Advantages of the Cloud Protection Layer

https://campus.barracuda.com/doc/54853825/

The Barracuda Cloud Protection Layer (CPL) feature of the Barracuda Email Security Gateway is an additional layer of cloud-based protection that blocks threats before they reach your network and prevents phishing and zero day attacks . CPL is available with a current Advanced Threat Protection (ATP) subscription.

Advantages of Using Cloud-Based Protection

CPL receives inbound email on behalf of the organization, insulating your organization's mail server from receiving direct Internet connections and associated threats. *This layer does not apply to outbound mail.* Here are some of the benefits of using CPL together with your Barracuda Email Security Gateway:

- Spooling – CPL polls your inbound mail server regularly and, if the mail server goes down, the service spools your inbound mail for up to 4 days. As soon as the mail server comes back up, email is released in a steady stream, resuming consistent inbound mail flow.
- Advanced Threat Protection (ATP) – The ATP service analyzes inbound email attachments 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 not detected by the Barracuda Email Security Gateway virus scanning features. See Advanced Threat Protection for details.
- Link Protection – Rewrites a deceptive URL in an email message to a safe Barracuda URL, and delivers that message to the user. See Anti-Fraud and Anti-Phishing Protection for details.
- Typosquatting protection – Checks for common typos in the URL domain name in an email message and, if found, rewrites the URL to the correct domain name so that the user visits the intended website. See Anti-Fraud and Anti-Phishing Protection for details.
- Email Burst Handling – Email surge suppression during peak traffic and spam spikes, which offloads a significant volume of spam email from your Barracuda Email Security Gateway to be filtered via the cloud.
- Immediate Response – Automatic updates in real time, leveraging threat intelligence from Barracuda Labs and Barracuda Central to continuously stay ahead of quickly morphing threats.

© 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.