

Malware Protection Policies

<https://campus.barracuda.com/doc/98210333/>

You can configure the Malware Protection policy to either scan or not scan traffic by default. Scanning is done according to the virus scanner configuration and, if an Advanced Threat Protection (ATP) license is present, also by the ATP engine. When performing an ATP scan, a hash DB lookup is performed before a user receives a downloaded file, which compares a hash of the file with the Barracuda database to see if it is a malicious file. Simultaneously, the file is uploaded to the Barracuda Advanced Threat Protection (ATP) cloud if the file size is 10 megabytes or less (see [Advanced Threat Protection \(ATP\)](#) for general information). Depending on the behavior of the file, it is assigned a threat level that is transmitted to the appliance. The file is then either blocked or delivered.

Malware Protection Shared Policy Profiles							
Name	Origin	References	Description				
0 GlobMalWA	Local	1					

GlobMalWA							
Malware Protection		References					
Name	Description	Action	Source	Destination	Application	User	URL Filter Match
0 AV		Do Not Scan	Service IPs	DHCP6 Local IP	Any	Any	Any
1 AVDefault		Scan	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

When using Malware Protection for HTTPS and FTPS, make sure that TLS Inspection is enabled in the **Security Settings**. For more information, see [How to Configure Outbound TLS Inspection](#).

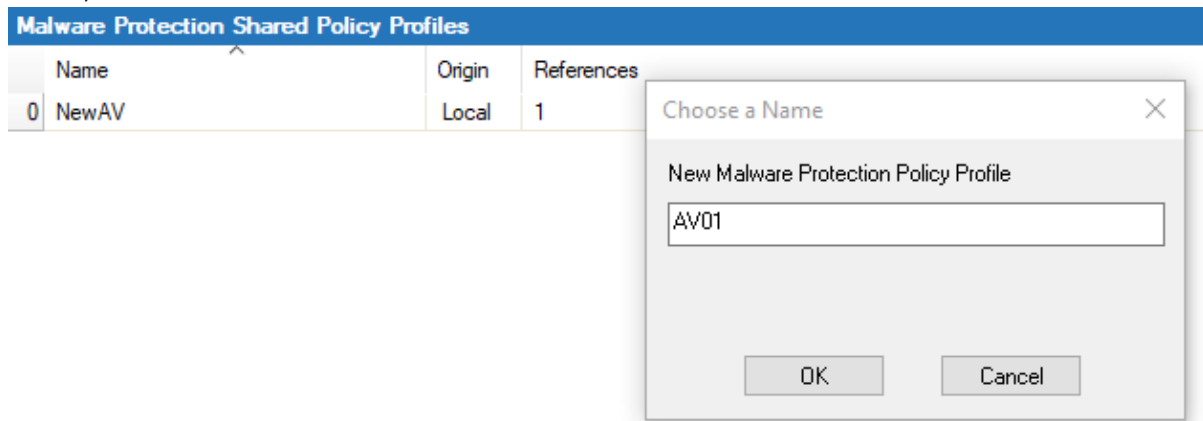
Create a Malware Protection Policy Profile

Create an explicit Malware Protection policy profile to match individual requirements.

Policy profiles are created on the Control Center. On standalone 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 **Malware Protection**.
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**.

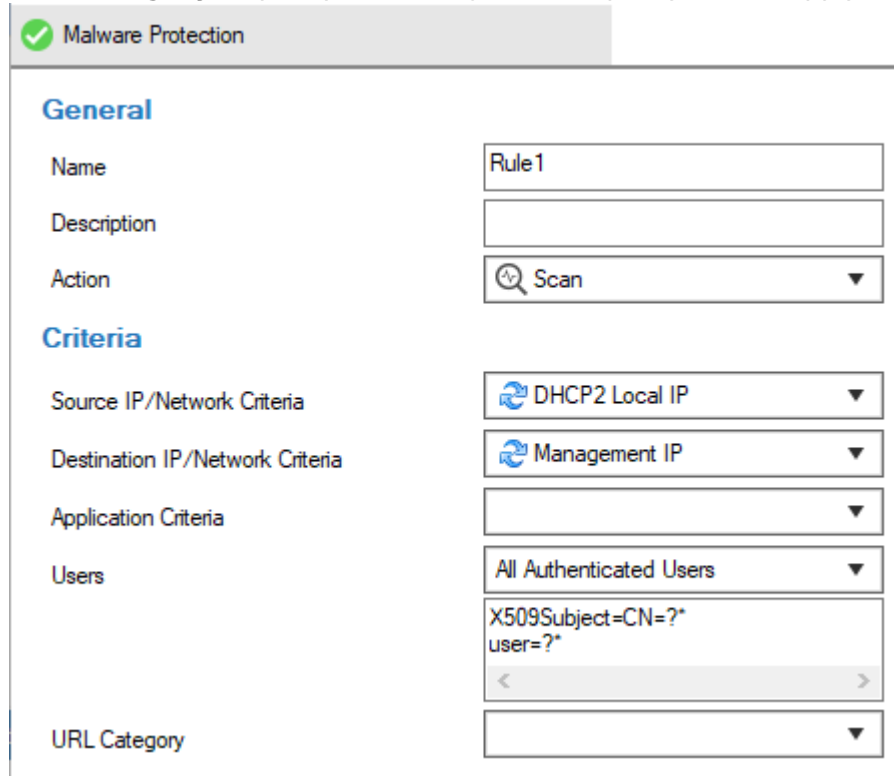
The policy profile now appears in the **Malware Protection Shared Policy Profiles** list, and you can create explicit policies for it.

Create an Explicit Malware Protection 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 **Malware Protection**. The malware protection policies window opens.
6. (Control Center only) Select the profile you wish to create the policy for. The related 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 **Scan** or **Do Not Scan**.
 - **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.



The screenshot shows the 'Malware Protection' configuration window. At the top, there is a green checkmark icon and the text 'Malware Protection'. Below this, the 'General' section contains fields for 'Name' (Rule1), 'Description' (empty), and 'Action' (Scan). The 'Criteria' section contains dropdown menus for 'Source IP/Network Criteria' (DHCP2 Local IP), 'Destination IP/Network Criteria' (Management IP), 'Application Criteria' (empty), 'Users' (All Authenticated Users), and 'URL Category' (empty). Below the 'Users' dropdown, there is a text box containing 'X509Subject=CN=?*' and 'user=?*', with left and right arrow buttons.

9. Click **OK**.
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. mal-pol_overview.png
2. +.ico.png
3. av_new.png
4. add_ico.png
5. add_ico.png
6. av_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.