Sonus Networks Cloud Link
Performance and Security Assessment

DR161118F

February 2017

Miercom

www.Miercom.com

Contents

1.0 Executive Summary

Sonus Networks, Inc. engaged Miercom to conduct independent performance and security testing of the Sonus Cloud Link for Microsoft® Cloud Connector Edition (CCE) appliance, based on the SBC 1000 session border controller with an upgraded embedded Applications Solutions Module (ASM). With the upgraded ASM hosting the Microsoft Skype for Business CCE software, the Sonus Cloud Link solution provides flexible local telephony service provider access for customers transitioning their VoIP services to the Microsoft Office 365 Cloud PBX.

Sonus Cloud Link testing focused on both the SBC 1000 and the embedded ASM housing the CCE software. The SBC was tested for performance in terms of connectivity, call handling and ability to sustain operation amid a broad spectrum of malicious attacks. The ASM with the CCE was tested for its ability to handle, route and load balance Skype for Business calls.

Key Findings and Observations:

- Sonus Cloud Link integrates new communications technologies (SIP, Skype for Business) with legacy systems, including TDM and analog telephony.
- The SBC 1000 maintains up to 192 concurrent SIP calls, including encrypted Secure RTP (SRTP) media streams. The SBC 1000 also supports 146 media sessions with G.711↔G.729 transcoding.
- With the updated Application Solution Module (ASM), up to 500+ Skype for Business calls can be simultaneously sustained using the Sonus Cloud Link solution.
- Sonus Cloud Link successfully fends off malicious DoS and protocol-fuzzing attacks, on both its private and public interfaces.
- The user interface is intuitive for management and for setting Call Administration Control (CAC) and Access Control Limits (ACL).
- The Sonus system readily deploys with Microsoft Skype for Business, by integrating Microsoft Cloud Connector Edition (CCE) with the ASM.
- The CCE Configuration Wizard setup takes one hour versus a multiple-hour manual setup effort.

The Sonus Cloud Link based on the SBC 1000 has now been awarded Miercom Performance Verified Certification, in addition to the previous Miercom certification on the Sonus SBC Core portfolio (Sonus SBC 5110, SBC 5210, SBC 7000, and SBC SWe).

Based on the results of our testing, we proudly award the Miercom Performance Verified Certification to the Sonus SBC 1000 and Sonus Cloud Link solutions.

Robert Smithers

CEO

Miercom

2.0 About the Product Tested

The need for both IP telephony and video conferencing is growing rapidly. Microsoft Skype for Business has emerged as a premier offering that gives enterprises calling, conferencing, video, audio and sharing capabilities. However, connecting an enterprise's current telephony system and carrier services with a Microsoft Office 365-based environment – whether on premises or cloud-based – can be challenging. What's more, many enterprises have long-term service provider contracts that can be costly to terminate.

To address this, Sonus Networks offers Sonus Cloud Link, which integrates Microsoft Skype for Business Cloud Connector Edition (CCE) software with its popular Sonus edge session border controllers – the SBC 1000 and SBC 2000.

Version 6.1.0.457 of the Sonus Cloud Link based on the SBC 1000 platform was tested. As noted, the SBC 1000 can be ordered to include Microsoft's CCE software; this combined feature set is labeled the Sonus Cloud Link based on the SBC 1000 platform. The Cloud Link's focus is to bridge alternate cloud access services to traditional telephony equipment.

The Sonus Cloud Link based on the SBC 1000 platform houses two processing units: the SBC 1000 CPU to handle SBC calls and the Application Solution Module (ASM) for managing activities involving the CCE software. The ASM is an embedded single board computer based on an Intel® Xeon® Processor ("Broadwell" family) featuring 8 cores, 16 threads operating at 1.7 GHz. The ASM also includes 32 GB of DDR4 ECC RAM and 512 GB of SSD storage. The ASM supports the operation of CCE-related virtual servers (Microsoft Edge and Mediation servers), which handle media processing, and come pre-configured so the customer is not required to set up this module during deployment. The Sonus Cloud Link also employs Call Admission Control (CAC), which provides call rate limiting and control for blocking malicious attacks.

Sonus Cloud Link for Microsoft Cloud Connector Edition – all together based on the Sonus SBC 1000 platform

3.0 How We Did It

Miercom and Sonus jointly developed the test plan, designed to assess both the call load handling over this bridge, and the ability of the Sonus Cloud Link to repel and continue working while under the most threatening attacks today.

Performance wise, the Sonus Cloud Link was assessed using a call and registration generator, simulating a real-world business telephony environment. Afterwards a suite of malicious attacks were launched against the system to observe the effect on loaded performance. We also verified the effectiveness of call admission control and the integrated ASM, attesting to the overall value of the Sonus Cloud Link solution.

Security tests involved running typical and maximum load scenarios while under malicious denial-of-service (DoS) and protocol-fuzzing attacks.

All test scenarios were recorded for replay and subsequent analysis. This can yield improved remediation and mitigation techniques.

Resource usage, the percent of CPU and memory utilized, for each test was also noted. Processing usage was observed for either the SBC 1000 or the ASM, depending on the test. For tests involving call-handling only, the SBC 1000 CPU was recorded, and the CPU of the ASM was recorded for tests involving the CCE for Microsoft Skype for Business calls.

3.1 Test Tools

An assortment of test tools was necessarily applied in this testing, given the scope of the testing. These are pictured and described below.

Source: Miercom February 2017

Device	Purpose	Version
Spirent Abacus	Call generator	Digital: 12HX9 Analog: 11JEM
Tektronix Spectra2	Call generator	8.5.0.R.1
Ixia BreakingPoint	Malicious Attack generator	3.5.0
Spirent Studio Security (Mu-8000)	Malicious Attack generator	6.5.2.r48322
Microsoft Skype for Business Cloud Connector Edition (CCE)	Provides a cloud Link for online Office 365 to an existing PBX or telephony service-provider gateway	1.4.1

Spirent Studio Security is a vulnerability-assessment and attack-generation system loaded on a Spirent Mu-8000 appliance. The package produces and launches protocol-mutation, DoS and other malicious-attack files. The Mu analyzer is used for service-assurance testing: determining reliability, availability and security of IP products, applications and services. Protocol-mutation attacks incorporate deviations from the expected operation of stateful protocols. Secure and robust systems should handle mutated-protocol packets by dropping them. However, a system with protocol-implementation flaws would respond abnormally, revealing an attack vector. The Spirent Mu system also recreates many published vulnerabilities and external attacks using real-world test cases and custom scripts. The analyzer provides complete data and actionable reports on any faults found to help remediate software flaws.

Ixia BreakingPoint can simulate over 200 applications and more than 35,000 live security attacks. It is capable of recreating complex simulations to test the throughput of network security appliances, which helps identify bottlenecks or security inefficiencies.

EXFO is a call generator for delivering SIP calls over IP. The system can perform registration, call signaling and set-up tasks over secure, encrypted Transport Layer Security (TLS) connections or regular, non-encrypted SIP/UDP connections.

Savvius Omnipeek captures network traffic and creates packet files for replay. Its statistics help monitor changes in real-time. By first baselining normal activity, changes that occur during the tests can be readily observed to analyze performance problems.

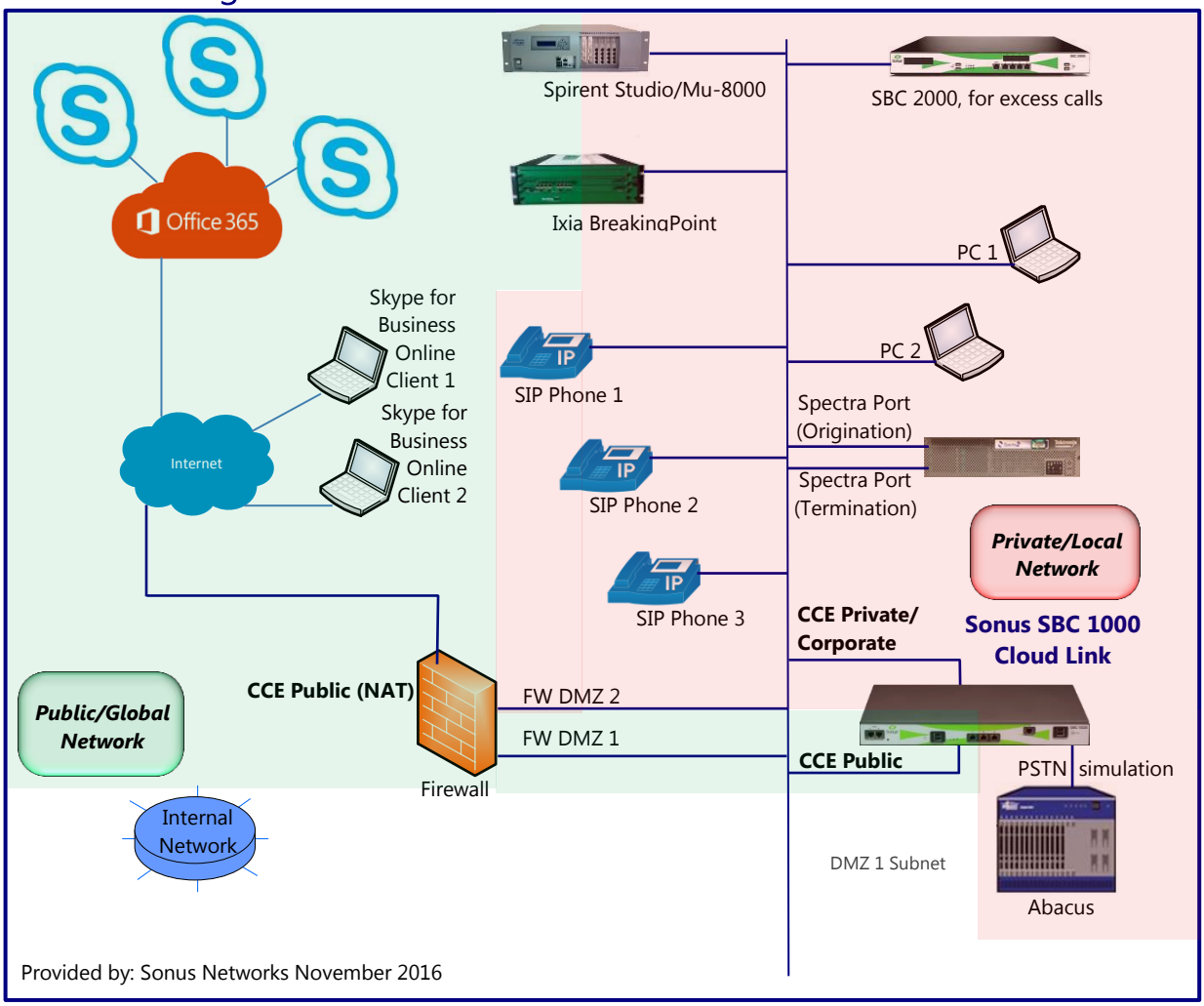
Touchstone Technologies WinSIP is a high-volume SIP call generator used for evaluating performance, functionality and the mean opinion score (MOS) quality of VoIP service.

Tektronix Spectra2 generates and maintains up to 1 million concurrent SIP-signaling calls, with or without media, and provides an easy to use test suite, with customizable scripts. A real-time display gives excellent visibility of all tests. It is designed for analyzing VoIP and SIP and supports over a dozen SIP protocols.

Spirent Abacus generates and analyzes analog/digital voice, video and VoIP calls to test performance, scalability and quality for analog and digital communications. It is capable of simulating IP telephones and gateways.

Nessus is a widely used vulnerability scanner used by penetration testers and other security consultants. Locating vulnerabilities helps to remediate these weak areas immediately.

3.2 Test Bed Diagram



Performance testing assessed several metrics, including completed calls and CPU utilization under different call loads.

Later, security testing monitored completed calls and CPU use for comparison at:

- The Private Sonus Cloud Link/CCE gateway
- The Public Sonus Cloud Link/CCE gateway
- Between the Sonus Cloud Link/CCE Public and Private gateways

A secondary Sonus SBC 2000 session border controller was used to handle the rollover of calls when the load surpassed the Sonus SBC 1000 limitation of 192 concurrent calls. Some tests employed up to 500 concurrent calls, and the SBC 2000 would pick up the balance beyond 192 calls. The SBC 2000 can handle 600+ concurrent calls. Even under a heavy load, all calls would still go through the Sonus Cloud Link– appliance and then be rerouted if necessary to the other SBC.

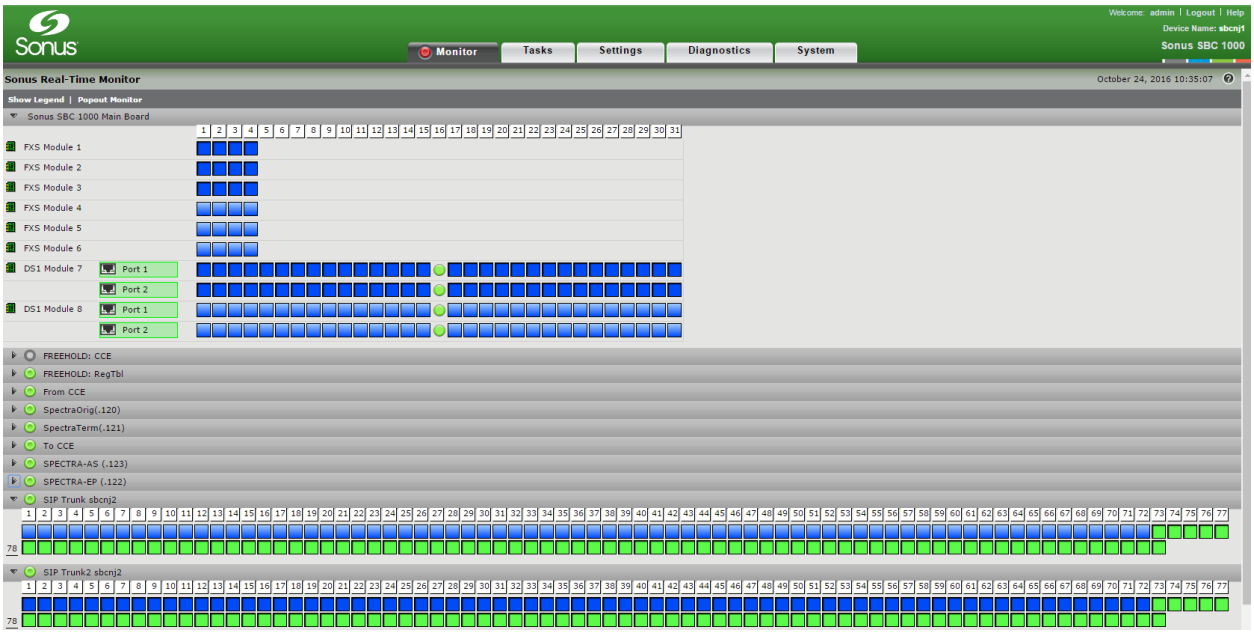
3.3 Set Up

The Sonus Cloud Link based on the SBC 1000 runs Microsoft Skype for Business CCE software, but still needs to work in conjunction with the Microsoft Office 365 Cloud PBX. Since cloud access may not always be available, Microsoft CCE software can be used to connect business telephony to the cloud, without the need to change service providers, while maintaining good performance and security.

Although the test bed setup differed somewhat from a traditional VoIP deployment, it was necessary that all VoIP capabilities be supported. Performance was verified using the Spectra and Abacus test tools, which generated different call loads to assess any dropped connections and CPU usage.

The Ixia BreakingPoint and Spirent Mu-8000 systems assessed how well the SBC 1000 system could mitigate threats while under call load. Using different test cases, we analyzed the capabilities of the Sonus package, including the load-balancing Application Solution Module, which bridges the controller to Microsoft Skype for Business. The CPU usage of the Microsoft Edge and Mediation servers were noted. During the DoS and protocol fuzzing attacks, we observed that there was only a localized effect on the Edge Server. The Mediation server was unaffected.

Figure 1: SBC 1000 Cloud Link Real-Time Monitor



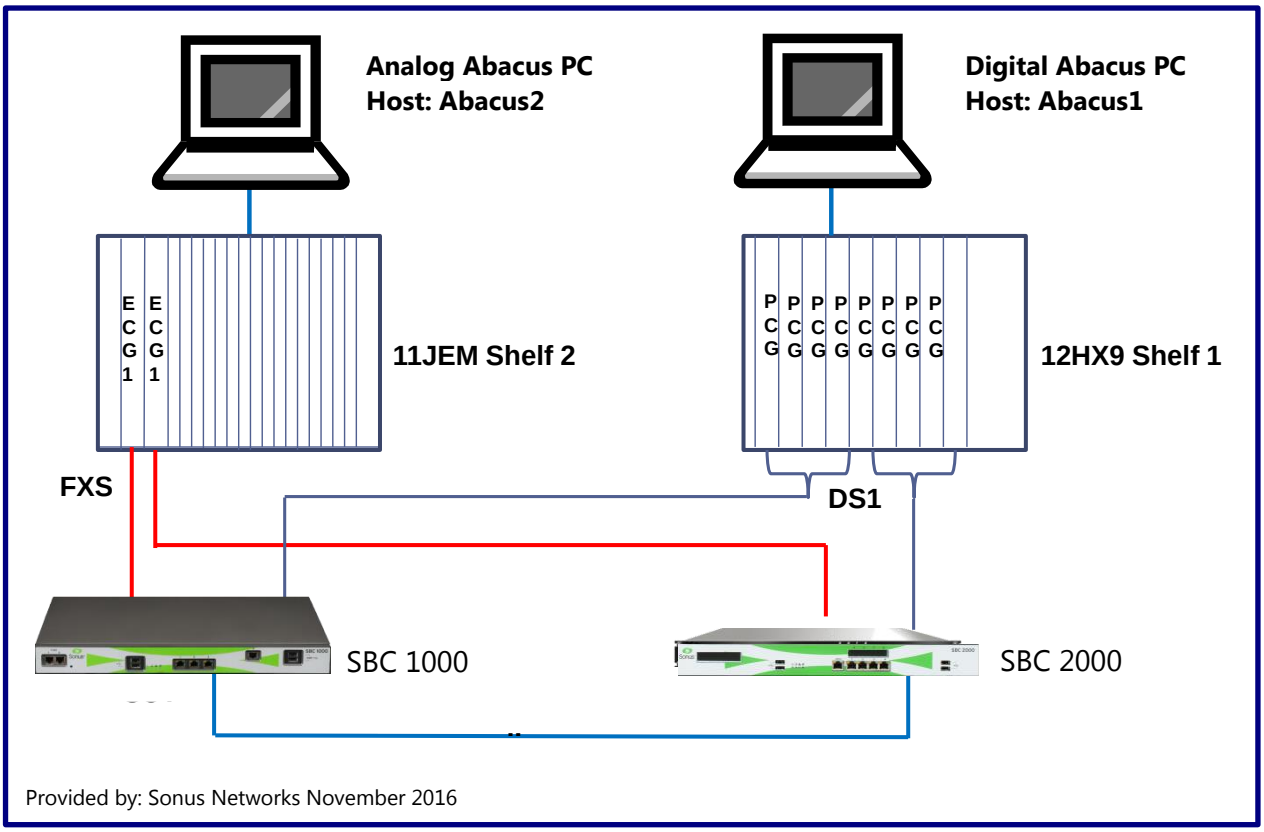
The Sonus Real-Time Monitor window of the SBC 1000, indicated which channels were used during testing. The SIP trunks located on the bottom show when calls are "C", collecting digits; "S", SIP trunking; "A", alerting or ringing.

4.0 Call Performance

The following sections detail the test-case scenarios, including call type, codec and translation of calls. For each call load, the registration rate, CCE performance and CAC abilities are noted. In some cases, the MOS is also calculated to gauge call quality.

4.1 TDM ↔ SIP G.711 Performance

A total of 192 concurrent calls, set up over a 400-second connect time, were generated by the Spectra and Abacus tools. The Abacus generated analog and digital calls at a 1 cps rate.



Bidirectional SIP trunks were used to route traffic to and from the two SBCs over IP. Call legs consisted of TLS version 1.2 encrypted SIP signaling associated with G.711 SRTP encrypted media.

Analog calls were placed at 1 cps with a 1-second delay for the first group and 15-second delay for the second group to allow the first set of originated calls to complete. All ports and calls were simultaneously active after 400 seconds. Digital calls were sent at 1 cps with a 30-second delay for the first group and 35-second delay for the second group to allow the analog calls to complete. After 400 seconds, all ports were simultaneously active. Both analog and digital calls passed successfully through the SBC 1000 and SBC 2000.

Table 1: TDM↔SIP G.711 Test Tool Call Flow Loads

Test Tool	Call Type (192 total)	Method
Spectra	48 SIP↔SIP calls	Generated SIP↔SIP calls at 3 cps
Abacus	60 ISDN E1↔SIP calls 60 SIP↔ISDN E1 calls	• 8 cards on the Abacus generated digital calls, each supporting an E1 port (30 calls) • 4 cards connect to the Sonus SBC 1000: 2 for originating calls; the other 2 for terminating calls • 4 cards connect to the SBC 2000: 2 for originating calls; the other 2 for terminating calls
	12 FXS↔SIP calls 12 SIP↔FXS	• 2 cards on the Abacus generated analog calls, each card has 24 ports • 1 card connected to the SBC 1000, with 12 ports originating calls to the SBC 2000 and 12 terminating calls from the SBC 2000 • 1 card is connected to the SBC2000, with 12 ports originating calls to the SBC 1000 and 12 ports terminating calls from the SBC 1000

Results

Table 2: TDM↔SIP G.711 Test Observations

Test	144 TDM↔SIP Calls; 48 SIP↔SIP G.711 calls
Metrics	Run for 400 seconds; TDM calls @ 1 cps, SIP calls @ 3 cps
Calls Dropped	0
CPU (%)	37%
Observations	Performed 3 iterations; no calls were dropped for any test run

4.2 SIP↔SIP Calls Testing Transport Layer Security (TLS) for Signaling and Secure RTP (SRTP) for Media

The Spectra tool was used to assess how well the SBC 1000 performed, in terms of resource usage, while encrypting/decrypting 192 SIP calls.

First we verified functionality by monitoring traffic with the Wireshark tool, tapping the SBC 1000/CCE Private link from the Spectra terminating side. We ran a single call, and then multiple calls, to capture traffic, to confirm that calls were successfully being made. Calls consisted of 192 G.711aμ (TCP for SIP signaling/RTP for media) to G.711a (TLS for SIP signaling/SRTP for media) at 3 cps.

Next we ran 192 calls – the maximum capacity handled by the Sonus SBC 1000.

Results

The SBC 1000 CPU houses three DSP complexes; each used only 60 percent of their CPU resources while running maximum call capacity. The SBC 1000 memory was impacted by the Web user interface and media, while the CPU was handled completely by the DSP modules.

Table 3: SIP↔SIP G.711 TLS/SRTP Test Observations

Test	192 SIP over TCP, G.711 RTP↔SIP over TLS, G.711 SRTP
Metrics	3 cps
Calls Dropped	0
Memory (% of 250 MB)	62%
SBC 1000 CPU (%)	60
MOS	4.14 (of 5)
Observations	Ample resources for each DSP, which handled most activity.

4.3 SIP↔SIP, with G.711↔G.729 Bidirectional Transcoding

SIP calls were generated using the Spectra tool. We looked for dropped calls and resource utilization used during these 146 calls, all transcoding between G.711 (TLS for SIP signaling/SRTP for media) and G.729 (TLS for SIP signaling/SRTP for media) vocoders.

We verified functionality using the same tapping configuration and call scheme as previous.

Then we ran a test of 146 calls to determine the CPU usage and Spectra's MOS assessment for this transcoding.

Results

Table 4: SIP↔SIP G.711↔G.729 Bidirectional Transcoding Observations

Test	146 SIP↔SIP Transcoded Calls
Metrics	3 cps, G.711↔G.729
Calls Dropped	0
CPU (%)	76%
MOS	G.711 calls: 4.11; G.729 calls: 3.61
Observations	CPU capacity was still available. Reduced MOS on G.729 is consistent with expectations for a compressed codec

4.4 Registration

Registrations and calls, generated by the Spectra tool, were made to show the CPU usage when 600 SIP endpoints registered at a rate of 5 registrations per second (rps), and then 192 G.711 SIP↔G.711 SIP calls with media were placed at 3 cps for 20 minutes.

After verifying proper call set-up, we registered two phone clients and 598 other registrations (generated by the Spectra tool) with the SBC 1000. A hard limit of 600 registrations was set within the SBC 1000, so that any excessive registrations (beyond 600) would be rejected.

Upon completion of registration, calls were made at 3 cps. While calls were active, the registrations were refreshed every five minutes.

Results

Table 5: Registration Test Observations for 600 Registrations

Test	600 Registrations
Metrics	600 registrations @ 5 rps
Calls Dropped	N/A
Core CPU (%)	5%
DSP CPU (%)	N/A
Observations	None

Table 6: Registration Test Observations for 600 Registrations with 192 SIP↔SIP Media Calls

Test	600 Registrations, with 192 SIP↔SIP calls with media
Metrics	G.711 SIP calls @ 3 cps; 20 minutes duration
Calls Dropped	0
Core CPU (%)	50%
DSP CPU (%)	65%
Observations	SBC 1000 CPU was still available; 115 channels per DSP supported

4.5 Cloud Connector Edition (CCE) Performance

The purpose of this test was to show how the Microsoft Skype for Business CCE, hosted within the Sonus SBC 1000 Cloud Link, handled 500 calls by load balancing between two SBCs:

- The Sonus Cloud Link solution based on the SBC 1000 platform;
- The second session border controller, an SBC 2000, used to handle overflow calls.

The Spectra tool generated 500 SIP↔SIP calls with G.711 media, the most intense vocoder on the CCE mediation server. Calls were generated to both the SBC 1000 and Office 365, routing through the CCE. Calls going out to the Office 365 Cloud looped back in through the same address from the CCE Public Interface. The CCE sent calls to the DUT until saturated (192 calls), then to the overflow SBC 2000. How the CCE decides is based on Microsoft settings.

Since the SBC 1000 can handle a maximum of 192 calls, the SBC 2000 handled the other 308 calls. Load balancing was expected to be managed by the CCE. Resource usage of both the DSPs and the ASM (CCE handling) was observed under this call load scenario.

To verify call path, packet captures were recorded of two PC clients, with MS Skype for Business placing a call to a registered phone through the SBC 1000 and then to the Cloud. The CCE handled the calls, and load balanced by using the signaling group, made up of the SBC 1000 to the phone, and the CCE to the SBC 2000 SIP trunk through the SBC 1000 back to the phone. We verified calls were completed by tapping the SBC 1000/CCE Private interface.

Results

A total of 500 calls, through the SBC 1000 and the SBC 2000, were managed by the CCE Mediation Server for calls from the laptop PC-2 to SIP Phone-1 resulting in the following:

Table 7: CCE Performance Test Observations for 500 Calls with CAC Enabled

Test	CCE Performance
Metrics	500 Calls; CAC Enabled
Calls Dropped	0
SBC 1000 CPU (%)	50%
CCE CPU (%)	70%
Observations	None

4.6 Call Admission Control (CAC) Performance

The purpose of this test was to verify the proper operation of call-admission control: to prevent the SBC 1000 from CPU overload when overwhelmed with a high number of calls made during these conditions.

First, we applied a low call rate of 2 cps for 180 seconds. Next, we increased the call rate, applied a limit and ran for 120 seconds. Lastly, we applied a low call rate, applied rate limiting and ran for 300 seconds.

Results

Table 8: CAC Performance for SIP↔SIP Calls

Test A, B, C	**Test A:** Low Call Rate	**Test B:** High Call Rate, with Rate Limiting	**Test C:** Low Call Rate, with Rate Limiting
Metrics	2 cps, for 180 seconds	12 cps, for 120 seconds	2 cps, for 300 seconds
Calls Rejected	0	Yes; Unestablished call attempts were rejected when the system was subjected to an excessive call rate.	Decrease in unestablished call attempts when the system was subjected to an excessive call rate.
SBC 1000 CPU (%)	40%	75%	40%
Observations	Steady state at 110 calls	System triggered overload alarm as expected. Rate Limiting worked as designed and intended.	Steady state at 110 calls; unestablished call attempts decreased and were no longer being rejected.

5.0 Security: Impact of Malicious and Malformed Traffic

Malicious attacks were conducted using Spirent, Ixia and EXFO tools. Tests such as Rogue RTP, Denial-of-Service, protocol fuzzing and mutations, invites from unconfirmed sources (zones) and spoofed IPs, TCP/UDP flooding and fragmented packets are used to evaluate security effectiveness while the SBC 1000 with Cloud Link solution is deployed.

Spirent Mu-8000 version 6.5.2.r48322 was deployed to run the following attacks:

Denial of Service (DoS)	Millions of flood attacks per second can be achieved and sent through the Sonus Cloud Link. These attacks disrupt access by consuming network or service resources. Overwhelming the network with new requests and holding them open, prevents new connections and causes the network to choke. We observe the following types of DoS attacks: • DNS Reflection • UDP Flood • ICMP Flood
Protocol Mutation and Fuzzing	Implementing mutations is an effective way to identify vulnerabilities. Examples of protocol-mutation attacks use ARP, DNS, ICMP, IPv4, SIP, TCP, RTP, UDP protocols. These types of attacks are generated while the DUT is under a traffic load to further expose otherwise undetectable weak spots. We observe the system under the following mutation attacks: • UDP Mutation • TCP Mutation

Test Networks

Private Network The private side of the test network consisted of the local, corporate network. When Skype for Business calls were made, they were routed through the demilitarized zone (DMZ) to the public network. This network was not reachable from the public network and less prone to intrusion or attack.

Public Network The public side of the test network was made of the public-facing SBC 1000/CCE, Skype for Business, external clients and public servers. A DMZ was created in the firewall to route Skype for Business calls to the private/corporate network through the CCE Edge Server, using a private network address. A class C private network was created to translate public to private address translation. The test assumed the Edge server's IP address as public, as it was public-facing and responsible for routing Skype for Business calls to the private/corporate network.

Preliminary Testing

During all BreakingPoint tests, 192 SIP↔SIP calls were initiated and kept connected for 20 minutes. The attacks were performed after all calls were established, and run until the SBC 1000 reached a steady state. After each test, the calls were terminated successfully unless otherwise stated.

CPU Analysis

SBC 1000 CPU The SBC CPU is responsible for handling all session and call processing.

CCE CPU The CCE CPU is dedicated to the CCE processing only and is comprised of the virtual Edge Server and virtual Mediation Server. Any use of the public network with Microsoft Skype for Business requires CCE services and its processing power. Resource usage was recorded if applicable.

5.1 Private to Private Testing

As in preliminary testing, 192 SIP↔SIP calls were generated for these tests. The purpose was to show the effect of security rules on the behavior of the SBC 1000 while under attack.

This configuration was performed with the following addresses:

Private Interface 1	Private Interface 2
Ixia BreakingPoint	SBC 1000/CCE Private Gateway (SIP/PSTN Gateway)

The Ixia BreakingPoint generated attacks from its private-facing port on the local network to the private side of the SBC 1000 gateway.

The maximum bandwidth for DoS testing was set to 500 Mbps, whereas the overall CCE Gateway capacity was 1 Gbps. 192 calls were running during the test, and no new calls were made. The Spirent Mu-8000 was used for protocol fuzzing and deployed using the same configuration as the Ixia BreakingPoint. Miercom was impressed with the Security Hardening checklist that Sonus provides for the SBC 1000 against malicious network-based attacks, which can be found at https://support.sonus.net/display/UXDOC61/SBC+Edge+Security+Hardening+Checklist .

Results

The SBC 1000 protected against all DoS and protocol mutation attacks by employing policies which only passed specific traffic protocols through its gateway. Customers have the freedom to tailor IP traffic from the GUI on a case by case basis, depending on their needs.

Table 9: Private/Corporate Network Attack Tests

Test	Metrics	Calls Dropped	SBC 1000 CPU (%)
UDP Flood to Port 5060	500Mbps	0	60%
ICMP Flood to CCE Gateway	500Mbps	0	<5%
DNS Reflection to Port 53	500Mbps	0	10%
TCP GET and POST	500Mbps	0	60%
DNS Flood	500Mbps	0	65%
TCP Flood to Port 8080	500Mbps	0	70%
TCP Flood to Port 8080	500Mbps	0	<10%
UDP Mutation	100,000pps	0	<5%
SSL/TLS Mutation	100,000pps	0	<5%
TCP Mutation	100,000pps	0	<5%
SIP Fuzzing	100,000pps	0	<5%

5.2 Public to Public Testing

This configuration was tested using the addresses below:

Public Interface 1	Public Interface 2
Ixia BreakingPoint	SBC 1000/CCE Public Gateway (MS Skype for Business Cloud Connector Gateway)

The Ixia BreakingPoint generated attacks from its ports on the public side of the network to the public-facing Skype for Business CCE gateway.

The SBC 1000 and SBC 2000 were deployed together to handle a 500-call-load distribution. The SBC 1000 handles the first 192 calls, and it will then reroute calls to the SBC2000. Approximately 10 calls were dropped before the rerouting started.

Results

The CCE Public Interface contains various virtual machines to handle traffic. Its mediation server handles data transfer for active calls, and the Microsoft Edge server handles incoming traffic. All Ixia BreakingPoint tests had a local-only impact on the Edge server and no effect on the mediation server. All CPU utilizations shown are the consolidated percent of maximum Edge server and Mediation server CPU.

The purpose of this test was to see how traffic is managed by the ASM. The BreakingPoint tool was used to send malicious traffic to the CCE Public Gateway. 516 Skype for Business calls were first established before the attacks; no new Skype for Business calls were subsequently made. The Spirent Mu-8000 was used for protocol fuzzing and deployed with the same configuration as the BreakingPoint.

Table 10: Public Network Attack Tests

Test (Attack)	Metrics	Consolidated CCE CPU (%)
UDP Flood	100Mbps	75%
ICMP Flood	100Mbps	75%
DNS Reflection	100Mbps	75%
UDP Mutation	100Mbps	75%
TCP DoS	100,000pps	75%

5.3 Public to Private Testing

As in Public to Public testing, 500 calls were distributed between the SBC 1000 and SBC 2000. This configuration was performed using the following addresses:

Public Interface	Private Interface
Ixia BreakingPoint	Ixia BreakingPoint
SBC 1000/CCE Public Gateway (MS Skype for Business Cloud Connector Gateway)	SBC 1000/CCE Private Gateway (SIP/PSTN Gateway)

The Ixia BreakingPoint generated attacks from its public-facing side of the network to the public-facing Skype for Business CCE gateway. These attacks propagate through to the private gateway of the CCE and back to the BreakingPoint's private-side of the network.

Results

The BreakingPoint tests had a local-only impact on the Edge server, with little to no effect on the Mediation server. All CPU utilizations shown are the consolidated percent of maximum Edge server and Mediation server CPU.

The purpose of this test was to see how traffic is managed by the ASM. The BreakingPoint sent malicious traffic through the Public and Private gateways of the CCE. The SBC 1000 was observed for any dropped calls. For each test, no calls were dropped.

Table 11: Public and Private/Corporate Attack Tests

Test	Security	Metrics	Calls Dropped	Consolidated CCE CPU (%)
TCP SYN Flood (Public Ixia BP to Private Ixia BP)	None	516 Skype for Business calls @ 100Mbps	0	30
UDP Flood	None	516 Skype for Business calls @ 100Mbps	0	64
DNS Reflection	Port 53 blocked	516 Skype for Business calls @ 100Mbps	0	61
TCP SYN Flood	Port 53 blocked	516 Skype for Business calls @ 100Mbps	0	42

6.0 Ease of Use

The Sonus Cloud Link solution based on the SBC 1000 readily deploys with Microsoft Skype for Business, due in large part to the integration of Microsoft CCE on the ASM.

Integrating several disparate products into a cohesive network requires time and attention to detail. Microsoft CCE supports legacy on-premises PBX systems and multiple virtual machines. The setup of CCE, by itself, is not necessarily intuitive, however – the drawback of a free software connector. The Sonus Cloud Link features a CCE Setup Wizard of its own, which can, in our estimation, reduce setup time, and therefore staff cost, by hours.

Multiple platforms – new and legacy-technology systems – can be integrated in the network environment using the Sonus CCE Setup Wizard. This makes the deployment much more intuitive and considerably quicker than the traditional Microsoft method.

6.1 CCE Configuration Wizard

The CCE Wizard was extremely simple to use and effectively reduces hours of both time and trial-and-error of manual configuration steps.

To introduce the Skype for Business CCE software, we must do two things – setup the CCE in the SBC Edge WebUI and then executing CCE specific Microsoft commands.

The first part requires a login to the SBC Edge WebUI, and configuration, or verification, of the network settings in the ASM.

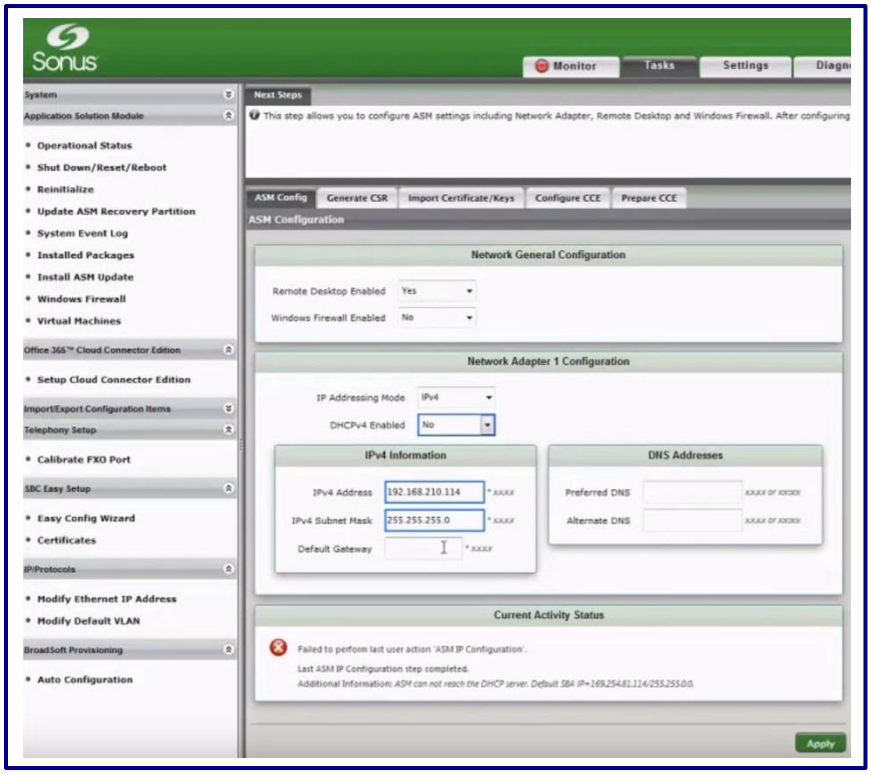
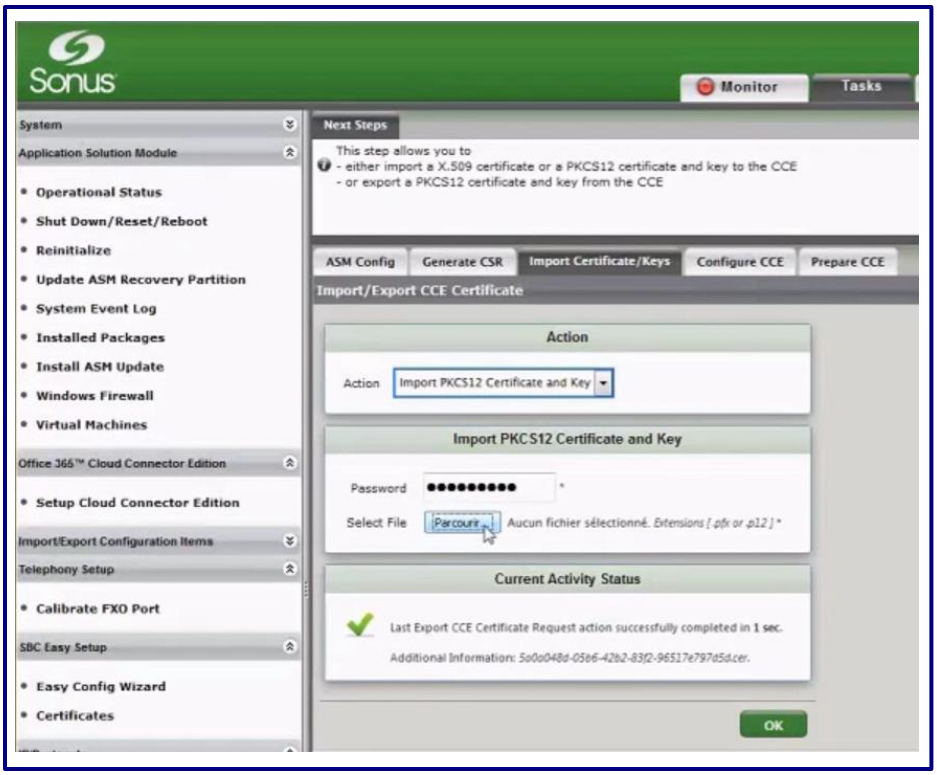


Figure 2: CCE Configuration Wizard – ASM Configuration



Next, a third-party signed, public certificate must be created and imported. The length of time to create this depends entirely on the third-party used and can range from five minutes or several hours.

Figure 3: CCE Configuration Wizard - Certificate Request

Once imported, the CCE can be connected to the network by declaring where it is to be installed. How many CCE and SBC are involved can also be declared here for high availability reasons. This is based on the customer's needs.

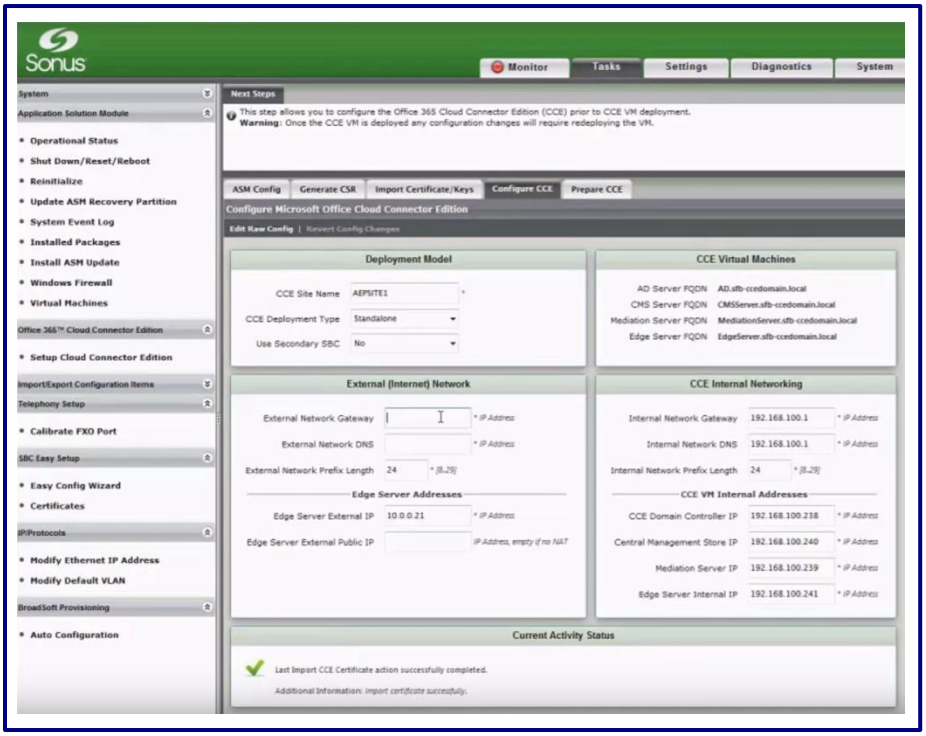


Figure 4: CCE Configuration Wizard - Configure CCE

Since the CCE faces both public and local networks, the IPs of its virtual machines must be assigned. It is important that, while this section is small, it is thoroughly and correctly completed. There is no feedback for misconfiguration within the CCE setup process.

Lastly, the Microsoft Powershell tasks on the ASM can be executed using CCE commands. This takes approximately one hour to complete.

After this is completed, the equipment should be configured to talk to the sever blade based on the deployment scheme desired by the customer (e.g. PSTN), and a name can be assigned.

To review, during the course of an hour the CCE builds four virtual machines, installs necessary software for all Microsoft Skype for Business tools, connects IPs and uses a signed, public certificate to ensure secured communication. The Microsoft Cloud will then assign a code to the customer for this newly created CCE.

The main benefit of this simple wizard: it takes about an hour to complete – replacing the manual process of setting up CCE on a server, which can take many hours for even an expert-level IT administrator. Keep in mind that a complex manual setup could also encounter multiple deployments resulting from human error. The CCE configuration is seamless and can have Skype for Business working on an existing network without any hassle or overhead of an alternative approach.

7.0 About "Miercom Performance Verified" Testing

This report was sponsored by Sonus Networks. The data was obtained completely and independently by Miercom engineers and lab-test staff as part of our Performance Verified assessment. Testing such as this is based on a methodology that is jointly co-developed with the sponsoring vendor. The test cases are designed to focus on specific claims of the sponsoring vendor, and either validate or repudiate those claims. The results are presented in a report such as this one, independently published by Miercom.

8.0 About Miercom

Miercom has published hundreds of network-product-comparison analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the Performance Verified program, the industry's most thorough and trusted assessment for product usability and performance.

9.0 Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.