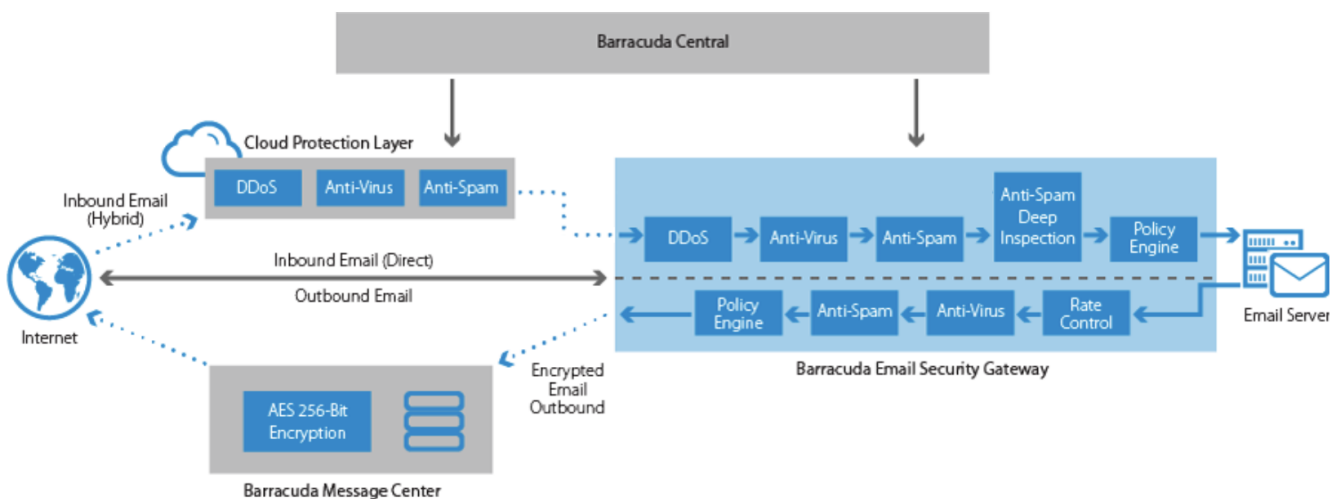


Overview

<https://campus.barracuda.com/doc/3866644/>

The Barracuda Email Security Gateway is an integrated hardware and software solution designed to protect your email server from spam, virus, spoofing, phishing and spyware attacks. Outbound filtering and encryption options also prevent confidential or sensitive information from being purposely or inadvertently leaked outside the organization (Data Leakage Prevention). The optional cloud protection layer (CPL) shields email servers from inbound malware and DoS attacks while filtering out normal spam before it ever touches the network's perimeter. Both hardware appliance and virtual machine options are available.



Where to Start

The selected deployment mode may depend on the email server configuration that currently exists at your site, as well as whether you want to deploy the Barracuda Email Security Gateway behind your corporate firewall or in front of your corporate firewall in the DMZ. Refer to [Deployment Options](#) for more information. For the Barracuda Email Gateway Defense (formerly Barracuda Email Security Service) cloud solution, see [Email Gateway Defense](#).

Device Deployment

- Go to the [Getting Started](#) section, or
- Download the [Barracuda Email Security Gateway Quick Start Guide](#).

Virtual Deployment

- Go to the [Barracuda Email Security Gateway Vx Quick Start Guide](#).

Key Features

- Spam and virus filtering, including:
 - The optional [Barracuda Exchange Antivirus Agent](#), a free add-in that you can install on your Microsoft Exchange *mailbox* server(s).
 - [Advanced Threat Protection](#), a subscription-based service that offers protection against advanced malware, zero-day exploits, and targeted attacks.
- Global or per-user quarantine
- Prevents spoofing, phishing and malware
- Data leakage prevention (DLP) with outbound email filtering
- SMTP/TLS site-to-site encryption – see [How to Use DLP and Encryption of Outbound Mail](#)
- Invalid bounce suppression
- Policy enforcement for compliance and corporate policies

Migrating From the Barracuda Email Security Gateway to the Barracuda Email Gateway Defense

For information about the migration process from your hardware or virtual appliance to the Barracuda Email Gateway Defense cloud offering, see [Moving from Barracuda Email Security Gateway to Barracuda Email Gateway Defense](#).

For information about Barracuda Networks' conversion tool to migrate configurations from the Barracuda Email Security Gateway to the Barracuda Email Gateway Defense, see [Conversion Tool for Migrating to Barracuda Email Gateway Defense](#).

Figures

1. CPLtoESGCorrected.png

© 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.