Journal of Digital Contents Society Vol. 8 No. 2 June. 2007(pp. 165-171)

네트워크 보안도메인 아키텍처 설계방법 연구

노시춘*

요 약

네트워크 구조상에서는 트래픽 소통경로상에서 악성코드 침투와 보안차단기능이 수행된다. 보안도메인이란 침투와 보안차단기능이 수행되는 네트워크 구조상에서의 트래픽처리 영역과 그룹을 차별화하여 구분시키는 개념이다. 각 보안도메인은 영역과 기능을 기준으로 타 도메인과 차별화가 가능하고 따라서 도메인별로 차별화된 보안 메커니즘이 개발되고 적용되어야한다. 네트워크는 구조적으로 어떤 기준으로 보안 도메인이 설정되어야하는가에 대한 방법론 개발을 위해 본 논문에서는 네트워크 형상(Topology) 결정 요소, 보안도메인 설정기준, 구조도 선택기준, 차단위치 결정, 경로방역망 구성기준을 도출한다. 설계된 방법론을 적용할 경우 전통적인 네트워크 구조상에서보다 바이러스 차단효율이 증대되고 있음이 실험을 통해 입증되었다. 따라서 보안도메인 영역기준에 따라 차별화된 차단기능이 필요하며 보안메커니즘 개발이 요구되고 있음을 본 연구를 통해 제시하고자한다.

The Study for the Method of Network Security Domain Architecture Designing

Si-Choon Noh*

Abstract

The penetration of malicious code and the function of security blocking are performed on the same course of traffic pathway. The security domain is the concept to distinguish the domain from the group handling with the traffic on the structure of network which is performed with the function of penetration and security. The security domain could be different from the criterion of its realm and function, which requires the development and the application of security mechanism for every domain. For the establishment of security domain it is needed to show what criterion of net work should be set up. This study is to research the criterion for topology factor, security domain. structure map selection, and blocking location and disinfection net. It is shown to increase the effective rate blocking the virus with the proposed method in this paper rather than the traditional network architecture. The purpose of this paper is to suggest the necessity of development of security mechanism and the distinguished blocking function according to the level of security domain.

Keywords : network security, domain, architecture

1. 서론

바이러스 방역 중심 메커니즘은 소위 네트워크상에서의 거점(Station또는 Traffic Node) 방역으로 대표된다. 거점 방역은 네트워크 경로(Traffic Route) 방역과 비교되는 개념으로 트래픽 유통단계의 최종 종단점 위치에서 시행되는 방역기능으로서 서버와 클라이언트 등 단말시스템장치에서 적용되는 방법이다. 현재의 방역 환경 하에서 소위 거점방역은 어느 정도 기능적 속성상의 취약 요인이 내재되어있다. 순간적으로 전파되는 모든 바이러스를 모든 종단점위치에서 일일이 삭제, 차단하므로 백신기술이 뛰어나고 그 방법이 자동화 방식이라 해도 시스템별 특성에 따라 일정 부분의 방역 누수가 발생한다. 두 번째의 취약점은 특히 심각하게 문제되는 부분

제1저자(First Author): 노시춘
접수일자:2007년05월13일, 심사완료:2007년06월20일
* 남서울대학교 컴퓨터학과
nsc321@nsu.ac.kr

으로 소위 네트워크 경로(Traffic Route)를 통한 바이러스 내부 확산인바 거점 상에서의 바이러스 진단, 삭제, 유입 차단이라는 방역망을 통과한 바이러스가 네트워크 내부 경로를 통해 확산되는 경우이다. 이 같은 환경에서 네트워크 보안 도메인은 물리적, 논리적인 네트워크 경로 상에서 보안기능 수행을 목적으로 트래픽 소통영역과 그룹을 구분하고 구성하는 방법론의 개념이다. 이때의 보안기능 수행은 도메인별로 네트워크 특성이 구분되며 이 특성을 보안기능 측면에서 관리함으로써 네트워크보안의 효율성을 제고하는 방법이 적용되어야한다. 모든 보안도메인은 타도메인과 차별화가 가능하고 따라서 도메인별로 차별화된 보안 메커니즘이 적용되어야한다. 본 연구는 네트워크는 어떤 구조와 기준으로 보안 도메인이 설계되어야하는가에 대한 방법론 개발을 위해 네트워크 형상(Topology) 결정 요소선정, 보안도메인 설정기준 결정, 구조도 선택기준 결정, 차단위치 결정, 경로방역망 구성기준을 도출하고 이를 보안기능효율성측면에서 검증한다.

2. 보안도메인 아키텍처 설계방법

2.1 네트워크보안 인프라 형상(Topology)결정요소

보안인프라 형상이란 일반적인 인트라넷, LAN 등 네트워크상에서 보안 기능과 관점에서 네트워크 구조를 정의하고 분류하는 개념이다. 보안인프라 형상은 일반 네트워크 구조상의 어느 접속점, 어떤 경로상에, 어떤 종류의 보안 기능을 배치하고 연계시키는가에 따라 그 형상적 의미와 종류가 결정된다. 이 같은 보안 인프라 구조의 성격을 고려해볼 때 보안네트워크는 <표 1>과 같이 일반적인 네트워크구조 분류 기준, 즉 트래픽 경로 설정 방법, 외부 네트워크 그룹간 접속방법, 내부 스테이션 배치방식 즉 서버와 클라이언트 그룹 배치방법에 따라 구조와 형상이 결정될 수 있다. 또한 순수 보안기능 관점으로만 분류해 본다면 트래픽 경로, 경로방역 구조, 거점방역 구조, DMZ 구성 등을 기준으로 삼을 수 있다. 그밖에 스위칭 구조, 침입차단시스템 필터링 구조, 게이트웨이 필터링 구조, 서버 방역 구조, 클라이언트 방역 구조를 기준으로 할 수도 있다, 어떤 방법을 택하든 그것은 업무 특성, 네트워크 인프라 구조, 보안 환경, 트래픽 볼륨, 트래픽 특성 등을 고려하여 각 사용자별로 선택할 사항이다. 다음의 <표 1>은 네트워크 구조 결정요소를 표시한 것이다. 이 분류 기준은 국내 대기업 정보시스템 구축 과정에서 수집 분류된 사례를 표본으로 조사하여 설정한 것이다.

<표 1> 네트워크 형상(Topology) 결정요소

분류 요소			판단 기준
유 형		항 목	
트래픽 경로 설정 방식	내부 경로	·공용 경로 사용	·인트라넷 접속 경로를 단일경로로 구성 - 모든 트래픽이 공용 경로로만 소통
		·분리경로 구성	·서브 네트워크 별로 경로를 분리하는 방식
	외부 경로	·복수 경로 구성	·인터넷, 비 인터넷 구간을 분리 ·인터넷 구간 복수 경로
		·단일 경로 사용	·인터넷, 비 인터넷 미 분리 공동 사용
외부 네트워크와의 접속방법		·다원화 접속	·하나의 게이트웨이 상에서 복수의 네트워크 그룹을 접속 ·동종의 프로토콜과 전송 표준 사용시 가능
		·분리 접속	·네트워크 그룹간 별도의 게이트웨이나 접속점을 관리
내부 스테이션 배치방식 -서버,클라이언트 배치		·별도 서버 Farm 설치 서버,클라이언트 분리	·서버 Farm 별도 구성 ·클라이언트 네트워크 별도 구성
		·서버,클라이언트를 동일 레벨로 배치	·서버, 클라이언트를 동일 레벨 배치 후 인터네트워킹 장비로만 분리

2.2 네트워크 보안도메인 설정기준

네트워크 도메인은 각 도메인 특성과 보안 취약성을 갖고 있다. 그리고 무엇보다도 보안 취약성에대한 대처가 필요하다. 즉 각 도메인이 처한 상황에 따른 보안 대책이 강구되어야 한다. 이를 위해 형상 결정요소를 기반으로 보안도메인을 설정하여야한다. 이때 검토될 수 있는 요소는 <표 2>와 같이

1. 외부 네트워크 -외부 라우터영역,
2. 외부 라우터 - 외부 스위치영역,
3. 외부 스위치 - 침입차단영역,
4. 침입차단 - 내부 게이트웨이영역,
5. 내부 게이트웨이 - 서버팜영역
6. 내부 게이트웨이 - 클라이언트영역

6개 범위로 설정될 수 있다. 이때의 도메인은 외부 라우터 구간, 외부 스위치 구간, 침입차단 구

간, 내부 게이트웨이 구간, 서버 구간, 클라이언트 구간으로 명명된다. 보안영역은 보안기술의 적용이 가능한 영역, 보안 기술 적용이 필요한 영역, 경로와 트래픽 성격의 타도메인과 차별화, 보안기술 적용시 타영역 보안기능과 중복여부 등 이 고려되어야 한다.

<표 2> 보안 도메인 설정기준

네트워크 구간	도메인명	검토 결과			
		A	B	C	D
1. 외부 네트워크 -외부 라우터	외부 라우터 구간	○	×	○	○
2. 외부 라우터 - 외부 스위치	외부 스위치 구간	○	○	○	○
3. 외부 스위치 - 침입차단	침입차단 구간	○	○	○	○
4. 침입차단 - 내부 게이트웨이	내부 게이트웨이 구간	○	○	○	○
5. 내부 게이트웨이 - 서버팜	서버 구간	○	○	○	○
6. 내부 게이트웨이 - 클라이언트	클라이언트 구간	○	○	○	○

<표 1>기준을 검토한 결과 보안도메인은 <표 2> 보안 도메인 설정기준 영역별 구분 항목에서 1번 항목을 제외한 5개 영역이 설정되었다. 1번 항목을 제외한 이유는 외부 네트워크와 외부 라우터 구간은 인트라넷을 기준으로 볼 때 인트라넷 외부 영역으로서 보안기능 적용이 불필요하며, 보안 기능은 인트라넷구간인 스위칭 단계부터 적용해도 가능하기 때문이다. 보안도메인 설정은 본 논문 제안, 설정방법보다 더 세부적으로 적용될 수도 있겠지만 그렇게 될 경우 보안기능 중복현상이 발생하고 무엇보다 Performance 지연과 필요이상의 네트워크 구조 복잡성을 초래할 가능성이 제기된다.

<표 3> 보안 도메인 유형

기준 유형	내 용
A	보안 기술의 적용이 가능하도록 구분 영역
B	보안 기술의 적용이 필요한 영역
C	경로와 트래픽 성격이 타도메인과 차별화가 가능
D	보안 기술과 적용시 타영역의 보안 기능으로 기능 중복이 발생치 않는 영역

2.3 보안차단 위치결정

네트워크 구조상에서 Tier 단계별로 바이러스를 차단해도 구간마다 잔류 바이러스가 발생한다. 네트워크 진입로에서 악성코드를 차단하면 네트워크 내부 구간에서 각종 오염원에 의한 바이러스가 발생, 잠복할 수 있다. 따라서 바이러스 박멸을 위한 근본 처방은 차단 구간별로 적용하는 앤티바이러스 기술의 완전성이 아니고 네트워크 구간별 차단막 형성을 통한 유통 바이러스 박멸이 필수이다. 차단 단계는 가급적 세분화하여 다양한 침투원에 대처할 수 있어야 한다. 다시 정리하면 네트워크 구간 마다 차단을 실시하되 내부 유통 바이러스 박멸을 위한 다단계 차단이 필요하다. 이때 차단단계를 얼마나 두어야 하는지와 단계마다 어떤 메커니즘을 적용해야 하는가가 관건이다. 그 결과에 의해 전체 네트워크 Topology가 결정된다. 이를 위하여 기존 네트워크상의 트래픽 유통경로 진단작업이 필요하며 그 결과를 토대로 차단 단계를 도출한다. 이어서 차단 단계별 방역 메커니즘을 설계한다. 차단위치별 장단점을 진단하고, 어떠한 구조가 효과적인지를 도출한다. 트래픽의 통과지점을 기준으로 차단위치를 점검하면 다음과 같이 몇 개의 핵심 지점이 도출된다. 인트라넷 전방에 인터넷에 접한 첫 번째 라우터가 가동되고 있고, 이어서 침입차단시스템, 그리고 내부 라우터가 가동되고 있다. 두 번째 라우터에서는 내부 클라이언트 네트워크와 서버 네트워크로 다시 분류된다. DMZ상에서는 별도 침입차단시스템이 가동된다. 네트워크 트래픽 소통경로상 이상의 5개 지점을 선택하여 차단 위치를 진단한다. 5개소는 일반적인 인프라 구조로 활용하고 있는 위치로서 이 진단을 통해 차단 위치에 대한 일차적 판단이 가능하다.

(1) 외부라우터 전방 차단

외부라우터 전방에 바이러스 월을 설치하면 실제로 네트워크에서 실행되는 모든 공격을 탐지할 수 있다. 따라서 공격 의도를 가진 요소들을 초기단계 파악할 수 있다. 그러나 이때 너무 많은 공격관련 정보를 관리함으로써, 네트워크에 대한 치명적인 공격에 대처하는 집중도가 취약해질 수 있다는 문제점을 가지게 된다.

(2) 외부라우터 후방 차단

외부 라우터 후방차단은 라우터의 패킷 필터

링이후 패킷들을 검사하는 방법이다. (1) 경우보다 좀 더 정제, 축소된 공격용 정보가 수집되고 탐지되며, 좀 더 강력한 공격자원이 발견된다.

(3) 침입차단시스템 후방 차단

침입차단시스템 후방 탐지는 공격에 대한 정책과 침입차단시스템과의 연동성이 가장 중요한 지점이다. 이지점은 내부에서 외부를 향한 공격 행위가 역시 탐지 가능한 위치이므로 내부 공격자에 대한 대책 구현이 가능해진다. 네트워크 특성과 목적에 따라 상이하지만 만약 침입탐지시스템을 전체네트워크 경로 중에서 한 개소에만 설치한다면 이위치가 최적 위치이다.

(4) 내부네트워크 진입경로 차단

침입차단시스템은 외부네트워크로부터의 침입에 대한 선행적 일차적 차단기능이 수행된다. 그러나 침입차단시스템은 네트워크 내부유통 침입에 대해서는 대처하지 못한다. FBI의 통계 자료에 의하면 보안 침해사고에서 가장 치명적 공격자는 내부의 공격자며, 실제로 해킹으로 인한 손실의 75%가량이 내부 공격자에 의해서 이루어진다는 보고를 발표하고 있다. 내부 클라이언트들을 신뢰할 수 없을 때나 내부 클라이언트에 의한 내부 네트워크 해킹을 감시하고자 할 때 차단위치로 선택해야할 지점이다.

(5) DMZ 진입경로 차단

DMZ상에 바이러스 월을 설치하는 것은 강력한 외부 공격자와 내부 공격자들에 의한 중요 데이터 손실이나 서비스의 중단을 막기 위한 것이다. 서버 바이러스월 설치시 특별한 위치는 없다. 보통 중요한 시스템별로 설치한다. 모든 시스템에 서버 바이러스 월을 설치하면 유지 관리 비용이 매우 많이 들기 때문에 보통은 웹 서버와 같은 중요지점의 효율성을 검토한 결과에 따라 설치위치를 결정한다.

이상과 같은 1차 검토안을 토대로 하여 다음과 같은 추가적인 검토기준을 작성했다. 차단 위치 결정 기준을 경로구간 상에서 차단 위치로 채용될 수 있는 지점을 추출하여 차단 지점의 타당성을 진단했다. 진단 대상이 된 지점은 기존 인프라 구조에서 트래픽 컨트롤이 이루어지고 있는 장비 설치 구간이다. 표에 나타난 바와 같이 전방위 바이러스 차단 지점은 웹 스위치 구간과 침입차단시스템 구간으로 파악되었다. 이 두 지점은 기존 인프라 구조상 차단 지점 결정 요건 5개 항목을 만족시킨다. 이 두 지점은 본 논문의 도메인 설계 사상인 경로 방역 구조의 외부 경계선 방어 위치에 해당되는 지점으로서 그 효율성이 필요한 위치이다. 따라서 경로 방역망의 차단 위치로 결정한다. 그러나 이 두 지점의 바이러스 차단 구간에 불구하고 내부 유통 바이러스 박멸에 대한 대책이 문제점으로 대두된다. 즉, 각종 감염 요인으로 내부 자원에 잠복중이거나 오염된 매체에 기생하는 바이러스의 네트워크 내부경로상 이동시 이에 대한 대책이 존재하지 않고 있다. 내부 네트워크상에서의 각종 유해트래픽 발생수준은 전체 트래픽 물량의 10%이상으로 조사되고 있다. 이 같은 막대한 수준의 악성트래픽을 해결할 수 있는 방법론이 강구되어야하며 이 같은 이유로 내부네트워크 방역메커니즘을 적용해야한다. 일반적으로 적용되고 있는 전통적 방법은 경계선 방어이다. 경계선 방어란 특정의 최전방위치에서 전체도메인 방역을 수행하는 방법이다.

<표 4> 차단 위치 검토 요소

기 준	선정사유
•네트워크 구조상 상위 구조의 트래픽 전량이 유입되는 유일한 하위 지점	•전체 트래픽 컨트롤 지점에서 방역 차단시 전체적 통제와 종합관리 효과가 가장 뛰어남
•네트워크 구조상 상위 구조 트래픽이 분기되는 유일한 하위 지점	•전체 트래픽 분기점은 방역 장치 설치와 방역 기능 대체 유연성이 절대적으로 유리
•기존 네트워크 구조에서 현재 패킷 검색, 컨텐츠 관독, 라우팅이 수행되고 있는 지점	•기존 네트워크 구조에서 수행되는 트래픽 컨트롤과 연동시키는 방역 기능이 가능
•기존 인프라 구조상에 없는 차단 지점 신설에는 차단기능 신설로 Performance 지연이 초래되지 않아야 함	•응답 시간 등 Performance 저하시 시스템 가동 자체의 생산성, 가용성 저하 발생
•기존 인프라 구조의 백본, 게이트웨이 구간의 설계를 근본적으로 변경치 않는 구간	•백본이나 게이트웨이 근본 구조 변경시 시스템 안정성 훼손

그러나 악성코드의 내부네트워크 유통시 경계선 방어 개념의 차단으로는 근본 대처가 불가능한 것이다. 따라서, 네트워크 내부 유통 바이러스 차단을 위한 별도의 방역 Zone을 구축해야 할 필요성이 대두되고 있다. 바이러스 차단을 위

한 별도의 방역 Zone은 서버나 클라이언트 개개 자원에 대한 방역이 아닌 유통 구간에서 서버나 클라이언트에 도달되기 전 구간 또는 서버나 클라이언트에서 유출된 직후 구간의 네트워크 경로 상에 설정되어야 한다는 결론에 도달한다.

2.4 보안도메인 설계기준

일련의 기준에 따라 차단 위치가 결정되었으며 차단 위치를 통해 차단 단계가 형성되었다. 차단단계는 방역구역을 네트워크 계층 기준으로 단계화 시킨 것이다. 설계된 차단 구조도 프레임워크는 소프트웨어 기술 방역의 취약점과 한계점을 보강할 수 있는 인프라 구조 방역 개념이며 전통적 거점방역 기조를 경로방역 기조로 개선한 것이다. 경로방역 구조로 설계된 5 Tiers 방역 분담 구조는 각 계층마다의 특성을 고려하여 계층별 방역 기능을 설계한 것이다. 네트워크 트래픽 처리과정에서 경로방역의 기능만을 기준으로 하여 구성되는 차단 장치는 스위치 – 침입차단시스템 – 내부 게이트웨이– 서버 바이러스월 – Real-time 방역망 등 5개 단계로 연동되고 있으며 각 단계마다 차단기능을 수행한다. 이 모든 구조와 기능은 바이러스 스캐너와 바이러스 백신 등 방역용 소프트웨어의 적용을 전제로 하고 있으며 신•구 백신 간 신속한 업데이트 과정을 필수적으로 요구하고 있다. 이상에서 구성한 일련의 설계 절차에 따라 보안도메인 종합구조도를 완성했다. 종합 구조도는 침입차단 구조도 내에서의 종합 구조도 편이다. 이 종합 구조도의 체계를 토대로 세부적인 차단 단계별 구조도가 설계되어야 한다. 본 연구에서는 차단 단계별 구조도를 5단계로 설계했다. 설계된 5단계는 스위칭 단계, 침입차단시스템 필터링 단계, 내부 게이트웨이 필터링 단계, 서버 방역 단계, 클라이언트 방역 단계이다. 이와 구분되는 또 하나의 설계 영역이 있는데 효율성 구조 부분이다. 효율성 구조도 부분은 고가용성 구조, 부하 분산 구조, 자동화 방역 구조, 종합운영 관리 구조로 편성되었다. 효율성 구조 부분은 그러나 독립된 구조와 기능이 아니고 각 단계별로 차단 구조 내에 기능이 포함되어 있으므로 단계별 침입차단 구조도 상에서 효율성 구조 반영 사항을 명확하게 도해하고 설명했다. 이상의 설계방법을 종합하면 보안도메인은 차단 구조도, 효율성 구조도로 구분되고 차단 구조도는 종합구조도와 차단 단계별구조도로 구분된다. 이상을 기반으로 세부적인 도메인 설계명칭은 <표 5> 보안도메인 설계기준으로 표시되었다.

<표 5> 보안도메인 설계기준

차단 구조도 설계		효율성 구조 적용
종합 구조도	차단 단계별 구조도	
· 인프라 구조 결정 요소 선정 · 보안 도메인 설정 · 구조도 선택 기준 결정 · 차단위치 결정 · 경로 방역망 구성 · 차단 단계 구성 · 구조도 형상 작성	· 스위칭 구조도 설계 · 침입차단시스템 필터링 구조도 설계 · 내부 게이트웨이 필터링 구조도 설계 · Real-time 방역 구조도 설계	· 고가용성 구조 적용 – 스위칭 고가용성 – 침입차단시스템 필터링 고가용성 · 부하 분산 구조 적용 – 스위칭 부하 분산 – 침입차단시스템 필터링 고가용성 · 자동화 방역 구조 적용 – Real-time 방역 · 종합 관리 구조 적용 – 단위 솔루션 구조 관리 – 방역 운용 관리
종합 구조도 완성		

3. 성능분석

3.1 분석 환경

설계된 네트워크 보안도메인 차단구조도 프레임워크는 소프트웨어기술 방역의 취약점과 한계점을 보강할 수 있는 인프라구조 방역개념이며 그 중에서도 전통적 거점방역 기조를 경로 방역 기조로 개선한 것이다. 설계된 차단 구조도 성능분석 환경은 S기업 인트라넷 시스템 상에서 실제업무를 대상으로 검증을 실시했다. 실제업무 인프라구조가 설계사상으로 사전에 구비된 것이 아니므로 본 검증작업을 위해 측정목적의 보강과 환경 준비 단계를 거쳤다. 인용된 S기업 업무 환경과 인트라넷의 트래픽 처리 환경은 인트라넷 시스템내 접속 자원 규모로서 각종 서버 1,000대, Workstation급 PC 35,000대, 내부 사용자 규모 35,000명수준이다. 네트워크 구조로서 인트라넷과 외부망과의 연결은 310Mbps 속도로 복수 회선 네트워크로 구성되었고 인트라넷 입구에 침입차단시스템이 구성되고 침입차단시스템 이후에는 인트라넷이 구성되었다. 인트라넷 내부 구조는 서버와 PC가 연결되어 있고 서버 전단에 별도의 메일 검색 시스템이 설치되었으

며 PC자원을 대상으로 개별 단위 바이러스 백신이 설치되어있다.

3.2 보안도메인 바이러스 방역성과

보안도메인에 의한 방역성과는 웜 바이러스 방지와 웜 바이러스 차단 등 두 가지 측면이다. Layer 7 컨텐츠 필터링을 통하여 Query 대상 및 DDoS 공격에 대한 사전 차단과 신규 인터넷 웜 바이러스를 차단한다. L7 스위칭 기능 수행은 공격 유형별, 검색 기간별 차단 실적으로 집계되었다. 보안도메인은 정교한 부하 분산과 함께 유해 트레픽 차단과 데이터 필터링 기능을 통해 네트워크 환경을 최적화하고 있다. 스위칭 기능은 Deep Inspection, 전체적인 트래픽 모니터링을 실시함으로서 종래의 로드밸런싱 위주의 L4 기능에서 보안 기능을 구현하는 차세대의 스위칭 기능으로 분석된다. 웰치아 웜의 경우 총 발생 건수 중 스위칭 단계 차단 실적은 평균 17.5% 이상의 실적을 보이고 있다. 이 차단은 악성코드를 방출시키는 사이트의 악성코드 다운로드를 방지하고 악성코드자체를 유입차단 하기 위해 스위칭 단계에서 Query를 차단한 것이다. 한편 바이러스 차단건수는 시간대별로 발생 및 차단이 이루어졌다.

3.3 보안도메인 침입차단 효율성

이상의 차단결과와 Latency 소요시간 조사결과를 토대로 하여 보안도메인 방역 효율을 분석했다. 효율 분석은 1단계 차단, 3단계 차단, 5단계 차단 유형별로 차단 효과와 Latency를 분석하고 그 결과를 종합 효율로서 평가하는 것이다. 이상적인 차단 구조 모델은 침입차단율은 높을수록 유리하고 Latency는 낮을수록 유리하다. 따라서 크게 세가지 유형과 세부적으로는 일곱가지 차단 경우의 수별로 차단율과 Latency를 모두 감안했을 때 가장 이상적인 모델을 찾아보는 것이다. 차단 단계가 다단계일수록 방역율은 높고 Latency는 증가한다. 종합 효율을 분석해보면 다단계 차단시 전체적 Performance에 지장을 초래하지 않고 차단기능이 수행된다. 즉 Performance 지연은 1단계 차단, 3단계 차단에서 미미한 정도이며 5단계 차단에서도 두드러지게 나타나지 않았다. 적어도 5단계 차단 구조까지는 Performance 영향을 걱정하지 않아도 된다. 차단의 완전성은 1단계보다 3단계, 3단계보다 5단계 차단이 절대 유리하다. 5단계 차단에서는 전방위의 Zone으로 차단 영역이 확대됨으로써 차세대형 차단 구조로서 가장 강력한 방역 기능 실현이 가능하다. 결론적으로 말하면 차단 단계를 추가하여도 적어도 5단계까지는 시스템 Performance 측면에서 업무 불편을 초래할 만큼의 지연이 발생치 않는다. 이 같은 분석 결과는 Performance 부담으로 인하여 다단계 차단 구조를 적용하기가 어려울 것이라는 일반적인 관념을 뒤집는 것으로서 향후 기업 현장의 보안 시스템 구축시 참고 되어야할 사항이다.

4. 결 론

슬래머 웜에서 경험했듯이 사이버 공격은 자연 재난과는 달리 사고 발생을 사전에 예측하게 하는 관련 변수가 극히 제한되어 있으며, 발생시 수십분안에 전 세계로 확산되는 전파력을 보이고 있기에 무엇보다 사고발생 즉시 이상 징후를 발견할 수 있는 환경을 조성하는 것이 중요하다. 현재 인트라넷 시스템 운용 현장에서는 갈수록 빨라지는 바이러스 침투 시간, 침투한 웜 바이러스의 급속한 내부 네트워크 재감염, 다수 서버와 클라이언트 차원에 대한 개별 방역 처리 시간의 과다 소요 등 현재 사용하고 있는 방어 메커니즘으로는 극복하기 어려운 문제점들이 노출되고 있다. 본 논문에서는 이러한 문제점을 해결하고 보다 강력한 방어를 수행하기 위하여 네트워크 보안도메인구조 적용을 통한통합구조의 정보보호 인프라스트럭처를 제안했다. 제안 보안도메인 구조 인프라스트럭처는 새로운 설계사상을 기반으로 하여 프레임워크를 도출하고 기능 메커니즘을 구성했으며, 기반 구조도를 설계했다. 보안도메인구조 인프라스트럭처는 다원화 차단, 다단계 차단, 차별화 차단을 실행하는 구조이다. 본 논문에서는 제안된 방법론에 대하여 성능분석 모델을 개발하고 사례연구를 통하여 성능분석 및 검증을 실시했다. 정보보호 인프라스트럭처의 효율성 여부는 사용자 또는 사용부서의 지속적인 진단과 튜닝을 필요로 한다. 본 논문으로 제안된 방법론은 향후 업무 현장에서 참고되고 응용될 수 있을 것으로 기대된다.

참고문헌

[1] Nortel Networks Korea, "애플리케이션 스위치를 이용한 네트워크 보안", 2003.

[2] 한국후지쯔, "L4 스위치를 이용한 방화벽 부하 분산", 2002.

[3] 이종환, "Layer 7 스위칭을 통한 애플리케이션 인식 및 제어", 탑레이어, 2000.

[4] 최성열, "다계층 스위치를 이용한 효율적인 전자 정부 구현 사례", (주)파이오링크, 2003.

[5] 구자만, "고가용성으로 보안 장비 한계를 극복하라", 네트워크타임스, 2003.

[6] 장윤정, "L7 스위치로 네트워크 활용도를 높여라", 네트워크타임스, 2003.

[7] Sichoon Noh, Dong Chun Lee, and Kuimam J.Kim, "Improved Structure Management of Gateway Fire wall Systems for Effective Networks Security", Spr inger, 2003.

[8] 월간 네트워크타임스, "Next Generation Network Sec urity Vision 2004", 2004.

[9] 서동일, "차세대 정보전 기술 및 제품 동향", ETRI, 2003.

[10] 박호영, 박상혁, "인터넷 방화벽 구축하기", 한빛 미디어, 2003.

[11] 홍승필, 고제욱, "정보보안 기술과 구현", 파워북, 2002.

[12] 시스코코리아, 시스코레포트, "네트워크의 가용성을 높여라", 2004.

[13] 이봉환 외2인, "네트워크 보안 에센셜", 도서출판 미래컴, 2004.

[14] 이만영 외3인, "인터넷 보안 기술", 생능출판사, 2003.

[15] Mart Bishop, "Computer Security", Addison Wesle y, 2000.

[16] 한국상공회의소, "2003 기업 정보보안 실태 조사", 2003.

[17] Timothy P.Appleby, "Building a Virus Protection Infrastructure", CHI Publishing Ltd, 2000.

노 시 춘

1987년 : 고려대학교 경영정보학(석사)

2005년 : 경기대학교 정보보호기술(박사)

1982년~2003년 : KT IT본부 시스템보안부장

2003년~2004년 : KT 충청전산국장

2005년~현 재 : 남서울대학교 컴퓨터학과 컴퓨터전공 교수

관심분야 : 차세대통신망, 정보보호, 컴퓨터네트워크