DATA SHEET

BreakingPoint on Microsoft Azure — Cloud Application and Security Testing

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

Moving IT infrastructure to public clouds creates a model of shared responsibility between the customer and the cloud provider. This shared model eliminates the operational burden on the organization using cloud services, however they are still responsible for the security, availability, performance, and management of all the controls and processes associated with operating over the cloud infrastructure. The move to the cloud needs to deliver the same or better performance and similar security efficacy than the on-premises infrastructure. Without a way to properly validate these cloud application workload and security controls, customer quality of experience (QoE) is at risk.

Solution: A Flexible Security Testing Ecosystem for Cloud Infrastructure

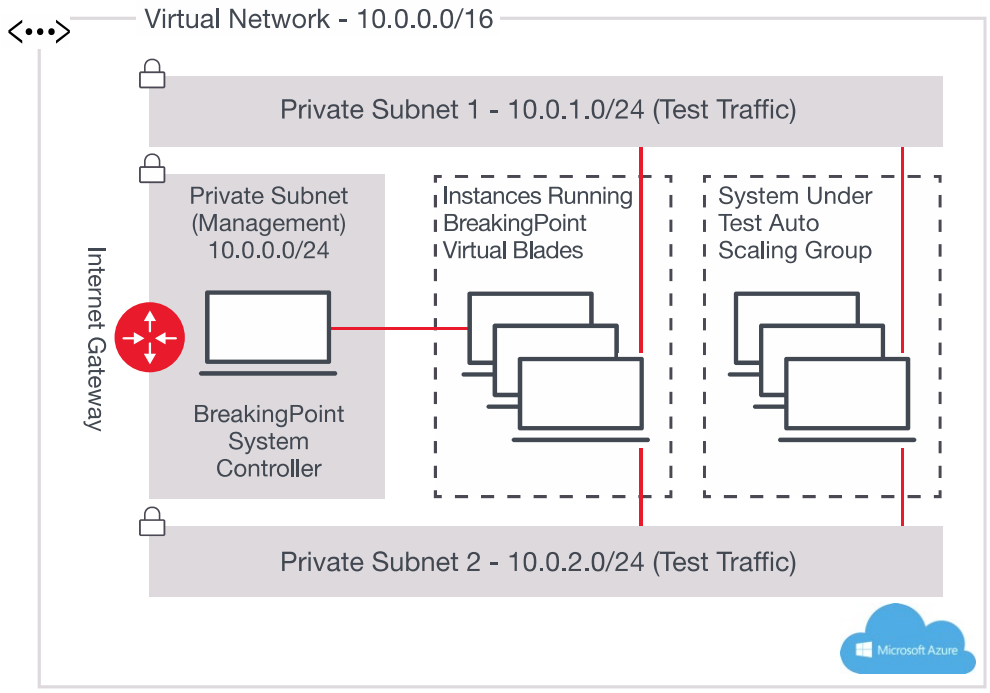
Keysight's BreakingPoint on Azure provides scalable real-world application and threat simulation in the public cloud. Build resilient cloud infrastructure you can rely on by using BreakingPoint to maximize security investments and optimize cloud architectures. Now cloud-enabled, the market-proven BreakingPoint application offers cost-effective, elastic, and sharable virtualized test capabilities that you can quickly deploy and scale across Microsoft public clouds.

Highlights

- Validate functionality of application-aware, cloud-enabled devices and networks
- Optimize cloud network security devices such as NGFW, IDS/IPS and DLP
- Measure and compare cloud infrastructures for your specific workloads and security controls
- Validate the elastic scalability of your cloud infrastructure and security architecture
- Understand the impact of multi-tenancy
- Get the best value when evaluating cloud security solutions by performing head-to-head "bake-offs"
- Keep current with new application and threat intelligence updates every two weeks
- Flexibly deploy Keysight virtual test tools that you can easily move, change, or scale up and down
- Leverage subscription-based BYOL for low startup cost and flexibility of a pay-as-you-grow OPEX model

KEYSIGHT TECHNOLOGIES

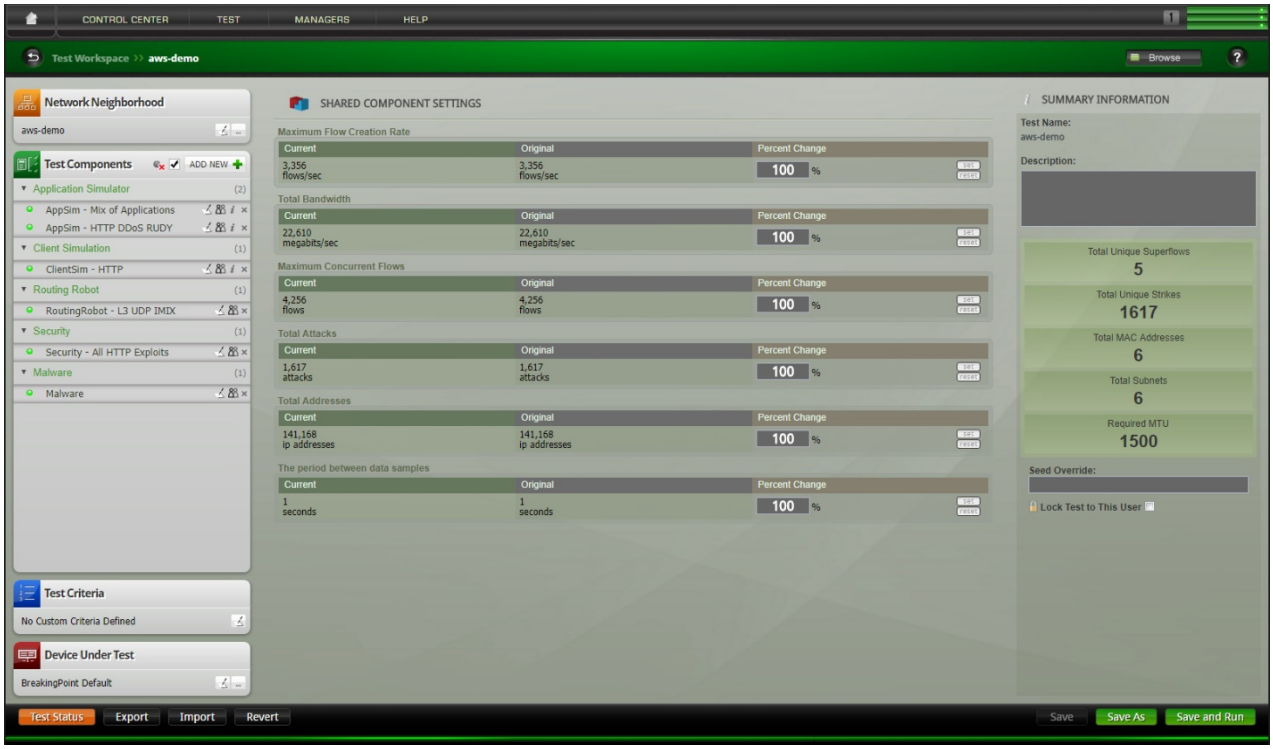
Realize the savings of cloud without compromising security by excising the unknows that come with the elastic scalability, multi-tenancy, and high-availability characteristic of a cloud infrastructure.



BreakingPoint deployment for testing elastic security

Key Features

- Simulates more than 300 real-world application protocols to emulate cloud application workloads
- Allows customization and manipulation of any protocol, including raw data, to validate data loss prevention (DLP), microsegmentation, and other application-based policing
- Emulates more than 37,000 attacks and malwares
- Delivers from a single test port all types of traffic simultaneously, including legitimate traffic and malware
- Bi-monthly Application and Threat Intelligence (ATI) subscription updates ensure you are current with the latest applications and threats
- Subscription-based bring your own licensing (BYOL) model comes with an all-inclusive license that reduces startup cost
- Seamless transition between hardware, virtual, and public cloud platforms enables easy translation of functional and performance testing in physical, virtual, and cloud environments
- Simple and fast deployment and orchestration using CloudFormation Templates
- Automate tests using REST API
- Support for SR-IOV to deliver highly-scalable application traffic generation
- Visit www.keysight.com for more details on the BreakingPoint product



BreakingPoint GUI configured with an enterprise cloud workload

Specifications

<table>
<tr><th>Feature</th><th>System Controller</th><th>Virtual Blade</th></tr>
<tr><td>Maximum # of Virtual Ports</td><td>96</td><td>8 (depends on VM size)</td></tr>
<tr><td>Maximum # of Virtual Load Modules</td><td>12</td><td>N/A</td></tr>
<tr><td>Maximum # of Users</td><td>20</td><td>8</td></tr>
<tr><td>Recommended Azure VM Size</td><td>Minimum:
Standard_F4s

Recommended:
Standard_F4s_v2

Minimum Disk Size:
20 GB+

Recommended Disk Size:
100GB+</td><td>
<table>
<tr><th>Instance Type</th><th>HTTP</th><th>HTTP AES128-SHA2</th></tr>
<tr><td>Standard_F4s</td><td>2.54 Gbps</td><td>0.6 Gbps</td></tr>
<tr><td>Standard_F8s</td><td>5.61 Gbps</td><td>1.18 Gbps</td></tr>
<tr><td>Standard_F16s</td><td>6.35 Gbps</td><td>2.49 Gbps</td></tr>
</table>
</td></tr>
<tr><td>Guest OS</td><td>Based on CentOS 7.0</td><td>Based on CentOS 7.0</td></tr>
</table>

Feature	System Controller	Virtual Blade
Distribution/ Packaging (Linux version)	Microsoft Virtual Hard Disk (VHD) available via Azure storage copy using bash script. Deployment examples available on “OpenIxia” “azure-bps” GitHub repository.	Microsoft Virtual Hard Disk (VHD) available via Azure storage copy using bash script. Deployment examples available on “OpenIxia” “azure-bps” GitHub repository.

Supported Azure Locations

Azure Region Name	Azure Region API Name
(US) East US	eastus
(US) East US 2	eastus2
(US) South Central US	southcentralus
(US) West US 2	westus2
(US) Central US	centralus
(US) North Central US	northcentralus
(US) West Central US	westcentralus
(US) West US	westus
(Africa) South Africa North	southafricanorth
(Africa) South Africa West	southafricawest
(Asia Pacific) Australia East	australiaeast
(Asia Pacific) Australia Southeast	australiasoutheast
(Asia Pacific) Australia Central	australiacentral
(Asia Pacific) Australia Central 2	australiacentral2
(Asia Pacific) Southeast Asia	southeastasia
(Asia Pacific) Central India	centralindia
(Asia Pacific) South India	southindia

Azure Region Name	Azure Region API Name
(Asia Pacific) West India	westindia
(Asia Pacific) East Asia	eastasia
(Asia Pacific) Japan East	japaneast
(Asia Pacific) Japan West	japanwest
(Asia Pacific) Korea Central	koreacentral
(Asia Pacific) Korea South	koreasouth
(Canada) Canada Central	canadacentral
(Canada) Canada East	canadaeast
(Europe) North Europe	northeurope
(Europe) UK South	uksouth
(Europe) UK West	ukwest
(Europe) West Europe	westeurope
(Europe) France Central	francecentral
(Europe) France South	francesouth
(Middle East) UAE Central	uaecentral
(Middle East) UAE North	uaenorth
(South America) Brazil South	brazilsouth

Protocols and features

BreakingPoint is powered by Keysight's ATI subscription service that delivers a wide variety of applications and attacks to emulate traffic mix and security threats of any-sized enterprise, service provider, or government organization at scale. The application and attack emulations are complemented with BreakingPoint's comprehensive network stack that simulates network components like IPv4, IPv6, DNS, and DHCP, helping to orchestrate the required network environments.

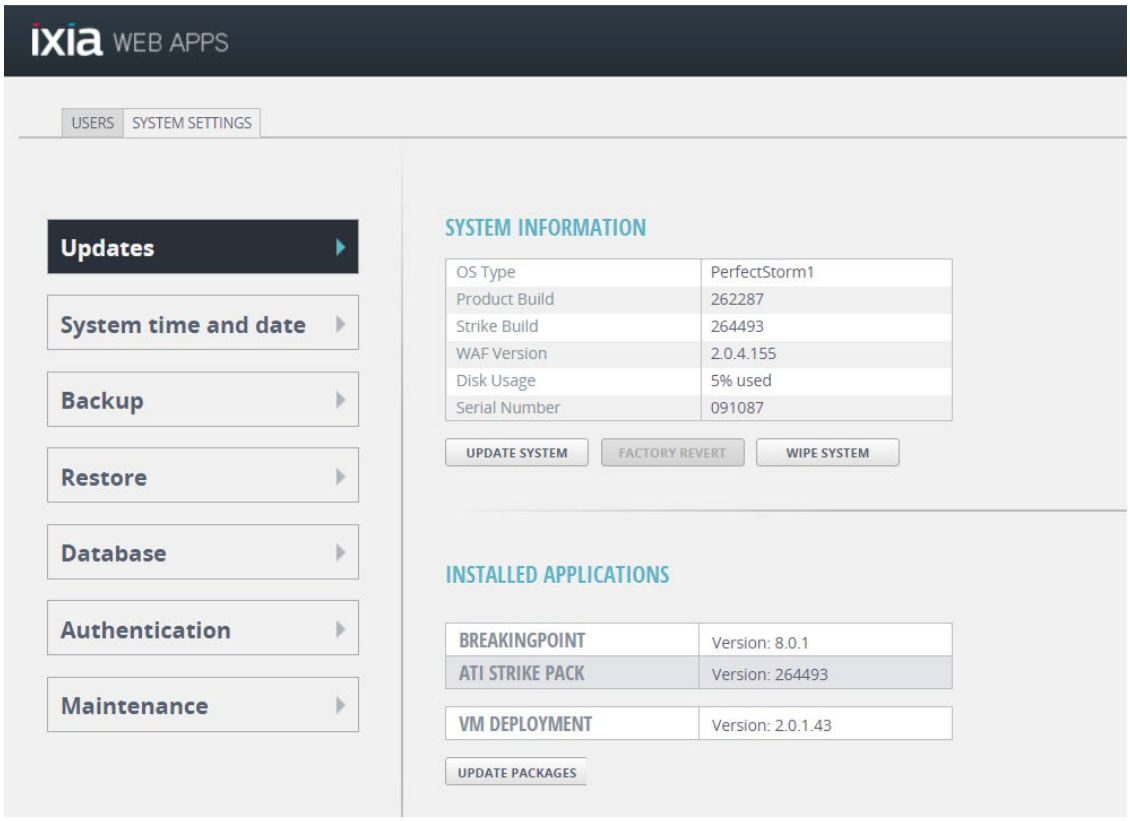
Specification	Description
Applications	300+ application protocols, including Yahoo! Mail and Messenger, Google Gmail, Skype, BitTorrent, eDonkey, RADIUS, SIP, RTSP, RTP, HTTP, SSL, Facebook, Twitter Mobile, YouTube, and Apple FaceTime, as well as other mobile, social, and gaming protocols – with multicast support
Network Access	• IPv4/IPv6 Static Hosts • IPv4/IPv6 External Hosts • IPv4/IPv6 Router • IPv4/IPv6 DNS • DHCPv4 clients
Security Exploits/ Malware	• 36,000+ total attacks • 6,000+ exploits • 30,000+ malware • 100+ evasion classes
	*Go to keysight.com to get more details about ATI attacks
Licensing	• All-inclusive BYOL 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 single security and security NP component (p/n: 939-9600) ◦ 10G-Tier - 10Gbps of throughput, 20M concurrent super flows and two security and security NP component (p/n: 939-9610)

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, 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

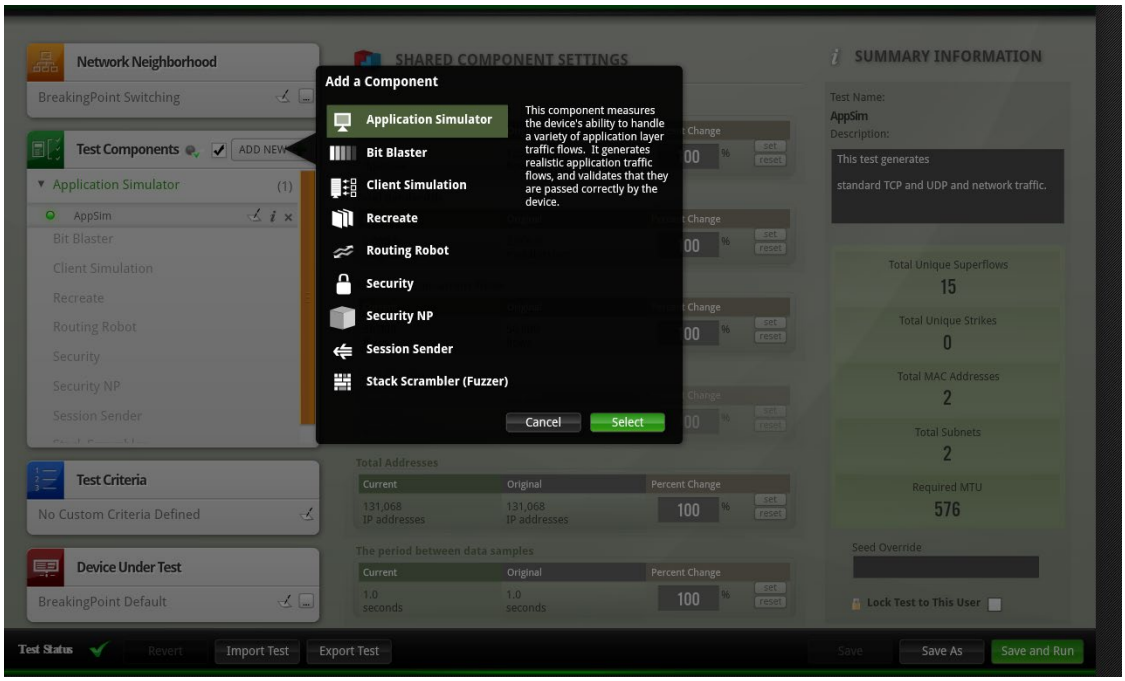


ATI packages can be updated through the intuitive BreakingPoint GUI

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
Client Simulation	Allows users to generate client traffic via Superflows against real servers (device under test) in 1-Arm mode (BreakingPoint being the client)
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 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
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



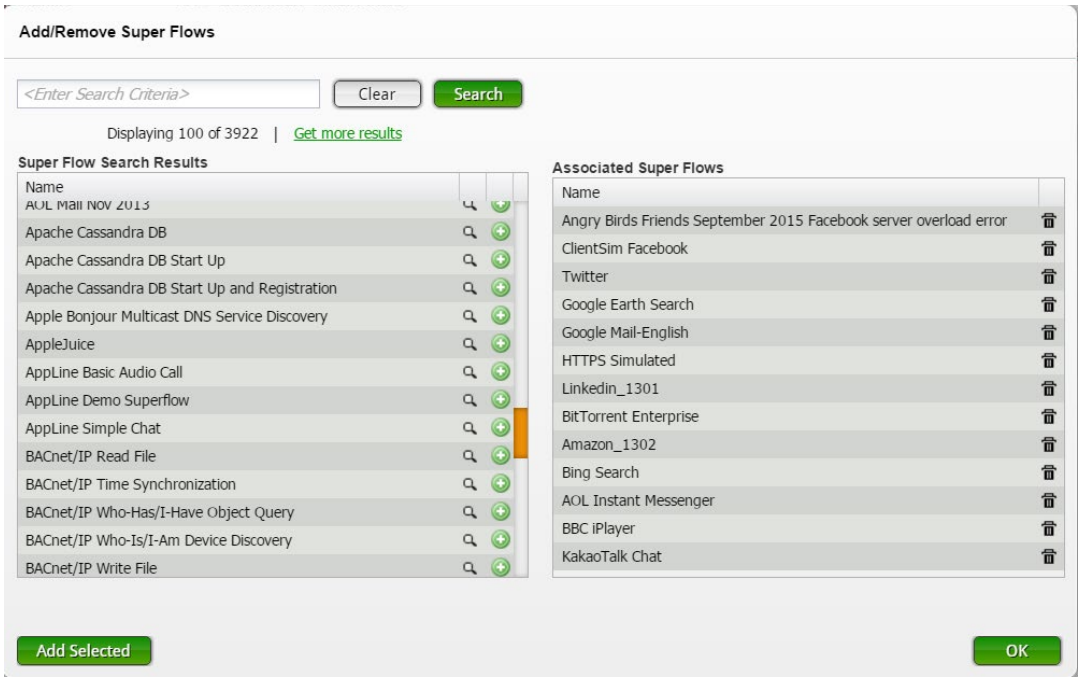
BreakingPoint purpose-built test components

Application simulation

BreakingPoint simulates over 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.



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

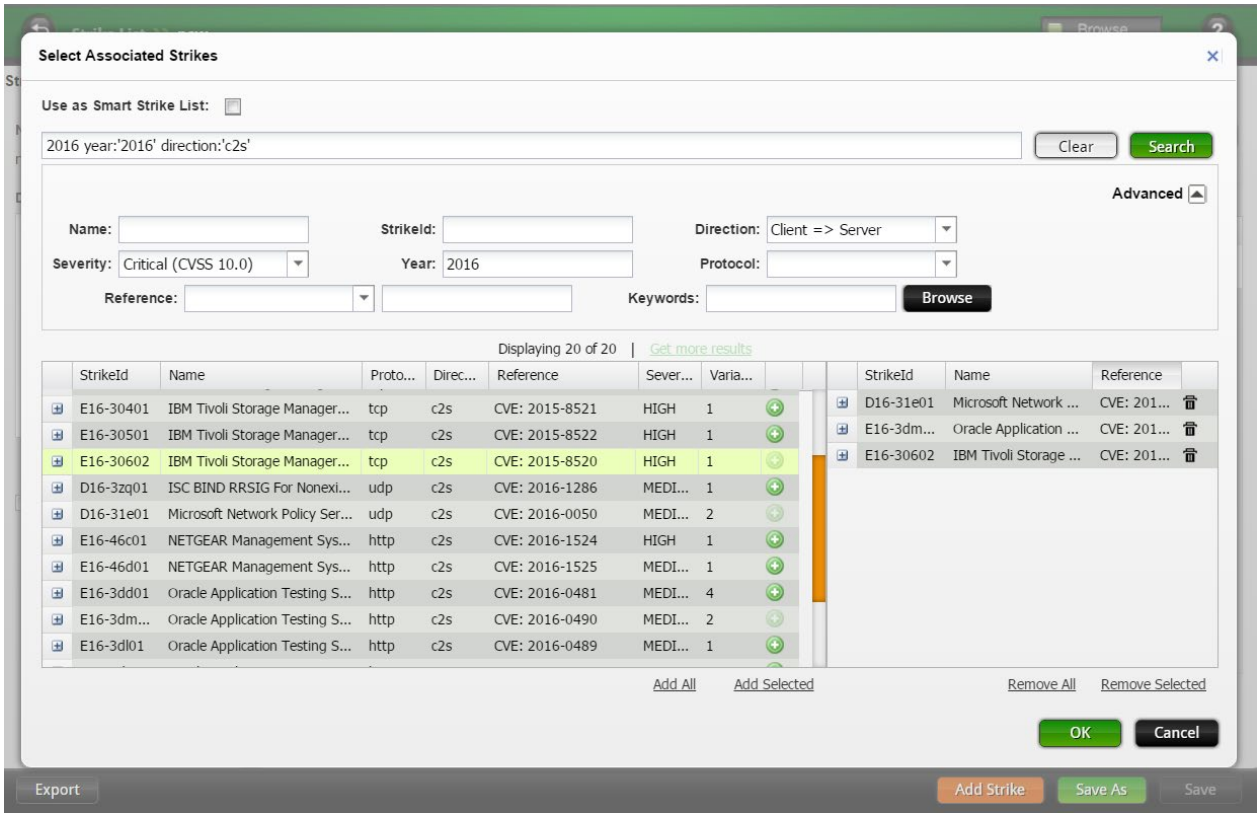
<! DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta content="text/html; charset=UTF-8" http-equiv="Content-Type"/><title>broach the subject of his</title><style type="text/css">p { 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> 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>

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

Comprehensive security

BreakingPoint delivers the industry's most comprehensive solution test network security devices—such as IPSs, IDSs, and firewalls. 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.

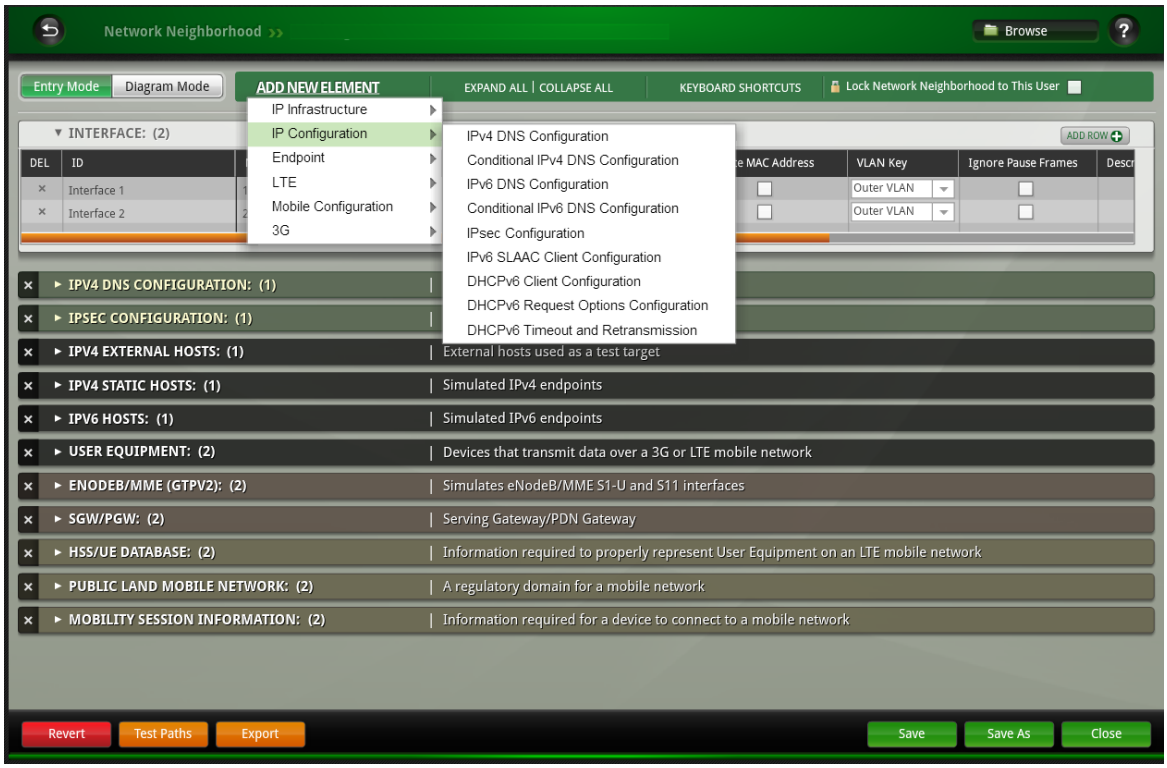
- Supports over 37,000 strikes and malware and the attacks can be obfuscated by over 100 evasion techniques
- Emulate botnets, from zombie to command and control (C&C) communication
- Generates legitimate and malicious traffic from the same port—purpose-built hardware design allows sending all types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



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

Network Neighborhood

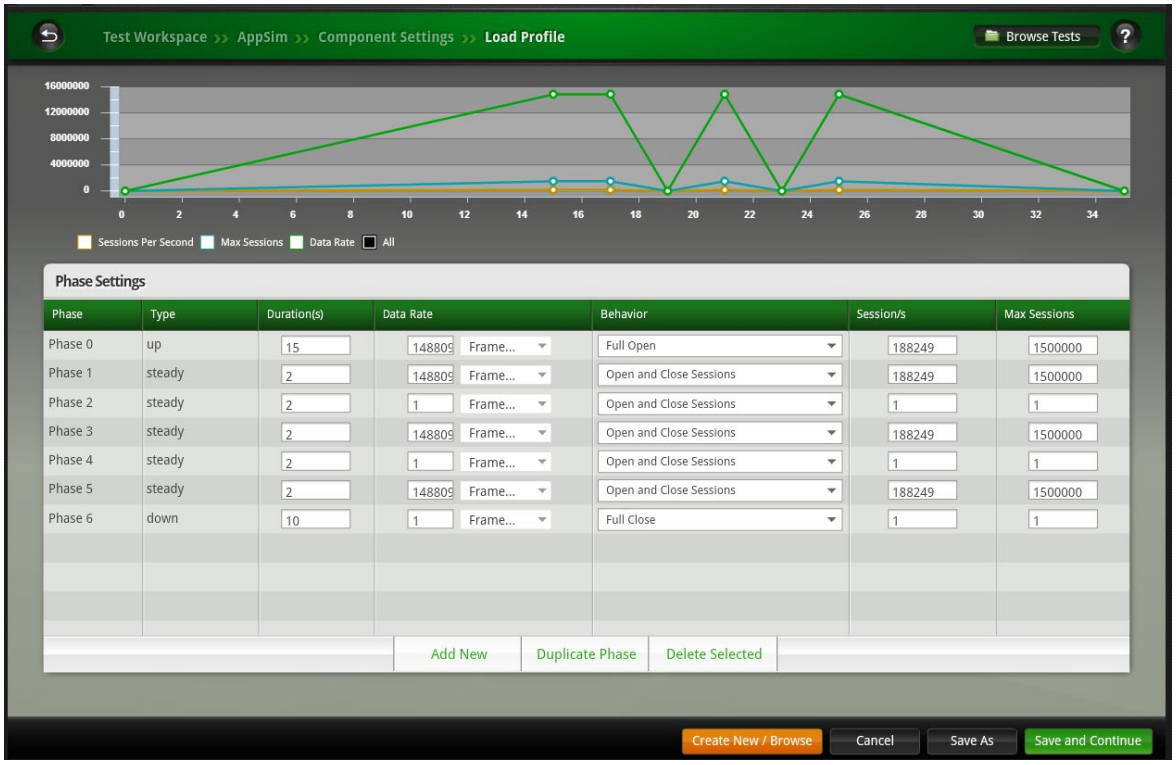
BreakingPoint's Network Neighborhood provides flexibility for the user to create simple to highly complex network environments.



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.

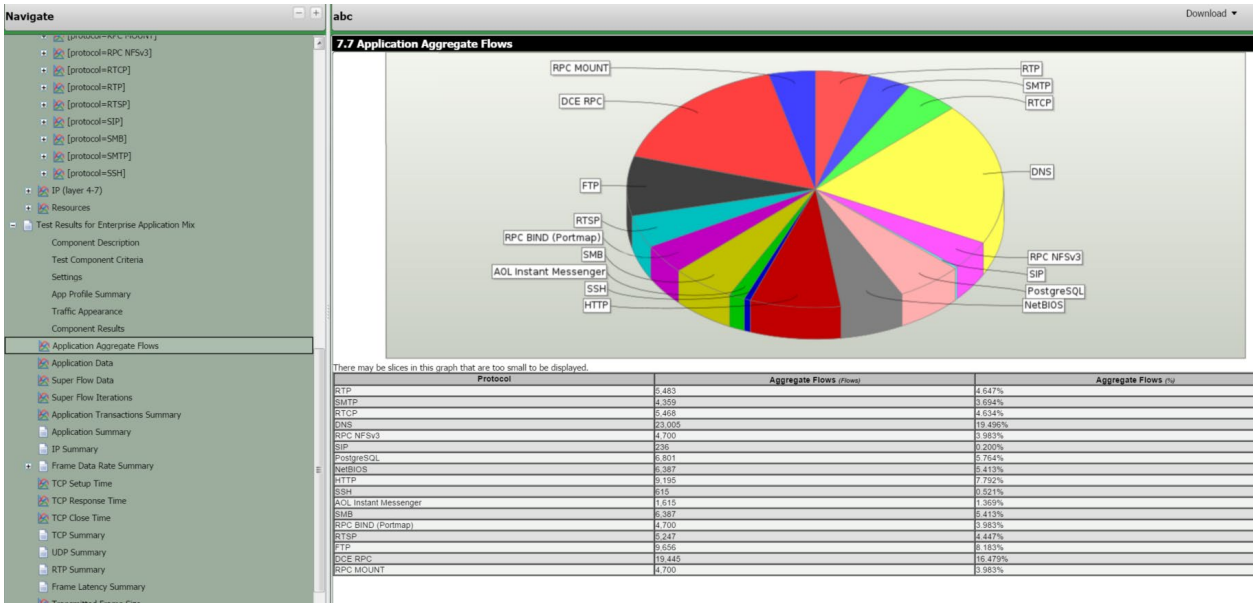


A BreakingPoint MicroBurst Load Profile

Built-in 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

Technology Solutions

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

- BreakingPoint – Application and Security Testing
- BreakingPoint Virtual Edition (VE) – Virtualized Application and Security Testing
- BreakingPoint on AWS – Amazon Web Services (AWS) edition of BreakingPoint for Cloud Performance and Security 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 Counted 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).

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

This information is subject to change without notice. © Keysight Technologies, 2019-2020, Published in USA, October 22, 2020, 3120-1268.EN