Step 1 - Understand the Concepts

https://campus.barracuda.com/doc/3866669/

The Barracuda Email Security Gateway takes a configured action when it identifies a message as spam or otherwise in violation of configured Block and Accept policies. Inbound messages may be Blocked, Quarantined, Tagged or Allowed, while outbound messages may be Blocked, Quarantined, Encrypted or Sent. Note that using the Quarantine or Tag actions with some scanning layers described below may use more system resources than Block or Allow actions.

Cloud Protection Layer

In addition to the built-in layers of protection described in this article, the optional Cloud Protection Layer feature provides 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 the Cloud Protection Layer, 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'll use Barracuda Cloud Control for central management of your Cloud Protection Layer and your Barracuda Email Security Gateway(s). See Cloud Protection Layer and How to Set Up Your Cloud Protection Layer.

Twelve Layers of Defense

Understanding each of the 12 layers of defense available, as described below, prepares you to make decisions about which - if not all - of the connection and mail scanning features to enable and tune for the best combination of performance and accuracy of the Barracuda Email Security Gateway.

Maximizing Efficiency and Performance of Spam Scanning

Using Rate Control, Barracuda Reputation (realtime RBLs) and Recipient Verification, as described below, can maximize filtering performance of the Barracuda Email Security Gateway for inbound mail. These layers have the greatest impact on filtering speed and performance relative to all the other layers such that any inappropriate incoming mail connections are dropped even before receiving the message.

Connection Management Layers

These layers provide the most value in your Barracuda Email Security Gateway deployment for inbound mail as they identify and block unwanted email messages before accepting the message body for further processing. The Connection Management layers generally require less processing time than the seven content scanning layers that follow. For the average small or medium business, **more than half of the total email volume can be blocked 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.

Denial of Service Protection

Built on a hardened and secure Linux operating system, the Barracuda Email Security Gateway 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 Gateway counts the number of incoming connections from a particular IP address (inbound mail) or sender email address (outbound mail) during a 30 minute interval and throttles the connections once a particular threshold is exceeded. See Rate Control Inbound for more on configuring this feature.

IP Analysis

After applying rate controls based on IP address, the Barracuda Email Security Gateway performs analysis on the IP address of inbound mail based on the following:

- **Barracuda Reputation** - This feature 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. IP addresses of incoming connections are compared to the Barracuda Reputation Blocklist and the Barracuda Reputation Whitelist, if enabled, and suspicious incoming messages are either blocked, tagged or quarantined.
- **External blocklists** - Also known as real-time blocklists (RBLs) or DNS blocklists (DNSBLs). Several organizations maintain external blocklists 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 of good email, both reducing processing requirements and eliminating the chances of false positives. Likewise, administrators can define a list of bad email senders for blocking. In some cases, administrators may choose to utilize the IP blocklists 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 by spammers. The Barracuda Email Security Gateway Sender Authentication layer uses a number of techniques on inbound mail to both validate the sender of an email message and apply policy, including domain name spoof protection, performing a DNS lookup of domain names and enforcing RFC 821 compliance.

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.

DomainKeys (DKIM) dictates that a sending domain cryptographically signs outgoing messages, allowing the sending domain to assert responsibility for a message. When receiving a message from a domain, the recipient can check the signature of the message to verify that the message is, indeed, from the sending domain and that the message has not been tampered with.

See Advanced Configuration for details on configuring this layer.

Recipient Verification

The Barracuda Email Security Gateway verifies the validity of recipient email addresses for inbound messages (not outbound) through multiple techniques to prevent invalid bounce messages.
See Advanced Configuration to learn about LDAP integration, SMTP recipient verification and using a local database for recipient verification.

Mail Scanning Layers

Virus Scanning

The most basic level of Mail Scanning is virus scanning. The Barracuda Email Security Gateway utilizes three layers of virus scanning and automatically decompresses archives for comprehensive protection. By utilizing virus definitions, Barracuda Email Security Gateway 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 Protection (BRTS), a set of advanced technologies that enables each Barracuda Email Security Gateway to immediately block the latest virus, spyware, and other malware attacks as they emerge. This feature provides fingerprint analysis, virus protection and intent analysis. When BRTS is 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 the ability 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 "whitelisted" IP addresses, sender domains, sender email addresses or recipients are still scanned for viruses and blocked if a virus is detected.

The Barracuda Exchange Antivirus Agent for the Microsoft Exchange Server is an add-in that empowers your mail server to do virus scanning of internal mail and of previously stored mail using constantly updated virus signatures detected by Barracuda Central. See How to Get and Configure the Barracuda Exchange Antivirus Agent 6.0.x for details about getting and installing the add-in from the Barracuda Email Security Gateway Web interface.

User-specified rules (custom policy)

Administrators can choose to define their own policies, perhaps for compliance or governance reasons, which take precedence over spam blocking rules delivered to the system automatically through Barracuda Energize Updates. Administrators can set custom content filters for inbound and/or outbound mail based on the subject, message headers, message bodies and attachment file type.

Fingerprint Analysis

A message "fingerprint" is based on commonly used message components (e.g., an image) across many instances of spam. Fingerprint analysis is often a useful mechanism for blocking future instances of spam once an early outbreak is identified. Engineers at Barracuda Central work around the clock to identify new spam fingerprints which are then updated on all Barracuda Email Security Gateways through hourly Barracuda Energize Updates. Both inbound and outbound email messages are subject to Fingerprint Analysis

Intent Analysis

All spam messages have an "intent" – to get a user to reply to an email, to visit a Web site 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. The Barracuda Email Security Gateway applies various forms of Intent Analysis to both inbound and outbound mail, including real-time and multi-level intent analysis.

Image Analysis

While Fingerprint Analysis captures a significant percentage of images after they have been seen, the Barracuda Email Security Gateway also uses Image Analysis techniques on both inbound and outbound mail which protect against new image variants. These techniques include:

- **Optical character recognition (OCR)** - Enables the Barracuda Email Security Gateway to analyze the text rendered inside embedded images.
- **Image processing** - To mitigate attempts by spammers to foil OCR through speckling, shading or color manipulation, the Barracuda Email Security Gateway also utilizes a number of lightweight image processing technologies to normalize the images prior to the OCR phase. More heavyweight image processing algorithms are utilized at Barracuda Central to quickly generate fingerprints that can be used by the Barracuda Email Security Gateway to block messages.
- **Animated GIF analysis** - The Barracuda Email Security Gateway contains specialized algorithms for analyzing animated GIFs for suspect content.

Bayesian Analysis

Bayesian Analysis applies only to inbound mail and is a linguistic algorithm that profiles language used in both spam messages and legitimate email for any particular user or organization. To determine the likelihood that a new email message is spam, Bayesian Analysis compares the words and phrases used in the new email against the corpus of previously identified email. The Barracuda Email Security Gateway only uses Bayesian Analysis after administrators or users profile a corpus of at least 200 legitimate (not spam) messages and 200 spam messages. Bayesian Analysis does not apply to outbound mail.

Spam Scoring

Once an inbound or outbound message has passed the initial Barracuda Email Security Gateway block/accept filters, it receives a score for its spam probability. This score ranges from 0 (definitely not spam) to 9 or greater (definitely spam). Based on this score, the Barracuda Email Security Gateway can take one of the following actions:

- Block
- Quarantine
- Tag (inbound mail only)
- Allow (inbound mail only)
- Send (outbound mail only)

Domain Level Spam Scoring: The Barracuda Email Security Gateway 400 and higher allows for setting spam score levels for inbound mail at the domain level. The administrator or the Domain admin role can set the spam scoring levels on the **BASIC > Spam Checking** page.

Per-User Spam Scoring: The Barracuda Email Security Gateway 600 and higher allows the

administrator to enable users to set their own spam score levels for inbound mail if per-user quarantine is enabled. If per-user spam scoring is enabled, when the user logs into their account, they will see the **PREFERENCES > Spam Settings** page from which they can set tag, quarantine and block scoring levels for that account.

Predictive Sender Profiling

When spammers try to hide their identities, the Barracuda Email Security Gateway can use Predictive Sender Profiling to identify behaviors of all senders and apply the applicable Barracuda Email Security Gateway defense tactic to 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 Gateway 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. The **Rate Control** feature on the Barracuda Email Security Gateway can be set to limit the number of connections made from any IP address within a 30 minute time period. Violations are logged to identify spammers. Rate Control is configured from the **BLOCK/ACCEPT > Rate Control** page.

  The **Messages Per SMTP Session** setting limits the number of messages allowed in one SMTP session. If the number of messages in one session exceeds this threshold, the rest of the messages are temporarily blocked and are displayed in the message log as being "Deferred" with "Per-Connection Message Limit Exceeded" as the reason for the postponement. The sender is required to make a new connection to continue sending messages, which may ultimately trigger a **Rate Control** deferral. For this and other SMTP security settings, see the **ADVANCED > Email Protocol** page.

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

  Using LDAP lookup or a local database to verify valid recipients as well as Sender Spoof Protection, which blocks email with "From" addresses which use an allowed recipient domain on the Barracuda Email Security Gateway, protects against receiving mail targeted to invalid recipients.

- **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. **Real-time Intent Analysis** on the Barracuda Email Security Gateway 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 Web sites to redirect to known spammer Web sites is a growing practice used by spammers to hide or obfuscate their identity from mail scanning techniques such as **Intent Analysis**. With **Multilevel Intent Analysis**, the Barracuda Email Security Gateway inspects the results of Web queries to URIs of well-known free Web sites for redirections to known spammer sites.

Journaling

The Barracuda Email Security Gateway provides an avenue for recording a copy of, or journaling, email communications in your organization and sending them to a dedicated email address that you specify. The process of journaling is different from archiving; journaling is simply a means of recording your users' messages. Archiving, on the other hand, is a means of storing those copies in a separate environment for the purpose of regulatory compliance, data retention, or server maintenance. For archiving, consider also deploying the Barracuda Message Archiver.

Continue with Deployment Options.