

Industry Trend Report

#NAC

네트워크 접근 제어(Network Access Control)

Definition

정의

네트워크 접근 제어(이하 NAC)는 네트워크에 접속하려는 단말의 보안정책 준수 여부를 검사하여 인가를 받지 않았거나 악성코드에 감염되는 등 보안정책을 미 준수 또는 위배된 단말의 네트워크 접속을 차단하여 시스템 및 네트워크를 보호하는 형태로 보안성을 강제할 수 있는 보안 인프라이다[1]. 보안성 확보를 위한 이러한 기능은 접속 전(Pre-Connect) 과 접속 후(Post-Connect)로 나누어 설명될 수 있다. 접속 전 보안 기능은 단말이 네트워크에 연결되고 정상적인 통신이 설정되기 전에 수행되는 작업을 의미한다. 이 때 단말은 이름 / 암호 / 인증서 / MAC 주소와 같은 ID 정보를 사용하여 식별되고 인증된다. 미 인증 시 네트워크 연결은 거부된다. 접속 후 보안 기능은 인증 이후에 단말의 상태변화를 지속적으로 추적하는 단계다. 상태변화가 감지되면 그에 적합한 보안정책이 할당되어 자동으로 제어된다. 이러한 프로세스는 단말이 네트워크에 분리될 때까지 지속적으로 유지된다. NAC 시스템은 정보보호 시스템으로 고유의 보안 기능과 안정성을 보충하기 위해서 높은 수준의 인증을 요구하고 있으며 CC(Common Criteria, ISO/IEC 15408)라는 국제 공통 평가 기준에 따라 작성된 보호 프로파일에 따라 제품을 개발하여 평가 받게 된다[2].

Market Status

시장상황

2019년 국가정보보호백서에 따르면 정보보안 제품 분야가 전체의 71.8%, 정보보호 서비스 분야가 나머지 28.2%를 차지하고 있다(기업 수 기준). 이 중에서 정보보안 제품으로 네트워크 보안시스템, 시스템보안 솔루션, 정보유출방지시스템, 암호/인증시스템, 보안관리시스템으로 분류하고 있으며, NAC 시스템은 네트워크 보안시스템에 속하는 제품이다[5].

IT 전문 시장조사 기관인 가트너와 프로스탠셜리번 보고서에 따르면, 글로벌 NAC 시장은 성숙 단계에 접어들었다. 하지만 여전히 IoT(Internet of Things security), ZTNA(zero trust network access) 등의 IT 환경의 변화와 코로나19로 인한 비대면 언택트 환경에서의 보안과 관련하여 수요의 지속적인 증가세를 보이고 있는 시장이다. 또한 급변하는 보안위협에 대한 모니터링과 네트워크의 가시성(network visibility)을 개선하기 위해 다른 보안 솔루션과의 통합이 주요 이슈로 등장하고 있다[3, 4, 6].

IoT 환경에서는 보다 많은 단말들이 다양한 통신방법으로 네트워킹에 참여하게 되며, 상호간의 데이터 교환을 통하여 새로운 가치를 창출할 수 있게 된다. 하지만 다양한 기기종 단말 간의 유·무선 통신으로 사내 네트워크에서 발생할 수 있는 다각적인 보안 위협을 내포하고 있다[7, 8]. 사내 네트워크의 영역은 더 넓어지고 복잡해지고 있다.

기업 네트워크는 더 이상 데스크톱과 스마트폰 뿐만 아니라 업무용 패드, 바코드스캐너, AP, Video Surveillance(IPTV 등), 디지털 도어, 방범 장치, 기타 IoT 장비 등 빠르게 증가하고 있으며, 이에 따라 보안위협 역시 증가하고 있다.

또한 코로나19로 촉발된 재택 및 원격근무 환경은 물리적인 업무환경의 확대를 통한 가시성의 저하와 공격표면(attack surface)의 확대를 증가시키고 있다. 이러한 환경에서 사용자 및 단말의 가시성을 확보하고 인증, 통합관리 등을 통한 공격표면의 감소를 위해 성숙기 시장에서의 NAC가 재 조명 받고 있다.

Main Driver

주요 동인

1. IoT 시대의 네트워크 가시성(Visibility) 확보

최근 사물인터넷 환경은 다양한 산업 분야로 관련 기술 및 응용 범위가 확대되면서 빠른 속도로 진화하고 있다. 컴퓨터, 스마트폰, 태블릿 PC를 비롯하여 IoT 기기들의 연결은 불과 몇 년 사이에 큰 폭으로 증가되고 있다. 단말 증가에 따른 관리의 어려움과 동시에 관리되지 않은 단말의 잠재적인 보안위협 역시 크게 증가하고 있다. 이러한 상황에서 기업의 보안위협은 다양한 공격 대상과 유형으로 나타나고 있어, 기업 네트워크의 단말의 가시성 확보가 보안의 중요한 측면으로 강조되고 있다.

2. 언택트 시대의 기업 네트워크 보안

NAC는 언택트 환경에서 각광을 받고 있다. 원격 및 재택근무는 보안 수준 강화가 필수적이며, 결국 사람과 네트워크에 접속하는 단말에 대한 보안이 중요하기 때문이다. NAC를 통해 접근을 통제하고 패치와 필수 소프트웨어의 운영 등을 강제화하여 강력한 보안정책을 유지할 수 있다.

기업은 BYOD 정책을 통해 업무효율을 높이고 비용을 절감하는 등 경제성, 개방성 및 다양성 측면에서 장점을 획득하였다. 하지만 사내 네트워크에 다양한 단말을 통한 보안위협 발생 가능성이 커진다. BYOD는 직원들의 업무효율성을 높여주었지만, 현재 기업 네트워크에 중대한 보안위협 요소로 작용하고 있으며, 이를 식별하여 조치하는 것이 중요하다.

Key Player & Product

주요 경쟁사 및 제품

국내 NAC 시장은 지니언스가 M/S 1위로 10년 이상 시장을 주도하고 있다. 아래는 국내 매출액 기준 주요 경쟁사 현황이다.

[표 1] 주요 경쟁사 현황

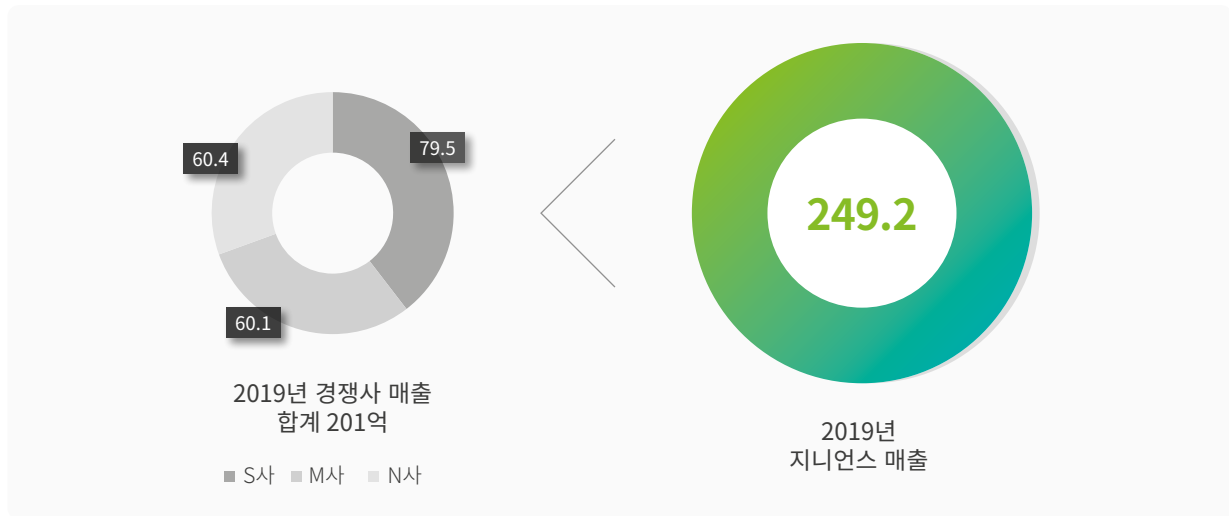
(단위: 백만원)

구분	설립일	솔루션	매출액 (2019년)	영업이익 (2019년)	당기순이익 (2019년)	주요판매처(%)
지니언스	2005.01	지니안 NAC	24,875	3,172	3,214	론스텍(28), 대신정보통신(18), 한국도로공사(4)
S사	1999.06	아**** NAC	7,947	-1,011	-1,160	에스넷시스템(17), 에스앤디정보(12), 유비콤(10)
N사	2005.05	S**** NAC	6,135	843	764	엘림넷(9), 현대오토에버(6), 제이제이에스티(5)
M사	1995.05	티*** NAC	6,008	87	31	시큐어스(12), 농협중앙회(10), 롯데렌탈(10)

*CRETOP 자료 기준(조회 일시: 2020.10.14)

[그림 1] 주요 경쟁사 2019년 매출 비교

(단위: 억)



[표 2] 주요 경쟁사 5년간 손익계산서 요약

(단위: 백만원)

구분		지니언스	S사	N사	M사
매출액	2019년	24,875	7,947	6,135	6,008
	2018년	21,348	7,771	5,848	5,702
	2017년	20,812	7,359	6,031	5,503
	2016년	20,615	5,748	6,268	5,218
	2015년	15,473	5,113	5,453	6,766
영업이익	2019년	3,172	-1,011	843	87
	2018년	3,325	581	29	239
	2017년	4,621	617	346	186
	2016년	4,208	62	331	247
	2015년	3,553	-1,290	404	692
당기순이익	2019년	3,214	-1,160	764	31
	2018년	3,593	559	130	98
	2017년	4,288	497	302	73
	2016년	3,658	120	307	68
	2015년	2,972	-818	475	564

1. S사

S사는 트래픽 관리 및 네트워크 관리를 기반으로 IP자원관리솔루션(IPAM)과 NAC 등 네트워크 정보 관리 솔루션을 제공하고 있는 기업이다. 네트워크 정보 관리 및 보안 전문 SW 시장의 플레이어로, 지난 10여년 간 지속적인 해외시장 개척에 집중해 노르웨이, 일본, 미국, 중국, 태국, 대만 등 전세계 20개국 1천여 고객사를 확보하였고, 2018년 기준으로 누적수출액 2,500만달러를 기록하고 있다.

아**** NAC는 보호하고자 하는 조직 내부의 네트워크에 설치되어, 조직이 운영하는 내부 네트워크로 접근하는 사용자를 사전 인증 과정을 통해 차단 또는 통제한다. 내부 네트워크를 안전하게 보호하는 NAC 제품으로 네트워크 접근제어·자산관리·유기적 연동시스템을 제공하는 통합 관리 시스템이다.

2. N사

N사는 네트워크 보안 및 관리 솔루션을 개발·공급하여 네트워크의 안전성과 가용성을 확보하는데 중점을 두고 있다. 차세대 네트워크 접근 제어(NAC)를 포함한 IP 주소 관리(IPAM), 트래픽 분석 및 엔드포인트 취약점 점검 제품을 공급하여 금융, 기업, 공공, 국방 등 다양한 고객사를 보유하고 있다.

S**** NAC은 네트워크 진입 시 단말과 사용자를 인증하고, 네트워크를 사용중인 단말에 대한 지속적인 보안 취약점 점검과 통제를 통해 내부 시스템을 보호하는 NAC 솔루션이다. 검증된 IPv4, IPv6 주소 및 네트워크 관리(IPAM) 기술을 적용한 유무선 네트워크를 모두 지원한다.

3. M사

M사는 휴대폰·PC 등 다양한 통신단말들을 시스템에 연결하는 엔드포인트(Endpoint)분야를 주력으로 하며, 네트워크 접근 제어(NAC) 기업이다. 2018년 한국전자통신연구소(ETRI)의 원천기술을 도입하여 소프트웨어 정의 경계(Software Defined Perimeter: SDP)를 개발하였다. 국민체육진흥공단에 서비스를 제공하는 등 상용화에 나서면서, 인터넷 기반에서 인프라에 구매 받지 않고 모든 연결을 보호하는 제로트러스트(Zero Trust Network Access: ZTNA)를 달성하고자 하는 기업이다.

T**** NAC는 네트워크에 접속하는 유·무선 엔드포인트에 대한 보안상태를 점검하여 사내망과 엔드포인트를 보호하는 네트워크 접근통제(NAC) 시스템이다.

Relative Policy

유관 정책

1. 정부 주도 사업

정보시스템 구축 및 운영 지침(행정안전부 고시 제2011-36호)에 따라 보안 분야(기술적 보안)에서 CC제품군(국제 CC인 경우 IT 보안인증사 무국의 인증 필요) ‘네트워크 접근통제’로 분류되어 있다.

행정안전부 고시 제2011-36호에 따라 정부기관에서는 정보시스템의 보안을 위하여 위험분석을 통한 보안 계획을 수립하고 이를 적용하여야 한다(기본지침). 이는 정보시스템의 구축 운영과 관련된 “서비스 접근 및 전달”, “플랫폼 및 기반구조”, “요소기술” 및 “인터페이스 및 통합” 분야를 모두 포함하여야 한다. NAC는 보안 분야 세부 기술 지침에 포함되어 있어, 정부기관에서 정보시스템의 보안을 위해 필수적으로 구매해야 하는 솔루션이다.

2. 표준화 및 상호운용성

초창기 1세대의 NAC는 과거부터 사용되던 네트워크 접속 사용자 인증 프로토콜인 802.1X를 기반으로 한 제품들이 주를 이루었다. 2세대 NAC는 802.1X에서 벗어나 네트워크 접속장치들과 SNMP를 통해 정보를 수집하거나 각 네트워크마다 센서 또는 Probe라 불리는 장치를 통해 독립적으로 정보를 수집할 수 있게 되었고 접근제어 또한 대체적인 수단으로 제공하기 시작했다. 네트워크 접속방법이 무선랜으로 변화됨에 따라 네트워크센서, 무선 컨트롤러, 에이전트를 통해 무선 네트워크에 대한 가시성을 확보하는 기능들도 추가되고 그를 바탕으로 Rogue AP와 같은 무선 보안에 대응할 수 있게 되었다. 3세대 NAC는 수집과 제어를 넘어서 다양한 자동화를 위한 기술들이 추가되었다. 네트워크에 존재하는 다양한 시스템들과의 연동을 통해 상호 협력적인 보안 모델을 구축할 수 있도록 해주었다. 이 같은 연동은 REST, Webhook, Syslog와 같은 표준화된 프로토콜을 통하여 제공되게 된다. 4세대의 NAC는 최근의 BYOD와 IoT 트렌드로 기하급수적으로 늘어난 접속 단말들로 인해 IT관리자의 가시성이 저하되고 네트워크 관리가 어려워지는 것을 해결하는 것에 중점을 두고 있다. 단말을 보다 정확히 식별하고 더 나아가서 다양한 비즈니스 상태(EoL, EoS 등)를 손쉽게 관리하거나 단말에 알려진 취약점들을 자동적으로 관리할 수 있도록 해주는 방향으로 진화하고 있다. 워크에 다양한 단말을 통한 보안위협 발생 가능성이 커진다. BYOD는 직원들의 업무효율성을 높여주었지만, 현재 기업 네트워크에 중대한 보안위협 요소로 작용하고 있으며, 이를 식별하여 조치하는 것이 중요하다.

Conclusion

결론

2000년 초 대두된 NAC는 많은 기술적 부침을 거치면서 발전하였고 BYOD 환경을 거치며 현재는 내부 보안관리를 위한 대표적인 솔루션으로 자리매김 하였다. 이제 NAC는 IoT 와 코로나19로 촉발된 재택/원격근무에 대응하기 위한 솔루션으로 다시 한번 도약을 준비하고 있다. NAC가 제공하는 가시성의 확보와 유무선통합인증, 접근통제는 최근 조명을 받고 있는 SDP(Software Defined Perimeter), ZTN(Zero Trust Network), SASE(Secure Access Service Edge) 등 새로운 보안 프레임워크가 요구하는 핵심 기술과 동일하다. 따라서 가까운 미래에 핵심 기술을 재 활용한 NAC 의 변화된 모습을 기대할 수 있을 것이다.

Reference

- [1] Seung-Hyun Paik, Sung-Kwang Kim, Hong-Bae Park, "Design and Implementation of Network Access Control for Security of Company Network", Journal of the Institute of Electronics Engineers of Korea, Vol. 47, No. 12, p. 91, 2010.
- [2] 이하용, & 양효식. (2017). 네트워크 접근제어 시스템의 보안성 메트릭 개발. 디지털융복합연구, 15(6), 217-227.
- [3] Gartner, "Market Guide for Network Access Control", <https://www.gartner.com/en/documents/3985032/market-guide-for-network-access-control>, 2020.05
- [4] Frost & Sullivan, Global Network Access Control Market, Forecast to 2024, 2020.03
- [5] KISA, 2019 국가정보보호백서, https://www.kisa.or.kr/public/library/etc_View.jsp?regno=0012001
- [6] Gartner, "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020", <http://www.gartner.com/newsroom/id/2636073>, 2011.
- [7] Zhou, L., & Chao, H. C, "Multimedia traffic security architecture for the internet of things", IEEE Network, Vol.25, No.3, pp.35-40, 2011.
- [8] Shaji, R. S., Dev, V. S., & Brindha, T. "A methodological review on attack and defense strategies in cyber warfare", Wireless Networks, Vol.25, No.6, pp.3323-3334, 2019.