Settings to Protect Your Mail Server

The following are best practice recommendations to protect your business email with SecurityGateway.

Verify That a User is Valid Before Creating an Account

Whenever an incoming message is addressed to an unknown local user, SecurityGateway will query the User Verification Sources configured for the user's domain to verify whether or not the unknown address is legitimate. If the address is valid then SecurityGateway will create a user account for that address and attempt to deliver the message to the domain's mail server. If the address is invalid then the message will be rejected.

We recommend using one of the five user verification sources in SecurityGateway (located under Setup / Users | Accounts | User Verification Sources) to verify the validity of a user before an account is created in SecurityGateway. Users can be verified via SMTP (call forward), Active Directory, Office 365, MDaemon (using Minger), or LDAP. We also recommend having at least one default user verification source. If no user verification sources are defined for a domain, then the default user verification source will be used.

> More information on user verification sources can be found here:
> https://www.altn.com/Support/KnowledgeBase/KnowledgeBaseResults/?Number=470

Use SMTP Authentication to Prevent Unauthorized Account Access

To help prevent unauthorized account access, we recommend requiring SMTP Authentication unless a message is transmitted from a domain mail server. This helps to ensure that the identity of users sending mail is valid.

> Instructions for configuring SMTP authentication in SecurityGateway can be found here:
> www.altn.com/Support/KnowledgeBase/KnowledgeBaseResults/?Number=KBA-01912

Use Strong Passwords

Spammers will often try to hijack an email account by guessing its password. Therefore, passwords that are easy to guess should always be avoided. If SecurityGateway is configured to create accounts automatically by querying a user verification source, then make sure your user verification source is configured to require strong passwords. Passwords can also be assigned to users manually via the Domains and Users menu.

> More information on user verification sources can be found in the SecurityGateway Help file:
> http://help.altn.com/securitygateway/en/index.html?user_verification_sources.htm

Enable Dynamic Screening

Enable Dynamic Screening to block connections that exhibit suspicious activity, such as failing too many authentication attempts, connecting too many times in a given time frame, attempting to keep a connection open too long, or sending to too many invalid recipients. Dynamic Screening makes it more difficult for a malicious person to guess passwords by detecting the malicious activity and blocking the connections.

Instructions for configuring Dynamic Screening can be found here:
https://www.altn.com/Support/KnowledgeBase/KnowledgeBaseResults/?Number=504

Enable Account Hijack Detection

If a spammer guesses an account's password, he can then use that account to send out spam. To limit the spammer's ability to abuse a compromised account, enable Account Hijack Detection, and then enter the maximum number of messages that can be sent in a given time frame. Once the limit has been reached, the account is disabled and the administrator is notified.

SecurityGateway's Account Hijack Detection feature is explained here:
http://help.altn.com/securitygateway/en/index.html?hijack_detection.htm

Enable at Least One Default Mail Server

When email arrives for a domain that has not been assigned its own mail server, SecurityGateway needs to know where to send those messages. We recommend adding a default mail server for all SecurityGateway domains that have not had domain mail servers specifically associated with them.

Instructions for configuring a domain mail server can be found here (see Step 10 to designate it as a default mail server):
www.altn.com/Support/KnowledgeBase/KnowledgeBaseResults/?Number=KBA-01865

Instructions for setting Office 365 as a default mail server can be found here:
https://www.altn.com/Support/KnowledgeBase/KnowledgeBaseResults/?Number=1233

Prevent Unauthorized Mail Relaying

Relaying occurs when mail that is neither to nor from a local account is sent through your server. Servers that are not properly configured to prevent relaying can end up on a blacklist.

By default, SecurityGateway does not allow mail relaying.

We recommend configuring your relay settings based on instructions found in this knowledge base article:
www.altn.com/Support/KnowledgeBase/KnowledgeBaseResults/?Number=KBA-01911

For optimal security, we recommend enabling only these settings:

- ✓ Only domain mail servers can send local mail
- ✓ SMTP MAIL address must exist if it uses a local domain

Note: *We do not recommend enabling any of the exceptions on this screen.*

Protect Your Domain with IP Shielding

IP Shielding is a security feature that only honors SMTP sessions claiming to be from someone at one of the listed domains if they are coming from an IP address associated with that domain.

The best way to secure outbound email is via SMTP authentication. However, for businesses that need to send email from a printer or other device that is not capable of authenticating, IP Shielding can be used to exclude certain IP's or ranges from having to authenticate. Messages from authenticated sessions can optionally be exempt from IP Shielding requirements.

Instructions for configuring IP Shielding can be found here:
www.altn.com/Support/KnowledgeBase/KnowledgeBaseResults/?Number=KBA-01913

Enable SSL to Ensure Data Privacy

To protect the privacy of transmitted data, we recommend enabling the SSL encryption features for SMTP and HTTP.

Instructions for enabling SSL encryption in SecurityGateway can be found here:
www.altn.com/Support/KnowledgeBase/KnowledgeBaseResults/?Number=KBA-01891

Enable Backscatter Protection

Most spam messages contain a forged return path. This often leads to users receiving thousands of delivery status notices, autoresponders, and other messages in response to messages that the user never sent. This is known as backscatter. To combat backscatter, SecurityGateway's Backscatter Protection feature can help to ensure that only legitimate Delivery Status Notifications and auto responders get delivered to your domains.

Backscatter Protection options are explained in this knowledge base article:
www.altn.com/Support/KnowledgeBase/KnowledgeBaseResults/?Number=KBA-01900

Don't Whitelist Local Email Addresses

In many cases, local IP addresses or host names may need to be whitelisted. However, we do not recommend whitelisting local email addresses. If a local address is added to the whitelist, messages sent to this address could bypass many of your security settings and put your server at risk of being blacklisted.

> Whitelist configuration settings are explained in this knowledge base article:
> www.altn.com/Support/KnowledgeBase/KnowledgeBaseResults/?Number=KBA-01919

Protect your Email Infrastructure from Virus and Spam Outbreaks

SecurityGateway scans all inbound and outbound mail using the Cyren and ClamAV antivirus engines. It also includes Cyren Outbreak Protection, which is real-time antispam and antivirus technology that is capable of proactively protecting your email infrastructure automatically and within minutes of an outbreak. Outbreak Protection can be enabled in SecurityGateway via **Security | Anti-Spam | Outbreak Protection**.

> More information on Outbreak Protection can be found here:
> www.altn.com/Products/SecurityGateway-Email-Firewall/Security-Features/#OutbreakProtection

Prevent Data Leaks

SecurityGateway includes over 70 Data Leak Prevention rules to help prevent unauthorized transmission of sensitive information such as personal identification numbers, credit card numbers, and other types of confidential data. These rules can be configured to send messages containing sensitive content to the administrative quarantine for further review, redirect the message to a designated address, or encrypt the message.

We recommend enabling the appropriate Data Leak Prevention rules to suit the needs of your specific business or industry.

> More information on Data Leak Prevention can be found here:
> https://www.altn.com/Products/SecurityGateway-Email-Firewall/Internal-Threat-Protection/#DataLeakPrevention

Enable Location Screening

Use Location Screening to block inbound SMTP and HTTP connections from unauthorized countries. If your company has no legitimate business need to communicate with a particular country, then refusing connections from that country can potentially block large amounts of spam. Alternatively, you can configure Location Screening to only prevent authentication from unauthorized countries.

> More information on Location Screening can be found here:
> http://help.altn.com/securitygateway/en/index.html?location_screening.htm

Enable Macro Detection in Microsoft Office Documents

Cybercriminals often use macros in email attachments to spread malware. In SecurityGateway 6.5 and up, the Virus Scanning settings (located at Security | Anti-Virus | Virus Scanning) include an option to detect macros in Microsoft Office documents and flag them as infected. SecurityGateway can refuse these messages or quarantine them for administrative review.

> More information on SecurityGateway's antivirus settings can be found here:
> http://help.altn.com/securitygateway/en/index.html?virus_scanning.htm

Summary

These best practices will help ensure that your email infrastructure is protected from spam, viruses, phishing attempts, unauthorized relaying, and other threats. Other helpful resources can be found under the Resources tab at www.securitygatewayforemail.com.

MDaemon® technologies