

## 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

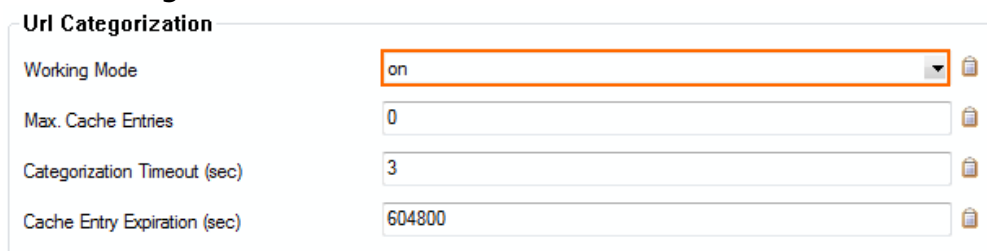
### Before you Begin

- 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**.



Url Categorization	
Working Mode	on
Max. Cache Entries	0
Categorization Timeout (sec)	3
Cache Entry Expiration (sec)	604800

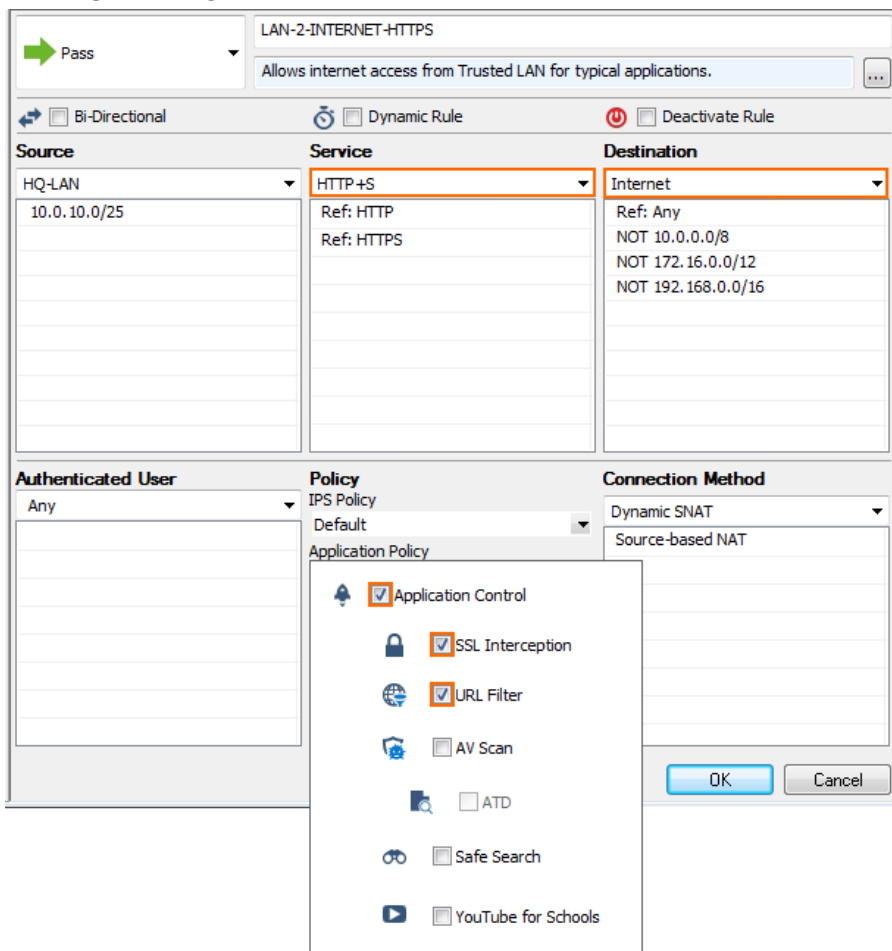
5. Click **Send Changes** and **Activate**.

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**

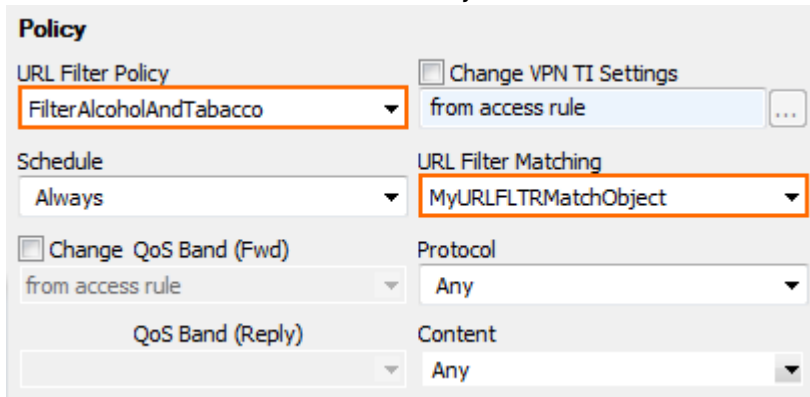


The screenshot shows the configuration for a forwarding rule named 'LAN-2-INTERNET-HTTPS'. The rule is set to 'Pass' and has a description 'Allows internet access from Trusted LAN for typical applications.' The 'Source' is 'HQ-LAN' (10.0.10.0/25), the 'Service' is 'HTTP+S' (Ref: HTTP, Ref: HTTPS), and the 'Destination' is 'Internet' (Ref: Any, NOT 10.0.0.0/8, NOT 172.16.0.0/12, NOT 192.168.0.0/16). The 'Authenticated User' is 'Any', the 'Policy' is 'IPS Policy' (Default), and the 'Connection Method' is 'Dynamic SNAT'. The 'Application Policy' dialog is open, showing 'Application Control', 'SSL Interception', and 'URL Filter' checked, and 'AV Scan', 'ATD', 'Safe Search', and 'YouTube for Schools' unchecked.

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.](#)
  - o **Source** - Select the same source used in the matching access rule.
  - o **Application** - Select **Any** to use only the web filtering. Otherwise, select an application object from the dropdown to combine application control and URL filtering.
  - o **Destination** - Select the same destination used in the matching access rule.
5. Set at least one URL Filter object for the application rule:
  - o Select a URL Filter Policy Object from the **URL Filter Policy** dropdown.
  - o 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.**

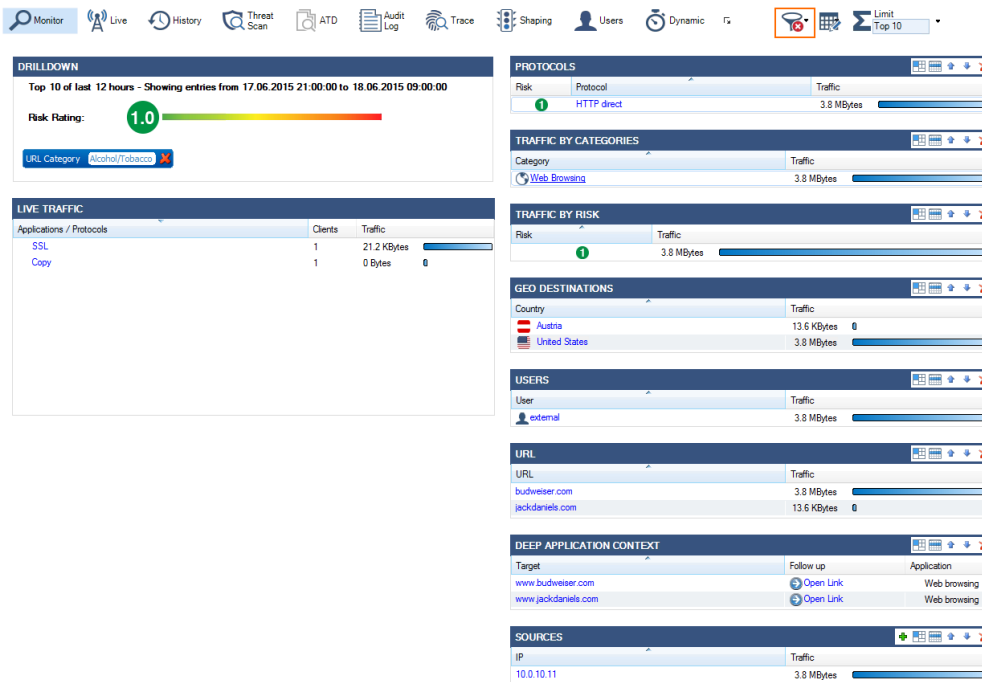
### Firewall Live View

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	52	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.



The screenshot displays the Firewall Monitor interface with the following panels:

- DRILLDOWN:** Shows a risk rating of 1.0 and a URL category filter set to 'Alcohol/Tobacco'.
- LIVE TRAFFIC:** A table showing traffic by application/protocol.
 

Applications / Protocols	Clients	Traffic
SSL	1	21.2 KBytes
Copy	1	0 Bytes
- PROTOCOLS:** Shows traffic by protocol, with 'HTTP direct' at 3.8 MBytes.
- TRAFFIC BY CATEGORIES:** Shows traffic by category, with 'Web Browsing' at 3.8 MBytes.
- TRAFFIC BY RISK:** Shows traffic by risk level, with a total of 3.8 MBytes.
- GEO DESTINATIONS:** Shows traffic by country, with 'Austria' at 13.6 KBytes and 'United States' at 3.8 MBytes.
- USERS:** Shows traffic by user, with 'external' at 3.8 MBytes.
- URL:** Shows traffic by URL, with 'budweiser.com' at 3.8 MBytes and 'jack-daniels.com' at 13.6 KBytes.
- DEEP APPLICATION CONTEXT:** Shows target URLs and their associated applications (e.g., 'www.budweiser.com' for 'Web browsing').
- SOURCES:** Shows traffic by IP address, with '10.0.10.11' at 3.8 MBytes.

## 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

© Barracuda Networks Inc., 2019 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.