보안 효율성 제고를 위한 인트라넷 네트워크 아키텍쳐 모델

노 시 춘*

요 약

인트라넷의 네트워크는 악성트래픽의 확산과 분산을 차단하는 역할이 수행되는 영역이다. 네트워크 구조상에서는 트래픽 소통경로상에서 악성코드 침투와 보안차단기능이 수행된다. 네트워크보안 아키텍쳐란 침투와 보안차단기능이 수행되는 네트워크 구조상에서의 트래픽처리 영역과 그룹을 차별화하여 구분시키는 개념이다. 인트라넷 네트워크 아키텍쳔,는 보안도메인은 영역과 기능을 기준으로 차별화가 가능하고 따라서 도메인별로 차별화된 보안 메커니즘이 개발되고 적용되어야한다. 본 논문는 네트워크 아키텍쳐의 보안 취약성을 진단하고 네트워크는 구조적으로 어떤 기준으로 보안 도메인이 설정되어야하는가에 대한 방법론 개발을 위해 네트워크 형상(Topology) 결정 요소, 보안 아키텍쳐 설정기준, 구조도 선택기준, 차단위치 결정, 경로 방역망 구성기준을 도출한다. 설계된 방법론을 적용할 경우 전통적인 네트워크 구조상에서보다 바이러스 차단 효율이 증대되고 있음이 실험을 통해 입증한다. 따라서 아키텍쳐 영역기준에 따라 차별화된 차단기능이 필요하며 보안 메커니즘 개발이 요구되고 있음을 본 연구를 통해 제시하고자한다.

A Designing Method of Intranet Security Architecture Model for Network Security Efficiency

SiChoon Noh*

ABSTRACT

Internet network routing system is used to prevent spread and distribution of malicious data traffic. The penetration of malicious code and the function of security blocking are performed on the same course of traffic pathway. The security architecture is the concept to distinguish the architecture from the group handling with the traffic on the structure of network which is performed with the function of penetration and security. The security architecture could be different from the criterion of its realm and function, which requires the development and the application of security mechanism for every architecture. For the establishment of security architecture it is needed to show what criterion of net work should be set up. This study is based on analysis of diagnostic weakness structure in the network security architecture and research the criterion for topology factor, security architecture 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.

Key words : Network Security, Architecture, Model

접수일 : 2010년 1월 6일; 채택일 : 2010년 2월 13일

* 남서울대학교 컴퓨터학과

1. 네트워크 Layer 별 공격패턴 유형

1.1 최근의 공격패턴

네트워크트래픽 처리과정에서의 보안기능 매커니즘 작동 과정을 설명하기 위해서는 OSI 계층별로 발생하는 보안 공격유형과 그 성격을 파악해야 한다. 최근의 해킹, 바이러스 공격은 OSI 계층 L2에서 L7까지 모든 계층에 걸쳐 발생하고 있다. 먼저 MAC 스푸핑(Spoofing)과 플러딩(Flooding)은 가장 대표적인 L2 레벨의 공격이다 이런 MAC 스푸핑과 플러딩이 백본 스위치까지 전달될 경우 네트워크 망 전체가 혼들리게 되며, 이를 이용한 공격이 늘어나고 있다. 다음으로 L3~L7 레벨의 공격으로 SYN 공격, 스푸핑, 플러딩이 대표적이다. 스머프(Smurf) 공격이 가장 대표적인 ICMP(Internet Control Message Protocol) 공격이고, 웰치아 웜은 애플리케이션 레벨의 ICMP 플러딩 공격이다. 사세르 웜은 DoS 공격의 한 형태로, 여기서 주목할 점은 DoS 공격을 의도하지 않은 사용자가 웜에 감염될 경우 자신의 의지와 상관없는 DoS 공격이 된다는 점이다. 즉 최근의 웜은 자신이 공격하고자 하는 호스트가 특정 서비스 포트가 열려 있는지 스캐닝하는데, 이런 스캐닝이 DoS 공격과 같은 형태로 나타난다.

1.2 네트워크 보안 메커니즘

네트워크 방역 중심 매커니즘은 소위 네트워크 상에서의 거점(Station 또는 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 어느정도 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 부분으로 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 보안도메인은 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].

1.3 악성트래픽 방역 취약성 요소

정보시스템에서의 방역취약점 요인은 방역기술, 인프라구조, 관리나 운용 절차 3개 측면에서 원인을 찾을 수 있다. 방역 기술은 바이러스 침투 기술의 변화에 대응하여 항구적이며 지속적으로 개선해야 할 과제이며 방역 관리방법, 운용 절차 등은 부분적인 문제점으로 거론될 수 있으나, 근본적인 문제 요인일 수는 없다. 따라서 기업정보시스템의 경우 다음과 같은 문제점이 인프라 구조 측면의 문제점으로 도출된다.

1.3.1 차단 기능상의 취약성

지금 가장 문제되는 바이러스 침투 형태는 진단, 삭제, 유입 차단으로 해결할 수 없는 내부네트워크를 통한 확산이다. 현재까지의 방역 방식인 백신 기법은거점상에서의 진단, 삭제, 유입 차단에는 효과적이지만 네트워크 경로를 통한 확산의 차단에는 극히 제한적 기능만을 발휘한다. 수많은 서버와 PC에서 바이러스를 삭제해도 네트워크 상에는 여전히 바이러스가 폭증하고 있다. 따라서 네트워크 경로상 확산에 취약한 기존의 차단 체계는 구.조적으로 결함 요인이 내재되어 있다. 내부 네트워크에 접속된 수많은 PC 자원에 대해서는 하나 하나의 PC마다 백신을 설치하고 업데이트하는 방법을 사용하여 왔으나 방역에서의 생명인 신속성 도모 측면에서 바이러스 침투를 방어하지 못한다. 특히 PC 자원 규모가 증가할수록 이 같은 문제점은 상대적으로 커진다[1].

1.3.2 네트워크 인프라구조상 취약성

네트워크 관문, 서버, PC로 고정된 방역 구조는 차단 Zone을 한정시킴으로서 일단 네트워크 관문 이후의 내부네트워크 유통 바이러스 차단기능이 없다. 무엇보다도 1차 방어망을 통과했거나 내부 감염으로 서버, PC에 잠복한 바이러스가 인트라넷 내부를 통해 확산될 경우 관문, 서버, PC에 집중된 차단으로는 근본적 해결이 되지 않는다. PC나 서버 단위로 바이러스를 삭제, 차단하는 거점 차단은 순간적으로 전파되는 바이러스를 서버나 PC 단위로 일일이 삭제하고 차단하므로 자동화 방식이라 해도 수많은 작업이 동시에 이루어지는 과정에서 방역 누수가 발생한다. 클라이언트 위주 방역은 트로이 목마 등 기승을 부리는 악성코드 감염 여부를 진단하고 치료하는 데는 효과를 나타내지만, 인터넷에 접속한 상태에서 공격용 패킷이 유입되거나 해킹 기술을 동반한 형태로 접속해오는 바이러스 움직임에 대한 대처기능이 없다[4].

2. 네트워크보안 아키텍처설계

2.1 네트워크 보안 아키텍쳐 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. 이를위해 형상 결정요소를 기반으로 보안도메인을 설정하여야한다. 이때 검토될 수 있는 요소는 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-클라이언트영역으로 6개 범위로 설정될 수 있다. 이때의 도메인은 외부 라우터 구간, 외부 스위치 구간, 침입차단 구간, 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 이고려되어야 한다.

〈표 1〉 보안 아키텍쳐 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 차단 단계를 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 침입차단 시스템, 그리고 내부 라우터가 가동되고 있다. 두 번째 라우터에서는 내부 클라이언트 네트워크와 서버 네트워크로 다시 분류된다. DMZ상에서는 별도 침입차단 시스템이 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[10].

2.3.1 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.

2.3.2 외부라우터 후방 차단

외부 라우터 후방차단은 라우터의 패킷 필터링이후 패킷들을 검사하는 방법이다. (1) 경우보다 좀 더 정제, 축소된 공격용 정보가 수집되고 탐지되며, 좀 더 강력한 공격자원이 발견된다.

2.3.3 침입차단 시스템 후방 차단

침입차단 시스템 후방 탐지는 공격에 대한 정책과 침입차단 시스템과의 연동성이 가장 중요한 지점이다. 이지점은 내부에서 외부를 향한 공격행위가 역시 탐지 가능한 위치이므로 내부 공격자에 대한 대책 구현이 가능해진다. 네트워크 특성과 목적에 따라 상이하지만 만약 침입탐지시스템을 전체 네트워크 경로 중에서 한 개소에만 설치한다면 이 위치가 최적 위치이다.

2.3.4 내부네트워크 진입경로 차단

침입차단 시스템은 외부 네트워크로부터의 침입에 대한 선행적 일차적 차단기능이 수행된다. 그러나 침입차단 시스템은 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.

2.3.5 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 기존인프라 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 네트워크 상에서의 각종 유해트래픽 발생수준은 전체 트래픽 물량의 10% 이상으로 조사되고 있다. 이같은 막대한 수준의 악성트래픽을 해결할 수 있는 방법론이 강구되어야하며 이 같은 이유로 내부 네트워크 방역메커니즘을 적용해야 한다. 일반적으로 적용되고 있는 전통적 방법은 경계선 방어이다. 경계선방어란 특정의 최전방위치에서 전체도메인 방역을 수행하는 방법이다. 그러나 악성코드의 내부 네트워크 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 위한 별도의 방역 Zone은 서버나 클라이언트 개개 자원에 대한 방역이 아닌 유통 구간에서 서버나 클라이언트에 도달되기전 구간 또는 서버나 클라이언트에서 유출된 직후 구간의 네트워크 경로상에 설정되어야 한다는 결론에 도달한다[11].

2.4 보안 아키텍쳐 설계기준

일련의 기준에 따라 차단 위치가 결정되었으며 차단 위치를 통해 차단 단계가 형성되었다. 차단 단계는 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 5Tiers 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 바이러스 월-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 종합 구조도를 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. 이

상의 설계방법을 종합하면 보안도메인은 차단 구조도, 효율성 구조도로 구분되고 차단 구조도는 종합구조도와 차단단계별구조도로 구분된다. 이상을 기반으로 세부적인 도메인 설계명칭은 <표 2> 보안도메인 설계기준으로 표시되었다.

〈표 2〉 보안도메인 설계기준

차단 아키텍처 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		

2.5 차단기능 구성

트래픽 관문과 거점방역성 기능의 취약성에 대처할 수 있는 기능으로 네트워크 내부 경로차단 메커니즘을 적용하기 위해 네트워크 구조를 기반으로하는 다단계 차단기능을 적용한다. 다단계 차단 기능은 외부 네트워크와의 접점에서부터 인트라넷 구간을 통과하는 최종거점, 즉 서버나 PC 접속 단계인 클라이언트 구간까지 단계 차단기능을 순차적으로 구성한다. 다단계 차단 구조를 도입하는 이유는 무엇보다도 네트워크 전구간의 트래픽 도메인 별로 소통 단계별로 차별화된 방역을 수행하고자하는 취지이다. 네트워크 경로 전단계의 방역 누수를 다음 단계에서 차단하므로서 방역 누수의 홀을 최대한 축소하는 방법이다. 이는 트래픽 소통 구간별로 방역을 관리하므로서 전통적 네트워크 방역 방법론인 거점방역과 경계선 방어 즉, 1개 네트워크 관문에서 모든 구간 방역을 전담하는 전수방역 방법을 수정하는 것 이다[8, 11].

다음으로 이 경로방역망에 차단 기능을 구성하여 적용한다. 차단 기능 구성이란 설정한 보안 도메인별로 그에 적합한 차단기능을 적용하는 것이다. 본 제안에서 설계한 다차단 구조를 적용하고 또한 도메인별로 차단 기능은 보안 도메인, 네트워크 구간, 도메인별 차단 매커니즘, 도메인별 차단 기능, 도메인별 세부 차단 기능으로 구성하였다. 이 같이 구성된 차단 기능은 기존의 차단 매커니즘을 설계 개념으로 구성한 것으로서 기능 자체를 기술적으로 새롭게 개발하거나 설계한 것은 아니다. 다음의 <표 3>은 보안도메인별 차단 기능 매커니즘 구성 내용이다[9].

이를 통해 각 단계의 특징적인 침투 유형이 존재하는 현상에 대해 이를 차단하는 방법론 또한 각각 특징적으로 대처하는 것이다.

〈표 3〉 차단 기능 구성

도메인	구간	매커니즘	차단 기능
내부 유통	내부게이트웨이침입차단구간	게이트웨이 필터링	◦ SMTP 프로토콜을 통한 악성코드 유출입 차단
서버군 도메인	내부 게이트웨이서버 방역구간	서버 바이러스 차단	◦ 서버군 자동화 방역망 구성 중앙 집중 관리형 차단
			◦ 악성코드 침입 차단
			◦ 악성코드 진단
			◦ 악성코드 삭제
			◦ 악성코드 치료
클라이언트군 도메인	내부 게이트웨이 클라이언트 방역구간	클라이언트 바이러스 차단	◦ 클라이언트 군 자동화 방역망 구성 중앙 집중 관리형 차단
			◦ 악성코드 침입차단
			◦ 악성코드 진단
			◦ 악성코드 삭제
			◦ 악성코드 치료

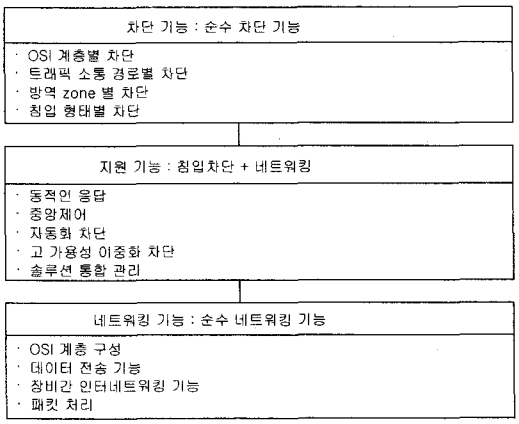
3. 차단기능 설계

3.1 설계방향

네트워킹 기능과 정보보호기능은 기술영역 기준으로는 별도의 카테고리로 출발하지만 응용현장에서는 연동기능구조로 가동된다. 다양한 레이어별 네트워킹 공격에 대응하기 위해서는 양기능 연동구도에 의한 단계별 차단을 실시해야한다. 연동구조기능은 네트워킹기능, 효율성지원기능, 보안차단기능으로 구성되고 기능 수행과정은 스위칭 단계 → 침입차단시스템 필터링 단계 → 내부 게이트웨이 필터링 단계 → 서버 바이러스 월 차단단계 → 자동화 방역 단계 순서로 이루어진다.

3.2 종합메커니즘

종합 매커니즘 구조는 (그림 1)과같이 네트워킹 기능, 지원기능, 정보보호기능 3단계로 계층화된다. 네트워킹기능은 네트워크 인프라상의 통신트래픽처리 기능이다. 네트워킹 기능은 OSI 7 layer별로 차별화된 네트워킹 기능 구조를 형성하고 이 구조상에서 라우팅, 스위칭, 브로드캐스팅등 인터네트워킹 기능, 데이터 전송기능 그리고 패킷처리 기능을 수행한다. 다이어그램으로 본다면 이 네트워킹 기능 영역내에 지원기능과 침입차단 기능이 존재한다. 지원기능은 네트워킹 기능을 토대로 하지만 침입차단 기능 구현시 적용되어야 할 필수적인 효율성지원기능 또는 연관기능이다. 지원기능은 성격상 3개 세부 영역으로 분류되데 고가용성 기능, 통합관리 기능 및 자동화처리와 실시간처리 기능이다. 정보보호기능은 인프라구조상에서의 바이러스와 각종 악성코드 차단기능이다. 침입차단 기능은 OSI 계층별 차단, 트래픽 소통 경로별 차단, 방역 Zone별 차단으로 분류될 수 있다. OSI 계층별 차단은 OSI Layer 2에서 Layer 7까지의 계층별로 수행되는 차단 기능이다. 경로별 차단은 외부 라우터에서부터 최종 클라이언트까지의 트래픽 경로별로 수행되는 차단이다.



(그림 1) 연동기능 종합메커니즘

4. 제안 아키텍쳐 성능분석

4.1 분석 환경

설계된 네트워크 보안 아키텍쳐 프레임워크는 소프트웨어기술 방역의 취약점과 한계점을 보강할 수 있는 인프라구조 방역개념이며 그 중에서도 전통적 거점방역 기조를 경로 방역 기조로 개선한 것이다. 설계된 아키텍쳐 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 35,000명 수준이다. 네트워크 구조로서 인트라넷과 외부망과의 연결은 310Mbps 속도로 복수 회선 네트워크로 구성되었고 인트라넷 입구에 침입차단시스템이 구성되고 침입차단시스템 이

후에는 인트라넷이 구성되었다. 인트라넷 내부 구조는 서버와 PC가 연결되어 있고 서버 전단에 별도의 메일 검색 시스템이 설치되었으며 PC 자원을 대상으로 개별 단위 바이러스 백신이 설치되어 있다.

4.2 차단유형별 방역효율

차단기능 분석시 인트라넷상의 내부 클라이언트상에서 악성코드 발생빈도상 특이점은 없었으며 내부 네트워크상 세션증가도 일어나지 않았다. 구조 성능 분석시 평균 Throughput Time은 증가했지만 프로세스상 Performance는 지장을 초래하지 않았다. 또한 강력한 각종 연동필터링 기능은 전체 트래픽 중 8~10%의 불필요한 트래픽을 걸러줌으로 서버와 클라이언트에 주는 부하는 오히려 상당량 감소되었다. 유입패킷을 먼저 수신해 네트워킹 기능의 패킷과 악성코드, 바이러스 검사를 수행하므로서 유해 트래픽 유입을 차단하고, 이렇게 1차적으로 걸러진 트래픽을 다시 첨부 파일명, 제목, 본문, 필터링 형태로 내부게이트웨이 상에서 검색함으로서 비정상적인 패킷을 네트워크 전송 과정에서 차단한다. 이상의 차단 결과와 Latency 소요시간 조사결과를 토대로 하여 차단 유형별로 종합적인 방역 효율을 분석했다. 효율분석은 네트워킹기능, 효율성지원기능, 보안차단기능 수행구조상에서 1단계 차단, 3단계 차단, 5단계 차단 유형별로 차단효과와 Latency를 각각 분석하고 그 결과를 종합 효율로서 평가하는 방법이다. 이상적 차단구조 모델은 보안차단율은 높을수록 유리하고 Latency는 낮을수록 유리하다. 1단계 차단의 경우는 1개 도메인의 방역만 가능하고 나머지 4개 도메인의 방역은 불가하다. 차단단계가 다단계일수록 방역율은 높고 Latency는 증가한다. 종합효율측면은 다단계 차단 구조 적용시 전체적인 Performance에 지장을 초래하지 않고 차단 기능이 수행된다. 즉 Performance 지연은 1단계 차단, 3단계 차단에서 미미한 정도이며 5단계 차단에서도 두드러지게 나타나지 않았다. 적어도 연동기능 5단계 차단 구조까지는 Performance 영향을 걱정하지 않아도 된다. 차단의 완전성은 연동기능 1단계보다 3단계, 3단계보다 5단계 차단이 절대 유리하다. 5단계 차단에서는 전 방위의 Zone으로 차단 영역이 획대됨으로써 차세대형 차단 구조로서 가장 강력한 방역 기능 실현이 가능하다.

5. 결 론

네트워크 아키텍처의 보안 취약성을 진단하고 네트워크는 구조적으로 어떤 기준으로 보안 도메인이 설정되어야하는가에 대한 방법론 개발을 위해 네트워크 형상(Topology) 결정 요소, 보안 아키텍처 설정기준, 구조도 선택기준, 차단위치 결정, 경로방역망 구성기준을 도출한다. 설계된 방법론을 적용할 경우 전통적인 네트워크 구조상에서보다 바이러스 차단효율이 증대되고 있음이 실험을 통해 입증되었다.

참 고 문 헌

[1] 김귀남, 노시춘, "다단계 바이러스 차단 구조 설계", 2004 한국 사이 버테러 정보전 컨퍼런스, 2004.

[2] 한국후지쯔, "L4 스위치를 이용한 방화벽 부하분산", 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 높여

라", 네트워크타임스, 2003.

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

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

[9] Sichoon Noh and Dong Chun Lee, "Multi-Level Protection Building for Virus Protection Infrastructure", SCIE Springer, LNCS 3036, 2004.

[10] Sichoon Noh, "Assurance Method of High Availability in Information Security Infrastructure System", LNCS, 3794, 2005.

[11] Sichoon Noh, "Building of an Integrated Multilevel Virus Protection Infrastructure", IEEE Computer Society, 2005.

[12] Sichoon Noh, "A Securing Method of Multispectral Protection Infrastructure for Malicious Traffic in Intrne System", DCS, 2006.

[13] Sichoon Noh, "Protection Structure Building for Malicious Traffic Protecting in Intrnwt Systems", SCIE LNCS3981, 2006.

[14] Sichoon Noh, "Active-Active High Availability of Information Infrastructure System for Effective Network Security", IEEE Computer Society, 2008.

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

노 시 춘

1987년 고려대학교 경영정보학 (석사)
2005년 경기대학교 정보보호 기술(박사)
2002년 KT 시스템보안부장
2004년 KT 충청전산국장
2005년~현재 남서울대학교 컴퓨터학과 교수
관심분야 : 차세대통신, 컴퓨터네트워크, 정보보호