Enabling Resilient, Secure and High Availability Voice Services in Microsoft Lync Deployments

SBCs for Increased Enterprise Voice Security and Resiliency
EXECUTIVE SUMMARY

Organizations are moving towards a centralized call processing model by leveraging converged IP networks to save costs. But consolidating infrastructure at the headquarters and extending the enterprise to include branch offices and remote sites, requires careful planning. Any downtime in voice services either at the headquarters or the branch offices leads to loss of productivity, profitability and competitiveness. In order to provide branch office employees the same voice experience as in the headquarters, organizations need to consider solutions that provide voice service continuity through a resilient, enterprise-grade telephony architecture. A single-point-of-failure architecture may render remote offices completely unreachable if the data network is down.

Leveraging the Sonus SBCs for Increased Enterprise Voice Security and Resiliency

Banks, retail enterprises, government agencies, educational institutions or any company with branch offices needs a solution that:

- Minimizes or eliminates impact of service disruption
- Provides secure voice connectivity
- Defends against denial-of-service attacks
- Provides a highly scalable architecture to meet the growing demands of the enterprise, and
- Consolidates infrastructure to reduce cost

The Sonus SBC 1000 and SBC 2000 session border controllers have been architected to provide reliable voice services for the headquarters, the branch and remote sites.

PROVIDING HIGHLY AVAILABLE AND RESILIENT SBCs FOR MICROSOFT LYNC DEPLOYMENTS

The security threat to VoIP services and systems is real and could cripple an organization’s ability to conduct business. Just as with traditional PBXs, IP telephony systems also have to offer high reliability and resiliency. A properly designed VoIP architecture should include features like high availability load balancing, and security features such as encryption and firewall capabilities to thwart DoS attacks. The type of transport protocol supported by the network also has an impact on the resiliency of the voice services.

SECURITY

Securing the network against malicious use, sabotage and DoS attacks are necessary for the successful implementation of VoIP. With access to the public Internet and other external networks, security becomes an important issue to consider.

Toll fraud can occur when malicious users try to make personal calls using an enterprise VoIP network. Under some conditions, certain SBCs provide users with a secondary dial tone. A knowledgeable user may be able to make calls by dialing an external access digit which is typically ‘9’ in most organizations. The Sonus SBC Series will never provide a secondary dial tone.

Other security issues such as eavesdropping and DoS attacks can be mitigated by implementing encryption and firewall capabilities. The Sonus SBC Series offers both TLS and SRTP encryption and a built-in firewall to protect against DoS attacks.

ENCRYPTION

In order to provide a high level of security, both signaling and media traffic needs to be encrypted. It is very easy to intercept SIP messages as they use plain text for signaling. The Sonus SBC Series uses the Transport Layer Security (TLS) protocol to secure signaling information from intruders. Secure Real Time Protocol (SRTP) is used by the gateway to encrypt the media packets.

To protect callers on the network, Sonus SBCs support 128-bit Advanced Encryption Standard (AES) media encryption via SRTP. An X.509 digital certificate either created by the SBC or supported by a third-party certificate authority provides the necessary encryption key. The encryption and secure key exchange supported by the SBC enables mutual authentication using the Message Digest 5 (MD5) Secure Hashing Algorithm (SHA).

Even as encryption provides voice security from eavesdropping, it creates a significant drain on call processing capacity. The Sonus implementation of security in a separate hardware accelerator card within the SBC 1000/2000 Series and in the DSP module for the SBC series ensures that there is no degradation of either call quality or capacity. The Sonus SBC 2000 supports up to 1000 simultaneous calls on a single box whether encryption is used or not.
DENIAL OF SERVICE ATTACKS
Malicious users launch DoS attacks to cripple voice services in an organization. DoS attacks may be targeted to a specific end point or to the entire network by sending a large volume of traffic over the IP network. A VoIP-aware SBC can be used to mitigate against DoS attacks.

The Sonus SBC 1000 and SBC 2000 provide protection through features like VLAN tagging and built-in firewall capabilities to stop DoS attacks. Using VLAN tagging, VoIP traffic can be separated from data traffic to provide additional security for voice. The built-in firewall in the SBC only allows VoIP traffic to pass through. Other packets that are not voice related are immediately dropped to minimize impact of DoS attacks.

RELIABLE TRANSPORT USING TCP PROTOCOL
User Datagram Protocol (UDP) is a widely used protocol for streaming audio and video. Early SIP RFCs required vendors to support SIP over UDP communications only. Now, RFC 3261 requires support for both UDP and Transport Control Protocol (TCP). TCP transport provides reliable message delivery and connection-based communications. The Sonus SBC 1000 and SBC 2000 support both UDP and TCP transport protocols for providing a reliable transport mechanism while also increasing the number of interoperable elements in the network.

HIGH AVAILABILITY AND LOAD BALANCING
The data networks may not always be operational due to a scheduled downtime or due to unscheduled events like power failure. A high availability solution ensures that the voice services are always available and the users are able to place and receive calls even under peak call rates or during network disruptions.

A pair of SBCs configured in an Active-Active mode provides the necessary enterprise-grade network resiliency for voice services through implementing high availability and load balancing architecture (see Figure 1). For incoming calls, Sonus SBCs load balance across multiple mediation servers in a Microsoft Lync environment. The calls to the mediation server are then load balanced using the round robin method. The Sonus SBC 2000 is engineered to handle up to 1000 simultaneous calls on a single node.

RECOVERING FROM MAJOR DISRUPTIONS
Disruptions happen and a resilient architecture provides protection for voice services from these interruptions. Availability of voice services can be impacted due to the following reasons:

- Hardware and power failure
- Link failure between sites

Recovering from Hardware Power Failure
Most Sonus SBC configurations come with a redundant power supply to minimize failures.

Recovering from Link Failures
Voice service can be disrupted due to failures of the IP network. Some Sonus SBCs rely on Link Quality Management (LQM) functionality to monitor the quality of the network. LQM works by sending “I’m alive” messages periodically to establish availability of the next node in the network. This technique is used to check the health of the network and other nodes on the IP network. Using LQM statistics, the gateway can collect statistics such as the average expected round trip time to the node, the average packet loss to a particular node on the network and the node’s availability. If the node is unreachable, then calls going to the node are skipped and the SBC will try alternate routes. In order to mark a node unreachable, the SBC:

- Sends an ICMP Ping command to the remote node’s domain address. If the ICMP ping is unsuccessful, then the SBC determines that the node is unreachable and tries alternate routes to complete the call.
- If the remote node is a SIP application, SIP-OPTIONS message is used to check if the SIP application is alive or not. The Options method is used to measure the delay. Depending upon the thresholds reached, the SBC may determine that the SIP application is unreachable and an alternate route is attempted to complete the call.

The Sonus SBC 1000/2000 can be configured to reroute incoming calls to a PSTN or mobile network in case of failure of the IP networks. The IT manager can configure up to thousands of alternate routes on a single SBC to provide a high degree of business continuity for the enterprise.
PROVIDING RELIABLE BRANCH OFFICE SOLUTION FOR MICROSOFT LYNC DEPLOYMENTS

Survivability
A centralized call processing model saves costs, reduces complexity and increases management flexibility. However, the unintended consequence of the centralized model is reduced service reliability. Since voice traffic is carried through the data network, branch offices will remain isolated when the data network goes down. An enterprise-grade SBC solution should ensure business continuity by restoring basic voice services at the branch office when the system failure occurs.

The Sonus SBC series supports Survivable Branch Appliance (SBA) for Microsoft Lync. Using the SBA, the branch office communications are always up and running even when the WAN network to HQ is down.

The Sonus SBC series can provide “Advanced call routing” functionality through integration of Active Directory/LDAP servers. IT managers can dynamically create routing decisions such that if the user is not reachable on their Microsoft Lync client, then the call routing decisions can be configured to reach their mobile phone, home phone or a SIP/Wi-Fi phone registered with the SBC (see Figure 2). Provisioning alternate routes is simple and easy as most administrators already know how to use the Active Directory databases. The Sonus SBC maintains alternate routing numbers in the cache locally. Maintaining local cache is especially useful in cases where the IP network is down and it is not possible to reach the Active Directory server at the headquarters.

CONCLUSION
As telephony networks are consolidated, organizations need a mature solution that provides highly resilient architecture for their unified communications deployments. The Sonus SBC 1000 and SBC 2000 provide a highly available and secure solution which increases voice service reliability and improves business continuity both at the headquarters and at the branch offices.

About Sonus Networks
Sonus is a leader in IP networking with proven expertise in delivering secure, reliable and scalable next-generation infrastructure and subscriber solutions. With customers in over 50 countries across the globe and over a decade of experience in transforming networks to IP, Sonus has enabled service providers and enterprises to capture and retain users and generate significant ROI. Sonus products include session border controllers, policy/routing servers, subscriber feature servers and media and signaling gateways. Sonus products are supported by a global services team with experience in design, deployment and maintenance of some of the world’s largest and most complex IP networks. For more information, call 1-855-GO-SONUS

North American
Headquarters
4 Technology Park Drive
Westford, MA 01886
U.S.A.
Tel: +1-978-614-8100

APAC
Headquarters
1 Fullerton Road #02-01
One Fullerton
Singapore 049213
Singapore
Tel: +65 6832 5589

EMEA
Headquarters
56 Kingston Road
Staines, Middlesex TW18 4NL
United Kingdom
Tel: +44-0-17-8422-5750

CALA
Headquarters
Mexico City, Campos Eliseos Polanco
Andrés Bello 10, Pisos 6 y 7, Torre Forum
Col. Chapultepec Morales,
Ciudad de México
Mexico City, 11560 Mexico
Tel: +52 55 36010600

To learn more, call your Sonus sales representative or visit us online at www.sonus.net

The content in this document is for informational purposes only and is subject to change by Sonus Networks without notice. While reasonable efforts have been made in the preparation of this publication to assure its accuracy, Sonus Networks assumes no liability resulting from technical or editorial errors or omissions, or for any damages resulting from the use of this information. Unless specifically included in a written agreement with Sonus Networks, Sonus Networks has no obligation to develop or deliver any future release or upgrade or any feature, enhancement or function.

Copyright © 2012 Sonus Networks, Inc. All rights reserved. Sonus is a registered trademark of Sonus Networks, Inc. All other trademarks, service marks, registered trademarks or registered service marks may be the property of their respective owners.

SON-WP-002 08/12