Hardened Security for an Untrusted Boundary

Ribbon SBCs – Protecting Enterprise Unified Communications

Now more than ever, enterprises are migrating from TDM to IP-based communications technology in order to best fit the way their customers and employees communicate in today's digital world. SIP communications is a simple, cost-effective method of accelerating the deployment of unified communications (UC) and gaining new efficiencies. SIP should be thought of as a core building block to secure UC—as important as the underlying IP network. Ribbon's session border controller (SBC) solutions allow a seamless and secure migration to SIP. With Ribbon, enterprises can quickly, easily and securely deploy new UC applications with centralized management across their UC networks.

The Threat

Session Initiation Protocol (SIP) attacks can occur for a variety of reasons and from a variety of sources, and can significantly impact an enterprise's productivity and revenue. Some attacks, such as a denial-of-service (DOS), are designed to bring communications networks down. By constantly flooding the network with SIP messages, bad actors can disrupt or even shut down operations, and much like kidnapping, will only stop once they have extracted ransomware payments from the target. To stop these SIP-based attacks enterprises need an SBC to protect their UC network and to ensure the security and flow of SIP sessions as they traverse between secure and non-secure endpoints.

The Solution

To protect voice networks against the widest possible range of attacks, an enterprise UC security strategy should protect both the endpoint and the media itself. This can be achieved with network border security elements such as Ribbon's session border controllers (SBCs), which provide privacy and compliance, protection for UC assets and securing UC networks.

Protecting Assets

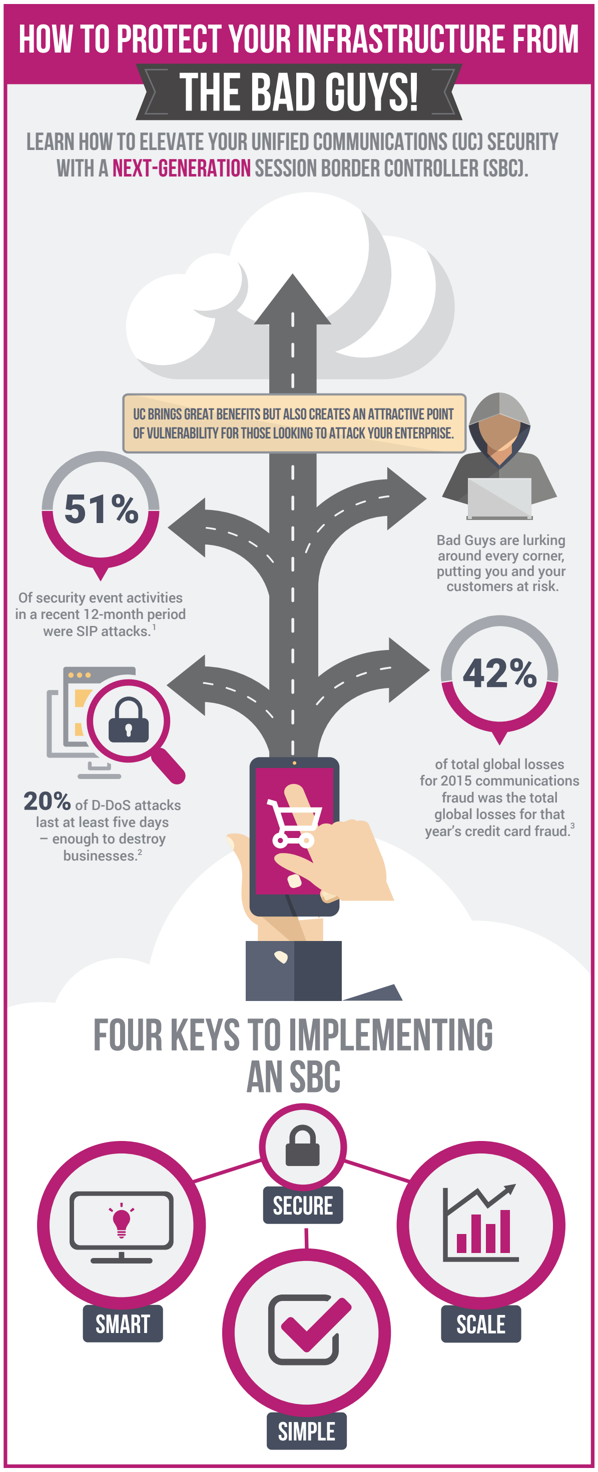
- **Network Topology Hiding**
- **Malformed Packet Protection Adaptive Overload Controls**
- **Endpoint Registration**
- **Full SIP Session State Awareness**

Securing Networks

- **Denial-of-Service (DoS) Attack Prevention**
- **Distributed DoS (DDoS) Attack Prevention**
- **Policers**

Privacy and Compliance

- **Secure RTP (SRTP) for \Media**
- **TLS & IPsec for Signaling**



HOW TO PROTECT YOUR INFRASTRUCTURE FROM THE BAD GUYS!

LEARN HOW TO ELEVATE YOUR UNIFIED COMMUNICATIONS (UC) SECURITY WITH A NEXT-GENERATION SESSION BORDER CONTROLLER (SBC).

UC BRINGS GREAT BENEFITS BUT ALSO CREATES AN ATTRACTIVE POINT OF VULNERABILITY FOR THOSE LOOKING TO ATTACK YOUR ENTERPRISE.

51% Of security event activities in a recent 12-month period were SIP attacks.[1]

Bad Guys are lurking around every corner, putting you and your customers at risk.

20% of D-DoS attacks last at least five days – enough to destroy businesses.[2]

42% of total global losses for 2015 communications fraud was the total global losses for that year's credit card fraud.[3]

FOUR KEYS TO IMPLEMENTING AN SBC

Protecting Assets

- Network Topology Hiding
- Malformed Packet Protection Adaptive Overload Controls
- Endpoint Registration
- Full SIP Session State Awareness

Protecting Assets

Hacking into UC sessions requires that the malicious party intercept signaling and/or media flowing between two endpoints at any of several points along the communications path. Several potential points of attack — or attack vectors — exist in RTC sessions, including:

- UC application servers
- Call control elements, such as PBXs and automatic call distributors (ACDs)
- Session-layer servers and proxies, such as SBCs
- Transport and network layer elements, such as routers
- Link-layer elements, such as Ethernet switches and wireless LANs
- Endpoints, such as desktop and laptop PCs, mobile devices, IP phones and video conferencing terminals

Ribbon SBCs protect UC assets from various threats and anomalies. They maintain their scale, quality and performance in processing known UC users, while leveraging several methods to prevent bad actors from initiating attacks and penetrating an enterprise's UC network.

Network Topology Hiding

Ribbon SBCs hide your network topology by acting as a back-to-back user agent (B2BUA) as defined by the Internet Engineering Task Force (IETF) RFC 3261. Serving as a B2BUA, Ribbon SBCs divide a SIP session into two distinct segments: one between the endpoint and the SBC; the other between the SBC and the IP private branch exchange (PBX) or unified communications (UC) server.

Trunk Groups are employed at the network edge to manage call admission, traffic controls, and other functions between the enterprise and service provider network. Accordingly, all call signaling traffic is routed through the SBC.

Similarly, real-time transport protocol (RTP) relay allows media flows to be proxied through the SBC. Thus, the Ribbon SBC translates IP addresses and ports for signaling and media streams that traverse the system to hide the core network addressing schemes and translations.

Malformed Packet Protection

Bad actors may attempt to send malformed packets to cause the UC application or service to crash, or exploit a vulnerability that provides unauthorized access. Ribbon SBCs maintain full session state information and is therefore able to detect and stop attempts to send malformed packets over the UC network.

Adaptive Overload Controls

Call admission control limits the number of UC sessions that can be simultaneously active in order to prevent network overload. An overload can degrade the performance of other calls on the network, or crash an RTC environment — in effect, a self-inflicted denial of service.

Ribbon SBCs allow the overload threshold parameters to be configured on the SBC based on CPU and memory utilization. When a threshold is reached, the SBC adjusts the system call and registration acceptance rate up or down to maintain the target CPU usage configured for that level. This capability maximizes the system throughput without exceeding the desired CPU utilization threshold. During adaptive throttling, the Ribbon SBC can assign different preferences (priorities) to normal calls, emergency calls, and initial SIP registrations.

Endpoint Registration

SIP signaling registration enables an SBC to relay SIP endpoint registration information between endpoints and the registrar. In Ribbon SBCs, the registration facility allows different expiration times on the untrusted versus trusted network. This is an important aspect of Ribbon SBCs as it can be used to reduce the registration refresh load on the registrars without sacrificing fast detection of failed endpoints.

Full SIP Session State Awareness

Full SIP session state awareness enables an SBC to initiate, reinitiate, maintain, or terminate UC sessions, as necessary. UC is only getting more complicated, and it's becoming increasingly difficult to capture and act on this information. Ribbon SBCs can dynamically process the deep UC signaling and messaging requirements associated with SIP statefulness, including parsing and inferring the following:

- Active and changing port numbers
- User Datagram Protocol (UDP) service types
- Stream activity/inactivity
- Bandwidth requirements

Ribbon SBCs provide full SIP stack and session state knowledge to protect downstream UC elements (such as phones, PBX, the UC stack itself, and more) against distributed denial of service (DDoS) attacks.

Securing Networks

- **Denial-of-Service (DoS) Attack Prevention**
- **Distributed DoS (DDoS) Attack Prevention**
- **Policers**

Securing Networks

Denial of service (DoS) and distributed denial of service (DDoS) attacks were virtually non-existent in legacy circuit-switched time-division multiplexing (TDM) telephony systems, which operated as monolithic systems on isolated voice networks. Unfortunately, DoS/DDoS attacks have new and specific motives in targeting UC. For example, an attacker can disrupt a target organization's communications infrastructure:

- At the desktop level, by crashing endpoints (such as phones and desktop PCs)
- At the gateway level, by taking out the network nodes that provide the interface between an enterprise SIP environment and the outside world
- At the network level, by directly targeting an enterprise IP private branch exchange (PBX) using SIP or other protocols to crash the session manager with an endless flood of session requests

An attacker's motivation for a DoS/DDoS attack may include extortion (demanding a ransom payment from the victim organization to suspend the attack) or other financial gain. Ribbon SBCs are specifically designed to provide a secure hardened edge that secures the enterprise UC network from discriminate or non-discriminant DoS/DDoS attacks.

DoS and DDoS Defense (Policers)

Ribbon SBCs uses specialized processing and policing software to manage high traffic volumes and protect the UC core network from denial of service (DoS) and distributed denial of service (DDoS) attacks. Ribbon SBC's numerous built-in policers include the following:

- **Black-list:** Static list of IP addresses and/or network prefixes that are discarded on ingress
- **Dynamic Blacklisting:** Designed to detect and block misbehaving endpoints for a configured period of time rather than prevent malicious attacks, for which the system already has other mechanisms
- **White-list:** Static list of IP addresses and/or network prefixes that are allowed to access the SBC
- **Micro-flow policer:** allows registered endpoints through the SBC
- **Unknown Peer:** Allows any unknown packet through the Ribbon SBC up to the specified packet rate limit

Privacy and Compliance

- **Secure RTP (SRTP) for \Media**
- **TLS & IPsec for Signaling**

Privacy and Compliance

There are myriad regulatory requirements for data security and privacy that are applicable in various industries and regions throughout the world. In UC environments voice, video, and other media are other forms of IP-based data in the network that must also be safeguarded.

Eavesdropping, or the unauthorized interception of UC traffic between endpoints can be a major security and privacy threat to organizations. A UC session can be tapped by compromising the network anywhere along the data route. Moreover, it's possible to remotely activate conferencing or handset/headset microphones on compromised endpoints. Eavesdropping can be implemented using SIP proxy impersonation or registration hijacking. To counter the eavesdropping threat, enterprises and service providers should encrypt media signaling in their UC environments.

Media Encryption

UC traffic needs to be encrypted for privacy and regulatory compliance purposes. Ribbon SBCs use Secure Real-time Transport Protocol (SRTP) to encrypt media packets and all those SRTP encrypted calls are routed through the SBC. SRTP can be used inside or outside the network. With Ribbon SBCs, SRTP on one call leg is independent of its use on other legs of the same call, and is negotiated for each packet leg. Moreover, unlike other SBC vendors that incur diminished scale and performance when encryption is turned on, Ribbon SBCs continue to perform normally with encrypted traffic.

Signaling Encryption

SIP signaling messages are plain text and relatively easy to intercept. Ribbon SBCs use Transport Layer Security (TLS) and Internet Protocol Security (IPsec) to encrypt signaling traffic. Ribbon's SBC TLS model supports peer authentication confidentiality, and message integrity while its IPSec model supports cryptographic protection for non-media IP packets using the management or packet interfaces.

Summary

Ribbon SBCs allow enterprises to focus on their core competencies and service providers to deliver best-in-class communications features to their customers, without fear of their networks being compromised. Ribbon SBC secure the UC network in the following ways:

- By invoking back-to-back user agent (B2BUA) functionality, the SBC can hide the enterprise's underlying network from bad actors attempting to infiltrate and steal mission-critical data over the UC infrastructure.
- Complete security for signaling and media, including traffic policing, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attack detection and blocking and rogue Real-Time Transport Protocol (RTP) protection.
- In the event of an equipment failure, physical attack or persistent DoS/DDoS attack, strong redundancy capabilities allow for service to be maintained. Additionally, a disaster recovery plan with redundant sites should also be considered to maintain continuous service availability.
- Ensure privacy on the media (SRTP) and signaling (IPSec/TLS) path without sacrificing scalability or performance.

Contact Us Contact us to learn more about Ribbon solutions.