

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.

The screenshot shows the NetBorder SBC configuration interface. The top navigation bar includes System, Network, Storage, Events, Configuration, Services, and a power icon. The left sidebar shows a tree view of configuration categories, with 'SIP Firewall' highlighted under the 'Security' section. The main content area is titled 'SIP Firewall' and contains two sections: 'SIP Security Monitor' and 'Rules'. The 'SIP Security Monitor' section has three toggle switches: 'Enable SIP Security Monitor' (set to 'Enable'), 'Log Level' (set to 'Info'), and 'Log in Syslog' (set to 'Enable'). Below this is an 'Edit' button. The 'Rules' section shows a table with one rule: 'Block_Sipvicious'. The table has columns for Name, Failed Attempts, Interval, and Source IP Filter. The 'Add' button is visible at the bottom of the table.

Name	Failed Attempts	Interval	Source IP Filter
Block_Sipvicious	1	1	

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

Rules basic Configuration

Failed Attempts ?

Interval ?

Source IP Filter ?

SIP Profile Filter ?

Account Registration Filter ?

User Agent Filter ?

Action ?

Action Parameter ?

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.

The screenshot shows the NetBorder SBC WebUI interface. The top navigation bar includes System, Network, Storage, Events, Configuration, Services, and a power icon. The left sidebar shows a tree view of configuration options, with 'SIP Firewall' highlighted. The main content area displays the configuration for a rule named 'Block1'. The configuration fields are: Failed Attempts (20), Interval (10), Source IP Filter (empty), SIP Profile Filter (none), Account Registration Filter (empty), User Agent Filter (empty), Action (Log), and Action Parameter (empty). There are 'Save' and 'Cancel' buttons at the bottom of the configuration panel.

If you want to keep all blocked users in your own 3rd party firewall you can let 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.

Home / Configuration / Security / SIP Firewall

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	

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

Home / Configuration / Security / SIP Firewall

SIP Security Monitor

Enable SIP Security Monitor:

Log Level:

Log in Syslog:

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

System Network Storage Events **Configuration** Services

Home / Configuration / Security / SIP Firewall

SIP Security Monitor

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

Configuration modified.
 SIP Security Monitor M

Rules

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.

NetBorder SBC Version: 2.2.2-002 (dev)

System Network Storage Events Configuration Services

Home / Overview / Security / SIP Firewall Status

Blocked IPs

IP	Block Time	Block Expiration	Blocking Rule
No Blocked IPs			

Overview Dashboard System Status Control Panel Signaling SIP Profiles Status SIP Trunks Status SIP Sessions Status Media Media Interfaces Status Security **SIP Firewall Status** Intrusion Detection Status Gateway TDM Interfaces Status Configuration System Reports Help

