The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 18, No. 5, pp.1-8, Oct. 31, 2018. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2018.18.5.1
JIIBC 2018-5-1

네트워크를 위한 보안 시스템의 기술 개발 동향 및 전망

Trend and Prospect of Security System Technology for Network

양경아*, 신동우*, 김종규**, 배병철**

Kyung-Ah Yang*, Dong-Woo Shin*, Jong-Kyu Kim, Byung-Chul Bae****

요 약 최근 사이버 공격은 진보된 기술을 활용하여 방어 기술의 발전 속도보다 빠르게 고도화되고 있어 그 위험수위가 갈수록 높아지고 있다. 이에 대응하기 위해 학계는 물론 산업계에서도 다양한 방법을 적용한 보안 기술을 개발하고 있으며 이를 기반으로 한 보안 시스템들이 적용되고 있다. 본 논문에서는 세대별로 진화하는 공격들을 살펴보고 이에 대응하여 발전하는 네트워크 보안 관련 현황을 소개한다. 특히, 네트워크 보안 시스템 중 최근까지 가장 큰 비중을 차지하고 있는 UTM과 관련하여 상용 제품을 중심으로 해외 및 국내 기술의 동향과 성능 및 기능에 관한 비교 분석을 수행하였다. 또한 차세대 네트워크 기술의 등장으로 인한 네트워크 인프라 변화에 대한 향후 전망에 대해 논의하고자 한다.

Abstract The latest cyber attack utilizing advanced technologies is more rapidly advancing than developing speed of defense technology, thereby escalates the security risk. In responding to this recent threat, academia and industries are developing some sophisticated security technologies applying various methods. Based on these technologies, security systems are used in many fields. This article aims to select noticeable network security related technologies for the security systems. In particular, we compared and analyzed the trend, performance, and functions of both foreign and domestic technologies in regard to UTM having the largest portions among network security systems so far. We will also discuss the prospect for the change in network infrastructure due to the emergence of the next-generation network technology.

Key Words : Network Security System, IPS, Firewall, UTM, NGFW, Threat Protect

Ⅰ. 서 론

최근 인터넷 속도가 빨라짐에 따라, 사물 인터넷(IoT)과 같이 다양한 분야에서 인터넷과 연결되고 있다. 이러한 환경에서 사이버 공격 분야 기술이 빠르게 고도화되는 반면 방어 기술 분야의 대응이 한걸음 늦게 이루어지는 양상을 띠고 있어 사이버 공격의 위협 수위가 갈수록 높아지고 있다.

이에 대응하기 위해 학계는 물론 산업계에서도 다양한 방법을 적용한 보안 기술을 개발하고 있으며 이를 기반으로 한 보안 시스템들이 많은 현장에 적용되고 있다.

정보 보안은 네트워크 보안, 단말 보안 콘텐츠, 정보유출방지, 인증 및 암호 보안 관리로 구분할 수 있다. 그 중 네트워크 보안 시스템은 TCP/IP 프로토콜을 비롯한 각 프로토콜이나 네트워크를 통해 연결된 수많은 호스트들 사이에서 정보의 유출과 불법적인 서비스 이용을 방지하는 기술이다.

네트워크 보안 시스템은 기존에 개별적으로 구축된

*정회원, ETRI 부설 연구소 미래연구센터
**정회원, ETRI 부설 연구소 미래연구센터
접수일자 : 2018년 9월 3일, 수정완료 : 2018년 10월 3일
게재확정일자 : 2018년 10월 5일

Received: 3 September, 2018 / Revised: 3 October, 2018 / Accepted: 5 October, 2018
*Corresponding Author: kayang@nsr.re.kr
Dept: Future Research Center, The Attached Institute of ETRI, South Korea

보안 솔루션들이 통합되는 양상을 보이고 있으며 기존 보안 기능에 점차 보안 인텔리전스를 확보해 나가고 있다.

또한 차세대 보안 기능으로 어플리케이션 인지(cognition), 사용자 인지, 콘텐츠 인지 기능이 제공되고 있으며 이를 통해 복잡하고 다양한 사용자 네트워크 환경에 맞춘 정교한 접근 제어 기능을 제공하고 있다.

본 논문에서는 네트워크 보안 시스템 분야의 주목할 필요가 있는 기술들을 선정하여 현재 동향과 향후 전망에 대해 논의하고자 한다. 네트워크 보안의 중요성을 강조하기 위해 세대별 진화하는 변화 위협과 이에 대응하여 발전하는 네트워크 보안 관련 현황을 살펴보고 각 기술의 동향과 기능을 분석하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 사이버 공격유형 및 네트워크 보안 시스템에 대해 살펴본다. 3장에서는 네트워크 보안 시스템 중 현재 큰 비중을 차지하고 있는UTM(Unified Threat Management)의 동향을 상세히 살펴본다. 마지막으로 조사에 대한 결론 및 향후 보안 연구 방향에 대해 제시한다.

Ⅱ. 네트워크 보안 시스템

1. 사이버 공격 유형

최근 보안 기업인 체크포인트는 새로운 보안 위협의 출현과 발전에 따라 다음과 같이 세대별 사이버 공격을 구분하였다[1].

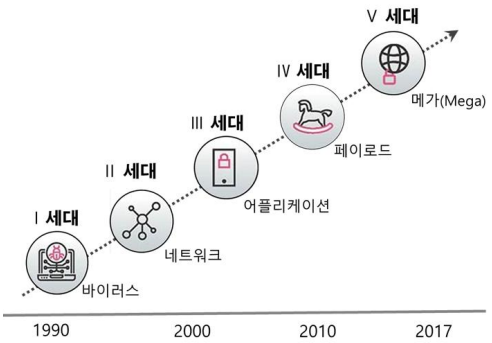

그림 1. 세대별 사이버 위협 특징 (참고: 체크포인트, 2018)
Fig. 1. Generation of Cyber Attack (source: Checkpoint, 2018)

- (1세대) 1980년대 후반
  - 개인용 PC를 대상으로 한 바이러스가 출몰한 시기로 바이러스는 PC 이용자들을 비롯해 기업들을 감염시킴
  - 이동식 플로피 디스크를 이용해 컴퓨터에 복제되는 악성 소프트웨어를 통한 공격 수행
  - 1세대 공격의 영향으로 안티바이러스 소프트웨어 개발

- (2세대) 1990년대 후반
  - 인터넷 온라인 시대가 도래하면서 악성 소프트웨어가 네트워크와 인터넷으로 연결된 컴퓨터 공격
  - 해커들이 www와 웹 사이트를 통해 활동
  - 2세대 공격의 영향으로 방화벽 출현

- (3세대) 2000년대 후반
  - 시스템 보안 정책을 위반하는데 악용될 수 있는 취약점을 활용하여 공격
  - 공격자들은 네트워크와 소프트웨어를 분석하여 특정 취약점을 식별
  - 3세대 공격의 영향으로 IDS(Intrusion Detection System)에서 진보한 IPS(Intrusion Detection System) 출현

- (4세대) 2010년 경
  - 보다 직업적이고 조직화된 단체들이 멀웨어를 통해 특정 목표를 설정하여 타겟팅된 공격을 수행하거나 국제적인 스파이 활동을 하는 형태 출현
  - 공격자들은 고도화된 정교함으로 목표를 특정하여 사전에 설계된 맞춤형 공격을 시도
  - 4세대 공격의 영향으로 안티-봇과 샌드박스 출현

- (5세대) 2017년 경
  - 워너크라이(WannaCry) 공격과 같이 정부 기관이 개발한 고도의 툴이 유출됨
  - 유출된 툴을 응용한 지능형 공격 툴을 사용하여 대규모·멀티벡터(네트워크, 클라우드, 모바일 등)의 메가(Mega) 공격 형태 출현
  - 멀웨어 판매, 봇넷 대여 등과 같이 공격이 상품화 되고 공격자 또는 공격 조직이 산업화되는 경향을 보임
  - 진보된 위협 방지 솔루션 개발

2. 네트워크 보안 시스템 분류

새로운 보안 위협이 출현함에 따라 방어를 위한 보안 제품도 지속적으로 발전해왔다. 네트워크 보안 시스템은 그 기능과 위치에 따라 방화벽(Firewall)과 VPN, IDP(IDS&IPS), 콘텐츠 필터링(Content Filtering), UTM으로 분류할 수 있다[2][3].

- 방화벽(Firewalls)

방화벽은 외부 사용자들이 내부 네트워크에 함부로 접근하지 못하도록 정해진 보안 규칙 집합을 기반으로 트래픽을 허용하거나 차단한다.

방화벽은 동작 방식으로 프록시(Proxy) 방식 방화벽과 스테이트풀 인스펙션(Stateful Inspection) 방식 방화벽으로 구분할 수 있다. 초기 유형인 프록시 방화벽은 특정 어플리케이션을 위해 네트워크 외부에서 직접 연결을 차단하여 콘텐츠 캐싱 및 보안 기능을 제공한다. 스테이트풀 인스펙션 방화벽은 상태, 포트 및 프로토콜에 따라 트래픽을 허용하거나 차단한다. 필터링 결정은 관리자가 정의한 규칙 외에 상황 정보를 기반으로 실행된다.

- VPN(Virtual Private Networks)

VPN은 인터넷과 같은 공중 데이터 통신망을 이용해 마치 개인이 구축한 통신망과 같이 이를 직접 운용할 수 있는 기술이다. VPN 기반 기술로는 크게 키 관리 기술, 터널링 기술이 있다. 통신 속도 및 대역폭 보장이 중요하고 암호화와 인증 기술도 필요하다. VPN은 라우터나 방화벽에 내장되거나 전용 VPN 서버로 구현되기도 한다.

- 침입 탐지 및 차단 시스템(IDS & IPS)

침입 탐지 시스템(IDS)은 기존의 방화벽이 탐지할 수 없는 악의적인 네트워크 트래픽을 탐지하는 시스템이다. 네트워크 기반 IDS는 네트워크 패킷 자료를 침입 판정에 사용하며 오탐이나 미탐 문제가 발생할 수 있다.

침입 탐지 시스템은 침입을 알려주는 시스템으로 침입에 대한 능동적인 기능은 없으나 침입 방지 시스템(IPS)은 외부 네트워크로부터 내부 네트워크로 침입하는 네트워크 패킷을 찾아 능동적으로 공격을 차단함으로써 공격 피해를 최소화하는 특징을 지닌다.

- 콘텐츠 필터링(Content Filtering)

네트워크 기반 기기를 위해 부적절하고, 비생산적인 웹 콘텐츠와 불법적인 악성 웹 콘텐츠를 차단하고 관리하는 기법이다. 웹 필터링, 웹 사이트 또는 페이지 차단, 전자 메일 필터링, 안티-스팸(Anti-Spam)의 기능을 제공한다.

- UTM (Unified Threat Management)

UTM은 단일 서버나 소프트웨어에 기존의 다양한 보안 솔루션들을 하나로 통합한 기술 및 장비를 말한다. 방화벽, IPS, VPN, QoS, Anti-Virus, Content Filtering) 등 다양한 솔루션이 하나의 장비 및 기기에 구축되어 관리가 용이한 장점이 있지만 장애 발생 시 전체 시스템에 영향을 미칠 수 있다.

3. UTM vs NGFW vs NGIPS

이전에는 보안 시스템이 담당하고 있는 보안의 영역 구분이 명확하였으나 모든 보안 기능이 통합되는 현재의 추세로 볼 때 그 경계는 불분명해지고 있다.

차세대 방화벽이라 불리는 NGFW(Next Generation Firewall)는 통합 네트워크 보안 장치로 네트워크 보안 정책 기능을 갖추고 실시간으로 작동한다는 점에서 UTM과 매우 유사하다. NGFW는 UTM 솔루션에 포함된 기술의 일부를 제공하고 있다.

- Unified Threat Management (UTM)

Kaspersky, Gartner 등의 정의에 따르면 UTM은 일반적으로 Firewall, IDS & IPS, VPN(IPSec, SSL), Anti-Virus, Content Filtering, 원격 라우팅, 네트워크 주소 변환(NAT) 등의 기능을 포함할 수 있다[4][5].

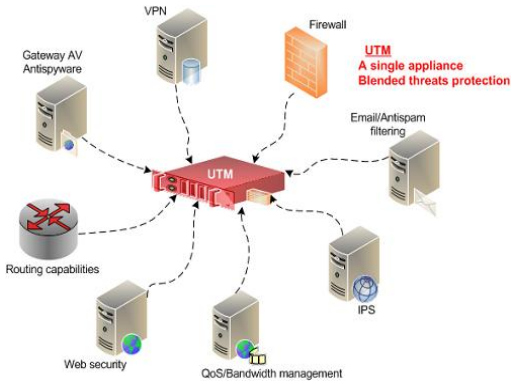

그림 2. UTM의 주요 기능
Fig. 2. Major Features of UTM

- Next Generation FireWall (NGFW)

기존 방화벽은 트래픽의 출발 도메인과 도착 포트를 추적하여 트래픽을 제어하지만, 차세대 방화벽은 포트가 아닌 어플리케이션 ID를 식별하여 트래픽을 분류한다. 또한 IP 주소가 아닌 사용자를 식별하는 기능을 지원한다.

Gartner, Inc.의 정의에 따르면 차세대 방화벽은 일반적으로 다음의 기능을 포함한다[6].

- Firewall(스테이트풀 인스펙션과 같은 표준 방화벽 기능)
- 통합 침입 방지 기능
- Content Filtering(위험한 애플리케이션을 식별하고 차단하기 위한 어플리케이션 인식 및 제어 기능)
- 향후 정보 피드를 포함하기 위한 업그레이드 경로
- 진화하는 보안 위협에 대응하기 위한 기술

- Next Generation IPS (NGIPS)

IPS 기술이 NGFW, UTM 등 다른 보안 시스템과 경쟁하게 되면서 IPS 전문 기업들도 기존 IPS 고유 기능을 강화하면서 APT 등 기능을 다양화하여 네트워크 보안 기능을 제공하며 이를 차세대 IPS라고 정의하고 있다.

Ⅲ. 기술 동향

본 장에서는 통합 보안 시스템 중에서도 현재 네트워크 보안 시스템으로 큰 비중을 차지하고 있는 UTM을 중심으로 시장 동향 조사 및 최신 기술 분석을 수행하도록 한다.

1. 시장 동향

보안 시스템 벤더별 글로벌 시장 점유율을 분석한 결과(2016 Q4 - 2018 Q2 기준) Cisco, PaloAlto Networks, Fortinet, CheckPoint, Symantec 등이 지속적으로 두각을 보이고 있다[7][8][9].

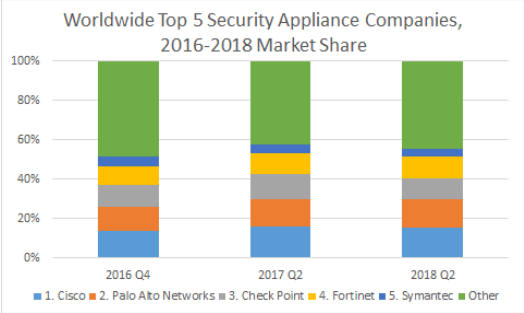

그림 3. 글로벌 상위 5대 벤더 보안시스템 시장 점유율 (2016-2018)

Fig. 3. World Top 5 Security Appliance Companies, 2016-2018

전 세계 보안 시스템 시장은 글로벌 상위 5대 벤더(2018년 2분기, 2017년 2분기 비교) 기준으로 공급 업체의 매출 규모가 전년 대비 17% 증가한 36억 달러를 기록하였다. 다음 표 1은 상위 5개 벤더에 대한 매출 및 성장률을 보인 것이다[10].

표 1. 글로벌 상위 5대 기업 보안 시스템 매출 및 성장률

Table 1. Top 5 Vendors, Worldwide Security Appliance Revenue & Growth (revenue in US$ millions)

Vendor	2Q 2018 Revenue	2Q 2017 Revenue	2Q 18/2Q 17 Growth
1. Cisco	$ 560.5	$ 450.2	24.5 %
2. PaloAlto Networks	$ 521.5	$ 421.9	23.6 %
3. Fortinet	$ 388.3	$ 320.1	21.3 %
4. Check Point	$ 387.9	$ 381.1	1.8 %
5. Symantec	$ 154.3	$ 157.4	-2.0 %
Other	$ 1,601.2	$ 1,356.6	18.0 %
Total	$ 3,613.7	$ 3,087.4	17.0 %

보안 시스템 시장 중 그 하위 시장인 글로벌 UTM 시장은 2017년 대비 16.2% 증가하였으며 네트워크 보안 시스템 시장을 지속적으로 주도하고 있는 것으로 나타났다. 반면 IPSec VPN과 SSL VPN 시장은 전년 대비 매출이 감소한 것으로 나타났다. 공격 대비를 위해 특정 목적의 전용 보안 솔루션보다 통합된 보안 솔루션에 대한 요구가 커지면서 나타난 현상으로 해석할 수 있다.

향후에도 UTM은 기존 UTM에 새로운 기능을 추가함으로써 네트워크 보안 시스템 시장을 주도해갈 것으로 예상된다.

한편 참고문헌[11]에 따르면 국내 보안 시스템 시장은 5년간(2016-2020) 연평균 3.2% 성장해 2019년 5,000억 원을 넘어서고 2020년 5,300억 원 규모에 이를 전망이다.

기존의 방화벽, 혹은 IDS/IPS에 대한 수요가 어플리케이션 계층까지 확대돼 통합 보안을 지원하는 NGFW를 포함한 UTM 시장으로 대체되는 것으로 조사되었다.

2. 국내・외 기술 개발 동향

현재 네트워크 보안 시장을 주도하는 UTM은 국내·외 다양한 제품들이 개발되고 있다. 이 절에서는 해외 및 국내 UTM의 기술 개발 동향들을 살펴보고 대표적인 모델들을 대상으로 기능 및 특징들을 비교·분석하고자 한다.

- 해외 UTM 기술 개발 동향

참고문헌[12]에 따르면 UTM 기술을 이끄는 Leaders와 Challengers 그룹으로 각각 Fortinet, Checkpoint, Sophos와 Cisco, SonicWall 등이 선정되었다. 5개 벤더들의 UTM 기능을 살펴본다.

다음 표 2에서는 5개 벤더들의 대표 UTM 제품들, Fortinet FortiGate Series[13], Checkpoint 3200 Security Gateway[14], Sophos SG Series[15], Cisco ASA Firepower 2100, 4100 Series[16], SonicWall Network Security appliance NSa) series[17] 등 5개를 선정하여 성능 및 기능을 비교정리 하였다.

UTM 제품들은 Small business부터 Enterprise 급까지 벤더 별 다양한 모델들이 출시되었다. 비교 제품들은 대부분 Branch & Small Office 급부터 DataCenter 급에 사용되는 제품들이다.

각 UTM 제품들이 지원하는 성능과 기능은 온라인을 통해 제공되는 각 벤더별 datasheet을 참고하였으며 조사 가능한 명시된 성능을 표기하였다. 명시되지 않은 자료는 △로 표기하였다.

다음 표 3은 해당 5가지 제품에 대한 기능 비교를 수행하였다. 기능 구분을 위한 특징으로 Firewall, Application, VPN, IPS, Contents Filtering, Anti-Virus, Anti-Spam 등을 선정하여 비교하였다.

표. 2. 해외 UTM 성능 비교
Table 2. Comparing the global UTM performance in the industry

(단위: bps)
(△: not specified)

Product		Fortinet[13]	Check Point[14]	Sophos[15]	Cisco[16]	Sonic wall[17]
Firewall Throughput		7.4G ~ 36G	4G ~ 128G	2.5G ~ 65G	3G ~ 75G	3G ~ 17.1G
IPS Throughput		1.9G ~ 11G	1.1G ~ 30G	350M ~ 16G	△	1.4G ~ 10.3G
VPN Throughput	SSL	250M ~5G	1.7G ~ 26G	300M ~ 10G	500M ~ 15G	1.3G ~ 10G
	IPSec	4G ~ 20G				
Threat Protect Throughput		250M ~4.7G	425M ~ 22.7G	380M ~ 5G	△	1.25G ~ 9.4G
Application Ctl Throughput		1G ~ 14G	△	△	△	1.4G ~ 11.5G

표. 3. 해외 UTM 기능 비교
Table 3. Comparing the global UTM features in the industry

Product	Fortinet[13]	Check Point[14]	Sophos[15]	Cisco[16]	Sonic wall[17]
Firewall	○	○	○	○	○
Application Control	○	○	○	○	○
IPSec VPN	○	○	○	○	○
SSL VPN	○	-	○	-	○
IPS	○	○	○	○	○
Contents Filtering	○	○	○	○	○
Anti-Virus/Malware	○	○	○	○	○
Anti-Spam	○	○	○	○	○
NGIPS	-	-	-	○	-

대부분의 UTM 어플라이언스는 방화벽, VPN 및 침입 방지 시스템을 갖추고 있으며 응용 프로그램 제어, 콘텐츠 필터링, 멀웨어 및 스팸 방지 기능을 지원한다. 또한 벤더별로 네트워크 또는 클라우드 기반 중앙 집중식 관리 기능을 지원하는 것을 살펴볼 수 있었다.

- 국내 UTM 기술 개발 동향

국내 상용 UTM 기술 분석을 위해 안랩, 시큐아이, 넥스지, 윈스 등 4개 벤더 등을 선정하였다.

다음 표 4에서는 4개 벤더들의 대표 UTM 제품들 중 안랩 Ahnlab TrusGuard Series[18], 시큐아이 SECUI MF2 Series[19], 넥스지 NexG VForce UTM Series[20], 윈

스 Sniper UTM/FW Series[21] 등 4개를 선정하여 성능을 비교·분석하였다.

표. 4. 국내 UTM 성능 비교
Table 4. Comparing the domestic UTM performance in the industry

(단위 : bps)
(△: not specified)

Product	Ahnlab[18]	SECUI[19]	NexG[20]	Wins[21]
Firewall Throughput	1.5G ~ 100G	300M ~ 40G	2G ~ 40G	2G ~ 50G
IPS Throughput	1G ~ 20G	△	△	△
VPN Throughput	600M ~12G	300M 5.5G	1.5G ~ 30G	△

표. 5. 국내 UTM 기능 비교
Table 5. Comparing the domestic UTM features in the industry

Product	Ahnlab[18]	SECUI[19]	NexG[20]	Wins[21]
Firewall	○	○	○	○
Application Control	○	○	○	○
IPSec VPN	○	○	○	○
SSL VPN	○	○	-	-
IPS	○	○	○	○
Contents Filtering	○	○	○	○
Anti-Virus/Malware	○	○	○	○
Anti-Spam	○	○	-	○
DLP	○	○	-	-
Anti-DDoS	○	○	○	○
Cloud based prevention	○	-	-	-

표 5를 살펴보았을 때, 국내 제품들은 해외 UTM 어플라이언스와 마찬가지로 방화벽, VPN 및 침입 방지 시스템을 갖추고 있으며 응용 프로그램 제어, 콘텐츠 필터링, 멀웨어 및 스팸 방지 기능을 지원한다. 특히 DDoS 공격에 대한 방어 능력을 강조하고 있으나 클라우드 서비스를 위한 가상 방화벽 서비스는 능동적으로 대처하지 못하는 것으로 조사되었다.

Ⅳ. 향후 전망 및 결론

본 논문에서는 세대별로 진화하는 공격에 대응하여 발전하는 네트워크 보안 관련 현황을 살펴보고 각 기술의 동향과 기능을 분석하였다. 특히, 네트워크 보안 시스템중 최근까지 가장 큰 비중을 차지하고 있는 UTM과 관련하여 해외 및 국내 기술의 동향에 대해 살펴보았다.

네트워크 보안은 향후 사물인터넷(IoT)을 통해 사물들이 상호 정보를 교환하면서 다양한 보안 이슈가 발생할 것으로 전망된다. 과거 네트워크 등의 인프라 중심이었으나 플랫폼 시스템 통합 응용 서비스 등 서비스 중심으로 시장이 확대되면서 보안 취약점도 다양한 영역에 걸쳐 복잡화되고 고도화될 것으로 예상된다.

현재 네트워크 보안 시스템 시장은 다수의 업체가 참여하는 경쟁체제로 되어 있고 기본적으로 통합된 보안 어플라이언스 형태로 지원되고 있어 SW 솔루션 대비 초기 투자 비용이 많이 소요된다.

한편 SDN(Software-Defined Networking), NFV (Network Functions Virtualization) 기술의 발전으로 HW가 아닌 SW 기반 네트워크로 인프라 변경되고 있는 추세이다.

이런 상황들을 고려하여 볼 때 SDN/Cloud/IoT 환경에 맞춰 SW 기반 네트워크 인프라로 변경이 요구될 경우 보안 시스템 역시 패러다임 변화가 뒤따를 것으로 보인다. 향후 네트워크 인프라 변화에 대비하여 네트워크 보안 시스템의 기술적 대응책을 마련할 필요가 있다.

References

[1] Checkpoint, “Achieving Fifth Generation Cyber Security, A Survey Research Report of IT and Security Professionals”, Mar 2018.

[2] Hee-Jae Park, Yu-Na Kim, Jong Kim, “Network Security Appliance”, The Korean Institute of Information Scientists and Engineers, Vol 19, No. 2, pp. 48-58, Dec 2005.

[3] IDC, “Asia/Pacific Quarterly Security Appliance Tracker”,https://www.idc.com/tracker/showproductinfo.jsp?prod_id=109

[4] Kaspersky, https://www.kaspersky.com/resource-

center/definitions/utm
[5] Gartner, https://www.gartner.com/it-glossary/unified-threat-management-utm
[6] Gartner, https://www.gartner.com/it-glossary/next-generation-firewalls-ngfws
[7] IDC, "UTM and Firewall Growth Drive the Worldwide Security Appliance Market Expansion in 2016, According to IDC", Mar 2016.
[8] IDC, "UTM and Firewall Growth Drive the Worldwide Security Appliance Market Expansion in Q2 2017, According to IDC", Sep 2017.
[9] IDC, "UTM and Firewall Growth Drive the Worldwide Security Appliance Market Expansion in Q2 2018, According to IDC", Sep 2018.
[10] IDC, "Top 5 Vendors, Worldwide Security Appliance Revenue & Growth", Jun 2018.
[11] Mun-Su Choi, Min-Cheol Kim, "Korea IT Security Products Forecast, 2016 - 2020", IDC Report, 2016.
[12] Gartner, "Magic Quadrant for Unified Threat Management", Jun 2017.
[13] Fortinet, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Product_Matrix.pdf
[14] CheckPoint 3200 Security Gateway, https://www.checkpoint.com/downloads/product-related/datasheets/ds-3200-appliance.pdf
[15] Sophos SG Series, https://www.sophos.com/en-us/medialibrary/pdfs/factsheets/sophos-sg-series-appliances-brna.pdf
[16] Cisco ASA Firepower 2100, 4100 Series, https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw/datasheet-c78-736661.html
[17] SonicWall Network Security appliance NSa) series, https://www.sonicwall.com/SonicWall.com/files/17/177b1c66-ae9f-4448-9ebf-c829e1acf3bf.pdf
[18] Ahlab, Ahnlab TrustGuard Series, https://www.ahnlab.com/kr/site/product/productView.do?prodSeq=10
[19] SECUI, SECUI MF2, https://www.secui.com/product/mf2
[20] NexG, NexG VForce UTM Series, https://www.nexg.net/products/network-security/vforce-utm/#tab-3
[21] Wins, Wins Sniper UTM/FW Series, http://www.wins21.co.kr/product/product_030101.html?num=14
[22] Hoyoung Hwang, Seung-Cheon Kim, "Design and Implementation of Unified Network Security System support for Traffic", International Journal of Internet, Broadcasting and Communication, Vol. 11, No. 6, pp.267-273, Dec 2011.
[23] Kyung-Shin Kim, "Security Analysis and Improvement of Integrated Security Management System", International Journal of Internet, Broadcasting and Communication, Vol. 15, No. 1, pp.15-23, Feb 2015.
DOI: 10.7236/JIIBC.2015.15.1.15
[24] Dae-Cheol Shin, Hong-Yoon Kim, "Implementation of abnormal behavior detection Algorithm and Optimizing the performance of Algorithm", Journal of the Korea Academia-Industrial cooperation Society, Vol. 11, No. 11, pp. 4553-4562, 2010.
DOI: 10.5762/KAIS.2010.11.11.4553
[25] Hyun-Seok Kim, Dong-Gue Park, "Implementation of Abnormal Behavior Detection System based Packet Analysis for Industrial Control System Security", Journal of the Korea Academia-Industrial cooperation Society, Vol. 19, No. 4, pp. 47-56, Apr 2018.

저자 소개

양 경 아(정회원)

• 2003년 2월 : 전북대학교 컴퓨터정보학과 석사
• 2008년 8월 : 전북대학교 컴퓨터통계정보학과 박사
• 2008년 ~ 2009년 : 케이테크 연구원
• 2009년 ~ 2014년 : ETRI 선임연구원
• 2014년 ~ 현재 : ETRI 부설연구소 선임연구원
<주관심분야 : 빅데이터, 기계학습, 네트워크 보안>

신 동 우(정회원)

• 2015년 2월 : 한국과학기술원 전기및전자공학과 석사
• 2015년 ~ 현재 : ETRI 부설연구소 연구원
<주관심분야 : 네트워크 보안, 병렬 처리, 정보보호>

김 종 규(정회원)

• 1997년 2월 : 경북대학교 전자공학과 석사
• 2002년 8월 : 경북대학교 전자공학과 박사
• 2012년 ~ 2013년 : Univ. of Florida 방문학자
• 2002년 ~ 현재 : ETRI 부설연구소 책임연구원
<주관심분야 : 전자공학, 통신공학, 안테나, 정보보호>

배 병 철(정회원)

• 1996년 2월 : 홍익대학교 전자계산학과 석사
• 2007년 3월 : 충남대학교 대학원 컴퓨터공학과 박사수료
• 1996년 ~ 1999년 : 국방정보체계연구소 연구원
• 1999년 ~ 2000년 : 국방과학연구소 연구원
• 2000년 ~ 현재 : ETRI 부설연구소 책임연구원
<주관심분야 : 정보보호, 사이버 보안관제, 네트워크 및 분산 시스템 보안>