How to Configure Policy Profiles

https://campus.barracuda.com/doc/98210329/

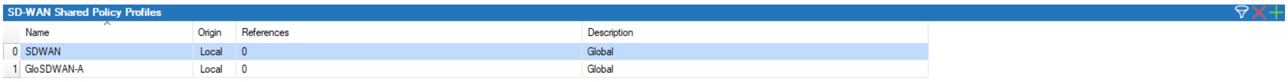
Some policy profiles come with preconfigured default rules. You can either customize the default profiles by adding or modifying policies, or create new profiles with explicit policies. Explicit policies have precedence over predefined ones. The matching algorithm works as follows: All policies (explicit and default) apply top down. That means the first policy in the list that matches applies. Policies below the first match will not apply. First, the explicit policies are searched for matches. If there is an explicit rule that matches, this explicit rule will be used. Otherwise, the default rules are searched, and if there is a rule that matches, this rule will be used. For general information on the different types of profiles, see Policy Profiles. Policy profiles can be applied to forwarding rules, for example, instead of introducing firewall objects (for general information, see Firewall Objects).

When configuring policy profiles on a range or cluster, you must enable firewall objects for the respective level. For more information, see How to Enable Firewall Objects on a Range or Cluster Level. Barracuda Secure Connector and the global and local rule sets of the Distributed Firewall only support globally defined policy profiles configured on a Control Center.

Policy Profiles - Configuration Functions

On the Firewall Control Center, the policy profiles configuration window offers the following functions, depending on the policy type:

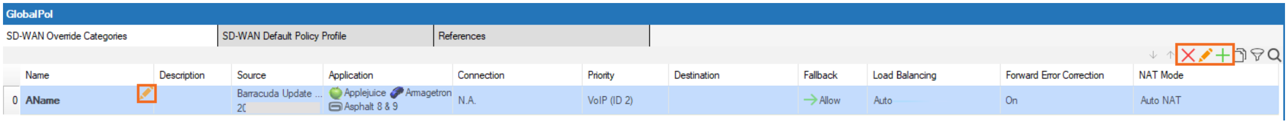
- **Shared Policy Profiles** – Displays the policy profiles in the upper window that contain default and/or explicit policies. Selecting a profile shows the policies under the corresponding tab in the lower window, where you can create and modify the policy entries. To create a new policy profile, click the green plus icon (+) in the top-right corner of the window. To remove a profile from the list, click the delete icon (✕).



SD-WAN Shared Policy Profiles

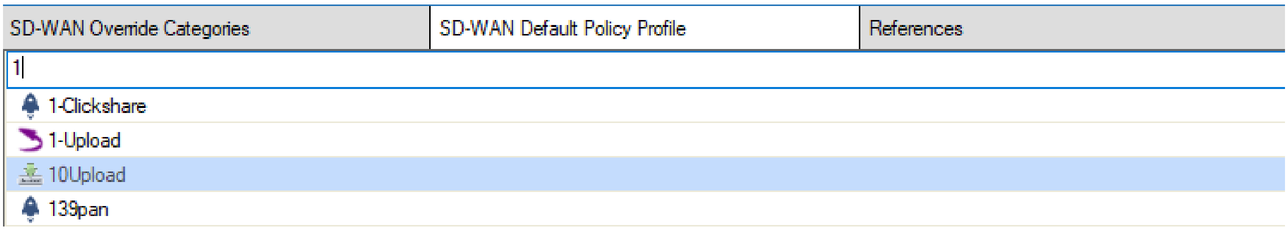
	Name	Origin	References	Description
0	SDWAN	Local	0	Global
1	GloSDWAN-A	Local	0	Global

- **Default / Explicit Policy Profile / SD-WAN Override Categories** – The tabs in the lower window show all policies that are available by default or that have been explicitly created for a selected profile, depending on the policy type. Click the plus icon (+) at the top right of the lower window to create a new policy for a selected profile. Double-click an entry, or use the pen icon (✎), to edit the settings. This icon also becomes visible in the top-right corner for in-place editing when hovering over a field. To remove a policy, click the delete icon (✕).



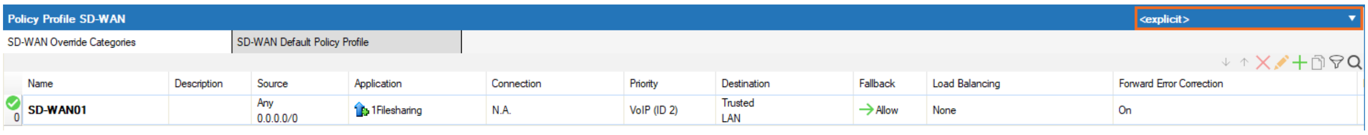
	Name	Description	Source	Application	Connection	Priority	Destination	Fallback	Load Balancing	Forward Error Correction	NAT Mode
0	AName		Barracuda Update ... 20	Applejuice Armagetron Asphalt 8 & 9	N.A.	VoIP (ID 2)		Allow	Auto	On	Auto NAT

To select applications, use the application filtering search bar.



- **References** – Shows profile-specific dependencies, such as type, range, cluster, and firewall unit a selected policy object refers to.

On the CloudGen Firewall, you can access the policies via the forwarding rule set. To view the profiles configured for an instance, go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**. Depending on the configuration level of the policies you want to use, you can select global profiles or profiles that have been created on a specific range or cluster by expanding the selection menu on the top-right of the rules window.



	Name	Description	Source	Application	Connection	Priority	Destination	Fallback	Load Balancing	Forward Error Correction
✓ 0	SD-WAN01		Any 0.0.0.0/0	1Filesharing	N.A.	VoIP (ID 2)	Trusted LAN	→ Allow	None	On

Configuring Policy Profiles

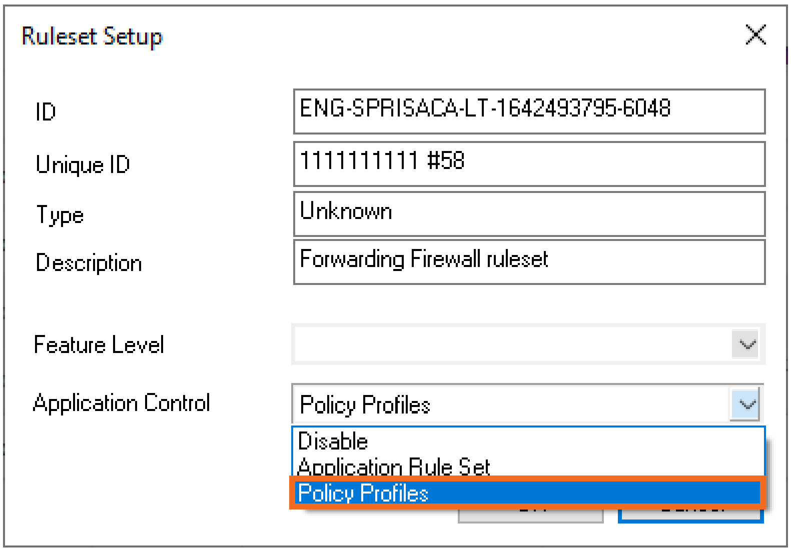
You can either edit a policy profile and make your adjustments to the associated policies, or create explicit profiles with custom policies. Policy profiles are created on the Control Center. On stand-alone CloudGen Firewalls, you can customize the default profiles and add explicit policies if required.

Before You Begin

When configuring policies on a CloudGen Firewall, enable policy profiles in the forwarding firewall rule set to switch from the application rule set to policies to be used in rules.

> If you have enabled application-based provider selection or other application-related details in an access rule, resetting the application rule set replaces the configured object with default settings. For this reason, make sure you save the rule to a file or repository if you want to revert to the old rule set later.

1. On the CloudGen Firewall, go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. In the left menu, expand **Settings** and select **Setup**. The **Ruleset Setup** window opens.
3. From the **Application Control** drop-down list, select **Policy Profiles**.



Ruleset Setup

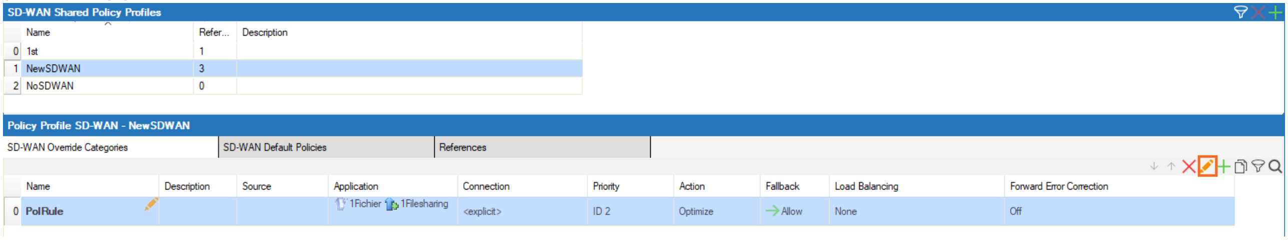
ID	ENG-SPRISACA-LT-1642493795-6048
Unique ID	1111111111 #58
Type	Unknown
Description	Forwarding Firewall ruleset
Feature Level	
Application Control	Policy Profiles

4. Click **OK**.

Customizing Policy Profiles

Edit a policy profile on the Firewall Control Center, or make your adjustments to the default policies according to the settings described in the individual steps for each profile type under the section **Create Policy Profiles and Policies** below.

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** and select the profile type you want to configure. The policy profile configuration window opens.
4. Select the profile you want to customize. If any policies are associated with a selected profile, they appear in the corresponding tab in the lower window. You can also select and customize a default policy in the lower window,
5. Edit the policy entries and configure the settings as described in the individual steps for each profile type.



SD-WAN Shared Policy Profiles

	Name	Refer...	Description
0	1st	1	
1	NewSDWAN	3	
2	NoSDWAN	0	

Policy Profile SD-WAN - NewSDWAN

	Name	Description	Source	Application	Connection	Priority	Action	Fallback	Load Balancing	Forward Error Correction
0	PolRule			1Fichier 1Filesharing	<explicit>	ID 2	Optimize	Allow	None	Off

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

Creating Policy Profiles and Policies

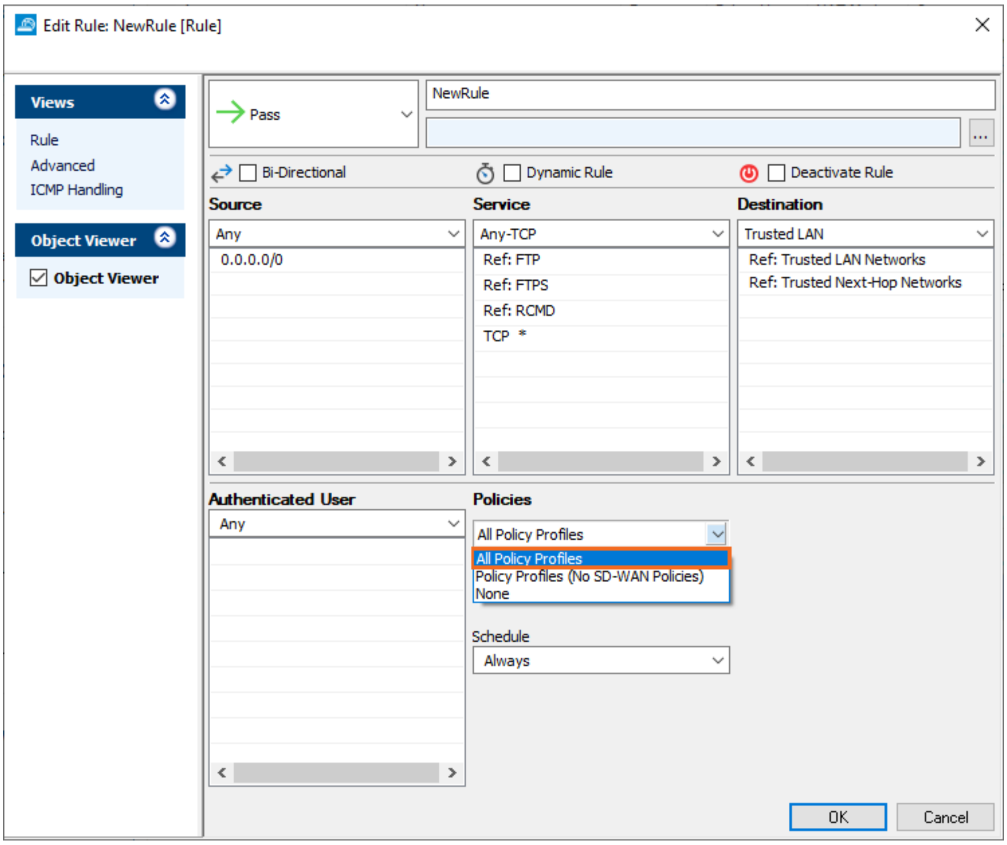
Create new profiles and add explicit policies to match individual requirements. See the following articles for instructions on how to create and configure policy profiles:

- SD-WAN Policies
- Application Policies
- URL Filtering Policies
- Malware Protection Policies
- TLS Inspection Policies
- IPS Policies

Applying Policies to Access Rules

The policy profiles listed under **Policies / Shared Profiles** can be selected when defining policy handling in forwarding rules. To enable policy profiles in an access rule, expand the **Policies** drop-down menu in the configuration and select how the rule should process traffic associated with the rule.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Create or edit the rule you wish to apply the profile to.
3. In the rule configuration window, expand the **Policies** drop-down menu and select one of the following options:
    - **All Policy Profiles** – Enable all policy profiles for the rule.
    - **Policy Profiles (No SD-WAN Policies)** – Enable all policy profiles except SD-WAN policies.
    - **None** – Do not use policy profiles.



Edit Rule: NewRule [Rule]

Pass

NewRule

☐ Bi-Directional ☐ Dynamic Rule ☐ Deactivate Rule

Source

Any

0.0.0.0/0

Service

Any-TCP

Ref: FTP

Ref: FTPS

Ref: RCMD

TCP *

Destination

Trusted LAN

Ref: Trusted LAN Networks

Ref: Trusted Next-Hop Networks

Authenticated User

Any

Policies

All Policy Profiles

All Policy Profiles

Policy Profiles (No SD-WAN Policies)

None

Schedule

Always

When creating an access rule, you can also specify the connection method. For detailed information on the **NAT Mode** parameter, see SD-WAN Policies. For general information on forwarding rules, see instructions on how to create rules under Access Rules.

Figures