CEM Solutions

STM (SIP Threat Manager)

Quick Installation Guide

Quick Installation Guide

SIP THREAT MANAGER

(aSTM)

Revision 2.0

Table of Contents

Overview

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

Package Content

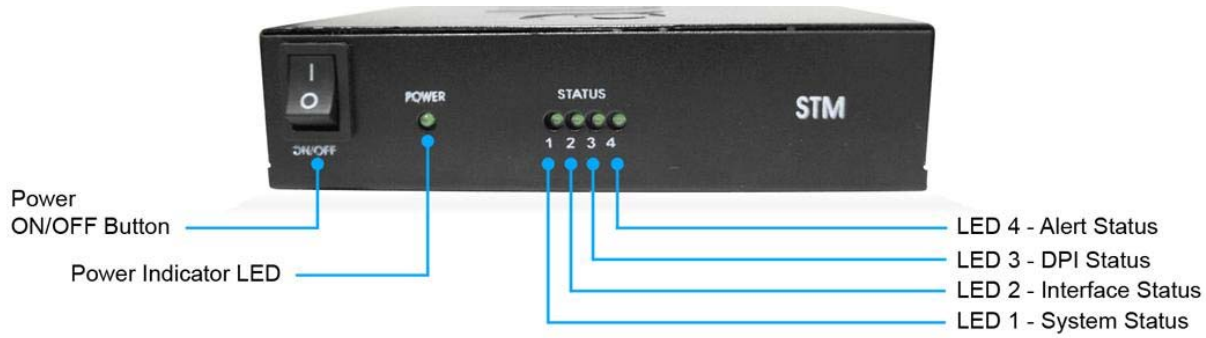
The STM Appliance package includes the following,

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

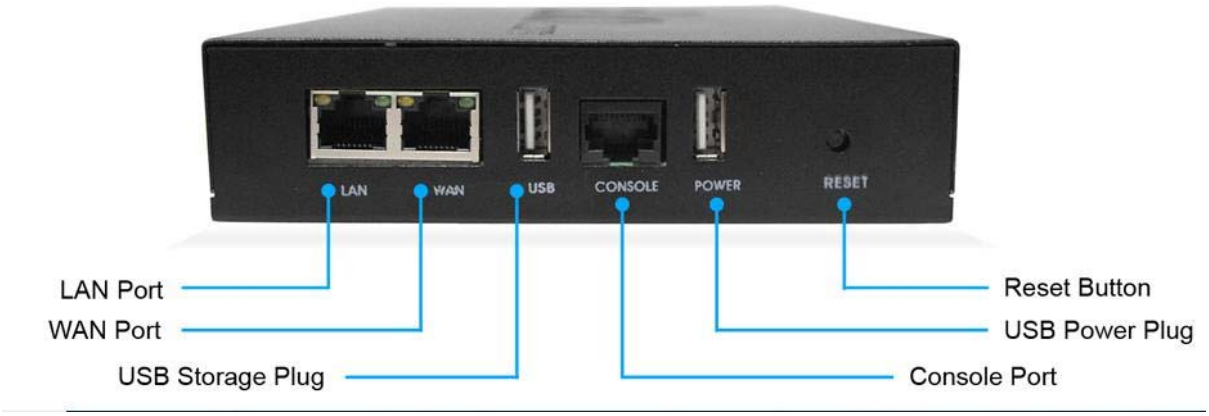
Appliance Hardware

The appliance hardware 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 alerts. The factory reset button is located next to the USB Power socket.

Notification LEDs (On the Front Panel of the STM)



STM Rear View:



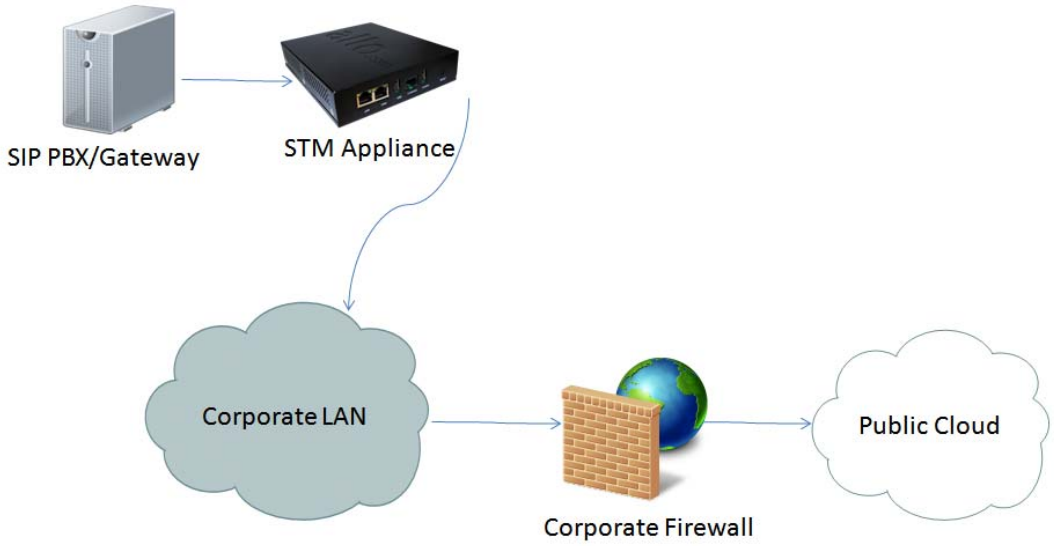
Deployment Considerations

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.

Scenario 1

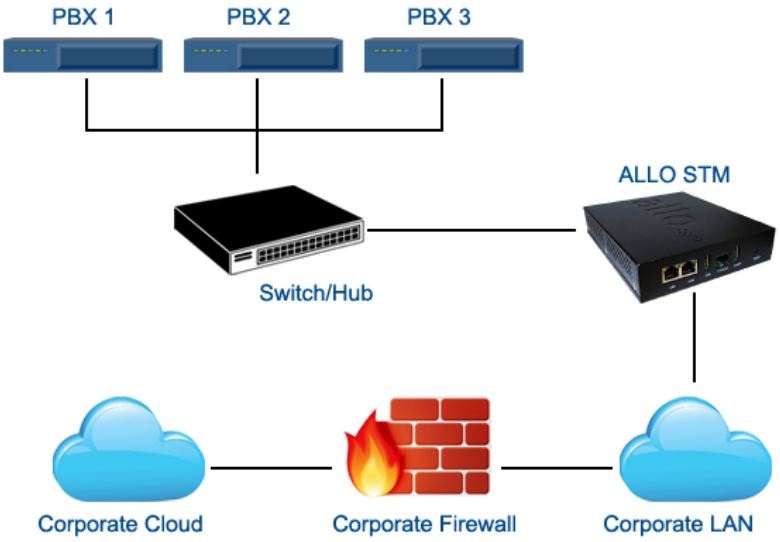
Scenario 2

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.



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.



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 appliance to the power socket using the USB power cable.
4. Connect the LAN port of the STM to the PBX/VOIP Gateway.
5. Connect the WAN port of the STM to the untrusted/public network.
6. The device will take about a minute to come up & will be fully functional with the default configuration.

Note:

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 (aka WAN/Public Interface).

The device operates as transparent bridging firewall with Deep Packet Inspection enabled on the SIP traffic. By default, the appliance has been made to acquire the IP Address via DHCP.

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, He/She 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	192.168.100.1/255.255.255.0

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 with 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 Netmask as 255.255.255.0.

Now you can access the device from the browser using the URL as given below

https://<192.168.100.1>

Note:

The WebUI has been made accessible only via HTTPS. The Device WebUI Server has been made to use Self signed PKI Certificate, Thus the browser will prompt to accept the self signed certificate generated by the device on accessing the WebUI.

The recommended browser for accessing STM WebUI is Mozilla Firefox.

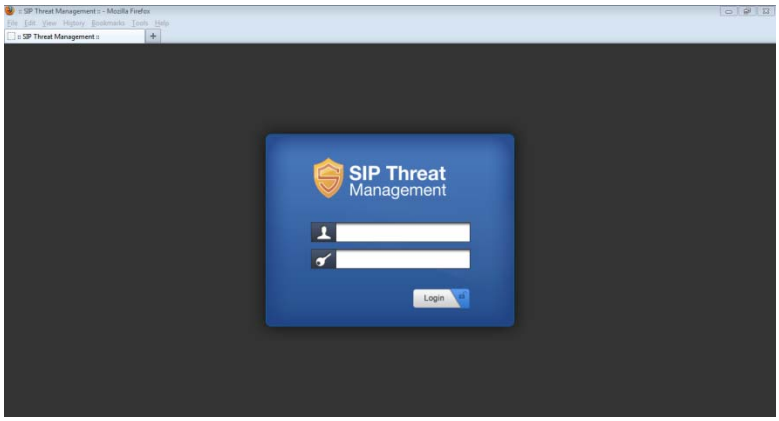
Configure the STM Device IP Address from the "Device Settings" Page as per your local network range. Verify the IP address set to STM from the dashboard page. Once the user assigns the STM Device IP Address successfully, he can access the device using that IP address further.

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

Note:

The UI allows the administrator to configure the management vlan ip address. 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 enter the administrator credentials to login.



Note:

The WebUI has been made accessible only via HTTPS.

The recommended browser for accessing STM WebUI is Mozilla Firefox.

THE FULL VERSION MANUAL WILL PROVIDE YOU DETAILED INSTRUCTIONS ABOUT THE FULL FEATURE SET OF THE SIP THREAT MANAGER

THANK YOU!