STM (SIP Threat Manager)

Overview

As a customer, you are responsible for securing your phone system. On average, an attack costs several thousands of US dollars. Our STM is installed in front of any SIP based PBX or gateway offering several layers of security against numerous types of attacks. Block specific IPs or countries, protect your PBX against hackers trying user names and passwords, someone is trying to flood your PBX with a DDos attacks? No problem!
Using the SNORT based Real Time Deep packet inspection engine, our STM analyzes each SIP packet going to your phone system, identifies the malicious and abnormal ones blocking the originating IP. See more features below: (Please read the feature list, see the video and get access to the STM user interface for the complete user experience)

The appliance has been made to seamlessly integrate with the existing network infrastructure and reduces the complexity of deployment.

Plug&Play

Key Features

- Analyze SIP packets using the Snort based Real time 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 / Whitelist / 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 device to your existing network
- Web/SSL based Device Management Access which will allow to manage 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 remote syslog server.
- Provides the SIP throughput upto ~10Mbps.

Product Models

aSTM1 - Up to 50 Concurrent calls
aSTM2 - Up to 250 Concurrent calls

Warranty Info

1 Year hardware warranty

allo.com
ADRASH ECO PLACE, #176, Ground Floor, EPIP INDUSTRIAL Area, Whitefield, Bangalore-66, India.
globalsales@allo.com / indiasales@allo.com ☎ +91 80 67080808