스팸메일차단 솔루션 제안서

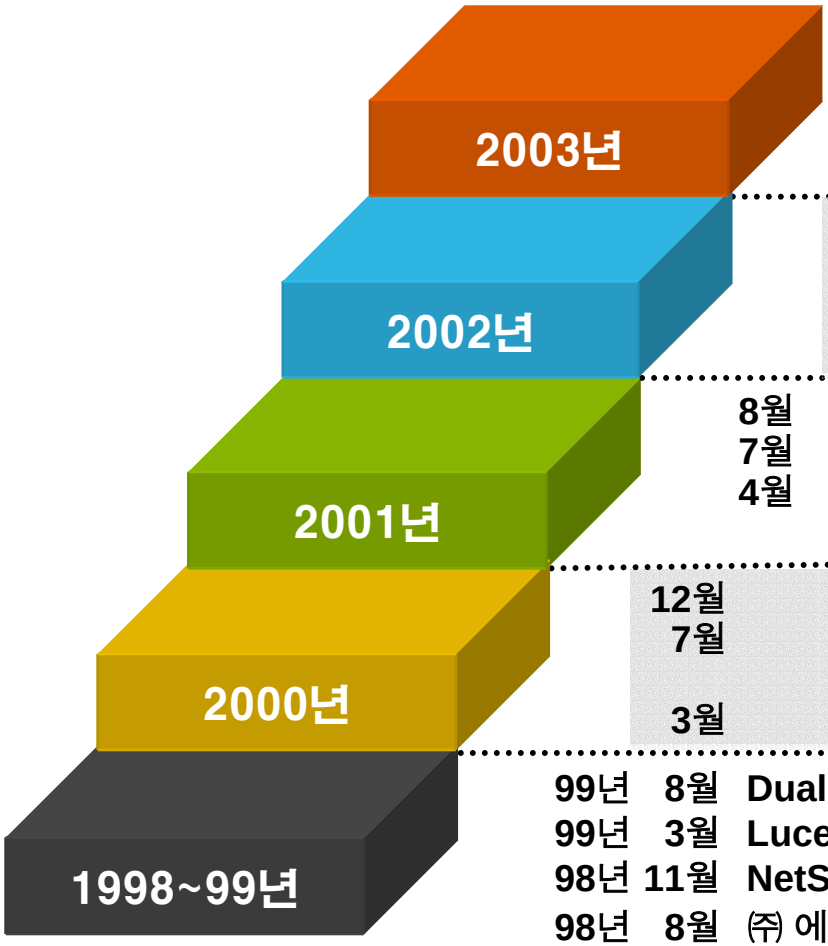
2003. 4

FNET ㈜에프넷트

Free & Safe Networking

* 목차 *

회 사 명	㈜에프네트
대표이사	김 영 근
설 립 일	1998년 8월 4일
자 본 금	33 억 (KTB / 기술보증기금 투자 유치)
직 원 수	35 명
매 출 액	2000년 55억 / 2001년 56억 / 2002년 93억



2003년
- 4월 지란지교소프트와 전략적 파트너십 체결
- 3월 시스원과 전략적 파트너십 체결

2002년
- 11월 TopLayer와 비즈니스 파트너십 체결
- 8월 SpectraLink와 파트너십 체결
- 7월 중기청 해외개척지원사업 참가
- 5월 중국 인민군 보안인증 획득

2001년
- 8월 대만 특허 획득 (NetSwitch II-M)
- 7월 중기청 해외개척지원사업 참가
- 4월 중국 공안부 보안인증 획득 (NetSwitch, DualNET)

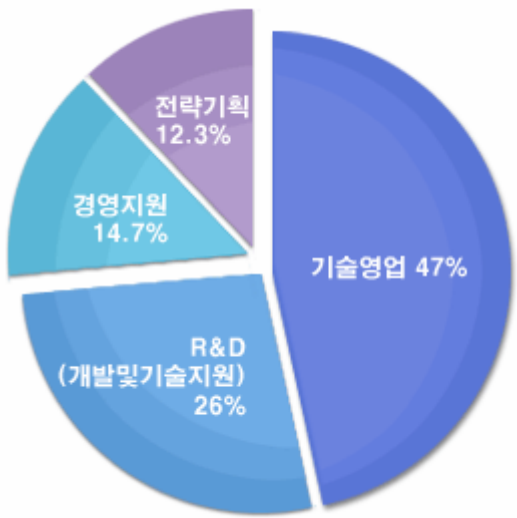
2000년
- 12월 AVAYA와 비즈니스 파트너쉽 체결
- 7월 KTB / 기보캐피탈 투자 유치
- 기술연구소 설립
- 3월 벤처기업 선정,중소기업청 우수기술기업 선정

1998~99년
- 99년 8월 DualNET 군 승인 획득
- 99년 3월 Lucent Technologies와 파트너십 체결
- 98년 11월 NetSwitch I, DualNET 개발
- 98년 8월 ㈜ 에프네트 설립

3. 조직구성


대표이사 (CEO)
전략기획부
영업 1부
영업 2부
해외영업부
기술연구소
경영지원부
외부감사

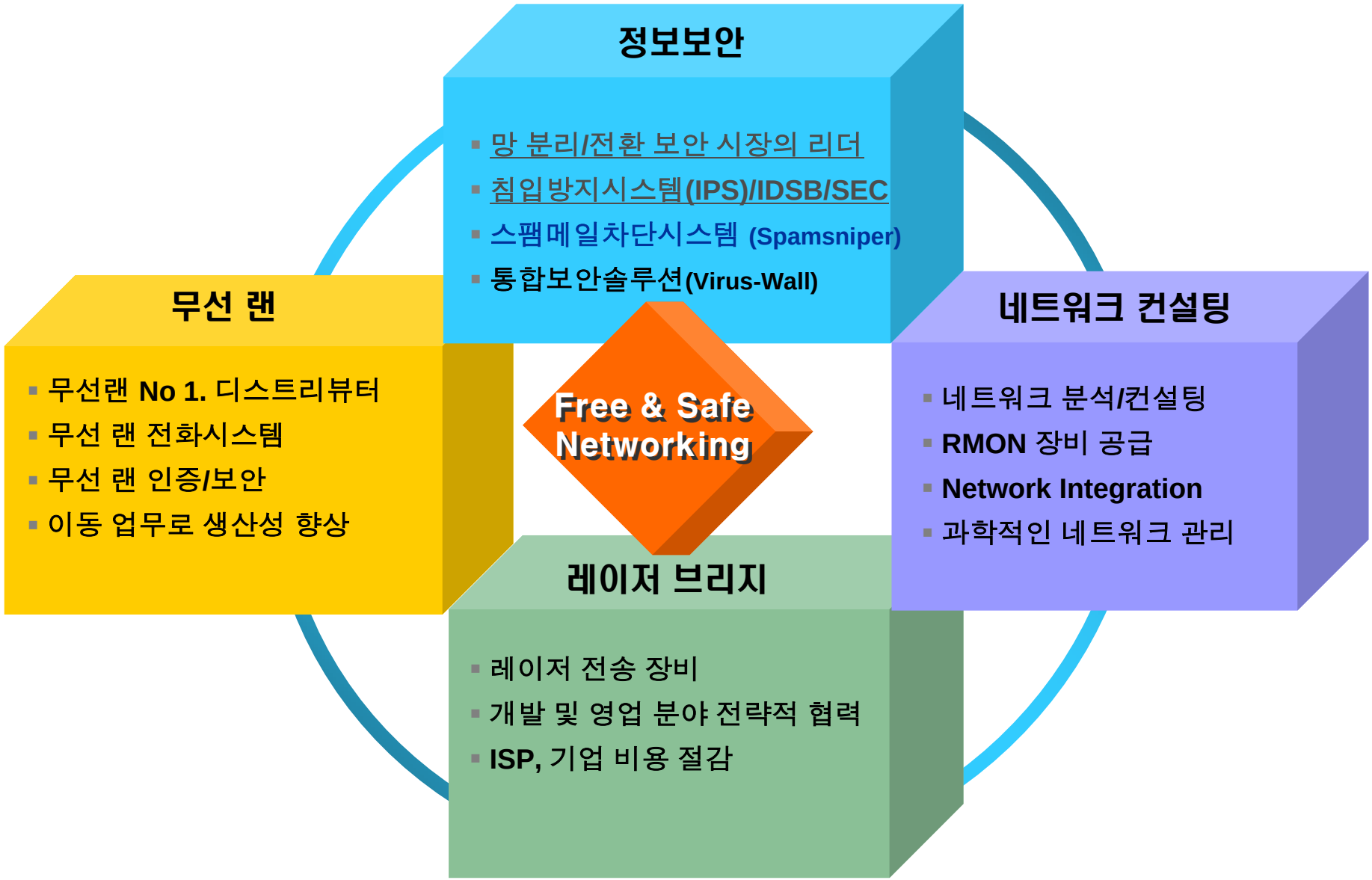
인력구성


전략기획
12.3%
경영지원
14.7%
기술영업 47%
R&D
(개발및기술지원)
26%

4. 기술보유현황

특허 현황	▪ **NetSwitch** 대만 특허 획득 ▪ **NetSwitch** 관련 국내 특허 출원 ▪ **NetSwitch** 관련 미국,일본,중국 특허 출원 ▪ **NetSwitch** 미국 특허 공고 중 ▪ **DualNET** 관련 국내 특허 출원
실용신안 등록	▪ **NetSwitch** 국내 실용신안 등록
상표등록	▪ **NetSwitch / DualNET**
인증	▪ 벤처기업지정 ▪ 기술신용 보증기금 우량 기술 기업 선정 ▪ **DualNET** 국방부 사용 승인 ▪ 중국 공안부 보안인증획득(**Netswitch Series** 포함 **6**개) ▪ 중국 인민해방군 보안 인증 획득(**Netswitch II-M, DualNET**)

5. 사업분야


정보보안
망 분리/전환 보안 시장의 리더
침입방지시스템(IPS)/IDSB/SEC
스팸메일차단시스템 (Spamsniper)
통합보안솔루션(Virus-Wall)
무선 랜
무선랜 No 1. 디스트리뷰터
무선 랜 전화시스템
무선 랜 인증/보안
이동 업무로 생산성 향상
Free & Safe Networking
네트워크 컨설팅
네트워크 분석/컨설팅
RMON 장비 공급
Network Integration
과학적인 네트워크 관리
레이저 브리지
레이저 전송 장비
개발 및 영업 분야 전략적 협력
ISP, 기업 비용 절감

SPAMSNIPER의 미래가 대한민국 MAIL보안의 미래입니다.

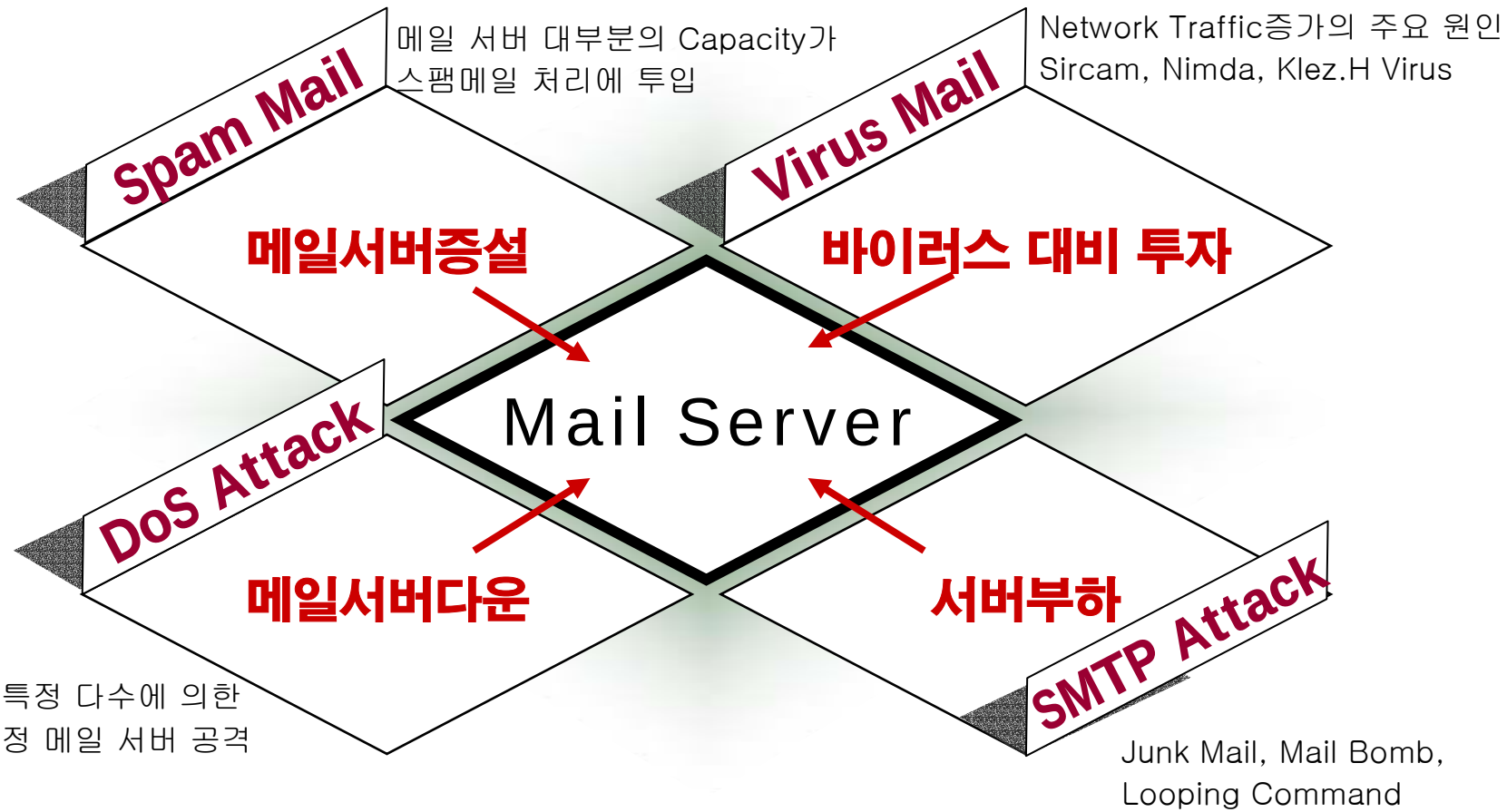
스팸메일차단 메일서버보호 바이러스차단 내부정보유출방지

spam sniper

SpamSniper 도입사

교육기관	서울대학교 충남대학교 안산1대학 공주교육대학교 광주과기원 연암원예축산대학 배재대학교 구미1대학 대구대학교
기 업	컴내꺼 대상정보기술 포스코 포스콘 링크웨어 애경유화 현대상선 침례병원 LG화학 지오다노 우리기술투자 동강무역 세아상역 한양ENG 등 30여개
금융권	동원증권 마이다스에셋
공공기관	한국전자통신연구원(ETRI) 대한설비건설공제조합 한국청소년보호위원회 대전교육과학연구원 국가보안기술연구소 한국해양연구원
제휴 서비스	안철수연구소 www.ahnlab.com : 보안클리닉제품 – MySpamsniper 공동서비스 오늘과내일 K.bis.NET : 스팸스나이퍼 기업ASP 호스팅 서비스 HanaFOS.com : 개인PC보안서비스(pc.hanafos.com) 청소년보호위원회 : 청소년을 위한 스팸메일 방지 캠페인

Mail Server 의 위협환경



왜 Spam차단솔루션을 도입해야 하는가?

스팸/바이러스 메일에 대한 메일서버 노출

도입 전

- 시스템 마비확률 높음
- 메일 서버 확장
- 네트워크 자원 낭비
- 시스템관리의 책임 증가
- 시스템관리자의 업무집중도 하락
- 종업원 업무효율 저하

도입 후

- **시스템 무정지**
- **메일 시스템 확장의 불필요**
- **Network 자원 보호**
- **중요 메일 자료 보호**
- **시스템 관리 비용 절감**
- **업무 시간 효율적 관리 가능**

SpamMail차단 솔루션 도입사례

C 대학

20,000 user 사용
일일 평균 메일 트래픽 5만 통

년간 110,069,778원의 시스템 비용 손실액을 절감하였음

* 바이러스 감염피해금액 미포함
시스템비용 : 스토리지비용+ 망사용료+H/W비용(H/W : Sun Enterprise 메일시스템 가격기준)

7일간 수신메일
전체메일 338,105개
정상메일 : 134,539개
스펨메일 : 234,443개
바이러스 메일 : 2,133개

일자	스팸메일		정상메일		바이러스메일		합계
15	25548	선택	7396	선택	177	선택	33121
16	29661	선택	16551	선택	928	선택	47140
17	36681	선택	22321	선택	295	선택	59297
18	38952	선택 선택	34351	선택 선택	161	선택 선택	73464
19	32387	선택	15764	선택	67	선택	48218
20	36270	선택 선택	21267	선택 선택	285	선택 선택	57822
21	34944		16879		220		52043

SpamMail차단 솔루션 도입사례

P 기업

1,000 user 사용
일일 평균 메일 트래픽 1만 통

년간 49,754,889원의 시스템 비용 손실액을 절감하였음

* 바이러스 감염피해금액 미포함
시스템비용 : 스토리지비용+ 망사용료+H/W비용(H/W : Sun Enterprise 메일시스템 가격기준)

1개월간 수신메일
전체메일 350,815개
정상메일 : 239,759개
스펨메일 : 114,510개
바이러스 메일 : 4,330개

일자	스팸메일		정상메일		바이러스메일		합계
01	3469	선택	3025	선택	28	선택	6522
02	5505	선택	12334	선택	203	선택	18042
03	6467	선택	12899	선택	690	선택	20056
04	4968	선택	10359	선택	373	선택	15700
28	4513	선택	6742	선택	164	선택	11419
29	3399	선택	4005	선택	10	선택	7414
30	5185	선택	13040	선택	117	선택	18342
31	4521	선택	12314	선택	103	선택	16938
합계	114510		231975		4330		350815

스팸차단 솔루션 도입 기대효과

스팸메일 차단 / 바이러스 차단 / 메일서버 보호

spam sniper

비용절감효과

스팸성 메일 처리를 위한 네트워크 및 메일서버 자원 낭비 방지

업무효율 향상

안전한 정상메일 수신 환경 확보

불건전한 메일차단으로 근무기강 확립

시스템관리 향상

Traffic통제관리

메일서버보호

Spam차단솔루션 도입 시 고려사항

차단기능이 다양한가?

- Inbound / Outbound 적용 되는가?
- Regular Expression이 적용되는가?
- 멀티서버/멀티도메인을 지원하는가?
- 그룹별/개인별 /서버별/도메인별 제각기 차단/허용 규칠설정이 가능한가?
- 외부 웹메일 차단기능도 제공하는가?

관리기능이 편리한가?

- 그룹별 /개인별로 정책설정이 자유로운가?
- 다양한 스마트업데이트가 되는가?
- 라이브 업데이트가 되는가?
- 다양한 통계기능이 지원되는가?
- 차단/허용 규칙 검색이 자유로운가?
- 차단메일 관리 기능이 다양한가?
- 체계적인 유지보수정책을 지원하는가?

안전한 구조인가?

- 동시처리 메시지가 최소 45call이상인가?
- CPU 부하율이 5% 미만인가?
- 대용량 메시지 처리가 가능한가?
- 시스템 모니터링 기능이 있는가?
- 타피팅기능이 되는가?
- SMTP세션 제어가 되는가?

Spamsniper란?

하드웨어 일체형의 스팸메일차단 시스템으로
스팸메일 차단, 바이러스메일 차단, 메일서버보호 역할을 합니다.
또한, 메일서버 앞단에 위치하여
프록시 서버와 Virus Wall 기능을 수행하여
들어오고 나가는 모든 메일에 대하여 통제·관리합니다.

spam sniper

Spamsniper의 특징

1 **개개인의 규칙설정이 가능합니다.**

- 개인별 / 그룹별 별도 규칙설정 및 통계관리가 됩니다.
- 예외적용이 자유롭습니다.

2 **Inbound / Outbound 메일 전체가 적용됩니다.**

- 들어오는 메일 / 나가는 메일에 대해서 별도 규칙설정 및 통계관리가 가능합니다.
- 전체 메일 트래픽 관리가 지원됩니다.

3 **멀티서버 / 멀티도메인이 지원됩니다.**

- 지원은 기본이며 도메인별 각각의 규칙설정 및 통계관리가 됩니다.

4 **다양한 스마트 기능이 있습니다.**

- 스팸메일 /바이러스메일에 대한 별도의 수동 update가 필요 없습니다.

5 **실시간 시스템 모니터링 기능이 완벽합니다.**

- 서버관리가 아주 용이합니다.

Spamsniper & 타사제품 비교

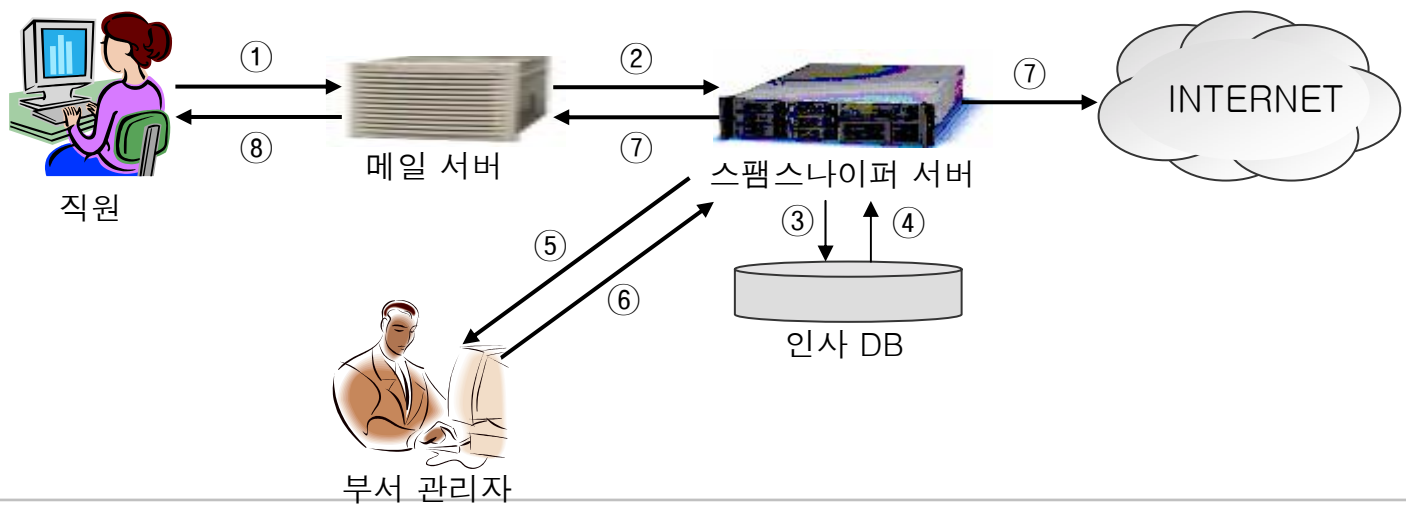
구 분	spam sniper	기존스팸차단 제품(A)	기존스팸차단 제품(B)	백신업체 바이러스월 제품
개인별 설정기능	O	O	X	X
Outbound 메일 가능여부	O	X	X	X
멀티도메인 지원	O	▲	▲	▲
스마트 기능	O	X	▲	X
실시간 모니터링 기능	O	X	O	X
Regular Expression	O	O	O	X
바이러스 차단	O	O	O	O

Spamsniper의 활용효과

- 메일트래픽의 적절한 분배 및 조절로 실제 수신 메일서버 보호
- 과도한 트래픽을 야기하는 스팸성 메일 방지
- 수신메일의 안전성 확보로 전반적인 메일 서비스 품질 제고
- 단 시간내에 쏟아지는 메일에 의한 트래픽 잠식제거
- 메일서버를 통해 들어오는 바이러스의 유입방지
- 내부사용자로 인한 바이러스메일 및 스팸메일 외부유출 차단
- 메일 트래픽 (Inbound / Outbound)에 관한 통제 및 관리

Spamsniper의 활용효과 – 내부정보유출탐지 및 통제

- 컨텐츠 필터링 및 파일 필터링
- 보안 정책상 지정해 놓은 특정 단어나 문장, 파일 사이즈를 지정하여 이에 해당하는 메일일 경우, 메일 전송자의 상위자에게 확인 메일을 전송
- 상위자는 메일을 수신하여 확인한 후, 해당 메일 전송을 승인, 또는 거부
- 최상위 관리자는 자사에서 어떤 정보가 외부로 전송이 되었는지 또는 차단되었는지에 대한 상세한 정보를 확인



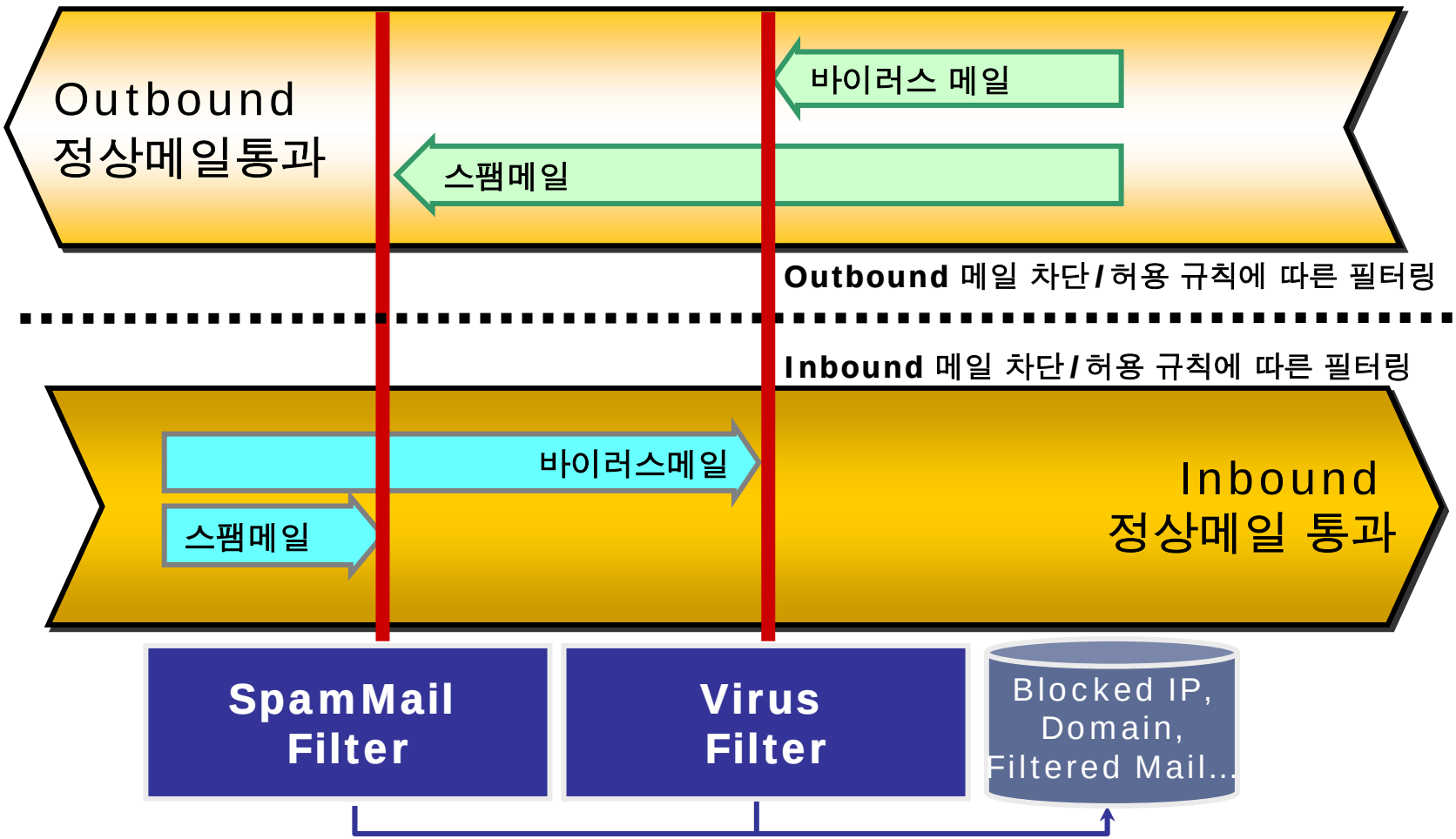
Spamsniper의 활용효과 – 내부정보유출탐지 및 통제

내부정보유출 탐지 및 통제를 위한 세부 단계

① 사내 직원 메일 송신 (파일 첨부)
② 메일 서버를 통하여 스팸스나이퍼 서버로 전달
③ 첨부 파일 크기 제한 등 외부 규제 방안에 해당되는 메일일 경우 해당 메일을 임시 보관 후 DB로 접근 (해당 사항 없을 경우 곧바로 인터넷으로 전송)
④ 해당 직원의 상급자 정보 획득
⑤ 상급자에게 다음의 내용을 메일로 통보
- 해당 직원의 정보, 메일 정보
- 메일 원본 첨부
- 상급자는 메일 내용 중 승인 허락 또는 승인 취소 버튼 클릭

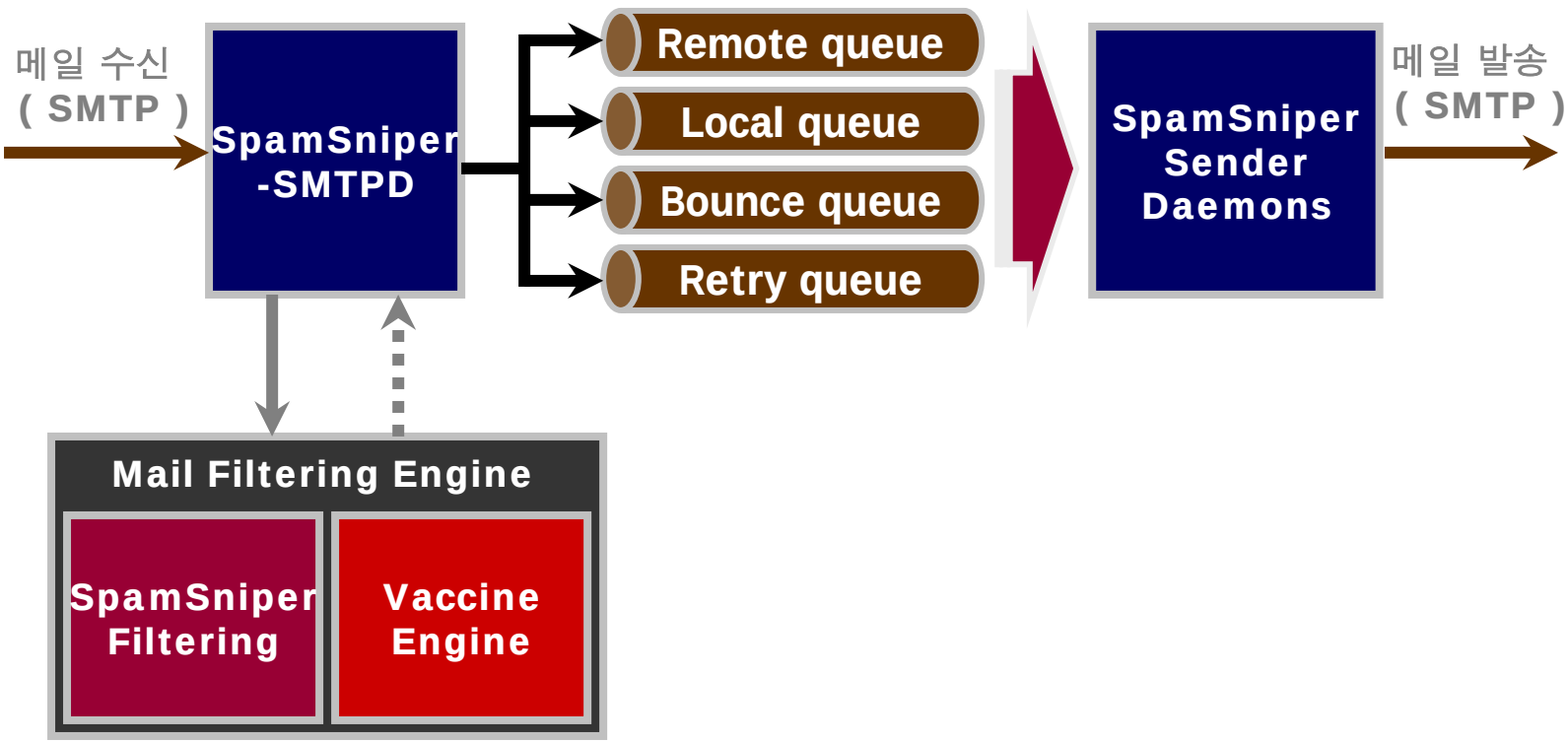
⑥ 상급자의 조치 (승인 / 취소)
⑦ 스팸스나이퍼 서버는 승인 허락된 메일인 경우 외부 (인터넷)로 송신, 승인 취소된 메일인 경우 메일 서버에게 반송
⑧ 반송된 메일 사용자에게 전달

SpamSniper의 필터링 구조



SpamSniper 시스템 구조도

✓ 최대의 안정성을 기한 시스템 구조
: Independent System (multi-process, multi-queue)



SpamSniper의 성능

✓동시메일처리건수 : **400~1000건** **(Network**사정에 따라 다를 수 있음**)**

✓**CPU** 점유율 : **5%** 미만

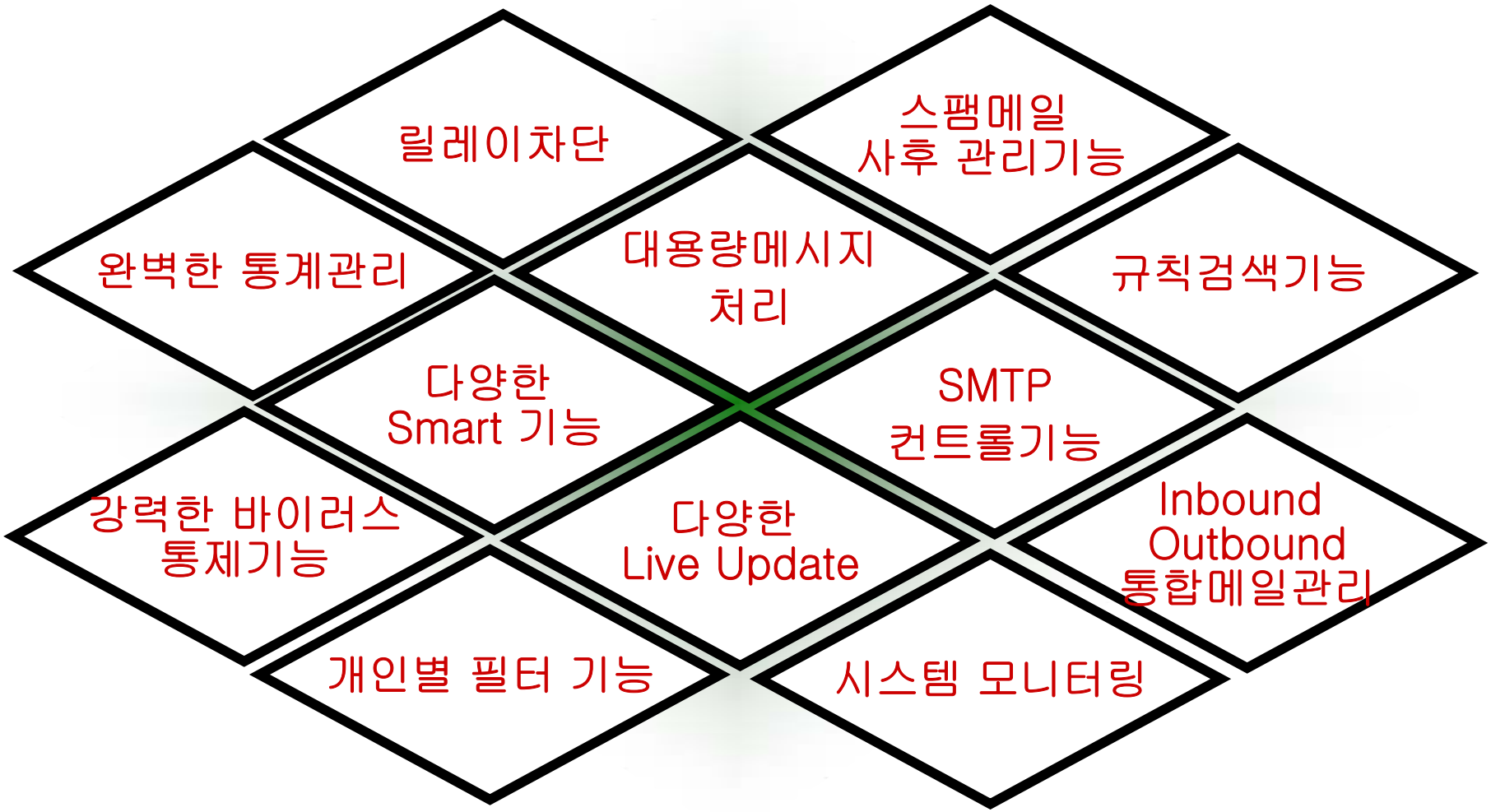
< 최대 처리 성능 >

	저사양서버 (ex. PIII)	고사양서버 (ex. Xeon)
초당처리수	17건	200건
시 간 당	61,200건	720,000건
1 일	1,468,800건	건

<스팸메일 1건처리시간>

8K : 0.005sec
16K : 0.01sec
32K : 0.02sec
64K : 0.03sec
128K : 0.05sec
1024K : 0.07sec
2048K : 0. 1sec

SpamSniper의 주요 기능



SpamSniper의 기능(1)

1 기본 기능

- Relay 허용 / 차단 기능
  - 외부로부터 불법적인 메일서버에 접근 방지
  - 차단 예외적용 가능

2 대용량 메시지 처리기능

- 메일수신 시 메모리에서 즉시 처리하는 구조
- 차단메일(스팸/바이러스)을 파일형식으로 로그관리

SpamSniper의 기능(2)

3 SMTP단에서 처리 기능

- 대량메일 발송자에 대한 차단
  - 특정 IP / Domain, 메일주소 실시간 차단
- 타피팅 기능(대량메일 발송시도에 대한 응답지연)
  - 응답지연을 적용할 단위시간 당 메일 수신 개수 설정 기능
  - 응답지연 시간 설정 기능
- 대량 메일 발송 허용 처리
  - 허용 IP 설정 기능
  - 허용 IP에 대한 최대 수신 개수 제한 기능
  - 대량발송자에 대한 IP/Domain Name 자동등록 및 제한 기능
- 세션당 메일수신 개수 및 커맨드 수 지정(해킹방어)
- 정크메일 대응
  - 정크메일로 의심되는 메일 개수 지정 기능
  - 정크메일로 확실시 되는 메일 개수 지정 기능
- 화이트 / 그레이 / 블랙리스트 설정 및 관리 기능
  - 자동 스마트 기능 지원

SpamSniper의 기능(3)

4 필터링 세부기능

- ▪ 헤더부분 필터링
  - -from, to, cc, bcc, received, reply-to, content-type, x-mailer, x-priority, x-mimeOLE에 대한 허용/차단 설정
  - -특수기호의 입력 및 대소문자 구분, 특수문자(?+*{})에 대한 Regular Expression 적용
  - -대소문자 구분 기능
  - -다국어 필터링 기능(한글, 영문, 한문)
  - -특정 헤더정보 부재 시 차단 기능
- ▪본문부분 필터링
  - -본문 필드내 특정단어 / 문장에 대한 허용/차단 기능
  - -본문 필드내의 유해차단사이트 IP/URL에 대한 허용/차단 기능
- ▪첨부파일부분 필터링
  - -첨부파일 개수, 파일명, 파일명 길이, 파일사이즈, 확장자에 대한 허용/차단 기능
- ▪필터 확장 기능
  - -포함하면, 시작하면, 끝나면, 포함하지 않으면 지정기능

SpamSniper의 기능(4)

5 바이러스 메일 처리 기능

- ▪ 기본기능
  - -SMTP 프로토콜에 대한 바이러스 검색, 치료 및 제거 기능
  - -첨부파일 및 본문 내 스크립트 형태의 바이러스 검색, 치료, 제거 기능
  - -치료결과에 대해 원래 수신자에게 알림기능
  - -압축파일에 대한 치료 기능
- ▪확장 기능
  - -최신 백신 엔진에 대한 라이브 업데이트 기능
  - -업데이트 된 엔진 버전 표기

6 표준권고안에 따른 필터링 기능

- ▪ 발신자,수신자, Domain Name , 제목, Date 부재시 차단 기능
- ▪ 부적당한 Mail from, To를 거부할 수 있는 기능

SpamSniper의 기능(5)

7 검색기능

▪ 현재 설정되어 있는 차단/허용 규칙 검색 기능
- -제목, IP/Host Name/Domain Name 별로 검색
- -전체/그룹/개인별 설정 규칙 검색
- -Inbound / Outbound별 설정 규칙 검색
- -멀티 도메인 적용시 도메인별 설정 규칙 검색

8 멀티 도메인 기능

▪ 멀티서버 / 멀티 도메인 설정 기능
- -도메인별 차단/허용 규칙 별도 설정 기능
- -도메인별 별도 통계 기능

SpamSniper의 기능(6)

9 다양한 통계기능

- 상세통계기능
  - -거부메일 , 스팸메일, 정상메일, 바이러스 메일에 대한 월별,일별 상세 통계
  - -거부메일 통계기능 (거부사유/보낸이/받는이/시간별분류/거부IP/Domain별 분류)
  - -스팸메일 / 정상메일 별 통계기능 (전체보기/보낸이별/받는이별/SMTP/시간별/규칙별 분류)
  - -바이러스 메일 통계 기능 (전체보기/보낸이/받는이/SMTP/시간별/바이러스 종류별 분류)
- 통계가능영역
  - -임의 기간 설정을 통한 통계
  - -필터규칙별 통계
  - -Inbound / Outbound에대한 별도 통계 기능
  - -전체/그룹/개인/도메인 별 통계기능
- 통계관리 기능
  - -자동 Fresh기능
  - -Text, Graphic, Excel File 지원

SpamSniper의 기능(7)

10 스팸메일 관리 기능

- 스팸메일 수신 시 알림 기능
  - -스팸메일 수신 시 관리자/송신자/수신자에게 경고메일 발송
  - -경고문구 편집 기능
- 사후관리 기능
  - -서버에 저장된 스팸 메일에 대한 유저별, 도메인별 조회 및 관리
  - -개인 사용자별로 로그인 후 스팸메일에 대한 조회 및 관리
  - -스팸메일 전송 또는 복구 후 자동 삭제 기능
  - -걸러진 스팸메일에 대하여 그현황/목록을 각 사용자에게 설정시간별 발송 기능
- 스펨메일 본문내용 제공 기능
- 스팸메일 검색 기능

SpamSniper의 기능(8)

11 스마트 및 라이브 업데이트 기능

- 차단규칙에 대한 스마트 기능
  - -스팸메일/바이러스의 유입경로(IP/Domain)에 대한 자동 블랙리스트 작성기능
  - -바이러스 파일명에 대한 자동 첨부파일 차단목록 등록 기능
  - -등록된 블랙리스트에 대하여 일정기간 동안 빈도수가 없을 경우 자동 삭제 기능
  - -스팸규칙 Live Update 기능(DB자동업데이트 / 인터넷망을 통한 자동 업데이트)

12 시스템 운영관리 기능

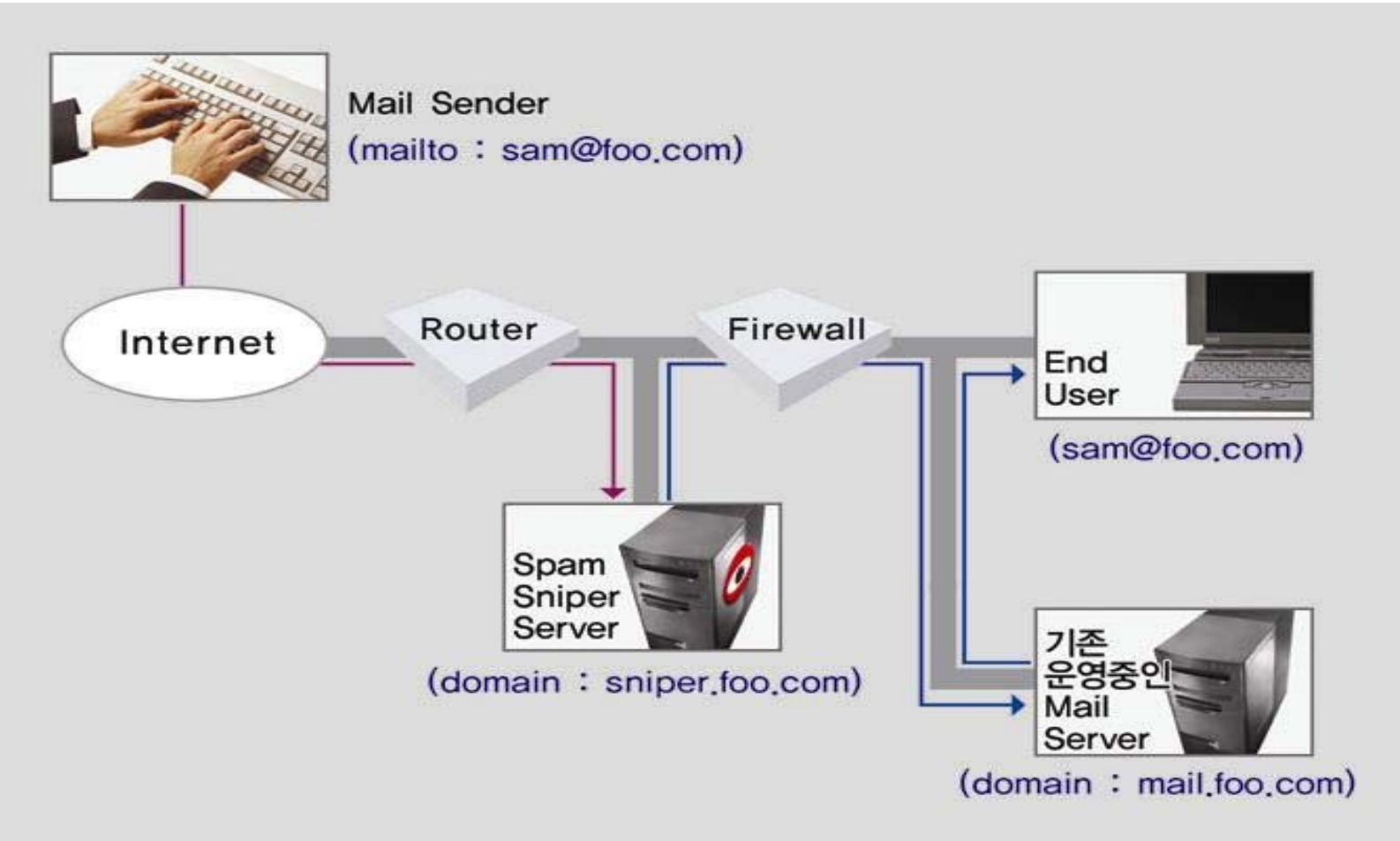
- 스팸스나이퍼 서버의 시작 및 종료
- Inbound/ Outbound 적용 여부 설정
- 각종 로그들의 조회 및 관리(삭제 및 백업)
- 복수개의 스팸스나이퍼 서버 설치 시 통합서버관리
- 시스템 및 메일 로그에 대한 실시간 모니터링
- 온라인 도움말 및 Q&A

SpamSniper의 기능(9)

13 시스템 모니터링 기능

- 시스템 리소스 모니터링 기능
  - -CPU점유율, disk사용율, 사용자수
  - -Mail Queue관리 기능
- 메일 트래픽의 변화율 모니터링 기능
  - -정상메일/스팸메일/바이러스메일의 시간별, 일별, 주별,월별 변화율
- 메일 송/수신자, 처리결과, 일시 등 정책 위반 사유 및 바이러스 감염내용
- 시스템 로그 분석 관리 기능
  - -시스템로그 삭제 기간 설정
  - -하드디스크 한계 용량 설정
  - -경보설정
- 서버운용모드 선택 기능
  - -필터링 기능 / 단순 모니터링 기능
- 처리될 메일이 시스템내의 큐에 머무를 수 있는 시간 설정 기능
- 스팸메일 검사 범위 설정 기능(메일헤더 / 헤더+본문)

SpamSniper 도입 후 네트워크 구성도



SpamSniper의 설치방법

1. SpamSniper 서버 설치 : 메일서버 앞 단 → LAN선 연결 & Power On

2. DNS서버의 MX Record 값 변경
예) **foo.com MX 10 mail.foo.com** 을
foo.com MX 10 sniper.foo.com으로 변경

※ 적용 즉시 모든 스팸 메일이 필터링 된 후, 정상 메일만 기존의 메일서버로 전송된다.

Q & A

FNET (주)에프넷트

Free & Safe Networking