DATA SHEET

BreakingPoint Virtual Edition (VE)

Virtualized Application and Security Testing

Problem: With Virtualization of Network and Security Functions, Everything Known Becomes Unknown

Today’s 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—like application delivery, load balancing, data packet inspection (DPI), firewall, intrusion prevention system (IPS), and sandbox components—off dedicated hardware onto virtualized servers. Virtualized tools need to deliver the same or better performance and similar security efficacy than the traditional hardware appliances. Without a way to properly test these virtualized application and security devices, customer quality of experience (QoE) is at risk.

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

Ixia’s 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. To build resilient physical or virtual networks, you can rely on by using BreakingPoint VE to maximize security investments and optimize network architectures. Now virtualization-enabled, 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.

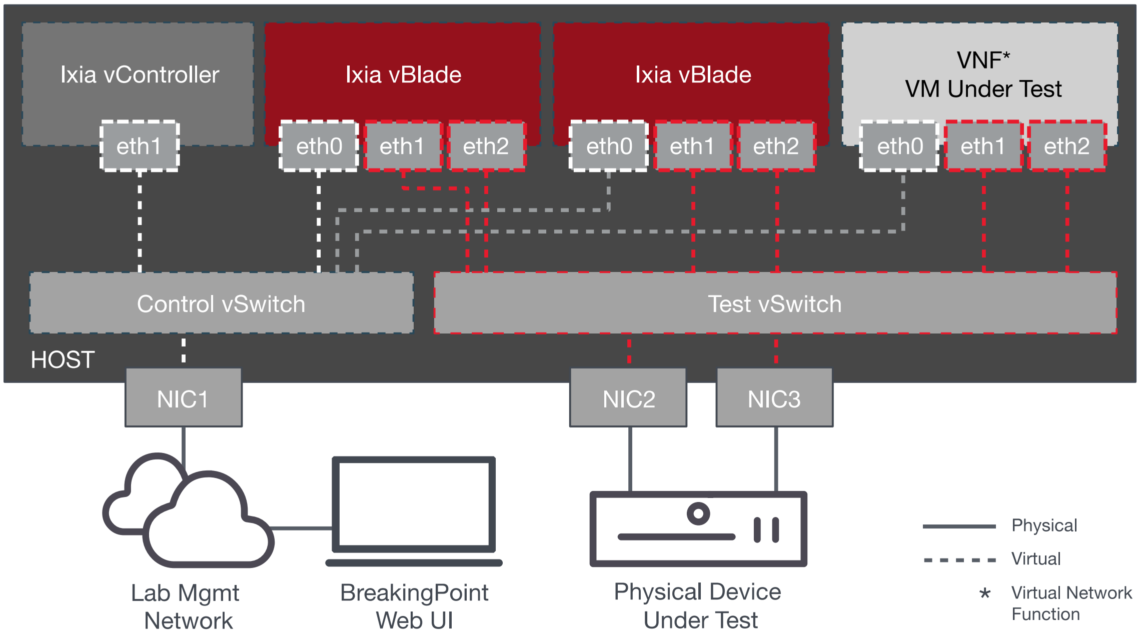
Highlights

- Validate functionality of application-aware devices and networks - virtual and physical
- Optimize virtual or physical network security devices such as IDS/IPS, DLP, UTM, NGFW, WAF, and web proxy
- Validate distributed denial of service (DDoS) and other attack defenses over cloud
- Get the best value when evaluating new security devices by performing head-to-head "bake-offs"
- Realize the savings of cloud and virtual network functions (VNF) without compromising security
- Keep current with new applications and threats Intelligence updates every two weeks
- Flexibly deploy Ixia virtual test tools that can be easily moved, changed, or scaled up and down
- Validate NFV migration by testing within OpenStack-based private clouds
- Leverage subscription-based licensing enabling low startup cost and flexibility of pay-as-you-grow OPEX model

BreakingPoint VE

KEYSIGHT TECHNOLOGIES

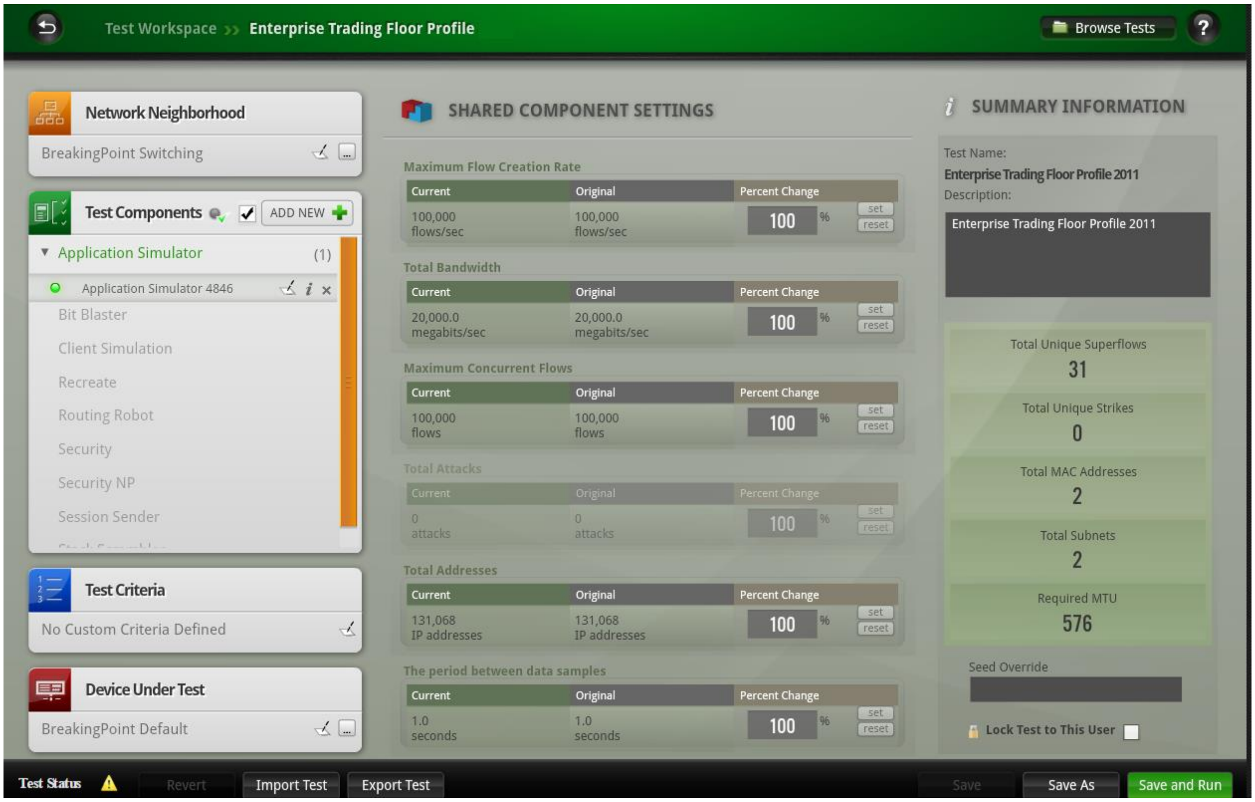
Just as important as the high-fidelity and flexible test functionality, the BreakingPoint VE subscription model is aligned with enterprise project-based IT OPEX funding requirements. Acquire the tools quickly, scale up and scale down as projects needs demand and deploy anywhere with virtualization speed and simplicity.



BreakingPoint VE deployment for both virtual and physical device tests

Key Features

- Simulates more than 300 real-world application protocols.
- Allows for customization and manipulation of any protocol, including raw data.
- Generates a mix of protocols at high speed with realistic protocol weight.
- Supports more than 37,000 attacks and malwares.
- Delivers all types of traffic simultaneously, including legitimate traffic, DDoS, and malware.
- Application and Threat Intelligence (ATI) subscription updates include latest applications and threats.
- Subscription based licensing model comes an all-inclusive license that reduces startup cost.
- Seamless transition between hardware and virtual platforms thanks to shared configuration files.
- Easy translation of functional and performance testing from physical to virtual environments.
- Supports major hypervisors allowing deployment in a wide variety of virtualized environments.
- Common Licensing Server shared among BreakingPoint VE, IxLoad VE, and IxNetwork VE.



Network Neighborhood

BreakingPoint Switching

Test Components ☑ ADD NEW

▾ Application Simulator (1)

● Application Simulator 4846

Bit Blaster

Client Simulation

Recreate

Routing Robot

Security

Security NP

Session Sender

Test Criteria

No Custom Criteria Defined

Device Under Test

BreakingPoint Default

SHARED COMPONENT SETTINGS

Maximum Flow Creation Rate

Current	Original	Percent Change
100,000 flows/sec	100,000 flows/sec	100 %

Total Bandwidth

Current	Original	Percent Change
20,000.0 megabits/sec	20,000.0 megabits/sec	100 %

Maximum Concurrent Flows

Current	Original	Percent Change
100,000 flows	100,000 flows	100 %

Total Attacks

Current	Original	Percent Change
0 attacks	0 attacks	100 %

Total Addresses

Current	Original	Percent Change
131,068 IP addresses	131,068 IP addresses	100 %

The period between data samples

Current	Original	Percent Change
1.0 seconds	1.0 seconds	100 %

SUMMARY INFORMATION

Test Name:
Enterprise Trading Floor Profile 2011

Description:
Enterprise Trading Floor Profile 2011

Total Unique Superflows: 31

Total Unique Strikes: 0

Total MAC Addresses: 2

Total Subnets: 2

Required MTU: 576

Seed Override

Lock Test to This User □

BreakingPoint GUI configured with an enterprise trading floor application mix test

Specifications

Feature	System Controller	Virtual Blade
Maximum # of Virtual Ports	96	8
Maximum # of Virtual Blades	12	N / A
Maximum Simultaneous # of Users	20	8
Guest OS	CentOS 7.6	CentOS 7.6
vCPU	8 vCPUs	4 vCPUs
Memory	8 GB RAM	8 GB RAM
Disk	20 GB	14 GB

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 format and packaging for **Manual Deployment** Scenario (using the platform specific tools for deploying the Ixia 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 Container	N / A	N / A

BreakingPoint VE distribution format and packaging for **Automatic Deployment** Scenario (using the Deployment Wizard within the BreakingPoint Web UI 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

Platform	System Controller	Virtual Blade
Microsoft Hyper-V	N / A	N / A
Docker Container	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, Ixia will make reasonable efforts to address them, but cannot guarantee specific outcomes or results. In such rare cases, the proposed solution is to use the qualified environment.

Category		Qualified	Compatible
Hypervisor and Host OS		VMware vSphere ESXi 6.X KVM over CentOS 7.X KVM over Ubuntu 16.04 LTS Microsoft Hyper-V Windows 2016	VMware vSphere ESXi 5.X KVM over CentOS 6.X KVM over Ubuntu 14.04 LTS KVM over Ubuntu 18.04 LTS KVM over RHEL 6.X KVM over RHEL 7.X
Management and Orchestration		VMware vCenter 6.X OpenStack Newton (vanilla distribution)	VMware vCenter 5.X Other OpenStack-based platforms (vanilla distributions) Other OpenStack-based platforms (vendor-specific distributions)
Network Connection and vNIC Driver	**Virtual Switch**	VMXNET3 (on VMware) VIRTIO (on KVM)	N / A
	PCI-PT	Intel 10G – IXGBE Intel 10G / 25G / 40G – I40E Mellanox 10G / 25G / 40G – MLX4 / MLX5*	N / A
	SR-IOV	Intel 10G – IXGBEVF Intel 10G / 25G / 40G – I40EVF Mellanox 10G / 25G / 40G – MLX4 / MLX5*	N / A

Category	Qualified	Compatible
Virtual Switch Model	Virtual Standard Switch (on VMware) Virtual Distributed Switch (on VMware) Linux Bridges (on KVM) Open Virtual Switch (on KVM) Open Virtual Switch (on OpenStack)	Linux Bridges (on OpenStack)
Physical CPU	DPDK Capable CPU Required	
* DPDK Performance Acceleration not supported with Mellanox NIC connected in PCI-PT / SR-IOV mode.		

Protocols and Features

BreakingPoint VE is powered by Ixia's application and threat intelligence (ATI) program that delivers a wide variety of applications and attacks to emulate traffic mix and security threats of small medium or large enterprises, service providers or government organizations at scale. The application and attack emulations are complemented with BreakingPoint's 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 – 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

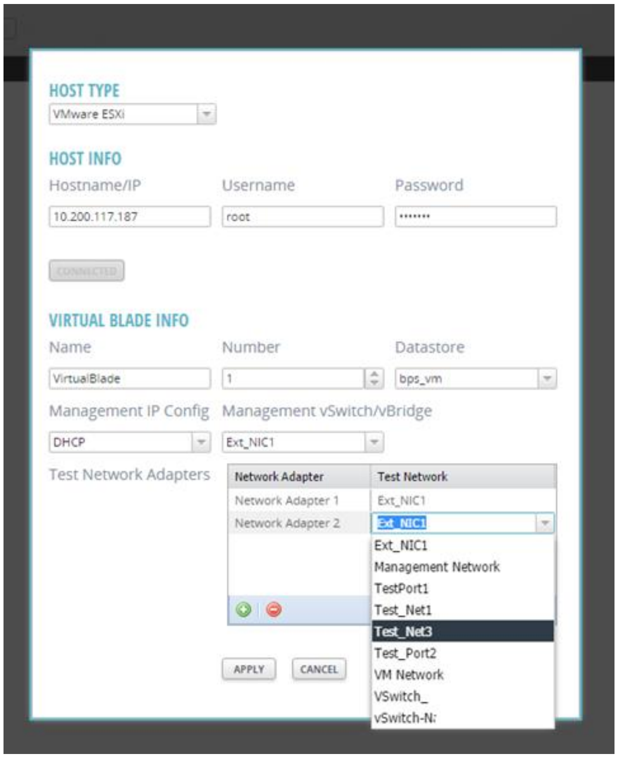
Specification	Description
Network Access	• IPv4 / IPv6 Static Hosts • IPv4 / IPv6 External Hosts • IPv4 / IPv6 Router • IPv4 / IPv6 DNS • IPv4 DHCP Client / Server • IPsec IKEv1 / IKEv2 • NAT • VLAN
Test Methodologies / Labs	• RFC 2544 Lab • Session Sender Lab • Multicast Lab • Lawful Intercept Lab • DDoS Lab
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

Specification	Description
	◦ 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 – 1Gbps of throughput, 2M concurrent super flows and 1x Security and Security NP component ◦ 10G Tier – 10Gbps of throughput, 20M concurrent super flows and 2x Security and Security NP component

Product Capabilities

Simple and Easy VM Deployment

Deploying and adding BreakingPoint VM card and test port can be achieved through the BreakingPoint's GUI. It's a simple process of providing credentials to the VM Host and there on the rest of the process has been entirely automated to do the VM deployment and getting it added to the BreakingPoint chassis.



HOST TYPE

VMware ESXi

HOST INFO

Hostname/IP: 10.200.117.187

Username: root

Password: •••••••

VIRTUAL BLADE INFO

Name: VirtualBlade

Number: 1

Datastore: bps_vm

Management IP Config: DHCP

Management vSwitch/vBridge: Ext_NIC1

Test Network Adapters

Network Adapter	Test Network
Network Adapter 1	Ext_NIC1
Network Adapter 2	Ext_NIC1

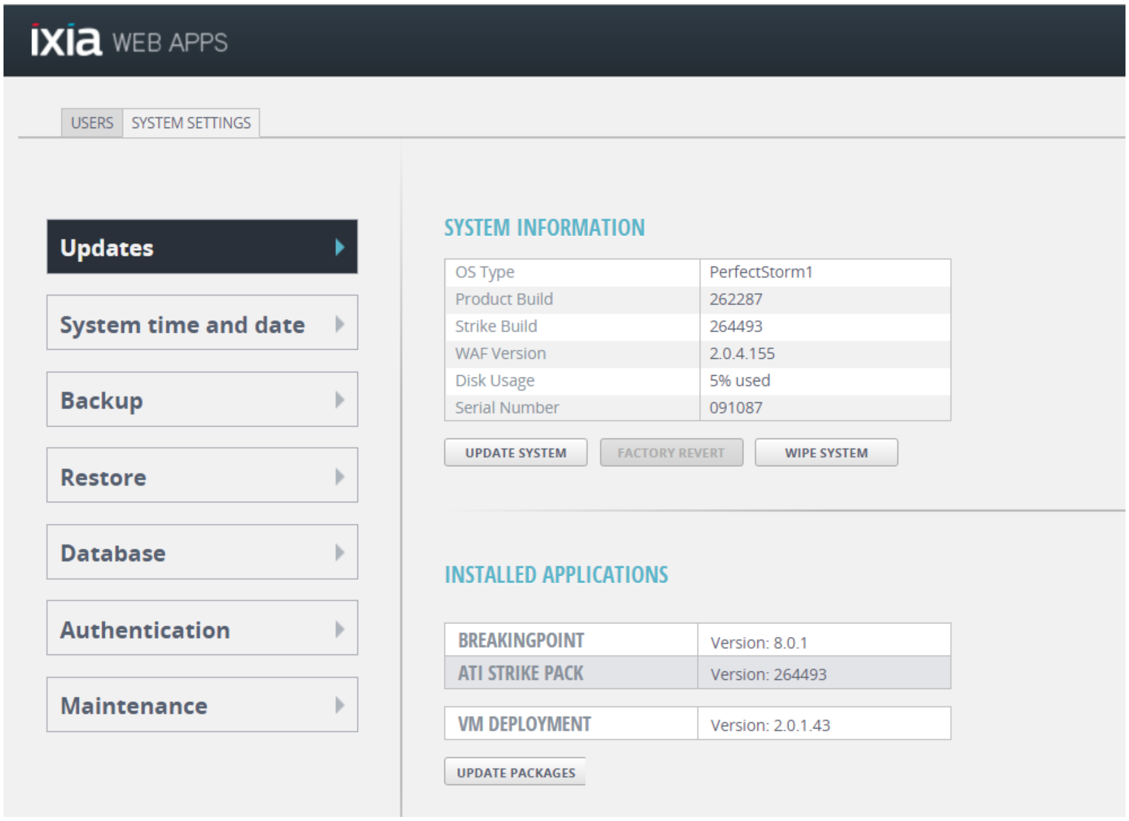
BreakingPoint VM deployment through the GUI Admin page.

Application and Threat Intelligence (ATI) Program

Ixia'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, etc.), 330+ popular applications, and over 2,000 canned tests.

Additionally, the ATI program ensures:

- Newer applications and attacks can be incorporated in BreakingPoint without the need of any firmware or OS updates
- Users stay up to date with the ever-changing cyber-world—new applications are added and popular applications are updated to current versions
- Monthly malware packages contain fast-changing malware and botnet attacks
- Well researched, real-world application mixes that emulate traffic patterns of diverse demographics and business verticals



SYSTEM INFORMATION

OS Type	PerfectStorm1
Product Build	262287
Strike Build	264493
WAF Version	2.0.4.155
Disk Usage	5% used
Serial Number	091087

INSTALLED APPLICATIONS

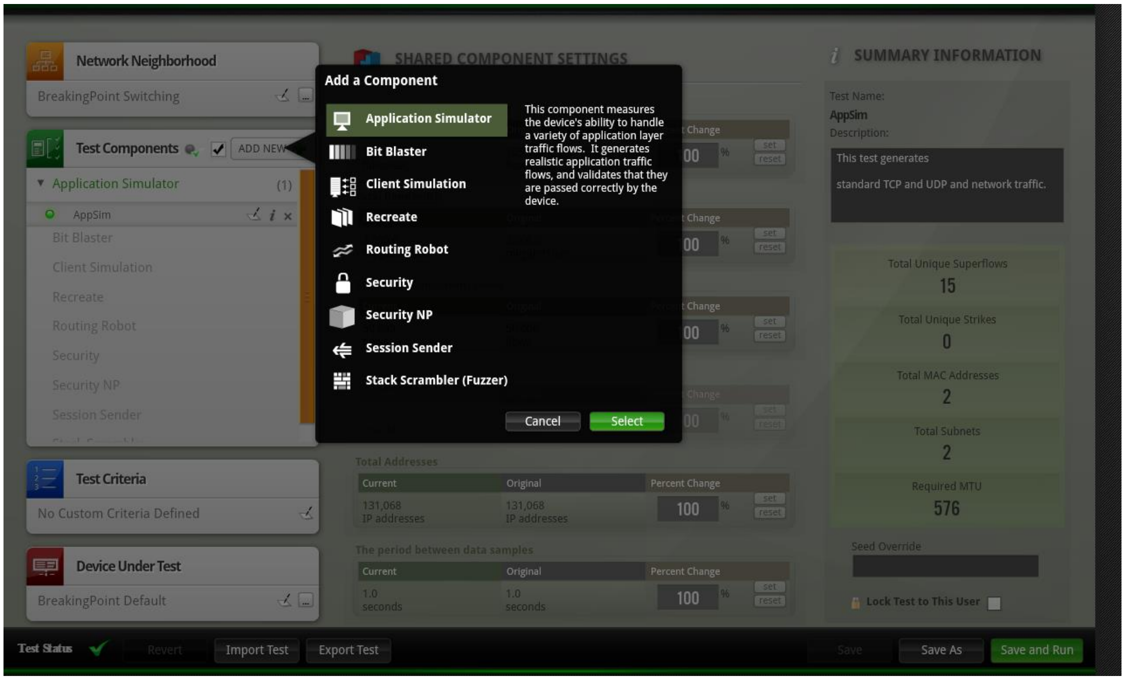
BREAKINGPOINT	Version: 8.0.1
ATI STRIKE PACK	Version: 264493
VM DEPLOYMENT	Version: 2.0.1.43

ATI packages can be updated through the intuitive BreakingPoint GUI

BreakingPoint Test Components

BreakingPoint offer a single Web GUI 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.

Test Components	
Application Simulator	Allows users to create mix of applications and run tests in 2-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 lows against real servers (device under test) in 1-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 TrafficREWIND's ability to record and synthesize production traffic characteristics over extended periods of time.
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 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 IP, TCP, UDP, ICMP, and Ethernet packets (produced by a fuzzing technique) to the DUT



This component measures the device's ability to handle a variety of application layer traffic flows. It generates realistic application traffic flows, and validates that they are passed correctly by the device.

This test generates

standard TCP and UDP and network traffic.

BreakingPoint purpose-built test components

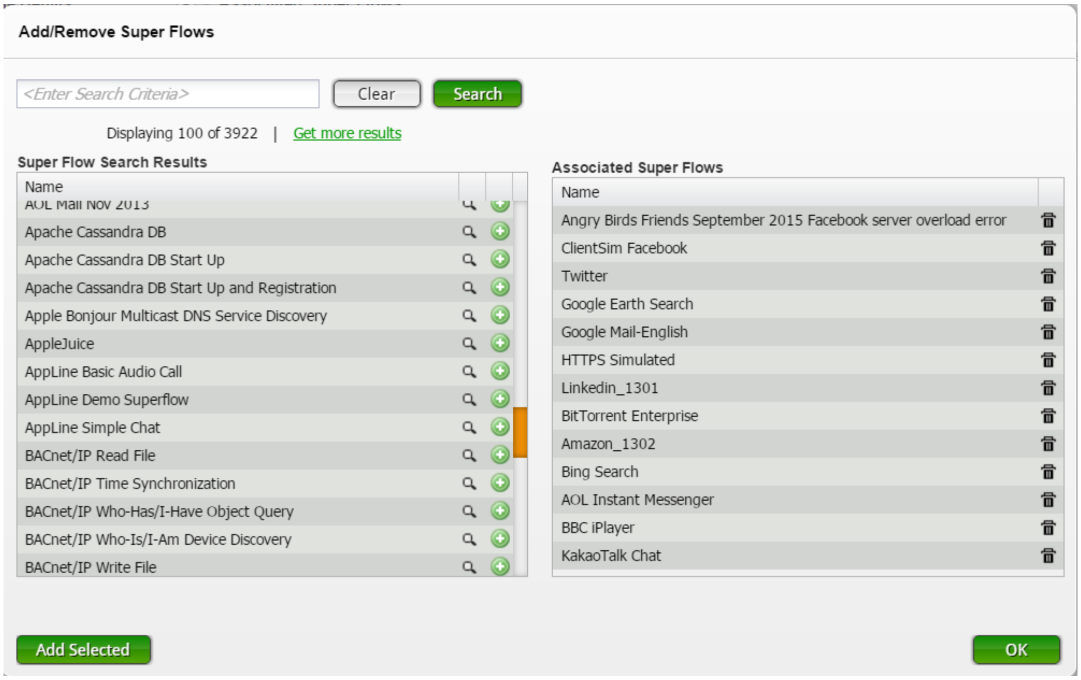
Application Simulation

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:

- 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.



Add/Remove Super Flows

Displaying 100 of 3922 | Get more results

Super Flow Search Results

Name
AOL Mail Nov 2013
Apache Cassandra DB
Apache Cassandra DB Start Up
Apache Cassandra DB Start Up and Registration
Apple Bonjour Multicast DNS Service Discovery
AppleJuice
AppLine Basic Audio Call
AppLine Demo Superflow
AppLine Simple Chat
BACnet/IP Read File
BACnet/IP Time Synchronization
BACnet/IP Who-Has/I-Have Object Query
BACnet/IP Who-Is/I-Am Device Discovery
BACnet/IP Write File

Associated Super Flows

Name
Angry Birds Friends September 2015 Facebook server overload error
ClientSim Facebook
Twitter
Google Earth Search
Google Mail-English
HTTPS Simulated
Linkedin_1301
BitTorrent Enterprise
Amazon_1302
Bing Search
AOL Instant Messenger
BBC iPlayer
KakaoTalk Chat

BreakingPoint provides flexibility to emulate a variety of apps 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><p>Copyright (C) 2005-2011 BreakingPoint Systems, Inc. All Rights Reserved.</p><p><h5><q>Aterrible country, Mr.</q><q>Bickersteth and yourself has, unfortunately</q><em>We sallied out at once</em><u>Corcoran's portrait may not have</u><b>Won't you have an egg</b><u>Who the deuce is Lady</u>
```

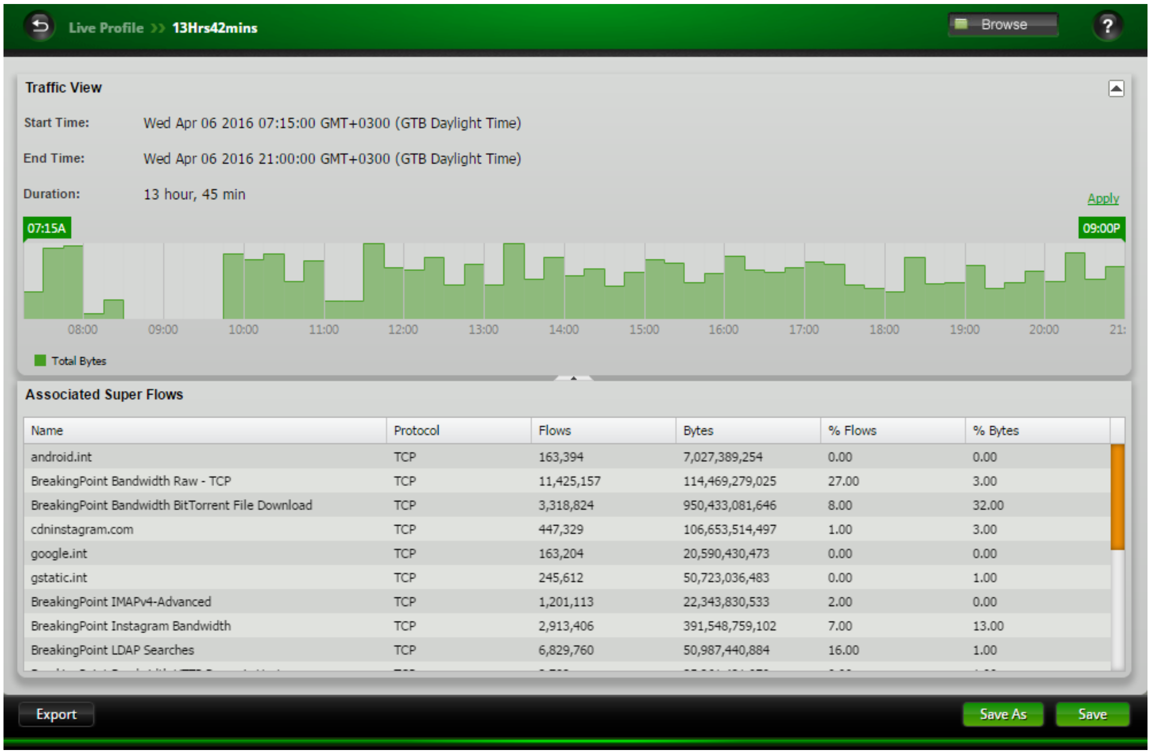
BreakingPoint generates real-world application and security strike traffic; this example shows an HTTP request and response

TrafficREWIND and Live AppSim

Ixia'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



Traffic View

Start Time: Wed Apr 06 2016 07:15:00 GMT+0300 (GTB Daylight Time)

End Time: Wed Apr 06 2016 21:00:00 GMT+0300 (GTB Daylight Time)

Duration: 13 hour, 45 min

Associated Super Flows

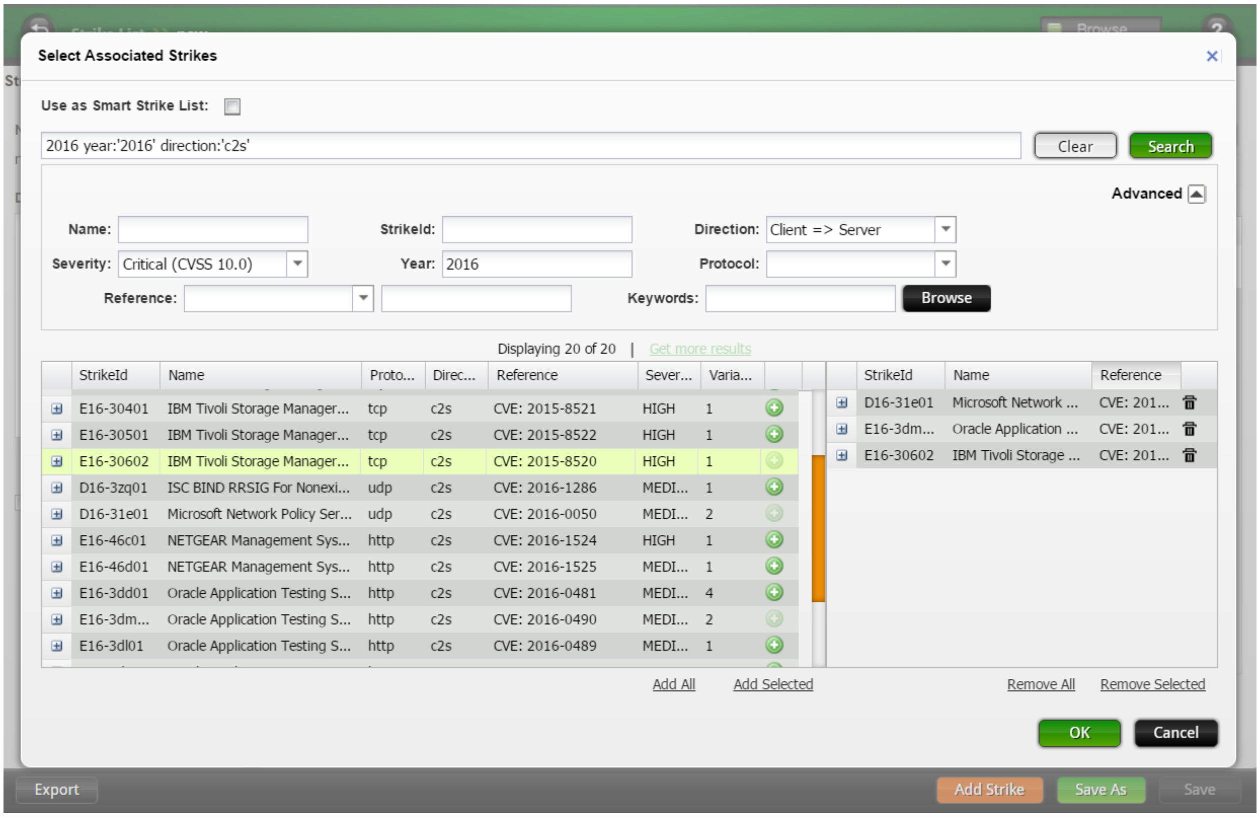
Name	Protocol	Flows	Bytes	% Flows	% Bytes
android.int	TCP	163,394	7,027,389,254	0.00	0.00
BreakingPoint Bandwidth Raw - TCP	TCP	11,425,157	114,469,279,025	27.00	3.00
BreakingPoint Bandwidth BitTorrent File Download	TCP	3,318,824	950,433,081,646	8.00	32.00
cdninstagram.com	TCP	447,329	106,653,514,497	1.00	3.00
google.int	TCP	163,204	20,590,430,473	0.00	0.00
gstatic.int	TCP	245,612	50,723,036,483	0.00	1.00
BreakingPoint IMAPv4-Advanced	TCP	1,201,113	22,343,830,533	2.00	0.00
BreakingPoint Instagram Bandwidth	TCP	2,913,406	391,548,759,102	7.00	13.00
BreakingPoint LDAP Searches	TCP	6,829,760	50,987,440,884	16.00	1.00

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
- Emulate 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



Select Associated Strikes

Use as Smart Strike List: □

2016 year:'2016' direction:'c2s'

Name:
StrikeId:
Direction: Client => Server
Severity: Critical (CVSS 10.0)
Year: 2016
Protocol:
Reference:
Keywords:

Displaying 20 of 20 | Get more results

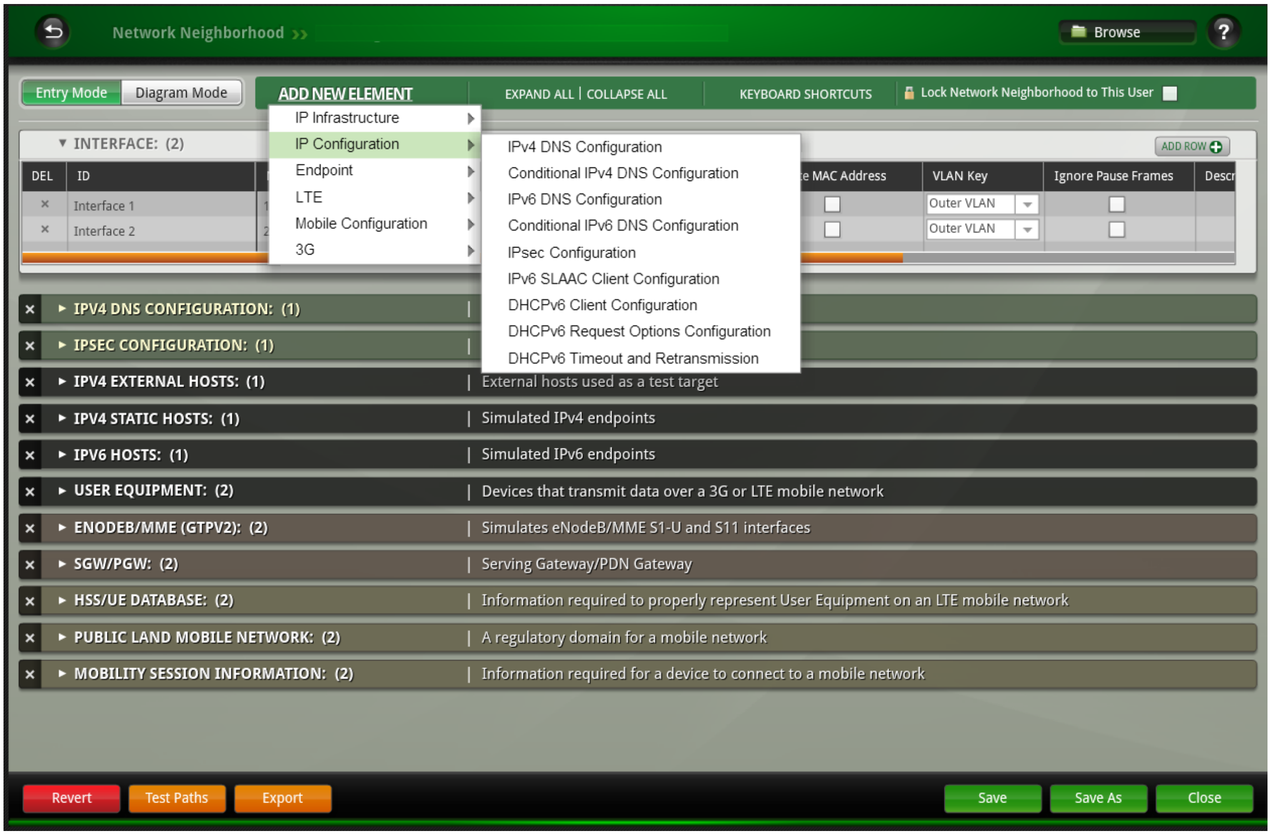
StrikeId	Name	Proto...	Direc...	Reference	Sever...	Varia...
E16-30401	IBM Tivoli Storage Manager...	tcp	c2s	CVE: 2015-8521	HIGH	1
E16-30501	IBM Tivoli Storage Manager...	tcp	c2s	CVE: 2015-8522	HIGH	1
E16-30602	IBM Tivoli Storage Manager...	tcp	c2s	CVE: 2015-8520	HIGH	1
D16-3zq01	ISC BIND RRSIG For Nonexi...	udp	c2s	CVE: 2016-1286	MEDI...	1
D16-31e01	Microsoft Network Policy Ser...	udp	c2s	CVE: 2016-0050	MEDI...	2
E16-46c01	NETGEAR Management Sys...	http	c2s	CVE: 2016-1524	HIGH	1
E16-46d01	NETGEAR Management Sys...	http	c2s	CVE: 2016-1525	MEDI...	1
E16-3dd01	Oracle Application Testing S...	http	c2s	CVE: 2016-0481	MEDI...	4
E16-3dm...	Oracle Application Testing S...	http	c2s	CVE: 2016-0490	MEDI...	2
E16-3dl01	Oracle Application Testing S...	http	c2s	CVE: 2016-0489	MEDI...	1

StrikeId	Name	Reference
D16-31e01	Microsoft Network ...	CVE: 201...
E16-3dm...	Oracle Application ...	CVE: 201...
E16-30602	IBM Tivoli Storage ...	CVE: 201...

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.



▼ INTERFACE: (2)

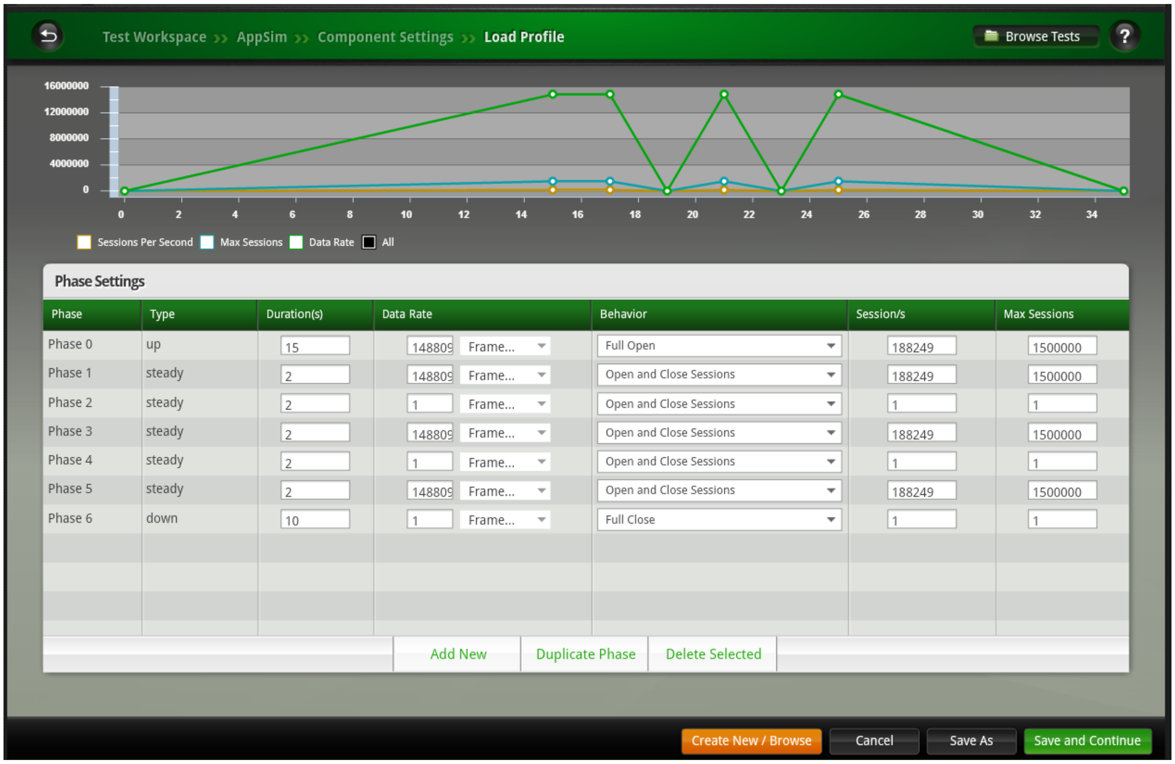
DEL	ID		e MAC Address	VLAN Key	Ignore Pause Frames	Descr
×	Interface 1	1	☐	Outer VLAN	☐	
×	Interface 2	2	☐	Outer VLAN	☐	

×	▸ IPV4 DNS CONFIGURATION: (1)	
×	▸ IPSEC CONFIGURATION: (1)	
×	▸ IPV4 EXTERNAL HOSTS: (1)	External hosts used as a test target
×	▸ IPV4 STATIC HOSTS: (1)	Simulated IPv4 endpoints
×	▸ IPV6 HOSTS: (1)	Simulated IPv6 endpoints
×	▸ USER EQUIPMENT: (2)	Devices that transmit data over a 3G or LTE mobile network
×	▸ ENODEB/MME (GTPV2): (2)	Simulates eNodeB/MME S1-U and S11 interfaces
×	▸ SGW/PGW: (2)	Serving Gateway/PDN Gateway
×	▸ HSS/UE DATABASE: (2)	Information required to properly represent User Equipment on an LTE mobile network
×	▸ PUBLIC LAND MOBILE NETWORK: (2)	A regulatory domain for a mobile network
×	▸ MOBILITY SESSION INFORMATION: (2)	Information required for a device to connect to a mobile network

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.



Phase Settings

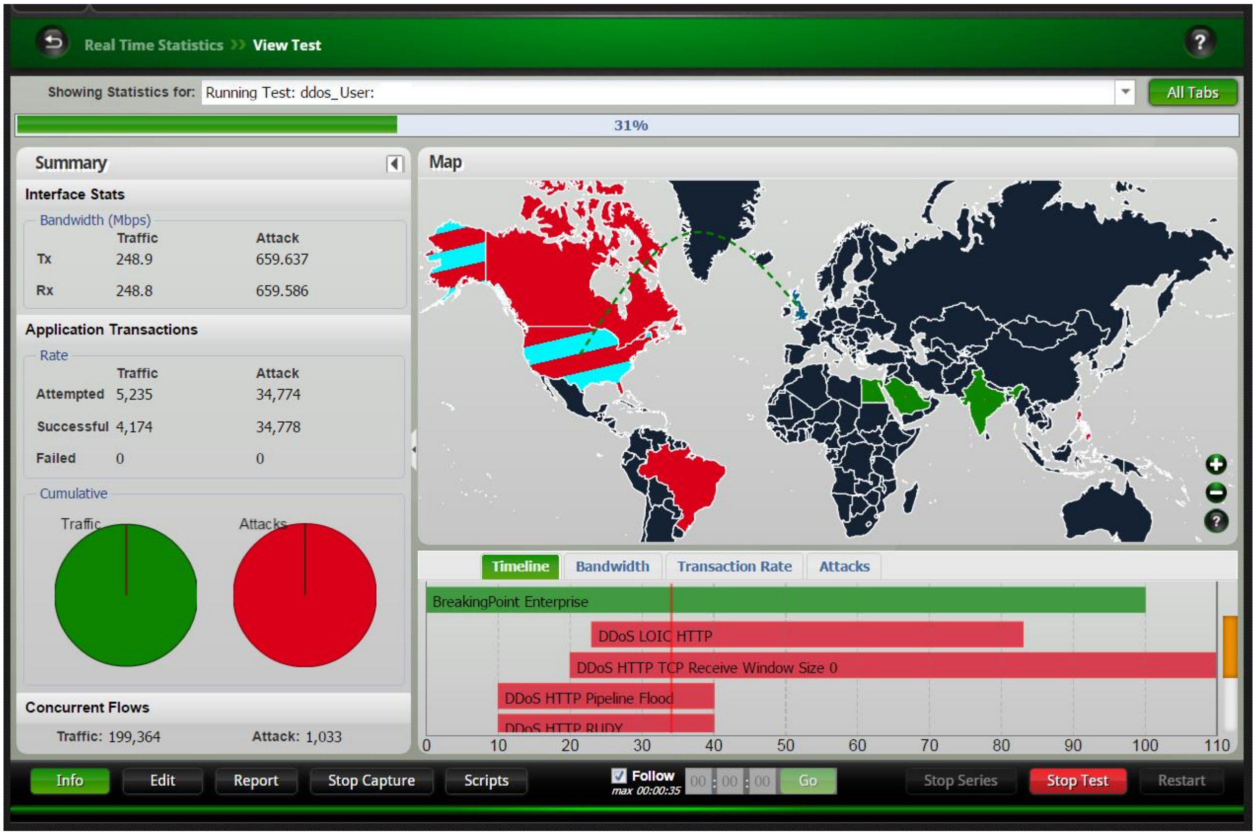
Phase	Type	Duration(s)	Data Rate		Behavior	Session/s	Max Sessions
Phase 0	up	15	148809	Frame...	Full Open	188249	1500000
Phase 1	steady	2	148809	Frame...	Open and Close Sessions	188249	1500000
Phase 2	steady	2	1	Frame...	Open and Close Sessions	1	1
Phase 3	steady	2	148809	Frame...	Open and Close Sessions	188249	1500000
Phase 4	steady	2	1	Frame...	Open and Close Sessions	1	1
Phase 5	steady	2	148809	Frame...	Open and Close Sessions	188249	1500000
Phase 6	down	10	1	Frame...	Full Close	1	1

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.



Showing Statistics for: Running Test: ddos_User:

Interface Stats

Bandwidth (Mbps)

	Traffic	Attack
Tx	248.9	659.637
Rx	248.8	659.586

Application Transactions

Rate

	Traffic	Attack
Attempted	5,235	34,774
Successful	4,174	34,778
Failed	0	0

Concurrent Flows

Traffic: 199,364 Attack: 1,033

☑ Follow

max 00:00:35

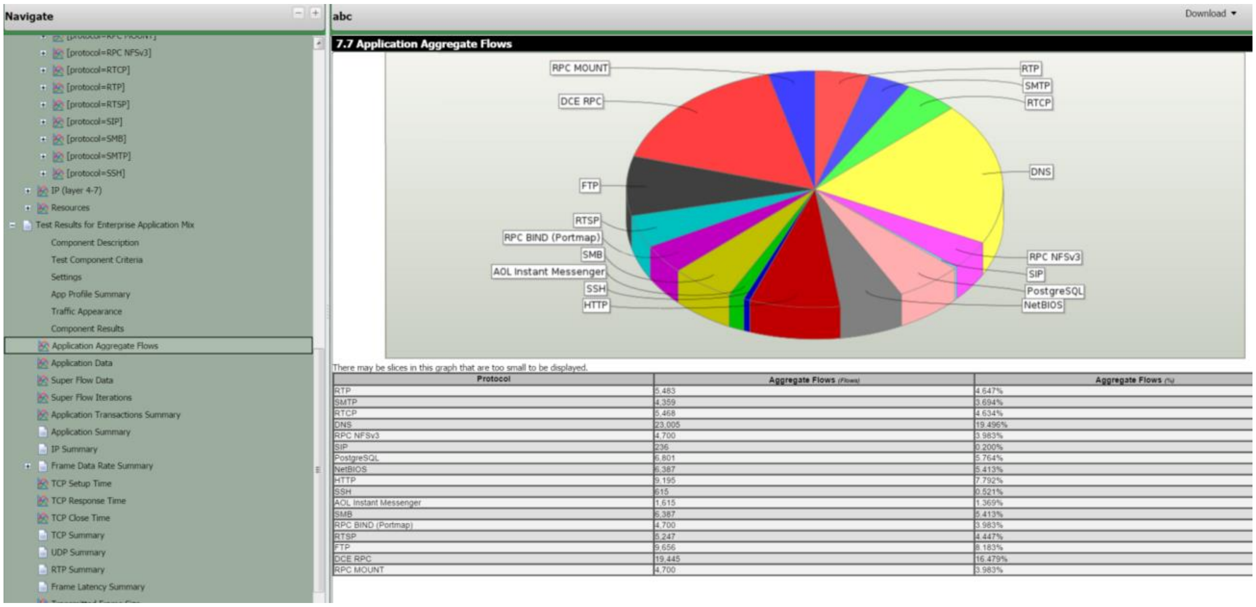
00 : 00 : 00

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.



7.7 Application Aggregate Flows

There may be slices in this graph that are too small to be displayed.

Protocol	Aggregate Flows (Flows)	Aggregate Flows (%)
RTP	5,483	4.647%
SMTP	4,359	3.694%
RTCP	5,468	4.634%
DNS	23,005	19.496%
RPC NFSv3	4,700	3.983%
SIP	236	0.200%
PostgreSQL	6,801	5.764%
NetBIOS	6,387	5.413%
HTTP	9,195	7.792%
SSH	615	0.521%
AOL Instant Messenger	1,615	1.369%
SMB	6,387	5.413%
RPC BIND (Portmap)	4,700	3.983%
RTSP	5,247	4.447%
FTP	9,656	8.183%
DCE RPC	19,445	16.479%
RPC MOUNT	4,700	3.983%

A segment of BreakingPoint report showcasing flow mix

Technology Solutions

Visit keysight.com for More Information on BreakingPoint and Ixia 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

Ordering Information

939-9600

BreakingPoint Virtual Edition (VE) SUBSCRIPTION FLOATING License. INCLUDES access to Application and Threat Intelligence Program (ATI) and updates for the purchased term (List price is per unit, per year). REQUIRES: License term to be specified (MUST be purchased in multiples of years). Supports 1 Gig throughput per unit.

939-9610

BreakingPoint Virtual Edition (VE) SUBSCRIPTION 10G FLOATING License. INCLUDES access to Application and Threat Intelligence Program (ATI) and updates for the purchased term (List price is per unit, per year). REQUIRES: License term to be specified (MUST be purchased in multiples of years). Supports 10 Gig throughput per unit.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT
TECHNOLOGIES