'03 춘계 학술발표회 논문집
한국원자력학회

원격감시시스템에 가상사설통신망 적용을 위한 모의 해킹 시험

A Study of Penetration Test for applying a Remote Monitoring System for Virtual Private Network

김정수, 김종수, 박일진, 민경식, 최영명*, 조도근**
* 한국원자력연구소, ** A3 시큐리티 컨설팅(주)

요 약

본 논문은 기존의 원격감시시스템에 인터넷을 적용하기위해 가상사설통신망(Virtual Private Network : VPN) 을 사용 시, 해킹에 대한 원격감시시스템의 취약성 시험에 대한 내용이다. 기존의 원격 감시 시스템은 사용 후 핵연료를 감시하기위한 감시 카메라 및 관련 서버 등이 설치 운영되고 있으며, 서버에 저장된 영상데이터는 전용 전화선을 이용하여 원자력 통제센터의 IAEA 서버에 모아져, 이 서버로부터 IAEA 본부 서버 및 SSAC 서버로 영상데이터가 보내진다. 현재 운영되고 있는 원격감시시스템은 1997 년 영광 3 호기에 현장시험을 거쳐 경수로 14 기에 운영 중에 있다. 하지만 국내에서 적용되고 있는 원격감시시스템의 경우, 전화선을 이용하여 통신함으로써 전화비등이 한해에 약 6,600 만원이상 소요되고있다. 그러므로 원격감시시스템을 활용한 당초 목적인 비용 절감 등에 대한 효과를 보지 못하고 있는 실정이다. 이러한 경비를 줄이기 위해 IAEA 에서는 인터넷기술로 대처할 수 있는 방법을 연구하고 있지만, 인터넷은 공개망을 이용함으로써, 해킹 등 보안에 무방비 상태로 노출되어 있다. 이를 보안할 수 있는 가상사설통신망 기술이 대안으로 부각되고 있다. 따라서 원격감시시스템에 가상사설통신망을 적용하기 위해 실험실 수준에서 가상사설통신망을 연결하여 영상데이터를 보내는 연구가 IAEA 와 공동으로 수행중에 있다. 본 논문에서는 VPN 에 대한 취약성을 알아내기 위한 모의 해킹 시험결과를 기술하였다.
시험 방법은 외부 및 내부 해킹, 두 가지 방법으로 나누어 시험하였고, 모의 해킹 도구를 사용하여 시험하였다. 시험 결과 가상사설 통신망에서 사용하는 통신장비 및 방호벽 등을 사용하면 취약성에 문제가 없는 것으로 판명되었다.

Abstract

A penetration test has been performed to verify the vulnerability of Virtual Private Network that is substitute for communication method of an existing Remote monitoring system. An existing RMS was used for the private telephone and the RMS was applied of all PWR in Korea. But, due to communication fee, IAEA wanted to replace current telephone line to the Internet line to reduce transmission cost in operating remote monitoring system. The communication cost of telephone line was estimated about $66,000/yr. Internet technology would reduce the operating cost up to 1/5. The purpose of the penetration test was to demonstrate the security of the data and system against both various external and internal hacking senarios. In most cases, hacker could not even identify the VPN system. In any cases, the system did not allow the access of the hacker to the system needless to say the data alteration or system shutdown. Two kinds of test method is chosen; one is external attack and another is internal attack. During the test, the hacking tool was used. The result of test was proved that VPN was secure against internal/external attack.

이 연구는 과학기술부 원자력 연구 중장기 개발 과제인 "국가 핵 물질 및 통제기술개발과제"의 지원을 받아 수행하였음.

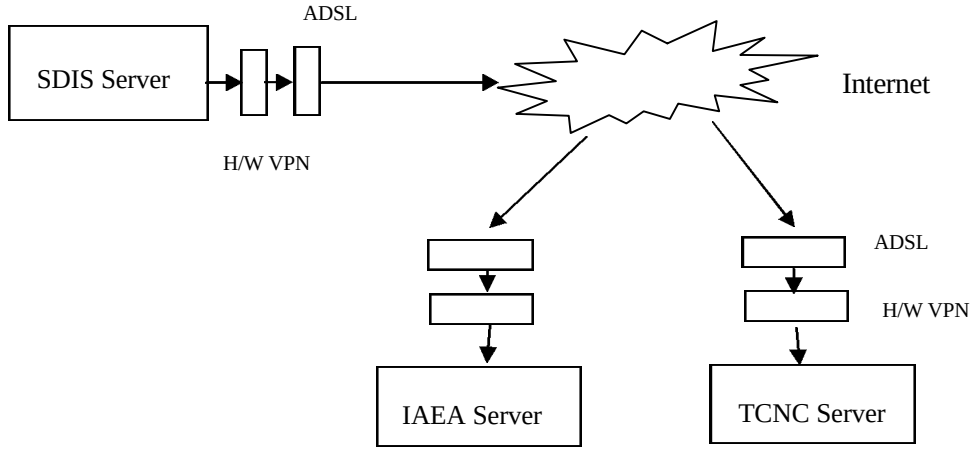
1. 서 론

핵물질의 효율적 관리를 위해 국제 원자력 기구(IAEA)는 미국 국립연구소가 중심이 되어 구축중인 원격감시시스템을 적극 수용함으로써 전 세계 원자력 발전소에 원격 감시기술을 적용하고 있다. 9 개 나라에 약 40 개의 원격감시시스템을 운영 중에 있다. 국내의 경우, 1997 년부터 영광 3 호기에 현장시험을 시작으로 현재에는 경수로 14 기 모두에 원격감시시스템이 설치되어 있으며, 이 자료들을 국가 및 IAEA 사찰 자료로 활용하고 있다[1-2]. 하지만 국내에서 적용되고 있는 원격감시시스템의 경우, 전화선을 이용하여 통신함으로써 전화비등이 한해에 약 6,600 만원 이상 소요된다. 그러므로 원격감시시스템을 활용한 당초 목적인 비용 절감 등에 대한 효과를 보지 못하고 있는 실정이다.

한편, 최근 인터넷 기술의 발달로 국내외의 통신 수단으로 인터넷이 이용되고 있으며, 비용 또한 상당히 저렴하게 제공되고 있다. 이에 착안하여 IAEA 에서는 원격감시시스템에 인터넷기술을 접목하려는 연구가 활발히 진행되고 있다. 하지만 인터넷은 공개망을 이용함으로써, 해킹등 보안에 무방비 상태로 노출되어 있다.

그러므로 이를 보안하기 위해 인터넷 상에서 암호화 기술 및 가상 사설 통신망(Virtual Private Network: VPN) 기술 등이 개발되고 있다. 또한 IAEA 경우, 발전소 시설에 핵 시설은 아니지만 환경 시료 데이터를 가상사설통신망 기술을 이용하여 IAEA 본부로 전송하는 연구과제가 1999 년 및 2000 년에 진행되었고, 성공적으로 완료되어 현재 운영 중에 있다. 그리고 이에 대한 경제적인 분석을 수행한 결과 초기비용은 현재 시스템에 비해 많이 소요되는 것으로 나타났지만, 약 1 ~ 2 년 이내에 초기 투자비가 상쇄되어 현 시스템에 비해 훨씬 적게 드는 것으로 분석되었다[3-4].

이의 일환으로 원자력연구소에서는 IAEA 와 공동으로 기존의 원격감시 시스템을 인터넷으로 대체 할 수 있는 가상사설 통신망 적용연구를 MSSP(Membership State Support Program)과제로 수행 중에 있다. 이 과제는 3 단계로 수행 중에 있는데 1 단계는 IAEA 와 TCNC 내의 발전소에 설치된 장비와 동일한 서버를 이용하여 가상 사설 통신을 수행한다. 수행시기는 2003 년 1 월에 가상사설통신망 시스템을 설치하여 약 3 개월에 걸쳐 발전소와 동일한 조건 하에서 시험을 수행하도록 되어있다. 또한 실험실 내에 설치 후 또는 설치 동안에 시스템의 취약성 분석을 위해 모의 해킹 시스템을 수행할 예정인데, 이를 통해 가상사설통신망 사용여부에 대한 정량적인 결과를 도출 할 수 있을 것이다. 1 단계 시험 완료 후, 경수로의 한 발전소를 선정하여 약 6 개월 정도 현재 시스템과 병행하여 시범 시험에 들어갈 예정이며, 이 결과를 보면서 전 발전소로 확대할 방침이다. 본 논문은 1 단계에서 각 시스템에 대한 취약성 분석을 위한 모의 해킹 시험결과 이다. 시험은 내부 및 외부로 나누어 최소의 정보(IP 정보)를 모의 해킹 공격자에게 제공하였고, 각각의 시나리오별로 수행하였다. 수행기간은 약 7 일 정도 소요되었으며, 수행 결과 내/외부 공격에도 시스템의 취약성 및 통신 시 데이터를 획득하는 데에 실패 한 것으로 판명되었다.그림 1 은 가상 사설통신 시험을 위한 전체 구성도를 보여주고 있다.



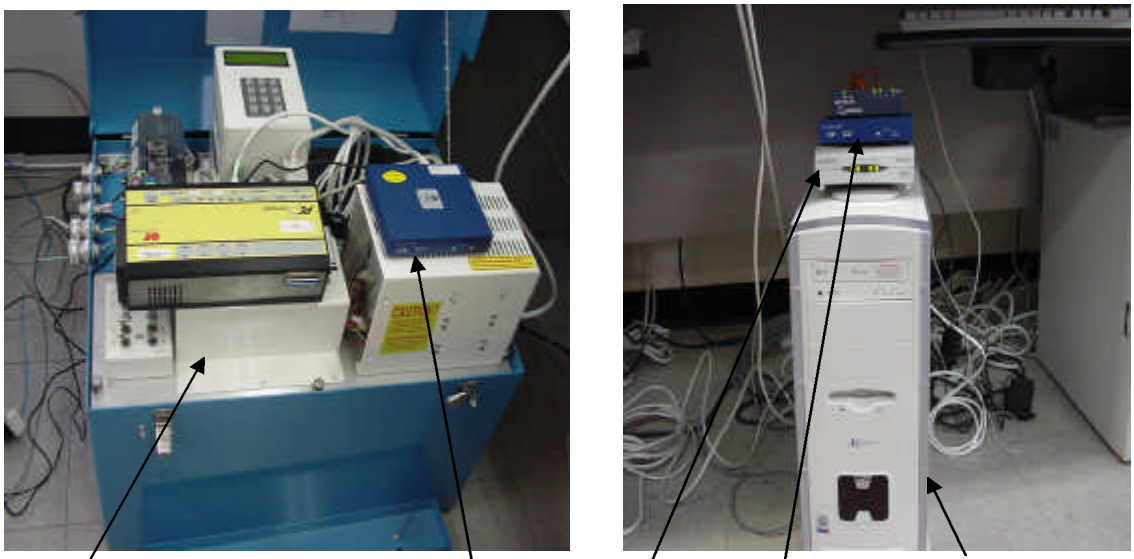


그림 1. 가상 사설 통신망을 위한 전체 구성도

본 논문의 구성은 다음과 같다. 2 장은 가상사설통신망 및 IPSec 통신방법에 대하여 언급되어 있으며, 3 장은 IAEA 와 TCNC 간의 통신 시스템 구성 및 통신방법에 대한 내용이며, 4 장은 취약성 분석을 위한 해킹 시나리오, 해킹 실험 및 결과를 언급하고, 마지막 5 장은 결론 및 향후 개발로 구성되어 있다.

2. 가상사설 통신망 및 IPSec 통신방법

가상사설 통신망은 인터넷과 같은 공개망을 사용하여 사설통신망을 구축하게 해주는 기술 또는 네트워크를 말한다[5-6]. 일반적으로 가상사설통신망은 TCP/IP 통신의 경우, IP Security 또는 IPSec 이나 Non-IPSec(PPTP, L2TP)기술을 사용하여 구축이 가능하다. IPSec(Internet Protocol Security)은 개방형 표준의 framework 으로써, IPSec 에 동일하게 연결되는 peer 들 간의 데이터 기밀성(confidentiality), 무결성(integrity), 부인방지(authentication)등을 제공한다. IPSec 은 이와 같은 보안 서비스를 IP(Internet Protocol)층에서 제공하는데, 이때

IKE(Internet Key Exchange)를 사용한다. IKE 를 사용하여, 내부정책에 기초한 프로토콜과 알고리즘의 협상 등을 관리하고, IPSec 에서 사용될 암호화 및 인증키를 생성한다. 그림 2 는 IPSec 의 암호화 및 인증 과정을 나타내고 있다.

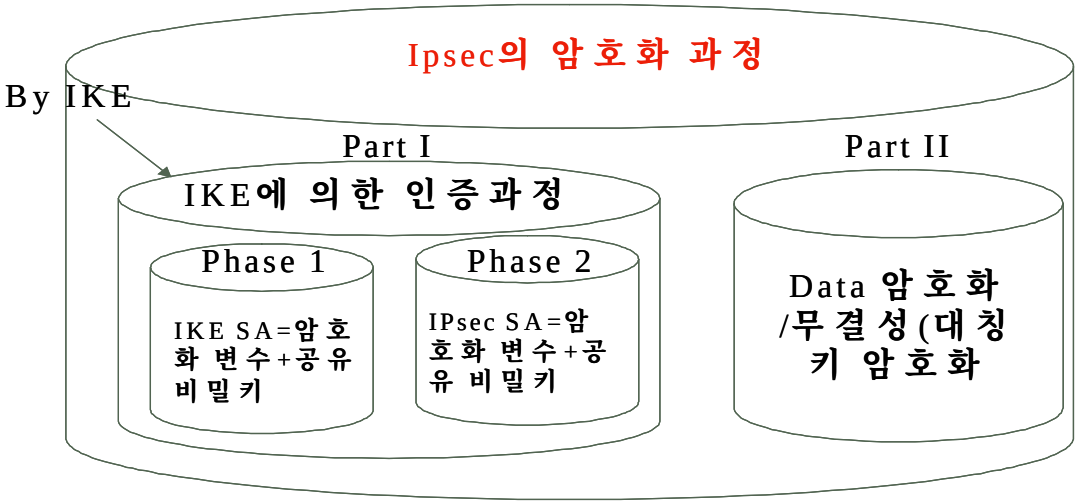


그림 2. IPSec 의 암호화 과정

그리고 각 단계별 인증 과정은 표 1 에 나타내고 있다[7]. 여기서 IKE 는 Internet Key Exchange 이고, SA 는 Security Association 이다.

표 1. IPSec 에 의한 암호화 및 인증과정

Part 1		Part 2
Phase 1	Phase 2	데이터 암호화
데이터는 non-VPN packet 으로 이동	Phase 1 의 결과를 이용 VPN packet 이용	
Secure 채널 형성 -> IKE 터널	Mode tunnel 형성	

위 표를 살펴보면 인증 전에 필요한 작업으로 터널링(tunneling)을 형성하고, 터널링이 형성된 후 암호화가 이루어짐을 알 수 있다.
한편, 일반적으로 암호화 알고리즘인 DES(Data Encryption Standard)의 경우, 56bit 의 키를 사용하는 것으로 1970 년대 미국에서 표준으로 정했지만, 이후 1990 년대에 들어와 brute-force attack 으로 쉽게 해체 될 수 있는 것으로 밝혀지면서 현재는 이 보다 더 강력한 새로운 알고리즘으로 대체되고 있다. 여기서 brute-force attack 이란 키 값이 될 수 있는 모든 경우의 수가 맞을 때까지 찾아내는 공격을 의미한다. 보통 56bit 키이면, 최상위 bit 는 1 이므로, 255 이 키 값 수이다. 하지만 컴퓨터의 성능이 향상되고 있기 때문에 이런 경우의 수를 풀 수 있는 시간이

점점 빨라지고 있다. 원칙적으로 모든 키는 이런 brute-force attack 으로 깨질 수 밖에 없다. 1998 년에 RSA(Rivest, Shamir, Adleman)conference 에서 Electronic Frontier Foundation 이라는 회사가 DES 키를 3 일 정도에 키 값을 알아냈다고 알려져 있다. 여기서 brute-force attack 을 방지하려면 키 값을 크게 하면 되지만, 키 값에 따라 암호화를 시키는 작업시간 또한 늘어난다. 그러면 이를 조화 있게 운영할 수 있은 키 값을 여러 실험을 통하여 크기가 128bit 로 밝혀졌다. 이 키 크기는 1998 년에 DES 를 깬 컴퓨터보다 백만 배 더 빠른 컴퓨터 백만 대를 가지고 brute-force attack 하면 키 값을 알아내는데 걸리는 시간이 31,623,153 년이다. 이로 인하여 triple DES 가 도입되었고, 이는 DES 를 세 번 암호화 시키는 것이므로 이들 키가 모두 다르다면 168 bit (56 * 3)의 키 사이즈가 되고, 첫 번째와 세 번째를 같은 키로 사용한다면 키 사이즈는 112bit 이다. 여기서 3DES 의 문제점은 보안성이 아니고 처리속도 이다. 즉, 처리속도가 DES 보다 세배나 느리게 된다. 참고로 기존 컴퓨터(Pentium IV)를 이용하여 112 bit triple DES 의 키 값을 알아내는데 최대 304 조년이 소요된다고 한다. 한편 소프트웨어 가상사설 통신망을 이용하여 IPSec 에 대한 인증 과정을 측정한 결과 Phase 1 의 경우, 암호화알고리즘은 DES 및 3 DES 를 혼합한 방법 그리고 인증의 경우, SHA-1 및 MD5 를 혼합한 알고리즘을 사용하는 것이 암호화 및 인증 시간 및 침투에 강인한 것으로 판명되었다[8-9]. 그림 3 은 IPSec 의 전체 형성과정을 flowchart 형태로 보여주고 있다.

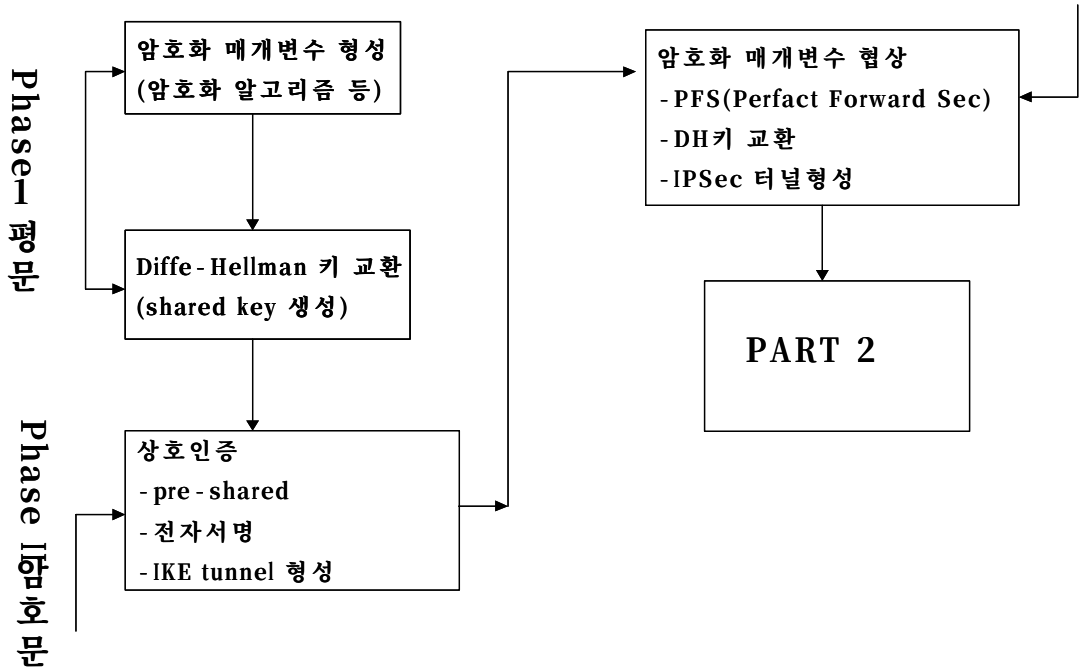


그림 3. IPSec 의 전체 흐름도

3. IAEA 와 TCNC 간의 통신 시스템 구성 및 방법

VPN 장비는 Net Screen 사의 NS5XP 장비를 사용하였다. 이 장비는 IAEA 와 협의를 거쳐 선정하였다. NS5XP 의 하드에어 version 은 3010 이며, 이에 대응하는 OS version 은 4.0 or 6.0 을 사용하고 있다. NS5XP 는 외부(Untrusted) 와 내부

(Trusted) IP(internet protocol)로 NAT(Network Address Translation) 기능을 사용하고 있다. 즉, 외부 IP 의 경우, ADSL 에서 사용하는 공인 IP 를 사용하고 있으며, 내부 IP 의 경우, 비공인 IP 인 10.0.0.x 를 사용한다. 통신 방법은 다음과 같이 설정하였다. IAEA 와 통신의 경우, SDIS 서버와 연결된 DCM-14 카메라에서 매 1 분마다 영상데이터를 찍어 저장하고, IAEA 서버로부터 매 1 시간씩 요청에 의해 영상데이터를 가져가도록 설정하였다. 그리고 TCNC 서버의 경우, 지정된 시간에 매일 1 번씩 저장된 영상데이터를 가져가는 것으로 설정하였다.
NS5XP 인 VPN 장비에 대한 구성은 Net screen 에서 제공하는 화면을 이용하여 설정하였다. 중요한 구성 파일은 다음과 같다. 그림 4 는 VPN 및 firewall 설정을 위한 초기화면을 나타내고 있다.

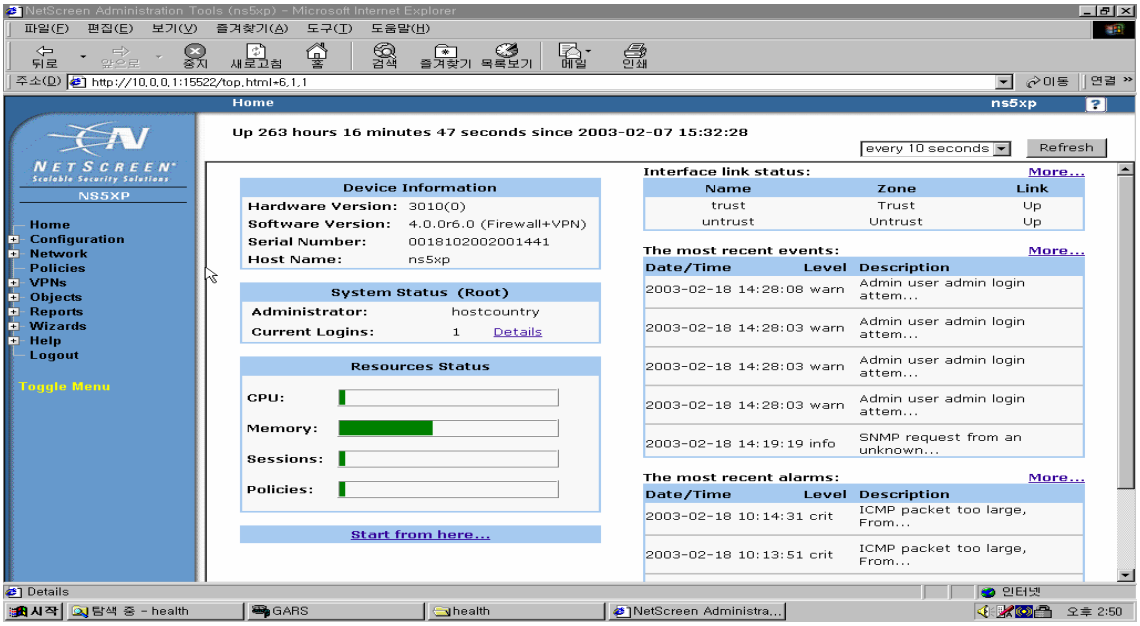


그림 4. VPN+firewall 초기화면

이 그림에서 왼쪽에 구성을 위한 메뉴들이 pull down 방식으로 설정되어 있다. 실제 VPN 설정은 통신하고자 하는 상대방 주소 및 IPSec 를 위한 암호화 알고리즘 선택 등 필수적인 구성 요소 등을 설정해야 한다. 그림 5 는 위 그림의 오른 쪽 메뉴 중 Event 에 대한 상세한 화면을 보여 주고 있다. 이 그림에서 공인 구간과 내부구간에 대한 상세한 이벤트 및 시스템의 event 등이 로그 파일로 기록되어 있음을 보여 주고 있다.

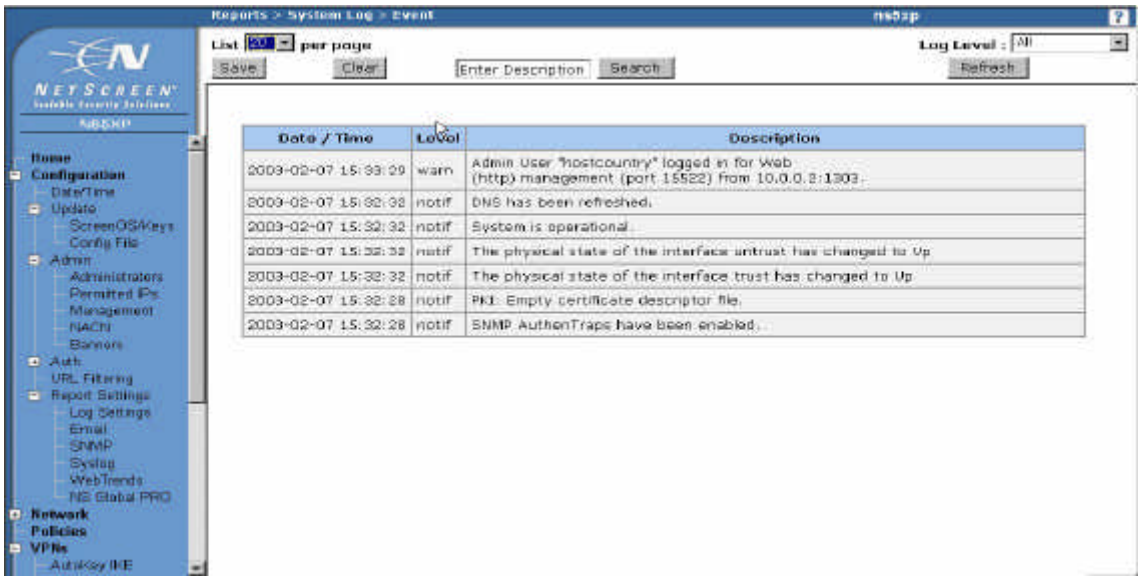


그림 5. 가상사설통신망중 Event 에 대한 상세 화면

가상사설통신망을 설정하기 위해서는 먼저 IPSec 에 필요한 Phase 1 의 변수 값들을 설정 해야 한다. 그림 6 은 이 과정을 보여주고 있다. 위 그림에서 Phase 1 은 다음과 같이 설정하였다. IPSec phase 1 은 IKE SA 로 키를 교환하고, 보안 협상을 맺기 위한 작업을 수행한다. 위 그림에서 Phase 1 의 경우, 인증 방식은 Pre-shared Secrete, 암호화는 3DES 그리고 Hash 알고리즘은 SHA-1, 마지막으로 Diffie-Hellman 알고리즘은 1024bit 를 선정하였다. Phase 1 의 결과로는 IKE 의 터널이 형성된다.

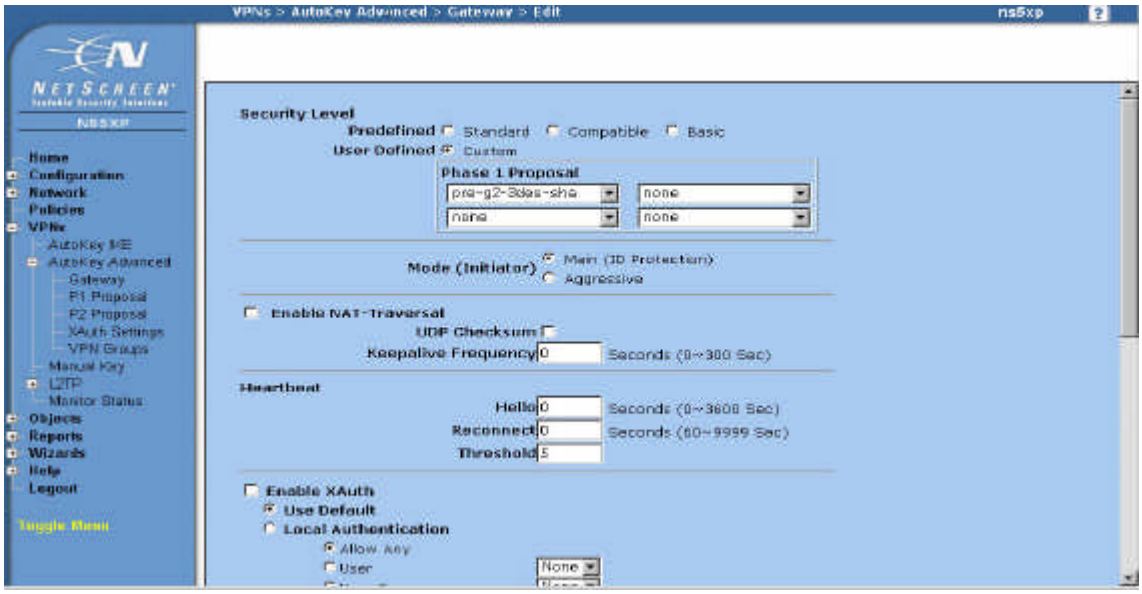


그림 6. IPSec Phase 1 설정을 위한 화면

그림 7 은 IPSec 의 두 번째 단계인 IPSec SA 로 암호화 매개변수 및 공유 비밀 키를 Phase 1 의 IKE Tunnel 을 이용하여 VPN 에 필요한 Packet(매개변수)들을 교

환한다. 위 그림에서 협상방법은 다음과 같다. 먼저 IPSec 프로토콜인 ESP(Encryption Security Protocol)을 정책협상을 통하여 교환하고, 그리고 암호화 알고리즘인 3DES 및 인증 알고리즘인 MD5 를 통하여 새로운 비밀 키를 만들어 내고 협상을 통하여 키 값들을 교환한다. 키 값들이 교환되면 IPSec 의 터널이 형성되며 IPSec 의 Part 2 로 넘어 간다.

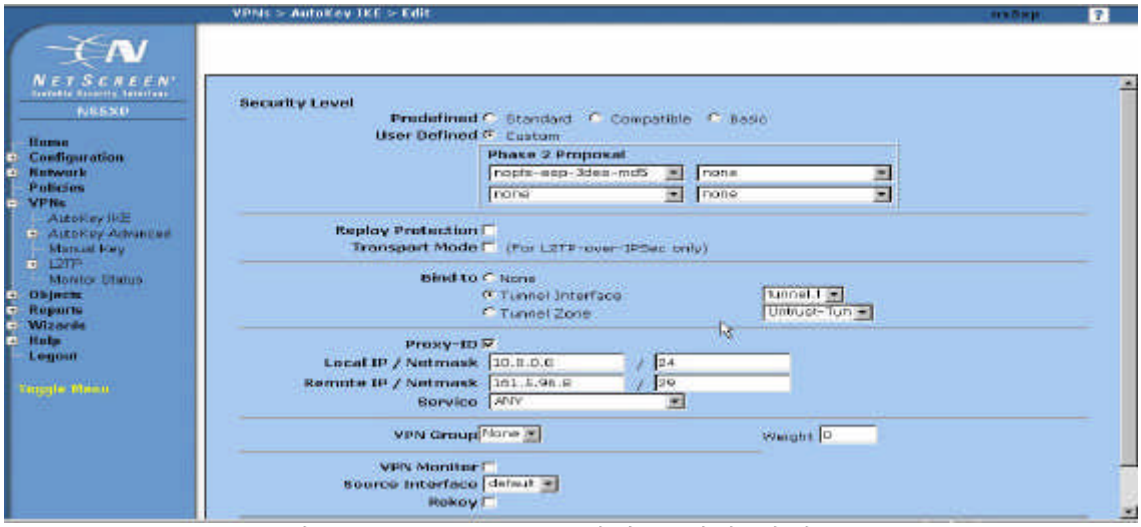


그림 7. IPSec Phase 2 설정을 위한 화면

마지막으로 정책에 대해 설정해 주어야 한다. 정책은 서버와 클라이언트를 설정해 주고 각 서버와 클라이언트 사이에 통신 방법 및 통신 포트 등을 어떻게 설정해야 하는지를 정해주는 것이다. 예를 들면, 시스템에서 인터넷 또는 ping 명령을 거부하도록 설정하면, VPN 은 외부에서 ping 명령이 와도 반응을 하지 않도록 설정하였다. 그림 8 은 정책 설정에 대한 화면을 보여주고 있다.

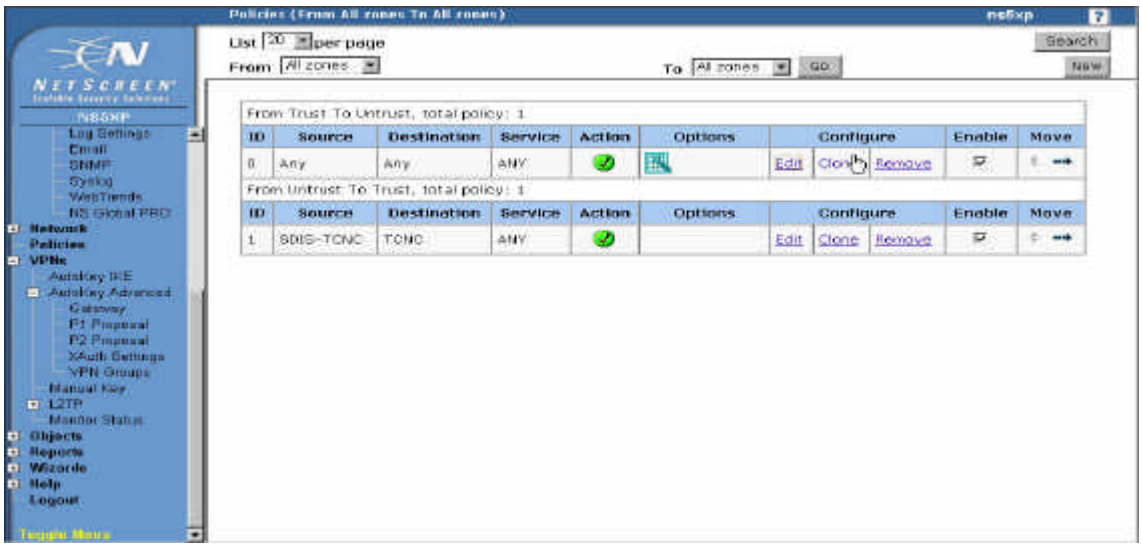


그림 8. VPN 의 정책 설정화면

그림 9 는 통신 감시 소프트웨어인 Network sniffer 를 이용하여, SDIS 및 TCNC

서버간에 데이터를 주고받는 상황을 포착한 그림이다. 아래 그림에서 회색으로 가려진 부분이 암호화된 통신을 하고 있음을 의미한다. 즉, 양쪽에 터널 링을 형성한 후 암호화된 데이터가 가상사설통신망을 이용하여, 데이터를 주고 있음을 보여주고 있다. 정상데이터의 경우는 ASCII 형태를 보여주고 있지만, 암호화된 부분은 마치 파일이 숨겨진 형태의 형상을 보여주고 있다.

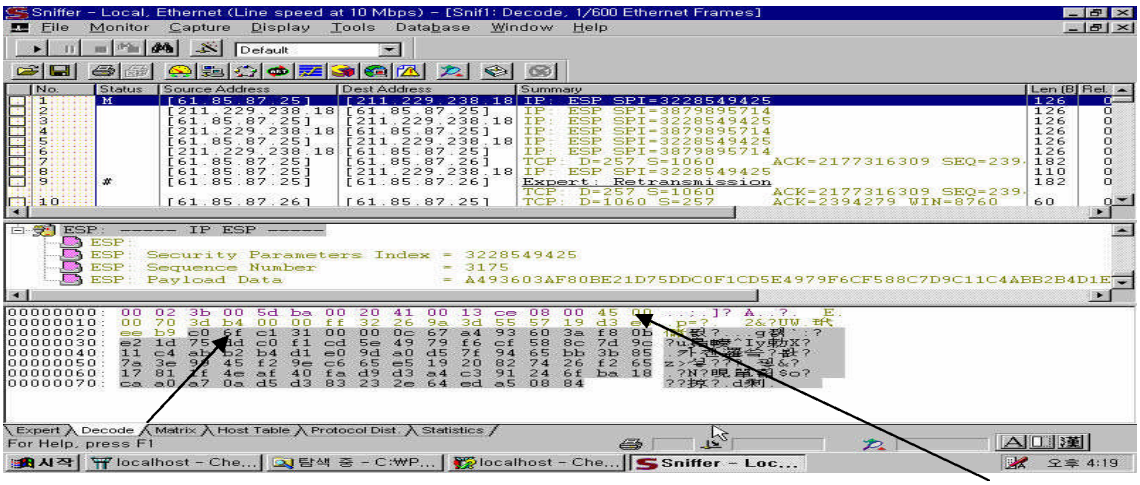


그림 9. 통신감시 소프트웨어를 이용한 VPN 통신 데이터

그림 10 은 통신을 이용하여 SDIS 서버로부터 TCNC 서버에서 받은 영상데이터를 보여주고 있다. 그림 10 에서 영상데이터를 통신 할 경우, 통신 시 그림 9 에서 암호화되어 통신하지만, 통신이 완료된 경우, 데이터가 완전 복원되어 정상적인 영상데이터를 볼 수 있다.

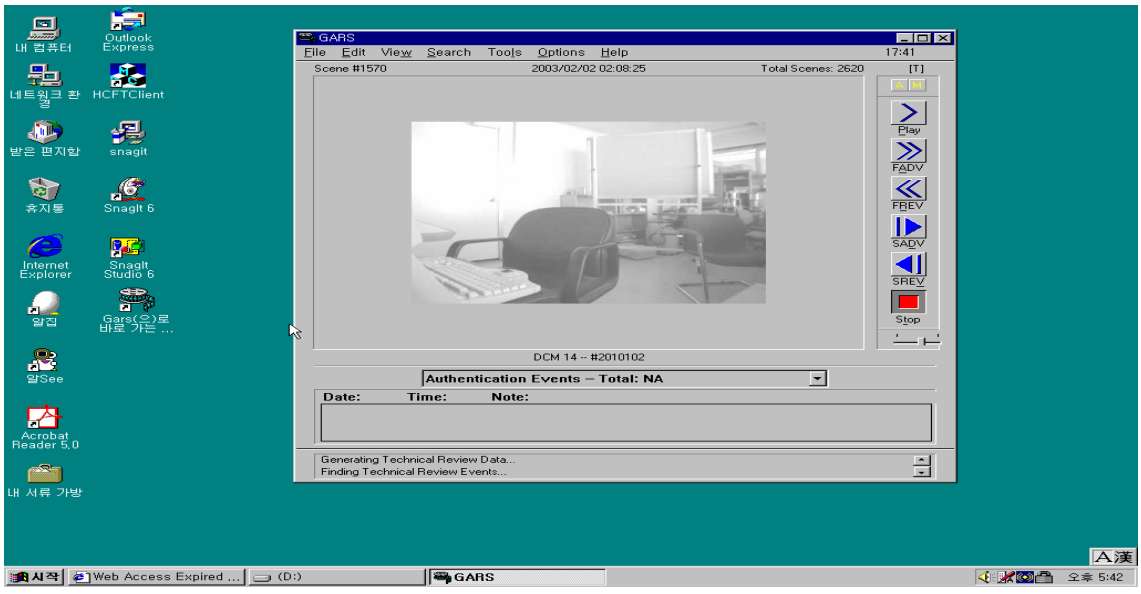


그림 10. TCNC 서버에서 받은 영상 데이터

4. 취약성 분석을 위한 모의 해킹 시험

각 시스템 및 가상사설통신망 장비에 대한 취약성 분석을 위해 모의 해킹 실험을 수행하였다. 모의 해킹에 목적 및 수행방법은 다음과 같다. 즉, SDIS 서버 및 TCNC 서버간의 VPN+Firewall 보안 시스템에 대한 보안 운영상의 취약점과 개선사항을 파악하기 위한 모의해킹 테스트(Penetration Test)로써, 대상 정보 시스템 자산들의 취약성 내역을 파악하기 위하여 해커 및 크래커들이 사용하는 기법들을 이용하는 모의해킹 시험을 수행하였다.

4.1 외부 모의 해킹 수행방법

외부 모의해킹은 공격자가 인터넷 구간에서 SDIS 및 TCNC 서버에 대한 최소한의 정보(IP Address)만을 인지한 상태라는 가정 하에서 수행하였다. 첫 번째 단계인 정보 수집단계에서 VPN 장비의 열려져 있는 포트 상태 및 VPN 시스템의 동작유무를 확인하기 위한 다양한 스캐닝을 시도하였다. 가상 사설통신망은 IPSec 프로토콜을 사용하여 TCP/IP 헤더 또는 데이터 영역을 암호화하기 때문에 일반적인 IP 스캐닝 및 공격방법은 불가능하다. 그러므로 IPSec 의 키 교환 프로토콜인 IKE(Internet Key Exchange)의 Phase 1(Main 모드/Aggressive 모드), Phase 2(Quick 모드) 단계의 통신 과정에서 발생할 수 있는 보안 허점을 주 공격대상으로 하여 모의해킹 테스트(Penetration Test)를 수행하였다. 그림 11 은 외부 모의 해킹 공격경로를 나타내고 있다.

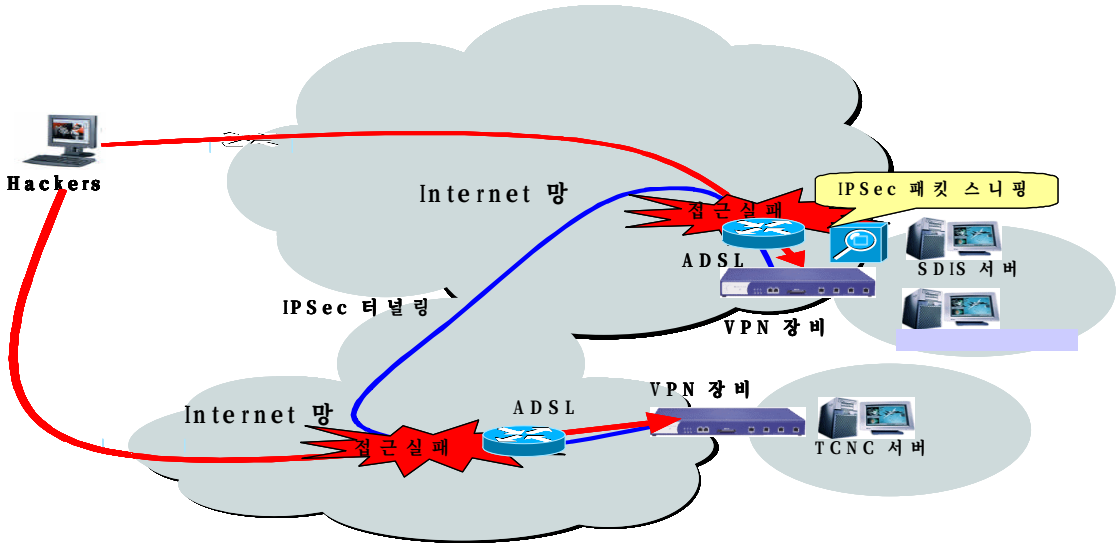


그림 11. 외부 VPN 모의 해킹 공격경로

4.2 내부 모의 해킹 수행방법

내부 모의해킹은 SDIS 또는 TCNC 서버의 내부 네트워크, 즉 Trusted 구간에 공격자의 컴퓨터를 연결하고, 내부에서 VPN+Firewall 장비에 대해서 외부 모의해킹과 동일한 방식을 사용하였다. 특히 패킷도청을 통해서 IPSec/IKE 패킷을 획득하여 키 추출 공격을 시도하거나, 직접적인 Trusted 구간의 VPN 장비나

Untrusted 상대편 VPN+Firewall 장비에 대한 다양한 해킹 방법을 사용하여 모의 해킹 테스트(Penetration Test)를 수행하였다. 그림 12 는 내부 모의 해킹 공격경로를 나타내고 있다.

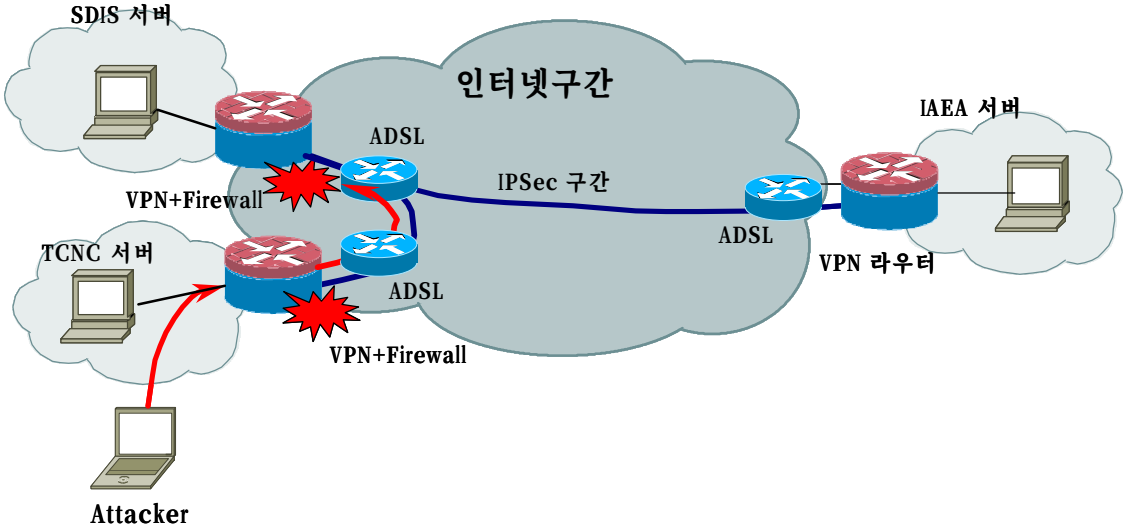


그림 12. 내부 VPN 모의 해킹 공격경로

4.3 모의 해킹 수행결과

표 2 는 모의 해킹 수행결과를 나타내고 있다.

표 2 . 모의 해킹 수행결과

시나리오 구분	대상(서버/VPN 장비)	IP 주소	결과
외부 모의해킹	SDIS Server	211.229.238.185	실패
	TCNC Server	61.85.87.25	실패
	SDIS VPN+Firewall	211.229.238.129	실패
	TCNC VPN+Firewall	61.85.87.1	실패
내부 모의해킹	SDIS Server	10.0.0.x	실패
	TCNC Server	10.0.0.x	실패
	SDIS VPN+Firewall	10.0.0.x	실패
	TCNC VPN+Firewall	10.0.0.x	실패

일반적으로 VPN 모의 해킹은 IP 보안 프로토콜인 IPSec 암호화 통신으로 인해 TCP/IP 해킹 방법을 사용할 수 없다. 특히 스캐닝에 대해서 정보 노출이 되지 않는 VPN+Firewall 의 패킷 필터링 정책으로 인해 시도할 수 공격 방법이 제한되어 IPSec 의 키 교환 프로토콜인 IKE(Internet Key Exchange) 교환 과정에서 발생할 수 있는 보안 취약점을 이용한 스캐닝 및 공격방법을 채택하였다. 그림 13 은 다수 열려진 UDP 포트 스캐닝의 예를 나타내고 있다

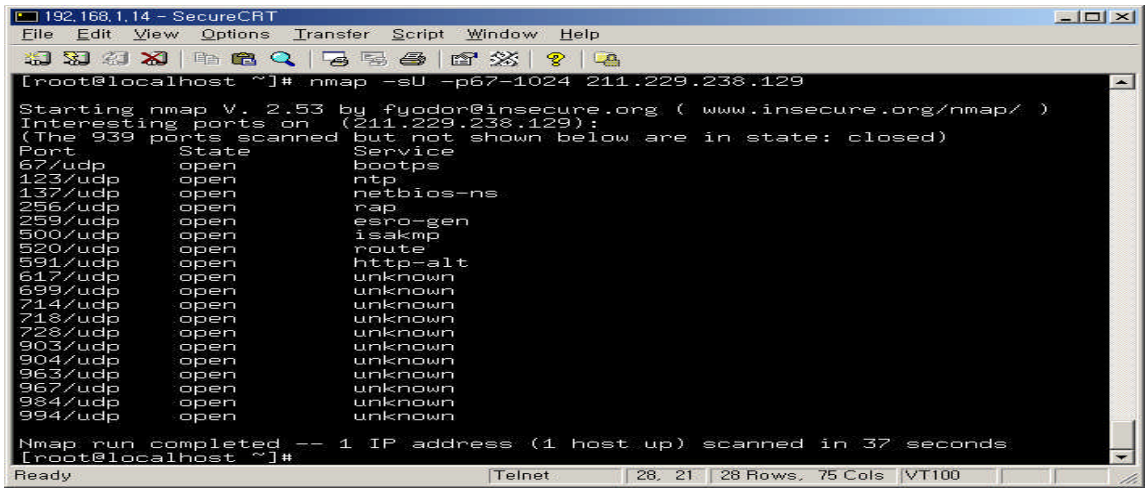


그림 13. SDIS VPN + Firewall 장비의 UDP 포트 스캔 화면

또한, 동일한 VPN+Firewall 장비(SDIS 서버단 VPN 장비-211.229.238.129)에 대해 포트 스캐닝을 한 결과, TCP(Transmission Control Protocol)를 사용하는 포트는 8888 번만 열려져 있는 것으로 확인할 수 있었으나, 접근은 차단되어 접속은 불가능하였다.

한편, VPN+Firewall 장비가 IPSec 채널을 형성하기 전에 신분 확인을 위해서 수행하는 IKE 키 교환의 첫번째 단계인 Phase 1 단계의 Main 모드에서의 Backoff (VPN 클라이언트가 보낸 IKE Security Association Request 패킷에 대해서 Responder 가 응답 패킷을 보내 주었음에도 불구하고, VPN 클라이언트로부터 응답이 없어 재 전송하기까지의 Delay 하는 기능) 패턴을 이용하여, SDIS 및 TCNC 서버의 VPN+Firewall 장비 식별을 요청하는 패킷을 보냈다. 결과는 VPN+Firewall 로 부터 어떠한 응답도 없거나, Time out 으로 인해 VPN 장비 식별에는 실패하였다. 그림 14 는 SDIS 서버의 VPN+Firewall 장비로부터 응답이 10 여개 정도가 와야 정상이지만, 나머지 응답이 모두 없어 확인에 실패하였다.

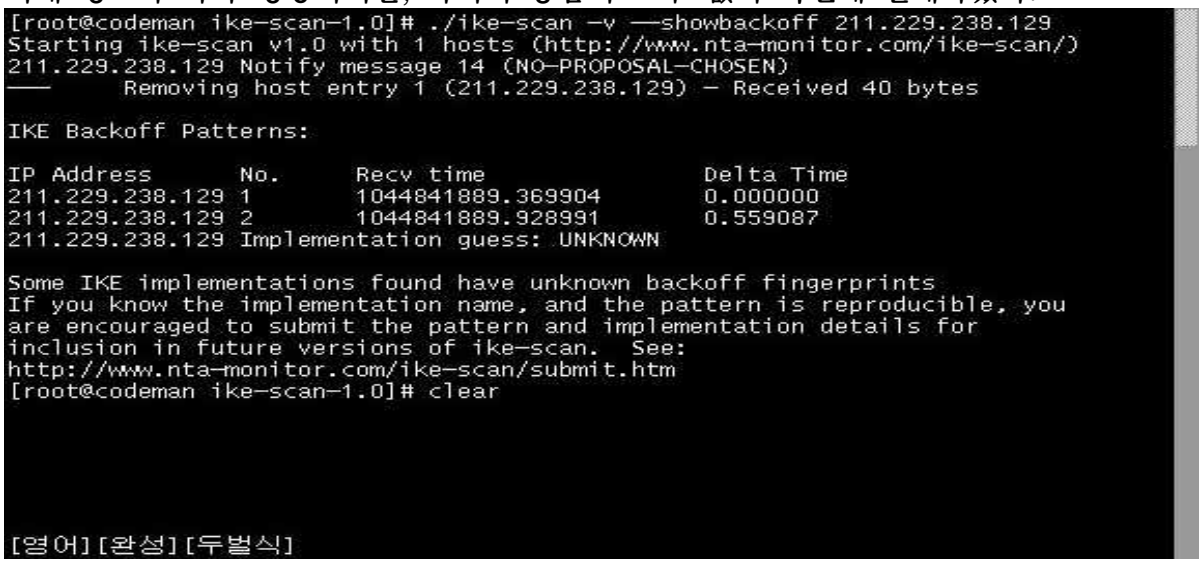


그림 14. SDIS VPN + Firewall 장비에 대한 위조 IKE 스캐닝

그 외의 여러 방법들을 이용하여, 패킷을 스캐닝 한 결과 외부 모의 해킹의 경우 실패하였다. 한편 내부의 경우, VPN+Firewall 장비의 내부 네트워크(Trusted)에서 VPN 장비에 대한 정보수집을 위해 “Nmap”툴을 이용하여 포트 스캐닝을 수행하였다. 하지만 VPN 장비자체에서 패킷 접근 차단으로 실패하였다. 다만 VPN+Firewall 의 WEB 관리자 모드가 존재하여, Web CGI 스캐닝 툴로 WEB 관련 취약점이 존재하는지 점검하였으나, 발견된 취약점이 존재하지 않았다.

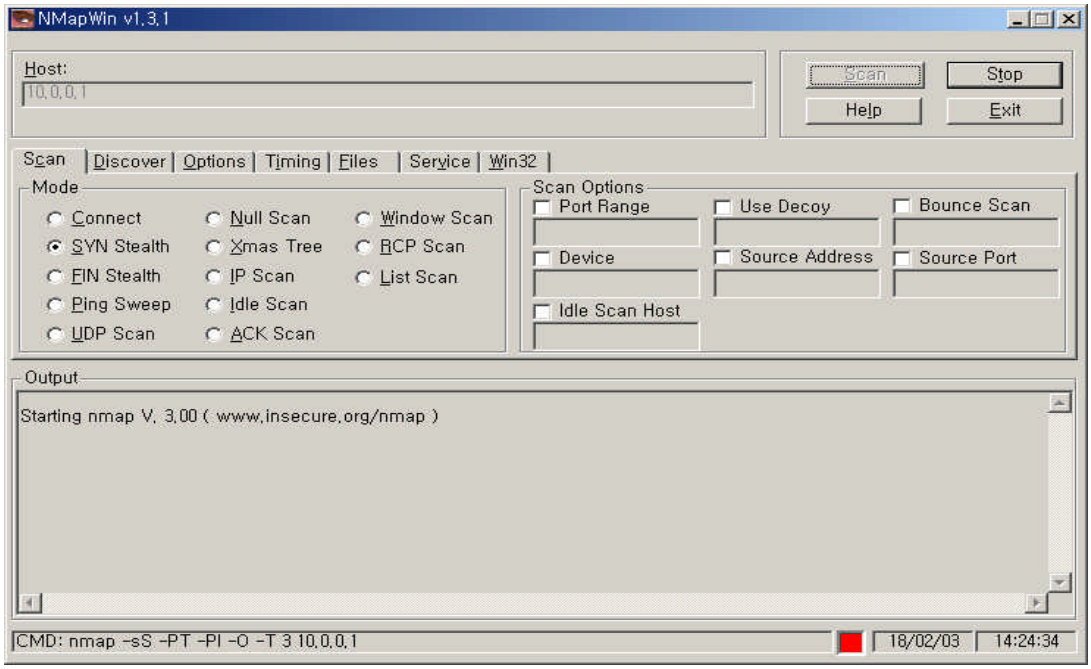


그림 15. “Nmap”툴을 이용한 TCNC VPN + Firewall 포트 스캐닝

5. 결론

본 논문은 기존의 원격감시시스템에 인터넷을 적용하기위해 가상사설통신망(Virtual Private Network : VPN) 을 사용 시, 해킹에 대한 원격감시시스템의 취약성 시험을 수행하였으며 이에 대한 시험결과 이다. 기존의 원격 감시 시스템의 경우, 전화선을 이용하여 통신함으로써 전화비등이 한해에 약 6,600 만원이상 소요되므로, 이를 줄이기 위해 IAEA 에서는 인터넷기술로 대처할 수 있는 방법을 연구하고 있으며, 인터넷의 보안성을 보안하기위해 가상사설통신망 기술을 사용해야 한다. 그러므로 IAEA 와 공동으로 수행중인 원격감시시스템에 가상사설통신망을 적용하기 위해 이와 관련한 MSSP 과제를 수행 중에 있으며, 이중 시스템 및 통신에 대한 취약성을 알아내기 위해 모의 해킹 시험을 수행하였다.
시험은 외부에서 공격자가 최소한의 정보만을 이용하여, 시스템에 침입을 시도하였지만 외부 침입이 실패하여, 공격자가 내부로 이동하여 시스템을 침입하였지만 모두 실패하였다. 내부 침입의 경우, 내부 공모자가 VPN 및 방호벽정보를 공격자에게 제공한 경우, 내부침입을 가정하여 실험하였다. 내/외부 모두 실패하였지만, 다만 내부 공격 중 Trust 구간에서 서비스 거부공격(Denial of Service)시 VPN 및

방호벽의 CPU 부하가 증가하여, VPN 기능을 제대로 수행하지 못하였다. 이를 좀 더 보완한다면, 전 발전소의 원격감시시스템에 기존시스템을 인터넷 통신으로 대체할 수 있을 것이며, 국가적으로 약 1/5 정도의 통신 비용이 절약 될 것으로 예상된다.

참고문헌

[1] James S. Regula, Communications Technologies Appropriate for Remote Monitoring, IAEA, 2001.5.

[2] W.K.Yoon, et al., Remote Monitoring for Enhanced Cooperation, 01 ESCRAD, 2001, May.

[3] H. Smart, S. Caskey, R. Martinez, Secure Transfer of Surveillance Data Over Internet Using Virtual Private Network Technology, STUK-YTO-TR174, 2001. Jan.

[4] H. Smart, et.al , Application of a Virtual Private Network to the Finnish Remote Environmental Monitoring System, 41st INMM, New Ore. 2000. Jul.

[5] J.S.Kim, et.al, The current status of developing the VPN technologies and application for Remote Monitoring, KAERI/GP-189/2002, VPN workshop for Remote Monitoring, Daejeon. 2002. Sept.

[6] Susan Caskey and Don Glidewell, Virtual Private Networks, KAERI/GP-189/2002, VPN workshop for Remote Monitoring, Daejeon. 2002. Sept.

[7] CheckPoint/Security Software, 교육 자료집(student Edition), Cybertek Holding, Jul. 2002

[8] Lee, Sang Yoon, Remote Monitoring Activities for DUPIC Facility and Planning, KAERI/GP-189/2002, VPN workshop for Remote Monitoring, Daejeon. 2002. Sept.

[9] Reid Gryder and Kerry Hake, Survey of Data Compression Tech., ORNL/TM-11797, 1991, Sept.