Miercom

Lab Testing Summary Report

May 2012

Report SR120426

Product Category:

Session Border Controller

Vendor Tested:

Sonus

Products Tested:

SBC 5100

Miercom Performance Verified™

Key findings and conclusions:

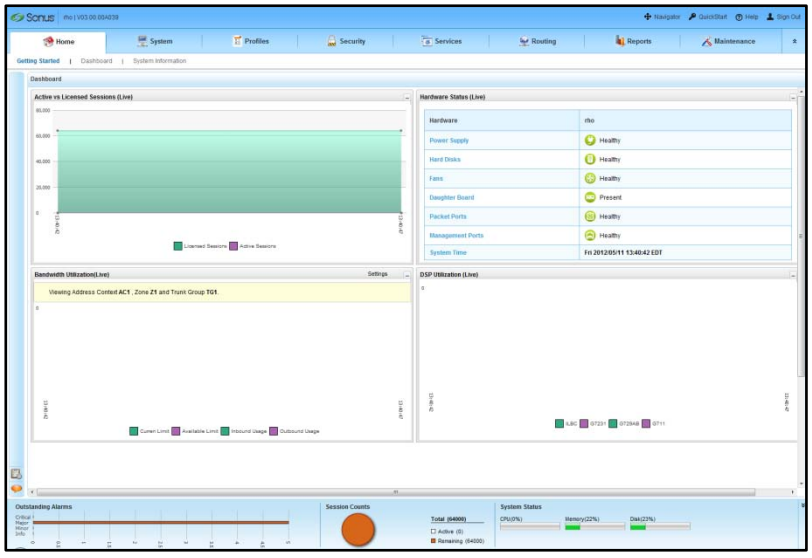
- **Sonus SBC 5100 capacity and performance characteristics enable it to be deployed as an access, peering or enterprise SBC**
- **Applications requiring high call loads easily handled - a peak of 570 cps and 5,493 concurrent calls when subjected to 4x engineered call load**
- **Sonus SBC 5100 protects against DoS attacks by processing calls from multiple peers during and following call flood attack**
- **SIP sessions - 100,000 IADs were registered in 4 minutes 12 seconds without dropping calls while maintaining low CPU and memory usage**
- **Sonus SBC 5100 processes 3,000 concurrent sessions while registering 100,000 endpoints with zero errors and low resource usage**

Sonus Networks submitted their SBC 5100 Session Border Controller to Miercom for an evaluation of performance and resiliency. The SBC 5100 is intended for enterprise and service provider deployments of 250 to 10,000 users.

The Sonus SBC 5100 includes a new UI and new Access Service Provider features. Some examples of new functions that are embedded in the new UI are intuitive SIP message manipulation for interoperability, and easy wizards for application installations/upgrades and OS upgrades.

The device supports SIP trunking, peering and access configurations. Baseline peering and access performance of the SBC 5100 was obtained for normal engineered call loads and overload conditions. In other tests, the ability of the device to easily maintain processing of the baseline call load while deflecting various attacks from invalid peers was examined.

Figure 1: Sonus SBC Embedded Management Interface



Source: Miercom, May 2012

Sonus SBC 5100 Management Interface monitors and reports vital system performance statistics such as CPU, disk, port and memory usage.

In the access configuration, the device was subjected to a real-world registration avalanche simulating a metro area outage. All devices attempt to re-register simultaneously following the outage, while concurrently continuing to process calls. The maximum registration and call capacity of the device in the access configuration were then verified. Additionally, a review of the newly enhanced web-based Element Management Application (EMA) demonstrated enhanced ease-of-use and functionality. See *Figure 1*.

Peering with Overload

With a performance baseline established, a 1x engineered call traffic load of 150 cps with a call hold time of 33 seconds was sent, resulting in 4,953 concurrent calls. Using a G.729 voice codec, call quality scores were recorded with an R-Factor of 81.7 and MOS of 4.08. Latency was low at 9.6 ms. The SBC displayed low CPU resource usage of 39% and 18% memory usage.

In addition, we wanted to see how the SBC handled an overload call condition. The call load was increased by 4x the 600 cps value. The SBC 5100 processed 5,493 concurrent calls. System resource usage was 95% for the CPU and 22% for memory. Recovery of the system back to the original load returned the CPU to 40%. The memory is not immediately reclaimed following the overload, and remained at 22%, but was reclaimed shortly thereafter.

Peering with Attack

With a baseline load established in peering mode, attack traffic was directed at the SBC to determine the effect on performance and resources. The attack sent a 3,000 cps call flood from invalid peers. The CAC policer was set to a rate limit of 50 cps before auditing traffic. Appropriately, during the attack, we observed a call rate of 194 cps, with 4,952 concurrent active calls. System resources were not strained, with 39% of CPU resources and 18% memory usage recorded. MOS scores remained at 4.08 and R-Factor remained at 81.7, with 10.5 ms latency. The quality of legitimate calls in progress was not impacted by the increased rate of malicious call traffic floods.

DoS attack floods were also tested with multiple peers. In this scenario, the 150 cps call load was evenly distributed among ten peers, for 15 cps each, with a 33 second call hold time. An attack flood of 3,000 call requests per second was sent to the SBC on the same port, for a total call load of 3,150 cps. The CAC policer was set to rate limit the traffic to 50 cps before auditing the stream. Again call processing performance was unaffected during the attack, and system resource usage increased only marginally. The total number of concurrent calls remained at the baseline level of 4,953, and the call rate increased by 50 cps to 194 cps. System resource usage increased slightly to 39.5% for the CPU and 18% for memory. Call media quality remained high throughout the attack. Following the attack, CPU usage returned to the pre-attack level of 37%. Memory usage remained at 18%.

Registration with NATTED IAD

The performance of the SBC 5100 was evaluated for access configuration, using the Navtel SIP PS application as a Proxy server and Registrar. The goal was to test the SBC performance in re-registering a mix of IADs of NATTED and non-NATTED types. This test configuration simulated a network provider's outage. During the outage, multiple endpoints attempt to re-register simultaneously, consuming SBC system resources.

There were 100,000 IADS in the test, with 75% non-NATTED. A call load of 25 cps with a call hold time of 200 seconds was directed at the SBC, for a maximum concurrent call rate of 5,000 calls. The registration threshold was set to 400 initial registrations per second, and 2,600 registration refresh per second. The baseline load on system resources prior to starting the registration avalanche was low, with only 7% of the CPU being used, and 17% memory usage. The SBC registered all 100,000 IADS in 4 minutes 12 seconds while maintaining call processing. During the avalanche, CPU usage peaked to 40% with 25% memory usage.

Baseline Load with Attacks

A baseline load with attack traffic was directed at the SBC 5100. 100,000 non-NATTED IADs were registered to the SBC. Registration threshold was set to 400 rps (registrations per second) and call rate was 100 cps for a target concurrent session rate of 3,000. The attack traffic consisted of a call flood of 1,000 cps and a registration flood of 500 rps. The test ran for 30 minutes. With just the legitimate baseline traffic, the CPU resource utilization only peaked to 33% and 23% for memory usage. When the attack traffic was added, the call rate was 1,100 cps, concurrent sessions remained at 3,000, and resource utilization increased as the SBC 5100 discarded the malicious traffic. Usage for CPU was 56% and memory was 26%. Call quality remained unaffected. When the attacks subsided, both the call rate and the CPU utilization returned to pre-attack levels. The SBC demonstrated that it could easily control these types of attacks without impacting

legitimate call traffic, or unduly stressing system resources. See *Figure 2*.

Registration and Call Capacity

To verify the ability of the SBC 5100 to handle normal call and registration loads, a test was performed to register 25,000 NATTED and 75,000 non-NATTED IADs. A steady load of 50 cps was also sent to the SBC simultaneously. This test was run for 40 minutes, during which the call rate, peak registration rate, number of active concurrent calls, and system resources were monitored and recorded.

The SBC registered all 100,000 IADS at 100 rps with zero errors. Calls were sent at 50 cps and a call hold time of 60 seconds. The SBC processed 3,000 active concurrent sessions and simultaneously recorded a peak registration refresh rate of 2,460 rps. No alarms were recorded on the SBC, no errors were observed on the Navtel call generator, and CPU and memory usage during the test was 29% and 24%, respectively. The SBC 5100 successfully registered all IADs and completed all calls.

IPv4/IPv6 Transcoding

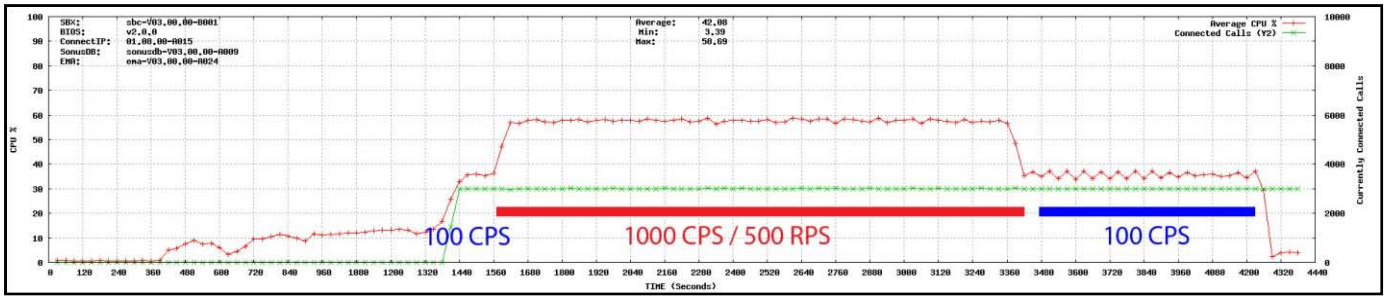
Transcoding is a necessary function for an SBC to resolve various incompatibilities between endpoints which could prevent the successful establishment of a media session between users. These incompatibilities can be caused by the use of dissimilar codecs or using different addressing schemes, such as IPv4 and IPv6. The SBC needs to perform this transcoding on the fly and at scale, while maintaining call quality. We evaluated the ability of the SBC 5100 to perform real-time transcoding for both ingress and egress streams to perform two conversions: from IPv4 to IPv6, and from G.711ulaw codec to G.729ab codec. We established a call rate of 150 cps with a call hold of 60 seconds. The SBC maintained 9,000 concurrent sessions, with a MOS of 4.09 and R-Factor of 81.8 for the G.729 encoding, and MOS of 4.39 and R-Factor of 92.5 for G.711ulaw encoding. We recorded a notification on the SBC that a high watermark threshold had been reached. Performance figures were measured and recorded again 30 minutes into the transcoding test. CPU usage was 42% and memory usage was 21%. The system was still processing 9,000 concurrent calls at 150 cps, with G.711ulaw MOS and R-Factor of 4.39 and 92.5, respectively, and G.729ab MOS and R-Factor of 4.09 and 81.8, respectively. We were impressed that all calls were processed using a 13 message SIP PRACK flow. This level of messaging is more detailed, CPU and memory intensive, adds to more processing overhead, and is a typical implementation in a customer network. During the ramp-down of the test, a low watermark threshold notification was recorded by the SBC 5100.

Bottom Line

The Sonus SBC 5100 maintained high levels of call processing rates with low system resource usage, and was resilient to several types of malicious attack traffic. CAC policing protected system resources and successfully rate-limited attacks from invalid endpoints. The SBC 5100 performed real-time transcoding to convert between IPv4 and IPv6 protocols, and G.711ulaw and G.729ab codecs for both ingress and egress traffic for 9,000 concurrent SIP sessions at a rate of 150 cps.

The SBC 5100 also performed very well in high load conditions, registering 100,000 NATTED and non-NATTED endpoints in 4 min 12 secs following a simulated network outage. It processed a peak of 570 cps and 5,493 concurrent calls when subjected to a 4x engineered load, without coming close to or exceeding the maximum CPU threshold level.

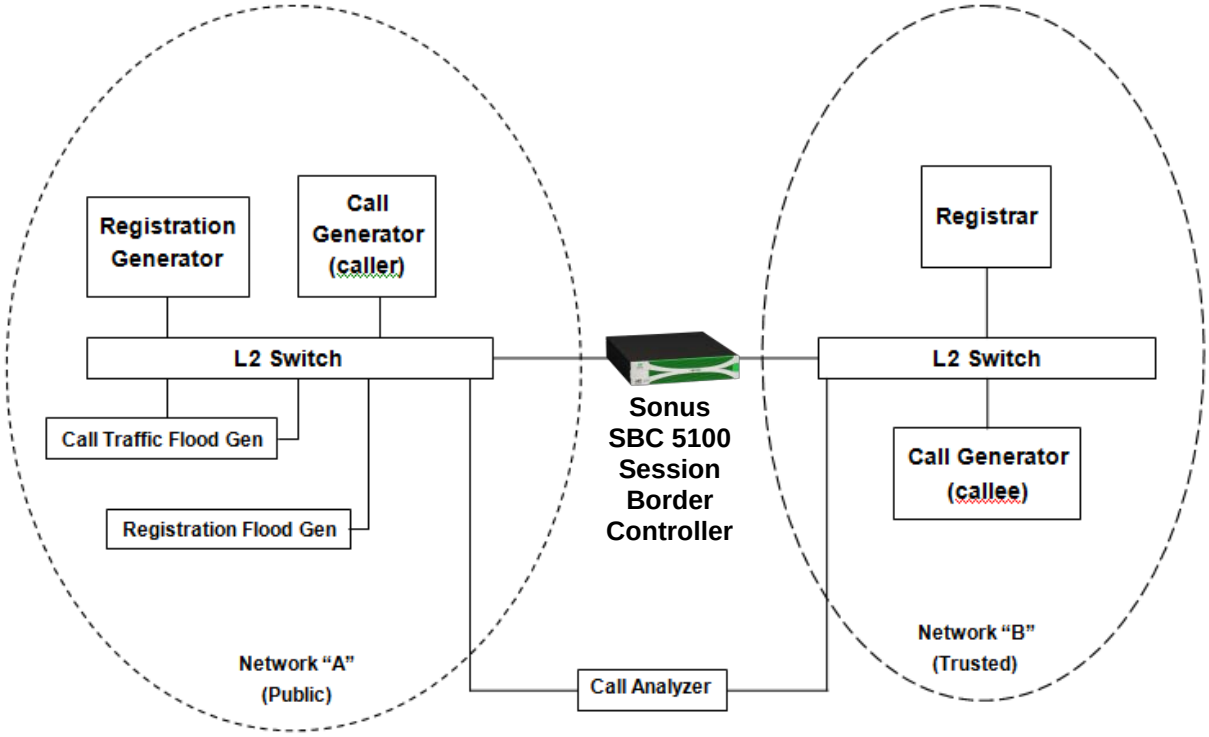
Figure 2: Sonus SBC 5100 Baseline Load with Attacks



Source: Miercom, May 2012

Sonus SBC 5100 maintained call processing during attacks including registration and SIP INVITE floods from invalid peers as well as other attacks.

Test Bed Diagram



Source: Miercom, May 2012

How We Did It

The Sonus SBC 5100, running Sonus SBX Release 3.0, was evaluated in a configuration utilizing one SBC 5100 and two L2 Extreme X450a-24x switches running Extreme OS version 12.0.3.16. All fiber and copper interfaces used for signaling or media were located on the Extreme X450a-24x switches.

Navtel QA604 Release 8.6 and Navtel R14 Release 8.3.1.62 network traffic generators were used to emulate NATTED and non-NATTED access mode scenarios, generating baseline registration and call traffic, registration avalanche, invite and registration floods from invalid peers. For scenarios emulating carrier peering test cases, we used SIPp to generate signaling and attack traffic. SIPp is a free Open Source test tool to generate SIP traffic. It includes user agent scenarios (UAC and UAS) and establishes and releases multiple calls with the INVITE and BYE methods. We used custom XML scenario files to run complex call flows using SIPp.

One interface on the Sonus device was connected through an Extreme Switch to traffic generators for registration generation, call generation (caller), call traffic flood and registration flood. A second interface on the Sonus device was connected through a second Extreme Switch that was configured to traffic generation for registrar, and call generation (callee). The Sonus SBC 5100 was controlled by a Sonus SBC 5100 Management console; and the Navtel QA604 was controlled by a Navtel Management console.

Security and DDoS prevention features were configured using the Sonus-issued DDoS Prevention Configuration guide and the SBC 5100 user guide.

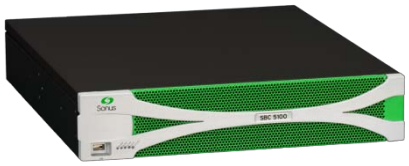
The tests in this report are intended to be reproducible for customers who wish to recreate them with the appropriate test and measurement equipment. Current or prospective customers interested in repeating these results may contact reviews@miercom.com for details on the configurations applied to the Device Under Test and test tools used in this evaluation. Miercom recommends customers conduct their own needs analysis study and test specifically for the expected environment for product deployment before making a product selection.

Miercom Performance Verified

Laboratory testing verified the peering and access performance capabilities of the Sonus SBC 5100 Session Border Controller.

Test results showed that the Sonus SBC 5100 is resilient and robust when exposed to attack traffic, can recover quickly from outages, and successfully processes up to 3,000 concurrent sessions at rates of 150 calls per second.

Miercom is pleased to award the Performance Verified Certification to the Sonus SBC 5100.



Sonus SBC 5100
Session Border Controller

Sonus
4 Technology Park Drive
Westford, MA 01886
1-855-GO-SONUS
www.sonus.net

About Miercom's Product Testing Services

Miercom has hundreds of product-comparison analyses published over the years in leading network trade periodicals including Network World, Business Communications Review, Tech Web - NoJitter, Communications News, xchange, Internet Telephony and other leading publications. Miercom's reputation as the leading, independent product test center is unquestioned.

Miercom's private test services 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. The Performance Verified program is a thorough and trusted assessment for product usability and performance.