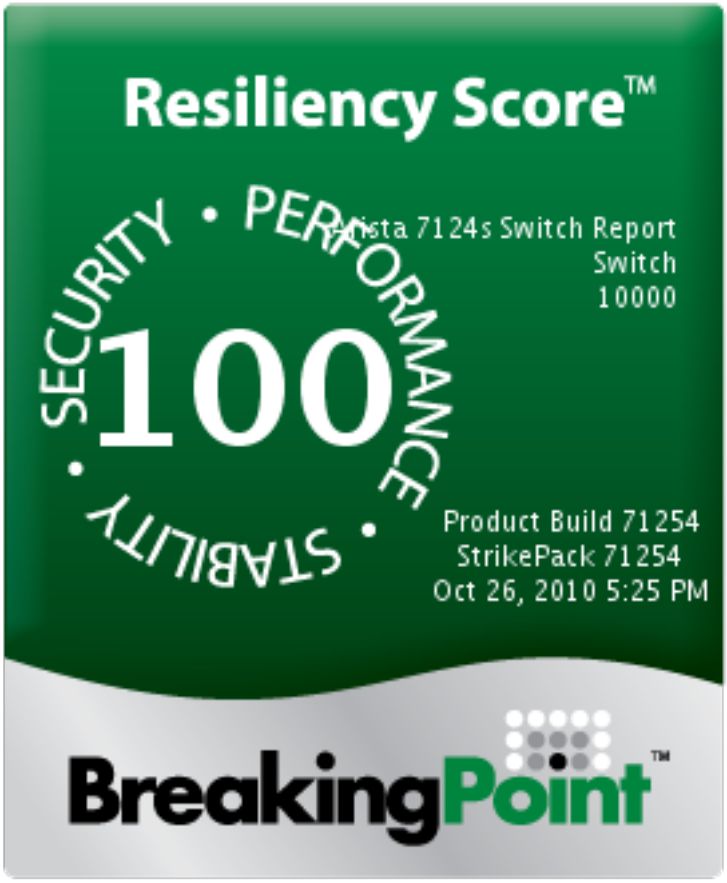
1. Arista 7124s Switch Report



2. Synopsis

	Lab	Real	Session Stress	Session Rate Stress
Throughput	64: 100.00 1518: 100.00	Rate: 100.00		
Sessions	Count: 100.00 Rate: 100.00	Count: 100.00 Rate: 100.00		
Robustness	IP: pass UDP: pass TCP: pass			
Security	pass	pass	pass	pass
Overall Score	99.99981			

Throughput

Scores are determined by a device's ability to handle large amounts of simulated realistic network traffic.

Sessions

Measures a device's ability to handle large numbers of TCP sessions and the rate at which it handles them.

Robustness

Measures a device's ability to correctly handle malformed traffic at different IP layers.

Security

Measures a device's ability to correctly block exploit traffic with and without background network traffic.

Overall Score

A blended average of all sub-tests. This number represents the overall score relative to expected performance for the resiliency test.

2.1. Score Calculation

Overall Score
Calculation:(A(99) + B(99) + C(100) + D(100) + E(100) + F(100) + G(100)) / 7
Overall Score = 100.00

Throughput
A) IEEE Throughput measurement of 64 byte frames
A = (100 X Throughput Achieved[w/64]) / Max Wireline Throughput
= (100 X 9999) / 10000
Score = 99
B) IEEE Throughput measurement of 1518 byte frames
B = (100 X Throughput Achieved[w/1518]) / Max Wireline Throughput
= (100 X 9999) / 10000
Score = 99
C) Throughput, Simulated Real World Conditions
C = (100 X Application Frames Rate) / Max Application Frames Rate
= (100 X 1860470) / 1500000
Score = 100

Sessions
D) Concurrent IETF 793 TCP Connections
D = (100 X Number Flows) / Max Number Flows
= (100 X 10000000) / 10000000
Score = 100
E) Concurrent IETF 2581 TCP and IETF 768 UDP Connections
E =(100 X Number Flows) / Max Number Flows
= (100 X 10065601) / 10000000
Score = 100
F) IETF 793 TCP Connections/sec
F = (100 X Flow Rate / Max Flow Rate
= (100 X 246705) / 150000)
Score = 100
G) IETF 2581 TCP and IETF 768 UDP Connections/sec
G = (100 X Flow Rate) / Max Flow Rate
= (100 X 150688) / 100000
Score = 100

Robustness
H) IETF 791 IP Stack Stability
H = Dropped Pings
Score = pass
I) IETF 768 UDP Stack Stability
I = Dropped Pings
Score = pass
J) IETF 793 TCP Stack Stability
J = Dropped Pings
Score = pass

Security

Security
K) CVE Security Fault Injection, Independent
K = Dropped Pings
Score = pass
L) CVE Security Fault Injection, Benign
L = Dropped Pings
Score = pass
M) CVE Security Fault Injection, Concurrent Sessions Stress
M = Dropped Pings
Score = pass
N) CVE Security Fault Injection, Session Rate Stress
N = Dropped Pings
Score = pass

2.2. Throughput

Scores are measured using traffic run separately with contrived data, in order to establish a baseline of performance for the device.

Network Packet Stress

This test will be repeated once with 64 byte and again with 1518 byte packets. These two packet sizes represent the smallest and larget valid packet size for a single network frame. The test begins by transmitting packets at half of the theoretical maximum rate for the given packet size. Any dropped or corrupted packets result in a failed iteration. Testing continues iterating in a binary search pattern; for each iteration testing at a rate halfway between the last passed test and the last failed test, until a maximum successful rate is found.

Benign Realistic Network Packets

This test will utilize application traffic representing a blend of realistic protocols that are high consumers of network bandwidth. The test begins by transmitting packets at half of the theoretical maximum rate for the given packet size. Any dropped or corrupted packets result in a failed iteration. Testing continues iterating in a binary search pattern; for each iteration testing at a rate halfway between the last passed test and the last failed test, until a maximum successful rate is found.

2.3. Sessions

Scores are measured using a blend of mixed traffic in order to simulate real world conditions.

TCP Sessions Stress

This test utilizes a selection of application traffic representing protocols observed in a real enterprise network. The test begins by opening a single TCP session. Every 5 seconds, 1500 additional TCP sessions are attempted, up to a maximum of 10,000,000 concurrent TCP sessions. Once completed, an analysis is made to determine the achieved concurrent sessions based on the measured number of active concurrent TCP sessions.

Benign Realistic Network Sessions

This test begins by opening a single TCP session, which remains open for the duration of the test. Every 5 seconds 1500 additional TCP sessions are attempted, up to a maximum of 10,000,000 concurrent TCP sessions. Once completed, an analysis is made to determine the achieved concurrent sessions based on the measured number of active concurrent TCP sessions.

2.4. Robustness

Measures a device's ability to correctly handle malformed traffic at different IP layers.

IP Robustness

This test limits the scope of random testing to Layer 3 by randomizing portions of the IP header (specifically, IPv4.) Packets will have random payload ranging in size from 46 to 1500 bytes, and will be transmitted at a rate between 2000 and 2500 packets per second. Data will be transmitted for at least one hour, for a minimum of 5,000,000 distinct packet configurations. The data to be randomized will include the IP Version, IP Options, the number of IP fragments, the Urgent pointer, and the IP checksum.

UDP Robustness

This test limits the scope of random testing to Layer 4, specifically targeting the UDP protocol by randomizing portions of the UDP header in addition to the IP header. Packets will have random payload ranging in size from 46 to 1500 bytes, and will be transmitted at a rate between 2000 and 2500 packets per second. Data will be transmitted for at least one hour, for a minimum of 5,000,000 distinct packet configurations.

TCP Robustness

This test limits the scope of random testing to Layer 4 by randomizing portions of the TCP header in addition to the IP header. Packets will have random payload ranging in size from 46 to 1500 bytes, and will be transmitted at a rate between 2000 and 2500 packets per second. Data will be transmitted for at least one hour, for a minimum of 5,000,000 distinct packet configurations.

2.5. Security

Measures a device's ability to correctly block exploit traffic with and without background network traffic.

Security - Laboratory conditions

This test only sends exploit related traffic. Device score is measured by ensuring that all packets carrying malicious payloads are blocked or neutered.

Security - Benign Realistic Conditions

This test has a stream of representative realistic traffic in the background, in addition to the exploit traffic. The realistic traffic should represent approximately 50% of the capabilities of the device as measured in the performance baseline.

Security - Concurrent Sessions Stress Conditions

This test has as a stream of representative realistic traffic in the background, in addition to the exploit traffic. The realistic traffic should represent approximately 95% of the maximum number of concurrent connections of the device as measured in the performance baseline.

Security - Session Open Rate Stress Conditions

This test has a stream of representative realistic traffic in the background, in addition to the exploit traffic. The realistic traffic should represent approximately 95% of the maximum session open rate of the device as measured in the performance baseline.

2.6. Settings

Setting	Value
Speed	10.00 Gigabits
Device Type	Switch
Run Type	Full
Session Rate	yes
Robustness	yes
Throughput	yes
Security	yes

2.7. Network Configuration

Client Configuration	Client Routing	Server Routing	Server Configuration
Network:10.0.0.0/23 Min:10.0.0.2 Max:10.0.0.254	DUT Address:10.0.0.1 Network:10.0.0.0/23	DUT Address:10.0.0.1 Network:10.0.0.0/23	Network:10.0.0.0/23 Min:10.0.1.1 Max:10.0.1.254