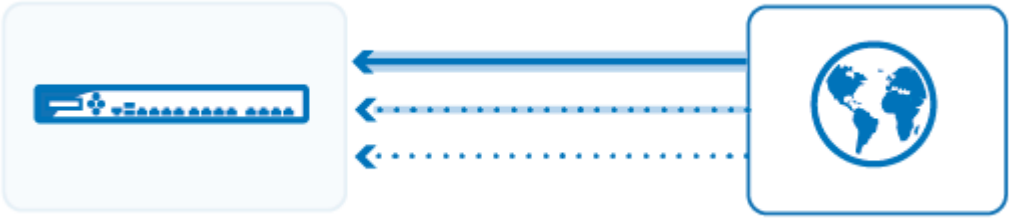
Example - Adjust Bandwidth for Application Traffic

https://campus.barracuda.com/doc/30113940/

Application Control lets you detect and manage application-based traffic. You can create policies to prioritize, limit, or block specific applications or application categories. This article provides an example of how to configure an application policy and a firewall rule to slow all connections to Facebook.



Step 1. Enable Application Control

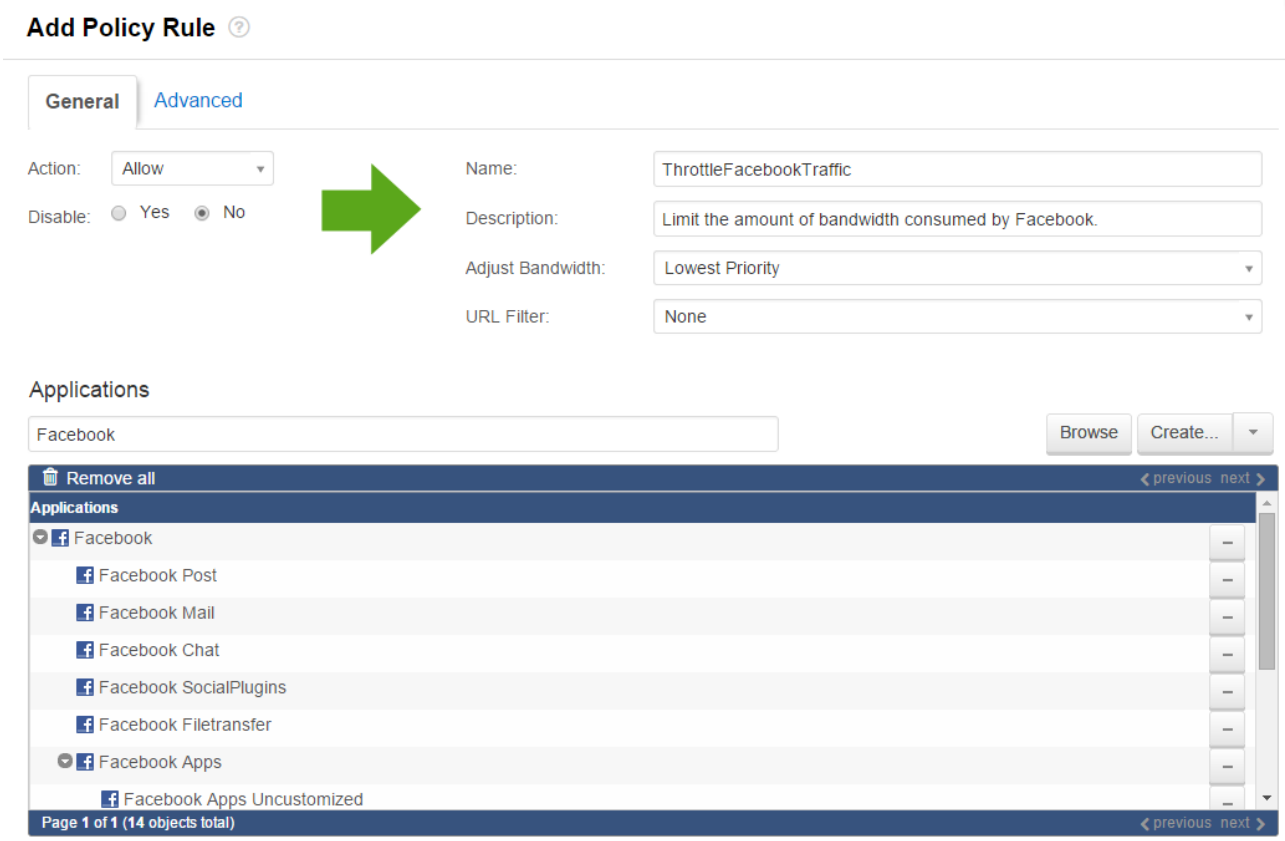
To enable Application Control,

1. Go to the **FIREWALL > Settings** page.
2. Click **Yes** to **Enable Application Detection**.
3. Click **Save**.

Step 2. Create an Application Policy

Create an application policy to assign a lower bandwidth priority to Facebook traffic.

1. Go to the **FIREWALL > Application Policy** page.
2. Click **Add Policy Rule**.
3. In the **ADD POLICY RULE** window, specify the following settings:
   - **Action** – Select **Allow**.
   - **Name** – Enter a name, e.g.: `ThrottleFacebookTraffic`
   - **Adjust Bandwidth** – Select **Choke**. This will slow the connection so that the application becomes unusable, blocking use without error messages.
   - **Applications** – Type the name of the application (e.g., `Facebook`) in the text box and then select **Facebook** from the **APPLICATIONS** list.
     The selected application including all sub-applications is now displayed in the **APPLICATIONS** section.



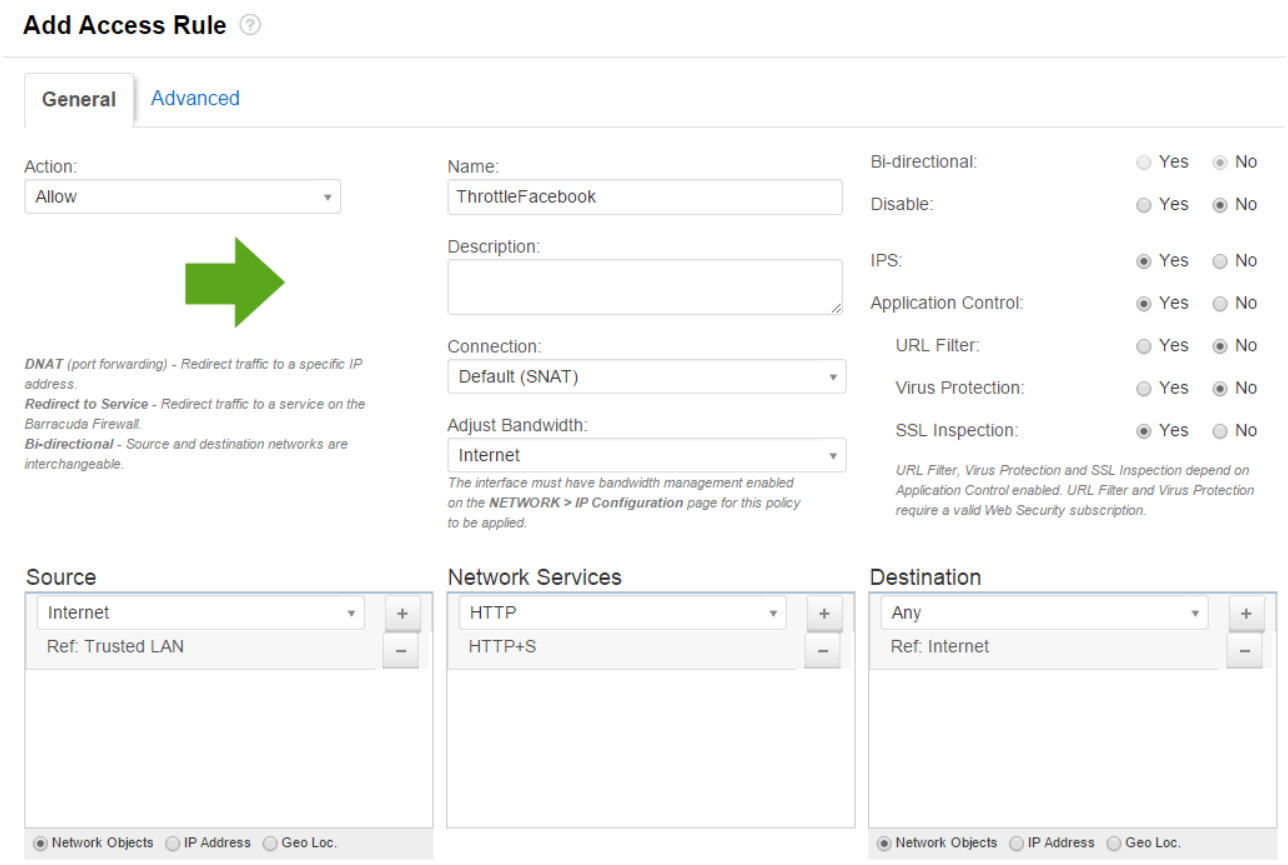
4. Click **Save**.

Step 3. Enable Application Control for a Firewall Rule

Because Application Control can impact the performance of the Barracuda NextGen Firewall X-Series, be as specific as possible with firewall rule settings.

Create a specific firewall rule for application traffic.

1. Go to the **FIREWALL > Firewall Rules** page.
2. Click **Add Access Rule**.
3. In the **ADD ACCESS RULE** window, specify the following settings under the **General** tab:
   - **Name** – Enter a name, e.g.: `ThrottleFacebook`
   - **Action** – Select **Allow**.
   - **Source** – Select **Trusted LAN Networks**.
   - **Network Services** – Select **HTTP+S** (Facebook only communicates over HTTP and HTTPS.)
   - **Destination** – Select **Internet**.



4. Click **Save**.

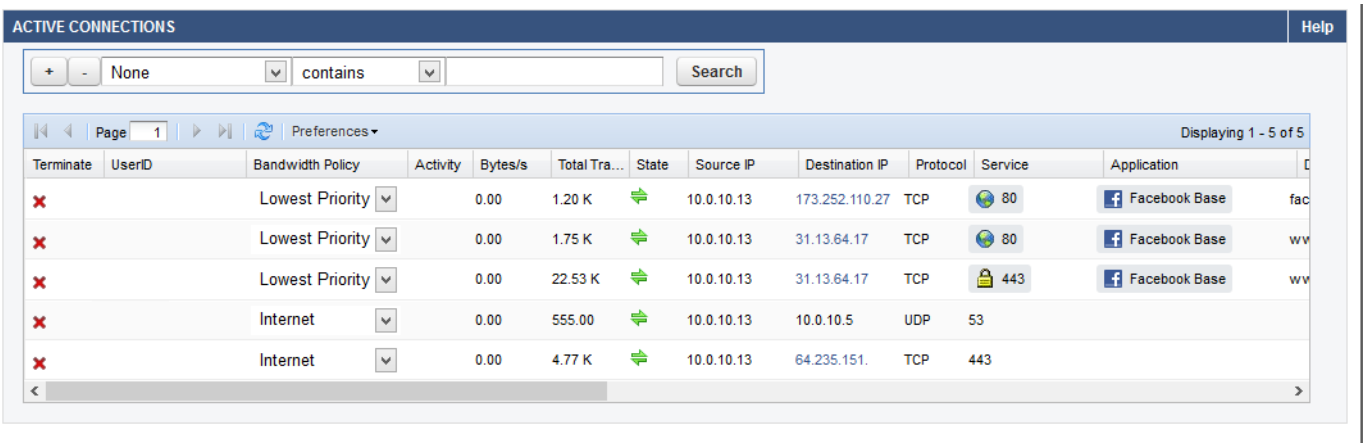
Step 4. Verify the Order of the Firewall Rules

Because rules are processed from top to bottom, you must place this rule before the **LAN-2-INTERNET** rule. After adjusting the order of the rules, click **Save**.

For more information, see Firewall Rules Order.

Monitoring Traffic for Detected Applications

To view blocked or throttled connections, go to the **BASIC > Active Connections** or **BASIC > Recent Connections** page. In the **Application** and **Bandwidth Policy** columns for each connection, the detected application and the assigned bandwidth policy is listed. To view specific connections, you can filter the list.


ACTIVE CONNECTIONS
Help
+
-
None
contains
Search
Page 1
Preferences
Displaying 1 - 5 of 5
Terminate
UserID
Bandwidth Policy
Activity
Bytes/s
Total Tra...
State
Source IP
Destination IP
Protocol
Service
Application
Lowest Priority
0.00
1.20 K
10.0.10.13
173.252.110.27
TCP
80
Facebook Base
Lowest Priority
0.00
1.75 K
10.0.10.13
31.13.64.17
TCP
80
Facebook Base
Lowest Priority
0.00
22.53 K
10.0.10.13
31.13.64.17
TCP
443
Facebook Base
Internet
0.00
555.00
10.0.10.13
10.0.10.5
UDP
53
Internet
0.00
4.77 K
10.0.10.13
64.235.151.
TCP
443

Figures

1. appctrl_ts.png
2. Example_throttle_app_67_01.png
3. Example_throttle_app_67_02.png
4. Example_throttle_app_03.png