

IPS Policies

<https://campus.barracuda.com/doc/98210335/>

Configure IPS scanning policies to control the behavior of the IPS engine when an attack is detected. By default, all access rules use the default IPS policy. You can also customize the default settings or create custom IPS policies to apply to your access rules. Each of the created policies can be applied individually.

IPS Shared Policy Profiles							
Name	Origin	References	Description				
0	GloIPSRule	Local	1				

GloIPSRule							
IPS		References					
Name	Description	Action	Source	Destination	Application	User	URL Filter Match
0	SC	Scan & Enforce	Management IP	DHCP1 Local IP	Any	Any	Any
1	IpsDefault	Scan & Enforce	Any 0.0.0.0/0	Any 0.0.0.0/0	Any	Any	Any

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

Before You Begin

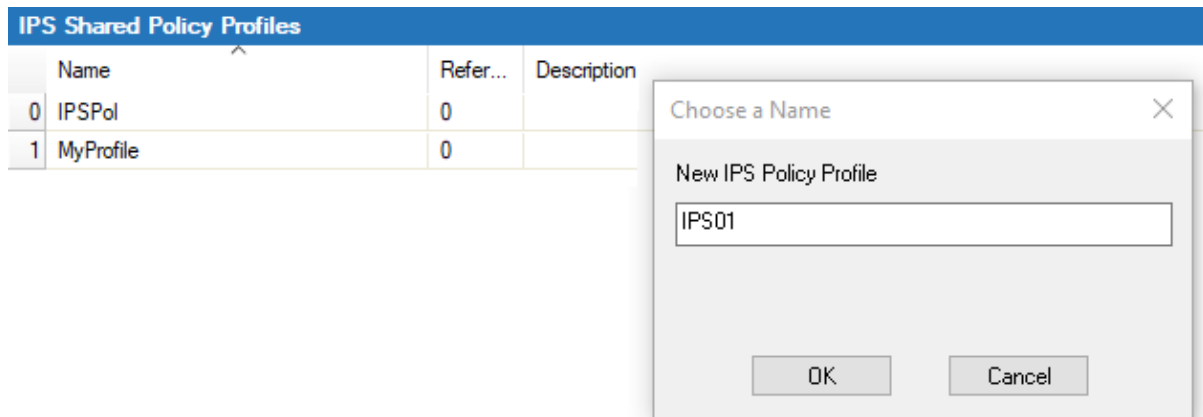
Make sure that TLS Inspection is enabled in the **Security Settings**. For more information, see [How to Configure Outbound TLS Inspection](#).

Create an IPS Policy Profile

Create an explicit IPS 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 **IPS**.
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 **IPS Shared Policy Profiles** list, and you can create explicit policies for it.

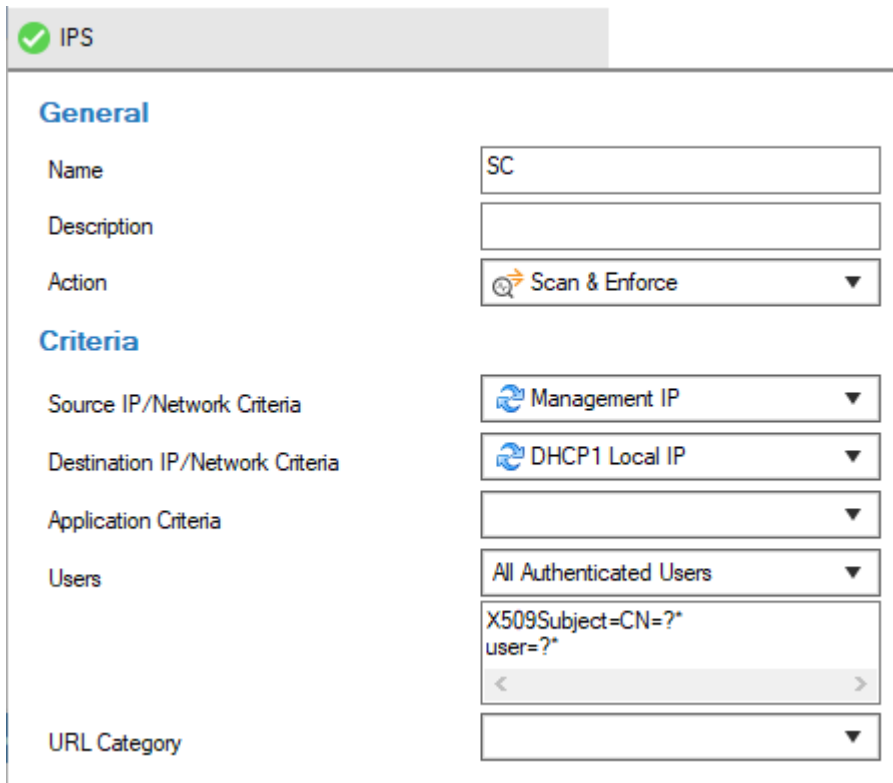
Create an Explicit IPS Policy

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 **IPS**.
6. (Control Center only) Select the profile you wish to create the policy for. The policy list appears under the corresponding tab 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 an action.
 - **Do Not Scan**- IPS does not scan traffic matching the criteria.
 - **Scan & Log**- IPS only scans and logs the events.
 - **Scan & Enforce** - IPS is enforced.
 - **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 similar to the process in the objects 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 to.
- **URL Category** – Specify URL categories the policy should apply to.

9. Click **OK**.



✓ IPS

General

Name SC

Description

Action Scan & Enforce

Criteria

Source IP/Network Criteria Management IP

Destination IP/Network Criteria DHCP1 Local IP

Application Criteria

Users All Authenticated Users

X509Subject=CN=?*
user=?*

URL Category

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

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

Figures

1. ips-pol_overview.png
2. +.ico.png
3. ips_new.png
4. add_ico.png
5. add_ico.png
6. ips_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.