# SIP Firewall

The SIP firewall can assist you in detecting failed SIP connections to the SBC.

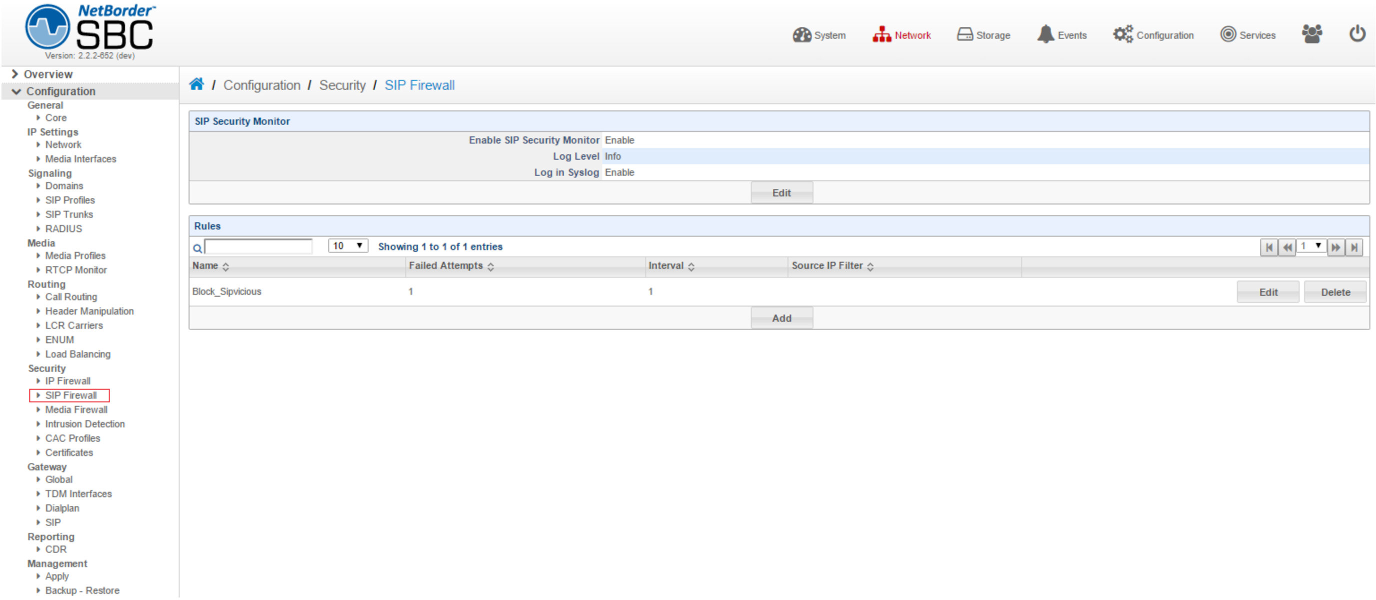
- The general concept is the SIP firewall is made up of rules that will either **Log** or **Block** the offender exceeding the failed attempts.
- These rules can be targeted towards every IP and User Agent, or only certain User Agents or IPs.
- As well, these rules can be associated with all SIP profiles or certain SIP profiles.

The SIP Firewall configuration works in conjunction with **SIP Security Monitor Service**
Refer to SBC Operation

## SIP Firewall Configuration

To start the configuration go to **Configuration->Security->SIP Firewall** then

- click **Add** to add rule in the SIP Security Monitor – Rules section.



SIP Security Monitor

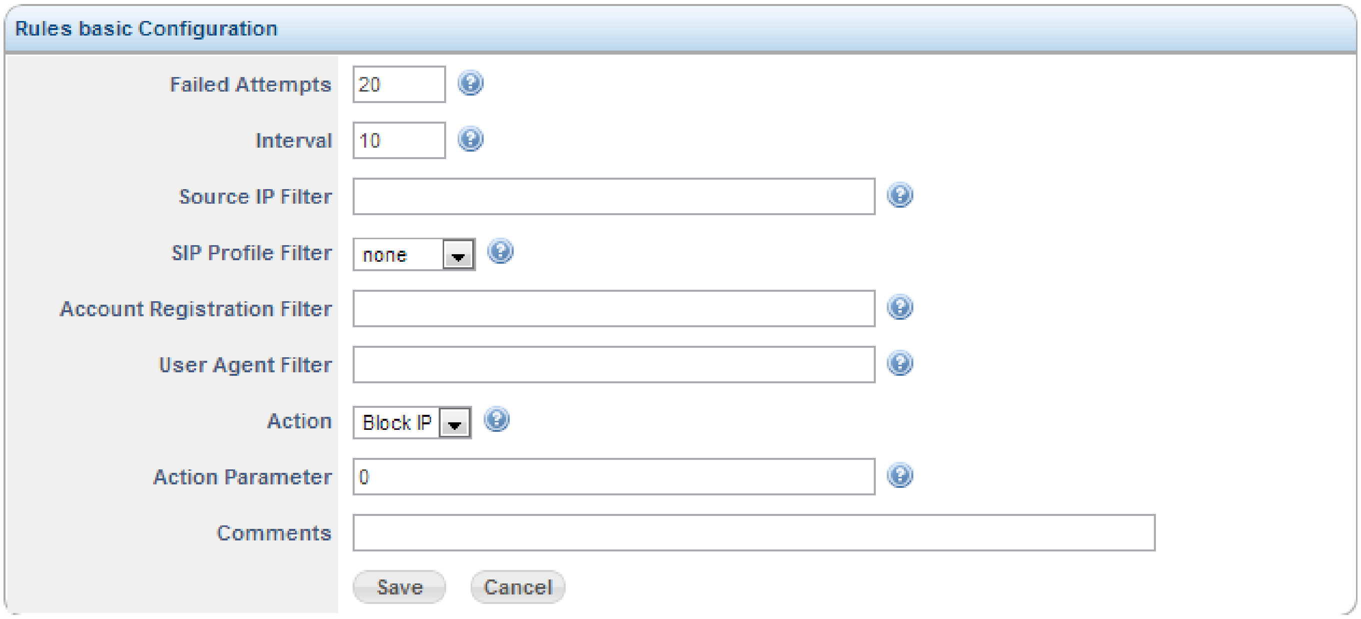
| | |
|---|---|
| Enable SIP Security Monitor | Enable |
| Log Level | Info |
| Log in Syslog | Enable |

Rules

Showing 1 to 1 of 1 entries

| Name | Failed Attempts | Interval | Source IP Filter | |
|---|---|---|---|---|
| Block_Sipvicious | 1 | 1 | | Edit Delete |

- Specify the **name** for the new rule, then click Add.

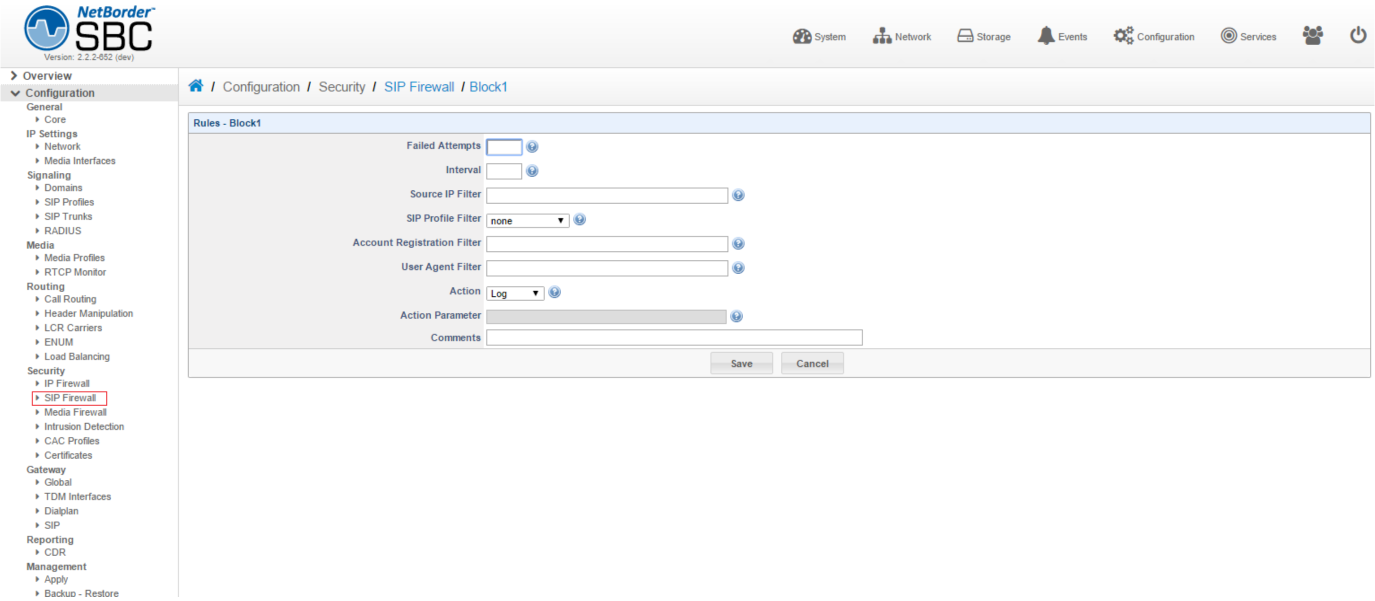


Rules basic Configuration

| | |
|---|---|
| Failed Attempts | 20 |
| Interval | 10 |
| Source IP Filter | |
| SIP Profile Filter | none |
| Account Registration Filter | |
| User Agent Filter | |
| Action | Block IP |
| Action Parameter | 0 |
| Comments | |

The rule below will look for any single source IP exceeding 20 failed attempts over 10 minutes.

- If a certain IP exceeds this then it will be blocked.
- The Action Parameter is set to 0 so this will block the host forever,
  - if you would like the host to be blocked for 15 minutes set the Action Parameter to 15.



Rules - Block1

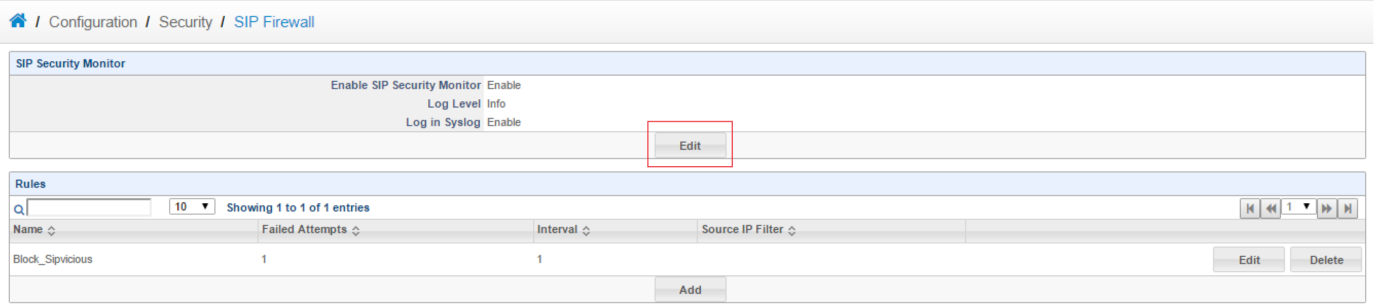
| | |
|---|---|
| Failed Attempts | |
| Interval | |
| Source IP Filter | |
| SIP Profile Filter | none |
| Account Registration Filter | |
| User Agent Filter | |
| Action | Log |
| Action Parameter | |
| Comments | |

If you want to keep all blocked users in your own 3rd party firewall youcanlet the SBC block the IPs then check the status of the blocked users as shown below.
Or you can write to the log file and have a utility which checks the NSC logs for these entries and act on this.

The log file is /var/log/sipsecmon.log on the unit or in the WebUI go to **Reports->System->NSCLogs** then click on SIP Security Monitor.

## SIP Firewall Logging

- To configure the log level click **Edit** under the SIP Security Monitor Configuration.



SIP Security Monitor

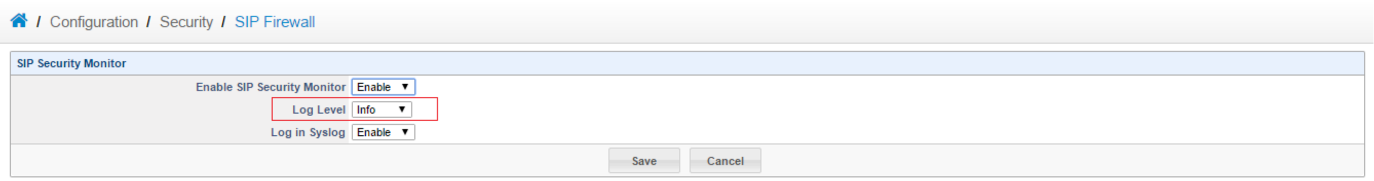
Enable SIP Security Monitor Enable
Log Level Info
Log in Syslog Enable

Rules

10 Showing 1 to 1 of 1 entries

| Name | Failed Attempts | Interval | Source IP Filter |
|---|---|---|---|
| Block_Sipvicious | 1 | 1 | |

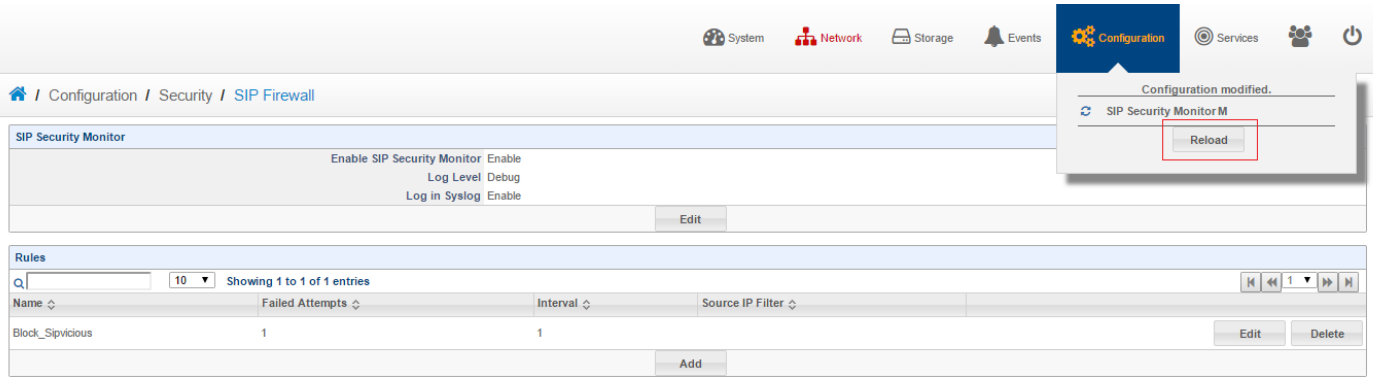
- On the next page the **Log Level** can be set to **Info** or **Debug**, once set, click save to exit.



SIP Security Monitor

Enable SIP Security Monitor Enable ▼
Log Level Info ▼
Log in Syslog Enable ▼

- To apply the changes click to **Configuration** top tool bar**,** then click Reload.



SIP Security Monitor

Enable SIP Security Monitor Enable
Log Level Debug
Log in Syslog Enable

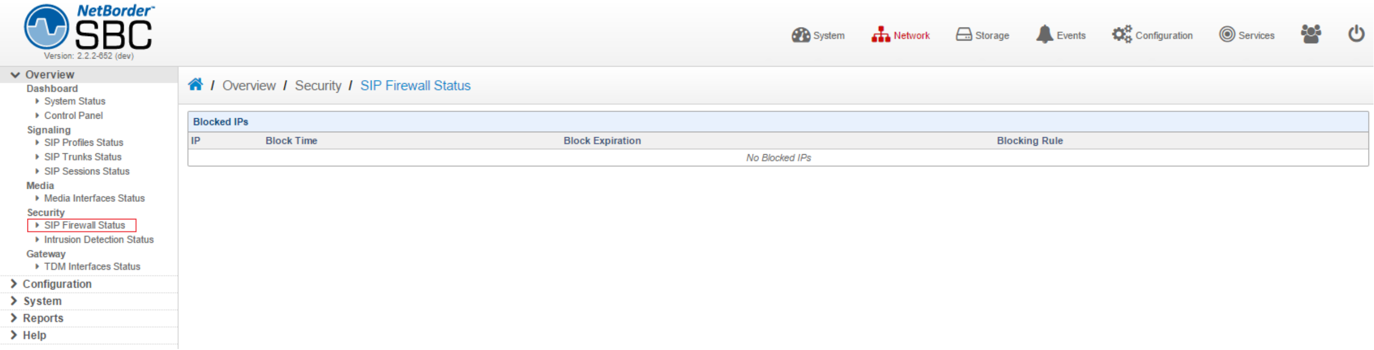
Rules

10 Showing 1 to 1 of 1 entries

| Name | Failed Attempts | Interval | Source IP Filter |
|---|---|---|---|
| Block_Sipvicious | 1 | 1 | |

# SIP Firewall Status

To get the status of blocked IPs on the SBC go to **Overview->Security->SIP Firewall Status** and the list of blocked IPs will be there.



Blocked IPs

| IP | Block Time | Block Expiration | Blocking Rule |
|---|---|---|---|
| | *No Blocked IPs* | | |