Virus Scanning and ATP in the Firewall

https://campus.barracuda.com/doc/79463044/

The CloudGen Firewall can transparently scan HTTP(S), FTP(S), POP3(s), and SMTP(S) traffic passing through the firewall. For in-depth scanning of more advanced malware for which there are no virus scanner patterns available, the CloudGen Firewall can also scan traffic using Advanced Threat Protection. The following subscriptions are required to use Virus Scanner and ATP:

- **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(S) traffic for malware, configure an access rule to match your web traffic and enable Application Control, SSL Inspection (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 Inspection 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(S) 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 FTP Traffic.

Virus Scanner in the Firewall Email Traffic

To scan email traffic for malware, you must configure mail security in the firewall. To scan clients sending via SMTP(S) and POP3(S) to servers on the Internet, configure an access rule to match your traffic and enable Application Control, SSL Inspection (optional, but mandatory for SMTPS and POP3S),

and the Virus Scanner. If malware is detected, the file is discarded and the connection is reset.

For more information, see How to Configure Virus Scanning in the Firewall for Outbound SMTP and POP3 Traffic and Mail Security in the Firewall.

Virus Scanner in the Firewall for SMB

To scan SMB traffic, you must first activate Virus Scanning and then create an access rule with activated Application Control so that SMB session related data streams will be forwarded to the Virus engine.

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

Advanced Threat Protection (ATP) in the Firewall

ATP can be used for HTTP(S), FTP(S), POP3(S). and SMTP(S) 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 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-type>** to the list. To exempt specific MIME types from virus scanning, enter the MIME type with a prepended "!". E.g., **!application/mapi-http**

© Barracuda Networks Inc., 2024 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.