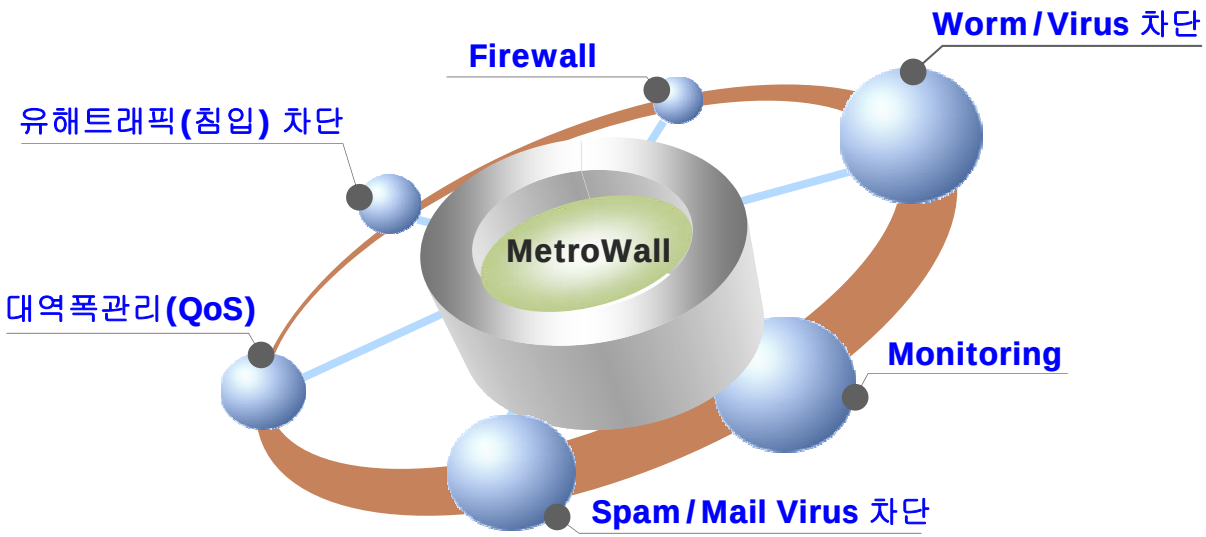
트래픽 통합 관리 시스템 (MetroWall)




MetroWall-L


MetroWall-S(300,500.1000,학내망)


MetroWall-E

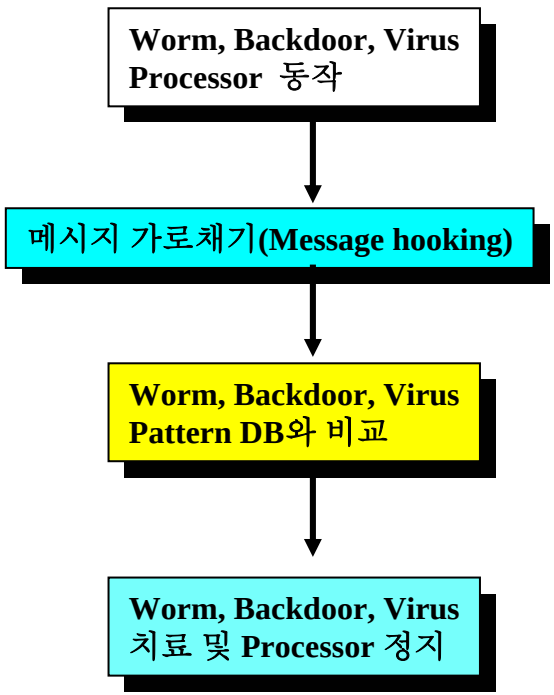

MetroWall-G

아이콤정보시스템
TEL:02)861-1175 , FAX:02)861-1176

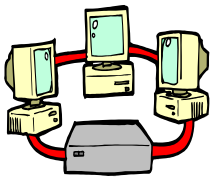
특허기술

특허기술 : 메시지 가로채기를 이용한 응용프로그램에 대한 보안방법(특허제0443203호)

특허기술을 이용하고 Worm, Backdoor, Virus Pattern 검증 DB를 사용함으로써 Worm, Backdoor, Virus 등이 활동을 위하여 Processor가 동작을 시작하면 Processor 기동 Message를 가로채어 DB의 Pattern과 비교한다.
검출된 Worm, Backdoor, Virus에 해당하면 내장된 Vaccine으로 치료하고 치료가 불가능한 Processor를 정지시킴으로써 Worm, Backdoor, Virus의 동작으로 인한 유해 트래픽을 원천적으로 차단한다.



1 Metro Ethernet의 급속한 보급

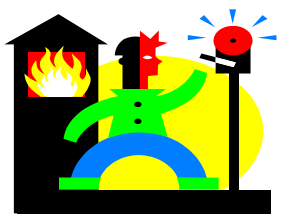


- 기존의 ATM, T1, E1, T3 인터넷 회선 속도가 WAN 구간을 100Mbps 까지 지원하는 Metro Ethernet의 급속한 보급
- Metro Ethernet 환경에 따른 Router S/W의 미사용

2 침입, Port Scan, Spam, Virus, Worm 등 모든 종류의 유해트래픽에 대한 대책이 요구됨

- WAN 구간에서 들어는 침입, PortSCan, Spam, Virus, Worm을 효과적으로 차단할 있는 시스템이 요구됨.
- LAN 구간의 Client PC에서 발생되는 Worm, Virus에 대한 효율적인 차단이 필요함.

3 IP별, 서비스별, 그룹별 대역폭 조절 및 사용량 모니터링이 요구됨



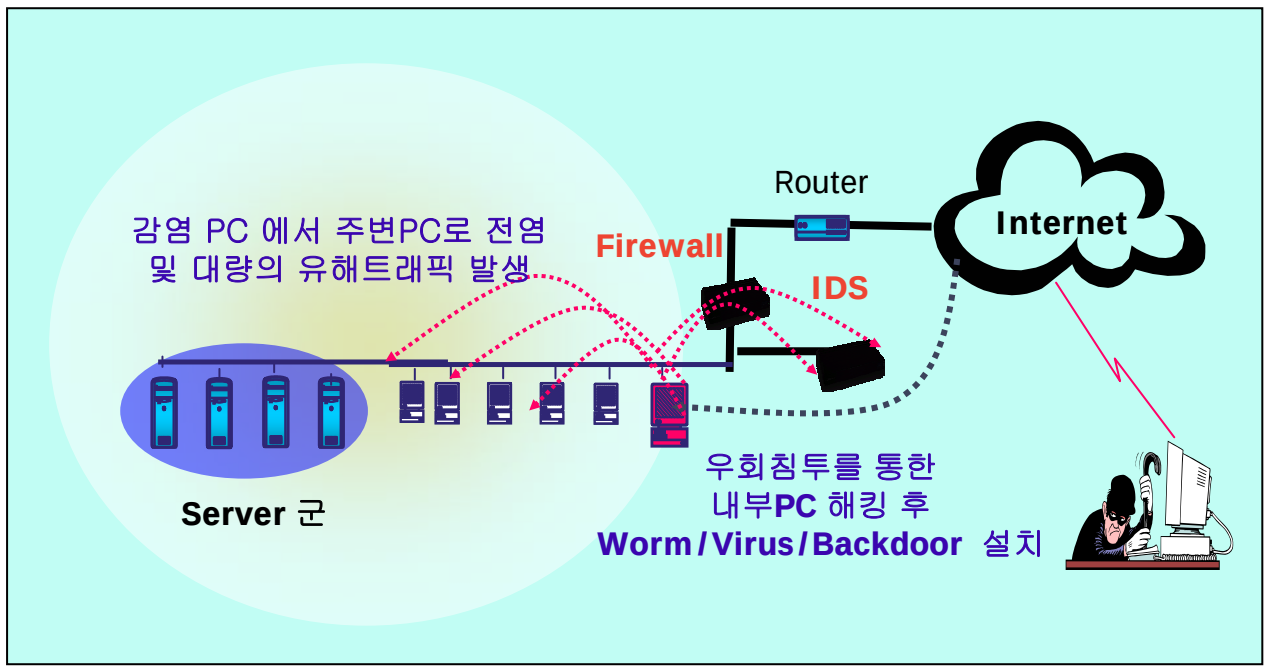
- 각종 P2P 서비스 및 업무용 서비스에 대한 대역폭 보장 및 제어가 요구됨.
- 실시간으로 네트워크 트래픽 현황을 파악하여 불필요한 트래픽의 효과적인 제어가 요구됨.

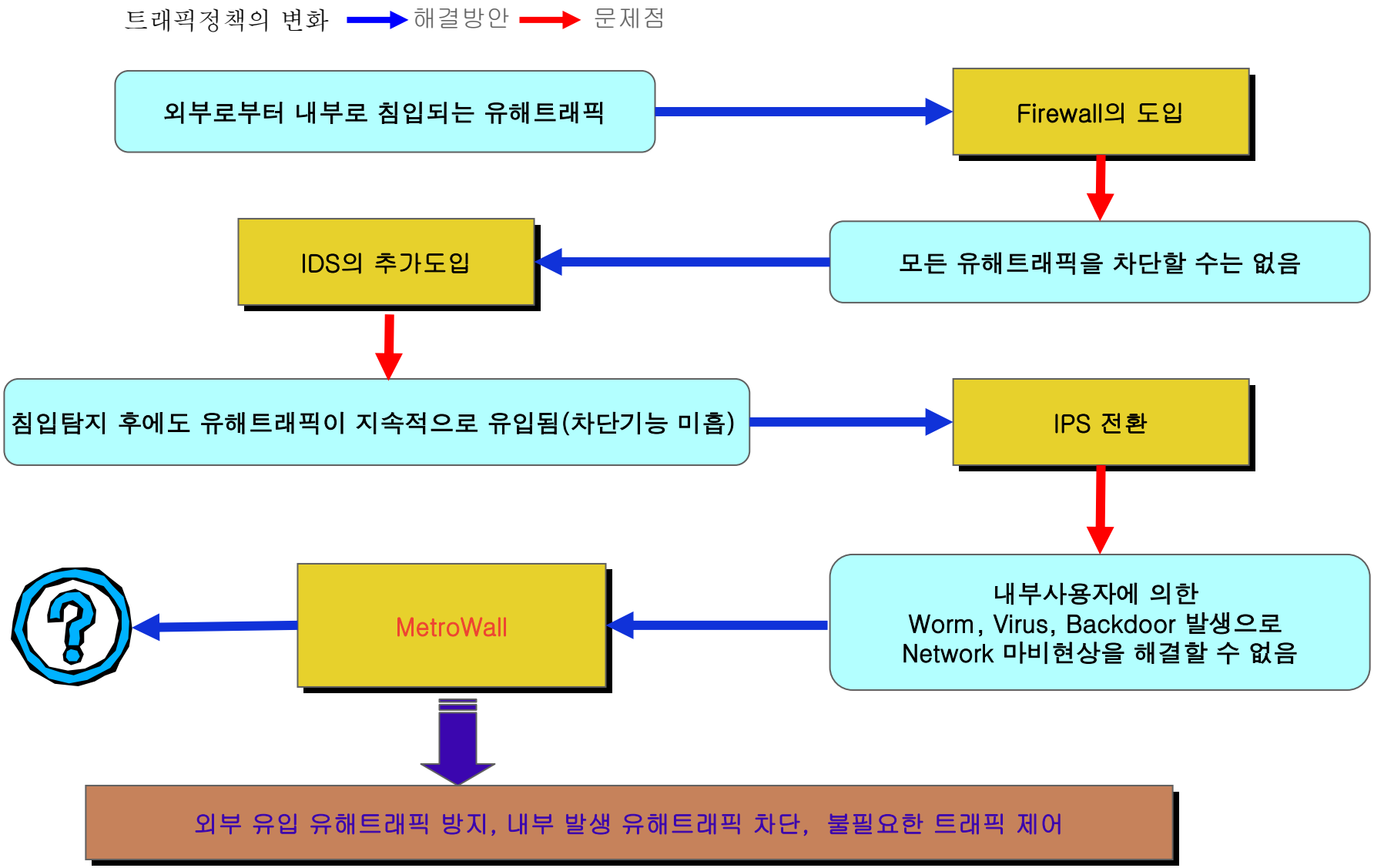
트래픽 폭주현상

- Firewall, IDS 우회하여 공격(IP Fragmentation)을 통한 기존의 보안시스템을 무력화 현상
- 내부 PC의 Worm, Virus, Backdoor 에서 발생하는 대량의 유해 트래픽으로 인한 전체 네트워크 마비현상

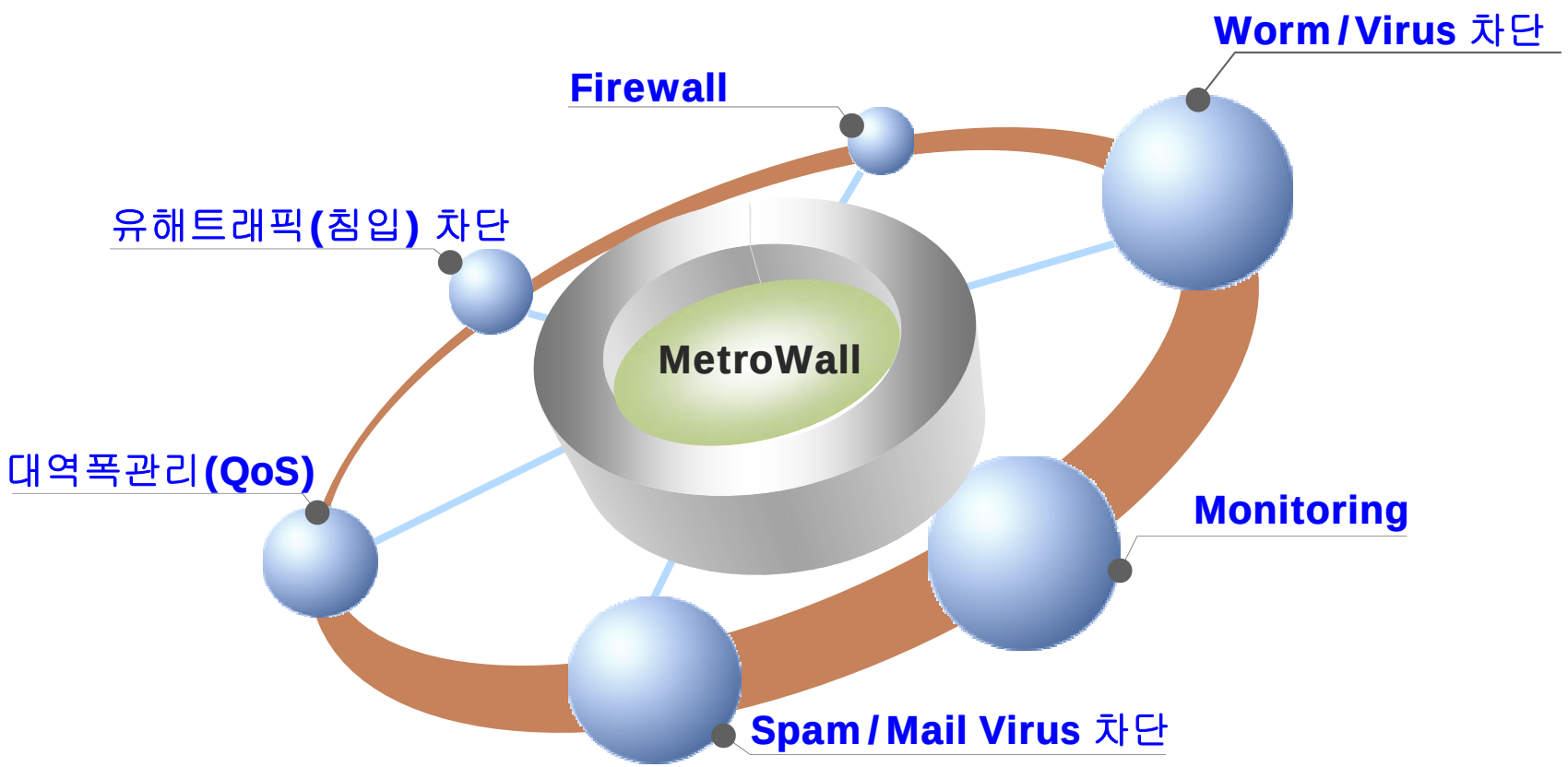
대응책

- 외부에서 유입되는 불필요한 트래픽 차단(침입, Worm, Virus, Spam등)
- 내부에서 발생하는 유해트래픽 차단 (Worm, Virus, Backdoor)
- 업무용 트래픽 우선보장 및 비업무용 트래픽 제어
- 모니터링을 통한 트래픽 현황파악

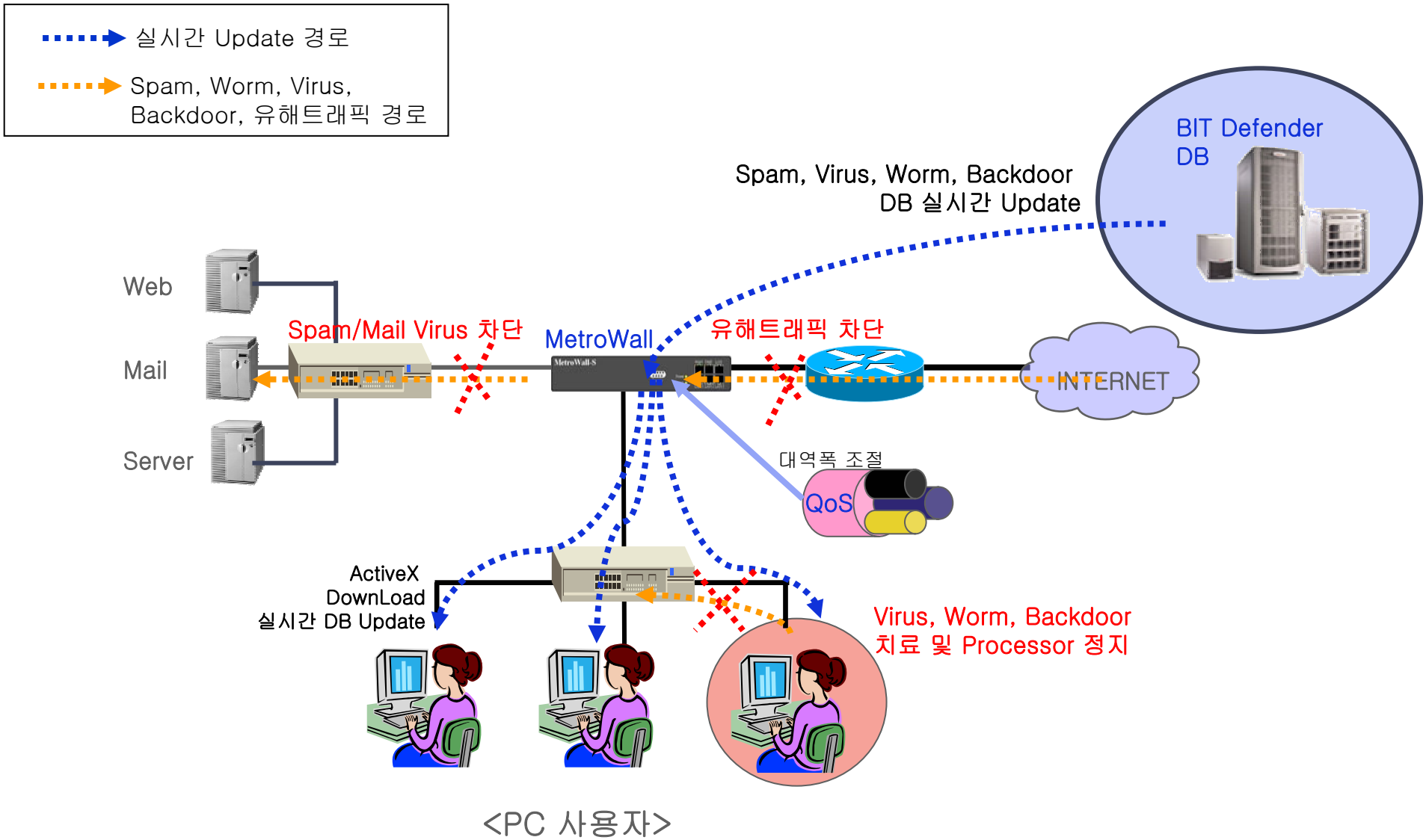



트래픽정책의 변화
해결방안
문제점
외부로부터 내부로 침입되는 유해트래픽
Firewall의 도입
모든 유해트래픽을 차단할 수는 없음
IDS의 추가도입
침입탐지 후에도 유해트래픽이 지속적으로 유입됨(차단기능 미흡)
IPS 전환
내부사용자에 의한
Worm, Virus, Backdoor 발생으로
Network 마비현상을 해결할 수 없음
MetroWall
외부 유입 유해트래픽 방지, 내부 발생 유해트래픽 차단, 불필요한 트래픽 제어

Firewall, 유해Traffic(침입) 차단, 대역폭관리(QoS), Spam/Mail Virus, Traffic Monitoring 기능, 사용자 PC에 대한 Worm, Virus, Backdoor 차단 기능을 갖는 특허기술을 활용한 국내외 유일한 트래픽 통합관리시스템



- 강력한 QoS 기능(IP/서비스 포트/ 그룹 별 최대 대역폭 제한, 최소 대역폭 보장) 으로 업무 우선 Traffic을 보장하고 특정사용자(P2P)의 대역폭 과점을 제한함.
- 불필요한 Spam Mail 을 차단 및 Virus 전파의 주범인 Virus 감염 Mail을 차단함.
- Client PC의 Worm/Virus/Backdoor 치료 및 차단함. (Virus Engine 실시간 Update)
- 인증되지않은 불법 접속을 차단 및 침입성 유해트래픽을 차단함.
- 네트워크 트래픽에 대하여 다양한 실시간 모니터링 (Top 5) 및 통계데이터를 제공함.


실시간 Update 경로
Spam, Worm, Virus,
Backdoor, 유해트래픽 경로
BIT Defender
DB
Spam, Virus, Worm, Backdoor
DB 실시간 Update
Web
Mail
Server
Spam/Mail Virus 차단
MetroWall
유해트래픽 차단
INTERNET
대역폭 조절
QoS
ActiveX
DownLoad
실시간 DB Update
Virus, Worm, Backdoor
치료 및 Processor 정지
<PC 사용자>

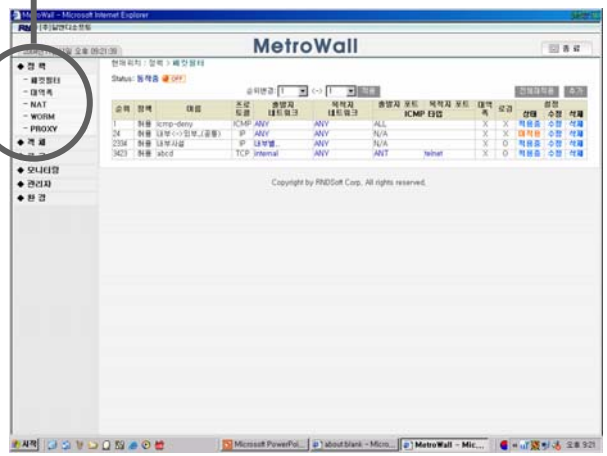
[트래픽 통합관리 운영환경 설명]

외부 유해 트래픽 유입차단	- Firewall 기능: 불필요한 트래픽 원천 차단 - 유해 트래픽 차단 기능 : Worm, Dos 공격, 침입성 트래픽 원천 차단 - Spam/Mail Virus 차단 기능 : E-Mail을 통한 Virus 차단 및 Spam Mail을 차단
내부 유해 트래픽 발생차단	- 자체 DB(Worm/Backdoor-8,000 여개 보유, Virus-BitDefender(90,000여개 보유, 하우리 바이로봇 엔진과 동일)) Worm, Virus, Backdoor Processor 치료 및 차단 - 신종 또는 변종 Worm, Virus, Backdoor Processor는 임계치 제어방식으로 차단
트래픽 관리 및 모니터링	- Client PC의 기동 및 Worm, Virus, Backdoor의 발생을 통합 관리 - 특정 서비스, 호스트 등의 대역폭을 QoS 기능으로 대역폭 보장 및 제한 - 특정 네트워크 대역, 개별 호스트(Client PC, Server) 등을 트래픽 발생량 모니터링

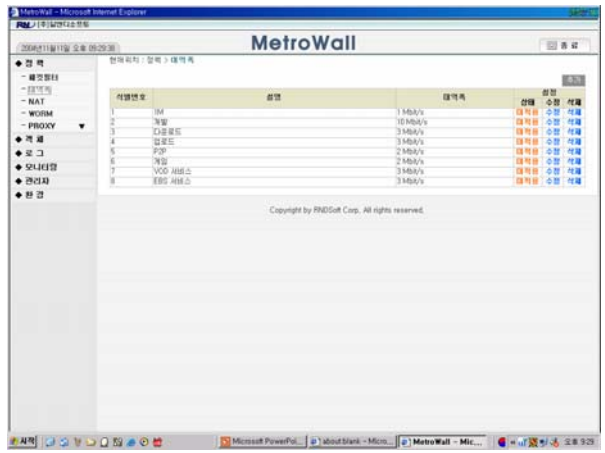
구분		- 사용 User수 - WAN 대역	Network	Capacity
MetroWall-L	 ₩6,000,000 (소비자금액)	▪100 이하 ▪5Mbps 이하 (MW-S기능으로 확장가능:옵션)	▪CPU : Intel P-III ▪RAM : 256MB ▪ROM :128MB ▪NIC ▪10/100BaseTX x 4	▪Policy : 1,000 ▪Concurrent Session : 400,000 ▪Max Throughput : 10Mbps ▪LOG : 40GB
MetroWall-S (300) (500) (1000)	 (300)경우: ₩10,0 00,000(소비자가) (500)경우: ₩12,5 00,000(소비자가) (1000)경우: ₩15,0 00,000(소비자가)	▪300 이하 ▪500 이하 ▪1,000 이하 ▪학내망용 (1,000 이하) ▪20Mbps 이하	▪CPU : Intel P-III ▪RAM : 512MB ▪ROM :128MB ▪NIC ▪100/1000BaseTX × 2 ▪100BaseTX x 4	▪Policy : 10,000 ▪Concurrent Session : 600,000 ▪Max Throughput : 100Mbps ▪LOG : 40GB
MetroWall-S (학내망용)	₩15,000,000 (소비자금액) - 학내망인 경우 공급가 조정 가능			
MetroWall-E	 ₩25,000,000 (소비자금액)	▪2,000 이하 ▪100Mbps 이하	▪CPU : Intel P-M ▪RAM : 512MB ▪ROM :128MB ▪NIC ▪100/1000BaseFX x 2 ▪100/1000BaseTX x 2 ▪100BaseTX x 3	▪Policy : 20,000 ▪Concurrent Session :1,000,000 ▪Max Throughput : 400Mbps ▪LOG : 40GB
Metrowall-G	 ₩60,000,000 (소비자금액)	▪3,000 이하 ▪1Gbps 이하	▪CPU : Inte Xeon ▪RAM : 2GB ▪ROM : 128MB ▪NIC ▪1000BaseFX × 4 ▪1000BaseTX x 4	▪Policy : 50,000 ▪Concurrent Session : 2,000,000 ▪Max Throughput : 2Gbps ▪LOG : 80GB

유지보수금액 : 판매 공급 금액의 20%

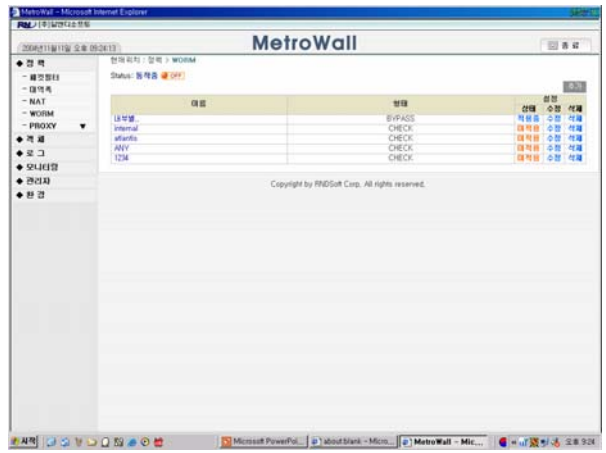
트래픽 통합 관리를 위한 각종 정책을 단일 인터페이스에서 처리함.
최대 50,000개의 정책을 통합 관리함.



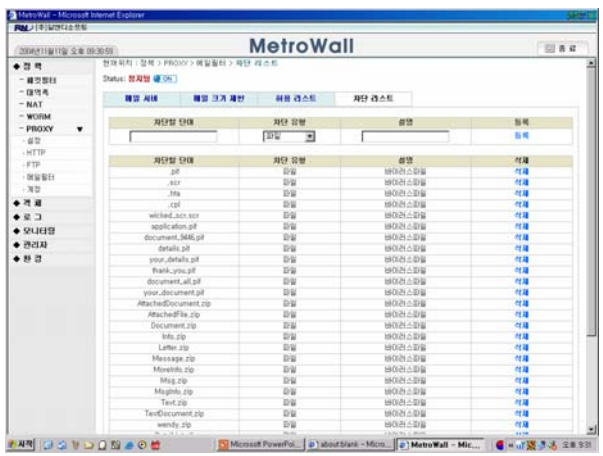
패킷 필터



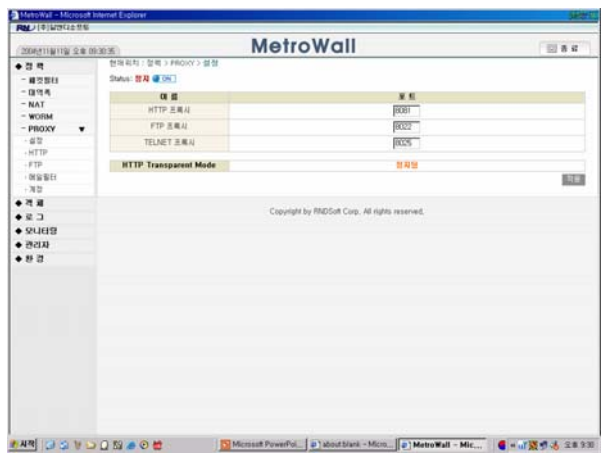
QoS



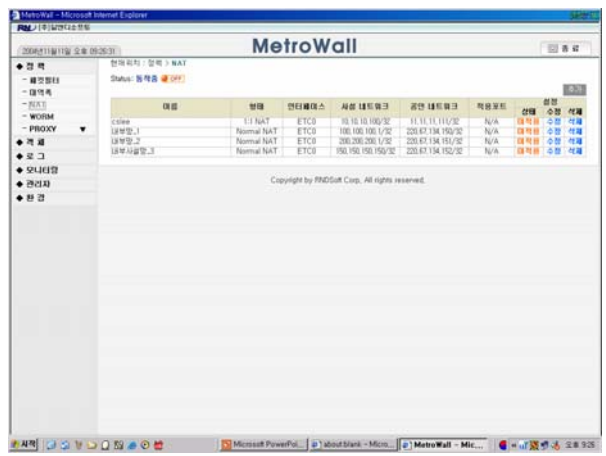
Worm & Virus



Spam 필터

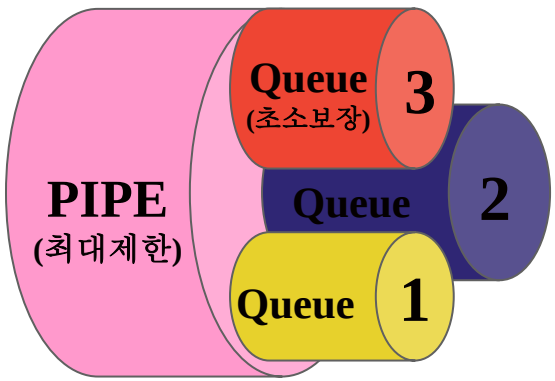


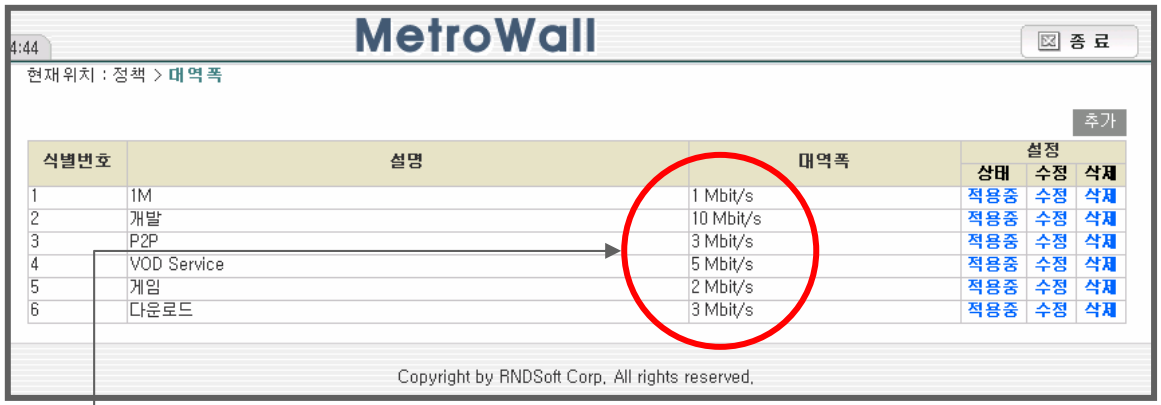
Proxy



NAT

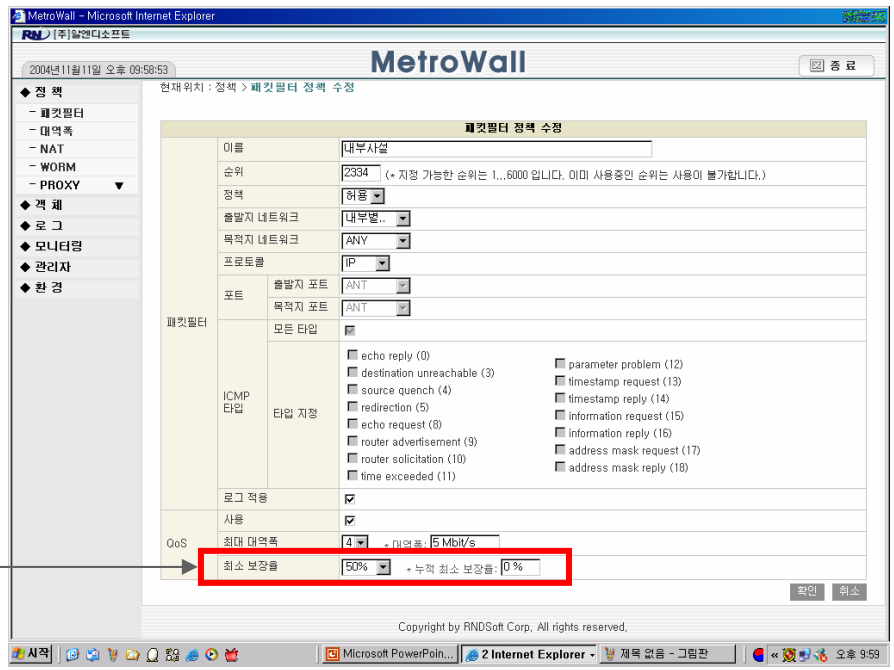
- ✓ WF2Q 지원
- ✓ 네트워크 대역폭의 실시간 비례분할
- ✓ 오차율 3%이내의 정확성
- ✓ IP, URL, Port, Range&Group 지원
- ✓ 100MB & 1GB 지원
- ✓ 최대 50,000개의 QoS 정책 지원

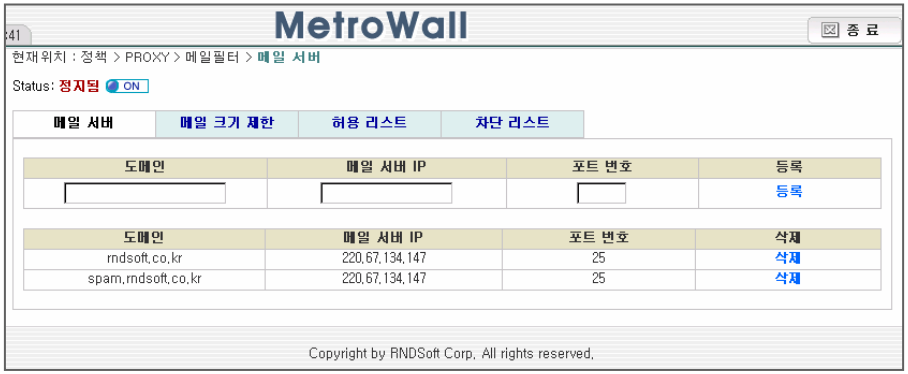




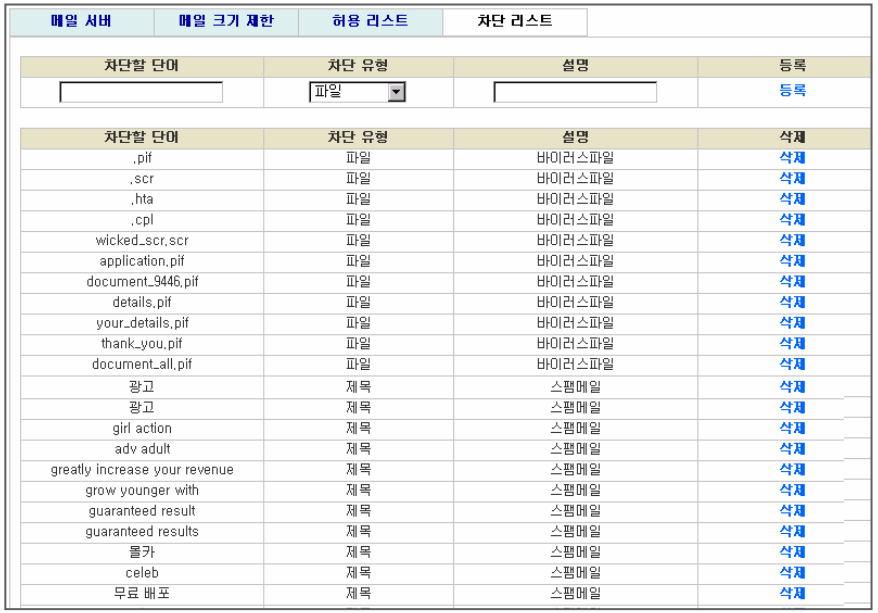
최대대역폭지정

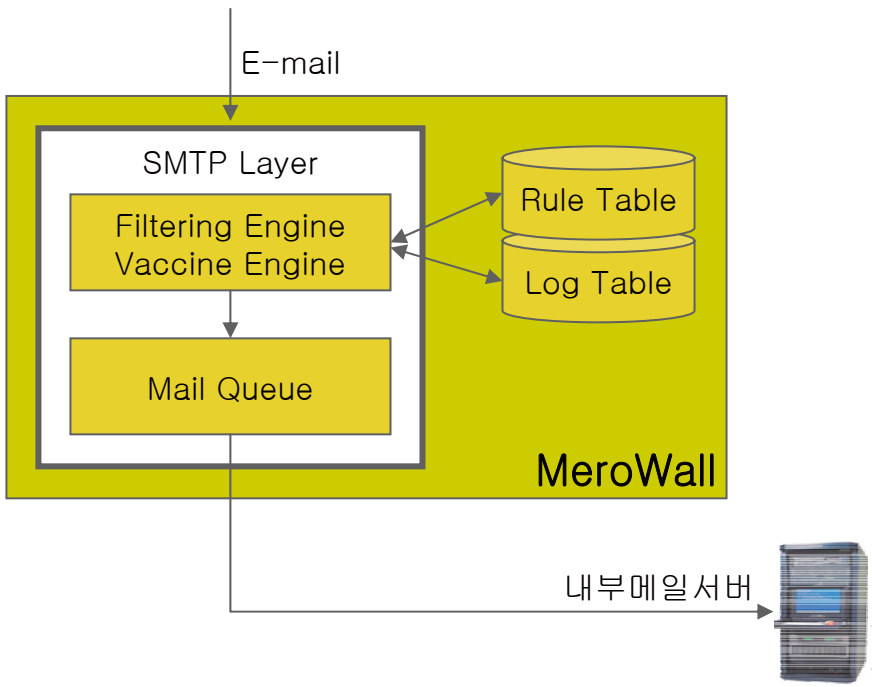
최소대역폭지정





(메일서버 설정 및 스팸 관리 Table)

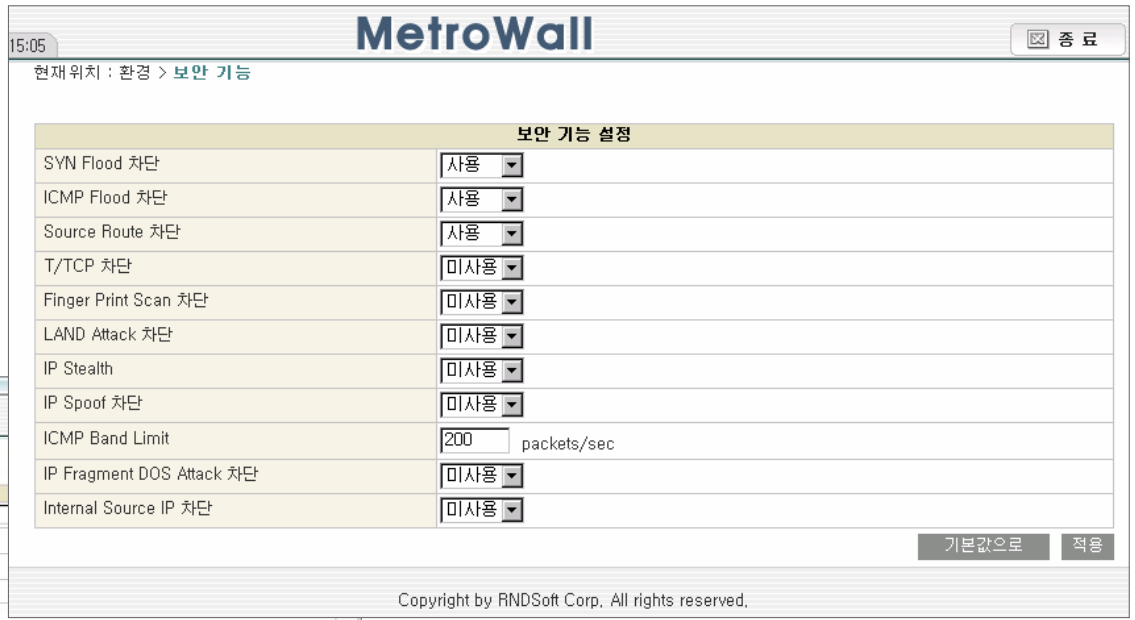




Filter	주요기능
SPAM Mail	메일 헤더/본문/첨부파일 필터링 대량메일 차단/허용 기능/메일크기 제한 White/Black List 관리
Mail Virus	SMTP에 프로토콜에 대한 Virus 검색 및 제거 첨부화일 Script에 대한 Virus 검색 및 제거 압축 File에 대한 Virus 검색 및 제거

* 실시간 원격 Pattern DB Update
* Gateway Mode에서만 지원됨

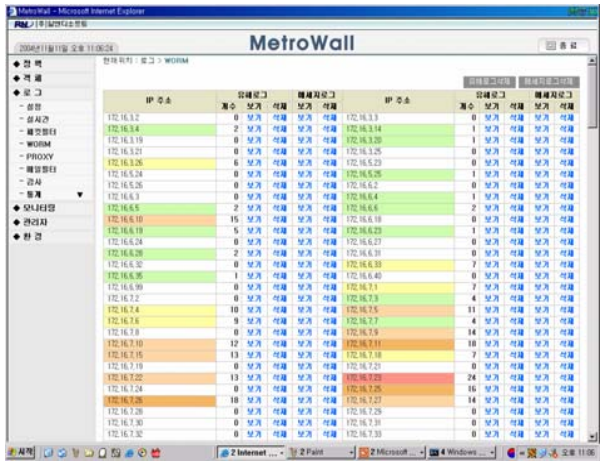
외부에서 내부로 유입되는 침입성
유해트래픽을 유해트래픽 차단필터,
문자열검사필터에서 사전에 차단함.



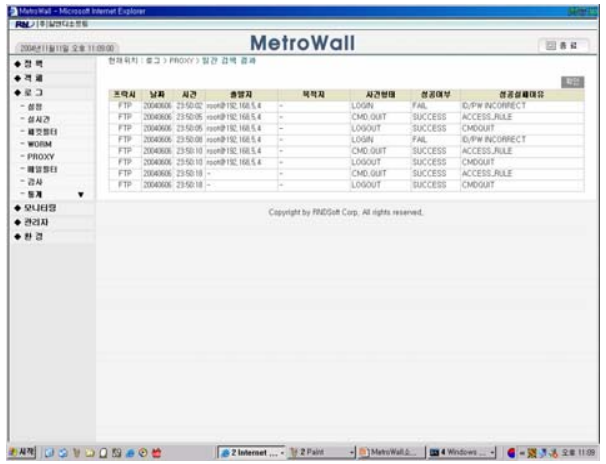
(유해 트래픽 차단 필터)

(문자열 검사 필터)

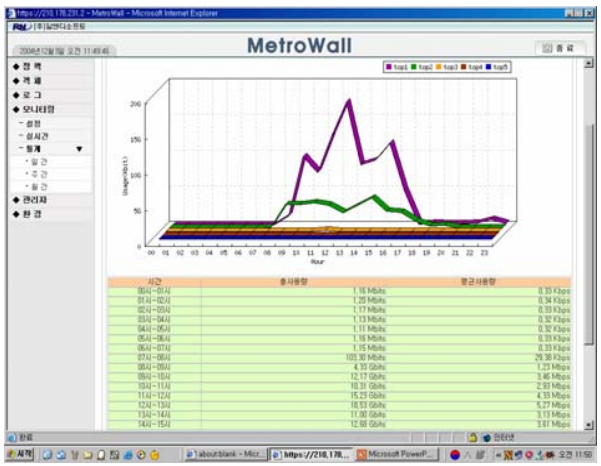
패킷 필터 실시간 로그



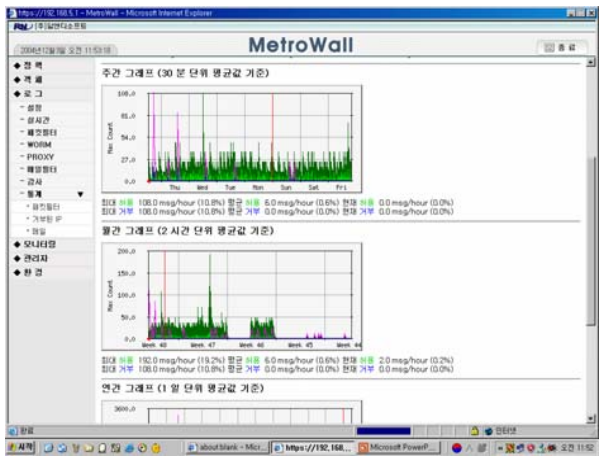
웜-바이러스 & 유해 트래픽 로그



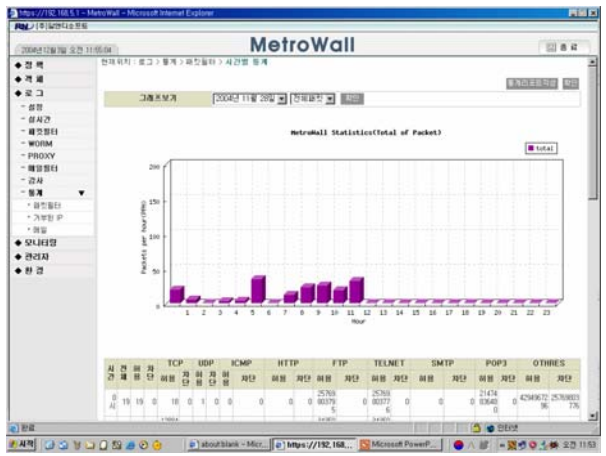
프록시 로그



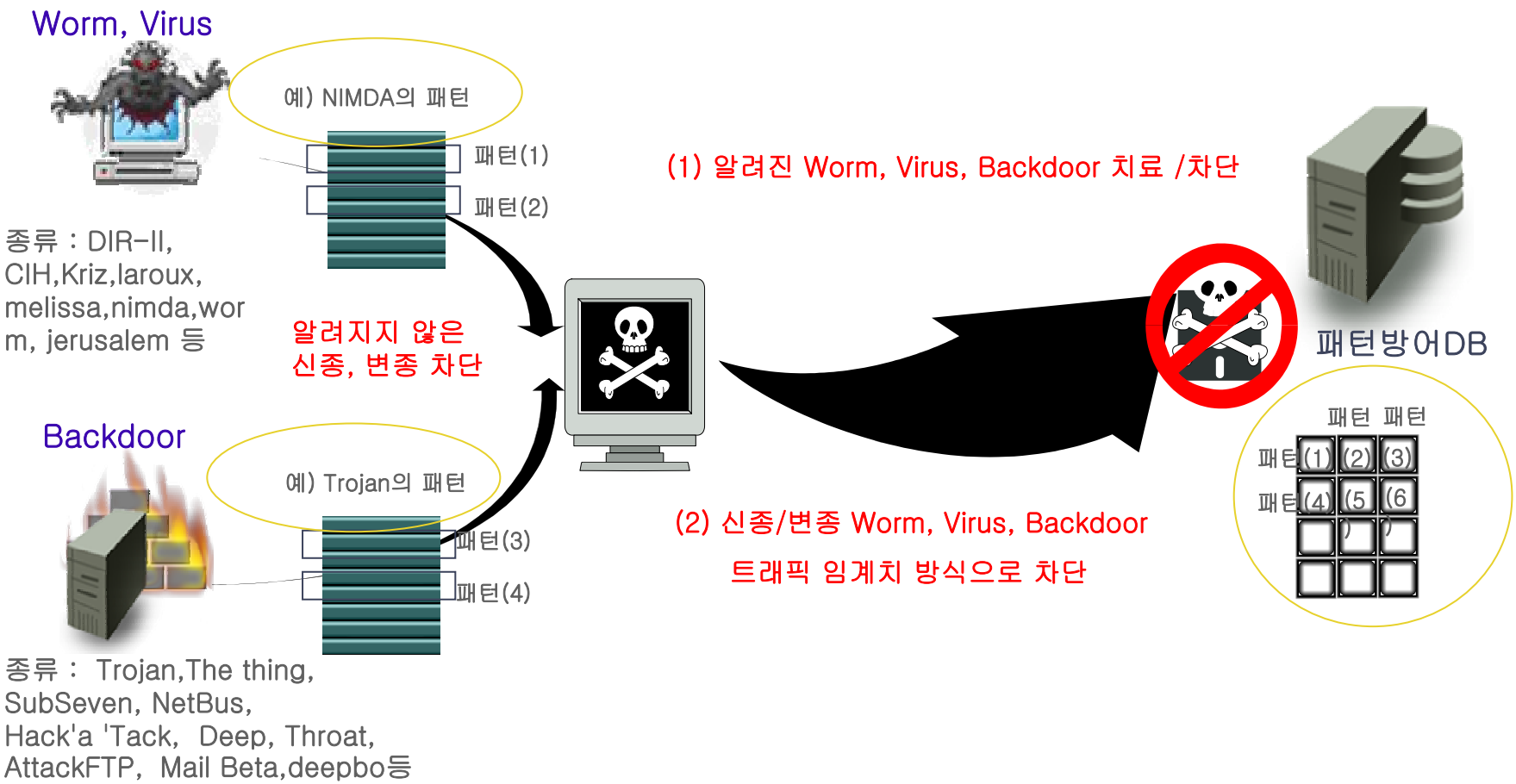
트래픽 모니터링
(실시간,일간,주간,월간)



스팸메일 & 메일 바이러스 로그

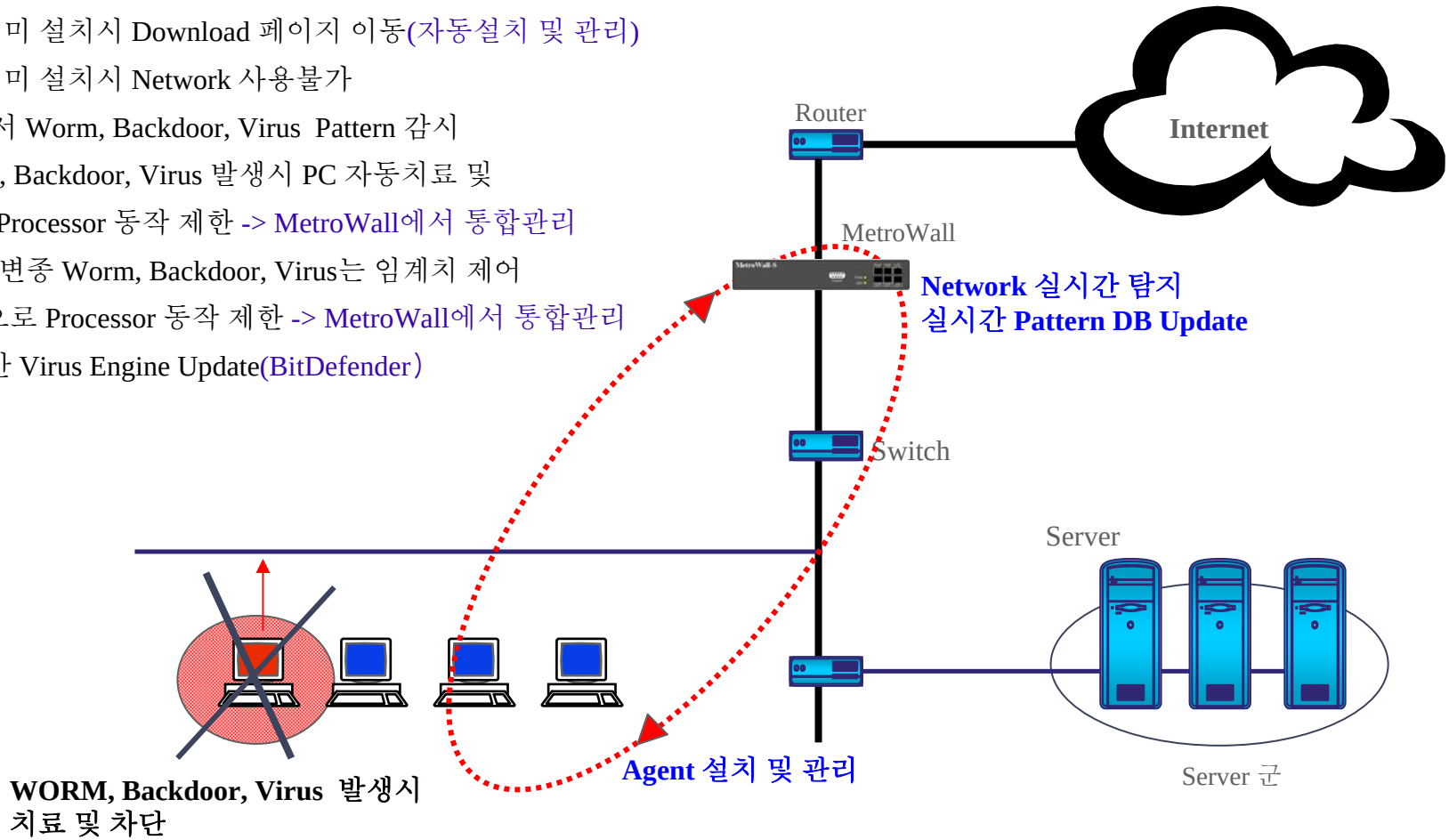


로그통계

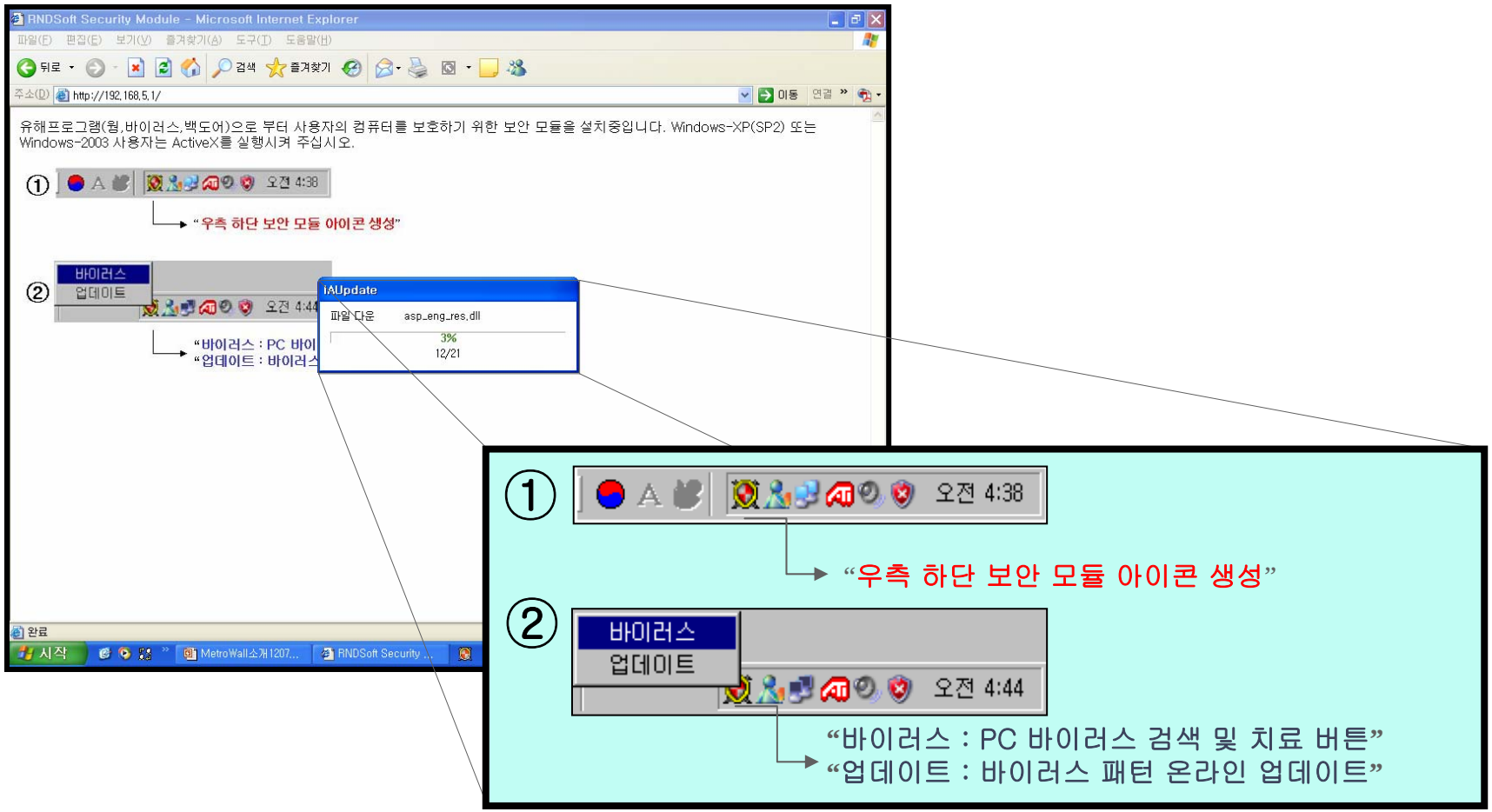

Worm, Virus
예) NIMDA의 패턴
패턴(1)
패턴(2)
종류 : DIR-II, CIH,Kriz,laroux, melissa,nimda,worm, jerusalem 등
알려지지 않은 신종, 변종 차단
Backdoor
예) Trojan의 패턴
패턴(3)
패턴(4)
종류 : Trojan,The thing, SubSeven, NetBus, Hack'a 'Tack, Deep, Throat, AttackFTP, Mail Beta,deepbo등
(1) 알려진 Worm, Virus, Backdoor 치료 /차단
(2) 신종/변종 Worm, Virus, Backdoor
트래픽 임계치 방식으로 차단
패턴방어DB
패턴 패턴
패턴 (1) (2) (3)
패턴 (4) (5) (6

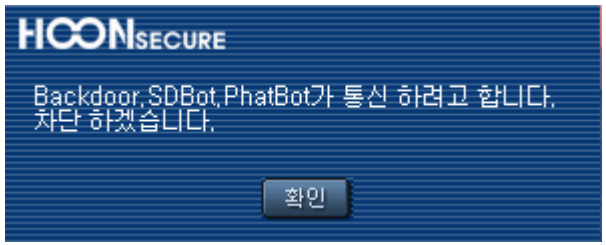
동작방법

1) PC에서 Network 접속시 Agent 실시간 탐지
2) Agent 미 설치시 Download 페이지 이동(자동설치 및 관리)
3) Agent 미 설치시 Network 사용불가
4) PC에서 Worm, Backdoor, Virus Pattern 감시
5) Worm, Backdoor, Virus 발생시 PC 자동치료 및
   해당 Processor 동작 제한 -> MetroWall에서 통합관리
6) 신종, 변종 Worm, Backdoor, Virus는 임계치 제어
   방식으로 Processor 동작 제한 -> MetroWall에서 통합관리
7) 실시간 Virus Engine Update(BitDefender)



보안 ASP 모듈 다운로드 화면





<유해프로그램 차단실행 화면>

현재 위치 : 로그 > WORM > 메세지로그 (IP_192.168.5.242)

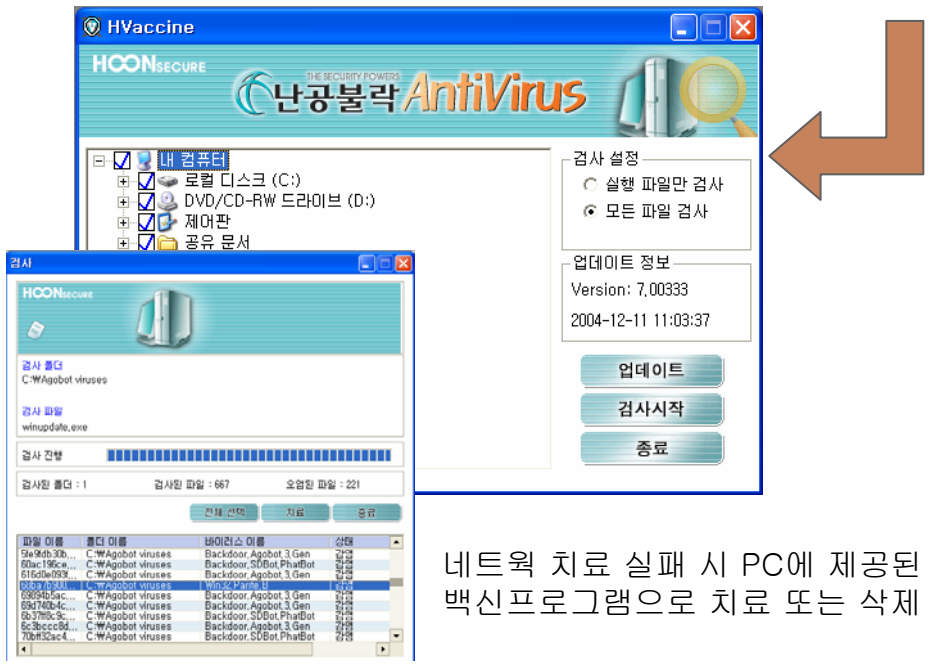
삭제 취소

검출시간	2004년 12월 23일 11시 6분 25초 [네트워크차단 - 검역소이동]
바이러스	Backdoor,SDBot,PhatBot
파일이름	soundman.exe
접속시도	IP 0.0.0.0 : 0
검출시간	2004년 12월 23일 11시 9분 15초 [검역소 - 치료실패]
바이러스	Backdoor,SDBot,PhatBot
파일이름	C:₩Program Files₩HoonSecure₩vc₩Temp₩soundman.exe
접속시도	IP : 0

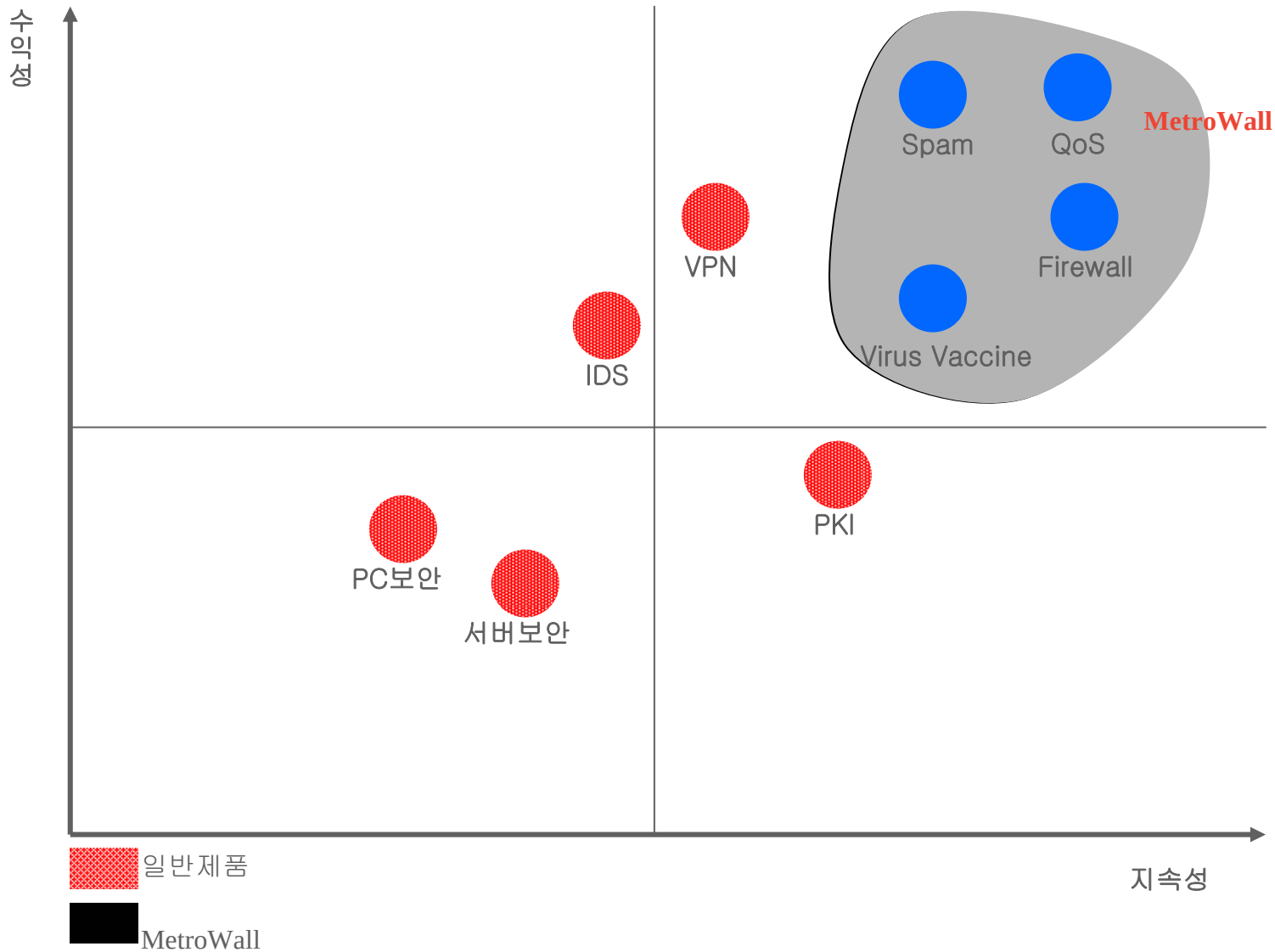
<MetroWall 로그>

- PC에서 바이러스(웜) 또는 유해 프로그램 발견시 불법 통신을 차단하며 검역소로 이동시켜 치료를 한다.

-치료 실패 시에는 검역소에서 프로세스를 Holding 시킨 후 파일 삭제에 권한을 PC사용자에게 이관한다.



네트웍 치료 실패 시 PC에 제공된 백신프로그램으로 치료 또는 삭제


수익성
Spam
QoS
MetroWall
Firewall
VPN
IDS
Virus Vaccine
PKI
PC보안
서버보안
지속성
일반제품
MetroWall

(정보출처 : KISA)

구 분		WatchGuard FireBox-X1000	Worm Captor	SeuwayGate	Sniper-IPS	WormBreaker	MetroWall-S
주요기능	세부기능						
Type		일체형 Network Type	PC Client Type	일체형 Network Type	S/W형 Network Type	일체형 Network Type	Hybrid Type(PC Client+ 일체형 Network Type)
Firewall 기능	Statefull Inspection Filtering	O	X	O	X	X	O
	Gateway/Bridge Mode 지원	?	X	O	▽	▽	O
	IP, Port 별 차단정책 적용	O	X	O	▽	X	O
	NAT 지원	O	X	O	X	X	O
	DMZ 지원	O	X	O	X	X	O
유해트래픽(침입) 차단	Dos Attack 차단	O	X	X	O	O	O
	SYN/ICMP Flooding	O	X	X	O	O	O
	IP Spoofing 차단	O	X	X	O	O	O
	Source Route 차단	O	X	X	O	O	O
	Internal Source IP 차단	O	X	X	O	O	O
	Network Worm 차단	O	X	X	O	O	O
	비정상 Packet 차단	O	X	X	O	O	O
대역폭관리(QoS)	IP별, Port 별, 대역폭관리	X	X	X	X	X	O
	최소대역 보장	X	X	X	X	X	O
	최대대역 제한	X	X	X	X	X	O
Spam/Mail Virus 차단	메일 헤더/본문/첨부파일 필터링	Option	X	X	X	X	O
	대량메일 차단/허용 기능/메일크기 제한		X	X	X	X	O
	White/Black List 관리		X	X	X	X	O
	SMTP에 프로토콜에 대한 Virus 검색 및 제거		X	X	X	X	O
	첨부화일 Script에 대한 Virus 검색 및 제거		X	X	X	X	O
	압축 File에 대한 Virus 검색 및 제거		X	X	X	X	O
Client Worm/Virus	Worm 검색 및 제거	X	O	X	X	X	O
	Virus 검색 및 제거	X	O	X	X	X	O
	Backdoor 검색 및 제거	X	O	X	X	X	O
	Network 자동 차단기능	X	O	X	X	X	O
Monitoring	IP별 Traffic 사용량	X	X	X	O	O	O
	Network 대역 Traffilc 사용량	X	X	X	O	O	O
	Port별 Traffic 사용량	X	X	X	O	O	O
	Group별 Traffic 사용량	X	X	X	▽	▽	O
	정책별 Traffic 사용량	X	X	X	▽	▽	O
Concurrent Sessions		200,000	?	?	?		1,000,000

1) 본 비교는 제품설명서를 기준으로된 비교로 제품에 따라서 차이가 있을 수 있읍니다.
2) 본 비교기준은 6개의 자사모듈에 대응하는 기능에 대한 비교 입니다.
3) 제품별 고유용도에 맞는 기능은 비교제품이 우수한 것도 있습니다.