# 내부 네트워크의 성능저하요인에 관한 연구

종신회원 전 정 훈*

# A Study of the Performance Degradation Factors of An Internal Network

Jeon-Hoon Jeon* *Lifelong Member*

요 약

최근 공격기술은 네트워크의 진화와 함께 다양한 형태로 나타나고 있으며, 대부분의 네트워크에서는 다양한 보안장치들을 통해 대응하고 있다. 또한 외부 공격으로부터 내부 네트워크의 정보자산을 보호하기 위해 기존 네트워크에 필요한 보안시스템들을 추가 배치하고 있다. 그러나 이와 같은 네트워크 구축방법 및 보안시스템의 사용은 내부 네트워크의 성능과 보안에 큰 영향을 미친다. 따라서 본 논문은 내부 네트워크의 보안시스템 사용 및 구축에 따른 성능저하요인을 분석함으로써, 향후 내부 네트워크의 성능 및 보안성 향상을 위한 자료로 활용될 것으로 기대한다.

**Key Words** : Security System, Firewall, VPN, NAT, Internal Network, Performance Degradation

ABSTRACT

Recently, Hacking Attacks are appearing as a various Attack techniques with evolution of the Network. and most of the network through a various Security Systems are responding to an attack. In addition, it should be placed adding the Security Systems to protect the Internal Network's Information Assets from External attacks. But, The use of Security Systems and Network deployment inside the network makes a significant impact on Security and Performance. Therefore, In this paper, it will be to analyze the Performance Degradation Factors of the Internal Network according to the Security System's use and placement. In a future, This paper is expected to serve as a valuable Information for the Network Performance and Security improvements.

## Ⅰ. 서 론

최근 네트워크 기술은 사용자들에게 다양한 콘텐츠와 편의성을 제공하기 위해 매우 빠르게 진화하고 있다. 다양한 콘텐츠들은 점차 대용량화 되고 있으며, 원활한 서비스 제공을 위해 네트워크 속도도 크게 향상되고 있다. 이러한 변화는 앞으로의 클라우드 컴퓨팅(cloud computing) 기술에 커다란 기반이 될 것이며, 무선 네트워크 서비스의 활성화를 가속화 할 것으로 기대된다. 그러나 변화를 바라보는 긍정적인 측면과는 달리 악의적인 공격기술도 진화하고 있음을 함께 고려해야 보아야 한다[1]. 이와 같은 악의적인 공격들은 정보자산을 위협할 뿐만 아니라, 시간과 경제적 손실을 야기 시키기 때문이다[2]. 최근 들어 클라우드 컴퓨팅 및 무선기술이 빠르게 진화하면서 고속의 데이터 전송이 가능하게 되었지만, 이와 같은 변화와는 달리, 원활한 서비스가 최 종단 시스템에까지 미치지 못하고 있다. 원인으로는 내부 네트워크(internal network)의 보호를 위한 보안시스템의 사용 및 배치와 중계 장비의 1대 다 연결특성에 따른 병목현상

※ 본 논문은 2010년도 동덕여자대학교 학술연구비 지원에 의해여 수행된 것임.
* 동덕여자대학교 컴퓨터학과 (nerdrandy@dongduk.ac.kr)
논문번호 : KICS2010-11-535, 접수일자 : 2010년 11월 8일, 최종논문접수일자 : 2011년 1월 3일

(bottleneck), 내부공격으로 인한 이상 트래픽(traffic)의 증가 등을 예로 들 수 있다. 이러한 요인들은 내부 네트워크의 성능과 보안 그리고 효율적인 구축과 배치를 저해하고 있다.

따라서 본 논문은 이와 같은 성능저하요인들에 대해 분석함으로써, 향후 네트워크의 효율적인 구축 및 확장뿐만 아니라, 내부 네트워크의 성능과 보안성 향상을 위한 자료로 활용될 수 있을 것으로 기대한다. 연구내용에 대한 논리적 근거를 위해 논문의 2장은 보안시스템(security system)의 성능저하요인에 대해 분석하고, 3장은 네트워크의 구조에 대한 저하요인을 분석한다. 그리고 4장은 내부공격의 저하요인과 5장의 결론 부분으로 이글을 마치도록 한다.

## Ⅱ. 보안시스템 분석

보안시스템은 내부 네트워크의 보안성을 보장해주며, 네트워크의 보호를 위한 필수장비로 널리 사용되고 있다. 그러나 대부분의 보안시스템들은 모든 트래픽들을 모니터링하고 식별 및 가공해야하기 때문에 보안시스템의 부하는 매우 클 수밖에 없다. 또한 보안시스템은 네트워크의 외부와 연결되는 관문에 배치되어 내부 네트워크의 성능에 영향을 미치게 된다.

따라서 본 절은 보안시스템으로 가장 널리 사용되는 방화벽(firewall)과 가상사설망(virtual private network), 주소변환(network address translation)에 대한 성능분석을 통해 보안시스템이 내부 네트워크의 성능에 미치는 영향을 알아본다.

### 2.1 보안시스템의 사용유무에 따른 성능분석

#### 2.1.1 방화벽의 사용유무

방화벽은 패킷필터링(packet filtering)과 주소변환, 프록시(proxy), 전송데이터 무결성(integrity), 기타 관리 및 감사(audit) 기능 등 다양한 기능들로 구성되어 있으며, 미리 정해 놓은 정책에 따라 구동된다. 그러나 방화벽은 모든 트래픽에 대한 모니터링을 위해 내·외부 네트워크의 관문(gateway)역할을 하는 게이트웨이로 배치되기 때문에 내부 네트워크의 성능에 적지 않은 영향을 미치게 된다. 이와 관련해 [3]에서는 방화벽의 사용유무와 정책허용에 따른 웹 서버(web server)의 응답시간(response time)을 실험하였고, 결과는 그림 1과 같다.

그림 1을 통해 방화벽의 사용이 내부 사용자의 HTTP 서비스를 지연(delay)시키고 있음을 확인할 수

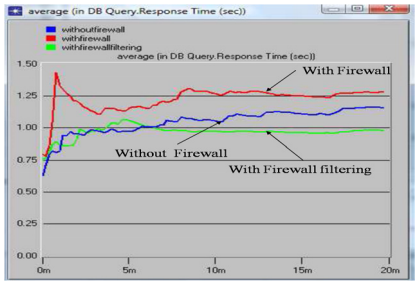


그림 1. HTTP 서버 응답시간

있다. 따라서 방화벽의 사용이 방화벽시스템 자체부하로 인해 방화벽을 게이트웨이로 하는 하부 네트워크의 성능에 영향을 미치고 있음을 알 수 있다.

#### 2.1.2 VPN의 사용유무

VPN은 안전한 데이터의 전송을 목적으로 비밀성, 무결성, 인증성 기능을 제공한다. 이와 같은 VPN은 모든 인바운드(inbound) 및 아웃바운드(outbound) 트래픽에 대해 다양한 기능들을 수행하기 때문에 VPN 시스템의 부하는 매우 클 수밖에 없다. 또한 VPN은 방화벽과 같이 내·외부 네트워크의 관문역할을 수행하도록 배치되기 때문에 VPN을 게이트웨이로 하는 하부 네트워크는 VPN시스템의 부하로 영향을 받게 된다. 이와 관련해 [4]에서는 VPN의 사용유무에 따른 성능을 실험하였고, 결과는 그림 2와 같다.

그림 2를 통해 VPN의 사용이 미사용일 때 보다 약 4배정도 지연되고 있음을 확인할 수 있다. 이로써 VPN의 사용이 VPN시스템의 자체부하로 인해, VPN을 게이트웨이로 하는 하부 네트워크의 성능에 영향을 미치고 있음을 알 수 있다.

| packet size | VPN off | VPN on |
|---|---|---|
| 1 KB | 38,868 | 10,325 |
| 2 KB | 38,580 | 10,190 |
| 4 KB | 38,701 | 10,978 |
| 8 KB | 37,932 | 10,971 |
| 16 KB | 38,918 | 10,959 |
| 32 KB | 38,292 | 10,882 |
| average | 38,549 | 10,718 |

그림 2. 네트워크 전송률

### 2.2 연결 수에 따른 성능분석

앞서 방화벽과 VPN의 사용이 내부 네트워크의 성능에 영향을 미치고 있음을 보았다. 본 절에서는 방화벽과 VPN의 연결(connection) 수가 내부 네트워크의 성능에 미치는 영향을 알아본다.

#### 2.2.1 방화벽의 연결 수

방화벽은 모든 트래픽의 출입을 통제하기 위해 네트워크의 관문에 배치되기 때문에 네트워크의 규모에 비례하여 연결 수가 증가하게 된다. 그리고 방화벽의 연결 수 증가는 방화벽시스템의 자체부하를 증가시켜, 내부 네트워크의 성능에 영향을 미치게 된다. 이와 관련해 [5]는 방화벽의 연결 수에 따른 성능변화를 보안레벨과 연결 수에 따라 처리시간을 측정하였고, 결과는 그림 3, 4와 같다.

그림 3, 4의 결과를 통해 연결 수를 늘리고, 보안레벨을 높일수록 응답시간이 지연되는 것을 확인하였다. 이로써 방화벽을 게이트웨이로 하는 시스템 및 사용자의 증가는 연결 수의 증가로 이어져 내부 네트워크의 성능을 저하시키는 요인이 되고 있다. 결과적으로 성능개선을 위해서는 네트워크 하부의 시스템과 세션(session) 수를 고려한 방화벽의 배치가 요구됨에 따라 하부 네트워크의 소규모화가 필요함을 알 수 있다.

**A**: No. of transaction **B**: No. of sequential connection

| A | 1 | 10 | 20 | 30 | . | 90 | 100 |
|---|---|---|---|---|---|---|---|
| B | 1x3 | 10x3 | 20x3 | .. | . | 90x3 | 100x3 |
| Cfg 1 | 0.94 | 10.40 | 22.20 | .... | . | 111.00 | 143.40 |
| Cfg 2 | 1.00 | 13.00 | 30.14 | ... | . | 125.00 | 150.33 |
| Cfg 3 | 1.50 | 63.88 | 304.38 | ... | . | 1558.86 | 1710.71 |
| Cfg 4 | 1.25 | 65.33 | 313.60 | ... | . | 1538.00 | 1716.33 |
| Cfg 5 | 2.86 | 70.88 | 316.38 | ... | . | 1552.43 | 1743.00 |
| Cfg 6 | 1.33 | 63.33 | 302.00 | ... | . | 1536.00 | 1674.33 |
| Cfg 7 | 2.75 | 63.25 | 304.50 | ... | . | 1526.25 | 1737.25 |

Note: Cfg x refers to firewall configuration x with security level defined as Level x.

그림 3. HTTP 전체 평균 전송시간

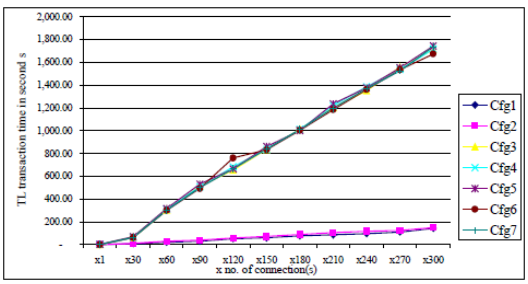


그림 4. HTTP 전체 평균 전송시간 대 연결 수

#### 2.2.2 VPN의 연결 수

VPN은 네트워크와 네트워크를 연결하며, 다중연결이 가능하다. 그리고 다중연결에 따른 전송량 증가로 인해 VPN시스템을 게이트웨이로 하는 하부 네트워크의 성능에 영향을 미치게 된다. 이와 관련해 [6]은 VPN 연결에 따른 네트워크의 수와 정책의 변화에 따른 성능을 측정하였고, 결과는 그림 5와 같다.

그림 5의 결과를 통해, VPN의 연결 수 증가가 수행시간의 지연 및 메모리의 점유율을 높이고 있음을 확인하였다. 이로써, VPN시스템의 하부에 연결된 '시스템' 및 '세션 수'의 증가가 내부 네트워크의 성능저하의 요인이 되고 있으며, 결과적으로 VPN은 시스템의 '성능'과 '세션', '터널(tunnel) 수', '전송량' 등을 고려한 배치가 필요하며, 규모를 축소할수록 성능이 개선됨을 알 수 있다.

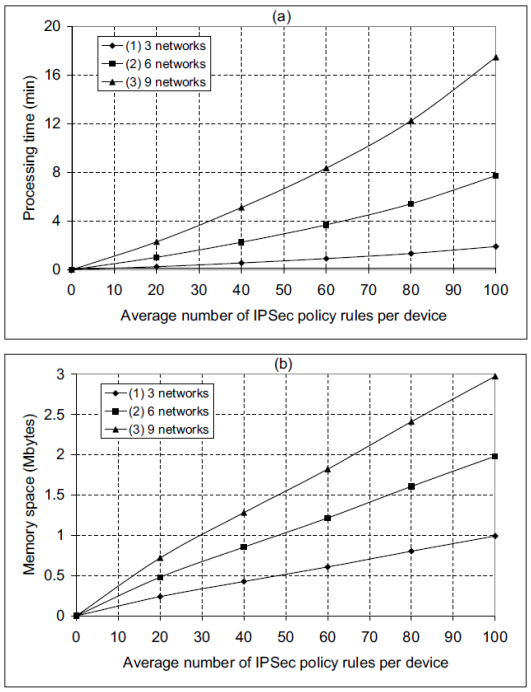


그림 5. 방화벽의 정책에 따른 수행시간과 메모리 사용률

### 2.3 정책 수에 따른 성능저하

#### 2.3.1 방화벽의 정책 수

방화벽은 미리 설정된 정책에 의해 비교 및 판단, 조치 등의 단계별 기능을 수행한다. 그리고 방화벽의 정책은 모든 인바운드 및 아웃바운드 트래픽에 대해 적용되기 때문에 정책 수는 서비스와 내부 네트워크가 확장될수록 증가하게 된다. 또한 정책 수의 증가는 방화벽시스템의 부하를 가중시켜, 하부 네트워크의 성능에 영향을 미치게 된다. 이와 관련해 [7]은 방화벽의 정책수가 성능에 어떠한 영향을 미치는지를 알아보기 위한 성능측정을 하였고, 결과는 그림 6과 같다.

그림 6의 결과를 통해 방화벽의 정책 수가 증가함에 따라 수행시간이 지연되고 있음을 확인하였다. 이

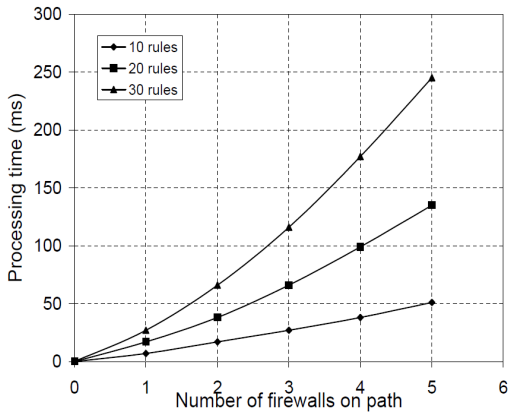


그림 6. 내부 방화벽의 정책 수에 따른 수행시간

로써 정책 수의 증가는 방화벽시스템의 부하를 증가시켜, 내부 네트워크의 성능을 저하시킨다. 따라서 방화벽의 정책 수 감소를 위해서는 소규모 단위 네트워크로의 구성이 효율적일 수 있음을 알 수 있다.

### 2.3.2 VPN의 정책 수

VPN은 암호화와 메시지 인증, 인증키 생성, 압축 등 여러 기능들을 포함하고 있으며, 전송할 데이터의 정보자산 가치에 따라 설정을 달리 할 수 있다. VPN 정책은 방화벽과 동일하게 VPN을 지나는 모든 트래픽에 대해 적용되기 때문에 정책 수는 내부 네트워크가 확장되거나 네트워크 간의 터널 수가 늘어날수록 증가하게 된다. 또한 정책 수의 증가는 VPN시스템의 부하를 가중시켜, 하부 네트워크의 성능에 영향을 미치게 된다. 이와 관련해 [6]은 보안정책 수에 따른 VPN의 성능변화와 메모리 사용에 대한 성능측정을 하였고, 결과는 그림 7과 같다.

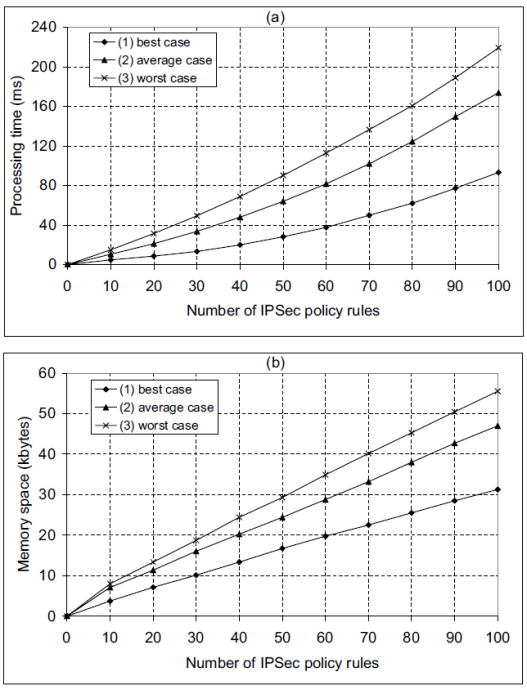


그림 7. IPsec의 내부 정책 수에 따른 수행시간과 메모리 사용률

그림 7의 결과를 통해 VPN의 정책 수가 증가할수록 수행속도의 저하와 메모리의 사용률이 증가하는 것을 알 수 있었으며, 정책 수의 증가가 VPN시스템의 부하를 증가시키고, 내부 네트워크의 성능을 저하시키는 것을 확인하였다. 따라서 VPN시스템에 연결된 내부 네트워크의 성능개선을 위해서는 2.2.2절과 같이 연결 및 시스템 수를 줄이고, 소규모 네트워크로의 운용과 전송 데이터에 대한 등급별 관리를 통한 정책 수의 감소가 필요함을 알 수 있다.

### 2.3.3 NAT의 정책 수와 전송량

NAT는 공인주소와 사설주소에 대한 주소변환 기능을 수행하며, 부족한 IPv4의 주소를 보완하기 위해 개발되었다. 그리고 NAT는 적은 수의 공인주소를 다수의 사용자가 사용할 수 있도록 한다. 따라서 NAT는 NAT를 게이트웨이로 하는 하부 네트워크의 모든 트래픽에 대해 주소변환을 수행함으로써 NAT시스템의 부하는 증가하게 된다. 그리고 네트워크가 확장될수록 부하는 증가하게 되어 하부 네트워크의 성능에 영향을 미치게 된다. 이와 관련해 [8]은 세션 수와 패킷 크기의 변화에 따른 NAT 시스템의 성능측정과 [9]는 다중 사용자에 대한 전송량 증가에 따른 성능측정을 하였고, 결과는 그림 8, 9, 10과 같다.

그림 8, 9, 10의 결과를 통해 NAT는 '연결 수'와 '전송량', '다중 사용자'의 증가가 NAT시스템의 부하를 증가시키고 있음을 확인하였다. 이와 같이 NAT의 '연결 수'와 '전송량', '다중 사용자'의 증가는 NAT 시스템의 부하를 증가시키고, 하부 네트워크의 성능을

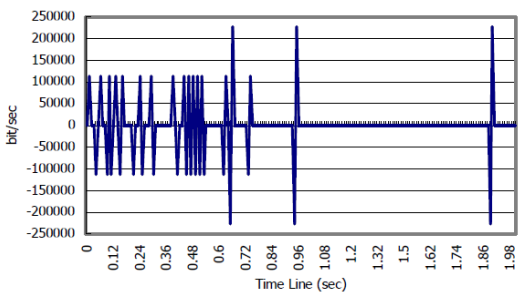


그림 8. 세션에 따른 처리율

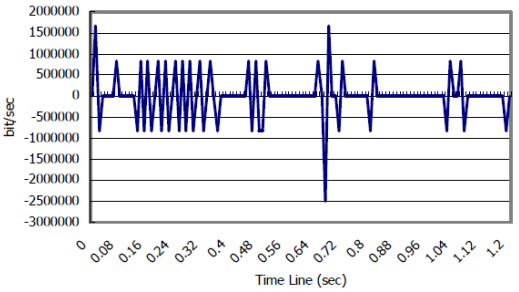


그림 9. 패킷 크기에 따른 처리율

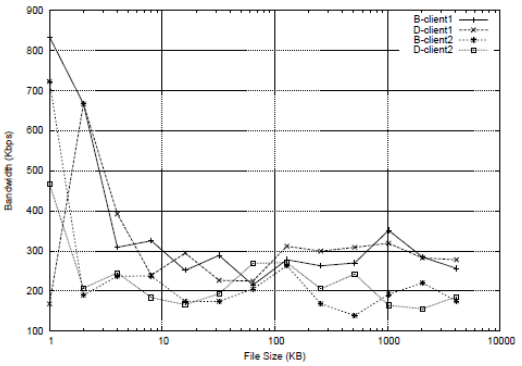


그림 10. 다중 사용자의 NAT 대역폭 사용률

저하시킨다. 그러므로 NAT의 성능개선을 위해서는 소규모 네트워크로의 구성 및 배치를 통해 정책과 연결 수, 전송량의 감소가 내부 네트워크의 성능향상에 효과적임을 알 수 있다.

### 2.4 다기능에 따른 성능저하요인

앞서 보안시스템의 시스템 부하에 대해 알아보았다. 보안시스템은 서비스 및 특정 IP에 대한 차단과 탐지를 위해 여러 기능을 필요로 하고 있다. 방화벽은 패킷필터링과 프록시, NAT, VPN 등의 기능을 포함하고 있으며, VPN시스템은 암호 및 메시지인증 등의 기능을 수행하고 있다. 또한 IPS(intrusion protection system)는 차단기능인 방화벽기능과 탐지기능인 IDS(intrusion detection system)기능을 함께 포함하고 있다.

이와 같은 보안시스템의 다기능구성은 앞서 2절의 '사용유무'와 '연결 수', '정책 수'에 대한 결과와 같이 다중 기능수행에 따른 정책 및 연결 수의 증가가 예상되며, 시스템 부하에 많은 영향을 미칠 뿐만 아니라, 네트워크의 구조적인 병목현상으로 전체 네트워크의 성능을 저하시켜, 내부 네트워크의 취약점을 가중시킨다. 결과적으로 보안성을 고려한 다기능 보안시스템의 배치는 보안시스템의 대응영역을 소규모 단위 네트워크로 구성하여, 정책 및 연결 수를 경감하고, 보안시스템의 기능 또한 최소 기능으로의 단순화가 성능측면에 효율적임을 알 수 있다.

## Ⅲ. 네트워크의 구조 분석

네트워크 구조는 허브 및 스위치와 같은 중계 장비의 1대 다 연결특성으로 인해 트리(tree)구조 및 스타(star)구조의 획일적인 계층구조로의 구현이 불가피하다. 또한 네트워크의 변경이나 재구축은 시간과 경제적인 추가손실을 예고하며, 성능저하 및 추가적인 보안문제도 함께 예상된다. 따라서 본 절에서는 네트워크의 구조가 내부 네트워크의 성능에 미치는 영향을 알아본다.

### 3.1 네트워크의 구조

내부 네트워크는 외부와의 연결을 위해 라우터와 게이트웨이, 스위치 등 중계 장비들을 이용하여 토폴로지들 간의 다양한 결합으로 확장된다. 그리고 네트워크의 구조는 규모와 보안요구사항에 따라, '전형적 구조'와 '이중화 구조', 'DMZ 구조'로 유형들을 구분해 볼 수 있으며, 다음에서 이러한 유형들의 성능에 대해 알아본다.

전형적 구조는 그림 11과 같으며, 트래픽의 량이 비교적 적은 중·소형 네트워크에 적합하다. 그러나 네트워크의 확장 시에는 병목현상으로 인해 외부 네트워크와의 연결을 담당하는 시스템의 부하를 증가시킨다. 그림 11의 '시스템 A'는 네트워크의 관문에 위치함으로써 모든 트래픽들이 집중되며, '시스템 A'의 부하는 하부 네트워크의 성능에 영향을 미쳐, 네트워크 전체를 마비시킬 수 있다. 이와 관련해 [10]의 보안시스템에 대한 부하실험에서도 전형적 구조가 병목현

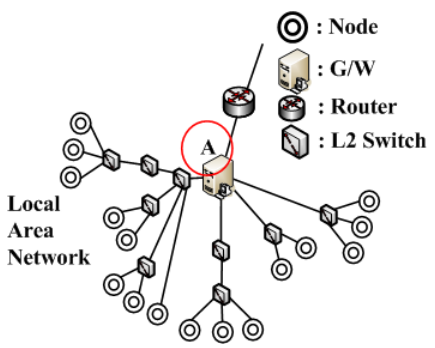


그림 11. 전형적 구조

상에 매우 취약함을 기술하고 있으며, 그림 11의 'A'와 같은 위치에 보안시스템을 배치할 경우, [3]과 [4]의 결과와 같이 시스템부하의 증가로 내부 네트워크의 성능저하를 더욱 가중시킨다.

이중화 구조는 그림 12와 같으며, '전형적 구조'보다 외부공격에 대한 가용성 기능을 보완하여, 보안시스템의 이중화를 통해 시스템의 부하를 절감하였다. 그러나 이중화 구조는 장비의 이중화에 따른 추가비용과 병목현상, 내부공격에 의한 이상 트래픽의 증가 문제는 여전히 남아 있다. 이와 관련해 [11]은 네트워크 확장 시, 전형적 구조와 동일한 문제들을 포함하고 있음을 기술하고 있다. 따라서 이중화 구조는 [2]의 내부공격 및 [3]과 [4]의 병목현상으로 인해 내부 네트워크의 성능저하는 불가피하다.

DMZ 구조는 그림 13과 같으며, 외부 공격의 유입을 차단하고, 서버의 서비스 공격에 대응이 뛰어나다. 또한 이중화 구조와 병행하여 대형 네트워크의 구조로 널리 사용되고 있으며, 네트워크의 확장에 유리하다. 그러나 내·외부 네트워크를 연결하는 시스템은 부하가 집중되어, 하부 네트워크의 성능을 저하시킨다. 이에 대해 [10]과 [11]은 내·외부 네트워크를 연결하는 시스템에 대한 부하가 하부 네트워크에 영향을 미치고 있음을 기술하고 있으며, DMZ 구조는 다른 유형의 구조와 마찬가지로 1대 다 연결에 따른 구조적 문제가 내부 네트워크의 성능에 영향을 미치고 있음을 알 수 있다.

결과적으로 3가지 유형의 네트워크 구조의 특징을 살펴볼 때, 내부 네트워크의 성능개선을 위해서는 다회선 연결을 기반 한, 단위 네트워크로의 규모 축소가 효과적일 수 있음을 알 수 있다.

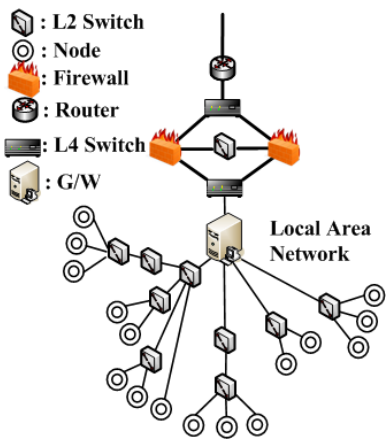


그림 12. 이중화 배치구조

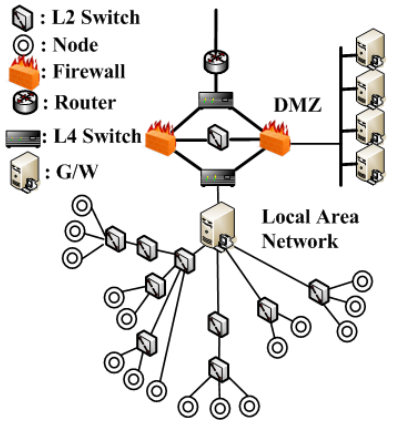


그림 13. DMZ 구조

## Ⅳ. 내부 공격에 대한 분석

공격은 바이러스(virus)나 봇(bot), DNS 스푸핑(spoofing), 스니핑(sniffing) 등의 내부 공격과 다양한 인터넷 서비스를 악용한 전자메일 및 ActiveX, P2P, DoS 등의 외부 공격으로 구분해 볼 수 있다. 최근 내부 공격이 증가함에 따라 새로운 보안문제로 등장하고 있으며, 이와 관련해 [1]에서는 내부 공격의 다양한 유형들이 시도되고 있음을 기술하고 있다. 그리고 [2]의 2008년 사고유형별 현황보고서에서 전체공격의 44%가 내부자에 의해 이뤄지고 있음을 그림 14와 같이 나타내고 있다.

이와 같은 내부 공격의 증가원인으로는 공격 대응에 필요한 보안시스템의 배치가 비교적 외부 공격 대응에 비중을 크게 두고 있다는 점과 내부 네트워크를 트러스티드 네트워크(trusted network)로 전제하는 데에 따른 취약점을 원인으로 꼽을 수 있다. 트러스트 네트워크에서 내부 사용자는 정책상 인가된 자로서, '자원의 공유' 및 '데이터 송수신', '기타 접근' 등이 허용되기 때문에 감지 및 차단이 어렵고, 네트워크 확장에 따른 관리가 매우 취약하다[1,2]. 또한 내부 공격은 공격대상이 시스템뿐만 아니라, 내부 네트워크 전체를 대상으로 하기 때문에 1차적으로는 내부 네트워

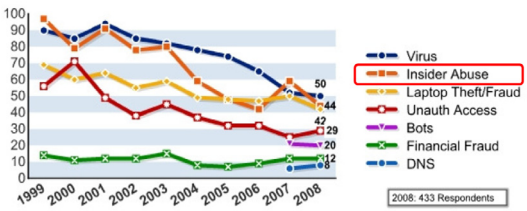


그림 14. 주요 사고유형별 현황

크의 불필요한 트래픽을 증가시키고, 2차적으로는 보안시스템의 부하가 내부 네트워크의 성능에 영향을 미치기 때문이다. 이와 관련해 [11]에서는 내부공격의 유형과 방어유무에 대해 실험을 통해 내부 네트워크의 취약성을 기술하고 있다.

실험은 내부 네트워크의 보안성을 분석하기 위해 그림 15와 같이 공격이 발생한 근원에 따라, 내부 및 외부 공격으로 구분하고, 내부 공격의 3가지 시나리오와 외부 공격에 대해 스니핑, 스푸핑, 공유, 플러딩, 패스워드 크래킹, 웜과 바이러스, 스캐닝을 시도하였으며, 결과는 표 1[11]과 같다.

표 1을 통해 내부 공격에 대한 내부 네트워크의 취약성을 알 수 있다. 이와 같이 내부 공격에 따른 이상 트래픽의 증가는 내부 네트워크의 성능을 저하시키는 요인이 되며, 내부 보안을 위한 보안시스템의 배치가 불가피하다. 따라서 내부 네트워크는 보안과 성능 모두의 향상을 위해서 소규모의 단위 네트워크로 분할 및 보안관리가 필요함을 알 수 있다.

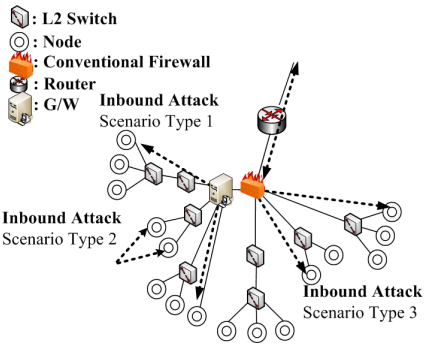


그림 15. 전형적인 방화벽에 대한 네트워크 공격

표 1. 방화벽 사용시 공격에 따른 방어유무 비교

| No. | 공격유형 | 내부 네트워크의 공격 | 외부 네트워크의 공격 |
|---|---|---|---|
| 1 | Sniffing Attack | 허용 | 차단 |
| 2 | Spoofing Attack | 허용 | 허용 |
| 3 | Shared Attack | 허용 | 차단 |
| 4 | Flooding Attack | 허용 | 일부 차단 |
| 5 | Password Cracking | 허용 | 차단 |
| 6 | Worm & Virus | 허용 | 허용 |
| 7 | Scanning Attack | 허용 | 차단 |

## V. 결 론

오늘날 네트워크 보호를 위해 다양한 보안시스템들이 네트워크의 보호를 위해 배치되고 있다. 그러나 대부분의 보안시스템들은 다기능 구성에 따른 자체부하와 정책 수의 증가로 내부 네트워크의 성능을 저하시키고 있다. 또한 네트워크의 확장은 성능과 상대적으로 반비례하며, 점차 증가추세에 있는 내부 공격은 실질적인 공격차단과 대응이 이뤄지고 있지 못하고 있어, 내부 네트워크의 보안성을 보장하지 못하는 실정이다.

본 논문은 내부 네트워크의 성능을 저하시키는 요인으로 '보안시스템'과 '다기능시스템', '네트워크의 구조', '내부 공격'에 대해 분석해 보았다. 결과적으로 네트워크의 1대 다 연결의 구조문제와 보안시스템의 배치 및 운용, 다기능을 사용하는 보안시스템, 내부 공격으로 인한 비정상트래픽의 증가 등이 내부 네트워크의 성능을 크게 저해하고 있음을 알 수 있었다. 또한 이러한 내부 네트워크의 성능저하요인들을 최소화하기 위해서는 네트워크의 확장보다 단위 네트워크로 규모를 축소하고, 서비스와 전송량, 연결 수의 최소화를 고려한 보안시스템의 배치 및 운용이 필요하며, 보안시스템은 다기능 구성보다 단순 기능의 보안시스템 배치가 오히려 성능에 효율적임을 알아보았다.

이와 같은 연구가 향후 클라우드 컴퓨팅 환경의 내부 네트워크 구축 시, 성능향상 및 효율적 관리를 위한 자료로 활용될 수 있을 것으로 기대한다. 그러나 내부 네트워크 구축에 따른 세부적인 정책마련과 이에 따른 구체적인 기준 모델이 제시되어야 할 것이며, 보안시스템의 효율적인 기능개선과 경제성에 관련하여 기능분산 보안시스템에 대한 추가적인 연구도 지속적으로 이뤄져야 할 것이다.

## 참 고 문 헌


〔1〕 한국정보보호진흥원 "2008년 인터넷 및 침해사고 동향 및 분석보고 월보(8월)" Aug, 2008.

〔2〕 Robert Richardson, CSI Director "CSI &FBI CSI Computer Crime & Security Survey" 2008.

〔3〕 H. Garantla, Gemilkonakli "Evaluation of Firewall Effects on Network Performance" 2009.

〔4〕 Jens Mache, Damon Tyman, Andre Pinter, Chris Allick "Performance Implication of Using VPN Technology for Cluster Integration and Grid Computing" *IEEE Computer Society*, pp.75-80, 2006.

〔5〕 Michael R. Lyu and Lorrien K. Y. "Firewall

Security: Policies, Testing and Performance Evaluation", *Lau Department of Computer Science and Engineering The Chinese University of Hong Kong, Shatin, HK IEEE Computer Society Washington DC* USA, pp.116-121, 2000.

〔6〕 Hazem Hamed, Ehab Al-Shaer and Will Marrero "Modeling and Verification of IPSec and VPN Security Policies" *IEEE International Conference on Network Protocols,* pp.259-278, 2005.

〔7〕 Al-Shaer, E. Hamed, H. Boutaba, R. Hasan, "Conflict classification and analysis of distributed firewall policies", *M. Telecommun. & Inf. Syst. DePaul Univ. Chicago IL USA, IEEE Journal,* pp.2069-2084, Oct 2005.

〔8〕 HAYASHI yu-ichi "NAT Router Performance Evaluation", *University of Aizu, Graduation Thesis,* Mar, 2002.

〔9〕 Jiejun Kong, Shirshanka Das, Edward Tsai, "A Decentralized and Localized Access Control System for Mobile Wireless Access to Secured Domains", *Mario Gerla Computer Science Department University of California, Los Angeles, CA 90095,* pp.51-60, 2003.

〔10〕 전정훈, 전상훈 "효율적인 네트워크 보안운영을 위한 Exclusive Firewall에 관한 연구", *한국컴퓨터정보학회논문지*, 12(2), pp.93-102, 2007

〔11〕 전정훈 "인바운드 네트워크의 성능 및 보안성 향상에 관한 연구" *한국통신학회논문지*, 33(8), pp.727-734, 2008

**전 정 훈** (Jeong-hoon Jeon) 종신회원

2008년 숭실대학교 컴퓨터공학과 공학 박사

2005년~현재 동덕여자대학교 교수

<관심분야> 네트워크보안, 시스템보안, 무선보안, 암호, 컴퓨터 포렌식