Network Access Control Overview

임재성 (ljs@unetsystem.co.kr)
PMP, 프로젝트관리전문가
유넷시스템주식회사

TABLE OF CONTENTS

Network Access Control Overview 3
1. 필요성 3
2. 정의 4
3. 기술표준 5
4. NAC 솔루션 형태 12
5. NAC업체 현황 15
6. 시장현황 및 전망 17
7. 적용전략 20
결론 23
Reference 24

Network Access Control Overview

임재성 / PMP (프로젝트관리전문가)

IT환경이 급변하면서 기존의 보안체계로는 최근 새롭게 증가하는 보안위협을 효과적으로 대응할 수 없는 한계상황에 와 있다. 이를 극복하기 위하여 새로운 보안기술이 제시되고 있고, 그 중에서도 네트워크 접근제어(NAC, Network Access Control) 보안기술은 이러한 한계상황을 해결할 수 있는 대안으로 떠오르고 있다.

네트워크 접근제어(이하 NAC라고 칭함)는 "내부 네트워크 및 자산을 다양한 보안위협으로부터 보호하기 위하여 네트워크 접속단말에 대한 엄격한 보안정책적용"을 핵심 목표로 하고 있다. 어쩌면 NAC는 IT환경 변화에 따른 필연적인 보안 패러다임으로 보는 것도 무리가 아니라고 판단된다.

본 고의 목적은 NAC에 대한 개념을 정확히 이해하고, NAC 아키텍처 표준의 진행상황을 이해함으로써, 이해관계에 있는 보안정책담당자, 보안관련 솔루션 업체, 보안IT 투자자들이 차세대 보안 체계인 NAC을 효과적으로 설계 · 구축하는데 도움을 주는 데 있다.

본 고에서는 가트너그룹의 NAC 모델을 기반으로 NAC이 무엇인지를 이해하고, NAC에 대한 각종 아키텍처를 분석하고, 관련기술 및 제품유형을 분석할 것이다. 또한, 현 벤더들의 동향을 살펴보고, 시장조사 기관에서 점치는 시장전망 및 시장현황 분석결과들을 살펴볼 것이다. 마지막으로 NAC를 도입하고자 하는 고객이, 미리 고민하고 준비하여야 하는 사항들을 제시한다.

1. 필요성

NAC(Network Access Control)은 "네트워크에 접근하는 접속단말의 보안성을 강제화 할 수 있는 보안 인프라(하드웨어 및 소프트 웨어)"로써 다음과 같은 IT환경의 변화에 따라 더욱 필요성이 커지고 있다.

모바일 환경의 일반화 : 근무자가 이동하면서 업무를 수행하는 경우, 즉 회사 이외의 장소에서 기업내부의 네트워크를 접속하여 사용하는 경우가 늘고 있다. 외근자의 접속단말은 제대로 관리가 되지 않기 때문에 외부에서 웜 · 바이러스가 감염된 상태로 기업 네트워크에 다시 접속하여 기업 네트워크에 웜 · 바이러스를 전파하는 경우가 많다. 물론, 일부 기업에서는 출장자의 접속단말을 재 반입 시, 일일이 수작업으로 보안상태를 점검하고 치료하는 업무를 수행하지만, 이 또한 상당한 비용이 드는 일이다.

접속단말의 다양화 : 최근에는 데스크탑 PC 외에 노트북, 팜PC, 스마트 폰, PDA 등 다양한 접속단말이 네트워크에 접속하고 있다. 스마트 폰, PDA 등에는 보안프로그램이 설치되지 않고 관리되거나 관리할 수 없는 경우가 대부분이다. 이러한 관리대상이 되지 못하는 접속단말들이 기업 네트워크에 접속하여 보안문제를 야기시키는 사례가 늘어나고 있다.

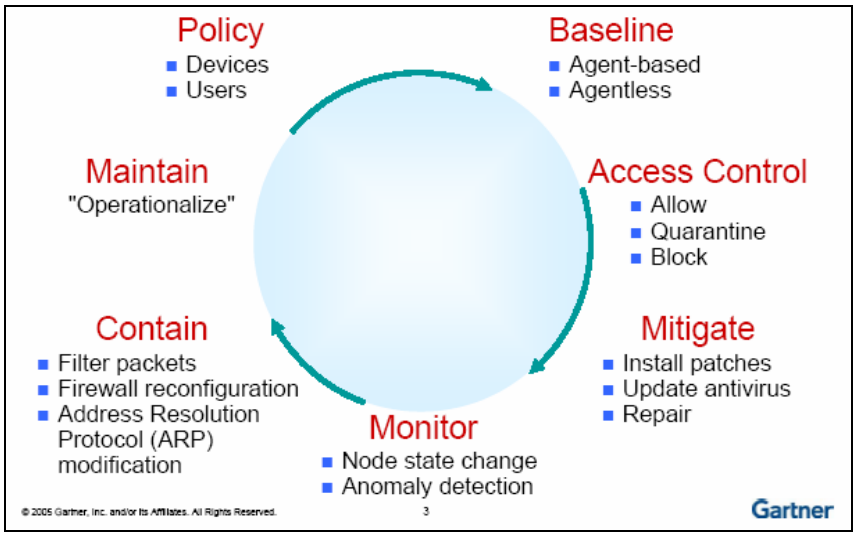
내부 보안관리의 필요성 증가 : 현재 기업IT 보안체계는 네트워크 관문에 주로 구성되어 있다. 즉, 외부 보안위협을 차단하기 위한 목적으로 주로 운영되고 있다. 그러나 최근 보안사고의 유형을 살펴보면, 내부로부터 발생하는 보안문제의 비중이 높아지고 있음을 알수있다. 물론, 대부분의 기업에서는 내부 보안을 위해 각 접속단말(서버 포함)에 패치관리 시스템, 바이러스 백신 프로그램, PC방화벽 등 단위보안 솔루션들을 각각 설치 · 운영하고 있으나 정상적인 운영이 되지 않거나, 기업의 보안정책을 따르지 않는 경우가 많다. 또한, 불법사용자에 대한 인증기능을 수행하지 못하고 있다. "Infonetics Research" 보고서에서는 "대부분의 기업은 네트워크 관문에서의 보안체계 구축이 완료되면 내부보안으로 관심을 가질 것이며, 이에 대한 해답으로 NAC을 구축하고자 할 것이다."라고 언급했다. [IR1],[MR1]

2. 정의

많은 산업 분석가들은 NAC기술에 대해 각각 다른 용어와 정의를 내리고 있다. (예를 들어 "Network Quarantine", "EndPoint Security") 본 고에서는 가트너그룹에서 정의한 NAC로 정의하고자 한다.

"가트너그룹" 정의 모델

가트너그룹은 2005년에 NAC 참조모델을 정의하였다. 본 모델에서는, 지속적인 접속단말에 대한 보안 평가, 보안문제에 대한 대응, 네트워크 접근 허용, 보안정책 준수에 대한 지속적인 모니터링 및 대응에 대한 업무 순환 절차로 정의하였다.[GTN]



[그림-1 : 가트너그룹의 NAC 모델]

가트너그룹의 모델이 가장 폭넓게 기능을 정의하고 있다. 가트너그룹의 NAC을 위한 절차는 보안정책(Policy)의 정의에서 출발한다. 보안정책은 네트워크에 접속하기 전에 관리자가 강제화 하고자 하는 보안 체크리스트다. 이러한 보안정책은 조직의 요구사항에 따라 추가적인 시스템 혹은 제 3의 소프트웨어 정책을 포함할 수 있다.

많은 기업의 전형적인 보안 정책으로는 "운영체제의 보안 패치가 최신을 유지하는가?, 바이러스 백신 프로그램이 정상적으로 구동되는가?, 백신 업데이트가 제대로 되어있는가?, 개인 방화벽이 정확히 설정되어 운영되고 있는가?"를 확인하는 것이다. 추가로, 특정한 보안 소프트웨어 혹은 특별한 보안 설정에 대한 새로운 확인을 원할 수 있다.

베이스라인(Baseline)은 보안정책이 먼저 수립되고 나서, 네트워크에 접속하려는 접속단말의 상태가 먼저 수립된 보안정책과 일치하는지 비교하는 것이다. 이러한 절차는 접속단말의 네트워크에 연결방식과 상관하지 않고 수행되어야 한다. 즉, 안전한 네트워크를 보장하기 위하여 LAN, WAN, 무선, IPsec, SSL VPN 접속 시 베이스라인 평가가 수행되어야 한다.

이러한 베이스라인 평가 결과에 기반하여, 접근통제(Access Control)는 접속단말에 미리 정의된 수준의 네트워크 접근권한을 부여한다. 예를 들어, 베이스라인을 따르는 접속단말의 경우 전체 네트워크에 대한 접근권한을 부여할 수 있고, 베이스라인을 따르지 않은 접속단말의 경우, 네트워크 접근을 완전히 차단하거나, 치료(Mitigate)를 위한 특정 네트워크 영역으로의 접근만을 허용할 수 있다. NAC의 가치를 높이기 위해서는 이러한 치료절차는 자동화되어야 한다. 즉, 헬프데스크의 도움을 받지않고 문제가 있는 접속단말이 치료될 수 있어야 한다는 것이다.

접속단말이 상기 절차를 거쳐 네트워크에 접속한 이후에도 “지속적으로 보안정책을 따르는지 혹은 비정상 행태를 하지 않는지”를 지속적으로 확인하기 위한 모니터링 기술이 필요하다. 모니터링 결과, 문제가 있는 경우 네트워크 전체의 관점에서 적절한 대응을 위한 기술 및 절차가 필요하다. 예를 들어 웜·바이러스의 활동 트래픽이 발생하는 경우, 해당 접속단말을 네트워크로부터 분리하고, 억세스 스위치의 접근제어정책에 등록하여 해당 포트로의 접속을 허용치 않도록 하는 것이 필요하다.

3. 기술표준

2006년 5월에 라스베가스에서 개최된 “Interop”에서 제시된 NAC 아키텍처는 크게 5가지로 분류될 수 있다. 산업계 공개 아키텍처 표준인 “TCG(Trusted Computing Group)”의 “TNC(Trusted Network Connect)”, 업체 아키텍처 표준인 Cisco의 “NAC(Network Admission Control)”, Microsoft의 “NAP(Network Access Protection)”, 기타 솔루션 업체들의 독립적인 아키텍처로 구분 되어진다. IETF “NEA(Network Endpoint Assessment)”그룹은 2006년에 기존 아키텍처 표준들의 문제를 해결하고 상호 연동될 수 있는 메타표준을 개발하기 시작했다.[IR1]

본 아키텍처 표준들은 현재 진행형으로, 아직 완성 단계가 아니다. 빠르면, 2006년 하반기 혹은 2007년도에 가서나 완벽한 아키텍처를 각자 제시할 것이라는 견해가 많다. 또한 현재, 어떤 아키텍처가 주도적인 표준으로 자리를 잡게 될 것인지에 대해서도 예측할 수 없는 상황으로 이러한 아키텍처 표준화 경쟁기간이 몇 년 간(2년 이상) 지속될 것으로 내다보는 전문가들이 많다.[NW1],[NW2]

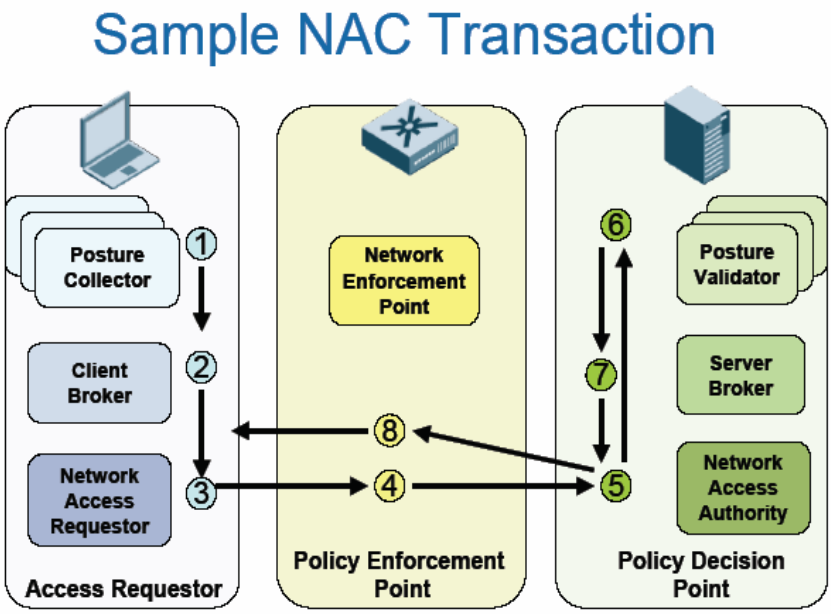
구분	주체	아키텍처	강점	단점(문제점)	상태
산업(공개)	IETF(Internet Engineering Task Force)의 NEA(Network Endpoint Assessment) 그룹	NAC 메타 표준	별도 아키텍처가 아니고 여타 아키텍처들을 상호호환성을 높이기 위한 인터페이스에 대한 표준 프로토콜을 정의하는 일종의 메타표준		· 2006년 초에 표준화 시작. · 2007년 여름에 완성될 계획
	TCG(Trusted Computing Group)	TNC(Trusted Network Connect)	· 공개 아키텍처 표준 · 특정 하드웨어, 서버, 운영체제와 독립적	· 미완성 · 다수 참여자의 이해관계 때문에 표준화가 쉽지 않을 것으로 예측	· 제품화가 아직 되어 있지 않음(2006년 하반기 예상) · 표준이 자주 업데이트 되고 있음
업체	Cisco	NAC(Network Access Control)	· 제3의 클라이언트를 지원함 · 네트워크 장비 기반	· Cisco 네트워크 장비에 종속 · 공개표준이 아님 · 무선 접속 프로그램(supplicant) 별도 필요	· 제품화 되어 있음(라우터, 스위치 단) · 2007년에 정책서버 재정의 예정
	Microsoft	NAP(Network Access Protection)	· 윈도우 운영체제에 번들 · 자동 치료 지원 · 네트워크 장비에 종속성 없음	· 윈도우 운영체제에 국한됨 · 클라이언트 지원 한계(지원 OS Vista 출시 지연) · 아직 기본 탑재 서버 OS인 Longhorn 출시 일정 지연 · 공개표준이 아님	· 아직 미완성 (2007년에 제공 예정)
	기타 (주니퍼네트웍스,유넷시스템)	N/A(업체 마다 고유의 아키텍처 보유)	· 완성도가 상대적으로 높고 레퍼런스가 많음 · 다양한 부가기능을 제공	· 표준(공개)을 완벽히 준수하지 않고 있어 호환성 확보가 관건	· 기타 아키텍처와의 연동성 확보 노력

[표-1 기술표준 비교표]

IETF에서는 2005년 3월에 "(NEA)Network Endpoint Assessment" BOF로 출범하였고, Cisco 및 TCG가 공동의장으로 되어있다.[IR8]

IETF의 NEA 그룹은 새로운 NAC 아키텍처를 정의하는 것이 아니라 여타 아키텍처들이 사용하는 공통 인페이스를 식별하고 중복을 제거하고 상호호환성을 확보할 수 있는 표준 프로토콜(6가지 컴포넌트간의 인터페이스 표준)을 정하는데 그 목적이 있다. 현재까지는 개별 아키텍처들을 위한 메타표준이라고 보는 것이 타당하다.

IETF의 NEA 그룹이 여타 아키텍처들을 통합하여 정리하고 있으므로 본 고에서는 IETF의 NEA 그룹의 아키텍처를 설명하고자 한다.



[그림-2 : NAC 아키텍처 및 흐름도]

1) 구성요소 [IR1],[IR8]

Access Requestor(AR)

접속단말에 설치되는 요소로, 크게 "Posture Collector", "Client Broker", "Network Access Requestor"로 구성된다. "Posture Collector"는 클라이언트에서 구동되는 제 3의 소프트웨로 접속단말의 보안 상태 정보(예: 백신 소프트웨어 및 개인 방화벽 운영 상태 등)를 각각 수집한다. "Client Broker"는 다수의 "Posture Collector"로부터 수집된 정보를 "Network Access Requestor"에게 전달하는 역할을 수행하는 미들웨어다. "Network Access Requestor"는 802.1X Supplicant 혹은 IPsec VPN 클라이언트와 같은, 네트워크 연결 소프트웨어로서 사용자 인증을 수행하며 추가적으로 클라이언트의 보안상태 정보를 서버(PDP) 측에 전달하는 기능을 수행한다.

Policy Enforcement Point (PEP)

802.1X 지원 스위치 장비, VPN 게이트웨이 혹은 방화벽 등과 같은 정책을 강제화기 위한 네트워크상의 장비를 말한다. 기타 별도 NAC Enforcement 장비도 이에 포함된다.

Policy Decision Point (PDP)

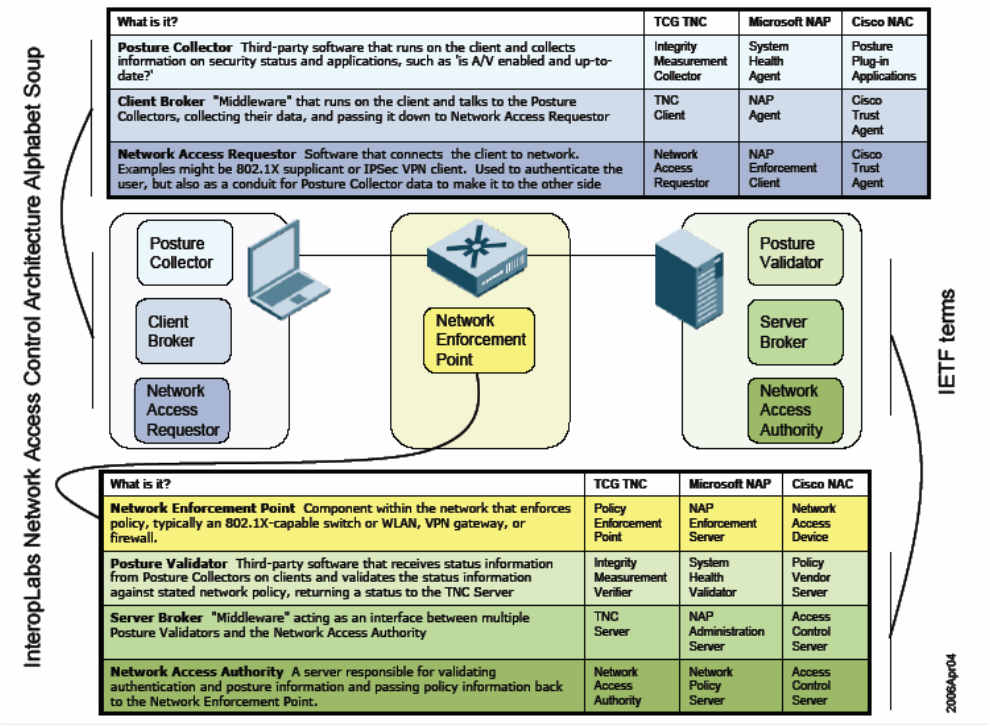
서버 측에 설치되는 소프트웨어로, 크게 "Posture Validator", "Server Broker", "Network Access Authority"로 구성된다. "Posture Validator"는 클라이언트로부터 전송된 보안상태정보를 기반으로 정책준수여부를 점검하는 제

3의 소프트웨어로서, 점검 후 결과를 "Server Broker"에게 전달한다. "Server Broker"는 다수의 "Posture Validator"로부터 점검한 결과를 수집하여 "Network Access Authority"에 전송하는 미들웨어다. "Network Access Authority"는 인증을 수행하고 점검결과 및 정책정보를 Network Enforcement Point에 전송하는 역할을 수행한다.

2) 처리흐름

[그림-2]는 전형적인 NAC 처리흐름을 나타내고 있다. 이러한 처리흐름은 다른 아키텍처도 통합적으로 설명되어질 수 있다. [그림-2]는 설명의 편의성을 위해 네트워크 접속 시점만의 처리흐름을 나타내고 있지만, 대다수 제품들은 네트워크 접근 이후에도 지속적으로 보안정책을 점검하고 점검결과에 따른 대응절차를 수행하는 순환구조로 이루어져 있음을 주의하여야 한다.[IR8],[IR5]

① 클라이언트의 보안상태정보를 수집하여 "Client Broker"에 전송한다.
② 다중의 "Posture Collector"로부터 보안상태를 통합적으로 수집한다.
③ 수집된 보안상태 정보 및 인증방식에 따른 인증토큰을 "Policy Enforcement Point"에 전송한다.
④ 전송된 보안상태 정보 및 인증토큰을 "Network Access Authority"에 제공한다. (예 : 802.1X 인증방식에서 Authenticator)
⑤ 사용자 인증을 수행결과, 적법한 사용자의 경우 "Server Broker"에 클라이언트 보안상태 점검을 의뢰한다. 인증에 실패한 경우 PEP에게 인증실패 사실을 전송한다.
⑥ 요청 받은 보안상태를 보안정책과 비교하여 점검한다.
⑦ "Posture Validator"로 부터 전달 받은 점검결과를 수집하여 접근허용여부를 결정하여 "Network Access Authority"에 전달한다.
⑧ 서버로부터 전송 받은 접근정책(접근권한)을 구현하고 결과를 클라이언트에 전달한다. (예 : 특정 네트워크로만 접근하도록 ACL 혹은 VLAN 설정)



[그림-3 : IETF NEA 메타표준과 기타 아키텍처와의 비교]

3) 대표적인 아키텍처

다음 3가지(Cisco NAC, TNC TNC, Microsoft NAP) 아키텍처 표준화가 아직 진행 중이고, 2006년 "Interop"에서 실시한 상호호환성 테스트 결과 상호 연동되지 않는 것으로 나타났다. 이러한 아키텍처들 간의 상호호환성 확보를 위한 노력이 IETF의 NEA 그룹에서 시작된 것이다.

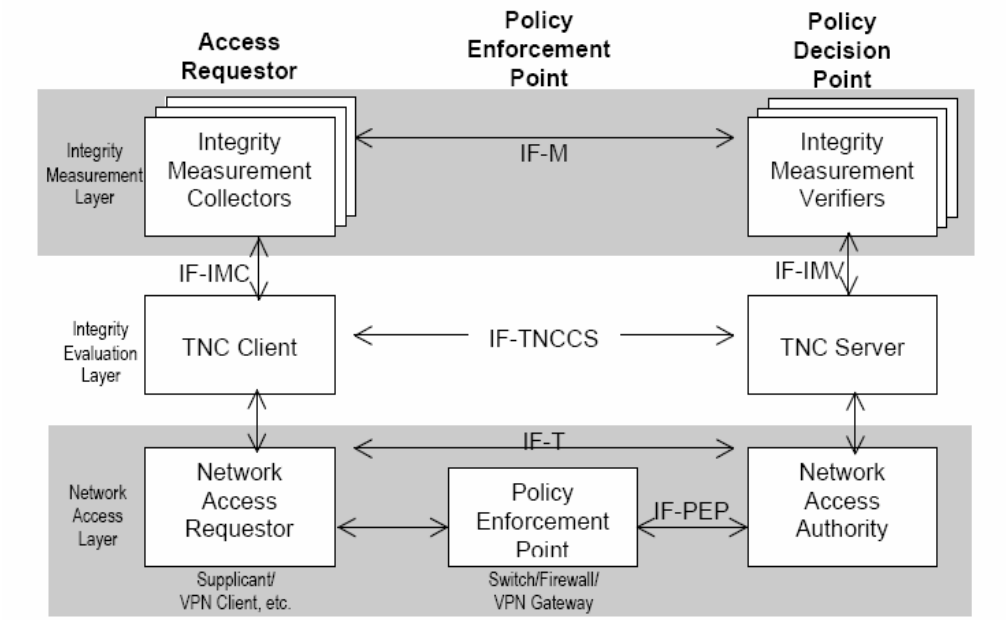
TCG의 TNC (Trusted Network Connect)

2003년에 설립된 산업연합체인 TCG는 당초 하드웨어 보안에 치중하였다. 디지털 인증서, 키 및 패스워드를 위한 "Trusted Computing Module"에 관련된 스펙을 개발하였다. 현재 네트워크 인프라, PC 클라이언트, 소프트웨어 및 서버 보안에 대한 스펙을 개발하고 있다.

NAC의 출현에 따라 Trusted Network Connect(TNC) 스펙을 개발하기 시작했고, TNC는 네트워크 자원에 접근하는 것을 허가 하기 전에 정책 기반 모델(Policy-based model)을 기반으로 접속단말의 보안준수 여부를 판단하는 공개된 아키텍처로 개발하고 있다. TCG에 따르면 "TNC 아키텍처는 네트워크 접근제어를 위한 상호호환성 및 이러한 솔루션들의 보안성 향상을 위한 기반으로서 신뢰된 컴퓨팅에 목표를 두고 있다"라고 말한다. 일 예로, TNC는 기 사용되는 네트워크 접근제어 메커니즘과 통합하는 것이다. [MR1],[IR5]

TNC 담당자는 "아직까지는 실용적이지 못하고 아키텍처 수준인 것이 사실이고, 12~18개월 이후에 이를 기반한 제품화가 가능할 것이다"라고 말한다.

TCG는 현재 Microsoft를 포함하고 12개 주요 업체가 활동하는 등, 산업계의 전폭적인 지지를 받고 있다. 그러나, Cisco는 회원이 아니다.



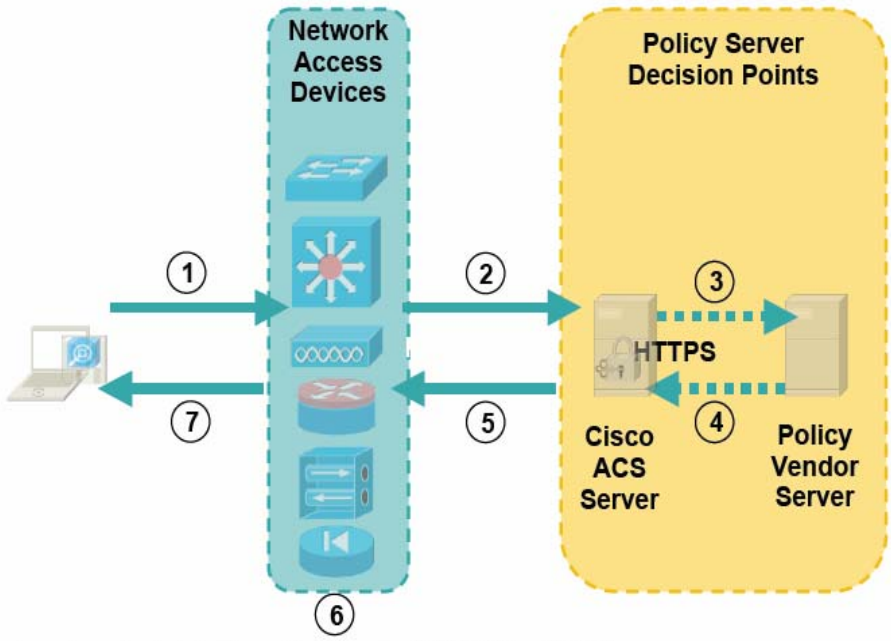
[그림-4 : TCG의 TNC 아키텍처]

Cisco의 NAC (Network Admission Control)

Cisco는 NAC(Network Admission Control) 기술과 프레임워크를 최초로 소개했다. NAC 프레임워크는 네트워크 인프라 요소들을 안티바이러스 및 안티스팸 솔루션과 같은 다양한 제 3의 툴들과 통합하는데 치중하고 있다. Cisco는 60여 보안 벤더들이 이러한 통합 프로그램에 참여하고 있다고 밝혔다.[IR7],[HVD]

Cisco NAC은 접속단말의 보안정보를 정책서버에 전송하기 위하여 접속단말 단에 "Cisco Trust Agent"를 설치해야 한다. 정책 서버는 접속단말을 완전히 허가할지 거부할지 혹은 일부에 대해서만 허가할 지를 결정한다.

양키 그룹에 따르면 Cisco 방식의 최대 문제점은 "Cisco 네트워크 장비에서만 동작한다"는 것이다. 반면에 여타 NAC 제품들은 불특정 다수의 라우터 및 스위치 환경에서도 작동한다.



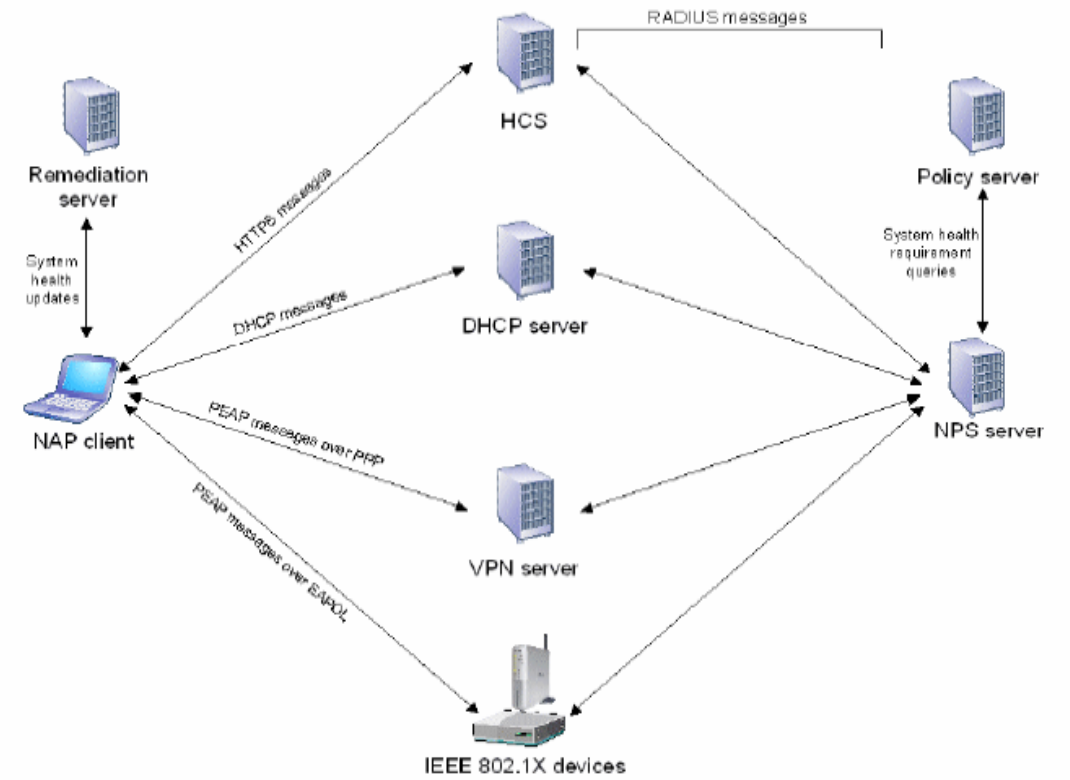
1) Host sends credentials to Access Device using EAP (UDP or 802.1X)
2) Access Device forwards credentials to Policy Server (ACS) using RADIUS
3) ACS Server authentications and passes posture information to Policy Vendor Server
4) Vendor Servers respond with Compliant/Non-Compliant Messages
5) Policy Server responds to Access Device with access rights and VLAN assignment
6) Access Device accepts rights, enforces policy, and (7) notifies client

[그림-5 : Cisco의 NAC 아키텍처]

Microsoft NAP (Network Access Potection)

Cisco NAC이 전적으로 Cisco 장비에 종속되는 것과 동일하게, Microsoft의 NAP(Network Access Protection) 역시 차세대 운영체제인 Vista, Longhorn에만 포함될 예정이다. 발표에 따르면 Microsoft에서는 문제가 있는 클라이언트의 어플리케이션에 대한 접근을 제한하는 것에 중점을 두고 있고, 네트워크 보안 아키텍처가 아니라 어플리케이션 보안 아키텍처라고 강조한다. 그러나, Cisco와 동일하게 클라이언트에 대한 무결성 확인, 문제가 있는 접속단말에 정책 기반의 통제 및 필요 시 치료 기능을 제공함으로 그 구분은 명확하지 않은 것이 사실이다. 물론, Cisco는 라우터, 스위치, 방화벽에 있어서 자기들 것을 고집하는 반면, Microsoft는 네트워크 인프라 구성요소들과 연동할 수 있는 API를 제공하고 있다.[IR6]

그러나 NAP은 Longhorn 서버 및 Vista 클라이언트를 요구하고 있다.(물론, 그들은 XP상의 Service Pack 3에서도 클라이언트를 구동하게 할 것이라고 말하고 있다.). Longhorn 서버는 2006년 하반기 혹은 2007년에나 출시할 것으로 예측이 되며 광범위하게 사용되기 까지는 상당한 시간이 필요할 것이다. 따라서, 현실적으로 Microsoft의 NAP을 기반으로 한 제품이 나오기 까지는 적어도 1-2 년 혹은 그 이상 걸릴 것으로 예측된다.



[그림-6 : Microsoft NAP 모델]

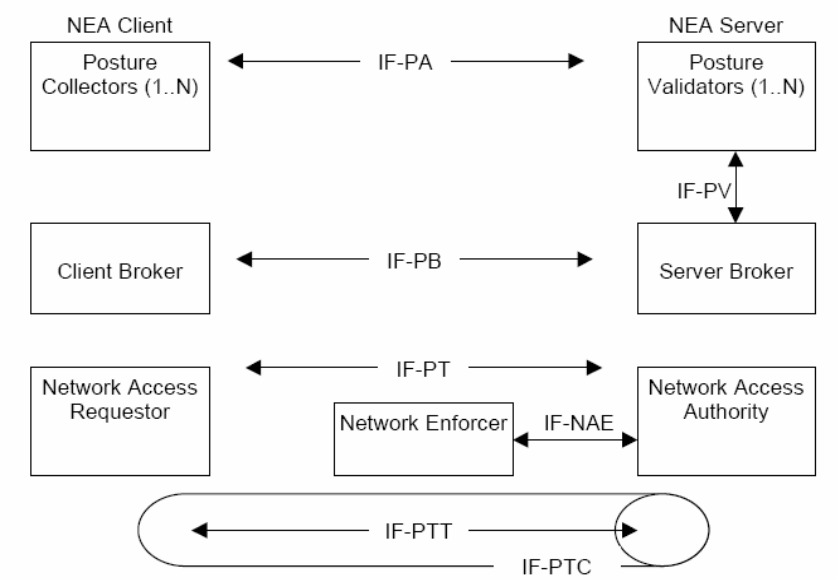
IETF NEA(Network Endpint Assessment)

"Interop" 의 랩테스트 결과에서 상기 3가지 아키텍처들이 현재 까지 상호 호환되지 않고 있는 것으로 밝혀졌다. 이러한 고민에 희망을 주는 것이 IETF NEA 그룹의 노력이다. 즉, IETF에서는 서로 다른 아키텍처가 상호호환 할 수 있는 메타 표준화 작업을 시작했다.

이들은 2007년 여름까지 표준화를 완료하는 것으로 계획 중에 있으나 확신할 수는 없다.

2006년 3월에 NEA 그룹은 상호호완성을 위하여, 문제영역(호환성을 떨어트리는 영역)을 인터페이스 기반으로 식별하여 어떠한 방법으로 표준화를 할 것인가를 결정하였다. NAC 아키텍처의 구성요소에 명칭을 새로이 표준화하여 문제영역과 같이 정리하여 IETF의 Draft문서로 작성하였다. 이 문서의 명확한 목적은 위에서 기술한 3가지 아키텍처들 간의 호환성을 높이는 것이다. [IR8]

NAC 아키텍처 상의 인터페이스를 크게 7가지로 분류하였고 이 중 4가지를 먼저 표준화 하고 나머지 2가지는 후에 진행하기로 하였다.



[그림-7 : IETF NEA 표준화 대상 인퍼페이스]

4. NAC 솔루션 형태

최근의 NAC 제품은 여러 가지 방식을 동시에 지원함으로 단일화된 기준의 제품구분은 문제가 있지만, "Forester"의 분류를 간단히 살펴보고자 한다.

"Forester"에서는 서버기반의 제품과 포트기반의 제품으로 구분하고 있다. "서버기반"은 DHCP, RADIUS 그리고 정책서버를 사용하는 소프트웨어 기반의 제품을 말한다. "포트기반"은 802.1X와 같은 포트기반 인증기능을 스위치 및 라우터에 통합하여 정책을 강제화 하고 격리시키는 하드웨어 기반의 솔루션들을 말한다. 물론, 최근 포트기반 및 서버기반 기능을 동시에 제공하는 제품도 출시되고 있다.[HVD]

아키텍처	포트 기반		서버기반
	어플라이언스	스위치	소프트웨어
적용 형태	Overlay: standalone network device	기존 네트워크 장비에 NAC 기능 추가	Overlay: standalone or server-integrated software
적용 선택사항	In-line 및 out-of-band	In-line	Out-of-band
격리 방식	L2 레벨 : VLANs , switch control 및 에이전트 방화벽	L2 레벨 : VLANs 및에이전트 방화벽	L3 레벨 : DHCP 및 에이전트 방화벽
상대 가격	비쌈	중간	저렴

[표-2 : NAC 제품 형태 구분]

Cisco NAC은 포트기반 중 스위치형 제품의 대표격이며, ConCentry, Nevis Networks 등이 포트기반 중 어플라이언스형 제품에 해당되고 ENDFORCE, MaAfee, Symantec은 소프트웨어 기반의 제품으로 분류할 수 있다.

그러나 상기 제품들을 포함해 현재 많은 제품들은 하나의 방식만을 지원하지 않고 다양한 방식을 동시에 지원함으로써 고객의 환경적 특성을 고려하여 선택적으로 구축하고 운영할 수 있도록 한다. (참조:표-3)

예를 들어, 유넷시스템의 제품은 소프트웨어 및 스위치 기반을 혼합한 형태이다. 즉, 802.1X 기반의 NAC를 구축하는 경우 스위치 기반의 802.1X 인증 및 에이전트 기반의 격리 방식(혹은 Dynamic ACL방식)을 선택적으로 사용할 수 있으며, DHCP 기반의 NAC을 구축하는 경우 어플라이언스 기반의 인증 및 에이전트 기반의 격리 방식을 선택적으로 사용할 수 있다.

표-3에서 제시하는 접근제어 범위, 인증방식, 에이전트 방식, 격리방식, 무결성 검증 방식, 어플라이언스의 경우 설치방식을 전략적으로 선정하여 구축할 수 있다.

방식구분 기준			설명	비교단점	비교장점
적용범위	(내부접속) 유.무선 LAN 접속단말	802.1X를 지원하는 네트워크 장비 기반	L2레벨의 대표적인 NAC 방식이며 802.1X 인증방식으로 사용자 인증시 접속단말의 무결성을 동시에 확인하는 방식	기존 스위치 장비(AP 포함)에서 802.1X를 지원하여야 함. 서버 단에 RADIUS서버	높은 보안성 보장 (표준화된 L2레벨의 인증방식)

방식구분 기준			설명	비교단점	비교장점
				필요.	
		DHCP 기반	L3 레벨의 대표적인 NAC 방식이며, IP 요청 시 사용자 인증 및 접속단말 무결성을 검사하는 방식으로 802.1X가 지원되지 않는 네트워크 환경에서 대안으로 사용됨.	고정 IP 환경에서 사용불가.(혹은 별도 강제화 장비 필요) 낮은 보안성(L3레벨의 인증방식) 별도 DHCP 프록시 서버 필요(임베드).	기존 네트워크 인프라의 업그레이드 불필요.
		별도 Enforcement Appliance	Cisco와 같은 특정 네트워크 장비의 종속성을 해결하기 위한 독립된 어플라이언스 장비 제공 방식이며, 트래픽 정보를 분석하고 단말의 무결성을 스캐닝하여 단말기의 무결성을 검증하는 방식으로 설치 형태에 따라 인라인 방식 또는 게이트 웨어 방식이 있음.	인라인 방식의 경우 네트워크 장애 요인이 됨. 인증방식이 취약함 (예:MAC/IP기반) 어플라이언스 장비 비용 부담(예:세부적인 격리를 위한 분산설치 필요)	기존 네트워크 인프라 업그레이드 불필요.
		IPsec 기반의 MS 내부 보안 네트워크 프레임	Microsoft에서 새롭게 제시하는 IPsec기반의 안전한 내부 논리 네트워크 을 말하며 네트워크 접속은 물론, 상호 점대점 방식의 컴퓨니케이션을 인증서 기반으로 수행	N/A	N/A
	(외부접속) VPN(SSL)을 이용한 외부 접속단말		보통 VPN 게이트웨이 뒷 단에 인라인 방식으로 추가 설치하는 방식과, 기존 VPN 게이트웨이 벤더들이 통합적으로 제공하는 방식이 있음.	N/A	N/A
에이전트 방식	에이전트 설치 방식		IETF NEA 그룹에서 정의한 AR 단의 소프트웨어를 설치하는 전형적인 방식.(전통적인 방식임)	클라이언트 프로그램 설치 및 관리 부담	보다 다양한 보안정책을 적용할 수 있음(세부적인 보안정책이 필요한 대기업 환경에 필요함) 비용이 상대적으로 저렴.
	에이전트 미 설치 방식		Enforcement Appliance 장비 방식의 경우 에 해당하며 Passive 방식으로 클라이언트의 건강정보를 스캐닝하는 기술을 주로 사용함.	스캐닝 방식의 정책점검 결과의 정확성이 떨어짐. 일반적으로 사용하는 ARP기반의 격리(강제화) 방식을 사용하기 위해 어플라이언스 장비가 분산되어 설치되어야 함.	클라이언트 관리비용 없음 (이동이 많은 캠퍼스환경에 적합)
격리방식	Dynamic VLAN 방식(네트워크 스위치 장비에 설정)		대상 접속단말이 접속한 스위치 장비에 SNMP, CLI Script등을 이용해 특정 VLAN ID를 유동적으로 부여하는 방식 (포트기반의	적용하지 못하는 네트워크 장비 존재 가능(허브, 오래된 스위치 장비) 네트워크 설정(VLAN)	ACL 방식에 비해 보안성 높음

방식구분 기준			설명	비교단점	비교장점
			경우 주로 사용)	변경 부담 VLAN 내부 보안 대책 추가 준비 필요	
	ACL(기존 네트워크 장비에 설정)		대상 접속단말이 접속한 스위치 장비에 ACL를 이용하여 특정 IP, 서비스 만을 사용하도록 통제하는 방식 (포트기반의 경우 주로 사용)	우회할 수 있는 보안문제 존대. 통제정책이 단순	기존 네트워크 환경변경 불필요
	ACL(클라이언트 방화벽에 설정)		클라이언트에 설치된 PC방화벽에 룰을 설정하여 특정 IP, 서비스 만을 사용 가능하게 하는 방법	클라이언트에 별도의 PC 방화벽 프로그램 설치 필요	ID 기반의 세밀한 격리 기능 제공가능 인증 및 치료 프로세스와 긴밀하게 연동하여 관리할 수 있음 네트워크 재설정(혹은 업그레이드) 불필요.
	ARP(별도 Enforcement Appliance에서 명령)		문제가 있는 접속단말의 ARP 테이블의 주소를 강제로 변경하여 트래픽이 외부로 나가지 못하도록 하는 방법(포트기반 중 어플라이언스 방식의 경우 사용)	일종의 편법(격리 후 대책 없음) 제어대상 접속단말이 동일 세그먼트에 존재하여야 함.(비용부담)	네트워크 인프라 변경 최소화 가능
	인라인 제어		문제가 되는 접속단말의 트래픽을 필터링 하는 방식(포트기반 중 인라인 어플라이언스의 경우 사용)	별도의 어플라이언스 장비를 인라인 모드로 설치하여야 함. (억세스 단에서 설치 시 비용 부담)	N/A
무결성 검사 방식	검사 범위	사용자 접속단말	접속단말의 무결성 및 관련 보안 솔루션 정상구동여부를 검사	N/A	N/A
		네트워크 상태	네트워크의 비정상 트래픽 행위를 지속적으로 검증하여 문제가 있는 접속단말 및 서비스를 제어하는 개념으로 소위 네트워크 행태분석(Network Behavior Analysis)를 말하며 별도 NBA제품과 연동하여 구축되기도 함.	N/A	N/A
	검사 시점	네트워크 접속 시	최초 네트워크에 접속 시 사용자 인증 및 접속단말의 무결성 검사를 수행	N/A	N/A
		네트워크 접속 후	네트워크 접속 후에도 지속적으로 접속단말의 무결성을 검사	N/A	N/A
인증방식	802.1X 인증방식		802.1X 인증서버와 연동하여 인증(포트기반 중 스위치 형의 경우)	네트워크 인프라가 802.1X를 지원하여야 함.	보안성이 가장 높음.
	기타 개별 인증(RADIUS, 기존 디렉토리 연동)		기존 인증디렉토리 및 방식과 통합하여 인증 수행 (어플라이언스 및 에이전트 형식의 제품인 경	보안성이 비교적 약함 때론 상당한 연동작업이	기존 연동방식을 확장하여 사용될 수 있음.

방식구분 기준			설명	비교단점	비교장점
			우)	필요.	
	MAC/IP기반		이미 등록된 MAC/IP를 기반으로 인증하는 방식(에이전트 비 설치형 제품의 경우)	보안성이 취약	N/A
Enforcer 위치	Edge 단	포트기반 중 스위치 형	기존 네트워크 장비에 NAC Enforcement기능이 포함되어 있는 경우 (예 : Cisco NAC 지원 라우터) 라우팅 정책에 의해 쿼런틴 기능 구현	별도 게이트웨이 도입 혹은 기존 네트워크 장비 업그레이드 비용 발생 세밀한 정책관리가 불가능(주로 인터넷 사용 통제만 가능)	클라이언트 부담 최소화 가능. Dist/Access 단보다 비용 저렴
		포트기반 중 어플라이언스 형	인라인 방식 혹은 미러링 방식으로 설치 인라인 모드인 경우 필터링 방식으로 쿼런틴 기능 구현		
	Distribution/Access 단	포트기반 중 스위치 형	기존 네트워크 장비에 NAC Enforcement기능이 포함되어 있는 경우(예:Cisco NAC 지원 스위치) 일반적으로 802.1X 기반으로 쿼런틴 기능 구현	별도 게이트웨이 도입 혹은 기존 네트워크 장비 업그레이드 비용 발생. 어플라이언스 형일 경우 세부적인 정책구현을 위해 다수의 장비가 분산 설치되어야 함.	클라이언트 부담 최소화 가능. Edge 단 보다는 세밀한 정책관리 가능
		포트기반 중 어플라이언스 형	인라인 방식 혹은 미러링 방식으로 설치. 인라인 모드인 경우 필터링 방식으로 미러링 모드인 경우에는 ARP 방식을 통한 격리기능 구현		
	접속단말 단	PC 방화벽 방식(에이전트)	NAC 정책서버에서 네트워크 접근제어 등의 명령을 접속단말에 설치된 PC 방화벽을 이용하여 쿼런틴 기능 수행	클라이언에 별도의 PC방화벽 기능이 탑재되어야 함.(물론 업체에서 같이 제공하는 경우가 많음)	세밀한 정책관리가 가능함 기존 네트워크 인프라 변경 없이 적용 가능. 별도 장비 불필요

[표-3 : NAC 관련 기술 분류]

5. NAC업체 현황

최근까지 많은 기업들이 NAC이 Cisco의 고유기술로 인식했었다. 그러나, 네트워크 통제기술의 필요성이 증가함에 따라, 다른 벤더들이 합류하기 시작했다. 이 후 네트워크 장비업체인 Enterasys Networks, Extreme Networks 그리고 Foundry Networks가 그들의 네트워크 장비 제품군에 NAC 제품을 추가하였다. (일부는 기능적으로 Cisco의 NAC의 개념을 따르기도 했고 일부는 다른 방식을 사용하고 있다.) 그러나, 이들 대부분의 네트워크 벤더들이 제시하는 NAC 제품을 구현하기 위해서는 동일 벤더사의 네트워크 장비를 도입하던지 혹은 업그레이드하여야 하는 문제점을 가지고 있다.

이러한 문제점들을 해결하기 위하여 새로운 방식의 NAC 제품이 제시되었다. 별도의 Enforce Appliance 장비를 제공하

는 방식과 에이전트 단에서 Enforcement 기능을 수행하는 방식이 바로 그것이다. Juniper Networks는 Cisco의 접근 방식과 완전히 다른 대안이 될 수 있는 제품을 제시하였고 이러한 개념으로 ConSentry, Lockdown Networks, Nevis Networks, ForeScout, StilSecure, Senforcer, Mirage networks 그리고 Vernier Networks는 경쟁력 있는 제품들을 제시하였다.

2006년 5월에 개최된 "Interop" 에서는 다양한 많은 벤더들이 NAC이라는 이름으로 다양하게 제품을 소개하였다. 물론, 제품 중에는 가트너그룹에서 정의한 NAC 기능 중 일부 기능에 특화된 제품들도 상당 수를 차지한다.

한국의 경우, 2006년 5월에 유넷시스템㈜에서 802.1X 제품을 기반으로 하여 에이전트 단에 PC 방화벽 기능을 포함하여 격리 및 정책강제화 기능을 수행하는 NAC 제품을 처음으로 선보였다. 본 제품은 가트너그룹에서 정의한 NAC 기능을 지원하기 위한 기반 구조를 완벽하게 제공하고 있다.[UN1] 지니네트웍스에서 패치관리 솔루션을 기반으로 접속단말의 패치관리를 능동적으로 강제화 할 수 있는 패치관리에 특화된 NAC 제품을 출시하였다.

산업공동체 차원 협력 현황

- 산업협력체인 TCG 그룹은 현재 60여 업체가 회원사로 구성되어 활동하고 있다. 스위치 및 네트워크 장비 업체, 솔루션 업체, 관리서비스 제공업체, 칩 생산업체 및 다수의 소프트웨어 업체들이 참여하고 있다. McAfee, TrendMicro, Symantec등이 주도적으로 참여하고 있다.
- IETF의 NEA그룹의 경우 Cisco와 TCG가 공동 의장으로 되어 있고 기타 다양한 업체들이 참여하고 있다.

개별 업체 차원의 협력 현황

- Cisco 에서는 Cisco NAC 연동 단위 보안 솔루션들과 연동 파트너들을 지속적으로 모집하고 있다. 2006년 2월 현재 63개 업체들과 파트너 관계를 형성하였고, 이 중 22개 벤더들은 연동테스트를 완료하였고 41개 업체는 연동작업을 진행 중에 있다. 대표적인 업체들이 McAfee, Symantec, CA, TrendMicro, F-Secure, Panda 등이 있다.
- Microsoft의 경우도 Cisco와 동일한 개념의 파트너들을 모집하고 있다. 2006년 2월 현재 53개 업체들과 파트너 관계를 형성했지만, NAP 기반 제품이(Vista, Longhorn) 출시되지 않고 있어 실 연동 테스트는 이루어지고 있지 않다. Cisco과 경쟁관계에 있는 Enterasys, Extreme, Foundry, ProCurve(HP), Juniper등이 주요 파트너들이다. Cisco와 연동파트너 업체인 McAfee, Symantec, CA, TrendMicro, F-Secure, Panda 역시 MS와도 파트너관계를 유지하고 있다.
- Vernier Networks는 PatchLink의 자동화된 치료 기능을 통합하기 위해 협력관계를 맺었다. 즉 Verinier의 NAC 제품을 기반으로 접속단말에 대한 자동화된 패치강제화 및 치료 절차를 제공하고 있다.
- 에이전트 설치를 하지 않는 NAC 제품의 대표적인 벤더인 ForeScout Technologies는 Vernier Networks와 같은 이유로 PatchLink사와 파트너 관계를 형성하였다.
- 네트워크 장비업체인 Juniper Networks에서 802.1X 인증 솔루션 업체인 Funk Software를 1억2천2백만 달러에 인수하여 NAC 사업을 강화시켰다. Juniper는 Cisco의 독주에 맞서기 위해 인수했다고 밝혔다. Juniper는 TNC 아키텍처 표준화의 주요 업체였던 Funk Software의 L2레벨의 정책 강제화 기술을 Juniper NAC에 추가할 예정이다. 가트너 그룹에서는 본 인수에 대한 분석 리포트에서 "Juniper의 접근방식 또한 공개 아키텍처 표준을 따르지 않고 있다" 는 것과 "완전히 네트워크 인프라가 802.1X 환경으로 변화되기 전 까지는 DHCP 방식과 같은 L3 기반의 NAC 제품이 여전히 필요하다. " 라는 것을 추가적으로 언급했다.
- Symantec에서 NAC업체였던 Sygate를 인수하여 NAC사업 업그레이드하였다.

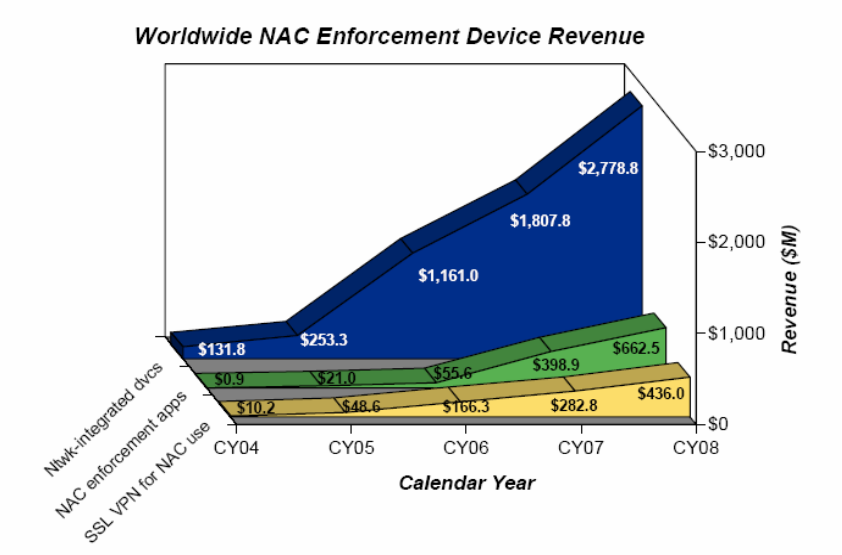
- Mirage Networks에서 백신업체인 Symantec과 기술협력 관계를 맺고 바이러스 점검 강제화 및 치료 기능을 보강하였다.
- Senforcer는 McAfee의 에이전트와 통합하여 NAC 제품을 라인업 하였다.
- 유넷시스템은 소프트런과 NAC 관련 사업 및 기술 제휴관계를 맺고 패치정책 강제화 및 패치 절차를 자동화할 수 있는 기능을 강화시켰다. 이들은 자국 내 NAC시장 활성화를 위해 지속적으로 단위보안솔루션 업체들과 사업 및 기술 제휴관계를 확대하여 궁극적으로는 한국내 NAC 산업공동체 형성할 예정이다.[UN2]

6. 시장현황 및 전망

2006년 1월의 "Infonetics Research" 보고서에서 NAC Enforcement 장비(PEP) 시장 예측자료를 제시하였다. 본 자료에서는 NAC 솔루션 중 다음 3가지 분야만을 대상으로 하였고나머지 AR, PDP 은 제외하였다. 또한 Enforcement 장비는 아래와 같이 크게 3가지로 구분하였다.[INF]

- NAC이 지원되는 네트워크 장비: 802.1X 인증을 지원하고 NAC 클라이언트(AR) 및 정책서버(PDP)와 연동하는 스위치, 라우터, 방화벽 혹은 타 보안장비를 말한다.
- Enforcement Appliance: NAC 아키텍처에서 PEP역할을 수행하는 장비로서 보통 추가적으로 IDS/IPS, 방화벽, 안티바이러스 기능을 제공한다. 보통 자사의 NAC 아키텍처에서 구동되기도 하고 타 NAC 아키텍처와 상호 연동할 수 도 있다.
- Enforcement를 위한 SSL VPN: NAC 기능이 지원되는 VPN 게이트웨이 장비로서 사용자 인증, 무결성 검증, 네트워크 접근통제기능을 제공한다.

[그림-8]에서 보듯이, NAC Enforcement 시장은 2005년과 2008년 사이에 323백만 달러(한화 3천2백3십억)에서 39억 달러(한화 3조9천억)로 급성장할 것으로 예측하고 있다. (연평균 성장율 1,101%) 대기업은 NAC의 필요성 및 개념을 알고 있고 많은 중소기업들이 도입을 위한 검토 단계라고 밝혔다.



[그림-8 : NAC Enforcement 시장 예측]

2004년에서 2005년 사이에 NAC이 지원되는 네트워크 장비가 NAC 성장의 주된 내용이었고 매출액 비중이 가장 큰 것으로 밝혔다. 이러한 NAC이 지원되는 네트워크 장비 시장은 기본적으로 네트워크 장비들이 고객이 원하든 원하지 않든 NAC 기능을 내장시키고 있는 데서 기인한 것으로 말했다. (실제 NAC 기능을 사용하지 않을 수도 있다.)

2008년까지 스위치 시장의 매출 중 21%가 NAC을 지원하는 스위치일 것이라고 예측하고 있다. 또한, 라우터에 있어서는 10%, 보안장비의 경우 16% 정도가 NAC을 지원하게 될 것으로 예측하고 있다. 스위치 장비가 가장 각광받을 NAC Enforcement 장비로 예측되고 있지만 모든 스위치가 NAC를 지원할 필요는 없을 것으로 예측하고 있다.

NAC Enforcement 어플라이언스 장비는 2006년을 시작으로 급격히 성장하고 있다고 밝혔다. 대부분의 벤더들이 라인업을 시작했고 시장에 전력투구하고 있다고 밝혔다. 또한 이 분야는 향후 3년 정도의 시한부 시장으로 예측 하고 있다. 어플라이언스 형태의 NAC은 기업의 네트워크 인프라를 업그레이드 하기 어려운 기업들에게 매력적일 것이고, 관리가 용이하고 가격이 저렴한 장비를 원하는 중소기업에도 매력적일 것이라고 말했다.

다만, 2008년 이 후에는 NAC을 지원하는 네트워크 장비들이 일반화되거나 추가적인 비용 없이 업그레이드 가능해 질 것으로 예측되며, 이 때에는 NAC Enforcement 어플라이언스 시장은 서서히 없어질 것으로 예상하고 있다.

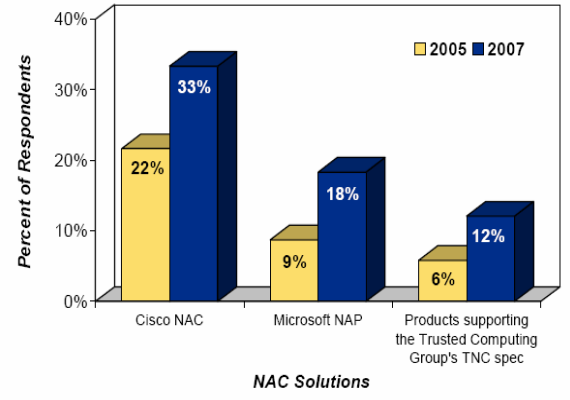
또한 2008년까지 2/3정도의 SSL VPN이 NAC를 지원할 것으로 예상하였다. 현재 주요 SSL VPN업체 중 일부는 2005년 초부터 NAC 시장을 겨냥하고 있고 50%이상이 NAC을 지원하는 방식의 장비가 판매된다고 언급한다. 나머지 SSL VPN업체들도 곧 NAC 시장에 눈을 돌릴 것으로 예측하고 있다.

기업대상 관련 설문 조사 결과

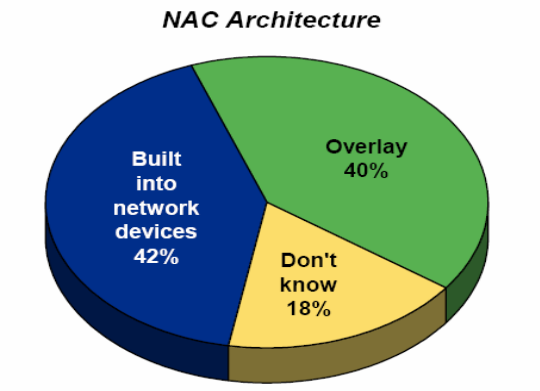
"Infornetics Research"에서는 직원수가 20명 이상인 북 아메리카의 240 기업을 대상으로 설문 조사를 한 결과를 다음과 같이 발표하였다.[INF]

대상자들은 NAC 시장은 아직 초기 시장이고, 완벽한 솔루션을 제공하는 벤더들이 거의 없고, 시장이 혼란스럽다고 대답했다고 밝혔다. 고객들이 NAC에 대한 정확한 인식이 이루어 지고 있지 않기 때문에 NAC의 주요한 인증 기반구조인 802.1X에 대한 적용여부에 대한 조사결과 2005년 후반까지 30%가 적용한 것으로 나타났고, 2007년 후반까지는 55%가 사용할 것이라고 대답했다고 밝혔다.

NAC 솔루션에 대한 벤더 별 조사에서는 Cisco, Microsoft, TCG 순으로 나타났고 NAC의 도입 형식은 NAC이 지원되는 네트워크 장비형태로 구축하는 것과 기타 형태(별도 Enforcement 어플라이언스 장비, 에이전트 방식 등)로 구축하는 방법이 거의 대등하게 나타났다고 밝혔다. 이는 아마도 두 형태에 대한 정확한 이해가 부족한 탓일 수도 있다.

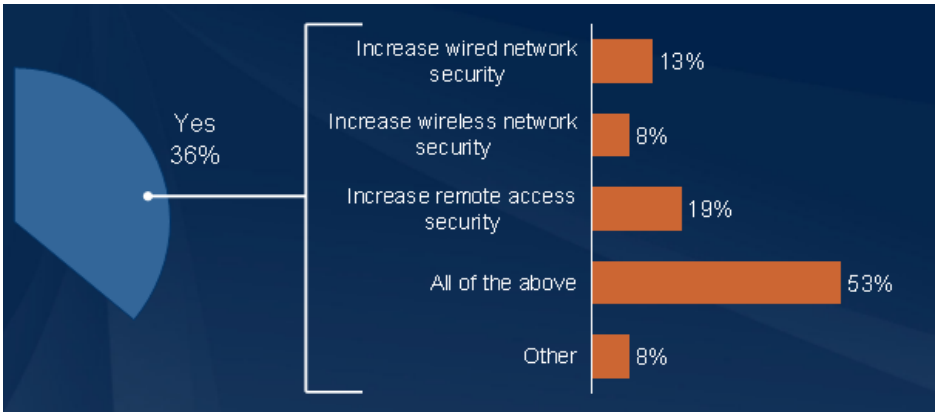


[그림-9 : 아키텍처 선호도 조사결과]



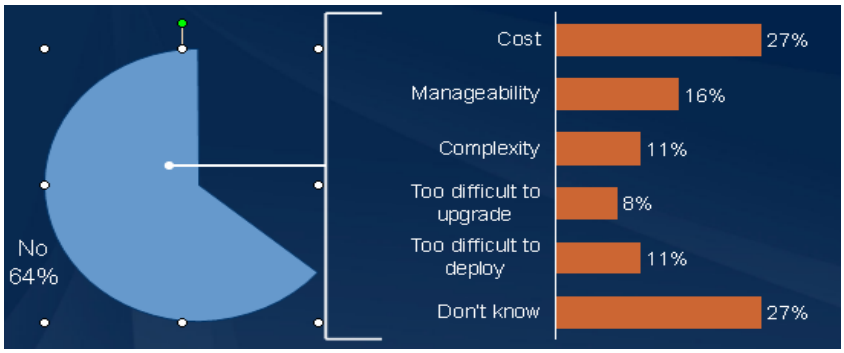
[그림-10 : NAC 구축 형태 조사결과]

"Forester" 에서 발표한 북미기업들을 대상으로 한 설문조사자료에 의하면 36%의 기업이 2006년 안에 NAC를 도입하거나 업그레이드 할 계획이라고 밝혔다. 또한 NAC을 도입하려고 하는 목적은 원격접근 보안강화, 유선 네트워크 보안강화, 무선 보안강화 순인 것으로 발표했다.[FRR]



[그림-11 : NAC 도입 사유 조사결과]

그리고, NAC를 도입하지 않는 이유로는 비용, 관리부담, 복잡성 순으로 나타났다고 발표했다.



[그림- 12: NAC 도입하지 않는 사유 조사결과]

도입계획이 없는 기업들 중에도 49%는 2006년 안에 802.1X를 지원하는 하드웨어로 업그레이드하여 네트워크 인증은 우선 추진하려고 한다고 밝혔다.

7. 적용전략

NAC을 구축 및 테스트 하고자 하는 경우, 다음의 3가지 사항에 대해 충분히 고민하여 대응전략을 수립하여야 한다. [IR3]

- 우리의 접근 통제 정책은 무엇인가?
- 보호하길 원하는 접근 방식은 무엇인가?
- 기존 인프라와 어떻게 통합(연동)할 것인가?

상기 질문에 대해 세부적인 답을 결정한 후, 제품 선정을 위한 BMT를 시작할 수 있어야 한다. 즉 관련하여 전략을 완벽하게 수립하면, PDP를 위한 장비, AR을 위한 접속단말들, PE를 위한 스위치, AP, VPN 게이트웨이 등을 문제없이 완벽하게 준비할 수 있을 것이다.

가. 우리의 접근 통제 정책은 무엇인가?

먼저, 접근제어 정책을 단순하게 정의하는 것으로 BMT 테스트와 실 적용하는 것의 기반이 되기 때문에 상당히 중요한 작업이다. 다음 테이블과 같은 형태로 정리하는 것이 유용하다.

사용자 및 그룹	접속단말 보안 상태	환경	접근제어
STAFF	백신S/W 구동 및 최신상태	건물 내 접근	모두 허용
STAFF	백신S/W 최신상태가 아님	건물 내 접근	치료목적의 별도 네트워크로만 접근 가능
GUEST	무관	건물 내 접근	인터넷만 접근가능
알지 못하는 사용자	무관	건물 내 접근	포탈 서버로 재 연결
STAFF	백신S/W 구동 및 최신상태	VPN 접근	모두 허용
STAFF	백신S/W 최신상태가 아님	VPN 접근	메일서버만 허용

[표-5 : NAC 접근제어 정책 예]

현재의 NAC 구축에서는 세밀한 접근제어 대신 다소 미흡한 제어방식을 사용하는 경향이 있다. 예를 들어 허용/불허 혹은 하나의 VLAN을 기반으로 한 제어방식 등을 주로 사용한다. 최근 가장 많이 사용되는 VLAN 기반의 접근제어는 완벽한 제어기능을 제공하지 못하고 있다. 다만 VLAN안에 방화벽이 설치되어 있다면 또 다른 이야기가 된다. VLAN 방식은 여러 가지로 미흡한 방식이지만 일반적으로 사용되고 있다.

현재 대부분의 제품들은 이 정도의 접근제어 정책만을 구사할 수 있다. 다만, 유넷시스템 등과 같은 일부 벤더 제품들은 PC 방화벽 기술을 사용하여 사용자 별로 세밀한 접근제어 정책을 구사할 수 있는 제품들이 있다.(예를 들어 사용자 ID별로 특정 자산 및 서비스 사용 제어하는 기능을 제공)[UN1]

나. 보호하길 원하는 접근 방식은 무엇인가 ?

NAC을 계획하는 경우, 적용하고자 하는 네트워크 접근 방식을 정해야 한다. 물론, IT상황에 따라 우선순위를 가지고 순차적으로 진행하거나 별도로 진행하는 경우도 필요하다.

- 유선, 무선 LAN 접근

- SSL VPN을 이용한 원격 접근 (IPsec 혹은 SSL VPN 클라이언트를 이용한)
- 원격 지사에서의 VPN 연결 (내부 LAN연결과 별도의 접근 정책이 필요할 수 있음)

위에서 1개 혹은 2개 혹은 3개 전부를 적용대상으로 할 수도 있지만, 어떤 것에 관심이 있고 집중할 것인지를 조기에 결정해야 한다. 또한, 접근방식과 무관하게 동일한 적용전략을 사용할 것인지 혹은 각각 다른 전략을 사용할 것인지 결정할 필요가 있다. 보안상태를 알지 못하는 PC가 원격에서 VPN을 이용하여 기업 내부 네트워크에 접근함에 따른 위험이 이슈화됨에 따라 오래 전에 오늘날 NAC의 개념이 VPN 산업에서는 중요하게 대두되었다.

SSL VPN 업계에서는 이것을 일반적으로 "End Point Security" 혹은 "Client Integrity"라고 명명했고, 본 명칭을 "SSL VPN에 적용한 NAC" 과 동일하게 보아도 된다. SSL VPN업체들이 NAC에 편승하면서 그들의 제품에 NAC 기능을 추가하기 시작했고, 일부 업체들은 단순히 기존에 있던 관련기능을 NAC이라고 재 포장하기도 했다.

이러한 VPN 접근방식의 상대적인 발전은 최근의 LAN 기반의 NAC 제품과 기존 SSL 혹은 IPsec VPN 제품과 쉽게 연동할 수 없게 하였다. 만약에 관심이 있어 적용대상으로 하고자 한다면, 조기에 심도 깊은 검토가 필요하다. 다행히도 적용대상에서 제외한다면 NAC 적용계획이 상당히 단순화될 수 있다. 또한, IPsec 및 SSL VPN 제품은 수 개월 혹은 몇 년 내에 NAC 기능을 제공할 것으로 예측된다.

무선 및 유선 LAN에서의 NAC을 구축하는 것도 쉽지 않는 일이다. 어쩌면, 대형 인프라의 변화가 필요할 수 있기 때문이다. 예를 들어, 소프트웨어 및 설정 변화로 시작하여 전사 장비의 업그레이드 혹은 교체 작업이 필요할 수 있다. 대부분의 기업들이 변경하기 원하지 않는 이미 완성된 전사적인 이더넷 네트워크를 갖고 있기 때문에 전사적인 NAC 적용은 쉽지 않은 일이다. 대부분의 정통한 네트워크 관리자들은 NAC을 구축하기 위해 802.1X 기술을 전사적으로 적용하는 것이 정당화될 수 밖에 없는 "killer app"(살인 어플리케이션)로 보고 있다. 단순히 유.무선 통합인증을 위한 용도로 802.1X를 이용하는 것은 전사 유선 LAN을 업그레이드 하는 것을 정당화하지 못할 수 있지만, NAC에서의 접속단말 보안성 평가 및 인증을 동시에 목적으로 하는 경우에는 정당화 될 수 있는 것이다.

무선 랜의 경우, 802.1X이 무선 보안을 위한 표준으로 자리를 잡았다. 여기서 중요한 것은 "802.1X를 지속적으로 사용하길 원하느냐가 아니고 기존의 무선에 NAC기능을 추가하길 원하느냐" 이다. 만약 802.1X를 무선 LAN에서 사용하지 않는다고 해도, NAC은 최종적인 무선보안체계를 완성하기 위한 다른 차원의 해결 방안인 것이다.

상기 3가지를 기반으로 하여, 어떠한 접근 방식에 대해 보호할 것인지를 결정한다면, 어떠한 장비가 필요한지를 알게 될 것이다. 궁극적으로 제품에 대한 선택범위를 좁혀줄 것이고 우선 테스트(혹은 BMT)해야 하는 것이 무엇인지 판단하게 할 것이다. 예를 들어, NAC을 유선에서 사용하길 원하고 스위치 장비가 802.1X 인증을 지원하지 않거나 VLAN 스위칭을 지원하지 않는다면 네트워크의 코어 혹은 기존 억세스 스위치의 상에서 동작하는 NAC 기술을 사용할 필요가 있는 것이다. 이러한 것을 빨리 결정해야 다양한 선택범위를 좁힐 수 있고 노력과 시간을 절약할 수 있다.

다. 기존 인프라와 어떻게 통합할 것인가 ?

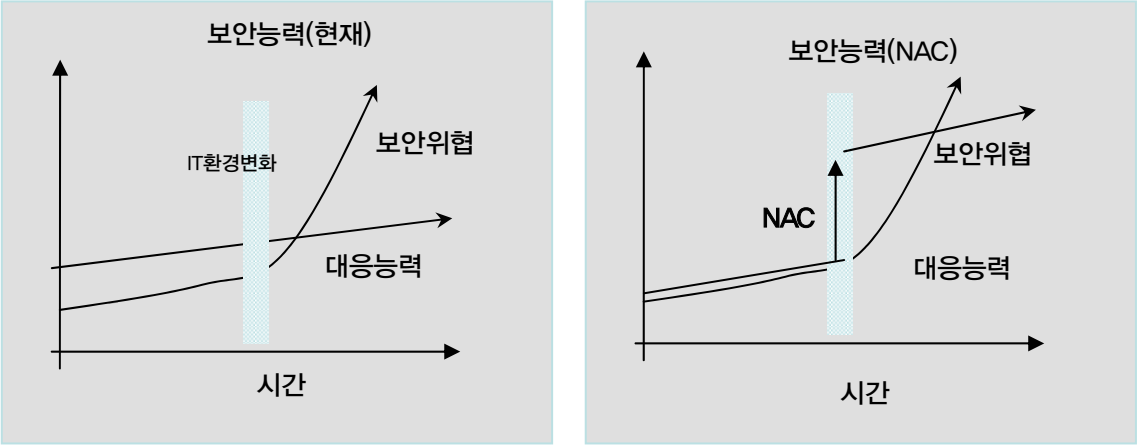
NAC 구축은 기존 네트워크 장비(스위치, 라우터), 방화벽 뿐만 아니라 데스크탑 및 랩탑에 설치된 소프트웨어, 인증 및 정책서버상의 트래픽 로드에도 영향을 준다. 구축에 의한 변화에 따른 상호호환 여부를 확인하는 작업은 BMT와 구축설계 시 중요한 일이다. 예를 들어, NAC 클라이언트 소프트웨어(에이전트)와 Posture Collector(백신 에이전트와 같은 단위 보안 클라이언트 소프트웨어) 툴을 동시에 설치하는 경우, 기존 기업 표준 환경의 데스크탑 및 랩탑 상에서 잘 동작하는 지를 확신할 수 없기 때문에 구축 후의 환경과 동일한 환경에서 미리 테스트를 할 필요가 있다. 만약, 클라이언트 소프트웨어 분배 툴 및 패치관리 서버를 사용하고 있다면, NAC 클라이언트와 기존 소프트웨어들과 충돌하지 않고 상호 보완적으로 동작할 수 있다는 것을 확인하여야 한다. 이 때가 패치관리 시스템, 소프트웨어 업데이트 서버, 안티바이러스, 안티스파이웨어, 개인 방화벽 툴을 포함하는 접속단말 보안관리툴 벤더들과의 커뮤니케이션이 무엇보다 중요하다. 이러한 벤더들은 어떠한 NAC 프로토콜을 및 아키텍처를 지원하는지를 이해할 수 있게 할 것이다.

NAC은 종종 “네트워크 보안 이슈로 생각되어 단순하게 설치될 수 있다”고 오해를 한다. 그러나 NAC을 도입하려면 데스크탑 및 노트북에서 엄청난 “해체 및 통합”이 일어날 수 있다. 이것이 구축 초기의 관련되는 다른 제품들과의 관계를 면밀히 파악해야 하는 중요한 이유다.

결론

기업 IT환경은 언제 어디서나 접근할 수 있는 공개된 환경으로 급격히 변하고 있다. 이러한 환경변화는 유비쿼터스 비즈니스 환경의 요구에 따라 더욱 가속화 될 수 밖에 없는 상황이다. 이러한 환경변화에 따라 현재의 IT보안정책은 획기적인 변화가 필요한 시점에 있다. 즉, 기존의 폐쇄된 환경, 알려진 단말 사용자 환경, 알려진 침입형태 등에 대응하기 위해 고안된 현재의 보안체계는 새로운 보안문제에 대응할 수 없다.

새로운 환경에서는 새로운 대응 방법이 필요한 것이다. 이에 대한 희망적인 새로운 대안이 네트워크접근제어(NAC)보안체계이다.



그러나, 현재 NAC 분야가 상당히 혼돈스러운 상황이어서 기업의 경우 구축하고자 할 경우 많은 고민을 갖게 되고, NAC 제품 벤더들 또한 제품 개발 로드맵 설정 시, 많은 고민을 갖고 있는 것이 사실이다. 이러한 원인에는 앞서 살펴본 NAC 아키텍처 표준화가 늦어지고 있기 때문에 현재 제시되는 제품들간 혹은 NAC 구축 시 연동되어야 할 기존 인프라(하드웨어, 소프트웨어)와의 통합 및 연동이 쉽지 않다는 것에서 기인한다.

2006년 5월에 개최된 “Interop”에 참여한 많은 전문가들은 “아키텍처 표준화 및 NAC 제품수준이 고객의 요구수준에 미치고 못하고 있고, 표준화가 완성되기 위해서는 상당한 시간이 더 필요한 것이 사실이다. 현재 시장에서 가장 어필할 수 있는 제품들은 표준화 작업만을 기다리지 않고 독자적으로 제품의 완성도를 높여가는 기업의 제품들이다”라고 말하고 있다.

따라서, 관련 단체들은 조속한 표준화 작업을 마무리 지어야 하며, NAC 벤더들은 이러한 표준화를 지속적으로 모니터링하며 관련 기술 및 기능을 발전시켜 상호호환성을 확보하면서 제품의 완성도를 높이려는 노력이 필요하다. 또한, NAC을 구축하고자 하는 기업들은 도입 전에 NAC 적용 범위, 적용 기능, NAC 적용 정책, 기존 인프라와의 통합방안에 대해 충분한 전략을 수립하고 기업환경과 동일한 상황에서 테스트를 수행한 후 도입하는 것이 필요하다.

Reference

[GTN] "Gartner's Network Access Control Model", Gartner, Lawrence Orans, 2 August 2005.

[MR1] "Getting the Knack of NAC", Mirrage Networks, Jan. 2006.

[MR2] "What you need to know about NAC", Mirrage Networks, Paul Desmond, 2006.

[SYN] "Network Access Control Technologies and Sygate Compliance on Contact", SYGATE, 2006.

[IR1] "Network Access Control", Interop Labs, Karen O'Donoghue, May 2006.

[IR2] "What is NAC", Iterop Labs, May 2006.

[IR3] "Getting Started with Network Access Control", Interop Labs, May 2006.

[IR4] "Network Access Control Resources", Interop Labs, May 2006.

[IR5] "What is TCG's Trusted Network Connect", Interop Labs, May 2006.

[IR6] "What is Microsoft's Network Access Protection", Interop Labs, May 2006.

[IR7] "What is Cisco NAC", Interop Labs, May 2006.

[IR8] "What is IETF NAC strategy", Interop Labs, May 2006.

[FRR] "Teleconference Implementation Access Control with Network Quarantine", Forrester, 01/02/2006

[HVD] "Network Access Control : Security Professionals Conference 2006 Seminar 02P", Kevin Amorin of Harvard Univ., Chris Misra of Messachusetts Univ.

[INF] "Enforcing Network Access Control : Market Outlook and Worldwide Forecast", Infornetics Research, January 2006.

[NW1] "End-to-End NAC remains difficult",, Network World, joel Snyder, 05/01/2006.

[NW2] "The Competition for NAC", Network World, Joel Snyder, 04/03/2006.

[NW3] "Interop : Trusted Computing demonstrates interoperability among vendors", Network World, Tim Green, 04/05/2006.

[NW4] "What is NAC anyway", Network World, Joel Snyder, 03/04/2006.

[EW1] "Sample RPF:Access Control", eWeek, Cameron Sturdevant, 31/10/2005.

[UN1] "2006 전략제품 발표회:Anyclick 설명 자료" , UNETsystem, 05/04/2006.

[UN2] "유넷시스넷-소프트런, NAC-PMS 통합솔루션 공동 개발" , 디지털데일리, 07/06/2006.