

**FORTINET**

THE POWER IN NETWORK PROTECTION

# **FORTIGATE**

**FortiOS 3.0  
MR5**

**사용자 매뉴얼**

**1**

**FORTINET.**

**Worldwide LEADER in UTM**

# 시작하기 전에

해당 매뉴얼은 시스템 운용을 위한 기본적인 내용만 기술되어 있으므로 기술되지 않은 내용과 각종설정의 변경 및 보안정책 적용에 대한 부분은 공급 및 설치, 기술지원을 담당하는 업체의 엔지니어 및 기술지원 센터로 문의 하거나 설정 전 사전검토를 권장합니다.

기능 및 기술에 대한 상세정보는 다음의 웹사이트를 참고하거나 영문 매뉴얼을 참고 하십시오.

1. <http://kc.forticare.com>
2. <http://docs.forticare.com>
3. <http://www.fortiguardcenter.com>
4. <http://www.fortinet.co.kr>

해당 매뉴얼은 가장 많이 배포된 FortiOS 3.0 MR5 시스템 기준으로 제작 된 것으로 상위, 하위 버전의 OS 시스템은 기능과 메뉴, 설정법 의 차이가 발생하며 모든 정보는 언제든지 변경 될 수 있습니다.

제품의 최대 동작시간은 버전에 따라 497일이며 해당기간 이상이 경과 되면 오작동을 할 수 있으므로 되도록 1년 마다 Reboot을 권장합니다.

# A

# System Features

## 1. GUI 의 새로운 menu 구성

- 서브 메뉴의 탭 내용 및 위치 변경
- 스크린 내에서 링크 활용
- 마우스 오버를 통한 정보전달
- Status 화면의 새로운 대쉬보드
- admin 사용자 로그인의 모니터와 통제기능
- 설치마법사 제외
- Content Filter 정보 통계의 그래프 지원
- 세션의 Multiple Filtering 지원
- Advanced Option 의 고급사용자 설정은 CLI로 대체되거나 간소화
- 대체메세지 4096 byte 까지 지원 / (Authentication disclaimer 12KB)

## 2. 유지 및 관리

- 설정 파일 백업의 Single File 지원
- NAT <=> TP 모드 변경 시 Reboot 안 함 / (단, Default GW 설정, 관리IP 적용 필수)
- 대량의 CLI Command 입력 지원
- 날짜 포맷의 ISO 8601 스타일로 적용 / (YYYY-MM-DD)
- SNMP MIB 강화 (MIB 와 Trap을 하나의 파일에 포함, 새로운 OID 추가)
- 언어변경 설정을 옵션 탭에서 관리자셋팅 탭으로 이동

## 3. Admin 계정의 인증연동

- admin 계정의 이름 변경 가능 / (단, admin 계정에 한해 설정 가능)
- Radius로부터 승인과 계정관리 지원
- TCP Port 조정 (HTTP > HTTPS)

## 4. 인터페이스 및 추가기능

- Link Aggregation 802.3ad 지원 / (FGT-800 모델 이상)
- Secondary Network 의 GUI 설정
- DHCP 다중서버 지원
- Inbound Traffic Shaping 지원 / (Set Inbandwidth by KB/sec)

## 5. VDOMs (Virtual Domain)

- root Domain 을 제외한 모든 모델에 10개로 제한 / (모드 무관)
- FGT-3K 이상 모델은 License 구매로 250 VDOM 지원
- NAT / TP 모드 동시지원
- Domain 별 설정영역 별도 지원 / (IP, Custom Port, Content List, VPN certs 등)
- Domain 별 administrator 계정 지정 로그인
- Inter VDOM Routing 지원 및 보호프로파일 별 bytes 값 설정 지원

## 6. HA (High Availability)

- 설정의 간소화 / (그룹이름+암호)
- 그룹 ID 와 AA 로드밸런싱 설정의 CLI 이동
- Cluster Member GUI 의 새로운 화면
- Session Pickup Option 지원 / (Default : Disable)

## 7. 라우팅

- BGP 지원
- OSPF Auto-Cost Reference Bandwidth
- RIP, OSPF GUI 설정 간소화

## 8. 방화벽

- Multiple Object 지원 / (다중범위 사용자정의)
- 정책 내에서의 Object 새로 생성 지원 / (주소, 서비스, 스케줄, 보호프로파일)
- FTP 의 Get, Put 서비스 탑재 분리
- FQDN 주소 지원
- IPv6 Policy 지원 / (CLI Only)
- 정책의 기본 Column에 Profile 표시 및 Column추가 지원 / (From, To, Count, VPN 등)

## 9. VPN

- SSL VPN 지원 / (Only Site To Host, Invest Internal Device IP)
- Policy Base IPSEC 지원
- FTP 의 Get, Put 서비스 탑재 분리
- L2TP 제거 (OS 2.80 Only)
- IKE 의 Phase1 과 Phase2 의 트리 구조화 병합 및 Phase2 의 그룹 주소 지원
- 인터넷 브라우징 제거 (OS 2.80 Only)
- Ping Generator를 Auto-Negotiate로 이동 (CLI Only) / Multiple Keep Alive 지원

## 10. 보호프로파일

- Profile 별 Anti-Virus Over Size 지원 (안티바이러스 항목에서 전체적용 설정이 이동됨)
- 웹필터 금지단어, 스팸필터 금지단어의 임계값 추가
- Client comforting 설정 추가
- Multiple Content 목록 선택 지원 (모델 별 최대값이 다름)
- IPS Severity 선택설정 가능 / MR6 이상부터 IPS Profile 선택적용 가능
- IM / P2P 가 OS 2.80 의 IPS 에서 이동되고 항목별 옵션 지원
- AV Scan 시 Client 알림 기능 제공

## 11. 인증 (Authentication)

- Active Directory 지원 (FSAE agent must be installed on AD server)
- HTTPS 추가
- RADIUS 의 MS-CHAP 과 Auto Mode 지원
- LDAP 의 regular 또는 anonymous auth 지원
- Auth 서버 타임아웃 지원 (Default 15분)

## 12. NAT

- Virtual IP Load Balancing 지원 (SLB)
- 정책 별 다중 IP – Pool 지원 (CLI Only)
- H.323, SIP 의 Session Helper 지원 향상
- LDAP 의 regular 또는 anonymous auth 지원
- Auth 서버 타임아웃 지원 (Default 15분)

## 13. 로그설정 (Logging)

- System 로그와 Auth 로그를 제외한 모든 로그설정이 보호프로파일로 이동
- Local Disk, Webtrends, 트래픽로깅 설정의 CLI 이동
- 로그보기의 Multiple Filtering 지원
- 프로토콜 별 Bandwidth 와 Volume 별 트래픽 리포트 Summary 제공

## 14. Intrusion Protection

- IPS 에서 명칭변경
- Signature severity 레벨 그룹핑 제공 (Critical, High, Medium, Low, Information)
- MR6 이상부터 IPS Sensor, Dos Sensor, Signature의 분리
- 프로토콜 Decoder 분리
- Signature 에 Trigger 되어 Packet 캡쳐가 가능하며 pcap파일로 저장 지원
- Signature 별 활성화 지정

## 15. URL 필터

- URL exempt & block + Web pattern 0| URL Filter 에 통합
- AV Scanning 을 위한 allow Action 추가
- URL 및 IP 동시 사용 가능
- Drag & Drop 을 이용한 순서 변경 지원

## 16. 컨텐츠 필터

- exempt Action 추가
- Scoring 지원 / 보호프로파일의 임계치 설정
- Pattern 80 자 이내의 Text string

## 17. 스팸 필터

- Scoring 지원 / 보호프로파일 의 임계치 설정 / 메시지당 금지단어 하나씩 Count 됨
- Black/White List 의 IP Address 와 Email Address 가 통합
- Drag & Drop 을 이용한 순서 변경 지원

## 18. New IM / P2P / VoIP

- IM : AIM 5.0+, ICQ 4.0+, MSN 6.0+, Yahoo 6.0+ 메신저들에 대한 컨트롤 지원
- QQ, Google Talk, MSN Web Messenger 는 Signature 에서 지원
- 접속 통계 (허용, 모니터 후 허용/차단 선택가능) 및 로깅 지원
- 보호프로파일에서 Action 설정 및 P2P 에 대한 Rate Limit 지정 설정 지원
- IM 의 Anti Virus Scan 지원

## B

# Fortigate OS Architecture

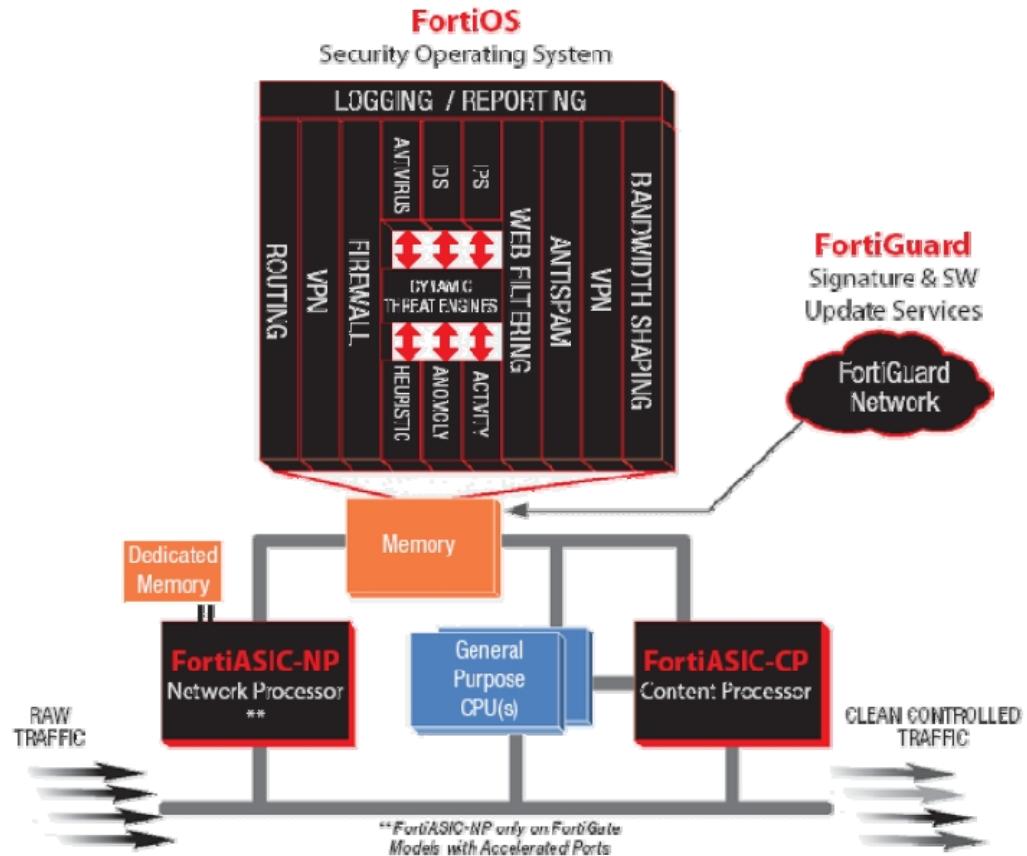
- ◆ Fortigate OS 는 다음 그림과 같이 Flexible한 Architecture를 사용하고 있습니다.

Fortigate는 주문형 반도체인 ASIC 에 의한 Packet의 고속처리가 이뤄지며 각 기능별 엔진이 별도로 동작합니다.

FortiASIC 은CP <Content Processor> 와 NP <Network Processor>를 가지고 있으며 NP는 High-End 모델에만 적용이 되어 있습니다.

NPU 시스템은 속도처리가 빠르지만 CF 메모리사용이 불가능 하기 때문에 SOHO, SMB, Enterprise를 대상으로 제공되는 모델은 NP가 탑재되어 있지 않습니다.

NP 가 탑재된 모델은 A시리즈 중 FGT-1000A-FA2 이상 모델이며 NP가 적용되는 Device를 이용해서만 사용 할 수 있습니다.



- ◆ Traffic 처리 순서는 Traffic Ingress > Routing Modul > VPN EID > F/W <ASIC>으로 처리됩니다.

ASIC 안에는 CF(AV엔진), F/W, VPN, QOS 가 동작하며 세션테이블은 CPU 에서 만들어 집니다.

Syn만 들어왔을때 테이블을 만드는 Half-Open 방식을 이용하기 때문에 Syn공격이 많아질 수 있으며 DDoS Syn Flood 공격에 대해 대응하기 위해선 고용량의 Fortigate 제품을 이용하거나 Full-Open 방식의 보안시스템을 이용하기를 권장합니다.

# C

# Brief Summary

◆ 모델 별 지원되는 기능은 동일하며 지원 인터페이스의 차이가 있습니다.

☞ Fortigate 제품은 전원이 공급되면 최초 동작 시 다음과 같은 설정이 되어 있습니다.

동작 모드	NAT / ROUTE	
관리자 계정	사용자명	admin
	비밀번호	(없음)
Internal	IP	192.168.1.99
	Subnet Mask	255.255.255.0
	Access	https, http, ping
DMZ	IP	10.10.10.1
	Subnet Mask	255.255.255.0
	Access	https, ping
DNS 서버 주소	주 DNS	65.39.139.53
	보조 DNS	65.39.139.63

☞ 회선과 연결할 외부 인터페이스인 wan1, wan2 인터페이스는 ISP로부터 IP Address를 부여 받은 VDSL 회선의 경우 DHCP 설정을 이용하여 자동으로 address를 부여 받을 수 있지만 PPPoE 방식의 ADSL회선을 이용하는 경우 접속에 필요한 계정과 비밀번호를 설정해야 합니다.

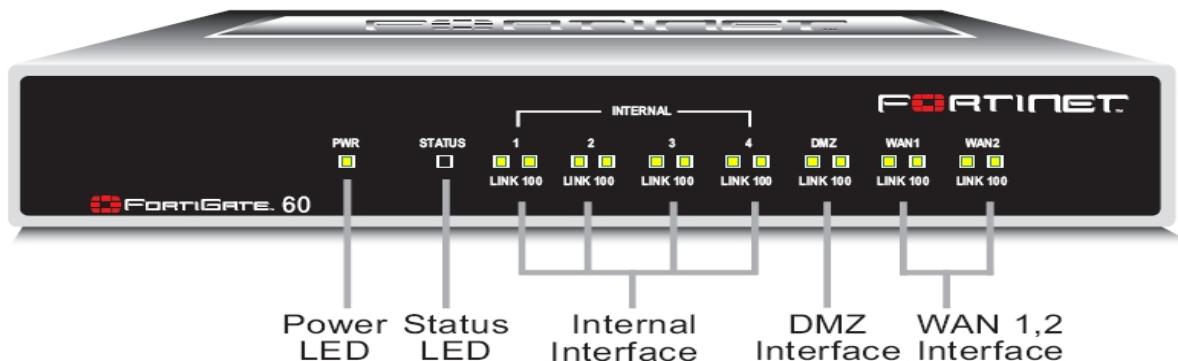
LCD가 있는 모델은 LCD 옆의 버튼을 이용하여 설정을 변경 할 수 있습니다.

☞ 제품은 바닥이 고른 곳에 설치를 해야 하며 이때 제품 좌우에 1.5인치(약 3.75cm) 의 공간을 두어 통풍이 잘 되도록 해야 합니다.

내부 동작 온도는 장비마다 다르나 0°C ~ 40°C이며 이상의 경우 장비가 다운 될 수 있습니다.

☞ 어댑터 사용 모델은 AC 입력 100~240V, DC 출력 12V 3A 의 UL 및 EMI 검증이 완료된 제품을 사용 해야 하며 전원의 보호를 위해 접지가 제공되는 콘센트를 이용해야 합니다.

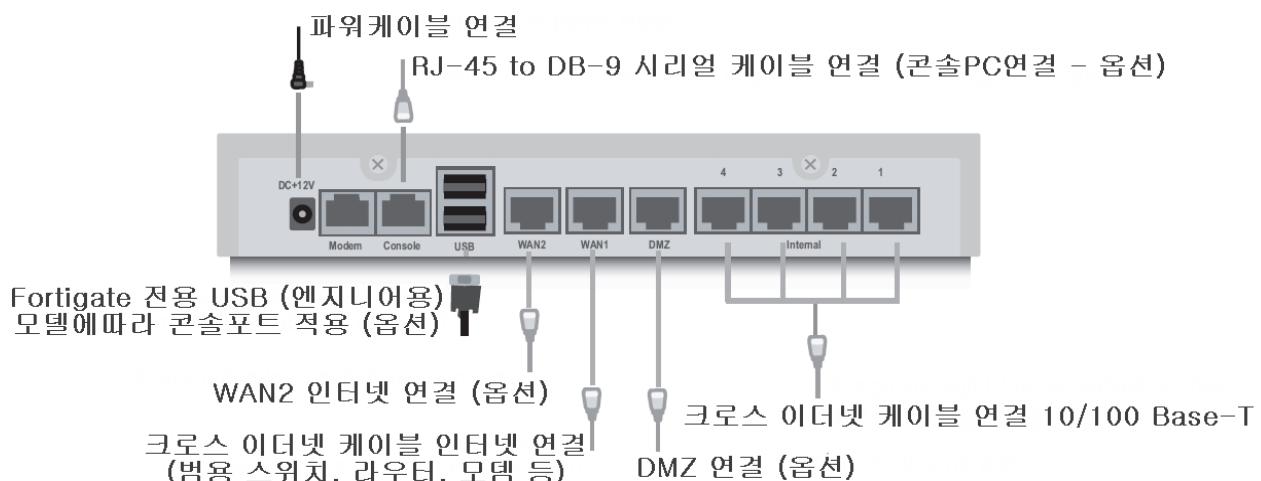
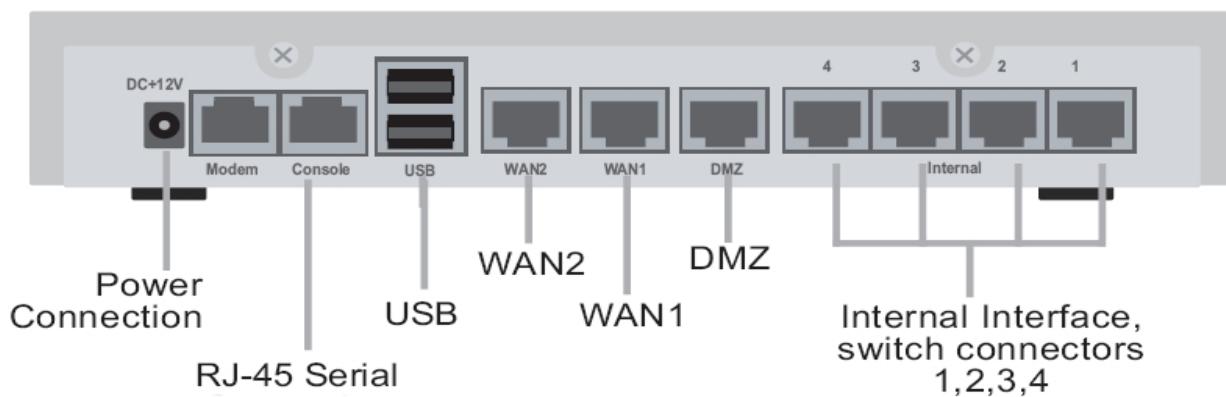
## D LED Status



이름	상태	내용
Power	녹색	전원이 공급 되었습니다.
	꺼짐	전원이 꺼져 있습니다.
Status	녹색	작동이 시작되었습니다.
	꺼짐	정상 작동 중입니다.
Link (Interface) Internal, DMZ, WAN1, WAN2	녹색	해당 인터페이스에 전원이 공급 되었습니다.
	녹색 점멸	해당 인터페이스에 네트워크 트래픽이 있습니다.
	꺼짐	케이블 연결 되지 않았습니다.
100 (Interface)	녹색	해당 인터페이스가 100 Mbps 로 연결되었습니다.

☞ Fortigate 60 은 정상 작동 시 Status LED 에 불이 들어오지 않지만 60 이외의 모델은 정상 작동 시 Status 에 녹색 램프가 표시됩니다.

## E Device Info

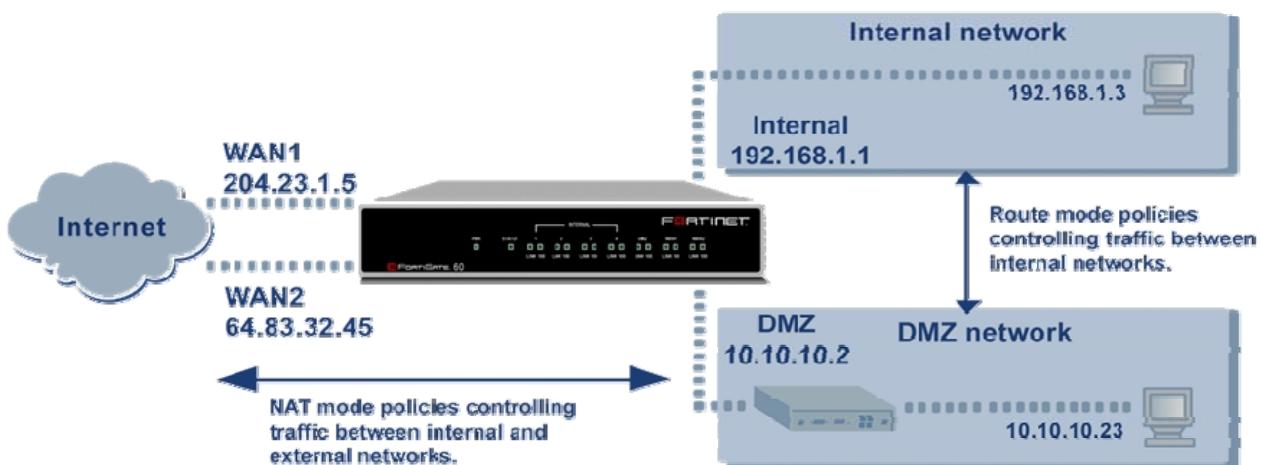


인터페이스	내용
Internal 1 ~4	RJ-45 10/100 Base-T 로 Switch 기능을 수행합니다. Speed Duplex 는 수정이 불가능 하며 모조건 Auto 로 동작합니다
WAN 1~2	RJ-45 10/100 Base-T 로 인터넷 구간과 연결합니다. WAN2 는 WAN1 과 동일하지만 선택사항 입니다..
DMZ	RJ-45 10/100 Base-T 로 DMZ 네트워크를 구성하며 선택사항 입니다.
RJ-45 Serial	DB-9, 9600 bps RS-232 로 연결하여 command 기반의 접속을 지원합니다. <b>Fortigate 300 모델만 115200 bps 이며 다른 모델은 모두 동일합니다.</b>

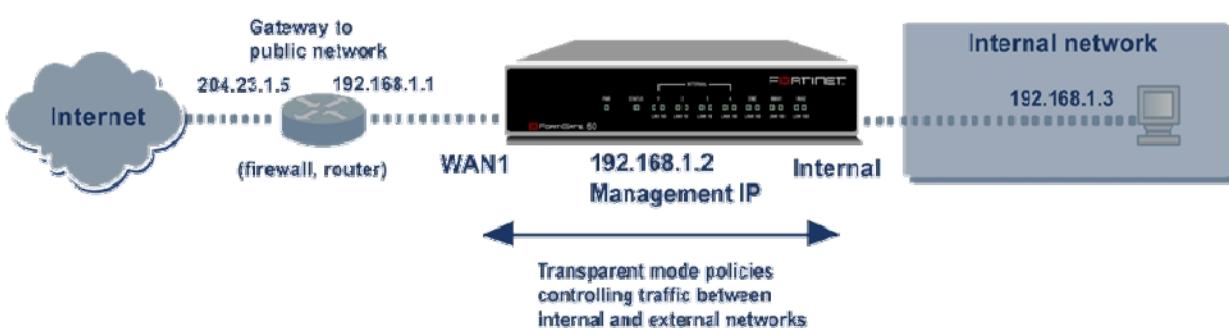
## F Fortigate Mode

◆ Fortigate 는 사설 IP를 공인 IP로 변환하여 사용하는 Network Address Translation <NAT> 모드와 공인 IP를 그대로 변환 없이 L2 스위치처럼 동작하는 Transparent <TP> 모드, Routing을 이용하여 공인 IP를 그대로 Routing 통신을 하도록 하는 Route 모드가 지원됩니다.

- ☞ NAT / Route 모드의 경우 다음 그림과 같이 구성이 됩니다.  
해당 모드의 기본 정책은 모든 트래픽이 외부로 나갈 수 있습니다.



- ☞ TP 모드의 경우 다음 그림과 같이 구성이 됩니다.  
해당 모드의 기본 정책은 모든 트래픽이 외부로 나가거나 외부의 트래픽이 들어 올 수 있습니다.



## G

# Additional Summary

- ◆ Fortigate는 웹 기반 관리자 UI로 접속하여 대부분의 설정을 할 수 있으나 특정 설정은 CLI에서만 가능하며 모든 설정이 웹 기반이 아닌 이유는 특정 기능의 경우 한번의 실수로 네트워크가 마비 될 가능성이 있기 때문입니다.

☞ 웹 기반 관리자 UI를 통해 다음과 같은 설정을 할 수 있습니다.

구성	지원 내용
시스템	상태모니터, 네트워크설정, DHCP, 관리자설정, 관리유지설정 및 백업
라우터	정적라우팅, 라우팅정책, 동적라우팅 (RIP, OSPF, BGP, 멀티캐스트) 라우팅 모니터링
방화벽	보안정책, 정책설정을 위한 object 관리, 가상주소, 보안기능
가상사설망	IPSEC, PPTP, SSL, VPN을 위한 인증서 관리
사용자	인증을 위한 사용자 계정 설정 및 인증서버
바이러스 탐지	파일차단을 위한 패턴리스트 관리, 바이러스패턴 관리, 그레이웨어 탐지 활성화
침입 방지	탐지패턴관리, 사용자정의 탐지패턴 추가, DoS Sensor (Anomaly)
웹 필터	컨텐츠필터, URL필터
안티 스팸	스팸 리스트
IM, P2P & VoIP	인터넷메신저 사용자 계정관리, P2P 사용량 통계, VoIP 사용량 통계
로그&보고서	로그관리 및 필터

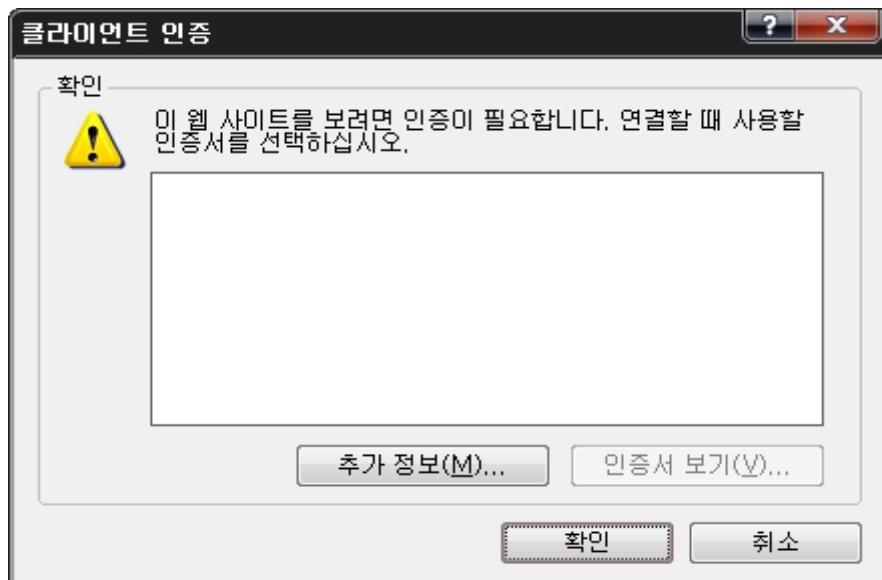
## H Web UI 접속

◆ 기본적으로 모든 Fortigate 의 Internal 의 Interface 에는 https 접속이 허용되어 있습니다.

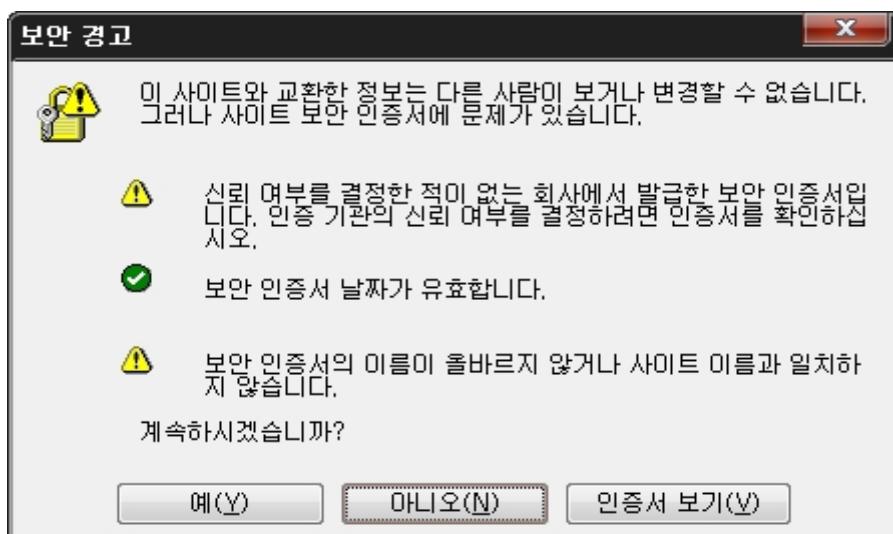
다른 Interface를 통해 관리 접속을 원하는 경우 해당 Interface의 관리적 접근 부분에 https를 활성화 해야 접근이 가능합니다.

☞ 인터넷 브라우저에 <https://<관리 IP>> 를 입력하고 접속합니다.

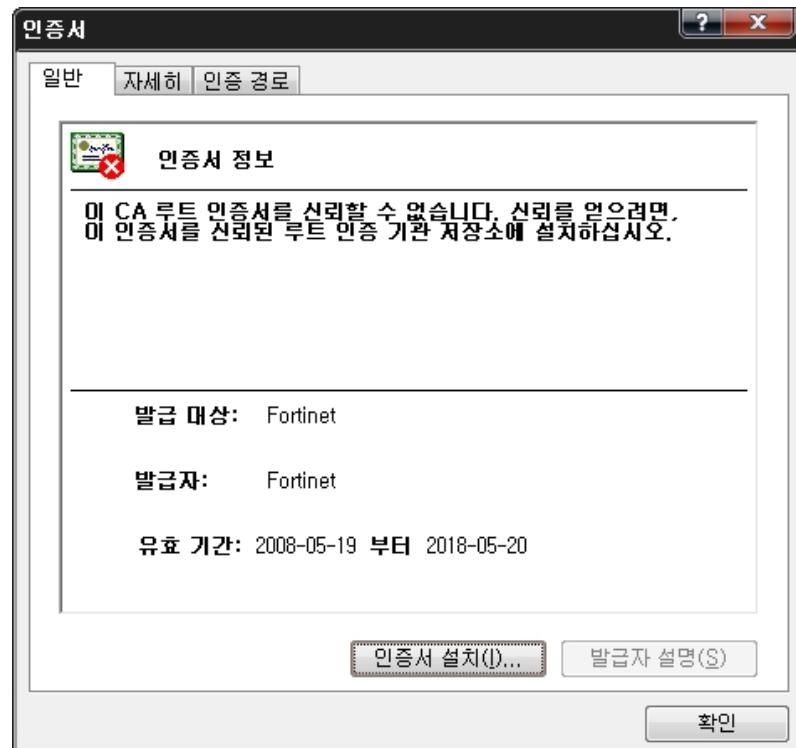
접속을 하게 되면 클라이언트 인증 창과 보안경고창이 나오게 되며 확인 버튼을 눌러 클라이언트 인증을 확인 후 보안경고창에서 ‘예’를 눌러 로그인 창으로 접속합니다.



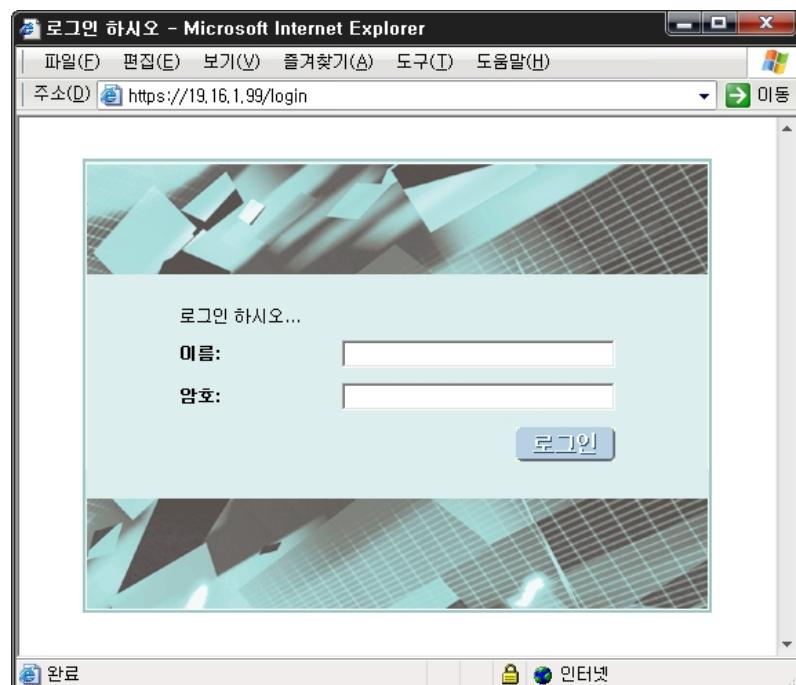
☞ 보안경고창은 인증시간이 지나기 전까지는 재 접속 시 표시되지 않습니다.



- ☞ 보안경고창에서 인증서 보기를 누르면 그림처럼 발급자가 ‘Fortinet’으로 되어 있는 것을 반드시 확인 하시기 바랍니다.



- ☞ 인증서를 확인하면 시스템에 설정된 언어로 로그인 화면이 나타나며 사용중인 시스템에 로그인을 할 수 있습니다.



## 1 시스템

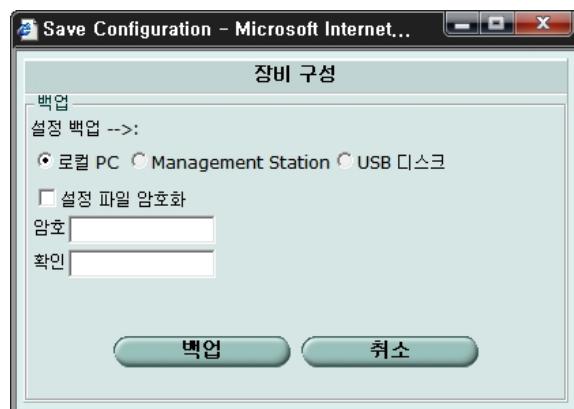
◆ 동작 시스템의 상태모니터 정보와 네트워크 관련 설정 및 관리자설정, 관리유지기능이 종합적으로 집합되어 있는 페이지입니다.

우측 제일 상단에 표시되는  아이콘을 이용하여 백업과 도움말 기능을 이용 할 수 있습니다.

 아이콘을 누르면 구매고객지원센터인 <http://support.fortinet.com> 홈페이지로 자동 연결되며 포티넷을 통해 직접 구매하여 지원을 받는 고객만 로그인 할 수 있는 계정이 생성되므로 임대고객 및 리셀러를 통한 구매자는 접근 권한이 없습니다.

 아이콘을 누르면 시스템에서 로그아웃이 됩니다.

 아이콘을 누르면 그림과 같이 시스템 설정 configuration 을 다운로드 할 수 있으며 파일의 암호화를 선택하면 백업된 파일은 워드패드 등의 프로그램으로 설정을 볼 수 없게 됩니다.  
Management Station 은 FortiManager 같은 중앙 집중 관리 시스템으로 백업이 되도록 하는 기능으로 해당 시스템과 연동이 되어 있지 않다면 상용할 수 없는 기능입니다.  
USB 디스크는 FortiUSB 제품만 지원됩니다.  
일반 USB 장치는 사용 할 수 없습니다.



 아이콘을 누르면 영어로 된 온라인헬프 페이지로 연결됩니다.

Fortigate GUI 접속 환경에서 알고자 하는 기능의 설정탭에서 해당 아이콘을 누르면 해당 기능에 대한 설명으로 바로 연결 됩니다.  
인터넷을 통한 웹브라우징이 가능한 환경에서만 사용 할 수 있으며 색인 및 검색이 가능합니다.



## 1-1 상태

◆ 상태 화면은 시스템에 접속하면 가장 먼저 보이는 화면으로 전체상태를 보여주는 기능입니다.

시스템상태, 자원사용, 라이센스, 패턴업데이트상황, 장비운영, 통계정보, 동작시간 등의 정보를 한눈에 확인 할 수 있습니다.

admin 계정 이외의 접속계정은 적용된 권한 설정에 따라 부분적 제한이 발생 할 수 있습니다.

The screenshot shows the Fortinet Web Config interface with the 'System' tab selected. On the left, there's a sidebar with various navigation options. The main content area is divided into several sections:

- System Logs:** Shows log entries such as "2008-05-14 11:38:54 폴웨어 업그레이드 by admin".
- Session Activity:** Displays current sessions and their status.
- Resource Usage:** Includes two circular gauge charts showing CPU usage at 20% and Memory usage at 65%.
- FortiGuard License:** Lists license details for various services.
- System Status:** A large section showing system status with a green bar indicating everything is OK.

☞ OS 3.0 에서는 메인 창에 JavaScript 로  
이뤄진 콘솔이 제공되며 각 대쉬보드별  
콘텐츠를 비활성화, 혹은 활성화 할 수 있습니다.

▶ 시스템 상태

타이틀 표시  
보이기/감추기

새로고침  
창없애기

## 1-1 #1 : 시스템 상태

시스템 상태	
제품 시리얼 번호	FGT-602103241916
운영시간	0 일 5 시간 23 분
시스템시간	Wed May 14 17:08:06 2008 <a href="#">[변경]</a>
HA 상태	Standalone <a href="#">[설정]</a>
호스트 명	Fortigate60 <a href="#">[변경]</a>
펌웨어 버전	Fortigate-60 3.00-b0574(MR5 Patch 5) <a href="#">[갱신]</a>
동작모드	NAT <a href="#">[변경]</a>
가상 도메인	비활성 <a href="#">[활성]</a>
현재 관리자	2 <a href="#">[상세정보]</a>

**제품 시리얼 번호** 시리얼 넘버는 펌웨어 업그레이드 및 각종 설정이 변경되는 경우에도 변하지 않는 유일한 식별번호로 기능별 라이센스정보를 확인하는 중요한 역할을 합니다.

**운영시간** 마지막 시작된 시간 이후 경과시간이 표시되는 것으로 부팅(전원ON) 이후 현재까지 동작 시간을 표시합니다.

**시스템시간** 장비가 확인하는 고유한 시간으로 각 나라 및 지역별 시간대를 지원하며 NTP 서버와 동기화 설정이 가능합니다.

‘변경’ 버튼을 눌러 설정을 변경 할 수 있습니다.

**HA 상태** High Availability 사용 상태를 확인 할 수 있으며 ‘설정’을 눌러 2개 이상의 장비를 이용 하여 HA 구성을 할 수 있습니다.

**호스트 명** 장비를 식별하기 위한 이름입니다. ‘

**펌웨어 버전** 현재 장비에 설치된 Forti-OS 의 버전이 표시되며 GUI 로 업그레이드를 할 수 있습니다.  
**설정이 초기화 되므로 반드시 주의를 요합니다.**

**동작모드** 현재 동작 모드를 표시하며 모드를 변경하면 인터페이스IP와 게이트웨이IP는 설정 할 수 있습니다.

**설정이 초기화 되므로 반드시 주의를 요합니다.**

**가상 도메인** 물리적으로 1개의 장비를 논리적으로 여러 개의 장비로 사용하기 위한 기능으로 다른 모드와 동시 사용이 가능하며 장비 모델 별 지원 개수가 다릅니다.

**현재 관리자** 장비에 접속한 사용자수를 표시하며 ‘상세정보’로 ID와 접속타입을 보여줍니다.

## 1-1 #2 : 통계 및 세션

☞ 현재 처리중인 세션통계를 표시하여 Fortigate 가 스캔하는 HTTP, HTTPS, SMTP, POP3, FTP, IM 프로토콜에 대한 컨텐츠 필터 및 AV, IPS 기능을 통해 저장된 로그 이력에 대한 간략정보 및 통계를 확인 할 수 있으며 해당 내용의 상세 정보는 각 항목의 [상세]를 눌러 확인 할 수 있습니다.

 통계 (기록시작일 2008-07-06 10:24:02)

세션	1194 현재 세션	[상세]
<b>콘텐츠 기록</b>		
HTTP	2103 사용한 URL들	[상세]
HTTPS	0 사용한 URL들	[상세]
이메일	3076 보낸 이메일 1134 받은 이메일	[상세]
FTP	14 사용한 URL들 0 파일 업로드 18 다운로드한 파일	[상세]
IM	0 전송된 파일 0 채팅 세션 0 메시지	[상세]
<b>침입 로그</b>		
AV	37 바이러스 차단	[상세]
IPS	327 침입 차단	[상세]
스팸	556 spams detected	[상세]
웹	0 URL 차단	[상세]

☞ 콘텐츠 기록 상세정보와 침입로그 상세정보는 보관할 수 있는 임계 값이 제한되어 있으며 리부팅 시 기록된 내용은 초기화 됩니다.

 최근에 차단된 바이러스 - Microsoft Internet Explorer

가장 최근의 트랜잭션(최대 10).				
날짜 & 시간	From	To	서비스	바이러스
2008-07-15 13:17:22	125.143.6.208	222.99.41.195	smtp	W32/Virut.A
2008-07-14 23:27:40	118.218.8.22	222.99.41.195	smtp	W32/Virut.A
2008-07-14 23:27:25	118.218.8.22	222.99.41.195	smtp	W32/Virut.A
2008-07-14 23:09:12	118.218.8.22	222.99.41.195	smtp	W32/Virut.A
2008-07-14 23:08:56	118.218.8.22	222.99.41.195	smtp	W32/Virut.A
2008-07-14 17:32:41	118.218.8.22	222.99.41.195	smtp	W32/Virut.A
2008-07-14 17:32:25	118.218.8.22	222.99.41.195	smtp	W32/Virut.A
2008-07-14 17:14:17	118.218.8.22	222.99.41.195	smtp	W32/Virut.A
2008-07-14 17:14:01	118.218.8.22	222.99.41.195	smtp	W32/Virut.A
2008-07-14 17:13:31	124.54.206.185	222.99.41.195	smtp	W32/Virut.B

종료

☞ 장시간 내용을 저장보관 하기 위해서는 FortiAnalyzer 로그전용 장비를 연동해야 합니다.

- ☞ 실시간 트래픽 정보를 통계>세션 의 [상세]를 누르면 아래 그림과 같이 상세 정보가 표시됩니다.  
처리중인 세션을 실시간 모니터링 및 검색과 필터링, 강제 삭제가 가능하며 적용되는 정책도 확인 할 수 있습니다.



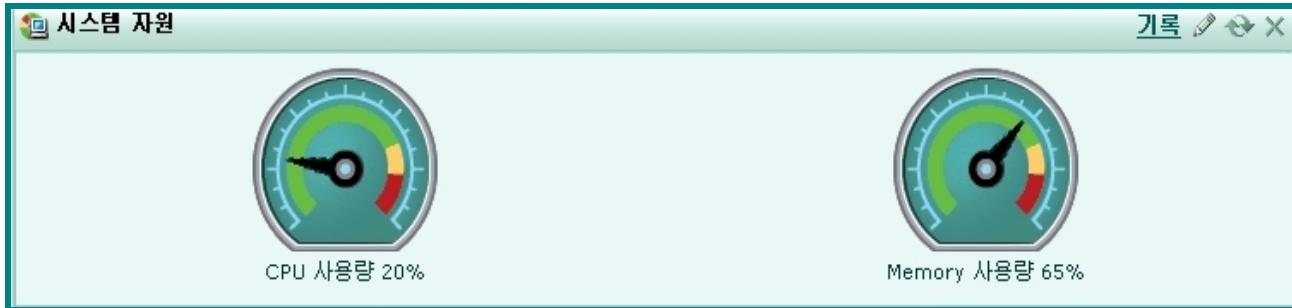
The screenshot shows the Fortinet Web Config interface under the 'WEB CONFIG' tab. On the left, there's a sidebar with various system settings like Network, Configuration, and Firewall. The main window is titled '상세' (Details) and displays a table of active sessions. The table has columns for #, 프로토콜 (Protocol), 출발지 주소 (Source IP), 출발지 포트 (Source Port), 목적지 주소 (Destination IP), 목적지 포트 (Destination Port), 정책 ID (Policy ID), 만기 (sec) (Expiration), and a trash icon. There are 18 entries in the table, mostly for TCP connections from 222.99.41.221 to various destination IPs and ports.

- ☞ 세션모니터링의 필터링은 각 필드의 필터아이콘을 눌러 필터링을 적용이 가능합니다.  
<출발지주소+출발지포트+정책 ID>와 같이 필터 조합은 가능하지만 <출발지주소+출발지주소> 와 같은 동일 필드의 중복 필터는 불가능 합니다.
- ☞ 세션의 기본 유지시간은 3600 초(1 시간)이며 CLI 에서 기본값 혹은 서비스 port 별로 수정 할 수 있습니다. (300 초 ~ 604800 초 범위 이내)  
단, UDP 와 ICMP 는 세션으로 간주하지 않습니다. 따라서 Session\_ttl 을 조절할 수 없습니다.
- ☞ 세션타임의 결정시 우선순위의 1 번째는 응답자와 요청자와 의 Negotiation 에 의한것이며 2 번째는 Fortigate 에서 수정 된 값, 3 번째는 Fortigate 의 기본값입니다.  
세션의 Timeout 의 결정은 목적지 기준으로 목적지의 시스템이 기본 세션타임이 정의된 세션타임 보다 작은 경우 최소값으로 적용됩니다.  
일정시간 경과 후 강제적으로 연결이 끊어진다면 세션의 만기시간에서 목적지 시스템과의 세션타임을 체크하시기 바랍니다.  
VoIP 시스템들과 같이 UDP 통신을 이용하는 시스템은 사용 포트로 주기적인 keepalive check 를 하게 되면 장애 없는 통신이 가능합니다.

## 1-1 #3 : 시스템 자원

☞ 장비의 CPU, Memory 사용량을 간략하게 그래프 형태로 보여줍니다.

현재 연결되어 있는 트래픽 처리량에 따라 차이가 있으며 90% 이상 점유를 하고 있다면 과부하가 발생 하는 것으로서 처리량 부족 및 내부의 유해 트래픽 발생에 의한 것이 원인의 대부분입니다.



☞ <기록>을 누르면 아래 그림과 같이 막대그래프 형태로 확인이 가능 하며 최대 24시간까지의 정보를 볼 수 있습니다.

네트워크 사용량은 Inbound 와 Outbound 트래픽을 합친 데이터 이므로 단방향 모니터링 및 IP별 트래픽 확인은 불가능 하지만 필요한 경우 SNMP와 트래픽 로깅을 이용한 MRTG, PRTG 등을 연동하면 네트워크 트래픽을 모니터링 할 수 있습니다.



## 1-1 #4 : 라이센스 정보

- ◆ 라이센스 계약 사항에 대한 상세 정보를 표시해주며  표시는 정상  는 비정상  는 사용할 수 없다는 표시입니다.

 지원계약은 현재 사용하는 라이센스의 만기 상황을 표시합니다.

안티바이러스와 침입방지에 대해 만기일이 동일하지만 웹필터, 안티스팸은 라이센스 만기일이 차이가 있을 수 있습니다.

만기 이후에는 자동 업데이트가 지원이 되지 않습니다.

라이센스 기간에 대한 부분은 임대서비스사업자 혹은 판매처에 문의 바랍니다.

라이센스 정보		
지원 계약	Valid FortiOS 3.000 (만기 2008-11-08)	
<b>FortiGuard 가입계약</b>		
안티 바이러스	정식 라이센스 (만기 2008-11-08)	
AV 패턴	9.203 (업데이트 됨 2008-06-16) <a href="#">[갱신]</a>	
침입 방지	정식 라이센스 (만기 2008-11-08)	
IPS 패턴	2.513 (업데이트 됨 2008-06-14) <a href="#">[갱신]</a>	
웹 필터링	라이센스 없음 <a href="#">[가입]</a>	
안티 스팸	라이센스 없음 <a href="#">[가입]</a>	
Management Service	도달불가 <a href="#">[설정]</a>	
Analysis Service	만료 <a href="#">[재개]</a>	
Services Account ID	<a href="#">[변경]</a>	
<b>가상 도메인</b>		
허용된 VDOM 수	10	

 FortiGuard 서비스란 Fortinet Distribution Server (FDS)에서 제공하는 AV, IPS 엔진과 패턴을 자동으로 업데이트 하여 최신에 상태를 유지해주는 서비스입니다.

FortiGuard 서비스가 사용하는 Port는 TCP 8690, TCP 8890, TCP 443, UDP 9443, UDP 8888, UDP 53이며 Fortigate 상단의 시스템에서 해당 포트가 차단되거나 FDS 서버의 라우팅 경로가 차단 되면 라이센스 체크 및 업데이트가 안됩니다.

 Management Service 와 Analysis는 Integrated FortiGuard Security Subscription Services라는 Fortinet에서 제공하는 정기구독 서비스입니다.

전용 중앙집중 관리 시스템인 FortiManager 와 전용 로그수집 및 리포팅 시스템인 FortiAnalyzer를 이용하는 것과 동일한 서비스입니다.

## 1-2 네트워크

◆ 네트워크 상황을 표시해주며 네트워크 관련 각종 설정을 하는 기능입니다.

Fortigate-60B 이상의 제품은 Internal 인터페이스를 별도의 분리된 인터페이스처럼 구성이 가능하며 Switch Port Interface 는 NAT/ROUTE 모드에서만 사용이 가능합니다.

**동작 모드에 따라 제공되는 기능의 차이가 있습니다.**

## 1-2 #1 : 인터페이스

- ☞ IP설정 및 접근 설정 관련 기능을 제공하며 NAT 모드의 경우 인터페이스에 고정IP, DHCP(VDSL) Client, PPPoE(ADSL) Client로 설정 할 수 있으며 동작모드와 상관없이 외부접근의 대한 허용 프로토콜의 활성화 및 비활성화가 가능합니다.
- ☞ NAT/Route 모드의 경우 인터페이스 IP설정을 변경 할 수 있으며 모든 인터페이스는 고정, 유동 설정이 가능합니다.

WEB CONFIG					
시스템		인터넷	지역	옵션	
<b>새로생성</b>					
이름	IP / 넷마스크	접근	상태		
dmz	10.10.10.1 / 255.255.255.0	HTTPS,PING	▣ 다운 시키기		
internal (사설)	19.16.1.1 / 255.255.255.0	HTTPS,PING,HTTP,TELNET	▣ 다운 시키기		
modem	/		▣ 다운 시키기		
wan1 (유동)	18.144.180.180 / 255.255.255.192	HTTPS,PING,HTTP,TELNET	▣ 다운 시키기		
wan2 (고정)	21.131.216.116 / 255.255.255.224	HTTPS,PING,HTTP,TELNET	▣ 다운 시키기		

- ☞ TP 모드의 경우 인터페이스에 IP가 할당 되지 않으며 인터페이스 자체에 설정은 불가능 해집니다. 하지만, 관리용 IP가 설정된 경우에 대한 외부 접근 라우팅테이블 설정이 추가됩니다.

관理용 IP의 설정은 시스템 > 구성 > 동작 탭에서 생성 및 수정이 가능합니다.

WEB CONFIG					
시스템		인터넷	지역	옵션	라우팅 테이블
<b>새로생성</b>					
이름	IP / 넷마스크	접근	상태		
dmz		HTTPS,PING	▣ 다운 시키기		
internal		HTTPS,PING,TELNET	▣ 다운 시키기		
wan1		HTTPS,PING,TELNET	▣ 다운 시키기		
wan2		PING	▣ 다운 시키기		

- ☞ NAT 모드의 경우 ISP로부터 부여 받은 IP가 유동회선인 경우 <서버로 부터 기본 게이트웨이 검색>이 활성화가 되어 있어야 게이트웨이 정보를 받아오게 되므로 반드시 활성화를 해야 합니다.  
Alias에 비고사항을 입력하면 인터페이스 용도 구분 및 정책생성시 관리가 편리 할 수 있습니다.

The screenshot shows the 'WEB CONFIG' interface under the '인터넷' tab. On the left sidebar, '네트워크' is selected. The main panel displays '인터넷' configuration. The '인터넷' tab is active. The '인터넷' section includes fields for '인터넷' 명 (wan1), 'Alias' (유동), and '모드' (DHCP selected). It also shows connection details like IP/Netmask (218.144.180.180/255.255.255.192), DNS (168.126.63.1, 168.126.63.2), and basic gateway (218.144.180.190). Below this, there are sections for DDNS, Ping server (168.126.63.1), management access (HTTPS checked), and MTU (1500 bytes). A note at the bottom says '서버로 부터 기본 게이트웨이 검색' (Search for default gateway from server) and '내부 DNS 오버라이드' (Override internal DNS). Buttons at the bottom include '확인' (Confirm), '취소' (Cancel), and '적용' (Apply).

- ☞ TP(투명) 모드의 경우 인터페이스에 IP를 부여할 순 없습니다.

The screenshot shows the 'WEB CONFIG' interface under the '인터넷' tab. On the left sidebar, '네트워크' is selected. The main panel displays '인터넷' configuration. The '인터넷' tab is active. The '인터넷' section includes fields for '인터넷' 명 (internal) and 'Alias'. It shows management access options (HTTPS checked, SSH, PING, SNMP, HTTP, TELNET) and MTU settings (1500 bytes). A note at the bottom says '나가는 패킷이 MTU 사이즈 보다 큰 경우' (If outgoing packets are larger than MTU size). Buttons at the bottom include '확인' (Confirm), '취소' (Cancel), and '적용' (Apply).

- ☞ Fortigate는 OSI 7 Layer 의 Layer 3 장비들과 동일하게 인터페이스에 Secondary Network를 추가 할 수 있으며 GUI 에서 설정이 가능합니다.

The screenshot shows the 'WEB CONFIG' interface with the 'Interface' tab selected. On the left, a sidebar lists various system and security settings. The main panel is titled '인터페이스 편집' (Interface Edit) and contains the following fields:

- 인터페이스 명:** dmz (00:09:0F:0A:7D:E9)
- Alias:** [empty input field]
- 매니얼 모드:**  매니얼  DHCP  PPPoE  
IP/넷마스크: 10.10.10.1/255.255.255.0
- DDNS:** 활성 (checkbox checked)
- 관리적 접근:**
  - Ping 서버: [empty input field] 활성 (checkbox checked)
  - HTTPS:
  - PING:
  - HTTP:
  - SSH:
  - SNMP:
  - TELNET:
- MTU:** 나가는 패킷이 MTU 사이즈 보다 큰 경우 1500 (바이트)
- 두번재 IP 주소(secondary):**
  - IP / 넷마스크: 20.20.20.1/24
  - Ping 서버: 0.0.0.0 활성 (checkbox checked)
  - 관리적 접근: HTTPS, PING, HTTP, TELNET (checkboxes checked)
- Add:** [button]
- Table:** A table showing the current interface configurations:
 

#	IP / 넷마스크	핑 서버	활성	관리적 접근
1	20.20.20.1/24	0.0.0.0	(edit)	HTTPS PING HTTP TELNET

- ☞ 핑 서버는 설정된 IP로 주기적인 핑 체크를 통해 회선의 정상적인 통신 상태를 체크 할 수 있으며 핑서버에 반응이 없으면 인터페이스는 자동 다운됩니다.  
회선 이중화 구성의 경우 NLB(Network Load Balacing) 와 FailOver 구성이 가능합니다.

- ☞ Fortigate는 인터페이스에 VLAN을 추가 할 수 있습니다.

IEEE 802.1Q 프로토콜만 지원하며 ISL 같은 특정 벤더사의 자체개발 Encapsulation 방식은 지원되지 않습니다.

L2 Switch 와 VLAN ID가 동일 해야 하며 숫자로만 구성, Fortigate 와 연결된 L2 Switch 인터페이스는 반드시 Trunk 설정이 되어 있어야 합니다.

The screenshot shows the 'WEB CONFIG' interface with the 'Interface' tab selected. On the left, a sidebar lists various system and security settings. The main panel is titled '새로생성' (Create New) and displays a table of existing VLAN networks:

이름	IP / 넷마스크	접근	상태
dmz (VLAN Network)	10.10.10.1 / 255.255.255.0	HTTPS,PING	디운 시키기
Vlan	1.1.1.1 / 255.255.255.0	HTTP	디운 시키기
internal (사설)	19.16.1.1 / 255.255.255.0	HTTPS,PING,HTTP,TELNET	디운 시키기
modem	/		디운 시키기
wan1 (유동)	218.144.180.180 / 255.255.255.192	HTTPS,PING,HTTP,TELNET	디운 시키기
wan2 (고정)	121.131.216.116 / 255.255.255.224	HTTPS,PING,HTTP,TELNET	디운 시키기

## 1-2 #2 : 지역 (Zone)

☞ 지역(Zone)이란 물리적인 2개의 인터페이스를 논리적으로 1개의 인터페이스처럼 사용하는 기능이며 하나의 지역(Zone)으로 묶인 인터페이스는 정책 적용 시 묶인 지역(Zone) 인터페이스로 표시됩니다.

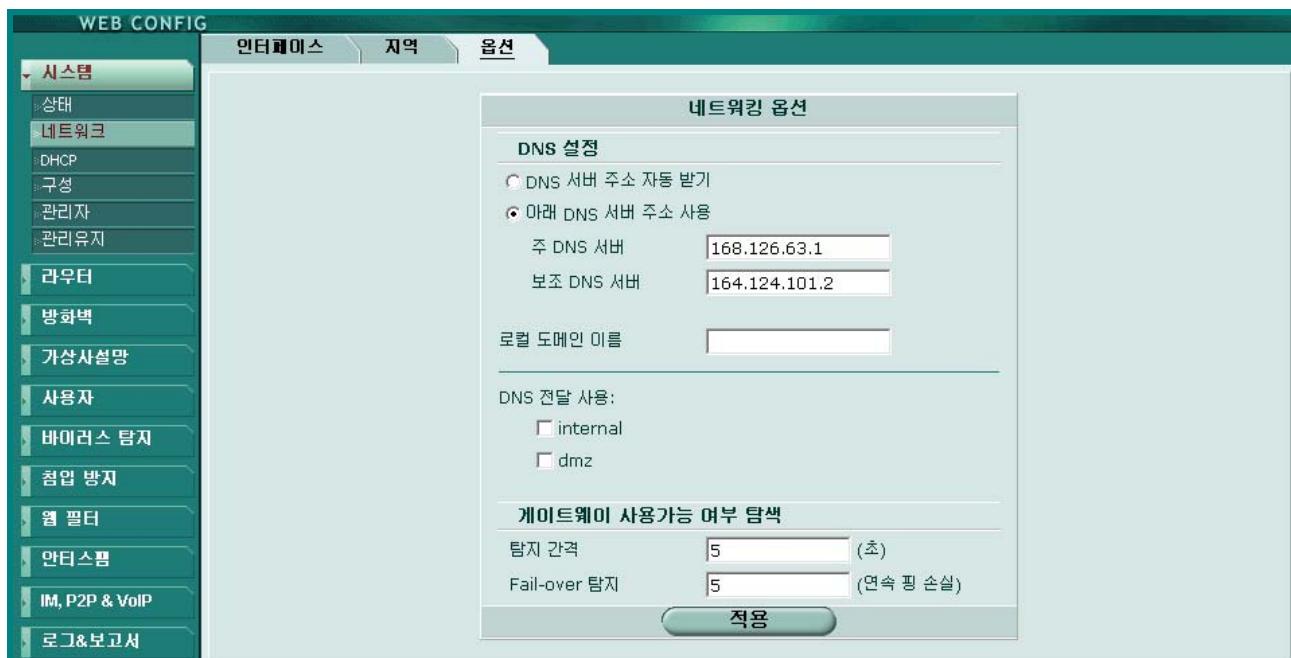


☞ <내부 영역으로의 트래픽 차단> 기능을 이용하여 내부끼리의 불필요한 통신을 차단 할 수 있습니다.



## 1-2 #3 : 옵션

- ☞ 옵션내의 DNS 설정은 Fortigate의 DNS Resolve Request를 위해 설정을 하는 기능입니다.  
업데이트 및 FQDN 과 URL 필터 등을 이용할 때 필요로 하며 DNS 설정은 사용하는 ISP 회선과 가장 가까운 DNS 서버로 설정하기를 권장합니다.



- ☞ DNS 전달 기능은 PC들의 DNS 서버를 Fortigate로 설정한 경우 사용이 가능하지만 제품의 과부하를 유발하게 되므로 사용을 비권장 합니다.
  - ☞ 게이트웨이 사용가능 여부 탐색 기능은 인터페이스에 설정된 Ping서버를 체크하는 Interval 값이며 기본값 사용을 권장합니다.
- Dual Active Wan 네트워크 구성 시 유용하게 적용 될 수 있습니다.

## 1-2 #4 : 라우팅 (TP Mode Only)

- ☞ 관리접속을 위해 외부에서 접근 시 Fortigate가 사용하는 게이트웨이를 설정하는 기능입니다.  
해당 기능은 TP(투명)모드인 경우에만 표시되는 부분이므로 NAT/Route 모드의 사용자에겐 해당되지 않습니다.  
NAT/ROUTE 사용자의 라우팅 설정은 트리항목에 별도로 지원됩니다.
  
- ☞ Fortigate 의 TP(투명) 모드는 L2 스위치처럼 관리용 IP가 존재합니다.  
외부에서 관리용IP 에 접속하기 위해서는 반드시 라우팅 테이블이 존재해야 하며 동일 서브넷에서 사용하는 회선 게이트웨이 IP 입니다.  
TP 모드에서는 라우팅 테이블이 없어도 동일 서브넷에서는 시스템의 접속이 가능합니다.



The screenshot shows the 'WEB CONFIG' interface of a Fortigate device. The left sidebar has a tree view with '시스템' expanded, showing '상태', '네트워크' (which is selected), '구성', '관리자', and '관리유지'. The main tab bar at the top has tabs for '인터넷', '지역', '옵션', and '라우팅 테이블' (which is selected). Below the tabs is a button labeled '새로생성' (Create New). A table below the button contains four columns: IP, 마스크 (Mask), 게이트웨이 (Gateway), and Distance. There is one row in the table with values: IP 0.0.0.0, Mask 0.0.0.0, Gateway 121.153.23.129, and Distance 10. To the right of the table are icons for delete and edit.

IP	마스크	게이트웨이	Distance
0.0.0.0	0.0.0.0	121.153.23.129	10

## 1-3 DHCP

- ◆ NAT/Route 기능을 사용하는 경우 DHCP서버 와 DHCP relay agent를 제공하며 DHCP Lease 상태에 대한 모니터링을 제공하는 기능입니다.

## 1-3 #1 : 서비스

☞ DHCP 는 해당 인터페이스에서 사용중인 IP 대역에 한해서만 범위 설정이 가능하며 사용 중이 아닌 대역으로 설정을 하면 적용이 되지 않습니다.

임대시간은 설정 및 범위 내에서 특정 IP만 제외하는 기능이 제공됩니다.

Wins 서버를 사용중인 경우 해당 서버에 대한 정보를 DHCP에 설정이 가능하고 bootp agent를 위한 추가 옵션이 제공됩니다.

bootp 상세정보는 ‘RFC 2132’번 과 ‘RFC 951’번 BOOTP Vendor Extensions 정보를 확인하십시오.



제외 범위:	추가
시작 IP: 19.16.1.15	삭제
끝 IP: 19.16.1.17	

- DHCP서버, 릴레이 설정은 각 인터페이스 별 설정이 가능합니다.

DHCP 서버에서 Lease 할 수 있는 IP는 인터페이스에 할당된 IP대역이 아니면 적용되지 않습니다.



The screenshot shows the Fortinet Web Config interface under the 'WEB CONFIG' tab. On the left, there's a sidebar with various system and network management options. The main area is titled '동적 IP' (Dynamic IP) and contains a table for configuring DHCP services across different interfaces and VLANs. The table has columns for '인터페이스' (Interface), '서비스' (Service), '타입' (Type), and '사용' (Usage). There are several sections listed:

- Vlan**: Contains entries for '릴레이' (Relay) and '서버' (Server).
- dmz(VLAN Network)**: Contains entries for '릴레이' (Relay) and '서버' (Server).
- internal(사설)**: Contains entries for '릴레이' (Relay) and '서버' (Server). The '서버' row is highlighted in yellow.
- wan1(유동)**: Contains entries for '릴레이' (Relay) and '서버' (Server).
- wan2(고정)**: Contains entries for '릴레이' (Relay) and '서버' (Server).

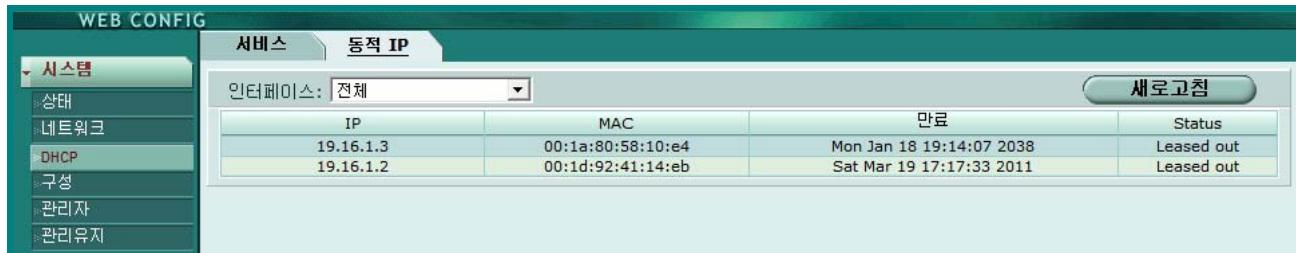
In the 'internal' section, the '서버' row is selected, and its details are shown below the table: 'Internal-DHCP' is listed under '서비스', and '레귤러' (Regular) is listed under '타입'. There are also icons for edit, add, and delete operations.

- 세컨드리 네트워크를 사용중인 경우 DHCP 서버를 여러 개 적용할 수 있으며 Reserved Address 를 제외하고 우선순위는 첫 번 째 서버부터 적용됩니다.

세컨드리 네트워크만 별도로 DHCP 기능적용은 불가능 하며 반드시 2 개 이상의 DHCP 서버를 이용하기 위해선 인터페이스의 Master DHCP 서버가 적용되어 있어야 하며 Master DHCP 서버의 DHCP 정보가 모두 할당 된 이후부터 순차적으로 할당 됩니다.

## 1-3 #2 : 동적 IP

☞ 동적 IP에서는 IP를 받아간 시스템의 mac address 와 매칭된 IP를 확인 할 수 있습니다.



IP	MAC	만료	Status
19.16.1.3	00:1a:80:58:10:e4	Mon Jan 18 19:14:07 2038	Leased out
19.16.1.2	00:1d:92:41:14:eb	Sat Mar 19 17:17:33 2011	Leased out

☞ OS 2.8 에서 사용하던 ‘IP/MAC Binding’ 기능은 GUI 에서 제외되었습니다.

대신 OS 3.0 에서 DHCP Reserved 란 명칭으로 변경되었으며 CLI 에서만 설정이 가능합니다.

60 모델의 경우 20개 까지만 제공되며 상위장비의 경우 더 많은 설정을 할 수 있습니다.

CLI 명령어는 한글 자 오타로도 장애가 발생 할 수 있으므로 반드시 주의를 필요로 합니다.

### ◆ DHCP Reserved Configuration Command

```
Fortigate # config system dhcp reserved-address
Fortigate (reserved-address) # edit <name>
Fortigate (name) # set ip <ip address>
Fortigate (name) # set mac <mac address>
Fortigate (name) # set type regular
Fortigate (name) # end
```

## 1-4 구성

- ◆ HA 이중화 구성설정, SNMP Agent 설정, Fortiget 가 표시해주는 대체 메시지 변경, 시스템의 동작 모드 변경 및 설정을 하는 기능입니다.

### 1-4 #1 : 이중화

☞ 2대 이상의 제품을 이용하여 HA Virtual Clustering 을 구성 할 수 있습니다.

단일 모드는 HA 비활성화 상태이며 이때 동작 방식은 Active-Passive 와 Active-Active 로 선택 할 수 있으며 연결하는 2개의 시스템에서 동일한 동작방식을 사용해야 합니다.

포트 모니터	Enable	Priority(0-512)
dmz(VLAN Network)	<input type="checkbox"/>	<input checked="" type="checkbox"/> 50
internal(사설)	<input type="checkbox"/>	<input type="checkbox"/> 0
wan1(유동)	<input type="checkbox"/>	<input checked="" type="checkbox"/> 50
wan2(고정)	<input type="checkbox"/>	<input type="checkbox"/> 0

## 1-4 #2 : SNMP

☞ SNMP(Simple Network Management Protocol)를 이용한 MRTG, PRTG 등을 구성하여 트래픽정보 및 하드웨어 상태정보 모니터링 시스템을 구축 할 수 있습니다.

OID 값은 <http://kc.forticare.com/default.asp?SID=&Lang=1&id=1370>에서 확인이 가능합니다.

MIBs 파일은 기술지원 엔지니어, 제품 구입처 및 기술지원센터를 통해 받으실 수 있습니다.

SNMP 를 구성하였다면 SNMP 서버가 위치한 인터페이스에 접근허용 설정이 되어 있어야 합니다.

이름	요청	트랩	활성
kt-bizmeka	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

☞ SNMP서버가 SNMP 에이전트에게 질의 요청 시 정보를 제공하며 호스트 IP 주소는 접근허용 SNMP 서버 IP 입니다.

호스트의 IP 주소를 0.0.0.0으로 설정 시 모든 서버의 접근이 허용됩니다.

SNMP는 Version1 과 Version2 가 지원되며 질의 및 트랩정보 포트 수정이 가능합니다.

☞ SNMP 이벤트는 16가지 정보 중 필요한 이벤트만 활성화 할 수 있습니다.

프로토콜	포트	활성
v1	161	<input checked="" type="checkbox"/>
v2c	161	<input checked="" type="checkbox"/>

프로토콜	로컬	원격	활성
v1	162	162	<input checked="" type="checkbox"/>
v2c	162	162	<input checked="" type="checkbox"/>

SNMP 이벤트	활성
CUP 과부하	<input checked="" type="checkbox"/>
메모리 부족	<input checked="" type="checkbox"/>
로그 기록용 고정 디스크 용량 부족	<input checked="" type="checkbox"/>
HA 클러스터 상태 변경	<input checked="" type="checkbox"/>
HA Heartbeat 실패	<input checked="" type="checkbox"/>
HA Member Up	<input checked="" type="checkbox"/>
HA Member Down	<input checked="" type="checkbox"/>

## 1-4 #3 : 대체메세지

☞ 대체메시지는 적용을 받는 사용자에게 보여지는 메시지로 시스템 언어가 한글인 경우 메시지내용도 한글로 수정이 가능합니다.

항목의 제일 앞부분인 ▶ 버튼을 누르면 상세항목이 펼쳐지며 화살표가 ▼ 모양으로 변경되며 각각의 기능에 대한 세부설정을 확인 및 변경 할 수 있습니다.

이름	설명
▶ 메일	유효하지 않은 메일 서비스 메시지.
▶ HTTP	유효하지 않은 웹 서비스 메시지.
▶ FTP	유효하지 않은 FTP 서비스 메시지.
▶ NNTP	유효하지 않은 NNTP 서비스 메시지.
▶ 경고 메일	경고 메일 메시지.
▶ 스팸	유효하지 않은 SMTP 서비스 메시지.
▶ Administration	Replacement for administration messages.
▶ 인증	인증 페이지 대체 메시지.
▶ FortiGuard 웹 필터링	FortiGuard 웹 필터링 대체 메시지.
▶ 인터넷 메신저와 P2P	차단된 메신저와 P2P 대체 메시지.
▶ SSL VPN	SSL VPN 대체 메시지.
SSL VPN 로그인 메시지	SSL VPN 로그인 메시지.

☞ HTML 포맷이 지원되며 java script를 이용하는 경우 시스템에 버그가 발생 할 수 있습니다.

메시지 설정: SSL VPN 로그인 메시지  
허용된 포맷: HTML  
크기: 8192 (글자)

```
window.opener.top.location; self.close(); } //--></script></head><body>
class="main"><center><table width="100%" height="100%" align="center" class="container"
valign="middle" cellpadding="0" cellspacing="0"><tr valign="middle"><td><form
action="%%SSL_ACT%%" method="%%SSL_METHOD%%"
name="f"><table class="list" cellpadding=10
cellspacing=0 align=center width=400 height=180>%%SSL_LOGIN%%</table>%%SSL_HIDDEN%%
</td></tr></table></form></center></body><script>document.forms[0].username.focus();</script></html>
```

**확인** **취소**

## 1-4 #4 : 동작

◆ 시스템의 동작모드가 표시되어 있으며 모드의 변경 설정을 할 수 있습니다.

**모드를 변경하게 되면 모든 설정이 초기화 되므로 반드시 주의가 필요합니다.**

☞ NAT/ROUTE 모드 사용자는 NAT로 표시되어 있으며 <동작 모드>를 변경 할 수 있습니다.



☞ 투명모드 사용자는 <관리 IP/넷마스크>가 표시되어 있으며 수정 할 수 있습니다.



- ☞ NAT 모드의 시스템을 투명 모드로 변경 설정하게 되면 <관리 IP/넷마스크>, <기본게이트웨이>를 동시에 입력 할 수 있습니다.



- ☞ 투명 모드의 시스템을 NAT 모드로 변경 설정하게 되면 지정된 <Interface IP/넷마스크>, <디바이스>, <기본 게이트웨이>를 동시에 입력 할 수 있습니다.



## 1-5 관리자

◆ 시스템에 접근 할 수 있는 관리자 계정, 패스워드, 접근허용 IP 및 접속포트의 변경과 시스템의 언어 설정을 제어하는 기능입니다.

### 1-5 #1 : 관리자

☞ 관리자의 계정을 추가하거나 삭제 및 관리자의 패스워드를 변경할 수 있습니다.

적용된 접근프로파일에 따라 보기, 읽기, 쓰기 제한을 적용 할 수 있습니다..

이름	내부(망) 호스트 IP	프로파일	타입
admin	0.0.0.0/0, 0.0.0.0/0, 0.0.0.0/0	super_admin	로컬
kt	168.126.63.0/32, 19.16.1.0/24, 10.10.0.0/16	prof_admin	로컬

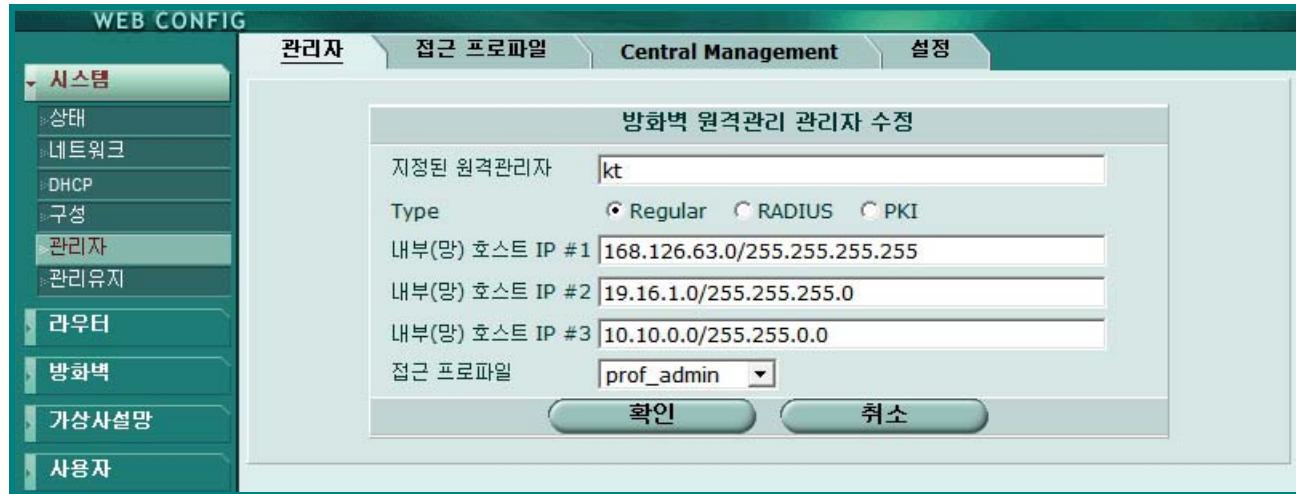
☞ 계정의 인증은 Local 인증 시 Type Regular, 인증서버 연동 시 Radius 혹은 PKI 서버를 설정 하여 연동 할 수 있습니다.

<내부(망) 호스트 IP>는 해당 계정의 접근허용 IP를 3개까지 설정 할 수 있습니다.

0.0.0.0/0.0.0.0으로 설정된 경우 모든 IP에서 접근이 가능합니다.

<내부(망) 호스트 IP #1>에 특정 IP가 설정되어 있다면 2번째와 3번째가 0.0.0.0/0.0.0.0 이라 해도 첫째 IP만 접근이 가능합니다.

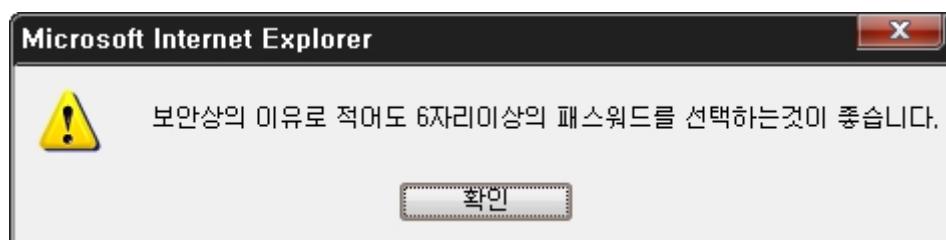
- ☞ 계정에 대한 수정과 암호변경은 따로 분리가 되어 있으며 수정을 누르면 접근프로파일 선택과 접근IP에 대한 설정 변경 및 인증 TYPE 을 설정 할 수 있습니다.



- ☞ 계정에 대한 패스워드 변경은 이전 암호를 모르면 변경이 안됩니다.  
이러한 경우 계정을 삭제하고 새로 만드는 방법을 이용하시기 바랍니다.



- ☞ 패스워드는 6자 이상을 권장하며 이하인 경우 경고 창이 표시지만 확인을 누르면 6자 미만으로 설정해도 정상 적용 됩니다.



## 1-5 #2 : 접근프로파일

☞ 접근 프로파일이란 관리자 계정에 적용될 프로파일을 말하는 것 입니다.

관리자 계정인 ‘admin’은 ‘super\_admin’ 이란 프로파일이 기본적으로 적용되며 추가되는 계정에 적용할 수 있으나 GUI에서 수정 및 변경이 불가능하며 패스워드 분실 시 복구가 어려워 질 수 있으므로 추가된 계정에서는 접근 프로파일을 추가하여 적용하시기 바랍니다.

접근프로파일은 각 기능에 대하여 읽기 및 쓰기를 매우 상세하게 적용할 수 있습니다.

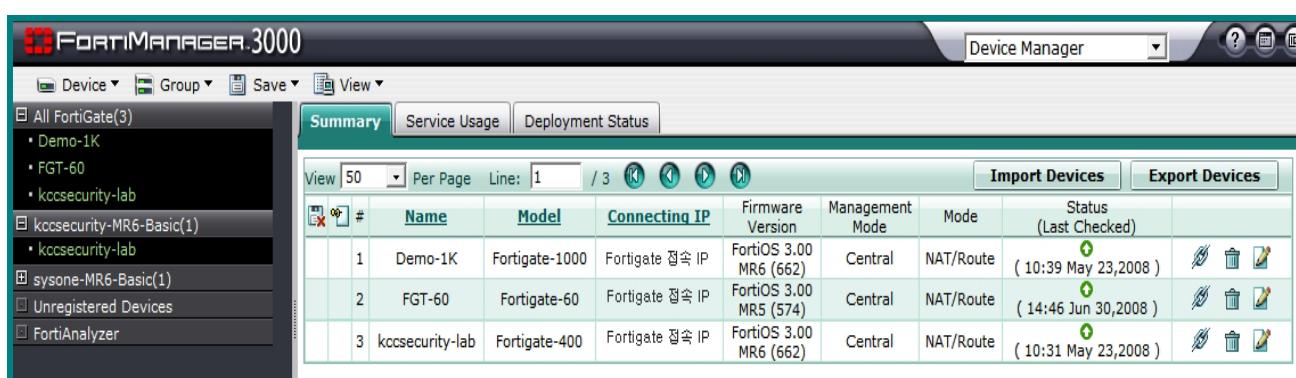
The screenshot shows the Fortinet Web Config interface under the 'Central Management' tab. On the left, a sidebar lists various management categories like System, Network, DHCP, Configuration, and Firewall. The 'Access Profile' section is highlighted. The main content area is titled '새 접근정책 파일' (New Access Policy File) and displays a table for configuring access permissions for different profile entries. The table has columns for '접근제어' (Access Control), 'None' (radio button), '읽기' (Read) (radio button), and '쓰기' (Write) (radio button). The rows list various system components: 유지보수 (Maintenance), admin 사용자 (Admin User), FortiGuard 업데이트 (FortiGuard Update), 인증된 사용자 (Authenticated User), 시스템 설정 (System Settings), 네트워크 설정 (Network Settings), 로그 & 보고서 (Logs & Reports), 웹 필터 설정 (Web Filter Settings), 스팸 필터 설정 (Spam Filter Settings), 암티 바이러스 설정 (Anti-virus Settings), IPS 설정 (IPS Settings), 라우터 설정 (Router Settings), VPN 설정 (VPN Settings), and Firewall Settings (including 정책 설정 (Policy Settings), 주소 설정 (Address Settings), 서비스 설정 (Service Settings), 일정 설정 (Schedule Settings), 프로파일 설정 (Profile Settings), and 기타 설정 (Other Settings)). Most rows have the 'None' radio button selected. The '정책 설정' row is highlighted in yellow. At the bottom are '확인' (Confirm) and '취소' (Cancel) buttons.

## 1-5 #3 : Central Management

☞ Central Management 기능은 중앙관리를 지원하는 FortiManager 시스템을 이용하거나 FortiGuard Management Service를 이용 하는 경우 연동이 가능하며 정기적인 config 백업 및 연동된 Client Fortigate 제품에 동시정책 적용 기능 등이 제공됩니다.



◆ FortiManager는 그림과 같이 Fortigate제품에 대한 중앙관리식 매니지먼트가 가능하며 많은 기능이 제공되지만 한국어는 제공되지 않습니다.  
제품구매 및 FortiGuard Management Service 가입은 판매처에 문의 하시기 바랍니다.



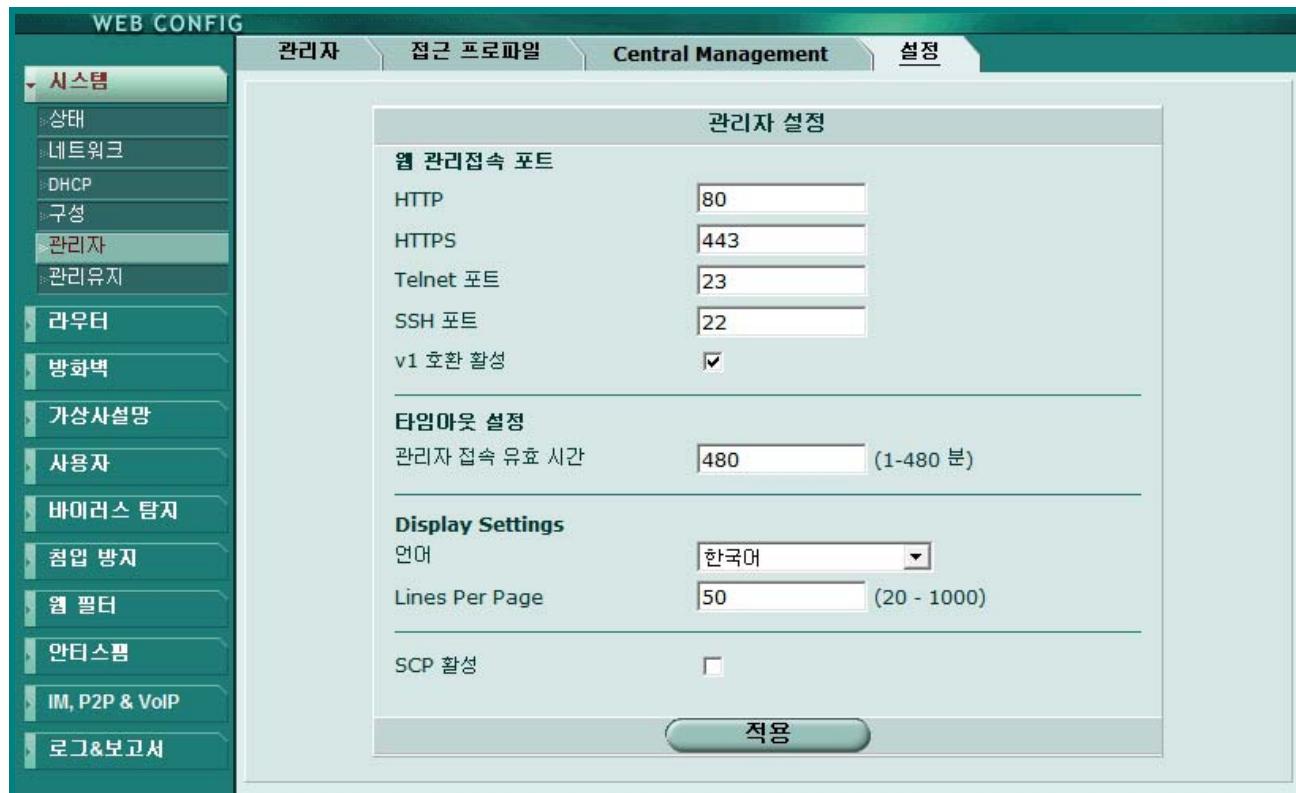
## 1-5 #4 : 설정

☞ 시스템의 관리접속 Port를 변경 할 수 있으며 접속연결 유지시간을 설정할 수 있습니다.

6개국의 시스템의 언어를 설정 및 변경할 수 있으며 적용 시 즉시 시스템의 언어가 변경됩니다.

한 페이지에 표시되는 Line의 수는 기본이 50줄이며 최대 1000줄까지 변경이 가능하며 로그페이지와 세션페이지에 적용됩니다.

SCP를 활성화 해두면 Secure Copy Client를 이용할 수 있습니다..



The screenshot shows the 'Central Management' tab selected in the Fortinet Web Config interface. On the left, a sidebar lists various system management options like Status, Network, DHCP, and Management. The 'Management' option is also listed under the 'Central Management' tab. The main panel displays the 'Manager Settings' section with the following configurations:

- Web Management Port**
  - HTTP: 80
  - HTTPS: 443
  - Telnet Port: 23
  - SSH Port: 22
  - v1 호환 활성:
- Display Settings**
  - 언어: 한국어
  - Lines Per Page: 50 (20 - 1000)
- SCP 활성**:

A large green '적용' (Apply) button is located at the bottom right of the settings panel.

## 1-6 관리유지

- ◆ 시스템 설정의 백업 및 복구와 사용중인 부가기능의 Update 설정을 하는 기능으로 침입탐지 및 안티바이러스 패턴 업데이트 시 수동업데이트의 경우에도 장비의 동작에는 영향을 주지 않습니다.

## 1-6 #1 : 백업과 복구

- ☞ 설정의 백업 및 복구를 하는 기능이 제공되며 설정백업 시 암호화를 선택하면 설정 백업 파일이 암호화가 되어 사용자가 응용프로그램으로 내용을 볼 수 없게 되며 암호화된 설정파일로 복구를 하는 경우엔 설정백업파일의 암호가 다르지 않아야 합니다.
- ☞ Formware는 시스템의 OS를 말하는 것으로 설치를 제공하는 업체에게만 공급되고 Upgrade는 수동으로만 가능하며 Downgrade 하는 경우 시스템은 초기화 됩니다.

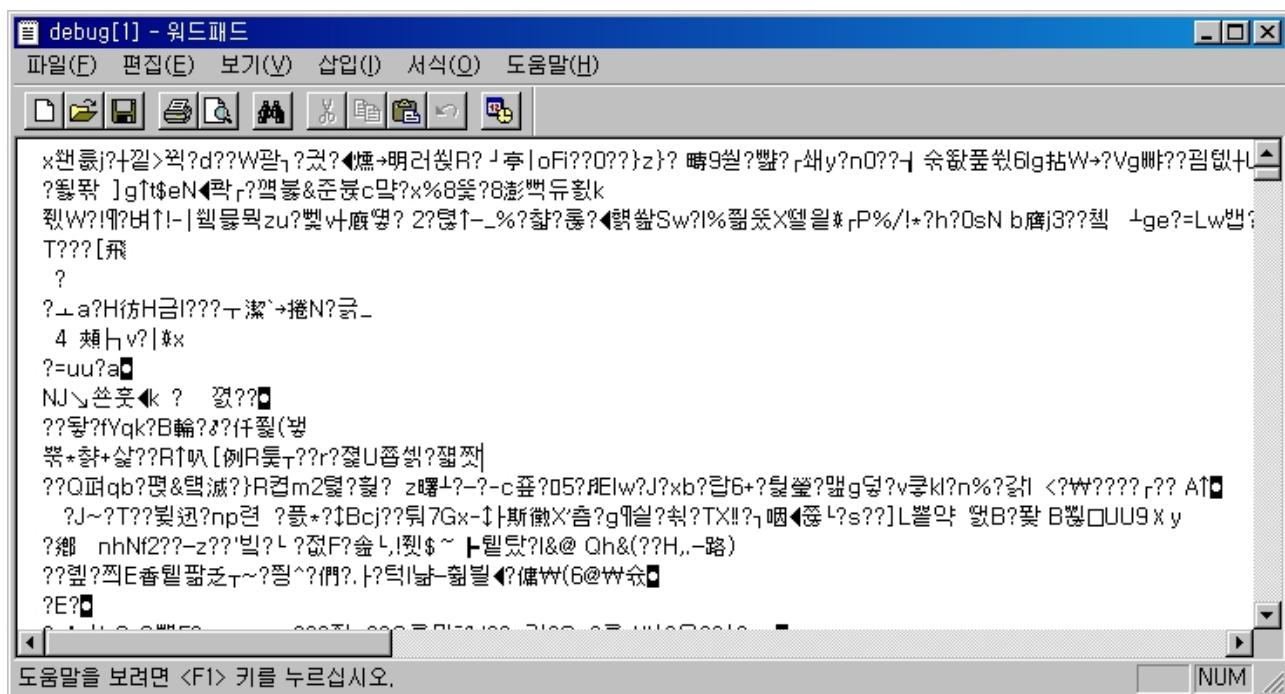


The screenshot shows the 'WEB CONFIG' interface with the 'Backup & Recovery' tab selected. On the left, a sidebar menu includes '시스템' (System) with '관리유지' (Maintenance) highlighted. The main panel displays two sections: 'Backup' and 'Recovery'. The 'Backup' section allows selecting between 'Local PC', 'Management Station', or 'USB Disk' and includes fields for '설정 파일 암호화' (Encrypt Configuration File) and password input. The 'Recovery' section also allows selecting between the same three options and includes a 'File Name' field and password input. Below these sections is a 'Firmware Upgrade' section with a note about upgrades through FortiGuard Management and a file selection field. At the bottom, there is a link for '고급설정(USB 자동-설치, CLI 명령어 가져오기, 디버그 로그 다운로드)' (Advanced Settings).

- ☞ 고급설정 기능 중 USB자동 설치 기능은 USB 메모리에서 설정과 Firmware를 임시로 불러오는 기능으로 FortiUSB 제품만 인식되며 엔지니어의 시스템설치 및 장애처리 시 이용됩니다.



- ☞ 대량의 CLI 명령어 가져오기란 command를 설정파일로 편집하여 한꺼번에 적용 할 수 있으며 txt, conf, cfg, dat 등의 확장명을 가진 파일 등이 포함됩니다.
- ☞ 디버그 로그는 RMA를 위해 제공되며 제조사인 Fortinet 이외에는 내용을 확인 할 수 없습니다.



## 1-6 #2 : Revision Control

☞ Revision Control 은 config 소스가 수정된 경우 이를 추적하는 기능입니다.

실수로 설정을 잘못 했다면 이전 시점으로 복구가 가능 하지만 이 기능은 Central Management 사용하는 경우에만 적용이 가능하며 해당 내용에 대해서 정보 메시지가 표시됩니다.



☞ Central Management 을 설정하면 Revision Control 정보를 보내준다는 메시지가 표시됩니다.



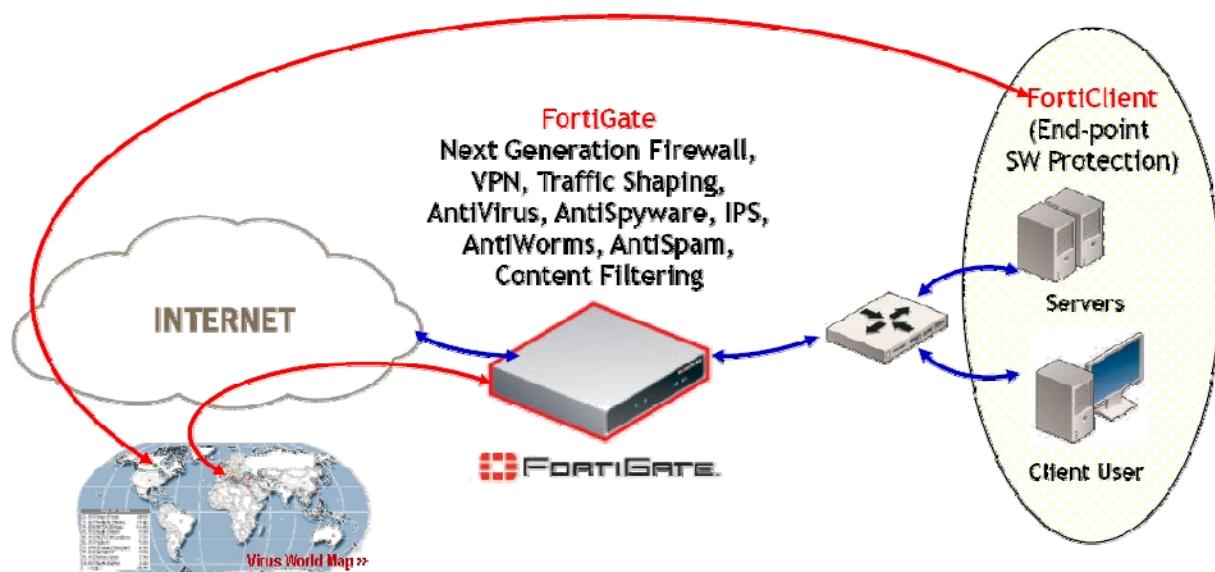
◆ Revision 정보는 Central Management System 에서만 확인이 가능하며 아래 그림과 같이 변경 된 내용을 모두 확인 할 수 있습니다.

Revision: 1		.VS.	Revision: 2	
Total	36382 Line(s)		Total	36409 Line(s)
Deleted	16 Line(s)		Added	43 Line(s)
Modified	20 Line(s)		Modified	20 Line(s)

```
#config-version= FGT-3.00-FW-build574-000000:opmode=0:vdom=0:user=admin
set password ENC AK1peFr/smy3comB9TeaJcJk/CdDhSDsCb160EFyXMxg=
set password ENC d5zDLf9ThdXT2eBAP0k77EyT+0SMoISlnSPxgfhAF10vXoX4c/l6PW8
#config-version=FGT-60-3.00-FW-build574-000000:opmode=0:vdom=0:user=admin
set password ENC JylmBx2CLNjhh+Oy/BYnknYyknu52FhsTULF1KI4Cilulm0oR3YoPOTs
set password ENC JylmBx2CLNjhh+Oy/BYnknYyknu52FhsTULF1KI4Cilulm0oR3YoPOTs
config system snmp sysinfo
set status enable
end
config system snmp community
edit 1
```

## 1-6 #3 : FortiGuard 센터

- ◆ FortiGuard 서비스는 지속적인 업데이트를 통해 최신의 혼합 위협으로부터 보호를 받을 수 있습니다. 글로벌 고속 배포 네트워크를 통해 신속하고 신뢰성 있는 신속하고 신뢰성 있는 업데이트가 제공되며 최신바이러스, 스파이웨어에 대한 휴리스틱 탐지 엔진을 사용함으로써, 모든 와일드 리스트 위협 및 수 천여의 OS, 애플리케이션 취약성으로부터 포괄적으로 보호합니다. 기업 네트워크에 침입하고자 하는 새로운 유형이나 아직 알려지지 않은 위협으로부터 보호해줄 뿐만 아니라 중요한 애플리케이션과 데이터까지도 급속도로 퍼지는 공격으로부터 보호할 수 있습니다.
- ◆ 유해 웹사이트, 안티스팸, 바이러스, 스파이웨어에 대한 방어와 감시 시스템을 지속적으로 업데이트되며 3700가지 이상의 IPS 시그니처와 변종트래픽, 종합 컨텐츠 검사가 제공되며 탄력적인 시스템을 운용하여 보안 애플리케이션을 구현하기 위해 모든 탐지 방식을 통합적으로 제어합니다. 또한 양방향 업데이트 기능은 PUSH & PULL 전송방식으로 가장 빠른 속도의 업데이트를 보장하며 충분 업데이트를 지원하여 엔진 및 패턴 업데이트 시 시스템의 부하를 주지 않습니다.

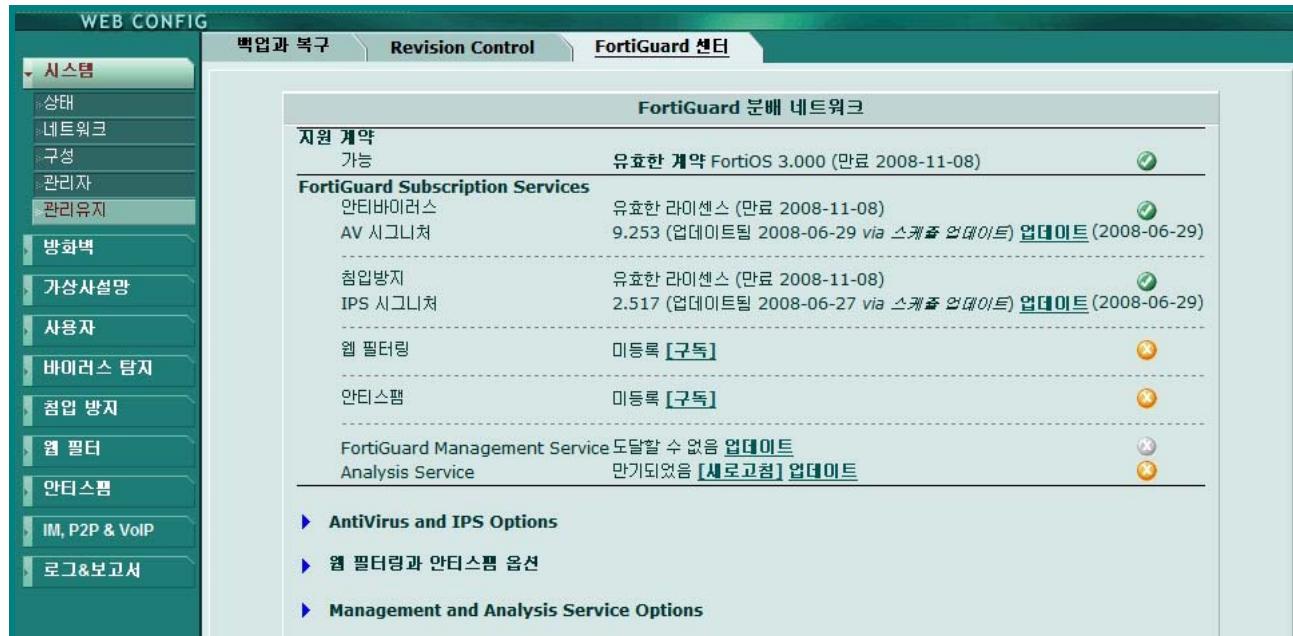


FortiGuard's worldwide teams to provide 24x7 online subscription services to customers

☞ 해당 페이지에는 시스템의 라이센스 정보, 패턴 업데이트 상태가 표시되며 안티바이러스, 침입방지 기능에 대한 업데이트 설정을 할 수 있습니다.

<AntiVirus and IPS Options>의 상세 내용에서 업데이트 설정을 할 수 있습니다.

FortiGuard 웹필터, 안티스팸을 이용하기 위해선 <웹 필터링과 안티 스팸 옵션>에서 기능의 활성화를 하여 라이센스 계약 상태가 체크 되어야 합니다.



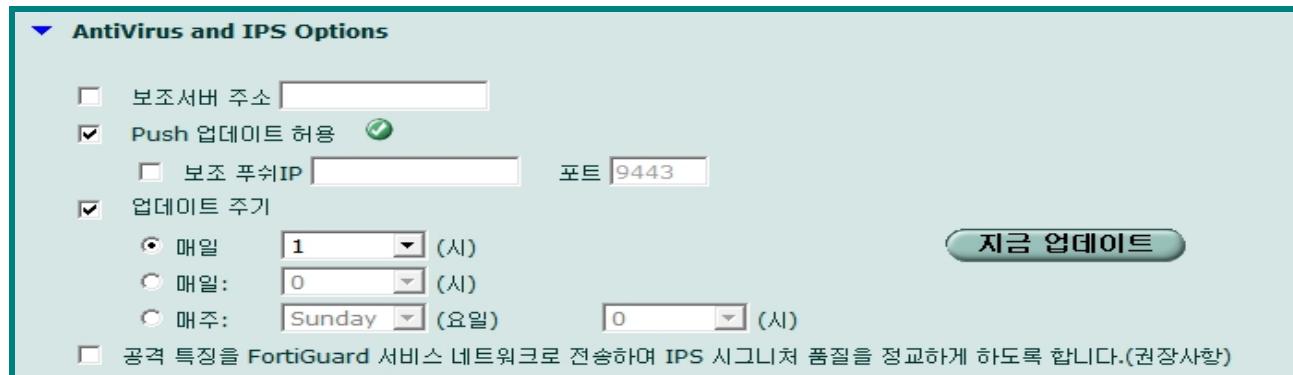
The screenshot shows the FortiGuard Subscription Services page under the FortiGuard Center tab. It displays the following information:

- FortiGuard 분배 네트워크**
- 지원 계약**: 가능, 유효한 계약 FortiOS 3.000 (만료 2008-11-08)
- FortiGuard Subscription Services**:
  - 안티바이러스: 유효한 라이센스 (만료 2008-11-08), 9.253 (업데이트됨 2008-06-29 via 스케줄 업데이트) 업데이트 (2008-06-29)
  - 침입방지: 유효한 라이센스 (만료 2008-11-08), 2.517 (업데이트됨 2008-06-27 via 스케줄 업데이트) 업데이트 (2008-06-29)
  - 웹 필터링: 미등록 [구독]
  - 안티스팸: 미등록 [구독]
- FortiGuard Management Service**: 도달할 수 없음 업데이트, Analysis Service 만기되었음 [새로고침] 업데이트
- ▶ AntiVirus and IPS Options**
- ▶ 웹 필터링과 안티스팸 옵션**
- ▶ Management and Analysis Service Options**

☞ Push업데이트는 FortiGuard 센터에서 Hot Virus가 확인 되었을 때 긴급 패턴을 업데이트 주기까지 기다리지 않고 강제로 시스템에 패턴을 업데이트하는 서비스이며 매우 중요한 기능입니다.

업데이트 주기는 업데이트를 체크하는 기능으로 제일 1번째 줄의 매일은 Every를 말하는 것으로 해당 시간 경과 시마다 체크 한다는 뜻이며 번역 과정에서 오역 된 것입니다.

2번째 줄의 매일은 매일 해당시간에 체크, 매주는 해당주의 해당 시간에 체크한다는 뜻입니다.



The screenshot shows the AntiVirus and IPS Options configuration page. The Push 업데이트 허용 checkbox is checked. Other settings include:

- 보조서버 주소: [empty input field]
- Push 업데이트 허용:
- 보조 푸쉬IP: [empty input field]
- 포트: 9443
- 업데이트 주기:
  - 매일: 1 (시)
  - 매일: 0 (시)
  - 매주: Sunday (요일) 0 (시)
- 지금 업데이트: [button]
- 공격 특징을 FortiGuard 서비스 네트워크로 전송하여 IPS 시그니처 품질을 정교하게 하도록 합니다.(권장사항):

- ☞ FortiGuard 웹필터는 FortiGuard 센터로 유해사이트를 질의하여 체크하는 기능입니다.  
FortiGuard 안티스팸은 FortiGuard 센터로 유해사이트를 질의하여 체크하는 기능입니다.  
SMTP서버(Sender)로부터 메일을 받으면 IP, URI, E-mail 주소 등에 대하여 스팸여부를 체크하고 지정된 설정에 따라 태깅 혹은 차단 처리를 합니다.
  
- ☞ FortiGuard 웹필터, 안티스팸을 이용하기 위해선 기능 사용 설정이 활성화(Enable)되어 있어야 하며 라이센스가 활성화 된 시스템에서만 사용이 가능합니다.  
캐쉬기능은 최근에 탐지된 리스트를 정해진 시간 동안 메모리에 담아두었다가 체크하는 기능으로 동일한 패턴으로 반복되는 리스트는 메모리의 저장 리스트 검색 후 FortiGuard 센터로 질의를 하게 되므로 처리속도를 향상시킬 수 있지만 메모리부터 검색하므로 FortiGuard 센터의 최신 데이터 체크가 되지 못하거나 메모리 사용량에 부하가 발생할 수 있습니다.

**▼ 웹 필터링과 안티스팸 옵션** **Enable 웹 필터** **Enable CacheTTL:** 3600 **Enable 안티 스팸** **Enable CacheTTL:** 1800**Port Selection** **Use Default Port (53)** **Use Alternate Port (8888)****Test Availability**

(FortiGuard 서비스는 포트 53을 사용합니다.)

URL 범주의 재분류를 원하시면, [이곳을 클릭 하시오.](#)

- ☞ FortiGuard 웹필터, 안티스팸 사용시 반드시 **방화벽>보호프로파일**에서 상세분류 Customizing이뤄져야 합니다.  
Customizing 되어 있지 않다면 원하지 않는 탐지가 되어 문제가 발생 할 수 있습니다.
  
- ☞ Management, Analysis 서비스는 해당 서비스 이용자만 사용이 가능하며 서비스 계약자의 경우 계약ID를 입력 후 서비스포탈 시스템(<https://fas.fortinet.com>)으로 이동 할 수 있습니다.

**▼ Management and Analysis Service Options**Account ID: [\*\*To launch the service portal, please click here.\*\*](#)

☞ Management, Analysis 서비스는 네트워크 트래픽 사용에 대한 각종 그래프제공 및 리포트와 실시간 시스템의 상세정보 표시, 로그관리를 해주는 중앙집중 관리형 서비스 입니다.

### FortiGuard Analysis & Management Service

Logout

Settings Device Script Log Log & Report & Archive e-Discovery + Dashboard-Zhen zl\_test1 My New Page Customize This Page Add Page

Demo-100 History External Bandwidth Linda's Console Add Device

**CPU Usage** **Memory Usage**

**Sessions** Session Monitor

**Trap monitor**

Time	Device Name	Trap Name
2008-06-10 10:10:18	My-demo-100	Memory low
2008-06-10 10:10:02	My-demo-100	Memory low
2008-06-10 10:10:00	My-demo-100	CPU usage high
2008-06-10 10:09:47	My-demo-100	Memory low
2008-06-10 10:09:31	My-demo-100	Memory low
2008-06-10 10:09:15	My-demo-100	Memory low
2008-06-10 10:09:09	Jimmy_FGT_846	VPN tunnel down
2008-06-10 10:09:08	My-demo-100	VPN tunnel down
2008-06-10 10:09:08	My-demo-100	VPN tunnel down
2008-06-10 10:08:59	My-demo-100	Memory low

Build Number:V1.1.6\_a84114 08/06/09 22:50 REAL TIME NETWORK PROTECTION

### FortiGuard Analysis & Management Service

Logout

Settings Device Script Log Log & Report & Archive e-Discovery Dashboard-Zhen zl\_test1 My New Page Customize This Page Add Page

Log & Report & Archive

Real-Time View Historical View Log Search Log Files IP Alias Reports Report Config Email Archive

Type: Event Log of FGT1002803026144\_C [change] Matches: 36 of 1073 Formatted | Raw

View 30 per page 1 of 2 [GO](#) [Print](#) [Email](#) Search:  [GO](#)

#	Date	Time	Level	User Interface	Action	Message
1	2008-06-09	16:07:44	alert	http(172.16.95.35)	login	Administrator admin login failed from http(172.16.95.35) because of invalid user name
2	2008-06-04	15:18:20	error	dpd		IPsec DPD detected a failure on the tunnel to 172.16.95.84:500
3	2008-06-03	15:00:51	warning	172.16.95.35	block	SSL Web Application HTTP from 172.16.95.35 to www.google.ca Blocked
4	2008-06-03	14:59:39	warning	172.16.95.35	block	SSL Web Application HTTP from 172.16.95.35 to www.google.ca Blocked
5	2008-06-03	14:58:37	warning	172.16.95.35	block	SSL Web Application HTTP from 172.16.95.35 to www.google.ca Blocked
6	2008-06-03	14:52:08	warning	172.16.95.35	block	SSL Web Application HTTP from 172.16.95.35 to www.google.ca Blocked
7	2008-06-03	14:51:50	warning	172.16.95.35	block	SSL Web Application HTTP from 172.16.95.35 to www.google.ca Blocked
8	2008-06-03	14:49:08	warning	172.16.95.35	block	SSL Web Application HTTP from 172.16.95.35 to www.google.ca Blocked
9	2008-06-03	14:47:07	warning	172.16.95.35	block	SSL Web Application HTTP from 172.16.95.35 to www.google.ca Blocked
10	2008-06-03	14:46:21	warning	172.16.95.35	block	SSL Web Application HTTP from 172.16.95.35 to www.google.ca Blocked
11	2008-06-03	14:43:20	warning	172.16.95.35	block	SSL Web Application HTTP from 172.16.95.35 to www.google.ca Blocked
12	2008-06-03	14:41:19	warning	172.16.95.35	block	SSL Web Application HTTP from 172.16.95.35 to www.google.ca Blocked
13	2008-06-03	14:27:47	alert			Administrator admin\ login failed from http(172.16.95.35) because of invalid user name
14	2008-06-03	14:25:05	warning	172.16.95.35	block	SSL Web Application HTTP from 172.16.95.35 to www.google.ca Blocked
15	2008-06-03	14:22:57	warning	172.16.95.35	block	SSL Web Application HTTP from 172.16.95.35 to 172.16.95.16 Blocked
16	2008-06-03	13:25:48	warning	172.16.95.35	block	SSL Web Application HTTP from 172.16.95.35 to www.google.ca Blocked
17	2008-06-03	13:11:17	warning	172.16.95.35	block	SSL Web Application HTTP from 172.16.95.35 to www.google.ca Blocked
18	2008-06-03	13:08:42	warning	172.16.95.35	block	SSL Web Application HTTP from 172.16.95.35 to www.google.ca Blocked
19	2008-06-03	13:01:11	alert	console	login	Administrator ATZ login failed from console because of invalid user name
20	2008-06-03	12:59:38	alert	console	login	Administrator AO login failed from console because of invalid user name
21	2008-06-03	12:52:05	warning	172.16.95.35	block	SSL Web Application HTTP from 172.16.95.35 to www.google.ca Blocked
22	2008-06-03	12:51:50	warning	172.16.95.35	block	SSL Web Application HTTP from 172.16.95.35 to www.google.com Blocked
23	2008-06-03	12:51:47	warning	172.16.95.35	block	SSL Web Application HTTP from 172.16.95.35 to www.google.com Blocked
24	2008-06-03	12:49:30	warning	172.16.95.35	block	SSL Web Application HTTP from 172.16.95.35 to www.google.ca Blocked
25	2008-06-03	12:32:23	warning	172.16.95.33	block	SSL Web Application HTTP from 172.16.95.33 to www.google.ca Blocked
26	2008-06-03	10:57:11	warning	172.16.95.35	block	SSL Web Application HTTP from 172.16.95.35 to www.google.ca Blocked

Build Number:V1.1.6\_a84114 08/06/09 22:50 REAL TIME NETWORK PROTECTION

## 2

## 라우터

- ◆ 네트워크 통신을 하기위한 라우팅을 설정하는 기능으로 정적(Static), 동적(Dynamic) 라우팅을 지원하며, OSI Layer3 Router에서의 Access control 같은 Policy Routing을 제공합니다.  
해당 메뉴는 NAT/ROUTE 모드에서만 제공되며 TP 모드에서는 제공되지 않습니다.

### 2-1

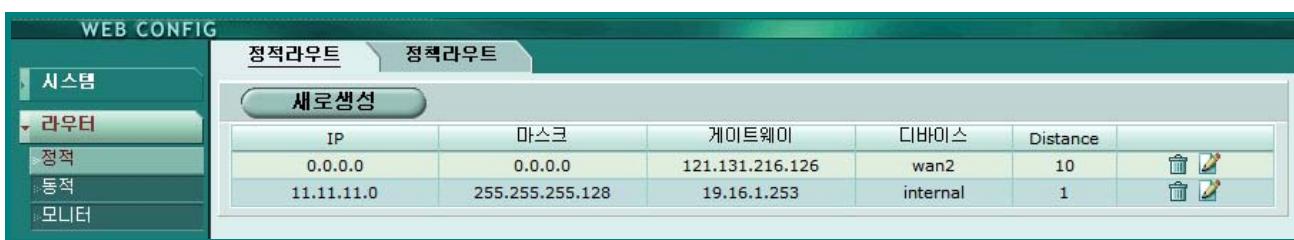
### 정적

- ◆ 목적지IP 혹은 출발지IP+목적지IP를 매칭하여 트래픽을 내보내는 기능으로 Packet을 지정된 곳으로 보내는 라우팅에만 적용되며 Fortigate의 트래픽 연산처리와는 관련이 없습니다.  
라우팅 정보는 외부에서의 관리자 접근, 패턴업데이트, FortiGuard 서비스, DNSBL, NTP 동기화, IPSEC-VPN 등의 동작에 영향을 주며 colsole에서 ping, trace 등을 실행 할 때 필요합니다.

### 2-1

### #1 : 정적라우트

- ☞ 정적 라우트란 Static L3 Routing 을 적용하는 것으로 고정IP 사용자의 경우 기본게이트웨이는 회선 장비의 IP가 될 것이며 다른 네트워크로 통신을 하는 경우 Distance 값은 기본게이트웨이 설정값 보다 낮아야 합니다.  
디바이스 지정을 잘못하는 경우 통신이 되지 않습니다.



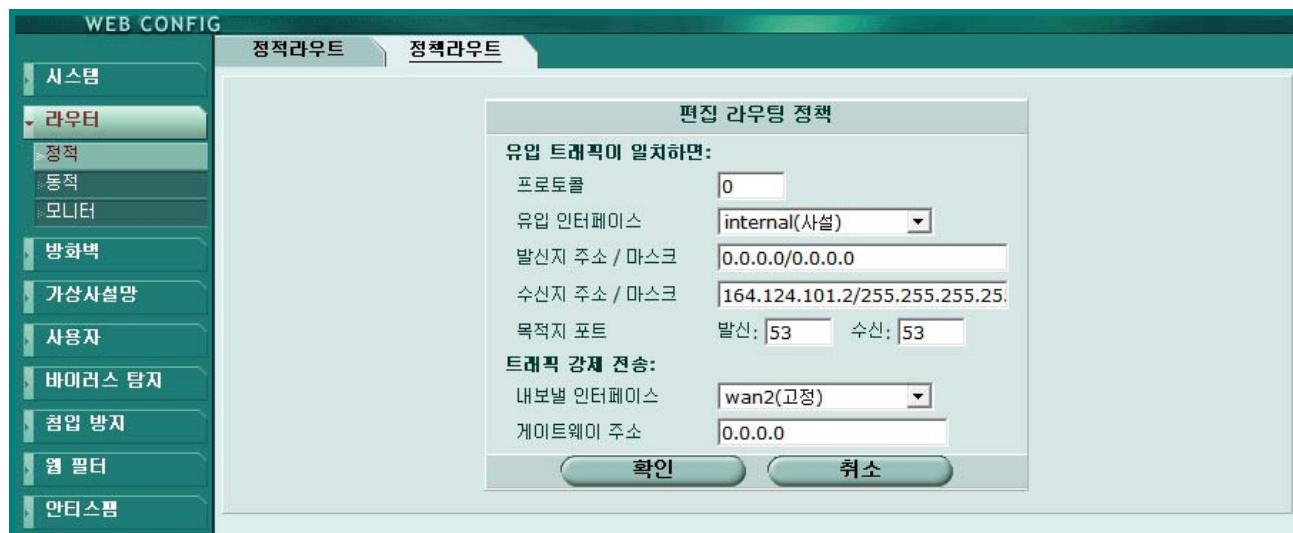
The screenshot shows the 'WEB CONFIG' interface with the 'Static Route' tab selected. On the left, there's a sidebar with '시스템' (System), '라우터' (Router), '정적' (Static), '동적' (Dynamic), and '모니터' (Monitor). The main area displays a table titled '새로생성' (Newly Created) with two static route entries:

IP	마스크	게이트웨이	디바이스	Distance	
0.0.0.0	0.0.0.0	121.131.216.126	wan2	10	
11.11.11.0	255.255.255.128	19.16.1.253	internal	1	

- ☞ 유동회선의 경우 <서버로부터 기본 게이트웨이 검색>기능을 활성화 하여 게이트웨이 정보를 받아올 수 있으며 정적라우트에 기본게이트웨이를 추가 설정하면 통신이 되지 않습니다.  
시스템>네트워크>인터페이스 의 해당 인터페이스에서 설정 할 수 있으며 Distance 값도 설정 할 수 있습니다.

## 2-1 #2 : 정책라우트

- ☞ 정책라우트는 (출발지인터페이스)+(출발지IP)+(목적지IP)+(목적지포트) 4가지가 모두 일치하는 경우 정해진 디바이스의 정해진 게이트웨이로 트래픽을 강제전송 하는 기능입니다.  
주로 회선 이중화 구현 시 사용됩니다.



- ☞ 적용되는 정책라우트(Policy Route)는 정적라우트(Static Route)보다 우선하며 정책라우트의 적용 우선순위는 제일 상위부터 적용되므로 순서에 주의해서 설정 해야 합니다.  
우선순위의 변경은 이동 아이콘을 눌러 우선순위를 변경 할 수 있습니다.  
목적지포트의 적용에 대한 설정상태는 표시되지 않으므로 편집 아이콘을 눌러 확인해야 합니다.

#	들어옴	나감	발신지	수신지	
4	internal	wan2	19.16.1.2 / 255.255.255.255	164.124.101.2 / 255.255.255.255	
3	internal	wan2	0.0.0.0 / 0.0.0.0	222.234.226.0 / 255.255.255.0	
1	internal	wan2	0.0.0.0 / 0.0.0.0	121.131.216.96 / 255.255.255.224	
2	internal	wan1	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	

## 2-2 동적 (RIP, OSPF, BGP, Multicast)

- ◆ 동적라우팅 프로토콜 중 RIP(v1, v2), OSPF, BGP, Multicast (PIM) v2 (RFC2117)을 설정하는 기능입니다.



## 2-3 모니터 (라우팅 모니터)

- ◆ 물리적으로 연결된 Device에 대하여 현재 적용된 Routing Info를 표시해 주는 기능입니다.

- ☞ 정적타입과 연결타입의 라우팅 Metric 값은 0으로 수정할 수 없으며 동적라우팅을 이용하는 경우가 아니라면 적용 받지 않습니다.
- 라우팅의 우선순위는 Distance 값에 따라 결정되며 낮을수록 우선합니다.

라우팅 모니터							
타입:		네트워크:	게이트웨이:			필터 적용	
타입	서브타입	네트워크	디스턴스	메트릭	게이트웨이	인터페이스	업 타임
정적		0.0.0.0/0	1	0	218.144.180.190	wan1	
정적		11.11.11.0/25	1	0	19.16.1.253	internal	
연결		19.16.1.0/24	0	0	0.0.0.0	internal	
연결		121.131.216.96/27	0	0	0.0.0.0	wan2	
연결		218.144.180.128/26	0	0	0.0.0.0	wan1	

- ☞ 정적라우팅이 설정된 정보는 정적 타입으로 표시되며 동적라우팅은 동적 타입으로 표시됩니다.
- 연결 타입의 라우팅은 인터페이스에 설정된 네트워크 정보이며 물리적 링크가 연결되어있어야 표시됩니다.

### 3

## 방화벽

◆ Fortigate는 기본적으로 방화벽 기능을 수행하며 Stateful Packet Inspection 방식을 이용합니다.

Session을 생성하기 위한 첫번째 조건인 3way handshake가 진행될 때 Syn Packet 만 방화벽 정책에서 체크하고 그 나머지 Packet은 Stateful Inspection 엔진에서 체크함으로 처리속도가 이상적으로 향상됩니다.

Stateful Inspection 엔진이 Packet을 가로채어서 그것이 Syn인지, Syn-Ack인지, Ack인지를 판단하여 Syn Packet (Session 성립을 위한 첫 번째 Packet) 이라면 Stateful Inspection Table에 해당 Packet의 Session이 기록된 후에 방화벽 정책을 체크하고 Syn 패킷이 아닐 경우, Stateful Inspection Table에 이전 Syn Packet의 Session이 기록되어 있으면 방화벽 정책을 체크하지 않고 바로 통과, 기록되어 있지 않다면 DROP시킵니다.

### 3-1 정책

◆ 정책은 보안정책과 더불어 AV, IPS, 가상사설망, 인증 등 모든 정책을 적용하는 기능입니다.

시스템을 기준으로 Internal 구간의 내부사용자를 Local, Wan 혹은 External 의 사용자를 Remote 라 칭하며 정책은 다음과 같은 방향성으로 불려집니다.

1. Outbound 정책 : Local (Internal) → Remote(Wan) 의 정책
2. Inbound 정책 : Remote(Wan) → Local (Internal) 의 정책

☞ 보안정책은 우선순위는 각 방향 그룹별 제일 상위의 정책부터 순서대로 적용됩니다.

즉, 범위가 작은 것을 범위가 큰 것보다 위에 만들어야 합니다.

그림과 같이 ID 2번 정책이 모든 사용자가 인터넷을 하도록 하는 정책이며 ID 5번 정책은 웹사이트의 차단 정책이므로 반드시 ID 2번 정책보다 이전에 위치해야 합니다.

정책 ID 번호는 식별자 ID로 정책의 우선순위와는 전혀 상관 없이 없습니다.



The screenshot shows the Fortinet Web Config interface under the 'WEB CONFIG' tab. On the left sidebar, '방화벽' (Firewall) is selected. The main area displays the '정책' (Policy) configuration screen. It lists several policy entries:

- internal -> wan1 (2)**
  - ID 5: all to www.naver.com, always, ANY, DENY
  - ID 2: all, always, ANY, Outbound, ACCEPT
- internal -> wan2 (1)**
  - ID 4: 19.16.1.[2-25] to all, always, ANY, Outbound, ACCEPT
- wan2 -> internal (1)**
  - ID 3: all to FTP 3389, always, ANY, ACCEPT

## 3-1 #1 : 정책 추가 및 편집

☞ 보안 정책을 추가하는 방법은 2가지 방법이 있습니다.

1번째 **Create New** 버튼을 눌러 추가하는 방법이 있으며 이렇게 추가된 정책은 그림의 ID 6번처럼 기존의 생성되어 있는 정책의 제일 하위에 만들어 지게 됩니다.

2번째 정책추가 방법은 원하는 위치의 하위에 오게 될 정책에서 보안정책 먼저설정 아이콘을 눌러 바로 추가하는 방법이 있습니다.

정책의 수정은 편집 아이콘을 눌러 편집하거나 삭제 아이콘을 눌러 삭제 할 수 있습니다.

ID	발신자	목적지	스케줄	서비스	프로파일	동작
5	all	www.naver.com	always	ANY		DENY
2	all	all	always	ANY	Outbound	ACCEPT
6	19.16.1.[2-25]	all	always	ANY		DENY
4	19.16.1.[2-25]	all	always	ANY	Outbound	ACCEPT
3	all	FTP 3389	always	ANY		ACCEPT

☞ 정책의 우선순위를 이동하기 위해선 이동 아이콘을 눌러 팝업 된 창에서 이동할 정책 ID 보다 이전인지 이후인지를 선택하면 해당 위치로 이동하게 됩니다.

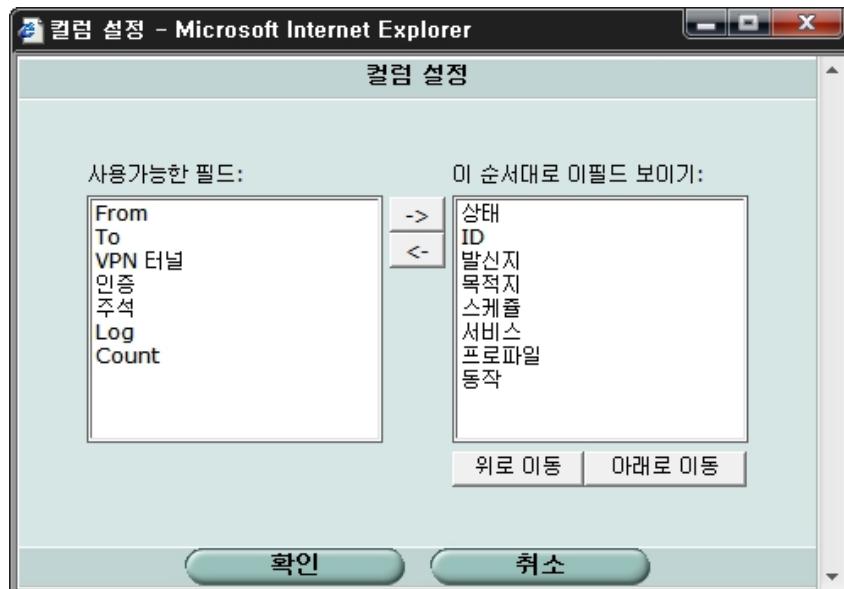


## 3-1 #2 : 컬럼 설정

☞ 방화벽>정책에서 보여지는 컬럼을 설정 할 수 있습니다.

정책페이지에서 오른쪽 상단에 위치한 [컬럼 설정]을 누르면 팝업이 표시되어 원하는 필드를 추가, 제외 할 수 있으며 보이는 필드의 순서를 변경 할 수 있습니다.

사용 가능한 필드 항목은 OS 의 Build 버전 별 차이가 있습니다



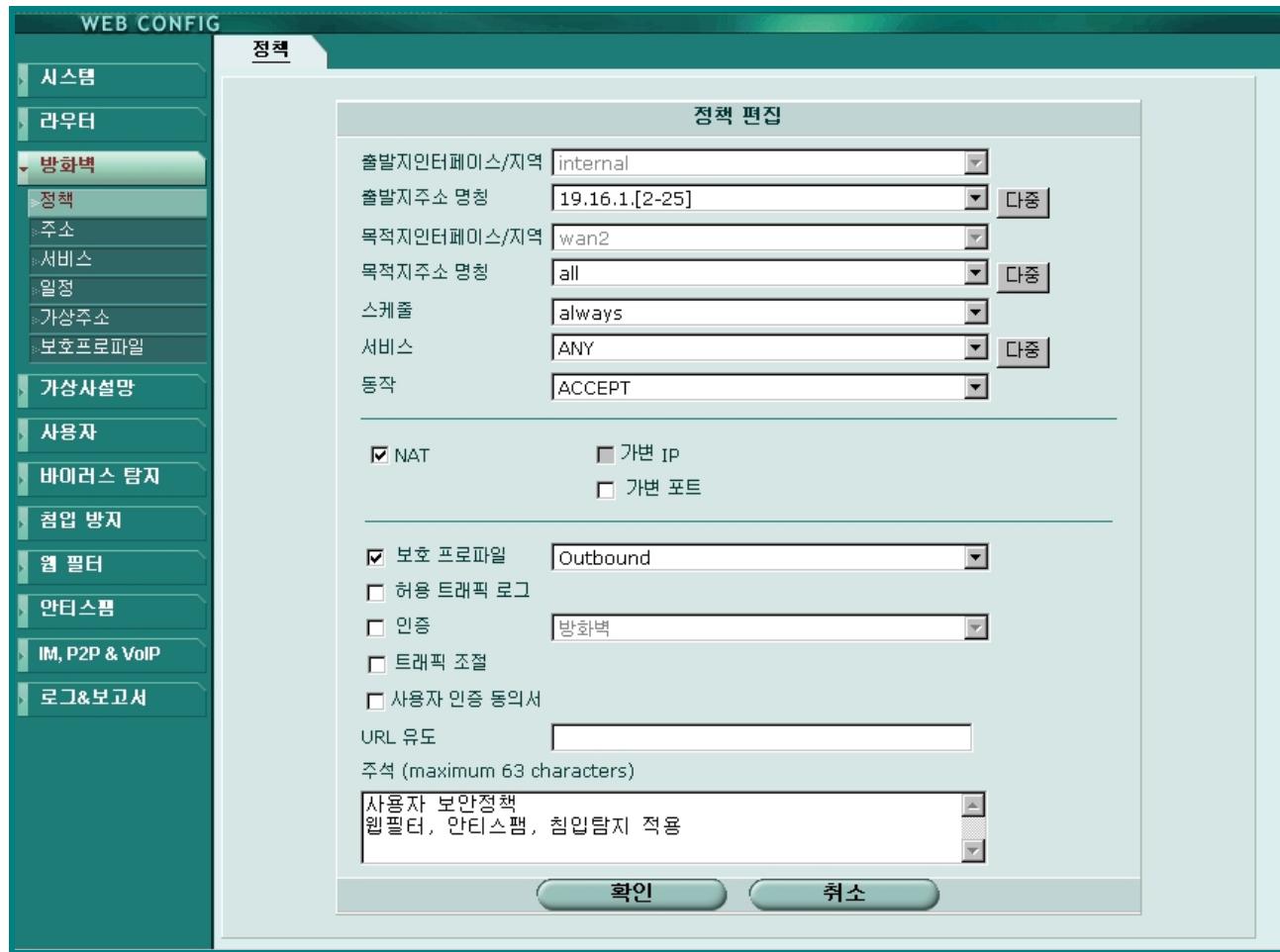
☞ 필드 항목 중 Count 항목은 해당 정책에서 사용된 트래픽을 Count 합니다.

해당 정책의 비활성화 시 Count 는 초기화 되며 활성화 시점부터 다시 Count 됩니다.

Count	상태	ID	발신지	목적지	스케줄	서비스	프로파일	동작	Action
90306 / 8 MB	✓	7	● 19.16.1.0/24	● 1.1.1.0/24	always	● ANY		ENCRYPT	
0 / 0 B	✓	5	● all	● www.naver.com	always	● ANY		DENY	
19620457 / 1 GB	✓	2	● all	● all	always	● ANY	Outbound	ACCEPT	
0 / 0 B	✓	6	● 19.16.1.[2-25]	● all	always	● ANY		DENY	
3857717 / 4 GB	✓	4	● 19.16.1.[2-25]	● all	always	● ANY	Outbound	ACCEPT	
▼ wan2 -> internal (1)									
16895 / 7 MB	✓	3	● all	● FTP ● 3389	always	● ANY		ACCEPT	

## 3-1 #3 : 정책 설정

- ☞ 정책을 추가하는 경우 NAT 모드의 사용자는 반드시 정책에서 NAT 기능을 활성화 해야 합니다. ROUTE 모드의 사용자는 NAT 기능을 비활성화 해야 하며 TP 모드의 사용자는 NAT 기능이 자체가 없으므로 정책설정 화면에 표시되지 않습니다.



- ☞ AntiVirus, IPS, 웹필터, 스팸필터, P2P/IM 제어 등의 기능을 사용하기 위해선 보호프로파일이 반드시 적용되어야 합니다.
- ☞ 트래픽 로그를 활성화 하면 해당정책에 적용되는 트래픽 로그가 저장되지만 메모리로그에는 저장 할 수 없으며 FortiAnalyzer, Syslog, HDD가 설치된 제품만 저장 할 수 있습니다.
- ☞ 사용자 인증을 적용하는 경우 URL유도 기능을 사용 할 수 있으며 보안정책에 주석정보를 입력하면 어떠한 보안 정책인지 쉽게 확인 할 수 있습니다.

## 3-1 #4 : 트래픽 조절

☞ 트래픽 조절 기능은 일정 사용량 이상 사용하지 못하도록 제한하는 기능입니다.

QoS 기술 중 Traffic Shaping 기술을 말하는 것으로 사용자단위의 1MB 는 128(Kbytes/s) 입니다.

트래픽 조절 기능을 활성화 해야 제한 값을 설정 할 수 있습니다.



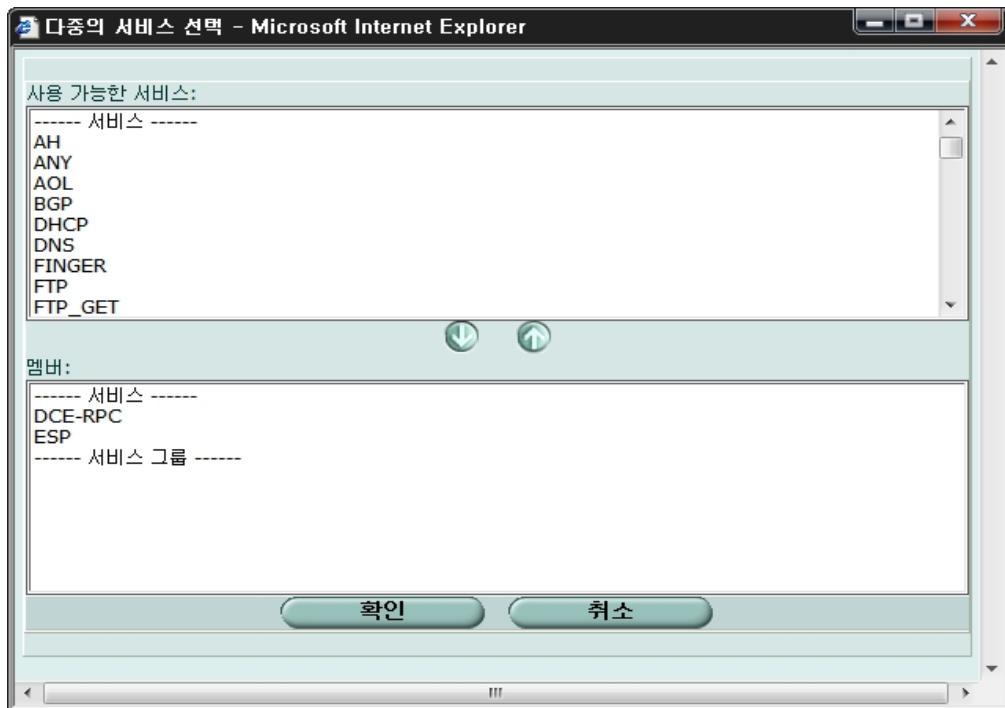
☞ 트래픽 조절이 적용된 정책 중 트래픽 우선순위는 내부적으로 동시에 처리되는 상황에서 적용됩니다.

보장된 대역폭의 지원은 전체 대역폭에서 가용여유 대역폭이 존재해야 보장이 되므로 설정 시 최대 대역폭만 제한 설정을 하는 것을 권장합니다.

## 3-1 #5 : 다중 객체 (Multiple Object)

☞ 정책을 추가하거나 편집하는 경우 Multiple 기능에 지원되며 <다중> 버튼을 눌러 다중의 서비스를 선택 할 수 있습니다.

출발지주소명칭(주소), 목적지주소명칭(주소), 서비스(서비스)를 그룹화 하지 않고 여러 항목을 동시에 선택하여 적용하는 기능입니다.



☞ 다중 서비스를 선택한 경우 아래 그림의 정책 6번처럼 최소 두줄 이상의 Object 가 표시되어 바로 적용됩니다.

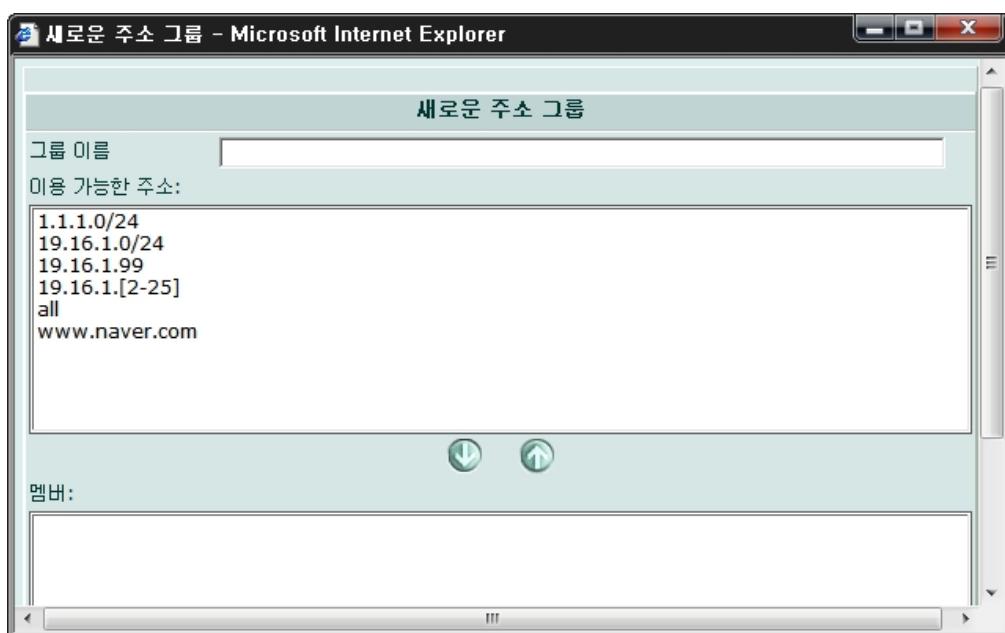
정책										[ 설정 설정 ]	
Create New											
		Count	상태	ID	발신자	목적지	스케줄	서비스	프로파일	동작	
<b>internal -&gt; wan1 (4)</b>											
90306 / 8 MB	<input checked="" type="checkbox"/>	7	<input checked="" type="radio"/> 19.16.1.0/24	<input checked="" type="radio"/> 1.1.1.0/24	always	<input checked="" type="radio"/> ANY		ENCRYPT			
5 / 224 B	<input checked="" type="checkbox"/>	6	<input checked="" type="radio"/> 19.16.1.99	<input checked="" type="radio"/> all	always	<input checked="" type="radio"/> DNS	<input checked="" type="radio"/> HTTP	ACCEPT			
0 / 0 B	<input checked="" type="checkbox"/>	5	<input checked="" type="radio"/> all	<input checked="" type="radio"/> www.naver.com	always	<input checked="" type="radio"/> ANY		DENY			
19806421 / 1 GB	<input checked="" type="checkbox"/>	2	<input checked="" type="radio"/> all	<input checked="" type="radio"/> all	always	<input checked="" type="radio"/> ANY	Outbound	ACCEPT			
<b>wan2 -&gt; internal (1)</b>											
3858049 / 4 GB	<input checked="" type="checkbox"/>	4	<input checked="" type="radio"/> 19.16.1.[2-25]	<input checked="" type="radio"/> all	always	<input checked="" type="radio"/> ANY	Outbound	ACCEPT			
<b>wan2 -&gt; internal (1)</b>											
16895 / 7 MB	<input checked="" type="checkbox"/>	3	<input checked="" type="radio"/> all	<input checked="" type="radio"/> FTP 3389	always	<input checked="" type="radio"/> ANY		ACCEPT			

## 3-1 #6 : 정책에서의 객체생성

☞ 정책을 추가하거나 편집할 때 원하는 객체의 <새로 만들기>를 이용하면 주소, 서비스, 가상IP, 그룹 등을 바로 생성 할 수 있습니다.



☞ <새로 만들기>를 선택하면 새로운 객체생성을 만드는 화면이 표시되어 바로 생성이 가능합니다.



## 3-1 #7 : 정책에서의 객체편집

☞ OS 3.0 은 정책 내에서의 Object 새로 생성/편집 이 지원되는 것 입니다.

편집을 원하는 Object에 마우스를 이동하면  손가락 모양으로 변하게 되며 선택한 Object를 편집 할 수 있습니다.



The screenshot shows the Fortinet Web Config interface under the 'Policy' tab. On the left, there's a navigation menu with '정책' (Policy) selected. The main area displays a table of policy objects. One object is highlighted with a yellow background: '19.16.1.0/24' (Source IP Range) and '1.1.1.0/24' (Destination IP Range). The table includes columns for Count, Status, ID, Sender, Destination, Scope, Services, Protocols, and Actions (Encrypt, Accept, Deny). There are also sections for 'internal -> wan1 (4)', 'internal -> wan2 (1)', and 'wan2 -> internal (1)'.

☞ 선택한 Object를 클릭하면 그림과 같이 편집 팝업 창이 나타나며 이름, 내용을 수정 할 수 있습니다.



## 3-1 #8 : 정책 활성화 & 비활성화

☞ 보안정책은 비활성화되면 적용되지 않으며 적용되지 않은 정책은 회색으로 표시 됩니다.



The screenshot shows the Fortinet Web Config interface under the '정책' (Policy) tab. The left sidebar includes options like 시스템, 라우터, 방화벽 (selected), 정책, 주소, 서비스, 일정, 가상주소, 보호프로파일, 가상사설망, 사용자, 바이러스 탐지, 첨입 방지, 웹 필터, 암티스팸, IM, P2P & VoIP, and 로그&보고서.

The main table displays security policies:

Category	ID	Source	Destination	Action	Profile	Behavior	Encryption	
internal -> wan1 (4)	90306 / 8 MB	<input checked="" type="checkbox"/>	7	19.16.1.0/24	1.1.1.0/24	always	ANY	ENCRYPT
	0 / 0 B	<input checked="" type="checkbox"/>	6	19.16.1.99	all	always	ANY	ACCEPT
	N/A	<input type="checkbox"/>	5	all	www.naver.com	always	ANY	DENY
internal -> wan2 (1)	19764365 / 1 GB	<input checked="" type="checkbox"/>	2	all	all	always	ANY	Outbound ACCEPT
	3858037 / 4 GB	<input checked="" type="checkbox"/>	4	19.16.1.[2-25]	all	always	ANY	Outbound ACCEPT
wan2 -> internal (1)	16895 / 7 MB	<input checked="" type="checkbox"/>	3	all	FTP 3389	always	ANY	ACCEPT

## 3-1 #9 : VPN 정책

☞ IPSEC VPN 사용을 위해선 ‘동작’에서 IPSEC을 선택 후 원하는 터널을 적용할 수 있습니다.

IPSEC VPN 터널 정책은 Outbound로 설정해야 합니다.

VPN 터널 적용 시 Inbound 와 Outbound 트래픽에 대해 허용설정을 적용할 수 있으며 VPN 내에서 NAT 가 되도록 설정 할 수도 있습니다.



☞ SSL VPN 설정과 PPTP VPN 의 정책설정은 Inbound로 설정 해야 합니다.

또한 반드시 사용자인증 설정과 연동이 되야 하므로 해당 매뉴얼을 참고하거나 영문 매뉴얼, 온라인 헬프 및 설치엔지니어 혹은 기술지원센터에 문의하시기 바랍니다.

## 3-1 #10 : IP POOL 정책

- ☞ NAT 모드에서는 Internal 구간의 사설 IP 사용자들의 IP는 시스템의 WAN 인터페이스 IP로 변환되어 외부와 통신하게 되며 IP-POOL 의 미 사용시 PAT (Port Address Translation)로 동작합니다. 이때 내부 IP를 WAN 인터페이스가 아닌 다른 IP로 변환되어 통신하기 위한 기능입니다. WAN 구간에서 사용할 수 있도록 ISP 전송사업자로부터 부여 받은 WAN 인터페이스에 적용된 IP에 한해서만 적용이 가능하며 유동회선 사용자 및 단일IP 사용자는 해당기능을 적용할 수 없습니다.
- ☞ 가변포트란 NAT 사용시 IP-POOL 을 사용하지 않으면 PAT로 동작 하기 때문에 원본 소스 Port가 변환되는 것을 막는 기능이며 Fixed Port가 오역된 것으로 포트를 고정하는 기능입니다. 간혹 특정 응용프로그램에서는 원본포트가 NAT 되어 변경되면 통신장애가 발생되는 경우 사용합니다. 이 기능은 IP-POOL 을 선택하지 않으면 한번에 하나의 연결에만 적용 됩니다.



## 3-2 주소

- ◆ 단일 IP, 범위 IP, 네트워크 IP, FQDN (정규화된 도메인 이름)을 설정하는 기능입니다.  
사용자가 생성하여 사용 할 수 있으며 정책 적용 시 반드시 필요합니다.

## 3-2 #1 : 주소

- ☞ 장비 최초동작 시 기본적으로 모든 IP를 뜻하는 ‘0.0.0.0/0.0.0.0’의 주소가 ‘all’ 이란 명칭으로 등록 되어 있으며 Any 인터페이스가 선택되어 기본 정책에 사용됩니다.
- ☞ 주소는 정책을 적용할 때 반드시 필요한 객체로 생성된 주소객체 리스트 중 정책에 사용 중 이거나 그룹으로 적용된 주소 객체는 편집 아이콘만 표시되며 편집만 가능합니다.  
어떤 곳에도 적용되지 않은 주소 객체는 삭제 아이콘이 표시되며 삭제가 가능합니다.  
생성된 IP는 타입 별 그룹화 되어 표시 되며 이름을 기준으로 자동 정렬 됩니다.

이름	주소 / FQDN	인터페이스	
1.1.1.0/24	1.1.1.0/255.255.255.0	Any	
19.16.1.0/24	19.16.1.0/255.255.255.0	Any	
19.16.1.99	19.16.1.99	internal	
all	0.0.0.0/0.0.0.0	Any	
19.16.1.[2-25]	19.16.1.[2-25]	Any	
daum.net	daum.net	Any	
news.naver.com	news.naver.com	wan1	

☞ 주소의 추가는 **새로생성** 버튼을 눌러 추가 할 수 있으며 편집의 경우도 유사합니다.

주소이름은 사용자편의대로 입력이 가능하며 한글로 입력한 경우 시스템언어가 영어라면 ANSI 코드로 표시되므로 주의가 필요합니다.

타입에서 IP, FADN 을 선택하거나 인터페이스를 지정하여 정책 설정 시 해당 인터페이스 항목에만 나타나게 할 수 있으나 주소그룹에도 적용을 받으므로 인터페이스는 Any 선택을 권장합니다.



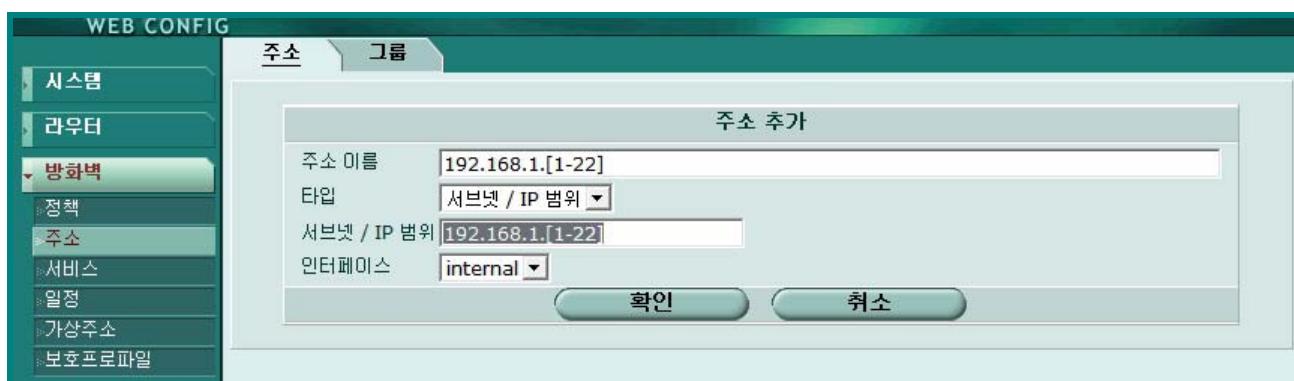
☞ 단일 IP를 추가하는 경우 그림과 같이 <서브넷 / IP범위> 에 단일 IP만 입력합니다.

편집을 하는 경우 생성과 동일하며 주소 이름도 변경이 가능합니다.



☞ 범위 IP는 순차적으로만 생성이 가능하며 C클래스인 IP의 제일 마지막 자릿수만 적용이 가능합니다.

그림과 같이 <서브넷 / IP범위> 에 192.168.1.[1-22] 같이 대괄호 [ ]로 적용합니다.



☞ 네트워크로 생성하는 경우 IP/Subnet 을 그림과 같이 순차적으로 입력할 수 있습니다.

192.168.1.0/255.255.255.0 의 경우 192.168.1.0/24 로 입력하거나 192.168.1.254/24 로 입력 하더라도 192.168.1.0/255.255.255.0 으로 자동 변경 됩니다.



☞ FQDN (Fully Qualified Domain Name) 의 약자로 정규화된 도메인 주소를 주소목록으로 사용할 수 있습니다.

단, 상위도메인과 하위도메인은 별도의 도메인 이므로 절대로 혼동 되어선 안될 것 입니다.

예를 들어 <[naver.com](http://naver.com)>을 등록하면 <[naver.com/r/d?kref](http://naver.com/r/d?kref)>의 경우 동일한 도메인의 서브쿼리가 URL에 연결되므로 동일한 도메인 적용됩니다.

<[news.naver.com](http://news.naver.com)> 의 경우 서브도메인은 동일한 도메인이 아닌 별도의 도메인 입니다.

즉, 정규표현은 적용되지 않습니다.



## 3-2 #2 : 주소그룹

☞ 그룹멤버는 정책에 적용 시 단일 객체를 포함하여 정책에서 사용 중이거나 다른 그룹에 포함된 객체는 편집 아이콘만 표시되어 편집이 가능하고 아무 곳에도 적용되지 않는 객체는 삭제 아이콘이 표시되며 삭제가 가능합니다.

생성된 그룹은 이름을 기준으로 자동 정렬 되며 그룹에 포함된 주소객체 목록이 표시됩니다.

주의할 점은 그룹에 해당된 주소목록 중 인터페이스가 정의된 객체가 있다면 정책적용 시 그룹객체도 해당인터페이스에만 표시되므로 정책 적용이전에 반드시 확인하시기 바랍니다.

그룹 이름	멤버
Local	19.16.1.99, 19.16.1.[2-25]
포털사이트	daum.net, naver.com

☞ 그룹의 **새로생성** 버튼을 눌러 그룹을 만들고 이용 가능한 주소 리스트 중 멤버로 이동 하면 선택 된 주소는 해당그룹으로 포함되며 정책 적용 시 그룹리스트에서 선택 할 수 있습니다.  
그룹생성시 그룹객체도 그룹에 추가포함 할 수 있습니다.

## 3-3 서비스

- ◆ 서비스란 TPC / UDP 프로토콜 별 각 통신규약 명칭과 사용하는 Port 번호를 Keyword로 매칭시킨 것으로 정책 적용 시 반드시 필요한 사용프로토콜을 정의하는 기능입니다.

## 3-3 #1 : 기본정의

- ☞ 서비스 중 기본정의는 Well Known Port 중 많이 사용하는 약 60 여 개의 리스트를 정의 한 것으로 수정은 할 수 없으며 OS 버전에 따라 항목은 차이가 발생 할 수 있습니다.

WEB CONFIG		기본정의	사용자정의	그룹
시스템		이름	내용	
라우터		AH	IP/51	
방화벽		ANY	ALL	
정책		AOL	TCP/5190-5194	
주소		BGP	TCP/179	
서비스		DCE-RPC	TCP/135 UDP/135	
일정		DHCP	UDP/67-68	
가상주소		DNS	TCP/53 UDP/53	
보호프로그램		ESP	IP/50	
가상설치망		FINGER	TCP/79	
사용자		FTP	TCP/21	
바이러스 탐지		FTP_GET	TCP/21	
첨입 방지		FTP_PUT	TCP/21	
웹 필터		GOPHER	TCP/70	
안티스팸		GRE	IP/47	
IM, P2P & VoIP		H323	TCP/1720,1503 UDP/1719	
로그&보고서		HTTP	TCP/80	
		HTTPS	TCP/443	
		ICMP_ANY	ICMP/ANY	
		IKE	UDP/500,4500	
		IMAP	TCP/143	
		INFO_ADDRESS	ICMP/17	
		INFO_REQUEST	ICMP/15	
		IRC	TCP/6660-6669	
		Internet-Locator-Service	TCP/389	
		L2TP	TCP/1701 UDP/1701	

## 3-3 #2 : 사용자정의

☞ 사용자 정의 서비스는 TCP/UDP, ICMP, ICMP, IP 타입이 지원되며 포트를 지정합니다.

타입 중 IP는 IANA에서 지정한 Protocol Number으로 IETF RFC 791인 IP와 혼동하면 안됩니다.  
정책에 적용되거나 그룹으로 적용된 객체는 편집 아이콘만 표시되며 어떤 곳에도 적용되지 않은 주소 객체는 삭제 아이콘이 같이 표시됩니다.

생성된 항목은 이름을 기준으로 자동 정렬되며 상세 내용이 표시됩니다.

서비스 이름	내용	
PC보안	TCP/1-65535:8888,1-65535:8900	
SMS	TCP/1-65535:2000-3000	
원도우터미널	TCP/1-65535:3389	

☞ **새로생성** 버튼을 눌러 새로운 서비스를 추가 할 수 있으며 하나의 객체에 여러 개의 서비스 포트를 부여 할 수 있습니다.

**추가** 버튼을 누르면 서비스항목이 추가됩니다.

대부분의 통신은 원본포트가 랜덤으로 발생되기 때문에 원본포트는 수정하지 않습니다.

세션의 상세 내용을 본 사용자라면 일반적인 통신의 경우 목적지 포트가 단일포트란 것을 확인 할 수 있었을 것 입니다.

하지만 예외적으로 대부분의 바이러스 및 P2P 트래픽의 경우 원본포트가 단일포트이며 목적지 포트가 랜덤하게 변경되며 통신하는 경우도 있습니다.

프로토콜	원본 포트	목적지 포트	
낮음	높음	낮음	높음
TCP	1	65535	0

- ☞ 하나의 포트를 생성할 때는 이름생성 후 프로토콜에서 TCP/UDP 선택 이후 목적지 포트의 낮음과 높음에 동일한 포트번호를 지정하고 해당 포트가 TCP 인지 UDP 인지 선택해주어야 합니다.



- ☞ 2개 이상의 포트를 정의는 **추가** 버튼을 눌러 포트번호 필드를 추가 하여 생성하면 됩니다. 그림과 같이 TCP 와 UDP 동시에 필드추가도 가능하며 삭제 아이콘을 눌러 삭제가 가능합니다.



- ☞ 포트범위가 순차적인 경우 낮음에 낮은수 높음에 높은수를 입력하면 해당 범위로 지정이 됩니다. 그림과 같이 TCP/8000~9000 인 경우 낮음에 8000, 높음에 9000을 입력하면 적용됩니다.



## 3-3 #3 : 서비스그룹

☞ 그룹멤버는 정책에 적용 시 단일 객체를 포함하여 정책에서 사용 중이거나 다른 그룹에 포함된 객체는 편집 아이콘만 표시되어 편집이 가능하고 아무 곳에도 적용되지 않는 객체는 삭제 아이콘이 표시되며 삭제가 가능합니다.

생성된 그룹은 이름을 기준으로 자동 정렬 되며 그룹에 포함된 서비스객체 목록이 표시됩니다.

그룹 이름:	멤버:
서비스포트	ESP, FINGER, PC보안, 원도우터미널
	DNS, HTTP

☞ 그룹의 **새로생성** 버튼을 눌러 그룹을 만들고 이용 가능한 서비스 리스트 중 멤버로 이동하면 해당 주소는 해당그룹으로 포함되며 정책 적용 시 그룹리스트에서 선택 할 수 있습니다.  
그룹생성시 그룹객체도 그룹에 추가포함 할 수 있습니다.

## 3-4 일정

- ◆ 일정이란 정책이 적용되기 위한 시간설정 기능입니다.

## 3-4 #1 : 일회

- ☞ 일회 일정은 정책에 설정된 시작 시간부터 종료시간까지만 적용되며 자동삭제 되지는 않습니다.  
일회성 일정을 적용하는 경우 시스템시간을 기준으로 동작하므로 적용 전 시스템의 시간이 사용자의  
지역시간과 동일한지 확인 후 적용 해야 합니다.

이름	시작	종지
1time	2008/02/01 00:00	2009/02/01 00:00
내일점심만	2008/01/01 11:00	2008/01/01 13:00

## 3-4 #2 : 반복

- ☞ 반복일정은 적용된 정책이 항상 동작하도록 적용됩니다.  
시스템 초기 설정 시 기본적으로 모든 시간을 정의하는 always 가 정의 되어 있습니다.

이름	요일	시작	종지
always	SMTWTFS	00:00	00:00

## 3-5 가상주소

- ◆ 공인 IP와 사설 IP를 1:1로 매핑하여 외부 매핑된 공인IP로 연결 시도 시 사설IP로 연결 해주는 기능입니다.

### 3-5 #1 : 가상주소

☞ 공인IP 와 매핑 할 사설IP가 표시되며 적용된 사설IP는 무조건 매핑된 공인IP로 변환됩니다.

공인 IP가 동일한 경우 포트포워딩 기능을 이용하여 문제를 극복 할 수 있습니다.

단, 동일 IP에 중복되는 포트는 설정이 불가능 합니다.

사용 중이거나 그룹에 포함된 객체는 편집 아이콘만 표시되어 편집이 가능하고 아무 곳에도 적용되지 않는 객체는 삭제 아이콘이 표시되며 삭제가 가능합니다.



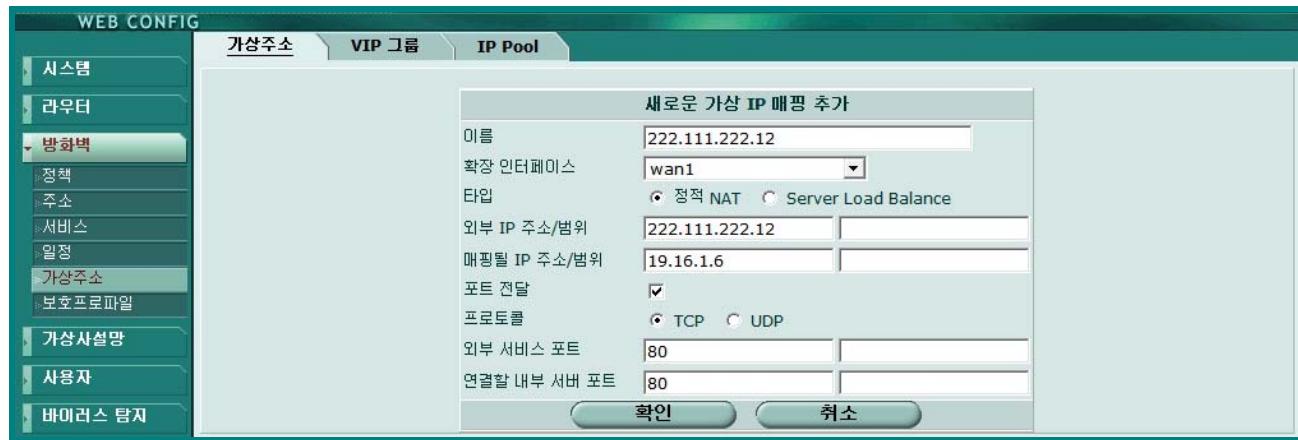
이름	IP	서비스 포트	IP 매핑	포트에 연결
222.111.222.10	wan1/222.111.222.10		19.16.1.5	
FTP	wan2/222.111.222.11	21/tcp	19.16.1.2	21/tcp
Terminal	wan2/222.111.222.11	3389/tcp	19.16.1.5	3389/tcp

☞ **새로생성** 버튼을 눌러 추가 할 수 있으며 외부공인 IP가 사용하는 확장인터페이스를 반드시 맞게 설정 해주어야 합니다.



☞ 포트전달 기능을 활성화 하면 포트번호를 입력할 수 있으며 외부에 서비스하는 포트와 서버에 설정된 서비스 포트 번호를 정확하게 입력해야 합니다.

포트전달 기능을 이용하면 부족한 공인 IP와 여러 개의 사설 IP를 매칭시킬 수 있습니다.



☞ Server Load Balance (SLB) 기능을 활성화 하여 여러 대의 서버로 SLB 구성을 할 수 있습니다.

단, SLB 구성에 맞도록 연결된 서버는 구성이 동일해야 합니다.

지원되는 알고리즘은 트래픽을 골고루 균등하게 모든 서버에 분배하는 Ststic 알고리즘과 서버에 균일한 횟수로 분배하는 Round Robin 알고리즘 그리고 가중치 값이 높은 서버에 우선적으로 분배하는 Weighted 알고리즘이 지원됩니다.



☞ Fortigate 의 SLB 기능은 L4 Switch의 부가적인 기능을 제공하는 것으로 전용 L4 Switch를 이용하는 것보다 Performance 가 좋지 않을 수 있으므로 되도록 전용시스템에서 구현하는 것을 권장합니다.

## 3-5 #2 : VIP 그룹

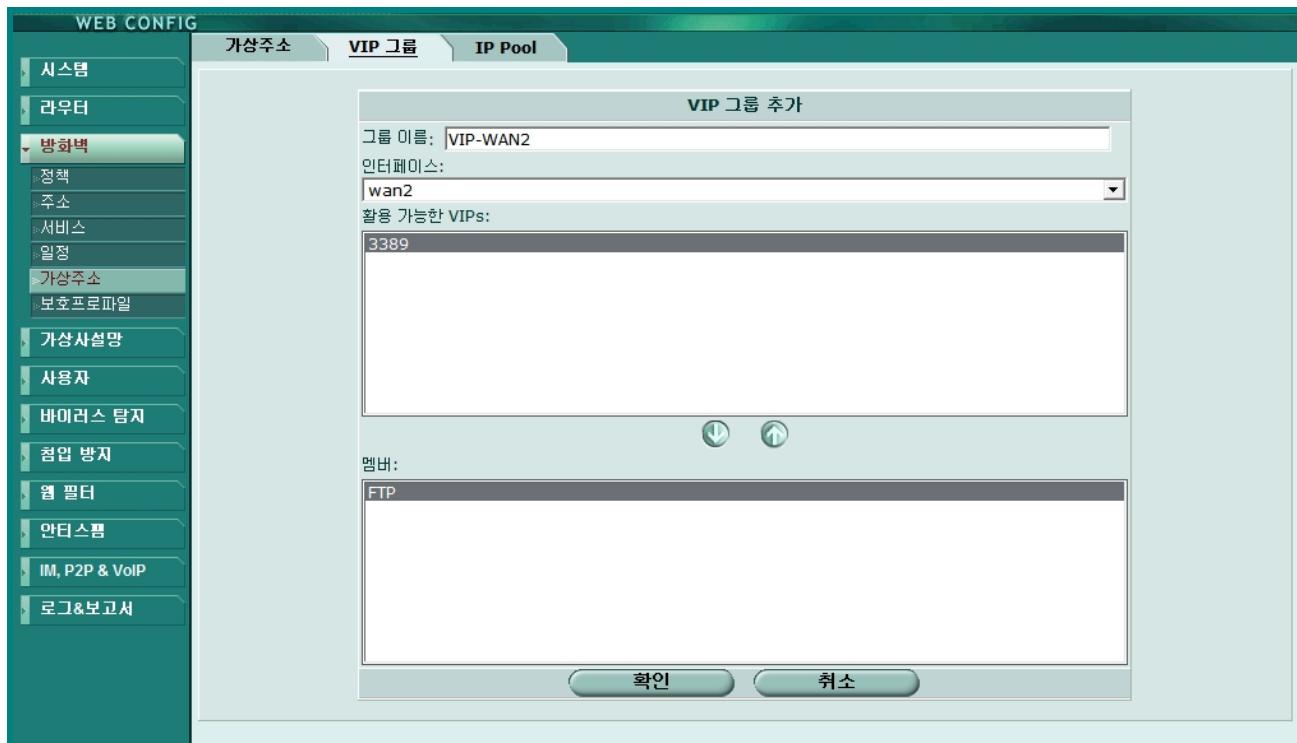
☞ VIP 그룹은 가상주소 리스트를 그룹으로 적용하는 기능입니다.

사용 중인 객체는  편집 아이콘만 표시되어 편집이 가능하고 아무 곳에도 적용되지 않는 객체는  삭제 아이콘이 표시되어 삭제가 가능합니다



그룹 이름	멤버	인터페이스
wan2-VIP서비스	FTP	wan2

☞ 그룹의 적용은 가상주소가 적용된 인터페이스를 선택하면 활용 가능한 VIPs 목록이 표시되며 해당 목록에서 멤버 목록으로 이동하면 적용이 되고 정책에 적용 할 수 있습니다.



**VIP 그룹 추가**

그룹 이름:   
 인터페이스:  
  
 활용 가능한 VIPs:  
 3389

멤버:  
 FTP

확인 취소

## 3-5 #3 : IP Pool

☞ 각 보안정책이 NAT 기능을 적용 받을 때 가용중인 공인 IP중 설정된 IP로 TCP/IP 의 헤더가 변환 되도록 하는 기능입니다.

IP POOL 범위 내에서 할당한 IP가 소진된 경우 자동으로 PAT로 전환되므로 별도의 설정을 추가 할 필요가 없으나 이 기능은 적용된 정책에 한해서만 적용 됩니다.



명칭	시작 IP	끝 IP
dmz		
wan1	222.222.222.2-15	222.222.222.2

☞ IP POOL은 반드시 해당디바이스에서 가용 가능한 대역의 IP로 적용 해야 합니다.

IP가 단일 IP 인 222.234.222.50 번으로 적용을 원하는 경우 <IP범위/서브넷>에 IP만 입력하면 되며 222.234.222.50부터 60까지 범위로 적용을 원하는 경우 222.234.222.50-222.234.222.60 로 순차적으로 입력하면 되며 네트워크 단위로 입력하면 자동으로 범위설정이 되지만 서브넷이 잘못 설정되면 범위로 설정이 되지 않고 단일 IP로 적용되므로 반드시 주의 해야 합니다..



새로운 유동 IP Pool 설정

이름:

인터페이스:  wan1

IP 범위/서브넷:  0.0.0.0-0.0.0.0

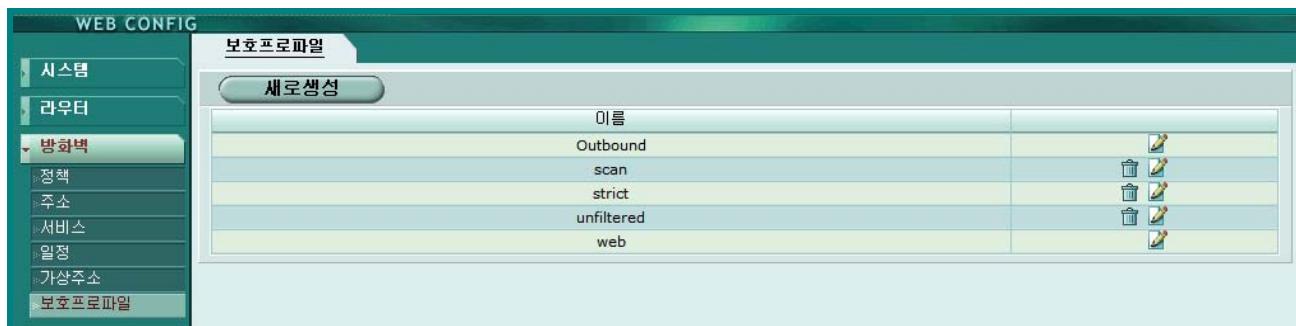
확인  취소

## 3-6 보호프로파일

◆ 보호프로파일은 방화벽정책 적용 시 필요한 부가기능을 적용하는 기능입니다.

☞ 적용된 보안정책만 부가기능이 적용되며 기본값으로 scan, strict, unfiltered, web 의 4가지 프로파일이 생성되어 있습니다.

기본적으로 생성된 객체는 상세설정이 각각 차이가 있으므로 되도록 새로 생성을 해서 사용하는 것을 권장 합니다.



이름	
Outbound	
scan	
strict	
unfiltered	
web	

☞ 보호프로파일은 각종 기능설정, 적용설정, 로깅설정 등을 할 수 있습니다.

보호프로파일은 설정된 정책에만 적용되므로 혼동이 없어야 합니다.

항목의 제일 앞부분인 ▶ 버튼을 누르면 상세항목이 펼쳐지며 화살표가 ▼ 모양으로 변경되며 각각의 기능에 대한 세부설정을 확인 및 변경 할 수 있습니다.



새 보호 프로파일

프로파일 명:

주석:

(maximum 63 characters)

- ▶ 앤티 바이러스
- ▶ 웹 필터링
- ▶ FortiGuard 웹 필터링
- ▶ 스팸 필터링
- ▶ 첨부 차단
- ▶ 콘텐츠 기록
- ▶ IM / P2P
- ▶ VoIP
- ▶ 로깅

확인 취소

## 3-6 #1 : 안티바이러스

◆ Fortigate 의 안티바이러스 기능은 특정 프로토콜 기반의 바이러스 방역기능입니다.

바이러스에 대해 차단만 되는 것으로 치료를 할 수 없으며 전송파일에 암호가 설정되어 있다면 스캔을 할 수 없습니다.

Fortigate가 탐지하는 7가지 프로토콜이 이외의 프로토콜을 통한 트래픽의 경우 바이러스가 감염 경로로 이용 될 수 있습니다.

인터넷 익스플로어를 이용하더라도 HTTP 가 8080 Port로 redirection 된다면 안티바이러스 스캔이 될 수 없으며 DISC, USB 등과 같은 이동식 매체로 바이러스가 이동되기 쉬우므로 사용자는 반드시 PC 전용 백신을 이용해야 하며 안티바이러스 백신프로그램의 기능과 혼동되어선 안됩니다.

☞ 안티바이러스기능을 활성화 하기 위해선 <안티바이러스 스캔>의 해당 프로토콜에 반드시 활성화가 되어 있어야 동작하며 7가지 프로토콜에만 적용이 가능합니다.

그레이웨어의 경우 바이러스탐지>구성>그레이웨어 리스트에서 활성화가 되어 있어야 차단됩니다.

	HTTP	FTP	IMAP	POP3	SMTP	IM	NNTP	옵션
안티바이러스 스캔	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
파일 패턴	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> builtin-patterns ▾				
조각 메일 통과			<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
클라미언트 알림	<input type="checkbox"/>	<input type="checkbox"/>						
간격 (1 - 900 초)	10	10						
량 (1 - 10240 바이트)	1	1						
설정 크기 초과 파일/메일	통과 ▾	통과 ▾	통과 ▾	통과 ▾	통과 ▾	통과 ▾	통과 ▾	
임계크기 (1 - 12 MB)	1	1	1	1	1	1	1	
외부로 나가는 메일에 서명 첨부하기	<input checked="" type="checkbox"/> 활성	FGT-Clean-Mail						<input type="checkbox"/> SMTP 만

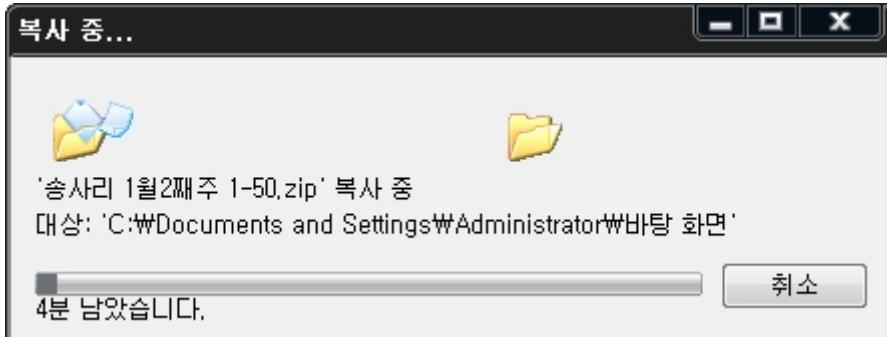
☞ <파일패턴>은 해당 프로토콜별 파일차단 및 안티바이러스 스캔을 예외 처리하는 기능이며 바이러스 탐지>파일패턴 리스트에 등록 및 조치 설정된 상태로 적용됩니다.

☞ <조각 메일 통과> 기능은 메일 데이터를 열었을 때 링크가 열려 나머지 데이터가 받아지는 조각 메일의 경우 AV가 스캔이 불가능 하므로 이에 대해 통과 시킬 것인지 설정을 하는 것입니다.

인터넷이 안되면 저장되어 있어도 볼 수 없는 메일들의 경우 이미 뉴스레터 등이 많이 이용됩니다.

PC에 응용프로그램백신을 사용 중이라면 문제가 없겠지만 미사용 중이라면 바이러스 감염에 노출될 가능성이 높으며 기능 활성화 시 조각메일은 통과됩니다.

- ☞ <클라이언트 알림> 기능은 인터넷 브라우저를 이용해 파일 다운로드 시 아래 그림과 같이 사용자 PC에 다운로드 상태를 표시해주는 기능입니다.



HTTP 와 FTP 프로토콜만 적용되며 FTP의 경우 브라우저를 이용하지 않는다면 상관이 없습니다.  
 Fortigate는 사용자가 파일을 다운로드 받을 때 조각을 내어 스캔을 한 후 완료된 파일에 대해 조합된 파일을 한번에 보내주므로 다운로드가 진행이 안되다가 갑자기 다 된 것처럼 처리됩니다.  
 이러한 현상 때문에 사용자는 다운로드를 다시 시작하는 사례를 방지하고자 지원되는 기능입니다.  
 단. HTTP 나 FTP 에 AV를 활성화 한 경우에만 해당됩니다.

- ☞ <임계크기>는 안티바이러스가 스캔을 하는 값을 지정하는 것입니다.

트래픽 특성상 큰 파일이 전송되는 경우 많은 delay를 수반 할 수 있으며 느리게 들어오는 트래픽을 시스템에 무한대로 적재되게 하는 것은 문제가 발생 할 수 있습니다.  
 파일이 전송되면 바이러스 스캔이 시작되고 이 데이터는 메모리에서 조각나 스캔 된 이후 사용자 PC에 전송되므로 **임계크기의 설정은 시스템의 과부하와 매우 관계가 높습니다.**

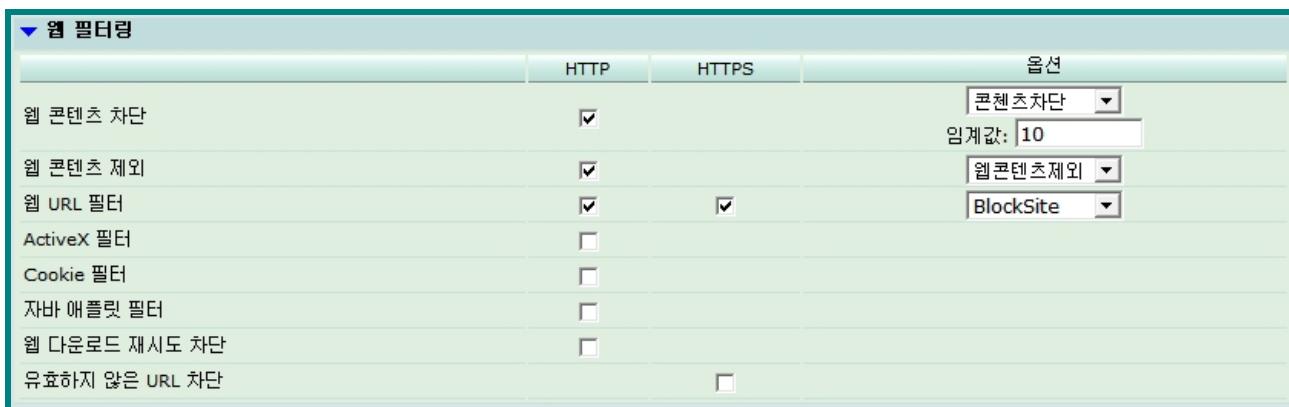
- ☞ <설정 크기 초과 파일/메일>은 임계크기 이상의 파일에 대한 처리방법을 설정하는 기능입니다.  
 FTP 등과 같이 프로토콜에 따라 전송될 파일 사이즈를 알려 주는 프로토콜인 경우에는 5MB라는 값을 받으면 그냥 바이패스 하지만 사이즈가 unknown 인 경우에는 1MB까지 buffering 을 한 후 1MB 버퍼가 꽉 찾는데도 EoF (End of File)가 들어 오지 않으면 그때 가서 임계 값에 대한 조치를 합니다.

- ☞ 임계크기가 1MB의 임계 값에 대하여 통과설정이 되어있는 경우 메일의 첨부파일에 30K, 100KB, 2MB 파일 3개가 첨부되었다면 각각 개별로 스캔 되므로 30K, 100KB 는 스캔 되고 2MB 는 바이패스 되지만 이 과정에서 하나라도 감염된 경우에는 splice mode 의 기본값은 활성화 이므로 모두 차단 됩니다.

- ☞ <외부로 나가는 메일에 서명 첨부하기> 기능을 사용하면 서명란에 설정내용이 첨부되어 발송되도록 하는 기능이며 SMTP 만 적용 됩니다.

## 3-6 #2 : 웹 필터링

- ☞ 웹필터링은 사용자가 HTTP나 HTTPS 프로토콜을 이용한 브라우징을 제한하는 기능입니다.  
내부사용자의 아웃바운드 데이터에 대하여 제한이 가능합니다.  
기능의 적용 시 웹필터 항목에 원하는 기능에 대한 리스트들이 설정 되어 있어야 합니다.  
각 항목별 리스트는 해당 기능의 옵션에서 선택이 가능하며 각 항목의 리스트 최대값은 모델 별 차이가 있습니다.



	HTTP	HTTPS	옵션
웹 콘텐츠 차단	<input checked="" type="checkbox"/>		콘텐츠차단 임계값: 10
웹 콘텐츠 제외	<input checked="" type="checkbox"/>		웹콘텐츠제외 BlockSite
웹 URL 필터	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
ActiveX 필터	<input type="checkbox"/>		
Cookie 필터	<input type="checkbox"/>		
자바 애플릿 필터	<input type="checkbox"/>		
웹 다운로드 재시도 차단	<input type="checkbox"/>		
유호하지 않은 URL 차단		<input type="checkbox"/>	

- ☞ <웹 콘텐츠> 차단은 웹페이지의 소스에 해당 단어가 있는 경우 차단하는 기능입니다.  
콘텐츠리스트의 단어 항목 각 설정된 값이 임계값과 동일하거나 이상인 경우 적용됩니다.  
임계값은 기본값은 10점이며 리스트 항목 중 <오빠 - 5점>, <아버지 - 7점>, <사랑해 - 3점>으로 등록했다면 <아버지와 오빠는 친합니다>의 경우 합계가 12점 이므로 차단됩니다.  
<오빠 사랑해>는 합계가 8점 이므로 허용되고 <아빠 사랑해>는 합계가 10점으로 차단됩니다.
- ☞ <웹 콘텐츠 제외>는 전체 항목 중 특정 예외항목만 제외하는 기능입니다.  
예를 들어 리스트에 ‘증권’을 차단 설정한 상태에서 ‘한국증권’만 예외리스트로 허용할 수 있습니다.
- ☞ <웹 URL 필터>는 전체 중 특정 예외항목만 제외하는 기능입니다.
- ☞ <ActiveX, Cookie, 자바애플릿 필터> 기능을 이용하면 등급에 따라 보안 노출 위험이 있는 기능들 차단될 수 있습니다..
- ☞ <웹 다운로드 재시도 차단> 기능은 파일이 조각나서 전송되는 경우 차단하는 기능이며 웹 재전송 기능은 다운로드 속도를 높이기 위한 방식으로 웹P2P, 플래쉬겟 등의 응용프로그램에서 많이 사용되며 PDF 문서의 다운로드 등에서 대표적으로 이용 됩니다.

## 3-6 #3 : FortiGuard 웹 필터링

- ☞ FortiGuard 서비스의 웹필터 라이센스를 구매한 사용자의 경우 해당 기능을 활성화 하여 사용 할 수 있으며 사용자가 URL Access를 요청할 경우 Fortigate는 FortiGuard 서버에 해당 URL 이 설정된 Category 분류 범주에 포함되는지 여부를 질의 하고 되돌아온 결과를 바탕으로 설정된 조치를 수행하는 기능입니다.
- ☞ FortiGuard 웹 필터링 기능은 HTTP 와 HTTPS 프로토콜을 지원하며 원하는 프로토콜 별 사용할 기능을 활성화 시 설정된 정책에 적용됩니다.

	HTTP	HTTPS
FortiGuard 웹 필터링 활성	<input checked="" type="checkbox"/>	<input type="checkbox"/>
FortiGuard 웹 필터링 오버라이드 활성	<input type="checkbox"/>	<input type="checkbox"/>
차단된 HTTP 4xx 와 5xx 오류의 상세 정보 제공	<input type="checkbox"/>	<input type="checkbox"/>
URL에 의한 이미지 래미팅 (차단된 이미지는 공백으로 대체 됨)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
분류 오류 발생한 웹 사이트 접속 허용	<input type="checkbox"/>	<input type="checkbox"/>
엄격 차단	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
도메인과 IP주소에 의한 URLs 필터링	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- ☞ FortiGuard 웹 필터링 사용시 상세분류 설정을 해두어야 원하는 효과를 얻을 수 있습니다. 대부분 필드의 ▶ 버튼을 누르면 소분류 항목이 펼쳐지며 대분류별 및 소분류별 분류 항목에 대하여 허용, 차단, 로깅 설정을 할 수 있습니다.
- ☞ 오버라이드를 사용하기 위해선 웹필터>FortiGuard 웹 필터>오버라이드 에 설정이 되어 있어야 합니다.
- ☞ 로컬분류 그룹은 웹필터>FortiGuard 웹 필터>로컬분류 에서 추가 할 수 있습니다.

분류	허용	차단	로그	오버라이드 허용
▶ 잠재적 위협	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
▶ 논쟁	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ 잠재적 비생산적	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ 잠재적 대역폭 소모	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ 잠재적 보안 위배	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ 일반적인 흥미	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ 앱무관련	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ 기타	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
다미내믹 컨텐츠	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
기타	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
웹호스팅	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
보안 사이트	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
컨텐츠 서버	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
미등급	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ 로컬 분류	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ 사용자필터	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>

분류	허용	차단	로그	오버라이드 허용
캐시된 컨텐츠	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
멀티미디어 검색	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
이미지 검색	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
오디오 검색	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
비디오 검색	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
스팸 URL	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>

## 3-6 #4 : 스팸 필터링

☞ FortiGuard 서비스의 안티스팸 기능과 사용자정의 스팸 필터 설정을 할 수 있습니다.

FortiGuard 안티스팸은 데이터베이스가 자동으로 업데이트 되며 라이센스를 구매한 사용자만 사용이 가능하지만 사용자정의 스팸필터 설정은 수동으로 패턴을 만들어 적용을 할 수 있습니다.

☞ FortiGuard 안티스팸은 IP주소, URI, 이메일체크섬에 대해 체크를 하며 스팸의뢰 기능을 제공 합니다. 사용자정의 필터는 IP주소BWL, 역DNS, 이메일주소 BWL, 반송이메일 DNS, 차단단어에 대한 체크 설정을 지원합니다.

스팸차단은 메일서버가 내부에 있는 경우만 SMTP에 대하여 폐기 및 태깅이 가능하지만 메일서버가 외부에 있다면 POP3 통신에 대한 태깅 설정만 가능하므로 메일서버의 스팸차단을 하기 위해선 Fortigate의 Internal 구간에 메일서버가 위치 해야 합니다.

업무상 메일은 주로 업무 시간대에 왕래하므로 반송 이메일 DNS 사용의 경우 업무 이후의 시간대 스케줄링으로 설정 하면 효과적으로 강력한 SPAM 차단 기능을 얻을 수 있습니다.

스팸 필터링				옵션
	<input type="checkbox"/> IMAP	<input checked="" type="checkbox"/> POP3	<input checked="" type="checkbox"/> SMTP	
<b>FortiGuard 안티스팸</b>				
IP 주소 체크	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
URL 체크	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
이메일 체크섬 체크	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
스팸 의뢰	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
IP 주소 BWL 체크	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	SpamIP <input type="button" value="▼"/>
역 DNS 검색	<input type="checkbox"/>			
이메일 주소 BWL 체크	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Spam-Email <input type="button" value="▼"/>
반송 이메일 DNS 체크	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
차단 단어 체크	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SpamWord <input type="button" value="▼"/> 임계값: <input type="text" value="10"/>
스팸 조치	태깅			<input type="button" value="폐기 ▾"/>
덧붙이기	<input type="radio"/> 제목 <input type="radio"/> MIME	<input type="radio"/> 제목 <input type="radio"/> MIME	<input type="radio"/> 제목 <input type="radio"/> MIME	
덧붙이기	<input type="text" value="Spam"/>	<input type="text" value="Spam"/>	<input type="text" value="Spam"/>	

☞ FortiGuard 안티스팸은 SMTP Sender로부터 메일 메시지를 받게 되면 FortiGuard 안티스팸 서버에 SMPMMER 여부를 체크하여 리스트에 포함되어 있다면 스팸조치에 설정된 조치를 수행하며 Caching 기능을 사용중인경우 설정된 시간동안 메모리에 담아두게 됩니다.

☞ 사용자정의 필터 기능의 적용 시 **안티스팸** 항목에 원하는 기능에 대한 리스트들이 설정 되어 있어야 하며 각 항목별 리스트는 해당 기능의 옵션에서 선택이 가능하며 각 항목의 리스트 최대값은 모델 별 차이가 있습니다.

## 3-6 #5 : 침입차단

- 침입차단 기능은 시그니처 기반의 탐지기법과 Anomaly 기반의 탐지기법을 제공합니다.
- 상위 레벨을 활성화 한 경우 하위레벨을 포함합니다.  
 침입방지>시그니처, Anomaly 에 설정 되어있는 사전정의, 사용자정의 Anomaly 패턴에 활성화 된 패턴 중 설정된 레벨에 대해서만 적용이 되며 시그니처별 다양한 조치설정을 할 수 있습니다.

	심각함	높음	중간	낮음	정보
IPS 시그니처	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IPS Anomaly	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## 3-6 #6 : 콘텐츠 기록

- 콘텐츠 기록은 스캔된 Packet Data 에 대한 상세 내용을 표시해주는 기능으로 시스템의 Proxy Daemon이 동작하는 프로토콜의 경우(바이러스스캔, 콘텐츠필터) 만 적용됩니다.
- 콘텐츠 기록을 원하는 프로토콜의 활성화시 설정으로 바로 적용되며 시스템>상태>통계 항목에서 확인이 가능합니다.  
 장시간의 모든 데이터를 적용하기 위해선 FortiAnalyzer 혹은 FortiGuard Analysis 서비스를 이용하는 경우만 적용됩니다.

	HTTP	HTTPS	FTP	IMAP	POP3	SMTP	NNTP
시스템 대쉬보드에 컨텐츠 메타정보 표시	<input checked="" type="checkbox"/>	<input type="checkbox"/>					
	AIM	ICQ	MSN	Yahoo!			
시스템 대쉬보드에 컨텐츠 메타정보 표시	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			

**For long-term archival of content information, please configure a FortiAnalyzer device or the FortiGuard Analysis Service.**

## 3-6 #7 : IM / P2P

- ☞ 국제적으로 많이 사용하는 4가지의 인터넷 메신저와 6가지 P2P 응용프로그램에 대한 제어설정 기능을 제공합니다.
- ☞ 인터넷 메신저의 경우 로그인 차단, 파일전송 차단, 음성차단, 비 표준 포트 검사 등을 적용 할 수 있으며 유사패턴의 메신저를 차단 할 수 있으며 IM, P2P&VoIP>사용자에서 ID에 대한 설정에 따라 다르게 동작 할 수 있습니다.  
애플리케이션 메신저가 아닌 MSN, Yahoo 웹메신저 및 중국에서 많이 사용하는 qq메신저의 경우 침입방지>시그니처에서 추가적으로 차단 설정을 해야 차단됩니다.  
인터넷 메신저가 SSH Proxy 통신인 암호화 통신을 하는 경우 차단이 불가능 합니다.  
P2P의 경우 차단, 통과, 사용량 제한을 적용 할 수 있습니다.

▼ IM / P2P					
	<input checked="" type="checkbox"/> AIM	<input checked="" type="checkbox"/> ICQ	<input checked="" type="checkbox"/> MSN	<input checked="" type="checkbox"/> Yahoo!	<input checked="" type="checkbox"/> SIMPLE
로그인 차단	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
파일 전송 차단	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
음성 차단	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
비 표준 포트 검사	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	BitTorrent	eDonkey	Gnutella	Kazaa	Skype
활동	차단	Rate 한계	통과	차단	차단
한계 (KBytes/s)	0	100	0	0	0

## 3-6 #8 : VoIP

- ☞ SIP, SCCP 프로토콜을 이용하는 VoIP 통신에 대한 제한설정을 제공하며 H.323 프로토콜을 이용하는 경우 제한 적용을 할 수 없습니다.
- VoIP 통신에 대한 제한 가능성을 이용하는 경우 M, P2P&VoIP>통계에서 상세정보 및 통계정보를 확인할 수 있습니다.

▼ VoIP		
	<input checked="" type="checkbox"/> SIP	<input checked="" type="checkbox"/> SCCP
REGISTER 요청 제한(초당 요청 수) (SIP only)	10	
INVITE 요청 제한(초당 요청 수) (SIP only)	50	
콜 셋업 제한(1분당 콜 셋업) (SCCP only)	50	

## 3-6 #9 : 로깅

적용된 프로파일에서 사용하는 기능에 대한 로깅 활성화를 하여 로그 설정을 적용 할 수 있습니다.  
 안티바이러스, 침입방지, 웹필터, 안티스팸 등의 모든 로그기록에 대한 설정을 할 수 있습니다.  
 로그&보고서>로그설정 과 로그정책 에 로깅설정 및 로그필터 설정이 되어 있어야 적용되며 해당 로그  
 는 적용된 보안저액과 사용중인 사용 중인 프로파일에 대해서만 적용됩니다.

▼ 로깅	
	로그
안티 바이러스	<input checked="" type="checkbox"/>
바이러스	<input checked="" type="checkbox"/>
차단된 파일	<input checked="" type="checkbox"/>
크기초과 파일 / 이메일	<input checked="" type="checkbox"/>
웹 필터링	<input checked="" type="checkbox"/>
콘텐츠 차단	<input checked="" type="checkbox"/>
URL 필터	<input checked="" type="checkbox"/>
ActiveX 필터	<input type="checkbox"/>
Cookie 필터	<input type="checkbox"/>
자바 애플릿 필터	<input type="checkbox"/>
FortiGuard 웹 필터링	<input type="checkbox"/>
분류오류 HTTP 만	<input type="checkbox"/>
스팸 필터링	<input checked="" type="checkbox"/>
스팸 로그	<input checked="" type="checkbox"/>
침입차단	<input checked="" type="checkbox"/>
침입 로그	<input checked="" type="checkbox"/>
IM / P2P	<input checked="" type="checkbox"/>
IM 사용 로그	<input checked="" type="checkbox"/>
P2P 사용 로그	<input checked="" type="checkbox"/>
VoIP	<input checked="" type="checkbox"/>
VoIP 사용률 로그	<input checked="" type="checkbox"/>

## 4 가상사설망

- ◆ 인터넷과 같은 공중망(public network)을 마치 전용선으로 사설망(private network)을 구축한 것처럼 사용할 수 있는 기능입니다.  
IPSEC, PPTP, SSL 방식이 지원되며 IPSEC은 Site To Site VPN과 Site To Host를 수반하지만 PPTP, SSL의 경우 Site To Host만 적용이 가능합니다.  
IPSEC은 VPN 표준을 지원하며 Site To Site VPN의 경우 VPN 표준을 지원하는 시스템끼리는 호환이 가능합니다.

### 4-1 IPSEC

- ◆ IPSEC (Internet Protocol Security)은 VPN 표준을 통해 VPN으로 연결하는 기능입니다.  
Site To Site VPN의 경우 VPN 표준을 지원하는 시스템끼리는 호환이 가능합니다.  
IP Layer에서 암호화된 패킷을 주고받는 방식으로 NAT/ROUTE 모드와 TP 모드에서도 암호화를 지원하며 Auto Key와 Manual Key 방식을 제공하며 IPv6를 지원합니다.  
IPSEC Concentrator 기능을 제공하므로 해당 기능을 이용하여 Hub & Spoke 기능 구현이 가능하며 DHCP over IPSEC을 지원합니다.

- ◆ IPSEC에서는 두 종류의 보안 프로토콜이 사용되며 어떠한 조합도 지원이 가능합니다.

#### 1. AH (인증헤더)

- IP 패킷에서 AH는 보내진 데이터의 인증과 연결의 무결성 검증에 이용됩니다.
- 인증은 단일방향의 해쉬 기반의 메시지 인증 코드(HMAC)를 사용합니다.
- MD5 (Message Digest Version 5) / 128bit 해쉬 지원
- SHA-1 (Secure Hash Algorithm-1) / 160bit 해쉬 지원

#### 2. ESP (캡슐화된 보안 페이로드 / 데이터 암호화)

- DES - 56bit 키
- 3DES - 168bit 키
- AES - 128, 192, 256 bit 키

## 4-1 #1 : Auto Key / IKE

☞ Internet Key Exchange 는 상호 시스템간에 Key를 자동으로 생성해 교환 하는 방식으로 PFS (Perfect Forward Secrecy), ID 보호, 인증서비스를 제공하며 신속한 Key 업데이트를 지원합니다.

☞ 일반적으로 2단계를 걸쳐 VPN 터널 생성이 이루어 집니다.

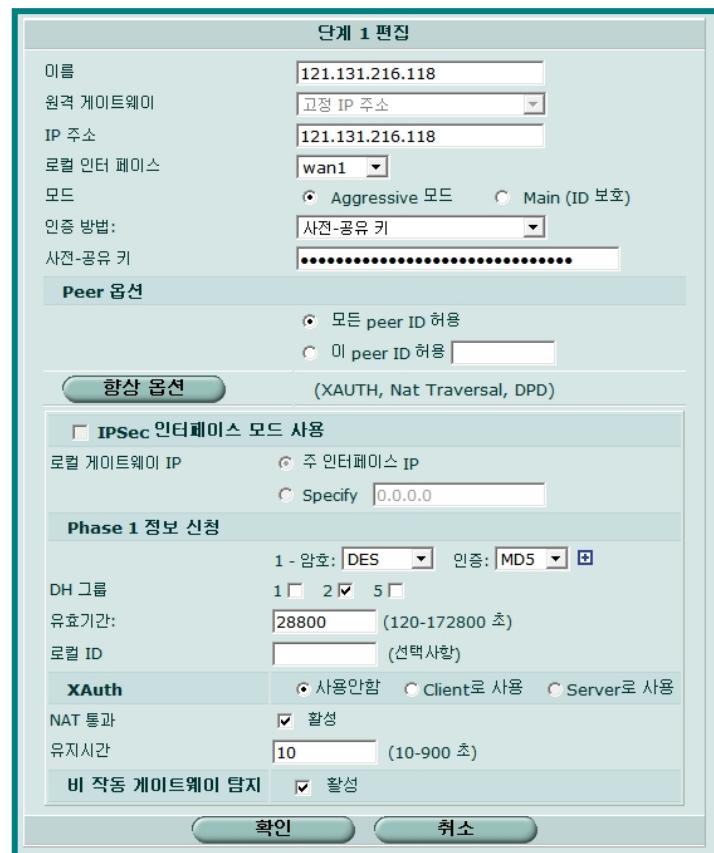
단계1 은 동일 IP에 대하여 중복생성은 불가능 하지만 단계2 는 중복사용이 가능합니다.



☞ 단계1 에서는 VPN을 연결하려는 Peer 와 IPSEC SA를 Negotiate 하여 보안 채널을 설정 합니다.  
원격게이트웨이에서 Peer 시스템이 고정 IP인지 유동IP 인지 선택을 해야 합니다.  
로컬인터넷페이스는 외부 트래픽이 들어 오는 인터페이스를 말합니다.  
사전공유키는 Peer 와 동일해야 합니다.

☞ 향상옵션을 이용하여 암호화, 인증 방식 과 DH그룹 및 Key의 유효기간을 지정 할 수 있습니다.

☞ 인증기능을 이용하여 Peer 인증을 적용 할 수 있습니다.



- ☞ 단계2 에서는 VPN을 연결하려는 Peer의 단계1을 선택해야 합니다.
  
- ☞ 향상옵션을 이용하여 암호화, 인증 방식 재생탐지기능 및 PFS 기능을 활성화 할 수 있으며 과 DH그룹 및 인증 유효 기간을 지정 할 수 있습니다.
  
- ☞ Quick 모드 기능을 이용하여 빠른 VPN 기능을 이용할 수 있습니다. 출발지 주소는 보안정책과 동일 해야 합니다.

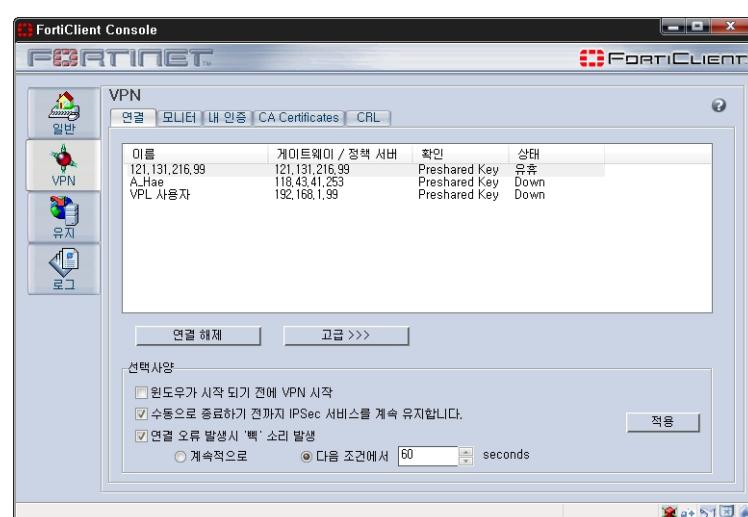


- ☞ IPSEC 보안정책은 아웃바운드로 설정해야 하며 동작모드는 ENCRYPT로 설정 해야 합니다. Dial UP IPSEC 을 제외한 모든 IPSEC 정책은 목적지가 반드시 지정 되어 있어야 합니다.



The screenshot shows the 'WEB CONFIG' interface under '정책' (Policies). It displays two IPSEC policies: one for 'internal -> wan1' (ID 7) and another for 'internal -> wan2' (ID 2). Both policies have source and destination addresses set to 'all'. The policy for wan2 is marked as 'Outbound' and 'ACCEPT'.

- ☞ IPSEC 을 이용한 Site To Host VPN 의 경우 전용 VPN 클라이언트 프로그램인 FortiClient를 이용하면 손쉽게 Mobile 사용자의 IPSEC VPN 을 이용할 수 있습니다.



## 4-1 #2 : 수동 키 값 교환

- ☞ 수동키는 Peer 시스템과 동일한 키를 가지고 있어야 합니다.  
키 값은 SA Database에 고유하게 설정되어 있는 값만 적용이 가능합니다.



## 4-1 #3 : Concentrator

- ☞ VPN 터널을 Concentrator로 연결하면 연결된 모든 Peer 터널이 센터 시스템을 통해서 통신이 되는 가능입니다.



## 4-1 #4 : 모니터

☞ 연결된 상태의 VPN은 모니터 탭에서 상태를 확인 할 수 있습니다.

Name	Type	Remote Gateway	Remote Port	Timeout	Proxy ID Source	Proxy ID Destination	Status
121.131.216.118	Static IP 와 동적 DNS	121.131.216.118	0	1206	19.16.1.0-255.255.255.0	1.1.1.0-255.255.255.0	Bring Down

☞ Type별 필터링을 설정 할 수 있으며 다이얼업 VPN의 경우 Peer ID 가 Username으로 표시됩니다.

Name	Remote Gateway	Remote Port	Username	Timeout	Proxy ID Source	Proxy ID Destination	Status
DIAL_0	218.144.180.142	0	(본점)	1774	1.1.1.*	19.16.1.*	Bring Down

## 4-2 PPTP

◆ PPTP (Point-to-Point Tunnelling Protocol)는 마이크로소프트, 3COM 등에서 공동으로 개발하였으며 컴퓨터와 컴퓨터가 1대 1 방식으로 데이터를 전송하여, 다른 시스템이나 인터넷으로 보안을 유지하면서 가상사설망을 지원해주는 기능입니다.

PPTP VPN은 NAT/ROUTE 모드만 제공되며 정책의 적용 및 사용자 접속 설정법은 영문메뉴얼, 설치 엔지니어, 기술지원센터, 특정기능 전용메뉴얼, 온라인헬프를 참고 하시기 바랍니다.

☞ PPTP는 통신을 하기 위해 사용중인 내부 IP대역에서 특정 IP를 HOST PC에 할당해야 사용이 가능하므로 내부의 사용중인 IP와 충돌이 나면 안됩니다.

PPTP의 사용시 인증사용자 계정과 인증사용자그룹을 먼저 생성 해두어야만 활성화가 가능하며 시작과 종료 범위를 지정해야만이 적용 됩니다.

사용자계정의 생성은 해당 부분의 매뉴얼에서 확인 하시기 바랍니다.



☞ PPTP는 보안정책은 아래그림의 정책 10번처럼 사용자 그룹에서 적용된 프로파일을 선택하면 적용되며 인바운드 방향의 정책으로 설정해야 적용됩니다.

정책의 적용 시 반드시 PPTP 대역의 Local 네트워크를 지정해야 합니다.



상태	ID	발신지	목적지	스케줄	서비스	프로파일	동작
▶ internal -> wan1 (2)							
▶ internal -> wan2 (2)							
▶ wan2 -> internal (4)							
<input checked="" type="checkbox"/>	10	<input checked="" type="radio"/> all	<input checked="" type="radio"/> 19.16.1.0/24	always	<input checked="" type="radio"/> ANY	PPTP	ACCEPT
<input type="checkbox"/>	11	<input checked="" type="radio"/> all	<input checked="" type="radio"/> 19.16.1.0/24	always	<input checked="" type="radio"/> ANY	SSL-VPN	ACCEPT
<input type="checkbox"/>	8	<input checked="" type="radio"/> all	<input checked="" type="radio"/> all	always	<input checked="" type="radio"/> 서비스 사용포트	ACCEPT	ACCEPT
<input type="checkbox"/>	3	<input checked="" type="radio"/> all	<input checked="" type="radio"/> Terminal	always	<input checked="" type="radio"/> ANY	ACCEPT	ACCEPT

## 4-3 SSL

◆ SSL (Secure Sockets Layer) VPN 은 Clientless VPN으로 사용자의 PC의 웹 브라우저를 이용해 가상 사설망 을 연결하는 기능입니다.

전용 SSL VPN 시스템처럼 Site To Site VPN 은 지원하지 않습니다.

SSL VPN 은 NAT/ROUTE 모드만 제공되며 정책의 적용 및 사용자 접속 설정법은 영문메뉴얼, 설치 엔지니어, 기술지원센터, 특정기능 전용메뉴얼, 온라인헬프 를 참고 하시기 바랍니다.

## 4-3 #1 : 설정

☞ SSL-VPN 을 활성화 하여 사용시 로그인 포트는 기본적으로 TCP 10443을 이용하지만 변경 할 수 있으며 사용자가 VPN 을 연결할 때는 [https:<접속IP>:로그인포트](https://<접속IP>:로그인포트) 로 접속을 합니다.

터널 IP 범위는 터널링을 연결할 Internal 구간의 IP 범위이며 지정하지 않아도 무방합니다.

서버인증은 사용자인증의 경우 셀프-사인을 선택합니다.

서버인증 방식을 Fortinet\_Local 을 선택한 경우 사용시스템의 인증서를 이용 할 수 있습니다.

클라이언트 인증 필요 기능 사용시 반드시 인증서가 설치된 사용자 계정만 접근허용이 되므로 예외 상황의 경우만 사용하기 바랍니다.



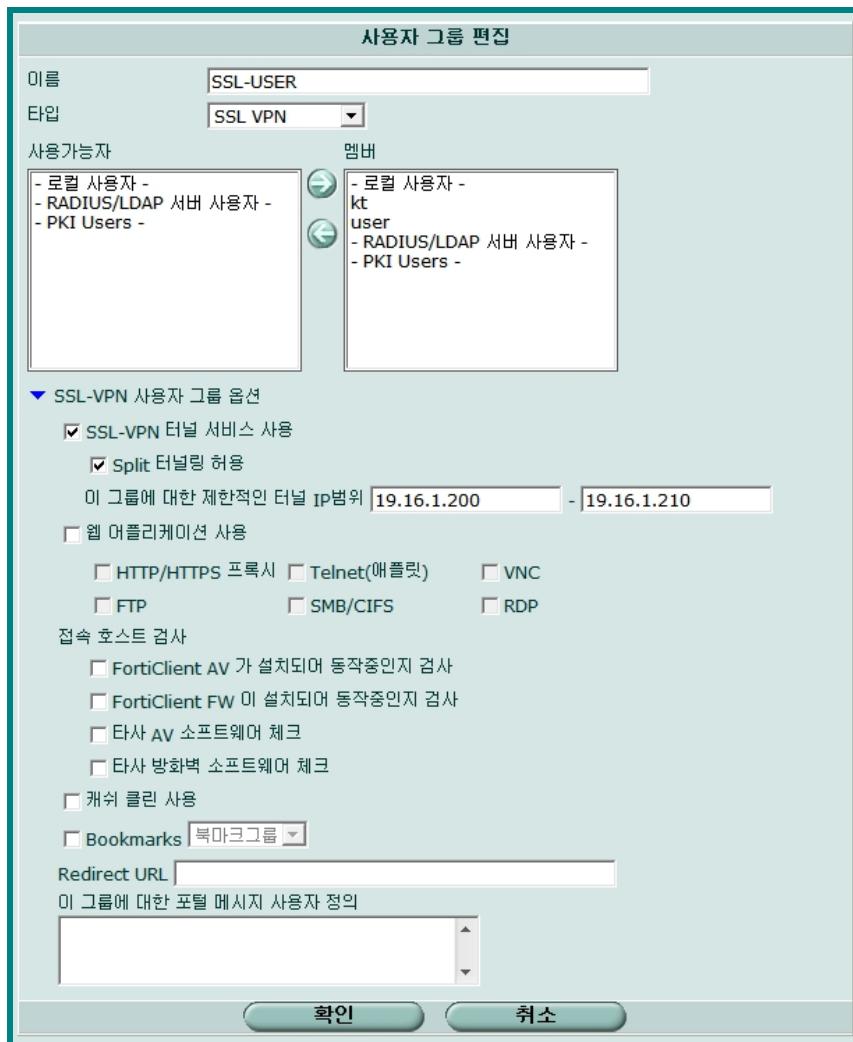
☞ SSL-VPN 도 PPTP처럼 인증사용자 계정과 인증사용자그룹을 먼저 생성 해 두어야 하며 사용자 PC에 할당 할 IP를 지정해야 합니다.

Split 터널링은 클라이언트PC의 라우팅을 변경하지 않도록 하는 설정이며 클라이언트에게 할당 해줄 IP를 Internal 대역 중에 할당 해주도록 합니다.

터널링의 제한적인 터널 IP 범위 안의 사용자에게 할당 될 IP를 설정해야 하며 사용자>사용자그룹에서 설정 할 수 있습니다.

웹 응용프로그램 사용을 활성화 하면 클라이언트에서 로그인 후 Proxy 응용프로그램을 이용 할 수 있습니다.

접속 호스트에 대한 AV 소프트웨어가 설치되어있는지 체크하는 기능은 모든 소프트웨어에 적용되는 것은 아니므로 해당기능을 사용하는 경우 사용중인 소프트웨어와의 호환 여부를 확인 해야 합니다.



☞ 보안정책은 PPTP 정책처럼 인바운드 방향으로 설정해야 하며 동작을 SSL로 선택해야 합니다.

## 4-3 #2 : 모니터

- ☞ SSL-VPN 을 통해 연결된 사용자에 대한 모니터 상태가 표시됩니다.  
접속한 계정과 접근한 외부 공인IP , 접속시간을 확인 할 수 있습니다.
- 刪 삭제 아이콘을 누르면 연결된 사용자의 접속이 끊어지게 됩니다.  
접속에 대한 USER Count 는 체크하지 않으므로 같은 공인 IP를 사용하는 공유기 혹은 NAT 환경의 사용자가 동시 접속한 경우 출발지 IP, 사용자 계정은 여러 개가 동일하게 표시 될 수 있습니다.

No.	사용자	출발지 IP	시작 시간	설명	Action
1	user	211.243.255.131	Sun Jul 13 04:50:38 2008		

## 4-3 #3 : Bookmark

☞ Bookmark 기능을 이용하여 Host 의 Access를 손쉽게 적용 할 수 있습니다.

Bookmark Name	Link	Actions
Telnet 19.16.1.1	telnet://192.168.1.1	
FTP 19.16.1.50	//server/folder/	

## 4-3 #4 : Bookmark Group

☞ Bookmark 그룹을 적용하면 Host 의 Access에 북마크 그룹을 제공 할 수 있습니다.

Bookmark 그룹의 적용은 사용자>사용자그룹에서 설정 할 수 있습니다.

Group Name	Bookmarks	Actions
북마크그룹	19.16.1.50, 19.16.1.1	

## 4-4 인증

◆ 가상사설망 사용시 사용할 수 있는 인증서를 제어하는 기능입니다.

Local 인증, 원격, CA인증에 대하여 인증서 생성 및 삽입 할 수 있습니다.

적용된 인증서는 가상사설망 사용시 Host 인증에 대하여 적용 할 수 있습니다.



이름	주제	상태
Fortinet_Local	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Fortigate, CN = Fortigate, emailAddress = support@fortinet.com	<input type="button" value="확인"/> <input type="button" value="검색"/> <input type="button" value="수정"/>



이름	주제
REMOTE_Cert_1	C = KR, O = SignKorea, OU = AccreditedCA, CN = SignKorea CA



이름	주제
Fortinet_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = support, emailAddress = support@fortinet.com

☞ CRL (Certificate Revocation List) 인증서 폐기목록은 네트워크상을 통한 서버 접근 제어에 PKI를 적용 할 때 쓰게 되는 일반적인 방식 중 하나입니다.

CRL은 가입자 이름과 인증서의 현재 상태로 구성된 목록인데, 폐기 사유와 인증서 발급일, 발급기관 등의 정보도 포함되어 있으며 이 기능을 이용하여 적극적인 인증서 관리를 할 수 있습니다.

## 5 사용자

- ◆ 가상사설망 인증 및 방화벽, 액티브 디렉토리, NTLM(NT LAN Manager) 인증기능을 사용하기 위해 접속허가를 설정하기 위한 사용자 인증 및 각종 인증서버 연동설정, PKI (Public Key Infrastructure) 공개키 생성 기능 등을 설정 하는 기능입니다.

### 5-1 로컬

- ◆ 로컬 사용자를 생성하거나 사용자계정에 대한 LDAP, RADIUS 계정을 생성을 하는 기능입니다.

사용자 이름	타입
USER-LDAP	LDAP
USER-RADIUS	RADIUS
kt	LOCAL
user	LOCAL

- ☞ 사용자 생성시 로컬인증은 암호를 선택한 후 생성해야 하며 LDAP, RADIUS를 선택하려면 인증서버 와의 연동 설정이 되어 있어야 적용이 가능합니다.

## 5-2 RADIUS

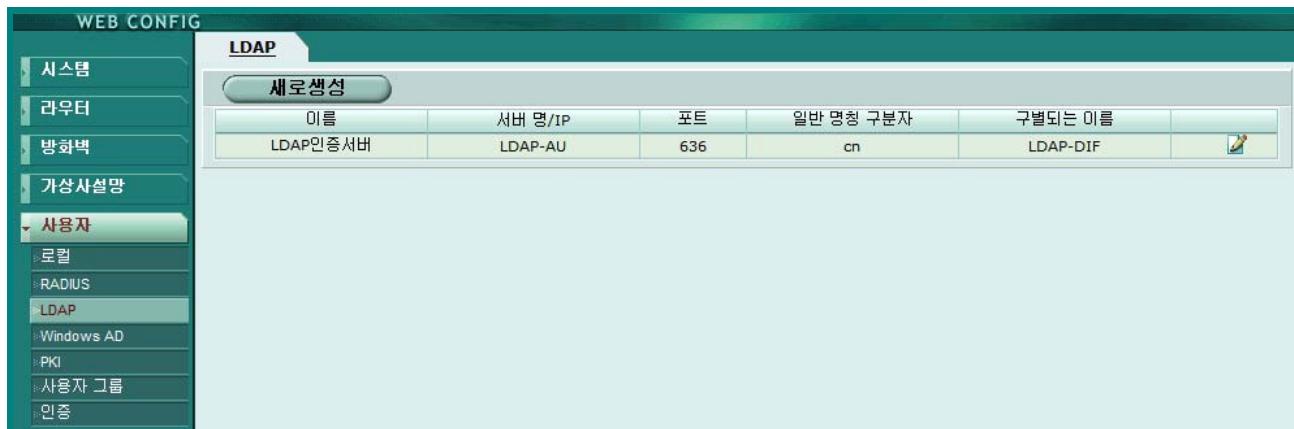
- ◆ RADIUS 인증을 위한 서버를 설정 하는 기능입니다.

이름	서버명/IP
RADIUS인증서버	R-AU-1 / 1.1.1.128

이름	RADIUS인증서버
Primary Server Name/IP	R-AU-1
Primary Server Secret	*****
Secondary Server Name/IP	1.1.1.128
Secondary Server Secret	*****
NAS IP/Called Station ID	1.1.1.129
Include in every User Group	<input checked="" type="checkbox"/> Enable

## 5-3 LDAP

◆ LDAP 인증을 위한 서버를 설정 하는 기능입니다.



이름	서버 명/IP	포트	일반 명칭 구분자	구별되는 이름
LDAP인증서버	LDAP-AU	636	cn	LDAP-DIF

☞ 서버 포트 및 보안연결 설정과 인증서를 지정 등을 변경 할 수 있습니다.



**LDAP 서버 편집**

이름: LDAP인증서버  
 서버 명/IP: LDAP-AU  
 서버 포트: 636  
 일반 명칭 구분자: cn  
 구별되는 이름: LDAP-DIF 

Secure Connection:   
 Protocol:  LDAPS  STARTTLS  
 Certificate: Fortinet\_CA

**확인** **취소**

## 5-4 Windows AD

- ◆ Windows 액티브 디렉토리 인증 서버와 연동 설정 하는 기능입니다.



The screenshot shows the 'WEB CONFIG' interface with the 'Windows AD' tab selected. On the left, a sidebar lists various configuration categories like System, Router, Firewall, and User. Under the 'User' category, 'Windows AD' is selected. The main panel displays a table titled 'Windows AD' with one entry: 'FortiClient AD' and '액티브디렉트리'. The IP addresses listed are 19.16.1.130:8000, 19.16.1.131:8000, and 19.16.1.158:8000. To the right of the table are three icons: a trash can, a pencil, and a shield.

- ☞ 하나의 목록에 최대 5개의 IP를 지정할 수 있으며 포트는 수정이 가능합니다.

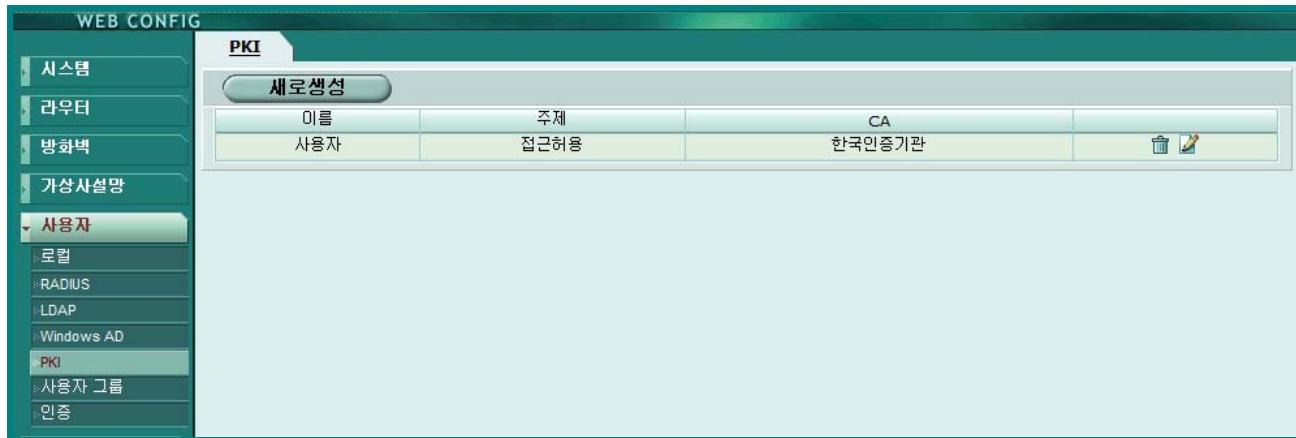


This screenshot shows the 'Windows AD' configuration page with the '편집' (Edit) button selected. It displays a list of five IP addresses for the '액티브디렉트리' entry. Each entry includes an IP address field, a port field set to 8000, and a password field containing '\*\*\*\*\*'. Below the table are two buttons: '확인' (Confirm) and '취소' (Cancel).

IP 주소	포트	암호
19.16.1.130	8000	*****
19.16.1.131	8000	*****
19.16.1.158	8000	*****
	8000	
	8000	

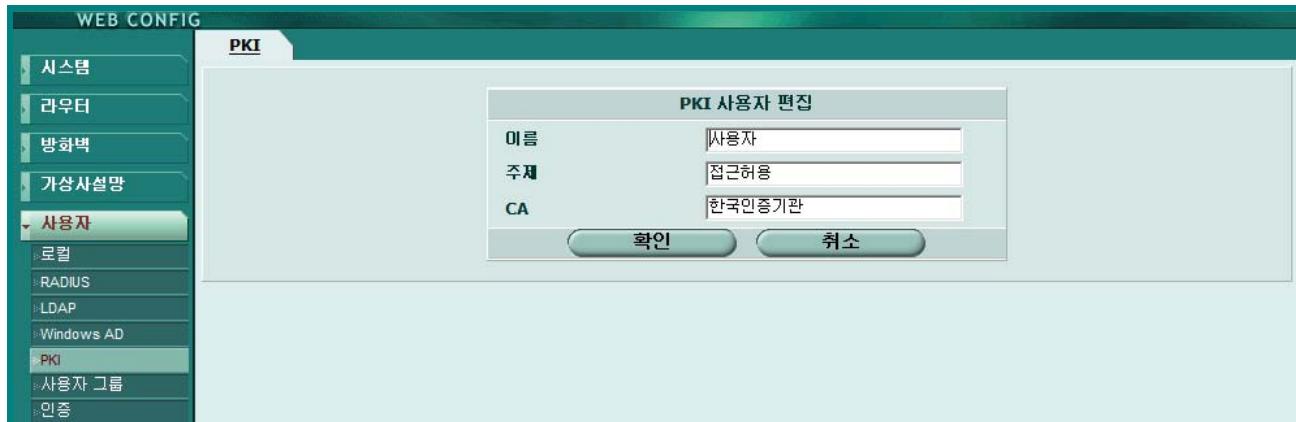
## 5-5 PKI

◆ Public Key Infrastructure를 생성하여 사용자가 보유한 암호를 이용하도록 설정하는 기능입니다.



The screenshot shows the 'WEB CONFIG' interface with the 'PKI' tab selected. On the left, a sidebar menu includes '시스템', '라우터', '방화벽', '가상사설망', '사용자' (selected), '로컬', 'RADIUS', 'LDAP', 'Windows AD', 'PKI' (selected), '사용자 그룹', and '인증'. The main content area displays a table titled '새로생성' (Create New) with columns '이름' (Name), '주제' (Subject), and 'CA'. The row contains '사용자' (User), '접근허용' (Allow Access), and '한국인증기관' (Korea Certification Authority). A trash can icon and a pencil icon are also present.

☞ PKI는 규격에 맞게 생성해야 합니다.



The screenshot shows the 'WEB CONFIG' interface with the 'PKI' tab selected. On the left, the same sidebar menu is visible. The main content area displays a dialog box titled 'PKI 사용자 편집' (Edit PKI User) with fields for '이름' (Name), '주제' (Subject), and 'CA'. The values are set to '사용자' (User), '접근허용' (Allow Access), and '한국인증기관' (Korea Certification Authority). At the bottom are '확인' (Confirm) and '취소' (Cancel) buttons.

## 5-6 사용자 그룹

◆ 사용자 그룹은 방화벽(PPTP, IPSEC, 보안정책), 액티브 디렉토리, SSL VPN 등의 인증을 위해 설정하는 기능입니다.

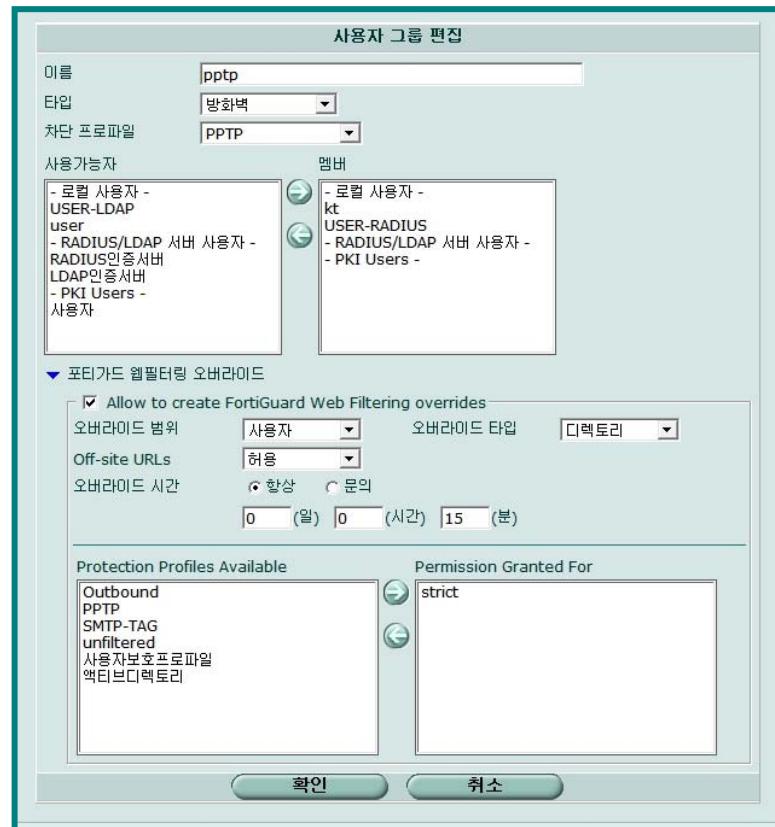
로컬 사용자 리스트를 설정된 타입의 멤버로 설정 후 보안정책에 적용하면 인증기능이 동작합니다.



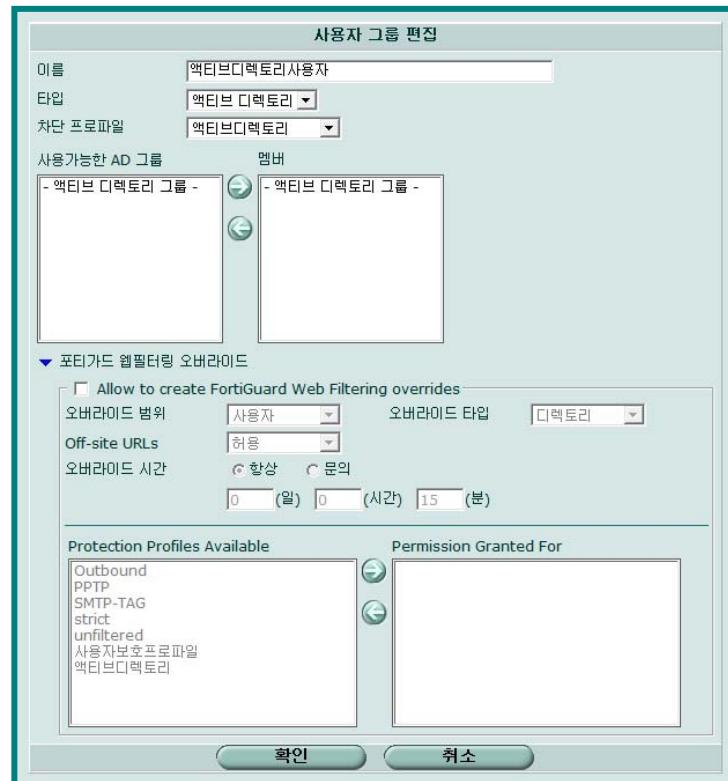
그룹명	멤버	차단 프로파일
▶ 방화벽		
pptp	kt, USER-RADIUS	PPTP
▶ 액티브 디렉토리		
액티브디렉토리사용자		액티브디렉토리
▶ SSL VPN		
SSL-USER	kt, user	

☞ 타입이 방화벽인 경우 PPTP, IPSEC, 및 각종 보안정책에 적용할 수 있으며 포티가드 웹필터링 오버라이드를 적용 할 수 있습니다.

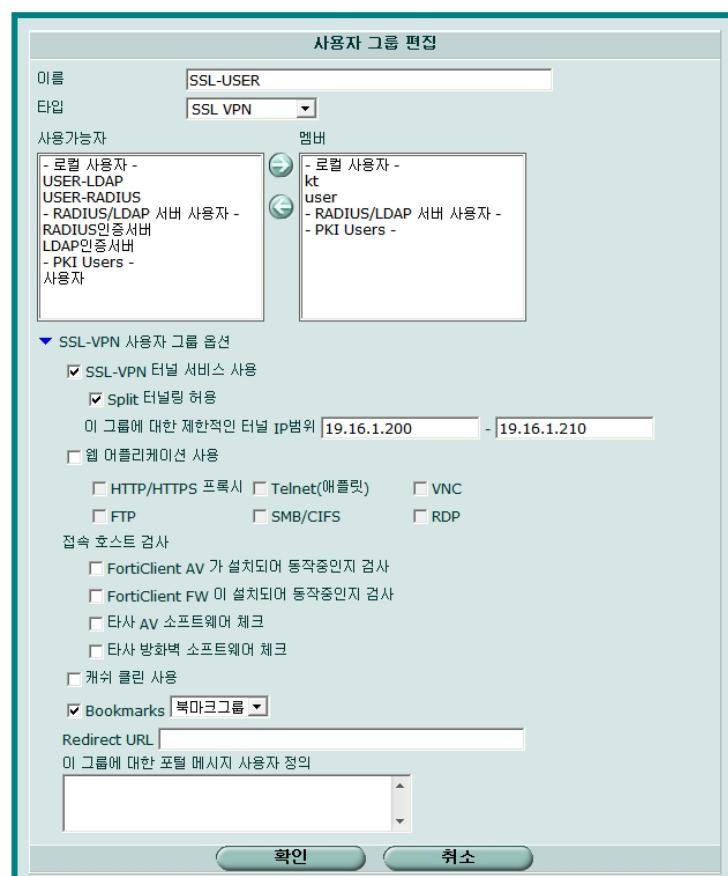
☞ 인증이 설정된 보안정책은 선택된 차단프로파일을 적용해야 하며 사용자 트래픽이 적용된 정책을 통과하기 전 인증 창이 표시됩니다.



- ☞ 탑이 액티브 디렉토리 인 경우  
AD 그룹이 멤버로 적용되어야 합니다.  
포티가드 웹필터링 오버라이드를  
적용 할 수 있습니다.



- ☞ 탑이 SSL VPN 인 경우 터널모드와  
웹응용프로그램 사용을 선택 할 수  
있습니다.  
Split 터널링을 사용시 HOST 에게  
할당할 IP 범위를 지정해야 합니다.



## 5-7 인증

◆ 사용자 인증을 적용 시 인증시간과 프로토콜에 적용 및 인증서방식을 선택 하는 기능입니다.



## 6

# 바이러스 탐지

- ◆ Fortigate의 바이러스 패턴정보제공 및 파일차단리스트를 설정하는 기능입니다.

포티가드 안티바이러스/안티스파이웨어 배포 서비스를 통해 최신의 패턴을 유지합니다.

최신의 바이러스패턴, 스파이웨어 리스트, 휴리스틱 탐지 엔진을 사용하며 모든 와일드 리스트 위협 및 수 천여의 OS, 응용프로그램 취약성으로부터 포괄적으로 보호 기능을 적용 할 수 있습니다.

의심되는 유해코드가 최신의 패턴정보에 있는 것인지 확인 하기 위해선 의심되는 파일을 Online Scan 웹사이트에서 Submission 하시기 바랍니다.

[http://www.fortiguardcenter.com/antivirus/virus\\_scanner.html](http://www.fortiguardcenter.com/antivirus/virus_scanner.html)

- ◆ 네트워크를 통해 유입되는 유해 코드를 완벽하게 차단하는 기술은 아래 예제 중 1번의 이유로 존재 할 수 없으며 Fortigate의 경우 다음과 같은 상황에 경우 바이러스나 유해코드를 내포한 컨텐츠를 그대로 통과 시킵니다.

1. 바이러스월이 암호화의 종단이 아닌채로 감염된 컨텐츠가 이미 암호화 된 상태로 통과하는 경우
2. 안티바이러스를 활성화한 보호프로파일이 설정되지 않은 보안정책을 이용한 트래픽의 경우
3. 안티바이러스 스캔 임계값 이상을 초과하는 파일이 Pass로 통과되는 경우
4. 12번 이상의 압축된 파일이 압축 해제 이후 안티바이러스 스캔 임계값 이상을 초과한 경우
5. 이메일의 조각메일 통과기능 사용시
6. 지정한 기본 Port를 변경하여 사용하면서 Fortigate의 프로토콜을 추가하지 않은 경우  
예) HTTP에서 8080을 사용하면서 Port를 추가하지 않아 TCP 80 만 계속 Scan 하는 경우
7. 최신 혹은 변종에 대한 패턴업데이트를 받지 못한 경우  
예) 라이센스 만료 및 네트워크오류로 인한 FDN 업데이트 서버 접속불가
8. Fortinet AV Lab 에서 패턴을 만들지 않은 경우
9. Fortigate가 Scan 을 하는 7가지 프로토콜 이외의 프로토콜로 통신하는 경우

- ◆ 일반적인 바이러스 감염 경로와 대응은 다음과 같이 대응을 할 수 있습니다.

1. CD, DVD, USB, Flash Memory 등의 전통적인 매체 감염
  - Host 기반의 고급형 백신 소프트웨어로 보안 및 치료
2. 방화벽 오픈 Port를 통한 감염
  - Network 기반의 바이러스월로 차단
3. 노트북, 무선, Mobile 단말기 등의 Backdoor를 통한 감염 및 웹브라우저를 통한 악성코드 감염
  - 사용자 Host 방화벽을 통한 보안정책 적용 및 안티스파이웨어 소프트웨어로 보안 및 치료

## 6-1 파일 패턴

◆ 등록된 파일 리스트를 차단 하는 기능으로 탐지기능이 동작하는 프로토콜에 대한 파일차단 및 안티바이러스 스캔 Bypass 기능을 수행합니다.

해당 목록은 방화벽>보호프로파일>안티바이러스>파일패턴 옵션에서 선택되어 탐지 활성화가 되어있는 경우만 적용 됩니다.

이름	# 엔트리	프로파일	주석
builtin-patterns	18	사용자보호프로파일	

☞ 차단리스트에서 확장명을 추가하여 차단리스트를 만들 수 있습니다.

조치가 차단인 경우 파일차단이 동작하며 조치가 허용인 경우 안티바이러스 스캔이 동작하지 않고 bypass 됩니다.

와일드카드 패턴을 지원하므로 순위의 적용 시 혼동되어선 안됩니다.

파턴	조치	사용	
*.bat	차단	<input type="checkbox"/>	
*.com	차단	<input checked="" type="checkbox"/>	
*.dll	차단	<input checked="" type="checkbox"/>	
*.doc	차단	<input type="checkbox"/>	
*.exe	차단	<input type="checkbox"/>	
*.gz	차단	<input type="checkbox"/>	
*.hta	차단	<input type="checkbox"/>	
*.ppt	차단	<input type="checkbox"/>	
*.rar	차단	<input type="checkbox"/>	
*.scr	차단	<input type="checkbox"/>	
*.tar	차단	<input type="checkbox"/>	
*.tgz	차단	<input type="checkbox"/>	
*.vb?	차단	<input type="checkbox"/>	
*.wps	차단	<input type="checkbox"/>	
*.xl?	차단	<input type="checkbox"/>	
*.zip	차단	<input type="checkbox"/>	
*.pif	차단	<input type="checkbox"/>	
*.cpl	차단	<input type="checkbox"/>	

## 6-2 격리

◆ 파일차단 및 바이러스로 탐지된 파일에 대하여 보관하는 기능입니다.

HDD가 장착된 모델이거나 FortiAnalyzer 가 연동된 경우만 사용이 가능합니다.

☞ 탐지된 파일이 격리설정에 의해 격리 폴더로 적용된 경우 해당 파일을 삭제하거나 다운로드를 하여 Forensic 에 이용할 수 있습니다.



☞ 격리 파일의 설정은 바이러스감염파일 및 의심되는 파일 및 차단설정된 파일에 대해 지원이 가능하지만 프로토콜에 따라 설정이 불가능 할 수 있습니다.

최대 격리 시간이 경과하면 자동으로 파일은 삭제되며 최대크기가 제한 값 이상인 경우 격리파일로 저장 할 수 없습니다.

## 6-3 구성

◆ 바이러스 탐지 리스트 alias에 대해 목록을 제공하여 그레이웨어 탐지 설정을 하는 기능입니다.

alias 는 McAfee, Symantec, Trend, Sophos 등의 전세계 백신 시장의 마켓쉐어가 큰 업체중 Fortinet 을 제외하고 가장 먼저 detect한 업체의 것을 표기하며 한국 Vendor 의 alias 는 포함되어 있지 않습니다. 따라서 alias 가 수십 개가 되더라도 그것을 모두 표기할 의무는 없으며 검색에서는 등록된 검색항목만 검색하므로 검색결과와 alias 는 무관하고 표기되는 목록은 패턴명칭으로 바이러스네임과 무관합니다.

WEB CONFIG		
시스템	바이러스 탐지 리스트	그레이웨어
라우터		
방화벽		
가상사설망		
사용자		
바이러스 탐지		
파일 패턴		
격리		
구성		
첨입 방지		
웹 필터		
안티스팸		
IM, P2P & VoIP		
로그&보고서		
0 - 9 A - F G - L M - R S - Z All		
A97M/Jet.A!exploit	A97M/JetEx.A!exploit	Ace.CP!tr.bdr
Ace.O!tr.bdr	AdClicker.B!tr	AdClicker.BW!tr
AdClicker.C!tr	AdClicker.D!tr	AdClicker.DB!tr
AdClicker.H!tr	AdClicker.I!tr	Adload.IK!tr
Adware	AFXrootkit!tr	AFXrootkit.B!tr
Agent.A!tr	Agent.AC!tr.spy	Agent.AK!tr.spy
Agent.AS!tr	Agent.AT!tr	Agent.AU!tr
Agent.BA!tr.spy	Agent.BC!tr.spy	Agent.BC!tr.spy!02
Agent.BC!tr.spy!04	Agent.BF!tr.spy	Agent.BH!tr.spy
Agent.CP!tr	Agent.CRV!tr	Agent.E!tr
Agent.Kl!tr.dldr	Agent.Nl!tr.dldr	Agent.O!tr.dldr
Agent.Rl!tr.dldr	Agent.Sl!tr.dldr	Agent.Vl!tr.dldr
Agent.Xl!tr.spy	Agent.Yl!tr.dldr	Alabama!tr
Allsum!tr	Aluigi!exploit	ANIfile!exploit
AntiCMOS.A	AntiCMOS_Family	AntiURL
APStrojan!tr	BackDoor.B!tr	BackDoor.BB!tr
BackDoor.BC!tr	BackDoor.BE!tr	Backdoor.BO2K.11
BackDoor.D!tr	BackDoor.DB!tr	BackDoor.F!tr
BackDoor.K!tr	BackDoor.L!tr	Backdoor.Netbus.170
BackDoor.Q!tr	Backdoor.Sub7.gen	BackDoor.T!tr
Backdoor/Sub7.gen	Baggle.C@mm	BagleDi.AG!tr
Baglet!spy	Baglet.F!tr	Bancos.ATH!tr
Bancos.AV!tr	Bancos.AVO!tr	Banker!tr.pws
Banker.AA!tr.pws	Banker.AD!tr.pws	Banker.AE!tr.pws
Banker.B!tr.pws	Banker.BA!tr.pws	Banker.BB!tr.pws
Banker.BF!tr.pws	Banker.BJ!tr.pws	Banker.C!tr.pws
Banker.D!tr.pws	Banker.DLD!tr	Banker.G!tr.pws
Banker.H!tr.pws	Banker.I!tr.pws	Banker.I!tr.pws!015
Banker.I!tr.pws!028	Banker.I!tr.pws!033	Banker.I!tr.pws!034
Banker.I!tr.pws!035	Banker.I!tr.pws!036	Banker.I!tr.pws!037
Banker.I!tr.pws!038	Banker.I!tr.pws!039	Banker.I!tr.pws!040
Banker.I!tr.pws!041	Banker.I!tr.pws!042	Banker.I!tr.pws!043
Banker.I!tr.pws!044	Banker.I!tr.pws!045	Banker.J!tr.pws
Banker.L!tr.pws	Banker.Q!tr.pws	Banloa.AMF!tr
BASH/Bind.A!exploit	BAT/Agent.MS!tr	BAT/AVkill.C!tr

☞ 확인된 바이러스에 대해 정확한 패턴을 확인 하기 위해서는 해당 사이트에 바이러스파일을 Fortinet 온라인 스캔 웹사이트에서 패턴을 확인 하시기 바랍니다.

[http://www.fortinet.com/FortiGuardCenter/virus\\_scanner.html](http://www.fortinet.com/FortiGuardCenter/virus_scanner.html)

해당 사이트는 유해코드로 의심되는 파일에 대해 Fortinet이 가장 최신의 패턴정보에 포함되어 있는지 여부를 확인 할 수 있으며 결과값을 가지고 있다면 Fortinet이 어떤 이름으로 차단하고 있는지 결과를 알려줄 것이고 패턴을 가지고 있지 않다면 clean으로 나옵니다.

타 백신에서만 차단되고 있는 경우 submit 페이지에 파일업로드를 하면 Fortinet AV팀이 분석 후 패턴을 추가할 것입니다.

☞ 그레이웨어는 20 여 Category 유해 응용프로그램에 대한 패턴을 제고합니다.

AV 패턴 업데이트시 함께 업데이트 되며 Category 항목의 활성화로 간단하게 적용 할 수 있습니다.



The screenshot shows the 'WEB CONFIG' interface of a Fortigate device. The left sidebar has a tree view with 'WEB CONFIG' selected. Under 'Virus Signature List', 'Category' is selected. The main pane displays a table of virus categories with checkboxes for 'Activation'. The categories listed are:

카테고리	활성
▶ Adware	<input checked="" type="checkbox"/>
▼ BHO	<input checked="" type="checkbox"/>
BHO/TEST_FILE	
▶ Dial	<input type="checkbox"/>
▶ Download	<input type="checkbox"/>
▶ Game	<input type="checkbox"/>
▶ HackerTool	<input type="checkbox"/>
▶ Hijacker	<input type="checkbox"/>
▶ Joke	<input type="checkbox"/>
▶ Keylog	<input type="checkbox"/>
▶ Misc	<input type="checkbox"/>
▶ NMT	<input type="checkbox"/>
▶ P2P	<input type="checkbox"/>
▶ Plugin	<input type="checkbox"/>
▶ RAT	<input type="checkbox"/>
▶ Spy	<input type="checkbox"/>
▼ Toolbar	<input type="checkbox"/>
Toolbar/Istbar	
Toolbar/SafetyBar	
ToolBar/SBSsoft.G	
ToolBar/Search	
Toolbar/TEST_FILE	

☞ Fortigate 의 바이러스 탐지는 FTP, HTTP, HTTPS, IM, IMAP, NNTP, POP3, SMTP 의 프로토콜만 지원하며 사용하는 TCP Port 는 기본 Port 만을 이용합니다.

HTTP Scan 의 경우 TCP 80만을 체크하며 TCP 8080을 체크하는 경우 Scan 이 되지 않습니다.

하지만 이러한 문제에 대응하기 위해 TCP Port를 추가 할 수 있습니다.

단, CLI 명령만 사용이 가능하며 Port 추가 시 시스템에 부하를 가져 올 수 있습니다.

#### ◆ Antivirus Service Configuration Command

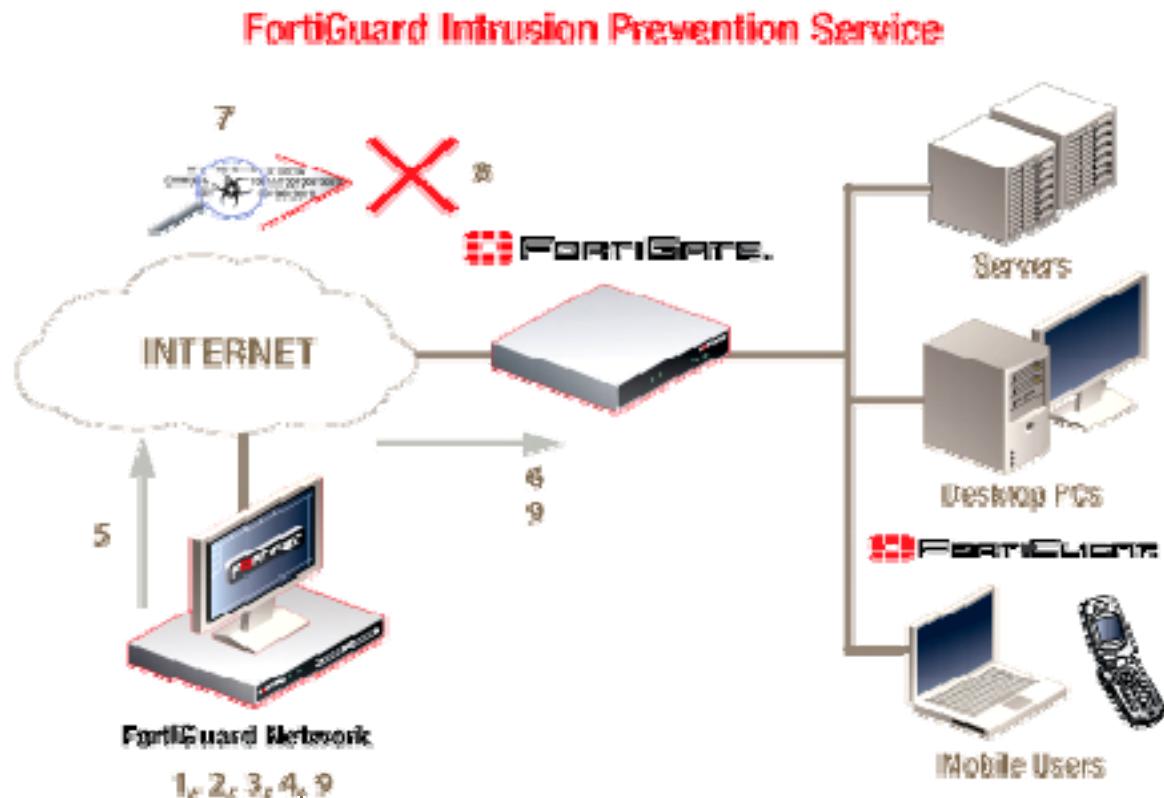
Fortigate # config antivirus service <port name>

Fortigate (port name) # set port <port no.>

Fortigate (port name) # end

## 7 침입 방지

- ◆ Fortigate 침입방지 시스템은 침입자의 공격 시그니처를 찾아 네트워크에 연결된 기기에서 수상한 침입 활동이 이뤄지는지를 감시하며, 정해진 설정에 따른 조치를 취함으로 유해 트래픽을 중단시키는 기능입니다.
- ◆ Fortigate는 침입방지 (IPS) 시스템은 과부하로부터 시스템을 보호하도록 설계 되어 있습니다. IPS FailOpen이라 부르는 이 기능은 IPS 동작 도중 시스템이 과부하를 받을 경우 IPS 기능을 잠시 멈춘 상태에서 트래픽을 통과 시키도록 되어 있습니다. 이 기능은 사이트의 특성 및 상황에 맞게 신중하게 사용되어야 하며 사용자가 동작방식을 정의 할 수 있습니다.
- ◆ 불법침입 이외의 서비스거부공격은 Anomaly 탐지 기능을 사용하여 정해진 임계 값 이상인 경우 정해진 조치를 취함으로 서비스거부공격에 대하여 보안을 이뤄 낼 수 있습니다.



## 7-1 시그니처

◆ 시그니처란 침입방지 기능을 수행할 때 트래픽분석 및 비교검색하기 위해 사용되는 패턴 리스트를 말하는 것으로 해당 항목에선 3700개 이상의 알려진 사전정의 Signature를 리스트에 대한 목록 제공 및 시그니처별 조치방법의 변경, 사용자 정의 패턴을 추가, 변형된 Protocol의 Decoder의 포트 변경 기능을 제공합니다.

시그니처는 Packet 의 Payload를 검사하므로 Payload가 작으면서 많은 데이터의 경우 (조각 파일 전송 응용프로그램, P2P, 메신저의 파일전송) IPS의 과부하를 유발하게 됩니다.

◆ 시그니처기반의 침입탐지 시스템은 완전한 컨텐츠 검사 CCI (Complete Content Inspection) 기술을 구현 할 수 없는 제품으로 DPI (Deep Packet Inspection) 기술만을 사용하여 Packet 단위의 Payload 내의 유해코드를 탐지하는 기술을 사용합니다.

이 경우 웜, 바이러스, 트로이목마 등의 유해코드를 정확하게 진단 해 낼 수 없으며 일부 유행하는 웜, 바이러스 등의 Foot Print 중에서 일부만 일치하면 해당 동일 패턴으로 간주하므로 오탐의 가능성을 항상 내재하고 있습니다.

## 7-1 #1 : 사전 정의

☞ 사전정의는 3700개 이상의 패턴에 대한 리스트를 확인 할 수 있으며 이름마다 해당 공격에 대한 설명페이지가 링크되어 있어 이름을 클릭하여 공격에 대한 설명을 볼 수 있습니다.

각 필드의 필터링을 통해 활성, 조치, 위험도, 적용되는 OS 및 프로토콜 항목에 대하여 별도로 설정 상태를 확인 할 수 있으며 위험도 레벨변경 및 조치상태 등 각종 설정을 변경 할 수 있습니다.

항목설정 기능을 통해 필드를 추가 및 제거 할 수 있습니다.

WEB CONFIG																																																																																																			
사전 정의																																																																																																			
사용자 정의																																																																																																			
프로토콜 디코더																																																																																																			
[ 1 / 70 ] [ 항목 설정 ] [ 모든 필터 지우기 ]																																																																																																			
<table border="1"> <thead> <tr> <th>이름</th> <th>활성</th> <th>로깅</th> <th>조치</th> <th>위험도</th> <th>Location</th> <th>프로토콜</th> <th>OS</th> <th>애플리케이션</th> <th>수정</th> </tr> </thead> <tbody> <tr> <td>2BGal.disp_album.php.SQL.Injection</td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td>통과</td> <td>낮음</td> <td>Server</td> <td>HTTP</td> <td>All</td> <td>PHP_app</td> <td></td> </tr> <tr> <td>3CDaemon.FTP.Server.Information.Disclosure</td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td>통과</td> <td>낮음</td> <td>Client</td> <td>FTP</td> <td>Windows</td> <td>Other</td> <td></td> </tr> <tr> <td>3COM.OfficeConnect.DoS</td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td>세션차단</td> <td>낮음</td> <td>Server</td> <td>HTTP</td> <td>Other</td> <td>Other</td> <td></td> </tr> <tr> <td>3COM.OfficeConnect.SoftReset</td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td>세션차단</td> <td>낮음</td> <td>Server</td> <td>HTTP</td> <td>Other</td> <td>Other</td> <td></td> </tr> <tr> <td>8Pixel.net.SimpleBlog.SQL.Injection</td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td>통과</td> <td>높음</td> <td>Server</td> <td>HTTP</td> <td>All</td> <td>Other</td> <td></td> </tr> <tr> <td>AA.bot.Botlist.File.Access</td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td>통과</td> <td>낮음</td> <td>Server</td> <td>HTTP</td> <td>Windows</td> <td>Other</td> <td></td> </tr> <tr> <td>Aardvark.Topsites.PHP.Arbitrary.Command.Execution</td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td>통과</td> <td>중간</td> <td>Server</td> <td>HTTP</td> <td>All</td> <td>PHP_app</td> <td></td> </tr> <tr> <td>Aardvark.Topsites.PHP.Remote.Command.Execution</td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td>통과</td> <td>중간</td> <td>Server</td> <td>HTTP</td> <td>All</td> <td>PHP_app</td> <td></td> </tr> </tbody> </table>										이름	활성	로깅	조치	위험도	Location	프로토콜	OS	애플리케이션	수정	2BGal.disp_album.php.SQL.Injection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	통과	낮음	Server	HTTP	All	PHP_app		3CDaemon.FTP.Server.Information.Disclosure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	통과	낮음	Client	FTP	Windows	Other		3COM.OfficeConnect.DoS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	세션차단	낮음	Server	HTTP	Other	Other		3COM.OfficeConnect.SoftReset	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	세션차단	낮음	Server	HTTP	Other	Other		8Pixel.net.SimpleBlog.SQL.Injection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	통과	높음	Server	HTTP	All	Other		AA.bot.Botlist.File.Access	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	통과	낮음	Server	HTTP	Windows	Other		Aardvark.Topsites.PHP.Arbitrary.Command.Execution	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	통과	중간	Server	HTTP	All	PHP_app		Aardvark.Topsites.PHP.Remote.Command.Execution	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	통과	중간	Server	HTTP	All	PHP_app	
이름	활성	로깅	조치	위험도	Location	프로토콜	OS	애플리케이션	수정																																																																																										
2BGal.disp_album.php.SQL.Injection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	통과	낮음	Server	HTTP	All	PHP_app																																																																																											
3CDaemon.FTP.Server.Information.Disclosure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	통과	낮음	Client	FTP	Windows	Other																																																																																											
3COM.OfficeConnect.DoS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	세션차단	낮음	Server	HTTP	Other	Other																																																																																											
3COM.OfficeConnect.SoftReset	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	세션차단	낮음	Server	HTTP	Other	Other																																																																																											
8Pixel.net.SimpleBlog.SQL.Injection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	통과	높음	Server	HTTP	All	Other																																																																																											
AA.bot.Botlist.File.Access	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	통과	낮음	Server	HTTP	Windows	Other																																																																																											
Aardvark.Topsites.PHP.Arbitrary.Command.Execution	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	통과	중간	Server	HTTP	All	PHP_app																																																																																											
Aardvark.Topsites.PHP.Remote.Command.Execution	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	통과	중간	Server	HTTP	All	PHP_app																																																																																											

## 7-1 #2 : 사용자 정의

☞ 사용자 정의는 사전정의 항목에 없는 패턴을 정의하여 탐지 패턴을 만드는 기능입니다.

확장 혹은 정교한 패턴의 제작을 위해서는 Perl Script 정규표현식을 사용 하여야 하며 상세 설정법은 FortiGate Intrusion Protection System Guide를 참조하시기 바랍니다.



☞ 상세 매뉴얼은 아래 링크페이지 및 기술문서를 참고 하시기 바랍니다.

[Fine tuning IPS predefined signatures for enhanced system performance](#)

[Tips for adding IPS custom signatures using the web-based manager](#)

[FortiGate Offline IPS Deployment](#)

[Using IPS to block HTTP POST, PUT and DELETE requests](#)

[Custom signature for streaming audio](#)

[IPS signatures in FortiOS 3.0 MR6](#)

## 7-1 #3 : 프로토콜 디코더

☞ 침입방지 기능을 수행할 때 사용하는 프로토콜을 해독하기 위한 기능입니다.

서비스하는 프로토콜을 변경하여 사용 시 원하는 침입방지 기능을 사용하기 위해선 프로토콜 디코더 포트번호를 수정 해야 침입방지 효과를 얻을 수 있습니다.



Protocols	Ports
Back Office	Auto
DCE RPC	135, 1026
DNS	53
FTP	21
H323	1720
HTTP	Auto
Instant Messaging	Auto
IMAP	143
LDAP	389
MSSQL	1433
NetBIOS	139, 445
Peer-to-Peer	Auto
POP3	110
Protocol (L3/4) Analyser	Auto
RADIUS	1812,1813
Sun RPC	111, 32771
SIP	5060
SMTP	25
SNMP	161, 162
SSH	Auto
TCP Reassembler	Auto
TFN DoS	Auto

☞ 디코더 항목의 port\_list 를 변경하는 경우 port 가 여러 개인 경우 콤마 (,)를 이용하여 설정 할 수 있습니다.

Port 가 Auto인 경우 수정이 불가능 하지만 TCP Reassembler 의 경우 TCP Flag 리스트를 이용하여 수정 및 추가 할 수 있습니다.



Edit Protocol Decoder Parameter

그룹 명칭	DCE RPC
port_list	<input type="text" value="135, 1026"/>

**확인**      **취소**

## 7-2 Anomaly

☞ Anomaly란 변칙적인 트래픽을 탐지하는 기능으로 프로토콜이 RFC와 같은 표준문서에 정의된 문법 규칙을 준수여부를 Packet Header에서 검사하여 Packet을 카운팅 하는 방식으로 체크합니다. 탐지 이벤트별 활성화, 조치, 위험도 레벨, 임계치 변경 등을 설정 할 수 있습니다.



The screenshot shows the 'WEB CONFIG' interface with the 'Anomaly' tab selected. On the left, there's a sidebar with various navigation options. The main area displays a table titled '위협도와 함께 트래픽 이상 보기' (View traffic anomalies with threat level) with the following data:

이름	활성화	로깅	조치	위험도
icmp_dst_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	통과	심각
icmp_flood	<input type="checkbox"/>	<input checked="" type="checkbox"/>	통과	심각
icmp_land	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	차단	심각
icmp_src_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	통과	심각
icmp_sweep	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	세션폐기	심각
ip_land	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	통과	심각
ip_loose_src_record_route	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	통과	중간
ip_record_route	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	통과	중간
ip_security_option	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	통과	중간
ip_stream_option	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	통과	중간
ip_strict_src_record_route	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	통과	중간
ip_timestamp_option	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	통과	중간
ip_unkn_option	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	통과	정보
large_icmp	<input type="checkbox"/>	<input checked="" type="checkbox"/>	통과	심각
ping_death	<input type="checkbox"/>	<input checked="" type="checkbox"/>	통과	심각
portscan	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	세션폐기	심각

☞ 이 기능을 이용하려면 네트워크 사용빈도분석 및 트래픽에 대한 심층 분석 이후 적용이 되어야 하며 네트워크 관리자, Fortigate 설치엔지니어와 충분한 협의와 검토를 한 이후 네트워크 규모에 맞게 Customizing이 이뤄져야 원하는 효과를 얻을 수 있습니다.  
설정되어 있는 임계치 이상의 경우 설정된 조치를 수행하며 위험도 레벨에 따라 보호프로파일에 적용된 임계치를 이상인 경우 바로 적용됩니다.



The screenshot shows the 'WEB CONFIG' interface with the 'Anomaly' tab selected. On the left, there's a sidebar with various navigation options. The main area displays a configuration form for '트래픽 이상 편집' (Traffic anomaly edit) with the following settings:

이름	icmp_flood
조치	통과
위험도	심각
임계치	250

At the bottom are '확인' (Confirm) and '취소' (Cancel) buttons.

☞ 상세 매뉴얼은 아래 링크페이지 및 기술문서를 참고 하시기 바랍니다.

### IPS anomaly thresholds

## 7-3 침입차단 조치

◆ 침입차단 기능의 조치방식은 OS 버전에 조치방식의 차이가 있습니다.

OS 3.0-MR6 이상의 버전에서는 단 3가지만의 조치를 지원하므로 절대 혼동이 없어야 합니다.

Action	Description
<b>Pass</b> <b>통과</b>	시그니처에 탐지된 Packet 에 대하여 Packet 을 조합하지 않고 통과 로깅 만 하는 경우 주로 사용
<b>Drop</b> <b>차단</b>	시그니처에 탐지된 Packet 에 대하여 Packet 을 조합하지 않고 차단 더 이상 세션이 증가하지 않아 IPS 의 부하가 줄어들게 됨
<b>Reset</b> <b>초기화</b>	TCP connections 에서만 적용이 되며 차단 후 서버와 클라이언트에게 Reset Packet 을 보낸 후 해당 세션테이블 제거
<b>Reset Client</b> <b>클라이언트 초기화</b>	TCP connections 에서만 적용이 되며 차단 후 클라이언트에게만 Reset Packet 을 보낸 후 해당 세션테이블 제거
<b>Reset Server</b> <b>서버 초기화</b>	TCP connections 에서만 적용이 되며 차단 후 서버에게만 Reset Packet 을 보낸 후 해당 세션테이블 제거
<b>Drop Session</b> <b>세션 차단</b>	시그니처에 탐지된 Packet 에 대하여 차단 후 동일세션의 모든 Packet 차단
<b>Pass Session</b> <b>세션 통과</b>	시그니처에 탐지된 Packet 에 대하여 이후 세션은 IPS 에서 Bypass 통과
<b>Clear Session</b> <b>세션 폐기</b>	시그니처에 탐지된 Packet 에 대하여 Reset Packet 을 보내지 않고 세션테이블 제거 서버와 클라이언트에서 차단된 것인지 확인 못하게 함 TCP connections 의 경우 차단되는 Packet 이 증가됨 UDP connections 의 경우 방화벽 레벨에서 즉시 새로운 세션이 만들어짐

## 8 웹 필터

- ◆ Local 구간의 사용자가 웹 브라우저를 통해 웹사이트 접근 시 금지단어, URL, 웹 패턴, 등 다양한 형태로 차단하는 기능으로 원하는 보안 정책에 맞는 웹 필터 목록을 적용 할 수 있습니다.
- 방화벽>보호프로파일 에 웹필터가 활성화가 되어 있어야 하며 설정된 보안정책에만 적용 됩니다.
- 패턴 리스트는 모델에 따라 최소 2개에서 최대 32,000 개, 패턴 엔트리 항목은 최소 1000개에서 최대 250,000개 까지 지원됩니다.

Models	File pattern lists per device	File pattern entries per device
<b>Fortigate 60 and below</b>	2	1,000
<b>Fortigate 60+ to 100A</b>	2	2,000
<b>Fortigate 200+ to 800</b>	4	32,000
<b>Fortigate 800+ to 3000</b>	25,000	50,000
<b>Fortigate 3000</b>	32,000	250,000

### 8-1 컨텐츠 필터

- ◆ 사용자가 웹 브라우저를 이용하여 인터넷을 이용하는 경우 금지단어가 포함된 페이지를 차단하거나 제외 하는 기능입니다.
- 등록된 단어는 HTML Source Script 로 변환되어 Match 되므로 사용자 화면에 보이지 않더라도 원본 소스에 포함되어 있다면 차단됩니다.
- 웹페이지 소스에서 주석 처리된 단어도 전부 체크되므로 설정 시 반드시 주의해야 합니다.
- 대부분의 포털 사이트처럼 한 페이지 내에 다른 웹페이지가 보이도록 링크된 페이지는 부분적으로 X 표시가 되는 형태로 열릴 수 있습니다.

## 8-1 #1 : 웹 콘텐츠 차단

☞ 금지단어를 이용하여 웹페이지를 차단하는 기능으로 적용할 리스트는 제한된 최대값만큼 추가할 수 있으며 적용된 프로파일과 엔트리 수가 표시됩니다.

리스트는 보호프로파일마다 별도 적용이 가능하며 각각의 보안정책에 적용이 가능합니다.

이름	# 엔트리	프로파일	주석
직원적용	2	사용자보호프로파일	직원전용
임원적용	1		임원전용

☞ 차단 단어는 7개국 언어가 지원되며 정확하게 동일한 경우 차단하는 와일드카드 패턴타입과 정해진 패턴을 인식하는 정규표현 패턴타입으로 등록 할 수 있습니다.

정규표현(Perl regular expressions)의 경우 잘못 적용한 경우 오탕 될 가능성이 매우 높으며 패턴의 언어에 따라 적용되지 않을 수 있습니다.

정규표현 문법 사용은 온라인헬프 및 링크된 웹페이지를 참조 하시기 바랍니다.

<http://perldoc.perl.org/perlretut.html>

엔트리 리스트에 활성화가 되어있지 않은 경우 적용 되지 않습니다.

파턴	패턴 타입	언어	점수
한게임	와일드카드	한국어	10
증권.*	정규 표현	한국어	10
게임+광고	정규 표현	한국어	10

## 8-1 #2 : 웹 콘텐츠 제외

☞ 웹 콘텐츠 차단 리스트 중에서 제외처리를 하는 기능입니다.

적용할 리스트는 제한된 최대값만큼 추가할 수 있으며 적용된 프로파일과 엔트리 수가 표시됩니다.

리스트는 보호프로파일마다 별도 적용이 가능하며 각각의 보안정책에 적용이 가능합니다.

이름	# 엔트리	프로파일	주석
웹콘텐츠제외	1	사용자보호프로파일	

☞ 차단단어에 <네이★>로 등록한 경우 [www.naver.com](http://www.naver.com)은 차단되지만 <검색어>란 단어를 제외 항목에 등록한 경우 [www.naver.com](http://www.naver.com) 내에 <검색어>란 단어가 포함되어 있으므로 페이지가 열리게 됩니다.

하지만 <http://section.blog.naver.com>의 경우 차단됩니다.

이처럼 차단단어를 포함한 페이지에서 제외단어로 설정 할 수 있습니다.

패턴	패턴 타입	언어
한국증권	와일드카드	한국어
검색어	와일드카드	한국어

## 8-2 URL 필터

◆ 사용자가 웹 브라우저를 이용하여 인터넷을 이용하는 경우 설정된 URL 을 확인하여 페이지를 차단하는 기능으로 차단, 허용, 예외 리스트를 하나의 리스트목록에서 관리 및 설정 할 수 있습니다.

☞ 적용할 리스트는 제한된 최대값만큼 추가할 수 있으며 적용된 프로파일과 엔트리 수가 표시됩니다. 리스트는 보호프로파일마다 별도 적용이 가능하며 각각의 보안정책에 적용이 가능합니다.



The screenshot shows the Fortinet Web Config interface under the 'WEB CONFIG' tab. On the left sidebar, 'URL 필터' (URL Filter) is selected. The main window displays the 'URL 필터' configuration page with a table titled '새로생성' (New Creation). The table has columns for '이름' (Name), '# 엔트리' (Number of Entries), '프로파일' (Profile), and '주석' (Comment). Two entries are listed: '차단사이트' (Block Site) with 821 entries and '게임사이트' (Game Site) with 1 entry. The '프로파일' column shows '사용자보호프로파일' (User Protection Profile) for the first entry and '전산팀적용' (Applied by IT Department) for the second. The '주석' column contains icons for edit and delete.

☞ 차단하고자 하는 URL 주소를 입력하면 해당 URL을 차단합니다.  
등록된 항목과 정확하게 동일한 경우 차단하는 간결타입과 정해진 패턴을 인식하는 정규표현 타입이 지원됩니다.  
정규표현으로 막은 URL에서 간결로 등록한 URL을 예외처리하기 위해선 허용항목이 차단항목보다 상위에 위치해야 합니다.  
이동 설정을 이용하지 않고 Drag & Drop으로도 엔트리 항목의 순위를 변경 할 수 있습니다.



The screenshot shows the Fortinet Web Config interface under the 'WEB CONFIG' tab. On the left sidebar, 'URL 필터' (URL Filter) is selected. The main window displays the 'URL 필터' configuration page with a table titled '새로생성' (New Creation). The table has columns for 'URL', '조치' (Action), and '타입' (Type). A search bar at the top left shows '차단사이트' (Block Site) and a dropdown menu shows '전작원적용' (Applied by IT Department). The table lists various URLs with their corresponding actions and types. Most entries are '차단' (Block) with '간결' (Simple) type, except for a few like 'game.auction.co.kr' which is '허용' (Allow) with '정규표현' (Regular Expression) type.

☞ 조치항목은 다음 3가지 방식을 지원합니다.

- 1) 차단 <block> – 즉시 차단
- 2) 예외 <exempt> – 무조건 AV Scan 을 하지 않고 무조건 통과
- 3) 허용 <allow> – 보호프로파일의 HTTP에 안티바이러스 사용시 바이러스 Scan 이후 통과

## 8-3 FortiGuard - Web 필터

◆ FortiGuard 웹필터 서비스 이용 시 사용자 정의 항목을 우선처리 하도록 하는 기능입니다.

## 8-2 #1 : 오버라이드

☞ FortiGuard 웹필터의 Category 리스트에 포함된 항목 및 등록된 디렉토리 혹은 도메인이 탐지된 경우 인증페이지가 나타나며 사용자, 사용자 그룹, IP, 보호프로파일 별 적용 기능과 설정한 시간을 기준으로 만기 기간을 적용 할 수 있습니다.



The screenshot shows the 'WEB CONFIG' interface under the 'Web Filter' section. The 'Overwrite' tab is selected. A table lists an item with ID 1, URL 'www.naver.com', category 'Web Filter Overwrite Group', and created by 'admin' on 'Tue Jul 15 23:04:20 2008'. There are edit and delete icons for each row.

#	URL/별주	점수	Off-site URLs	개시자	만기일
1	www.naver.com	웹필터오버라이드그룹		admin	Tue Jul 15 23:04:20 2008



The screenshot shows the 'WEB CONFIG' interface under the 'Web Filter' section. The 'Overwrite' tab is selected. A configuration dialog for an override entry is open. It shows the URL 'naver.com' and specifies the 'User Group' as 'Web Filter Overwrite Group'. The 'Off-site URLs' dropdown is set to '허용' (Allow). The 'Overwrite' duration is set to 1 day, 0 hours, and 0 minutes. The 'Expiration Date' is 'Tue Jul 15 23:04:20 2008'. At the bottom are '확인' (Confirm) and '취소' (Cancel) buttons.

## 8-2 #2 : 로컬분류

☞ FortiGuard 웹필터의 Category 리스트를 생성할 수 있으며 로컬레이팅에 적용 할 수 있습니다.



The screenshot shows the 'WEB CONFIG' interface under the 'Local Category' tab. On the left sidebar, 'Web Filter' is selected. The main area displays a table with two entries:

#	URL	Category
1	gw.kt.com	사용자필터
2	p2p.net	PP 파일공유...

## 8-2 #3 : 로컬 랜이팅

☞ FortiGuard 웹필터의 Category 리스트에 포함할 항목을 정의 할 수 있습니다.

설정된 도메인은 속해있는 FortiGuard 웹필터의 Category 적용시 바로 적용됩니다.



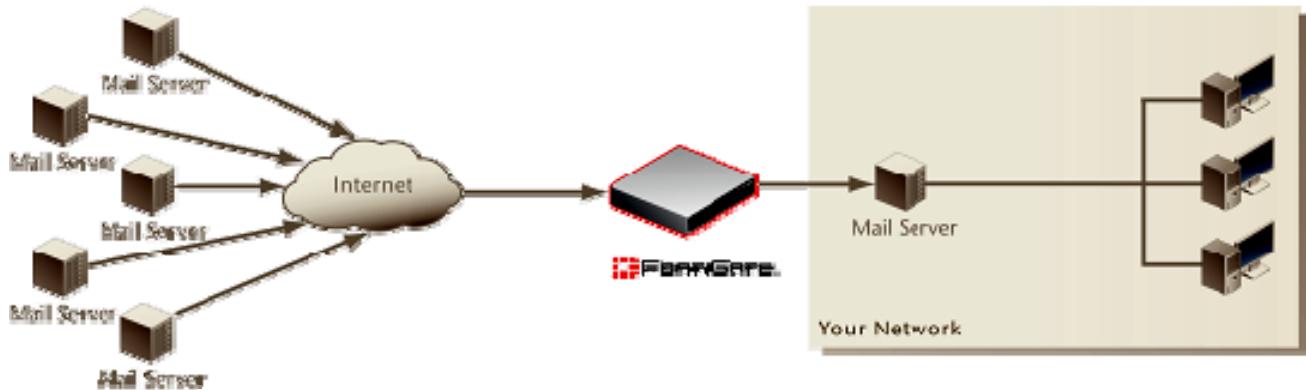
The screenshot shows the 'WEB CONFIG' interface under the 'Local Rating' tab. On the left sidebar, 'Web Filter' is selected. The main area displays a table with two entries:

#	URL	Category
1	gw.kt.com	사용자필터
2	p2p.net	PP 파일공유...

## 9

## 안티스팸

- ◆ E-mail 전송 프로토콜인 IMAP, SMTP, POP3에 대하여 사용자가 지정한 금지단어, IP, E-mail 등을 이용하여 복합적으로 SPAM mail을 차단 하는 기능입니다.



- ◆ POP3(메일 가져오기 프로토콜)는 메일서버에 도착한 메일을 사용자가 가져갈 때 체크되므로 태깅만 가능하며 SMTP(메일 보내기 프로토콜)는 메일서버에 도착하기 이전 체크되므로 태깅과 차단이 가능합니다.

PROTPCOL	Email Address	Banned Word
SMTP	Block	Block or Replace
POP3	Subject Tag	Replace
IMAP	Subject Tag	Replace
HTTP	Not Applicable (N/A)	Not Applicable (N/A)

- ◆ SPAM 차단 여부에 대한 문의가 오면 먼저 해당 사이트에 접속하여 해당 도메인이 등록되어 있는지 검색하십시오. (해당 기능은 RBL 서버에서도 동일하게 적용 됩니다.)

<http://www.fortiguardcenter.com/antispam/antispam.html>

Black list 는 SPAM 메일을 대량으로 보내는 것으로 확인되어 사이트에 등재된 것으로 삭제해 달라고 요청하면 Fortinet 뿐만 아니라 어떤 Spammer DB 업체도 그냥 지워주지 않습니다.

해당 사이트가 SPAM 을 대량으로 보내지 않는다는 것이 확인되어야만 삭제가 가능합니다.

따라서 삭제 process 는 고객이 직접 모든 차단 DB 사이트에서 해야 하는 것이지 누구도 대행할 수 없습니다만 등록되어 있더라도 해당 메일을 Whitelist 에 추가하여 검사하지 않고 통과 시키는 방법을 이용할 수 있습니다.

◆ SMTP 의 SPAM 여부 체크의 순위는 다음과 같습니다.

1. IP 주소 Black & White 리스트 (On Last Hop IP)
2. DNSBL & ORDBL, FortiGuard 안티스팸 중 IP 리스트(On Last Hop IP), HELO DNS Lookup
3. MIME headers, E-mail 주소 Black & White 리스트
4. E-mail 제목의 금지단어
5. headers 에 “Received” 가 있는 IP 주소 Black & White 리스트
6. E-mail 본문의 금지단어
7. 반송 E-mail DNS, FortiGuard 안티스팸, DNSBL (IP Header 가 공인 IP 인 경우)

◆ POP3 의 SPAM 여부 체크의 순위는 다음과 같습니다.

1. MIME headers, E-mail 주소 Black & White 리스트
2. E-mail 제목의 금지단어
3. IP 주소 Black & White 리스트
4. E-mail 본문의 금지단어
5. 반송 E-mail DNS, FortiGuard 안티스팸, DNSBL & ORDBL

◆ 이전 버전에서 지원하던 DNSBL/ORDBL 설정은 CLI 에서만 가능합니다.

DNSBL의 적용은 Query 질의가 일반적인 DNS Query 처럼 동작하는 RBL 서버만 적용이 가능합니다. SPAMhaus.org 같은 경우 적용이 가능하지만 ‘한국정보보호진흥원’에서 제공하는 SPAMlist.or.kr 처럼 <% nslookup 121.113.22.15.SPAMlist.or.kr> 같은 역순의 쿼리 및 zone 파일 형태로 제공하는 RBL 서버는 이용이 불가능 합니다.

DNSBL 서버를 2개 이상 적용 할 경우 두 곳에 동시에 Query 하여 먼저 얻은 결과에 따라 동작하게 되므로 경우에 따라 SPAM으로 차단 되었다가 안되었다가 하는 현상이 반복적으로 나타나게 됩니다. DSNBL 의 사용시 1개만 적용하는 것을 권장하며 제공서버가 탐지하는 동작 알고리즘을 반드시 확인 후 설정 하시기 바랍니다.

◆ 탐지율은 다음과 같습니다.

FortiMail (95~99%) > FortiGuard AS 3.0(90%~98%) > FortiGuard AS 2.80 (88%~95%) >  
RBL (~80% with high false positive)

FortiGuard AS를 구매한 고객이라면 반드시 FortiOS v3.0 MR3 이상의 버전을 사용해야만 탐지율의 정확도가 상승하며 탐지속도가 빨라집니다.

최근 많이 유입되는 wrote:, it's 와 이미지로 들어오는 주식투자 Trade 등은 이메일 checksum 에서 차단되는데 이 기능은 FortiOS 3.0을 사용해야만 활성화 됩니다.

즉 DNSBL 같은 무료로 제공되는 서비스의 경우 FortiGuard AS 에 비교하여 오탐이 많고 탐지 기법 자체가 다르므로 많은 신뢰도를 기대하기 어렵습니다.

강력한 차단기능을 원하는 경우 FortiGuard AS 혹은 FortiMail 어플라이언스의 이용을 권장합니다.

## 9-1 차단단어

◆ 등록된 단어가 포함된 경우 SPAM 처리를 하는 기능입니다.

적용할 리스트는 제한된 최대값만큼 추가할 수 있으며 적용된 프로파일과 엔트리 수가 표시됩니다.

리스트는 보호프로파일마다 별도 적용이 가능하며 각각의 보안정책에 적용이 가능합니다.

이름	# 엔트리	프로파일	주석
스팸단어	1660	사용자보호프로파일	

☞ 차단 단어는 7개국 언어가 지원되며

와일드카드, 정규표현식 패턴이 지원됩니다.

등록된 단어의 체크 위치는  
제목, 본문, 혹은 전부 체크로  
선택이 가능합니다.

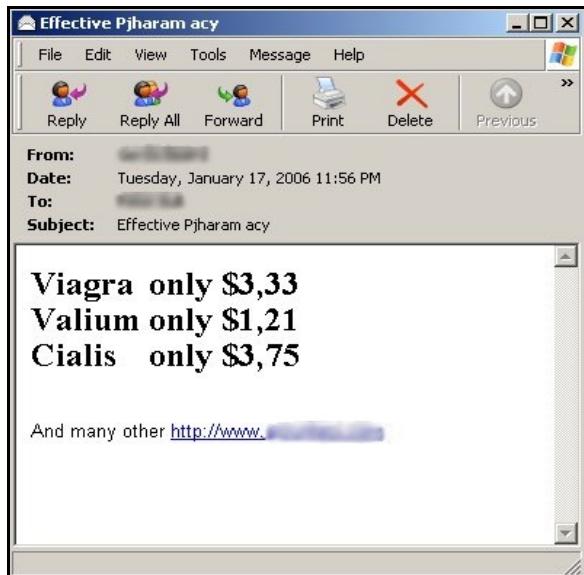
패턴	패턴유형	언어	위치	점수
에바스11종	와일드카드	한국어	제목	10
교통사고	와일드카드	한국어	제목	10
현금게임사이트	와일드카드	한국어	제목	10
시계의	와일드카드	한국어	제목	10
안전운전	와일드카드	한국어	제목	10
굿아도	와일드카드	한국어	제목	10
대출금리로	와일드카드	한국어	제목	10
보건복지부	와일드카드	한국어	제목	10
최신PDA스윙폰	와일드카드	한국어	제목	10
안전대출서비스	와일드카드	한국어	제목	10
핸드폰처럼	와일드카드	한국어	제목	10
shop	와일드카드	영어	전체	10
tail-now\.com	표현정규식	영어	본문	10
\.ce\.\ro	표현정규식	영어	본문	10
123zontheweb\.info	표현정규식	영어	본문	10
sites-only-for-you\.info	표현정규식	영어	본문	10
hankukloan\.net	표현정규식	영어	본문	10

## 9-1 #1 : 차단단어가 통과 되는 사례

☞ 차단단어를 이용한 SPAM 체크 사용시 Outlook 등의 HTML로 Display 되는 경우 Fortigate 는 Source Script를 분석하므로 원하지 않는 Bypass로 처리되거나 차단, 태깅 이 될 수 있습니다.

예를 들어 금지단어에 Viagra, Valium, Cialis 세단어가 등록 되어 있습니다.

수신 메일을 그림과 같이 Outlook 나 HTML로 Display 되면서 금지단어로 등록한 단어가 SPAM 조치 되지 않고 정상메일로 Bypass 되었습니다.



```
<STYLE></STYLE>
</HEAD>
<BODY bgColor="#FFFFFF">
<DIV style = "FLOAT
: left ; "><H2>Via<BR>Val<BR>
Cia<BR></H2></DIV>
<DIV style = " FLOAT
:
left
: "><H2>gra<BR>iun <BR>lis<BR>
</H2></DIV>
<DIV style = "
FLOAT
: left ;
"><H2>only<BR>only<BR>only <BR></H2></DIV>
```

하지만 실제 원본 소스를 보면 단어들이 반절씩 쪼개져 있습니다.

굵은 검정색 글씨가 순차적으로 조합되어 HTML로 변환되면서 사용자에게 보여지기 때문에 이런 SPAM 메일은 탐지 할 수 없습니다.

## 9-1 #2 : 차단단어를 등록하는 패턴 예제

☞ 최근의 Spammer 들은 점점 지능화 되고 강력한 SPAM Mail Send 기술을 이용합니다.

HTML 구문을 이용한 변칙적인 단어조합, JavaScript 나 그림파일 첨부를 통한 ANTI-SPAM 솔루션을 우회 합니다.

HTML 구문설정 기법들로 발송하는 메일을 탐지하기 위해선 차단단어를 이용할 경우 여러 가지 조합으로 대응해야 합니다.

아래 예제를 참고로 차단단어를 설정 하시기 바랍니다.

영어 이외의 언어로 설정한 경우 적용이 되지 않을 수 있습니다.

Wildcard	Matched pattern	Unmatched pattern
forti*	fortinet, forticare, fortification	fort
?ort	fort, port	sport

Regular expression	Matched pattern	Unmatched pattern
forti*	fortii, fortiii	fortiice
go*gle	google, goooogle	Goggle
go.gle	google, goggle	go-ogle
goo.*	google, goo goo dolls	goggle
google\..*	google.com, google.news	googles, googled
google/i	GOOGLE, Google, GooGLE	

## 9-2 블랙 / 화이트목록

◆ SPAM 탐지 시 IP, 이메일주소를 탐지하여 차단 혹은 예외처리 하는 기능입니다.

블랙리스트는 SPAM 리스트, 화이트리스트는 스팸예외 리스트 입니다.

적용할 리스트는 제한된 최대값만큼 추가할 수 있으며 적용된 프로파일과 엔트리 수가 표시됩니다.

리스트는 보호프로파일마다 별도 적용이 가능하며 각각의 보안정책에 적용이 가능합니다.

The screenshot shows the 'WEB CONFIG' interface with the 'IP 주소' tab selected. On the left, a sidebar lists various configuration categories under 'WEB CONFIG'. The 'Black/White List' option is highlighted. The main panel displays a table titled '새로생성' (New Creation) for IP addresses. The table has columns for '이름' (Name), '# 엔트리' (Entry Count), '프로파일' (Profile), and '주석' (Comment). One entry is listed: 'IP리스트' with '# 엔트리' 840, '프로파일' set to '사용자보호프로파일', and '주석' empty. A pencil icon is at the bottom right of the table.

This screenshot shows the same 'WEB CONFIG' interface, but the '이메일 주소' tab is selected instead of 'IP 주소'. The sidebar and table structure are identical to the previous screenshot, but the table data reflects email addresses. One entry is listed: '메일주소' with '# 엔트리' 1098, '프로파일' set to '사용자보호프로파일', and '주석' empty. A pencil icon is at the bottom right of the table.

## 9-2 #1 : IP 주소

☞ SPAM 탐지 시 IP를 이용하여 탐지하는 기능으로 주소의 등록은 단일IP 및 네트워크단위로 설정할 수 있습니다.

SPAM 예외 조치를 하기 위해선 SPAM으로 조치되는 항목보다 우선순위에 위치해야 합니다.

	IP/넷마스크	조치	
<input checked="" type="checkbox"/>	125.188.11.234	스팸아님	
<input checked="" type="checkbox"/>	150.150.103.88	차단	
<input checked="" type="checkbox"/>	210.114.168.161	스팸	
<input checked="" type="checkbox"/>	210.180.123.3	스팸	
<input checked="" type="checkbox"/>	210.180.123.4	스팸	
<input checked="" type="checkbox"/>	210.207.128.0/24	스팸	
<input checked="" type="checkbox"/>	210.213.138.0/24	스팸	
<input checked="" type="checkbox"/>	210.213.139.0/24	스팸	
<input checked="" type="checkbox"/>	210.213.140.0/24	스팸	
<input checked="" type="checkbox"/>	210.213.141.0/24	스팸	
<input checked="" type="checkbox"/>	210.213.142.0/24	스팸	
<input checked="" type="checkbox"/>	210.213.143.0/24	스팸	
<input checked="" type="checkbox"/>	210.213.144.0/24	스팸	
<input checked="" type="checkbox"/>	210.213.145.0/24	스팸	

☞ 조치항목은 다음 3가지 방식을 지원합니다.

- 1) 스팸으로 표시 <Mark as Spam> – 보호프로파일에 적용된 상태로 조치 <폐기, 태깅>
- 2) 스팸아님으로 표시 <Mark as Clear> – 스팸필터 체크 제외
- 3) 차단으로 표시 <Mark as Reject> – 세션 차단 <SMTP 만 적용되며 로그에 남지 않음>

## 9-2 #2 : 이메일 주소

☞ SPAM 탐지 시 이메일주소를 이용하여 탐지하는 기능으로 주소의 등록은 단일IP 및 네트워크단위로 설정할 수 있습니다.

등록 패턴은 와일드

SPAM 예외 조치를 하기 위해선 SPAM으로 조치되는 항목보다 우선순위에 위치해야 합니다.

	이메일 주소	패턴유형	조치
<input checked="" type="checkbox"/>	@daum.net	와일드카드	스팸
<input checked="" type="checkbox"/>	kt@daum.net	와일드카드	스팸아님
<input checked="" type="checkbox"/>	^-_a	정규표현식	스팸
<input checked="" type="checkbox"/>	^cqrto002@	정규표현식	스팸
<input checked="" type="checkbox"/>	^kkddkdd@	정규표현식	스팸
<input checked="" type="checkbox"/>	^lsong\d\d@	정규표현식	스팸
<input checked="" type="checkbox"/>	^lsong[1-9]@	정규표현식	스팸
<input checked="" type="checkbox"/>	^song\d\d@	정규표현식	스팸
<input checked="" type="checkbox"/>	^song[1-9]@	정규표현식	스팸
<input checked="" type="checkbox"/>	^long\d\d@	정규표현식	스팸
<input checked="" type="checkbox"/>	^long[1-9]@	정규표현식	스팸
<input checked="" type="checkbox"/>	^ong\d\d@	정규표현식	스팸
<input checked="" type="checkbox"/>	^ong[1-9]@	정규표현식	스팸
<input checked="" type="checkbox"/>	^originalbrain	정규표현식	스팸
<input checked="" type="checkbox"/>	^iku754k	정규표현식	스팸
<input checked="" type="checkbox"/>	^iku7548k	정규표현식	스팸

☞ 조치항목은 다음 2가지 방식을 지원합니다.

- 1) 스팸으로 표시 <Mark as Spam> – 보호프로파일에 적용된 상태로 조치 <폐기, 태깅>
- 2) 스팸아님으로 표시 <Mark as Clear> – 스팸필터 체크 제외

☞ 정확하게 동일한 경우 차단하는 와일드카드 패턴과 정해진 패턴을 인식하는 정규표현식 패턴으로 등록 할 수 있습니다.

엔트리 리스트에 활성화가 되어있지 않은 경우 적용 되지 않습니다.

## 10 IM, P2P & VoIP

◆ 인터넷 메신저, P2P, VoIP 의 통계정보를 표시하거나 인터넷 메신저의 사용자 계정에 대한 제한 설정을 하는 기능입니다.

해당 기능을 사용하기 위해선 방화벽>보호프로파일>IM/P2P 의 활성화가 되어 있어야 합니다.

### 10-1 통계

◆ 인터넷 메신저 별 상세통계정보 및 프로토콜 별 통계 정보를 표시해 주는 기능으로 활성화된 내용에 대해서만 통계 정보를 확인 할 수 있습니다.

### 10-1 #1 : 통계

☞ 보호프로파일에 제한 설정이 적용되어 있는 경우 세부 통계정보를 확인 할 수 있습니다.

메신저 사용자의 통계 정보, P2P 사용 통계 정보, VoIP 사용 통계정보를 상세히 볼 수 있으며 초기화하여 일정 시점부터 새로 갱신하여 확인 할 수 있습니다.

WEB CONFIG							
		통계	프로토콜				
		자동 새고침 간격	none	새로고침	사용량: 2008-06-23 00:15:21		
사용자		메신저 사용		MSN	Yahoo!	AIM	ICQ
		현재 사용자		1	0	0	0
		마지막 초기화 이후		3	0	0	0
		차단됨		6	0	0	0
채팅		전체 채팅 세션		1	0	0	0
		전체 메시지		3	0	0	0
파일 전송		마지막 초기화 이후		0	0	0	0
		차단됨		0	0	0	0
음성 채팅		마지막 초기화 이후		0	0	0	0
		차단됨		0	0	0	0
P2P 사용		BitTorrent		eDonkey	Gnutella	KaZaa	WinNY
P2P 사용		전체 바이트	858.52 KB	0.00 B	0.00 B	0.00 B	0.00 B
		평균 대역폭	1.67 KB/s	0.00 B/s	0.00 B/s	0.00 B/s	0.00 B/s
VoIP 사용					SIP	SCCP	
세션		활성화 세션(연결된 전화, etc)			0	0	
		음성 콜			0	0	
		전체 콜 (마지막 리셋 이후)			0	0	
		콜 실패/드롭			0	0	
		콜 성공			0	0	

## 10-1 #2 : 프로토콜

☞ 오른쪽 상단의 프로토콜을 선택하여 각 메신저 별 상세 통계정보를 확인 할 수 있습니다.

통계 탭의 통계초기화 시 프로토콜의 정보도 초기화 됩니다.

사용자	
현재 사용자	1
마지막 초기화 이후	3
차단됨	6

채팅	
전체 채팅 세션	1
서버 기반 채팅	1
그룹 채팅	0
직접/사적인 채팅	0

메시지	
전체 메시지	3
보냄	1
받음	2

파일 전송	
마지막 초기화 이후	0
보냄	0
받음	0
차단됨	0

음성 채팅	
마지막 초기화 이후	0
차단됨	0

## 10-2 사용자

- ◆ 인터넷 메신저의 사용자 계정을 제어하는 기능입니다.

### 10-2 #1 : 현재 사용자

☞ 현재 로그인하여 메신저를 사용중인 사용자 계정과 IP 그리고 로그인 시간이 표시되며 차단 버튼을 누르면 사용자 목록의 차단 사용자로 적용되면서 실시간으로 차단됩니다.

#	프로토콜	사용자명	사용자 IP	마지막 로그인	차단
1	MSN	com@hotmail.com	19.16.1.2	2008-07-16 08:07:42	<b>차단</b>

## 10-2 #2 : 사용자 목록

☞ 메신저 사용자 계정의 사용자 정책 상태를 표시해 줍니다.

허용으로 되어있는 사용자라도 방화벽>보호프로파일>IM/P2P 의 로그인 차단이 설정되어 있는 경우 사용자를 로그인 이 차단 됩니다.

**사용자 설정보다 보호프로파일의 제한이 우선적으로 적용됩니다.**



The screenshot shows the 'User List' tab selected in the 'WEB CONFIG' interface. On the left, there's a sidebar with various security modules: 시스템, 라우터, 방화벽, 가상사설망, 사용자, 바이러스 감지, 첨입 방지, 웹 필터, 앤티스팸, IM, P2P & VoIP (which is expanded), 통계, 사용자, and 로그&보고서. The main panel has tabs for '현재 사용자', '사용자 목록' (selected), and '설정'. A '새로생성' (New) button is visible. Below it, there are dropdown menus for '프로토콜' (All) and '정책' (전체). A table lists users with their email addresses and policies: MSN (com@hotmail.com, 허용), MSN (mahoto@hotmail.com, 차단). Each row has edit and delete icons.

프로토콜	사용자명	정책
MSN	com@hotmail.com	허용
MSN	mahoto@hotmail.com	차단

## 10-2 #3 : 설정

☞ 메신저 사용자 계정에 대한 기본 설정을 하는 기능으로 기본은 자동차단입니다.

방화벽>보호프로파일>IM/P2P 의 기능이 활성화 되어 있는 경우 사용자정책에 따라 적용됩니다.

기본 사용자 정책은 자동 차단이며 자동 차단된 리스트는 임시사용자 목록에 표시됩니다.



	MSN	Yahoo!	AIM	ICQ
자동 허용	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
자동 차단	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>

#	프로토콜	사용자명	정책	적용
1	MSN	com@hotmail.com	차단	영구 허용 영구 차단

☞ 자동허용으로 되어 있다면 임시 사용자 목록에 허용으로 표시됩니다.



	MSN	Yahoo!	AIM	ICQ
자동 허용	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
자동 차단	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>

#	프로토콜	사용자명	정책	적용
1	MSN	com@hotmail.com	허용	영구 허용 영구 차단

☞ 영구허용, 영구차단을 클릭하면 사용자 목록으로 이동됩니다.

사용자 정책 및 설정보다 보호프로파일의 제한이 우선적으로 적용됩니다.

## 11 로그 & 보고서

- ◆ 각종 로그 보기, 로그설정 관련 기능입니다.

기능별 로깅은 보호프로파일이 로그설정이 반드시 되어 있어야만 하며 해당보호 프로파일이 적용되어 있고 활성화 중인 보안정책에 대한 로그만 로깅됩니다.

트래픽로그의 경우 보안 정책에 트래픽로깅이 활성화가 되어 있어야만 정상적으로 로깅이 됩니다.

- ◆ 이벤트, 공격탐지, 안티바이러스, 웹차단, 안티스팸, IM/P2P/ VoIP 관련 로그가 제공되며 장기간 로그저장, 보고서, 트래픽로그, 컨텐츠기록을 이용하기 위해선 FortiAnalyzer를 이용하거나 Syslog, FortiGuard Snalysis Service를 이용해야 합니다.
  - ◆ FortiAnalyzer는 Fortinet 제품들에 대한 전용 로그분석 시스템으로 1대의 장비에 Fortigate 제품을 최대 10대까지 연동 가능하며 상위모델 일수록 더 많은 제품을 연결 할 수 있습니다.
- FortiAnalyzer를 연동한 경우 Fortigate에서 더욱 많은 내용과 보고서를 제공 받을 수 있습니다.



The screenshot shows the FortiAnalyzer 100A Web Configuration interface. The left sidebar has a 'System' section with 'Dashboard', 'Network', 'Admin', 'Network Sharing', 'Config', 'Maintenance', 'Device', 'Log', 'Content Archive', 'Report', 'Quarantine', 'Network Summary', 'Alert', and 'Tools'. The main dashboard has several sections: 'System Information' (Serial Number: FL100A2106000140, Uptime: 1 day(s) 2 hour(s) 0 min(s), System Time: Thu Jul 17 17:20:33 2008, Host Name: KT-SecureNet, Firmware Version: FortiAnalyzer-100A 3.00-b0645(MR6 Patch 1)), 'System Resources' (CPU Usage: 11%, Memory Usage: 54%, Hard Disk Usage: 15%), 'Alert Message Console' (No serious outstanding events), 'System Operation' (FortiAnalyzer-100A status with 4 slots, buttons for Reboot, Shutdown, Format log disks, Reset), 'Statistics' (since 2008-07-16 15:21:55: Connections: 38 current connections, Logs: 20 new log files for 6 devices, Log Volume: 588.97 MB/day for past 7 day(s), Reports: 0 reports generated for 0 devices, Content: 0 new log files for 0 devices), and 'License Information' (RVS Engine: 2.021 (Tue Dec 4 22:53:00 2007), RVS Plugins: 2.035 (Tue Dec 4 22:53:00 2007), Device License: Registered vs Unregistered for FortiGate, FortiManager, FortiMail, and Syslog).

## 11-1 로그 설정

- ◆ 로깅을 위한 각종 설정, 이메일 통보 설정, 로그 정책을 설정 하는 기능입니다.
- 각종이벤트 로그에 대한 로그정책을 정의 할 수 있습니다.

### 11-1 #1 : 로그 설정

- ☞ FortiAnalyzer 어플라이언스, 메모리 버퍼, 원격 Syslog 서버, ForiGuard Snalysis Service의 IP 설정 및 로그 레벨 등을 설정 할 수 있습니다.
- 로그레벨은 긴급 ~ 디버그 레벨까지 선택 할 수 있으며 설정된 레벨의 로그만 남게 됩니다.
- 최상위 레벨인 디버그 레벨 선택 시 하위 레벨이 전부 포함되므로 모든 로그를 확인 하기 위해선 로그 레벨을 디버그로 설정하는 것을 권장합니다.

- ☞ FortiAnalyzer 어플라이언스를 설정 후 연결성 검사를 하면 다음 그림과 같이 연동 상태가 표시되어며 상세 정보를 확인 할 수 있습니다.

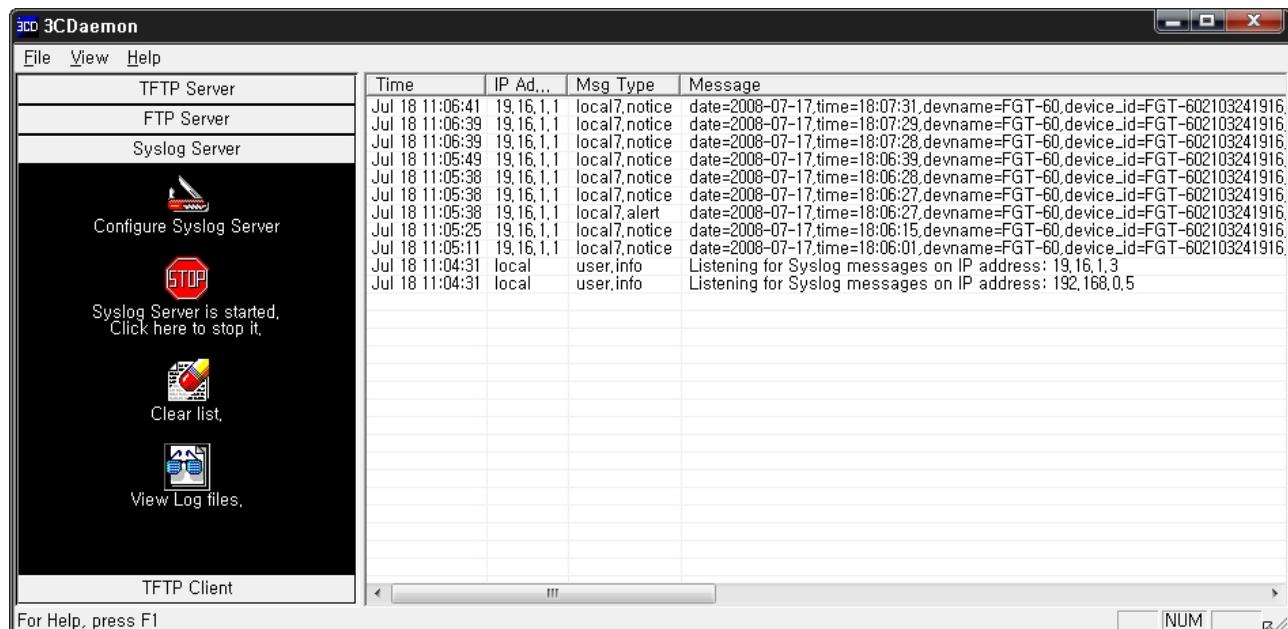


- ☞ 원격 Syslog는 기본 포트인 UDP 514를 이용하지만 포트는 변경이 가능합니다.

CSV 포맷으로 Log를 수집 할 수 있으며 모든 Syslog 프로그램과 호환이 가능합니다.

설정 시 서비스 종류는 1대의 Syslog server에 여러 대의 장비로부터 로그를 받을 경우 구분하기 위한 것이며 FortiReporter 프로그램을 염두 하여 개발된 기능으로 해당 이유 이외에는 의미가 없습니다.

원격 Syslog는 외부에 있거나 내부에 있어도 상관이 없으며 OS 버전에 따라 Log의 필드 항목이 추가 될 수 있습니다.



## 11-1 #2 : 이메일 통보

☞ 이메일 통보 기능을 통해 실시간으로 로그를 받을 수 있습니다.

경고 이메일 설정 후 연결성 검사를 눌러 테스트 메일이 발송되는지 확인 할 수 있으며 정상연결이 된 이후부터 정해진 조건마다 메일이 발송되고 수신자의 메일 주소는 3개까지 적용이 가능합니다.

<div style="background-color: #006699; color: white; padding: 5px;">         WEB CONFIG       </div> <div style="background-color: #006699; color: white; padding: 2px;">         시스템       </div> <div style="background-color: #006699; color: white; padding: 2px;">         라우터       </div> <div style="background-color: #006699; color: white; padding: 2px;">         방화벽       </div> <div style="background-color: #006699; color: white; padding: 2px;">         가상사설망       </div> <div style="background-color: #006699; color: white; padding: 2px;">         사용자       </div> <div style="background-color: #006699; color: white; padding: 2px;">         바이러스 탐지       </div> <div style="background-color: #006699; color: white; padding: 2px;">         침입 방지       </div> <div style="background-color: #006699; color: white; padding: 2px;">         웹 필터       </div> <div style="background-color: #006699; color: white; padding: 2px;">         암티스팸       </div> <div style="background-color: #006699; color: white; padding: 2px;">         IM, P2P &amp; VoIP       </div> <div style="background-color: #006699; color: white; padding: 2px;"> <b>로그&amp;보고서</b> </div> <div style="background-color: #006699; color: white; padding: 2px;">         로그 설정       </div> <div style="background-color: #006699; color: white; padding: 2px;">         로그 접근       </div> <div style="background-color: #006699; color: white; padding: 2px;">         콘텐츠 기록       </div> <div style="background-color: #006699; color: white; padding: 2px;">         보고서 설정       </div> <div style="background-color: #006699; color: white; padding: 2px;">         보고서 접속       </div>	<div style="background-color: #006699; color: white; padding: 2px;">         로그 설정       </div> <div style="background-color: #006699; color: white; padding: 2px;">         미메일 통보       </div> <div style="background-color: #006699; color: white; padding: 2px;">         로그 정책       </div> <div style="background-color: #006699; color: white; padding: 2px;">         경고 미메일       </div> <div style="background-color: #006699; color: white; padding: 2px;">         다음의 조건에서 경고 이메일 발송       </div> <div style="background-color: #006699; color: white; padding: 2px;">         위험도 로그 기반 경고 이메일 전송       </div> <div style="background-color: #006699; color: white; padding: 2px;">         Minimum Log Level: [디버그]       </div> <div style="text-align: center; background-color: #006699; color: white; padding: 5px;">         적용       </div>
--	--

☞ 이메일 통보 기능을 통해 수신되는 메일은 Message meets Alert condition 이란 제목으로 통보되며 설정된 내용의 로그가 보내집니다.



## 11-1 #3 : 로그 정책

☞ 이벤트 로그에 대한 각종 로그 정책을 설정 할 수 있습니다.

활성화 된 로그는 해당 기능을 사용하는 경우에 대해서만 로깅 됩니다.

The screenshot shows the Fortinet Web Config interface. The left sidebar menu is titled 'WEB CONFIG' and includes categories like 시스템, 라우터, 방화벽, 가상사설망, 사용자, 바이러스 탐지, 첨입 방지, 웹 필터, 암티스팸, IM, P2P & VoIP, and '로그&보고서'. Under '로그&보고서', '로그 설정' is selected. The main content area has tabs for '로그 설정', '이메일 통보', and '로그 정책', with '로그 정책' currently active. A sub-section titled '미벤트 로그' is displayed, containing a list of checked checkboxes under the heading '사용'. The checked items include: 시스템 활동 이벤트, IPSec 터널 이벤트, DHCP 서비스 이벤트, L2TP/PPTP/PPPoE 서비스 이벤트, Admin 이벤트, 미중화 활동 이벤트, 방화벽 인증 이벤트, 패턴 업데이트 이벤트, SSL VPN 사용자 인증 이벤트, SSL VPN 관리 이벤트, and SSL VPN 세션 이벤트. A green '적용' (Apply) button is located at the bottom right of this section.

## 11-2 로그 접근

◆ 저장된 로그를 확인하는 기능으로 FortiAnalyzer 와 메모리에 저장된 로그를 확인 할 수 있습니다.

### 11-2 #1 : FortiAnalyzer

☞ FortiAnalyzer를 연동한 경우만 사용이 가능하며 연동되어 있지 않은 경우 FortiAnalyzer를 설정할 수 있는 링크 페이지가 표시됩니다.



The screenshot shows the Fortinet Web Config interface. On the left, there is a navigation menu with various options like 시스템, 라우터, 방화벽, 가상사설망, 사용자, 바이러스 탐지, 첨입 방지, 웹 필터, 앤티스팸, IM, P2P & VoIP, and Log&Reporting. Under Log&Reporting, '로그 설정' and '로그 접근' are listed, with '로그 접근' being highlighted. The main content area has tabs for 'FortiAnalyzer' and '메모리'. The 'FortiAnalyzer' tab is active, displaying the message 'FortiAnalyzer를 설정 하십시오.' (Please configure FortiAnalyzer).

☞ FortiAnalyzer를 연동한 경우  
그림과 같이 장기간 로그를  
확인 할 수 있으며 HDD 장착형  
제품처럼 트래픽 로그도  
확인 할 수 있습니다.



The screenshot shows the FortiAnalyzer log viewer. At the top, it says '로그 타입' (Log Type) is set to '트래픽' (Traffic). Below that is a search bar with the number '1 / 2585' and a button '검색 설정 열 모든 필터 지우기' (Search settings open all filters clear). The main area is a table of log entries:

#	날짜	시간	수준	서비스	출발지	목적지	보냄	수신
1	2008-07-17	22:43:05	notice	61902/udp	19.16.1.2	41.234.22.26	393	0
2	2008-07-17	22:43:05	notice	15248/udp	19.16.1.2	71.52.79.144	131	0
3	2008-07-17	22:43:05	notice	26175/udp	19.16.1.2	200.127.136.237	131	0
4	2008-07-17	22:43:05	notice	60008/udp	19.16.1.2	189.18.48.149	131	159
5	2008-07-17	22:43:05	notice	45294/udp	19.16.1.2	60.166.189.140	131	0
6	2008-07-17	22:43:05	notice	35677/udp	19.16.1.2	201.242.188.168	131	0
7	2008-07-17	22:43:05	notice	44882/udp	19.16.1.2	70.171.38.33	131	0
8	2008-07-17	22:43:03	notice	11824/udp	19.16.1.2	87.203.119.1	131	0
9	2008-07-17	22:43:03	notice	58386/udp	19.16.1.2	78.37.22.134	131	0

## 11-2 #2 : 메모리

- ☞ 캐쉬 메모리에 저장로그를 보여주는 기능으로 최대 128줄 까지만 저장이 가능하고 새로 만들어진 로그는 자동으로 Rolling 되어 항상 최신의 로그를 확인할 수 있으며 리부팅시 로그는 초기화 됩니다.
  - ☞ 한 페이지에서 보여지는 Line의 수정은 시스템>관리자>설정>Display Settings>Lines Per Page에서 변경 할 수 있으며 로그타입을 선택하여 원하는 로그타입 별 확인을 할 수 있습니다.
  - ☞ 로그 페이지의 이동은 로그 탑재의 아래 줄의 화살표 아이콘을 클릭하거나 페이지 숫자를 입력하여 원하는 페이지로 이동 할 수 있습니다.
  - ☞ 세션 필터와 마찬가지로 로그도 필터링을 통해 원하는 로그만 확인이 가능하며 각 필드의  필터 아이콘을 눌러 필터링을 할 수 있습니다.  
<필터 지우기>를 클릭하면 모든 필터가 초기화 됩니다.

WEB CONFIG											
FortiAnalyzer		메모리									
시스템											
방화벽											
가상사설망											
사용자											
바이러스 탐지											
첨입 방지											
웹 필터											
안티스팸											
IM, P2P & VoIP											
로그&보고서											
로그 설정											
로그 접근											
콘텐츠 기록											
보고서 설정											
보고서 접속											
로그 타입	이벤트										
◀	1	▶	3	▶	컬럼 설정 열 모든 필터 지우기						
#	날짜	시간	수준	사용자	인터페이스	동작					
1	2008-07-16 09:36:06	information	GUI(218.144.180.142)	login	Administrator admin logged in successfully from GUI(218.144.180.142)						
2	2008-07-16 09:09:45	information	GUI(222.99.41.221)	login	Administrator neotis logged in successfully from GUI(222.99.41.221)						
3	2008-07-16 09:08:52	information	GUI(222.99.41.221)	login	Administrator neotis logged in successfully from GUI(222.99.41.221)						
4	2008-07-16 09:08:35	information	telnet(121.131.216.114)	login	Administrator admin logged in successfully from telnet(121.131.216.114)						
5	2008-07-16 09:08:28	alert	telnet(121.131.216.114)	login	Administrator admin login failed from telnet(121.131.216.114) because						
6	2008-07-16 09:02:08	information	telnet(121.131.216.114)	login	Administrator admin logged in successfully from telnet(121.131.216.114)						
7	2008-07-16 08:58:03	information	telnet(121.131.216.114)	login	Administrator admin logged in successfully from telnet(121.131.216.114)						
8	2008-07-16 08:57:53	information	GUI(121.131.216.114)	login	Administrator admin logged in successfully from GUI(121.131.216.114)						
9	2008-07-16 08:52:05	information	telnet(222.234.226.80)	logout	User admin Logs out from telnet(222.234.226.80)						
10	2008-07-16 08:50:10	notice			Fortigate scheduled update virdb(9.265) idsdb(2.517) aven(2.006) idsen						
11	2008-07-16 08:49:21	information	GUI(222.99.41.221)	login	Administrator neotis logged in successfully from GUI(222.99.41.221)						
12	2008-07-16 08:37:43	information	telnet(222.234.226.80)	login	Administrator admin logged in successfully from telnet(222.234.226.80)						
13	2008-07-16 08:24:57	information	telnet(222.234.226.75)	login	Administrator admin logged in successfully from telnet(222.234.226.75)						
14	2008-07-16 08:22:38	information	GUI(222.234.226.75)	login	Administrator admin logged in successfully from GUI(222.234.226.75)						
15	2008-07-16 08:18:58	information	GUI(222.99.41.221)	login	Administrator neotis logged in successfully from GUI(222.99.41.221)						
16	2008-07-16 08:16:48	information	GUI(222.99.41.221)	login	Administrator neotis logged in successfully from GUI(222.99.41.221)						
17	2008-07-16 07:50:07	notice			Fortigate scheduled update virdb(9.265) idsdb(2.517) aven(2.006) idsen						
18	2008-07-16 06:50:07	notice			Fortigate scheduled update virdb(9.265) idsdb(2.517) aven(2.006) idsen						
19	2008-07-16 05:50:08	notice			Fortigate scheduled update virdb(9.265) idsdb(2.517) aven(2.006) idsen						
20	2008-07-16 04:50:09	notice			Fortigate scheduled update virdb(9.265) idsdb(2.517) aven(2.006) idsen						
21	2008-07-16 03:50:11	notice			Fortigate scheduled update virdb(9.265) idsdb(2.517) aven(2.006) idsen						
22	2008-07-16 02:53:26	notice			Fortigate scheduled update virdb(9.265) idsdb(2.517) aven(2.006) idsen						

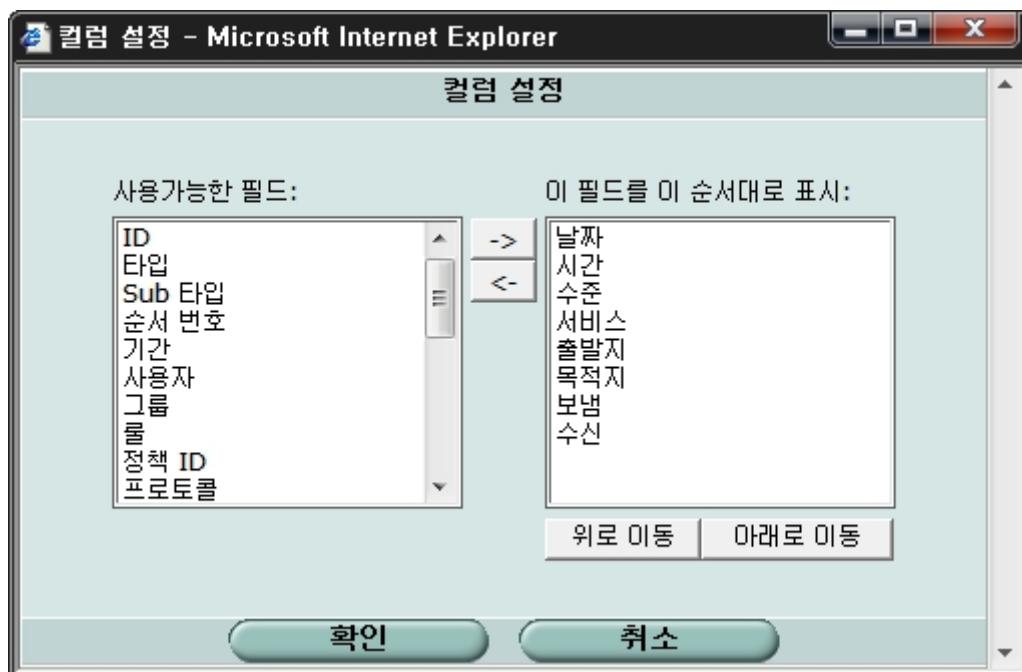
- ☞ 안티바이러스, 공격탐지 로그는 참조사항을 클릭하면 이벤트에 대한 설명이 되어있는 FortiGuard Center 웹사이트의 설명 페이지로 연결됩니다.



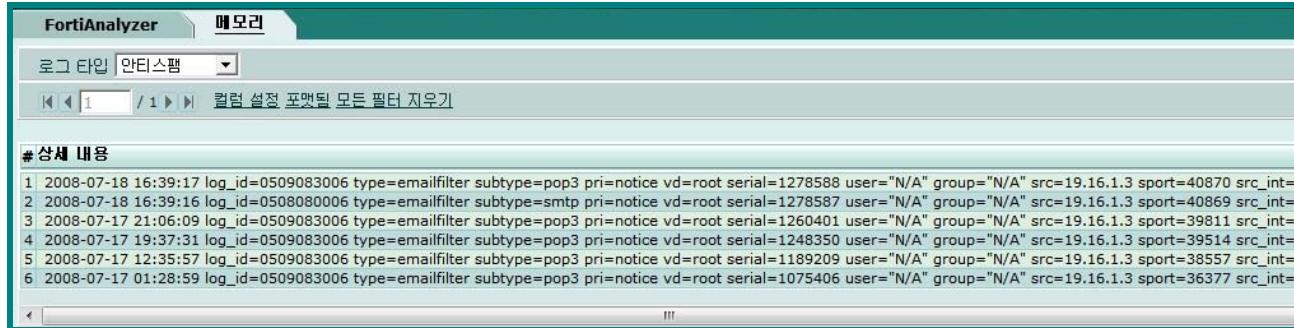
#	날짜	시간	수준	출발지	목적지	메시지	참조사항
1	2008-07-16	08:56:19	alert	61.97.71.12	222.99.41.221	http_decoder: HTTP.Request.Smuggling, repeated 6 times	<a href="http://www.fortinet.com/ids">http://www.fortinet.com/ids</a>
2	2008-07-16	08:56:13	alert	61.97.71.12	222.99.41.221	http_decoder: HTTP.Request.Smuggling	<a href="http://www.fortinet.com/ids">http://www.fortinet.com/ids</a>
3	2008-07-16	08:56:13	alert	61.97.71.12	222.99.41.221	http_decoder: HTTP.Request.Smuggling	<a href="http://www.fortinet.com/ids">http://www.fortinet.com/ids</a>
4	2008-07-16	08:55:04	alert	61.97.71.12	222.99.41.221	http_decoder: HTTP.Request.Smuggling, repeated 2 times	<a href="http://www.fortinet.com/ids">http://www.fortinet.com/ids</a>
5	2008-07-16	08:54:57	alert	61.97.71.12	222.99.41.221	http_decoder: HTTP.Request.Smuggling	<a href="http://www.fortinet.com/ids">http://www.fortinet.com/ids</a>
6	2008-07-16	08:54:50	alert	61.97.71.12	222.99.41.221	http_decoder: HTTP.Request.Smuggling	<a href="http://www.fortinet.com/ids">http://www.fortinet.com/ids</a>
7	2008-07-16	08:53:19	alert	61.97.71.12	222.99.41.221	http_decoder: HTTP.Request.Smuggling, repeated 13 times	<a href="http://www.fortinet.com/ids">http://www.fortinet.com/ids</a>
8	2008-07-16	08:53:09	alert	61.97.71.12	222.99.41.221	http_decoder: HTTP.Request.Smuggling	<a href="http://www.fortinet.com/ids">http://www.fortinet.com/ids</a>
9	2008-07-16	08:53:09	alert	61.97.71.12	222.99.41.221	http_decoder: HTTP.Request.Smuggling	<a href="http://www.fortinet.com/ids">http://www.fortinet.com/ids</a>
10	2008-07-15	19:40:12	alert	222.231.34.37	222.99.41.221	operating_system: MS.Compressed.Folder.Buffer.Overflow.A	<a href="http://www.fortinet.com/ids">http://www.fortinet.com/ids</a>
11	2008-07-15	17:40:33	alert	61.97.71.12	222.99.41.221	http_decoder: HTTP.Request.Smuggling, repeated 6 times	<a href="http://www.fortinet.com/ids">http://www.fortinet.com/ids</a>
12	2008-07-15	17:40:25	alert	61.97.71.12	222.99.41.221	http_decoder: HTTP.Request.Smuggling	<a href="http://www.fortinet.com/ids">http://www.fortinet.com/ids</a>
13	2008-07-15	17:40:24	alert	61.97.71.12	222.99.41.221	http_decoder: HTTP.Request.Smuggling	<a href="http://www.fortinet.com/ids">http://www.fortinet.com/ids</a>
14	2008-07-15	17:25:29	alert	218.237.50.80	222.99.41.221	http_decoder: HTTP.Request.Smuggling	<a href="http://www.fortinet.com/ids">http://www.fortinet.com/ids</a>
15	2008-07-15	15:13:46	alert	61.97.65.5	222.99.41.221	http_decoder: HTTP.Request.Smuggling, repeated 7 times	<a href="http://www.fortinet.com/ids">http://www.fortinet.com/ids</a>
16	2008-07-15	15:13:41	alert	61.97.65.5	222.99.41.221	http_decoder: HTTP.Request.Smuggling	<a href="http://www.fortinet.com/ids">http://www.fortinet.com/ids</a>
17	2008-07-15	15:13:32	alert	61.97.71.12	222.99.41.221	http_decoder: HTTP.Request.Smuggling	<a href="http://www.fortinet.com/ids">http://www.fortinet.com/ids</a>
18	2008-07-15	15:13:17	alert	61.97.71.12	222.99.41.221	http_decoder: HTTP.Request.Smuggling, repeated 2 times	<a href="http://www.fortinet.com/ids">http://www.fortinet.com/ids</a>
19	2008-07-15	15:13:09	alert	61.97.71.12	222.99.41.221	http_decoder: HTTP.Request.Smuggling	<a href="http://www.fortinet.com/ids">http://www.fortinet.com/ids</a>
20	2008-07-15	15:13:09	alert	61.97.71.12	222.99.41.221	http_decoder: HTTP.Request.Smuggling	<a href="http://www.fortinet.com/ids">http://www.fortinet.com/ids</a>

- ☞ 방화벽의 정책 필드와 동일하게 컬럼 설정이용 할 수 있습니다.

사용한 가능한 필드에서 원하는 항목을 추가하고 표시되는 순서 위치도 변경 할 수 있습니다.



- ☞ 로그의 상세 내용이 필요한 경우 <열> 이란 글씨를 누르면 상세 로그가 표시되며 어떠한 로그라도 상세 내용을 확인 할 수 있으며 <포맷됨> 이란 글씨를 누르면 다시 원래의 상태로 표시됩니다.



The screenshot shows the FortiAnalyzer FortiMemory interface. The top navigation bar includes 'FortiAnalyzer' and '메모리'. Below it is a dropdown menu for '로그 타입' (Log Type) set to '안티스팸'. A search bar contains the query '컬럼 설정 포맷됨 모든 필터 지우기'. The main area displays a table titled '# 상세 내용' (Detailed Content) with several log entries. The logs are as follows:

```

1 2008-07-18 16:39:17 log_id=0509083006 type=emailfilter subtype=pop3 pri=notice vd=root serial=1278588 user="N/A" group="N/A" src=19.16.1.3 sport=40870 src_int=
2 2008-07-18 16:39:16 log_id=0509080006 type=emailfilter subtype=smtt pri=notice vd=root serial=1278587 user="N/A" group="N/A" src=19.16.1.3 sport=40869 src_int=
3 2008-07-17 21:06:09 log_id=0509083006 type=emailfilter subtype=pop3 pri=notice vd=root serial=1260401 user="N/A" group="N/A" src=19.16.1.3 sport=39811 src_int=
4 2008-07-17 19:37:31 log_id=0509083006 type=emailfilter subtype=pop3 pri=notice vd=root serial=1248350 user="N/A" group="N/A" src=19.16.1.3 sport=39511 src_int=
5 2008-07-17 12:35:57 log_id=0509083006 type=emailfilter subtype=pop3 pri=notice vd=root serial=1189209 user="N/A" group="N/A" src=19.16.1.3 sport=38557 src_int=
6 2008-07-17 01:28:59 log_id=0509083006 type=emailfilter subtype=pop3 pri=notice vd=root serial=1075406 user="N/A" group="N/A" src=19.16.1.3 sport=36377 src_int=

```

- ☞ 안티스팸 로그의 경우 Spammer의 IP와 이메일 주소는 상세로그를 통해 확인이 가능 하지만 차단 단어에 탐지된 단어의 경우 CLI에서만 확인이 가능합니다.



The screenshot shows the FortiAnalyzer FortiMemory interface with a sidebar containing various system and security modules. The main area displays a table of log entries. One specific log entry is highlighted, showing its detailed content. The log entry is:

```

1 2008-07-16 09:08:19 notice 58.245.64.191 222.99.41.195 wan2 internal from ip is in dnsbl/ordbl(connection black ip 58.245.64.191)
2 2008-07-16 09:08:18 notice 58.245.64.191 222.99.41.195 wan2 internal from ip is in dnsbl/ordbl(connection black ip 58.245.64.191)
3 2008-07-16 09:08:17 notice 58.245.64.191 222.99.41.195 wan2 internal from ip is in dnsbl/ordbl(connection black ip 58.245.64.191)
4 2008-07-16 09:08:16 notice 58.245.64.191 222.99.41.195 wan2 internal from ip is in dnsbl/ordbl(connection black ip 58.245.64.191)
5 2008-07-16 09:08:16 notice 58.245.64.191 222.99.41.195 wan2 internal from ip is in dnsbl/ordbl(connection black ip 58.245.64.191)
6 2008-07-16 09:07:04 notice 71.184.131.90 222.99.41.195 wan2 internal from ip is in dnsbl/ordbl(connection black ip 71.184.131.90)
7 2008-07-16 08:59:49 notice 222.99.41.221 211.202.13.200 internal wan2 The email contains banned word(s).(1-n7 10 )
8 2008-07-16 08:59:46 notice 222.99.41.221 211.202.13.200 internal wan2 The email contains banned word(s).(1-nB 10 )
9 2008-07-16 08:45:17 notice 122.49.112.11 222.99.41.195 wan2 internal from ip is in dnsbl/ordbl(connection black ip 122.49.112.11)
10 2008-07-16 08:45:17 notice 122.49.112.11 222.99.41.195 wan2 internal from ip is in dnsbl/ordbl(connection black ip 122.49.112.11)
11 2008-07-16 08:45:17 notice 122.49.112.11 222.99.41.195 wan2 internal from ip is in dnsbl/ordbl(connection black ip 122.49.112.11)
12 2008-07-16 08:45:17 notice 122.49.112.11 222.99.41.195 wan2 internal from ip is in dnsbl/ordbl(connection black ip 122.49.112.11)
13 2008-07-16 08:45:17 notice 122.49.112.11 222.99.41.195 wan2 internal from ip is in dnsbl/ordbl(connection black ip 122.49.112.11)
14 2008-07-16 08:42:14 notice 200.42.87.232 222.99.41.195 wan2 internal from ip is in dnsbl/ordbl(connection black ip 200.42.87.232)
15 2008-07-16 08:28:34 notice 222.99.41.221 220.73.156.153 internal wan2 The email contains banned word(s).(1-4 )
16 2008-07-16 08:28:27 notice 222.99.41.221 220.73.156.153 internal wan2 The email contains banned word(s).(1-n10 8 )
17 2008-07-16 08:28:21 notice 222.99.41.221 220.73.156.153 internal wan2 The email contains banned word(s).(1-n10 8 )
18 2008-07-16 08:17:46 notice 210.223.88.32 222.99.41.195 wan2 internal The email contains banned word(s).(1-n2 80 )
19 2008-07-16 07:05:26 notice 200.31.127.154 222.99.41.195 wan2 internal The email contains banned word(s).(1-n13 2 )
20 2008-07-16 06:50:43 notice 190.76.6.237 222.99.41.195 wan2 internal The email contains banned word(s).(1-n7 40 )
21 2008-07-16 06:34:32 notice 24.85.16.48 222.99.41.195 wan2 internal The email contains banned word(s).(1-n7 40 )

```

- ☞ 안티스팸 로그의 메시지 중 차단단어의 로그는 The email contains banned word(s).(1-n7 10) 같이 표기 되며 뒷부분의 팔호()를 제외한 string 값을 이용하여 탐지된 차단단어를 검색해 낼 수 있습니다. string 값의 처음 부분은 리스트 번호이며 명령어는 CLI 모드에서 다음과 입력 하시기 바랍니다.

diagnose spamfilter bword matchfilter <string값>

**영어 이외의 단어는 표시되지 않으며 결과값은 다음과 같이 보여집니다.**

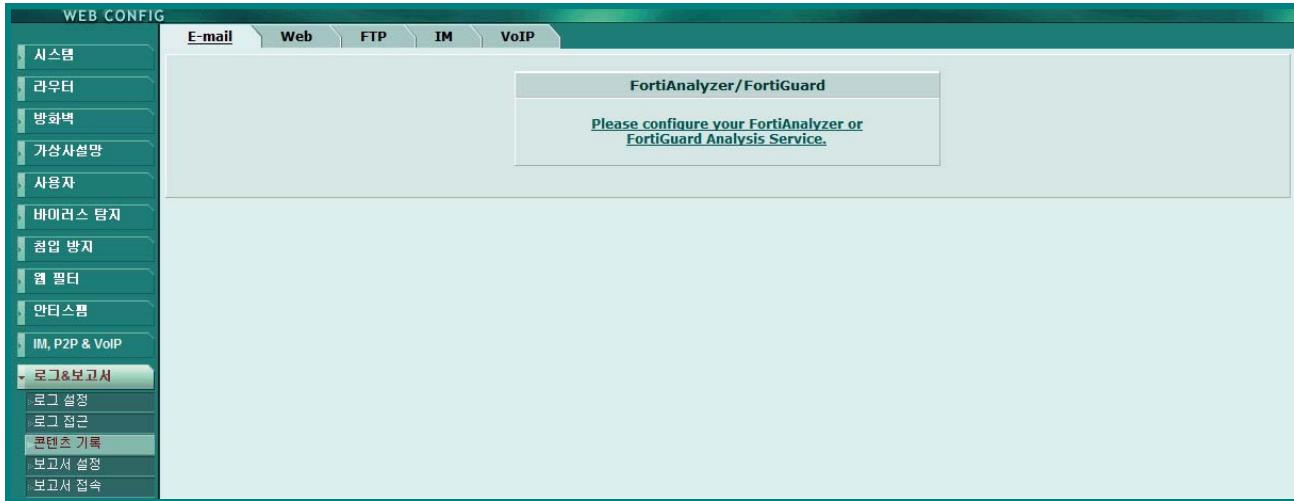


The screenshot shows the FortiGate CLI interface with the command 'diagnose spamfilter bword matchfilter 2-2' entered. The output table is as follows:

ID	pattern	score
1	sex.*	10

## 11-3 콘텐츠 기록

- ☞ 시스템>상태>통계>콘텐츠기록 에 있는 내용들이 저장되는 기능으로 FortiAnalyzer를 연동한 경우 만 내용이 표시됩니다.  
FortiAnalyzer를 연동한 사용자의 경우 FortiAnalyzer 전용 한글 매뉴얼을 참고 하시기 바랍니다.



## 11-4 보고서 설정

- ☞ FortiAnalyzer를 연동한 경우 리포트 이용 할 수 있으며 연동한 경우만 내용이 표시됩니다.  
FortiAnalyzer를 연동한 사용자의 경우 FortiAnalyzer 전용 한글 매뉴얼을 참고 하시기 바랍니다.



## 11-5 보고서 접속

☞ 시스템에서 확인되는 보고서를 보여주는 기능입니다.

FortiAnalyzer 보고서에서는 상세 리포트를 확인 할 수 있으며 메모리 보고서에서는 그래프 형태의 정보를 확인 할 수 있습니다.

## 11-5 #1 : FortiAnalyzer

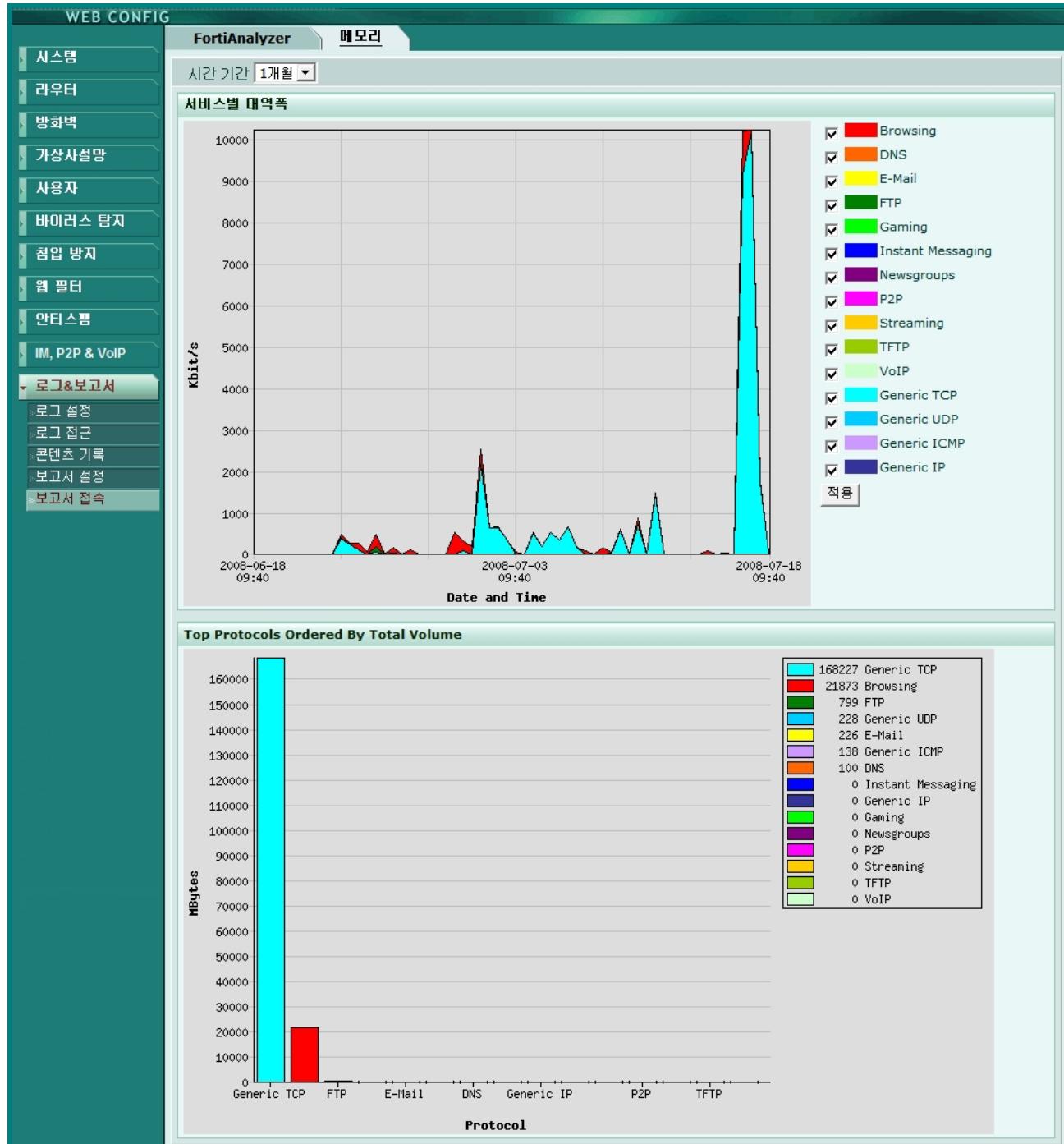
☞ FortiAnalyzer를 연동한 경우 리포트 이용 할 수 있으며 연동한 경우만 내용이 표시됩니다.

FortiAnalyzer를 연동한 사용자의 경우 FortiAnalyzer 전용 한글 매뉴얼을 참고 하시기 바랍니다.



## 11-5 #2 : 메모리

☞ 최소1일부터 최대 1개월까지의 사용량 통계를 그래프로 확인 할 수 있으며 인바운드+아웃바운드 트래픽이 통합된 데이터입니다.



# 마치면서

Fortinet의 전 제품은 각 국가마다 전자파적합등록 및 테스트를 마치고 인증을 획득한 것을 공급하고 있습니다.

국내에도 모델마다 정식으로 인증을 진행하여 정전기 및 전자파 방사 및 전도, 적합시험 (EMI, EMS)을 통과하였습니다.

‘전압강하’ 한계치 및 ‘순시 정전 내성시험 규격’ 한계치 이상의 과전류가 발생 했을 경우 하드웨어가 손상 될 수 있습니다.

Fortigate는 (주)BWS TECH ([www.bws.co.kr](http://www.bws.co.kr))에서 시험인증이 완료되었으며 인증 결과는 시험업체와 contact하여 열람을 요청하시기 바랍니다.