



Elastic SIP Firewall

Quick Installation Guide

Elastix SIP Firewall

Quick Installation Guide

Table of Contents

Overview	2
Deployment Considerations	3
Initial Setup & Configuration.....	5
Accessing the WebUI.....	6

Overview

Congratulations on your purchase of the Elastix SIP Firewall appliance to protect your SIP based PBX, VOIP Gateway deployments. This Quick Start Guide describes the steps involved in setting up the Elastix SIP Firewall Appliance.

It comes with 1 fast Ethernet LAN interface and 1 fast Ethernet WAN interface. An additional USB port has been provided for adding the secondary USB storage that will be used by the appliance for archiving the security alert lock. The factory-reset button is located next to the USB Power socket.

Notification LEDs (On the Front Panel of the SIP Firewall)

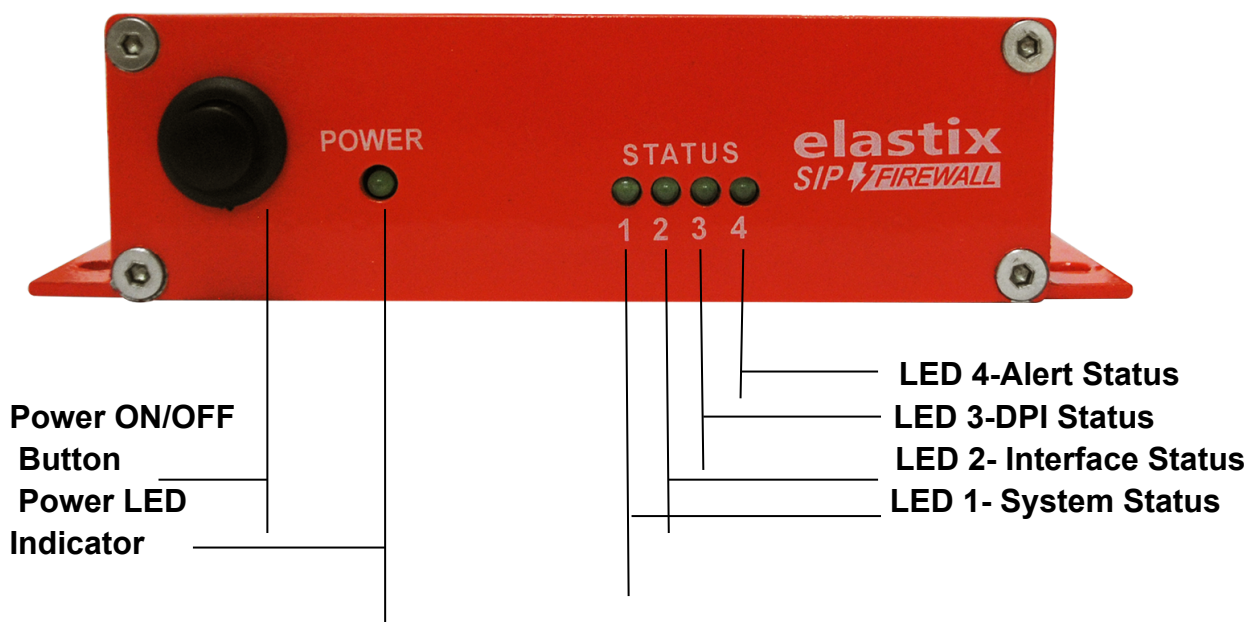


Figure 1: Front Panel LED Notifications

SIP Firewall Rear View:

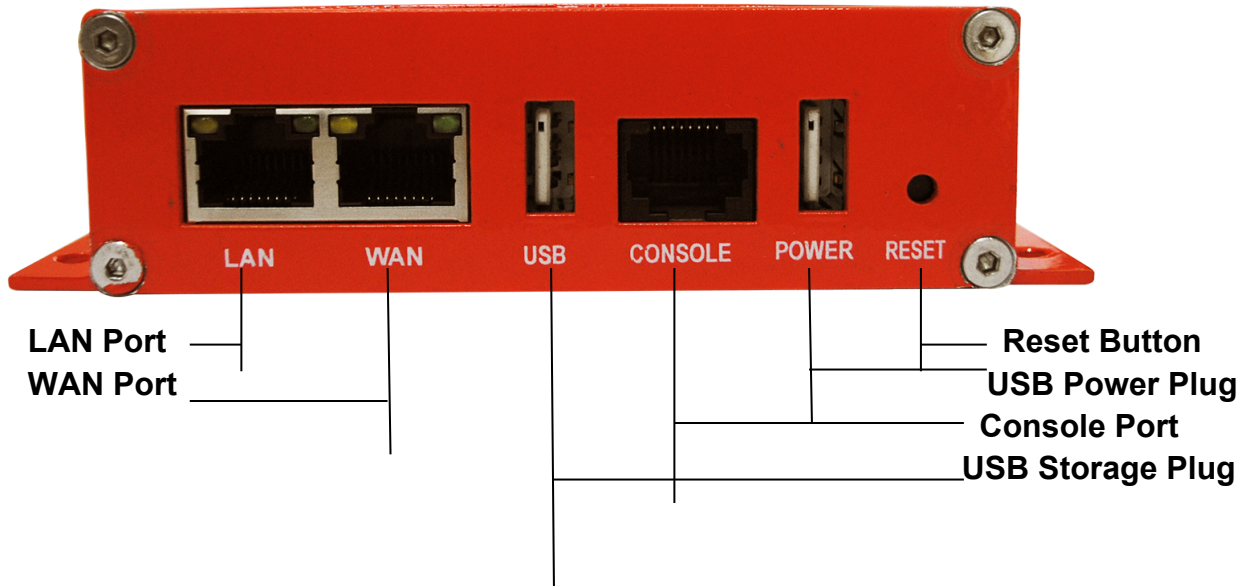


Figure 2: SIP Firewall Rear View

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.

Scenario 1



Figure 3: Scenario 1

Scenario 2

In the case of PBX 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.

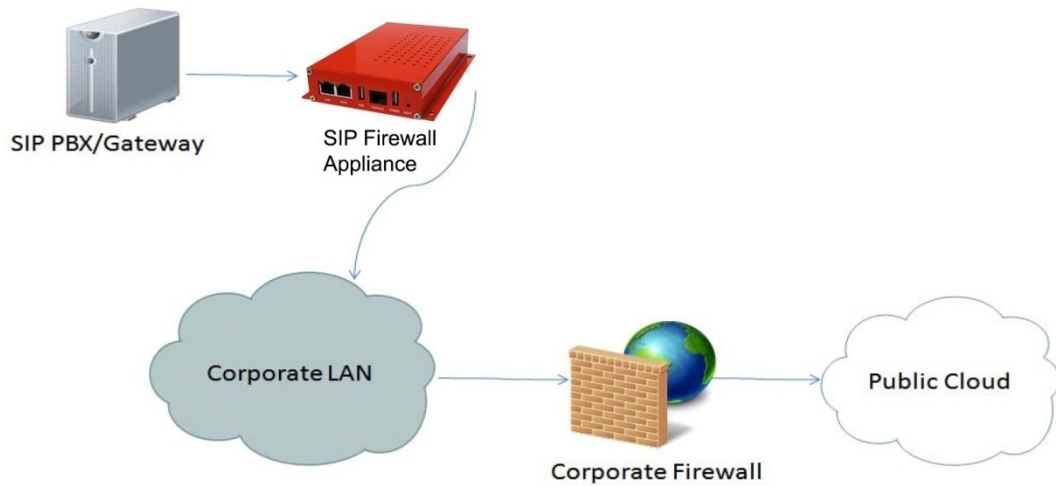


Figure 4: Scenario 2

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.

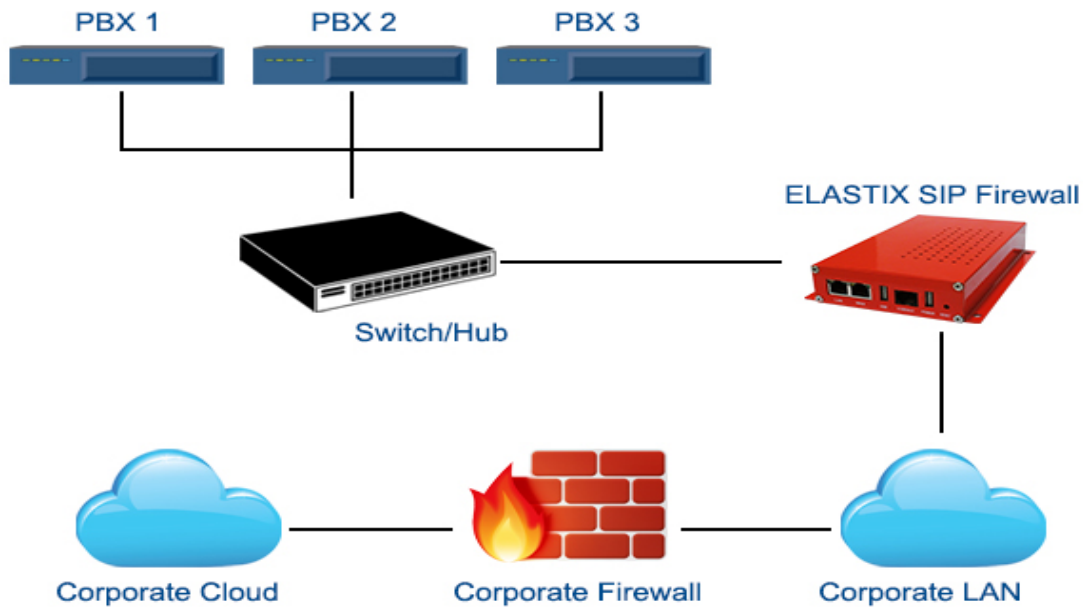


Figure 5: Scenario 3

The SIP Firewall package includes:

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

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 LAN port of the SIP Firewall to the PBX/VOIP Gateway.
4. Connect the WAN port of the SIP Firewall to the untrusted/public network.
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 the WAN/Public Interface). In such cases LAN port of the SIP Firewall should be connected to the Data Interface (WAN/Public Interface).

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, they can tune the configuration via the Device WebUI.

The device also provides the command line interface accessible via SSH, which will allow configuring the basic settings and viewing device status.

Management Access	Login Credentials
Web GUI	admin/admin
SSH CLI	admin/stmadmin
Management Vlan IP	192.168.100.1/255.255.255.
Default Device IP	10.0.0.1/255.255.255.0

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 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 <https://<192.168.100.1>> 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 Vlan IP addresses. In case if the user has changed the management Vlan IP address, they need to assign the corresponding network address to his PC for the management access subsequently.



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.

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

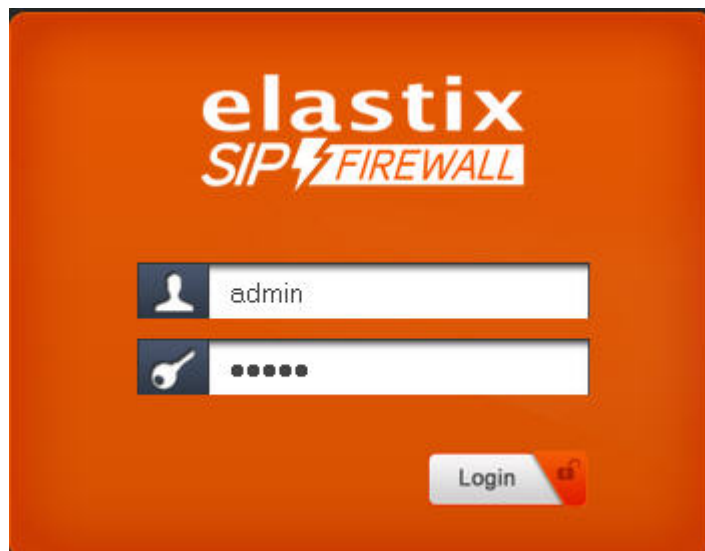


Figure 6: Login Page

THE FULL VERSION MANUAL WILL PROVIDE YOU DETAILED INSTRUCTIONS ABOUT THE FULL FEATURE SET OF THE ELASTIX SIP FIREWALL



Any Technical assistance required, Kindly contact the support at:
support@elastix.com

THANK YOU!