AHP를 이용한 NAS 연동형 망분리 시스템에 관한 연구★

김민수* · 신상일* · 이동휘** · 김귀남***

요 약

국가 공공기관이나 기업에서는 질 높은 서비스를 제공하기 위하여 인테넷 망을 통해 정보 및 자료를 제공하고 있다. 하지만 자료의 송수신간에 악성코드 감염에 노출되어 각종 보안위협에 노출되게 된다. 이러한 이유로 2008년부터 국가 기관의 망 분리 사업이 진행되고 있고, 망 분리 기술로 망 연계 스토리지를 이용하여 물리적 망 분리와 더불어 데이터 연동을 하게 된다. 하지만 망 연계 스토리지는 동일 데이터가 내부 망 스토리지와 외부 망 스토리지에 각각 존재하게 되어 자원의 낭비와 더불어 데이터 관리에 문제점을 가지게 된다. 따라서, 본 연구는 물리적 망 분리의 한계점을 극복하기 위한 방안으로, NAS 스토리지를 이용한 내외부망 데이터 연계 방안을 제안하고, 망 분리 최적화를 위한 항목의 우선순위를 AHP기법을 통하여 검증하고자 한다.

A Study on NAS-Linked Network Separation System Using AHP

Min Su Kim* · Sang Il Shin* · Dong Hwi Lee** · Kui Nam J. Kim***

ABSTRACT

To provide high-quality services, national public institutions and companies have provided information and materials over the internet network. However, a risk of malware infection between transmission and reception of data leads to exposure to various security threats. For this reason, national institutions have proceeded with projects for network separation since 2008, and data linkage has been made using network connection storage through network separation technologies, along with physical network separation. However, the network connection storage has caused waste of resources and problems with data management due to the presence of the same data in internal network storage and external network storage. In this regard, this study proposes a method to connect internal and external network data using NAS storage as a way to overcome the limitations of physical network separation, and attempts to verify the priority of items for the optimization of network separation by means of AHP techniques.

Key words : DAS, SAN, NAS, NFS, AHP

접수일(2013년 6월 4일), 수정일(1차: 2013년 6월 16일), 게재확정일(2013년 6월 20일)

★ 본 연구는 2013학년도 경기대학교 대학원 연구원장학생 장학금 지원에 의하여 수행되었음.

* 경기대학교 산업보안학과
** 경기대학교 산업보안학과 (교신저자)
*** 경기대학교 융합보안학과

1. 서 론

국가 공공기관이나 기업에서는 질 높은 서비스를 제공하기 위하여 인터넷망을 통해 정보 및 자료를 제공하고 있다. 그러나 업무 망과 인터넷 간 자료를 송수신하는 과정에서 악성코드에 감염되어 발생되는 정보유출, 시스템다운 및 사이트 및 망 마비 등과 같은 보안위협의 가능성에 대한 대책이 필요하다. 이러한 이유로 2008년부터 국가 기관의 망 분리 사업이 진행되고 있다[1].

망 분리 기술은 물리적으로 내부 망과 외부 망을 이중으로 분리하는 물리적 망 분리와, 가상화 기술을 이용하는 논리적 망 분리로 구분되어 진다. 망 분리는 그 의미와 부합되게 내부 망과 외부 망을 물리적으로 완전히 분리되어야 하지만, 특정 데이터는 내·외부에서 모두 사용해야 하는 경우에 부득이 내부 망과 외부 망을 연동해야 하는 문제점이 발생하게 된다. 일반적으로 내·외부망의 연동은 중간에 연계 방화벽을 사용하여 구현하지만, 새로운 해킹 기법이 속속 출현하고 있는 상황에서 현실적으로 완벽히 방어하는 것은 어려운 만큼, 물리적으로 망이 연결되어 있는 경우 취약점이 생길 수밖에 없는 한계점을 가지고 있다. 이러한 취약점을 극복하기 위해 일부 정부 부처에서는 망 연계 스토리지라는 기법을 사용하고 있다. 이 기법은 연계 방화벽을 통한 데이터 연동에 비해 보안성은 우수하지만, 동일 데이터가 내부 망 스토리지와 외부 망(망 연계) 스토리지에 각각 존재하게 되어 자원의 낭비를 초래하고, 내부 망의 데이터 변경 시 망 연계 스토리지도 변경해주어야 하는 데이터 관리의 문제점을 가지고 있다.

따라서, 본 연구는 물리적 망 분리의 한계점을 극복하기 위한 방안으로, 공공기관에서 논리적 망 분리로 NAS 스토리지를 이용한 내외부망 데이터 연계 방안을 제안하고, 망 분리 최적화를 위한 항목의 우선순위를 AHP기법을 통하여 검증하고자 한다.

2. 관련연구

네트워크 기반의 대용량 저장 장치는 연결 형태에 따라, DAS(Direct Attached Storage), NAS(Network Attached Storage), SAN(Storage Area Network)로 구분할 수 있다[2][3][4][5]. SAN은 스토리지에 대한 고속 액세스 및 공유를 목적으로 하는 네트워크로, 디스크를 통합하여 관리하기 때문에 백업(Backup), 데이터의 보안등의 관리하는데 발생할 수 있는 문제를 해결해 줄 수 있는 최선의 방안으로 인식되고 있다[6][7][8][9]. 하지만 SAN 기법은 연계 방화벽을 통한 데이터 연동에 비해 보안성은 우수하지만, 자원의 낭비 및 관리적 문제점을 가지고 있다. NAS는 파일 서버 기능이 내장된 네트워크 저장 장치로[10], SAN에서 가지는 문제점인 자원의 낭비를 NFS(Network File System)을 이용하므로 관리적 문제점을 해결할 수 있다.

본 연구에서 망 분리 기술의 적용은 NAS와 SAN으로 한정하여 각 기술을 적용 시 나타날 수 있는 장단점을 비교하여 보고, AHP 기법을 이용하여 보안 전문가 10인의 의견을 상대비교 행렬을 이용하여 가중치를 산출하고, 산출된 값을 통해 일관성 비율과 타당도를 분석할 것이다. AHP 기법은 T. L. Satty(1980)에 의해 제안된 AHP 기법은 복잡한 의사결정(decision problem)을 조직화하고 분석하는 구조화된 기술이다[11][12].

$$A=\begin{Bmatrix} W_1/W_1 & W_1/W_2 & \cdots & W_1/W_n \\ W_2/W_1 & W_2/W_2 & \cdots & W_2/W_n \\ \vdots & & & \vdots \\ W_n/W_1 & W_n/W_2 & \cdots & W_n/W_n \end{Bmatrix} \quad (1)$$

행렬 A의 일관성의 정도가 클수록 λmax 는 n에 가까워지며, 이러한 특성을 이용하여 일관성 지수(Consistency Index : CI)를 다음의 식을 통해 구할 수 있다[13][14][15][16].

$$\text{일관성 지수 : } CI=(\lambda max - n)/(n-1) \quad (2)$$

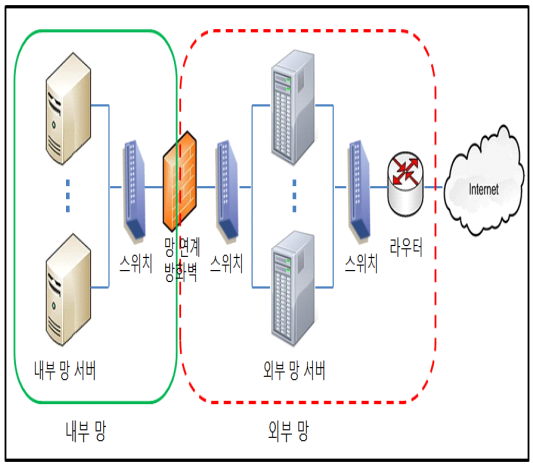
일관성 지수와 경험적 자료로 얻어진 평균 무작위 지수(random index : RI)의 비율을 일관성 비율이라 하고, 10% 이내인 경우에 가중치에 무리가 없는 신뢰할 수 있는 결과라 할 수 있다.

3. 제안하는 방법

네트워크 기반의 대용량 저장 장치의 각 형태에 대하여 알아보고, 본 논문의 제한적인 연구로서 공공기관에서의 NAS 스토리지 연동방안을 제안한다.

3.1 망 연계(DAS) 방화벽을 사용한 연동

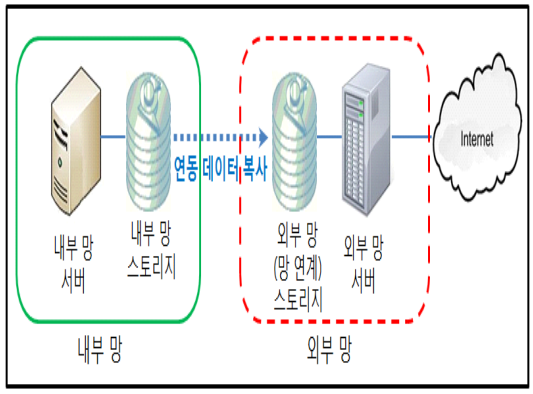
일반적인 망 연계(DAS) 방화벽을 사용할 경우는 (그림 1)과 같은 물리적으로 망이 연결된 구조를 이루게 되고, 이때 외부 망에서 내부 망으로 혹은 내부 망에서 외부 방으로의 보안 위협에 노출되게 되는 문제점이 발생하게 된다.



(그림 1) 망 연계(DAS) 방화벽 연동

3.2 망 연계 스토리지(SAN)를 사용한 연동

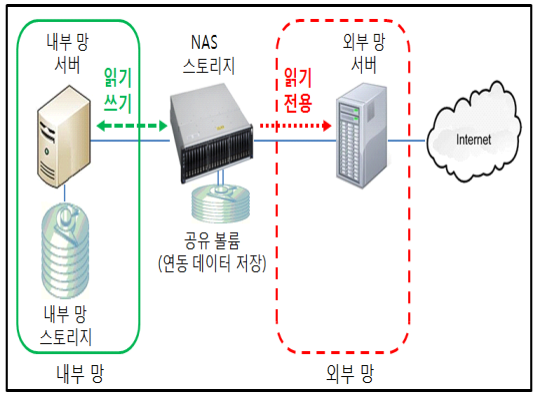
망 연계 스토리지(SAN)를 사용하여 연동하는 경우 (그림 2)와 같은 구조를 이루게 되고, 외부 망과 내부 망을 논리적으로 분리하여 내부 망의 데이터의 변경 시 연동 데이터를 복사하여, 외부망에 저장하는 과정을 거쳐야 한다. 이는 망 연계 방화벽(DAS)을 사용한 경우에 비해 내부 망 스토리지와 외부 망(망 연계) 스토리지에 각각 존재하게 되어 논리적으로 망 연계가 되어 보안성은 우수하지만, 데이터의 이중 저장으로 인한 자원의 낭비 및 데이터 변경에 따른 관리적 문제점이 발생하게 된다.



(그림 2) 망 연계 스토리지(SAN) 연동

3.3 NAS 스토리지를 사용한 연동

(그림 3)은 본 연구에서 제안된 구조로 연동될 모든 데이터는 NAS 스토리지의 공유 볼륨에 저장되고, 내·외부 망 서버는 NFS(Network File System)를 이용하여 해당 볼륨을 마운트 하게 된다. 보안성을 확보하기 위해 읽기/쓰기 권한은 NAS에 연결된 내부 망 서버에만 주어지고, 외부 망 서버는 해킹에 의한 데이터 위변조를 막기 위해 읽기 권한만 부여한다.



(그림 3) NAS 스토리지 연동

제안된 구조는 물리적으로는 망이 연동된 것처럼 보이나 NAS 스토리지는 공유 볼륨에 대한 접근 정책 등의 보안 설정을 할 수 있으며, NFS 서비스 외에는 다른 서비스를 하지 않으므로 논리적으로 망이 차단되어 실질적인 망 분리 효과를 얻을 수 있다.

이처럼 제안된 구조를 사용하면 망 분리의 효과뿐만 아니라 중복 데이터로 인한 자원 낭비와 효율적인 데이터 관리가 가능하다.

4. 논리적 망 구분 최적화 비교검증

본 연구를 위해 보안 전문가들을 대상으로 논리적 망 구분의 최적화에 대하여 설문 및 설문 분석을 통한 평가요소들을 계층화하였다.

4.1 비교검증을 위한 설문지 작성

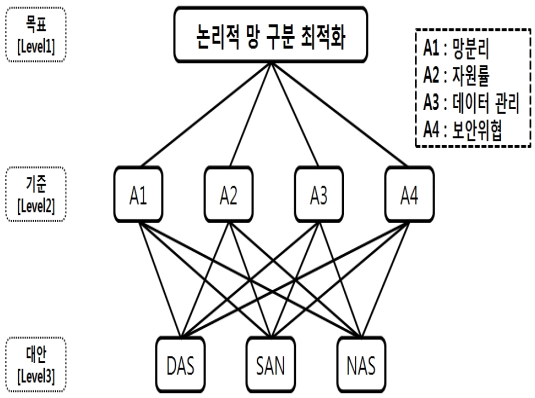
상대비교 행렬은 응답자의 상대비교 값을 이용하여 응답한 것으로, 두 평가요소의 상대적 합리성 정도를 17개의 값(9, 8, 7, 6, 5, 4, 3, 2, 1, 1/2, 1/3, 1/4, 1/5, 1/6, 1/7, 1/8, 1/9) 중 하나로 평가하게 된다. <표 1>은 설문지의 샘플로서 평가에 대한 특성을 세분화하여 4가지의 대분류 항목으로 구성되었다.

<표 1> 설문지 샘플

얼마나 더 합리적인가 평가하시오.(9, 8…1/8, 1/9)	망분리	자원률	데이터 관리	보안 위협
망분리	1			
자원률	X	1		
데이터 관리	X	X	1	
보안 위협	X	X	X	1

4.2 논리적 망 구분 최적화의 계층구조

(그림 4)는 논리적 망 구분 최적화 계층구조로써 목표(Level 1)인 논리적 망 구분 최적화를 검증하기 위하여 기준(Level 2)의 항목으로 망분리, 자원률, 데이터 관리, 보안위협의 요소로, 대안(Level 3)의 항목으로는 DAS, SAN, NAS로 구성되었다.



(그림 4) 논리적 망 구분 최적화 계층구조

4.3 비교검증 결과

4.3.1 설문 응답자의 일관성 비율

<표 2>는 논리적 망 구분 최적화 요소(망분리, 자원률, 데이터 관리, 보안위협)에 대한 상대 합리성 평가의 상대비교 행렬로부터 얻어진 최대 고유치와 일관성지수, 일관성 비율을 정리한 것이다. 응답자의 일관성 비율이 0.1 미만으로 모두 평가에 대한 일관성을 나타내고 있다.

<표 2> 설문 응답자의 일관성 비율

응답자	최대 고유치 λ_{max}	일관성지수 CI	일관성 비율 CR(%)
1	5.355	0.452	0.502
2	4.894	0.298	0.331
3	5.155	0.385	0.428
4	5.573	0.524	0.582
5	5.052	0.351	0.390
6	5.155	0.385	0.428
7	5.073	0.358	0.397
8	5.927	0.642	0.714
9	4.697	0.232	0.258
10	5.373	0.458	0.508

4.3.2 타당도 분석 결과

<표 3>의 최대 고유치 는 2.187이고, 일관성 지수는 0.604, 일관성 비율은 0.671%(10%미만)로 그룹 전체가 평가의 일관성을 유지하고 있음을 알 수 있다.

그리고 4개의 요소 중 망 분리(0.274) 항목이 가장 높게 나타나, 논리적 망 구분의 최적화를 위하여 망 분리가 우선순위로 나타났다. 그 뒤로 보안위협(0.272), 데이터관리(0.235), 자원률(0.219)의 순으로 나타났다.

<표 3> 평가요소 타당도 분석 결과

	망분리	자원률	데이터 관리	보안위협	결과
망분리	1	1.214	1.214	1	0.274
자원률	0.823	1	0.851	0.851	0.219
데이터 관리	0.823	1.174	1	0.823	0.235
보안위협	1	1.174	1.214	1	0.272
λ_{max} = 2.187 C.I (일관성 지수) = 0.604 C.R (일관성 비율) = 0.671					

5. 결 론

본 연구는 물리적 망 구분의 한계점을 극복하기 위한 방안으로, NAS 스토리지를 이용한 내외부망 데이터 연계 방안을 제안하였다. 제안된 구조는 물리적으로는 망이 연동된 것처럼 보이나 NAS 스토리지는 공유 볼륨에 대한 접근 정책 등의 보안 설정을 할 수 있으며, NFS 서비스 외에는 다른 서비스를 하지 않으므로 논리적으로 망이 차단되어 실질적인 망 분리 효과를 얻을 수 있다. 읽기/쓰기 권한은 DAS에 연결된 내부 망 서버에만 주어지고, 외부망 서버는 해킹에 의한 데이터 위변조를 막기 위해 읽기 권한만 부여하여, 보안위협으로부터 데이터를 보호하게 된다.

또한 제안된 구조를 사용하면 망 분리의 효과뿐만 아니라 중복 데이터로 인한 자원 낭비와 효율적인 데이터 관리가 가능하다. 이러한 NAS의 논리적 망 구분의 최적화를 위한 요소에 대한 우선순위를 AHP 기법을 통하여 검증한 결과 망 분리(0.274), 보안위협(0.272), 데이터관리(0.235), 자원률(0.219)의 순으로 나타났다. 즉, 보안 전문가들의 의견은 물리적 혹은 논리적 망 구분이 우선 시 되어야 보안위협으로부터 데이터를 보호할 수 있고, 이후 데이터의 효율적 관리와 중복 데이터 저장에 대한 기준을 제시하였다.

참고문헌

[1] 국가정보원, “2009 국가정보보호백서”, pp.66-67, 2009.

[2] 탁병철, 정연돈, 김명호, “대용량 공유 분산 파일 시스템에서 망 분할 시 순환 리스를 사용한 고장 감내성 향상”, 한국정보과학회, Vol.32, No.6, pp.616-628, 2005.

[3] Curtis, P. W, "Using SANs and NAS", O'Reilly, Cambridge, U.S.A, 2002.

[4] Gibson, G. A, R. V. Meter, "Network Attached Storage Architecture", Communications of the ACM, Vol.43, No.11, pp.37-45, 2000.

[5] 이원복, 박진원, “Group Master Cache를 활용한 SAN과 NAS의 통합 방안”, 한국시뮬레이션학회, Vol.16, No.2, pp.9-15, 2007.

[6] 김광혁, 이상도, 정태명, “SAN의 취약성 분석 및 대응방안”, 한국정보과학회, Vol.29, No.1A, pp.841-843, 2002.

[7] 황규진, 조율제, 김선일, “IEEE 1394로 구성된 Storage Area Network(SAN)의 성능평가”, 한국정보과학회, Vol.30, No.2, pp.655-657, 2003.

[8] Marc Farley, "Building Storage Networks", McGraw-Hill, 2000.

[9] 남상수, 피준일, 송석일, 유재수, 최영희, 이병엽, “SAN 논리볼륨 관리자를 위한 혼합 매핑 기법”, 한국정보과학회, Vol.9, No.6, pp.718-731, 2003.

[10] 김영신, 허의남, 권혁빈, 오채수, 최상현, “NAS에서 병렬 전송을 이용한 원격 미러링 시스템 설계”, 한국인터넷정보학회, Vol.6, No.2, pp.487-490, 2005.
[11] T. L. Saaty, The Analytic Hierachy Process, mcGraw Hill, New York, 1980.
[12] 성기훈, 공희경, 김태한, “AHP를 이용한 SNS 정보보호 위협요인 분석”, 한국정보보호학회, Vol.20, No.6, pp.261-270, 2010.
[13] 김태성, 전효정, “AHP를 이용한 정보보호인력 양성 정책 분석”, 한국통신학회, Vol.31, No.5B, pp.486-493, 2006.
[14] 최상현, 김진욱, 한관희, “정량적·정성적 평가치 적용을 위한 Hybrid-AHP 시스템 개발 및 응용”, 한국경영과학회, Vol.2010, No.10, pp.689-697, 2010.
[15] 강구홍, 강동호, 나중찬, 김익균, “계층분석과정을 이용한 융합보안을 위한 물리 보안 이벤트 활용 : 정보 보안 중심”, 한국정보보호학회, Vol.22, No.3, pp.553-564, 2012.
[16] 김현우, “전자상거래를 위한 보안 항목 우선순위 분석 : 연구자그룹과 실무자그룹을 중심으로”, 한국산업정보학회, Vol.16, No.5, pp.163-171, 2011.

[저 자 소 개]

김 민 수 (Min-Su Kim)

2004년 컴퓨터공학사
2012년 경호안전학석사
2013년 현재 경기대학교
산업보안학과 박사과정

email : fortcom@hanmail.net

신 상 일 (Sang-Il Shin)

2004년 컴퓨터공학사
2007년 컴퓨터공학석사
2013년 현재 경기대학교
산업보안학과 박사과정

email : sishin69@hanmail.net

이 동 휘 (DongHwi Lee)

2000년 경기대학교 컴퓨터과학과
(이학사)
2003년 경기대학교 정보보호기술공학과
(공학석사)
2006년 경기대학교 정보보호학과
(정보보호학박사)
2011년~2012년 5월 University of Colorado Denver, Dept. of Computer Science and Engineering
현재 경기대학교 산업보안학과

email : dhclub@naver.com

김 귀 남 (Kuinam J. Kim)

미국 캔자스대학(학사)
미국 콜로라도주립대학(석사)
미국 콜로라도주립대학(박사)
현재 경기대학교 융합보안학과 교수

email : harap123@daum.net