Journal of the Korea Academia-Industrial cooperation Society
Vol. 15, No. 10 pp. 6310-6316, 2014

http://dx.doi.org/10.5762/KAIS.2014.15.10.6310
ISSN 1975-4701 / eISSN 2288-4688

IPv6 기반의 네트워크 접근제어 시스템 설계 및 구현

신해준[1*]
[1](주)넷맨 연구소

Design and Implementation of Network Access Control based on IPv6

HaeJoon Shin[1*]
[1]**Research Institute, NetMan Co., Ltd.**

요 약 인터넷 사용자 및 스마트 디바이스의 증가로 네트워크 보안의 중요성이 점차적으로 커지고 있다. 네트워크 보안의 세부기술들은 방화벽, IPS, DDoS차단시스템, UTM, VPN, 네트워크 접근제어시스템, 무선네트워크보안, 모바일보안, 망분리 등으로 구성된다. 현재 하드웨어 인프라는 이미 IPv6를 위한 기능을 지원하고 있지만 IPv6 기반 서비스의 제공은 미진하여 대부분의 보안제품들은 IPv4에서 동작하고 있다. 그러므로 본 논문에서는 IPv6를 지원하는 보안 기술인 네트워크 접근제어 기능을 설계하고 이를 위해 필수적으로 요구되는 IPv6 단말의 탐색, 차단/격리 그리고 128bit IPv6 주소의 효율적인 관리를 위한 도메인자동 할당 기능을 설계 및 구현하였다. 이를 위해 KISA에서 실제 구축한 IPv6 환경에서 보편적 단말들에 적용이 가능하도록 구현하였다. 결과적으로 보편적으로 사용하고 있는 IPv6 장비들에 대해서 유·무선 호스트 검출, 차단, 격리 및 도메인 할당이 정상적으로 동작하는 것을 확인할 수 있었다.

Abstract The increase in the Internet and smart device users requires high-level network security. Network security consists of Web Firewall, Network Firewall, IPS, DDoS system, UTM (Unified Treat Management), VPN, NAC (Network Access Control), Wireless security, Mobile security, and Virtualization. Most network security solutions running on IPv4, and IPv6 network services are not sufficiently ready. Therefore, in this paper, this study designed and implemented important functions of Network Access Control (NAC), which include IPv6 host detection, isolation, blocking and domain assignment for the IPv6 network. In particular, domain assignment function makes 128 bits IPv6 address management easy. This system was implemented on a KISA IPv6 test-bed using well known devices. Finally, the test result showed that all IPv6 based wired and wireless devices were well-controlled (detection, blocking, isolation and domain assignment).

Key Words : Pv6, Network Access Control, Host Detection, Network Blocking, Domain Assignment

1. 서론

ICANN의 IPv4 주소의 고갈과 최종할당 정책에 따라 전세계적으로 IPv6 로의 전환이 급속히 이루어지고 있다. 특히 클라우드 네트워킹과 사물인터넷(IoT)의 시장 확대로 IPv6의 요구는 지속적으로 확대될 것으로 판단된다. 이미 네트워킹 장비(라우터, 스위치)와 같은 인프라 구성장비는 이미 IPv6를 위한 기능을 포함하여 지원하고 있지만 이러한 네트워크 상에서 적용되는 서비스들 중에서 현재 IPv6 지원이 가능한 기술은 미비한 상황이다. 물론 기존의 솔루션을 IPv6에서 적용할 수 있도록 IPv4/IPv6 듀얼스택, 터널링, 주소변환 등의 IPv6 전환기술을 활용하고 있으나 IPv6로의 확대는 시점의 문제일 뿐 필연적이라 할 수 있다[1,2].

인터넷사용자의 증가와 모바일 디바이스의 증가로 인한 유▪무선 네트워크의 확대는 다양한 보안 문제를 야기하고 있고, 사물인터넷(IoT)의 확대는 지금까지 고려되지 않았던 더 많은 보안문제를 발생시킬 것이다. 일반

*Corresponding Author : HaeJoon Shin(NetMan Co., Ltd.)
Tel: +82-53-652-8051 email: fisher@yumail.ac.kr
Received June 5, 2014 Revised (1st July 2, 2014, 2nd July 15, 2014) Accepted October 10, 2014

적으로 네트워크 보안은 기능분류상으로 웹 방화벽, 네트워크 방화벽, 침입방지시스템(IPS), DDoS 차단 시스템, 통합보안시스템(UTM), 가상사설망(VPN), 네트워크 접근제어(NAC), 무선 네크워크 보안, 모바일 보안, 가상화(망분리) 영역으로 구성이 된다[3]. 다양한 보안제품과 기술들이 제시되고 있지만 대부분의 경우가 IPv4 환경에서 동작하고 있다. 실제로 IPv6를 지원하는 네트워크 장비는 72.8%, 서버 단말은 68.7% 인 반면에 보안은 19.1%로 준비율이 매우 낮다[4].

그러므로 본 연구에서는 IPv6 네트워크에 적용 가능한 네트워크 접근제어 시스템을 제안하고자 한다. IPv6 기반의 네트워크 접근제어는 IPv6 단말의 탐색, 미인가 단말의 차단/격리 및 사용자인증 유도, IPv6 주소의 효율적인 관리를 위한 인가된 단말의 도메인 자동 할당 기능은 필수적으로 포함해야 하므로 이에 대한 구현 방안을 제시한다. 이러한 기능을 포함하는 네트워크 접근제어 기술은 IPv6 only 네트워크 뿐 만 아니라 IPv4/IPv6 듀얼스텍을 가지고 있는 네트워크 환경에서도 적용이 가능하다.

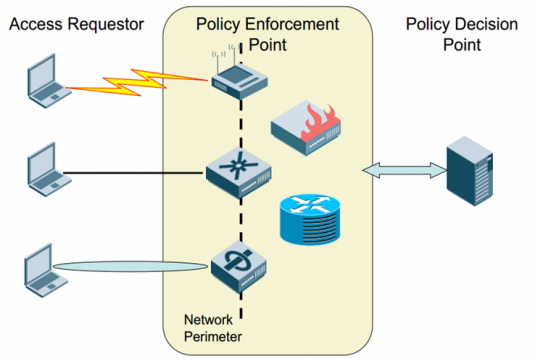
본 논문의 2장에서는 현재까지 개발된 IPv4 기반의 네트워크 접근제어의 기능과 제어위치에 따른 NAC의 특성을 분석하고, 3장에서는 본 논문에서 제안하는 IPv6 환경에서의 네트워크 접근제어 구현 방안을 설명한다. 4장에서는 실험결과를 분석하고, 5장에서 본 논문의 결론을 맺는다.

2. 관련연구

2.1 Network Access Control

네트워크 접근제어(Network Access Control : NAC)는 내부 네트워크로 접근하려는 단말기와 네트워크 상태를 검사해 위험 요소의 접속을 원천 차단하는 시스템으로 내부보안 강화를 위한 목적으로 개발되었다. 네트워크 스스로 무결성을 유지할 수 있도록 하는 NAC는 데스크톱PC, 노트북, 스마트폰, 태블릿PC 등 업무에 사용되는 단말의 종류가 다양해지면서 더욱 중요도가 높아지고 있다. NAC는 네트워크에 접속하려는 단말기가 본인에 의해 사용되고 있으며, 권한에 따라 접근을 시도하는지 검증해야 한다. 특히 일반 유선 환경에서는 최소한의 보안요구 사항을 충족하기 위해서 ID/PW, MAC, IP 주소 인증 등이 필수적으로 요구된다.

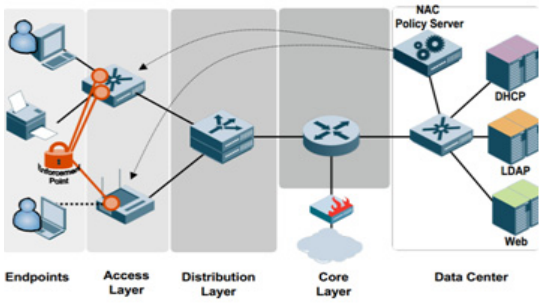
일반적인 NAC의 구조는 Fig. 1과 같이 네트워크 접근 정책을 결정하는 정책서버(Policy Decision Point)와 정책을 강제하는 에이전트(Policy Enforcement Point) 그리고 내부망에 접속을 요청하는 단말(Access Requester)로 구성된다.



[Fig. 1] Structure of Network Access Control

2.2 Control의 위치에 따른 NAC의 분류

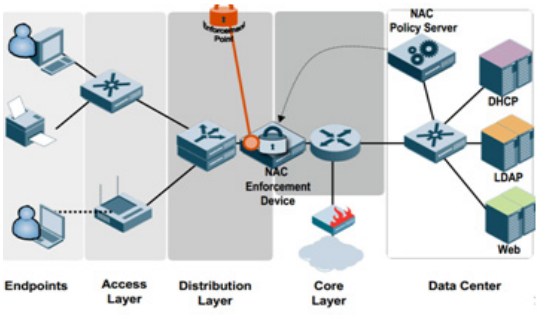
네트워크 접근제어(NAC)는 정책을 강제하는 Policy Enforcement Point의 위치와 기능에 따라서 크게 4가지 종류로 구분된다[5].



[Fig. 2] Edge Enforcement NAC

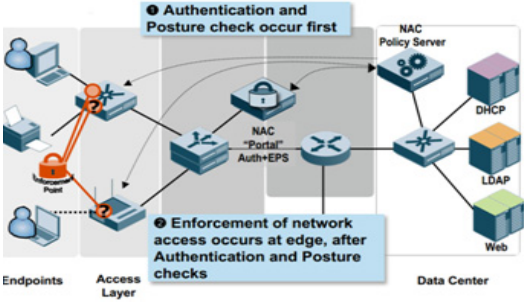
Edge Enforcement NAC은 Fig. 2와 같이 정책서버가 네트워크의 끝단에 있는 장치(Switch, AP 등)에게 정책을 내리고, 네트워크 장치들이 접속제어를 강제할 책임을 가지며 접속 단말의 탐지, 격리, 차단 등의 기능을 실행하게 된다. MAC 기반의 802.1x 인증이 대표적인 기술이라 할 수 있다. 네트워크 접속점에서 정책이 실행되므로 실행속도가 빠른 장점이 있다. 하지만 이를 위해서 모든 네트워크 장비가 802.1x를 지원해야 하므로 인프라 구축에 비용이 많이 발생하는 것이 단점이다.

Fig. 3에서 보여주고 있는 Inline Enforcement NAC에서는 정책강제 에이전트가 스위치의 미러링 포트에 연결되어 네트워크 트래픽 분석을 통해서 상태를 파악하고 문제가 있는 단말에 대해서 접속을 차단 또는 격리하게 된다.



[Fig. 3] Inline Enforcement NAC

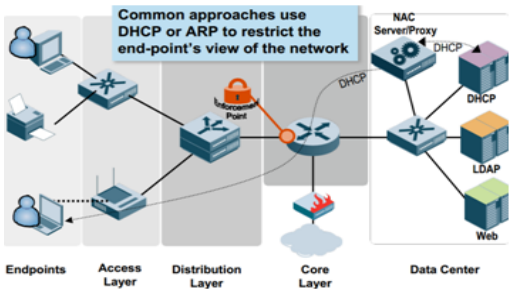
장비의 구성이 가장 간단한 장점이 있다. 하지만 대규모 사이트의 경우 발생하는 트래픽의 양이 커지게 되어 정책강제 에이전트의 부하가 크게 발생하는 단점이 있다.



[Fig. 4] Hybrid(inline+edge) Enforcement

Edge Enforcement NAC와 Inline Enforcement NAC의 장점을 조합하여 만든 방식이 Fig. 4의 Hybrid Enforcement NAC이다. 사용자 인증 등은 Edge 방식을 사용하고, 인증을 제외한 네트워크 접속과 관련된 정책 실행은 Inline 방식을 사용한다. Edge 방식에 비해 다양한 정책적용이 가능하고, Inline 방식에 비해 정책강제 에이전트의 부하를 줄일 수 있는 장점이 있다. 단점은 Edge 방식처럼 인프라 구축에 많은 비용이 발생한다.

마지막으로 살펴볼 Network Protocol NAC의 동작 구조는 Fig. 5와 같다. 현재 가장 많이 사용하는 NAC 기법이며 정책강제 에이전트가 DHCP 또는 ARP 같은 프로토콜을 활용하여 단말의 탐색, 접속의 차단과 격리 그리고 IP주소의 할당을 수행하게 된다. 단일 서브네트워크 또는 VLAN 사용시 다수개의 서브네트워크 단위로 정책강제 에이전트가 배치되어 정책을 실행한다. 서브네트워크별로 정책강제 에이전트가 설치되어야 하는 비용적인 단점이 있으나, IP관리 기술을 효율적으로 적용할 수 있고 다양한 IP기반의 기술로의 확장이 가능한 장점이 있다.



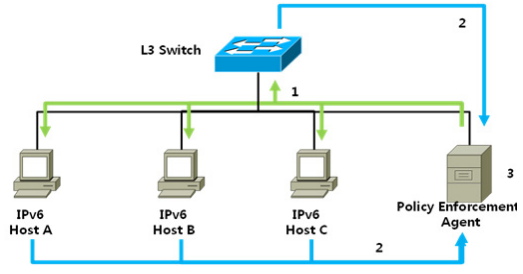
[Fig. 5] Network Protocol(ARP, DHCP)

그러므로 본 논문에서는 NAC의 분류상 Network Protocol 방식의 접근제어 기술을 활용하고 IPv6 네트워크로의 확장을 위해 IPv6 호스트의 탐색, 미인가 호스트의 차단/격리 알고리즘을 제안하고 또한 IPv6 주소의 효율적인 관리를 위한 도메인 할당 방안을 제안하고자 한다.

3. IPv6 기반 NAC

3.1 IPv6 호스트 탐색

네트워크 접근제어 기능 구현에 있어서 호스트의 탐색은 가장 기본 기능이며 핵심 기능이라 할 수 있다. 그러므로 본 논문에서는 MLD(Multicast Listener Discovery) 활용한 IPv6 호스트 탐색방법을 제안하고자 한다.



[Fig. 6] Searching Procedure by MLD

1. 정책강제 에이전트가 MLD 패킷을 네트워크에 전송(Broadcasting)
2. MLD를 수신한 네트워크 내 호스트는 자신이 속한 Multicast 그룹 정보를 참조하여 Multicast Listener Report 패킷을 정책강제 에이전트에 전송
3. 정책강제 에이전트가 호스트들에게서 수신한 Multicast Listener Report 패킷에서 호스트 정보(IP, MAC) 획득

MLD는 IPv4에서 사용되는 IGMP(Internet Group Management Protocol)을 대체해서 만들어진 IPv6 기반의 프로토콜이다. 본 논문에서 제안하는 MLD를 이용한 IPv6 호스트 탐색 절차는 Fig. 6과 같다.

MLD를 이용한 IPv6 호스트의 탐색 결과는 Fig. 7과 같이 IP주소와 MAC 주소가 정상적으로 획득되었고 정상적으로 동작을 수행하였다.

[Fig. 7] Searching Result by MLD

3.2 IPv6 호스트의 차단과 격리

탐색된 IPv6 호스트는 관리 정책에 따라 차단 또는 격리될 수 있다. 차단은 내부망 접근을 원천적으로 차단하는 방법으로 본 논문에서는 IPv6의 NDP(Neighbor Discovery Protocol)을 사용하여 구현하였다. NDP는 IPv6 환경에서 인접 호스트와 통신을 하기위해 사용되는 프로토콜로 ICMPv6에 포함되어있으며 IPv4 환경에서 ARP(Address Resolution Protocol)의 기능을 대신한다. NDP의 기능은 Table 1 과 Table 2 와 같다.

[Table 1] NDP Functions

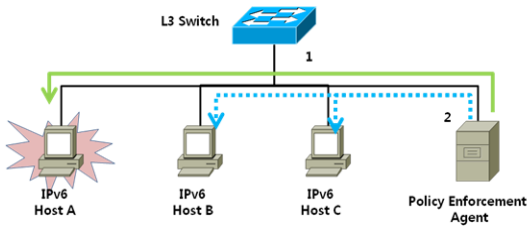
Type	Details
Router/Prefix Discovery	Find router in the network using RS and RA(Getting Network prefix)
Address Resolution	Translate IPv6 to MAC using NS and NA (Same as ARP over IPv4)
Redirect	Same as IPv4 redirect message

[Table 2] NDP Packet Type

Type	Details
RS (Router Solicitation)	Host sends RS packet to get network prefix information
RA(Router Advertisement)	Router sends RA packet which includes MAC, IP and network prefix to host which requests RS
NS(Neighbor Solicitation)	Host sends NS packet to get MAC address to communicate neighbor
NA(Neighbor Advertisement)	Send NA in response to NS Send an unsolicited NA to propagate new information quickly
Redirect	Inform a host of a better first-hop node on the way to the intended destination node

격리는 정상적인 인증을 통해서 네트워크에 접속할 수 있도록 해당 단말이 인증페이지로 리다이렉션되고 인증절차를 거쳐 최종 네트워크에 접속하기 전까지의 상태를 의미한다. 격리는 웹 리다이렉션으로 테스트가 가능하기 때문에 본 장에서는 IPv6 호스트의 차단 방법만을 기술하고자 한다.

본 논문에서는 IPv6 호스트의 차단기능을 대상 호스트에 변조된 NA(Neighbor Advertisement) 패킷을 보내거나 또는 나머지 노드에 차단 호스트의 변조된 NA를 Multicast 함으로 구현하였다. 차단의 세부적인 동작 방안은 Fig. 8과 같다.



[Fig. 8] Host Blocking

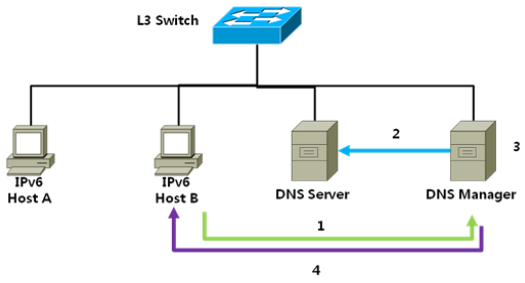
Type 1. 대상 호스트로 변조된 NA 전송하여 외부와의 통신 차단

Type 2. 대상 호스트를 제외한 나머지 노드에 차단 호스트의 변조된 NA를 Multicast하여 외부와 통신 차단

3.3 IPv6 호스트 도메인 할당

IPv6 주소는 32자리 16진수로 구성되어 있어 직접 관리하는 것이 불가능하기 때문에 이의 효율적인 관리를 위한 도메인 주소의 활용은 필수적이다. 본 논문에서 제

안하는 도메인 할당 절차는 Fig. 9와 같다.



[Fig. 9] Domain Assignment

1. 호스트가 DNS 매니저에게 사용하는 IP에 대한 도메인 설정 요청
2. 도메인 설정 요청이 수신되면 DNS매니저는 호스트에 도메인을 자동생성
3. DNS서버에 관련 정보를 추가/삭제/업데이트를 수행한 후 호스트에 결과 전송
4. DNS매니저에서 결과를 수신받은 호스트는 등록된 도메인으로 통신 가능

도메인의 할당은 수집된 호스트의 MAC 주소, 호스트의 IPv4 주소, 호스트의 컴퓨터명 또는 인사DB와 연계한 사용자의 ID, 사용자의 이름, 사용자의 사번 등을 이용한 자동할당 및 사용자에 의한 수동 할당이 가능하도록 구현하였다.

3.4 IPv6 NAC 과 IPv4 NAC의 비교

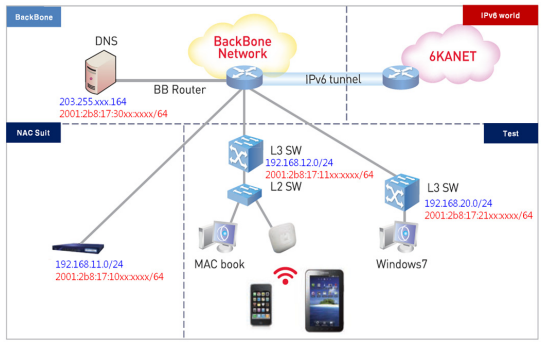
본 논문에서 제안하는 IPv6 기반의 NAC 기능(탐색, 격리, 차단 등)을 구현관점에서 IPv4 NAC과 비교하면 Table 3과 같다.

[Table 3] Comparison of IPv6 NAC with IPv4 NAC

Device	IPv6 NAC	IPv4 NAC
Detection	MDL	ARP
Blocking	NDP(NA)	ARP
Isolation	Redirection	Redirection
Domain Assign	Used	Not used

4. 실험(구현) 결과

IPv6 기반의 네트워크 접근제어의 테스트 환경을 수행하기 위하여 Fig 10과 같이 테스트 환경을 구성하였다. 해당 테스트는 한국인터넷진흥원(KISA)에서 실제 구축한 IPv6 환경에서 테스트를 진행하였다. 또한 인사DB 연동 ID/PW를 활용한 사용자 인증을 수행하였다. 위 테스트를 진행하기 전에 테스트 시나리오를 작성하고 실험결과 값을 예측하여 실험결과와 비교하여 해당 기능의 동작 여부를 확인하였다.



[Fig. 10] Testbed for Network Access Control

4.1 IPv6 호스트 탐색

호스트 탐색 테스트는 Macbook, Windows7(유선)와 아이폰과 갤럭시탭(무선)을 이용하여 IPv6 유·무선 테스트를 동시에 진행하였다. 기능의 호환성을 위해 하위 버전 장비를 사용하였고 실험 결과는 Table 4와 같다.

[Table 4] Result of IPv6 Host Searching

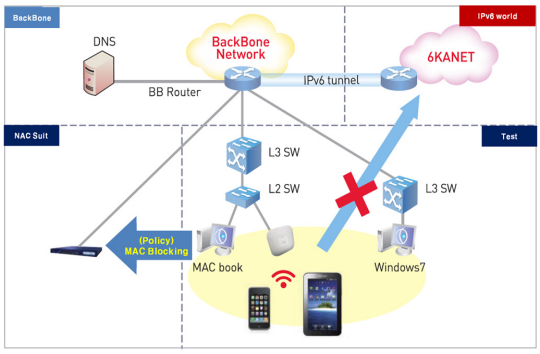
Device	OS	Access	IPv6 Detection
PC	Win7	Wired	O
Macbook	OS X(Lion)	Wired	O
iphone	IOS 5.0	Wireless	O
Galaxy Tab	Jelly Bean	Wireless	O

4.2 IPv6 호스트 차단

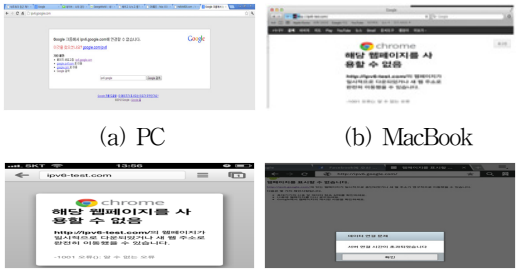
실험을 위해 유·무선 IPv6 환경에서 호스트 MAC을 차단하도록 정책을 설정하고 외부 네트워크의 접속이 정상적으로 차단되는지 Fig. 11과 같이 시나리오를 구성하고 테스트 하였다. 정상적인 차단 동작은 기본적으로 IPv6 사이트(http://ipv6-test.com) 웹 접속에 실패해야 한다.

유선단말인 PC와 MacBook, 무선단말인 아이폰과 갤럭시탭에서 IPv6 외부 네트워크 웹사이트

(http://ipv6-test.com)에 접속 여부를 실험하였고 실험결과는 Fig. 12와 같이 성공적으로 IPv6 호스트의 접속이 차단 되었다.



[Fig. 11] IPv6 host Blocking scenario



(a) PC (b) MacBook

(c) iphone (d) Galaxy Tab

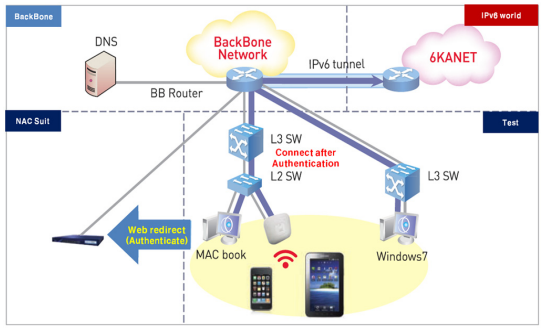
[Fig. 12] Host Blocking

4.3 IPv6 가입자 격리 및 도메인등록

네트워크 접근을 위한 사용자 인증을 획득하지 못한 호스트는 격리되어 외부 네트워크와 통신할 수 없고 단지 인증화면으로만 접속이 가능해야 한다. 실험을 위하여 임시사용자를 등록하고 IPv6 인터넷 웹서버에 접속을 시도한다. 미인증 사용자는 웹 리다이렉션을 통하여 사용자인증 페이지로 이동하고 사용자인증 후 호스트의 도메인을 설정한다. 격리와 도메인 등록을 위해 Fig. 13과 같이 시나리오를 구성하고 테스트 하였다.

정상적인 동작은 미인증 호스트가 네트워크 접근 시 격리되며 사용자 인증 이후 도메인 설정을 수행한 후 IPv6 웹서버로 정상적으로 접근하는 것이다. 또한 도메인 등록된 호스트는 등록된 도메인 주소로 정상적인 Ping이 가능해야 한다.

실험결과 Fig. 14와 같이 정상적인 격리 후 사용자 인증페이지로 리다이렉션, 사용자 인증, 도메인 등록, 등록 도메인으로 통신, IPv6 웹페이지 접속이 모두 성공적으로 동작하였다.



[Fig. 13] Host Isolation Scenario

[Fig. 14] Host Isolation and Domain Assignment

5. 결론

본 논문에서 제안한 IPv6 기반의 네트워크 접근제어 시스템은 유·무선 IPv6 테스트 환경에서 시험한 결과 IPv6 테스트베드와 연동하여 IPv6 호스트들과 원활한 통신이 이루어졌으며 유·무선 호스트 검출, 라우터 검출 및 모니터링 기능이 정상적으로 동작하였다. 또한 호스트 차단기능과 호스트 격리 및 도메인 할당 기능도 현재 가장 보편적으로 사용하고 있는 운영체제의 장비들과 모두 정상적으로 동작하였음을 확인할 수 있었다. Table 5는 본 논문의 최종적인 실험 결과를 보여주고 있다.

본 연구를 통해 외부의 IPv6 서버와 접속을 통하여 실

제 IPv6 트래픽을 이용하여 테스트 하였다는 점에서 큰 성과가 있었으며 향후 IPv6 기반의 IPT(IP Telephony) 환경에는 바로 적용이 가능할 것으로 판단된다. 향후 연구에서는 IPv6 환경에서 요구하는 추가적인 기능 개발 및 연구를 통해 업무용 환경에 적용 가능하도록 기능을 확장하고자 한다.

[Table 5] Test Result

Device	Test Item			
	Host Detection	Host Blocking	Host Isolation	Domain Assign
Desktop PC	O	O	O	O
Macbook	O	O	O	O
iphone	O	O	O	O
Galaxy Tab	O	O	O	O

References

[1] KANI, "The reference model for IPv6 network conversion", pp.10, 2013, Available From : http://nec.kani.or.kr//main/main.php?categoryid=08&menuid=02&groupid=00 (accessed May 26 2014)

[2] Ministry of Science, ICT and Future Planning, "Roadmap of expanding IPv6 for promotion of new internet industry", 2014, Available From : http://www.kisa.or.kr/notice/noticeView.jsp?cPage=1&mode=view&p_No=4&b_No=4&d_No=1421&ST=&SV= (accessed May 26 2014)

[3] KISIA, KDCA, "Survey for Information Security Industry in Korea : Year 2013", pp.54, 2014

[4] Jae-Ho Lee, "IPv6 deployment state and expanding strategy on government area", *Proc. of IPv6 day 2103 Korea*, pp.23-34, 2013

[5] Joel Snyder, "Selecting An Approach For NAC Enforcement: Five Key Issues", pp.2-4, *Whitepaper*, Opus One, Sept. 2007. Available From : http://www.kisa.or.kr/notice/noticeView.jsp?cPage=1&mode=view&p_No=4&b_No=4&d_No=1421&ST=&SV= (accessed June 4 2014)

신 해 준(HaeJoon Shin) **[정회원]**

- 1999년 2월 : 영남대학교 대학원 정보통신공학과 (공학석사)
- 2003년 2월 : 영남대학교 대학원 정보통신공학과 (공학박사)
- 2004년 8월 ~ 2012년 2월 : 영진전문대학 컴퓨터정보계열 교수
- 2012년 3월 ~ 현재 : (주)넷맨 연구소 기술책임자

<관심분야>
정보보안, 네트워크보안, 융합보안