How to Create an Application Rule

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

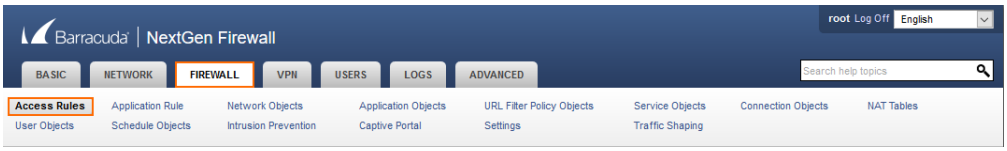
Configuring an application rule is similar to configuring an access rule. You can enable Application Control features on a per-access-rule basis. Application rules allow you to block or throttle traffic for detected applications. You can also combine the application rule with a URL filter policy object.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

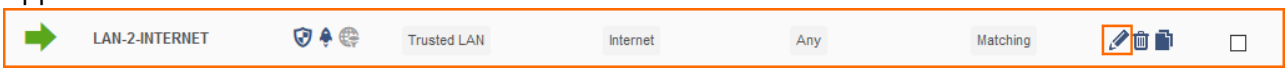
- Verify that you have enabled Application Control and that you are using the latest feature level of the firewall service. For more information, see How to Enable Application Control.
- Create **Application Objects** and/or **Application Filters** necessary for your application policies. For more information,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

Step 1. Enable Application Control Features for the Access Rule

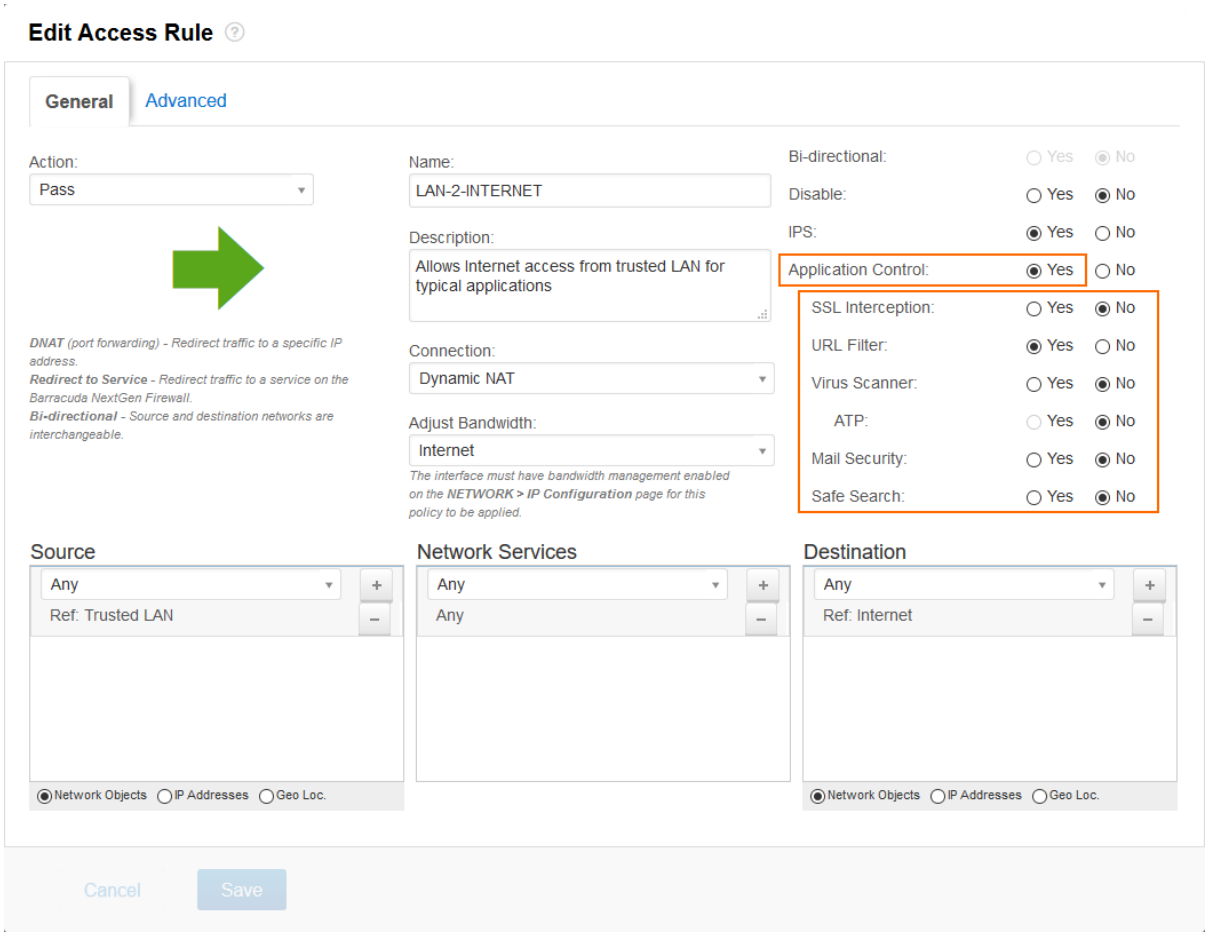
1. Go to **FIREWALL > Access Rules**.



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**

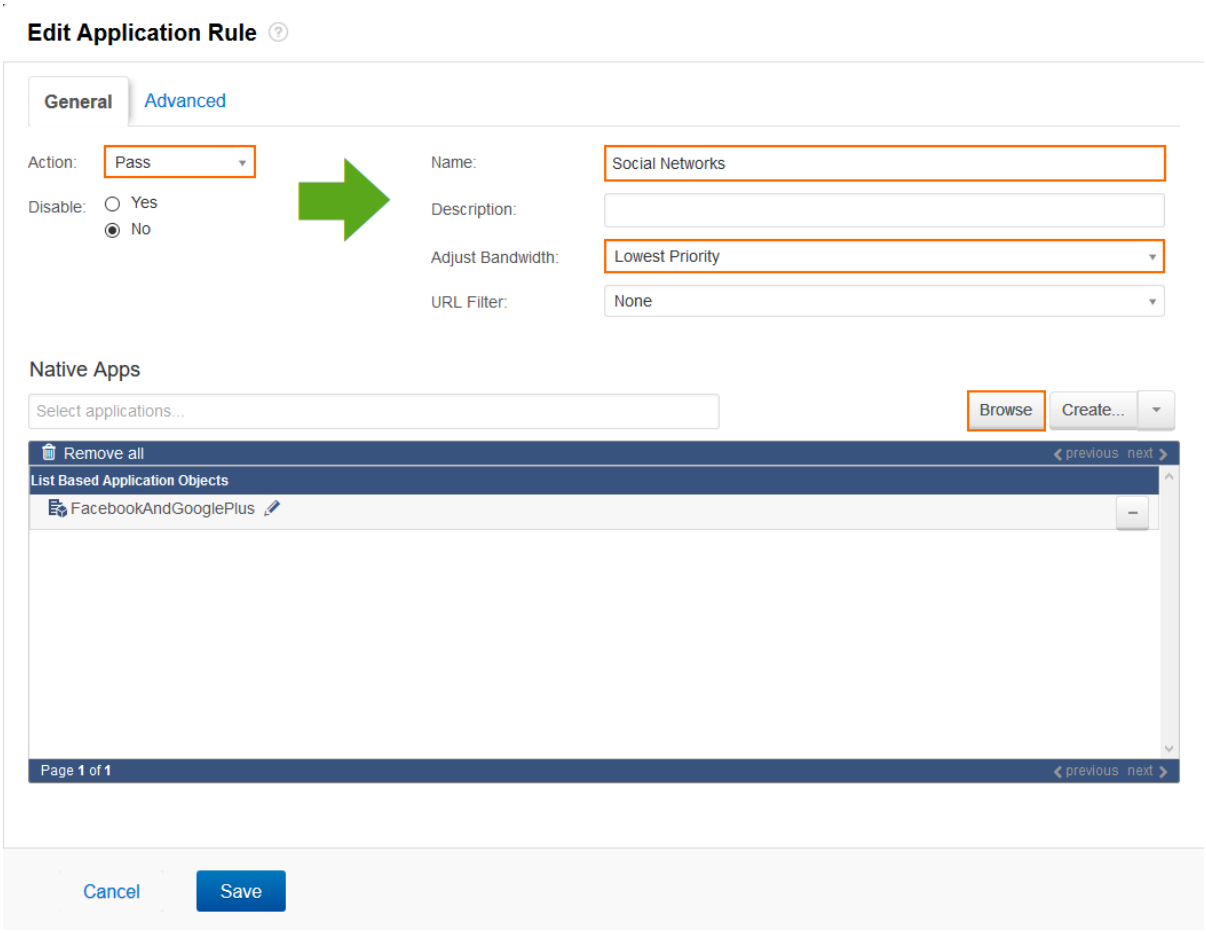


6. Click **Save**.

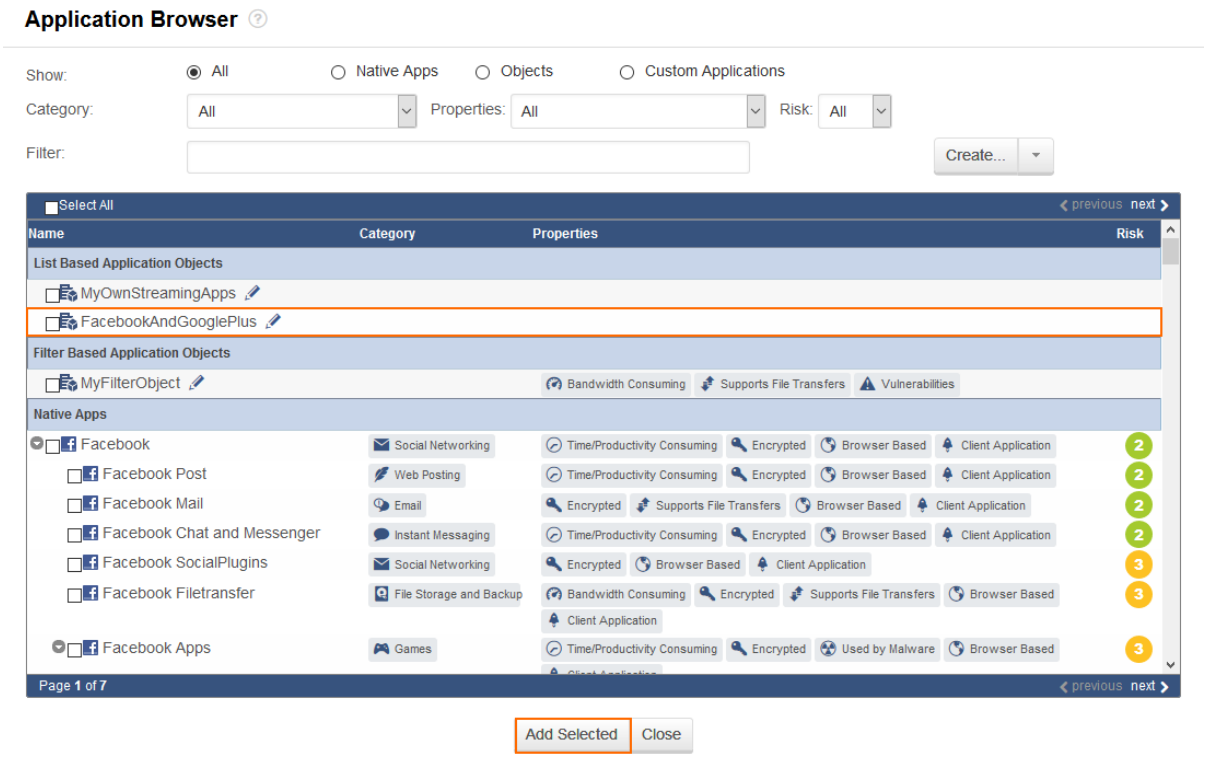
Step 2. Create an Application Rule

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.

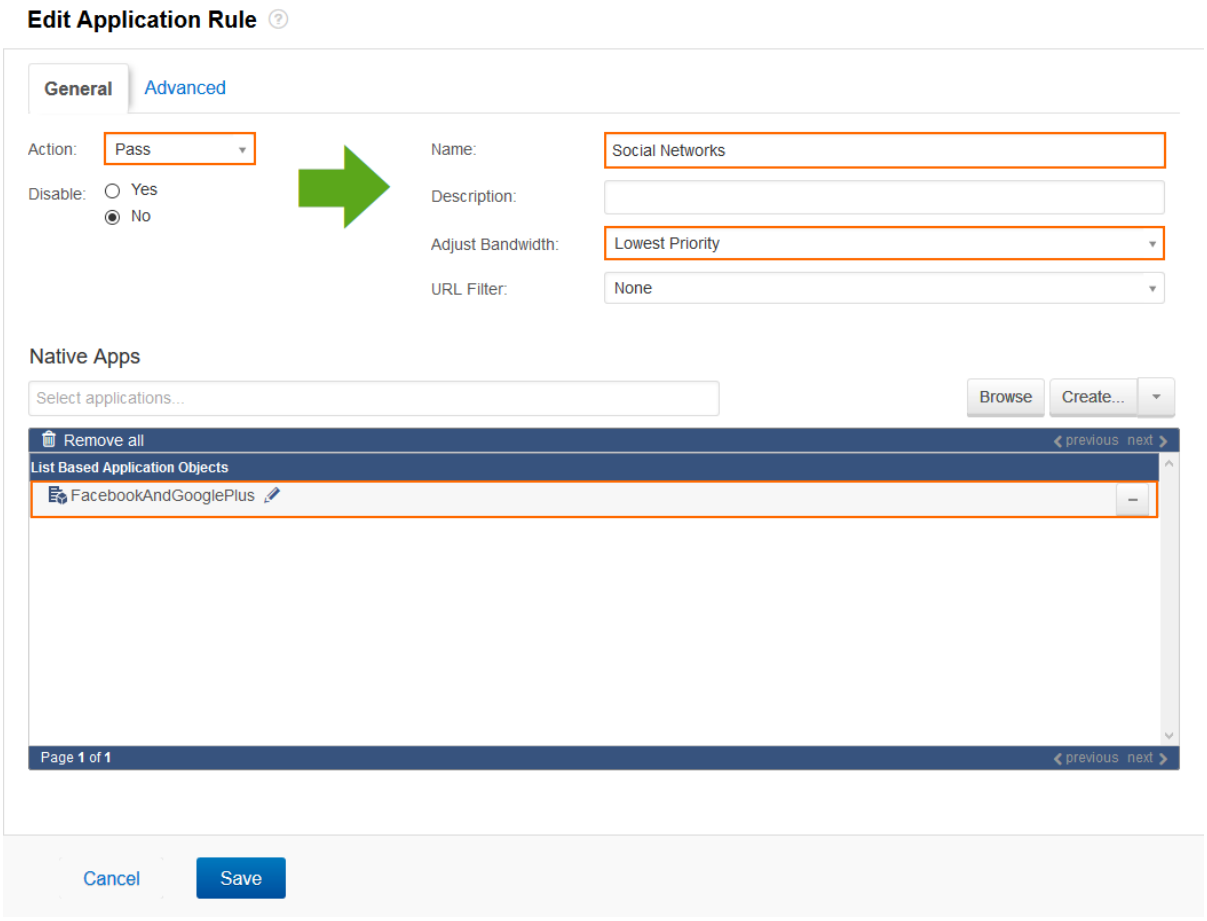
1. Go to **FIREWALL > Application Rule**.
2. Click **Add Application Rule**.
3. The **Edit Application Rule** window opens.
4. In this case, an application rule for minimizing the bandwidth to the lowest priority will be created:
   - **Action** – Select **Pass** to let the traffic continue to flow.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



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**.

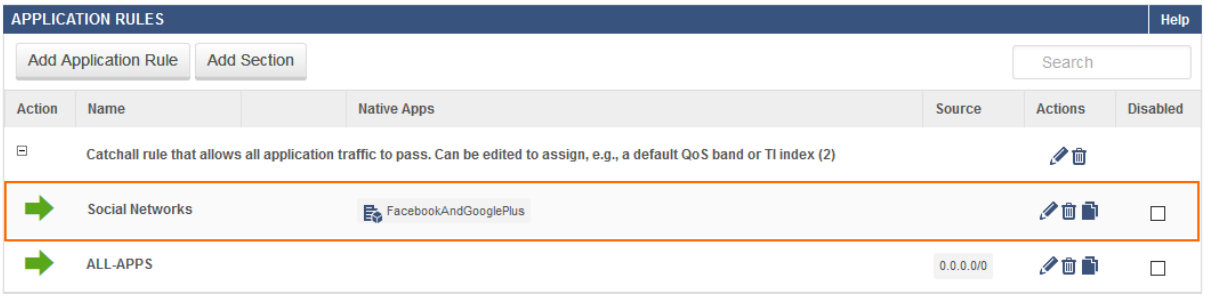

Application Browser
Show: All Native Apps Objects Custom Applications
Category: All
Properties: All
Risk: All
Filter:
Create...
Select All
previous next
Name
Category
Properties
Risk
List Based Application Objects
MyOwnStreamingApps
FacebookAndGooglePlus
Filter Based Application Objects
MyFilterObject
Bandwidth Consuming
Supports File Transfers
Vulnerabilities
Native Apps
Facebook
Social Networking
Time/Productivity Consuming
Encrypted
Browser Based
Client Application
Facebook Post
Web Posting
Facebook Mail
Email
Facebook Chat and Messenger
Instant Messaging
Facebook SocialPlugins
Facebook Filetransfer
File Storage and Backup
Facebook Apps
Games
Used by Malware
Page 1 of 7
Add Selected
Close

9. Click **Save**.


Edit Application Rule
General
Advanced
Action: Pass
Disable: Yes No
Name: Social Networks
Description:
Adjust Bandwidth: Lowest Priority
URL Filter: None
Native Apps
Select applications...
Browse
Create...
Remove all
previous next
List Based Application Objects
FacebookAndGooglePlus
Page 1 of 1
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.



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