IP 기반의 SAN 보안

윤철환, 류대현*, 김학영**, 전성택***

*한세대학교 IT학부

**ETRI 컴퓨터 소프트웨어 연구소 컴퓨터시스템연구부

***영산대학교 컴퓨터 정보공학부

IP Based SAN Security

Chul-Hwan Yoon, Hae-Hyun Ryu*

*Department of IT Hansei Univ.

Hag-Young Kim**

**ETRI, Computer & Software Laboratory,

Dept. of Computer System Research

Sungateg Jun***

***Dept. of Comp. Info. Eng., Youngsan Univ.

요 약

네트워크 저장장치가 새롭게 IT 인프라 구축방안중의 하나고 부각되고 있으며 그중에서도 SAN은 많은 장점을 갖고 있다. 본 논문에서는 SAN의 보안상의 취약점과 그 대응방안에 대한 연구동향을 검토하고, IP 기반의 SAN의 장점과 VPN을 이용한 보안에 대해 분석한다.

I. 서론

현재 기업 규모의 시스템에서는 데이터 웨어하우스(Data Warehouse)의 구축과 ERP(Enterprise Resource Planning) 시스템 등의 도입으로 대용량 스토리지에 대한 요구가 계속 높아지고 있으며, 인터넷의 폭발적인 성장, 온라인상에서의 정보유지 필요성, 의사결정 지원정보의 수집/추적에 대한 필요성, 서버 통합, 비즈니스 중심 어플리케이션으로의 PC 서버 움직임, 그리고 어플리케이션의 복잡성 증가 등 다양한 요인들도 이러한 요구를 부채질하고 있는 실정이다.

이러한 높은 신뢰성과 성능, 내장애성(fault tolerance), 그리고 통합된 관리와 고속 백업이라는 요구에 대한 솔루션으로 등장한 것이 바로 SAN(Storage Area Network)인데, SAN은 분산 네트워킹에서 주류가 되고 있으며 조만간 스토리지 부착 및 공유에 대한 일반적인 방법이 될 것으로 전망된다.

그러나 현재의 SAN 솔루션 공급은 스토리지 기능에만 치우쳐 있으며 데이터 보호에는 많은 관심을 기울이지 않고 있다. 이것은 향후 보안 문제를 야기할 가능성이 있으며 SAN의 Security에 많은 투자가 이뤄져야 할 것이다.

본 논문에서는 SAN의 보안상의 취약점과 그 대응방안에 대한 연구동향을 검토하고, IP 기반의 SAN의 장점과 VPN을 이용한 보안에 대해 분석한다. 본 논문의 구성은 다음과 같다. 2장에서는 SAN의 보안상의 취약점과 그 대응방안에 대한 연구동향을 검토, 3장에서는 SAN의 발전 방향과 IP 기반의 SAN과 보안문제를 고려해보고 4장에서는 결론을 제시한다.

II. SAN 보안

SAN 보안을 위해 고려해야할 사항은 여러 가지가 있을 수 있다. 우선 SAN에서는 다수의 사용자가 동일한 물리적인 디스크 공간에 중복해서 쓸 수가 다는 점 때문에 발생하는 문제점이 있다. 이는 LUN(Logical Unit Number)에 대한 보안 즉 마스킹(masking)과 구역화(Zoning)가 필요하다. 또한 허가되지 않거나(unauthorized) 인증되지

않은(unauthenticated) 접근, 안전하지 않은 관리자 접근(Insecure management access), WWN spoofing 그리고 다른 여러 access points에서 허용된 관리자 제어(management control) 등이 SAN 보안을 위해 고려해야할 사항이다.

LUN masking은 SAN을 논리적으로 재구성하여 SAN 가상풀(SAN virtual pool)을 구성하는 것으로 SAN의 일부분만을 접근할 수 있도록 동작하게 만든 것이다. 이렇게 함으로서 응용 서버는 사용허가를 받은 LUN에만 접근할 수 있다.

Zoning(Partitioning)은 스위치에서 주어진 Port로부터 특정 데이터로의 접근만을 허용함으로써 유사한 효과를 낼 수 있다. Zoning에는 다음과 같은 방법들이 있다.

- Zoning by host software
- Zoning by Host Bus Adapter Utilities
- Zoning by Fabric Switch
- Zoning by Storage Controller

그러나 LUN Masking이나 Zoning을 사용하더라도 보안상의 취약성을 완전히 제거할 수는 없다.

SAN은 많은 장점을 갖고 있으나 아래와 같은 문제점도 제기되고 있다.

- Interoperability between each products
- Lack of available skill for management
- High implementation costs
- Lack of management standards

이러한 문제점을 해결할 수 있는 기술로 Internet protocol(IP)에 기반한 SAN 기술이 부각되고 있다.

이러한 문제점 이외에 보안상의 문제점으로서 보안상 중요한 데이터가 링크로 지나갈 때 분석기로 링크를 훔쳐보거나(sniff) 취득(capture) 할 수 있다. 이 때문에 링크에 대한 비밀성(confidentiality)과 인증(authentication)이 요구되고 IP Security(IPsec) mechanism은 이러한 문제를 해결할 수 있다.

III. IP 기반의 SAN

1. IP based Storage

IETF 산하의 IP Storage 워킹 그룹에서는 SAN을 구현하기 위하여 IP 기술을 사용하는 것을 연구하고 있다.

(http://www.ietf.org/html.charters/ips-charter.html)

여기에는 두가지 접근방법이 있는데 하나는 tunneling이고 다른 하나는 Native IP based SAN이다. tunneling은 데이터를 다른 곳의 SAN으로 전송하기 위해 Fibre Channel frame을 IP packet으로 encapsulate하는 것이다. Native IP based SAN은 현재의 storage protocols(SCSI, Fibre Channel)을 IP protocol로 구현하는 것이다.

IP based Storage의 장점은 다음과 같다.

- Low implementation cost and operational cost
- easy for Remote data backup
- Numerous IP applications can be applied

2. Tunneling approach

Tunneling의 개념은 FC frame을 IP packet으로 encapsulate하고 이를 인터넷을 통해 원격지 SAN으로 전송하고 decapsulate한다는 것이다. 이 때 사용되는 프로토콜을 FCIP(Fibre Channel Over IP)라 하는데 이 방식의 목적은 IP를 사용하여, FC로 구성된 두 SAN을 연결하는 것이라 할 수 있다. 따라서 이 방식은 단지 두 SAN을 연결하는 용도(데이터 백업과 미리링 용도)로서 유용하나, FC의 interoperability and management problem은 그대로 존재하며, FC SAN에 비해 상대적으로 낮은 대역폭을 갖는다는 단점이 있다.

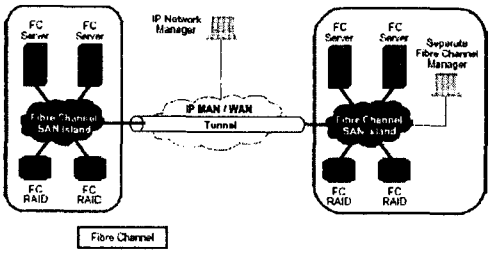

그림 1: Tunneling approach

3. Native IP-based SAN

이 방식은 IP가 SCSI Protocol을 전송하며 이 프로토콜을 iSCSI(Internet over SCSI)아라 한다. 이 방식에서 각 저장장치는 TCP layer에서 SCSI command을 포함하는 IP packet을 만들어 낸다.

이 방식의 목적은 FC를 사용하지 않고, IP와 Gbps이더넷으로 SAN을 구성하는 것이다. 이 방식을 구현하기 위해서는 1Gbps 또는 10Gbps 이더넷으로 Storage Device를 연결하고, 기존 SCSI/FC Storage Device에 IP Adaptation mechanism을 부착한 SAN 구성하거나 Native IP

Storage Device를 사용하여 SAN을 구성할 수 있다.

이 방식은 구현비용이 적게 들고, IP 응용을 사용한 통합관리가 가능하며, 관리를 위한 교육훈련 대한 부담이 적으며 기존의 SCSI 나 FC 저장장치를 사용할 수 있다는 장점이 있다.

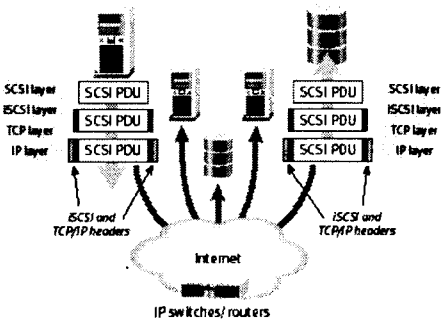

그림 2: Native IP-based SAN

IV. IP 기반의 SAN 보안 : VPN

1. VPN 개요

SAN이 기존 IP 네트워크에 연결될 경우에 기존 TCP/IP의 취약성을 대부분 그대로 갖고 있으므로 Security는 매우 중요하다 특히 SAN이 인터넷에 연결될 경우, 인터넷의 위협에 노출될 수 있다. 이러한 경우 VPN (Virtual Private Network : 가상 사설망)이 그 보안 해결책이 될 될 수 있다.

VPN은 공중 데이터 통신망을 마치 자체적으로 설치한 사설망과 같이 사용할 수 있도록하는 기술이다. 이 기술을 사용하여 공중 인터넷을 이용하여 저렴한 비용으로 사설망을 구축할 수 있으며, 암호화 알고리즘을 이용하여 데이터의 기밀성을 유지할 수 있다.

VPN의 동작은 먼저 IKE 프로토콜로 두 VPN Gateway간 암호화 터널 형성하고, 네트워크 내부에서 발생한 IP패킷을 VPN Gateway가 암호화하여 IPSEC패킷 전송하며, VPN Gateway가 수신한 IPSEC패킷을 복호화하여 IP패킷 전송하는 순서로 이루어진다.

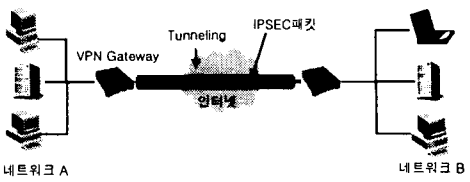

그림 3 : VPN 개념

IKE(Internet Key Exchange) 프로토콜은 VPN Gateway가 서로 상대방을 인증하고 IPSEC 프로토콜에 필요한 암호화 키를 주기적으로 생성하는데 다음과 같은 과정으로 이루어 진다.

1) 공개키 알고리즘을 사용한 상호 인증 (RSA-SIG, PSK)

2) Phase 1과 Phase 2를 순차적으로 수행하여 키 생성

- Phase 1(Main Mode) : 인증 단계를 수행하여 ISAKMP tunnel을 형성

- Phase 2(Quick Mode) : 암호화 패킷으로 통신하며, IPSEC tunnel을 형성

IPSEC(IP Security) 프로토콜은 암호화 알고리즘과 해쉬 알고리즘을 이용하여 Confidentiality, authentication, integrity, anti-replay 기능을 제공하며 AH(Authentication Header) protocol과 ESP(Encapsulated Security Payload), Tunnel mode와 transport mode로 구분된다.

1) AH protocol : 해쉬 알고리즘을 이용하여 패킷 인증(authentication), 무결성(integrity) 기능을 제공

2) ESP(Encapsulated Security Payload) protocol : 암호화 알고리즘과 해쉬알고리즘을 이용하여 데이터의 기밀성(Confidentiality)과 패킷 인증(authentication) 기능 제공

3) Tunnel mode와 transport mode

- Tunnel mode : IP 패킷을 IPSEC Header와 New IP Header로 캡슐화하여 IPSEC 패킷 생성(host-net, net-net, host-host통신에 사용)

- Transport mode : IP헤더와 IP데이터 사이에 IPSEC Header를 삽입하여 IPSEC 패킷 생성(host-host간 통신에 사용)

2. IP Based SAN에 VPN의 적용

Tunneling SAN에 VPN을 적용한다는 것은 FC frame을 캡슐화한 IP Packet에 IPSEC을 적용한다는 것이다. 즉 인터넷으로 두 SAN을 연결 시, VPN을 적용함으로서 IPSEC의 confidentiality, authentication, integrity 기능을 제공하게 된다.

Native IP Based SAN에서는 iSCSI 패킷에

IPSEC을 적용함으로서 VPN을 구현하게 된다. 즉인터넷으로 두 SAN을 연결시 VPN을 적용함으로서 IP Device에서 iSCSI 패킷을 IPSEC화하여 SAN 내부에서 기밀성 제공하게 된다. 이를 위하여 IP Device내에 IPSEC 기능 구현이 필요하게되고 암호 연산에 의한 Storage와 Server의 성능 지하될 수 있다. 따라서 H/W 암호 가속기를 사용한 성능 향상이 요구되며 IP Device에 별도의 VPN Gateway부착할 수도 있다.

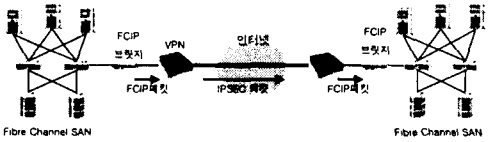

그림 4: IP Based SAN에 VPN의 적용

V. 결론

기존의 SAN에서 보안 위협 요소는 대부분 SAN 내부에 존재하며, storage공유로 인한 LUN Security Problem 발생한다. 이러한 문제는 LUN masking, zoning 보안 방법 적용을 적용하여 해결할 수 있으나 전송시의 기밀성 유지 불가등의 보안 문제는 여전히 존재한다.

IP 기술을 적용한 SAN은 관리의 편의성 등으로 부각되고 있으나 TCP/IP 자체의 취약성으로 인해 인터넷으로 연결 시, 외부에서 접근이 용이하다는 등 보안상의 문제점이 존재한다. 그러나 이러한 문제는 VPN기술을 적용하여, 데이터의 confidentiality, authentication, anti-replay, authorization 기능 제공하는 방법으로 해결될 수 있다.

본 논문에서는 SAN의 보안상의 취약점과 그 대응방안에 대한 연구동향을 검토하고, IP 기반의 SAN의 장점과 VPN을 이용한 보안에 대해 분석하였다.

그러나 SAN 보안을 위해서는 기술적인 문제이외에 신뢰성 있는 인원 배치라든지 신중한 보안정책 수립 Application Server 자체의 보안 관리 등 기본적인 요구사항에 충실할 필요가 있다.

참고문헌

[1] Dave Tang, "Storage Area Networking-The Networking Behind the Server", 1997, Gadzoox Microsystems. Inc

[3] Hu Yoshida, "LUN Security Considerations for Storage Area Networks", 1999, HITACHI Data Systems Corporation.

[5] 신범주, "네트워크 자료 저장 시스템 연구동향", 2001

[6] Dan McConnell, "IP Storage: A Technical Overview"

[9] "Storage over Internet Protocol-SoIP : The Next Generation SAN", Nishan Systems, 2000

[10] 손재기, 김영환, 박창원, "IP 기반 저장장치 기술", 2002, 춘계 자료저장시스템 학술대회논문집

[11] 김광혁, 이상도, 정태명, "SAN 취약성 분석 및 대응 방안" 2002, 정보과학회 춘계학술발표대회