역할 기반 변동 보안 룰셋 적용을 위한 네트워크 보안 게이트웨이 설계에 관한 연구

정회원 이 춘 재*, 조 기 량**

A Study on the Design of the Security Gateway for Role-based Dynamic Security Rule-Set

Chun-jae Lee*, Ki-ryang Cho** ***Regular Members***

요 약

본 논문에서는 보안 게이트웨이가 서브넷 상의 단말기의 네트워크 접근 시도 시에 해당 단말기를 자동으로 인식하여 단말기 사용자의 인증 및 접근 제어 보안 룰셋을 기간 데이터베이스와 비교 판별하여 동적으로 조직 내의 역할 기반 접근 권한을 부여, 관리하는 방식에 대해 연구하였다. 덧붙여, 네트워크 관리자가 조직 구조와 관련하여 네트워크 레벨(L2)과 어플리케이션 레벨(L7)의 통합 액세스 제어를 지정할 수 있도록 사용자 중심의 권한 부여 모델을 제시하였다.

Key Words : Authentication-based, Security gateway network

ABSTRACT

In this thesis investigate the security gateway that manage authorization for user access dynamically by recognizing automatically and comparison & distinction between database and User-information while a terminal unit(PC) trying to access to the network of subnet. Also, it present User-interfaced authorization allowance role model, so administrator can assign united access control between network level(L2) and application level(L7) in relation to system construction.

Ⅰ. 서 론

IT 인프라에 기반을 둔 업무환경에서 심각한 보안위협의 60%가 내부로부터 발생하거나 중요정보 시스템에 대한 불법적인 접근의 70%가 내부자에 의해 시도 되는 등 내부보안문제는 심각한 이슈로 부상하고 있다[1]. 이와 같은 내부보안문제 등 최근 급변하는 IT 보안 환경의 변화에 대응하여 많은 네트워크 및 보안업체들이 허가되지 않거나 웜·바이러스 등의 악성코드에 감염된 개인용 컴퓨터나 노트북, 모바일 단말기 등이 네트워크에 접속되는 것을 원천적으로 차단하여 시스템을 보호하기 위한 다양한 네트워크 접근 제어 솔루션들을 선보이고 있다[2-4].

임의의 사용자가 해당 정보통신 네트워크의 자원을 사용할 수 있도록 하는 접근 권한에 대해 기존의 방식에서는 단말기를 기준으로 IP와 MAC address로 포트 기반 패킷을 차단 또는 허가하는 방식으로 제어하여 왔다. 그러나 보안 사고의 상당 부분이 내부로부터 발생하는 상황에서는 IP에 의한 보안문제 해결보다는 조직 내 사용자 그룹의 네트워크 레벨과 어플리케이션 레벨의 복잡 다양한 접

* 남양정보기술 (jason@nyinfo.co.kr), ** 전남대학교 공학대학 교수 (krcho@chonnam.ac.kr)
논문번호 : KICS2008-02-078, 접수일자 : 2008년 2월 22일, 최종논문접수일자 : 2008년 7월 23일

근 제어를 개체 중심이 아닌 사용자 중심으로 사용자 인증과 동시에 네트워크 접근 제어 보안 룰셋[5]을 동적으로 생성하여 관리하는 방법이 더욱 효과적인 방법이라고 보고되고 있다[6].

이에 따라, 본 논문에서는 사용자 ID와 조직 내의 역할을 기반으로 하는 접근 제어[7-8]를 위해 네트워크 보안 게이트웨이[9]를 이용하여

1) 네트워크 내의 단말기 사용자의 신분 확인과 인증여부에 따라 네트워크 접근을 허가, 차단하고 인증된 사용자에 한해 어플리케이션 접근 권한 여부에 따라 특정 어플리케이션까지 접근 제어할 수 있도록 하며,
2) 관리 네트워크 내에 있는 자원을 효과적으로 관리할 수 있도록 하기 위하여 보안 게이트웨이의 이상적인 위치 선정 및 연결방식 설정으로 내부 자원의 유연한 접근 제어를 가능하게 하는 저비용, 고효율 시스템을 설계하며,
3) 보안 게이트웨이의 커널을 통과하는 패킷의 헤더를 제어하는 룰셋을 네트워크 관리자에 의해 수립된 사용자 인증 정책과 네트워크 공유 어플리케이션의 접근 제어 정책에 맞게 재정의함으로써 보다 융통성 있는 패킷의 흐름을 관리할 수 있는 방안 등에 대하여 연구하였다.

Ⅱ. 시스템 설계

그림 1은 본 논문에서 제안한 시스템 구성도로서 크게 패킷을 필터링하고 제어하는 다수의 보안 게이트웨이와 보안 게이트웨이를 관리하고, 사용자의 인증을 담당하는 관리 서버로 구성하였다.

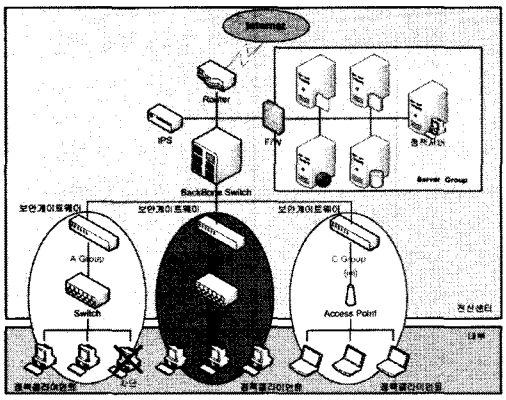


그림 1. 시스템 구성
Fig. 1. System architecture

그림 1에서, 보안 게이트웨이는 커널 기반 패킷 필터링을 수행하도록 설계하여 브리지 방화벽 형태로 네트워크에 위치시켰으며, 각각의 서브네트워크에 대해 별도의 독립적인 보안 정책을 적용하기 위해 지역방어 형태로 구성하였다.

하나의 정책 서버와 여러 정책클라이언트로 하나의 도메인을 구성하며, 도메인이 광범위할 경우 계층구조로서 여러 정책 서버를 관제하는 상위계층의 정책 서버를 구축하여 확장할 수 있도록 하였다.

보안 게이트웨이는 패킷의 흐름을 감시하여, 발생된 이벤트(활성, 인터넷 사용)를 정책 서버로 전송한다. 정책 서버는 전송받은 이벤트에 따라 클라이언트의 초기정책을 결정하여 보안 게이트웨이에 전송하고, 클라이언트는 보안 게이트웨이의 지시에 따라 네트워크 접근 제어 절차를 거치게 하였다.

시스템 모듈은 보안 게이트웨이의 모듈과 정책 서버 모듈 그리고 클라이언트 모듈 세 가지로 구분하였다.

보안 게이트웨이 모듈은 패킷 캡쳐 모듈, 패킷 인식 모듈, 패킷 분배 모듈, 사용자 인증 모듈, 보안정책 실행 모듈, 초기정책 수령 모듈로 구성되어 있으며, 정책 서버 모듈은 패킷 인식 모듈, 패킷 분배 모듈, 사용자 인증 모듈, 초기 정책 하달 모듈로 구성하였다. 그리고 클라이언트 모듈은 Active-X 기술을 이용한 사용자 인증 클라이언트 모듈로 구성하였다.

또한, 사용자 인증과 역할 기반 변동 보안 룰셋을 실시간으로 구현하기 위하여 보안 게이트웨이 내에 10 단계 정책 체인으로 보안 룰셋을 구성하였다.

2.1 보안 게이트웨이 시스템

패킷 캡쳐 모듈에서 발생한 이벤트를 정책 서버로 전송한 후 정책 서버에서 전송되어온 보안 룰셋에 따라 클라이언트의 네트워크 접근을 허가하거나 차단하게 된다. 특히 보안 게이트웨이는 사용자 단말기에 별도의 에이전트를 설치하지 않고, 사용자 단말기의 인터넷 사용 패킷이 발생하는 시점에서 자동으로 판단하여 정책 서버에 관리 대상으로 등록시키며 관리자에 의해 세워진 보안 룰셋에 의해 해당 클라이언트의 패킷을 관리·통제하도록 구성되어 있다.

2.2 정책 서버 시스템

정책 서버 시스템은 다수의 보안 게이트웨이 시스템 기동 시 필요한 환경설정 파일을 관리하며, 각

각의 보안 게이트웨이 내에 실시간으로 변동되는 보안 룰셋을 보안게이트웨이의 재 기동 시에 최종 보안 룰셋을 전송하여 이전 보안 룰셋을 복원하도록 구성하였다. 또한 관리 데이터베이스 내에 클라이언트의 존재여부를 판별해주며, 네트워크 관리자에 의해 수립된 역할 기반 보안 룰셋을 동적으로 생성하여 보안 게이트웨이에 정책을 전송하고, 보안 게이트웨이가 해당 보안 룰셋을 실시간으로 적용 제어하도록 구성되어 있다.

Ⅲ. 시스템 모듈

사용자 인식과정은 사용자가 발생시킨 패킷을 시작으로 보안 게이트웨이의 패킷 캡쳐 모듈에서 패킷 인식 모듈을 거쳐 정책서버의 패킷분배 모듈을 지나 패킷 인식 모듈까지 관계를 갖게 된다.

마찬가지로, 사용자 인증과정은 사용자 모듈의 인증 요청을 시작으로 정책서버의 사용자 인증 모듈을 거쳐보안 게이트웨이의 패킷 분배 모듈을 지나 사용자 인증 모듈로 향하게 된다.

이와 같은 시스템 모듈의 세부구조는 아래와 같다.

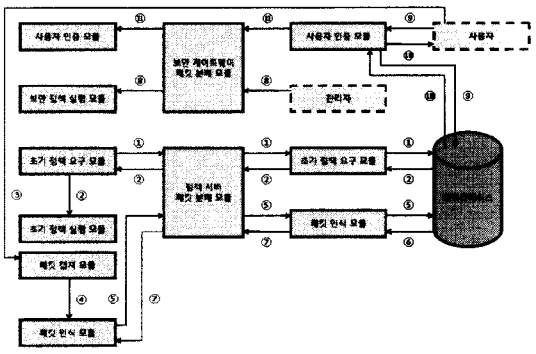


그림 2. 시스템 모듈 세부구조
Fig. 2. System Module architecture

① 초기 정책 요청, 보안 게이트웨이 식별자
② 초기 정책
③ 사용자 이더넷 패킷(ARP, IP)
④ IP 활성, 패킷 사용 이벤트
⑤ 이벤트, 사용자 식별자
⑥ 사용자 초기 허용 정책, 패킷 제한량
⑦ 사용자 허용 정책 (허용, 차단)
⑧ 보안 정책
⑨ 사용자 인증 패킷 (사용자 식별자, 컴퓨터 자원, 로그인 정보)
⑩ 로그인 일치, 사용자 초기 명령
⑪ 로그인 일치

3.1 보안 게이트웨이 모듈

3.1.1 초기 정책 실행 모듈(PolicyGet, ia.000)

정책 서버에 저장된 초기 정책을 요청하여 파일 시스템에 저장한 후 실행하는 모듈로써 정책 서버와의 통신이 차단된 경우 기존에 저장된 정책을 실행한다.

3.1.2 패킷 캡쳐 모듈(Traffic Watch)

패킷 캡쳐 모듈은 ARP[10] 패킷을 분석하여 클라이언트의 활성여부를 판별하고, IP 패킷(TCP, UDP)을 분석하여 클라이언트의 인터넷 사용을 감시한다. 이렇게 판별, 감시된 정보를 이벤트화하여 보안 게이트웨이 내의 패킷 인식 모듈로 전송한다.

3.1.3 패킷 인식 모듈(DhcpAuth)

패킷 캡쳐 모듈에서 발생한 이벤트를 정책 서버로 전송한 후, 정책 서버에서 전송되어온 정책에 따라 클라이언트의 인터넷 사용을 허가하거나 차단하게 된다.

특정 서버 시스템의 경우, 클라이언트의 활성이 인식되지 않은 상태에서 인터넷 사용 이벤트가 발생하기도 한다. 이러한 경우에는 정책 서버에서 클라이언트의 활성 이벤트를 강제로 발생시켜 정책 서버에 등록하여 인터넷 사용을 관리하게 된다.

3.1.4 패킷 분배 모듈(PagcketAgent)

모든 모듈들은 각각의 TCP 포트를 가지고 있기 때문에 네트워크상에 여러 개의 포트를 허가해야 하는 부담이 존재할 수 있다. 이러한 부담을 줄이기 위하여 보안 게이트웨이와 정책 서버 각각에 포트를 하나만 허용하고, 허용된 포트로 들어온 패킷을 분석하여 각각의 모듈에 분배해주는 역할을 한다.

3.1.5 사용자 인증 모듈(ClientAuth)

정책 서버에서 보내온 클라이언트의 인증, 허가, 차단 정책을 수행하여 클라이언트의 네트워크의 접근을 제어한다.

3.1.6 보안 정책 실행 모듈(PolicyRun)

관리자의 필요에 따라 정책의 변경이나 추가가 필요한 경우에 정책 서버 모듈을 이용하여 보안 게이트웨이의 정책 실행 모듈에 정책을 보내면 실시간으로 정책을 반영하는 역할을 한다.

3.2 정책 서버 모듈

3.2.1 초기 정책 하달 모듈(PolicyPut)

보안 게이트웨이가 재부팅 될 경우, 요청하는 초기 정책을 하달하는 모듈로써 정책 서버에 저장되어 있는 역할기반 보안 룰셋 정책을 보안 게이트웨이에 하달하고, 보안 게이트웨이의 부팅 로그를 저장하는 기능을 한다.

3.2.2 패킷 인식 모듈(DhcpAuth)

패킷 인식 모듈은 보안 게이트웨이의 패킷 인식 모듈이 보내온 데이터를 받아 데이터베이스 내에 클라이언트가 존재하는지의 여부를 비교하여 만일 존재하지 않을 경우, 보안 게이트웨이에 클라이언트 강제 활성 명령을 전송하고, 존재할 경우에는 이벤트 데이터(패킷 사용량, 접속 빈도)를 분석하여 과도한 트래픽을 검출하는 역할을 한다.

3.2.3 패킷 분배 모듈(PacketAgent)

보안 게이트웨이의 패킷 분배 모듈과 동일한 기능을 하며 정책 서버로 들어오는 모든 패킷을 하나의 포트에서 각각의 모듈로 분해해 주는 역할을 한다.

3.2.4 사용자 인증 모듈(ClientAuth)

클라이언트용 인증 모듈에서 보내온 사용자 로그인정보를 정책 서버가 받은 후 데이터베이스에 저장되어 있는 사용자 로그인정보와 비교하여 일치하면 네트워크 관리자에 의해 수립된 역할 기반 보안 룰셋을 동적으로 생성하여 보안 게이트웨이에 정책을 전송한다.

3.3 사용자 인증 모듈

클라이언트 활성 후, 웹을 통해 인터넷 접속을 시도 할 때에 보안 게이트웨이는 단말기 인증 여부를 판단하여 인증 받지 않은 단말기 패킷의 목적지를 인증 사이트로 변경하여 인증 화면으로 유도한다. 이 때, 클라이언트용 인증 모듈은 Active-X 형태로 설치되며, 정책 서버의 인증 모듈과 통신하게 된다. 이 클라이언트용 인증 모듈은 클라이언트의 기본 정보와 사용자의 로그인 정보를 정책 서버의 인증 모듈로 보낸 후, 정책 서버의 명령을 기다린다. 정책 서버에서는 해당 로그인 정보와 기간 데이터베이스 내용과의 일치 여부를 확인한 후에 네트워크 사용허가 명령과 함께 해당 사용자의 보안 룰셋을 동적으로 생성하여 보안 게이트웨이에 보낸다. 클라이언트 모듈은 정책 서버에서 사용자 인증과 보안 룰셋이 보안 게이트웨이에 적용되었다는 신호를 받음과 동시에 종료되며, 보안 룰셋의 한도 내에서 각종 네트워크 자원 액세스 동작을 수행한다.

Ⅳ. 보안 게이트웨이 정책 룰셋

보안 게이트웨이의 패킷 필터링은 리눅스 커널에 있는 netfilter를 이용하여 커널을 통과하는 사용자의 모든 패킷을 필터링하며 그림 3의 정책 체인을 통하여 netfilter의 룰이 관리 되어 진다.

일반적인 보안 시스템의 기본적인 정책 룰셋은 미리 정의된 영역에 허용이나 차단 정책이 모아진 상태로 존재하나 이러한 룰셋은 수립된 순서대로 실행되는 구조이기 때문에 인증을 위해 수시로 변동하는 본 시스템에 는 좀 더 확장된 형태의 룰셋이 필요 하였다. 이러한 확장된 룰셋을 통해 인터넷 사용 허가 및 차단을 구분하여, 사용자의 인증 상태에 따라 수시로 변경 가능하게 되었고, 기본 룰셋을 변경하지 않은 상태로 인증을 유도할 수 있게 되었다.

본 논문의 패킷 필터 보안 게이트웨이 보안 체인의 역할은 표 1과 같이 나타낼 수 있다.

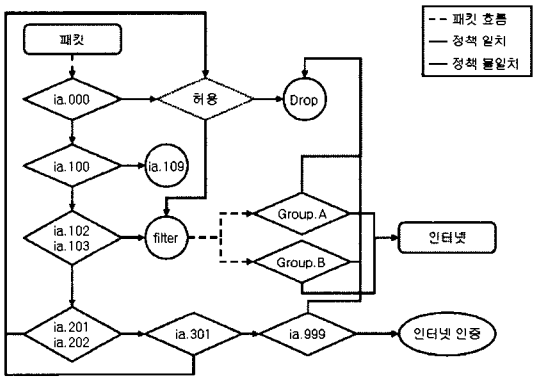


그림 3. 제안한 보안 룰셋 체인 구성
Fig. 3. Proposed system architecture

4.1 최상위 정책

4.1.1 시스템 허용 정책

표 1에서 ia.000 체인은 시스템에서 기본적으로 사용하는 룰셋으로서 여기에는 허용 룰셋이 위치한다.

4.2 인증 전 정책

4.2.1 사용자 인증 룰셋

ia.100, ia.102, ia.103, ia.109 체인은 클라이언트의 차단, 허용에 관련된 정책이 위치한다.

표 1. 체인별 보안 룰셋

위치	역 할	체 인	체 인 역 할
최상위	시스템 허용 룰셋	ia.000	인증 전/후 최상단 정책
인증전	사용자 인증 룰셋	ia.100	관리자에 의한 차단 룰셋
	사용자 인증 룰셋	ia.102	관리자에 의한 허용 룰셋
	사용자 인증 룰셋	ia.103	스케줄에 의한 허용 룰셋
	사용자 차단 룰셋	ia.109	Redirect를 통한 Drop 정책
	상위 허용 룰셋	ia.201	인증 전 허용 정책
	상위 차단 룰셋	ia.202	인증 전 차단 정책
	서브넷 허용 룰셋	ia.301	동일 서브넷 인증 정책
	시스템 차단 룰셋	ia.999	보안 게이트웨이 기본 정책
인증후	역할 기반 룰셋	filter	역할 기반 사용자 보안 룰셋

관리자가 정책적으로 사전에 차단하고자 하는 패턴을 가진 패킷은 하부 체인의 정책 위반여부를 판단하는 단계를 생략하고, ia.000의 상위 체인에서 판별하여 ia.109체인으로 보낸다. ia.109는 존재하지 않는 IP로 패킷을 Redirect 시킴으로써 대량의 비정상적인 패킷의 보안 룰셋 위반 여부 판별로 인한 시스템의 부하를 줄이면서 해당 패킷을 효과적으로 격리 시킬 수 있다.

4.2.2 상위 인증 룰셋

ia.201, ia.202 체인으로서 인증 절차 없이 인터넷을 사용해야 하는 특정 기기(웹/FTP 서버, ATM 기기, Network Printer, ...) 등을 위한 정책이 위치하며 상위 인증 룰셋에 적용되는 시스템은 하위 보안 룰셋에 적용을 받지 않고 자유로이 해당 서비스를 유지 할 수 있다.

4.2.3 동일 서브넷 인증 룰셋

ia.301 체인으로서 보안 게이트웨이가 관리하는 서브넷의 클라이언트들은 상호 접근이 가능하도록 하는 정책이 위치한다.

4.2.4 시스템 차단 룰셋

ia.999 체인으로서 보안 게이트웨이의 기본 기능인 인증 받지 않는 단말기의 패킷을 인증 서버로 유도하는 URL Redirect 기능과 차단 정책이 위치한다.

4.3 인증 후 정책

필터 체인으로서 역할 기반 보안 룰셋이 위치한다. 인증 후 정책은 사용자 인증 시, 조직 내에서 해당 사용자에게 부여한 보안 룰셋이 동적으로 생성되어 적용되는 정책이다. 인증 후에 동적으로 생성되는 역할 기반 정책은 네트워크 레벨(L2)과 어플리케이션 레벨(L7)의 보안 룰셋 적용이 가능하다.

V. 보안 게이트웨이 내 패킷 흐름

본 논문에서 제안한 보안 룰셋 정책 흐름은 그림 3과 같다. 여기에서, 최초 사용자의 패킷은 최상의 체인인 ia.000을 시작 하부 체인으로 정책의 위반여부를 비교 판단하며, 보안 룰셋에 위배되지 않는 모든 패킷은 그림 3의 정책 흐름도에 따라 이동하게 된다. 또한 보안 룰셋에 위배되는 모든 패킷은 커널에서 격리되거나 특정 목적지로 Redirection 된다.

보안 게이트웨이는 DHCP, DNS, NETBIOS 서비스를 시스템 구동과 동시에 기본적으로 허용한다. 다음에, 관리자에 의해 세워진 상위 보안 룰셋인 ssh 포트 허용과 FTP 차단은 다수의 보안 게이트웨이를 통과하는 패킷이 적용을 받는다. 또한, 사용자 인증과 동시에 동적으로 Group A 사용자의 P2P 접속을 차단하며, Group B 사용자의 기간 데이터베이스 접근을 차단하는 역할 기반 보안 룰셋이 적용되도록 시스템을 설정하였다.

VI. 패킷 필터 보안 게이트웨이 운용

보안 게이트웨이의 하드웨어적인 구성은 메모리에 파일시스템을 구성[11]함으로써 정전 등의 일시적인 장애에 대한 위험성을 제거하고, system bypass를 통한 무정지 시스템을 구현하였다.

보안 게이트웨이 내·외부로 이동하는 패킷을 완벽하게 제어하기 위해 브리지 방식을 취했으며, 장애 시점을 로그화 할 수 있도록 구성하여 담당자의 문제 분석에 도움이 될 수 있도록 하였다.

정책 기반 네트워크 보안 시스템에서 보안 게이트웨이와 정책 서버간의 안전한 통신을 위해서는 암호화된 정책 전달을 구현하였다.

6.1 보안 게이트웨이 기동 및 운용

6.1.1 서브넷 상 클라이언트 인식 및 인증 방식

보안 게이트웨이 내의 트래픽 감지 데몬에 의해서 캡쳐된 패킷을 분석하여, 등록된 서브넷 상의 클라이언트인가를 판별한 후, 등록된 서브넷 상의 클라이언트일 경우 맥 주소를 패킷 인식 모듈로 전송하여 인증 단계를 거치게 된다.

6.1.2 정책 서버와 보안 게이트웨이와의 통신 기술

본 논문에서 정책 서버와 보안게이트와의 모든 통신 패킷은 일회성 암호키를 통해 암호화 된 후 전송되며, 한번 접속에 하나의 명령만 실행하도록 설계되었다.

6.1.3 패킷 필터링을 통한 클라이언트 네트워크 접근 제어

6.1.3.1 클라이언트 고립화 기술

비정상 패킷을 발생시키는 클라이언트의 존재는, 동일 서브넷 상의 클라이언트들에게 해를 입히게 된다. 따라서 비정상 패킷을 발생시키는 클라이언트를 고립시킬 필요가 있다.

그러나, 패킷필터 보안 게이트웨이의 차단 정책으로는 내부에서 외부로의 인터넷 사용과, 외부에서 내부로의 접근만을 차단하기 때문에 보안 게이트웨이 하부 단의 동일 서브넷 상의 클라이언트들은 여전히 해를 입게 된다. 따라서 동일 서브넷 상의 클라이언트에 접근하는 방식을 파악하여 그 과정을 차단하는 방법을 강구해야 한다. 그리고 사용자 단말기에 에이전트를 설치하지 않고 보안 룰셋에 위반되는 패킷을 발생하는 단말기를 네트워크 레벨에서 고립화 시켜야 하는 문제점을 가지고 있다.

TCP/IP의 경우에 동일 서브넷 상의 클라이언트에 접근하기 위해서는 OS의 ARP 캐쉬를 이용하여 목적지를 정한 뒤에 패킷을 전송하는데, 이 목적지를 존재하지 않는 곳으로 설정한다면, 동일 서브넷 상의 클라이언트들에게 접근하지 못하도록 할 수 있다.

이러한 특성을 이용하여, 비정상 패킷을 발생시키는 클라이언트의 경우에, 보안게이트웨이에서 ARP 패킷을 강제로 발생시켜서 클라이언트의 OS ARP 캐시를 업데이트시킴으로써, 비정상 패킷을 발생시키는 클라이언트를 서브넷 상에서 고립시킬 수 있다.

6.1.3.2 역할 기반 접근 권한 부여 기술

패킷 필터 보안 게이트웨이는 사용자 인증이 완료된 후, 네트워크 관리자에 의해 세워진 역할 기반 보안 룰셋을 사용자가 속해있는 그룹 정책에 따라 동적으로 생성하여 패킷 필터 보안 게이트웨이에 실시간으로 적용시킨다.

또한 다수의 사용자가 개방형 네트워크 내의 불특정 다수의 공용단말기를 사용할 경우에도 단말기 사용자의 네트워크 자원 접근 권한을 실시간으로 관리 · 제어할 수 있다.

6.2 클라이언트 모듈 운용

6.2.1 사용자 인증 방식

인증 단계를 수행하는 클라이언트는 정책 서버의 인증 정책에 의해 인터넷 사용이 차단되거나 허용될 수 있다. 이와 같이, 인터넷 사용이 차단되거나 허용되지 못한 클라이언트는 정상적으로 인증 단계를 거치게 되는데, 이때 가장 먼저 거치게 되는 곳이 정책 서버 내의 인증 페이지이다. 이 인증 페이지를 거칠 때에 클라이언트용 모듈이 동작하면서 클라이언트의 제어에 필요한 모든 동작을 수행하고, 정책 서버에 인증을 요청하여 정상적으로 인터넷을 사용할 수 있도록 한다.

6.2.2 네트워크 기반 사용자 인증 유도

패킷 필터 보안 게이트웨이는 사전 허가 대상(서버 시스템, 무인 발급기, 공용 프린터 서버 등)을 제외한 모든 시스템의 패킷을 차단하며, 다만 인증 대상의 패킷의 목적지가 인증 서버이면서 80 포트인 패킷만 허용한다.

클라이언트가 최초로 IP를 할당 받을 때에 발생하는 ARP 패킷을 통해 맥 주소를 추출하여 사전 차단 및 허가 대상자인지를 판단하는 1차 인증 단계와, 차단 대상자가 아니면서 인증을 받지 않은 사용자의 HTTP 패킷을 인증 시스템으로 URL Redirection 시켜 사용자를 별도의 조작 없이 인증을 유도하는 2차 인증 단계로 구분하여 사용자 인증을 구현하였다.

6.2.3 정책 서버 운용

6.2.3.1 인증 그룹설정

다수의 사용자의 보안 룰셋을 효과적으로 관리하기 위하여 그림 4와 같이 그룹별로 변동 보안 룰셋을 적용할 수 있도록 하였으며, 모든 사용자는 자신이 속한 그룹에 부여된 보안 룰셋에 따라 네트워크 접근 권한을 인증과 동시에 동적으로 획득할 수 있도록 구성하였다.

그림 4. 보안 그룹 설정
Fig. 4. security group setting

6.2.3.2 역할 기반 보안 룰셋 생성

본 논문에서는 그림 5와 같이 조직 내 그룹별로

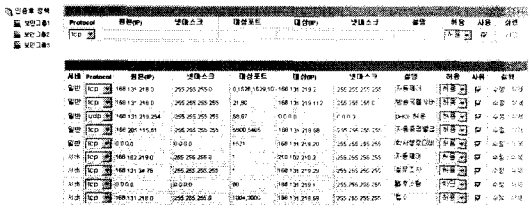


그림 5. 보안 룰셋 설정
Fig. 5. security rule-set setting

네트워크 자원 접근 제어 보안 룰셋을 설정하여 기존 단말기 중심의 단일 보안 룰셋 설정을 벗어나 조직 내 사용자권한 중심으로 네트워크 접근 제어 및 어플리케이션 접근 제어 보안 룰셋을 구현하였다

6.2.3.3 상태 모니터링

단말기와 사용자를 매칭시켜 실시간으로 네트워크 상황을 모니터링을 할 수 있도록 구성함으로써 그림 6과 같이 기존 단말기의 상태뿐만 아니라 단말기를 사용하는 실 사용자까지 실시간으로 모니터링 할 수 있다.

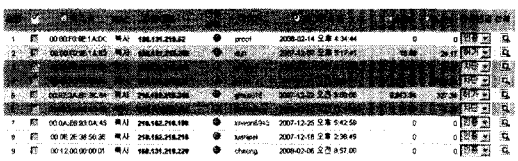


그림 6. 네트워크 상태 모니터링
Fig. 6. Realtime network monitoring

Ⅶ. 성능 테스트

7.1 보안 게이트웨이를 이용한 보안 룰셋 성능 테스트

본 논문에서 제안한 패킷 필터 보안 게이트웨이는 Xeon 2.4 Single CPU와 Memory 512M의 하드웨어 사양과 Linux OS Kernel 2.6.11을 이용하여 구성하였다. 이를 이용한 보안 룰셋의 성능 검증은 조직 내 관리 인원 3,000여명, 유동 인구 500여명에 달하는 광주 지역의 모 대학을 표본 대상으로 패킷 제어 실험을 실시하였다. 이 대학의 경우, 내부 네트워크 관리 시에 약 2,000여개의 역할 기반 보안 룰셋을 필요로 하였다.

7.1.1 역할 기반 보안 정책 개수에 따른 시스템 성능

그림 7은 보안 게이트웨이 내의 보안 룰셋 증가에 따른 시스템의 영향을 분석한 것으로 정책 개수

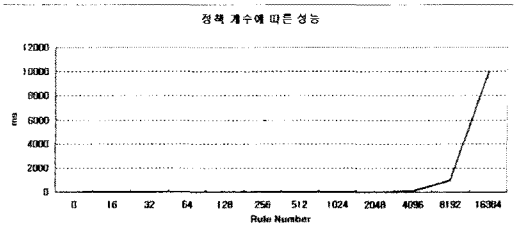


그림 7. 정책 개수에 따른 성능
Fig. 7. Performance by policy count

가 4,000개 이하일 때에는 패킷의 전송 속도에 변화가 없었지만, 4,000개를 초과하는 순간에 전송 속도가 증가하기 시작하였다.

실험 결과, 관리 인원 6,000명 정도 규모의 사이트를 4,000여개의 역할 기반 보안 룰셋을 이용하여 패킷 전송 속도의 부하 없이 운용할 수 있을 것으로 예상된다.

7.1.2 CPU와 Kernel에 따른 시스템 성능

그림 8은 보안 게이트웨이의 시스템 커널 버전과 하드웨어 사양에 따른 패킷 제어 처리 시간의 관계를 나타낸 것이다. 실험 결과, 정책 개수가 15,000개 이하 일 때에는 CPU와 커널의 종류에 관계없이 패킷의 전송 속도가 일정하게 증가하다가, 정책 개수가 15,000개를 초과하는 순간 CPU와 커널 특성에 따라 성능이 변화함을 알 수 있다. 그림 8에서 15,000개를 초과하는 보안 룰셋을 적용하였을 때에 패킷 필터 보안 게이트웨이의 CPU 성능과 OS 커널 버전이 보안 룰셋의 처리 지연 시간에 영향을 미치는 것을 확인할 수 있다.

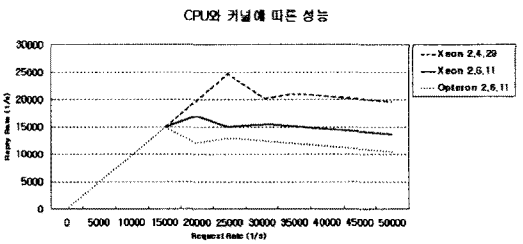


그림 8. CPU와 커널에 따른 성능
Fig. 8. Performance by CPU & kernel

Ⅷ. 결 론

8.1 사용자 중심의 보안 시스템 구현

네트워크 접근 제어를 단말기와 사용자를 매칭시켜 관리/관제함으로써 침해사고가 발생할 경우에 즉

각적인 대응이 가능하다. 또한, 네트워크 레벨뿐만 아니라 어플리케이션 레벨의 복잡 다양한 접근 제어 정책을 조직그룹별 네트워크 자원 접근 권한과 연동하여 광범위하고 개방적인 내부 네트워크를 안정적이고 효과적으로 관리감독 할 수 있다.

8.2 네트워크의 안정성 향상

서브네트워크별 방어 체계와 불법 사용자의 자동 차단을 통해 해킹과 웜 바이러스의 확산을 예방함으로써 안정적이고, 지속적인 네트워크 서비스가 가능하다.

8.3 네트워크의 보안 강화

외부 방어의 강화는 물론 보안의 사각지대였던 내부 네트워크에 방어 체계를 구축하여 네트워크 침해사고를 예방할 수 있다.

8.4 네트워크 자원의 활용성 증대

불법 사용자의 무분별한 네트워크 사용을 차단하여 네트워크 자원의 효율적인 활용이 가능하다.

참 고 문 헌

[1] 김석수, 강민균, 1999, 한국콘텐츠학회 통합보안관리 시스템에서 내부 보안을 향상시킨 보안 솔루션 구조의 설계 및 구현

[2] Network times. 통권156호 (2006. 8), pp.115-121

[3] 이경규, 이용우, 2007,The NAC Application for Wireless Sensor Networks, *한국정보과학회 07 종합학술대회논문집(D)*,257-260(4)

[4] 권덕일, 2007, NAC(Network Access Control)기술 동향 분석 및 적용방안에 관한 연구,동국대 국제정보대학원

[5] 윤종철, 강홍식, 2004, "Implement of Network Intrusion Detection System", 仁濟論叢, 503-516.

[6] 김광조, 여운동, 『KISTI 기술정보분석보고서』 30 면 2005-12.

[7] 조기천, 김은희, 신문선, 류근호, 신기수, 2001, Configuring RBAC to Object-Oriented Database Security Model, 한국정보처리학회 01 추계학술발표논문집 (상), 93-96(4).

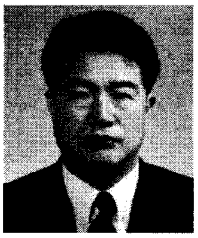
[8] Richard Kuhn,1992,"Rol3-Based Access Cont-rol", Proceedings of 15th National Computer Security Conference.

[9] 김충석, 임채호, 1994, "Implementation of Secure internet Gateway System", 論文集(Silla University Journal), 269-279.

[10] 이선중, 김정문, 예홍진, 2003, "Study Response Mo-del against ARP Redirect attack on Local Area Network", 한국정보처리학회 03 춘계학술발표논문집 (하), 2237-2240.

[11] 이은주, 박현주, 2004, "Regular File Access of Embedded System Using Flash Memory as a Storage", 정보통신전문대학원 논문집, 133-141.

이 춘 재 (Chun-jae Lee) 정회원



1987년 조선대학교 전산통계학과

2003년 조선대학교 전산통계학과 공학석사

2004년~현재 전남대학교 전자통신공학과 박사과정, 멀티미디어 기술사

<관심분야> 적응제어, 네트워크 보안

조 기 량 (Ki-ryang Cho) 정회원

1981년 광운대학교 통신공학과

1983년 건국대학교 대학원 전자공학과 공학석사

2002년 일본 오카야마대학 자연과학연구과 공학박사

현재 전남대학교 공학대학 교수

<관심분야> 파동 · 압전문제의 수치해석, 최적제어 등