효율적인 VPN 통신을 위한 NMS 구현

박종혁*, 이상진*, 이종필**

*고려대학교, 정보보호대학원

** 씨큐어넥서스

A NMS Implementation for efficient VPN communication

Jong-Hyuk Park*, Sang-Jin Lee*, Jong-Pil Lee**

*CIST, Korea Univ.

**Xecurenexus

요 약

네트워크의 급속한 발전과 더불어 컴퓨터 보급 확산을 통해 현대 사회는 정보화 사회로 한층 발돋움하고 있다. 이에 인터넷 환경의 급속한 확산과 개방성, 확장성으로 인한 해킹 등에 의해 정보의 유출, 변조, 도용 등의 보안상 문제점이 심각하게 대두되며, 네트워크를 공유함에 따라 자원의 독점이 불가능하게 되었다. 이로 인해 원하는 시간에 원하는 만큼의 정보를 전송할 수 있는 기능을 보장할 수 없게 되었으며, 네트워크 공유로 인한 속도 저하 등의 서비스 질(QoS: Quality of Service)이 불확실해진 것이다.

현재 TCP/IP 기술이 많은 네트워크 표준 기술로 사용되어 있으며, 이를 기반으로 인터넷에서 사설망의 기능을 제공하기 위해 도입된 기술이 VPN(Virtual Private Network)이다.

본 논문에서는 효율적인 VPN통신을 관리하기 위하여, Web Interface 지원으로 별도의 Management S/W를 설치할 필요가 없는 시스템을 구축하였고, 안정성, 보안성, 신뢰성 등 차별화된 서비스로 네트워크를 통합 관리하도록 하고 있다.

I. 서론

현대사회는 고도의 정보화사회로 인해 컴퓨터의 보급이 급속화되고 있으며, 정보공유 마인드로 인해 네트워크 및 인터넷 사용이 급속히 증가하고, 활용분야가 넓어지며, 대역폭 요구량 또한 급격히 증가하고 있다. 이에 네트워크 시스템의 효율적인 자원관리의 필요성이 대두되고 있다.[1]

1990년대 초반 IETF(Internet Engineering Task Force)에서는 SNMP(Simple Network Manage- ment Protocol)을 제안하였으며, 이를 기반으로 대부분 네트워크 관리에 SNMP를 이용 특정장비의 MIB값을 분석 및 보고 해주고 있다. [2]

인터넷의 확장성과 개방성으로 인해 해킹등에 의한 정보의 유출, 변조, 도용등의 보안상 문제가 심각하게 대두됨에 따라 자원의 독점이 불가능하게 되었다. 이로 인해 특정시간에 필요로 하는만큼의 정보를 전송할 수 있는 기능을 보장할 수 없게 되었으며, 네트워크 공유로 인한 속도저하로 인해 서비스질(QoS:Quality of Service)이 불확실 하게되었다. 그리하여, 현재 TCP/IP를 기반으로 한 네트워크에서 사설망의 기능을 제공하기 위해 도입된 기술이 VPN(Virtual Private Network)이다.

본 논문의 네트워크 장비와의 호환성, 불법행위로부터 정보/ 컴퓨터 시스템 보호등을 목적으로 NMS(Network Management System)을 구현하였으며, 특히 VPN통신을 실시간 감지하여 효율적인 통신을 할 수 있도록 하고 있다. 또한 Web 기반의 인터페이스 제공으로 별도의 S/W가 필요없으며, 보안성, 신뢰성등 차별화된 서비스를 제공 할수있는 자원관리를 위한 시스템을 구현하였다.

II. 관련연구

본 장에서는 구현된 시스템에 사용되는 기반기술들에 관해 간략하게 살펴보기로 한다.

VPN이란 인터넷망 또는 공중망을 사용하여 둘 이상의 네트워크을 안전하게 연결하기 위한 가상의 터널을 만들어 암호화된 데이터를 전송할 수 있도록 만든 가상 사설망 네트워크이

다.[3] 값싼 비용으로 WAN을 통해 네트워크를 연결해 주며 원격 접속 시에 투명하게 네트워크 내부에서 접속하는 것과 동일한 정도의 신뢰도와 보안을 제공해 준다.

현재 인터넷 보안을 위한 주요 기술로는 방화벽(Firewall), 침입탐지 시스템(IDS : Internet Detection System), 그리고 가상사설망(VPN:Virtual Private Network) 등이 있다. 방화벽 기술은 주로 TCP/IP 헤더를 이용한 접근통제가 주 역할로서 복잡한 네트워크 공격 및 호스트 해킹을 차단하는 데에는 한계가 있으며, 침입탐지 시스템의 경우, 로컬 네트워크 측면의 불법행위를 탐지하기 위한 방법으로 제안되었으나, 나날이 발전하는 다양한 네트워크의 공격과 네트워크 광역화에 대응하기에는 약점이 있다. 따라서 최근 사내간, 사내-사외간 통신에 사용되는 네트워크가 점차 인터넷 기반으로 변모함에 따라 인터넷을 이용하면서도 종단간에 안전한 통신이 가능하도록 하는 VPN 기술의 도입이 요구된다.[3]

네트워크는 인터넷의 보편화와 함께 급속도로 번지고 있다. 또한 데이터망(Data Network)과 기존 통신망(Telecommunication Network)의 통합과 서로 다른 시스템, 네트워크 장비, 운영체계(Operating System), 통신규약(Protocol) 등이 복잡하게 묶여 있으며 이를 사용하는 서비스와 사용자가 급격하게 증가하여 점점 규모가 커지고 있다. 따라서 안정적이고 효율적인 네트워크 환경을 제공하기 위해서 네트워크 상에 존재하는 다양한 자원들을 모니터링하고 제어하는 네트워크 관리의 개념이 필요하게 되었다.

NMS는 네트워크상의 전 장비들의 중앙 감시체제를 구축하여 Monitoring, Planning 및 분석이 가능하여야 하며 관련 데이터를 보관하여 필요 즉시 활용 가능하게 하는 관리 시스템이다. 다시 말하면, NMS는 네트워크 관리자가 NMS 제품을 사용하여 현재 운영되는 workstation으로부터 네트워크를 control and monitor할 수 있게 한다.[4]

NMS가 관리하는 객체를 정의하고 객체의 특성을 기술해서 모아놓은 데이터베이스로서, 관리하는 객체는 SMI의 기초 아래 정의된다. MIB는 개념적으로 트리(Tree)구조로 이루어져 있으며 관리되는 최하위 객체들을 leaf node라 한다. 실제 leaf node들이 구현될 때는 객체의 수에 따라 하나 혹은 여러 개의 인스턴스(Instance)로 만들어진다. 예를 들면 하나의 NIC(Network Interface Card)는 한 시스템에 여러 개 존재할 수 있다. 여기서 객체는 NIC가 되며 인스턴스화 되면 NIC[0], NIC[1] 등이 된다. MIB는 어떤 항목에 대하여 문의하면 어떤 대답이 되돌아올지를 각각 정해놓고 있는데 MIB에는 MIB-1, MIB-2, 확장MIB 세 종류가 있다.[5]

인터넷의 규모가 커짐에 따라, 인터넷을 효과적으로 관리하기 위한 체제의 필요성이 대두되었고, 이 같은 필요성을 만족시키기 위한 대안으로 등장한 것이 SNMP이다. SNMP는 1988년 초안(draft)으로 상정되어 1990년 인터넷 관리 프로토콜의 표준으로 제정되었으며, 그 후 대부분의 워크스테이션과 브리지, 라우터, 스위치, 허브 등의 네트워크 장비에 SNMP Agent가 장착되었고, 시스템과 여러 응용 프로그램에도 이들을 SNMP상에서 관리할 수 있도록 하는 MIB들이 정의되었다.

SNMP는 서비스를 제공하는 Agent와 서비스를 이용하는 Manager로 구성되며, IP (Internet Protocol)에서 작동하는 UDP(User datagram Protocol)에 장치되어 있다. Manager측에서 모든 명령어가 발신되지만 Agent측에서는 장애 등의 예상치 못한 사태가 발생했을 때에만 SNMP Manager에게 TRAP명령을 통지하는 구조로 되어 있다. [5]

MRTG(Multi Router Traffic Grapher)는 네트워크 링크 간의 트래픽 부하량을 측정하여 트래픽총량을 확인할 수 있다. Web기반으로 동작하며 그래픽화하여 보여주기 때문에 시각적인 확인에 편리하며, 유닉스, 리눅스 뿐만아니라 윈도우즈계열 플랫폼에서도 동작한다. 또한 SNMP MIB정보를 사용하므로, 패킷을 저장하지 않아 패킷손실이 없다.[6]

III. 시스템 설계

본 장에서는 앞에서 살펴본 기반기술들을 바탕으로 구현된 특화된 NMS에 대해 살펴본다. 본 논문에서는 효율적인 VPN통신을 위한 웹기반의 NMS 관련부분에 대해서만 자세히 다루기로 한다. 각 구성요소에 대해 설명후, 이 시스템의 주요기능과 장점에 대해 살펴보기로 한다.

1. 기존 시스템 고찰 및 개선방향

기존의 NMS는 네트워크상의 라우터, 브릿지 등 일반적인 네트워크 장비의 구성요소(Network Element)들의 중앙감시체제를 구축하여 수집(Monitoring) 및 분석(Planning)하여, 수집된 자료들을 토대로 현재의 망 분석, 중단 없는 서비스를제공하였다. 하지만 현대와 같이 보안이 중요시되는 시대에 VPN통신까지 감시하여 결과를 보고해주는 NMS는 나와있지 않다.

이에 VPN GateWay에 대한 세부적인 정보를 수집하여 효율적인 VPN통신 관리 기능이 부가된 NMS를 구현하도록 한다.

2. 구조

설계구조는 그림 1과 같다.

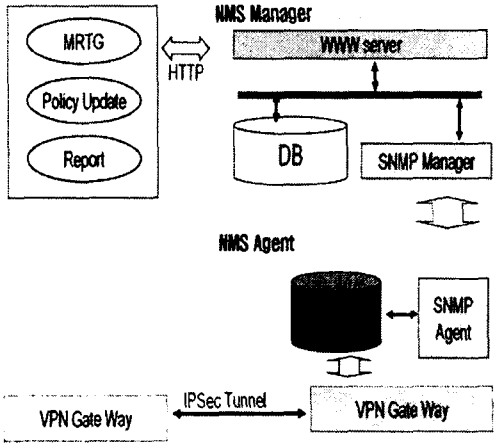

그림 1 : 효율적인 VPN통신을 위한 NMS의 설계

1) NMS Agent

NMS Agent는 SNMP Agent가 IPSec Tunnel을 통해 VPN통신의 정보를 VPN게이트웨이로부터 읽어들여 저장하는 IPSecFlowMonitorMIB[7]으로 구성되어 있으며, SNMPv2를 사용하는 독립적인 SNMP Agent이다. IPSec Flow Monitor MIB 에 대한 자세한 정보는 [7]에서 자세히 나와있다.

2) NMS Agent SNMP Manager를 통한 원격관리로 동작된다. 명령어를 통해 얻어진 정보는 DB에 저장되며, 이후 원하는 일시에 기록을 확인할수 있다.

3. 시스템 설계

본 논문에서 구현된 시스템은 실시간 VPN통신을 통한 트래픽의 흐름을 분석하여 보여주도록 설계되었으며, 또한 SNMP를 통해 얻어진 정보는 IPSec에 대한 여러 가지 정보(사용된 암호알고리즘, 인증 프로토콜, SA, SPI등) 및 통신시 송.수신된 메시지에 대한 자세한 정보를 확인할 수 있다.

4. 시스템 주요기능

1) SNMP를 이용하여 이용률 및 에러율을 실시간 정보로 제공하므로서 IPSec을통한 Packet 정보를 분석하여 제공해 준다.

2) 수집 설정된 노드에 대한 트래픽 정보를 지속적으로 수집하며, 이정보를 DB에 저장, 다양한 항목분석에 의한 통계보고서를 제공한다.

3) 일,월,기간별 IPSec Packet의 통계분석 정보를 다양한 형태의 그래프로 제공한다.

5. 시스템의 장점

1) 기존의 NMS의 사용자 인터페이스와 달리 친숙한 웹기반의 인터페이스 사용으로 사용방법에 대한 숙지가 용이하다.

2) 시간 및 장소에 관계없이 고정된 NMS 서버에 접근하지 않고도 웹브라우저를 통해 관리할 수있다.

3) 통신장비에 추가적인 비용부담이 없이 관리가 가능하다.

IV. 시스템 구현

1. 시스템 개발환경

Linux Kernel 2.4.18 운영체제인 Pentium III 366MHz, 64MB 메모리의 컴퓨터와 Apache Web Server를 사용하였으며, GUI환경을 위해 PHP, MRTG를 사용하였다. 데이터베이스 구축을 위해 MySQL, Agent로 Net-SNMP, IP Security를 위해 VPN GateWay로 FreeS/Wan을 사용하였다.

시스템 요구사항으로는 NMS Manager로 사용할 컴퓨터(1대), VPN GateWay(2대), VPN 장비용 컴퓨터(2대)가 필요하다. 또한 MRTG를 지원하기 위한 IMG library와, 패킷을 수집하기 위한 libpcap이 설치되어 있어야 한다.

3. 시스템 구현

1) 화면구성

그림2는 웹브라우저에서 실행된 시스템의 화면구성이다. 왼쪽메뉴를 통해 인증된 관리자만이 IPSec 흐름에 대한 정보를 볼수 있으며, Introduction은 본 시스템의 구조와 기능을 소개한다.

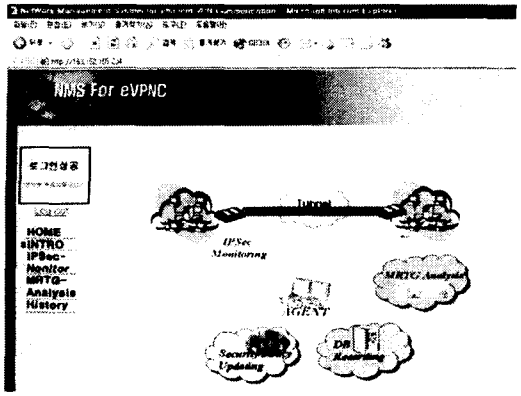

그림 2 : 시스템 소개 화면

2) NMS를 이용한 결과

NMS의 IPSec 흐름에 대한 전체적인 Connection부분과 각 메시지의 State별 자세한 정보로 나뉘어진다. 또한 트래픽량의 실시간적인 추이를 시각화하여 그래프로 나타내준다.

그림3은 현재 Connection 및 메시지의 State 정보를 보여주고 있다.

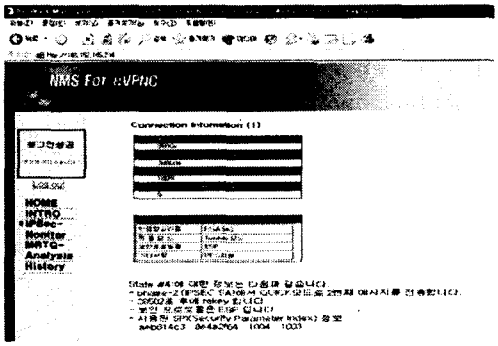

그림 3: VPN통신에 대한 연결 및 State별 메시지에 대한 세부사항 보고

V. 결론 및 향후과제

본 연구에서 TCP/IP를 기반으로한 인터넷에서의 VPN통신을 효율적으로 하기 위한 NMS를 구현하였다. 또한 관리의 편의성을 도모하고, 각종 트래픽의 분석된 데이터를 시각화하여 그래프형태의 보고서를 제공하며, 로그의 데이터베이스화로 필요할 때마다 확인 가능하게 되었다. 이로써, 관리자는 네트워크 현황 및 성능분석과 사용현황 파악이 더 쉽게 되었으며, 불필요한 트래픽을 막고 다양한 로그기록을 이용하여 보다 안전하고 효율적인 시스템을 위한 보안정책 수립에 영향을 미칠 것으로 기대된다.

참고문헌

[1] John Bommers, "Practical Planning for Network Growth", Prentice Hall PTR, 1996

[2] William Stallings, "SNMP, SNMPv2, SNMPv3, adn RMON 1 and 2", 3rd Edition, Addison Wesley, 1998

[3] Virtual Private Network Consortium Web- Site. http://www.vpnc.org/

[4] Leinwand, Allan, and Fang, Karen, "Network Management: A Practical Perspective", Addison -Wesley, 1993.

[5] J. Case, M.Fedor, M.Schoffstall and C.Davin, "The Simple Network Management Protocol(SNMP)", RFC 1157, May 1990

[6] Tobias Oetiker and Dave Rand, "MRTG: Multi Router Traffic Grapher", http://www.mrtg.org

[7] C. Madson, L. Temoshenko, C. Pellecuru and S.Ramakrishnan, "draft-ietf-ipsec-flow-moni toring-mib-01.txt", IPsec Working Group, 21 April 2001