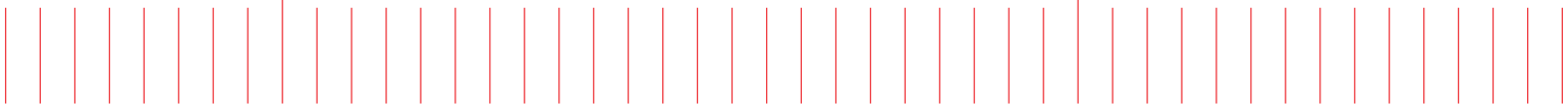
BreakingPoint Quick Test

Release 1.2

User Guide



Document version: 202003311537-05:00

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.

Safety Information

A **CAUTION** notice denotes a hazardous situation that, if not avoided, could result in minor or moderate injury.

A **WARNING** notice denotes a hazardous situation that, if not avoided, could result in death or serious injury.

Contacting 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
Regional and local support contacts:		
APAC Support	+91 80 4939 6410	support@ixiacom.com
Australia	+61-742434942	support@ixiacom.com
EMEA Support	+40 21 301 5699	support-emea@ixiacom.com
Greater China Region	+400 898 0598	support-china@ixiacom.com
Hong Kong	+852-30084465	support@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	+65-6215-7700	support@ixiacom.com
Taiwan (local toll-free number)	00801856991	support@ixiacom.com

Documentation conventions

The following documentation conventions are used in this guide:

Describing interactions with the UI

You can interact with products by using different input methods: keyboard, mouse, touch, and more. So in most parts of the user documentation, generic verbs have been used that work with any input method. In cases where input-neutral verbs do not work, mouse-specific verbs are used as the first choice, followed by touch-specific verbs as the second choice.

See the following table for examples on how you can interpret the different input methods.

Input-neutral	Mouse	Touch
Select **Modify**.	Click **Modify**.	Tap **Modify**.
Select **Accounts** > **Other accounts** > **Add an account**.	Click **Accounts** > **Other accounts** > **Add an account**.	Tap **Accounts** > **Other accounts** > **Add an account**.
To open the document in Outline view, select **View** > **Outline**.	To open the document in Outline view, click **View** > **Outline**.	To open the document in Outline view, tap **View** > **Outline**.
Select **Protocols**.	Click the **Protocols** tab.	Tap **Protocols**.
-NA-	Double-click the **Client** wizard.	Double-tap the **Client** wizard.
Open the **Packages** context menu.	Right-click **Packages** to open the shortcut menu.	Long tap **Packages** to open the shortcut menu.

Deprecated words

The following words have been replaced with new words, considering the audience profile, our modern approach to voice and style, and our emphasis to use input-neutral terms that support all input methods.

Old usage...	New usage...
shortcut menu, right-click menu	context menu
click, right-click	select
drag and drop	drag

CONTENTS

Welcome

Welcome to BreakingPoint QuickTest. BreakingPoint QuickTest (BPS QT) simplifies application and security assessments by providing individual test methodologies and assessments based on the type of test needed. These easy-to-use test methodologies leverage the ongoing research from our global Application and Threat Intelligence (ATI) team and the many years of experience Ixia engineers have in testing various application and security devices and networks. These test suites will be continuously updated to ensure that the assessments are based on the current state of the internet.

Within each test suite there are several categories of assessments that you can optionally select based on your test needs. Test suites also employ powerful stabilization and goal-seeking algorithms that ensure accurate assessment of a diverse set of devices and systems and provides actionable insights after each test run.

BPS QT test suites

BPS QT provides the following test suites:

- **Performance**: The Performance suite measures system performance while handling various types of application traffic mixes, Web clear text traffic and encrypted traffic mixes of various sizes.
- **Encryption Performance**: Performs a series of tests with various well-known ciphers to measure performances of the device or network while handling encrypted traffic.
- **NETSECOPEN**: The NetSecOpen standard provides guidelines and best practices for testing modern network security infrastructure including Firewall, IPS, NGFW and Threat Detections solutions and services.
- **Perimeter Assessment** (coming soon): Performs exhaustive application performance measurement and security checks of the network perimeter.
- **DDoS Performance** (coming soon): Performs a series of tests with various DDoS methods ranging from IP, TCP, UDP and applications like HTTP, NTP, and DNS.
- **Security**: Measures the security efficacy of Network Infrastructure Devices. Examples include, Next Generation Firewalls, routers, DPI devices, proxies or a mix of all these devices and more.

CHAPTER 1 Installation instructions

This section provides detailed instructions for BPS QT installation on a PerfectStorm or CloudStorm system.

Supported platforms and compatibility matrix

BPS QT is supported on PerfectStorm ONE, XGS12 and XGS2.

Supported Hardware:

- PerfectStorm 40GE2NG with 8x10G in fan out mode
- PerfectStorm 10GE8NG
- PerfectStorm 10GE8QT
- CloudStorm with 8x10G in fan-out mode

Compatibility Matrix

BreakingPoint QuickTest	9.02
IxOS	9.00 Patch1/Patch2
IxLoad	9.0
IxNetwork	9.0
Licensing	5.10/5.20

Note: To see the most the up-to-date compatibility version information, see the BPS QT Release Notes. The BPS QT Release Notes can be obtained at: https://support.ixiacom.com/user-guide **> BreakingPoint**.

Supported HTML browsers

The following table lists the supported the HTML browsers. HTML browser versions that are more current than the versions listed in the table may work, but have not been tested at this time. Beta versions of HTML browsers are not supported.

Browser	Recommendations for Windows	Recommendation for MAC
Google Chrome	77.0.3865.120 (64-bit)	77.0.3865.120 (64-bit)
Firefox	69.0.3 (64-bit)	69.0.3 (64-bit)
Microsoft Edge	44.18362.387.0	N/A
Safari	Not supported	13.0.2
Internet Explorer	Not supported	Not supported

Installation

Systems running Windows IxOS (PS One)

If your system is running Windows IxOS, please follow the steps below to convert to Native IxOS and install the BreakingPoint image to the system.

You can download the conversion guide along with the necessary files from the Ixia support web page.

1. Go to: https://support.ixiacom.com/ and then log in.
2. Select **Software Downloads > IxOS > 9.0**.
3. For question #1, select the **PS One***.
4. For question #2, select **Windows** for Base software.
5. For question #3, select the **Yes** radio button to get to the conversion guide.
6. Follow the instruction from the *Converting XGS and PSOne to NativeIxOS Guide* (PDF).
7. Follow the steps in the Upgrading IxOS on Native IxOS systems section.

Note: After conversion to Native IxOS there may not be enough available disk space to restore a previously exported backup (especially for files larger than 1GB). If there is not enough space available, you can delete the preconversion BreakingPoint data by using the IxOS CLI command, uninstall bps legacy (which frees up 250GB of disk space). Be aware that if you are reverting back to a Windows-based architecture, BPS application (BPS VM) will not start after uninstalling BPS legacy.

Note: For systems running Native IxOS, we strongly recommend that you create backups of your system before upgrading the BreakingPoint Firmware.

Upgrading IxOS on Native IxOS systems

Online:

1. Access the Ixia Chassis CLI with the following command, - ssh admin@<chassisIP> -p 22, password: admin
2. Then apply command **enter Chassis** to access the Chassis CLI.

You will be notified through the CLI when new builds of IxOS are available.

3. Run the install ixos <version> command to perform the install. The build will be installed automatically from Ixia IxOS online repository (which is predefined in the OS).

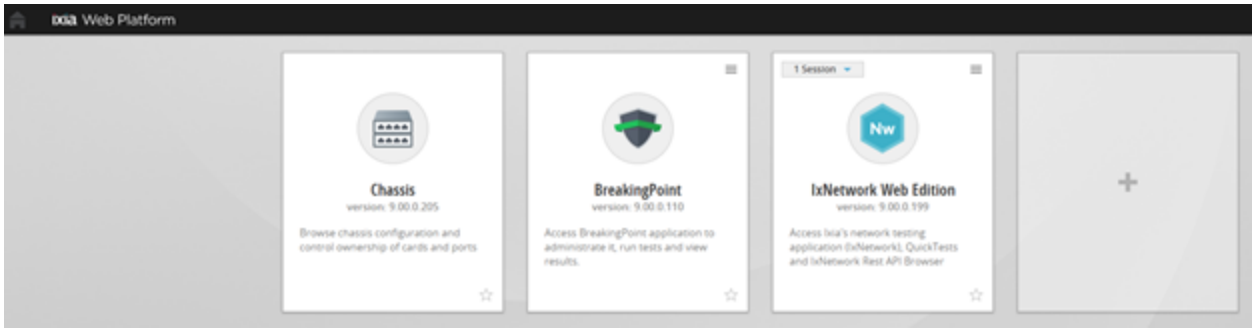
Offline:

1. Download the IxOS build from http://support.ixiacom.com/supportoverview/product-support/downloads-updates/versions/21.2.
   a. Use FTP to put the file on to the Chassis.
      i. ftp://<chassisIP> user: admin password: admin
      ii. put Ixia_Hardware_Chassis_XX.XX.XX-EA.tar.gz.gpg
2. Access the IxOS using the following command, CLI - ssh admin@<chassisIP> -p 22, password: admin
3. Then apply command **enter Chassis** to access to Chassis CLI.
4. Run the install ixos <version> command to perform the install of the version that was downloaded.
5. Reboot the chassis.

Install BPS QuickTest

1. After the IxOS installation is complete, connect to Chassis IP as follows: https://<Chassis IP>
2. Log in by using user id: admin, password: admin.

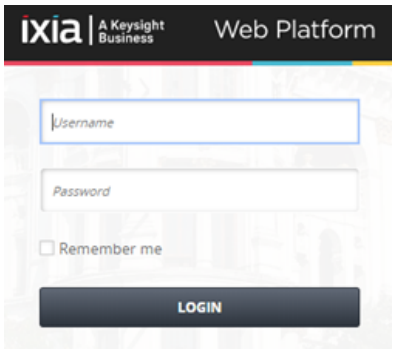
After logging in, the WebPlatform Dashboard will display as shown in the image below.



3. Select the **Install New Applications** icon (+) to install BreakingPoint QuickTest using the BreakingPoint QuickTest installer Package (ixia-web-platform-bpse-9.0…..waf). You can download the installer package (ixia-web-platform-bpse-9.0…..waf) from the IXIA support download webpage.
4. Select the Installer Package.
5. Select **OK** to start the BreakingPoint QuickTest installation.

CHAPTER 2 Login procedure

1. Open a supported web browser.
2. In the URL field, type the IP address or hostname of the Ixia chassis where the Ixia Web App server components are installed.
   a. For example: 192.168.100.56
   b. The Login prompt appears.



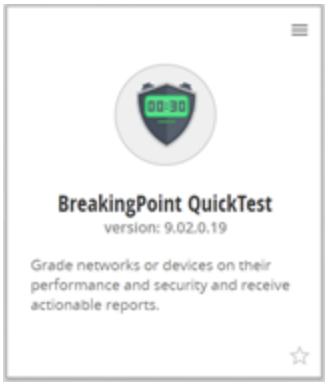
3. In the **Username** field, type your user ID.
4. In the **Password** field, type your password.

If you want the browser to automatically fill in the Username and Password field for future logins, select the **Remember Me** box.

5. Select Login.

The Ixia Web Platform Dashboard displays.

6. Select the **BreakingPoint QuickTest** application icon.

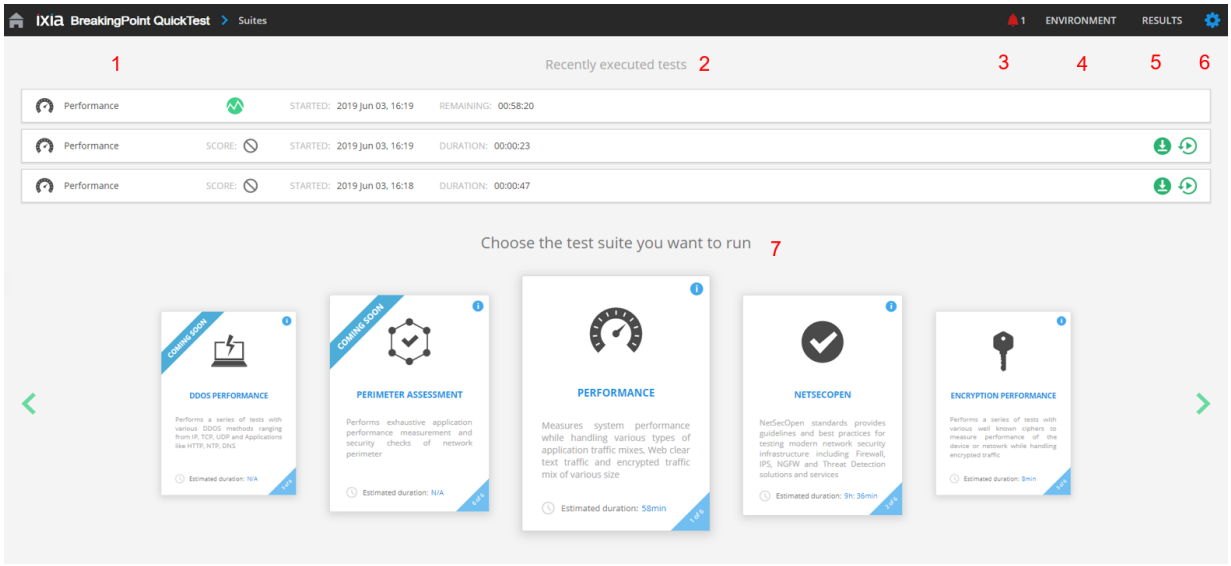


Note: While the version number displayed in this guide may be different than the version number displayed in your BPS QT user interface, the procedures are the same.

CHAPTER 3 User Interface overview

This section provides an overview of the BPS QT user interface.

Tip: The BPS QT user interface is very intuitive. Tooltip help is provided, and several objects also display helpful text. For example, text displayed on the test suite icons (shown in the image below) indicate the estimated duration required for the completion of the entire test suite.



1	**Breadcrumb navigation**: Provides links back to each previous page that the user navigated through to get to the current page. Select the Home icon to jump back to The Ixia Web Platform Dashboard.
2	**Recently executed tests**: This area of the page displays recently executed and currently running tests. Test status information (when started, test score, remaining time until completion, duration, etc.) is displayed. You can select the test score to jump to the detailed **Assessment Score** or select the Running Test symbol to jump to the test Performance detail. Tests can also be restarted from this area. Note that nothing will appear in this area until a test suite is run.
3	**Notifications indicator**: A number will display next to this icon to indicate the number of current notifications. Select the icon to view informational messages, warning and errors. An error notification will change the indicator color to red.

4	**Environment**: Select Environment to configure your test environment setup including ports and IP addresses. A **Validate** option allows you to validate the network connectivity of your setup before you save your configuration.
5	**Results**: Select Results to view test results and the status of currently running tests. Results can be saved to a PDF file.
6	**Settings gear**: Select the Settings Gear to report an issue, take system diagnostics or to logout.
7	**Test suite area**: Select the test suite that you want to run from this area. Select the green arrows at the left and right of the test suites to navigate through the available test suites in a carousel display.

CHAPTER 4 Test methodology overview

This section provides a high-level overview of the test methodology.

1. Configure the Environment
   a. Configure traffic ports and IP addresses
   b. Validate the network connectivity of the environment
   c. Save the environment configuration
2. Select, configure and run a test suite
   a. Optionally customize the test suite by selecting/clearing the category of tests that will be run
   b. Run the test suite
3. View test progress and statistics
   a. Select your test from the **Currently running tests** area of the home page or select the **Results** and then select your test suite results
   b. View the test **Observations** and select test categories for detailed information on their test run

See Understanding test behavior and interpreting results for details on test run indicators, the test algorithm and grading.

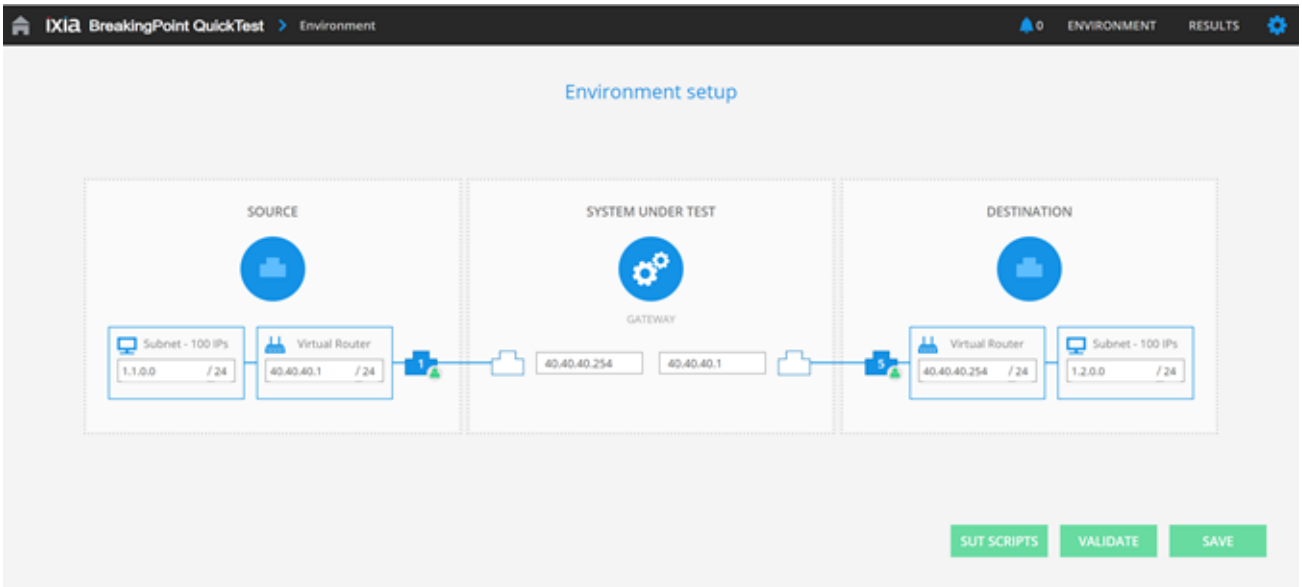
CHAPTER 5 Configure the environment

Note: Ensure that the IP addresses that are assigned during this procedure allows for IP network connectivity between the source ports, the system under test and destination ports. Static routes must also be configured on the DUT or System Under Test to ensure end-to-end connectivity between the DUT and BPS QT endpoints.

Note: Before you begin testing in BPS QT, please make sure that the card that is selected for testing is set to BPS L47 mode from the chassis interface.

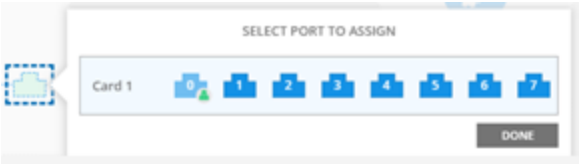
To configure the environment:

1. Select **Environment** from the BPS QT menu. The Environment page displays as shown in the following image.



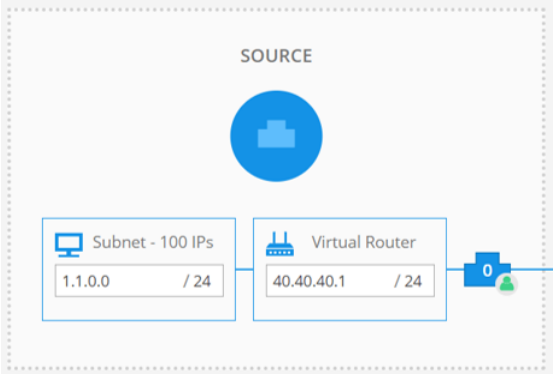
2. Select **Ports**

   a. Select the pulsing port icon ( ) in the **Source** area. The port assignment window will display as shown in the following image.



b. Choose one of the non-reserved source traffic ports. Reserved ports will be grayed out. Unavailable ports will be shown in red.

c. Select **Done**.



d. In the **Subnet** field, enter the base or starting IP address that will be used to create the 100 IP addresses that will be used in your test.

e. Select the pulsing port icon ( ) in the **Destination** area.

f. Repeat steps 2b – 2d for the **Destination** Ports and then proceed to step 3.

3. Select **Validate** to validate the IP connectivity of the configured environment. If validation fails, modify the configured settings as necessary (verify physical connectivity and that the configured IP addresses, in the environment and on the DUT, allow for proper network connectivity). If validation passes, proceed to the next step.
4. Select **Save** to save the environment configuration.

SUT Scripts

The **Environment** window provides a **SUT Scripts** button which allows you to connect to a System Under Test (SUT) via SSH and upload a script to that can be run before each test (such as SUT Session Cleanup).

Note: After configuring the SUT script in the environment you can enable or disable the script's execution at the suite configuration level. This is done from the Suite view - **Configuration** > **Run SUT Script**. By default, this setting is disabled.

The following dialog is displayed when the **SUT Scripts** button is selected.

Follow the steps below to configure the SUT Scripts dialog and run a script on the SUT:

1. Enter the **Username** and **IP** of the SUT.
2. Select port number 22 for the SSH connection (default) using the **Port** selector.
3. Select the **BROWSE** button to upload a CSV file that contains the commands that will be sent to the SUT. The CSV file must have the following script format:
   `COMMAND TYPE(send/expect/wait/expect-close), <command>`
4. Select **SAVE** to save the script to the database. A confirmation message will display if the uploaded script has correctly formatted commands.
5. Select the **VALIDATE** button to check both the connection with the SUT and integrity of the uploaded script.
6. To activate this feature:
   a. Select the BPS QT Suite that you want run.
   b. Select the **Configuration** button.
   c. Select the **Run SUT Script** option.
   d. Select **SAVE**.

Generating the SUT Script

As a best practice, Ixia recommends using BPS Classic (BPS running on a hardware chassis) to create a model for the script in order to preview the commands to be added in the CSV script file.

The following example describes the procedure:

1. Open a new session with BPS Classic.
2. Select **Create a Test** from the home page.
3. Edit the SUT script by selecting **BreakingPoint Default** on the **Device Under Test** tab on the left side of the menu
4. For **Connection Type**, select **SSH** and fill in the fields with the SUT's credentials.
5. Select **Create New** in the **Generic Scripts** window and provide a name for the script.
6. In the **Script Commands** select **Auto Create**.
7. After the connection with the SUT is established, enter the commands one by one in the BPS terminal.

8. Copy and paste the **Command** (send/expect/wait/expect-close) and **Command Text** content from the script generated in BPS Classic into a text editor and save the file in CSV format. Ensure to place a comma between the command and the command text on each line and that there are no extra characters or blank spaces. The following is an example of what the resulting CSV file should look like:

```
expect,Password: $
send,ixia\r
expect,C6500>$
send,enable\r
expect,Password: $
send,ixia\r
expect,C6500#$
send,show sessions\r
expect,C6500#$
wait,60000
send,exit\r
expect-close
```

Tip: This training video demonstrates how to create a SUT script by using BPS Classic to generate a model: https://youtu.be/zWKFi51AP6c.

Notes:

- Please consider providing a **wait** command before the **expect-close** command which indicates the time (in milliseconds) that the SUT would take to close all sessions. This command is not sent to the SUT, so it does not need to end with "$" character.
- All commands that are sent to SUT must end with "\r" and all **expect** commands must end with "$".
- All non-alphanumerical characters must be preceded by "\" character (as BPS Classic generates it).

CHAPTER 6 Select, configure and run a test suite

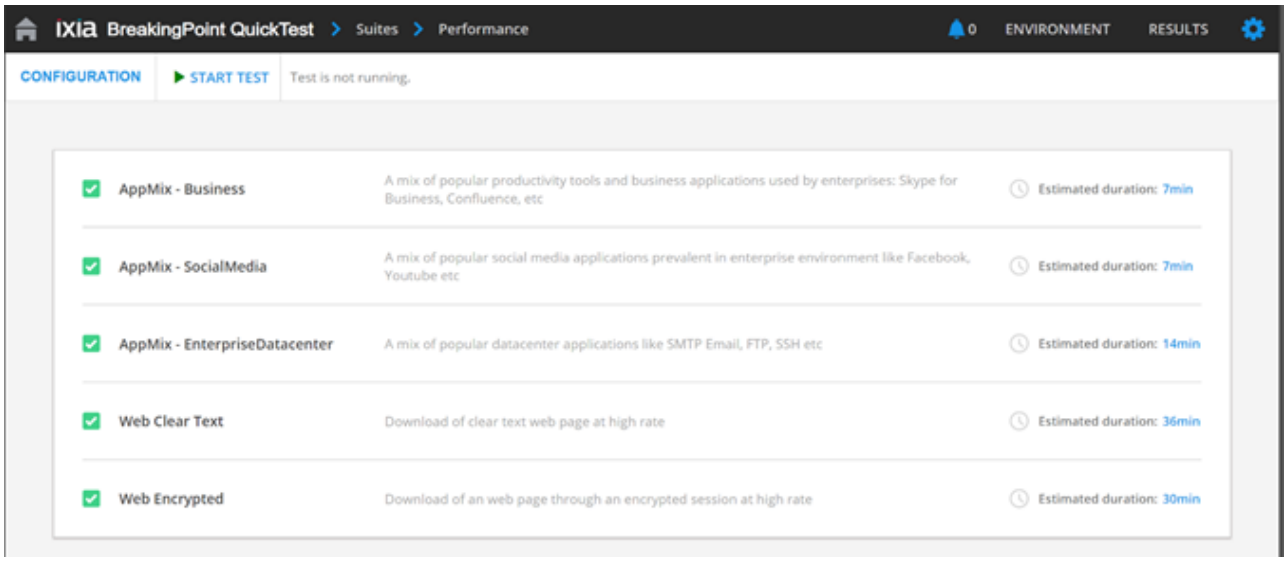
Note: If a legacy BreakingPoint license is installed after BPS QT is installed, BPS QT must be restarted in order to use a card for testing.

Note: Before you begin testing in BPS QT, please make sure that the card that is selected for testing is set to BPS L47 mode from the chassis interface.

Note: After tests that create a high number of concurrent connections have completed, please ensure that the device sessions are cleared. The suites > categories that create a high number of concurrent connections are:

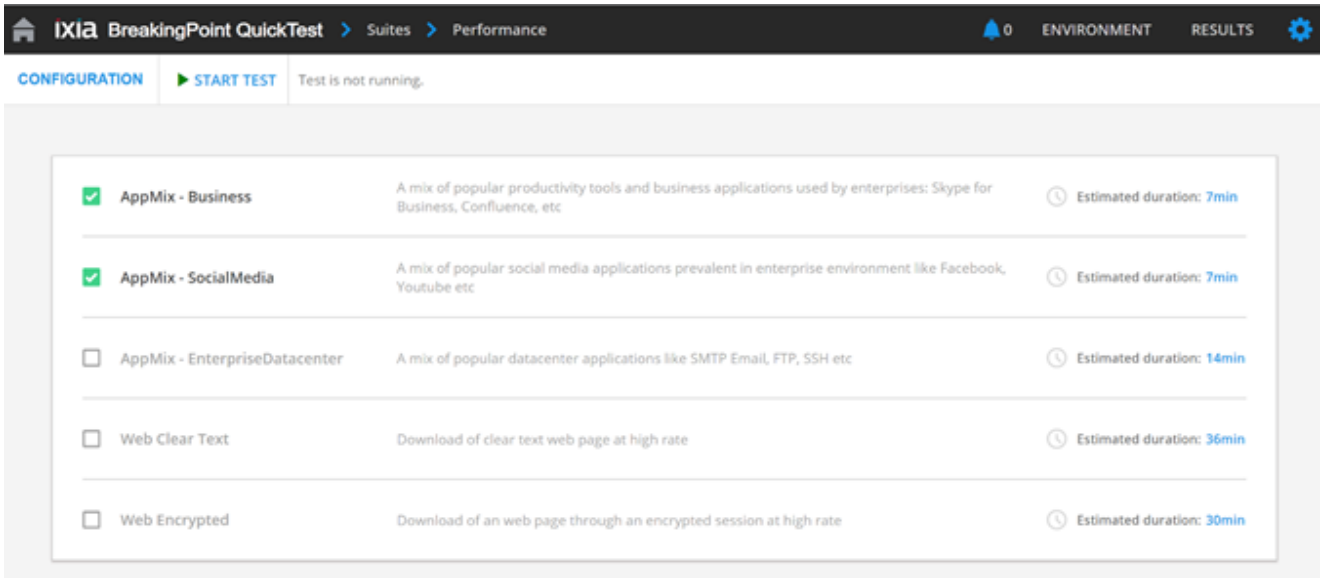
- Performance > Enterprise Datacenter – Stage 2
- NetSecOpen > NetSecOpen Testcase 7.5 HTTP Concurrent Connections – Stage 1
- NetSecOpen > NetSecOpen Testcase 7.9 HTTPs Concurrent Connections – Stage 1

A BPS QT test suite is composed of categories. You are provided the option of choosing which categories you want to enable or disable. Each category is composed of on one or more tests.



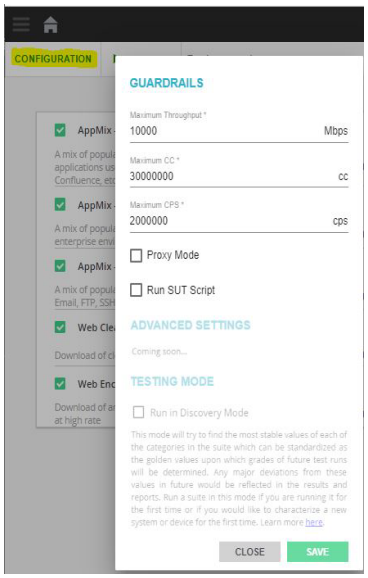
To select, configure and run a test:

1. From the BPS QT home page, select a test suite. You can also select the green arrows at the left or right of the test suites to navigate through the available test suites in a carousel display before making your selection.
2. The Test Categories page will display as shown in the following image. You can clear or select a check box to have a test category included or excluded in the test suite run.



3. Optionally, you can select **Configuration** (located towards the top of the page) to configure **Guardrails** values.

Guardrails are limitations on the Connections Per Second, Maximum Throughput, and Concurrent Connections. The available guardrail settings may vary based on the test that is run. If guardrail values are not manually configured, the test will run with the default guardrail values. Note that grayed out configuration options are designed to be available in future releases.



Proxy Mode: This option should be enabled if the SUT is working in a **Transparent Proxy** mode. Explicit Proxy is not supported by the current suites. Note that this setting is displayed for all of the available suites but was only released for the NetsecOpen suite.

Run SUT Script: When this option is enabled, the SSH/expect script set in the environment setting will be executed before a new **Suite** > **Category** > **Stage** starts or stage new recalibration takes place.

Tip: The **Run SUT Script** feature is useful for setting the system under test to the same state before each measurement. It is recommended to use one script to clean up the connection cache on the device as this can accumulate and impact the SUT performance.

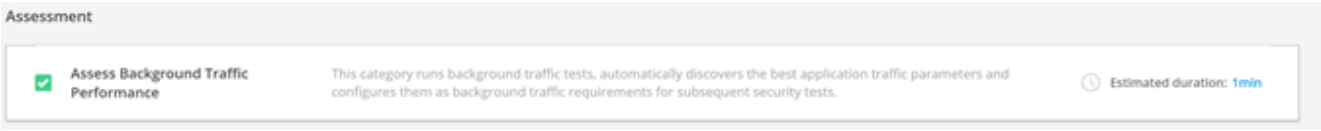
Maximum Segment Size (MSS): MSS is an optional setting that is only available for the NetsecOpen suite. It should be used when the device has optimal results for a specific MSS. By default, the 1460 bytes MSS will be used.

4. Select **Start Test**.
   After a test has been started, a test progress page will display.

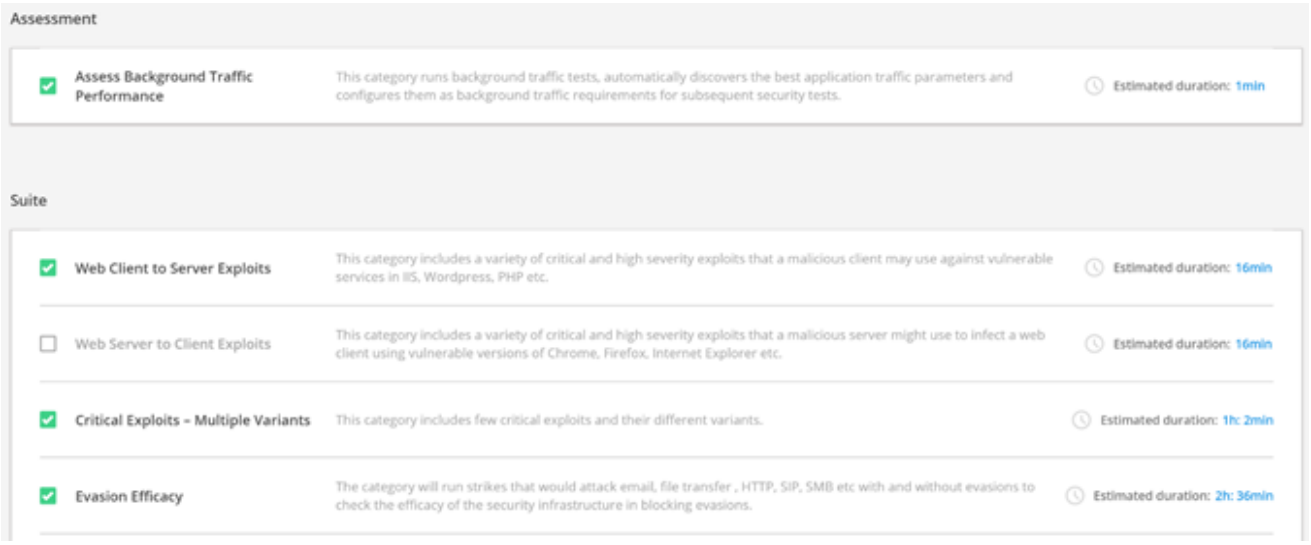
Security test suite classes and weights

The Security test suite is unique because it has two types of classes: Assessment and Suite, both of which are described below.

- **Assessment class**: Unlike the other suites, this class of security suite contains a test category which discovers the best application traffic parameters and configures them as background traffic requirements for the security tests. This configuration will only be enabled if the security tests are selected in the same run with the Assess Background Traffic Performance test category, otherwise default values will be used for each test selected in the Suite class.



- **Suite class**: Contains the security test categories, such as: Evasion Efficacy, Database, Botnets, etc. Each test in this category will run with application background traffic to simulate real-world traffic.



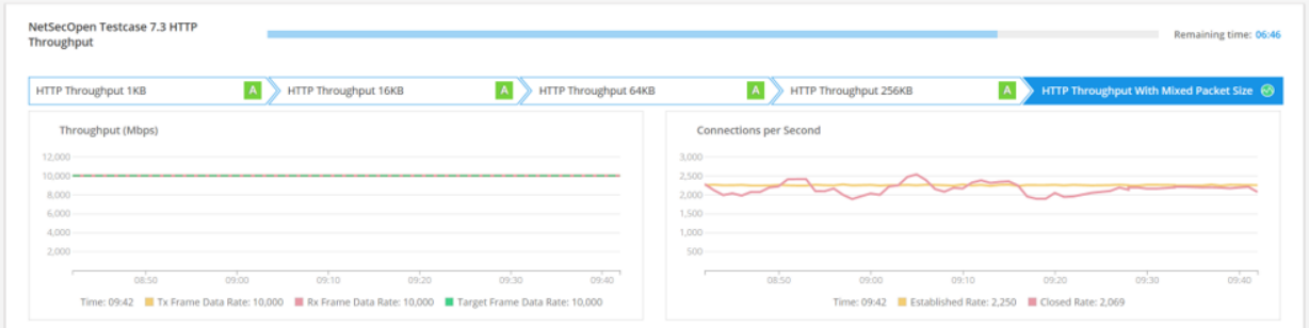
Note: The Security suite has a weight associated with each security test category (as shown in the table below). The grade of the entire run is calculated with a weighted average formula (sum of category score times weight, divided by the sum of weights).

Category	Weight
Web Client to Server Exploits	10%
Web Server to Client Exploits	10%
Critical Exploits-Multiple Variants	10%
Email Vulnerabilities	10%
Dangerous Attachments	10%
Evasion Efficacy	8%
File Server Attacks	8%
Botnet	8%
Malware	6%

Category	Weight
Denial of Service	6%
Database	5%
Reconnaissance Strike	5%
Fuzzing	4%

CHAPTER 7 View test progress and statistics

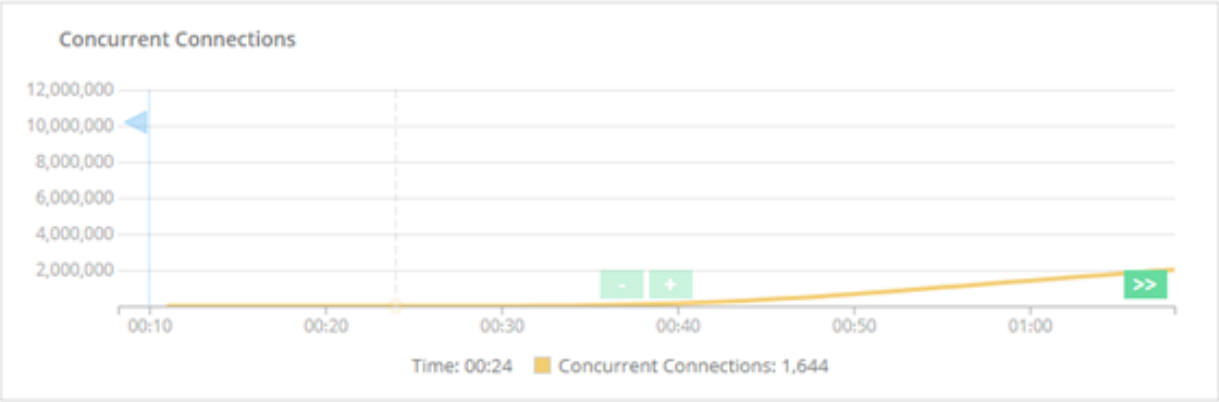
After a test has been started, a test progress page will display. At that time, test progression data from the first test category will be displayed on several statistical graphs. Progress bars are provided to help visualize the progression through the test category. A grade for each completed stage of the test category is also displayed. For example, the following image shows that the 5th stage of the NetSecOpen 7.3 HTTP Throughput test category is currently running, the first 4 stages received an "A", and there is 6 minutes and 46 seconds remaining until the test category is complete.



Upon completion of a test category, the test category receives a grade based on the average grade from all stages and then the test proceeds to the next test category. After the entire test has completed, you can optionally write a description of the test run which be displayed in the **Description** field in the **Test Results** view.

Features for viewing statistical graphs

During a Test Suite run, you can use the following features to view various aspects of a statistical graph.



- Zoom in/out
- **CTRL** + Scroll to zoom in and out
- Jump to the end of the displayed data and continue updating stats
- Select and drag the entire graph to move through the timeline

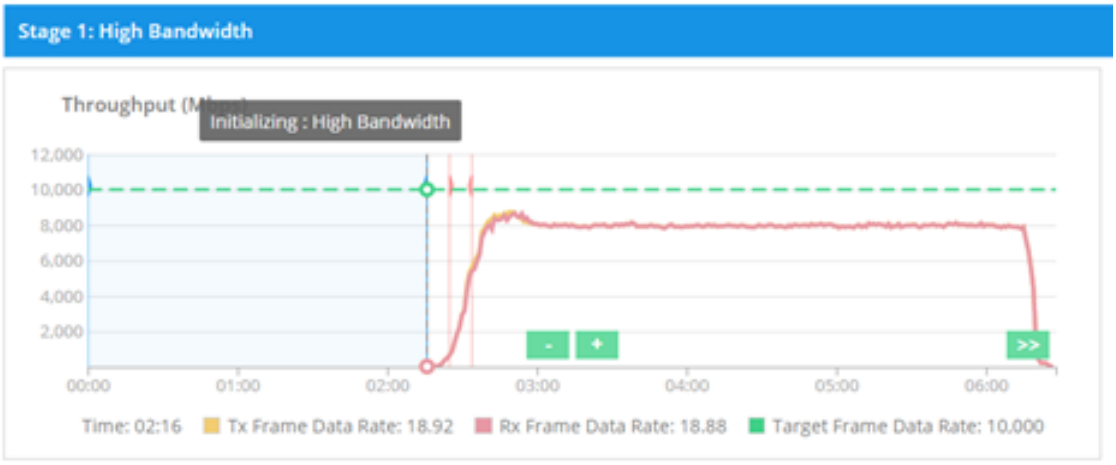
CHAPTER 8 Understanding test behavior and interpreting results

The following information provides detailed information about phases of a test suite run and how to interpret test results.

Initializing phase

The initializing phase of a test consists of a time interval in which the traffic is being applied on the ports. This time interval is not part of the grading algorithm and its length depends on the complexity of the traffic that will be sent through the device under test.

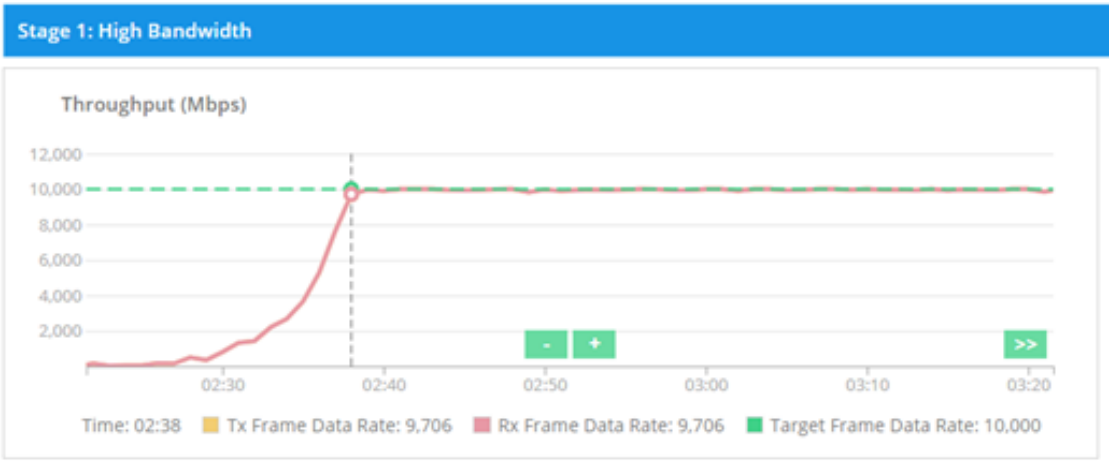
It is visually exposed as an interval between two blue flags as shown in the image below:



During the initialization phase there is no traffic sent through the DUT. This phase has similar phases as **stopping** and **aborting** that are also being signaled with blue flags. There are no requirements for this phase and its duration is not included in the Suite/Category/Stage duration.

Ramp-up phase

The ramp-up phase is the first stage of the test in which traffic is being sent through the device under test.

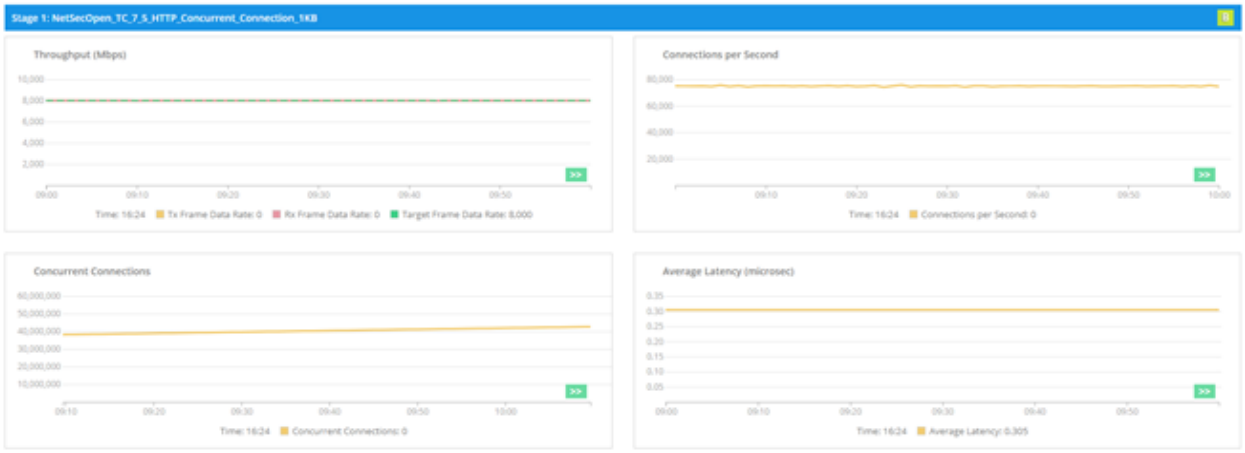


Traffic is sent using an exponentially increasing rate to achieve the desired objective. The objective can be either Throughput or Concurrent Connections or Connections per second.

This ramp-up interval is required so that the device under test will not be overwhelmed with instant traffic. The objective of the test is to determine a device's capability for sustaining an objective once reached. Some stages will also stop and recalibrate the objective of the test if Key Performance Indicators (KPI) degradations (latency, loss, connectivity, etc.) are seen during this phase.

Steady phase

The steady phase represents the time interval for which the stabilized objective must be sustained. This duration depends on the specification of each test. This phase directly affects the grading of the test.

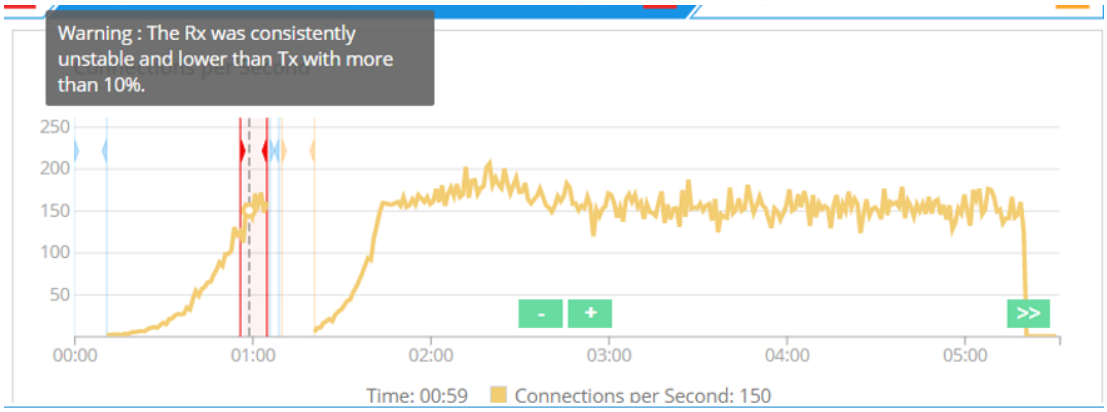


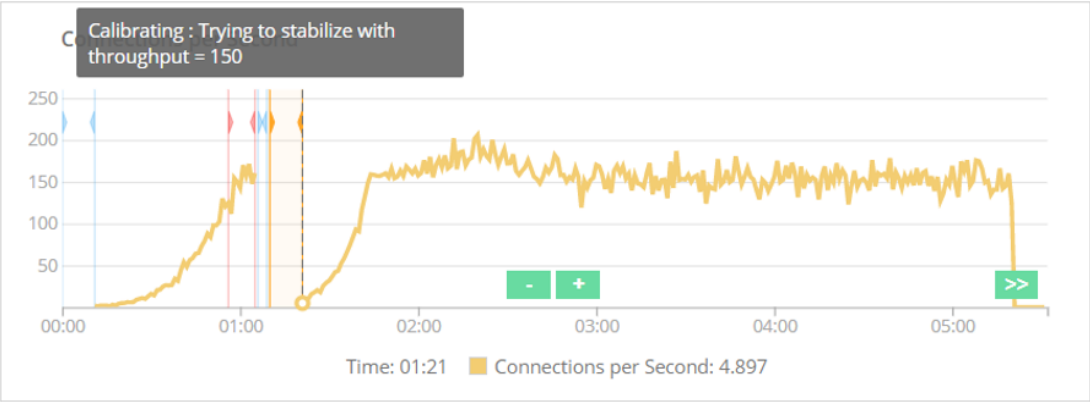
The steady phase has various durations depending on the test type and it tries to keep the same traffic for the configured time interval. During this phase, grades are primarily based on the DUT performance.

Stabilization phase

During this phase, the test will attempt to stabilize based on the test objective. Various messages about stabilization progress are displayed. These messages are described in detail in the Test run indicators section.

Tip: See Notes on Stabilization and Recalibration for more information about the stabilization process.





Notes on stabilization and recalibration

After the Initializing phase, the algorithm will try to stabilize the objective (Throughput, Concurrent Connections and Connections per second) to a value. The following scenarios will cause the algorithm to seek a more stable value.

- Selected value generates large latency spikes
- Selected value does not maintain a per stage specified delta between TX and RX for several acceptable time intervals
- Selected value produces an averaged objective that is unstable
- Selected value causes layer 3 TCP failures
- For the NetSecOpen suite, the algorithm is also looking at the "close with reset action". If the server or client is closing a connection with reset for more than 5 samples in a row, the test will be recalibrated.

If any of these scenarios are encountered, the algorithm will start the recalibration phase and adjust the target objective to a lower value. The test will then restart with the newly calculated value and start searching for a new lower max value that will not generate the mentioned conditions.

If the objective eventually stabilizes to a specific value until the end of the test, the algorithm will wait for the stage duration and then give a grade based on the average value obtained for 90% of the test.

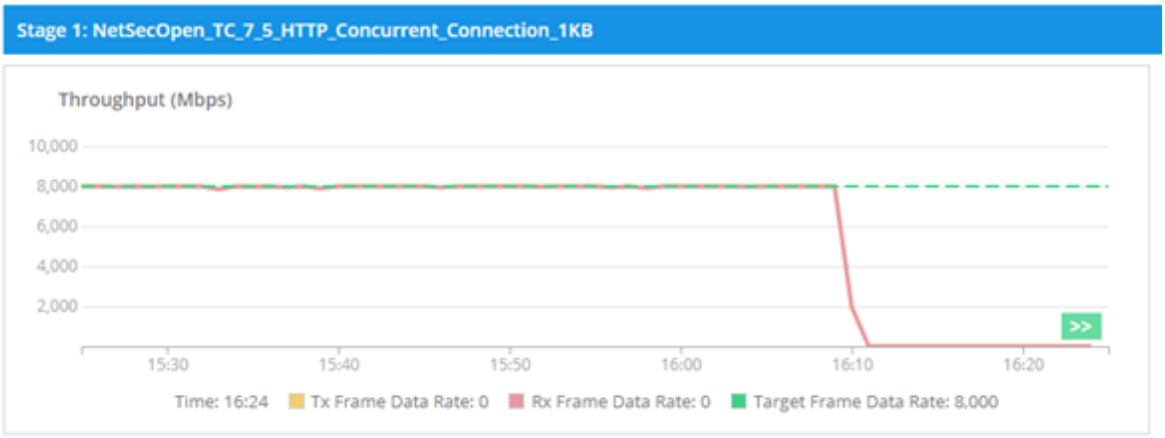
Note the following:

- The Ramp-down phase is not included in the algorithm requirements
- Some tests may not include the Ramp-up phase (or portions of it) in their requirements
- The Steady state is monitored to ensure that all of its requirements are met

Ramp-down phase

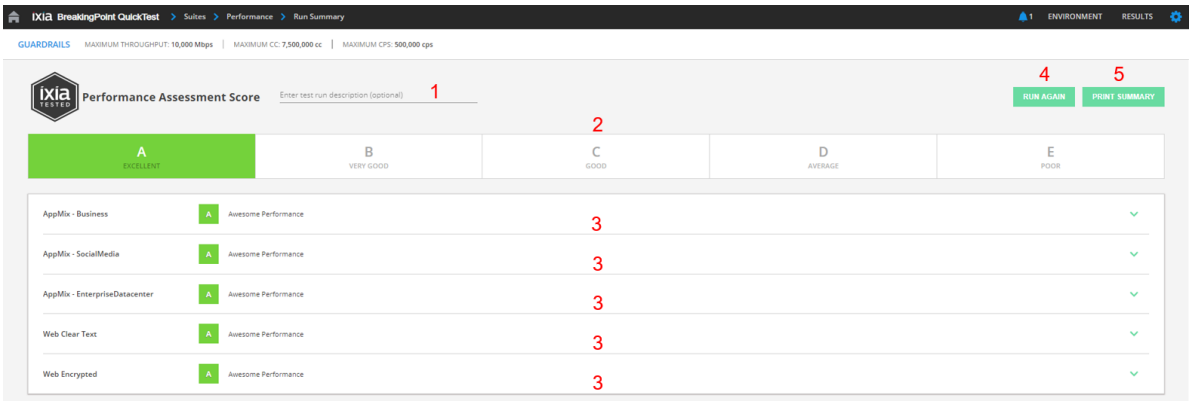
The ramp-down phase is where traffic flow is being stopped during the last stage of the test. The duration for this phase can vary based on how long it takes for all TCP sessions to end. This phase is not included in the grading algorithm, so any fail conditions encountered during this time will not be

considered in the final results. Also note that BPS QT will not stop the test to search for a more stable value.



Run summary

The Run Summary page appears after the Test Suite run has completed.



The Run Summary page contains the following elements:

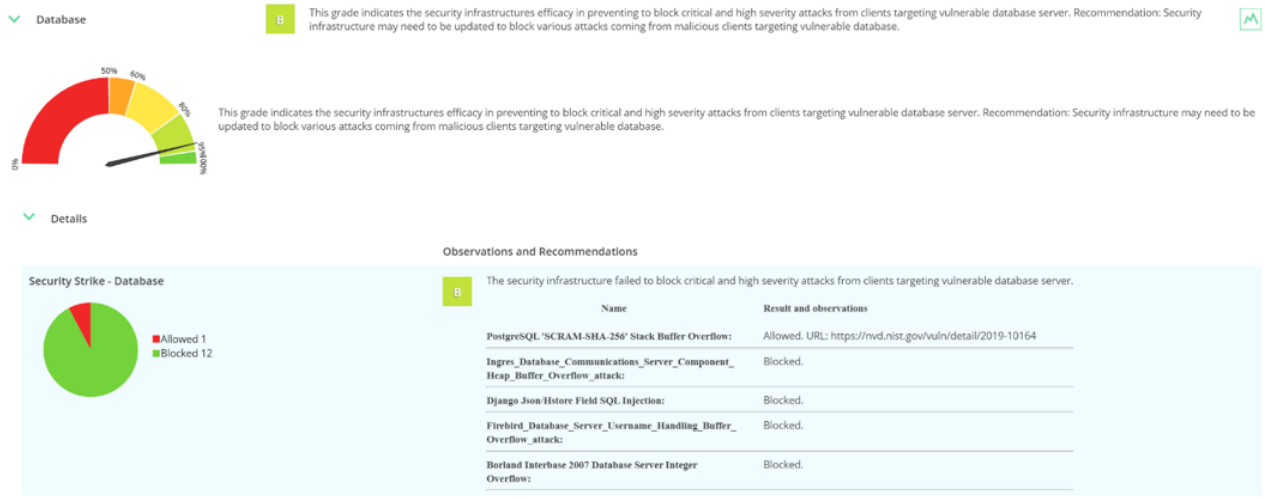
1	**Test Description** field: After the entire test has completed, you can optionally write a description of the test run which will be displayed in the **Description** field in the **Test Results** view.
2	**Grade** area: Displays the average grade for the entire suite run (based on its current configuration). The letter that is highlighted in a green box is the current grade.
3	**An interactive summary for each category**: The initial view shows each category grade. It also indicates which categories were skipped. See Category Summary Details for information about the interactive portion of this area.
4	**Run Again** button: Runs the test again with the same settings and test categories that were

	selected before the last run.
5	**Print Summary** button: Generates a downloadable test report for further reference.

Category Summary Details: The Category summary section can be expanded using the downward facing arrow towards the right side of the category as shown in the preceding image. Expanding the section exposes the entire timeline of the test for a post-test analysis. This section also contains the observations related to each stage run and briefly explains why the category got its grade.

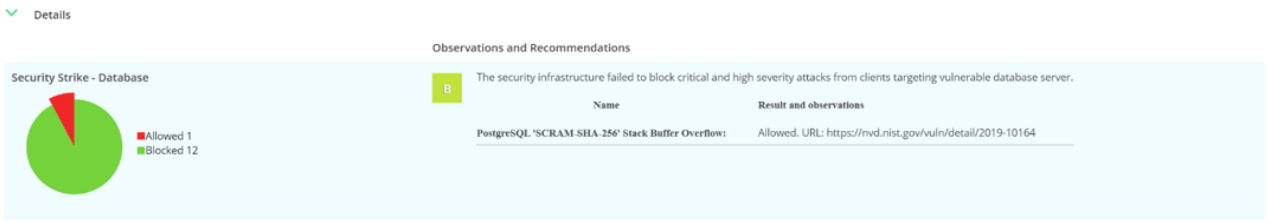
> You can toggle between the **Observations** and **Statistics** views by selecting the icons described below.

Select the **Observations** icon ( ) to display the **Observations view of a completed category** (shown in the following image). The needle indicator represents the highest value reached before test completion.

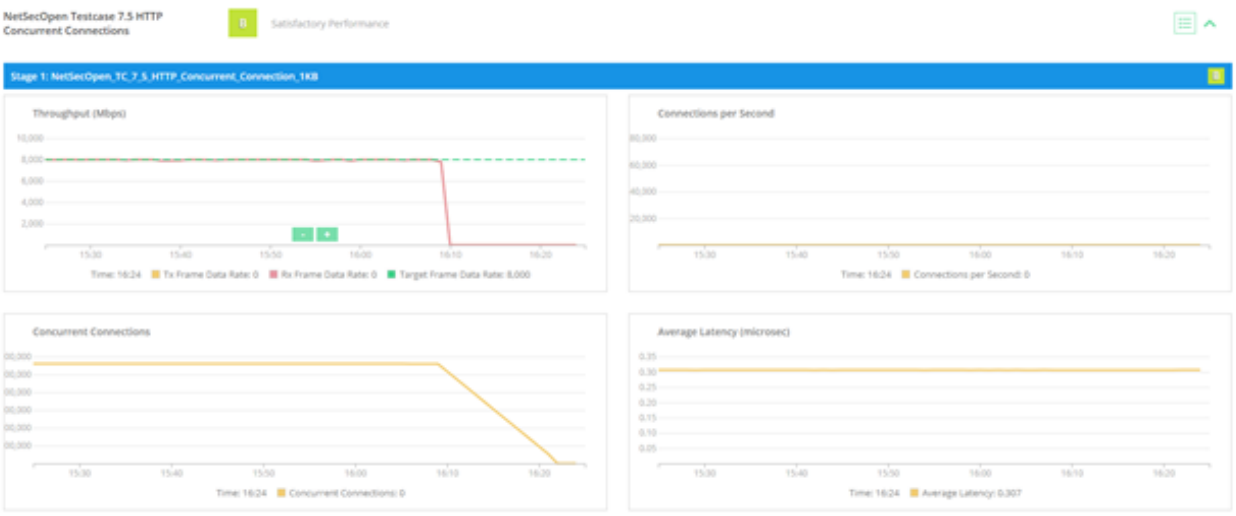


Only for Security suite

You can select the red portion of the pie chart to only view the allowed strikes or the green portion of the pie chart to only view the blocked strikes.



Select the **Statistics** icon ( )to display the **Statistics view of a completed category** (shown in the following image).



Tip: See Features for viewing statistical graphs for information on Statistics view options.

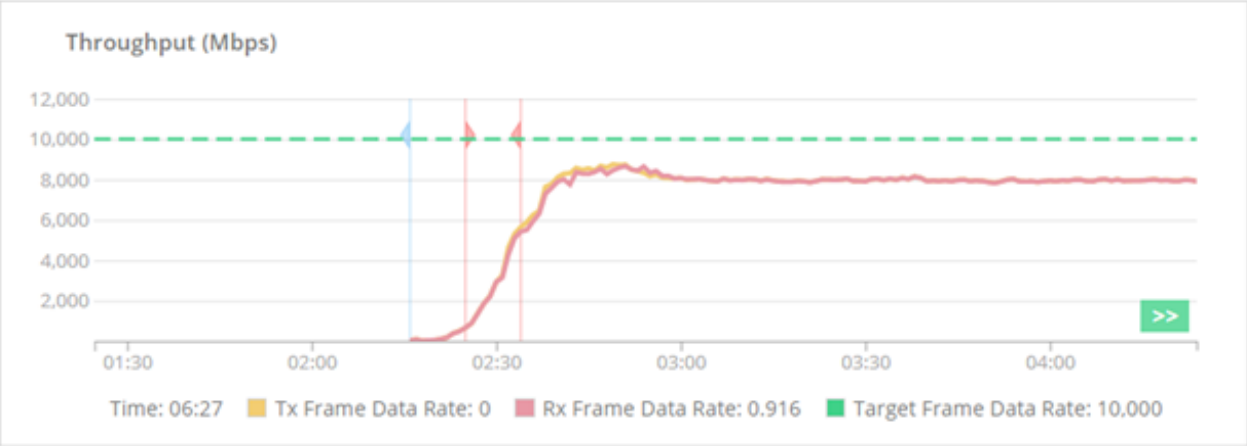
Statistics

There are five graphic statistic types produced by the test algorithm:

- Throughput (Mbps)
- Connections per Second
- Concurrent Connections
- Average Latency (microseconds)
- Connections Closed by Reset per Second

Throughput, Connections per second and Concurrent connections can be selective targets for some test stages. When throughput is a target objective, a green segmented line will be shown on the throughput graph indicating the limit that the algorithm is trying to achieve. When tests are aiming to determine other parameters like maximum concurrent connections or maximum connections per second, then the green line will be placed on the corresponding graph.

A **Throughput statistics graph** is shown in the image below.

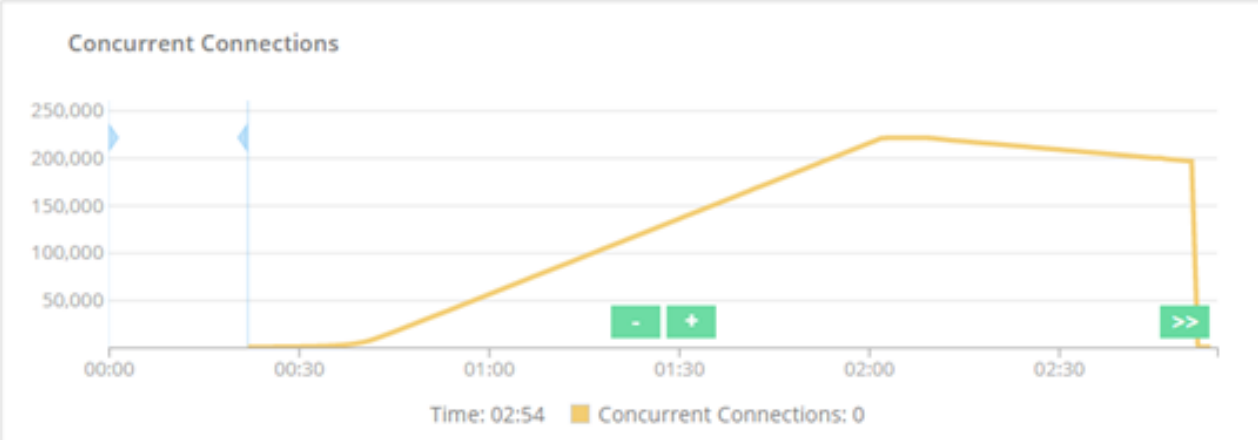


- **Time**: The timestamp
- **TX Frame Data Rate**: The rate at which the traffic is being sent
- **RX Frame Data Rate**: The rate at which the traffic is being received
- **Target Frame Data Rate**: The desired maximum rate to be achieved for grade A

Note: The target frame data rate might be higher than the TX Frame data rate due to the DUT throttling down our device using TCP mechanisms or because of loss.

A **Connections per Second statistics graph** is shown in the image below.

- **Time**: The timestamp
- **Established Rate**: The connections rate that has been established
- **Closed Rate**: The closed connections rate
- **Target Connections per Second**: The desired maximum rate to be achieved for a grade of "A"



- **Time**: The timestamp
- **Concurrent Connections**: The achieved concurrent connections count

Test run indicators

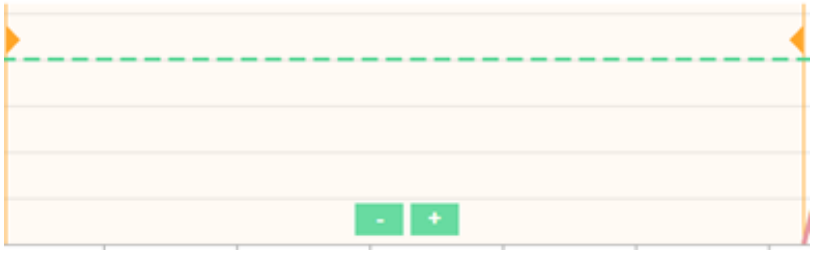
In a test suite run, along with the usual information about the rates and counts achieved, there are several additional indicators that provide useful information when it comes to interpreting statistics and recognizing the algorithm steps.

The image above shows many of these indicators and below is the description for multiple markers than can be displayed during the test suite run.

Note: Flag indicators are also accompanied by pop-up help to assist with understanding the current state of a test.

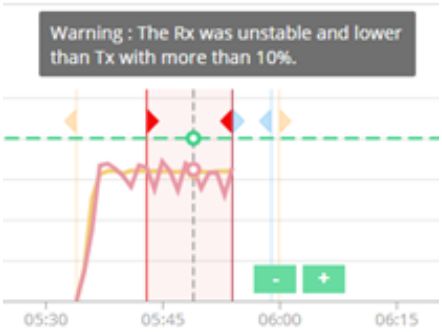
1. **Initializing/Aborting indicator** (blue): Indicates test initialization or test abort (if the algorithm decides not to continue).

2. **Calibrating flag** (orange): This indicator appears when the algorithm decides to try different values in order to determine the performance of the device.

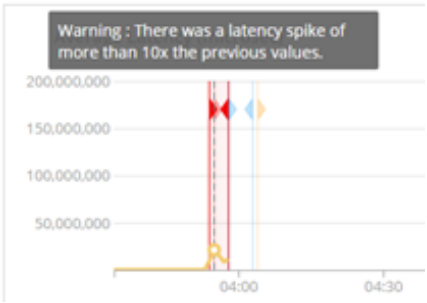


3. **Warning flags** (red): These flags can be of various types based on test conditions. Flags can influence the decisions made by the test algorithm to decrease the target objective in order to find a stable value suitable for a grade. Warning flags are accompanied by pop up messages that display when certain lossy conditions are met. The pop up messages appear in the exact location where the event took place. Some examples are shown below.

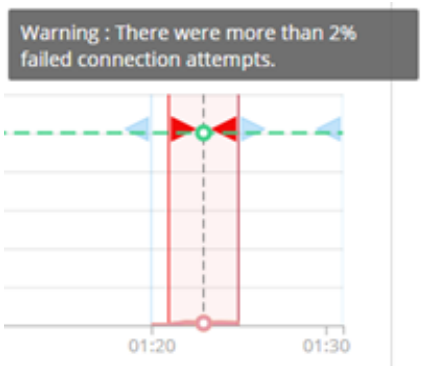
RX Throughput is lower than TX Throughput for a significant interval and with more than 10% loss



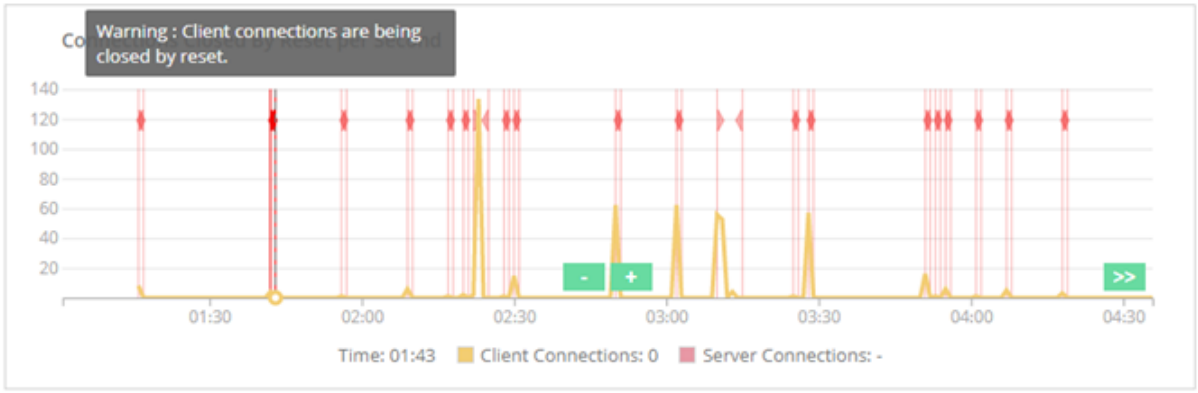
Average Latency instantly increased 10 times when compared to the previous value



More than 2 percent of the connection attempts have failed

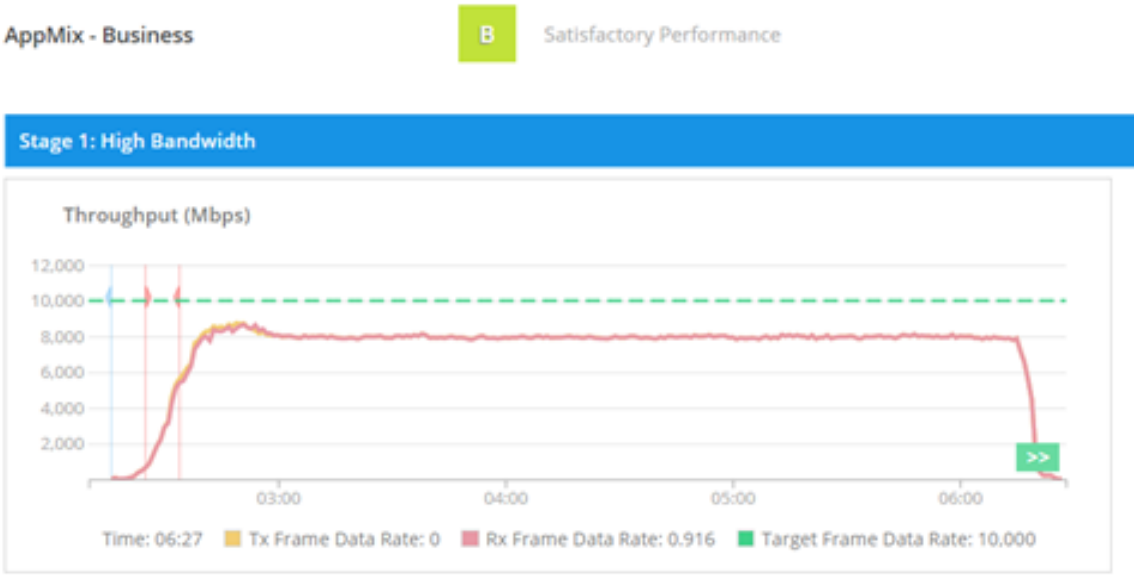


For the NetSecOpen suite, the algorithm is also looking at the "close with reset" action. If the server or client is closing a connection with reset for more than 5 samples in a row, the test will be recalibrated with 0.97 times of maximum CPS which respects the following condition: (tcpClientEstablishRate - tcpClientCloseRate) <= 0.05 * tcpClientCloseRate.



Test algorithm and grading

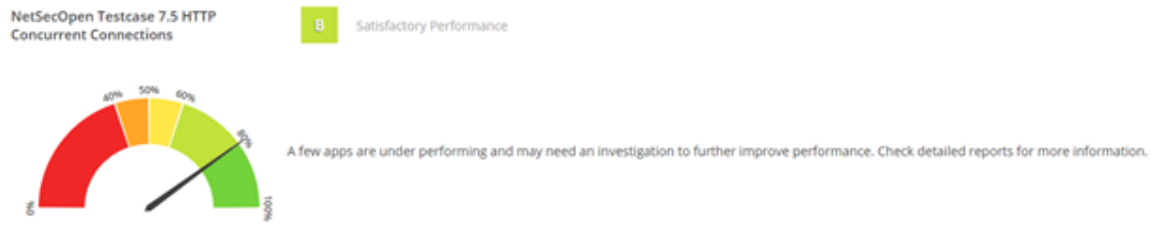
BPS QuickTest uses a custom algorithm to speed up the search for the target objective. The goal of the algorithm is to bring the desired metric to a stable state based on some quality constraints and then to give a grade to the obtained value.



The three candidate targets are:

- Throughput
- Concurrent Connections
- Connections per Second

BPS QuickTest has test suites that contain categories with all three variations of targets. Therefore, in successive stages, throughput, concurrent connections and connections per second can be targets and the algorithm will work to maximum them through a device under test and give a grade when compared to the desired target.



The grades and the criteria for each grade are listed below:

Grade A: 80 to 100% of the objective sustained for more than 90% of the steady state duration

Grade B: 60 to 80% of the objective sustained for more than 90% of the steady state duration

Grade C: 50 to 60% of the objective sustained for more than 90% of the steady state duration

Grade D: 40 to 50% of the objective sustained for more than 90% of the steady state duration

Grade E: 0 to 40% of the objective sustained for more than 90% of the steady state duration

After the initializing state, the algorithm will try to stabilize the objective (Throughput, Concurrent Connections and Connections per Second) to a value that does not generate the following:

- A per stage specified delta between Tx and Rx for several acceptable time intervals
- A per stage specified average latency spike. Example - for Performance suite, 10 times latency spike.
- A good averaged objective but highly unstable
- Layer 3 routing errors
- More than 5 server or client "close with reset" actions in a row

If any of these conditions are met, the algorithm will start the recalibration phase and adjust the target objective to a lower value. The test will then restart with the newly calculated value and start searching for a new lower max value that will not generate the mentioned conditions.

If the objective eventually stabilizes at a certain value until the end of the test, the algorithm will wait for the stage duration and give a grade based on the average value obtained for 90% of the test.

The ramp down phase is not included in the algorithm requirements. Some tests may not include the entire ramp up phase, or portions of the ramp up phase, in their requirements. But the steady state is also monitored for all of the requirements to be met.

Appendix A: Third-Party Components

BreakingPoint QuickTest may contain software that is licensed to Ixia by third parties.

To review the list of third party components, see the BreakingPoint QuickTest Third Party Software Licenses file which can be found in the same location (support.ixiacom.com) where you download BreakingPoint QuickTest software.

This page intentionally left blank.

INDEX

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