Settings to Protect Your Mail Server

The following are best practice recommendations specific to SecurityGateway.

Prevent Spammers from Guessing 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. Strong passwords are at least six characters long, and contain at least one number and one capital letter. 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.

> Requirements for strong passwords can be found in the following knowlege base article:
> www.altn.com/Support/KnowledgeBase/KnowledgeBaseResults/?Number=KBA-01542

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 Domain Mail Servers. If the address is invalid then the message will be rejected.

We recommend using one of the four user verification sources in SecurityGateway to verify the validity of a user before an account is created in SecurityGateway. Users can be verified via SMTP (call forward), Active Directory, 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.

> Instructions for configuring a user verification source can be found here:
> www.altn.com/Support/KnowledgeBase/KnowledgeBaseResults/?Number=KBA-01867

Prevent Unauthorized Account Access

To help prevent unauthorized account access, you should require your users to use 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

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. You should add 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:
> www.altn.com/Support/KnowledgeBase/KnowledgeBaseResults/?Number=KBA-01865

Prevent Unauthorized Mail Relaying

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

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

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

Enable IP Shielding to prevent unauthorized use of your domain. 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. This helps to prevent spoofing.

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

Ensure Data Privacy

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

Instructions for enabling 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 Addresses

You should ensure that there are no local addresses, hosts, or IP addresses on your whitelists. If a local address is found on a whitelist, and a message arrives with a spoofed address that resides on one of your whitelists, it could possibly 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 includes 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

Disable Greylisting

Greylisting is located under **Security | Anti-Spam | Greylisting**. We recommend disabling this feature because it can delay legitimate mail.

> For more information on configuring Greylisting, please see the following knowledge base article:
> www.altn.com/Support/KnowledgeBase/KnowledgeBaseResults/?Number=KBA-01898

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 Support tab at www.altn.com.