낙(NAC)·알·못

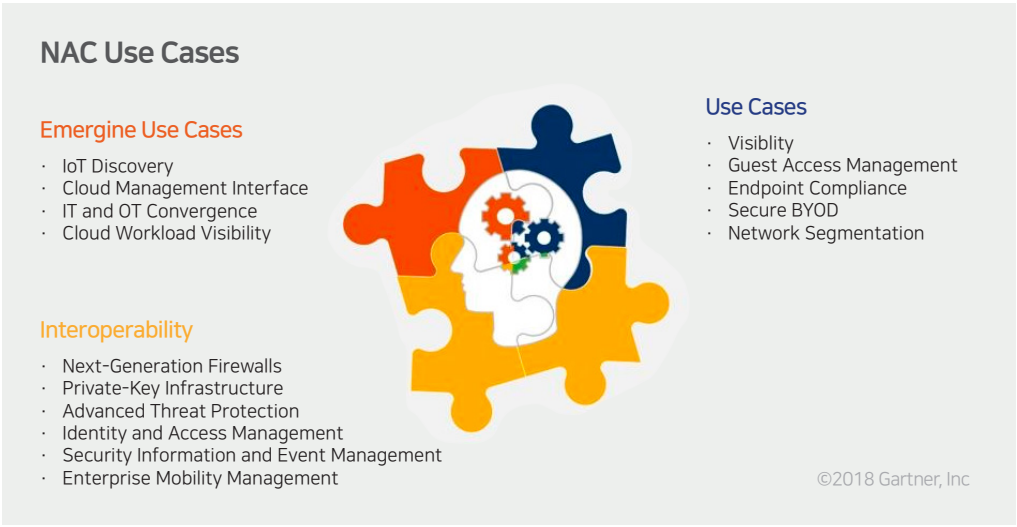
저는 NAC를 하나도 모르는데요...

GENIANS, INC.
Next-Gen Network Access Control for the IoT era
본 자료 및 내용문의: mkt@genians.com

Introduction *

과거 조직의 대표적인 보안 정책은 외부로부터의 침입차단(Prevention)이었습니다. 그 결과 우리의 보안 솔루션은 외부에서 침입하는 악성코드, 해킹, 서비스거부공격(DDoS) 등을 차단하기 위한 '방화벽 / IDS(침입탐지) / IPS(침입차단) / AV(백신)' 등에 집중되어 있었습니다. 하지만 오늘날 기업의 상황은 그 어느 때보다 복잡합니다. 관리 환경은 급변하고 보안 위협은 지능적으로 발전하고 있습니다. 네트워크는 내부에 국한되지 않고 클라우드(CLOUD), BYOD(Bring Your Own Device), 사물인터넷(IoT) 등으로 확장되고 있습니다. 원격 업무와 재택근무 등으로 외부 네트워크와 내부 네트워크를 정확히 구분하기는 불가능해졌습니다. 증가하는 사용자와 단말들이 네트워크에 접속하면서 상황을 정확하게 파악하기 어려워졌습니다. 가시성(Visibility)을 확보하는 것은 더욱더 어려워지고 있습니다. 컴퓨터, 스마트폰, 태블릿 PC를 포함한 IoT 기기들의 연결은 불과 몇 년 사이에 큰 폭으로 증가되고 있습니다. 사용자는 지리적 제한 없이 내부와 외부 그리고 클라우드를 통하여 24시간 서비스를 제공받기 희망하고 있습니다. 이러한 환경에서 어떻게 조직의 네트워크를 보호하고 효과적으로 보안정책을 수립하고 운영할 수 있을까요? 앞으로 '가시성(Visibility)'과 '보안(Security)'에 대한 요구 사항은 어떻게 변하게 될까요? 우리는 무엇을 준비해야 할까요?

이러한 고민이 존재한다면 이제 NAC 솔루션에 대한 이해가 필요한 시점입니다.



NAC Use Cases (Gartner, July 2018)

NAC란 무엇인가?

2005년 글로벌 시장조사 기업인 가트너(Gartner)는 증가하는 비인가 단말(랩톱 등)로 인한 보안 위협에 대응하기 위한 방법으로 NAC에 대한 개념을 처음 제시하였습니다. 이후 다양한 기술발전과 솔루션의 출시가 이어졌으며 2007년 스마트폰 출시 이후 BYOD(Bring Your Own Device) 등의 IT Consumerization이 확대되면서 NAC는 빠르게 성장하여 현재에 이르게 되었습니다.
NAC(Network Access Control, 네트워크 접근 제어)는 네트워크에 접속하는 단말에 대한 접근 가능 여부를 확인하여 인가된 단말만이 접근할 수 있도록 제한하는 것에서 출발하였습니다. 즉, 단말이 사내 네트워크에 접근하기 전 보안정책의 준수 여부를 검사하여 네트워크 사용을 제어하는 것입니다. 과거 다수의 네트워크 접근 제어는 802.1X라 불리는 기술을 통하여 제공되었는데 이때 AAA(Authentication, Authorization, Accounting)라 불리는 3가지 중요한 기능이 제공됩니다.

✕ 인증(Authentication)

네트워크에 접속하는 사용자나 단말을 검증하는 과정입니다. 일반적으로 사용자명과 비밀번호를 통해 검증되며 경우에 따라 단말의 MAC 주소가 인증 수단으로 사용되기도 합니다.

✕ 권한부여(Authorization)

단말이 네트워크에 연결되어 정상적인 통신이 이루어지기 이전에 수행되는 작업들을 의미합니다. 단말이 네트워크에 연결하고자 할 경우, 단말에서 제공되는 '사용자명 / 비밀번호 / 인증서 / MAC 주소'와 같은 신원 정보를 이용하여 단말을 식별하고 인증을 진행하게 됩니다. 이 과정을 통해 네트워크에 접속 가능한 단말로 인가되지 못하면 네트워크 연결이 거부됩니다.

✕ 계정관리(Accounting)

단말이 네트워크에 접속한 기록을 통해 향후 보안 관리의 목적으로 사용할 수 있도록 하는 과정입니다. 이 과정을 거치면서 어떤 단말을 누가, 언제, 어디서, 어떠한 목적으로 사용했는지 확인할 수 있습니다.

이와 같이 AAA는 네트워크 접근 제어의 기본 기능으로 오랜 기간 사용되어 왔습니다. 그러나 최근 네트워크에 접속하는 단말들로 인한 보안 문제가 증가하면서 단말의 보안 준수 상태에 따라 네트워크 접속 가능 여부를 결정하도록 요구 사항이 증가하고 있습니다. 이에 따라 단말 사용자의 인증 및 식별을 뛰어넘어 단말의 종류, 현재 보안 설정, 단말 상태 등을 확인하여 관리자가 정한 조건을 만족하는 단말만이 네트워크에 접속할 수 있게 하는 솔루션을 NAC라 부르게 되었습니다.

네트워크 연결 시점을 기준으로 NAC를 살펴보면, 연결이 이루어지기 이전 단계에서 수행되는 작업과 연결 이후 수행되는 작업으로 구분하여 설명할 수 있습니다.

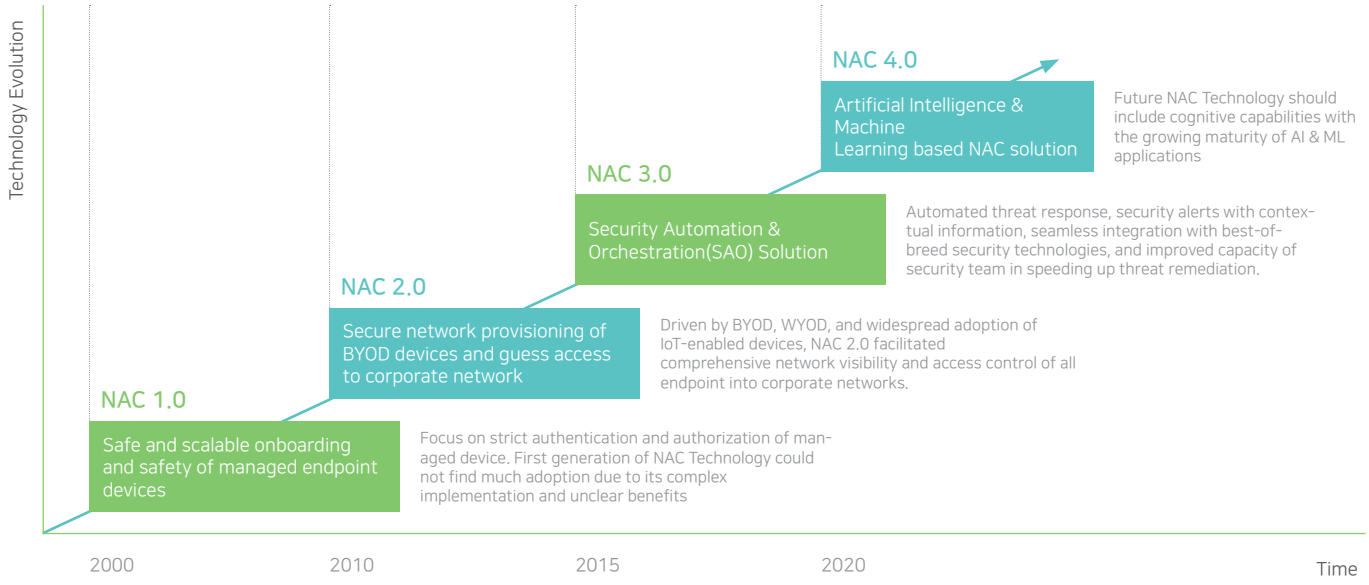
✕ NAC 연결 이전 단계 (Pre-Connect)

단말이 네트워크에 연결되어 정상적인 통신이 이루어지기 이전에 수행되는 작업들을 의미합니다. 단말이 네트워크에 연결을 시도하는 경우 단말에서 제공되는 '사용자명 / 비밀번호 / 인증서 / MAC 주소' 와 같은 신원정보를 이용하여 단말을 식별하고 인증을 진행하게 됩니다. 이 과정을 통해 네트워크에 접속 가능한 단말로 인가되지 못하면 네트워크 연결이 차단(거부) 됩니다.

✕ NAC 연결 이후 단계 (Post-Connect)

단말이 Pre-Connect 단계에서 요구 사항을 충족하면 주어진 권한에 따라 사내 네트워크를 사용할 수 있습니다. 이때 NAC는 지속적으로 단말의 상태와 정보를 수집하여 관리자의 요구 조건을 충족하는지 모니터링하게 됩니다. 만약 단말이 보안정책을 위반하는 상태로 변경되는 경우 즉시 단말을 네트워크로부터 격리합니다. 단말의 상태를 지속적으로 모니터링하기 위해 선택적으로 에이전트를 사용할 수 있습니다. 에이전트는 단말에 설치되어 시스템의 상태를 모니터링하면서 변경이 감지되면 즉시 NAC 정책서버로 변경 사실을 알려 새로운 정책을 적용받도록 합니다.

NAC의 발전 과정



NAC Technology Trend (Quadrant, Jul 2018)

✕ 태동기 - 1세대 NAC

초기의 NAC 솔루션은 802.1X(네트워크 접속 사용자 인증 프로토콜) 기반의 제품이 주를 이루었습니다. 이는 스위치 및 무선 접속 장치(AP 등)에서 제공되는 802.1X 표준을 이용하여 인터페이스에 연결이 감지되면, 정해진 인증서버(RADIUS)를 통하여 사용자명, 비밀번호 또는 인증서를 통해 사용자를 식별한 뒤 인증서버에서 접속이 허가되면 포트(Port) 등의 연결 인터페이스를 활성화시켜주는 방식입니다(연결 시도 – 인증 – 연결 활성화). 이 방식은 스위치의 포트 수준에서 작동되기 때문에 가장 완벽한 접근 제어를 제공할 수 있습니다. 하지만 802.1X를 지원하지 않는 장치들에 대한 인증 문제와 모든 접속 장치가 802.1X를 지원해야 하는지 확인해야 하는 등 기존 네트워크에 NAC를 한 번에 적용하기에 어려운 점이 많았습니다.

✕ 성장기 - 2세대 NAC

802.1X에서 벗어나 네트워크 접속 장치들과 SNMP(Simple Network Management Protocol)를 통해 정보를 수집하거나, 각 네트워크마다 센서 또는 프로브(Probe)라 불리는 별도의 장치를 설치하여 독립적으로 정보를 수집할 수 있게 되었습니다. 802.1X 이외에 네트워크에서 적용이 가능한 접근제어는 VLAN Steering(VLAN을 조정하여 단말을 제한된 VLAN으로 이동) / ACL(Access Control List) / ARP Spoofing(센서 기반 ARP를 이용한 제어) / SPAN(미러링) 포트를 통한 연결 해제 등 사용자의 환경이나 요구 사항에 적합한 다양한 방식으로 진화되었습니다. 네트워크 접속방법이 유선에서 무선으로 변화됨에 따라 네트워크 센서, 무선 컨트롤러, 에이전트를 통해 무선 네트워크에 대한 가시성을 확보하는 기능들이 추가되고, 이를 바탕으로 비인가 접속 장치(Rogue AP)와 같은 무선 보안에도 추가적으로 대응할 수 있게 되었습니다.

✕ 도약기 - 3세대 NAC

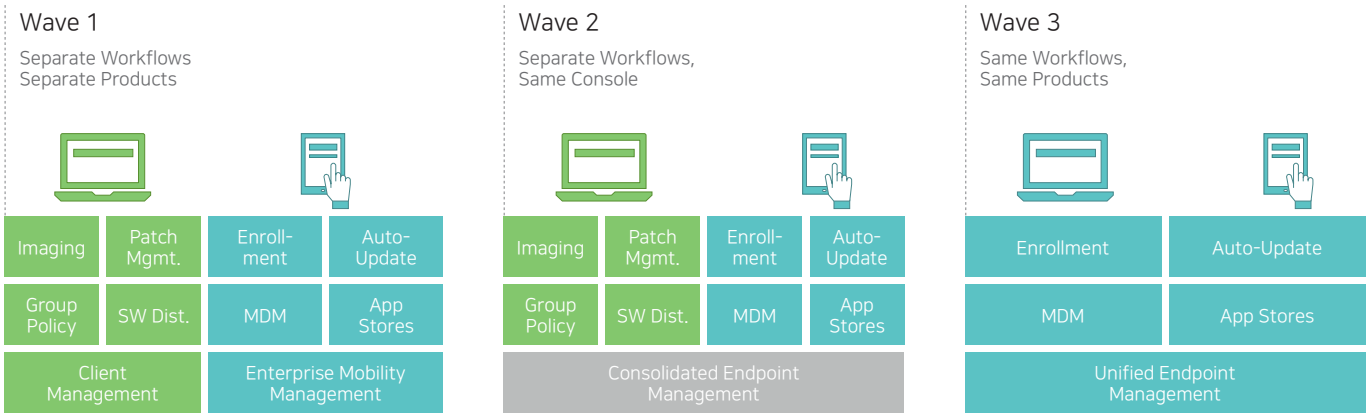
정보 수집과 접근제어를 넘어 다양한 자동화를 위한 기술들이 3세대 NAC에 추가되었습니다. 에이전트를 통해 기업이 원하는 상태로 단말의 보안 수준을 자동적으로 설정하는 것이 가능해졌으며, REST, Webhook, Syslog 등의 표준화된 연동 프로토콜을 통하여 네트워크에 존재하는 다양한 시스템들과의 상호 협력적인 보안 모델을 구축할 수 있게 되었습니다. 예를 들어 방화벽, IPS와 같은 많은 경계선(Perimeter) 보안 솔루션은 서브 네트워크에서 단말과 단말이 직접 통신하는 것을 제어할 수 없습니다. 이러한 한계는 NAC와의 연동으로 해결될 수 있습니다. 또한 NAC와의 연동을 통하여 IP에 대한 사용자 정보 및 단말 정보 등을 확인할 수 있으며 이를 바탕으로 보다 광범위하고 효과적인 접근제어 정책을 수립하고 운영할 수 있게 되었습니다.

✕ 완성기 - 4세대 NAC

현재의 NAC 솔루션은 다양하게 증가하는 단말들로 인해 IT 관리자의 가시성이 저하되고, 네트워크 관리가 어려워지는 문제를 해결하는 것에 중점을 두고 있습니다. 많은 보고서에서 BYOD뿐 아니라 5G, 사물인터넷(IoT) 등의 확대로 200억 개 이상의 사물이 연결될 것으로 전망하고 있습니다. 기하급수적으로 증가하는 단말을 보다 정확히 탐지하여 식별하고, 단말의 다양한 비즈니스 상태(End-of-Life, End-of-Support 등)를 손쉽게 관리할 뿐만 아니라 단말에 알려진 취약점 정보(CVE, Common Vulnerability & Exposure)까지도 자동으로 관리할 수 있도록 4세대 NAC는 진화하고 있습니다. 또한 최근 IT 환경의 변화에 맞게 클라우드를 지원하거나 클라우드 기반 NAC 서비스 등도 새롭게 선보이고 있습니다.

내부 네트워크와 NAC

최근 정보 보안의 중심이 네트워크에서 단말로 이동하고 있습니다. 단말의 증가와 함께 위협 역시 증가하고 있으며 APT, 랜섬웨어 등 공격의 최종 목표가 단말로 바뀌고 있습니다. 그러나 많은 경계선 보안 솔루션으로는 단말 위협에 효과적으로 대응하기 어렵습니다. NAC는 이러한 문제를 해결하기 위한 다양한 기능을 제공하며, 그 출발점은 사용자와 단말입니다. NAC의 운영을 통하여 다음에 명시된 많은 문제점을 해결할 수 있으며, 보다 강력하고 효율적인 단말 보안 관리를 시작할 수 있습니다.



3 Waves of Evolution in Endpoint Management (©2018 Gartner, Inc)

✕ 비인가 단말의 무단 반입

NAC가 없는 네트워크의 경우 어떠한 단말을 연결하더라도 즉시 네트워크를 사용할 수 있습니다. 이는 사무실이 물리적으로 안전하게 보호되고 있는 경우에도 직원들이 회사 자산이 아니거나 허용되지 않은 임의의 단말을 회사 네트워크에 연결하여 랜섬웨어(Ransom-ware) 등의 악성코드를 유포하는 등 사내 IT 시스템에 심각한 손상을 초래할 수 있게 됩니다. NAC는 이러한 문제를 해결하기 위해 연결되는 모든 단말을 탐지하고 인증을 수행하여 일정 수준 이상의 보안 요구 사항을 충족하는 경우에만 사내 네트워크에 연결할 수 있도록 제어합니다.

✕ 보안사고 발생 시 IP 추적 불가

다수의 보안 시스템은 감사기록을 위해 IP 주소를 기록합니다. 보안 사고 발생 시 감사기록의 확인을 통해 문제가 되는 IP를 확인하더라도 현재 그 IP가 과거에 사용되었던 시스템과 같은지, 사용자는 누구인지, 어떤 시스템인지 등에 대한 최신 정보를 얻는 것은 굉장히 어렵고 복잡한 일입니다. NAC는 지속적인 네트워크 감시를 통해 연결되는 모든 단말에 대한 기록을 저장합니다. 수개월 전 특정 시점에 해당 IP를 사용했던 단말에 대한 다양한 정보를 제공할 뿐 아니라 지금 현재의 정보 역시 실시간으로 확인할 수 있습니다.

✕ 보안 규제에서 요구되는 IT 자산관리

오늘날 기업의 IT 환경은 5G, 사물인터넷(IoT) 등의 변화로 과거에 비해 훨씬 복잡합니다. 이로 인해 많은 보안 규제가 필요하며 IT 자산에 대한 철저한 관리가 요구되고 있습니다. 하지만 IT 자산을 정확하게 파악하고 그 상태를 항상 확인하는 것은 관리자에게 간단한 일이 아닙니다. IT 자산을 관리하기 위해서는 MAC 주소와 같은 식별 값부터 단말의 제조사 / 제품명 / 이름 / 위치(스위치 포트 또는 물리적 위치) / 사용자명 / 네트워크 연결 및 단절 시간 등의 정보가 정확히 수집되어야 합니다. NAC는 네트워크에 연결되는 IT 자산을 실시간으로 감시하여 상시 원하는 데이터를 출력할 수 있어 IT 관리자의 부담을 크게 줄여줄 수 있습니다.

✕ 무선랜과 공유 패스워드

스마트폰, 태블릿PC 등 모바일 기기가 확산되고 업무에 활용되면서 무선랜 사용이 크게 증가하고 있습니다. 고가의 관리형 무선 접속 장치를 사용하는 경우 무선랜 접속 시 개인의 아이디와 비밀번호를 이용한 사용자 인증이 이루어질 수 있습니다. 그러나 여전히 많은 무선 네트워크는 공유 패스워드를 통해 무선랜에 접속하고 있습니다. 공유 패스워드는 손쉽게 노출될 수 있고 접속한 사용자에 대한 식별이 불가능하여 추적이 어렵습니다. 회사의 공유 패스워드는 원칙적으로 그 패스워드를 아는 직원이 회사를 떠나는 경우 변경해야 합니다. 그러나 전 직원이 공유하는 패스워드를 매번 변경하는 것은 쉬운 일이 아닙니다. 이를 위해 무선랜 접속 시 개인의 패스워드를 이용할 수 있도록 해주는 802.1X 시스템이 필요합니다. NAC는 기본적으로 802.1X를 지원하여 보다 향상된 무선랜 보안을 구축할 수 있습니다.

✕ 허가되지 않은 외부 네트워크 접속

사용자 단말은 기업에서 제공하는 네트워크 이외에도 다양한 형태의 외부 네트워크 접속이 가능합니다. 통신사의 Wi-Fi 서비스뿐 아니라 스마트폰을 이용한 테더링(tethering), 핫스팟(Hotspot), 공공(Public) Wi-Fi 등은 대표적인 사례입니다. 이러한 접속은 기업 보안 시스템을 우회하는 인터넷 연결을 만들어 내부 자료 유출과 같은 문제점을 발생시킬 수 있습니다. NAC를 통해 기업 내부에서 접속 가능한 Wi-Fi를 모니터링하고 어떤 사용자가 접속하는지를 관리하고 통제할 수 있습니다. 또한 사용자 단말에서 IT 관리자가 설정하지 않는 네트워크 대역에 접속하는 이벤트 등을 모니터링하여 내부 보안 시스템을 우회하려는 시도를 차단할 수 있습니다.

✕ 필수 소프트웨어 미 설치 및 구동

관리자는 다양한 보안 문제를 해결하기 위해 사용자의 시스템에 설치해야 할 필수적인 소프트웨어나 운영체제 설정을 직원들에게 요구하게 됩니다. 하지만 모든 사용자의 단말이 그 요구 사항을 항상 준수하는 것은 아니기 때문에 보안 사고는 끊임없이 발생되고 있습니다. NAC는 AV(백신)와 같이 단말에 필수적인 소프트웨어 설치나 화면보호기 설정과 같은 규정을 준수하는지를 지속적으로 모니터링하여 규정을 위반한 경우 차단, 치유, 격리 등의 방법을 적용할 수 있습니다. 이를 통해 사용자 인식을 높이고 보안 수준을 균일하게 유지할 수 있게 됩니다.

✕ 운영체제 최신 보안패치 미 적용

단말의 보안을 위해 무엇보다 중요한 것은 최신 보안패치의 적용입니다. NAC는 단말의 보안패치 적용 상태를 지속적으로 모니터링하여 패치가 적용되지 않은 단말을 네트워크에서 격리하는 등 다양한 조치를 취할 수 있습니다. 이는 제어가 단말이 아닌 네트워크 수준에서 동작한다는 점에서 기존 단말을 관리하는 소프트웨어가 제공하는 것과 크게 다르다고 할 수 있습니다. IT 관리자는 네트워크 통제를 통해서 사용자가 우회할 수 없는 강력한 규제를 할 수 있습니다.

NAC와 Firewall(방화벽)의 차이점

네트워크(Network) 상의 접근제어(Access Control)라는 기능으로 보았을 때 NAC는 자칫 방화벽(Firewall)과 유사해 보일 수도 있습니다. 그러나 두 제품은 다음과 같은 큰 차이점을 가지고 있습니다.

✕ 단말 중심 vs 네트워크 중심

방화벽은 일반적으로 두 개 이상의 서로 다른 네트워크 경계에 위치하여 네트워크를 오가는 통신에 대한 접근제어를 제공합니다. 이에 반해 NAC는 각 단말 간 통신에 대한 접근제어를 제공합니다. 예를 들어 동일한 네트워크에 존재하는 두 PC 사이에 이루어지는 파일공유에 대해서 일반적으로 방화벽은 제어하지 못하는 반면 NAC는 제어가 가능합니다.

✕ 동적 접근제어 vs 정적 접근제어

방화벽의 접근제어 정책은 일반적으로 '출발지, 목적지 IP 주소 / 포트 정보 / 프로토콜 정보' 등과 같은 객체를 통해서 이루어집니다. 최근 차세대 방화벽(NGFW) 등에서 사용자와 같은 추가적인 객체를 통한 접근제어를 제공하기 시작했으나 그 수가 많지 않습니다. 반면 NAC는 다양한 조건으로 단말들을 그룹으로 정의할 수 있으며 단말의 조건 및 상태에 따라 자동으로 해당 그룹에 포함 / 해제가 됩니다. 그리고 해당 그룹에 특정 보안정책이 적용되는 구조를 제공합니다. 예를 들어 'AV(백신) 미 설치 그룹'이라는 그룹에는 PC의 상태에 따라서 실시간으로 그룹의 사용자가 변하게 되며 서로 다른 보안정책을 적용받게 됩니다.

✕ 내부망 vs 외부망

이러한 이유로 방화벽은 단말의 사용자를 특정할 수 없고 상세한 정보를 수집할 수 없는 외부 사용자(단말)와 내부 시스템 간의 접근제어의 목적에 보다 적합하며, NAC는 다양한 상태 정보를 얻을 수 있는 내부 사용자에 대한 접근제어 시스템으로 적합합니다.

두 개의 제품은 각각의 역할에 맞는 위치 및 구성으로 네트워크 보안을 보다 효과적으로 구축할 수 있는 상호 보완적인 역할을 수행하며 실제로 많은 제품 간의 연동이 이루어지고 있습니다.

NAC의 구축과 고려사항

✕ 단말 가시성 확보

앞에서 살펴본 바와 같이 NAC 구축의 궁극적인 목적은 보안규정을 준수하지 않는 단말의 네트워크 접속 및 사용을 통제하고 관리하는 것입니다. 그러나 단말에 대한 통제 기능을 네트워크에 즉시 적용하기는 매우 어렵습니다. 예를 들어 802.1X를 각 스위치 별로 설정하기에 앞서 네트워크에 있는 스위치들이 모두 802.1X를 지원하는지, 그리고 현재 각 스위치에 연결된 단말이 802.1X 인증을 지원하는지, 지원하지 않는다면 MAC 주소 기반 인증을 위해 필요한 각 단말의 MAC 주소는 어떻게 수집할 것인지 등의 많은 사전 고려 사항이 필요합니다. 따라서 네트워크에 대한 가시성을 확보하는 것이 가장 처음으로 필요한 작업입니다. 이때 통제 없이 가시성 확보가 가능해야 하는데 802.1X는 제어가 이루어져야만 가시성을 얻을 수 있는 구조이므로 가시성 확보만을 위한 목적으로는 적합하지 않습니다.

가시성은 단말이 가진 IP / MAC 주소와 같은 기본 정보를 시작으로 플랫폼 / 이름 / 제조사 / 호스트명 / 연결 스위치 / 포트 / 연결 SSID / 서비스 포트 / 동작 상태와 같은 정보들이 제공되어야 합니다. 추가적으로 단말에 대한 보다 상세한 가시성 확보를 위해 Agent가 제공될 수 있습니다.

✕ 단말의 분류

가시성이 확보되면 보안정책을 수립해야 합니다. 보안정책 수립의 첫 단계는 수집된 데이터를 바탕으로 단말을 분류하는 것입니다. NAC에서 제공되는 다양한 조건을 이용하여 단말을 분류하고 제어가 필요한 그룹이 어떤 그룹인지 결정해야 합니다. 단말을 분류하는 기준은 관리자의 일상적인 관리 업무에 필요한 그룹이나 기업의 규정을 미 준수하는 단말을 식별하는 것 등이 우선적으로 고려될 수 있습니다.

✕ 네트워크 접근제어

제어는 네트워크 환경이나 단말의 상태에 따라 다양하게 이루어져야 합니다. 802.1X는 물론 ARP 통제 / 스위치 제어 / SPAN 방식 / 에이전트 기반 / 타 보안 시스템 연동까지 다양한 방법을 선택적으로 적용할 수 있어야 합니다.
이때 가장 먼저 고려되어야 하는 것이 단말에 대한 사용자의 인증입니다. 인증은 단말을 어떤 사용자가 사용하는 것인지 식별하는 매우 중요한 작업입니다. 이때 사용되는 사용자 데이터베이스는 일반적으로 기업이 이미 보유한 인증 시스템과 연동하는 것이 권장됩니다. Microsoft Active Directory와 같은 LDAP 연동이나, Google G-Suite, Office 365와 같은 기업용 서비스, 이메일, 심지어는 RDBMS까지 다양한 외부 시스템과의 연동이 필요할 수 있습니다.
이후 단계로 사용자 인증 및 단말의 속성에 따라 역할 기반 접근제어(Role Based Access Control)가 제공되어야 합니다. 영업 조직과 기술 조직이 각기 다른 접속 권한을 가질 수 있도록 VLAN을 할당하거나 연결을 차단하는 제어를 수행할 필요가 있습니다.
방문자 등 접근제어를 통해 연결이 차단된 사용자에게는 웹브라우저 사용 시 관리자가 지정한 페이지로 사용자의 접속을 우회시켜 사용자가 스스로 필요한 조치를 취할 수 있도록 하는 Captive Web Portal 페이지를 구성할 수 있습니다. 이 페이지를 통해 사용자는 자신에게 요구되는 보안정책을 확인하고 조치를 취해 네트워크에 접속 가능한 자격을 확보할 수 있습니다.

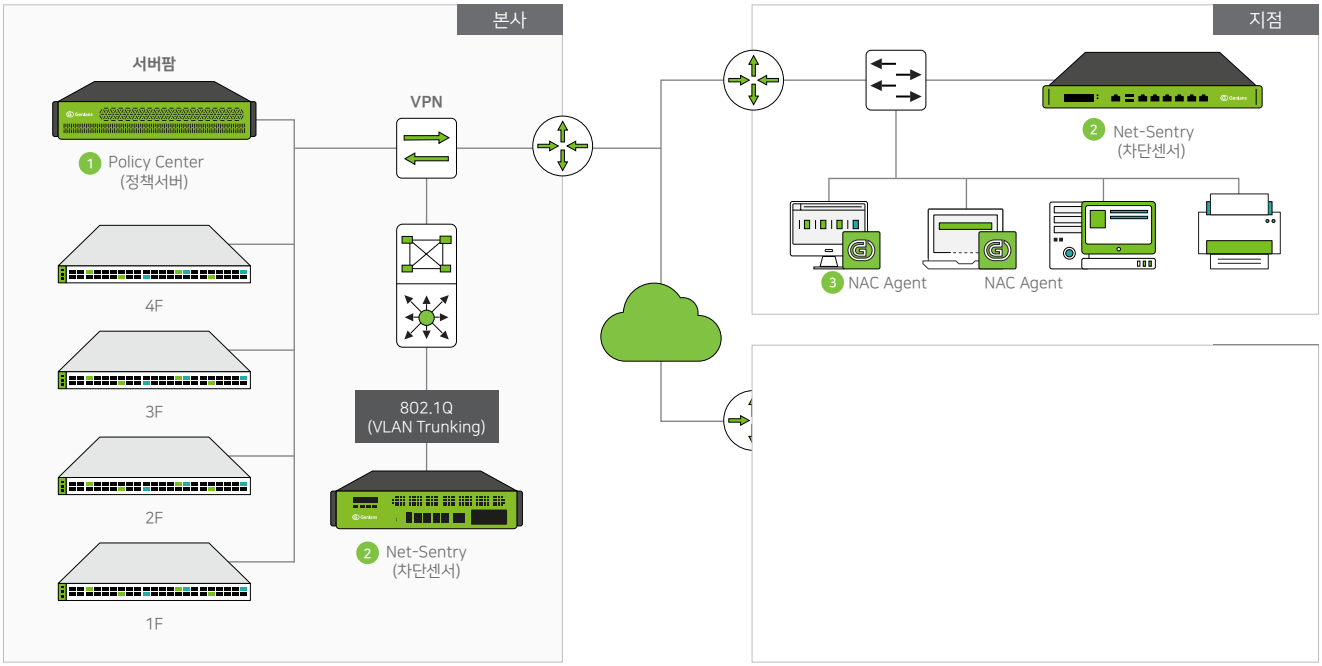
✕ IT보안 자동화

자동화는 사용자들이 따라야 할 보안규정 (운영체제 업데이트 및 설정, 필수 소프트웨어 설치 및 동작 등)을 관리자가 정한 정책에 따라 자동으로 적용해주는 것입니다. 제어가 필요한 단말에 대해서 인증과 같이 제어 자체가 목적을 달성하는 수단이 되기도 하지만 또 다른 경우에는 제어에 앞서 자동화를 통해 사용자의 단말이 치유되는 것이 더 필요할 수도 있습니다.

예를 들어 전체 사용자의 90%가 준수하지 않는 보안정책이 있다고 가정할 때 90%의 사용자에 대해 네트워크 접근제어 정책을 수행하는 것보다는 에이전트를 통하여 자동으로 정책을 따르도록 처리된다면 보다 손쉽게 NAC을 도입할 수 있습니다. 또한 자동화는 사내에 보유된 다양한 시스템들과의 연동을 통해 상호 정보나 이벤트를 주고받아 관리자의 개입 없이 업무가 자동적으로 처리될 수 있도록 도와줍니다.

Genian NAC

Genian NAC는 IT 환경의 변화를 반영한 4세대 NAC로써 앞서 기술한 모든 내용이 반영되어 있습니다. 진보된 단말 플랫폼 정보(DPI)를 기반으로 다양한 접근제어, IT 보안 자동화, 향상된 무선랜 보안, 뛰어난 연동성 등을 통해 안전한 사내 네트워크 환경을 구축할 수 있습니다.



1 Policy Center & Console (정책서버)

- 유무선 네트워크를 통합 관리
- 내부 보안 강화 지원

2 Net-Sentry (차단센서)

- PC등 에이전트 설치 단말에 대한 자산 관리 및 장치 사용 통제
- 에이전트 설치에 따른 비용 부담 없음(필요에 따라 사용/미사용 가능)

3 Agent (에이전트)

- 유무선 단말에 대한 정보 수집
- 강력한 통제 수행

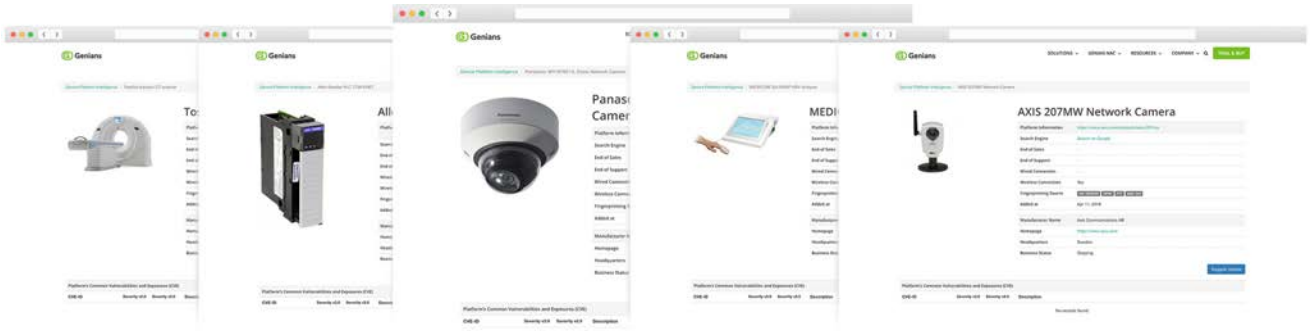
Genian NAC 설치 및 구성요소

✕ 네트워크 센서 기반의 진보된 가시성

Genian NAC는 각각의 서브 네트워크에 직접 연결되는 차단 센서를 사용하여 가시성을 확보합니다. 센서는 기존 IT 인프라와의 연동을 최소화하여 도입이 간편하고 허브와 같은 기존 네트워크(legacy network) 환경에서도 문제없이 동작합니다. 또한 네트워크 가시성 확보에 필요한 각 서브 네트워크의 중요 트래픽 – Broadcast(ARP, DHCP, uPNP, mDNS), Multicast 등 – 을 모니터링할 수 있기 때문에 스위치 등 네트워크 장치와 연동을 통한 NAC 제품군에 비해 진보된 가시성을 제공합니다.

✕ 진보된 단말 플랫폼 정보

DPI(Device Platform Intelligence) 기술을 이용하여 가장 정확하고 다양한 단말의 정보를 제공받을 수 있습니다. 단말의 식별 정보뿐 아니라 판매 종료, 지원 종료, 네트워크 연결 방식, 제조사 운영 여부, 제조 국가, 발표된 취약점 목록 등의 정보를 제공하여 IT 관리자의 일상적인 관리 업무를 손쉽게 만듭니다.



DPI 를 이용한 단말 가시성 확보

✕ 다양한 접근제어 방식

802.1X부터 ARP 통제, DHCP 서버, 스위치 제어, SPAN 기반 제어, 에이전트 기반 제어, 타 솔루션과의 연동을 통한 제어 등 기존 NAC 제품 대비 가장 폭넓은 제어 방식을 지원합니다. 이를 통해 IT 관리자의 요구 사항에 맞춘 단계적 보안정책을 빠르고 쉽게 수립하고 운용할 수 있습니다.

✕ 다양한 IT보안 자동화

Genian NAC에서 제공되는 에이전트는 단말의 정보 수집을 넘어 운영체제 설정 관리, 애플리케이션 관리, 장치 제어, 업데이트 관리 등 관리자가 원하는 다양한 IT 보안 자동화를 손쉽게 구축할 수 있게 합니다. 또한 다양한 신청 / 승인 시스템을 제공하여 IT 관리자의 일상 업무를 단순화시켜주고 사용자에게는 편리성을 제공합니다.

✕ 뛰어난 연동성

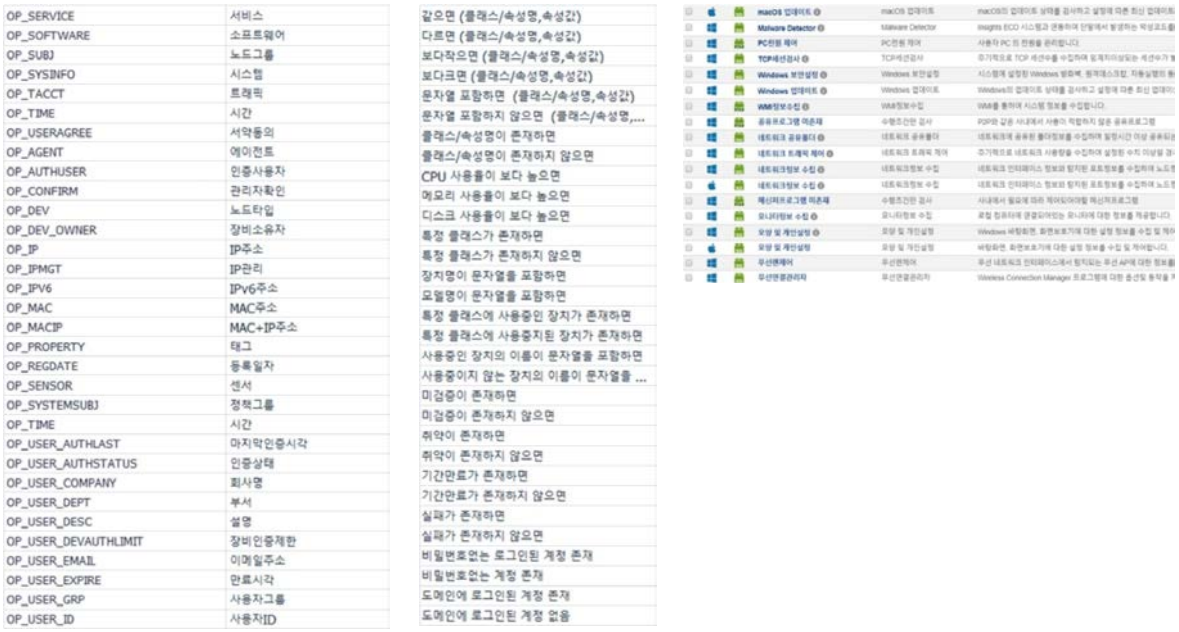
REST API, Webhook, Syslog와 같이 표준적인 연동 기술을 제공하고, 기존 IT 시스템과의 다양한 연동을 통해 보안 오케스트레이션(orchestration) 도구로써 활용할 수 있습니다.

✕ 향상된 무선랜 보안

네트워크 센서 및 에이전트를 통해 무선 정보를 수집하여 비인가 접속 장치(Rogue AP) 탐지, 비인가 무선랜 접속 모니터링 및 제어, Soft AP 차단 등의 무선랜 보안 기능을 제공합니다.

✕ IT 환경의 변화를 반영한 4세대 NAC

Genian NAC은 4세대 NAC의 대표적인 제품으로 네트워크 센서를 통해 기존 IT 환경의 변화 없이 가장 진보된 가시성을 제공합니다. 이를 통해 500여 개 이상의 다양한 그룹 조건을 제공하여 단말 상태에 따른 동적인 그룹을 상세히 관리할 수 있습니다. 다양한 구성 방식을 지원하여 빠르고 쉽게 성공적인 NAC 구축을 할 수 있습니다.



OP_SERVICE	서비스
OP_SOFTWARE	소프트웨어
OP_SUBJ	노드그룹
OP_SYSINFO	시스템
OP_TACCT	트래픽
OP_TIME	시간
OP_USERAGREE	서약동의
OP_AGENT	에이전트
OP_AUTHUSER	인증사용자
OP_CONFIRM	관리자확인
OP_DEV	노드타입
OP_DEV_OWNER	장비소유자
OP_IP	IP주소
OP_IPMGT	IP관리
OP_IPV6	IPv6주소
OP_MAC	MAC주소
OP_MACIP	MAC+IP주소
OP_PROPERTY	태그
OP_REGDATE	등록일자
OP_SENSOR	센서
OP_SYSTEMSUBJ	정책그룹
OP_TIME	시간
OP_USER_AUTHLAST	마지막인증시각
OP_USER_AUTHSTATUS	인증상태
OP_USER_COMPANY	회사명
OP_USER_DEPT	부서
OP_USER_DESC	설명
OP_USER_DEVAUTHLIMIT	장비인증제한
OP_USER_EMAIL	이메일주소
OP_USER_EXPIRE	만료시각
OP_USER_GRP	사용자그룹
OP_USER_ID	사용자ID

같으면 (클래스/속성명,속성값)
다르면 (클래스/속성명,속성값)
보다작으면 (클래스/속성명,속성값)
보다크면 (클래스/속성명,속성값)
문자열 포함하면 (클래스/속성명,속성값)
문자열 포함하지 않으면 (클래스/속성명,...
클래스/속성명이 존재하면
클래스/속성명이 존재하지 않으면
CPU 사용률이 보다 높으면
메모리 사용률이 보다 높으면
디스크 사용률이 보다 높으면
특정 클래스가 존재하면
특정 클래스가 존재하지 않으면
장치명이 문자열을 포함하면
모델명이 문자열을 포함하면
특정 클래스에 사용중인 장치가 존재하면
특정 클래스에 사용중지된 장치가 존재하면
사용중인 장치의 이름이 문자열을 포함하면
사용중이지 않는 장치의 이름이 문자열을 ...
미검증이 존재하면
미검증이 존재하지 않으면
취약이 존재하면
취약이 존재하지 않으면
기간만료가 존재하면
기간만료가 존재하지 않으면
실패가 존재하면
실패가 존재하지 않으면
비밀번호없는 로그인된 계정 존재
비밀번호없는 계정 존재
도메인에 로그인된 계정 존재
도메인에 로그인된 계정 없음

동적 그룹 생성을 위한 객체 및 조건분류

Conclusion *

2005년 가트너에 의해 처음 등장한 NAC는 급격하게 변화하는 IT 환경에 대응하면서 현재까지 지속적으로 발전하고 있습니다. Genian NAC는 이러한 환경의 변화와 요구를 적극적으로 반영한 결과 2018년 7월 국내 NAC 최초로 가트너 'Market Guide for Network Access Control'의 대표기업(Representative Vendors)으로 선정되었습니다. 가트너는 Genian NAC가 사물인터넷(IoT) 환경에서 다양한 단말을 정확하게 판별할 수 있는 특화된 '단말 플랫폼 인텔리전스(DPI)' 기술을 보유하고 있는 NAC 기업이라고 강조했습니다. 또한 4세대 NAC의 대표 제품으로 지능화, 고도화되어 가고 있는 보안 위협에 보안 관리자들과 함께 적극적으로 대응하고 있습니다.

한국인터넷진흥원(KISA)의 사이버 위협 동향 보고서(2019년, 2018년) 및 IEEE, MTAP저널 등 다수의 보고서에 따르면 전 세계적으로 보안 위협에 대응하기 위해 막대한 양의 인적·물적 자원을 투자하고 있지만 보안 위협은 지속해서 증가세를 보이며 피해 규모도 크게 증가하고 있는 추세입니다. 이와 같은 추세라면 향후 얼마나 다양한 종류의 위협이 발생할까요? 어떻게 안전한 사내 네트워크를 유지할 수 있을까요? 이것이 NAC가 필요한 이유입니다. 명심하십시오. NAC는 단순히 사용자, 단말의 정보 분석만을 위한 솔루션이 아닙니다. NAC에 대한 올바른 이해는 안전한 사내 네트워크 환경의 구축을 위한 기본 척도이며 보안 관리의 완성입니다.

참조 URL
https://www.genians.co.kr/product_intro/genian-nac/nac_info/
https://docs.genians.com/release/intro.html
https://www.gartner.com/document/3884483

CONTACT US
본 자료 및 내용문의 : mkt@genians.com

Genians
Next-Gen Network Access Control for the IoT era

2005년 설립된 지니언스㈜는 국내 NAC(Network Access Control) 시장을 선도하며 글로벌 비즈니스 확장을 통해 보안 소프트웨어 전문기업으로 성장하고 있습니다. 네트워크 보안 및 단말 분석 분야 특화기술을 기반으로 내부 보안에 특화된 제품 라인업을 보유 중입니다. 네트워크에 접속하는 단말의 가시성을 확보하여 제어하는 네트워크 접근 제어 솔루션 '지니안 NAC (Genian NAC)'를 통해 국내 시장을 선도하고 있습니다. 2017년 단말 기반 지능형 위협 탐지 및 대응 솔루션 '지니안 인사이츠 E (Genian Insights E)'를 출시하며 EDR (Endpoint Detection & Response) 시장에 진출했습니다. 2016년 1월 해외사업 시작과 함께 미국 보스턴에 현지법인을 설립한 바 있으며 2017년 8월 코스닥에 상장했습니다.

Doc. v 1.0-KO