How to Enforce Safe Search in the Firewall

https://campus.barracuda.com/doc/46209067/

You can protect users behind a Barracuda NextGen Firewall F-Series from undesired content in search results by enabling Safe Search for the access rule handling web traffic. The necessary parameters are automatically appended to the URL when the request is forwarded by the firewall to enforce SafeSearch. Safe Search is supported for Google, Bing, Yahoo and YouTube search engines.

Limitations

- Safe Search relies on the supported search engines to honor and filter the search results. The firewall can enable this feature, but the execution is left up to the search engine.
- Safe Search is not enforced for mobile search apps.
- Safe Search is always set to **strict**.
- The URL Category **Search Engine** may not be set to **override** when URL Filtering is used in combination with Safe Search.

In this article

Before You Begin

- The **Feature Level** of the Forwarding Firewall must be **6.1** or higher.
- Enable Application Control. For more information, see How to Enable Application Control.
- Enable SSL Interception. For more information, see How to Configure SSL Interception in the Firewall.

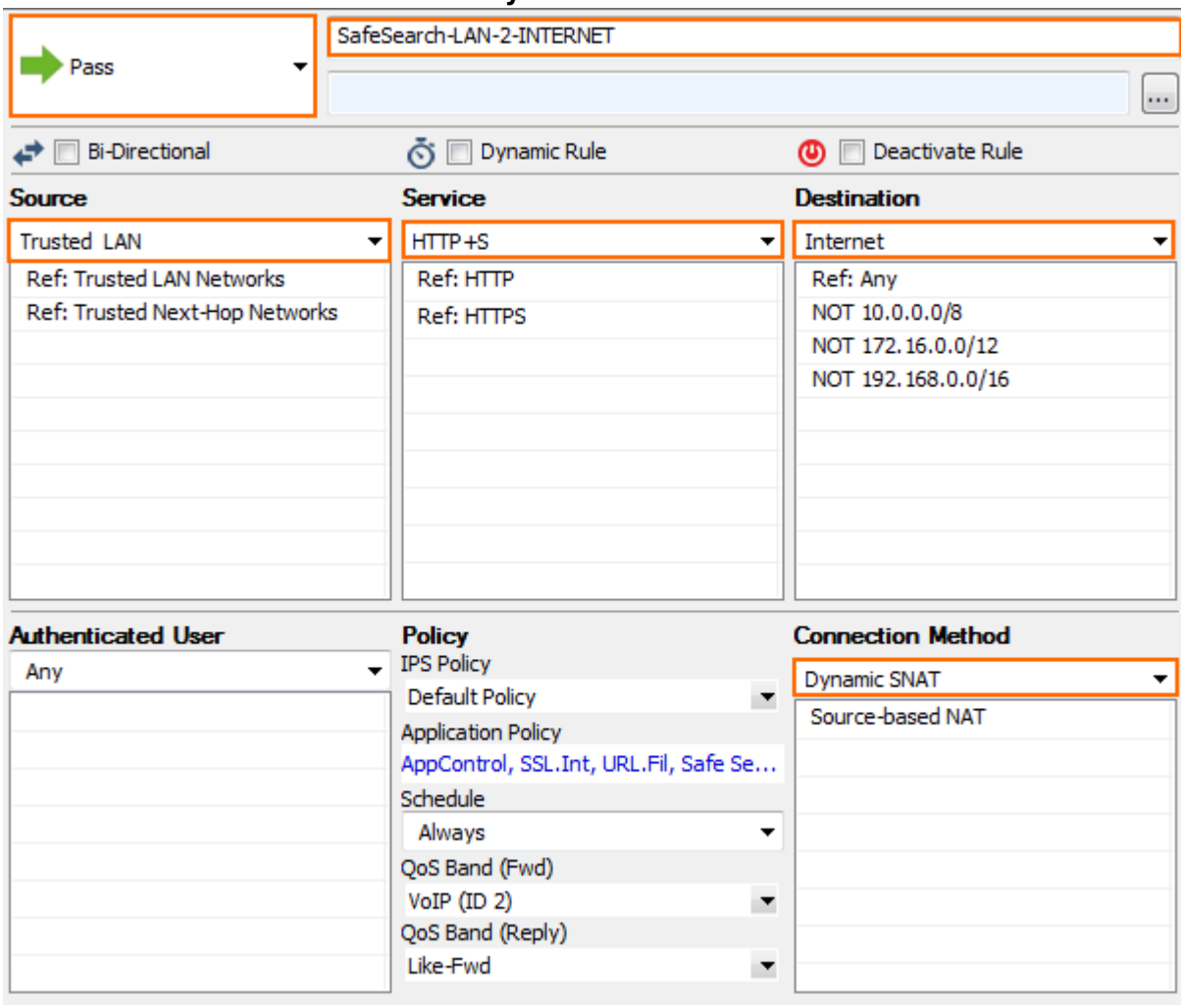
Create an Access to Enforce Safe Search

You can enforce the usage of Safe Search for all web traffic matching an access rule by enabling the Safe Search settings in the Application Control settings of the access rule.

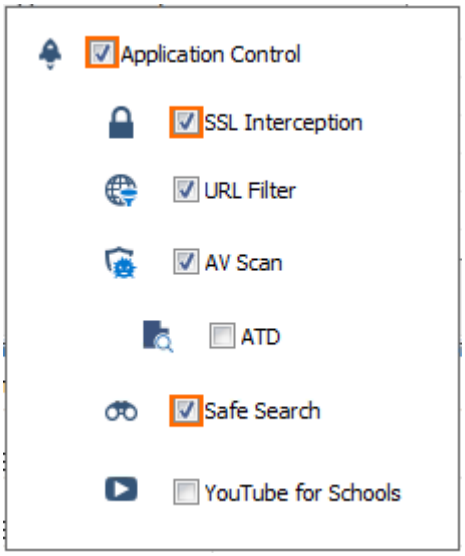
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Either click the plus icon (**+**) at the top right of the ruleset, or right-click the ruleset and select **New > Rule**.

4. Select **Pass** as the action.

5. Enter a **name** for the rule. For example, `SafeSearch-LAN-2-INTERNET`
6. Specify the following settings to match your web traffic:
   - **Source** – The source addresses of the traffic.
   - **Destination** – Select **Internet**.
   - **Service** – Select **HTTP+S**.
   - **Connection Method** – Select **Dynamic SNAT**.

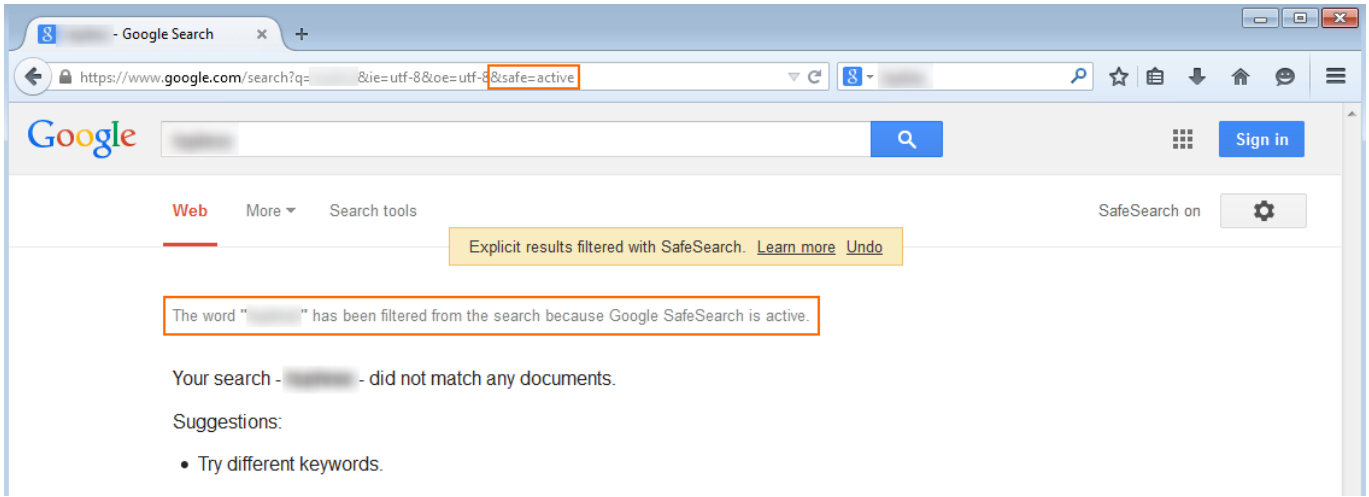


7. Click on the **Application Policy** link and select**:**
   - **Application Control** – required.
   - **SSL Interception** – Required for search provides which are available exclusively via HTTPS.
   - **URL Filter** – optional.
   - **Safe Search** – required.



8. (optional) Set additional matching criteria:
   - **Authenticated User** – For more information, see User Objects.
   - **Schedule Object** – For more information, see Schedule Objects.
9. Click **OK**.
10. Click **Send Changes** and **Activate**.

Every search query handled by this access rule now automatically enables the Safe Search feature of the search engine provider.



Disabling SafeSearch for YouTube

In addition to removing the policy on the matching access rules, it is also necessary to clear the browser cache to remove the YouTube safe search cookie.

Figures

1. FW_Rule_Add01.png
2. safe_search01.png
3. safe_search02.png
4. safe_search03.png