u-Campus내 네트워크 신뢰성 확보를 위한 NAC 도입 및 구축 로드맵*

이원진†, 김기원†, 부기동†
† 경일대학교 컴퓨터공학부
e-mail:wjlee@kumoh.ac.kr, nirk@paran.com, kdbu@kiu.ac.kr

Adopting NAC to guarantee reliability of u-Campus network*

Won-Jin Lee†, Kee-Won Kim†, Ki-Dong Bu†
† School of Computer Engineering, Kyungil University

요 약

오늘날 IT 환경의 변화는 내부 네트워크에서 새로운 보안위협이 발생하면서, 네트워크에 접근하는 접속단말기의 보안성을 강제화 할 수 있는 보안 인프라로서, NAC(Network Access Control)의 필요성이 증대고 있다. 최근 u-Campus 네트워크에서 다양한 보안위협에 대한 문제점을 해결하기 위해 NAC 도입 및 구축의 필요성이 높아지고 있지만, 기존 보안 솔루션과의 복잡한 연계관계 및 운영체제에 대한 유연성 결여 등 여러 문제가 도출되고 있다. 따라서 본 논문에서는 u-Campus 내 네트워크 신뢰성 확보를 위해 NAC 도입 및 구축 시 필요한 로드맵을 제시함으로서, 각 대학에서는 효율적인 NAC 솔루션 선택에 필요한 지침이 되며, 다양한 보안 위협을 사전에 방어하여 네트워크의 신뢰성 증진과 무결성을 유지할 수 있는 방안을 제시한다.

1. 서론

최근 급변하는 IT 환경에서 기존 보안체계로는 새롭게 증가하는 보안위협으로부터 효과적으로 대응할 수 없는 한계상황에 직면하고 있으며, PC, 노트북, PDA 등 다양한 모바일 단말기기의 이용 증가와 유·무선, 가상사설망(VPN) 등 내부 네트워크의 접속 방법이 다양화되어 외부에서 들어오는 유선 네트워크 통제만으로 내부 네트워크의 안전성이 보장되기 어렵다[1]. 또한 다양한 보안위협(해킹, 웜, 바이러스, 서비스 거부, 정보유출 등)이 외부가 아닌 내부 네트워크에서 많이 발생함에 따라 보안 문제가 중요시되고 있으며, 네트워크에 접근하는 접속단말기의 보안성을 강제화 할 수 있는 보안 인프라로서, IT 환경의 변화에 따라 NAC(Network Access Control)의 필요성이 증대고 있다. NAC는 사용자 단말(PC, 노트북, PDA 등)의 네트워크에 접근 시도 시 사용자가 정당한 사용자인지, 사용자 접속단말기는 사전에 정의해 놓은 보안 정책을 준수하고 있는 여부를 검사해 네트워크 접속을 통제하는 기법으로 기업·공공기관·대학 등에서 보안 위협에 노출된 접속단말 및 비인가 사용자는 내부 네트워크에 접속하지 못하도록 제어하는 솔루션이다[2].

u-Campus내에는 활동공간에 존재하는 센서·칩·라벨 등을 포함하는 사물들이 지능화·네트워크화라는 특징으로 인해 신뢰성 확보를 위한 정보보호 정책의 구현에 많은 어려움이 있으며, 다양한 보안위협 요소가 존재한다[3]. 특히 불특정 다수가 네트워크에 접속하므로, 각종 웜 및 바이러스, 해킹사고가 끊임없이 발생할 수 있는 가능성이 타 기관에 비해 높고, 외부 사용자보다 내부 사용자들이 시스템을 공격하는 경우가 많다. 그리고 학생들은 다양한 어플리케이션을 이용하며, 서버 구축 등 다양한 용도로 접속단말기를 사용하기 때문에 유해 트래픽이 많이 발생하고, 핸드폰, PDA, PMP 등 제어가 어려운 접속단말기가 u-Campus 네트워크에 접속하여 심각한 보안문제를 발생하였다. 이러한 문제점을 해결하기 위해 대학에서도 NAC 도입 및 구축 사례가 높아지고 있다. 하지만 다양한 보안 솔루션과의 복잡한 연계관계가 발생하여, 운영체제에 대한 제약이 많고 유연성이 떨어지며, 전산망 관리자들의 업무량도 높아지는 등 여러 가지 문제가 도출되고 있다.

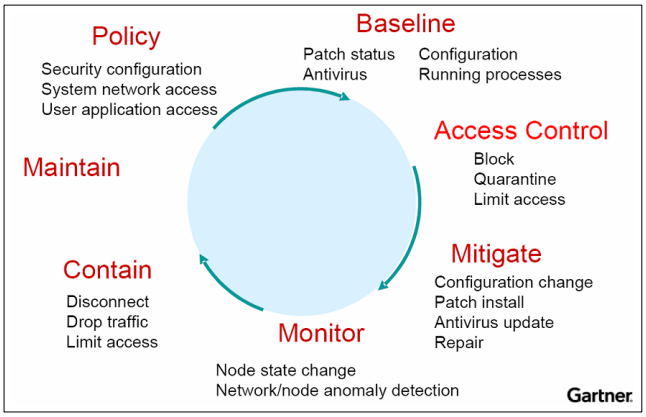
본 논문은 u-Campus 내 네트워크 신뢰성 확보를 위해 NAC 도입 및 구축 시 필요한 로드맵을 제시함으로서, 각 대학에서는 효율적인 NAC 솔루션 선택에 필요한 지침이 되며, 지능적으로 진행되는 다양한 보안 위협을 사전에 방어하여 네트워크의 신뢰성 증진과 무결성을 유지하고, 교육기관의 활용 및 효율을 극대화 시킬 수 있는 방안을 제시한다.

* 본 연구는 2008년 한국교육전산망 운영본부 연구 지원에 의하여 수행되었습니다.

2. NAC(Network Access Control)

NAC(Network Access Control)는 사용자 단말(PC, 노트북, PDA 등)의 네트워크에 접근 시도 시 사용자가 정당한 사용자인지, 사용자 접속단말은 사전에 정의해 놓은 보안정책을 준수하고 있는지 여부를 검사해 네트워크 접속을 통제하는 기법이다[4]. 이러한 NAC는 네트워크에 접속되는 단말기의 무결성을 확인하고, 보안정책에 위배되는 단말기를 예외 없이 통제 할 수 있도록 자동화 시켜주는 통제시스템이라고 할 수 있다[5][6][7]. 최근 차세대 보안의 핵으로 부상하고 있는 NAC는 다양한 방법으로 지능적으로 진행되는 보안위협으로부터 네트워크를 보호하기 위해 제시된 보안 방안으로 기존 보안 방법과는 여러 면에서 차별화된다. 기존 보안이 게이트웨이단의 방어를 수행했다면, NAC는 네트워크에 접근하는 모든 단말기를 검사하고, 보안정책에 위배되는 악성 단말의 접근을 차단함으로써 네트워크를 보호한다[8].

특히 2005년 가트너(Gartner) 그룹은 NAC 참조 모델을 정의 하였으며, 지속적인 접속단말기에 대한 보안평가, 보안문제에 대한 대응, 네트워크의 접근 허용, 보안 정책 준수에 대한 지속적인 모니터링 및 대응에 대한 순환 절차를 정의하였다. 그림 1은 가트너가 제시한 NAC 모델의 처리과정이다[9].



(그림 1) 가트너 NAC 모델의 프로세스

NAC 처리 과정은 안전하지 않은 시스템들이 네트워크 접근 권한을 얻는 것을 막고, 이미 연결되어 있는 시스템인데 만약 안전하지 않다면 네트워크 접근을 차단하여 네트워크 자원을 보호한다. NAC 처리 과정은 네트워크에 연결하려고 하는 단말기 또는 사용자의 보안 상태를 평가하고, 이미 연결되어 있는 단말기의 보안 상태를 모니터한다. 그리고 단말기의 상태, 위협 환경 및 사용자의 식별자의 상태를 기반으로 네트워크 접근과 시스템 치료(remediation) 정책을 시행한다.

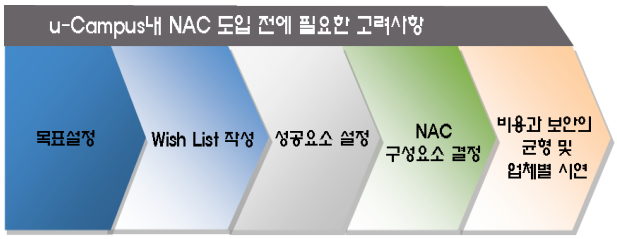
최근 각 대학에서는 다양한 IT 환경의 변화에 따라 대학 내 네트워크에 접근하는 접속단말기의 보안성을 강제화 할 수 있는 NAC 도입의 필요성이 커지고 있다.

3. 제안된 로드맵

본 장에서는 u-Campus 내 네트워크 신뢰성 확보를 위해 NAC 도입 및 구축 시 필요한 로드맵을 NAC 도입 전 고려사항, 도입 후 운영, 선도망 구축 사례의 3단계로 제안함으로서, 대학에서는 효율적인 NAC 솔루션 선택과 지능적으로 진행되는 다양한 보안 위협을 사전에 방어하여 네트워크의 신뢰성 증진과 무결성을 유지할 수 있는 방안을 제안한다.

3.1 NAC 도입 전 고려사항

u-Campus내 NAC를 도입하기 전에 고려해야 할 사항은 그림 2와 같이 목표설정, Wish List 작성, 성공요인 설정, 비용과 보안 균형, 업체 시연을 고려해야 한다.



(그림 2) NAC 도입 전 필요한 고려사항

1. 목표설정 : NAC 도입 전에 가장 먼저 고려해야 할 항목으로 네트워크 이용하는 대상자가 누구이며, 보안의 위협요소들은 어떤 것들이 존재하는지 분석해야하며, 도입할 NAC의 주요 역할은 어떤 것들이 있는지 확인하여, 실제 u-Campus 내 어느 곳에 적용할 것인가를 파악해야 한다.
2. Wish List 작성 : 대학에서는 사전에 철저한 계획과 분석 없이 NAC를 도입할 경우 실패하는 사례가 많으므로, NAC 도입에 따른 목표 설정과 더불어 Wish List를 작성해서 대학이 꼭 필요로 하는 것이 무엇인가를 상세히 살펴볼 필요가 있다. 이러한 Wish List는 u-Campus 내 NAC를 도입하기 전에 고려되어야 할 중요한 사항으로, NAC의 모든 기능을 사용하고 적용하는 것이 항상 최선은 아니다.
3. 성공요소 설정 : u-Campus내에 NAC를 도입에서 성공요인들은 어떤 것인 있는지 파악하여 성공 요인 리스트를 작성하는 것은 NAC 도입이 잘 진행될 수 있도록 도와준다.
4. NAC 구성요소 결정 : 위험요소의 명확한 리스트, 우선순위가 정해진 NAC 구성요소와 어디에 NAC를 적용할지에 대한 판단을 가지고 각 구성요소의 자세한 부분들이 결정되어야 한다. 각 구성요소는 사용자의 인증 방법, 엔드 포인트 보안 평가 방법, 접근 제어 강제 방법이다.
5. 비용과 보안의 균형 및 업체별 시연 : NAC의 보안성과 구축비용에 대해서 사전에 고려되어야 한다. 이처럼 보

안과 비용, 편의성간의 trade-off가 존재하며, 비용에 따른 적합한 수준의 보안성이 필요하다. 즉 어느 정도의 위협, 정보자산의 가치, 위험의 수용 정도도 고려해야 하며, 보안성의 성능과 편리성 저하 등의 관리 비용도 고려되어야 한다. 끝으로 마지막 사항은 업체 시연이다. NAC 도입의 목표 설정과 Wish-List 작성, 보안과 비용의 균형 등을 고려하여 설정한 목표와 요구 사항을 만족하는지, 어떠한 운영비용이 발생되는지를 업체 시연을 통해 확인한 후 제품을 선정해야 한다.

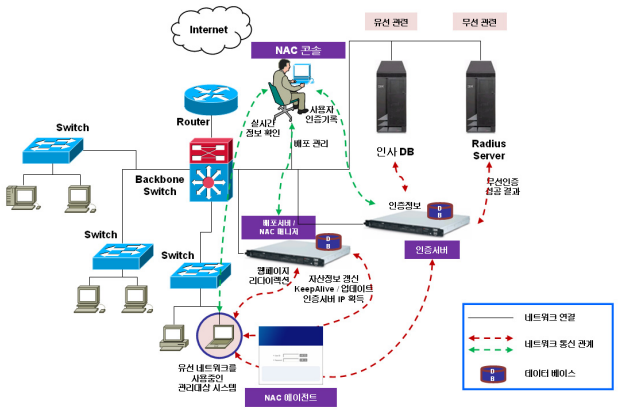
3.2 NAC 도입 후 운영

u-Campus내 NAC 도입 전 고려사항을 고려하여 NAC를 구축하였다면, 도입 후 최적의 운영(best practices) 정책이 필요하다. 최적의 운영(best practices)을 위해서는 보다 다양한 관점에서 살펴볼 수 있다. 다음 내용은 도입 후 운영에 필요한 항목들이다.

1. 보안 정책들은 단순하게 유지
2. Walk-before-you-run의 운영 과정이 필요
3. 지속적인 교육이 필요
4. 다양한 예외 사항에 대한 대책 수립이 필요
5. 이기종의 접속단말의 유형에 대한 대책
6. 비인가 사용자와 접속단말에 대한 대책

3.3 NAC 선도망 구축 사례

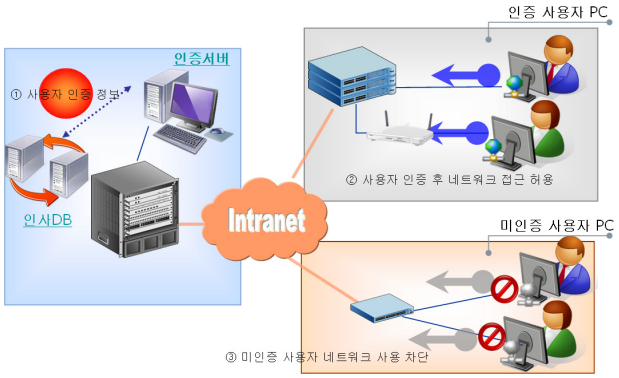
본 소절에서는 NAC 도입 전 고려사항들과 도입 후 운영 정책에 따라 NAC 구축 사례를 보여주고 있다. 그림 3은 도입한 NAC의 전체 구성도이다.



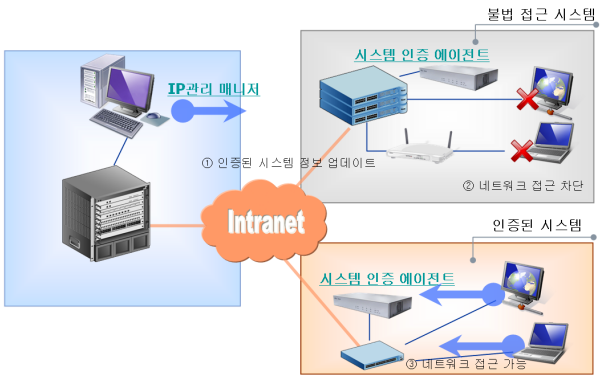
(그림 3) 도입한 NAC 전체 구성도

도입한 NAC는 NAC 콘솔, 배포서버/NAC 매니저, 인증서버, NAC 에이전트로 구성되어 운영된다. NAC 콘솔은 NAC의 전반적인 기능을 확인하거나 수행하며, 배포서버/NAC 매니저는 NAC 에이전트를 배포하고 에이전트가 설치된 시스템의 등록 정보를 관리한다. 배포서버는 NAC 에이전트 배포를 담당하고, NAC 매니저는 NAC 에이전트에 대한 등록 정보를 관리한다. 그리고 관리자가 관리하고자 하는 네트워크 접근 제어 대상 시스템인 NAC 에이전트는 배포서버에 의해서 NAC 에이전트가 설치되게 되면 시스템 사용자는 네트워크 사용을 위해서는 반드시 설치된 NAC 에이전트를 이용해서 인증을 받아야 네트워크 사용이 가능하게 된다.

도입한 NAC를 통하여 사용자 및 시스템 인증 절차는 그림 4와 그림 5 같이 수행된다. 먼저 사용자 인증 절차는 사용자 인증을 위해 대학 내 인사 데이터베이스 또는 인증 서버와 연동한 ID 기반의 사용자 인증 방식을 사용하며, NAC 에이전트를 이용한 사용자의 PC 자산 현황 정보도 수집할 수 있다. 그리고 비인가 사용자의 손쉬운 인프라 접근을 통제할 수 있고, 사용자에 대한 인증 및 권한을 수행한다. 그리고 시스템 인증 절차는 시스템(접속단말) 인증을 위해 시스템 인증 정보를 통해 접근 시스템에 대한 허용 및 차단 여부를 결정할 수 있으며, 시스템 인증 에이전트를 통하여 네트워크 접근 시스템의 IP, MAC, NIC제조사, 동작상태, 컴퓨터명, 사용자 인증 에이전트 동작 상태 등의 정보 제공한다. 또한 시스템의 네트워크 접근 정보와 IP변경 정보, IP정책 위한 정보를 모니터링 할 수 있다.



(그림 4) 구축한 NAC에서 사용자 인증 절차



(그림 5) 구축한 NAC에서 시스템 인증 절차

4. 결론

u-Campus내 네트워크 환경에 NAC 구축은 오늘날의 다양한 지능적 위협을 사전에 방어할 수 있다. 하지만 대학 네트워크는 오픈 서비스를 지향하는 대학의 특성상 교내 네트워크에 누구나 쉽게 접속이 가능하다. 이러한 대학 캠퍼스 망의 문제점은 다양한 보안 위협이 존재한다. 이러한 이유로 일부 대학에서는 NAC 솔루션을 도입하고 있지만, 여러 가지 문제가 도출되고 있다. 그래서 본 논문에서는 u-Campus내 NAC 도입 및 구축 시 필요한 로드맵을 NAC 도입 전 고려사항, 도입 후 운영, 선도망 구축 사례의 3단계로 제시함으로서, 각 대학에서는 효율적인 NAC 솔루션 선택에 필요한 지침이 되며, 교육기관망의 활용 및 효율을 극대화 시킬 수 있는 방안을 제시하였다.

참고문헌

[1] 권덕일, “NAC(Network Access Control) 기술동향 분석 및 적용방안에 관한 연구”, 동국대학교 국제정보대학원, 2006.

[2] Daniel V. Hoffman, "Implementing NAP and NAC Security Technologies: The Complete Guide to Network Access Control", Wiley, 2008.

[3] 임재현, “대학에서의 u-Campus 구축”, 한국교육학술정보원, 2006.

[4] 김성훈, 이강신, 최광희, 이진태, “최종 사용자단(Endpoint) 정보보호 키워드, NAC(Network Access Control)”, 한국정보보호진흥원 CSO 브리핑 기술정책 06-05, 2006.

[5] Mirage Network, “Getting the Knack NAC: Understanding Network Access Control”, A Mirage Networks Industry Report, 2006.

[6] Interop Labs, “Getting Started with Network Access Control”,2006.

[7] Interop Labs, “Network Access Control Resources”, 2006.

[8] 임재성, “Network Access Control Overview”, UNET White Paper, 2006.

[9] Gartner, “Gartner’s Network Access Control Model”, 2005.