보안요구사항 기반의 기업형 FMC 시스템 보안모듈 설계

정현미*, 장수진**, 이강수*

요약

FMC (Fixed Mobile Convergence) 표준화 문서에 따르면 FMC 서비스는 강화된 VPN을 이용하여 다양한 퍼블릭 네트워크 자원(즉, 유선 네트워크, 무선 네트워크 및 융합된 네트워크, 및 다양한 단말장치 상의 일관성 있는 VPN 서비스)을 사용해 일관성 있는 가상 사설 네트워크 서비스를 제공 가능 하게하여야 한다. 이후 FMC 서비스는 통신부분과 업무용시스템을 모두 아우르는 UC(Unified Communication)환경으로 발전하여야 한다. 이에 본 논문에서는 FMC표준화 문서를 바탕으로 중소기업형 FMC 시스템 요구사항을 설계하였다. 더불어 SSL(Secure Socket Layer) VPN의 기반의 보안이 강화된 FMC 보안 Controller, FMC 보안 Client, FMC 보안 관리도구 모듈을 설계하고 요구사항에 맞추어 각 모듈별 기능을 명세하였다.

Design of Enterprise FMC System Security Module by Security Requirements

Hyun Mi Jung*, Gang Soo Lee*, Su Jin Jang**

ABSTRACT

According to FMC standardization document, by using the various public network resources by using strengthened VPN, the FMC service can offer the consistent virtual private network service. The FMC service has to develop into UC environment putting together the communication part and business system altogether. In this paper, enterprise FMC system was designed by FMC General Requirements. SSL VPN based security for security-enhanced FMC of FMC Controller, FMC Security Client and FMC security management tool module was designed and module-specific functions were depending on FMC General Requirements.

Key Words : Enterprise FMC, ITU-T, Security Module, Security System, Unified Communication

* 한남대학교 컴퓨터공학과(✉mihj@se.hannam.ac.kr)
** 대전보건대학교 컴퓨터정보통신과
· 제1저자(First Author) : 정현미 · 교신저자(Correspondent Author) : 이강수
· 접수일(2012년 1월 10일), 수정일(1차 : 2012년 2월 7일), 게재확정일(2012년 2월 10일)

Ⅰ. 서 론

FMC 환경은 기존의 이동통신기술, UMA 기술, 유선 인터넷기술 등 다양한 기존 유・무선 기술들이 통합되는 환경이다. 특히 기업형 FMC(Enterprise Fixed Mobile Convergence) 는 기업 내 외부 에서 사내구성원들이 언제 어디서나 기존 통화업무를 기본으로 업무메일을 송수신 하거나 메신저, 전자결재 등을 수행할 수 있는 환경 즉 스마트 오피스가 실현되어야 한다[1]. 기존 원격 접속 시스템 장치 보다 원격지 이동 사용자에 대한 가용성, 보안성, 편리성을 제공하는 시스템이며 특히 음성 및 데이터들이 이동 경로인 기존 이동통신기술, UMA 기술, 유선 인터넷 기술등 다양한 유 무선 기술들이 통합되는 환경이므로 보안기능이 가장 중요한 필수요소이다. 이에 따라 물리적 환경(FMC Controller, Client)및 유무선 통신 기술(PSTN, VoIP, WiFi 등) 위협 사항 및 보안 요구사항을 분석하여 기업의 특성에 맞는 FMC서비스 설계가 선행 되어야 한다.

따라서 본 논문 본론에서는 기업형 FMC 환경에서 대두될 수 있는 다양한 보안 이슈 중 FMC 표준화 문서를 바탕으로 FMC 서비스 요구사항을 분석한다. 이에 따라 보안이 강화된 SSL VPN 장비를 활용한 기업형 FMC 보안 시스템을 각 Controller, Client 및 관리 모듈별로 설계하고 상세기능을 명세 한다. 결론에서는 기업형 FMC 시스템 개발의 향후 과제 및 연구방향을 제시 한다.

Ⅱ. 본 론

2.1 FMC 표준화 문서를 바탕으로 한 보안 요구사항 분석

ITU-T(International Telecommunication Union - Telecommunication Standardization Sector,국제전기통신연합 전기통신표준화부분)의 FMC 기술표준화를 담당하고 있는 SG19에는 산하에 5개의 Questions 이 있으며 이중 Q.5/19에서 FMC 표준화 이슈를 다루고 있다. Q.5/19는 본래 이동통신망에서의 FMC 이슈를 다루어 왔으나 NGN(Next Generation Networks) 표준화를 담당하는 SG13과 연계하여 표준화 작업이 진행되면서 현재는 'NGN 망에서의 FMC 이슈'를 고려하고 있다. FMC 작업이 SG13과 SG19가 공동으로 진행함에 따라, 각 문서에 대하여 권고안 번호가 Q 및 Y 시리즈로 할당된다. Q.1762문서의 경우, FMC 서비스 및 기능 요구사항을 기술하며 Q.1763문서에서는 모바일 사용자가 PSTN 혹은 ISDN 망을 접속망 으로 사용하는 경우에 대한 FMC서비스 규격을 기술하고 있다[2][3][4]. 특히 Q.1762문서에서는 다음 표 1과 같이 FMC 서비스 요구사항을 정의 하고 있다[5].

표 1. FMC 서비스 요구사항
Table 1. FMC Service Requirements

기능요구사항	세부요구사항
접근 서비스 지원	· FMC 통합서비스를 사용자 단말 의 접속기술에 독립적으로 제공해야한다.
강화된 VPN	· 강화된 VPN은 다양한 퍼블릭 네트워크 자원(즉, 유선 네트워크, 무선 네트워크 및 융합된 네트워크, 및 다양한 단말장치 상의 일관성 있는 VPN 서비스)을 사용해 일관성 있는 가상 사설 네트워크 서비스를 제공 가능 하게한다.
통합된 메시징	· 통합된(unified) 메시징은 사용자가 여러 종류의 메시지를 수신 할 수 있음을 의미 한다. (예: 단 메시지 서비스, 멀티미디어 메시지 서비스, 인스턴트 메시징, e-mail, 등)8 · FMC는 종단 사용자는 수신 되야 하는 메시지 타입을 선택할 수 있어야 한다. 종단 사용자는 선호, 온라인 상태 또는 단말 장치 타입에 기반 해 수신 되야 하는 메시지 타입을 기술한다. FMC는 송신자로 부터의 모든 유형의 메시지를 지원하고, 수신자가 수신가능 한 가능한 포맷으로 메시지를 변환 해야한다.

FMC 서비스 요구사항에서 보여지 듯이 FMC 서비스는 강화된 VPN 서비스를 요구한다. 이는 기업 외부에서 스마트폰과 같은 FMC 단말기로부터 기업 내부망에 접속하기 위해서는 보안이 필수 요소이기 때문이다. 이는 다중 단말 타입을 지원하고 접근 독립적 가상 사설 서비스 네트워크를 지원 할 수 있어야함을 의미한다. VPN방식 중에서 IPSec 방식의 VPN의 경우 업무 특성상 스마트폰을 사용하려는 공공기관 등에 적합하고 이외에 일반적인 업무에 스마트폰을 사용하려는 기업들은 SSL 방식의 VPN이면 충분하므로 본 시스템은 SSL VPN 장비를 활용한 보안이 강화된 기업형 FMC 시스템을 설계하고자 한다.

2.2 FMC 보안 시스템 설계

제안하는 기업형 FMC 보안 시스템은 SSL VPN 기반의 FMC 보안 Controller 모듈, FMC 보안 Client 모듈 및 보안 관리 도구 모듈로 구성되며 다음 그림 1은 전체서비스 구성도이다.

FMC 보안 Controller 모듈은 PCI (peripheral component interconnect) 인터페이스 기반의 암호화 연산 보드 개발 및 암호알고리즘에 사용되는 난수 생성 및 키 생성을 통하여 메시지 암/복호화 수행하고 국내 표준 암호알고리즘(ARIA, SEED) 적용 되며 세션 키 및 인증서 관리 모듈 및 사용자 전자서명 검증 모듈로 구성되어있다.

FMC 보안 Client는 국내 표준 암호알고리즘 (ARIA, SEED)을 적용 하고 세션 키 및 인증서 관리 모듈 및 사용자 전자서명 검증 모듈로 구성되어있다.

FMC 보안 관리도구 는 시스템 관리 및, 보안정책 관리 모듈 및 관리자 및 사용자 인증 모듈 로 구성되어 있다.

그림 1에서 보여 지듯이 FMC Client가 공용 무선 인터넷을 통해 Local Network로 접근하면 FMC Controller는 허가된 FMC Client 에 대해 내부 자원에 접근하거나, VoIP, 메신저, 메일서버 등의 서비스를 이용할 수 있도록 제어한다. 또한, FMC Client와 FMC Controller 사이에 보안 터널링을 이용하여 안전한 보안서비스를 제공한다.

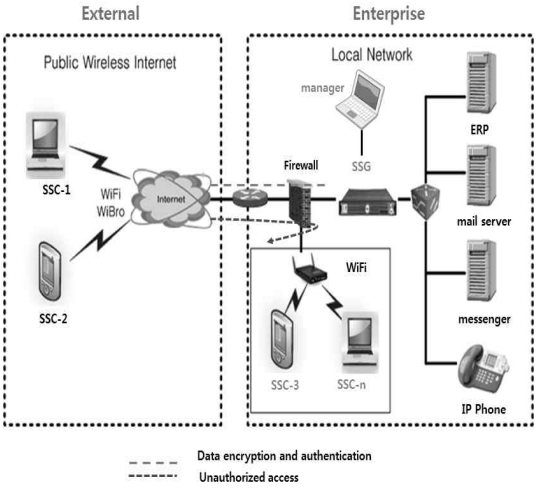

그림 1. 전체 시스템 상세 구성도
Fig. 1. System Configuration

다음 그림 2는 FMC 서비스 구조를 보여준다.

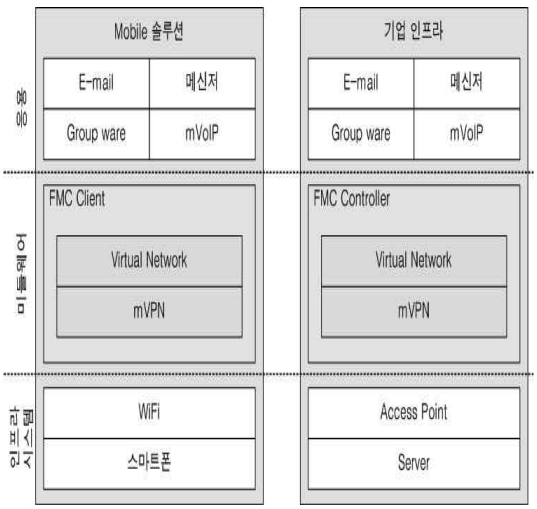

그림 2. 기업형 FMC 서비스 구조
Fig. 2 System Service Architecture

2.2.1 FMC 보안 Controller

FMC 보안 Controller는 SSL VPN의 핵심 기술로써 보안터널 및 보안 게이트웨이의 역할을 수행하며, 클라이언트 접속에 대해 보안정책에 따라 접근통제 서비스를 제공한다. 보안터널 형성을 위해서는 인증서 및 CA 인증서, 설정정보가 필요하고 FMC 보안 관리도구를 통해 제공된다. 다음 그림 3은 SSL VPN 구성도를 보여주며 그림 4 은 모듈 구조를 보여준다. FMC 보안 Controller는 각 클라이언트에 대해 인증 수행 후 보안터널을 형성하여 내부 자원에 접속할 수 있도록 도와준다.

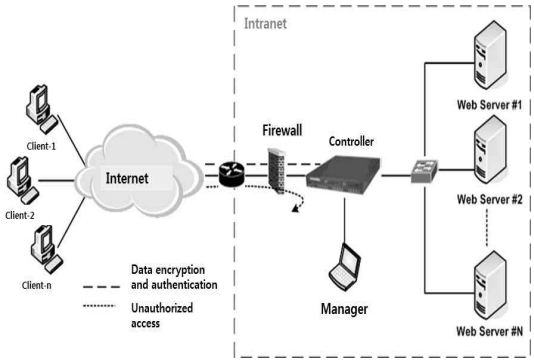

그림 3. SSL VPN 구성도
Fig. 3. SSL VPN Configuration

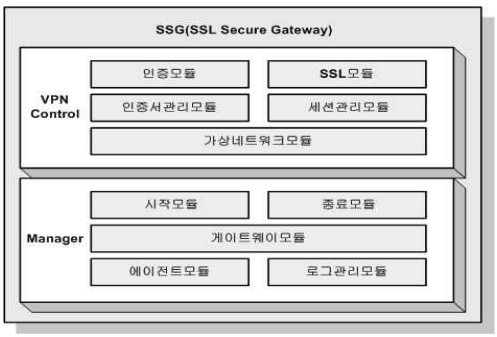

그림 4. FMC 보안 Controller 모듈 구조
Fig. 4. FMC Secure Controller Module

보안 Controller에 관한 자세한 기능명세는 다음 표 2에서 보여진다.

표 2. FMC 보안 Controller 기능명세
Table 2. FMC Secure Controller Functional specification.

구분	모듈	기능
VPN Control	인증모듈	• 사설인증서를 이용한 장치인증 수행 • 제어기와 클라이언트에 대해 상호 인증 수행
	가상네트워크모듈	• 가상네트워크 드라이브 설치 • 클라이언트에 가상 IP 할당 • 보안터널 형성을 위해 필요한 가상 네트워크 드라이브 관리
	세션관리모듈	• 보안터널 형성 및 유지에 필요한 세션 관리
	인증서관리모듈	• SSL VPN 인증에 필요한 CA, 서버, 클라이언트 인증서 관리
	SSL모듈	• SSL Protocol 수행 • 핸드쉐이크 및 레코드 프로토콜 수행
Manager	게이트웨이모듈	• 클라이언트 서비스 요구 대행 • 내부서버와 통신 수행
	시작/종료모듈	• 제어기 시작 및 종료 기능 수행
	에이전트모듈	• 일반 사용자가 SSL VPN 서비스를 제공받기 위해서는 사용자 PC에 에이전트 프로그램 필요 • 사용자 PC에 설치할 에이전트 프로그램 관리
	로그관리모듈	• 시스템 상태 및 접속정보 관리

2.2.2 FMC 보안 Client

FMC 보안 Client 모듈은 클라이언트에 설치되는 사용자 프로그램으로 보안터널 형성 및 사용자 접속정보 관리 등의 기능을 수행한다. Client 역시 Controller 와 마찬가지로 보안터널 형성을 위해 사설인증서, CA 인증서, 환경정보가 필요하며 각 정보는 FMC 관리도구 웹 서버에 접속하여 사용자 로그인후

전송받는다.

다음 그림 5는 FMC 보안 Client의 모듈 구조를 보여주며 자세한 기능명세는 표 3에서 보여진다.

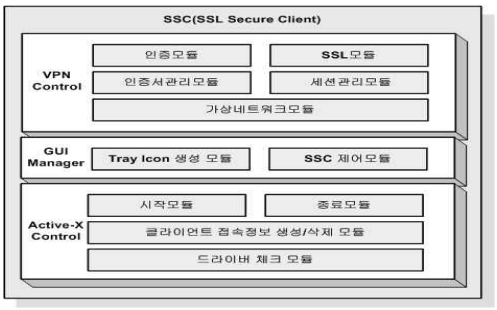

그림 5. FMC 보안 Client 모듈 구조
Fig. 5. FMC Secure Client Module

표 3. FMC 보안 Client 기능명세
Table 3. FMC Secure Client Functional specification.

구분	모듈	기능
VPN Control	인증모듈	• 사설인증서 기반 • 인증 모듈에서는 사설인증서를 이용한 장치인증 수행 • 제어기와 클라이언트에 대해 상호인증 수행
	가상네트워크모듈	• 가상네트워크 드라이브 설치 • 보안터널 형성을 위해 필요한 가상네트워크 드라이브 관리
	세션관리모듈	• 보안터널 형성 및 유지에 필요한 세션 관리
	인증서관리모듈	• SSL VPN 인증에 필요한 CA, 클라이언트 인증서 관리
	SSL모듈	• SSL Protocol 수행 • 핸드쉐이크 및 레코드 프로토콜 수행
GUI Manager	트레이 아이콘 생성모듈	• 클라이언트에 클라이언트제어를 위한 트레이 아이콘 생성
	클라이언트 제어모듈	• 클라이언트 종료 및 Proxy 설정
Active-X Control	시작/종료모듈	• 클라이언트 시작 및 종료 기능 수행
	접속정보관리모듈	• 클라이언트 종료시에 클라이언트에 남아있는 접속정보 삭제 기능
	드라이브 체크모듈	• 가상네트워크모듈 설치 유무 확인 기능

2.2.3 FMC 보안 관리도구

FMC 보안 관리도구 는 SSL VPN의 관리도구로 제어기에 웹서버로 동작하며, 제어기와 클라이언트에 인증서 및 접속정보 등을 제공하고, 사용자 및 운영자 관리, 보안정책 설정, 서버 및 그룹 관리 등의 기능을 제공한다. 다음 그림 6는 FMC 관리도구 모듈 구조를 보여주며 표 4는 관리도구에 관한 기능명세를 보여준다.

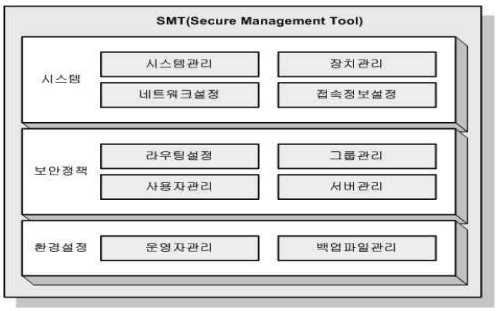

그림 6. FMC 관리도구 모듈 구조
Fig. 6. FMC Management Tool Module

표 4. FMC 관리도구 기능명세
Table 4. FMC Management Tool Functional specification.

구분	모듈	기능
시스템	시스템관리모듈	• SSL VPN System Shutdown 기능 • 제어기 시작/정지 기능
	장치관리모듈	• SSL VPN 추가 기능 • 이중화/로드벨런싱 기능
	네트워크설정모듈	• 내부 IP/외부 IP 설정 기능 • DNS 설정 기능
	접속정보설정모듈	• 터널링 Port 설정 기능

		• 터널링 Protocol 설정 기능 • 세션 접속 시간 설정 기능
보안정책	라우팅설정모듈	• 라우팅 추가 설정 기능 • 라우팅 목록 View
	서버관리모듈	• 서버 등록/수정 기능 • 서버 삭제 기능
	그룹관리모듈	• 그룹 등록/수정 기능 • 그룹 삭제 기능
	사용자관리모듈	• 사용자 등록/수정 기능 • 사용자 삭제 기능
환경설정	운영자관리모듈	• 운영자 등록/수정 기능 • 운영자 삭제 기능
	백업파일관리	• 설정 정보 백업 기능

III. 결 론

본 논문에서는 기업환경에서 효율적인 SSL VPN 기반의 보안이 강화된 FMC 서비스 시스템 모듈을 설계하였다. 또한 이러한 연구결과를 활용하면 이동통신 사업자와 모바일 단말기 사업자의 연동 없이 독립적인 중소기업형 FMC 서비스를 구성할 수 있다.

앞으로 FMC 시스템과 같이 통합 환경에서의 보안이 강화된 시스템 설계를 위해서는 각종 물리적 환경 및 네트워크 환경 내 에서의 보안 위협 사항을 바탕으로 공격시나리오를 분석하여 보다 상세한 요구사항 설계가 필요하며 앞으로 이 연구를 기반으로 이동통신 사업자와 단말 사업자의 결합으로 향후 UC 단계로 발전해 나갈 수 있을 것이다.

또한 이런 요구사항에 따른 시스템 설계 뒤에는 반드시 개인 및 기업의 정보보호가 보장되도록 특화된 보안기술에 관한 꾸준한 연구가 필요하다.

이에 본 논문에 제시한 기업형 FMC 보안 모듈을 토대로 보다 특화된 시스템 설계방안을 연구해 나가야 한다.

참고문헌

[1] The Start of Full-fledged Enterprise FMC Service, ATLAS Research (2009)

[2] Ko, S.-j.: Standardization on FMC in the ITU-T. *Telecommunications Review 18(4)* , 2008

[3] *ITU-T Recommendation Y.2001*, General Overview of NGN, 2000

[4] *ITU-T Recommendation Y.2011*, General Principles and General Reference Model for Next Generation Networks, 2004

[5] *ITU-T Recommendation Q.1762/Y.2802*, Fixed Mobile Convergence General Requirements, Sep. 2007

[6] Final report of Joint industry-university cooperation development, Development of an enterprise FMC security system, Small and Medium Business Administration, 2010

[7] Hyun Mi Jung, Kyung Su Han, Jae In Sin, Gang Soo Lee, Enterprise FMC (Fixed Mobile Convergence) System Requirements Analysis and Design, Korea Multimedia Society ,2011

[8] Hyun-mi Jung, Kyung-su Han, and Gang-soo Lee, A SSL VPN Design Method for Enterprise FMC Security System Development, ICHIT 2011, CCIS 206, pp. 204 - -211, 2011.

저자소개

정현미(Hyun Mi Jung)

1998 : 한남대학교 컴퓨터공학과 (공학사)

2010 : 한남대학교 컴퓨터공학과 (공학 석사)

2010 ~ 현재 : 한남대학교 컴퓨터공학과 박사과정

※ 관심분야 : 소프트웨어공학, 보안공학, 위험분석 및 지식보안 컨설팅, IT 보안시스템 개발

이강수(Gang Soo Lee)

1983 : 서울대학교 전산학
(이학 석사)
1989 : 서울대학교 전산학 박사
(이학 박사)

1987 ~ 현재 : 한남대학교 컴퓨터공학과 교수

※ Research Interest : 소프트웨어공학, 보안공학, IT 보안시스템 개발, 멀티미디어교육

장수진(Su Jin Jang)

1991 : 충남대학교 전산학
(이학석사)
2003 : 한남대학교 컴퓨터공학
(공학박사)

1994 ~ 현재 : 대전보건대학 컴퓨터정보통신과 교수

※ Research Interest : 소프트웨어 개발, 소프트웨어공학, 정보 보안