Abuse Detection

Help Documentation

Abuse Detection

SmarterMail has several methods of preventing abuse and denial of service (DoS) attacks. The ones that can be configured are explained below. Any number of detection methods can be added.

To view the configurable abuse detection settings, click the security icon . Then expand the Advanced Settings folder and click Abuse Detection in the navigation pane. A list of abuse detection rules will load in the content pane and the following options will be available in the content pane toolbar:

- New - Creates a new abuse detection rule.
- Edit - Edits the selected abuse detection rule.
- Delete - Permanently deletes the selected abuse detection rule(s).
- Wizard - Displays the Abuse Detection section of the SmarterMail setup wizard, which offers the following preset security options:

- Do not change abuse detection settings
- Relaxed abuse detection (Includes: DoS, SMTP Brute Force)
- Strict abuse detection (Includes: DoS, SMTP Brute Force, Email Harvesting, Internal Spammer Notifications, Bounces Indicate Spammer)

To create a new abuse detection rule, click New in the content pane toolbar. The abuse detection settings will load in the content pane and the following options will be available:

Denial of Service (DoS) - Too many connections from a single IP address can indicate a Denial of Service (DoS) attack. Enable this option to block IPs that are connecting too often to the server. It is recommended that you whitelist any trusted IP addresses that may send out large mailing lists or make many connections if you enable this option.

- Service - Select the service that will be monitored for this type of attack (SMTP/IMAP/POP/XMPP/LDAP).
- Time Frame - The period of time in the past that is examined to determine if an IP address should be blocked. Too many connections in this period of time, and a block will be initiated.
- Connections Before Block - The number of connections before a block is placed. It is common for several connections to be open at once from an IP address. Set this to a relatively high value so that you can catch DoS attacks while not impacting legitimate customers.
- Time to Block - The number of minutes that a block will be placed once an IP address hits the threshold.
- Description - A friendly name or brief description of the rule.

Bad SMTP Sessions (Harvesting) - A bad session is any connection that ends without successfully sending a message. Many bad sessions usually indicate spamming or email harvesting. Leaving all of these options set to 0 (zero) will disable this type of abuse detection. Note: It is recommended that you whitelist any trusted IP addresses that may send out large mailing lists if you enable this option.

- Time Frame - The period of time in the past that is examined to determine if an IP address should be blocked. Too many bad sessions in this period of time, and a block will be initiated.
- Bad Sessions Before Block - The number of bad sessions before a block is placed. A few bad sessions happen once in a while, for instance when a person sends an email to an email account that does not exist. It is not these people that you are targeting, but rather those that are attempting to compromise or harass your customers.
- Time to Block - The number of minutes that a block will be placed once an IP address hits the threshold.
- Description - A friendly name or brief description of the rule.

Internal Spammer - Enabling this rule in SmarterMail will block or quarantine an account from sending mail, as well as alert an administrator, whenever multiple emails from a single sender are received on the server during a specified time frame.

- Action - Choose whether to send a notification email only, block messages from the sender or quarantine messages from the sender.
- Time Frame - The period of time in the past that is examined to determine if the rule triggers. Too many emails from a single sender in this period of time, and the email notification is sent and the Action chosen is performed.
- Messages Before Notify - After this many messages are received within the time period specified, the email notification is sent and the Action chosen is performed.
- Time to Block - The number of minutes that a block will be placed once an IP address hits the threshold.
- Email to Notify - The email address of the administrator account to which the notification will be sent.
- Description - A friendly name or brief description of the rule.

Password Brute Force by Protocol - A common ploy by spammers and hackers is attempting to guess passwords for users. Many times this entails continual log in attempts to an account using different passwords, each a bit different than the one before it. This thereby brute forcing the password.

- Service - Select the service that will be monitored for this type of attack (SMTP/IMAP/POP/XMPP/LDAP).
- Time Frame - The period of time in the past that is examined to determine if an login attempt

is a brute force attempt. Too many connections in this period of time, and a block will be initiated.

- Connections Before Block - The number of failed login attempts before the IP is blocked.
- Time to Block - The number of minutes that a block will be placed once an IP address hits the threshold.
- Description - A friendly name or brief description of the rule.

Bounces Indicate Spammer - Enabling this rule in SmarterMail will block or quarantine an account from sending out mail, as well as alert an administrator, after receiving a certain number of bounce messages in the specified time frame.

- Action - Choose whether to send a notification email only, block messages from the sender or quarantine messages from the sender.
- Time Frame - The period of time in the past that is examined to determine if the rule triggers. Too many emails from a single sender in this period of time, and the email notification is sent and the Action chosen is performed.
- Bounce Threshold - After this many bounce messages are received within the time period specified, the email notification is sent and the Action chosen is performed.
- Time to Block - The number of minutes that a block will be placed once an IP address hits the threshold.
- Email to Notify - The email address of the administrator account to which the notification will be sent.
- Description - A friendly name or brief description of the rule.