논문 2011-48TC-12-6

업무망/기관망의 보안 연결 방안 연구 및 테스트베드 구축

(Security Association and Testbed Implementation for Separated Business and Organizational Networks)

박 세 철*, 장 인 식**, 이 재 용***, 김 병 철***, 이 명 신*, 현 대 환*, 정 대 원*

(Se Chul Park, In Sik Jang, Jae Yong Lee, Byung Chul Kim, Myung Sin Lee, Dae Hwan Hyun, and Dae Won Chung)

요 약

현대의 네트워크를 이용한 IT산업은 폭발적으로 발전하여 기존에 오프라인으로 행해지던 작업들이 온라인상에서 행해지는 일이 빈번해지고 있고 인간관계까지 온라인상에서 이루어지는 경우가 많아지고 있다. 이에 따라 오프라인으로 이루어지던 침해 사고 같은 범죄가 온라인상에서도 빈번하게 이루어지고 있고 그 수도 나날이 증가하고 있기 때문에 보안 네트워크의 구축이 매우 중요해졌다. 이러한 노력의 일환으로 업무 망과 기관 망 간의 망 분리를 국가적으로 추진하고 있으나 이는 망 사용자 측면의 불편과 효율성 저하를 가져온다. 본 논문에서는 현재 많은 곳에서 추진 중인 네트워크 망 분리 사업에서 분리된 망을 제한적으로 연결시킬 수 있는 안전한 방안을 제시하고 그 중 NAT를 이용한 연결과 공유 스토리지를 이용한 연결 방법에 대해 테스트베드를 구현하고 실험한 결과를 보였다.

Abstract

As IT industry using networks have been developed explosively, online operations that were conducted in offline are increasing rapidly, and even relationship with other people made online. As online crimes are increasing accordingly, building security networks is getting very important. As a result, network separation between business and organization network has been performed recently, but this causes network user inconvenience and efficiency reduction. In this paper, we propose reassociation methods for already separated networks for many public organizations. We implement two reassociation methods using NAT device and shared storage and show their experimental results.

Keywords: Security networks, Shared storage, NAT, network design

Ⅰ. 서 론

IT산업의 폭발적인 발전은 인간의 생활방식을 많이 바꾸어 놓았다. 금융, 교육, 쇼핑 등 일상생활에 필요한 대부분의 행위를 오프라인이 아닌 온라인 기반의 사이버 영역에서 하는 것이 가능해 졌으며, 직장에서 행해지는 작업 또한 집이나 직장이 아닌 다른 곳에서 할 수 있도록 편의를 제공하였다. 그 결과로 기존에 오프라인에서 행해지던 일상생활 및 직업적인 활동이 온라인 기반의 사이버 영역으로 대체되었고 이를 호기심, 경제적 이익을 위해 공격하는 경우도 나날이 증가하게 되었다. IT산업이 발전하던 초기 사이버 환경에 대한 공격은 정치나 군사적 목적에 의해 정부나 군대로의 공격이 대부분이었으나 현대에 와서는 기업에서 운영하는 시스템과 더불어 개인이 사용하는 IT 시스템까지 공격이 행해질 정도로 그 범위가 확장 되고 있다. 또한 공격 범위뿐만 아니라 공격 방법 또한 매우 다양해지고 있다. 이에 따

* 정회원, 한국항공우주연구원 (KARI)
** 학생회원, *** 평생회원, 충남대학교 정보통신공학과 (Chungnam National University)
※ 본 연구는 한국항공우주연구원의 임무관제국 네트워크 보안설계 및 보안평가기술 연구의 일환으로 수행하였음.
접수일자: 2011년4월5일, 수정완료일: 2011년12월9일

라 개개인이 이용하는 PC나 소규모 네트워크에서도 네트워크 보안의 중요성이 커지고 있지만 특히 높은 보안성을 요구하는 데이터가 생성 및 저장되고 때에 따라서는 다른 네트워크 사이트로 전송해야 하는 국가 기관망의 네트워크 보안은 더욱 중요시 되고 있다. 현재 국가 기관망은 물리적인 망 분리 정책[1]에 따라 인터넷 망에서 업무를 수행해야 하는 업무 망과 직접적으로 인터넷 망에 연결되지 않고 폐쇄적으로 작업을 수행하는 기업 망으로 네트워크를 분할하는 작업이 벌어지고 있다. 하지만 여러 국가 기관망의 데이터 공유를 통해 효율적인 데이터 활용의 필요성이 있음에 따라 인터넷망과의 제한적인 연결 허용은 반드시 필요하다. 이 경우 인터넷망과의 제한적인 연결허용은 보안 공격에 쉽게 노출될 수 있기 때문에 위험이 뒤따른다.

본 논문에서는 현재 추세에 따라 물리적으로 분리되어 있는 국가 및 회사 기관 망과 업무망간의 제한적인 연결 시 고려할 수 있는 보안 설계 방안에 대해서 기술하였다. 또한 이중 비교적 소규모 네트워크 시설에서 많이 쓰이는 NAT(Network Address Translator)[2]를 이용한 보안망 설계 방안과 보안상 가장 강력한 망 연결 방법인 중계 스토리지를 이용한 망 연결 방안의 테스트베드를 구축하고 보안 안정성을 실험하였다.

Ⅱ. 업무 망과 기관 망과의 망 분리 방안

현재 보안 네트워크 구축 시 가장 중요시 되는 방향이 내부 네트워크와 외부 네트워크를 분리하는 것이다. 즉 인터넷에 직접적으로 연결되어 관련 서비스를 제공하거나 인터넷 관련 업무를 수행하는 외부 네트워크와 회사의 내부에 관련된 업무를 수행하고 인터넷에 직접적으로 연결이 허용되지 않는 내부 네트워크로 망을 나누어 운영하는 것이다.

그림 1과 같이 상대적으로 보안상 위협이 크고 내부 네트워크로 악성 코드 감염을 유도할 수 있는 외부 네트워크를 물리적으로 완전히 내부 네트워크와 분리하여 관리하는 방법이 있지만 내부 네트워크를 완전히 폐쇄하여 관리 할 경우 내부 네트워크의 중요 데이터를 다른 기관과 공유하는 것이 불가능하기 때문에 효율적으로 데이터를 이용할 수 없고 다른 기관과의 데이터를 통한 상호작용도 이루어 질수 없기 때문에 인터넷 망과의 제한적인 연결은 불가피 하다.

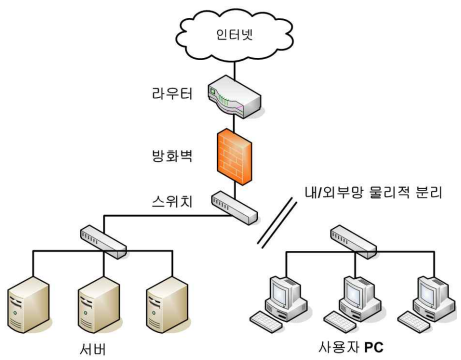

그림 1. 물리적 망 분리
Fig. 1. Physical network separation.

Ⅲ. 분리망의 제한적 보안 연결 방안

물리적으로 분리되어 있는 내부 네트워크와 외부 네트워크를 제한적으로 보안성을 유지하며 연결하는 방법은 여러 가지가 있다. 본 장에서는 분리 망을 연결하는 네 가지 설계에 대해 제시한다.

3.1 NAT를 이용한 연결

NAT를 이용한 연결 방법은 그림 2 와 같이 NAT 역할을 하는 하나의 경계 라우터 (border router)와 하나의 방화벽으로 보안 시스템을 구축한 설계로 경계 라우터를 통해 1차적인 패킷 필터링이 이루어지고 보다 심도 있고 중점적인 패킷 필터링은 경계 라우터 후방에 있는 방화벽에 의해 이루어진다. NAT는 기본적으로 외부에서 시작되는 인터넷 통신을 통과시키지 않기 때문에 뛰어난 보안성을 유지할 수 있다. 이 설계는 현재 서비스되고 있는 유선 인터넷 망에 널리 사용되고 있으며 보안에 사용되는 장치가 상대적으로 적기 때문에 구축 및 유지비용이 절감되고 장비에 대한 정책 설정도 간단

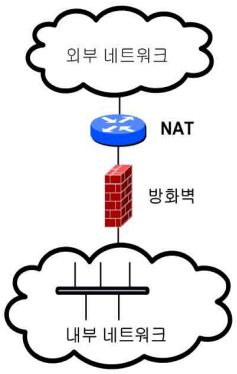

그림 2. NAT를 이용한 연결
Fig. 2. Interconnection using NAT.

하다. 하지만 경계 라우터나 방화벽의 공격을 통해 오류가 발생하면 내부 네트워크 전체가 고립되는 단점이 있다.

3.2 방화벽 이중화를 이용한 연결

방화벽 이중화를 이용한 연결 방법은 그림 3 과 같이 이전 설계에 방화벽을 하나 더 배치한 방식으로 외부 방화벽을 통해 네트워크가 DMZ와 내부 네트워크로 분리되는 것이 큰 특징이다. DMZ에는 외부 망과 관련된 작업을 수행하는 웹 서버나 메일 서버를 배치하여 외부에서의 접근을 용이하게 하였고 내부 네트워크로의 접근은 내부 방화벽의 배치를 통해 쉽게 접근할 수 없도록 했다. NAT를 이용한 연결과 마찬가지로 경계 라우터는 1차적인 패킷 필터링 작업을 수행하고 중점적인 방어는 두 개의 방화벽에 의해 수행된다. 이 설계의 내부 네트워크에 접근하기 위해서는 두 개의 방화벽을 거쳐야 하므로 이전 설계에 비해 보안이 강화된 것이라고 할 수 있으며 상대적으로 취약해질 수 있는 DMZ 구역이 공격당하더라도 내부 방화벽으로 인해 내부 네트워크에는 큰 영향을 미치지 않는다. 반면에 경계 라우터에 트래픽이 몰리거나 공격을 당하여 오류가 발생하면 내부 네트워크가 고립되는 현상이 발생할 수 있다.

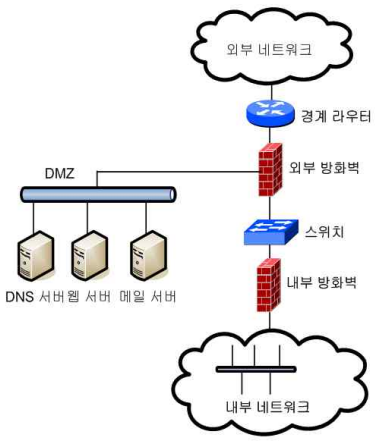

그림 3. 방화벽 이중화를 이용한 연결
Fig. 3. Interconnection using dual firewall.

3.3 병렬 이중화된 라우터와 방화벽을 이용한 연결

이중화된 라우터와 방화벽을 이용한 연결은 그림 4 와 같이 방화벽 이중화를 이용한 연결과 유사하지만 두 개의 경계 라우터와 두 개의 방화벽을 병렬 이중화로 배치한 것이 특징이다. 이는 트래픽에 대해서 부하 분산(Load balance)을 제공하고 하나의 라우터나 방화벽이 동작 하지 않을 경우 즉시 다른 하나의 쌍이 역할을 이어 받아 네트워크 전체가 고립되는 현상을 방지하게 해주는 역할을 한다. 경계 방화벽의 양단에 설치되어 있는 L4 스위치는 특정 세션에 포함되어 있는 패킷들이 이전에 통과했던 동일한 방화벽만을 통과하도록 한다. 즉 세션 내의 일부 패킷이 다른 쪽의 방화벽으로 가면 설정에 의해 패킷이 통과를 할 수 없으므로 각 세션마다 동일한 방화벽을 통과하게 만들어 세션을 유지할 수 있게 해주는 것이다. 또한 DMZ 구역과 내부 네트워크를 분리시켜 상대적으로 내부 네트워크를 안전하게 방어 한다. 하지만 보안에 사용되는 장치가 상대적으로 많기 때문에 구축과 유지에 있어서 많은 비용이 들 수 있고 각 장치에 대한 정책 설정이 복잡해질 수 있는 단점도 존재하는 설계이다.

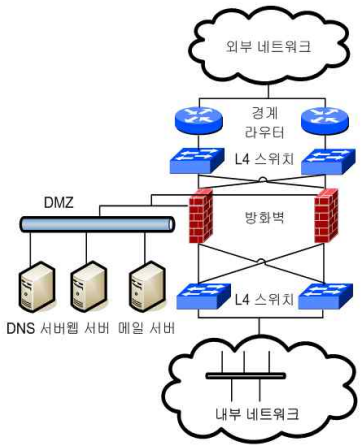

그림 4. 병렬 이중화된 라우터와 방화벽을 이용한 연결
Fig. 4. Interconnection using parallel routers & firewalls.

3.4 공유 스토리지를 이용한 연결

공유 스토리지를 이용한 연결은 그림 5와 같이 외부 네트워크와 내부 네트워크를 중계 서버와 중계 저장장치를 통해 연결하는 방법이다. 외부 혹은 내부에서 요청된 패킷은 중계 서버를 통해 중계 저장장치로 요청되고 중계 저장장치는 반대쪽 중계 서버에 패킷을 다시 요청하게 된다. 요청된 패킷은 요청 과정의 역순으로 망 분리 장치를 통과하여 전달되게 된다.

중계 저장장치가 일종의 캐쉬 역할을 하여 외부 인터넷 망과 내부 네트워크를 연동시킴으로써 앞서 언급한 설계들보다 더욱 강력한 보안을 제공하게 되고 망 분리 장치 이외에 방화벽을 추가로 설치 할 경우 더욱 향상

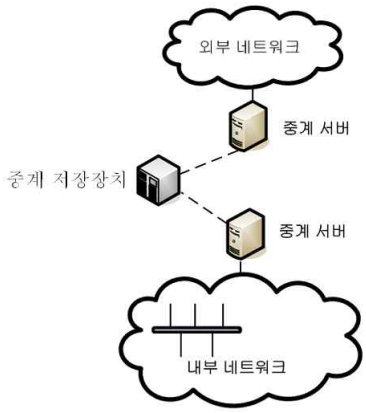

그림 5. 공유 스토리지를 이용한 연결
Fig. 5. Interconnection using shared storage.

된 보안을 제공할 수 있다. 또한 현재 기관망에 대한 정부의 보안정책에 부합한다는 장점도 가지고 있다.

Ⅳ. 분리 망 보안 연결을 위한 테스트베드

본 장에서는 앞 장에서 제시한 NAT를 이용한 망 연결 방안과 공유 스토리지를 이용한 망 연결 테스트베드를 구축하고 실험한 내용에 대해 설명한다.

4.1 NAT를 이용한 망 연결 테스트베드

NAT를 이용한 망 연동 방법은 공격자의 입장에서 공격해야하는 보안 장비의 수가 상대적으로 적기 때문에 공유 스토리지와 같이 강력한 보안을 제공해 주지는 않지만 설치 및 관리가 간단하기 때문에 일부 보안 등급이 상대적으로 낮은 내부 네트워크의 보안에 많이 쓰이는 방법이다. 이러한 NAT를 이용한 망 연동 테스트베드의 환경은 그림 6과 같다. 전체적인 시나리오는 내부 네트워크의 192.168.1.3의 주소를 가진 FTP 클라이언트가 134.75.85.146의 주소를 가진 인터넷망의 FTP 서버에 접속하는 것과 168.188.48.207의 주소를 가진 외부 네트워크 FTP 클라이언트가 192.168.1.4의 주소를 가진 내부 네트워크 FTP서버에 접속할 수 있도록 NAT의 packet filter를 설정하였다.

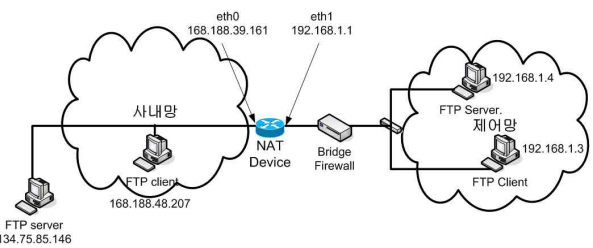

그림 6. NATA 테스트베드 환경
Fig. 6. Topology of NAT testbed.

NAT 장비의 OS는 리눅스를 사용하였으며 주소 변환 및 패킷 필터링은 리눅스에서 제공하는 iptables를 이용하였다. 우선 두 개의 네트워크 인터페이스 카드를 사용하기 때문에 각 인터페이스 카드 간 패킷의 포워딩을 허용하기 위해 다음과 같은 명령어를 입력해야 한다.

```
~#echo 1 > /proc/sys/net/ipv4/ip_forward
```

이러한 iptable의 NAT 체인을 바탕으로 테스트베드에서의 수행한 명령은 다음과 같다.

```
~#Iptables -t nat -A POSTROUTING -o eth0 -j
  SNAT --to 168.188.39.161
~#Iptables -t nat -A PREROUTING -p tcp -s
  168.188.48.207 -d 168.188.39.161 -j
  DNAT -to 192.168.1.4
```

먼저 첫 번째 명령어는 NAT의 POSTROUTING 체인에 정책을 추가하는 명령어로써 eth0의 카드를 통해 나가는 모든 패킷의 소스 주소는 168.188.39.161로 주소가 변환되어 나간다는 것을 의미한다. 즉 168.188.39.161이라는 고정된 주소를 통해 NAT 내부에 있는 모든 네트워크들이 외부 네트워크와 접속을 할 수 있다는 뜻이다. 두 번째 명령어는 NAT의 PREROUTING 체인에 정책을 추가하는 명령어로써 NAT 장비로 들어오는 패킷 중 송신 주소가 168.188.48.207이고 목적지 주소가 168.188.39.161, 그리고 사용 되는 프로토콜이 TCP인 경우 목적지 주소를 192.168.1.4로 변환하라는 명령이다. NAT를 사용하면 외부에서 내부의 주소를 모르기 때문에 외부에서 먼저 시작되는 접속이 불가능하다. 따라서

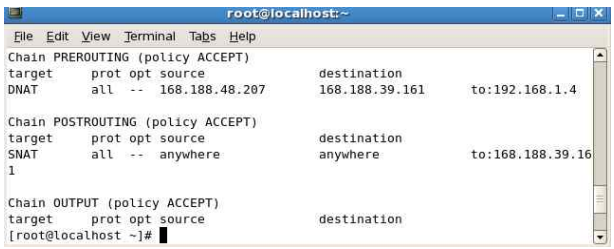

그림 7. NAT 정책
Fig. 7. Policy of NAT.

이 명령을 통해 168.188.48.207의 주소를 가진 호스트의 경우에만 내부의 192.168.1.4 주소를 가지는 호스트와 접속을 할 수 있도록 허용하는 것이다. 이 명령어들을 통해서 그림 7 과 같이 iptables 상에 정책 테이블이 만들어지게 된다.

NAT 후방에 배치되어 있는 방화벽의 설정은 리눅스 커널의 네트워크 설정을 브리지로 바꾸는 것으로부터 시작된다. 네트워크 설정을 브리지로 바꾸는 방법은 리눅스 기반의 브리지 모듈인 brctl을 설치하는 것으로 간단히 구현된다. 최근에 업데이트 된 리눅스 버전에서는 기본적으로 설치가 되지만 설치가 안 되어 있다면 다음의 명령어로 설치하면 된다.

```
~#apt-get install brctl
```

브리지 모듈이 설치되었다면 PC에 설치된 두 개의 네트워크 인터페이스 카드를 브리지 형태로 동작하도록 설정해야 한다. 두 개의 인터페이스 카드가 각각 eth0, eth4라면 다음과 같은 명령어로 브리지로 설정할 수 있다.

```
~#brctl addbr br0
~#brctl addif br0 eth0
~#brctl addif br0 eth4
~#ifconfig eth0 down
~#ifconfig eth4 down
~#ifconfig eth0 0.0.0.0 promisc up
~#ifconfig eth4 0.0.0.0 promisc up
~#ifconfig br0 192.168.1.2 promisc up
```

우선 br0라는 가상의 브리지 인터페이스를 만들고 그것에 eth0과 eth4 인터페이스 카드를 추가시키고 IP 주소를 제거한다. 또한 모든 패킷을 받아들여서 내보내기 위해 promisc라 옵션을 주고 마지막으로 가상 브리지 인터페이스에 IP주소 하나를 할당하는 것으로 마무리 된다. 이 명령어를 실행한 후 그림 8과 같이 가상의

그림 8. 가상 네트워크 인터페이스
Fig. 8. Virtual network interface.

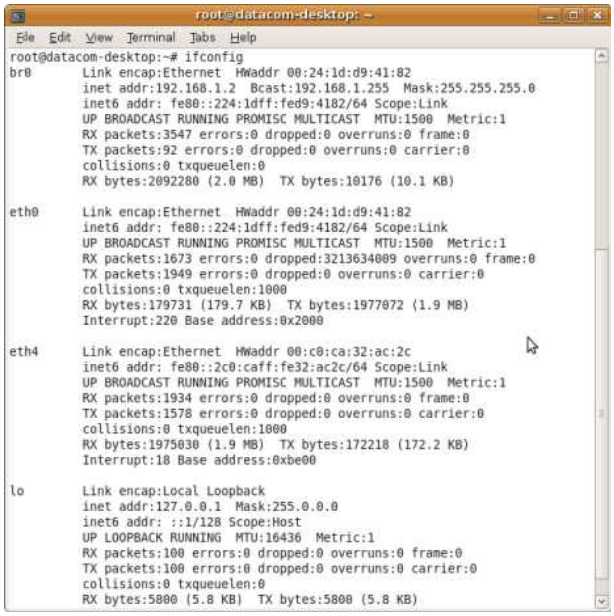

그림 9. 가상 인터페이스 확인
Fig. 9. Confirm of virtual network interface.

브리지 인터페이스가 만들어 졌음을 확인할 수 있다.

브리지 인터페이스의 확인은 brctl show라는 브리지 모듈상이 아닌 커널에서의 ifconfig명령어를 통해서도 가능하다. 그림 9를 보면 IP가 할당되지 않은 두 개의 실제 인터페이스 카드와 br0라는 가상 브리지 인터페이스가 설정되어있음을 확인할 수 있다.

테스트베드에 사용되는 방화벽은 Firewall builder[3]라는 오픈 소스 기반의 방화벽을 사용하였다. 리눅스에서 사용되는 방화벽은 대부분이 수동적인 iptables의 정책 설정을 보다 간편하게 하기 위한 방화벽으로써 결론적으로 GUI환경에서 방화벽을 설정한다 하더라도 이는 모두 iptables의 정책을 변경시키는 것과 동일하다고 볼 수 있다. 그러한 여러 방화벽 중 정책 설정을 가장 자세한 부분까지 할 수 있고 대부분의 방화벽이 브리지 모드에서는 잘 동작하지 않는 반면, Firewall builder는 브리지 모드를 문제없이 지원하기 때문에 사용하였다. 최초 방화벽 설정 시 그림 10과 같이 브리지 방화벽 모드를 활성화하면 문제없이 작동을 하게 된다.

그림 11은 브리지 설정 완료 후 실제적인 방화벽 정책을 작성한 것이다. 먼저 첫 번째 정책은 내부 네트워크에 있는 특정 호스트가 특정 주소를 가진 인터넷망의 FTP 서버에 접속하는 것을 허용하는 정책이 되겠고 두 번째 정책은 외부 네트워크의 특정 주소를 가진 호스트가 내부 네트워크의 FTP 서버에 접속할 수 있게 해주는 정책이다. 특히 두 번째 정책은 NAT 장비의

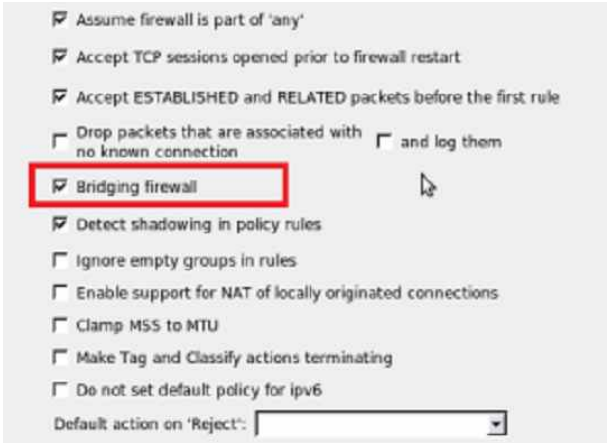

그림 10. 방화벽의 브리지 모드 설정
Fig. 10. Firewall setting with bridge mode.

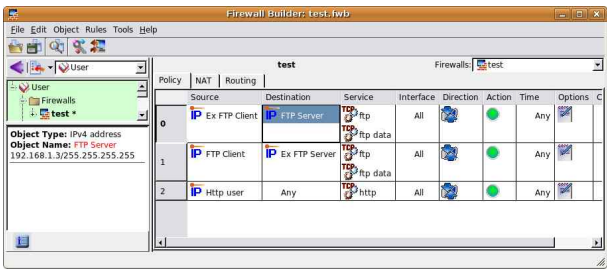

그림 11. 방화벽 정책 설정
Fig. 11. Firewall policy configuration.

PREROUTING 체인과 융합되어 해당 IP에 대한 확인을 두 번 해주는 효과를 나타낸다. 마지막 정책은 내부 네트워크의 일부 호스트들에 대해 웹서비스를 허용하는 정책이 되겠다. Firewall builder는 정책 테이블 설정 후 정책을 제외한 패킷은 모두 거부하는 정책이 기본적으로 수행되기 때문에 따로 이외의 패킷에 대한 정책을 만들어주는 작업은 필요가 없다. 또한 외부 네트워크와의 통신에는 NAT의 체인설정과 방화벽의 정책 추가를 통해 간단히 구현할 수 있다.

이러한 테스트베드 설정 작업을 통해 외부 네트워크에서 내부 네트워크 FTP 서버로의 접속과 내부 네트워크에서 인터넷망의 FTP 서버로의 접속이 원활히 이루어짐을 그림 12 를 통해 확인할 수 있다. 또한 외부 네트워크에서 시작되는 접속은 NAT 장비와 방화벽, 두 군데에서 필터링이 이루어지기 때문에 상대적으로 안전하다고 볼 수 있다.

내부 네트워크의 FTP 클라이언트에서 인터넷망 FTP 서버로의 FTP 접속과 외부 네트워크 FTP 클라이언트에서 내부 네트워크 FTP 서버로의 접속이 가능한 테스트베드를 구축하였지만 보안 측면에서 안전한

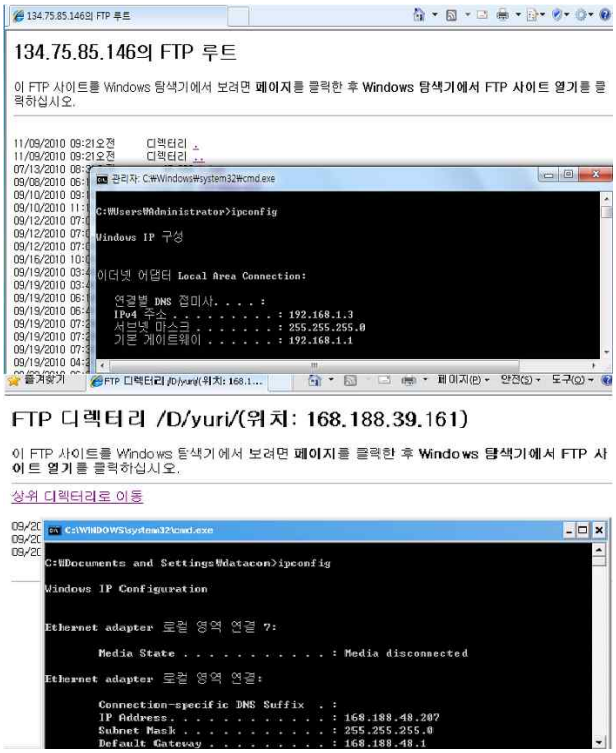

그림 12. 각 망에서의 FTP 접속 확인
Fig. 12. Confirm of FTP connection for each network.

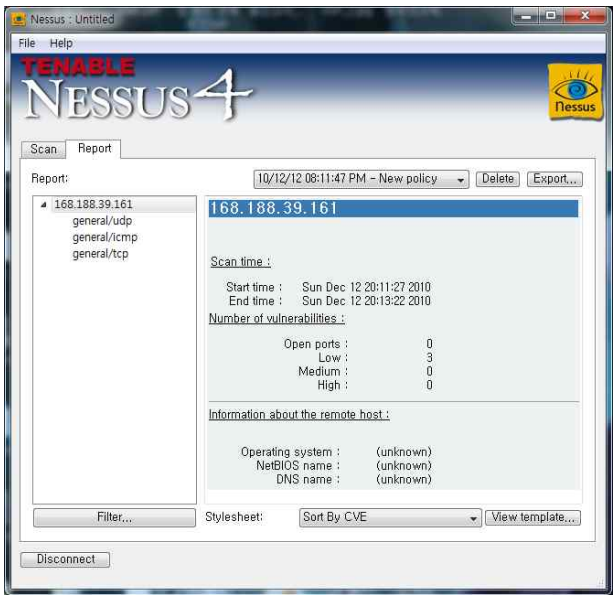

그림 13. NAT 테스트베드에 대한 Nessus 스캔
Fig. 13. Nessus scanning for NAT testbed.

것인지는 겉으로는 알 수 없다. 비록 NAT 장비를 이용해 내부 주소를 알 수 없기 때문에 일반 공용주소를 쓰는 것 보다는 안전할 수 있겠지만 정확한 안전성을 확인하기 위해 Nessus[4]툴을 이용하여 테스트베드의 취약점을 스캔해 보았다. 스캔 정책은 가능한 모든 취약점

을 찾아서 보고하는 Full-scanning을 사용하였고 그 결과는 그림 13과 같다. 우선 테스트베드에 열려있는 포트는 없음을 알 수 있으며 총 3개의 취약점이 발견되었다. 하지만 발견된 취약점은 위험성이 낮은 취약점으로써 udp, icmp, tcp를 이용하여 해당 호스트나 서버까지 traceroute가 가능했다는 결과이다. 즉 호스트나 서버 자체에는 취약점이 없다는 결과와 같다.

4.2 공유 스토리지를 이용한 망 연결 테스트베드

물리적으로 분리되어있는 망을 연동시키는 방법은 여러 방법이 있지만 그 중 네트워크 보안을 가장 강력하게 유지해주고 현재 정부의 보안정책에 가장 부합하는 방법이 공유 스토리지를 이용한 망 연동 방법이다. 하지만 공유 스토리지와 각 망의 데이터를 받아 공유 스토리지에 전송하거나 공유 스토리지의 데이터를 가져오는 전송 통제 서버의 도입은 금전적으로 상당한 부담을 야기한다. 여기에 보안을 더욱 강화하기 위해 공유 스토리지와 전송 통제 서버사이에 Fiber 채널까지 도입할 경우 적게는 수천만 원에서 많게는 수억 원까지의 금전적 부담을 예상해야 한다. 본 절에서는 물리적으로 분리된 망에 대한 공유 스토리지를 이용한 연동 방법을 일반적인 PC 3대와 인터넷을 통해 쉽게 구할 수 있는 각종 툴을 이용해 저비용으로 구현하고 실험한 내용에 대해 서술한다.

가. 공유 스토리지 구현

공유 스토리지는 두 개의 전송 통제 서버로부터 데이터를 전송 받아 임시적으로 저장하고 다른 편의 전송 통제 서버가 자신으로 전송될 데이터가 있는지 확인할 경우 데이터를 넘겨주는 역할을 한다. 따라서 일반 PC로 공유 스토리지를 구현하기 위해서는 각 전송 통제 서버와 양방향 통신이 가능해야 하기 때문에 두 개의 네트워크 인터페이스 카드가 기본적으로 설치되어 있어

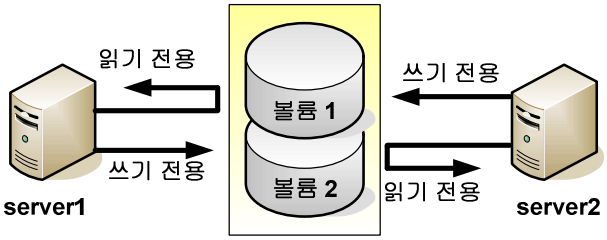

그림 14. 공유 스토리지 테스트베드 구조
Fig. 14. Structure of shared storage testbed.

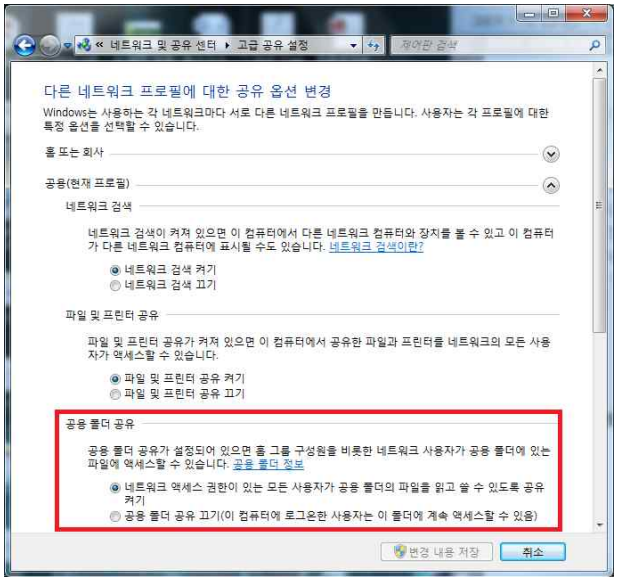

그림 15. 특정 폴더 공유의 허용
Fig. 15. Admission of specific folder sharing.

야 한다. 전체적인 테스트베드 구조는 그림 14와 같은 구조로 공유 스토리지의 볼륨을 두 개로 나누어 각 볼륨의 권한 설정을 통해 각 전송 통제 서버가 읽을 수 있고 쓸 수 있는 볼륨으로 나누어야 한다.

권한 설정에 앞서 각 전송 통제 서버가 공유 스토리지에 어떠한 방법으로 접근 할 것인지 설정해야 한다. 이에 따라 공유 스토리지의 디스크를 다른 PC에 공유하기 위해서 OS에서 기본적으로 지원되는 특정 폴더 혹은 특정 디스크의 네트워크 공유 방법을 사용하였다. 구현에 쓰는 OS는 마이크로 소프트 윈도우 7이며 그림 15 의 설정을 통해 현재의 네트워크 도메인에서 특정 폴더를 공유할 수 있다. 초기에 공유 폴더 공유 부분의 설정이 '공용 폴더 공유 끄기'로 설정되어 있다. 이를 공유 켜기로 바꾸어 줌으로써 특정 폴더에 대한 공유가 1차적으로 허용이 된다.

공유 스토리지는 권한에 따라 두 개의 볼륨으로 나누어지기 때문에 구현하는 공유 스토리지도 마찬가지로 물리적 혹은 논리적 방법을 통해 볼륨을 나누어야 한다. 네트워크 공유 폴더를 통해 디스크 전체를 볼륨으로 지정할 수도 있지만 본 논문에서는 특정 폴더를 볼륨으로 지정하여 구현하였다. 폴더를 하나의 볼륨으로 지정하는 방법은 그림 16과 같이 특정 폴더 내에 각 전송 통제 서버가 사용할 폴더를 생성하는 것으로 시작한다.

여기서 server1이라는 폴더는 1번 서버가 쓸 수 있고 2번 서버가 읽어 올 수 있는 공간이고 server2는 그 반

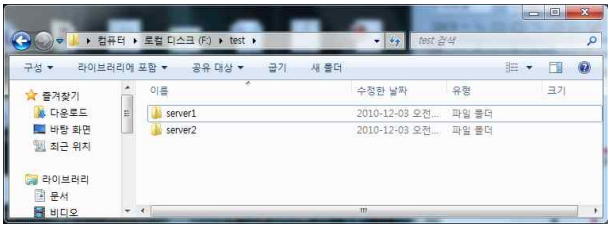

그림 16. 공유 폴더 생성
Fig. 16. Generation of shared folder.

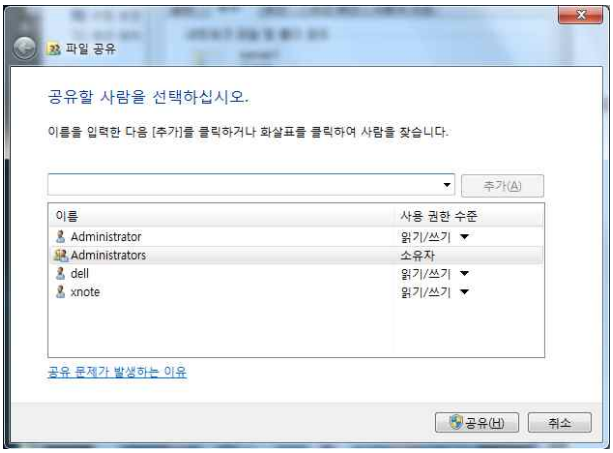

그림 17. 공유 폴더 설정
Fig. 17. Configuration of shared folder.

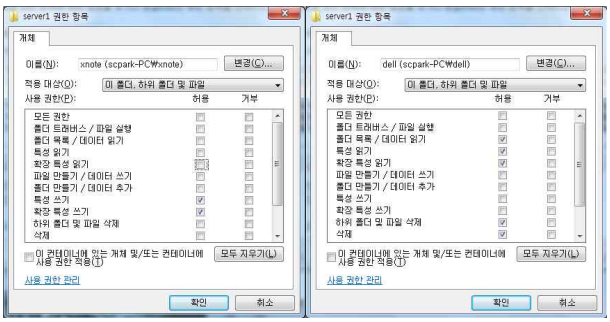

그림 18. 폴더 권한 상세 설정
Fig. 18. Detailed configuration of folder authority.

대로 2번 서버가 쓸 수 있고 1번 서버가 읽어 올 수 있는 공간이 된다. 각 폴더의 생성이 끝나면 생성된 폴더를 하나의 볼륨으로써 공유를 해야 하기 때문에 공유 설정을 해야 한다. 그림 17과 같이 폴더의 속성 수정을 통해 공유하도록 설정할 수 있는데 이때 공유 스토리지 내의 로그인 계정에 따라 기본적인 권한 설정까지 가능하다. 하지만 읽기, 쓰기와 같은 매우 기초적인 권한 설정만이 가능하기 때문에 더욱 심도 있는 권한의 설정을 위해서는 폴더 보안 설정 부분을 수정 해야만 한다. 그림 18은 server1 폴더에 대한 권한을 각 전송 통제 서버에 맞게 수정한 것으로 xnote라는 사용자는 폴더에 대해 오직 데이터를 쓰기만 할 수 있는 권한을 가지게 설정하였고 dell이라는 사용자는 데이터를 읽고 삭제만 할 수 있는 권한을 가지게 했음을 알 수 있다.

server2 폴더에 대한 권한 설정은 그림 18 의 권한을 반대로 설정하면 간단하게 구현된다. 이로써 공유 스토리지에 대한 구현 설정은 마무리 된다.

나. 전송 통제 서버 구현

전송 통제 서버의 구현은 위에서 구현했던 공유 스토리지의 각 폴더를 자신의 권한에 맞게 사용하도록 설정하는 것으로부터 시작된다. 일반적으로 공유 스토리지의 설정이 이상 없이 잘 되었다면 전송 통제 서버를 구현할 PC의 네트워크 환경 부분에 그림 19와 같이 공유 폴더가 화면상에 표시가 된다. 네트워크상의 공유 폴더로만 설정을 해놓을 경우 폴더 자체가 전송 통제 서버 입장에서 하나의 디스크 드라이브로 설정된 상태가 아님으로 데이터를 가져오는데 있어서 주기적으로 가져와야 하는 자동화 작업의 구현이 쉽지 않다. 따라서 네트워크 공유 폴더 자체를 하나의 디스크로 설정을 해야 한다. 이를 위해 각 네트워크 공유 폴더를 네트워크 드라이브로 따로 설정해주는 것이 필요하다.

그림 20은 윈도우 OS에서 기본적으로 제공해주는 네트워크 드라이브 연결로써 각 네트워크 공유 폴더나 공유 디스크를 하나의 디스크 드라이브로 인식시켜 사용

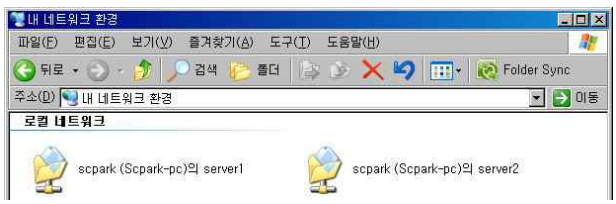

그림 19. 네트워크 공유 폴더
Fig. 19. Shared folder in network.

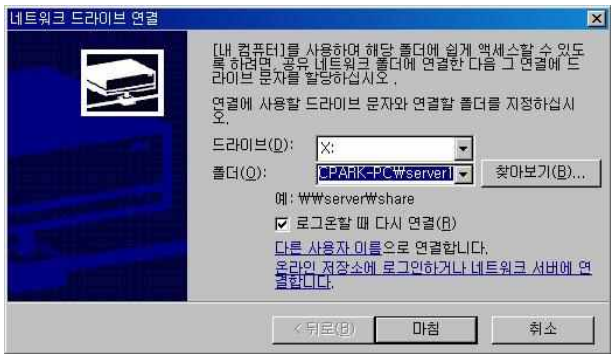

그림 20. 네트워크 드라이브 연결
Fig. 20. Connection to network drive.

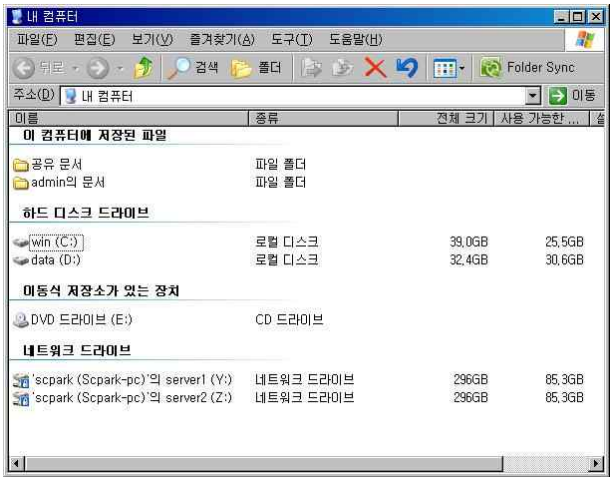

그림 21. 네트워크 드라이브 연결 완료
Fig. 21. Completion of connection to network drive.

함에 있어서 편의를 제공해주는 설정이다. 이 설정을 통해 server1과 server2 폴더를 드라이브로 인식시킨 결과가 그림 21에 나타나있다.

위와 같은 방법으로 두 개의 전송 통제 서버를 설정하면 기본적인 공유 스토리지를 이용한 망 연동의 구현이 완료된다. 공유 스토리지 내부의 두 개의 폴더를 두 대의 전송 통제 서버와 모두 공유하기 때문에 각 서버가 기록한 데이터를 다른 쪽의 서버에서 쉽게 가져올 수 있는 것이다. 하지만 현재 상태는 상대방 서버에서 전송하는 데이터를 수동으로 가져와야 하기 때문에 완전한 연동이라고는 볼 수 없다.

다. 주기적 데이터 전송

공유 스토리지를 이용한 망 연동의 기본동작 중 하나가 전송 통제 서버가 공유 스토리지에 주기적으로 접근하여 자신이 가져와야할 데이터가 있는지 확인하고 있을 경우 그 데이터를 가져오는 것이다. 또한 가져간 데이터가 공유 스토리지에 계속해서 남아있을 경우 공격자에 의해 남아있는 데이터가 유출 될 수 있기 때문에 데이터를 가져감과 동시에 삭제하는 작업도 수행해야 한다. 따라서 위에서 언급한 공유 스토리지와 전송 통제 서버의 구현은 기본적인 데이터의 왕래만이 구현된 상황이라고 볼 수 있다. 구현에 있어서 주기적으로 데이터가 있는지 확인하고 가져오기 위해 Second copy[5] 라는 툴을 사용하였다.

Second copy는 원래 데이터의 주기적인 백업을 위해 만들어진 툴이지만 설정에 따라 주기적으로 데이터를 가져오고 가져온 데이터에 대해 삭제하도록 하는 기능

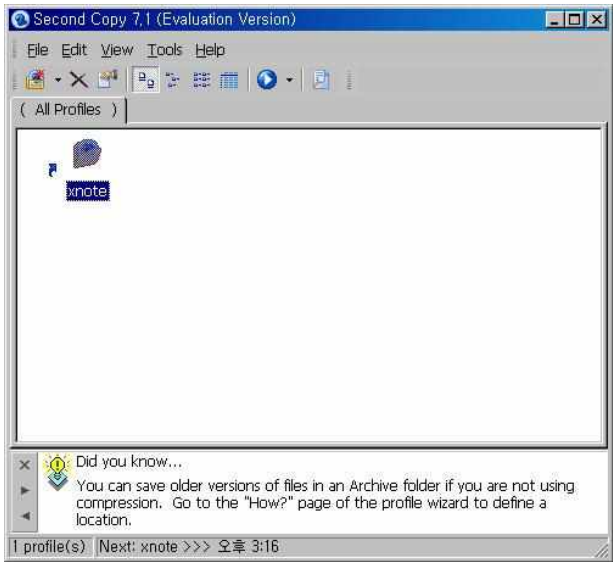

그림 22. Second copy 툴
Fig. 22. Second copy tool.

도 구현할 수 있다. 그림 22는 Second copy를 실행한 화면으로써 사용자가 데이터 백업에 대한 일정 및 각종 설정이 포함된 하나의 프로파일을 만들고 만들어진 프로파일을 계속적으로 반복하는 방식으로 작업이 진행된다. 따라서 프로파일을 만들시 가져올 폴더의 위치를 상대방 전송 통제 서버에서 데이터를 쓰는 네트워크 드라이브로 지정하고 전송 통제 서버의 디스크에 가져오도록 설정함으로써 공유 스토리지로부터 주기적으로 데이터를 가져오는 작업이 구현되는 것이다. 이러한 second copy를 각 전송 통제 서버에 설치하고 가져오는 위치를 상대방 전송 통제 서버가 쓰는 디스크 영역을 지정함으로써 구현이 가능하다.

라. 공유 스토리지 테스트베드 보안 강화

현재 구현된 망 연동 테스트베드는 분리된 망을 연동한다는 의미에서 강력한 보안을 제공하지만 그 외의 보안에 대한 어떠한 시스템도 설치되지 않았기 때문에 더욱 보안을 강화할 필요성이 있다. 악성 코드나 바이러스는 각 전송 통제 서버에 안티 바이러스 툴을 설치함으로써 막을 수 있고 접근 제한을 위해 공유 스토리지에 방화벽을 설치하고 방화벽으로 하여금 접근 통제 정책을 수행하게 함으로써 인가된 IP나 포트번호가 아니면 공유 스토리지에 접근조차 할 수 없게 해야 한다.

그림 23은 방화벽 중의 하나인 Comodo 방화벽을 설정한 것으로 각 전송 통제 서버의 주소인 192.168.1.3과 192.168.1.4를 제외한 어떤 접근도 허락하지 않는 정책

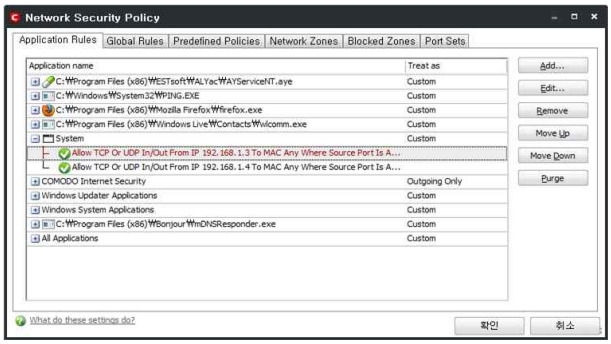

그림 23. 방화벽의 IP 필터링
Fig. 23. IP filtering of firewall.

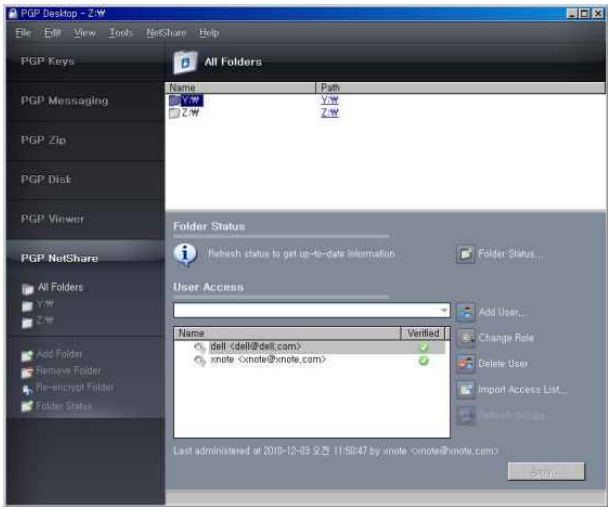

그림 24. 네트워크 드라이브 암호화
Fig. 24. Encryption of network drive.

을 보여준다. 또한 139번 포트만을 열어둠으로써 이중적인 필터링을 제공하게 된다.

공유 스토리지를 통해 전송되는 파일의 암호화는 PGP(pretty good privacy) 툴을 이용해 구현하였다. 그림 24 는 PGP를 사용하여 전송 통제 서버에서 네트워크 드라이브로 설정 해놓은 공유 폴더들에 대해 폴더 전체를 암호화해놓은 모습을 나타낸 것으로 네트워크 드라이브인 Y:\와 Z:\가 암호화되어 있음을 확인할 수 있다. 따라서 해당 드라이브에 전송되는 파일은 모두 미리 생성된 각 서버의 키를 통해 자동으로 암호화가 되며 해당 파일을 받은 상대방 전송 통제 서버에서는 자동으로 복호화 시켜 파일을 확인할 수 있다.

전체적인 암호화 전송의 과정은 그림 25와 같다. 각 전송 통제 서버는 사전에 나눠받은 두 개의 대칭키를 가지고 있고 server1에서 server2로 파일을 전송할 경우 1번 키를 통해 암호화, 복호화가 이루어지고 server2에서 server1로 파일을 전송할 경우 그 2번 키를 통해

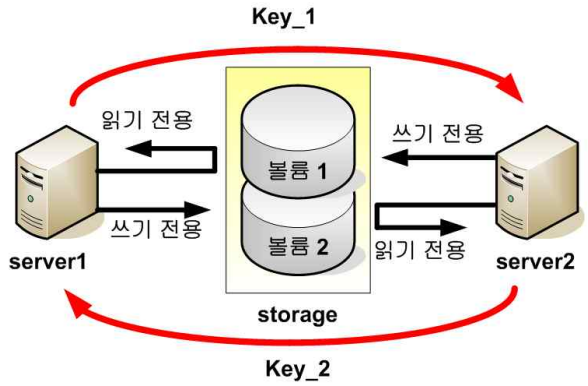

그림 25. 암호화 전송 과정
Fig. 25. Process of encrypted transmission.

그림 26. 평문의 암호화
Fig. 26. Encryption of plain text.

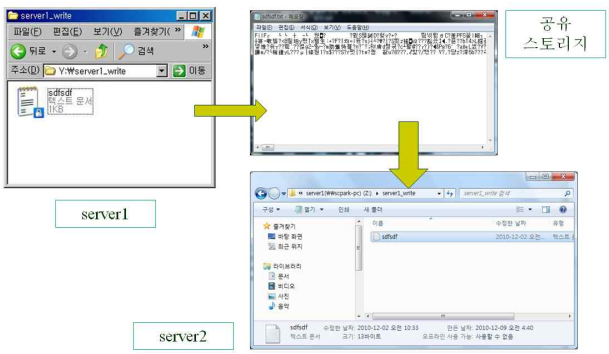

그림 27. server1에서 server2로 파일 전송
Fig. 27. File transmission from server1 to server2.

암호화, 복호화가 이루어진다. 암호화 알고리즘은 AES (Advanced Encryption Standard)[6]방식이 사용되며 알고리즘에 사용되는 키를 모를 경우 그림 26과 같이 평문에 대한 확인이 불가능하다. 또한 대칭키 두 개를 모르는 공격자의 경우에는 암호화된 폴더 자체에 진입조차 할 수 없다.

그림 27은 테스트를 위해 server1에서 네트워크 드라이브를 통해 파일을 전송한 것으로써 반대편 서버인

server2에서 마찬가지로 네트워크 드라이브를 통해 확인할 수 있음을 나타내고 있다.

V. 결 론

본 논문에서는 네트워크의 발전으로 인해 더욱 위협을 받게 된 국가나 회사 기관망의 보안 네트워크 구축 동향에 대해서 알아보았고 외부 네트워크와 내부 네트워크가 분리된 환경에서 각 망을 안전하게 연결할 수 있는 방법에 대해 제시하였다. 또한 제시된 연결 방법 중 NAT를 이용한 연결 방법과 공유 스토리지를 이용한 연결 방법에 대한 테스트베드를 구축하였고 그 안전성에 대해서도 검증하였다. 향후 공유 스토리지를 이용한 연결 방안에 웹 데이터나 FTP와 같은 응용 데이터를 교환하는 방안에 대한 구현 실험을 진행할 계획이다.

참 고 문 헌

[1] 행정안전부, 국가정보원, 한국정보사회진흥원, “국가기관 망 분리 구축 가이드”, 2008.05.
[2] K. Egevang, “The IP Network Address Translator (NAT)”, RFC1631, May 1994.
[3] firewall builder 개발사 홈페이지, http://www.fwbuilder.org
[4] nessus 홈페이지, http://www.nessus.org/
[5] Second copy 개발사 홈페이지, http://www.centered.com
[6] P. Chown, “Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)”, RFC3268, June 2002.

저 자 소 개

박 세 철(정회원)
2008년 충남대학교 전자전파정보통신공학과 학사
2008년～2011년 충남대 정보통신공학과 석사과정
2011년～한국항공우주연구원 저궤도위성관제팀 연구원
<주관심분야 : 컴퓨터 네트워크, 데이터 통신, NetFPGA 위성통신프로토콜>

장 인 식(학생회원)
2007년～2010년 충남대학교 전자전파정보통신공학 학사
2011년～현재 충남대학교 전자전파정보통신공학 석사 과정
<주관심분야 : 컴퓨터 네트워크, 데이터 통신, NetFPGA 위성통신프로토콜>

이 명 신(정회원)
1998년 전북대학교, 제어계측공학 학사
2009년 정보통신기술사
2010년 충남대학교, 정보통신공학 석사
1999년～현재 한국항공우주연구원 저궤도위성관제팀 선임연구원
<주관심분야 : 산업제어시스템 보안, 보안정책 관리, 위성지상시스템 설계>

정 대 원(정회원)
1992년 경북대학교, 전자공학과 학사
1994년 경북대학교, 전자공학과 석사
2007년 충남대학교, 전자공학과 박사
1995년～현재 한국항공우주연구원 저궤도위성관제팀장 책임연구원
2009년～현재 과학기술연합대학원대학교 부교수
2009년～현재 SpaceOps Committee 이사
2010년～현재 위성전파감시자문위원회 위원
<주관심분야 : 위성 시스템 엔지니어링, 위성 지상국 설계, 위성통신 간섭, 위성궤도결정, 위성임무운용>

이 재 용(평생회원)-교신저자
1988년 서울대학교 전자공학과 학사
1990년 한국과학기술원 전기 및 전자공학과 석사
1995년 한국과학기술원 전기 및 전자공학과 박사
1990년～1995년 디지콤 정보통신 연구소 선임연구원
1995년～현재 충남대학교 정보통신공학부 교수
<주관심분야 : 초고속통신, 네트워크 성능분석>

김 병 철(평생회원)
1988년 서울대학교 전자공학과 학사
1990년 한국과학기술원 전기 및 전자공학과 석사
1996년 한국과학기술원 전기 및 전자공학과 박사
1993년～1999년 삼성전자 CDMA 개발팀
1999년～현재 충남대학교 정보통신공학부 부교수
<주관심분야 : 이동인터넷, 이동통신 네트워크, 데이터통신>

현 대 환(정회원)
1998년 우송대학교 컴퓨터공학과 학사
2002년 국민대학교 정보통신공학 석사
2001년～현재 한국항공우주연구원 저궤도위성관제팀 선임기술원
<주관심분야 : 네트워크 엔지니어링, 산업제어시스템 보안, 정보보안, 클라우드 컴퓨팅>