Miercom

Lab Testing Summary Report

October 2013

Report 130905

Product Category:

Carrier Class SBC

Vendor Tested:

REVE Systems

Product Tested:

REVE Session Controller RSCw15

Miercom PERFORMANCE VERIFIED™

Key findings and conclusions:

- **REVE Session Controller RSCw15 handled 10,000 SIP requests per second with round-trip response time of less than 10 ms**
- **Exhibited high performance and low latency during 5,000 unauthorized SIP registrations per second with a 3 ms response**
- **Operating in non-media proxy mode, RSCw15 maintained a maximum of 6,500 active calls at 625 calls per second**
- **Highly resilient to SIP torture tests and handled DoS and ICMP Flood attacks of 100,000 pps without impacting active calls**
- **RSCw15 has robust simultaneous session capacity, a maximum of 15,000 in non-media proxy mode and 5,000 using media proxy mode**

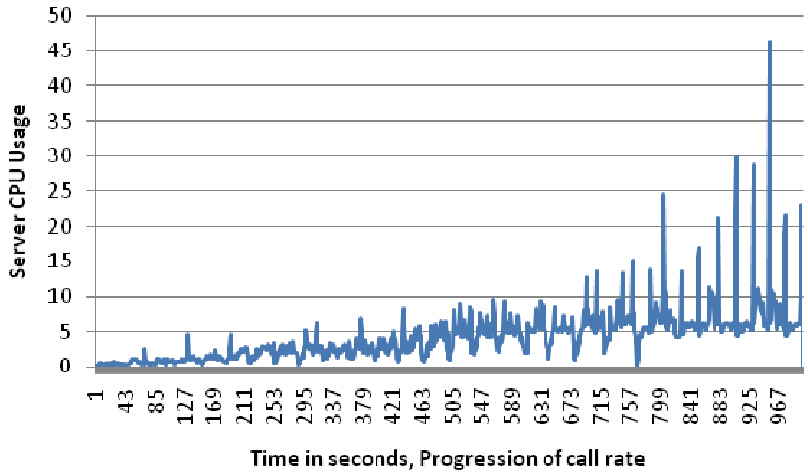
REVE Systems engaged Miercom to conduct an independent evaluation of the REVE Session Controller RSCw15 for performance under normal and adverse traffic conditions. Hands-on testing verified capacity, resiliency and security of the software-centric RSC operating on a high-performance, high-density Commercial Off-the-Shelf (COTS) server.

The RSCw15 is a carrier-grade advanced IP switching platform designed to handle large volumes of traffic. It provides softswitch and billing functionality to meet the high service-level requirements for carriers. Available as part of a bundled 2U solution, the RSC is pre-loaded on a REVE-branded Dell PowerEdge R820 server.

By performing real-time policing of traffic between various IP network boundaries, the RSC contributes to high availability, security and

REVE Session Controller RSCw15

CPU Usage, Non-Media Proxy Mode Call Overload



Source: Miercom, October 2013

During overload testing, the RSCw15 was stable with 625 cps for up to 6,500 active calls before new calls failed. CPU utilization peaked above 45% when the maximum of 5,000 calls was exceeded.

manageability of an enterprise network. Integrated firewalls in its Management System and Web Portal are username / password-protected to enhance security.

Comprehensive, hands-on testing assessed the performance of the RSCw15, simulating a variety of relevant, real-world scenarios that included:

- Saturation with SIP transactions
- Handling a high volume of unauthenticated and authenticated SIP registrations
- Unauthenticated SIP registration overload
- Protecting the CPU in SIP torture tests and two different ICMP flood attacks

The foundation of the RSC consists of two distinct and independently scalable software components, the Signaling Server and the Media Proxy Server. They can be integrated at a single location or geographically dispersed depending on the size and the topology of the network.

The Signaling Server provides subscriber registration, call routing and billing. It handles all SIP signaling traffic from individual SIP endpoints and SIP trunk providers.

For calls that require media hairpinning, the Signaling Server instructs the Media Proxy Server to set up the appropriate RTP media traffic flows.

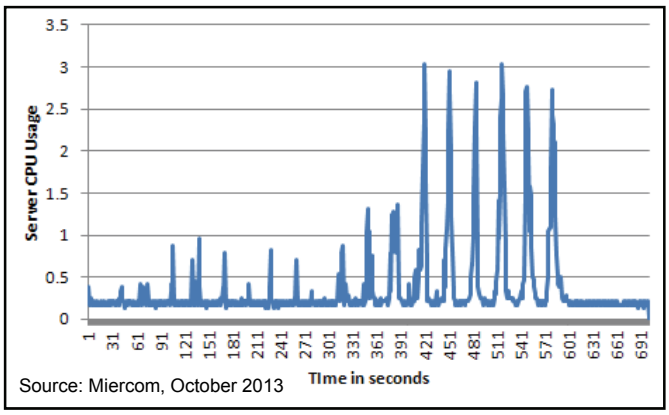
SIP Transaction Saturation

Performance was assessed while the RSC was saturated by various kinds of independent, non-dialog-forming SIP requests, such as OPTIONS and REGISTER.

RSC had good performance for throughput, latency and low CPU usage. It easily handled 10,000 SIP requests per second. The round-trip time (RTT) response never exceeded 10 milliseconds (ms).

The following graph shows the CPU usage as SIP requests were ramped from 100 to 10,000 requests per second during the 10-minute test.

CPU Usage during the SIP Transaction Saturation Test



CPU usage was low throughout the test and maximum usage exceeded 3% twice.

Unauthenticated SIP Subscriber Registrations

To assess its ability to handle unauthenticated registrations, the RSCw15 was subjected to approximately 5,000 SIP registrations per second for 15 minutes.

All registration responses were received within 3ms of the request. Just 0.1% of SIP messages were retransmitted and no messages were lost due to retransmission.

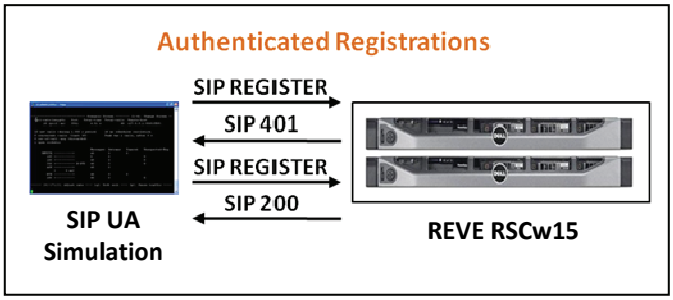
Registration Details

Average traffic rate	4997.984 rps
Request messages	4,499,995
Response messages	4,499,995
SIP retransmissions	4,160
Registration failures	0
Test execution time	15 minutes

CPU utilization and RTT was less than 3%.

Authenticated SIP Subscriber Registrations

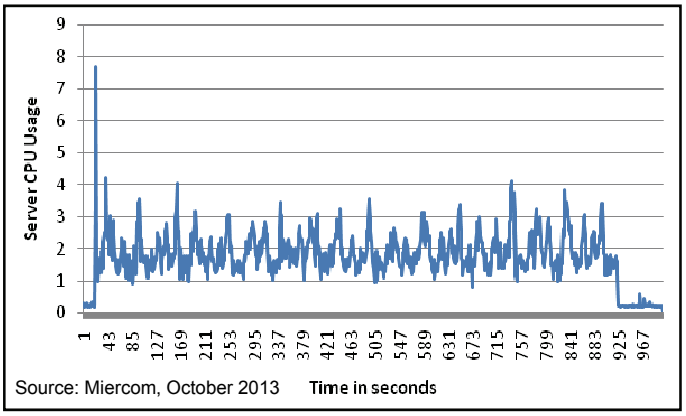
In this 15-minute test, a software component of the RSC, the Registrar, challenged incoming subscriber registration requests for authenticity. An authenticated registration request involves four SIP messages, double that of an unauthenticated request. The additional processing would require more CPU usage.



SIP Authenticated Registration traffic diagram

The CPU usage graph below shows the utilization remained less than 3% during the majority of the testing while the RSC handled 5,000 authenticated rps or a total of 10,000 SIP transactions.

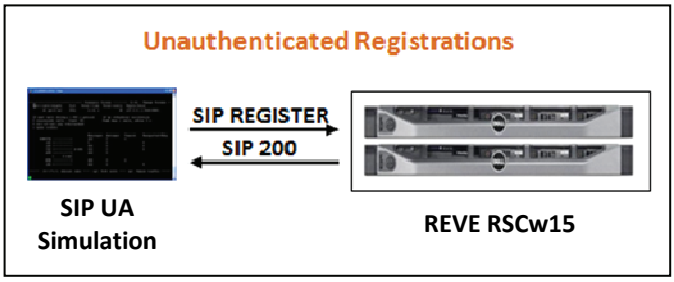
CPU Usage, 5,000 Authenticated SIP RPS



CPU usage exceeded 4% only three times during the course of the 15-minute test.

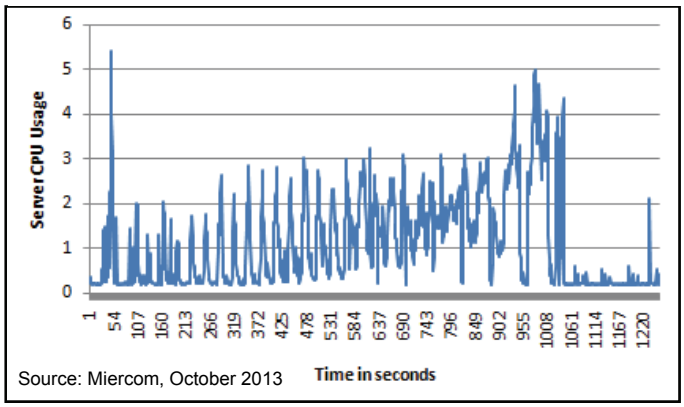
SIP Unauthenticated Registration Overload

In this overload test, the RSC was subjected to an increasing volume of unauthenticated SIP REGISTER requests. Traffic was ramped up from 1,000 to 14,000 unauthenticated SIP rps. The number of rps was increased by 1,000 every 60 seconds.



SIP Unauthenticated Registration traffic diagram

SIP Unauthenticated Registration Overload Performance



CPU utilization exceeded 5% twice during the unauthenticated SIP registration overload test.

CPU usage as the registration traffic was ramped up is displayed in the following chart. At the end of the test, the RSC successfully handled 14,000 unauthenticated SIP REGISTER rps while CPU usage peaked at just over 5% twice. The first occurrence was during initial ramp up. The second occurrence was at the end of the test when rps reached the maximum of 14,000.

Call Handling Modes

The RSCw15 can be deployed in two standard call handling modes, non-media proxy and media proxy.

When the RSC is operating in non-media proxy mode, the media, participating in a call, flows directly between the endpoints. The signaling path of the call flows through the RSC while the media path bypasses it. Additionally, while the RSC is operating in proxy mode, the media between the endpoints hairpins through the Media Proxy Server subsystem.

Non-Media Proxy Mode: Sustained Call Rate

This test challenged the ability of the RSC in non-media proxy mode to sustain calls.

The RSC met the challenge of a sustained SIP Back-to-Back User Agent (B2BUA) message sequence of 100 cps for 15 minutes. Its robust performance included providing 99% of the SIP requests received with an end-to-end response within 10 ms. Complete results are in the following table.

Sustained Call Details

Call rate	99.999 cps
Calls established	90,000
183 progress responses	89,853
Failed calls	0

CPU utilization remained below 4% for this test and exceeded 5% only in the third minute.

Non-Media Proxy Mode: Overload Call Rate

The RSC was subjected to a call rate that started at 25 cps and increased 25 cps every 60 seconds. New calls began to fail with active calls remaining stable at 625 cps, while 6,500 active calls were in the system. The active calls exceeded the target for the test, 5,000. *Figure 1* on *page 1* shows CPU utilization during this test.

Call Session Capacity

A signaling session established through the RSC is a SIP back-to-back user agent call with an independent SIP dialog established at each half of the call. Likewise, when a media session is proxied through the RSC, the media proxy server subsystem terminates two RTP ports, one for each half of the call.

The RSC exhibited strong scalability in simultaneous signaling and media session capacity. The simultaneous session capacities were verified for the RSC operating in non-media proxy mode and media proxy mode. CPU consumption was less than 50% in media proxy mode, and less than 5% in non-media proxy mode.

In non-media proxy mode, the session capacity was 15,000. Media proxy operating mode had a 5,000 capacity.

SIP DoS Torture Testing

SIP torture tests challenge the resiliency of the RSC, stressing its SIP stack implementation and assessing the SIP protocol grammar compliance. These tests can identify security vulnerabilities.

The tests were conducted in accordance with the RFC 4475 benchmark methodology using the PROTOS Test Suite software, as well as a portfolio of SIP torture and compliance tests provided by Spirent Studio Performance.

The RSC proved to be highly resilient to SIP torture tests. The SIP stack implementation running in the Signaling Server rejected or ignored malformed SIP messages. Valid but unusual SIP INVITE messages were successfully processed with end-to-end call setups.

No service failures occurred during the SIP torture tests. The RSC demonstrated a high level of compliance with SIP protocol grammar.

SIP ICMP Flood Attacks

The RSC was tested against a variety of ICMP security attacks. The attacks are designed to assess the vulnerability of the RSC to resource starvation, which can cause disruption of service.

Two types of ICMP attacks, Ping of Death and Ping Flood, using malformed ICMP packets and ICMP ping packets, were conducted. The rate for both attacks was 100,000 pps.

While simultaneously handling active call traffic, the RSC did not show any noticeable degradation in SIP call handling. There was no increase in CPU and memory usage.

Bottom Line

The ability to handle a high volume of IP traffic regardless of the network condition, normal or adverse, is a must for a carrier-grade session controller.

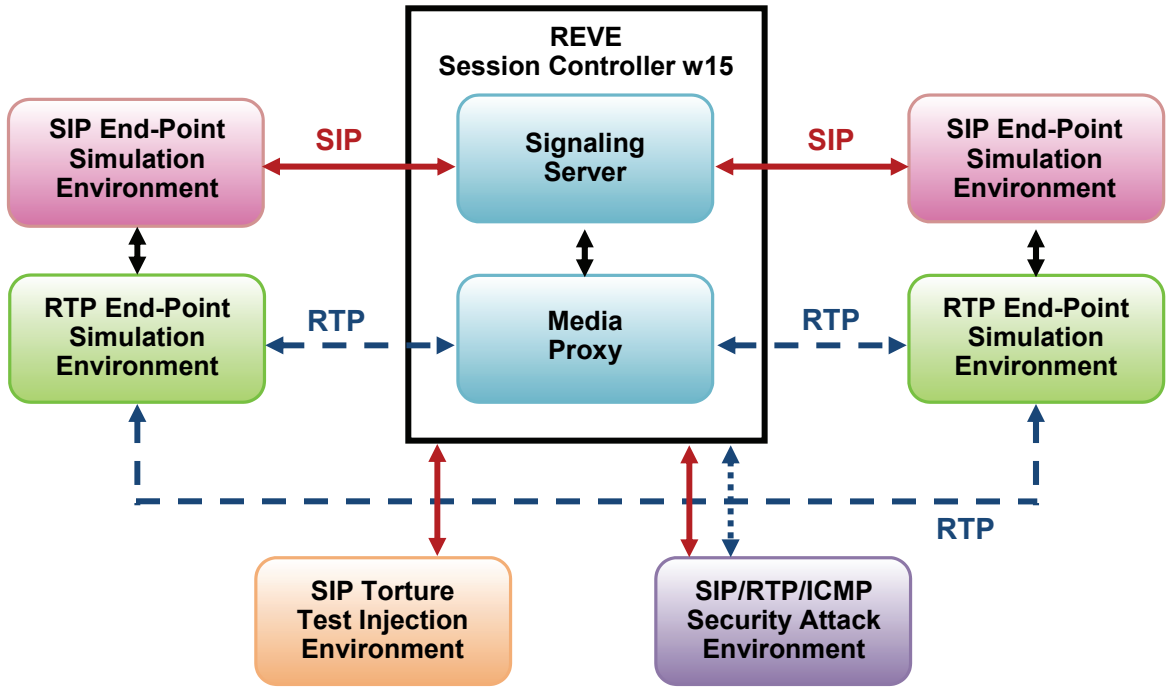
The software-centric REVE Session Controller RSCw15 proved in testing to have the required capacity, resiliency and security while operating in a real-world network, on a COTS server.

The RSC performed impressively when challenged by high volumes of legitimate traffic as well as by security attacks that sought to overwhelm the CPU.

In all of these instances, the RSC handled a high volume of traffic while maintaining a low rate of CPU utilization.

Based on these results, the RSC has earned the Miercom Performance Verified Certification.

Test Bed Diagram



Source: Miercom, October 2013

How We Did It

All tests were conducted with the REVE Session Controller RSCw15 operating in a real-world network, on a COTS server. The test server was a 4U Dell PowerEdge R900, similar to the Dell PowerEdge R820 on which the RSC is marketed pre-loaded software.

Test tools used included SIPp, the PROTOS Test Suite and Spirent Studio Performance.

SIPp, open-source software that can be downloaded for free, is a call-load generation tool that was installed on a server. The test script can be configured for different types of SIP traffic. SIPp was used to verify the simultaneous session capacity of RSCw15 operating in non-media proxy mode and media proxy mode. SIPp was hosted by a Dell PowerEdge 1950 server with 20 GB RAM.

The PROTOS Test Suite and Spirent Studio Performance were used to conduct the SIP Torture tests.

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

The REVE Session Controller RSCw15 was subjected to a comprehensive series of performance tests under normal and adverse network conditions.

Security tests included a simulated SIP DoS attack and two types of ICMP Flood Attack, Ping of Death and Ping Flood.

Throughout, the RSC exhibited the capacity, resiliency and security characteristics for the high service levels required in a carrier class environment. While maintaining performance handling traffic during tests, CPU usage remained consistently low.

Based on hands-on testing and performance results, the REVE Session Controller RSCw15 has earned the Miercom Performance Verified Certification.

REVE
Session Controller RSCw15

REVE Systems

REVE Systems
WCEGA Tower
21 Bukit Batok Crescent
Singapore 658065
65 3157 5040
www.revesoft.com

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. Products may also be evaluated under the NetWORKS As Advertised program, the industry's most thorough and trusted assessment for product usability and performance.

Miercom

Before printing, please consider electronic distribution