논문 2011-2-8

RFC 3511방화벽 성능측정 방법론 분석

정연서*

Analysis of Benchmarking Methodology for Firewall Performance(RFC 3511)

Youn-Seo Jeong*

요 약

IETF에서는 여러 영역으로 나누고 주제별로 WG과 BOF를 구성하여 인터넷 표준규격을 개발하여 배포하고 있다. BMWG 워킹그룹에서는 인터네트워킹, 네트워크 장치, 시스템, 서비스 등의 품질특성, 측정과 관련된 다수의 권고안들을 제정하고 있다. RFC 3511은 4개(전송, 접속, 지연, 필터링)영역에서 10개의 방화벽 성능시험 항목을 다루고 있으며, 해당표준(RFC 3511)은 방화벽 성능측정시 가이드 라인으로 활용할 수 있다. 본 논문에서는 RFC 3511을 시험방법들을 분석하고, IP throughput, concurrent connection, connection throughput 항목에 대하여 시험을 실시하고 결과를 분석하였다.

Abstract

The Internet Engineering Task Force (IETF) develops and promotes Internet standards(a guideline, standards specification, etc). The IETF is organized into a large number of working groups and informal discussion groups (BoF)s, each dealing with a specific topic. The Benchmarking Methodology Working Group (BMWG) will continue to produce a series of recommendations concerning the key performance characteristics of internetworking technologies, or benchmarks for network devices, systems, and services.

RFC 3511 discusses and defines a number of tests that may be used to describe the performance characteristics of firewalls. It covers ten items in four areas: forwarding, connection, latency and filtering. We can use this standard as a guideline to make an objective evaluation for the performance of firewalls. In this paper, we discussed testing methodologies of RFC 3511. And then examined the IP throughput and the concurrent connections for Firewall. We also tested TCP connection throughput.

한글키워드 : 성능측정, 방화벽

1. 서 론

IETF(Internet Engineering Task Force)는 인터넷 표준규격을 개발하고 있는 미국 IAB(Internet Architecture Board) 산하의 위원회이다. IETF에서는 구현에 필요한 표준을 제정하고 문서를 발행하고 관리하기 위한 정기적인 회의를 개최하고 있다. 이러한 문서들을 RFC

* 한국전자통신연구원 (교신저자)
(email: jys847@etri.re.kr)
접수일자: 2011.10.24 수정완료: 2011.11.26

(Request For Comments)라고 지칭되며 고유의 번호를 부여하여 관리하고 있다. 현재 활동 중인 주요 영역으로는 Applications Area, Internet Area, Operations and Management Area, Real-time Applications and Infrastructure Area, Routing Area, Security Area, Transport Area 영역(area)이 있으며 각 영역 아래에는 131개의 워킹그룹이 활동하고 있다. 워킹그룹들 중에서 Transport area의 IP Performance Metrics (IPPM)과 Operation & Management 영역의 Benchmarking Methodology (bmwg) 워킹그룹에서는 프로토콜이나 관련 장비들의 성능측정과 관련된 표준문서들을 제정하여 보급하고 있다[1].

2. IETF 표준화 동향

2.1 IETF 성능측정 표준

현재 IETF에서 제정된 성능과 관련된 주요 RFC 문서는 표 1과 같다. 정리하면 리피터, 스위치, 라우터 등의 네트워크 장비 성능을 측정하는 방법(RFC 2544, RFC 2889, RFC 5180)과 ATM(RFC 3116), Firewall(RFC 3511), IP Multicast(RFC 3918), OSPF(RFC 4061), MPLS(RFC 5695) 등의 성능측정 방법을 위한 문서들이 있으며 IGP(Interior Gateway Protocol) 성능(RFC 6413)과 관련된 표준이 최근 제정되었다[2~10].

새롭게 작업중인 문서(draft)들로는 네트워크 장비 성능측정 확장(RFC 2544 AS), 콘텐츠(L7) 처리 장비 성능측정, IP 플로우(flow) 측정, MPLS 보호(protection) 관련된 문서들이 조사되고 있었으며 각각 제출되어 작업이 진행되고 있었다[11~14].

표 1. IETF 성능측정 관련 RFC 목록

번호	내용
RFC 2544	Benchmarking Methodology for Network Interconnect Devices 1999.3
RFC 2889	Benchmarking Methodology for LAN Switching Devices 2000.8
RFC 3116	Methodology for ATM Benchmarking 2001.6
RFC 3511	Benchmarking Methodology for Firewall Performance 2003.4
RFC 3918	Methodology for IP Multicast Benchmarking 2004.10
RFC 4061	Benchmarking Basic OSPF Single Router Control Plane Convergence 2005.4
RFC 5180	IPv6 Benchmarking Methodology for Network Interconnect Devices 2008.5
RFC 5695	MPLS Forwarding Benchmarking Methodology for IP Flows 2009.11
RFC 6413	Benchmarking Methodology for Link-State IGP Data-Plane Route Convergence 2011.11

2.2 정보보호제품 성능평가

정보보호제품의 성능을 측정하기 위한 표준문서로는 앞에서 본 바와 같이 RFC 3511이 있다.

RFC 3511은 정보보호 제품인 방화벽의 성능을 측정과 관련된 내용을 기술하고 있으며 모두 10개의 항목으로 구성되어 있다[6].

표 2. RFC 3511

번호	내용
1	IP throughput
2	Concurrent TCP Connection Capacity
3	Maximum TCP Connection Establishment Rate
4	Maximum TCP Connection Tear Down Rate
5	Denial Of Service Handling
6	HTTP Transfer Rate
7	Maximum HTTP Transaction Rate
8	Illegal Traffic Handling
9	IP Fragmentation Handling
10	Latency

국내에서는 TTA(한국정보통신기술협회)에서 RFC 2544와 RFC 3511을 기반으로 '네트워크 보안 장비에 대한 성능측정 방법'이 제정되었으며, IPv4 뿐만 아니라 IPv6 트래픽 내용을 포함하고 공격 트래픽의 차단, 탐지규칙과 다양한 트래픽 조합을 통한 시험 등에 대한 내용을 추가하여 방화벽 뿐만 아니라 다양한 네트워크 보안장비(Firewall, IDS, IPS 등)의 성능측정 기준과 측정방법을 제시하고 있다[15].

3. RFC 3511 측정항목 분석

RFC 3511은 방화벽의 성능에 대하여 처리율(전송), 지연시간(지연), TCP 연결용량(접속), TCP 연결생성/해지율(접속), HTTP 전송율(전송)의 측정방법을 제시하고 있다. 그리고, DDoS 패킷에 대한 처리(필터링), Fragment 패킷 처리 확인과 룰 설정에 따른 트래픽 차단율(필터링) 등의 시험과 측정방법에 대하여 상세하게 기술하고 있다. 각 항목별로 살펴보면 다음과 같다.

3.1 IP Throughput

RFC 1242[16]에서 정의된 DUT/SUT(Device Under Test/System Under Test, 이하 DUT)의 네트워크 계층에서 데이터를 전달하는 것을 측정하고 Throughput과 Forwarding Rate 결과 값을 도출한다. 주요 환경변수로는 Protocol 종류, Packet size가 있다.

3.2 Concurrent TCP Connection Capacity

RFC 2647[17]에 정의된 대로 DUT가 참여한 동시에 관리할 수 있는 최대 TCP 연결 수를 측정한다. DUT가 연결테이블(Connection Table)에 저장할 수 있는 최대 entity의 수를 찾는 것도 포함된다. 주요 환경변수는 Connection Attempt Rate, Aging Time, 사용된 HTTP protocol version, Object Size가 있다.

3.3 Maximum TCP Connection Establishment Rate

최대 TCP 연결 성립율은 DUT가 처리할 수 있는 최대 TCP 연결성능 수치를 측정한다. RFC 2647[17]에 정의된 대로 DUT를 통해 시험한다. 3.2 항목의 시험과 동일한 환경변수를 갖고 시험을 진행한다.

3.4 Maximum TCP Connection Tear Down Rate

최대 TCP 연결 해지율을 측정하는 것으로 주요 환경변수는 Number of Connections, Aging Time, Close Method, Close direction이 있다.

3.5 Denial Of Service Handling

DoS 공격(TCP SYN Flood attack 등)에 대해 대상 DUT가 처리하는 동작결과를 측정한다. 3.3 최대 TCP 연결성립률 시험과 3.6 HTTP 전송률 시험을 수행 한 후 시험을 하며 결과를 비교/분석하게 된다.

3.6 HTTP Transfer Rate

HTTP request 메시지에 관한 전송률을 측정한다. HTTP 1.1 이상을 사용하고, Get 요청에 의한 Object size는 동일하게 설정하여 시험을 하고, Object 크기를 변경하여 가면서 반복하여 시험을 한다. 평균전송률은 다음과 같은 산술식

에 따라 계산한다.

$$\text{전송률(Bits/sec)} = \frac{\text{Objects} \times \text{Object size} \times 8}{\text{전송기간(Duration)}}$$

3.7 Maximum HTTP Transaction Rate

HTTP 최대 처리율은 얼마나 많은 사용자가 object를 접근할 수 있는지 최대 트랜잭션 처리율을 측정하게 된다.

3.8 Illegal Traffic Handling

DUT에 차단룰(Drop rule)을 설정하고 정상 트래픽과 비정상(차단) 트래픽을 동시에 전송하여 해당 트래픽의 처리상태를 측정한다.

3.9 IP Fragmentation Handling

정상 트래픽과 Fragmented packet(단편화 패킷)을 전송하고 처리 성능을 측정한다. DUT에 규칙을 설정하고 이에 따른 단편화 패킷 처리하는 동작을 측정한다.

3.10 Latency

DUT가 전송되는 패킷을 전달할 때 지연되는 시간(Latency)을 측정한다.

4. 성능시험

4.1 방화벽 성능척도

RFC 3511에서는 살펴본 바와 같이 10가지 항목에 대하여 방화벽 성능측정 기준을 제시하고 있다. 기술된 모든 항목이 일반적인 방화벽 성능측정을 위한 지표로 사용되지는 않으나 제시된 측정기준들 중 일반적으로 방화벽의 성능을 나타내기 위해 주로 사용되고 있는 패킷처리성능(throughput), 동시세션성능(concurrent connections), 연결성능(connection per second)등 세 가지 메트릭(metric)에 대하여 시험을 실시하고 결과를 분석하였다[18,19,20].

패킷처리성능은 방화벽 장비가 전달되는 트래픽을 처리(전달)하는 성능을 측정하는 것으로 BPS로 표시하며 처리하는 패킷의 수를 표시하는 PPS(packet per second)로 측정하기도 한다. 동시세션성능은 DUT가 세션을 동시에 관리할 수 있는 성능을 측정하는 것이며 연결성능은 동시에 처리할 수 있는 TCP 연결 최대 값을 측정하게 된다.

4.2 시험환경 구성

시험환경은 패킷을 발생시키는 장비(BPS, IXIA 사용)와 DUT(Firewall, 100M급)를 직접 연결하여 구성하였다. 정확한 성능측정을 위하여 관리콘솔은 원격 컴퓨터를 설치하고 별도의 DUT의 관리포트에 연결하였다.

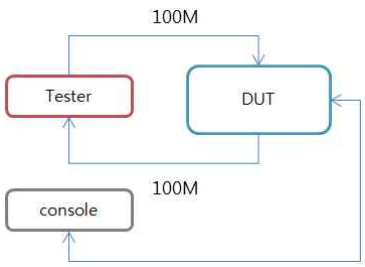

그림 1. 시험환경

4.3 IP throughput 측정

패킷처리성능은 방화벽 장비가 전달되는 트래픽을 받아서 전달하는 성능을 측정하는 것으로 BPS로 표시하며 처리하는 패킷의 수를 표시하는 PPS(packet per second)로 나타내기도 한다.

시험시 설정된 파라미터는 다음과 같다.

패킷크기(byte) : 64, 128, 256, 512, 1024, 1280, 1518
IP 프로토콜 : UDP
발생시간(초) : 30 (s)
클라이언트/서버 : 200개/200개
Aging Time(초) : 3 (s)
Intended Load : 100 Mbps
전송방향 : 단방향(Uni-directional)

세 번 동일조건하에서 반복 시험을 시험을 통해 나온 결과를 아래 <표 3>에 나타내었다.

표 3. IP Throughput

Packet Size	Average Throughput(%)		
	1st	2nd	3rd
64	12.39	12.39	12.84
128	21.08	22.33	22.45
256	51.61	40.75	39.65
512	83.35	67.94	68.74
1024	100	100	100
1280	100	100	100
1518	100	100	100

Packet Size	Throughput(PPS)			
	1st	2nd	3rd	전송가능한 패킷수
64	18437.7	18437.7	19109.82	148009
128	17805.36	18856.98	18960.08	84459
256	23374.7	18454.29	17956.72	45289
512	19701.62	15964.36	16150.8	23496
1024	11973.18	11973.18	11973.18	11973
1280	9615.38	9615.38	9615.38	9615
1518	8127.44	8127.44	8127.44	8127

측정 기준에서는 패킷이 100% 모두 전달되는 경우만을 통과기준으로 하고 있으며[11], DUT 장비가 소프트웨어로 패킷을 처리하고 있기 때문에 패킷크기가 작은 경우의 시험은 측정된 결과가 조금씩 다르게 나타나고 있음을 확인할 수 있다.

1024byte 이상 패킷크기가 큰 패킷전송시는 100% 모두 처리되었다. 시험에 사용된 DUT의 경우 패킷크기가 가장 작은 64byte의 경우 12Mbps, 가장 큰 1518byte의 경우는 100Mbps의 성능을 제공하고 있음을 알 수 있다.

4.4 Concurrent connections 성능측정

동시세션성능은 DUT의 세션관리능력을 측정하는 것으로 최대 세션관리 테이블의 크기를 측정할 수 있다. DUT와 외부의 네트워크를 통한 연결이 없는 환경에서 콘솔을 통해 세션정보를 초기화한 후 반복시험을 실시하여야 정확한 시험을 진행할 수 있다.

TCP 연결을 위한 트래픽을 발생하면서 해당 세션을 종료(close)하지 않고 연결(open)된 상태를 유지하도록 TCP 트래픽을 생성하여 전송하여야 하며, 세션 값을 측정하여 더 이상의 증가가 없을 때까지 지속하여 시험을 진행한다. <그림 2>에서처럼 세션의 수가 증가하다가 일정시간이 되면 더 이상 증가되고 있지 않는 것을 확인할 수 있다. 해당시험의 경우 장비 제조사에 실제 시스템의 세션테이블의 크기를 확인한 후 진행을 하는 것이 적당하며 일반적인 방화벽들의 경우 BSD나 Linux 등을 이용한 경우가 대부분인 관계로 각 OS별 설치된 방화벽 프로그램의 명령구문을 이용하여 시스템에 할당된 테이블 크기를 확인하고 실험 성능수치와 비교할 수 있다.

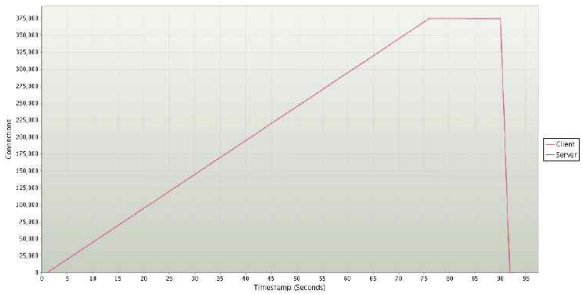

그림 2. CC 측정결과

4.5 CPS(Connections per second) 측정

접속연결성능은 DUT가 동시에 처리할 수 TCP 접속연결 성능을 측정하는 것으로 접속연결의 수(HTTP Get 사용)를 계속해서 늘려가면서 측정한다. 4.2 시험과는 달리 TCP연결을 위한 트래픽 발생시 연결(open)된 상태로 유지하지 않고 요청되는 접속연결의 세션을 정상적으로 관리하고 종료하면서 처리할 수 있는 최대 접속처리 성능수치를 측정하게 된다. 요청하는 Object의 크기를 256byte, 1024byte, 4096byte, 128Kbyte로 변경하면서 실험을 실시하였다. Object의 크기에 따라 성능수치가 다르게 나타나는 것을 <그림 3> 시험결과에서 확인할 수 있다.

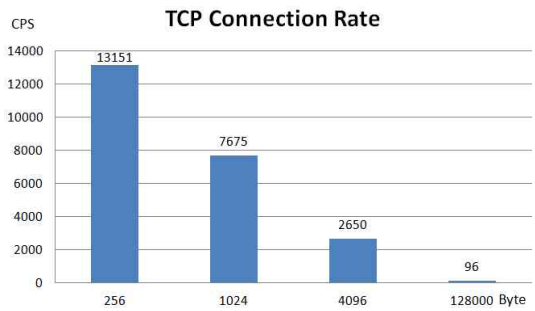

그림 3. CPS 시험결과

5. 결론

방화벽 성능 측정을 위한 IETF RFC 3511의 시험항목 중 세 가지 항목에 대하여 DUT (Firewall)를 연결하고 실험을 실시하였다. 전송하는 패킷의 크기에 따라 측정되는 전송성능 차이를 확인 할 수 있었다. 동시세션성능을 측정하는 방법에 따라 테이블 크기를 확인하였고 HTTP Get 요청에 따른 응답 Object의 크기에 따른 TCP 연결성능의 차이도 확인하여 볼 수 있었다. 시험결과는 실제 제품성능 확인시 보조자료로 활용이 가능할 것으로 판단된다.

향후 다른 시험항목들에 대한 시험이 추가로 진행될 예정이며, 단순한 UDP 패킷전송 시험 뿐만 아니라 TCP, UDP 및 HTTP, MSN 등 응용 프로토콜을 혼합한 실 환경 트래픽을 모델링하여 전달성능 시험을 진행하고, 다른 파라미터들의 변화에 따른 실험을 진행, 관찰하고 결과를 분석하여 해당 파라미터의 변경에 따른 영향을 분석할 계획이다.

참 고 문 헌

[1]IETF WG introduction , http://www.ietf.org/wg/concluded/

[2]Bradner, S. and J. McQuaid, "Benchmarking Methodology for Network Interconnect Devices", RFC 2544, Mar. 1999

[3]Mandeville, R. and J. Perser, "Benchmarking Methodology for LAN Switching Devices", RFC 2889, Aug. 2000

[4]Popoviciu, C., Hamza, A., Van de Velde, G., and D. Dugatkin, "IPv6 Benchmarking Methodology for Network Interconnect Devices", RFC 5180, May 2008

[5]Dunn, et al., "Methodology for ATM Benchmarking", RFC 3116, Jun. 2001

[6]Hickman, et al., "Benchmarking Methodology for Firewall Performance", RFC 3511, Apr. 2003
[7]Stopp, et al., "Methodology for IP Multicast Benchmarking", RFC 3918, Oct. 2004
[8]Manral, et al., "Benchmarking Basic OSPF Single Router Control Plane Convergence", RFC 4061, Apr. 2005
[9]Akhter, et al., "MPLS Forwarding Benchmarking Methodology for IP Flows", RFC 5695, Nov. 2009
[10]Poretsky, et al., "Benchmarking Methodology for Link-State IGP Data-Plane Route Convergence", RFC 6413, Nov. 2011
[11]Bradner, et al., "RFC 2544 Applicability Statement: Use on Production Networks Considered Harmful", Internet Draft, Oct. 2011
[12]Hamilton, et al., "Benchmarking Meth odology for Content-Aware Network Devices", Internet Draft, Sep. 2011
[13]Jan Novak, "IP Flow Information Accounting and Export Benchmarking Methodology", Internet Draft, Dec. 2011
[14]Papneja, et al., "Methodology for benchmarking MPLS protection mechanisms", Internet Draft, Oct. 2011
[15]네트워크 보안 장비에 대한 성능 측정 방법, TTAS.KO-12.0044, Dec. 2006
[16]Newman, D., "Benchmarking Terminology for Firewall Devices", RFC 2647, August 1999
[17]Bradner, S., "Benchmarking Terminology for Network Interconnection Devices", RFC 1242, July 1991
[18]Product Certification Report, 'Fortigate-3810A', NSS labs, Feb. 2008
[19]Test Summary, 'Secui.com NXG2000', Tolly Group, Feb. 2005
[20]White paper, 'Cisco IOS Firewall Performance Guidelines for Cisco Integrated Services Routers', Mar. 2007

저 자 소 개

정 연 서

1996년 2월: 충북대학교 컴퓨터공학과 석사
2001년 8월: 충북대학교 컴퓨터공학과 박사
현재: 한국전자통신연구원 네트워크품질연구팀
<관심분야> 네트워크/정보보호 시험평가, 정보보안, 보안성평가