NAC(Network Access Control)을 이용한 컴퓨터 네트워크 보안 플랫폼 구성

Computer Network Security Platform Configuration with NAC

노철우, 강경태, 이지웅, 전재현
신라대학교 컴퓨터정보공학부

Ro chul-woo, Kang kyung-tae, Lee ji-woong, Jeon jae-hyun
Division of Computer and Information Engineering, Silla University

요약

본 논문에서는 Extreme 스위치와 Cisco 라우터를 이용하여 가상의 네트워크를 구현하였으며 PIX 방화벽을 통해 외부 네트워크로부터의 보안을 강화하였고 내부 네트워크에 대한 보안 문제점은 802.1X 기반의 인증방식을 사용한 NAC를 적용시켜 구현함으로써 외부와 내부 네트워크의 통합적인 보안 플랫폼을 구성하였다.

Abstract

NAC(Network Access Control) technology is intended for authentication of internal networks access through various paths. In this paper, we build computer network platform using NAC and Extreme switch and confirm authentication for the platform. The platform consists of PIX, NAC and authentication server.

Ⅰ. 서론

기존의 바이러스 백신이나 방화벽 등을 이용한 보안 체계에서는 적합한 보안패치 및 업데이트를 하지 않아 많은 취약점들이 늘어나고 있는 실정이다. 따라서 사전에 인가되지 않는 사용자, 보안에 위협을 줄 수 있는 사용자의 접근이 불가피할 뿐만 아니라 악성 코드 및 바이러스 침입과 더불어 트래픽으로 인한 피해가 증가하고 있다. 이러한 취약점을 보완하기 위해서, 기존 네트워크 보안체계에 추가적으로 엔드 포인트에 대한 보안 기술정책을 마련하여 내부 네트워크 제어, 트래픽 탐지 및 허가되지 않은 사용자에 대한 접근 제한 그리고 보안에 취약한 시스템에 대한 안전성을 고려한 최적의 보안이 이루어져야 할 것이다[1,2].

Ⅱ. NAC

NAC의 동작원리는 어느 경로를 통한 접근인지에 관계없이 모든 사용자의 인증을 수행하며 사용자의 컴퓨터에 대한 검사를 수행한다. 패치 및 바이러스 백신과 개인 방화벽 유무 등의 검사 그리고 인증 등의 절차를 Radius-Server (RS)에 설정된 정책과 비교하여 검사 결과를 바탕으로 사용자의 접근을 허용 또는 차단한다. 이와 같이 네트워크 전반적인 보안 구축 시스템이 이루어지는 것이 NAC이다.

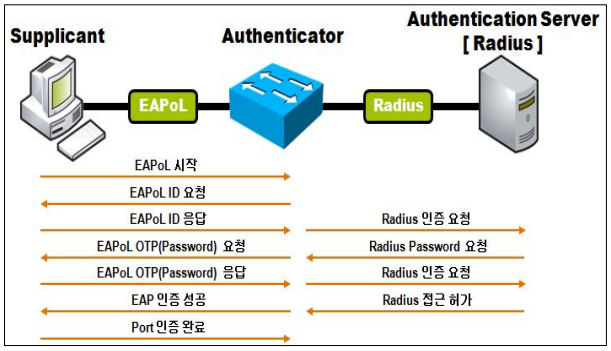
NAC은 기업마다 소프트웨어 기반과 네트워크 기반의 솔루션을 모두 포함시키기도 한다. 몇몇 기업들은 Infrastructure 기반 NAC 이라고 부르기도 하나 기업에서 채택한 기술 기반과 구현 기능에는 조금씩 차이가 있기 때문에 뚜렷한 표준이 정해지지 못하였다. 따라서 NAC 솔루션을 분류하는 기준과 관점이 제 각각 다르게

정의되어 있다[1,2].

Ⅲ. NAC을 이용한 네트워크 보안 플랫폼

1. 구현 방식

NAC의 인증 방식에는 802.1X 인증, MAC 인증 그리고 Web 기반 인증이 있으며, 본 논문에서는 기존에 흔히 쓰이던 보안 플랫폼 기반 위에 802.1X 인증을 이용한 NAC을 적용시켜 새로운 보안 플랫폼을 구현하였다[2]. 그림 1은 802.1X의 인증 절차를 나타낸 것이다.

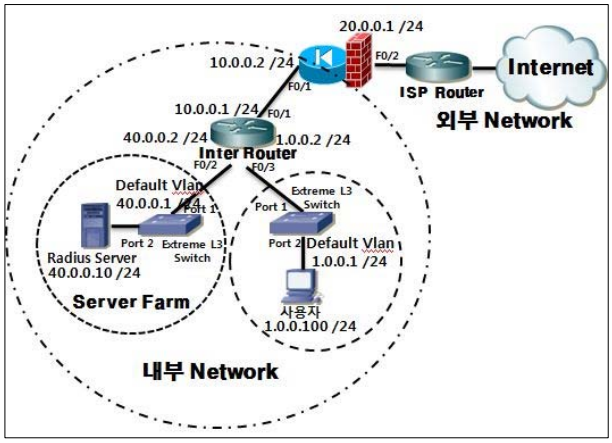


▶▶ 그림 1. 802.1X의 인증 절차

보안 플랫폼 기반 위에 802.1X 인증을 이용한 NAC을 적용시켜 새로운 보안 플랫폼 구현방식은 기존에 흔히 사용되는 PIX 방화벽을 이용한 외부 네트워크로부터의 보안 플랫폼을 구현하고 사용자와 직접 연결되는 스위치에 NAC을 설정함으로써 사용자는 Server Farm의 RS로부터 접근에 대한 인증을 받게 된다. 이러한 구현을 통해 PIX 방화벽을 통한 외부 네트워크로부터의 보안과 NAC을 이용한 내부 네트워크의 보안을 동시에 접목시킬 수 있다[3,4].

2. 라우터, 스위치, PIX 의 구현 설정

본 논문에서는 Extreme Networks의 L3 스위치를 사용하여 RS와 사용자에 각각 연결시켰다. 그리고 Extreme Networks에서 NAC 기능인 Netlogin(넷로그인)을 구현하였다. 구현한 전체 구성도는 그림 2와 같으며, 그림 3과 그림 4는 RS와 사용자에 각각 연결된 스위치의 설정이다.



▶▶ 그림 2. 전체 구성도

```
# config default ipaddress 40.0.0.1 /24
# create ospf area 40.0.0.0
# enable ipfowarding default
# conf ospf add default area 40.0.0.0
# enable ospf
```

▶▶ 그림 3. Server Farm의 스위치 설정

```
# config default ipaddress 1.0.0.1 /24
# create ospf area 0.0.0.0
# enable ipfowarding default
# config ospf add default area 0.0.0.0
# enable ospf
# config radius primary server 40.0.0.10 1812
client-ip       1.0.0.1
# config radius primary shared-secret TEST
# enable radius
# enable netlogin ports 1-24 default
# enable dot1x
```

▶▶ 그림 4. 사용자와 연결된 스위치 설정

RS 서버의 IP와 Client-IP(사용자와 연결된 스위치의 IP)를 입력하고 공유키를 서버와 같은 TEST로 설정하였다[4]. 그리고 그림 5는 내부 네트워크내의 Inter Router 설정을 나타낸 것이고, 그림 6은 외부 네트워크로부터의 내부 네트워크 보안을 위한 PIX 방화벽의 설정이다.

```
# interface FastEthernet 0/1
# ip address 1.0.0.1 255.255.255.0
# no shutdown
# interface FastEthernet 0/2
# ip address 40.0.0.2 255.255.255.0
# no shutdown
# interface FastEthernet 0/3
# ip address 1.0.0.2 255.255.255.0
# router ospf 0
# network 1.0.0.0 0.0.0.255 area 0
# network 10.0.0.0 0.0.0.255 area 0
# network 40.0.0.0 0.0.0.255 area 0
```

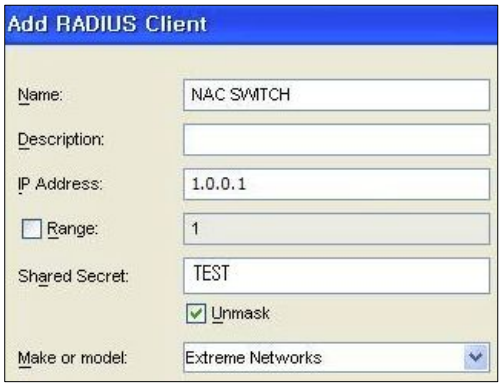
▶▶ 그림 5. Inter Router 설정

```
# interface FastEthernet 0/1
# nameif inside
INFO: Security level for "inside" set to 100 by default
# ip address 10.0.0.2 255.255.255.0
# no shutdown
# interface FastEthernet 0/2
# nameif outside
INFO: Security level for "outside" set to 0 by default
# ip address 20.0.0.1 255.255.255.0
# no shutdown
# router ospf 0
# net 10.0.0.0 0.0.0.255 area 0
# net 20.0.0.0 0.0.0.255 area 0
```

▶▶ 그림 6. PIX 방화벽 설정

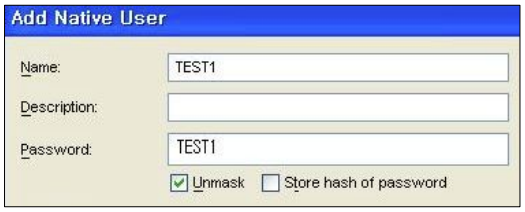
PIX 방화벽 설정 시 inside 보안 레벨은 100, outside 보안 레벨은 0의 값으로 각각 default설정이 이루어진다[5,8]. 이로 인하여 내부 네트워크에서는 특별한 제한 없이 외부 네트워크와의 통신이 이루어지지만 외부 네트워크에서 내부 네트워크로의 접근에는 정책에 따른 제한이 이루어지게 된다[6,7].

3. Radius-Server의 구현 설정



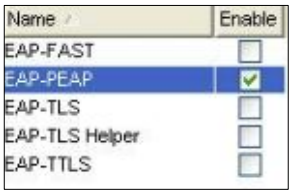
▶▶ 그림 7. RS 클라이언트 설정

그림 7은 Radius-Server의 클라이언트 설정으로 여기서 클라이언트는 사용자와 직접 연결되는 스위치를 나타낸다. 그림 2의 구성도에 표기된 것과 같이 IP는 1.0.0.1을 설정하였고, 공유키는 TEST로 설정한다.



▶▶ 그림 8. 접근이 허가 될 사용자 등록

그리고 그림 8과 같이 허가된 사용자가 내부 네트워크로 접근을 할 수 있도록 서버에 해당 사용자의 이름과 패스워드를 등록시킨다.

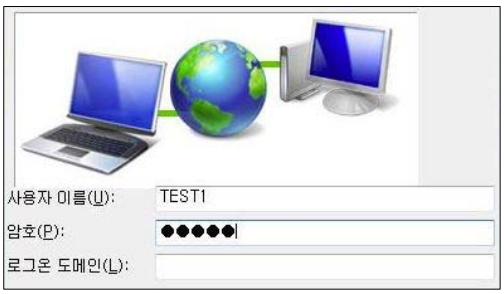


▶▶ 그림 9. EAP 인증 유형

또한 그림 9는 접근 허가를 원하는 사용자가 이름과 패스워드를 입력하였을 경우, 해당 정보를 EAP-PEAP 방식을 통해 서버와의 안전한 인증과정을 거칠 수 있게 한다[2,9].

Ⅳ. 실험 및 결과 분석

본 논문에서 구현한 보안 플랫폼을 설정한 뒤, 사용자가 내부 네트워크로의 접근을 원할 경우 사용자의 자격증명을 요구한다. 사용자의 자격증명은 사용자의 접근 허용 여부를 구분하기 위함이다.



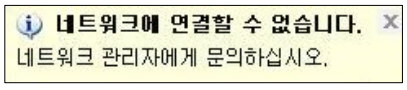
▶▶ 그림 10. 사용자 자격증명

그림 10은 서버에 등록된 사용자 TEST1 으로 접속을 시도한 그림이고, 인증에 성공하였을 경우 클라이언트 스위치에서 그림 11과 같은 인증확인 화면을 볼 수 있다.

```
port:1,          vlan: Default,        State: Authenticated
    Mac          IP address    Auth    Type      User
00:1A:80:D6:96:21   1.0.0.100      Yes     802.1x
TEST1
```

▶▶ 그림 11. 인증 성공 후 show netlogin

하지만 허가되지 않은 사용자가 자격증명을 하였을 경우에는 그림 12-1과 같은 메시지와 함께 스위치에서는 그림 12-2와 같은 인증 실패를 화면을 볼 수 있다.



▶▶ 그림 12-1. 자격 증명 실패

```
port:1,          vlan: Default,        State: Unauthenticated
    Mac          IP address    Auth    Type      User
00:1A:80:D6:96:21     0.0.0.0        No      802.1x
PC-Name
```

▶▶ 그림 12-2. 인증 실패 시 show netlogin

Ⅴ. 결론

본 논문에서는 기존의 외부 네트워크에서 내부 네트워크로의 접근에 중점을 둔 보안 플랫폼을 기반으로 하여 내부 네트워크의 보안 정책인 NAC을 적용시켜 구현해보았다. PIX를 통해 외부 네트워크로부터의 보안을 강화시키고 NAC을 통해 내부 네트워크에 대한 보안까지 강화시켰다. 그 결과 더욱 확실하고 체계적인 보안성을 보장할 수 있으며, 더불어 관리자의 편의성 또한 제공할 수 있는 것을 확인할 수 있었다.

그리고 내부 네트워크로 접근하는 사용자의 바이러스 백신, 특정 소프트웨어의 버전, 업데이트 상태 등 지정된 요구 사항을 정하고, 그 요구사항에 맞지 않을 경우 접근을 제한하는 NAP(Network Access Protection) 솔루션 까지 구현하여 연동하게 될 경우 한층 더 발전된 보안 플랫폼을 연구할 계획이다.

■ 참 고 문 헌 ■

[1] Knipp, "시스코 : 네트워크 보안", 에이콘, 2005.

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

[3] 노철우, 박상식, 이희성, 이지웅 "컴퓨터 네트워크 보안 기술에 대한 연구" , IT.디자인연구 논문집, 제4호, 2009.

[4] 노철우, "Extreme 네트워크 아카데미", 신라대학교 출판부, 2004.

[5] 하재철, "(실무로 배우는) 네트워크 보안 = Network Security", 미래컴, 2008.

[6] 김재선, "(About)Firewall & Network security", 영진닷컴, 2002.

[7] Held, Hilbert, "Cisco Security architectures", McGraw-Hill, 1999.

[8] Behtash, Behzad. "CCSP self-study : Cisco Secure PIX Firewall advanced (CSPFA)", Cisco Press, 2004.

[9] Network Working Group of The Internet Society, Request for Comments: 3748, Extensible Authentication Protocol (EAP), The Internet Society, 2004.