FreeS/WAN과 cIPe의 VPN 보안 프로토콜 성능 시험

신용녀[0] 정태인 박희운
한국정보보호 진흥원
{ynshin[0], tijung, hupark}@kisa.or.kr

Performance Evaluation of VPN Protocol for FreeS/WAN and cIPe

Yong-Nyuo Shin[0] Tae-In Jung Hee-Un Park
Korea Information Security Agency

요 약

가상사설망이 중요한 정보를 원격에 전송한다는 개념만으로 여겨질 때에는 암호화 강도에 주목했었다. 그러나 가상사설망 시장이 활성화되면서 보다 많은 트래픽을 효율적으로 처리하기 위하여, 가상사설망 고성능화에 대한 요구가 증대되고 있다. 본 논문에서는 가상사설망에서 성능 측정 시 필요한 항목들을 제시하고 설치한 네트워크 성능에 얼마만큼의 영향을 미치는지에 대해 살펴본다. 이를 위해 네트웍 환경을 IPSec 프로토콜을 사용하는 FreeS/WAN 패키지를 활용하여 구성해보고, 자신의 독자적인 프로토콜인 CIPE 프로토콜을 사용하는 cIPe 패키지를 사용하여 다양한 성능지표들을 반영한 성능 측정을 실시하였다. IPSec 표준을 준수하여 구현된 FreeS/WAN은 적용하는 방법에 따라 네트워크 성능 차가 상대적으로 크고 cIPe 방법은 암호화 적용 전에 비해서 그다지 큰 차이를 보이지는 않는다. 본 결과들을 고려할 경우, 가상사설망의 성능과 보안을 적절히 유지하는 범위에서 정책과 시스템 사양을 고려하여 가상사설망을 도입하여야 할 것이다.

1. 서 론

현재 시행되는 정보보호제품의 성능시험에서는 가장 일반적으로 적용 가능한 처리량(throughput)과 지연(latency), 동시 커넥션 수 정도를 시험항목으로 사용한다[1]. 이러한 항목들은 일반적인 네트워크 제품 성능 측정에는 적합하지만 정보보호 제품을 시험하기 위해서는 보다 특화된 성능 지표가 필요하다. 가상사설망(Virtual Private Network)이 네트웍 제품임엔 틀림없지만 정보보호 제품의 보안요구사항들이 시험항목이나 시험조건에 보다 적극적으로 반영되어야만 한다.

가상사설망이 중요한 정보를 안전하게 전송한다는 개념만으로 여겨질 때에는 암호화 강도에 주목했었다. 하지만 현재는 모든 인터넷에 관련된 트래픽을 보내는데 있어서 가상사설망 내지는 암호화 방법을 사용하게 되었다. 결과적으로 안전한 인터넷 사용에 대한 필요성이 커짐에 따라 보다 많은 트래픽을 처리하기 위한 가상사설망 성능에 대한 요구가 증대되고 있다. 따라서 본 논문에서는 가상사설망 성능 측정시 필요한 항목들을 제시하고 이들 항목들이 제품의 성능에 미치는 영향을 고찰하여 향후 나아갈 방향을 고려하도록 한다. 본 논문은 2장 성능측정 시 필요한 항목들을 기술하고, 3장에서는 다양한 성능 지표들을 반영하여 구성한 성능측정 환경을 설명하고 4장에서 테스트 결과를 고찰하여, 5장에서 결론을 맺는다.

2. 성능 측정 항목

2.1 성능 측정 기본 항목

시장에 다양한 가상사설망 제품이 나오기 시작하면서 더욱 더 세분화되고 전문적인 성능 시험이 이루어 져야 할 것이다. 성능 시험을 위한 일반적인 시험 항목들은 다음과 같다.

- 처리량(Throughput) : 디바이스에 의해 폐기되어지는 프레임이 없을 때 초당 처리되는 최대 Bits 수[2]
- 지연(Latency) : 패킷의 비트가 DUT(Device Under Test)의 출력비트에서 나오는 시간과 패킷의 비트가 DUT의 입력포트에서 나오는 시간간의 차이
- 최대 동시 세션(Maximum Concurrent Sessions) : 원격사용자의 네트웍 이용의 돌발성 때문에 필요한 지표, 초당 일정 처리량 속도로 유지될 수 있는 최대 세션 수
- 연결 수립 지연(Connection Establishment Latency) : 처음 연결 수립 시 암호화를 위한 키 교환 과정의 지연시간
- Back-to-back frames : 오류 없이 처리될 수 있는 연속된 패킷의 수

2.2 확장성을 고려한 시험 항목

초기 제품들은 가상사설망의 보급성에 대해서는 고려하지 않았음으로 확장성에 따르는 문제들을 해결하려는 노력이 없었다. 하지만 최근에 나오는 가상사설망 제품들을 고려해보면 이러한 문제들을 접근하려는 노력들이 있다. 제품의 신뢰성제고를 위해서는 성능 평가에서 있어서 다양한 조건들에 대한 고려가 있어야 한다.

- 암호화 시 처리량(Encryption Throughput) : Security 보장을 위해서 outgoing traffic에 대해 보통 Layer-3 암호화를 수행 시 처리량[3]
- 단편화(fragmentation) 처리 능력 : 부가적인 암호화

부하와 매체의 MTU(Maximum Transfer Unit)를 고려한 단편화 처리 능력
- 고 가용성(High Availability) : 업그레이드 시나 시스템의 문제 발생 시 VPN 성능 유지 능력
- 상호 운용성(Interoperability) : 다양한 제품들 간에 데이터를 서로 주고받는데 문제가 없는지를 시험
- Stress Test : 극한적 부하(조건)에 대한 시스템의 대응성을 시험하는 것으로 시간 속성을 평가하고 부하의 변화에 따른 영향을 측정[4]
- 지속성 테스트 : VPN의 네트웍 장비적 특성에 의거하여 단순 성능을 떠나 연결된 하나의 세션이 장기간 문제없이 끊기지 않아야 함
- 신규 세션 수립 능력 : 초당 맺어질 수 있는 신규 세션 갯수[5]

3. 다양한 성능지표들을 반영한 성능 측정

위에서 언급한 성능 지표들이 모두에게 필요한 것은 아니다. 가상사설망이 어디에 이용되느냐에 따라 적절한 성능 지표가 선택되어져야 한다.

모든 TCP/IP 프로토콜을 적절히 암호화하여 전송하는 일반적인 게이트웨이 시스템을 구현하는데 가상사설망이 자주 이용된다. 이러한 경우에 가상사설망의 처리량이 매우 중요한 요소가 되며, 구성상 효과적인 성능을 내는지 여부를 측정할 필요가 있다. 따라서 본 논문에서는 상호네트웍사이에 가상사설망을 구성하여 성능측정을 하기 위해, 상기 제시된 지표 중에서 처리량, 암호처리량, 지연에 한하여 시험을 수행한다.

이 시험에서는 일반적인 하드웨어 가상사설망 제품을 사용하는 것이 아니라 리눅스 운영체제상의 가상사설망 구성이 가능한 두가지 방법을 비교한다.

첫 번째는 IPSec 프로토콜을 사용하는 FreeS/WAN 패키지를 활용하는 구성방법이고 두 번째는 자신의 독자적인 프로토콜인 CIPE 프로토콜을 사용하는 cIPe 패키지를 사용하는 구성방법이다.

IPSec은 IP 자체에 대해 보안 설정을 하기 때문에, 모든 패킷을 IPSec에 근거해 암호화 한 후 또 다른 IP 패킷으로 캡슐화해서 상대방한테 보낸다. CIPE는 상호간에 UDP 터널을 형성 후에 암호화된 IP 패킷을 해당 터널로 전송하는 방법이다.

두 방식 모두 커널 패치 형태로 제공되지만 FreeS/WAN은 IPSec 표준을 따르나, cIPe는 독자적인 구성 방법으로 암호화하여 보내주는 경량 패키지이다.

3.1 FreeS/WAN

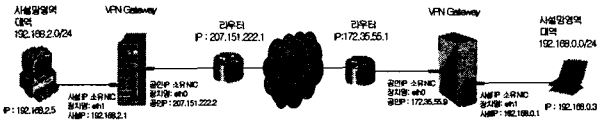
FreeS/WAN(Secure Wide Area Network)은 IPSec 표준기능을 준수하는 오픈 소스 패키지이다[6]. 리눅스 커널 모듈로서 KLIPS(Kernel IP Security)와 IPSec IKE 키 교환을 수행하고 IPSec keyring을 관리하는 데몬인 Pluto등으로 구성되어 있다. 레드햇 리눅스 7.2[7] 와 WOLK(Working Overloaded Linux Kernel) 커널[8] 버전 3.5를 사용하였다. Sourceforge 의 WOLK 프로젝트는 주로 실험적인 커널 패치들을 포함하는 프로젝트로서 다양한 기능들을 커널에 넣고 실험을 할 수 있도록 만들어진 커널 패치 모음이다. 여기에는 다양한 신규 파일시스템이나 네트워크 코드, 신규VM 등과 같은 실험적인 기능들이 들어가 있는데 이들 중에 IPSec 에 관련된 패치가 포함되어 있다. WOLK 프로젝트 커널에 포함된 IPSec 부분은 FreeS/WAN 프로젝트에서 만들어지고 있는 IPSec 커널 패치를 넣어놓은 것이다. 현재 IPSec 부분은 커널 모듈로 컴파일 및 사용 가능하다.

3.2 cIPe

cIPe(Crypto IP Encapsulation)는 UDP상에서 암호화된 IP 패킷의 터널링을 제공하는 최적화(Customized)된 경량 패키지이다[9]. 이 실험에서는 버전 1.5.4 를 사용했으며, 리눅스 커널 버전 2.{2,3,4}을 지원하고 기본적으로 i386 플랫폼에서 운영 가능하다. 커널모듈과 user-level 데몬으로 구성되어 있다. 커널 모듈은 해당 게이트웨이에서 발생하는 모든 IP 패킷을 암호화하여 UDP 패킷으로 만든 후에 터널을 통하여 상대편 cIPe 게이트웨이로 보낸다. user-level 데몬은 키 교환을 수행한다.

cIPe는 Blowfish, IDEA, Diffie-Hellman의 암호화 알고리즘을 지원하고, Blowfish가 기본 암호화 방법이다.

3.3 시험 환경 구성



(그림 1) 구성된 시험 환경

네트웍 대 네트웍 가상사설망을 구성하였으며, 한 네트웍에 속한 개별 호스트에서 상대편 네트웍에 속한 개별 호스트로 각각 10번씩의 iperf를 수행한다. iperf 프로그램은 서버와 클라이언트로 동작하며 클라이언트가 IP 패킷을 일정량만큼 생성하여 상대편 iperf 서버로 전송 할 때, 전송이 완료된 시간을 측정하는 툴이다. 이외에도 가장 간단한 테스트 툴인 ping을 사용하여 응답시간을 측정한다.

구성에 사용된 환경은 인터넷 망을 제외하고 개별 네트웍의 라우터까지는 100Mbps 이더넷이고 Full Duplex 모드를 사용한다. 각 네트웍에 속해서 iperf 테스트를 수행하는 개별 호스트도 리눅스 시스템을 사용한다.

4. 시험 결과 분석

4.1 시험 시나리오

FreeS/WAN의 시험은 IPSec의 운영방법에 따라서 시험하고 cIPe 테스트는 기본 구성상에 지원되는 Blowfish 암호화 방법을 시험한다. 그리고 상호간의 비교를 위해서 일반 터널링을 시험한다. 이 때 사용한 테스트 시나리오는 다음과 같다.

- 일반 터널링 - 어떤 암호화 방법도 적용 안됨
- FreeS/WAN 가상사설망
  96bit MD5 알고리즘과 RSA 서명알고리즘을 이용한 AH 인증
  128비트 3DES를 사용한 ESP 암호화
  ESP 암호화와 96bit MD5를 이용한 인증
  ESP 암호화와 AH 인증
- cIPe에서 Blowfish 암호화 및 터널링

4.2 시험 결과

4.2.1 처리량 (Throughput)

iperf를 사용한 각 시나리오별 처리량 측정 결과는 다음과 같다.

<표 1> 적용정책에 따른 처리량의 변화

적용정책	처리량
IPSec 없음	56 (Mbits/sec)
AH 인증	37.5 (Mbits/sec)
ESP 암호화	16.8 (Mbits/sec)
ESP 암호화 + 인증	11.1 (Mbits/sec)
AH 인증 + ESP 암호화	11.3 (Mbits/sec)
cIPe Blowfish 암호화	50 (Mbits/sec)

FreeS/WAN은 적용하는 방법에 따라 네트워크 성능 차가 상대적으로 크고 cIPe 방법은 암호화 적용 전에 비해서 그다지 큰 차이를 보이지는 않는다. 하지만 표준적인 방법이 아닌 자신의 독자적인 암호화 방법을 수행하고 인증과정이 없기 때문에 man-in-the-middle 공격과 같은 크래킹에 취약할 수 있다.

4.2.2 응답시간

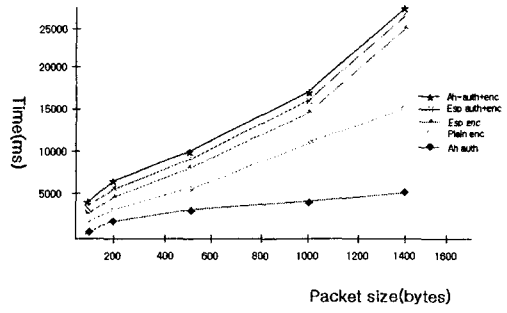
ping을 사용한 각 시나리오별 응답시간 측정 결과는 다음과 같다. 32byte 만을 실험한 결과이다.

<표 2> 적용정책에 따른 응답시간의 변화

적용정책	응답시간
IPSec 없음	0.57 (sec)
AH 인증	0.65 (sec)
ESP 암호화	0.80 (sec)
ESP 암호화 + 인증	0.85 (sec)
AH 인증 + ESP 암호화	0.88 (sec)
cIPe Blowfish 암호화	0.60 (sec)

ping 의 패킷길이가 32byte 로 고정되어 있기 때문에 각 시나리오별 절대적인 응답시간에는 그다지 큰 차이를 보이지 않는다. 그러나 상대적인 비교에서 처리량 측정 실험과 비슷한 결과가 발생했다.

4.2.3 운영체제의 네트워크 스택상의 부하



(그림 2) IP Stack 상의 소요시간 비교

각 실험에 사용한 시나리오에서 모두 운영체제 네트워크 스택에 영향을 줄 수 있게 되어 있다. IPSec의 경우 운영체제에서 처리하여 실제 물리인터페이스까지 전달되기 전까지의 시간에 대한 각 시나리오별 측정 결과는 그림2와 같다.

IP 패킷에 대한 암호화와 인증부분을 수행하는 점에 있어서 복잡도가 높기 때문에 운영체제에서 암호화와 인증처리를 위해서 다양한 정책이 사용되는데 이러한 때 가상사설망 성능에 어떠한 영향이 있을 수 있는지 보여준다. IPSec을 운영하는 경우에 부하가 없을 수 없기 때문에 성능과 보안을 적절히 유지하기 위한 균형점에서 정책과 시스템 사양을 생각하여 리눅스 가상사설망 도입을 수용해야 할 것이다. 또한 도입하려는 가상사설망 시스템에서 IPSec에 관한 부분을 지원하고 IPSec을 운용하려고 한다면 위의 결과를 참고하여 각 애플리케이션별 또는 네트웍 어플라이언스별 비교가 이루어질 수 있을 것이다.

5. 결론

본 논문에서는 가상사설망을 설치했을 경우 성능측정항목을 도출하고 네트워크 성능에 어떠한 영향을 미치는지 대한 결과를 보였다. IP VPN 기술은 계속적으로 급속한 전개를 해오고 있으므로, 가상사설망 기술을 지원하는 네트웍 장비가 앞으로의 네트워크들의 필요성에 부합되도록 확장될 필요가 있다. 이를 위해서, 네트웍 장비 제조업체들은 그들의 디바이스들이 강력한 보안 기능들을 지원하면서 높은 수준의 성능을 제공함을 보장하고 있다. 동시에 이러한 개발 요구 사항들을 만족시키기 위해서는 확장성있고 정확한 성능 시험이 이루어져야 한다. 여기서 다루었던 시험을 통하여 IPSec 표준을 준수하여 구현된 FreeS/WAN은 적용하는 방법에 따라 네트워크 성능 차가 상대적으로 크고 cIPe 방법은 암호화 적용 전에 비해서 그다지 큰 차이를 보이지 않음을 볼 수 있었다. cIPe는 가상사설망의 사용 부하를 최소화시킨 경량화 패키지이기 때문이고 표준적인 방법이 아닌 자신의 독자적인 암호화 방법을 수행하고 인증과정이 없기 때문에 man-in-the-middle 공격에 취약할 수 있다. VPN의 성능과 보안을 적절히 유지하기 위한 균형점에서 정책과 시스템 사양을 생각하여 가상사설망을 도입하여야 한다. 향후에는 보다 다양한 성능지표를 활용한 성능 시험 방법론에 대하여 제시할 수 있을 것이다.

6. 참고 문헌

[1] NSTL 보고서,"Intel NetStructure 3130 VPN gateway Test Report", 2001
[2] IETF RFC 2544, Benchmarking methodology network interconnect devices,1999
[3] Tolly 보고서,"NetScreen Technologies Inc. Test summery",2001
[4] KISA,정보보호시스템 평가 방법론 연구, 1996
[5] ICSA Labs IPSec Product Certification Version 1.0B,2002
[6] FreeS/WAN 홈페이지, http://www.freeswan.org/
[7] 리눅스 커널, http://www.linuxhq.com/
[8] "WOLK 커널", http://sf.net/projects/wolk
[9] Oleg Kolesnikov, Building Linux Virtual Private Networks, 2002