# IDS Rules

Help Documentation

# IDS Rules

Through the use of SmarterMail's intrusion detection system (IDS), there are several methods for preventing abuse and denial of service (DoS) attacks on your mail server. For example, IDS rules (also known as abuse detection rules) can be configured to monitor a variety of activity on the mail server, including the number of connections coming from a single IP address, the number of messages sent within a specific timeframe, the number of login attempts and more. These rules allow SmarterMail to alert System Administrators of suspicious behavior or take action to prevent the attack.

To access the IDS Rules, log into SmarterMail as a System Administrator and click on the Settings icon . Then cick on Security in the navigation pane and select the IDS Rules tab.

Jump To:



## Abuse Detection Overview

Some rules are configured upon installation by default. The following details can be seen for each entry in the list:

- Type - The type of Abuse Detection rule configured: Denial of Service (DOS), Bad SMTP Sessions (Harvesting), Internal Spammer, Password Brute Force by Protocol or Bounces Indicate Spammer.
- Service - The protocol service associated wtih the rule: SMTP, IMAP, POP, LDAP, or XMPP.

- Time Frame - The period of time, in minutes, that is examined to determine if the rule's action should be triggered.
- Threshold - The threshold that is examined to determine if the rule's action should be triggered. For example, the number of messages sent, the number of connections made from an IP address, the number of bounce messages received, etc.
- Block Time - The time frame, in minutes, in which the IP address will be blocked.
- Description - A friendly name or brief description of the rule.

Click on the Actions (...) button and then click Reset IDS Rules to replace all existing rules with the default configuration that's available upon installation.

## Abuse Detection Rules

To create a new Abuse Detection rule, click the New button. When adding or editing an entry, the following configuration settings will be available, based on the Detection Type chosen:

## 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 or LDAP.
- Time Frame - The period of time, in minutes, 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.
- Block Time (Minutes) - 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 minutes, 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.
- Block Time (Minutes) - 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 delivered externally from 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 minutes, 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 delivered within the time period specified, the email notification is sent and the Action chosen is performed.
• Block Time (Minutes) - The number of minutes that a block will be placed once an IP address hits the threshold.
• Notify Email - 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 or LDAP.
• Time Frame - The period of time, in minutes, 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.
• Failures Before Block - The number of failed login attempts before the IP is blocked.
• Block Time (Minutes) - 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 minutes, 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.
• Block Time (Minutes) - The number of minutes that a block will be placed once an IP address hits the threshold.
• Notify Email - The email address of the administrator account to which the notification will be sent.
• Description - A friendly name or brief description of the rule.