DATA SHEET

BreakingPoint Cloud—Microsoft Azure DDOS Protection Validation

Know Your Cloud Security

Problem: Ensuring Cloud DDOS Protection Is Working

The frequency and scale of distributed denial-of-service (DDoS) attacks are increasing and they are becoming easier to carry out. It is no surprise that DDoS is a leading cause of business service outage and a top concern for companies today.

While cloud providers enable a variety of options to build cost-effective, elastic, and highly available applications, enterprises have a shared responsibility to ensure their DDoS protection controls are properly configured. To protect both their bottom line and user experience, companies need a way to validate their cloud-based DDoS protection.

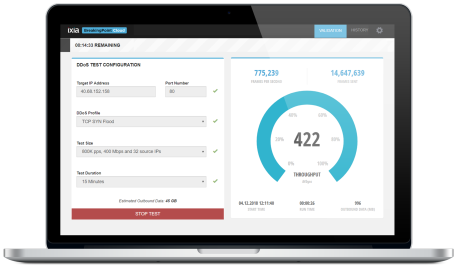
Solution: Proactive, Continuous Cloud DDOS Protection Validation

As cloud is the new normal, continuous testing of DDoS protection services on cloud infrastructures needs to be the new normal too.

Keysight BreakingPoint Cloud—Microsoft Azure DDoS Protection Validation provides continuous insights into the security posture of cloud environments by safely modeling DDoS traffic so you can assess the effectiveness of your DDoS protection services.

Highlights

- Validate DDoS defenses of your production workloads hosted on Microsoft Azure
- Microsoft Azure approved
- Safely and cost-effectively simulate botnets to prepare security teams for a DDoS attack before it happens
- Trade assumptions for real data so you know that security controls are deployed correctly
- Ensure optimal configuration of DDoS protection services
- Continuously prove your DDoS mitigation compliance with data-driven evidence
- Reduce data security compliance audit time
- Prove DDoS attacks are accurately identified and reported
- Perform regularly scheduled validations using an always up-to-date library of DDoS attacks



00:14:33 REMAINING

DDoS TEST CONFIGURATION

Target IP Address: 40.68.152.158
Port Number: 80
DDoS Profile: TCP SYN Flood
Test Size: 800K pps, 400 Mbps and 32 source IPs
Test Duration: 15 Minutes

Estimated Outbound Data: **45 GB**

775,239 FRAMES PER SECOND
14,647,639 FRAMES SENT
422 THROUGHPUT Mbps
04.12.2018 12:11:40 START TIME
00:00:26 RUN TIME
996 OUTBOUND DATA (MB)

BreakingPoint Cloud builds on more than 20 years of leadership in network security testing to reveal your security exposure across public, private, and hybrid networks.

KEYSIGHT TECHNOLOGIES

Key Features

- Validation-as-a-service through a software-as-a-service (SaaS)—consume it with your browser, no software to install, always up to date
- Built-in safety features validate the target IP address is owned by the Azure account that executes the DDoS validation
- Offers a simplified user interface and an ‘out-of-the-box’ experience
- Pre-defined DDoS test sizing and test duration profiles enables safer validations by eliminating the potential of configuration errors
- Pay-per-use model, enables the flexibility to grow validations with your business and network growth
- Elastically scales DDoS simulation agents
- Large-scale DDoS validation available with assistance from Microsoft Azure and Keysight
- Register now to get a free trial https://breakingpoint.cloud/trial

Key Use-Cases

DDoS attacks are a big risk to any business with an online presence. Even a basic test of a DDoS attack can help you discover critical data, including how many packets your DDoS mitigation solution drops, how your mitigation solution functions in a real attack, how your mitigation solution reports DDoS events, what level of service you are able to provide while under attack, and how your people and process react to and withstand an attack. Here are several use cases for BreakingPoint Cloud:

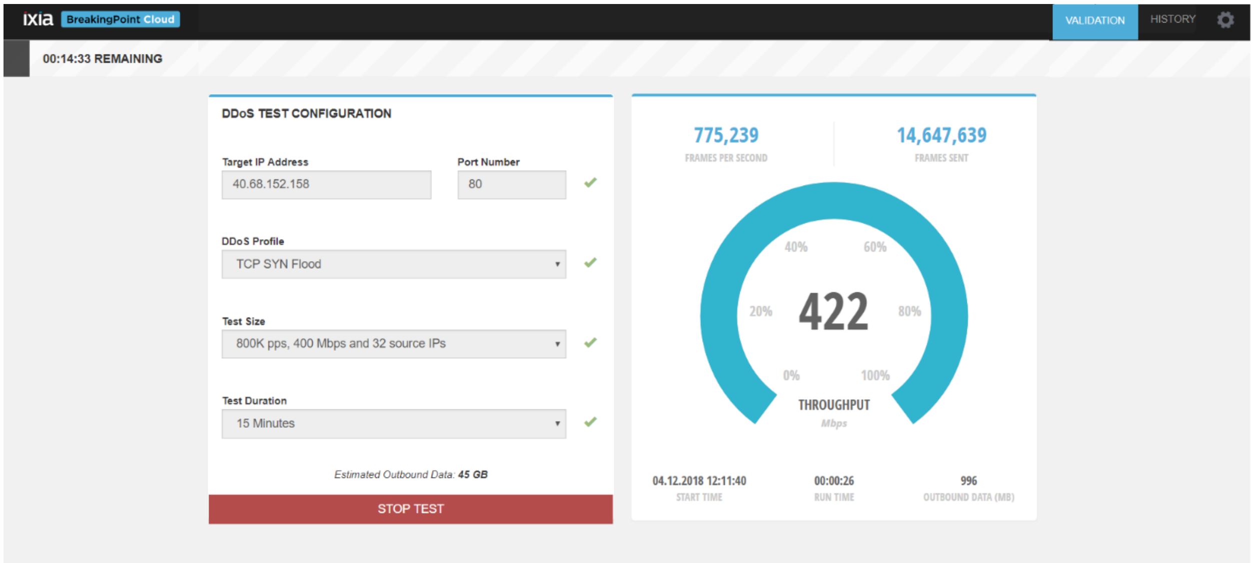
- Validate Microsoft Azure DDoS protection service defenses for your Azure resources
- Produce evidence to document DDoS protection compliance
- Optimize your incident response process while under DDoS attack
- Assure protection service continuity with ongoing DDoS simulation testing
- Train your network security teams

Product Capabilities

Keysight’s BreakingPoint Cloud provides a safe and cost-effective way to validate DDoS cloud protection service activation, produce evidence to document DDoS compliance, optimize operational responses, and confirm service level agreements (SLAs) and controls.

Delivered as a SaaS solution, BreakingPoint Cloud eliminates common anxieties with deployment, especially where network architectures are more complex. It offers a modern, simplified web user interface with an ‘out-of-the-box’ experience. Pre-defined templates for configuring DDoS test sizing and test duration enables additional safety features by eliminating the potential of configuration errors and keeping the DDoS simulation within safety thresholds for production cloud deployments.

To eliminate misconfigurations of the target IP address, Keysight’s BreakingPoint Cloud provides a real-time IP validation, confirming you can simulate DDoS tests only against resources on your Microsoft Azure cloud infrastructure.



00:14:33 REMAINING

DDoS TEST CONFIGURATION

Target IP Address: 40.68.152.158 ✓
Port Number: 80 ✓
DDoS Profile: TCP SYN Flood ✓
Test Size: 800K pps, 400 Mbps and 32 source IPs ✓
Test Duration: 15 Minutes ✓

Estimated Outbound Data: ***45 GB***

775,239 FRAMES PER SECOND
14,647,639 FRAMES SENT
422 THROUGHPUT Mbps
04.12.2018 12:11:40 START TIME
00:00:26 RUN TIME
996 OUTBOUND DATA (MB)

BreakingPoint Cloud—DDoS Validation Dashboard

Hardening your network architecture and preparing for a DDoS attack mitigates damage and allows your organization to become more resilient, even under attack. But you also need to know that DDoS preparations and investments will work as planned, stop bad traffic, and allow good traffic to pass. Testing attack scenarios prior to deployment ensures that you are protected.

With BreakingPoint Cloud—Microsoft Azure DDoS protection validation, you'll gain the actionable intelligence needed to quickly and easily understand how your cloud DDoS protection works and to prove compliance of DDoS protection assurance.

Specifications

General Features	• SaaS DDoS validation platform using safe botnet modeling • Validates DDoS protection service across all Microsoft Azure regions (see Microsoft Azure website for list of regions) • DDoS test traffic originates from public IPv4 addresses • Modern, easy to use, web-based user interface • Automation control with Python API • Built-in safety features to validate that the DDoS target IP address is owned by the Azure account that executes the DDoS validation
DDoS Patterns	• TCP SYN Flood • DNS Flood • UDP Flood (64 bytes) • UDP Flood (128 bytes)

	• UDP Flood (256 bytes) • UDP Flood (512 bytes) • UDP Flood (1024 bytes) • UDP Flood (1500 bytes) • NTPv2 Flood • SSDP Flood • Memcached Flood
DDoS Test Size Profiles	4 profiles to define scale based on selected DDoS pattern ranging from 50 Mbps to 2.4 Gbps **Note**: Larger tests can be coordinated by contacting Keysight's Professional Services team
Test Duration Profiles	• 10 minutes • 15 minutes • 20 minutes • 25 minutes • 30 minutes **Note:** Longer tests can be coordinated by contacting Keysight's Professional Services team

Ordering Information

The following new part numbers are released and available for purchase.

972-5901	Ixia, Self- Service DDoS Testing as a Service (972-5901) IXIA BreakingPoint Cloud Services, Self-Service DDoS Testing as a Service - Cloud Based; INCLUDES initial Onboarding Meeting, response to up to Five (5) Service Tickets and DDoS traffic from the cloud (self-service through the BreakingPoint Cloud portal). Price is per 1000 Gigabytes of outbound DDoS traffic.

More information: https://www.keysight.com/in/en/products/network-security/breakingpoint-cloud.html

Get a free trial: https://breakingpoint.cloud/trial

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