Independent Performance Testing:

Cataleya Enhanced Session Border Controller Orchid One

Capacity-Handling and Performance Verification

DR150501D
May 2015

Miercom
www.miercom.com

Contents

1.0 Executive Summary

Miercom was engaged by Cataleya Pte, Ltd to conduct independent performance testing and an assessment of key features and capabilities of the Enhanced Session Border Controller (eSBC) Orchid One, a carrier-class VoIP-control system. Testing, which employed industry-leading traffic generation and security threat equipment, was conducted in late April 2015.

Testing concentrated in two main areas:
- Performance: specifically, registration capacity, call-processing rates supported, concurrent-call-handling capability, and related metrics.
- Security and resiliency: active/standby controller failover and the ability to sustain operations under numerous malicious-assault and stressful environments.

Key Findings and Observations:

- The Cataleya Enhanced SBC (eSBC) Orchid One delivers impressive call-handling capacity: Tests confirmed that it can handle 512,000 concurrent registrations, 200,000 calls without media, and 100,000 calls with full RTP media, all on a sustained basis.
- The eSBC Orchid One supports 80,000 encrypted TLS connections, the interworking of 30,000 Secure RTP (SRTP) media streams and transcoding of 14,500 media channels.
- The system exhibits a high level of resiliency, successfully fending off over a dozen malicious assaults and Denial-of-Service attacks. What's more, in an active-standby configuration, an eSBC Orchid One fail-over resulted in just a single failed call.
- The system is built to address all manner of differences between service providers, able to convert between IPv4 and IPv6 call requests, dynamically modifying call headers as needed, and transcoding between different codecs. Effective utilities are included for monitoring QoS and SLAs, for tracing calls and for policy configuration.

Based on the impressive results of our testing, we proudly award the Miercom Performance Verified Certification to the Cataleya Enhanced SBC, having turned in outstanding performance in Miercom's ongoing SBC study.

Robert Smithers
CEO
Miercom

2.0 Product tested

Cataleya is a subsidiary of eGlobal Communications Group, the leading provider of software solutions for mobile carrier networks. Its product, the latest 1.7.0.197 release of the Enhanced Session Border Controller (eSBC) Orchid One package, was tested for full SBC functionality, handling and quality of service (QoS). The product was received as a hardware/software package, pre-installed by Cataleya, and tested on a high-end, off-the-shelf, virtualized server. State-of-the-art session initiation protocol (SIP) traffic generation equipment was provided by the EXFO, along with custom test gear for volume message generation and security testing.

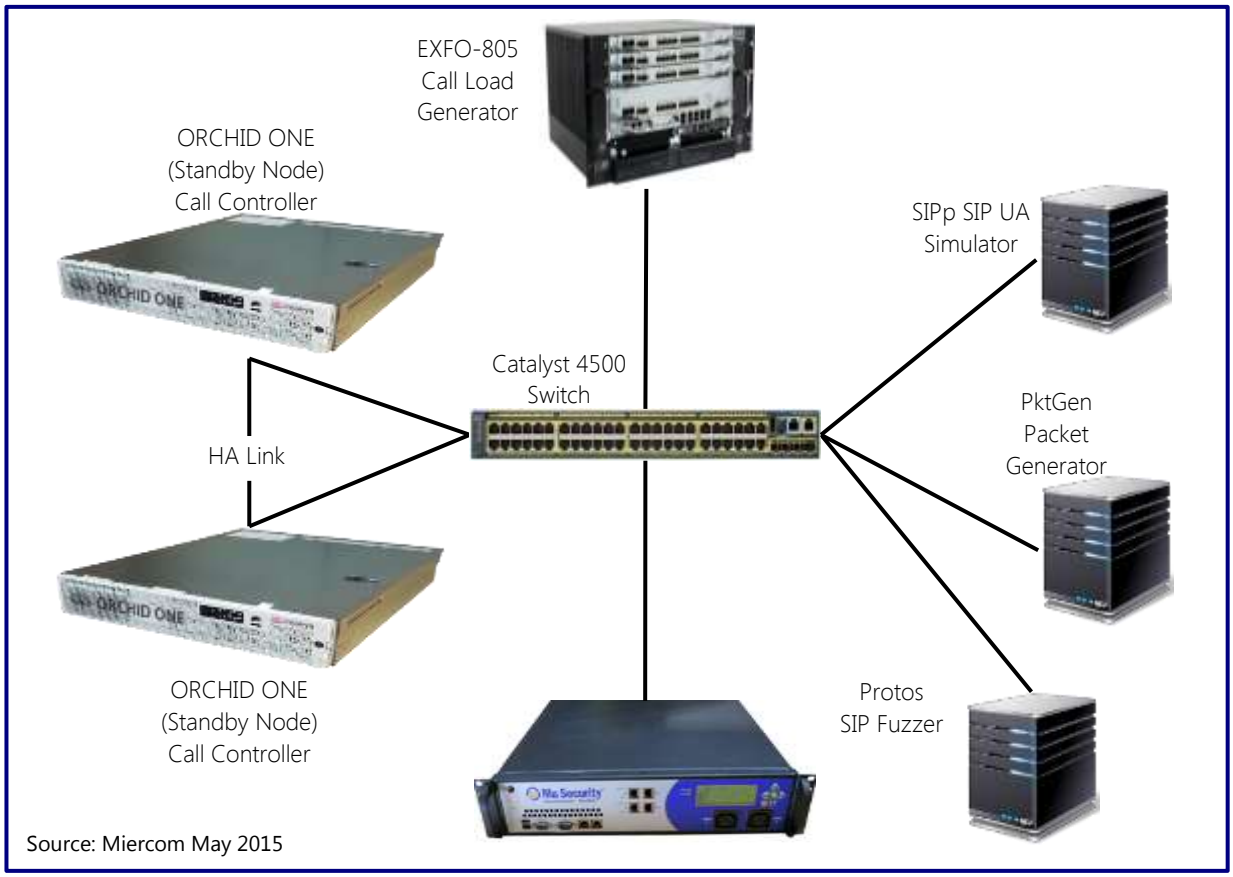
The Enhanced Session Border Controller (eSBC) Orchid One is a 2U rack-mount appliance that is deployed primarily in interconnect SBC roles, although it includes all the features and functionality of an access SBC as well.

The unit supports up to four 1 or 10-Gigabit/s Ethernet connections, a requirement given the high volume of calls supported: 100,000 concurrent calls with full RTP media. eSBC Orchid One comes with 2 x 300GB RAID1 hard disk and up to 128GB RAM.

The eSBC Orchid One supports 1:1 box redundancy to maximize uptime, including stateful session recovery, and features that make the eSBC Orchid One, one of the most resilient SBCs we have tested, including Ethernet link bonding for bandwidth aggregation and link-failure recovery. Many of these features were exercised in this testing.

Up to two optional cards can be configured within the system, which facilitate transcoding of 7,500 voice and 750 video channels each.

3.0 Test bed Diagram



How We Did It

Enhanced Session Border Controller (eSBC) Orchid One, running eSBC Release V 1.7.0.197, was evaluated in this test. All of the eSBC Orchid One's fiber and copper interfaces were used for SIP signaling, RTP traffic and security robustness tests.

Traffic from the subscriber/user organization was simulated by SIP traffic generators from Canada-based EXFO, and from SIPp servers. SIPp is an open source SIP call generator. The EXFO gear also performed automated quality assessments of the VoIP calls (R-Factor and MOS ratings).

The testing used four ports on an EXFO Model 805 and up to 5 SIPp interfaces depending on the specific test. The EXFO systems ran firmware/software version 9.3. The EXFO and SIPp call generators delivered SIP calls over IPv4 and/or IPv6, depending on the test. Registration, call signaling and set-up were accomplished over secure, encrypted TLS (Transport Layer Security) connections or regular, non-encrypted SIP/UDP connections.

The Test Bed Diagram shows the logical connectivity between key functional and test nodes. Much of the service-provider functionality and test equipment including PCKgen, SIPp and Protos ran as discrete partitions on a powerful VM server.

We used Spirent's Mu system for six different DoS and SIP torture tests. PCKgen, SIPp and Protos, all Open Source tools, were used for SIP call generation and bulk SIP/UDP packet generation.

The eSBC Orchid One tested was controlled by an eSBC management console. The EXFO QA-805 was controlled by its associated Navtel management console. Security and DoS prevention features on the eSBC Orchid One were configured in accordance with the vendor's configuration guide.

The tests in this report are intended to be reproducible by customers who wish to recreate them using the appropriate test and measurement equipment. Current or prospective customers interested in repeating these results should contact reviews@miercom.com for details on the configurations applied to the device under test and the test tools used in this evaluation. Miercom recommends customers conduct their own needs analysis for Session Border Control functionality and test specifically for the environment they expect to support, prior to making a product selection.

List of Equipment Used

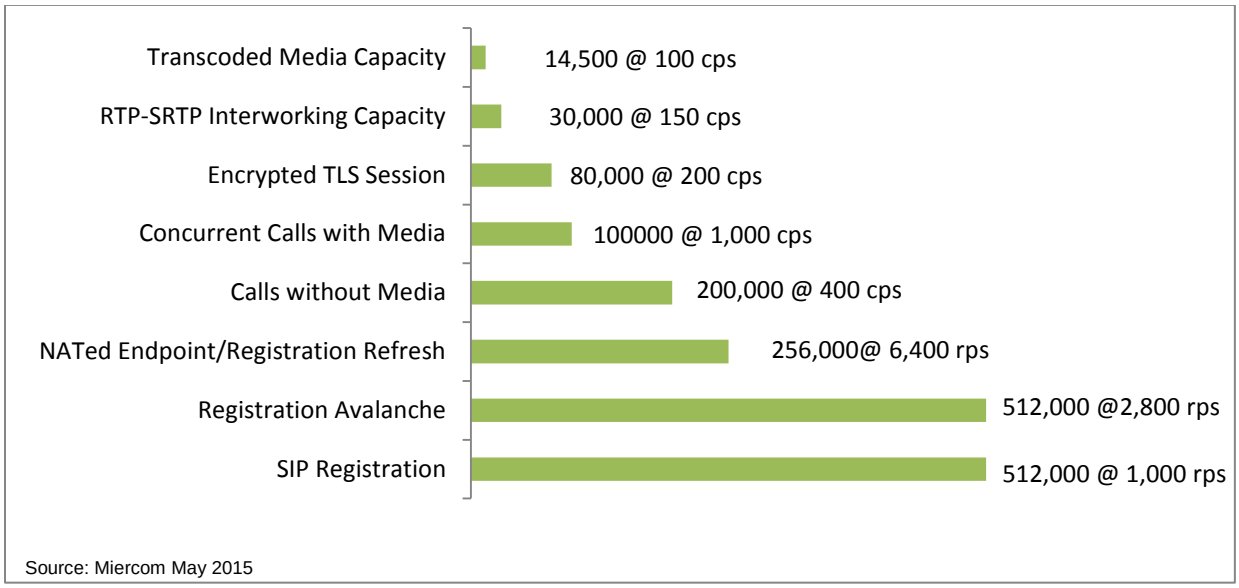
Name	Function	Version
Enhanced SBC Orchid One	Device Under Test (DUT)	V 1.7.0.197
EXFO QA-805	Wireless, IMS and VoIP test tool; traffic, call and load generation	Release 9.3
PktGen	Open source tool; Bulk packet generator	V 2.7.7
SIPp SIP UA Simulation	Open source tool; SIP call-traffic generation	v 3.4
Spirent Mu-8000/Studio	Security tool; DoS and malicious attack tool	Mu Test Suite 6.5.2.r48322
PROTOS	Open source tool SIP Fuzzer	V 1.4
Wireshark	Packet and traffic analysis	Release 1.99.5

4.0 SBC Performance

The eSBC Orchid One sustained high volumes and rates of call processing with low-to-moderate system resource usage, and proved to be remarkably resilient to the malicious attacks launched against it.

Our testing exercised and assessed aspects of the eSBC Orchid One that address SIP signaling and call performance, security, reliability, and resilience. The eSBC Orchid One exhibited excellent resilience and continued performance and call quality under all the high-duress scenarios tested, including six DoS attacks.

Fig 1: Overview of Confirmed eSBC SIP Signaling and Call-Handling Performance



Key security and efficacy tests performed on the eSBC Orchid One

Malicious attacks that were launched and successfully averted include:

- SIP Invite flood from a spoofed IP address
- SIP "Fuzzing" – malformed SIP message attack
- Invites from an unconfirmed zone
- Rogue RTP packets (from EXFO)
- Malformed and mutated messages, from Protos
- UDP packets at high volume (to fill bandwidth)
- Denial of Service (DoS) attack: UDP packet storm
- DoS attack by Spirent Mu system

Other resiliency, reliability and High Availability features tested and verified:

- Session Detail Record (SDR) and tracing for every call
- Routing based on SLA (Service Level Agreement)
- Robust SAF (Signalling Adaptation Framework)
- End-to-end media Quality of Service (QoS)
- Node failover test

5.0 SIP Signaling and Call Performance Tests

5.1 Registration Performance

Description

Two call generators, EXFO and SiPp, simultaneously sent streams of 256,000 registration requests each to the eSBC Orchid One, to determine whether it could process and maintain a total of 512,000 registrations.

Purpose

To verify the products ability to process and sustain 512,000 registrations, within CPU and memory thresholds.

Expected Results

That the eSBC Orchid One operates properly and CPU and memory usage does not exceed a reasonable threshold while achieving the maximum registration performance point without any error.

Results

SIP Registration

Registrations	512,127
CPU Usage	6%
Memory Usage	20.1 GB

5.2 Concurrent Calls with Full RTP Media

Description

The EXFO system generated 100,000 concurrent calls at 100 cps, with full RTP G.729 media.

Purpose

To confirm whether the eSBC Orchid One can establish and maintain 100,000 calls with media, without calls dropping, and with CPU and memory utilization within thresholds.

Expected Results

That the eSBC Orchid One operates properly, that CPU usage does not exceed the flow-control threshold of 75 percent, and that memory usage does not exceed threshold of 85 percent.

Results

Concurrent Calls with Full RTP Media

Concurrent Calls	100,000 @ 1000 cps
Call Duration	100 sec
Media Codec	G.729
Delay	0.018ms
Lost Calls	0
Jitter	0
CPU Usage	47%
Memory Usage	29 GB
R-Factor (0-100)	81.4
MOS (1-5)	4.07

5.3 Calls without Media

Description

We used SIPp to send 200,000 UAC (user agent - client) calls without RTP Media, or five-minute duration, and received all UAC calls at SIPp UA servers

Purpose

To confirm that eSBC Orchid One can switch and maintain 200,000 no-media calls without calls dropping, and with CPU and memory utilization within thresholds.

Expected Results

That the eSBC Orchid One operates properly and CPU usage does not exceed the flow-control threshold of 75 percent and memory usage does not exceed threshold of 85 percent while achieving maximum no-media calls without any call drops or errors.

Results

Calls without Media

Calls	200,000 @ 400 cps
Call Duration	500 sec
CPU Usage	18%
Memory Usage	26 GB

5.4 Transcoded-Media Call Capacity and Quality

Description

EXFO test equipment places VoIP calls with full RTP media between groups of simulated mobile-phone users. Callers and called users use different codecs and the eSBC Orchid One is required to transcode each call between G.729 and G.711 – 7,000 in one direction and 7,000 in the other. A total of 14,500 transcoded calls were placed and observed for 40 minutes.

Purpose

To confirm that the eSBC Orchid One can transcode 14,500 calls between simulated mobile callers using G.729 and G.711 codec, while CPU utilization remain within threshold. For this test we used two DSP (Digital Signal Processor) cards to transcode call between UAC and UAS.

Expected Results

That the eSBC Orchid One operates properly, and CPU usage does not exceed the flow-control threshold of 75 percent, while transcoding 14,500 calls without any errors.

Results

Transcoded G.711 Codec Media Capacity & Quality

Calls	14,500 @ 100 cps
Call Duration	145 sec
Media Codec	G.711
Total Run Duration	40 min
CPU Usage	13%
Memory Usage	21.4 GB
R-Factor (1-100)	92.5
MOS (1-5)	4.39

Transcoded G.729 Codec Media Capacity & Quality

Calls:	14,500 @ 100 cps
Call Duration	145 sec
Media Codec	G.729
Total Run Duration	40 min
CPU Usage	14%
Memory Usage	23 GB
R-Factor (1-100)	81.7
MOS (1-5)	4.08

5.5 Network Address Translated Endpoints/Re-Registration

SBCs configured for access deployment often need to support network address translation (NAT) traversal. This is an added network security measure where the IP address of SIP user endpoints are obscured, and calls out onto the network us a different, temporary address assigned by the NAT.

Description

With EXFO, we registered 192,000 subscribers at 1,000 rps. After registration of all 192,000 subscribers, we set 30-second refresh registrations for all 192,000 subscribers, which resulted in 6,400 re-registrations per second.

Purpose

To confirm that the eSBC Orchid One can typically establish and maintain these IP translations through the NAT, and in so doing maintain endpoint IP connections for incoming and outgoing calls.

Expected Results

That the eSBC Orchid One operates properly and CPU usage does not exceed the flow-control threshold of 75 percent while doing NAT traversal and fast registration without any error.

Results

NAT'ed Endpoints / Fast Registration Refresh

Subscribers	192,000 @ 6,400 rps
Refresh Rate	30 sec
Media Codec	G.711
CPU Usage	29%
Memory Usage	17.7 GB

5.6 Encrypted TLS sessions

Description

SIPp test equipment issues a TLS and a SIP registration request to the eSBC Orchid One from each of up to 80,000 simulated SIP user endpoints.

Purpose

To confirm the eSBC Orchid One can support secure access via TLS, and via encrypted TLS connections the registration of a large number of simulated SIP subscribers, and that it can sustain this number within acceptable levels of CPU and memory utilization.

Expected Results

That the eSBC Orchid One operates properly and supports up to 80,000 registrations, all via secure TLS access connections without any error.

Results

Encrypted TLS Session

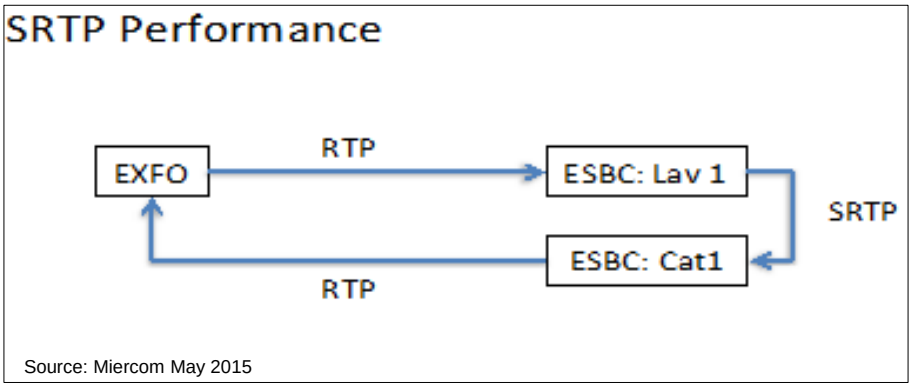
Calls	80,592 @ 200 cps
Media	None
CPU Usage	20%
Memory Usage	20.5 GB

5.7 RTP-SRTP Interworking Capacity

Description

Two eSBC Orchid Ones were used for this test due to insufficient Secure RTP (SRTP) capacity of the EXFO tool. The EXFO system generated 30,000 RTP calls, and encrypted SRTP connections were set-up between the eSBC Orchid One nodes (see diagram). The EXFO system generated RTP calls to the first eSBC, which encrypted them into SRTP calls and sent them to the second eSBC. The second eSBC converted (decrypted) the SRTP calls back to RTP and delivered them to the EXFO system.

Figure 2: RTP-SRTP Diagram



Purpose

To verify that eSBC Orchid One could successfully set up and maintain 30,000 simulated Real-time Protocol to/from Secure Real-Time (RTP-SRTP) media calls.

Expected Results

That the eSBC Orchid One operates properly while doing RTP-SRTP transformation without any errors.

Results

RTP-SRTP Internetworking Capacity

Calls	30,000 @ 150 cps
Call Duration	200 sec
CPU Usage	42%
Memory Usage	19 GB
R-Factor (1-100)	81.3
MOS (1-5)	4.07

5.8 MOS code for Different Media

Description

From EXFO we placed one call of each on these media codecs:

a. G.711 b. G.729 c. G.723

We observed the MOS and R-factor for each codec call.

Purpose

To verify performance of specific codecs.

Expected Results

That the eSBC Orchid One operates properly with different codecs and maintains good MOS and R-factor ratings.

Results

G.711 Codec Quality

Calls	1
Media Codec	G.711
Jitter	0
Delay	0
R-Factor (1-100)	93.2
MOS (1-5)	4.40

G.729 Codec Quality

Calls	1
Media Codec	G.729
Jitter	0
Delay	0
R-Factor (1-100)	81.04
MOS(1-5)	4.07

G.723 Codec Quality

Calls	1
Media Codec	G.713
Jitter	0
Delay	0
R-Factor (1-100)	76.8
MOS (1-5)	3.89

5.9 Registration Avalanche

Description

From EXFO and SIPp at 2,000 and 800 rps respectively, we registered 512,000 subscribers.

Purpose

To verify that the eSBC Orchid One can register all 512,000 subscribers within a reasonably fast timeframe, as would be the case after a power loss/restoral (non-High Availability) reboot scenario.

Expected Results

That the eSBC Orchid One operates properly and CPU usage does not exceed the flow-control threshold of 75 percent while doing registration of all 512,000 subscribers in just over three minutes.

Results

Registration Avalanche

Subscribers	512,000 @ 2,800 rps
CPU-Usage	42%
Memory Usage	19 GB
Errors	None

5.10 IPv4-IPv6 Translation

Description

Two systems were set up, one using IPv4 addressing and the other with IPv6. The eSBC Orchid One was evaluated for its ability to translate calls from IPv4 to IPv6.

Purpose

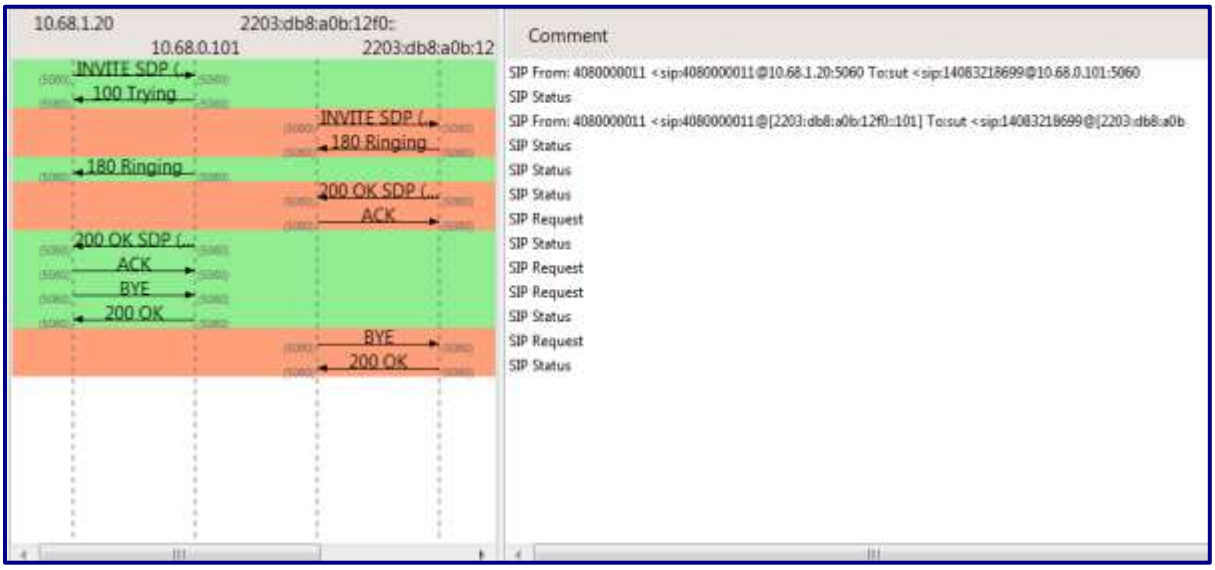
To test its compatibility between the two IP standards.

Expected Results

That the product will act as a compatibility layer between the system which uses IPv4 and the other which uses IPv6 addressing and protocol format.

Results

Figure 3: Protocol Diagram from Call over IPv4<->IPv6Translated Path



This figure shows the screen shot of Orchid One's call connection process between a system running IPv4 and a remote system running IPv6. The Cataleya Orchid One handles the addressing interconnection by providing a transparent bridge between these two protocols.

Results

IPv4-IPv6 Translation

Calls	8 @ 2 cps
Call Loss	0%
R-Factor (1-100)	81.4
MOS (1-5)	4.07

6.0 Security and efficacy tests

6.1 Rogue RTP

Description

Some valid RTP packets were sent to eSBC Orchid One from the EXFO tool, for a call that had been released 10 seconds earlier. This testing with rogue RTP was done while the eSBC Orchid One was handling 20,000 regular concurrent calls with 500 cps.

Purpose

To verify that the any open ports used for calling are properly closed after call is released.

Expected Results

That the eSBC Orchid One operates properly and any extra RTP media packets generated by UAC should be dropped at the data plane layer.

Results

Rogue RTP

Concurrent Calls	20,000 @ 500 cps
Call Duration	40 sec
Extra RTP Traffic Duration	10 sec
Extra Traffic Dropped	100%

6.2 ICMP Echo Request

Description

An Internet Control Message Protocol (ICMP) Echo Request, known as a ping, is a network administration message that tests reachability by sending packets to a target system and expecting a response. While waiting, it measures the time from transmission to reception, or "round-trip" time and records packet loss, if any.

Purpose

This is a type of DoS (Denial-of-Service) attack where the eSBC Orchid One is flooded with ICMP Echo Requests from the Spirent Mu system. This flood of requests was sent to the calling port, or main port, of the SBC to observe performance and call quality while filtering traffic. The testers then note if there were any dropped calls or errors.

Expected Results

The eSBC Orchid One should not have any dropped calls or errors, and the call performance and quality should remain the same as if there was no flood of pings.

Results

ICMP Echo Request

ICMP/s	100 @ 100,000 pps
Calls	100,000 @ 1,000 cps
Test Duration	10 min
Call Error	None
Control Plane CPU Usage	52%
Data Plane CPU Usage	55.67%
CPU Usage Increase	+3.67%
Memory Usage	23.4 GB
R-Factor (1-100)	81.4
MOS (1-5)	4.07

6.3 UDP Packet

Description

From the PktGen we generated and sent one million UDP packets/sec with 50-byte payload to port 3, a redundant 10GE interface of the eSBC Orchid One. While receiving this UDP packet attack the eSBC Orchid One was handling 100,000 concurrent calls at 1,000 cps.

Purpose

To verify that the eSBC Orchid One can sustain and maintain concurrent calls while being attacked on a redundant interface.

Expected Results

That the eSBC Orchid One operates properly and CPU usage does not exceed the flow-control threshold of 75 percent while maintaining 100,000 concurrent calls and receiving new ones at a rate of 1,000 cps.

Results

UDP Packet

Concurrent Calls	100,000 @ 1,000 cps
Payload Packet Size	50 Bytes @ 1,000,000 pps
Call Duration	100 sec
Media Codec	G.729
Call Error	None
Control Plane CPU Usage	52%
Data Plane CPU Usage	62%
CPU Usage Increase	+10%
Memory Usage	24.5 GB
R-Factor (1-100)	81.4
MOS (1-5)	4.07

6.4 Malformed Message Attack

Description

With the EXFO we placed 50,000 regular calls at 500 cps. Then we modified the SIP packet header length on the SIPp traffic generator to 20 bytes, to confuse the system with an improperly short header size. This malformed-message attack was then launched while the eSBC Orchid One was maintaining 50,000 concurrent calls and handling 500 cps.

Purpose

To verify that the eSBC Orchid One can sustain and maintain concurrent calls while receiving a malformed-message attacked from SIPp.

Expected Results

That the eSBC Orchid One operates properly and CPU usage does not exceed the flow-control threshold of 75 percent while maintaining 50,000 calls at 500 cps while under malformed message attack.

Results

Malformed Message Attack

Packet Header Length	20 Bytes
Payload Data Length	Random
Calls	50,000 @ 500 cps
R-Factor (1-100)	81.4
MOS (1-5)	4.07

6.5 Invite from Unconfirmed Zone

Description

With EXFO we generated 100,000 regular concurrent calls at 1,000 cps. At the same time, from SIPp we sent 1,000 call set-up requests per second, where the destination IP was the same as UAS (the destination of legitimate calls) but the source IP was different than the UAC (not in the known client community).

Purpose

To verify that the eSBC Orchid One can identify any unconfirmed zone and drop those call requests.

Expected Results

That the eSBC Orchid One operates properly and CPU usage does not exceed the flow-control threshold of 75 percent while maintaining 100,000 calls at 1,000 cps during the invitation from unconfirmed zone.

Results

Invite from Unconfirmed Zone

Calls	100,000 @ 1,000 cps
Extra Packets Dropped	100%
Control Plane CPU Usage	51%
Data Plane CPU Usage	55%
CPU Usage Increase	+4%
Memory Usage	22 GB
R-Factor (1-100)	81.4
MOS (1-5)	4.07

6.6 Invite from Spoofed IP

Description

With EXFO we generated 50,000 long-duration regular calls. Then, after the calls were set-up, we sent 5,000 cps from SIPp, pretending to be unwanted callers. The system was configured to allow up to 50 cps from such callers, with a tolerance of 50 percent – that is, a tolerance of 75 cps. Any source (legitimate or spoofed) attempting to place calls beyond 75 cps was to be blocked and black listed.

Purpose

To verify that the eSBC Orchid One can identify any irregular calling pattern notify the respective administrator.

Expected Results

That the eSBC Orchid One operates properly and CPU usage does not exceed the flow-control threshold of 75 percent while maintaining 50,000 long-lasting calls and receiving a high volume of call requests (Invites) from spoofed IP source addresses.

Results

Invite from Spoofed IP

Packets per second	100,000 pps
Calls	100,000 @ 1,000 cps
Call Error	None
Control Plane CPU Usage	53%
Data Plane CPU Usage	55%
CPU Usage Increase	+2%
Memory Usage	24.6 GB
R-Factor (1-100)	81.4
MOS (1-5)	4.07

6.7 Attack Traffic to Fill the Bandwidth

Description

From the PktGen we generated one million UDP packets/sec, each with 1,000-byte payload, targeted to port 3 – a redundant 10GE interface of the eSBC Orchid One. 100,000 concurrent calls were running at 1,000 cps when launching this UDP-packet attack.

Purpose

To verify that the eSBC Orchid One can sustain and maintain concurrent calls while getting full bandwidth attacked on redundant interface.

Expected Results

That the eSBC Orchid One operates properly and usage does not exceed the flow-control threshold of 75 percent while maintaining 100,000 calls at 1000 cps.

Results

Attack Traffic to Fill Bandwidth

Packet Length	1,000 Bytes @ 1,000,000 pps
Data Plane CPU Usage	64%
R-Factor (1-100)	81.4
MOS (1-5)	4.07

6.8 Malformed Mutation Attack from Protos

Description

From the Protos tool we issued malformed SIP messages. The eSBC Orchid One system was configured to allow two malformed SIP messages per second, with 200 percent tolerance – that is, up to six malformed SIP messages per second. We ran 50,000 regular calls at 500 cps from the EXFO system, while delivering the malformed mutation attack from the Protos.

Purpose

To verify that the eSBC Orchid One can sustain and maintain concurrent calls while getting malformed SIP messages

Expected Results

That the eSBC Orchid One operates properly and CPU usage does not exceed the flow-control threshold of 75 percent while maintaining 50,000 calls at 500 cps.

Results

Malformed Mutation Attack from Protos

Malformed SIP/second	2
Tolerance	200% or 6 Malformed
Calls	50,000 @ 500 cps
Media Codec	G.729
Call Error	None
CPU Usage	27%
Memory Usage	26.1 GB
R-Factor (1-100)	81.4
MOS (1-5)	4.07

6.9 Large Ping Flood

Description

A ping, or Internet Control Message Protocol (ICMP) Echo Request, sends packets to a target host and waits for a response, while measuring round-trip time of transmission and packet loss, if any. A flood of pings is sent from the Spirent Mu test system to the SBC, to determine how the eSBC Orchid One performs, and if any data is lost in the process.

Purpose

To determine if the eSBC Orchid One would sustain and maintain 100,000 calls and 100,000 pps at 1,000 cps without any being dropped, or having any errors, while remaining within a reasonable CPU and memory usage threshold.

Expected Results

No calls, or message packets, should be lost. The eSBC Orchid One should function normally, and CPU usage should remain relatively the same.

Results

Large Ping Flood

Packets per second	100,000 pps
Calls	100,000 @ 1,000 cps
Call Error	None
Control Plane CPU Usage	53%
Data Plane CPU Usage	55%
CPU Usage Increase	+2%
Memory Usage	24.6 GB

6.10 TCP SYN Flood

Description

The 6-bit Synchronize (SYN) flag in the 20-byte TCP headers is set when a host system sends a packet, to indicate to the target system that it will be receiving a packet. During an attack of TCP SYN Flooding, the packets have their SYN flag set, but use a spoofed source IP address. This can overwhelm a system since the source address isn't known and the system is unable to properly respond, or to send a set Acknowledge (ACK) flag to the server. This can cause the packet to appear "lost".

A flood of TCP SYN flagged packets are sent from the Spirent Mu towards the eSBC Orchid One to determine device performance, lost information or errors, and call quality.

Purpose

To verify that the eSBC Orchid One remains stable and can sustain the set parameter of calls at 1,000 cps while flooded with TCP SYN attack.

Expected Results

The eSBC Orchid One should drop these SYN-flagged packets at the data plane level since they have a spoofed source. The flood of SYN flagged packets should not affect the call performance, or quality, and have minimal impact, if any, on CPU usage.

Results

TCP SYN Flood

Calls	100,000 @ 1,000 cps
Call Error	None
TCP Packets Dropped at Data Plane Level	100%
Control Plane CPU Usage	54%
Data Plane CPU Usage	55%
CPU Usage Increase	+2%
Memory Usage	25.2 GB
R-Factor (1-100)	81.4
MOS (1-5)	4.09

6.11 TCP SYN-FIN Flood

Description

The 6-bit Synchronize (SYN) flag in 20-byteTransmission Control Protocol (TCP) headers are set when the host system sends a packet, to indicate to the target system that it will be receiving a packet. The server acknowledges the packet by setting the 6-bit ACK flag, and then sends its own packet, with the 6-bit Finish (FIN) flag set, to indicate that the client has closed the connection. During an attack of TCP SYN-FIN Flooding, the packets have set SYN and FIN flags but a spoofed source IP address. This can overwhelm the target system since the source address doesn't exist and the excess packets with FIN flag set are simply there to bypass security systems that otherwise only block other packet types.

A flood of TCP SYN-FIN flagged packets are sent from the Spirent Mu, for 10 minutes, towards the eSBC Orchid One to determine device performance, information loss, and errors when, or if, dropping these types of TCP packets.

Purpose

To verify that the eSBC Orchid One remains stable and can sustain the set parameter of calls at 1,000 cps while flooded with TCP SYN-FIN attack.

Expected Results

The eSBC Orchid One should drop these SYN-FIN flagged packets at the data plane level since they have a spoofed source. The flood of SYN-FIN flagged packets should not affect the call performance, or quality, and have minimal effect, if any, on the CPU usage.

Results

TCP SYN-FIN Flood

Packets per second	100,000 pps
Calls	100,000 @ 1,000 cps
Flood Duration	10 min
TCP Packets Dropped at Data Plane Level	100%
Control Plane CPU Usage	54%
Data Plane CPU Usage	55%
CPU Usage Increase	+1%
Memory Usage	25.7 GB

6.12 Denial-of-Service (DoS) Test for UDP

Description

From the Spirent Mu system we sent 100,000 UDP packets per second while 100,000 calls were running at 1,000 cps.

Purpose

To verify the system's resistance under DoS attack.

Expected Results

That the eSBC Orchid One operates properly and the CPU usage does not exceed the flow-control threshold.

Results

DoS Test for UDP

Packets per second	100,000 pps
Calls	100,000 @ 1,000 cps
DoS Attack Duration	10 min
Call Error	None
Control Plane CPU Usage	52%
Data Plane CPU Usage	58.8%
CPU Usage Increase	+6.8%
Memory Usage	26.4 GB
R-Factor (1-100)	81.4
MOS (1-5)	4.09

6.13 DoS Test for Large IP Fragments

Description

From the Spirent Mu system large IP fragmented packets are sent.

Purpose

To verify the system's resistance under DoS attack.

Expected Results

That the eSBC Orchid One operates properly and the CPU usage does not exceed the flow-control threshold.

Results

DoS Test for Large IP Fragments

Calls	100,000 @ 1,000 cps
DoS Attack Duration	10 min
Call Error	None
Control Plane CPU Usage	54%
Data Plane CPU Usage	59%
CPU Usage Increase	+5%
Memory Usage	22 GB
R-Factor (1-100)	81.4
MOS (1-5)	4.09

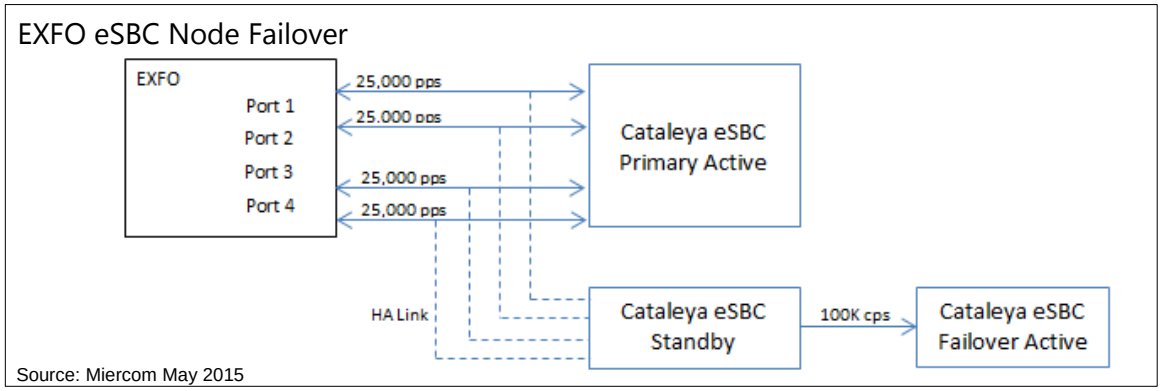
7.0 Resiliency, Reliability and High Availability

7.1 Node Failover Test

Description

Multiple nodes of a system like the eSBC Orchid One provide redundancy; clustering of two or more computers avoids single points of failure. Clustering entails failure detection and the ability to restart all operations on another system, also known as failover.

Figure 4: Node Failover Diagram



25,000 pps on four ports are simultaneously delivered to the primary active node. When the primary active node fails, a standby node is linked to the failed primary node by a high availability link. This link enables the standby node to handle the load and becomes the active node during failover.

In this case, two systems are deployed in an Active/Passive node configuration. Full redundancy is only apparent when the primary (active) node fails. Failing the primary node enabled our assessment of the system's failover process, performance and call quality.

Purpose

To verify that the products function in full redundancy so that one eSBC Orchid One remains active if the other one fails.

Expected Results

That the eSBC Orchid One Standby node becomes the primary active node to handle the full load of 100,000 calls and does not exceed a reasonable threshold of CPU and memory usage.

Results

Node Failover Test

Calls	100,000 @ 800 cps
Calls after Active Node shutdown	2,000 @ 1,000 cps
Media Codec	G.729
Call Error	Single Missed Call
Control Plane CPU Usage	47%
Failover CPU Usage	49%
CPU Usage Increase	+2%
Memory Usage	21.2 GB
Failover Memory	21.4 GB
R-Factor (1-100)	81.4
MOS (1-5)	4.07

We generated 1,000 cps to make 100K concurrent calls. When 80K calls connected we gracefully shutdown the active node to send all concurrent calls to the standby node. Only one call failed during this test. The remaining 20,000 calls were connected successfully and transferred to the standby node.

7.2 End to End Media QoS

Description

Quality of service monitoring by the eSBC Orchid One was tested for transparent visibility of system control and data flow. Features of focus were the eSBC Orchid One dashboard and analysis deck that facilitate management of the network state and associated system details.

Purpose

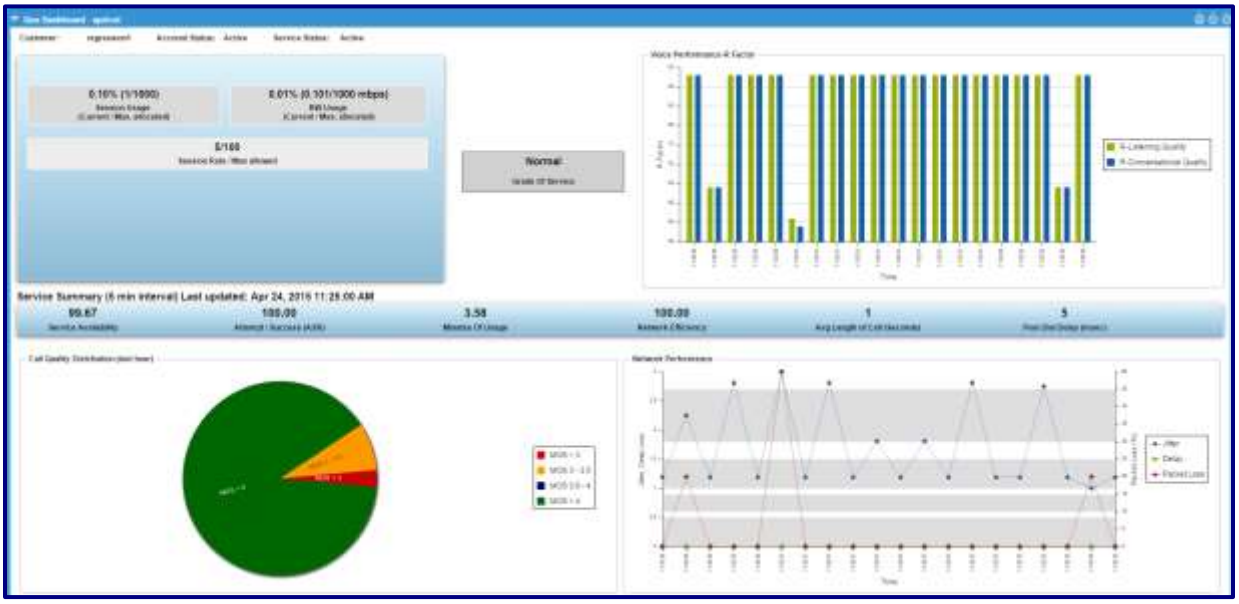
To evaluate the subjective experience of the eSBC Orchid One device, and its ability to extract relevant data in a clear and concise manner.

Expected Results

To encounter and work within a simplified, visual-based environment that yields accurate data in table and graph formats.

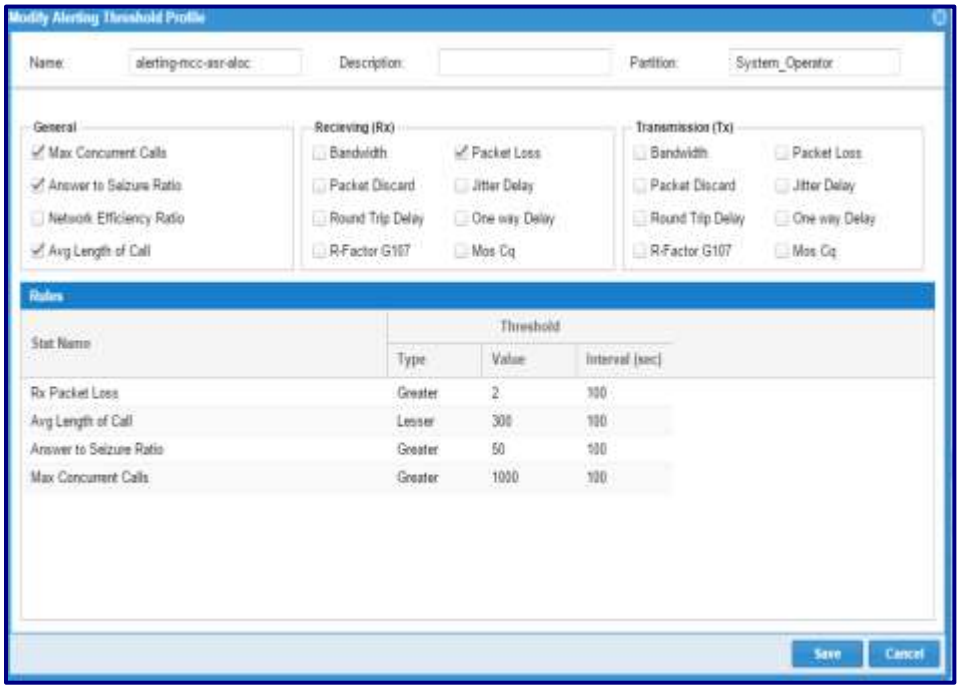
Observations

Figure 5: QoS Dashboard



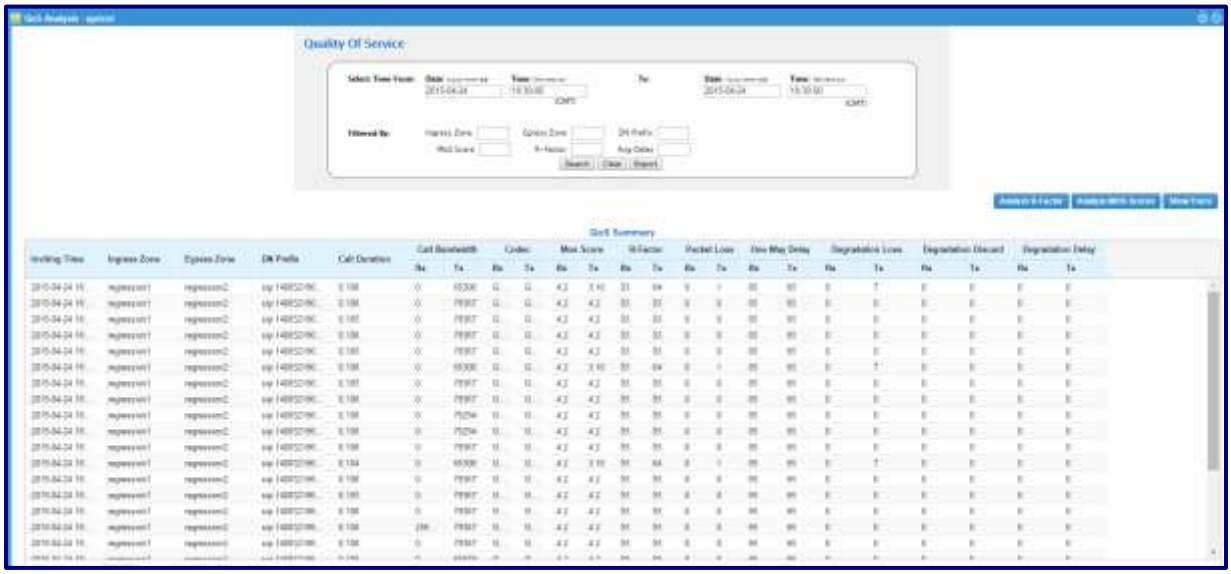
The QoS dashboard provides a comprehensive visual of the state of the network, managed by Orchid One. All call quality measures and connection flows can be seen throughout testing.

Figure 6: Threshold Profile



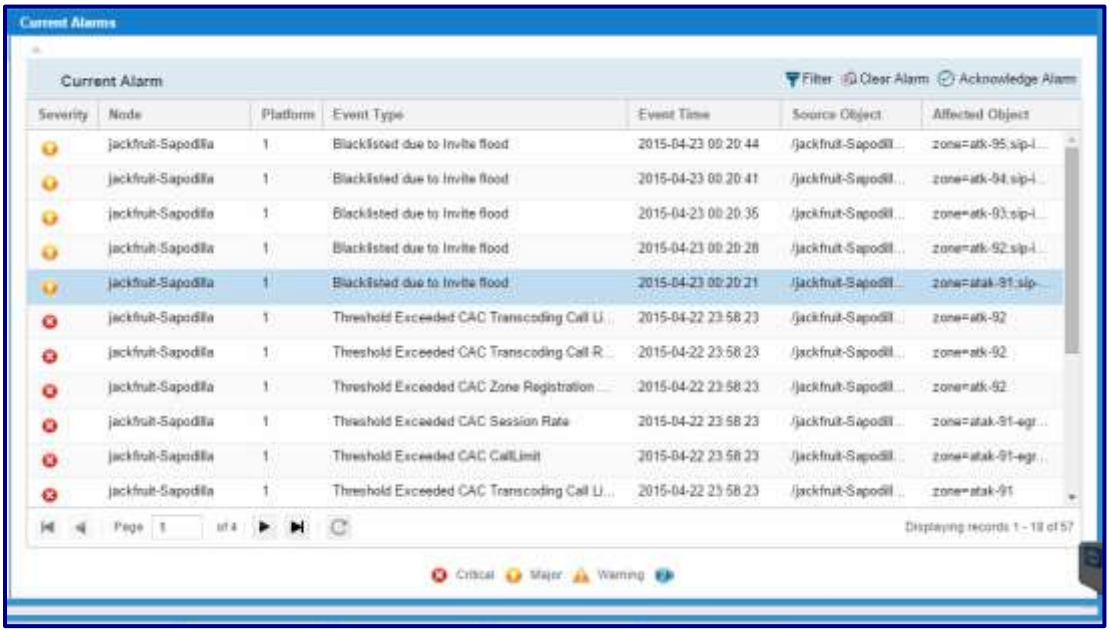
A user can create a list of statistics by clicking the checkboxes of desired parameters.

Figure 7: QoS Analysis



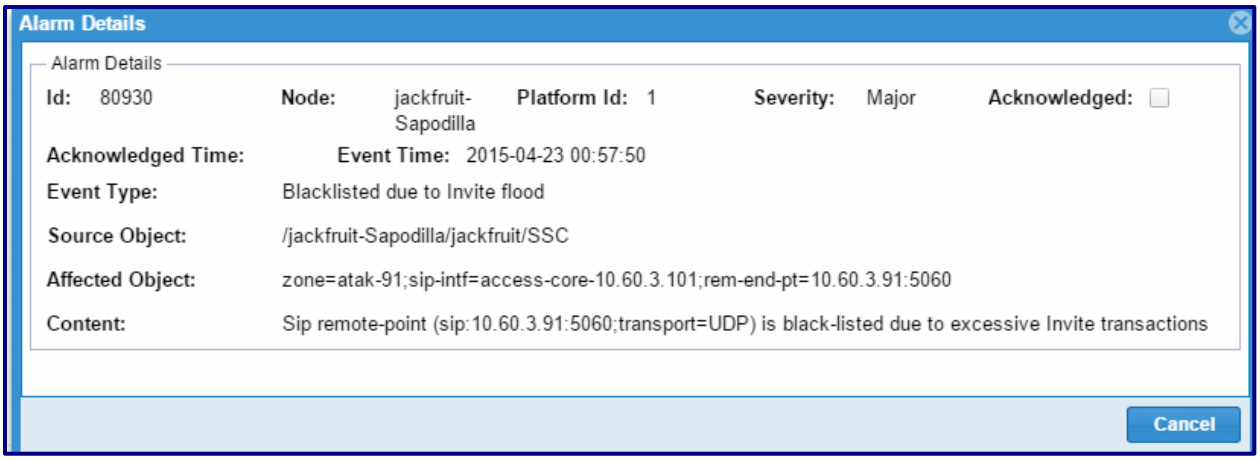
At each stage, drilling down is simple to get tables or graphs to show aspects of the associated system details.

Figure 8: Blacklist Screen



By setting thresholds low for a DoS style attack, and setting up to blacklist the originating node of such an attack, we could see how all traffic was stopped from that node when thresholds were exceeded.

Figure 9: Blacklist Notification



The product brings up an alarm notification if a blacklist occurs.

7.3 Robust SAF (Signaling Adaptation Framework)

Description

From the eSBC Orchid One graphical user interface, we manipulated call headers to accommodate third-party service providers' conventions.

Purpose

To verify interoperability between service providers by dynamically changing call headers.

Expected Results

That the eSBC Orchid One can make calls between different service providers with different header options.

Results

Robust SAF

Calls	100,000 @ 1,000 cps
DoS Attack Duration	10 min
Control Plane CPU Usage	53%
Data Plane CPU Usage	58.8%
CPU Usage Increase	+5.8%
Memory Usage	22.3 GB
R-Factor (1-100)	81.4
MOS (1-5)	4.09

7.4 Other Features on the eSBC Orchid One

Description

Observing capabilities of the eSBC Orchid One for the following features:

- Service Level Agreement (SLA) in which the administrator can readily see, for a particular set of customers, call response time, latency, jitter and packet loss;
- Session Detail Record (SDR), which can be used to trace any single call;
- A Wizard for configuration, which can be used to create policies, and to manage SIP message differences across systems.

Purpose

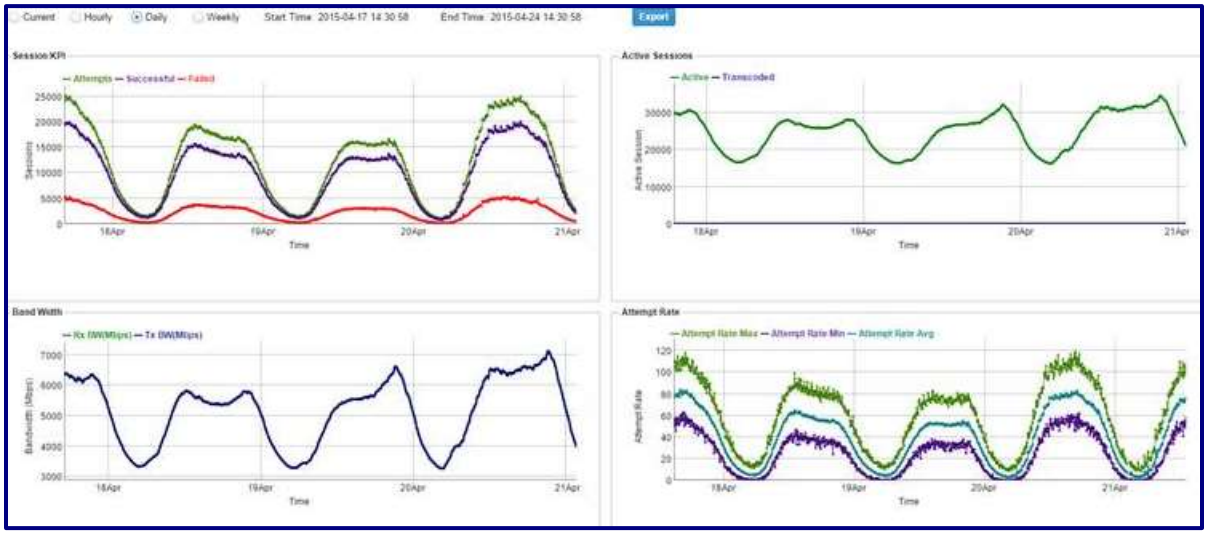
To determine how various policies can be created that are sensitive, for example, to call quality or bandwidth, and that could control system routing.

Observations

In the eSBC Orchid One, we saw in the various dashboards for visibly showing call quality.

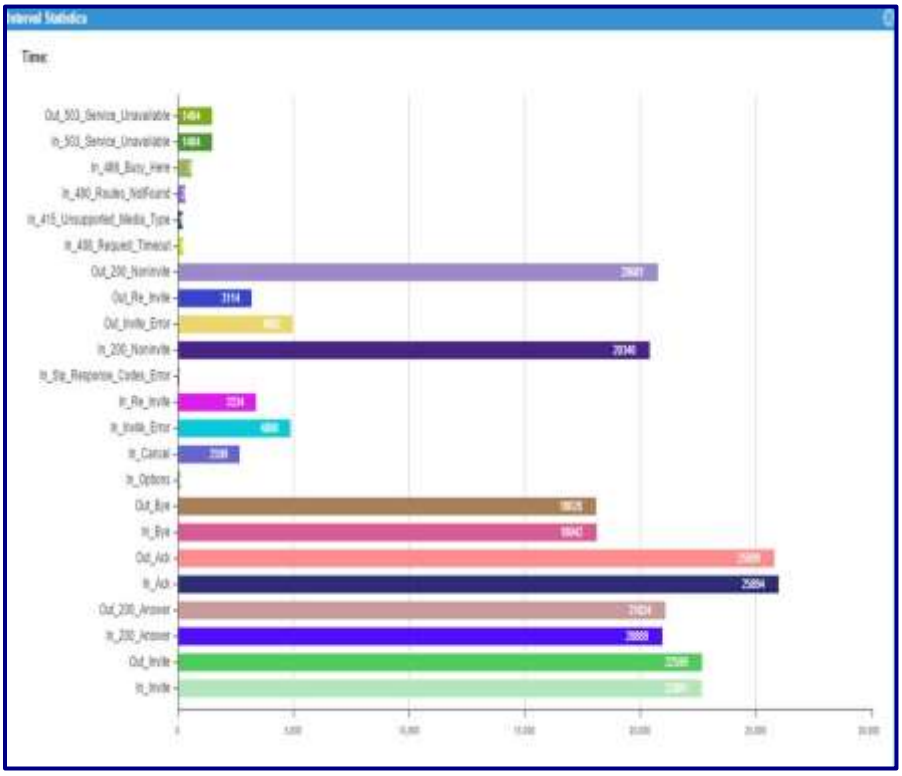
Message content is traceable but is turned off by default. This may be used to call data to be traced and played back to check for vocal quality.

Figure 10: SIP Charts



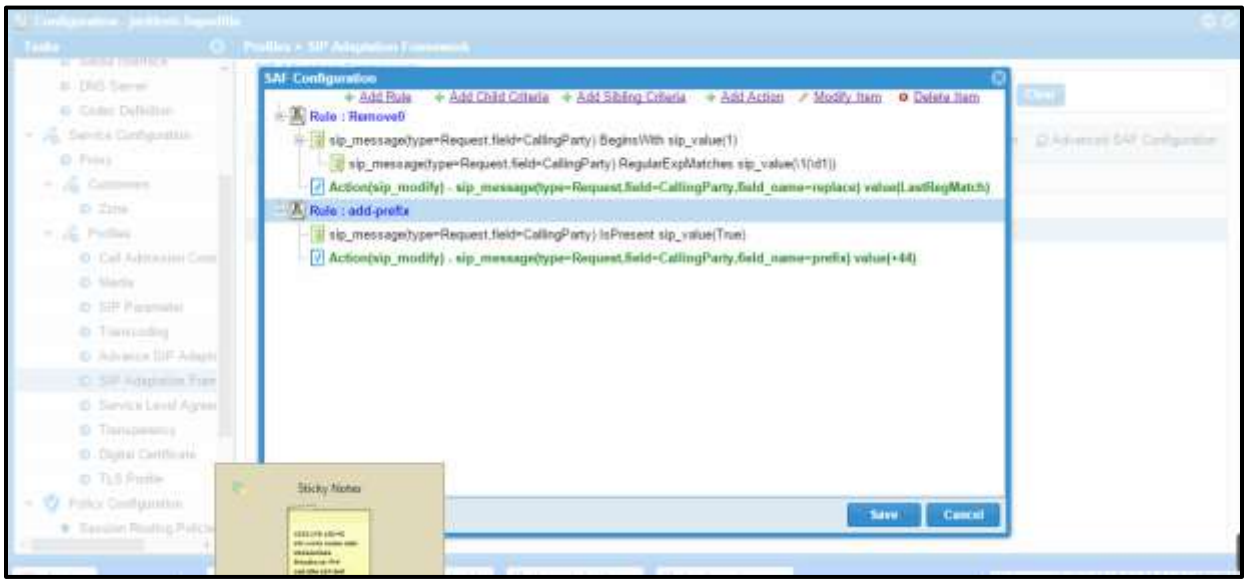
Network traffic is displayed graphically. A zooming tool allows the user to select specific sections of the graph by simply clicking and dragging your mouse.

Figure 21: Error Statistics



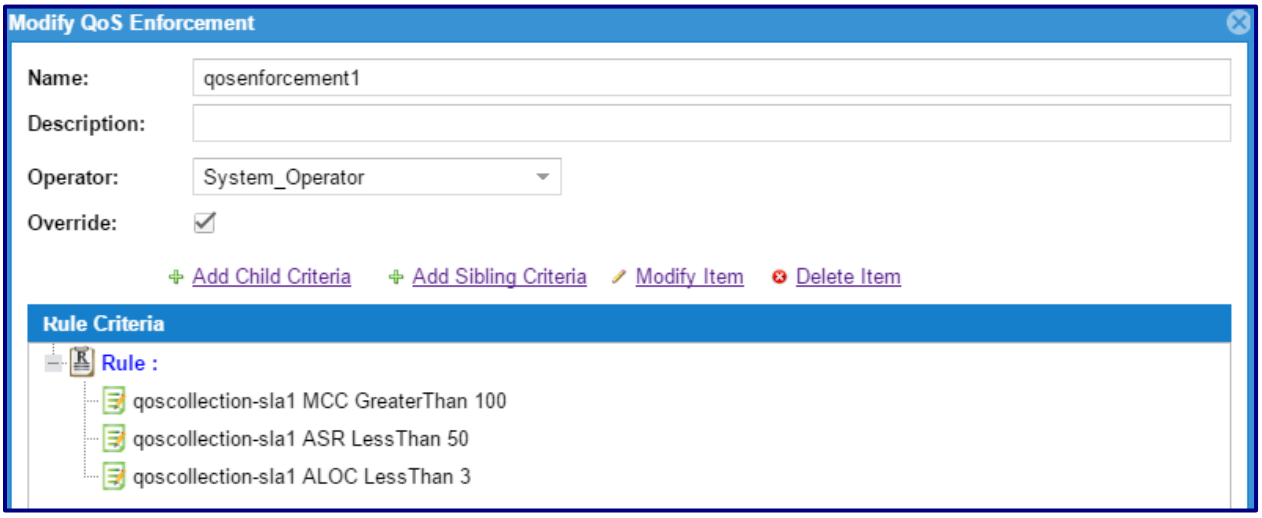
Error statistics for a selected interval can be displayed as a bar graph.

Figure 12: Wizard for Configuration



The Wizard for Configuration can be used to create rules and can be done with the GUI.

Figure 33: Setting Limits for QoS Enforcement



Configuration wizards create rules, raise warnings, display critical errors, and can be used to alter routes based on SLAs or blacklisted suspicious sources which have gone past critical limits.

9.0 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.

10.0 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.