

How to Configure Botnet and Spyware Protection for Web Traffic

<https://campus.barracuda.com/doc/73719207/>

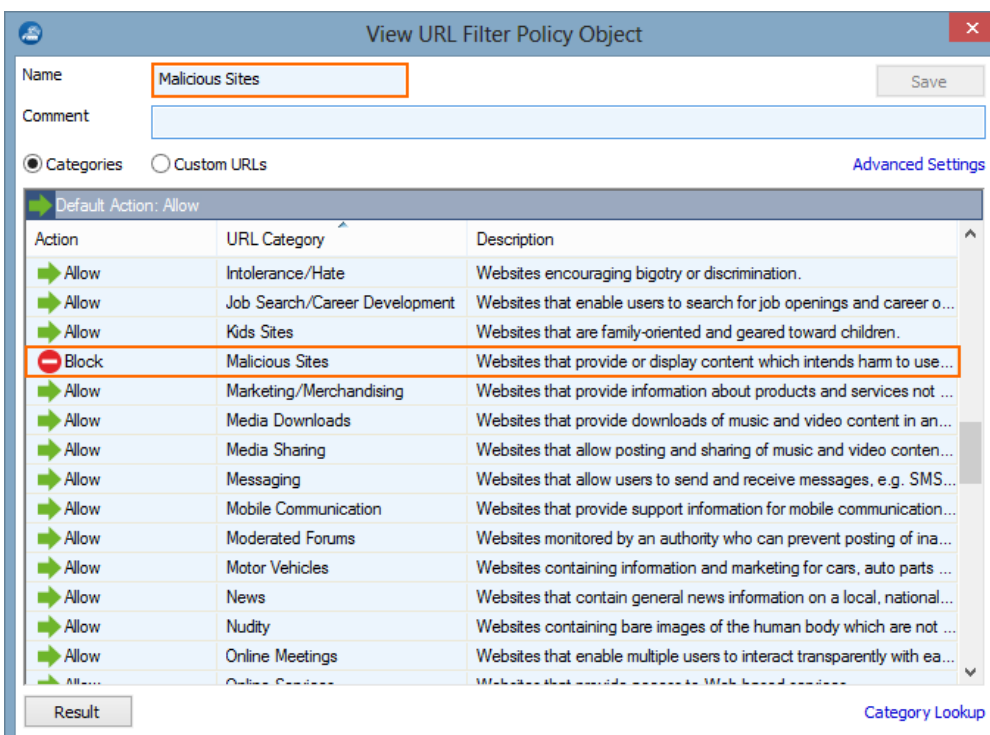
If you are not using a DNS sinkhole you can configure the URL filtering in the firewall to achieve similar results for HTTP and HTTPS traffic. This allows you to restrict access to malicious websites that may compromise the security of your client. The **Malicious Sites** URL category also uses the spyware and botnet database. Create a URL Filter policy object blocking access to websites in the **Malicious Sites** category and use it in the application rule matching your web traffic. When access to a malicious site is detected, the user is redirected to a custom block page. A valid Energize Updates subscription is required.

Before You Begin

- (optional) Configure an outbound SSL Inspection policy. To use SSL Inspection the **Feature Level** of the Forwarding Firewall must be set to **7.2** or higher. For more information, see [SSL Inspection in the Firewall](#) and [How to Configure Outbound SSL Inspection](#).

Step 1. Create a URL Filter Policy Object

Create a URL Filter policy object and set the **Action** for **Malicious Sites** category to **Block**.



View URL Filter Policy Object

Name: Malicious Sites

Comment:

Categories Custom URLs [Advanced Settings](#)

Default Action: Allow

Action	URL Category	Description
Allow	Intolerance/Hate	Websites encouraging bigotry or discrimination.
Allow	Job Search/Career Development	Websites that enable users to search for job openings and career o...
Allow	Kids Sites	Websites that are family-oriented and geared toward children.
Block	Malicious Sites	Websites that provide or display content which intends harm to use...
Allow	Marketing/Merchandising	Websites that provide information about products and services not ...
Allow	Media Downloads	Websites that provide downloads of music and video content in an...
Allow	Media Sharing	Websites that allow posting and sharing of music and video conten...
Allow	Messaging	Websites that allow users to send and receive messages, e.g. SMS...
Allow	Mobile Communication	Websites that provide support information for mobile communication...
Allow	Moderated Forums	Websites monitored by an authority who can prevent posting of ina...
Allow	Motor Vehicles	Websites containing information and marketing for cars, auto parts ...
Allow	News	Websites that contain general news information on a local, national...
Allow	Nudity	Websites containing bare images of the human body which are not ...
Allow	Online Meetings	Websites that enable multiple users to interact transparently with ea...
Allow	Online Services	Websites that provide access to Web-based services.

Result [Category Lookup](#)

For more information, see [How to Create a URL Filter Policy Object](#).

Step 2. 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 > Virtual Servers > your virtual server > 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

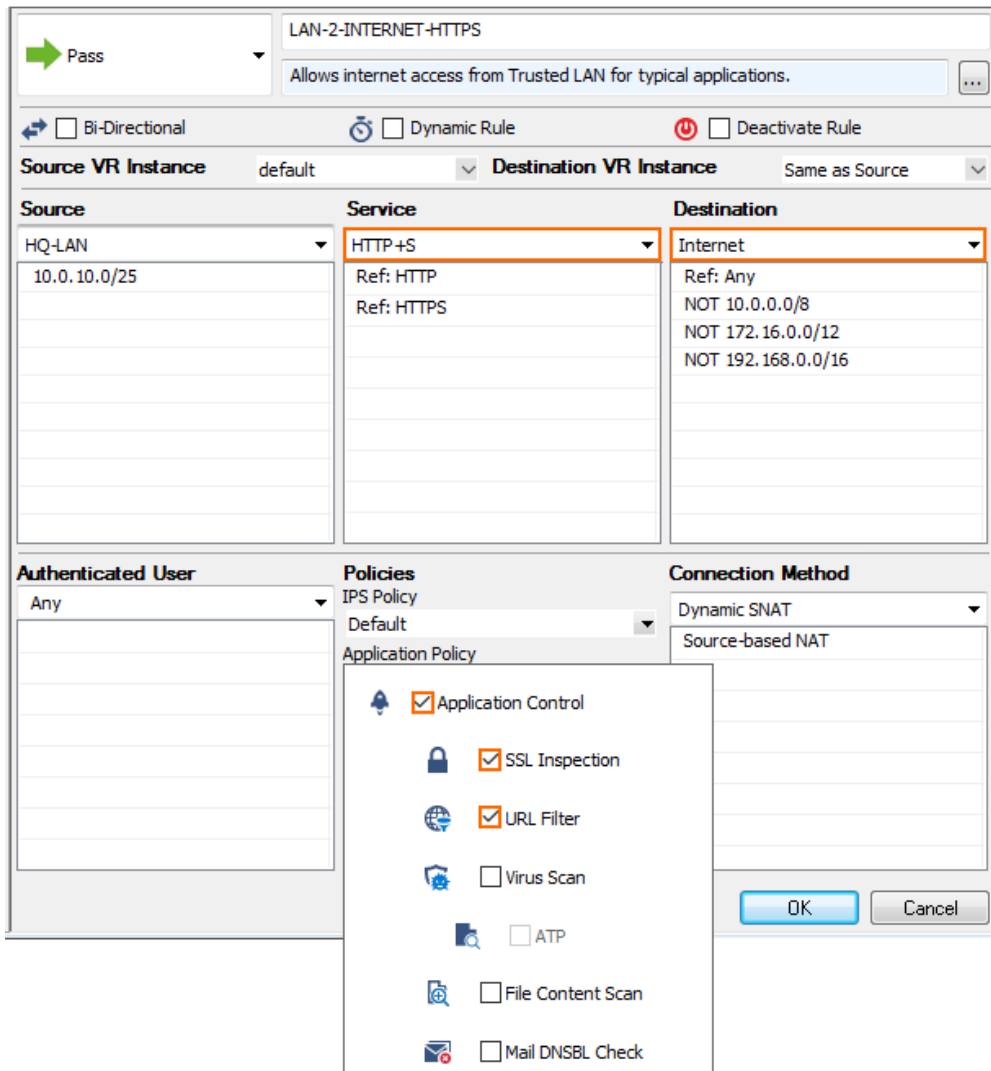
4. Click **Send Changes** and **Activate**.

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

Step 3. Enable the URL Filter for the Access Rule Handling Web Traffic

Enable Application Control, SSL Inspection, 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 HTTP and HTTPS traffic.
3. Click on the **Application Policy** link and select:
 - **Application Control** - required.
 - **SSL Inspection** - recommended.
 - **URL Filter** - required.



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	Service	Destination
HQ-LAN 10.0.10.0/25	HTTP+S Ref: HTTP Ref: HTTPS	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

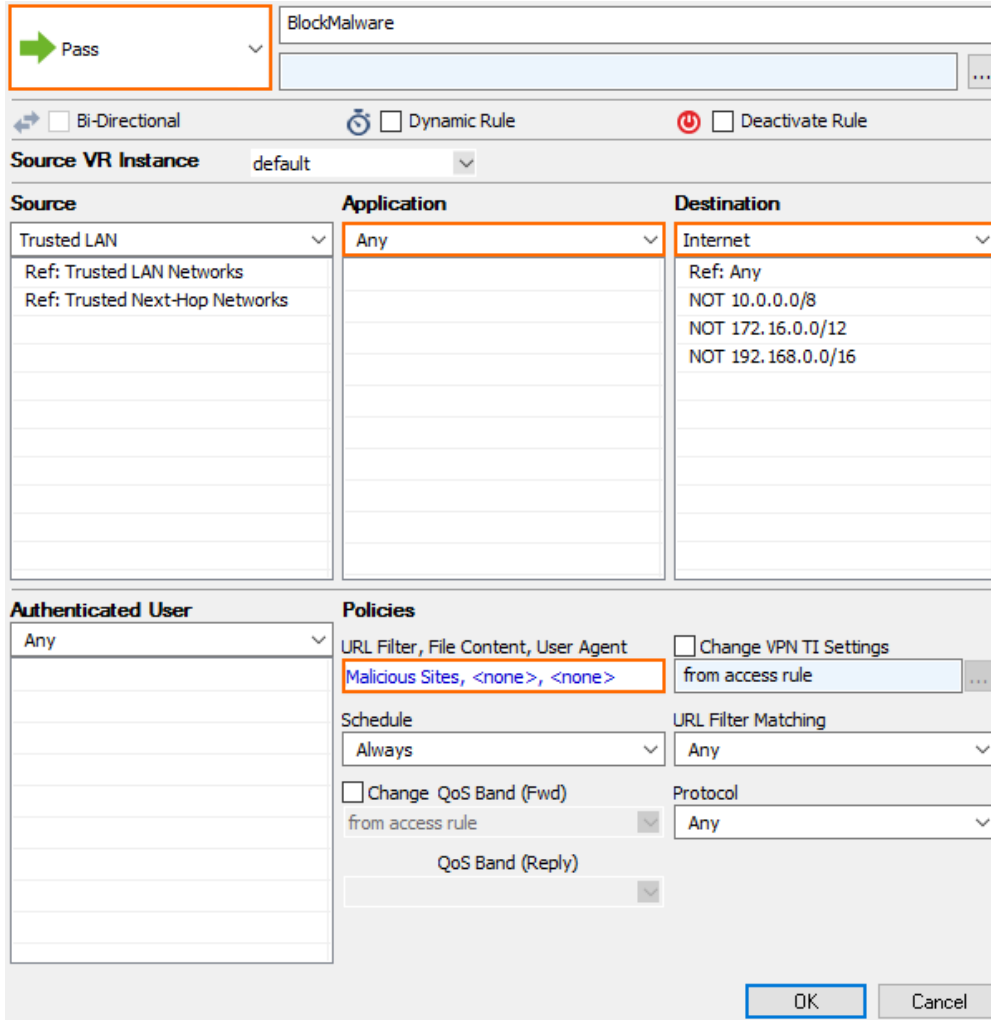
OK Cancel

4. Select a policy from the **SSL Inspection Policy** drop-down list.
5. Click **OK**.
6. Click **Send Changes** and **Activate**.

Step 4. Create an 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 drop-down list to combine application control and URL filtering.
 - **Destination** - Select **Internet**.
5. Click the **URL Filter, File Content, User Agent** link.

6. Click **URL Filter**.
7. Click the URL Filter policy object created in step 1.



BlockMalware

Pass

Bi-Directional
 Dynamic Rule
 Deactivate Rule

Source VR Instance: default

Source	Application	Destination
Trusted LAN Ref: Trusted LAN Networks Ref: Trusted Next-Hop Networks	Any	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: URL Filter, File Content, User Agent
 Malicious Sites, <none>, <none>

Change VPN TI Settings
 from access rule

Schedule: Always
 URL Filter Matching: Any

Change QoS Band (Fwd)
 from access rule
 QoS Band (Reply)

Protocol: Any

OK Cancel

8. Click **OK**.
9. Click **Send Changes** and **Activate**.

Firewall Monitor

Go to **FIREWALL > Monitor** and drill down into the **Malicious Sites** category to receive a summary of all clients attempting to access websites in this category.

DRILLDOWN Show Bytes Add Element ⚙️

Top 10 ▼ Current month ▼ All ▼

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

RISK RATING ✕

Risk Rating: 1.2



URL CATEGORY ✕

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	→

DOMAIN ✕

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	→
pinit.com	736.1 KB	→

USER AGENT ⌵ ☰ ✕

Firefox Windows 7	1	9.3 MB	<input type="text"/>
Microsoft Windows Upda...	1	2.9 KB	<input type="text"/>

Figures

1. spy_bot_url_filter_01.png
2. enable_URL_Filter.png
3. Conf_WF_Firewall_03.png
4. spy_bot_url_filter_02.png
5. firewall_monitor.png

© Barracuda Networks Inc., 2020 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.