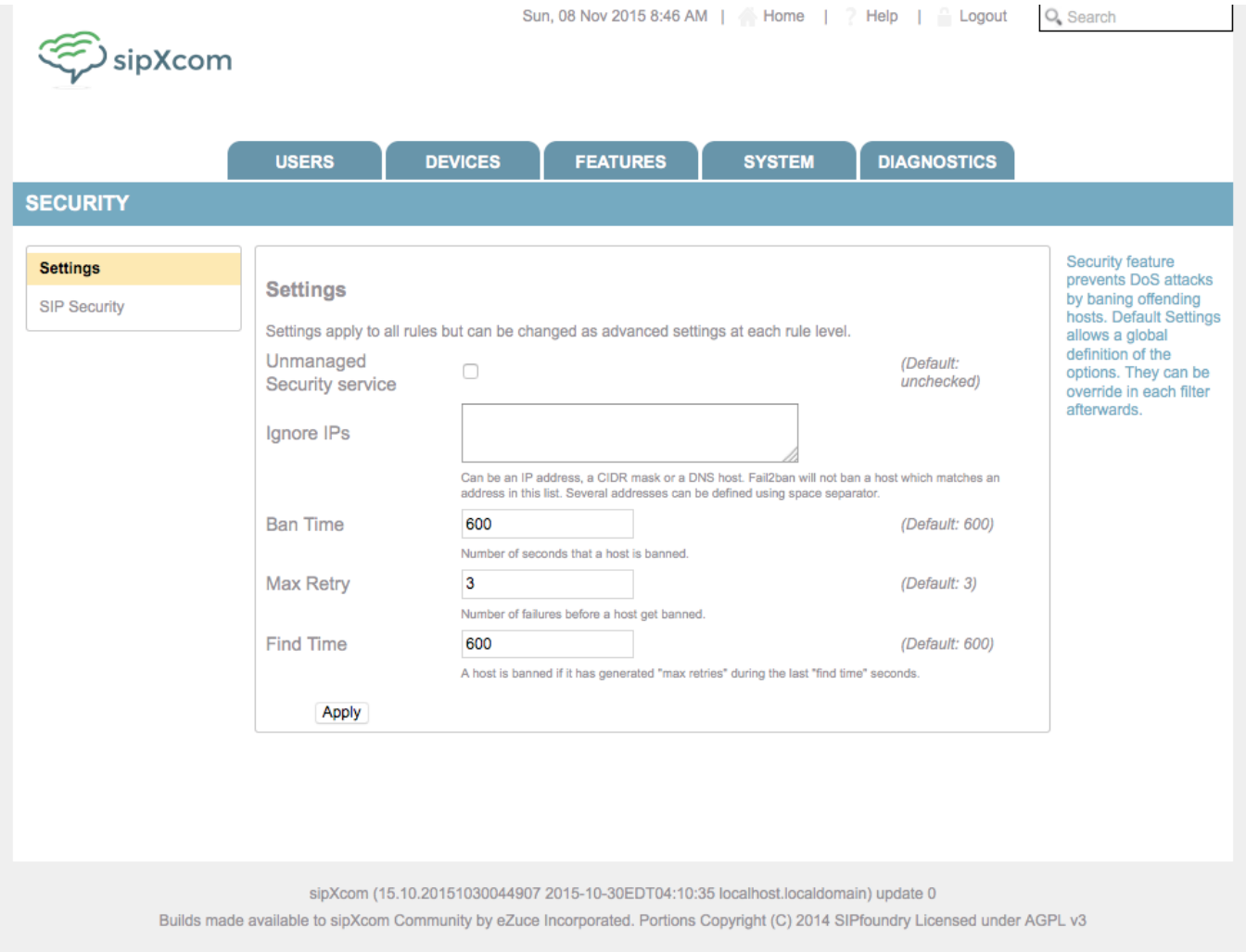
Security

Overview

The system Security settings control fail2ban. Configuration can be found in System -> Security.

Settings

The Settings Page (System -> Security -> Settings) allows the administrator to set defaults across all of the fail2ban rules.



Unmanaged Security service

If checked this allows the administrator to write his or her own fail2ban rules.

Ignore IPs

Sets specific IP addresses or IP address ranges that fail2ban will ignore.

Ban Time

The number of seconds that a host will be banned. Setting this to -1 will ban an IP address until IPTables restart.

Max Retry

The number of times a fail2ban rule is hit before a host gets banned.

Find Time

The time period over which "Max Retry" is evaluated.

SIP Security

The following are the fail2ban rules that are enabled in the system. For each of the rules logging of the specific messages must be enabled in the firewall settings page.

SECURITY

Settings

SIP Security

Hide Advanced Settings

Block DoS attackers

This rule blocks IPs considered to be DoS attackers. You need to enable Log SIP DoS packets option in Firewall Setting tab in order to take effect.

Enable Rule [x] *(Default: checked)*

Ignore IPs

Ban Time: -1 *(Default: -1)*
Number of seconds that a host is banned.

Max Retry: 1 *(Default: 1)*
Number of failures before a host get banned.

Find Time: 60 *(Default: 60)*
A host is banned if it has generated "max retries" during the last "find time" seconds.

SIP REGISTER messages

This rule blocks IPs that send excessive number of REGISTER messages. You need to enable Log SIP REGISTERs option in Firewall Setting tab in order to take effect.

Enable Rule [ ] *(Default: unchecked)*

Ignore IPs

Ban Time: 600 *(Default: 600)*
Number of seconds that a host is banned.

Max Retry: 180 *(Default: 180)*
Number of failures before a host get banned.

Find Time: 60 *(Default: 60)*
A host is banned if it has generated "max retries" during the last "find time" seconds.

SIP INVITE messages

This rule blocks IPs that send excessive number of INVITE messages. You need to enable Log SIP INVITEs option in Firewall Setting tab in order to take effect.

Enable Rule [ ] *(Default: unchecked)*

Ignore IPs

Ban Time: 600 *(Default: 600)*
Number of seconds that a host is banned.

Max Retry: 180 *(Default: 180)*
Number of failures before a host get banned.

Find Time: 60 *(Default: 60)*
A host is banned if it has generated "max retries" during the last "find time" seconds.

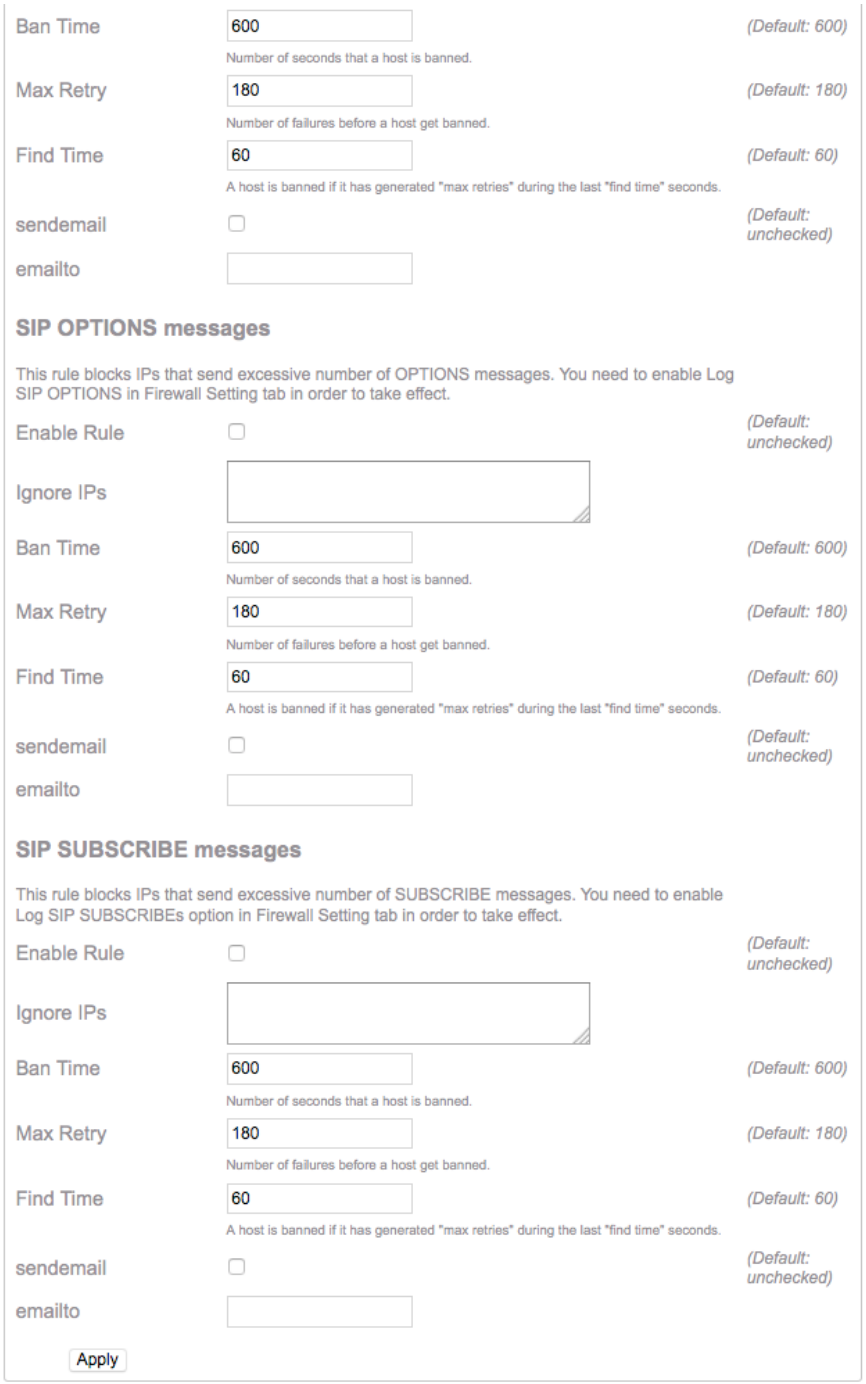
SIP ACK messages

This rule blocks IPs that send excessive number of ACK messages. You need to enable Log SIP ACKs option in Firewall Setting tab in order to take effect.

Enable Rule [ ] *(Default: unchecked)*

Ignore IPs

Security feature prevents DoS attacks by baning offending hosts. Default Settings allows a global definition of the options. They can be override in each filter afterwards.



Enable Rule

Enables this specific fail2ban rule.

Ignore IPs

Sets specific IP addresses or IP address ranges that fail2ban will ignore.

Ban Time

The number of seconds that a host will be banned. Setting this to -1 will ban an IP address until IPTables restart.

Max Retry

The number of times a fail2ban rule is hit before a host gets banned.

Find Time

The time period over which "Max Retry" is evaluated.

Send eMail

Enables sending of eMail when this particular fail2ban rule is hit.

eMail To

The email address to send fail2ban notifications to.