

Facebook Control Over HTTPS

<https://campus.barracuda.com/doc/17106244/>

The Barracuda Web Security Gateway can be configured for scanning of HTTPS traffic at the URL level when the **SSL Inspection** feature is enabled. This means that the administrator has granular control over what applications are blocked or allowed on websites like Facebook.com. The administrator can control Facebook traffic, for example, by specifying domain/sub-domain patterns associated with Facebook applications to be inspected over HTTPS. With SSL Inspection, the Barracuda Web Security Gateway can apply policies granularly to HTTPS traffic at the URL level as well as detect malware and viruses. For more information about this feature, see [Using SSL Inspection With the Barracuda Web Security Gateway](#). This article provides several use cases as examples.

SSL Inspection of HTTPS traffic for this use case is available:

- With either WCCP or Forward Proxy deployments on the Barracuda Web Security Gateway 610 and higher, or the Barracuda Web Security Gateway 410 running version 10 and higher.
- With either inline, WCCP, or Forward Proxy deployments on the Barracuda Web Security Gateway 910 and 1010.

Use Case #1 - Blocking Facebook Apps

Suppose you want allow access to Facebook.com for students, but want to **ONLY** allow Facebook *Applications (Apps)* during school lunch time. Using the URL pattern for Facebook Apps (<https://apps.facebook.com>, <https://www.facebook.com/appcenter/>), you would first configure **SSL Inspection**, then create a policy on the **BLOCK/ACCEPT > Exceptions** page.

Step 1. Enable and configure SSL Inspection:

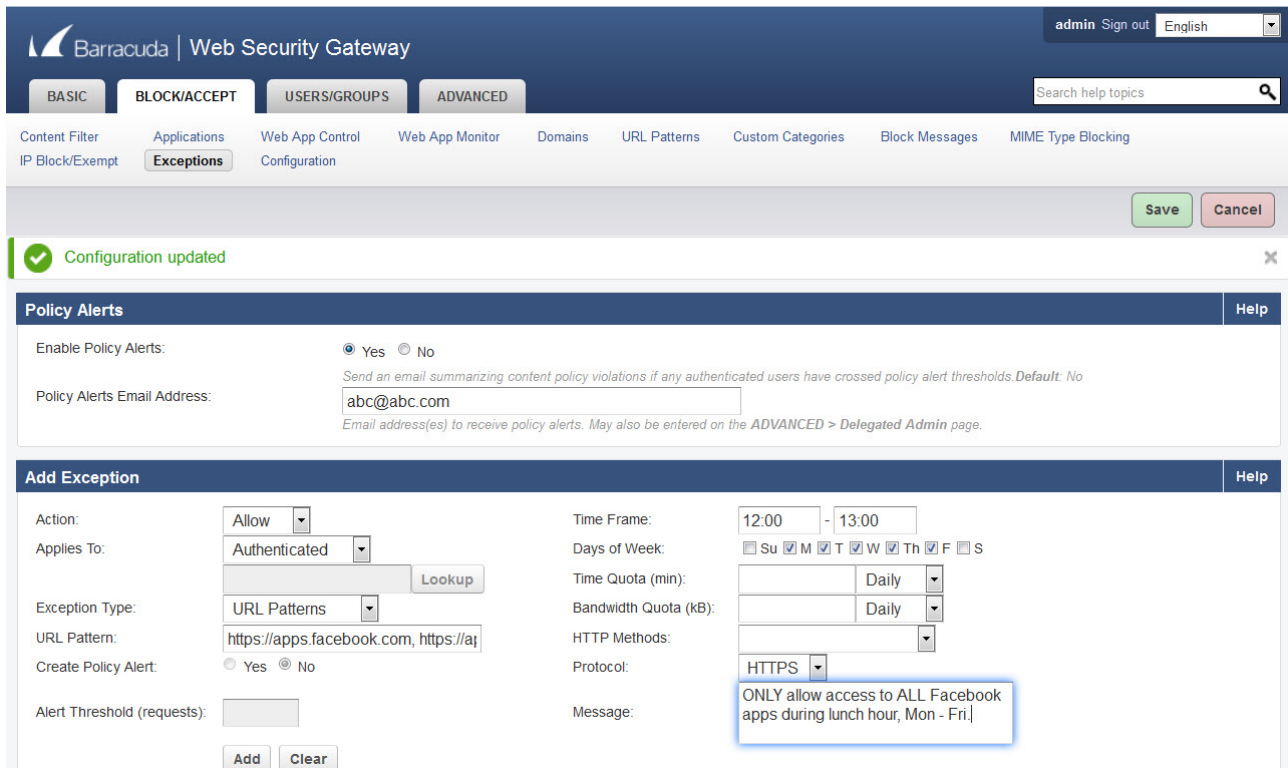
1. Log into the Barracuda Web Security Gateway web interface as an administrator.
2. On the **ADVANCED > SSL Inspection** page, set **Enable SSL Inspection** to Yes.
3. In the Inspected Domains field, enter Facebook.com and click **Add**.
4. Install an SSL certificate. There are two recommended options:
 - Select **Create** to generate your own signed SSL certificate and download it to install in or push out to each client browser. If you don't, users will see a warning each time they browse an HTTPS site when **SSL Inspection** is enabled. For detailed instructions on creating and installing the certificate, see [How to Create and Install a Self-Signed Certificate for SSL Inspection](#).
 - Use the [Barracuda Networks Default Certificate for SSL Inspection](#), available on the **ADVANCED > SSL Inspection** page. This is the simpler of the two methods. If you are

only using one Barracuda Web Security Gateway (as opposed to clustering two or more systems using Linked Management), the private key is more secure as it never leaves the device. If you have a high availability deployment, you will need to install the same root certificate on each Barracuda Web Security Gateway. For detailed instructions on installing the certificate, see [How to Use the Barracuda Networks Default Certificate for SSL Inspection](#).

Step 2. Create the policy:

1. On the **BLOCK/ACCEPT > Exceptions** page, in the **Add Exceptions** section, select the **Allow Action**. See **Figure 1** below. Select the type of users you want to allow (*Authenticated, Local Group*, etc.) in the **Applies To** field. In this case we've chosen *Authenticated* users. If your set of authenticated users includes teachers, you might want to create a group for students using the **USERS/ GROUPS** pages and then select the student group for **Applies To**.
2. Select **URL Pattern** as the **Exception Type**.
3. Enter `https://apps.facebook.com,` `https://www.facebook.com/appcenter` as the **URL pattern** (make sure to include a comma between URLs).
4. Set the **Time Frame** from 12:00 - 13:00 Mon. - Fri., or whatever constitutes 'lunch hour'.

Figure 1: Creating a limited Allow policy for Facebook applications during school lunch hours



The screenshot shows the Barracuda Web Security Gateway configuration interface. The top navigation bar includes tabs for BASIC, BLOCK/ACCEPT, USERS/GROUPS, and ADVANCED. The 'BLOCK/ACCEPT' tab is active, and the 'Exceptions' sub-tab is selected. A green notification bar at the top indicates 'Configuration updated'. Below this, the 'Policy Alerts' section is visible, with 'Enable Policy Alerts' set to 'Yes' and 'Policy Alerts Email Address' set to 'abc@abc.com'. The 'Add Exception' section is the primary focus, showing the following configuration:

- Action:** Allow
- Applies To:** Authenticated
- Exception Type:** URL Patterns
- URL Pattern:** https://apps.facebook.com, https://www.facebook.com/appcenter
- Create Policy Alert:** No
- Alert Threshold (requests):** 1
- Time Frame:** 12:00 - 13:00
- Days of Week:** Mon, Tue, Wed, Thu, Fri (checked)
- Time Quota (min):** Daily
- Bandwidth Quota (kB):** Daily
- HTTP Methods:** All
- Protocol:** HTTPS
- Message:** ONLY allow access to ALL Facebook apps during lunch hour, Mon - Fri.

5. Select the **Protocol** as **HTTPS**. Enter a message if you like to describe what the policy is about.
6. Configure policy alerts as needed. With **Enable Policy Alerts** set to **On**, the Barracuda Web Security Gateway will send an email summarizing content policy violations to the email address(es) entered in the **Policy Alerts Email Address** field.

7. Click **Add**. You have now created your policy.

Use Case #2 - Blocking Facebook Chat for students

Suppose you want allow access to all Facebook activities *except* chat for students. Using the URL pattern for Facebook *Messages* (`https://www.facebook.com/messages`), you would first configure SSL Inspection, then create a policy on the **BLOCK/ACCEPT > Exceptions** page.

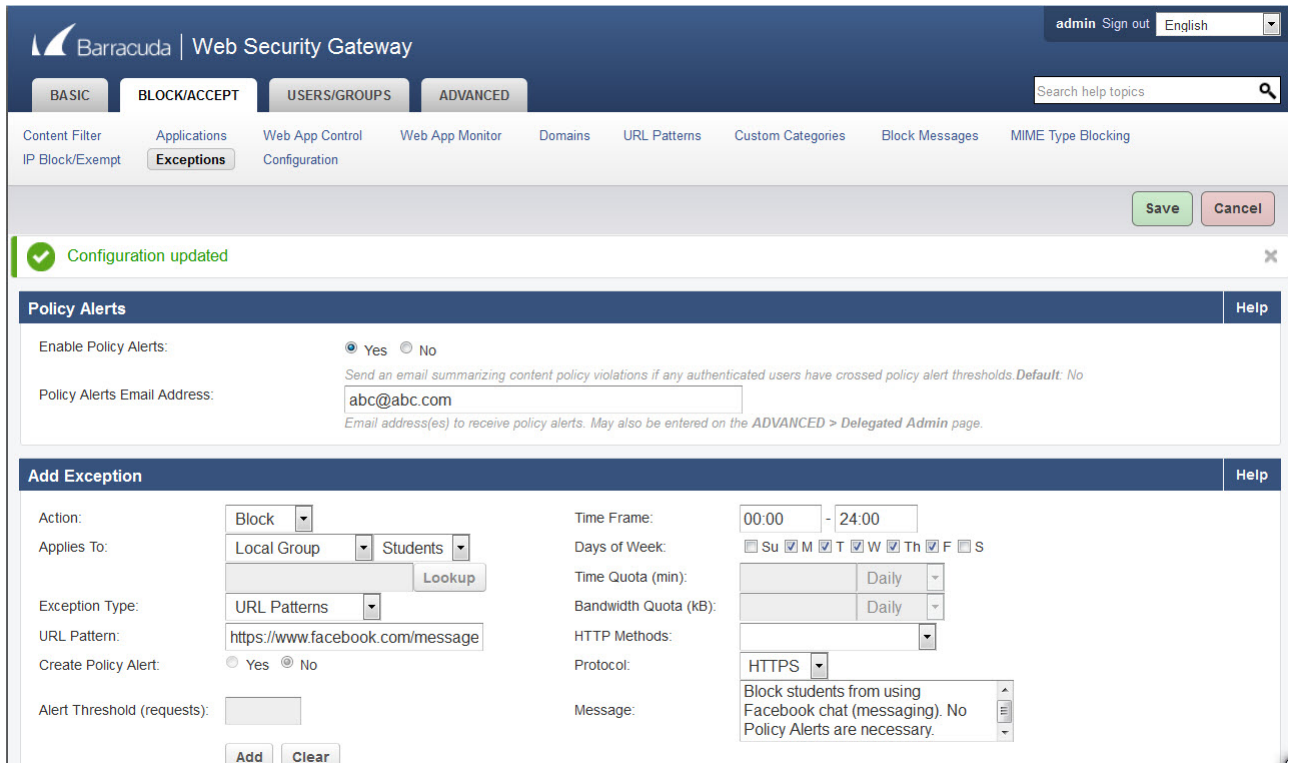
Step 1. Enable and configure SSL Inspection (if not already done):

1. Log into the Barracuda Web Security Gateway web interface as an administrator.
2. On the **ADVANCED > SSL Inspection** page, set **Enable SSL Inspection** to Yes.
3. In the **Inspected Domains** field, enter Facebook.com and click **Add**.
4. Install an SSL certificate as described in step 1-4 above.

Step 2. Create the policy:

1. On the **BLOCK/ACCEPT > Exceptions** page, in the **Add Exceptions** section, select the *Block Action*. See **Figure 2** below.
Select the type of users you want to allow (*Authenticated, Local Group*, etc.) in the **Applies To** field. In this example we've created a group called *Students* from the **USERS/ GROUPS > Local Groups** page, and here, we have selected that group for **Applies To**.
2. Select *URL Pattern* as the **Exception Type**.
3. Enter `https://www.facebook.com/messages` as the **URL pattern**.
4. There is no need to set a time frame unless you want to allow access to Facebook chat OUTSIDE the hours you're blocking.

Figure 2: Creating a *Block* policy for Facebook chat



5. Select the **Protocol** as **HTTPS**. Enter a message if you like to describe what the policy is about.
6. Configure policy alerts as needed. In this example, the **Message** field explains that **Policy Alerts** were purposely not enabled.
7. Click **Add**. You have now created your policy.

Figures

1. ExceptionsFacebookApps.jpg
2. ExceptionBlockFacebookChat.jpg

© Barracuda Networks Inc., 2024 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.