles, see [How to Configure Policy Profiles](#).

Before You Begin

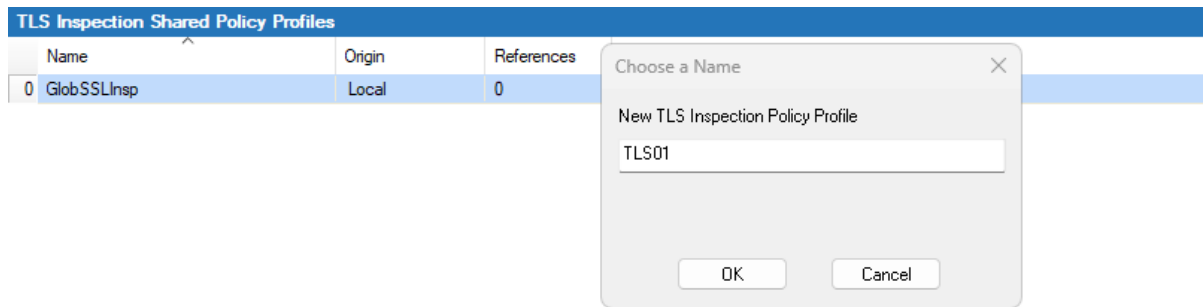
- Create or upload the server certificate to be used for TLS Inspection. For more information, see [How to Manage Certificates in the Certificate Store](#).

Create a TLS Inspection Policy Profile

Create an explicit TLS inspection policy profile to match individual requirements.

Policy profiles are created on the Control Center. On stand-alone CloudGen Firewalls, you can customize the default profiles and add explicit policies if required.

1. (On the Control Center) Go to **CONFIGURATION > Configuration Tree > Multi-Range > Global Settings > Global Firewall Objects/Policies**.
2. Click **Lock**.
3. In the left menu, expand **Policy Profiles**.
4. Select **TLS/SSL Inspection**. The TLS inspection policies window opens.
5. To add a new policy profile, click the plus icon at the top right of the window, enter a profile name, and click **OK**.



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

The policy profile now appears in the **TLS Inspection Shared Policy Profiles** list, and you can create explicit policies for it.


Create an Explicit TLS Inspection Policy

1. (On the Control Center) Go to **CONFIGURATION > Configuration Tree > Multi-Range > Global Settings > Global Firewall Objects/Policies**.
2. (On a CloudGen Firewall) Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
3. Click **Lock**.
4. In the left menu, expand **Policy Profiles**.
5. Select **TLS/SSL Inspection**. The TLS inspection policies window opens.
6. (Control Center only) Select the profile you wish to create the policy for. The explicit policy list appears in the lower window.
7. (Control Center only) To add a new policy, click the plus icon (+) at the top right of the lower window. You can also right-click the list and select **Add Policy**.
(CloudGen Firewall only) To add a new policy, click the plus icon (+) at the top right. You can also right-click the list and select **Add Policy**.
8. Specify values for the following:
 - **Name** – Enter a descriptive name for the explicit policy.
 - **Description** – Enter a description for the policy.
 - **Action** – Select either Inspect or Do Not Inspect.
 - **TLS Policy** – Select either the default or an explicit policy.
 - **Source / Destination IP / Network Criteria** – Select the source and destination network, or select **<Explicit Network>** and enter an IP address/network or a domain that gets resolved to an IP address for the matching.
 - **Application Criteria** – Define the application match condition. Add an application the policy should apply to, or create explicit applications. To open the selection menu, double-click the corresponding field. Selecting applications in the application editor works similarly to the process in the object configuration for the application rule set. For more information, see [How to Create an Application Object](#) and [How to Create a Custom Application Object](#).
 - **Users** – Select the users or groups the policy should apply.

- **URL Category** – Specify URL categories the policy should apply to.

☒ TLS Inspection

General

Name	<input checked="" type="checkbox"/> TLSDefault
Description	<input type="text"/>
Action	<input checked="" type="checkbox"/>  Inspect ▼
TLS Policy	Default ▼

Criteria

Source IP/Network Criteria	Any ▼ ... 0.0.0.0/0
Destination IP/Network Criteria	Any ▼ ... 0.0.0.0/0
Application Criteria	▼ ... Match for any Application
Users	▼ ...
URL Category	▼ ...

9. Click **OK**.

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

The policy is now listed in the lower window and can be selected in your forwarding rules. For more information, see the last step in [How to Configure Policy Profiles](#).

Figures

1. tls_pol_overview.png
2. tls_new.png
3. add_ico.png
4. add_ico.png
5. TLS_exp.png

© Barracuda Networks Inc., 2024 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.