
How to Create an Application Rule

<https://campus.barracuda.com/doc/43846958/>

Configuring an application rule is similar to configuring an access rule. You can enable Application Control 2.0 features on a per access rule basis. Application rules allow you to block or throttle traffic for detected applications. You can optionally combine the application rule with a URL filter policy objects. The application ruleset is evaluated every time an access rule matches that has enabled any of the Application Control options. Make sure the matching access rule allows all protocols needed for the applications you are creating policies for. The application ruleset can be created as a positive or negative list, depending on whether the default policy is set to allow or block undetected applications per default. In most cases setting the default policy to allow undetected applications and then creating application rules to block or throttle application traffic is the recommended setup.

In this article:

Before you Begin

- Verify that you have enabled Application Control 2.0 and that you are using the latest feature level of the Firewall service. For more information, see [How to Enable Application Control 2.0](#).
- Create **Application Objects** and/or **Application Filters** necessary for your application policies. For more information, see [How to Create an Application Object](#) and [How to Create an Application Filter](#).

Step 1. Enable Application Control Features in the Access Rule

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**.
2. Double-click to edit the access rule you want to enable application control for.
3. Click on the **Application Policy** link.

Authenticated User	Policy	Connection Method
Any	IPS Policy	Dynamic SNAT
	Default	Source-based NAT
	Application Policy	
	No AppControl	
	Schedule	
	Always	
	QoS Band (Fwd)	
	Internet (ID 4)	
	QoS Band (Reply)	
	Like-Fwd	

4. Select the Application Control 2.0 features used for this access rule:

- **Application Control**
- **SSL Interception**
- **URL Filter**
- **AV Scan**
- **ATD**
- **Safe Search**
- **YouTube for Schools**

- Application Control
- SSL Interception
- URL Filter
- AV Scan
- ATD
- Safe Search
- YouTube for Schools

5. Click **OK**.

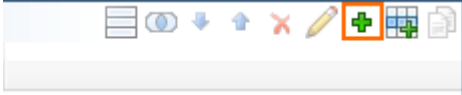
6. Click **Send Changes** and **Activate**.

Step 2. Create an Application Rule

For each application policy create an application rule. Rules are evaluated from the top to bottom. The action set in the first matching rule is executed.

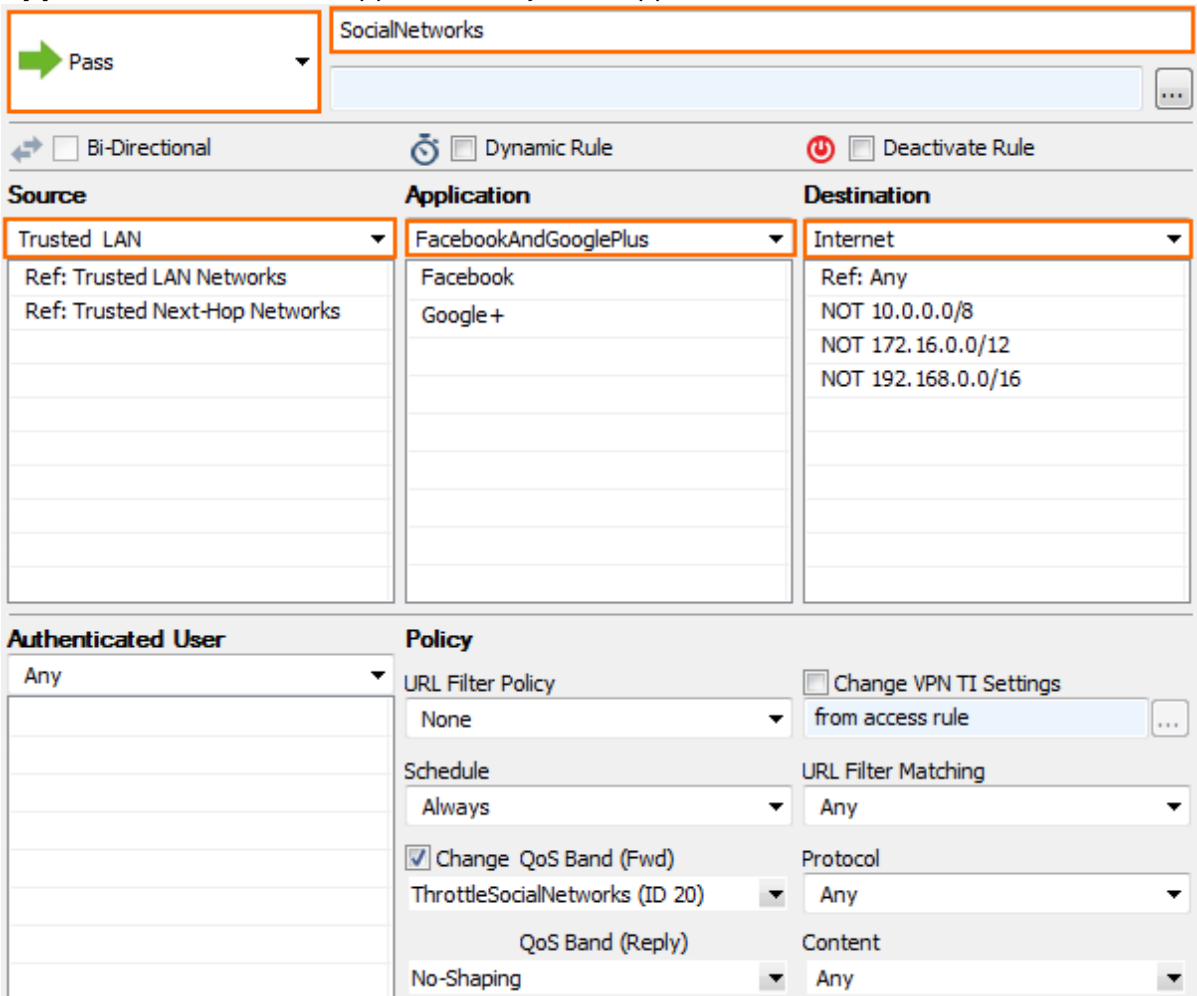
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**.
2. In the left menu, click **Application Rules**.

3. Click **Lock**.
4. Click the green plus sign (+) in the top right of the page or right-click the rule set and select **New > Rule**. An application rule **New Rule** is added to the application ruleset.



5. Double click on the **New Rule** application rule you just created. The **Edit Rule** window opens.
6. Select **Pass** or **Deny** as the action.
7. Enter a **name** for the rule. For example, LAN-DMZ.
8. Specify the following settings that must be matched by the traffic to be handled by the access rule:

- **Source** - The source addresses of the traffic. The source must be the same or a subset of the source of the matching access rule.
- **Destination** - The destination addresses of the traffic. The destination must be the same or a subset of the destination of the matching access rule.
- **Application** - Select the application object or application filter.



Bi-Directional Dynamic Rule Deactivate Rule

Source	Application	Destination
Trusted LAN	FacebookAndGooglePlus	Internet
Ref: Trusted LAN Networks Ref: Trusted Next-Hop Networks	Facebook Google +	Ref: Any NOT 10.0.0.0/8 NOT 172.16.0.0/12 NOT 192.168.0.0/16

Authenticated User	Policy
Any	URL Filter Policy: None Schedule: Always <input checked="" type="checkbox"/> Change QoS Band (Fwd): ThrottleSocialNetworks (ID 20) QoS Band (Reply): No-Shaping <input type="checkbox"/> Change VPN TI Settings: from access rule URL Filter Matching: Any Protocol: Any Content: Any

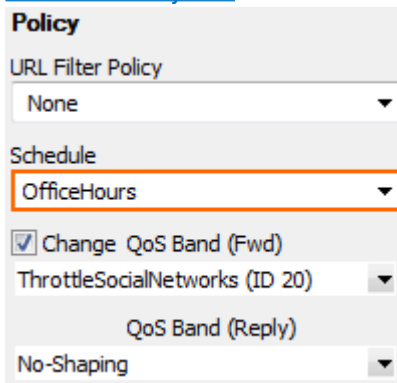
For the example access rule displayed above, a network object named **FacebookAndGooglePlus** has been created. For more information, see [How to Create an Application Object](#) and [How to Create an Application Filter](#).

9. Set **Additional Matching Criteria** or change the **QoS Bands** as needed (see below).

10. Click **OK**.
11. Drag and drop the application rule so that it is the first rule that matches the traffic that you want it to forward. Ensure that the rule is located *above* the BLOCKALL rule; rules located below the BLOCKALL rule are never executed.
12. Click **Send Changes** and **Activate**.

Additional Matching Criteria

- **Authenticated User** – Select a user object to apply this application policy only to a specific user group. For example, you can use this to allow social media access to specific employees, whereas an application policy below denies it for everybody else. For more information, see [User Objects](#).
- **Schedule Objects** – Applies time restrictions to the application policy. For example, you can use a schedule object to throttle social media during office hours. For more information, see [Schedule Objects](#).



The screenshot shows a configuration window for a Policy. The 'URL Filter Policy' is set to 'None'. The 'Schedule' dropdown menu is highlighted with an orange border and shows 'OfficeHours' selected. Below the schedule, there is a checked checkbox for 'Change QoS Band (Fwd)' and a dropdown for 'ThrottleSocialNetworks (ID 20)'. The 'QoS Band (Reply)' dropdown is set to 'No-Shaping'.

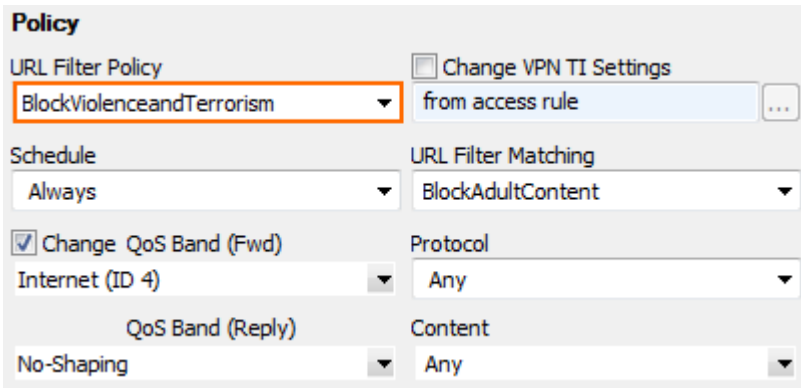
- **Protocol** – Selecting a protocol object for a detected application allows to apply a policy that will deny an application the usage of this protocol, or alternatively apply a higher traffic shaping queue to the VOIP feature of an application. Protocols not allowed by the matching access rule cannot be allowed in the application rule. For more information, see [How to Create a Protocol Object](#).
- **Content** – To block or allow specific content types, you can select from the following content types:
 - Any
 - AVI
 - Flash
 - MPEG
 - Quicktime
 - Realmedia

URL Filter

You can combine URL filtering with application control. Use URL filter policy objects or URL Filter

Match objects to block website categories.

- **URL Filter Policy** – URL Filter policies define the allow/block/warn/alert policy for every URL filter category. To apply that policy to the application rule select the URL filter policy object from the list. For more information, see [How to Create an URL Filter Policy Object](#).



Policy

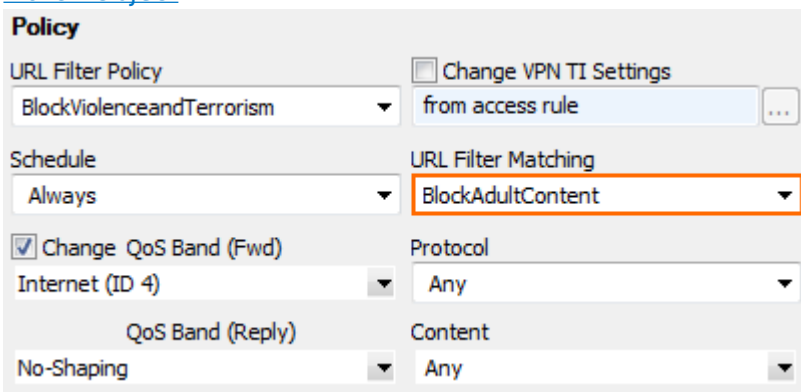
URL Filter Policy Change VPN TI Settings
 BlockViolenceandTerrorism from access rule ...

Schedule URL Filter Matching
 Always BlockAdultContent

Change QoS Band (Fwd) Protocol
 Internet (ID 4) Any

QoS Band (Reply) Content
 No-Shaping Any

- **URL Filter Matching** – URL Filter matching is used to assign additional policies such as traffic shaping or TI settings to web categories. For more information, see [How to Create an URL Filter Match Object](#).



Policy

URL Filter Policy Change VPN TI Settings
 BlockViolenceandTerrorism from access rule ...

Schedule URL Filter Matching
 Always BlockAdultContent

Change QoS Band (Fwd) Protocol
 Internet (ID 4) Any

QoS Band (Reply) Content
 No-Shaping Any

Applying Traffic Shaping to Detected Applications

Applications can not only be allowed or denied, you can also change the QoS Band assigned to the traffic matching this application rule. This allows you to throttle or prioritize applications as needed. By default the QoS Band of the matching access rule is used. For more information, see [Traffic Shaping](#).

- **Change the QoS Band** – Select this checkbox to use a different QoS band than the QoS band used by the matching access rule.
- **QoS Band (Fwd)** – Select the QoS Band to be applied to the outgoing application traffic matching this application rule.
- **QoS Band (Reply)** – Select the QoS Band to be applied to the incoming application traffic

matching this application rule.

Policy

URL Filter Policy
None

Schedule
OfficeHours

Change QoS Band (Fwd)
ThrottleSocialNetworks (ID 20)

QoS Band (Reply)
No-Shaping

Figures

1. app_rule01.png
2. app_rule02.png
3. app_rule03.png
4. app_rule04.png
5. app_rule06.png
6. app_rule07.png
7. app_rule08.png
8. app_rule05.png

© Barracuda Networks Inc., 2019 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.