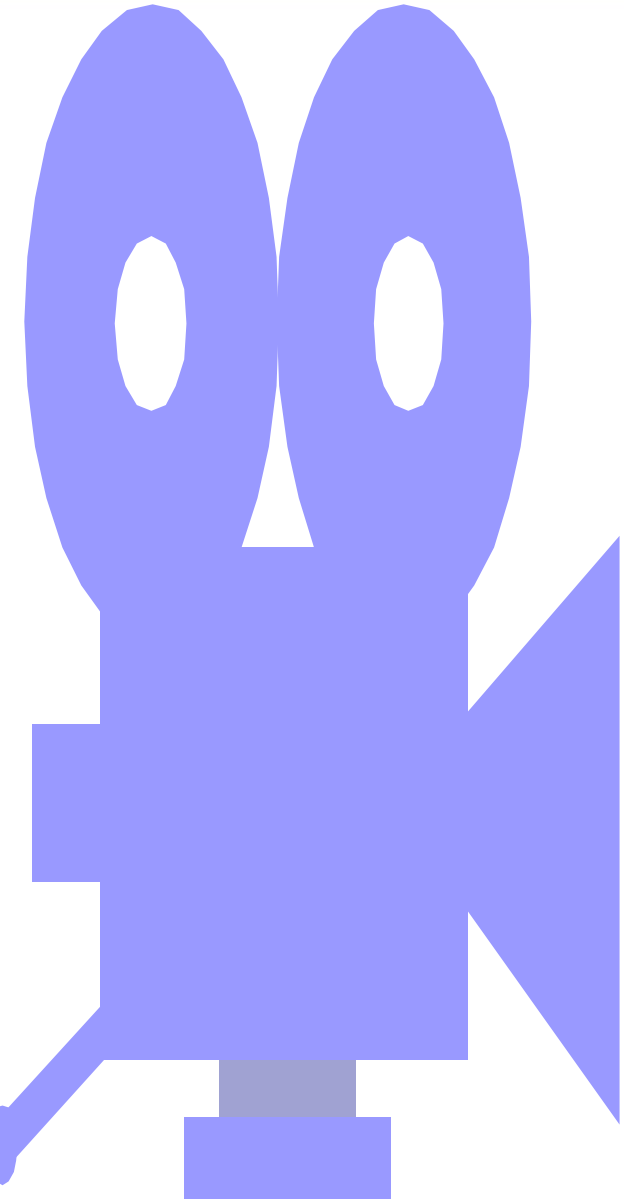
신제품 NXG 시리즈 제품 소개

2003년 06월 18일

시큐아이닷컴
NXG 개발 PM
나원택 (wtna@secui.com)

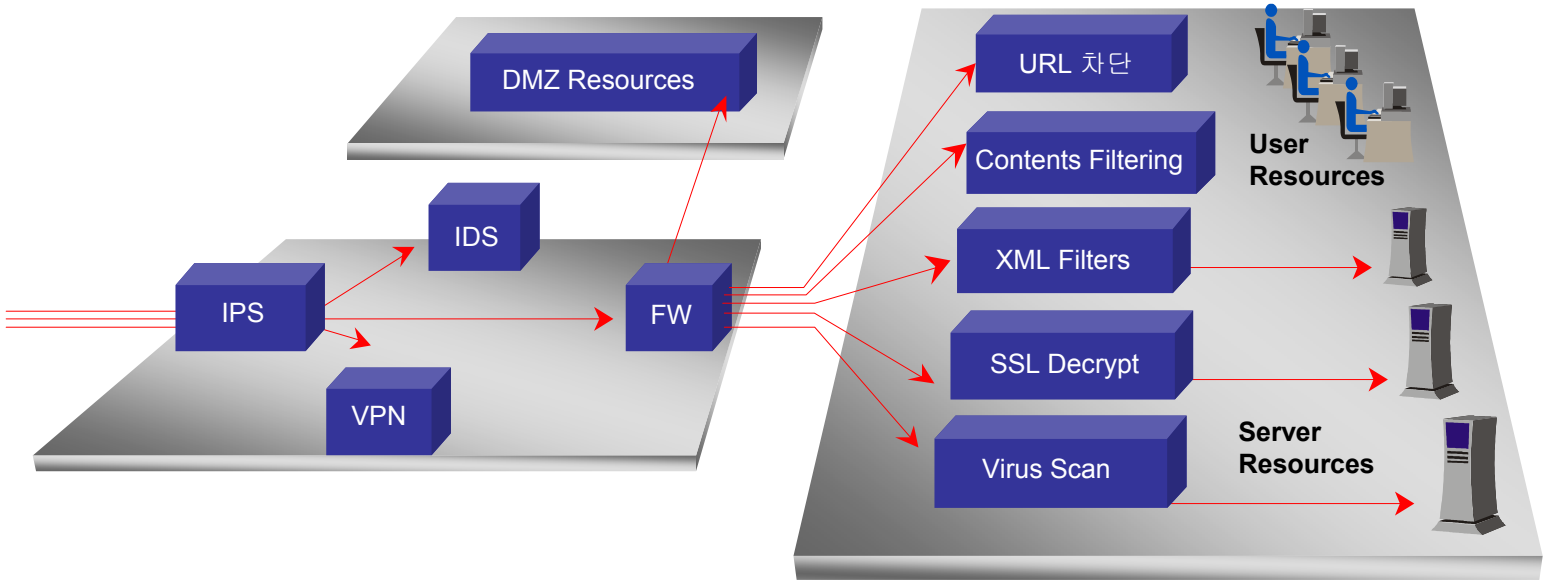
목 차



NXG 4000 – 개요

개발 배경

- 인터넷 트래픽의 기하 급수적 증가에 따른 고성능 보안 장비의 요구
  - 작은 패킷의 증가, 세션 수의 증가
  - WORM, DDoS 공격 위협
- 다양한 보안 요구
  - VPN, IDS, IPS, Contents Filtering, URL 통제, SSL 스위치, Virus Scan
  - 각종 서버 보안 및 Client 보안 Tool
- 네트워크 구성, 관리 및 통제의 간소화 요구
  - 투자비 및 관리 비용의 증대

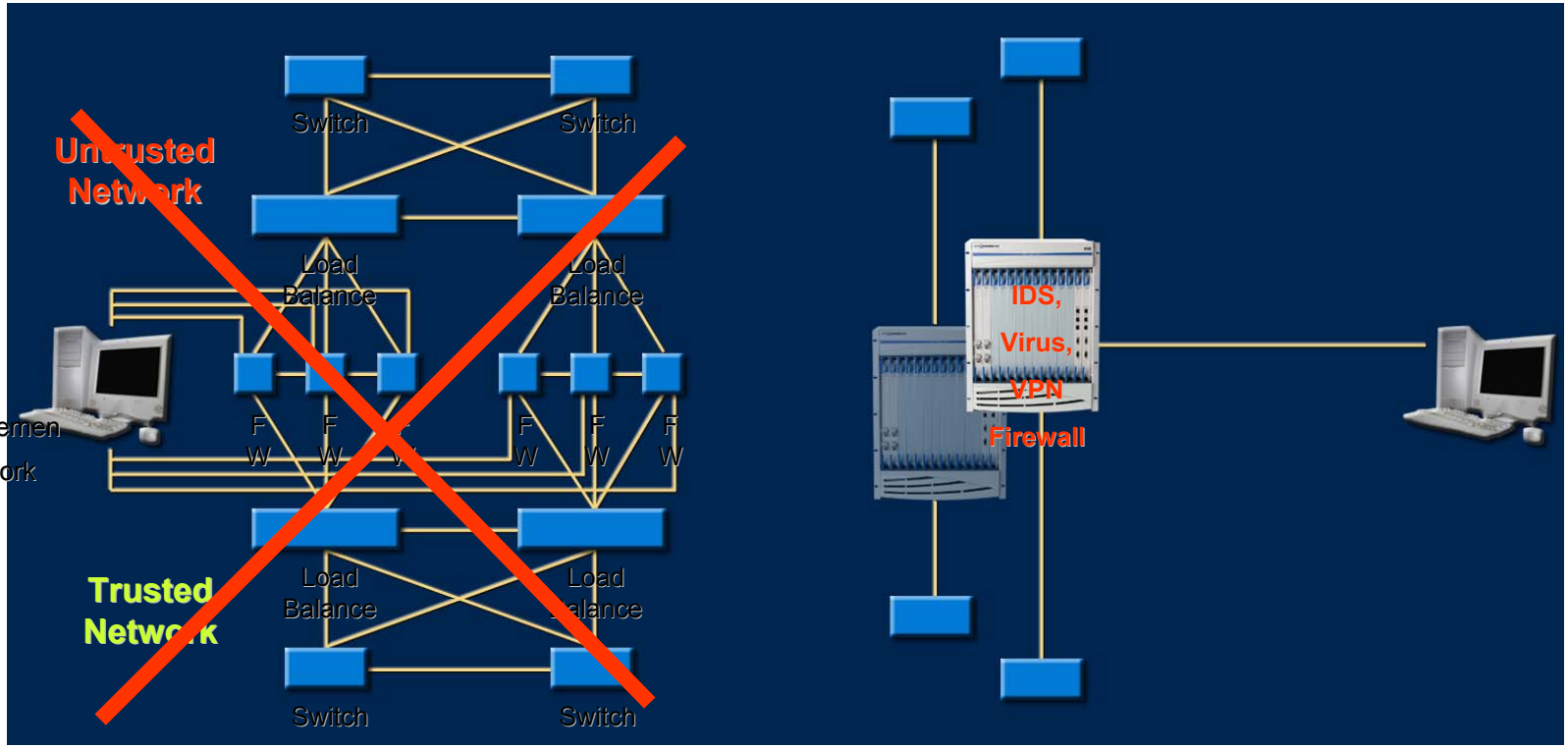


보안 네트워크 구성

NXG 4000 – 개요

목표

- **Wire Speed 보안 장비**
  - 64byte 패킷으로 1Gbps Throughput 달성
- **방화벽/VPN 토대 위의 다목적 보안 장비**
  - Open Security Platform : Crossbeam X40
  - 다양한 보안 Solution(IDS, Virus Scanner, SSL Switch 등)을 독립된 형태로 탑재
  - Simple한 네트워크 구조



NXG 4000 – 개요

기대 효과

- **All in One Solution**
  - 하나의 장비로 다양한 보안 목적을 달성
  - 단순한 구성의 극대화
  - 여러 보안 Application(최대 10가지)들이 동시에 수행
- **관리 비용 및 투자비 절감**
  - 합리적이고 단순한 운영
  - 새로운 보안 Solution 도입의 용이성
  - 편리한 각 Solution에 대한 Upgrade
- **대폭적으로 향상된 성능**
  - 기존 평균적 Gigabit 급 보안 장비 대비 최대 10배 성능 향상
  - 각 Solution의 병렬 처리로 전체 Latency Delay의 절감
- **확장성의 확보**
- **안정성**
  - 자체 Redundancy (Single Box High Availability)
  - 이중화 구성

Dramatically Simplifies and Strengthens Your Network

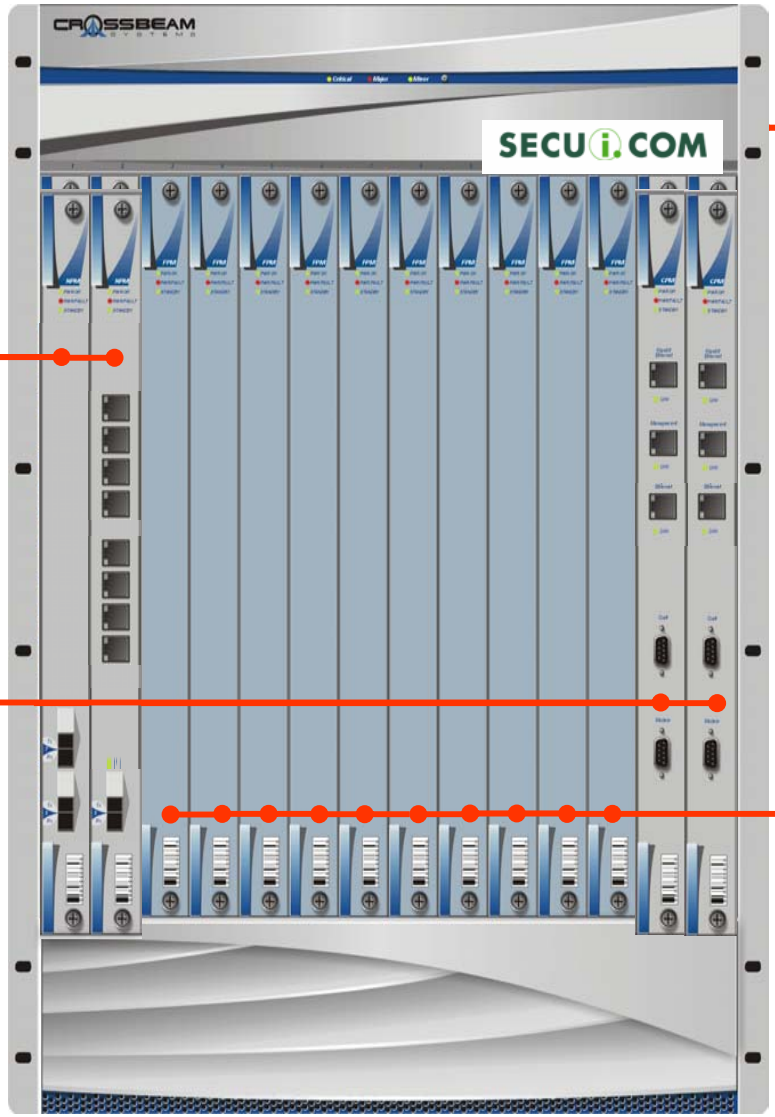
NXG 4000 – Architecture

Network Processing Modules (NPMs)

최대 2개 모듈
고성능 NPU 탑재
Gigabit 2 Port 또는
1x1GE + 8x10/100E

Control Processing Modules (CPMs)

최대 2개 모듈
Pentium III
하드디스크 탑재
10/100/1G 로그포트
10/100 관리포트
10/100 HA포트
Modem/Console 포트



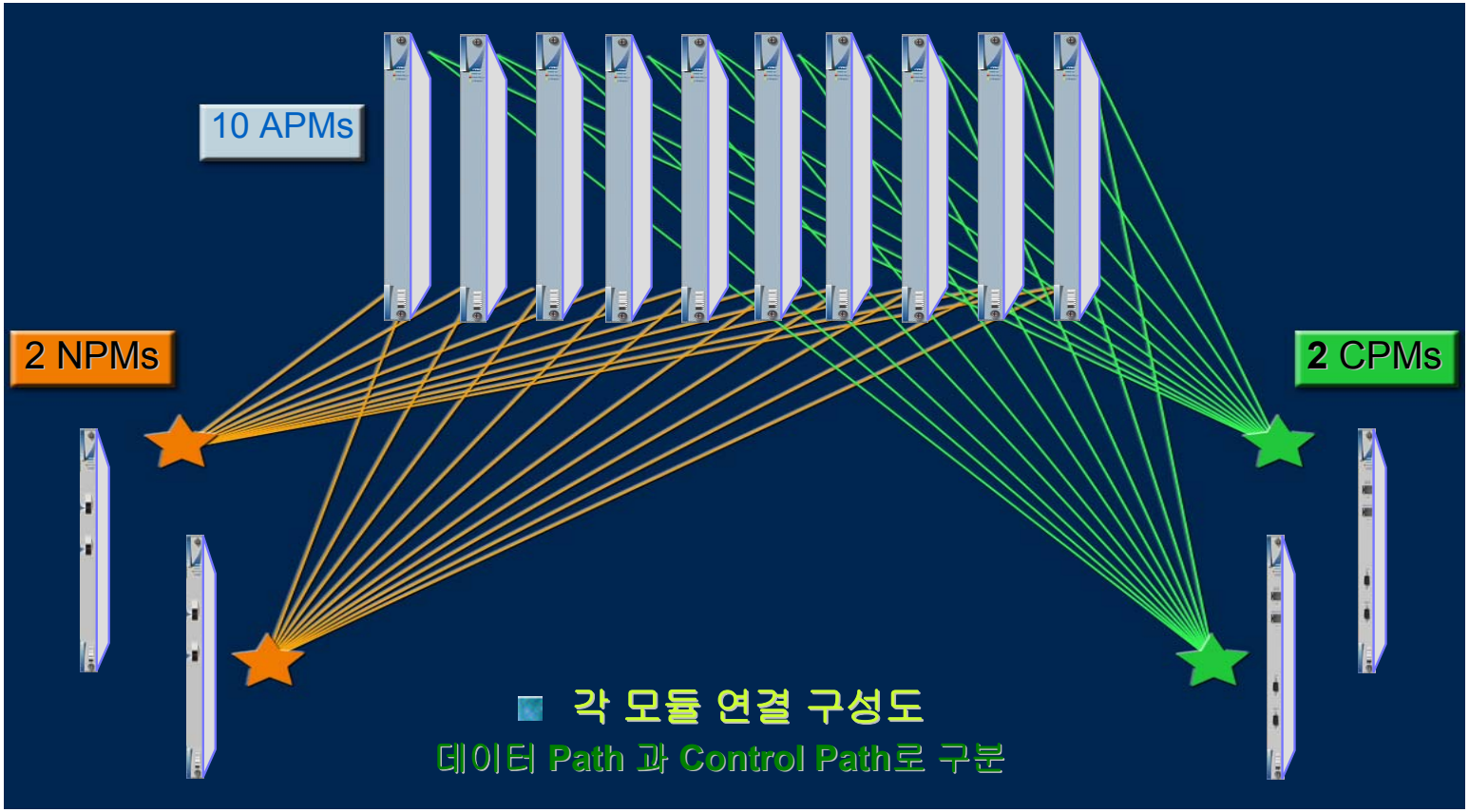
Backplane

Dual non-blocking 구조
최대 44.8 Gbps 처리
데이터 : 1.6 Gbps
관리용 : 100 Mbps

Application Processing Modules (APMs)

최대 10개 모듈
Pentium III
Hardened OS
보안 Solution 탑재

NXG 4000 – Architecture



데이터 경로

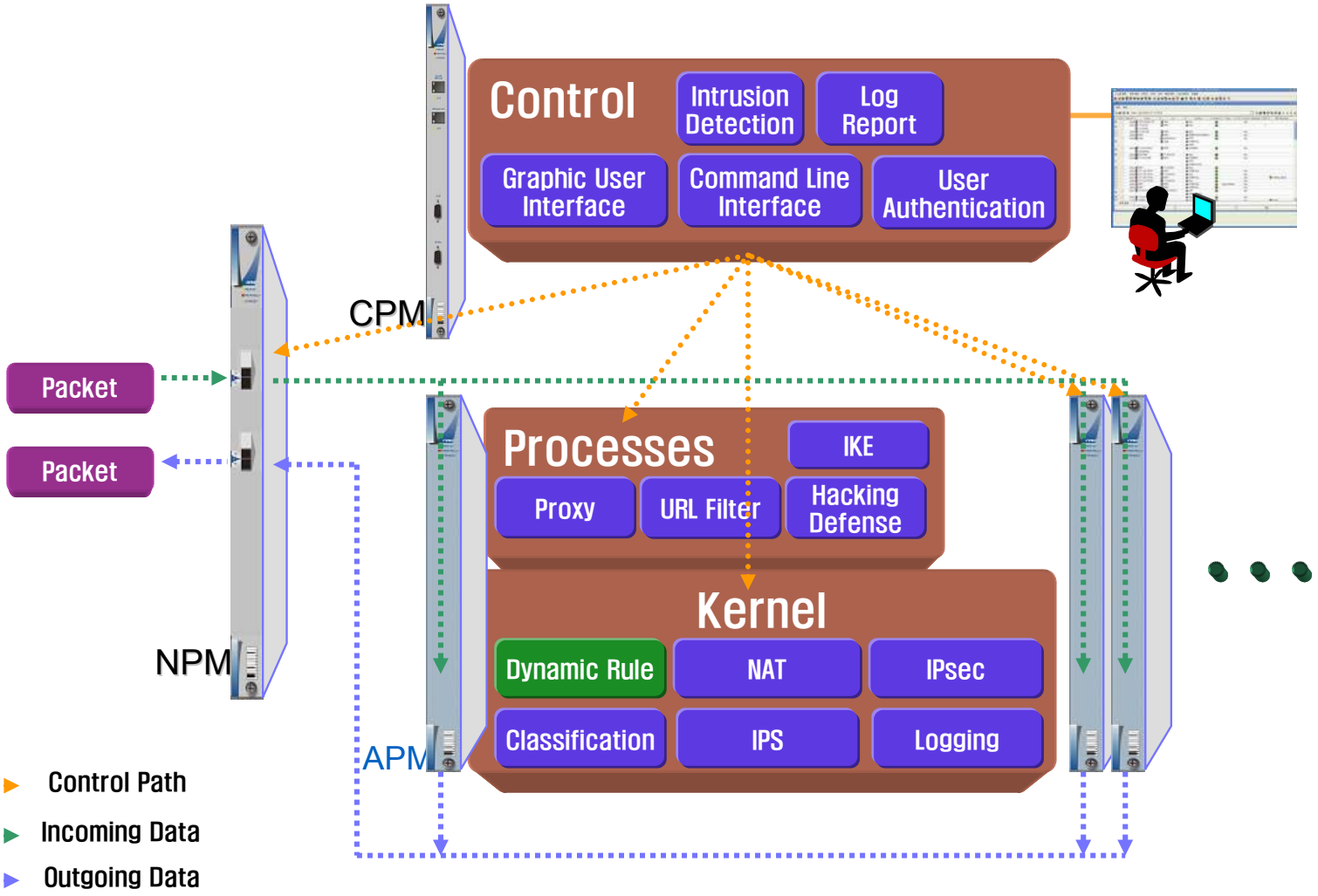
- 2개 경로 **Switch** (NPM당 하나)
- **Path** 당 **25 Gbps** 용량
- 각 **APM** 당 두개의 **1.6 Gbps link**가 생성

Control 경로

- 2개 경로 **Switch (CPM** 당 하나)
- 관리 경로의 **Redundancy**
- **Path** 당 **1.6 Gbps** 용량
- 각 **APM** 당 **100 Mbps link** 생성

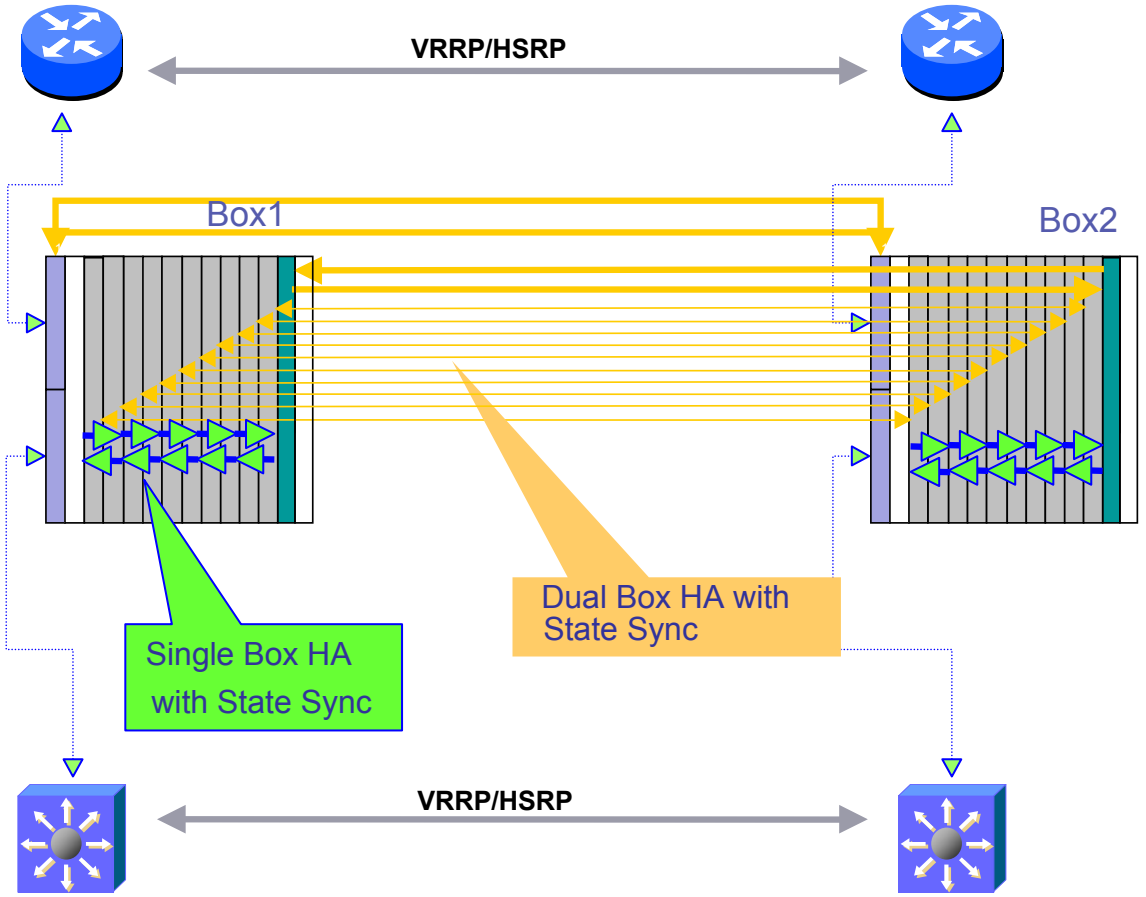
NXG 4000 – Architecture

Firewall/VPN/IPS Architecture



HA Architecture

- Active-Active
- Active-Standby
- Interface redundancy
- Control redundancy



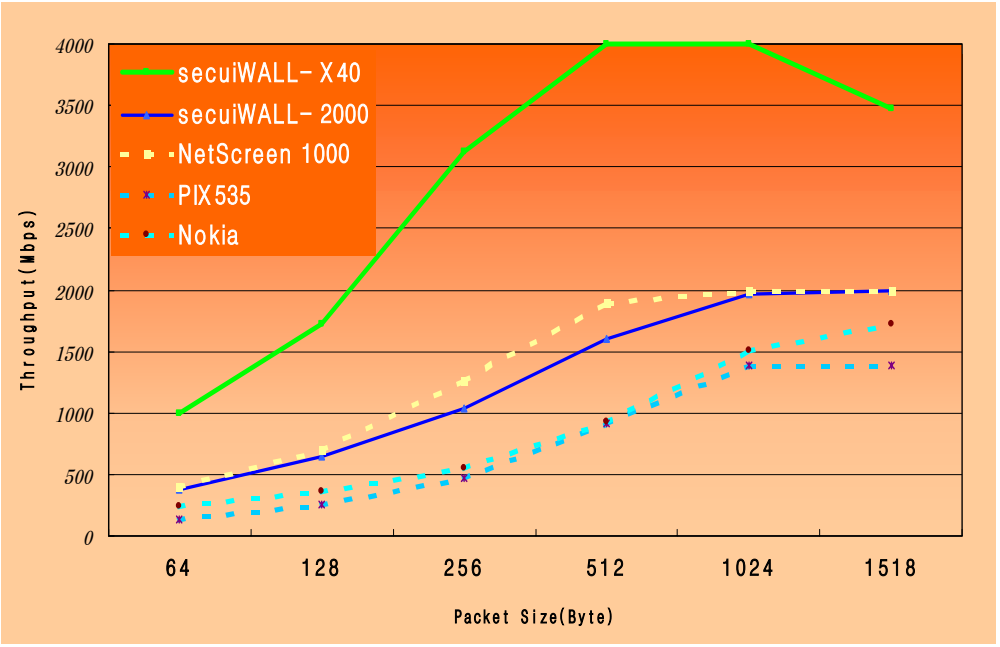
기타 Architecture 특징

- 수천개의 VLAN 지원
- 16 개의 분리된 별도의 DMZ port 지원
- 4개의 Giga 포트 또는 16개의 10/100 포트 또는 이들의 조합
- 저전력 : 최대 600W 사용
- 데이터 경로와 Management 경로가 별도로 구성 : 데이터 경로 상의 각종 위협으로부터 Management 경로의 안전을 보장
- SSH/GUI(JAVA)/HTTPS를 이용한 시스템 관리
- 이중화 구성 시 세션 동기화 지원
- 10/100 Mbps HA 포트 및 Control 포트, 1Gbps 로깅 포트 별도 지원

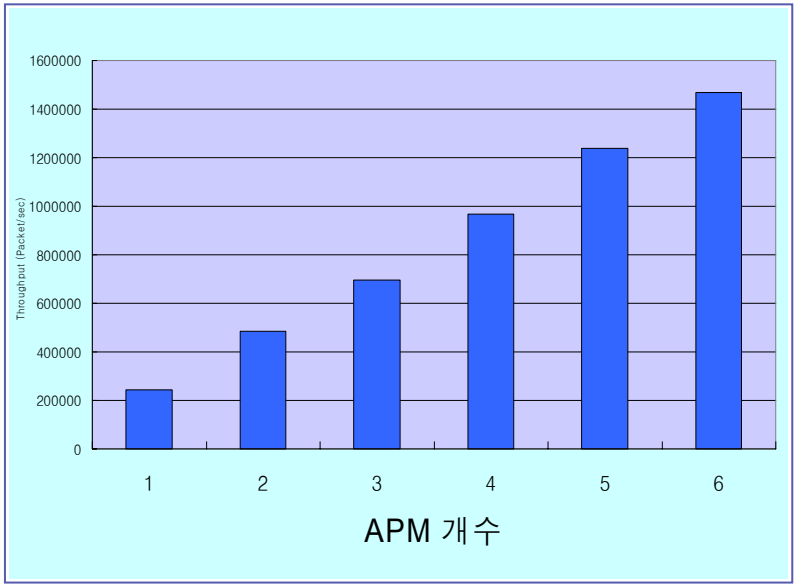
NXG 4000 – 성능

- ✓ 최대 처리 성능 : 4 Gbps (2 NPU)
- ✓ 최대 패킷 처리 성능 : 최대 초당 250만 패킷
  (APM 10개, 세션 비동기화 모드)
- ✓ 최대 동시 처리 세션 수
  - 세션 동기화 모드 : 500,000 세션
  - 세션 비동기화 모드 : 5,000,000 세션 (APM 10개)

4Gbps 성능 비교 (secuiWALL-X40 APM 6장 장착 시)



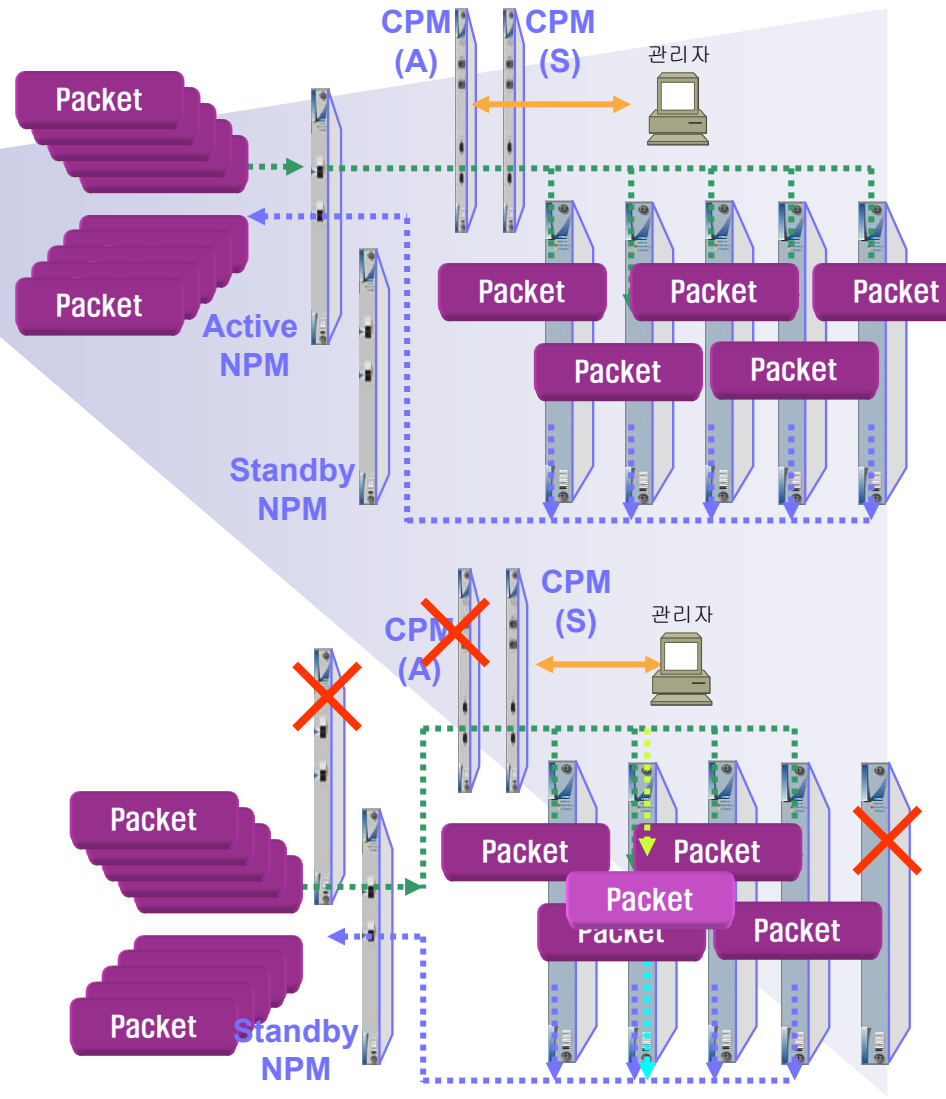
APM 개수에 따른 초당 패킷 처리 성능



NXG 4000 – High Availability

Single Box HA

- ✓ 3-Bay Power Supply
- ✓ Active-Standby NPMs/CPMs
  - 선택적으로 NPM과 CPM 이중화가 가능
  - 이중화된 NPM과 CPM은 Active-Standby로 구성
  - Active 상태의 NPM 또는 CPM Fail시 Standby 상태의 모듈이 즉시 대체
- ✓ 복수 Active-Active APM
  - 평소 각 APM이 부하 분산을 수행
  - 특정 APM 장애 시, 즉각적인 세션 재분산이 이루어 짐
  - 세션 동기화 모드 : 세션 단절이 없음
  - 세션 비동기화 모드 :
    Fail 된 APM 상의 세션들은 단절됨
- ✓ Active-Standby 형태의 APM 구성도 가능

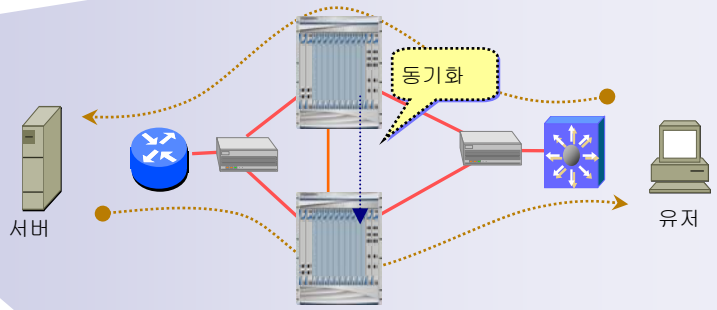


NXG 4000 – High Availability

Dual Box Active-Active HA

- ✓ 고유의 독창적 기술로 국내외 특허출원
- ✓ **Distributed Stateful Inspection**
  - **Kernel Level**에서 신속히 이루어지는 **Session** 정보의 동기화
  - 여러 장비에 분산되는 패킷으로 **Session**을 유지관리
  - **Session Synchronization**(장애발생 시, **Session** 지속 보장)
- ✓ 다양한 이중화 네트워크 구성 가능
  - **Router Mode HA : 특정 인터페이스 장애 발생 시, 해당 인터페이스의 가상 IP주소를 정상동작 중인 인터페이스가 사용**
  - **Bridge Mode HA**
- ✓ 고가의 **L4 Switch** 없이 부하분산과 **HA**를 동시에 달성

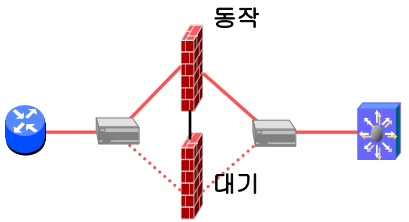
Session Synchronization



기존 HA 문제점

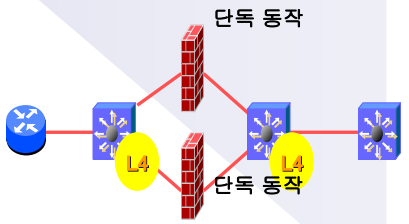
◆ Active-Standby 구성

-2대를 설치해 1대 만 운영
-변환 시에 세션을 단절



◆ L4 Switch를 이용한 로드밸런싱

-고가의 L4 Switch구입에 부담
-4대의 장비를 개별관리가 곤란



NXG 4000 – High Availability

VPN Active-Active HA

✓ 자체 VPN 부하 분산 기능

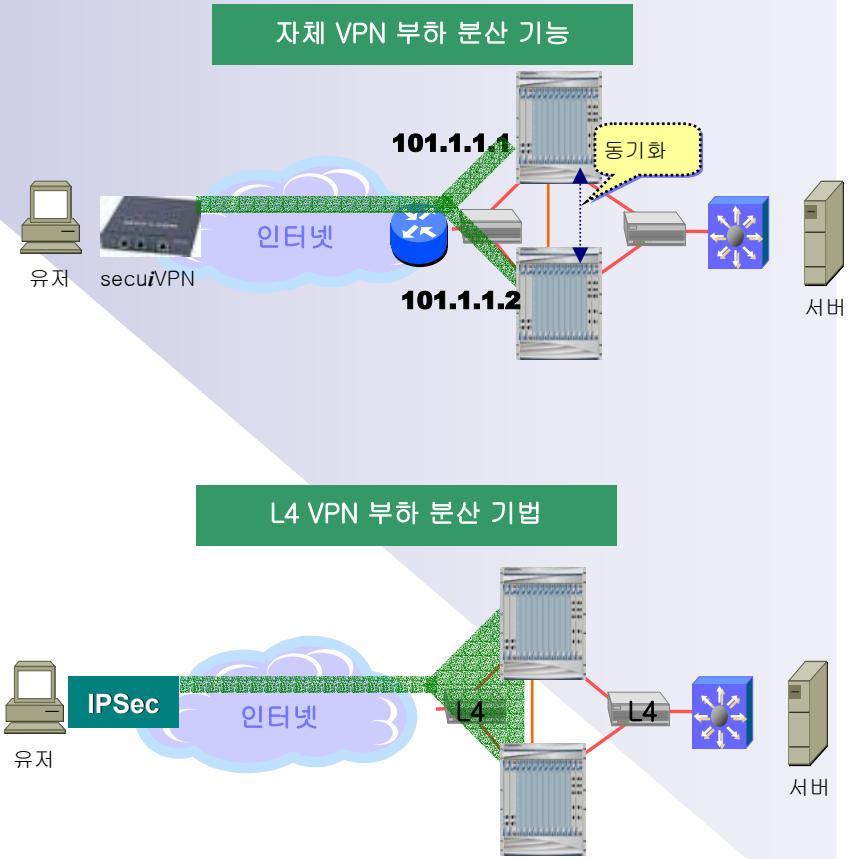
- L4 스위치 또는 VPN 전문 부하 분산 장비가 불필요
- 1 대의 Remote VPN Gateway가 2 대의 중앙 VPN Gateway로의 가상 Tunnel 생성 (Remote VPN Gateway가 secuiVPN Series인 경우)
- VPN 세션 동기화 발생

✓ L4 VPN 부하 분산 기능

- 가상 IP 주소로 복수 VPN Gateway에 동시 유입된 각 VPN 패킷들을 부하 분산하여 처리
- Remote VPN Gateway 타사 제품 가능 IPSec 표준을 지켜야 함

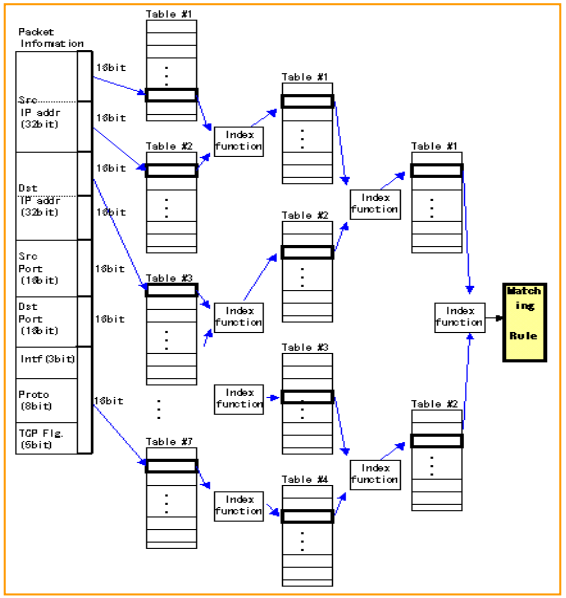
✓ Active-Standby HA 지원

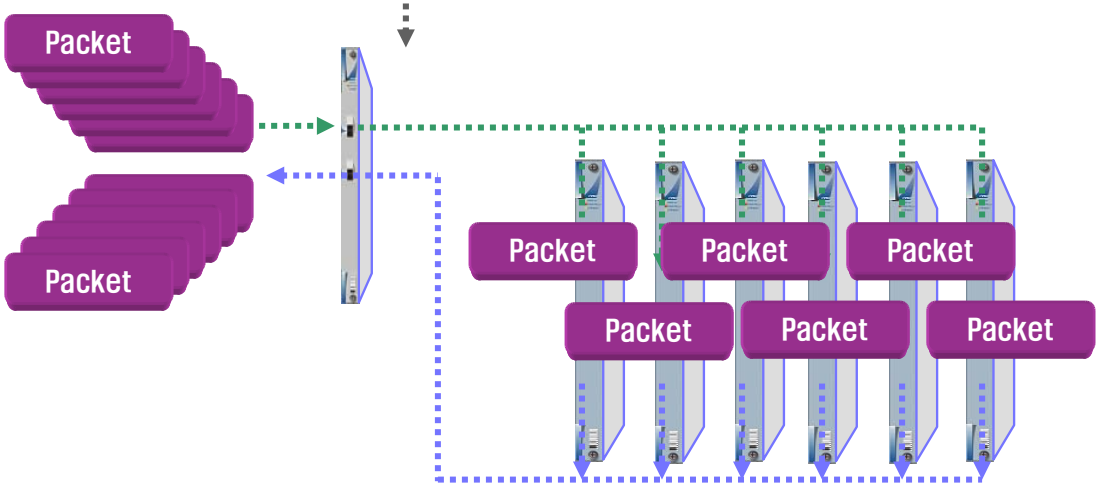
- VRRP, Lease-Line-Backup 지원



NXG 4000 – FIREWALL

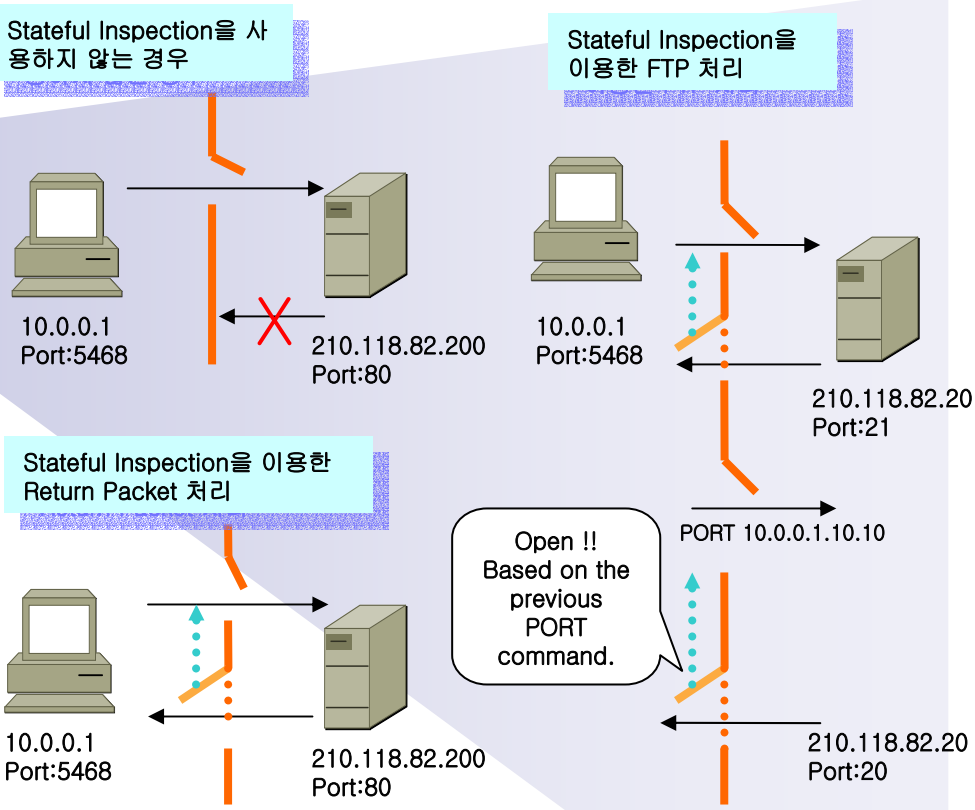
- ✓ secuiWALL 고유의 독창적인 Classification 알고리즘
  - KT 마크 획득
  - 국내 및 미국 특허 출원
    (국내 출원번호: 10-2001-0020524)
  - 정책의 수와 동시 접속 세션 수에 무관한 성능
  - 고속의 정책 판별 수행
- ✓ Kernel Level에서 의 Stateful Inspection Traffic 처리
- ✓ 각 APM에서 고속의 분산 처리





Stateful Inspection

- ✓ Application 특성에 따라 선행 트래픽을 기초로 예측된 트래픽에 대한 동적제어
- ✓ Dynamic Port를 이용하는 Application에 대한 Secure Channel 제공
  - SUN RPC, H.323, SQL*NET, TFTP
    * Port 1521 등을 사용하지 않는 SQL*NET 처리
  - FTP(Passive/Active), Dialpad, WOWcall
    * Port 21을 사용하지 않는 FTP 처리
  - Traceroute, PING
  - Real-Player
  - Windows Media Player
  - MSN 파일 주고받기 및 음성채팅 지원

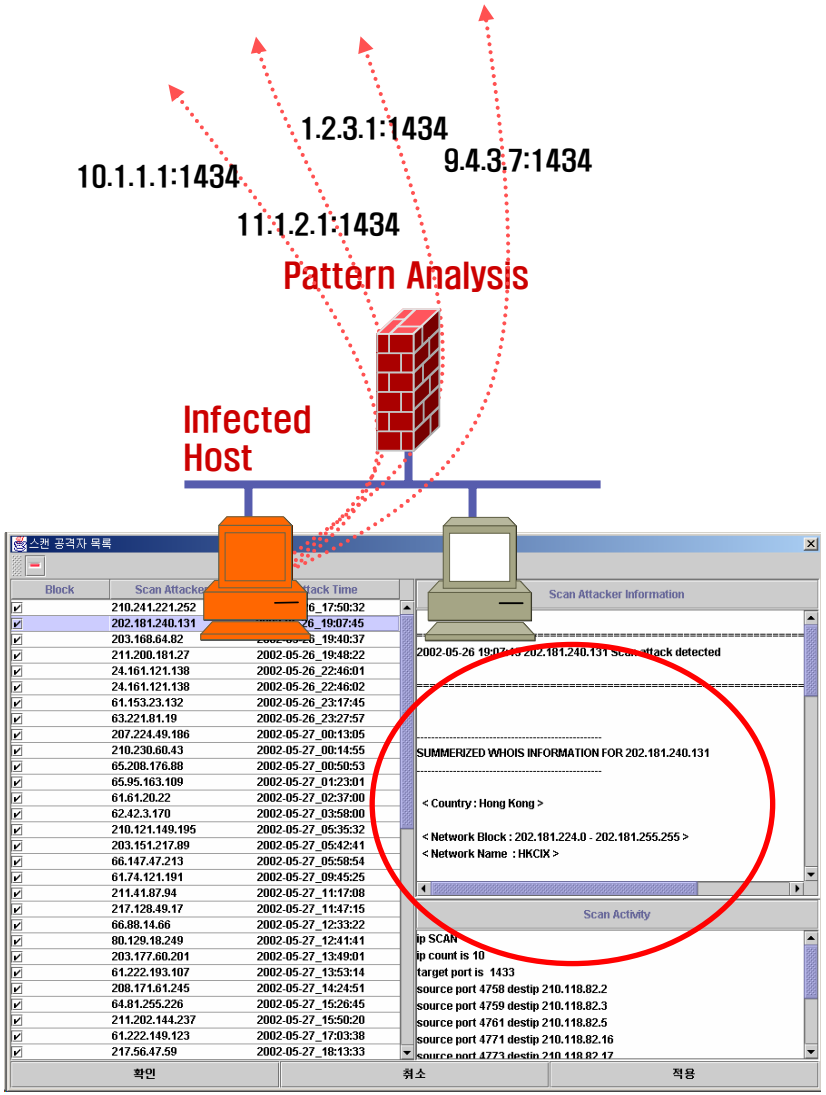


NXG 4000 – 유해트래픽 차단(IPS)

SCAN 시도 탐지 및 차단 기능

▣ WORM 트래픽의 전형적인 패턴은 다음과 같음
- ✓ 동일한 발신지 IP 주소에서 초당 수만개의 서로 다른 목적지 IP 주소로, 동일한 서비스 번호로 전송
- ✓ 이러한 패턴은 전형적인 SCAN 트래픽 패턴(즉, 어떤 서비스를 OPEN하고 있는 호스트를 찾는 행위)

▣ **NXG Series** 에서 "SCAN 공격자 팀지 및 방어" 기능을 활성화하면 다음과 같이 동작
- ✓ 단, 10개의 초기 발생 패킷의 패턴을 통해 감지하고, SCAN 패턴의 트래픽을 발생시키는 발신지 IP 주소를 커널 상의 블랙리스트에 설정된 차단 시간과 함께 전달
- ✓ 커널 상의 블랙리스트는 **NXG Series**에 패킷 인입 시 최초로 비교되는 리스트로서, 해당되는 패킷은 방화벽에 진입하지 못하고 설정된 차단 시간 동안 삭제

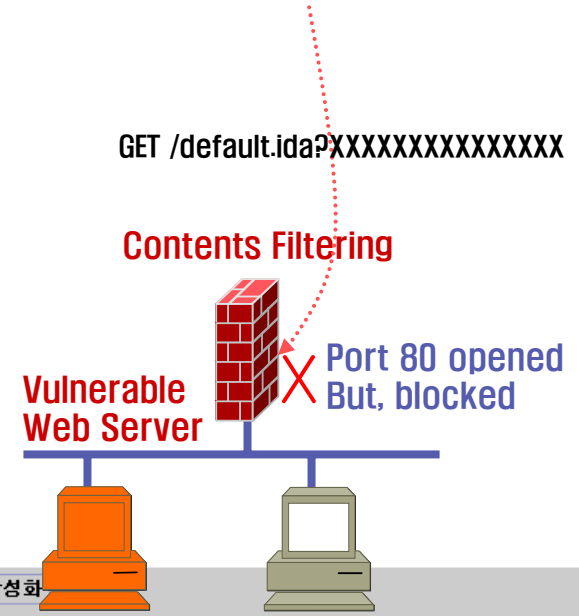


NXG 4000 – 유해트래픽 차단(IPS)

WEB 취약점 차단 기능

▣ 가장 Popular 한 웹 취약점 공격
- ✓ UNICODE Bugs
- ✓ CGI-Vulnerability
- ✓ Code-Red, Nimda WORM 전파 경로
- ✓ "한게임"에 대한 시큐브레인 IDS 설치 결과 50,297건 탐지 결과 중, 웹 취약점 공격이 47,949 건

▣ 취약한 웹 서버의 운영 위험
- ✓ Code-Red, Nimda 및 이들의 30여 가지 변종의 전파 기지로 전락
- ✓ 웹 서버 변조
- ✓ 방화벽 정책으로는 차단할 수가 없음
- ✓ 취약점 리스트는 자동 Update



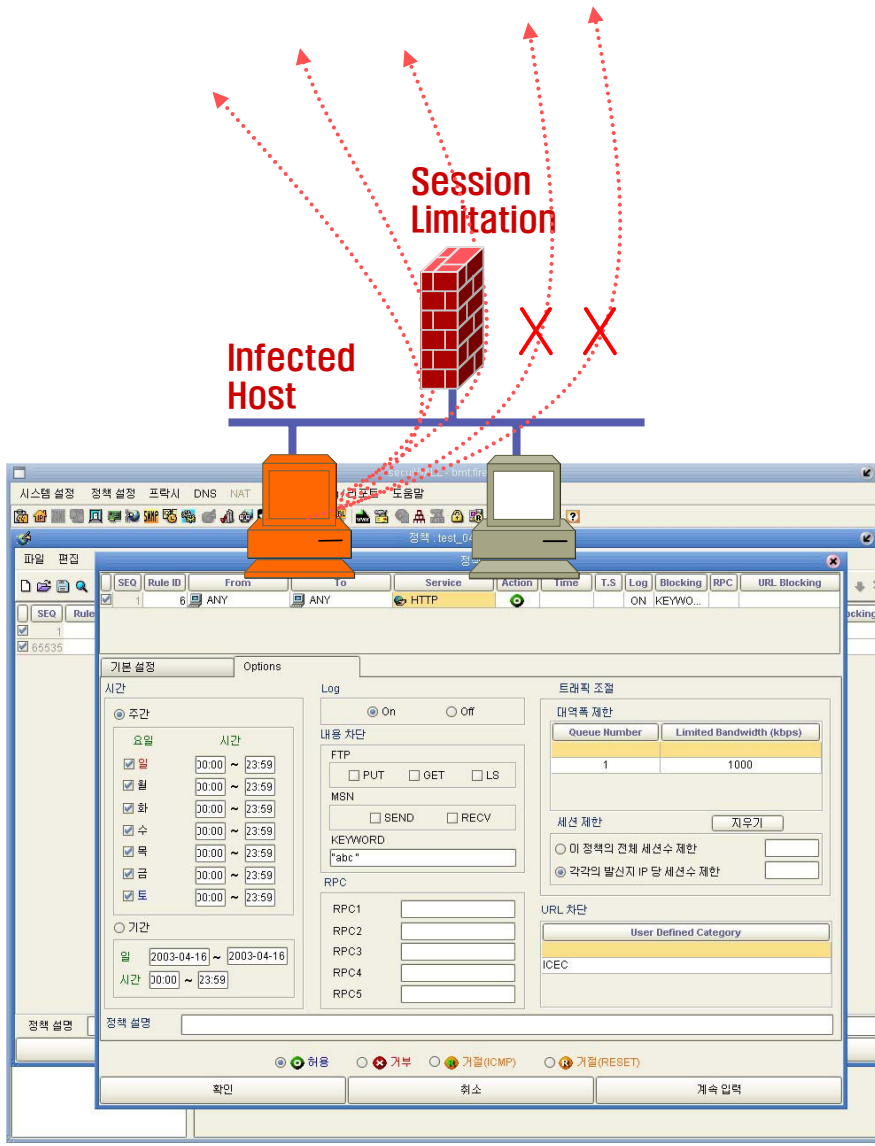
CGI 취약점 차단 활성화

Blocking	Blocking Expression	
✔	%dg%o0%ae%dg%o0%ae%dg%o0%ae%dg%o0%ae	UNICODE Bugs - "/scripts/%dg%o
✔	%dg%o0%9u%dg%o0%9u%dg%o0%9u%dg%o0%9u	UNICODE Bugs - "/scripts/%dg%o
✔	%dg%o0%qe%dg%o0%qe%dg%o0%qe%dg%o0%qe	UNICODE Bugs - "/scripts/%dg%o
✔	%u0%80%ae%u0%80%ae%u0%80%ae%u0%80%ae	UNICODE Bugs - "/scripts/%u0%8
✔	%u0%80%qe%u0%80%qe%u0%80%qe%u0%80%qe	UNICODE Bugs - "/scripts/%u0%8
✔	%u0%80%9u%u0%80%9u%u0%80%9u%u0%80%9u	UNICODE Bugs - "/scripts/%u0%8
✔	%u0%7g%ae%e0%7g%ae%e0%7g%ae%e0%7g%ae	UNICODE Bugs - "/scripts/%u0%7
✔	%u0%7g%9u%e0%7g%9u%e0%7g%9u%e0%7g%9u	UNICODE Bugs - "/scripts/%u0%7
✔	%u0%7g%qe%e0%7g%qe%e0%7g%qe%e0%7g%qe	UNICODE Bugs - "/scripts/%u0%7
✔	%u0%o0%ae%e0%o0%ae%e0%o0%ae%e0%o0%ae	UNICODE Bugs - "/scripts/%u0%o
✔	%u0%o0%9u%e0%o0%9u%e0%o0%9u%e0%o0%9u	UNICODE Bugs - "/scripts/%u0%o
✔	%u0%o0%qe%e0%o0%qe%e0%o0%qe%e0%o0%qe	UNICODE Bugs - "/scripts/%u0%o
✔	/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNN...	Notice! Code Red pattern
✔	/default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXX...	Notice! Code Red II pattern
✔	root.exe?/c+dir	NIMDA or Other scanning pattern
✔	cmd.exe?/c+dir	NIMDA or Other scanning pattern

세션 제한 기능

▣ WORM 피해의 주된 특징
- ✓ 세션 폭주에 따른 장애
- ✓ 동일 발신지 주소에서 많은 세션이 생성
- ✓ 세션 제한 기능으로 효과적 대처가 가능

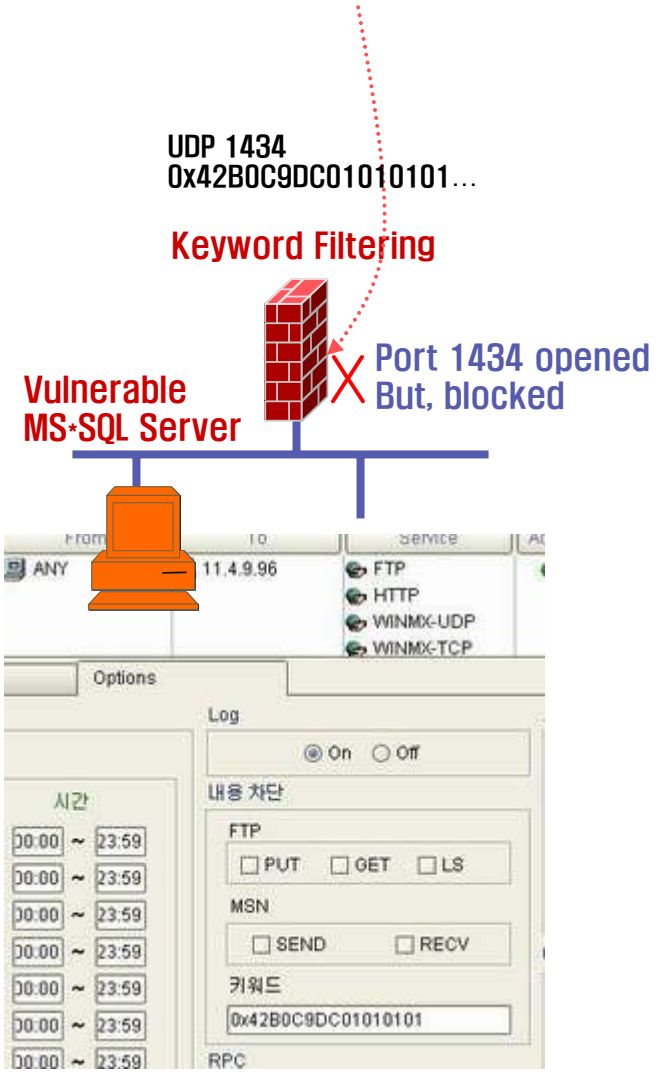
▣ **NXG Series**의 세션 제한 기능
- ✓ 정책과 무관하게 전체적으로 각 발신자 주소 당 정해진 Threshold 이상의 신규 세션은 차단
- ✓ 또는, 유연성을 위해 각 정책 별 총 세션 수를 지정하여, 발신지 주소와 무관하게, Threshold 이상의 신규 세션들을 차단
- ✓ 정책별로 각 발신지 주소별 Threshold 설정 역시 가능



NXG 4000 – 유해트래픽 차단(IPS)

Keyword Filtering 기능

- ▣ Slammer WORM과 같은 80번 이외의 공격
  - ✓ WORM의 특징 String을 이용하여, Contents Filtering
  - ✓ Slammer WORM의 경우:
    "0x 42 B0 C9 DC 01 01 01 01"로 시작
  - ✓ KT망에 폭주했던 DNS Inverse Query에 대한 선택적 차단 역시 가능
    "in-addr" 문자열 필터링
  - ✓ Telnet, NNTP 등에서 특정 명령어 차단 가능
- ▣ **NXG Series** 의 정책별 키워드 Filtering 기능
  - ✓ 각 정책별로 설정 가능하여, 유연성 확보 및 문제시되는 특정 트래픽 이외의 트래픽에 대한 품질 보장
  - ✓ 임의의 ASCII 단어 및 문자열
  - ✓ 임의 크기의 "0x"로 시작하는 HEXA 값

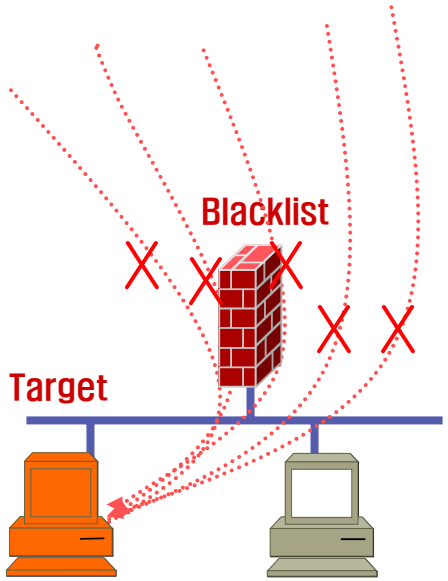


NXG 4000 – 유해트래픽 차단(IPS)

DDoS 방어 기능

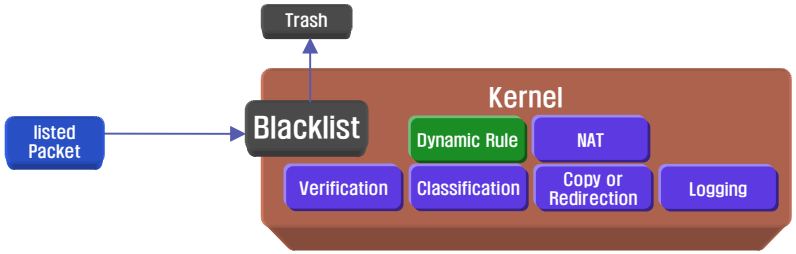
▣ 패턴 분석을 통한 각종 DDoS 방어 기능

- ✓ SYN Flooding 공격 탐지 및 차단
- ✓ Ping Flooding 공격 탐지 및 차단
- ✓ UDP Flooding 공격 탐지 및 차단
- ✓ DNS 질의 공격 탐지 및 차단
- ✓ 잘못된 Fragmented Packet을 이용한 공격 차단
- ✓ Ping of Death 공격 차단
- ✓ Smurf 공격 차단



▣ **Black-List의 활용**

- ✓ 모든 패킷들이 방화벽 진입 즉시 블랙리스트와 비교됨
- ✓ 블랙리스트에 의한 차단은 방화벽에 거의 부하를 주지 않음
- ✓ 위 DDoS 방어 기능에 의해 검출된 패킷은 블랙리스트에 일정 시간(기본값 60초)과 함께 등록되어, 해당 패킷들은 주어진 시간동안 차단

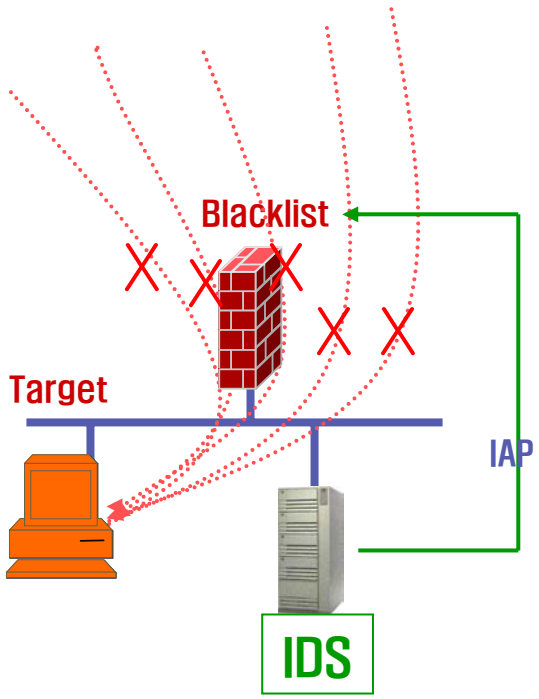


NXG 4000 – 유해트래픽 차단(IPS)

기타 패킷 필터링 및 IDS 연동

▣ 의심스러운 모든 패킷의 차단
- ✓ 내부망 IP 주소를 가지고 외부에서 들어오는 패킷들의 차단
- ✓ RFC 1918 등록된 비공인 IP 주소를 발신지로 한 패킷들의 차단
- ✓ 존재할 수 없는 발신지 IP 주소의 패킷들을 차단
  255.255.255.255, 127.0.0.1 …
- ✓ LAND 공격성 패킷들의 차단
- ✓ Source Port와 Destination Port가 같은 TCP 패킷들의 차단
- ✓ ICMP Destination Unreachable 패킷 차단
- ✓ Source Route Option IP 패킷 차단

▣ **IDS 연동**
- ✓ IAP(Internet Alert Protocol)을 이용
- ✓ 국산 5개사 IDS 제품과 연동 테스트 성공
- ✓ 블랙리스트를 이용한 효과적 차단



NXG 4000 – VPN

FastIKE

- ✓ **Active-Active Dual Line VPN** 구성 지원 :
  N * M 회선에서 가상 **Tunnel**을 동시에 생성하여 **Multipath IPsec Load-Balancing** 하는 기능
- ✓ **Privacy Enhanced Routing Config** 지원 :
  Default Routing이 내부 **Private Network**으로 지정할 경우에도 정상적인 **Key**교환 가능
- ✓ **DPD** 표준 지원
- ✓ **Zero-Packet Loss SA Rekeying** 지원
- ✓ **Perfect Forward Secrecy** 지원:
  - **DH Group 1, 2, 5**
- ✓ **PSK(Pre-shared Key), X.509** 인증지원**(PKI)**
- ✓ **X-Auth** 지원
  - **LDAP** 인증 , **RADIUS** 지원
- ✓ **VPN Client IP Pool** 할당기능

TrustCA

- ✓ **CA server** 내장
- ✓ 하드웨어 방식의 암호키 저장
  해커의 물리적인 탐지에도 안전한 키 보관
- ✓ 자동 인증서 발급 메카니즘 탑재
- ✓ **X.509 v3 Certificate** 지원
  - **Verisign, Entrust certificate**호환
  - 국내인증기관 인증서 지원
    한국전자인증,
- ✓ **External** 인증서버 지원
  - **RADIUS**
  - **LDAP**
  - **OCSP**

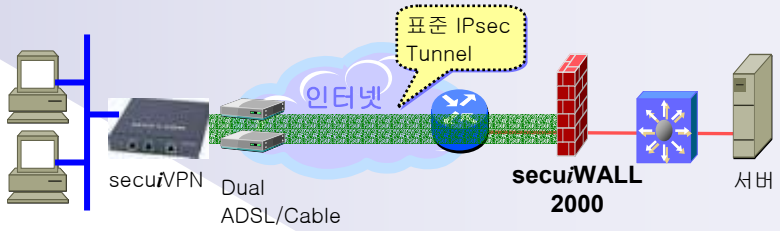
NXG 4000 – VPN

RobustIPSec

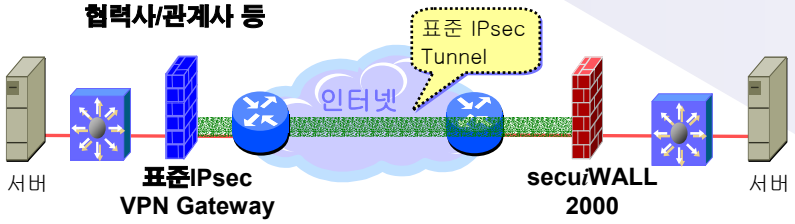
- ✓ IPSec 국제표준 준수
- ✓ 50,000 동시 터널
- ✓ Transport / Tunnel Mode
- ✓ 암호화 알고리즘
  - 3DES, DES, AES : 고성능 HW 암호화
  - Blowfish, CAST128, SEED : SW 암호화
- ✓ 인증 : SHA-1, MD5
- ✓ Multipath IPsec 지원
  IPsec에서 Packet 단위 Load-Balancing 지원
  N * M 회선을 이용한 회선 대역폭 확장 가능
- ✓ DPD(Dead Peer Detection) 표준 기능 지원 :
  장비 Rebooting, SA 삭제 등에 즉각적인 Re-keying
- ✓ DLD(Dead Link Detection) 기능 지원:
  Multipath IPsec 구성시 path 단절을 감시
- ✓ Split-tunneling 지원

Access VPN

Intranet VPN



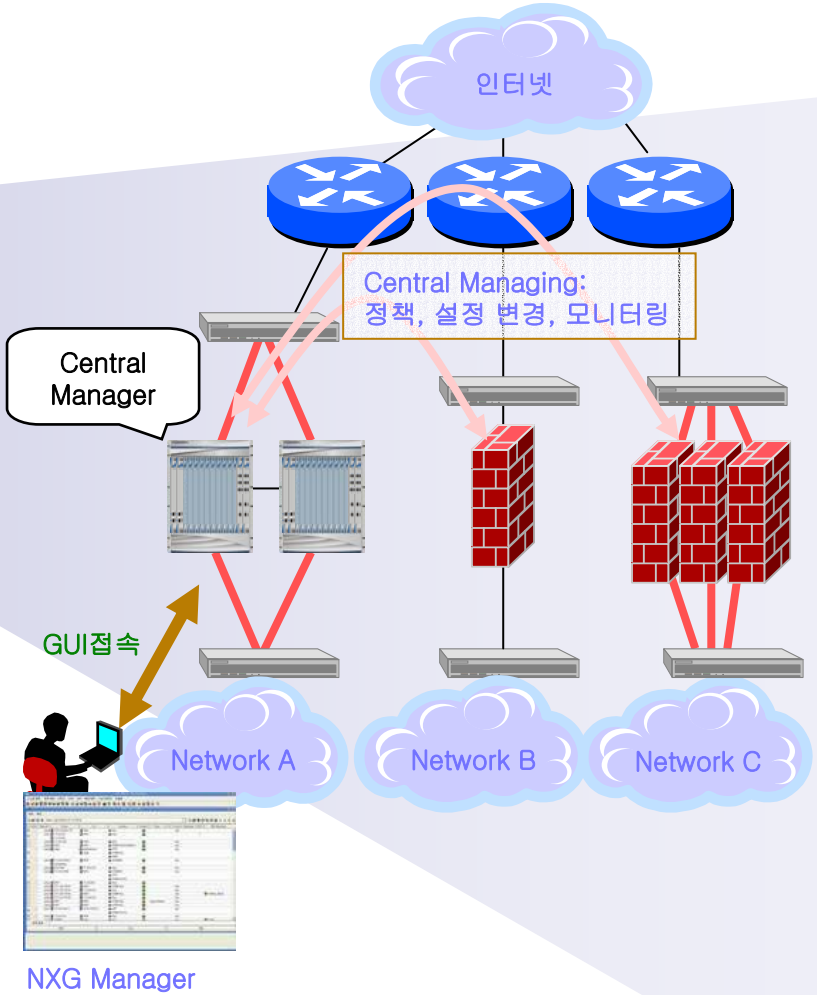
Extranet VPN



NXG 4000 – 주요 기능

Enterprise Manager

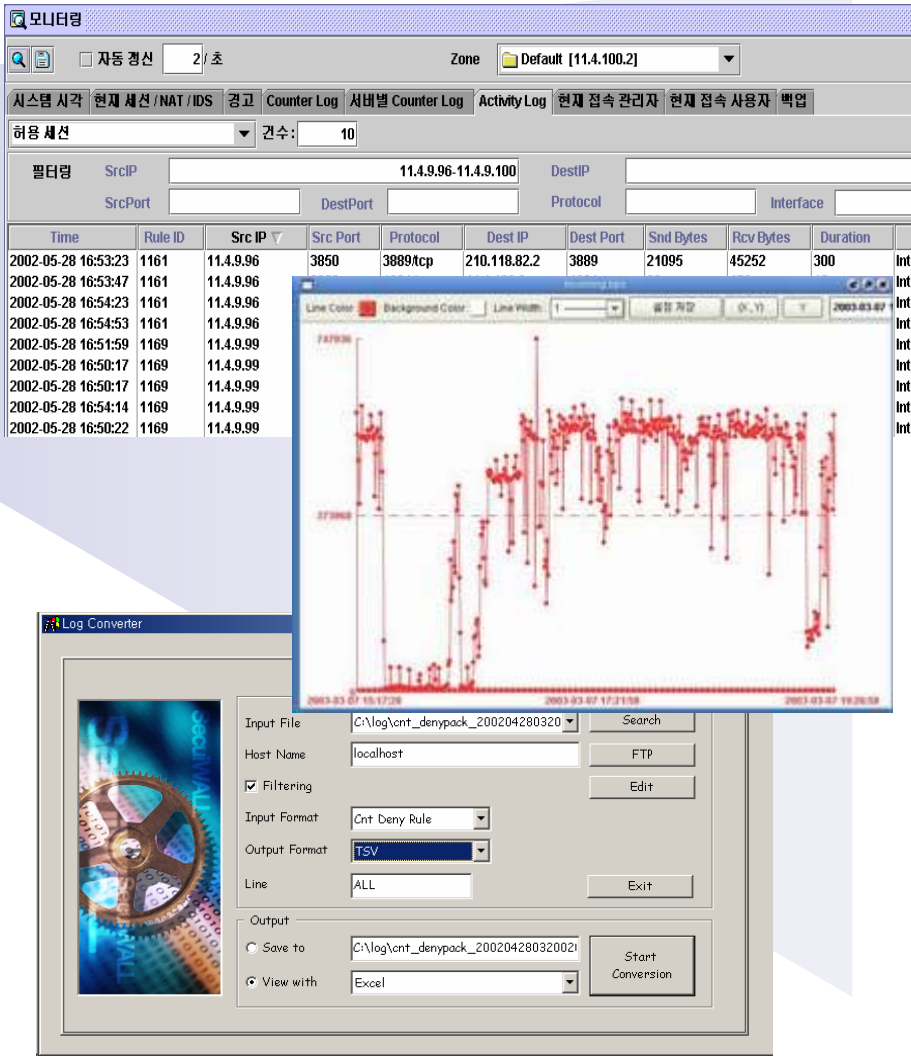
- ✓ 원격지에 분산 설치된 여러 대의 NXG Series를 그룹화하여 중앙에서 집중관리
- ✓ 정책 중앙 설정 및 관리
  - 관리대상 방화벽에 대해 일괄적용
  - 각기 상이한 정책에 대해 개별적용
  - 정책 설정 시 객체 검색 가능
  - 객체 설정 시 Sorting 기능
- ✓ 서비스별 Timeout 기능
  - Telnet 또는 FTP와 같이 IDLE 시간이 긴 세션들에 대한 차별적인 연장 가능
- ✓ Java를 사용하여 관리자 콘솔의 Platform과 무관한 Remote Control
- ✓ SSL 암호화를 통한 관리 데이터 보호
- ✓ 다국어 지원(한국어, 영어, 일본어, 중국어) : HTML 형태의 다국어 도움말 지원
- ✓ CLI모드 하에서의 콘솔 및 SSH를 이용한 관리 기능



NXG 4000 – 주요 기능

Logging

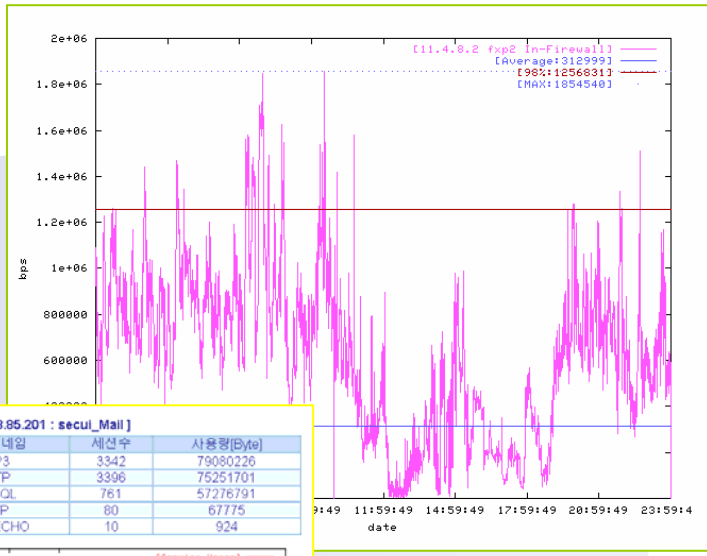
- ✓ Activity Log
  - 세션 단위 로그 (*NOT* Per Packet Log)
  - HTTP 프락시, 메일, URL 차단
  - NAT, 관리자, 사용자 인증, 사용자 활동
  - IDS 연동 결과, 거부된 패킷
- ✓ Counter Log
  - 거부 또는 허용된 Packets/Bytes/Session 수
  - 인터페이스별 Packet수 Byte수 및 BPS
  - HTTP, Reverse HTTP Proxy를 통한 Bytes 수
  - 메일 수.발신 건수, 메일 폐기건수, URL 차단건수
  - CPU/Memory 평균 사용율
  - Traffic 조절 건수
  - 특정 프로세스 CPU 점유율, 디스크 사용량
- ✓ Log File 형식 : Binary, CSV, TSV, WELF
  - Log 파일 자동 압축 및 FTP 자동 전송 지원
- ✓ 실 시간 Graph Monitoring 및 Off-Line Log 분석기 제공
  - 다양한 검색 조건에 따른 Filtering 제공
  - 각 Field 별 실 시간 Sorting 제공
  - Graph로 표시
- ✓ Log의 Network Syslogd전송기능 : ESM 연동 가능



NXG 4000 – 주요 기능

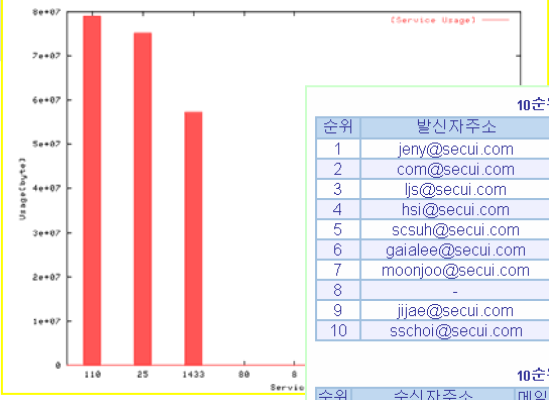
Report

- ✓ 리포팅 생성
  - 주기적 생성 : 일간-시간,주간-날짜/시간
  - 즉석 생성 : 대상 로그 범위를 지정
- ✓ 리포팅 종류 : Format HTML
  - 해킹시도 탐지 결과
  - 패킷허용 및 차단건수
  - 패킷차단 내역
  - 설정된 서비스별 Top 10 사용자
  - Top 10 사용자/서비스
  - 시스템 문제상황
  - 네트워크 사용율
  - 최다 사용 Web Site 및 사용자
  - 최다 차단 Web Site 및 사용자
  - 최다메일 사용자 및 차단메일
  - 부하분산 내역
  - 각 Queue별 트래픽 조절 결과
  - 설정된 호스트들의 서비스 사용량
  - IDS 연동 결과
- ✓ 관리자 Email로 리포트 자동 전송



[210.118.85.201 : secui_Mail]

서비스포트	서비스 네임	세션수	사용량[Byte]
110	POP3	3342	79080226
25	SMTP	3396	75251701
1433	MS-SQL	761	57276791
80	HTTP	80	67775
8	ICMP-ECHO	10	924



10순위 메일 트래픽 발신자

순위	발신자주소	메일Size[Byte]	최대수신자주소
1	jeny@secui.com	25785344	wonpoet@coponet.com
2	com@secui.com	21515968	com@orgio.net
3	ljs@secui.com	10700800	sskwon@thinkm.co.kr
4	hsi@secui.com	4233216	auditor@i39.co.kr
5	scsuh@secui.com	2283520	scsuh@korea.com
6	gaialee@secui.com	1804288	sae@youngjin.com
7	moonjoo@secui.com	1414172	ytcha@samsung.co.kr
8	-	1224524	jijae@samsung.co.kr
9	jijae@secui.com	402432	zzlee@hynix.com
10	sschoi@secui.com	380019	thkim@idcc.co.kr

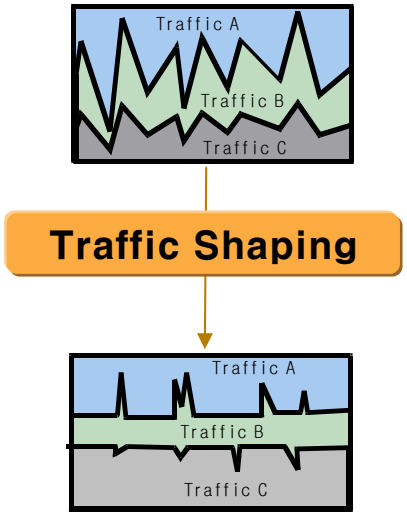
10순위 메일 트래픽 수신자

순위	수신자주소	메일Size[Byte]	최대발신자주소
1	jijae@secui.com	619000	jijae@samsung.co.kr
2	whan92@secui.com	569300	stillnow@empal.com
3	kotaeji@secui.com	490356	owner-ips@ece.cmu.edu
4	gslim@secui.com	387558	trend@kisti.re.kr
5	carnival@secui.com	285382	root@ha1.secuiwall.com
6	ridia@secui.com	274920	mmsc@wealthia.com
7	tachyon@secui.com	269994	Report_Program@firewall.hpcnet.ne.kr
8	hnam@secui.com	217858	zizibebe@itsbank.net
9	boani@secui.com	210267	impexp@formil.com.br
10	webloving@secui.com	176101	dots@edots.co.kr

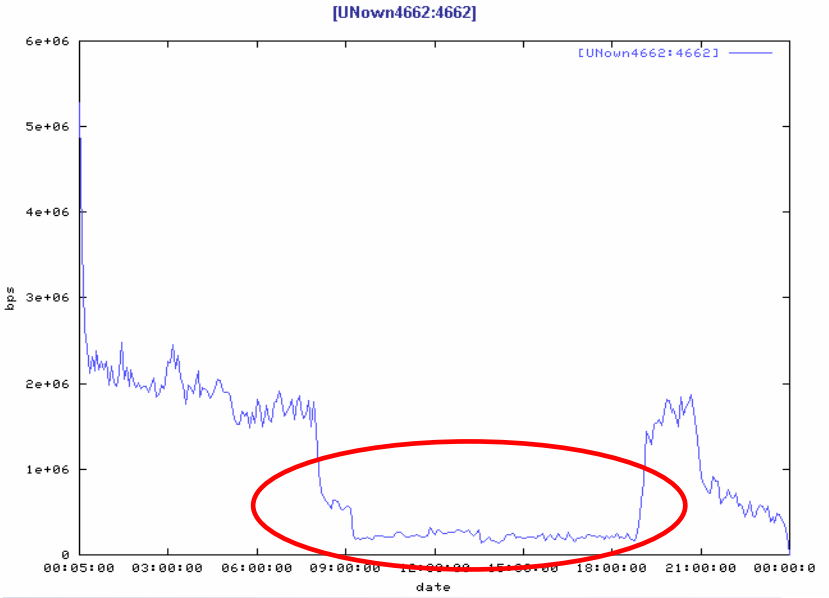
Traffic Shaping

✓ 특정 정책에 해당하는 트래픽의 대역폭 제한을 통한 한정된 대역폭에 대한 효율적 사용 및 회선비용 절감

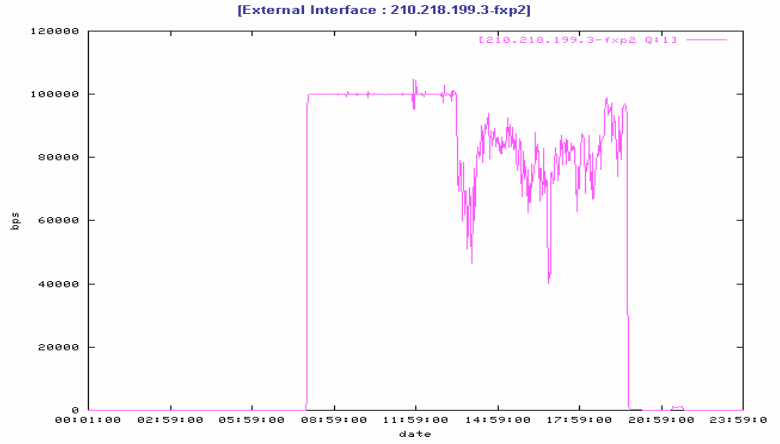
- 업무용 트래픽과 비업무용 트래픽을 구분하여 우선순위에 따른 대역폭 할당 : 비업무용 트래픽의 대역폭 과다점유 문제 해결
- VoIP와 같이 실시간성이 보장되어야 하는 트래픽에 대한 안정적인 대역폭 확보



Traffic Shaping에 의해 제한 받는 Application의 사용률 Report



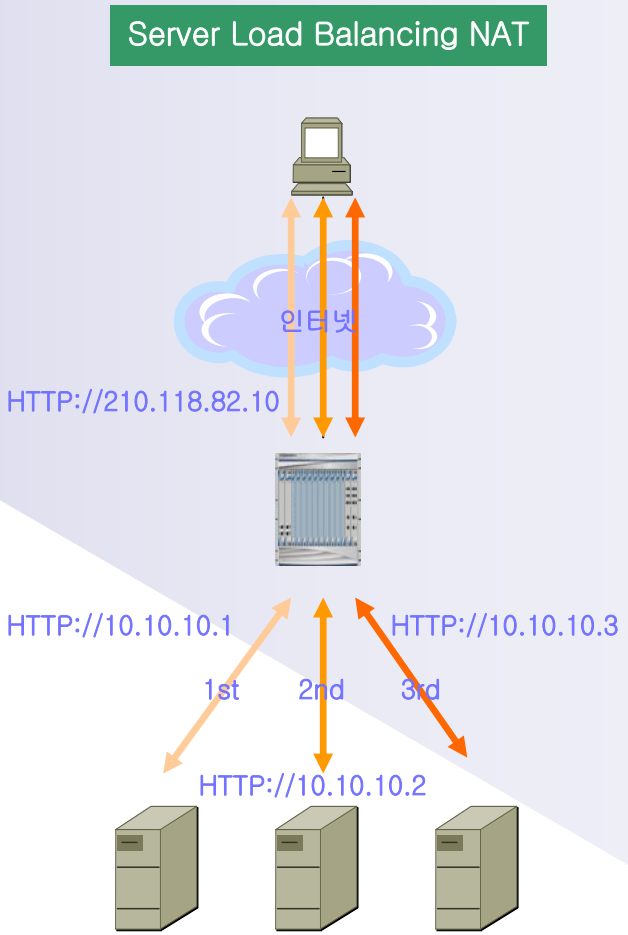
Traffic Shaping 결과 Report



NXG 4000 – 주요 기능

NAT

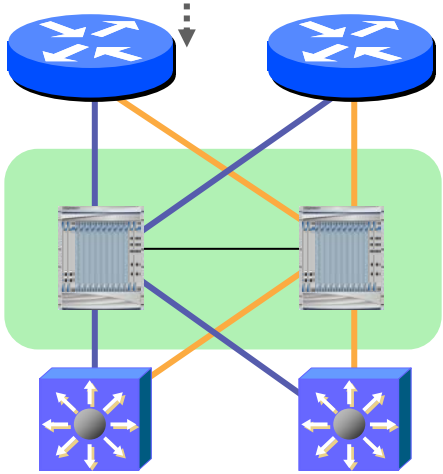
- ✓ 내부 IP Address정보 보안 및 공인 IP Address자원 절약
- ✓ 지원 Application
  - FTP, DialPAD, WOWCall
  - VoIP(H.323 V4)
  - MSN File 송수신, 음성 채팅
  - Windows Media Player, Real Player G2
- ✓ 형태
  - Static NAT : 내부 비공인 IP Address를 외부 공인 IP Address로 1:1 Mapping
  - Dynamic NAT : 한정된 공인 IP Address를 Pool방식으로 M:N Mapping
  - PAT : 단일 공인 IP Address에 대한 M:1 Mapping
  - SLB(Load Share Network Address Translators) : 네트워크 트래픽이 특정 서버에 집중되지 않고 여러 개의 서버 풀에 분산되도록 하는 "로드 공유" 기능을 기반으로, 네트워크 주소를 변환

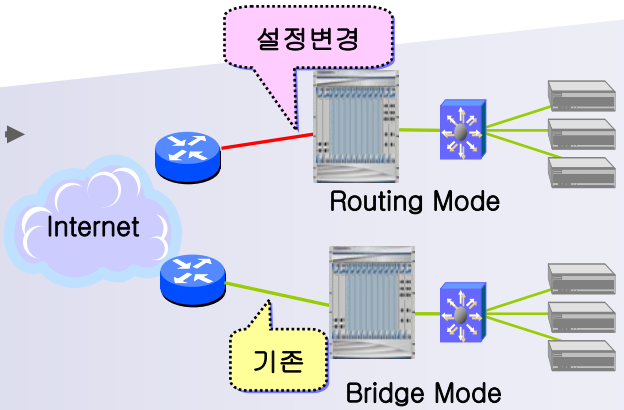


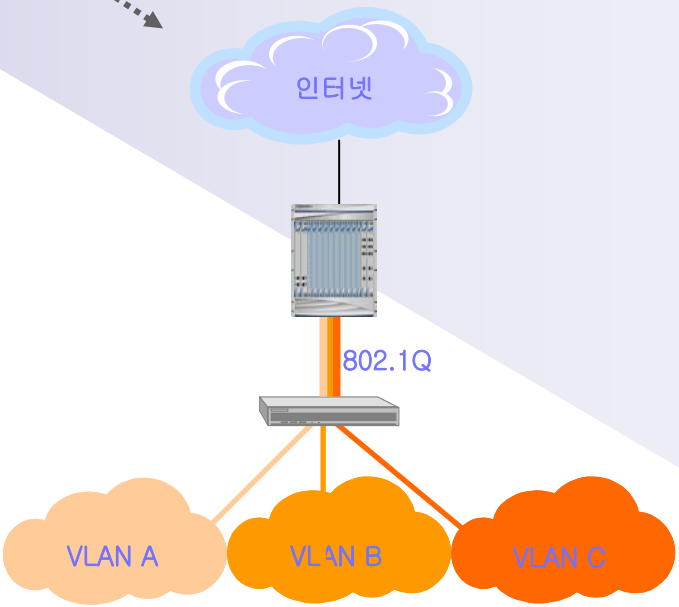
NXG 4000 – 주요 기능

Network 연결

- ✓ Bridge(Transparent) Mode 구성 지원으로 기존 네트워크 설정 변경 없이 손쉽게 설치
- ✓ VLAN 802.1q Trunk 지원 : 각 인터페이스에 대한 Sub Interface 구성
- ✓ External, Internal, DMZ 각각에 대해 Multiple Interface 지원(총 16개 10/100 포트 또는 4개 1Gbps 포트)

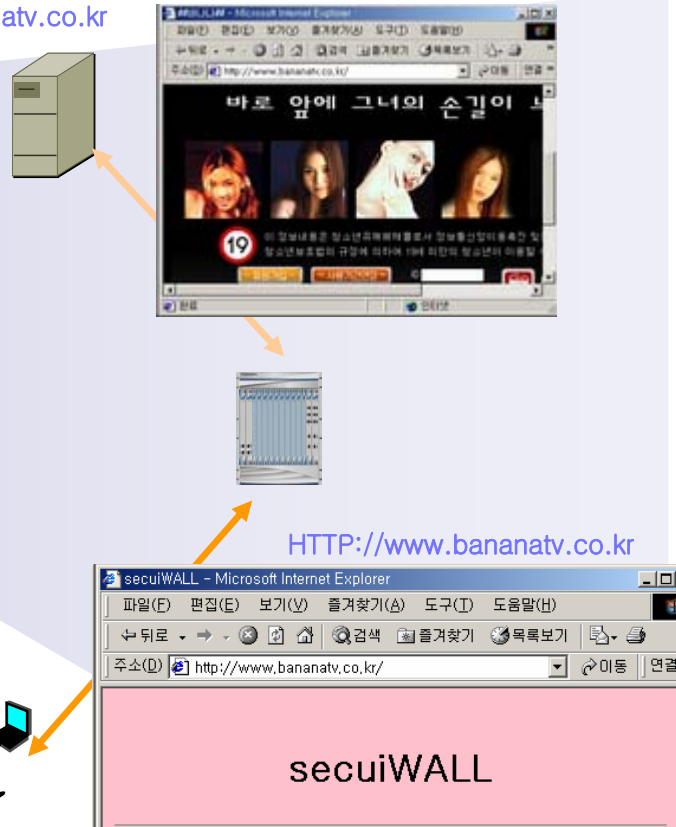






URL Filtering

- ✓ URL Filtering ; 유해 사이트 접속차단
- ✓ 기업내부의 보안정책에 의해 접속이 금지된 사이트 리스트를 Category화
  - 사용자 정의 차단목록 정의 기능
  - 정보통신 윤리위원회(ICEC, Information Communication Ethics Committee) 유해 사이트 목록 기본 탑재(약 30만건, 주1회 자동 Update)
  - 사용자가 URL을 이용하지 않고, DNS를 통해 알아낸 IP Address로의 접속 역시 차단



URL 차단 건수: 3

필터링 SrcIP DestIP SrcPort DestPort Protocol

Time	Src IP	Dest IP	URL
2002-05-28 16:35:47	11.4.9.99	66.40.23.81	www.kgirls.com
2002-05-28 16:35:47	11.4.9.99	66.40.23.81	www.kgirls.com
2002-05-28 19:04:17	11.4.9.96	211.115.220.21	www.bananatv.co.kr

NXG 4000 – 부가 기능

Secure Proxy

✓ 메일 보안
- 각종 광고성 메일 차단 ([광*고], [과앙고],[광~~고] ...)
- 수발신 메일크기 제한
- 메일주소/키워드 필터링
- 첨부파일의 바이러스 유무 검사, 치료 (V3, ViRobot, Norton Anti-Virus 지원)
- SPAM 메일 방지

✓ HTTP 보안
- 내부사용자는 웹 브라우져 상의 설정 변경 없이 Web 사용
- Java/VB Script, Java Applet, ActiveX 차단
- 기업 내부정보 유출방지를 위해 Web Posting Restriction 기능
  - -파일첨부 금지
  - -Posting Size 제한
- Thread 방식을 이용 성능 향상
- Reverse HTTP Proxy를 통한 Contents Distribution, Contents Server Load Balancing

Alarm/SNMP

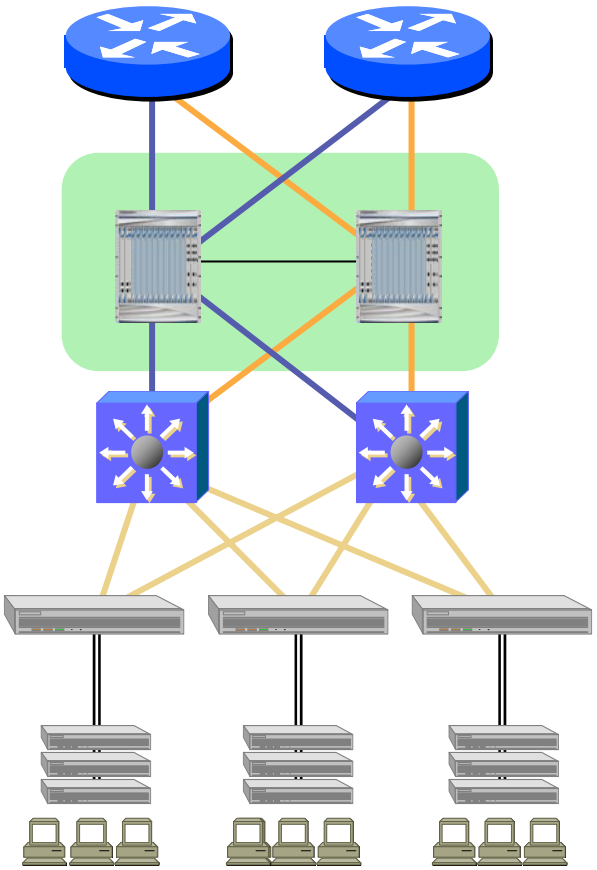
✓ 시스템 문제상황에 대한 경고 설정
- CPU 및 Memory 과다 사용
- 과다한 트래픽 및 세션 발생
- 파일시스템 포화 경고
- 인터페이스의 Down, 비정상적인 트래픽 발생
- 과다한 로그 및 NAT 변환 등등

✓ SNMP지원을 통한 NMS(예 : HP OpenView)연동 기능
- 모든 Counter Log에 대해 별도의 MIB 지원
- 경고에 대해서는 지정한 SNMP서버에 Trap 발생

참고자료 – HA Config.(Bridge Mode)

구성도

• With secuiWALLs configured as bridge Active-Active HA mode



부하분산

✓ 각 라우터 들과 Core L3 Switchs간에 상호동작 중인 부하분산을 지원하는 라우팅 프로토콜(OSPF;Open Shortest Path First, EIGRP; Enhanced Internet Gateway Routing Protocol 등)에 의해 트래픽을 분산

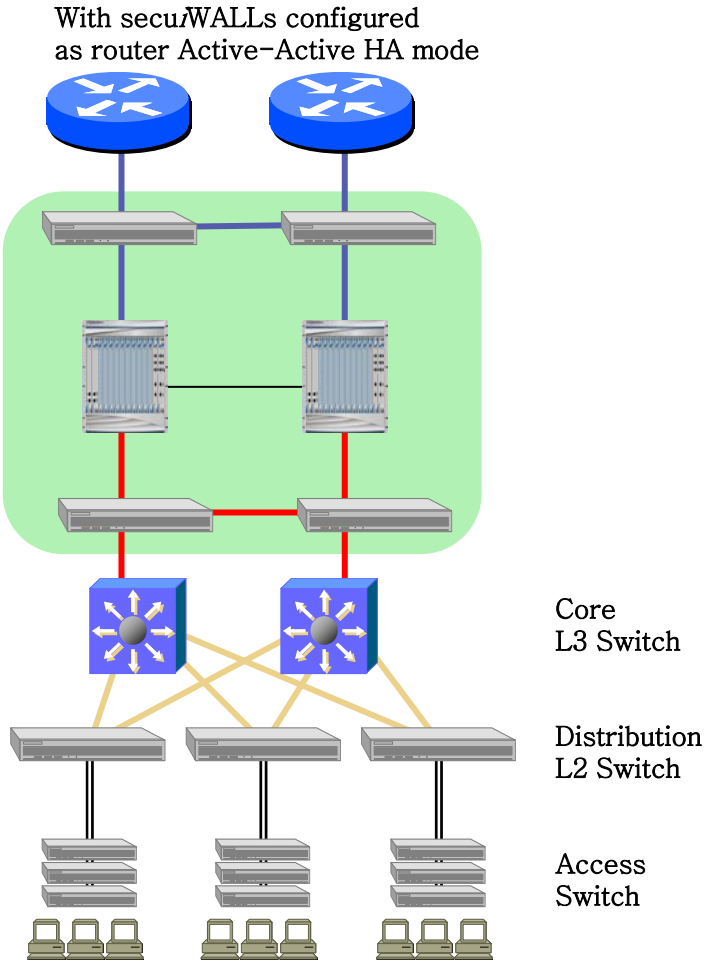
✓ Bridge Mode의 secuiWALL은 라우팅 프로토콜 패킷을 Transparent하게 통과

장애대응

✓ 장애 발생구간은 라우팅 프로토콜에 의해 자동 인식되며, 이를 패킷전송경로에서 자동삭제 한다.

참고자료 – HA Config.(Router Mode)

구성도

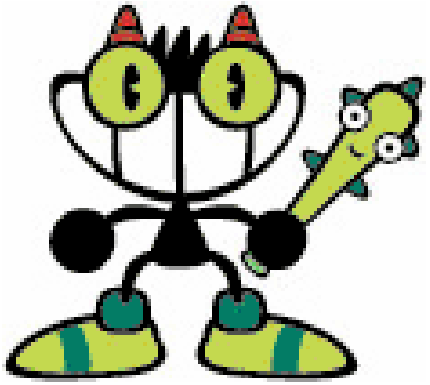


부하분산

- ✓ Routers - Core L3 Switchs - secuiWALL간에 부하분산을 지원하는 라우팅 프로토콜인 OSPF;Open Shortest Path First를 설정하여 트래픽 분산
- ✓ OSPF를 이용하지 않을 경우, 동일 Metric Static Route 부하분산을 이용

장애대응

- ✓ 장애 발생구간은 OSPF 라우팅 프로토콜에 의해 자동 인식되며, 이를 패킷 전송경로에서 자동삭제
- ✓ Static 경로 이용 시에는 “가상IP주소기법”을 이용



감사합니다.