Security Solutions for SIP-based Networks

Bringing Secure SIP Network and Remote Access to Businesses of Any Size

To benefit from the latest communication and collaboration solutions, businesses are increasingly turning to Session Initiation Protocol (SIP) based networks.

Whether it's to lower costs in the enterprise or the contact center (CC) or to take advantage of the latest multimedia messaging, conferencing, and unified communications (UC) applications, SIP has proven to be the industry standard.

Advantages of SIP

Because they are designed for high-fidelity voice, high-definition video and other real-time collaboration applications, carriers are increasingly offering SIP trunking. SIP trunks cost-effectively support more telephone extensions, permit trunking consolidation, and help reduce local, toll-free, domestic and international long-distance communications costs.

With the support of a SIP network, a growing business can more easily and cost effectively roll out the latest Unified Communications and Customer Contact applications to employees regardless of where they are working: in the office, in the contact center, at home or on the road. The productivity that results from these collaborative, real-time applications is a major competitive advantage.

SIP Trunk Security

However, SIP trunks also present a security challenge: there is vulnerability at the point where the SIP trunk connects to the public network, which can leave a business exposed to hacker attacks including spoofing, call hijacking, eavesdropping and toll fraud, which traditional firewalls cannot address. In addition to potential damage to business operations, privacy and security mandates such as those for credit and health information (e.g., PCI and HIPAA) require that these vulnerabilities be addressed, imposing significant financial and legal penalties for non-compliance.

Customer service is at the heart of what we do, and as a leader in outsourced contact center services, our clients count on us to ensure superior functions and secure service. The Avaya SBCE helps us deliver this, and does so with an eye towards cost-savings. We can reduce our hardware expenses, simplify implementations, and use fewer resources, saving us time and money. Avaya SBCE is critical in helping protect our network, while delivering the cost-saving benefits of SIP trunking."

—Richard Blake, Manager, IT Telecom, Teleperformance.

Avaya Session Border Controller for Enterprise with Avaya Aura® and IP Office™

Avaya Aura and Avaya IP Office are the solutions many growing businesses turn to for comprehensive, easily implemented unified communications.

With thousands of systems installed worldwide, Avaya is an industry standard- bearer, delivering the communications and productivity tools today's employees need to perform at their best.

When Avaya solutions are implemented in conjunction with SIP trunks, the Avaya Session Border Controller for Enterprise works hand in hand to help protect against security threats.

VPN-less Remote Worker Security

Business customers are now facing an evolving world where users are no longer confined inside the walls of the enterprise. Trends towards mobile access to system resources, telecommuting, and BYOD are creating the need to deliver SIP-based services to these remote users in a flexible yet secure manner. Only the Avaya Session Border Controller for Enterprise delivers the complete set of Avaya security and user capabilities for both remote UC and CC, including Avaya Workplace and MAC based authentication, including all Avaya SIP endpoints.

Multi Domain Security

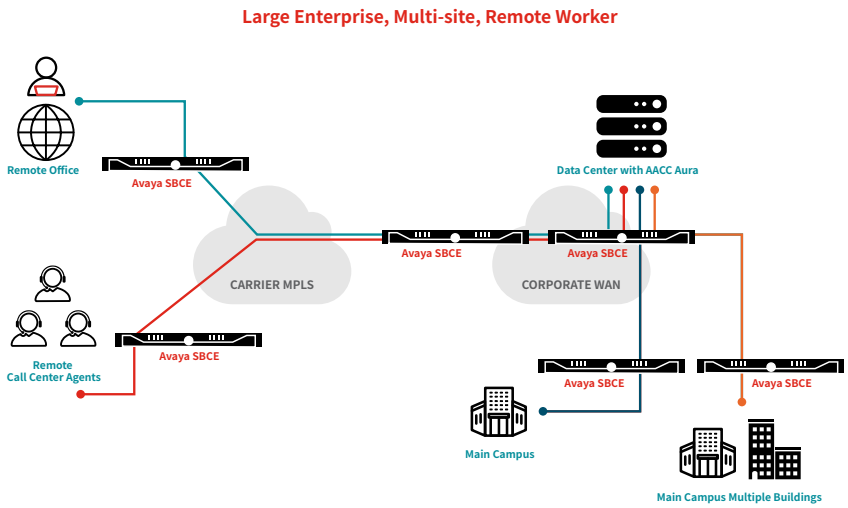
Network support for multiple users connecting via multi-tiered networks, both private and public cloud based, is a necessity. This is especially true for large multinational enterprises or large scaled government communication installations. The criticality of maintaining secure access regardless of location is understood, but the solution is not always as obvious. Avaya Session Border Controller for Enterprise helps provide the necessary functions for network-to-network security as well as network-to-user security. This means that for a large scale, geographically extended network, all layers of network access can be kept secure. The back-to-back-to-back capabilities of the Avaya Session Border Controller for Enterprise will help ensure secure user access no matter how extended and diverse.

Security for SIP-based networks

- A clear line of defense where the SIP trunk meets the public network
- Securely supporting SIP-based communications applications that drive competitive advantage
- Protection against:
  - Denial of Service (DoS) attacks
  - Spoofing
  - Fuzzing
  - Call Hijacking
  - Stealth attacks
  - Toll-fraud
  - Eavesdropping and theft of information
  - Zero day attacks
  - Media Anomaly
- Fine-grained policy enforcement
- Features and Capabilities:
  - JITC Certified
  - Encryption
  - IPv6
  - SIPREC
  - Transcoding
  - Transrating
  - Extensive CDR
  - Support more than 30,000 concurrent sessions on a single box
- Virtualization and IaaS:
  - VMware
  - KVM
  - Nutanix AHV
  - vSphere
  - Amazon Web Services (AWS)

Cloud, On Premise or Hybrid: The Choice is Yours

As more enterprises are looking at hosted alternatives for their Unified Communications and Customer Contact environments, it becomes even more critical for the interfaces between enterprise and host to be secure and manageable. The Avaya Session Border Controller for Enterprise offers an interface that helps to support network protection and enterprise control of SIP traffic. Avaya is the leader in delivering a hybrid architecture, hosted applications as well as enterprise on premise applications. The Session Border Controller for Enterprise is the protection needed to help address proper protocol support and a truly integrated and secure network infrastructure.



A Solution for Growing Businesses

The Avaya Session Border Controller for Enterprise (Avaya SBCE) addresses the security vulnerabilities in SIP networks in a cost-effective, easily-implemented, single-box solution.

Easily operated from an intuitive graphical user interface (GUI), the Avaya SBCE establishes a precise demarcation where the SIP trunks meet the enterprise network, presenting a clear line of defense. It helps deliver enterprise-class security that helps mitigate the risks of Denial of Service (DoS) and application-layer threats as well as toll-fraud. Fine-grained policy enforcement helps support ongoing compliance.

With Avaya SBCE in place, growing businesses can adopt the collaborative and unified communications applications that drive competitive advantage with confidence.

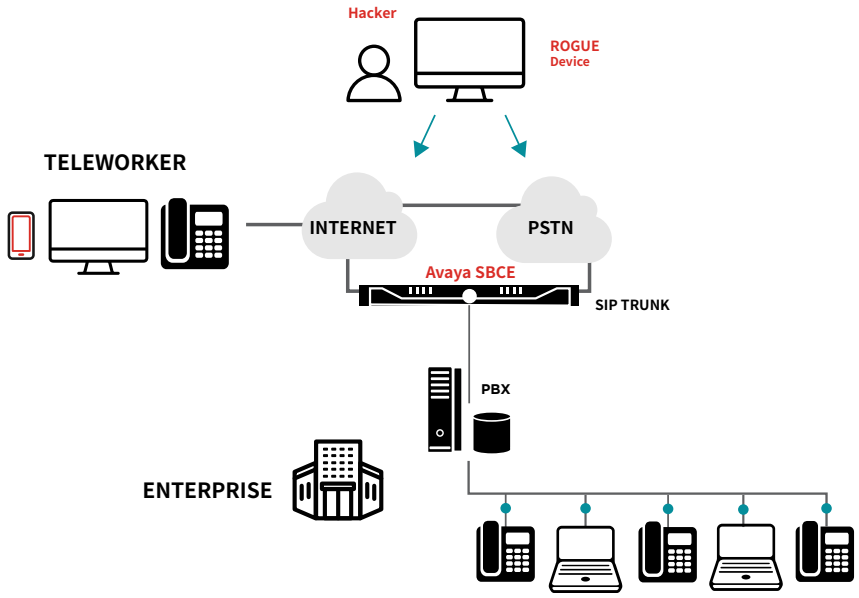
As more enterprises are looking at Hosted and Private Cloud alternatives for their Unified Communications and Customer Contact environments, it becomes even more critical for the interfaces between enterprise and host to be secure and manageable.

The Session Border Controller for Enterprise is the protection needed to help support proper protocol support and a truly integrated and secure network infrastructure. In addition, it provides multi-vendor compatibility:

- **Cisco**
- **Microsoft (including Lync and SfB)**
- **Mitel**

Single-box Solution for SIP Network Security

Avaya Session Border Controller for Enterprise provides an advanced application-layer security architecture in one device: SIP Firewall, Session Border Controller, Access Controller, Authentication, Unified Communications Proxy and Policy Enforcement for all real-time unified communication applications.



Help Secure and Support BYOD

Consumer devices are pouring into the enterprise. Businesses can leverage BYOD—Bring Your Own Device—as a way to reduce TCO, increase productivity, and enhance communication and collaboration. The challenge is how to say yes to BYOD while maintaining control of the network.

Every enterprise is influenced with BYOD, but what gets lost in the conversation is the fact that BYOD is more than just device management. Avaya supports BYOD with a combination of security, authentication, networking, and policies. The Avaya solution includes device authentication, access control for wired and wireless devices, secure remote access, and support via a range of services.

The Avaya Session Border Controller for Enterprise is designed to securely enable many deployments, including:

- Enabling remote workers to connect without VPN, offering support of Bring Your Own Device (BYOD) without the administrative overhead of a Virtual Private Network (VPN) solution
- Secure UC applications entering the enterprise core
- Secure Border Access for incumbent and competitive local exchange

The Avaya Session Border Controller for Enterprise provides a complete set of virtualization options including VMware and Infrastructure as a Service (IaaS).

Support for Legacy Communications

Security for remote access is not just a challenge for new systems; even legacy call systems see requirements to add secure mobile collaboration. The Avaya Session Border Controller for Enterprise has been extensively tested for compatibility with Avaya Aura® and Avaya IP Office installations as well as to support the legacy systems of our customers. The Avaya Session Border Controller for Enterprise supports:

- Avaya Aura platform Release 7.1 and higher
- Avaya IP Office 10.0 and higher
- Avaya Communication Server 1000 Release 7.6

Maintaining secure remote access is our goal for all collaboration solutions and enterprise mobility requirements.

Virtualization

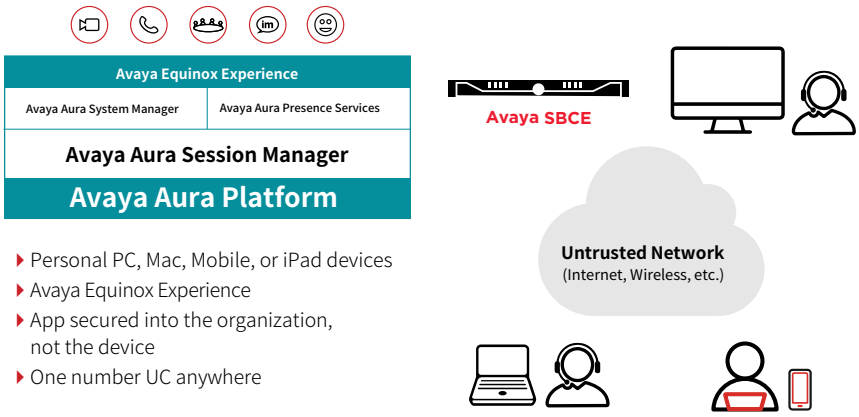
The need to reduce CapEx and consolidate the network environment has led many enterprises to utilize a virtual application solution for real-time collaboration. Extending the benefits of infrastructure virtualization offers a less costly implementation. In addition, the move to virtualization can provide ongoing savings in IT operating expenses due to support for a common system architecture. The secure access requirements for SIP based communications can also significantly reduce the hardware requirements for system design.

The Avaya Session Border Controller for Enterprise offers a virtualized solution for the management as well as the core appliance.

The Avaya Session Border Controller for Enterprise offers a virtualized solution for the management as well as the core appliance. This will support the overall move to a virtualized collaboration solution for all customers as they fulfill the enterprise requirements for SIP access and remote worker security.

Avaya Session Border Controller for Enterprise core application software and the Element Management System (EMS) are available as OVA files for installation on VMware and KVM.

Secure Remote Worker with BYOD



- Personal PC, Mac, Mobile, or iPad devices
- Avaya Equinox Experience
- App secured into the organization, not the device
- One number UC anywhere

VPN -less Remote Worker

About Avaya

Businesses are built by the experiences they provide, and every day millions of those experiences are delivered by Avaya Holdings Corp. (NYSE: AVYA). Avaya is shaping what's next for the future of work, with innovation and partnerships that deliver game-changing business benefits. Our cloud communications solutions and multi-cloud application ecosystem power personalized, intelligent, and effortless customer and employee experiences to help achieve strategic ambitions and desired outcomes. Together, we are committed to help grow your business by delivering Experiences that Matter. Learn more at www.avaya.com.

AVAYA | Experiences That Matter

02/21 • UC4834EN-14