How to Configure URL Filtering in the Firewall

https://campus.barracuda.com/doc/45025999/

To enforce web filtering policies, you can add URL Filter objects to the application rules as an additional matching criteria. When the application rule matches, the website URL is compared with the on-device cache or online Barracuda URL category database. Once classified, the policy set for this URL category is executed. A valid Energize Updates subscription is required for URL Filtering in the Firewall service.

In this article

Before you Begin

- Create URL Filter Policy Objects and URL Filter Match Objects as needed. For more information, see How to Create an URL Filter Policy Object and How to Create an URL Filter Match Object.
- A URL Filter service is required.

Step 1. Enable URL Categorization

You must enable the URL categorization engine to be able to process URL categorization requests.

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > General Firewall Configuration**.
2. Click **Lock**.
3. From the **Configuration** menu in the left pane, click **Application Detection**.
4. Set **Working Mode** to **on**.

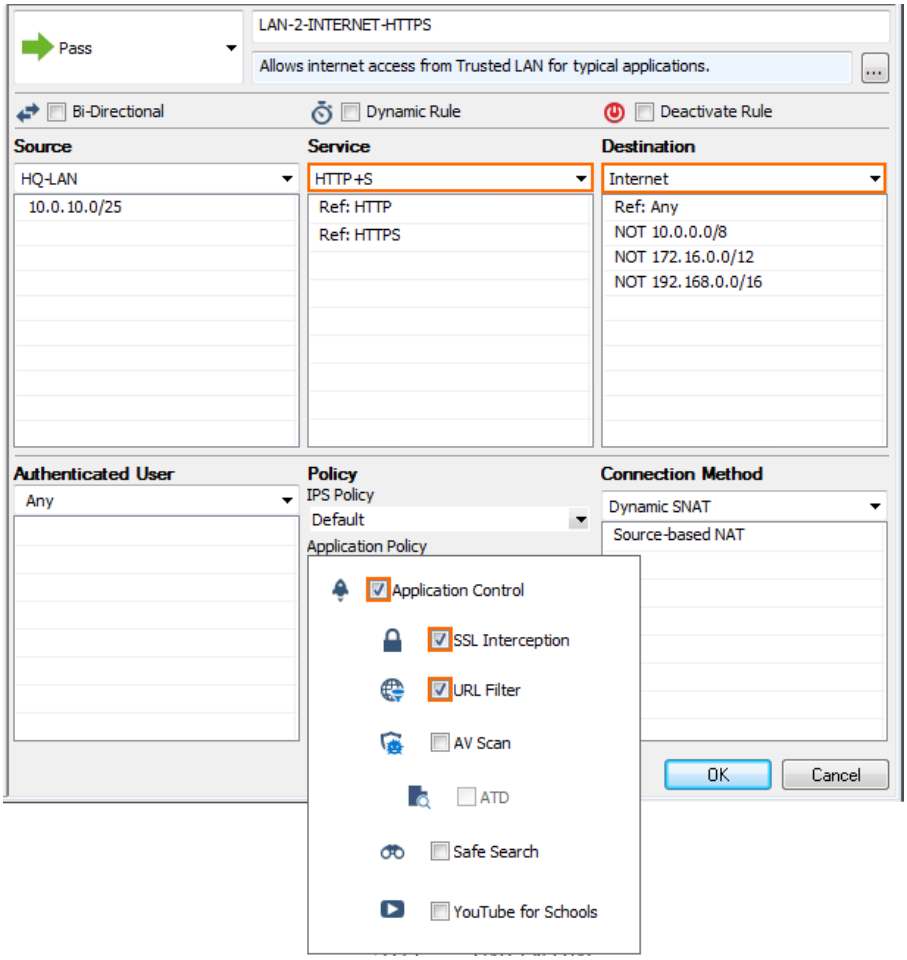
5. Click **Send Changes** and **Activate**.

The Barracuda URL Filter is now enabled and can handle URL categorization requests.

Step 2. Enable URL Filter for the Access Rule Handling Web Traffic

Enable Application Control 2.0, SSL Interception (optional), and URL Filter for the access rule matching web traffic.

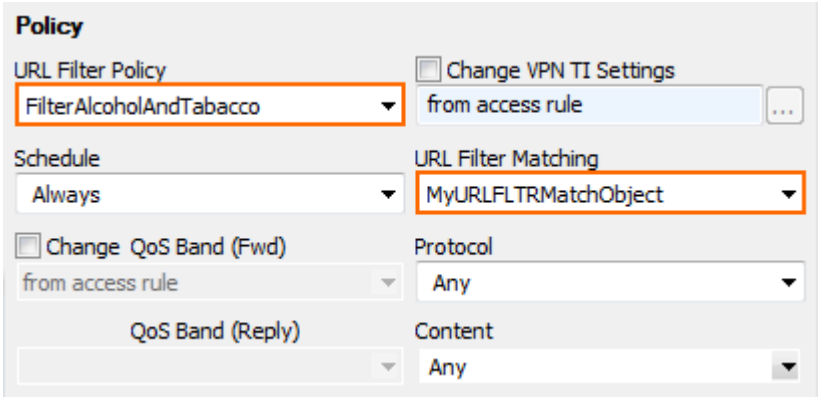
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
2. Double-click to edit the access rule matching outgoing web traffic generated by your users.
3. Verify that the access rule matches on both HTTP and HTTPS Internet traffic.
4. Click on the **Application Policy** link and enable the following Application Control 2.0 features:
   - **Application Control**
   - **(optional) SSL Interception**
   - **URL Filter**



5. Click **OK**.
6. Click **Send Changes** and **Activate**.

Step 3. Create Application Rule using URL Filter Objects

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
2. In the left menu, click **Application Rules** .
3. Click **Lock**.
4. Create a PASS application rule. For more information, see How to Create an Application Rule.
   - **Source** – Select the same source used in the matching access rule.
   - **Application** – Select **Any** to use only the web filtering. Otherwise, select an application object from the dropdown to combine application control and URL filtering.
   - **Destination** – Select the same destination used in the matching access rule.
5. Set at least one URL Filter object for the application rule:
   - Select a URL Filter Policy Object from the **URL Filter Policy** dropdown.
   - Select a URL Filter Match Object from the **URL Filter Matching** dropdown.



6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Monitoring URL Filtering in the Firewall

You can either check individual connections to see which policies are applied in the **FIREWALL > Live View** or see a summary of all Application traffic in the **FIREWALL > Firewall Monitor**.

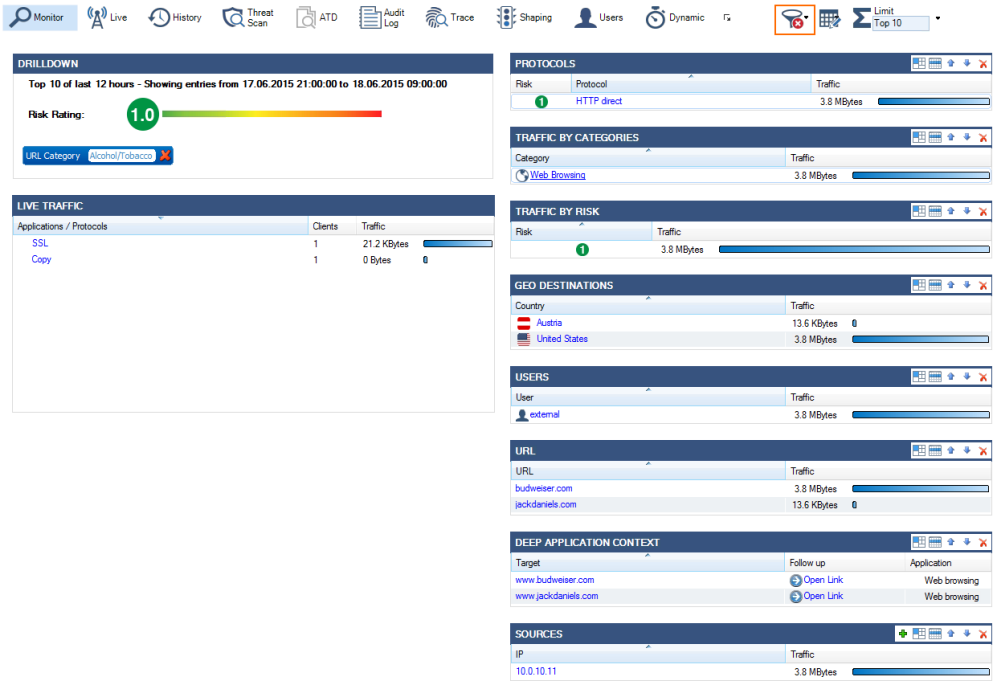
Firewall Live View

Go to **FIREWALL > Live View** and add the **URL Category** column to see the matching access and application rule, and the detected URL Filter category.

ID	State	IP Protocol	Port	Source	Interface	Destination	Output-IF	Application	Application Context	QoS	URL Category	Rule	Bit/s	Total	Idle
21112		TCP	80	10.0.10.11	eth0	192.230.80.163	eth1	Web browsing	www.budweiser.com	Internet /	Alcohol/Tobacco	LAN-2-INTERNET/<App>:FilterAlcoholandTabacco	744	34....	0s
21114		TCP	80	10.0.10.11	eth0	192.230.80.163	eth1	Web browsing	www.budweiser.com	Internet /	Alcohol/Tobacco	LAN-2-INTERNET/<App>:FilterAlcoholandTabacco	744	31....	0s
21108		TCP	80	10.0.10.11	eth0	192.230.80.163	eth1	Web browsing	www.budweiser.com	Internet /	Alcohol/Tobacco	LAN-2-INTERNET/<App>:FilterAlcoholandTabacco	744	33....	0s
21110		TCP	80	10.0.10.11	eth0	192.230.80.163	eth1	Web browsing	www.budweiser.com	Internet /	Alcohol/Tobacco	LAN-2-INTERNET/<App>:FilterAlcoholandTabacco	744	41....	0s
21119		TCP	80	10.0.10.11	eth0	192.230.80.163	eth1	Web browsing	www.budweiser.com	Internet /	Alcohol/Tobacco	LAN-2-INTERNET/<App>:FilterAlcoholandTabacco	744	14....	1s
21111		TCP	80	10.0.10.11	eth0	192.230.80.163	eth1	Web browsing	www.budweiser.com	Internet /	Alcohol/Tobacco	LAN-2-INTERNET/<App>:FilterAlcoholandTabacco	0	62....	38s
21113		TCP	80	10.0.10.11	eth0	192.230.80.163	eth1	Web browsing	www.budweiser.com	Internet /	Alcohol/Tobacco	LAN-2-INTERNET/<App>:FilterAlcoholandTabacco	0	42....	42s

Firewall Monitor

Go to **FIREWALL > Monitor** to receive a summary of all application and web traffic that matches Application Control 2.0-enabled access rules. Click on the links in the individual elements to apply filters to the monitor. Click the filter icon in the taskbar to see only specific URL Filter policies.



Figures

1. Conf_WF_Firewall_02.png
2. Conf_WF_Firewall_03.png
3. Conf_WF_Firewall_04.png
4. Conf_WF_Firewall_05a.png
5. Conf_WF_Firewall_06.png