Vega SMB SBC Appliance
Use Cases

IP communications across multiple, sometimes untrusted, networks needs to be normalized, managed and secured. There is a need to guarantee interoperability of multiple devices, carriers and protocols in a transparent way to the user of the network. Session border controllers take care of the conversion between protocols, transcoding, threat prevention, resource limiting, and accounting at the edge of VoIP networks of enterprises and carriers alike.

In hosted deployments, having an E-SBC at the edge of the enterprise network puts a control point local to the remote network. This E-SBC control point is used to provide security features, such as TLS and SRTP, over the Internet to secure signaling and audio. The E-SBC also provides security policies specific to VoIP traffic, thus enhancing the security into the enterprise network.

The E-SBC is also used as a demarcation point into the enterprise network, allowing a single point of entry and exit for all VoIP traffic. This ensures the enterprise network as a VoIP knowledgeable device monitoring all traffic and applying routing and security policies.

The E-SBC provides the hosting provider the ability to ensure SLA compliance by having a device local to the enterprise network edge to monitor and analyze voice quality issues and determine the most efficient action to resolve.

Quick Facts

- Supports 5 or 10 Simultaneous Calls
- Migrate to SIP Trunking or Hosted PBX Securely
- Empower Remote Workers
- Interoperates with All Major IP PBXs & UC Systems
- DoS/DDoS Attack Protection
- Network Interconnect Point for SIP Trunking
- Topology Hiding for Fraud Protection
- Optional Annual Support & Software Maintenance Plans

ADVANCED CAPABILITIES

High Availability

Ensure business continuity with our new High availability (HA) feature, allowing mirroring of your main SBC with a standby SBC ready to automatically take over calls in case of failure. This feature is included free of charge!

Protection from Enterprise Security Threats

Denial of Services

- Call/registration overload
- Malformed messages (fuzzing)

Configuration Errors

- Mis-configured devices
- Operator and application errors

Theft of Service / Fraud

- Unauthorized users
- Unauthorized media types

BYOD

- Smartphones running unauthorized apps
- Viruses and malware attacking your VoIP network

Protect Hosted Deployments

Use an E-SBC to secure and enhance VoIP deployemnts:

- Encrypt SIP signaling and audio media
- Remote site VoIP demarcation point
- Reduce firewall and NAT issues
- Secondary Registration for Failover to Local Gateway Access
- Ensure SLA compliance