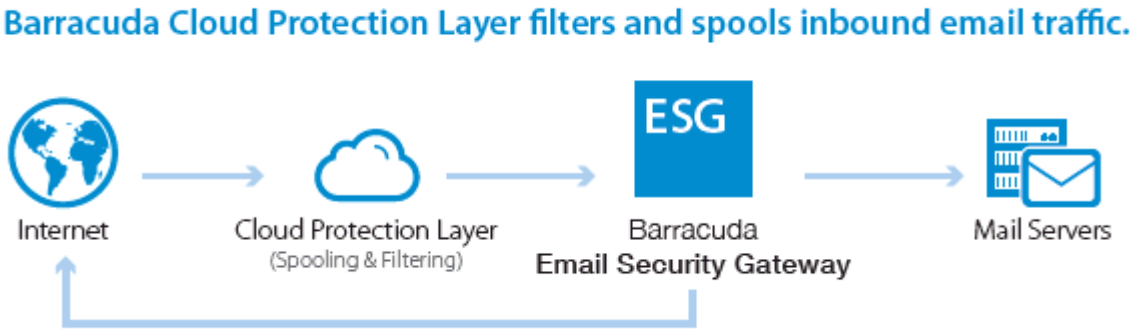
Cloud Protection Layer

https://campus.barracuda.com/doc/3866716/

The optional 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, prevents phishing and zero day attacks, and provides email continuity. Once email passes through CPL, the Barracuda Email Security Gateway filters email according to the more granular policies, further recipient verification, quarantining, and other features you configure on the appliance or virtual machine. You can use Barracuda Cloud Control for central management of your CPL and your Barracuda Email Security Gateway(s). See Advantages of the Cloud Protection Layer.

How to Get the Cloud Protection Layer

The Barracuda Cloud Protection Layer is available with a current Advanced Threat Protection (ATP) subscription. See setup instructions below.



1.If your mail server becomes unavailable, mail is spooled for up to 96 hours.

Aggregated Statistics with CPL and the Barracuda Email Security Gateway

With Barracuda Cloud Control, you can view email statistics from both your Barracuda Email Security Gateway(s) and CPL in an aggregated view/report; however, currently, if you have configured CPL to use a non-US region, those statistics are *not* included in aggregated reports/views in Barracuda Cloud Control. You can still view those statistics in CPL.

For a single Barracuda Cloud Control account, you cannot use a linked Barracuda Email Security Gateway with an active Email Gateway Defense subscription. If that configuration is required,

you must create a Barracuda Cloud Control account for each.

How to set up and use the Cloud Protection Layer

1. Set up your Barracuda Email Security Gateway.
2. If you do not already have an active Advanced Threat Protection subscription, contact your Barracuda Networks reseller or representative to purchase one. This subscription includes the Barracuda Cloud Protection Layer.
3. Continue with How to Set Up Barracuda Cloud Control, if you have not already configured your free account.
4. Follow instructions for initial setup of the Cloud Protection Layer with How to Set Up Your Cloud Protection Layer.
5. Use this article to configure filtering policies for the Cloud Protection Layer to apply to inbound mail before it reaches your Barracuda Email Security Gateway.

Policies Configurable in the Cloud Protection Layer

Some of the policies that are available on the Barracuda Email Security Gateway are also configurable in the Cloud Protection Layer, offloading policy enforcement from your Barracuda Email Security Gateway and further protecting your network from threats. These policies, as well as some additional protections, include:

Advanced Threat Protection (ATP)

The subscription-based 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.

Anti-phishing, antivirus, anti-spam protection

- Anti-phishing, configurable on the Cloud Protection Layer **INBOUND SETTINGS > Anti-Phishing** page**:**
  - Intent analysis
  - Link protection
  - Typosquatting protection
  - Anti-fraud intelligence, which uses a special Bayesian database that is constantly learning for the detection of phishing scams.
- Anti-spam, antivirus, configurable on the Cloud Protection Layer **INBOUND SETTINGS > Anti-**

Spam/Antivirus page**:**

- Barracuda Reputation Block List (BRBL)
- Virus scanning
- Barracuda Real-Time System (BRTS) – An advanced service to detect zero-hour spam and virus outbreaks even where traditional heuristics and signatures to detect such messages do not yet exist.
- CloudScan – A cloud-based spam scanning engine, which assigns a score to each message processed ranging from 0 (unlikely spam) to 10 (definitely spam). Setting a score of 1 will likely block legitimate messages while setting a score of 10 will allow more messages through the system.
- Bulk email detection

IP analysis

- Custom RBLs – On the **INBOUND SETTINGS > Custom RBLs** page, you can add any additional free or subscription block lists. External IP block lists, also known as DNSBLs or RBLs, are lists of Internet addresses that have been identified as potential originators of spam. These lists can be used to block potential spammers.
- Rate Control – This feature protects your mail server from spammers or spam-programs (also known as "spam-bots") that send large amounts of email to the server in a small amount of time. You can exempt known and trusted IP addresses or IP ranges from IP based Rate Control. Email messages are still scanned for spam and virus content. Configure on the **INBOUND SETTINGS > Rate Control** page.
- IP address block/accept policies – Add IP addresses or networks to the Allow List to always exempt, or to the Block List to always block. Allow Listed IP addresses/networks bypass spam scoring as well as all other block lists, but virus scanning still applies. This list of IP addresses that you choose to block takes precedence over the Barracuda Reputation Block List and Custom RBL entries. Configure on the **INBOUND SETTINGS > IP Address Policies** page.

Recipient and sender policies

- Recipient Policies – Add recipient email addresses you specifically want to always exempt to the Allow List, or always block to the Block List. Or you can apply a default behavior to all recipients, by selecting either *Scan* or *Exempt* from the **Default policy for all users** drop-down. Exempt (Allow Listed) recipients bypass spam scoring as well as all other block lists. Virus scanning still applies. Configure on the **INBOUND SETTINGS > Recipient Policies** page.
- Sender Policies – Sender policies allow you to exempt or block messages by username in a sender email address, domain name, or both. For details, see the **INBOUND SETTINGS > Sender Policies** page.
- Sender Authentication – Configure reverse DNS lookups for sender domain verification, domain-spoofing protection, DomainKeys Identified Mail (DKIM), Sender Policy Framework (SPF) and Domain-based Message Authentication, Reporting, and Conformance (DMARC) for sender authentication. See the **INBOUND SETTINGS > Sender Authentication**. For more details about these methods, see Sender Authentication.

Note that the Cloud Protection Layer can be configured with many of the same block/accept

policies you would apply to the Barracuda Email Security Gateway, but only provides the Block (or Scan) and Allow (exempt) actions. The Cloud Protection Layer does not support tagging or quarantine of email.

Figures

1. CPLGraphic.png