Getting to Know Email Gateway Defense

https://campus.barracuda.com/doc/96023090/

Email Gateway Defense protects both inbound and outbound email against the latest spam, viruses, worms, phishing, denial of service attacks, and zero-day threats. Email Gateway Defense acts as a filter in front of your hosted email service or servers. Spam and viruses are blocked in the cloud prior to delivery to your network, saving network bandwidth and providing additional Denial of Service protection. Email Gateway Defense is flexible, allowing in-depth configuration and customization.

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.

Connection Management Layers

Connection Management layers identify and block unwanted email messages before accepting the message body for further processing. Connection filtering allows you to block or allow:

- Sender IP addresses
- Sender email addresses / domains
- Email messages written in specific languages
- Email messages sent from specific countries / regions

Denial of Service Protection (DoS)

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.

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. Customers

can 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 Barracuda Reputation, external blocklists, and allowed and blocked IP address lists.

Sender Authentication

Declaring an invalid "from" address is a common practice used by spammers. 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, Barracuda Networks offers the subscription-based Advanced Threat Protection (ATP) service, a cloud-based virus service that applies to inbound messages. ATP analyzes email attachments in a separate secured cloud environment to detect new threats and determine whether to block such messages.

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.

Intent Analysis

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 on 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 Email Gateway Defense 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.

Encryption

To prevent data leakage and ensure compliance with financial, health care and other federally-regulated agency information policies, Email Gateway Defense provides several types of encryption for inbound and outbound message traffic.

Encrypted Channel

TLS provides secure transmission of email content, both inbound and outbound, over an encrypted channel using the Secure Sockets Layer (SSL) - also known as TLS.

To require mail to be sent outbound from Email Gateway Defense over a TLS connection, enable **Force TLS** for each domain on the **Outbound Settings > DLP/Encryption** page. Mail sent to these domains must be transmitted across a TLS connection. If a TLS connection cannot be established, mail will not be delivered.

To require mail coming inbound to Email Gateway Defense to use a TLS connection, set SMTP Over TLS to **Required** on the **Domains > Settings** page for each domain. When set to **Required**, if TLS is available on your organization's mail server, inbound mail is sent over a TLS channel. If not, mail is sent in cleartext.

Outbound Mail Encryption

For guaranteed message encryption and ensured outbound message delivery, use the Barracuda Message Center to encrypt the contents of certain outbound messages. Create policies for when to encrypt outbound messages on the **Outbound Settings > Content Policies** page for a domain.

Advanced Threat Protection

The Advanced Threat Protection (ATP) service analyzes inbound email attachments with most MIME types 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 Email Gateway Defense virus scanning features. Enable ATP on the **ATP Settings** page in the Email Gateway Defense web interface.