ixia
A Keysight Business

BreakingPoint Cloud

Microsoft Azure DDoS Protection Validation

User Guide

Release 1.1.0

Notices

Copyright Notice

Warranty

The material contained in this document is provided “as is,” and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Keysight disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Keysight shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Keysight and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

U.S. Government Rights

The Software is "commercial computer software," as defined by Federal Acquisition Regulation ("FAR") 2.101. Pursuant to FAR 12.212 and 27.405-3 and Department of Defense FAR Supplement ("DFARS") 227.7202, the U.S. government acquires commercial computer software under the same terms by which the software is customarily provided to the public. Accordingly, Keysight provides the Software to U.S. government customers under its standard commercial license, which is embodied in its End User License Agreement (EULA), a copy of which can be found at http://www.keysight.com/find/sweula or https://support.ixiacom.com/support-services/warranty-license-agreements. The license set forth in the EULA represents the exclusive authority by which the U.S. government may use, modify, distribute, or disclose the Software. The EULA and the license set forth therein, does not require or permit, among other things, that Keysight: (1) Furnish technical information related to commercial computer software or commercial computer software documentation that is not customarily provided to the public; or (2) Relinquish to, or otherwise provide, the government rights in excess of these rights customarily provided to the public to use, modify, reproduce, release, perform, display, or disclose commercial computer software or commercial computer software documentation. No additional government requirements beyond those set forth in the EULA shall apply, except to the extent that those terms, rights, or licenses are explicitly required from all providers of commercial computer software pursuant to the FAR and the DFARS and are set forth specifically in writing elsewhere in the EULA. Keysight shall be under no obligation to update, revise or otherwise modify the Software. With respect to any technical data as defined by FAR 2.101, pursuant to FAR 12.211 and 27.404.2 and DFARS 227.7102, the U.S. government acquires no greater than Limited Rights as defined in FAR 27.401 or DFAR 227.7103-5 (c), as applicable in any technical data. 52.227-14 (June 1987) or DFAR 252.227-7015 (b) (2) (November 1995), as applicable in any technical data.

EULA

The ISG SaaS Terms of Service sets forth the terms of use and service for BreakingPoint Cloud. You can view and download a copy of ISG SaaS Terms of Service by selecting **Terms of Service** from the gear (⚙) menu. The current release of BreakingPoint Cloud does not require an end user license agreement; however, use, download, and access to the BreakingPoint Cloud API is covered by the *Keysight Software End-User License Agreement* (found at www.keysight.com/find/sweula).

Contact Us

Ixia headquarters

26601 West Agoura Road
Calabasas, California 91302
+1 877 367 4942 – Toll-free North America
+1 818 871 1800 – Outside North America
+1.818.871.1805 – Fax
www.ixiacom.com/contact/info

Support

Global Support	+1 818 595 2599	support@ixiacom.com
APAC Support	+91 80 4939 6410	support-asiapac@ixiacom.com
EMEA Support	+40 21 301 5699	support-emea@ixiacom.com
Greater China Region	+400 898 0598	support-china@ixiacom.com
Hong Kong	+86 10 5732 3932	support-china@ixiacom.com
India Office	+91 80 4939 6410	support-india@ixiacom.com
Japan Head Office	+81 3 5326 1980	support-japan@ixiacom.com
Korea Office	+82 2 3461 0095	support-korea@ixiacom.com
Singapore Office	+656 494 8910	support-asiapac@ixiacom.com

CONTENTS

Product overview

BreakingPoint Cloud – Microsoft Azure DDoS Protection Validation is a cloud-based service for validating the DDoS protection controls that safeguard your production environments hosted on Microsoft Azure. By safely modeling DDoS attacks against your Azure-hosted applications and services, you can:

- Validate the effectiveness of your DDoS protection controls
- Use the data from each validation test to optimize your protection control configurations
- Prepare and train your attack response teams
- Produce evidence of DDoS mitigation compliance with your organization's risk governance policies

In this section:

Usage requirements

To use BreakingPoint Cloud, you need the following:

- Ixia identity account
  An Ixia identity account is used for various Ixia services and support, including BreakingPoint Cloud.
- BreakingPoint Cloud subscription (or free trial subscription)
  BreakingPoint Cloud is a subscription-based software as a service (SaaS).
- Access to a Microsoft Azure subscription
  Any IP address designated as the *Target* in a BreakingPoint Cloud test must be owned by an Azure subscription to which you have access. At a minimum, you need *Reader* role for the Resource Groups associated with the Public IP Addresses that you will target using BreakingPoint Cloud. *Reader* role at the Azure subscription level is recommended.

The *Getting Started Guide* provides detailed information about each of these.

Active tests per account

In the current release, BreakingPoint Cloud supports one active test for each user account.

Available user interfaces

BreakingPoint Cloud DDoS provides two user interfaces:

GUI: A web-based interface, as described in this *User Guide*.

API: A Python API, as described in the *API Reference Guide*.

Product information

The following product information is available for BreakingPoint Cloud users:

Documents	Description
Release Notes	To review the Release Notes, open the **About** box from the gear (⚙) menu, then click **Release Notes**.
Third Party License Information	To view the list of third party software licenses, open the **About** box from the gear menu, then click **Third Party Components**.
User Documentation	The the following product documentation is available—in HTML and PDF format—from the gear menu: • *User Guide*: Provides instructions for creating tests, running tests, and analyzing the test results in the web-based user interface. • *Python API Reference Guide*: Provides a complete reference for every public method and property associated with the objects provided by the BreakingPoint Cloud Python API.
Web page	Refer to https://www.ixiacom.com/products/breakingpoint-cloud for cybersecurity-related reports, white papers, and additional product information.

Use cases

When planning your DDoS validation tests, consider both the business goals and the specific environment when deciding whether each test will target a production environment, a test environment, or both. The following use cases can help you with these decisions.

Service Activation

Business Goal:	Generate evidence that the DDoS protection service has been properly enabled (activated)
Environment:	Production: the business goal is achieved only when validating on production environments.
Strategy:	Validate using: • smallest DDoS test sizes • each type of DDoS attack
Approach:	Suited for self-service

Training Security Operations Team

Business Goal:	Train security operations teams and optimize your security processes and procedures to "detect, react, and improve" with realistic attack simulations.
Environment:	Both: The best business value can be achieved when validating in a production environment. However, a staging environment is well suited when it properly mirrors the production environment.
Strategy:	Create multiple test variations: • range of small to large attacks • full range of attack vectors (DDoS Profiles) • Both single attacks and multiple concurrent attacks • concurrent attacks on multiple protected resources
Approach:	Suited for self-service as well as using Ixia professional services

Continuous Service Validation

Business Goal:	Proactively validate that DDoS protection operates as expected on a continuous basis. When DDoS protection is provided as a managed security service, you are losing visibility when provider's upgrades may impact your protection.

Environment:	Production: the business goal is achieved only when validating on production environments.
Strategy:	Validation periodicity: • daily, using small DDoS test sizes, configured with a range of attack types • more frequently, if attack frequency and intensity indicates the need
Approach:	Suited for self-service (automated)

Compliance

Business Goal:	Prove compliance by producing evidence demonstrating DDoS protection has been in place and properly logs DDoS attacks.
Environment:	Production: the business goal is achieved only when validating on production environments.
Strategy:	Validation periodicity and type: • daily, using small DDoS test sizes • use the full range of DDoS attack profiles
Approach:	Suited for self-service (automated)

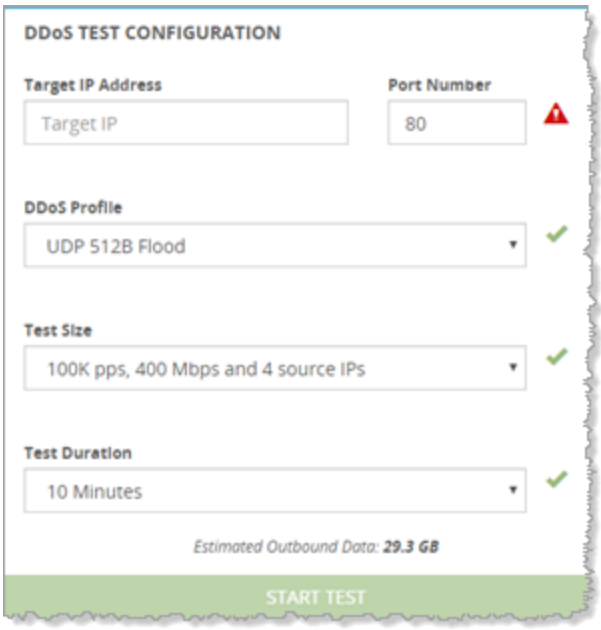
Proof-of-concept validation

Business Goal:	Gain confidence you are selecting the proper DDoS protection by validating with real-life DDoS simulation scenario.
Environment:	Staging environment
Strategy:	Validate using: • Small to larger DDoS tests • Variation of DDoS attack profiles • Concurrent DDoS patterns
Approach:	Involve Ixia professional services

How it works

BreakingPoint Cloud – Microsoft Azure DDoS Protection Validation is designed for Security Operations Center personnel to use in conjunction with your Microsoft Azure DDoS Protection Validation DDoS mitigation services.

Using a simple web interface, you model DDoS attacks to collect data and insights into your current DDoS security posture. The basic test workflow is as follows:



1. You configure and start a test that specifies:
   - the DDoS attack target (IP address and port number)
   - the DDoS profile (specific type of DDoS attack)
   - the test size and duration
2. BreakingPoint Cloud prepares the resources for the test.

   The resources comprise a group of simulated bots and the appropriate DDoS data. For example, if you have chosen an HTTPS Excessive GET attack, the attacking bots will attempt to flood the target web server application with multiple GET requests within each HTTPS session.
3. BreakingPoint Cloud executes the test.
4. Once the test is running, you can examine your Azure DDoS Protection metrics to verify that your mitigation controls are working as expected for the target node.

Refer to Create and run tests on page 13 for detailed instructions.

FAQs

- How safe is DDoS validation?

  Ixia has worked with Microsoft to develop a methodology to make Microsoft DDoS Protection Validation extremely safe.

  Recommended best practices:

  - Conduct the initial tests in a sandbox environment.
  - For production environments, start tests at very low levels, monitor for any impact, and only then increase the level.
- What are the safety limits implemented on a self-serve account?

  DDoS traffic can be initiated only after properly authenticating with your Azure account, and can be transmitted only against IP addresses in your Azure account that have the DDoS protection enabled.

  Self-service DDoS validation is limited to 1M packets/sec or up to 2 Gbps.
- What if I need to run larger-scale validations?

  Larger validations can be executed, with support from Ixia and Microsoft. Contact your account representative for more information.
- Can I validate the DDoS protection for hosts (IP addresses) residing outside of my Azure account?

  The self-service version of BreakingPoint Cloud allows you to validate DDoS protection only for hosts in your Azure account.

  For DDoS testing outside of Microsoft Azure, please contact Ixia at support@ixiacom.com.
- Can multiple DDoS profiles be run simultaneously?

  For the current release, BreakingPoint Cloud supports one active test for each user account. A single DDoS test can be configured to simulate a single DDoS attack — for example, TCP SYN Flood.
- Can I validate the DDoS protection for IPv6 resources?

  No. This release supports only IPv4 addresses.
- How do I cancel my monthly or yearly subscription plan?

  To cancel your subscription, please email us at support@ixiacom.com.
- Should I target a production environment or a test environment?

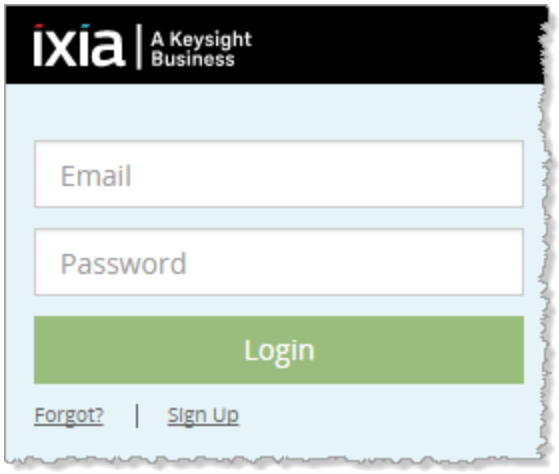
  If you are new to DDoS validation testing, we recommend that you run the initial tests in a sandbox environment.

  There are several situations where DDoS validation can be valuable for an organization, and the decision to target a production or test environment needs to be driven based on your business goals. Refer to Use cases on page 4 for a description of some use cases that can help you with these decisions.

Log in to the BreakingPoint Cloud console

To access the BreakingPoint Cloud console:

1. Go to the BreakingPoint Cloud login page: https://breakingpoint.cloud.
2. Enter the email address and password associated with your BreakingPoint Cloud subscription.



3. Click **Login**.

The console screen opens.

Web console description

BreakingPoint Cloud provides a simple web console for creating and executing DDoS validation tests.

Windows

The BreakingPoint Cloud web console comprises two main windows:

VALIDATION	You work in the **Validation** window while configuring and executing tests. All of the required test configuration fields are provided, along with the **Start Test** and **Stop Test** buttons. Test-progress statistics are displayed in this window during test execution.
HISTORY	The **History** window provides a list of recent test results. You can select any test from the list, load it into the **Validation** window, and re-run it (as described in Re-run a test on page 16). You can also get support for a specific test by clicking the icon for a specific test. This opens a window containing support instructions.

Menu

The BreakingPoint Cloud web console provides a drop-down menu (⚙) providing access to common operations and product information.

Option	Description
Target Subscriptions	Opens the **Target IP Address Validation** dialog. Refer to Authorize Azure subscription access on page 11 for detailed information.
Terms of Service	Opens the **Terms of Service** dialog, which displays the text of the legal agreement governing this product's service usage. The dialog provides a **Download** button with which you can download a copy of the document (PDF format).
Billing	Opens the **Billing** dialog, which displays usage metrics. You can select the billing interval from a drop-down list, and you can download a copy of your invoice.
User Guide (HTML)	Opens the HTML version of the BreakingPoint Cloud User Guide (in a separate browser window or tab).
User Guide (PDF)	Downloads a copy of the PDF version of the BreakingPoint Cloud User Guide.

Option	Description
API Reference (HTML)	Opens the HTML version of the BreakingPoint Cloud API Reference Guide (in a separate browser window or tab).
API Reference (PDF)	Downloads a copy of the PDF version of the BreakingPoint Cloud API Reference Guide.
Python API Client	Downloads the Python API Client to your downloads folder. The API client is documented in the *API Reference Guide*, which is available (HTML and PDF format) from this menu.
Contact Ixia Support	Opens the **Contact Ixia Support** page (https://support.ixiacom.com/contact/support).
About	Opens the **About** dialog, which displays the BreakingPoint Cloud version that you are currently using, plus other related information. In addition, it provides a link to the Release Notes, the listing of third-party components, and a Contact Us link.
Logout	Logs you out of BreakingPoint Cloud.

Authorize Azure subscription access

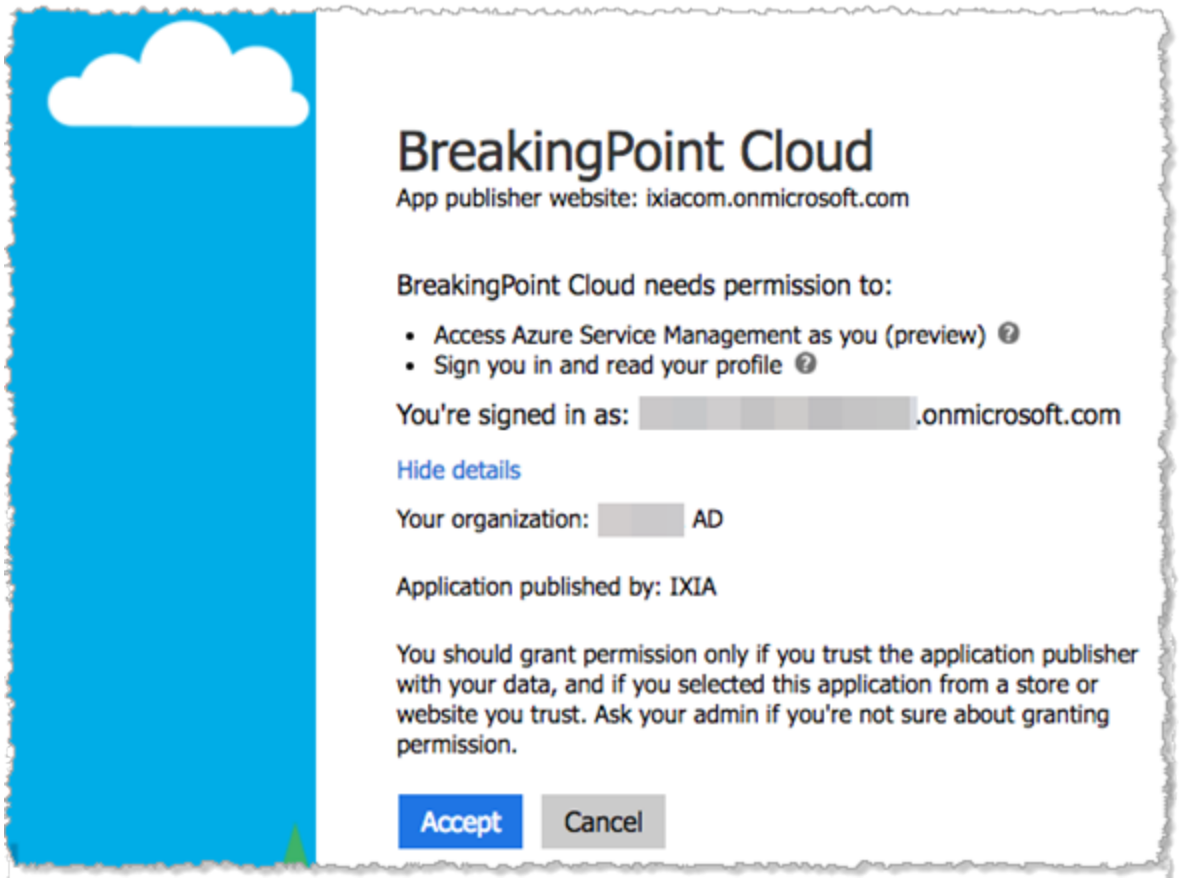
Any IP address that you designate as the target of a test must be owned by an Azure subscription to which you have access. You allow BreakingPoint Cloud to access your Azure subscriptions using the BreakingPoint Cloud **Target IP Address Validation** window.

Adding an Azure subscription ID

To validate an Azure subscription ID for use with BreakingPoint Cloud:

1. Select **Target Subscriptions** from the gear (⚙) menu.
   The **Target IP Address Validation** window opens.
2. Enter your Azure Subscription ID.
3. Click **Add Subscription**.
   When first adding an Azure subscription ID using a specific Azure Active Directory (AD) user account, you need to grant permission for BreakingPoint Cloud to access the Azure account:
   a. When prompted, pick a user account.
   b. Click **Accept** to grant permission.

For example …



Removing an Azure subscription ID

To remove authorization to use an Azure subscription ID in BreakingPoint Cloud:

1. Select **Target Subscriptions** from the gear (⚙) menu.
   The **Target IP Address Validation** window opens.
2. Enter your Azure Subscription ID.
3. Click **Remove Subscription**.

Removing BreakingPoint Cloud permissions

To remove BreakingPoint Cloud permissions to access to an Azure AD user account:

1. Go to https://myapps.microsoft.com.
2. Log on using the Azure AD user account for which you are revoking permissions.
3. Select the BreakingPoint Cloud app, then click **Remove** from the drop-down menu.

Create and run tests

This section provides instructions for creating and running BreakingPoint Cloud validation tests.

In this section:

Configure and start a test

To configure and start a DDoS validation test:

1. Log on to the BreakingPoint Cloud web console: https://breakingpoint.cloud.
   Upon successful logon, you will see the configuration screen.
2. Configure the settings for the test, as described below.
3. Click **Start Test**.

Once you start the test, BreakingPoint Cloud:

- validates the *Target IP Address* that you specified
- prepares the required resources, and initiates the test actions
- starts collecting and displaying test statistics

Normally, you will allow the test to run through to completion (based on the Test Duration that you selected), but you can abort the test at any time by clicking **Stop Test**.

Configuration settings

Setting	Description
Target IP Address	Enter the IPv4 address of the node that you are validating. When you start the test, BreakingPoint Cloud will verify that the IP address that you entered is owned by the Azure account that is executing the attack.
Port Number	Enter the appropriate TCP/UDP port number for the specific protocol and service that you are validating. Examples: port 53 for DNS, port 88 for Kerberos, port 464 for Kerberos kpasswd. **Important!** BreakingPoint Cloud does not validate port numbers. Be sure to enter a valid port number for the protocol and service that you are targeting in your test.
DDoS Profile	Select from the list of profiles. Each profile specifies the type of DDoS attack that will be generated. Refer to DDoS profiles on page 21 for profile descriptions.

Setting	Description
Test Size	Select one of the *Test Size* profiles for the selected *DDoS Profile*. Each Test Size profile is a set combination of: • **Data volume and rate:** The amount of data that the test will send to the Target during the test. This is expressed as packets per second (pps) and bits per second (bps). • **Source IPs:** The number of source IPs (simulated bots) from which the test data will originate (from 5 to 50 source IPs). Each *DDoS Profile* has its own associated set of *Test Size* profiles. These profile associations have been established to ensure that the DDoS validations remain within safety thresholds for production cloud deployments. In addition, it ensures that the available test sizes are suitable for the protocols that the DDoS attacks are exploiting.
Test Duration	Select the desired duration of the test. The durations range from 10 minutes to 30 minutes.

See also:

- Manage data usage on page 19
- Analyze the test results on page 17

Re-run a test

BreakingPoint Cloud maintains a history of the tests that you have run.

To re-run a test:

1. Select **History** from the BreakingPoint Cloud tool bar.
   The **Recent Test History** screen opens.
2. Click the desired test to select it.
3. Click **Load Test**.
   The test opens in the **Validation** window.
4. Optionally, make any desired modifications to the test.
5. Click **Start Test**

Analyze the test results

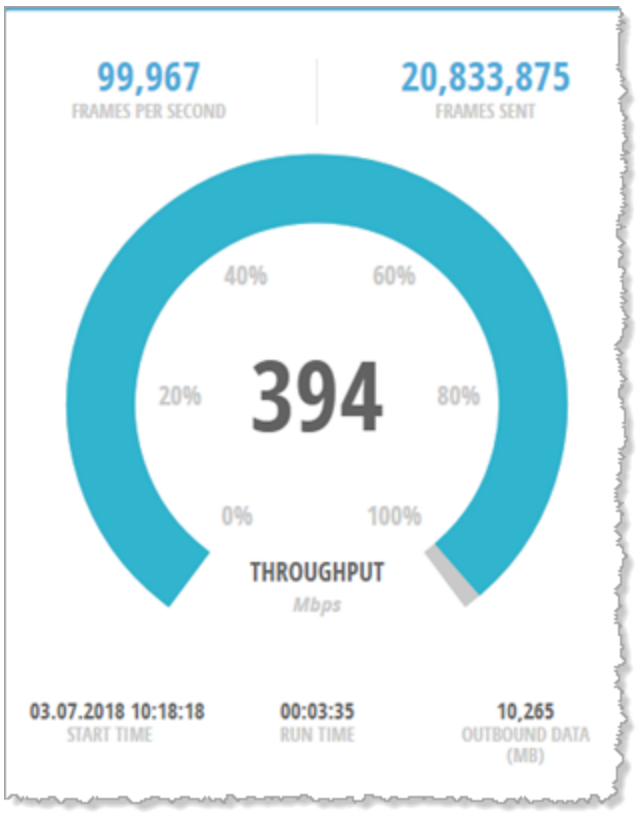
When you start a test, BreakingPoint Cloud starts transmitting packets to the test's *Target IP*. You can analyze the test progress and results from the traffic origination and destination sides:

- BreakingPoint Cloud displays outbound data statistics throughout the duration of the test.
- Assuming that Azure Standard DDoS Mitigation is enabled in your network, the Azure Monitor service should collect and report detailed metrics throughout the duration of the test (inbound traffic rates are reported in the Azure Public IP Metrics). You should also receive alerts, if you have configured alerting for any of the Azure Monitor metrics exposed by DDoS Protection.

Note: The Azure portal statistics are delayed by 7 minutes.

BreakingPoint Cloud statistics

While a test is in progress, the BreakingPoint Cloud window displays data throughput and timing statistics. For example:



These statistics are continuously updated throughout the duration of test.

Statistic	Description
Frames per second	The average number of frames transmitted per second.
Frames sent	The total number of frames sent.
Throughput	The **Throughput** graphic shows the current percentage of the *Test Size* (400 Mbps, for example), as well as a periodically-updated numeric value. At the completion of the test, the average throughput is displayed.
Start time	The date and time that the test started.
Run time	The exact amount of time during which the test was running.
Estimated Outbound Data	The estimated amount of outbound data that the test will transmit to the *Target IP*. This is calculated as maximum data rate (from the *Test Size*) multiplied by the run time.
Outbound data	The actual amount of outbound test traffic. The values are aggregated from each of the source IPs configured for the test (the number of source IPs is part of the *Test Size* profile). In most cases, this value will be close to the Estimated Outbound Data value. Differences between the Estimated Outbound Data value and the actual value are generally attributed to a few seconds of test setup time (the estimated value does not account for this).

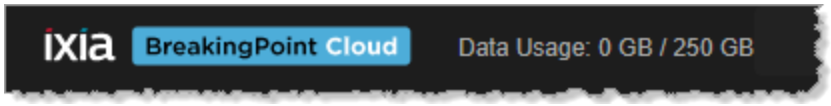
Test History results

When the test stops, the test results are added to the **History** window (as described in Web console description on page 9).

Manage data usage

BreakingPoint Cloud is a subscription-based SaaS and, as such, your costs are based only on data consumption. To best manage your data usage (and, therefore, costs):

- Observe the **Data Usage** report that appears in the title bar. It shows how much data you have presently consumed. For example, for a new subscription you will see:



- When preparing a validation test, check the **Estimated Outbound Data** display in the configuration window. If the amount shown would put you over your quota, BreakingPoint Cloud will prompt you to increase your quota if you have a paid subscription. Otherwise, you may be able to modify your settings to decrease the outbound data; for example, choosing a smaller *Test Size* or shorter *Test Duration*.

Trial mode usage quota

A free trial gives you 100 GB of data to use for evaluating the product. The functionality is the same as that of a subscription user, except that the data quota is fixed at 100 GB. If a you attempt to run a test that will exceed the trial quota, you will receive a notification and the test will not run. (You can upgrade from a trial user to a subscription user using the **Buy Now** link in the BreakingPoint Cloud title bar.)

Paid mode threshold increase

When you have an active subscription, you purchase data for validation testing in increments of 250 GB. The process is as follows:

- BreakingPoint Cloud monitors your data usage and, if it drops to 100 GB (or less), you will be prompted to increase your threshold. For example:

  You have consumed 1137.91 GB. To avoid accidental overspend, we require acknowledgement every 250 GB to proceed. YES, I UNDERSTAND.

- When you click **YES, I UNDERSTAND**, BreakingPoint Cloud increases your threshold by 250 GB and you can proceed with further testing.

See also, Display billing and usage metrics on page 20.

Display billing and usage metrics

1. Select **Billing** from the gear menu (⚙).

   BreakingPoint Cloud opens the Billing dialog, which shows traffic usage and costs for the current billing interval.
2. To view the metrics for a different billing interval, select it from the drop-down list.
3. To download a copy of your invoice, click **Download Invoice**.

DDoS profiles

When you configure a DDoS test, you will select a specific *DDoS Profile*. That profile determines the specific type of attack that will take place.

The following sections provide descriptions of the available DDoS profiles.

TCP profiles

TCP flood attacks are typically state exhaustion attacks that attempt to consume all available connections or force a target node to exhaust is resources by processing the incoming flood of packets. BreakingPoint Cloud provides one TCP DDoS profile:

TCP SYN Flood

In a TCP SYN Flood attack, the attacking botnets exploit the basic TCP three-way handshake process by sending syntactically-valid TCP SYN packets toward the target host. Upon receiving each SYN packet, the host responds with a SYN-ACK packet, and then waits for the expected ACK packet. Normally, the TCP socket connection will be established once the ACK is received. In a DDoS attack, the attacking bots never responds with the proper ACK packets, resulting in a large number of sessions that remain open until a session timeout is triggered. The incomplete sessions exhaust the target server by depleting system memory and requiring CPU cycles to process the TCP handshakes. Without proper mitigation procedures in place, this will result in severe performance degradation or complete server shutdown.

UDP-based profiles

There are several variations of flood attacks that use UDP packets in an effort to overwhelm the attack target. UDP flood attacks typically exploit the simplicity of the UDP protocol. Because there is no need to establish a connection and no provision to limit the volume of traffic, the attacker can easily send a flood of traffic over a UDP channel, targeting either random or selected ports. BreakingPoint Cloud provides the following set of UDP-based DDoS profiles:

DNS Flood

In a DNS Flood attack, the attacking botnets send a flood of DNS requests to the target domain, resulting in potential traffic congestion and a processing overload on the part of the domain name server as it attempts to resolve the requests. Unless properly detected and mitigated, this type of DDOS attach can compromise that domain's ability to respond to valid queries. UDP port number 53 is registered to the domain service (Domain Name Server).

NPTv2 Flood

In an NTPv2 Flood attack, the attacking botnets send MONLIST requests to an NTP server, using a forged source IP address. The intended effect is to overwhelm the target (the forged IP) with the MONLIST responses. BreakingPoint Cloud simulates the NTPv2 attack by internally generating the MONLIST responses and sending them to the node that is configured as the Target IP for the test. UDP port number 123 is registered to the ntp service (Network Time Protocol). Refer to http://www.ntp.org for detailed information about NTP.

SSDP Flood

An SSDP Flood attack is an amplification attack in which the botnets exploit the fact that many devices implementing the Simple Service Discovery Protocol (SSDP) do not verify that a request has originated within the same network as the server: they will send their responses over the public internet. UDP port number 1900 is registered to the ssdp service. If a firewall has not closed port 1900, the SSDP DDoS attack can use a forged source IP address to generate a flood of UDP responses directed towards the target node. BreakingPoint Cloud simulates the SSDP responses sent to the Target IP from SSDP-enabled servers.

UDP Flood

BreakingPoint Cloud provides UDP Flood DDoS profiles with packet sizes ranging from 64 bytes (minimum frame size for IPv4) to 1514 bytes (Ethernet frame maximum).

A UDP flood attack relies on a large number of attackers sending multiple UDP packets to the victim's computer, saturating its bandwidth with useless UDP packets. The attack packets can target open and closed ports, and will often use random ports. If the packets are targeting ports on which the victim is not listening, ICMP Destination Unreachable (Port Unreachable) packets will be sent in response to the source IP (typically spoofed) included with each UDP packet. This will result in additional processing time and potentially an additional storm of UDP packets destined to other computers.

UDP Fragmentation

In a UDP Fragmentation attack, the attacking botnets send a flood of UDP fragments to the target host. The host can exhaust its CPU resources as it attempts to reassemble the packet fragments.

UDP Memcached

In a UDP Memcached attack, the attacking botnets send forged UDP packets to UDP-enabled Memcached servers that are open to the Internet. In response, these servers send large numbers of UDP packets to the attack target. UDP port number 11211 is registered to the memcache service (Memory Cache Service). BreakingPoint Cloud simulates the Memcached responses sent to the Target IP from the UDP-enabled Memcached servers. (Refer to https://memcached.org/ for detailed information about Memcached.

INDEX

Ixia, a Keysight Business
26601 West Agoura Road
Calabasas, California 91302