

# Business Continuity Communications Solution

## Foundation For Pandemic Planning, Workforce Flexibility, Distributed Enterprises, Disaster Recovery

When crisis strikes, enterprises need to be ready to easily and quickly respond with a technology foundation that enables business processes to flow uninterrupted.

The Sipera Business Continuity Communications Solution (SBCCS) enables you to securely extend rich, fully functional communications to any employee in any location with IP network connectivity.

Most importantly, these communications are comprehensively secure, ensuring that privacy, communications archiving, policy enforcement and access to mission-critical resources continue without disruption.

SBCCS is based on Sipera's award-winning UC-Sec appliance, seamlessly and simply applying comprehensive security controls to a Unified Communications (UC) infrastructure.

With plug-and-play ease, UC-Sec appliances permit you to extend your VoIP, IP Video, Messaging, Collaboration and other communications to any worker in any location on any device. UC-Sec ensures these communications meet the information security requirements required by law or best practices, even when these communications cross untrusted networks such as the Internet.

As a result, enterprises can plan for dramatically greater workforce flexibility and availability in responding to public health concerns, such as Pandemic Planning in response to the Swine Flu (H1N1 Virus) or other outbreaks; natural disasters such as hurricanes and snowstorms; national security issues; and other crises.

SBCCS is production-proven, based on successful UC deployments in the financial services, healthcare, and education sectors, and Sipera has significant experience assisting government entities with UC-related security threat analysis and mitigation.



### CHALLENGES

Unlike classic security controls for data networking, protecting and securing VoIP and UC traffic poses a set of new challenges:

- VoIP and UC are real-time and media intensive, and traditional VPNs, firewalls and virus scanners can hamper performance, especially when these communications are offered to an extended, distributed workforce outside the enterprise boundary.
- Firewalls and classic Network Address Translation methods can reduce the ability to offer fully featured, rich communications that are required for the "in-the-office" user experience.
- Privacy and encryption, network access control, threat detection and mitigation, user authentication, and security policy enforcement are all required to comprehensively manage distributed workforce communications. But in the traditional security architecture these will often be managed by many separate systems and control points, creating an unwieldy management headache.

### SOLUTION REQUIREMENTS

#### UC-Sec: Comprehensive and Simple

The Sipera UC-Sec appliance offers comprehensive VoIP/UC security, enabling you to simply and easily extend communications to home workers, teleworkers, mobile workers, partners, the supply chain and anyone outside the trusted enterprise boundary.

For your business continuity plan, this means that you can be assured that communications can be safely extended to any alternate location in case your corporate facilities are no longer usable. As long as IP connectivity is available, your distributed workforce can communicate and access information resources with the same capabilities as if they were still in their offices.

#### The UC-Sec appliance offers

- **Privacy** – Encryption that ensures mission-critical information is kept private and confidential
- **Access Control** – Authentication of users, including seamless, clientless use of 2-factor authentication for even greater protection of enterprise information resources
- **Threat Mitigation** – Detection and mitigation of thousands of attacks and security threats, based on the most advanced library of vulnerabilities built from years of primary research by Sipera's industry-leading VIPER Lab™

- **Policy Enforcement** – The ability to apply policies on UC traffic with no performance hit, including differentiated policies based on user, network, application, time of day and other characteristics

These essential security functions represent the best practices for managing a distributed communications infrastructure that makes use of any available network for consistent and secure communications. The award-winning UC-Sec makes this power available to you today in one easy to deploy and easy to manage appliance.

### UC-Sec: Production-Proven

UC-Sec is a real-time, purpose built appliance with multiprocessor, multi-core, and on-chip crypto acceleration architecture. All media processing, including encrypted media even under load and attack conditions, is done deterministically in under 50 micro seconds. UC-Sec supports 1+1 high availability deployments and clustering across multiple sites for scalability, geographic redundancy, and real-time call preserving failover.

UC-Sec can be deployed to terminate SIP trunk traffic and to provide extended communications to remote and distributed workers in the same appliance.

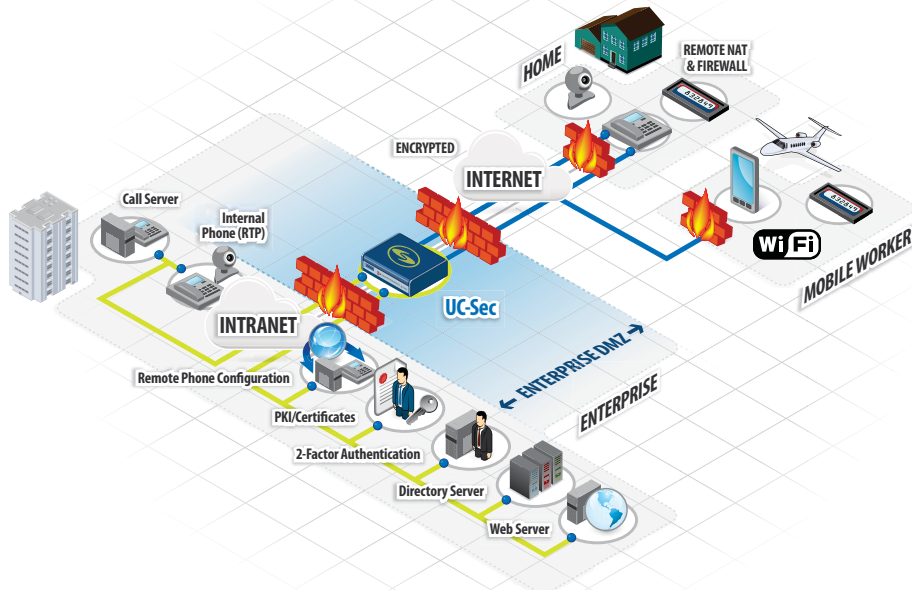
UC-Sec appliances are deployed in the enterprise DMZ for SBCCS and are centrally managed with UC-Sec EMS deployed in the core.

### The Sipera UC-Sec appliance

- terminates TLS/SRTP encrypted UC traffic to prevent reconnaissance and eavesdropping, provides fine-grained policy enforcement to apply different security and call routing rules, and supports multiple authentication mechanisms for strong access control
- supports proxying and NAT rewrites of files and communication protocols to allow for remote phone configuration management and remote phone PKI and certificate management

## RESULT

Business continuity planning is a critical responsibility in today's enterprise. When unexpected crises hit, Sipera's solutions enable you to quickly and easily establish remote workspaces and a distributed workforce, to permit your essential business processes to continue without interruption.



## UC Security in a Box

Sipera's UC-Sec appliance 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
- VPN / Encryption
- Policy Enforcement

... for all real-time Unified Communication applications

## UNIFIED COMMUNICATIONS UNLEASHED

### About Sipera Systems

Sipera Systems, the leader in real-time Unified Communications (UC) security solutions, is the choice of enterprises and service providers around the world to support their mission-critical UC deployments.

Sipera offers groundbreaking solutions that secure voice, video, messaging, collaboration, and other real-time communications in converged IP networks, boosting compliance with information security requirements and simplifying the adoption of UC. Sipera's innovative *Borderless UC™* architecture delivers secure and private enterprise-class communications to any device over any network in any location.

Backed by the industry-leading research of the VIPER Lab, Sipera's award-winning UC-Sec appliance provides comprehensive threat protection, policy enforcement, access control, and encryption in a single, flexible, plug-and-play device. The UC-Sec is pre-integrated with all market-leading UC vendor solutions and is the world's first UC security device to be Common Criteria certified, meeting the stringent international standard for IT security.



www.sipera.com

www.twitter.com/siperasystems

### Sipera Systems

1900 Firman Drive, Suite 600  
Richardson, TX  
75081, USA

T: +1 214 206 3210  
F: +1 214 206 3215  
E: info@sipera.com