

## Advanced Threat Detection (ATD)

<https://campus.barracuda.com/doc/43847122/>

Advanced threat detection offers protection against advanced malware, zero-day exploits and targeted attacks, which are not detected by the virus scanner or intrusion prevention system. ATD analyzes files in the Barracuda ATD cloud and assigns a risk score. Local ATD 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 blacklisting policies. To check local files you also have the option to manually upload a file via NG Admin.

ATD can be used for HTTP and HTTPS traffic in combination with the [firewall service on a per access rule basis](#) or with the [HTTP proxy service](#). You must have energize updates, malware and advanced threat detection subscriptions for each NG Firewall using ATD. 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 ATD 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 ATD cloud. The report includes details on the file classification and file behavior.

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

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

### In this article

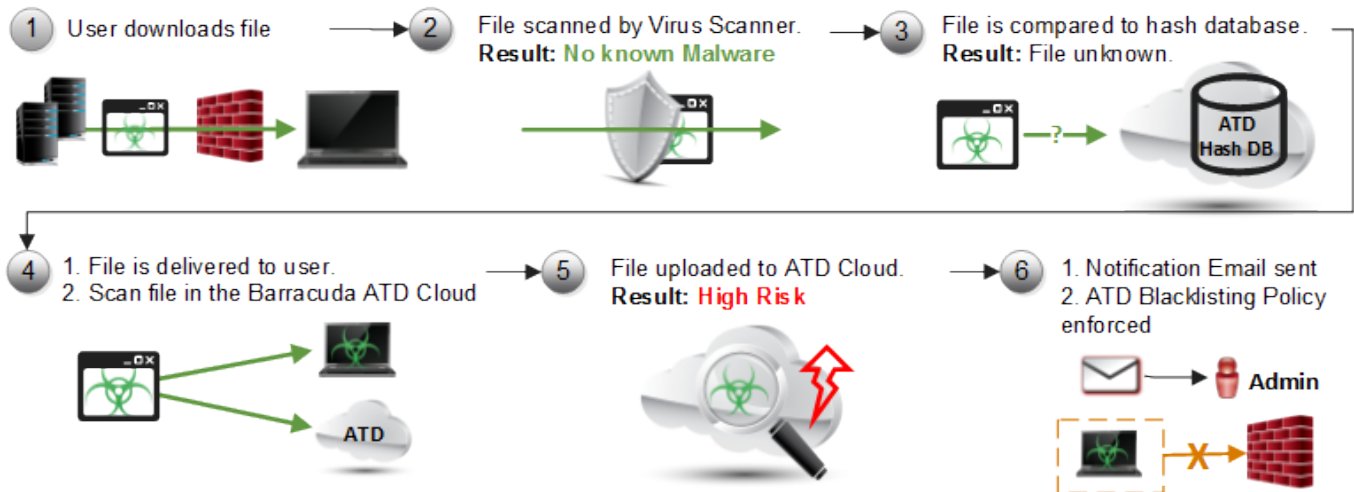
### ATD File Scanning

---

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 ATD. The hash of the file is then compared to the local cache and online hash database in the Barracuda ATD Cloud. If the file was previously scanned, it is immediately blocked or forwarded, depending on the result of the previous scan and your local **ATD**

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

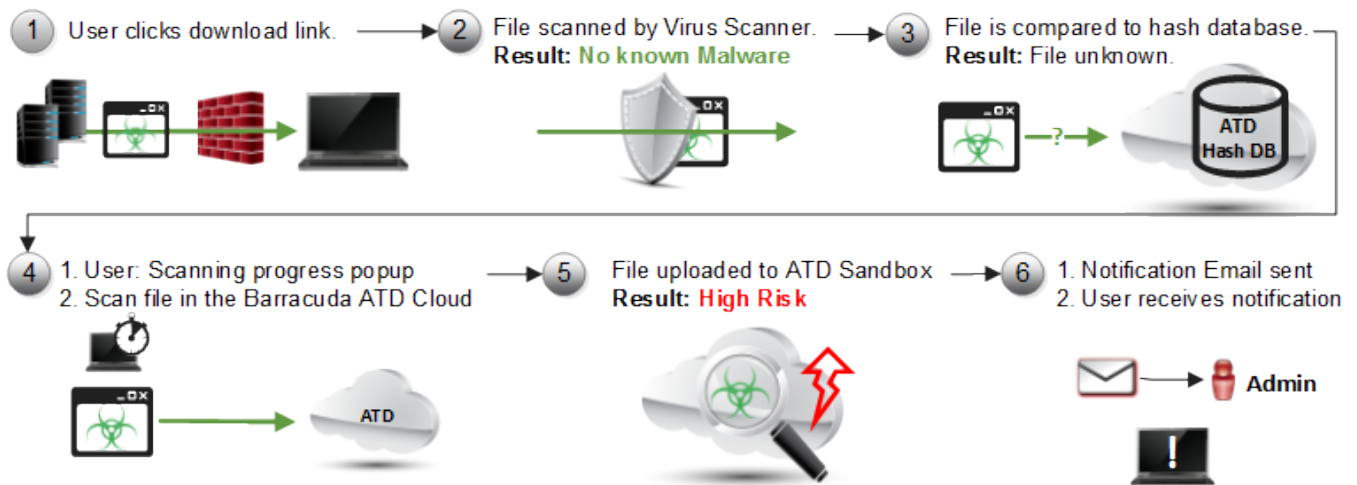
#### Deliver first, then Scan



The user receives the downloaded file immediately after the virus scan and the hash DB lookup. Simultaneously the file is uploaded to the Barracuda ATD 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 Barracuda NG Firewall. If the threat level exceeds the ATD threat level threshold, an email notification is sent to the administrator and the automatic blacklisting policy enforced. This policy is least disruptive to the user, as he receives the file immediately and is only blocked if the file is a threat. It is also less secure as potential malware can bypass detection for the time period it takes to upload and emulate the file.

For more information, see [How to Configure ATD in the Firewall](#).

#### Scan first, then Deliver



The user has to wait for ATD 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 **ATD 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 ATD in the Firewall](#).

## Automatic Blacklisting Policy

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 Barracuda NG Firewall is exempt from the blacklist policy.

- **No auto blacklisting** – 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, as 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 different workstation, connections are blocked, because the infected user is blocked.

---

## Quarantine Block Page

---

To inform blacklisted 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](#).

---

## Risk Scores

---

The ATD 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 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 ATD Cloud.

For more information, see [ATD Page](#).

---

## Manual File upload

---

If you want to manually check a local file using ATD, you can use NG Admin to upload the file to the ATD 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 ATD](#).

## Figures

1. ATD\_DeliverFirstThenScan.png
2. ATD\_ScanFirstThenDeliver.png

© Barracuda Networks Inc., 2019 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.