BcN 환경을 고려한 차세대 네트워크 보안 구조에 관한 연구

오승희* · 서동일*

*한국전자통신연구원 정보보호연구단 네트워크보안구조연구팀

The Study on Next Generation Network Security Architecture in the BcN Environment

Seung-hee Oh* · Dongil Seo*

*ETRI Information Security Research Division, Network Security Architecture Research Team

E-mail : seunghee5@etri.re.kr

요 약

BcN 네트워크 환경은 정통부의 지원 아래 2007년까지 단계적으로 공중망, 지역망 및 대부분의 단말에 도입될 예정이다. BcN 환경의 인프라인 IPv6 도입과 함께 현재의 네트워크 보안 구조도 IPv6 트래픽 및 네트워크 환경을 고려한 차세대 네트워크 구조로 진화해야만 한다. 차세대 네트워크 보안 구조는 IPv6 적용과 함께 네트워크의 또 다른 흐름인 유무선 통합에 대한 고려도 필요하다. 따라서, 본 논문에서는 향후 IPv6가 적용되고 유무선이 통합될 네트워크 환경을 고려한 차세대 네트워크 보안 요구사항을 분석하고 차세대 네트워크 보안 구조를 제안한다.

ABSTRACT

The BcN is applying from public networks to local networks and each terminal step by step under supporting MIC(Ministry of Information and Communication Republic of Korea) until 2007. The architecture of network security should considers BcN environment and evolves to manage IPv6 traffics. The next generation network security architecture can manage not only IPv6 environment but also wire and wireless integrated network. We suggest the next generation network security architecture for IPv6 environment and wire-wireless integrated network environment and verify the performance of the suggested architecture using network security scenario.

키워드

네트워크 보안, 차세대 네트워크, IPv6, 보안 구조, 유무선 통합, BcN

Ⅰ. 서 론

네트워크의 진화 상황을 예측해 볼 때 2007년부터 국내 주요 ISP망에서 광대역통합망 (Broadband convergence Network: BcN) 환경이 구축될 예정이다. 또한, MIC에서는 네트워크 장비의 수명(약 5년)을 고려하여, 그림 1과 같은 과정을 거쳐 2005년부터 2009년까지 모든 공공기관 통신 장비를 순차적으로 업그레이드하고 2009년 이후에 IPv6가 단계적으로 공중망 및 지역망 단말기에 도입될 할 것으로 예측하고 있다.

이러한 네트워크 진화 방향에 맞추어 네트워크 보안 요구사항도 변하고, 이에 따른 네트워크 보안 구조도 새롭게 재정립되어야 한다.

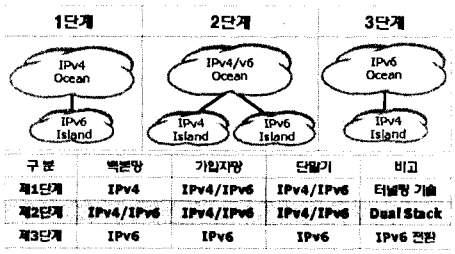

그림 4. IPv6 적용 단계[1]

따라서 본 논문에서는 IPv6를 기반으로하는 차세대 네트워크에 적합한 차세대 네트워크 보안구조를 제안한다.

II. 차세대 네트워크 보안의 요구사항

본 장에서는 차세대 네트워크 보안을 위한 고려사항을 현재 네트워크 진화의 큰 흐름인 IPv6와 유무선 통합으로 나누어 분석한다.

그림 2는 BcN 환경에서의 계층별 네트워크의 구조를 나타낸 것으로, BcN환경에서는 다양한 단말의 특성을 모두 수용하면서도 사용자의 요구에 맞는 QoS(Quality of Service)를 지원할 수 있어야 한다.

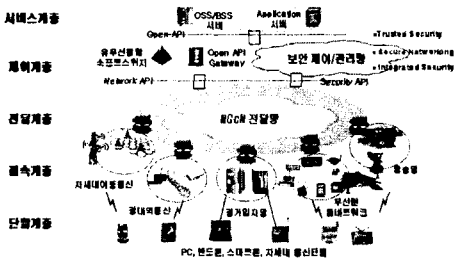

그림 5. BcN 환경의 네트워크 구조

표 1은 BcN 환경에서의 계층별로 보안 요구사항을 정리한 것이다.

표 1. 계층별 보안 요구사항

구분	주요 대상	주요 이슈
서비스	- 서비스 응용 프로그램 - 개방형 인터페이스	- 접근 인증 및 권한 부여 - 개방형 인터페이스 제공에 따른 악성 서비스 발생 - 사용자 프라이버시 보장 - 반사회적·반윤리적 유해 정보 유통 - 지적 재산권 보호 - 개별 단위망 응용 프로그램 통합에 따른 상호인증, 접근제어, 권한제어
관리/제어	- OPEN API 게이트웨이 - 소프트스위치 - BcN 망 관리	- 서비스 게이트웨이 서버의 안전성 및 신뢰성 보장 - 소프트스위치의 신뢰성 보장 - 구성 정보 유출로 인한 대규모 피해 발생 - 네트워크 생존성 보장을 위한 제어전용채널 구축 - 통신망 보안성 확보를 위한 법·제도
전달	- 네트워크 구성 - 각종 게이트웨이	- 네트워크 생존성을 보장할 수 있는 전송노드 구축 - 전달망 QoS 보장 - 고성능 정보보호 처리 - 유해 암호 트래픽 차단 - 트래픽 재밍(jamming)공격 - 전송매체에 대한 도청 방지
접속	- 전달 계층 접속 기술	- 단말과 망간 상호 인증 - 접속구간의 도청, 데이터 위·변조 용이 - 유해 TV 방송 부가서비스의 노출 용이
홈/단말	- 유선·무선 단말 시스템 - 음성·방송 단말 시스템	- 홈 게이트웨이 안전성 보장 - 홈 가전기기 및 통신단말기의 보안 취약성 - 휴대 단말의 이동성과 익명성을 이용한 사이버 공격 위협 증대

2.1 IPv6 환경을 위한 보안 고려사항

BcN 환경은 네트워크 인프라가 IPv6로 진화할 것으로 보고 있으며, IPv6 네트워크 환경에서 요구되는 보안 고려사항을 정리하면 크게 다음과 같다.

- 암호화된 트래픽 처리 방식 고려

End-to-End 방식의 VPN 서비스 제공이 일반화될 경우, 암호화된 트래픽 처리 방식에 대해서 고려해야 한다. 예를 들어, VPN 트래픽을 복호화해서 데이터에 포함되어 있는 침입 패턴을 탐지할지 등의 여부와 어떤 프로세싱을 거쳐 복호화할 지에 대해서 고려해야 한다.

- VPN 트래픽을 이용한 침입에 대한 대응 방식 고려

End-to-End VPN 서비스의 경우, VPN 트래픽을 이용한 공격은 네트워크에 대한 위협보다는 특정 서버나 호스트/단말에 대한 공격일 것이다. 따라서 이러한 공격 유형에 대해 네트워크 보안에서 위협 완화 방식을 제공할지 아니면 이를 시스템 보안으로 대체할 지에 대해서 고려해야 한다.

- VPN외의 보안에 대한 고려

IPv6에서는 IPSec이 mandatory로 적용되면서 그 동안 보안의 많은 부분을 IPSec을 통해 해결할 수 있으나, IPSec만으로 네트워크 보안은 부족하다. 따라서 이 외의 다른 보안 메커니즘에 대한 연구도 추가적으로 요구된다.

2.2 유무선 통합 네트워크 환경을 위한 보안 고려사항

BcN 환경에서는 유무선 통합으로 진화할 것으로 예측하고 있으며, 유무선이 통합된 네트워크 환경에서 요구되는 보안 고려사항을 정리하면 다음과 같다.

- 무결성, 인증 및 암호화 방안

전송하는 데이터의 무결성 제공 및 공격자 신원확인을 위해 인증, 암호화에 대한 방안과 이와 더불어 법적인 제도가 요구된다.

- 소프트스위치의 보안 방안

소프트스위치를 위한 자체 보안 및 소프트스위치와의 통신 보안 강화를 위한 방안이 요구된다.

- 안전한 QoS 지원 방안

이종망간의 핸드오버를 안전하고 효율적으로 제공하면서 안전한 QoS를 지원할 수 있는 시스템 및 메커니즘이 요구된다.

III. 제안하는 차세대 네트워크 보안 구조

차세대 네트워크인 BcN 환경을 위한 차세대 네

트워크 보안 구조는 II장에서 언급한 IPv6와 유무선 통합 네트워크 환경에서의 보안 요구사항을 만족해야 한다. 그림 3은 차세대 네트워크의 각 계층별로 요구되는 정보보호에 대해 정리한 것이다.

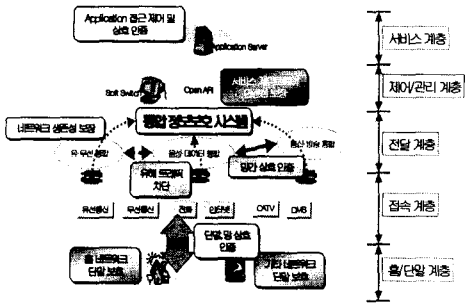

그림 3. 차세대 네트워크의 보안 구조

차세대 네트워크 보안 구조는 다음과 같은 보안 고려사항들을 수용해야 한다.

- 유무선 통합용 VPN이 제공되어야 하므로 이에 따른 VPN 기술의 변화가 요구된다.
- ISP 망에 소프트스위치와 같은 유무선망을 연동시켜주는 시스템에 대한 취약성 관리 및 패치 서비스 제공도 필요하다.
- 통합 패킷망의 QoS 보장 방안을 보안 서비스 측면에서도 고려해야 한다. 특히, 음성 서비스의 경우 기존 전화망과 동일한 품질을 보장하기 위해서는 음성 데이터의 packet loss 문제와 packet sniffing/spoofing 등의 문제를 반드시 해결해야 한다. 또한, 멀티미디어 서비스의 경우 기존 방송망에서 제공하는 품질 기준을 만족해야 하는 등의 문제점을 해결하기 위한 보안 기술이 필요하다.
- 보안 서비스 제공 측면에서, 다양한 형태의 유무선 단말들이 네트워크에 접근하여 트래픽 생성이 가능하므로 트래픽 폭주를 고려한 개별 시스템 및 유무선 단말에 대한 강력한 인증이 요구되고, 이를 처리할 수 있는 기능이 필요하다.
- 응용 서비스별로 요구하는 보안 강도가 다르므로 서비스별 보안 제공 방식의 차별화에 대한 고려가 필요하다.
- Mobile IPv6에서도 보안을 위한 IPSec이 적용될 것이다. 무선 보안을 위해 사용하는 IPSec은 유선의 IPSec보다는 lightweight하고 이동성을 빠르게 제공할 수 있어야 한다.
- Mobile phone이나 노트북과 같이 이동성을 지닌 단말기로 인한 트래픽의 양이 폭주하면서 기존의 유선과는 달리 단말에 대한 AAA (Authentication, Authorization, Accountability) 기능의 강화가 요구되고, 특히 보안 서비스에 대한 과금을 부과하기 위한 Accountability 측면에의 기능 추가도 요구된다.

앞서 언급한 차세대 네트워크 보안 요구사항을 만족시킬 수 있는 차세대 네트워크 보안 구조를 제안한다. 제안하는 구조는 Access Network와 Customer Network에서 보안 기능을 제공하기 위한 Security platform과 전체적으로 보안 관리를 제어하는 보안관리시스템(Security Management System: SMS)으로 구성된다.

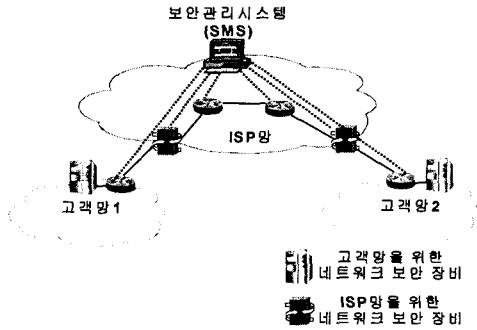

그림 4. 제안하는 차세대 네트워크 보안 구조

3.1 액세스망을 위한 보안 플랫폼

액세스망은 일반적으로 서비스 제공자가 관리하는 네트워크로 여러 다양한 고객망과 연결된다. 따라서 고속의 트래픽을 처리할 수 있는 라우팅 기술과 더불어 신속하게 새로운 유형의 사이버 공격 및 위협에 대처할 수 있는 정책기반의 보안 관리가 요구된다.

그림 5와 같이 보안 블록(Security Block)에는 보안관리시스템과의 안전한 통신을 위한 SSL/TLS, SSH가 제공되고, 전송되는 데이터의 안전성을 확보하기 위한 유무선용 VPN, 이상 증후 트래픽을 차단하면서도 성능과 속도 측면을 고려한 NP 기반의 Clustered Firewall 또는 패킷 필터링과 proxy 기능을 통합하여 가지고 있는 Stateful Firewall, 항바이러스 기능, content filtering, 그리고 침입 탐지를 위한 IDS/IPS/IDP 기능을 제공해야 한다. 관리 블록(Management Block)에서는 정책을 집행할 수 있는 Policy Enforcement Engine과 새로운 관리 및 보안용 정책들을 자동적으로 수용하기 위한 Update Engine이 존재해야 한다. 이외에도 시스템이 설치되는 환경의 요구사항에 따라 보안 기능이 추가될 수 있어야 한다.

3.2 고객망을 위한 보안 플랫폼

고객망은 액세스망과는 다르게 고속의 트래픽 전송보다는 강력하고 안전한 보안 제공이 더 중요하다. 따라서 고객망을 위한 보안 플랫폼의 보안 블록에서는 보안관리시스템과의 안전한 통신을 위한 SSL/TLS, SSH가 제공되고, 전송되는 데이터의 안전성 확보를 위한 유무선용 VPN, 이상 증후 트래픽을 차단하고 데이터 레벨까지 검사하기 위한 application level의 Proxy Firewall, 데이터베이스

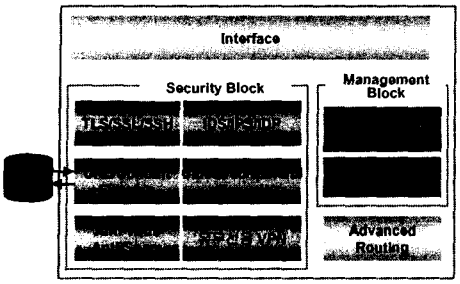

그림 5. 액세스망을 위한 보안 플랫폼의 기능 블록

와 접근 제어 리스트를 관리하여 Access Control, 침입탐지를 위한 IDS/IPS/IDP 기능, 그리고 MD5 Routing Authentication을 제공한다. 관리 블록에서는 보안관리시스템에서 생성한 정책을 집행하기 위한 Policy Enforcement Engine이 필수적으로 존재해야 한다. 액세스망을 위한 보안 플랫폼과 마찬가지로 시스템이 설치되는 환경의 요구사항에 따라 보안 기능이 추가될 수 있어야 한다.

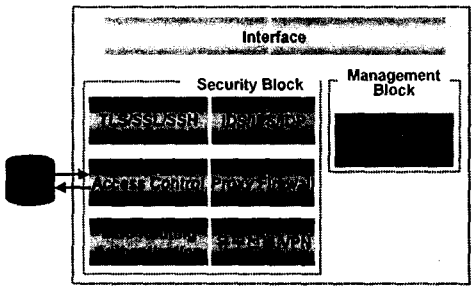

그림 6. 고객망을 위한 보안 플랫폼의 기능 블록

3.3 보안관리시스템(SMS)

보안관리시스템은 서비스 제공자망에 중앙 집중적으로 존재하여 보안 플랫폼에서 수행할 보안 정책을 생성, 결정, 관리하고 기존의 NMS 시스템의 기본 기능을 포함하고 있는 시스템이다.

제안하는 보안관리시스템의 보안 블록에서는 보안 플랫폼과의 안전한 통신을 위한 SSL/TLS, SSH를 제공하고, Role-based Access Control을 통해 체계적이고 권한에 따른 접근 제어 방식을 제공해야 한다. 관리 블록에서는 기본적인 NMS 기능인 장애 관리, 구성 관리, 서비스에 대한 비용 청구를 위한 Accounting 뿐만 아니라 데이터베이스로 보안 및 관리를 위한 정책 생성, 결정 및 관리와, 새로운 규칙 생성을 확인하기 위한 Rule Checking Engine, 성능 및 트래픽 흐름을 위한 모니터링 기능이 제공되어야 한다.

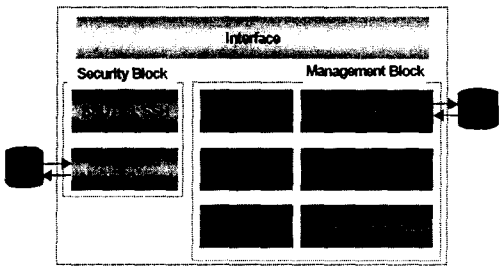

그림 7. 보안관리시스템의 기능 블록

V. 결 론

본 논문에서는 네트워크 환경이 IPv6 도입과 유무선 통합 네트워크로 진화하는 상황을 반영하기 위한 차세대 네트워크 보안 구조에 대해서 제안하였다.

차세대 네트워크 보안이 반드시 갖추어야 하는 보안 요구사항을 도출하였고, 이를 만족하는 보안 플랫폼과 보안관리시스템으로 이루어진 차세대 네트워크 보안 구조를 제안하였다. 제안한 보안 구조는 필수 기능을 중심으로 구성한 것으로, 네트워크 환경에 맞추어 여러 보안 기능들을 추가시킬수 있다.

참고문헌

[1] "인터넷 산업강국 건설을 위한 IPv6 보급 촉진 계획", 정통부, 2003. 9

[2] "고성능 네트워크 정보보호시스템 기능 분석서", ETRI 정보보호연구본부, 2003.11.30

[3] 오승희, 남택용, "차세대 네트워크 보안 구조 제안", COMSW2003, Vol1, p37-40, 2003