How to Configure ATP in the HTTP Proxy

https://campus.barracuda.com/doc/96026343/

Configure when and which types of files are uploaded to the Barracuda ATP Cloud for traffic passing through the HTTP proxy service. Users will receive downloaded files immediately. When files with a risk factor higher than the define risk threshold are detected, the associated users and/or IP addresses are placed in quarantine. Files allow listed in the Malware Protection configuration of the HTTP Proxy are never scanned by ATP.

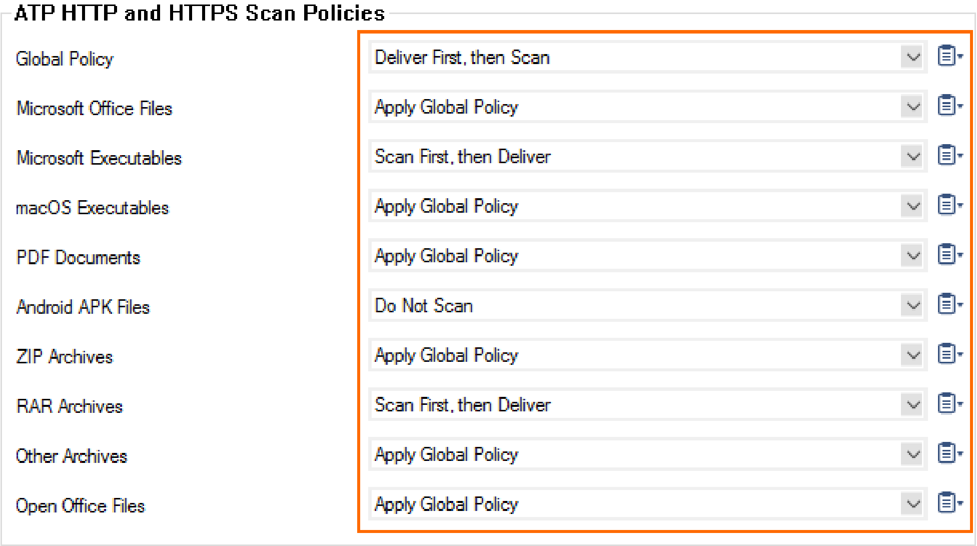
Before You Begin

- You must have an Advanced Threat Protection license subscription. For more information, see CloudGen Firewall Licensing.
- Verify that you have configured a **System Notification Email** address. For more information, see How to Configure the System Email Notification Address.
- Verify that you have enabled malware protection for the HTTP proxy. For more information, see How to Configure Malware Protection in the HTTP Proxy.
- Verify that all file types you want to scan with ATP are not listed in the Virus Scan Exceptions. For more information, see How to Configure Malware Protection in the HTTP Proxy.

Step 1. Configure ATP Scan Policy and Risk Threshold

Configure the ATP scan policy to determine if the user will have to wait for scanning to complete before the file is forwarded.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Virus Scanner > Virus Scanner Settings**.
2. Click **Lock**.
3. In the left menu, click **ATP**.
4. In the **ATP HTTP and HTTPS Scan Policies** section, select the **Global Policy**:
   - **Deliver First, then Scan**
   - **Scan First, then Deliver**
5. If needed, set the individual scan policies for each file type:
   - **Apply Global Policy (default)**
   - **Do Not Scan** – This file type is not scanned. It is immediately forwarded to the user.
   - **Deliver First, then Scan** – The user receives the file immediately. If malware is found, the quarantine policy applies.
   - **Scan First, then Deliver** – The users are redirected while they wait for the scan to finish. Malicious files are not delivered to the user.



ATP HTTP and HTTPS Scan Policies

Global Policy	Deliver First, then Scan
Microsoft Office Files	Apply Global Policy
Microsoft Executables	Scan First, then Deliver
macOS Executables	Apply Global Policy
PDF Documents	Apply Global Policy
Android APK Files	Do Not Scan
ZIP Archives	Apply Global Policy
RAR Archives	Scan First, then Deliver
Other Archives	Apply Global Policy
Open Office Files	Apply Global Policy

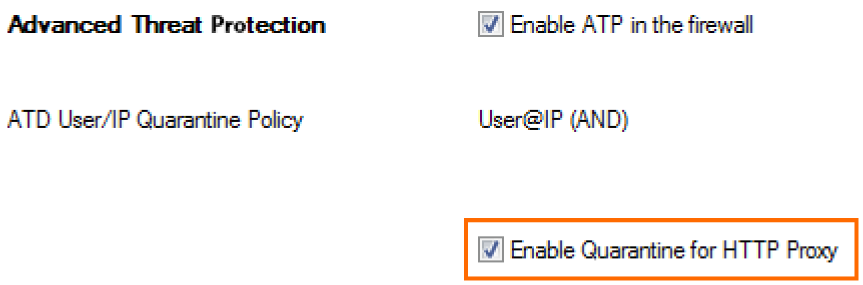
6. In the **ATP Threats** section, select the **Block Threats** policy:
    - **High Only** – Files classified as high risk are blocked.
    - **High and Medium (Default)** – Files classified as high or medium risk are blocked.
    - **High, Medium and Low** – Files classified as high, medium, or low risk are blocked. Only files with classification **None** are allowed.
7. Set **Send Notification Emails** to:
    - **No** – No notification emails are sent when malware is found.
    - **To System-Settings Address (Default)** – A notification email is sent to the system notification email address. For more information, see How to Configure System Email Notifications.
    - **To Explicit Address** – Enter the **Explicit Email Address** and **Explicit SMTP Server** the Barracuda CloudGen Firewall will use to send the notification emails.
8. (optional) Set the **ATP Data Retention** (in days). These values determine how long files are kept on the system before they are deleted.
9. Click **Send Changes** and **Activate**.

Step 2. Enable ATP in the Firewall, and Configure Automatic Quarantine Policy and Quarantine for the HTTP Proxy

You must enable ATP in the security policy of the forwarding firewall and enable the quarantine for the HTTP proxy.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Security Policy**.
2. Click **Lock**.
3. In the **Advanced Threat Protection** section, click **Enable ATP in the firewall**.
4. Select the **Automatic Block List Policy**:
    - **No auto quarantining** – No connections are blocked.

   - **User only** – All connections by the infected user are blocked regardless of the source IP address.
   - **User@IP (AND)** – All connections originating from the infected source IP address and the infected user are blocked.
   - **User, IP (OR)** – All connections coming from the infected source IP address and/or the infected user are blocked.
5. Select the **Enable Quarantine for HTTP Proxy** check box.



Advanced Threat Protection	☑ Enable ATP in the firewall
ATD User/IP Quarantine Policy	User@IP (AND)
	☑ Enable Quarantine for HTTP Proxy

6. Click **Send Changes** and **Activate**.

Quarantine Management

Manually Placing a User and/or IP Address in Quarantine

If you are not using automatic quarantine policy, the administrator can also place a user in quarantine manually.

1. Go to **FIREWALL > ATP**.
2. Click the **Scanned Files** tab.
3. Double-click the malicious file. The **ATP File Details** window opens.
4. In the **File Download** section, select the user in the list.
5. Click **Quarantine**. The **Select Quarantine Policy** window opens.
6. Select the **Quarantine Policy**:
   - **Block only Users** – Place the user in quarantine, but not the source IP address.
   - **Block only IP Addresses** – Place the IP address in quarantine, but not the user.
   - **Block User @ IP (logic AND)** – Place user@IP address in quarantine. Both user and IP address must match.
   - **Block User, IP (logic OR)** – Place the user and IP address in quarantine. Either user or IP address must match.
7. Click **OK**.

The user and/or IP address are now in the quarantine network object (Click the **Quarantine** tab to verify). Create an access rule using the ATP User Quarantine network object to block connections to and from the infected users and/or IP addresses.

Removing a User and/or IP Address from Quarantine

1. Go to **FIREWALL > ATP**.
2. Click the **Quarantine Tab**.
3. Right-click the user or IP address you want to remove from quarantine.
4. Click **Remove from Quarantine**.

The user and/or IP address is removed from the quarantine network object.

Download a Scan Report

You can download a short or long version of scan report.

1. Go to **FIREWALL > ATP**.
2. Double-click the scanned file.
3. Click **Download Report** and select the report type:
   - **Summary Report**
   - **Full Report**

Figures