네트워크 펌웨어를 이용한 Agent-less 방식의 네트워크접근제어 구현에 관한 연구

김진석*, 민성기**, 오상석***
*고려대학교 컴퓨터정보통신대학원
**고려대학교 융합소프트웨어전문대학원
***고려대학교 컴퓨터·전파통신공학과
*jinseok@songpa.go.kr, **sgmin@korea.ac.kr, ***ssoh94@korea.ac.kr

Research of Agent-less Network Access Control Using Network Switch Firmware

JinSeok Kim*, Sung-Gi Min**, Sang-Seok Oh***
*Graduate School of Computer Information & Communication, Korea University
**Graduate School of Convergence IT, Korea University
***Dept. of Computer & Radio Communications Engineering, Korea University

요 약

내부 네트워크의 IP관리를 위해 많은 네트워크 관리 방안 및 솔루션들이 기 구축되어 운영 중이고, 이를 위해 내부 네트워크에 연결된 모든 단말에 특정 Agent를 설치하여 IP를 관리하고 있어 단말(PC, IPT전화기 등)의 OS에 따른 기종별 Agent의 호환문제 및 단말에 기 설치 운영중인 응용프로그램과의 충돌문제가 발생한다. 본 연구에서는 이러한 네트워크 IP관리를 위해 Agent가 필요 없는 네트워크 관리 방식을 제안한다. 네트워크 Switch장비 Firmware의 포트차단 설정을 이용한 기법으로 Agent의 설치 없이 Switch장비의 Firmware를 이용하여 네트워크의 접근제어가 가능함을 제안한다. 이를 위하여 인가되지 않은 IP를 Switch장비의 Firmware로 차단하여 네트워크의 접근제어가 가능함을 증명하였다.

Keyword : NETWORK, NAC, IP, SWITCH

1. 서론

방화벽, IPS, IDS등의 장비를 통해 외부로부터의 전체 네트워크에 대한 공격을 예방하고 있지만 결국 대부분의 보안문제는 내부 사용자의 보안 불감증에서 비롯한 개인 PC의 허술한 보안관리 및 불특정인의 손쉬운 내부 네트워크의 접속으로 인해 발생하고 있다.

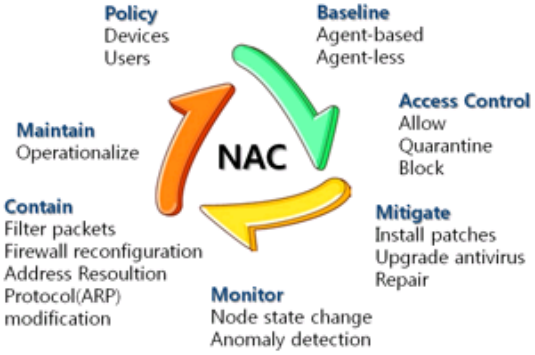
이러한 문제는 외부의 침입에 대비하는 보안과 더불어 내부 네트워크 관리의 필요성을 대두하게 되었고 그 일환으로 네트워크접근제어(NAC, Network Access Control) 보안기술이 효과적인 대응 방안으로 대두 되었다[1].

현재 상용화 되어 설치 운영중인 네트워크접근제어 솔루션 중 Switch에 연결된 모든 단말에 Agent를 설치하여 구동하는 방식의 경우 단말의 종류에 따른 Agent 설치불가 및 단말에 기 설치 운영중인 특정 응용프로그램과의 충돌 등의 문제가 야기되어, Agent-less방식의 네트워크 접근제어 방식이 대두 되었으나 이 역시 Backbone의 Mirror Port를 이용한 IP Spoofing이나 Backbone 상단에 컨트롤 장비를 통한 IP관리로 차단 대상 IP가 Backbone으로 접근을 하지 않는다면 내부 네트워크의 모든 단말로 접근이 가능한 문제점을 갖고 있다.

본 연구에서는 Backbone에 의존한 Agent-less방식의 문제점을 해결하고 전체 네트워크 속도에 추가 리스크가 전혀 발생하지 않는 Switch장비의 Firmware를 이용한 네트워크 접근제어 방식을 제안하였으며 본 논문의 구성은 다음과 같다 2장에서는 Agent-less 방식의 네트워크접근제어에 대해 설명하였고 3장에서는 Switch장비의 Firmware를 이용한 Agent-less 방식의 네트워크접근제어를 구현하고 4장에서는 제안한 네트워크접근제어 방식을 실험을 통해 입증 하였으며 5장에서는 종합적인 결론과 앞으로 수행해야 할 연구 과제에 대하여 언급하였다.

2. Agent-less 방식의 네트워크접근제어

네트워크 접근제어의 사전적 의미로는 망의 감독 및 조정을 위한 제어와 관련된 여러 가지 일. 시스템 동작의 감시, 데이터의 정확성 보장, 사용자 확인 기록, 시스템의 접근 및 변경, 사용자의 접근을 위한 방법들을 포함한다[2]. (그림1)은 가트너그룹에서 정의한 참조모델이다.



(그림1) 네트워크접근제어 흐름도

<표1>에서와 같이 네트워크접근제어(NAC)는 무선/모바일 보안(79.3%) 다음으로 다른 보안 시스템에 비해 전년(2009)대비 네트워크접근제어(58.6%)의 높은 매출 증가율을 보여 내부 네트워크 보안의 필요성이 대두됨을 확인할 수 있다[3].

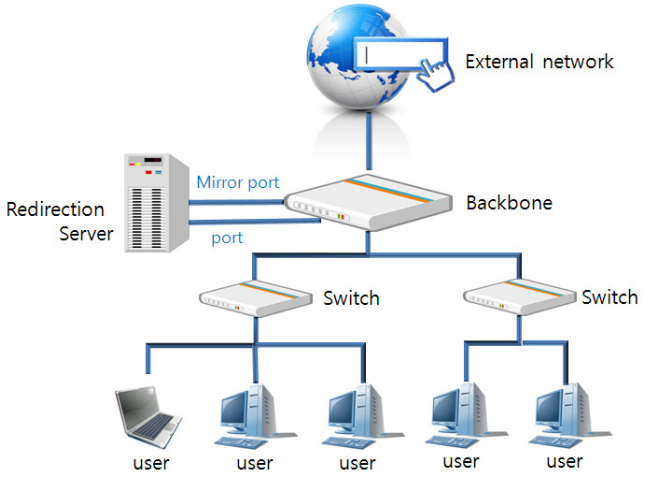
<표1> 정보보안 제품의 매출 현황

구분	2009년	2010년	증감률
웹 방화벽	43,411	49,957	15.1
네트워크 방화벽	41,602	49,572	19.2
침입방지시스템(IPS)	62,850	71,337	13.5
DDoS차단시스템	13,048	18,850	44.5
통합보안시스템(UTM)	42,283	62,336	47.4
가상사설망(VPN)	51,357	45,714	-11.0
네트워크접근제어(NAC)	**16,940**	**26,875**	**58.6**
무선/모바일보안	14,872	26,672	79.3

단위 : 백만원

(그림1)에서와 같이 상용화된 네트워크접근제어 솔루션은 크게 Agent-based방식과 Agent-less방식 두 가지로 나눌 수 있다. Agent-based방식은 내부 네트워크에 연결된 모든 단말에 Agent를 설치하여 네트워크를 관리하는 방식으로 모든 단말에 설치된 Agent를 통해 강력한 통제 및 관리가 가능하지만 이를 위해 단말의 OS별 Agent 설치 호환, 미설치단말의 확인불가 및 단말에 기 설치되어 운영 중인 특정 응용프로그램과의 충돌 등의 문제가 발생한다.

(그림2)와 같은 Agent-less방식은 Backbone에 의존한 Web Page Redirection기법으로 모든 단말에 Agent의 설치 없이 내부 네트워크에 간단한 작업만으로도 네트워크 접근제어가 가능하다 하지만 모든 단말이 외부 인터넷을 사용한다는 것을 전제로 하기 때문에 인터넷만 사용하지 않는다면 내부의 모든 단말에 악성코드배포 및 해킹등의 범죄를 방지할 수 없는 치명적인 문제가 발생한다.



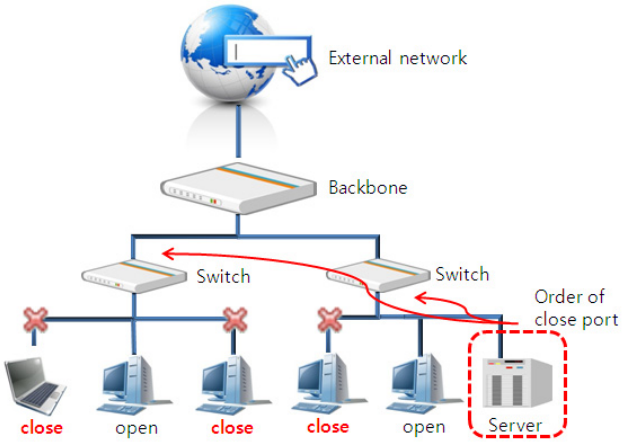
(그림2) Agent-less방식의 네트워크접근제어 구성도

3. Firmware를 이용한 네트워크접근제어 구현

Agent-less 네트워크접근제어 방식의 문제점인 Backbone에 국한된 네트워크 트레픽 차단 및 유도를 Switch단에서 차단하여 인가받지 않은 IP는 내부 네트워크에 Port자체를 차단하는 방식을 제안한다.

일반 기업체에서 사용하는 Switch장비는 대부분 자체 Firmware가 존재하며 Firmware에는 자체 브랜드사에서 제공하는 접속 ACL(Access Control List)기능을 포함한다.

본 연구에서는 Extreme Networks Switch장비의 Firmware인 Extremeware XOS Software의 동적 ACL을 이용하여 Agent-less 네트워크접근제어를 구현하였다.



(그림3) Firmware를 이용한 네트워크접근제어 구성도

Switch장비의 Firmware를 이용하면 (그림2) Agent-less 방식의 네트워크접근제어 구성도에서 사용되던 Redirection Server의 도움 없이 같은 네트워크 망에 연결된 PC 1대로 새로운 Agent-less방식의 네트워크접근제어 구성이 가능하다 (그림3)은 Switch장비의 Firmware를 이용한 네트워크접근제어 구성도이다.

인가되지 않은 IP의 Port 차단은 Extremeware XOS Software의 Dynamic ACL 명령인 (명령어1)을 이용하여 차단정책을 생성하고 (명령어2)를 이용하여 (명령어1)에서 생성한 차단정책을 Switch장비에 적용한다[4].

```
create access-list <dynamic-rule> <conditions>
<actions> {non-permanent} {application
<appl_name> }                                    (1)
```

```
configure access-list add <dynamic_rule> [[[first
| last]{priority <p_number>}][[before | after]
<rule>] | [priority <p_number>]] [any | vlan
<vlanname> | ports <portlist>] {ingress | egress}
{zone <zone>} {application <appl_name>}          (2)
```

(명령어1)과 (명령어2)를 이용하여 인가되지 않은 IP의 차단된 Port는 (명령어3)을 이용하여 해당 IP가 정상적인 통신이 가능하도록 적용할 수 있다[4].

configure access-list delete <dynamic_rule> [any | vlan <vlanname> | ports<portlist> | all] {ingress | egress} {application <appl_name>} (3)

4. 구현한 네트워크접근제어 방식의 실험

성능평가를 위해 Switch장비 1대와 PC2대를 이용하였다. 테스트를 위한 Switch장비는 “Extreme Summit X 150-24p” 장비를 사용하였고 IP는 192.168.10.1을 이용한다. 차단 명령을 내릴 PC의 IP는 192.168.10.61을 이용하였으며, 대상이 될 PC의 IP는 192.168.10.60을 사용하였다.

실험은 (그림4)과 같이 Switch장비의 차단 IP조회 명령을 통해 차단된 Port 및 IP가 존재하지 않음을 확인하였고, (그림5)와 같이 차단 대상PC(192.168.10.60)로의 Ping 테스트를 통해 네트워크의 접근이 가능함을 확인하였다.

```
ExtremeXOS
Copyright (C) 2000-2008 Extreme Networks. All rights rese
Protected by US Patent Nos: 6,678,248; 6,104,700; 6,766,4
7; 6,859,438; 6,912,592; 6,954,436; 6,977,891; 6,980,550;
7,017,082; 7,046,665; 7,126,923; 7,142,509; 7,149,217; 7,
45,619; 7,245,629; 7,269,135.
================================================================

Press the <tab> or '?' key at any time for completions.
Remember to save your configuration changes.

* X150-24p.1 # show access-list
No entry found!
```

(그림4) Switch 장비에서 대상PC 차단 전

```
C:₩Documents and Settings₩user>ping 192.168.10.60

Pinging 192.168.10.60 with 32 bytes of data:

Reply from 192.168.10.60: bytes=32 time=1ms TTL=128
Reply from 192.168.10.60: bytes=32 time<1ms TTL=128
Reply from 192.168.10.60: bytes=32 time<1ms TTL=128
Reply from 192.168.10.60: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.60:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:₩Documents and Settings₩user>_
```

(그림5) 대상 PC의 네트워크 가능 확인

이제 (그림6)과 같이 Switch장비에 차단 ACL을 등록 후 (그림7)과 같이 대상 PC(192.168.10.60)로의 Ping이 차단됨을 확인 하였다.

```
* X150-24p.5 # create access-list name1 "source-address 192.168.10.60/32;
ation-address 0.0.0.0/0;" "deny"
Error:  Entry name1 has already been created
* X150-24p.5 #
* X150-24p.5 #
* X150-24p.5 #
* X150-24p.5 #
* X150-24p.5 #
* X150-24p.5 # create access-list test1 "source-address 192.168.10.60/32;
ation-address 0.0.0.0/0;" "deny"
* X150-24p.6 # configure access-list add test1 last any
 done!
* X150-24p.7 # show access-list
Vlan Name     Port   Policy Name          Dir      Rules  Dyn Rules
================================================================
*             *                           ingress  0      1

* X150-24p.8 #
```

(그림6) Switch 장비에서 대상PC 차단 후

```
C:₩Documents and Settings₩user>ping 192.168.10.60

Pinging 192.168.10.60 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.60:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:₩Documents and Settings₩user>_
```

(그림7) 대상 PC의 네트워크 불가능 확인

마지막으로 (그림8)의 Switch장비의 차단명령 해지 후 (그림9)와 같이 대상PC(192.168.10.60)로의 Ping 테스트를 통해 다시 네트워크의 접근이 가능함을 확인하였다.

```
* X150-24p.8 # configure access-list delete test1 all
* X150-24p.9 # show access-list
No entry found!
* X150-24p.10 #
```

(그림8) Switch 장비에서 대상PC 차단 해지 후

```
Pinging 192.168.10.60 with 32 bytes of data:

Reply from 192.168.10.60: bytes=32 time=1ms TTL=128
Reply from 192.168.10.60: bytes=32 time<1ms TTL=128
Reply from 192.168.10.60: bytes=32 time<1ms TTL=128
Reply from 192.168.10.60: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.60:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:₩Documents and Settings₩user>
```

(그림9) 대상 PC의 네트워크 다시 가능 확인

5. 결론

이 실험에서 알 수 있듯이 네트워크접근제어의 구현에 있어서 Agent나 Redirection Server 등 추가 장비나 솔루션 없이 단지 Switch장비의 Firmware 명령(ACL)만으로 전체 네트워크의 특정 IP를 차단 및 해지가 가능함을 확인하였고, 이를 이용해 네트워크접근제어가 가능함을 증명 하였다. 지금의 실험방식은 Telnet을 이용해 Switch장비에 직접 접속하여 확인하고 차단하는 방식으로 이루어 졌으나 향후 텔넷 접속이 가능한 응용 프로그램을 개발하여 보안관리자가 원하는 IP를 클릭 한번으로 차단 및 해지가 가능하게 한다면, 네트워크접근제어를 위해 단지 관리자가 보유한 실행파일(exe) 한 개로 가능할 것이다.

참 고 문 헌

[1] 전한수, “NAC시스템 구축에 따른 사용자 보안강화에 대한 연구” 고려대학교 석사 2008. 07

[2] 백승현, 김승광, 박홍배, “사내 네트워크 보안을 위한 네트워크 접근제어시스템 설계 및 구현” 전자공학회지 47(12) 90-96 ISSN 1975-2377 KCI 2010

[3] KISA, “(KISA보도자료)2010년 국내 정보보안시장은 1조1천억원” 2011. 03

[4] Extreme, “Extremenetworks 스위치 운영자메뉴얼 / 정비교본” 2007