IPv6 환경에서 방화벽 기반 VPN 의 성능 향상에 관한 연구

이은선*, 양진석*, 정태명*
*성균관대학교 컴퓨터공학과
이동형 응급의료 정보 시스템 개발센터
e-mail : *{eslee99, jsyang}@imtl.skku.ac.kr,
*tmchung@ece.skku.ac.kr

A Study on Performance Improvement of Firewall based VPN in IPv6 environment

Eun-Seon Lee*, Jin-Seok Yang* and Tai-Myoung Chung*
*Cemi: Center for Emergency Medical Informatics,
Dept. of Computer Engineering, Sungkyunkwan University

요 약

IP VPN 의 사용은 현재 보편화 되었고 네트워크 장비의 통합 추세에 따라 IP VPN 과 방화벽 통합제품의 생산이 활발히 이루어지고 있다. 통합 보안 제품은 비용 효율성과 관리의 편리성, 확장성, 유연성과 같은 장점을 제공하지만 높은 성능 지원을 요구한다. 방화벽의 성능 인자의 하나로서 정책의 개수는 그 수에 비례하여 검색 시간이 지연되는 문제를 발생시키고, 이러한 성능 저하 문제는 VPN 과 통합 시 더욱 가중된다. 더욱이 차세대 네트워크인 IPv6 로 환경에서는 IP 의 비트수가 증가하여 검색 성능 문제 해결이 필수적으로 요구된다. 본 논문에서는 이러한 통합 제품의 검색 성능 문제에 관한 해결 방안으로 IPv6 주소의 특성을 사용한 메커니즘을 제안한다. 제시한 메커니즘은 보안 정책 테이블의 주소 필드를 IPv6 주소에 포함된 인터페이스 식별자로 대체하여 보안 정책 테이블의 검색 속도를 향상시키는 방법이다. 이 방법은 차세대 네트워크 환경에서 주목 되고 있는 보안 및 성능 문제에 대해 큰 역할을 할 것으로 기대된다.

1. 서론

IPv6 는 인터넷의 주소 고갈과 보안, 이동성 지원, 서비스 품질보장 등의 문제를 해결하기 위해 설계된 차세대 인터넷 프로토콜이다. 이 중 보안을 위해서는 IPv4 에서 선택적으로 사용되었던 IPsec(IP Security)을 기본 기능으로 포함하여 통신의 기밀성과 무결성을 제공한다[4]. 그러나 IPsec[1]의 적용 이후에도 여전히 존재하는 네트워크 위협들에 대해서는 방화벽과 같은 다른 보안 메커니즘이 추가적으로 요구된다. 또한 방화벽만으로 구성된 보안체계 역시 도청, IP spoofing, connection hijacking 등의 취약점 이 존재하며 이는 IPsec 을 통한 IP 데이터그램의 기밀성, 인증, 무결성 보장으로 해결할 수 있다[3]. 현재 IP VPN 이 가진 높은 비용 효율성과 통신의 안정성으로 인해 기업에의 사용량이 크게 증가하면서, 위에 언급한 장점을 바탕으로 방화벽과의 통합 현상이 급증하고 있다. VPN 서비스 제공업체는 기존 시장의 유지를 위해 현재 운용중인 보유장비에 VPN 기능을 부가하고, 주요 네트워크 장비 업체들은 방화벽과 통합된 IP VPN 제품을 출시하고 있다[11]. 가트너는 방화벽과 IP VPN 보안기능이 브랜치 오피스나 소형 오피스에서 일반화되어 2006 년까지는 약 80%까지 확산될 것으로 보고 있으며, 2003 년부터는 시장에 출시되는 거의 모든 소형 오피스용 제품들을 방화벽과 IP VPN 기능이 통합된 형

본 논문은 보건복지부 보건의료기술진흥사업회 지원에 의하여 이루어진 것임(과제번호: 02-PJ3-PG6-EV08-0001)

태로 예상하고 있다[11].

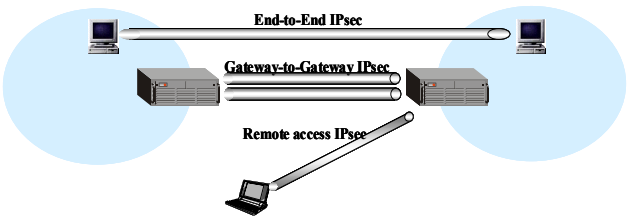
이 같은 통합된 보안 제품은 비용 효율과 관리의 편리성, 확장성, 유연성과 같은 장점이 존재하지만 높은 성능이 요구된다. 현재 방화벽에서 존재하는 성능 문제는 정책의 수에 비례하여 증가하며 처리속도가 감소할 경우 병목이 발생함과 함께 동시 접속 세션 수가 감소한다. 장비가 소유한 보안 정책 수의 증가와 그에 따른 검색 소요 시간의 지연은 시스템의 트래픽 처리량, 즉 성능을 지연시키는 요인이다. IP VPN 에서 'End-to-End IPsec'을 위해서 노드는 통신하고 있는 모든 상대 노드에 대한 보안 정책을 소유해야 하며, 'Gateway-to-Gateway IPsec' 또는 'Remote access IPsec'을 위해서 게이트웨이는 상대 게이트웨이 또는 개별 원격 노드에 대한 정책 정보를 포함 해야 하므로 VPN 적용 방식에 따라 저장해야 할 정책의 수가 기하급수적으로 증가할 수 있다. 이로 인해 발생하는 성능 문제는 통합 장비에서 더욱 심화된다[8]. 본 논문에서는 이러한 성능 문제의 개선을 위해 IPv4 주소와 차별화된 IPv6 의 주소체계를 정책 테이블의 검색 효율성 증가에 활용하는 방안을 제안한다. IPv6 주소에 포함된 인터페이스 식별자로 IPsec 의 보안정책 테이블에 입력되는 주소를 대체하여 보안정책 테이블의 검색속도를 향상시킬 수 있다.

본 논문의 구성은 다음과 같다. 2 장에서 VPN/방화벽 통합 제품의 정책 테이블과 IPv6 주소체계에 포함된 인터페이스 식별자에 관한 내용을 기술하고 3 장에서는 인터페이스 식별자를 사용하는 정책 테이블을 설계한다. 4 장은 제안 메커니즘의 예상 활용 부분을 기술하고 5 장에서 향후 계획과 결론을 제시한다.

2. 관련 연구

2.1. VPN/방화벽의 정책 테이블

통합제품의 정책 테이블은 VPN 의 SPD(Security Policy Database : 보안정책 데이터베이스)와 방화벽의 정책 테이블이 결합된 형태로, VPN/방화벽 정책 테이블의 기본적인 형태를 <표 1>과 같이 정의할 수 있다. [그림 1]에서 Gateway-to-Gateway 의 경우, 정책이 적용되는 IP 주소는 양 게이트웨이에 할당된 일정 IP 주소의 범위의 형태가 주로 사용되고, End-to-End 와 Remote access 의 경우, 개별 호스트의 IP 에 대해 정책이 적용되는 형태로 주로 나타난다. 이에 따라 VPN/방화벽 장비의 정책 테이블에서 IP 주소 필드에 입력되는 주소의 유형은 네트워크 유형과 호스트 유형으로 분류할 수 있다.



[그림 1] 방화벽과 VPN 의 결합 형태

(가) 호스트 유형

호스트 유형의 주소는 단일 IP 를 명시하며 <표 1>의 1 번째 엔트리와 같이 IP 주소 전체를 사용해서 표현한다. IPv4 는 32 비트, IPv6 주소는 128 비트를 사용하게 된다. IPv6 를 사용하는 네트워크에서는 IPsec 이 기본기능으로 포함되므로 게이트웨이 내부에 위치한 개별 종단 노드에서 시작, 종료되는 'End-to-End IPsec' 형태가 증가한다. 이에 따라 호스트 유형 주소의 사용은 증가하며 정책 엔트리의 증가로 인한 성능 문제가 수반된다.

(나) 네트워크 유형

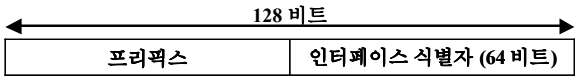
네트워크 유형은 일정 IP 범위를 나타내는 주소를 의미하며 <표 1>의 2 번째 엔트리와 같이 프리픽스(prefix)를 통해 표현되는 주소 형태를 갖는다.

<표 1> VPN/방화벽의 정책 테이블

index	목적지 IP 주소 (IPv6) (128 비트)	송신지 IP 주소 (IPv6) (128 비트)	Name	전송계층 프로토콜	송신지/목적지 포트(tcp/udp)	Action	SA pointer
1	FEDC:BA98:7654:3210:3210:FEDC:BA98:7654	BA98:FEDC:7654:3210:8:800:0:0:417A	dlsid@jjcom15.skku.ac.kr	ESP or Any	Any	Encrypt (IPSEC)	3
2	A590:0:304C::/48	6004:2CA5:0:920D::/64	-	TCP	21	Permit	5

2.2. IPv6 주소의 인터페이스 식별자

비상태형 자동 주소 설정 방식[9]을 통해 생성되는 IPv6 주소는 [그림 2]와 같이 네트워크 프리픽스와 노드의 인터페이스 식별자를 결합한 형태이다[4].



[그림 2] IPv6 주소의 구성

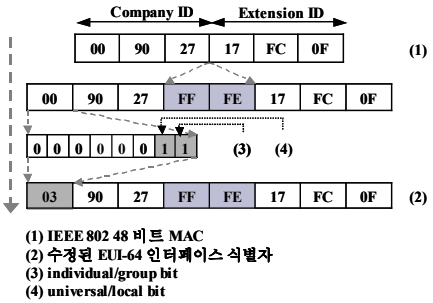
노드는 직접 생성한 주소의 중복 여부를 확인하기 위해 중복 주소 탐지(Duplicated Address Detection) 과정을 수행한 후, 중복되지 않음이 확인되면 자신의 주소로 사용한다. 이 때 한 네트워크에서 프리픽스는 동일하므로 인터페이스 식별자가 노드가 생성하는 주소에 유일성을 부과하는 기능을 한다. IPv6 의 인터페이스 식별자는 IEEE(Institute of Electrical and Electronics Engineers) 802 48 비트 MAC(Media Access Control) 주소를 가진 노드, IEEE EUI-64 식별자를 가진 노드, 지역적인 식별자를 가진 노드, 식별자가 없는 링크 등에 각기 다른 방법으로 생성되는데 이 중 앞의 두 종류는 전역적 유일성을 갖는 "수정된 EUI 인터페이스 식별자 (Modified EUI-64 Interface Identifier)" 로의 변경이 가능하다[4][7].

2.3. 수정된 EUI 인터페이스 식별자의 구성

이더넷 환경과 무선 환경에 사용하도록 정의된 수정된 EUI 인터페이스 식별자의 생성 방법에 대해 자세히 기술한다.

(가) 이더넷 환경의 IPv6 인터페이스 식별자

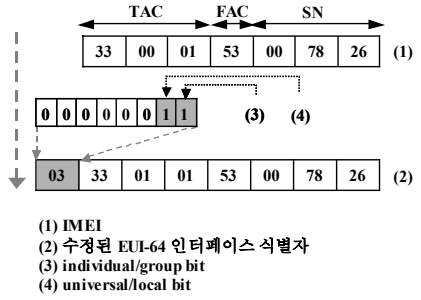
IEEE 802 48 비트 MAC 주소는 네트워크 카드 생산 회사에 고유한 값인 company ID 와 그 회사 제품에 고유한 값인 extension ID 로 이루어진다. [그림 3]과 같이 두 값의 사이에 FFFE 를 추가한 후, (4)번 비트를 1 로 설정하면 전역적인 유일성을 만족하는 수정된 EUI-64 인터페이스 식별자가 생성된다[5].



[그림 3] 이더넷 환경을 위한 IEEE 802 48 비트 MAC 주소 기반의 수정된 EUI 인터페이스 식별자 생성

(나) 무선 환경의 IPv6 인터페이스 식별자

IMEI(International Mobile station Equipment Identity)는 GSM 또는 UMTS 단말의 식별 정보이다. [그림 4]와 같이 IMEI 에 추가된 옥텟의 (3), (4)번 비트를 1 로 설정하면 전역성을 갖는 수정된 EUI-64 인터페이스 식별자가 생성된다[2].



[그림 4] 무선 환경을 위한 IMEI 기반의 수정된 EUI 인터페이스 식별자 생성

3. VPN/방화벽의 정책 테이블의 개선

3.1. 인터페이스 식별자를 사용한 정책 테이블

2.1 절에서 설명한 주소 유형 중 인터페이스 식별자의 값이 모두 표현되는 호스트 유형의 주소가 이 논문에서 제안하는 인터페이스 식별자 사용 메커니즘을 적용할 수 있는 주소 형태이다. 따라서 호스트 유형의 주소와 네트워크 유형의 주소를 위한 정책 테이블을 별개로 사용해야 하며 두 종류의 테이블의 형태를 각각 <표 2>와 <표 3>으로 나타낼 수 있다. 두 테이블에서 주소 필드 외의 다른 필드 구성은 동일하다.

(가) 호스트 주소 유형 정책 테이블

본 논문에서 제안하는 메커니즘이 적용되는 대상 테이블로 전역적으로 유일한 인터페이스 식별자를 노드 식별자로 사용한다. <표 2>와 같이 정책 테이블의 주소 필드에는 IPv6 주소가 아닌 인터페이스 식별자가 사용되며 주소필드의 길이 역시 인터페이스 식별자의 길이와 같은 64 비트로 고정된다.

정책 테이블의 주소필드에 입력되는 IPv6 주소를 인터페이스 식별자로 대체하면 검색 시에 비교해야 할 비트수가 128 비트에서 64 비트로 감소된다. 엔트리의 개수가 일정 수치보다 많이 존재할 경우, 검색해야 할 비트 수의 감소는 성능 향상을 이룰 수 있다. IP VPN 은 각 사이트간 완전한 메쉬(mesh) 형태의 연결을 해야 하는 특성이 있다. 그러므로 연결 노드의 수에 비례하여 각 노드가 소유해야 하는 보안 연계의 개수와 정책 테이블의 크기가 증가하기 때문에 연결의 수가 많아질수록 부담이 커지게 된다. 정책 테이블의 엔트리의 수와 요구 메모리, 큰 테이블의 유지비용은 IPsec 과 방화벽의 처리 성능에 영향을 미치는 요인들로 정책 테이블의 설계 과정에서 크게 고려되는 사항들이다[6].

<표 2> 인터페이스 식별자를 사용한 호스트 주소 유형 정책 테이블

index	목적지 IP 주소 (IPv6) (64 비트)	송신지 IP 주소 (IPv6) (64 비트)	Name	전송계층 프로토콜	송신지/ 목적지 포트(tcp/udp)	Action	SA_ Poi- nter
1	3210:FEDC: BA98:7654	800:0:0: 417A	dlsid@ jjcom15. Skku.ac.kr	TCP	Any	IPSEC	3

(나) 네트워크 주소 유형 정책 테이블

프리픽스로 표현되는 IP 주소 유형을 위한 테이블로, 유동적인 프리픽스 길이를 수용하기 위해 주소필드는 최소 128 비트가 요구된다.

<표 3> 네트워크 주소 유형의 정책 테이블

index	목적지 IP 주소 (IPv6) (128 비트)	송신지 IP 주소 (IPv6) (128 비트)	Name	전송계층 프로토콜	송신지/ 목적지 포트(tcp/udp)	Action	SA poi- nter
3	A590:0: 304C::/48	6004:2CA5: 0:920D::/64	-	Any	Any	Permit	5

3.2. 패킷 처리 과정

정책 테이블에 엔트리가 삽입될 때, 해당 엔트리가 명시하는 IPv6 주소가 호스트 주소 유형일 경우, IPv6 주소의 인터페이스 식별자를 추출하여 주소 필드에 입력한다. 한편 해당 엔트리가 명시하는 IPv6 주소가 네트워크 주소 유형일 경우 프리픽스 정보와 함께 네트워크 주소 유형 테이블에 입력한다.

송수신 패킷 처리 과정에 이루어지는 정책 테이블 검색 시, 대상 패킷의 IPv6 주소의 인터페이스 식별자를 추출하여 전송계층 프로토콜, 송신지, 목적지 포트 값 등과 결합하여 검색자로 사용한다. 이 때, 호스트 유형 정책 테이블에 대한 검색이 네트워크 유형 정책 테이블보다 우선하며, 호스트 유형 정책 테이블에서 패킷에 맞는 엔트리를 찾지 못한 경우에 네트워크 정책 테이블을 검색한다. 네트워크 유형 정책 테이블을 검색하기 위해서는 IPv6 패킷의 128 비트 주소와 전송계층 프로토콜, 송신지 · 목적지 포트 값 등을 검색자로 사용한다.

4. 제안된 메커니즘의 사용을 통한 예상 효과

4.1. 여러 IPv6 주소의 정책 중복 문제 해결

IPv6 에서는 하나의 인터페이스에 여러 개의 주소가 할당될 수 있다.

<표 4> IPv6 노드가 소유하는 다양한 주소 종류

주소의 종류	표현 형식
Link-local IPv6 주소	FE80::Interface ID (64 비트)
Global IPv4 주소	global routing prefix:Subnet ID:Interface ID (64 비트)
6to4 주소	2002:v4addr::/48 :Interface ID (64 비트)

<표 4>의 주소들은 한 노드가 동시에 소유할 수 있는 주소 중 인터페이스 식별자를 포함한 형태로, 각기 다른 프리픽스와 동일한 인터페이스 식별자 정보로 구성된다. Link-local IPv6 주소는 한 링크 내에서, Global IPv4 주소는 전역적으로 노드를 식별하는 주소이며 6to4 주소는 IPv6 네트워크와 IPv4 네트워크와의 통신을 지원하는 6to4 터널링 메커니즘을 위해 노드에 할당되는 주소이다. 이처럼 한 노드를 가리키는 주소가 다양한 형태로 사용될 수 있으므로 주소를 식별자로 사용하는 정책 테이블에서는 한 노드에 대한 주소 종류마다 동일한 정책을 저장하는 문제가 발생한다. 이 경우에 IPv6 주소는 노드를 유일하게 식별하는 기능을 수행하지 못하며 이를 인터페이스 식별자가 대신할 수 있다. 이를 통해 중복된 정책의 저장을 지양하고 이는 차후 검색속도의 향상 뿐만 아니라 메모리 절약에도 기여한다.

4.2. 유비쿼터스 환경의 고성능 처리 지원

유비쿼터스는 사용자가 컴퓨터나 네트워크를 의식하지 않는 상태에서 장소에 관계없이 자유롭게 네트워크에 접속할 수 있는 환경을 의미한다. 주변 모든 물체에 컴퓨터, 센서가 내장되어 무선을 포함한 여러 통신수단으로 연결된다.

유비쿼터스 네트워크를 위해서는 모든 전자기기에 컴퓨팅과 통신 기능이 부가돼야 한다. IPv6 기술로 모든 전자 기기에 독립적인 IPv6 주소를 부여할 수 있으며 한 사람 당 5×1026 의 IP 주소를 소유할 수 있다. 손톱만한 크기의 컴퓨터로 언제 어디서든지 400Mbps 의 무선 LAN 을 사용하고 멀티미디어 분야에서는 영상 음성인식이 가능한 스마트폰, PDA 등이 번성할 것으로 예측된다. 또한 2012 년에는 착용 가능한 PC 와 3 차원을 실현하는 TV, 사람의 오감을 인식하는 컴퓨터 시스템 등이 상용화될 것으로 전망된다[10]. 이와 같이 미래 환경의 통신 모델은 몸에 부착할 수 있는 컴퓨터, 개인 한명을 위해 무수히 많은 컴퓨터가 운영되어지는 PAN(Personal Area Network)의 형태로 예상되며 이를 위해 이동 단말에 대해 보안 및 인증 기술, 실시간 서비스 지원기능, 고도의 처리를 위한 성능 향상 등이 요구되고 있다.

매우 많은 사용자와 단말들이 상호 작용하고 통신 보안을 위해 IPsec 이 사용될 때 통신 세션을 중앙 관리하는 네트워크 지점에서의 과부하는 대폭 증가할 수 밖에 없다. 특히 백본 네트워크에서 고성능의 처리 능력이 요구되며, 이를 위해 고대역의 네트워크 등이 계획되고 있다[10]. 기간 네트워크와 액세스 네트워크 장비 처리성능의 효과적 개선 방안으로 본 논문에서 제안한 메커니즘을 적용할 수 있을 것이다.

5. 결론 및 향후연구

네트워크 보안을 제공하는 다양한 메커니즘을 한 장비로 통합하는 현상이 증가하면서, 각 장비의 개별 기능을 통합한 데에 따른 처리 과부하가 발생하고 있다. 이 중 방화벽과 VPN 의 통합제품에서 병목으로 작용하는 곳은 패킷 정책 테이블의 검색 기능이다.

본 논문에서는 이의 해결방안으로 IPv6 에서 노드가 유일하게 소유하는 인터페이스 식별자로 정책 테이블의 IPv6 주소를 대체하여 성능을 향상시키는 방법을 제안하였다. 이는 고가의 메모리를 사용하는 라우터 또는 방화벽 등의 네트워크 기반 장비에 적용되어 검색과 메모리 활용도를 향상시킬 수 있다. 향후에 제안된 방식의 성능 평가를 통한 증명 과정이 필요하다. 나아가 VPN/방화벽 뿐 아니라, 라우터/VPN 와 같이 통합된 장비가 증가하는 환경에서, IP 주소를 정책 식별자로 사용하는 타 통합 장비에 제안된 메커니즘을 적용하는 확장된 시나리오를 연구하겠다. IPsec 을 사용하는 노드 수가 크게 증가하는 IPv6 환경과 All-IP 환경에서는 제안된 메커니즘의 적용이 보다 적절할 것이다.

참고문헌

[1] N. Doraswamy, D. Harkins, "IPSec The new Security Standard for the Internet, Intranets, and Virtual Private Networks", Prentice Hall PTR, July 1999.

[2] F. Dupont, “IMEI-based universal IPv6 interface Ids”, IETF DRAFT, December 2003.

[3] U. Ellermann, “IPv6 and Firewalls”, ICCCSP, June 1996.

[4] R. Hinden, S. Deering, “Internet Protocol Version 6 (IPv6) Addressing Architecture”, RFC3513, April 2003.

[5] IEEE Standards Systems/Network Staff, "GUIDELINES FOR 64-BIT GLOBAL IDENTIFIER (EUI-64™) REGISTRATION AUTHORITY", IEEE, December 2003.

[6] S. Kent, R. Atkinson, “Security Architecture for the Internet Protocol”, RFC2401, November 1998.

[7] A. Landron, “Public OUI and company_id Assignments”, IEEE, January 2004.

[8] D. Newman, “WatchGuard Firebox V200 firewall/VPN”, NetworkWorldFusion, April 2003.

[9] S. Thomson, T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC2462, December 1998.

[10] 이성용, “유비쿼터스 연구 동향 및 향후 전망”, 산업자원부기술표준원, April 2003.

[11] 이윤철, “VPN 기술 및 국내외 시장 동향”, ETRI 주간기술동향, December 2002.