Benchmarking Methodology for Network Security Device Performance

draft-ietf-bmwg-ngfw-performance-00

IETF104 / Prague / 2019-03-27

B. Balarajah, C. Rossenhoevel, B. Monkman

Draft Updates since IETF 103

- Merged both HTTP and HTTPS transaction per second test cases with throughput test
  - PoC tests showed there is no separate test run needed to measure both KPIs
- Added more SUT features, including security features
- Improved test procedures based on PoC test experience
  - Executable and reproducible test procedure
- Defined TCP stack parameters
  - Congestion window size, delayed ack and windows size
- Exact parameterization enabled test automation

Draft Comparison with RFC 3511

Test Setup	RFC 3511	Draft-ietf-bmwg-ngfw-performance
Test traffic requirements	• Not defined	• Object size • Traffic mix • Cipher suite(s) … defined for individual test cases

Draft Comparison with RFC 3511

Test Setup	RFC 3511	Draft-ietf-bmwg-ngfw-performance
Test traffic requirements	• Not defined	• Object size • Traffic mix • Cipher suite(s) … defined for individual test cases
Rule set	• Recommend to use rule set depending on the capabilities of the DUT/SUT • Number and type of rules are not defined	• Recommended to configure a realistic number of rule set • Determined the rule set for four different classes of DUT/SUT • Defined multiple layer of rules

Draft Comparison with RFC 3511

Test Setup	RFC 3511	Draft-ietf-bmwg-ngfw-performance
Test traffic requirements	• Not defined	• Object size • Traffic mix • Cipher suite(s) … defined for individual test cases
Rule set	• Recommend to use rule set depending on the capabilities of the DUT/SUT • Number and type of rules are not defined	• Recommended to configure a realistic number of rule set • Determined the rule set for four different classes of DUT/SUT • Defined multiple layer of rules
TCP stack consideration	• Not specified, but required to be documented	Specified: • Maximum Segment Size • TCP window size • Initial congestion window • TCP retry • TCP port range

Draft comparison with RFC 3511 (continued)

Test Setup	RFC 3511	NetSecOpen Test Methodology
Test validation criteria (Pass/Fail criteria)	• Single criterion per test case	• Multiple criteria per test case
SUT features covered	• Web Cache • Network Address Translation • Authentication	• SSL inspection • Intrusion detection and prevention • Antivirus • Anti Spyware • Anti Botnet • Logging and Reporting • Application Identification

NGFW PoC Testing Program

- Goal 1: Validate that test procedures produce accurate results
- Goal 2: Ensure that results are comparable independent of tool used for testing (conducted tests with two commercial test tools)

- Started in October 2018
- Two labs, two tool vendors, four firewall vendors participating
- Initial results available internally, being reviewed

Comparison of PoC Testing Results with Vendor Datasheet

Test Case	Vendor Datasheet	Draft-ietf-bmwg-ngfw-performance	Result Comparison
Throughput	• HTTP with 64 KB transaction • IPS, antivirus, vendor-specific anti-spyware, vendor-specific malware analysis and logging enabled	• HTTP with 10x 64 KB transactions per TCP connection • Antivirus, Anti-spyware, vulnerability protection, botnet protection and logging enabled	IETF-NGFW test result 40 % higher than vendor datasheet

Comparison of PoC Testing Results with Vendor Datasheet

Test Case	Vendor Datasheet	Draft-ietf-bmwg-ngfw-performance	Result Comparison
Throughput	• HTTP with 64 KB transaction • IPS, antivirus, vendor-specific anti-spyware, vendor-specific malware analysis and logging enabled	• HTTP with 10x 64 KB transactions per TCP connection • Antivirus, Anti-spyware, vulnerability protection, botnet protection and logging enabled	IETF-NGFW test result 40 % higher than vendor datasheet
Session Capacity	No parameters provided	• HTTP with 10X 1 KB transactions per TCP connection with think time in between • Same features to be configured as before	Results identical

Comparison of PoC Testing Results with Vendor Datasheet

Test Case	Vendor Datasheet	Draft-ietf-bmwg-ngfw-performance	Result Comparison
Throughput	• HTTP with 64 KB transaction • IPS, antivirus, vendor-specific anti-spyware, vendor-specific malware analysis and logging enabled	• HTTP with 10x 64 KB transactions per TCP connection • Antivirus, Anti-spyware, vulnerability protection, botnet protection and logging enabled	IETF-NGFW test result 40 % higher than vendor datasheet
Session Capacity	No parameters provided	• HTTP with 10X 1 KB transactions per TCP connection with think time in between • Same features to be configured as before	Results identical
Connections per second	• 1-byte HTTP transactions • Classification of applications suppressed	• HTTP with 1x 1 KB transaction per TCP connection	IETF-NGFW yields 50 % of the vendor datasheet numbers

Comparison of PoC Testing Results with Vendor Datasheet: Further Findings

- False Positives
  - Both SUT and test tool vendors needed to fine-tune their configurations
- Multiple iterations of manual test runs needed for troubleshooting
  - All test cases must be successfully pre-staged before automation is started
- Test validation criteria for latency was critical
  - 10 % of delay variation as test validation criteria was too low for lab test environment

Next Steps

- Continue to review and revise the (relatively stable) draft
  - Focusing security effectiveness tests
  - Focusing traffic profiles
- Prepare open certification program in NetSecOpen group
  - Define fair and transparent rules
  - Work with multiple labs and multiple test tool vendors
- Elaborate open source implementation of NGFW methodology
  - Realistic configurations are complex and overwhelming for open source test tools
  - Open source groups are invited to participate in PoC testing!