



The Power of We™

Avaya Session Border Controller Advanced for Enterprise



Unified Communications transformation is underway in enterprises of all types:

- Convergence on Internet Protocol; voice, video, data, instant messaging, presence, collaboration applications
- Session Initiation Protocol (SIP) chosen as open standard protocol for Unified Communications
- Highly efficient, extended communications, eliminates network redundancies, improves disaster recovery, reduces carbon footprint
- Competitive advantage is achieved via improved customer relationships and a leaner supply chain

Security is essential for any successful unified communications deployment

Extended unified communications exposes sensitive traffic to potentially untrustworthy networks. At risk may be:

Proprietary data, financials, patient information, confidential communications, credit card numbers

Multiple vulnerabilities can put information at risk

- Denial of service
- Spoofing
- Eavesdropping
- Fuzzing
- Callwalking

Traditional data security provides only partial protection

Gaps: policy enforcement, access control, Private Branch Exchange and phone protection, privacy, authentication

Voice over Internet Protocol / Unified Communications security is different from data security

- Complex protocols/state machines
- Weak endpoints
- Human interactive
- Peer-to-peer
- Application layer
- Real-time

True unified communications require real-time, multi-layer security to achieve the benefits

Avaya offers security solutions for virtually every enterprise. Avaya solutions offer plug-and-play security, enabling mission-critical unified communications. Backed by the Avaya team of unified communication security experts, Avaya appliances are equipped with the most up-to-date vulnerability safeguards to help ensure enterprises are protected from unified

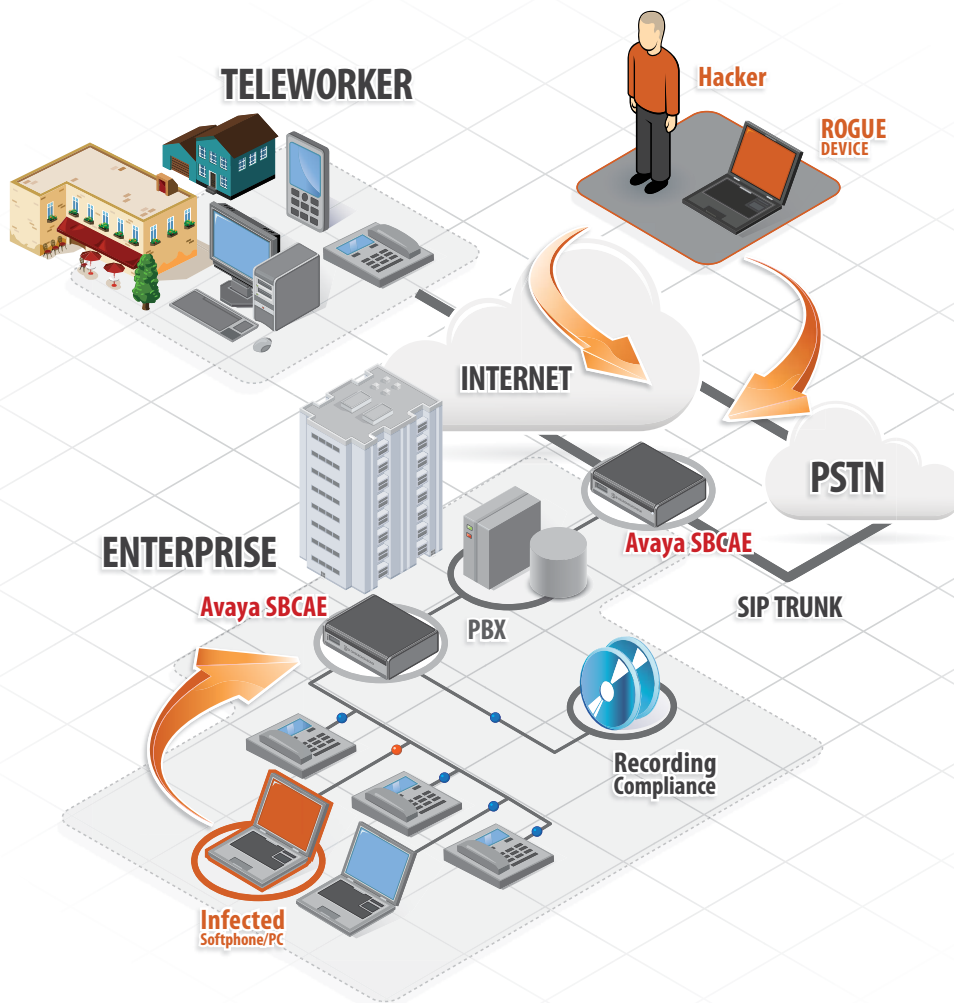
communication related attacks. The Avaya Session Border Controller Advanced for Enterprise is designed to securely enable many deployments, including:

- Internet Protocol Private Branch Exchange and Virtual Local Area Network
- Session Initiation Protocol trunks
- Secure Border Access for Incumbent and Competitive Local Exchange Carriers
- Remote Workers

Benefits of Mobile Enterprise

Accessibility: With mobile Unified Communications, employees essentially carry their desk phone extensions and features with them – via Voice over Internet Protocol clients on their smartphones.

Cost Savings: Today's dramatically higher roaming costs can be substantially reduced or eliminated with use of enterprise mobile unified communications over WiFi or 3G/4G networks.



Enterprise Control: Mobile phone numbers typically are users' personal numbers which stay with them if they leave the company. With mobile unified communications, the mobile phone has a business extension from the company's phone system (the Private Branch Exchange), allowing enterprises to maintain control of business numbers.

Productivity: With rich unified communications features such as transfer, conference, corporate directory, and presence, enterprise users have access to the advanced features necessary to perform their jobs more efficiently.

Mobile Unified Communications Security and Management Challenges

Today's enterprise Private Branch Exchange systems are managed and owned by information technology departments, but mobile devices are not. Because mobile unified communications solutions lack essential security and management functionality, enterprise information technology groups have been slow to embrace them.

Mobile Device Security Posture and Compliance

With most standard internal corporate security measures it is virtually

impossible for information technology personnel to regulate individual's smartphones and:

- Centralize management.
- Secure configurations.
- Enforce corporate regulatory policies.
- Record or monitor conversations or instant messaging chats.
- Ensure that users install only information technology-approved applications.
- Prevent users from installing applications which may be malicious, that share data with third parties, or contain bugs that compromise the phones.

Network and Infrastructure Security

With mobile unified communications, communications travel the public Internet, where information technology cannot protect it from tampering or theft. Today's mobile unified communications clients rarely support encryption or authentication. Even for those clients that support these features, information technology personnel cannot easily link these functions with the enterprise's key management and identity systems. The public certificate solution used for browsing, for example, is not the same used by information technology departments.

Unified Communications Security in a Box

Avaya Session Border Controller Advanced for Enterprise provides a complete application-layer security architecture in one device:

- Firewall
- Session Border Controller
- Intrusion Detection System and Intrusion Prevention System (IDS/IPS)
- Access Controller
- Authentication
- Unified Communications Proxy
- Virtual Private Network / Encryption
- Policy Enforcement

for all real-time unified communication applications



Physical Security

Physical and access control security features that protect desk phones and PCs inside the physically secure corporate office are not available for mobile unified communications. Because the phones are by definition “mobile”, they travel with

users to hotels, airports, taxi cabs. They are sometimes lost, misplaced, or stolen. Without overcoming these security and management challenges, enterprises cannot really embrace mobile unified communications and fully realize the benefits.

Avaya Avaya Session Border Controller Advanced for Enterprise

Avaya SBCAE 100	Avaya SBCAE 100 Security Appliance <ul style="list-style-type: none"> • 100 Registered Devices, • 50 Simultaneous Sessions, • 250 IM Sessions
Avaya SBCAE 200	Avaya SBCAE 200 Security Appliance <ul style="list-style-type: none"> • 200 Registered Devices, • 100 Simultaneous Sessions, • 500 IM Sessions
Avaya SBCAE 500	Avaya SBCAE 500 Security Appliance <ul style="list-style-type: none"> • 500 Registered Devices, • 250 Simultaneous Sessions, • 1,250 IM Sessions
Avaya SBCAE 1000	Avaya SBCAE 1000 Security Appliance <ul style="list-style-type: none"> • 1000 Registered Devices, • 375 Simultaneous Sessions, • 2,500 IM Sessions
Avaya SBCAE 2000	Avaya SBCAE 2000 Security Appliance <ul style="list-style-type: none"> • 2000 Registered Devices, • 500 Simultaneous Sessions, • 5,000 IM Sessions.
Avaya SBCAE 3000	Avaya SBCAE 3000 Security Appliance <ul style="list-style-type: none"> • 3000 Registered Devices, • 750 Simultaneous Sessions, • 7,500 IM Sessions
Avaya SBCAE 5000	Avaya SBCAE 5000 Security Appliance <ul style="list-style-type: none"> • 5000 Registered Devices, • 1,250 Simultaneous Sessions, • 12,500 IM Sessions
Avaya SBCAE 10000	Avaya SBCAE 10000 Security Appliance <ul style="list-style-type: none"> • 10,000 Registered Devices, • 2,000 Simultaneous Sessions, • 25,000 IM Sessions

Active encryption reduces appliance capacity by 50%

Learn More

To learn more and to obtain additional information such as white papers and case studies about **Avaya Session Border Controller Advanced for Enterprise** please contact your Avaya Account Manager or Authorized Partner or visit us at **www.avaya.com**

© 2011 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. and are registered in the United States and other countries. All trademarks identified by ®, ™, or SM are registered marks, trademarks, and service marks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. Avaya may also have trademark rights in other terms used herein. References to Avaya include the Nortel Enterprise business, which was acquired as of December 18, 2009.

11/11 • UC4834

About Avaya

Avaya is a global provider of business collaboration and communications solutions, providing unified communications, contact centers, data solutions and related services to companies of all sizes around the world. For more information please visit **www.avaya.com**.