How to Configure an Application Policy

https://campus.barracuda.com/doc/13306481/

Enable Application Control to block, allow, report, or choke network traffic for specific application types. Application Control uses deep packet inspection to detect and manage the bandwidth for web applications and services like instant messaging, social networking, or video streaming. It can also detect applications that try to evade pattern-based detection mechanisms by port-hopping, protocol obfuscation, or traffic encryption.

You can enable Application Control for each firewall rule individually. When the rule is executed, the application policy rules are processed from top to bottom.

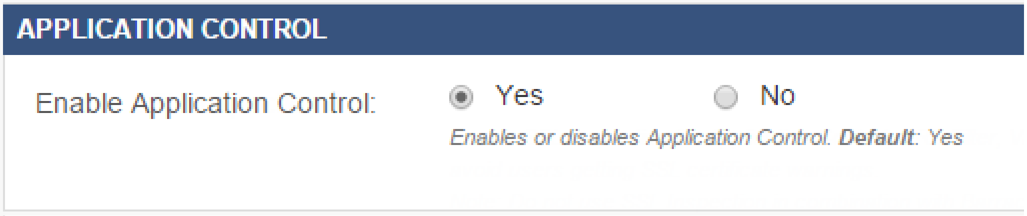
Application policies can allow or block application traffic based on:

- Application or sub-application
- Time
- User
- Content
- Source network
- Protocol

Step 1. Enable Application Control and SSL Inspection

To detect and manage application traffic, you must first enable application control.

1. Go to the **FIREWALL > Settings** page.
2. Enable **Application Control** in the **Application Control** section.

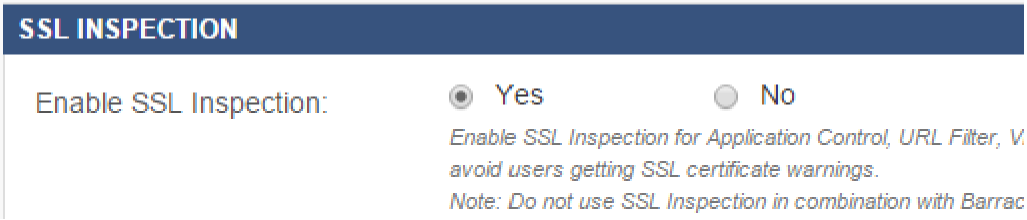


APPLICATION CONTROL

Enable Application Control: ● Yes ○ No

*Enables or disables Application Control. **Default**: Yes*

3. (Optional) Enable **SSL Inspection** in the **SSL Inspection** section.



SSL INSPECTION

Enable SSL Inspection: ● Yes ○ No

Enable SSL Inspection for Application Control, URL Filter, V.
avoid users getting SSL certificate warnings.
Note: Do not use SSL Inspection in combination with Barrac

4. Click **Save**.

Step 2. Install SSL Certificates on the Client

To avoid SSL certificate errors in the browser when a user connects to an SSL-encrypted website, install the self-signed SSL certificate of the Barracuda NextGen X-Series Firewall on your client computers.

1. Go to the **FIREWALL > Settings** page.
2. In the **Active Root CA** section, click **Download**.
3. Choose the certificate format (e.g., **CER** if you are on a Windows computer).
4. Install the root certificate in your local certificate store.

With the certificates installed, your clients no longer receive SSL certificate warnings when SSL inspection is used.

Step 3. Configure the Firewall Rule

Configure firewall rules to use Application Control. The pre-installed LAN-2-INTERNET firewall rule allows network traffic for all types of data from the trusted LAN to the Internet. You can edit the LAN-2-INTERNET rule or create a new firewall rule if required.

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

1. Go to the **FIREWALL > Firewall Rules** page.
2. Edit the rule that you want to add Application Control to by clicking the **Edit** icon.
3. Set **Application Control** to **Yes**.
4. Click **Save**.

Step 4. Verify the Order of the Firewall Rules

Because rules are processed from top to bottom, verify that your rules are arranged in the correct order. Click **Save**.

Your firewall rule must be placed above the BLOCKALL rule.

Step 5. Create Application Policies

Create an application policy for every application you want to modify or block.

Adjust the Bandwidth of an Application

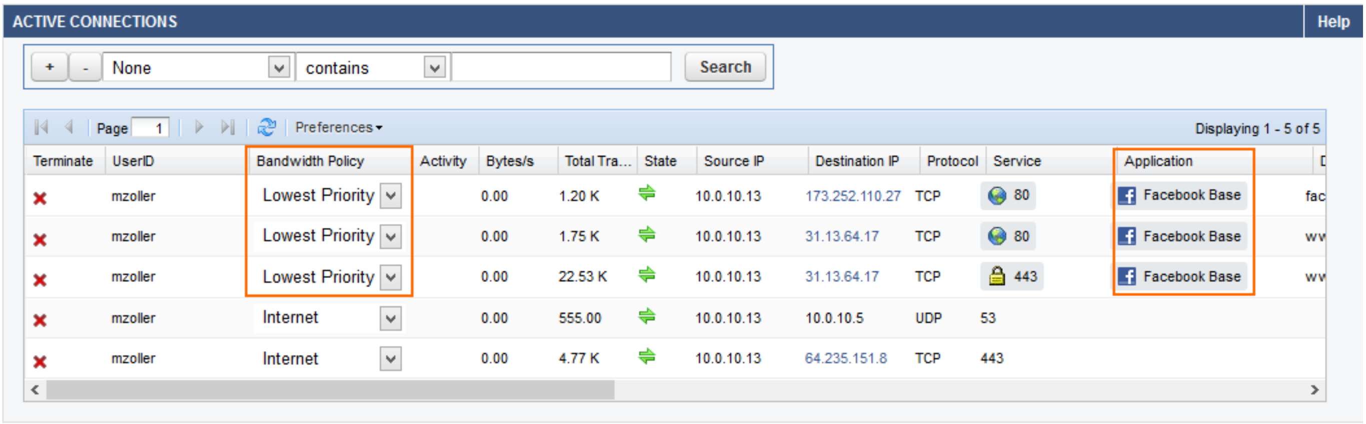
1. Go to the **FIREWALL > Application Policy** page.
2. Click **Add Policy Rule**.
3. In the **Add Policy Rule** window, enter a **Name** for the policy rule.
4. Select **Allow** from the **Action** list.
5. Select the applications that this policy should apply to. You can either:
   - Start typing the name of the application, and then select the application from the dynamically generated applications list.
   - Click **Browse** and use the **Application Browser** to add multiple applications by category or properties.
6. Optionally, you can add more matching criteria in the **ADVANCED** tab:
   - **Time**
   - **Source Network**
   - **Content** - You can block specific kinds of content like FLASH or MPEG videos.
   - **Users**
   - **Protocols**
7. Click **Save**.

Block an Application

1. Go to the **FIREWALL > Application Policy** page.
2. Click **Add Policy Rule**.
3. In the **Add Policy Rule** window, enter a **Name** for the policy rule.
4. Select **Block** from the **Action** list.
5. Select the applications this policy should apply to. You can either:
   - Start typing the name of the application, and then select the application from the dynamically generated applications list.
   - Click **Browse** and use the **Application Browser** to add multiple applications by category or properties.
6. Optionally, you can add the more matching criteria in the **ADVANCED** tab:
   - **Time**
   - **Source Network**
   - **Content** - You can block specific kinds of content like FLASH or MPEG videos.
   - **Users**
   - **Protocols**
7. Click **Save**.

Monitoring Blocked and Throttled Connections

To view blocked or throttled connections, go to the **BASIC > Recent Connections** page. In the **Application** column for each connection, the controlled application is listed. To view specific connections, you can filter the list of recent connections.



Terminate	UserID	Bandwidth Policy	Activity	Bytes/s	Total Tra...	State	Source IP	Destination IP	Protocol	Service	Application	D
✖	mzoller	Lowest Priority		0.00	1.20 K	⇄	10.0.10.13	173.252.110.27	TCP	80	Facebook Base	fac
✖	mzoller	Lowest Priority		0.00	1.75 K	⇄	10.0.10.13	31.13.64.17	TCP	80	Facebook Base	ww
✖	mzoller	Lowest Priority		0.00	22.53 K	⇄	10.0.10.13	31.13.64.17	TCP	443	Facebook Base	ww
✖	mzoller	Internet		0.00	555.00	⇄	10.0.10.13	10.0.10.5	UDP	53		
✖	mzoller	Internet		0.00	4.77 K	⇄	10.0.10.13	64.235.151.8	TCP	443		

Figures