ALL COVERED MANAGED VOICE
TOP REASONS TO USE AN SBC WITH SIP TRUNKING

WHY SBCS ARE INDISPENSABLE

"The Session Border Controller is truly a work-horse element of a good SIP trunking environment." - Steve Johnson, Ingate SBCs.

Connect the company's communication infrastructure to the public Internet, SIP trunking service providers and/or private vendor network. They have multiple critical roles in maintaining and securing the network.

ENSURING QUALITY

SBCs enhance call quality and ease of use. They allow the PBX to be located on the LAN with a private IP address, normalize SIP trunking signaling between the PBX and the service provider, and provide signification routing capabilities. SBCs also ensure interoperability of VoIP and video devices, testing VoIP lines, monitoring call quality, and more.

MONITORING TRAFFIC

SBCs work by using pattern analysis to spot unusual activity, such as a DoS attack that manifests in the form of an overwhelming amount of traffic from a single IP address or a number of machines that are simultaneously trying to make requests from the same server.

SECURITY MAINTENANCE

Once an SBC spots a potential threat, it can quickly block the problem. It then notifies the CPU and host of the details of the threat and the protocols that have been implemented to neutralize it. The SBC can even send details of the threat to a business's other locations to ensure that they are on the lookout for similar breaches.

STAYING UP TO DATE ON POSSIBLE THREATS

Hackers are constantly becoming more sophisticated, changing and upgrading their methods to bypass older security measures. SBC vendors update their protocols just as quickly to ensure that security breaches don't happen. Users simply need to install all updates and patches as soon as they are made available to maintain an effective defense program.

SBCS AREN'T A LUXURY—THEY'RE A NECESSITY FOR SIP TRUNKING

When it comes to voice systems, firewalls just aren't enough to prevent attacks. SBCs are critical to protecting businesses' communications systems against DoS attacks, which can disrupt phone calls and video conferences, steal important information, eavesdrop on calls or infect systems with malware and viruses.

It's surprising to see that so many companies don't use SBCs; but as technology grows more complex and security concerns become more threatening, the interoperability and security capabilities of SBCs will prove to be a necessity for quality SIP trunking.