

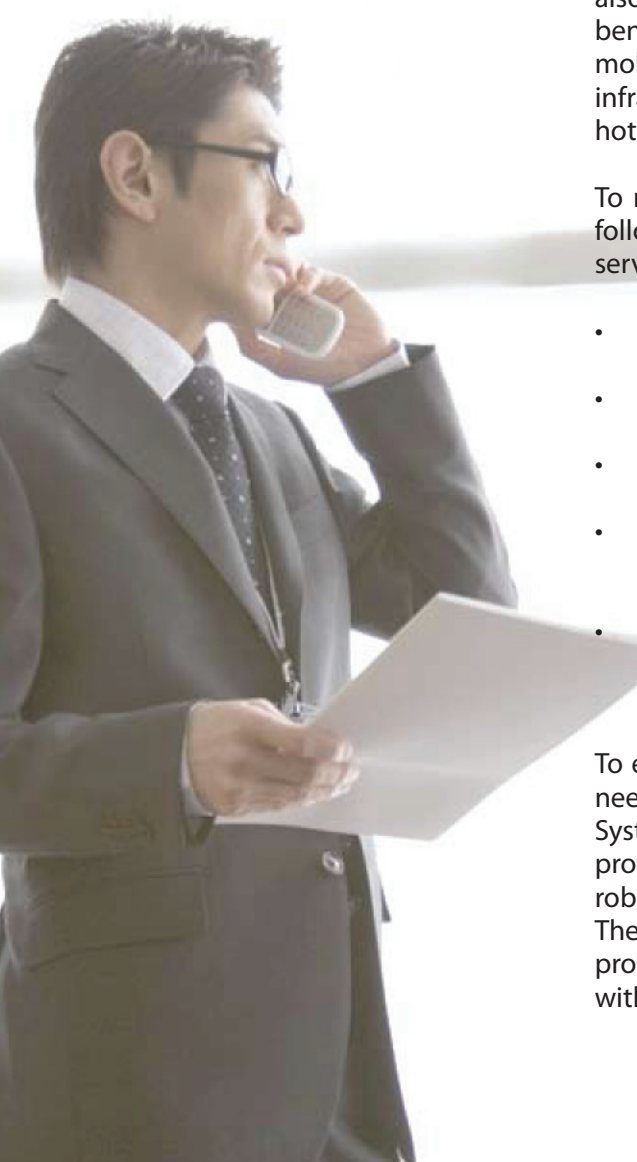
Securing Mobile Workspaces

Today, enterprises realize more than ever that leveraging their IP PBX to extend VoIP and unified communications (UC) over the Internet to remote IP phones, soft phones, and WiFi/dual-mode phones can enhance employee productivity and improve collaboration. Opening communications beyond the traditional enterprise perimeter can also mean cost reductions, enhanced business continuity, and other benefits. But too many enterprises have yet to realize the benefits of mobile workspaces due to the risks of extending their VoIP and UC infrastructure to workers at home or in remote locations like Internet hotspots, hotels, and airline clubs.

To make mobile workspaces a reality, enterprises must address the following security imperatives when extending critical VoIP/UC services over the Internet:

- VoIP vulnerabilities and anomalies that put the network, services, and confidential data at risk must not be exposed.
- Privacy of confidential communication sent over the Internet must be preserved.
- Robust authentication of both phones and remote employees must be employed to ensure strong access control.
- Fine-grained policies must be enforced based on network, user, device, and time of day (especially important for remote employees and mobile devices).
- The security solution for mobile workspaces must not compromise enterprise firewalls and must work with any type of remote network address translation (NAT) environment.

To ensure the deployment of secure mobile workspaces, enterprises need a solution that overcomes these security challenges. Sipera[™] Systems offers a comprehensive, real-time UC security solution that provides comprehensive threat protection, strict policy enforcement, robust access control, and privacy in a single security appliance. The Sipera solution securely enables remote workers to increase productivity by having a complete, in-office phone experience without being physically in the office.



PROBLEM

Although mobile workspaces provide many business benefits, they also present serious security problems for enterprises. When enterprises grant remote users access to their internal UC networks, those enterprises must offer privacy and authentication for all users while addressing vulnerabilities in the UC protocols. At the same time, IT administrators must also:

- Maintain control over the enterprise firewall
- Enforce granular UC policies
- Ensure the quality of service (QoS) required for VoIP and UC services

Enterprises also need to protect their critical VoIP/UC infrastructure and services against VoIP/UC-specific attacks.

Protection against VoIP and UC protocol vulnerabilities

VoIP offers many more real-time services than data, including transfer, conference, and hold, making VoIP protocols more complex, flexible, and exploitable. Because of this, more than 50 Requests for Comments (RFCs) exist for SIP in the IETF, compared with only about 10 for HTTP, which has been around more than twice as long.

With known ports open on enterprise firewalls to allow inbound and outbound VoIP and UC traffic, enterprises must perform deep-packet inspection and continuously police application traffic to protect the VoIP network, endpoints, and IP PBXs from thousands of application-layer attacks that can cause such problems as IP PBX crashes, lost services, and degradation of voice quality.

These types of VoIP/UC-specific application layer attacks include:

- Reconnaissance
- Spoofing
- Eavesdropping
- Signaling and media manipulation
- Service theft/fraud
- Denial of Service (DoS)/Distributed DOS (DDoS) attacks
- Fuzzing and buffer overflow exploits
- VoIP spam
- VoIP phishing

Confidentiality and privacy concerns

When VoIP traffic is sent over the Internet, both signaling and media traffic must be encrypted to ensure complete privacy of real-time communications. Because attackers can use sniffing methods to easily exploit signaling traffic for reconnaissance purposes and to learn detailed call-related information (such as caller and call recipient IP addresses, date, and time of the call), it is essential to encrypt signaling traffic. Similarly, media must be encrypted to ensure privacy of the actual communication. However, encrypting media traffic can potentially degrade quality of service (QoS). The problem is compounded by management and operational costs if the artificial requirement for a VPN client on the phone or a home VPN gateway is imposed.

Access and authorization

Before establishing a signaling or media session, remote users must be authenticated. This authentication can be done in a variety of ways, including the use of digests or certificates. Many enterprises require the use of two-factor authentication schemes such as RSA SecurID for remote access to prevent unauthorized calls on stolen or lost phones.

Policy compliance for UC traffic

To deploy mobile workspaces without compromising established security policies, enterprises must also enforce fine-grained UC policies. VoIP and IT administrators must control voice, video, IM, and other UC applications by defining the way the applications are used and the networks, devices, and users that are authorized to interact with the applications. Policies for mobile users and devices must be dynamic and flexible to satisfy these requirements.

Firewall/NAT traversal on both near-end and far-end

When deploying firewall/NAT devices, signaling and media streams must be able to traverse the firewalls on both sides of the end-to-end session. This requirement presents both near-end and far-end firewall/NAT traversal challenges. Besides signaling and media traffic, VoIP phones also use dynamic ports for remote configuration protocols, such as TFTP, and for other web-based services such as corporate directory access.

The solution for securing mobile workspaces must not compromise the enterprise firewall and/or make its policies too complex (for example, by requiring an update to the firewall for every addition, update, or deletion of a VoIP endpoint). The solution also must work with any type of remote NAT environment, as these devices are seldom under the control of the enterprise.

Voice and video quality monitoring
Although the biggest challenge of ensuring appropriate QoS levels for VoIP has been solved in recent years by implementing better networks and new codecs, extending VoIP over an uncontrolled network such as the Internet is still very new. Therefore, easy access to voice quality metrics for latency and jitter must be available to troubleshoot any performance degradation issues that occur.

SOLUTION

The Sipera UC-Sec™ security appliances offer real-time VoIP and UC security, including comprehensive threat protection, strict policy. The Sipera Systems UC-Sec™ security appliances offer comprehensive, real-time UC security that includes threat protection, policy enforcement, access control, and privacy to address the security issues associated with deploying mobile workspaces. Built on a real-time platform and based on the groundbreaking vulnerability research of the Viper Lab, Sipera's research and services unit, UC-Sec performs the following functions for mobile workspaces:

- Protects against threats by blocking them at the enterprise perimeter.
- Offers fine-grained policy enforcement based on user, network, device and time-of-day.
- Integrates with AAA and two-factor authentication servers for strong access control.
- Serves as the termination point for encrypted Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP) streams traversing the uncontrolled Internet.

- Simplifies the deployment of mobile workspaces by providing firewall/NAT traversal security, phone configuration proxy, and preservation of voice QoS, bandwidth-based call admission control, and other key features.

VoIP and UC threat protection in the DMZ

All inbound Internet traffic that goes to high-value VoIP and UC servers must pass through the Sipera UC-Sec security appliance, which inspects and validates the traffic. UC-Sec is VoIP-aware and performs deep-packet inspection while it tracks call states, which is crucial for UC threat mitigation.

Define and implement strong UC policies

The first step in deploying a mobile workspace is to define rules for VoIP and UC traffic. Sipera's UC-Sec enforces these policies based on network, user, device, and time-of-day. If any of these attributes changes, UC-Sec applies a different policy.

Integrate with existing infrastructure for strong access control

Loss of a remote enterprise phone is a genuine concern. Device authentication is done via X.509 certificates. However, it is more important for enterprises to authenticate users. The Sipera UC-Sec solution offers strong access control by ensuring VoIP users and devices are authenticated against existing AAA or two-factor authentication servers.

Ensure signaling and media privacy

Traffic that passes over an untrusted network is susceptible to reconnaissance activities such as sniffing and eavesdropping attacks. Encryption, using TLS for signaling traffic and SRTP for media traffic, must ensure privacy without compromising performance. With the Sipera UC-Sec appliances, internal phones, media gateways, conference bridges, and call servers do not require upgrades to support encryption natively because UC-Sec terminates encrypted traffic from the public Internet and sends unencrypted streams to the private enterprise intranet.

Ensure signaling and media privacy

Traffic that passes over an untrusted network is susceptible to reconnaissance activities such as sniffing and eavesdropping attacks. Encryption, using TLS for signaling traffic and SRTP for media traffic, must ensure privacy without compromising performance. With the Siperia US-Sec appliances, internal phones, media gateways, conference bridges, and call servers do not require upgrades to support encryption natively because UC-Sec terminates encrypted traffic from the public Internet and sends unencrypted streams to the private enterprise intranet.

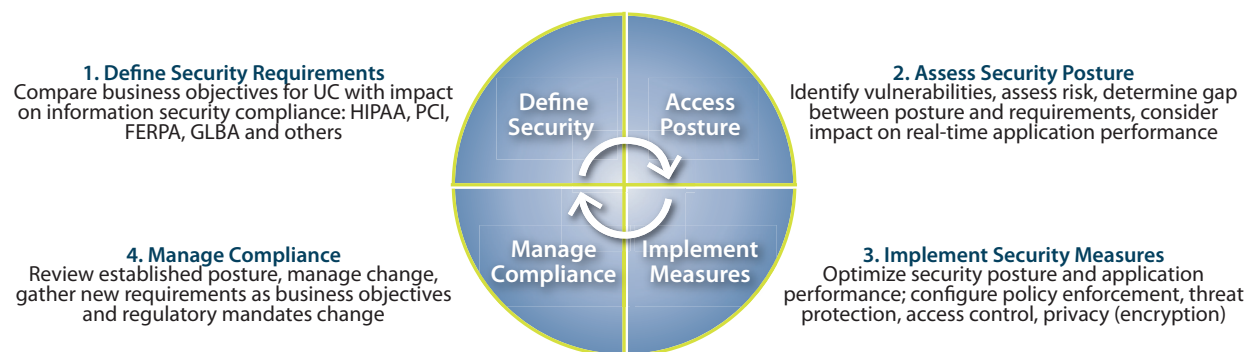
Ensure and monitor voice and video quality

If voice and video quality suffers, the whole mobile workspace solution becomes unusable. IT and telecom administrators require separate intranet and Internet reports and logs for VoIP quality metrics to troubleshoot problems. Siperia's real-time UC-Sec appliances offer deterministic performance with delays for media packets measured in hundreds of microseconds (even when encryption is involved and call volume grows) while reporting VoIP quality metrics such as latency and jitter.

Simplify firewall/NAT traversal

Employee home routers and WiFi hotspots are usually not under the control of enterprises, so enterprises must place a security appliance in their enterprise "demilitarized zones" (DMZs) to solve far-end firewall/NAT traversal issues for VoIP deployments. Because enterprises have multiple firewalls and DMZs, changing rules on firewalls can be a multi-day process. Siperia's UC-Sec solution simplifies near-end NAT traversal using static rules that do not require updates when changes occur in the enterprise VoIP network.

Unified Communications Security Life Cycle



Companies around the world rely on Siperia Systems to ensure their UC and VoIP deployments support compliance with information security requirements and mission-critical corporate objectives. Through dozens of successful vulnerability assessments, security architecture consulting projects, and security appliance deployments, Siperia has developed a standardized Unified Communications Security Life Cycle. This process represents a best practice for continuous improvement of the security architecture, enabling an enterprise to be certain that essential security functions can keep pace with the transforming communications infrastructure.

To learn more about Siperia's solutions and for personal consultation about your UC security requirements, please visit www.siperia.com

IMPLEMENTATION

The Sipera UC-Sec appliances are deployed in the enterprise DMZ to secure mobile workspaces and are centrally managed by the Sipera UC-Sec Element Management System (EMS) deployed in the core. In addition, UC-Sec can be deployed in secure channel deployments to minimize dynamic pinholes across firewalls and simplify any required changes in the future. UC-Sec also supports high-availability deployments and clustering across multiple sites for scalability and geographic redundancy.

The following figure shows two UC-Sec security devices - one in the DMZ and another in front of the IP PBX - that handle firewall/NAT traversal (as shown in step 1) and allow the use of secure tunneling, which provides a level of security not available in any other type of configuration. Secure Channel (as shown in step 2) minimizes the number of pinholes the firewalls would normally have to open at any time to accommodate normal network activity. This deployment scheme also accommodates multiple/redundant call servers without degrading the network's security profile or increasing latency.

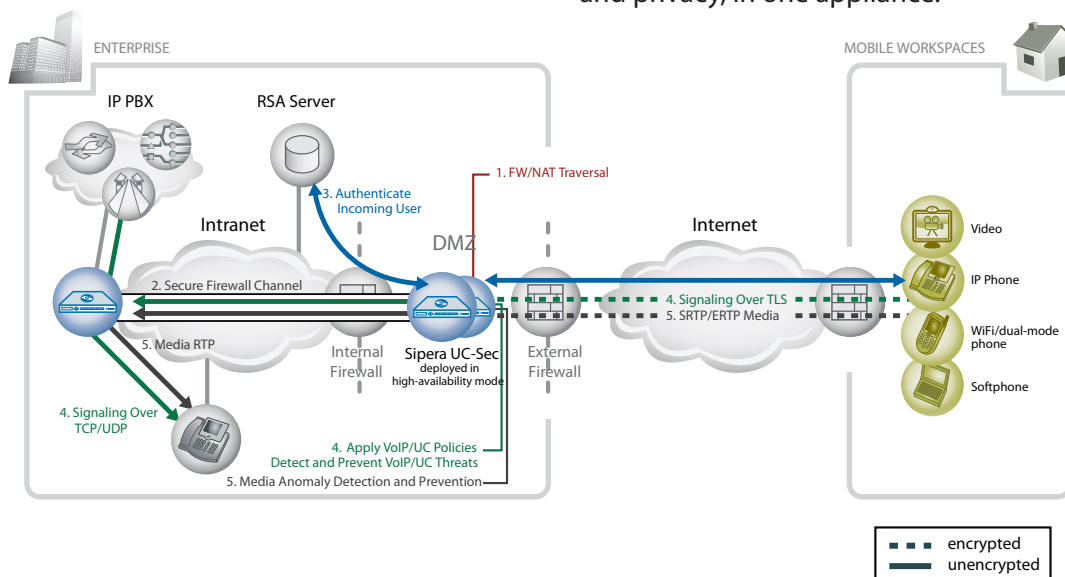
In the deployment shown here, the Sipera UC-Sec security device, deployed between the internal and external firewalls, uses two-factor authentication to verify users (as shown in step 3) and decrypts all TLS-encrypted SIP or SCCP signaling traffic in real-time. Once the decryption takes place (as shown in step 4), this UC-Sec device looks for anomalous behavior and attacks and applies the VoIP/UC policies before

forwarding the packets through the virtual tunnel to the second UC-Sec device, deployed in front of the IP PBX, to establish the requested call session. If the call is from an external phone to an internal phone (as shown in step 5), the UC-Sec appliance also decrypts the SRTP media coming into the enterprise from the IP network, performs any required NAT traversal, applies the relevant media policies, and looks for media anomalies before sending it to the second UC-Sec appliance.

RESULT

Companies around the world rely on Sipera UC-Sec in their VoIP/UC networks to secure, and realize the many business benefits of, VoIP and UC mobile workspaces. These enterprises have decreased telecommunications charges by leveraging internal IP PBXs to handle calls within the enterprise for free or by routing international calls at much lower rates. Mobile employees have significantly reduced overages and roaming charges while enjoying true mobility, with one phone and number, by using WiFi/dual-mode phones. In other cases, enterprises support mobile workspaces as an integral part of their business continuity plan so that VoIP/UC remote users can conduct business activities from virtually any location, allowing the business to continue to function in an ongoing fashion.

For organizations that want to realize the many benefits of unified communications, the solution is simple. The Sipera UC-Sec products provide comprehensive, real-time security for mobile workspaces and offer comprehensive threat protection, policy enforcement, access control and privacy, in one appliance.



UC Security Defined

About Siper Systems

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

Sipera offers groundbreaking, production-proven solutions that secure voice, video, messaging, collaboration, and other real-time communications in converged IP networks, boosting compliance with information security requirements.

Backed by the industry-leading research of the VIPER lab, Sipera's solutions provide comprehensive threat protection, policy enforcement, access control, and encryption in a single flexible appliance.

 www.sipera.com

V#05-09-09



Sipera Systems Inc.
1900 Firman Drive, Suite 600
Richardson, TX 75081, USA
T: 214 206 3210
F: 214 206 3215
E: info@sipera.com