Virus Scanning and ATP in the Firewall

https://campus.barracuda.com/doc/48202982/

The Barracuda NextGen Firewall F-Series can transparently scan HTTP, HTTPS, FTP, SMTP, and SMTPS traffic passing through the Forwarding Firewall service for malware. For in-depth scanning of more advanced malware for which there are no virus scanner patterns available, the F-Series Firewall can also scan traffic using Advanced Threat Protection. The following subscriptions are required to use the Virus Scanner and ATP in the firewall:

- **Energize Updates** – Required for Virus Scanner pattern updates.
- **Malware** or **Web Security** – Required for the Virus Scanner service.
- **Advanced Threat Protection** – To use ATP, both Energize Updates and either the Malware or Web Security Service subscription are required.

Virus Scanner in the Firewall for Web Traffic

To scan HTTP and HTTPS traffic for malware, configure an access rule to match your web traffic and enable Application Control, SSL Interception (optional), and the Virus Scanner. If malware is detected, the file is discarded and the user is redirected to a customizable block page. HTTPS connections can be scanned only if SSL Interception is enabled.

For more information, see How to Configure Virus Scanning in the Firewall for Web Traffic.

Virus Scanner in the Firewall for FTP

To scan FTP traffic for malware, configure an access rule to match your web traffic and enable Application Control, the Virus Scanner, and File Content Scan (optional). Since the FTP protocol does not include MIME-type information, all files are scanned. If malware is detected, the file is discarded and the file transfer is terminated. Since a local file is created before the transfer starts, the user may see a file with 0 bytes or a small, partially downloaded file if the file is detected as malware.

For more information, see How to Configure Virus Scanning in the Firewall for Web Traffic.

Virus Scanner in the Firewall for SMTP

To scan incoming and outgoing SMTP and SMTPS mail traffic for malware, you must configure mail security in the firewall.

For more information, see Mail Security in the Firewall.

Advanced Threat Protection (ATP) in the Firewall

ATP can be used for HTTP, HTTPS, FTP, SMTP, and SMTPS traffic in combination with the firewall service on a per-access-rule basis. Two modes are available: **scan first, then deliver** and **deliver first, then scan**. When malware is detected in HTTP and FTP traffic, the user/IP address who downloaded the malware is placed in quarantine.

For more information, see Advanced Threat Protection (ATP) and How to Configure ATP in the Firewall.

Default MIME Types

Only the MIME types listed in the Virus Scanner configuration are scanned by the F-Series Firewall. The firewall comes with a preconfigured list **<factory-default-mime-types>** that includes all **application/*** MIME types. To also scan content for which no MIME type is available, add **<no-mime-types>** to the list. To exempt specific MIME types from virus scanning, enter the MIME type with a prepended "!". E.g., **!application/mapi-http**