패킷트레이서를 이용한 중소규모 병원 네트워크 인프라 구축

김동환 · 박남혁 · 김진덕

동의대학교

A Construction of Network Infrastructure for Small-size Hospital using Packet Tracer

Dong-hwan Kim · Nam-hyuk Park · Jin-Deog Kim

Dong-Eui University

E-mail: typedefmee@naver.com, jdk@deu.ac.kr

요 약

패킷트레이서는 라우터/스위치 등 네트워크 장비를 가상으로 구성하고 각 장비의 CONFIG를 세팅, 실습 할 수 있는 프로그램이다. 고객의 요구를 받아서 중소규모 네트워크의 보안설정을 추가하여 보다 높은 안정성과 효율성 있는 네트워크를 구성하고 고객의 정보를 DB서버에 저장하여 DB서버에 접근시 데이터를 불러 올수 있도록 한다.

이 논문에서는 중소규모 병원 네트워크 인프라 구축을 위한 방안을 제시한다. 부서별로 스위치를 한대씩 배치하고 외부기관은 멀티포인트 프레임릴레이를 설정하여 전용회선으로 만들어 사용한다. 각종개인정보가 들어있는 DB는 외부에 두고 보안기능을 넣어서 신뢰성을 향상시킨다. 단순히 네트워크 구축뿐만 아니라 DB를 연동하여 정보를 저장하고, 보안 기능을 넣어서 네트워크의 취약점을 보안하고자 한다.

키워드

패킷트레이서, 중소규모 네트워크, 데이터베이스, 보안기능

Ⅰ. 서 론

패킷트레이서는 PC환경에서 라우터/스위치 등 네트워크 장비를 가상으로 구성하고 각 장비의 설정을 통해 실습 할 수 있는 프로그램이다. 서버 또는 데스크탑 간의 100BASE-T 기술을 이용한 네트워크 기술이 보편화 되면서 대용량 파일전송이 증가 되었고, 기하 급수적으로 늘어나고 있는 데이터 트래픽에 비해 원활한 데이터 전송이 부족하였다. 실제 중소규모 병원 네트워크 인프라는 병원내의 통신기기 및 의료기기들의 증가와 의료기술의 발전에 따라 고속의 네트워킹 기술들이 요구되어지고 있다. 병원의 부서별로 네트워크를 연결하여 보다 효율적인 업무가 가능하다.

중소규모 병원 네트워크 인프라를 구축하면서 단순히 네트워크 구축뿐만 아니라 데이터베이스를 연동하여 각종 정보를 저장하고, 보안기능을 넣어서 네트워크의 취약점을 보안한다. 적용된 기술은 VLAN, 포트보안, ACL, 프레임릴레이, 동적 라우팅 이다. 본 논문에서는 외부에서의 침입을 막을수 있는 보안과 함께 효율적인 전송이 이루어질수 있는 방법에 대해 기술한다.

Ⅱ. 관련연구

병원 네트워크를 구축하기 위해서는 다양한 기술들이 사용되어 진다. VLAN[1]은 하나의 LAN안에서 스위치가 가상의 LAN을 나눔으로써 브로드캐스트 도메인을 분리시켜 주는 기술이다.

포트보안(Port security)[2]는 특정 포트에 학습할 수 있는 MAC주소의 수를 제한하여 허가된 MAC만 접속 가능하도록 설정하는 것으로 가장 기본적이면서도 다양한 공격을 막을 수 있는 효과적인 보안 설정이다.

그림1,2,3은 모의 해킹툴 Cain and Abel[3]인용 가상머신을 활용하여 ARP flooding attack에 대한 방어 실험 결과를 나타낸다.

그림2에나오는e0/0포트는mac-address가 “0800.27D1.6942” 가 아닌 다른mac-address가 접근하면 포트 자체를 shutdown 하도록 설정되어 있다. 그림3과 그림4를 보면 Cain and Adel에서 mac-address를 “0011.2233.4455” 로 변조하여 ARP 패킷을 보내자 e0/0 포트가 Shutdown 되어 더 이상 변조 된 패킷이 오지 않게 되었다. .

```
IOU1(config)#interface e0/0
IOU1(config-if)#switchport mode access
IOU1(config-if)#switchport port-security
IOU1(config-if)#switchport port-security maximum 1
IOU1(config-if)#switchport port-security mac-address 0800.27D1.6943
IOU1(config-if)#switchport port-security violation shutdown
```

그림 1.Port Security를 이용한 ARP flooding attack 보안 설정

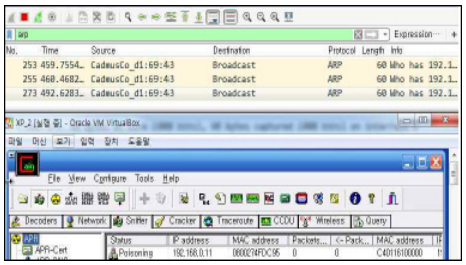

그림 2 ARP flooding attack과 Wire Shark를 통한 패킷 결과

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Et0/0	1	1	1	Shutdown

Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 4096

그림 3. ARP flooding attack에 대한 Port shutdown

ACL(Access Control list)[4]은 OS등의 보안 기능의 하나로, 파일 등 이용자의 액세스 권한을 열거한 목록이다. 파일이나 폴더(디렉토리)등 시스템 관리 개별 자원에 대해 각 이용자 나 이용자 그룹에 대해 어떠한 액세스를 허용할 것인지를 열거한 것을 의미한다.

프레임 릴레이[5]는 양단의 라우터가 직접 데이터를 전송하는 Point-to-Point 링크에 비해 효율적이고 유연한 WAN기술을 위해 개발된 2계층 프로토콜이다. 전용선을 이용할 경우에는 라우터에 독립적인 serial Interface를 설치해야 하며 물리적 회선이 필요하다. 하지만 프레임 릴레이는 하나의 물리적 회선을 통해 다수의 라우터에 통신을 가능하게 한다.

동적라우팅[6] 기술은 라우터가 네트워크 연결 상태를 스스로 파악하여 최적의 경로를 선택해 전송하는 방식이다. 동적라우팅은 네트워크 연결 형태가 변경되어도 자동으로 문제가 해결될 수 있다는 큰 장점이 있다.

Ⅲ. 병원 네트워크 시스템 구축

그림4는 패킷 트레이서를 이용한 병원 시스템 구축이다. 이에 적용한 기술에는 Subnetting, ACL, Dynamic Routing, Fram-Relay, DB보안이 있다.

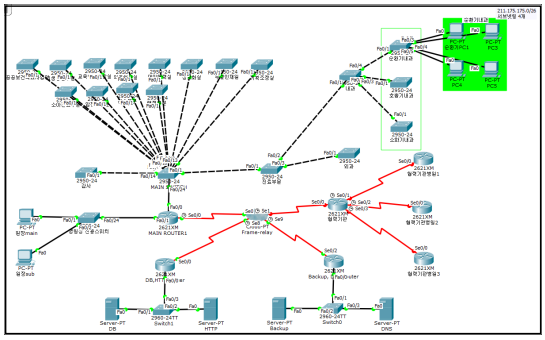

그림 4. 병원 네트워크 시스템 구축

그림5 Subnetting은 IP주소의 낭비와, 네트워크를 분리하여 보안성을 강화하기 위해 사용한다. 각 부서별로 필요한 주소를 할당하여 각각 네트워크주소를 다르게 설정한다.

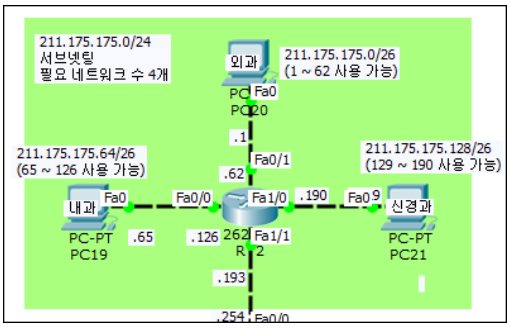

그림 5. 각 부서별 서브넷팅

ACL은 1개이상의 서브넷 내부와 외부의 트래픽을 제어하기 위한 방화벽 역할을 하는 기술이다. 외부나 내부로 통하는 라우터에 트래픽제어를 사용하여 HTTP, SSH, TCP, ICMP 등의 프로토콜 등을 제어 가능하다.

그림6는 HTTP서버로의 접근제어 방식이다. 외부에서 WEB접근만 가능하며, 나머지 모든 접근은 차단하였다. 단, 내부 사설대역의 네트워크는 모든 접근을 허용함을 보여주고 있다.

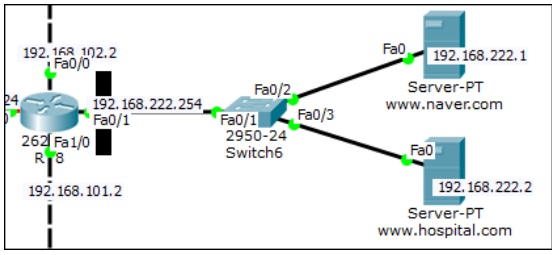

그림 6. HTTP서버로의 접근제어(ACL)

```
     1.0.0.0/24 is subnetted, 1 subnets
C       1.1.1.0 is directly connected, Serial0/3
     2.0.0.0/24 is subnetted, 1 subnets
R       2.1.1.0 [120/1] via 1.1.1.1, 00:00:23, Serial0/3
     100.0.0.0/24 is subnetted, 1 subnets
C       100.100.100.0 is directly connected, Serial0/0
     200.200.200.0/24 is variably subnetted, 3 subnets,
R       200.200.200.0/25 [120/3] via 1.1.1.1, 00:00:23,
R       200.200.200.128/26 [120/3] via 1.1.1.1, 00:00:23
R       200.200.200.192/27 [120/3] via 1.1.1.1, 00:00:23
     211.175.175.0/26 is subnetted, 4 subnets
R       211.175.175.0 [120/3] via 1.1.1.1, 00:00:23, Ser
R       211.175.175.64 [120/3] via 1.1.1.1, 00:00:23, Se
R       211.175.175.128 [120/3] via 1.1.1.1, 00:00:23, S
R       211.175.175.192 [120/2] via 1.1.1.1, 00:00:23, S
     211.175.176.0/28 is subnetted, 1 subnets
R       211.175.176.0 [120/2] via 1.1.1.1, 00:00:23, Ser
C    211.175.185.0/24 is directly connected, FastEtherne
```

그림 7. Dynamic routing 테이블 모습

그림7 Dynamic Routing은 RIP, OSPF, EIGRP 등이 있으며 패킷을 보내는 경로를 결정할 때 참조하는 경로 설정표를 동적으로 작성, 관리한다. 라우팅 테이블로 R로 보여지는 네트워크는 각 Dynamic Rounting으로 연결된 동적 네트워크를 뜻한다. 네트워크 형태가 변경되더라도 자동으로 문제가 해결될 수 있다.

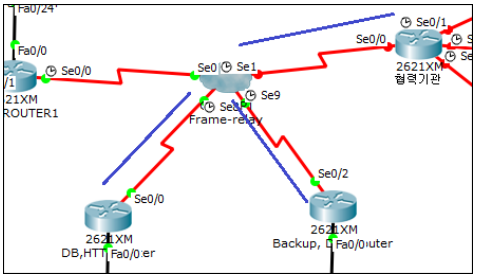

그림 7 Frame-relay 환경설정

그림8 Frame-Relay[7]은 전용회선 비용을 내지 않고서도, 전용선과 유사한 고정 가상회선(PVC)를 제공하며, 서비스 제공업체들은 목적지로 향하는 각 프레임들의 경로를 설정하고, 사용량에 따라 요금을 매길 수 있다. 또한 프레임들에 대해 서비스 품질(QoS)과 같은 우선순위를 할당하여 서비스를 제공할 수도 있다.

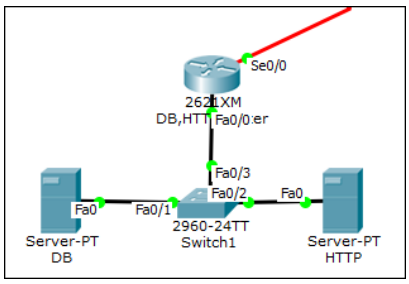

그림 8. DB보안 ZFW 적용

DB 보안 솔루션은 암호화 솔루션 및 접근제어 솔루션으로 나뉘며, 말 그대로 접근에 대한 감사 및 통제 목적의 솔루션이 DB접근제어 솔루션 인 반면, 접근 하더라도 중요 정보에 대해 조회가 불가능 하도록 DB 의 특정 칼럼에 암호화 를 적용하는 것이 DB 암호화 솔루션이다.

DB는 Oracle SQL을 사용하였으며, 사용자가 필요로 하는 정보를 요청받아 DB Server로부터 제공하고 있다. DB접근시 허용되지 않은 네트워크에서는 접근하지 못하도록 ZFW[8],ACL을 이용하여 보안성을 높인다. ZFW기술은 Inside, outside, dmz구역으로 나누어 내부 또는 외부로부터의 침입을 막고 내부 네트워크를 보호한다. DB다운시 Backup Server로 저장하여 데이터 손실 피해 또한 최소화 시킬수 있다.

Ⅳ. 결론

중소규모 네트워크를 다양한 보안과 함께 직접 구성을 해보았다. 기업 활동에서 IT에 대한 의존도가 높아짐에 관련해, 다른 많은 소프트웨어 및 하드웨어 플랫폼에서 제공하는 서비스들을 운영하게 되면서 네트워크 보안 시스템의 필요성도 높아져가고 있다.

데이터베이스 보안은 DB서버 구역을 dmz구역으로 나누어 외부로부터의 서비스를 제공하지만 외부에서의 침입으로부터 내부 네트워크를 보호하도록 하였다.

참고문헌 및 사이트

[1] https://docs.oracle.com/cd/E26925_01/html/E25835/ fpjve.html : VLAN
[2] http://bigsecurity.tistory.com/9 : port security
[3] http://techblog.j2.co.kr/index.php?document_srl=337&mid=upgletyle : Cain & Abel
[4] http://docs.aws.amazon.com/ko_kr/AmazonVPC/latest/UserGuide/VPC_ACLs.html : ACL
[5] http://blog.daum.net/_blog/BlogTypeView.do?blogid=0GCVJ&articleno=1764550&_bloghome_menu=recenttext - 프레임 릴레이
[6] http://bosungs2y.tistory.com/entry/Router-Dynamic-Routing - 동적 라우팅
[7] 정진욱, 김현철, 조강홍, 안성진 공저, Computer Network, 생능출판사, pp203, 2014
[8] http://byeong9935.tistory.com/3 : ZFW(Zone-Based Firewall)