BreakingPoint Virtual Edition (VE)

Virtualized application and security testing

Problem: The Virtualization of Network Security Functions Brings Many Unknowns

The current generation of networks need to adapt quickly and facilitate change. Strategies like Network Functions Virtualization (NFV) and Software Defined Networking (SDN) provide powerful flexibility gains by moving traditional application and security functions (such as application delivery, load balancing, data packet inspection, firewall, intrusion prevention system, and sandbox components) off dedicated hardware onto virtualized servers. These virtualized devices must deliver the same or better performance and security efficacy comparing with the traditional hardware appliances. Without a way to properly test these virtualized application and security devices, customer quality of experience is at risk.

Solution: An Easy-to-Use Testing Ecosystem for Virtualized Infrastructure

BreakingPoint VE provides scalable real-world application and threat simulation in a deployment model that fits IT budgets by leveraging virtualization and industry-standard hardware platforms. Build resilient physical or virtual networks you can rely on by using BreakingPoint VE to maximize security investments and optimize network architectures. The market-proven BreakingPoint application offers cost-effective, elastic, and sharable virtualized test capabilities that are quickly deployed and scaled across geo-diverse enterprise-wide networks. This is made possible by a flexible traffic generation and analysis solution to validate physical and virtual devices and networks at scale. The real-time statistics allow quick identification of security problems and isolate the breaking points. Because BreakingPoint VE is as easy to use as it is effective, you do not have to be a security or virtualization expert to achieve complete end-to-end service validation.

The BreakingPoint VE subscription model is aligned with enterprise project-based IT OpEx funding requirements. Acquire the tools quickly, scale up and scale down as project needs demand, and deploy anywhere with virtualization speed and simplicity.

Visit www.keysight.com for more information on the BreakingPoint VE product.

KEYSIGHT

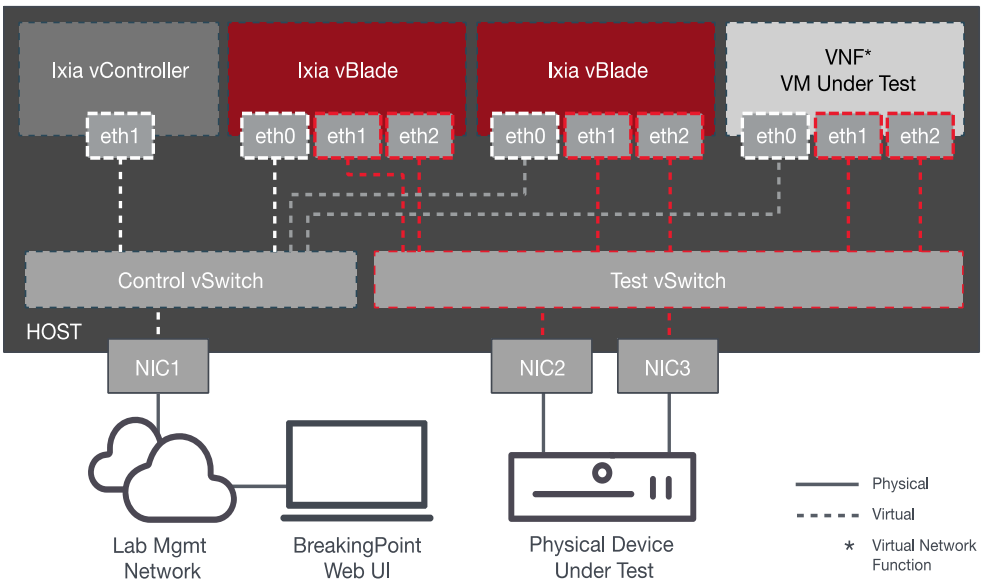

Figure 1. BreakingPoint VE deployment for both virtual and physical device tests

Highlights

- Test the most critical components of virtual and physical application-aware devices and networks. Validate various attacks and distributed denial of service (DDoS) defenses.
- Optimize the configuration of virtual or physical network security devices such as IDS, IPS, DLP, UTM, NGFW, WAF, web proxy, and others.
- Keep up with the ever-evolving threat landscape by updating your applications, attacks, and malware via the daily Applications and Threats Intelligence updates.
- Assess how virtual machine mobility impacts application reliability and scalability. Run the tests during live migration to ensure minimum network downtime.
- Validate next generation 5G / NFV networks by testing within Private Clouds / Telco Clouds powered by OpenStack or VMware vCenter orchestration.
- Understand how network applications are affected by deployment within different Public Clouds such as Alibaba Cloud, Amazon AWS, Google Cloud, or Microsoft Azure.
- Leverage subscription-based licensing that enables the flexibility of pay-as-you-grow OpEx model with different licenses available in multiple performance levels (such as 1G / 10G / 100G).

BreakingPoint VE

Table of Contents

Key Features

- Provides comprehensive protocol coverage across a large set of network security applications.
- Simulates more than 300 real-world application protocols and 37,000 attacks and malwares.
- Allows for customization and manipulation of any protocol field, including raw data.
- Generates a mix of protocols at high speed with realistic protocol distribution.
- Delivers all types of traffic simultaneously, including legitimate traffic, DDoS, and malware.
- Application and Threat Intelligence (ATI) subscription includes latest applications and threats.
- Measures metrics like concurrent connections, connection rate, simulated users, or throughput.
- Powerful statistics engine with high level aggregated views as well as detailed drilldown views.
- Common BreakingPoint user interface and experience across both Hardware / Virtual products.
- Easy transition between Hardware / Virtual platforms through common configurations and scripts.
- Comprehensive hypervisor support for stand-alone platforms like VMware ESXi / KVM / Hyper-V.
- Comprehensive orchestration support in Private Clouds based on VMware vCenter / OpenStack.
- Comprehensive support for Public Clouds inside Amazon AWS / Google Cloud / Microsoft Azure.
- Includes Virtual Machines with Virtual System Controller / Virtual Blade roles.
- Provides software optimized for protocol emulation and traffic generation in virtual environments.
- Flexible all-inclusive subscription licensing model reduces startup cost and enables easier growth.
- Common License Server shared among IxLoad VE, IxNetwork VE, BreakingPoint VE, and others

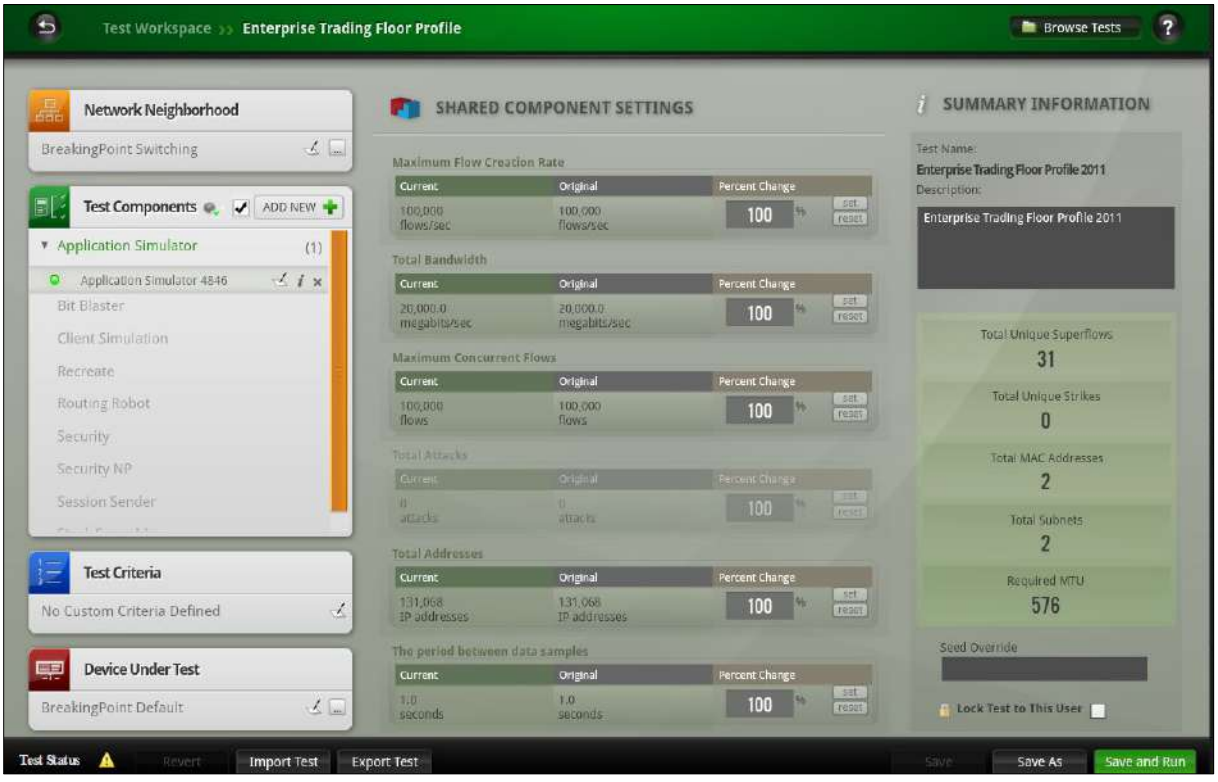

Figure 2. BreakingPoint GUI configured with an enterprise trading floor application mix test

Specifications

BreakingPoint VE features, functions, and capacities for the System Controller and Virtual Blade:

Feature	System Controller	Virtual Blade
Maximum # of Virtual Ports	96	8
Maximum # of Virtual Blades	12	N / A
Maximum # of Simultaneous Users	20	8
Guest OS	Based on CentOS 7.9 / 64-bit / Linux 3.10 Kernel	
vCPU	4 vCPU – Minimum 8 vCPU – Default 16 vCPU – Maximum	1 vCPU – Minimum 4 vCPU – Default 16 vCPU – Maximum
Memory	4 GB RAM – Minimum 8 GB RAM – Default 16 GB RAM – Maximum	2 GB RAM – Minimum 8 GB RAM – Default 32 GB RAM – Maximum
Disk	20 GB HDD – Minimum 20 GB HDD – Default 512 GB HDD – Maximum	15 GB HDD – Minimum 15 GB HDD – Default 15 GB HDD – Maximum
Login via Web UI	admin / admin	N / A
Login via SSH	netadmin / netadmin	netadmin / netadmin
Management IPv4	Yes	Yes
Management IPv6	N / A	N / A

BreakingPoint VE can also operate with a different amount of compute resources allocated to the Virtual Blade. This impacts the performance (determined as number of packets per second), scalability (determined as number of concurrent sessions), and maximum number of test components supported.

	System Controller	Virtual Blade
Performance = Low Test Components (DPDK On) = 1 Test Components (DPDK Off) = 2	8 vCPUs 8 GB RAM	1 vCPUs 2 GB RAM
Performance = Medium Test Components (DPDK On) = 2 Test Components (DPDK Off) = 4	8 vCPUs 8 GB RAM	2 vCPUs 4 GB RAM
Performance = High Test Components (DPDK On) = 4 Test Components (DPDK Off) = 8	8 vCPUs 8 GB RAM	4 vCPUs 8 GB RAM
Performance = Very High Test Components (DPDK On) = 8 Test Components (DPDK Off) = 16	8 vCPUs 8 GB RAM	8 vCPUs 16 GB RAM

BreakingPoint VE distribution and packaging format for **Private Cloud** platforms with **Manual Deployment Scenario** (by using the platform specific tools for deploying the Virtual Edition products):

Platform	System Controller	Virtual Blade
VMware ESXi	OVA	OVA
VMware vCenter	OVA	OVA
KVM / stand-alone	QCOW2	QCOW2
KVM / OpenStack	QCOW2	QCOW2
Microsoft Hyper-V	VHD	VHD
Docker Containers	N / A	N / A

BreakingPoint VE distribution and packaging format for **Private Cloud** platforms with **Automatic Deployment Scenario** (by using Deployment Wizard for creating large scale deployments with ease):

Platform	System Controller	Virtual Blade
VMware ESXi	OVA	OVA
VMware vCenter	N / A	N / A
KVM / stand-alone	QCOW2	QCOW2
KVM / OpenStack	N / A	N / A
Microsoft Hyper-V	N / A	N / A
Docker Containers	N / A	N / A

BreakingPoint VE distribution and packaging format for **Public Cloud** platforms with **Cloud Deployment Scenario** (by using the platform specific tools for deploying the Virtual Edition products):

Platform	System Controller	Virtual Blade
Alibaba Cloud	QCOW2	QCOW2
Amazon AWS	AMI	AMI
Google Cloud	QCOW2	QCOW2
Microsoft Azure	VHD	VHD
Oracle Cloud	N / A	N / A

Qualified and Compatible Environments

BreakingPoint VE is designed to work best when used in a qualified environment. Our recommendation is to always use one of the qualified versions of the virtualization platforms.

BreakingPoint VE is also compatible with different environments. In case there are issues encountered in these environments, Keysight will make reasonable efforts to address them, but cannot guarantee specific outcomes or results. In such rare cases, the proposed solution is to use a qualified environment.

Category		Qualified			Compatible
Hypervisor and Host OS		VMware vSphere ESXi 7.X VMware vSphere ESXi 8.X KVM over CentOS 7.X KVM over CentOS 8.X KVM over CentOS Stream KVM over Rocky Linux KVM over Ubuntu 18.04 LTS KVM over Ubuntu 20.04 LTS KVM over Ubuntu 22.04 LTS			VMware vSphere ESXi 6.X KVM over RHEL 7.X KVM over RHEL 8.X Microsoft Hyper-V Windows 2016 Microsoft Hyper-V Windows 2019 KVM over Ubuntu 14.04 LTS KVM over Ubuntu 16.04 LTS
Management and Orchestration		VMware vCenter 7.X VMware vCenter 8.X OpenStack Zed (vanilla distribution)			VMware vCenter 6.X Other OpenStack-based platforms (vanilla distributions) Other OpenStack-based platforms (vendor-specific distributions)
Public Cloud		Amazon Web Services Google Cloud Platform Microsoft Azure *			Alibaba Cloud
Network Connection and vNIC Driver	**Virtual Switch**	VMware vSwitch KVM Linux Bridges KVM OVS	1G –> 100G 1G –> 100G 1G –> 100G	vmxnet3 virtio virtio	N / A
	PCI-PT	Intel 350 Intel 5xx Intel 7xx Intel 8xx Mellanox ConnectX-3 Mellanox ConnectX-4 Mellanox ConnectX-5	1G 10G 10G / 25G / 40G 10G / 25G / 50G / 100G 10G / 25G / 40G 10G / 25G / 50G / 100G 10G / 25G / 50G / 100G	igb ** ixgbe i40e ice mlx4*** mlx4*** mlx5***	N / A
	SR-IOV	Intel 350 Intel 5xx Intel 7xx Intel 8xx Mellanox ConnectX-3 Mellanox ConnectX-4 Mellanox ConnectX-5	1G 10G 10G / 25G / 40G 10G / 25G / 50G / 100G 10G / 25G / 40G 10G / 25G / 50G / 100G 10G / 25G / 50G / 100G	igbvf ** ixgbevf iavf iavf mlx4 *** mlx4 *** mlx5 ***	N / A
Virtual Switch Model		Virtual Standard Switch Virtual Distributed Switch Linux Bridges Open Virtual Switch Open Virtual Switch	(on VMware) (on VMware) (on KVM) (on KVM) (on OpenStack)		Hyper-V Virtual Switch (on Microsoft Hyper-V) Linux Bridges (on OpenStack)

* DPDK Performance Acceleration not supported when running in Microsoft Azure Public Cloud.
** DPDK Performance Acceleration not supported by Intel 1G NICs connected in PCI-PT / SR-IOV mode.
*** DPDK Performance Acceleration not supported by Mellanox NICs connected in PCI-PT / SR-IOV mode.

Protocols and Features

BreakingPoint VE is powered by the Keysight Application and Threat Intelligence (ATI) program that delivers a wide variety of applications and attacks to emulate traffic mixes and security threats of small, medium, or large enterprises, service providers, or government organizations at scale. The application and attack emulations are complemented with the BreakingPoint VE comprehensive network stack that simulates network components like IPv4, IPv6, IPsec, LTE, 3G / 4G, and DNS, helping in orchestrating a wide variety of network environments.

Specification	Description
Applications	300+ application protocols, including Yahoo! Mail and Messenger, Google Gmail, Skype, BitTorrent, eDonkey, RADIUS, SIP, RTSP, RTP, HTTP, SSL, Facebook, Twitter Mobile, YouTube, and Apple FaceTime, as well as other mobile, social, and gaming protocols, including with Multicast support.
Wireless Interfaces (IPv4 only)	S1-U (eNodeB and SGW sides) S1-MME (eNodeB side) SGi (PDN side) S5/8 (SGW and PGW sides) S11 (MME and SGW sides) Wireless Protocols Supported: S1AP GTP-C v1, GTP-C v2, GTP-U v1 SCTP (over UDP or IP)
Wireless Operational Modes (IPv4 only)	User Equipment eNodeB / MME (GTPv2) eNodeB / MME / SGW (GTPv2) eNodeB (S1AP / GTPv1) SGW / PGW MME / SGW / PGW PGW
Network Access	IPv4 / IPv6 Static Hosts IPv4 / IPv6 External Hosts IPv4 / IPv6 Router IPv4 / IPv6 DNS IPv4 DHCP Client / Server IPsec IKEv1 / IKEv2 NAT VLAN
Test Methodologies / Labs	RFC 2544 Lab Session Sender Lab Multicast Lab Lawful Intercept Lab DDoS Lab

Specification	Description
Security Exploits / Malware	36,000+ total attacks 6,000+ exploits 30,000+ malware 100+ evasion classes
	Attacks include: IP-based DoS attack types: ◦ ICMP flood test case ◦ ICMP fragmentation test case ◦ Ping flood test case UDP-based DoS attack types: ◦ UDP flood test case ◦ UDP fragmentation test case ◦ Non-spoofed UDP flood test case TCP-based DoS attack types: ◦ Syn flood test case ◦ Syn-ack flood test case ◦ Data ack and push flood test case ◦ Fragmented ack test case ◦ Session attack test case Application-layer attack types: ◦ DNS flood attack case ◦ Excessive verb attack case ◦ Recursive GET Floods ◦ Slow POSTs Botnets: ◦ Zeus ◦ SpyEye ◦ BlackEnergy ◦ Duqu ◦ Pushdo Cutwail
Licensing	All-inclusive license unlocks all features. All new features available at no additional cost during subscription duration. Each licensing unit enables: ◦ 1G Tier: 1 Gbps of throughput 2M concurrent super flows 1x Security and Security NP components ◦ 10G Tier: 10 Gbps of throughput 20M concurrent super flows 2x Security and Security NP components ◦ 100G Tier: 100 Gbps of throughput 200M concurrent super flows 4x Security and Security NP components

Product Capabilities

Simple Virtual Machine Deployment

Creating new BreakingPoint Virtual Blades and Virtual Ports can be achieved through the BreakingPoint GUI via the embedded Deployment Wizard capability. It is a simple process of supplying the credentials of the virtualization host (ESXi / KVM) and the rest of the process is completely automated to perform the Virtual Machine deployment and attachment to the BreakingPoint System Controller.

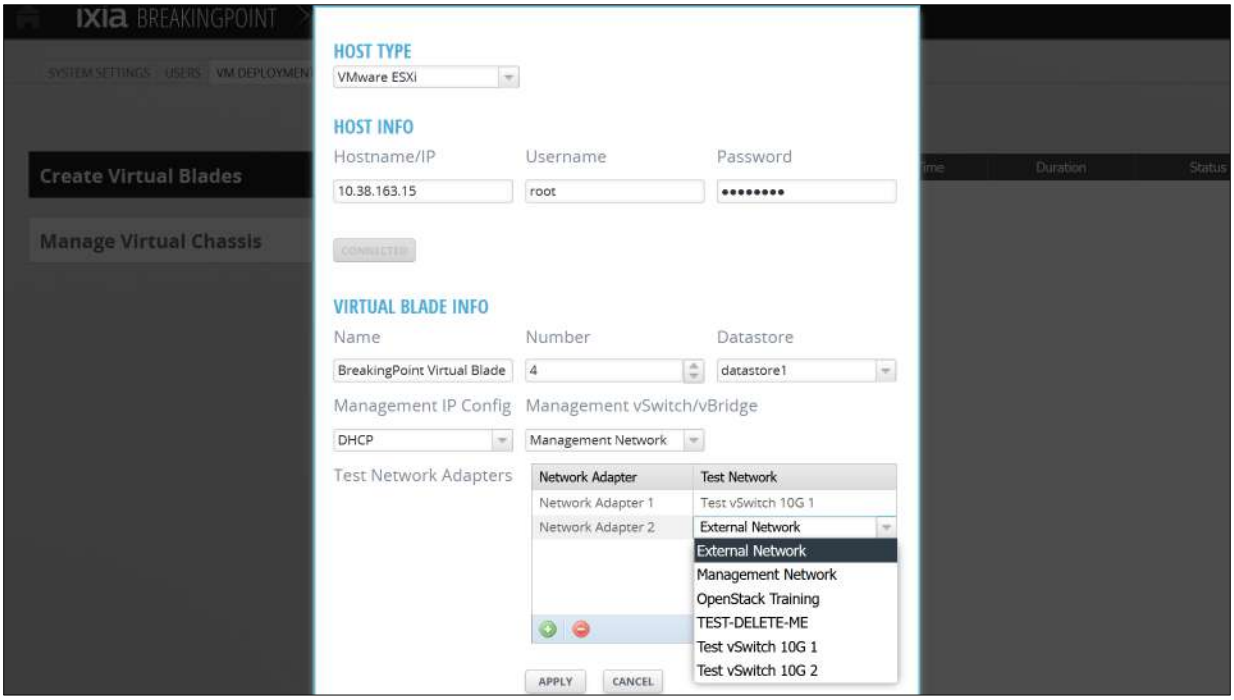

Figure 3. BreakingPoint VM deployment through the GUI Admin page

Application and Threat Intelligence (ATI) Program

Keysight's ATI program consists of several engineering units spread across the world, engaging in coordinated research and leveraging years of experience in understanding application behaviors, malicious activities, and attack methods to ensure BreakingPoint software is always updated and always current. The ATI team uses advanced surveillance techniques and cutting-edge research to identify, capture, and rapidly deliver the intelligence needed to conduct meaningful and thorough performance and security validation under the most realistic simulation conditions. Releasing updates every two weeks for more than 10 years, the ATI program comprises a library of 37,000+ attacks (Exploits, Malwares, DDoS, and more), 330+ popular applications, and over 2,000 canned tests. Additionally, the ATI program ensures the following:

- New applications / attacks are added to BreakingPoint without needing any platform updates.
- Users are always up to date with the ever-changing cyber security world.
- New applications are added, and popular applications are updated to current versions.
- Monthly malware packages contain fast-changing malware and botnet attacks.
- Real-world app mixes emulate traffic patterns of diverse demographics and business verticals.

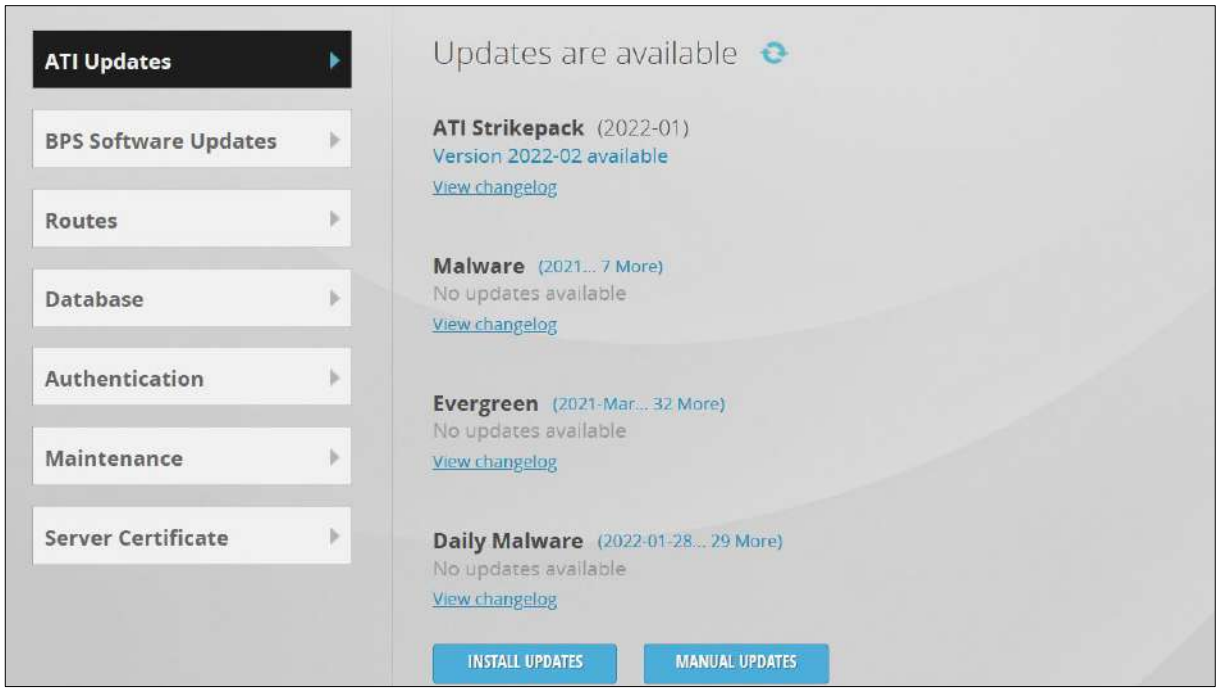

Figure 4. ATI packages can be updated through the intuitive BreakingPoint GUI

BreakingPoint Test Components

BreakingPoint offers a single Web UI for management results in simple, central control of all components and capabilities. Test components help configure legitimate application, malicious, malformed, and stateless traffic to validate application-aware devices and networks.

Specification	Description
Application Simulator	Allows users to create mix of applications and run tests in two-arm mode (BreakingPoint being the client and server) to test application-aware devices.
BitBlaster	Transmits layer 2 frames and analyzes a device's ability to handle stateless malformed or normal traffic at high speed.
Client Simulation	Allows users to generate client traffic via Super Flows against real servers (device under test) in one-arm mode (BreakingPoint being the client).
Live AppSim	Amplifies BreakingPoint traffic realism by running TrafficREWIND summary configurations that replicate the dynamic nature of production networks and applications. It leverages the TrafficREWIND ability to record and synthesize production traffic characteristics over extended periods of time.

Specification	Description
Recreate	Helps users to import captured traffic from network and replay it through BreakingPoint ports.
Routing Robot	Determines if a DUT routes traffic properly by sending routable traffic from one interface and monitoring the receiving interface. This is useful to perform RFC2544 and network DDoS testing.
Security	Measures a device's ability to protect a host by sending strikes and verifying that the device successfully blocks the attacks.
Security NP	This subset of security allows users to send malware traffic with higher performance at higher loads.
Session Sender	Enables testing of pure TCP and / or UDP behavior and performance and is also capable of performing advanced DDoS attacks.
Stack Scrambler	Validates integrity of different protocol stacks by sending malformed Ethernet / IP / ICMP / TCP / UDP data (produced by a fuzzing technique) to the DUT.

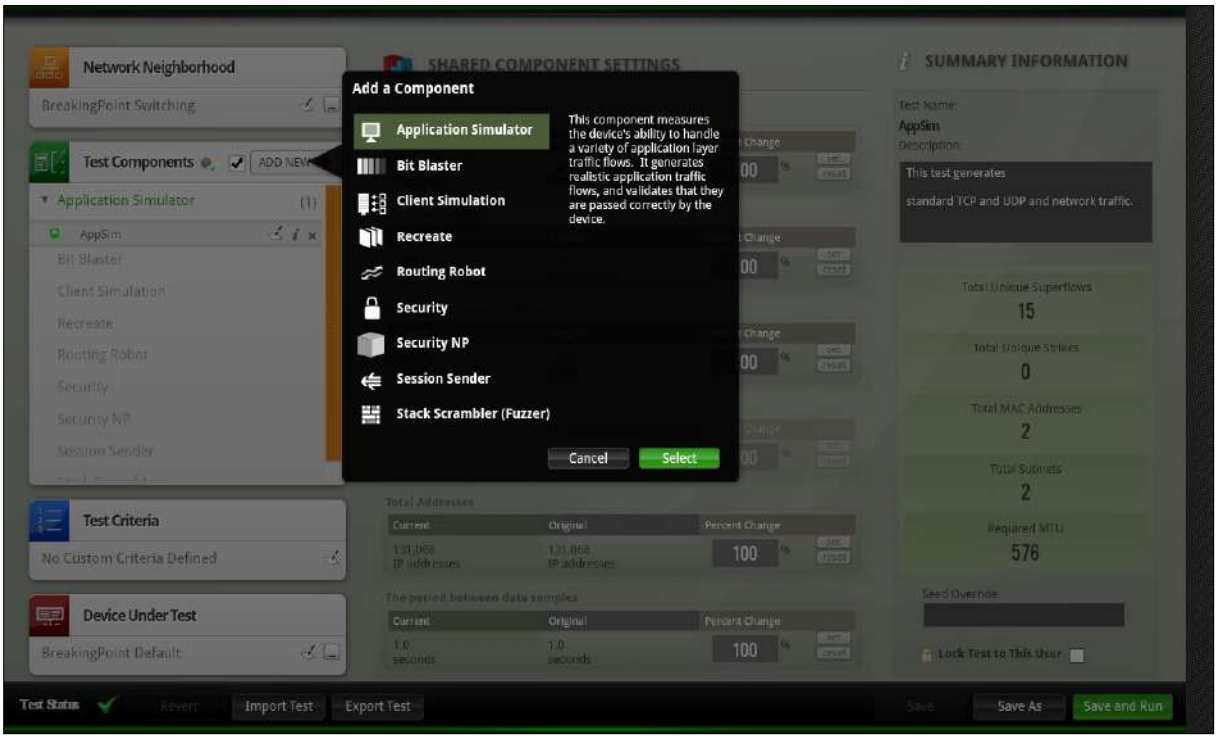

Figure 5. BreakingPoint purpose-built test components

Application Simulation

BreakingPoint simulates over 300 real-world applications, each configurable with application actions (flow) to simulate multiple user behavior and dynamic content. BreakingPoint also provides 100s of predefined application mix profiles representative of various enterprise and carrier networks.

Content realism is critical in validating performance of application-aware devices and networks, as it has a direct impact on inspection performance. BreakingPoint offers various functionality to easily parametrize applications with representative payloads such as the following:

- Tokens that allow users to randomize data as part of the application flow to prevent devices from accelerating bandwidth or detecting static data patterns.
- Markov text generation, which is a unique way of converting documents into new documents to generate random data by word instead of by character, allowing the data to look realistic, but at the same time to be dynamic.
- Dictionary functionality that allows users to input a table of rows as an input to a field. These are highly useful for emulating scenarios such as brute force attacks, where a user can input a huge list of passwords that are randomly sent one after the other through the 'password' field in a flow.
- Dynamic file generation capability that allows users to generate different types of attachments like exe, jpg, pdf, flash, and mpeg and helps in testing a device's file handling or blocking capabilities.
- Multi-Language capability that allows users to send emails, chats, or texts in languages like French, Spanish, German, and Italian, making the contents demographically realistic.

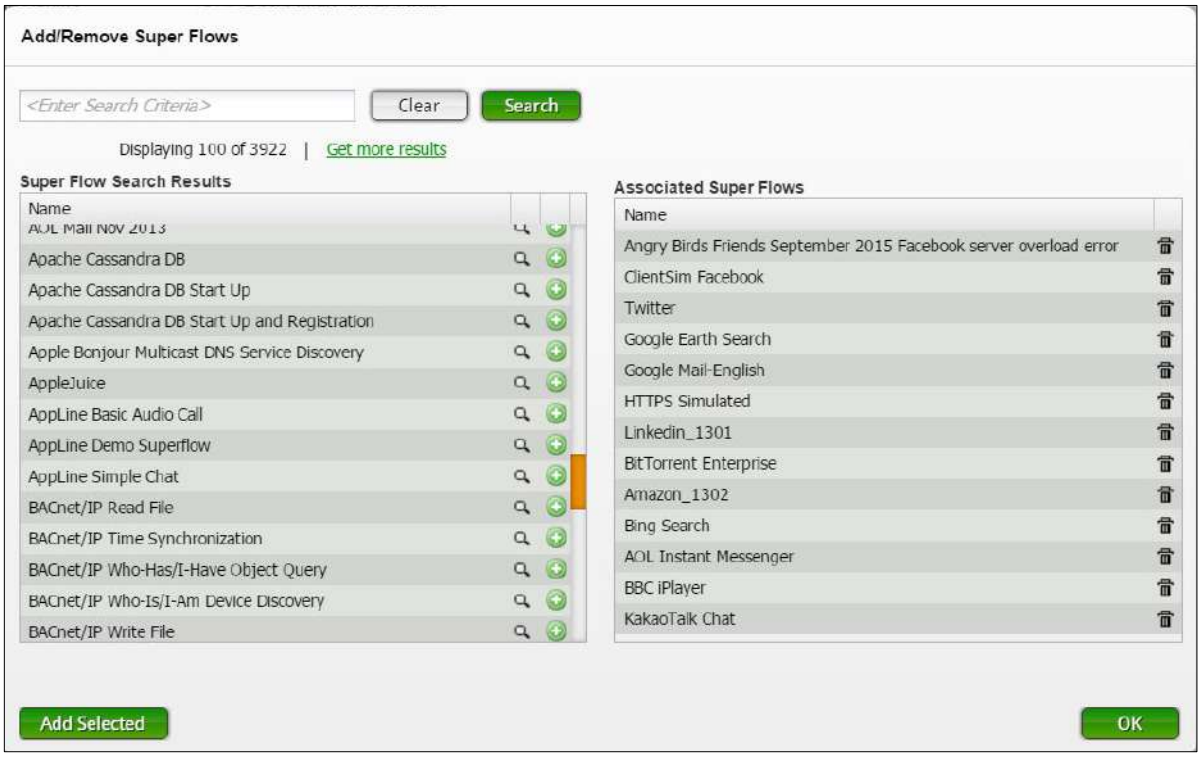

Figure 6. BreakingPoint provides flexibility to emulate a variety of applications and protocols that can be assembled to create real-world application mixes

Last-Modified: Mon, 12 Jul 13 05:56:39 GMT
Date: Wed, 22 Jun 14 19:16:20 GMT
Connection: Keep-Alive
Server: BreakingPoint/1.x
Content-Type: text/html
Content-Length: 2037

<! DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"><html
xmlns="http://www.w3.org/1999/xhtml"><head><meta content="text/html; charset=UTF-8" http-equiv="Content-Type"/><title>broach the subject of his</title><style type="text/css">p { vertical-align: text-bottom; background-color: #1ec4cc; background-image: none; display: inline; list-style-image: none; clear: right; font-family: cursive; border-width: thin; }</style></head> <body> Copyright (C) 2005-2011 BreakingPoint Systems, Inc. All Rights Reserved. <h5><q>Aterrible country, Mr.</q><q>Bickersteth and yourself has, unfortunately</q>We sallied out at once<u>Corcoran's portrait may not have</u>Won't you have an egg<u>Who the deuce is Lady</u>

Figure 7. BreakingPoint generates real-world application and security strike traffic; this example shows an HTTP request and response

TrafficREWIND and Live AppSim

Keysight's new TrafficREWIND solution complements BreakingPoint to easily translate production network insight into test traffic configurations with high fidelity. TrafficREWIND is a scalable, real-time architecture that uses production traffic metadata to record and synthesize traffic characteristics over extended periods of time (up to 7 days). The resulting test configuration from TrafficREWIND is used in BreakingPoint`s Live AppSim test component. Live AppSim adds a new testing dimension by empowering users not only replicate traffic profiles with associated real-world applications, but also dynamically changing traffic composition over time to model the temporal nature of production networks and applications in the lab.

Live AppSim is used to run TrafficREWIND exported traffic summary configurations, opening up unprecedented test possibilities:

- Faster fault analysis and reproduction capabilities
- Reference architectures and pre-deployment validation with production-like application mixes
- Relevant what-if scenarios by combining real production traffic with other test traffic, including security strikes, incremental applications, or even fuzzing

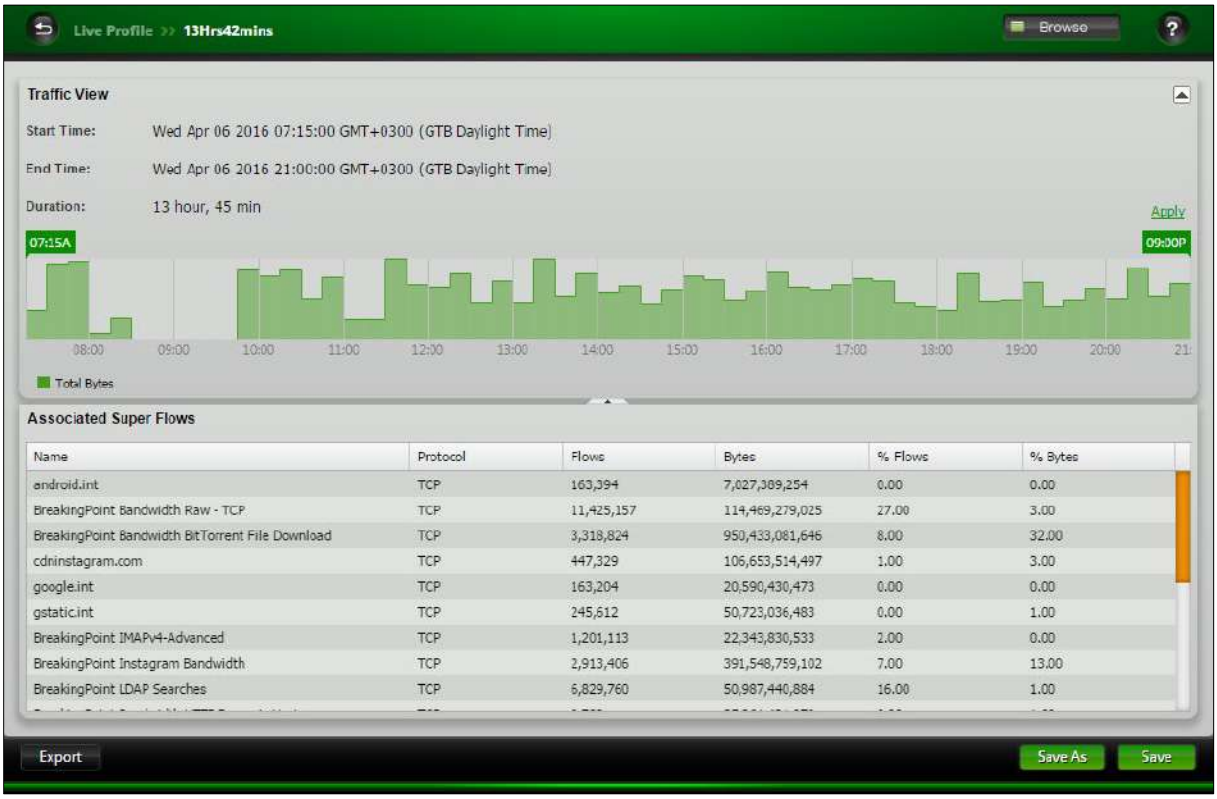

Figure 8. Live Profile created by importing a TrafficREWIND traffic summary configuration

Comprehensive Security

BreakingPoint delivers the industry's most comprehensive solution test network security devices—such as IPSs, IDSs, firewalls, and DDoS mitigation. It measures a device's ability to protect a host by sending strikes and verifying that the device successfully blocks the attacks. Simply select a Strike List and an Evasion Setting to create a security test or use one of the default options.

- Supports over 37,000 strikes and malware and the attacks can be obfuscated by over 100 evasion techniques
- Emulates botnets, from zombie to command and control (C&C) communication
- Simulates a variety of volumetric, protocol, and application-layer DDoS attacks
- Generates legitimate and malicious traffic from the same port—purpose-built hardware design allows sending all types of traffic simultaneously from a single port, with full control of the weight/mix of legitimate traffic, DDoS and other attacks, malware, and fuzzing

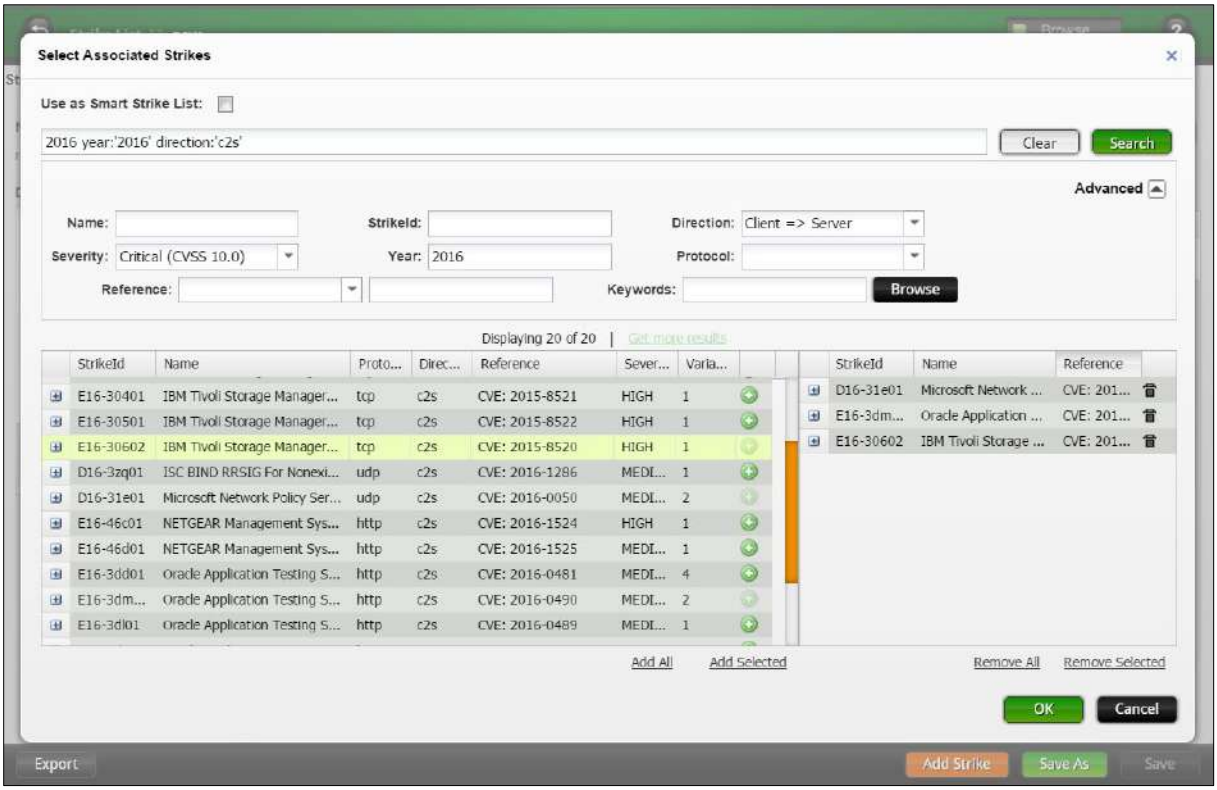

Figure 9. An intelligent search bar makes it easier to browse through the 37,000+ attacks

Network Neighborhood

BreakingPoint's Network Neighborhood provides flexibility for the user to create simple to highly complex network environments. It includes support of commonly used network elements like IPV4, IPV6, VLAN, IPsec, DHCP, DNS, and for 3G/4G mobile infrastructure network elements.

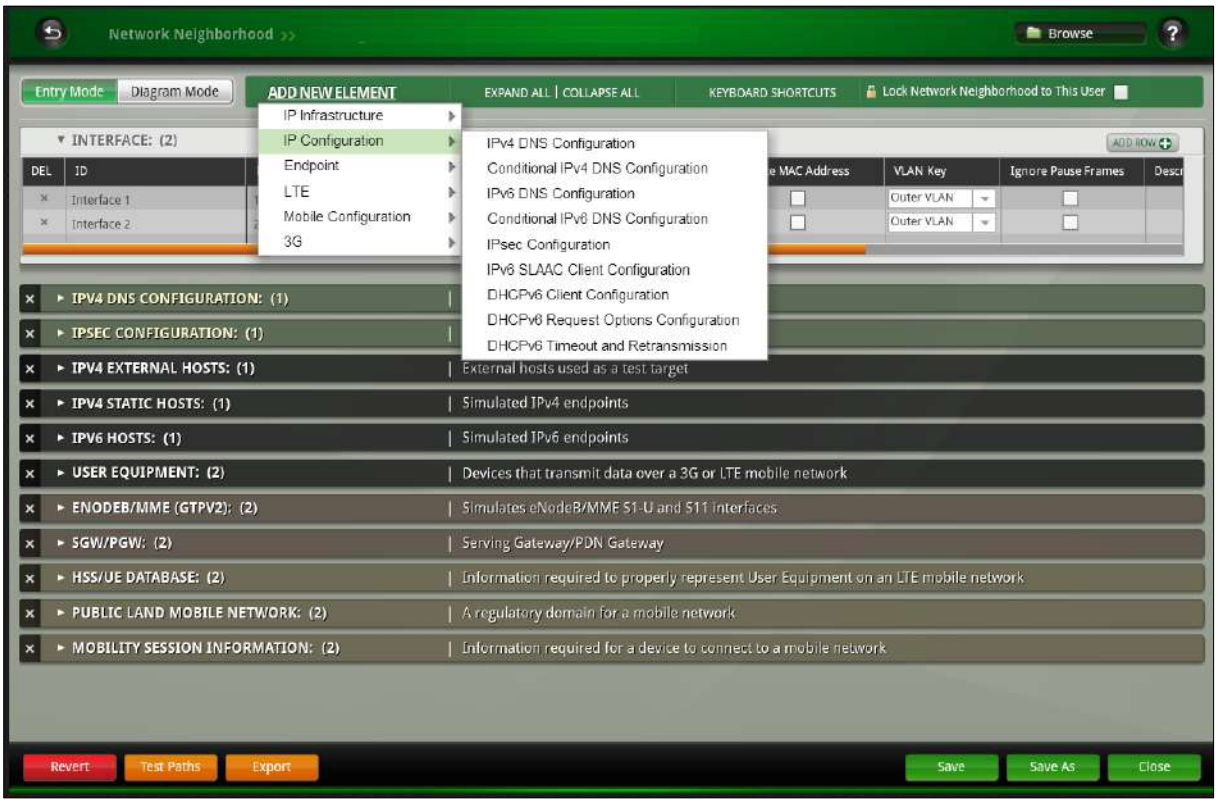

Figure 10. A complex mobile Network Neighborhood created in BreakingPoint that include some key network elements

Load Profiles

Load profiles and constraint provides users options to have more granular controls over the test run. This helps users create varied network conditions and load dynamics like rate controls, burst profiles, and Poisson distribution.

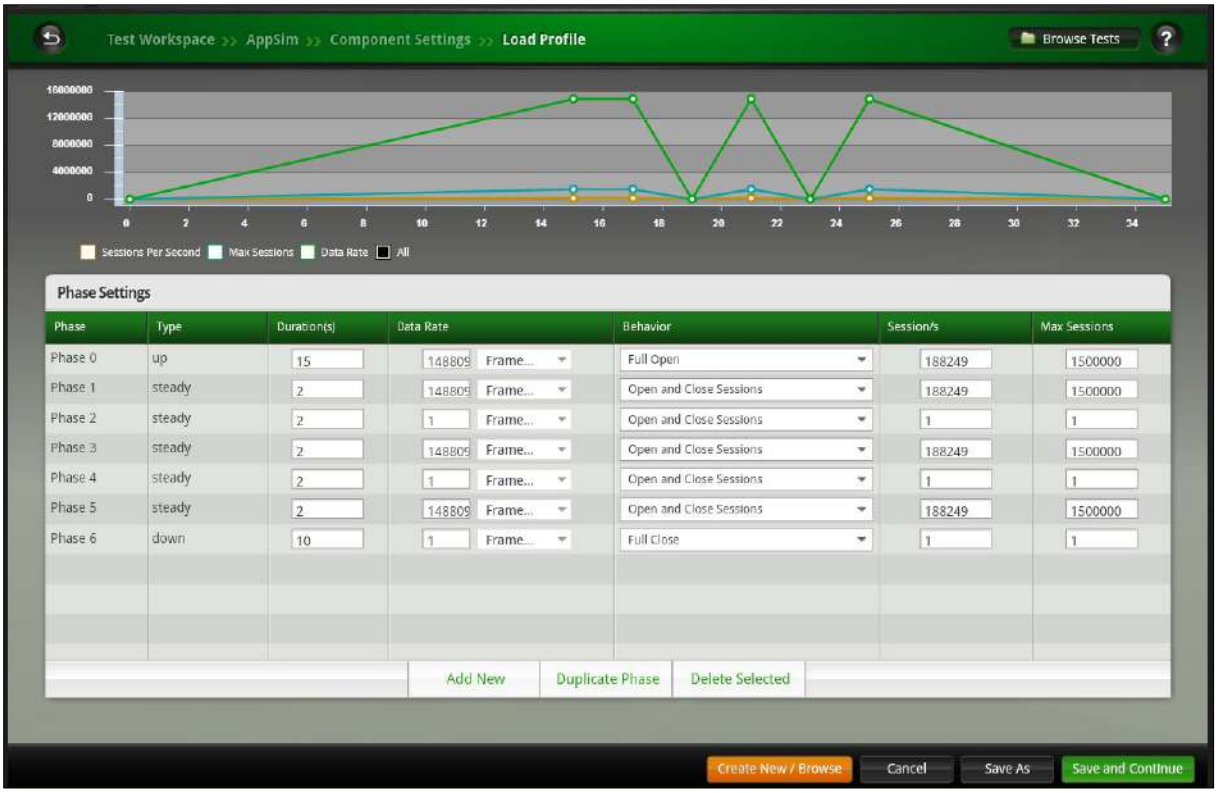

Figure 11. A BreakingPoint MicroBurst Load profile

Pre-Defined Test Methodologies / Labs

Leverage extensive automation and wizard-like labs that address many use-case scenarios, including validation of lawful intercept and data loss prevention (DLP) solutions, RFC2544, DDoS, Session Sender, and Multicast.

In addition, a REST and TCL API are provided for building and executing automated tests.

Figure 12. A test configured with DDoS Lab

Built-In Reporting

BreakingPoint's extensive reports provide detailed information about the test, such as the components used in a test, addressing information, DUT profile configuration, system versions, and results of the test.

- All reports include an aggregated test results section, which provides the combined statistics for all of the test components. It also includes the information over time, to pin-point a potential error within the time-slot it happened.
- All reports are automatically generated in HTML and viewable with a web browser; however, you may export the test results in XLS, HTML, PDF, RTF, CSV, or ZIP (CSV files). Reports are automatically generated each time a test is run and are viewable from the Results page.
- Comparison Report feature allows you to run multiple iterations of the same test on different load modules or different ports and compare the results. You have the option of comparing all sections of the tests, or you can select only certain sections to be included in the comparison.

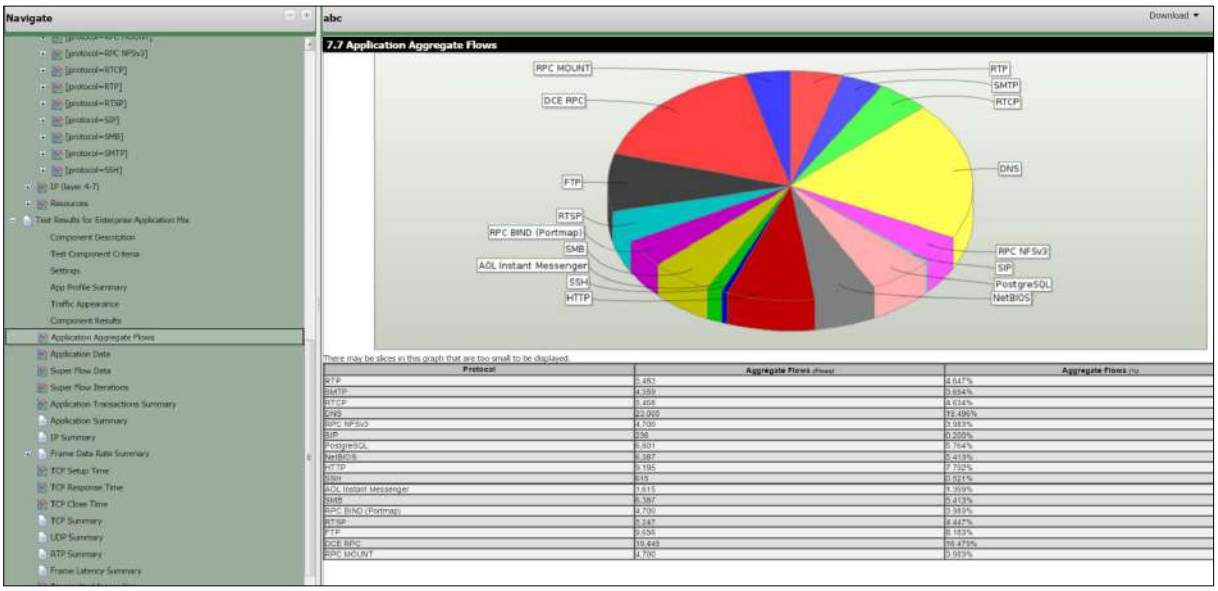

Figure 13. A segment of BreakingPoint report showcasing flow mix

Technology Solutions

Visit keysight.com for More Information on BreakingPoint and Keysight Virtualization Solutions

BreakingPoint – Applications and Security Testing
BreakingPoint Virtual Edition (VE) – Virtualized Application and Security Testing
IxLoad Virtual Edition (VE) – Virtualized Multiplay Services Testing
IxNetwork Virtual Edition (VE) – Virtualized Network Performance Testing
Cloud Peak – Virtualized Infrastructure Benchmarking

Ordering Information

939-9600

IXIA BreakingPoint VE (Virtual Edition) 1G (12-Months Floating Worldwide License, Keysight software support subscription). Enables 1 Gbps of throughput, 2M concurrent SuperFlows, and 1 Security / Security-NP components. Includes access to Application and Threat Intelligence Program (ATI) and updates for the purchased term. Requires license term to be specified (must be purchased in multiples of years, list price is per unit per year). TAA Compliant.

939-9610

IXIA BreakingPoint VE (Virtual Edition) 10G (12-Months Floating Worldwide License, Keysight software support subscription). Enables 10 Gbps of throughput, 20M concurrent SuperFlows, and 2 Security / Security-NP components. Includes access to Application and Threat Intelligence Program (ATI) and updates for the purchased term. Requires license term to be specified (must be purchased in multiples of years, list price is per unit per year). TAA Compliant.

939-9640

IXIA BreakingPoint VE (Virtual Edition) 100G (12-Months Floating Worldwide License, Keysight software support subscription). Enables 100 Gbps of throughput, 200M concurrent SuperFlows, and 4 Security / Security-NP components. Includes access to Application and Threat Intelligence Program (ATI) and updates for the purchased term. Requires license term to be specified (must be purchased in multiples of years, list price is per unit per year). TAA Compliant

939-9609

IXIA BreakingPoint VE (Virtual Edition) 1G (Floating Worldwide Perpetual License). Enables 1 Gbps of throughput, 2M concurrent SuperFlows, and 1 Security / Security-NP components. Includes access to Application and Threat Intelligence Program (ATI) and updates for 1-year (list price is per unit). Access to ATI updates the after purchased term can be renewed using the BreakingPoint VE ATI Renewal (909-0859) license. TAA Compliant.

939-9619

IXIA BreakingPoint VE (Virtual Edition) 10G (Floating Worldwide Perpetual License). Enables 10 Gbps of throughput, 20M concurrent SuperFlows, and 2 Security / Security-NP components. Includes access to Application and Threat Intelligence Program (ATI) and updates for 1-year (list price is per unit). Access to ATI updates the after purchased term can be renewed using the BreakingPoint VE ATI Renewal (909-0859) license. TAA Compliant.

939-9649

IXIA BreakingPoint VE (Virtual Edition) 100G (Floating Worldwide Perpetual License). Enables 100 Gbps of throughput, 200M concurrent SuperFlows, and 4 Security / Security-NP components. Includes access to Application and Threat Intelligence Program (ATI) and updates for 1-year (list price is per unit). Access to ATI updates the after purchased term can be renewed using the BreakingPoint VE ATI Renewal (909-0859) license. TAA Compliant.