DATA SHEET

BreakingPoint® Applications and Security Testing

Problem: Real-Time Challenges for Real-World Testing

These days, organizations rely on a wide variety of security solutions to protect their networks from cyber-attacks and traffic anomalies. But the more tools deployed, the more complex a security infrastructure becomes. The result: a hodgepodge of security solutions that are tough to verify and challenging to scale. Worse yet, these complex system interactions pose a serious risk to security performance and network resiliency.

Solution: An Easy-to-Use Testing Ecosystem for Modern Network Needs

To counter such challenges, businesses require an application and security test solution that can verify the stability, accuracy, and quality of networks and network devices.

Enter BreakingPoint. By simulating real-world legitimate traffic, distributed denial of service (DDoS), exploits, malware, and fuzzing, BreakingPoint validates an organization's security infrastructure, reduces the risk of network degradation by almost 80%, and increases attack readiness by nearly 70%.

How might a particular configuration or security setup withstand a cyber-attack? BreakingPoint addresses that by simulating both good and bad traffic to validate and optimize networks under the most realistic conditions. Security infrastructures can also be verified at high-scale, ensuring ease of use, greater agility, and speedy network testing.

Highlights

- Measure and harden the performance of network and security devices
- Validate network and data center performance by recreating busy hour Internet traffic at scale
- Stress network infrastructures with 46,000+ security attacks, malware, botnets, and evasion techniques
- Find network issues and prepare for the unexpected with the industry's fastest protocol fuzzing capabilities
- Emulate sophisticated, large-scale DDoS and botnet attacks to expose hidden weaknesses
- Ensure the always-on user experience in the midst of complexity and exploding traffic volume
- Train staff by simulating highly realistic cyber-range/training environment
- Validate the performance and security resiliency of service provider networks using emulations over 3G/4G/LTE
- Amplify test traffic realism by running TrafficREWIND summary configurations that replicate the dynamic nature of production networks and applications

KEYSIGHT TECHNOLOGIES

BreakingPoint test solutions ensure:

- Network security
  - Maximize security investments with onsite network-specific proof-of-concept (PoC) validation
  - Optimize next-generation firewalls (NGFWs), intrusion prevention systems (IPS), and other security devices
  - Validate DDoS defenses
  - Build networks and cloud infrastructures that are resilient to attacks
- Network performance
  - Ensure the always-on user experience in the midst of complexity and exploding traffic volume
  - Validate and optimize 3G and 4G/LTE networks under the most realistic conditions, using real mobile applications over mobile tunneling and roaming, and get per-user equipment (UE) statistics

Key Features

- Simulates more than 450 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 46,000 attacks and malwares
- Delivers from a single port all types of traffic simultaneously, including legitimate traffic, DDoS, and malware
- Bi-monthly Application and Threat Intelligence (ATI) subscription updates ensure you're are current with the latest applications and threats
- Combined with the CloudStorm™ platform, BreakingPoint reaches a staggering performance with a fully-populated chassis—2.4 Tbps / 1.44 billion sessions and 42 million connections per second—to emulate enterprise-wide networks to continent-scale mobile carrier networks

Product Capabilities

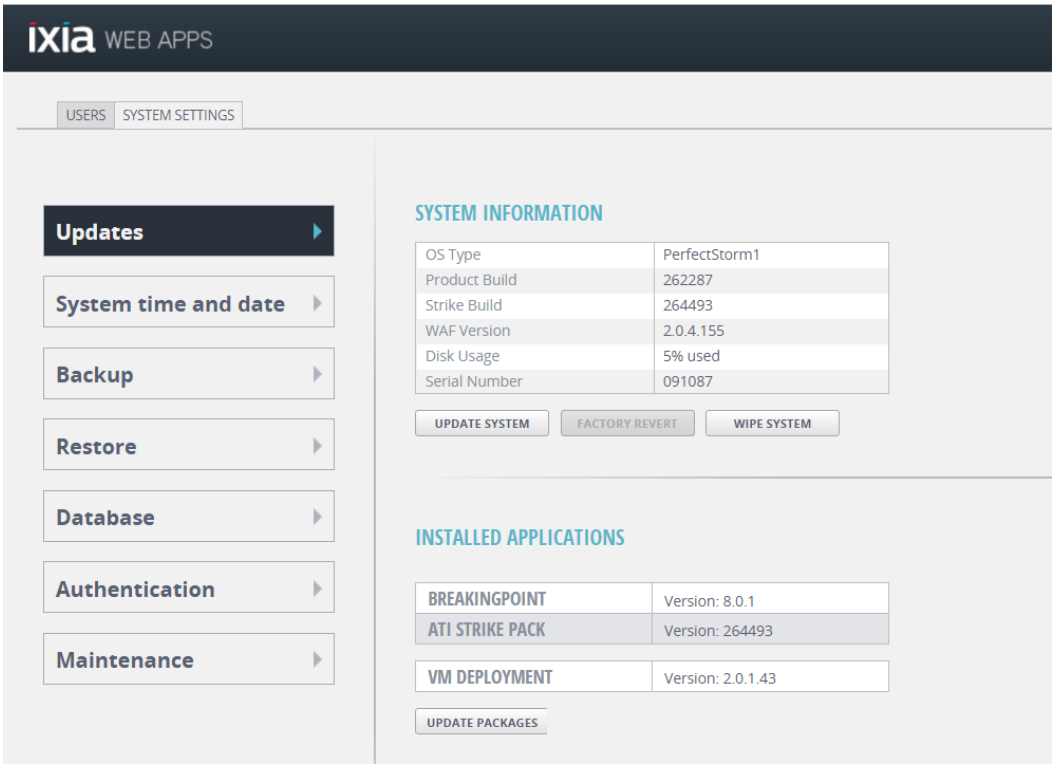
Application and Threat Intelligence (ATI) program

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 46,000+ attacks (Exploits, Malwares, DDoS, etc.), 360+ popular applications, and over 2,000 canned examples.

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.



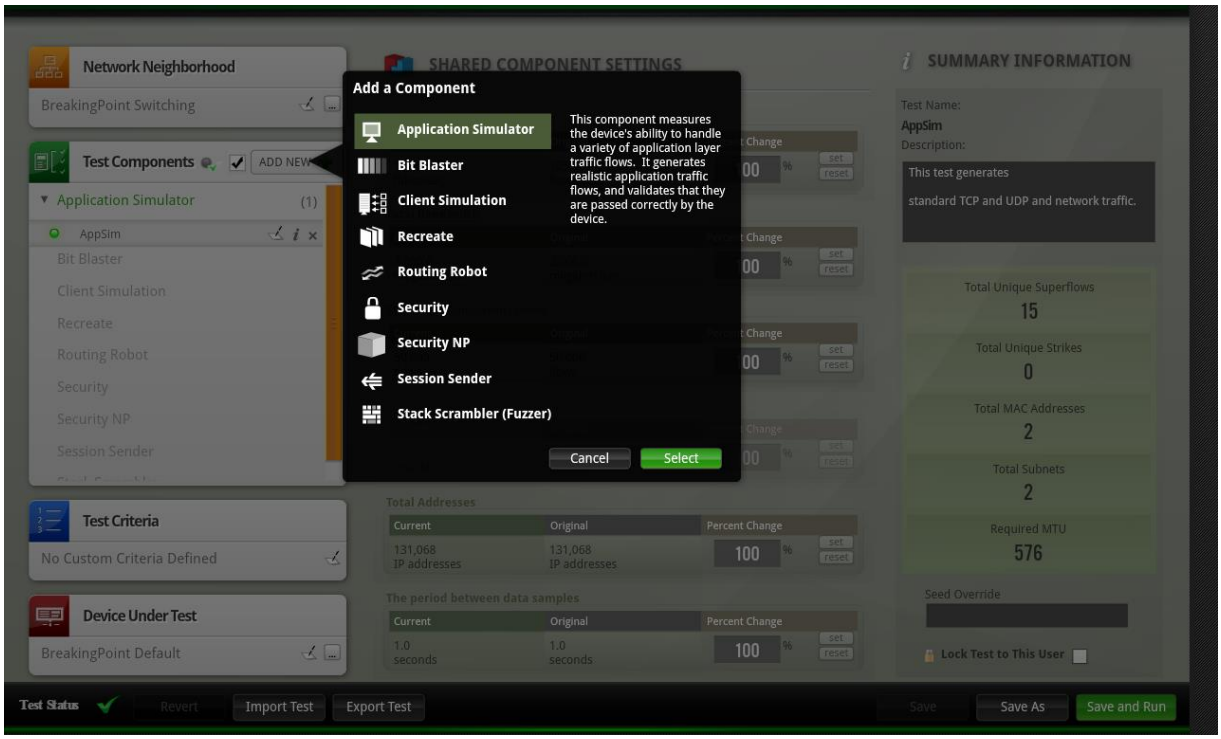
ATI packages can be updated through the intuitive BreakingPoint GUI

BreakingPoint test components

BreakingPoint offer a single Web GUI for management results in simple, central control of all components and capabilities. Test components helps 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 Superflows against real servers (device under test) in 1-Arm mode (BreakingPoint being the client)

Test Components	
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



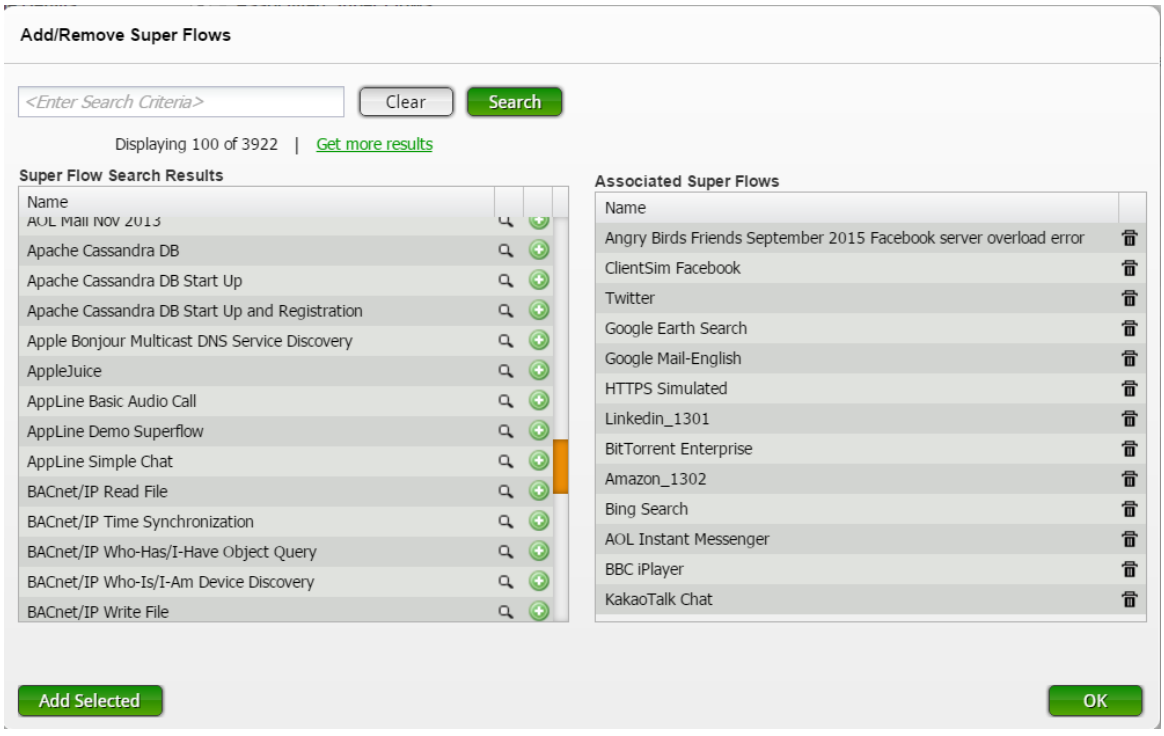
BreakingPoint purpose-built test components

Application simulation

BreakingPoint simulates over 450 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.



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><met
a 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>
```

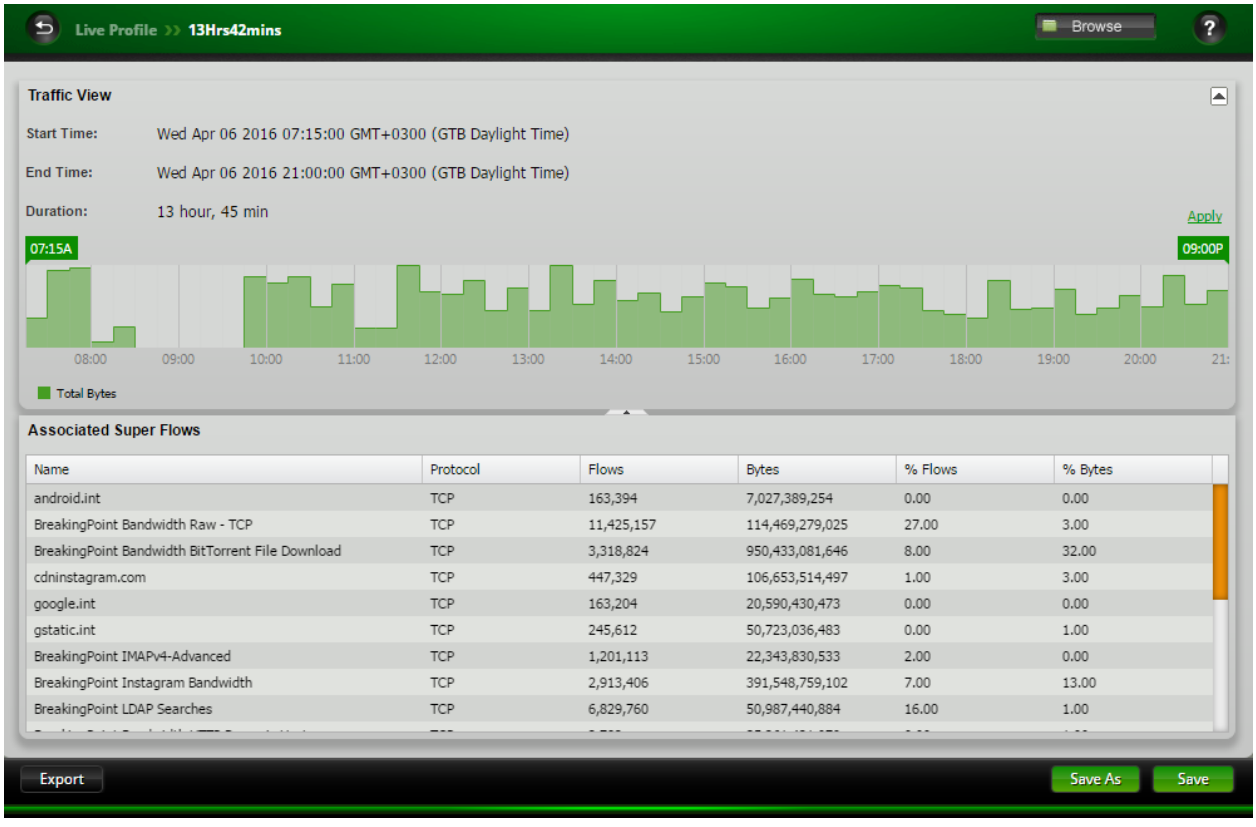
BreakingPoint generates real-world application and security strike traffic; this example shows an HTTP request and response

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

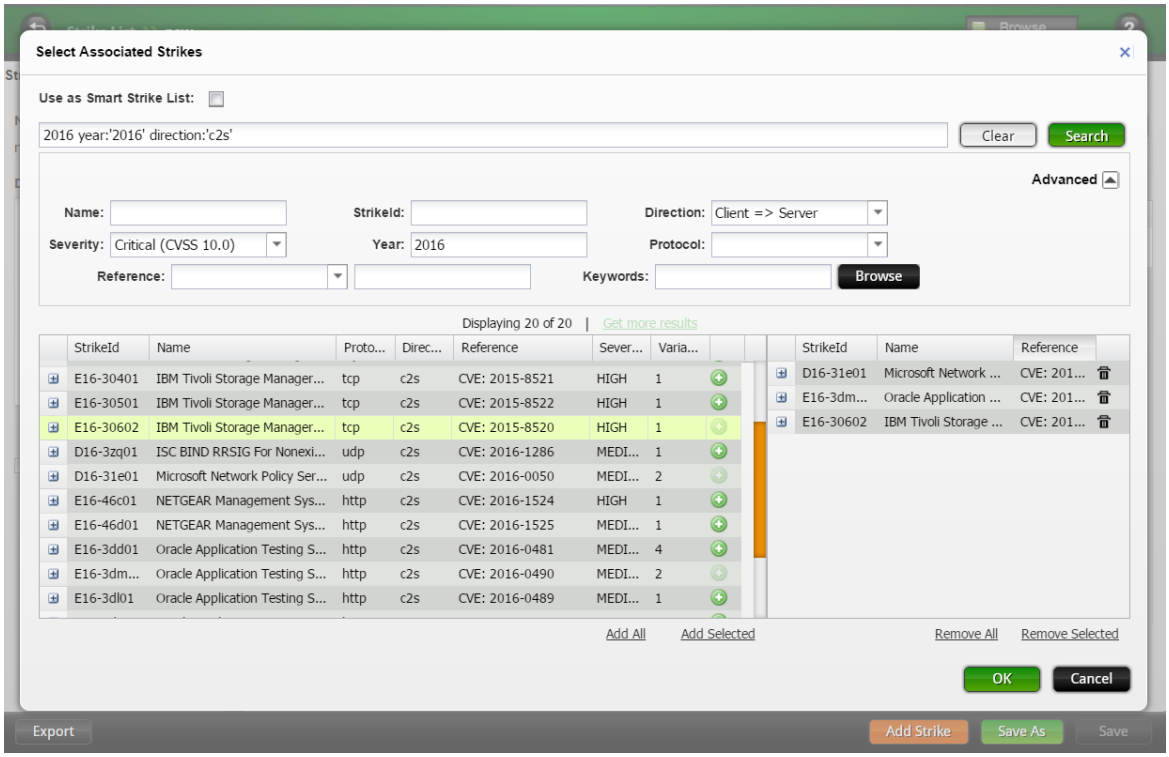


Live Profile created by importing a TrafficREWIND traffic summary configuration

Comprehensive security

BreakingPoint delivers the industry's most comprehensive solution to 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.

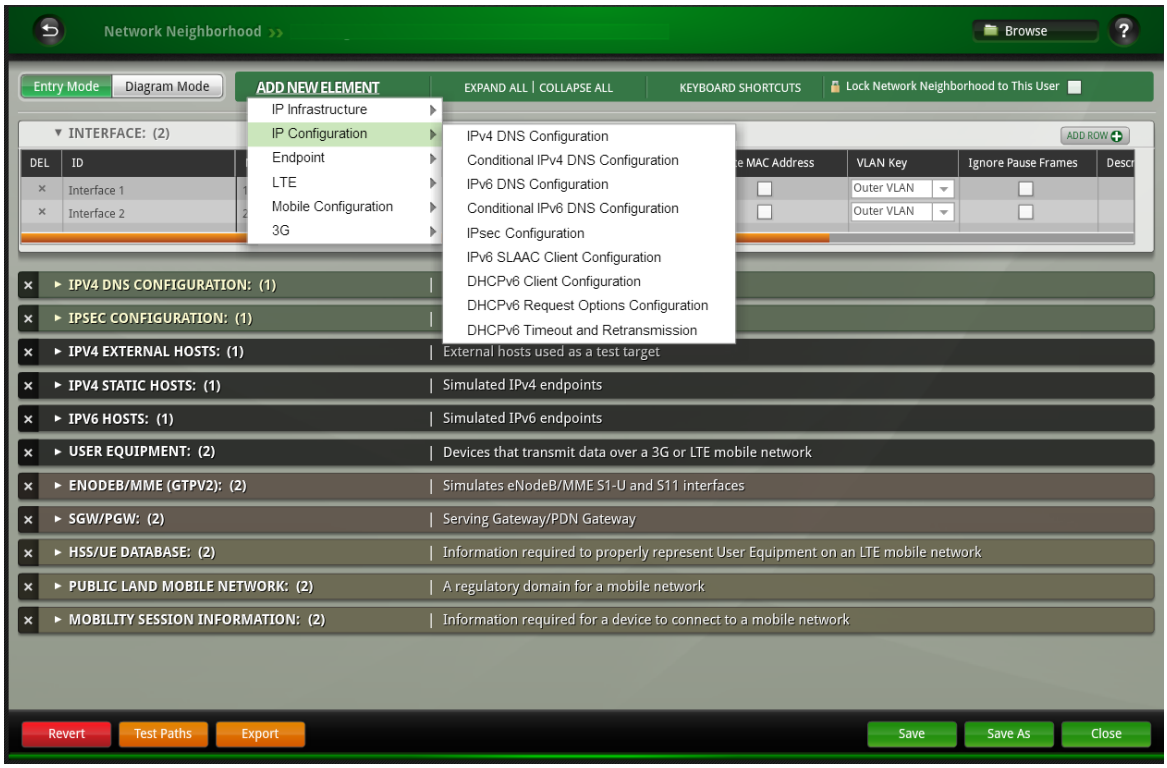
- Supports over 46,000 strikes and malware and the attacks can be obfuscated by over 100 evasion techniques
- Emulate botnets, from zombie to command and control (C&C) communication
- Simulates a variety of volumetric, protocol, and application-layer DDoS attacks
- Generates legitimate and malicious 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



An intelligent search bar makes it easier to browse through the 46,000+ attacks

Network Neighborhood

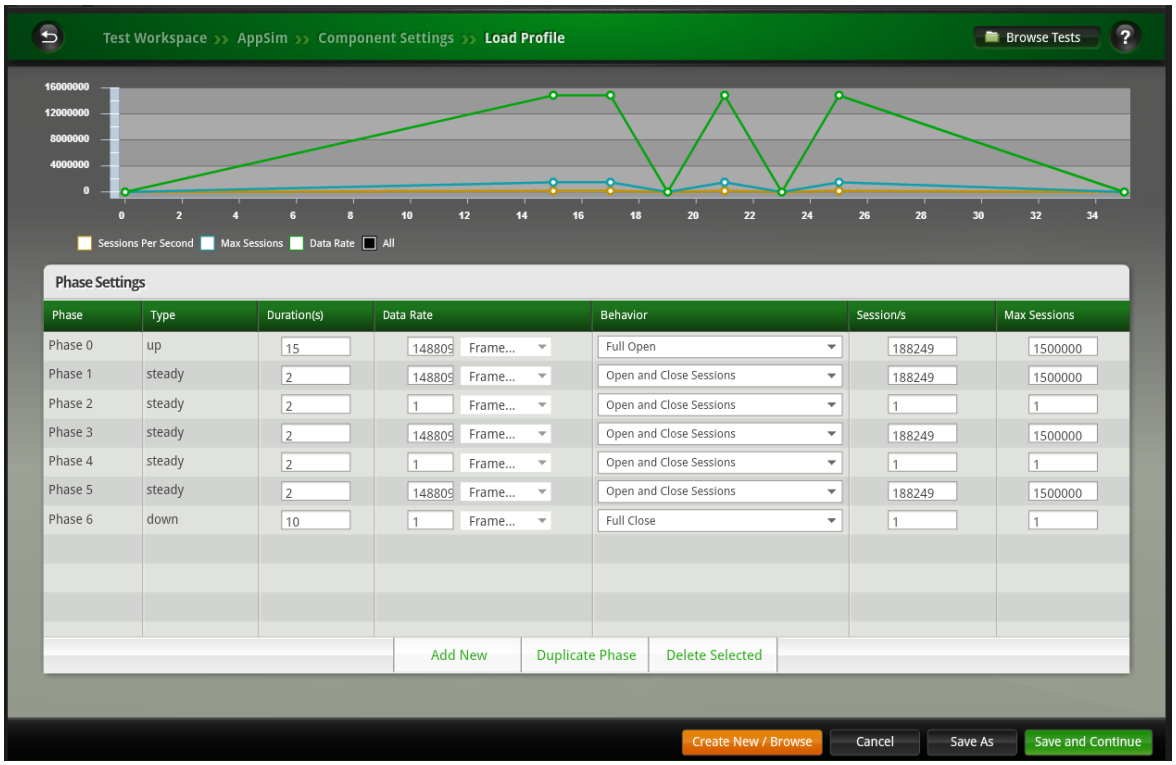
BreakingPoint's Network Neighborhood provides flexibility for the user to create simple to highly complex network environments. It includes support of commonly used network elements like IPV4, IPV6, VLAN, IPsec, DHCP, DNS and for 3G/4G mobile infrastructure network elements.



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.

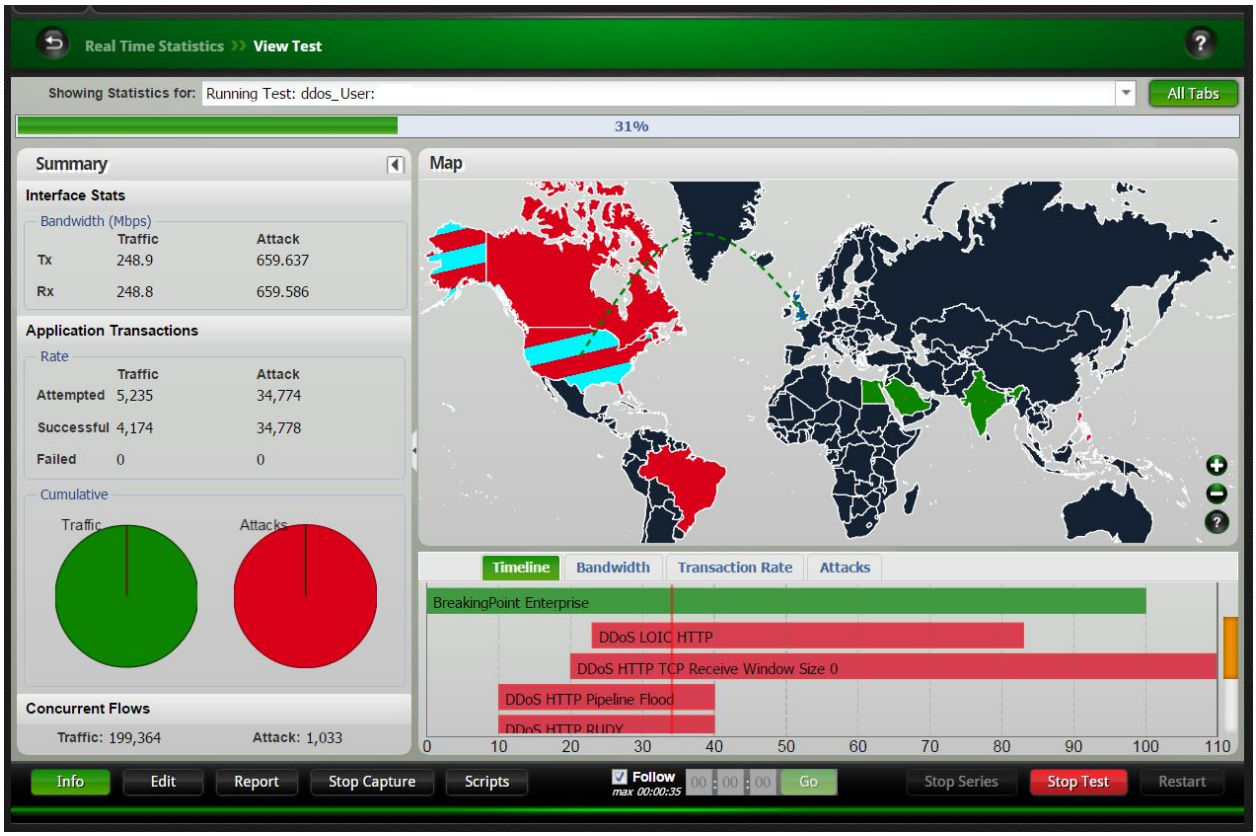


A BreakingPoint MicroBurst Load profile

Built-in test 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.



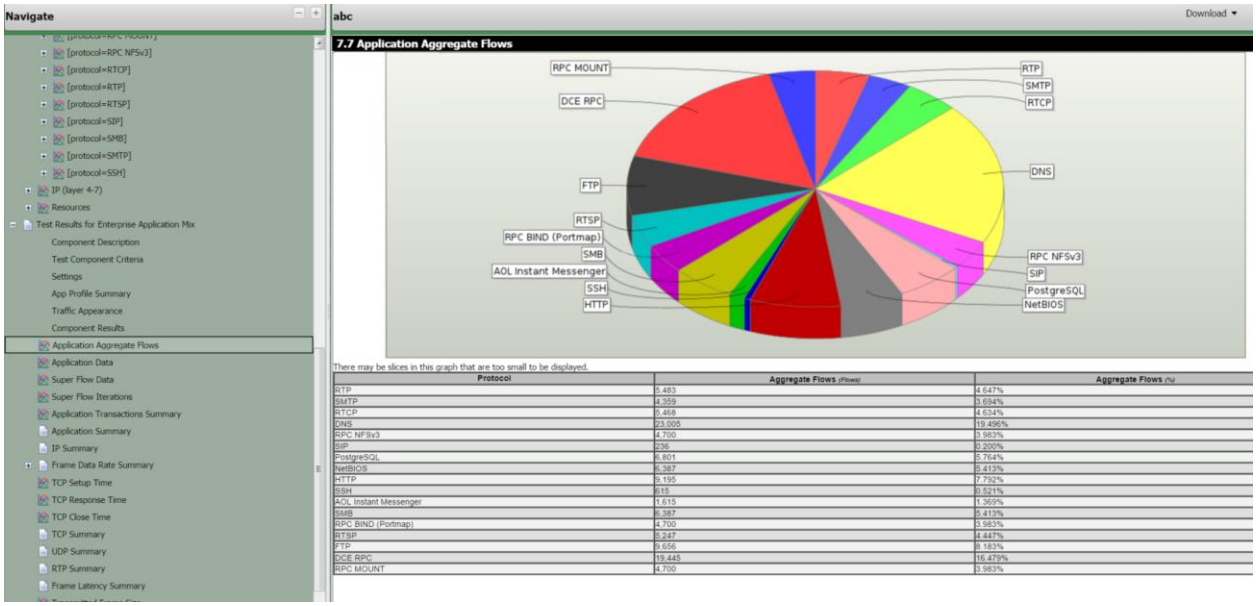
A test configured with DDoS Lab

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.

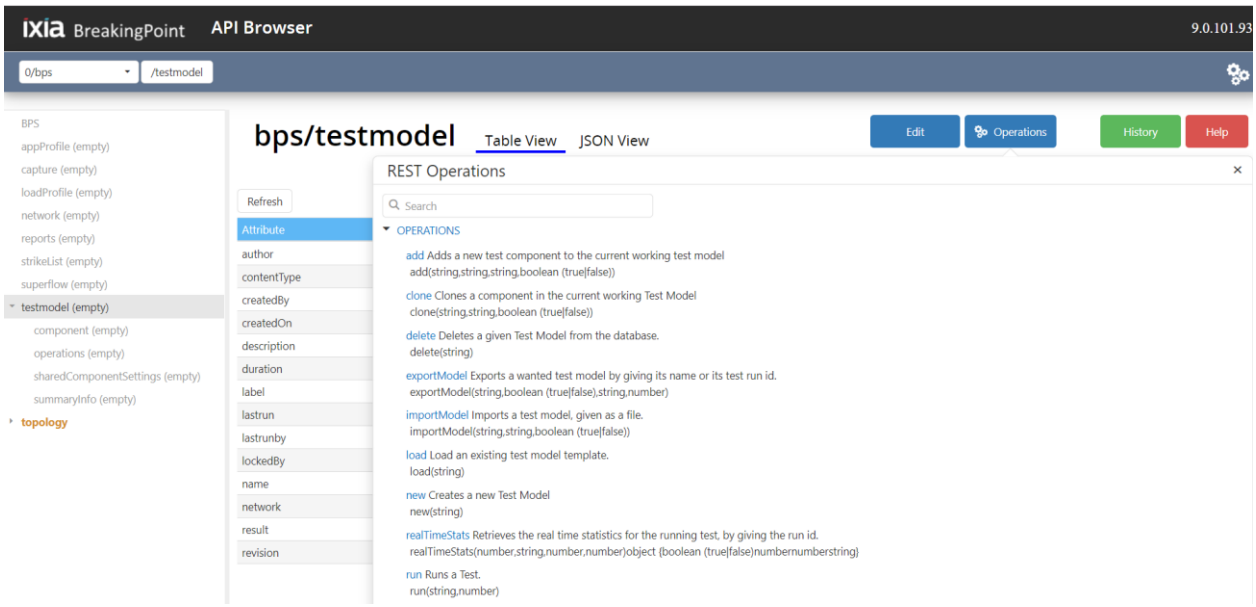


A segment of BreakingPoint report showcasing flow mix

Automation using rest

State of the art REST framework that has been engineered ground-up to deliver a scalable and easy to use REST solution with features like:

- REST API Browser
- JSON Structured Responses
- Autogenerated Python Wrappers and Documentation



API Browser with documentation

BreakingPoint Hardware Platforms

Ixia's **CloudStorm™** platform is the world's first multi-terabit applications and security test solution, modularly scaling to more than two terabits of application traffic in a single, integrated system. It consists of a 2-port SFP28 100GE load module with an innovative architecture that allows concurrent emulation of complex applications and a large volume of stateless DDoS traffic at 200Gbps line-rate per module— without any mode switch. Its seamless proxy support enables web proxy and SSL inspection scenarios using simple 2-arm configurations. The full crypto offload delivers stellar IPsec and SSL performance.

Ixia's **PerfectStorm™** platform modularly scales to nearly a terabit of application traffic in a single, integrated system. It generates stateful applications and malicious traffic that simulate millions of real-world end-user environments to test and validate infrastructure, a single device, or an entire system. With PerfectStorm Fusion load modules, Ixia delivers the first platform to seamlessly unify the IxLoad® and BreakingPoint software applications into a single, more powerful system to ensure the secure delivery of mission-critical applications.

Ixia's **PerfectStorm ONE™** network test and assessment solutions are developed specifically to make BreakingPoint solutions available in a compact form-factor for enterprise IT, operations, and security personnel. PerfectStorm ONE condenses Ixia's PerfectStorm massive-scale, stateful Layer 4-7 testing platform into a versatile appliance. Scaling from 4Gbps to 80Gbps of application traffic simulation, PerfectStorm ONE supports a buy-only-what-you-need business model to align with enterprise budgets and future-proof your growing test needs.

Visit www.keysight.com for more details on BreakingPoint hardware platforms.

BreakingPoint Virtual Platforms

The Virtual Edition (VE) platform is a virtualized form factor of our BreakingPoint hardware that can be deployed in a range of private and public cloud computing environments based on technologies from VMware, KVM, OpenStack, Amazon Web Services, Microsoft Azure, Oracle Cloud, and Alibaba Cloud.

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, use BreakingPoint VE to maximize security investments and optimize network architectures. Now virtualization-enabled, 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. 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 leverages performance acceleration technologies such as DPDK, SR-IOV, and PCI-PT to maximize performance and reduce application simulation cost.

BreakingPoint Performance by Platform

			
Metric	**PerfectStorm ONE Fusion 8x10G/2x40G**	**PerfectStorm Fusion 8x10G/2x40G**	**CloudStorm Fusion 2x100G**
App Throughput	80Gbps	80Gbps	200Gps
TCP Connections per Second	1.45 Million	1.45 Million	3.5 Million
App Concurrent Flows	60 Million	60 Million	120 Million
SSL Bandwidth	20Gbps	20Gbps	92Gbps
SSL Handshake Rates (2K Key and AES256)	200,000	200,000	400,000
SSL Handshake Rates (ECDHE ciphers 256-P curve)	22,000	22,000	52,000
SSL Concurrent Flows	700K	700K	1.5 Million
App Throughput over SCTP	5Gbps	5Gbps	10Gbps
App Throughput over IPsec	25Gbps	25Gbps	60Gbps
IPsec Concurrent Tunnels	500,000	500,000	1 Million
IPsec Tunnel Setup Rates	2,000	2,000	4,000
App Throughput over GTP	80Gbps	80Gbps	170Gbps
GTP UE Attachment Rate	2M per second	2M per second	5 M per second
GTP Tunnels	18 Million	18 Million	27 Million

Specifications

Specification	Protocols
Applications	450+ 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
TLS	TLS 1.0, 1.1, 1.2, and 1.3 All relevant and popular ciphers supported
Wireless Interfaces	• S1-U (eNodeB and SGW sides) • S1-MME (eNodeB side) • SGi (PDN side) • S5/8 (SGW and PGW sides) • S11 (MME and SGW sides) • Gn (SSGN and GGSN sides) • Wireless Protocols Supported: ◦ S1AP ◦ GTP-C v1, GTP-C v2, GTP-U v1 ◦ SCTP (over UDP or IP)
Wireless Operational Modes	• User Equipment • 3G GGSN • 3G SGSN • 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 DHCP Hosts • IPv4/IPv6 DHCP Server • IPv6 SLAAC + Stateless DHCPv6 • DHCP-PD • VLAN • IPv4/IPv6 Router • 6rd CE Routers • DS-Lite B4 and AFTR

Specification	Protocols
	• IPv4/IPv6 DNS • IPsec IKEv1/IKEv2 • NAT Support
Test Methodologies/Labs	• RFC 2544 Lab • DDoS Lab • Multicast Lab • Lawful Intercept Lab • Session Sender Lab • LTE Lab • Device Validation Lab • MultiBox testing • Resiliency Score (*Not supported on PerfectStorm 100GE)* • Data Center Resiliency • LTE Lab • DDoS Lab
Security Exploits and Malware	• 46,000+ total attacks • 8,000+ exploits • 39,000+ 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

Specification	Protocols
	◦ Recursive GET Floods ◦ Slow POSTs • Botnets: ◦ Zeus ◦ SpyEye ◦ BlackEnergy ◦ Duqu ◦ Pushdo Cutwail

Platform Options

Visit www.keysight.com for More Information on BreakingPoint Platform Options	
Virtual Platform	• BreakingPoint Virtual Edition (VE) – VMWare, KVM, OpenStack, AWS, and Azure
Chassis	• XGS-12 HS Chassis • XGS-12 HSL Chassis • XGS-2 HS Chassis • XGS-2 HSL Chassis
Appliances/Load Modules	• CloudStorm Fusion 100GE • PerfectStorm Fusion 10/1GE • PerfectStorm Fusion 40/10GE • PerfectStorm Fusion 100GE • PerfectStorm ONE Fusion 10/1GE • PerfectStorm ONE Fusion 40/10GE

Product Ordering Information

BreakingPoint Software	
BreakingPoint Application and Threat Intelligence (ATI)	
909-0856	BreakingPoint – Application & Threat Intelligence Program
BreakingPoint VE	
939-9600	BreakingPoint Virtual Edition (VE) 1G Floating Subscription Counted License
939-9619	BreakingPoint, Virtual Edition (VE) 10G Floating Subscription Counted License

BreakingPoint on CloudStorm	
Chassis	
940-0016	XGS12-HSL 12-slot chassis bundle with High Performance Controller
940-0014	XGS2-HSL 2-slot chassis with High Performance Controller
Fusion Load Modules (Includes BreakingPoint Application)	
944-1231	CloudStorm 100GE Fusion 2 QSFP28 ports (CS100GE2Q28NG)
Transceivers and Cables	
QSFP28-LR4-XCVR	QSFP28 100GBASE-LR4 100GE pluggable optical transceiver, SMF (single mode fiber), 1310nm, 10km reach
QSFP28-SR4-XCVR	QSFP28 100GBASE-SR4 100GE pluggable optical transceiver, MMF (multimode), 850nm, 100m reach
942-0087	QSFP28 Active Optical Cable (AOC), multimode fiber, 850nm, 3-meter length
942-0088	QSFP28 passive, copper, Direct Attach Cable (DAC), 3-meter length
942-0092	QSFP28 Active Optical Cable (AOC), multimode fiber, 850nm, 3-meter length

BreakingPoint on PerfectStorm	
Chassis	
940-0006	XGS12-HS 12-slot chassis bundle with High Performance Controller
940-0016	XGS12-HSL 12-slot chassis bundle with High Performance Controller
940-0012	XGS2-HS 2-slot chassis with High Performance Controller
940-0014	XGS2-HSL 2-slot chassis with High Performance Controller
Fusion Load Modules (Includes BreakingPoint Application)	
944-1203	PerfectStorm 1GE Fusion 8-port (PS1GE8NG)
944-1200	PerfectStorm 1/10GE Fusion 8-port (PS10GE8NG)
944-1209	PerfectStorm 1/10GE Fusion 4-port (PS10GE4NG)
944-1210	PerfectStorm 1/10GE Fusion 2-port (PS10GE2NG)

BreakingPoint on PerfectStorm	
944-1201	PerfectStorm 40GE Fusion 2-port (PS40GE2NG)
944-1202	PerfectStorm 100GE Fusion 1-port (PS100GE1NG)
Transceivers and Cables	
988-0011	SFP+, 10Gb/1Gb SR optical Xcvr, 850nm (cable included)
988-0012	SFP+, 10Gb/1Gb LR optical Xcvr, 1310nm (cable included)
948-0016	SFP+10GSFP+Cu, Accessory, Passive Direct Attach Cable Assembly, Copper Wire, 3-meter length (cable not included)
988-0004	1GbE, Copper Xcvr (cable included)
948-0031	QSFP+ 40GBASE-SR4 optical transceivers (cable not included)
942-0041	MT 12-Fiber Multimode cable for 40GBASE-SR4 optical transceivers with MT Flat F-F connectors, 850nm, 3-meter length
942-0067	MT-to-4x10GE LC fan-out, MMF, 3-meter – required for 40 Gig to 4x10Gig fan-out
942-0068	MT-to-4x10GE LC fan-out, MMF, 5-meter – required for 40 Gig to 4x10Gig fan-out
948-0030	CXP,100GE, MMF, 850NM, PLUGGABLE TRANSCEIVER (cable not included)
942-0041	MT 12-Fiber MM cable for 40GBASE-SR4 optics, F-F, 850nm, 3-meter length
942-0052	CXP-to-CXP 100GE Active Optical Cable, point-to-point (AOC), 3-meter length

BreakingPoint on PerfectStorm ONE Appliances (Includes BreakingPoint Application)	
941-0028	PerfectStorm ONE Fusion, 40 Gig 2-PORT QSFP+ appliance (PS40GE2NG)
941-0027	PerfectStorm ONE Fusion, 1Gig/10 Gig 8-PORT SFP+ appliance (PS10GE8NG)
941-0031	PerfectStorm ONE Fusion, 1Gig/10 Gig 4-PORT SFP+ appliance (PS10GE4NG)
941-0032	PerfectStorm ONE Fusion, 1Gig/10 Gig 2-PORT SFP+ appliance (PS10GE2NG)
941-0033	PerfectStorm ONE Fusion, 1 Gig 8-PORT SFP+ appliance (PS1GE8NG)
941-0034	PerfectStorm ONE Fusion, 1 Gig 4-PORT SFP+ appliance (PS1GE4NG)

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