Dialogic Session Border Controller Performance Validation

14 February 2019

DR190108F

Miercom
www.miercom.com

Contents

1.0 Executive Summary

Voice over Internet Protocol (VoIP) and Voice over LTE (VoLTE) networks require high performance Session Border Controllers (SBCs) to handle increasing call volumes that include both signaling and media. Without an SBC, the network is vulnerable to dropped calls, poor quality and even more importantly – attacks.

Dialogic engaged Miercom to test its Dialogic BorderNet SBC, implemented in public cloud, virtual environments, and on bare-metal for performance, functionality and security in real-world network deployments. The BorderNet SBC was subjected to high call rates over extended periods of time to confirm call handling capabilities, as well as its resiliency during high-volume traffic and Denial-of-Service (DoS) attack scenarios.

During testing, the Dialogic BorderNet SBC proved to be highly interoperable with multiple deployment environments and performed automatic scaling (elasticity) without interruption as it successfully managed and secured offered calls.

The following key points highlight our results found in this detailed report:

Key Findings of the Dialogic SBC

- **Over 100K Concurrent Calls**: Successfully established more than 100,000 calls on a Hewlett Packard (HP) commercial off-the-shelf (COTS) mid-range Gen 10 HP DL380*
- **Over 6,800 Calls with Software Transcoding:** Successfully established more than 6,800 calls with software transcoding from G.729 to G.711.
- **Single Software for Wide Ranging Deployment Models:** Full featured high scale performance from "cloud native" deployment in Amazon (AWS) and Microsoft Azure to virtualized deployment on VMware and KVM to bare metal deployment on HP COTS servers.
- **Heightened Security:** Demonstrated secure and uninterrupted call handling during periods of intense call loading and DoS attacks.
- **VoLTE Compatibility:** Successfully tested SIP, IMS/VoLTE P-CSCF and WebRTC calls flows with SRTP and transcoding. Call registration, SIP header manipulation, call admission control (CAC) and transport layer security (TLS) were also successfully tested and verified.

Based on results of our testing, the Dialogic BorderNet Session Border Controller (SBC) was found to fully support commercial-off-the-shelf (COTS) and virtualized functions to enhance signaling and media communications. Its scalable performance and wide breadth of security earns the ***Miercom Performance Verified*** certification.

Robert Smithers

CEO

Miercom

* 2 x Intel Xeon-Silver 4114 Processors @ 2.2 GHz 10 cores

2.0 Test Summary

5.0 Performance							
5.1 SIP Call (COTS)	**CPS**	**Duration (s)**	**Calls**	**CPU (%)**	**Mem (%)**	**MOS**	**Codec**
Max CPS No Media	1,800	30	54,000	42	50	NA	NA
Max Calls No Media	650	180	117,000	11	50	NA	NA
Max CPS with Media	1,150	30	34,500	48	50	3.88	G.729
Max Calls with Media (3 min)	490	180	90,000	64	50	3.88	G.729
Max Calls with Media (5 min)	320	300	96,000	77	47	3.88	G.729
5.2 VoLTE Call (COTS)	**CPS**	**Duration (s)**	**Calls**	**CPU (%)**	**Mem (%)**	**MOS**	**Codec**
Max CPS No Media	1,000	30	30,000	31	52	NA	NA
Max Calls No Media	650	180	117,000	17	52	NA	NA
5.3 SIP Call (VMware 32 vCPU)	**CPS**	**Duration (s)**	**Calls**	**vCPU (%)**	**Mem (%)**	**MOS**	**Codec**
Max CPS No Media	1,350	30	40,500	31	40	NA	NA
Max Calls No Media	650	180	117,000	12	42	NA	NA
Max CPS with Media	1,000	30	30,000	36	42	3.88	G.729
Max Calls with Media	250	300	75,000	28	42	3.88	G.729

5.4 SIP Transcoding*	**CPS**	**Duration (s)**	**Calls**	**CPU (%)**	**Mem (%)**	**MOS (a)**	**MOS (b)**	**Codec (a)**	**Codec (b)**
Max CPS with Media (Software)	38	180	6,840	89	35	4.09	4.38	G.729	G.711A
Max Calls with Media (4 x PCIe DSP cards + Software)	90	180	16,200	90	35	4.09	4.38	G.729	G.711A

5.5 SIP Encryption*	**CPS**	**Duration (s)**	**Calls**	**CPU (%)**	**Mem (%)**	**MOS**	**Codec**
Max Calls with Media SRTP-RTP	200	180	36,000	25	41	4.09	G.729
Max Calls with Media SRTP-SRTP	180	180	32,400	21	41	4.07	G.729

5.6 Registration Performance	**RPS**	**Duration (s)**	**CPU (%)**	**Mem (%)**	**Total Registrations**
Registration Performance	1,000	250	7	48	250,000

* HP DL380 - 2 x Intel Xeon-Silver 4114 Processors @ 2.2 GHz 10 cores

6.0 Security				
6.1 TCP SYN Flood	**Port**		**CPU (%) (Orig.)**	**CPU (%) (Attack)**
TCP SYN Flood	6000		7.9	9.2
TCP SYN Flood	5060		7.9	9.6
TCP SYN Flood (Spoofed IP)	5100		7.9	9.4
6.2 TCP Connection Flood	**Port**		**CPU (%) (Orig.)**	**CPU (%) (Attack)**
TCP Connect Flood	6000		8.2	14.5
TCP Connect Flood	5100		8.2	15.0
6.3 UDP Flood	**Port**		**CPU (%) (Orig.)**	**CPU (%) (Attack)**
UDP Flood	7000		8.3	9.6
UDP Flood (Spoofed IP)	5100		8.3	15.4
6.4 Ping of Death	**CPU (%) (Orig.)**			**CPU (%) (Attack)**
ICMP Ping of Death	7.9			8.7
6.5 IP Malformed Packet	**Port**		**CPU (%) (Orig.)**	**CPU (%) (Attack)**
TCP Malformed Packet	80		8.0	9.3
6.6 SIP INVITE Flood	**Port**	**CPS**	**CPU (%) (Orig.)**	**CPU (%) (Attack)**
SIP INVITE Flood (Unauthorized)	5100	1000	5.2	6.7
SIP INVITE Flood (Authorized)	5100	1000	5.2	27.8
6.7 SIP Registration Flood	**Port**	**CPS**	**CPU (%) (Orig.)**	**CPU (%) (Attack)**
SIP Registration Flood	5100	2000	5.2	5.7
6.8 Nessus Local Scan	**Status: Pass**			
6.9 SIP Fuzzing	**Status: Pass**			
7.0 Functionality				
7.1 CPS & Call Limitations	**Status: Pass**			
7.2 SBC Resiliency/HA	**Status: Pass**			
7.3 SIP Header Manipulation	**Status: Pass**			
7.4 Peering CAC	**Status: Pass**			
8.0 Deployability				
8.1 Multi-Platform Support	**Status: Pass**			
8.2 Interop: WebRTC	**Status: Pass**			
8.3 Autoscaling Up/Down	**Status: Pass**			
8.4 Scaling CPU Impact with Media	**Status: Pass**			
8.5 Scaling CPU Impact No Media	**Status: Pass**			

3.0 Introduction

Our testing validated or observed the following areas:

- **Performance Benchmarking – Call Performance:** Call performance includes max concurrent calls and maximum calls per second (CPS) for different protocols and deployment scenarios.
- **Performance Benchmarking – Resiliency:** Resiliency benchmarking includes high availability (HA) testing and successful threshold limitations on maximum calls and maximum CPS.
- **Security Assessment:** Demonstrates impact of various DoS attacks, ability to withstand SIP Fuzzing attacks, and vulnerabilities found by Nessus Scans.
- **Interoperability:** Shows deployment and call creation for Dialogic BorderNet SBC "Cloud Native" capabilities.

Dialogic BorderNet Session Border Controller, *version BN-SBC 3.8.0 (build 144)*

The BorderNet SBC is a scalable high-performance SBC that provides high-performance, feature-rich scalability while ensuring protected connectivity and management of real-time voice, video and data services over IP networks. This "single-software" SBC is built on a service-oriented software architecture enabling flexible deployment models and automation-enabling points of integration through extensive RESTful API support.

SCALABILITY

The BorderNet SBC supports ease of scaling from 1 session to 100,000 concurrent sessions and up to 1,000 sessions per second in a single instance, reducing upfront costs and operation expenses without the need to replace or add additional SBCs.

SINGULAR SOFTWARE

A common software and feature set are supported across all deployment models, including physical (COTS), virtual and cloud-based platforms to create a simplified migration strategy from legacy appliances to new software-only real time communication networks.

RAPID DEPLOYMENT

Powerful easy-to-use SIP header manipulation tools and profile-based provisioning enable rapid operator and orchestrated deployment options.

RESOURCE EFFICIENCY

Dynamic virtual central processing unit (vCPU) sharing for all sessions and processing profiles, including transcoding and encryption, providing a highly attractive price/performance curve across all types of network infrastructure.

HEIGHTENED SECURITY

Dependable security against network threats, vulnerabilities and spoofing are visible with an intelligent dashboard and reporting interface in real-time.

Technical Specifications

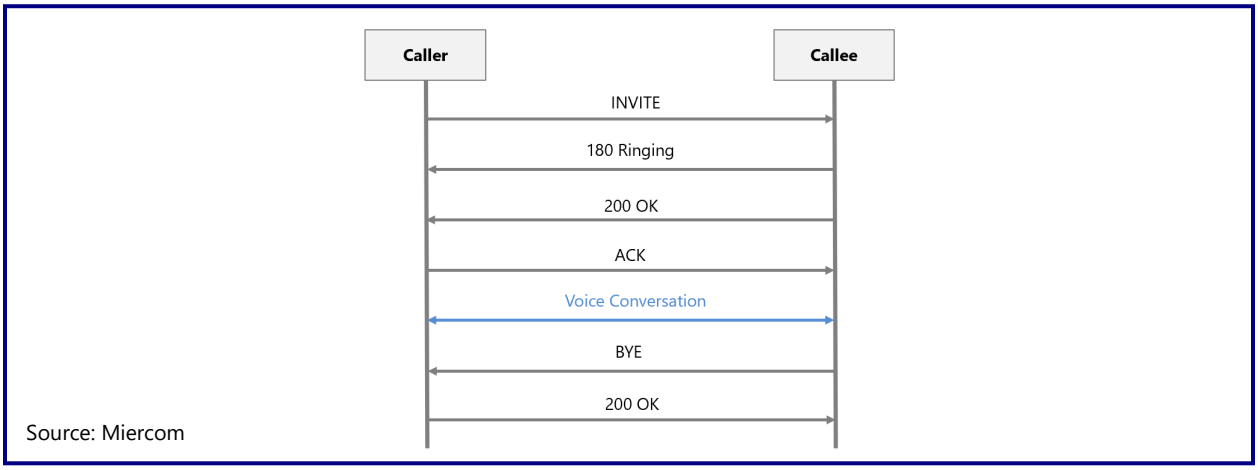
Interfaces	
Signaling and Media	4+4 x 1 Gb Ethernet (10/100/1000 Base-T or MM fiber each), or 2+2 Fiber 10 Gb
Management	1 redundant GbE (10/100/1000 Base-T)
High Availability	1 redundant GbE (1000 Base-T)
Protocol Internetworking	
Signaling	SIP, SIP-I, SIP-T, H.323
Other	VLAN, IPv4, IPv6, UDP, TCP, RTP, RTCP
Network	IPv4, IPv6, Overlapped IP networks
Security Features	
• Access Control List (ACL) • Signaled pinhole media firewall • Network topology hiding for both signaling and media • Encryption support: TLS, IPsec, HTTPS, SSH, SRTP • NAT traversal • DoS and overload protection • Rate Limiting • Dynamic blacklisting	
Media Security Features	
• Media profiling • Rogue RTP detection • Packet rate monitoring and limiting • Dynamic bandwidth limiting • Bandwidth determination and enforcement	
Media Support	
Software transcoding	Audio: G.711-PCMA, G.711-PCMU, G.729A, G.729AB, G.723.1, G.722, G.726, AMR-NB, AMR-WB, OPUS, iLBC, and EVS narrow-band
Hardware transcoding	Audio: G.711-PCMA, G.711-PCMU, G.729A, G.729AB, G.723.1, AMR-NB, AMR-WB, OPUS, iLBC, and EVS narrow-band
Fax	G.711 fax, T.38
Tones	In Band, SIP INFO, RFC2833 DTMF
Performance and Capacity	
Max Concurrent Sessions	100,000 (G.729) / 75,000 (G.711) including media
Max Concurrent (TLS/SRTP)	20,000
Max Sessions/Sec (SPS)	1,000 SPS signaling and media
SIP messages per sec (7 per session)	7,000
Media packets per second	6 million
Access (subscribers)	256,000
Scalability	
VLANs	1,024
IP Addresses	2,048 (signaling and media)
SIP Interfaces	500
Peers	4,000
Profiles	1,024
Local DNS Entries	65,000
Policies	5,000

4.0 How We Did It

A custom-built network was created to simulate a real-world deployment. Traffic was generated and delivered through the network to evaluate the Dialogic BorderNet SBC functionality and performance.

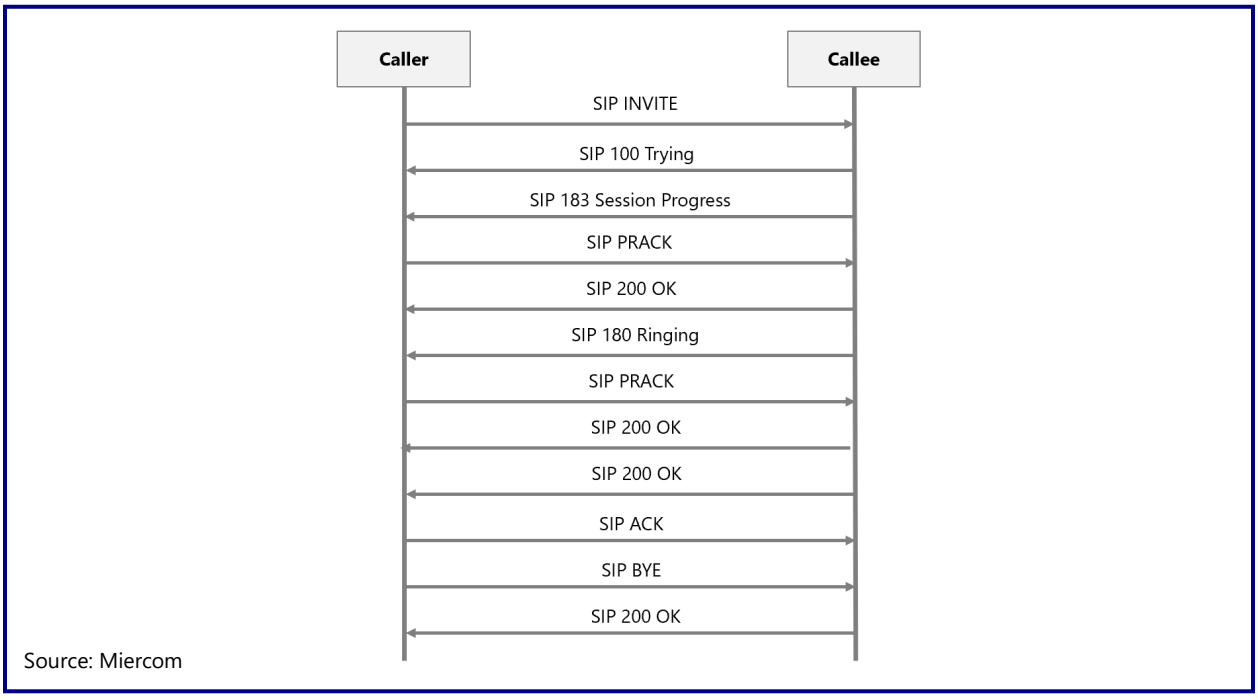
Calls generated were made up of 7-message UDP calls or 12-message VoLTE calls as shown below.

7-message UDP Call Diagram



Source: Miercom

12-message VoLTE Call Diagram

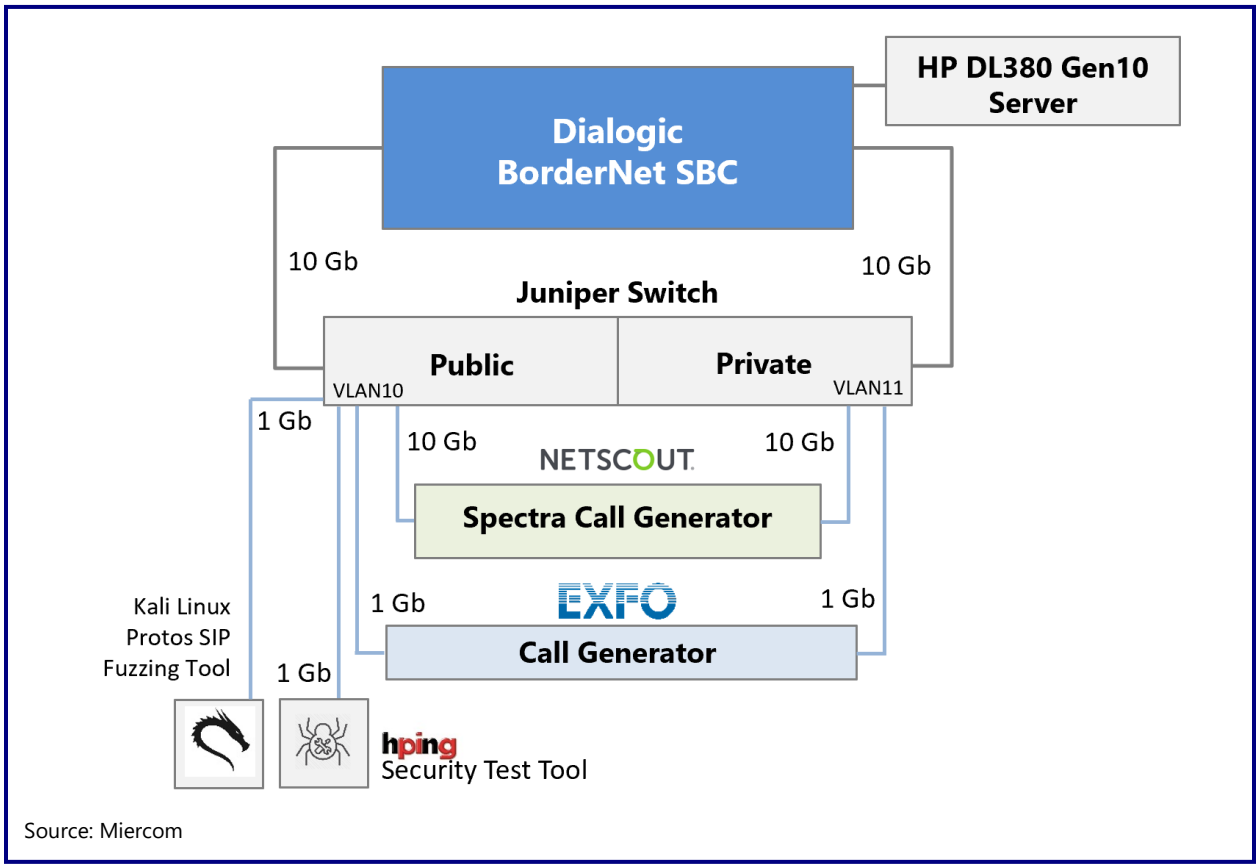


Source: Miercom

Test Bed Setup

Our hands-on testing replicated a typical production environment by using call generation and security testing tools to challenge the SBC. Each test is detailed in the remainder of this report.

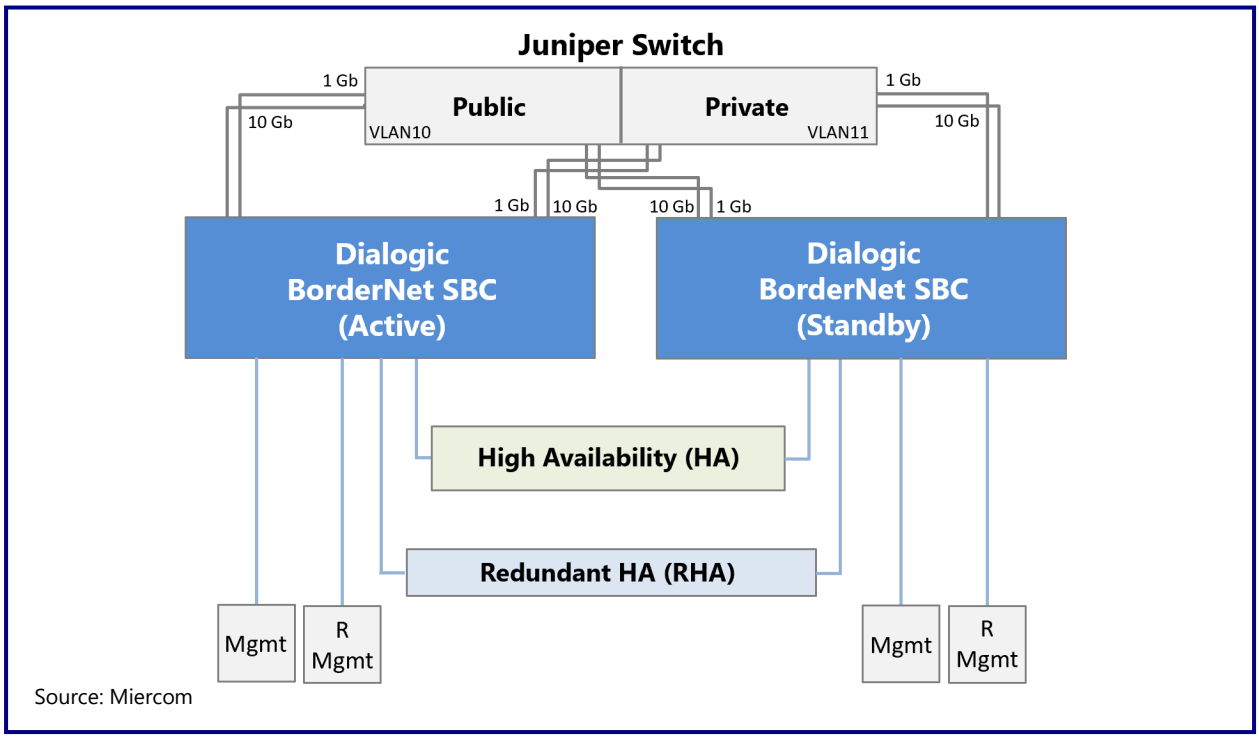
Test Bed Diagram



The SBC is connected to the public and private sides of the network through a Juniper switch. The Spectra call generator has 4 interfaces, with 2 cards each. Two cards were used for signaling (1 Gb interfaces each), and two cards were used for media (10 Gb interfaces each). The EXFO generated calls with TLS 1.0 for both the public and private sides of the network. The hping3 security test tool was connected to the public side to deliver DoS attacks to the network. The SBC was connected to an HP DL380 Gen10 server (2 x Intel Xeon-Silver 4114 Processors @ 2.2GHz 10 cores).

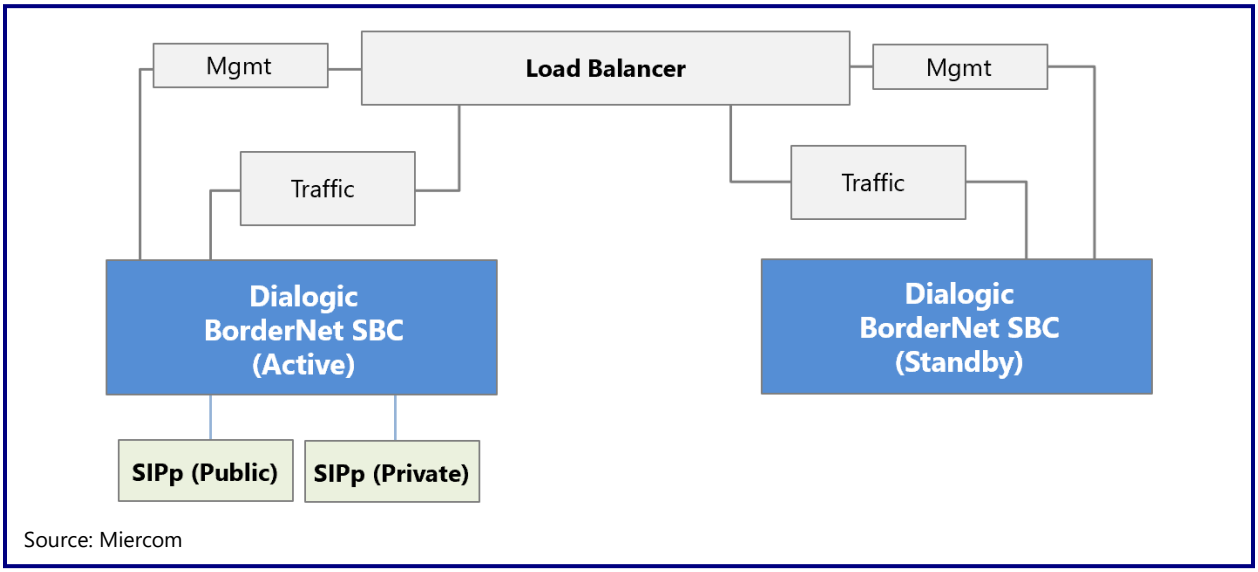
When testing high availability and integration functionality, the following test deployments were used.

High Availability Deployment



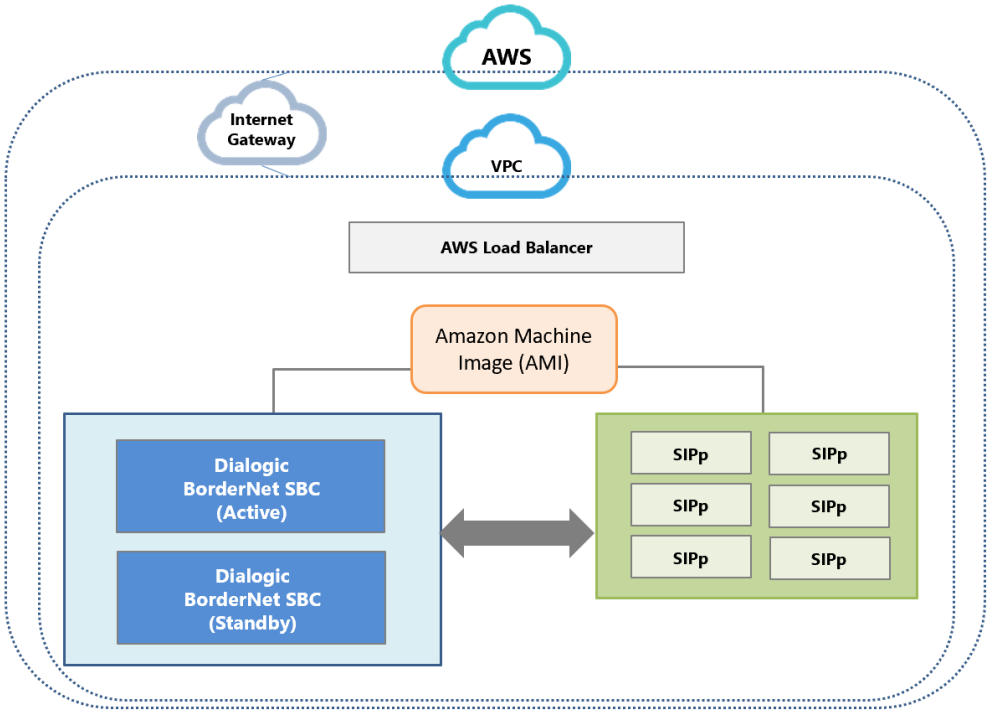
Both SBCs have 4 x 10 Gb and 4 x 1 Gb ports. Two 10 Gb ports were used for public and private sides. The other two ports were used for redundancy. It also has redundant management (R Mgmt) and high availability (RHA) ports.

Microsoft Azure Deployment



The load balancer is for management and traffic; it checks for SBC management and availability for Port 5060. If this port is unavailable, it transfers the call to the standby SBC.

Amazon Web Services Deployment



Source: Miercom

The Dialogic BorderNet was deployed in the Amazon AWS EC2. Multiple BorderNet virtual machines can be created depending on the scalability needed. Scale-up options were created, in this case, through the AWS AMI. The SBC successfully scaled up to c4.2xlarge from c4.xlarge when call loads exceeded 2,000 and vice versa to scale-down.

Test Tools

NETSCOUT Spectra2 *(FW version 8.8.0.0.R1)* tests functionality of VoIP and IMS network deployments using protocol emulation to identify bottlenecks, latency and QoS for comprehensive performance validation.

EXFO provides voice quality verification and configurable threshold testing for a wide range of protocols for network deployment troubleshooting. It also supports MOS and R-factor metrics for quality-assured service testing.

SIPp is an open source tool that generates traffic for the SIP protocol for traffic, stress and performance testing and optimization. It has a dynamic display of call statistics – call rate, round trip delay and message statistics. Other supported protocols include: IPv6, TLS and SCTP. SIPp can perform SIP authentication, conditional scenarios and transmission of RTP audio or video media.

5.0 Performance

5.1 SIP Call Processing (COTS)

Performance was measured for the BorderNet SBC deployed on bare-metal (COTS), utilizing two Intel Xeon-Silver 4114 (2.2 GHz/10-core/85W) with a total of 20 cores/40 vCPUs and 64 GB of memory. Each call consisted of 7 SIP messages.

Test Name	CPS	Duration (s)	Calls	CPU (%)	Mem (%)	MOS	Codec
Max CPS No Media	1,800	30	54,000	42	50	NA	NA
Max Calls No Media	650	180	117,000	11	50	NA	NA
Max CPS with Media	1,150	30	34,500	48	50	3.88	G.729
Max Calls with Media (3 min)	490	180	90,000	64	50	3.88	G.729
Max Calls with Media (5 min)	320	300	96,000	77	47	3.88	G.729

5.2 VoLTE Call Processing (COTS)

Performance was measured for the BorderNet SBC deployed on bare-metal (COTS), utilizing two Intel Xeon-Silver 4114 (2.2 GHz/10-core/85W) with a total of 20 cores/40 vCPUs and 64 GB of memory. Each UDP call consisted of 12 SIP messages.

Test Name	CPS	Duration (s)	Calls	CPU (%)	Mem (%)	MOS	Codec
Max CPS No Media	1,000	30	30,000	31	52	NA	NA
Max Calls No Media	650	180	117,000	17	52	NA	NA

5.3 SIP Call Processing (VMware)

Performance was measured for the virtual BorderNet SBC deployed on VMware, utilizing 32 vCPU and 64 GB of memory. Each call consisted of 7 SIP messages. Additional results for 2/4/8/16 vCPUs are listed in the Appendix.

Test Name	CPS	Duration (s)	Calls	CPU (%)	Mem (%)	MOS	Codec
Max CPS No Media	1,350	30	40,500	31	40	NA	NA
Max Calls No Media	650	180	117,000	12	42	NA	NA
Max CPS with Media	1,000	30	30,000	36	42	3.88	G.729
Max Calls with Media	250	300	75,000	28	42	3.88	G.729

5.4 SIP Call Processing with Transcoding (COTS)

Performance was measured for the BorderNet SBC deployed on bare-metal (COTS), utilizing two Intel Xeon-Silver 4114 (2.2 GHz/10-core/85W) with a total of 20 cores/40 vCPUs and 64 GB of memory. Each call with transcoding consisted of 7 SIP messages.

Test Name	CPS	Duration (s)	Calls	CPU (%)	Mem (%)	MOS (a)	MOS (b)	Codec (a)	Codec (b)
Max Calls with Media (Software)	38	180	6,840	89	35	4.09	4.38	G.729	G.711A
Max Calls with Media (Hardware [4x] & Software)	90	180	16,200	90	35	4.09	4.38	G.729	G.711A

5.5 SIP Encrypted Call Processing (COTS)

Performance was measured for the BorderNet SBC deployed on bare-metal (COTS) SBC, utilizing two Intel Xeon-Silver 4114 (2.2 GHz/10-core/85W) with a total of 20 cores/40 vCPUs and 64 GB of memory. Each call with encryption consisted of 7 SIP messages.

Test Name	CPS	Duration (s)	Calls	CPU (%)	Mem (%)	MOS	Codec
Max Calls with Media SRTP-RTP	200	180	36,000	25	41	4.09	G.729
Max Calls with Media SRTP-SRTP	180	180	32,400	21	41	4.07	G.729

5.6 Registration Performance

The SBC successfully registered 250,000 users at 1,000 registrations per second (RPS).

Test Name	RPS	Duration (s)	CPU (%)	Mem (%)	Total Registrations
Registration Performance	1,000	250	7	48	250,000

6.0 Security

All tests were run against the public side of the physical instance of the Dialogic SBC, unless specified otherwise. A security test is considered failed if the SBC was observed having excessive CPU usage or crash.

Performance under Denial-of-Service (DoS)/Distributed DoS (DDoS)

Determine if the system can remain operational, with acceptable performance, while under attack. The (D)DoS test is executed toward all interfaces with a public facing IP address.

This test was configured to run on the public-facing interface of the SBC. Utilizing access control list (ACL) rules, the DoS attacks will originate from an unauthorized IP (except in the IP spoofing cases).

The test was executed to both an unconfigured port and to a configured port. Unauthorized SIP INVITE flood configuration was altered for the Public Access (5060, 5100). SIP invites from the IP range were unauthorized by the SBC. Authorized SIP REGISTRATION and INVITE flood were configured with maximum CPS settings: 1000 Registrations and 500 Invites per second.

All DoS attacks, except the SIP INVITE flood, were performed with background traffic running: A total of 9,000 SIP calls with media at 100 CPS for a call hold time of 180 seconds. Calls were continuously made every 3 minutes; once the call was over, the EXFO tool made another call. The SIP INVITE flood attack had background traffic of 18,000 SIP calls with media.

6.1 TCP SYN Flood

SYN floods (single attack source) are effective if the server allocates resources after receiving a SYN, but before it has received the ACK. If these half-open connections bind server resources, the server can be flooded with SYN messages. No new connections (legitimate or not) can be made, resulting in denial of service. Some systems may malfunction badly or crash if other operating system functions are starved of resources this way.

Status: Pass

Test Name	Port	CPU (%) (Orig.)	CPU (%) (Attack)
TCP SYN Flood	6000	7.9	9.2
TCP SYN Flood	5060	7.9	9.6
TCP SYN Flood (Spoofed IP)	5100	7.9	9.4

6.2 TCP Connection Flood

This attack shows how a system behaves with a large number of attempted concurrent connections.

Status: Pass

Test Name	Port	CPU (%) (Orig.)	CPU (%) (Attack)
TCP Connect Flood	6000	8.2	14.5
TCP Connect Flood	5100	8.2	15.0

6.3 UDP Flood

UDP flooding targets the application by listening on a specific port. It may cause process crashing, restart or a memory leak.

Status: Pass

Test Name	Port	CPU (%) (Orig.)	CPU (%) (Attack)
UDP Flood	7000	8.3	9.6
UDP Flood (Spoofed IP)	5100	8.3	15.4

6.4 Ping of Death

A Ping of Death (POD) attack sends a malformed, or otherwise malicious, ping to a computer. A ping is normally 64 bytes (B); many computer systems cannot handle a ping larger than the maximum IP packet size, which is 65,535 B. Sending a ping of this size can crash the target computer. Traditionally, this bug has been relatively easy to exploit. While illegal to send a 65,536 B ping packet according to networking protocol, a packet of such size can be sent if fragmented; when the target computer reassembles the packet, a buffer overflow can occur and often causes a system crash.

Status: Pass

Test Name	CPU (%) (Orig.)	CPU (%) (Attack)
ICMP Ping of Death	7.9	8.7

6.5 IP Malformed Packet (TCP Short Header)

As specified in RFC 791, IP packets must follow the same format. This attack tries to send IP packets which are not compliant with this RFC standard to cause the receiving system to misbehave or even crash. It is used to test the robustness of the receiving system.

Status: Pass

Test Name	Port	CPU (%) (Orig.)	CPU (%) (Attack)
TCP Malformed Packet	80	8.0	9.3

6.6 SIP INVITE Flood

Verify the system behavior under SIP INVITE flooding using a simple SIP INVITE message. This test demonstrates whether the SIP stack is vulnerable to INVITE flood attacks. For this test, background traffic of 18,000 simultaneous SIP calls with media was used.

Status: Pass

Test Name	Port	CPS	CPU (%) (Orig.)	CPU (%) (Attack)
SIP INVITE Flood (Unauthorized)	5100	1000	5.2	6.7
SIP INVITE Flood (Authorized)	5100	1000	5.2	27.8

6.7 SIP Registration Flood

Verify the system behavior under SIP REGISTER flooding using a simple SIP REGISTER message. This test demonstrates whether the SIP stack is vulnerable to REGISTER flood attacks.

Status: Pass

Test Name	Port	CPS	CPU (Orig.)	CPU (Attack)
SIP Registration Flood	5100	2000	5.2	5.7

6.8 Nessus Local Scan

Verify if there are any missing operating system security patches. For each host, open ports should be listed.

Test Name	Status
Nessus Local Scan (Public)	**Pass**
Nessus Local Scan (Private)	**Pass**

6.9 SIP Fuzzing

Verify resiliency of SBC to all SIP INVITE fuzzing scenarios.

Test Name	Status
SIP INVITE Fuzzing	**Pass**

7.0 Functionality

These tests focus on SBC resilience, including SBC signaling and media planes protection using automatic software failover procedures.

7.1 CPS and Call Limitations

The capability of the user to administer limitations on CPS and calls is tested. Once the limitation is exceeded, calls are dropped for a short time until traffic is allowed again. Each time the threshold is reached, this process repeats.

Two tests were run with a call rate of 650 CPS and for a duration of 180 seconds. Test 1 limited CPS to 500 (~90,000 calls); calls were expected to drop when exceeding 500 CPS. Test 2 limited calls to 115,000; calls were expected to drop when exceeding 115,000.

Status: Pass

Once the call rate reached the configured limitation, calls were dropped from the port for approximately 5 seconds, and traffic was passed again. Once reaching the rate limit, calls were dropped again. This repeated if the threshold remained violated, proving the system could successfully reject extra calls.

Like the call rate, if the session maximum was reached, the system successfully rejects extra calls.

7.2 SBC Resilience/High Availability (HA)

Initial condition is a VoLTE load with background traffic consisting of 18,000 calls configured with a Call Hold Time of 180 seconds, recycled every three minutes, generated by the Spectra for physical interfaces and SIPp for deployments of Microsoft Azure (1 CPS for 30 seconds) and Amazon (5 CPS for 300 seconds).

During failover via VM reboot, verify:

1. Target VM failover does not cause other VMs to failover
2. There is no impact to transient or stable calls

Status: Pass

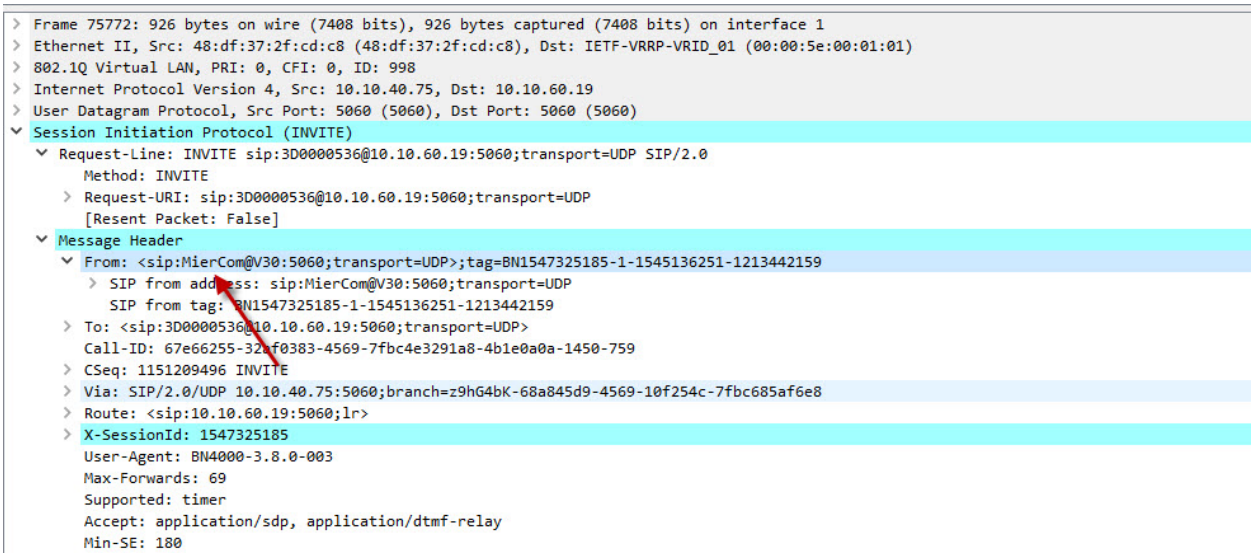
18,000 calls were created and successfully held without failure. The SBC successfully transferred traffic between primary and standby ports when primary ports went down, and again when the SBC went down.

7.3 SIP Header Manipulation

Demonstrate use of SIP filtering, a set of programmable rules, for manipulating SIP information.

Status: Pass

SIP header was successfully changed to a value of Miercom for 18,000 calls. SIP header was successfully modified to from 'field' to 'Miercom' for 18,000 calls. The screenshot below shows this change.



Source: Miercom

7.4 Peering Call Admission Control (CAC)

This test focuses on restricting the number of concurrent calls from a given peering partner (trunk group) to a certain limit to avoid SBC overloading and verifies that over-the-limit calls are properly rejected.

The SBC was configured not to accept more than 500 calls per second. Gradually increasing CPS to 680 generated system alarm. The SBC stopped accepting any new calls and when calls are low enough – in our scenario 350 simultaneous calls – the SBC started to accept calls again.

Status: Pass

Successfully limited CPS to 500.

8.0 Deployability

8.1 Multi-Platform Support

Flexible deployment of the BorderNet SBC software is evaluated within typical real-world environments that include public cloud (AWS/Azure), private cloud (VMware/KVM), and commercial off-the-shelf (COTS). The BorderNet SBC software is expected to provide services across all deployment models.

Status: Pass

8.2 Interoperability: WebRTC

WebRTC capabilities were demonstrated using the online application SIP.js (Chrome). SRTP-to-RTP and SRTP-to-SRTP calls with video were successfully demonstrated using a network configuration that included the Dialogic BorderNet SBC, two clients (SIP.js or Bria), and a proxy server with TekSIP (for remote client registration).

Status: Pass

8.3 Scalability: Automatic Scale-Up, Scale-Down

The Amazon Cloud should be able to handle increased call volumes as the network expands without negatively impacting usability; depending on virtual CPU allocation.

The SBC successfully demonstrated the capability to automatically scale a deployment in AWS (scale up in about 5-7 minutes without any interruption).

Scale up and down was tested by configuring a threshold of 2,000 concurrent calls. SIPp generated calls at 10 cps with 300-second call hold time to ramp up calls to 3,000 concurrent calls. Once the call load increased above 2,000 calls, the c4.xlarge instance was dynamically replaced with a c4.2xlarge EC2 instance. This scale up was accomplished by first transferring all calls to the standby SBC instance and then instantiating a new primary SBC instance on a c4.2xlarge EC2 instance. Once the new c4.2xlarge primary instance was instantiated all calls were migrated back to it and the standby SBC instance was also migrated to a c4.2xlarge EC2 instance.

No calls failed during the scale-up. For scale-down, the opposite behavior was observed. When the call volume fell below 2,000 calls for a period of 60 second the c4.2xlarge EC2 instances were automatically replaced with the lower cost c4.large EC2 instances, demonstrating dynamic infrastructure cost reduction.

Status: Pass

About Miercom

Miercom has published hundreds of network product 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.

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.

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

Appendix: Engineering Notes

5.3 Performance: UDP SIP Call Processing (VMware)

In addition to the results for 32 vCPU, we have observed the following:

PERFORMANCE VMWARE	PLATFORM	CPS	CHT	CONCURENT SESSIONS	CPU	MEM	MOS
Media: G.729							
Max CPS	2 vCPU 6 GB RAM	80	30	2,400	84	82	3.9
Max Calls	2 vCPU 6 GB RAM	27	180	4,860	82	84	3.9
Max CPS	4 vCPU 8 GB RAM	210	30	6,300	79	77	3.9
Max Calls	4 vCPU 8 GB RAM	80	180	14,400	92	83	3.9
Max CPS	8 vCPU 16 GB RAM	490	30	14,700	80	52	3.9
Max Calls	8 vCPU 16 GB RAM	160	180	28,800	70	57	3.9
Max CPS	16 vCPU 32 GB RAM	850	30	25,500	78	40	3.9
Max Calls	16 vCPU 32 GB RAM	300	180	54,000	77	44	3.9