GB-OS® 6.2

Mail Proxy

Anti-Spam & Anti-Virus

Feature Guide

MSFG201607-01

Global Technology Associates, Inc.

Global Technology Associates
3361 Rouse Rd, Suite 240
Orlando, FL 32817

Tel: +1.407.380.0220
Fax. +1.407.380.6080
Email: info@gta.com
Web: www.gta.com

Table of Contents

Introduction **1**
About GTA Mail Proxy Features **1**
Features 1
Anti-Spam Requirements 1
Anti-Virus Requirements 1
About GTA's Anti-Spam Subscription Option **2**
Mailshell Anti-Spam Engine 2
Greylisting 2
About GTA's Anti-Virus Feature **3**
Registration & Activation **3**
Activation Codes 3
About this Guide **4**
Conventions 4
Using GTA's Mail Proxy **5**
Enabling the Mail Proxy **5**
Configuring Mail Proxy Policies **6**
Defining Email White (Allow) or Black (Deny) Lists 9
DNS White List 9
Defining a Mail Abuse Prevention System (MAPS) 9
RDNS (Reverse DNS) 10
Anti-Spam Subscription Option **11**
Using Greylisting 11
How Greylisting Works 12
Using Categorization 13
Threshold Values 14
Anti-Virus Feature **15**
Defining Quarantine Objects 16
Viewing Activity **17**
Graphs and Reports **18**
Logging and Email Headers **19**
Email Headers **19**
Firewall Logs **20**
Email Delivered 20
Email Rejected Due to Source or Destination of Policy 20
Email Rejected Due to Exhaustion of Policies 20
Email Rejected Due to Reverse DNS 20
Email Rejected Due to MAPS 20
Email Rejected Due to Invalid Recipient 20
Email Connection Incomplete 20
Email Confirmed Spam by Anti-Spam but Delivered 20
Email Confirmed Spam by Anti-Spam and Quarantined 20
Email Confirmed Spam by Anti-Spam and Rejected 20
Email Postponed by Anti-Spam 21
Email Virus Found by Anti-Virus and Cured Then Delivered 21
Email Virus Found by Anti-Virus but Delivered 21
Email Virus Found by Anti-Virus and Quarantined 21
Email Virus Found by Anti-Virus and Rejected 21
Troubleshooting **22**
Symptoms **22**
Mail Proxy Options Are Disabled 22
Email Quarantine Does Not Work 22
Mail Proxy Rejects Too Little Email 22
Mail Proxy Rejects Too Much Email 23
Mail Proxy Rejects All Email 23

Introduction

About GTA Mail Proxy Features

The Mail Proxy Anti-Virus feature and the Mail Proxy Anti-Spam subscription option allow network administrators to take back control of their email using GTA's full featured solutions. GTA's Anti-Spam and Anti-Virus options provide additional features to the standard GB-OS email proxy — Mail Proxy — by using commercial grade configuration options powered by Mailshell Anti-Spam and an Anti-Virus engine.

Features

- Support for ESMTP EHLO
- Support for ESMTP SIZE commands
- DNS White List
- Mail Abuse Prevention System (MAPS)
- Mail maximum size limit
- Reverse DNS (RDNS) checking

GTA's Anti-Spam features include:

- Adjustable threshold system for spam scoring
- Alteration of the subject line ("tagging") of suspect or verified spam email
- Redirection of spam email to a quarantine email address
- Rejection of email categorized as spam or potential spam
- Adjustable greylisting settings
- Automatic update cycles for up-to-date protection

GTA's Anti-Virus features include:

- Rejection of email containing viruses
- Removal of viruses from email attachments where possible
- Alteration of the subject line ("tagging") of email containing viruses
- Redirection of email containing viruses to a "quarantine" email address
- Automatic update cycles for up-to-date protection

Anti-Spam Requirements

- GB-OS version 3.6 and above.
  - Greylisting is supported in GB-OS version 5.0 and above.
- Web browser and Internet connection.
- GTA Firewall UTM Appliance or GB-Ware product registration.
- Anti-Spam subscription and feature activation code.

Anti-Virus Requirements

- GB-OS version 5.1.2 and above.
- Web browser and Internet connection.
- GTA Firewall UTM Appliance or GB-Ware product registration.
- Valid GTA Support Contract

About GTA's Anti-Spam Subscription Option

The Anti-Spam option uses greylisting to block spam email from reaching your network and the Mailshell Anti-Spam engine to scan and categorize email. The Mailshell Anti-Spam engine uses both local and network-updated Bayesian rules and other statistical models to rate the likelihood of spam email, while greylisting uses sophisticated email proxy settings that has a minimal impact on users.

Mailshell Anti-Spam Engine

The Mailshell Anti-Spam engine uses a combination of technologies to offset known Bayesian weaknesses such as dictionary attacks, spoofed sender addresses, or foreign domains. It also uses SpamCompiler technology to dramatically improve efficiency, especially when thousands of Bayesian rules are used to reach a final decision.

Mailshell Anti-Spam is more accurate than standard open-source Bayesian filters because of proprietary enhancements. As a result, it requires less training time, takes fewer resources, and responds better to adaptive spammers, yet maintains a near-zero rate of false positives.

On other Bayesian systems, adaptive spammers can evade detection by leveraging knowledge of common rule weights on certain words and email constructs. With an awareness of common spammer tricks, Mailshell Anti-Spam improves over traditional Bayesian systems.

The Mailshell Anti-Spam engine combines the results of:

- A bulk message determination
- A reputation rating
- A content rating
- A database of known spammer tricks

This multi-faceted decision-making process tunes the accuracy of GTA's Anti-Spam option. Settings can be fine tuned to accurately categorize suspect or confirmed spam. Anti-Spam automatically updates itself periodically with new spam definitions.

Greylisting

In addition to the Mailshell Anti-Spam engine, GTA's Anti-Spam option uses greylisting. Greylisting works under the assumption that legitimate email is sent from servers that adhere to RFC 821, which specifies that well behaved message transfer agents should attempt to retry sending a message should they receive a temporary failure code when attempting a delivery.

When greylisting is enabled, the email proxy will temporarily reject any email it does not recognize as a trusted source. If the rejected email is legitimate, the server from which the email originated from will attempt to re-send the email, at which time it will be accepted by the email proxy. A majority of spam is sent from applications that are designed to "fire and forget", meaning the application sends the spam message, but never attempts to retry if a temporary failure code is received. Greylisting takes advantages of this, and blocks mail sent by "fire and forget" applications before they reach the email server.

About GTA's Anti-Virus Feature

The Anti-Virus feature uses an anti-virus engine to scan email. Rather than mere pattern matching, common to most anti-virus software, the anti-virus engine also employs behavior heuristics to catch attacks that may not yet have virus definitions, or whose behavior is by definition randomized to disguise the attack.

It detects viruses, worms, trojans and other malicious programs according to a database of nearly 100,000 current definitions, but also uses algorithmic detection, looking for common email attack patterns such as repeated nested file compression characteristic of email bombs.

GTA's Anti-Virus feature will scan email when enabled. If it is not set to reject email containing viruses, any virus email capable of being cleansed will have the virus removed, and the email message will be delivered or quarantined according to the set policy.

Anti-Virus automatically updates itself periodically with new virus definitions to keep you current.

Registration & Activation

If you have not yet registered your firewall products, go to the GTA Online Support Center (https://www.gta.com/support/center/login/). In the login screen, enter your user ID and password. Click the **Register Product** link and enter your product serial numbers and firewall activation (unlock) codes, then click **Submit**.

If you do not already have a GTA Online Support Center account, click the **Create an Account Now!** link on the GTA Online Support Center login screen.

Activation Codes

Anti-Spam, a subscription option for GB-OS, requires an activation code. Anti-Virus is available with a valid support contract.

The feature activation code can be found in **View Your Registered Products** on the GTA Online Support Center by selecting the serial number of your GTA Firewall UTM Appliance. Copy the feature activation code and enter it in the **Configure>System>Activation Codes** screen in the next available row. Click **Save** to apply the activation code.

Note

If the feature activation codes do not appear in your GTA Online Support Center account, please contact GTA support via email, and put your serial number and Support Center User ID in the message subject.

About this Guide

This feature guide is a supplement to the *GB-OS User's Guide*. It includes a description of configuration of GTA's Mail subscription options as well as information about the configuration of standard Mail Proxy email features.

Organization of the chapters in this feature guide reflects the configuration order for the Anti-Spam subscription option and Anti-Virus feature. For the location of specific topics, please see the table of contents.

Conventions

A few conventions are used in this guide to help you recognize specific elements of the text. If you are viewing this guide in PDF format, color variations may also be used to emphasize notes, warnings and new sections.

Bold Italics	Emphasis
Italics	Publications
Blue Underline	Clickable hyperlink (email address, Web site or in-PDF link)
SMALL CAPS	On-screen field names
`Monospace Font`	On-screen text
Condensed Bold	On-screen menus, menu items
BOLD SMALL CAPS	On-screen buttons, links

Using GTA's Mail Proxy

To use GTA's Mail Proxy, the email proxy must be enabled and DNS must be available from the firewall's DNS Proxy, DNS Service or from a separate DNS server. Additionally, access to the Internet over port 443 (SSL) must not be blocked.

The email proxy requires at least one address object of type Mail Proxy to indicate the destination of processed email. This address object typically contains a primary and secondary internal email server, in that order. IP address ranges and regular expressions will be ignored, and may not be used in this address object. To prevent errors and time delays related to DNS, IP addresses should be used instead of domain names for email server addresses.

The Anti-Virus feature and Anti-Spam subscription option are enabled on a per-policy basis. If you wish to process ***all*** email using Anti-Spam or Anti-Virus, be sure they are enabled for every Mail Proxy Policy. Conversely, you may white list or black list only some email, thus bypassing other Mail Proxy option restrictions, by setting the appropriate Mail Proxy policy.

Note

The Anti-Spam and Anti-Virus options must have an Internet connection to function correctly. The services update themselves with new spam and virus definitions by using an encrypted connection (SSL) over TCP port 443 to contact GTA's servers. If Anti-Spam and Anti-Virus do not have a valid route to GTA servers over the Internet, it will be disabled.

Enabling the Mail Proxy

In order to use the standard Mail Proxy or the optional Anti-Spam or Anti-Virus, the mail proxy must be enabled.

1. Navigate to **Configure>Threat Management>Mail Proxy>Proxy**.
2. Check the Enable checkbox.
3. Under Connections, define how long an idle connection to an email server should remain active, as well as the maximum number of simultaneous connections Mail Proxy should allow.
4. Advanced options provide the ability to enable or disable automatic policies as well as logging and reporting of Mail Proxy data.

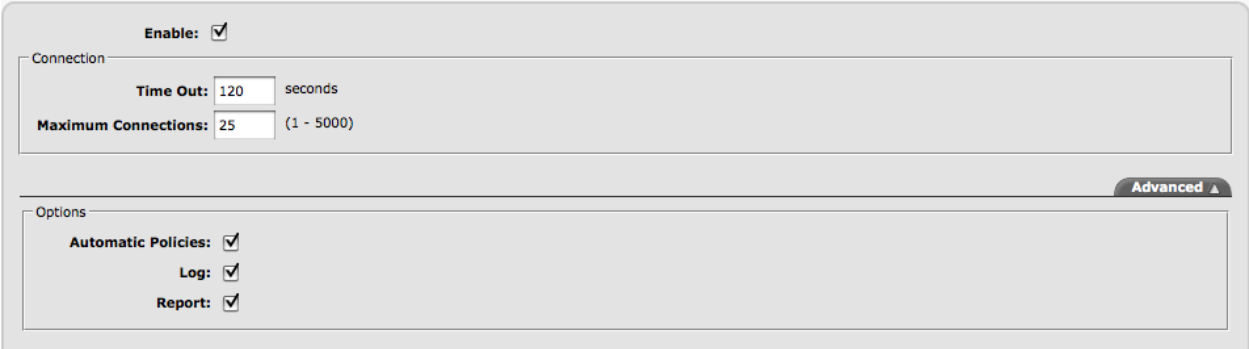

Figure 1: *Enabling the Mail Proxy*

Table 1: Enabling the Mail Proxy	
Field	**Description**
Enable	A toggle to enable the mail proxy.
Connection	
Time Out	The amount of time, in seconds, before the connection will time out.
Maximum Connections	The number of simultaneously allowed connections. The maximum number of connections for GB-250, GB-820, and GB-Ware 10 user license is 50. GB-2100 has a maximum of 1000 connections and GB-2500 and GB-Ware Enterprise have a maximum number of 5000 connections.
Advanced	
Options	
Automatic Policies	Enables GB-OS to automatically configure the necessary security policies to allow Mail Proxy to operate.
Log	Enables Mail Proxy logging.
Report	Enables saving of Mail Proxy data for Reports.

Configuring Mail Proxy Policies

With every email message, Mail Proxy must choose to accept or deny transmission. Mail Proxy policies contain the criteria that cause an email to be accepted or denied (much like white lists and black lists), and can define the destination server. Policies also contain Anti-Spam and Anti-Virus options which you may apply on a per-policy basis.

By default, the email proxy denies all email. This default will be enacted if an email does not match any listed policy. To ensure that email is not rejected by default, at least one policy of type **<Accept>** must be created.

Mail Proxy policies also contain Anti-Spam subscription options and Anti-Virus features which you may apply on a per-policy basis. The Anti-Spam subscription option must be purchased separately. To purchase the Anti-Spam subscription option, please contact a GTA Channel Partner or GTA Sales. If you have already purchased a subscription, you must enter your activation code in the **Configure>System>Activation Codes** section to activate your subscription.

Note

Mail Proxy policies are evaluated in the order in which they are listed. When the email proxy receives an email, policies are each tested for matching conditions. Once an email property is matched with a policy indicating acceptance or denial, that policy action is performed and no further policies will be tested for matching. If the policy list has been exhausted but no match has been found, the email will be rejected.

Policies accept or deny email based upon address objects, reverse DNS, message size, mail exchange (MX) or mail abuse prevention system (MAPS) criteria. Using multiple policies in conjunction can sort email types to different destination SMTP servers.

When considering the destination domain for a policy match, three cases arise:

- No email recipients match the policy's destination domain
- One or more email recipients match the policy's destination domain
- All the email recipients match the policy's destination domain

If no email recipients match, Mail Proxy checks the next policy for a match. Behavior for the other two cases is controlled by the MATCH ALL ADDRESSES check box: when unchecked, any one or more matching email recipients will cause a policy match, but when checked, all of the email recipients must match to cause a policy match.

To create a new Mail Proxy policy, navigate to **Configure>Threat Management>Mail Proxy>Policies** and click the **NEW** icon.

Note

To accept or reject email regardless of their file size, enter 0 (zero) as the maximum file size in your Mail Proxy policy. A maximum size of zero does not mean that only email with no file size will be considered; instead, it means that the size limit consideration has been removed from the policy.

CAUTION

The IP address receiving email from the Mail Proxy should not simultaneously have an inbound tunnel on TCP port 25 because this will bypass the email proxy, and could compromise your security.

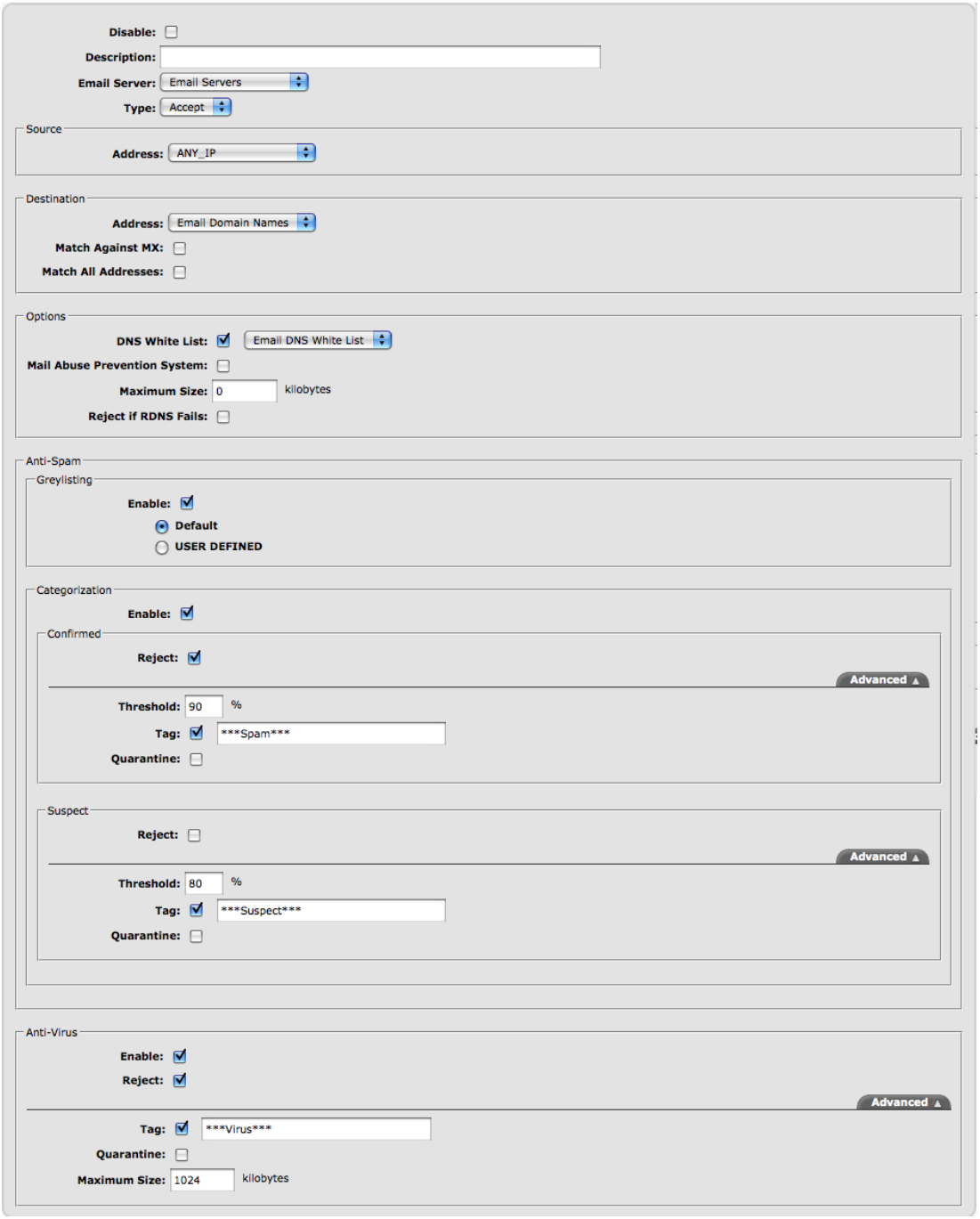

Figure 2: *Configuring Mail Proxy Policies*

Table 2: Configuring Mail Proxy Policies	
Field	**Description**
Disable	Disables the configured Mail Proxy policy.
Description	Enter a description to explain the function of the policy.
Email Server	Specifies which email server should receive email if the policy's criteria has been matched.
Type	Specifies the action that should be done to an email matching the source, destination and other criteria. **<Accept>** allows transmission while **<Deny>** disallows it.
Source	
Address	Specifies a source (sender) match criteria for email. Only address objects of type ALL or MAIL PROXY are available for selection.
Destination	
Address	Specifies a destination (recipient) match criteria for email.
Match Against MX	Makes a DNS MX (Mail Exchanger) recorded query that tries to match the target IP address to the recipient in the SMTP mail header. The email is rejected if there is no match, preventing the domain from being used to relay email to other domains.
Match All Addresses	If checked, the policy will match only if all email recipients contain the destination address. If unchecked, the policy will match if any one or more email recipients contain the destination address.
Options	
DNS White List	Select the check box to enable the DNS white list and then select an address object.
Mail Abuse Prevention System	MAPS; a special DNS server that contains only reverse DNS entries of known spam servers.
Maximum Size	The maximum size (in kilobytes) of an email message to be accepted. Configuring a maximum size can prevent "email bombs" (large attachments that cause problems for email clients). Enter a value of 0 to allow any email message size.
Reject if RDNS Fails	If enabled, the policy will perform a Reverse DNS lookup on the remote host and refuse the connection if the lookup fails to match the host's offered identity.
Anti-Spam *	
Enable	Enables the Anti-Spam service.
Anti-Spam - Confirmed *	
Reject	Rejects email evaluated as confirmed spam if enabled.
Anti-Spam - Suspect *	
Reject	Rejects email evaluated as suspect spam if enabled.
Anti-Virus	
Enable	Enables the Anti-Virus service.
Reject	Rejects email containing known viruses if enabled.

*The Anti-Spam subscription option is purchased separately. Feature activation codes must be entered before Anti-Spam can be utilized.

Defining Email White (Allow) or Black (Deny) Lists

White lists and black lists consist of policies set to unconditionally accept or deny connections from a group of email servers. For example, you may wish to white list the email server of a known business partner to accept all email from that IP, or black list a known spam server to reject all email from that IP.

To define a white (allow) or black (deny) list:

1. Create an address object of type Mail Proxy (you may use the pre-defined white list and black list defaults as templates).
2. Add the IP addresses from which you want to accept or deny transmissions and save the object.
3. Save the address object.
4. Create a Mail Proxy policy that specifies an accept or deny action for that address object. Click the **OK** and then the **Save** button.

To ensure that your white list or black list has priority over other policy rules, place it at the top of your Mail Proxy policy list.

White listing or black listing by source, destination, or a combination of the two may have very different effects. For example, black listing a sender (source) will prevent everyone on your network from receiving email from that source; however, setting a destination of `employee@example.com` in addition to a source will block email from that source only when it is sent to `employee@example.com`. Conversely, setting a white list for all email with a destination of `sales@example.com` would allow anyone to email that address, but allow you to black list sources sending to any other destination in subsequent policies. A combination of policy order (priority) and source and/or destination contents can provide for complex email accept and deny rules.

DNS White List

The DNS White List is a list of trusted email servers. If the Mail Proxy policy is configured to use a DNS white list, the firewall will query the defined white list server. If a Trust Level of **High** or **Medium** is returned, the email will not have greylisting applied and will not be processed against anti-spam categorization. The use of the DNS White List option speeds up email processing by skipping greylisting and anti-spam scanning. Anti-virus scanning is still applied to email.

DNS white list Trust Levels are: High, Medium, Low and None.

The default GTA Email White list is **DNS White List**, containing list.dnswl.org via http://dnswl.org.

Defining a Mail Abuse Prevention System (MAPS)

When deciding to accept or reject email, you may wish to check the message for criteria known to a Mail Abuse Prevention System (MAPS). When validating email connections, you may use one of the pre-defined MAPS or specify a custom MAPS by using an Email Abuse type address object.

A custom MAPS object may refer to a MAPS provider (such as zen.spamhouse.org and list.dsbl.org) or to your own MAPS server. A MAPS server is a DNS server whose reverse DNS entries are spam servers. Any name resolved by the MAPS server therefore indicates that the email originated from a spam server. Additional information on creating your own MAPS server or subscribing to MAPS services is available from many sources.

To specify which address object to use as a MAPS, select an object from the pull-down menu labeled Mail Abuse Prevention System under the Email To Block heading in your Mail Proxy policy.

To define a custom MAPS solution:

1. Create an address object of type Mail Proxy and name it `MAPS server`.
2. Specify your domain name or IP address under the Address field and add a Description if you wish. Note that you can define multiple MAPS servers in a single address object; this can be useful if the first MAPS is slow or unresponsive.
3. Save the address object.

In the Mail Proxy policy, select the Mail Abuse Prevention System toggle and select the previously defined address object. To finalize your MAPS object definition, click the OK and then the Save button.

RDNS (Reverse DNS)

Selecting the REJECT IF RDNS FAILS check box can prevent the reception of spoofed or spam email. It performs a reverse DNS lookup on the IP address of the remote host trying to make an SMTP connection, and then compares it to a DNS lookup of the offered host name. If the lookup fails or domain name and IP address records don't match (as may be the case with illegitimate mail servers), the connection is refused. RDNS requires a defined DNS server to function correctly.

Note

If REJECT IF RDNS FAILED is selected, legitimate hosts with misconfigured DNS entries will not be able to deliver email to your domain.

Anti-Spam Subscription Option

If you have purchased the Anti-Spam option for your firewall, you may apply it to your Mail Proxy policies. Verify Internet access on TCP port 443 (SSL) is not blocked in order to allow the Anti-Spam option to receive automatic authorization and definition updates.

To enable the use of Anti-Spam:

1. Navigate to **Configure>Threat Management>Mail Proxy>Policies** and click New.
2. In the Greylisting box in the Anti-Spam section, check the Enable checkbox to use defined Greylisting settings.
3. In the Categorization box in the Anti-Spam section, check the Enable checkbox and Confirmed and Suspect spam settings as desired.

Using Greylisting

Greylisting is designed to complement Anti-Spam's category based spam filtering. Greylisting takes advantage of the standards set forth by RFC 2821, which defines the acceptable behavior of a message transfer agent (MTA). RFC 2821 specifies that a MTA should retry sending a message should it receive a temporary failure code for a delivery attempt. The majority of known spammers use applications for delivering spam that "fire and forget", meaning they never attempt to re-send a message if the original delivery attempt fails. Greylisting effectively blocks these spam emails while allowing legitimate email to come through. Using greylisting in conjunction with Anti-Spam's categorization features creates a robust anti-spam solution.

Greylisting is applied on a per-policy basis. To enable greylisting for a Mail Proxy policy, select the Enable checkbox in the Greylisting section of the Anti-Spam box of the Mail Proxy policy. By default, Anti-Spam uses settings that should integrate well with most networks. Customized greylisting settings can be defined by selecting the **User Defined** radio button and entering settings as desired.

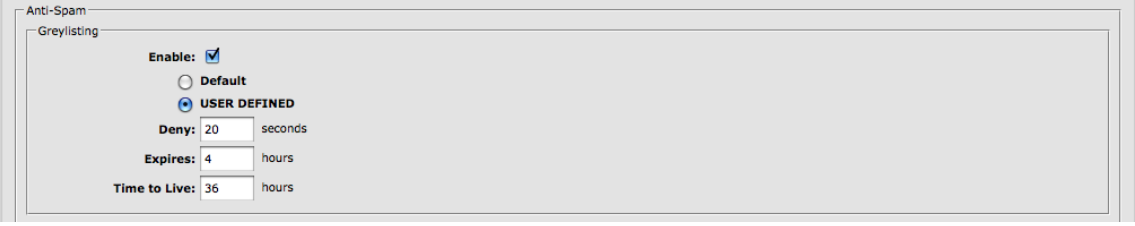

Figure 3: *User Defined Greylisting Settings*

Table 3: Defining Anti-Spam Options

Field	Description
Greylisting	
Enable	Enables greylisting. Requires the entry of a Anti-Spam activation code. Select Default or User Defined.
Deny	The amount of time before the Mail Proxy will accept a repeat delivery attempt from the originating mail server. Default is 20 seconds.
Expires	The amount of time until the Mail Proxy stops waiting for a repeat delivery attempt from the originating mail server. Default is 4 hours.
Time to Live	The amount of time that the Mail Proxy will keep a record of the connection. Default is 36 hours.

CAUTION

Setting a large Time to Live value may result in excessive database usage.

How Greylisting Works

When greylisting is enabled, Anti-Spam tracks three data items (referred to as a “triplet”):

1. The IP address the email originated from
2. The email’s sender address
3. The email’s recipient address

Using this triplet, greylisting follows a simple rule:

> If the triplet has never been encountered before, then the email proxy will refuse the delivery and any subsequent deliveries that may arrive within a certain period of time by responding with a ‘451, please try again later’ message.

To implement greylisting, Anti-Spam uses a database that tracks the following information in relationship to the triplet:

- The time the triplet was first encountered
- The time at which the blocking of the triplet will expire
- The number of delivery attempts that have been blocked
- The number of emails that have been allowed
- The time at which the record of the triplet will expire

When an email arrives at the mail proxy, it is checked against the greylisting database. If the triplet has never been encountered before, Anti-Spam will make a record of it and send a temporary failure code to the originating server. Anti-Spam assumes that the originating server adheres to RFC guidelines, meaning a legitimate email server will attempt to connect again to re-deliver the email, while the majority of spam email applications and servers will ignore the temporary failure code. When the originating email server re-sends the email after the temporary block on the triplet has expired, Anti-Spam will deliver the email to its recipient.

Note

When using greylisting, there is the possibility that email sent from poorly configured email servers may be permanently blocked. This can be prevented by creating and using white lists.

GB-OS contains a default, built-in address object named Email Greylisting that contains known, legitimate email servers that do not comply with RFC 2821 guidelines.

The following illustrates the logic behind the email proxy when greylisting is enabled in a Mail Proxy policy:

1. Check if the email’s sender is white listed. If the email’s sender is white listed, deliver the email.
2. Check if the email’s recipient is white listed. If the email’s recipient is white listed, deliver the email.
3. Check if the email’s triplet has been stored in the database.
   - If a record of the triplet does not exist, create a record in the database and return a temporary failure code.
   - If a record of the triplet does exist, and the temporary block has not expired, return a temporary failure code.
   - If a record of the triplet does exist, and the temporary block has expired, deliver the email.

Mail Proxy provides default greylisting settings that should block most spam email while allowing legitimate email to be delivered. These default settings can be adjusted to more accurately match your organization’s email requirements by navigating to **Configure>Threat Management>Mail Proxy>Proxy**, selecting the **User Defined** toggle and entering settings as desired.

Using Categorization

During the mail filtering process, Anti-Spam will evaluate email for spam content, and reject, tag or quarantine email that fits your policies. If spam status for a message is uncertain (“Suspect”), Anti-Spam can also reject, tag or quarantine that message as well.

You may specify whether to reject, tag or quarantine email according to its threshold group (“Confirmed” or “Suspect”). All email with a spam score lower than the Suspect threshold will be considered valid email, and will be delivered normally.

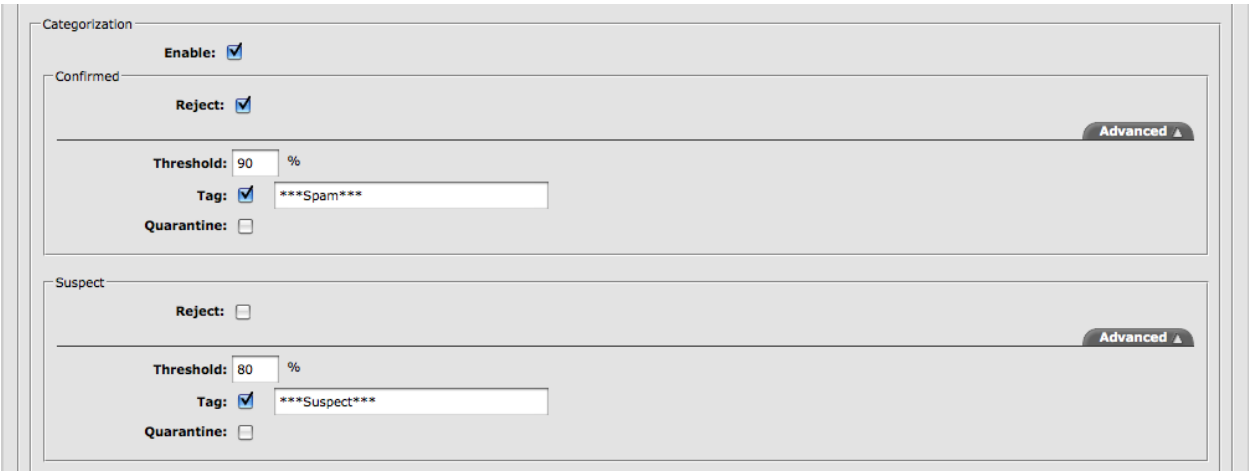

Figure 4: *Configuring Anti-Spam Categorization*

Table 4: Configuring Anti-Spam Categorization	
Field	**Description**
Categorization	
Enable	Enables Anti-Spam categorization. Requires the entry of a Anti-Spam activation code.
Confirmed	
Reject	When enabled, Anti-Spam will reject confirmed spam.
Advanced	
Threshold	Enter the score email must receive before being categorized as confirmed spam. Higher scores are more tolerant of spam-like qualities. See Threshold Scores for more information.
Tag	When enabled, the message subject of confirmed spam will be tagged with the entered string.
Quarantine	When enabled, confirmed spam will be redirected to the entered email address. See Defining Quarantine Objects for more information.
Suspect	
Reject	When enabled, Anti-Spam will reject suspected spam.
Advanced	
Threshold	Enter the score email must receive before being categorized as suspected spam. Higher scores are more tolerant of spam-like qualities. See Threshold Scores for more information.
Tag	When enabled, the message subject of suspected spam will be tagged with the entered string.
Quarantine	When enabled, suspected spam will be redirected to the entered email address. See Defining Quarantine Objects for more information.

When configuring Anti-Spam options, keep in mind:

- Rejecting an email will send a '501 Rejected as spam' message to the sender.
- Quarantining an email will not send it to its destination. Instead, it will be sent to a new email address for review, from where valid email can be re-sent to their intended destinations, and spam email can be deleted.
- Tagging an email's subject line can be used in conjunction with, or instead of, a quarantine. Tagging allows the end user final discretion over the spam status of a message; client email programs may apply rules that, for example, put all email tagged with `***SUSPECT***` into a folder called "Potential Spam."

CAUTION

Allowing end users to read spam email can pose a serious security risk to your network, and is not suggested by GTA. Such email may be fraudulent ("spoofed"), contain illegal content, contain viruses, or contain content intended to coerce money or sensitive information from users.

To tag the subject line of confirmed or suspected spam, check the **TAG** option and specify text that will act as the tag. For example, `***SPAM***` might be a useful tag for spam email.

To quarantine an email, check the **QUARANTINE** option and choose a quarantine object. (To define a quarantine object, create a new address object of type MAIL PROXY containing only your quarantine email address, e.g. spam-quarantine@example.com.)

To reject an email entirely and return a '501 Rejected as spam' signal to the sender, check the **REJECT** option.

Threshold Values

Anti-Spam scores email on a scale from 1 to 100 that rates the probability of the email being spam, with 100 being most spam-like. Thresholds determine what spam score an email must receive before being marked as spam ("Confirmed") or suspiciously spam-like ("Suspect"). For example, high threshold numbers mean that an email must have a high score to be marked as spam or spam-like.

Anti-Spam provides reasonable default spam threshold scores for spam detection: 90 for confirmed and 80 for suspect. However, you may customize the score to be as permissive or restrictive as is necessary. For more permissive email filtering, choose a high threshold value. For more restrictive email filtering, choose a low threshold value.

Table 5: Anti-Spam Threshold Values

Value Range	Description
90-99	Lenient spam catching. Most email will be delivered normally, but this may also allow a significant amount of spam.
80-89	Moderate spam catching. Many spam messages will be marked, but a few spam-like normal email ("false positives") may also be marked.
60-79	Aggressive spam catching. Most spam will be marked, but spam-like normal email ("false positives") may also be marked.
1-59	Extremely aggressive spam catching. Almost all spam will be marked, but a significant amount of normal email ("false positives") may also be marked. This threshold range is not recommended for normal use.
0	Exclusive spam catching. All email not on the list of Mailshell approved senders will be treated as spam. This threshold is not recommended for normal use.

Anti-Virus Feature

When applying Anti-Virus settings to your Mail Proxy policies, Verify Internet access on TCP port 443 (SSL) is not blocked in order to allow the Anti-Virus feature can receive automatic authorization and definition updates.

To enable the use of Anti-Virus:

1. Navigate to **Configure>Threat Management>Mail Proxy>Policies** and click NEW.
2. In the ANTI-VIRUS box, check the ENABLE checkbox and configure the policy as desired.

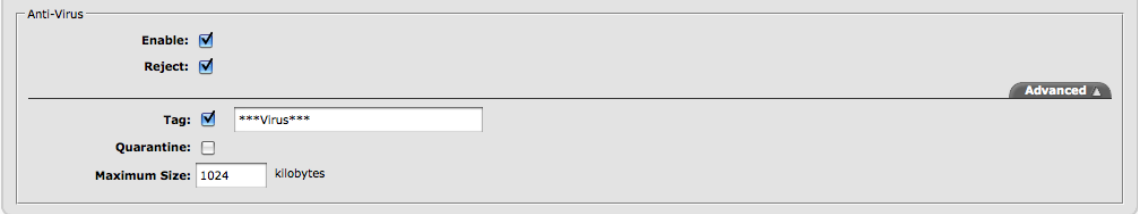

Figure 5: *Defining Anti-Virus Options*

Table 6: Defining Anti-Virus	
Field	**Description**
Enable	Enables Anti-Virus.
Reject	If enabled, all email containing known viruses will be rejected.
Advanced	
Tag	If enabled, email containing known viruses will be tagged with the configured text field.
Quarantine	If enabled, select the address object of type Mail Proxy that contains the email address that should receive quarantined (redirected) email. See Defining Quarantine Objects for more information.
Maximum Size	Maximum size in kilobytes (KB) of email message to scan for viruses. If this value is lower than the Mail Proxy policy's Maximum Size, email may not be fully scanned for viruses. The default, 0, will scan any size email.

During the email filtering process, Anti-Virus will evaluate email for virus content, and reject, tag or quarantine email that fits your definitions. It compares email attachments to a database of approximately 100,000 current virus definitions.

Because anti-virus scanning is a time-intensive procedure, it can effect the performance of your firewall's mail proxy. To improve performance, you may wish to specify the maximum size of an email that will be accepted for scanning – the smaller the accepted email size, the better your email proxy throughput will be. Any email over this maximum size will be delivered normally; any email under this size will be scanned and evaluated for virus status. To specify the largest acceptable email file size, edit the size in kilobytes (KB) in the MAXIMUM SIZE field.

CAUTION

If the maximum size of email accepted for processing by a Mail Proxy policy is greater than the maximum size indicated for Anti-Virus processing, email will be delivered without being completely scanned. This poses a serious threat to your network security, and is not recommended by GTA.

To reject all email that is too large to be completely scanned, make the Anti-Virus and general Mail Proxy policy maximum size threshold values identical, or set the Anti-Virus maximum size to 0 (zero) to scan all email regardless of size.

If an email has been categorized as containing a virus, you can choose to reject the email, tag its subject line, or quarantine the email. If scanned email contains a virus but you have not chosen to reject it, Anti-Virus will attempt to remove the virus before delivering the email; if successful in virus removal, the phrase "cured" will be added to the `X-GB-AV` email header.

When configuring Anti-Virus, keep in mind:

- Rejecting an email will send a '501 Rejected, contains virus' signal to the sender.
- Quarantining an email will not send it to its destination; instead, it will be sent to a new email address for review, from where valid email can be re-sent to their intended destinations, and virus email can be deleted.
- Tagging an email's subject line can be used in conjunction with, or instead of, a quarantine. Tagging allows the end user final discretion over the virus status of a message; client email programs may apply rules, for example, that put all email tagged with "***VIRUS***" into a folder called "VIRUS." Then the end user can choose to read or delete the tagged email according to individual preference.

CAUTION

Allowing end users to read email containing viruses poses a serious security risk to your network, and is not recommended by GTA. Choose the **REJECT** or **QUARANTINE** option to reject or quarantine all scanned email that contains a known virus.

- To **tag** the subject line of a virus email, check the **TAG** option and specify text that will act as the tag. For example, `***VIRUS***` might be a useful tag for virus email.
- To **quarantine** an email, check the **QUARANTINE** option and choose a quarantine object. (To define a quarantine object, create a new address object of type MAIL PROXY containing only your quarantine email address, e.g. virus-quarantine@example.com .)
- To **reject** an email entirely and send a '501 Rejected, contains virus' signal to the sender, check the **REJECT** option.

Defining Quarantine Objects

It is often useful to set up an email account to receive quarantined email before configuring Mail Proxy optional features, e.g. quarantine@example.com. Defining a quarantine object allows Mail Proxy configuration to refer to this email account.

When using Anti-Spam or Anti-Virus, you may redirect suspect spam or virus email to an administrator's email account, thereby allowing analysis of problem email. (It may be useful, for example, to analyze `X-GB-Received` email headers to add persistent spam servers to a black list Mail Proxy policy on your firewall.)

Redirect (quarantine) email by providing the email proxy with a quarantine email address in the form of an address object for each category of scanned email. You may wish to make separate quarantine objects, one for each category of email you quarantine (e.g. virus-quarantine@example.com, confirmed-quarantine@example.com, suspect-quarantine@example.com).

To define a quarantine object:

1. Navigate to **Configure>System>Object Editor>Address Objects**.
2. Create a new address object of type MAIL PROXY containing only your quarantine email address, e.g. `spam _ quarantine@example.com`.
3. Give a name and description appropriate to the type of email that the quarantine email address will receive.
4. Click the **OK** button, then the **SAVE** button.

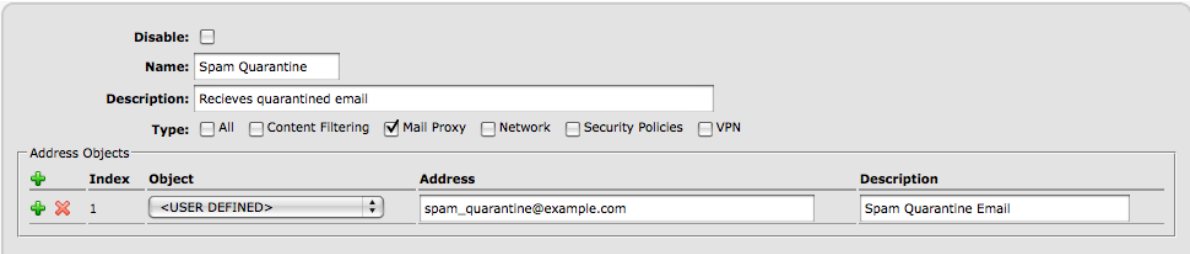

Figure 6: *Defining Quarantine Objects*

Viewing Activity

Mail Proxy statistics, such as SMTP proxy connections and email processing, can be viewed in a concise format. These statistics can be viewed by navigating to **Monitor>Activity>Threat Management>Mail Proxy**.

Inside the Mail Proxy menu are three options:

- **Anti-Spam:** The **Greylisting** sub-menu tracks usage and contains a tabular display of all data related to triplets currently stored in the Anti-Spam database. The **Statistics** sub-menu contains a statistical summary on the number of processed emails with spam, number of rejected emails that are both suspected and confirmed, number of quarantined emails that are both suspected and confirmed as well as the total number of received emails of unknown status.
- **Statistics:** Contains a statistical summary which includes fields describing total connections, rejected and timed-out connections, as well as email processed by the Mail Proxy's policies.
- **Anti-Virus:** Contains a statistical summary on the number of processed emails with viruses, number of rejected emails, number of quarantined emails as well as the total number of confirmed viruses.

Note

Anti-Spam activities will not be available unless the associated subscription has been purchased and activated.

Statistics and data displayed are a static snapshot of current Mail Proxy activity. If you wish to update the list, click the **Refresh** icon.

Rejected email are those for which a '501 Rejected as spam', '501 Rejected, contains virus ' or '451, please try again later' signal has been returned to the sender. Quarantined email are those that have been sent to a quarantine email address. Other email are delivered normally.

Percentages are relative to the total for the section. For example, the percentage of rejected Confirmed spam email is relative to the total number of email processed by Anti-Spam - not relative to the total number of email processed by the email proxy as a whole.

Policy statistics assist troubleshooting by indicating the count of messages that triggered a Mail Proxy policy of a given index number. The index and description columns describe which policy was triggered by email of the given number (count).

Note

Not all email processed by the email proxy are necessarily processed by Anti-Spam or Anti-Virus (unless every Mail Proxy policy has Anti-Spam or Anti-Virus enabled), so these email totals may not be equivalent

Graphs and Reports

Graphical data is available for Mail Proxy at **Monitor>Reporting>Graphs>Mail Proxy**. Hourly, Daily, Weekly, Monthly and Yearly data is displayed for rejected and allowed email.

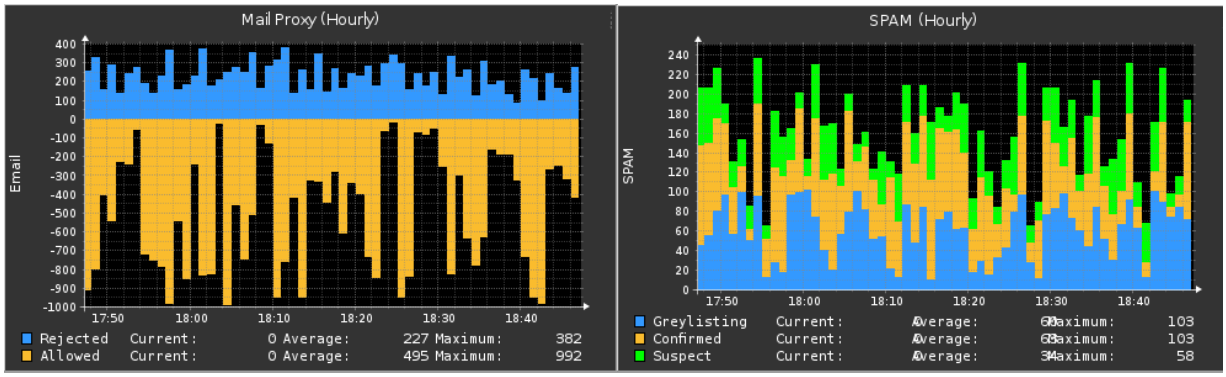

Figure 7: *Mail Proxy and Anti-Spam Hourly Graphs*

Mail Proxy reports are available through the firewall at **Monitor>Reporting**. The number of Top reports is based upon the firewall product and available memory.

For more information on scheduling reports, running reports, and report preferences, see the *GB-OS User's Guide* section on Reporting in the Monitoring and Tools chapter.

The following reports are available:

- Mail Proxy - Allowed
  - SMTP Messages by Source and Destination
  - SMTP Traffic by Source and Destination
  - SMTP Messages by Source
  - SMTP Traffic by Source
  - SMTP Messages by Destination
  - SMTP Traffic by Destination
  - SMTP Messages by Recipient
  - SMTP Traffic by Recipient
  - SMTP Messages by Sender
  - SMTP Traffic by Sender
- Mail Proxy - Denied, Anti-Virus
  - Recent Viruses
  - Recent Viruses by Traffic
  - Viruses by Recipient
  - Virus Traffic by Recipient
  - Viruses by Sender
  - Virus Traffic by Sender
- Mail Proxy - Denied, Anti-Spam
  - SPAM Messages by Recipient
  - SPAM Traffic by Recipient
  - SPAM Messages by Sender
  - SPAM Traffic by Sender
- Mail Proxy - Denied, Quarantined
  - Quarantined Messages by Recipient
  - Quarantined Traffic by Recipient
  - Quarantined Messages by Sender
  - Quarantined Traffic by Sender

Logging and Email Headers

Email Headers

Email headers, often invisible to a user unless they view the email source or view it as plain text, contain information about email delivery and processing.

Mail Proxy's email proxy adds additional X-headers to processed email. These headers can help diagnostic or tracking processes. Some X-headers specifically track events of an email proxy that has enabled options.

Email header formats are as follows:

- `X-GB-Mail-Format-Warning : Bad RFC2822 line length (%s)`
  - Describes a badly-formatted email.
- `X-GB-AS: Confirmed (score 98, 0 seconds)`
  - Lists the spam category assigned to the email (e.g. Confirmed, Suspect, or Unknown).
  - Lists the spam score that was assigned to the email. Higher scores reflect more spam-like email attributes. This number may be useful to analyze when adjusting your score thresholds.
  - Lists the processing time for spam status evaluation.
  - May describe any error conditions that occurred during Anti-Spam processing, causing it to not process the email. These errors can include an expired Anti-Spam license or inability to contact the Anti-Spam license server.
- `X-GB-AS-Summary`
  - Contains the Anti-Spam engine processing summary.
- `X-GB-AV`
  - Lists any viruses found; if they could be removed from the email, it will also say "cured".
  - May describe any error conditions that occurred during Anti-Virus processing, causing it to not process the email. These errors can include an expired Anti-Virus license or inability to contact the Anti-Virus license server.
- `X-GB-Quarantined`
  - Lists the email address that a quarantined email was sent to.
- `X-GB-Rule`
  - Lists the ACL that the email matched during processing.
- `X-GB-DNSWL-Trust-Level: High`
  - Lists the DNS White List response, Trust Level High.
- `X-GB-DNSWL-Trust-Level: Medium`
  - Lists the DNS White List response, Trust Level Medium.
- `X-GB-DNSWL-Trust-Level: Low`
  - Lists the DNS White List response, Trust Level Low.
- `X-GB-DNSWL-Trust-Level: None`
  - Lists the DNS White List response, Trust Level None.
- `X-GB-DNSWL-Trust-Level: No response`
  - Lists the DNS White List response, Trust Level no response.

Firewall Logs

Email Delivered

```
Nov 5 12:48:34 pri=5 msg="SMTP: Close" smtp _ action=pass virus="none found"
spam=unknown,2 rule=5 server=192.168.71.1 proto=smtp user="user@example.com"
srcuser="user2@source.com" src=199.120.225.254 srcport=4711 dst=199.120.225.5 dstport=25
duration=2 sent=136 rcvd=1709
```

Email Rejected Due to Source or Destination of Policy

```
Nov 5 03:46:28 mailgate2 id=firewall time="2004-11-05 08:46:28" fw="10000003" pri=4
msg="SMTP: Rejected (rule)" smtp _ action=block rule=6 proto=smtp user="user@example.
com" srcuser="sender@source.com" src=199.120.225.254 srcport=34813 dst=199.120.225.5
dstport=25 duration=2 sent=42 rcvd=67
```

Email Rejected Due to Exhaustion of Policies

Reject by default if no match is found.

```
Nov 5 14:48:15 pri=4 msg="SMTP: Rejected (rule)" smtp _ action=block rule=0 proto=smtp
user="user@example.net" srcuser="sender@source.net" src=199.120.225.254 srcport=2107
dst=199.120.225.5 dstport=25 duration=13 sent=70 rcvd=68
```

Email Rejected Due to Reverse DNS

```
Nov 5 14:31:26 pri=4 msg="SMTP: Rejected (RDNS)" smtp _ action=block rule=1 proto=smtp
user="user@example.com" srcuser="sender@source.com" src=199.120.225.254 srcport=1696
dst=199.120.225.5 dstport=25 duration=10 sent=74 rcvd=60
```

Email Rejected Due to MAPS

```
Nov 5 12:48:09 pri=4 msg="SMTP: Rejected (MAPS list.dsbl.org)" smtp _ action=block rule=2
proto=smtp user="user@example.com,user2@example.com" srcuser="spammer@source.com"
src=199.120.225.254 srcport=2327 dst=199.120.225.5 dstport=25 duration=4 sent=111 rcvd=107
```

Email Rejected Due to Invalid Recipient

```
Nov 8 07:19:55 pri=4 msg="SMTP: Server returned, 550 Invalid recipient <dale@
amcicomputers.com>" type=mgmt proto=smtp user="user@example.com" srcuser="sender@
source.com" src=199.120.225.254 srcport=4599 dst=199.120.225.5 dstport=25 duration=5
```

If there is no spam or virus scanning enabled for that email, you may see that message paired with one for an incomplete SMTP connection. This message occurs when the email data is stopped during transmission. The internal email server may have determined that an email account does not exist, and cause the email proxy to terminate the SMTP data reception.

Email Connection Incomplete

```
Nov 8 07:19:55 pri=4 msg="SMTP: Incomplete" smtp _ action=block virus="not found"
spam=confirmed,96 rule=8 server=192.168.71.1 proto=smtp user="user@example.com"
srcuser="sender@source.com" src=199.120.225.254 srcport=4599 dst=199.120.225.5 dstport=25
duration=5 sent=214 rcvd=2765
```

Email Confirmed Spam by Anti-Spam but Delivered

```
Nov 5 12:47:37 pri=4 msg="SMTP: Close" smtp _ action=pass virus="none found"
spam=confirmed,99 rule=5 server=192.168.71.1 proto=smtp user="user@example.com"
srcuser="spammer@source.com" src=199.120.225.254 srcport=3260 dst=199.120.225.5 dstport=25
duration=4 sent=110 rcvd=3396
```

Email Confirmed Spam by Anti-Spam and Quarantined

```
May 26 14:44:04 pri=4 msg="SMTP: Close" smtp _ action=quarantine virus="none found"
spam=confirmed,98 rule=8 server=192.168.71.1 proto=smtp user="user@example.com"
srcuser="sender@source.com" src=199.120.225.254 srcport=4655 dst=199.120.225.5 dstport=25
duration=2 sent=110 rcvd=1548
```

Email Confirmed Spam by Anti-Spam and Rejected

```
May 26 00:00:07 pri=4 msg="SMTP: Rejected (spam)" smtp _ action=block virus="none found"
spam=confirmed,98 rule=8 proto=smtp user="user@example.com" srcuser="sender@source.
com" src=199.120.225.254 srcport=59954 dst=199.120.225.5 dstport=25 duration=1 sent=120
rcvd=9126
```

Email Postponed by Anti-Spam

```
Mar 9 12:30:08 pri=4 msg="SMTP: Postponed" smtp _ action=block rule=10 proto=smtp
user="user@example.com"; srcuser="sender@source.com"; src=61.231.65.141 srcport=2875
dst=199.120.225.5 dstport=25 duration=2 sent=86 rcvd=97
```

Email Virus Found by Anti-Virus and Cured Then Delivered

```
Nov 5 13:02:24 pri=4 msg="SMTP: Close" smtp _ action=block virus=Cured,"I-Worm.Bagle.
au" spam=unknown,50 rule=5 server=192.168.71.1 proto=smtp user="user@example.com"
srcuser="sender@source.com" src=199.120.225.254 srcport=4124 dst=199.120.225.5 dstport=25
duration=83 sent=82 rcvd=26436
```

Email Virus Found by Anti-Virus but Delivered

```
Nov 5 12:28:27 pri=4 msg="SMTP: Close" smtp _ action=pass virus="I-Worm.Bagle.
as" spam=unknown,64 rule=5 server=192.168.71.1 proto=smtp user="user@example.com"
srcuser="sender@source.com" src=199.120.225.254 srcport=3364 dst=199.120.225.5 dstport=25
duration=10 sent=82 rcvd=31669
```

Email Virus Found by Anti-Virus and Quarantined

```
Nov 5 12:10:00 pri=4 msg="SMTP: Close" smtp _ action= quarantine virus="I-Worm.
NetSky.q" spam=confirmed,98 rule=5 server=192.168.71.1 proto=smtp user="user@example.com"
srcuser="sender@source.com" src=199.120.225.254 srcport=4272 dst=199.120.225.5 dstport=25
duration=5 sent=110 rcvd=41496
```

Email Virus Found by Anti-Virus and Rejected

```
Nov 5 13:02:24 pri=4 msg="SMTP: Close" smtp _ action=block virus="I-Worm.Bagle.
au" spam=unknown,50 rule=5 server=192.168.71.1 proto=smtp user="user@example.com"
srcuser="sender@source.com" src=199.120.225.254 srcport=4124 dst=199.120.225.5 dstport=25
duration=83 sent=82 rcvd=26436
```

Troubleshooting

Log messages, reports and activity snapshots are your first reference for general troubleshooting. This section contains useful troubleshooting procedures and frequently asked questions for solving firewall configuration errors.

Troubleshooting issues discussed in this chapter are specific to Anti-Spam and Anti-Virus. For all other troubleshooting issues regarding your GTA firewall, please refer to the *GB-OS User's Guide*.

Symptoms

Mail Proxy Options Are Disabled

Anti-Spam and Anti-Virus require Internet access over TCP port 443 (SSL) in order to authorize and update from GTA servers. If Mail Proxy cannot access GTA servers (*gta.com) on TCP port 443, or if there is no DNS Proxy or Service enabled, the email proxy may wait for option authentication that it cannot get; if the SSL connection times out, the email proxy will ***disable*** Mail Proxy options and continue processing email according to standard ACL rules.

The proxy will then log that it has disabled Mail Proxy options, and will periodically check for Internet SSL connection restoration. If the connection is restored and feature activation codes are valid, the proxy automatically re-enables those Mail Proxy options that were automatically disabled.

To correct this problem, check that your network allows SSL connections to the Internet over an external network interface (no filtering rules may deny port 443). Use ping and traceroute to verify connectivity to the Internet, including gta.com and its sub-domains, and check all routers that may block Internet SSL access.

Email Quarantine Does Not Work

An email quarantine object must be an address object of type Mail Proxy that contains only a single email address such as "email-quarantine@example.com". It is not valid to enter only the domain name of your email server; your quarantine object must have a full email address that contains an account as well as a domain name. Use of wild card (regular expression) characters is also not allowed.

If you wish to use multiple email addresses as quarantines in different firewall configuration areas, you should create one quarantine address object per quarantine email address. For example, if you wish to separate suspect spam email and virus email, you might create address objects named "Suspect Quarantine" (containing "suspect-quarantine@example.com") and "Virus Quarantine" (containing "virus-quarantine@example.com").

Mail Proxy Rejects Too Little Email

First check that your Mail Proxy policies reject those domains or IP address ranges that are known spam servers. Remember that Mail Proxy policies evaluate in the order they are listed. Make sure that an all-accepting policy is listed underneath those exclusion policies to ensure that every email is not accepted ***before*** being tested for a spam domain.

Check the specific Mail Proxy policy that you expected the email to match for configuration errors that may cause failed matches. Correct configuration errors in any policies before it that may cause a premature match.

To rule out either Anti-Spam or Anti-Virus options as a source of the problem, un-check all of the **ENABLE** check boxes in the Anti-Spam and Anti-Virus sections of your Mail Proxy policies. When you re-enable Anti-Spam and Anti-Virus in each policy, be sure to do it one at a time so you can narrow down the source of the misconfiguration.

Note

The Mail Proxy System Activity reports can provide useful diagnostic information to determine whether Mail Proxy options are causing email rejection.

Indicating a large maximum email file size in either the Email to Block or Anti-Virus sections of your Mail Proxy policy will allow larger email through. To limit the size of email that your firewall accepts for transmission, reduce the maximum file size to a small, non-zero number.

Be sure to allow external Internet access from your firewall to the Internet. Mail Proxy uses various servers to keep its Mail Proxy options up-to-date; if you have routing rules preventing this access, your Mail Proxy options may lapse or use old spam and virus definitions, allowing newer spam and viruses through.

Note

A maximum size of zero ***does not mean*** that only zero-sized email will be considered; instead, it means that the size limit consideration has been removed from the policy, and all files will be considered scanned..

If you notice that some spam email is still not being caught by Anti-Spam, consider adjusting your Anti-Spam threshold to a more aggressive setting. You might also choose to restrict Suspect category email as well as Confirmed category email. Additional use of a MAPS (a kind of real-time black list, or RBL) can also help.

Mail Proxy Rejects Too Much Email

When the firewall evaluates a packet for acceptance or rejection, many rules may be used. It is important to check other rules such as routing rules before investigating Mail Proxy ACL rules.

Remember that Mail Proxy policies evaluate in the order they are listed. Make sure that any white list ACLs are listed above any black list policies to ensure that all email is not rejected before being tested for a known-good email address.

To rule out Mail Proxy optional subscription features as a source of the problem, un-check the Enable options in the Anti-Spam and Anti-Virus sections of your Mail Proxy policies. When you re-enable Anti-Spam and Anti-Virus, be sure to do it one at a time so you can narrow down the source of the misconfiguration.

Note

The Mail Proxy System Activity reports can provide useful diagnostic information to determine whether Mail Proxy options are causing email rejection

Indicating a small maximum email file size is a common cause for rejected email. Indicating a low threshold for too many Anti-Spam categories can also be a common cause.

Mail Proxy Rejects All Email

If your firewall rejects all email, first check to see that email TCP ports (especially the standard SMTP port 25) have not been filtered out in other policies, and that your email proxy is enabled. If your firewall accepts port 25 connections but still rejects all email, check your Mail Proxy policy settings. If your policy is set to reject email fitting your rules and all email matches your rules, all email will be rejected. Make sure you have at least one Mail Proxy policy set to accept email; denial-type policies or an absence of policies will cause email to be rejected.

Note

The Mail Proxy System Activity report can provide useful diagnostic information to determine whether Mail Proxy options or other Mail Proxy policy configurations are causing email rejection.

Additionally, if all email servers are listed on your MAPS, all email could be rejected.

Copyright

© 1996-2016, Global Technology Associates, Incorporated (GTA). All rights reserved.

Except as permitted under copyright law, no part of this manual may be reproduced or distributed in any form or by any means without the prior permission of Global Technology Associates, Incorporated.

Technical Support

GTA includes 30 days “up and running” installation support from the date of purchase. See GTA’s Web site for more information. GTA’s direct customers in the USA should call or email GTA using the telephone and email address below. International customers should contact a local Authorized GTA Channel Partner.

Tel: +1.407.380.0220 **Email:** support@gta.com

Disclaimer

Neither GTA, nor its distributors and dealers, make any warranties or representations, either expressed or implied, as to the software and documentation, including without limitation, the condition of software and implied warranties of its merchantability or fitness for a particular purpose. GTA shall not be liable for any lost profits or for any direct, indirect, incidental, consequential or other damages suffered by licensee or others resulting from the use of the program or arising out of any breach of warranty. GTA further reserves the right to make changes to the specifications of the program and contents of the manual without obligation to notify any person or organization of such changes.

Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation for their use. GTA assumes no responsibility with regard to the performance or use of these products.

Every effort has been made to ensure that the information in this manual is accurate. GTA is not responsible for printing or clerical errors.

Trademarks & Copyrights

GB-OS and GB-Ware are registered trademarks of Global Technology Associates, Incorporated. Global Technology Associates and GTA are service marks of Global Technology Associates, Incorporated.

Microsoft, Internet Explorer, Microsoft SQL and Windows are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe and Adobe Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

UNIX is a registered trademark of The Open Group.

Linux is a registered trademark of Linus Torvalds.

BIND is a trademark of the Internet Systems Consortium, Incorporated and University of California, Berkeley.

WELF and WebTrends are trademarks of NetIQ.

Sun, Sun Microsystems, Solaris and Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Java software may include software licensed from RSA Security, Inc.

Some products contain software licensed from IBM are available at http://oss.software.ibm.com/icu4j/.

Some products include software developed by the OpenSSL Project (http://www.openssl.org/).

All other products are trademarks of their respective companies.

Global Technology Associates, Inc.

3361 Rouse Rd, Suite 240 • Orlando, FL 32817 USA

Tel: +1.407.380.0220 • **Fax**: +1.407.380.6080 • **Web**: http://www.gta.com • **Email**: info@gta.com