情報保護學會論文誌
第 21 卷 第 2 號, 2011. 4

Virtual Clustering 기법을 적용한 Integration Security System 구축에 관한 연구

서 우 석,[1†] 박 대 우,[2‡] 전 문 석[3]
[1]숭실대학교 일반대학원, [2]호서대학교 벤처전문대학원, [3]숭실대학교

A Study on Building an Integration Security System Applying Virtual Clustering

Woo-seok Seo,[1†] Dea-woo Park,[2‡] Moon-seog Jun[3]
[1]Soongsil Graduate School, [2]Hoseo Graduate School of Venture, [3]Soongsil University

요 약

최근 Application에 대한 공격을 통하여 네트워크와 데이터베이스에 대한 방어정책인 침입탐지 룰(rule)을 무력화시키고, 침해사고를 유발한다. 이러한 공격으로부터 내부 네트워크와 데이터베이스의 안전성을 확보하기 위한 통합보안에 관한 연구가 필요하다. 본 논문에서는 침입탐지 룰을 설정한 Application에 대한 공격을 차단하기 위한 통합보안 시스템 구축에 관한 연구이다. 네트워크 기반의 공격을 탐지하여 대응하고, 내부 Integration Security System을 Virtual clustering과 Load balancing 기법으로 공격을 분산시키며, Packet 모니터링과 분석을 통하여 공격 목적지 Packet에 대한 방어정책 설정, 공격 Packet 분석, 기록, 룰 업데이트를 한다. 또한 공격 유형별 방어정책을 설정하여 Virtual Machine 분할 정책을 통한 접근 트래픽 해소, 공격차단에 적용하는 Integration Security System을 제안하고 방어를 실험한다. 본 연구 결과는 외부 해커의 공격에 대한 통합보안 방어를 위한 현실적인 자료를 제공하게 될 것이다.

ABSTRACT

Recently, an attack to an application incapacitates the intrusion detection rule, the defense policy for a network and database and induces intrusion incidents. Thus, it is necessary to study integration security to ensure the security of an internal network and database from that attack. This article is about building an integration security system to prevent an attack to an application set with intrusion detection rules. It responds to network-based attack through detection, disperses attack with the internal integration security system through virtual clustering and load balancing, and sets up defense policy for attacking destination packets, analyzes and records attack packets, and updates rules through monitoring and analysis. Moreover, this study establishes defense policy according to attacking types to settle access traffic through virtual machine partition policy and suggests an integration security system applied to prevent attack and tests its defense. The result of this study is expected to provide practical data for integration security defense for hacking attack from outside.

Keywords: Master & Standby Integration Security System, Virtual Clustering

접수일(2011년 1월 18일), 게재확정일(2011년 3월 14일)

† 주저자, ssws2003@yahoo.co.kr
‡ 교신저자, prof1@paran.com

I. 서 론

최근 해외로부터 네트워크와 자원에 대한 공격으로 침해사고가 발생하고 있다. 외부 네트워크에 노출된 Application에 대한 공격을 통하여 네트워크와 데이터베이스에 대한 방어정책인 침입탐지 룰을 무력화 시키고 있어, 방어 대책으로 네트워크 보안장비들을 종합적으로 운영, 관리, 모니터링 하는 Integration Security System인 Enterprise Security Management(이하 ESM이라 한다)가 일반적으로 운영되어지는 보안관제 기술이 되었다.

그러나 현재 ESM의 성능 향상과 구축비용 증대, 기기 확장성과 용이성, 신규 보안장비 증설시 빠르고 효율적인 적용에 호환성의 문제가 발생하고 있다. 이는 ESM의 솔루션이 다양화되고 기술의 진보가 이루어짐에 따라 다수의 시스템과 데이터베이스로 구분되어지고 공격에 대한 방어방법 역시 모니터링 이원화, Master ESM 구성 등을 구성했다. 하지만, 기존 구성의 가장 큰 문제점인 이원화 기반의 실시간 침입정보의 활용 비율이 저하되고 네트워크 영역이 분리되는 경우는 ESM 솔루션 적용에 보안상의 취약점이 발생하고 있어 연구가 필요하다.

본 논문에서는 두 대의 Integration Security System을 Clustering으로 묶고 그 중 1차적인 침입관제 및 방어 ESM을 Master Integration Security System(이하 MISS라 한다)이라 칭하고 보안정책 구현을 위해 자원공유를 위한 ESM을 Standby Integration Security System(이하 SISS라 한다)이라 한다. 또한 MISS와 SISS에 Virtual Machine(이하 VM이라 한다)을 구현함으로써 논리적인 2차 방어 솔루션을 구현한다. 또한 Load balancing이 가능한 Clustering 기법을 적용해서 급속도로 진보하고 있는 공격 형태를 일반적인 통합 보안관리 시스템만으로 탐지하고 대응하는 한계점을 높일 수 있는 방안을 제시하여 실험하고, 구축한다. 외부로부터 접근하는 네트워크 경로에 Virtual clustering 통합 보안관리 시스템을 동일 네트워크 또는 이질적인 네트워크상에 확장된 프로그램 설치나 환경설정 변경파일 업로드 및 데이터변경을 위한 모니터링 등 일괄적으로 동시에 처리할 수 있게 구현함으로써 침해로 인한 장애를 최소화하고 빠르게 대처 가능한 방안을 연구해야 한다.

본 논문에서는 Clustering을 통합 보안관리 시스템에 VM와 함께 접목함으로써 공격기법을 분석하고 학술적인 차원에서 공격 형태에 따른 체계적인 분류, 분류된 공격기법에 따른 방어기법과 학습된 데이터베이스 동기화를 연구하여야 하며, 연구된 내용을 실험을 통해 제안되어진 통합보안 공격방어 체계구축을 연구할 필요가 있다. 또한 제안하는 기법에 대한 개념과 정의를 하고 침해와 방어기법을 실험하고 실험결과를 기술한다.

본 논문의 구성은 다음과 같다. 2장에서는 최근 네트워크 공격 사례와 네트워크 공격분석을 확인하고, 3장에서는 Virtual Clustering 기법을 적용한 Integration Security System에서 침입 방어 기법 제안들이 기술되고, 4장에서는 침입공격에 대한 방어 실험을 제안하고, 5장에서는 결론을 기술한다[1][2].

II. 관련연구

2.1 최근 네트워크 공격 현황

2009년 7.7 DDoS(Distributed Denial of Service attack) 공격 이후에도 2010년 변종공격으로 다양한 공공기관, 행정기관, 금융기관 등에 대한 공격이 발생했고 방어기술과 솔루션이 보안부문에 적용되었다. 그러나 [표 1]과 같이 과거 네트워크를 통한 공격유형과 침해 빈도수를 보면 공격방법이 다양해지고 침해비율도 2009년까지 지속적으로 증가함을 알 수 있다. 하지만 2010년 국가 전반에 걸친 집중적인 DDoS 공격과 함께 많은 보안 솔루션들이 적용되어지면서 침해비율이 다소 낮아졌음을 알 수 있으나, 여전히 침해 비율은 년도 별 증가 추세이다[3][4].

[표 1] 년도 별 네트워크 침해 공격 현황

구분	단순침입	DDoS	Warm & Virus	홈페이지 변조시도	자료훼손 유출시도	경유지 악용시도	합계
합계	1,567	137	3,059	114	222	88	5,187
2006년	369	35	86	28	53	11	582
2007년	467	47	135	14	74	4	741
2008년	488	45	325	59	69	5	991
2009년	243	10	1,545	9	24	46	1,877
2010년	0	0	968	4	2	22	996

2.2 네트워크 공격 분석

공중망에서 발생되는 공격형태가 최근에는 네트워크 기반 하에서 다양한 공격절차를 거쳐 접근하고 자기방어를 위한 역추적 차단 제어 기능까지 탑재한 공

격성향을 가진다. 또한 제2의 공격을 위한 Agent 탑재 Zombie 공격기법으로 1차 공격 대상이었던 네트워크에 지속적으로 존재하기 때문에 정확한 Agent 활동 시점인 공격 포인트를 사전에 파악하고 차단할 수는 없다.

다만, 공격성 Packet 유입에 따른 신속하고 빠른 방어정책을 적용하고 공격정보 학습과 공격성향 분석을 통하여 침입탐지 룰을 데이터베이스화함으로써 동일한 공격성향과 변형된 공격방법을 가진 침해를 사전에 차단하는 역기능적인 방법으로 방어하는 기법이 가장 일반적으로 운영되어 지는 방법이다. 통합 보안관리 시스템을 통해서 가상 사설 통신망, 방화벽, 웹-방화벽 등과 같이 목적별 분리를 통해 통합 관제 모니터링으로 정확한 공격시점을 파악하기 위해서는 〔표 2〕와 같이 다양한 공격 형태를 사전에 분석하고 침해 공격 Tool의 성향을 파악해야 한다〔5〕〔6〕.

〔표 2〕 네트워크 공격 형태 분석

구분	공격유형	세부공격 형태
Network Base Attack	Dos	Land Attack / Teardrop / Targa / NewTear / Nestea / Ping of Death / Inconsistent Fragmentation / Syn Flooding Attack / Smurf Attack / UDP Flooding / Brute-Force Attack
	DDoS	Trinoo Attack / TNF Attack / Stacheldraht Attack / TFN2K Attack
	Network Scanner	Remote Finger Printing / IP Scanner / Port Scanner / Third Party Effect
	Spoofing	IP / E-mail / Web / ARP / DNS
	Session Hijacking	-
	Sniffing	Hub Attack / Switch Jamming / ARP Redirect / ICMP Redirect / ICMP Router Advertisement
	Remote Attack	Remote Active Attack / Etc

2.3. 침입탐지 룰에 대한 Application 공격 분석

ESM 등 기존의 보안시스템에서 방어를 위한 침입탐지 룰에 대한 공격성향과 분류된 공격방법과 기술을 분석하고 최종 공격으로 인한 침해결과 등을 알아본다〔7〕〔8〕.

* Application Layer에 대한 공격

OSI 7 Layer를 공격하는 방법으로는 HTTP Flooding 공격과 VOIP 공격, SQL 공격, RPC 공격, Cache Control 공격, Botnet 공격 등이 있다. MISS 보안정책과 관제 및 모니터링을 위한 침입탐지 룰을 구현하는 Application이 탑재되어 있는 Layer를 공격하는 침입 환경은 서로 다른 네트워크 사이에서 통신 Packet 등과 같은 통신규약을 정의하는 프로토콜이 통신정보를 Encapsulation 또는 De-capsulation 하는 과정을 공격하는 방법과 직접 Application Layer를 침해 포인트로 하는 공격이 주를 이룬다〔9〕.

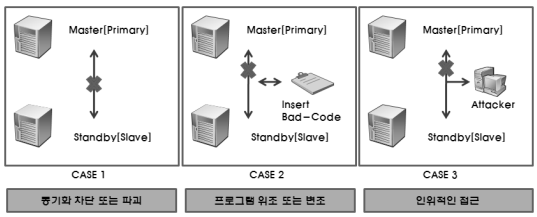
* 데이터베이스에 대한 공격

MISS 보안정책에 대한 다양한 침입탐지 룰을 탑재한 데이터베이스를 대상으로 하는 공격은 3가지 보안특성인 비밀성, 무결성, 가용성의 3대 보안특성을 공격하는 방법으로 분류된다. 데이터베이스가 가장 많은 공격을 당하는 시점은 일반적으로 인위적인 위험에 노출되는 경우와 제3자의 의도적인 공격으로 구분된다. 인위적 위험은 데이터 운영상의 변질과 삭제, 관리자의 보안정책 등급 조정 실수, 디폴트 데이터베이스 관리자 및 유저 계정 관리소홀, 기관 또는 사내 기밀에 해당하는 문서화일 공유 등의 방치, 파일서버 관리소홀 등을 들 수 있다.

또한 제3자의 의도적인 공격으로는 불법접근, 아이디 또는 비밀번호 도용을 통한 데이터베이스 침입경로 노출과 유통되는 데이터베이스에 대한 보안솔루션 미적용 등을 들 수 있다.

* Load balancing에 대한 공격

침입 접근기록인 로그 등을 인위적으로 파괴, 변조, 위조하여 SISS로 동기화를 차단하는 〔그림 1〕과 같은 3가지 기본적인 공격이 있다. 또한, Load balancing에 대한 동기화를 저해하는 공격은 시스템에 대한 부분적인 공격과는 달리 가장 치명적인 침해피해를 발생한다. 논리적 Application 계층에 속하는 VM 역시 모듈 공격이 가능하다〔10〕.



〔그림 1〕 SISS와 동기화되는 Load balancing 구현정책에 대한 공격유형

* Clustering Integration Security System 동기화 데이터베이스에 대한 공격

공격자는 MISS와 SISS가 데이터베이스 동기화

과정을 공격하는 공격기법과 동기화가 이루어진 2차 시스템인 SISS에 대한 공격을 동시에 진행이 가능하다. 최초 MISS를 공격하고 방어 정책을 무력화시킨 공격은 SISS에서 보안정책 등급이 상향되기 이전의 동기화 과정에 공격을 진행함으로써 최종 시스템 하단의 네트워크를 침해한다[11][12].

2.4 다양한 시스템에 대한 Virtual Clustering 적용 현황

현재 Virtual Clustering기법을 적용한 사례로는 분야별로 데이터베이스, 디스크, 시스템 등에서 이루어지고 있으나, 최초 특정 대상을 공격하기 위한 경로인 네트워크에 대한 연구는 다양하게 이루어지지 않고 있다. 또한, 네트워크를 기반으로 하는 침해와 공격에 대한 연구 역시 다각적으로 이루어지지 않고 특정한 방어 영역만을 위한 솔루션에서 단편적으로 이루어지고 있는 실정이다.

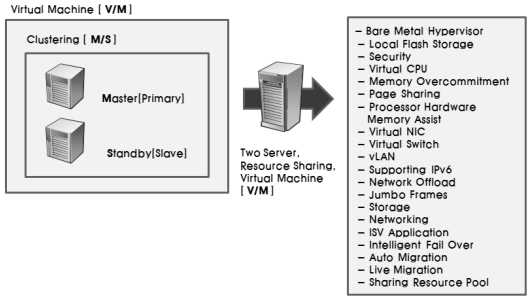
III. Virtual Clustering Integration Security System에서 침입 방어 기법 제안

네트워크에서 최종 방어기법을 제안하기 위한 4단계의 방어기법인 Application Layer, 동기화와 실시간 룰 암호화 연결, VM을 이용한 병렬 ESM과 분리 정책을 구현함으로써 최종 실험을 통한 최적화 방어기법을 제시코자 한다.

3.1 네트워크에서 Application Layer에 대한 공격 방어

Clustering기반의 VM은 [그림 2]와 같은 물리적 계층 위에 가상의 논리적 계층을 둠으로써 하나의 침입탐지 룰 Application이 단일화 또는 일원화된 서비스를 제공하는 형태의 방어 방법을 적용한다. 또한 각각의 방어 시스템에 탑재되어진 VM 침입방어 Application 역시 여러 개의 물리적 Application을 논리적인 서비스 계층에서 침입방어 서비스를 구현한다. 그러나 최초 네트워크 공격이 1차 방어 시스템인 MISS 구성 자원대비 보안정책에 따른 방어가 이루어지지 않고 침해가 지속되는 경우 2차적으로 SISS가 가동되어 공격을 방어한다.

Clustering 기반으로 MISS와 SISS를 하나의 서버처럼 환경을 구성함으로써 정책과 방어기법 적용



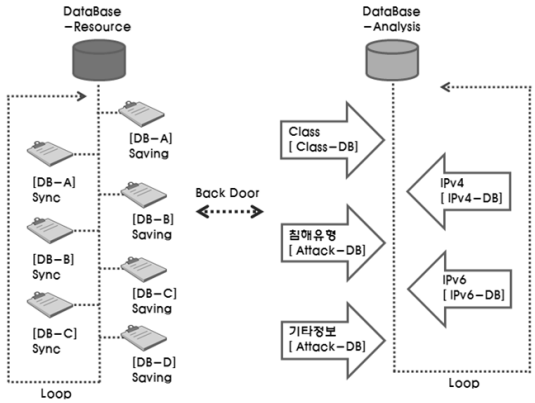
[그림 2] 두 개 서버의 VM을 이용한 Clustering 방어 기능

을 위한 논리적 Application 계층의 성능을 VM를 통해서 MISS와 SISS의 리소스를 활용하여 향상시킨다.

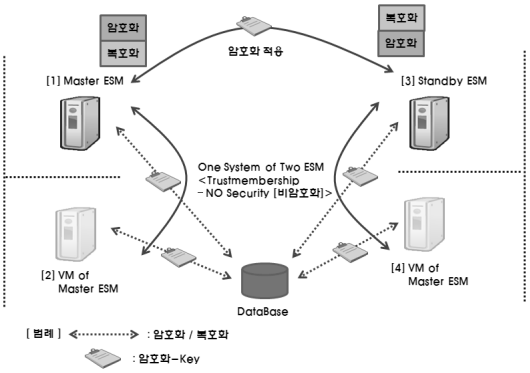
3.2 침입탐지 룰에 대한 동기화와 실시간 룰 암호화 연결을 이용한 공격 방어

Zero Base 공격, 크래킹 공격기법 등은 기존의 침입탐지 룰로 침해사고가 발생 할 수 있다. 따라서 침입탐지 룰은 실시간으로 동기화되어 업그레이드가 되어야 공격을 실시간으로 분석하고 룰을 업데이트하여 공격을 방어 할 수 가 있다.

Clustering 기법을 기반으로 하는 MISS 및 SISS는 동일한 침입탐지 룰에 대한 데이터베이스를 실시간으로 동기화되어 업그레이드가 한다. 이는 최초 공격을 방어하는 시스템과 이질적인 데이터베이스를 보유한 SISS로 구성되어진 경우는 1차적인 공격성향과 방법을 학습하지 못한 상태에서 동일한 공격을 받아야함으로 Clustering 기법하의 시스템 데이터베이스는 일원화 시키면 방어가 가능하다.



[그림 3] 침입탐지 룰을 위한 공격형태(정보) 분석



〔그림 4〕 Master ESM과 Standby ESM 간의 상호 침입 탐지 룰 데이터베이스 보안

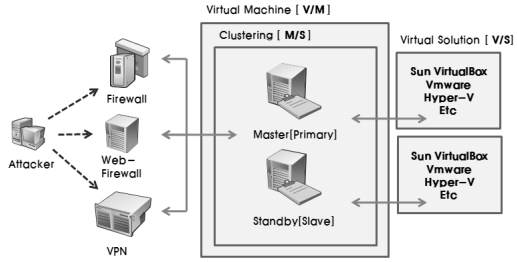
첫 번째 주요 방어대책은 Clustering 기반의 VM 구현에 대한 침해정보를 가진 데이터베이스 보안이며, VM을 적용함으로써 MISS, VM-MISS, SISS, VM-SISS의 4단계의 방어기법이 동일한 정보를 학습한다. 또한, 정보에 대한 동기화를 이루어 방어를 함에 따라 〔그림 3〕과 같이 데이터베이스에 대한 학습 정보 업그레이드와 분석과정이 필요하다.

두 번째 주요 방어대책은 〔그림 5〕와 같이 상호보안을 위한 여러 각도의 데이터 흐름에 따른 보안정책을 적용함으로써 물리적 보안과 논리적인 보안 기본정보를 유지 및 구현이 가능하다.

3.3 VM을 이용한 병렬 ESM의 방어 기법

Integration Security System 방어정책은 가상 사설 통신망, 방화벽, 웹-방화벽, 침입탐지시스템 등 물리적인 계층을 관리하도록 하는 솔루션을 적용하고 이중화 Clustering을 통한 방어기법을 적용한다.

Clustering의 경우는 물리적 계층 기반 하에서 논리적 Application을 적용함으로써 반드시 1차적인 침해에 대한 방어가 이루어지지 않는 경우 2차 적인 SISS가 구동되어야 하므로 결국 물리적인 Load balancing이 이루어진다. 따라서 각각의 ESM 서버마다 논리적인 VM 방법을 이용한다. 이용방법으로는 Sun VirtualBox, Vmware, Hyper-V 등을 이용해서 서버 내에 또 다른 Virtual clustering을 구현함으로써 두 대의 물리적인 시스템을 이용한 병렬 통합보안과 각 ESM 서버 내에 또 다시 논리적 자원공유 병렬 통합보안 솔루션을 적용함에 따라 〔그림 5〕와 같이 1차 물리적 방어와 2차 논리적 방어 솔루션을 적용한다. 따라서 MISS를 이용해서 1단계 물리적 침입



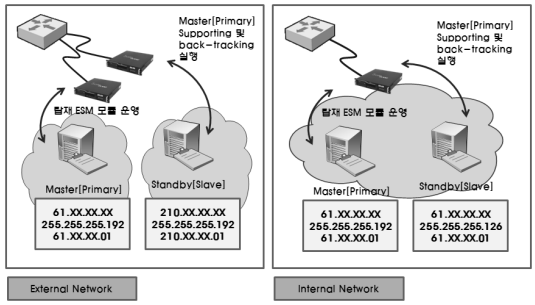
〔그림 5〕 병렬 ESM에 대한 Integration Security System과 VM 솔루션 구조

방어, 2단계 논리적 침입방어, 3단계로는 SISS의 물리적 침입방어, 4단계 논리적 침입방어 솔루션으로 4단계 병렬 Integration Security System을 구현한다.

3.4 Clustering 기법을 적용한 동일 네트워크와 이기종 네트워크에서 ESM 분리 정책

접근 네트워크를 내부 또는 외부 망을 이용해서 Clustering 기반의 가상 분산처리 방어기법을 활용한다. 서로 다른 망에 방어정책을 탑재한 MISS와 SISS를 논리적인 네트워크 영역으로 분리하여, 1차 피해 정도에 따라 2차 방어 네트워크 영역의 서버를 Virtual Integration Security System으로 구성함으로써 침입자가 실제 침해 또는 파괴코자 하는 목적지 게이트웨이로 판단하도록 하는 방어기법이다.

외부 망을 병렬 방어 네트워크로 구성하는데, 활용하는 방어방법은 〔그림 6〕과 같이 MISS와 SISS의 네트워크가 논리적인 분리가 아닌 실제 물리적으로 전혀 다른 망으로 구성함에 따라 침입자의 역추적을 위한 솔루션을 Clustering된 SISS에 탑재하여 1차 MISS에 대한 공격과 함께 침입정보가 동기화 되어



〔그림 6〕 동일 네트워크와 이기종 네트워크에서 ESM을 이용한 정책

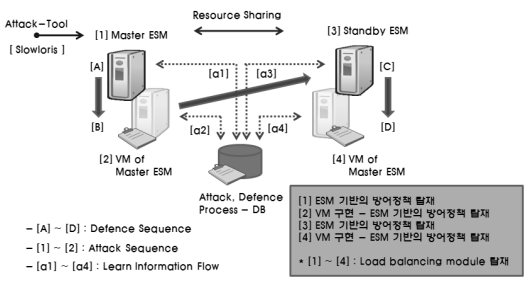
실시간으로 공격자에 대한 방어와 역추적을 동시에 시행하는 방법이다.

IV. Virtual Clustering Integration Security System 공격에 대한 방어 실험

4.1. 실험 환경과 실험 내용

CPU 2.66GHz * 2, Memory 2GB, HDD 500GB, NIC 10/100/1000 TX*4 & 1000 SX*4의 하드웨어 사양을 가진 방화벽을 기반으로 1차 DMZ를 구성하고 Integration Security System을 DMZ내에 Clustering 기법을 적용해서 2대를 병렬로 Master ESM과 Standby ESM으로 구현한다. 또한, 각각의 ESM 서버에 CPU VT Type, Integration Component & VHD Prog, VSP, VCS기반의 VM 솔루션을 적용하고, Master ESM에는 시스템 자원을 유동적으로 변경 가능한 VM 기법을 적용한다. Standby ESM 역시 시스템 자원 공유를 제한하는 VM 솔루션을 적용하고, 실험환경에서 공격 툴은 DDoS 공격 툴인 NetBot Attacker ver. 1.6 Public을 이용해서 지속성을 가진 공격의 유형과 단순 반복형의 공격을 Master ESM에 최초 공격을 시행한다. 또한, 구현하는 기본적인 ESM 기반은 Event monitoring Tool, Agent Analysis Tool, Center Manager Tool 등으로 구성한다.

〔그림 7〕과 같이 이번 실험에서는 최초 공격에 대한 MISS 공격으로 인한 부하를 2차적으로 VM 솔루션을 이용해 보안등급을 상향한다. 상향된 등급을 운영가능 하도록 자원을 유동적으로 증가시키며, 방어를 진행하고 최초 공격으로 MISS와 VM-MISS 방어의 한계점을 넘기게 되는 순간 2차로 통합 보안관리 SISS로 Load balancing 정책에 따라 공격 트래픽을 분할하여, 방어하는 형태로 구성해서 제안한 Virtual Clustering 기반의 통합 보안관리 시스템 방어 현황과 방어기법의 확인 및 분석을 통해 실험결과와 내용을 확인한다.



〔그림 7〕 실제 Virtual ESM 구현환경

4.2. 취약점에 대한 공격 실시

보안을 위한 다양한 기기들인 방화벽, 침입 탐지 시스템, 가상 사설 통신망 등의 장비들을 통합 관리하는 방안의 하나로 1단계 MISS, 2단계 VM-MISS, 3단계 SISS, 4단계 VM-SISS를 제안했다.

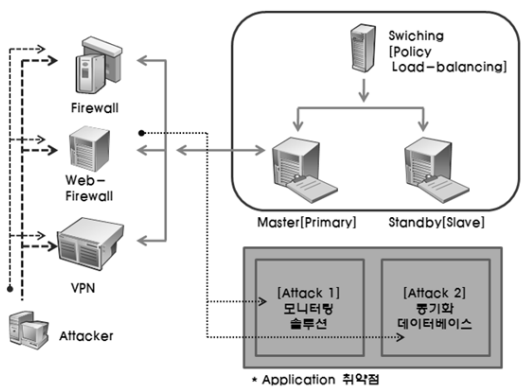
4.2.1 Application 계층에 대한 취약점 공격과 방어

Integration Security System의 첫 번째 Application 취약점 공격은 초당 5Gbps 이상의 공격 Packet을 전송함으로써 전체적인 장비들을 관제하고 운영하기 위한 모니터링 솔루션인 Application에 부하를 발생시켰다.

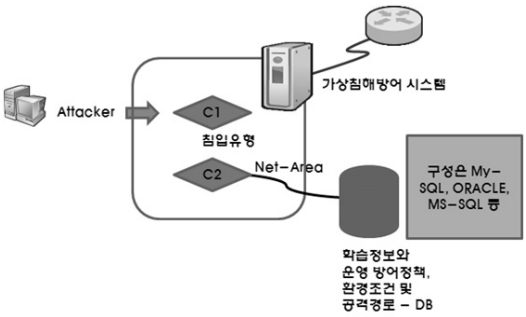
두 번째 Application 취약점 공격방법은 2차적인 방어를 위한 SISS의 방어정책 자체를 무력화하는 공격을 목적으로 초당 1,000,000개의 Session Flooding 공격을 시행했으나, 〔그림 8〕과 같이 Integration Security System의 Application 공격 형태와 흐름에 대한 파악이 가능했으며, 2단계 VM-MISS 수준에서 방어가 가능했다.

4.2.2 데이터베이스에 대한 취약점 공격과 방어

Clustering 기법을 기반으로 하는 MISS와 SISS 간의 공격에 대한 학습정보와 운영 방어정책, 환경조건 및 공격경로 등과 같은 공격에 대한 성향정보를 가



〔그림 8〕 Integration Security System 관제를 위한 탑재 Application에 대한 공격 형태와 흐름

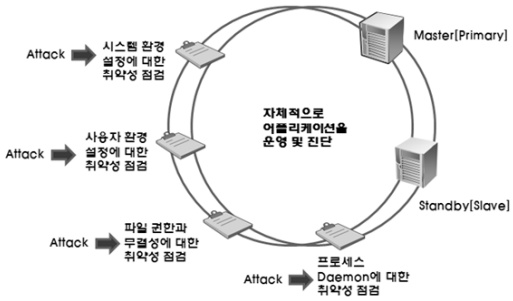


〔그림 9〕 MISS와 SISS의 침해 학습정보의 동기화 및 암호화 과정에 대한 데이터베이스 침해

진 데이터베이스 동기화를 위한 Application 공격을 초당 2,000,000개의 Session Flooding으로 접근 공격을 시도한다. 그러나 〔그림 9〕와 같이 침입탐지 룰을 구성하는 데이터베이스 형태는 My-SQL, ORACLE, MS-SQL 등과 같이 다양하지만, 각 침입 유형에 따른 방어 조건〔C1, C2〕을 구성함으로써 1단계 MISS 수준에서 일부 방어가 가능했으며, 초당 Session을 지속적으로 증가시킨 경우에도 2단계 VM-MISS 수준에서 방어가 가능했다.

4.2.3 제한된 ESM에 대한 실시간 룰 업데이트 공격과 방어

Integration Security System의 경우는 자체 취약성 점검 솔루션을 Application 계층에서 진행한다. 1단계는 시스템 환경 설정에 대한 취약성 점검, 2단계는 사용자 환경 설정에 대한 취약성 점검, 3단계는 파일 권한과 무결성에 대한 취약성 점검, 프로세스 Daemon에 대한 취약성 점검 등 다양한 단계별 취약성 점검을 운영한다. 또한, 다양한 보안 기기로부터 침해와 관제 정보를 모니터링 하는 부문에 대한 취약성 점검 역시 자체적으로 Application을 운영함으로써 진단한다. 이때 각 점검 Event별 자체점검 프로그램에 대해 〔그림 10〕과 같이 설정 값 반영 차단을 위한 프로세서 점유비율이 90% 이상이 될 때까지 무한 DDoS 공격을 초당 3,000,000개 이상의 Session 접근 Flooding 공격과 초당 5,000개의 공격 Packet, 통신 대역폭 점유율을 1,5Gbps까지 증가시켜 공격을 시행했으나, 4단계의 VM-SISS의 자원공유와 지원정책으로 3단계 SISS 수준에서 방어가 가능했다.



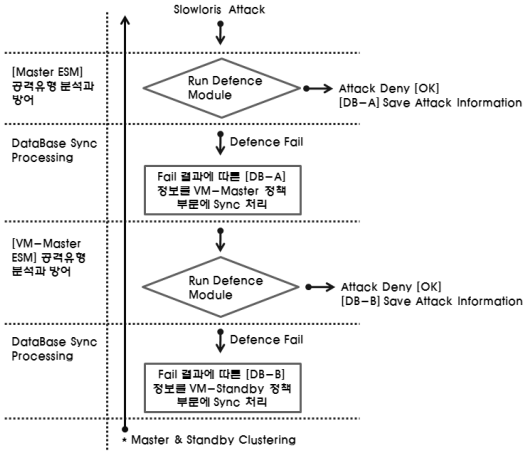
〔그림 10〕 ESM의 각 점검 Event별 자체점검 프로그램에 대한 침해 포인트

〔표 3〕 VM 기반의 Clustering ESM 4단계 보안 정책

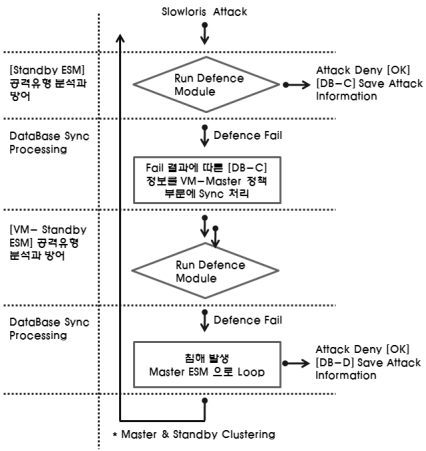
단계	적용 솔루션	비고
1	Master 등급 등급 시스템	Standby Resource Sharing
2	Master VM	In Master of Virtual Machine
3	Standby 등급 등급 시스템	Restrictive Master Resource Sharing
4	Standby VM	In Standby of Virtual Machine

4.3. 공격에 대한 4 단계 방어 전략과 방어 알고리즘

방화벽, 침입 탐지 시스템, 가상 사설 통신망 등 내부 네트워크 보안을 위한 1차 방어기기인 ESM을 통합적으로 관리하여 Clustering과 VM 기반의 MISS와 SISS를 구현하였다. Master ESM의 경우는 Clustering 정책과 데이터베이스 공유 및 Master ESM 서버 내의 VM을 통한 1차 방어와 Standby ESM의 경우는 Master ESM 공격 침해 시 자원공유를 통한 방어 정책 및 소스지원과 Standby ESM 서버 내의 VM을 통한 2차 방어를



〔그림 11〕 ESM MISS 구축을 통한 방어 알고리즘



〔그림 12〕 ESM SISS 구축을 통한 방어 알고리즘

구현함으로써 거시적인 방어정책은 2차 방어로 구성하였다. 방어에 대한 단계를 구분하여 보면 〔표 3〕과 같이 4단계의 세부방어 정책으로 나누어 볼 수 있다.

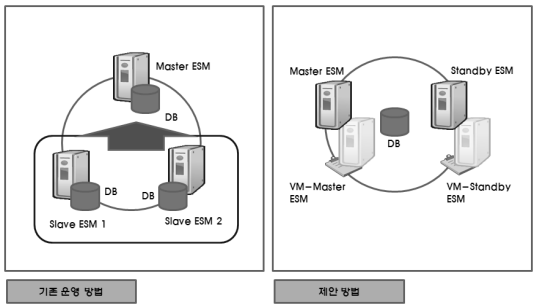
또한, VM을 통한 2차 방어에 대한 4단계의 물리적인 ESM에서 4단계의 논리적인 방어 흐름은 〔그림 11〕의 MISS 흐름과 〔그림 12〕의 SISS 알고리즘으로 구축한다.

4.4. 공격에 대한 결과 분석

Clustering 기반의 Integration Security System을 구성하고 운영하는 부분은 방어를 위한 시스템 자원공유를 통해서 성능을 최적화 및 최대화하고 1차적인 방어를 한다. 하지만 침입자의 공격을 VM 솔루션을 각 ESM 서버별로 탑재 운영함으로써 공격에 대한 다차원적인 방어가 가능하다.

그러나 Clustering 기법이 기반이 되어진 MISS와 SISS의 경우는 VM 솔루션 종류에 대한 선택에 따라 침해 방어정책의 구현 등급이 구분되며, 추가적으로 침해방어를 위한 자원공유와 활용에 따른 결과는 MISS와 SISS에 CPU 등을 포함한 자원과 그 공유비율에 따라 성능의 확연한 차이를 나타낸다.

즉, Virtual clustering 통합 보안관리 시스템 모델인 MISS, VM-MISS, SISS, VM-SISS를 단계별로 적용하고 자원의 경우는 병렬처리 함으로써 VM 적용에 따른 침해방어 비율이 다소 차이는 있으나, 각 단계별 6내지 7% 이상의 효과가 있어 최종 VM-MISS까지 적용시 최종 침해방어 비율은 약 21~24% 상승과 2,000,000개의 Session 이상의



〔그림 13〕 기존 구축 방법과 제안 방법과의 비교

접근 Session은 가능하지만, 손실률을 감안한 최종 1,000,000 Session 이상의 접근 Session 허용비율, 최대 통신 트래픽 허용량은 2Gbps까지 상승했다.

4.5. 기존 방어 방법과 제안한 방법의 비교분석

현재 Integration Security System의 솔루션이 다양화되고 기술의 진보가 이루어져서 〔그림 13〕과 같이 Master ESM, Slave ESM 1, Slave ESM 2로 시스템을 구분하고 데이터베이스 역시 분리 운영함으로써 공격에 대한 방어와 모니터링을 이원화하고 최종 Master ESM에서 전체 관리를 하는 형태로 구성되어진다. 하지만 기존 구성의 문제점으로는 첫째 하드웨어 인프라 구축상의 비용의 문제와 둘째 데이터베이스의 이원화로 인한 실시간적인 침입정보의 활용 비율의 저하 그리고 세 번째 가장 큰 문제는 각 내부 또는 외부 네트워크 영역을 분리 운영 시에는 네트워크마다 장비가 운영하는 통합보안 솔루션이 다르다는 부분이다.

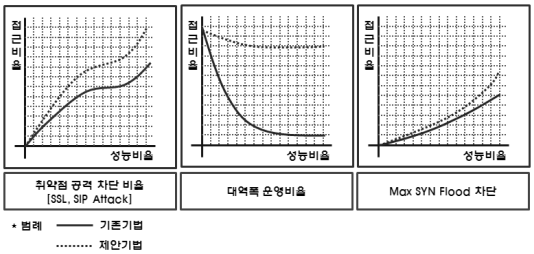
상호 다른 솔루션으로 구축 시에는 모니터링과 관제로 얻어진 정보에 대한 일원화해야 하는 단계가 소요된다. 하지만 Virtual Clustering으로 Integration Security System을 구현 시에는 적은 인프라 구축 비용과 침입 정보에 대한 데이터베이스의 공격정보 일원화 및 실시간 공격차단 등급 조정 등의 관리자단에서 효율성과 단계별 침입에 대한 보안 등급 조정이 자유롭다.

〔표 4〕에서는 시스템 성능을 비롯한 15가지의 운영방법에 따른 비교 결과를 나타내고 있으며,

〔그림 14〕는 취약점 공격 비율과 대역폭 운영비율, Max SYN Flood 차단의 3가지 주요 성능향상 척도 측정을 통해 결과를 얻었으며, 향후 병행평가 수행이 반드시 필요하다.

〔표 4〕 기존방법과 제안방법의 비교

구분	세부내용	General Form 기법	Proposal Form 기법
침해방어 비율 [%]	침해 손실율	제한없음	21% 상승 [패킷 손실율 2% 포함]
유지세션 허용비율 [%]	세션수	제한 / 500,000	제한 폭 상승 / 1,000,000
통신량 [Gbps]	통신 트래픽 허용량	1 ~ 1.6	1.7 ~ 2
이벤트 처리	DataBase 수집 방법	장비별 기록 취합과정	종합 취합과정
	Filtering	장비별	종합
관제 성능	실시간 접근	개별 접근 방식	단일경로 접근
	이벤트 모니터링	개별 모니터링	종합 모니터링
	장애탐지	각 장비별 로그분석	종합 로그분석
	공격탐지	직렬방식 탐지	병렬방식 탐지
	연관분석	미구현	구현
운영관리	권한, 로그 관리	개별관리	종합관리
논리적 기능	로드 밸런싱	제한	무제한
	방어정책 및 모니터링 처리	제한	무제한
경제성	도입 및 구축과 운영비용	↑	↓
구현	효율성과 접근성	단순 [구현결과 반비례]	복잡 [구현결과 비례]



〔그림 14〕 최종 제안기법과 기존기법과의 3대 방어성능 비교결과

V. 결 론

본 논문에서는 새로운 침해공격과 시차를 두고 지속적으로 공격 방법에 대한 ESM 등 보안 시스템 자원의 효율적인 활용과 구축에 관한 연구이다. ESM 등 공격에 대한 방어가 가능한 보안시스템에 VM 솔루션을 탑재한 Clustering 병렬 1차 MISS와 병렬 2차 SISS를 구성하고, 논리적인 Load balancing을 통해서 공격 트래픽과 유형에 따라 분산 대응하여 공격에 대한 방어 정책을 제안하고, 공격과 방어를 실험하였다.

본 논문의 제안으로 통합 보안관리 시스템 ESM에 대한 보안 정책을 확장한 Virtual clustering 통합 보안관리 시스템 모델을 적용함으로써, 기존의 2대 ESM에 침해방어 비율 약 21% 상승과 1,000,000 Session 이상의 접근 Session 허용비율, 최대 통신 트래픽 허용량은 2Gbps까지 상승했다.

향후 연구에서는 탑재된 VM 솔루션의 특성과 종류에 따라 방어하는 비율과 방어의 적정성 그리고 효율성이 차이점을 분석하여 통합 보안관리 시스템의 공격에 대한 방어비율이 상호 비례가능한 수준의 모듈을 개발을 연구해야 한다. 또한 보안 종합 관제 시스템과 공격 방어를 위한 개별 방어 기술들이 융합되고 발전하는 확장된 방어 시스템에 대한 연구와 대응모델에 대한 개발과 연구가 필요하다.

참고문헌

〔1〕 Il-Hyung Park, Seong-Woo Kim, and Seung-Woo Seo, "Improving Research Information Security in Academic Institutes through the Analysis of Security Awareness and Activities," Korean Institute of Information Security and Cryptology , vol.20, no.2, pp. 91-108, Apr. 2010.

〔2〕 Tavares and Rodrigo, "Regional clustering of peace and security," Global change, peace & security, vol. 21 no. 2 pp. 153-164, 2009.

〔3〕 보안뉴스, http://www.boannews.com/media/view.asp?idx=22545&kind=1&search=title&find=%C1%F6%B3%AD%C7%D8+%C1%A4%BA%CE+%C3%E2%BF%AC%B1%E2%B0%FC+%C7%D8%C5%B7, "지난해 정부 출연기관 해킹 2,551건...5년간 138% 급증," 김정완 기자, 2010년 8월 25일.

〔4〕 인터넷침해대응센터, "인터넷 침해사고 동향 및 분석 월보," 2010년 10월호, pp. 2-6, 2010년 10월.

〔5〕 Cheng, F, Roschke, S, and Meinel, C, "Implementing IDS Management on Lock-Keeper," Lecture notes in computer science, vol.5451, pp. 360-371, Apr. 2009.

〔6〕 Burns, Tom, Catty, and Jocelyn, "IPS in Europe: the EQOLISE trial," Psychiatric rehabilitation journal, vol. 31 no. 4, pp. 313-317, 2008.

〔7〕 임철수, "클라우드 컴퓨팅 보안 기술," 정보보호학회지, 제 19권, 제 3호, pp. 14-17, 2009년 6월.

〔8〕 Myung-Ho Yeo, Yu-Mi Kim, and Jae-Soo Yoo, "A Dual-layer Energy Efficient Distributed Clustering Algorithm for Wireless Sensor Networks," Journal of KISS, vol.35, no.1, pp. 84-95, Feb. 2008.

〔9〕 Gyeong-Yong Heo, Se-Woon Choe, and Young-Woon Woo, "Improvement of the PFCM(Possibilistic Fuzzy C-Means)

Clustering Method," The journal of the Korean institute of maritime & communication sciences, vol13, no1, pp. 177-185, Jan. 2009.
〔10〕 Young-Bok Cho, Jae-Min Choi, and Sang-Ho Lee, "An Efficient Dynamic Prediction Clustering Algorithm Using Skyline Queries in Sensor Network Environment," Journal of the Korea society of computer and information, vol.13, no.17, pp. 139-148, Dec. 2008.
〔11〕 Chi-Yoon Jeong, Seon-Gyoung Sohn, Beom-Hwan Chang, and Jung-Chan Na, "An Efficient Method for Analyzing Network Security Situation Using Visualization," Journal of the Korean Institute of Information Security and Cryptology , vol.19, no.3, pp. 107-117, June. 2009.
〔12〕 Seung-Mok Kim, Jong-Hyun Lim, and Seung-Hoon Kim, "An Energy-Efficient Clustering Scheme based on Application Layer Data in Wireless Sensor Networks," Journal of Korea Multimedia Society, vol.12, no.7, pp. 997-1005, July. 2009.

〈著者紹介〉

서 우 석 (Woo-seok Seo) 종신회원
2006년: 숭실대학교 정보과학대학원 정보통신융합학과 석사
2009년 9월~현재: 숭실대학교 컴퓨터학과 박사과정
〈관심분야〉 정보보호, 네트워크 보안, 방화벽, Router & Network Design

박 대 우 (Dea-woo Park) 종신회원
1998년: 숭실대학교 컴퓨터학과 석사
2000년: 매직캐슬정보통신 연구소 소장, 부사장
2004년: 숭실대학원 정보과학대학원 정보보안학과 겸임조교수
2004년: 숭실대학교 컴퓨터학과 박사
2006년: 정보보호진흥원(KISA) 선임연구원
2007년~현재 : 호서대학교 벤처전문대학원 조교수
〈관심분야〉 정보보호, 유비쿼터스 네트워크 및 보안, 보안 시스템, CERT/CC, Forensic, VoIP 보안, 이동통신 및 WiBro 보안, IT-Convergence

전 문 석 (Moon-seog Jun) 종신회원
1981년 2월: 숭실대학교 전자계산학과 졸업
1986년 2월: University of Maryland Computer Science 석사
1989년 2월: University of Maryland Computer Science 박사
1986년 9월~1989년 12월: University of Mary 강사
1989년 3월~7월: Morgan State University 조교수
1989년 9월~1991년 2월: New Mexico State University Physical Science Lab. 책임연구원
1991년 3월~현재: 숭실대학교 정교수
〈관심분야〉 정보보호, 네트워크 보안, 전자여권, 암호학