Security

Help Documentation

Security

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:

IDS Rules Overview

By default, SmarterMail offers several rules that are pre-configured upon installation. These include Denial of Service rules for all major protocols, Brute Force protection for protocols and webmail, and more. 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.

- Action - The action to be taken when the rule is triggered.
- 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. (NOTE: If a notification email is sent, then this setting is ignored as a Block does not occur.)
- 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.

By default, SmarterMail has several pre-configured IDS Rules for System Administrators. These rules are completely editable, and while most can be deleted as needed, there are 3 Rules that are permanent:

- Password Retrieval Brute Force
- Webmail Brute Force by IP
- Webmail Brute Force by Email

It is possible to edit the settings for these Rules, but they are permanent due to the likelihood of a System Administrator having brute force attacks against their various webmail URLs. To help mitigate these issues, SmarterMail has these permanent Rules in place as they are the most common types of attacks agains mail servers.

IDS 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 - Where applicable, select the service that will be monitored for this type of attack: SMTP, IMAP, POP, XMPP or LDAP.
- Time Frame (Minutes) - 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. (NOTE: If a notification email is sent, then this setting is ignored as a Block does not occur.)
- 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. (NOTE: If a notification email is sent, then this setting is ignored as a Block does not occur.)
- 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.

Blacklist / Whitelist

System Administrators are able to control the IP addresses that are blacklisted from accessing, or whitelisted for access to, mail services. Blacklisting an IP address prevents it from making inbound connections, while whitelisting an IP address adds the IP as a trusted source, allowing connections to bypass relay restrictions that may be imposed, including spam filtering, greylisting and IDS rules.

Exercise caution when granting whitelist status to a server, and be sure that you know what services on that server may send mail through your own.

To manage the blacklist or whitelist, log into SmarterMail as a System Administrator and click on the Settings icon. Then click on Security in the navigation pane and select the Blacklist or Whitelist tab.

By default, both of these tabs will be empty as SmarterMail has no way of knowing the IPs or IP Ranges that need to be blocked or granted access to its various services. To create a new entry in the blacklist or whitelist, click New . When adding or editing an entry, the following options will be available:

- IP Addresses (single, range or CIDR block) - Enter a single IP address or an IP range in dotted quad notation (e.g., 123.45.678.90, or 12.345.67.89 - 12.345.67.890). If an IP range is entered, all IP addresses within that range will be contained in the list.
- Description - Use this field to enter optional notes for understanding the various whitelist / blacklist entries. For example, "Office LAN IPs"
- Protocol - Enable this setting to add the protocols you wish to include in the blacklist or whitelist entry. The available options are: SMTP, POP, IMAP and XMPP.
- SMTP Auth Bypass - Used for whitelists only, enabling this bypasses the need for SMTP authentication for whitelisted IPs.
- SMTP Spam Bypass - Used for whitelists only, enabling this bypasses spam checks for whitelisted IPs.

Note: SmarterMail runs a check against the IPs listed in whitelist, blacklist and authentication bypass settings. This check looks at the number of IPs listed and will display a warning if the IPs listed represent a significant number. (E.g., a range greater than a /24.) While the warning does not affect the ability to save the settings, it is an indication that the System Administrator may want to review the settings prior to adding the IP range.

SMTP Auth Bypass

Whitelisted IP addresses can bypass SMTP authentication, which is a security measure that can be very beneficial in the fight against spam and unauthorized email as it forces the sender to authenticate their username and password before an email is sent through the mail server. Unfortunately, some applications do not have support for SMTP authentication when sending mail. Most often, these are web sites that have automated mail sending mechanisms. The solution is to add the IP addresses of these servers/sites to SmarterMail's Whitelist and enable SMTP Authentication Bypass. Whitelist entries with SMTP Auth Bypass enabled will not be asked to provide an SMTP Authentication login.

Blacklist / Whitelist

System Administrators are able to control the IP addresses that are blacklisted from accessing, or whitelisted for access to, mail services. Blacklisting an IP address prevents it from making inbound connections, while whitelisting an IP address adds the IP as a trusted source, allowing connections to bypass relay restrictions that may be imposed, including spam filtering, greylisting and IDS rules. Exercise caution when granting whitelist status to a server, and be sure that you know what services on that server may send mail through your own.

To manage the blacklist or whitelist, log into SmarterMail as a System Administrator and click on the Settings icon. Then click on Security in the navigation pane and select the Blacklist or Whitelist tab.

By default, both of these tabs will be empty as SmarterMail has no way of knowing the IPs or IP Ranges that need to be blocked or granted access to its various services. To create a new entry in the blacklist or whitelist, click New . When adding or editing an entry, the following options will be available:

- IP Addresses (single, range or CIDR block) - Enter a single IP address or an IP range in dotted quad notation (e.g., 123.45.678.90, or 12.345.67.89 - 12.345.67.890). If an IP range is entered, all IP addresses within that range will be contained in the list.
- Description - Use this field to enter optional notes for understanding the various whitelist / blacklist entries. For example, "Office LAN IPs"
- Protocol - Enable this setting to add the protocols you wish to include in the blacklist or whitelist entry. The available options are: SMTP, POP, IMAP and XMPP.
- SMTP Auth Bypass - Used for whitelists only, enabling this bypasses the need for SMTP authentication for whitelisted IPs.
- SMTP Spam Bypass - Used for whitelists only, enabling this bypasses spam checks for whitelisted IPs.

Note: SmarterMail runs a check against the IPs listed in whitelist, blacklist and authentication bypass settings. This check looks at the number of IPs listed and will display a warning if the IPs listed represent a significant number. (E.g., a range greater than a /24.) While the warning does not affect the ability to save the settings, it is an indication that the System Administrator may want to review the settings prior to adding the IP range.

SMTP Auth Bypass

Whitelisted IP addresses can bypass SMTP authentication, which is a security measure that can be very beneficial in the fight against spam and unauthorized email as it forces the sender to authenticate their username and password before an email is sent through the mail server. Unfortunately, some

applications do not have support for SMTP authentication when sending mail. Most often, these are web sites that have automated mail sending mechanisms. The solution is to add the IP addresses of these servers/sites to SmarterMail's Whitelist and enable SMTP Authentication Bypass. Whitelist entries with SMTP Auth Bypass enabled will not be asked to provide an SMTP Authentication login.

SMTP Blocks

SMTP Blocks are an effective method for temporarily preventing a domain or indiviual user from sending email from the server. For example, if a particular account is sending an abnormal amount of email, you can add their address to the SMTP Blocks list and they will be unable to send email until you remove them. Users and/or domains can be left on the list for whatever time you deem appropriate. This action can be an effective stop-gap versus actually deleting the user and/or domain from the server, giving users or Domain Admininstrators the ability to clean up their act before having their mail server privileges revoked.

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

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

SMTP Blocking

- Block Type - Whether the block affects an email address or an entire domain, or an EHLO domain. An "EHLO domain" is the return value given when SmarterMail sends the EHLO or HELO command. A standard EHLO domain is the fully qualified domain name set up for the mail server you're wanting to block. (E.g., "mail.your_domain.com".) However, it IS possible that it will be something different based on whether the command is sent by the SmarterMail web interface or an email client. For example, it may be the local IP address of the sending machine. Therefore, there is no well-established rule for what should be entered until some testing is done by the System Administrator.
- Blocked Address - The complete email address of the user, the domain name or the value used for the EHLO domain.
- Direction - For user/domain (non-EHLO domain) blocks, this refers to the types of messages that should be blocked from sending: Inbound, Outbound or All Messages.
- Description - A friendly name or brief description of the block.

Note: SMTP blocking does NOT occur immediately when the EHLO command is given. Instead, a "soft" block is used and SmarterMail will fail any authentication attempts or RCPT TO commands. This is because if the failure occurs right after the EHLO commaned, any person attempting to spam from a mail server could figure out what the problem is and change the domain given with the

command on each send. A "soft" failure should, instead, make the spammer believe he is using an incorrect password.