How to Configure Malware Protection in the HTTP Proxy

https://campus.barracuda.com/doc/96026346/

The Malware Protection service tightly integrates antivirus software with the Barracuda CloudGen Firewall gateway. Configure the Avira scan engine and enable Advanced Threat Protection (ATP) for content scanning in the Barracuda cloud to reduce the load on the firewall. You can also configure content filtering, content caching, and additional features to optimize file downloads with virus scanning.

Configure the Virus Scanner

When configuring the virus scanner, you can:

- Specify the behavior of local and remote virus scanning.
- Exempt specific files and domains from scanning.
- Limit the size of files that are scanned locally with a big file policy. You can configure a small system (for example Barracuda CloudGen Firewall F100) to scan small files, while sending bigger files to a remote system that is more capable of scanning large files (for example Barracuda CloudGen Firewall F600).

To configure the virus scanner:

1. Verify that you properly created the Virus Scanner service. For more information, see Virus Scanner.
   If the Virus Scanner service runs on the same Barracuda CloudGen Firewall as the HTTP Proxy server or all other services, do not change its service IP addresses. By default, the service listens on 127.0.0.1, which is a loopback IP address. This IP address is predefined in the services that require access to the malware scanning engines.
2. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > HTTP-Proxy > HTTP Proxy Settings**.
3. Click **Lock**.
4. From the **Configuration Mode** menu on the left, select **Advanced View**.
5. From the **Configuration** menu on the left, select **Malware Protection**.
6. To enable virus scanning, select **Yes** from the **Enable Virus Scanning** list.
7. From the **Scanner Location** list, select one of the following options to specify on which system the Virus Scanner service is running:
   - **Local** – Select if the Virus Scanner service is running locally on the Barracuda CloudGen Firewall.
   - **Remote** – Select if the Virus Scanner Service is running on another Barracuda CloudGen Firewall. In the **Remote Scanner IP** field, enter the IP address of the remote service which is used for virus scanning.
8. In the **Virus Scan Exceptions** section, you can specify which files and domains should not be

scanned. Click **Edit** and then specify the following settings:
  - **MIME Types** – In this table, add MIME types that are excepted from being scanned and thus are delivered directly to the web browser. Wildcards and regular expressions are allowed. Examples:
    - `x-rpm$` – Excludes all files with "rpm" at the end of the string.
    - `[mp]` – Excludes all files that contain the characters "m" or "p".
    - `audio/mpeg` – Excludes all MPEG files.
  - **Domains** – In this table, add the domains that are excepted from being scanned.
  - **Raw** – In this table, you can enter raw Squid configurations.
9. In the **Virus Scan Filter** section, you can specify the MIME types and files suffixes to be scanned. Click **Edit** and then specify the following settings:
  - **Mime Types** – In this table, add MIME types.
  - **File Suffixes** – In this table, add file suffixes.
10. To configure the big file policy:
  1. In the **Big File Watermark (MB)** field, enter the size limit for files that are scanned locally.
  2. From the **Big File Policy** list, select a policy to handle files whose size exceeds the **Big File Watermark (MB)** limit:
    - **Scan** – All files are scanned locally.
    - **Alternative Scanner** – All files that are bigger than the watermark size are sent to a remote scanner. In the **Big File Scanner IP (ICAP)** field, enter the IP address of the remote scanner.
    - **Bypass** – All files that are bigger than the watermark size are forwarded to the client without scanning.
11. Click **Send Changes** and **Activate**.

Optimize File Downloads

To optimize file downloads, you can configure these settings:

Data Trickling

Because the virus scanning engine scans files before sending them, there may be a delay when large files are sent, giving users the impression that their download request is unsuccessful. With data trickling, the proxy sends small pieces of data to the client, so that the client does not run into a timeout during virus scanning; however, this data is not scanned. Before configuring data trickling, note the following information:

- When data trickling is enabled and malware is found within a scanned file by the virus scanning engine, the remaining portion of the file is not transmitted. This creates a small, incomplete stub file in the user's download location.
- Trickling of all destinations appears if no special restrictions are defined. The data trickling access control list (ACL) is processed prior to the header trickling ACL.

- Data trickling is not possible with HTTPS downloads over the Secure Web Proxy service.

How to Configure Data Trickling

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > HTTP-Proxy > HTTP Proxy Settings**.
2. Click **Lock**.
3. From the **Configuration** menu on the left, select **Malware Protection**.
4. From the **Enable Trickle Feature** list, select **Yes**.
5. In the **Trickle Size Low Watermark (MB)** field, enter the minimum size for files that must be trickled.
6. In the **Trickle Period** field, enter the delay in seconds between trickle packets.
7. To edit more detailed trickling settings:
    1. Expand the **Configuration Mode** menu in the left navigate pane and click **Switch to Advanced**.
    2. Click **Set** or **Edit** next to **Advanced Trickle Settings**. For more details about these settings, see Malware Protection Settings.
    3. Click **OK**.
8. Click **Send Changes** and **Activate**.

Pop-Up Progress Bar

The pop-up progress bar displays the status of file downloads. The progress bar can be configured for web browsers such as Internet Explorer, Firefox, or Opera. Additionally, only certain MIME types are handled by the proxy progress bar. Granular configurations let you fine-tune exceptions for the progress bar. You can also configure HTML templates for the progress bar. Before configuring the pop-up progress bar, note the following information:

- The progress bar does not work with HTTPS connections or SSL Inspection.
- Supported browsers are Mozilla Firefox 2 and 3, and Microsoft Internet Explorer (IE) 6 at least.
- By default, the progress bar detects the following browsers:
    - Mozilla Firefox
    - Microsoft Internet Explorer (IE)
    - Opera
    - Apple Safari
    - Google Chrome
- When the pop-up progress bar is enabled, no header trickling is performed.
- With some browsers and websites, the progress bar process cannot discriminate between when you click **Save result as** and when you directly click the specified link in the browser window (for example, download areas at www.microsoft.com). This may lead to unexpected behavior where the pop-up progress bar does not display when you directly click the link.
- When a progress popup is opened, the main window is set to blank for IE 6 and 7. The user has to enter a new web address manually or use the back button to return to the previous page. If IE 8 or Firefox is used, the main window displays the page where the download was started automatically. This is done by getting back in the browser history by two steps. Stepping back

two sites is important for download sites where the download is started via javascript or HTTP redirects. Otherwise the download would start in an endless loop. On the other hand it may happen that the main browser window is set to the last opened web site.

To configure the progress bar:

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > HTTP-Proxy > HTTP Proxy Settings**.
2. Click **Lock**.
3. From the **Configuration** menu on the left, select **Malware Protection**.
4. Click **Edit** next to **Progress Bar Policy**.
5. In the **Popup Bar Policy** window, specify the settings for the progress bar and then click **OK**. For more details about these settings, see Malware Protection Settings.
   When you configure the **Progress Template** and **Unknown Downloads Template**, it is recommended that you start with the default template. Incorrect settings can seriously damage your pop-up progress bar.
6. Click **Send Changes** and **Activate**.

MP3 and PDF File Downloads

With the progress bar, there may be some issues with downloading MP3 and PDF files. To enable the downloading of these files types, select **Yes** from the **Show Save Button** list in the pop-up progress bar settings. To download MP3 and PDF files with the progress bar:

1. Right-click **Save target as** and select **Save Target As**.
2. Browse to the folder where the file should be saved and click **Save**.

Configure Content Filtering and Caching

For content filtering and caching, you can configure these settings:

Content Filtering

To protect clients and servers from Internet attacks and threats, enable content filtering.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > HTTP-Proxy > HTTP Proxy Settings**.
2. From the **Configuration** menu in the left navigation pane, select **Web Filter**.
3. From the **Enable Content Filtering** list, select **Yes**.
4. Click **Send Changes** and **Activate**.

Content Scanning in the Cloud

For content scanning in the cloud, enable the Barracuda Web Security Service .

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > HTTP-Proxy > HTTP Proxy Settings**.
2. Click **Lock**.
3. In the **Barracuda Web Security** section, select **Yes** from the **Enable Barracuda Web Security** list.
4. Next to **Web Security Settings**, click **Edit**.
5. Specify your Barracuda Web Security Service connection settings. For more details about these settings, see the Malware Protection Settings section.
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Cache Manager

The integrated proxy service of the Barracuda CloudGen Firewall is based on the Squid Web Proxy Cache. The labeling of configuration parameters in the Barracuda CloudGen Firewall follows the labeling applied in the Squid Web Proxy Cache. If you are not familiar with the labels used for Squid proxy configuration, refer to the official Squid documentation at www.squid-cache.org.

To enable the cache manager:

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > HTTP-Proxy > HTTP Proxy Settings**.
2. Click **Lock**.
3. In the left navigation pane, expand **Configuration Mode** and click **Switch to Advanced View**.
4. From the **Configuration** menu in the left navigation pane, select **Advanced**.
5. From the **Enable Cache Manager** list, select **Yes**.
6. If required, enter your login details in the **Cache Manager Password** section.
   The password can consist of small and capital characters, numbers, and non alpha-numeric symbols, except the hash sign (#).
7. Click **Send Changes** and **Activate**.

Fail Cache

To configure the fail cache:

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > HTTP-Proxy > HTTP Proxy Settings**.
2. Click **Lock**.
3. In the **Fail Cache Configuration** section, specify the following settings:
   - **Enable Fail Cache** – Select **Yes**.
   - **Keep Fail Cache Entries (d)** – Enter the maximum number of entries for the HTTP Proxy fail cache.
4. Click **Send Changes** and **Activate**.

Malware Protection Settings

These sections provide more detailed descriptions of the settings that you configure for malware protection:

Data Trickling Settings

This table provides more detailed descriptions of the settings that you can configure in Data Trickling. The HTTP Proxy service supports data trickling and header trickling. Data trickling is the recommended trickling mechanism.

Setting	Description
Enable Data Trickle	Select **Yes** to enable data trickling.
Initial Data Trickle Size	The size of the first trickle packet.
Data Trickle Size	The size of subsequent data trickle packets. In most cases, you do not need to change this setting.
Data Trickle Buffer Size	The overall size of the trickle buffer. Note that a large buffer size increases memory usage.
Data Trickle Dest. Domains	In this table, can add domains to which data trickling is restricted. If you leave this table and the **Data Trickle URL Pattern** table empty, data trickling is not restricted.
Data Trickle URL Pattern	In this table, add URL patterns to which data trickling is restricted. If you leave this table and the **Data Trickle Dest. Domains** table empty, data trickling is not restricted.

Progress Bar Settings

This table provides more detailed descriptions of the settings that you can configure in Pop-Up Progress Bar.

Setting	Description
Enable Progress Popups	Select **Yes** to enable the pop-up progress bar.

Browsers	In this table, you can edit or add browsers to be detected by the progress bar. For each browser, specify the following settings: • **Detection Regex** – A regular expression which will be applied to the client requests HTTP header for browser evaluation. For example: *Mozilla/.+\(compatible; MSIE 7.+\).** • **ExceptionRegex** – A regular expression which will be applied to the client requests HTTP header for actions where the progress bar should not open, such as when a user right-clicks a URL and clicks **Save target as**. Most browsers are sending a slightly different request in such a case. For example: *Accept: */** • **Show Save Button** – If the download should not be fetched automatically but the **Save file as** option should open instead, select *Yes*.
MIME-Types	In this table, add MIME types for which the progress bar should display. The default settings already contain commonly used MIME types. Usually, the progress bar should not be displayed for MIME types that are handed over to a browser plug-in (e.g. application/pdf) because users expect these MIME types to open automatically. If the browser and the plug-in both try to download the requested file, the download request will fail (usually for the plug-in) because the temporary link is only valid for a single download. To add text and plain types, enter: *text/plain**
Popup After	If you are using the pop-up progress bar and data trickling, make sure the **Trickle Period** setting for data trickling has a smaller value than the **Popup After** setting.
Excluded Domains	In this table, add domains for which the progress bar must never be used (e.g. domains that provide automated downloads). Only enter domains and subdomains (until the first slash (/) in the path).
Excluded Sources	In this table, add a list of sources from which the progress bar must never be used.
Custom Template Logo	To import a logo for display in Internet Explorer, click **Ex/Import**. To be able to display a logo in Internet Explorer, disable the bypass proxy server for local addresses in the Internet Explorer's proxy settings.
Progress Template	In this field, you can enter an HTML template for your customized download progress pop-up window.
Unknown Downloads Template	In this field, you can enter an HTML template that is displayed when users try to access a temporary URL that is no longer available.