Advanced Threat Protection (ATP)

https://campus.barracuda.com/doc/98210343/

Advanced Threat Protection offers protection against advanced malware, zero-day exploits, and targeted attacks, which are not detected by the virus scanner or intrusion prevention system. ATP analyzes files in the Barracuda ATP cloud and assigns a risk score. Local ATP policies then determine how files with a high, medium, or low risk scores are handled. You can configure email notification of the administrator and/or enable one of the automatic blocklisting policies. To check local files, you also have the option to manually upload a file via Barracuda Firewall Admin.

ATP can be used for HTTP, HTTPS, FTP, FTPS, SMTP, and SMTPS traffic in combination with the firewall service on a per access rule basis or for HTTP and HTTPS with the HTTP proxy service. You must have Energize Updates and Advanced Threat Protection subscriptions for each CloudGen Firewall that uses ATP. Depending on the model size there are burst (number of files uploaded per minute) and monthly limits on the number of files you can upload to the Barracuda ATP cloud. If you exceed this limit, files will not be uploaded and either passed through or blocked according to the fail policy of the virus scanner. For more information, see Licensing.

To receive more information, you can download a short or detailed report for every file analyzed in the Barracuda ATP cloud. The report includes details on the file classification and file behavior.

The following file types are scanned by the Barracuda ATP Cloud:

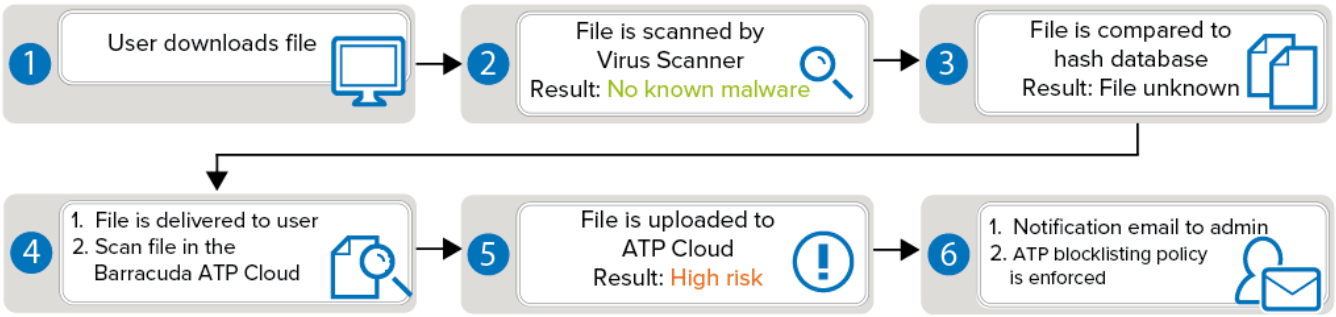
- **Microsoft Office files** – doc, docx ,ppt, pps, pptx, ppsx, xls, xlsx
- **OpenOffice** – rtf, open office document extensions
- **Microsoft executables** – exe, msi, class, wsf
- **macOS executables**
- **PDF documents** – pdf
- **Android APK files** – apk
- **ZIP Archives** – 7z, lzh, bz, bz2, chm, cab, zip
- **RAR Archives** – rar4 and rar5
- **TAR Archives** – tar
- **GZ Content** – Content compressed with gzip
- **Javascript** – Manual scan

ATP File Scanning

The Virus Scanner scans files up to the **Large File Watermark** size set in the Security Policy. If no malware is found by the Virus Scanner and the file size is 10 MB or smaller, a hash of the file is created. Files larger than 10 MB are not processed by ATP. The hash of the file is then compared to the local cache and online hash database in the Barracuda ATP Cloud. If the file was previously scanned, it is immediately blocked or forwarded, depending on the result of the previous scan and

your local **ATP Block Threshold**. If the hash of the file is unknown, the **ATP Scan policy** set for that file type is executed.

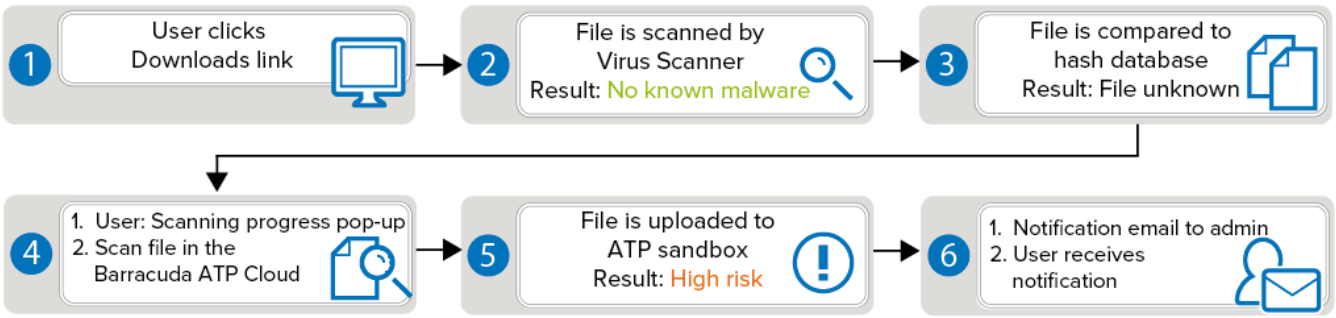
Deliver first, then Scan:



This ATP scan policy is available for HTTP(S), FTP(S), and SMTP(S) connections.The user receives the downloaded file immediately after the virus scan and the hash DB lookup. Simultaneously, the file is uploaded to the Barracuda ATP Threat Cloud and emulated in a virtual sandbox. Depending on the behavior of the file, it is assigned a threat level and the result transmitted to the firewall. If the threat level exceeds the ATP threat level threshold, an email notification is sent to the administrator and the automatic blocklisting policy enforced. This policy is least disruptive to users because they receive the file immediately and are only blocked if the file is a threat. It is also less secure because potential malware can bypass detection for the time period it takes to upload and emulate the file.

For more information, see How to Configure ATP in the Firewall.

Scan first, then Deliver:



This mode is supported for HTTP(S) and SMTP(S). The user must wait for ATP to finish scanning the file. In the interim, a browser window informs the user of the scan in progress. When the scan is complete and the file is not classified higher than the **ATP Block Threat Threshold**, the download begins. This scan policy offers higher security at the expense of the user having to wait for sandboxing of the file to finish. Detected malware never enters your network.

Limitations for Scan First, Then Deliver

Scan first, then deliver may break websites using AJAX for file retrieval. The file is scanned, but it is not possible to show the scan-in-progress page with the download button for the scanned file, and so the scanned file is never delivered to the client. Some browsers download the scan-in-progress page instead of the file. Scanned files can be retrieved during the **ATP Data Retention** period by the firewall admin directly in the **/var/phion/virscan/quarantine** or **/var/phion/virscan/virusfree** directories on the firewall.

Websites utilizing JavaScript or hidden frames to download files, can have issues with the scan first, then deliver setting. It can happen that downloads are not delivered to the user. An example for this behavior is download of the GoToMeeting application.

For more information, see How to Configure ATP in the Firewall.

Automatic Blocklisting Policy

Automatic blocklisting fills a dynamic network object with the infected users and/or IP addresses. You must create an access rule using that network object to block these users and IP addresses. Management access to the firewall is exempt from the blocklist policy. Automatic blocklisting is not available for SMTP or SMTPS connections.

- **No auto blocklisting** – 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. If a different user logs in to the infected computer, all connections are allowed because only one criteria, the source IP address, matches. If the username for the connection is unknown, only the IP address is blocked.
- **User, IP (OR)** – All connections coming from the infected source IP address and/or the infected user are blocked. If a different user logs into the infected computer, all connections are blocked because the source IP is blocked. If the infected user logs in to a different workstation, connections are blocked because the infected user is blocked.

Quarantine Block Page

To inform blocklisted users, you can add a **Transparent Redirect on Port 80** to the Block or Deny access rule. When the user tries to access HTTP content, the connection is automatically redirected to the quarantine page. The quarantine page can be customized to fit your needs.

For more information, see How to Configure Custom Block Pages and Texts.

Risk Scores

The ATP service classifies all files in one of four categories:

- **High** – Files classified as high risk exhibit behavior normally only found in malware.
- **Medium** – Files classified as medium risk pose a potential risk.
- **Low** – Files classified as low risk are considered to be harmless. Some residual risk remains.
- **None** – No suspicious activity was detected.

Reporting

You can view a short or detailed report on the scan results for every file uploaded to the Barracuda ATP Cloud.

For more information, see ATP Tab.

Manual File Upload

If you want to manually check a local file using ATP, you can use Barracuda Firewall Admin to upload the file to the ATP cloud. After the file has been scanned, you are mailed a report with the scan results.

For more information, see How to Manually Upload Files to ATP.

Figures

1. atp_deliver_scan.png
2. atp_scan_deliver.png