국방정보통신망 VPN 활용에 관한 연구

전영남, 남길현

국방대학교, 전산정보학과

A Study on utilizing Virtual Private Network in National Defense Information Communication Networks

Young-Nam Jun, Kil-Hyun Nam

Department of Computer & Information Science, National Defense Univ.

요 약

미래전에 능동적으로 대비하기 위해서는 제 전장 요소를 연결하여 지휘결심관련 정보를 신속하고 신뢰성 있게 유통시킬 수 있는 기반체계 구축과 구축된 체계를 안전하게 보호할 수 있는 네트워크 보안기술이 필수적으로 요구된다. 이에 본 논문에서는 미국의 국방정보통신망 기반체계인 DISN(Defense Information Systems Network) 구조와 보안체계를 살펴본 후, 확장성, 보안성, 생존성이 향상된 경제적인 국방정보통신망 구축을 위해 전용망 내부의 보안강화와 전용망 기반의 국방정보통신망과 연결하기 위한 인터넷 기반 VPN의 안전성 보장을 위해 다양한 보안 메커니즘을 제공하는 IPSEC VPN의 국방정보통신망 활용 모델을 제안한다.

I. 서론

미래전에 능동적으로 대비하기 위해서는 예하부대에 정보통신망을 설치하고 제 전장 요소를 연결하여 지휘결심관련 정보를 신속하고 신뢰성 있게 유통시킬 수 있는 기반체계 구축이 필수적이므로 확장성, 보안성, 생존성이 보장되는 초고속 국방정보통신망 구축의 필요성이 크게 부각되고 있다.

본 논문에서는 이동성, 생존성과 안전성이 제공되는 저 비용 고효율의 국방정보통신망 구축을 위해 네트워크에서의 수동적·능동적 공격에 대한 대응책으로 터널링, 암호화, 인증, 데이터 무결성, 접근제어의 보안 메커니즘을 제공하여 최근에 가장 각광받고 있는 IPSEC VPN 기술을 살펴보고, 이를 활용한 국방정보통신망 구축방안을 제시하고자 한다.

II. VPN(가상사설망)

인터넷 표준화 기구인 IETF(Internet Engineering Task Force)에서는 VPN을 상용 인터넷이나 개인 IP 백본 같은 IP설비(Internet Protocol facility)를 사용한 전용 WAN기능의 대리실행이라 정의하고 있다[1].

1. VPN 적용기술

네트워크 보안을 보장하기 위한 VPN 구현 기술은 VPN 내의 두 호스트간에 가상경로를 설정해 주는 터널링, 형성된 가상경로를 비인가 사용자로부터 격리시켜 안전한 채널로 만들어 주는 암호화/인증, VPN내의 자원에 대한 접근 통제를 통해 보안 정책을 구현하게 해주는 접근제어로 나뉘어 진다.

1) 터널링

터널링은 VPN 내의 두 호스트간에 가상경로를 설정해 주어 사용자에게 투명한 통신 서비스를 제공하고, 인터넷과 같은 안전하지 못한 네트워크 환경에서 전용선과 같은 강력한 보안을 제공하는 기능으로 IP 패킷이 공중망을 통과할 때 사용자간에 터널이 뚫린 것 같은 가상통로를 마련해 이 통로를 통해 데이터를 안전하게 전송하는 것이다.

터널링에 사용되는 표준 프로토콜은 IETF가 주도하는 L2TP(Layer2 Tunneling Protocol), IPSec(IP Security Protocol)과 MPLS(MultiProtocol Label Switching)로 대표될 수 있다. L2TP는 자체적으로 터널 인증 기술은 제공하지만 패킷 인증과 패킷 암호화, 키관리 기능을 제공하지 못하기 때문에 IPSec ESP를 이용해 보안기능을 제공한다. IPSec은 AH, ESP 프로토콜을 이용하여 패킷 인증과 암호화를 제공하며, IKE(Internet Key Exchange)와 같은 자동화된 키 관리를 제공한다.

MPLS는 패킷 전송 처리와 경로계산 처리를 분리하여 패킷의 고속전송을 실현하는 기술로서, 기존의 라우팅 방식을 기반으로 ATM의 고속 전송 교환 기능을 결합하여 IP 패킷을 전달하는 기술이다.

2) 암호화 및 인증

네트워크를 통해 전달되는 IP패킷은 spoofing, session hijacking, Eavesdropping 및 Sniffing을 통해 패킷 정보가 유출될 수 있는데 정보의 기밀성을 제공하기 위해 VPN에서는 대칭키 암호를 사용한다. 암호화에 사용되는 대칭키는 공개키 암호 방식을 사용한 키 교환을 통해 공유된다.

메시지인증은 수신된 메시지가 주장된 출처에서 왔고, 변경되지 않았다는 것을 확인하기 위한 절차인데 VPN에서는 MD5나 SHA1을 인증알고리즘으로 사용한다. 사용자인증은 VPN 접속 요구 시 요구주체의 신원을 확인하는 프로세스인데 IPSEC VPN에서는 사용자 인증을 위해 공유키, 공개키, 인증서, 전자서명 등을 사용할 수 있다.

3) 접근제어

패킷 필터링은 지나가는 임의의 패킷에 대한 허용/거부에 대한 판단을 수행하는 것으로 IP 데이터그램의 IP헤더, TCP 헤더, 발신지 및 목적지 주소, 프로토콜 형태, 발신지 및 목적지 포트번호 등을 조사하여 미리 지정된 필터링 규칙에 따라 패킷의 수용 혹은 거부를 결정한다.

NAT(Network Address Translation)은 내부 IP주소를 외부 IP 주소와 맵핑시켜 주는 기술로, 내부로 접속이 허가된 외부 IP주소에 대해서만 내부 IP주소로 변환 작업을 수행하는데, 내부 LAN에서는 사실 IP 주소를 사용하고 인터넷으로 나가는 경우엔 인터넷 주소로 변환하여 전달함으로써 외부 인터넷에 내부 LAN에 대한 정보를 비밀로 할 수 있다.

2. IPSec

IPSec은 IETF에서 응용계층과 독립적인 네트워크 보안을 가능하게 하기 위해 IP 계층에 표준 기반의 인증 및 암호화 기능을 추가하여 만든 것으로 RFC가 인증한 프로토콜이다. IPSEC은 데이터 무결성·기밀성 보장, 데이터 기원 인증, 재생 공격 방지 등의 네트워크 보안 기능을 제공하고, 안전하고 견고한 VPN이 구성되어지도록 지원하는 융통성 있는 구성 요소를 지원한다.

1) AH, ESP

AH(Authentication Header)는 IP 패킷의 데이터 무결성과 인증을 제공한다. ESP(Encapsulation Security Payload)는 암호화 기법을 사용하여 데이터의 무결성, 기밀성의 기능을 제공하는 프로토콜로 사용하는 형태와 모드에 따라 인증기능도 제공한다.

2) 전송(transport)모드, 터널(tunnel)모드

전송모드는 두 통신 호스트간 단-대-단 통신에 사용되어 상위계층 프로토콜에 대한 암호화와 선택적 인증을 제공하는데 IP header를 제외한 IP payload가 보호되므로 전송되는 패킷의 트래픽 분석에는 노출된다. 터널모드는 한쪽 또는 양쪽 종단이 IPSec이 실행되는 방화벽이나 라우터 같은 보안 게이트웨이일 때 사용되어 전체 IP 패킷에 대한 보호를 제공하는데, 안쪽 IP헤더는 출발지와 목적지 주소를 가지고 바깥 IP헤더는 보안 게이트웨이 주소를 가짐으로써 트래픽 분석에 의한 공격을 방지할 수 있다.

3) SA, IKE

IPSec은 SA(Security Associations)를 통해 AH와 ESP의 암호화, 무결성 및 인증 서비스를 제공하는데 SA는 통신 양단 간 IPSec 보호 방법과 절차 협상 내용이다.

IKE(Internet Key Exchange)는 통신 상대가 정당한 사용자임을 확인하는 사용자 인증기능, 통신 양단의 엔티티 사이의 안전한 터널 형성, IPSec에서 사용될 프로토콜 및 알고리즘을 협상하는 IPSec SA협상, 공유키의 생성뿐만 아니라 생성된 키의 소멸과 재생성(re-keying)과 같은 키 관리 기능 등을 동시에 제공한다[2].

III. 한·미 국방정보통신망

1. 미 국방정보통신망

1) 국방정보통신망 구조[3]

DoD는 상호운용이 가능하고 정보공유와 통합이 가능한 전송서비스 구현, 사용자에게 좀 더 빠르고 신속한 서비스 제공, COTS와 국제표준을 적용하여 개방적이고 비독점적인 아키텍쳐 구현, DoD 통신 비용 절감을 목표로 1991년 DISA에 DISN(Defense Information Systems Network)구축을 요청하여 1995년부터 본격적으로 사용하게 되었다. DISN은 데이터망 서비스로 NIPRNET, SIPRNET, JWICS(Joint Worldwide Intelligence Communication Systems), Top Secret WAN서비스를 제공하고 있는데, Top Secret WAN은 NIPRNET이나 SIPRNET에 단-대-단 암호화를 적용해 데이터그램을 암호화하여 NIPRNET이나 SIPRNET을 이용해 통신하기 때문에 별도의 라우팅 기반 네트워크를 구성하지 않았다. 또한 DISN CSs(Communications Servers)를 두어 전용선을 필요로 하지 않는 가입자나 임시적인 임무로 계속 이동해야 하는 가입자에게 NIPRNET이나 SIPRNET(dial in link에 암호화 기능 부가) WAN에 dial-in 접속을 가능하게 하고 있다.

2) SIPRNET, NIPRNET 정보보호체계[4]

SIPRNET(Secret Internet Protocol Router Network)은 비밀로 분류된 자료를 처리하기 위해 DISN내에서 운용되는 데이터 통신망으로, SIPRNET과 DISN 전송로 사이에 KG, KIV 등의 비화장비를 설치하고 전용 라우터를 이용하여 DISN 전송로에 연결되는데 인터넷망과 직접적으로 연결되어 있지 않아 전송로가 외부로부터 보호되고 있다. 망 외부에서의 비인가 접근을 방지하기 위해 라우터 전·후에 B2급 이상의 침입차단시스템을 설치 운영 중인데, 사용자 체계 및 데이터에 대한 책임은 사용자에게 부과하고 있다.

그림 1 : 비화망(SIPRNET) 전송개념

NIPRNET(Non-classified Internet Protocol Router Network)은 SBU(Sensitive But Unclassified) 정보와 평문을 처리하기 위해 DISN 내에서 운용되는 데이터 통신망으로, SIPRNET과 달리 DISN 전송로 사이에 비화장비는 설치되어 있지 않고, 전용 라우터를 이용하여 DISN에 직접 연결되고 DISN을 통하여 인터넷에 접속된다. 망 외부에서의 비인가 접근을 방지하기 위해 라우터 전·후에 침입차단시스템을 설치 운영 중인데, 적절한 보안조치를 전제로 하여 군사적 위협이 되지 않는 평문 및 SBU 정보 송수신에 대해 상용망 활용을 허용하여 국방전산망의 트래픽 부하를 감소시키고, 인터넷 자료 검색 및 활용, 민간인과의 원활한 정보교환을 가능하게 한다.

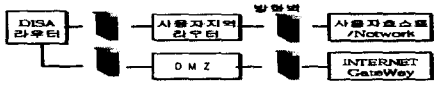

그림 2 : 비비화망(NIPRNET) 정보보호 개념

2. 한국 국방정보통신망

1) 국방정보통신망 구조

TCP/IP에 의한 표준 통신체계를 채택함으로써 이기종간 상호통신이 가능한 국방정보통신망은 각 군의 지휘 통제를 지원하는 기반 전송 체계이다. 정보 체계의 추진 목적에 따라 개별적으로 구축·운영되고 있던 여러 망들은 국방정보통신망 종합발전계획에 의해 ATM기반으로 통합되고 있다.

국방정보통신망은 간선구간에는 T3 전용선으로 토폴러지 Connectivity를 3 이상으로 구성한 ATM 백본망을 구축하여 생존성을 중시하였다. 지선구간인 주요노드부터 예하 부대로는 64Kbps~T3의 전용선이 연결되어 있으나 토폴러지 Connectivity는 1인 상태이다.

전용망인 국방정보통신망과는 별도로 부대소개 및 민원처리를 위한 홈페이지 운영, 자료검색, 전산교육 등을 위해 T1 ~ E1 속도의 상용 인터넷이 활용되고 있는데, 부대 내부에 별도로 분리된 인터넷 LAN을 구성하여 사용하고 있다.

2) 정보보호체계

정보보호를 위해 국방부에서는 CERT팀을 편성하고 침입차단시스템, 침입탐지시스템, 보안 진단도구, 모니터링시스템 같은 정보보호시스템을 도입하여 활용하고 있고, 국방정보통신망에서 정보의 유출, 변조, 훼손 등으로부터 보호하기 위한 주요 보안수단으로는 선로용 보안장비가 활용되고 있다.

IV. 국방정보통신망 VPN 활용

1. 보안장비와 VPN 특성 분석

선로용 보안장비와 VPN 장비는 다음과 같은 고유한 특성을 가지고 있다.

표 1 : 보안장비와 VPN장비 특성 비교

	선로용 보안장비	VPN (IPSec)
암호화	· 패킷헤더 포함 정보	· 패킷헤더 제외 정보
키분배	· 수동분배	· 자동(IKE), 수동분배
사용자 인증	· 인증 기능 없음	· 다양한 인증 방법 - pre_shared 키, 전자서명, 공개키 등
네트웍 접근제어	· 접근제어 기능 없음	· 패킷 필터링 제공 · NAT 기능 제공

전용망 상에서 현재 운용되고 있는 보안장비의 암호화 알고리즘을 접목시킨 VPN 장비를 터널모드로 운용하면 현 보안장비에 준하는 기밀성을 제공할 수 있게되고, 추가적으로 인증, 자동 키교환, 패킷 필터링 기능을 활용할 수 있게 된다.

또한 인터넷 기반 VPN 도입은 국방정보통신망의 경제적 확장과 생존성을 제공할 수 있다. VPN의 터널링 기술은 인터넷에 전용선과 같은 안전한 터널을 형성해 주고, 암호화 기능이 추가된 VPN은 전용선에 실치되어 있는 보안장비와 같이 기밀성을 제공하는 역할을 수행하며, 인증기능은 사용자 인증을 통해 인가된 사용자만 접근하게 허락해 준다. 패킷필터링을 통한 접근제어 기술은 접속을 요청하는 임의의 패킷에서 허가된 패킷만 선별해 접근을 허락해 줄 수 있게 하여 비인가 패킷의 접근을 방지한다. NAT기능을 사용하면 내부로 접속이 허가된 외부 IP주소에 대해서만 내부 IP주소 변환 작업을 수행하고, 내부 LAN에서는 사설 IP 주소를 사용하고 인터넷으로 나가는 경우에만 인터넷 주소로 변환하여 전달함으로써 외부 인터넷에 내부 LAN에 대한 정보를 비밀로 할 수 있게 한다.

2. VPN 활용 모델 제안

본 논문에서 제안하는 구조는 전용망 체계와 연동되는 인터넷 기반 VPN을 백업망으로 활용할 수 있게 되고, 여러 망으로 운용되던 지선 구간 가입자 선로가 비화망과 비비화망으로 통합되고, 내부 LAN도 비화망과 비비화망에 연결되는 비화 LAN과 비비화 LAN으로 통합·운영되며, 비비화망은 상용 인터넷과 연결되어 인터넷을 활용할 수 있는 체계이다. 또한 훈련이나 업무상 이동중인 사용자도 인터넷망을 이용해 국방정보통신망에 접속해 업무를 수행할 수 있게 하는 체계로 세부 구성도는 그림 3과 같다.

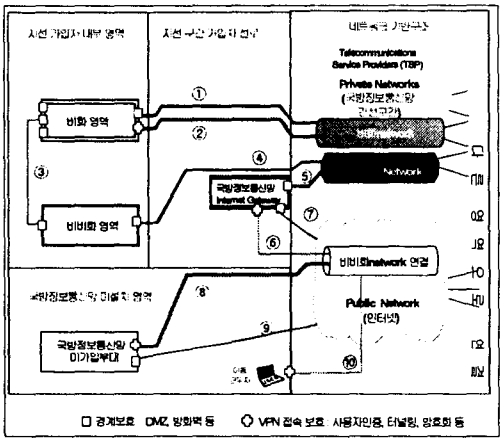

그림 3 : VPN 활용 국방정보통신망 구조

1) 세부 구조 기술

• 전용망 구간 : ①, ②, ③, ④, ⑤ 구간

①, ②는 비화망 접속 구간으로, 비화영역과 국방정보통신망 전송로 사이에 비밀용 보안장비를 설치하고 전용라우터에 의해 국방정보통신망에 연결되는 구간이다. ②는 비화망 내부에서도 민감한 기밀을 다루는 영역으로 VPN의 터널링 기술을 활용하여 비화망을 논리적으로 분리시킨 구간이다. 불법적인 공격이 이루어져도 터널링과 암호화에 의해 자료가 보호되기 때문에 안전하다. ③은 비화망, 비비화망 접속 구간으로, 비밀로 분류된 자료의 불법 노출을 방지하기 위해 접근제어, 식별 및 인증을 위한 전자서명 기술 적용이 필요한 부분으로 국방 인증체계와 접근통제정책 시스템이 구축된 후 활용 가능한 영역이다. ④는 비비화 통신을 위한 영역으로 SBU용 보안장비 설치가 필요한 구간이다. ⑤는 전용망에서 인터넷으로 연결하기 위해 인터넷 게이트웨이와 연결되는 구간이다.

• 전용망·인터넷 연결 구간 : ⑥, ⑦ 구간

⑥, ⑦은 전용망과 인터넷의 연결 부분으로 외부에 노출되어 침해를 받기 쉬운 구간이다. ⑥은 ⑧,⑩과 연결되는 VPN의 안전한 터널이 형성된 인터넷 구간이고, ⑦은 비비화망 내부 사용자들이 인터넷을 활용할 수 있게 연결되는 구간으로, 외부에 정보를 제공하는 인터넷 서버들이 연결된다.

• 인터넷 구간 : ⑧, ⑨, ⑩ 구간

⑧, ⑩은 전용 국방정보통신망 외부에서 인터넷 VPN으로 국방정보통신망에 접속되는 부분으로 외부의 비인가된 침입을 막기 위해 사용자 인증이 필요한 부분이다. 국방인증체계가 구축되기 전에는 VPN 정책서버의 사용자 관리 기능을 활용할 수 있고, 인증체계 구축완료 시엔 인증자료를 활용한 인증이 이루어져야 한다. ⑧,⑩은 ⑥과 연결되어 안전한 VPN 터널이 형성된다. ⑨는 국방정보통신망 미가입부대 내부 사용자들이 인터넷을 활용할 수 있게 연결되는 구간으로, 외부에 정보를 제공하는 인터넷 서버들이 연결된다.

• 인터넷 게이트웨이

VPN 전용장비 및 VPN 정책 서버가 위치하여 인터넷과 사용자 인증 및 암호화를 통한 안전한 터널 형성, 인터넷 기반 VPN 접속자를 대상으로 인터넷 주소를 국방정보통신망 인트라넷 주소로 변경시켜주는 NAT 수행, 국방정보통신망 내부 사용자의 인터넷 사용을 지원하기 위해 내부 인트라넷 주소를 인터넷 주소로 변경시켜주는 NAT을 수행한다.

2) 제안모델의 특성 분석

기존통신망과 제안 통신망의 세부 특성은 표 2와 같다.

표 2 : 기존 통신망과 제안 통신망 분석

	기존 통신망	제안 통신망
지선 구간	· 정보체계 목적에 따른 여러 종류의 망	· 비화망, 비비화망
통신료	· 고비용	· 경제적
백업망	· 없음	· 인터넷 기반 VPN
확장 / 유지보수	· 어려움	· 용이
이동 사용자	· 접속 불가	· 접속 용이
인터넷 활용	· 전용 단말 사용 · 인터넷 주소 사용 (인트라넷과 별도의 주소체계 유지)	· 비비화망 단말 사용 · 인트라넷 주소 사용 (NAT 기능 활용)
보안 서비스	· 기밀성 위주	· 기밀성, 무결성, 발신처 확인, 신분확인 및 인증

3) 목표구조 구축단계

본 논문에서 제안한 구조를 구축하기 위해서는 다음과 같은 수행 단계가 필요하다.

• 1단계 : 비화망과 비비화망 분류 및 조정

• 2단계 : 비화망 내부 군사정보업무 VPN 활용(강화된 보안성)

• 3단계 : 인터넷 기반 VPN 활용

- 국방정보통신망 미연결 부대 비비화망 연계(경계적 확장성)

- 전용망인 국방정보통신망 down시 인터넷 VPN 활용 업무 수행 가능(생존성 확보)

- 비비화망 인터넷 사용 가능(업무 효율성)

• 4단계 : 이동중인 근무자 연계

• 5단계 : 비화망 · 비비화망 연동(상호운용성)

V. 결론

본 논문에서는 국방정보통신망 기반환경을 고찰하고, 전용망 내부보안을 위해 사용하고 있는 보안장비와 상용 VPN 장비의 특성을 분석하여 VPN 기술의 국방정보통신망 활용 모델을 제안하였다. 제안된 모델은 전용망 내부의 보안성 향상, 저비용의 상용 인터넷 활용, 인터넷 활용간 보안성 제공, 상용정보보호 기술의 국방분야 적용, 통신망의 생존성 향상 및 확장 · 신설의 용이성, 이동 근무자의 통신망 활용 등을 고려하였다.

향후 본 논문에서 제시된 VPN 활용 모델에 대한 국방용 암호 모듈 이식 기술, 국방 인증체계 연동, 접근통제 정책 수립, 침입차단시스템 연계에 대한 세부적인 연구가 이루어진다면 보안성, 효율성, 생존성이 향상된 경제적인 국방정보통신망 기반체계를 구축할 수 있을 것이다.

참고문헌

[1] B. Gleeson 외 4명, "A Framework for IP Based Virtual Private Networks", *RFC 2764*, p. 3, Feb. 2000.

[2] D. Harkins and D. Carrel, "The Internet Key Exchange (IKE)", *RFC 2409*, p.1, Nov. 1998.

[3] DISA 홈페이지,"Defense Information Systems Network(DISN) ARCHITECTURE", Sep. 1996

[4] 한미연합사, NIPRNET & SIPRNET 소개, 2001

[5] 국방부, 군사보안업무 시행규칙, 2001년 12월

[6] William Stallings, *Cryptography and Network Security*, Prentice-Hall, Inc., 1999.

[7] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol", *RFC* 2401, Nov. 1998.