한국항행학회 논문지 제11권 제1호 2007년 3월

네트워크 보안성 측정방법에 관한 연구

A Study on Method for Network Security Measurement

성 경*

Kyung Sung*

요 약

정보기술의 급격한 발전과 함께 정보보호 분야에서 다양하고 복잡한 제품 및 서비스가 등장하게 되었다. 본 연구에서는 다양하고 복잡한 네트워크 보안성과 보안성능부분에 초점을 맞추어 네트워크 보안성을 평가하기 위해 필요한 평가 시스템들을 추출하고 이들 각각을 평가할 수 있는 체크리스트와 각 시스템들이 네트워크 보안성에 얼마만큼 기여하는지를 결정하여 네트워크 보안성을 평가할 수 있는 방법을 제시하였다. 또한 네트워크 보안성능을 평가할 수 있는 평가 모델과 테스트 시에 필요한 테스트 시나리오를 제시하였다.

Abstract

In recent, one of the interesting research areas is about quality of network system. Therefore many research centers including ISO are preparing the measuring and evaluating method for network quality. This study will represent an evaluating model for network security based on checklist. In addition, we propose an measuring and evaluating method for network performance.

The purpose of two studies is to present the evaluating procedure and method for measuring security of network on set workwill be identified and a measuring method and procedure will be proposed.

Key words : IDS, Firewall, Network Security, Security Evaluation, Test Scenarios

I. 서 론

네트워크정보보호제품은 특성상 일반적인 제품의 시험인증 체계와는 다른 체계를 가진다. 기존에는 네트워크정보보호제품의 보안성에 중점을 두어서 시험이 이루어져 왔다. 이러한 보안성 평가 인증에 사용되는 기준으로는 TCSEC, ITSEC 등을 사용하여 왔고, 점차 공동평가기준(CC)을 사용하는 추세이다[1].

국내의 경우에도 TCSEC, ITSEC을 참조한 네트워크정보보호제품 평가제도에 의해서 침입차단시스템과 침입탐지시스템의 K시리즈 인증이 이루어져 왔고, 향후에는 국제공통평가기준에 의해 가상사설망(VPN) 등을 인증하려는 움직임을 보이고 있다[1,2].

그러나 이러한 평가들은 정보보호 제품들에 관련된 사항들에 중점을 맞추어 평가가 되어지고 있을 뿐 이들이 유기적으로 결합되어 있는 네트워크 수준의 보안성 평가나 보안성능에 초점을 맞춘 평가는 제대로 이루어지지 않고 있는 상황이다[3,4].

또한 네트워크 보안성에 관련된 평가 방법은 기준조차 잡혀있지 않은 상황이고, 평가가 이루어진다고 하여도 객관적 평가 방법이 아닌 평가자의 주관적인 평가 방법에 의존하고 있으며 네트워크 보안성능 평가는 제품의 성능평가 방법이 보안성능 평가방법이 대체되어 평가 되어지고 있다[5,6]. 따라서 현재 평가

* 목원대학교 사범대학 컴퓨터교육과(Dept of Computer Education, Mokwon University)
· 제1저자 (First Author) : 성경
· 접수일자 : 2007년 1월 11일

되어 지고 있는 네트워크 보안성능과 보안성에 관련된 정확한 정의와 이를 평가할 수 있는 객관적인 평가 방법을 제시함으로써 보다 정확한 평가를 내릴 수 있는 연구가 필요하다[8],[9].

II. 네트워크 보안성 평가

네트워크 보안성을 평가한다는 것은 정적인 시스템이 아닌 동적으로 네트워크 상에 흐르고 있는 데이터의 안정성을 평가한다고 해야 할 것이다. 하지만 이런 동적인 데이터들에 관한 안정성을 평가할 수 있는 방법은 존재하지 않는다고 해야 할 것이다. 이렇게 동적인 데이터들에 대한 안정성을 평가할 수 있는 방법은 유기적으로 조합된 네트워크의 구성 요소들이 네트워크상에서 안정적으로 동작하는지 또한 구성 요소들이 안정성이 만족되어지는지를 평가함으로써 네트워크 보안성을 대신 평가할 수 있다.

네트워크의 보안성을 측정하기 위해서 네트워크의 구성요소들에 대한 안정성을 측정 한다고 하였다. 그런 측정을 위해서는 네트워크의 구성요소들 중 네트워크 보안성과 관련 있는 구성요소들을 분류해야만 할 것이다.

2-1 서버

서버는 우리가 알고 있듯이 통신망상에서 다른 컴퓨터에 대하여 그 통신망의 전부 또는 일부에 대한 접속과 그 통신망의 자원에 대한 접속을 제어하는 관리 소프트웨어를 운용하는 시스템을 말한다. 서버의 정의에서 알 수 있듯이 통신망의 자원에 대한 접속 제어를 담당한다. 따라서 서버에 취약한 부분이 존재하게 된다면 이는 서버 자체에 대한 치명적인 문제를 항상 안고 있는 것이며 또한 더 나아가서는 네트워크상에 다른 모든 시스템에도 영향을 미칠 수가 있는 것이다. 서버 하나의 보안성을 따진 다면 하나의 컴퓨터 시스템의 보안으로 그칠지 모르지만 서버는 항상 유기적인 네트워크 집합에 속하기 때문에 서버 하나의 시스템 문제가 아닌 네트워크 전체에 대한 보안성에도 밀접한 관계에 있다고 할 수 있다.

• 서버의 보안 요구사항

1) 서버 취약성 관리 : 서버의 취약성 관리는 서버에서 제공하는 서비스들 중 보안 취약점이 있는 서비스를 하는지, 불필요한 명령들을 사용할 수 있게 해놓았는지 주기적으로 보안 취약성에 관련된 문제들에 대해서 점검하고 있는지에 관하여 체크한다.

2) 사용자 계정 관리 : 사용자 계정에 관련하여 접근제어에 관련된 정책이 이루어지는지 사용하지 않는 불필요한 계정이 존재하는지에 관하여 체크한다.

3) 패스워드 보안 : 패스워드 보안에 대해서는 패스워드의 사용에 대한 정책에 관련된 사항들을 체크한다.

2-2 침입탐지 시스템

방화벽은 외부에서의 침입은 막을 수 있지만, 내부에서 일어나는 해킹 사고와 불법 행위에 대해서는 속수무책일 수밖에 없다는 한계가 있다. 이러한 방화벽의 단점을 보완하기 위해 개발된 시스템이 침입탐지 시스템(IDS : Intrusion Detection System)이다.

IDS는 침입탐지 시스템이 효과적인 차단에 실패했을 때, 이에 따른 피해를 최소화하고 해커의 공격에 방어하고 추적하는 기능이 내장되어 있으며 네트워크와 시스템 관리자가 부재중일 때도 정해진 규칙에 따라 해킹에 적절히 대응할 수 있게 설계된 시스템이다.

침입탐지 시스템은 허가되지 않은 사용자로부터 접속, 정보의 조작, 오용, 남용 등 컴퓨터 시스템 또는 네트워크 상에서 시도되었거나 진행 중인 불법적인 침입의 예방에 실패한 경우 취할 수 있는 방법으로 의심스러운 행위를 감시하여 침입자를 조기에 발견하고 실시간 처리를 목적으로 하는 시스템이다. 이는 네트워크 상에서 네트워크 보안에 위배 되는 행동들을 조기에 발견할 수 있는 기능을 지원해 주기 때문에 이를 평가함으로써 네트워크 보안성을 평가할 수 있다.

• 침입탐지 시스템 보안 요구사항

1) 감사 데이터 생성 기능 : 감시 대상 시스템으로부터 감사 데이터를 수집할 수 있는 기능에 대한

체크

2) 보안위반 분석 : 알려진 시스템 보안위반 사건에 대한 목록을 바탕으로 보안 위반임을 판단할 수 있는가를 체크

3) 보안감사 대응 : 보안 감사에 대하여 실시간으로 발견 및 조치를 취할 수 있는가에 대한 체크

4) 보안정책 기능 : 보안정책의 변경 수정 삭제에 관련된 기능을 체크

5) 자동 업데이트 기능 : 자동 업데이트를 통해 항상 최신의 침입탐지 패턴을 유지할 수 있는가를 체크

6) 다양한 네트워크 환경 지원

2-3 방화벽

방화벽은 네트워크의 보안 사고나 위협이 더 이상 확대되지 않도록 막고 격리하는 것이라고 할 수 있다. 특히 어떤 기관의 내부 네트워크를 보호하기 위해서는 외부로부터 불법적인 트래픽이 들어오는 것을 막고, 허가 인증된 트래픽만 허용하는 적극적인 방어 대책이라고 할 수 있겠다. 시스템은 기관 또는 조직의 보안 정책에 따라 인가된 인터넷 서비스에 대한 접근을 허용하고, 인가되지 않은 서비스에 따르는 트래픽을 철저하게 막음으로써 효율적인 보안 서비스를 제공하도록 한다.

이러한 시스템은 네트워크의 흐름을 정해진 정책에 따라 통제할 수 있는 기능을 가지고 있는 시스템을 의미한다. 네트워크상의 불법적인 공격이나 취약한 부분을 막아줌으로써 보다 안전하게 내부 네트워크를 유지할 수 있도록 도와준다. 때문에 이러한 방화벽에 보안성을 평가함으로써 네트워크의 보안성을 평가할 수 있는 척도로 삼을 수 있다.

• 방화벽의 보안 요구사항

1) 보안정책 : 보안정책에 관련하여 지켜져야 할 정책들이 제대로 지켜지고 있는지 또는 효율적으로 이루어지고 있는지 체크한다.

2) 로깅 : 보안에 필요한 로깅 데이터들이 정확하게 기록되는지 체크한다.

3) 운영 : 운영기능의 사용성에 관련된 부분들을 체크한다.

4) 필터링 : 패킷 필터링에 관련된 규칙들에 대한 설정 항목들을 체크한다.

Ⅲ. 보안성 평가방법

지금까지 네트워크 보안성을 평가할 수 있는 대상들을 선별하고 대상들의 평가 요구사항들에 대해 정리하였다. 이를 바탕으로 각 대상들의 각각의 요구사항을 평가할 수 있는 방법으로 요구사항별 체크리스트를 제시하여 이를 평가할 수 있는 지표를 제시하도록 하겠다.

각각의 평가 대상별 체크리스트의 체크항목은 Yes, No, N/A로 구성되어진다. 평가 대상별 체크 항목의 개수와 체크 항목 중 Yes로 체크된 항목의 퍼센트(%)율로 각 대상의 보안성을 측정하고 전체 네트워크 보안성은 각 대상별 보안성을 전체 네트워크 보안성 참여 비율로 계산한 합으로 구해질 수 있다.

• 각 대상별 보안성 측정방법

$$\frac{Yes\text{로체크된체크항목의개수}}{\text{전체체크항목의수}(N/A\text{로체크된항목은제외})} \times 100$$

• 전체 네트워크 보안성 측정방법

$$\sum(\text{평가대상별보안성} \times \text{각대상별} \mathit{weight}\text{값})$$

•각 대상별 가중치 값 : 서버(15%), 방화벽(40%), 개인용컴퓨터(10%), 보안취약성 진단 도구(15%), 침입탐지 시스템(30%)

Ⅳ. 네트워크 보안성 성능평가

보안 성능을 평가한다는 것은 유기적으로 연결된 네트워크가 외부로부터의 공격에 얼마만큼 대응을 할 수 있는지를 평가하는 것이라 할 수 있겠다. 그러나 유기적으로 연결된 실제 네트워크 상에서 보안성능을 시험할 수 없다는 것은 잘 알고 있는 사실이다. 현재 많은 시험기관에서는 단순히 장비들의 처리량과 지연, 연결 수 등을 평가하는 장비의 성능시험에 초점을 맞추어 장비의 인증을 하고 있다. 이는 엄격하게는 같은 성능평가지만 단순히 장비의 성능만을

측정하는 수준에서 끝나고 있다고 말할 수 있겠다. 하지만 실제 네트워크 상에서 보안성능을 시험할 수 없기에 네트워크의 보안성능을 평가할 수 없다. 따라서, 장비시험을 통한 네트워크 보안성능을 평가할 수밖에 없기 때문에 기존의 장비의 성능평가 측정방법에 보안성을 측정할 수 있는 요인을 더하여 네트워크의 보안성능을 측정할 수 있는 방법을 제시 하도록 하겠다. 본 연구에서는 네트워크 보안장비인 침입탐지시스템에 대한 보안성능 평가 방법만을 제시하도록 하겠다.

4-1 성능시험 지표

• 처리량(throughput)

DUT(Device Under Test)/SUT(System Under Test)가 패킷을 폐기(drop)하지않으면서 처리할 수 있는 최대량

• 동시 연결수(concurrent connection)

호스트들 혹은 호스트와 DUT/SUT 사이의 연결의 총합. '연결(CONNECTION)'은 호스트 혹은 호스트와 DUT/SUT 사이에서 알려진 프로토콜을 이용하여 데이터를 교환하도록 합의한 상태를 의미하지만, 동시 연결에서는 모든 존재하는 연결이 데이터를 전송할 수 있는 상태라는 것을 의미한다. 즉, 연결이 데이터를 전송하지 못한다면, 그 연결은 동시 연결수에서 제외.

•지연(latency)

DUT/SUT가 패킷을 받아서 목적하는 인터페이스로 전송하는 사이에 걸리는 시간. DUT/SUT의 패킷 처리 방식에 따라 컷 스루우(cut through)방식으로 구분되나, 일반적으로는 다음과 같이 정의할 수 있다.

지연 시간 = 수신 시간 - 송신 시간

4-2 성능시험 구성

•시험구성

시험구성도는 Tester는 하드웨어 기반의 시험장비이고, SUT(System Under Test)가 시험 대상인 침입차단 시스템이다. PC1, PC2, PC3은 애플리케이션 레이어에서의 시험에서, 에플리케이션 테스트 제품을 설치하여 사용한다. Tester는 두 개의 시험 포인트(testing point)를 가지는데, 시나리오에 따라서 두 지점을 입력과 출력으로 연결하여 시험한다.

•규칙 집합

처리량 시험에 많이 사용되는 침입탐지시스템 단일 규칙(single rule)은 다음과 같다. 즉, 각각의 인터페이스에서 출발지 주소, 목적지 주소, 사용하는 프로토콜이나 포트번호에 상관없이 무조건 허용하는 규칙이다. 일반적인 침입탐지시스템 성능시험 시에 자주 사용되는 단일 규칙대신에 제안하는 50개의 규칙집합은 대략 다음과 같이 비교적 실제환경에 적용가능한 규칙들로 구성하였다.

내부 → DMZ: 주요 서비스만 허용
(예: HTTP, telnet, ftp, DNS, SMTP, POP3 등)
내부 → 외부: 주요 서비스만 허용
(예: HTTP, telnet, ftp, DNS, SMTP, POP3 등)
외부 → DMZ: 주요 서비스만 허용
(예: HTTP, telnet, ftp, DNS, SMTP, POP3 등)
DMZ → 내부: 모든 서비스 거부
DMZ → 외부: 주요 서비스만 허용
(예: DNS, SMTP, POP3 등)
Default로 위의 규칙에 해당하지 않는 모든 패킷은 거부

규칙 집합은 1번부터 순서적으로 비교를 한다. 규칙에 일치(match)하는 것이 있으면, 정책에 따라서 패킷의 허가(allow)/거부(deny)를 결정한다. 규칙이 일치하지 않으면, 다음 규칙을 비교하고, 마지막 규칙의 비교가 끝나면 기본(default)정책에 따라서 허가/거부가 결정된다. 일반적으로 기본정책은 모든 패킷을 거부하는 것이다. 따라서, 규칙 집합에서는 허용할 패킷들의 규칙을 설정하고, 여기에서 허용되지 않은 모든 패킷은 거부된다.

ext와DMZ 인터페이스에는 내부 네트워크에서 시작한(initiate) 접속만 허용하도록 ACK 필드를 확인한다고 가정한다. 이러한 규칙 설정은 침입차단 시스템에 따라서 다양하기 때문에 여기서는 일반적인 규칙만 열거 하였다. 또한 규칙을 실제 패킷과 비교하는경우, 각각의 인터페이스에 해당하는 규칙만을

사용한다. 따라서, 각각의 인터페이스별로 50개의 규칙이 있는 것으로 가정하였다.

표 1. 시험용 규칙집합
Table. 1 Test Scenario

순서	인터페이스	출발지 주소	목적지 주소	프로토콜	서비스	정책
int.1	int	내부망	DMZ	TCP	80(HTTP)	허용
int.2	int	내부망	DMZ	TCP	8080(HTTP)	허용
int.3	int	내부망	DMZ	TPC	23(telnet)	허용
…	…	…	…	…	…	…
int.48	int	내부망	any	TCP	80(HTTP)	허용
int.49	int	내부망	any	TCP	8080(HTTP)	허용
int.50	int	내부망	any	TCP	23(telnet)	허용
default	int	any	any	any	any	거부
ext.1	ext	외부망	DMZ	TCP	80(HTTP)	허용
ext.2	ext	외부망	DMZ	TCP	8080(HTTP)	허용
…	…	…	…	…	…	…
ext.50	ext	외부망	DMZ	TCP	23(telnet)	허용
default	int	any	any	any	any	거부
DMZ 1	DMZ	DMZ	내부망	any	any	거부
…	…	…	…	…	…	…
DMZ.47	DMZ	DMZ	외부망	TCP	25(SMTP)	허용
DMZ.48	DMZ	DMZ	외부망	TCP	53(DNS)	허용
DMZ.49	DMZ	DMZ	외부망	UDP	53(DNS)	허용
DMZ.50	DMZ	DMZ	내부망	TCP	110(POP3)	허용
default	DMZ	any	any	any	any	거부

4-3 성능시험 시나리오

●시험 시나리오1 - 처리량
① 시험 목적
- 다양한 조건에서의 처리량 측정
② 시험 조건
- 규칙 집합 수 변경(1, 50)
- 로깅 기능
- 패킷 사이즈 변경(64, 512, 1024, 1518 byte)
③ 시험 방법
- 규칙 집합이 50개인 경우, 50번 규칙에 의해서 허용되는 패킷을 사용하여 시험 수행(예) 외부망에서 DMZ로의 telnet 접속 패킷

표 2.. 시나리오 1
Table. 2 Scenrio 1

번호	로깅	규칙집합	패킷 사이즈	처리량
1-1	Off	1	64	80
			512	58
			1024	90
			1518	100
1-2	Off	50	64	60
			512	70
			1024	80
			1518	90
1-3	On	1	64	70
			512	80
			1024	85
			1518	90
1-4	on	50	64	65
			512	75
			1024	80
			1518	85

●시험 시나리오2 - 지연
① 시험 목적- 다양한 조건에서의 지연측정
② 시험 조건- 규칙 집합 수 변경(1, 50)- 로깅 기능(off/on)- 패킷 사이즈 변경(64, 512, 1024, 1518 bytes)
③ 시험 방법- 규칙 집합이 50개인 경우, 50번 규칙에 의해서 허용되는 패킷을 사용하여 시험 수행- 시나리오 1과 동일(예) 내부망에서 외부망으로의 telnet 접속 패킷

표 3. 시나리오 2
Table. 3 Scenario 2

번호	로깅	규칙집합	패킷 사이즈	처리량
2-1	Off	1	64	30
			512	40
			1024	50
			1518	60
2-2	Off	50	64	40
			512	45
			1024	50
			1518	65
2-3	On	1	64	50
			512	55
			1024	60
			1518	70
2-4	on	50	64	55

표 4. 규칙집합(시나리오 3)
Table. 4 Regular Set(Scenario 3)

순서	인터페이스	출발지 주소	목적지 주소	프로토콜	서비스	정책
ext.50	ext	외부망	DMZ	TCP	21(FTP)	허용
ext.50	ext	외부망	DMZ	TCP	80(HTTP)	허용

표 5. 시나리오 3
Table. 5 Senario 3

번호	로깅	규칙집합	애플리케이션	처리량
3-1	Off	1	FTP	80
			HTTP	90
3-2	Off	50	FTP	75
			HTTP	85
3-3	On	1	FTP	80
			HTTP	95
3-4	on	50	FTP	70
			HTTP	80

•시나리오 4-세션 용량

① 시험 목적- 초당 유지 가능한 세션 용량 측정

② 시험 조건- 단일 규칙 적용- 로깅 기능(off/on)- 연결 요청 비율(개/sec) 변경 (1,000~2,000)

③ 시험 방법- 외부망과 DMZ내 2대의 PC에 설치된 Chariot을 이용하여 연결 요청 비율(개/sec)을 변경하며, 일정 시간 후 세션 수가 더 이상 증가되지 않을 때, 동시 연결(concurrent connection)수 측정- 시나리오 3과 동일

표 6. 시나리오 4
Table. 6 Scenario 4

번 호	연결 요청 비율(개/sec)	동시 연결(개)
4-1	1,000	800
4-2	2,000	800
4-3	5,000	750
4-4	10,000	700
4-5	15,000	600
4-6	20,000	450

•시나리오 5-비트 전달 비율

① 시험 목적- 규칙에 의해서 허가된 패킷의 처리량측정- 거부 패킷의 비율을 증가시키며 처리량을 측정하여, DoS 공격시 침입탐지시스템의 대처 능력을 파악

② 시험 조건- 규칙 집합 적용(50)- 로깅 기능(on)- 패킷 사이즈 변경(64, 1418 bytes)- 허용/거부 패킷의 비율 변경(0~100%)- 최대 부하(100/1000 Mbps)

③ 시험 방법- 허용 패킷은 50번 규칙에 의해서 허용되는 패킷 사용(예) 외부망에서 DMZ로의 telnet 접속 패킷- 거부 패킷은 50번 규칙 이후 기본(default) 정책에 의해서 거부되는 패킷 사용(예) 외부망에서 DMZ로의 SNMP 패킷- firewall에서 허용하는 최대부하로 시험 수행- 시나리오 1과 동일 - 거부 비율이 100%인 경우, down되면 Dos 공격에 취약하다는 것을 알 수 있음

표 7. 시나리오 5
Table. 7 Scenario 5

번호	허용 비율	거부 비율	패킷사이즈	처리량
5-1	100	0	64	50
			1518	60
5-2	80	20	64	60
			1518	60
5-3	50	50	64	70
			1518	80
5-4	20	80	64	75
			1518	85
5-5	0	100	64	80
			1518	90

4.4 성능시험 기준

비교시험을 하는 경우에는 동일한 성능시험 지표 및 성능시험 시나리오를 사용하여 대상 제품들의 결과를 비교하면 되지만, 인증을 목적으로 한 단독시험의 경우에는 어느 정도의 성능을 기준으로 하여 통과/실패를 판정할 것인지를 정할 필요가 있다. 다음의 기준들은 실제로 제품에 적용하여 검증된 기준이 아니기 때문에, 실제 시험 및 인증을 하는 경우에는 현황에 맞도록 수정 보완이 필요할 것이다.

처리량의 경우, 100 Mbps 제품을 가정하였다. 현재 Gbps를 지원하는 제품이 출시되고 있는 상황이어서, Gbps급 제품인 경우에는 각각의 비율에 따라 0～500 Mbps, 501～750 Mbps, 751～1000 Mbps로 바꾸어서 적용하면 될 것이다.

표 8. 등급기준
Table. 8 Grade Standard

등 급	E	D	C	B	A
처리량 (Mbps)	0 ~ 45	46 ~ 60	61 ~ 75	76 ~ 90	91 ~ 100
연결(개)	0 ~ 20,000	20,000 ~ 30,000	30,000 ~ 40,000	40,000 ~ 50,000	50,000 이상
지연(%)	처리량에서 45% 이상의 감소	처리량에서 35% ~ 45% 사이의 감소	처리량에서 25% ~ 35% 사이의 감소	처리량에서 15% ~ 25% 사이의 감소	처리량에서 15%이내의 감소

지연의 경우, 직접적인 지연의 증가로 등급을 정하기가 곤란한 경우가 있다. 예를 들어, A사 제품은 지연이 1 [micro sec]에서 3 [micro sec]로 증가하고, B사 제품이 10 [micro sec]에서 20 [micro sec]으로 증가한 경우, 비율상으로는 A사 제품이 200% 증가지만, 실제적으로는 2 [micro sec] 증가라서, B사 제품보다 성능이 좋을 수가 있다. 따라서, 처리량에 영향을 미치는 정도로 바꾸어서 등급을 정하는 것이 타당하다.

위의 기준은 다음과 같이 인증 여부를 결정하는 경우 사용될 수 있다. 즉, 인증 여부를 판단할 시나리오를 적절히 선택하고, 각각의 측정값에 대하여 등급 기준을 적용하여 A, B, C, D, E의 등급을 부여하고, 전체 시나리오에서 D등급 이상을 받은 경우에만 성능시험 기준을 만족하는 것으로 하여 인증할 수 있다. 이렇게 하여 최저 등급(D)을 만족하는 제품을 인증하고 인증을 받은 제품들의 성능을 객관적인 성능 수치로 표시 가능할 것이다.

Ⅴ. 결 론

네트워크 보안에 대해 전문적으로 평가해주는 기관이나 업체들이 많이 존재하고 있지도 않을뿐더러 설사 있다 하더라도 네트워크 보안에 대한 공통적인 평가 방법의 부재로 인하여 자체적으로 주관적인 평가 방법만을 실시하고 있다.

이에 본 연구에서는 네트워크 보안 성능을 평가할 수 있는 테스트 시나리오를 제시하였다.

참 고 문 헌

[1] A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2, NIST SP 800-29
[2] An Introduction to Computer Security: The NIST Handbook, NIST Special Publication 800-12
[3] Common Criteria for Information Technology Security Evaluation
[4] Guidelines on Firewalls and Firewall Policy, NIST SP 800-41
[5] Intrusion Detection Systems (IDS), NIST SP 800-31
[6] ITSEC(Information Technology Security Evaluation Criteria
[7] ITU-T Recommendation M.3000, CCITT 2000
[8] ITU-T Recommendation M.3000, CCITT 1998
[9] ITU-T Recommendation M.3000, CCITT 1997

성 경 (成 鏡)

2003년 : 한남대학교 컴퓨터공학과 (공학박사)

1994년 ~ 2004년 : 동해대학교 컴퓨터공학과 교수

2004년 ~ 현재 : 목원대학교 컴퓨터교육과 교수

관심분야 : 정보보호 및 정보관리, 컴퓨터네트워크 신경회로망, 컴퓨터교육