

How to Block FTP and Other Non-HTTP Standard Protocols

<https://campus.barracuda.com/doc/75694844/>

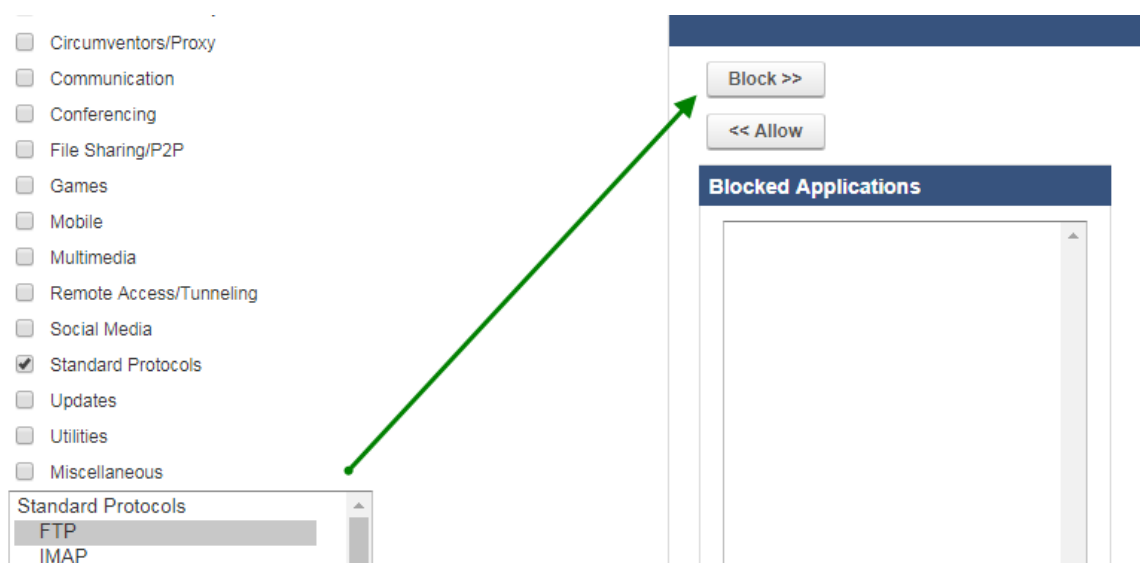
You can choose to block or allow applications that communicate over non-HTTP or HTTP protocols, such as applications like Skype or BitTorrent, or standard protocols like FTP or SSH. Depending on the granularity of blocking that you need, use either the **BLOCK/ALLOW > Applications** page or the **BLOCK/ALLOW > Exceptions** page as follows:

- To block either all *Authenticated* or *Unauthenticated* users, use the **BLOCK/ALLOW > Applications** page.
- To block ALL users or a specific user or group of users, such as users who authenticate with LDAP or Kerberos, or an IP group or Local Group, use the **BLOCK/ALLOW > Exceptions** page.

Note that application blocking is only available for inline deployments. To follow along with the examples below, log in as **Username: admin Password: admin**

Example 1. Block all FTP protocol traffic for *Unauthenticated Users*.

1. Click on the **BLOCK/ACCEPT > Applications** page.
2. At the upper right, for **Policy**, select *Unauthenticated*.
3. In the **Applications** section, under **Allowed Applications**, de-select the check boxes, leaving only the **Standard Protocols** category selected.
4. Click on **Standard Protocols** to see the list of protocols.
5. Select *FTP*, and then click **BLOCK>>** under **Blocked Applications** on the right side of the page.



6. *FTP* should appear in the **Blocked Applications** list. Click **Save**.

Example 2. Block all FTP protocol traffic for *Students* local group.

1. Go to the **USERS/GROUPS > Local Groups** page and create a group called *Students*.
2. From either the **USERS/GROUPS > Account View** or **USERS/GROUPS > New Users** pages, add users to the *Students* group.
3. Click on the **BLOCK/ACCEPT > Exceptions** page.
4. For **Action**, select *Block*.
5. For **Applies To**, select *Local Group*. From the drop-down to the right, select *Students*.
6. For **Exception Type**, select **Applications**.
7. For **Application Name**, click **S** to bring *Standard Protocols* to the top of the list. Scroll to find and click on *FTP* in the *Standard Protocols* list.
8. Select other attributes for the exception such as **Time Frame**, for example, if desired.
9. Click **Add**. Your new exception to block all FTP traffic for the *Students* group appears in the **List of Exceptions** further down the page.

Add Exception

Action:	<input type="text" value="Block"/>	Time Frame:	<input type="text" value="00:00"/> - <input type="text" value="24:00"/>
Applies To:	<input type="text" value="Local Group"/> <input type="text" value="Students"/>	Days of Week:	<input checked="" type="checkbox"/> Su <input checked="" type="checkbox"/> M <input checked="" type="checkbox"/> T <input checked="" type="checkbox"/> W <input checked="" type="checkbox"/> Th <input checked="" type="checkbox"/> F <input checked="" type="checkbox"/> S
	<input type="button" value="Lookup"/>	Time Quota	<input type="text"/> <input type="text" value="Daily"/>
Exception Type:	<input type="text" value="Applications"/>	(min):	
Application	<input type="text" value="- FTP"/>	Bandwidth	<input type="text"/> <input type="text" value="Daily"/>
Name:		Quota (kB):	
		Protocol:	<input type="text" value="All"/>
		Message:	<input type="text"/>
Create Policy	<input type="radio"/> Yes <input checked="" type="radio"/> No		
Alert:			
Alert Threshold	<input type="text"/>		
(requests):			
	<input type="button" value="Add"/> <input type="button" value="Clear"/>		

Example 3. Block SSH traffic for all Kerberos users

1. Go to the **USERS/GROUPS > Authentication** page. Configure a Kerberos authentication server on the Kerberos tab.
2. Click on the **BLOCK/ACCEPT > Exceptions** page.
3. For **Action**, select *Block*.
4. For **Applies To**, select *Kerberos* and, from the drop-down, select the Kerberos server. In this example, the server name is *QA2K8.COM*.
5. For **Exception Type**, select **Applications**.

6. For **Application Name**, click **S** to bring *Standard Protocols* to the top of the list. Scroll to find and click on *SSH* in the *Standard Protocols* list.
7. Select other attributes for the exception such as **Time Frame**, for example, if desired.
8. Click **Add**. Your new exception to block all SSH traffic for all Kerberos-authenticated users appears in the **List of Exceptions** further down the page.

Add Exception

Action:	Block	Time Frame:	00:00 - 24:00
Applies To:	Kerberos User/Group QA2K8.COM	Days of Week:	<input checked="" type="checkbox"/> Su <input checked="" type="checkbox"/> M <input checked="" type="checkbox"/> T <input checked="" type="checkbox"/> W <input checked="" type="checkbox"/> Th <input checked="" type="checkbox"/> F <input checked="" type="checkbox"/> S
	<input type="text"/> <input type="button" value="Lookup"/>	Time Quota	<input type="text"/> Daily
Exception Type:	Applications	(min):	<input type="text"/> Daily
Application	Standard Protocols	Bandwidth	<input type="text"/> Daily
Name:	<ul style="list-style-type: none">- NNTPS- RTSP- SFTP- SNMP- SMTP- SMTPS- SSH- Telnet- TFTP	Quota (kB):	<input type="text"/>
Create Policy		Protocol:	All
Alert:		Message:	<input type="text"/>
Alert Threshold (requests):			
	<input type="button" value="Add"/> <input type="button" value="Clear"/>		

Figures

1. FTPBlock.png
2. FTPException.png
3. SSHBlock.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.