NAC, 아는만큼 성공한다.
IT 관계자라면 꼭 알아야 할

NAC 기술백서

I

엔드포인트연구소

NAC, 아는만큼 성공한다.
IT 관계자라면 꼭 알아야 할

NAC 기술백서

IT 관계자라면 꼭 알아야 하는 NAC 기술백서

금융권에서의 보안사고, 대형 포털사의 보안사고, 3.20 전산망 마비사태 등 최근 벌어지고 있는 해킹 및 보안 사고가 끊이질 않습니다.

NAC(네트워크접근통제 시스템)는 사내망에 접근하는 모든 기기를 검사하고 악성코드에 감염되거나 기업 보안정책에 따르지 않는 기기를 차단함으로써 네트워크의 안전을 보장하는 솔루션으로 정보보안의 새로운 패러다임으로 관심을 끌고 있지만, NAC의 복잡성은 여전히 IT 담당자들을 힘들게 하는 상황입니다.

NAC에 관련된 해외 전문자료가 많이 있으나 어려운 원서로 되어있어 꼭 알아야 하는 포인트를 놓치고 구축에 실패할 확률이 높아 미디어랜드 엔드포인트 연구진들이 쉽게 풀어 설명하고자 노력하였습니다.
IT 보안 관계자분들의 기술 길잡이가 되길 바랍니다.

Medialand
Endpoint
Laboratory

Contents

NAC 바로알기

NAC란 무엇인가? ---------- 4
NAC를 왜 사용할까?---------- 5
NAC의 구성---------- 6
1. Pre-admission과 Post-admission
2. Agent와 Agentless의 비교
3. Out-of-band와 Inline의 비교
4. 검역, 격리와 종속 포털

NAC의 정의와 역사 ---------- 9
[비교분석] NAC구현방법 및 통제방식 ---------- 12
1. 802.1x
2. VLAN
3. ARP
4. SW Agent
5. DHCP

[개인정보보호] 고객DB서버로의 통신 원천 차단하는 방법 - 18

NAC TECH GUIDE

NAC 10분만에 이해하기 ---------- 20
NAC 1주만에 구축하기 ---------- 24
NAC 도입은 반드시 성공해야 한다 ---------- 28

CEO 포럼

성안의 성, 두개의 성문 Tgate ---------- 32
IT 보안, 패러다임이 바뀌어야 한다 ---------- 34
NAC 관심높여 보안 위험 덜자 ---------- 36

언론

성안의 성, IT이중보안 시스템 ---------- 38
NAC솔루션 Tgate(티게이트) ---------- 39

고객 추천글

고객 추천글 ---------- 40

NAC 바로알기

NAC란 무엇인가?
NAC를 왜 사용할까?
NAC의 구성
NAC의 정의와 역사
NAC구현방법 및 통제방식 [비교분석]

NAC란 무엇인가?

NAC는 'Network Access Control' 의 약어로 '네트워크 접근제어 및 네트워크 접근통제' 라고도 한다.

NAC(네트워크접근제어)는 일련의 프로토콜들을 사용해 '엔드포인트(Endpoint)' 가 처음 내부망 네트워크에 접근시도를 할 때 기존 내부망에 피해를 끼치지 않도록 접속하는 '엔드포인트' 에 일련의 보안 정책을 적용할 수 있도록 하는 컴퓨터 네트워킹 솔루션이다.

'네트워크 접근 제어' 라는 명칭에서 알 수 있듯이 정책에 따라 네트워크 접근을 제어하고 통제한다.
내부망 접근 전 엔드포인트 안전 검사 그리고 내부망 접근 후 사내망의 어떤 영역 접근이 가능한지와 무엇을 할 수 있는지를 정의하고 이에 맞게 제어한다.
NAC는 엔드포인트 자동 검역 과정(접근을 허용하기 전에 보안정책을 따르지 않은 기기들을 검역)을 네트워크 시스템에 통합시켜서 라우터, 스위치 그리고 방화벽 같은 네트워크 기반 시설과 맞물려 작동되게 한다.
이로써 사내 내부망과 통신이 이루어지기 전에 엔드포인트가 안전하게 작동되는지 확인하도록 한다.

처음에는 802.1x가 NAC라고 생각 되어졌다.
아직도 802.1x가 가장 간단한 NAC형태라고 생각하는 소수

의 사람들이 있지만, 현재는 NAC가 더 큰 범위를 포함하고 있다고 여겨진다.

Tgate(티게이트) 에서는..

802.1x는 인증되지 않은 엔드포인트를 스위치에서 포트를 차단 함으로서 통신을 제어하는 방식 입니다.
이는 사내망에 모든 스위치가 802.1x 프로토콜을 지원해야 가능한 방법으로 실현 가능성이 매우 낮으며, 전세계적으로 NAC 도입 실패를 초래한 대표적 사례입니다.
따라서 Tgate는 어떤 네트워크 환경에서도 구현 가능한 자체 기술로 NAC를 구현하고 있습니다.

엔드포인트가 사내망에 연결될 때 백신 보호 레벨, 시스템 업데이트 레벨 그리고 환경설정이 회사가 정해놓은 정책과 맞지 않는다면 내부망에 접근을 못하게 된다.
미리 설치되어 있는 NAC(네트워크 접근제어)에이전트가 엔드포인트를 검역하는 동안 이 엔드포인트는 오직 패치나 백신을 받을 수 있는 서버와만 통신이 가능하다.

정해져 있는 NAC보안 정책에 맞게 엔드포인트가 준비 되었을때 비로소 내부망과 인터넷에 접근 할 수 있다.
NAC는 주로 엔드포인트 검역을 위한 것이지만 종종 역할기반 통신제어의 용도로 사용되기도 한다.
이때, 내부망 접근은 사용자의 직위 또는 직책과 점검상태의 결과에 따라 다르게 주어진다.
예를 들어, 만약 회사에 인사팀 직원이 사내 내부망에 접속하려 할 때, 인사팀 서버에 접근하기 위한 보안 수준의 백신이 설치 되었는지 확인 후 다른 팀 서버가 아닌, 오직 인사팀 서버에만 접근이 가능하게 된다.
NAC는 새로 생긴 보안 제품군이기 때문에 NAC의 정의는 계속 진화하고 있으며, 논란도 계속되고 있다.

NAC를 왜 사용할까?

1. Zero-day attack의 경감

NAC솔루션의 가장 중요한 역할은 엔드포인트들이 네트워크에 접근했을 때 네트워크 상의 엔드포인트들이 새로 접근한 엔드포인트에 의해 바이러스에 감염되는 것을 막는 것이다.

2. 정책의 강제화

NAC솔루션은 네트워크 관리자들이 어떤 종류의 엔드포인트들이나 사용자들이 네트워크에 허용되는지 방침을 세우고 스위치, 라우터, 네트워크 중간 장비들로 구성된 네트워크에 정책을 강제화할 수 있게 해준다.

3. 계정 및 접근관리

옛 방식은 IP를 기준으로 통제를 했다면 NAC는 IP기준이 아니라 사용자를 기준으로 네트워크를 통제한다.

엔드포인트(endpoint)란 노트북 컴퓨터 스마트폰 등 네트워크에 접속하는 모든 유무선 기기들을 일컫는 말입니다.

NAC의 구성

NAC에서 꼭 알아야 하는 주요 개념들..
그러나 이해를 도와주는 자료가 부족하여 어려움을 겪는 분들을 위해 위키피디아에 정의되어 있는 NAC에 대한 정보들을 한글로 번역하여 쉽게 정리 하였습니다. 많은 분들이 NAC를 이해하는데 조금이나마 도움이 되길 바랍니다.

1. Pre-admission과 Post-admission

NAC에는 두 가지 설계기준이 있다. 하나는 엔드포인트가 내부망에 접근하기 전에 방침을 따르게 하는 방법이고 다른 하나는 엔드포인트가 내부망에 접근 한 후의 방침이다.

전자의 경우를 Pre-admission이라 하고, 엔드포인트들이 내부망에 접근 허용이 되기 전에 검역을 하는 것을 말한다. 대표적인 예로 가장 최신으로 패턴으로 업데이트가 되지 않은 엔드포인트가 내부망 서버에 연결되는 것을 금지한다.

후자의 경우를 Post-admission이라 하고, 사용자가 내부망에 접근한 후에 사용자의 역할에 기반한 통제를 실행한다.

Tgate(티게이트) 에서는..

Pre-admission :
내부 망에 단말이 접속하기 전에, 장비 및 사용자 인증, IP/MAC인증(DHCP기능 구현), 인사DB, LDAP, AD연동을 통한 인증처리, AGENT 미설치 PC차단, S/W검역, 보안 업데이트 등을 실시하여, 회사 보안정책을 준수한 단말만을 접속시킵니다.

Post-admission :
내부 망 접속 후 에도, 지속적으로 보안 정책 수준 유지 및 관리, 업데이트 유지, 유해트래픽 관리, 권한별 통제, 그룹별 통제, 무결성 유지, 로그 기록 등을 지속적으로 적용하여, 항상 단말의 보안을 유지하도록 합니다.

2. Agent와 Agentless의 비교

NAC의 필수적인 개념은 엔드포인트에 대한 정보를 기반으로 네트워크 접근에 대한 결정을 하고 이를 네트워크에 반영하는데 있다. 따라서, 네트워크가 어떻게 엔드포인트에 대한 정보를 받을 수 있게 할 것인지에 대한 디자인이 핵심적인 부분이다.
NAC 시스템들간의 가장 큰 차이점은 엔드포인트 정보를 얻기 위해 Agent 소프트웨어가 필요하냐와 그러한 정보를 원격에서 스캐닝 또는 네트워크 인벤토리 기술을 사용하냐이다. 전자가 Agent방식 후자가 Agentless 방식이다.

NAC가 일반화 되면서 마이크로소프트는 자사의 NAC 솔루션인 NAP(Network Access Protection)에 접근제어 Agent를 Windows7, Vista 그리고 XP에 포함에 제공하고 있다. Linux와 MAC OS X에도 유사한 성능을 제공하는 NAP호환 에이전트가 있다.

Tgate(티게이트) 에서는..

오해:
일반적으로 NAC솔루션이 Agent 소프트웨어를 설치할 경우 Agent 방식이며, 설치되는 것이 없을 경우 Agentless 방식이라고 잘못 오해되고 있습니다.
오늘날의 기술로는 Agent 소프트웨어 없이 컴퓨터기기에 설치된 보안 소프트웨어 및 일반 소프트웨어의 상태를 확인할 수 있는 방법이 없습니다. 컴퓨터의 소프트웨어 상태를 확인하기 위해서는 Agent 소프트웨어가 반드시 필요합니다. 또한, 문제 발견시, 최신 보안 패치 및 소프트웨어를 설치하기 위해서도 Agent 소프트웨어가 반드시 필요합니다. 따라서, 대부분의 NAC솔루션들이 PC보안 상태를 확인하기 위해 Agent 소프트웨어를 제공하고 있습니다. NAC를 구축하였음에도, 아무런 Agent 소프트웨어가 PC에 설치되지 않았다면, PC보안 검사를 하지 않고 있는 것이므로 NAC 본래의 목적(내부망의 모든 PC는 최신 보안 패치를 설치한 상태이어야 함)과 다르게 사용되고 있는 상태 입니다.

올바른 정의:
네트워크 통제를 하는 위치에 따라 구분하는 것이 올바른 방법입니다. 네트워크 장비에서 통제를 하는 경우, Agentless 방식이라 칭하며, Agent 소프트웨어에서 통제하는 경우, Agent 방식이라 할 수 있습니다.
Tgate는 Agent와 Agentless 둘 다 제공하는 Hybrid 형태를 취하고 있습니다.
윈도우 기반 PC의 경우, 단말기에 Agent 소프트웨어를 설치하여 더욱 강력한 보안 수준을 유지하게 할 수 있으며 이 방식은 네트워크 부하를 최소화 합니다.

모바일 기기, 인터넷 전화기 등 기타 모든 네트워크에 접속된 엔드포인트에는 Agentless방식으로 인증 및 차단을 하여 인증되지 않은 사용자 및 엔드포인트들로 부터 내부망을 보호합니다.

3. Out-of-band와 Inline의 비교

일부 Out-of-band 시스템의 경우, Agent 소프트웨어가 엔드포인트 설치되어 엔드포인트에 대한 정보를 중앙 서버 및 콘솔로 전달 된다. 정보를 수집한 중앙 서버는 이 정보를 기준으로 네트워크 접속에 대한 결정을 하고 스위치장비에게 통신을 제어하도록 명령한다.
이와 대조적으로 Inline솔루션은 하나의 장비로 된 솔루션으로 Access Layer를 위한 내부 방화벽과 같이 동작되고 정책을 강제화한다.

Out-of-Band 시스템은 기존의 인프라를 그대로 쓰는 장점이 있고 Inline 시스템은 기존 네트워크 인프라 보다는 새로운 네트워크상에서는 구축하기가 용이하다. 이 방법은 유선상에 있는 각각의 패킷을 직접적으로 통제할 수 있기때문에 더 향상된 강제화 기능을 제공할 수 있다.

Agent가 없으면서 Out-of-band와 같이 구축이 용이하고 위험성이 적은 Agnetless 방식의 제품들도 있다.
Out-of-band 방식이면서도, 강제화가 필요한 정책 미준수 기기들에 대해선 Inline 과 같은 효과를 낼 수 있다.

Tgate(티게이트) 에서는..

Tgate 는 위키피디아서 마지막에 언급한 Out-of-band 방식이면서도 Inline과 같은 강력한 효과를 내는 방식으로 작동합니다. 즉, Out-of-band 방식으로 기존 네트워크 구성 변경 없이 쉽게 구축이 가능하며, 더욱 안정적며 유연한 NAC 구현을 위해 Agentless 방식과 Agent 방식을 모두 적용할 수 있습니다.
Out-of-band 방식으로 인증 및 차단 패킷으로 인한 네트워크 부하최소화 및 네트워크 장비의 재구성을 하지 않아도 되게 하였습니다.
Agentless 방식의 경우, 특허 받은 가상 게이트웨이 방식으로 Inline처럼 강력한 보안 정책 집행이 가능합니다.
Agent 방식은 당연히 네트워크에 부담을 주지 않고 PC단에서 보안정책 집행이 가능합니다. 따라서, 어떤 경우에도 네트워크 부하 및 NAC서버의 부담을 최소화하여 네트워크 항상성을 유지합니다.

4. 검역, 격리와 종속 포털

네트워크 관리자는 보안에 문제가 없는 엔드포인트들만 내부망에 연결되길 기대하며 NAC를 도입할 것이다. (사용자들의 PC의 백신 업데이트 상태가 항상 최신이라면 NAC는 필요하지 않을 것이다.) 이때문에, NAC는 엔드포인트 를 격리하고 치료할 수 있는 메카니즘이 필요하다.

격리:

격리된 네트워크는 특정한 서버들로만 통신이 가능한 별도의 IP네트워크 영역을 말한다. VLAN 설정으로 격리된 네트워크 영역을 만들 수 있기도 하다.

NAC제품은 사용자 엔드포인트의 보안 업데이트 상태가 최신이 아닐경우 스위치 포트로 하여금 특정 VLAN으로 격리되게 오직 업데이트 서버로만 접근되도록 한다. VLAN방식으로 격리시 생기는 과부하를 피하기 위해 IP주소 관리 기술 ARP(Address Resolution Protocol) 또는 NDP(Neighbor Discovery Protocol)를 사용하기도 한다.

강제 웹화면:

엔드포인트 사용자가 HTTP 웹사이트로의 접근 시 강제적으로 특정 웹화면으로 이동킨다. 사용자들은 자신들의 컴퓨터를 어떻게 업데이트 되는지 이 웹 화면을 통해 확인할 수 있다. 엔드포인트가 보안 정책 수준을 충족할 때까지 강제 웹 화면 이외의 네트워크 사용은 금지된다.

이것은 일상 생활 속의 유료 Wi-fi 사용 법과 비슷하다. 유료 Wi-fi망과 처음 통신을 시도할 경우 자동으로 그 통신사 웹 사이트나 어플리케이션으로 가게 되어, 결제를 하거나 사용법을 볼 수 있게 되는 것이 하나의 예이다.

Tgate(티게이트) 에서는..

VLAN 차단 방식의 경우, 사내 모든 스위치 장비들이 VLAN을 지원해야 합니다. 모든 스위치가 VLAN을 지원하는 경우는 많지않아, 새로운 스위치 장비들로 네트워크를 재구성 해야 할 수 있습니다.

Tgate의 경우, 스위치 변경 또는 신규 구축과 같이, 기존 네트워크의 구성을 변경할 필요 없이 어떠한 네트워크 환경에도 바로 적용 가능합니다.

격리 및 검역 상태를 사용자에게 보여주는 UI의 경우, 위키피디아에서 언급된 강제 웹화면 방식과 Agent 소프트웨어가 더욱 사용자 친숙하게 보여주는 UI방식을 모두 제공하고 있습니다.

발췌 : 위키피디아
번역 : 미디어랜드 엔드포인트 연구소

NAC의 정의와 역사

NAC는 2005년 워싱턴 DC에 소재한 메리어트 호텔에서 열린 Gartner IT Security Summit 에서, 가트너사의 전문 컨설턴트인 로렌스 오랜스와 마크 니콜렛의 발표로 세상에 공유되고 전 세계적인 열기가 타오르기 시작합니다.

도대체 어떤 내용이었길래 불씨가 되었을까요?
아래 내용은 2005년 발표된 "Gartner' s Network Access Control Model" 을 기준으로 핵심적인 부분을 추려 재정리한 내용입니다.

무엇이 문제인가?

1. 현재 상태

보안 패치가 발표된 이후 공격자들은 빠르게 움직인다.
시스템의 약점을 바로 파악하여 악성 코드를 만들고 여러가지 방법으로 엔드포인트들을 공격한다. 반면, 기업의 보안 담당자들을 보안 패치 발표 이후 여러가지 방법으로 패치를 전사 PC에 배포 하려 하지만 마지막 PC까지 모두 보안 패치를 설치하기 까지는 상당한 시일이 걸린다.
보안 패치 및 약점이 발표된 이후 악성 코드가 공격을 감행하기까지의 시간은 점점 짧아지고 있다.

VPN을 통해 PC가 내부망에 접근하거나, 노트북이나 모바일 기기가 회사 네트워크에 접근할때, 방화벽이나 게이트웨이는 어떠한 보안 메커니즘을 제공하지 않는다.
특히, 협력사 또는 계약 직원이 집 또는 노트북을 이용하여 사내망에 접근할때, 패치 관리 시스템이나 백신을 이용한 보안 시스템들은 무용지물이 된다. 점점 증가하는 무선랜 환경은 이러한 문제점을 점점 더 가속시킨다.

2. 필요한 상태

이러한 피해를 줄이기 위해 기업들은 인증되고 검역이 된 단말들만 내부 망으로 받아드리고 오염된 단말들을 빠르게 내부 망과 단절 시켜놓을 시스템 구축을 해야 한다. 스캔과 차단이라는 두 기술을 접목 시킬 필요가 있다. 패치와 검사, 검역을 통한 오염된 단말들의 정화, 개인 정보 인증을 통한 내부 망 접속 허용이 같이 이루어 질 수 있는 솔루션이 필요하다.

NAC(네트워크접근제어)는 오염된 기기들이 내부 망에 접근을 못하게 하여 내부 망을 안전하게 지키는 역할을 한다.

NAC는 오염된 기기들이 내부 망에 접근을 못하게 하여 내부 망을 안전하게 지키는 역할을 한다. 접근하는 기기뿐만 아니라 연결되어 있는 기기들의 보안이 보안 정책에 맞는지 계속 확인하여 혹시나 발생할 수 있는 위협에 대비한다. 보안 정책을 만들때는, 보안 수준은 어느 정도가 되어야 하는지, 단말 정보, 접근 방법, 네트워크 제어와 검역에 대한 부분들을 명시하고 있어야 한다. 외부에서 접근하는 단말들

은 보안 정책에 따라 모든 접근이 가능한 경우, 검역이 필요한 경우, 접근이 불가능한 경우로 나뉜다. 검역이 필요한 경우, 혹은 접근이 불가능한 경우로 분류된 기기들은 보안 정책에 맞게 검역 또는 업데이트를 해야만 접근이 가능해진다. 그 후 내부 망에 맞도록 백신 업데이트, 패치, 기기 설정을 변경하여 접근시킨다.

3. NAC 구성 요소

RADIUS나 Kerberos같은 인증서버는 NAC의 주요한 구성요소이다.
이 인증서버는 사용자 식별/접근 관리 기능과 보안 관리기능(패치를 최신화 시키고, PC 환경 설정을 보안정책에 맞게 수정하고, 소프트웨어를 검역함)을 같이 수행할 수 있어야 한다. 이때, 사용자의 PC가 따라야 하는 보안 수준에 따라, 네트워크 접근 허용 단계를 구분한다.

PC의 보안 수준을 검사하는 방법에는 설치형 에이전트를 이용한 방식, 필요할 때만 작동하는 에이전트를 이용하는 방식, 네트워크에서 스캔을 하는 방식, 이렇게 세가지가 있다. 설치형 에이전트 방식은 관리 소프트웨어 사용자PC에 설치하여 지속적으로 검사하는 방법이다.

필요할 때만 작동하는 에이전트를 이용하는 방식은, 단말이 웹에 접근할 때 자바 애플릿이나 액티브X 컨트롤을 다운받아서 이용하는 방식이 방식이다. 이 방식은 SSL VPN을 이용하여 접속하는 외부 PC에 NAC를 적용할 수 있도록 한다. 세 번째 방법은 네트워크 인프라를 이용해 802.1X가 사용되는 유선 또는 무선 랜에서 접근 제어를 하는 방법이다. 802.1X가 사용되지 않는 경우에는 방화벽이나, 침입 방지 시스템 등이 사용된다. 기존의 보안 패치 관리 기술과 PC 환경 설정 관리 기술이 NAC에서 기기들의 보안 문제를 해결하는데 쓰여야 한다.

설치형 에이전트

장점:
- 관리되는 시스템 (기존 직원 PC등)을 위한 가장 효과적인 시스템
- 규칙적으로 시스템을 상세하게 스캔
- 접속 지연 시간 최소화
- 시스템 개선에도 쓰임
- 백신, 개인 방화벽, 패치 관리, NAC 기능에 맞는 설정관리
- PC 관리에 최적화

단점:
- 에이전트가 설치 되지 않을 경우 NAC관리 영역에서 벗어남
- 기기 사용자가 소프트웨어를 지웠을 경우 사용 불가

동적 에이전트

장점:
- 관리되지 않는 시스템 (방문객 PC, 개인PC 등등)을 위해 사용될 때 좋음

단점:
- 관리자 승인이 있어야 자세한 스캔가능(협조 필요)

네트워크 스캔

장점:
- 취약점 검사와 비슷
- 관리되지 않은 시스템을 검사하는데 좋음
- 에이전트가 있지 않은 시스템들 검사 가능

단점:
- 보안 패치는 할 수 없음
- 기기에서 나오는 통신을 제어 할 수 있는 다른 구성요소가 필요
- 스캐닝 전, 후, 중간에도 통신차단이 가능한 다른 요소가 필요

4. NAC필수 사항

기기가 네트워크 접근이 허용된 후, NAC(네트워크접근제어) 솔루션은 그 기기가 감염이 되었는지, 면역기능이 제대로 작동하는지, 혹은 수상하게 작동하는지에 대한 보안 체크를 해야 한다.
NAC가 더욱 더 널리 쓰임에 따라, 악성 소프트웨어들은 초기 스캔과 차단 과정을 피하고 네트워크에 접속되는 순간 실행 되도록 설계될 것이다. 만약 보안정책을 너무 강하게 설정해 놨다면 사용자들은 네트워크 접속 후 보안 기능을 비 활성화 시켜 보안정책을 피해가려 할 수도 있을 것이다.

모니터링

1. 상태 변화 감지: 기기에 설치된 NAC 소프트웨어 에이전트는 그 기기에 새로운 소프트웨어가 설치되거나 기기의 환경 설정이 바뀌었을 때 관리자에게 알려준다.

2. 네트워크 상태 모니터링: 모니터링 시스템은 변칙적이거나 감염이 된 것 같은 연결 고리를 감지해 낼 수 있다.

격리
웜 같은 위협은 네트워크 전반의 피해를 줄이기 위해 빠르게 격리 되어야 한다.

1. 구역 나누기: 보안 기기를 설치해 네트워크상에 구역이나 셀들을 나누어 문제가 있는 기기들은 즉시 네트워크에서 분리 시킨다.

5. NAC은 패러다임 전환

NAC에 대한 관심이 증가함에 따라, 많은 회사들이 NAC 배치 프로젝트에 구조적인 지원과 과정 계발에 투자를 했다. NAC를 계획하고 적용하는 것은 다양한 IT 지원이 필요하다. 보안 그룹은 보안 설정, 기기정보 그리고 접근 관리 정책을 수립 해야 하고, 프로젝트 그룹은 보안 정책을 최신화 시키는 방법을 만들어야 한다.
네트워크 부분에선 네트워크 격리를 할 수 있도록 네트 워크 분할을 해야 한다. 서버와 PC지원 팀은 관리 시스템에 새로운 프로그램을 배치 하거나 만약 NAC기능이 통합되어 있다면 존재하는 프로그램을 재설정 해야 한다. 격리된 기기들이 보안 수준을 맞출 수 있도록 하기 위해 PC지원 팀을 위한 프로세스가 정립되어야 한다.

추천하는 방법

1. 공격에만 신경쓰지말고, 약한 부분을 관리하기 시작하라
2. 우선 막고 패치를 나중에하라
3. 변칙적인 움직임을 빠르게 인지하고 격리시키거나 봉쇄해라
4. 항상 처음인 것처럼 검사해라
5. 첫 NAC 배치 때 위험성이 큰 시스템과 일반 시스템을 구분 하라
6. VPN과 다이얼 접속부터 시작하라
7. 관리되지 않는 시스템만 격리/차단 하는 방법도 고려해 보아라.

Tgate(티게이트) 에서는..

NAC가 탄생하게 된 배경은, 가트너 발표에서 언급한 대로, "보안 패치를 최대한 빨리, 가장 안전한 방법으로 전사에 적용" 해야 한다는 전세계적인 공감대가 있었기에 가능했습니다.

미디어랜드의 네트워크 접근 제어 솔루션 Tgate(티게이트)는 NAC의 본질에 충실하여, 보안패치가 발표되는 순간 최대한 빠르고 안전하게 전사 PC에 적용 될 수 있도록 설계되었습니다.

실시간 해킹을 탐지할 수는 없지만, 알려진 해결책(패치)만큼은 최대한 빨리, 확실하게, 전사 적용을 시킬 수 있습니다.

이것은, 엔드포이트를 통제/관리 하는 중앙 시스템만 고집스럽게 개발/판매 해왔기 때문에 가능했습니다.

가트너에서 언급된 대로 NAC는 PC 환경설정 관리 기술(TCO!stream), 보안 패치관리기술(TCO!hotpatch), 격리 기술(TCO!secuIP + Tgate)이 종합적으로 필요합니다. 미디어랜드는 이 모든 솔루션들을 전문적으로 개발/판매해 오고 있으며 Tgate(티게이트)에 최고의 기술들 만을 집약 시켜놓았습니다.

또한, NAC 구성 방식인 설치형 에이이전트 방식, 동적 방식, 네트워크 방식을 모두 지원하고 있으며, 회사의 요구에 따라 적합하게 사용될 수 있습니다.

NAC는 무려 10여년전에 발표되었으나, 영업적, 기술적 시행착오로 인해 아직도 격리/검사없이 PC를 사내망에 연결시키는 기업이 더 많습니다. 또는, NAC가 "인증을 하기 위한 솔루션"인 것으로 인식되어 소프트웨어 검사 및 치료는 전혀 하지 않은채로 NAC를 사용하고 있는 기업도 더러 있는 듯 합니다. 치료제가 확실히 있는데도 무관심 때문에 제때 적용을 못해서 일어나는 보안사고들 만큼은 하루 빨리 조치를 취해 우리나라가 더욱더 안전한 업무환경이 되길 바래 봅니다.

발췌 : "Gartner's Network Access Control Model
번역 : 미디어랜드 엔드포인트 연구소

[비교분석] NAC구현방법 및 통제방식

NAC(네트워크 접근제어)의 가장 핵심적인 부분은 바로 네트워크를 통제하는 방식 입니다.

NAC(네트워크 접근제어)의 가장 핵심적인 부분은 바로, 네트워크를 통제하는 방식 입니다.

모든 엔드포인트의 보안 수준을 최적화 하기 위해, 사내 네트워크에 접근하려하는 단말이 탐지되면 우선 격리 시켜놓은 채로 보안 검사를 해야하는데, 이때 어떻게 격리를 시키는 것이 가장 효율적인 방식인지가 관건입니다.

2006년도 한창 NAC(네트워크접근제어)가 붐이었을때, 하버드 대학과 앰허스트 매사추세츠 대학에서 공동 발표한 NAC 통제방식 비교 분석 자료를 토대로, NAC의 통제 방식에 대해 기업IT 관계자분들과 공유해보고자 합니다.

2013년 현재 판매/도입 되고 있는 NAC 솔루션들도 아래 기술들을 토대로 네트워크를 통제하고 있다고 보시면 됩니다.

본 비교 분석은, 이 당시 미국에서 출시되었던 약 30여개의 NAC 솔루션들의 통제방식을 기반으로 작성 되었습니다. NAC솔루션 제작 업체들은 아래와 같습니다.

*약 30여개의 미국의 NAC솔루션 제작 업체들

3com
Bradford
Cisco
Checkpoint
ConSentry
EndForce
Extreme
Enterasys
ForeScout
Full Armor
HP ProCurve
Impluse Point
InfoBlox
InfoExpress
Ipass
Juniper
Latis Networks
Lanscope
LANDesk
Lockdown Networks
Nevis
Nortel
Mazu Networks
Permeo
Q1 Labs
Reflex Security
Roving Planet
Seclarity
SenForce
Symantec
Vernier
Wave

1. 802.1x

802.1X 방식인 NAC 인증은 세가지 구성 요소가 있다.

Supplicant(인증받고자 하는 단말) : 유저 정보를 입력하고 인증결과를 받는 단말 클라이언트

Authenticator(인증 기기) : 이더넷 스위치, 무선 엑세스 포인트 같은 네트워크 기기를 말한다.

Authentication server(인증 서버) : 유저 정보를 판별하여 허가&불허가를 결정하는 인증서버(Radius)

〈차단방식〉

인증 기기는 보호된 네트워크의 경비원과 같은 역할을 한다. 인증 기기는 승인 되지 않거나 적합하지 않은 단말의 네트워크 접속을 막는다. 적합한 비자가 없으면 출입국 사무소를 통과할 수 없는 것과 같은 원리다.
단말이 정확한 ID/비밀번호나 증명을 인증기기에 전달하면 인증기기는 인증 서버에 확인 요청을 하고 승인된 단말이라면 사내 망에 접근을 시켜준다.

장점
· Windows 와 Mac OS 모두 지원한다
· 암호화된 통신을 한다
· 대부분의 AP와 스마트 스위치들이 지원한다.
· 안정적인 터널을 제공한다.

단점
· 승인 전에 보안상태를 스캔하는 절차가 없다.
· 스위치, AP, Radius 서버, 클라이언트는 EAP 타입(PEAP, TTLS)과 암호 타입(WEP, WPA,WPA2)을 지원해야만 한다.
· 가장 설치하기 어렵다.
· Windows가 지원하는 것이 제한적이다.
· 실패할 경우 기준으로 제시된 해결방법이 없다.
· 이 규격은 암호화는 행하지 않기 때문에 별도의 암호화를 채택해야 한다.

Tgate(티게이트) 생각

스위치 포트를 차단 하는 것은 매우 강력하고 우수한 방법입니다. 특히 802.1x의 경우 무선도 지원하는 차단방식이기 때문에 앞으로도 사내 환경에 더욱 많아질 무선 장비들을 고려하면 강점이 있습니다.

하지만 802.1x를 이용한 NAC 방식에는 큰 결점이 두가지 있습니다.

첫번째, 구축이 너무 어렵다는 것입니다. 모든 스위치가 802.1x를 지원해야 합니다. 따라서, 구형 스위치를 모두 교체해야 합니다.

두번째, 단말이 보내는 정보를 기준으로 인증만 한 후, 포트를 바로 엽니다. 보안 검사는 포트를 개방한 후에 합니다. 즉 신분 확인만 하고, 내부망에 연결되어서야 보안 검사를 하게 됩니다. "회사 보안 정책을 준수한 단말만을 연결시킨다"는 NAC의 취지를 고려한다면, 매우 약한 수준의 NAC입니다.

따라서, 802.1x로 NAC를 구축하게 될 경우에는 위 두가지의 일반적인 802.1x 단점이 잘 보완 되었는지를 확인할 필요가 있겠습니다.

2. VLAN

컴퓨터의 네트워크에서 여러 개의 구별되는 브로드캐스트 도메인을 만들기 위해 단일 2계층 네트워크를 분할할 수 있는데, 이렇게 분리되면 패킷들은 하나 이상의 라우터들 사이에서만 이동할 수 있다. 이러한 도메인을 가상 랜(Virtual LAN,VLAN)이라고 한다.

〈차단방식〉

VLAN을 이용해서 '허가' 된 네트워크 영역과 '비허가' 된 네트워크 영역을 만들어 접속하는 단말의 MAC주소를 DB와 확인하여 해당 단말을 '허가' 된 VLAN으로 할당시켜 주거나 '비허가' 된 VLAN으로 이동시켜 차단하는 NAC 방식이다.

장점
- 차단된 호스트들은 허가된 호스트들과 다른 VLAN으로 격리되기 때문에 **보안이 뛰어남**
- 우회하기가 어려움

단점
- **사내 모든 스위치 장비들이 VLAN을 지원해야함.**
- 장비 교체를 해야 할 경우, 많은 비용이 들어감
- 속도가 느림
- 허브나 VLAN 미지원 스위치들, 공유하고있는 포트, AP에서 작동하지 않음

Tgate(티게이트) 생각

VLAN 방식은 신규 단말 접근시 망을 분리하는 방식입니다. 따라서, 접근하는 장비들이 문제가 있다 하더라도, 신규 진입 장비들만 모여있는 망에서 문제를 일으키기 때문에, 기존 단말들을 신규 단말들로 부터 매우 안전하게 보호할 수 있습니다.

VLAN방식 NAC의 단점은, 회사 네트워크를 연결하는 스위치들이 모두 VLAN을 지원해야 한다는 점입니다. 이 부분은 802.1x를 지원하기 위해 모든 스위치가 802.1x를 지원해야 하는 것과 유사한 문제점 입니다. 또한 VLAN이 작동되도록 모든 스위치의 환경설정을 변환해 주어야 합니다.

따라서, VLAN 방식으로 NAC를 구축하게 될 경우에는, 전사 스위치의 호환성 부분이 잘 검토 되어야 하고 구축 시 필요한 환경설정 부분도 잘 검토 되어야 하겠습니다.

3. ARP

주소 결정 프로토콜(Address Resolution Protocol, ARP)은 네트워크 상에서 IP 주소를 물리적 네트워크 주소로 대응시키기 위해 사용되는 프로토콜이다. 여기서 물리적 네트워크 주소는 이더넷 또는 토큰링의 48 비트 네트워크 카드 주소를 뜻한다.

이를테면, IP 호스트 A가 IP 호스트 B에게 IP 패킷을 전송하려고 할 때 IP 호스트 B의 물리적 네트워크 주소를 모른다면, ARP 프로토콜을 사용하여 목적지 IP 주소 B와 브로드캐스팅 물리적 네트워크 주소 FFFFFFFFFFFF를 가지는 ARP 패킷을 네트워크 상에 전송한다. IP 호스트 B는 자신의 IP 주소가 목적지에 있는 ARP 패킷을 수신하면 자신의 물리적 네트워크 주소를 A에게 응답한다.

이와 같은 방식으로 수집된 IP 주소와 이에 해당하는 물리적 네트워크 주소 정보는 각 IP 호스트의 ARP 캐시라 불리는 메모리에 테이블 형태로 저장된 다음, 패킷을 전송할 때에 다시 사용된다. ARP와는 반대로, IP 호스트가 자신의 물리 네트워크 주소는 알지만 IP 주소를 모르는 경우, 서버로부터 IP주소를 요청하기 위해 RARP를 사용한다.

〈차단방식〉

IP Spoofing을 통하여 차단하고자 하는 단말의 ARP 테이블을 조작하여 차단하는 NAC 방식이다. 가령 인터넷을 사용하기 위해 게이트웨이의 MAC주소를 알기위한 ARP 요청을 보내면 그것을 감지하여 해당 게이트웨이의 MAC주소를 단말 자기자신이라는 응답을 하게된다. 이렇게 함으로써 단말은 게이트웨이의 주소를 자기 자신으로 알기 때문에 패킷이 나가지 못하고 고립되게 된다.

장점
- Layer3 독립적이다.
- 고정된 IP는 우회하지 않는다.
- 타임 아웃 없이 즉각적으로 고립시킨다.
- 가장 빠르다.
- 네트워크 인프라를 바꿀 필요가 없다.

단점
- ARP는 원래 이런 용도로 개발된 것이 아니다.
- 한 개의 네트워크 구역당 한 개의 장비가 필요하다.
- 디버그 하기 힘들다.
- 고정 ARP는 접근 가능하다.

Tgate(티게이트) 생각

네트워크 인프라의 변경 없이 가장 유연하게 NAC를 적용할 수 있는 방법입니다. 격리 속도가 가장 빠르며 구축 성공 확률이 큽니다. 유무선 모두 적용 가능하다는 것도 장점입니다.

ARP방식의 단점은 MAC과 IP의 변조가 가능하다는 것 입니다. 따라서 이를 방지하는 메커니즘이 반드시 필요합니다. 또한 발표 자료에 언급된 것 처럼 고정 ARP를 차단할 수 있는 체계도 따라와야 합니다.

따라서, 가장 구축 성공 확률이 크지만, 단점도 분명히 있는 만큼 이러한 문제점들을 잘 보완했는지에 대한 검토가 필요합니다.

Tgate(티게이트)는 Agentless NAC 구현을 위하여 이 방식을 취하고 있으며, 2006년 설계 초기 단계부터 위에 언급된 단점들을 인식하고, 변조할 수 없는 인증 메커니즘으로 설계되어 작동 되고 있습니다.
또한, 고정ARP가 접근 할 수 없으며, 기타 ARP방식에서 발생할 수 있는 취약점을 지속적으로 연구하며 방어하고 있습니다.

4. SW Agent

제조사에서 제공하는 에이전트를 제어하고자 하는 단말에 설치, 관리자가 관리하는 서버와의 상호작용을 통해 단말의 네트워크를 효율적으로 제어할 수 있다.

〈차단방식〉

각각의 모든 단말에 에이전트를 설치하는 NAC 방식으로 서버에서 차단정책을 설정하고 설치된 에이전트를 통해 네트워크를 차단한다. PC 자체에서 나가는 패킷들을 차단한다. PC 방화벽과 유사한 원리이다.

장점
· 원하는 단말에 정확하게 적용할 수 있다.
· 서버와 에이전트가 지속적으로 통신하기 때문에 안정적이다.
· 즉각적인 차단이 가능하다.
· 네트워크 특성에 구애받지 않는다.

단점
· 에이전트가 설치되어있지 않은 단말은 차단하기 어렵다.
· 모든 단말에 일일이 에이전트를 설치해야 한다.
· 사용자가 임의로 에이전트를 무력화 시킬 수 있다.

Tgate(티게이트) 생각

단말에 대한 제어를 가장 강력하게 구현할 수 있는 방법입니다. PC방화벽 방식으로, 문제있는 단말에서 패킷자체가 새어 나오지 않게 할 수 있으므로, 다른 네트워크 기반의 방식들 보다 격리 수준이 가장 강력합니다. 또한 세밀한 제어 및 모니터링이 가능합니다. 단순 초기 네트워크 제어 뿐만 아니라, 네트워크 접속 후에도 지속적인 관리 및 통제가 가능합니다.
다만, 소프트웨어 에이전트가 반드시 설치가 되어야만 가능하다는 점이 최대 단점입니다. 또한 사용자에 의해 에이전트가 무력화 되었을 경우에도 제어가 불가능합니다. 따라서, 강제적으로 에이전트를 설치시킬 수 있는 체계가 같이 수반되어야 하며, 에이전트를 보호 할 수 있는 방법도 강구 되어야 합니다.

미디어랜드는 지난 18년간의 지속적인 중앙 엔드포인트 통제/관리 시스템 연구를 통하여, 에이전트 소프트웨어에서 발생할 수 있는 수천가지 경우의 예외적으로 발생할 수 있는 이슈들을 해결해왔습니다. 단말에 소프트웨어 에이전트를 전사적으로 최단시간안에 장애 없이 설치 시키는 것은, 국내의 중간 관리자급 이상의 IT관리자 분이라면 미디어랜드의 기술력을 익히 알고 계시는 분이 많습니다.

에이전트 보호 기술 또한 오랜시간동안 기술을 축적해 왔으며, Tgate(티게이트) 에이전트에 에이전트 보호기술은 물론, 모든 최첨단 엔드포인트 기술을 집약 시켜놓았습니다.

이로써, 티게이트는 Agent 방식과 Agentless 방식을 합한 Hybrid NAC로 기업의 보안수준 및 네트워크 환경에 맞게 최적화된 솔루션을 제공하고 있습니다.

5. DHCP

동적 호스트 설정 통신 규약 (Dynamic Host Configuration Protocol, DHCP, 動的-設定通信規約)은 호스트 IP구성 관리를 단순화하는 IP 표준이다. 동적 호스트 설정 통신 규약 표준에서는 DHCP 서버를 사용하여 IP 주소 및 관련된 기타 구성 세부 정보를 네트워크의 DHCP 사용 클라이언트에게 동적으로 할당하는 방법을 제공한다.

DHCP는 네트워크 관리자들이 조직 내의 네트워크 상에서 IP 주소를 중앙에서 관리하고 할당해줄 수 있도록 해주는 프로토콜이다. 인터넷의 TCP/IP 프로토콜에서는, 각 컴퓨터들이 고유한 IP 주소를 가져야만 인터넷에 접속할 수 있다. 조직에서 컴퓨터 사용자들이 인터넷에 접속할 때, IP 주소는 각 컴퓨터에 반드시 할당되어야만 한다. DHCP를 사용하지 않는 경우에는, 각 컴퓨터마다 IP 주소가 수작업으로 입력되어야만 하며, 만약 컴퓨터가 네트워크의 다른 부분에 속한 장소로 이동되면 IP 주소를 새로이 입력해야 한다. DHCP는 네트워크 관리자가 중앙에서 IP 주소를 관리하고 할당하며, 컴퓨터가 네트워크의 다른 장소에 접속되었을 때 자동으로 새로운 IP 주소를 보내줄 수 있게 해준다.

〈차단방식〉

VLAN 차단방식과 비슷한데, '허가' 된 IP대역과 '비허가' 된 IP대역(ex. 사설 IP대역)을 만들어 접속하는 단말의 MAC 주소를 DB와 확인하여 해당 단말을 '허가' 된 IP대역로 할당시켜 주거나 '비허가' 된 IP대역의 IP를 할당시켜 차단하는 NAC 방식이다.

장점
- 적용하기 가장 쉽다
- DHCP는 발전이 다 된 기술이다
- 제조사에 상관없이 잘 작동한다.

단점
- 고정 IP를 사용하는 사용자에 대해서는 차단을 할 수가 없다.
- 우회하기 쉽다
- 새로운 주소를 할당 받을 때까지 시간이 오래 걸린다. 느리다.
- 침범에 대한 조절을 잘 못한다.
- 어떤 사용자가 감염되었거나 연결후에 사용자를 차단하는 정책이 필요한 경우 DHCP lease가 만료될 때까지는 해당 IP를 회수할 수 있는 방법이 없다.

Tgate(티게이트) 생각

DHCP를 이용한 NAC 구현 방법은 가장 간단하고 적용하기 쉬운 방법입니다. 다만, 전제조건이 따릅니다. 모두가 유동 IP를 이용하는 환경이어야 한다는 점이지요.

고정IP를 사용할 경우 너무나 쉽게 우회할 수 있기 때문에, 이 문제에 대한 보완이 없으면, 무력화하기가 쉬워 신중히 검토되어야 하는 기술 방식입니다.

[개인정보보호] 고객 DB 서버로의 통신 원천 차단하는 방법

금융권에서의 보안 사고로 인해 많은분들이 피해를 입었던 일이 엇그제 같은데 이번에는 대형 포탈사에서 보안 사고가 터져 사상 최대 규모의 개인정보가 유출 되었다고 합니다.

많은 전문가들이 지적하듯이 이번 사고는 해커들의 APT 공격(지능형 지속 해킹, Advanced persistent threat) 기법을 가장 큰 원인으로 지적하고 있습니다. 이 기법은 해커들이 우선 공격지/목표물이 정해지면 여러지 기법을 동원하여 오랜시간동안 천천히 타겟을 공격하는 방법이라고 합니다.

어느 곳에서도 가장 정확한 원인은 찾아내고 있지 못하고 있는 상황인것 같습니다만 대략적으로 유출 경로를 정리해 보면 내부 사용자의 PC관리 부주의를 틈타 PC 담당자들도 모르는 사이에 지속적으로 공격을 해온 것으로 추정되고 있습니다.

이는 IT전산 관련 내부 기술지원 담당자가 될수도 있고 개발자가 될 수도 있고, 또한 지난 사건에서 보듯이 외주 협력사 직원이 될 수도 있습니다.

물론 APT공격은 막을 수 있는 정확한 해결 방법은 알아내기 힘든 것으로 판단하고 있다고 하지만,내부 직원들의 PC에 악성코드가 침투하지 않도록 하는 보안 관리가 소홀했다는 점은 그냥 지나쳐 버리긴 힘들 것 같습니다.

원인이 될만한 직원 PC에서 수십개의 악성 코드가 발견되고 불필요한 동영상 파일들, 악성코드가 침투 경로가 되가 너무나 쉬운 P2P 프로그램등등이 발견되는 점은 어떻게 보아야 할까요?

실제로 조사에 의하면, 많은 기업에서 백신프로그램을 구매하여 사용하지만 실제로 백신이 정상적으로 구동되는 비율은 60%가 되지 않는다고 합니다. 이것은 사용자가 여러가지 이유로, 예를 들면 백신때문에 PC 속도가 느려진다고 판단하녀 백신을 지우거나, 최신 패치 업데이트가 번거로워서 하지 않는 등의 경우가 될 수 있겠습니다.

윈도우 패치도 마찬가지이겠지요. 그렇다고 일일이 패치 하라고 IT담당자들이 요청만 할 수도 없는 노릇입니다.

정리하면, “사람” 입장에서 보면 이번 사고는 관리 부주의로 인한 “보안정책 미준수” 가 큰 원인 중에 하나라고 할 수 있겠습니다.

이번에는 보안 대상을 조금더 구조적으로 분리하여 보겠습니다.
그동안에는 보안 시스템을 구축하고 신경써야할 부분을 “외부 보안” 에 많이 신경써 온 것이 사실입니다.
“외부 보안” 이라함은 외부 인터넷을 통해 내부 인프라로 공격하는 여러 위협 요소들에 대해 방어하는 것을 말합니다.

예를 들면 외부망에서 내부망으로 들어오는 길목에 설치하는 방화벽, IPS, IDS 같은 시스템들이 있겠네요.

실제로 중견기업 규모 또는 그 상의 기업에서는 대부분 이 부분에 대한 방어는 그동안 꽤 잘 해 오고 있는 것을 많은 곳에서 확인 할 수 있습니다.

하지만, 실제 내무망을 사용하는 임직원들의 PC에서 일어날 수 있는 보안 위협에 대해서는 거의 무방비 상태로 있는 것이 또한 많은 곳에서 확인할 수 있는 현실입니다. 임직원들의 PC또는 기타 단말 기기로 인해 벌어질 수 있는 위협을 막는 것을 “내부 보안” 이라고 합니다.

그런데 잘 살펴 보면, 최근 여러번 터졌던 보안 사고의 경로를 보면 해커들이 어렵게 방화벽,IPS,IDS 등의 철벽수비를 뚫고 들어오려 하는 것이 아닌, 내부 사용자의 PC에 여러 우회경로를 통해 침투하여 공격을 하는 행태를 확인할 수 있습니다.

바로 “내부 보안” 이 엄청 허술한 기회를 놓치지 않은 것이지요.

그럼 위와 같은 문제가 보완할 수 있는 최선의 해결책은 무었일까요?

바로 "내부 보안" 강화 입니다.
APT 기법을 연구하고 방지할 수 있는 방법이 꾸준이 선행됨과 동시에 기업은 "개인정보보호" 및 "고객DB보호" 를 위해 시스템적으로 내부 사용자들의 PC를 경유한 사고가 일어나지 않도록 대처해야 합니다.

우선 가장 먼저 해야 할 부분은 "서버 보안" 입니다.
아무나 들어오지 못하고 또한 아무나 특정 명령 (예를 들면 삭제 명령) 같은 것을 못하도록 대처를 해야 하겠습니다.
또한 접근을 시도하는 사람에 대한 접근 권한 및 DB 보안 등의 조치가 필요하겠습니다.

서버에 접근을 하더라도 권한이 없으면 작업을 할 수 없는 것이지요.

더 좋은 방법은 꼭 접근해야 될 사람 몇명을 제외 하고는 아예 고객DB서버로의 통신 자체가 안되도록 하는 것입니다.
흔히 예기하는 "Ping" 조차 가지 않게 하는 것 입니다.
서버 관계자도 아닌 임직원이 불필요하게 같은 통신 영역(내부망)에 있다는 이유만으로 서버로 통신이 될 이유가 없기 때문입니다.
통신만 가능하다면 해커는 어떻게든 들어올 방법을 찾을 것 입니다.

이렇게 "Ping" 이 가능한 내부 사용자들을 불필요하게 많이 두어서 해커가 공격할 수 있는 확율을 높여둘 필요가 있을까요?

정리해 보겠습니다.

1. 꼭 필요한 관계자만 고객 DB서버와 통신"Ping"이 가능하게 한다.
2. 통신 가능한 관계자의 PC가 무결한지 확인한다.
   (불필요한 P2P프로그램 같은 것은 없는지, 백신 및 윈도우 패치 상태는 최신인지 등)
3. 서버에 통신이 가능한 담당자라 하더라도 "인증" 절차를 통해 꼭 필요한 "권한"만 부여한다.
4. DB 자체에 대한 보안 조치를 취해 놓는다.

위의 조치가 위의 보안 사고를 완벽히 방지할 수 있는 100% 확실한 해결 방법은 아닙니다.
하지만 현재 업계에서 상당히 간과하고 방치되고 있어 보안 사고의 원인을 제공하고 있는 것만큼은 확실합니다.
특히, 불필요한 내부 직원의 고객DB로의 통신 원천 차단하는 방법~ 어떻게 생각하시나요?

NAC 10분만에 이해하기

복잡한 기능보다 손쉬운 필수 기능이 '중요'

NAC
TECH
GUIED

네트워크접근제어(NAC)는 접근하는 모든 기기를 검사, 악성 코드에 감염되거나 기업 보안정책에 따르지 않는 기기를 차단함으로써 네트워크의 안전을 담보하는 솔루션으로 정보보안의 새로운 패러다임으로 관심을 끌고 있다. 하지만 NAC의 복잡성은 여전히 기업 담당자를 괴롭히는 상황이다. 손쉬운 NAC에 대해 3회에 걸쳐 알아본다.

"NAC 너무 복잡하고 어렵다." 최근 기업 보안 및 관리를 담당하고 있는 현업 담당자들의 푸념 섞인 목소리들이다.

기업 보안의 새로운 패러다임으로 화두가 되고 있는 NAC이지만, 관심을 갖고 막상 알아보려 하면 공부해야 할 내용이 상당하다. NAC솔루션을 제공한다는 업체도 한 둘이 아니고, 각 업체에서 제안하는 NAC 구현 방법도 가지각색이다. 기업 보안 업무에 있어서 NAC 아니고도 신경 쓸 것들이 많은데 과연 이렇게까지 시간 투자를 해서 도입할 가치가 있는 것인지 고민하며, 도입 검토 엄두도 내지 못하고 있을 담당자들의 표정이 눈에 선하다.

이런 담당자들의 어려움을 덜어주고자, 단순히 3분 정도 분량의 글을 읽는 것만으로도 NAC 검토에 필요한 필수 지식을 쉽고 빠르게 이해할 수 있도록 3편의 글을 연재한다. 첫 시작은 NAC 개념 및 올바른 구현 방법이며, 다음으로 구축 방법과 비용을 절감할 수 있는 방법에 대해 차례로 알아보겠다. 그럼 이번 편에서는 도대체 NAC가 무엇이길래 관심을 가져야 하는 것인지, 어떻게 구현하는 것이 맞는 방법인지 알아보자.

NAC는 출입국관리소다

지난해 봄부터 한 해가 끝나기까지, 전 세계는 신종 인플루엔자 A(H1N1), 즉 초기 '돼지독감'으로 알려진 바이러스성 질병으로 한차례 큰 홍역을 치렀다. 국내에서도 감염된 사람이 만명을 넘었으며 사망자도 10여명을 넘겼다.

초기 미주 지역에 방문했던 수녀를 시작으로 외국인 강사들 집단 감염, 초등생 집단감염, 그리고 나중에는 연예인 감염까지 한 해 내내 떠들썩했다. 다행히 타미플루라는 치료제가 효과가 있는 것으로 알려지면서 급한 대로 불은 껐지만 타미플루만으로는 근본적인 해결이 될 수 없었다. 이에 정부는 뒤늦게나마 인천공항 등 출입국 심사가 있는 곳에 검역을 강화했다. 외국에서 인천공항에 도착했을 때를 회상해

보면, 검역 담당 직원들이 온도계를 귀에 대고 체온을 측정하고, 입국 심사장으로 걸어가는 동안에도 여러 개의 감지 센서로 지나가는 승객들을 한차례 더 온도 측정을 했던 것으로 기억한다.

NAC는 바로 이 공항에서 출입국관리소가 하는 업무와 매우 닮았다. 더 정확히 얘기하자면, 보호해야 할 대상이 국가 자산이냐 아니면 기업 IT자산이냐 정도의 차이는 있지만, 입국 심사와 거의 똑같다고 할 수 있다. 입국 심사가 국내로 들어오려는 사람이 사회적 범죄를 일으킬 사람이거나 병균을 퍼트릴 사람인지 또는 문제를 일으킬 만한 물건을 들여오는 것은 아닌지를 확인함으로써 국민을 보호하고 국내 산업에 피해가 가지 않도록 확인하는 것이라면 NAC는 사내망으로 들어오려는 단말기, 또는 사람은 누구인지, 단말기가 사내 네트워크를 마비시키거나 다른 단말기들을 오염시킬만한 잠재적 요소가 있는지를 확인함으로써 사내 네트워크, 서버, 데이터, 및 사내 망에 접속되어 있는 단말기들을 보호하는 역할을 한다.

"NAC, 입국심사와 같다"

땅은 한국 땅이지만 사실상 한국이 아닌 제3의 DMZ같은 영역인, 입국심사대의 풍경을 다시 한 번 되돌아보자. 경찰복 비슷한 유니폼을 입은 심사관들은 들어오려는 사람이 내국인인지, 외국인이지를 판단하고 문제가 있는 사람은 아닌지 확인한다. 또 여러 검역 담당관들은 신종 플루 의심 환자인지를 판단하기 위해 여러 방법으로 체온을 측정한다.

▲ 출입국검사. NAC는 공항의 출입국관리소가 하는 역할과 매우 비슷하다.

NAC가 하는 역할도 같다. 내부 직원이던 외부직원이던 유선랜을 PC에 꽂거나 무선랜으로 사내망에 접속했을 때 NAC는 우선 이 사용자들의 PC를 DMZ존으로 격리시켜 놓는다. 그리고 사내망으로 들어오려는 PC가 등록이 된 PC인지, IP 또한 사용해도 되는 등록 IP인가를 확인한다. 또 PC가 백신이 설치돼 있는지, 최신 패턴이 업데이트된 백신인지, 보안 패치도 최신 업데이트돼 건강한지 등을 확인한 후 이 모든 검사에 합격했을 경우에 사내망으로 접근을 허용한다.

종종 기업 보안 담당자들은 백신 소프트웨어를 사용하고 있고 패치관리시스템(PMS)가 있는데 NAC가 왜 필요하냐고 반문하는 경우가 있다. 비슷하지만 확연히 다른 이유를 입국심사 컨셉에서 다시 확인할 수 있다. 핵심은 바로, 입국심사를 통과하기 전까지 내외국인들은 땅은 한국땅이지만 한국이 아닌 엄연히 분리되고 격리된 DMZ 존에 있다는 사실에 있다. 간단해 보이지만 엄격한 이 심사를 통과하지 못하면 외국인들의 경우에는 실질적인 한국땅에 한 발짝도 못 디딘 채 바로 본국으로 송환될 수 있는 것이다.

기존의 백신 및 PMS에 의존한 보안 관리의 가장 큰 문제점을 예로 들어 보면, 신종플루에 걸린 내 외국인이 특별한 심사 없이 바로 한국땅에 들어와서 전국 방방곡곡을 돌아 다니다가 뒤늦게 감염 사실이 발견돼 찾아다니면서 신분확인도 하고 타미플루로 치료해주는 개념이라고 보면 되겠다. 잠재적으로 문제를 일으킬 수 있는 단말들을 다른 영역으로 격리시키지 않고 방치했을 때 생기는 문제점은 기업 보안 담당자라면 필자가 이 지면을 할애하지 않더라도 충분히 가늠해볼 수 있을 것이다. 지금까지는 백신이 보안의 대명사로 인식됐지만 타미플루만 갖고 신종플루를 근본적으로 해결할 수 없었듯 사전 차단 방식의 NAC가 필수적인 보안 컨셉으로 등장했다.

스마트 사내망 보안, 'NAC'

보안에 있어서 망분리는 큰 의미가 있다. 공공기관이나 몇몇 기업 연구소는 아예 물리적으로 내부망 사용 전용 PC와 인터넷용 PC를 분리시켜 놓고 사용한다. PC 두 대를 따로 쓰는 불편함을 감소하고라도 인터넷 등 외부로부터의 감염 가능성을 원천 차단하겠다는 의지이다. 최근에는 가상화를 통해 한 PC에서 다른 두 개의 망을 사용하는 기술까지 등장하고 있다.

오늘날 '스마트폰', '스마트워크' 등이 화두가 되면서 똑똑하고 효율적으로 일하자는 움직임이 산업전반에 걸쳐 일어나고 있는데 NAC 또한 '스마트 사내망 보안'이라고 할 수 있다. 물리적으로 PC를 두개를 배치해 망분리해 운영할 필요없이 PC가 내부망에 접속하기 전에 일단 별도의 DMZ 망에 격리시켜놓고, 접속하려는 자가 누구인지, 건강한지를 철저히 확인한 후에 안전하다 판단되면 내부망 사용을 허용하는 것이다. 또한 내부망에 들어온 이후에도 주기적으로 검사해 감염이 의심되는 즉시 다시 별도 DMZ망으로 재격리시킨다. 혹시 단순 인터넷만 사용하길 원하는 외부 방문자의 경우에는 이 별도 DMZ망에서 인터넷만 사용 가능하게 하면 된다. 이는 추가적으로 인터넷만 사용하게 하는 별도의 PC를 배치하는 개념과 크게 다르지 않다.

출입국 관리소에서 인증과 검역은 둘 모두 필수다. 약 50년 전으로 돌아가서 국제공항을 처음 만든다고 가정해보자. 해외 공항을 한 번도 가보지 않은 담당자가 공항을 만든다고 한다면 입출국 심사 절차가 필요한 것인지 수하물 검사는 해야 하는 것인지 잘 모를 수 있을 것이다. 현재 NAC를 도입하는 담당자들이 그런 경우라고 볼 수 있겠다.

현재 NAC 시장에서는, 인증만 해도 NAC고, 검역만 해도 NAC고, 둘 다 해도 NAC이니 고객이 원하는 만큼만 하면 된다는 식의 허울만 좋은 형태로 NAC가 제안되고 도입되는 것을 종종 볼 수 있다. 명절마다 공항이 해외여행객으로 북새통일 정도로 해외 경험을 한 국민이 많아진 오늘날에 누군가가 "인천국제공항에서 출입국 검사만 하고 수하물 검사는 불편하니 하지 맙시다"라고 주장한다면 납득할 만한 사람이 과연 얼마나 될까.

모든 길은 출입국 관리소로 통한다.

현재 기업 보안 담당자가 검토해야 할 NAC 구현 기술은 너무 많다. 이것은 시장의 리더가 시장 형성에 실패했기 때문에 초래된 결과다.

최근 거의 매일 같이 그 성공사례가 언급되고 있는 아이폰을 예로 들어보자. 만약 애플이 아이폰을 지금 같이 혁신적으로 사용이 간편하고 예쁘게 만들지 못했다면 오늘날 스마트폰 시장은 어땠을까? 구글 안드로이드는 만약 애플 아이폰을 만나지 않았다면 현재의 경쟁력 있는 모습으로 만들 수 있었을까? 삼성이 이렇게 빨리 스마트폰을 제조하려 했을까? 아이폰이 실패했다면, 아마 스마트폰 시장도 현재의 NAC 시장과 같이 여러 업체들이 각자의 기술적 강점만을 내세우며 시장을 다양하게 분산시켜 놓아 선택을 어렵게 하면서 느린 성장을 이어갔을 것이다.

대형 네트워크 장비 업체가 초기에 제안했던 네트워크 장비 기반의 NAC 프레임워크는 기술적 컨셉이 잘못됐다기보다는 현실적 환경에 맞지 않았다고 볼 수 있다. 외부 공격보다 내부에서의 관리 소홀로 보안 사고가 빈번했던 문제를 정확히 짚어내고 이를 해결할 수 있는 방법으로 NAC를 제안했을 때는 업계로부터 폭발적인 호응을 받았다.

하지만 이익을 추구하는 기업이라는 태생적 한계에서 벗어나지 못하고 주력상품 중 하나인 스위치 기반의 기술을 제안했고, 초기 NAC 시장은 이 방법이 정석인 것처럼 이해하고 받아들였다. 나아가 달궈지기 시작한 NAC 시장에서 가능성을 보고 신규 진입한 기업들 또한 같거나 비슷한 방법으로 제작된 솔루션을 판매하거나 이 스위치 기반 NAC 프레임워크와 호환되도록 제품 구성을 했다. 이것이 무엇이 문제였는지를 우선 알아보자.

▲ 비행기 게이트. 유선이든 무선이든 스위치 기반의 NAC 구현방식과 관련이 있다.

출입국 관리소는 적재적소의 길목에서 완벽한 제 기능을 해야 한다. 다시 신종플루 이야기로 돌아가 보자. 만약 입국 심사를 현재같이 공항 메인 터미널 건물에서 한꺼번에 하지 않고, 더욱 철저한 심사를 위해 내외국인들이 비행기에서 내리는 순간에 이를 수행한다고 가정해보자. 그곳도 국내로 들어오는 입구라고 말할 수 있으며, 아무 문제없이 확실히 이행될 수 있다면 이 방법은 매우 훌륭한 방법일 수 있다.

하지만 조금만 더 생각해 보면 이 방법은 구축비용이나 운영 측면에서도 매우 비싼 방법임을 쉽게 알 수 있다. 일단 수적인 면부터 생각해보자. 우선 게이트마다 약 둘 셋 정도의 심사관을 배치하고, 체온 감지 센서의 배치도 요구된다. 인천국제공항의 경우, 게이트 수는 약 40개 이상에 달하는데, 모든 게이트에 신분 심사관 및 체온 측정 센서기를 각 2개 이상씩 배치하기 위한 비용은 대략적으로만 생각해도 상당할 것임을 예상할 수 있다. 나아가 항공사들 중에 만약 게이트에서 특정 요구 조건을 내세우는 곳이 있다거나 체온 측정기가 고장이라도 날 경우에는 이를 처리 해결하기 위한 운영비용 또한 적지 않을 것이다.
이는 무선이든 유선이든 스위치 기반 NAC 구현 방식의 문제이다. 출입구처럼 보이는 곳을 모두 막겠다는 것이다. 언뜻 보면 가장 확실히 문제를 해결하는 듯 보이기에 기업 보안 담당자가 처음 들었을 때는 그럴듯하게 들렸을 수 있다. 약간 의심을 했더라도, 스스로 전문가임을 자처한 업체들이 영업적으로 설득하고 시장을 드라이브하고 있는 상황이라면, 기업 입장에서는 실제 구매해 운영 해보기 전까진 그 실상을 파악하기 힘들 수밖에 없다.

물론 기업내 모든 스위치들이 수문장 역할을 하면서 어떤 문제없이 명령을 잘 듣고 유무선으로 접속하려는 PC들을 확실히 제어한다면 매우 훌륭할 것이다. 하지만 현실적으로 이는 쉽지 않거나 효율적이지 않다.

모든 입구를 막을 필요는 없이 꼭 필요한 적재적소에 통제소를 배치해 놓으면 되는 것이다. 밖으로 나가기 위해 어차피 지나갈 터미널 출구 이전 길목에서 한 번에 검사하는 것이 투자비 및 운영 비용 측면에서 모두 각 비행기 게이트에서 실시하는 것보다 훨씬 비용효율적임은 자명한 사실이다.

인천국제공항의 경우에는 메인 터미널로 나가기 전 입국 심사장 한곳에만 확실히 신분 심사 및 검역을 하면 되며, 다른 국제공항들도 마찬가지이다. NAC를 도입하려는 회사의 경우도 동일하다. 서울 본사에 하나, 다른 네트워크를 사용하는 지방 사무소에 각각 하나씩만 놓으면 된다. 이렇게 되면 초기 투자뿐 아니라 운영 측면에서도 엄청난 비용을 절약할 수 있다.

출입국 관리소는 스스로 운영돼야

실제로 인천국제공항에 가보면 입국 심사관들이 직접 심사를 하는 곳 옆에 서너대의 자동 입국 심사기가 설치돼 있다. 필자도 사용해 본 적이 있는데 심사관들 앞에서 길게 서거나 혹시 모를 걱정 때문에 심사관과 눈을 마주치며 긴장할 필요 없이 여권과 지문 한 번씩 스캔만 하면 되기에 여간 편리한 게 아니었다. 심사관도 덜 바쁘고, 입국하는 사람도 편하고 시간을 대폭 절약할 수 있는데 이렇게 좋은 것을 이제야 도입했나 싶었다. 자동 입국 심사기를 관리하는 책임자는 등록되지 않은 입국자가 발견될 경우 격리시키고 당일 담당자에게 보고시키게 했을 것이라고 쉽게 짐작할 수 있었다.

▲ 자동 출입국심사기. NAC는 기능이 많다고 좋은 것이 아니라 우선 사용이 매우 쉬워야 한다.

NAC는 단순히 보안을 강화해주는 보안용 단말기 관리도구가 아니다. 간단하게 몇 가지 정책만 하달받으면 알아서 작동하는 시스템으로, NAC에게 일을 시켜놓고 바쁜 보안 담당자는 더 중요한 업무에 집중할 수 있다. 쉽게 말해 "백신 최신 업데이트 꼭 하세요.", "IP 주소 함부로 바꾸면 안됩니다", "외부 방문자는 함부로 회사 네트워크에 접속하면 안 됩니다"라고 안내해놓고 지켜지지 않을까 전전긍긍하는 하는 것이 아니라 NAC 시스템이 알아서 위의 일들을 처리하고 다른 더 중요한 업무를 보다가 가끔 정기적으로 이상이 없는지 확인하며, 문제발생시에만 보고를 받으면 된다. 이렇게 운영하려면 우선 사용이 매우 쉬워야 한다.

기능이 많다고 더 좋은 것이 절대로 아니다. 현대인은 피곤하다. 신경 쓸 것들이 너무 많다. 애플은 쓸데 없는 기능을 최대한 줄이고 꼭 필요한 핵심 기능을 쉽게 사용할 수 있게 함으로써 아이폰이라는 초대박 상품을 만들어 냈다. 컴퓨터를 잘 쓸 줄 모르는 50대 60대 아주머니들도 아이폰은 사고 싶어 한다고 한다.
기업용 소프트웨어도 마찬가지다. 기능이 많으면 훨씬 더 잘 쓰고 유용할 것 같지만 절대 그렇지 않다. 대부분의 직장인들이 거의 매일 사용하는 마이크로소프트 워드, 파워포인트 같은 오피스 제품을 보면, 그 수많은 기능들을 모두 알고 잘 사용하는 사람은 많지 않다. 달리 보면, 필요하지도 않고 사용하지도 않는 그 수많은 기능이 탑재된 오피스를 쓰기 위해 기업이나 개인이 지불한 비용은 적절하지 않다고 말할 수 있다.

NAC 시스템 또한 많은 기능을 가지고 있을 필요가 없다. 너무 많은 기능은 사용 방법을 어렵게 할 뿐이다. 오토 방식의 차를 사용하는 운전자에게 매뉴얼 방식의 차를 운전하라 하면 약간의 부가적인 기능만 더 있을 뿐인데도 무척이나 어려워하는 것을 보면 알 수 있다. 사용자는 간단하게 명령하고 시스템은 스마트하게 알아서 움직여야 한다.

지금까지 NAC가 무엇인지, 어떤 기술이 올바른 것인지, 그리고 어떤 특징이 있어야 하는지를 알아보았다.
NAC는 '입국 심사' 와 같은 간단하면서 필수적인 개념이며, 적재적소에 하나만 있으면 충분하고, 간단한 명령 만으로도 스스로 잘 작동하게 해야 한다. 다음호에서는 '1주일만에 NAC 구축하기' 를 통해 간단히 NAC 구축방법에 대해 알아보도록 하겠다.

이원규 | 미디어랜드 기획팀장
qlee66@medialand.net
네트워크타임즈 기술기고

NAC 1주만에 구축하기

[NAC] 간단한 정책·정확한 타깃·스마트한 판단 '필수요소'

NAC는 '입국심사' 와 같은 간단하면서 필수적인 개념이며, 적재적소에 하나만 있으면 충분하고, 간단한 명령만으로도 스스로 잘 작동하게 해야 한다는 점이 핵심이다. 이번 호에서는 'NAC 구축이 너무 복잡하고 어렵다' 라는 인식의 전환을 돕기 위해 NAC 를 회사에 구축할 때 꼭 알아야 할 핵심 포인트에 대해 쉽게 이야기해 보고자 한다. 그리고 1주일이라는 설정 하에 도입에서부터 구축할 때까지 꼭 짚고 넘어가야 할 포인트들에 대해서 알아보겠다.

우선 NAC를 구축할 때 꼭 알고 있어야 하는 기준이 되는 개념이 있다. 이 개념들만 잘 숙지하고 있으면 설령 어려운 상황이 발생한다 하더라도 수월하게 올바른 판단을 내릴 수 있다. 나무 기둥이 튼튼하면 바람이 아무리 불어도 쓰러지지 않는 것과 같은 이치로 만약 이 핵심 개념을 잘 이해하지 못하고 NAC 구축을 진행한다면, 상사나 동료 또는 솔루션 업체들이 하는 한 마디 한 마디 말에 흔들리게 돼 더딘 구축 또는 최악의 경우 구축 실패까지 초래할 수 있다.

따라서 세 가지 핵심 포인트는 매우 중요하며, 이 세 가지 핵심 포인트만 알고 있으면 NAC를 구축할 준비가 됐다고 말할 수 있다.
세 가지 핵심 포인트는 첫째가 '정책은 간단해야 하고 통제는 강력해야 한다' 이며 둘째는 '타깃이 정확해야 한다' 다. 그리고 마지막 세 번째 핵심포인트는 '스마트하게 판단하고 강력하게 추진해야 한다' 이다.

간단한 정책, 강력한 통제

첫 번째 핵심 포인트는 '정책은 간단해야 하고 통제는 강력해야 한다' 이다. 다양한 곳에서 사용되기에 정책이라는 단어가 포함하는 의미가 어렵게 느껴질 수 있겠지만 NAC에서 말하는 정책은 간단하다. 지난호에서 언급했던 인천국제공항의 입국 심사장으로 가보자. 입국심사에 적용되는 정책은 매우 간단해 대부분의 승객들이 이해하고 있다. 바로, 내가 누구인지를 검사하고 내가 어떤 소지품을 가지고 들어오려 하는지 심사해 아무 문제가 없을 경우에 입국을 허가한다는 것이다. 또 이것은 국가 및 국민을 보호하기 위한 필수 과정이라는 것이다.

정책이 모두 이해할 수 있을 정도로 간단하지 않고 복잡할 경우, 정책을 내리는 책임자와 정책 운영 담당자, 그리고 승객 모두 정책에 대한 이해가 어려워 각각의 접점에서 혼돈이 초래된다. 이의 결과는 입국 시간이 길어질 뿐만 아니라 국내를 방문하는 외국인으로부터 이미지가 실추될 수 있다. 이처럼 사람에게 직접 영향을 미치는 보안 정책은 그 목적 및 방법이 모두가 이해할 수 있을 만큼 쉬워야 한다.

NAC 정책도 마찬가지로 매우 간단해야 한다. 가장 큰 이유는 내부 외부 직원에게 직접적인 영향을 미치기 때문이며, 이에 보안 정책을 만드는 사람, 운영하는 사람, 영향을 받는 PC를 이용하는 직원 모두 그 정책의 목적 및 방법에 대해서 쉽게 인지할 수 있어야 하는 것이다. 물론 사람의 의견은 다양하기에 해당 정책에 공감 또는 이해하지 못하는 사람들이 있기 마련이겠지만 적어도 그 목적과 방법은 알기 쉬워야 한다.

예를 들면, '우리회사는 누가 회사 네트워크에 접속하는지를 모니터링하고 사내 네트워크를 사용자로부터 보호하기 위한 시스템을 운영합니다. 모든 직원은 사내망 접속시에 로그인을 해야 하며, PC보안 상태가 최적화돼 있지 않을 경우 사내 네트워크 사용이 불가능할 수 있습니다.' 와 같은 정책이다. 회사 환경에 따라 약간 다를 수 있겠지만 NAC 정책은 이렇게 단순해야 모든 관계자가 같은 생각으로 NAC 구축에 동참할 수 있다.

하지만 사용방법이 쉽고 기능이 단순하다고 해서 구현 방법까지 쉬운 것은 아니다. 예를 들어 최근 몇 년 전 히트를 친 닌텐도 Wii나, 여전히 화두가 되고 있는 아이폰의 경우, 그 사용 방법은 누구나 이해할 수 있고 즐길 수 있을 정도로 간단하지만, 그 안에 녹아 들어가 있는 기술은 최첨단이다.

NAC의 경우도 마찬가지다. PC 사용자 입장에서 보면 웹메일이나 포털 서비스를 사용할 때 항상 하는 같은 로그인 절차처럼 보이지만, 그 안에는 IP 관리 기술, 데스크톱 관리 기술, 패치 관리 기술 등이 모두 유기적으로 녹아 있어야 한다. 대부분 보안 업체가 NAC의 컨셉에만 매료돼 자사가 보유한 특정 기술을 토대로 한 NAC를 제공하면서 제공 못하는 기술들은 제 3자 솔루션을 사용하면 된다고 한다. 하지만 다른 솔루션들을 연동할 때 유기적인 연동이 가능한지 잘 살펴봐야 한다. 실제로 아무리 대형 업체라 하더라도 써드파티 솔루션과 유기적인 연동을 제공하기는 쉽지 않은 까닭이다.

기구축된 솔루션과의 호환성도 고려해야 할 부분이다. 이미 많은 기업들이 DMS나 IPMS 같은 솔루션들을 도입해 사용하고 있다. NAC는 PC관리나 제어, 그리고 IP와 뗄 수 없는 깊은 연관이 있기에 기존에 구축돼 있는 이러한 시스템들을 잘 활용해야 한다. 스위치와 같은 네트워크 장비를 기반으로 하는 NAC의 경우, 기존에 구축된 네트워크 장비들을 이용하면 활용도가 높을 수 있지만, 지난호에서 언급했듯 스

위치 호환 관련 문제나 성공 스토리를 잘 검토해 봐야 한다. 나아가 실제 도입을 검토하다 보면 PC 사용자의 편의성 문제도 고려하지 않을 수 없다. 대표적인 경우가 기존에 구축된 다른 목적의 기업 솔루션, 예를 들어 싱글사인온(SSO) 등이 이미 로그인을 요구하고 있을 수 있다는 점이다. A 솔루션 때문에 로그인 한 번 하고, B 솔루션 때문에 한 번 다시 하고, C솔루션 때문에 또 로그인해야 한다면, 그만큼 업무 효율성이 떨어질 수밖에 없다. 이러한 장애물 또한 NAC를 통해 유기적으로 해결돼야 할 부분이다.

다시 입국 심사장으로 돌아가서 통제 이야기를 해보자. 입국 심사는 정책은 매우 간단한 반면에 통제는 매우 강력하다. 문제가 있는 인물이거나 허가되지 않은 물품을 들어오려 하는 것이 감지됐을 경우 강력하게 입국을 차단하고, 재심사, 벌금 또는 추방해야 한다. 만약 통제가 허술하다면 입국 심사 자체의 존재 가치가 떨어질 것이며, 국민 또한 불안해 할 수밖에 없다. 만일 총기류나 마약과 같은 물품들이 강력하게 통제되지 않을 경우 많은 사회적 문제를 일으킬 수 있는 것이다.
이와 같이 NAC의 통제도 강력해야 한다. 문제가 있는 경우에도 통제가 안되면 NAC의 도입 목적 자체가 무의미해진다. 따라서 인증되지 않은 사람이나 PC상태가 회사가 원하는 기본적인 보안 상태를 유지하고 있지 않다면, 강력하게 차단해야 한다.

물론 처음에는 불편할 수 있다. 해외로 출국하려 할 때 보안 검색대가 어떤 통제를 하는지 모르는 사람은 로션, 치약, 물과 같은 크게 문제되지도 않을 것 같은 액체 물품류를 갖고 갔다가 검색대에 가서야 보안요원들의 요구로 바로 버려야 하는 어처구니없는 경우를 경험하고 화가 날 수도 있다. 하지만 한 번 경험한 사람은 액체류는 큰 가방에 넣어 화물칸으로 보내거나 꼭 필요한 경우 검색대를 통과한 후 게이트 근처 터미널에서 구입 하는 방법 등으로 자체 대응해 문제없이 바로 통과할 수 있다. 또 검색대 통과를 기다리는 줄이 너무 길어서 탑승 시간을 놓치게 되어 여행 및 출장 일정을 망쳤다고 화를 내는 사람도 있을 수 있다. 하지만 출입국관리소는 이러한 사람들 때문에 검색대를 없애거나 검색 강도를 낮추지 않는다.

이와 마찬가지로 NAC 도입도 처음에는 이런 불만이 있을 것을 예상해야 한다. 그리고 이에 대처하는 의연하고 주관있는 자세 또한 갖추고 있어야 한다. 자주 해외여행이나 출장을 가는 사람에게는 입국 심사 때 검색대 통과하는 장애 정도는 큰 문제가 되지 않는 것처럼 NAC에 대한 인식이 정착되면, 오히려 NAC를 도입하지 않고 사내망을 운영하는 회사들을 보게 되면 되려 걱정스런 눈으로 보게 될 것이다. 마치 옆 동료가 백신 없이 컴퓨터를 사용하는 것을 보면 걱정되듯 말이다.

〈그림 1〉 간단한 정책과 강력한 통제

정확한 타깃

두 번째 핵심요소는 '타깃이 정확해야 한다' 는 점이다. 여기서 타깃은 사용자 PC를 지칭한다. 결론부터 말하면 사용자, PC, IP, MAC이 정확히 일치해야 한다. 이는 강력한 통제와 같은 맥락으로, 강력한 통제를 하려면 정확한 사용자와 그 PC를 파악하는 것이 전제조건이다. 특히 NAC는 네트워크 접근 차단이라는 수단을 이용해 통제하기에 타깃이 정확하지 않으면 엉뚱한 사람이 사내망을 통한 업무를 못하게 되는 결과를 초래할 수 있다.

예를 들어 A라는 협력사 직원이 사내망 네트워크를 접속하려 할 때 인가되지 않은 사용자라 판단해서 차단했는데 그 타깃 PC가 B라는 내부 직원의 것이라면, B라는 직원은 영문도 모른 채 갑자기 업무를 못하게 될 수 있다. 또 보안상 문제가 있는 A라는 PC가 발견돼 해당 PC에 매칭되는 IP주소가 X라는 것을 알고 차단했는데 결과적으로는 B라는 PC가 차단된다면 이 또한 엉뚱한 사람이 일을 못하게 되는 문제를 초래하게 된다.

IP관리 기술력 및 노하우가 타깃을 정확히 일치시키는데 큰 역할을 한다. 바로 정확한 장비 인증을 가능케 하기 때문이다. 수시로 변경되거나 변조될 수 있는 IP와 MAC 정보를 일치시킴과 동시에 로그인을 통한 PC 사용자 계정 정보 또한 일치시킴으로써 항상 타깃이 정확히 일치되도록 유지시켜준다. 간단해 보이는 기술이지만 정확한 타깃은 매우 중요한 요소이기에 실제 NAC 도입에 있어서는 이 분야에 오랜 시간 동안 여러 회사를 통해 그 전문성 및 안정성이 검증된 업체를 잘 판단하는 것도 큰 도움이 될 것이다.

다양한 환경의 PC로부터 정확한 필수 소프트웨어 설치 정보를 추출할 수 있어야 한다. 보다 확실한 검역을 위해서는 어떠한 형태로든 PC에 소프트웨어가 설치돼야 하며, 이때 정확한 소프트웨어 및 하드웨어 정보를 추출해 낼 수 있는 안정적인 프로그램 솔루션이 필요하다. 조언한다면 고도의 기술력보다는 다양한 플랫폼의 PC를 안정적으로 자산관리해온 솔루션을 잘 검토해 보는 것이 장기적인 안목에서 도

움이 될 것이다.
마지막으로 윈도우 패치 및 백신 패치의 설치 현황을 파악하고 업데이트 해주는 PMS 기술력 또한 중요 검증 포인트다. 패치 없이는 어제의 PC 보안 상태와 오늘의 보안 상태가 같다고 할 수 없다. 얼마나 자주 패치돼야 하느냐는 보안 담당자의 견해에 따라 다르겠지만 최신의 패치가 업데이트돼야 함은 분명하다. 위의 기술력에 보태 PMS 기술력까지 갖춘 솔루션이라면 보다 안정적인 시스템 운영이 가능할 것이다.

〈그림 2〉 정확한 타깃

'스마트' 한 판단과 강력한 추진력

어떤 솔루션이던 현명하게 선택해야 하겠지만, NAC의 경우는 보다 스마트하게 도입 여부와 방법을 판단해야 한다. 우선 경제적으로 이득이 되는지 잘 판단해야 한다. NAC는 네트워크 차단을 다루는 솔루션이기 때문에 PC를 사용하는 직원 입장에서 보면 업무상 불편이 따를 수 있기에 도입 자체가 조심스러운 것이 현실이다. 일 잘하는 것과 보안을 놓고 단순 비교하면다면, 이윤을 추구하는 기업이라는 주체의 특성상 당연히 일 잘 하는 것이 중요하다. 하지만 비용적인 측면을 세밀하게 따져 본다면 보면 이야기는 달라진다.

먼저 도입 비용을 생각해보자. 시스템 솔루션의 경우 잘만 도입하면 10년 이상 사용할 수 있다. 보수적으로 생각해서 3년 정도 사용한다고 했을 때의 예상 솔루션 구매비용을 우선 생각할 수 있다. 이에 더해 사내망 접속 시, 로그인 및 PC 보안 수준 미달로 네트워크 접속 차단됐을 때의 업무상 불편한 정도에 대한 비용도 포함시켜야 한다. 마지막으로 솔루션의 기술적 장애에 의한 네트워크 차단으로 인한 업무상 장애를 생각해 볼! 수 있으며, 기타 회사 환경에 따른 추가 비용들도 고려해야 한다.

반대로 도입하지 않았을 때 비용을 생각해보자. 가장 눈에 보이는 큰 비용은 바로 기존 타 시스템의 운영 효율성 증대 효과를 포기하는 비용이다. NAC는 강력한 사용자 및 장비 인증으로 거의 100%에 가까운 자산관리를 가능케 한다. 비싼 비용을 들여 도입한 백신 또한 거의 완벽히 설치 및 운영시킬 수 있다. 큰 비용을 들여 도입했을 PMS 또한 거의 완벽하게 설치·운영할 수 있다. 필수 소프트웨어 및 불법 소프트웨어도 강력하게 관리할 수 있다. 큰 비용을 지불하고 도입했지만 PC단의 설치가 완벽하지 않아 보안 취약점으로 남아 있어 그 도입 효과가 의심될 수 있을 여러 솔루션의 가치를 살려 줄 수 있는 것이 바로 NAC로, 도입하지 않았을 때는 10~20% 정도의 백신, PMS, DMS 운영 효율성을 높일 수 있는 기회비용을 포기하는 것과 같다.

다음은 관리 비용을 생각해 볼 수 있다. '백신 끄면 안 됩니다', '최신 업데이트 항상 하세요', '관리자 허가받고 사내망을 써야 합니다', '불법 소프트웨어 설치하면 안! 됩니다' 등등 관리자가 신경 쓰고 해야 할 직접 해야 할 인건비 및 같은 시간에 다른 더 중요한 일을 했을 때의 기회비용을 추가할 수 있겠다.

마지막으로, 가장 예측하기 어렵지만 파장이 적지 않은, 백신 및 필수 소프트웨어/패치 미설치로 인한 잦은 장애 비용도 생각할 수 있다. 이런 장애 발생시 PC 사용자의 업무 지연은 물론 IT담당자의 시간 비용이 발생한다. 나아가 누가 사내망에 접속하는지 관리가 안 됨으로써 핵심정보가 유출될 경우의 수도 고려해야 한다. 내부 사용자PC 관리 부주의로 인한 보안 사고가 전체 보안 사고의 20% 이상인 점도 고려 요소다. 물론 NAC 도입만으로 내부 정보 유출을 방지할 수는 없다. 하지만 회사 대문 또는 뒷문이 잠겨있을 때와 열려 있을 때의 도둑이 침입할 확률 정도를 계산해 보면 답은 쉽게 나온다.

경제적인 판단 후에는 기술적으로도 NAC의 역할에 대해 정확히 판단해야 한다. NAC는 다양한 관리 솔루션들과 밀접한 관련이 있다. IPMS, DMS, PMS 등의 관리 솔루션, 백신과 SSO같은 시스템과도 연관이 있다. 따라서 종종 관리자들은 통합이라는 이름 하에 모두 한꺼번에 되는 솔루션을 찾기도 한다. 하지만 각각의 전문성을 가진 솔루션들을 하나의 콘솔 또는 하나의 시스템으로 운영 또는 도입하는 것은 무리가 있을 수도 있고 전문성이 현저히 떨어질 수도 있으므로 주의해야 한다.

예를 들어, 직장인들이 가장 많이 사용하는 마이크로소프트 워드, 엑셀, 파워포인트의 경우 각각의 전문적인 기능이 있는 소프트웨어다. 하지만 누군가 업무용 프로그램들은 하나로 '통합' 돼야 한다고 하고 각각 프로그램들을 따로따로 실행하는 것이 번거로워 하나의 콘솔 프로그램으로 돼야 한다고 어떨까. 전문 프로그램간의 유기적 연동이 더 중요하며, 잘못된 통합은 피해야 할 것이다.

'스마트' 한 ROI 분석으로 도입이 결정됐다면 도입 추진은 강력해야 한다. 중소기업의 경우, 적은 규모의 인력들이 NAC 운영을 함께 맡아서 하겠지만 큰 회사의 경우 네트워크팀, 보안팀, PC 관리팀 등으로 세분화돼 있을 수 있다. 이런 경우 각 부서의 이해관계 때문에 전체적인 효과를 보지 못해 NAC 구축에 실패할 가능성이 있다. 그러나 일단 그 효용성에 대해 최고 책임자가 판단이 섰다면 각 부서 및 이해 관계자들을 잘 설득해서 강력하게 추진해야 한다. 최고 책임자의 강력한 의지 없이 진행될 경우에는 구축 후에도 작은 불만 하나 둘에 어렵게 도입한 솔루션 운영이 쉽게 포기되거나 무너질 수 있다. NAC 구축은 반드시 해야 하는 시스템이라는 인식이 확고할 때 성공할 수 있다.

〈그림 3〉 NAC = 기존 시스템 성능 향상

1주일 만에 NAC 구축하기

지금까지 NAC 구축에 앞서서 꼭 알고 있어야 할 핵심 포인트 세가지에 대해 알아보았다. 이번에는 약 1주일을 기준으로 구축에 필요한 팁들에 대해 알아보도록 하겠다.

1단계(약2일) – 구축 시나리오 구상

구축이 결정되면 어떻게 구축을 진행할 것인지 구상해야 한다. 네트워크 현황을 재점검하고 어떤 순서로 진행을 할 것인지 일정 점검을 한다. 다음은 보안 정책 점검을 확실히 해야 한다. NAC를 사용하는 기본 개념은 비슷하겠지만 회사마다 어떤 소프트웨어들을 필수 소프트웨어로 사용할 것인지, 꼭 설치시킬 것인지 아닌지, 백신의 최신 버전을 얼마나 강력히 설치시킬 것인지 등등을 확립한다.

점검이 끝나면, 기존 시스템과 연동할 필요가 있는 것들이 어떤 것이 있는지 결정해야 한다. 로그인에 필요한 인사 DB 및 직원에 대한 정보는 어디에서 연결해 쓸 것인지, ID/PW는 어디서 가져다 쓸 것인지, 또는 새로 생성할 것인지 등을 잘 판단해야 한다. 기존에 이미 도입하고 사용하고 있는 SSO, 백신, PMS, DMS, 매체제어 등의 솔루션이 있다면 그 효과를 증대시키기 위해 유기적으로 연동시키는 방안에 대해서도 점검할 필요가 있다. 더불어 구축전 사용자에게 미리 공지 및 홍보를 충분히 해 구축시 발생되는 사용자 불편을 최소화해야 한다. 공지시에는 혹시 발생할 수 있는 장애 상황일 경우에 어떻게 사용자가 직접 대처할 수 있는지도 잘 안내해야 한다.

2단계(약2일) – 구축 시작 및 단계별 적용

구축에 있어 가장 먼저 해야 할 작업은 타깃을 정확하게 일치시키는 작업이다. 우선 부서별 혹은 영역별로 가장 먼저 적용할 곳과 순차적으로 적용할 곳을 선정한다. 가장 먼저 적용할 곳부터 장비를 통해 IP 정보를 스캔, 타깃과 비타깃을 구분짓는 것이 우선이다. 타깃이 정해지면 설치유도를 통한 에이전트 설치로 PC자산정보와 IP정보를 정확하게 매칭시킨다. 다음은 패치관리 솔루션 설치 또는 연동을 통해 패치가 가능하게 한다.

첫 부서의 설치가 완료되면 정책을 적용시켜 본다. 내부 직원, 공용PC, 외부 방문객 PC 등 각 사용자 타입별로 미리 컨설팅 단계에서 정한 시나리오대로 사용자 인증이 잘 되는지 테스트를 해본다. 다음은 네트워크가 차단된 상태에서 검역이 잘 되는지를 확인하는 단계다. 백신, 윈도우 패치, 필수 소프트웨어 등의 설치 또는 미설치 상황이 잘 나타나는지와 검역이 끝난 PC의 경우, 정상적으로 네트워크 사용을 승인받았는지를 확인하면 우선 NAC의 기본 기능은 잘 되는 것임을 알 수 있다. 부수적으로 부서별, 직급별 권한 관리 기능을 적용할 수 있겠지만 이것은 회사 환경마다 많은 차이가 있어 세부적 조정이 필요하다. 정책이 잘 적용되는 것이 확인된다면 다음 부서에 같은 순서로 작업해 전사 적용이 될 때까지 진행한다.

3단계(약2일) – 모니터링 및 완료

NAC 구축이 완성 된 후에는 전체적으로 이상이 없는지 확인한다. 우선 콘솔상에 나타나는 통계, 보고서상에 이상이 없는지 점검한다. 하루 동안 모니터링하고 큰 이상이 없으면 구축 완성 결과를 책임자에게 보고한다.

현실적으로는 테스트 과정은 적어도 1주 이상 잘 지켜봐야 한다. 본편에서는 이해를 돕기 위해 1주라는 가상의 시나리오로 이야기했지만 회사 환경 및 새 시스템을 도입하는 업무 처리 문화에 따라 다양한 시간이 걸릴 수 있다.

이번 편에서는 NAC 구축에 있어서 꼭 알아야 할 핵심 포인트 세 가지에 대하 알아보고 간단하게 구축 과정에 대해 알아보았다. ▲정책은 간단하고 통제는 강력해야 한다 ▲타깃은 정확해야 한다 ▲도입 검토는 '스마트'하게 판단하고 추진은 강력해야 한다 등이 바로 NAC 구축의 세 가지 핵심 포인트다. 다음호에서는 보안 제품 도입시의 가장 큰 고민인 '비용'을 최대한 줄일 수 있는 방법에 대해 알아보겠다. 어떻게 하면 최소 비용으로 NAC 구축/운영을 할 수 있는지에 대한 정보를 통해 많은 보안/네트워크 담당자에게 도움이 되기를 기대해 본다.

이원규 | 미디어랜드 기획팀장
qlee66@medialand.net
네트워크타임즈 기술기고

NAC 도입은 반드시 성공해야 한다

부서간 원활한 협업체계 구축 '필요조건'

지난 2회에서는 NAC 구축에 있어서 꼭 알아야 할 핵심 포인트 세 가지에 대해 알아보고 간단한 구축 과정을 제시했다. 핵심을 다시 정리하면 ▲정책은 간단하고 통제는 강력해야 한다 ▲타깃은 정확해야 한다 ▲도입 검토는 '스마트'하게 판단하고, 추진은 강력해야 한다 등이다.

지난 2회를 통해 NAC가 무엇인지, 또한 구축시 핵심 포인트는 무엇인지를 이해했으니, 이번 마지막호에서는 보안 솔루션 도입 시 가장 큰 고민인 '비용'을 최대한 줄일 수 있는 노하우를 알아보고, 3회에 걸친 'NAC 쉽게 이해하기' 연재를 마무리 하고자 한다.

지금부터 알고자 하는 최소 비용으로 구축/운영하는 노하우는 NAC 솔루션 업체와 거래를 잘 해서 가장 저렴한 가격을 쟁취할 수 있는 방법에 대한 얘기를 하려는 것이 아니다. NAC 솔루션은 보안을 관장하는 중요한 시스템이다. 컨셉을 잘 잡아야 하고 조금 거창하게 말하자면 IT 컨설팅에 의해 도입돼야 할 필요가 있는 시스템인 것이다. 다시 말해 성능에 큰 차이가 없어 단순히 가격만 비교하면 되는 사무용 가구나 집기같은 것이 아니기에 가격 위주로 저렴한 제품을 도입했다가는 최소 몇 년간 쓰라린 경험을 할 수도 있다.

최소 비용으로 NAC 구축/운영을 이룰 수 있는 핵심 노하우를 먼저 제시하면 첫째 '반드시 성공해야 한다', 둘째 '중복 투자를 피해야 한다', 셋째 '운용하기 쉬워야 한다', 넷째 '첫째,둘째 그리고 셋째 노하우를 절대 잊지 않는다' 등으로 요약할 수 있다.

NAC는 실패할 수 있다

NAC 도입은 반드시 성공해야 한다. 실패할 경우 그 피해 비용은 단순 도입 비용뿐 아니라 도입을 위해 관계자들이 투자한 정신적, 시간적 비용의 낭비란 문제가 추가로 발생한다. 레퍼런스가 있는 이름난 업체의 솔루션을 도입을 하는데 성공/실패를 운운하는 것이 이상하게 생각할 수 있을 것이지만, NAC는 구매했다고 해서 반드시 기대했던 대로 잘 작동하고 잘 사용할 수 있는 것이 아니다.

간단히 말해 NAC는 실패할 수 있다. 이것은 주관적인 의견이 아니며 단순히 우리나라 만에 국한된 문제도 아니다. 전 세계적으로 많은 기업들이 NAC 도입 실패를 경험했다. 유명 IT전문 글로벌 매체도 다음과 같은 제목의 NAC에 대한 기사를 내보내 왔다. "Is NAC dead?", "NAC, not Dead yet". NAC 자체가 실패냐 아니냐를 운운하고 있는 것이다. 실패 경험이 나오는 배경에 대한 의견들도 다양하다.

NAC 도입에 있어 가장 큰 비용은 바로 '실패 비용'이다. 야심차게 큰 비용을 들여 NAC를 구축했다가 실패했을 때 비용은 단순히 구매 비용만 고려하더라도 상당히 크다. 도입시에 솔루션 업체와 거래를 잘 해서 10%, 20% 저렴하게 구매하는 것과는 비교도 안 된다. 전 직원에게 영향을 미치는 시스템인 만큼 실패했을 경우 IT 부서에 대한 신뢰도 역시 낮아질 수 있다. 새로운 시스템을 구매하려 해도 실패 비용의 여파때문에 재도입하는데 시간이 걸릴 수밖에 없으며, 그 기간 동안에 보안은 타사에 비해 취약해질 수밖에 없다. 게다가 시간적 비용 등을 고려한다면, 실패비용은 가파르게 증가하게 된다.

〈그림 1〉 NAC 도입 사례

따라서 '성공 사례'를 꼭 확인해야 한다. 특정 솔루션 도입을 고려할 때 현재 많은 보안 담당자들은 실패를 피하기 위해 레퍼런스를 참고하고 있다. 솔루션 업체들 또한 홍보할 만한 레퍼런스를 만들기 위해 최선을 다한다. 그만큼 레퍼런스는 중요하다. 하지만 여기서 반드시 확인해야 할 사항이 있다. 그것은 바로 '도입 사례'와 '성공 사례'는 다르다는 점이다. 누구나 알 만한 업체가 도입했다고 해서 반드시 성공했다고 말하기 어렵다. 또한 레퍼런스가 많이 있다고 해서 반드시 좋은 솔루션은 아니다.

사실 이름난 기업일수록 실패 사실이 알려지길 꺼려 한다. 따라서 도입을 고려하고 있는 기업의 담당자들은 특정 회사가 솔루션을 구매했는지, 안 했는지만 알 수 있을 뿐, 잘 사용하고 있는지, 또는 사용하길 포기했는지의 여부는 알기 힘들다. 다시 강조하지만, 실패했을때의 비용은 너무 크기 때문에 NAC 도입을 고려하는 담당자는 꼭 '성공 사례'를 알기 위한 노력을 게을리 해서는 안 될 것이다.

나아가 담당자가 NAC를 정확하게 알아야 한다. 그동안 SI 업체나 국내외 솔루션 업체가 제품을 판매하기 위해 잘못된 환경을 조성하고, 컨설팅함으로써 기업이 도입된 시스템을 잘못 사용하는 경우를 종종 볼 수 있다.

NAC는 특히 내부 보안의 컨트롤 타워 역할을 해야 할 솔루션인 만큼 기업 내 담당자가 기본 컨셉을 알아야 한다. 아무리 솔루션 업체가 전문성 있는 벤더라 하더라도 담당자는 어떤 것이 올바른 컨셉인지 정도는 이해하고 판단할 줄 알아야 한다.

각 제품들의 세세한 기능까지는 알 수도 없고 알 필요도 없겠지만 장기적인 안목으로 어떻게 NAC를 구성하고 동작돼야 하는지에 대한 컨셉만큼은 확실히 알고 있어야 한다. 그래야만 실패하지 않는다. 단순히 솔루션 업체에게 맡기는 식의 NAC 도입이라면 차라리 안하는 것이 낫다. 기다렸다가 NAC도입을 훌륭히 성공한 업체가 나왔을 때, 그 때 따라하더라도 늦지 않다. 성공하는 NAC는 스마트하고 강한 의지가 있는 담당자의 노력에 달려있다.

기존 솔루션 대체 아닌 '활용·통제'

NAC는 기존의 내부 PC 관리 및 보안 솔루션과 밀접한 관계가 있다. 그것은 NAC의 태생 자체가 치료할 수 없었던 문제를 해결해 주는 혁신적인 새로운 보안 제품이 아니라, 기존에 있는 보안 및 자산 솔루션의 도입 효과를 최대한 증대시켜 확실히 통제하자는데 그 목적을 두고 있는 까닭이다.

회사 내부 솔루션을 함부로 사용 못하게 하는 사용자 인증 시스템도 이미 존재해 왔고, 내부망 외부망을 분리하는 시스템도 있다. 안티바이러스, 자산관리 솔루션, IP관리 솔루션, 패치관리 솔루션도 이미 시장에 등장한 지 꽤 됐다. 하지만 아무리 위의 솔루션들을 잘 써도 취약점은 존재하고 그 효과를 모두 누릴 수 없기에 강력한 통제 시스템을 마련, 기구축 솔루션들의 역량을 최대한으로 끌어 올려야겠다는 아이디어가 창출됐으며, 이것이 NAC인 것이다. 그리고 이러한 NAC는 그동안 '관리'라는 패러다임을 '통제'라는 새로운 개념으로 바꾸는 계기가 되고 있다.

NAC의 역할은 기구축된 시스템을 '통제'하는 것이다. NAC가 백신 소프트웨어를 대체할 수는 없으며, 전문 IP관리 솔루션을 대체할 수도 없다. 마찬가지로 전문 자산관리 솔루션을 대체할 수도 없고, 전문 패치관리 솔루션을 대체할 수도 없다. NAC는 이를 대체하는 것이 아니라 위의 솔루션들을 통제하는 시스템이기 때문이다.

〈그림 2〉 비용효율적인 NAC 투자

하지만 현실은, 솔루션 업계들이 경쟁을 하고 상품화에 힘을 쓰다 보니 위의 모든 관리 기능을 모두 수행할 수 있는 것이 NAC 솔루션으로 인식이 돼 버린 양상이다. 많은 NAC 제품들 또한 위의 기능들이 조금씩 모두 되는 형태로 개발돼 판매되고 있고, 가격도 자연스레 모든 기능들의 개발 비용이 녹아들어간 가격으로 형성되고 있다.

기구축된 솔루션들은 고유의 중요한 역할과 가치가 있다. 다시 한 번 강조하지만, NAC는 기존의 내부 보안 및 자산관리 시스템의 성능을 향상시키고 앞으로 도입할 시스템들이 확실히 모든 단말에 적용되도록 하는 강력한 지휘자 역할을 하는 시스템이다. NAC란 것이 기존에 구축된 엔트포인트 보안 및 관리 시스템의 역할을 모두 다 해주는 만능 시스템이 아니란 얘기다.

따라서 기존에 구축된 관련 시스템들이 이미 있는 상황에서 NAC 솔루션을 도입한다면, NAC 본연의 역할에 전문성이 있는 것인지를 살펴보고, 이미 도입돼 사용되고 있는 기능들이 제안된 NAC 제품에 포함돼 있는 것은 아닌지를 꼼꼼히 따져 봐야 한다. 많은 대기업, 중견기업 및 공공기관들의 경우에는 이미 엔드포인드 보안 및 관리 솔루션들이 하나 이상 갖춰져 있을 것이다. 빈약한 각각의 기능들이 모두 포함돼 있는 솔루션이 아닌 NAC 기능을 확실히 하는 솔루

션을 잘 찾는 것만으로도 중복투자를 피하고 적절한 가격에 NAC를 도입할 수 있을 것이다.

손쉬운 운용, 비용절감 '지름길'

운용상에 들어가는 비용은 원하는 기능을 적용하는데 요구되는 시간이다. 사용법이 어려우면 우선 정책을 내리기가 힘들어진다. 또한 정책 적용 방법이 간단하지 않으면, 정책이 잘 못 반영될 수 있다.

NAC는 단순한 관리 시스템이 아니라 '통제' 시스템이기 때문에 정책이 정확히 내려지지 않을 경우에는 큰 혼란을 초래할 수 있음은 꼭 기억해야 한다. 간단히 말해 정상적으로 일을 할 수 있어야 하는 직원의 업무를 마비시킬 수 있다. 이 경우 각각 직원들의 업무 마비로 인한 손해 비용 및 관리자가 문제를 해결하기 위해 투자해야 할 시간 등을 모두 비용으로 환산하면 그 크기는 엄청나다.

가능한 직관적으로 사용할 수 있어야 한다. '트레이닝 코스트(Training Cost)' 라는 용어가 있다. 특정 기기나 제품을 사용하고, 익숙해지는데 필요한 시간 및 비용을 말하는 것이다. 하버드 비즈니스 스쿨 프레스에 기고한 UC버클리 대 칼 샤피로 교수의 'Information Rules' 이란 글에 따르면, 윈도우가 80~90%에 가까운 시장 지배력을 가지고 매킨토시가 10% 이상의 시장 점유율을 극복하기 힘든 원인이 바로 이 트레이닝 코스트에 있다고 한다. 이미 대부분의 사용자들이 윈도우 환경에 익숙해져 있고 쉽다고 느끼기 때문에 다른 인터페이스를 제공하는 OS에 거부감을 느끼고 또 새로운 시스템을 사용하고 익숙해지는데 시간이 걸릴 뿐 아니라 다른 OS에 대한 거부감 또한 생각보다 크다는 것이다.

NAC 역시 마찬가지다. 시스템 관리자 또한 UI나 그 사용법이 직관적이지 않으면 잘 쓸 수 있는 기능도 활용 못 할 수도 있고, 또한 통제를 잘 하지 못해 문제를 일으킬 수 있으며, 이러한 우려 때문에 사용이 꺼려질 수도 있는 것이다.

〈그림 3〉 NAC 고속도로(내부보안 인프라)

첫째, 둘째 그리고 셋째 노하우를 절대 잊지 않는다.

앞서 언급한 세 가지 노하우는 NAC 도입에 있어서 비용을 최소화하기 위해 너무나 중요한 원칙이다. 이 가운데 특히 '반드시 성공해야 한다' 는 '중복투자를 피야야 한다' 와 '운용이 쉬워야 한다' 를 모두 포괄하는 가장 중요한 원칙이다. 성공 여부가 너무나 중요한 이유를 다시 종합 정리해 얘기하자면, NAC는 바로 '내부 보안 인프라' 기 때문이다. 앞서 언급했듯 기존의 백신, 패치 관리 솔루션, 자산관리 솔루션, 내부망 사용자 관리 등을 확실히 하기 위한 내부 보안 인프라인 것이다.

NAC가 제대로 구축, 정립되면 향후에는 NAC라는 인프라 위에서 앞으로의 엔드포인트 보안 솔루션들이 컨트롤될 것이며, 그 대상은 데이터유출방지(DLP) 솔루션일 수도 있고 불법소프트웨어 방지 솔루션이 될 수도 있다. 그 이외의 어떤 새로운 엔드포인트 보안 솔루션이 나온다 하더라도 NAC 위에서 통제될 것이다. 이러한 상황을 가정한다면 NAC 인프라 투자가 실패할 경우는 심각한 문제가 야기됨을 알 수 있다.

여기에 한 가지 더 첨언한다면 성공적 NAC를 위해서는 부서간 긴밀한 협조가 절대적으로 필요하다. 대기업의 경우 NAC와 관련이 있는 부서나 담당자가 다수 존재하게 된다. NAC는 내부보안 인프라기 때문에 백신을 관리하는 조직, 자산관리를 담당하는 조직, IP를 관리하는 조직 등등과 협의를 피할 수 없다. 각각 시스템의 '관리' 는 계속 유지하더라도 '통제' 권은 NAC에 넘겨야 하기 때문이다. 하지만 각각 부서의 이권을 고려하다 보면 NAC는 절대로 될 수가 없고 도입되더라도 실패할 가능성이 크다. 각 부서의 협의를 끌어 낼 수 있는 강력한 리더의 의지가 반드시 있어야 한다.

1회에서 예로 들었던 출입국 심사장의 경우에도 마찬가지다. 입국 심사는 법무부가 담당하고, 항공 및 수하물은 건교부가 담당하고, 치안은 행자부 소속의 경찰이 담당한다. 위 인프라를 구축하려는 국가의 강력한 의지와 부서간의 긴밀한 협조가 없었다면 공항에서의 국가보안은 이뤄지지 않았을 것이다.

마지막으로 솔루션간 유기적 연동을 언급하고 싶다. NAC는 단독 솔루션이 아닌 여러 엔드포인트 보안/관리 솔루션을 관장하는 인프라이다보니 기존 시스템 및 앞으로 추가 도입할 시스템들을 유기적으로 연결시킬 수 있어야 한다. 때에 따라서는 이기종간의 연동을 위해 커스터마이징이 필요할 수도 있다.

이러한 이유로 기업 환경에 따른 커스터마이징을 고려해 빠른 지원이 가능한 NAC 솔루션을 추천한다. 커스터마이징 비용은 특성상 개발자의 인건비를 수반하기 때문에 추가 비용이 발생할 수 있다. 기존 시스템에 대한 커스터마이징뿐 아니라 새로 도입하게 될 수 있는 시스템에 대한 연동도 고려한 유지보수 계약도 체결하는 것이 중요하다.

지금까지 NAC가 무엇이고 올바른 기술은 어떤 것이며, 구축시 꼭 알아야 할 핵심 포인트 및 비용을 최소화하기 위한 노하우들을 알아봤다. 3회에 걸친 연재가 기업 CEO 또는 보안 담당자들이 NAC에 대해 쉽게 이해하는데 도움이 됐기를 바라며, 'NAC 너무 어렵고 복잡하다' 라는 푸념섞인 목소리 또한 조금 줄었기를 희망한다.

이원규 | 미디어랜드 기획팀장
qlee66@medialand.net
네트워크타임즈 기술기고

네트워크에 의한 논리적 망분리
성안의 성, 두개의 성문

Two gates

Tgate
티 게 이 트

Tgate는 네트워크에 접속하는 모든 기기들을 보안 정책에 따라 강력히 통제해 인증과 검역을 통과 했을 때만 내부망까지 접근하게 허용해주는 네트워크 보안 솔루션입니다.
사내망을 안전한 내부망과 완충지대 역할을 하는 외부망으로 분리하는 논리적 망분리 기술을 통해, 인증되지 않은 사용자나 기기로부터 내부망을 강력히 보호합니다.

사내망 접속 시
장비 인증, 사용자 인증

세달 동안
보안패치
받은적 없음

방문객
백신없음

CC 인증제품 GS 인증제품 조달등록

IT 보안, 패러다임이 바뀌어야 한다

CEO포럼

인류의 발전 과정에는 끊임없이 창과 방패의 연속성이 존재한다. 요즘의 대형 보안사고도 어쩌면 필연적인, 또한 누구를 탓하거나 피할 문제가 아닌 더욱 강하고 성숙한 IT 강국으로 향하는 한 과정이 아닐까 싶다. 물론 피해를 당한 당사자들의 참담함은 이루 말할 수 없겠지만 우리의 근성과 오뚝이 같은 저력을 볼 때 충분히 이 위기를 극복해 나갈 수 있을 것이라 생각한다.

중요한 것은 사이버 보안에 대비하는 우리의 개념과 자세의 재정립이다. 결론부터 말하자면 근본적인 사고의 축, 즉 패러다임이 바뀌어야 한다는 것이다. 서버보안에서 엔드포인트 보안으로, 보안관리에서 보안통제로, 개별관리에서 통합통제로, 백신위주 정책에서 네트워크접근통제(NAC) 정책으로 바뀌어야 한다. 대형전산실 위주의 메인프레임 시대에서 PC 와 인터넷 세대로 흘러온 것을 생각해보면 이해하기 어렵지 않을 것이다.

문제 해결의 본질은 네트워크와 엔드포인트다. PC를 포함하여 네트워크에 연결 및 사용되는 모든 장비를 엔드포인트라 부르는데, 보안사고의 중심에는 어김없이 엔드포인트가 등장한다.

“

일정 규모 이상의 금융회사에서는 망분리가 의무화 된다고 한다.
그러나 정작 망, 즉 네트워크는 배제된 채 PC를 두 대씩 쓰거나 서버의 가상화 또는 한 PC에 OS를 두 개씩 두는 방법 중에서 선택하려는 움직임을 보이고 있어 비용과 효과 면에서 의구심이 드는 것이 사실이다.

근본적으로 네트워크에 의한 망 분리를 구축한 후
부가적으로 또는 특수한 경우에 한해 더욱 강화된 물리적 망 분리 또는 가상화 시스템을 구축하는 것이 바람직하다고 본다.

”

그 숫자와 종류가 방대하며 사용하는 소프트웨어 또한 헤아릴 수 없이 많기에 이를 잠시라도 방치하는 순간 대형사고는 이미 예고된 것이나 다름없다.

때문에 우선적으로 네트워크에 연결되어 있는 모든 엔드포인트가 통제 가능한 수준으로 완벽하게 관리되어야 한다. 엔드포인트의 네트워크접근통제(NAC)가 바로 문제 해결의 핵심인 것이다. 성공적인 NAC 구축을 위해서는 개념 정립이 가장 중요하며 이미 구축된 기존 시스템들의 통합과 유기적 연동을 위한 협조 또한 절대적으로 필요하다.

앞으로 일정규모 이상의 금융회사에서는 망 분리가 의무화 된다고 한다.
그러나 정작 망, 즉 네트워크는 배제된 채 PC를 두 대씩 쓰거나 서버의 가상화 또는 한 PC에 OS를 두 개씩 두는 방법 중에서 선택하려는 움직임을 보이고 있어 비용과 효과 면에서 의구심이 드는 것이 사실이다.

근본적으로 네트워크에 의한 망 분리를 구축한 후 부가적으로 또는 특수한 경우에 한해 더욱 강화된 물리적 망 분리 또는 가상화 시스템을 구축하는 것이 바람직하다고 본다.

우리는 이미 결과가 뻔한 싸움을 하고 있는 것은 아닌지 생각해 보아야 한다. 미래를 준비하지 못하고 현실에 안주하는 한 승패는 이미 결정된 것이다. IT 강국으로서 그 동안 우리는 많은 것을 준비해 왔지만 차라리 백지에 그림을 그리면 더 쉬울 것을, 지우고 다시 그리려니 그 흔적과 아쉬움이 길을 막고 있다는 생각이 든다.

이무성 미디어랜드 대표

[CEO포럼] NAC 관심높여 보안 위험 덜자

금융 전산망 마비사태
3.20 전산망 마비사태
끊이지 않는 각종 보안사고..

It is the endpoint, stupid!
(문제는 엔드포인트야, 바보야!)

클린턴 대통령
대선 어록 인용

1992년 부시와의 대선에서 클린턴이 이기게 된 결정적인 선거 캐치프레이즈는 '문제는 경제야, 바보야' 라는 것은 익히 알려진 바이다. 최근 발생하는 대 형 보안사고의 중심에는 어김없이 PC가 주인공으로 등장한다. 대책마련에 분주하고 이렇다 할 해결기미 는 보이지 않지만 '문제는 엔드포인트야, 바보야' 가 그 해답이 아닌가 싶다.

엔드포인트란 네트워크에 연결된 모든 장치를 총칭하며 여기에는 PC, 노트북, 스마트폰, VoIP전화기등이 있고 내부망에 있는 주전산장비와의 통신으로 정보를 생산, 유통, 폐기하는 등 일상적인 주요업무를 수행하는 정보의 보고다.
내가 만일 해커라도 철통수비의 서버를 공격하는 것보다 허술한 엔드포인트를 먼저 공격해 연결된 서버와 주변의 엔드포인트를 장악하고 마비시키는 것이 훨씬 쉽겠다는 생각을 하게된다.

그렇다면 종류도 많고 사용자 수준도 각기 틀린 중구난방의 엔드포인트를 과연 어떻게 해야 하는가? 해결방안으로는 크게 다음의 세가지로 요약할 수 있다.

첫째, 엔드포인트 보안의 개념이 바뀌어야 한다.

백신 위주로 엔드포인트를 지키던 시대는 끝났다. 타미 플루 위주로 신종플루를 해결하겠다는 것이 답이 아닌 것과 같은 논리다. 사후약방문이 아니라 사전처방 전으로 바뀌어야 한다. 주요 내부망에 들어와서 백신치료를 하는 것이 아니라 백신치료를 하고 나서 주요 내부망에 들어와야 한다.
즉 신종플루 환자를 검역소에서 미리 찾아내고 치료 후 입국시키는 것이 맞는 이치와 같다. 패스포트 확인에 이상이 없다고 해서 입국시킨 후에 문제가 생기면 쫓아 다니면서 타미 플루를 투약하는 것이 맞는 방법인가. 비슷해 보이지만 끝이 안 보이는 최근 보안사고 해결의 중요한 실 마리임에는 틀림이 없다.

둘째는 엔드포인트는 관리의 한계를 넘어 통제되어야 한다.

그 동안 엔드포인트는 관리의 대상 이었다. 자산관리, 패치관리, 백신관리, IP관리, 불법소프트웨어관리, 개인정보보호관리 등 앞으로 얼마나 더 많은 관리시스템이 도입, 운영되어야 하고 그렇다고 산적한 문제가 해결될 것인가. 관리를 더 잘 해서 해결될 문제가 아니라 이제는 통제를 해야 한다. 강력한 통제에 의해서만 관리도 더 정확하고 운영 도 간단하게 할 수 있다. 치안이 강력해야 많은 사람들이 더 자유롭게 각자의 일을 잘 할 수 있는 것과 같은 이치이다.
1995년에 가트너그룹이 PC관리의 중요성을 총소유비용(TCO)이라는 컨셉트로 발표하 고 10년 뒤인 2005년에는 PC 통제의 중요성을 네트워크접근통제(NAC)라는 컨셉트로 발표한 것도 이를 뒷받침해 준다.

셋째는 엔드포인트 통제는 간단하고 쉬워야 한다.

엔드포인트 통제의 가장 좋은 해결방안은 네트워크접근통제(NAC)나 대부분 성공하지 못하는 가장 큰 이유는 구축이 복잡하고, 사용이 어렵고, 비용 이 많이 들기 때문이다. 이에 NAC은 구축이 간단하고, 사용이 쉽고, 비용이 적게 들어야 한다.

조금 더 구체적인 설명을 하면 NAC는 기술이 아니고 개념이다. NAC의 중요성을 알고 많은 업체들이 시도를 해왔지만 대부분 성공하지 못하는 가장 큰 이유는 개념에 충실하지 못했기 때문이다.

정확한 개념 의 이해가 무엇보다 중요하며 단순한 기능비교로 판단하고 도입할 경우 실패 확률이 매우 높다. 가장 큰 문제는 일반 사내망과 주요 내부망 사이의 DMZ(또는 외부망)에 대한 명확한 구분과 오염된 PC의 검역 을 DMZ에서 먼저 해야만 한다는 것이다. 또 인증과 인가의 확실한 이해가 필요하고 이들 간의 실행순서가 바뀌어서도 안된다. 자칫 아이디/패스워드가 맞으니 사람과 장비에 대해 이상 없음을 확인하고 내부 망에 접근을 허용하는 경우 가많은데 이러한 것이 치명적인 문제를 야기하기 때문이다.

유 무선 엔드포인트(Endpoint) 네트워크 접근통제 시스템

성공적인 NAC 시스템을 구축하기 위해서는 네가지의 주요한 시스템이 유기적으로 통합되어 연계 작동 되어야만 한다.

정확한 타깃을 잡기 위한 자산관리시스템(DMS), 통제수단으로서의 IP관리시스템 (IPMS), 무결성상태를 지속적으로 유지하기 위한 패치관리시스템(PMS), 그리고 정책수립과 통제를 하기 위한 컨트롤타워 역할의 네트워크 접근통제시스템(NAC)이 그 것이다.

이미 기업들은 이러한 각자의 시스템을 한 두개씩은 구축 운영하고 있어 인증시스템만 추가로 구축하면 된다라고 생각하는데 이는 크 게 잘못된 생각이고 실패의 중요한 원인이다. 구슬을 가지고 있는 것과 실에 꿰매 보석을 만드는 것과 같은 차이다.

이무성 미디어랜드 대표

네트워크 접근 통제(NAC)를 위해서는 적용 대상을 수집하고 차단하는 역할을 하는 IP제어 기술(IPMS), 무결성 유지 및 보안 상태를 관리할 수 있는 중앙 PC제어 기술 (DMS), 보안패치 기술(PMS) 기술이 필요하고 또한 이 시스템들이 유기적으로 연동 되어야 강력하게 엔드포인트를 통제하고 효율적으로 관리 할 수 있습니다.

미디어랜드는 4가지 시스템을 모두 전문적으로 자체 개발하는 국내 유일의 기업으로, 각각의 시스템이 유기적으로 운용될 수 있어보다 안정적이고 강력하게 엔드포인트를 통제 관리할 수 있습니다.

언론

‘성안의 성’ IT이중보안시스템

미디어랜드 ‘티게이트’

최근 대형 보안사고가 빈번히 발생하면서 기존 사고의 축을 바꿔 새로운 보안시스템을 마련하는 일이 시급하다는 시각이 주를 이루고 있다.

때문에 이제는 서버보안에서 엔드포인트보안으로, 보안관리에서 보안통제로, 개별관리에서 통합통제로, 백신 위주의 정책에서 NAC(네트워크접근통제) 정책으로 보안의 개념을 바꿀 필요가 있다는 주장이 힘을 얻고 있다. 또한 이에 가장 부합할 만한 프로그램으로 미디어랜드의 ‘티게이트’가 주목받고 있다.

‘티게이트’는 네트워크에 접속하는 모든 유,무선 엔드포인트기기들을 정책에 따라 중앙에서 강력히 통제하며 인증과 검역을 통과한안전한 기기만이 주전산망에 접속할 수 있도록 하는 IP 기반의 전문 보안시스템이다. 기존 자물쇠 방식의 보안과 다른 울타리식 경비시스템에 의한 새로운 보안시스템이다.

‘성안의 성’과 같이 망 구분에 의해 완충지대를 둬 메인망을 이중보안 하므로 비인가자와 오염된 PC의 주 전산망 접근을 근원적으로 차단할 수 있다.

머니투데이
고문순 기자

NAC솔루션 Tgate(티게이트)

2013 디지털타임스 상반기 히트상품

개인이 들고 다니는 스마트폰과 태블릿PC로 회사 업무까지 처리하다보니 이를 통한 정보유출이나 보안 위협이 증가하고 있다. 따라서 방화벽, 백신 등 개인기기만 검사, 보호할 수 있는 단계가 아닌 회사 사내 망을 보호할 수 있는 전 방위적인 보안체계마련이 필요하다.

Tgate(티게이트)는 이같은 개인 기기와 사내망을 편리하고 안전하게 통합 관리할 수 있는 기능을 제공해 업계로부터 러브콜을 받고 있다.
이 제품은 네트워크에 접속하는 모든 기기들을 보안 정책에 따라 강력히 통제해 인증과 검역을 통과 했을때만 내부 망까지 접근하게 허용해주는 네트워크 보안 솔루션이다.

사내 망을 안전한 내부망과 완충지대 역할을 하는 외부망으로 분리하는 논리적 망분리 기술을 통해, 인증되지 않은 사용자나 기기로부터 내부망을 보호한다. 비용도 저렴해 효율적이고 편리한 보안 정책을 수립할 수 있다.

이 제품은 PC의 소프트웨어를 통제하는 기능도 제공한다. 접속과 동시에 로그인 화면이 나타나고 소프트웨어 검사를 수행을 통해 보안정책 기준을 통과한 사용자와 장비만이 네트워크에 접근할 수 있도록 허용한다.

Tgate(티게이트)는 종류에 관계없이 모든 단말에 인증기능을 수행할 수 있으며 사내망 접근 시 한층 강화된 통제와 보안을 제공한다. 개인 노트북, 스마트폰, 스마트패드, 개인 태블릿PC, 외부 방문객 PC까지 통제할 수 있어 사내 망 보안을 책임지는 전산 관리자들의 고민과 수고를 한번에 해결해 줄 수 있다.

"각종 보안 사고들로 많은 기업들이 내부보안에도 많은 신경을 쓰기 시작했고 기업 들에게 강력한 내부보안을 제공할 수 있는 솔루션이 주목을 받기 시작했다" 면서 "앞으로도 많은 위협 이 개인용 기기로부터 발생할 것이라고 예상되는 만큼, Tgate(티게이트)가 기업 보안 유지의 핵심이 될 수 있을 것" 이라고 내다본다.

디지털타임즈
강은성 기자

고객 추천글

고객사 : 롯데쇼핑
부서명 : IT운영팀
담당자 : 김종욱 과장

"Tgate"를 통해 엔드포인트 보안 뿐만 아니라 전체 자산관리 정확도를 매우 높일 수 있었습니다.
인사DB와 연동한 PC의 사용자인증을 통해 기존 자산정보 일치율을 100% 가까이 올릴 수 있었습니다. 회사 내 자산파악이 정확해짐으로써 관리나 통제하기가 한결 쉬워졌습니다.

고객사 : 싸이버로지텍
부서명 : Infra 운영팀
담당자 : 유승주 수석

"Tgate"를 통해 인사DB와 연동하여 Software 자산관리 정확도를 높일수 있었습니다. 그리고 AD와 연동하여 NAC을 구축함으로서 내부 사용자 불편없이 비 인가자 탐지 및 접근정책을 구현할 수 있었습니다.

고객사 : 창원파티마병원
부서명 : 전산운영파트
담당자 : 유형호 부장

우리 병원은 몇 개의 병동으로 나누어져 있어 외부 업체에서 가지고온 노트북을 효과적으로 관리할 수 없었습니다.
그런데 "TCO!secuIP"를 도입하고 나서부터 내부 네트워크에 연결하는 모든 PC는 반드시 허락을 받고 IP를 할당 받음으로써 네트워크 보안 사고를 원천적으로 차단하고 있습니다.

고객사 : 목포시청
부서명 : 정보화 담당관실
담당자 : 김중섭 팀장

목포시청에서 사용하는 모든 IP를 "TCO!seculP"를 통하여 관리하고 있습니다. 특히, 망분리 후 내부 IP와 외부 IP를 엄격히 분리하여 사용하는데 좋은 효과를 가지고 있습니다.

고객사 : 목포해양대학교
부서명 : 전산실
담당자 : 김중섭 팀장

"TCO!seculP"를 통하여 학교내의 모든 IP정보를 수집 관리하고 있습니다.
또한, 학생들이 불법으로 반입한 무선기기를 효과적으로 차단하여 IP에서 발생하는 문제점을 상당 부분 해결하고 있습니다.

고객사 : 삼성창원병원
부서명 : 전산실
담당자 : 유형호 부장

삼성창원병원은 이미 IP관리 시스템을 사용중에 있었습니다.
그런데 기존의 노후화된 IP관리 시스템 때문에 여러가지 헛점이 발생했고, 이로인해 네트워크 보안 사고를 효과적으로 막을 수 없었습니다.
이후, TCO!seculP로 고도화를 하고 나서는 관리의 헛점이 없이 모든 네트워크에 대해서 관리가 가능해졌습니다.

고객사 : 삼광의료재단
부서명 : 전산관리실
담당자 : 김지훈 부실장

"TCO!seculP"를 통하여 3곳으로 분산된 건물의 네트워크 IP 정보를 수집 관리하고 있습니다.
불법 IP 사용을 통제하며, IP 변경으로 인해 발생하는 IP 충돌을 막고 있습니다.

고객사 : 농심
부서명 : SM운영팀
담당자 : 안홍기 차장

농심 그룹사 전체를 "TCO!stream"을 통하여 자산관리하고 있으며 특히 불법소프트웨어 관리에 대해 잘 운영되고 있습니다.

고객사 : 광주광역시청
부서명 : 정보화 추진팀
담당자 : 김중섭 팀장

"TCO!seculP"로 시청 청사내 모든 IP와 6개 사업소에 분산되어 있는 IP를 중앙에서 통합 관리 합니다.
이를 통해 IP의 발행, 할당, 회수를 원활히 처리하고 있습니다.

고객사 : 금호타이어
부서명 : 인프라운영팀
담당자 : 박현우 대리

금호타이어는 제조사라 공장이 여러곳에 분산되어 있습니다.
IP는 광주에서 TCO!seculP를 통하여 통합관리하고 있습니다.
원격지 이동없이 IP를 관리, 모니터링, 통제할 수 있어 매우 효과적입니다.
이에 효과적으로 IP를 관리하고 불법 IP를 차단하기 위해 NAC기능이 탑재된 TCO!seculP를 도입 하였습니다.
도입 후 사내 IP에 대한 보안은 잘 관리되고 있습니다.

고객사 : 제이씨엔터테인먼트
부서명 : 사업지원본부 IT실
담당자 : 구모성 대리

저희 회사는 "TCO!seculP"와 "TCO!steam"을 쓰고 있는데 IP관리, 자산관리에 용이점이 많은것 같습니다. 특히 쉽게 설계된 솔루션의 UI는 일처리함에 있어서 빠르게 진행시킬 수 있는 장점이 있습니다.
그 외 각 세부적인 설정을 통해 각각의 클라이언트의 맞는 시스템을 제공하고 관리하는 측면에서 효율적이라 할 수 있습니다.

차세대 NAC

Tgate

티 게 이 트

CC 인증제품 GS 인증제품 조달등록

www.medialand.net

www.medialand.net

미디어랜드 홈페이지에서 자세한 제품정보 확인 및 제품문의를 하실 수 있습니다.

blog.naver.com/medialand7

미디어랜드 엔드포인트연구소에서 유용한 기술문서를 보실 수 있습니다.

Medialand
Pioneer of Endpoint Management

엔드포인트연구소

기술문의 techlab@medialand.net
문의전화 02-501-3221
홈페이지 www.medialand.net

서울시 영등포구 양평동5가 18번지
우림라이온스밸리 B동 7층 (주)미디어랜드

차세대 NAC

Tgate
티 게 이 트

네트워크에 의한 논리적 망분리

성 안의 성, 두개의 성문

Tgate(티게이트)는 네트워크에 접속하는 모든 기기들을 보안 정책에 따라 강력히 통제해 인증과 검역을 통과 했을때만 내부망까지 접근하게 허용해주는 네트워크 보안 솔루션입니다.

사내망을 안전한 내부망과 완충지대 역할을 하는 외부망으로 분리하는 논리적 망분리 기술을 통해, 인증되지 않은 사용자나 기기로부터 내부망을 강력히 보호하여 사내망과 유무선 엔드포인트를 완벽하게 보호하는 시스템입니다.

성안의 성, 두개의 성문 Two gates = Tgate

CC 인증제품 GS 인증제품 조달등록

Medialand
Pioneer of Endpoint Management
TEL. 02-501-3221 E-mail. techlab@medialand.net www.medialand.net