

How to Create an Application Rule

<https://campus.barracuda.com/doc/72516074/>

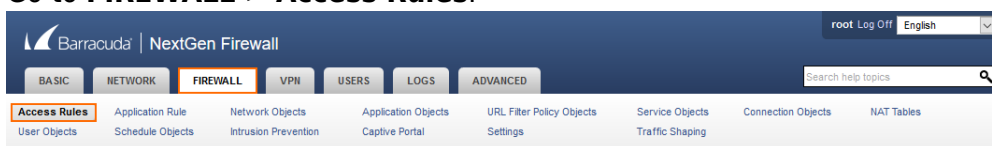
Configuring an application rule is similar to configuring an access rule. You can enable Application Control features on a per-access-rule basis. Application rules allow you to block or throttle traffic for detected applications. You can also combine the application rule with a URL filter policy object. 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.

Before You Begin

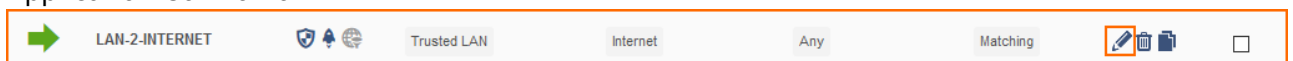
- Verify that you have enabled Application Control and that you are using the latest feature level of the firewall service. For more information, see [How to Enable Application Control](#).
- Create **Application Objects** and/or **Application Filters** necessary for your application policies. For more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

Step 1. Enable Application Control Features for the Access Rule

1. Go to **FIREWALL > Access Rules**.



2. Double-click the row or click edit in the **Actions** column of the access rule you want to enable Application Control for.



3. The **Edit Access Rule** window opens.
4. Click **Yes** for **Application Control**.
5. Select the Application Control features to be used for this access rule:
 - **SSL Interception**
 - **URL Filter**
 - **Virus Scan**
 - **ATP**
 - **File Content Scan**
 - **Mail Security**
 - **Safe Search**

Edit Access Rule ?

General **Advanced**

Action:

Name:

Bi-directional: Yes No

Disable: Yes No

Description:

IPS: Yes No

Application Control: Yes No

SSL Interception: Yes No

URL Filter: Yes No

Virus Scanner: Yes No

ATP: Yes No

Mail Security: Yes No

Safe Search: Yes No

Connection:

Adjust Bandwidth:

The interface must have bandwidth management enabled on the NETWORK > IP Configuration page for this policy to be applied.

Source:

Network Services:

Destination:

Network Objects IP Addresses Geo Loc.


Network Objects IP Addresses Geo Loc.

6. Click **Save**.


Step 2. Create an Application Rule

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

1. Go to **FIREWALL > Application Rule**.
2. Click **Add Application Rule**.
3. The **Edit Application Rule** window opens.
4. In this case, an application rule for minimizing the bandwidth to the lowest priority will be created:
 - **Action** – Select **Pass** to let the traffic continue to flow.
 - **Name** – Enter the name for your application rule, e.g., Social Networks.
 - **Adjust Bandwidth** – Select **Lowest Bandwidth**.
5. Click **Browse**.

Edit Application Rule 

General **Advanced**

Action: 

Disable: Yes No

Name:

Description:

Adjust Bandwidth:

URL Filter:

Native Apps

Select applications...

List Based Application Objects

FacebookAndGooglePlus

Page 1 of 1

6. The **Application Browser** window opens.
7. Select your **List Based Application Object** that you have already configured, e.g., FacebookAndGooglePlus.
8. Click **Add Selected**.

Application Browser ?

Show: All Native Apps Objects Custom Applications

Category: All Properties: All Risk: All

Filter: Create... ▾


Name	Category	Properties	Risk
List Based Application Objects			
<input type="checkbox"/> MyOwnStreamingApps			
<input checked="" type="checkbox"/> FacebookAndGooglePlus			
Filter Based Application Objects			
<input type="checkbox"/> MyFilterObject		Bandwidth Consuming Supports File Transfers Vulnerabilities	
Native Apps			
<input checked="" type="checkbox"/> Facebook	Social Networking	Time/Productivity Consuming Encrypted Browser Based Client Application	2
<input type="checkbox"/> Facebook Post	Web Posting	Time/Productivity Consuming Encrypted Browser Based Client Application	2
<input type="checkbox"/> Facebook Mail	Email	Encrypted Supports File Transfers Browser Based Client Application	2
<input type="checkbox"/> Facebook Chat and Messenger	Instant Messaging	Time/Productivity Consuming Encrypted Browser Based Client Application	2
<input type="checkbox"/> Facebook SocialPlugins	Social Networking	Encrypted Browser Based Client Application	3
<input type="checkbox"/> Facebook Filetransfer	File Storage and Backup	Bandwidth Consuming Encrypted Supports File Transfers Browser Based Client Application	3
<input checked="" type="checkbox"/> Facebook Apps	Games	Time/Productivity Consuming Encrypted Used by Malware Browser Based	3

Add Selected Close

9. Click **Save**.

Edit Application Rule ?

General **Advanced**

Action: 

Disable: Yes No

Name:

Description:

Adjust Bandwidth:

URL Filter:

Native Apps

Select applications... Browse Create... ▾

Name	Category	Properties	Risk
List Based Application Objects			
<input checked="" type="checkbox"/> FacebookAndGooglePlus			

Cancel Save

10. Drag the application rule above the standard rule ALL-APPS.

The application rule is now added to the list of application rules.

APPLICATION RULES						Help
Add Application Rule		Add Section		Search		
Action	Name	Native Apps	Source	Actions	Disabled	
	Catchall rule that allows all application traffic to pass. Can be edited to assign, e.g., a default QoS band or TI index (2)					
	Social Networks	FacebookAndGooglePlus			<input type="checkbox"/>	
	ALL-APPS		0.0.0.0/0		<input type="checkbox"/>	

Figures

1. mnu_firewall_access_rules.png
2. select_access_rule_for_application_control.png
3. configure_application_control.png
4. edit_application_rule.png
5. select_from_application_browser.png
6. complete_application_rule.png
7. application_rule_added.png

© Barracuda Networks Inc., 2020 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.