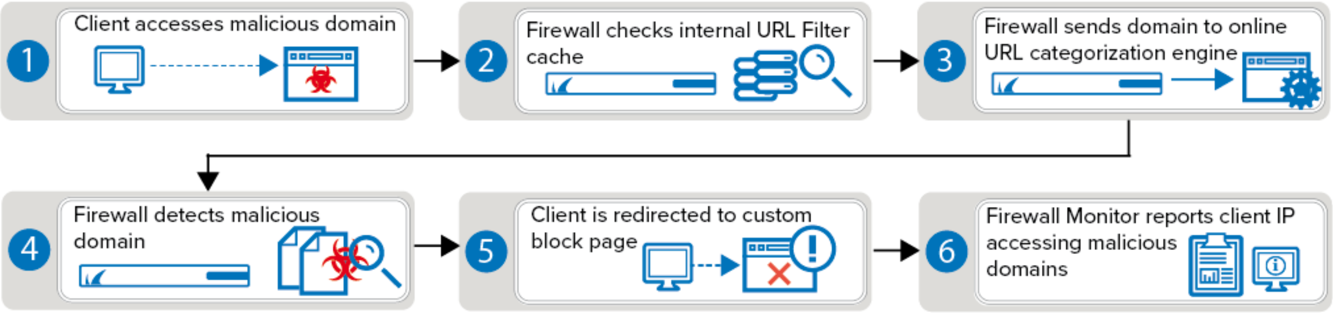
How to Configure URL Filtering in the Firewall

https://campus.barracuda.com/doc/79463028/

To enforce web filtering policies, add URL Filter objects to the application rules as an additional matching criteria or as a policy object. 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.


1
Client accesses malicious domain
2
Firewall checks internal URL Filter cache
3
Firewall sends domain to online URL categorization engine
4
Firewall detects malicious domain
5
Client is redirected to custom block page
6
Firewall Monitor reports client IP accessing malicious domains

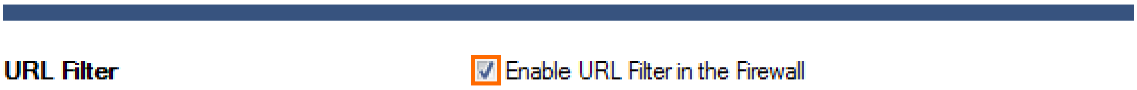
Before You Begin

Create URL Filter Policy Objects and URL Filter Match Objects as needed. For more information, see How to Create a URL Filter Policy Object and How to Create an URL Filter Match Object.

Step 1. Enable URL Categorization

You must enable the URL Filter to be able to process URL categorization requests. To change additional settings for the URL Filter service, see the **Application Detection** section in General Firewall Configuration.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Security Policy**.
2. Click **Lock**
3. In the **URL Filter** section, click **Enable URL Filter in the Firewall**.



URL Filter ☑ Enable URL Filter in the Firewall

4. Click **Send Changes** and **Activate**.

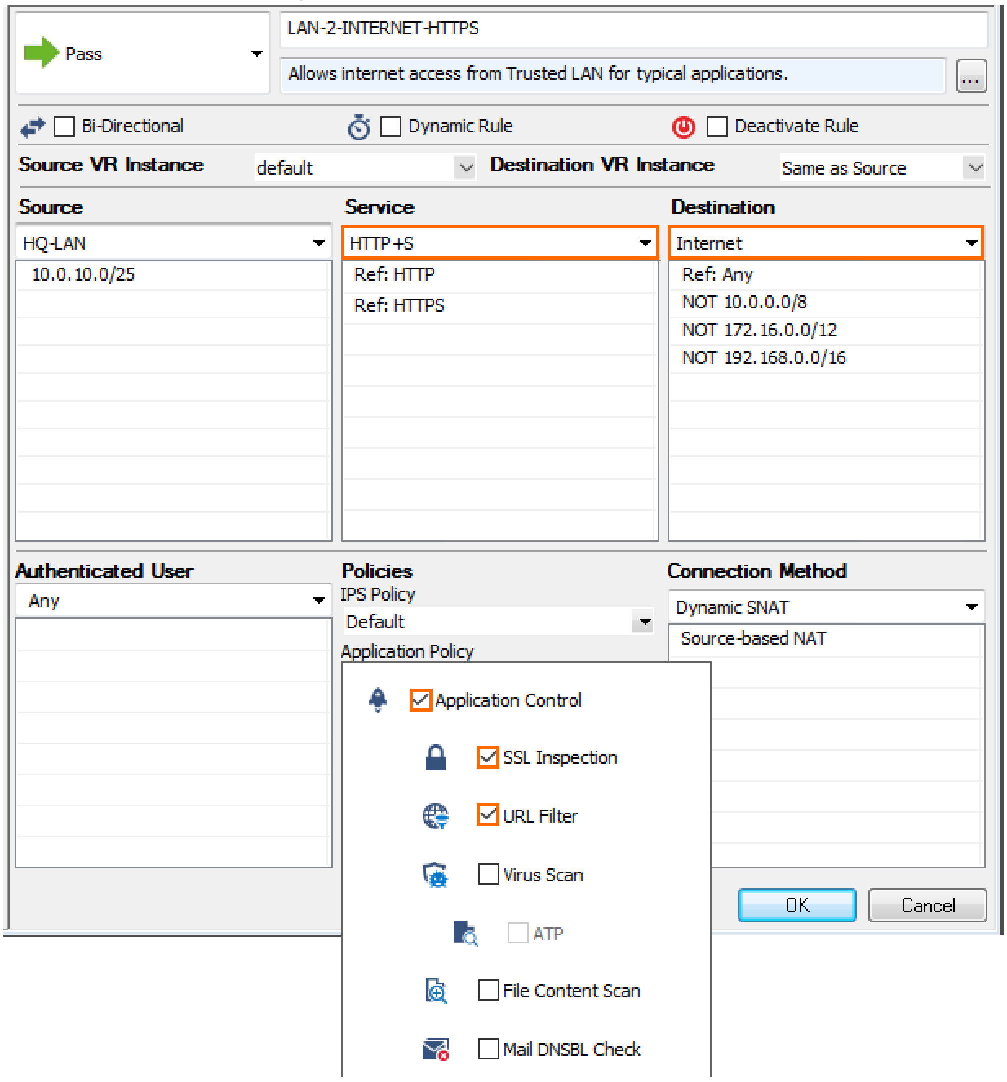
The Barracuda URL Filter is now enabled and can handle URL categorization requests.

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

---

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

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Double-click to edit the access rule matching HTTP and HTTPS traffic.
3. Click on the **Application Policy** link and select:
    - **Application Control** – required.
    - **SSL Inspection** – optional. If configured, select a policy from the **SSL Inspection Policy** drop-down list. For more information, see SSL Inspection in the Firewall.
    - **URL Filter** – required.



Pass

LAN-2-INTERNET-HTTPS

Allows internet access from Trusted LAN for typical applications.

☐ Bi-Directional ☐ Dynamic Rule ☐ Deactivate Rule

Source VR Instance: default

Destination VR Instance: Same as Source

Source: HQ-LAN
10.0.10.0/25

Service: HTTP+S
Ref: HTTP
Ref: HTTPS

Destination: Internet
Ref: Any
NOT 10.0.0.0/8
NOT 172.16.0.0/12
NOT 192.168.0.0/16

Authenticated User: Any

Policies
IPS Policy: Default
Application Policy:
☑ Application Control
☑ SSL Inspection
☑ URL Filter
☐ Virus Scan
☐ ATP
☐ File Content Scan
☐ Mail DNSBL Check

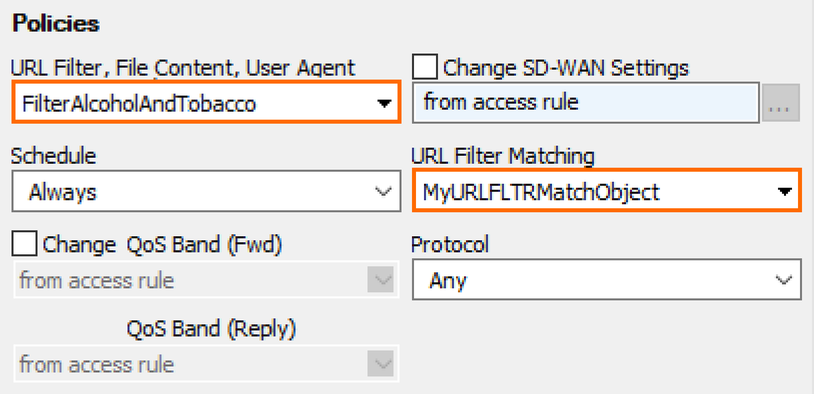
Connection Method: Dynamic SNAT
Source-based NAT

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

Step 3. Create an Application Rule Using URL Filter Objects

---

1. Go to **CONFIGURATION > Configuration Tree > Box > 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 drop-down list 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** drop-down list.
    - Select a URL Filter Match Object from the **URL Filter Matching** drop-down list.



Policies

URL Filter, File Content, User Agent: FilterAlcoholAndTobacco

☐ Change SD-WAN Settings: from access rule

Schedule: Always

URL Filter Matching: MyURLFLTRMatchObject

☐ Change QoS Band (Fwd): from access rule

Protocol: Any

QoS Band (Reply): from access rule

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

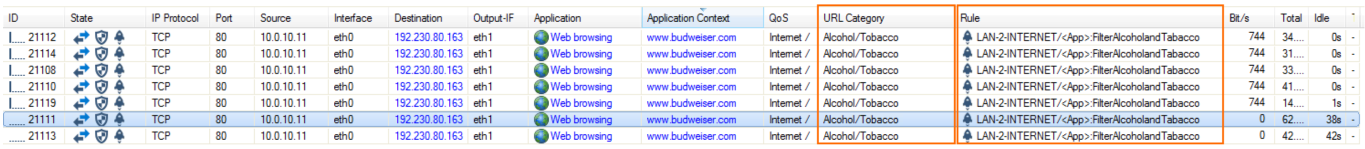
Rules are evaluated from top to bottom. Only the policy set in the first matching PASS rule that has URL Filter enabled is executed.

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

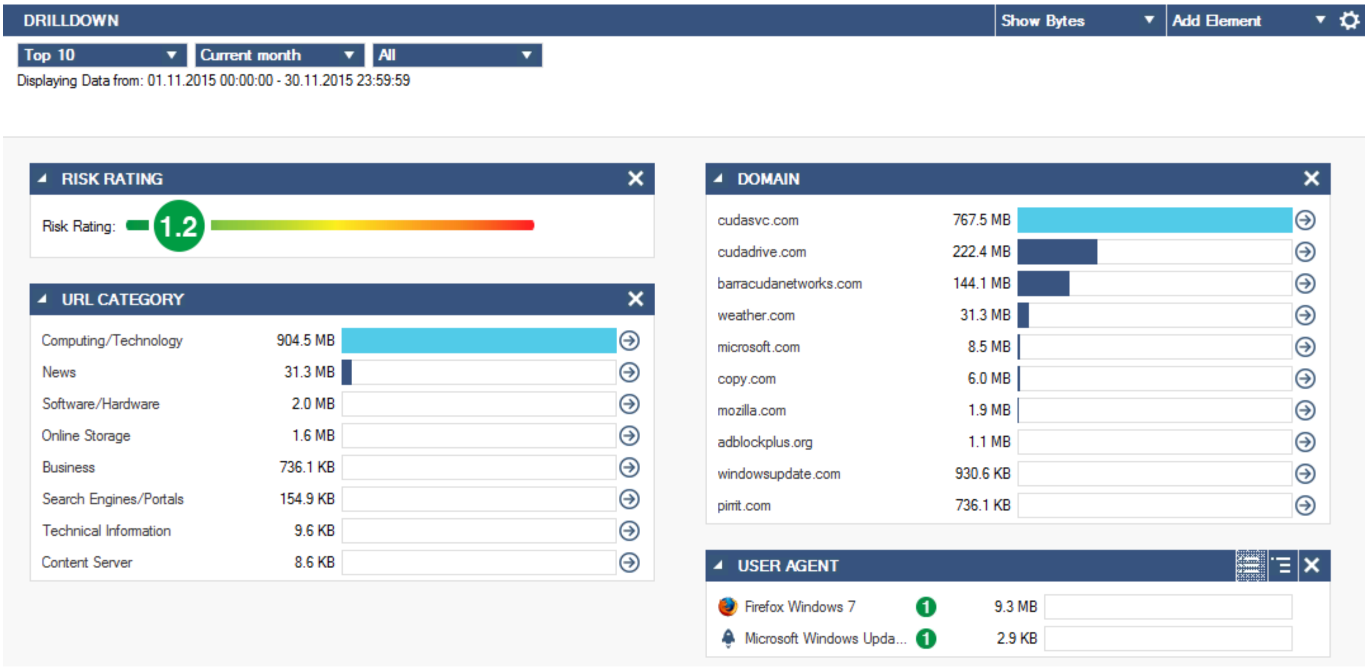
Go to **FIREWALL > Live View** and add the **URL Category** column to see the matching access and application rule, and the detected URL Filter category.



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-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.



Displaying Data from: 01.11.2015 00:00:00 - 30.11.2015 23:59:59

Risk Rating: 1.2

Computing/Technology	904.5 MB
News	31.3 MB
Software/Hardware	2.0 MB
Online Storage	1.6 MB
Business	736.1 KB
Search Engines/Portals	154.9 KB
Technical Information	9.6 KB
Content Server	8.6 KB

cudasvc.com	767.5 MB
cudadrive.com	222.4 MB
barracudanetworks.com	144.1 MB
weather.com	31.3 MB
microsoft.com	8.5 MB
copy.com	6.0 MB
mozilla.com	1.9 MB
adblockplus.org	1.1 MB
windowsupdate.com	930.6 KB
pirrit.com	736.1 KB

Firefox Windows 7	1	9.3 MB
Microsoft Windows Upda...	1	2.9 KB

Figures

1. url_filtering.png
2. enable_URL_Filter.png
3. Conf_WF_Firewall_03.png
4. Conf_WF_Firewall_04.png
5. Conf_WF_Firewall_05a.png
6. firewall_monitor.png