차세대 C4I망 설계를 위한 NAC 기반의 보안체계 구축 방안

신창건*, 이희조**
*고려대학교 컴퓨터정보통신대학원 소프트웨어공학과
**고려대학교 컴퓨터. 통신공학부
e-mail : {seraph81, heejo}@korea.ac.kr

A Way to make network secure with NAC for next-generation C4I network

ChangGun Shin*, HeeJo Lee**
*Graduate School of Computer and Information Technology, Korea University
**Dept. of Computer Science & Engineering, Korea University

요 약

현재 우리군의 C4I망은 전략용 A망, 화력용 B망, 정보용 C망 등 각기 업무 및 기능의 특성에 따라 별도의 망을 구축하여 사용하고 있으나 상호 서버간의 데이터 연동을 위해 별도의 연동망을 추가로 구성하여 운용함에 따라 네트워크의 구조가 복잡하고 보안기능을 구성하기 위한 소요도 많이 발생하고 있다. 또한 타 전산망에서 들어오는 웜·바이러스 보다 내부 사용자에 의해서 유포되는 웜·바이러스의 문제가 전체 네트워크에 미치는 영향이 더욱 심각한 실정이다. 그럼으로 각 C4I 전산망 통합에 따라 발생하는 문제점 해소 및 종단 보안강화의 새로운 대안으로 네트워크 접근 제어 즉 NAC(Network Access Control)는 가장 적합한 보안 기술 이다. 본 논문에서는 군의 C4I 망에서 NAC 시스템을 구축 할 때 고려해야할 사항과 네트워크 인프라의 교체를 최소화하는 방법으로 단계적인 구축방법을 제시하여 사용자와 관리자 모두에게 최적의 환경을 제시 할 수 있는 방법에 대해서 연구를 수행한다.

1. 서론

최근 IT기술의 급속한 발전과 해킹 기술의 다변화에 따른 복합적인 위협 환경에 대처하기 위해 우리군의 C4I 망은 네트워크의 보안과 보호를 위해 기본적으로 각 전산망의 최전방에 방화벽을 도입하고 IPS, 바이러스 월 등 수많은 게이트웨이용 솔루션을 도입하여 운영 중이며 CERT 전문 인력 양성을 통해 24시간 침해행위 관제 및 바이러스 방역활동을 실시하고 있지만 아직도 윈도우 운영체제 보안취약점을 이용해 공격하는 새로운 형태의 네트워크 웜의 피해에 신속하게 대처하기는 어려운 실정이다. 이러한 현상은 전산망을 운영하는 그 어떤 기업이나 학교기관도 마찬가지 이며 이런 형태의 바이러스로 부터 절대 자유롭지 않은 상태이다. 이런 문제에 대한 해답으로 떠오른 것인 '엔드포인트 보안'이다 많은 웜이나 악성코드의 공격 대상이 취약점을 가진 사용자의 컴퓨터로 옮겨가고 있다. 결국 적절한 보안 정책이 이루어지지 않은 컴퓨터, 예를 들어 윈도우 운영체제 보안 패치 미 적용 혹은 컴퓨터 바이러스백신 미 설치 컴퓨터들이 이런 네트워크 웜의 공격 대상이 되고 있으며 공격당한 내부 컴퓨터는 바이러스를 유포하는 숙주가 되어 내부 컴퓨터를 공격, 감염시키며 나아가서는 내부 네트워크 전체를 위협하는 존재가 되고 있다.

NAC(Network Access Control, 네트워크 접근제어)는 결국 위와 같이 엔트포인트 사용자 보안에 대한 고민에서 시작되었다. 엔드포인트 사용자 보안에 대한 고민이란 부적합 컴퓨터에 대한 네트워크 접근제어와 감염 컴퓨터에 대한 적절한 교정 작업을 어떻게 현재의 기업이 가지고 있는 통합된 환경 속에서 구현할 수 있을까 하는 고민으로부터 비롯된 것이다.

이에 본 논문에서는 일반적으로 웜, 바이러스 확산 방지 및 사용자 통제에 사용되고 있는 NAC(Network Access Control, 네트워크 접근제어)를 이용하여 차세대 C4I망을 구축하기 위한 방안을 연구하고자하며 이를 위해 각종 C4I 네트워크 통합 및 단위 보안 솔루션을 통합함으로써 사용자 및 관리자 측면에서의 기대교화를 극대화 하고 웜 및 바이러스, 비인가 사용자에 의한 피해 및 정보유출의 대응으로 활용할 수 있는 방안을 연구해 보고자 한다.

2장에서는 NAC에 대한 관련 연구로써 NAC가 무엇인지를 이해하고, NAC에 대한 각종 아키텍처와 관련기술 및 활용범위를 분석할 것이다. 3장에서는 NAC를 이용한 차세대 C4I망 구축 방안을 제안하며, 4장에서는 결론을 제시 하였다.

2. 관련연구

2.1 NAC 개념

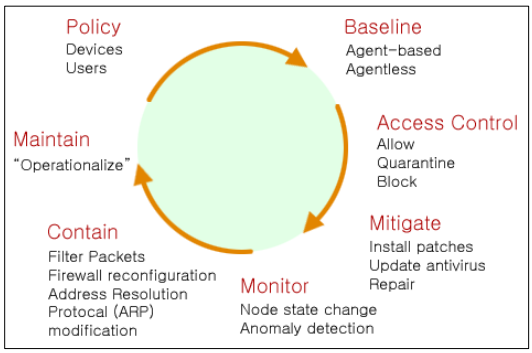
NAC 솔루션은 적절한 권한을 가진 사용자가 보안이 검증된 안전한 PC로 내부 네트워크 자원에 접속할 수 있도록 제어하는 사용자 접속 제어 솔루션이다. NAC 보안기술에 있어 핵심은 바로 엔드포인트의 보안기술을 기존 네트워크 보안체계와 결합해 전체 네트워크에 통합보안 체계를 구현하는 것이다. NAC 솔루션의 가장 큰 기능은 첫 번째, 네트워크에 접속하는 PC의 사용자가 올바른 사용자인진 먼저 인증을 하고, 두 번째, 사용자가 사용하는 PC가 현재 보안위협에 적절히 방어할 수 있는 메커니즘(안티바이러스, 윈도우 패치, 개인방화벽 등)이 제대로 운용되고 있는지 확인하며, 세 번째, 이렇게 인증된 결과에 따라 최종적으로 사내 전산망에 접속할 수 있는 권한을 부여 또는 제한하는 것이다.

즉, '적적한 권한을 가진 사용자가 보안 검증이 된 안전한 PC로 사내 네트워크 자원에 접속할 수 있도록 제어할 수 있게 되는 것'이다. 이렇게 올바른 사용자가 바이러스, 웜, 그리고 악성코드에 안전하다고 검증된 PC로 사내 네트워크에 접속한다면 접속하는 장소가 어디건, 어디서 접속하건 IT관리자는 사내망 보호와 보안을 보다 손쉽게 관리 운용할 수 있게 되는 것이다. 또한 사용자별 또는 그룹별 접근 권한 지정을 통하여 각종 서비스 및 망에 선택적으로 접근 할 수 있도록 사용자를 통제 할 수 있다

이러한 설정을 하기위하여 보안 관리자가 보안정책을 적용시 가장 기본이 되는 정책을 베이스라인(Baseline) 이라고 한다. 베이스라인은 보안정책이 먼저 수립되고 나서, 네트워크에 접속하려는 접속 단말의 보안상태를 비교하여 수립된 보안정책의 요구조건을 충족한 단말에 대해 네트워크 사용을 허가 하는 것이다. 이러한 절차는 접속단말의 네트워크 연결방식을 상관하지 않고 수행되어야 한다.

즉, 안전한 네트워크를 보장하기 위하여 LAN, WAN, 무선, IPsec, SSL, VPN 접속 시 베이스라인 평가가 먼저 수행되어야 한다.

아래의 (그림 1)은 Gartner에서 제시한 NAC의 접근통제 흐름을 나타낸 것이다.

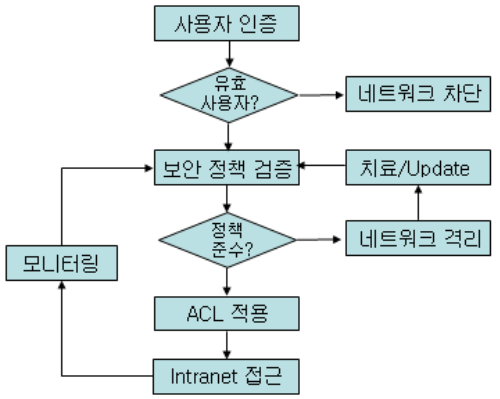


(그림1) NAC 접근통제 흐름도

Gartner의 NAC 구축 모델은 접속 단말에 대한 보안 평가, 보안문제에 대한 대응, 네트워크 접근허용, 보안정책 준수에 대한 지속적인 모니터링 및 대응에 대한 업무 순환 절차 등에 대하여 표현한 것으로 주요 골자는 다음의 여섯 단계로 정리할 수 있다.

① 장비・유저에 대한 인증정책과 시스템 체크 정책 수립
② 수립된 정책을 기반으로 한 접속 단말에 대한 보안 평가 실시
③ 평가결과에 의한 접근통제 실시
④ 격리 단말의 치료를 위한 패치 및 백신업데이트 조치
⑤ 단말 상태 변화에 대한 세팅과 네트워크 허용
⑥ 지속적인 모니터링 및 대응

등이 Gartner가 제시하고 있는 NAC의 기능이며 이 여섯 단계의 업무 순환 절차를 반복하면서, 보안을 향상시킬 수 있어야 한다. (그림 2)는 NAC 시스템 동작 절차 개념도이다.



(그림 2) NAC 시스템 동작 절차 개념도

이러한 베이스라인 평가 결과에 기반 하여, 접근통제(Access Control)는 접속 단말에 미리 정의된 수준의 네트워크 접근권한을 부여한다.

예를 들어, 베이스라인을 따르는 접속단말의 경우 전체 네트워크 또는 권한에 맞는 네트워크 영역에 대한 접근권한을 부여할 수 있고, 베이스라인을 따르지 않는 접속단말의 경우, 네트워크 접근을 완전히 차단하거나, 치료를 위한 특정 네트워크 영역으로의 접근만을 허용할 수 있다.

NAC의 가치를 높이기 위해서는 이러한 치료절차가 자동화 되어야 한다.

즉, Help Desc의 도움을 받지 않고 문제가 있는 접속 단말이 치료될 수 있어야 한다는 것이다.

접속 단말이 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 접속 단말을 네트워크로부터 분리하고, 엑세스 스위치의 접근제어 정책에 등록하여 해당 포트로의 접속을 허용치 않도록 하는 것이 필요하다.

2.2 NAC의 구성요소

NAC의 구성을 위해서는 필수적으로 NAC 서버, NAC 업데이트 서버, NAC Controller, NAC Enforcer, NAC Agent 와 같은 구성 요소가 필요하다. 경우에 따라 모든 네트워크 환경이 802.1X를 지원한다면 802.1X를 지원하지 않는 네트워크를 위한 장비인 NAC Enforcer는 필요가 없을 것이다. <표 1>는 NAC의 구성 요소에 대한 설명이다.

<표 1> NAC의 구성 요소

구성요소	설 명
NAC 서버	• 사용자 인증관리, IP관리, 사용자 계정, 정책 관리 기능을 제공하는 서버 • 장애시를 위한 이중화 필요
NAC Controller	• 802.1X가 지원하는 환경에서 NAC를 구현하기 위한 장비 • NAC Agent 설치 유무와 인증을 위한 장비
NAC Enforcer	• 802.1X가 지원되지 않는 환경에서 NAC를 구현하기 위한 장비 • NAC Agent 설치 유무와 인증을 위한 장비
NAC Agent	• NAC 구성을 위한 PC에 설치되는 프로그램
NAC Update 서버	• 필수 S/W의 설치를 위하여 격리존에 구성되는 서버 • 설치 유도 화면을 구성하는 서버

3. NAC를 이용한 차세대 C4I망 구축

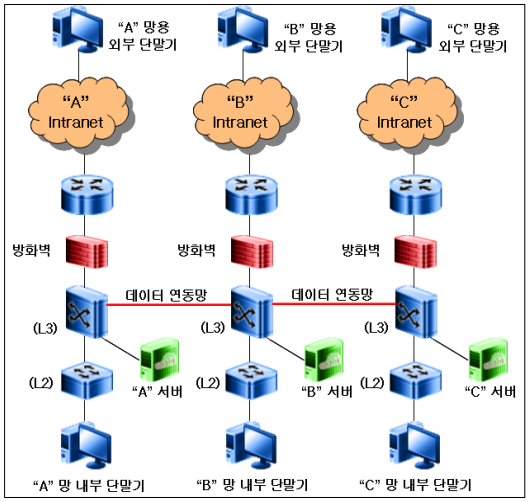
지금까지 살펴본 NAC의 기능을 이용하여 실제 보안솔루션을 C4I망에 적용하기 위한 방안과 기대효과, 그리고 효과적인 구성을 위한 고려사항 등을 살펴보도록 하겠다.

3.1 현재의 C4I 연동망 구조

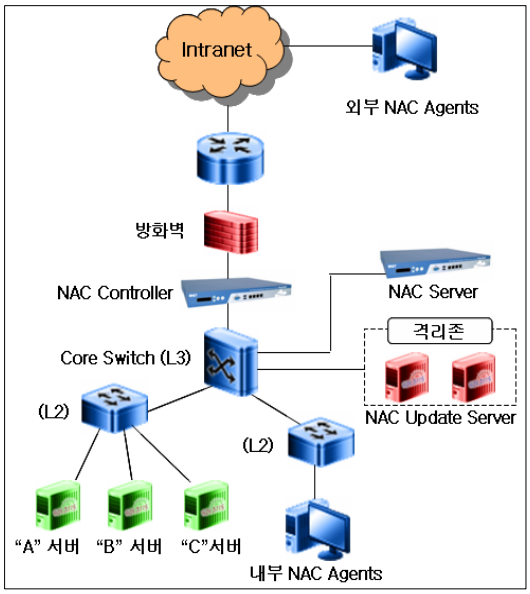
(그림 3)은 현재의 C4I 연동망 구조이다. 현재의 C4I 구조는 각기 업무 및 기능의 특성에 따라 별도의 망을 구축하여 사용하고 있으나 상호 데이터의 연동을 위해 별도의 연동망을 추가로 구성하여 운용함에 따라 네트워크의 구조가 복잡하고 보안기능을 구성하기 위하여 각각 보안시스템을 구축하여 운용함으로서 통합관제가 어려우며 관리자의 관리소요도 많이 발생하고 있다. 또한 웜·바이러스에 대한 신속한 대처와 단말기에 대한 백신업데이트 및 윈도우 업데이트 등의 관리가 어려운 실정이다.

3.2 NAC를 적용한 C4I 연동망 구조

(그림 4)는 NAC를 적용한 C4I 연동망 구성 방안 이다. 이 경우는 802.1X를 지원하는 네트워크라고 가정하고 구성하였다. 그럼으로 802.1X를 지원하는 환경을 구성하기 위해서 내부 네트워크의 관문인 방화벽 하단에 NAC Controller를 설치였고 이를 통해 외부에서 접속하는 원격 단말기 및 내부 단말기에 대한 NAC Agent 설치 유무 확인과 인증을 실시한다. 그리고 내부 네트워크 L3에 사용자의 기능별, 권한별 특성에 따른 사용자 인증 및 정책관리를 위한 NAC Server를 설치한다. NAC 서버는 장애시를 위해 이중화로 구성한다. 그리고 정책 미준수 PC의 격리 및 치료를 위한 격리존을 만들고, 설치유도를 위한 NAC 업데이트 서버를 설치한다.



(그림 3) 현재의 C4I 연동망 구조



(그림 4) NAC를 적용한 C4I 연동망 구조

3.3 NAC 적용시의 기대효과

NAC의 적용시 기대할 수 있는 효과로는 첫째 접근통제, 이는 네트워크에 접속한 PC의 사용자가 올바른 사용자인지를 판단하여 비인가 사용자의 경우 네트워크를 차단하고 인가된 사용자라 할지라도 PC가 보안 요구조건을 충족하였는지를 판단하여 미 충족시 별도의 격리존으로 이동 사용자가 쉽게 필요한 패치를 설치한 후 재접속 할수 있도록 사용자를 통제할 수 있다.

둘째 정보유출 차단, IT기술의 급격한 발전으로 인해 최근의 웜·바이러스는 시스템의 무력화를 위한 목적에서 개인정보나 기업의 정보를 수집하는 목적으로 변화하고 있다. 이는 개인이나 기업뿐만 아니라 국가와 국민을 지키는 군의 입장에서도 예외라 할 수 없다. 아무리 인터넷과 독립되어 있는 네트워크라 할지라도 USB와 같은 보조기억매체를 통해 웜·바이러스가 네트워크내에 유입되면 취약한 PC에 감염되고 웜·바이러스가 정보를 수집하여 다시 인터넷 PC에 보조기억매체를 접속시 정보가 유출될 수 있기 때문이다. 그러나 NAC를 적용하면 사용자의 PC가 보안위협에 적절히 방어할 수 있는 메커니즘(안티바이러스, 윈도우패치, 개인방화벽 등)을 구축함으로써 웜·바이러스로 인한 정보유출을 예방할 수 있다.

셋째 네트워크 통합, 우리군의 C4I망은 각기 업무 및 기능의 특성에 따라 네트워크를 분리하여 사용하고 있다. 이는 불필요한 정보의 접근을 차단함으로서 정보의 유출을 방지하기 위한 목적이 있지만 네트워크 인프라 구축 및 보안시스템 구축 등 관리적 측면 및 유지보수 측면에 어려움이 많다. 하지만 NAC를 적용하면 각각 분리되어 있는 네트워크를 통합 하더라도 NAC Server의 사용자 인증관리 기능을 통해 사용자 PC에 설치된 NAC Agent 통제함으로써 필요한 서버 및 그룹의 네트워크에만 접근할 수 있도록 통제할 수 있다. 그럼으로 NAC의 활용은 정보유출의 예방 및 탐지, 각종 네트워크 및 보안시스템의 통합의 효과가 있으며 결과적으로 사용자 및 관리자 측면에서 보안수준을 높일 수 있는 기대효과를 가지고 있다.

3.3 NAC 적용시 고려사항

일반적으로 NAC를 적용할 때 고려해야할 사항은 각종 네트워크 장비들과의 호환성 문제, 802.1X를 지원하는 환경과 그렇지 않은 환경의 구분, 사용자 인증을 위한 내부의 인증서버와의 연동을 충분히 고려해야 한다. 그리고 NAC는 Windows XP이상의 운영체제에서만 운영이 가능하기 때문에 PC 운영시스템과의 호환성 문제도 고려해봐야 할 사항이다. 군의 C4I망은 각종 인증시스템 및 선로, 단말기의 암호모듈 등 보안을 위한 추가적인 시스템이 있지만 이는 NAC를 적용하기 전이나 후나 동일하게 적용하는 부분이고 군의 특성상 보안장비의 언급을 할 수 없음으로 본 논문의 고려사항에서 생략했다.

4. 결론

현재의 IT 보안기술은 여러 가지 다양한 변화를 요구하고 있다. 왜냐하면 기존의 폐쇄된 환경, 알려진 단말 사용자 환경, 알려진 침입형태 등에 대응하기 위해 고안된 현재의 대응기술로는 새로운 보안문제에 대해서 신속하게 대응할 수가 없기 때문이다. 이러한 상황에서 NAC의 기술동향을 분석하고 네트워크 보안의 효율적 적용방안을 모색함으로서 NAC의 무결성 기반의 보안기술이 네트워크 보안의 효육적 방안이 될 수 있는지를 연구해 볼 필요가 있었다. 본 논문에서는 NAC의 군 C4I망 적용 방안 분석을 통해 NAC 구성 방식, 개념에 대해서 알아보았으며, NAC 아키텍처 분석을 통하여 NAC 구성요소와 데이터 흐름에 대해서 알아보았다. 그리고 기존 군 C4I망의 단말 사용자PC 보안 강화 및 사용자 관리강화, 망의 복잡성 해결 등에 대한 방안으로 NAC를 적용한 차세대 C4I망 설계 방안을 제안 하였으며 위에서 언급한 기대 효과와 적용시 고려사항을 도출하였다.

참고문헌

[1] 디지털 데일리, “2006년 차세대 네트워크, 엔드 포인트 통합보안세미나” 발표자료, 2006.09

[2] 권덕일, “NAC(Network Access Control) 기술동향 분석 및 적용방안에 관한 연구, 동국대학교 국제정보대학원 석사학위 논문, 2007.

[3] 김홍승, “기업 정보유출 대응을 위한 NAC(Network Access Control) 활용 방안에 關한 硏究

[4] Heary, Cisco NAC Appliance : Enforcing Host Security With Clean Access, Macmillan Technical Pub, 2007.

[5] Cisco NAC, 기술백서. http://www.cisco.com/go/nac

[6] Microsoft NAP, 기술백서. http://www.microsoft.com/nap

[7] 디지털데일리, “특별기획 NAC/3부 마이크로 소프트‘NAP’

[8] 한수진, “NAC, 네트워크 보안의 새 지평 연다.”, 보안뉴스, 2006.10. http://www.boannews.com/know_how/view.asp?idx=882&search=title&find=NAC

[9] 장성일, “NAC의 불은 꺼지지 않는다”, 유넷시스템

[10] 안호철, “”기업내부의 보안파수꾼 NAC” CIO Korea 2007. 1. http://www.ciokorea.com/jsp/article/article_magazine_view.jsp?nm_gubun=PPCD01&&nm_id=6918