Recommended Security Settings - Best Practices Guide

This guide provides a list of recommended SecurityGateway settings to protect against spam, malware, hacking & abuse.

Use Email Authentication

❑ Require SMTP Authentication

SMTP authentication is a security feature that requires a user to authenticate with a valid username and password when an email claims to come from a local user. SecurityGateway can be configured to require SMTP authentication for all mail sent from local users. These settings can be found by navigating to **Security | Anti-Abuse | SMTP Authentication**.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/smtp_authentication.html

❑ Use the IP Shield

The IP Shield is used to associate a domain with IP addresses that are authorized to send mail on behalf of that domain. Enabling the IP Shield and checking the "Check FROM header address against IP Shield database" box can help prevent what one could call "semi-spoofing" (the "MAIL FROM" command contains a non-local email address but the "From" header contains a local address). In SecurityGateway, IP Shield settings are located under **Security | Anti-Abuse | IP Shielding**.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/ip_shielding.html

Protect Sensitive Data from Unauthorized Access

❑ Enable SSL & TLS

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are used to encrypt the connection between email clients and servers, and between sending and receiving email servers during delivery. SSL & TLS settings in SecurityGateway are located under **Setup/Users | System | Encryption**.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/encryption.html

❑ Enable RequireTLS & MTA-STS

RequireTLS allows you to flag messages that must be sent using TLS. If TLS is not possible (or if the parameters of the TLS certificate exchange are unacceptable) messages will be bounced rather than delivered insecurely.

MTA-STS, or Mail Transfer Agent Strict Transport Security, is an email security standard that enforces secure connections between email servers. It ensures emails are delivered using encrypted connections (TLS), preventing potential man-in-the-middle attacks.

These settings are located in SecurityGateway under **Setup/Users | System | Encryption**.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/encryption.html

❑ Use the Secure Messaging Portal to Send Emails Containing Sensitive Data

When an email is sent via the Secure Messaging portal, the recipient receives an email notification that a secure message for them is available, with a link to create a Secure Message Recipient account so that they can view the message located on the SecurityGateway server. The secure message is accessed via the recipient's browser, and end-to-end encryption is maintained between the SecurityGateway server and the recipient via HTTPS encryption.

Knowledge Base Article:
https://knowledge.mdaemon.com/setup-securitygateways-secure-messaging-feature

❑ Use Data Leak Prevention to Protect Against Leaks of Sensitive Data

SecurityGateway includes a variety of data leak prevention rules to block or quarantine outbound emails containing sensitive data such as Social Security numbers, driver's license numbers, and other types of confidential information. These settings can be found in SecurityGateway under **Security | Data Leak Prevention**.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/data_leak_list.html

Protect Against Hacking & Abuse

❑ Don't Allow Open Relay

Relaying (also known as "open relay") is where mail that is neither to nor from a local domain is allow to pass through a mail server or gateway. By default, SecurityGateway does not allow relaying. You can configure exceptions for mail sent from your own domain mail servers. Mail servers that are allowed to relay mail can be exploited by spammers, which can cause your server to end up on a blocklist.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/relay_control.html

❑ Enable AntiVirus

SecurityGateway includes two antivirus engines - Ikarus and ClamAV. We recommend enabling virus scanning under **Security | Anti-Virus | Virus Scanning**. This allows all inbound and outbound email traffic to be scanned for malware.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/virus_scanning.html

We also recommend enabling automatic updates of virus definitions to protect against the latest malware threats.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/configure_updates.html

❑ Enable Dynamic Screening to Protect Against Hackers

Dynamic screening is used to block connections based on their activity - for example, when a given IP address connects too many times in a given time frame, when too many reset (RSET) commands are detected in an attempt to keep a connection open, or when too many invalid recipients are detected in a session.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/dynamic_screening.html

❑ Enable Account Hijack Detection

Account hijack detection allows administrators to specify the maximum number of messages that an account can send in a given time frame. Often, when a spammer manages to guess an account's login credentials, his goal is to send out as many spam messages as possible before being blocked. Account hijack detection can prevent this kind of behavior. In SecurityGateway, Account Hijack Detection settings can be accessed by navigating to **Security | Anti-Abuse | Account Hijack Detection**. Simply specify the maximum number of messages that can be sent, and enter a time frame. You can disable the account when the message count limit is reached.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/hijack_detection.html

❑ Use Location Screening to Block Connections from Unauthorized Countries

Use Location Screening to disable SMTP/IMAP/POP connections from unauthorized regions of the world. Because spam is sent from many countries all over the world, enabling Location Screening can potentially block large amounts of spam.

Knowledge Base Article:
https://help.mdaemon.com/SecurityGateway/en/location_screening.html

❑ Use Blocklists to Block Connections from Untrusted Addresses, Hosts & IPs

Blocklists (located in SecurityGateway under **Security | Blocklists**) can be used to refuse or quarantine messages from untrusted email addresses, domains, hosts, and IP addresses. When an incoming sender matches a blocklisted address, the connection can optionally be disconnected.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/blocklists.html

❑ Enable QR Code Detection

Spam and phishing emails often contain QR codes intended to bypass spam filters and other security features. SecurityGateway can detect and take action if a QR code image is attached to a message. Messages containing QR codes can be refused, quarantined for administrator review, or delivered with a special tag inserted into the message subject for content filtering on the mail server.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/qr_code_detection.html

❑ Use Allowlists Only for Trusted Connections

Many security features include a setting to exempt emails from allowlists hosts & IPs (located under **Security | Allowlists**) from being filtered by that particular feature. When adding IP addresses and host names to these lists, ensure that they are only used to send legitimate mail and that they are not used to send spam. Adding a spammer's IP or host name to these lists by mistake can result in unwanted spam.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/allowlists.html

❑ Require Encrypted HTTPS Connections for the Web Interface

HTTPS ensures an encrypted connection between a user's browser and SecurityGateway's built-in web server. SecurityGateway can be configured to redirect HTTP connections to encrypted HTTPS connections when logging into SecurityGateway's graphical interface. These settings are located under **Setup / Users | System | HTTP Server**.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/http_interface.html

❑ Enable Two-factor Authentication

Two-factor authentication is a security mechanism that requires users to use two forms of authentication (such as a password and a one-time code) when logging into SecurityGateway. Administrators can enable two-factor authentication requirements for SecurityGateway users via **Setup/Users | Accounts | User Options**.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/user_options.html

❑ Block or Quarantine Executable Files

Executable files can pose significant threats to a business. They are common vectors for spreading malware, they can potentially bypass antivirus tools, and users may be tricked into opening these file types via clever social engineering tactics. To protect against these threats, SecurityGateway can be configured to block or quarantine these files via **Security | Filtering | Attachments**.

From the SecurityGateway Manual:

https://help.mdaemon.com/SecurityGateway/en/attachment_filtering.html

Protect Against Spoofing

❑ Enable Reverse Lookups

When performing reverse lookups, SecurityGateway will attempt to acquire all of the MX and A record IP addresses for a given domain. Then the IP of the server making the connection is compared to this list in an attempt to determine whether the sender might be using a forged identity. Reverse lookup settings can be found in SecurityGateway at **Security | Anti-Spoofing | Reverse Lookups**.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/reverse_lookups.html

❑ Enable SPF Verification Lookups

Sender Policy Framework (SPF) is an email validation method that uses a DNS record (the SPF record) to specify what hosts are allowed to send email for a given domain. SecurityGateway will query the SPF record of the domain taken from the MAIL FROM header, and compare the connecting IP address with the IP addresses listed in the SPF record. If no match is found, then it is likely that the FROM header was spoofed. The spam score is then adjusted upward for messages that fail SPF lookups, and the connection can optionally be closed. SPF verification settings can be found in SecurityGateway at **Security | Anti-Spoofing | SPF Verification**.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/sender_policy_framework_spf.html

❑ Enable DKIM Lookups

DomainKeys Identified Mail (DKIM) is another email validation method that can be used to verify that an incoming message has not been altered in any way. When this feature is enabled and an incoming message has been cryptographically signed, SecurityGateway will retrieve the public key from the DNS record of the domain taken from the signature and then use that key to test the message's DKIM signature to determine its validity. If the DKIM signature passes the verification test, the message will continue on to the next step in the regular delivery process and can optionally have its message score adjusted.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/dkim_verification.html

❑ Enable DMARC Lookups

DMARC (Domain-based Message Authentication, Reporting & Conformance) is an anti-spoofing feature that helps protect against incoming spam and phishing messages that forge (spoof) the sending domain in the messages's From header. It uses a combination of SPF and DKIM lookups to validate the sender, along with policies outlined by domain owners to determine whether to quarantine or reject messages that fail DKIM & SPF lookups.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/dmarc_verification.html

❑ Enable From Header Screening to Help Users Identify Suspicious Senders

Spam and phishing emails often change the display name (the name-only portion) of the sender to make it appear as if the message came from someone else. Because some smaller screens only show the display name and not the full sender email address, users can sometimes get tricked into responding to a phishing email. From Header Screening helps users identify spoofed emails by placing the actual email address found in the From header in the visible portion of the email header.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/from_header_screening.html

Protect Against Spam

❑ Enable the Spam Filter & Spam Scoring Settings (Heuristic Rules)

SecurityGateway's spam filter (located under **Security | Anti-Spam | Heuristics and Bayesian)** is based on industry-standard SpamAssassin. Inbound email messages are analyzed & compared against a list of SpamAssassin rules, and based on these rules, a spam score is assigned to the message.

To enable the spam filter, check the box next to **Use heuristic rules and Bayesian classification to analyze messages**.

Check the box **Add score returned by SpamAssassin to message score**. Enabling this setting provides another tier of spam protection and increases the likelihood of catching spam that wouldn't score high enough to be caught by SpamAssassin alone or by the other individual anti-spam scoring options.

Enable the following two settings:

- **Reject message if SpamAssassin score greater or equal to**
- **Quarantine message if SpamAssassin score greater or equal to**

The default scoring values of these settings should be sufficient for most business environments, however, these values can be adjusted up or down to make the spam filter more strict or more lenient as needed.

- If you need to view a message's spam score, you can open it in the message log (**Logging | All Messages**), and in the transcript, locate "Passing message through SpamAssassin." This section provides a breakdown of the various spam rules that were used to calculate the messages's spam score. In this section of the transcript, you'll see "Adding ___ to message score."

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/heuristics_and_bayesian.html

❑ Train the Spam Filter via Bayesian Learning - Artificial Intelligence

Enable Bayesian Classification to train the spam filter by feeding it samples of spam and non-spam messages. You can designate a folder for spam messages and non-spam message that can be scanned manually or automatically at regular intervals. All of the messages in these folders will be analyzed and indexed so that new messages can be compared to them statistically in order to determine the likelihood that they are spam. The Spam Filter can then increase or decrease a message's spam score based upon the results of its Bayesian comparison.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/sgspamd_configuration.html

❑ Use DNS Blocklists to Block Mail from Known Spammers

DNS blocklists (DNSBL) are lists of servers that are known to relay spam. When DNSBL queries are enabled under **Security | Anti-Spam | DNS Blocklists (DNSBL)**, SecurityGateway will query each listed host when performing a DNS-BL lookup on the sending IP address. If a host replies to the query with a positive result, SecurityGateway can refuse the message, quarantine it, or accept it and optionally tag its subject with a series of characters. You can then configure the content filter on your mail server to look for this tag and filter the message accordingly. There are several DNS blocklist services available. Zen.spamhaus.org is included by default.

By default, the option **...add score returned by DNSBL engine to message score** is enabled, providing extra protection against email sent from a server found on a DNS blocklist.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/dns_blocklists_dnsbl.html

❑ Use URI Blocklists to Block Messages Based on URLs in the Message Body

Spam and phishing emails often contain malicious URLs. Also known as Spam URI Realtime Blocklists (SURBLs), URIBLs differ from DNS Blocklists in that they are not used to identify spam based on the content of message headers or on the connecting IP address. Instead, URIBLs block spam based on message content. Complete details on how URIBLs work can be found at www.surbl.org.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/uri_blocklists_uribl.html

❑ Use Backscatter Protection to Block Unwanted Bounceback Messages & Auto-responders

"Backscatter" refers to response messages that your users receive to emails that they never sent. This occurs when spam messages or messages sent by viruses contain a "Return-Path" address that is forged. Consequently, when one of these messages is rejected by the recipient's s mail erver, or if the recipient has an autoresponder or "out of office"/vacation message associated with his account, the response message will then be directed to the forged address. This can lead to huge numbers of bogus Delivery Status Notifications (DSNs) or auto response messages ending up in your users' mailboxes. Further, spammers and virus authors frequently take advantage of this phenomenon and will sometimes use it to launch Denial of Service (DoS) attacks against email servers, causing a flood of invalid emails to arrive from servers located all over the world.

Backscatter Protection can be enabled in SecurityGateway under **Security | Anti-Spam | Backscatter Protection**.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/backscatter_protection.html

❑ Enable Automatic Spam Filter Updates

When heuristic engine updates are available, they can be applied automatically by enabling automatic spam filter updates. To access these settings in SecurityGateway, navigate to **Security | Anti-Spam | Heuristics and Bayesian**), click on **Click here to configure SGSpamD**, and then select one of these options:

- **Check for heuristic rule updates at midnight each night**
- **Check for heuristic rule updates once every __ hours.**

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/sgspamd_configuration.html

❑ Enable the Spamhaus Data Query Service (DQS)

The Data Query Service (located under **Security | Anti-Spam | Data Query Service (DQS)** is a set of DNS blocklists that are updated in real-time. When enabled, this feature can block up to 99% of email-borne threats.

- This is a subscription service offered by Spamhaus. More information can be found here: https://www.spamhaus.com/product/protect-email-with-spamhaus-and-mdaemon-technologies/

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/spamhaus_data_query_service.html

❑ Enable Outbreak Protection

Outbreak Protection (located in SecurityGateway under **Security | | Anti-Spam | Outbreak Protection**) uses recurrent pattern detection and zero-hour technologies to identify spam and malware outbreaks often within minutes (or even seconds) after an initial outbreak. By analyzing distribution and structural mail delivery patterns in real-time, Outbreak Protection can identify malware-infected messages often before traditional antivirus software has been updated with new virus definitions.

When an incoming message is determined to be part of a spam or virus outbreak, SecurityGateway can be configured to refuse, quarantine, or accept the message and optionally tag its subject with a series of characters. Points can also be added to the message's spam score.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/outbreak_protection.html

Install the Latest Patches & Security Updates

❑ Keep SecurityGateway Updated

SecurityGateway can be configured to periodically check for software updates and display a notification on the dashboard when an update becomes available. Regular software updates help ensure the latest patches and security updates are installed.

From the SecurityGateway Manual:
https://help.mdaemon.com/SecurityGateway/en/software_update.html

---

When used together, these SecurityGateway features can help protect businesses against spam, phishing, spoofing, hacking, malware, data breaches, and other email-borne threats.

MDaemon® technologies