Advanced Threat Protection (ATP/ATD)

https://campus.barracuda.com/doc/49745918/

Advanced Threat Protection (ATP), also known as Advanced Threat Detection (ATD), 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 notifications of the administrator and/or enable one of the automatic blacklisting policies. To check local files, you can also manually upload a file. ATP can be used for HTTP, HTTPS, FTP, SMTP, and SMTPS traffic in combination with the firewall service on a per access rule basis.

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

- Microsoft Office files
- Microsoft Executables
- PDF documents
- Android APK files
- ZIP archives
- RAR archives

Licensing

The following subscriptions are required to use ATP in the firewall:

- **Energize Updates** – Needed for virus scanner pattern updates.
- **Web Security** – Required for the virus scanning service.
- **Advanced Threat Protection** – This subscription is required to use ATP.

You must have Energize Updates, Web Security and Advanced Threat Protection subscriptions for each X-Series Firewall using 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.

Model	Burst limit (files/min)	Files per month
X50, X51, X100, X101, X200	5	108,000
X300	10	216,000
X400	15	324,000
X600	25	540,000

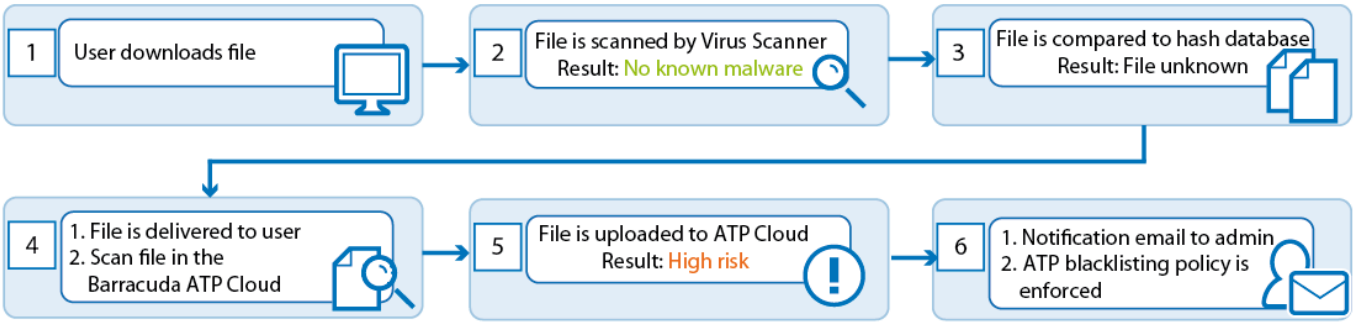
If you exceed the burst limit (files/min), files will be queued and uploaded at the beginning of the next

minute. If you exceed the monthly limit, files will not be uploaded. Instead, they will be either passed through or blocked according to the fail policy of the virus scanner.

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 8 MB or smaller, a hash of the file is created. Files larger than 8 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.

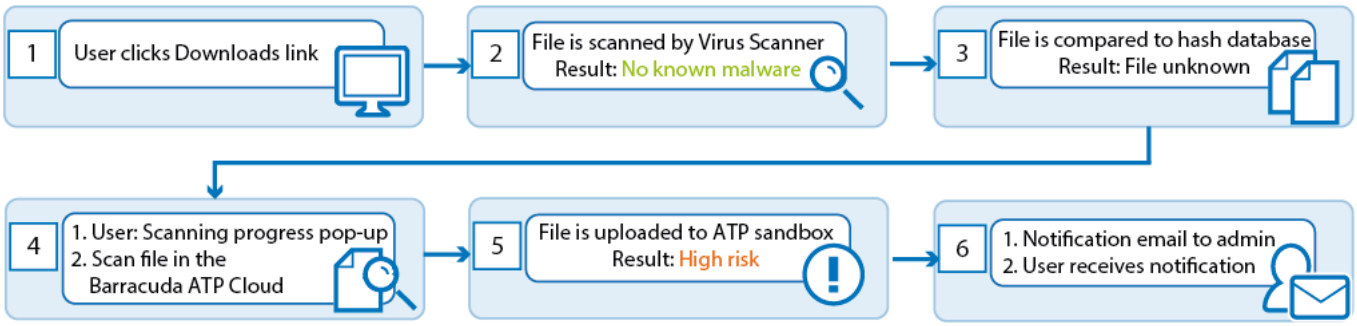
Deliver first, then scan:



This ATP scan policy takes effect when **Deliver before scan complete** is enabled and is available for HTTP and HTTPS. FTP, SMTP, and SMTPS 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 blacklisting policy is 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 ATP scan policy takes effect when **Deliver before scan complete** is disabled and is supported for HTTP and HTTPS only. 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.

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

Automatic Blacklisting

Configuring a quarantine policy allows automatic blacklisting of connections by the infected source. Automatic blacklisting 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 blacklist policy. Automatic blacklisting is not available for SMTP or SMTPS connections.

- **No automatic blacklisting** – No connections are blocked.
- **User** – All connections by the infected user are blocked regardless of the source IP address.
- **IP** – All connections by the infected source IP address are blocked regardless of the user.
- **User AND IP** – 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 OR IP** – 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.

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

Quarantine Block Page

To inform blacklisted users, you can add a **HTTP Block Page** to the *Block* 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 Custom Block Pages.

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 How to Configure ATP in the Firewall.

Figures

1. atp_deliver_then_scan.png
2. atp_scan_then_deliver.png