Understanding Advanced Threat Protection

https://campus.barracuda.com/doc/96023015/

The Advanced Threat Protection (ATP) service analyzes inbound email attachments with most file types and publicly accessible direct download links in a separate, secured cloud environment, detecting new threats and determining whether to block such messages. ATP offers protection against advanced malware, zero-day exploits, and targeted attacks, such as phishing, not detected by Email Gateway Defense virus scanning features. Enable ATP on the **ATP Settings** page.

When ATP determines an attachment or publicly accessible direct download link contains a threat and blocks the message, review the ATP Report before determining whether to deliver the message. See Advanced Threat Protection Reports and Understanding Advanced Threat Protection Reports for more information.

If you make setting changes, allow a few minutes for the changes to take effect.

Advanced Threat Protection Options

Configure policies on the **Inbound Settings > Content Policies** page, and specify how and when attachments are scanned on the **ATP Settings** page.

Deliver First, then Scan

When selected, the ATP service attempts to scan the mail in real time. If the ATP scan completes in real time and a malicious artifact is detected, the message is blocked and is not delivered. If the ATP scan does not complete in real time, the message is delivered; if the ATP service determines the attachment to be suspicious or malware-infected upon completion, the recipient is notified, and if **Notify Admin** is set to **Yes**, an email alert is sent to the specified admin address.

Figure 1. Scan is Complete in Real Time; no Threat Detected.

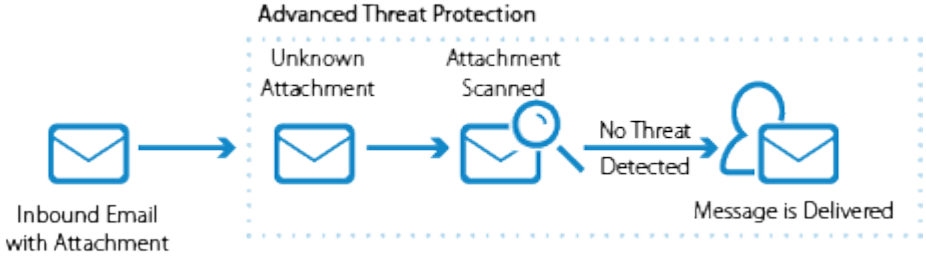


Figure 2. Mail is Delivered Before Scan Complete; Threat Detected.

This option does not delay email processing, however, the email recipient can potentially open an infected attachment.

Scan First, then Deliver

When selected, the ATP service scans new messages with attachments before delivery. If a malicious artifact is detected in an attachment, or the attachment is a known threat, the message is blocked, otherwise, the message is delivered to the recipient.

This option provides more security and prevents the email recipient from opening infected attachments. These messages appear in the Message log and **Pending Scan** displays in the **Reason** column. The sending mail server must retry until the scan is complete and no malicious artifact is detected in the attachment, at which point the message is delivered. Note that messages with attachments may be temporarily deferred while queued for scanning. If the message status is deferred for more than two hours, the message is quarantined.

Figure 3. Attachment is Recognized as a Known Threat.

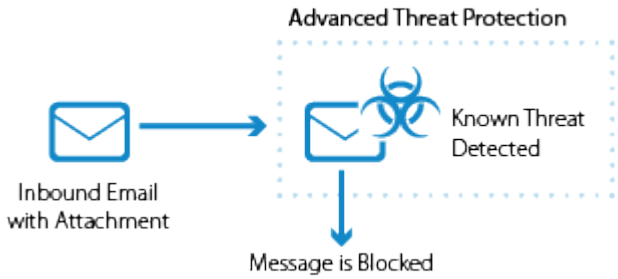


Figure 4. Attachment is Scanned and Determined to be Suspicious.

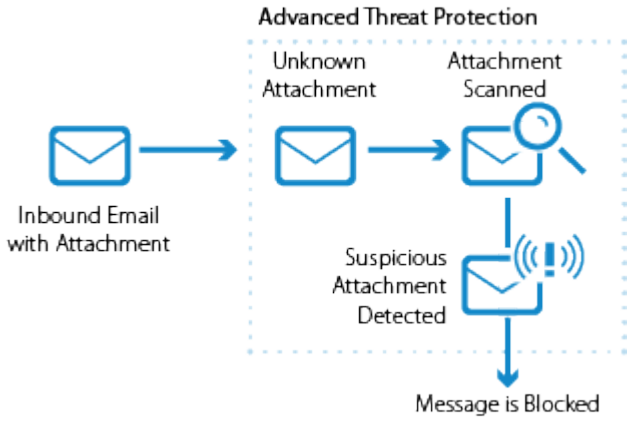
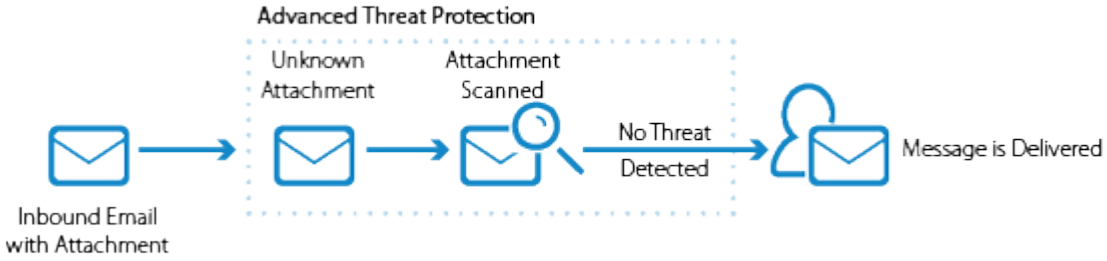


Figure 5. No Threat Detected in Attachment.



Advanced Threat Protection Disabled

When set to **No**, ATP is disabled.

Advanced Threat Protection Exemptions

When ATP is set to either **Deliver First, then Scan** or **Scan First, then Deliver**, you can exempt sender email addresses, sender domains, recipient email addresses, recipient domains, or sender IP addresses from ATP scanning in the **ATP Exemptions** section on the **ATP Settings** page.

Attachments from exempted entries are not sent to the ATP cloud. Note that these exemptions apply to *ATP scanning only* and do not apply to Email Gateway Defense virus scanning.

Scanned File Types

Table 1 lists the common file types scanned by the ATP service. Note that this is not an extensive list.

Table 1.

File Type	File Extension
Adobe Acrobat	**.pdf**
MS Office	**.doc, .ppt, .xls, .mdb, .docx, .ppx, .xlsx**
Executable	**.exe**
Windows Cabinet File	**.cab**
DOS Batch	**.bat**
HTML	**.htm, html**
iCalendar	**.ics**
Rich Text Format	**.rtf**
Android Package Kit	**.apk**
ZIP	**.zip**
TAR	**.tar**
Java Archive	**.jar**
Javascript	**.js**

Administrator Notification

When **Deliver First, then Scan** is selected, select **Yes** for **Notify Admin** to notify the administrator when a malicious artifact is detected by the ATP service in a scanned attachment. The email notification includes the sender, recipient, attachment type, and detected malware. Enter the admin email address in the **ATP Notification Email** field address. Infected attachments are listed in the **ATP Log**.

User Notification

If the ATP service determines an attachment is suspicious or malware-infected, the recipient is notified, and the Message Log displays the action as **Advanced Threat Protection**.

Additionally, the Message Log displays: **Envelope From: no-reply@barracudanetworks.com**

ATP Exemptions

When ATP is set to either **Deliver First, then Scan** or **Scan First, then Deliver**, you can exempt sender email addresses, sender domains, recipient email addresses, recipient domains, or sender IP addresses from ATP scanning. Attachments from exempted entries are not sent to the ATP cloud. Note that these exemptions apply to *ATP scanning only* and do not apply to Email Gateway Defense virus scanning. Note that the exemption is for the envelope from address or envelope from domain. To add an exemption by "envelope from" address or "envelope from" domain:

1. In the **Exemptions by Email Address / Domains** section, enter the email address or domain in the **Exemptions** field.
2. Select **Sender** or **Recipient**.
3. Optionally, enter a **Comment** for the exemption.
4. Click **Add**; the exemption displays in the list.

Message Log

Messages blocked or deferred by the ATP service are listed in the **Message Log** with the following codes listed in the **Reason** column:

- **Advanced Threat Protection** – Message is blocked by the ATP service due to an infected attachment.
- **Pending Scan** (**Scan First, then Deliver** enabled) – Message is deferred while the attachment is scanned. The sending mail server must retry until the scan is complete. Once complete, if no malicious artifact is detected, the message is delivered.
- **ATP Service Unavailable** – Message is deferred because the ATP service is temporarily unavailable. The message is retried and, when the scan is complete and if no malicious artifact is detected, the message is delivered.

View ATP Statistics

The **Dashboard** page displays statistics of scanned attachments determined to be infected by the ATP service.

Deferred Delivery

If the message is deferred, the sending mail server must retry the deferred message. Note the following events that can occur:

- The sending mail server retries the deferred message. If the ATP scan completes, the message is delivered or blocked.
- The sending mail server retries the deferred message for longer than 2 hours. If the pending ATP scan does not complete within that time period, the message is quarantined.
- The sending mail server does not retry the deferred message. The message can be downloaded by the admin and sent as an attachment to the recipient.

If a message scanned by ATP is quarantined or blocked (for example, ATP determines the message attachment is suspicious), the admin can select to deliver the message.

Determine Whether to Deliver Message

1. Log into Email Gateway Defense as the administrator, and go to **Overview > Message Log**.
2. Set message filters and search criteria as needed, and click **Search**.
3. Messages blocked by ATP display as **Not Delivered**.
4. Click on the message, and in the reading pane, click **ATP Reports**.
5. The **Email Delivery Warning** dialog box displays a list of attachments, one or more of which is suspected of being **Infected**. If you want to deliver the email and the associated attachments, first review the report for each attachment.
6. Click **View Report** for the suspicious attachment, and review the report details.
7. Repeat *step 6* for each attachment.
8. Once you review all attachments, and if you determine you want to deliver the email and the associated attachments, review and accept the disclaimer, and click **Deliver** in the **Email Delivery Warning** dialog box.
9. If the message is delivered successfully, the **Delivery Status** changes to **Delivered**. If the mail cannot be delivered, this is reflected as a notice in your browser window and the **Delivery Status** does not change.

Figures

1. ATPRealTime.png
2. ATPNotify.png
3. ATPKnownThreat.png
4. ATPUnknownAttachment.png
5. ATPMsgDelivered.png