
How to Block Search Terms using a Custom Application Object

<https://campus.barracuda.com/doc/79463031/>

If the search term you want to block is not covered by the Safe Search feature (because it does not represent adult content), you can still block specific search terms or queries by creating a custom application. Custom search applications are supported for Google, Yahoo, Bing, and YouTube. These custom application objects can then be selected in the matching application rule. Custom search applications do not override the **Safe Search** settings of the matching access rule.

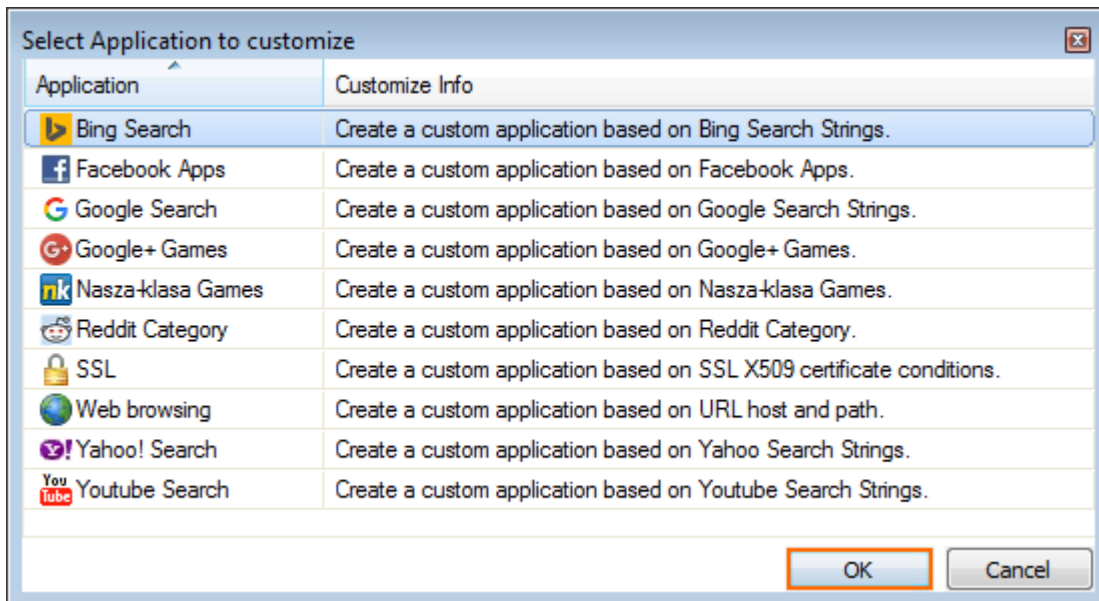
Before You Begin

- Define the search terms you wish to block. Wildcard characters (* and ?) are allowed. E.g., *searchterm?searchterm*
- (optional) Enable SSL Inspection. 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](#).

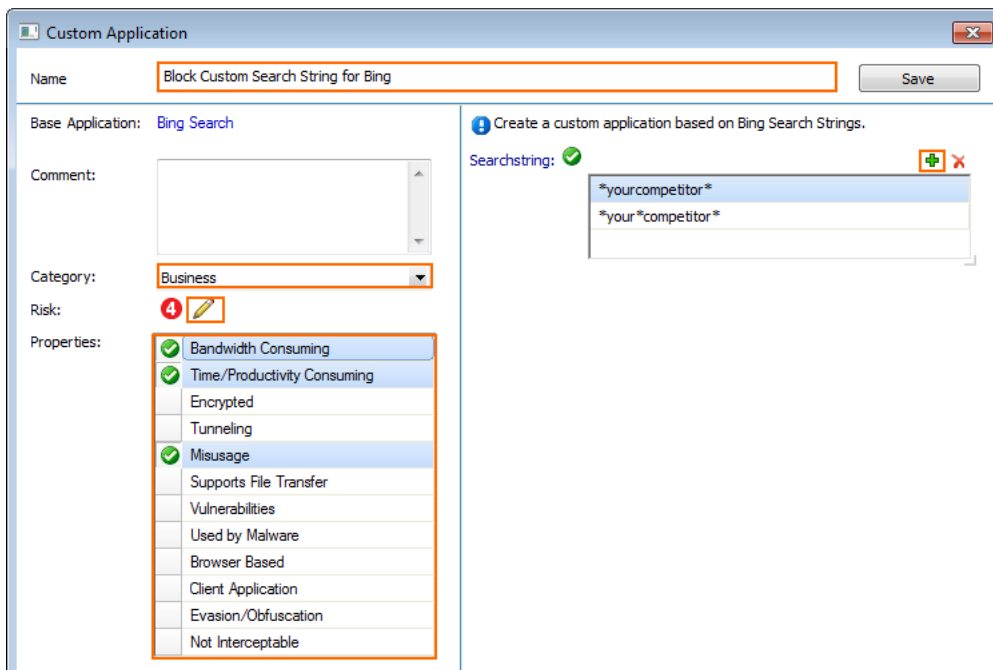
Step 1. Create a Custom Application Object

Create a custom application object for each search engine provider.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**.
2. In the left menu, click **Applications**.
3. Right-click in the main area, and select **New > Custom Application**. The **Select Application to customize** window opens.
4. Select the search engine provider. E.g. **Bing Search**
5. Click **OK**. The **Custom Application** window opens.



6. Enter a **Name**.
7. Select a **Category**.
8. Click the **edit** icon to select the **Risk** factor.
9. Select the **Properties**.
10. Click **+** to add a **Search String**. Wildcards * and ? are allowed. Multiple search entries are combined with a logic OR.
11. Click **Save**.



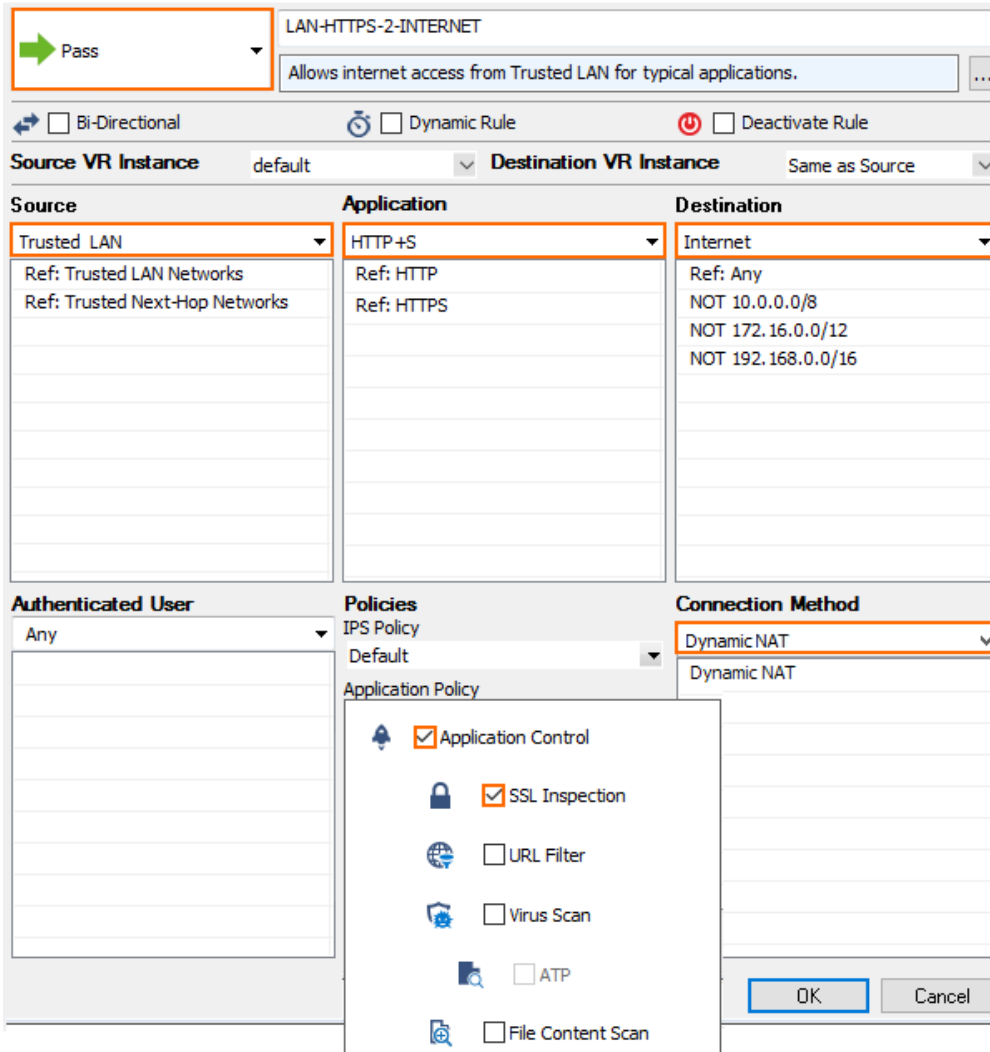
12. Click **Send Changes** and **Activate**.

To block this search term for all supported search engine providers, repeat this step for each search engine.

Step 2. Create a PASS Access Rule

Create a PASS access rule that matches outgoing HTTP and HTTPS traffic. Because most search engines use HTTPS, using SSL Inspection is recommended.

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 both HTTP and HTTPS traffic.
4. Click on the **Application Policy** link and enable the following Application Control features:
 - o **Application Control**
 - o **(optional) SSL Inspection**



The screenshot shows the configuration for a 'Pass' rule named 'LAN-HTTPS-2-INTERNET'. The rule description is 'Allows internet access from Trusted LAN for typical applications.' The rule is configured with the following settings:

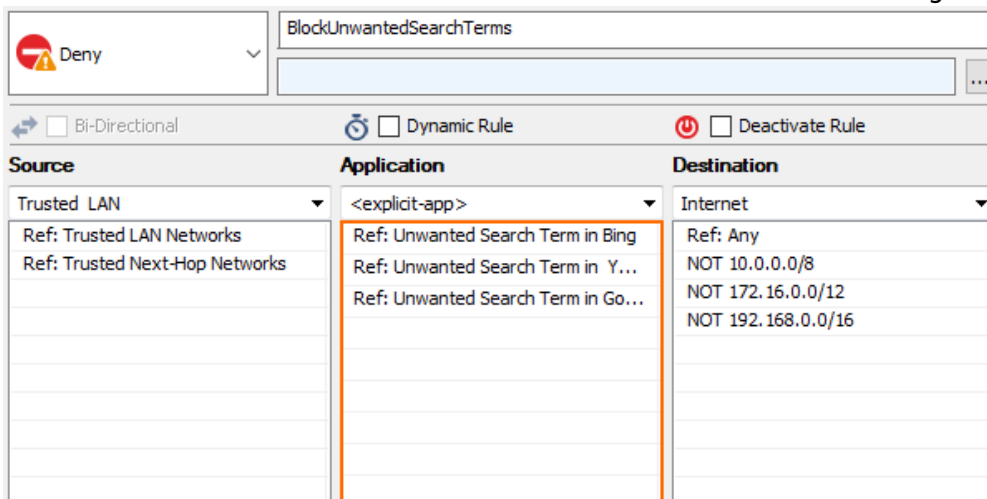
- Source VR Instance:** default
- Destination VR Instance:** Same as Source
- Source:** Trusted LAN (References: Trusted LAN Networks, Trusted Next-Hop Networks)
- Application:** HTTP+S (References: HTTP, HTTPS)
- Destination:** Internet (References: Any, NOT 10.0.0.0/8, NOT 172.16.0.0/12, NOT 192.168.0.0/16)
- Authenticated User:** Any
- IPs Policy:** Default
- Application Policy:** Application Control (checked), SSL Inspection (checked), URL Filter (unchecked), Virus Scan (unchecked), ATP (unchecked), File Content Scan (unchecked)
- Connection Method:** Dynamic NAT

5. If configured, select a policy from the **SSL Inspection Policy** drop-down list. For more information, see [SSL Inspection in the Firewall](#).
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Step 3. Create an Application Rule using the Custom Application Objects

Create an application rule matching the same traffic that matches the access rule created in Step 2.

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 DENY 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 the custom application objects created in Step 1.
 - **Destination** - Select the same destination used in the matching access rule.



The screenshot shows the configuration interface for a Deny application rule. The rule name is "BlockUnwantedSearchTerms". The action is set to "Deny". The rule is configured with the following settings:

Source	Application	Destination
Trusted LAN	<explicit-app>	Internet
Ref: Trusted LAN Networks	Ref: Unwanted Search Term in Bing	Ref: Any
Ref: Trusted Next-Hop Networks	Ref: Unwanted Search Term in Y...	NOT 10.0.0.0/8
	Ref: Unwanted Search Term in Go...	NOT 172.16.0.0/12
		NOT 192.168.0.0/16

Additional options shown include Bi-Directional, Dynamic Rule, and Deactivate Rule, all of which are currently unchecked.

5. Click **OK**.
6. Place the application rule so that no application rule above it matches the same traffic.
7. Click **Send Changes** and **Activate**.

You are now blocking searches for the unwanted search terms listed in the custom application objects. Users searching for these terms are redirected to the customizable block page. For more information, see [How to Configure Custom Block Pages and Texts](#).

Figures

1. custom_searchterm_app_01.png
2. custom_searchterm_app_02.png
3. custom_searchterm_app_03.png
4. custom_searchterm_app_04.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.