EMAIL GATEWAY DEFENSE

BEST PRACTICES GUIDE

JUNE 2024

CONTENTS

INVESTIGATING FALSE POSITIVES

Follow these best practices to investigate false positives effectively:

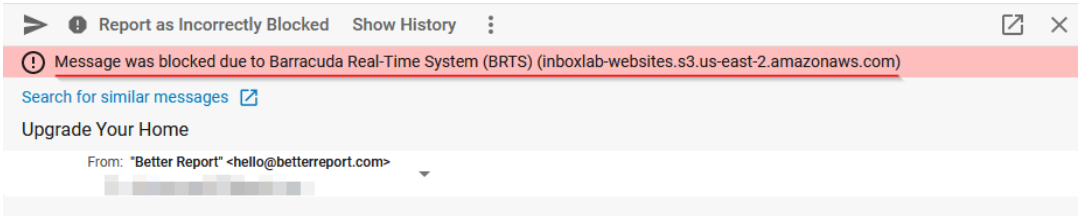
1. **Identify the Block Reason:**

    - **Barracuda-Controlled:**

        - **Report Message:** Click “Report as Incorrectly Blocked” from the message log. This information will be used to retrain our systems. *Note: There is no guarantee that reporting the message this way will prevent future emails from being blocked. You must still consider alternative methods to ensure delivery.*

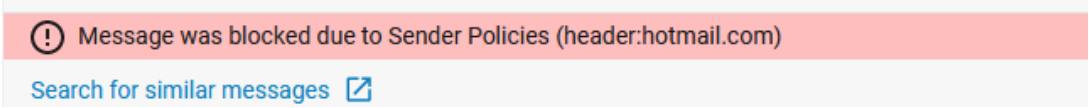
        - **Contact Support**: For issues that require more immediate attention, a support ticket can be opened to have the block cleared. Blocks are typically cleared within 24 hours. Use an exemption policy temporarily, reviewing it after 24-48 hours.

        - **Examples:** BRTS, BRBL, Intent, ATP



    - **Custom Policy:** Adjust your policies to be less strict if it causes false positives.

        - **Examples:** Spam score, sender policies, content policies, regional policies.



2. **Exemption Ability:**

    - Make specific exemptions instead of a full exemption to maintain other layers of filtering.

    - The following policies allow for specific exemptions:

        - Sender authentication checks: DMARC, DKIM, SPF, PTR

        - Regional (GeoIP) policies

        - Intent Analysis

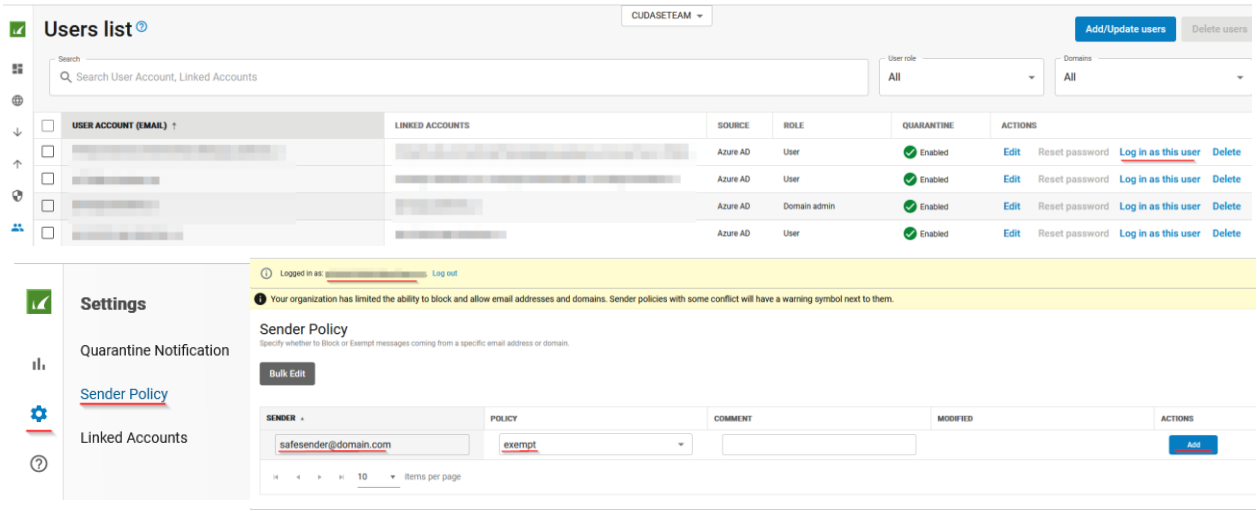
        - Advanced Threat Protection

- Machine Learning

3. **Policy Scope:**

   - **Company-Wide vs. Single User:** Create exemptions at the user level when possible or allow users to manage their own exemptions.

     - Leverage your ability to sign in as a user via the user list to create the policy on their behalf.



4. **Alternative Exemptions:**

   - **IP Policy:** Exempt IPs instead of domains, useful for services like DocuSign.

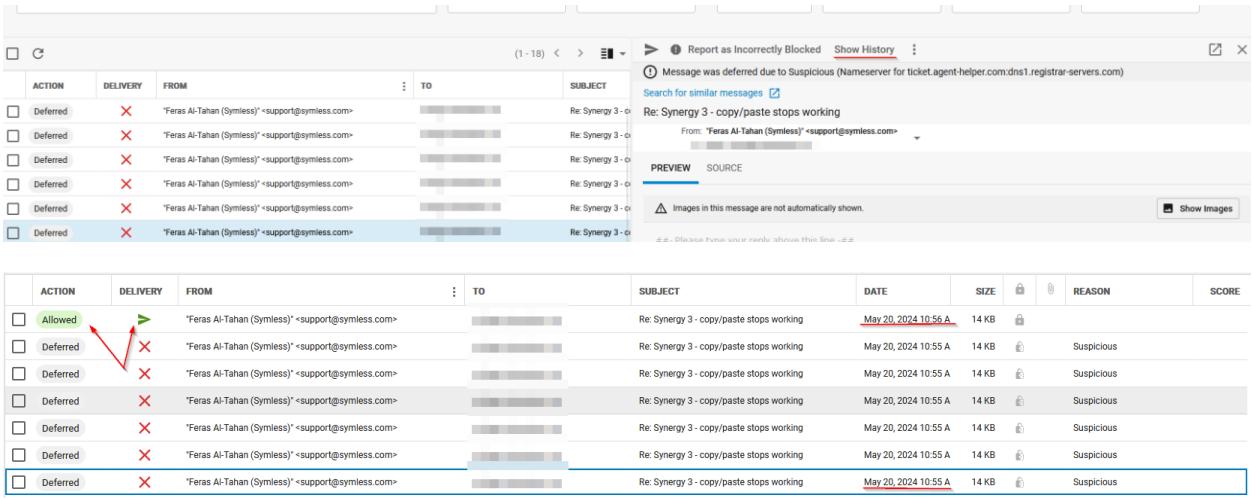
     - Make sure to not exempt IP that belong to hosting platforms such as: Microsoft, Google, SendGrid, Rackspace.

   - **Content Policy:** Use unique email identifiers, such as Salesforce account IDs, for exemptions.

     - How to use content filters to allow Salesforce emails

5. **Leverage Message History:**

   - Use the **Show Message History** functionality to bring a messages history into focus. In cases where messages are deferred or released by an end user, the message history will show when a message was reprocessed/redelivered. Deferred messages are often retried and delivered within 15 minutes; in which case no policies are needed.



We can see in this example, the email was deferred and then retried/delivered one minute later

SENDER POLICIES

Creating sender policies can be a quick solution for delivery issues, but overuse can lead to unintended consequences. Follow these best practices when creating sender policies:

1. **Understand Full Exemptions**:
   - Sender policies are full exemptions; only antivirus checks will be done. Ensure this is the desired action for the domain/email address you are entering.

2. **Check DMARC Status**:
   - Before making a full sender exemption, verify if the sending domain is protected with DMARC
   - If the domain uses p=reject DMARC policy, consider alternative solutions like content policies.

3. **Avoid Exemptions for Your Own Domain**:
   - If legitimate external emails using your domain are blocked, address the root cause instead of exempting your own domain to prevent spoofing and extortion attacks.

4. **Avoid Exemptions for Well-Known Services**:
   - Do not exempt domains for services like Microsoft, Google, DocuSign, ADP, etc., as this defeats their anti-spoofing controls and allows harmful emails through.

5. **Prefer Email-Specific Exemptions**:
   - Use specific email exemptions instead of full domain exemptions whenever possible.

6. **Document Sender Policy Entries**:
   - Include comments like internal ticket numbers in sender policy entries for easier policy review and cleanup.

7. **Review Policies Regularly**:

- Limit sender policies to the last 90 days. Remove older policies when possible.

8. **Use as Temporary Solutions**:
   - Treat sender policies as temporary fixes while addressing the root cause. Look for other aspects of the email to allow messages through without a sender policy.

SENDER AUTHENTICATION

Sender authentication checks are a common source of "false positives" when inbound messages are blocked due to improper sender configurations. Here are best practices for handling these situations:

DMARC (Domain-based Message Authentication, Reporting, and Conformance)

- **Function**: Ensures emails that fail DMARC checks (with a reject or quarantine policy) are blocked or quarantined.
- **Importance**: By not enforcing DMARC, fraudulent messages can enter your organization.
- **Handling Misconfigurations**: Implement a DMARC exemption for misconfigured domains.
- **Default**: Yes
- **Recommendation**: Yes

DKIM (DomainKey Identified Mail)

- **Function**: Validates DKIM signature found within an email by calculating a body hash
- **Limitations**: Does not help to protect against domain spoofing
- **Handling Misconfigurations**: Enter a DKIM exemption
- **Default**: Off
- **Recommendation**: Off or Quarantine

SPF (Sender Policy Framework)

- **Function**: Validates if an email originates from an authorized mail system using the SPF record published by the envelope sender domain
- **Hard Fail (-all)**: Block emails that fail this check.
  - **Default**: Block
  - **Recommendation**: Block
- **Soft Fail (~all)**: Tag or quarantine emails, do not block outright.
  - **Default**: Off
  - **Recommendation**: Quarantine or Off

No SPF Record

- **Context**: SPF records help verify that an email is sent from an authorized server for the domain. If a domain lacks an SPF record, it cannot be authenticated, making it vulnerable to spoofing.

- **Significance**: Domains without SPF records are easier targets for spoofers and malicious actors to send fraudulent emails appearing legitimate.
- **Risks**: Rejecting emails from domains without SPF records can prevent potential spoofed emails but may also block legitimate emails from domains that haven't set up SPF due to lack of awareness or technical capability.
- **Handling**: Monitor emails from domains without SPF records closely to minimize false positives and ensure there is no significant impact on business operations.
- **Default**: Off
- **Recommendation**: Off or Quarantine

SPF Exemptions:

- Exemptions can be made using an IP or a domain. It's recommended to use the envelope domain for exemptions rather than an IP.
- Exempt senders that fail SPF checks, ensuring other malicious content is still scanned.

No PTR Record

- **Function**: Checks if the IP resolves to a hostname (reverse lookup).
- **Significance**: Missing PTR records often indicate nefarious sources (botnets, infected PCs).
- **Handling**: Use PTR exemptions for legitimate sources without PTR records.
- **Default**: Block
- **Recommendation**: Block

REGIONAL POLICIES

GeoIP

Creating regional policies is an effective way to strengthen perimeter defenses by blocking spam and scams originating from countries where organizations rarely conduct business.

Recommendation for US-based Organizations:

- Start with a baseline geoIP block list, focusing on countries where spam originates.
    - Use sources like Spamhaus for updated lists.
- Avoid blocking countries hosting SaaS exit nodes (e.g., Ireland, Singapore, Netherlands) to prevent blocking legitimate mail due to sender domain's load-balancing scenarios.

Regional Policy Exemptions:

- Create exemptions for specific domains, emails, or IP addresses to bypass regional blocks.
    - For instance, block emails from China but exempt a specific vendor's domain for business purposes.

Regional Insights (For Incident Response or Premium/Premium Plus Customers):

- Utilize Regional Insights for detailed insights on countries sending emails to users.
- Create new regional block policies or policy exemptions in EGD using this information as your guide.
- For more information, see Geographical Insights

Language Policies

Language policies help filter out unwanted emails containing languages not relevant to the organization.

Languages include:

- Arabic
- Chinese
- German
- Greek
- Hebrew
- Japanese
- Korean
- Russian
- Thai
- Turkish
- Vietnamese

ANTI-SPAM/ANTIVIRUS

Barracuda Reputation Block List (BRBL)

The Barracuda Reputation Block List (BRBL) is maintained by Barracuda Central, containing IP addresses of known good and bad senders. It helps identify legitimate messages and spammers based on sending history. Barracuda Central continuously updates BRBL.

- **Default**: Block
- **Recommendation**: Block

Virus Scan

Virus scanning utilizes powerful virus definitions from open-source communities and Barracuda Central.

- **Default**: Yes
- **Recommended**: Yes

Barracuda Real-Time System (BRTS)

BRTS detects zero-hour spam and virus outbreaks, even without traditional heuristics and signatures. Using fingerprinting and domain reputation checks.

- **Default**: Block
- **Recommended**: Block

Cloudscan

Cloudscan assigns a score to each message processed, indicating the likelihood of spam. Adjust settings to balance filtering legitimate messages and blocking spam.

- **Default Block**: 5
- **Recommended Block**: 4-5

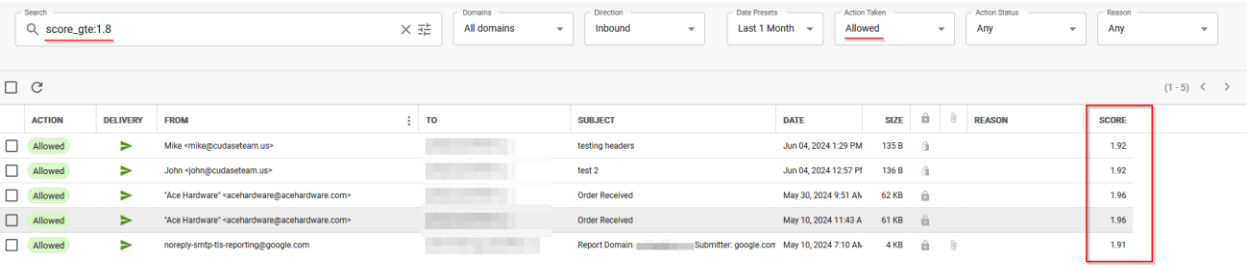
- **Default Quarantine**: Off
- **Recommended Quarantine**: 3-4

Pro Tip! Fine-Tuning Spam Score with Message Log Search

Utilize the message log search capabilities to fine-tune the spam score beyond the recommended thresholds. While default and recommended settings provide a starting point, customers may need to adjust their scores to align with the organization's needs and end users' preferences.

Utilizing Message Log Search:

- Analyze messages in the message log to assess their impact on the current spam score thresholds.
- Use search parameters like "score_gte" or "score_lte" to identify messages within specific score ranges.
- Example search parameters:
    - Score_lt(e): Lists messages with a score less than (or equal to) the specified value.
    - Score_gt(e): Lists messages with a score greater than (or equal to) the specified value.



Adjusting Spam Score: Based on the analysis from the message log search, adjust the spam score thresholds up or down as needed to better align with organizational requirements and end users' preferences.

In the provided example, a query of **score_gte:1.8** with an action of **Allowed** was run. The existing spam quarantine score was set to **2**. By performing this search, we can identify emails that would end up getting quarantined if the score was lowered to 1.8 (from 2).

Email Categorization

This feature offers administrators greater control over email categorization, allowing them to manage messages that might not meet the technical definition of spam but could still be considered unwanted.

1. Corporate Emails

   Emails from authenticated organization's Barracuda-verified mail servers, intended for general corporate communications.

   - **Default**: Allow
   - **Recommended**: Allow

2. Transactional Emails

   Emails related to specific transactions or orders, including confirmations, notices, bills, and account updates.

   - **Default**: Allow
   - **Recommended**: Allow

3. Marketing Materials

   Promotional emails and newsletters from companies such as Constant Contact.

   - **Default**: Off
   - **Recommended**: Quarantine

4. Mailing Lists

   Emails from mailing lists, newsgroups, and other subscription-based services.

   - Note: These types of emails have become a significant source of spam, contributing to unwanted clutter in users' inboxes.
   - **Default**: Off
   - **Recommended**: Block

5. Social Media

   Notifications and emails from social media sites like Facebook and LinkedIn.

   - **Default**: Allow

- **Recommended**: Allow or Quarantine

Bulk Email Detection

Bulk email makes up many of the emails that users receive daily. In some cases, these emails may be work or industry-related, but often, they are not work-related and serve as a distraction. These distractions can hamper the productivity of employees.

By leveraging bulk mail quarantine, you can limit these distractions by placing bulk mail into quarantine. The end users can then release the ones they need while ignoring the others. Limiting distractions in the Inbox while still allowing access can keep your users more productive.

Choosing "block" is only appropriate in specific situations. In most cases, choosing this option will result in requiring you to allowlist many domains, which is not ideal as it potentially leads to additional exposure against spoofed attacks.

If you decide to enable the setting, please make sure you **inform your end users** beforehand as it will almost certainly capture emails they expect to be delivered and the users will need to know. The process is rather easy for the user, but it can cause some friction. The user simply needs to click "allow list" from the digest email on any bulk sender they wish to receive communication from. Once the users build their safe sender list, then the bulk emails they want get delivered and the ones they don't stay in the quarantine and out of the Inbox.

- **Default**: Off
- **Recommended**: Quarantine or Off

CUSTOM RBLS

Consider leveraging external block lists like Spamhaus within the terms of service. Paid versions may be required for full functionality. Adding additional RBLs can help reduce spam but may increase false positives. Barracuda Support cannot assist with messages blocked due to third-party RBLs.

More information on third party RBLs can be found here

RATE CONTROL

Inbound rate control protects your mail server from spammers sending large amounts of email in a short time. It limits the number of messages from a sender's IP address within a 30-minute period.

- **Default**: 1,000
- **Recommended**: 1,000

IP ADDRESS POLICIES

When creating IP policies, it's crucial to consider the following points:

1. **Avoid Shared IPs**: Only make IP exemptions when you are certain that the IP is not shared by multiple senders. For instance, it's not recommended to add Microsoft or SendGrid IPs as these ranges are shared by many customers.

2. **Use for Known Applications**: An IP exemption can be appropriate for known applications like DocuSign if the IP space is solely dedicated to the application. Refer to a list of popular applications with dedicated IPs for guidance.

3. **Proper IP/Subnet Notation**: Ensure you use proper IP/subnet mask notation. Invalid entries will not be evaluated during mail scanning.

4. **Be Specific**: Be as specific as possible. If you only need to allow or block a single IP, create an entry using /32 (255.255.255.255). Avoid exempting entire network ranges.

Trusted Forwarder

Most customers should not configure trusted forwarders. Only set up if a server forwards mail from the original source. Incorrect setup may affect IP-based checks and lead to missed or incorrect detections.

RECIPIENT POLICIES

Recipient policies are generally discouraged because there are limited scenarios where a recipient should be exempt from external email filtering. However, in certain situations, recipient policies might be necessary. Some examples include:

- **Lead Generation**: If your business relies heavily on leads coming in through emails, ensuring that no leads are accidentally blocked is critical.
- **Help Desk Operations**: For businesses that operate help desk services where external helpdesk tickets are submitted via email, recipient policies can ensure that these tickets are not blocked.
- **Upper Management Requests**: Occasionally, requests from upper management may necessitate specific recipient policies to ensure their communication is not hindered.

CONTENT POLICIES

Content policies provide finer control over the types of emails you want to prevent or allow into your organization. However, these policies can increase false positives (FPs), requiring exemptions that can complicate configurations and yield unintended results over time.

Attachment Policies

Attachment policies allow you to create rules around filenames and MIME types. With the advancements in Advanced Threat Protection (ATP) and sandboxing, the necessity for filename attachment policies has diminished. The use of these filters depends on organizational requirements.

Password-Protected File Types

Given the rise in cloud usage for sharing sensitive files, password-protected email attachments are often malicious or unwanted. Password-protected files cannot be scanned for malware, making them a potential attack vector. Barracuda Email Gateway Defense (EGD) allows blocking or quarantining password-protected archives, office documents, and zips.

- **Archives**:
  - **Default:** Block
  - **Recommended:** Block
- **Office Documents**:
  - **Default:** Off
  - **Recommended:** Block
- **PDFs**:
  - **Default**: Off
  - **Recommended**: Block

While the default for Office and PDF files is **Off** due to their common use for secure data transmission, blocking these can enhance security for organizations without such requirements.

False positives can be reviewed and released from the message log. A modern approach is to use SharePoint or OneDrive for file sharing, reducing multiple versions of the same document in mailboxes.

Message Content Policies

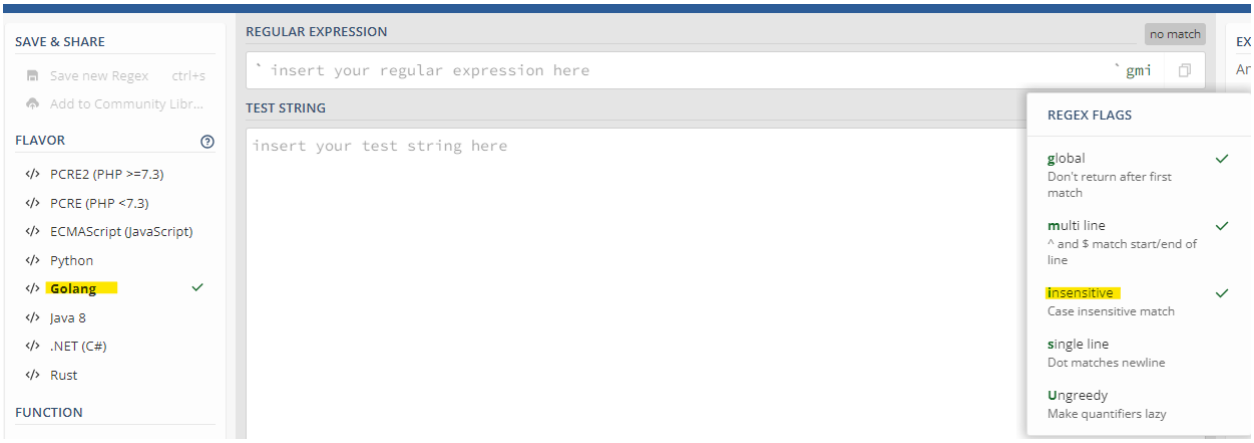
Content policies can filter emails based on specific patterns, such as headers like a Salesforce account ID. While powerful, these policies must be used cautiously. Aggressive policies can disrupt communication by generating false positives, while permissive policies might miss genuine threats.

Here are some resources to learn more:

- How to create a content policy to prevent employee impersonation

- Strengthening email security - Blocking display name spoofing
- What is email backscatter and how to prevent it

Regex Support: Message content filters support case-insensitive regex (re2) queries written in Golang. To test your regex pattern, you can use a tool such as regex101.com.



ANTI-PHISHING

Phishing scams are typically fraudulent email messages appearing to come from legitimate senders, such as universities, Internet service providers, or financial institutions. These messages often direct recipients to spoofed websites or otherwise trick them into revealing private information like logins, passwords, or other sensitive data, which is then used for identity and monetary theft.

Anti-Fraud Intelligence

This feature uses a special Bayesian database that continuously learns to detect new phishing scams.

- **Default**: Block
- **Recommended**: Block

Intent Analysis

Intent analysis is a method for identifying phishing attacks by examining email addresses, web links, and phone numbers embedded in email messages and attachments to determine their legitimacy. Domains incorrectly flagged by intent analysis can be excluded using an Intent Ignore policy.

- **Default**: On (Block)
- **Recommended**: On (Block)

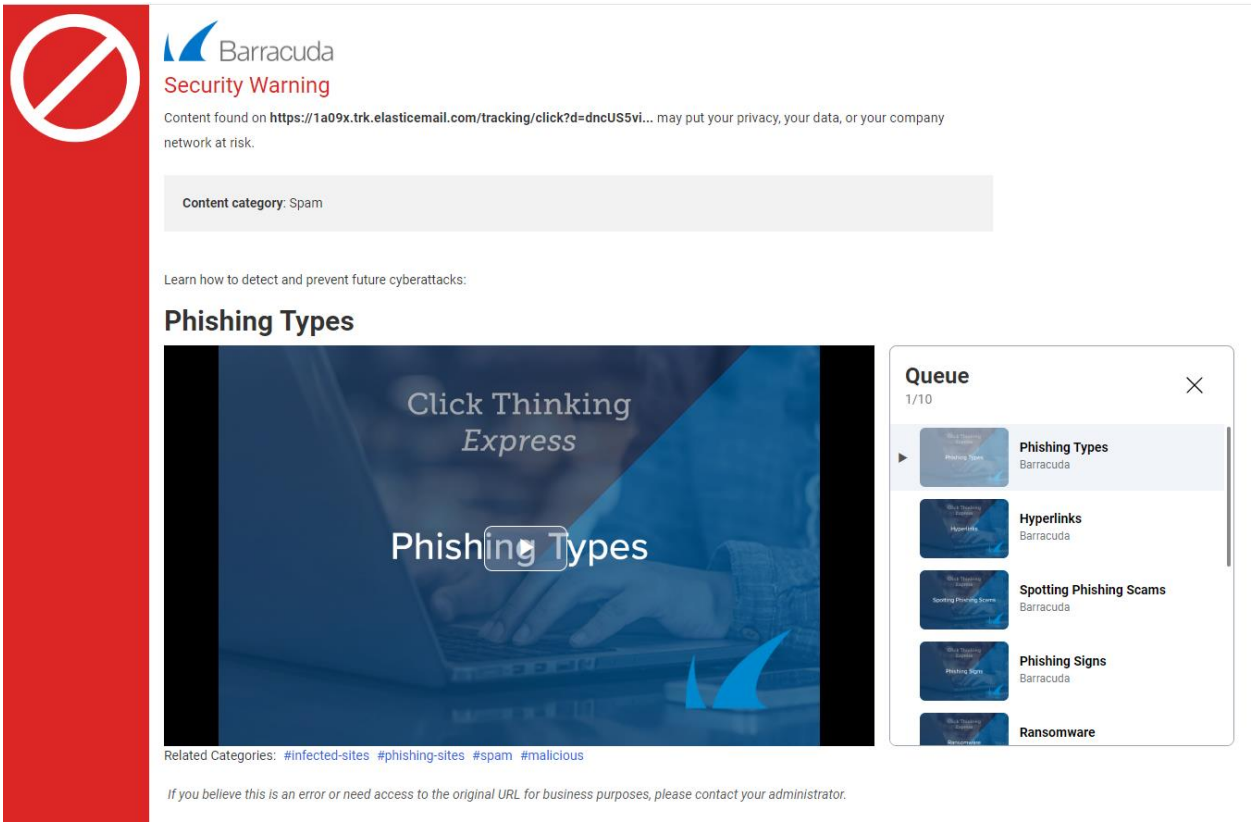
Content Intent

Content Intent is a subset of Intent Analysis that identifies messages with URLs in the body leading to suspicious websites.

- **Default**: Block
- **Recommended**: Block

Link Protection

Email Gateway Defense automatically rewrites URLs in email messages, replacing them with secure links provided by Barracuda Networks. When a user clicks a rewritten URL, the service assesses its legitimacy in real time. If the site is trustworthy, the user is redirected; if not, access is blocked to prevent fraud. This real-time protection ensures user safety while browsing.



To exclude a URL or domain from link analysis, including rewriting, create an **Ignore** policy under Intent Domain Policies on the Anti-Phishing page. Domains listed here will not undergo link analysis but will still be scanned by other security layers. Note that these policies apply only to new emails going forward. For existing links, contact Barracuda Support.

- **Default**: On
- **Recommended**: On

Typosquatting Protection

Typosquatting, or URL hijacking, tricks users into visiting a misleading domain by subtly altering the domain name (e.g., "bankofamerlca.com" instead of "bankofamerica.com"). The Typosquatting Protection feature checks for common typos in domain names and, if found, rewrites the URL to the correct domain so the user visits the intended website.

- **Default**: On
- **Recommended**: On

ATP SETTINGS

Advanced Threat Protection (ATP) is a cloud-based virus scanning service designed to analyze email attachments with most MIME types in a separate, secured cloud environment. This advanced scanning detects new threats and determines whether to block such messages, enhancing the security of your email communications.

- **Default**: Scan First, then Deliver
- **Recommended**: Scan First, then Deliver

ATP Exemptions

While ATP exemptions are available, it is strongly recommended to minimize their use. If you believe an ATP exemption is necessary, please ensure the following:

1. **Verify Attachment Status**: Confirm that the attachment was **Not Delivered**. Often, attachments are deferred for **Pending Scan** but are delivered upon sender retry. Use the **Show Message History** button when reviewing messages that show as **Pending Scan** to ensure accurate status.

2. **Use IP Addresses Over Domains/Emails**: If an exemption is required, use an IP address instead of a domain or email address. Exempting a domain or email can be risky, as it allows anyone sending from that domain or email to bypass malware scanning.

3. **Never Exempt Your Own Domain**: Exempting your own domain can create significant security vulnerabilities and should be avoided.

USERS

Within email security, we always talk about defense in depth and the need for multiple layers. Your users are viewed as the “human firewall” layer and are the last line of defense against any attack. Just like we integrate the Barracuda layers, we also need to integrate the human layer. The best way to do this is through Email Gateway Defense (EGD).

There are several ways that users can engage with EGD:

1. **Outlook Add-in**:
    - The Outlook add-in, which is deployed from the Microsoft app store, allows end users to report suspicious or unwanted messages directly from Outlook. The Outlook add-in integrates with Barracuda’s threat platform, as well as your Incident Response and Awareness Training tenants.
2. **Quarantine Digest Email:**
    - Provides a digest of quarantined emails received since the previous digest was sent out. Users can allow or block the sender and release the held message directly from the digest.
3. **Web UI:**
    - Users can seamlessly access the Barracuda web portal, where they have full message log and policy options at their disposal.

Each of these requires some level of training/enablement for the end user so they are familiar with the tools and understand how to use them effectively and efficiently.

Leveraging the end user quarantine digest will give you a way to limit distractions caused by certain types of emails, such as bulk or marketing, newsletters, and mailing lists. Additionally, it allows you to tighten up perimeter defenses without worrying so much about a legitimate email getting caught (compared to not having user quarantine, which would require blocking). It’s critical to ensure you train users to recognize the signs of harmful emails since they may end up in the digest occasionally.

USERS LIST

Importance:

The user list is essential for various email security functions and ensures smooth mail flow by synchronizing with either LDAP or AzureAD.

Functions:

1. **Outbound Rate Control**:

   - **Purpose**: Applies rate limits per user to prevent mail flow disruption. Default is 150 messages/30 min per sender.
   - **Example**: Prevents a single user from affecting the entire domain's outbound mail if they exceed rate limits.

2. **User Quarantine**:

   - **Purpose**: Allows the quarantine digest schedules to be enabled for users.

3. **Recipient Verification:**

   - **Purpose**: Provides proper recipient verification for inbound mail in rare cases where the mail server cannot handle it.
   - For more information, see Recipient Verification

4. **End User Access:**

   - **Purpose**: Provides an account in which the end user can manage their emails and allowed/blocked sender list.

Policies:

1. **Default Policy:**

   - **Managed Users:** Users found on the user list
     - **Default:** Scan
     - **Recommended:** Scan
   - **Unmanaged Users:** Users not found on the user list
     - **Default:** Scan
     - **Recommended:** Scan
       - **Note:** If recipient verification cannot be done at the mail server, then this will need to be set to **Block**

2. **Exempt Senders**:

    - Gives users the ability to create sender allow policies
    - **Default:** Allow users to exempt senders.
    - **Recommended:** Allow exemptions but do not override admin block lists.

3. **Block Senders:**

    - Gives users the ability to create sender block policies
    - **Default**: Yes
    - **Recommended**: Yes

4. **View and Deliver Blocked Messages:**

    - Allows end users to view/deliver blocked messages from their end user portal
    - **Default**: No
    - **Recommended**: No

5. **View and Deliver Quarantined Messages:**

    - Allows end users to view/deliver quarantined messages from their digest or end user portal
    - **Default**: Yes
    - **Recommended**: Yes

Default Time Zone:

- **Purpose**: Controls the time zone on the message log for both end users and administrators.

Quarantine Messages for Intent Analysis

- **Purpose:** Intent analysis identifies phishing and scam emails
- **Function:** Changes blocked phishing emails to quarantined emails
- **Risk:** Exposes potentially harmful emails to users.
- **Default:** No
- **Recommended:** No

Default Interval for User Quarantine Notifications

- **Function**: Configures automatic digest delivery.
- **Options**: Users can also manage quarantined emails via web UI.
- **Default**: Never
- **Recommended**: Scheduled (1-2 digests per day)

Allow Users to Specify Interval

- **Purpose**: Gives users control over digest frequency.
- **Default**: No
- **Recommended**: Based on customer requirements.

Allow Users to Log In with Temporary Passcodes

- **Purpose**: Enables management of quarantined emails for shared mailboxes/distribution groups.
- **Default**: No
- **Recommended**: If needed

Email Continuity

- **Purpose**: Ensures email functionality when primary mail servers are unavailable.
- **Function**: Allows sending, receiving, composing, and forwarding emails during outages; syncs sent/received mail when services are restored.
- **Default**: Off
- **Recommended**: Auto-Enable (will also enable spooling on all domains if not already enabled)

DOMAIN SETTINGS

Domain Level Settings

- **Purpose**: Useful for managing multiple clients on a single account with different policies.
- **Identification**: Look for the orange indicator on the Domains tab.
- **Policy Identification**: Use keyword search ***reason_extra:domain*** in the message log.
- **Default**: Not configured
- **Recommended**: Not needed for most customers.

Spooling

- **Function**: Spools mail for up to 96 hours if your mail system goes offline, ensuring no email loss.
- **Default**: No
- **Recommended**: Yes
- **Note**: Contact Barracuda Support if more than 96 hours are needed.

Automatically Add Users

- **Function**: Automatically creates user accounts based on email activity for customers without LDAP or AzureAD.
- **Default**: Off

- **Recommended**: Off (use LDAP or AzureAD)
- **Important**: Ensure proper recipient verification to avoid creating invalid user accounts.

Sender Spoof Protection

- **Function**: Blocks inbound emails where the sender's domain matches your domain to prevent spoofing.
- **Default**: Off
- **Recommended**: Off (use DMARC, SPF, and DKIM)
- **Note**: Create sender policy exemptions for necessary external emails but be aware this bypasses all scanning.

SMTP Encryption

- **Function**: Enforces TLS policies for inbound emails. Settings vary by customer requirements.
- **Recommendation**: Configurable based on customer needs.

Encryption Validation

- **Function**: Enables email encryption features after domain validation.
- **Default**: Not validated
- **Recommended**: Validate

- **Features Enabled by Validation:**
  - Add company logo to notification messages.
  - Customize notification message text and subject.
  - Allow recipients to reply to messages.
  - Enable read receipts.

Directory Integration

- **Default**: Off
- **Recommended**: Use LDAP or AzureAD for automatic synchronization and SSO enabled.

RESOURCES

EMAIL GATEWAY DEFENSE IPS:

Region	Network Traffic to EGD	Network Traffic from EGD
Australia (AU)	3.24.133.128/25	3.24.133.128/25

Canada (CA)	15.222.16.128/25	15.222.16.128/25
Germany (DE)	35.157.190.224/27 18.185.115.192/26 18.184.203.224/27	35.157.190.224/27
United Kingdom (UK)	35.176.92.96/27 18.133.136.128/26 18.133.136.96/27	35.176.92.96/27
United States (US)	209.222.80.0/21	209.222.80.0/21

BARRACUDA CLOUD CONTROL ACTIVE DIRECTORY IPS:

- 35.170.131.81
- 54.156.244.63
- 54.209.169.44

BARRACUDA SPF RECORDS:

- AU (Australia): include:spf.ess.au.barracudanetworks.com -all
- CA (Canada): include:spf.ess.ca.barracudanetworks.com -all
- DE (Germany): include:spf.ess.de.barracudanetworks.com -all
- UK (United Kingdom): include:spf.ess.uk.barracudanetworks.com -all
- US (United States): include:spf.ess.barracudanetworks.com -all

CAMPUS ARTICLES

Step 2 - Configure Microsoft 365 for Inbound and Outbound Mail

Moving from Barracuda Email Security Gateway to Email Gateway Defense

User Guides

Enhanced Connectors vs. Mail Flow Rules for Spam Filtering

[How to disable PhishETR override alerts]

[Understanding Inbound and Outbound message flow]

[Self-service domain move]

[How to use DLP and outbound mail encryption]

[Configuring recipient verification]

[Understanding per global, domain and user settings]