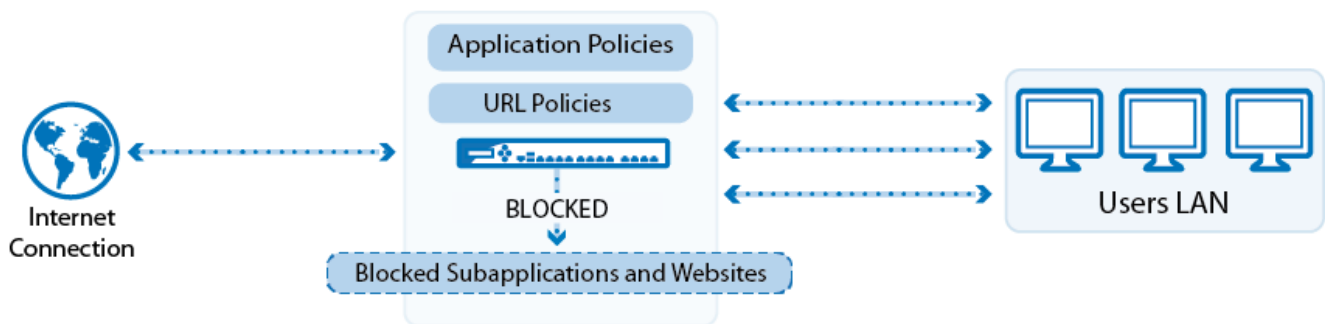


How to Introduce Application Control to Your Network

<https://campus.barracuda.com/doc/41093369/>

To use application control efficiently, it is recommended that you first monitor your application traffic over a certain period of time. Analyzing your bandwidth usage helps you determine how to improve the use of available resources and then configure policies to manage application traffic accordingly.

After your analysis, create application policies to ensure that business-critical applications receive the bandwidth that they need. Then configure application and URL policies to block or choke any unwanted applications and websites. You can adjust and tune these policies by defining exceptions for certain resources or users.



Step 1. Activate Application Control

Enable Application Control and activate it in a firewall rule to start gathering application data. Configure one or more firewall rules that forward traffic from the clients to the internet. If you want to use pre-installed rules, configure the LAN-2-INTERNET and WIFI-2-INTERNET rules. If you are not using the pre-installed firewall access rules, use the corresponding firewall rules.

1. Go to the **FIREWALL > Settings** page, enable **Application Control**, and click **Save**.
2. Go to the **FIREWALL > Firewall Rules** page.
3. Edit the LAN-2-INTERNET and WIFI-2-INTERNET rules to enable **Application Control** and **SSL Inspection**.
4. Install SSL certificates on the client computers to avoid SSL warnings when using SSL Inspection. For more information, see [How to Configure an Application Policy](#).

The Barracuda NextGen Firewall X-Series can now start collecting information on the application-based traffic that is handled by these firewall rules. If you configured a captive portal or the Barracuda DC Agent, user information is also collected.

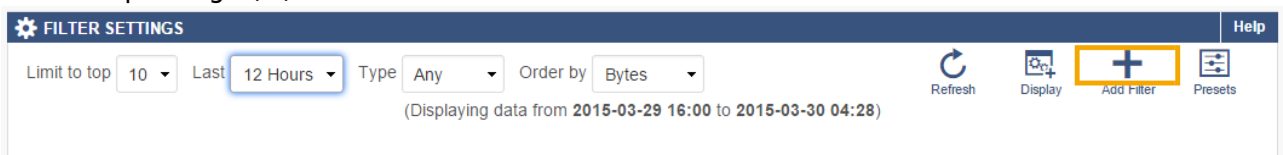
Step 2. Analyze Application Traffic

Go to the **BASIC > Application Monitor** page to view information about the application traffic that passes through the X-Series Firewall and determine which applications use the most bandwidth. You can either use filters or create custom reports to track this information and view it in more detail.

Example - Define a Filter to see all Employees Using High Risk Applications.

If you want to see all data about high risk applications that were used in your network, configure a filter for the application monitor:

1. Go to the **BASIC > Application Monitor** page.
2. Click the plus sign (+) to create a new filter.



3. In the **Filter** window, select **>=3** from the **Risk** list.

Filter ?

Application:	<input type="text"/>
URL Category:	All ▼
Application Category:	All ▼
Geo Destination:	All ▼
Geo Source:	All ▼
Risk:	>=3 ▼
Source IP:	<input type="text"/>
User:	<input type="text"/>
Protocol:	Unknown ▼
Application Detail:	<input type="text"/>
Domain:	<input type="text"/>
<input type="button" value="Ok"/> <input type="button" value="Reset to Defaults"/>	

4. Click **Ok**.

You can now see a list of all the data for high risk applications in the time period that you selected in the **Last** list. To remove the filter click the **x** icon next to the filter.

⚙️ FILTER SETTINGS

Help

Limit to top 10 Last 12 Hours Type Any Order by Bytes (Displaying data from 2014-02-25 01:00 to 2014-02-25 01:07)

🔄 Refresh

📺 Display





➕ Add Filter

⚙️ Presets

⌕ Risk (>=3)

📱 APPLICATION

⌕ ⚙️ Help

#	RISK		APPLICATION		BYTES	SESSIONS
1	4		BitTorrent General	Show	314.58 MB	24028
2	4		Vimeo Watch Video	Show	272.80 MB	6934
3	3		Youtube Watch Video	Show	156.27 MB	6233
4	3		Ustream	Show	76.31 MB	3002

Example - Create a Custom Report on How much Bandwidth is used by Business Applications

You can create daily reports using the Barracuda Report Creator (**BASIC > Administration**). You can

define custom report types to get daily update on how much traffic your business critical applications are using.

For more information, see [Barracuda Report Creator](#).

Step 3. Create Application Policies to Prioritize Business-Critical Applications

Create an application policy to ensure that important applications receive enough bandwidth.

1. [Create a list based application object](#) to include all the business-critical applications that you want to prioritize.
2. [How to Configure an Application Policy](#) with **Adjust Bandwidth** set to **Business**.

You are not limited to a single application object for important applications. If you are using VOIP applications like Skype or Facetime, you can define an application object with **Adjust Bandwidth** set to **VOIP**, to ensure that these time-sensitive applications are forwarded without delay.

Step 4. Create Application Policies to Block or Limit Unwanted Applications

Unwanted applications can either be blocked or limited. When applications are blocked, they display connection errors to inform users that the resource is not available. Some applications try to evade being blocked by changing protocol or port. As an alternative, you can limit, or choke, the bandwidth of the applications. When applications are choked, they can still connect but at such an extremely limited rate that they are unusable. If you want to block only parts of an application (e.g., Facebook chat) you can define the application policy to only block the subapplication, while still allowing access to the rest of the site.

1. [Create list- or category-based application objects](#) to include the applications that you want to block or limit.
2. To block applications, [How to Configure an Application Policy](#) and add all the applications that you want to block.
3. To limit applications, [How to Configure an Application Policy](#). In the policy settings, add all the applications that you want to limit and set **Adjust Bandwidth** to **Choke**.

Step 5. Create URL Filter Policies

The URL filter can be configured as a blacklist, allowing all sites except specifically blocked URL

categories, or as a whitelist blocking everything except for specifically allowed categories.

1. Create an URL object.
2. Define the default policy and behavior for all unlisted sites.
3. Go through the URL categories and select **Allow** or **Block** for each one.
4. Edit the application policies and select which URL policy to include.

Step 6. Define Exceptions

If exceptions are required for special use cases or privileged users, you can configure exceptions for your policies:

- To specify exceptions to the categories of websites that you allow or block, click the **URLs** tab in the URL policy settings. Then explicitly enter the URL of websites that must always be allowed or blocked.
- To create exceptions to your application policies, create new application policies. Then place the new application policies over the policies that they are overriding.

Example - Block Everyone from using Facebook Except for Exempt Users

To define an exception from the standard policy, create an application policy specifically allowing access for the exempted users.

1. On the **FIREWALL > User Objects** page, create a user object that includes all users and groups who are allowed to access Facebook.
2. On the **FIREWALL > Application Policy** page, create an **ALLOW** application policy that includes the user object you just configured for allowed users and groups.
3. Place the new exception application policy above the policy rule blocking Facebook for everyone.

Step 7. Monitor Your Changes to Application Traffic

View the application monitor to detect changes in application usage, and adapt and tune the application policies. Configure the [Barracuda Report Creator](#) to send regular updates of what passes through your X-Series Firewall.

Figures

1. Intro_appctrl.png
2. AppControl_Intro_67_01.png
3. AppControl_Intro_67_02.png
4. AppControl_Intro03.png

© Barracuda Networks Inc., 2024 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.