인바운드 네트워크의 성능향상을 위한 보안 클러스터링 기법과 기능성방화벽의 배치

정회원 전 상 훈*, 종신회원 전 정 훈**

A Secure Clustering Methodology and an Arrangement of Functional Firewall for the Enhancement of Performance in the Inbound Network

Sang-Hoon Jeon* ***Regular Member***, Jeong-Hoon Jeon** ***Lifelong Member***

요 약

오늘날 네트워크에 대한 침해사고가 급증하고 있으며, 점차 증가하고 있는 인바운드 네트워크에 대한 공격도 함께 증가하고 있다. 이러한 공격에 대응하기 위해서 보안시스템의 개발이 지속적으로 이뤄지고 있지만, 인바운드 네트워크의 성능 감소의 문제가 발생하기 때문에, 성능 향상과 보안성 강화를 위한 모두를 고려한 보안시스템 개발이 시급한 실정이다[1]. 따라서 본 논문에서는 네트워크를 분할하여 보안등급에 따라 관리함으로써 성능을 향상시키기 위한 보안클러스터링을 제안하고자 한다.

Key Words : Conventional Firewall, Functional Firewall, Inbound Network, Secure Clustering

ABSTRACT

Nowadays, the network attack occurs frequently. At the same time, the inbound network is also attacked. Even though the security system has been continuously developed in order to prevent from attacks, the network performance is sacrificed for the network security. Therefore, a security system which obtains performance and security together is urgently needed.

In this paper, an arrangement of functional firewall and a secure clustering methodology, obtained from distributing functions of a conventional firewall, are proposed based on the idea that performance and security should be obtained together.

Ⅰ. 서 론

최근 개인정보보호에 대한 중요성이 부각되고 있는 상황에서 네트워크에 대한 공격이 다양해지고, 침해사고율이 높아짐에 따라 다양한 보안시스템들이 개발되고 있다. 그리고 이러한 보안시스템의 대부분은 네트워크 외부로부터 유입되는 트래픽 공격에 대응하도록 개발 및 배치되고 있다. 그러나 차단 및 탐지, 역추적 등의 대표 기능들로 구성하고 있지만, 네트워크의 내부 공격에 대한 대응은 매우 미약한 상황이다[1],[2]. 따라서 이와 같은 내부 공격에 효율적으로 대응하기 위한 보안시스템으로 방화벽을 꼽을 수 있다. 그러나 방화벽은 시스템부하와 병목현상으로 내부 네트워크의 성능을 저해하며, 이를 대신하는 분산방화벽 또한 방화벽의 다중 적용으로 내부 네트워크의 성능저하를 야기 시킨다. 또한 중앙의 정책관리 방화벽으로부터

* 기획재정부 정보화담당관실(randyjeon@gmail.com), ** 동덕여자대학교 컴퓨터학과 (nerdrandy@hanmail.net)
논문번호 : KICS2009-01-015 접수일자 : 2009년 1월 13일, 최종논문접수일자 : 2010년 7월 7일

IPsec 연결과 IDS(Intrusion Detection System)간의 적용을 어렵게 하는 문제점들을 포함하고 있다[3].

따라서 내부 공격에 대한 보안성과 성능 모두를 향상시키기 위한 방안으로 기능성방화벽과 네트워크 클러스터링을 [5]에서 제안하였고. 본 논문에서는 내부 네트워크의 보호를 위한 네트워크 클러스터링기법 설계와 기능성방화벽의 배치에 대한 보다 구체적인 설계방법에 대해 제안하고자 한다. 제안내용에 대한 논리적 근거를 위해 논문의 Ⅱ장에서는 관련분야에 대한 연구내용으로 전형적인 방화벽기능과 기능성방화벽에 대해 분석하고, Ⅲ장에서는 제안하는 보안클러스터링 기법과 기능성방화벽의 배치방법에 대해 기술하였다. 그리고 Ⅳ장의 성능에 대한 비교분석과 Ⅴ장의 결론부분으로 이글을 마치도록 한다.

Ⅱ. 관련연구

2.1 공격유형분석

공격유형에는 TCP 서비스 스캔이 34.3%, NetBIOS에 의한 공유공격 유형이 16.2%, Nmap Scan이 12.5%, 기타 37% 등을 차지하고 있다. 이중 TCP 80번 포트를 이용한 스캔이 가장 높은 비율을 차지하고 있으며, 80번 포트 외에도 다른 포트들을 이용한 서비스 공격이 지속적으로 이뤄지고 있다. 이와 같은 대표적인 공격유형들에는 플러딩, 스캔, 스니핑, 스푸핑, 공유, 크랙킹, 바이러스, 웜, 스팸메일 등이 있으며, 공격에 이용되는 서비스로는 ActiveX와 웹 메일, 메신저, 웹 하드 등이 대표적이다. 이러한 다양한 서비스들은 보편적 또는 필수적으로 사용되고 있기 때문에 공격 가능성을 더욱 높이고 있다. 따라서 지속적으로 생성되고, 보편적으로 사용되는 서비스를 차단하기 위해서는 보안시스템의 추가배치가 불가피하며, 이는 네트워크의 성능을 저하시키는 또 다른 요인으로 작용하고 있다[4].

2.2 전형적인 방화벽(Conventional Firewall)

전형적인 방화벽의 대표적인 주요기능으로는 프락시, 주소변환, 패킷필터링 등이 있으며, 이러한 기능들은 상호 연동성을 갖고 운영되기 때문에 각 기능별 정책들을 참조한다. 그리고 방화벽의 기능들마다 독립적으로 운용되기 때문에 방화벽을 운용하는데 있어 기능들 간의 정책들은 연동되어야만 한다. 만약, 외부로부터의 접근이나 내부 사용자에 대한 출입허용정책을 수립하기 위한 패킷필터링 기능의 경우, 출입하는 모든 트래픽을 통제하기 위해서 네트워크 내에 존재할 소규모 사설 네트워크와 시스템에 대한 정책들을 모두 설정해야 한다. 그리고 이러한 각 기능에 대한 정책들은 다른 기능들과 연계성과 그룹 및 시스템 단위의 정책 설정으로 정책의 수를 증가시키는 문제를 야기 시킨다. 따라서 네트워크의 규모가 확장되고, 그룹 및 시스템이 증가함에 따라 정책은 더욱 복잡해지며, 중복된 정책으로 인해 오동작 및 성능저하 등의 문제를 초래한다[5-8].

2.3 분산방화벽(distribute firewall)

분산방화벽은 내부 네트워크를 소규모 네트워크로 분할하고, 이에 방화벽을 분산 배치함으로써 내부 공격에 대한 보안성을 향상시킨다. 그리고 내부 트래픽에 대한 필터링이 가능하며, 독립성을 보장한다. 그러나 표1과 같이 DoS공격에 대응하기 어렵고, 기존의 애플리케이션들에 대해 보안성 보장할 수 없으며, 침입탐지시스템(IDS)과 같은 탐지기능의 수행이 어렵다. 그리고 네트워크의 규모가 커질수록 전형적인 방화벽과 동일하게 방화벽 하부단의 성능저하를 야기 시키며, 중앙 정책관리로 인해 신속한 대응이 어려운 문제가 있다[3,9].

2.4 기능성 방화벽(Functional Firewall)

기능성방화벽은 전형적인 방화벽의 주요기능 3가지의 독립적인 시스템구성을 통해 성능향상과 효율적인 운영 및 관리를 위해 이미 [5]의 논문에서 제안한 바 있다.

2.4.1 Gate방화벽(G/F: gateway firewall)

Gate방화벽은 유입되는 트래픽들을 서비스 별로 구분하고, 정책에 따라 필터링함으로써, 인가되지 않은 서비스를 차단한다. 네트워크의 1차 대응을 수행하며, 서비스를 통제하는데 매우 효과적이다. 배치는 그림 1과 같으며, '프락시' 기능을 수행하고, 인증과 접근통제성을 제공한다[5,6].

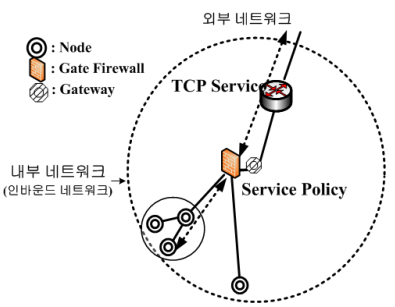


그림 1. Gate 방화벽

2.4.2 NAT방화벽(N/F: NAT firewall)

NAT방화벽(N/F)은 네트워크의 분할 및 관리에 매우 효과적이며, 네트워크에 대한 접근을 통제한다. 배치는 그림 2와 같으며, 동일 네트워크 사용자라 할지라도, 보안목적과 대상, 구조적인 위치 조건 등에 따라 팀별, 부서별, 층별, 목적별로 내부 공격에 대해 대응이 가능하다[5,6,10].

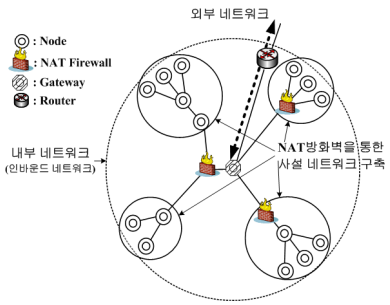


그림 2. NAT 방화벽

2.4.3 IO방화벽(IO/F: inner & outer firewall)

IO방화벽(IO/F)은 외부 공격 및 트래픽 차단에 매우 효과적이고, 내부 공격에 대한 실질적인 차단을 수행할 수 있다. 배치는 그림 3과 같으며, 보안대상은 사용자와 데이터(패킷)가 되며, 접근통제성을 제공한다[5,6].

표 1의 내용과 같이 전형적인 방화벽이나 분산방화

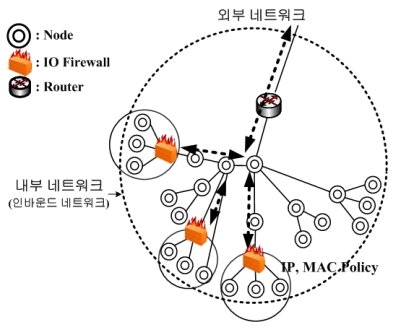


그림 3. IO 방화벽

표 1. 방화벽 비교

	전형적인 방화벽	분산 방화벽
주요 기능	패킷필터링, 프락시, 주소변환 등	패킷필터링, 프락시, 주소변환 등
방화벽 수	1대	다수
정책관리	1대의 방화벽	중앙통제
Dos방어	못함	못함
IDS연동	배치용이	어려움

벽은 주요 기능을 한 대의 시스템으로 운용하는 반면 기능성방화벽은 기능을 분산하여 불필요한 기능으로 인한 정책의 증가와 성능저하를 개선하였다. 그리고 독립성과 보안성을 함께 제공하며, 기타 보안시스템의 배치가 용이하다.

2.5 클러스터

[5]에서는 네트워크를 보안대상에 따라 보안영역으로 분할하고, 단위 네트워크로 클러스터링 한다. 그리고 클러스터링 된 단위 네트워크를 '클러스터'라 정의하고, 클러스터 유형을 분류하여 보안등급을 부여한다. 이러한 보안등급은 내부 네트워크의 토폴로지에 의존적이다[5,6].

Ⅲ. 보안클러스터링 기법과 기능성방화벽의 배치

3.1 보안클러스터링 기법

3.3.1 인바운드 네트워크의 보안영역의 분할

보안클러스터링은 기능성방화벽을 배치하기 전에 인바운드 네트워크의 영역분할이 필요하다. 이는 보안대상에 따라 클러스터링하여 네트워크를 효율적으로 관리하기 위해서이다. [5]에서는 보안영역을 기능성방화벽에 직접 대입하여 3개의 영역으로만 구분하였지만, 보안대상의 세분화와 네트워크의 확장에 따라 다양한 유형의 기능성 방화벽의 혼합배치를 위해 본 논문에서는 표 2와 같이 보안영역을 대상에 따라 구분하고, 이에 보안영역을 'S1, S2, S3' 3가지로 기본 정의하였다.

서비스의 중요도에 따라 보호대상을 정의할 경우, 다양한 서비스로 정책이 증가하게 되며, 보다 중요한 것은 대부분 서비스 사용자는 보안레벨이 낮아, 이로 인해 내부 공격이 증가하기 때문에 서비스의 중요도로 보안대상을 정의하지 않는다. 따라서 그림 4의 보안영역들의 설명은 다음과 같다[5,6].

S1영역은 Gate방화벽만이 배치되어 서비스에 따른 인증성을 보장하고 접근통제성을 제공하는 1차 보안영역으로, 불필요한 서비스의 필터링과 검증작업에 따른 부하를 최소화하는데 목적이 있다. 그리고 S2영역

표 2. 보안대상에 따른 보안영역분류

보안대상	보안영역
서비스	제1보안영역 'S1'
네트워크	제2보안영역 'S2'
데이터 및 시스템	제3보안영역 'S3'

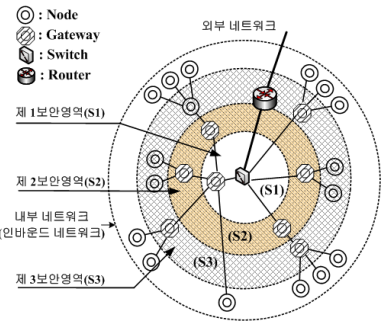


그림 4. 보안영역 구분

은 NAT방화벽의 배치로 특정 소규모 네트워크에 독립성 보장을 위해, 접근통제성을 제공하는 2차 보안영역으로 내부 공격의 차단에 목적이 있다. S3영역은 IO 방화벽의 배치로 접근하는 모든 트래픽에 대해 필터링을 수행하여 접근통제성을 보장하는 3차 보안영역으로 보안대상에 대한 공격에 직접 대응이 가능하며, 정책 수와 시스템 부하를 경감하고, 높은 보안성을 제공하는데 목적이 있다.

3.1.2 보안영역에 따른 클러스터링

인바운드 네트워크는 그림 5와 같이 '보안영역'에 따라 클러스터링되며, 영역화된 네트워크를 효율적으로 관리 및 트래픽 분산을 위해 보다 다양한 배치유형들을 그림 5와 같이 나열하고, 이를 하나의 클러스터로 표현하였다.

배치유형들은 표 3과 같이 Type 1~7로 분류하여 설치될 기능성 방화벽의 수에 따라 단일, 이중, 다중으로 다음과 같이 정의하였다. 설치될 기능성방화벽이 1개인 경우로 Type 4와 6, 7을 '단일영역'으로, 2개인 경우인 Type 2와 3, 5를 '이중영역'으로 하며, 3개인 경우인 Type 1을 '다중영역'으로 분류하였다. 이와 같은 분류기준은 기능성방화벽의 중복에 따른 성능저하 정도에 따라 구분하였으며, '보안대상'의 증가는 보안영역의 증가를 의미하고, '보안대상'을 보호하기 위한

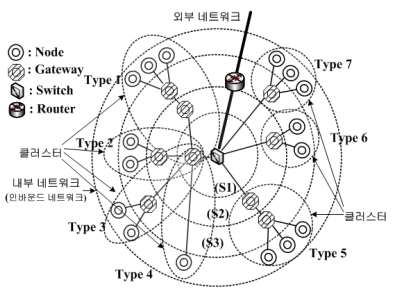


그림 5. 인바운드 네트워크의 클러스터링

표 3. 클러스터링의 유형

보안대상	보안영역	클러스터 유형	정책
(서비스), (네트워크), (데이터 및 시스템)	(S1), (S2), (S3)	Type 4,6,7 (단일영역)	단순 보안성 낮음
(서비스, 네트워크), (서비스, 데이터 및 시스템) (네트워크, 데이터 및 시스템)	(S1, S2) (S1, S3) (S2, S3)	Type2,3,5 (이중영역)	↕
(서비스, 네트워크, 데이터 및 시스템)	(S1, S2, S3)	Type1 (다중영역)	복잡, 보안성 높음

보안시스템이 증가하게 된다. 따라서 클러스터의 유형은 '단일영역'일수록 보안성은 감소하고, '다중영역' 일수록 보안성은 높아지나, 성능은 감소하게 된다.

3.1.3 보안등급의 생성

보안등급(SL)은 인바운드 네트워크의 분할과 이에 적합한 기능성방화벽의 배치를 통해 보안성과 성능을 함께 향상시킬 수 있도록 하는 데 궁극적인 목적이 있다. 따라서 보안등급은 표 3의 보안대상을 세부적으로 분류할 경우, 다양한 보안등급이 생성될 수 있지만, 본 논문에서는 보안대상을 3가지로 제안하여 보안등급을 표 4와 같이 분류하였다.

보안등급(SL)의 생성은 다음과 같다. 보안대상을 서비스, 네트워크, 시스템 3가지로 구분하고, 보안영역인 S(i)를 S1(서비스), S2(네트워크), S3(시스템)의 3개 영역으로 정의하였다. 그리고 보안등급의 경우의 수를 나열하기 위해 표4와 같이 '4×4'의 배열로 나타낸다. 단 S(0)는 기본 등급인 SL1~3을 생성하기 위해서만 사용되며, 실제 등급으로서는 사용하지 않는 것을 전제한다. 보안등급은 기본영역(S1,S2,S3) 3가지를 '보안영역'의 가로축 S(x')와 세로축 S(x)을 순차적으로 나열하고, 해당 영역의 값을 $x+x'=z$로 계산

표 4. 네트워크의 보안등급

단일 이중 다중

보안영역	S0 ′	S1 ′	S2 ′	S3 ′	SL
S0	제외	S(0+1 ′)	S(0+2 ′)	S(0+3 ′)	SL1, SL2,SL3
S1	S(1+0 ′)	S(1+1 ′)	S(1+2 ′)	S(1+3 ′)	S3, SL5
S2	S(2+0 ′)	S(2+1 ′)	S(2+2 ′)	S(2+3 ′)	S3, S4, SL5
S3	S(3+0 ′)	S(3+1 ′)	S(3+2 ′)	S(3+3 ′)	SL3,SL5
SL	SL1,SL2, SL3	SL3,SL4	SL3, SL4, SL5	SL5	SL6

한다. 그리고 생성 가능한 수 는 세 개의 영역($0 \leqq x \leqq 3$), ($0 \leqq x' \leqq 3$) 내에서 SL(1)~SL(6)의 보안등급으로 표4와 같이 영역등급을 통해 '단일' 및 '이중', '다중'의 7가지가 보안영역이 생성되며, 보안등급(SL)으로 표기한다. 보안등급은 기능성방화벽에서 방화벽의 수의 증가는 보안성을 높이지만, 성능은 저하된다. 따라서 이러한 사실과 표 2의 정의에 따라 등급을 표기한다.

3.1.4 보안등급에 따른 기능성방화벽의 배치

네트워크 관리자는 내부 네트워크의 보안등급에 해당하는 유형을 선택하여 기능성방화벽을 배치한다.

클러스터의 유형에 따라 그림 6과 같이 '기능성방화벽'을 표 5의 '단일', '이중', '다중'으로 배치하며, 표기한 숫자는 클러스터에 필요한 '기능성방화벽'의 수를 의미한다. 표 5는 클러스터의 게이트웨이가 속하는 보안영역에 따라 단일 또는 이중, 다중으로 분류하였으며, 3가지 유형들의 특징은 다음과 같다. 단일배치는 각 보안영역이 독립적인 클러스터로 동작함으로써 각 클러스터에 기능성방화벽의 수가 1대일 경우를 의미하며, 이는 성능저하가 적고, 비용이 저렴하다. 이중배치는 두 개의 보안영역으로 이뤄진 클러스터이며, 기능성방화벽의 수가 2대일 경우이다. 해당 클러스터는 2개의 보안영역을 포함하고 있어, 2대의 기능성방화벽을 사용함으로 단일배치 보다는 성능이 비교적 낮다. 마지막으로 다중배치는 클러스터에 게이트웨이가 3개의 보안영역을 모두 포함하고 있어, 기능성방화벽의 수가 3대일 경우로 보안성이 가장 뛰어나다. 그러나 다중배치는 전형적인 방화벽의 주요 기능을 모두 적용하고 있기 때문에 비교적 낮은 성능을 나타낸다.

단 SL3은 표 4의 보안영역 정의에 따라 S($x + x'$)는 S3인 IO/F와 'S(1+2)'인 G/F, N/F 두 가지의 동일한 보안등급을 부여받게 되기 때문에 이러한 두 가지 경우는 관리자에 의해 표 d6과 같이 등급부여 및 배치한다. 인바운드 네트워크는 6가지의 'SL'등급이 부여됨으로써, '보안대상'에 따른 보안클러스터가 구축되고, 클러스터별 관리가 가능하게 된다.

그리고 '보안영역'별로 보안시스템을 배치함으로써, 시스템의 정책수와 부하를 경감시키고 성능을 향상시킨다. 보안등급은 네트워크의 관리정책에 따라 보안대상을 세부적으로 분류할 경우, 보안대상에 따라 SL등급을 선택하고, 인바운드 네트워크의 보안성과 성능을 보장한다. 그러나 보안등급 및 보안대상을 무한정 추가할 경우, 전체 네트워크의 관리 및 감독에 있어, 관리자 및 사용자의 변경 및 네트워크의 재구축, 시스템의 교체 등의 예상하지 못한 문제가 발생할 수 있기 때문에 네트워크의 규모와 네트워크에 전송량 및 세션 수, 보안성, 관리성 등을 고려해야 한다.

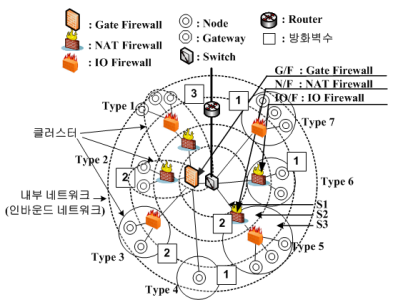


그림 6. 클러스터에 배치된 기능성 방화벽

표 5. 기능성 방화벽 배치

보안영역	클러스터 유형에 다른 배치	기능성 방화벽	기능성 방화벽 수
(S1), (S2), (S3)	단일 배치	(G/F), (N/F), (IO/F)	1
(S1, S2) (S1, S3) (S2, S3)	이중 배치	(G/F-N/F), (G/F-IO/F), (N/F-IO/F)	2
(S1, S2, S3)	다중 배치	(G/F-N/F-IO/F)	3

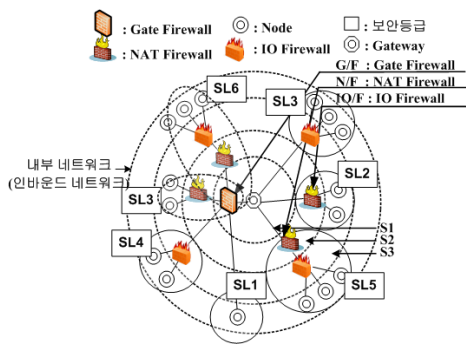


그림 7. 보안영역에 부여된 보안등급

표 6. 보안등급에 따른 기능성 방화벽의 배치

보안등급	보안영역	기능성방화벽
SL1	S1	G/F
SL2	S2, (S1, S1)	N/F
SL3	S3, (S1, S2)	IO/F, (G/F, N/F)
SL4	(S1, S3), (S2,S2)	G/F, IO/F
SL5	(S2, S3)	N/F, IO/F
SL6	(S1, S2, S3)	G/F, N/F, IO/F

Ⅳ. 성능평가

성능실험은 방화벽의 주요기능을 한 대의 시스템에서 모두 사용하는 전형적인 방화벽과 분산방화벽의 경우와는 달리, 방화벽의 주요 기능만을 독립시스템으로 재구성한 기능성방화벽이 인바운드 네트워크의 성능에 어떠한 영향을 미치는지 분석한다.

4.1 보안클러스터링에 따른 정책 수와 성능분석

4.1.1 정책 수의 비교

방화벽의 정책 수가 인바운드 네트워크의 성능에 미치는 영향을 알아보는 실험은 [5]의 실험결과를 통해 정책수의 경감을 확인하였다.

이와 같은 원인으로는 전형적인 방화벽을 통해 사설 네트워크에 있는 사용자가 원하는 서비스를 받기 위해서 주소변환 정책과 프락시 정책, 패킷필터링 정책에 네트워크 그룹설정 및 IP, Port에 대한 허용 및 차단 정책이 설정되고, 각 기능들은 이에 대해 중복 정책이 적용되기 때문이다.

그러나 [5]의 결과는 제한된 기능의 기능성방화벽의 경우, '보안등급'에 따라 분류된 클러스터에 필요한 정책만을 적용함으로써 정책수를 경감시킬 수 있었다. 따라서 정책 수가 전체 인바운드 네트워크에 미치는 영향을 분석해 보기 위해 전형적인 방화벽과 3가지 기능성방화벽의 성능실험결과를 그림 9로 나타냈다.

실험은 측정할 정책 수를 동일하게 하였으며(사설 주소의 2개의 사용자 그룹에 각각 사용자 IP 10개를 할당하고, 이를 프록시에서 FTP와 HTTP 서비스 외에 모두 차단, 패킷필터링은 이외 서비스 및 IP를 모두를 차단하도록 설정) 각각의 방화벽 전단 게이트웨이에 Iperf1.7.0 서버를 설치한다. 그리고 방화벽에 속한 시스템에 Iperf1.7.0 클라이언트를 설치하여 양단간에 4M의 메시지파일을 전송하였을 경우에 대한 성능을 20초간 측정하였다. 그림 9의 "①"은 전형적인 방화벽의 결과로 5.8~10.3Mbps로 큰 변화 없이 안정적인 성능분포를 나타냈으며, "②"의 G/F는 65.1~97.6Mbps의 비교적 큰 변동폭으로 가장 불안정한 성능분포를 나타냈다. 그리고 "③"의 N/F는 76.7~93.4Mbps로 가장 안정적인 성능분포를 나타냈으며, "④"의 IO/F는 74.1~93.4Mbps의 변동 폭으로 N/F 결과와 거의 동일하게 나타났다. 결과적으로 3가지의 기능성방화벽들은 비교적 전형적인 방화벽보다 높은 성능을 나타냈다. 이 실험으로 시스템 및 기능의 독립화로 성능향상과 정책 수의 절감되었음을 확인할 수 있었다.

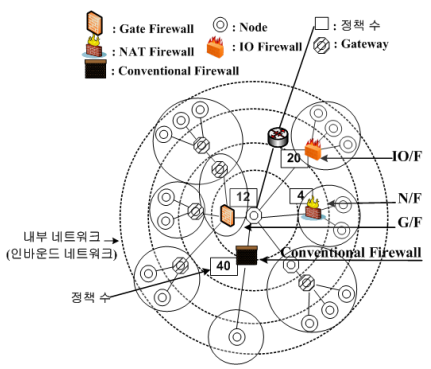


그림 8. 기능성 방화벽의 정책 수

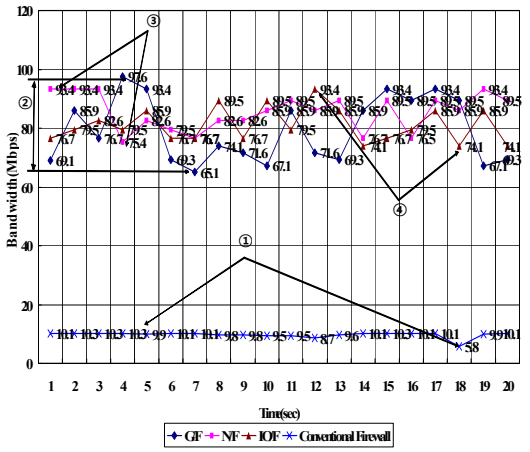


그림 9. 정책 수에 따른 네트워크 성능비교

4.2 보안등급에 따른 기능성방화벽의 성능분석

실험은 전형적인 방화벽과 보안등급에 따른 기능성방화벽을 사용했을 경우에 대한 성능을 비교분석한다. 성능측정을 위해서 Iperf를 사용하며, 4Mbyte 데이터를 전송할 경우, 기능성방화벽들의 처리효율을 측정한다. 그리고 정책에 따른 성능변위를 고려하여, 각 기능들에 적용하는 정책들을 프락시는 HTTP와 TELNET, FTP에 대해서 설정하고, 주소변환은 192.168.1.1~192.168.1.100까지의 IP를 변환하며, 패킷필터링은 모두 차단한 상태에서 사설 네트워크의 사용자에 대해 허용하는 정책으로 설정한다. 실험환경으로 CPU 1.5Ghz에 메모리 1G, NIC 10/100Mbps의 동일 조건의 시스템 3대와 운영체제로는 리눅스 9.0(kernel 2.4.20-8)을 설치하고, 100Mbps 스위치 장

비로 인바운드 네트워크의 사용자용 노트북을 2대 연결한다.

그리고 (1)의 방화벽을 사용하지 않을 경우와 7가지의 기능성방화벽을 사용할 경우((2) G/F (3) N/F, (4) IO/F, (5) G/F와 N/F, (6) G/F와 IO/F, (7) N/F와 IO/F, (8) G/F와 N/F, IO/F), 그리고 (9)의 전형적인 방화벽을 사용할 경우에 대해 실험한다.

그림 10은 실험결과로 전형적인 방화벽의 평균측정값은 9.72Mbps이며, 'SL1~SL6'에 대한 각각의 평균 성능측정값 중 최저 39.88Mbps에서 최고 85.7Mbps로 측정되어, 전형적인 방화벽에 비해, 약 4~8배 정도의 성능향상을 나타냈다.

그리고 전형적인 방화벽을 사용하지 않았을 경우와 사용할 경우 그리고 기능성방화벽(G/F, N/F, IO/F) 모두를 사용할 경우에 대한 성능비교는 그림 11과 같다.

실험결과 전형적인 방화벽의 사용은 사용하지 않았을 때보다 약 9배의 성능이 저하됐으며, 기능성방화벽은 약 4배 정도 성능이 향상됐다. 결과적으로 보안등급에 따른 기능성방화벽의 배치와 독립된 시스템의

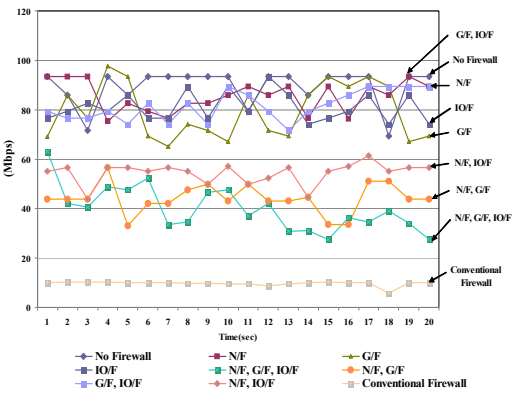


그림 10. 전형적인 방화벽과 기능성방화벽의 실험결과

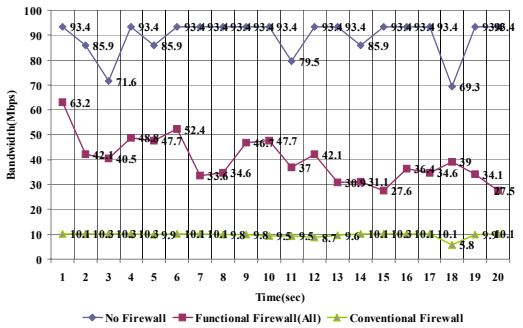


그림 11. 방화벽 미사용, 기능성방화벽, 전형적인 방화벽의 네트워크 성능비교

운영으로 인바운드 네트워크의 성능이 향상되었음을 확인하였다.

V. 결 론

오늘날 다양한 보안시스템들은 대부분 외부 공격방어를 위해 배치되고 있으며, 다기능으로 구성으로 인해, 자체부하와 정책 수의 증가로 오히려 인바운드 네트워크의 성능을 저하시키고 있다. 또한 네트워크가 확장됨에 따라 성능저하는 비례하게 되고, 점차 증가하는 내부 공격에 대해서는 실질적인 공격차단과 방어가 이뤄지고 있지 못하고 있다. 따라서 본 논문은 전형적인 방화벽과 분산방화벽을 기능별로 분리하여 기능성방화벽으로 구성하고, 인바운드 네트워크의 보안클러스터링을 통해 보안영역분할과 보안등급부여를 하였으며, 이와 같은 제안내용의 논리적 근거를 위해 실험을 통한 인바운드 네트워크의 성능과 보안성을 확인해 보았다. 향후 제안하는 기능성방화벽과 보안클러스터링 기법은 네트워크의 독립성과 보안성 제공함으로써 실질적인 예방 및 대응을 수행할 수 있을 것으로 기대한다. 그러나 보안대상에 대한 세부적인 정의 및 표준마련이 필요하며, 이에 따른 보안클러스터링의 기준 모델이 제시되어야 할 것이며, 기능성방화벽의 기능개선 및 보완과 통합관리를 위한 시스템 간의 연동에 대해서도 추가적인 실험과 연구가 지속적으로 이뤄져야 할 것이다.

참 고 문 헌

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

〔2〕 한국정보보호진흥원 "2006년 국내 정보보호 산업 통계조사" p.25, 32, 2006.

〔3〕 Daniel Wan GSEC Practical Assignment Version 1.2c "Distributed Firewall" 2002.

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

〔5〕 전정훈 "인바운드 네트워크의 성능 및 보안성 향상에 관한 연구" 한국통신학회논문지 Vol.33, 제8호, pp.727-734, 2008.

〔6〕 전정훈, 전상훈 "효율적인 네트워크 보안운영을 위한 Exclusive Firewall에 관한 연구", 한국컴퓨터정보학회논문지, Vol.12, 제2호, pp.93-102, 2007.

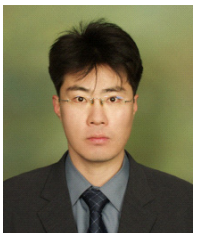
〔7〕 Evaluating Application-aware Firewall Perfor-

mance “Evaluating Application-aware Firewall Performance” www.agilent.com/comms. 2004.
〔8〕 Michael R. Lyu and Lorrien K. Y. Lau Department of Computer Science and Engineering The Chinese University of Hong Kong, Shatin, HK “Firewall Security: Policies, Testing and Performance Evaluation”, 2000.
〔9〕 Sotiris Ioannidis, Angelos D. Keromytis, Steve M. Bellovin, and Jonathan M. Smith, Implementing a Distributed Firewall, http://www.cis.upenn.edu/~angelos/Papers/df.pdf
〔10〕 HAYASHI yu-ichi University of Aizu, Graduation Thesis. “NAT Router Performance Evaluation” Mar, 2002.

전 상 훈 (Sang-Hoon, Jeon) 정회원

2009년 8월 숭실대학교 컴퓨터학과 박사
2009년 11월~7월 전자부품연구원 연구원
2010년 7월~현재 기획재정부 정보화담당관실
2010년 현재 ISO/IEC JTC1 SC27 전문위원
<관심분야> 정보보호, 정보보호 표준화, 인증, IC카드 보안, Biometric

전 정 훈 (Jeong-Hoon, Jeon) 종신회원



2009년 2월 숭실대학교 컴퓨터학과 박사
2005년 3월~현재 동덕여자대학교 컴퓨터학과 전임강사
<관심분야> 네트워크 보안, 디지털 포렌식, 인증, 무선보안