Journal of Digital Contents Society Vol. 8 No. 4 Dec. 2007(pp. 483-489)

차세대통신망(NGN) Infrastructure에서의 정보보호시스템 고가용성 차단구조 설계

노시춘*, 방기천**

요 약

NGN인프라 환경에서의 정보보호시스템 고가용성 구조는 정보보호 인프라스트럭쳐에 우선적으로 적용되어야 한다. 왜냐하면 NGN 환경의 정보시스템 상에서는 접속점의 다원화와 접속기술의 다양성으로 인하여 정보보호에 위배되는 침입 발생가능성이 현저하게 높아짐으로 인하여 매 순간마다 더욱 정밀한 침입차단 장치와 기능이 요구되기 때문이다. NGN인프라 환경에서 정보보호 고가용성 기능 확보는 정보시템 보안을 위한 선결과제로서 정보보호 인프라스트럭 구조와 기능 재설계를 통해 보증될 수 있다. 정보보호 인프라스트럭쳐 시스템상의 active-active 고가용성 구조는 정보시스템 운용구조상에서 구조설계와 기능상 failover 메커니즘을 구현하므로서 확보된다. 본 연구에서 제안한 정보보호고가용성 인프라 구조를 적용할 경우 트러블패킷에 의한 시스템오버로드를 감소시키고 SNMP polling trap 과 ICMP transport factor 소통을 향상시키고 있음이 실험을 통해 검증 되었다.

A Building Method of High Availability Protection Architecture in Next Generation Network (NGN) Information Security System

Si-Choon Noh*, Kee-Chun Bang**

Abstract

The high availability of information security system shall be primarily studied in relation to the Next Generation Network(NGN) Information Security infrastructure, because it is very important to maintain availability at each moment as a variety of intrusions occur continuously.The high availability of the security system can be realized with the topology and configuration properly defined to fully utilize the recovery function of the security system in the thoroughly planned optimized method. The active-active high availability on the NGN information security infrastructure systemin is assured by letting the failover mechanism operate upon the entire structure through the structural design and the implementation of functions. The proposed method reduces the system overload rating due to trouble packets and improves the status of connection by SNMP polling trap and the ICMP transport factor by ping packet

Keywords : NGN, high availability, security infrastructure

1. 서론

고가용성이란 하드웨어나 소프트웨어 장애에 불구하고 사용자가 특정 애플리케이션이나 디바이스를 지속적으로 사용할 수 있도록 고안한 컴퓨터 시스템기능을 의미한다. NGN인프라 환경의 정보시스템 상에는 네트워크 접속점의 다원화와 접속기술의 다양성으로 인하여 정보보호에 위배 되는 침입 발생가능성이 현저하게 높아지는 상황에 직면하게 된다. 따라서 매 순간마다 더욱 정밀한 침입차단을 위한 장치가 요구되며 이를 위해 시스템의 가용성 확보가 요구되고 있다. 그러나 정보보호시스템 설계와 운용시 일반적으로는 정보보호 본래 기능인 탐지, 차단에 주

※ 제일저자(First Author) : 노시춘
접수일자:2007년10월15일, 심사완료:2007년10월25일
* 남서울대학교 컴퓨터학과
nsc321@nsu.ac.kr
** 남서울대학교 멀티미디어학과
▣ 이 논문은 2007학년도 남서울대학교 학술연구비 지원에 의하여 연구되었음

력하고 시스템가용성에대한 대책은 간과되고 있다. 그 결과 정보보호시스템 운용현장에서는 인프라스트럭쳐에서 가장 먼저 가용성위협이 발생함으로서 결과적으로 보안처리 기능 자체 효율을 저하시킨다. 본 연구는 이 같은 NGN인프라 환경에서 인프라구조 측면의 향상된 고가용성을 구현함으로서 정보보호시스템 전반의 안정운용을 보증할 수 있는 방법을 제안한다. 새롭게 전개되는 NGN인프라구조에서 ① 정보보호인프라 고가용성 구조는 어떤 모양으로 구현되어야 하는지 ② 인프라구조 각 단계간 기능간 역할분담은 어떻게 이루어져야 하는가 ③ 고가용성구조의 효과가 무엇인지를 측정하는 것이 본연구의 목표이다. 본 연구는 이상의 현안과제를 해결하기위해서 정보보호 인프라스트럭쳐의 고가용성 Framework를 연구하여 제안한다. 그 내용은 NGN인프라환경의 정보보호 인프라스트럭쳐 구성방법론을 모형화 하는 것이다. 이를 위해 NGN인프라환경의 정보보호 인프라구조와 체계에 대한 효과적 대안을 도출하고 그 효율성을 검증했다. 본 연구는 정보기술패러다임 변화에 따라 변화된 공격 패턴에 대응할 수 있는 변화된 방어전술체계를 차세대통신망 정보보호시스템에 우선적으로 적용함으로서 NGN전반의 안정운용을 보증할 수 있는 방법을 모색하고자한다.

2. 정보보호시스템 Infrastructure 취약점

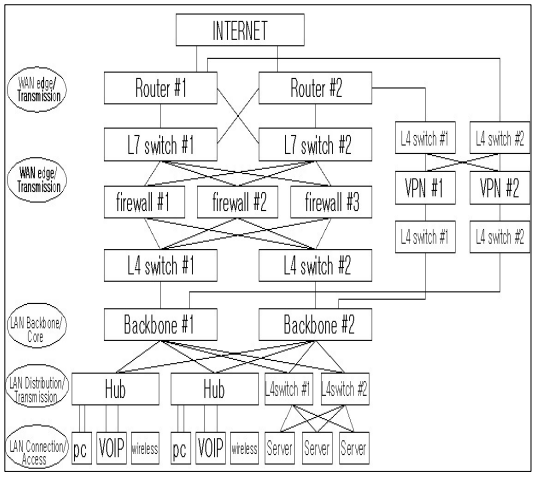
정보시스템상에서 일반구조 인프라스트러쳐의 기본적 컴포넌트는 외부라우터, 어플리케이션 스위치, 백본과 분배계층 그리고 정보보호시스템으로 구성된다. 선택적으로 사용되는 다른 시스템은 DMZ, Proxy서버, NAT 그리고 Cache서버이다. 일반구조는 각 구성요소를 하나의 단일 형상으로 구성함으로서 구조적, 기능적으로 유사성을 갖는다. 이 유사성은 역할, layout, topology, host간 부하분산, 정보보호시스템가용성, 네트워크구조, 정보보호침입차단 기능이다. 내부네트워크로부터 외부네트워크로 접속되는 접속점은 한곳으로 집중화되어있다. 이 같은 일반구조인프라의 비효율과 잠재적 위험성은 인프라를 가동하는 순간부터 발생한다. 먼저 하나로 집중된 네트워크 exit point로서 전체 네트워크의 외부와의 단일접속점인 게이트웨이 섹션에서 트래픽 과부하 발생 순간부터 전체 시스템의 병목구간으로 변하게 된다. 둘째는 half duplex 구조와 기능의 backbone, distributing network인데 반이중화 구조는 이중화기능을 시스템 상에서 부분적으로만 적용한다. 이 아키텍쳐는 backbone과 distributing network 장애시 장애를 전체네트워크 장애로 확대시킨다. 세 번째의 취약점은 packet handling 시 특정 네트워크 layer만을 switching 하는 것인데 패킷 핸드링을 특정 layer에만 한정시킴으로서 나머지계층에서 발생하는 잠재적 위험이 초래된다. 특정layer만의 switching구조는 모든 종류의 패킷진단과 악성코드 차단을 수행 할 수 없게 한다. Non-clustering 구조의 정보보호 환경 에서는 한쪽사이드 시스템장애를 다른 한편에서 기능을 인수 유지하지 못한다. 이 구조 하에서는 트래픽경로상에서 한 세션 다운시 모든 트래픽은 하나의 경로로 집중되고 추가적인 stand-by 경로가 존재하지 않으므로 시스템 위험도가 극대화 된다. 이 상황 속에서는 하나의 active 경로가 모든 트래픽 소통의 유일경로 이기 때문이다.

3. NGN Infrastructure 환경의 정보보호 고가용성 기반설계

3.1 기본적 설계사상

NGN 인프라스트럭쳐 환경의 고가용성 정보보호시스템 주요 구성요소는 diagnostics configuration, 상호 의존적 고가용성 구성에 대한 구조적인 기술, 서비스를 보호하고 복구할 수 있는 recovery actions, 다양한 시스템 구성 요소의 상태를 감시하고 관리하는 state management기능으로 설정한다. 설계사상에 따라 먼저 고가용성 시스템 인프라 기본구조는 core, transmission, access로 계층화 한다. 계층화된 구조상에서 softswitch를 backbone으로 구조와 기능을 적용한다. 외부 접속점은 외부라우터가 최전방에 위치하여 WAN edge층을 구성한다. WAN edge층은 LAN edge층으로 연결되며 core 층인 LAN backbone 구간을 거쳐 access층인 LAN 접속구간까지 연계된다. 인프라구조는 이같이 전 계층에서 고가

용성 구조로 개선된 topology를 적용, 구성한다. NGN 고가용성 인프라 구조도의 설계원칙은 구조상으로 전계층에서 구조 이중화, 기능적으로는 full-mesh 기능 도입이다. 이 구조는 cluster 형태로써 한대의 loadbalance 서버가 여러 대의 real서버로 요청을 분산한다. 두 대의 loadbalance 서버가 master와 standby 역할을 가지는 failover 형태이다. 만약 master서버가 loadbalance를 담당 하다가 장애를 일으키면 대기 상태의 standby 서버가 즉각적으로 loadbalance를 담당 하게 된다. master서버가 복구되면 standby 서버는 다시 대기상태가 되는 가장 안정적인 형태를 보증하게 된다.



(그림 1) Full-mesh형 고가용성 인프라구조

Master-server 두 대가 동일하게 작동하므로 서버 중 한대가 fail시 나머지 서버가 계속해서 임무를 수행 각 서버에 동일한 데이터가 저장되므로 어플리케이션 접근에 의한 부하를 분산 시킬 수 있다. Master-server 중 한대는 primary server로서 기능을 수행하다 failure발생시 stand by server가 임무를 수행한다. 데이터 insert, update, delete는 모두 마스터 서버에서 이루어지고, 데이터 select는 slave 서버들이 담당하게 되어 select query가 많은 사이트에서 성능을 발휘할 수 있다. 실시간으로 데이터 복제가 가능하며, 서버에 거의 영향을 주지 않는다.

3.2 정보보호 고가용성 기반구조

3.2.1 트래픽 Exit point 구조

트래픽외부 접속점 분산기능은 다수의 인터넷 접속라인을 사용하여 네트워크의 속도와 안정성을 개선하기 위한 기능이다. NGN 환경의 트래픽 분산은 다수의 ISP 전용선과 VDSL, 케이블 모뎀 등의 초고속 인터넷 회선을 결합시켜 단일한 전용선처럼 사용하게 한다. 또한 인터넷 트래픽을 효율적으로 관리하여 불필요한 특정 회선에 대한 트래픽 집중현상을 완화하여, 트래픽 처리 효율을 최적화한다. 내부망의 IP 대역은 전용선 IP대역을 동시에 사용하거나, 사설 IP 대역을 설정하여 PAT(Port Address Translation) 구성을 설정하여 사용할 수 있다. 특히, 인터넷라인이나 ADSL/VDSL 라인에 할당된 IP가 적은 경우에 내부망이 PAT를 사용하여 IP를 공유하도록 처리한다. 부하분산 방식에는 기존의 round-robin, hashing, least connection, maximum bandwidth방식을 선택적으로 사용한다.

3.2.2 Backbone 및 Distributing layer 구조

NGN 환경의 정보보호고가용성 네트워크 설계에서 첫 번째 요건은 backbone 및 distributing 계층에 대한 구조와 기능의 이중화 이다. 인트라넷 시스템을 기준으로 할 때 core계층은LAN backbone 구간이면 전송계층은 LAN distributing층, access계층은 LAN 접속층이다. 완전이중화 계층구조는 전통적인 반 이중화 구조로 부터의 탈피를 의미한다. 전통적인 반이중화구조는 침입차단시스템 중심으로 부분적으로만 이중화 구조를 도입하고 core와 distributing계층에 대해서는 가용성 구조를 적용 하지 않고 있다. 부분적 이중화는 시스템 가용성 보장에 한계를 나타낸다. 그 이유는 네트워크 접속점의 다원화, 트래픽 볼륨 비대화, 데이터 형태의 다양화로 인해 네트워크 가용성 위협 증가에 따라 부분적 이중화로서 고가용성 달성에 한계가 있기 때문이다. 정보보호시스템 가용성은 웹 컨텐트와 트랜잭션 시스템에 최대의 access 성능을 보장할 수 있도록 네트워크의 모든 계층에서 최대화 한다.

3.2.3 Multi -layer switching 구조

layer7 이상의 multi-layer스위치를 통해 load balancing을 통한 고가용성 확보로 보안시스템의 한계를 보강한다. Multi-layer스위치를 활용하여

패킷 처리기능과 viruswall 역할을 수행하고 multi-layer 패킷 핸드링을 시행한다. Multi-layer 스위치는 상위 계층으로 올라가면서 TCP, UDP 등의 프로토콜에 대한 컨트롤 역할을 하면서 트래픽 제어 등의 기능이 추가된다. 여기에 7계층인 애플리케이션 계층처리 기능 추가로 직접적인 패킷 필터링 및 QoS (Quality of Service)기능이 가능하다. 전용 ASIC을 사용하고 기본기능인 SLB(Server Load Balancing)나 LLB(Line Load Balancing) 외에 firewall, VPN, IDS등 보안장비의 loadbalancing 기능이 추가된다.

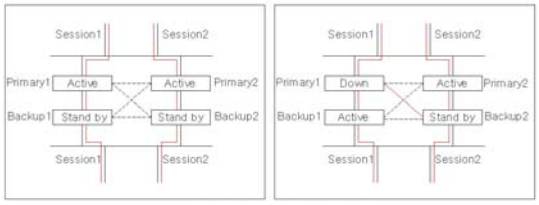
3.2.4 Clustering 구조

Clustering 메커니즘을 적용하여 2대 이상 보안 시스템을 하나의 virtual시스템으로 운영하는 구조를 선택한다. 이 경우 최대한 가용성 확보를 위해 mesh 구조 보안 네트워크 구축으로 한 방향 채널의 보안서비스 중단시 다른 채널에서 processing 인수가 가능 하도록 구성한다. 돌발상황 down-time이 발생하면 보안 프로세스들은 시스템 절체 및 원상회복을 위한 가용성 확보를 99.999% 수준, 즉 수초 이내 즉,99.999% 가용성으로 ping이 10개 이내로 drop되는 정도로 이뤄지는 것을 목표로 한다. 이 메커니즘은 네트워크로 연결된 서로 독립적인 복수 보안시스템 구성, clustering 방법 및 고가용성을 갖춘 보안소프트웨어와의 combination-connection 메커니즘을 통해 얻어진다.

3.3 Functional Mechanism of Failover

3.3.1 Scheduling Algorithm

Real서버로의 부하분산 스케쥴링 알고리즘은 여러 가지가 있는데 웹사이트의 운영방침에 따라 가장 적합한 알고리즘은 채택할 수 있다. Loadbalance 서버는 real서버가 정상적으로 서비스 되는지 체크하기 위해 real서버로부터 2초 간격으로 체크페이지를 읽어 들여 문자열을 체크한다. 장애복구된 real서버는 실시간으로 cluster 멤버에 등록된다. 웹페이지 방문자의 세션 유지를 위해 클라이언트와 real서버간의 연결 유지를 설정할 수 있으며 유지시간은 웹사이트 특성에 따라 조정 가능하다. 이기능하에서는 master 서버와 standby 서버간의 컨넥션동기화가 가능하도록 설계하는데 만약 master 서버가 장애를 일으키면 클라이언트와 real서버간의 세션유지를 위한 연결상태 정보를 standby 서버 그대로 유지하면서 loadbalance를 인수한다.



(그림 2) Active-Active hartbeat Connection

- Session상태 정상, 에러 동작 Mechanism
  - 정상session상태를 0, 에러session상태를 1로 나타낼 경우 가능한 primary, backup session구성
    0/0 : 두개 session이 모두 정상인 상태
    1/0 : primary 서버가 에러인 상태
  - Network이 동작하지 않는 경우 : firewall down발생함. 대응방법은 backup 서버로 전환 및 admin. tool에 alarm 전달
  - Network은 동작하나 IDS가 동작하지 않는 경우, 대응방법은 admin. tool에 alarm전달
  - OS상의 fault, 대응방법은 backup 서버로 전환 및 admin. tool에 alarm 전달
    0/1 : backup 서버가 에러인 상태
  - Backup 서버는 외부로 드러나지 않기 때문에 공격에 의한 fault 위험 없음, 대응방법은 admin. tool에 alarm 전달

3.3.2 Failovering

라우팅, layer7 switching, 침입차단시스템, 패킷필터링, layer4 switching, backbone네트워킹기능의 primary-secnndary 두 기능 모두 active 상태로 동작 하고 각 장비를 통과하는 네트워킹 트래픽과 VPN 트래픽을 처리한다. 한 세션 장애 발생시 다른 세션이 master가 되어 트래픽을 100% 인수한다. Full-mesh형 모드에서 fail-over가 발생할 경우 장비 성능이 방해를 받지 않도록 구간별 트래픽 volume을 조절 한다. 가용성을 달성하고 두 장비 간의 동기화를 보장하기 위해 전용 고가용성 인터페이스 쌍을 보유한다. 인터페이스에 대한 연결이 손실되면 다른 인터페이스를 사용해 동기화 정보를 fail-over한다.

Fail-over가 시작되는지 확인하기 위해 구성 가능한 최소 200ms 간격으로 hartbeat 메시지를 보낸다. 이때 hartbeat손실, interface-link 손실, 구성된 IP 주소 또는 모니터링된 IP주소 세트 손실 이벤트를 통해 fail-over 메커니즘을 가동시킨다. 시스템간 클러스터 hartbeat 통신으로 장애 발생시 3초안에 클러스터 재분배 및 자동 분산기능을 가동한다.

Failover Scenario

- Scenario 1
  -상황: session 1 이 normal channel로 연결
  -결과: backup으로 takeover되지 않음
- Scenario 2
  -상황: session 1,2가 crossover channel로 연결
  -결과 : backup으로 takeover 연결
- Scenario 3
  -상황 :session1이 normal channel로 연결, session2는 crossover channel로 연결
  -결과 : alarm 발생, backup으로 takeover
- Scenario 4
  -상황 :session 1이 crossover channel로 연결, session 2는 normal channel로 연결
  - 결과 : alarm 발생, backup으로 takeover

3.3.3 Hot-Sparing과 Hartbeat Connection

NGN환경에서 core 시스템은 완벽한 redundance를 내장하여 hot-sparing 기능을 적용한다. Core 스위치와 라우터의 경우, switching fabric과 supervisor engine은 손실율 제로의 hartbeat 기능으로 설계한다. Interface port module과 multi service blade 역시 내부 spare를 보유해야 하며, 몇 초 이내에 서비스로 전환될 수 있는 기능을 갖게 한다. Core시스템은 충분한 처리용량을 보유해야 하며 voip폰이나 wap기반 공중 무선액세스 등 NGN 서비스가 네트워크에 추가될 경우 이를 수용할 수 있도록 확장성을 갖춘다.Primary 서버와 backup 서버간 서버 상태 정보와 세션 정보를 주고 받기위해 hartbeat connection을 연결한다. Hartbeat connection이 없을 경우 primary 시스템에서 back-up시스템이 정상 동작 후에도 back-up 시스템은 primary 시스템에게 역할을 양도하지 않는다. 이 메커니즘에서는 하나의 세션 다운시 즉각적인 hartbeat connection이 이루어지고 유입 또는 유출 트래픽은 두개 경로의 백업루트로 분산되어 1개 경로로의 세션 집중화 현상이 발생되지 않는다.

3.3.4 Core,Transport 계층 자동복구

Core, transport, access 계층에 대해 기기와 link, 프로토콜, 애플리케이션 레벨에서 연동되는 네트워크의 복구성을 최대화 한다. 기기레벨의 복구성은 multi processor, SSO(Stateful Switch over), IOS(input output software) 기술연동으로 구현한다. Link레벨의 복구성은 RPR(Recovery Packet Ring), 멀티 링크 PPP(Point to Point) 프로토콜, EtherChannel(r), IEEE802.1w과 802.1s spanning tree 향상판 기술을 통해 확보한다. 프로토콜 레벨 복구성을 위해 GLBP(Gateway Load Balancing Protocol)과 라우팅 및 접속 프로토콜을 위한 라우팅 프로토콜 통합 최적화 기능을 도입 한다. 애플리케이션 레벨의복구성은 SNAT(StatefulNetwork Address Translation)과 서버로드밸런싱 기술을 적용한다.

4. 성능시험

4.1 측정환경

측정시스템은 데이터센타, 연구소를 보유한 A기업 시스템으로서 600대의 스위치와 150대의 라우터, 150여대의 콘솔서버, 400개의 access point와 컨텐츠스위칭 기기로 구성되었다. 측정시스템은 ISP의 softswitch를 기반으로 하는 NGN네트워크에 연결된 정보보호 인프라스트럭쳐를 구비하였으며 정보보호시스템 고가용성 구조로서 네트워크구조 계층화와 트래픽 부하분산 구조, layer7 mulilayer 스위칭과 clustering구조, 그리고 프로토콜과 소프트웨어기능의 fail-over 기능을 적용했다. 고가용성에 대한 측정실적 기록은 모든 유형의 기기목록이 포함되어 있는 스프레드시트의 메트릭스로서, 장비의 수, 총 장비 장애시간, 장애에 견딘 총시간, 기기가용성, 가동시간 및 다운시간 등을 제공하는 분석 소프트웨어에 의해 수집되었다. 가장 중요한 데이터는 MTBT(Mean Time Between Failure)와 MTTR(Mean Time To Recovery)로, 네트워크

의 기기와 경로에서 수집 및 분석이 시행되었다.

4.2 측정결과

4.2.1 Trouble 패킷에 의한 시스템 과부하율

스위치는 외부 라우터의 트래픽 라우팅 처리를 통과한 패킷에 의해 1차적으로 과부하 트러블이 발생하는 구간이다. 다음의 표는 애플리케이션 스위치에서 발생하는 과부하트러블 트래픽 물량이다. 고가용성 구조에서 밸런싱 물량 폭주로 인한 애플리케이션 스위치 병목화 가능성은 27%정도로 낮아진다. 또한 만약 발생한다 해도 그것은 메인 구간으로 국한되며 타구간에는 영향을 주지 않는다.

<표 1> 패킷스위칭시의 시스템 과부하 발생수준(%)

구 분	일반 인프라구조	고가용성 인프라 구조	
패킷처리인프라 구조	main	primary	Backup
스위칭 데이터 종류	packet	contents	contents
일간패킷처리량	44	51	49
패킷처리분담율	100%	73%	27%

단위 : mill. packets/day

4.2.2 SNMP polling trap에 의한 접속상태

애플리케이션 스위치에 의해 loadbalancing 처리된 트래픽이 각 시스템별로 어떻게 분배 되는가에 대한 측정 결과이다. 구조개선 전 게이트웨이 구간 병목화 요인이 되고 있는 침입차단 시스템은 메인 침입차단 시스템으로서 메인 침입차단 시스템의 부하 경감 여부가 측정 포인트이다. 메인 침입차단 시스템에서 부하 감소된 트래픽은 각 기능별 침입차단 시스템으로 분산된 결과를 보여준다. 기존 구조에서 메인 침입차단 시스템이 처리하는 총 트래픽량 100%가 고가용성 구조에서는 73%로서 27%가 감소되었다.

4.2.3 Ping 패킷에 의한 ICMP도달율

전송 패킷량이 점차 증가하는 과정에서 트래픽량이 CPU 처리 가능 한계를 초과하면 네트워크 지연 현상이 갑자기 증가하고 패킷 유실이 발생하기 시작한다. 고가용성 구조의 처리 능력 향상은 시스템 과부하를 축소시켜 정보 손실율을 감소시키고 있다. 조사에서는 침입차단시스템 하단 내부 네트워크에서 침입차단 시스템을 통과하는 전송구간의 특정 사이트를 향해 "ping" 테스트를 실시하고 결과를 집계한 것이다.

<표 2> Ping 패킷 ICMP 도달성능(%)

구 분	일반 인프라구조			고가용성 인프라구조		
	전송량	수신량	유실율	전송량	수신량	유실율
다 음	1,701	1,235	28.7%	1,307	1,220	7.0%
야 후	1,520	1,400	8.0%	1,300	1,272	2.2%
네이버	1,988	1,881	5.4%	1,541	1,499	2.7%
알타바스타	1,708	1,609	5.8%	1,601	1,555	2.9%
일간평균	1729	1531	11.5%	1437	1386	3.5%

단위: mill. packets/day

5. 결 론

측정대상 시스템의 업무량 규모와 복잡성에도 불구하고 네트워크는 100% UPS와 비상 발전기를 갖춘 네트워크에서 99.999%의 가용성을 달성했다. 이 검증을 통해 정보보호 고가용성 인프라를 갖추고 정교한 fail-over 알고리즘 사용하여 시스템상에서 장애가 발생할 경우, 중단 없이 작동 가능하다는 것을 보여줬다. Fail-over 처리시 back-up unit는 거의 즉각적인 fail-over 시간 내에 기존 트래픽을 지속적으로 처리할 수 있도록 필수 네트워크 구성, 세션 상태 및 보안 연결을 하고 있다. 내장된 fail-over 프로토콜과 동적 라우팅을 사용함으로서, 고가용성과 테크놀로지는 정보를 액세스하고 전달하는 네트워크 성능과 유연성을 향상 시키며 또한 보안시스템의 중단 없는 서비스를 통해 생산성 손실을 방지할 수 있다. NGN인프라 환경에서 보안시스템의 고가용성을 실현하려면 최적의 방식으로 infrastructure와 보안시스템의 topology 및 성능 mechanism이 확보되고 구현되어야 한다.

참 고 문 헌

[1] Willam Stallings, "Network and Internetwork Security". Prentice Hall, 1995.

[2] D. Dias, W. Kish, R. Mukherjee and R. Tewari, "A Scalable and Highly Available Server", COMPCON 1996, pp. 85-92, 1996.

[3] Xuehong gan, Trevor Schroeder, Steve Goddard and Byrav Ramamurthy", in submission to The Eighth IEEE international Conference on Computer Communications and Networks , 1999

[4] G. Hunt, G. Goldszmid, R. King, and R. Mukherjee,"Network Dispatcher: A Connection Router for Scalable Internet Service, Computer Networks and ISDN Systems, Vol.30, pp.347 357, 1998.

[5] D. Dias, W. Kish, R. Mukherjee and R. Tewari ," A scaleable and highly available Web server" IEEE international Conference on Data Engineering. New Orleans, February 1996.

[5] G. Trent and M. Sake, WebStone, "the First Generation in HTTP Benchmarking", MTS Silicon Graphics, February 1995.

[6] IA-LVS,"Design of the Improving Availability for Linus Virtual Server", 2nd International Conference on Software Engineering, Artificial Intelligence, Networking & Parallel/Distributed Computing August 20-22, 2001 Nagoya Institute of Technology, Japan

[7] Sookheon Lee, Geunyoung Chun, Myongsoon Park," Load balancing mechanism for dispatchers in Web server Cluster", International Conference on ITCC 2002, Orleans, Las Vegas, U.S.A, 2002

노 시 춘

1987년 : 고려대학교 경영정보학(석사)
2005년 : 경기대학교 정보보호기술(박사)
1982년~2003년 : KT IT본부 시스템보안부장
2003년~2004년 : KT 충청전산국장
2005년~현 재 : 남서울대학교 컴퓨터학과 컴퓨터전공 교수
관심분야 : 차세대통신망, 정보보호, 컴퓨터네트워크

방 기 천

1981년 : 서울대학교 전자공학과(학사)
1988년 : 성균관대학교 정보처리학과(석사)
1996년 : 성균관대학교 전산통계학전공(박사)
1984년~1995년 : MBC 기술연구소
1995년~현 재 : 남서울대학교 멀티미디어학과 교수
관심분야 : 멀티미디어콘텐츠, 멀티미디어 응용, 인터넷 방송 등