Miercom

Lab Testing Summary Report

May 2014

Report SR140428D

Product Category:

Carrier Class SBC

Vendor Tested:

HUAWEI

Product Tested:

SE2900 Session Border Controller

Miercom PERFORMANCE VERIFIED™

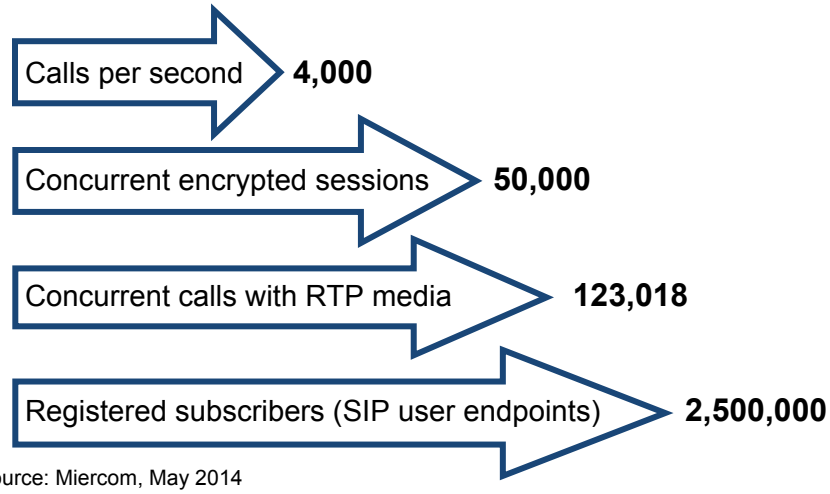
Key findings and conclusions:

- **Testing showed the Huawei SE2900 carrier-class SBC delivers outstanding performance – supporting registration of 2.5 million SIP user endpoints and 12,600 registrations per second, 277,600 concurrent calls without media or 123,000 concurrent calls with full RTP media, with no failed or dropped calls – all exceeding vendor's specs**
- **Huawei SE2900 can provide powerful encryption for service security: supporting 50,000 fully encrypted SRTP media sessions, as well as IMS AKA and TLS encryption of SIP signaling**
- **The highly survivable Huawei SBC successfully manages registration storms after a power outage, call overloads, malformed SIP REGISTER and INVITE assaults, blacklists rogue users and defends against RTP floods and short calls**
- **Huawei SBC easily handled a multi-day, high-load test of 1.4 million BHCA, 53.4 million calls, all with media, 376 calls/second, 550,000 registrations, without dropping a call**

Huawei Technologies engaged Miercom to conduct comprehensive hands-on testing of its SE2900 Session Border Controller, a next-generation, carrier-class SBC, exhibiting the performance and comprehensive security needed in VoLTE (Voice over Long-Term Evolution) and Fixed-Mobile Convergence (FMC) networks. Dozens of discrete tests were applied to evaluate performance and capacity, survivability and resilience. The Huawei SE2900 fared well in all respects.

An assortment of leading-edge test tools (see "How We Tested") measured the system's concurrent call-sustaining capacity, first without

Figure 1: Huawei SE2900 Session Border Controller



Source: Miercom, May 2014

Performance verified. *Some of the key performance and capacity metrics validated in lab tests of the Huawei SE2900 session border controller are shown above. It is one of the highest capacity SBCs we have tested to date. These results are from tests using one subrack. The SBC supports a maximum of three subracks cascaded but this was not tested.*

media – stressing the system's call-setup handling – then with full RTP media, and also with encrypted (Secure RTP) media streams. The maximum rates at which calls could be accepted and processed – with and without media – were also carefully measured.

The Huawei SE2900 is based on an enhanced commercial off-the-shelf (COTS) platform housing the Huawei FusionEngine, employing high-performance chips and proprietary hardware-acceleration technology.

A single SE2900 platform was tested. The 3RU chassis (5.25 inches high) was equipped with two pairs of Service Processing Units (SPUs), used for signaling, media processing and encryption. Each SPU offers four 10GE ports and either four or eight 1GE ports.

Two power supplies in the SE2900 work in 1+1 backup mode (one handles the full load; the other is a hot standby). Two fan modules work in 1+1 redundancy and provide front-to-back ventilation.

Scalability is built into the SE2900. Capacity can be incrementally expanded by adding SPUs to a single SE2900 chassis (up to four per chassis), or by cascading. Up to three SE2900 units can be cascaded – essentially stacked – to become an expanded system. High-speed management and data buses interconnect two or three of the cascaded SE2900 chassis. Cascaded units are managed as a single logical system.

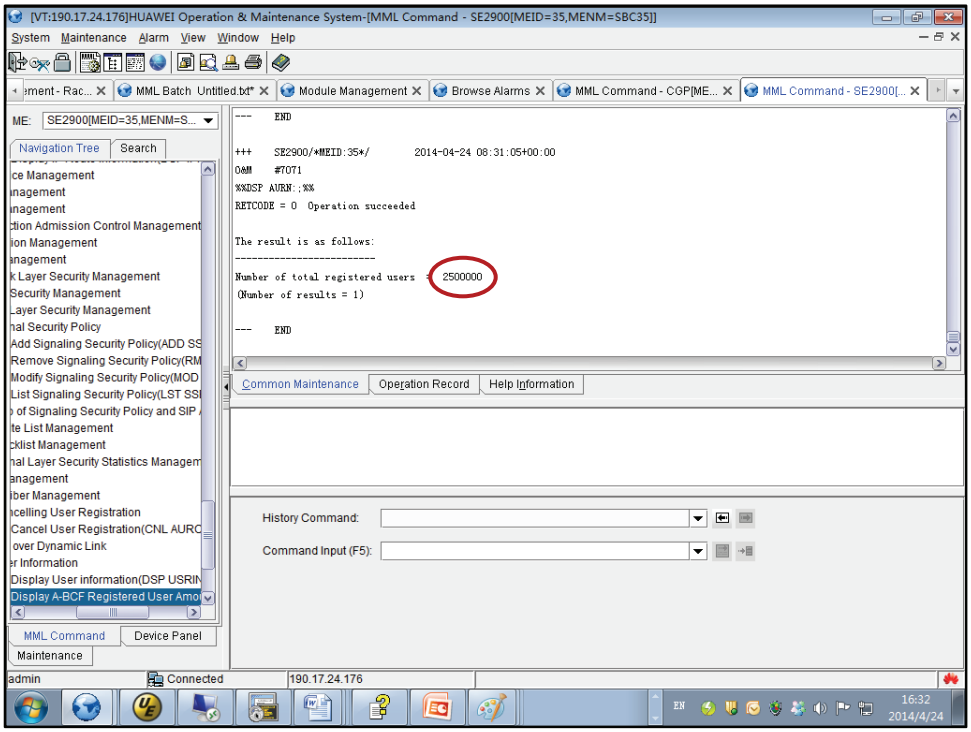
Capacity

Miercom engineers confirmed that the SE2900 could handle the registration of 2.5 million SIP UEs (user endpoints). This test employed the EXFO call-load-simulation system, including an EXFO QA-805 wireless/IMS and VoIP test platform and EXFO QA-604 IMS and VoIP test platform. The QA-805 delivered REGISTER requests on 16 x 1GE ports and the QA-604 on two other 1GE ports.

Registration requests were delivered by the EXFOs at a rate of 700 per second on each of 18 x 1GE ports on the SE2900 – an aggregate rate of 12,600 registration requests per second. An additional ten x 1GE ports on the EXFO QA-805 functioned as proxy servers. Each proxy could handle up to 250,000 SIP user endpoints.

Huawei's product spec sheets claim the SE2900 supports 1.2 million registrations and 3,000 registrations per second. This turned out to be very conservative: Our testing confirmed that 2.5 million

Figure 2: Huawei SE2900 Session Border Controller
2.5 Million SIP User Endpoint Registrations



Source: Miercom, May 2014

Testing confirmed the Huawei SE2900 registered 2.5 million SIP User Endpoints. The EXFO QA-805 test platform with 2 x 10GE interfaces was configured with 10 SIP proxies (a single proxy supports only up to 250,000 UEs). The registration rate was 700 per second on each of the 18 ports used – 12,600 total registrations per second. 16 x 1GE ports on the EXFO QA-805 and 2 x 1GE ports on the EXFO QA-604 delivered the registration requests.

registrations were supported, and that registrations were processed, with no fails, at a rate of 12,600 registrations per second.

IPsec Subscribers, per IMS AKA

Separately, testing was also conducted to ascertain the SE2900's capacity for handling SIP signaling within IPsec tunnels, per a protocol called IMS AKA, now an integral component of IMS (IP multimedia subsystem) and LTE (Long-term evolution) network architectures.

With IMS AKA, SIP user endpoints exchange two regular SIP register requests and responses with network control, which uses information from the message headers to setup authenticated, encrypted IPsec links with the user endpoint. Then all subsequent call signaling between the network and the user endpoint is secure.

EXFO call simulators were used for this test, and verified that the SE2900 could sustain 1.2 million IMS AKA IPsec secure sessions with SIP user endpoints.

Maximum Concurrent Calls

A separate battery of tests was conducted to verify the maximum number of concurrent calls the SE2900 can set up and maintain, and the rate at which the system can process and set up calls.

Three different call environments were tested:

- Calls with no media. This taxes mainly the ability of the SBC to process call requests and achieve a maximum sustained call load. The corresponding media streams normally associated with VoIP calls are not present.
- Calls with full RTP (real-time transport protocol) audio media streams.
- Calls with encrypted SRTP (Secure RTP) media streams. These are resource-intensive calls. Each such call actually comprises two discrete encrypted 'sessions' – one from the caller to the SBC, and another from the SBC to the called party.

The EXFO QA-805 test system was used for the first two tests. The EXFO QA-604 was used for the third encrypted test, as the QA-805 did not support media encryption.

For these concurrent-call-load tests, a security policy was set on the SE2900. A threshold of 70 percent was set on CPU utilization, this is to avoid triggering flow control. If CPU usage rose above 70 percent, the SE2900 could reject new call requests, as necessary and appropriate. Below 70 percent, no call throttling would be applied.

As noted, separate testing verified the maximum number of calls **without** media that could be processed, and then the number of concurrent calls **with** media that could be sustained.

For testing calls without media, the RTP media-generation functionality on the EXFO QA-805 was disabled. The test system delivered 4,000 call

Figure 3: Huawei SE2900 Session Border Controller
Verification of Concurrent Calls Supported

Call Load	Max Sustained Call Load (1)	CPU Utilization	Calls per Second (1)
Call requests with no media	277,609	60-70%	4,000
Calls with full RTP media (G.711)	123,018	60-70%	1,504
Calls with encrypted SRTP streams	25,000 (caller and called-party pairs) = 50,000 encrypted "sessions"	60-70%	1,200

(1) With no dropped calls or rejected call attempts

Source: Miercom, May 2014

Testing confirmed the Huawei SE2900 could sustain over 277,000 concurrent calls without media, and over 123,000 concurrent calls with full RTP media, with no calls dropped or rejected. 50,000 SRTP encrypted sessions, equating to 25,000 fully encrypted caller-to-called-party calls, could be sustained. More than 1,500 calls per second with full media could be set up with no calls dropped.

These results are from tests using one subrack. The SBC supports a maximum of three subracks cascaded but this was not tested.

attempts per second over 16 x 1GE ports to the SE2900. Call duration time was set to infinite.

Besides registering 1.2 million user endpoints, the SE2900 maintained up to 277,608 concurrent calls without media. No calls were dropped and no call attempts failed. This is comfortably more than the vendor's published spec of 250,000 concurrent calls without media.

In the test for maximum calls **with** media, the EXFO QA-805 delivered over 1,500 call attempts per second. Each call employed G.711 audio streams and lasted 73 seconds.

After registering 1.2 million user endpoints, the SE2900 reached a maximum of 123,018 concurrent sustained calls with media, appreciably more than Huawei's published figure of 100,000 such calls. At this level no calls were dropped and no call attempts failed.

Security and Overload Protection

Testing examined the ways the SE2900 protected itself and calls in progress from malicious networks attacks, as well as call overloads. It is a given that an SBC may have to reject call requests when its resources are fully tapped, but such transient overload events should not impact calls in progress.

Security: Signaling Flood Attack

In this test, involving the EXFO tools and Codenomicon's Defensics system, a malicious flood of SIP INVITE requests is launched against the SE2900 SBC, seeking to overwhelm its resources. Flood attacks were sent using one source IP address initially and subsequently with multiple, random source IP addresses and ports.

Each such DDoS (Distributed Denial of Service) attack was a flood of SIP INVITE requests sent from random spoofed IP addresses and ports.

The attacks were launched as the SE2900 was busily engaged – with 1.2 million user endpoints registered, 100,000 concurrent calls (without media) in progress, and 2,000 new call attempts per second coming in.

We noted via the SE2900's real-time graphical interface that the flood-attack packets were blocked almost immediately. In addition, within a few minutes the SE2900 had blacklisted the attack source – the offending IP address and port.

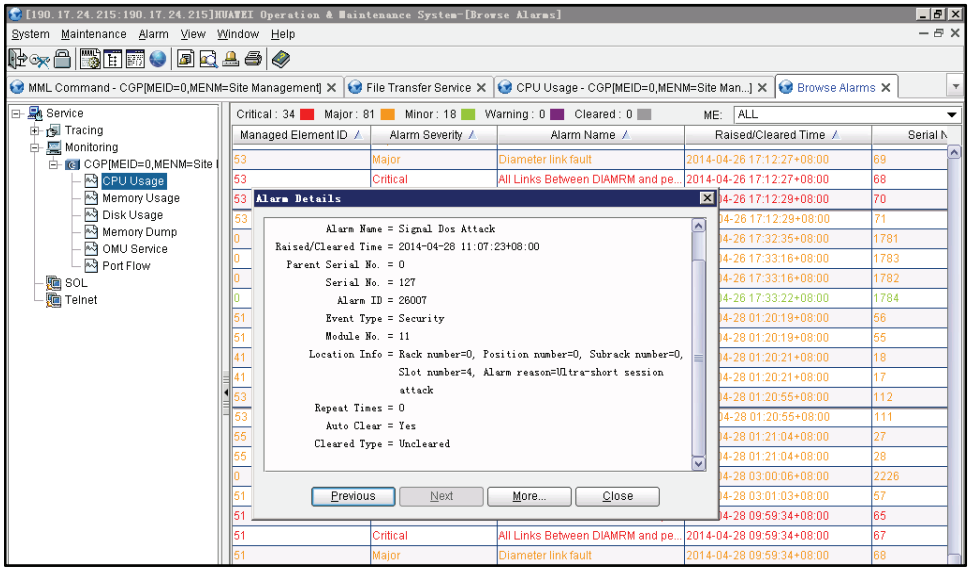
CPU utilization increased to 50 percent during the attack but returned to 35 percent immediately afterwards. There was no impact on either control or background traffic. The attacks were effectively thwarted.

Security: Nessus Scanning

The professional version of the Nessus Vulnerability Scanner, from Tenable Network Security, was used to assess the vulnerability of the SE2900's control software to malicious attacks. The Nessus software, with all the latest scan plug-

One of many DoS attack alarms triggered and recorded by the Huawei session border controller.

Figure 4: Huawei SE2900 Session Border Controller Signaling DoS Attacks



Source: Miercom, May 2014

ins, ran on a test computer linked directly to the SE2900.

The widely used Nessus system launches various probes and assaults (see table below) and then issues a report detailing any aspects of the device under test that may be exposed or open to attack. A "Pass" indicates no detected open vulnerability.

Huawei SE2900 SBC – Nessus Vulnerability Results

Test #	Test Script Name	Result
34277	Nessus UDP Scanner	Pass
10113	ICMP Netmask Request Information Disclosure	Pass
10114	ICMP Timestamp Request Remote Date Disclosure	Pass
10180	Ping the Remote Host	Pass
10287	Trace Route Information	Pass
11834	Source-routed Packet Weakness	Pass
12264	Record Route	Pass
19506	Nessus Scan Information	Pass
27576	Firewall Detection	Pass
33930	PCI DSS Compliance	Pass
60020	PCI DSS Compliance: Handling False Positives	Pass

Source: Miercom, May 2014

The above table details some of the key Nessus scan results. All of these completed successfully and revealed no security vulnerabilities in the Huawei SE2900 SBC.

Security: SIP Fuzz Testing

Fuzz testing, also called robustness testing, tests a system's software by sending it malformed and unexpected input data. Conducted by Codenomicon's Defensics system, malformed SIP REGISTER and SIP INVITE requests were delivered to stress the SE2900.

The test ran overnight, during which time 30 call attempts per second of legitimate calls were delivered to the SE2900. Intermingled with that background traffic were over 450,000 malformed SIP INVITE requests and 300,000 malformed SIP REGISTER requests.

All of the legitimate calls were properly serviced and all of the malformed packets were detected and blocked. No abnormal or adverse impact on CPU utilization was detected during this period, and none of the background calls or call load was affected. The attack was thwarted.

Security: Signaling Encryption

An effective defense against many security threats in the VoIP world (including 'interception,' or man-in-the-middle, attacks) is to encrypt SIP call-control messages. Typically, encrypted SIP signaling messages are sent to the proxy server or SBC within an encrypted TLS (transport layer security) connection.

Both the EXFO QA-805 and EXFO QA-604 were employed as SIP user-endpoint simulators in this testing, delivering new subscriber requests via secure TLS connections.

At the end of the roughly one hour test period, a total of 600,000 user endpoints had registered – at a rate of 2,400 registrations and 1,200 calls per second on the SE2900 via encrypted TLS-based signaling connections.

Overload Protection: RTP Flood Attacks

Another threat to VoIP networks is malicious floods of RTP (real-time transport protocol) packets, designed to confuse and overwhelm equipment like SBCs. The Huawei SE2900 proved capable of detecting and blocking RTP flooding – from a single source IP address, as well as from random and spoofed IP addresses.

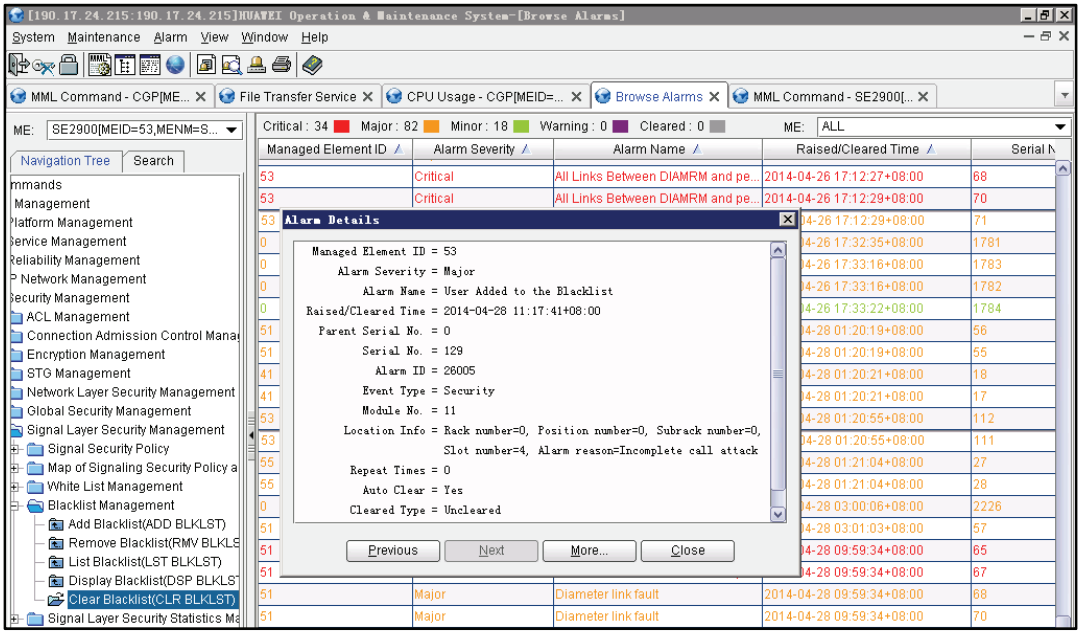
The key to this defense is a settable security policy on the SE2900, which blocks all user endpoints that have sent more than 1,000 packets per second. Legitimate VoIP conversations typically generate no more than a few hundred packets per second, or less – the packet rate depending on the voice encoding that is used.

This test employed a special software tool called Hping3, which ran in the test lab on a Linux server.

In the first test, a flood of Layer 4 UDP (user datagram protocol) packets from a single IP address was sent in an effort to spoof the SE2900. The packets were disguised to look like legitimate RTP traffic coming from a source IP address registered with the SE2900. With the rate-limiting security policy in place, the SE2900 effectively blocked this traffic and blacklisted the source.

Then RTP packet floods were launched from random IP addresses which formed an IP address pool that were all legitimately registered with the SE2900. These flood assaults were all successfully blocked as well, as the flood rates exceeded 1,000 packets per second and the rate-limiting security policy was applied.

Figure 5: Huawei SE2900 Session Border Controller
User Added to Blacklist



Source: Miercom, May 2014

This DoS attack alarm was triggered and recorded by the Huawei SE2900 SBC when a user was added to the blacklist.

Overload Protection: Blacklist for Rogue Users

In this test, we validated the ability of the SE2900 to blacklist the IP address of a "rogue user" that was exceeding the Call Admission Control (CAC) policy for maximum call attempts per second.

The EXFO QA-604 was set up to emulate a gateway IP port with many associated user endpoints. It connected and sent call requests to the SE2900 via two 1GE connections.

Then, to trigger the blacklist response on the SE2900, we set the maximum call attempts per second (CAPS) from any IP address to 2,000.

With the EXFO QA-604 injecting 240 call attempts per second – well below the threshold for blacklisting – the SE2900 allowed all the call attempts. We ramped up the call-attempt rate and, in response to the injection of 3,000 call attempts per second, the SE2900 placed the IP address and port number of the EXFO QA-604 on the blacklist, and all subsequent call attempts from it were blocked.

The SE2900 interface for setting and applying blacklist restrictions is very configurable. Also settable is the period of time, such as 15 minutes, for automatically removing an IP address from the blacklist after it has stopped sending bogus traffic.

Overload Protection: Tenfold Overload

An overload of incoming call attempts, far in excess of what equipment is designed to handle, will overwhelm an SBC unless there are built-in overload protections.

This test sought to find out how effectively the SE2900's overload protections worked. Huawei's published call-handling rate for the SE2900 is 1,200 call attempts per second. We decided to deliver up to ten times that load and see what happened.

We first set the SE2900 to apply flow control when CPU utilization hit 80 percent. Then we delivered call attempts at a moderate rate, to set up 20,000 long-duration calls, without media.

With the background calls established, we delivered 12,000 new call attempts per second – ten times the vendor's specified load capacity.

The result: The SE2900 would accept and process up to 4,000 call attempts per second – up to and beyond the 80-percent CPU utilization threshold we had set. This is what our earlier testing found was the SE2900's maximum call-handling rate for non-media calls. Call requests beyond the 4,000 per second were responsibly rejected. What's more, throughout the testing, none of the background calls dropped or were otherwise affected.

Overload Protection: Registration Storm

This test simulated a real-world scenario – where a power outage takes down the SBC and then power is restored. The SE2900 faces 1.2 million SIP phones coming back online at once. The hoped-for

result is that all of the phones will re-register as quickly as possible.

The SE2900 allows a limit to be set on the number of registration attempts per second that will be processed. We set that to 60,000 registrations per second. Flow control was enabled, with a CPU utilization threshold of 80 percent - meaning that CPU usage over 80 percent would trigger throttling and rejection of new incoming requests including registration.

With both overload mechanisms enabled - the registrations-per-second limiting mechanism and the 80-percent-CPU flow control - the SE2900 effectively handled the situation. All 1.2 million simulated SIP user endpoints were re-registered in five minutes. The SE2900 processed the registration requests at a rate of 4,000 per second. Earlier testing found that the SE2900 could actually handle as many as 12,500 registrations per second.

CPU utilization throughout this testing remained around 33 percent, never even approaching the 80-percent threshold that would have triggered rejection of re-registration requests.

Resiliency and Failover

Several additional tests were conducted to assess how well the SE2900 responds to unexpected and infrequent events and scenarios, which inevitably, and regrettably, do occur in carrier VoIP networks.

These resilience tests assessed the following:

- The ability of the SBC to note and alert when a high incidence of too-short or incomplete calls occurs
- The SBC's ability to failover a port to an appropriately configured redundant port, or to failover a failed card to a back-up card
- The ability to block improper media sends – when a media stream is received before the call is fully set up via SIP signaling
- The attrition test: the SE2900's ability to run under moderate-to-heavy load for days with no problems or dropped calls.

Resiliency: Too-Short and Incomplete Calls

Too-short or short-duration calls, typically lasting just a few seconds, are bad calls. They are indicative of a call-completion issue, especially when the same user endpoint is the source of multiple call (and re-call) attempts.

The SE2900 includes a configurable setting for tracking this and other call anomalies, and then issuing an alert based on threshold settings. We set a threshold to alert on 30 such too-short-call events occurring within five minutes, and then confirmed that the too-short-call events were noted and alerted when the threshold was exceeded.

Incomplete calls are a different issue and may indicate a hacking attempt, though any incorrect SIP call sequence can result in an incomplete call.

The SE2900 can be configured to alarm on incomplete calls, and can also usually block the call attempt (by issuing the appropriate INVITE CANCEL message sequence). Testing confirmed both responses are configurable and can be invoked to effectively deal with incomplete calls.

Resiliency: Port and Card Failover

Tests also confirmed that, to significantly bolster system uptime, availability and resilience, ports and key cards within the SE2900 can be provisioned in hot-standby or failover-redundant mode.

We confirmed that ports can be provisioned to be load-shared or hot-standby-failover, depending on the L2 or L3 method used. With 10,000 concurrent calls in progress and 375 new incoming call attempts per second, we pulled a 1GE port on the SE2900 and observed the result. None of the concurrent calls dropped and there were no failed call attempts.

Similarly, we provisioned service processing (SP) cards, which handle signaling, media processing and encryption, to be active and hot-standby and then unplugged the active board. With 200 call attempts per second being processed there were no incomplete calls resulting from the failover.

Resiliency: Unauthorized Media Send

Problems can occur in SIP call setup when an RTP media stream is received before the call is properly established per SIP signaling (before a 200 OK message is sent back to the user endpoint). In such cases, where an INVITE message is followed immediately by the RTP media stream from the endpoint, the normal procedure is to block the RTP traffic.

Our test confirmed that the SE2900 effectively blocks such "unauthorized" media streams, sent before proper completion of the call setup. In addition, we confirmed that legitimate call

attempts received before and after the unauthorized-media events were all handled properly.

Resiliency: Attrition Test

It is customary to conclude a comprehensive set of performance tests with an 'attrition' test, where the device under test is set up to run for a protracted period with a moderate to heavy load of traffic under normal operating conditions. Afterwards, the engineers will scrutinize alerts, test-equipment statistics and/or message logs for any anomalies.

Two EXFO QA-805s were used for this test to generate calls with full RTP media. The duration of each call was 73 seconds.

The test ran for two days. A constant load of 10,000 concurrent calls, with media, was maintained by the SE2900, along with 376 new incoming call attempts per second – equating to a BHCA (Busy Hour Call Attempts) of 1.4 million.

We could find no anomalies to report. No calls were dropped and none of the 53.5 million call attempts failed. The SE2900's CPU utilization hovered between 25 and 40 percent during the entire period of this testing. Memory utilization averaged 69 percent.

In short, the SE2900 performed flawlessly, handling a substantial load for two days while barely breaking a sweat.

Built-in Scalability

As noted earlier, Huawei delivers scalability with the SE2900 in several ways. Within a single system (subrack) users can incrementally add processing engines – Service Processing Units, or SPUs – to accommodate growing load. Then, when substantial additional service capacity is required, multiple SE2900 subracks can be aggregated in a cascaded arrangement.

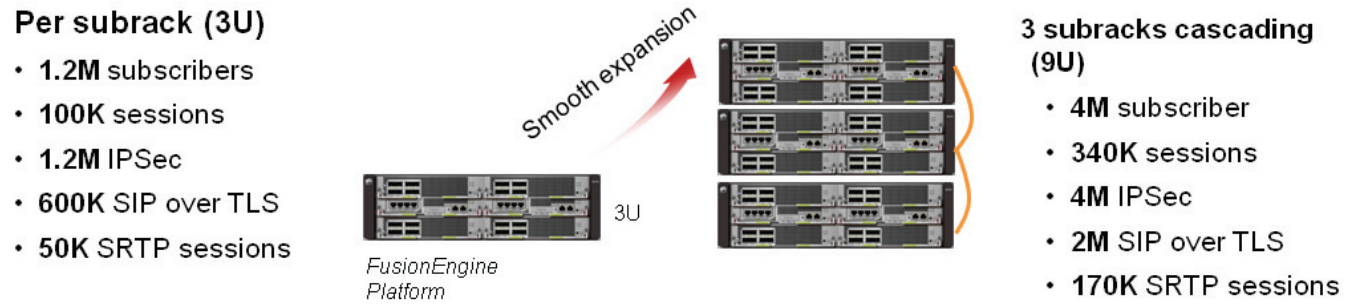
Up to four SPU modules can be incrementally deployed within a single, multislot SE2900 chassis. Each SPU independently handles signaling, media processing and encryption, and provides four 10GE interfaces and up to eight 1GE interfaces.

To achieve maximum capacity with one subrack, all SPUs can be active and load-sharing. Or, for maximum redundancy and survivability, pairs of SPUs can be deployed in an active/hot-standby arrangement.

When traffic volume exceeds the aggregate capacity of a single SE2900 subrack, one or two additional SE2900 subracks can be incrementally added. These can likewise be provisioned in load-

Figure 6: Huawei SE2900 Session Border Controller

Cascaded SE2900 Session Border Controllers support Scalability

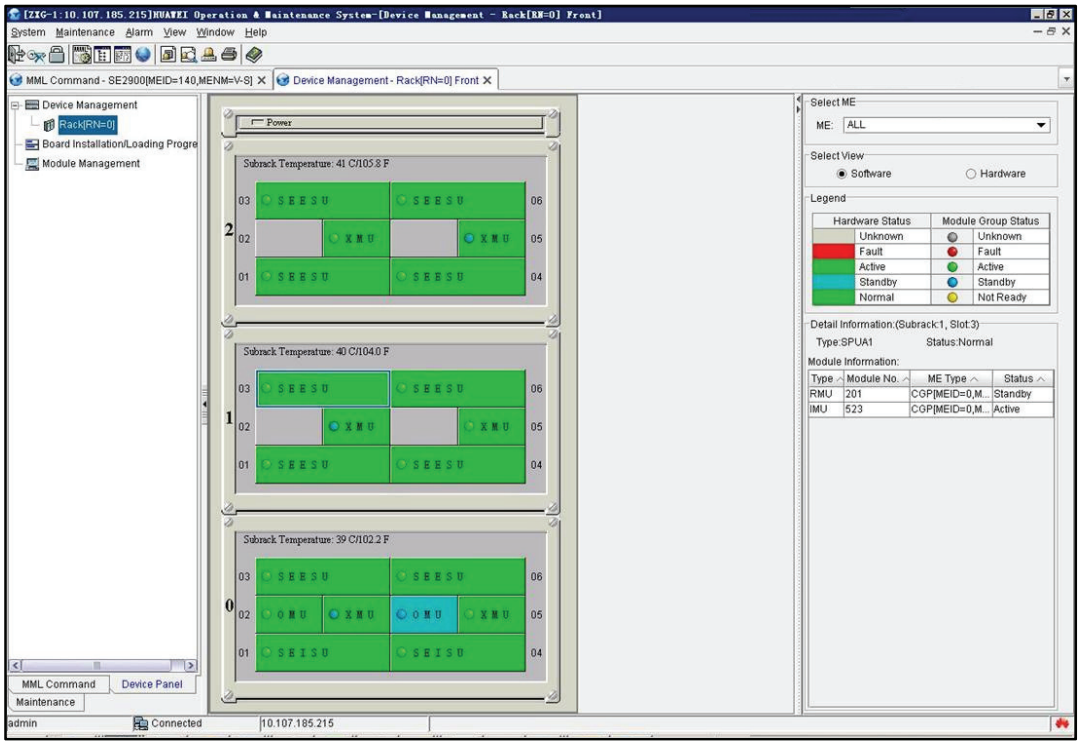


***The sum of the parts**. Cascaded SE2900s can yield impressive aggregate service-processing capacities. Shown above are the vendor-stated specs for three cascaded SE2900 SBCs. These figures assume that the modules in each unit are deployed in a 1+1 back-up mode. Our testing has found that actual performance usually exceeds Huawei's stated capacity.*

Figure 7: Huawei SE2900 Session Border Controller

Cascaded SE2900 Session Border Controllers support Scalability

Consolidated management. *The screenshot shows how three cascaded SE2900s are represented in real-time and managed via the same consolidated interface. At this level the status of every module within each of the three cascaded SE2900 subracks is readily apparent.*



Source: Miercom, May 2014

sharing or back-up modes. Akin to "stacking" of switch modules, cascaded units can be positioned above each other in a rack. Three subracks consume just 9RU, or 15.75 inches, of rack space.

The Huawei SE2900 is the first session border controller we have seen that is designed to support scalability via multi-unit cascading in this manner. Two high-speed busses link the cascaded units: a data bus, used mainly for transmitting service messages between the service plane of the systems; and a management bus, which links the control planes, is used for software loading and exchange of alarm and maintenance information.

Bottom Line

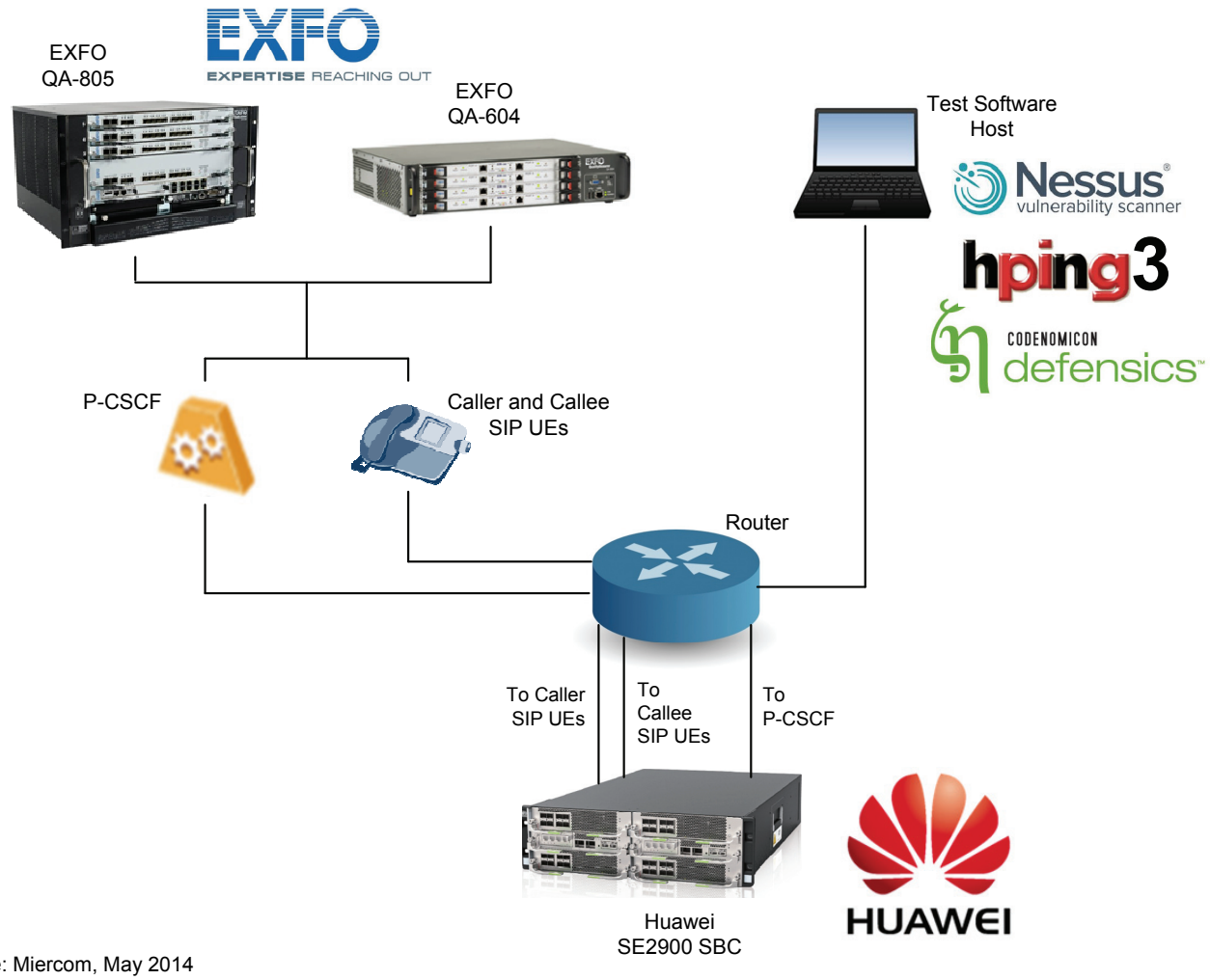
We found the Huawei SE2900 to be a full-featured, high-capacity, solidly performing, carrier-class Session Border Controller (SBC).

The SE2900 can, in our estimation, readily satisfy the intense all-IP and high-security requirements of carriers that are implementing or migrating to a VoLTE (voice over long-term evolution) network or fixed-mobile convergence (FMC) architecture.

The SE2900 is one of the best-performing, highest-capacity SBCs for the carrier market that we have tested to date. Huawei has used the last few years while the industry has migrated to VoIP and SIP to its benefit, and has built into the SE2900's operating software safeguards against the leading threats to VoIP network continuity – from Denial of Service attacks to malformed, too-short, incomplete or out-of-order SIP call requests.

Our testing addressed and examined the many aspects of the SE2900 that address reliability, resilience and continued uptime. And we note that capacity can be incrementally increased by adding modules in the same multislot chassis, or by adding one or two more load-sharing SE2900 chassis in a stacked arrangement.

Test Bed for Load Testing



Source: Miercom, May 2014

How We Did It

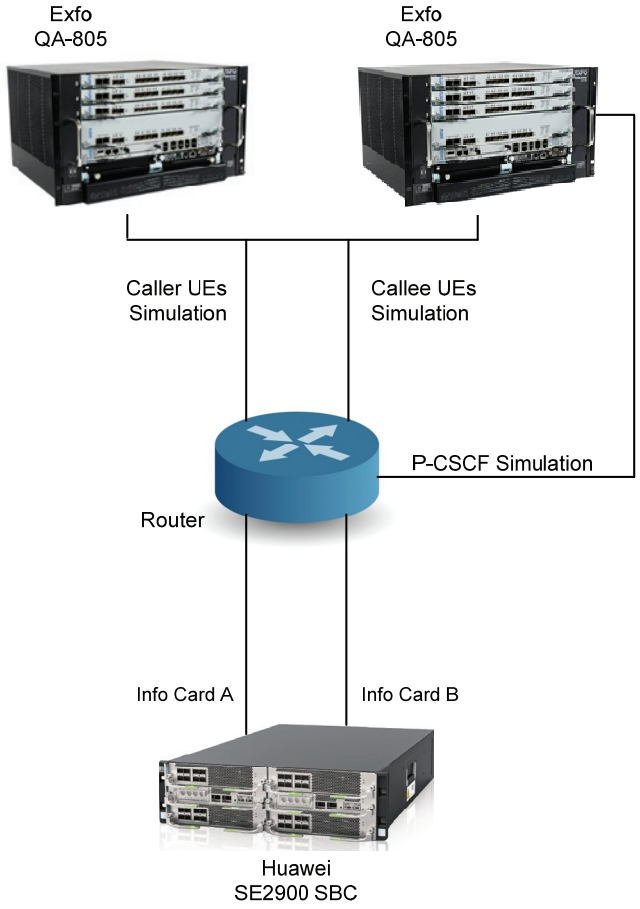
A broad variety of tests requires an equally broad assortment of test tools. The Huawei SE2900 session border controller received simulated traffic in testing from two models of the EXFO QualityAssurer series of IP Multimedia Subsystem (IMS) and Voice over Internet Protocol (VoIP) test platforms.

EXFO (www.exfo.com) is a leading provider of next-generation test and service assurance solutions for wireless and wireline network operators and equipment manufacturers in the global telecom industry. The EXFO QA-805 is a 6RU test platform with impressive performance characteristics, including the ability to emulate more than 5 million subscribers, more than 5 million data sessions and 1.25 million RTP (Real-time Transport Protocol) streams.

The entry-level QA-604 is a 2RU test platform, which can emulate more than 2 million SIP endpoints, over 2 million subscribers and 128,000 RTP and RTP Control Protocol (RTCP) streams. The QA-805 and the QA-604 were used individually or together depending on the specific tests we were running.

In some of the testing two QA-805s systems were used. For example, the QA-805 was used in tests to ascertain the maximum concurrent calls maintained by the Huawei SBC, with and without media. In testing calls with media, the QA-805 was equipped with one W²CM card that provided two 10GE ports. In the test for maximum concurrent calls without media, the QA-805 equipped with two W²CM cards was used, yielding 16 x 1GE ports and eight proxy servers.

Test Bed for High Availability Testing



Test 1. Port-Based Failover
Port on Card A is Active (Master)
Port on Card B is Standby (Slave)
Both cards are active

Test 2. Card-Based Failover
Port on Card A is Active (Master)
Port on Card B is Active (Master)
Card A is Active
Card B is Standby

Source: Miercom, May 2014

In determining the maximum number of concurrent SRTP (secure real-time protocol) encrypted calls that the SE2900 can maintain, the QA-604 was the simulation tester we used, since the QA-805 does not support SRTP encryption.

The QA-805 and QA-604 were used side by side in testing to ascertain the maximum SIP registrations supported. On the QA-805, one 10GE port was used to create 10 x 1GE ports while 16 x 1GE ports were used to generate SIP user endpoints (UEs) on the SE2900. On the QA-604 two additional 1GE ports were used to create SIP UEs.

Two QA-805s were used in the 48-hour attrition test, in which the SE29000 maintained 10,000 concurrent calls without a call dropped or rejected.

Specialty software tools employed in the testing ran on a laptop computer that was connected to the SE2900. One of these was Version 5.0.1 of the Nessus Vulnerability Scanner, which was used to probe the software that controls the SE2900 for attack vulnerabilities.

The Nessus Vulnerability Scanner is a product of Tenable Network Security (www.tenable.com). The company's mission is to help secure and protect any device from threats on the Internet, such as malicious software, hackers, viruses and more.

Hping3 is free software, which was used in our testing to generate UDP traffic that sought to spoof the SE2900. We were evaluating the SE2900's ability to defend against RTP floods.

Version 11.2.10 of Defensics software from Codenomicon (www.codenomicon) generated the malformed SIP REGISTER and INVITE requests in SIP fuzz testing.

Defensics is a leader in this area of vulnerability testing and software quality assurance, providing pre-emptive security testing for network equipment manufacturers, carriers, consumer electronics companies, private-sector organizations with enterprise networks, and government entities.

The tests in this report are intended to be reproducible for customers who want to recreate them using the same or appropriately similar test and measurement equipment. Current or prospective customers interested in reproducing 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 a needs analysis study for their particular environment and then test specifically for that expected deployment scenario before making a product selection.

Miercom Performance Verified

With the SE2900 session border controller, Huawei has raised the bar in providing the capacity and performance that carriers need to realize VoLTE (voice over long-term evolution) or fixed-mobile convergence (FMC) networks.

One of the most powerful and resilient SBCs we have tested, the SE2900 performed well in all areas of this comprehensive, hands-on testing – notably capacity, performance and survivability, all essential requirements in carrier networks.

The Huawei SE2900 session border controller has earned the Miercom Performance Verified Certification for its exceptional showing in all aspects of this testing.

Huawei SE2900
Session Border Controller

Huawei Technologies, Co., Ltd.
www.huawei.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*, UBM *Tech Web*, *No Jitter*, *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.