



NSS LABS TEST PACK

Next Generation Firewall

User Guide

v1.0

Test Pack Name:	Ixia Test Pack by NSS Labs – Next Generation Firewall 1.0
Test Pack Creation Date:	June 24, 2015
Test Pack Based On:	NSS Next Generation Firewall: Test Methodology v6.0
BreakingPoint Details:	Ixia BreakingPoint PerfectStorm software version 3.4.0 Product Build 230019, (ATI 231337)

Table of Contents

1	Introduction	4
1.1	The Need for Ixia Test Packs by NSS Labs	4
1.2	About This Test Pack	4
1.3	Additional Help and Documentation	5
1.4	Document Assumptions	6
2	Test Pack Licensing	7
3	Using Ixia Test Pack by NSS Labs – Next Generation Firewall 1.0	9
3.1	Scope of this Test Pack	9
3.1.1	<i>Security Effectiveness Testing Metrics</i>	9
3.1.2	<i>Performance Testing Metrics</i>	9
3.1.3	<i>Stability and Reliability Testing Metrics</i>	9
3.2	Test Environment	11
3.2.1	<i>Test Architecture</i>	11
3.2.2	<i>Test Pack Configuration</i>	11
4	Security Effectiveness	12
4.1	Next Generation Firewall Policy Functionality Testing	12
4.2	Baseline Policy	12
4.3	Simple Policy	13
4.4	Complex Policies	14
4.4.1	<i>Multiple Policy Configuration Testing</i>	14
4.4.2	<i>Static NAT (Network Address Translation)</i>	15
4.4.3	<i>Dynamic/Hide NAT (Network Address Translation)</i>	16
4.5	Denial of Service and Evasion Testing	17
4.5.1	<i>SYN Flood</i>	17
4.5.2	<i>IP Address Spoofing</i>	18
4.5.3	<i>TCP Split Handshake</i>	19
4.6	Exploits	20
5	Performance	22
5.1	Raw Performance Testing with UDP Traffic and Latency Testing	22
5.1.1	<i>Example: Interpreting Performance Results – Throughput (Mbps)</i>	24
5.1.2	<i>Example: Interpreting Performance Results – Latency (milliseconds)</i>	25
5.2	Maximum Capacity (Per Second) Testing	26
5.2.1	<i>Example - Gathering and Interpreting Performance Results</i>	27
5.3	Maximum Capacity Testing	29
5.4	Maximum HTTP Capacity Testing	32
5.4.1	<i>Testing with Delay</i>	34
5.5	Real-World Traffic Mix Performance	35
6	Stability and Reliability Testing	37
6.1	Stability and Security - Attack Leakage	37

6.2	Protocol Fuzzing and Mutation.....	39
7	Best Practices	40
8	Frequently Asked Questions.....	41
9	Appendix A: Change Log.....	46
10	Appendix B: About This Test.....	47
11	Appendix C: Combined Scorecard	48

1 Introduction

1.1 The Need for Ixia Test Packs by NSS Labs

The Ixia/NSS Labs test packs combine the testing expertise of two of the largest security and network testing companies in the industry. Use of these test packs provides four distinct advantages:

- **Industry Standard Testing** – Because test packs are based on the same methodology used by NSS in evaluating products from vendors across the industry, you are assured that you are testing on a level playing field. This allows you to determine precisely how your equipment performs not only against previous versions, but also across the rest of the industry. The result is improved decision making during evaluation and capacity planning.
- **Repeatability** – The use of test packs ensures that tests are run in an identical manner during each test iteration. All changes made to the device under test (DUT) can be validated against previous results, and can be compared to NSS' own group tests. This eliminates uncertainty around whether problems have been resolved, and results in fewer variables to troubleshoot in the event of a questionable test. In addition, because the tests are locked to prevent inadvertent tampering, you can be confident no changes have occurred between test iterations.
- **Reduced Test Development Time** – The use of test packs allows you to focus on the testing, not the test development. Not only is test development eliminated, it is no longer necessary to validate, refine, recode or retest against known situations. This can be a dramatic time savings in some instances.
- **Opportunity for Education** – The test packs are set up to provide learning opportunities for both junior and senior testing staff, enabling cross training opportunities for testing staff more accustomed to singularly traditional network stress testing and capacity planning.

1.2 About This Test Pack

Performance and long-term stability are critical for an in-line device such as a next generation firewall (NGFW), as failure can produce network outages or place assets under malicious threat.

The goal of this document is to enable an understanding of how to properly utilize Ixia BreakingPoint traffic generation tools in combination with the Next Generation Firewall Test Pack in order to effectively facilitate stress, bandwidth, and network performance testing of a NGFW within a security context. A next generation firewall is required to remain operational and stable throughout these tests and to block 100% of any malicious traffic presented while not falsely alerting on legitimate traffic (also known as false positives).

This test pack combines the deep expertise of NSS Labs security engineers with the industry's most robust testing hardware and software from Ixia to provide the most comprehensive and rigorous firewall test available today. This test pack has been created to assist network and security professionals when configuring and managing next generation firewalls.

The tests provided within this test pack are based on an actual *NSS Lab Next Generation Firewall Test Methodology*. The specific test methodology version is listed on the front page of this report and in Appendix B: About This Test. To aid in scoring and recording results for this test methodology version, a detailed product scorecard is included in Appendix C: Combined Scorecard.

Use with any deviation from the combination referenced within this report may lead to results that vary from what is documented within this test pack.



Note: Although the test pack is an important tool for evaluating security devices, it is not a substitute for a private consulting engagement with NSS security professionals. Contact NSS at info@nsslabs.com to set up an appointment.

1.3 Additional Help and Documentation

This test pack documentation is intended to assist users when running the specific Ixia Test Pack by NSS Labs – Next Generation Firewall tests. Inline documentation is available for help with specific BreakingPoint environment needs. This documentation can be accessed as needed by selecting the “Help” icon or the “Help” menu at the top of the main BreakingPoint user interface (select “Documentation” and then “BPS Control Center”). See Figure 1.

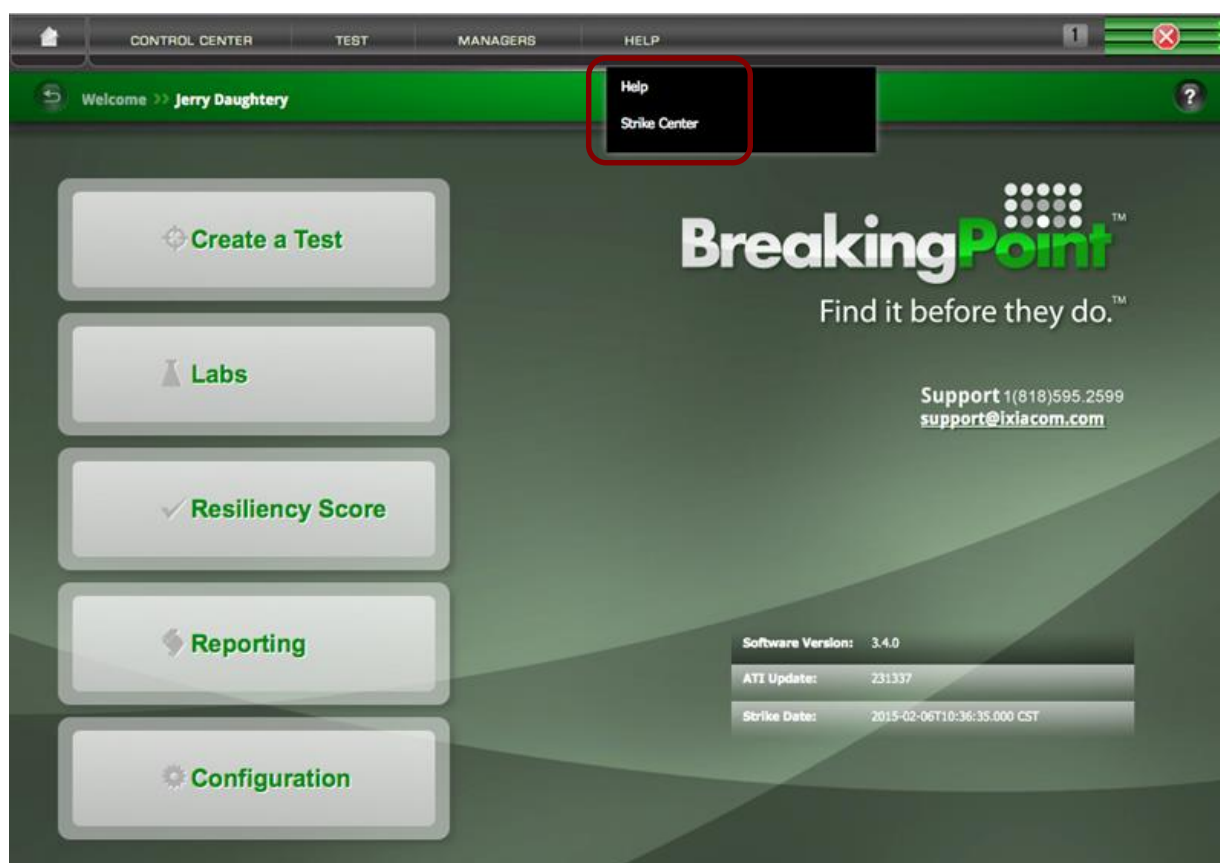


Figure 1 – Accessing BreakingPoint Help

Figure 2 illustrates BreakingPoint guides and documentation options. For further details, reference the BreakingPoint documentation.

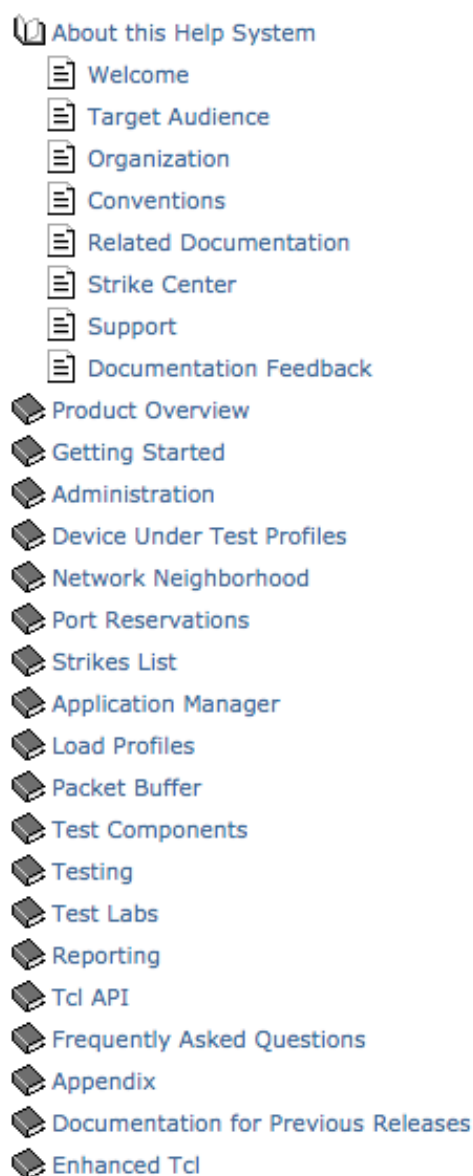


Figure 2 – BreakingPoint 3.4 Help Menu

1.4 Document Assumptions

It is assumed that the test engineer has a moderate-to-intermediate level of understanding of the use of an Ixia BreakingPoint and PerfectStorm appliance. It is also assumed the test engineer has a basic-to-moderate understanding of firewall configuration and usage.

It is beyond the scope of this document to outline all steps required to implement the test. Please contact the appropriate sales team for additional insight if needed.

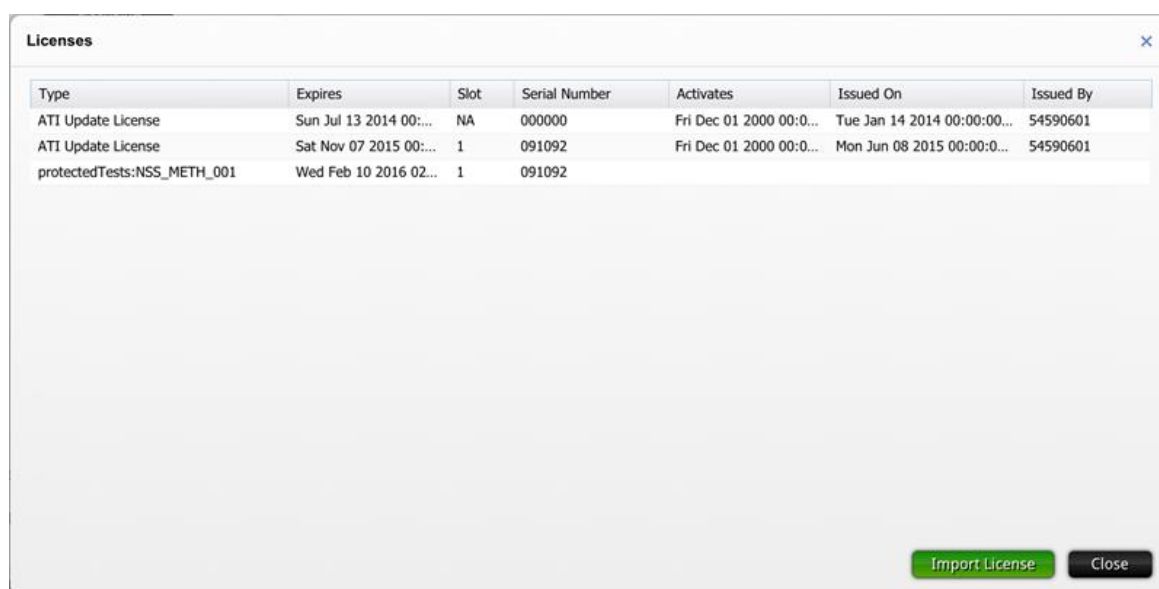
2 Test Pack Licensing

In order to import and run this Ixia Test Pack, you must first obtain the appropriate license file from the Ixia sales representative. The license files are configured for your specific device and the license number is tied to the specific PerfectStorm blade from which the test pack will be run. This license will be required when the test pack is loaded onto the selected device. If you have any questions about the license feature, contact the Ixia support representative. For information about using the BreakingPoint application, see the Ixia PerfectStorm Fusion User Guide.

To import the BreakingPoint license, perform the following steps:

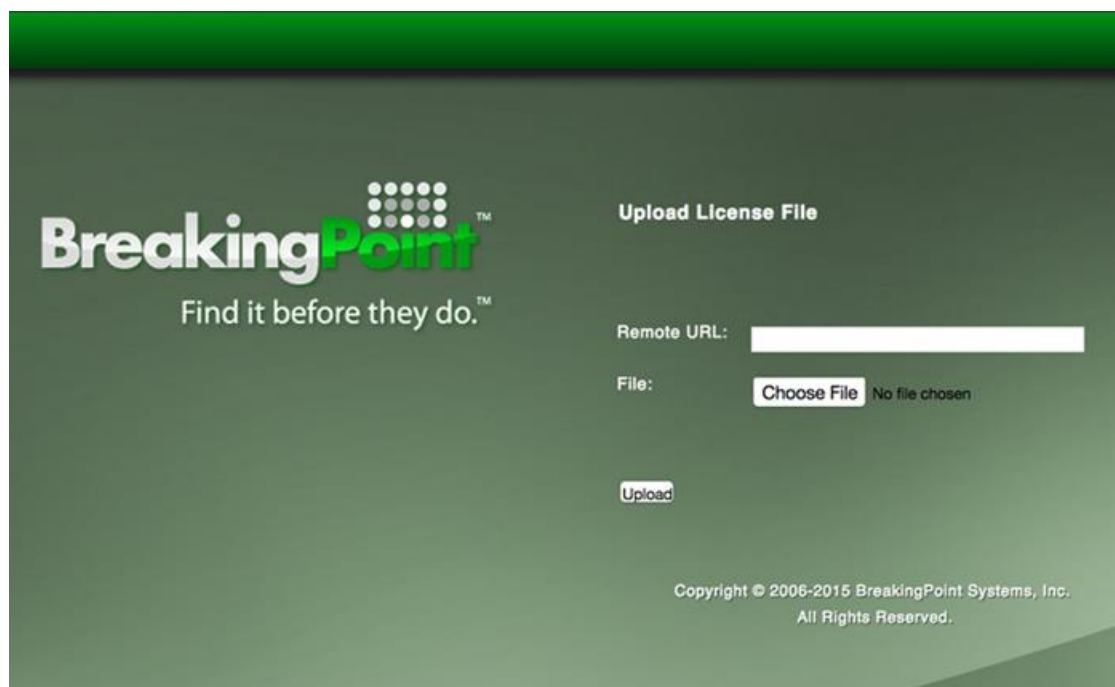
1. On the BreakingPoint home screen, select **Control Center > Administration > Licensing**.

The **Licenses** dialog box opens.



2. Click **Import License**.

The BreakingPoint application displays the **Upload License File** screen.



3. Click **Choose File**, then browse to the location of the **.lic** file for the test pack.
4. Select the file name and click **Upload**.

BreakingPoint briefly displays a message stating that the license file successfully uploaded, and the new license is visible in the **Licenses** dialog box.

Licenses						
Type	Expires	Slot	Serial Number	Activates	Issued On	Issued By
ATI Update License	Sun Jul 13 2014 00:...	NA	000000	Fri Dec 01 2000 00:0...	Tue Jan 14 2014 00:00:00...	54590601
ATI Update License	Sat Nov 07 2015 00:...	1	091092	Fri Dec 01 2000 00:0...	Mon Jun 08 2015 00:00:00...	54590601
protectedTests:NSS_METH_001	Wed Feb 10 2016 02:...	1	091092			
protectedTests:NSS_METH_001	Wed Feb 10 2016 02:...	1	091092			
protectedTests:NSS_METH_002	Fri Feb 26 2016 02:0...	1	091092			

Import License Close

3 Using Ixia Test Pack by NSS Labs – Next Generation Firewall 1.0

3.1 Scope of this Test Pack

NSS Labs' test packs are designed to address the challenges faced by IT professionals in selecting and managing security products. The scope of this test pack includes:

- Security effectiveness
- Performance
- Stability and reliability

This document outlines the specific test names and parameters for each of the pre-built NSS tests that are provided as part of this test pack. Information within each of the pre-built NSS tests includes running, scoring, and evaluating the device under test (DUT).

3.1.1 Security Effectiveness Testing Metrics

An array of pre-built security effectiveness tests are bundled within this test pack, including:

- Baseline Policy
- Simple Policies
- Complex Policies
- Static NAT (Network Address Translation)
- Dynamic/Hide NAT (Network Address Translation)
- SYN Flood
- IP Address Spoofing
- TCP Split Handshake
- Exploits

3.1.2 Performance Testing Metrics

An array of pre-built performance tests are bundled within this test pack, including:

- Raw packet processing performance (UDP)
- Maximum capacity
- HTTP capacity (with and without transaction delays)
- Latency (UDP)
- Application average response time (HTTP)

3.1.3 Stability and Reliability Testing Metrics

An array of pre-built stability and reliability tests are bundled within this test pack, including:

- Stability and Security - Attack Leakage
- Protocol fuzzing and mutation

3.2 Test Environment

3.2.1 Test Architecture

The aim of this test pack is to provide a thorough test of all the main components of a routed next generation firewall device in a controlled and repeatable manner and in the most “real-world” environment that can be simulated in a test lab.

Traffic generation equipment—such as the hosts generating exploits and BreakingPoint transmit ports—is connected to the “external” network, while the “receiving” equipment—such as the vulnerable hosts for the exploits and BreakingPoint receive ports—is connected to the internal network. The firewall is connected between two “gateway” switches, one at the edge of the external network and one at the edge of the internal network. Figure 3 illustrates the basic test environment.

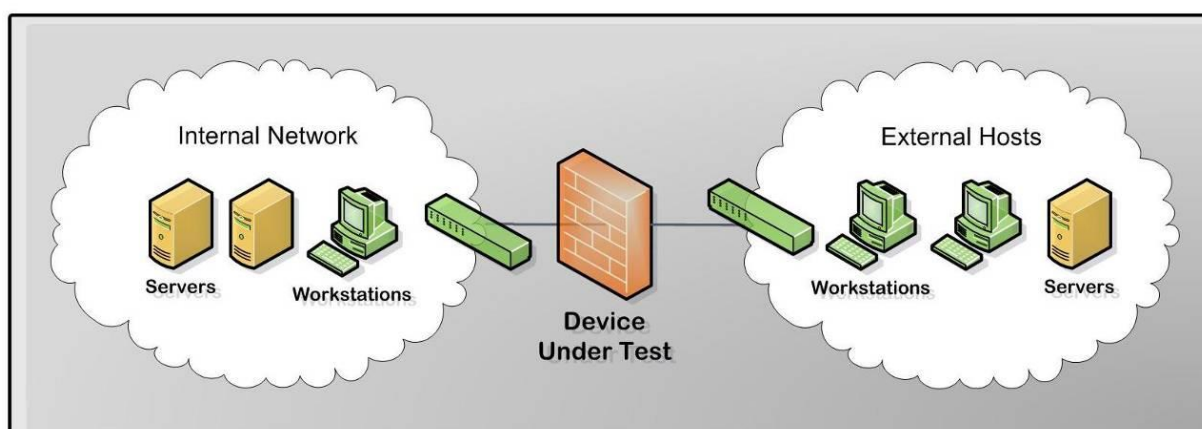


Figure 3 – Test Environment for the DUT

All network traffic, i.e. “normal” network traffic, background load traffic, and exploit traffic, is transmitted through the firewall, from external to internal. Responses will flow in the opposite direction. A management interface is used to connect the DUT to the management console on a private subnet. This ensures that the firewall and console can communicate even when the target subnet is subjected to heavy loads, and follows best practice guidelines for the prevention of attacks on the console itself from external hosts.

At a minimum, it is required to address BreakingPoint environment configuration such as IP address assignments and routing.

It is beyond the scope of this document to provide a comprehensive list of steps necessary for the configuration of the BreakingPoint chassis and DUT. See the manufacturer’s documentation for additional information.

3.2.2 Test Pack Configuration

This test pack has been designed to run without requiring test customization. Once the specific physical environment (DUT and BreakingPoint) has been prepared, the tests are ready to be run. The specific names of the tests and the order in which they should be run are outlined in the following sections.

4 Security Effectiveness

This section verifies that the next generation firewall is capable of enforcing a specified security policy effectively. NSS Labs' next generation firewall analysis is conducted by incrementally building upon a baseline configuration (simple routing with no policy restrictions and no content inspection) to a complex, real-world, multiple-zone configuration supporting many addressing modes, policies, applications and inspection engines.

The firewall must support stateful firewalling either by managing state tables to prevent "traffic leakage" or as a stateful proxy. The ability to manage firewall policy across multiple interfaces/zones is a required function. At a minimum, the firewall must provide a "trusted" internal interface, an "untrusted" external/Internet interface, and (optionally) one or more DMZ interfaces. In addition, a dedicated management interface (virtual or otherwise) is preferred.

The tests are listed in the order commonly used by NSS Labs test engineers and is the recommended order for first time use. However, individual tests within this category can be tested separately, and in any order.

4.1 Next Generation Firewall Policy Functionality Testing

This section provides the steps necessary to test commonly used firewall policies, from simple to complex. This test pack configuration file has been designed to provide exemplar traffic flowing in the following directions and is illustrated in the following ways:

- Into the firewall from a untrusted network
- Out of the firewall from the trusted network
- From the trusted network to the Demilitarized Zone (DMZ)
- From the untrusted network to the DMZ
- From the DMZ to both the trusted and untrusted networks

<Insert Graphic illustrating the use cases listed above>

Figure 4 – Common Firewall Use Cases

The steps listed below start with basic connectivity testing and moves to more complex traffic control.

4.2 Baseline Policy

Description	This is a basic routed configuration with an "allow all" policy. This policy is used to validate the setup of the DUT, and ensure that there are no issues with traffic reaching any of the networks.
Test Pack Configuration File(s)	NSS_NGFW_PS8_10G_Security_Policy_LAN_WAN.bpt

First, create a "cleanup rule" on the DUT that denies all traffic and run the test.

Step 1 – Configure the DUT

From: ANY	To: ANY	Application/Ports: ANY	Action: DENY
-----------	---------	------------------------	--------------

Step 2 – Run the Test

Click “Save and Run” on the BreakingPoint Console.

Step 3 – Success Criteria

Confirm that all traffic is blocked.

Next, add the “allow all” policy on the DUT *before* the cleanup rule and run the test. Both rules should be active in the DUT.

Step 1 – Configure the DUT

From: ANY	To: ANY	Application/Ports: ANY	Action: ALLOW
From: ANY	To: ANY	Application/Ports: ANY	Action: DENY

Step 2 – Run the Test

Click “Save and Run” on the BreakingPoint Console.

Step 3 – Success Criteria

Confirm all traffic proceeds unimpeded.

4.3 Simple Policy

Description	This is a simple outbound policy allowing browsing and email access for internal clients and is considered the most basic policy for traffic. No traffic from the untrusted network should be allowed through the DUT, while traffic from the trusted network should continue unimpeded to the outside.
Test Pack Configuration File(s)	NSS_NGFW_PS8_10G_Security_Policy_LAN_WAN.bpt

Prepare the environment and run the test:

Step 1 – Configure the DUT

From: TRUSTED	To: ANY	Application/Ports: ANY	Action: ALLOW
From: ANY	To: ANY	Application/Ports: ANY	Action: DENY

Step 2 – Run the Test

Click “Save and Run” on the BreakingPoint Console.

Step 3 – Success Criteria

Confirm that traffic flowing from TRUSTED to UNTRUSTED is allowed to pass through the DUT, while traffic from UNTRUSTED to TRUSTED is blocked.

4.4 Complex Policies

Complex outbound and inbound policies consisting of many rules, objects, and services. This should be a multi-step test. Using various setups, it should be ensured that the firewall honors all rules regarding traffic in and out of the firewall.

4.4.1 Multiple Policy Configuration Testing

Description	<p>Multi-policy configurations may be tested using the following example:</p> <p><i>The firewall has rules that specify only Web (80, 443) traffic is allowed into the trusted network (and only to specific addresses), while Web (80, 443), SMTP (25), SSH (22) and DNS (53) are allowed out of the trusted network.</i></p> <p>Using this example, verify that no traffic outside of those rules is allowed in either direction, and that traffic from one direction does not affect the other direction.</p>
Test Pack Configuration File(s)	NSS_NGFW_PS8_10G_Security_Policy_LAN_WAN.bpt

Prepare the environment and run the test:

Step 1 – Configure the DUT

```

From: ANY      To: TRUSTED  Applications/Ports: 80,443      Action: ALLOW
From: TRUSTED  To: ANY      Applications/Ports: 80,443,22,53  Action: ALLOW
From: ANY      To: ANY      Applications/Ports: ANY         Action: DENY

```

Step 2 – Run the Test

Click “Save and Run” on the BreakingPoint Console.

Step 3 – Success Criteria

Confirm that traffic flowing from TRUSTED to UNTRUSTED is allowed to pass through the DUT, while traffic from UNTRUSTED to TRUSTED is blocked.

4.4.2 Static NAT (Network Address Translation)

Description	<p>Inbound network address translation (NAT) to DMZ using fixed IP address translation with one-to-one mapping.</p> <p>This is a test of the firewall's ability to provide 1:1 mapping of external IP addresses to services provided within the DMZ. This should also test that any rules are honored in addition the address translation.</p> <p>Two options are provided, one using DMZ, the other using a specific range of IP addresses.</p>
Test Pack Configuration File(s)	<p>NSS_NGFW_PS8_10G_Security_Policy_LAN_WAN_DMZ.bpt</p> <p>NSS_NGFW_PS8_10G_Security_Policy_LAN_WAN.bpt</p>

If you choose to configure as a separate DMZ network, run the test once the following policies have been configured on the DUT.

Step 1 – Configure the DUT

From: ANY	To: DMZ	Applications/Ports: 80,443,25,53	Action: ALLOW
From: DMZ	To: ANY	Applications/Ports: 80,443	Action: ALLOW
From: ANY	To: ANY	Applications/Ports: ANY	Action: DENY

Step 2 – Run the Test

Click "Save and Run" on the BreakingPoint Console.

Step 3 – Success Criteria

Verify that no traffic outside of those rules is allowed in either direction, and that traffic from one direction does not affect the other direction.

Alternately, if you do not wish to test with a separate DMZ network, you can set up inbound network address translation (NAT) to a specific range of IP Addresses within TRUSTED using fixed IP address translation with one-to-one mapping. In this instance, use the NSS_NGFW_PS8_10G_Security_Policy_LAN_WAN.BPT configuration file .

Step 1 – Configure the DUT

From: ANY	To: TRUSTED	Applications/Ports: 80,443,25,53	Action: ALLOW
From: TRUSTED	To: ANY	Applications/Ports: 80,443	Action: ALLOW
From: ANY	To: ANY	Applications/Ports: ANY	Action: DENY

Step 3 – Run the Test

Click “Save and Run” on the BreakingPoint Console.

Step 4 – Success Criteria

Verify that no traffic outside of those rules is allowed in either direction, and that traffic from one direction does not affect the other direction.

4.4.3 Dynamic/Hide NAT (Network Address Translation)

Description	Outbound network address translation (NAT) (from internal to external) where all outbound traffic “hides” behind the IP address of the external interface of the DUT utilizing a pool of high ports to manage multiple connections.
Test Pack Configuration File(s)	NSS_NGFW_PS8_10G_Security_Policy_LAN_WAN.bpt

Prepare the environment and run the test:

Step 1 – Configure the DUT

From: TRUSTED	To: ANY	Applications/Ports: 80,443	Action: ALLOW
From: ANY	To: ANY	Applications/Ports: ANY	Action: DENY

Step 2 – Run the Test

Click “Save and Run” on the BreakingPoint Console.

Step 3 – Success Criteria

Verify that no traffic outside of those rules is allowed in either direction, and that traffic from one direction does not affect the other direction.

4.5 Denial of Service and Evasion Testing

Due to the dynamic nature of evasions, NSS utilizes multiple tools to perform evasion testing. Currently, NSS utilizes multiple freely available open source tools. The following is a list of evasion types that may be seen in an NSS test:

- SYN Flood
- IP Address Spoofing
- TCP Split Handshake
- Packet Fragmentation
- Stream Segmentation
- RPC Fragmentation
- URL Obfuscation
- HTML Obfuscation
- Payload Encoding
- FTP Evasions
- Layered Evasions (for example IP Fragmentation combined with TCP Segmentation)
- Session Hijacking

Three of the tests are included in this test pack; SYN Flood, IP Address Spoofing, TCP Split Handshake. The tests for SYN Flood and IP Spoofing are included as components in the test pack configuration file; the TCP Handshake is implemented using a built-in BreakingPoint test (outlined in the relevant test below).

4.5.1 SYN Flood

Description	<p>The basis of a SYN flood attack is to fail to complete the three-way handshake necessary to establish a legitimate session. The objective of SYN flooding is to disable one side of the TCP connection, which will result in one or more of the following:</p> <ul style="list-style-type: none">• The server is unable to accept new connections.• The server crashes or becomes inoperative.• Authorization between servers is impaired. <p>The DUT is expected to protect against SYN floods.</p>
Test Pack	<p>Configuration File(s) NSS_NGFW_PS8_10G_Security_Policy_SYN_Flood.bpt</p>

The goal of this test is to determine the next generation firewall SYN flood protection capabilities.

Prepare the environment and run the test:

Step 1 – Configure the DUT

From: ANY	To: ANY	Applications/Ports: ANY	Action: ALLOW
From: ANY	To: ANY	Applications/Ports: ANY	Action: DENY

Step 2 – Run the Test

Click “Save and Run” on the BreakingPoint Console.

Step 3 – Success Criteria

The test will PASS if all traffic is blocked.

4.5.2 IP Address Spoofing

Description	<p>This test attempts to confuse the DUT into allowing traffic to pass from one network segment to another. By forging the IP header to contain a different source address from where the packet was actually transmitted, an attacker can make it appear that the packet was sent from a different (trusted) machine. The endpoint that receives successfully spoofed packets will respond back to the forged source address (the attacker).</p> <p>The DUT is expected to protect against IP Address spoofing.</p>
Test Pack Configuration File	NSS_NGFW_PS8_10G_Security_Policy_IP_Spoof.bpt

Prepare the environment and run the test:

Step 1 – Configure the DUT

From: ANY	To: ANY	Applications/Ports: ANY	Action: ALLOW
From: ANY	To: ANY	Applications/Ports: ANY	Action: DENY

Step 2 – Run the Test

Click “Save and Run” on the BreakingPoint Console.

Step 3 – Success Criteria

The test will PASS if all traffic is blocked.

4.5.3 TCP Split Handshake

Description	<p>This test attempts to confuse the DUT into allowing traffic to pass from one network segment to another. The TCP split handshake blends features of both the three-way handshake and the simultaneous-open connection. The result is a TCP spoof attack that allows an attacker to bypass the firewall by instructing the target to “initiate” the session back to the attacker. Popular TCP/IP networking stacks respect this handshaking method, including Microsoft, Apple, and Linux stacks, with no modification.¹</p> <p>The DUT is expected to protect against TCP split handshake spoofing.</p>
Test Pack Configuration File(s)	NSS_NGFW_PS8_10G_Security_Policy_TCP_Split_Handshake.bpt

Prepare the environment and run the test:

Step 1 – Configure the DUT

From: ANY	To: ANY	Applications/Ports: ANY	Action: ALLOW
From: ANY	To: ANY	Applications/Ports: ANY	Action: DENY

Step 2 – Run the Test

Click “Save and Run” on the BreakingPoint Console.

Step 3 – Success Criteria

The pass/fail criteria for the default BreakingPoint test is based on the **payload delivered** and **not the method of delivery**. In other words, the test should be considered failed if the malicious session is established.

The default test will report a FAIL if the malicious payload, which is sent over the LEGITIMATE session (*not* the malicious session) is allowed through and reports a PASS if the malicious payload is blocked. This is incorrect because the test is about the establishment of a malicious (split handshake) session, not the delivery of a malicious PDF over a legitimate session established with the three-way handshake.

¹ “The TCP Split Handshake: Practical Effects on Modern Network Equipment”, Tod Alien Beardsley & Jin Qian, <http://www.macrothink.org/journal/index.php/npa/article/view/285>

4.6 Exploits

Description	<p>This test is used to determine the DUT's security effectiveness against multiple exploits. Multiple attack vectors are tested, including system exposure, service exposure and system-service faults. Exploits affecting web servers, web browsers, databases, ActiveX, Java and browser plugins are present. These exploits may result in arbitrary code execution, buffer overflows, code injection, cross-site scripting, directory traversal, and privilege escalation.</p> <p>Critical metrics for this test are as follows:</p> <ul style="list-style-type: none"> • Strike Name • Strike Result • Strike Reference <p>The DUT is expected to protect against exploits.</p>
Test Pack Configuration File(s)	NSS_NGFW_PS8_10G_Security_Strikes.bpt

Prepare the environment and run the test:

Step 1 – Configure the DUT

From: ANY	To: ANY	Applications/Ports: ANY	Action: ALLOW
From: ANY	To: ANY	Applications/Ports: ANY	Action: DENY

Step 2 – Run the Test

Click "Save and Run" on the BreakingPoint Console.

Step 3 – Success Criteria

The test will PASS if all strikes are blocked.

Important:

- The exploits run in **NSS_NGFW_PS8_10G_Security_Strikes.bpt** are a subset of what you will see in an NSS testing. **A score of 100% in the test pack does not guarantee a 100% in NSS testing.**
- This should be run after all performance testing has been completed and false positives have been found and removed. Failure to do so may result in scores that are inflated by poorly written signatures that fire on real world traffic.

Follow these steps in sequence for data gathering and test scoring:

1. Expand “Test Results for Security_1” and then expand “Detail”
2. The list of allowed strikes is found under “Allowed Strike List.”
The name of the strike is the key element to record.
3. The list of blocked strikes is found under “Blocked Strike List.”
The name of the strike is the key element to record.
4. After recording the list of allowed strikes, expand “Component Detection Assessment,” then Strikes, and finally each category of exploit.
5. Click into each section, such as “Denial of Service: Browser” and note the pertinent information regarding the Strike Reference that matches the list of allowed strikes from step 2. This is where information such as the CVE of the missed exploit will be found.
6. NSS recommends scoring exploits as a percentage of strikes blocked.
Block percentage is calculated as the number of strikes blocked divided by the number of strikes run. To convert the decimal to percentage, multiple by 100.

5 Performance

This section provides steps for measuring the maximum throughput of the next generation firewall in a variety of conditions. This information can be used for the purpose of firewall benchmark evaluation as well as ongoing firewall management.

A large amount of test result data is output from running and saving all the tests necessary for proper NGFW evaluation. This section details the tests within this test pack and how to score and evaluate the NGFW.

5.1 Raw Performance Testing with UDP Traffic and Latency Testing

Description	<p>This is a basic routed configuration with an “allow all” policy. This policy is used to validate the setup of the DUT, and ensure that there are no issues with traffic reaching any of the networks.</p> <p>Multiple tests will be run, each recording the following critical metrics:</p> <ul style="list-style-type: none"> • Mbps (UDP data rates) • Latency rate per millisecond <p>Ethernet data rates and latency are determined from the same tests and the same test reports.</p> <p>Once it is determined the maximum capacity of the DUT, it is necessary to determine the timestamp and the UDP data rate immediately before failure. Once the raw UDP performance is determined, then latency can be determined.</p>
Test Pack Configuration File(s)	<p>NSS_NGFW_PS8_10G_Performance_UDP_64_Byte.bpt</p> <p>NSS_NGFW_PS8_10G_Performance_UDP_128_Byte.bpt</p> <p>NSS_NGFW_PS8_10G_Performance_UDP_256_Byte.bpt</p> <p>NSS_NGFW_PS8_10G_Performance_UDP_512_Byte.bpt</p> <p>NSS_NGFW_PS8_10G_Performance_UDP_1024_Byte.bpt</p> <p>NSS_NGFW_PS8_10G_Performance_UDP_1514_Byte.bpt</p> <p>NSS_NGFW_PS8_20G_Performance_UDP_64_Byte.bpt</p> <p>NSS_NGFW_PS8_20G_Performance_UDP_128_Byte.bpt</p> <p>NSS_NGFW_PS8_20G_Performance_UDP_256_Byte.bpt</p> <p>NSS_NGFW_PS8_20G_Performance_UDP_512_Byte.bpt</p> <p>NSS_NGFW_PS8_20G_Performance_UDP_1024_Byte.bpt</p> <p>NSS_NGFW_PS8_20G_Performance_UDP_1514_Byte.bpt</p> <p>NSS_NGFW_PS8_30G_Performance_UDP_64_Byte.bpt</p> <p>NSS_NGFW_PS8_30G_Performance_UDP_128_Byte.bpt</p>

```

NSS_NGFW_PS8_30G_Performance_UDP_256_Byte.bpt
NSS_NGFW_PS8_30G_Performance_UDP_512_Byte.bpt
NSS_NGFW_PS8_30G_Performance_UDP_1024_Byte.bpt
NSS_NGFW_PS8_30G_Performance_UDP_1514_Byte.bpt
NSS_NGFW_PS8_40G_Performance_UDP_64_Byte.bpt
NSS_NGFW_PS8_40G_Performance_UDP_128_Byte.bpt
NSS_NGFW_PS8_40G_Performance_UDP_256_Byte.bpt
NSS_NGFW_PS8_40G_Performance_UDP_512_Byte.bpt
NSS_NGFW_PS8_40G_Performance_UDP_1024_Byte.bpt
NSS_NGFW_PS8_40G_Performance_UDP_1514_Byte.bpt

```

Prepare the environment and run the test:

Step 1 – Configure the DUT

From: ANY	To: ANY	Applications/Ports: ANY	Action: ALLOW
From: ANY	To: ANY	Applications/Ports: ANY	Action: DENY

Step 2 – Configure the Test Pack

Configuration will vary each time this test is run. The following tests are the names of the pre-built performance tests available once this test pack has been installed:

1. NSS NGFW UDP 64 Byte
2. NSS NGFW UDP 128 Byte
3. NSS NGFW UDP 256 Byte
4. NSS NGFW UDP 512 Byte
5. NSS NGFW UDP 1024 Byte
6. NSS NGFW UDP 1514 Byte

The tests are to be run in the order listed. Each test is provided with multiple bandwidth settings. Choose the test set that most closely matches the maximum performance of your next generation firewall.

Step 3 – Run the Test

1. Choose the UDP packet size
2. Choose the appropriate bandwidth
3. Click “Save and Run” on the BreakingPoint Console

Once the test is complete, save the results for interpretation (listed in section below).

Step 4 – Success Criteria

The test should be considered successful if all traffic proceeds unimpeded.

5.1.1 Example: Interpreting Performance Results – Throughput (Mbps)

Follow these steps in sequence for data interpretation and test scoring for each test run.

1. Open the test report. Go to the “Ethernet Data Rates” category, within the test report under “Detail”. There will be a graph similar to Figure 5.

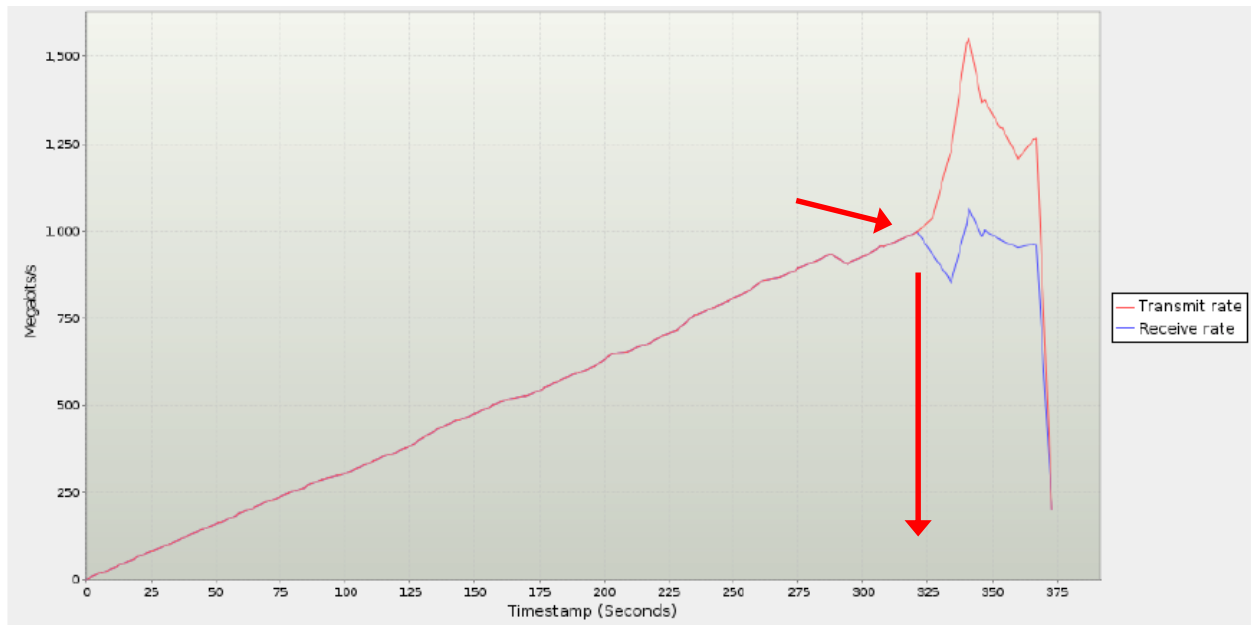


Figure 5 – Ethernet (UDP) Data Rates

2. The two arrows indicate where the two graph lines of “Transmit rate” and “Receive rate” begin to diverge. This is a visual indication (note second arrow pointing down) within the timestamp that the maximum capacity on the DUT has been reached.
3. Note the timestamp (in this case approximately 321 seconds.)
4. The timestamp *table data* is located directly under the Figure 5 graphic on the BreakingPoint console, shown in the figure below. Scroll down to the closest timestamp to the one determined in the previous steps (in the example, approximately 321 seconds). Record both rates.

288.015	931.6	931.5
294.015	904.8	905.1
295.014	910.9	910.7
301.014	929.2	929.1
307.014	955.6	955.5
308.015	954.8	954.9
314.015	973.3	~973
320.015	993.1	993.2
321.015	997.1	~997
327.018	~1037	931.6
333.018	~1206	~867
334.018	~1229	850.5

Figure 6 – UDP Bandwidth Table @timestamp

- The firewall maximum capacity is the point at which the “Mbps” drops off from the previously held maximum (note the arrows below). In this case, the firewall failed at 327 seconds, having held a previous high traffic load of 997 Mbps at 321 seconds. 997 Mbps is the maximum throughput discovered for this test.
- Document this result** in the appropriate section of the Scorecard in Appendix C: Combined Scorecard for each test.

5.1.2 Example: Interpreting Performance Results – Latency (milliseconds)

Using the same test report, a similar process is used to determine latency.

- Within the test report, refer to Section 7.19.24.23 for the “Frame Latency” category.
- Within the Frame Latency category, refer to the previously determined timestamp. The previous table data revealed a timestamp of 321 seconds at maximum operational throughput. Data and timestamps rarely match from category to category within the test report. In the table below, the arrows indicate the best timestamp immediately prior to firewall failure is at timestamp 322.

308.005	1,774.083	51	29,110
309.004	1,844.495	57	25,714
315.004	2,118.086	109	37,677
321.004	2,542.333	109	27,737
322.005	3,766.503	123	44,779
328.005	10,559.843	104	39,100
334.005	12,030.271	175	45,946
335.006	12,323.145	190	52,194

Figure 7 – Frame Latency Table at Previous Timestamp

Note: the above table records timestamps using microseconds. If a conversion to milliseconds is desired, divide this value by 1,000.

- The Latency score is calculated by taking 90% of the chosen timestamp (in this case $322 \times 0.9 = 289.8$).
- Document this result** in the appropriate section of the Scorecard in Appendix C: Combined Scorecard for each test.

5.2 Maximum Capacity (Per Second) Testing

The following tests are completed within this section:	
Description	<ul style="list-style-type: none"> • HTTP Capacity With No Transaction Delays • Application Average Response Time: HTTP • HTTP Capacity with Transaction Delays
Test Pack Configuration File(s)	NSS_NGFW_PS8_10G_Performance_Max_TCP_CPS.bpt NSS_NGFW_PS8_10G_Performance_HTTP_CPS.bpt NSS_NGFW_PS8_10G_Performance_HTTP_TPS.bpt NSS_NGFW_PS8_20G_Performance_Max_TCP_CPS.bpt NSS_NGFW_PS8_20G_Performance_HTTP_CPS.bpt NSS_NGFW_PS8_20G_Performance_HTTP_TPS.bpt NSS_NGFW_PS8_30G_Performance_Max_TCP_CPS.bpt NSS_NGFW_PS8_30G_Performance_HTTP_CPS.bpt NSS_NGFW_PS8_30G_Performance_HTTP_TPS.bpt NSS_NGFW_PS8_40G_Performance_Max_TCP_CPS.bpt NSS_NGFW_PS8_40G_Performance_HTTP_CPS.bpt NSS_NGFW_PS8_40G_Performance_HTTP_TPS.bpt

Prepare the environment and run the test:

Step 1 – Configure the DUT

From: ANY	To: ANY	Applications/Ports: ANY	Action: ALLOW
From: ANY	To: ANY	Applications/Ports: ANY	Action: DENY

Step 2 – Configure the Test Pack

Configuration will vary each time this test is run. The following tests are the names of the pre-built performance tests available once this test pack has been installed:

1. NSS NGFW Max HTTP Connections per Second
2. NSS NGFW Max HTTP Transactions per Second
3. NSS NGFW Max TCP Connections per Second

The tests are to be run in the order listed. Each test is provided with multiple bandwidth settings. Choose the test set that most closely matches the maximum performance of the DUT.

Step 3 – Run the Test

Make sure to manually clear out the TCP connections and/or transactions tables from the DUT prior to each test. Click “Save and Run” on the BreakingPoint Console.

Once the test is complete, save the results for interpretation (listed in section below).

Step 4 – Success Criteria

Stop the test when the Concurrent Flows value begins to rise abruptly and consistently.

5.2.1 Example - Gathering and Interpreting Performance Results

Follow these steps in sequence for data interpretation and test scoring for each test run.

1. Open the test report. Go to Section 7.19.24.8 – Concurrent Flows. There will be a graph similar to Figure 8.

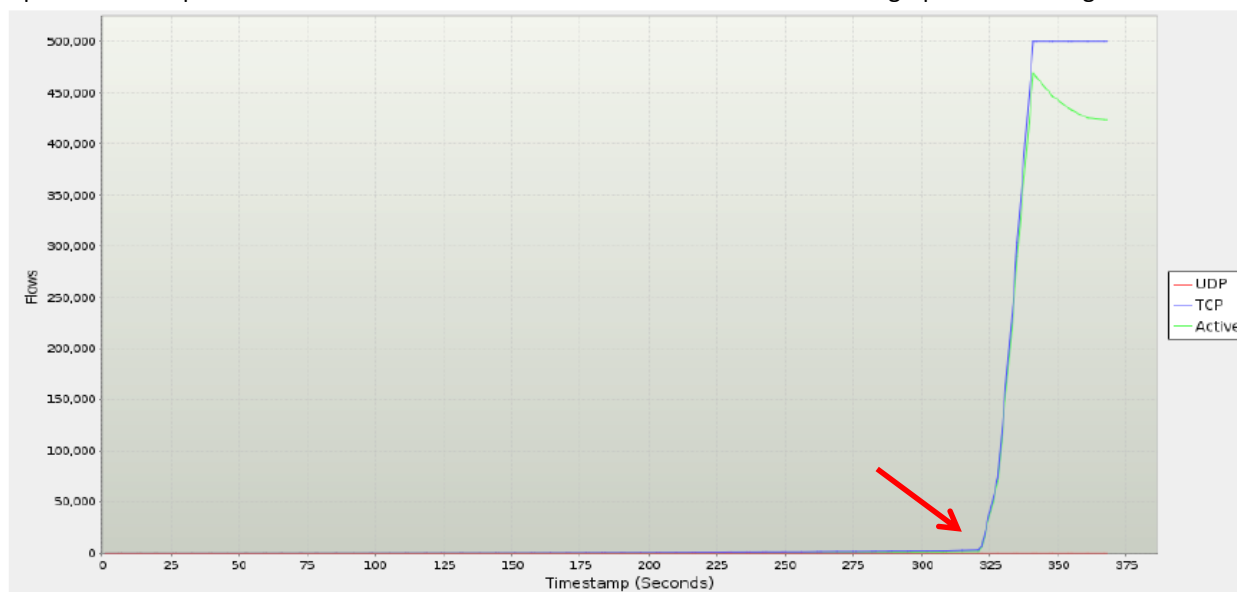


Figure 8 – Frame Latency Table @timestamp

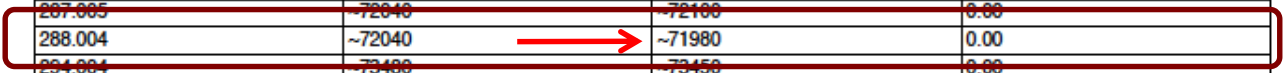
2. Note the timestamp immediately prior to the rise in Concurrent Flows (in this case approximately 321 seconds.)
3. The timestamp *table data* is located directly under the Figure 8 graphic on the BreakingPoint console, shown in the figure below. Scroll down to the closest timestamp to the one determined in the previous steps (in the example, approximately 321 seconds). Identify the timestamp immediately prior to the rise in Concurrent Flows as shown in the figure (note the jump from 6,574 at 322 milliseconds and 74,061 at 328 milliseconds).

309.004	0	2,153	1,385
315.004	0	2,594	1,649
321.004	0	2,956	1,744
322.005	0	6,574	5,538
328.005	0	74,061	69,978
334.005	0	261,027	240,037

Figure 9 – Concurrent Flows Spike Table View

Note: the above table records timestamps using microseconds. If a conversion to microseconds is desired, divide this value by 1,000.

4. The Latency score is calculated by taking 90% of the chosen timestamp (in this case $322 \times 0.9 = 289.8$).
5. Using the value calculated above, go to Section 7.19.24.9 – Flow Rate. The timestamps may not match exactly between the two tables due to recording deltas and flow aging. The drop-off in concurrent flows will be easily found, highlighted as 71,980 in Figure 10.



281.004	~70560	~70570	0.00
282.004	~70490	~70490	0.00
287.005	~72040	~72100	0.00
288.004	~72040	~71980	0.00
294.004	~73400	~73450	0.00
295.004	~74000	~74070	0.00
301.004	~75570	~75650	0.00

Figure 10 – Concurrent Flows Spike Table View

6. Record the observed value as both **Maximum TCP Connections Per Second** and **Maximum HTTP Connections per Second** (one HTTP connection per TCP connection).
7. For `NSS_NGFW_PS8_Raw_Performance_Maximum_HTTP_Transactions_per_Second.bpt`, record the value located under Application Transactions Rate at the timestamp.
8. Document this result in the appropriate section of the **Scorecard** in Appendix C for each test.

5.3 Maximum Capacity Testing

Description	<p>The following tests are completed within this section:</p> <ul style="list-style-type: none"> NSS NGFW Theoretical Maximum TCP Concurrent Connections NSS NGFW Theoretical Maximum TCP Concurrent Connections with Data <p>Critical test metrics for these tests are:</p> <ul style="list-style-type: none"> Raw number (without data) Raw number (with data)
Test Pack Configuration File(s)	<p>NSS_NGFW_PS8_10G_Performance_Max_Concurrent_TCP_connections.bpt</p> <p>NSS_NGFW_PS8_10G_Performance_Max_Concurrent_TCP_connections_with_data.bpt</p> <p>NSS_NGFW_PS8_20G_Performance_Max_Concurrent_TCP_connections.bpt</p> <p>NSS_NGFW_PS8_20G_Performance_Max_Concurrent_TCP_connections_with_data.bpt</p> <p>NSS_NGFW_PS8_30G_Performance_Max_Concurrent_TCP_connections.bpt</p> <p>NSS_NGFW_PS8_30G_Performance_Max_Concurrent_TCP_connections_with_data.bpt</p> <p>NSS_NGFW_PS8_40G_Performance_Max_Concurrent_TCP_connections.bpt</p> <p>NSS_NGFW_PS8_40G_Performance_Max_Concurrent_TCP_connections_with_data.bpt</p>

Prepare the environment and run the test:

Step 1 – Configure the DUT

From: ANY	To: ANY	Applications/Ports: ANY	Action: ALLOW
From: ANY	To: ANY	Applications/Ports: ANY	Action: DENY

Step 2 – Configure the Test Pack

Configuration will vary each time this test is run. Choose the test that most closely matches the rated throughput of the DUT. The following tests are the names of the pre-built performance tests available once this test pack has been installed:

1. NSS FW Theoretical Maximum TCP Concurrent Connections
2. NSS FW Theoretical Maximum TCP Concurrent Connections with Data

Run the test names in the order listed and save each test report.

Step 3 – Run the Test

Make sure to manually clear out the TCP connections and/or transactions tables from the DUT prior to each test. Click “Save and Run” on the BreakingPoint Console.

Once the test is complete, save the results for interpretation (listed in section below).

Follow these steps in sequence for data gathering and test scoring:

1. Open the test report. “TCP Concurrent Connections” can be found in the test report within Section 7.19.24.11 under “Detail”.
2. When testing for Maximum Concurrent Connections, the best solution is to use the firewall in order to track the open connections. Once the firewall has ceased tracking new connections, it should either drop new incoming or begin to age existing connections, and this will be illustrated by the built-in connection tracking counters. Each tested firewall will have different methods of obtaining this data.
3. If there is no means to track connections through the firewall, the BreakingPoint UI can be used to track them. As the test is running, the test status page tracks open and established connections. When the firewall ceases accepting new connections, the “Attempted” and “Open” connection trackers will diverge. The “Open” rate will stop advancing, while the “Attempted” rate will continue to climb at the requested load profile.
4. Identify the timestamp at which either of these events happens first in Section 7.19.24.6 – Application Transaction Rates:
 - a. A connection is reset **or**
 - b. The establish rate falls behind the attempted rate

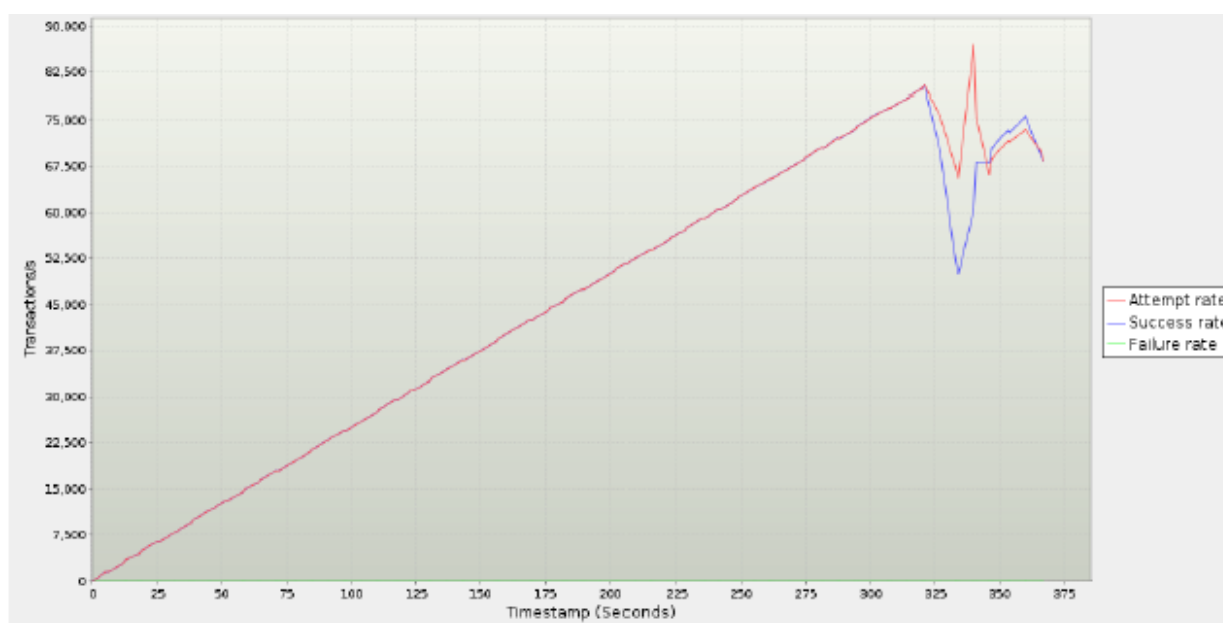


Figure 11 – Establish Rate Falling Behind Attempted Rate In Graph View

307.005	~76930	~76930	0.00
308.005	~77050	~77030	0.00
314.005	~78450	~78470	0.00
320.005	~79910	~79910	0.00
321.004	~80550	~80550	0.00
327.005	~75600	~69910	0.00
333.005	~67400	~52200	0.00

Figure 12 – Establish Rate In Table View

5. Fall back to the timestamp immediately prior to this failure.
6. Find this timestamp in the table 7.19.24.8 – Concurrent Flows

309.004	0	2,153	1,385
315.004	0	2,394	1,045
321.004	0	2,956	1,744
322.005	0	6,574	5,538
328.005	0	74,061	69,978
334.005	0	261,027	249,037

Figure 13 – Maximum Concurrent Flows

7. This value is the Maximum Concurrent Flow.
8. Prior to repeating the remaining TCP or HTTP maximum-connections tests, make sure to manually clear out the TCP connections and/or transactions tables from the firewall.
9. Complete both tests.
10. **Document this result** in the appropriate section of the Scorecard in Appendix C: Combined Scorecard for each test.

5.4 Maximum HTTP Capacity Testing

Description	<p>The following tests are completed within this section:</p> <ul style="list-style-type: none"> • HTTP Capacity With No Transaction Delays and Application Average Response Time • HTTP Capacity with Transaction Delays and Application Average Response Time <p>Critical test metrics for these tests are:</p> <ul style="list-style-type: none"> • HTTP capacity With No Transaction Delays • Application Average Response Time: HTTP • HTTP Capacity with Transaction Delays
	<p>HTTP Capacity With No Transaction Delays and Application Average Response Time (HTTP)</p> <p>NSS_NGFW_PS8_10G_Performance_HTTP_44KB_Response.bpt NSS_NGFW_PS8_10G_Performance_HTTP_21KB_Response.bpt NSS_NGFW_PS8_10G_Performance_HTTP_10KB_Response.bpt NSS_NGFW_PS8_10G_Performance_HTTP_4_5KB_Response.bpt NSS_NGFW_PS8_10G_Performance_HTTP_1_7KB_Response.bpt NSS_NGFW_PS8_20G_Performance_HTTP_44KB_Response.bpt NSS_NGFW_PS8_20G_Performance_HTTP_21KB_Response.bpt NSS_NGFW_PS8_20G_Performance_HTTP_10KB_Response.bpt NSS_NGFW_PS8_20G_Performance_HTTP_4_5KB_Response.bpt NSS_NGFW_PS8_20G_Performance_HTTP_1_7KB_Response.bpt NSS_NGFW_PS8_30G_Performance_HTTP_44KB_Response.bpt NSS_NGFW_PS8_30G_Performance_HTTP_21KB_Response.bpt NSS_NGFW_PS8_30G_Performance_HTTP_10KB_Response.bpt NSS_NGFW_PS8_30G_Performance_HTTP_4_5KB_Response.bpt NSS_NGFW_PS8_30G_Performance_HTTP_1_7KB_Response.bpt NSS_NGFW_PS8_40G_Performance_HTTP_44KB_Response.bpt NSS_NGFW_PS8_40G_Performance_HTTP_21KB_Response.bpt NSS_NGFW_PS8_40G_Performance_HTTP_10KB_Response.bpt NSS_NGFW_PS8_40G_Performance_HTTP_4_5KB_Response.bpt NSS_NGFW_PS8_40G_Performance_HTTP_1_7KB_Response.bpt</p>

HTTP Capacity with Transaction Delays and Application Average Response Time (HTTP)

NSS_NGFW_PS8_10G_Performance_HTTP_21KB_Response_with_delay.bpt
NSS_NGFW_PS8_10G_Performance_HTTP_10KB_Response_with_delay.bpt
NSS_NGFW_PS8_20G_Performance_HTTP_21KB_Response_with_delay.bpt
NSS_NGFW_PS8_20G_Performance_HTTP_10KB_Response_with_delay.bpt
NSS_NGFW_PS8_30G_Performance_HTTP_21KB_Response_with_delay.bpt
NSS_NGFW_PS8_30G_Performance_HTTP_10KB_Response_with_delay.bpt
NSS_NGFW_PS8_40G_Performance_HTTP_21KB_Response_with_delay.bpt
NSS_NGFW_PS8_40G_Performance_HTTP_10KB_Response_with_delay.bpt

Maximum capacity test metrics are determined with test result data from different sections of the respective test reports and utilize different methods for scoring and evaluation.

As the testing is concerned with maximum performance of the firewall, the tests must run for the duration and the appropriate values gathered from the test report.

Follow these steps in sequence for data gathering and test scoring:

1. Run the test names in order and save each test report.
2. Make sure to manually clear out the TCP connections and/or transactions tables from the firewall.
3. What is needed is the exact timestamp when the firewall failed, and at the precise moment prior to failure is when the appropriate test metric is acquired. **Stop the test when the Concurrent Flows value begin to climb rapidly and show no sign of returning to a lower number of concurrent flows.**
4. After the test has been stopped, open the Test Report and find Section 7.19.24.8 – Concurrent Flows

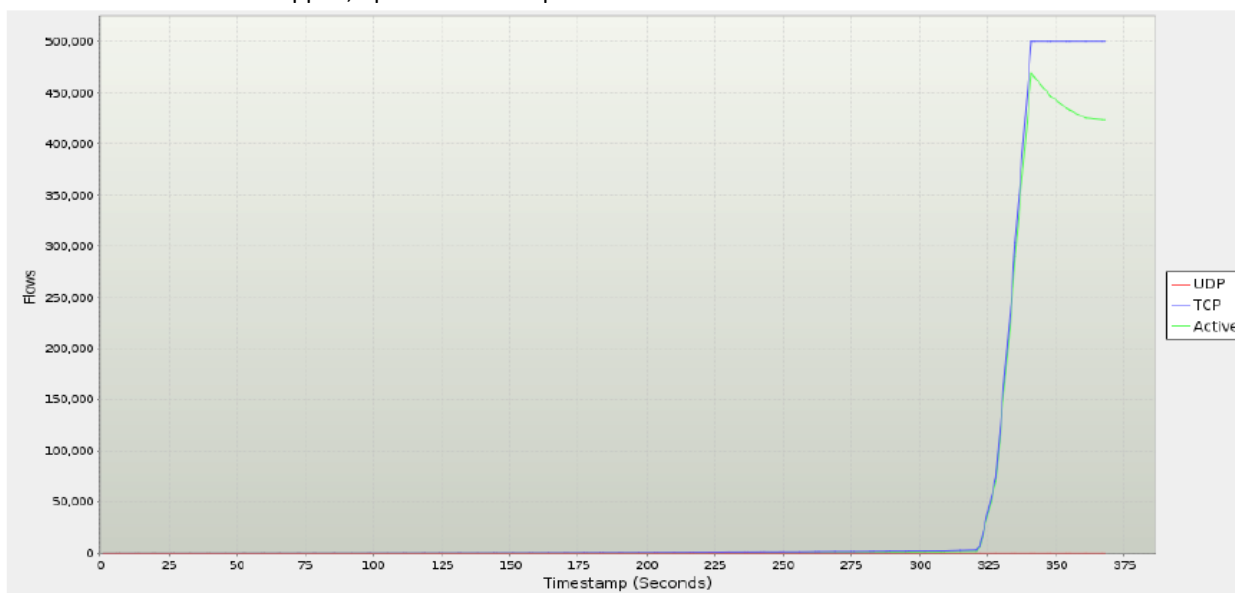


Figure 14 – Maximum Concurrent Flows

5. Identify the timestamp immediately prior to the rise in Concurrent Flows.

309.004	0	2,153	1,385
315.004	0	2,594	1,649
321.004	0	2,956	1,744
322.005	0	6,574	5,538
328.005	0	74,061	69,978
334.005	0	261,027	249,037

Figure 15 – Concurrent Flows Spike Table View

6. Multiply the timestamp by 90% in order to determine the timestamp where you will measure the connection rate. (Example: Failure at 321 seconds x 90% = 289 seconds. Start Test to the 289 second timestamp and find the corresponding flow rate / connection rate.) This timestamp value is now found in section 7.19.24.9 – Flow Rate. The timestamps may not match exactly between the two tables due to recording deltas and flow aging. The dropoff in concurrent flows will be easily found.

282.005	0	70030
288.004	0	~72070
289.005	0	~72430
293.004	0	74,000
296.005	0	~73930
302.005	0	~75420
308.005	0	77,000

Figure 16 – Table View

7. Record the value as **Maximum TCP Connections Per Second**.
8. The timestamp value determined in step 5 is now multiplied by 90% in order to determine the timestamp where you will measure the (average) application response time.
9. Find this timestamp in Section 7.19.24.7 – Application Response Time: HTTP.

281.004	2.2201	5.1120
282.004	2.2405	5.1165
287.005	2.3491	5.5763
288.004	2.3712	5.5544
294.004	2.5072	5.6665
295.004	2.5302	5.9189

Figure 17 – Average Response Time

10. Record this value as the **Average Response Time**.

5.4.1 Testing with Delay

Tests with delay are scored in much the same manner as without delay, with the following difference:

- If an HTTP Transaction failure occurs *before* the Maximum Connection Rate determined above, then the time stamp is determined from immediately before the failure in Section 7.19.24.5.1 – Application Transactions: HTTP. Flow Rate is then determined exactly as above.
- If they meet or exceed the value found without delay, then the same value is used.

5.5 Real-World Traffic Mix Performance

Description	<p>The following tests are completed within this section:</p> <ul style="list-style-type: none"> • NSS Real World Data Mix – Enterprise Perimeter • NSS Real World Data Mix – Financial • NSS Real World Data Mix – Education • NSS Real World Data Mix – Datacenter • NSS Real World Data Mix – US Mobile • NSS Real World Data Mix – EU Mobile <p>Critical test metrics for these tests are:</p> <ul style="list-style-type: none"> • Raw number (without data) • Raw number (with data)
Test Pack Configuration File(s)	<p>NSS_NGFW_PS8_10G_Performance_Real_World_Perimeter.bpt NSS_NGFW_PS8_10G_Performance_Real_World_Financial.bpt NSS_NGFW_PS8_10G_Performance_Real_World_Education.bpt NSS_NGFW_PS8_10G_Performance_Real_World_Datacenter.bpt NSS_NGFW_PS8_10G_Performance_Real_World_US_Mobile.bpt NSS_NGFW_PS8_10G_Performance_Real_World_EU_Mobile.bpt NSS_NGFW_PS8_20G_Performance_Real_World_Perimeter.bpt NSS_NGFW_PS8_20G_Performance_Real_World_Financial.bpt NSS_NGFW_PS8_20G_Performance_Real_World_Education.bpt NSS_NGFW_PS8_20G_Performance_Real_World_Datacenter.bpt NSS_NGFW_PS8_20G_Performance_Real_World_US_Mobile.bpt NSS_NGFW_PS8_20G_Performance_Real_World_EU_Mobile.bpt NSS_NGFW_PS8_30G_Performance_Real_World_Perimeter.bpt NSS_NGFW_PS8_30G_Performance_Real_World_Financial.bpt NSS_NGFW_PS8_30G_Performance_Real_World_Education.bpt NSS_NGFW_PS8_30G_Performance_Real_World_Datacenter.bpt NSS_NGFW_PS8_30G_Performance_Real_World_US_Mobile.bpt NSS_NGFW_PS8_30G_Performance_Real_World_EU_Mobile.bpt NSS_NGFW_PS8_40G_Performance_Real_World_Perimeter.bpt NSS_NGFW_PS8_40G_Performance_Real_World_Financial.bpt NSS_NGFW_PS8_40G_Performance_Real_World_Education.bpt NSS_NGFW_PS8_40G_Performance_Real_World_Datacenter.bpt NSS_NGFW_PS8_40G_Performance_Real_World_US_Mobile.bpt</p>

NSS_NGFW_PS8_40G_Performance_Real_World_EU_Mobile.bpt

Prepare the environment and run the test:

Step 1 – Configure the DUT

From: ANY	To: ANY	Applications/Ports: ANY	Action: ALLOW
From: ANY	To: ANY	Applications/Ports: ANY	Action: DENY

Step 2 – Configure the Test Pack

Configuration will vary each time this test is run. The following tests are the names of the pre-built performance tests available once this test pack has been installed:

- NSS Real World Data Mix –Perimeter
- NSS Real World Data Mix – Financial
- NSS Real World Data Mix – Education
- NSS Real World Data Mix – Datacenter
- NSS Real World Data Mix – US Mobile
- NSS Real World Data Mix – EU Mobile

Run the test names in the order listed and save each test report.

Step 3 – Run the Test

Make sure to manually clear out the TCP connections and/or transactions tables from the firewall prior to each test.

Click “Save and Run” on the BreakingPoint Console.

Once the test is complete, save the results for interpretation (listed in section below).

For each real-world data mix that was run, follow this procedure to determine data rate.

1. Each test should be stopped when a Transaction Failure occurs, Maximum Data Rate is achieved, or the Data Rate plateaus.
2. Find the timestamp prior to where the transaction failure occurred (7.20.26.5 – Application Transactions (Failures), or the max data rate occurred.

Find that timestamp in Section 8.7.5.3 – Ethernet Data Rates, and record the value in Receive Rate column.

6 Stability and Reliability Testing

6.1 Stability and Security - Attack Leakage

Description	<p>This is a basic routed configuration with an “allow all” policy. This policy is used to validate the setup of the DUT, and ensure that there are no issues with traffic reaching any of the networks.</p> <p>Critical test metrics for these tests are:</p> <ul style="list-style-type: none"> • Pass / Fail for duration • Time to fail or Duration • Fail Open or Fail Close <p>Ethernet data rates and latency are determined from the same tests and the same test reports.</p> <p>Once it is determined the maximum capacity of the DUT, it is necessary to determine the timestamp and the UDP data rate immediately before failure. Once the raw UDP performance is determined, then latency can be determined.</p>
Test Pack Configuration File(s)	<p>NSS_NGFW_PS8_10G_Stability_Attack_Leakage.bpt</p> <p>NSS_NGFW_PS8_20G_Stability_Attack_Leakage.bpt</p> <p>NSS_NGFW_PS8_30G_Stability_Attack_Leakage.bpt</p> <p>NSS_NGFW_PS8_40G_Stability_Attack_Leakage.bpt</p>

Prepare the environment and run the test:

Step 1 - Configure the DUT

From: ANY	To: TRUSTED	Applications/Ports: 80	Action: ALLOW
From: TRUSTED	To: ANY	Applications/Ports: ANY	Action: ALLOW
From: ANY	To: ANY	Applications/Ports: ANY	Action: DENY

Step 2 - Run the Test

1. Choose the appropriate bandwidth
2. Click “Save and Run” on the BreakingPoint Console
3. Once the test is complete, save the results for interpretation (listed in section below).

Stability and reliability are determined in a much simpler manner than the previous tests. Primarily, test scoring is based on whether the firewall blocked what it was supposed to block and remained operational. For all tests regarding stability and reliability testing, the tests must run for the duration of 8 to 72 hours.

Follow these next steps in sequence for data gathering and test scoring:

1. Run the appropriate attack leakage test from the test pack.
1. At various points throughout the test (including after the maximum has been reached), confirm that the firewall is still capable of blocking traffic that is in violation of the currently applied security policy, whilst confirming that legitimate traffic is not blocked. The firewall needs to be able to apply policy decisions effectively based on inspected traffic at all load levels. Any traffic that passes through the device in violation of the firewall policy is an immediate fail. Both the fail and the time to fail should be recorded in Appendix C: Combined Scorecard.
2. After the test has completed, the following test results can be determined from both BreakingPoint and firewall logs/reports.

a. BLOCKING UNDER EXTENDED ATTACK

The firewall is exposed to a constant stream of security policy violations over an extended period of time. The device is configured to block and alert, and thus this test provides an indication of the effectiveness of both the blocking and alert handling mechanisms.

A continuous stream of security policy violations mixed with legitimate traffic is transmitted through the device at a maximum of 100 Mbps for 8 hours with no additional background traffic. This is not intended as a stress test in terms of traffic load (covered in the previous section) - merely a reliability test in terms of consistency of blocking performance.

This test will ramp up connections to 75% of both the average rated NSS NGFW maximum concurrent sessions and connections per second over a four-hour period. The test will then ramp up to the average maximum concurrent sessions (based on 2014 NSS NGFW testing) after the initial four-hour period. The complete test duration will be a minimum of eight hours.

The security component **will remain active for the duration of the test**, constantly evaluating the blocking ability of the device under test while under load. Any allowed security strikes/exploits will result in a FAIL result.

Note: “Application Transaction” counters may not be counted as 100% completed by the end of the test, as the competing devices in the NGFW market may not be able to complete all of the existing TCP/UDP sessions and/or Superflows within the specified ramp down period. The failure to complete all active Superflow iterations and associated application transactions will not be counted as a failure on this test, as the focus is to block all security attacks while the NGFW is under the extended maximum concurrent load conditions. Any variation in the blocking ability of the NGFW under load will result in a FAIL result

The device is expected to remain operational and stable throughout this test, and to block 100 per cent of recognizable violations, raising an alert for each. If any recognizable policy violations are passed - caused by either the volume of traffic or the sensor failing open for any reason - this will result in a FAIL.

b. PASSING LEGITIMATE TRAFFIC UNDER EXTENDED ATTACK

This test is identical to blocking under extended attack, where the external interface of the device is exposed to a constant stream of exploits over an extended period of time.

The device is expected to remain operational and stable throughout this test, and to pass most/all of the legitimate traffic. If an excessive amount of legitimate traffic is blocked throughout this test - caused by either the volume of traffic or the firewall failing for any reason - this will result in a FAIL.

3. **Note:** If a firewall allows traffic to “leak” due to the way it expires old connections, the result will be an FAIL for the entire test.

6.2 Protocol Fuzzing and Mutation

Description	<p>Protocol fuzzing and mutation are determined in a much simpler manner than the previous performance and capacity tests. Primarily, test scoring is based on whether the DUT blocked what it was supposed to block, remained operational, or “Failed Closed” versus “Failed Open”.</p> <p>For all tests regarding protocol fuzzing and mutation testing, the tests must run for the duration of 8 to 72 hours. NGFWs enforce the separation of networks. Therefore should the NGFW fail/crash for any reason it must fail so that no traffic passes through the device (a.k.a. “Fail Closed”).</p> <p>Critical test metrics for these tests are:</p> <ul style="list-style-type: none"> • Pass / Fail for duration • Time to fail or Duration • Fail Open or Fail Close <p>This test stresses the protocol stacks of the DUT by exposing it to traffic from various protocol randomizer and mutation tools.</p>
Test Pack Configuration File(s)	<p>NSS_NGFW_PS8_10G_Stability_72hr_Fuzzer.bpt</p> <p>NSS_NGFW_PS8_20G_Stability_72hr_Fuzzer.bpt</p> <p>NSS_NGFW_PS8_30G_Stability_72hr_Fuzzer.bpt</p> <p>NSS_NGFW_PS8_40G_Stability_72hr_Fuzzer.bpt</p>

Follow these next steps in sequence for data gathering and test scoring:

1. Run the appropriate NSS NGFW Security 72hr Protocol Fuzzer test.
2. “Page 1” will reflect pass or fail on the summary page, but there is more data within the report that may be useful in providing more insight into the firewall sensor and its limitations. Under “Synopsis” and “Summary” the test results for these tests are “Pass / Fail”.

Test Results for 10G x2 - Protocol Fuzzer 7...

1. 10G x2 - Protocol Fuzzer 72Hr

2. Revision History

▼ 3. Synopsis

3.1. Component Description

3.2. Test Criteria

3.3. Summary of Results

4. Table of Contents

▼ 5. Test Environment

5.1. Settings

3.2. Test Criteria

Component	Test Criteria
Stack Scrambler 1-2	Valid ICMP echo requests are periodically sent through the test.: ((pingsSent>=1) and ((pingsSent-pingsReceived)<=5))

3.3. Summary of Results

Component	Test Results	Explanation
Stack Scrambler 1-2	Test passed	
Overall	Test passed	

Figure 18 – Protocol Fuzzer Summary

Note: The BreakingPoint report may report a FAIL based on a loss of pings during the test. It is NSS Labs’ policy that the device will PASS if it is still up and passing traffic at the end of the 72 hour test.

3. **Document results** in the appropriate section of the Scorecard in Appendix C: Combined Scorecard.

Note: For this test to be successfully run, PING must be allowed through the device. If PING is not allowed, the test will report a fail, regardless of how the device performed.

7 Best Practices

It is recommended to review the following best practices prior to beginning any tests.

- When upgrading BreakingPoint to the latest UI version, EACH test that you have previously created or purchased (any .bpt files) must be checked for accuracy, paying close attention to the ramp rate of each test. Ixia may recommend exporting, deleting, and reimporting the tests with each upgrade to the BreakingPoint PerfectStorm chassis. Confirm all tests are configured properly based on byte size of packet with the overall capacity of the firewall sensor, or the test will ramp too slowly and fail due to either too much time to maximize traffic; or a ramp time that is too quick and is perceived as a potential flood attack.
- Consistency of network, firewall(s), and test components is critical to ensuring proper scoring and evaluation.
- Device Upgrade Considerations - When upgrading your current firewall from a known stable release to a new release, it is recommended that performance impact be taken into consideration as part of the migration process. Software or firmware revisions, along with signature or security updates, may have a negative impact on the total performance of the firewall. This impact may manifest itself in a number of ways, including increases in the latency of packets traversing the firewall or the overall HTTP transaction performance/application response time. This test pack can be utilized to benchmark all firewall performance metrics pre- and post-upgrades as well as against vendor-stated performance metrics and to gain valuable insight into potential impacts (if any exist). This test pack can also assist with firewall best practices, fitness for purpose, and ongoing management considerations.

8 Frequently Asked Questions

The following FAQs are organized by general topic and then by specific questions for quick navigation:

Purpose of the Test

Q: What is the purpose of this test?

A: To effectively understand and manage NGFW for proper protection.

Physical Setup

Q: What is the chassis?

A: The chassis refers to the physical Ixia PerfectStorm device and the ports for each card that must be configured to the NGFW prior to testing.

The BreakingPoint User Interface

Q: Why are components of my Network Neighborhood using same words for different meanings?

A: Some confusion may be evident for the use of “Interface” regarding port/pairs as well as for a “user interface,” but for clarity, “interface” generally refers to the chassis port on the chassis.

Q: Why can’t I find my Network Neighborhood?

A: If a Network Neighborhood was properly created and saved, it will be found under the dropdown menu list for “Network Neighborhood”. You may always use the Network Neighborhood included with the test pack or one of the default BreakingPoint Network Neighborhoods.

Q: Why am I having problems with my browser when using BreakingPoint?

A: It is recommended that you clear the browser cache prior to running BreakingPoint tests.

Q: Where do I input our specific IP addresses for the Test?

A: Under Network Neighborhood.

Understanding Test Interfaces

Q: What is a *test interface*?

A: Each test interface in the Network Neighborhood corresponds to a data port on the chassis. When you add an interface to a Network Neighborhood, the system will automatically number the interface based on the order in which it was added. If you delete any of the interfaces, the system will automatically re-sequence the interfaces. The succeeding interfaces (following the deleted interface) will be renumbered to the preceding interface’s value (e.g., “6” will become “5”)

Q: How do I add a test interface?

A: Perform the following steps to add a test interface:

- Select Control Center > Network Neighborhood from the Menu bar.
- Select a Network Neighborhood from the Network Neighborhoods list.
- Click the Add Row button.

Understanding Ports

Q: What are port mappings?

A: Port mappings map ports on the BreakingPoint to an interface in the Network Neighborhood.

Q: What is the purpose behind port mappings?

A: Port mappings allow you to virtually “rewire” your port connections without having to physically enter the lab to do it yourself.

Port Reservations

Q: Do I have to reserve ports in order to run a test?

A: Yes. You must have locked port reservations if you want to run a test. If you are running a test that uses a non-VLAN Network Neighborhood, then you must lock at least two port reservations. However, if you are running a test that uses a VLAN-enabled Network Neighborhood, then you only need one locked port reservation.

Q: What is the difference between a locked port reservation and a regular port reservation?

A: A locked port reservation provides you with the ability to run tests and export packet buffers from the ports. A regular port reservation simply reserves the port under your account; no other users can use these ports, however, there’s not much you can do with these ports until you have locked the reservation on them. To lock a port’s reservation, simply click on the port. All ports that have locked reservations under your account will have a key icon displayed over them.

Q: Another user has a slot reserved. How can I reserve those ports for myself?

A: If you click on a reserved port, the system will ask you if you would like to force reserve the port. If you click Yes, the system will reserve all ports on that slot under your account, while lock reserving the port you clicked on.

Q: What is the difference between a port that has a lock icon and a port that has a key icon?

A: A port that has a lock icon has been reserved by another user. A port that has a key icon is reserved by you.

Port Settings

Q: For the BPS-10K and BPS-1K, I was able to manually set the port speed. Can I manually set the port speed for the BreakingPoint?

A: Yes. From the Device Status screen, you can right-click on a port and select Configure Port. From here, you can select a port speed that is available from the Speed Settings drop-down box.

Q: Can I change the port mappings?

A: Yes, you can change the port mappings from the Device Status screen. First, select the Active Group whose ports you want to modify, and then click on the Open port mapping options button. From this screen, you use the drop-down buttons located under each interface to change the port/slot mapping.

Q: Why is [RUN] or [SAVE and RUN] not working?

A: It is possible the port pairs/Interfaces on the chassis are not setup properly.

Q: Why is my test failing while it is running before it has finished?

A: The first indicator of a failed test is the NGFW is firing false positives as soon as the tests begin to run.

A: The resources of the NGFW are exhausted and it is dropping traffic.

Q: What are the main items to monitor during my NGFW test that I should monitor?

A: Monitor the “Summary” Tab and monitor “Tx” and “Rx” to note the absence of False Positives and that traffic is actually running into the NGFW.

Q: Why does “Interface” error keep popping up when I run a test?

A: Within Network Neighborhood, EVEN FOR PRE-DEFINED and SAVED TESTS, one must also double check the Interface in order for NULL / full / real values and parameters to be established which would prevent the test from properly running.

Q: How do I find my test results?

A: After a test is run, there will be a pop-up for quick results. However, the test report will be an icon for a PDF at the top right of the final page/screen of the test.

Q: How can I tell if my TEST is failing versus my NGFW is failing?

A: Connect the BreakingPoint chassis in “back to back” mode such that the sending interface is connected to the receiving interface with no product in the middle. Rerun the test and confirm it meets the objectives defined. If it does not, please contact Ixia support to confirm the modifications you have performed have not broken the test. If the test meets the objectives, then the NGFW is failing.

Reporting Questions

Q: How is a flow defined?

A: A flow includes both UDP and TCP flows.

Q: What is the difference between a flow and a connection?

A: In the report, a flow is counted when a packet is sent on a particular 5-tuple, regardless of whether an actual TCP connection is established or not. A connection, on the other hand, is counted only when a finishing handshake has created a new connection.

Q: Do you track UDP connections?

A: No. Since UDP flows are stateless, only statistics for UDP flows are posted.

Q: Can I email test reports to myself?

A: Yes. If you go to the Administration area and select the My Preferences tab, you will see an option called Email Test Results. If you enable this option and then select a format from the Default Report Format drop-down menu, the system will email the report to you.

Q: What is the difference between connections per second (cps) and sessions per second (sps)?

A: Connections per second refers to only the rate at which sessions are opened. Sessions per second refer to the rate at which sessions are opened, data is sent, and closed.

Q: Why does the Traffic Overview section of the report for my RFC 2544 test show that it has received slow start packets at every data rate?

A: BreakingPoint will send slow start packets in the reverse direction to the NGFW for each iteration, enabling the NGFW to identify the MAC addresses used by BreakingPoint.

Q: I am trying to view several multi-box reports at once; however, after I open five reports, my browser will not load any additional reports. Is there a limitation on the number of reports I can have open?

A: There are no limitations on the number of reports you can have open; however, the number of reports you can view at a time may be restricted by the web browser you are using. Therefore, we recommend that you do not open more than five multi-box test reports at a time. If you experience any problems after you have attempted to open multiple reports, you should log out of the Control Center and log back in again.

Q: Why is my report missing the Ethernet Data Rates section?

A: Either the test duration was not long enough or there were not enough frames transmitted for the Ethernet Data Rate to be calculated. To get results for the Ethernet Data Rate, try increasing the duration of the test (either in frames or in seconds).

Q: What email server is used to send our reports?

A: BreakingPoint will act as a mail server. It retrieves the IP address of the SMTP server via DNS. It will use the DNS server and hostname you specified during the initial configuration of the system.

To see what your DNS server and hostname settings are, telnet to the chassis. After you log into the box, use the networkInfo command to display the network configuration for the BreakingPoint.

To edit the network information, use the updateNetwork command and any of the following options - hostname <dhcp hostname>, -ip <IPaddress>, -netmask <netmask>, -gateway <gateway IP address>, -dns1 <DNS server>, -dns2 <DNS server>, and -dns3 <DNS server>.

Test Questions

Q: How many tests can I run concurrently?

A: The number of tests that you can run concurrently depends on the number of ports you have on your BreakingPoint. For example, if your BreakingPoint has 8 ports, you can run 8 tests at a time; if you have 16 ports, then 16 tests can run simultaneously.

Q: How do I run a test without saving the changes I have made to the test?

A: You can run a test without saving your changes by selecting Test > Run from the Menu bar. However, after you run the test, you can click the Edit button on the Real-Time Statistics window to return to the saved version of the test. Any changes that you made prior to running the test will be restored to their saved settings.

Q: How can I delay the start of a test component?

A: Each component has a parameter called Delay Start that enables you to delay the start of a test component by the time specified. This parameter is measured in seconds and supports floating values.

Q: I am trying to run a test, but the run functionality is disabled. Why is this happening?

A: The ports you are trying to use are in use by another user. You may want to remap your ports on the Device Status page, or wait until the user has finished using the ports. This can also occur if you do not have any ports reserved. Functionality can also become disabled if the test you are attempting to run is invalid due to oversubscribing (for example, if you are attempting to run a 10 Gb test on a 1 Gb blade).

Test Component Questions

Q: Can components be run at the same time?

A: All test components can be executed with a single test. Tests can contain multiple occurrences of a test component, but bandwidth and hardware resources will affect the number and type of test components that can be added to a test.

Q: How many occurrences of each test type of component does a test support?

A: Session Sender, Application Simulator, and Recreate support up to 8 components per test. Security and Stack Scrambler support 4 components per chassis. Bit Blaster and Routing Robot support up to 4 components per port.

9 Appendix A: Change Log

Document Revision	Date	Changes/Comments
1.0	June 24,2015	Test Pack updated to reflect NGFW v6.0 Methodology.

10 Appendix B: About This Test

Test Pack Name: NSS Test Pack – Next Generation Firewall 1.0

Test Pack Creation Date: June 24, 2015

Test Pack Based On: NSS Next Generation Firewall: Test Methodology v6.0

BreakingPoint Details: IXIA BreakingPoint PerfectStorm software version 3.4.0
Product Build 230019, (ATI 231337).

11 Appendix C: Combined Scorecard

Security Effectiveness	
NGFW Policy Enforcement	
Baseline Policy	PASS/FAIL
Simple Policy	PASS/FAIL
Complex Policy	PASS/FAIL
Static NAT	PASS/FAIL
Dynamic / Hide NAT	PASS/FAIL
SYN Flood Protection	PASS/FAIL
Address Spoofing Protection	PASS/FAIL
TCP Split Handshake	PASS/FAIL
Performance	
UDP Throughput	Mbps
64-Byte Packets	0
128-Byte Packets	0
256-Byte Packets	0
512-Byte Packets	0
1024-Byte Packets	0
1514-Byte Packets	0
Latency - UDP	
64-Byte Packets	0.0
128-Byte Packets	0.0
256-Byte Packets	0.0
512-Byte Packets	0.0
1024-Byte Packets	0.0
1514-Byte Packets	0.0
Connection Dynamics - Concurrency & Connection Rates	
Theoretical Max. Concurrent TCP Connections	0
Theoretical Max. Concurrent TCP Connections w/Data	0
Maximum TCP Connections Per Second	0
Maximum HTTP Connections Per Second	0
Maximum HTTP Transactions Per Second	0

HTTP Connections per Second & Capacity	CPS
2,500 Connections Per Second – 44-Kbyte Response	0
5,000 Connections Per Second – 21-Kbyte Response	0
10,000 Connections Per Second – 10-Kbyte Response	0
20,000 Connections Per Second – 4.5-Kbyte Response	0
40,000 Connections Per Second – 1.7-Kbyte Response	0
HTTP Average Application Response Time	
2,500 Connections Per Second – 44-Kbyte Response	0
5,000 Connections Per Second – 21-Kbyte Response	0
10,000 Connections Per Second – 10-Kbyte Response	0
20,000 Connections Per Second – 4.5-Kbyte Response	0
40,000 Connections Per Second – 1.7-Kbyte Response	0
HTTP Connections per Second & Capacity with Delays	CPS
5,000 Connections Per Second – 21-Kbyte Response with Delays	0
10,000 Connections Per Second – 10-Kbyte Response with Delays	0
“Real World” Traffic	
“Real World” Protocol Mix (Enterprise Perimeter)	0
“Real World” Protocol Mix (Financial)	0
“Real World” Protocol Mix (Education)	0
“Real World” Protocol Mix (Datacenter)	0
“Real World” Protocol Mix (US Mobile Carrier)	0
“Real World” Protocol Mix (EU Mobile Carrier)	0
Stability & Reliability	
Blocking Under Extended Attack	PASS/FAIL
Passing Legitimate Traffic Under Extended Attack	PASS/FAIL
Protocol Fuzzing & Mutation	PASS/FAIL
Power Fail	PASS/FAIL
Redundancy	YES/NO/OPTIONAL
Persistence of Data	PASS/FAIL