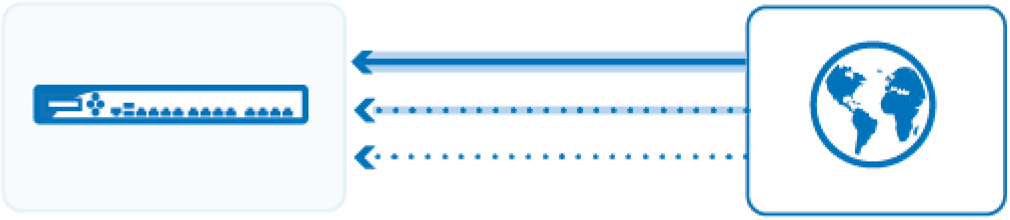
Example - Adjust Bandwidth for Application Traffic

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

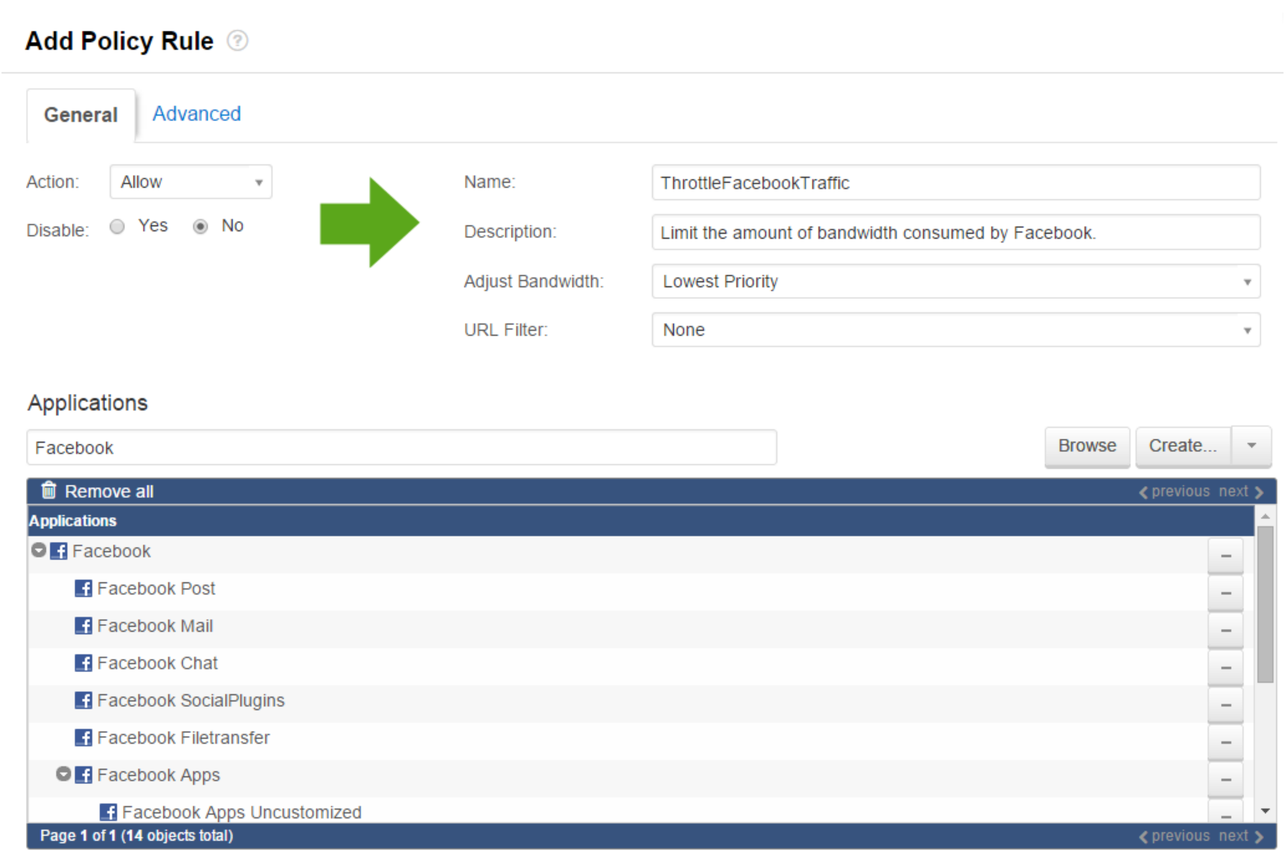
To enable Application Control,

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.



Add Policy Rule

Action: Allow

Disable: ○ Yes ● No

Name: ThrottleFacebookTraffic

Description: Limit the amount of bandwidth consumed by Facebook.

Adjust Bandwidth: Lowest Priority

URL Filter: None

Applications

Facebook

Applications
- Facebook
  - Facebook Post
  - Facebook Mail
  - Facebook Chat
  - Facebook SocialPlugins
  - Facebook Filetransfer
  - Facebook Apps
    - Facebook Apps Uncustomized

Page 1 of 1 (14 objects total)

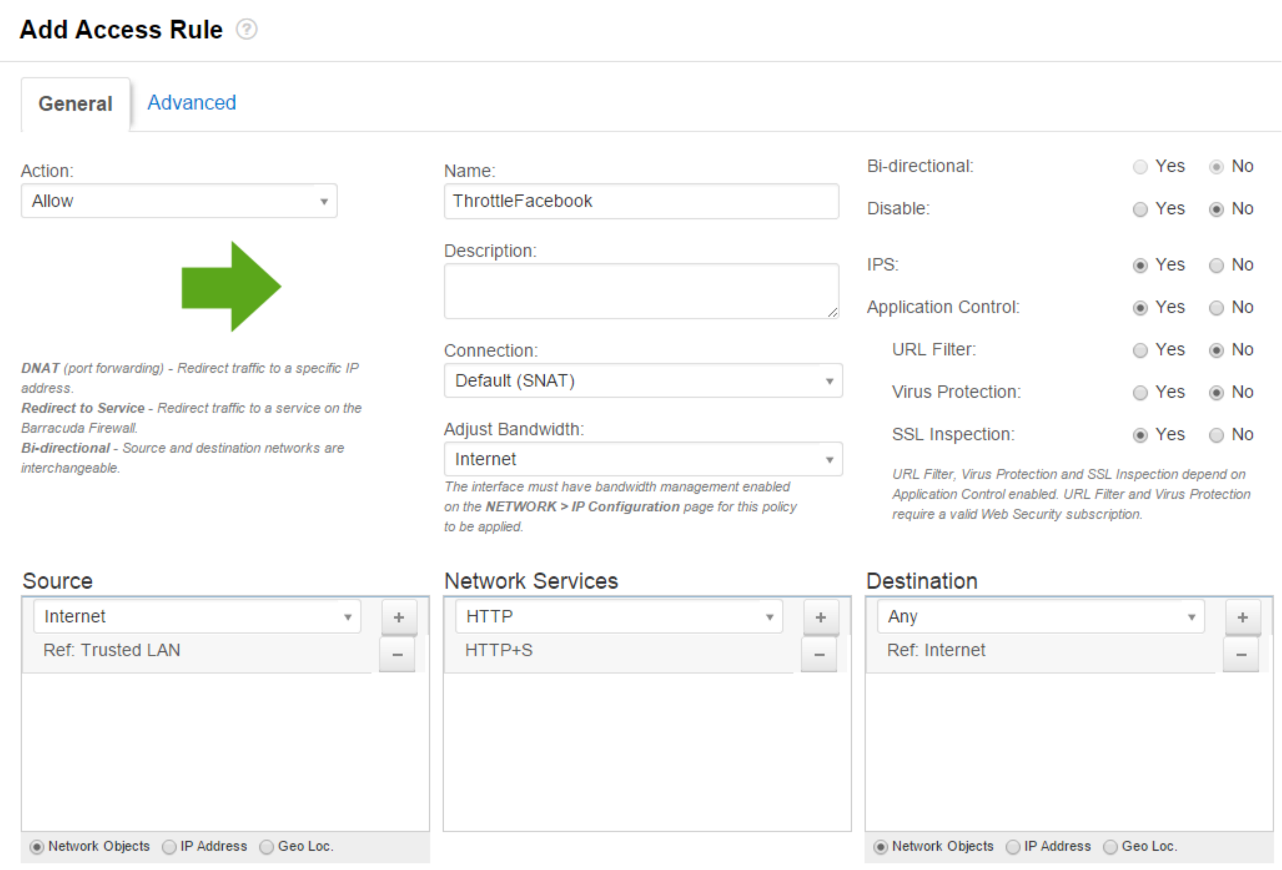
4. Click **Save**.

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**.



Add Access Rule

General | Advanced

Action: Allow

DNAT (port forwarding) - Redirect traffic to a specific IP address.
Redirect to Service - Redirect traffic to a service on the Barracuda Firewall.
Bi-directional - Source and destination networks are interchangeable.

Name: ThrottleFacebook

Description:

Connection: Default (SNAT)

Adjust Bandwidth: Internet

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

Bi-directional: ○ Yes ● No

Disable: ○ Yes ● No

IPS: ● Yes ○ No

Application Control: ● Yes ○ No

URL Filter: ○ Yes ● No

Virus Protection: ○ Yes ● No

SSL Inspection: ● Yes ○ No

URL Filter, Virus Protection and SSL Inspection depend on Application Control enabled. URL Filter and Virus Protection require a valid Web Security subscription.

Source: Internet
Ref: Trusted LAN
● Network Objects ○ IP Address ○ Geo Loc.

Network Services: HTTP
HTTP+S

Destination: Any
Ref: Internet
● Network Objects ○ IP Address ○ Geo Loc.

4. Click **Save**.

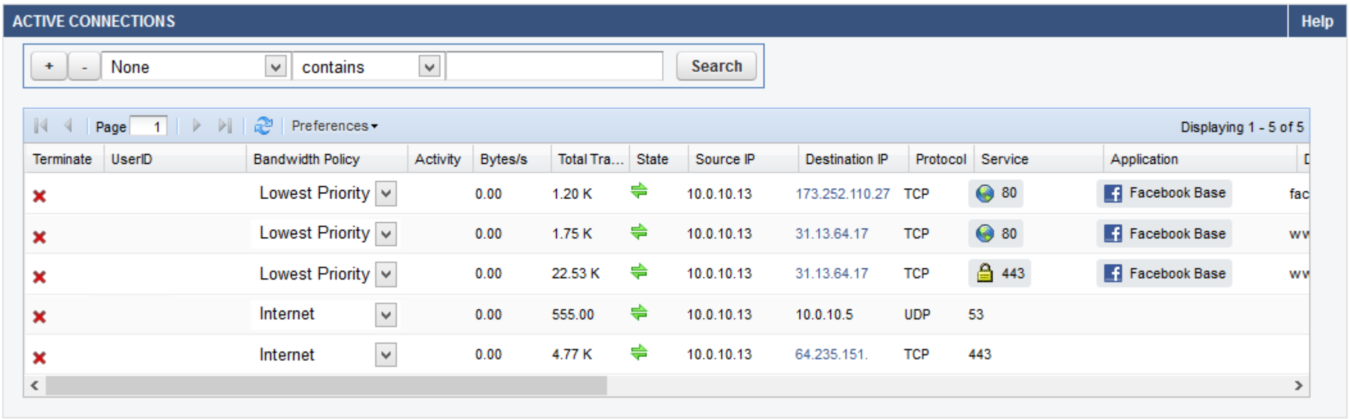
Step 4. Verify the Order of the Firewall Rules

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.



Terminate	UserID	Bandwidth Policy	Activity	Bytes/s	Total Tra...	State	Source IP	Destination IP	Protocol	Service	Application	D
✖		Lowest Priority		0.00	1.20 K	⇄	10.0.10.13	173.252.110.27	TCP	80	Facebook Base	fac
✖		Lowest Priority		0.00	1.75 K	⇄	10.0.10.13	31.13.64.17	TCP	80	Facebook Base	wv
✖		Lowest Priority		0.00	22.53 K	⇄	10.0.10.13	31.13.64.17	TCP	443	Facebook Base	wv
✖		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