# BREAKINGPOINT QUICKTEST— TURN-KEY PERFORMANCE AND CYBERSECURITY TESTING

DATA SHEET

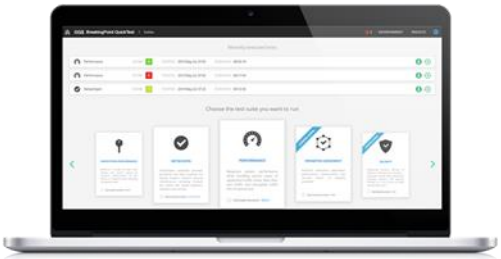
## PROBLEM: COMPLEXITY OF CYBERSECURITY TESTING

A properly conducted cybersecurity assessment provides details about network or device performance while handling traffic of various complexities — from basic Layer 2-3 to web to complex application mixes with and without various threat vectors. Similarly, a deep security-effectiveness assessment will need a combination of threat vectors and evasion techniques to accurately gauge an infrastructure's capability to detect, allow, or block different types of attacks. This validation is critical to ensuring a high-performing and secure network.

However, many organizations do not perform these assessments on a regular basis because the tools capable of such testing are too complex, network configuration changes are too frequent, or they lack staff with the knowledge required to analyze test results.

## HIGHLIGHTS

- Simplified user interface that enables execution of complex test cases in two to three clicks
- Pre-created problem-based test methodologies covering the top performance and security scenarios
- A self-stabilizing, goal-seeking algorithm to assess performance and security of a variety of infrastructures
- Expert post analysis of each test run that also provides actionable insights and recommendations based on the results
- Continuously updated suites that ensure the assessments are based on the current state of the internet
- Ability to use both BreakingPoint and BreakingPoint QuickTest from the same test platform



## SOLUTION: TURN-KEY TESTS DESIGNED TO ACCELERATE TESTING AND REDUCE LEARNING CURVE

BreakingPoint QuickTest simplifies application performance and security-effectiveness assessments by providing individual test methodologies based on the type of test needed. Test suites included or planned near-term include encryption performance, NetSecOPEN, system performance, perimeter assessment, and device security. 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. The test suites employ powerful stabilization and goal-seeking algorithms and expert analysis that ensure accurate assessment of a diverse set of devices and systems and deliver actionable insights after each test run.

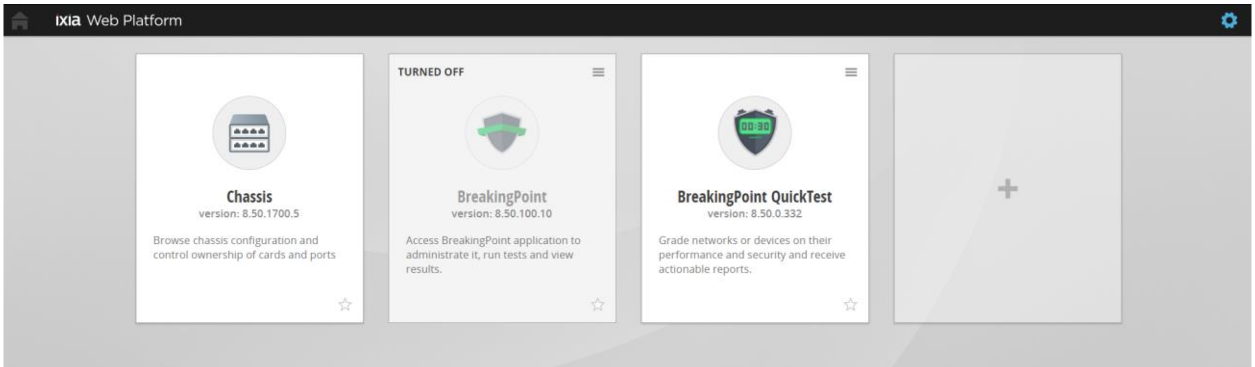
BreakingPoint QuickTest delivers all the power of our industry-leading BreakingPoint, enabling organizations to optimize the speed of their cybersecurity testing without compromise.

## KEY FEATURES:

- Pre-created, turn-key test suites designed to obfuscate complex testing
- Self-adjusting, self-learning, goal-seeking algorithms designed to work in varied environments
- Every assessment is followed by an actionable report/recommendation and observations
- Continuous updates with new suites and categories to cover newer scenarios

## PRODUCT CAPABILITIES

A simplified user interface ensures a short learning curve for both new and existing BreakingPoint customers. BreakingPoint QuickTest is available in the same web application framework (WAF) used to access the BreakingPoint Chassis.



Chassis
version: 8.50.1700.5
Browse chassis configuration and control ownership of cards and ports

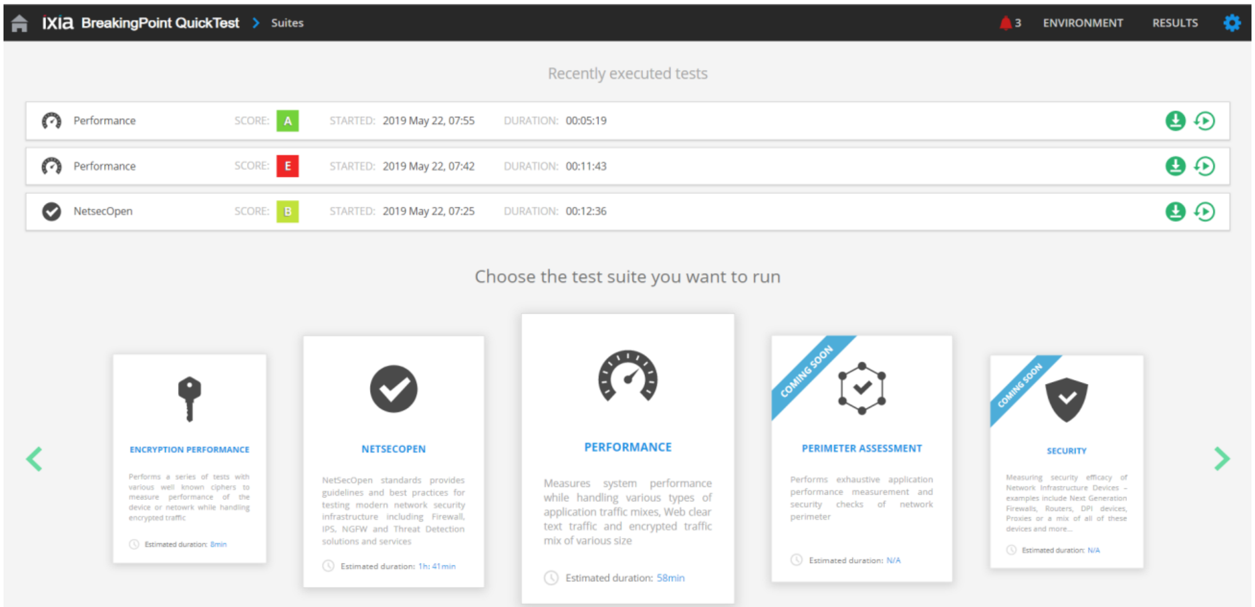
TURNED OFF
BreakingPoint
version: 8.50.100.10
Access BreakingPoint application to administrate it, run tests and view results.

BreakingPoint QuickTest
version: 8.50.0.332
Grade networks or devices on their performance and security and receive actionable reports.

BreakingPoint QuickTest login screen

## PRE-PACKAGED TRAFFIC PROFILES WITH ADJUSTABLE LOAD

Once logged in, users see their recently executed test runs and the available turn-key test methodology suites. The “Performance” test suite runs a series of web, encrypted-web, data center, social-media, and business application mix tests to characterize the performance aspects of any system or device under test (SUT or DUT). Similarly, the “Security” test suite will run various types of attacks like exploits, malware, malicious URL access, and attacks with different evasion strategies along with a steady stream of background traffic to accurately measure the security efficacy of a DUT/SUT in detecting and blocking attacks while maintaining seamless traffic continuity. The Guardrails button allows users to set the maximum traffic load for the test run.



Recently executed tests

| | | | |
|---|---|---|---|
| Performance | SCORE: A | STARTED: 2019 May 22, 07:55 | DURATION: 00:05:19 |
| Performance | SCORE: E | STARTED: 2019 May 22, 07:42 | DURATION: 00:11:43 |
| NetsecOpen | SCORE: B | STARTED: 2019 May 22, 07:25 | DURATION: 00:12:36 |

Choose the test suite you want to run

**ENCRYPTION PERFORMANCE**

Performs a series of tests with various well known ciphers to measure performance of the device or netowrk while handling encrypted traffic

Estimated duration: 8min

**NETSECOPEN**

NetSecOpen standards provides guidelines and best practices for testing modern network security infrastructure including Firewall, IPS, NGFW and Threat Detection solutions and services

Estimated duration: 1h: 41min

**PERFORMANCE**

Measures system performance while handling various types of application traffic mixes, Web clear text traffic and encrypted traffic mix of various size

Estimated duration: 58min

COMING SOON

**PERIMETER ASSESSMENT**

Performs exhaustive application performance measurement and security checks of network perimeter

Estimated duration: N/A

COMING SOON

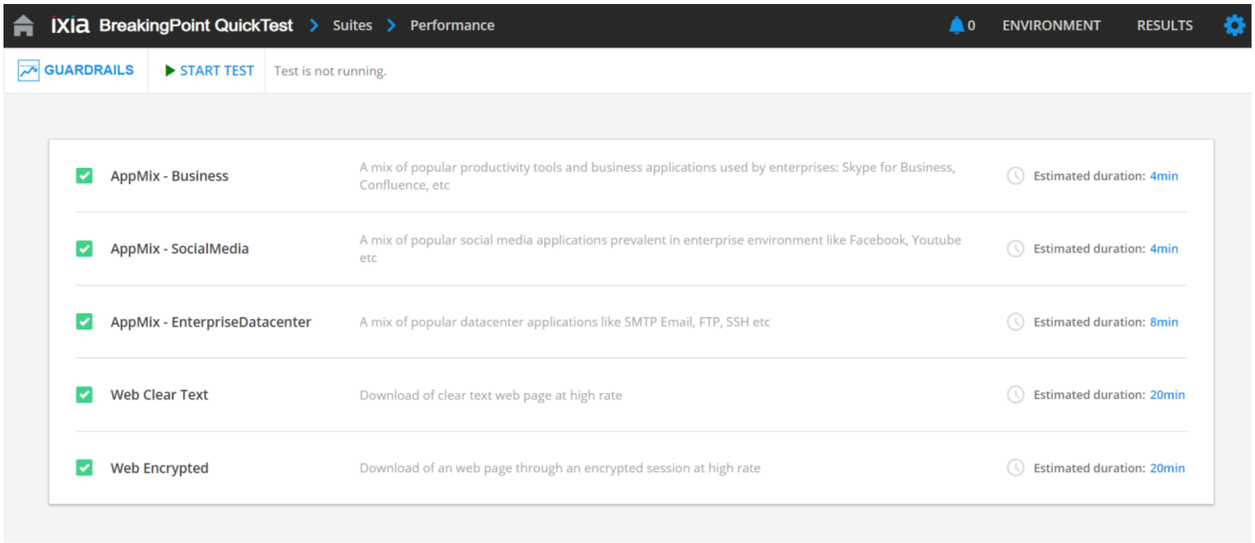
**SECURITY**

Measuring security efficacy of Network Infrastructure Devices – examples include Next Generation Firewalls, Routers, DPI devices, Proxies or a mix of all of these devices and more…

Estimated duration: N/A

**BreakingPoint QuickTest welcome screen showcasing recent test runs and available test suites**

Under each suite there are several categories of assessments that you can select or deselect. The carefully designed user interface (UI) ensures that most of the complex decision making has been packaged so you can run any of the pre-canned suites with minimal clicks. For example, the “Performance” suite uses several multifaceted application mixes, which are usually complex to configure, and time consuming to run and stabilize over various environments. However, with BreakingPoint QuickTest, you can qualify your datacenter performance with a click of a button and receive realistic performance numbers.



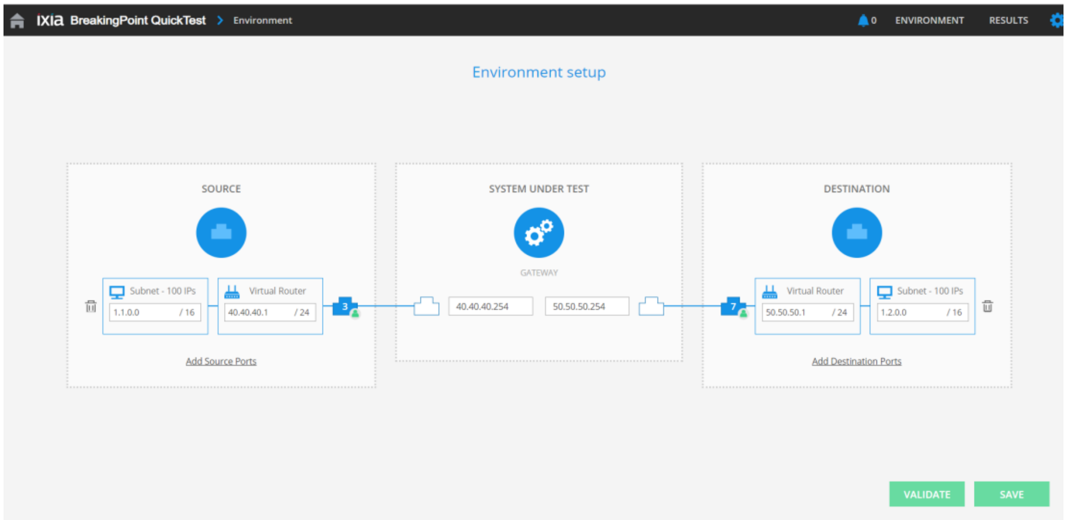
Test is not running.

| | | | |
|---|---|---|---|
| ☑ | AppMix - Business | A mix of popular productivity tools and business applications used by enterprises: Skype for Business, Confluence, etc | Estimated duration: 4min |
| ☑ | AppMix - SocialMedia | A mix of popular social media applications prevalent in enterprise environment like Facebook, Youtube etc | Estimated duration: 4min |
| ☑ | AppMix - EnterpriseDatacenter | A mix of popular datacenter applications like SMTP Email, FTP, SSH etc | Estimated duration: 8min |
| ☑ | Web Clear Text | Download of clear text web page at high rate | Estimated duration: 20min |
| ☑ | Web Encrypted | Download of an web page through an encrypted session at high rate | Estimated duration: 20min |

**Upon selecting any of the suites, users select the types of traffic to use in the test**

## ERROR-FREE ENVIRONMENT SETUP

Simplicity is the theme of BreakingPoint QuickTest, which is also reflected in the environment setup where the user can configure the IP addresses for the test tool simulating a client “source” and server “destination”, and the DUT gateway all in one page. The validate button validates port/traffic connectivity, further reducing debug cycles usually spent in figuring out traffic connectivity.



Subnet - 100 IPs: 1.1.0.0 / 16

Virtual Router: 40.40.40.1 / 24

40.40.40.254

50.50.50.254

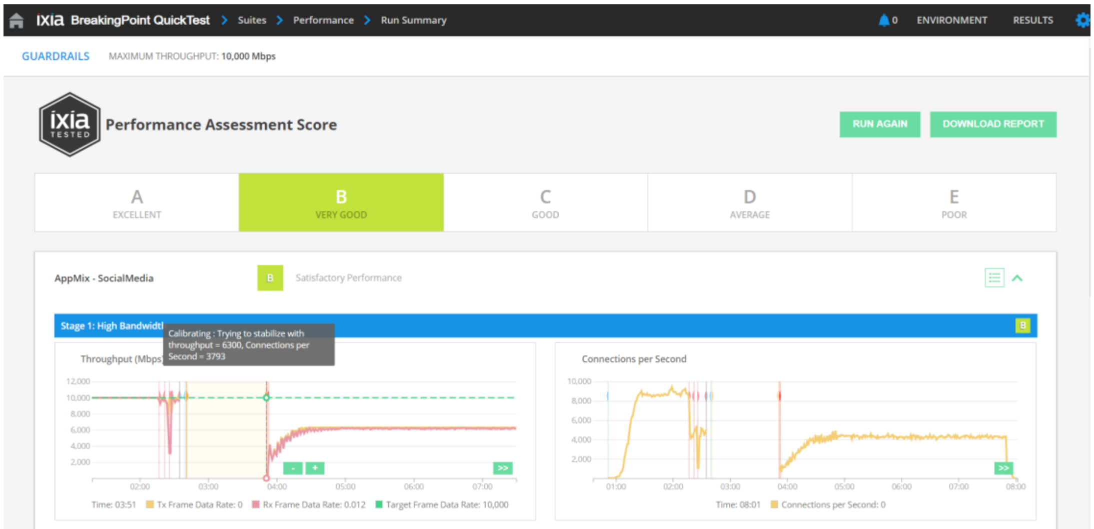
Virtual Router: 50.50.50.1 / 24

Subnet - 100 IPs: 1.2.0.0 / 16

A graphical form-fill simplifies how users connect the traffic generator test system to the SUT/DUT

## INTELLIGENT STABILIZATION/CALIBRATION

Each suite comes with a stabilization/calibration algorithm that handles a diverse setup of traffic conditions and finds the optimum performance/security results of these environments accurately. By continuously assessing for failure points and recalibrating the test, BreakingPoint QuickTest challenges the system or device under test to its breaking point, but then automatically adjusts the load to maintain the peak throughput for the test duration.



MAXIMUM THROUGHPUT: 10,000 Mbps

AppMix - SocialMedia B Satisfactory Performance

Calibrating : Trying to stabilize with throughput = 6300, Connections per Second = 3793

Time: 03:51 🟨 Tx Frame Data Rate: 0 🟥 Rx Frame Data Rate: 0.012 🟩 Target Frame Data Rate: 10,000

Time: 08:01 🟨 Connections per Second: 0

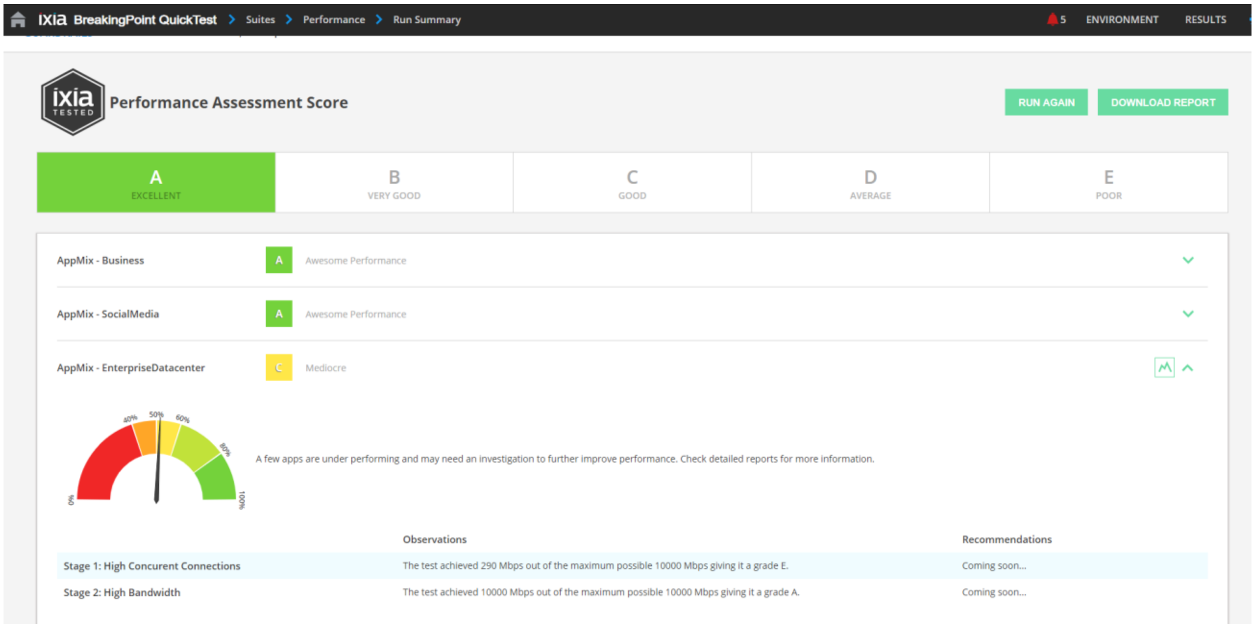
BreakingPoint QuickTest runs showcasing the stabilization/callibration algorithms

## REPORTS AND ACTIONABLE PERFORMANCE SCORES

Once the test concludes, the report and results have actionable grades and insights that can help users:

1. Understand the “real” performance of their SUT/DUT
2. Take corrective actions based on results and the actionable insights provided
3. Evaluate the impacts of change management by comparing before/after scenarios
4. Gain more flexibility beyond that offered in BreakingPoint QuickTest by selecting the option to move to BreakingPoint classic for features like our rich network neighborhood, configuration and editing of application mixes, and creation of customized tests

The test reports have a high-level synopsis that provides overall scores for the entire suite based on the weighted average of each of the categories and scores for each individual category so users can get more in-depth insights. Apart from scores, the reports also have observations and recommendations.

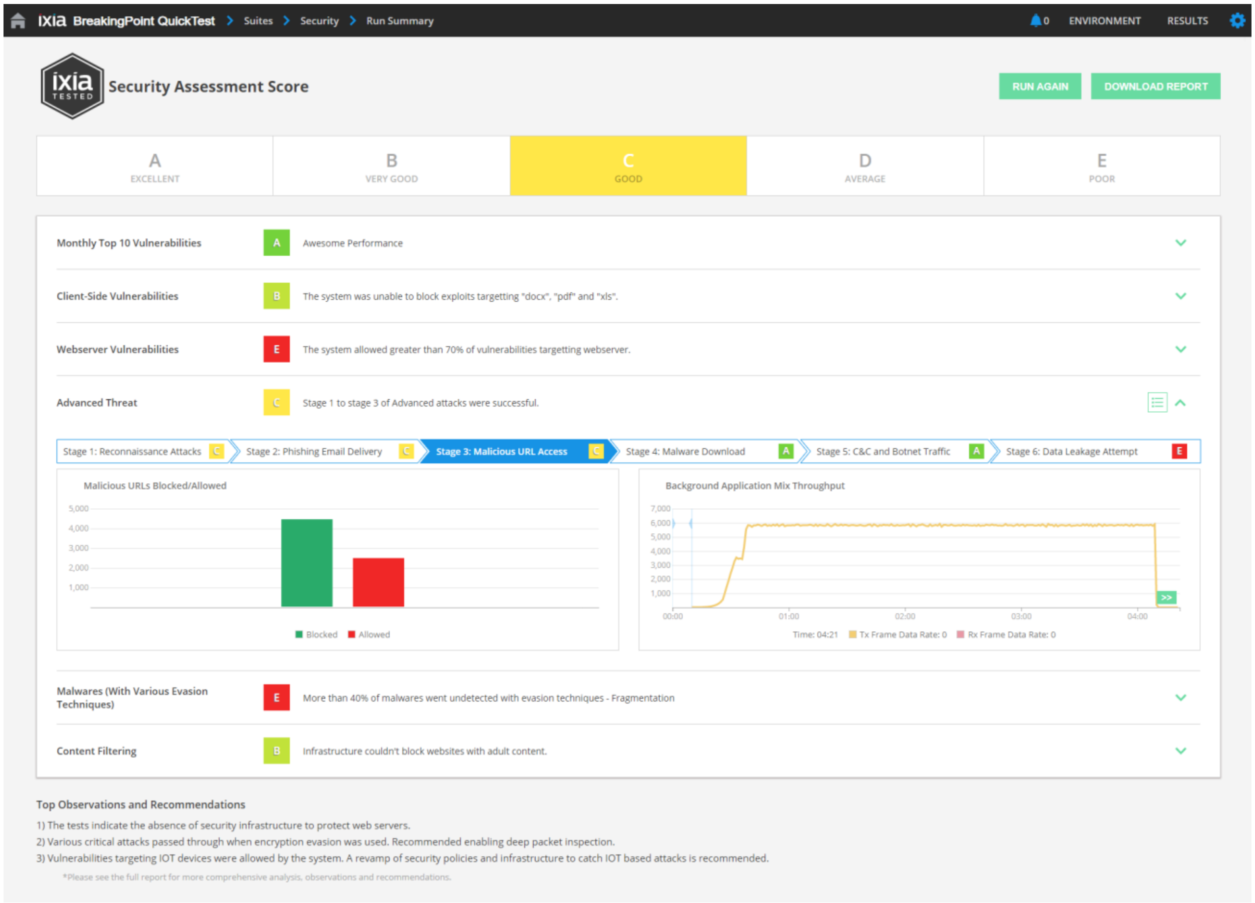


| AppMix | Grade | |
|---|---|---|
| AppMix - Business | A | Awesome Performance |
| AppMix - SocialMedia | A | Awesome Performance |
| AppMix - EnterpriseDatacenter | C | Mediocre |

A few apps are under performing and may need an investigation to further improve performance. Check detailed reports for more information.

| | Observations | Recommendations |
|---|---|---|
| Stage 1: High Concurent Connections | The test achieved 290 Mbps out of the maximum possible 10000 Mbps giving it a grade E. | Coming soon... |
| Stage 2: High Bandwidth | The test achieved 10000 Mbps out of the maximum possible 10000 Mbps giving it a grade A. | Coming soon... |

**BreakingPoint QuickTest Performance Assessment results and reports showing grade of the suite and individual categories**



Security Assessment Score

| A | B | C | D | E |
|---|---|---|---|---|
| EXCELLENT | VERY GOOD | GOOD | AVERAGE | POOR |

| | | |
|---|---|---|
| Monthly Top 10 Vulnerabilities | A | Awesome Performance |
| Client-Side Vulnerabilities | B | The system was unable to block exploits targetting "docx", "pdf" and "xls". |
| Webserver Vulnerabilities | E | The system allowed greater than 70% of vulnerabilities targetting webserver. |
| Advanced Threat | C | Stage 1 to stage 3 of Advanced attacks were successful. |
| Malwares (With Various Evasion Techniques) | E | More than 40% of malwares went undetected with evasion techniques - Fragmentation |
| Content Filtering | B | Infrastructure couldn't block websites with adult content. |

| Stage 1: Reconnaissance Attacks | Stage 2: Phishing Email Delivery | Stage 3: Malicious URL Access | Stage 4: Malware Download | Stage 5: C&C and Botnet Traffic | Stage 6: Data Leakage Attempt |
|---|---|---|---|---|---|
| C | C | C | A | A | E |

Top Observations and Recommendations

1) The tests indicate the absence of security infrastructure to protect web servers.
2) Various critical attacks passed through when encryption evasion was used. Recommended enabling deep packet inspection.
3) Vulnerabilities targeting IOT devices were allowed by the system. A revamp of security policies and infrastructure to catch IOT based attacks is recommended.

*Please see the full report for more comprehensive analysis, observations and recommendations.

BreakingPoint QuickTest Security Assessment results and reports showing grade of the suite and individual categories

## SPECIFICATIONS

| SUITE | CATEGORIES |
|---|---|
| **Performance** | • **Web-ClearText – Mix Traffic Performance:** Download and upload of a mix of small to large clear text web pages<br>• **Web Encrypted – Mix Traffic Performance:** Download and upload of a mix of small to large web pages that are encrypted with popular ciphers<br>• **AppMix – Enterprise Datacenter:** A mix of popular datacenter applications; includes Oracle, SMB, Citrix, HTTPS<br>• **AppMix – Business:** A mix of popular enterprise productivity tools and business applications; includes Office 365, Salesforce, Webex<br>• **AppMix – SocialMedia:** A mix of popular social media applications prevalent in enterprise environments; includes Twitter, Facebook, YouTube |
| **Security*** | • **Security – Malware:** A collection of the latest malwares that spans different applications, operating systems and hardware types<br>• **Security – Malware (with various evasion techniques):** A collection of the latest malware that spans different applications, operating systems and hardware types under different types of clever evasions<br>• **Security – Exploits (high, medium and low severity):** A collection of different-severity vulnerabilities that are designed to exploit network-based protocols grouped under different CVE scores<br>• **Security – Exploits (with various evasion techniques):** A collection of high severity vulnerabilities that are designed to exploit network-based protocols grouped under different CVE scores; this time sent with different kinds of evasion techniques<br>• **Security – DOS:** A collection of DDoS vulnerabilities<br>• **Security – Application and Volumetric DDoS:** A collection of DoS and DDoS attacks like SYN-Flood, UDP Flood, Slow Loris, RuDY, NTP Flood<br>• **Security – Advanced Threats:** A series of threats in sequence to create an advanced persistent threat (APT)-like scenario |

| SUITE | CATEGORIES |
|---|---|
| **NetSecOPEN** | • **Throughput Performance with NetSecOPEN Traffic Mix:** Using NetSecOPEN traffic mix, determines the maximum sustainable throughput performance supported by the DUT/SUT<br>• **TCP/HTTP Connections Per Second:** Using HTTP traffic, determines the maximum sustainable TCP connection establishment rate supported by the DUT/SUT under different throughput load conditions<br>• **HTTP Transaction per Second:** Using HTTP 1.1 traffic, determines the maximum sustainable HTTP transactions per second supported by the DUT/SUT under different throughput load conditions<br>• **TCP/HTTP Transaction Latency:** Using HTTP traffic, determines the average HTTP transaction latency when DUT is running with sustainable HTTP transactions per second supported by the DUT/SUT under different HTTP response object sizes<br>• **HTTP Throughput:** Determine the throughput for HTTP transactions varying the HTTP response object size<br>• **Concurrent TCP/HTTP Connection Capacity:** Determines the maximum number of concurrent TCP connections that DUT/ SUT sustains when using HTTP traffic<br>• **TCP/HTTPS Connections per second:** Using HTTPS traffic, determines the maximum sustainable SSL/TLS session establishment rate supported by the DUT/SUT under different throughput load conditions<br>• **HTTPS Transaction per Second:** Using HTTPS traffic, determines the maximum sustainable HTTPS transactions per second supported by the DUT/SUT under different throughput load conditions<br>• **HTTPS Transaction Latency:** Using HTTPS traffic, determines the average HTTPS transaction latency when DUT is running with sustainable HTTPS transactions per second supported by the DUT/SUT under different HTTPS response object size<br>• **HTTPS Throughput:** Determines the throughput for HTTPS transactions varying the HTTPS response object size<br>• **Concurrent TCP/HTTPS Connection Capacity:** Determines the maximum number of concurrent TCP connections that DUT/SUT sustains when using HTTPS traffic |

| SUITE | CATEGORIES |
|---|---|
| **Encryption Performance*** | • **Cipher RSA 4K key size – CPS performance:** Max simultaneous sessions per second performance test using involving small file transfer using the TLS 1.2-RSA public key exchange with a public key size of 4K for encryption<br>• **Cipher RSA 2K key size – CPS performance:** Max simultaneous sessions per second performance test using involving small file transfer using the TLS 1.2-RSA public key exchange with a public key size of 2K for encryption<br>• **Cipher ECDHE-RSA 256-P curve size – CPS performance:** Max simultaneous sessions per second performance test involving small file transfer using the TLS 1.2-ECDHE-RSA public key exchange with a 256-P curve for encryption<br>• **Cipher ECDHE-RSA 512-P curve size – CPS performance:** Max simultaneous sessions per second performance test involving small file transfer using the TLS 1.2-ECDHE-RSA public key exchange with a 512-P curve for encryption<br>• **Cipher ECDHE-ECDSA 256-P curve size – CPS performance:** Max simultaneous sessions per second performance test involving small file transfer using the TLS 1.2-ECDHE-ECDSA public key exchange with a 256-P curve for encryption<br>• **Cipher ECDHE- ECDSA 512-P curve size – CPS performance:** Max simultaneous sessions per second performance test involving small file transfer using the TLS 1.2-ECDHE-ECDSA public key exchange with a 512-P curve for encryption<br>• **Cipher TLS1_3 EC CPS Performance:** Max simultaneous sessions per second performance test with TLS 1.3 EC cyphers<br>• **Block Cipher AES128-CBC – Throughput Performance:** Max throughput performance involving large file transfer with TLS 1.2 and AES128-CBC as the block cipher for encryption<br>• **Block Cipher AES128-GCM – Throughput Performance:** Max throughput performance test involving large file transfer with TLS 1.2 and AES128-GCM as the block cipher for encryption<br>• **Block Cipher AES256-CBC – Throughput Performance:** Max throughput performance test involving large file transfer with TLS 1.2 and AES256-CBC as the block cipher for encryption<br>• **Block Cipher AES256-GCM – Throughput Performance:** Max throughput performance test involving large file transfer with TLS 1.2 and AES256-CBC as the block cipher for encryption<br>• **Block Cipher Cha-Cha-Poly – Throughput Performance:** Max throughput performance test involving large file transfer with TLS 1.2 and cha-cha-poly as the block cipher for encryption |

| SUITE | CATEGORIES |
|---|---|
| **DDoS*** | • **Botnet Mix**<br>• **DDoS – SYN Flood**<br>• **DDoS – SYN FIN**<br>• **DDoS – Christmas Tree**<br>• **DDoS – UDP Flood**<br>• **DDoS – Application DNS**<br>• **DDoS – Application NTP**<br>• **DDoS – Slow Webpage Upload**<br>• **DDoS – Slow webpage download**<br>• **DDoS – HTTP Request Flood**<br>• **DDoS – HTTP Upload Flood** |
| **Perimeter Security*** | • **Web-ClearText – Mix Traffic Performance:** Download and upload of a mix of small to large clear text web pages<br>• **Web Encrypted – Mix Traffic Performance**: Download and upload of a mix of small to large web pages that are encrypted with popular ciphers<br>• **AppMix – Enterprise Datacenter:** A mix of popular data center applications; includes Oracle, SMB, Citrix, HTTPS<br>• **AppMix – Business**: A mix of popular enterprise productivity tools and business applications; includes Office 365, Salesforce, Webex<br>• **Security – Malwares:** A collection of latest malwares that spans different applications, operating systems and hardware types.<br>• **Security – Exploits:** A collection of high severity vulnerabilities that are designed to exploit network-based protocols.<br>• **Security – DOS:** A collection of denial of service vulnerabilities<br>• **Security – Application and Volumetric DDoS:** A collection of DOS and DDoS attacks like SYN-Flood, UDP Flood, Slow Loris, RuDY, NTP Flood<br>• **Security – Malicious URLs:** A series of attacks emulating clients accessing URLs<br>• **Security – Advanced Threats:** A series of threats in sequence to create an APT like scenario |

*Not all categories or suites are available in the first release but will be  available as part of incremental updates.

## Learn more at: www.ixiacom.com

For more information on Ixia products, applications, or services,
please contact your local Ixia or Keysight Technologies office.
The complete list is available at: www.ixiacom.com/contact/info

I