



Elastix SIP Firewall User Manual

Copy Right

Copyright © 2014 Elastix[®]. All rights reserved.

No part of this publication may be copied, distributed, transmitted, transcribed, stored in a retrieval system, or translated into any human or computer language without the prior written permission of http://www.elastix.org. This document has been prepared for use by professional and properly trained personnel, and the customer assumes full responsibility when using it.

Proprietary Rights

The information in this document is Confidential to Elastix[®] and is legally privileged. The information and this document are intended solely for the addressee. Use of this document by anyone else for any other purpose is unauthorized. If you are not the intended recipient, any disclosure, copying, or distribution of this information is prohibited and unlawful.

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.elastix.org.** 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.

1.1. About this manual

This manual describes the Elastix[®] 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.

1.1. 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.



- **Bold** indicates the name of the menu items, options, dialog boxes, windows and functions.
- The color <u>blue</u> 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. <u>http://www.elastix.org</u>

1.2. 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: sales@elastix.com

Table of Contents

1.1. Document Conventions 2 1.2. Support Information 3 1. Introduction 6 1.1. Overview: 6 1.1. Notification LEDs (On the Front Panel of the SIP Firewall) 8 1.1.2. SIP Firewall Rear View: 9 1.1.3. SIP Firewall Deployment Considerations 9 2. Initial Setup & Configuration 11 2.1. Default Configuration 11 2.4. Accessing the WebUI 11 2.4. Accessing the WebUI 11 2.4. WebUI Setsion timeout 14 2.5. WebUI Settings 14 2.4 Dashboard 15 3. Device Configuration 16 3.1. General Settings 17 3.2. Time Settings 18 3.3. Management Access 18 3.4. Signature Update 20 3.5. Logging 20 4. Configuring the SIP Security Policies 22 4.1. SIP Attacks Detection Policies 22 4.2. SiP Protocol Compliance 24 4.3. Firewall Rules 26 4.4. Firewall Settings 27 4.5. Blacklist Rules (Static) 29	1.1. About this manual	2
1.2. Support Information 3 1. Introduction 6 1.1 . Overview: 6 1.1.1. Notification LEDs (On the Front Panel of the SIP Firewall) 8 1.1.2. SIP Firewall Rear View: 9 1.1.3. SIP Firewall Deployment Considerations 9 2. Initial Setup & Configuration 11 2.1. Default Configuration 11 2.2. Accessing the WebUI 11 2.4. WebUI Session timeout 14 2.5 WebUI Settings 14 2.4 Dashboard 15 3. Device Configuration 16 3.1. General Settings 18 3.3. Management Access 18 3.4. Signature Update 20 3.5. Logging 20 4. Configuring the SIP Security Policies 22 4.1. SIP Attacks Detection Policies 22 4.2. SIP Protocol Compliance 24 4.3. Firewall Rules 26 4.4. Firewall Settings 27 4.5. White list Rules (Static) 29 4.7. Dynamic Blacklist Rules 30 4.8. Geo IP Filter 30 5. Status 32	1.1. Document Conventions	2
1. Introduction 6 1.1 Overview: 6 1.1.1 Notification LEDs (On the Front Panel of the SIP Firewall) 8 1.1.2 SIP Firewall Rear View: 9 1.1.3. SIP Firewall Deployment Considerations 9 1.1.3. SIP Firewall Deployment Considerations 9 2. Initial Setup & Configuration 11 2.1 Default Configuration 11 2.4 Configuration 11 2.5 VebUI Session timeout 14 2.5 WebUI Session timeout 14 2.5 WebUI Session timeout 14 2.4 Dashboard 15 3. Device Configuration 16 3.1 General Settings 17 3.2 Time Settings 18 3.3 Management Access 18 3.4 Signature Update 20 3.5 Logging 20 4. Configuring the SIP Security Policies 22 4.1 Sir Protocol Compliance 24 4.3 Firewall Settings 27	1.2. Support Information	3
1. Introduction 6 1.1 Overview: 6 1.1.1. Notification LEDs (On the Front Panel of the SIP Firewall) 8 1.1.2. SIP Firewall Rear View: 9 1.1.3. SIP Firewall Deployment Considerations 9 2. Initial Setup & Configuration 11 2.1 Default Configuration 11 2.2. Accessing the WebUI 11 2.4 Cacessing the WebUI 11 2.4 WebUI Session timeout 14 2.5 WebUI Settings 14 2.4 Dashboard 15 3. Device Configuration 16 3.1. General Settings 17 3.2. Time Settings 18 3.3. Management Access 18 3.4. Signature Update 20 3.5. Logging 20 4. Configuring the SIP Security Policies 22 4.1. SIP Protocol Compliance 24 4.3. Firewall Rules 26 4.4. Firewall Settings 27 4.5. White list Rules 28 4.6. Blacklist Rules (Static) 29 4.7. Dynamic Blacklist Rules		
1.1 Overview: 6 1.1.1. Notification LEDs (On the Front Panel of the SIP Firewall) 8 1.1.2. SIP Firewall Rear View: 9 1.1.3. SIP Firewall Deployment Considerations 9 1.1.3. SIP Firewall Deployment Considerations 9 2. Initial Setup & Configuration 11 2.1 Default Configuration 11 2.2. Accessing the WebUI 11 2.4 WebUI Session timeout 14 2.5 WebUI Session timeout 14 2.4 Deshboard 15 3.Device Configuration 16 3.1 17 3.1 General Settings 17 3.2 Time Settings 18 3.3. Management Access 18 3.4. Signature Update 20 3.5. Logging 20 4. Configuring the SIP Security Policies 22 4.1. SIP Attacks Detection Policies 22 4.2. SiP Protocol Compliance 24 4.3. Firewall Rules 26 4.4. Firewall Settings 27 4.5. White list Rules (Static) 29 <td< th=""><th>1. Introduction</th><th>6</th></td<>	1. Introduction	6
1.1.1. Notification LEDs (On the Front Panel of the SIP Firewall) 8 1.1.2. SIP Firewall Rear View: 9 1.1.3. SIP Firewall Deployment Considerations 9 2. Initial Setup & Configuration 11 2.1 Default Configuration 11 2.1 Default Configuration 11 2.2. Accessing the WebUI 11 2.4. Accessing the WebUI 11 2.4. Accessing the WebUI 11 2.4. Accessing the WebUI 14 2.5. WebUI Settings 14 2.4. Dashboard 15 3. Device Configuration 16 3.1. General Settings 17 3.2. Time Settings 18 3.3. Management Access 18 3.4. Signature Update 20 3.5. Logging 20 4. Configuring the SIP Security Policies 22 4.1. SIP Protocol Compliance 24 4.3. Firewall Rules 28 4.6. Blacklist Rules (Static)	1.1 . Overview:	6
1.1.2. SIP Firewall Rear View: 9 1.1.3. SIP Firewall Deployment Considerations. 9 2. Initial Setup & Configuration 11 2.1. Default Configuration 11 2.1. Default Configuration 11 2.2. Accessing the WebUI 11 2.4. Accessing the WebUI 11 2.4. WebUI Session timeout 14 2.5. WebUI Settings 14 2.4. Dashboard 15 3. Device Configuration 16 3.1. General Settings 17 3.2. Time Settings 18 3.3. Management Access 18 3.4. Signature Update 20 3.5. Logging 20 4. Configuring the SIP Security Policies 22 4.1. SIP Attacks Detection Policies 22 4.2. SIP Protocol Compliance 24 4.3. Firewall Rules 26 4.4. Firewall Rules 28 4.6. Blacklist Rules (Static) 29 4.7. Dynamic Blacklist Rules 30 4.8. Geo IP Filter 30 5. Status 32	1.1.1. Notification LEDs (On the Front Panel of the SIP Firewall)	8
1.1.3. SIP Firewall Deployment Considerations 9 2. Initial Setup & Configuration 11 2.1. Default Configuration 11 2.2. Accessing the WebUI 11 2.4. WebUI Session timeout 14 2.5. WebUI Settings 14 2.4. Dashboard 15 3. Device Configuration 16 3.1. General Settings 17 3.2. Time Settings 18 3.3. Management Access 18 3.4. Signature Update 20 3.5. Logging 20 4. Configuring the SIP Security Policies 22 4.1. SIP Attacks Detection Policies 22 4.2. SIP Protocol Compliance 24 4.3. Firewall Rules 26 4.4. Firewall Settings 27 4.5. White list Rules 28 4.6. Blacklist Rules (Static) 29 4.7. Dynamic Blacklist Rules 30 4.8. Geo IP Filter 30 5. Status 32	1.1.2. SIP Firewall Rear View:	9
2. Initial Setup & Configuration 11 2.1 .Default Configuration 11 2.2 Accessing the WebUI 11 2.4 WebUI Session timeout 14 2.5 WebUI Settings 14 2.4 Dashboard 15 3. Device Configuration 16 3.1 General Settings 17 3.2 Time Settings 18 3.3. Management Access 18 3.4. Signature Update 20 3.5. Logging 20 4. Configuring the SIP Security Policies 22 4.1. SIP Attacks Detection Policies 22 4.2. SIP Protocol Compliance 24 4.3. Firewall Rules 26 4.4. Firewall Settings 27 4.5. White list Rules 28 4.6 Blacklist Rules (Static) 29 4.7. Dynamic Blacklist Rules 30 4.8 Geo IP Filter 30 4.8 Geo IP Filter 30 5. Status 32	1.1.3. SIP Firewall Deployment Considerations	9
2.1 Default Configuration 11 2.2. Accessing the WebUI 11 2.4. WebUI Session timeout 14 2.5 WebUI Settings 14 2.5 WebUI Settings 14 2.4. Dashboard 15 3. Device Configuration 16 3.1. General Settings 17 3.2. Time Settings 18 3.3. Management Access 18 3.4. Signature Update 20 3.5. Logging 20 4. Configuring the SIP Security Policies 22 4.1. SIP Attacks Detection Policies 22 4.2. SIP Protocol Compliance 24 4.3. Firewall Rules 26 4.4. Firewall Settings 27 4.5. White list Rules 28 4.6. Blacklist Rules (Static) 29 4.7. Dynamic Blacklist Rules 30 4.8. Geo IP Filter 30 5. Status 32 5.1 Security Alerts 32	2. Initial Setup & Configuration	11
2.2. Accessing the WebUI 11 2.4 WebUI Session timeout 14 2.5 WebUI Settings 14 2.4 Dashboard 15 3. Device Configuration 16 3.1. General Settings 17 3.2. Time Settings 18 3.3. Management Access 18 3.4. Signature Update 20 3.5. Logging 20 4. Configuring the SIP Security Policies 22 4.1. SIP Attacks Detection Policies 22 4.1. SIP Protocol Compliance 24 4.3. Firewall Rules 26 4.4. Firewall Settings 27 4.5. White list Rules 28 4.6. Blacklist Rules (Static) 29 4.7. Dynamic Blacklist Rules 30 4.8. Geo IP Filter 30 5. Status 32 5.1 Security Alerts 32	2.1 .Default Configuration	11
2.4 WebUI Session timeout 14 2.5 WebUI Settings 14 2.4 Dashboard 15 3. Device Configuration 16 3.1. General Settings 17 3.2. Time Settings 18 3.3. Management Access 18 3.4. Signature Update 20 3.5. Logging 20 4. Configuring the SIP Security Policies 22 4.1. SIP Attacks Detection Policies 22 4.2. SIP Protocol Compliance 24 4.3. Firewall Rules 26 4.4. Firewall Settings 27 4.5. White list Rules 28 4.6. Blacklist Rules (Static) 29 4.7. Dynamic Blacklist Rules 30 4.8. Geo IP Filter 30 5. Status 32 5.1 Security Alerts 32	2.2. Accessing the WebUI	11
2.5 WebUI Settings 14 2.4 Dashboard 15 3. Device Configuration 16 3.1 General Settings 17 3.2 Time Settings 18 3.3 Management Access 18 3.4 Signature Update 20 3.5 Logging 20 4. Configuring the SIP Security Policies 22 4.1 SIP Protocol Compliance 22 4.2 SIP Protocol Compliance 24 4.3 Firewall Rules 26 4.4 Firewall Settings 27 4.5 White list Rules 28 4.6 Blacklist Rules (Static) 29 4.7 Dynamic Blacklist Rules 30 4.8 Geo IP Filter 30 5 Status 32 5.1 Security Alerts 32	2.4 WebUI Session timeout	14
2.4 Dashboard 15 3. Device Configuration 16 3.1. General Settings 17 3.2. Time Settings 18 3.3. Management Access 18 3.4. Signature Update 20 3.5. Logging 20 4. Configuring the SIP Security Policies 22 4.1. SIP Attacks Detection Policies 22 4.2. SIP Protocol Compliance 24 4.3. Firewall Rules 26 4.4. Firewall Settings 27 4.5. White list Rules 28 4.6. Blacklist Rules (Static) 29 4.7. Dynamic Blacklist Rules 30 4.8. Geo IP Filter 30 5. Status 32 5.1 Security Alerts 32	2.5 WebUI Settings	14
3. Device Configuration 16 3.1. General Settings 17 3.2. Time Settings 18 3.3. Management Access 18 3.4. Signature Update 20 3.5. Logging 20 4. Configuring the SIP Security Policies 22 4.1. SIP Attacks Detection Policies 22 4.2. SIP Protocol Compliance 24 4.3. Firewall Rules 26 4.4. Firewall Settings 27 4.5. White list Rules 28 4.6. Blacklist Rules (Static) 29 4.7. Dynamic Blacklist Rules 30 4.8. Geo IP Filter 30 5. Status 32 5.1 Security Alerts 32	2.4 Dashboard	15
3.1. General Settings 17 3.2. Time Settings 18 3.3. Management Access 18 3.4. Signature Update 20 3.5. Logging 20 4. Configuring the SIP Security Policies 22 4.1. SIP Attacks Detection Policies 22 4.2. SIP Protocol Compliance 24 4.3. Firewall Rules 26 4.4. Firewall Settings 27 4.5. White list Rules 28 4.6. Blacklist Rules (Static) 29 4.7. Dynamic Blacklist Rules 30 4.8. Geo IP Filter 30 5. Status 32 5.1 Security Alerts 32	3. Device Configuration	
3.2. Time Settings 18 3.3. Management Access 18 3.4. Signature Update 20 3.5. Logging 20 4. Configuring the SIP Security Policies 22 4.1. SIP Attacks Detection Policies 22 4.2. SIP Protocol Compliance 24 4.3. Firewall Rules 26 4.4. Firewall Settings 27 4.5. White list Rules 28 4.6. Blacklist Rules (Static) 29 4.7. Dynamic Blacklist Rules 30 4.8. Geo IP Filter 30 5. Status 32 5.1. Security Alerts 32	3.1. General Settings	17
3.3. Management Access183.4. Signature Update203.5. Logging204. Configuring the SIP Security Policies224.1. SIP Attacks Detection Policies224.2. SIP Protocol Compliance244.3. Firewall Rules264.4. Firewall Settings274.5. White list Rules284.6. Blacklist Rules (Static)294.7. Dynamic Blacklist Rules304.8. Geo IP Filter305. Status325.1. Security Alerts32	3.2. Time Settings	18
3.4. Signature Update 20 3.5. Logging 20 4. Configuring the SIP Security Policies 22 4.1. SIP Attacks Detection Policies 22 4.2. SIP Protocol Compliance 24 4.3. Firewall Rules 26 4.4. Firewall Settings 27 4.5. White list Rules 28 4.6. Blacklist Rules (Static) 29 4.7. Dynamic Blacklist Rules 30 4.8. Geo IP Filter 30 5. Status 32 5.1. Security Alerts 32	3.3. Management Access	18
3.5. Logging204. Configuring the SIP Security Policies224.1. SIP Attacks Detection Policies224.2. SIP Protocol Compliance244.3. Firewall Rules264.4. Firewall Settings274.5. White list Rules284.6. Blacklist Rules (Static)294.7. Dynamic Blacklist Rules304.8. Geo IP Filter305. Status325.1 Security Alerts32	3.4. Signature Update	20
4. Configuring the SIP Security Policies 22 4.1. SIP Attacks Detection Policies 22 4.2. SIP Protocol Compliance 24 4.3. Firewall Rules 26 4.4. Firewall Settings 27 4.5. White list Rules 28 4.6. Blacklist Rules (Static) 29 4.7. Dynamic Blacklist Rules 30 4.8. Geo IP Filter 30 5. Status 32 5.1 Security Alerts 32	3.5. Logging	20
4.1. SIP Attacks Detection Policies 22 4.2. SIP Protocol Compliance 24 4.3. Firewall Rules 26 4.4. Firewall Settings 27 4.5. White list Rules 28 4.6. Blacklist Rules (Static) 29 4.7. Dynamic Blacklist Rules 30 4.8. Geo IP Filter 30 5. Status 32	4 Configuring the SIP Security Policies	22
4.2. SIP Protocol Compliance 24 4.3. Firewall Rules 26 4.4. Firewall Settings 27 4.5. White list Rules 28 4.6. Blacklist Rules (Static) 29 4.7. Dynamic Blacklist Rules 30 4.8. Geo IP Filter 30 5. Status 32 5.1 Security Alerts 32	4.1. SIP Attacks Detection Policies	
4.3. Firewall Rules 26 4.4. Firewall Settings 27 4.5. White list Rules 28 4.6. Blacklist Rules (Static) 29 4.7. Dynamic Blacklist Rules 30 4.8. Geo IP Filter 30 5. Status 32 5.1 Security Alerts 32	4.2 SIP Protocol Compliance	24
4.4. Firewall Settings 27 4.5. White list Rules 28 4.6. Blacklist Rules (Static) 29 4.7. Dynamic Blacklist Rules 30 4.8. Geo IP Filter 30 5. Status 32 5.1 Security Alerts 32	4.3. Firewall Rules	
4.5. White list Rules 28 4.6. Blacklist Rules (Static) 29 4.7. Dynamic Blacklist Rules 30 4.8. Geo IP Filter 30 5. Status 32 5.1 Security Alerts 32	4.4. Firewall Settings	
4.6. Blacklist Rules (Static) 29 4.7. Dynamic Blacklist Rules 30 4.8. Geo IP Filter 30 5. Status 32 5.1 Security Alerts 32	4.5. White list Rules	
4.7. Dynamic Blacklist Rules	4.6. Blacklist Rules (Static)	
4.8. Geo IP Filter	4.7. Dynamic Blacklist Rules	
5. Status	4.8. Geo IP Filter	
5.1 Security Alerts 32	5. Status	
	5.1. Security Alerts	

6. T	ools	33
6	.1. Administration	33
6	.2. Diagnostics	34
6	.3. Ping	35
6	.4. Trace route	35
6	.5. Troubleshooting	36
6	.6. Firmware Upgrade	37
6	.7. Logs Archive	38
APF	PENDIX	39
7. A	ppendix A – Using Console Access	39
8. A	ppendix B – Configuring SIP Firewall IP Address via Console	40

1. Introduction

1.1 . Overview:

This User manual describes the steps involved in setting up the Elastix[®] SIP Firewall Appliance. Elastix[®] SIP Firewall 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 SIP Firewall)



The SIP Firewall package includes:

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

1.1.2. SIP Firewall Rear View:



Figure 2: SIP Firewall Rear View

1.1.3. SIP Firewall Deployment Considerations

The SIP Firewall 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 SIP Firewall 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





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 SIP Firewall 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.



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 3: Scenario 3

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 SIP Firewall to the untrusted/public network.
- 4. Connect the LAN port of the SIP Firewall 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 SIP Firewall 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 provides a 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 VIan to access WebUI during initial setup. The management VIan 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 SIP Firewall 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 <u>https://<192.168.100.1></u> Configure the SIP Firewall Device IP Address from the "Device Settings" Page as per your local network range. Verify the IP address set to SIP Firewall from the dashboard page. Once the user assigns the SIP Firewall 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 SIP Firewall WebUI is Mozilla Firefox.

The UI allows the administrator to configure the management VIan IP addresses. In case if the user has changed the management VIan IP address, he needs to assign the corresponding network address to his PC for the management access subsequently. On launching the SIP Firewall 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 SIP Firewall 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 4: 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 5: Timeout message

If somebody is already logged in to SIP Firewall 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.

4. 594		
An administrate Management U 192.168.0.148 attempt.	or is already logged II that administrator's Click "Continue" to p	in from the host 192.168.0.177 . If you continue to log in the STM Configuration session will be dropped. Currently you are trying to login as administrator from preempt that user and continue to log in. Click "Not Now" to cancel your login

Figure 6: Select Login attempt

2.4 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.

2.5 WebUI Settings

To change the WebUI settings, click the settings icon that appears top right corner (below the Apply Changes button). The Web 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.

Session Timeout :	900	
User Name :	admin	0
Old Admin Password :		(<u>i</u>)
New Admin Password :		œ
Confirm Admin Password :		0

Figure 7: WebUI Settings

2.4 Dashboard

lastix Pfanawau							c
17-September-14 12:4	8:35 pm	SIPFW 1.0.00 Tue_Sep_	_9_14:33:57_IST_2014		0		Welcome admin
Dashboard 🔉	Dashboard 🛛						
Device							
Security Settings	System Status		Sig Update Ver	rsion		DPI Status	
Security Alerts	Up-Time		Elastix SIP Fire	ewall Signa	atures 1.0.	00 😑 Enabled	🖯 Running
Tools	2:46 Memory Usage (Total Mem	nory:64MB)	Security Alert S	Summarv			
	79%						
	Flash Usage (Flash Size:16	SMB)	Top 10 Signatu Top Sre	Top D	<u>o Categori</u>	<u>es</u>	
	CPU Usage		Last 10 Alerts			_	
	100%	b	Time	ю	Category	Message	Src IP
	Network Status		09/17-12:46:09	70090001	7009	"Sig: SIP Bruteforce Pas	192.168.10.121
	Network Info Device IP : 192.168.10.237 LAN MAC : 00:17.F7.00:3C:A0 WAN MAC : 00:17.F7.00:3C:A1 Gateway : 192.168.10.264		09/17-12:46:09 09/17-12:46:09 09/17-12:46:09 09/17-12:46:09 09/17-12:46:09 09/17-12:46:09 09/17-12:46:09	70090001 27 70090001 70090001 70090001 70090001 20	7009 7009 140 7009 7009 7009 140	"Sig: SIP Bruteforce Pas "Sig: SIP Bruteforce Pas "(spp_sip) Maximum dial "Sig: SIP Bruteforce Pas "Sig: SIP Bruteforce Pas "Sig: SIP Bruteforce Pas "(spp_sip) Invite replay "Sig: CIP Bruteforce Pas	192.168.10.121 192.168.10.121 0192.168.10.226 192.168.10.121 192.168.10.121 192.168.10.121 192.168.10.226

Figure 8: Dashboard

On logging into the SIP Firewall WebUI, the dashboard will be shown.

The user can visit the dashboard page from the any configuration page in the SIP Firewall WebUI, by clicking the SIP Firewall 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 SIP Firewall 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 SIP Firewall 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.

3. Device Configuration

Configuration pages of the SIP Firewall 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.

Device Access Filter Configuration	I
1. Device Access rule edited	
2. Device Access rule edited	
Global Firewall Settings	
1. Global Firewall Settings updated	
2. Global Firewall Settings updated	
Logging	
1. Logging settings updated	

Figure 9: 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

The General settings page will allow configuring the host/network settings of the SIP Firewall 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 SIP Firewall appliances or not.

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

and the second	Ceneral Setting	5 😈		
Device >				
 General Settings 	Device Settings			
 Time Settings 	Host Name	sip_secure	0	
Management	IP Configuration	DHCP 💌 🖲		
ACCESS	IP Addr/Mask			G
 Signature Update 	Gateway		0	
- Logging	Dns Server		®	
 Security Settings 	Enable SSH			
 Security Alerts 	SSH Port	22 💿		
Tools	Allow ICMP			
	Mgmt Vlan Addr/Mask	192.168.100.1	255.255.255.0	G

Figure 10: General Settings

3.2. 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.

 Dashboard 	Date / Time Settings 🥝
• Device 🔷 🗲 🗲	
General Settings	Date / Time Settings ()
 Time Settings 	Configuration Type NTP 💽 🕄
Management Access	Date/Time 10: 15 01 / 09 / 2014 0
Signature Update	
 Logging 	Add Add
 Security Settings 	3.in.pool.ntp.org Delete
 Security Alerts 	
Tools	
	Apply Cancel

Figure 11: Date/Time Settings

3.3. Management Access

The access the SIP Firewall 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.

Name	Default
IP Type	IP_HOST 🕑 💿
Address	192.168.0.24 💿
Enable	
Comments	Access from Management <u>ylan</u> network
	0

Figure 12: Create Management Access Rule

board >	Ma	inagement A	ccess 🔞						
ce									
urity Settings	8		1				Search:		
irity Alerts		Name +	IP Type 🛊	Address \$	Comments ¢	Enabled \$	Options		
		DefaultAllAccess	ANY		Default rule that al		V	1	X
		MgmtVlanAccess	IP_NETWORK	192.168.100.0/24	Access from Mgmt Via		V	1	X

Figure 13: Management access

Add New Delete Selected

The administrator needs to configure the IP Address or the IP Network or the Range of IP Addresses that will have access to the device and 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.

3.4. 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.

 Dashboard 	Signature Update 🥝
Device >	~ .
🗏 General Settings	Signature Update Settings ()
⊣ Time Settings	Enable Update 🔽
⊣ Management Access	Time Schedule 2 00 AM 💙 Daily 💟 Sunday 💙 1 😒
📮 Signature Update	
🗏 Logging	Apply Cancel Update Signatures now
 Security Settings 	
Security Alerts	
Tools	

Figure 14: Signature Update

When the user buys the SIP Firewall 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 Elastix's Sales representative about getting the details of purchasing the SIP Firewall signature subscription key.

3.5. Logging

The administrator can configure the SIP Firewall 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 the address of the SYSLOG server where we want to forward the alerts.

 Dashboard 	Logging 😰
Device >	
🗉 General Settings	Logging
🗉 Time Settings	Remote Logging: 🔽
⊣ Management Access	Syslog server 192.168.0.109 0
🗉 Signature Update	
🔺 Logging	Save Cancel
 Security Settings 	
Security Alerts	
 Tools 	

Figure 15: Logging

4. Configuring the SIP Security Policies

4.1. SIP Attacks Detection Policies

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 SIP Firewall 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.

Dashboard	SIP Attacks Detection Ø					
Device	-					
 Security Settings 	Category	Action	Blocking Duration (seconds)	Enabled	Options	
SIP Attacks	Reconnaissance Attacks	Log	none		1	
Detection	Sip Devices Scanning	Block	120		1	
SIP Protocol	SIP Extensions Discovery	Block	120	V	1	
Compliance	Multiple Authentication Failures/Bruteforce password cracking Attempt	Block	1800		1	
 Firewall Rules 	Ghost calls Attempt	Block	1800			
 Firewall Settings 	SIP Protocol Compliance	Log	none	V	1	
Whitelist IP	Sip Anomaly Attacks	Block	1800		1	
Addresses	Sip Dos Attacks	Block	1800		1	
Blacklist IP	Sip DDos Attacks	Block	1800	•	1	
Auuresses	Sip Cross site scripting Attacks	Block	1800		1	
 Dynamic Blacklist IP Addresses 						
• Geo IP Filters	_					
 Security Alerts 						
 Tools 						

Figure 16: SIP Attacks Detection

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

Category	Description	User Configurable options
SIP Reconnaissance Attacks	The intruder is trying to detect what version of Asterisk you are running. With that info, he will start exploiting the numerous vulnerabilities of that version. The SIP Firewall will not respond to his query.	N/A
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 SIP Firewall will not respond to his query.	N/A
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 SIP Firewall will not respond to that query.	Invalid SIP User Registration Attempts/Duration
Multiple Authentication Failures/Brute force password Attempt	The intruder will try to log in with different user names and passwords multiple times. Once he succeeds, he will have control of that extension. The SIP Firewall can block, log or blacklist the IP for a period of time if it exceeds the authorized number of trials/second.	Failed Authentication 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 SIP Firewall 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 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 Anomaly attacks	The intruder will send abnormal SIP packets to the PBX. His goal is to crash the PBX resulting in disrupted	N/A

	communication. The SIP Firewall can block, log or blacklist the IP for a period of time if it exceeds the authorized number of trials/second.	
SIP Buffer ove attacks	Buffer overflow attempts resulted from improper validation of user inputs.	N/A
SIP Cross site scripti	SIP is vulnerable to cross-site scripting, caused by improper validation of user-supplied input in a SIP request. A remote attacker could exploit this vulnerability to inject malicious script into a Web page which would be executed in a victim's Web browser, when the victim accessed a web page containing information taken from the SIP request.	N/A
3rd Party vendor vulnerabilities	Attacks targeted towards PBX/SIP Gateway appliances exploiting their vulnerabilities.	N/A

4.2. SIP Protocol Compliance

The SIP Deep packet inspection engine running the SIP Firewall 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.

 Dashboard 	SIP Protoco	ol Compliance 👩	A Please make sure	e to refer to the user manual befo	re making changes in this	configuration pag
Device	G	12				
 Security Settings 	SIP Protocol Compl	liance Settings	0	SIP/MEDIA Ports Configuratio	n	
 SIP Attacks Detection 	Max Sessions	4096 SIP Methods/Headers	invite	SIP Transport	any 🔽 🕄	
 SIP Protocol Compliance 	Max Dialogs per session	2048	ack bye register	Media Transport	udp 🗸 🛈	
 Firewall Rules 	Max URI length	256	options refer	Media Ports	1024-65535 💿	
 Firewall Settings 	Max Call ID length	80	update			
→ Whitelist IP Addresses	Max Request name Iength	20 ©	notify			
Blacklist IP Addresses	Max From length	256 ©	do 💌			
 Dynamic Blacklist IP Addresses 	Max To length Max Via length	1024 ©				
- Geo IP Filters	Max Contact length	1024				
 Security Alerts 						
Tools						

Figure 17: SIP Protocol Compliance

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. The 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.

4.3. 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.

Name	Webaccess	
Enabled	I	
Src Type	ANY 💽 💿	
Src Address	(i)	
Dst Type	ANY 💽 🖲	
Dst Address	()	
Protocol	any 💌	
Port	24	
Action	Block 😒 💿	

Figure 18: Create Firewall Rule

4.4. 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.

 Dashboard 	Firewall Settings 🔞	
 Device 		
 Security Settings 	Global Firewall Settings	
 SIP Attacks Detection 	TCP Syn Flood Rate	1024
COD Date and	TCP Syn Flood Burst	128
Compliance	TCP Flood Rate	4096
Firewall Rules	TCP Flood Burst	96
• Firewall	UDP Flood Rate	8192
Settings	UDP Flood Burst	198
 Whitelist IP Addresses 	ICMP Flood Rate	128
Addresses	ICMP Flood Burst	64
Addresses		
⇒ Dynamic Blacklist IP Addresses	Save Cancel	
→ Geo IP Filters		
Security Alerts		
Tools		

Figure 19: Firewall Settings

4.5. White list Rules

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 SIP Firewall.

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.

reate whitelist Ri	Kaliaat	
Name		
Ір Туре	IP_HOST M	
Address	192.168.10.79 🙃	
Enable		
Comments	Kali blocked	
		0

Figure 20: Create White list Rule

 Dashboard 	Whitelist IP	Addresses 🔞	1			
Device						
Security Settings	🗹 Whitelist IP Rules	Precedes over Blacklist IP	Rules			
SIP Attacks Detection	Name -	IP Type \$	Address 🌢	Comments +	Search:	Options
 SIP Protocol Compliance 	🗌 Kalitest	IP_HOST	192.168.10.79	Kali blocked		× ×
 Firewall Rules 						
 Firewall Settings 						
⇒ Whitelist IP Addresses						
→ Blacklist IP Addresses						
 Dynamic Blacklist IP Addresses 	Add New De	Hete Selected				
- Geo IP Filters						
Security Alerts						
Tools						

Figure 21: White list IP Addresses

4.6. Blacklist Rules (Static)

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 SIP firewall.

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.

Create Blacklist Ru	le	×
Name	Kalitest	
IP Type	IP_HOST 💽 🗉	
Address	192.168.10.79 ①	
Enable		
Comments	Kali blocked	
		(Î)
	SA	CANCEL
		GRANDEL

Figure 22: Create Blacklist Rule

 Dashboard 	Blacklist IP	Addresses 👩				
Device						
 Security Settings 					Search:	
 SIP Attacks Detection 	Name +	IP Type +	Address +	Comments ÷	Enabled ¢	Options
SIP Protocol Compliance	Transfor		102.100.101.0			2.0
 Firewall Rules 						
 Firewall Settings 						
 Whitelist IP Addresses 						
 Blacklist IP Addresses 	Add New De	lete Selected				
 Dynamic Blacklist IP Addresses 						
, Geo IP Filters						
Security Alerts						
Tools						

Figure 23: Blacklist IP Addresses

4.7. Dynamic Blacklist Rules

The dynamic blacklist rules are the blocking rules added by the SIP Firewall 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 rules 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 rules page.

Dashboard	Dynamic Blacklist IP Addres	ses 🛿	
Device			
 Security Settings 		Search:	
 SIP Attacks Detection 	Address - 192.168.10.79	Options	×
 SIP Protocol Compliance 			
→ Firewall Rules			
 Firewall Settings 			
 Whitelist IP Addresses 			
 Blacklist IP Addresses 	Delete Selected		
 Dynamic Blacklist IP Addresses 			
- Geo IP Filters			
Security Alerts			
• Tools			

Figure 24: Dynamic Blacklist IP Addresses

4.8. Geo IP Filter

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

 Dashboard 	Geo IP Filters 🛿		
Device			
 Security Settings 	Allow All Countries Block All Countries Update Geo IP		
SIP Attacks Detection	Country Name	Search: Allowed	Options
SIP Protocol Compliance	RUSSIAN FEDERATION		A
Firewall Rules	SYRIAN ARAB REPUBLIC	V	
Firewall	SUDAN	\checkmark	
Settings	NIGERIA		
- Whitelist IP	KOREA, REPUBLIC OF		
Addresses	CHINA	V	1
 Blacklist IP Addresses 	UKRAINE		
 Dynamic Blacklist IP Addresses 	AL GERIA		1
- Geo IP Filters			

Figure 25: Geo IP Filters

Security Alerts
 Tools

5. Status

5.1. Security Alerts

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

The administrator can choose to set log viewer page refresh interval in this page.

The administrator can choose 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.

Dashboard	Security	Alerts	2									
Device												
 Security Settings 	Log Viewer Se	ettings							0			
Security Alerts 🗲	300	Upda	ate Refresh Inter	val Refresh	Download L	ogs E-ma	il Server Sett	ngs	1			
Security Alerts									Sea	arch:		
Tools	Time +	ID ¢	Category \$	Category Name 🕈	Message ¢	Src IP +	Src Port \$	Dst IP 🕈	Dst Port 🕈	Protocol ¢	Action \$	l
	09/01-15:54:27	70020001	7002	Sip Devices Scanning	"STM Sigs: SIP Devices Identification Attempt"	192.168.10.79	5060	192.168.10.0	5060	UDP	Blacklist	
	09/01-12:26:26	70030046	7003	Sip Anomaly Attacks	"STM Sigs: To header format string attempt"	192.168.10.80	5060	224.0.1.75	5060	UDP	Blacklist	
	09/01-12:26:26	70030058	7003	Sip Anomaly Attacks	"STM Sigs: From header format string attempt"	192.168.10.80	5060	224.0.1.75	5060	UDP	Blacklist	1

Figure 26: 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 a USB storage, they can connect the USB storage to the USB data port of SIP Firewall appliance. The rotated logs will be automatically archived in CSV format into USB storage by the SIP Firewall appliance.

6. Tools

6.1. 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 Elastix SIP Firewall appliances support taking the configuration backup and restore the configuration later.

 Dashboard 	Administration 🛛
Device	
Security Settings	(1) Factory Reset
Security Alerts	(A) Restart STM Services
• Tools >	Hestart STM Services
🚽 Administration	C Reboot
- Diagnostics	(h) Shuddaun
⇒ Ping	Shudowi
- Traceroute	Config Back-up
- Troubleshooting	Select configuration file : Browse No file selected. (Requires Reboot)
🗉 Firmware Upgrade	
🗏 Logs Archive	

Figure 27: 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

The diagnostics page will allow the administrator to gather the troubleshooting logs which will help Elastix's Support team in debugging any issues faced with SIP Firewall 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 the Elastix's Support team (**Note:** You can send an email to <u>support@elastix.com</u>)

• Dashboard	Diagnostics 🥝	
Device	annach Chairte	
Security Settings	Run Diagnostics Get Report	
Security Alerts		<u>^</u>
• Tools >	Hostname sip secure	
- Administration	-	
🗕 Diagnostics	Time Mon Sep 1 06:54:03 UTC 2014	~
⇒ Ping		
- Traceroute		
+ Troubleshooting		
– Firmware Upgrade		
 Logs Archive 		

Figure 28: Diagnostics

Click the above link to download the diagnostics.



6.3. Ping

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

The administrator needs to enter the IP address that needs to be pinged from the SIP Firewall, select the 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.

Dashboard	Ping 📀
Device	
Security Settings	Host 192.168.0.127 Count 1 V 0
• Security Alerts	Ping Reset
Tools >	PING 192.168.0.127 (192.168.0.127): 56 data bytes
- Administration	64 bytes from 192.168.0.127: icmp_seq=0 ttl=64 time=1.1 ms
- Diagnostics	192.168.0.127 ping statistics l mackets transmitted, l mackets received, 0% macket loss
🤿 Ping	round-trip min/avg/max = 1.1/1.1/1.1 ms
- Traceroute	
- Troubleshooting	
⇒ Firmware Upgrade	
→ Logs Archive	

Figure 30: Ping Result

6.4. Trace route

The administrator can troubleshoot the network connectivity issues running a trace route from the SIP Firewall device.

The administrator needs to enter the IP address to which the route needs to be traced from the SIP Firewall, select the 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.

Dashboard	Traceroute 🔞	
Device		
Security Settings	Host 192.168.0.127	6
Security Alerts	Hop Count 2	
Tools >		
- Administration	Traceroute Reset	
 Diagnostics 	1 * * * 2 * * *	
⇒ Ping		
🦂 Traceroute		
 Troubleshooting 		
🦂 Firmware Upgrade	4	
Logs Archive		

Figure 31: Trace route

6.5. Troubleshooting

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

 Dashboard 	Troubleshooting 📀
Device	
Security Settings	Enable DPI
Security Alerts	
- Tools 🔷 🔉	
- Administration	
→ Diagnostics	
- Ping	
- Traceroute	
🚽 Troubleshooting	
🗉 Firmware Upgrade	
- Logs Archive	

Figure 32: Troubleshooting

6.6. Firmware Upgrade

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

To install the firmware,

- Download the SIP Firewall firmware update package from Elastix website and keep it your local system.
- From the browser on your local system, login to SIP Firewall WebUI and launch the SIP Firewall firmware upgrade page.
- Click the 'Browse' in the firmware page and select the SIP Firewall 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.

 Dashboard 	Upgrade Firmware 🔞
Device	
Security Settings	Current Firmware Version: SIPFW 1.0.00
Security Alerts	(Choose the filepath of the new firmware)
• Tools >	Filename: Browse STM-Quick Installation Guide-Version 2.docx (Need Reboot)
🚽 Administration	
- Diagnostics	Upgrade
🖃 Ping	
🗏 Traceroute	
- Troubleshooting	
🔺 Firmware Upgrade	
→ Logs Archive	

Figure 33: Upgrade Firmware

6.7. Logs Archive

If the USB storage device attached to SIP Firewall, 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.

Dashboard	Logs Archive 🛛
Device	
Security Settings	Logs Archive Summary: No USB media found for logs archive
• Security Alerts	
Tools >	
+ Administration	
- Diagnostics	
⇒ Ping	
- Traceroute	
- Troubleshooting	
– Firmware Upgrade	
🗕 Logs Archive	

Figure 34: 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 SIP Firewall appliances support taking the configuration backup and restore the configuration later.

APPENDIX

7. Appendix A – Using Console Access

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

8. Appendix B – Configuring SIP Firewall IP Address via Console

The user can choose to view/set the IP address of the SIP Firewall device Elastix > 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.

Elastix > 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 support@elastix.com