ribbon™

Ribbon Analytics - TDoSProtect

Stopping Floods of Malicious Calls

How do you know if you are protecting your real-time communication networks from unwanted calls coming in that appear to be valid but in fact they are malicious attempts to tie up communication applications such as IVRs or PBX trunks with long call duration times.

Telephone Denial-of-Service (TDoS) attacks are increasing every day. They are often part of an extortion scheme where a bad actor demands payment, then launches a continuous stream of phantom calls that block normal calls in your business until payment is received. Usually, the attacks start and stop randomly until the ransom is paid. Frequent targets include hospitals, government offices and public-safety answering point offices.

Ribbon Analytics TDoSProtect application uses advanced algorithms to mitigate these attacks. Advanced policies are applied at the edge of the network to siphon out these unwanted, disruptive calls from your communications networks and applications.

TDosProtect

TDosProtect is designed to protect against malicious activity such unauthorized users flooding the system with bogus access requests preventing legitimate users from accessing the system. Or, bad actors keeping malicious calls active for long duration, which enables the bad actors to prevent voice network resources from being used by legitimate callers.

TDoSProtect models baselines network behavior to establish a characteristic "normal" activity. Once a baseline is created the analytics application monitors your communication network activity for anomalies and deviations from the established baseline. These anomalies are identified, graded as to the likelihood that these incidents are fraudulent, and reported to the you for mitigation.

How it works

TDoSProtect tracks the number of SIP invites based on "Calling Number" patterns on a per-interval basis (for example, by 5 minute intervals). When the number of calling number invites exceeds the customer-defined threshold, then that calling number is tagged as "problematic" and escalated for investigation and/or mitigation.

It is possible to configure TDoSProtect to automatically initiate mitigation against that calling number(s) creating service disruptions. Blocking policies are promulgated throughout the entire communications network to block any additional calls from that calling number or calling number prefix.

Thus, mitigating any loss in access by legitimate callers. Moreover, administrators can create "whitelist" policies for specific Calling Numbers to always allow them to automatically bypass the TDoSProtect threat detection algorithms. Figure 2 below shows TDoSProtect functionality.

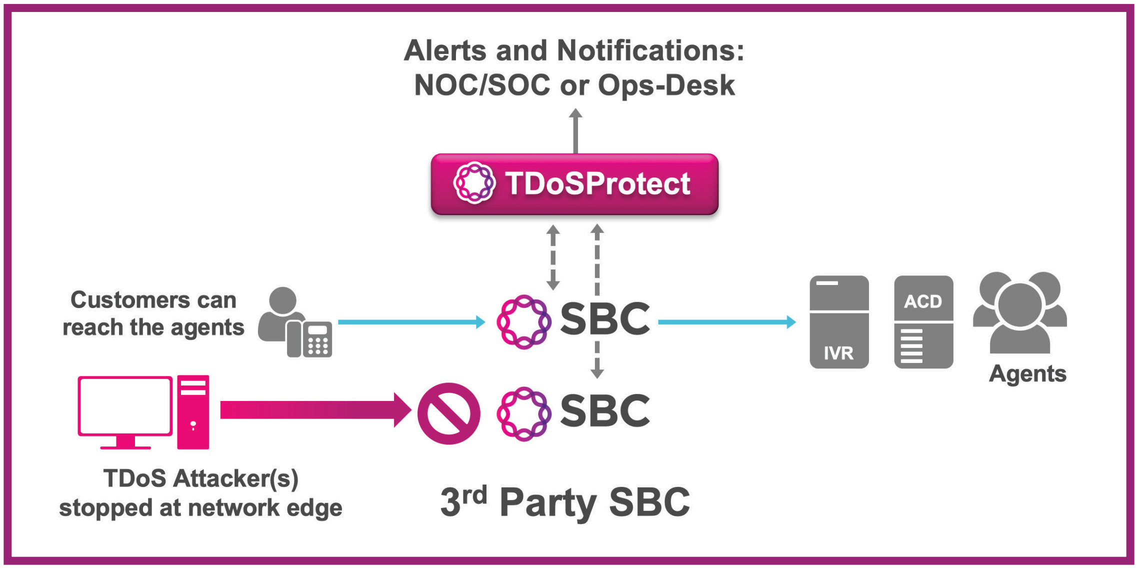
Alerts and Notifications:
NOC/SOC or Ops-Desk
TDoSProtect
Customers can reach the agents
SBC
SBC
IVR
ACD
Agents
TDoS Attacker(s) stopped at network edge
3rd Party SBC

Figure 2. TDoSProtect functionality

TDoSProtect Features and Benefits:

- Advanced algorithms to siphon out unwanted, disruptive calls from your communications networks and applications
- Detect calling anomalies based on metrics such as CAC by Calling number
- Automatically alerts on and blocks rogue calling patterns throughout the entire network

Ribbon Protect Platform

TDoSProtect leverages Ribbon Protect, a big data analytics platform, to respond to real-time communications security and network quality incidents faster, more intelligently, and more efficiently.

The heart of the Protect platform is its UC anomaly detection and policy mitigation capability. The anomaly detection module collects and analyzes data across the entire communications network that is then made available to Ribbon Analytics applications. With customer-defined policy management functionality, detected anomalies generate alerts (e.g. SMS, email) and can be mitigated with actions to the appropriate network elements in real-time.

Rapid revelation, rapid review, rapid resolution…so your mission-critical communications remain secure and available.

www.rbbn.com

www.rbbn.com