SIP Threat Manager

User Manual

allo.com

Copy Right

Proprietary Rights

Disclaimer

Information in this document is subject to change without notice and should not be construed as a commitment on the part of **http://www.allo.com.** And does not assume any responsibility or make any warranty against errors. It may appear in this document and disclaims any implied warranty of merchantability or fitness for a particular purpose.

About this manual

This manual describes the Allo product application and explains how to work and use it major features. It serves as a means to describe the user interface and how to use it to accomplish common tasks. This manual also describes the underlying assumptions and users make the underlying data model.

Document Conventions

In this manual, certain words are represented in different fonts, typefaces, sizes, and weights. This highlighting is systematic; different words are represented in the same style to indicate their inclusion in a specific category. Additionally, this document has different strategies to draw User attention to certain pieces of information. In order of how critical the information is to your system, these items are marked as a note, tip, important, caution, or warning.

Icon	Purpose
	**Note**
	**Tip/Best Practice**
	**Important**
	**Caution**
	**Warning**

- **Bold** indicates the name of the menu items, options, dialog boxes, windows and functions.
- The color blue with underline is used to indicate cross-references and hyperlinks.
- Numbered Paragraphs - Numbered paragraphs are used to indicate tasks that need to be carried out. Text in paragraphs without numbering represents ordinary information.
- The Courier font indicates a command sequence, file type, URL, Folder/File name e.g. http://www.allo.com

Support Information

Every effort has been made to ensure the accuracy of the document. If you have comments, questions, or ideas regarding the document contact online support: http://support.allo.com

Contents

Table of Contents

Introduction

1. Introduction

1.1. Overview

This User manual describes the steps involved in setting up the allo STM Appliance. Allo STM is an appliance based VoIP threat prevention solution dedicated to protect the SIP based PBX/Telecom Gateway/IP Phones/Mobile device deployments. The appliance runs the Real time Deep Packet Inspection on the SIP traffic to identify the VOIP attack vectors and prevents the threats impacting the SIP based devices. The appliance has been made to seamlessly integrate with the existing network infrastructure and reduces the complexity of deployment.

The appliance feature set includes,

- Analyze SIP packets using the Realtime Deep Packet inspection engine.
- SIP Protocol Anomaly detection with configurability of detection parameters.
- Detection and Prevention of the following categories of SIP based Attacks.
  - Reconnaissance attacks (SIP Devices Fingerprinting, User enumeration, Password Cracking Attempt)
  - Dos/DDos Attacks
  - Cross Site Scripting based attacks.
  - Buffer overflow attacks
  - SIP Anomaly based attacks
  - 3rd Party vendor vulnerabilities
  - Toll Fraud detection and prevention
  - Protection against VOIP Spam & War Dialing

- Attack response includes the option for quietly dropping malicious SIP packets to help prevent continued attacks
- Dynamic Blacklist Update service for VOIP, SIP PBX/Gateway Threats
- Configurability of Blacklist/White list/Firewall rules.
- Support for Geo Location based blocking.
- Provide the option to secure against PBX Application vulnerabilities
- Operate at Layer 2 device thus transparent to existing IP infrastructure - no changes required to add the device to your existing network
- Web/SSL based Device Management Access which will allow managing the device anywhere from the Cloud.
- Ability to restrict the device management access to specific IP/Network.
- Provide System Status/Security events logging option to a remote Syslog server.
- Provides the SIP throughput up to ~10Mbps.
- Support for Signature update subscription and automated signature update mechanism.
- The device has been made to operate with default configuration with just powering on the device. No administrator intervention is required to operate the device with default configuration.
- USB based power supply
- Optional support for security events logging on the USB based storage.

Technical Specifications

Functional Mode	Transparent Firewall with SIP Deep Packet Engine.
SIP Intrusion/Prevention	~400+ SIP Attack Signatures Support
Throughput	~10Mbps
No of concurrent calls supports	Up to 50 concurrent calls
Logging	Local Security Event Console, Remote Syslog
Device Management	Web GUI via Https & SSH CLI
Hardware	MIPS based 32bit Processor Single core, 300MHz
Primary Storage	16 MB Flash
RAM	64MB
Secondary Storage	USB Storage devices support for logging (Optional)
Interfaces	Two Fast Ethernet Interfaces.

1.1.1. Notification LEDs (On the Front Panel of the STM)

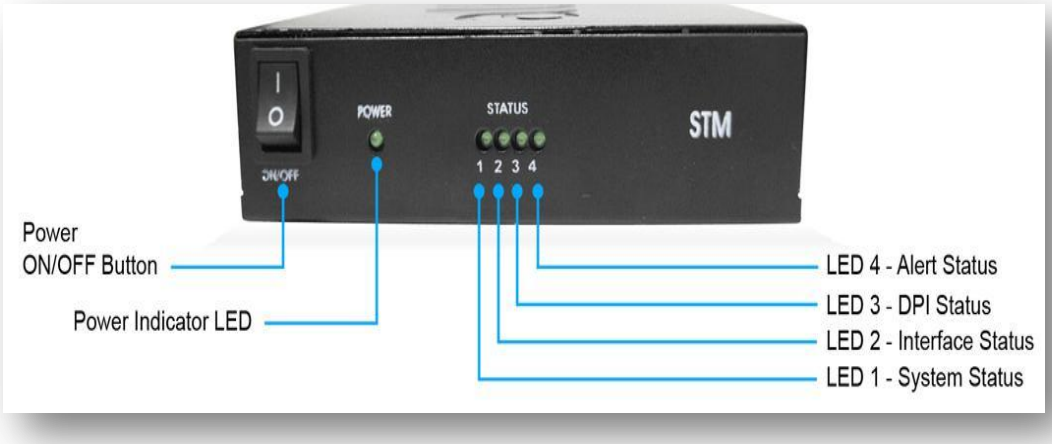

Figure 1: Front Panel LED Notifications

The STM package includes:

- 1 STM Appliance
- 1 USB Power Adapter
- 1 Serial Console Cable
- 2 Ethernet Cables

1.1.2. STM Rear View:

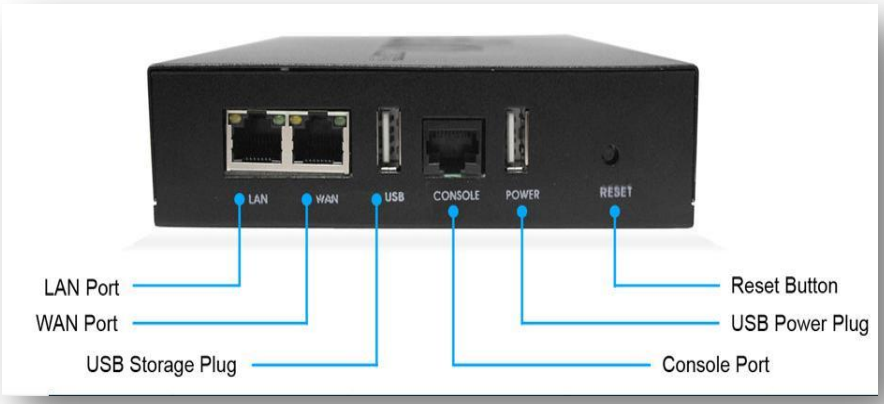

Figure 2: STM Rear View

1.1.3. STM Deployment Considerations

The STM has been made to protect the SIP based PBX/Gateway Servers against SIP based network threats and anomalies. Thus it is recommended to deploy the STM along with the PBX/Gateway deployment as given in the following scenarios based on what is applicable in the user's setup.

Deployment Scenario 1

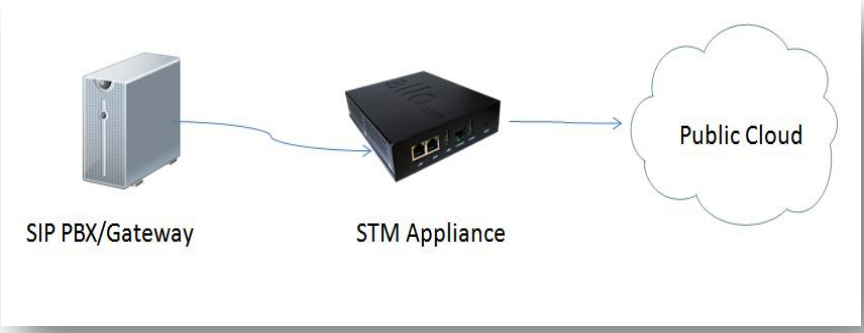

Figure 3: Scenario 1

Some of the PBX/Gateway devices may have an exclusive LAN/Mgmt Interface for device management purpose other than the Data Interface (also referred as WAN/Public Interface). In such cases LAN Port of the STM should be connected to the Data Interface (WAN/Public Interface).

Deployment Scenario 2

In the case of IPPBX deployed in the LAN Setup, the following setup is recommended as it would help to protect against the threats from both Internal Network as well as the threats from the Public Cloud penetrated the Non SIP aware Corporate Firewall.

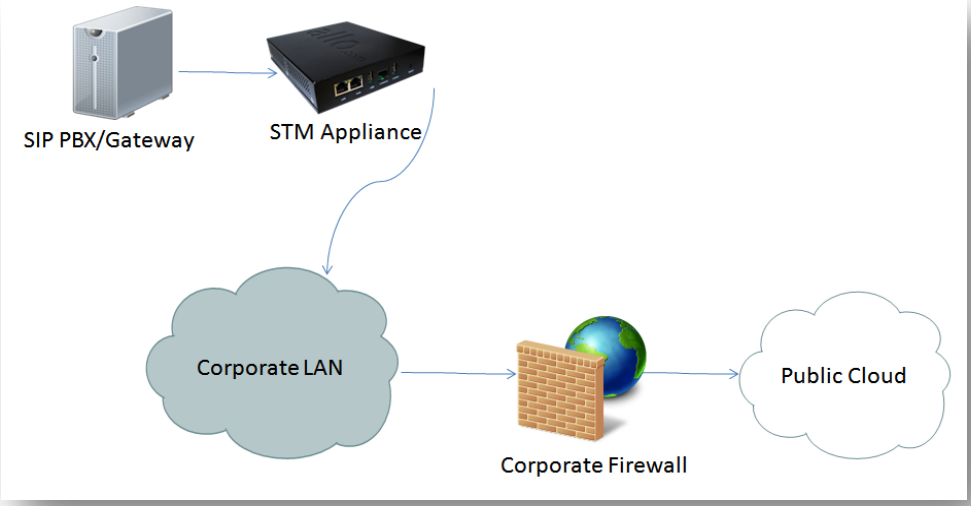

Figure 4: Scenario 2

Deployment Scenario 3

In the case of multiple IPPBX/ VOIP Gateways are deployed in the LAN Setup, the following setup is recommended as it would help to protect against the threats from both Internal Network as well as the threats from the Public Cloud penetrated the Non SIP aware Corporate Firewall.

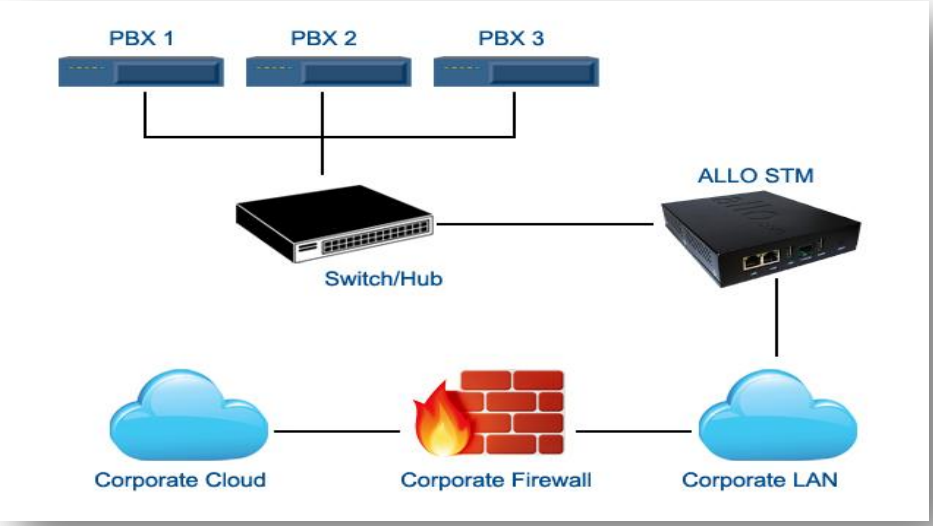

Figure 5: Scenario3

Setup

2. Initial Setup & Configuration

1. Unpack the items from the box
2. Check that you have all the items listed in the package content.
3. Connect the WAN port of the STM to the untrusted/public network.
4. Connect the LAN port of the STM to the PBX/VOIP Gateway.
5. Connect the appliance to the power socket using the USB power cable.
6. The device will take about a minute to boot up & will be fully functional with the default configuration.

Some of the PBX/Gateway devices may have an exclusive LAN/Mgmt Interface for device management purpose other than the Data Interface (also referred as WAN/ public Interface). In such cases LAN port of the STM should be connected to the Data Interface (WAN/ Public Interface).

2.1.Default Configuration

The device operates as a transparent bridging firewall with Deep Packet Inspection enabled on the SIP traffic. By default, the appliance has been configured with static IP of 10.0.0.1 (Net mask 255.255.255.0)

The device has been made to be fully functional with the default configuration. However if the user needs to tune the device settings & the DPI policies, user can tune the configuration via the Device WebUI.

The device all provides the command line interface accessible via SSH, which will allow to configure the basic settings and view device status.

Management Access	Login Credentials
WebUI	admin/admin
SSH CLI	admin/stmadmin
Management Vlan IP	192.168.100.1/255.255.255.0
Default Device IP	10.0.0.1/255.255.255.0

2.2. Accessing the WebUI

The user can connect to the device via management Vlan to access WebUI during initial setup. The management Vlan configured on the device, is accessible via the LAN/WAN ports & is made assigned to the default IP address '192.168.100.1'

Use the procedure given below to access the WebUI,

1. Connect the LAN port of the STM to a PC.
2. Assign the IP Address 192.168.100.2 to the PC. Set the Net mask as 255.255.255.0.

Now you can access the device from the browser using the URL https://<192.168.100.1>

Configure the STM Device IP Address from the "Device Settings" Page as per your local network range. Verify the IP address set to STM from the dashboard page. Once the user assigns the STM Device IP Address successfully, he can access the device using that IP address further.

Now he can disconnect the PC and connect the LAN Port to the PBX/PBX Network that needs to be protected.

The WebUI has been made accessible only via HTTPS. The recommended browser for accessing STM WebUI is Mozilla Firefox.

The UI allows the administrator to configure the management Vlan IP addresses. In case if the user has changed the management Vlan IP address, he needs to assign the corresponding network address to his PC for the management access subsequently.

On launching the STM WebUI, the web application will prompt to enter the administrator credentials to login.

Alternatively the user can access the device via the static IP 10.0.0.1 and configure the network settings during first time installation. Connect a PC to the LAN port of the STM and assign the IP address 10.0.0.100/255.255.255.0 to the PC. Now you can access the device from the browser using the URL https://<10.0.0.1>

If the device is not accessible after configuring the new network configuration, Try rebooting the device and check the device dashboard accessing via Management Vlan.

Figure 6: Login Page

The WebUI login session has been made to time out and if the user does not enter the login credentials for 30 seconds and will redirect to the informational page. The user can click the hyperlink named as 'login' appearing on the information page, to visit the login page again.

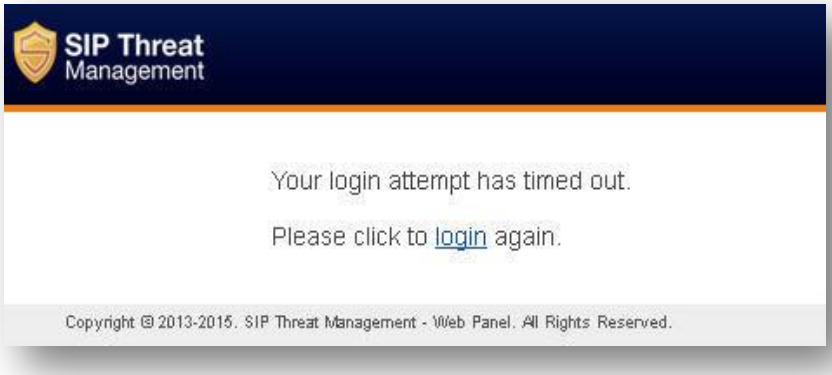

Figure 7: Timeout Message

If somebody is already logged in to STM WebUI session, the subsequent attempts to login will notify the details previous login session as illustrated below and will prompt the user to override the previous session and continue OR to discard the attempt the login.

Figure 8: Select Login Attempt

2.3. WebUI Session timeout

After logging into the WebUI, if there is no activity until the WebUI session timeout period (By default, the WebUI session timeout is set to 900 seconds), then the login session will automatically terminated and browser will be redirected to login page again.

2.4. WebUI Settings

To change the WebUI settings, click the settings icon that appears top right corner (below the Apply Changes button). The WebUI settings dialog will be displayed in the browser and allow the administrator to configure WebUI session timeout & WebUI login password. To configure the WebUI login password, the user needs to enter the previously set administrator password.

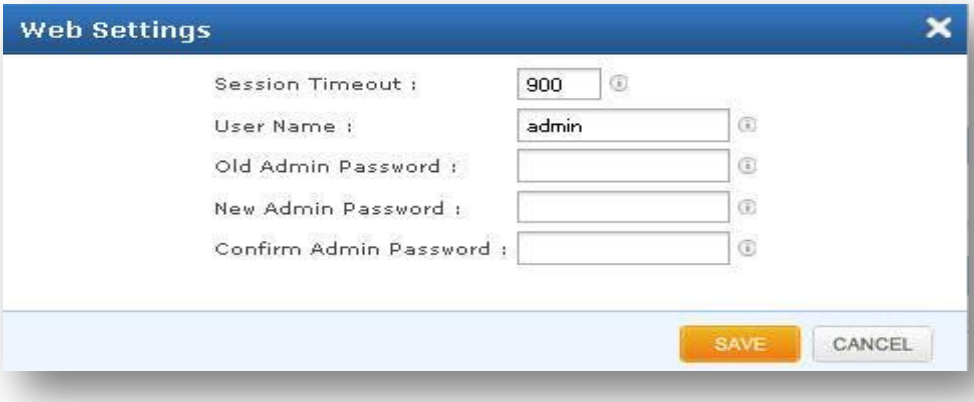

Figure 9: Web Settings

2.5. Dashboard

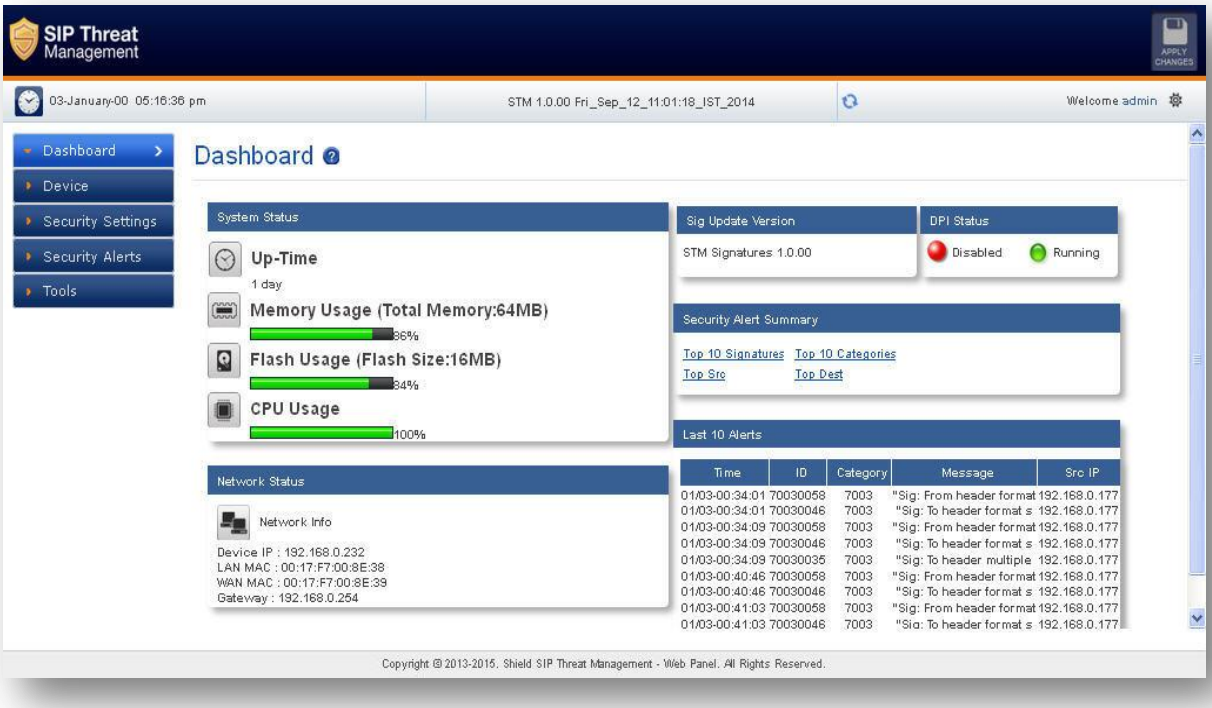

Figure 10: Dashboard

On logging into the STM WebUI, the dashboard will be shown.

The user can visit the dashboard page from the any configuration page in the STM WebUI, by clicking the STM Product Icon that appears in the left corner of the Top panel.

The status panel that appears below the top panel shows the time settings on the device and STM firmware version, Page refresh icon and Setting icon.

On clicking the page refresh button, the main content area in the current page will be refreshed.

On clicking the settings icon, the pop menu which contains menu options logout, WebUI settings will be shown.

System Status Panel shows Device up time, Memory Usage, Flash Usage & CPU Usage.

Sig Update Version Panel shows the STM Signature version and Release State.

Network Status Panel shows IP, LAN MAC, WAN MAC and Gateway of the device.

Security Alert Summary Panel shows hyperlinks for viewing of Top 10 Signatures hit, Top 10 Categories hit, Top Attacker IP Addresses & Top 10 target destinations.

Device Settings

3. Device Configuration

Configuration pages of the STM WebUI have been made as self- intuitive and easy to configure. All the configuration pages have been made to work with the two-phase commit model.

The two-phase commit model is not applicable to time settings and signature update settings. In these settings, the changes will be applied directly by clicking the 'Apply' in the content area of the configuration editor.

I.e. When the administrator changes the settings in the configuration pages and click the Save button, the settings will be saved in a temporary buffer location on the device. On saving the configuration changes, the 'Apply Changes' button that appears in the right top corner will be enabled & the 'Ignore Changes' button will appear next.

Figure 11: Device Configuration

The number of configuration changes will appear on the immediate left to the 'Apply Changes' button. To view the details of the configuration changes, the user can click the number icon, which will open the configuration changes listing.

The user can apply the configuration changes to the device, by clicking 'Apply Changes' button. On clicking the 'Apply Changes' button, the configuration changes will be applied to the system and updated configuration will be persisted permanently onto the device.

In case if the user wants to abandon the configuration changes made, he can click the Ignore Changes button. On clicking the 'Ignore Changes' button, the configuration changes stored in the temporary buffer location will be discarded.

To apply the configuration changes, the 'Ignore Changes' button will be displayed and they cannot choose to ignore configuration changes. The 'Ignore Changes' button will be disabled, only when there are pending configuration changes that need to be applied yet to the device.

If the administrator tries to configure a configuration element to the inappropriate value, the tooltip icon that appears next to each configuration element will provide the details on the error.

On clicking the help icon that appears next to the configuration title, the help section corresponds the current configuration page will be launched.

3.1. General Settings

Navigate through **Device**> **General Settings**

The General settings page will allow configuring the host/network settings of the STM appliance. The device that has been made to work in bridging mode can either choose to work with static IP assignment or to acquire the device IP via DHCP.

The page also allows to enable/disable the SSH Access to the device. The 'Allow ICMP' option will configure the device to respond to the ICMP ping messages sent to STM appliances or not.

By the SSH Access and ICMP Ping messages are allowed to the STM appliance.

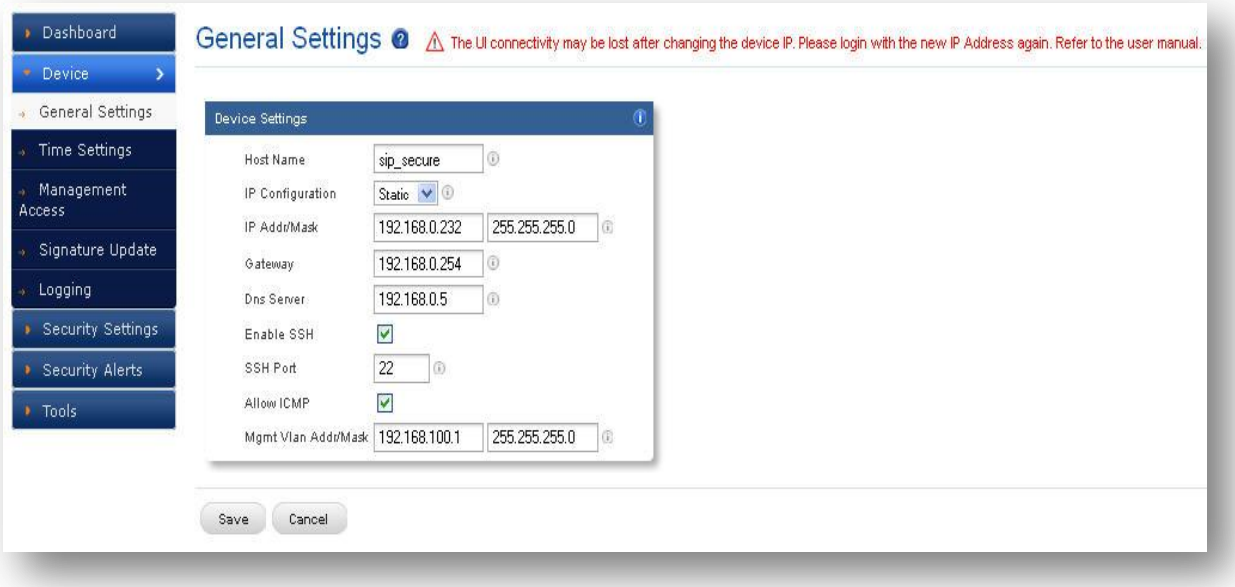

Figure 12: General Settings

Host Name	It allows user to specify the Host name for general settings.
IP Configuration	User can configure IP to be static or DHCP.
IP Addr/Mask	It specifies the IP address and Netmask of STM General Settings.
Gateway	It specifies the Gateway IP of the STM device. E.g. 10.0.0.254 or 10.0.0.1
Dns Server	It helps for domain name resolutions and it stores the DNS records for a domain name.E.g.:10.0.0.5
Enable SSH	It allows the user to either enable or disable SSH port.
SSH Port	User can specify a particular range of SSH port numbers.
Allow ICMP	It allows the user to either enable or disable ICMP.
Management Vlan Addr/Mask	It specifies the management Vlan IP address and Netmask of STM device.

The UI connectivity may be lost after changing the device IP. Please login with the new IP address again.

3.2. Time Settings

Navigate through **Device**> **Time Settings**

The administrator can choose to set the manual time settings on the device or configure the device to sync the time settings from an NTP server. Appropriate time settings/time zone should be set on the device to the correct timestamp to appear on the SIP security alerts generated by the device.

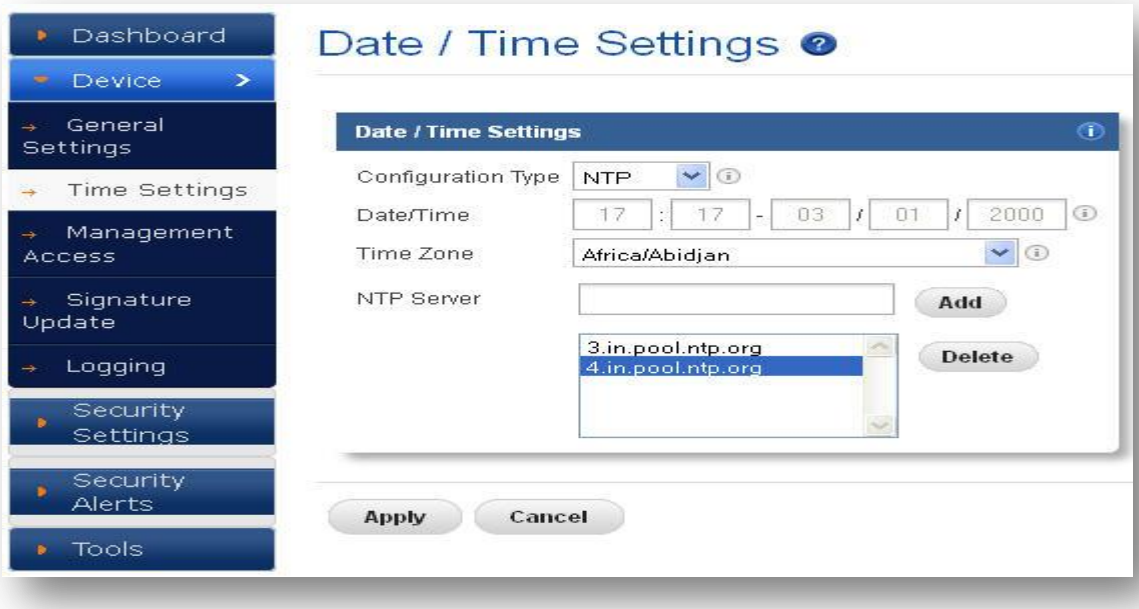

Figure 13: Date/Time Settings

Configuration Type	User can configure either Manual or NTP from the drop down list.
Date/Time	User can configure Date/Time in the format hh:mm-D/MM/YYYY.
Time Zone	User can select time zones from the drop down list.
NTP Server	Enter the NTP server name to synchronize the time of a computer or server. E.g.: 3.in.pool.ntp.org

3.3. Management Access

Navigate through **Device**> **Management Access**

The access the STM Device management (SSH CLI / WebUI Access) can be restricted with the management access filters. By default, the access has been allowed to any global address and

management Vlan network configurations on the device. The administrator can override these settings.

Figure 14: Create Management Access Rule

Name	Enter the name of the Management access for user reference.
IP Type	User can select the appropriate IP type from the drop down list.
Address	Specify IP Address/Netmask or IP range or MAC address.
Enable	It allows the user to either enable or disable Management access rule.
Comments	User can specify the comments in the length of 64 char's. (optional)

The administrator needs to configure the IP Address or the IP Network or the Range of IP Addresses from with management access to the device should be allowed in the management access filter rule. The IP Type 'ANY' indicates global networks (Any network/IP address).

The search option in the management access filters table will help in selectively viewing the management access filter rules whose name/address values that match with the search criteria.

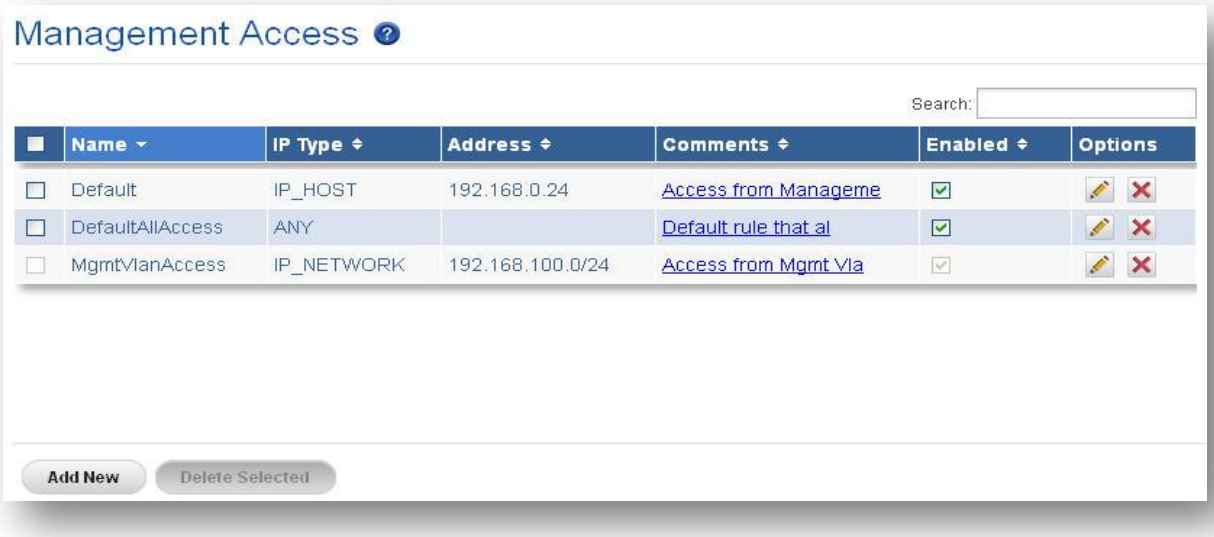

Figure 15: Management Access Results

3.4. Signature Update

Navigate through **Device**> **Signature Update**

To enable the automatic signature update, select the checkbox 'enable update' on the device and configure the signature update schedule. The valid subscription key and correct signature update URL should be configured for the signature update to happen.

To update the signatures on the device instantaneously, Click 'Update Signatures now' button.

Figure 16: Signature Update

Enable Update	It allows the user to either enable or disable Signature Update.
Time Schedule	It schedule signature update at Configured time in UI.

When the user buys the STM appliance, the device will be shipped with the SIP signatures that will help in protecting against the SIP based attacks known as of date.

However, if the user wants to ensure their SIP deployments get the protection against the newest attack vectors, it is recommended to enable the signature update on the device. Please check with an allo Sales representative about getting the details of purchasing the STM signature subscription key.

3.5. Logging

Navigate through **Device**> **Logging**

The administrator can configure the STM appliance to send the security alerts generated on detecting the SIP based attacks, to the remote SYSLOG server.

The logging page will allow enable/disable the remote logging of security alerts and to which SYSLOG server the security alerts are to be forwarded.

Figure 17: Logging

Remote Logging	It allows user to configure Remote Log Server settings.
Syslog Server	User can configure the remote Syslog server where it gets log from the STM device.

Security Settings

4. Configuring the SIP Security Policies

4.1. SIP Attacks Detection

Navigate through **Security** > **SIP Attacks Detection**

The SIP Attack Detection page allows to configure the SIP Deep packet Inspection rules categories. The administrator can enable/disable the inspection against a particular category of rules, action to be taken on detecting attacks matching the rules in the categories.

The possible actions that the STM can execute are logging the alert, block the packets containing the attack vector and blacklist the attacker IP for the given duration. The blocking duration of how long the attacker up needs to be blocked is also configured per category level.

Figure 18: SIP Attacks Detection

The table given below lists the SIP Deep packet Inspection rules categories supported in STM and configuration parameters in each category.

Category	Description	User Configurable options
Reconnaissance Attacks	This can be considered as the first step of attacking any system or a network. In this a hacker tries to learn information about our network typically conducts a ping sweep of the target network to determine which IP addresses are alive. Then the intruder determines which services or ports are active on the live IP addresses. From this information, the intruder queries the ports to determine the type and version of the application and operating system running on the target host. The attacker often uses port scanning, for example, to discover any vulnerable ports. After a port scan, an attacker usually exploits known vulnerabilities of services associated with open ports that were detected.	-
SIP Devices Scanning	The intruder will scan the PBX ports to see what devices are connected to it. With that info, he can exploit 3rd party vulnerabilities. The SBC will not respond to his query.	-
SIP Extensions Discovery	The intruder will ask the PBX to divulge the range of the extension numbers. With that info, he can try different passwords to take control of these extensions. The SBC will not respond to that query.	Invalid SIP User Registration Attempts/Duration
Multiple Authentication	The intruder will try to log in with different user names and passwords multiple times. Once he	Failed Authentication

Failures/Brute force password Attempt	succeeds, he will have control of that extension. The SBC can block, log or blacklist the IP for a period of time if it exceeds the authorized number of trials/second.	Attempts/Duration
Ghost calls Attempt	The intruder will generate calls to an extension and it will look like the calls come from that same extension. His goal is to crash the PBX resulting in disrupted communication. The SBC can block, log or blacklist the IP for a period of time if it exceeds the authorized number of trials/second.	No of Anonymous Invite Responses/Duration
SIP Protocol Compliance	This kind of attacks refers to use of some kind of automated tool like SIPP to generate false script where some of the most important fields of SIP headers and body can body can be modified in terms of their length like "**From header length", "To Header length", "Contact length".** It can also be useful in handling the correct use of Maximum Dialog within a session, SIP Ports and its Protocol.	-
SIP Anomaly Attacks	The SIP Deep packet inspection engine running the STM appliance has been made to inspect the SIP traffic with the SIP Security Compliance rules in built into the SIP DPI engine. The anomalies in the SIP Message headers can result to various erroneous conditions, SIP parser failures & malformed packets which will lead to SIP applications vulnerable to attacks. The Default parameters will be used by the SIP deep packet engine for identifying the different	-

	protocol anomaly conditions and take the action configured by the administrator. Configuring inappropriate values for these parameters can result to the disruptive impact in the VOIP deployment. Administrators with more in-depth understanding with the SIP Protocol can choose to tune these parameters for their specific deployment needs. Otherwise, it is recommended to use the default settings for these parameters.	
SIP Dos Attacks	Flooding attempts using various SIP messages.	No of SIP Request Messages/Duration
SIP DDos Attacks	Distributed flooding attempts using various SIP messages.	No of SIP Response Messages/Duration
SIP Cross site scripting Attacks	Cross Site Scripting (also known as XSS or CSS) is one of the most common application layer hacking techniques. In general, cross-site scripting refers to that hacking technique that leverages vulnerabilities in the code of a web application allow an attacker to send malicious content from an end-user and collect some type of data from the victim. The use of XSS might compromise private information, manipulate or steal cookies, create requests that can be mistaken for those of a valid user, or execute malicious code on the end-user systems. It can be used to steal data about **"From Header", "To Header", "Call -ID", "CONTACT ","Extension Password** and other such confidential	-

	data.	
Buffer overflow Attacks	This refers to illegally trying to access the resources of the SIP device like its memory address for which it does not have the authenticate permissions leading to data corruption of this address along with its adjacent address.	-
3rd Party Vendor Vulnerabilities	This attack refers to any malicious activities from 3rd party like DIGIUM Asterisk channel driver DOS attempt and other such attack.	-
TCP Syn Flood	It's a kind of DOS attack in which a large number of **TCP SYN** packets are sent to the victim's device .Each of these packets will try to establish a new session, thus consuming the victim's device resources. Such attack is also called open half connection as these new sessions are not terminated and finally the legitimate users are barred from availing the Device resources.	No of TCP Syn Packet within specified duration
TCP Flood	This refers to flooding the device with general TCP packet on any port where legitimate users are barred from availing the Device resources after some interval of time.	No of TCP Packet within specified duration
TCP Distributed Flood	In a **TCP DDos** attack, the incoming **TCP traffic** flooding the victim originates from many different sources – potentially hundreds of thousands or more. This effectively makes it impossible to stop the attack simply by blocking a single IP address; plus, it is very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin.	No of TCP Packet within specified duration

UDP Flood	This refers to flooding the device with general **UDP** packet on any port where legitimate users are barred from availing the Device resources after some interval of time.	No of UDP Packet within specified duration
UDP Distributed Flood	In a **UDP DDos** attack, the incoming **UDP traffic flooding** the victim originates from many different sources – potentially hundreds of thousands or more. This effectively makes it impossible to stop the attack simply by blocking a single IP address; plus, it is very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin.	No of UDP Packet within specified duration
Generic Attacks	Some of the common attacks under this category are Bye Teardown, Registration Hijack, Registration Adder, and Registration Eraser. 1) Bye Teardown attack disrupts a call that is in session between two users. 2) **Registration Hijack:** The first step in hijacking a registration is to find register able addresses and it hijacks the already registered extension. 3) **Registration Adder:** This tool attempts to bind another SIP address to the target, effectively making a phone call ring in two places (the legitimate user's desk phone and the attacker's phone). 4) **Registration Eraser:** This tool will effectively cause a denial of service by sending a spoofed SIP REGISTER message to convince the proxy that a phone/user is unavailable.	-

4.2. SIP Protocol Compliance

Navigate through **Security Settings** > **SIP Protocol Compliance**

The SIP Deep packet inspection engine running the STM appliance has been made to inspect the SIP traffic with the SIP Security Compliance rules in built into the SIP DPI engine.

The anomalies in the SIP Message headers can result to various erroneous conditions, SIP parser failures & malformed packets which will lead to SIP applications vulnerable to attacks.

The following parameters will be used by the SIP deep packet engine for identifying the different protocol anomaly conditions and take the action configured by the administrator.

Configuring inappropriate values for these parameters can result to the disruptive impact in the VOIP deployment. Administrators with more in-depth understanding with the SIP protocol can choose to tune these parameters for their specific deployment needs. Otherwise, recommended to use the default settings for these parameters.

Figure 19: SIP Protocol Compliance

SIP Protocol Compliance Settings

Max_sessions

A SIP session is the application level connection setup created between the SIP server and SIP client for exchanging the audio/video messages with each other.

The max_sessions parameter defines the maximum number session that SIP deep packet inspection engine can keep track of. The default value has been set at 4096.

Max Dialogs per Session

Max_Dialogs_per_session specifies the maximum number of SIP message transaction that can happen between the SIP server and client.

Methods

This specifies on what methods to check for SIP messages. Following are the SIP messages that SIP DPI Engine can identify: (1) invite, (2) cancel, (3) ack, (4) bye, (5) register, (6) options, (7) refer, (8) subscribe, (9) update (10) join (11) info (12) message (13) notify (14) prack.

Max_uri_len

The Uri identifies the user or service to which SIP request is being addressed. Max_uri_len specifies the maximum Request URI field size. The Default is set to 256. The allowed range for this option is 1 - 65535.

Max_call_id_len

The Call-ID header field in SIP message acts as a unique identifier that relates to sequence of messages exchanged between SIP client and server. Max_call_id_len specifies the maximum Call-ID field size. The Default is set to 256. The allowed range for this option is 1 - 65535.

Max_requestName_len

Max_requestName_len specifies the maximum request name size that is part of the CSeq ID. The Default is set to 20. The allowed range for this option is 1 - 65535

Max_from_len

The From header field indicates the identity of the initiator of the SIP request. Max_from_len specifies the maximum from field size. The allowed range for this option is 1 - 65535.

Max_to_len

The to header field specifies the desired recipient of the SIP request. Max_to_len specifies the maximum to field size. The Default is set to 256. The allowed range for this option is 1 - 65535.

Max_via_len

The Via header field indicates the transport used for the SIP transaction & identifies the location where the SIP response is to be sent.

Max_via_len specifies the maximum via field size. The Default is set to 1024. The allowed range for this option is 1 - 65535.

Max_contact_len

The Identifier used to contact that specific instance of the SIP client/server for subsequent requests. Max_contact_len specifies the maximum Contact field size. The Default is set to 256. The allowed range for this option is 1 - 65535.

Max_content_len

Max_content_len specifies the maximum content length of the message body. The Default is set to 1024. The allowed range for this option is 1 - 65535.

SIP Ports Configuration

SIP Transport – User can select SIP transport type either TCP or UDP or any which are related to SIP communication from GUI.

SIP Ports – User can configure SIP ports which are related to the SIP communication from GUI. E.g.: 5060,5061,5070

SIP Methods- User can select options from the SIP method lists.

SIP/Media Ports Configuration

It allows users to configure SIP/Media port configuration.

It is used to store and deliver information or data over communication medium. Media may be TCP based or UDP based communications.

STM media settings allows user to choose the communication medium of the SIP traffic. It supports TCP, UDP or Both as communication media for SIP Communications. Media ports allow user to configure media ports like 1024-65535.

SIP/Media Ports Configuration	
SIP Transport	It allows user to select the type of Media Transport. EX.TCP, UDP or any.
SIP Ports	User can specify a value for SIP ports. E.g.: 5060,5061
Media Transport	It allows user to select the type of Media Transport. EX.TCP, UDP or any.
Media Ports	User can configure SIP Media ports which are related to SIP communication media. Ex: 1024-65535

4.3 Call Blocker Rules

Navigate through **Security Settings** > **Call Blocker Rules**

A user can block the calls statically by making use of "Call Blocker Rules" feature in STM. This feature will block the calls by various viable options such as Phone number, Phone number prefix, Phone Extension, Phone Extension Prefix, IP address and User Agent. It allows you to configure multi rules to block different calls.

It displays the Call Blocker Rules along with name, Caller Block type, Value, Comments, Enabled, and Options.

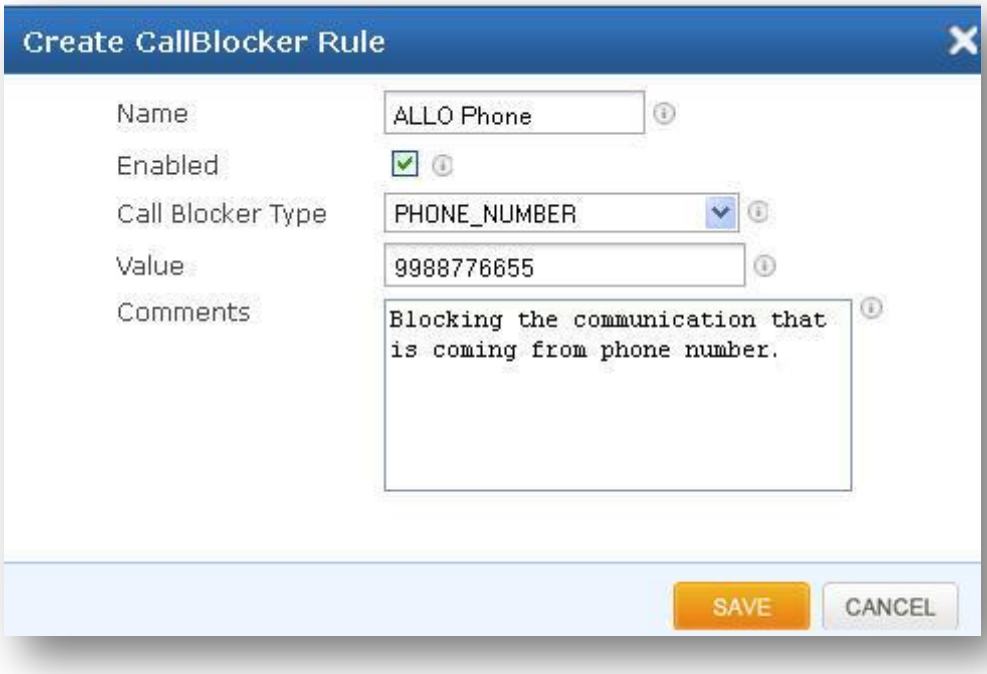

Figure 20: Create Call Blocker Rule

Name	Specify the name for the Call Blocker Rule for user's reference. The user can choose any name to recognize the Call Blocker Rules.
Enabled	It allows the user to either enable or disable Call Blocker Rule.
Call Blocker Type	User can select the appropriate Call Blocker type from the drop down list. It allows user to block the calls that reaching to PBX system i.e. protected by the STM. E.g. 1. **Phone number:** User can block the SIP communication which is originated from any phone number. E.g. 9988776655 2. **Phone number prefix:** User can block the SIP communication which is originated from any phone number by specifying phone extensions. E.g.: 0 or +91 3. **Phone Extension**: User can block the SIP communication by specifying phone extensions. E.g.: 100,101, 3004 4. **Phone Extension Prefix:** User can block the SIP communication by specifying prefix of phone extensions. E.g.: 0

	5. **IP Address:** User can block the SIP communication which is coming from configured IP in GUI. E.g192.168.0.58 6. **User Agent:** Each phones having their unique user agents. They can block the SIP communication by configuring user agent in GUI. E.g.: eyebeam release 1003s stamp 31159
Value	User can specify the value of Call blocker types like IP address, Phone number, user agent etc. E.g.: Phone number- 9988776655 IP Address- 192.168.0.58
Comments	User can specify the comments in the length of 64 char's. (optional)

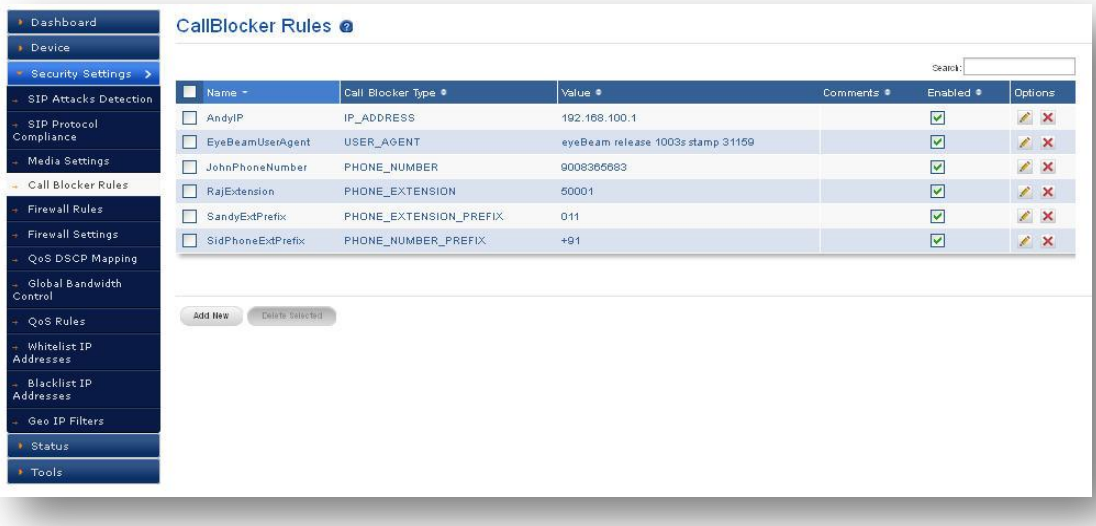

Figure 21: Call Blocker Rules Result

4.4 Firewall Rules

Navigate through **Security Settings** > **Firewall Rules**

The firewall rules configuration will allow the administrator in configuring what traffic should be allowed to protect SIP PBX/Gateway network from an untrusted wan zone, besides DPI enabled SIP traffic and RTP traffic. The administrator needs to specify the source and destination networks and port numbers and protocol that will be used as the matching criteria in the filtering rules and action to be taken on matching the filtering rule. The possible actions are to block the

traffic and allow the traffic on matching the filtering rule. The rules precedence will be in the order in which the rules configured on firewall rules table.

Figure 22: Create Firewall Rule

Name	Specify the name for the Firewall Rules for user's reference. The user can choose any name to recognize the Firewall Rules.
Enabled	It allows the user to either enable or disable Firewall Rules.
Src Type	User can select the appropriate Src type from the drop down list.
Src Address	User can configure and apply the Firewall rule to particular Source Address (Src Address). E.g.10.0.0.3
Dst Type	User can select the appropriate Dst type from the drop down list.
Dst Address	User can configure and apply the Firewall rule to particular destination Address (Dst Address). E.g.:192.168.0.8
Protocol	Protocols specify interactions between the communicating entities. User can select the type of protocol whether it is TCP or UDP from the drop down list.
Port	User can configure and apply the Firewall rule to particular port number.E.g.:5060
Action	User can select the action either block or action from the drop down list.

Figure 23: Firewall Rules

4.5 Firewall Settings

Navigate through **Security Settings**> **Firewall Settings**

Firewall Settings allows user to configure TCP Flood Rate, TCP Flood Burst, UDP Flood rate and UDP Flood Burst in Global firewall settings.

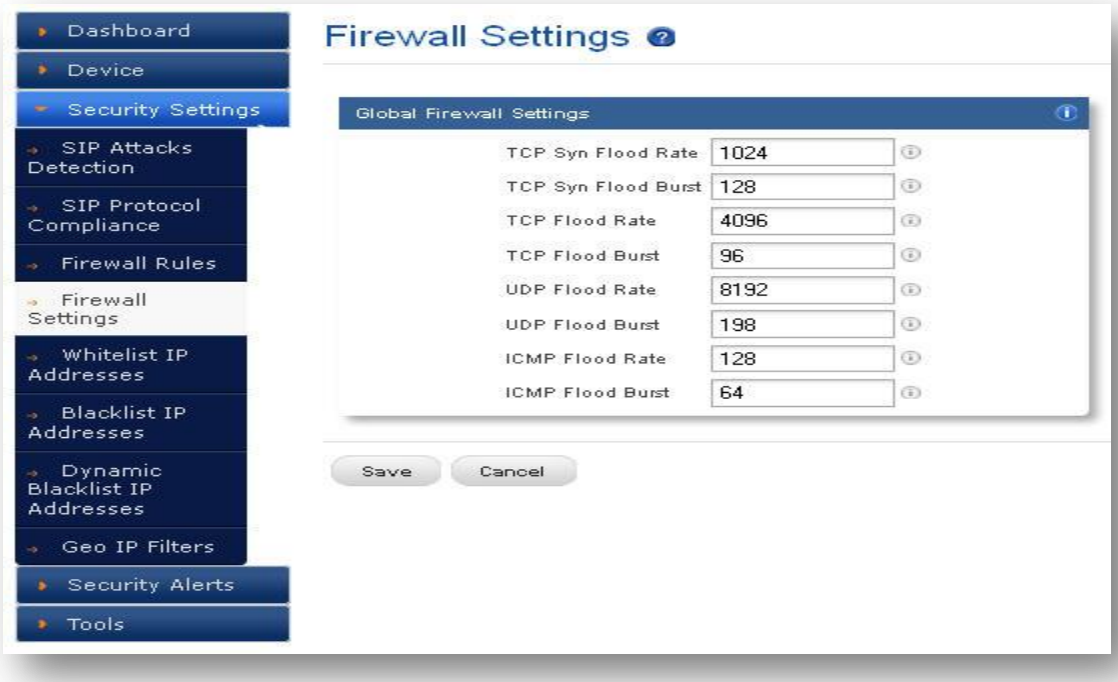

Figure 24: Firewall Settings

4.6 Whitelist IP Addresses

Navigate through **Security Settings** > **Whitelist IP Addresses**

This page allows to configure the white listed IP addresses in the untrusted wan zone from which the access to communicate with the protected SIP network will be allowed by the STM.

This page will also allow configuring whether the white rules take precedence over the blacklist rules (both static and dynamic) configured on the device at any instant.

Figure 25: Create White list Rule

Name	Specify the name for the White list Rules for user's reference. The user can choose any name to recognize the White list Rules.
IP Type	User can select the appropriate IP type from the drop down list.
Address	Specify IP Address/Netmask or IP range or MAC address.
Enable	It allows the user to either enable or disable White list Rules.
Comments	User can specify the comments in the length of 64 char's.

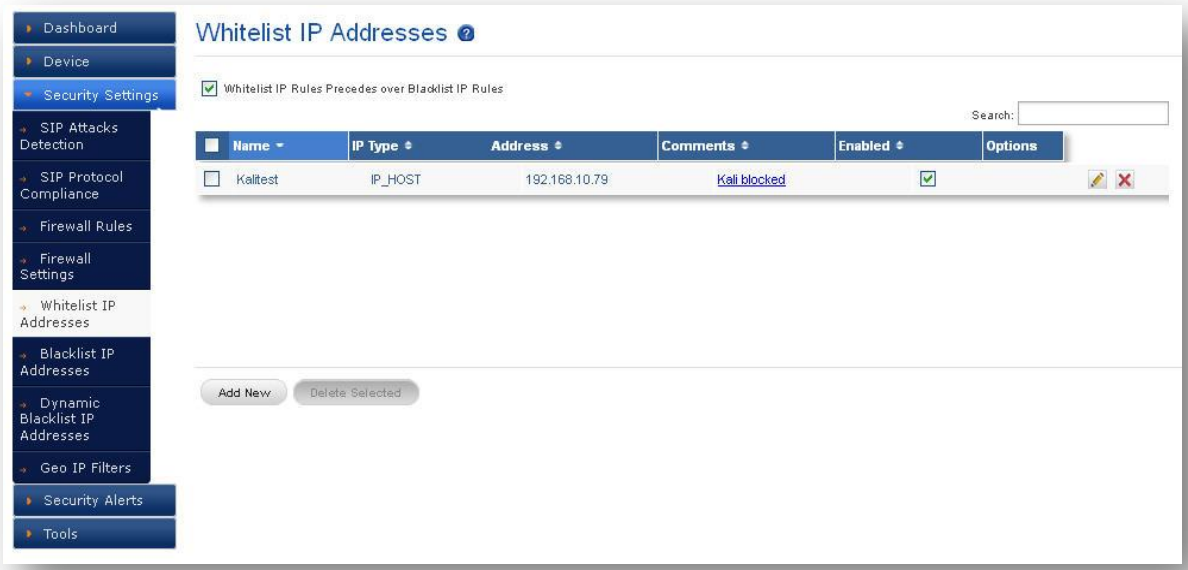

Figure 26: White list IP Addresses

4.7. Blacklist IP Addresses

Navigate through **Security Settings** > **Blacklist IP Addresses**

This page allows to configure the blacklisted IP addresses in the untrusted wan zone from which the access to communicate with the protected SIP network will be blocked by the STM.

This page will also allow configuring whether the white rules take precedence over the blacklist rules (both static and dynamic) configured on the device at any instant.

Figure 27: Create Blacklist Rules

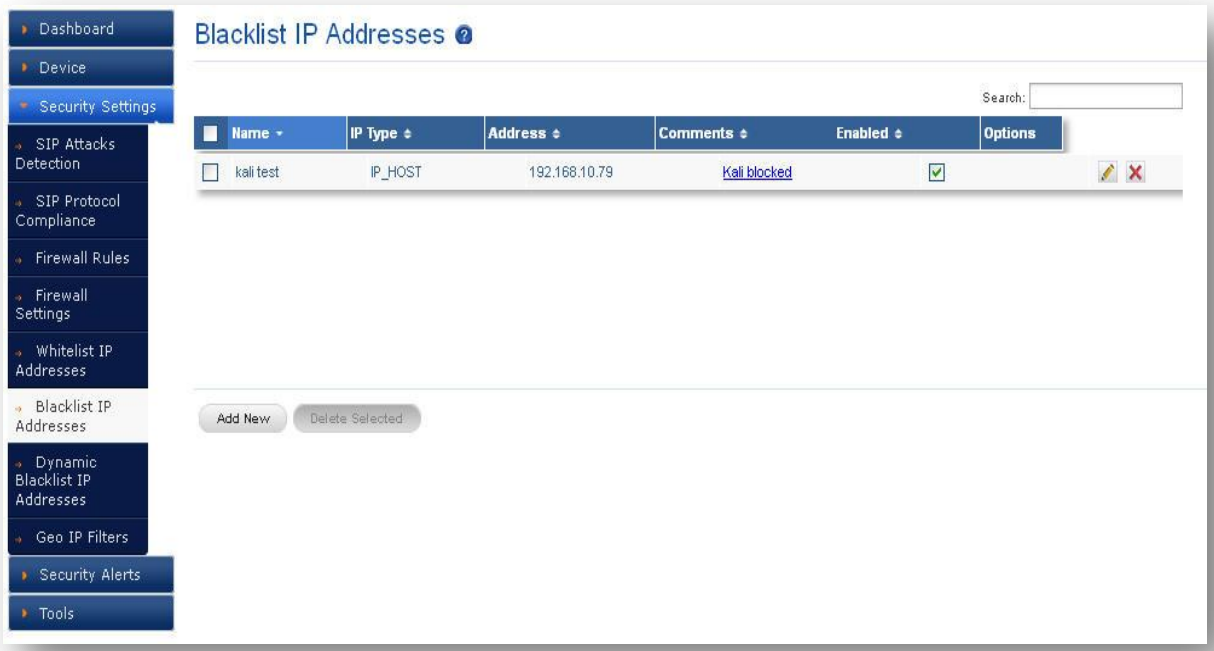

Figure 28: Blacklist IP Addresses

4.8. Dynamic Blacklist IP Addresses

Navigate through **Security Settings** > **Dynamic Blacklist IP Addresses**

The dynamic blacklist IP Addresses are the blocking rules added by the STM deep packet inspection engine to block the traffic from attacker IP addresses for the blocking duration configured in the rules category, on detecting the attack.

The dynamic blacklist IP addresses will allow the administrator to see the dynamic blacklist rules currently configured on the device at any instant. In case, if the administrator wants to override and allow the traffic from particular blacklisted IP, he can delete the rule from the dynamic blacklist IP addresses page.

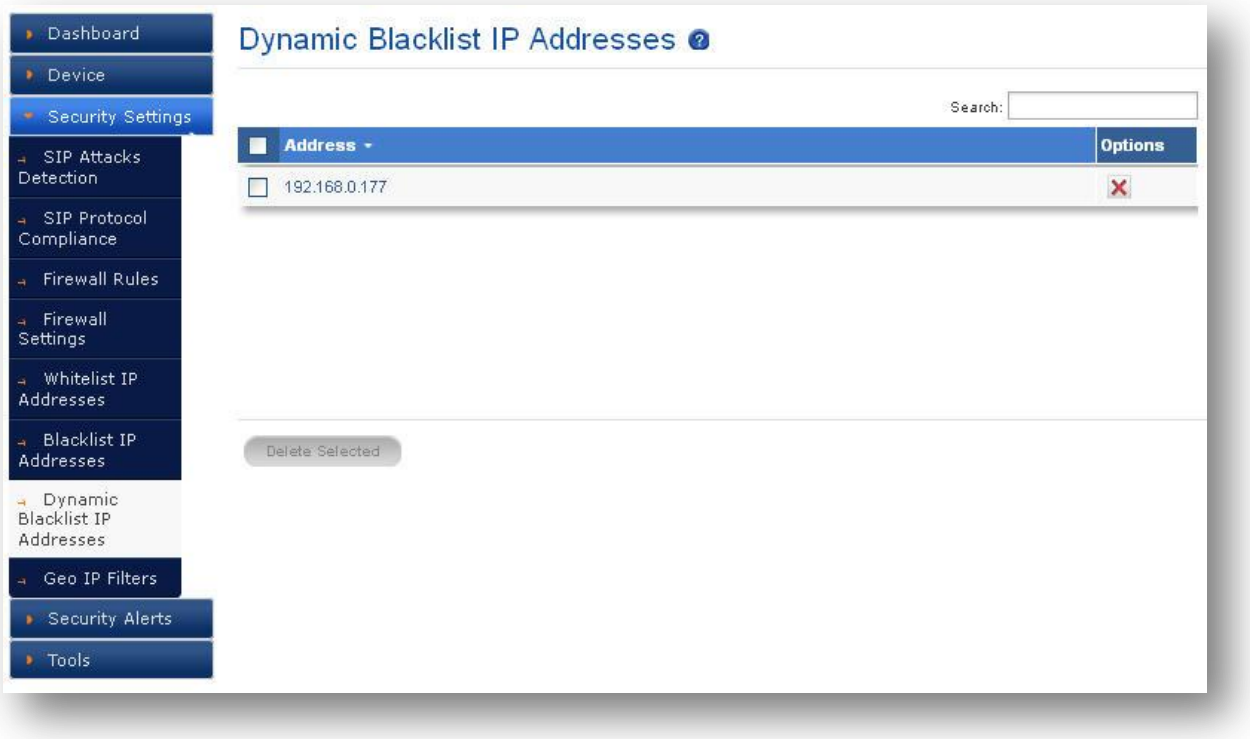

Figure 29: Dynamic Blacklist IP Addresses

4.9. Geo IP Filters

Navigate through **Security Settings** > **Geo IP Filters**

The administrator can choose to block the traffic originating from the specific countries towards the protected SIP network, by configuring the GeoIP filter rules in STM.

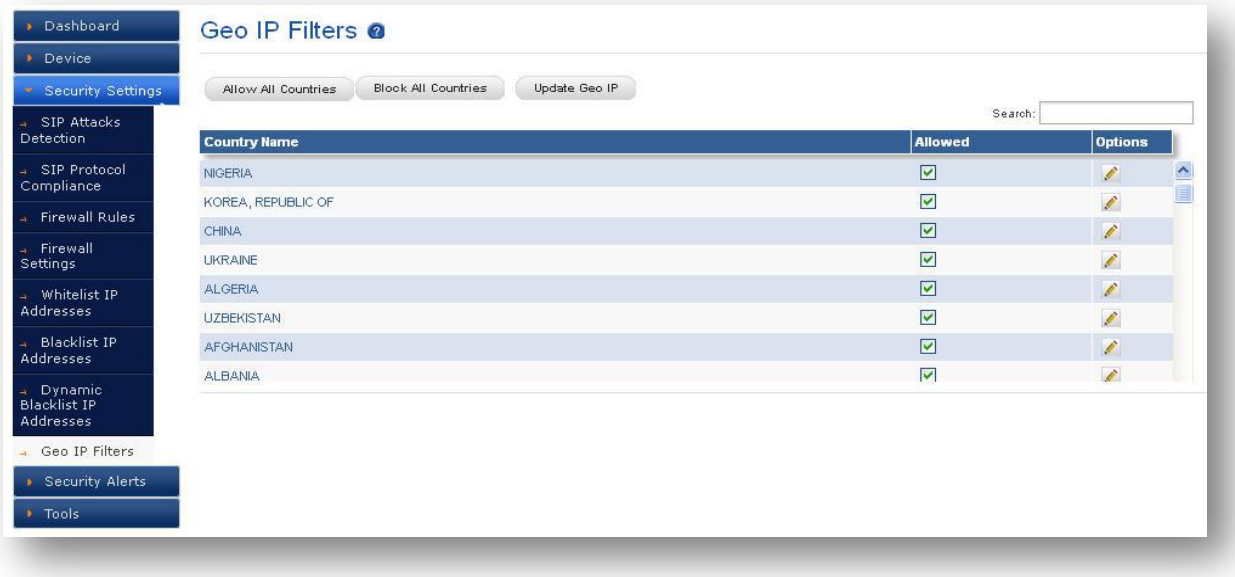

Figure 30: Geo IP Filters

Status

5. Status

5.1. Security Alerts

Navigate through **Status**> **Security Alerts**

The status alerts page shows the list of alerts pertaining to the SIP attacks detected the STM Deep packet inspection engine at any instant.

The administrator can choose to set log viewer page refresh interval in this page. It also chooses to configure the device to send email notifications summary about the security alerts generated by the device.

The option to download the security alerts shown in this page in CSV format is available on the page.

Figure 31: Security Alerts

Unless the user configures to forward the security alerts to remote SYSLOG server, the security alerts are not persisted permanently on the device. The logging buffer location will be flushed at the predefined interval (not configurable) will once the logging threshold criteria met. However if the administrator wants to persist the alerts into an USB storage, they can connect the USB storage to the USB data port of STM appliance. The rotated logs will be automatically archived in CSV format into USB storage by the STM appliance.

Email Server Settings

Navigate through **Security Alerts**> **Email Server Settings**

This feature allows user to send the generated alerts in STM to the specified user.

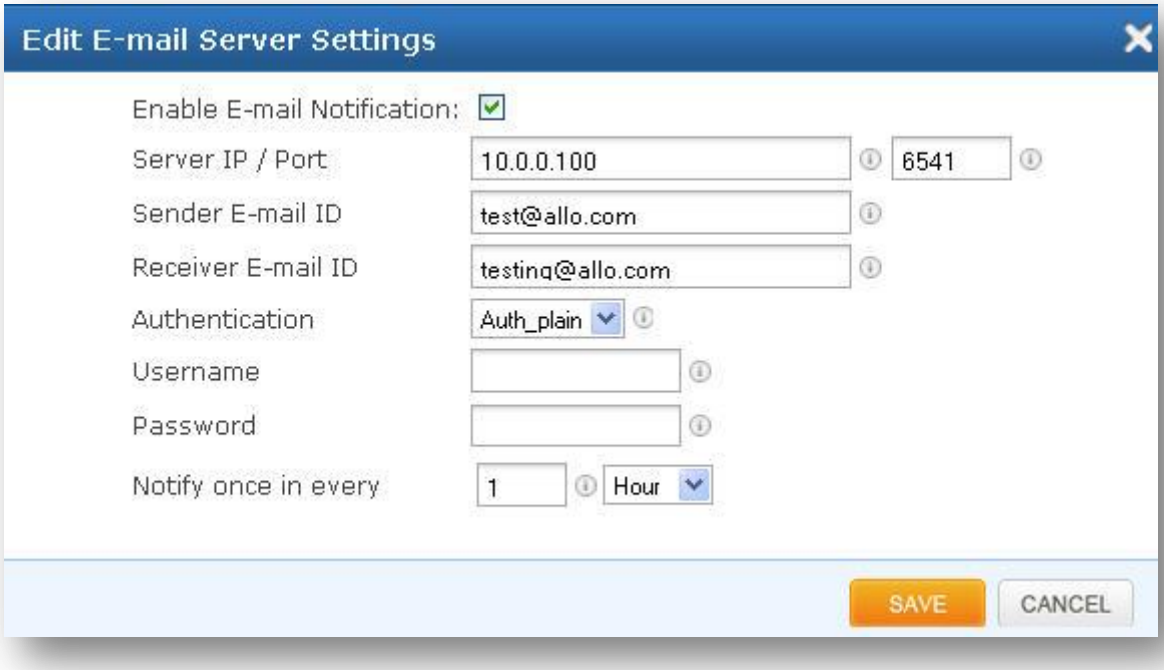

Figure 32: Edit Email Server Settings

Enable E-mail Notification	User can either enable or disable this email notification.
Server IP/Port	User can specify the Email server IP address and Server port.
Sender Email ID	The user can extends the verification process to include professed responsible addresses. Eg: test@allo.com
Receiver Email ID	The user can specify the Receiver email id Eg: testing@allo.com
Authentication	User can select authentication from the drop down list. If authentication is required by the End point.
Username	Username of endpoint (e.g.: Testing) will use to authenticate with the Email server settings.
Password	Enter the Password and its authenticating Email server settings.
Notify once in every	User can notify the alerts in email for every week, every day etc.

6. Tools

6.1. Administration

Navigate through **Tools**> **Administration**

The Administration user interface page provides the option for running a factory reset on the device, restarting the device, device reboot, device shutdown & Configuration backup/restore.

Running factory-reset on the device requires reboot, thus the administrator will be redirected wait notification page on clicking the factory reset button and will be prompted login once the device comes up with the default configuration.

The STM appliances support taking the configuration backup and restore the configuration later.

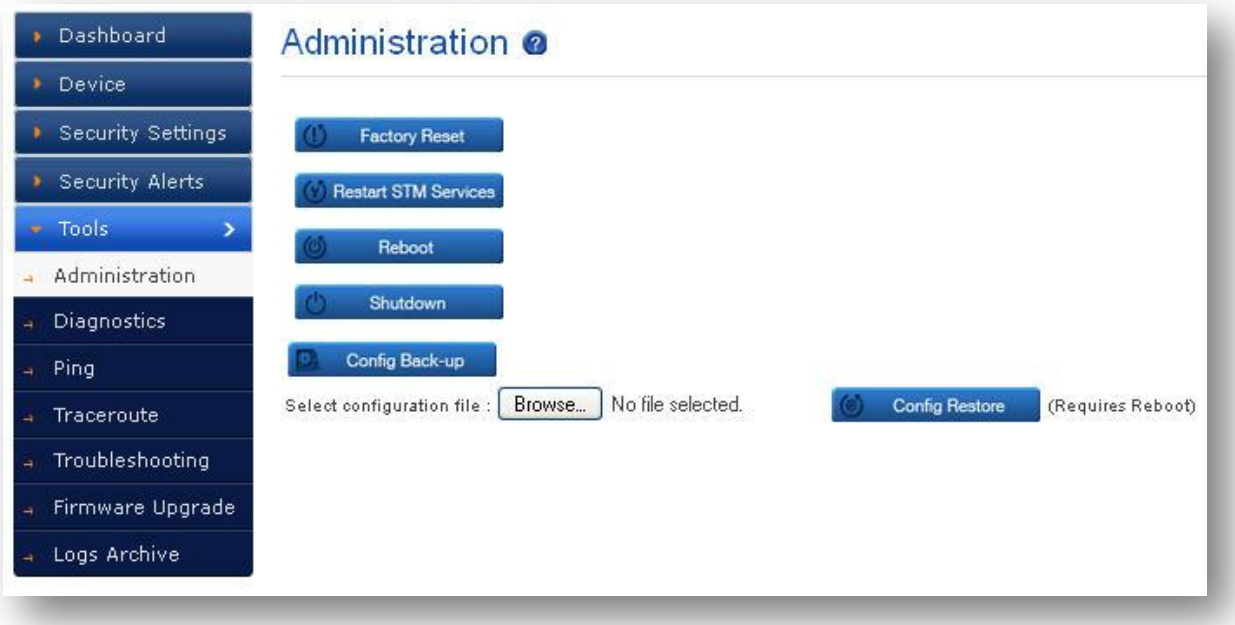

Figure 33: Administration

The configuration backup will contain the lastly persisted configuration, if there are any transient changes that are yet to be applied while taking the backup; those configuration changes will not be included in the configuration backup archive.

6.2. Diagnostics

Navigate through **Tools**> **Diagnostics**

The diagnostics page will allow the administrator to gather the troubleshooting logs which will help allo Support team in debugging any issues faced with STM deployment setup.

To run the utility on the device, the administrator needs to click the 'Run diagnostics' button. The device will run the diagnostics task in the backend and display the results once the task is complete. The administrator can download the reports by clicking the 'Get Report' button and send the report to allo Support team (Note: You can submit through support ticket: http://support.allo.com

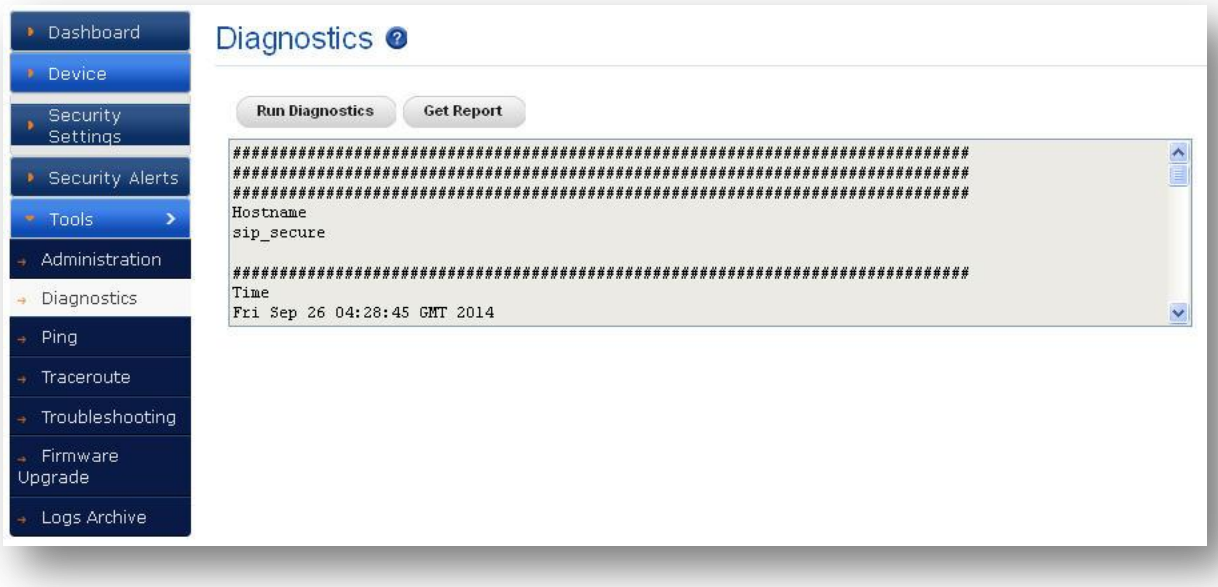

Figure 34: Diagnostics

Click the above link to download the diagnostics.

Figure 35: Download Report

6.3. Ping

Navigate through **Tools**> **Ping**

The administrator can troubleshoot the network connectivity issues with running ping from the STM device.

The administrator needs to enter the IP address that needs to be pinged from the STM appliance/ping count and click the 'Ping' button to run the task. The ping results will be displayed in the text area once the ping task is complete.

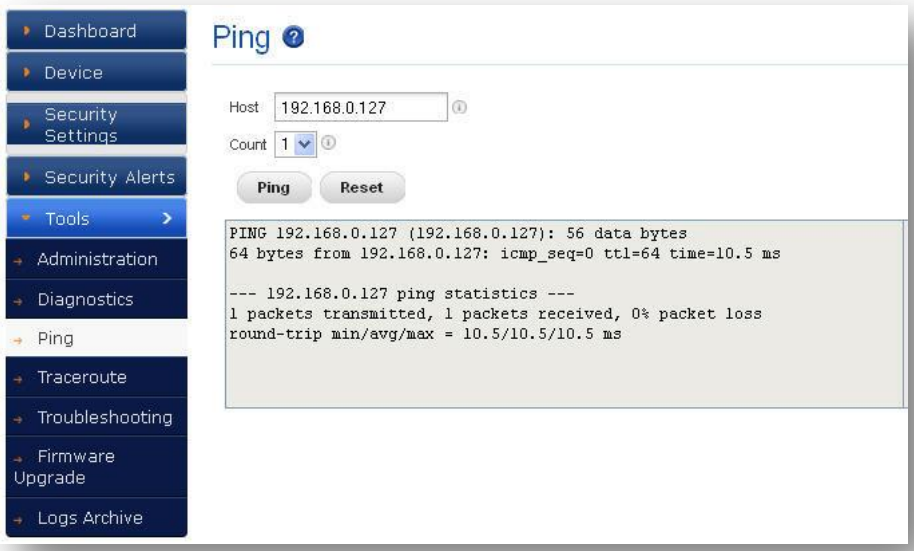

Figure 36: Ping Result

6.4. Trace route

Navigate through **Tools**> **Trace route**

The administrator can troubleshoot the network connectivity issues with running a trace route from the STM device.

The administrator needs to enter the IP address to which the route needs to be traced from the STM appliance/hop count and click the 'Trace route' button to run the task.

The trace route results will be displayed in the text area once the trace route task is complete.

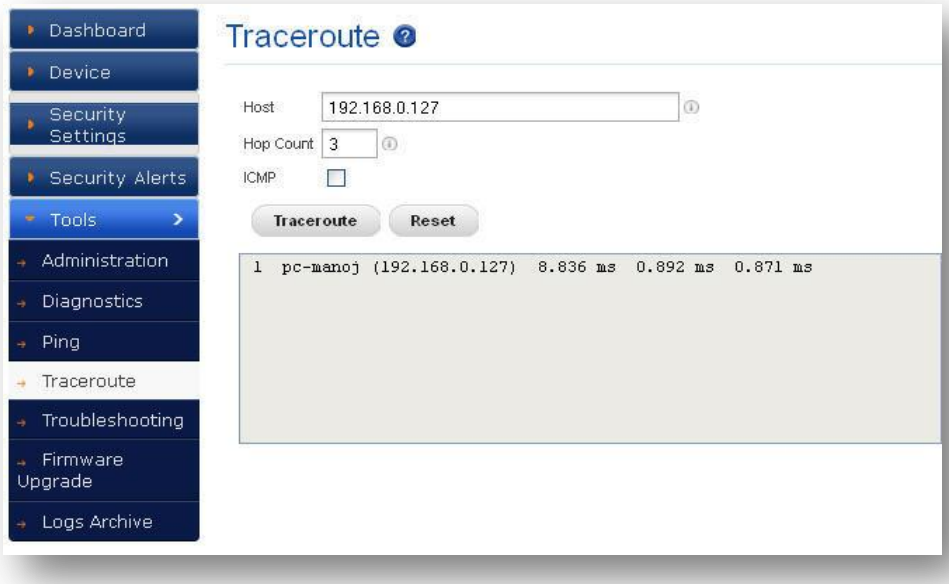

Figure 37: Trace route

6.5. Troubleshooting

Navigate through **Tools**> **Troubleshooting**

This page will allow disable/enable the DPI on the STM appliance for troubleshooting purposes.

Figure 38: Troubleshooting

6.6. Firmware Upgrade

Navigate through **Tools**> **Firmware Upgrade**

The STM appliance supports the manual upgrade on the STM firmware running on the appliance. The firmware upgrade page shows the currently running STM firmware version and allows the administrator to upload the firmware update package onto the device and install.

To install the firmware,

- Download the STM firmware update package from allo website and keep it your local system.
- From the browser on your local system, login to STM WebUI and launch the STM firmware upgrade page.
- Click the 'Browse' in the firmware page and select the STM firmware update package file that you saved on your local system.
- After selecting the file, click the 'Upgrade' button.
- The device will verify the firmware uploaded and install. After install the device will reboot and administrator will be redirected the login page.

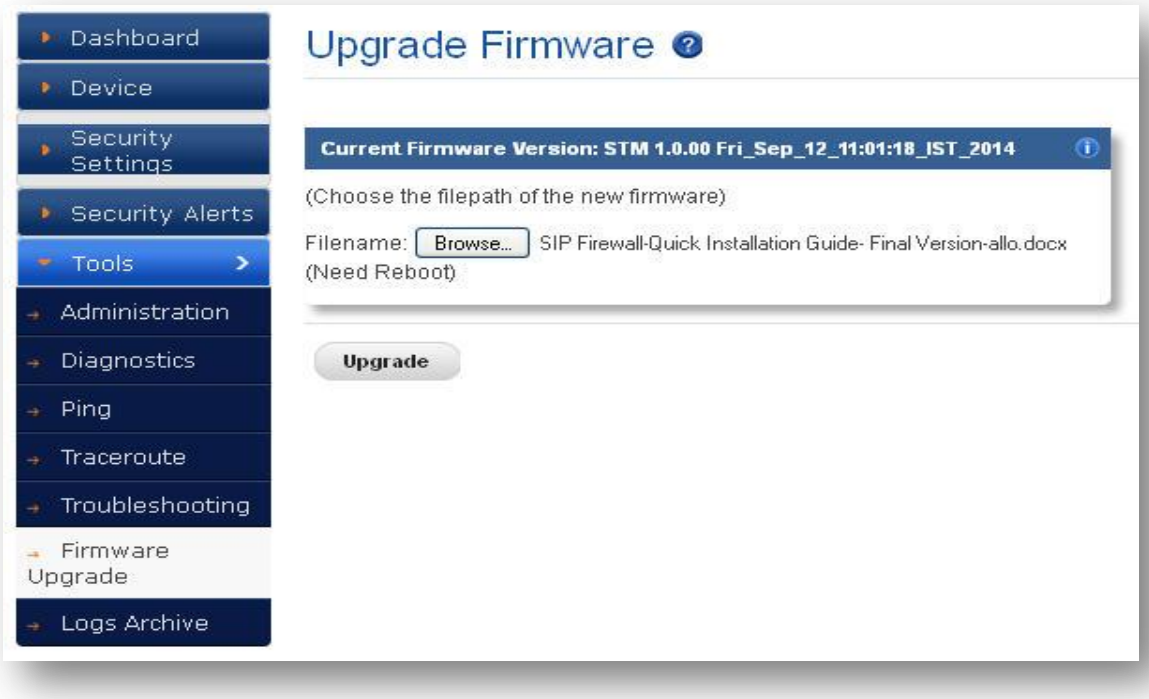

Figure 39: Upgrade Firmware

6.7. Logs Archive

Navigate through **Tools**> **Logs Archive**

If the USB storage device attached to STM, the device will attempt to archive older logs in the USB storage device. The summary information on the logs stored on the archive will be shown on the Logs Archive Page.

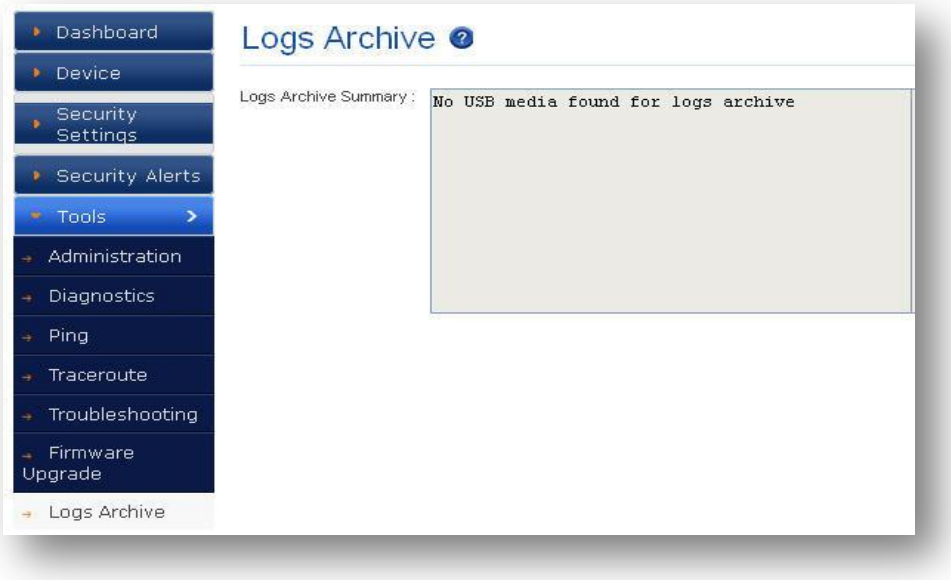

Figure 40: Logs Archive

The Administration user interface page provides the option for running a factory reset on the device, restarting the device, device reboot, device shutdown & Configuration backup/restore.

Running factory-reset on the device requires reboot, thus the administrator will be redirected wait notification page on clicking the factory reset button and will be prompted login once the device comes up with the default configuration.

The STM appliances support taking the configuration backup and restore the configuration later.

FAQs

7. Frequently Asked Questions (FAQs)

What are SIP Threat Management (STM) devices?

SIP threat management (STM) is an approach to security management that allows an administrator to monitor and manage a wide variety of security-related applications and infrastructure components through a single management console. SIP Threat Management (STM) devices combine an Intrusion Prevention System (IPS), Firewall into a single hardware platform.

What is a Network Security? How STM gives security to Network?

Network security consists of the provisions and policies adopted by a network administrator. It is to prevent, monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. STM gives security to internal network by making use of Firewall, IPS (Intrusion Prevention System) etc.

What are the advantages of SIP Threat Management?

SIP Threat Management is a cost-effective solution to integrate multiple features into a single appliance.

I. Easy to configure
II. Less time used for maintenance
III. Better performance
IV. Cost Effective

What does SIP Threat Management Include?

SIP Threat Management includes the following features

1. Firewall
2. IPS (Intrusion Prevention System)
3. Network QoS
4. Bandwidth Control

Glossary

8. Glossary

Term	Definition
DoS *(Denial of Service)*	DoS are an attempt to make a machine or network resource unavailable to its intended users.
DDos *(Distributed Denial of Service)*	DDOS is a type of DOS attack where multiple compromised systems which are usually infected with a Trojan are used to target a single system causing a Denial of Service (DoS) attack.
RTP *(Real Time Transport Protocol)*	RTP defines a standardized packet format for delivering audio and video over IP networks
RTCP- *Real-time control protocol*	The RTP Control Protocol (RTCP) is a sister protocol of the Real-time Transport Protocol (RTP). Its basic functionality and packet structure is defined in RFC 3550. RTCP provides out-of-band statistics and control information for an RTP session.
BPS*- Bit Per Second*	Its abbreviated bps or bit/sec is a common measure of data speed for computer modems and transmission carriers.
SSH*- Secure SHell*	It's a UNIX-based command interface and protocol for securely getting access to a remote computer.
DSCP - Differentiated Services Code Point	DSCP is a field in an IP packet that enables different levels of service to be assigned to network traffic. This is achieved by marking each packet on the network with a DSCP code and appropriating to it the corresponding level of service.
QoS -Quality of Service	QoS is the idea that transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance.
HTTP *-Hyper Text Transport Protocol*	It works on TCP protocol & Port number is 80. It's an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web. Hypertext is

Term	Definition
	structured text that uses logical links (hyperlinks) between nodes containing text.
HTTPS *-Hyper Text Transport Protocol over Secure Socket Layer*	It makes more difficult for hackers, the NSA, and others to track users. The protocol makes sure the data isn't being transmitted in plain-text format, which is much easier to eaves drop on.
NTP *- Network Time Protocol*	It is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
DNS*- Domain Name Server*	DNS are the Internet's equivalent of a phone book. They maintain a directory of domain names and translate them to Internet Protocol (IP) addresses. This is necessary because, although domain names are easy for people to remember, computers or machines, access websites based on IP addresses.
SIP*-Session Initiation Protocol*	It is a signaling communications protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP) networks.
DHCP*- Dynamic Host Control Protocol*	It is a standardized network protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.
FTP*- File Transfer Protocol*	It is a standard network protocol used to transfer computer files from one host to another host over a TCP-based network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.
TFTP- Trivial File Transfer Protocol	It's a simple, lock-step, file transfer protocol which allows a client to get from or put a file onto a remote host. One of its primary uses is in the early stages of nodes booting from a Local Area Network.
SMTP *- Simple Mail Transfer Protocol*	A protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP.

Term	Definition
SSL *- Secure Socket Layer*	This is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.
IP *- Internet Protocol*	It's a set of rules governing the format of data sent over the Internet or other network. The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.
MAC *- Media Access Control*	This is one of two sub layers of the Data Link Control layer and is concerned with sharing the physical connection to the network among several computers.
ICMP *- Internet Control Message Protocol*	It is one of the main protocols of the Internet Protocol Suite. It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached.
IMAP*- Internet Message Access Protocol*	IMAP is a protocol for e-mail retrieval and storage.
POP3*- Post office Protocol version 3*	It's a standard protocol for retrieving e-mail. The POP3 protocol controls the connection between a POP3 e-mail client and a server where e-mail is stored. The POP3 service uses the POP3 protocol for retrieving e-mail from a mail server to a POP3 e-mail client.
TCP *- Transmission Control Protocol*	It is a standard that defines how to establish and maintain a network conversation via which application programs can exchange data. TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other. Together, TCP and IP are the basic rules defining the Internet.
UDP *- User datagram protocol*	It is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control

Term	Definition
	Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP.
TCP/IP- *Transmission Control Protocol/Internet Protocol*	This is the suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP.
LAN *- Local Area Network*	This is a group of computers and associated devices that share a common communications line or wireless link. Typically, connected devices share the resources of a single processor or server within a small geographic area.
WAN *- Wide Area Network*	It's a geographically dispersed telecommunications network. The term distinguishes a broader telecommunication structure from a local area network.

Appendix

9. Appendix A – Using Console Access

1. Connect the serial console the serial port of STM device.
2. Use the following serial console settings to access the 'allo' CLI
    i. Speed : 38400
    ii. Parity : None
    iii. Data : 8
    iv. Stop bits : 1
    v. Flow control : No
3. The user should see the 'allo' command prompt on the terminal
4. Type ‘help’ to view the list of troubleshooting commands available.

10. Appendix B – Configuring STM IP Address via Console

The user can choose to view/set the IP address of the STM device allo>show IP

Now you can access the device from the browser using the URL https://<device-ip>

If you are not running the DHCP server in your deployment OR device fails to acquire the IP address, set the IP address from the console CLI using the command line.

Allo > Set IP < IP address><mask><gateway>

Verify the address using the 'show IP' command. Then use this IP address, to access the WebUI/SSH to configure the device for further configuration.

Any Technical assistance required, Kindly contact the support at http://support.allo.com

Thank you for choosing

allo.com

Adarsh Eco Place, #176, Ground Floor, EPIP Industrial Area, Kundalahalli
KR Puram Hobali, Whitefield, Bangalore - 560066.

Email: globalsales@allo.com
indiasales@allo.com

Phone: +91 80 67080808