

New Security Network

1. S/W명: New Security Network

2. 제작자: 김태현

주소: 대전광역시 서구 월평동 황실타운 118동 1407호. (우) 302-172

전화 번호: (042) 489-1802

핸드폰 : 017-403-0867

호출기 : 015-421-6447

한남 대학교 컴퓨터 공학과 96학번, 현재 3학년 재학중

3. S/W 전체 요약 설명

1) 개요

20세기가 첨단 산업화 시대였다면, 다가오는 21세기는 첨단 정보화 시대일 것이다. 이러한 21세기 첨단 정보화 시대에서 필요한 것은 우리의 중요한 정보자원을 우리의 경쟁자들로부터 안전하게 보호하는 것이다.

이러한 첨단 정보화 시대에 뒤지지 않는 시스템을 구현하고자 이미 Firewall 이라는 제품이 나와 있지만, Firewall은 Server 대 Server 혹은, Network 대 Network 의 정보 보호를 위한 솔루션은 될 수 있지만 이러한 정보 보호의 밑바탕이 되는 개인과 개인 혹은 개인과 Network 상의 정보 보호를 실현 시켜 줄 수 없는 단점이 있다.

New Security Network (NSN)는 이러한 Firewall의 단점 보완과 첨단 정보화 시대에 맞는 네트워크 최상의 정보 보호 솔루션을 제공하고자 개발 되었다.

2) 시스템 구조

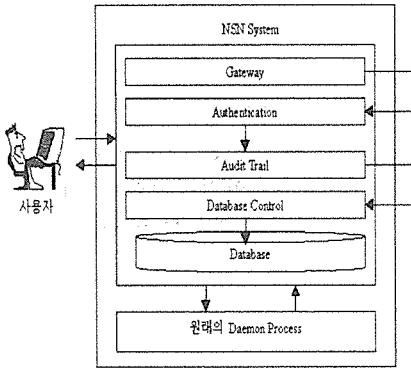


그림 211 NSN 시스템 구조도

NSN은 크게 인증 (Authentication), 데이터 베이스 (Database), 게이트웨이 (Gateway), 클라이언트(Client), 감사기록(Audit)의 5가지 모듈로 구성되어 있다.

모듈 설계부터 독립적인 설계로 모듈간에는 통신기법을 이용하여 정보를 전달하고, 모듈은 모두 독립적으로 실행되어 분산 처리가 가능하다.

a. 인증

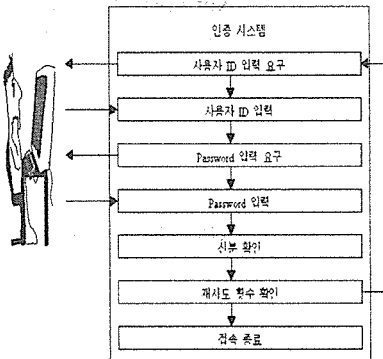


그림 22 인증 시스템의 구조도

인증은 NSN을 이용하려는 사용자의 신분을 확인 하는 절차다. 인증의 방법으로는 현재 UNIX Password 방식을 지원하며 사용자는 소정의 신분확인 절차에 따라 정확한 입력을 하였을 경우에만 시스템을 사용할 수 있으며, 그렇지 못한 경우에는 접속 해제를 요청한다.

b. 데이터 베이스

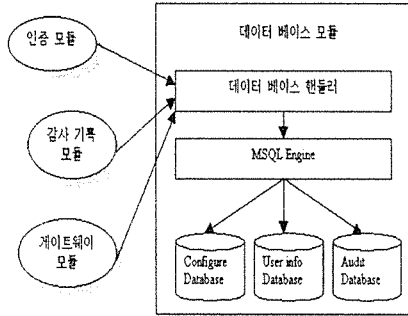


그림 231 데이터 베이스의 구조도

데이터 베이스는 모든 보안 프로그램에서 가장 중요한 부분의 하나이다. 모든 Logging관련된 데이터 정보나 시스템 환경 설정과 같은 정보를 Database 관리하고 있으며, 사용자의 인적사항이나 ID와 비밀번호 등도 Database로 관리 하고 있다.

c. 게이트웨이

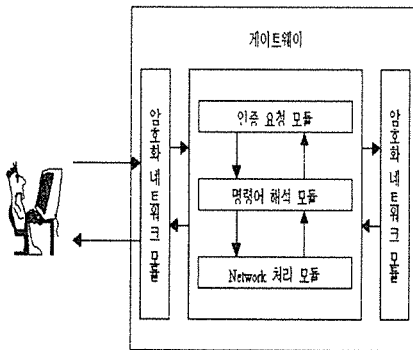


그림 261 게이트웨이 구조도

New Security Network의 핵심 부분으로 사용자의 접속 요청이 왔을 때, inetd에서 fork()되어 실행된다. 게이트웨이는 사용자 Control의 주된 기능이며, 사용자는 이 Gateway를 통하여 New Security Network의 다른 모듈과 통신을 한다.

d. 클라이언트

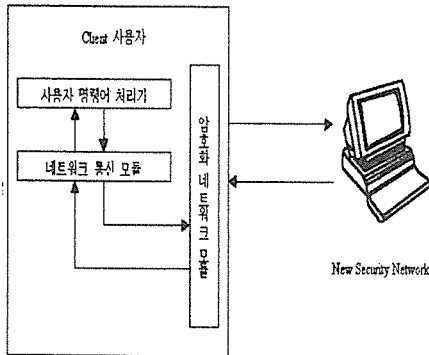


그림 27 Client의 구조도

Client는 사용자에게 요구되는 New Security Network의 구성 요소이다. Client 프로그램은 사용자에게 암호화 네트워크를 사용할 수 있는 인터페이스를 제공한다.

e. 감사기록

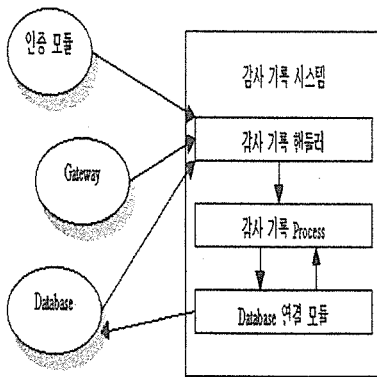


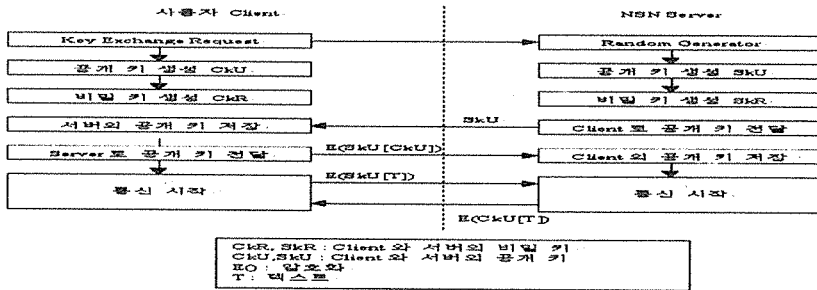
그림 28 감사 기록 구조도

감사 기록 모듈은 사용자나 관리자가 New Security Network를 사용하거나, 환경 세팅을 변경하거나 할 때, 모든 정보를 Database 엔진을 이용하여 기록하는 모듈이다.

사용자의 접속, 사용, 해제, 관리자의 접속, 환경 조정 등 모든 게 Logging의 대상이 되며, 사용자의 비정상적인 사용에 대해서도 감사 기록을 남기게 된다.

3) 기능 설명

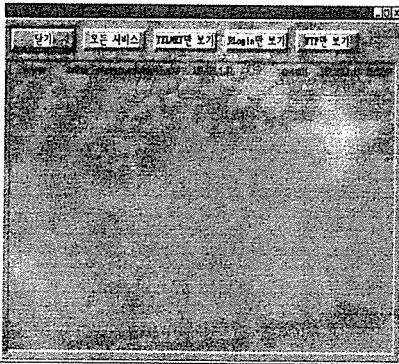
a. 암호화 네트워크 지원 : 클라이언트/서버간에 공개키 기반의 스트림 암호화를 지원하여, 정보 유출을 차단하고, 신뢰성 있는 통신을 구현한다.



[그림 3.4] Client와 Server간의 키 교환 구조

b. 키관리 문제 해결 : 자신이 사용하고 있는 암호의 키는 사용하는 사용자조차도 알 수 없는 알고리즘을 이용하여 키 관리문제를 새롭게 해결하였다.

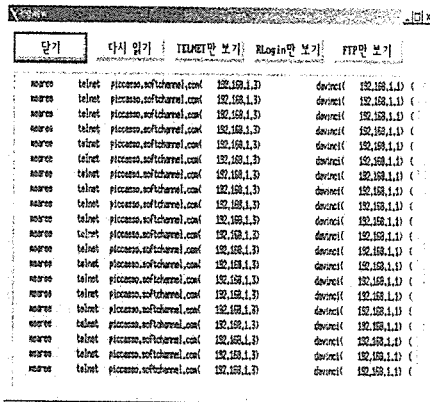
c. 리얼타임 모니터 : 현재 New Security Network를 사용하고 있는 사용자들의 정보를 Real Time Monitor 프로그램을 이용하여 실시간 감시를 할 수 있다.



Real Time Monitor는 현재 New Security Network를 사용하고 있는 사용자에게 대한 정보를 보여 준다.

또한, 각 서비스별 필터링을 제공하고 있어, TELNET, RLOGIN, FTP등 필요한 정보만을 출력 할 수 있다.

d. 로그 관리 : 사용자가 New Security Network를 사용한 흔적에 대해 기록된 감사기록 정보를 GUI로 쉽게 관리 할 수 있다.



망기	다시 읽기	TELNET만 보기	Login만 보기	FTP만 보기
source	telnet	picasso.softchanel.com	192.168.1.1	destnet(192.168.1.1)
source	telnet	picasso.softchanel.com	192.168.1.1	destnet(192.168.1.1)
source	telnet	picasso.softchanel.com	192.168.1.1	destnet(192.168.1.1)
source	telnet	picasso.softchanel.com	192.168.1.1	destnet(192.168.1.1)
source	telnet	picasso.softchanel.com	192.168.1.1	destnet(192.168.1.1)
source	telnet	picasso.softchanel.com	192.168.1.1	destnet(192.168.1.1)
source	telnet	picasso.softchanel.com	192.168.1.1	destnet(192.168.1.1)
source	telnet	picasso.softchanel.com	192.168.1.1	destnet(192.168.1.1)
source	telnet	picasso.softchanel.com	192.168.1.1	destnet(192.168.1.1)
source	telnet	picasso.softchanel.com	192.168.1.1	destnet(192.168.1.1)
source	telnet	picasso.softchanel.com	192.168.1.1	destnet(192.168.1.1)
source	telnet	picasso.softchanel.com	192.168.1.1	destnet(192.168.1.1)
source	telnet	picasso.softchanel.com	192.168.1.1	destnet(192.168.1.1)
source	telnet	picasso.softchanel.com	192.168.1.1	destnet(192.168.1.1)
source	telnet	picasso.softchanel.com	192.168.1.1	destnet(192.168.1.1)
source	telnet	picasso.softchanel.com	192.168.1.1	destnet(192.168.1.1)
source	telnet	picasso.softchanel.com	192.168.1.1	destnet(192.168.1.1)
source	telnet	picasso.softchanel.com	192.168.1.1	destnet(192.168.1.1)
source	telnet	picasso.softchanel.com	192.168.1.1	destnet(192.168.1.1)
source	telnet	picasso.softchanel.com	192.168.1.1	destnet(192.168.1.1)

감사 추적 시스템은 New Security Network를 사용하는 사용자들이 남긴 Logging을 출력한다.
 감사 추적 시스템에서는 모든 감사 기록을 출력하며, 서비스별 필터링을 제공한다.

e. 다양한 인증 : 일반적인 UNIX-Password 방식과 OneTime Password 방식을 지원한다.

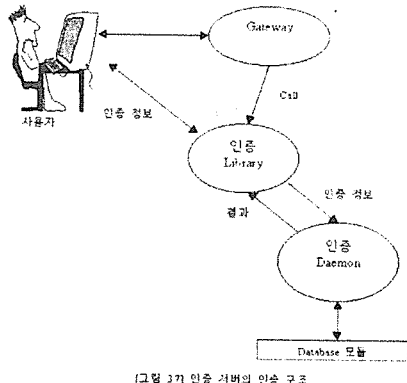
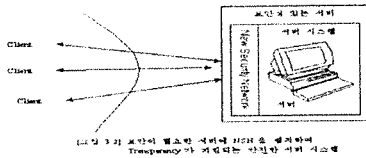


그림 3기 인증 서버의 인증 구조

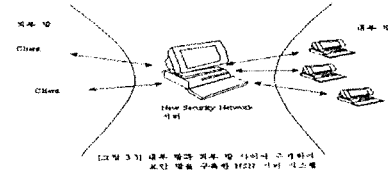
인증 시스템은, 인증 Daemon Process와 연동하여 두가지 인증 방법을 선택적으로 수행한다.
 하나는 일반적인 Password방식의 인증 시스템이며, 하나는 OneTime Password방식의 인증 시스템이다

f. 분산 처리 : NSN을 구성하는 모든 요소들이 분산 처리 시스템을 지원한다.

g. 자유로운 네트워크 구성 : NSN 네트워크 구성을 내부망/외부망 형식으로 만들 수 있고 아니면 독자적인 하나의 NSN 시스템으로 구축 할 수 있다.

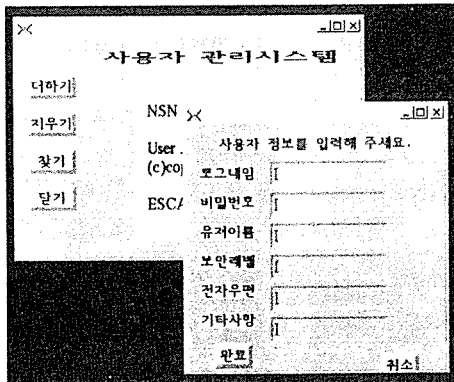


위의 그림은 New Security Network를 이용하여 보안이 필요한 서버를 안정적인 서버로 만드는 구성을 나타낸다.



밑의 그림은 보안이 필요한 네트워크 구성을 위하여 내부망과 외부망을 나누어 시스템 구성을 하였다.

h. 사용자 관리 : NSN을 사용하는 사용자 관리를 운영자가 GUI 시스템을 이용하여 쉽게 Click 함으로 생성/삭제/수정을 할 수 있다.



사용자의 추가/삭제/수정등 관리 시스템이 GUI 환경에서 쉽게 사용자를 등록 시킬 수 있다.

New Security Network에서는 사용자의 정보를 Database를 이용하여 기록 한다

개발 단계별 소요시간 및 투입 공수

프로그램 라이브러리 개발: 96년 1/4분기 ? 97년 2/4 분기

New Security Network 개발: 97년 2/4분기 ? 98년 4/4분기

개발자: 김 태 현 1명

관계 프로그램 수

약 20여개의 시스템 프로그램과 Database 엔진

사용한 개발 언어 및 툴

개발 언어: UNIX C/C++

개발 툴: Database ? msql, GUI ? Motif/OpenLook

사용 시스템

모든 종류의 UNIX 시스템 (BSD계열/SVR 계열)

직접 효과

Internet 에서 해커의 침입 차단

안정성 있는 통신 선로 확보

간접 효과

정보 통신 관련 기술 축적

NSN을 이용한 산업 확산