How the Service Works

https://campus.barracuda.com/doc/96022976/

For each Barracuda Cloud Control account, you can have either a linked Barracuda Email Security Gateway appliance or an Email Gateway Defense subscription. You cannot use a single Barracuda Cloud Control account for both a linked appliance and the service subscription.

If you make setting changes, allow a few minutes for the changes to take effect.

Email Gateway Defense is not designed to handle internal mail (e.g., from domain `x.com` to domain `x.com`). It will see such mail as inherently suspicious and might block it as a spoof or spam. For on-premises email servers, this internal mail should never leave the server. For hosted solutions, wherever possible, configure the system to keep the mail internal to the service, rather than routing it through Email Gateway Defense.

Email Gateway Defense is a pass-through service, accepting connections from a mail server, getting the initial "rcpt to" line and connecting to the destination mail server. The service then monitors the data stream for any spam or virus content and applies policies you configure in the web interface.

Barracuda Networks recommends understanding the concepts described in this article before customizing your Email Gateway Defense.

Connection Management Layers

Connection Management layers identify and block unwanted email messages before accepting the message body for further processing. For the average small or medium organization, you can block more than half of the total email volume using Connection Management techniques. Extremely large Internet Service Providers (ISPs) or even small web hosts, while under attack, may observe block rates at the Connection Management layers exceeding 99 percent of total email volume.

Table 1. Connection Management Layers.

Layer	Description
Denial of Service Protection	Email Gateway Defense 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.

Rate Control	Automated spam software can be used to send large amounts of email to a single mail server. To protect the email infrastructure from these flood-based attacks, Email Gateway Defense counts the number of recipients from a sender to a domain during a 30 minute interval and defers the connections once a particular threshold is exceeded. Inbound Rate Control is a threshold for the number of recipients a domain is willing to receive from a sender (a single IP address) during a 30 minute interval. Inbound rate control is configurable while outbound rate control is set automatically by Email Gateway Defense. Senders and IP addresses cannot be exempted from Email Gateway Defense outbound rate control.
Suspicious Email Monitoring	Suspicious Email Monitoring inspects incoming mail from all over the world looking for mail with common subject lines and suspicious content. If any are found, Email Gateway Defense defers this mail, forcing the sender to retry the mail at a later time. Normally, the mail will be allowed when it is retried. However, a few retries may be required, especially if they are made too quickly. Add a sender address to the sender allow policy to bypass the suspicious filtering or contact Barracuda Networks Technical Support to have the suspicious policy turned off.
IP Analysis	After applying rate controls based on IP address, Email Gateway Defense performs analysis on the IP address of email based on the following: • **Barracuda Reputation** – Leverages data on network addresses and domain names collected from spam traps and throughout other systems on the Internet. The sending histories associated with the IP addresses of all sending mail servers are analyzed to determine the likelihood of legitimate messages arriving from those addresses. Incoming connection IP addresses are compared to the Barracuda Reputation list, if enabled, and connections from suspicious senders are dropped. • **External block lists** – Also known as Real-Time Block Lists (RBLs) or DNS Block Lists (DNSBLs). Several organizations maintain external block lists of known spammers. • **Allowed and blocked IP address lists** – Customer-defined policy for allowed and blocked IP addresses. By listing trusted mail servers by IP address, administrators can avoid spam scanning good email, reducing processing requirements and eliminating the chance of false positives. Likewise, administrators can define a list of bad email senders for blocking. In some cases, it may be necessary to use the IP block lists to restrict specific mail servers as a matter of policy rather than as a matter of spam protection.
Sender Authentication	Declaring an invalid "from" address is a common practice used by spammers. The Email Gateway Defense Sender Authentication layer uses a number of techniques on inbound mail to both validate the sender of an email message and apply policy. Sender Policy Framework (SPF) tracks sender authentication by having domains publish reverse MX records to display which machines are designated as mail sending machines for that domain. The recipient can check those records to make sure mail is coming from a designated sending machine.

Mail Scanning Layers

The most basic level of mail scanning is virus scanning. Email Gateway Defense utilizes three layers

of virus scanning and automatically decompresses archives for comprehensive protection. By utilizing virus definitions, Email Gateway Defense customers receive the best and most comprehensive virus and malware protection available. The three layers of virus scanning of inbound and outbound mail include:

- Powerful open source virus definitions from the open source community help monitor and block the latest virus threats.
- Proprietary virus definitions, gathered and maintained by Barracuda Central, our advanced 24/7 security operations center that works to continuously monitor and block the latest Internet threats.
- Barracuda Real-Time System (BRTS). This feature provides fingerprint analysis, virus protection and intent analysis. When enabled, any new virus or spam outbreak can be stopped in real-time for industry-leading response times to email-borne threats. BRTS allows customers to report virus and spam propagation activity at an early stage to Barracuda Central. Virus Scanning takes precedence over all other mail scanning techniques and is applied even when mail passes through the Connection Management layers. As such, even email coming from exempt IP addresses, sender domains, sender email addresses, or recipients are still scanned for viruses and quarantined if a virus is detected.

Additionally, Email Gateway Defense includes the Advanced Threat Protection (ATP) service. The ATP service analyzes inbound email attachments with most MIME types and publicly accessible direct download links in a separate, secured cloud sandbox, 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 Email Gateway Defense virus scanning features.

Barracuda Antivirus Supercomputing Grid

An additional, patent-pending layer of virus protection offered by Email Gateway Defense is the Barracuda Antivirus Supercomputing Grid, which can protect your network from polymorphic viruses. Not only does it detect new outbreaks similar to known viruses, it also identifies new threats for which signatures have never existed using "premonition" technology.

All spam messages have an "intent" – to get a user to reply to an email, to visit a website, or to call a phone number. Intent analysis involves researching email addresses, web links and phone numbers embedded in email messages to determine whether they are associated with legitimate entities. Frequently, Intent Analysis is the defense layer that catches phishing attacks. When enabled, Email Gateway Defense applies various forms of Intent Analysis to both inbound and outbound mail, including real-time and multi-level intent (or 'content') analysis. Multi-level intent is the process of identifying URLs in an email message body that redirect to known spam or malware sites.

Advanced Spam Detection

You can configure spam detection for custom categories by setting a content type score. This score ranges from 0 (definitely not spam) to 10 (definitely spam). Based on this score, Email Gateway Defense blocks messages that appear to be spam. These messages display in the user's Message Log with the category responsible for the block.

Predictive Sender Profiling

When spammers try to hide their identities, Email Gateway Defense can use Predictive Sender Profiling to identify behavior of all senders and reject connections and/or messages from spammers. This involves looking beyond the reputation of the apparent sender of a message, just like a bank needs to look beyond the reputation of a valid credit card holder of a card that is lost or stolen and used for fraud. Some examples of spammer behavior that attempts to hide behind a valid domain, and Email Gateway Defense features that address them, include the following:

- Sending too many emails from a single network address – Automated spam software can be used to send large amounts of email from a single mail server. Through Rate Control Email Gateway Defense limits the number of connections made from any IP address within a 30 minute time period. Violations are logged to identify spammers. Inbound rate control is configurable while outbound rate control is set automatically by Email Gateway Defense.
- Attempting to send to too many invalid recipients – Many spammers attack email infrastructures by harvesting email addresses. Recipient Verification in Email Gateway Defense allows the system to automatically reject SMTP connection attempts from email senders that attempt to send to too many invalid recipients, a behavior indicative of directory harvest or dictionary attacks.
- Registering new domains for spam campaigns – Because registering new domain names is fast and inexpensive, many spammers switch domain names used in a campaign and send blast emails on the first day of domain registration. Realtime Intent Analysis on Email Gateway Defense is typically used for new domain names and involves performing DNS lookups and comparing DNS configuration of new domains against the DNS configurations of known spammer domains.
- Using free Internet services to redirect to known spam domains – Use of free websites to redirect to known spammer websites is a growing practice used by spammers to hide or obfuscate their identity from mail scanning techniques such as Intent Analysis. With Multi-level Intent Analysis, Email Gateway Defense inspects the results of web queries to URIs of well-known free websites for redirections to known spammer sites.

Notifications

Email Gateway Defense sends out two kinds of notifications:

- Quarantine Digest – For email recipients listed in the database, a notification email containing a summary of quarantined email is sent to their email address at an interval you specify for users.
- Attachment Blocking for Content – A notification is sent to the message sender when it is blocked due to attachment content filtering.

Monitored Outbound Email Volume

Email Gateway Defense monitors the volume of outbound email from the system to the Internet. If the volume exceeds normal thresholds during any given 30 minute interval, the rate control function takes effect, causing all outbound mail to be deferred until the end of the 30 minute time frame. The outbound mail flow then continues unless the volume is exceeded again in the next 30 minute interval. If so, Rate Control is again triggered and outbound mail is deferred until the end of the time frame. For more information, see Outbound Rate Control.