Next-Generation Firewall Performance Benchmarking Methodology Draft

draft-balarajah-bmwg-ngfw-performance-02
IETF 101, London, March 20, 2018

Bala Balarajah / Carsten Rossenhövel

Goals

- Provide benchmarking terminology and methodology for next-generation network security devices including
  - Next-generation firewalls (NGFW)
  - Intrusion detection and prevention solutions (IDS/ IPS)
  - Unified threat management (UTM)
  - Web Application Firewalls (WAF)
- Strongly improve the applicability, reproducibility and transparency of benchmarks
- Align the test methodology with today's increasingly complex layer 7 application use cases

Projected Use Cases

Enterprises

- Perimeter Firewall
- Web Application Firewall
- Industrial and IoT Firewall
- Next Generation Intrusion Detection/Prevention System (IDS/IPS)
- Remote Services/VoIP Firewall
- Unified Threat Manager

Telecom Service Providers

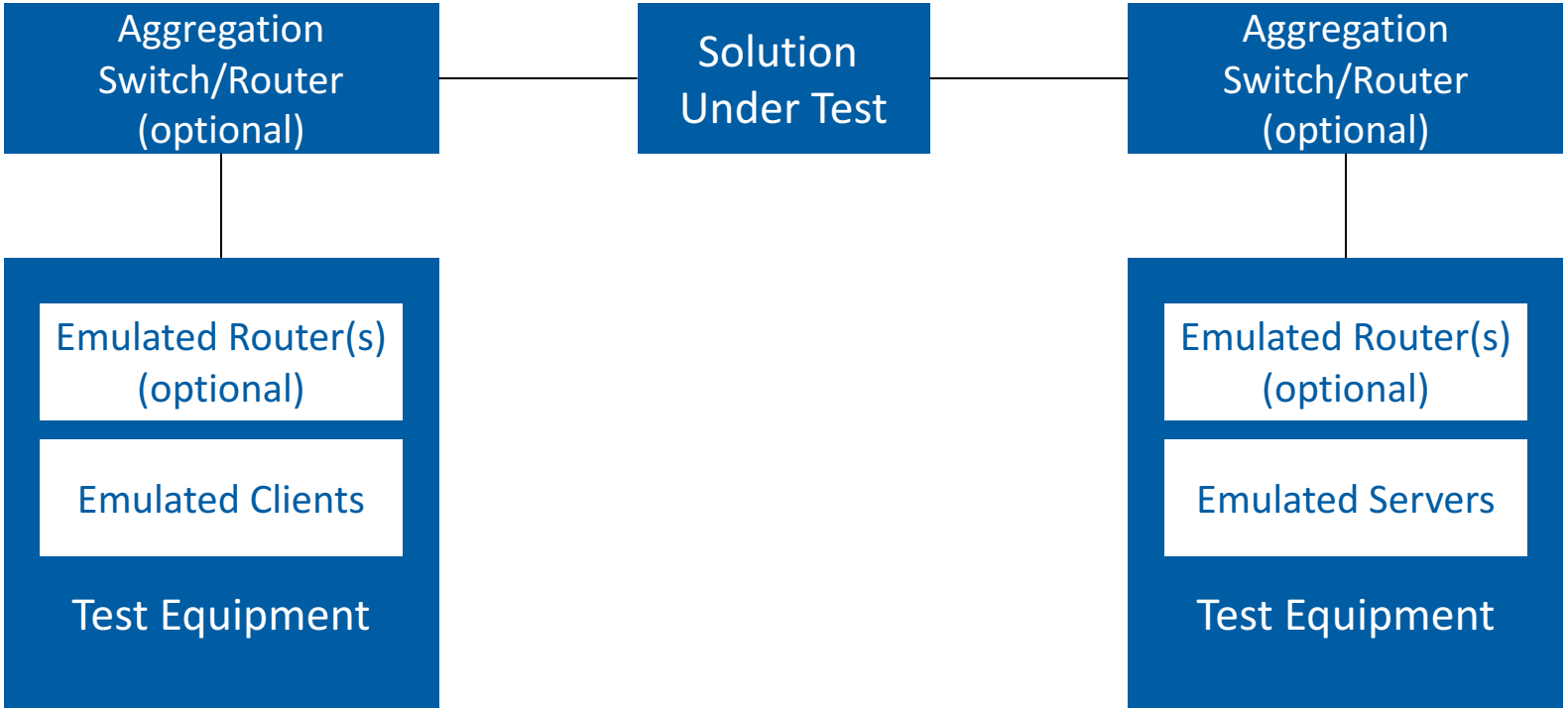
- Business VPN Service Firewall, IDS and UTM
- Mobile Core and Roaming Firewall
- Residential Customers Protection
- Network Management Perimeter Firewall, IDS/IPS
- Application Services, Web Portal Firewall

(most use cases with virtualized implementations)

Test Areas

- Benchmarking Tests
  - HTTP, HTTPS Throughput Performance With NetSecOPEN Traffic Mix
  - Concurrent TCP, SSL/TLS Connection Capacity With HTTP Traffic
  - HTTP, HTTPS Transactions Per Second
  - HTTP Transaction Latency
  - SSL/TLS Handshake Rate
- Security Effectiveness Tests
  - Test of Attack Vectors (aligned with NIST and other vulnerability databases)

Test Setup – Lab Environment



Feature Profiles

	NGFW Initial	NGFW Future	NG-IPS	AD	WAF	BPS	SSL Broker
SSL Inspection	x						
Intrusion (IPS/IPS)	x						
Web Filtering		X					
Antivirus	x						
Anti Spyware	x						
Anti Botnet	x						
DLP		x					
DDoS		x					
Certificate Validation		x					
Logging and Reporting	x						
App Identification	x						

Key Performance Indicator (KPI) Definitions

- TCP Concurrent Connections
- TCP Connection Setup Rate
- Application Transaction Rate
- TLS Handshake Rate
- Throughput
- URL Response Time, Time To Last Byte (TTLB)
- Application Transaction Time
- Time To First Byte (TTFB)
- TCP Connect Time
- … more to come

7.1: Throughput Performance With Traffic Mix

Objective: Determine the average throughput performance of the system under test when using application traffic mix

Variable test parameters

- Number of clients and servers
- IPv4/v6 traffic distribution
- Initial and target throughput

Test Procedure: Run with initial, then target objective; iteration with binary search

Test Results Acceptance Criteria

- Failed application transaction rate < 0.01 %
- Unexpected TCP RST < 0.01 %
- Max TTLB deviation < X
- Max TCP connect time < Y; max TTFB < 2 * Max TCP connect time

7.2: Concurrent TCP Connection Capacity With HTTP Traffic

Objective: Determine the maximum number of concurrent TCP connections the SUT sustains when using HTTP traffic

Variable Test Parameters

- As before, plus:
- HTTP object size 10 KBytes
- Test to be conducted at 25 % maximum throughput

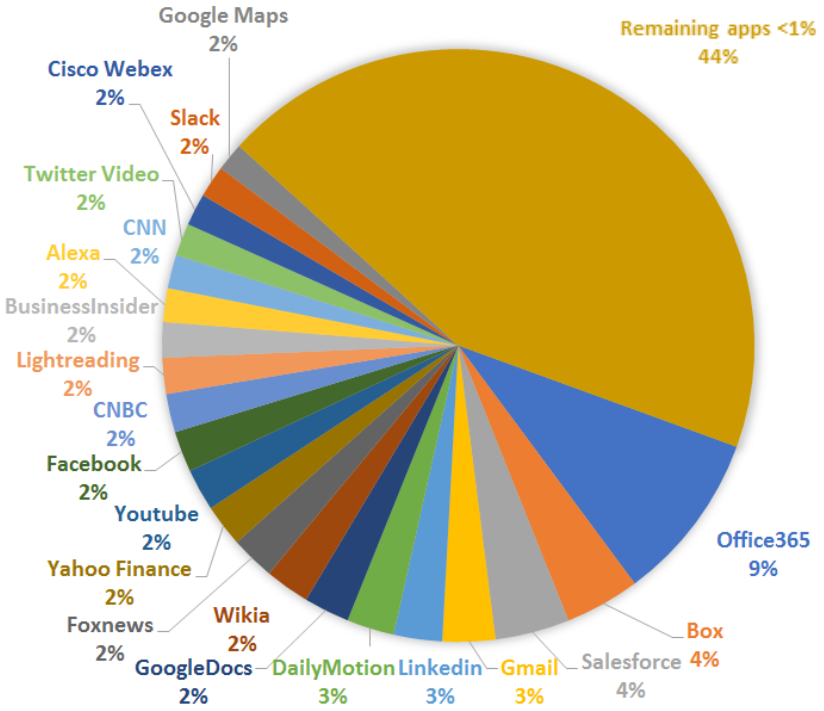
Test Procedure: Run with initial, then target objective; iteration with binary search

Test Results Acceptance Criteria

- Consistent with test case 7.1

Traffic Mix

- Modern Enterprise Perimeter Traffic Mix for Firewall, IPS and NGFW tests
- Blend of 70% HTTPS and 30% HTTP
- Over 10,000 unique URLs and approximately 1,000 FQDNs
- Approximately 400 unique Certs
- Future traffic mixes will be developed that represent specific industry verticals and/or use cases
- Already implemented in at least one emulator



Source: netsecopen.org

Proposed Schedule

Draft	Date	Changes
03	2018-03-05	Added test case 7.2
04	2018-03-21	Add traffic mix annex, test cases 7.7/7.8
05	2018-04-15	Add test cases 7.3-7.6
06	2018-06-01	Add security effectiveness sections
07	2018-06-30	Modifications resulting from PoC testing
08	2018-07-02	Stable draft to be submitted

Outlook: NetSecOPEN Certification

- Non-profit, membership driven organization
- Lead a continuing collaborative effort between network security vendors, tool vendors, labs and enterprises to create open and transparent testing standards in the area of network security
- NetSecOPEN certification testing will be conducted by NetSecOPEN accredited test labs using NetSecOPEN approved test tools
- All testing will be conducted in an open and transparent manner
- Testing requirements will not be changed arbitrarily
- Certified products will be listed on the NetSecOPEN website. All reports and supporting documentation will be freely available to the public

Request for Action

- Please review
  - More test cases with every draft version
- Please contribute
  - Specifically new traffic mixes (SP, web application firewall)
  - Security effectiveness test methods

Thank you for your interest!

For further information, please contact the authors:

Carsten Rossenhoevel – cross@eantc.de
Bala Balarajah – balarajah@eantc.de

FAQs

1. Do you have any public cloud traffic (Amazon EC2, Azure, Google Cloud etc.) included in this mix?
   - The FQDN list in the traffic mix includes some AWS and Azure FQDNs
   - No specific packet sizes have been selected for cloud traffic
2. What about non-HTTP traffic such as SSH/SSL, IPsec VPNs?
   - These are not included because they are insignificant in volume for a typical NGFW deployment with office clients connecting to the internet
   - The traffic mix does not cover intranet applications based on other legacy protocols that don't go to the internet
   - Adding more protocols would increase complexity and make it harder to achieve reproducible results across test tools

FAQs

3. Are alternative transport protocols such as Google QUIC already covered?
   - Most enterprises block QUIC in order for HTTPS visibility and security controls to work without changes
   - Test tool support for QUIC is limited today
   - QUIC could be included in a traffic mix for service provider firewalls
4. Why is Microsoft Office 365 traffic the biggest share of the traffic mix?
   - It's a popular application which consumes a significant portion of bandwidth at enterprises.
5. What SUT detection/inspection mechanisms does the traffic mix support?
   - FQDN, HTTP HOST, TLS SNI, TLS Cert Subject Common Name and Partial URL Path detection

FAQs

6. Overall, what is the projected life time of the traffic mix? How often will it need to be updated in the RFC to stay relevant?
    - While almost a year old, the mix is still first of its kind in stressing all the described parameters of NGFWs including logging, profiling and by app decisions as block or inspect.
    - Vendor feedback so far has been no mix is truly realistic but if every one tests with the same mix the comparison is better and closer to real NGFW throughout numbers vs. single large HTTP transaction performance numbers typically found on datasheets.