Getting to Know Barracuda Essentials

https://campus.barracuda.com/doc/78810355/

Barracuda Email Security Service

The Barracuda Email Security Service protects both inbound and outbound email against the latest spam, viruses, worms, phishing, denial of service attacks, and zero-day threats. The Barracuda Email Security Service 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. The Barracuda Email Security Service is flexible, allowing in-depth configuration and customization.

The Barracuda Email Security Service 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)

The Barracuda Email Security Service 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, the Barracuda Email Security Service 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 the Barracuda Email Security Service.

IP Analysis

After applying rate controls based on IP address, the Barracuda Email Security Service performs analysis on the IP address of email based on Barracuda Reputation, external blocklits, and allowed and blocked IP address lists.

Sender Authentication

Declaring an invalid "from" address is a common practice used by spammers. The Barracuda Email Security Service 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. The Barracuda Email Security Service utilizes three layers of virus scanning and automatically decompresses archives for comprehensive protection. By utilizing virus definitions, Barracuda Email Security Service 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 the Barracuda Email Security

Service 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, the Barracuda Email Security Service 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, the Barracuda Email Security Service 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, the Barracuda Email Security Service 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 the Barracuda Email Security Service 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 the Barracuda Email Security Service 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 the Barracuda Email Security Service.
- Attempting to send to too many invalid recipients – Many spammers attack email infrastructures by harvesting email addresses. Recipient Verification on the Barracuda Email Security Service 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 the Barracuda Email

Security Service 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, the Barracuda Email Security Service inspects the results of web queries to URIs of well-known free websites for redirections to known spammer sites.

Notifications

The Barracuda Email Security Service sends out two kinds of notifications:

- Quarantine Digest – For email recipients listed in the Barracuda Email Security Service 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

The Barracuda Email Security Service 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, the Barracuda Email Security Service 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 the Barracuda Email Security Service 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 the Barracuda Email Security Service 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 the Barracuda Email Security Service virus scanning features. Enable ATP on the **ATP Settings** page in the Barracuda Email Security Service web interface.

Barracuda Cloud Archiving Service

The Barracuda Cloud Archiving Service is a Software as a Service (SaaS) solution hosted in the Barracuda Cloud, previously referred to as direct-to-cloud. The Barracuda Cloud Archiving Service is designed for customers that do not want to manage a physical or virtual appliance. It is simpler to deploy than public cloud versions of Barracuda Message Archiver, without additional infrastructure investment.

Emails are archived without the need to install any email client or server software. Barracuda Networks' extensive and robust global cloud infrastructure ensures security, and centralized management through the Cloud Control portal makes it simple.

Understanding Compliance

The Barracuda Cloud Archiving Service provides everything an organization needs to comply with government regulations in a cloud solution. The Barracuda Cloud Archiving Service stores and indexes all email for easy search and retrieval by both regular users and third-party auditors. Backed by Energize Updates, delivered by Barracuda Central, the Barracuda Cloud Archiving Service receives automatic updates to its extensive library of virus and policy definitions to enable enhanced monitoring of compliance and corporate guidelines as well as document file format updates needed to decode content within email attachments.

The Barracuda Cloud Archiving Service features an easy-to-use web user interface, creating an intuitive and cost-effective administration tool for the Software as a Service (SaaS) solution. The web user interface allows administrators to define, manage, and control corporate archiving settings and rules from a central location.

The Barracuda Cloud Archiving Service provides:

- Litigation Support
- Storage Management
- Knowledge Management
- Compliance
- Regulatory Compliance

Litigation Support

Litigation discovery involves all parties in a lawsuit and requires that all data or information relevant to the lawsuit be provided as requested by the court of law. All email is stored and indexed for easy search and retrieval by both regular users and third-party auditors.

Storage Management

Not only does the volume of email messages continue to increase, the size of the average email itself is also on the rise. Due to the increased use of file attachments in email messages, the average email size can range between 22KB and 350KB. As such, the ability for an organization to adequately keep up with the storage demands of email can be costly. While storage solutions can be used to deal with the problem of email message growth in the short term, the Barracuda Cloud Archiving Service provides a more resourceful way of handling the issue over a longer period of time.

Knowledge Management

A company’s email system contains a vast amount of vital corporate intelligence, some of which is not replicated in any other data or material. If email is lost or is not easily accessible, a company runs the risk of losing that intelligence. The Barracuda Cloud Archiving Service provides management tools essential to storing and controlling access to an organization's knowledge base.

Compliance

Compliance issues are perhaps the driving force behind the increase in demand for an email archiving solution. The sheer number of regulations requiring some form of email retention, as well as the more specific parameters of how the email should be stored and for how long, can be confusing for administrators.

Although many regulations exist and have varying requirements, compliance is based on three concepts:

- **Email permanence** – Email must be maintained in its original form without alteration or deletion
- **Email security** – Information must be protected against all threats including unauthorized access to the email as well as physical damage. This same concept applies to the process of legal discovery which often specifies who can access the email (i.e., legal teams) as well as safeguards against the destruction of hard copies of the data
- **Auditability** – Email must be easily accessible in a timely fashion by authorized personnel upon request

Data Retention

By default, automated purging of messages archived on the Barracuda Cloud Archiving Service is disabled. When enabled, the Global Retention Policy and any Saved-Search retention policies are run against all the archived messages once a week. You can allow messages to be deleted from the Barracuda Cloud Archiving Service when the age of any message exceeds the maximum age allowed by all matching Saved Search retention policies, or the Global Retention Policy if no Saved Search retention policy matches the message. Retention policies are the only way to purge messages; data cannot be deleted directly by a user.

Litigation Holds

Litigation Holds are created by auditors to prevent messages that meet the criteria for a specific Saved Search from being removed from the Barracuda Cloud Archiving Service.

Barracuda Cloud-to-Cloud Backup

Barracuda Cloud-to-Cloud Backup for Office 365 protects Exchange Online and OneDrive for Business data by backing it up directly to Barracuda Cloud Storage. Use Barracuda Cloud-to-Cloud Backup for Office 365 as an add-on to an on-premises Barracuda Backup appliance or as a standalone subscription without an appliance. Barracuda Cloud-to-Cloud Backup for Office 365 provides completely customizable and unlimited backup scheduling and retention, the ability to restore or download data to different sources, and the ability to back up multiple instances of Microsoft Office 365 without purchasing additional licenses.

- **Scheduled Backups** – Create schedules to automatically back up data or run backups on-demand at any time. Optionally, backup schedules can be repeated throughout the day as fast as every 60 seconds, achieving near-continuous data protection. All Exchange Online and OneDrive for Business data is deduplicated and compressed for maximum storage efficiency before being stored in the Barracuda Cloud.
- **Restore Data** – All Office 365 data backed up to the Barracuda Cloud is accessible, searchable, and retrievable from anywhere with an Internet connection. Select specific dates from a built-in calendar, for point-in-time data recovery. Restore files or email messages back to the original user account and location, to a different location within the account, or to a completely different

user account. If you are looking for a specific file or message but are unsure of its location, use the search feature to quickly and easily find the item, and then restore or download the item.Downloading folders puts them into a compressed ZIP file for quick downloads, while email messages are downloaded using the industry-standard EML format. Files are downloaded using their same file format. If you select to download multiple files, the files are downloaded as a ZIP file.

- **Reports and Statistics** – Barracuda Cloud-to-Cloud Backup provides backup status and health monitoring for each backup source. Automated email alerts are delivered after each backup to specified email recipients containing a summary of the backup and detailed information about which email messages and files were added, modified, and removed since the last backup. The **Status** page includes graphs showing the number of items added and amount of data backed up each day. Storage statistics and graphs detail how much data has been backed up overall and the storage efficiency, and how much data is actually being stored in the Barracuda Cloud after deduplication and compression. An Audit Log tracks and provides details about every action performed within the Cloud-to-Cloud interface.
- **Security** – With Barracuda Cloud-to-Cloud Backup, all Office 365 data is encrypted in-transit with 128-bit SSL encryption, the same level of security used by most banks and financial institutions. Data stored in the Barracuda Cloud is encrypted at-rest using 256-bit AES encryption. Barracuda Cloud Storage regularly undergoes third-party audits and is SSAE 16 Type II certified. Additional layers of protection included in Barracuda Cloud Control are multi-factor authentication (MFA or 2FA), IP address login restrictions, and role-based administration.