White Paper

TrusGuard,
The integrated security technology beyond F/W & VPN

Revision Version: AhnLab TrusGuard White Paper ver. 1.0.1
Release Date: October 8, 2008

AhnLab, Inc.
6th Fl., CCMM Bldg.
12 Yeouido-dong,
Yeongdeungpo-gu, Seoul 150-869,
Korea
82-2-2186-6000
www.ahnlab.com

Table of Contents

Ⅰ. Introduction

인터넷은 현재 개인의 Life Style로부터 기업의 사업 영역까지 전 분야에 걸쳐 막대한 영향력을 행사하고 있다. 주변을 둘러보면 웹 커뮤니티를 통해 서로의 일상을 공유하거나, PDA를 들고 다니며 무선인터넷을 즐기는 사람들을 쉽게 볼 수 있다. 인터넷을 기반으로 사업을 영위해 나가는 인터넷 포털/ 온라인 게임/ 온라인 쇼핑몰 등이 새로운 산업 영역으로 자리 잡았다. 또한 온라인 은행거래 /증권거래, 온라인 교육 등 기존 Off-line 산업과 결합되어 새로운 부가가치를 창출하는 형태로 발전하고 있다. 이렇게 인터넷이 Business의 중심으로 자리잡으면서 이와 더불어 보안위협의 종류 및 그로 인한 피해의 규모도 기하급수적으로 늘어나고 있다. 인터넷 초기 단순 해킹이나 바이러스 중심에서 최근에는 웜, 스파이웨어, 트로이목마, DDoS, Phishing, Application 취약점 공격 등으로 발전하면서 기법의 종류와 복잡성 그리고 파괴력이 배가되고 있다.

본 문서에서는 이러한 보안위협의 증가에 대한 대안으로 부각되고 있는 통합 보안 시스템(Integrated Security System)의 정의 및 역할 그리고 향후 전망 등을 다뤄보기로 한다

Ⅱ. 보안위협 최근 동향

최근 들어, 인터넷상의 위협 및 공격의 패턴은 다양화, 지능화, 악성화, 복합화의 양상을 보이고 있다. 과거에는 바이러스, 웜, 스파이웨어, Bot, 트로이목마, 피싱, DDoS 등 단일 형태의 공격들이 주를 이루었지만 이제는 스파이웨어+웜, 트로이목마+바이러스 등 악성 코드의 범위를 넘나들면서 제작 유포되고 있다. 또한, 예전에는 단순한 개인적인 명성이나 성취감을 얻기 위한 수단으로 제작되었던 악성코드들이 최근에는 금전적인 이득을 취하려는 수단으로 악용되면서 그 피해는 더욱 심각해지고 있다. 특히 최근에는 기업 내 On-line 비즈니스에 대한 의존도와 중요성이 증가하면서 웹/ IE 등 특정 어플리케이션 취약점을 활용한 공격이 주를 이루고 있다. 또한 기업의 인터넷 비즈니스의 얼굴이라 할 수 있는 Main 홈페이지에 대한 DDoS 공격도 날이 갈수록 그 강도를 더해가고 있다. 실제로 최근 몇몇 대형 금융기관이나 인터넷 비즈니스 기업의 홈페이지가 DDoS 공격을 받아 다운되는 사태가 발생하기도 하였고, 국가를 상대로 한 Cyber 공격의 도구로 활용되어지기도 하였다.

최근 성행하고 있는 보안위협의 유형을 살펴보면 아래와 같다.

■ 웹 관련 공격의 증가

웹 애플리케이션의 취약점을 이용해 해킹하거나 DDoS(Distributed Denial of Service; 분산서비스거부) 공격을 하는 일이 증가하고 있다. 많은 웹사이트가 보안에 대해 고려되지 않은 채 개발•적용되기 때문에 보안에 매우 취약한 상태이다. 이로 인해 많은 사이트들이 무방비 상태로 공격을 당

하고 있는 것이다. 또한 이를 통해 악성코드와 스파이웨어를 유포하거나 해당 웹 페이지로 유도하는 일이 전년에 이어 지속적으로 발생하고 있다. 또한 DDoS 공격은 금전을 요구하기 위한 수단으로 이용되는 일이 더욱 많아질 것으로 예측된다.

■ 애플리케이션 취약점 공격 증가

현재 MS사의 운영체제나 애플리케이션 취약점을 노리는 공격이 가장 비중이 높지만 그 수는 점차 줄어드는 추세이다. 반면 PDF, 애플 맥 OS X, Active X, 멀티미디어 플레이어, 이미지 뷰어, 메신저 등 사용자들이 많이 사용하는 애플리케이션들에 대한 공격이 증가하고 있다. 이런 흐름은 당분가 지속적으로 이어질 것으로 예상된다

■ 트로이 목마, 웜, 스파이웨어의 증가

트로이목마와 변형된 Worm 공격 그리고 스파이웨어가 증가 추세에 있다. 동북아시아 한국의 경우 중국발 트로이 목마의 기승으로 2008년 상반기 전체 악성코드 중 약 70%가 트로이목마로 집계되었고, 그 뒤를 Dropper 종류의 스파이웨어가 따랐다. 동유럽 루마니아의 경우 광고 목적의 악성 애드웨어 종류의 트로이목마가 전체 악성코드 중 1위를 차지했다. 러시아의 경우 변형된 웜인 넷스카이 웜과 브론톡 웜 (Brontok Worm)이 가장 많이 발생했다.

■ 사이버 블랙 마켓의 활성화

가상의 재화를 현금으로 교환하는 '사이버 블랙 마켓'의 규모가 커지고 있다. 여기에서는 신상 정보 및 신용카드 정보, 온라인 게임 계정 등이 거래되고 있으며, 악성코드가 판매되는가 하면 피싱, DDoS 공격 등을 대가를 받고 해주는 것으로 알려져 있다. 금전적 이익을 위해 불특정다수를 공격하는 것보다 특정 타깃을 노리는 국지적 공격이 증가하고 있다

III. Network Security의 진화

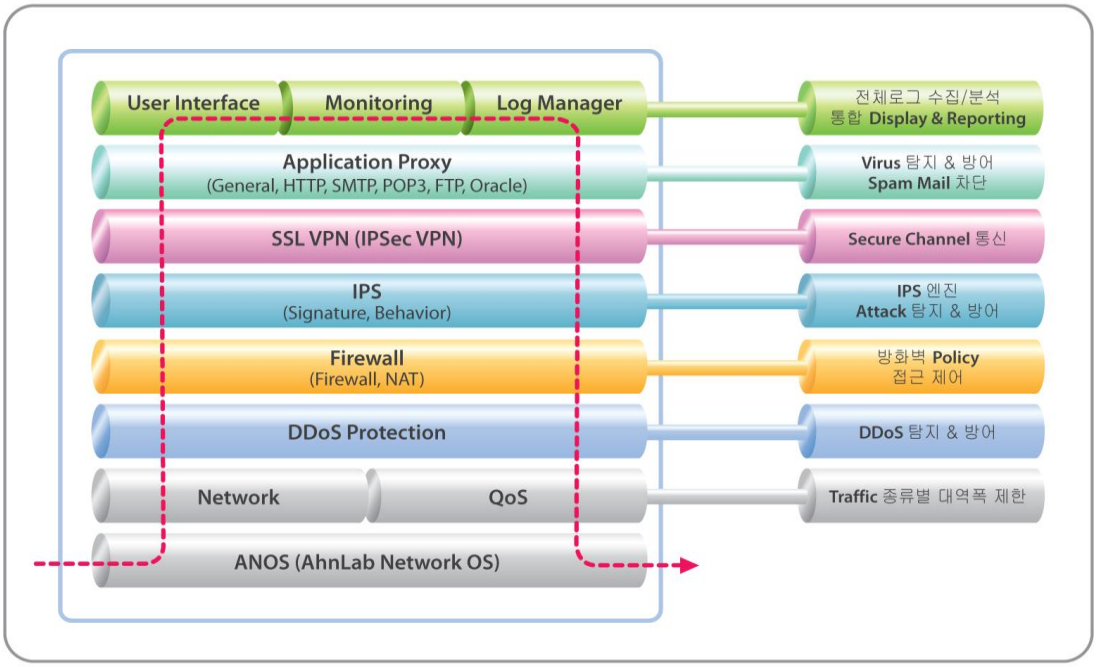
이렇게 보안 위협이 다양화, 지능화, 복합화, 악성화 되면서 Network기반의 Security Appliance의 기술 및 기능도 함께 발전해 왔다. 제 1세대는 S/W기반의 단순 Packet Filtering 수준의 방화벽에서부터 출발하였다. 이 때의 주요 방어 대상은 Layer 3/4 기반의 허가되지 않는 불법적인 접근을 차단하는 것이었다. 인터넷이 발달하고, 웹을 통한 정보 교류가 급속도로 증가하면서 기존의 단순한 Packet Filtering 만으로는 늘어나는 Traffic과 보안위협을 감당하기 어려워졌다. 이에 제 2세대는 전용 하드웨어 Appliance 기반의 고성능 Stateful 방화벽과 Packets의 Payload를 들여다보는 IDS/IPS로 발전하게 된다. 2세대 제품들은 멀티코어/ 전용 Chipset 등의 활용으로 대용량 Traffic 처리에 강점을 갖도록 설계되었으며, Layer 3/4 기반의 Packet Filtering 수준을 넘어 Layer 7 기반의 Packet Inspection으로 발전하여 내부 network으로 유입되는 Network 기반의 공격을 차단할 수 있는 수준에 이르렀다.

인터넷 Business가 주요 산업으로 성장하고 웹을 통한 금전적인 거래 등이 활발해지면서, 보안위

협도 기업간 거래나 웹 비즈니스에 실질적인 타격을 입히면서 금전적인 보상을 취득하려는 형태로 변화하고 있다. 웜에 트로이목마를 결합하여 내부정보를 빼낸다던가, 특정 Application 취약점을 이용한 공격으로 시스템을 다운시키거나 내부정보를 빼내는 등의 공격들이 주류를 이루고 있다. 이러한 복합적이고 다양한 공격에 대응하기 위해 제 3세대 Network Security는 Layer2부터 Layer7까지 다양한 방어 Mechanism이 유기적으로 통합된 Unified Threats Prevention 시스템으로 진화하고 있다. 제 3세대 Network Security는 Layer 3/4 기반의 방화벽, DDoS방어, Layer 7 기반의 IDS/IPS, Contents 기반의 Anti-virus/ Anti-spam/ Web Sites Filtering 등의 기능들이 상호 연동하여 복합적인 악성코드 및 네트워크 공격을 효과적으로 방어하면서 현재 시장의 주류로 부각하고 있다

IV. 통합 보안 시스템 (Integrated Security System) 이란

진정한 통합 보안 시스템 (Integrated Security System)이란 여러 가지 보안기능을 단순하게 통합해 놓았다기 보다는 각각의 여러 보안 기능을 유기적으로 결합해 다양한 레벨의 공격에 대응할 수 있다는 것이다. 통합 보안 시스템의 아키텍처는 그림 1과 같다.



[그림 1] 통합 보안 시스템의 아키텍처

통합 보안 시스템의 보안 기능간 유기적인 결합의 예를 살펴보자. 기업 내부로 유입되는 Packets들은 가장 먼저 DDoS 엔진에 의해 DDoS 공격인지 아닌지에 대한 판단을 받게 되고, 정상적으로 통과된 Packets들만이 방화벽의 Stateful Inspection 방식의 Filtering을 거치게 된다. 이 때 불법적인 접근시도나 비인가 Packets은 상당부분 걸러지게 되고 소수의 정상 Packets만이 IPS 엔진에 의해 악성코드 보유 여부를 검사 받게 된다. IPS 엔진을 통과하면 Contents Filtering Process 거치면

서 File 기반의 바이러스/악성코드를 보유한 Packets이나 Spam 등이 걸러지게 되고 정상적인 Packets만이 내부 Network에 유입되는 것이다.

이러한 개별 기능간 유기적인 결합 및 상호 연동을 통해 다양한 Layer의 수많은 공격들을 효과적으로 방어할 수 있다. 네트워크의 계층별 대표적 공격을 살펴보면, Layer 2에서의 ARP Spoofing, Layer 3에서의 IP spoofing, ICMP 공격, DHCP 공격, Layer 4에서의 flooding 및 D(D)oS 공격, Scanning, Layer 7에서의 바이러스, 웜, 스파이웨어, 트로이목마, OS 및 application의 취약점 공격 등 다양한 계층에서 공격이 이루어지고 있다. 이러한 보안 위협을 효과적으로 방어하기 위한 대안으로서 통합 보안 시스템의 필요성이 지속적으로 부각되고 있다.

V. Integrated Security Technology

1. 통합 보안 시스템의 H/W 기술

▪ Muti-Core 기반 H/W 지원

통합 보안 시스템은 다양한 방어 메커니즘을 제공함에 따라 개별 보안 솔루션에 비해 성능이 떨어질 것이라는 우려가 있다. 하지만 일반적으로 1Gbps 이하 급의 SMB 시장은 CPU 기반의 프로세싱으로도 그에 걸맞은 트래픽을 처리할 수 있으며, Multi-Giga 급의 트래픽에서는 NP(Network Processor)나 Multi-Core CPU 등의 기반 기술 하에 구현된 시스템을 선택하면 성능 관련 이슈는 없을 것이다.

통합 보안 시스템은 이와 관련해 S/W에서의 최적의 성능을 보장하기 위해 SMP(symmetric multiprocessing)를 지원하고 있다. SMP는 두 개 또는 그 이상의 프로세서가 한 개의 공유된 메모리를 사용하는 다중 프로세서 컴퓨터 아키텍처이다. 현재 사용되는 대부분의 다중 프로세서 시스템은 SMP 아키텍처를 따르고 있다. SMP 시스템은 부하의 효율적 분배를 위해 프로세서간 작업 스케줄링을 쉽게 조절할 수 있게 해준다.

2. 통합 보안 시스템이 가져야 할 네트워크 기반 기술

통합 보안 시스템은 네트워크 상에서 동작하는 네트워크 보안 장비이므로, 네트워크상에 설치되었을 때 기존의 네트워크와 맞물려 돌아가야 한다. 따라서, 통합 보안 시스템은 스위치, 라우터에서 제공하는 기본적인 네트워크 기반 기술을 제공해야 한다.

▪ 네트워크 인터페이스 기술

통합 보안 시스템은 일반적으로 이더넷(Ethernet) 기반의 스위치, 라우터와 연결되어 동작하므로 스위치, 라우터와 연관된 Secondary IP, VLAN, Link Aggregation 등의 기본적인 인터페이스 기능을 제공해야 한다.

- Secondary IP: 하나의 물리적 / 논리적 인터페이스에 여러 대역의 IP를 할당 할 수 있어야 한다.
- VLAN(Virtual LAN): VLAN은 이더넷 프레임에 VLAN ID를 삽입하여 가입자 그룹을 가상 랜으로 Grouping 하는 기술로 IEEE에서는 802.1Q로 표준화되었다. 통합 보안 시스템에서는 802.1Q 관련해 VLAN별 제어 및 관련 필터링을 할 수 있어야 한다.
- Link Aggregation: 인터페이스를 이중화하는 기술로, 두 개 이상의 물리적 인터페이스를 하나의 논리적 인터페이스로 묶는 기술이다. Link Aggregation은 단순 인터페이스 대역폭의 확장 개념 및 인터페이스의 이중화뿐만 아니라 네트워크를 이중화시키는데도 적용될 수 있는 기술이다.

▪ 통합 보안 시스템의 동작 모드 및 관련 기술

통합 보안 시스템은 Route(+ NAT), Transparent(or Bridge) 모드로 동작 가능해야 한다.

첫째, Route 모드라 함은 네트워크 세그먼트를 분리하여 통합 보안 시스템이 라우터 장비와 같이 동작하는 것을 말한다. 즉, 라우터의 기본 동작을 포함해야 하며 통합 보안 시스템이 3계층의 라우터 동작을 위해 라우팅 프로토콜을 지원해야 한다. 라우팅 프로토콜에는 정적 라우팅(Static Routing)과 동적 라우팅(Dynamic Routing) 프로토콜로 나눌 수 있다.
다시, 정적 라우팅은 목적지별 라우팅과 출발지별 라우팅으로 나누어 볼 수 있다. 그리고 동적 라우팅 프로토콜은 RIP v1/v2, OSPF, IS-IS 등과 같은 Interior Routing Protocol과 BGP, EGP 등과 같은 Exterior Routing Protocol로 나눌 수 있다.
통합 보안 시스템은 일반적으로 Interior Routing Protocol을 지원되어야 하며, 많이 사용되고 있는 OSPF 와 같은 프로토콜도 지원되어야 한다.

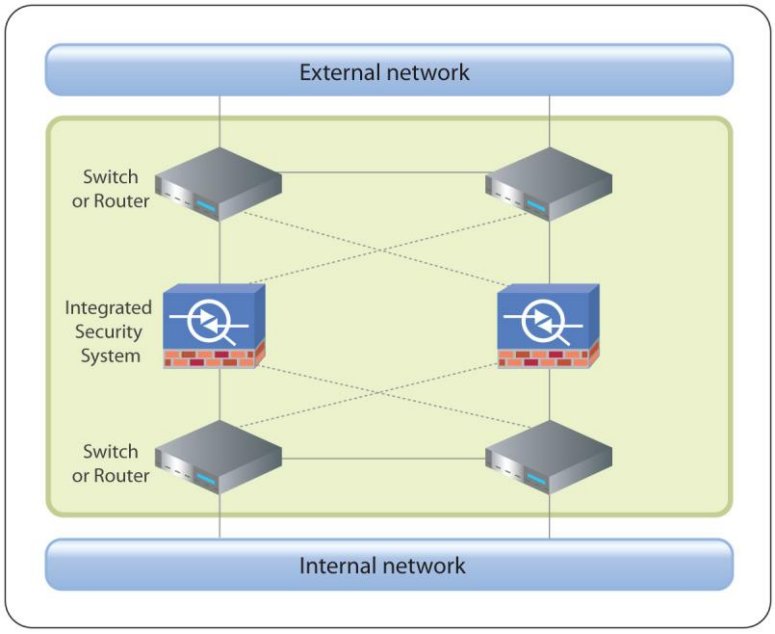
둘째, Transparent 모드는 네트워크 세그먼트를 분리하지 않고 Bridge 장비와 같이 사용하는 것이다. Transparent 모드의 동작 모드 지원은 Route 모드와는 달리 기존 네트워크의 변경 없이 설치가 가능하다는 장점을 가진다.

셋째, NAT 모드는 Network 주소를 변경해 주는 기능을 사용하는 모드로 Route 모드에서 일반적으로 사용되며, Transparent 모드에서도 NAT 기능을 제공할 수 있다.

▪ 이중화 및 망 관리 기술

통합 보안 시스템은 라우터의 이중화 기술로 많이 알려진 VRRP(Virtual Router Redundancy Protocol)라는 프로토콜을 지원해야 한다.
장비 및 네트워크의 이중화는 서비스 및 네트워크의 안정성 측면에서 매우 중요한 요소라 할 수 있다. Router와는 달리 통합 보안 시스템은 패킷 필터링을 수행하기 때문에 관련 필터링을 통과한 패킷의 세션 정보를 이중화된 장비에서 서로 공유하는 기술을 기본적으로 탑재하고 있어야 한쪽 장비 혹은 네트워크에 이상이 생겼을 때 세션의 끊김 없는 서비스가 가능하다.
일반적으로 네트워크에서 구성 가능한 그림 2와 같은 Full-Mesh 형태의 이중화 구성이 가능해야 한다. 대부분의 네트워크 장비들은 SNMP(Simple Network Management Protocol)를 이용하여 망 관리 될 수 있는 기능을 제공하며, 통합 보안 시스템도 SNMP를 이용하여 관리될 수 있는 기능을

제공해야 한다.



[그림 2] Full-Mesh Network 구성도

3. 통합 보안 시스템이 가져야 할 보안 요소 기술

통합 보안 시스템은 네트워크 공격의 차단을 위한 Firewall/IPS, 바이러스/웜/스팸메일/Phishing/유해사이트 차단 등의 유해 콘텐츠 차단을 multi-layer에서 막기 위한 Proxy, DDoS 공격 대응 엔진, 신뢰할 수 없는 구간으로부터의 안전한 연결을 위한 VPN 기능을 보안 요소 기술로 가지고 있어야 한다.

▪ 방화벽 관련 기술

방화벽은 가장 기본적인 네트워크 보안 시스템으로 ACL(Access Control List)-> SPI(Stateful Packet Inspection)-> DPI(Deep Packet Inspection) 방식으로 진화되어 왔다

DPI는 SPI의 한계에서 한 단계 더 나아가 Application Layer 즉, Layer 7인 페이로드 내용까지 검사하는 방식이다.

방화벽에는 기본적인 패킷 필터링 기능 이외에도 NAT(Network Address Translation), QoS(Quality of Service), 시간대별 다른 정책 적용이 가능한 스케줄링 기능이 부가적으로 탑재되어 있다. NAT 기능은 1:1, M:N 등 다양한 IP, Port 주소 변환이 가능하며, QoS는 보안 정책별 혹은 서비스별 트래픽 제한이 가능한 구조를 가지고 있다.

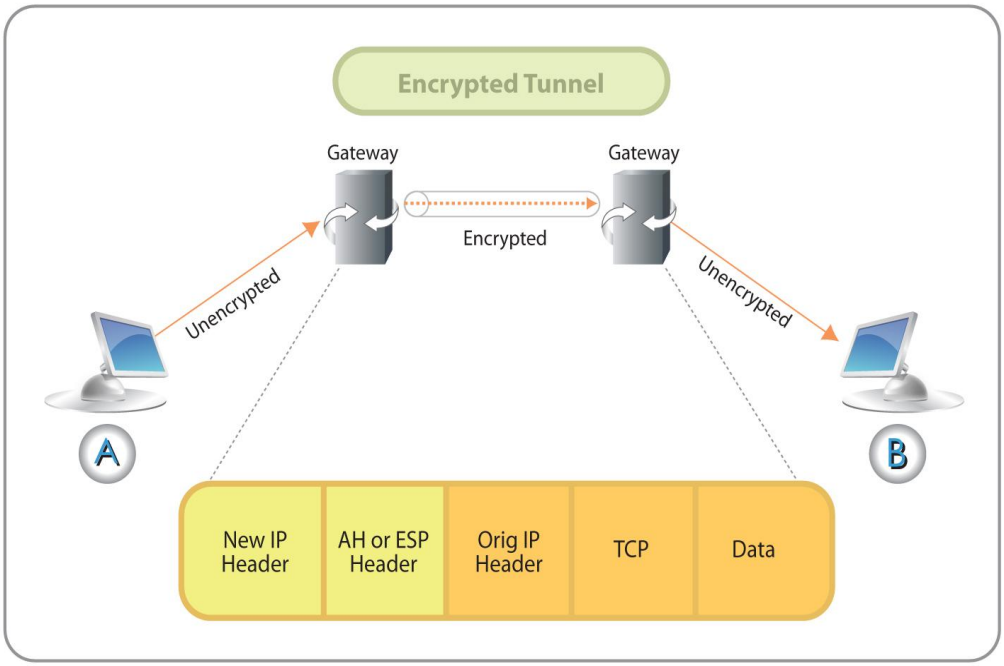
▪ **VPN 관련 기술**

VPN은 Virtual Private Network의 약어로 공중망을 사설망처럼 이용 가능하도록 구현한 기술이다. 터널링을 위한 encapsulation과 암호화 및 인증이 기본적으로 사용되며 전용망 구축 비용 절감 효과와 보안 문제를 동시에 해결 할 수 있다. VPN을 구현할 수 있는 방식은 네트워크 계층에 따라 PPTP/L2TP, L2F, GRE, IPsec, SSL VPN 등으로 나뉘는데, 요 근래에는 IPsec과 SSL VPN이 주로 많이 사용되고 있다.

- IPsec VPN

IPsec은 IP 계층에서 암호화를 수행할 수 있는 방식으로 키 협상을 위한 IKE(Internet Key Exchange), 패킷의 암호화 및 무결성을 위한 ESP(Encapsulating Security Payload)와 AH(Authentication Header) 프로토콜이 있으며, IPsec 동작 방식에 따라 트랜스포트(Transport), 터널(Tunnel) 모드로 나뉜다.

IPsec 통신은 AH, ESP를 활용해 보호하고자 하는 데이터를 암호화 혹은 무결성 점검 기능을 추가해 전달하는 것이라 할 수 있다. 전달하는 방식은 터널 모드와 트랜스포트 모드로 구별할 수 있는데, 원래 패킷에 새로운 IP 헤더를 이용해 캡슐화할지 여부로 구분할 수 있다.
네트워크 장비인 통합 보안 시스템은 게이트웨이 장비이므로 터널 모드를 주로 제공한다.



[그림 3] 터널 모드 IPsec VPN

- SSL VPN

SSL VPN은 SSL(Secure Sockets Layer) 프로토콜을 이용하여 데이터를 암복호화 한다. SSL은 웹 서버와 웹 브라우저간에 안전한 통신을 위해 사용되는 프로토콜로 현재 사용중인 Internet Explorer, Firefox 등 대부분의 웹 브라우저에 채용된 기술이다.

따라서, IPsec VPN과는 달리 별도의 프로그램 설치 및 설치된 프로그램에 대한 별도의 설정이 없이 이용 가능하다는 것이 가장 큰 장점이다. 하지만 별도의 Client S/W 없이 고정되지 않은 외부 PC의 내부 접속을 허용하기 때문에 접속 PC의 보안상태가 중요하다. 이에 SSL VPN을 이용하기 전후에 추가적인 보안 메커니즘을 반드시 결합하여 작동해야만 한다. 예를 들면, SSL VPN 을 연결하기 전에 해당 접속 클라이언트 PC에 대한 해킹 툴 검사, 키보드 스트로크 검사, PC방화벽 수행 등과 같은 사전 보안 점검 메커니즘을 함께 제공할 필요가 있다. 또한 SSL VPN 연결 종료 후에 접속 클라이언트 PC의 Cookie 및 Cache 정보 삭제 등을 통한 보안 메커니즘은 SSL VPN과 더불어 함께 제공되어야만 내부 네트워크를 안전하게 보호하며 VPN 접속 환경을 제공해 줄 수 있다. 이러한 방식은 우리가 인터넷 뱅킹을 할 때 흔히 볼 수 있는 메커니즘으로 강력한 보안 접속 환경을 보장해 준다.

▪ IDS / IPS 관련 기술

IPS(Intrusion Prevention System)는 능동형 보안솔루션으로 인터넷 웜/스파이웨어와 같은 악성코드 및 해킹 등으로 인한 유해트래픽을 차단해 주는 보안 기술이다.

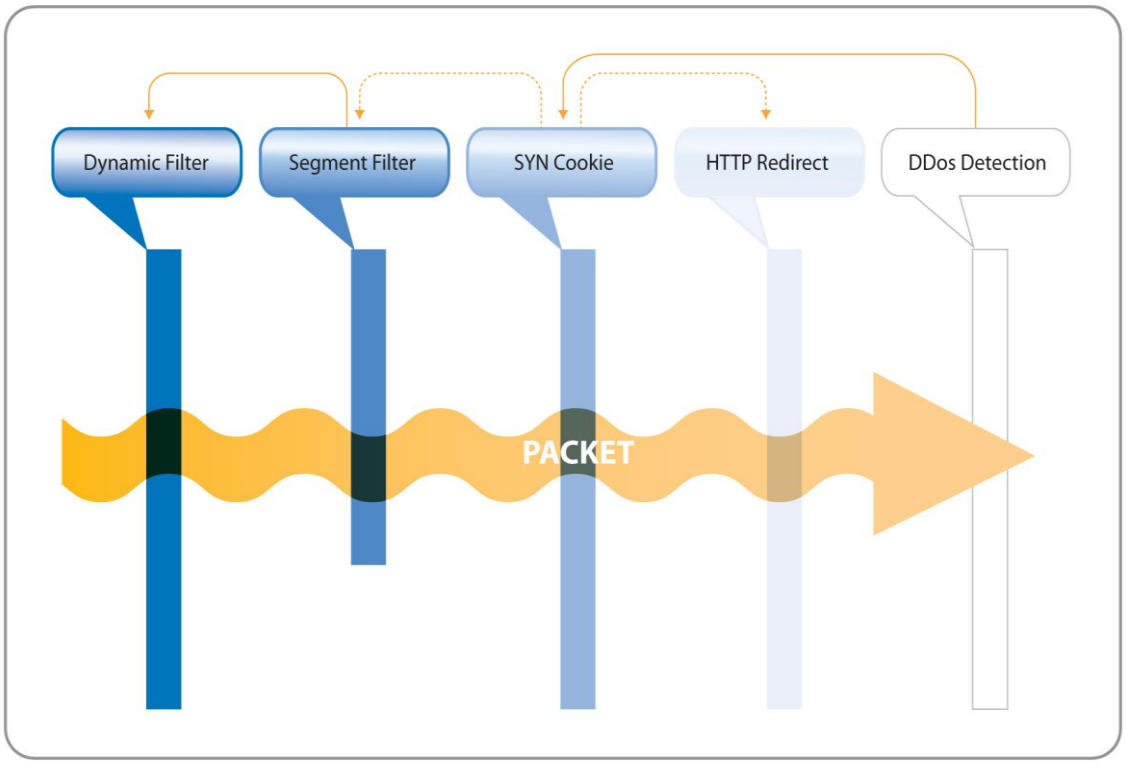
IPS 관련 침입 탐지 기법은 크게 다음과 같이 3가지로 분류할 수 있다.

- Signature 기반의 공격 방어
- Behavior 기반의 공격 방어
- Anomaly 기반의 공격 방어

Signature 기반의 공격 탐지는 패킷의 헤더 및 페이로드의 내용을 보고 탐지하는 기법이다. Behavior 기반의 공격 탐지 기법은 패킷의 행동을 보고 탐지하는 기법으로 flooding 공격을 포함한 D(D)oS, Scan 등이 그 대표적인 예라 할 수 있다.

Anomaly 기반의 공격 탐지는 프로토콜 표준을 따르지 않을 경우 탐지하는 프로토콜 anomaly, 자가 학습(Self Learning)에 의해 학습된 평상시의 네트워크 트래픽 또는 세션의 임계치에 비해 갑작스런 변화가 발생했을 때 탐지하는 Statistical anomaly 등으로 나눌 수 있다.

최근 사회적 이슈가 되고 있는 DDoS 공격 방어 기술은 TCP를 이용한 DDoS 공격인 경우 통합 보안 시스템에서 TCP 프로토콜의 3-way hand shake를 활용한 가상 대리 응답(일명, Syn Cookie)을 이용해 공격 호스트를 판별하는 기법이 기본적으로 사용되고 있다. TCP 이외의 공격일 경우, Statistical anomaly 기법 등을 활용하여 DDoS 공격을 방어하고 있다. DDoS 공격을 방어하는데 있어서 중요한 것은 해당 포트를 단순하게 막는 것이 아니라 DDoS 공격 하에서도 정상적인 사용자는 서비스의 이용이 가능해야 한다는 것이다. 특히, 대부분의 어플리케이션이 사용하는 TCP 프로토콜의 경우 반드시 이러한 메커니즘이 포함되어야 DDoS 공격을 방어한다 할 수 있다.

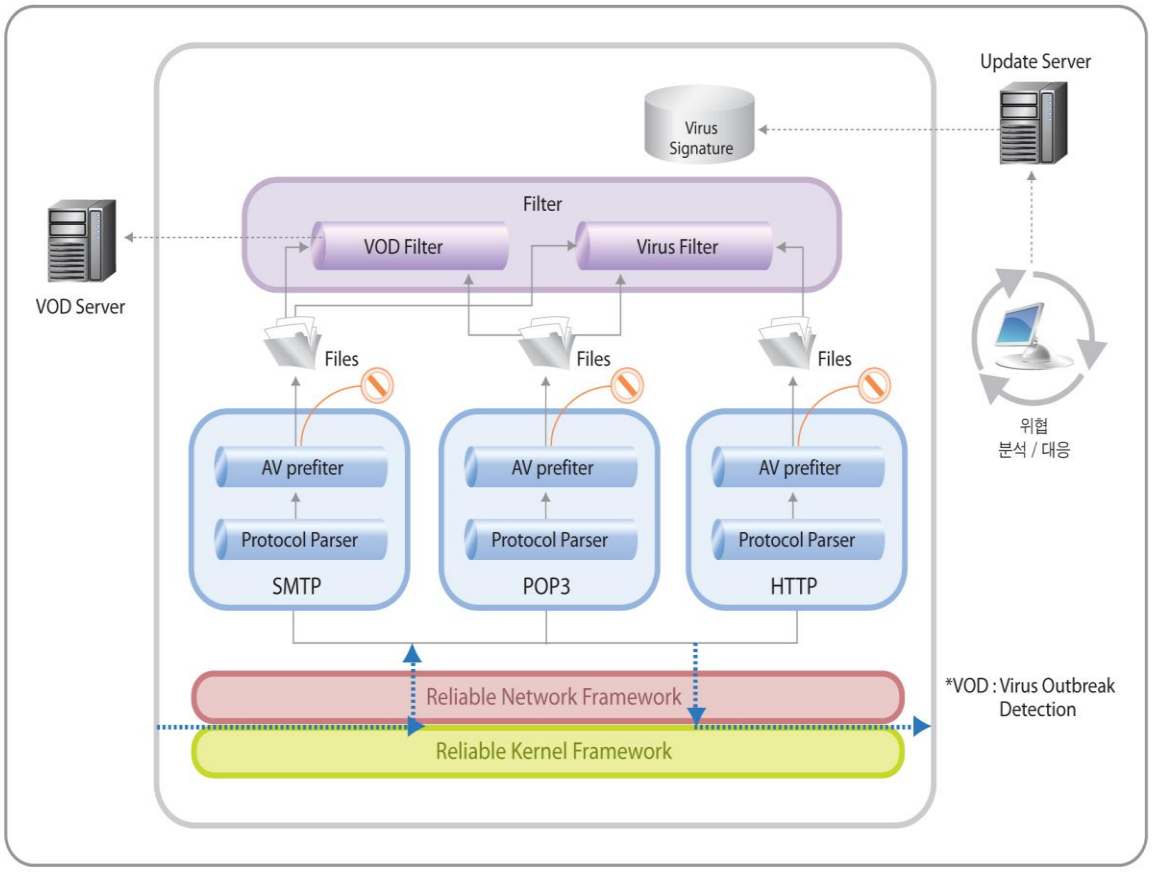


[그림 4] DDoS Filter 엔진 Flow

▪ **Anti-virus/spam, 유해사이트 차단 관련 기술**

- Anti-Virus

Anti-virus의 경우 대부분 파일을 검사해야 하는 관계로 Application layer에서 처리한다. 바이러스를 검사하는 대상 프로토콜은 파일 송수신과 관계된 프로토콜인 SMTP, POP3, IMAP, HTTP, FTP 등이 대표적이다.

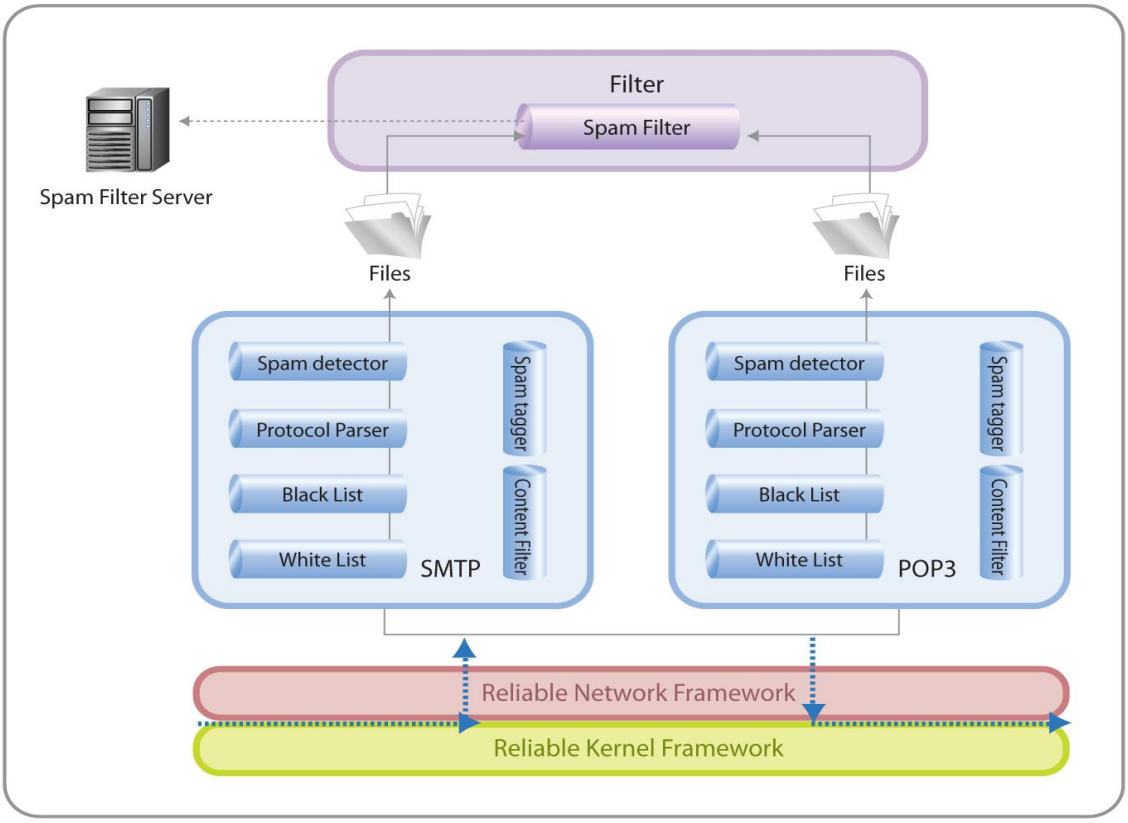


[그림 5] Anti-Virus Filter 구성

- Anti-Spam

스팸 메일은 불특정 다수에게 대량으로 송부되는 원하지 않는 메일로 정의할 수 있다. 최근 들어 스팸의 경우, 단순한 광고 및 홍보를 넘어 바이러스나 기타 악성 코드의 유포 수단으로 활용되고 있다.

이러한 스팸 메일을 차단하는 방식은 초창기 기술인 기본적인 키워드 필터링을 이용하는 방식, Black List에 등록된 메일 서버 domain을 검사해 차단하는 RBL(Real-time Black List) 방식, 통계적 확률 분석 데이터로 스팸여부를 판단하는 베이지언(Bayesian) 알고리즘 분석 방식, 메일의 특정 패턴 분석 데이터로 스팸 여부를 판단하는 휴리스틱 알고리즘 분석 방식, 송신자의 송부 재확인 후 메일을 수신하는 Challenge/Response 방식 등 다양한 기법들이 활용되고 있다.



[그림 6] Anti-Spam Filter 구성

- 유해 사이트 필터링

통합 보안 시스템에서의 유해 사이트 차단 방식은 기본적으로 유해 사이트에 대한 목록을 가지고 있는 유해 정보 Database를 활용하는 방식과 PICS(Platform for Internet Content Selection)라는 규격을 활용해 차단하는 방식이 대표적이다.

▪ **End-Point Security 기술**

- VPN을 통한 End-Point Security 기술

통합 보안 시스템에서 VPN 기술과 End-Point Security 기술의 결합은 매우 중요하다. VPN 기술은 단지 공중망을 사설망처럼 이용할 수 있게 해주는 기술일 뿐 VPN을 사용하는 호스트에 대한 보안을 제공하는 기술은 아니다. 따라서, 우리가 인터넷 뱅킹을 이용할 때와 마찬가지로 VPN을 연결하기 전에 바이러스 검사, 키보드 스트로크 차단, PC 방화벽 수행 등과 같은 사전 보안 점검 메커니즘과 연결 종료 후에 관련 이용 정보를 삭제하는 기능이 결합되어 있어야 한다.

- IAC를 통한 End-Point Security 기술

인터넷 접근 제어 기술 즉, IAC(Internet Access Control)는 보안상 취약한 PC client로부터 네트워크를 보호하고 취약성 PC를 격리하기 위한 메커니즘을 제공한다.

IAC 기능을 통해 개별 PC의 보안성 강화, System/Network 등의 내부 IT Resources의 가용성이 증대되고, Intelligent한 Security 환경을 구축 할 수 있다.

▪ **Web Application Security 기술**

최근 들어 웹 어플리케이션의 취약점을 노린 공격이 증가되고 있다. 웹 서버 차원에서 보안을 강화하고는 있지만 공격 방법이 점점 지능화되어 피해가 증가되고 있는 실정이다.
통합 보안 시스템은 웹 어플리케이션의 취약점 및 접근, 공격에 대한 차단기능을 제공한다.
웹 어플리케이션 공격에는 여러 유형이 있지만 통합 보안 시스템에서는 다음과 같은 차단 기능을 제공한다.

- Command Access 차단: 웹을 통한 설정 파일 및 프로세스 접근 차단.
- Buffer Overflows 차단: 어플리케이션 오류를 통한 서비스 거부 공격 차단, 무결성(integrity) 위반 방지, 기밀성(confidentiality) 파괴 차단
- Cross-Site Scripting 취약점 차단: 공격자가 다른 사용자들에게 악성코드를 설치 차단 (개인정보 유출 차단)
- Injection 차단: 데이터 입력 값에 대한 삽입 차단
- Application 다운로드 및 파일 업로드 차단: HTTP/FTP 프로토콜 등을 통한 취약 데이터의 다운로드 및 업로드 차단

VI. Advantages of Integrated Security

1. Firewall-based Security 외 다양한 보안위협에 효과적으로 대응할 수 있다.

보안의 Basic Infrastructure는 Gateway 단에서 내부/외부로 흐르는 Traffic의 기본적인 통제를 해주는 방화벽이라고 할 수 있다. 방화벽은 정해진 내부 보안정책에 따라 합법적인 접근과 불법적인 접근을 구분하고 불법적인 접근에 대한 효과적인 접근 제어를 목적으로 하고 있다. 하지만 합법적인 접근 내에 숨어 있는 비정상적인 보안위협은 방어할 수 없다는 한계가 존재한다. 이러한 합법적인 Traffic 내에 숨어있는 악성코드나 Network 기반의 공격을 방어하기 위해 나온 솔루션들이 IDPS (Intrusion Detection & Prevention System)/ Anti-Virus / Contents Filtering System (Anti-Spam, 웹 사이트 필터링)/ DDoS 방어 시스템 등이다. 통합 보안 시스템은 방화벽 기반 위에 이러한 Security Features 들이 유기적으로 결합되어 보다 진보된 Network Security를 제공한다.

Worm은 내부 네트워크에 침투하여 자기복제 및 전파를 통해 내부 시스템을 마비시키는 치명적인 악성코드이다. 방화벽 정책에 의해 합법적으로 열린 서비스 port를 통해 들어오는 Worm은 방화벽만으로는 막을 수 없다. 통합 보안 시스템은 IPS 및 Anti-Virus 기능을 통해 방화벽을 통과하여 내부로 들어오는 Worm을 탐지/제거 할 수 있다.

최근에 웹 취약점을 활용하여 내부정보 또는 사용자 계정을 탈취하는 SQL Injection 해킹이 기승을 부리고 있지만 방화벽만으로는 이 공격 역시 막을 수 없다. 통합 보안 시스템은 IPS Signatures에 SQL Injection 공격 기법의 Patterns을 보유하고 있어 효율적인 방어를 제공할 수 있다.

웹 취약점을 이용한 공격 못지않게 공격대상 시스템에 일시에 대용량의 Traffic을 쏟아 부어 시스템 및 network을 마비시키는 (D)DoS 공격도 화두로 떠오르고 있다. 통합 보안 시스템은 IPS

Signature 기반의 (D)DoS 방어 기능에 더하여 별도의 DDoS 방어 엔진을 보유하고 있어 다양한 종류의 DDoS 공격에 효과적으로 대응할 수 있다.

2. Garbage Traffic 제거를 통한 내부 IT 리소스 절감 및 업무효율성 향상을 가져 올 수 있다.

최근에는 방화벽을 우회하는 다양한 비업무용 또는 Garbage Traffic이 기업의 업무 생산성을 저하시키고 있다. 그러한 Traffic을 유발시키는 원인은 악성코드나 Network 기반의 공격 외에도 Spam mail, P2P, Messenger, 증권/도박/성인 Sites 등이 있다. 특히, Spam mail의 경우에는 Spam mail로 인해 정상적인 메일 송수신에 영향을 준다던가 Spam mail을 통한 Virus/ Worm 등의 감염 전파가 비일비재하게 발생하고 있어서 많은 주의가 요구된다.

통합 보안 시스템은 기업내부에서 발생할 수 있는 다양한 Garbage Traffic에 대한 포괄적인 제어환경을 제공한다. IPS/ Ant-Virus를 통한 악성코드 내부 유입방지, Contents Filtering을 통한 Spam Mail 차단 및 유해 사이트 접속 차단 기능을 제공함으로써 내부 IT 자원의 효율적인 활용을 가능케 할 뿐만 아니라 임직원들의 업무생산성 향상에 기여한다.

3. 고가의 Point Solution을 구입할 필요가 없어 구축 및 운용에 있어 비용절감 효과를 가져온다.

방화벽 외 별도의 IPS, Anti-Spam Gateway, Anti-Virus Gateway 등의 솔루션을 도입하려면 엄청난 초기 구축비용이 들 것이다. 초기 비용뿐만 아니라 각 솔루션 별 유지보수 계약을 별도로 체결하고 이에 더하여 별도의 유지보수 비용과 관리 인력을 책정하여 운영해야 하는 매우 비효율적인 상황이 발생할 수 있다. 회사의 보안 정책에 의해 고비용 구조임에도 반드시 Point Solution을 도입해야 하는 기업이 아니라면 통합 보안 시스템으로 강력한 비용절감 효과를 거둘 수 있다.

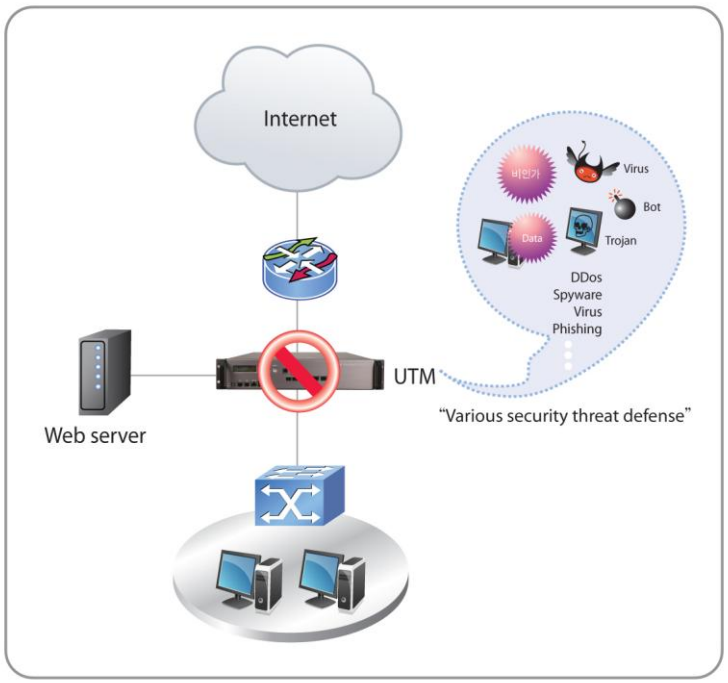
통합 보안 시스템은 License 기반으로 다양한 보안기능을 기업의 입맛에 맞게 사용할 수 있도록 구성되어 있다. 한 대의 장비만 구매하면 되므로 초기 구축비용이 절약되고, S/W License 기반으로 운용되므로 간편한 유지보수가 가능하다. 또한 한 대의 장비로 다양한 기능을 제공할 수 있으므로 여러 대의 Point 솔루션 운영 대비 상당한 전력소비 절감효과를 가져올 수 있다.

4. Network 통합보안 관리가 가능하다.

Point Solution을 도입하여 방화벽/ IPS/ Contents Filtering 등의 통합설정 및 통합로그를 관리하기 위해서는 별도의 ESM(Enterprise Security Management) 솔루션이 필요하다. 그렇지 않다면 기업보안 담당자는 각 개별 솔루션에서 제공되는 Log Server 및 Manager의 사용 방법뿐만 아니라 각 솔루션 별 로그의 유형 및 로그가 의미하는 내용에 대해 모두 숙지하고 있어야 한다. 또한 여러 개의 모니터를 띄어 놓고 각 솔루션에서 발생하고 있는 이벤트에 대한 모니터링을 개별적으로 수행해야 한다. 이에 반해 통합 보안 시스템은 다양한 보안기능에 대한 통합설정과 통합로그 환경을 제공한다. 통합 Manager를 통해 개별 장비의 보안기능 설정뿐만 아니라 다수 장비의 공통 정책 설정기능을 제공한다. 또한 공통 포맷으로 각 보안기능에서 발생한 로그를 보여줄 수 있으며, 개별 보안기능로그 간 연관분석 보고서도 제공한다.

VII. Deployment of Integrated Security

1. 중소규모 기업/기관 보안환경 구성방안

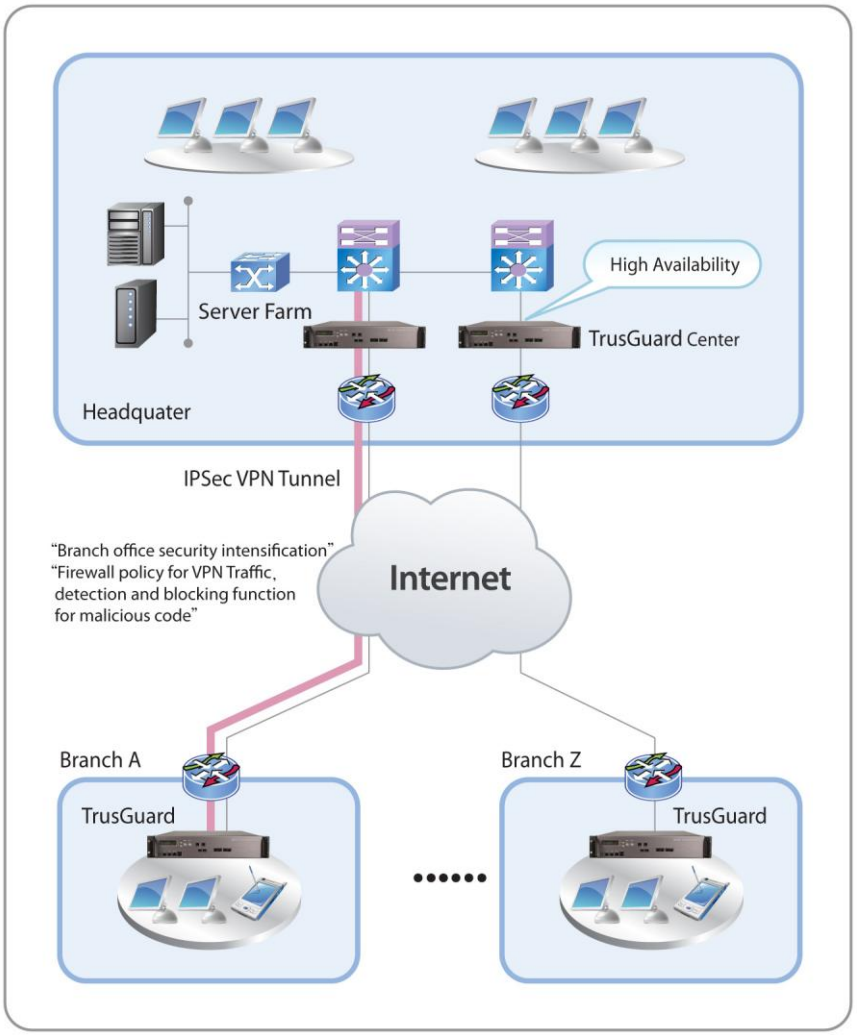


[그림 7] 중소규모 기업에서의 통합 보안 시스템 적용 예

중소규모 기업/기관의 경우에는 대부분 방화벽만으로 보안 환경을 구성하고 있어 다양한 보안위협에 노출되어 있다. 단순 방화벽을 통합 보안 시스템으로 교체함으로써 아래와 같은 강화된 보안 환경을 구축할 수 있다.

1) Stateful 기반의 Packet Filtering으로 불법적인 접근 및 Scanning 공격 차단
2) 방화벽으로 막지 못하는 다양한 악성코드/ Network 기반 공격 차단
3) Web 취약점을 이용한 홈페이지/ 웹 DB 공격에 대한 효과적인 방어
4) 고가의 전용장비 도입 없이도 DDoS 공격에 대한 효과적인 방어
5) Spam 메일, 비업무용 Traffic 제어를 통한 효율적인 Network 환경 구축
6) SSL VPN을 통한 안전하고 유연한 원격접속 환경 제공

2. 본사-지사 보유 기업 VPN 구성방안

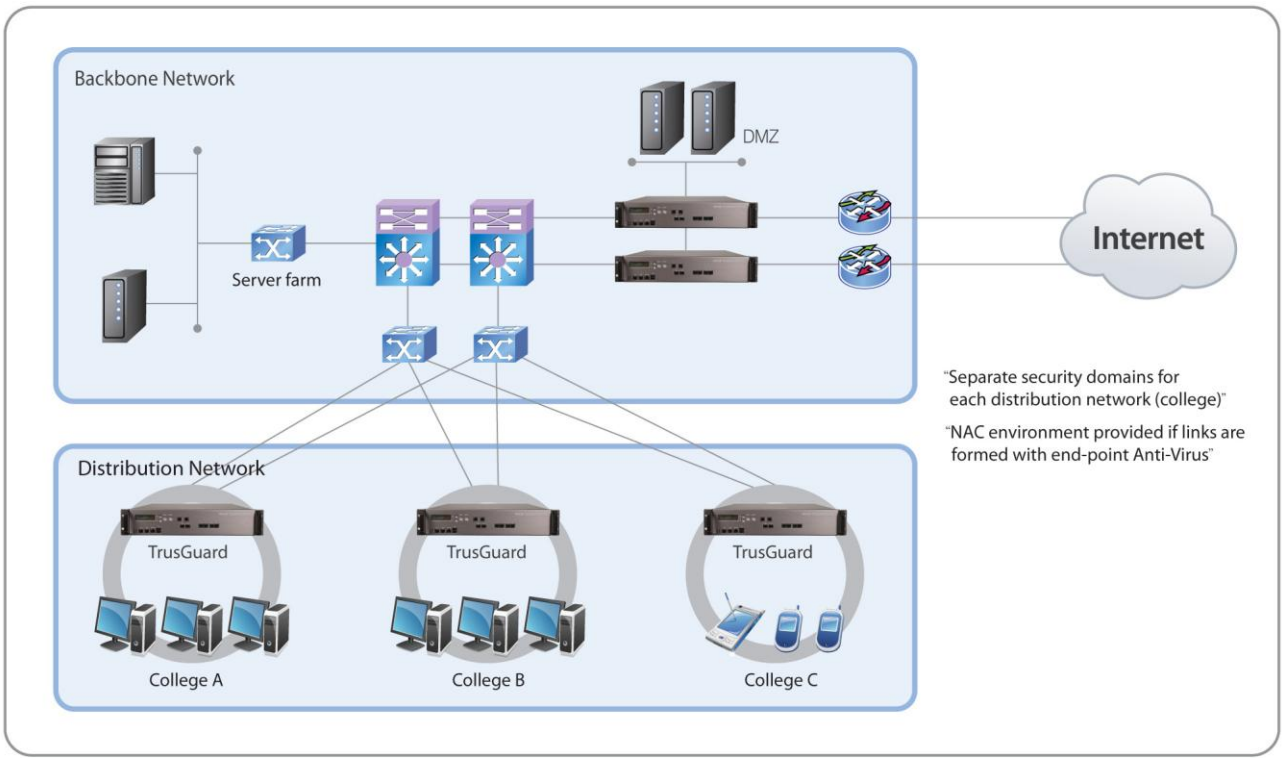


[그림 8] 본사-지사 보유 기업의 VPN 구성 예

본사와 여러 개의 지사를 보유하고 있는 기업/기관의 경우 VPN 전용장비를 사용하여 본-지사 간 안전한 통신채널을 구축한다. 하지만 VPN은 단순 암호화된 통신 방식만을 제공할 뿐 데이터의 악성코드 감염 여부나 불법접근 여부를 판단하지 못한다. 통합 보안 시스템을 이용하여 본-지사 간 VPN Network을 구축하면 아래와 같은 안전한 보안환경을 구축할 수 있다.

1) 본사와 같은 수준의 지사 보안환경 구축: 방화벽, VPN, IPS, Anti-Virus, Contents Filtering 등
2) VPN Tunnel을 통해 흐르는 Traffic으로 인한 악성코드 전파 제어
   - VPN Traffic에 대한 방화벽 정책적용 및 악성코드 탐지•차단 가능
3) High Availability (Active-Active, Active-Standby)구성을 통한 본사 보안장비 이중화 구성
   - Session 동기화 기법 및 L4 스위치 없이 이중화 구성 가능

3. Campus Network 구성방안



[그림 9] Campus Network 구성 예

Backbone Network과 여러 개의 Distribution Network으로 구성되어 있는 대학 Campus (또는 유사한 구성의 기업들)의 경우 인터넷과의 접점에만 Network 보안을 구축하는 것이 일반적이다. 대학 Campus나 이와 유사한 구조/규모의 Network을 운영하는 기업/기관은 인가된 PC 또는 내부 사용자 외에 수많은 비인가 PC 또는 외부 사용자들의 내부 Network 접속이 빈번하게 발생한다. 이로 인해 비인가된 PC로 부터 감염된 악성코드가 전체 Network에 영향을 주기도 한다. 인가된 PC라 하더라도 USB 등을 통해 악성코드에 감염되어 내부 Network에 영향을 주는 위협도 상존하고 있다. 이러한 구조의 Network에 권장되는 통합 보안 시스템의 구축방안은 Distribution Network (단과대학) 단에 통합 보안 시스템을 설치하여 Security Domain을 나누어 주는 것이다. 이러한 구축방식을 통해 아래와 같은 안전한 보안환경을 구축할 수 있다.

1) Distribution Network (단과대학) 개별 Security Domain 구성가능
   - 단과대학 별 상이한 보안정책 적용 (방화벽, IPS, Contents Filtering 등)
2) 단과대학 내부로부터 발생한 악성코드의 전체 Backbone Network으로의 확산 방지
   - Security 위협의 국지화 효과 (단과대학 Network에 한정)
3) PC/서버에 설치된 백신과 연동 시 NAC (Network Access Control) 환경 제공 가능
   - 악성코드 감염 PC의 Network 격리 및 자동치료 수행
   - PC/서버 Security 상태 Check 및 기준 미달 시 Network 접속 차단 및 이슈 해결 유도

VIII. Evolution of Integrated Security System

1. Integrated Security - End-point Security 연동을 통한 통합보안환경 제공에 역점을 두어야 한다.

통합 보안 시스템과 End-point 보안 연동이라 함은 Network 보안 장비와 PC/서버에 설치된 Anti-Virus 백신과의 연동을 통해 상호 부족한 보안 기능을 보완해 주는 것을 의미한다. 예를 들어, PC/ 서버 단의 Anti-Virus 백신 설치 여부와 백신 Signature 업데이트 상태, 그리고 PC/서버의 보안 상태 등을 점검하여 문제가 있는 PC/서버가 네트워크에 접속하려 할 때 통합 보안 시스템에서 접속을 차단하고 문제점을 처리할 수 있도록 유도한다. 또한 통합 보안 시스템에서 먼저 특정 PC에서 발생한 악성코드 등을 감지하면 감염된 PC를 격리하고 PC에 설치되어 있는 백신을 통해 자동치료를 수행하도록 강제하는 방법 등이 있다. 이와 더불어 기업 내 사용하고 있는 인증 서버와의 연동을 통해 네트워크에 접속하려는 PC에 대한 인증제어 기능을 제공한다면 고가의 NAC 솔루션을 도입하지 않더라도 통합보안 관점에서 효율적인 NAC 환경을 구성할 수 있을 것이다.

2. 최근 Network 기반 공격의 주류로 급부상 하고 있는 DDoS 공격에 대한 효과적인 방어기능을 제공되어야 한다.

DDoS 공격은 향후 2~3년 간 Network기반 공격의 주요한 부분을 차지할 것으로 예측된다. 다시 말해 다양한 DDoS 변종 기법들이 나타날 것이며, 그로 인한 피해 또한 적지 않을 것으로 관측된다. 통합 보안 시스템은 방화벽 대체 솔루션으로써 Gateway 단에서 이러한 공격을 효과적으로 차단할 수 있는 방법론을 제공해야 한다. 그러기 위해서는 IPS엔진에 새로 발생하는 공격들의 방어 Signature를 정기적으로 업데이트 하는 것과 마찬가지로 새로 발견되는 DDoS 공격기법에 대한 방어 Pattern도 DDoS 엔진에 정기적으로 업데이트되는 방식의 서비스가 제공되어야 한다. 통합 보안 시스템은 고가의 DDoS 전용장비를 도입할 수 없는 중소규모 기업/기관들에게 DDoS 공격으로부터 IT 자원을 보호할 수 있는 방향으로 진화할 것이다.

3. 중소규모의 기업/ 기관용 솔루션이라는 편견을 넘어서 대규모의 Enterprise, 금융, 공공 시장에 진출할 수 있도록 지속적인 성능 개선 노력이 필요하다.

통합 보안 시스템의 발목을 잡고 있는 이슈 중에 하나가 바로 다양한 보안기능을 한 장비에 사용하기 때문에 성능저하가 발생한다는 선입견이다. 물론 다양한 보안기능을 한 장비에서 구동시키기 때문에 성능저하가 발생할 수 있다. 하지만 하드웨어 기술의 비약적인 발전과 더불어 통합 보안 시스템의 성능에 있어서도 상당한 개선이 이루어지고 있다. 멀티코어 기술의 발전으로 Quad Core를 탑재한 통합 보안 시스템이 등장하고 있고, Packet Filtering 이나 Packet Classification과 같은 성능저하를 가져올 수 있는 Process에 전용 Chip-Set을 사용하여 성능저하를 최소화하는 노력들이 상당 수준 진행되고 있다. 이미 IPS 성능 기준 5G급 통합 보안 시스템이 시장에 나와있는 상태이며, 성능상의 이슈로 인해 Point 솔루션 도입을 선호했던 대형 고객시장에도 곧 통합 보안 시스템의 진입이 이루어 질 것으로 예측된다.

4. 실제 Network에 적용될 수 있는 수준의 IPv6 지원기능이 있어야 한다.

현재 미국/유럽/일본/한국 등 인터넷이 발전한 나라들을 중심으로 IPv6로의 전환논의가 급물살을 타고 있다. 대부분의 공인된 기관의 발표에 따르면 현재 사용중인 IPv4의 사용률이 85%에 다다르

고 있으며, 빠르면 2011년 IPv4 주소의 고갈을 예측하고 있다. 이에 각 국가에서는 정부기관을 중심으로 IPv6로 전환하려는 움직임이 활발하게 진행되고 있으며, 향후 1~2년 안에 IPv4 & IPv6 Dual Stack을 지원하는 보안장비의 도입이 공공기관을 중심으로 급속도로 증가할 것으로 예상된다. 머지 않아 일반 기업 시장에도 동일한 현상이 일어날 것이다. 이에 통합 보안 시스템에서도 단순 기능상의 IPv6 지원이 아니라 실제 망에 적용되었을 때 IPv4의 보안/성능 수준으로 동작할 수 있도록 개발되어야 할 것이다.

IX. Conclusion

IDC 보고서에 따르면 전세계 통합 보안 시스템 시장의 규모는 2010년 2,800백만 달러가 될 것으로 예상하고 있다. 매년 통합 보안 시스템 시장의 성장 폭은 25% 이며, 방화벽/VPN 시장의 2.5배에 이르는 엄청난 시장으로 성장할 것으로 내다보고 있다. 통합 보안 시스템 성장의 발판은 중소규모 기업/기관들의 통합보안 needs에 기인한다. 통합 보안 시스템은 중소규모 기업/기관의 방화벽 교체 수요와 VPN 교체수요를 상당부분 흡수하면서 Market Share를 확장시켜 왔고, 그러한 움직임은 향후에도 지속될 것으로 보인다. 향후 2~3년 통합 보안 시스템 시장의 성장견인은 High-end 급 시장에 얼만큼 성공적으로 진출하느냐에 달려있다고 해도 과언이 아니다. 이미 많은 Vendors들이 High-end 시장에 도전장을 내밀고 있으며, 좋은 성과를 보이고 있는 Vendor도 속속 나타나고 있다. 이러한 성과들은 '통합'이란 명제가 단순히 보안기능의 집합 이상의 가치를 고객에게 제공할 수 있다는 것을 시장에서 증명하고 있다고 볼 수 있다. 또한 그 가치는 향후 상당기간 Network 보안시장을 지배할 핵심개념으로 자리매김 할 것으로 보인다.