System Administration
사용자 매뉴얼 FortiOS 5.0

목차

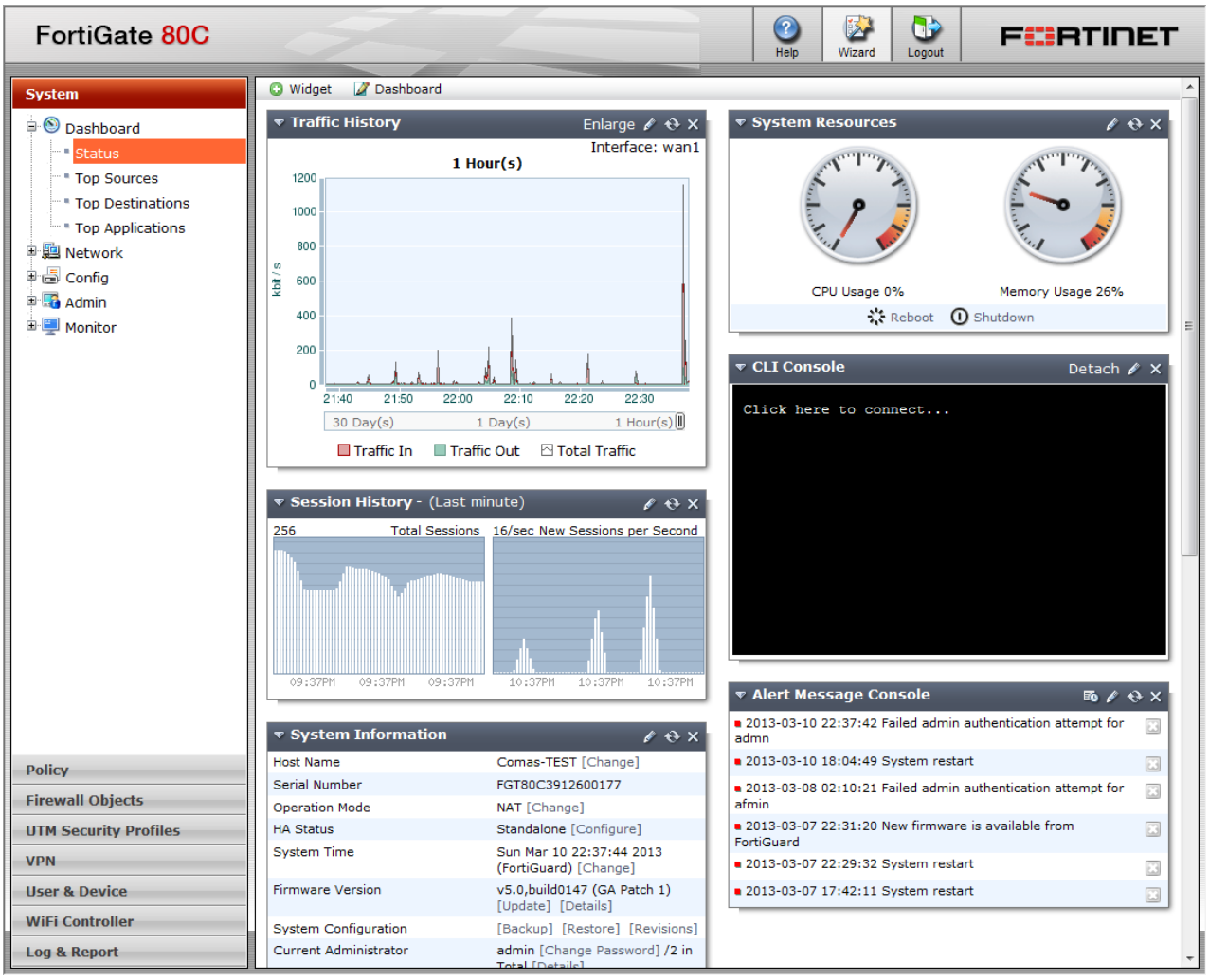
1.시스템(System)

Fortigate 시스템의 정보와 모니터링 및 네트워크 설정, 관리자 설정 등 전반적인 관리유지 기능을 설정하고 모니터링을 합니다.

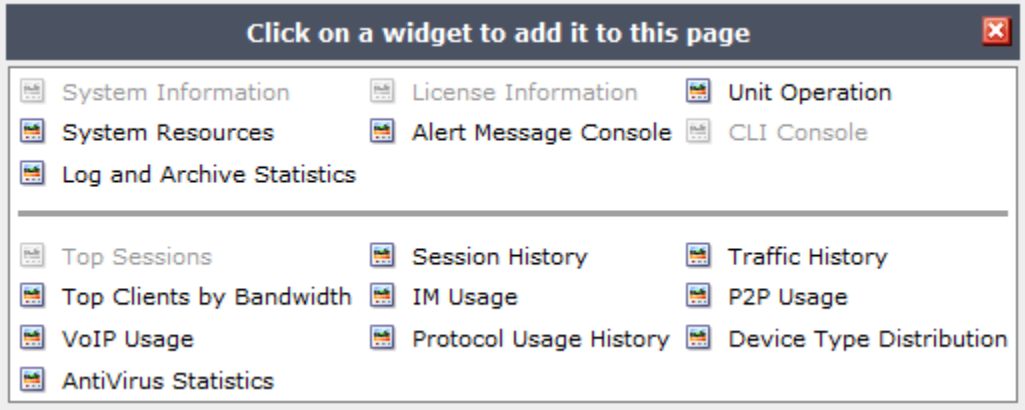
1. 대시보드(Dashboard)

Fortigate에 접속하면 가장 먼저 보이는 화면으로, 시스템의 Resource, 라이선스 상태, 인터페이별 트래픽 그래프, 세션 그래프 등의 정보를 확인 할 수 있습니다.

Dashboard 메뉴를 이용하여 여러 개의 대시보드의 생성이 가능하고 각각의 대시보드 마다 다른 위젯(Widget 메뉴를 이용)으로 구성하여 다양한 목적의 대시보드 구성이 가능합니다.

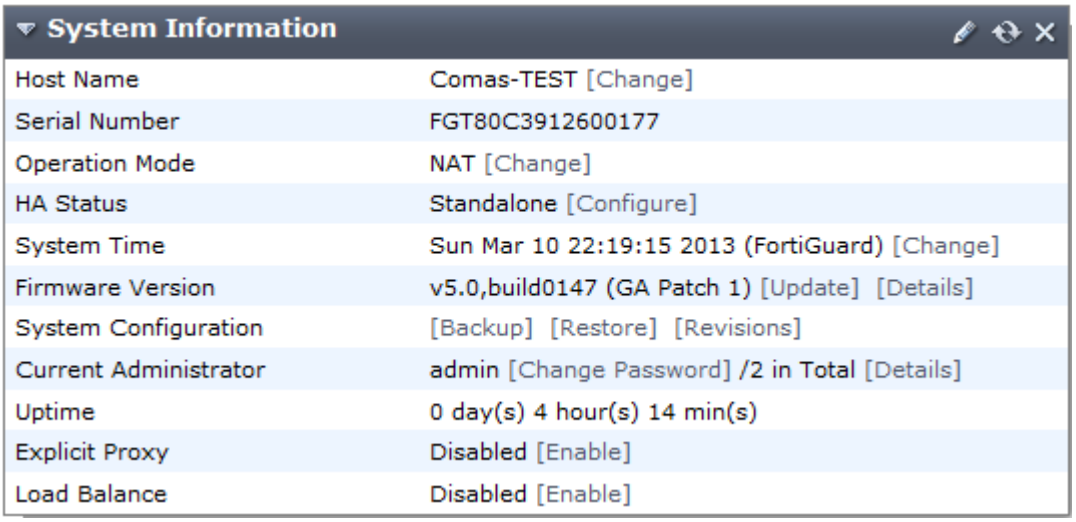


– 대시보드 화면 –



- 위젯 추가 화면 -

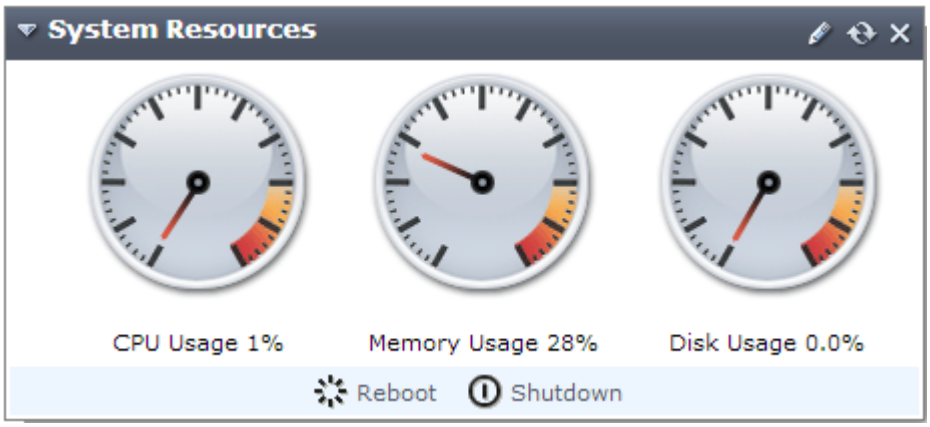
1-1. 시스템 상태(System Information)



Host Name	시스템의 식별을 위한 설정 이름입니다.
Serial Number	Fortigate 하드웨어의 고유 식별번호로 라이선스 및 유지보수를 확인하기 위한 중요한 식별코드 입니다.
Operation Mode	시스템의 현재 운영 모드로 NAT와 TP로 구성이 가능합니다. **변경 시에는 기존 설정이 초기화 되므로 주의가 필요합니다.**
HA Status	High Availability(이중화) 상태를 보여줍니다.
System Time	Fortigate 시스템 시간으로 Local 및 NTP 설정을 지원합니다.
Firmware Version	현재 시스템에서 운용중인 FortiOS 버전을 보여줍니다. GUI상에서 Upgrade, Downgrade가 가능하며 Firmware 변경 시 리부팅을 하게 됩니다.
System Configuration	시스템 설정의 백업, 복구를 하고 변경 이력을 확인 합니다.
Current Administrator	현재 시스템에 로그인 되어있는 계정의 정보를 보여줍니다.
Uptime	시스템의 가동 시간을 보여줍니다.
Explicit Proxy	캐싱 기능을 활성화 합니다.

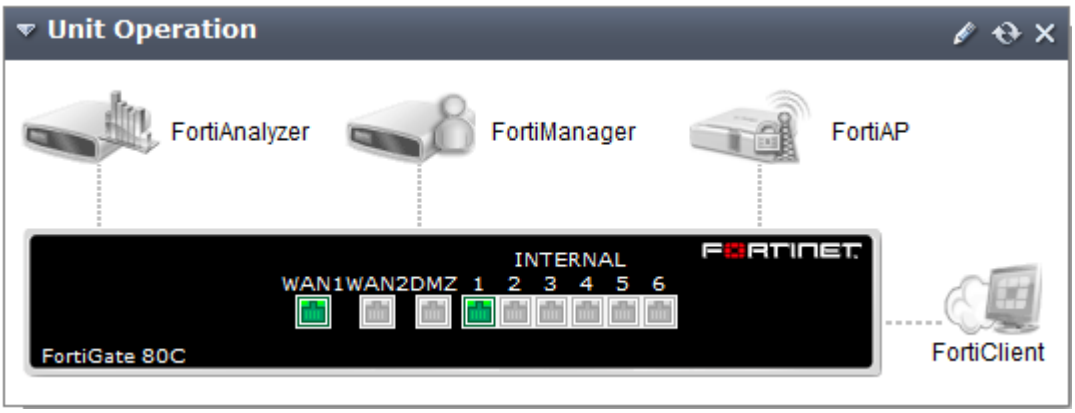
Load Balance 서버 로드밸런싱 기능을 활성화 합니다.

1-2. 시스템 자원(System Resources)



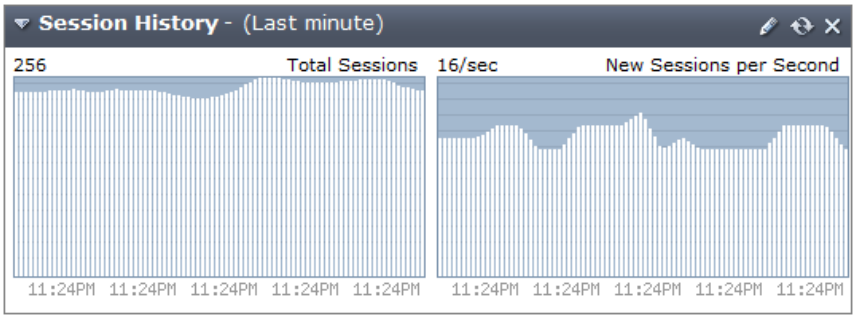
시스템의 CPU, Memory 실시간 사용량을 확인 할 수 있고, 시스템을 리부팅 또는 Shutdown을 시킬 수 있습니다. 위젯 수정을 통하여 Historical 모드로 변경이 가능합니다.

1-3. 장비 운영(Unit Operation)



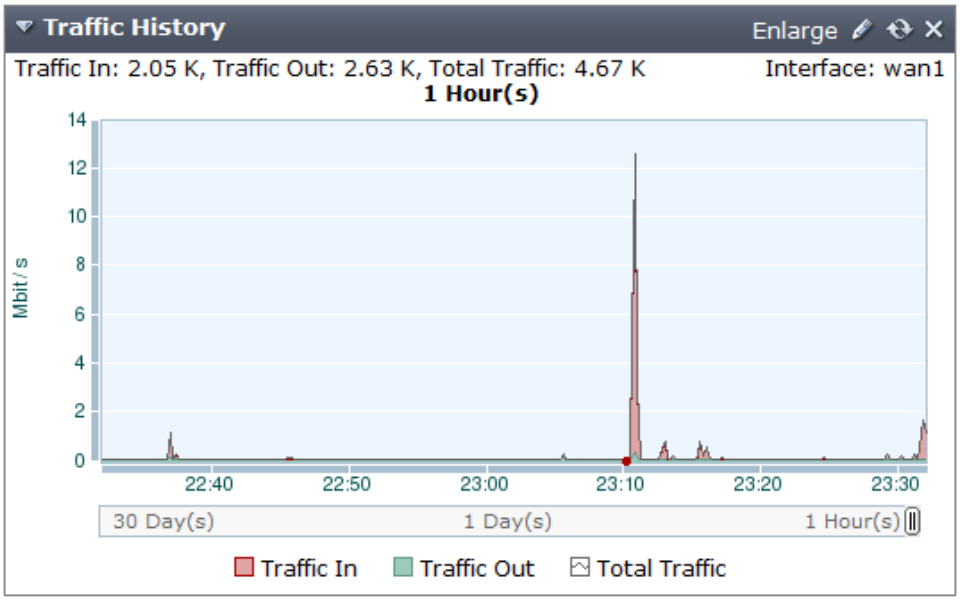
시스템의 인터페이스 UP, Down상태와 FortiAnalyzer, FortiManager, FortiAP, FortiClient와의 연동 상태를 보여줍니다.

1-4. 세션 히스토리(Session History)



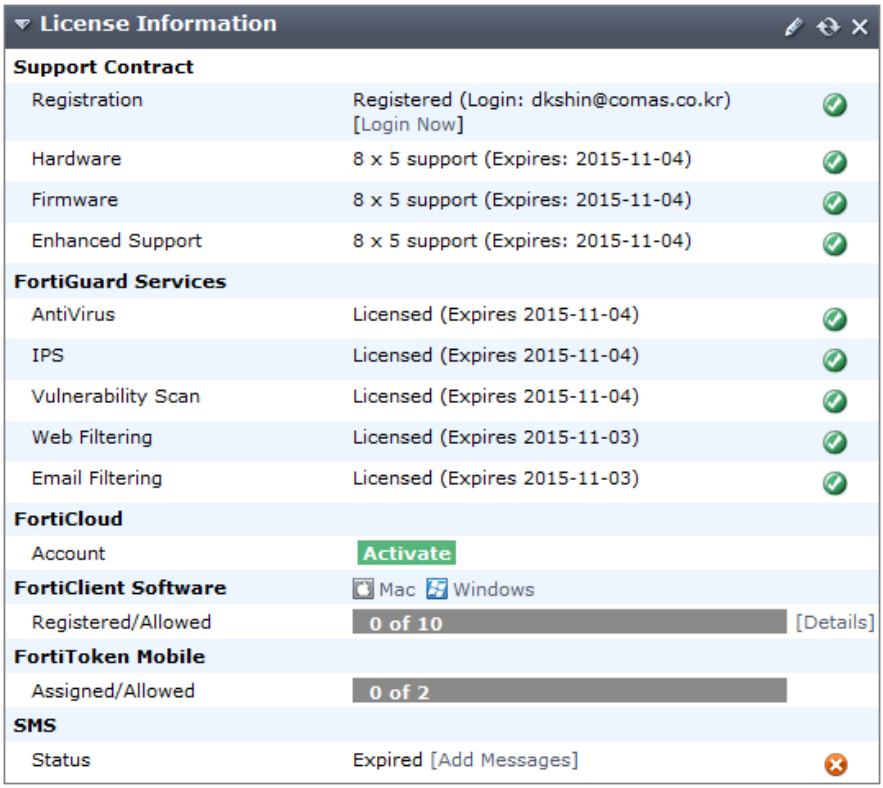
현재 전체 세션의 수와 초당 세션의 수를 보여줍니다.

1-5 트래픽 히스토리(Traffic History)



해당 인터페이스의 IN, OUT 트래픽의 정보를 그래프로 보여줍니다. 그래프를 클릭하면 좀 더 자세한 그래프를 볼 수 있습니다.

1-6. 라이선스 정보(License Information)



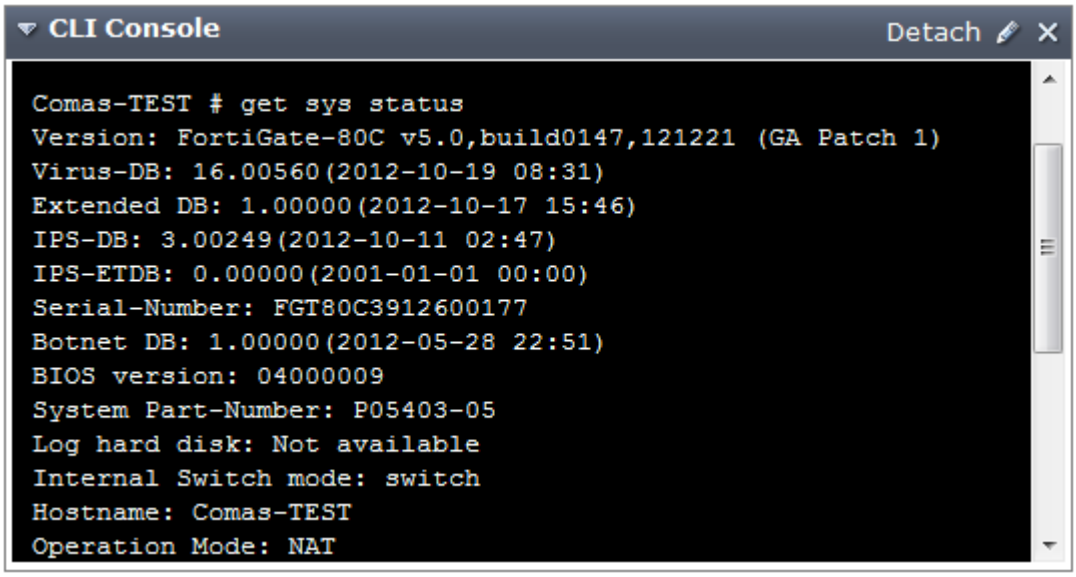
Support Contract 장비 유지보수 관련 정보를 보여줍니다.

FortiGuard Services	AV, IPS, Webfiltering 등 FortiGuard 서비스를 사용하기 위한 라이선스 정보를 보여줍니다.
FortiCloud	FortiCloud와의 연동 정보를 나타냅니다.
FortiClient Software	FortiClient 를 다운로드 할 수 있습니다.
FortiToken Mobile	사용중인 FortiToken Mobile 정보를 나타냅니다.
SMS	Fortinet에서 제공하는 SMS서비스 정보를 나타냅니다.

1-7 경고 메시지 콘솔(Alert Message Console)

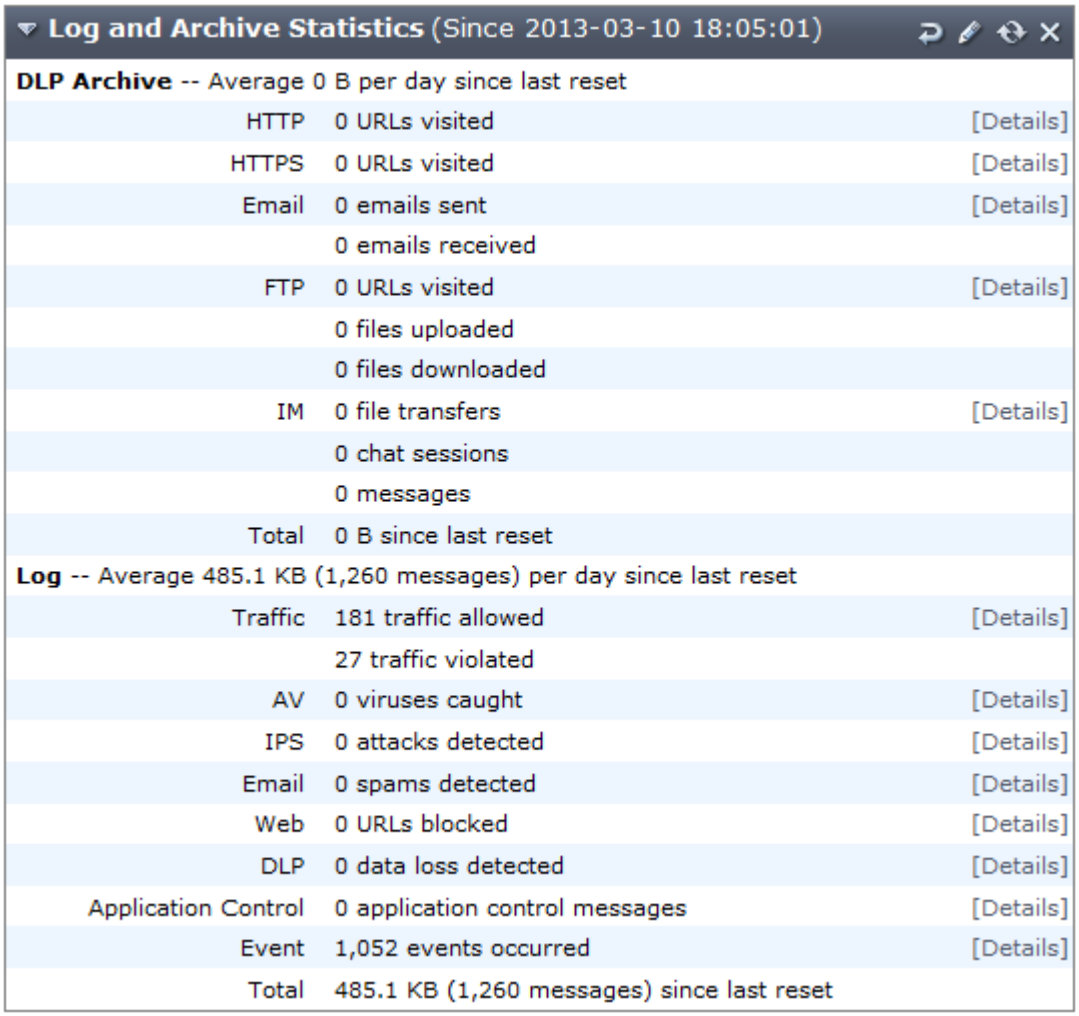
시스템에 중요한 이벤트가 발생한 내역을 보여줍니다.

1-8. CLI 콘솔(CLI Console)



GUI화면에서 CLI(Commang Line Interface)사용을 가능하게 합니다. Detach를 누르면 큰 화면으로 작업을 할 수 있습니다.

1-9. 로그와 아카이브 통계(Log and Archive Statistics)

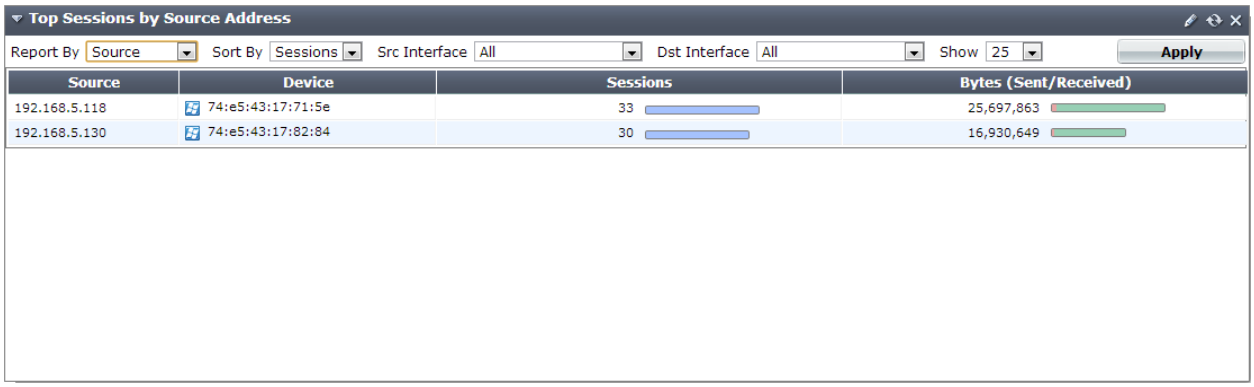


Log and Archive Statistics (Since 2013-03-10 18:05:01)

DLP Archive -- Average 0 B per day since last reset		
HTTP	0 URLs visited	[Details]
HTTPS	0 URLs visited	[Details]
Email	0 emails sent	[Details]
	0 emails received	
FTP	0 URLs visited	[Details]
	0 files uploaded	
	0 files downloaded	
IM	0 file transfers	[Details]
	0 chat sessions	
	0 messages	
Total	0 B since last reset	
Log -- Average 485.1 KB (1,260 messages) per day since last reset		
Traffic	181 traffic allowed	[Details]
	27 traffic violated	
AV	0 viruses caught	[Details]
IPS	0 attacks detected	[Details]
Email	0 spams detected	[Details]
Web	0 URLs blocked	[Details]
DLP	0 data loss detected	[Details]
Application Control	0 application control messages	[Details]
Event	1,052 events occurred	[Details]
Total	485.1 KB (1,260 messages) since last reset	

DLP, AV, IPS, Email, Web등 Fortigate에서 제공하는 UTM 기능으로 인해 발생한 이벤트의 요약정보를 보여줍니다. Details를 누르면 세부 로그를 확인 할 수 있습니다.

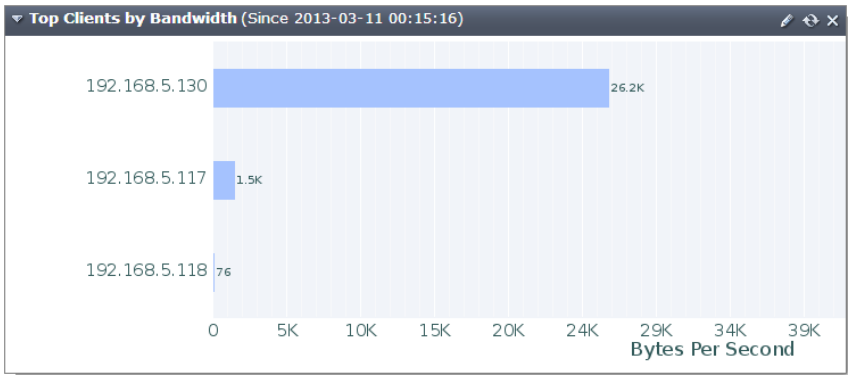
1-10. Top 세션(Top Sessions)



현재 네트워크 사용량이 많은 IP별 세션, 트래픽 사용 정보를 보여줍니다. SourceIP, DestinationIP,

Sessions, Bytes, 인터페이스를 기준으로 네트워크 사용량이 많은 사용자를 찾아 낼 수 있습니다. 해당 라인을 더블클릭하면 상세 세션 정보를 확인 할 수 있습니다.

1-11. Top 네트워크 사용자(Top Clients by Bandwidth)



현재 네트워크 사용량이 많은 상위 사용자를 보여줍니다.

1-12. IM 사용률(IM Usage)

IM Usage (Since 2013-03-10 18:05:02)

	MSN	Yahoo!	AIM	ICQ
Users				
Current Users	0	0	0	0
Since Last Reset	0	0	0	0
Blocked	0	0	0	0
Chat				
Total Chat Sessions	0	0	0	0
Server-based Chat	0	0	0	0
Group Chat	0	0	0	0
Direct/Private Chat	0	0	0	0
Messages				
Total Messages	0	0	0	0
Sent	0	0	0	0
Received	0	0	0	0
File Transfers				
Since Last Reset	0	0	0	0
Sent	0	0	0	0
Received	0	0	0	0
Blocked	0	0	0	0
Voice Chat				
Since Last Reset	0	0	0	0
Blocked	0	0	0	0
Video Chat				
Since Last Reset	0	0	0	0
Blocked	0	0	0	0

인터넷 메신저(MSN, Yahoo!, AIM, ICQ)의 사용 정보를 보여줍니다.

1-13. P2P 사용률(P2P Usage)

P2P Usage (Since 2013-03-11 00:23:34)

	BitTorrent	eDonkey	Gnutella	KaZaa	WinNY
P2P Usage					
Total Bytes	0.00 B	0.00 B	0.00 B	0.00 B	0.00 B
Average Bandwidth	0.00 B/s	0.00 B/s	0.00 B/s	0.00 B/s	0.00 B/s

P2P(Bittorrent, eDonkey, Gnutella, KaZaa, WinNY)의 사용량을 보여줍니다.

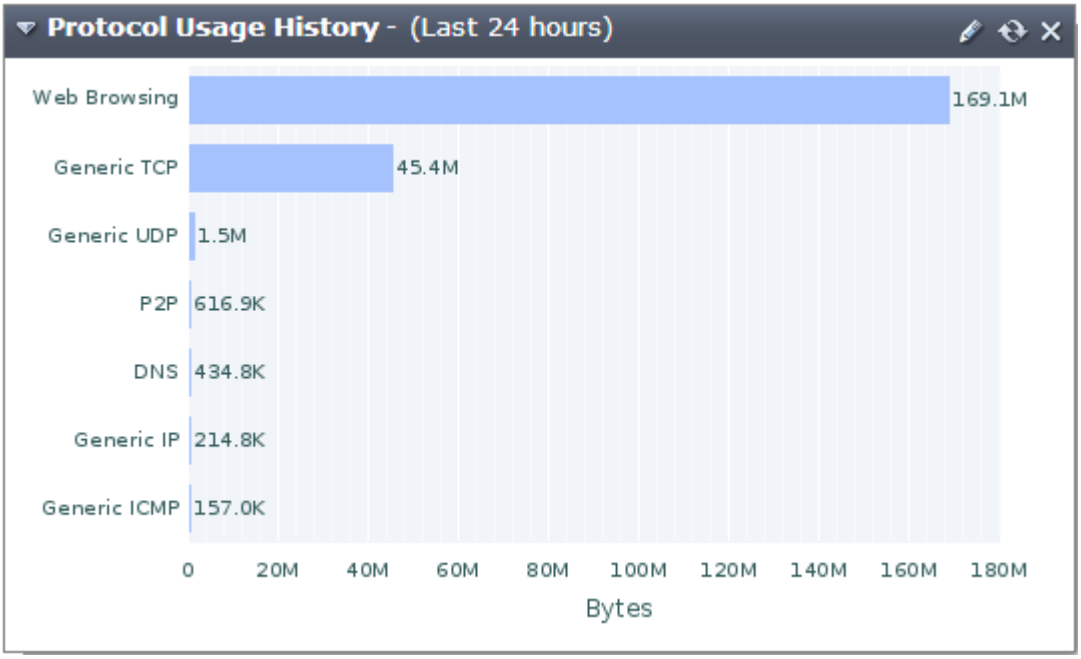
1-14. VoIP 사용률(VoIP Usage)

VoIP Usage (Since 2013-03-10 18:05:02)

	SIP	SCCP
Voice Calls		
Currently Active Calls	0	0
Total Calls (since last reset)	0	0
Calls Failed/Dropped/Unanswered	0	0
Calls Succeeded	0	0

VoIP(SIP, SCCP)의 사용 정보를 보여줍니다.

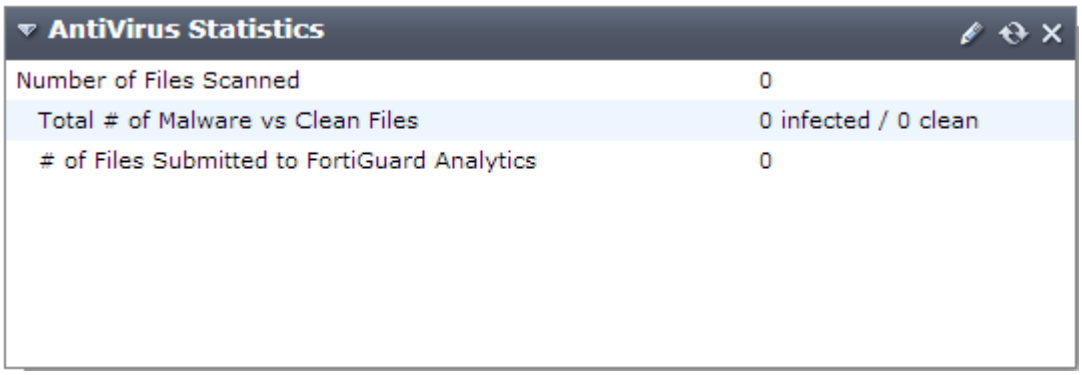
1-15. 프로토콜 사용률 히스토리(Protocol Usage History)



프로토콜 별 사용량을 보여줍니다. 해당 프로토콜을 클릭하면 자세한 사용량 그래프를 확인 할 수

있습니다.

1-16. AntiVirus 통계 (AntiVirus Statistics)



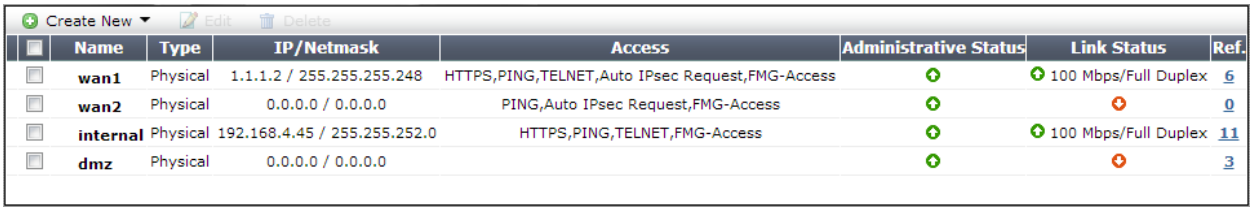
바이러스를 검사한 파일의 통계를 보여준다.

2. 네트워크(Network)

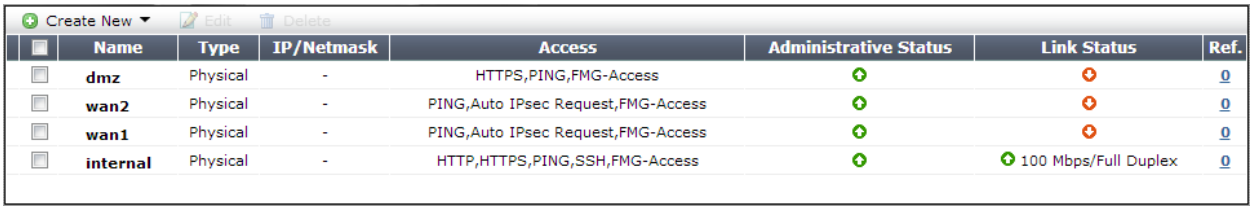
Fortigate 시스템의 인터페이스IP, 라우팅 등의 네트워크 관련 설정을 할 수 있습니다. Vlan, Link Aggregation, Software Switch의 설정도 가능하기 때문에 다양한 네트워크 구성이 가능합니다. (Software Switch의 경우 NAT모드에서만 지원합니다.)

2-1. 인터페이스(Interface)

전체적인 인터페이스의 IP, 접근 프로토콜, Link상태를 확인 할 수 있습니다. 해당 인터페이스를 더블클릭 하거나 체크박스를 체크하고 Edit버튼을 누르면 편집화면으로 이동합니다.



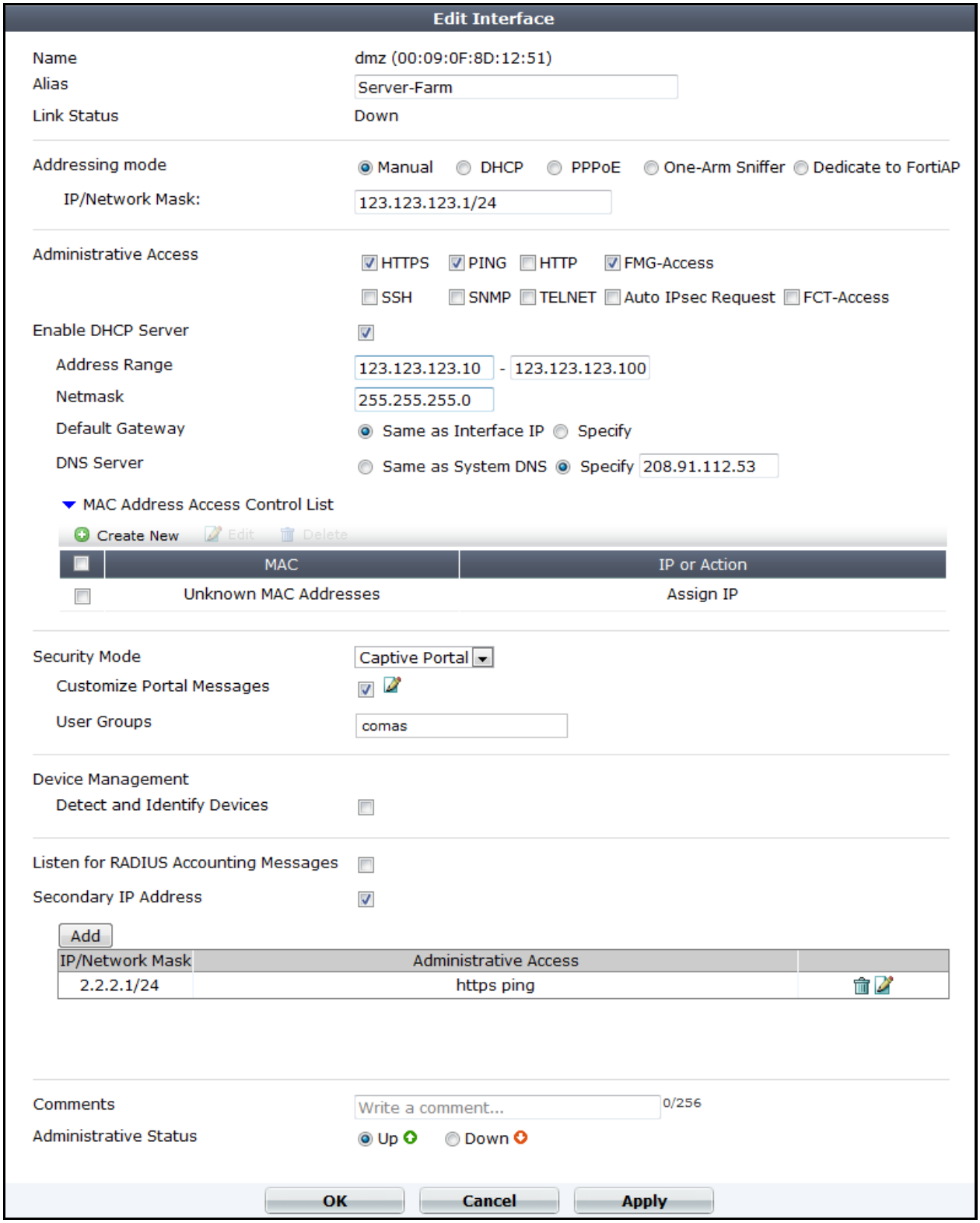
- NAT 모드 -



- TP 모드 -

TP모드의 경우 관리IP만 설정 되기 때문에 인터페이스에 IP를 설정 할 수 없습니다.

2-1-1. 인터페이스 설정



Name 해당 인터페이스의 이름입니다.

Alias	어떤 용도의 인터페이스인지 별명을 설정 할 수 있습니다.
Link Status	해당 인터페이스의 Link 상태를 나타냅니다.
Addressing Mode	인터페이스에 설정 할 IP의 형식 또는 형태를 설정합니다. IPv6도 설정이 가능합니다.
	Manual : 고정회선 IP를 설정 합니다.
	DHCP, PPPOE : 유동회선 IP를 설정합니다. **유동 회선의 경우 Retrieve default gateway from server 항목이 체크가 되어야 게이트웨이를 받아옵니다.**
	One-Arm Sniffer : 해당 인터페이스를 트래픽 모니터링을 위한 One-Armd 형태로 설정합니다.
	Dedicate to FortiAP : 해당 인터페이스를 FortiAP와 연동 할 전용포트로 설정합니다. IP를 설정하면 자동으로 DHCP서버가 설정 됩니다.
Administrative Access	Fortigate의 해당 인터페이스로 가능한 관리적 접근을 설정 합니다.
DHCP Server	해당 인터페이스에 DHCP를 설정합니다. (DHCP Server 장에서 자세히 설명합니다.)
Security Mode	해당 인터페이스로 인입되는 트래픽에 Captive Portal 사용자 인증 설정을 합니다. 인증을 거치기 위해서는 먼저 HTTP또는 HTTPS로 해당 인터페이스를 통하여 연결하는 시도가 있어야 합니다.

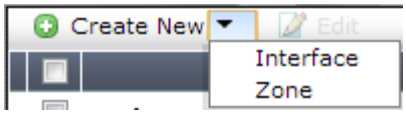
- Security Mode 설정 시 인증 화면 -

Device Management	Fortigate는 네트워크에 존재하는 기기들의 MAC주소, IP주소, OS, 호스트명 등의 정보를 모니터링 합니다. *User & Device > Device > Device Definition* 에서 확인 가능합니다.
Enable STP	STP(Spanning Tree Protocol)을 활성화 하여 Looping을 방지 합니다. 여러 포트가 묶여있는 스위치 인터페이스에서만 설정이 가능합니다.
Listen for RADIUS Accounting Messages	RADIUS 콘텐츠에 대한 수신대기 포트로

사용합니다.

Secondary IP Address	기본 IP외에 추가적으로 IP를 설정 합니다.
Comments	해당 인터페이스에 대한 설명을 씁니다.
Administrative Status	해당 인터페이스를 UP 또는 Down 시킵니다.

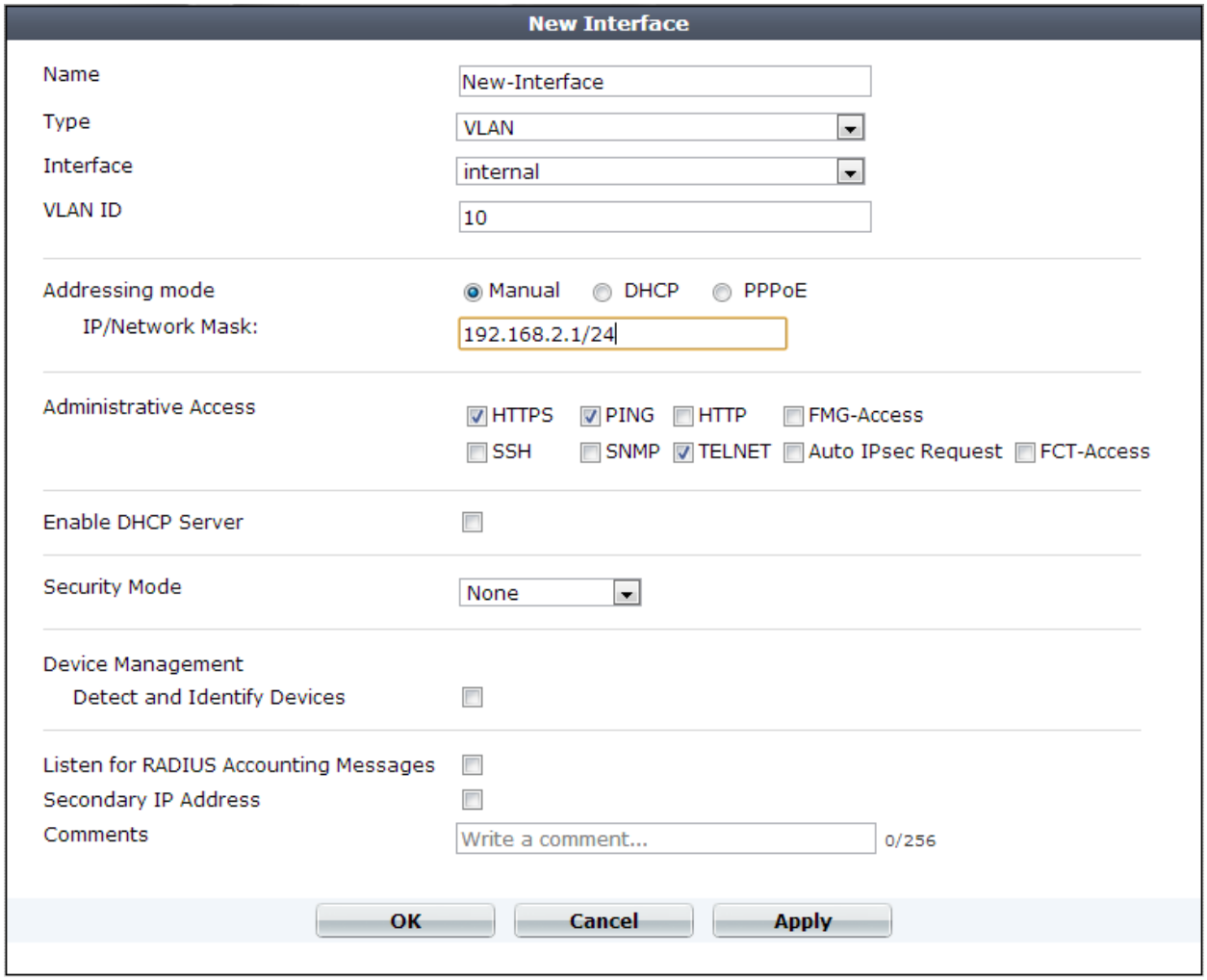
2-1-2. 인터페이스 생성



System > Network >Interface > Create New 에서 인터페이스를 생성합니다.

- Interface에서는 Vlan, Loopback, Software Switch, 802.3ad Aggregate, Redundant 의 인터페이스를 만들 수 있습니다. 802.3ad Aggregate, Redundant의 경우 모델에 따라 지원여부가 다르기 때문에 확인이 필요합니다.

Vlan 생성

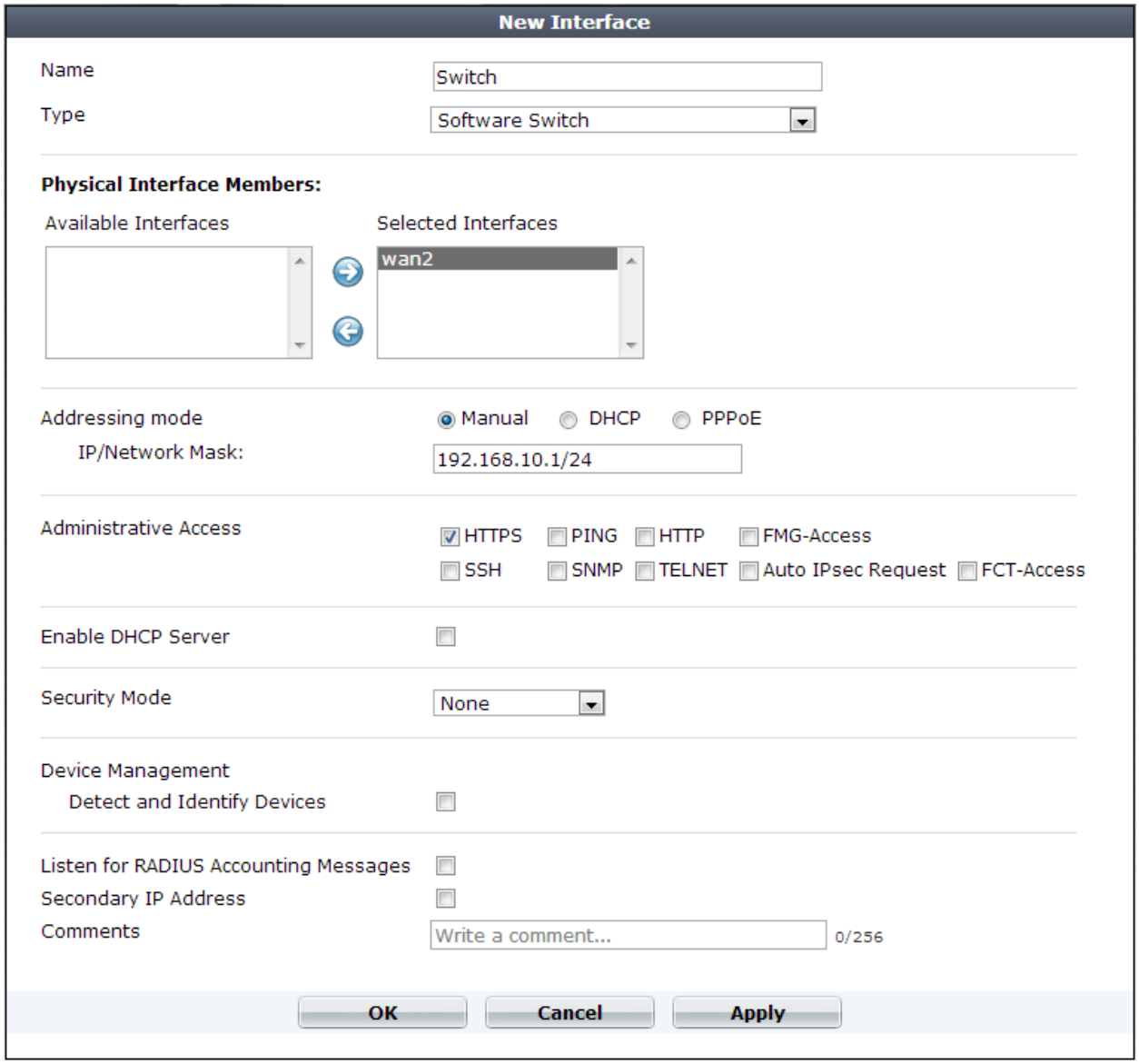


- Vlan 설정 화면 -

1. *System > Network > Interface* 에서 *Create New* 를 선택하고, *Type* 을 VLAN 으로 설정합니다.
2. Vlan 의 이름을 설정합니다.
3. Vlan 을 생성할 물리 인터페이스를 선택합니다.
4. *VLAN ID* 를 설정합니다.
5. *Addressing Mode*(주소형식) 를 설정하고 IP 를 설정 합니다.
6. *Administrative Access* (관리접근)을 설정 합니다.
7. *OK* 를 누릅니다..

Fortigate는 Vlan Trunk 포트 기능이 없습니다. 그래서 Vlan Trunk 구간에 연결 될 경우 적용할 모든 Vlan을 생성해 주어야 합니다.

Software Switch 생성

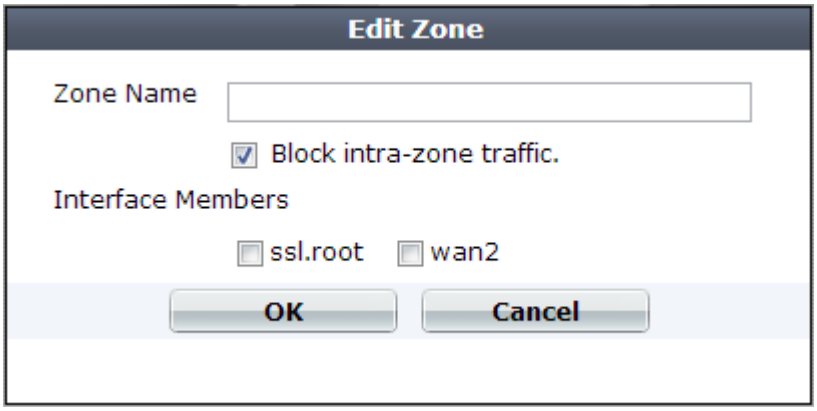


– Software Switch 설정 화면 –

1. *System > Network > Interface* 에서 *Create New* 를 선택하고, *Type* 을 Software Switch 로 설정합니다.
2. 인터페이스 이름을 설정합니다.
3. 묶어줄 인터페이스를 Selected Interfaces 로 넘겨줍니다.
4. *Addressing Mode*(주소형식) 를 설정하고 IP 를 설정 합니다.
5. *Administrative Access* (관리접근)을 설정 합니다.
6. *OK* 를 누릅니다.

- Zone은 동일한 정책을 적용시킬 인터페이스들을 하나로 묶어줍니다. Zone을 이용하면 적은 정책으로도 여러 세그먼트에 동일한 정책을 적용할 수 있습니다.

Zone 생성

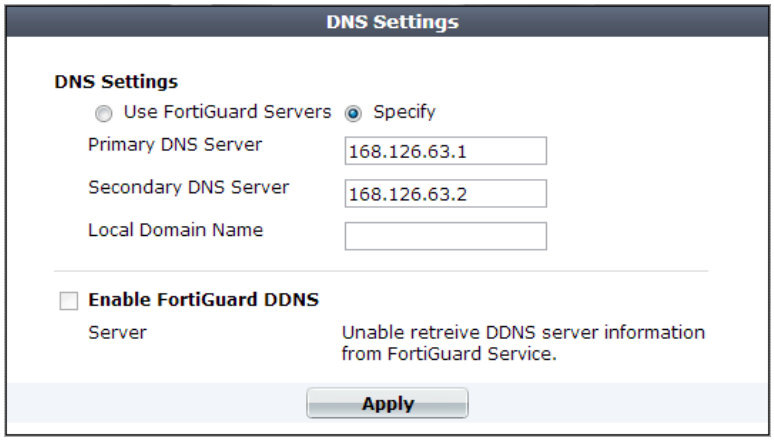


– Zone 설정 화면 –

1. *System > Network > Interface* 에서 *Create New > Zone* 을 선택한다.
2. Zone 의이름을 설정합니다.
3. 묶어줄 인터페이스의 체크박스에 체크합니다.
4. *OK* 를 누릅니다..

2-2. DNS

Fortigate가 참조할 DNS 서버를 설정합니다. DNS는 FortiGuard 서비스의 업데이트와 관련이 있으니 정확하게 설정합니다.

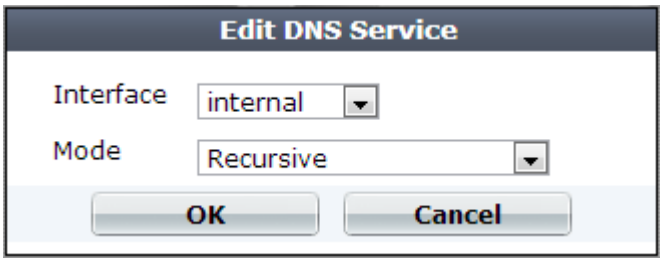


– DNS 설정 화면 –

2-3. DNS Server

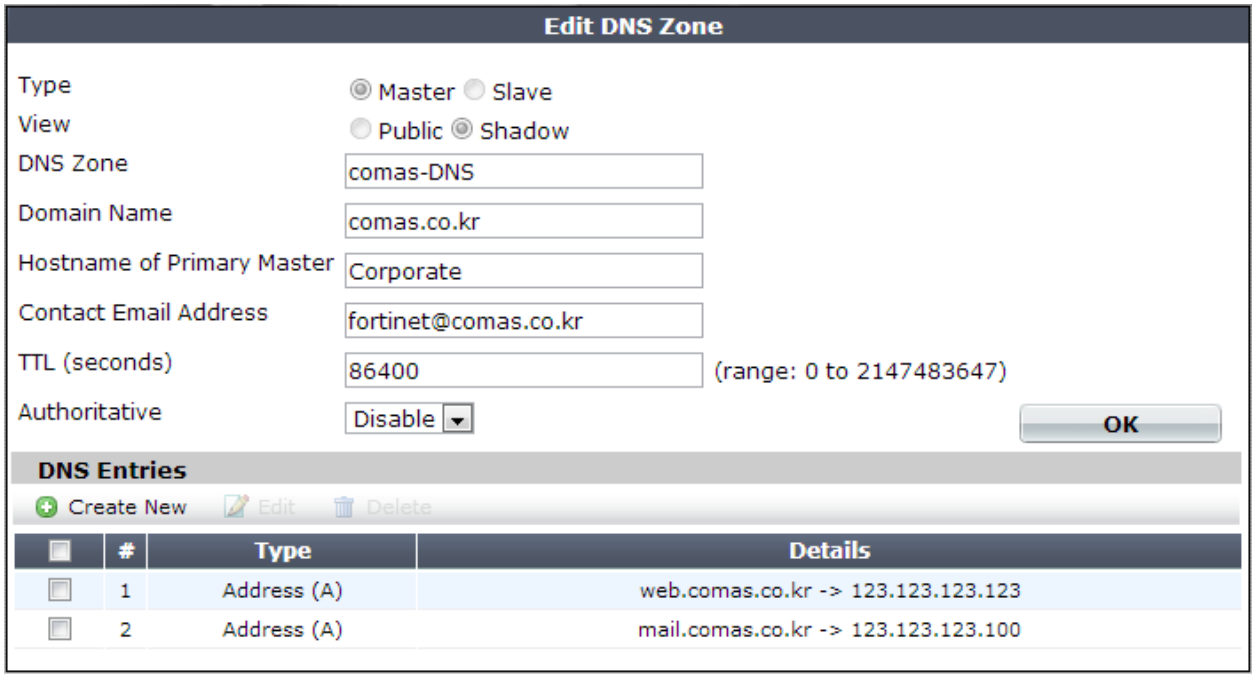
Fortigate는 간단한 DNS서버 역할을 할 수 있습니다.

■DNS를 서비스 할 인터페이스 설정



1. *System > Network > DNS Server* 에서 *DNS Service on Interface > Create New* 를 선택한다.
2. DNS 서비스를 할 인터페이스를 선택한다.
3. Mode 를 선택한다.
   - Recursive : 사용자가 Fortigate DNS 에 쿼리를 보내 완성된 답을 받습니다. 서비스를 하려면 DNS Database 를 설정해야 합니다.
   - Non-recursive : Fortigate DNS 가 다른 DNS 서버에게 쿼리를 보내어 답을 요청합니다.
   - Forward to System DNS : Fortigate 에 설정된 DNS 서버로 쿼리를 전달합니다.
4. *OK* 를 누릅니다.

■DNS Database 설정



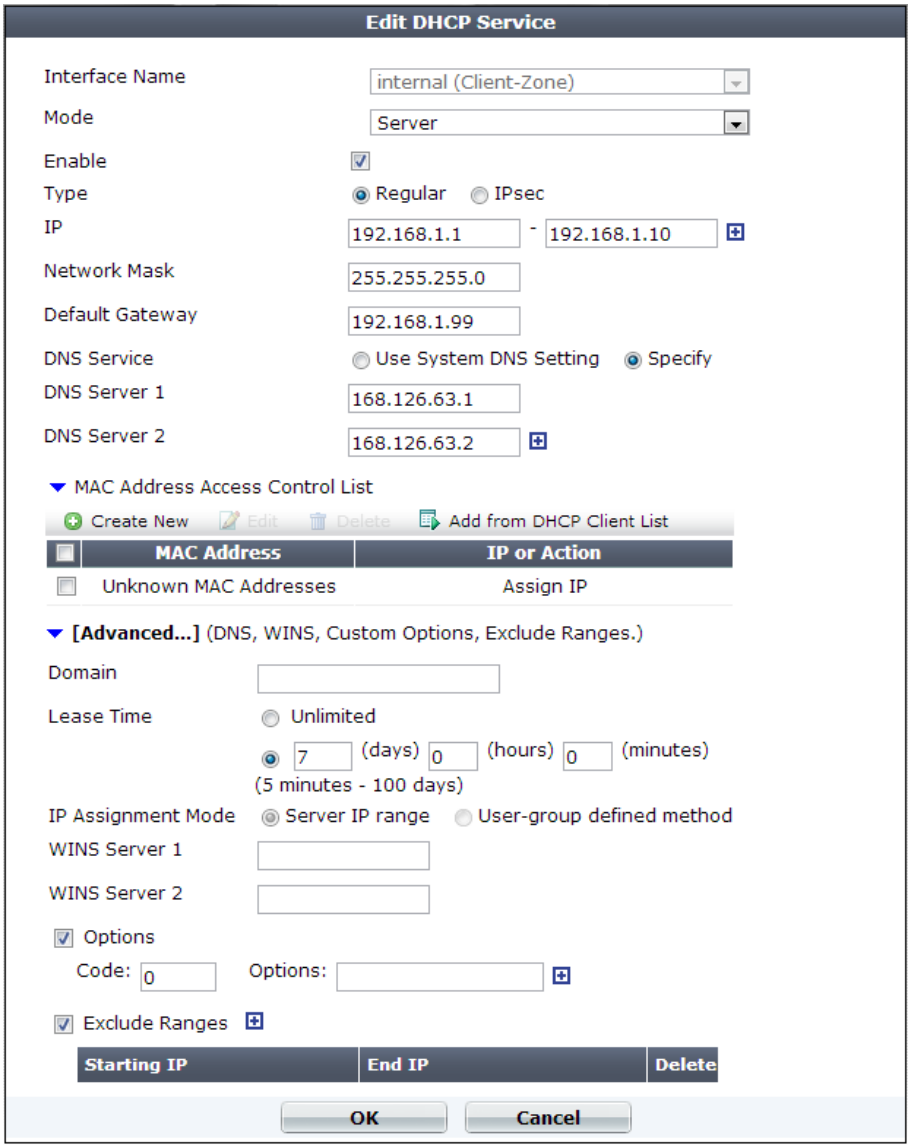
1. *System > Network > DNS Server* 에서 *DNS Database > Create New* 를 선택한다.
2. *Type* 을 *Master* 로 설정합니다.

3. *View* 를 *Shadow* 로 설정합니다(Shadow 는 내부사용자만 사용가능, Public 은 외부사용자도 사용가능).
4. DNS *Zone* 을 설정합니다.
5. 해당 Zone 의 도메인 네임을 설정합니다. 예) comas.co.kr
6. DNS server 의 호스트 네임을 설정합니다. 예) Corporate
7. 관리자의 메일 주소를 설정합니다.
8. *Authoritative* 를 *Disable* 로 설정합니다.
9. *OK* 를 누릅니다.
10. *Create New.*를 선택하여 DNS 엔트리를 추가 합니다.
11. *Type* 을 설정합니다. 예) *Address (A)*.
12. *Hostname* 과 *IP Address* 를 설정합니다.
13. *OK* 를 누릅니다.

2-4. DHCP Server

Fortigate는 NAT/Route 모드에서 DHCP 서비스를 제공하며, DHCP Monitor를 통하여 IP의 임대 상태를 확인 할 수 있습니다.

2-4-1. DHCP 서버 설정



- DHCP 설정 화면 -

Interface Name	DHCP 서비스를 할 인터페이스 입니다.
Mode	Fortigate가 직접 DHCP 서비스를 하려면 Server를 선택하고, 다른 DHCP서버와 연동하려면 Relay를 선택합니다.
Enable	DHCP 서비스 활성화 또는 비활성화를 합니다.

Type

IP DHCP 서비스를 할 IP범위를 설정합니다.

Network Mask DHCP 서비스를 할 넷마스크를 설정합니다.

Default Gateway DHCP 서비스를 할 디폴트 게이트웨이 설정합니다.

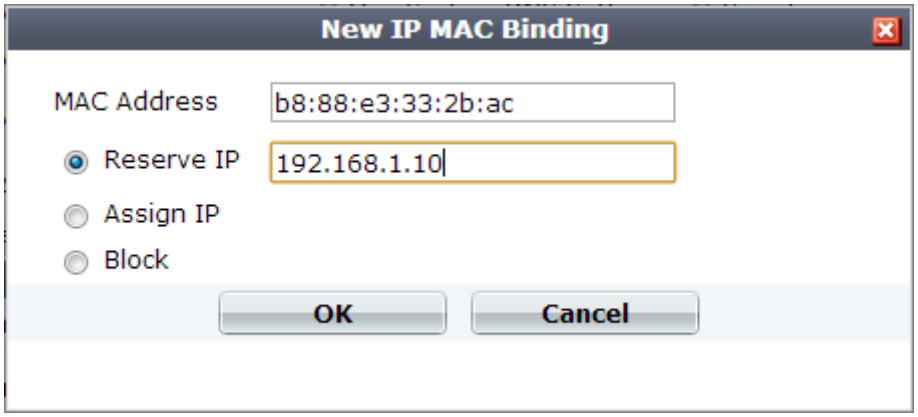
DNS DHCP 서비스를 할 DNS를 설정합니다.

MAC Address Access Contorl List MAC주소 기반으로 IP주소 할당을 차단하거나, 특정IP를 맵핑하여 항상 동일한 IP를 할당하도록 설정합니다.

Reserve IP MAC주소와 IP주소를 맵핑하여 주소를 할당합니다.

Assign IP 해당 MAC주소에 대하여 IP주소 할당을 허용 합니다.

Block 해당 MAC주소에 대하여 IP주소 할당을 차단 합니다.



Lease Time 주소 임대시간을 설정합니다. 설정시간 동안 DHCP 테이블에 할당 정보를 저장합니다.

Exclude Ranges IP주소 할당 범위에서 제외할 IP를 설정합니다.

2-3-2. DHCP Monitor(모니터링)

System > Monitor > DHCP Monitor 에서 Fortigate를 통해 임대된 IP의 정보를 보여줍니다.

3. 설정(Config)

Fortigate 시스템의 HA 이중화, SNMP 설정, Fortigate가 보여주는 메시지의 편집 등을 설정합니다.

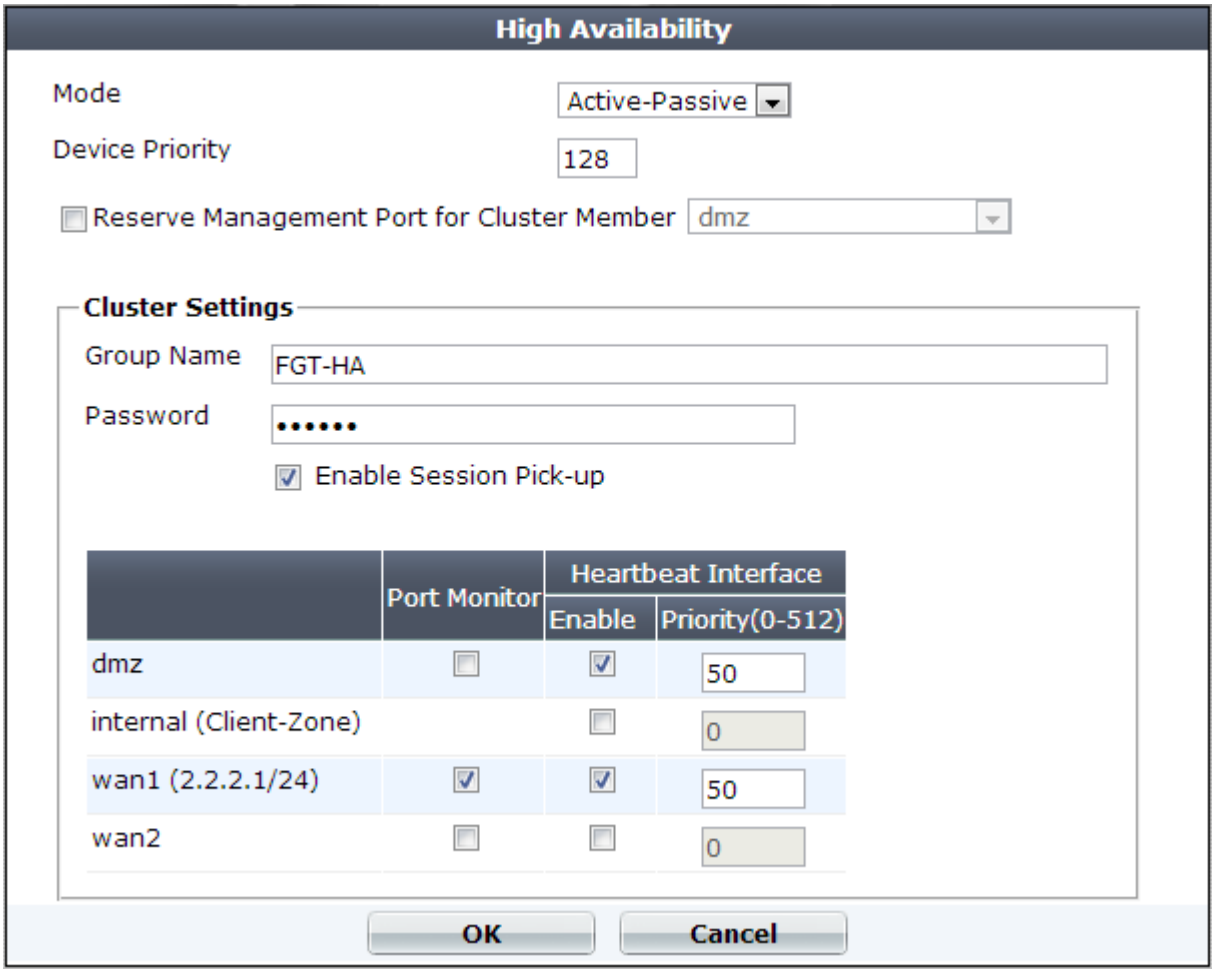
3-1. HA(고가용성) 이중화

FGCP프로토콜을 이용하여 2대 이상의 Fortigate시스템을 HA 클러스터 구성 할 수 있습니다. HA구성은 Master 장비의 하드웨어 장애에도 Standby 장비로 지속적인 서비스가 가능하도록

합니다. **HA구성을 위해서는 클러스터링 할 장비들이 동일 모델, 동일 Firmware를 사용하여야 합니다.** HA기능은 유동회선(DHCP, PPPOE)에서는 지원하지 않습니다.

FGCP는 VRRP와 달리 Virtual IP와 Real IP를 각각 필요로 하지 않고, 하나의 IP로 구성하기 때문에 하나의 장비를 운영하는 하는 듯한 관리적인 장점이 있습니다.

HA 설정



- HA 설정 화면 -

*System > Config > HA*에서 설정합니다.

Mode — HA 모드를 설정합니다.

- **Standalone** — 이중화가 아닌 단일장비로 동작합니다.
- **Active-Pasive** — Master 장비만 트래픽을 처리하고 Slave장비는 Standby상태로 대기 합니다.
- **Active-Active** — Master, Slaver 장비 모두 트래픽을 처리합니다.

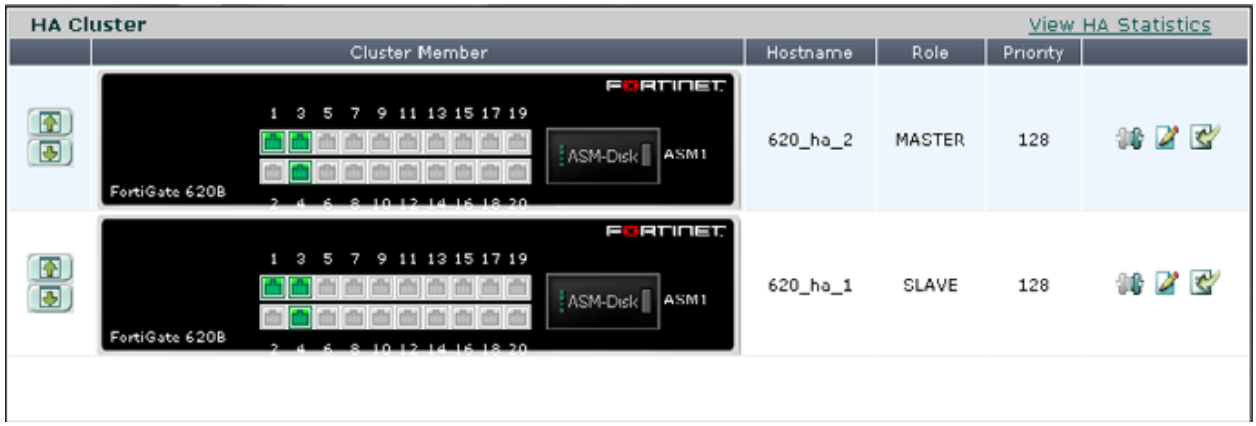
Device Priority — 장비의 우선순위를 정합니다. 숫자가 클수록 우선순위가 높습니다. 숫자가 같을 경우 장비 시리얼에 의해 우선순위가 결정됩니다.

Reserve Management Port for Cluster Member	클러스터 멤버에 대하여 각각 SNMP 원격 관리를 하기 위한 설정입니다.
Group Name	클러스터 그룹 식별이름으로 여러개의 클러스터를 구성할 경우 클러스터를 구분하기 위한 이름입니다. 동일한 Group Name의 장비끼리만 클러스터링 됩니다.
Password	클러스터를 식별하기 위한 암호 입니다. 클러스터링 할 멤버들은 동일할 암호가 설정되야 합니다. 기본 암호는 없습니다.
Enable Session Pick-up	Master 장비의 세션을 Slave 장비로 Copy합니다. 이 기능을 활성화하면 장애 시에도 세션의 끊김 없이 서비스가 가능합니다. TCP와 IPSec VPN 세션 만 적용됩니다.
Port Monitor	장애 판단을 위하여 모니터링 하는 인터페이스 입니다. 체크된 인터페이스가 장애가 발생하면 Master의 권한이 넘어갑니다.
Heartbeat Interface	HA 하트비트 통신을 할 인터페이스와 우선순위를 설정합니다. 숫자가 작을수록 우선순위가 높고, 숫자가 같을 경우 가장 낮은 Hash map order vlaue를 가진 인터페이스가 모든 하트비트 트래픽을 처리합니다.

HA 모니터링

HA 설정이 완료되면 *System > Config > HA*에서 HA 정보에 대한 모니터링이 가능합니다.

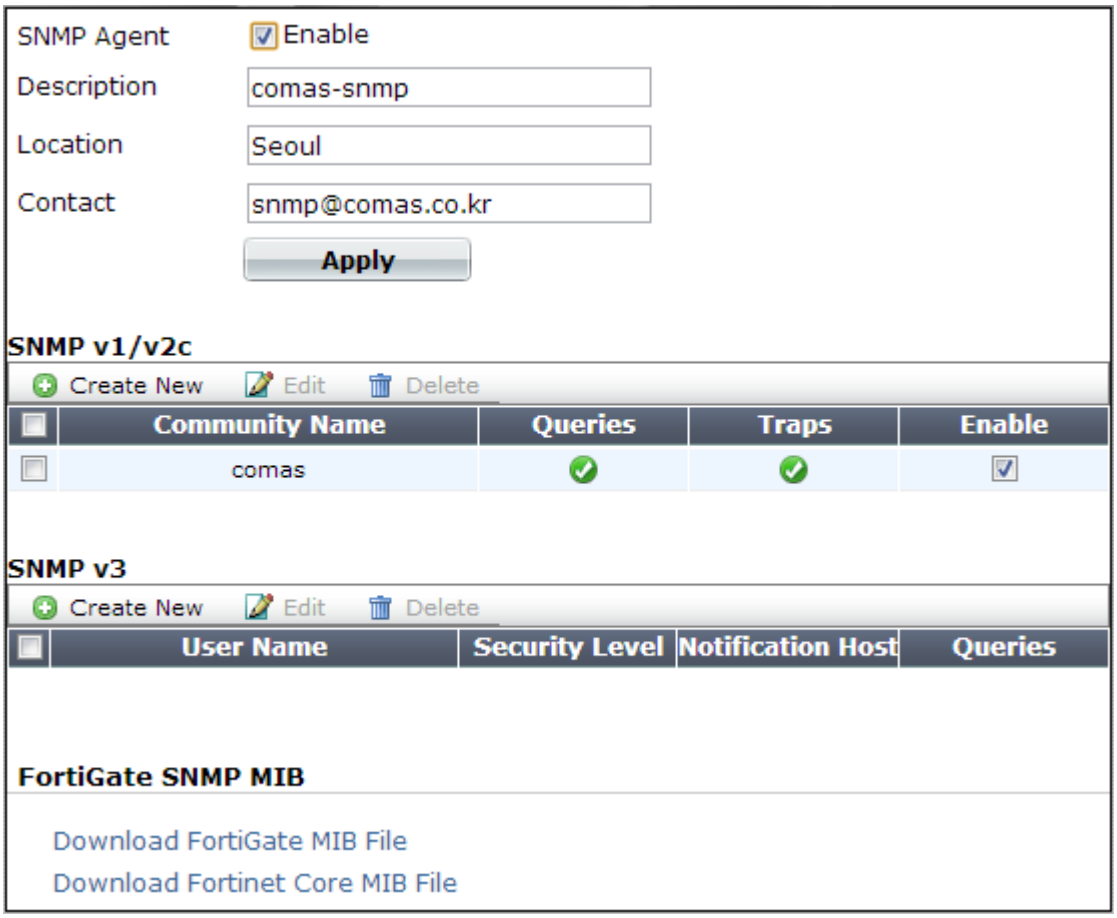
View HA Statistics를 누르면 장비 별 상세 통계를 확인 할 수 있습니다.



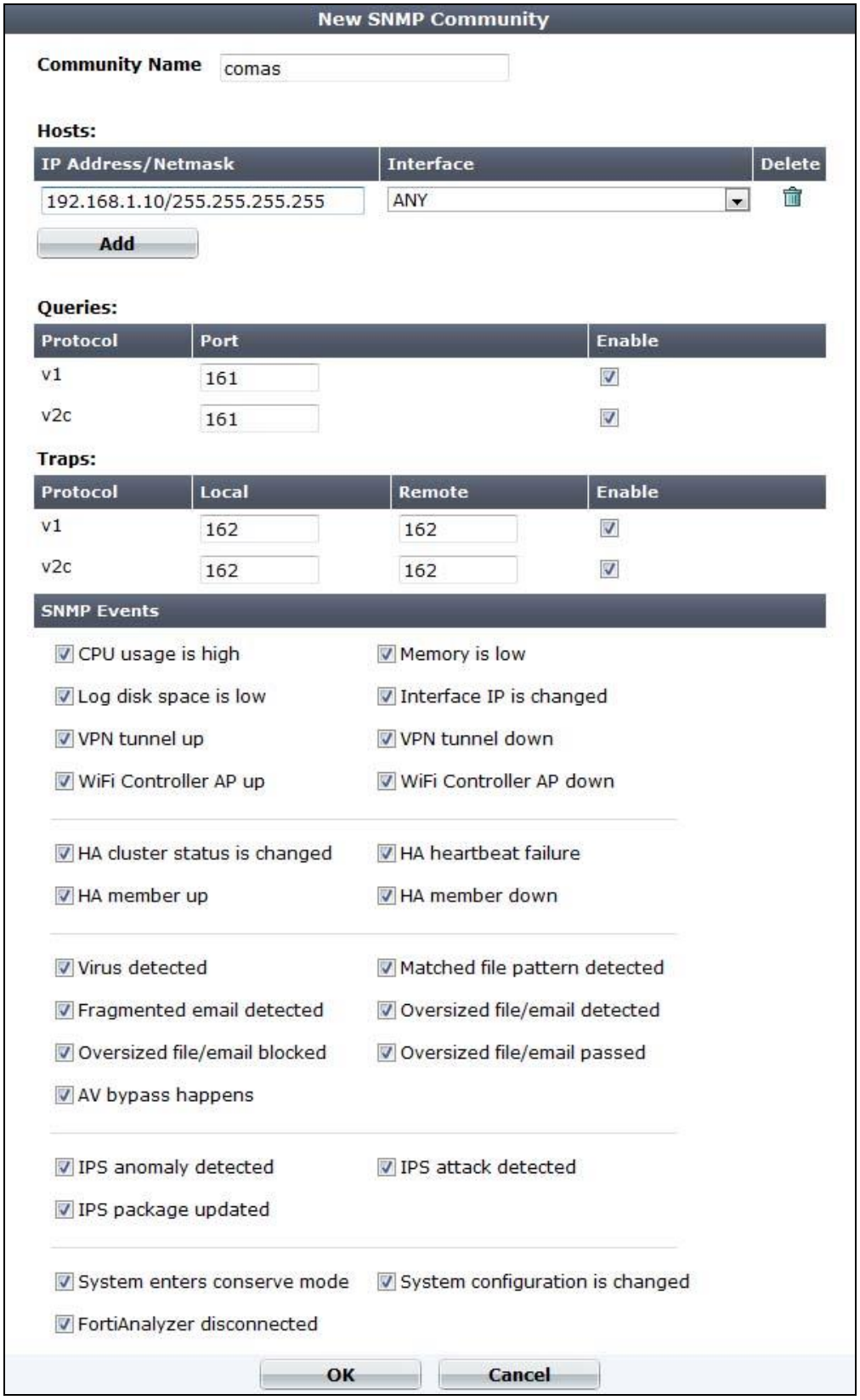
- HA 모니터링 화면 -

3-2. SNMP

SNMP(Simple Network Management Protocol)를 이용하여 Fortigate 시스템의 상태정보를 모니터링 할 수 있는 환경(MRTG, PRTG 등)을 구성 할 수 있습니다. SNMP 설정을 구성하려면 SNMP서버와 통신할 Fortigate의 인터페이스에 SNMP접근이 허용되어야 합니다. MIB파일은 SNMP설정 페이지에서 다운로드 할 수 있습니다.



- SNMP 에이전트 설정
  1. *System > Config > SNMP* 로 이동합니다.
  2. *SNMP Agent* 를 활성화 합니다.
  3. 에이전트에 대한 설명을 넣습니다.
  4. FortiGate 장비의 위치를 넣습니다.
  5. 관리자 정보를 넣습니다.
  6. *Apply* 를 누릅니다.

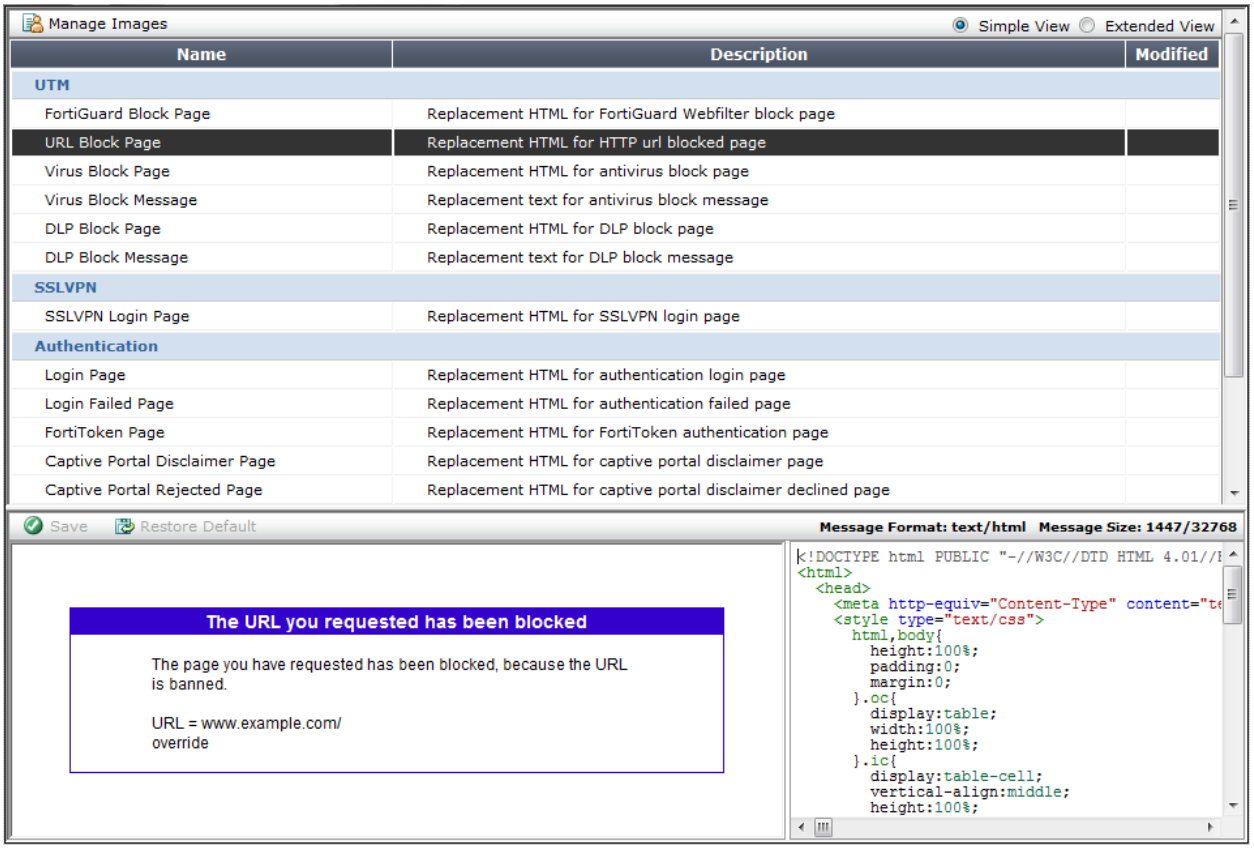


-SNMP 커뮤니티 설정 화면 -

- SNMP 커뮤니티 설정
  1. *System > Config > SNMP* 로 이동합니다.
  2. *SNMP v1/v2c* 에서 *Create New* 를 누릅니다.
  3. *Community Name* 을 설정합니다 .
  4. SNMP 연동할 SNMP 매니저의 주소를 설정합니다.
  5. SNMP 매니저와 통신할 포트를 설정합니다.
  6. SNMP 쿼리와 트랩을 설정합니다.
  7. *OK* 를 누릅니다.

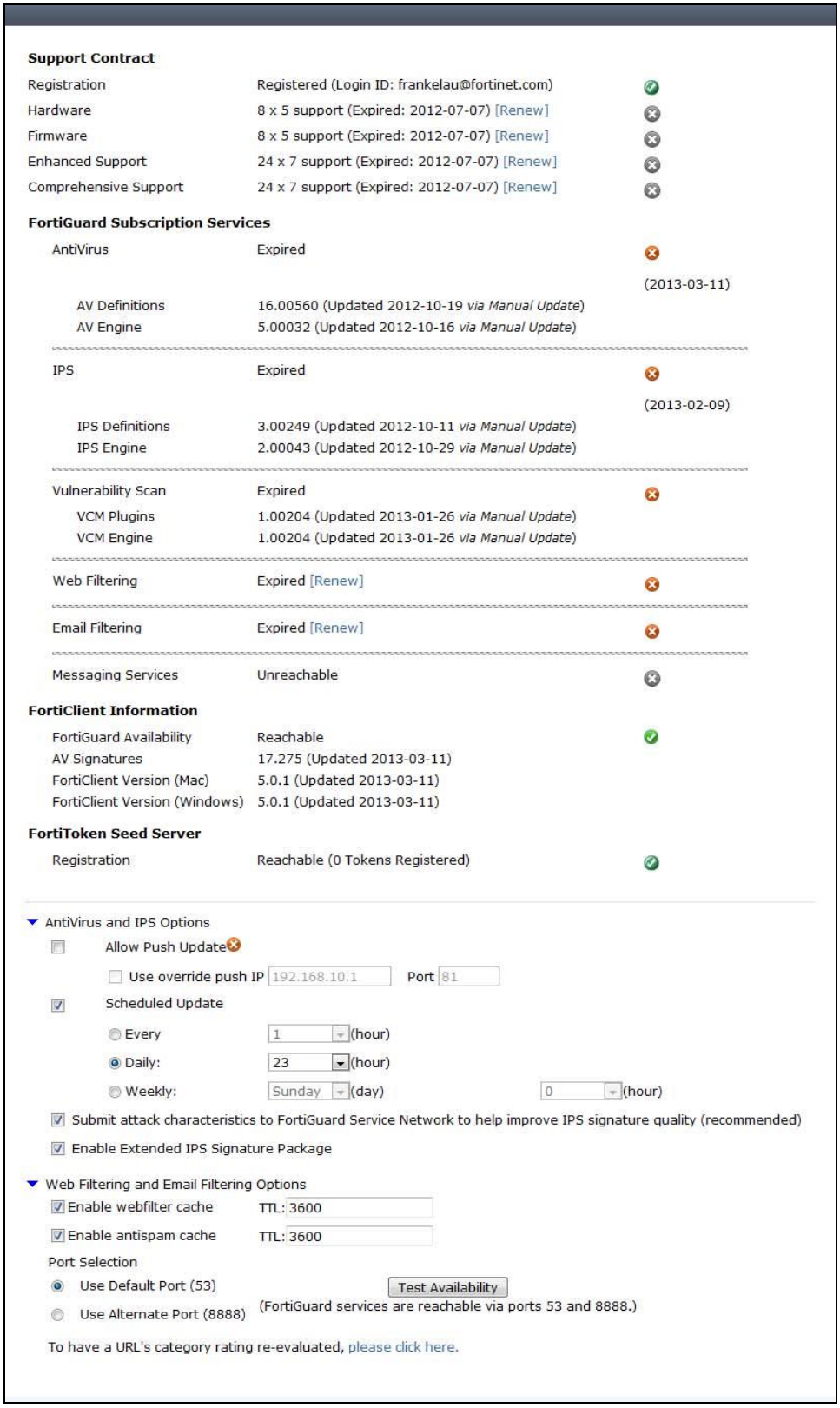
3-3. 대체메시지(Replacement Message)

Fortigate에서 제공하는 각종 차단 메시지, 로그인 화면 등 사용자에게 보여지는 메시지 화면을 편집 할 수 있습니다.



HTML 태그로 되어있기 때문에 간단히 메시지를 수정 할 수 있고, Manage Images 기능을 통하여 이미지를 넣을 수 있기 때문에 사용자에게 다양한 메시지를 보여줄 수 있습니다.

3-5. FortiGuard



FortiGuard메뉴에서는 Fortigate의 유지보수 라이선스 및 FortiGuard서비스 라이선스를 확인 할

수 있습니다. 또한 패턴 업데이트에 대한 설정을 할 수 있습니다.

Support Contract 장비의 등록 계정, 하드웨어 유지보수 등 시스템 지원 계약 정보를 확인 할 수 있습니다.

- **회색** Fortigate가 FDN에 도달 하지 못합니다.
- **오렌지** Fortigate가 FDN과 연결 되나 계약이 되어 있지 않습니다.
- **노란색** Fortigate의 라이선스가 만료되었습니다.
- **녹색** Fortigate의 라이선스가 유효한 상태 입니다.

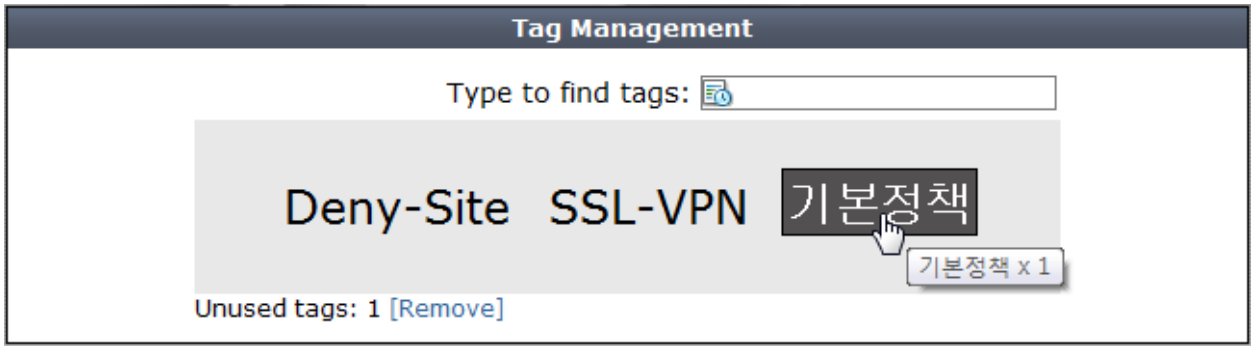
FortiGuard Subscription Services Fortigate장비의 FortiGuard 에서 제공 받는 서비스(AV, IPS등) 계약 정보를 확인 할 수 있습니다. 패턴 파일을 수동으로 업데이트 할 수 있습니다.

AntiVirus and IPS Options AV와 IPS의 자동 업데이트 설정을 합니다.

- **Allow Push Update** FDS에서 패턴을 푸시 업데이트 합니다.
- **Scheduled Update** 정해진 시간에 Fortigate가 업데이트를 시도합니다.

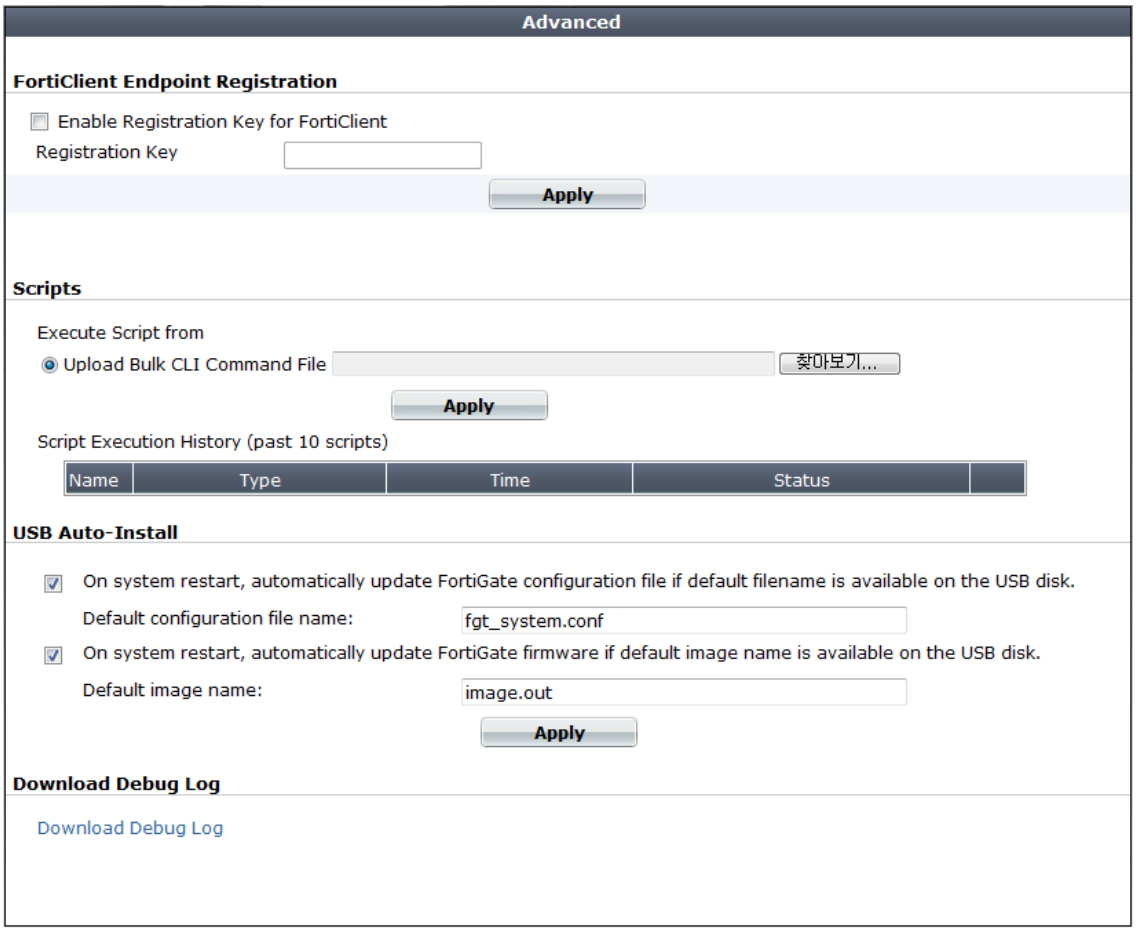
3-6. 태그 관리(Tag Management)

보안 정책의 관리 및 추적을 위한 기능입니다. 보안 정책 수립 시 특성을 나타내는 태그를 설정하면 태그관리에서 리스트를 확인 할 수 있습니다. 특정 태그에 마우스를 이동 하면 몇 개의 보안 정책이 적용되어 있는지 확인이 가능합니다.



3-7. 고급(Advanced)

스크립트를 이용하여 Configuration 설정을 하거나 USB를 이용하여 FortiOS, 설정파일을 Upload 하는 설정 등을 할 수 있습니다.



FortiClient Endpoint Registration　Fortigate시스템에서 FortiClient VPN에 사용 할 등록키를 설정합니다.

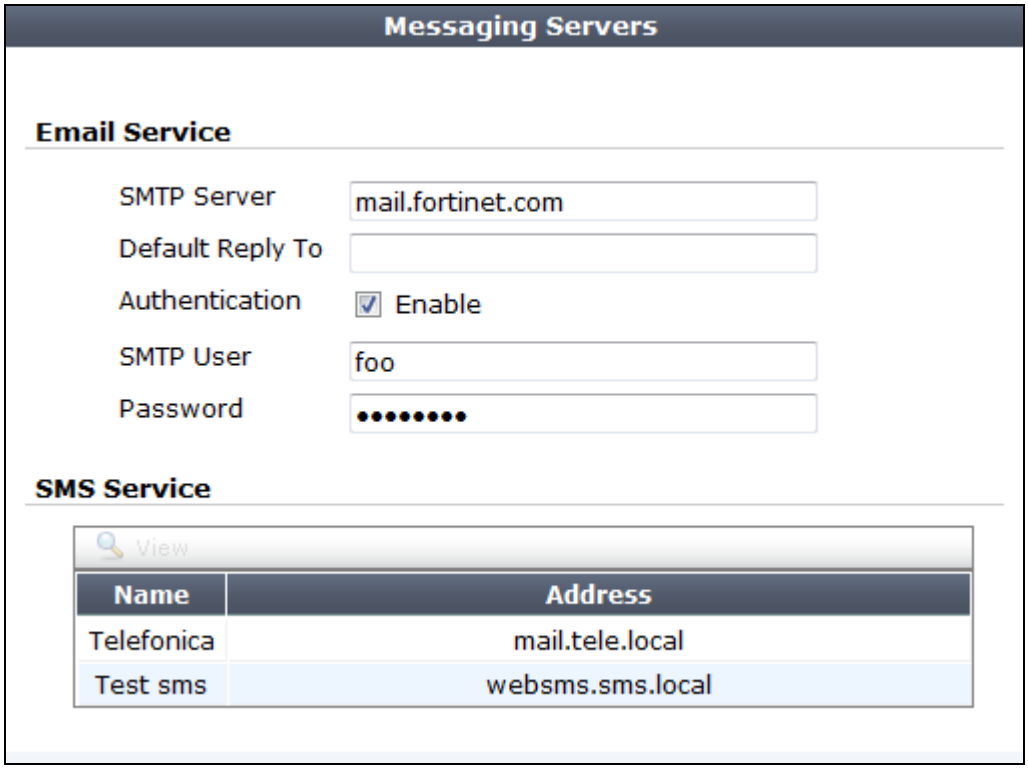
Scripts　Text로 된 스크립트 파일을 업로드 하여 간단하게 Fortigate시스템의 설정을 변경 할 수 있습니다.

USB Auto-Install　시스템 재 시작 시 USB를 이용하여 설정파일 및 FortiOS를 업로드 합니다.

Download Debug Log　디버그 로그를 다운로드 합니다.

3-8. 메시징 서버(Messaging Srervers)

Fortigat시스템이 관리자에게 메일을 보내거나 SMS를 보내기 위한 서버 설정을 합니다.

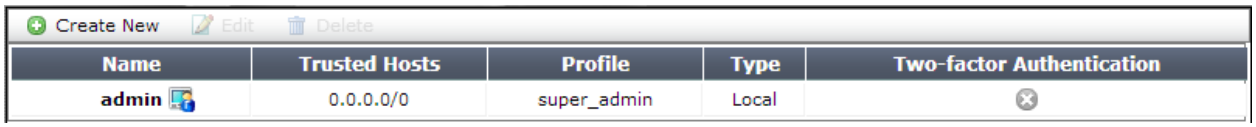


4. 관리자(Admin)

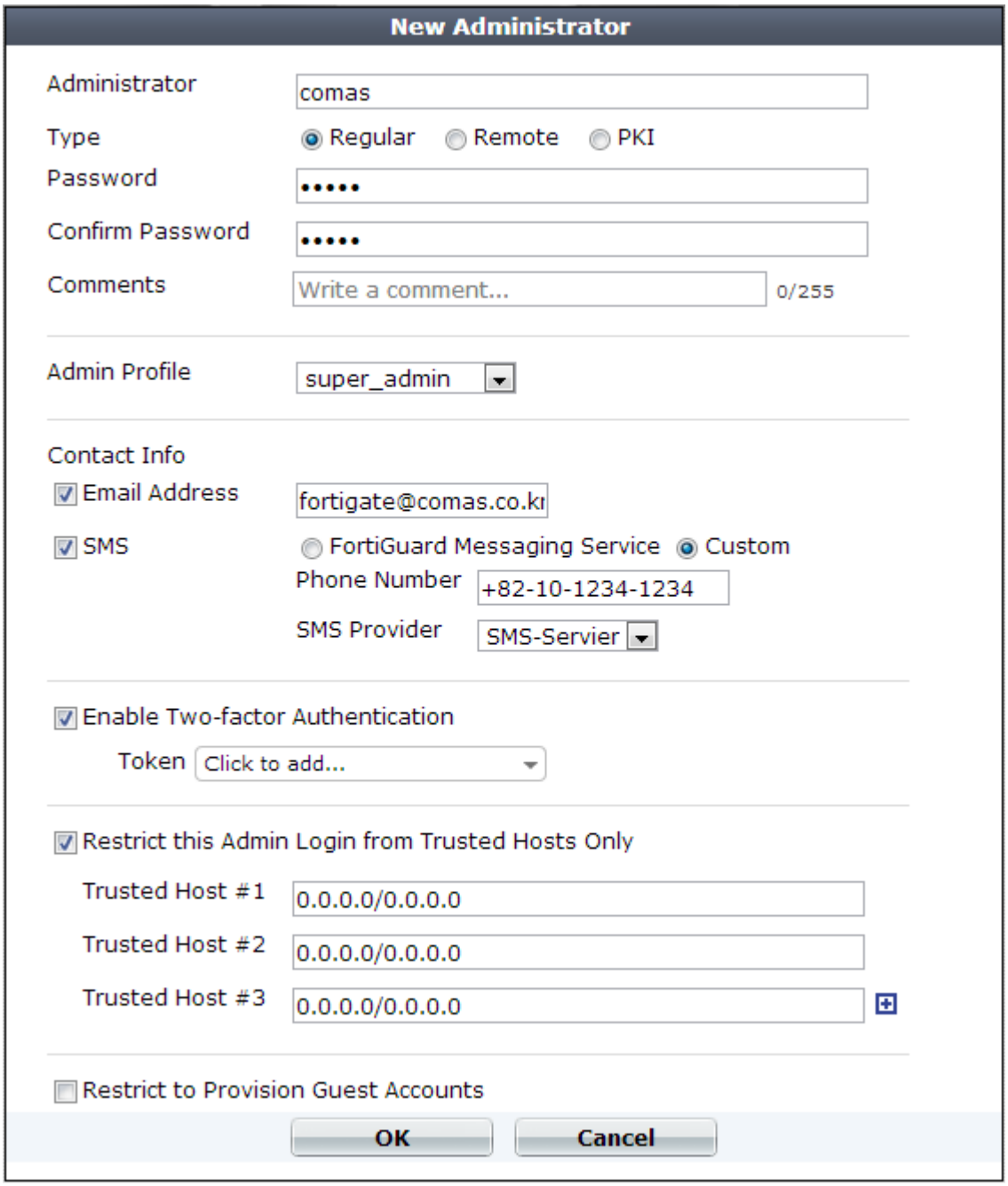
Fortiate 시스템의 관리자 계정, 패스워드, 접근권한 및 시스템 언어등을 설정할 수 있습니다.

4-1. 관리자(Administrators)

Fortigate 시스템의 관리자 계정을 생성, 삭제하고 설정 변경을 할 수 있습니다.



– 관리자 계정 리스트 화면 –



- 관리자 계정 생성 화면-

Administroator 관리자 계정 ID를 설정합니다.

Type 계정의 종류를 설정 합니다.

- **Regular** Fortigate에 로컬에 저장된 계정 정보을 이용합니다.
- **Remote** RADIUS, LDAP, TACACS+ 등 인증서버를 이용합니다.
- **PKI** 공개키 기반 구조를 이용하여 인증을 합니다.

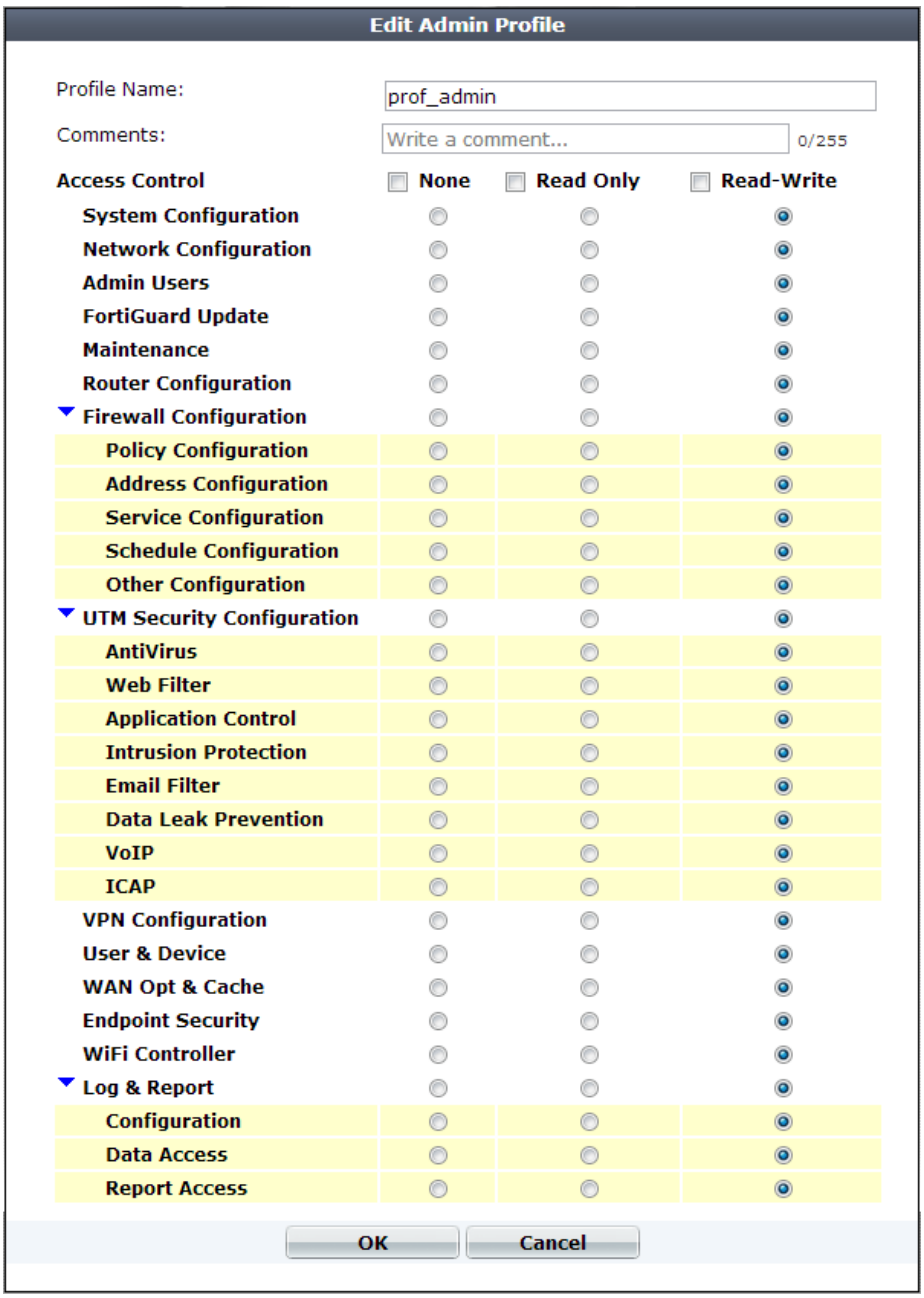
Password, Confirm Password 패스워드를 설정합니다.

Comments 계정에 대한 설명을 넣습니다.

Admin Profile	계정의 권한을 설정합니다.
Contact Info	관리자의 연락 정보를 설정합니다.
Enable Two-factor Authentication	관리자 접속시 포티토큰을 이용한 2Factor인증을 구현 합니다.
Restrict this Admin Login from Trusted Hosts Only	해당 계정의 접속 허용 IP를 설정합니다.
Restrict to Provision Guest Accounts	게스트계정만을 관리하는 관리자계정을 생성합니다. 이 기능을 활성화하면 Fortigate의 설정은 불가하고 특정 User Group에 계정을 생성, 삭제, 변경 만이 가능합니다.

4-2. 접근프로파일(Admin Profile)

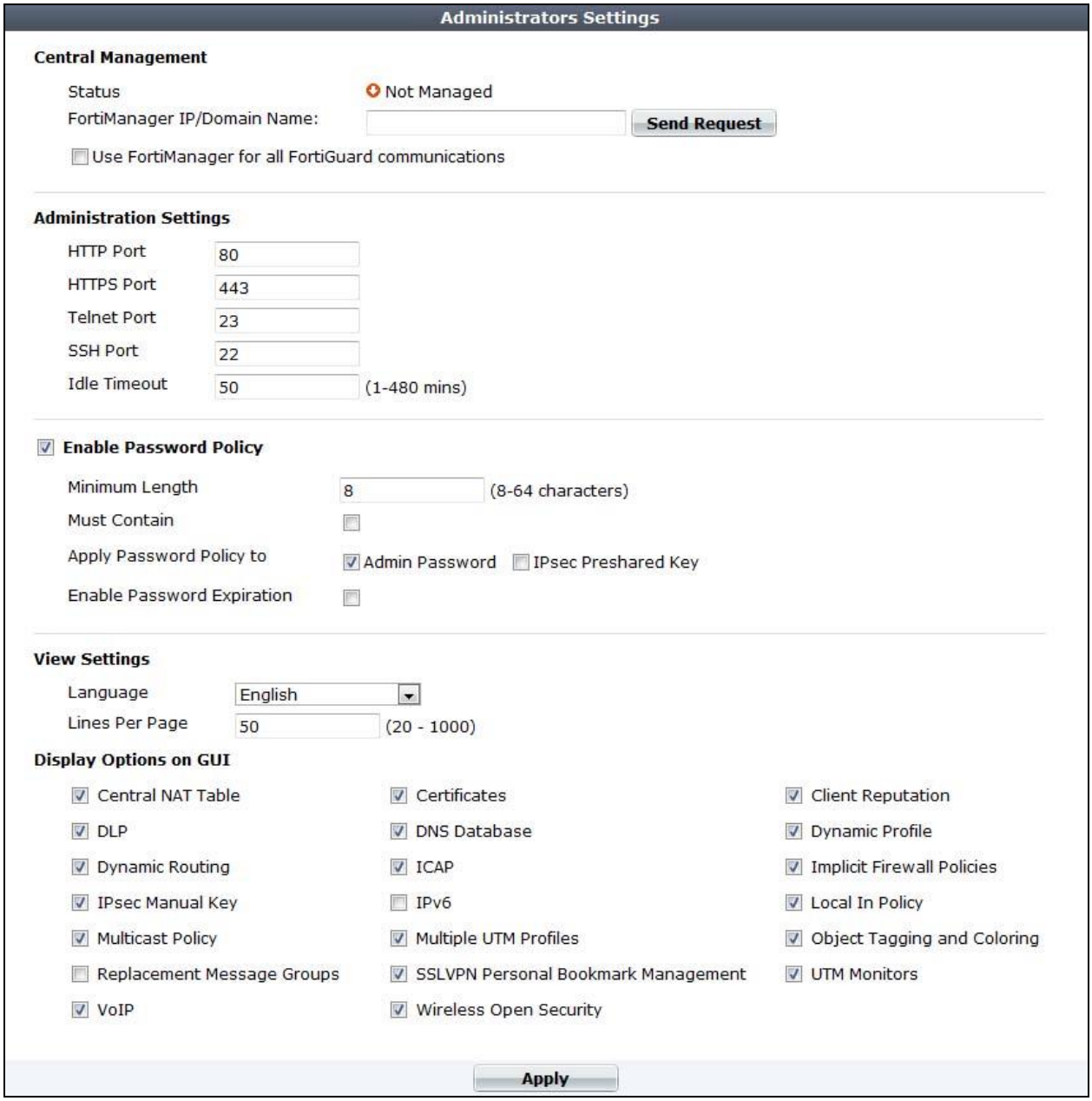
접근프로파일은 관리가 계정에 적용할 권한을 설정합니다. 각 계정 별로 다른 권한을 줄 수 있기 때문에 여러 명의 관리자가 있어도 서로 다른 권한을 줄 수 있습니다. Fortigate의 기본 계정인 admin 의 프로파일인 super_admin은 최상위 권한을 나타냅니다. **super_admin 프로파일은 시스템의 중요한 부분을 control 할 수 있는 권한이기 때문에 절대로 수정하면 안됩니다.**



- 접근프로파일 설정 화면 -

4-3. 설정(Settings)

Fortigate시스템의 관리접속 Port변경, 접속 유지시간 등을 설정 합니다. 8개국의 시스템 언어 설정이 가능하며 한국어를 지원합니다.



Central Management — Fortimanager와 연동을 합니다. Fortimanager는 여러 대의 Fortigate시스템과 연동 가능하며, 중앙집중적으로 장비를 관리할 수 있습니다.

Administration Settings — 장비에 접속 시 접근하는 Port를 설정합니다. 기본적으로 TCP 80, 443, 23, 22를 사용을 합니다.Fortigate의 인터페이스에 설정된 IP로 포트포워딩을 설정 할 경우 위 포트들은 충돌이 발생하기 때문에 구성을 할 수 없습니다.

Enable Password Policy — 관리자계정의 패스워드 정책을 설정합니다. 기본적으로는 비활성화 되어있어 패스워드 설정에 아무런 제약이 없습니다.

View Settings — 시스템 언어와 한 페이지에 보여지는 Line의 수를 설정합니다.

	Line Per Page는 20~1000줄 까지 변경이 가능하며, 로그페이지와 세션페이지에 적용됩니다.
Display Options on GUI	Fortigate 시스템의 추가적인 메뉴의 활성/비활성을 설정합니다. 기본적으로 보여지는 기능 이외의 기능을 설정할 경우 해당 기능에 활성 체크하여 설정을 합니다.

5. 인증(Certificates)

Fortigate시스템에서 사용자 인증이나 SSL 검사를 위한 인증서를 등록합니다.

1. 로컬 인증 (Local Certificates)

로컬 인증은 사설 인증서로 분류되며, 내부 기업 네트워크에서 사용됩니다. 인증파일에 개인키 파일이나 PEM(전자인증메일)을포함 합니다.

2. 원격(Remote)

원격인증은 개인키가 없는 공개인증서로 OCSP서버를 사용하여 인증을 받습니다.

3. CA 인증 (CA Certificates)

CA 인증은 로컬 인증과 유사하지만 인증서가 폭넓은 주소 범위나 회사 전체에 적용됩니다.

4. CRL

CRL(Certificate Revocation List) 인증서 폐지목록을 참고하여 인증서를 이용한 전자서명을 받았을 때 상대의 인증서가 폐지 되지 않았는지를 확인합니다.

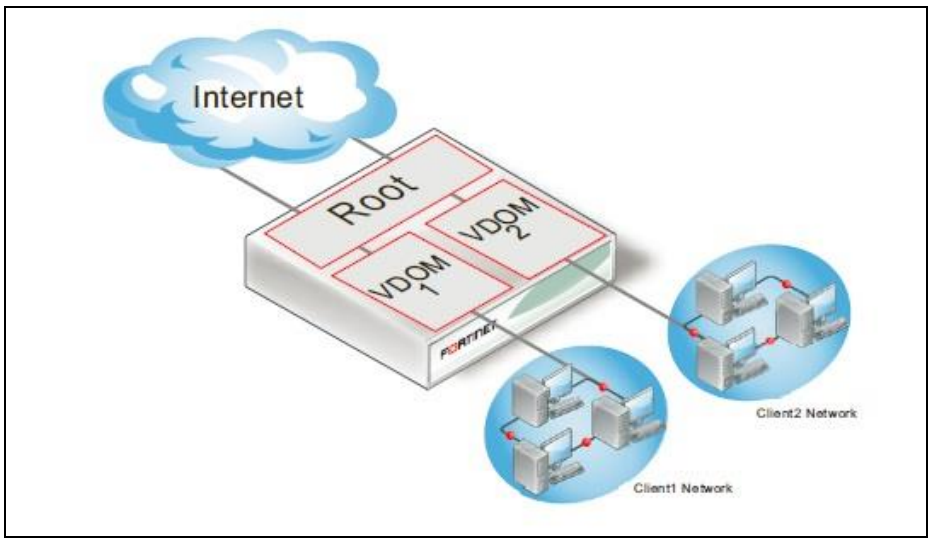
6. 모니터(Monitor)

1. DHCP 모니터 (DHCP Monitor)

2-3-2. DHCP Monitor(모니터링)을 참고 합니다.

7. 가상도메인(Virture Domains)

Fortigate시스템은 하나의 물리적인 Fortigate 장비에서 여러 개의 논리적인 Fortigate를 구성 할 수 있는 Vdom(Virture Domains)기능을 지원합니다.
생성된 각각의 Vdom은 방화벽 정책, 라우팅 및 VPN 서비스 등, 모든 것에 대해서 완전히 독립성을 가집니다. 이러한 기능은 한 대의 장비로 다수의 고객에게 각각의 방화벽 서비스를 제공 할 수 있는 장점이 됩니다. 기본적으로 10개의 Vdom을 지원하며 10개 이상의 Vdom구성 시 별도의 라이선스를 필요로 합니다.



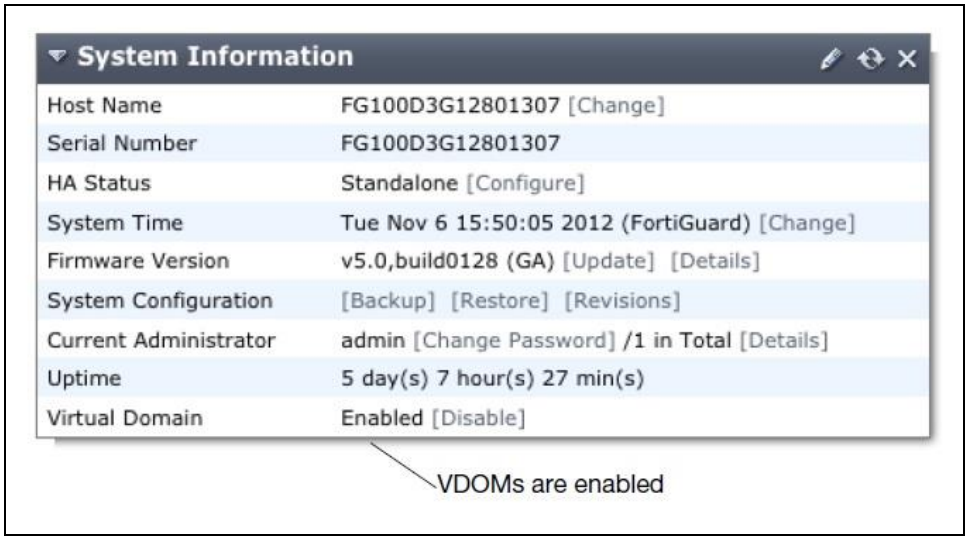
- 가상 도메인 개념도 -

기본적으로 Vdom 기능은 비활성화 되어있습니다.

7-1. 가상도메인 활성화 방법

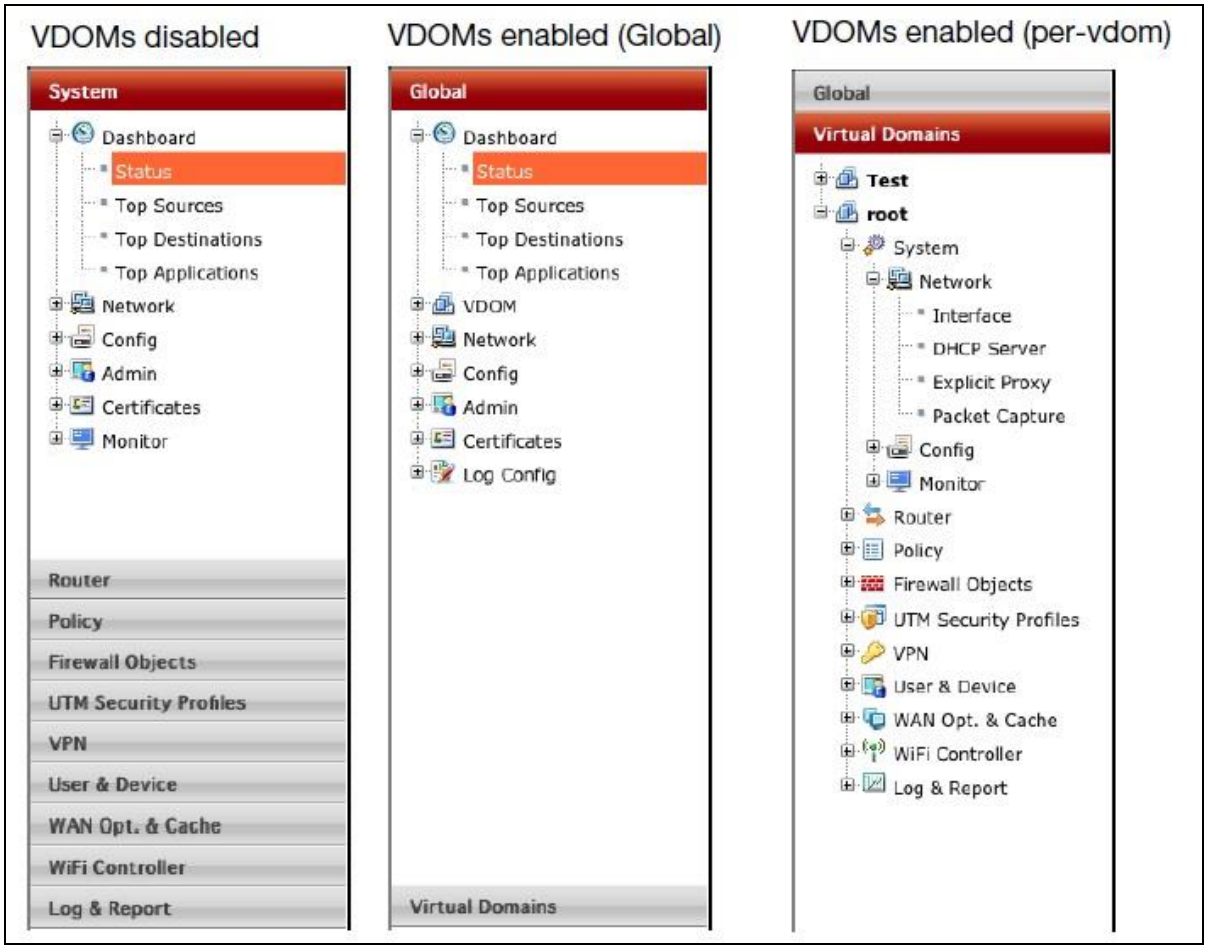
Super_admin 권한이 있는 관리자계정으로 로그인 합니다.

System > Dashboard > Status 로 이동 후 System Information 위젯의 Virtual Domain 항목을 Enable 후 확인을 선택 합니다.



- 가상도메인이 활성화 된 화면 -

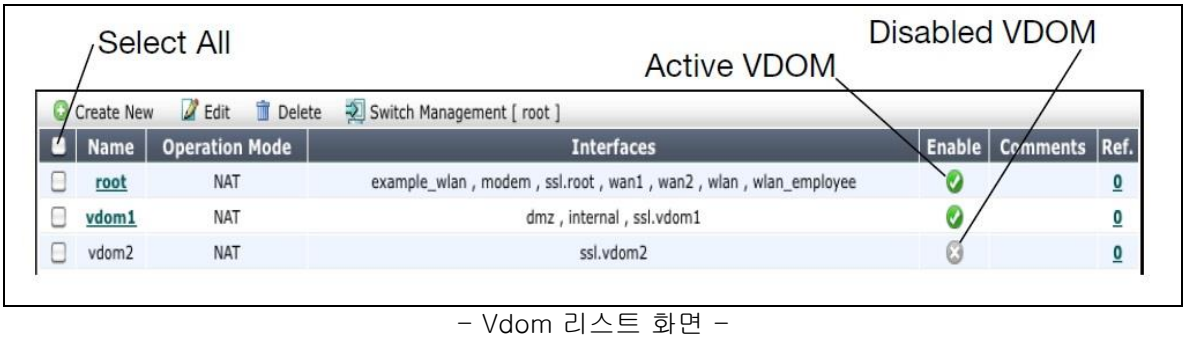
가상도메인 기능이 활성화 되면 Fortigate시스템의 메뉴 구성이 변경 됩니다. 기존 System 설정 메뉴가 Global로 옮겨져 장비의 전체적인 시스템 설정을 하고, Virtual Domains메뉴가 생기면서 각 도메인에 대한 보안 정책을 설정하게 됩니다.



– 가상 도메인 활성화 전, 후 메뉴의 변경 화면 –

7-2. 가상도메인 생성

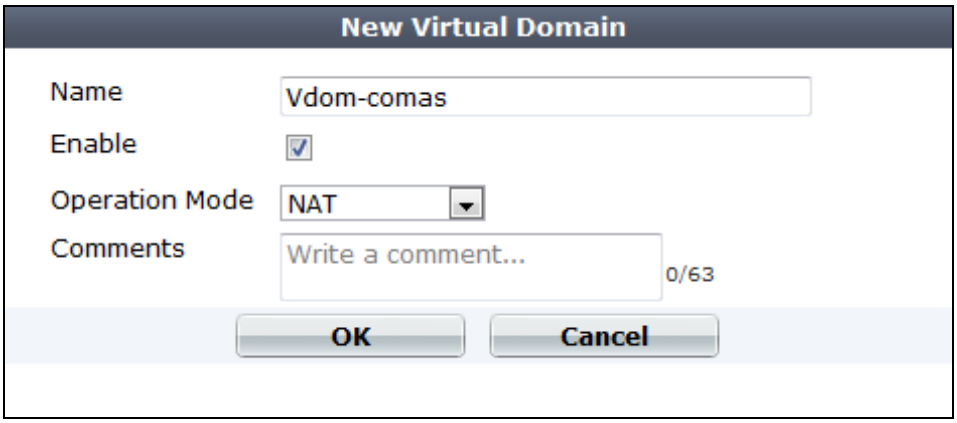
가상도메인의 생성은 *System > VDOM > VDOM* 메뉴에서 가능합니다. Vdom의 생성, 삭제는 Super_admin 권한의 관리자만이 할 수 있습니다.



– Vdom 리스트 화면 –

Create New 새로운 Vdom을 생성합니다.
Edit 선택된 Vdom의 설정을 변경합니다.
Delete 선택된 Vdom을 삭제 합니다.
Switch Management 관리권한을 가진 Vdom의 설정을 변경 합니다. 관리권한을 가진 Vdom

	을 통해서 패턴업데이트를 하기 때문에 관리도메인은 외부와 통신이 되어야 합니다.
Name	Vdom의 이름을 나타냅니다.
Operation Mode	해당 Vdom의 운영모드를 나타냅니다.
Interface	해당 Vdom에 할당 된 Interface를 보여 줍니다 .



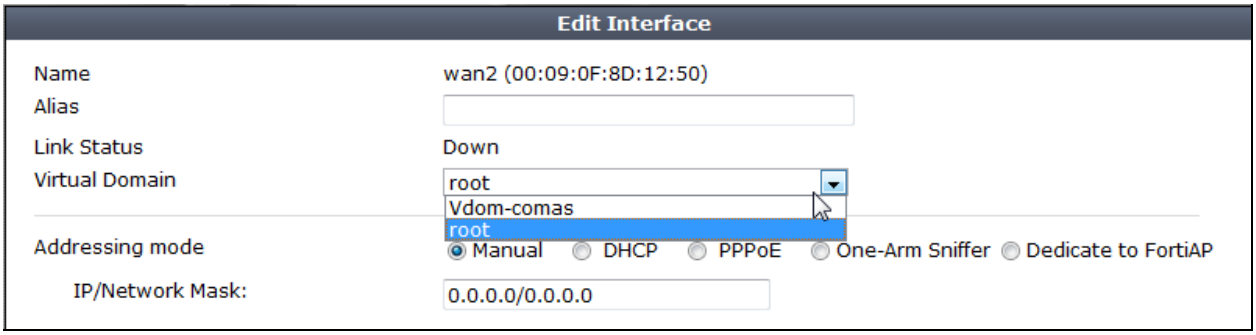
- 가상도메인 생성 화면 -

7-3. 가상도메인으로 인터페이스 할당

생성된 Vdom에 인터페이스를 할당해야 비로소 Vdom의 네트워크 구성을 할 수 있습니다. 인터페이스의 Vdom 할당 변경을 하기 위해서는 해당 인터페이스가 사용되고 있지 않아야 합니다. 인터페이스의 "Ref." 항목이 "0"이어야 할당이 가능합니다.

인터페이스 할당 방법은 다음과 같습니다.

1. *Global* > *Network* > *Interface* 로 이동하여 Vdom 변경을 할 인터페이스를 선택하고 Edit 버튼을 누릅니다.
2. Virtual Domain 항목에서 할당할 Vdom을 선택합니다.
3. OK를 누릅니다.



- 인터페이스 Vdom 변경 화면 -

이렇게 생성된 Vdom은 각각의 방화벽처럼 설정이 가능합니다. 또한 관리자 별로 접속할 수 있는 Vdom을 설정 할 수 있어 각 Vdom 설정에 대한 신뢰성을 가질 수 있습니다.

2. 라우터(Router)

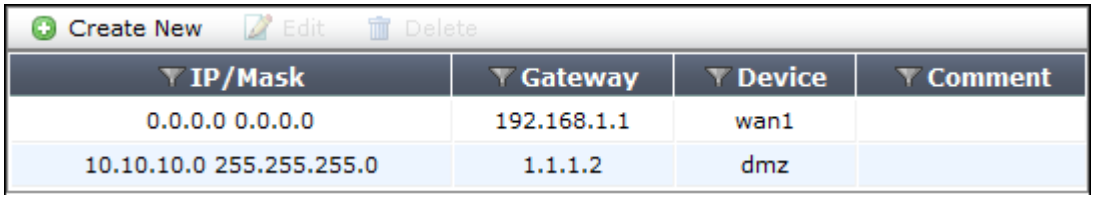
네트워크 통신을 위한 경로를 지정하는 기능으로 Fortigate는 정적(Static), 동적(Dynamic) PBR(Policy Based Routing)의 설정을 지원합니다. (TP모드의 경우 라우터 메뉴가 없습니다)

1.정적(Static)

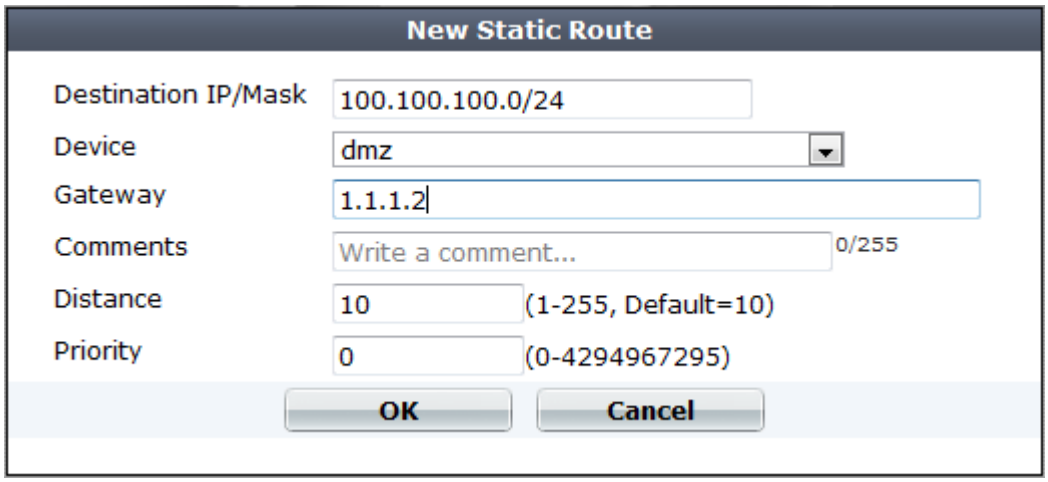
미리 Fortigate 시스템에 정의해 놓은 경로 설정에 의해 트래픽을 처리 합니다.

1-1. 정적(Static) 라우트

목적지 주소를 기준으로 경로를 지정합니다. 라우팅 간 우선순위 설정이 가능 하며 우선순위가 동일한 경우 서브넷이 작은 정책이 우선으로 처리 됩니다. Default Gateway의 목적지 주소는 0.0.0.0/0으로 설정 합니다.



- 정적 라우트 리스트 화면 -



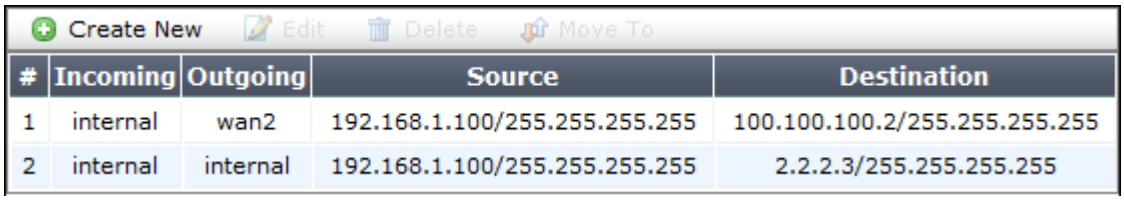
- 정적 라우트 설정 화면 -

Destination IP/Mask	경로설정을 할 목적지 주소를 설정 합니다.
Device	패킷을 내보낼 인터페이스를 설정 합니다.
Gateway	목적지 주소로 가기 위해 Fortigate가 패킷을 내보낼 장비의 IP를 설정합니다.
Distance	라우팅의 거리값(Distance)을 설정합니다. 값이 작을 수록 라우팅의 우선순위가 높습니다.

Priority 라우팅의 우선순위를 설정 합니다. 목적지 주소와 Distance 값이 동일 할 경우 Priority 값이 작은 라우팅의 우선순위가 높습니다.

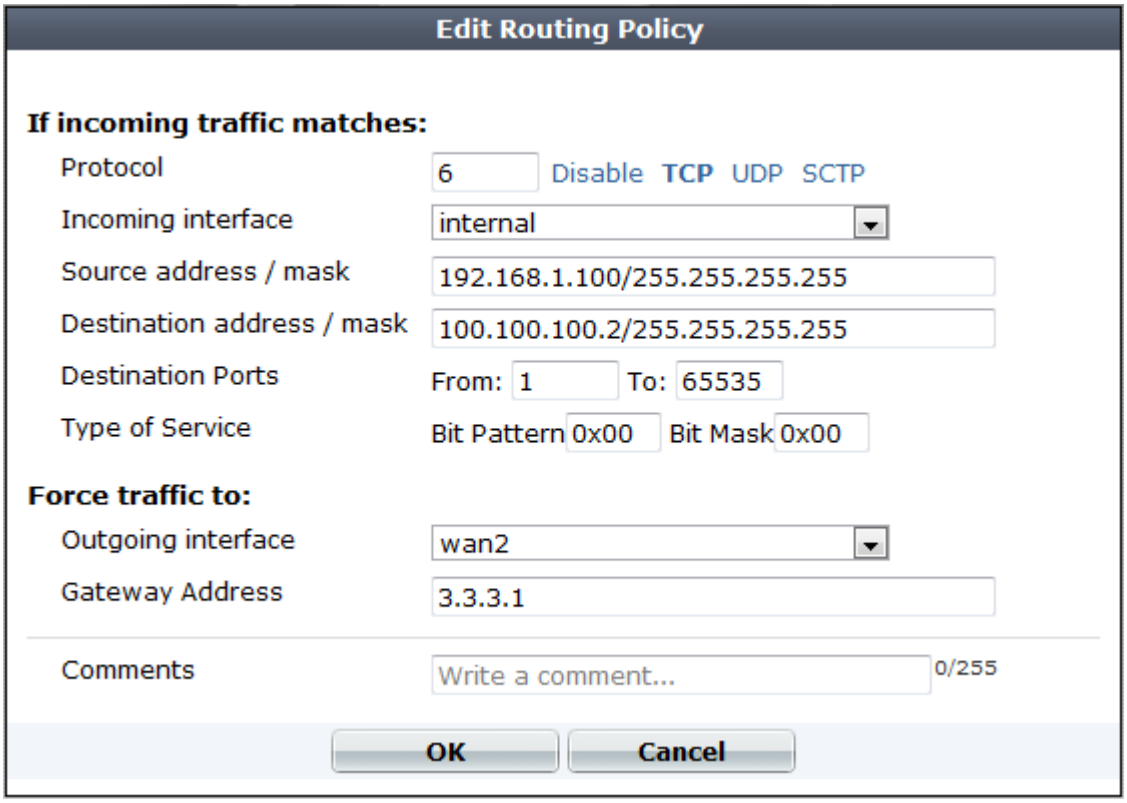
1-2. 정책(Policy) 라우트

프로토콜, 유입 인터페이스, 출발지 주소, 목적지 주소, 목적지 포트를 기준으로 경로를 지정합니다. 라우팅 간의 우선순위는 정책 라우트 리스트에서 상위에 있을 수록 우선순위가 높습니다. 정적라우트 보다 우선순위가 높고, 기준이 여러 가지 이기 때문에 다양한 경로설정이 가능합니다.



#	Incoming	Outgoing	Source	Destination
1	internal	wan2	192.168.1.100/255.255.255.255	100.100.100.2/255.255.255.255
2	internal	internal	192.168.1.100/255.255.255.255	2.2.2.3/255.255.255.255

- 정책 라우트 리스트 화면 -



- 정책 라우트 설정 화면 -

"If incoming traffic matches"의 조건을 만족하는 패킷은 Force traffic to에 정의된 게이트웨이로 보냅니다.

Protocol 목적지 포트의 프로토콜을 설정합니다.

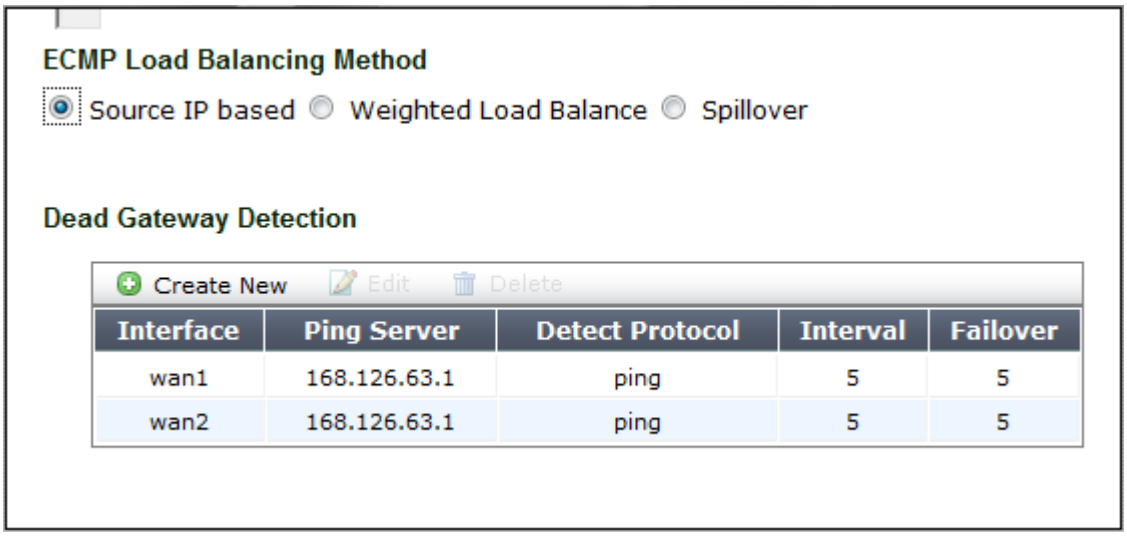
Incoming interface 패킷의 유입 인터페이스를 설정합니다.

Source address / mask 출발지 주소를 설정합니다.

Destination address / mask	목적지 주소를 설정합니다.
Destination Ports	목적지 포트를 설정합니다.
Outgoing interface	패킷을 내보낼 인터페이스를 설정합니다.
Gateway Address	패킷을 내보낼 장비의 IP를 설정합니다.

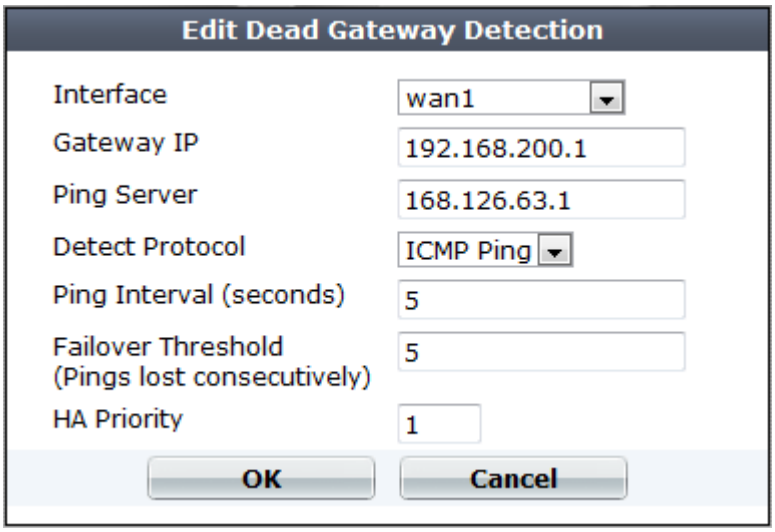
1-3. 설정 (Settings)

Fortigate시스템은 ECMP(Equal Cost Multi Path)를 이용하여 두 개 이상의 회선으로 구성 되어 있을 때 동일한 목적지주소에 대해서 트래픽 분산처리를 합니다. ECMP를 사용하기 위해서는 모든 회선의 라우팅 설정 우선순위가 동일해야 한다. (Distance, Priority 값이 동일해야 함)



- ECMP 설정 화면 -

ECMP Load Balancing Method	로드밸런싱의 방식을 선택합니다.
Source IP based	출발지 주소를 기준으로 밸런싱을 합니다.
Weighted Load Balance	인터페이스에 할당 된 Weight값을 기준으로 밸런싱 합니다. Weight값이 높은 인터페이스로 더 많은 트래픽이 처리 되도록 보내집니다.
Spillover	인터페이스에 설정된 임계값을 기준으로 밸런싱을 합니다. 가장 낮은 값을 가진 인터페이스로 우선 보내지고 임계값을 넘어가면 다음으로 낮은 값의 임계값을 가진 인터페이스로 트래픽이 보내집니다.
Dead Gateway Detection	회선 Healthcheck를 위한 설정입니다. Ping Server 항목으로 Ping, TCP echo, UDP echo 등을 체크하여 회선상태를 확인합니다. Ping Server로 응답체크가 안되면 해당 회선을 장애로 판단하고 라우팅 처리를 하지 않습니다.



- Dead Gateway Detection 설정 화면 -

2. 동적(Dynamic)

네트워크 장비 간의 라우팅 정보를 이용하여 효율적인 경로를 산출하여 트래픽을 처리 합니다.
Fortigate시스템은 RIP(V1, V2), OSPF, BGP, Multicast 라우팅 프로토콜을 지원합니다.
(자세한 설정 방법은 docs.fortinet.com에서 Routing 문서를 참고하시기 바랍니다.)

3. 모니터(Monitor)

Routing Monitor Fortigate시스템에서 운용중인 라우팅 테이블 정보를 확인 할 수 있습니다.

Type	Subtype	Network	Gateway	Interface	Up Time
Static		0.0.0.0/0	192.168.200.254	wan1	
Connected		192.168.1.0/24	0.0.0.0	internal	
Connected		192.168.10.0/24	0.0.0.0	FortiAP-comas	
Connected		192.168.200.0/24	0.0.0.0	wan1	

- 라우팅 모니터 화면 -

3. 정책(Policy)

Fortigate시스템은 정책(Policy)을 기반으로 방화벽 기능을 수행합니다. Stateful Inspection 방식(처음 세션을 생성하기 위해 패킷이 지나가면 방화벽은 세션테이블을 생성하고 이 정보를 기반으로 응답해오는 패킷을 통과 시킴)을 지원하여 패킷 기반의 초기 방화벽 보다 정책의 수가 적고 처리속도가 뛰어납니다.

1. 정책(Policy)

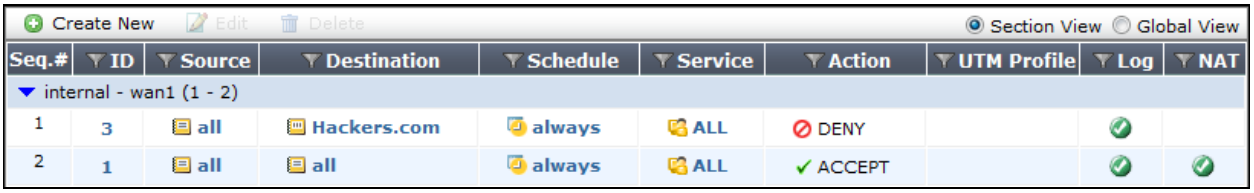
IP주소와 서비스포트를 기반으로 하는 방화벽 정책을 설정하고 Fortigate에서 제공하는 UTM , VPN, 사용자 인증 등의 정책을 설정합니다. 인터페이스를 기준으로 Internal 구간의 내부사용자를 Local, Wan 혹은 External 의 사용자를 Remote 라 가리키고 정책은 다음과 같은 방향성으로 나타냅니다.

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

1-1. 방화벽 정책(Firewall Policy)

Fortigate시스템의 방화벽 정책은 4가지 기준(출발지주소, 목적지주소, 스케줄, 서비스포트)으로 정책의 적용여부를 결정 합니다.

정책의 우선순위는 정책 섹션 별로 제일 상위의 정책(Seq 넘버가 작은)부터 순서대로 적용됩니다. 그렇기 때문에 정책 적용의 기준이 되는 객체들의 범위가 작은 정책이 상위에 위치해야 합니다.

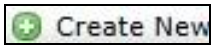


위 그림과 같이 내부사용자가 외부로 모든 통신이 가능하되 Hackers.com 사이트를 막고자 한다면 목적지 범위가 작은 ID 3번 정책이 ID 1번 보다 상위에 위치해야 합니다. 정책의 ID번호는 우선순위와는 상관이 없습니다.

정책페이제의 오른쪽 상단의 Global View 보기를 선택하면 정책 통합 보기로 변경 됩니다.

1-2. 정책의 생성, 편집 및 삭제 (Create, Edit & Delete)

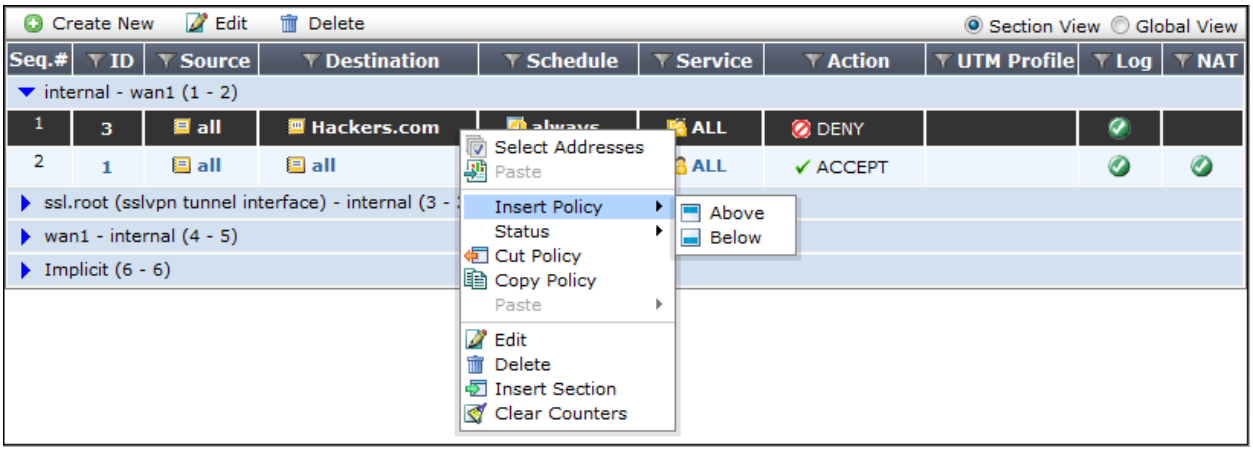
방화벽 정책을 생성하는 방법은 2가지를 제공합니다.

첫 번째,  버튼을 눌러 생성이 가능합니다. 이 경우 해당 정책섹션의 제일 하위에 생성이 됩니다.

두 번째, 정책을 생성할 위치의 위, 아래 정책 중 하나를 선택하고 오른쪽 클릭을 하면 팝업 메뉴가 나타납니다. 메뉴 중 Insert Policy > Above(위) / Below(아래)를 선택하여 생성을 할 수 있습니다.

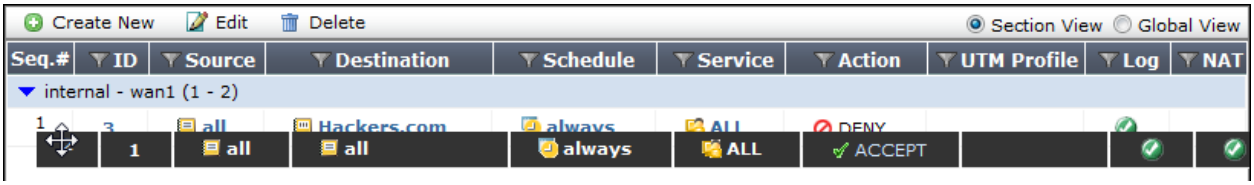
정책의 편집은 해당 정책을 선택 하고 정책 상위에 있는Edit 아이콘  을 눌러 편집 할 수 있고,

Delete 아이콘  을 눌러 삭제 할 수 있습니다.



- 메뉴 팝업 화면 -

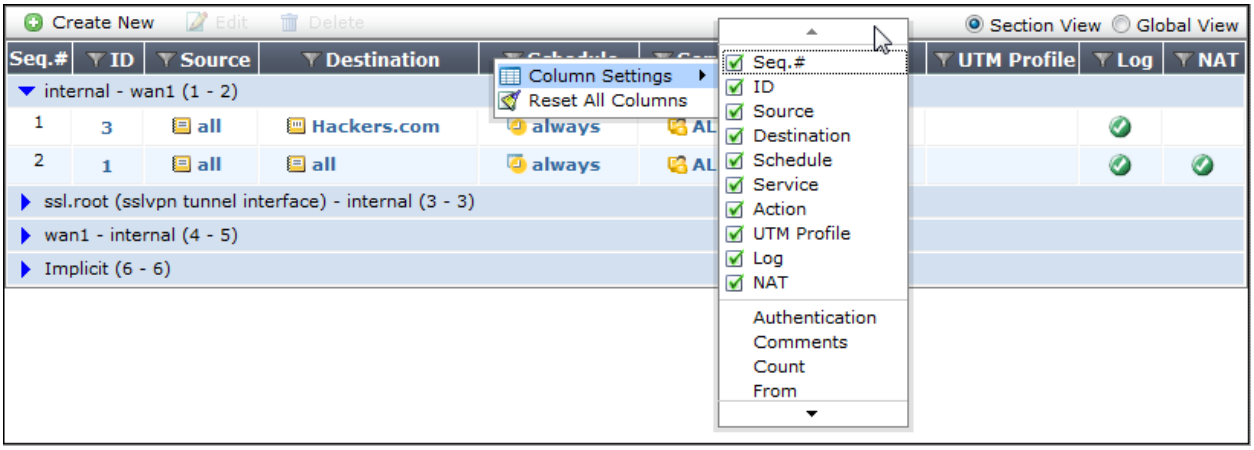
정책의 위치를 이동하기 위해서는 해당 정책의 왼쪽 끝 부분(Seq 넘버 부분)을 마우스로 드래그 하여 이동할 위치로 옮길 수 있습니다.



- 정책 이동 화면 -

1-3. 컬럼 설정(Column Setttings)

방화벽 정책 리스트에서 보여지는 컬럼을 설정 할 수 있습니다. 정책 리스트 페이지의 컬럼 바에서 마우스 오른쪽 클릭을 하면 팝업 메뉴가 나타납니다. Column Setting에서 항목을 선택하면 해당 항목이 추가 됩니다.



컬럼 항목

Source	출발지 주소
Destination	목적지 주소
Schedule	스케줄(일회성, 반복 등)
Service	서비스 포트
Action	ACCEPT= 허용, DENY= 차단, IPsec= IPsec VPN , SSL-VPN =

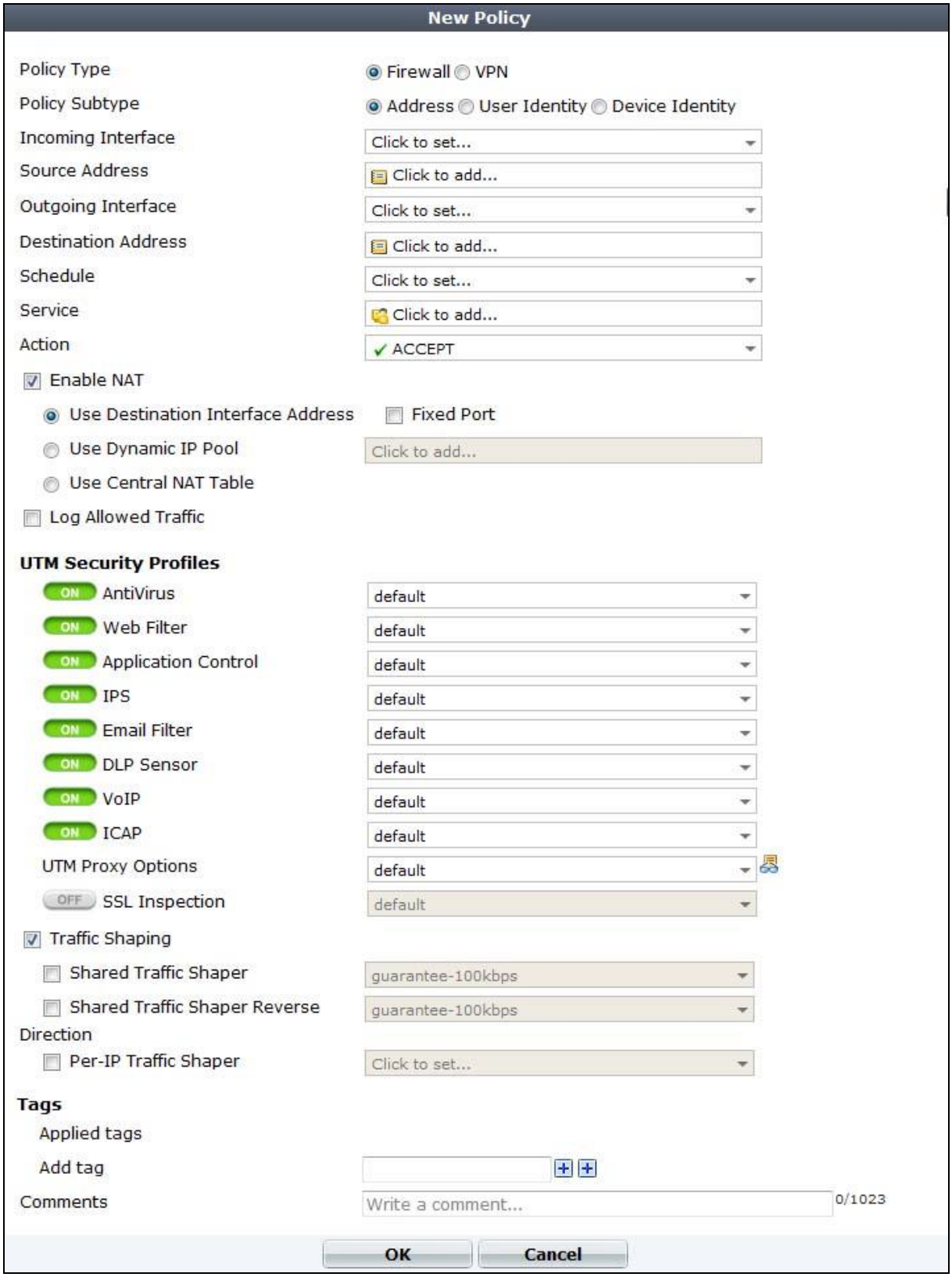
	SSL VPN
UTM Profile	UTM 프로파일 적용 내역
Log	= 활성화 , = 비활성화
NAT	= 적용 , 공란 = 미적용
ID	정책의 생성 순서
Status	= 정책활성화, = 정책비활성화
Authentication	사용자 및 Device 별 인증
Comments	주석
Count	해당 정책의 총 사용 트래픽 현황
From	출발지 인터페이스
Seq.#	정책 우선 순위
To	목적지 인터페이스
Tunnel	VPN 터널 이름

1-4. 정책 설정

Fortigate시스템은 Address(IP주소), User Identity(사용자), Device Identity 의 3가지 기준으로 방화벽 정책을 설정 할 수 있습니다. **내부 IP가 사설인 경우 외부와 통신을 하기 위해서는 NAT 기능을 활성화 해주어야 합니다.(기본은 비활성화 되어있음)**

1-4-1. 주소 정책 (Address)

출발지 IP, 목적지 IP 객체를 이용하여 정책을 설정합니다.



– Address 정책 설정 화면 –

Policy Type	방화벽 정책 설정 시 Firewall을 선택합니다.
Policy Subtype	Address 정책 설정 시 Address를 선택합니다.
Incoming Interface	유입 인터페이스를 설정합니다.
Source Address	출발지 주소를 설정합니다.
Outgoing Inteface	내보낼 인터페이스를 설정합니다.
Destination Address	목적지 주소를 설정합니다.
Schedule	스케줄을 설정합니다.
Service	서비스포트를 설정합니다.
Action	정책의 동작 형태를 설정합니다.
Enable NAT	NAT의 사용 여부를 선택합니다.
Use Destination Interface Address	내보낼 인터페이스의 IP로 NAT 됩니다.
Use Dynamic IP Pool	미리 정의해 놓은 Pool 대역으로 NAT 됩니다.
Use Central NAT Table	Central NAT를 사용합니다.
Log Allowed Traffic	정책에 적용 받는 트래픽의 로그를 발생합니다.
UTM Security Profiles	UTM기능을 적용합니다. UTM기능을 사용하기 위해서는 해당 기능을 활성화 시키고 적용할 Profile을 설정하여야 합니다. OFF UTM 비활성화 , ON UTM 활성화
Traffic Shaping	트래픽의 대역폭을 조절하는 기능입니다. 정책을 기준으로 일정 사용량을 쓰지 못하게 하거나 IP별로 트래픽을 조절 할 수 있습니다.
Shared Traffic Shape	일반적인 outbound 트래픽에 대한 보장 대역폭.
Shared Traffic Shaper Reverse	Inbound 트래픽에 대한 보장 대역폭
Per-IP Traffic Shaper	IP별 트래픽에 대한 보장 대역폭.

1-4-2. 사용자 인증 정책 (User Identity)

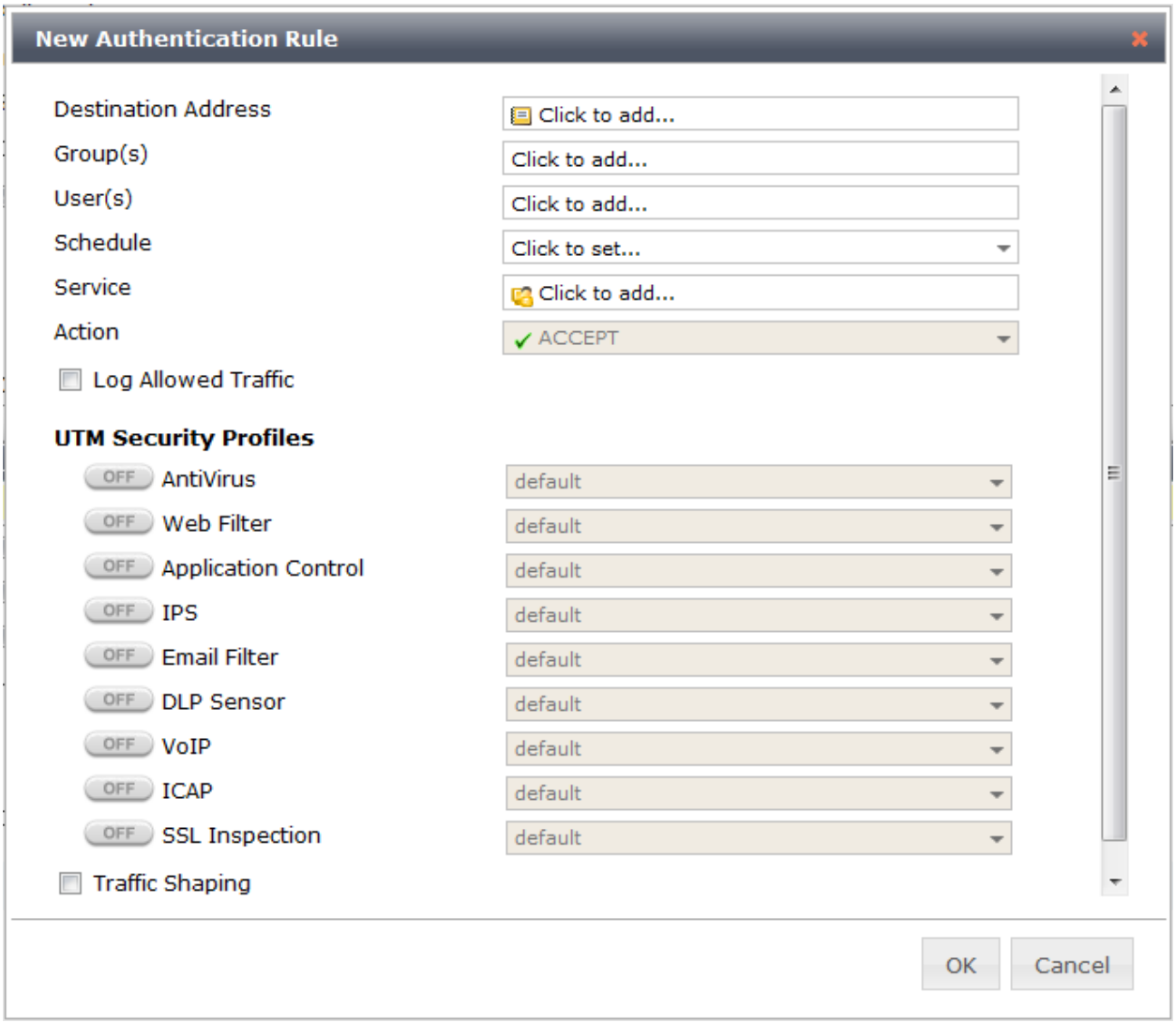
사용자 인증을 통하여 정책을 설정합니다.

- 사용자 인증 화면 -

사용자 인증 정책은 기본 Address 정책에 사용자의 ID/PW 인증을 통하여 네트워크 접속자에 대한

신뢰를 높임으로써 보안을 강화 할 수 있습니다. 사용자 생성은 User & Device에서 할 수 있고, 생성 후 정책의 Group(s), User(s) 항목에서 해당 객체를 사용할 수 있습니다.

Policy Subtype을 User Identity로 설정하고 Configure Authentication Rules의 Create New 버튼을 눌러 사용자 인증 정책을 생성합니다.

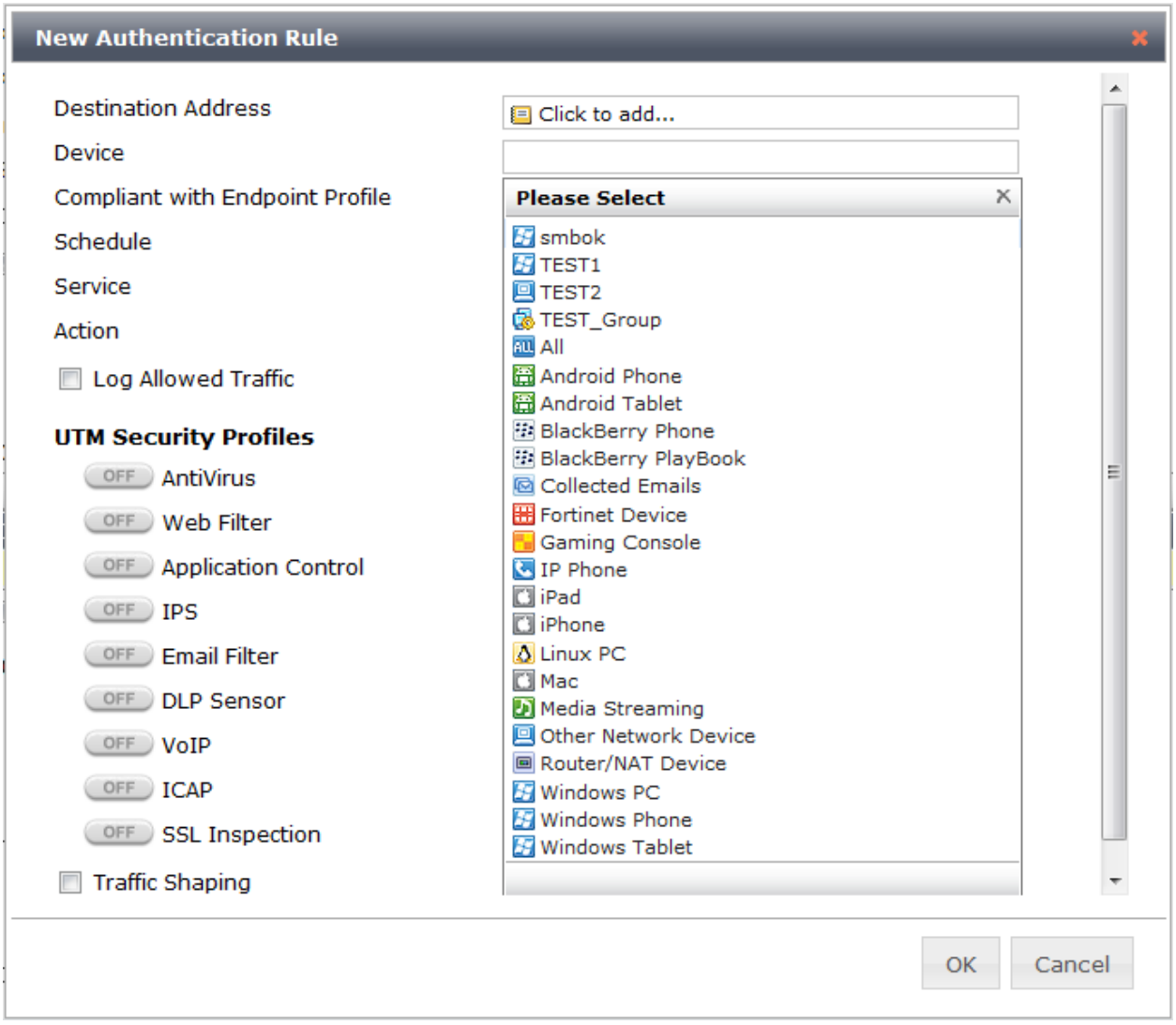


- 사용자 인증 정책 설정 화면 -

Group(s) 인증을 허용할 그룹입니다.
User(s) 인증을 허용할 사용자 입니다.

1-4-3. 장치 정책 (Device Identity)

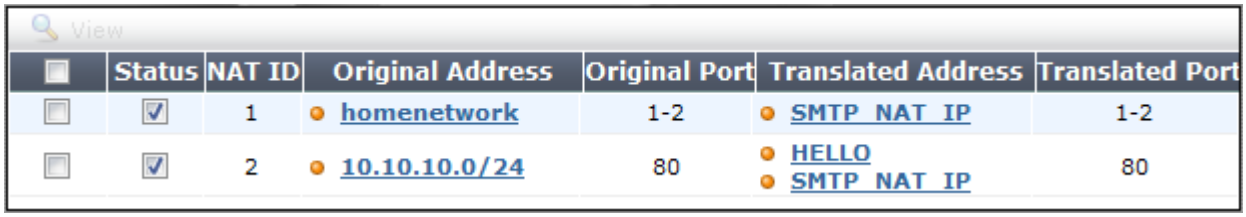
장치의 MAC주소나 장치 타입을 기준으로 정책을 설정합니다. 장치 객체 생성은 User & Device에서 할 수 있습니다.



– Device Identity 정책 설정화면 –

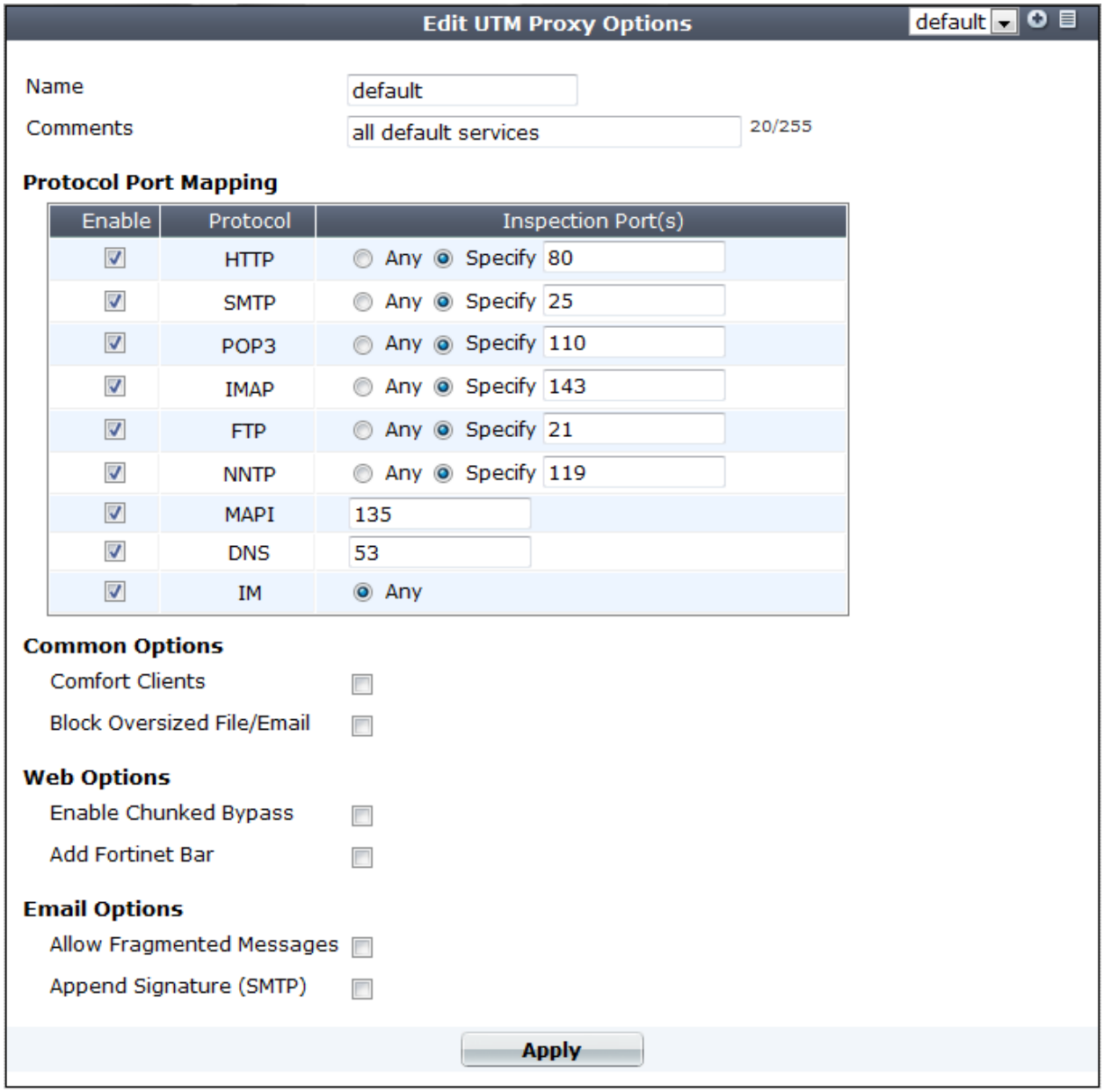
2. 중앙 NAT 테이블(Central NAT Table)

미리 정의해 놓은 NAT 테이블을 정책에 적용함으로써 각각의 NAT정책을 만들지 않고 하나의 정책으로 여러 개의 NAT 정책을 처리 할 수 있습니다. NAT 테이블의 우선순위는 상위 정책이 우선 합니다. 정책 설정화면에서 NAT항목을 Use Central NAT Table로 설정하고 적용할 테이블을 선택하면 적용됩니다.



3. UTM Proxy 옵션

UTM 기능들이 참고 할 프로토콜들의 설정 입니다. 프로토콜 별 포트 및 옵션을 설정합니다.



– UTM Prosy 옵션 설정 화면 –

Comfort Clients — 프록시 기반의 AV 기능이 수행 될 경우 Fortigate에서 파일을 버퍼링하고 스캔하는 동안 회선 속도가 느린 경우 사용자는 약간의 Delay현상이 발생 할 수 있습니다. 때문에 사용자가 정상적으로 파일의 전송이 진행되고 있다는 것을 알려 주는 옵션입니다.

Block Oversized File/Email — 설정된 임계 값 이상의 파일이나 Email에 대하여 차단을 합니다.

Enable Chunked Bypass — HTTP 섹션은 "Chunked Bypass"의 사용으로 허용한다 HTTP의 버전 1.1의 메커니즘을 보면 웹 서버는 동적으로

생성된 chunks 을 보내기를 시작하고 실제 내용의 크기를 알기 전에 요청에 대한 응답을 하는 것 허용한다. 동적으로 생성된 콘텐츠는 Http request 에 대한 초기 응답이 더 빠른 다는 것을 의미하기 때문에 문제가 된다. 이것은 보안 기준점에서는 콘텐츠가 전체 파일이 되기 전에는 Proxy에서 수행되지 않는다는 것을 의미한다

Add Fortinet Bar

Fortigate를 통하여 웹 페이지에 접속 할 때마다 페이지 오른쪽 상단에 

Fortinet Top Bar를 표시 합니다. Fortinet Top Bar는 Fortigate로 인증을 받은 사용자에게 사용자에 대해 아래 정보들을 보여줍니다.

- Application 제어 위반
- Endpoint 제어 시행
- 웹 브라우징 할당량
- 인증된 사용자의 ID(로그아웃 가능)
- SSL VPN 상태 및 즐겨찾기

Allow Fragmented Messages

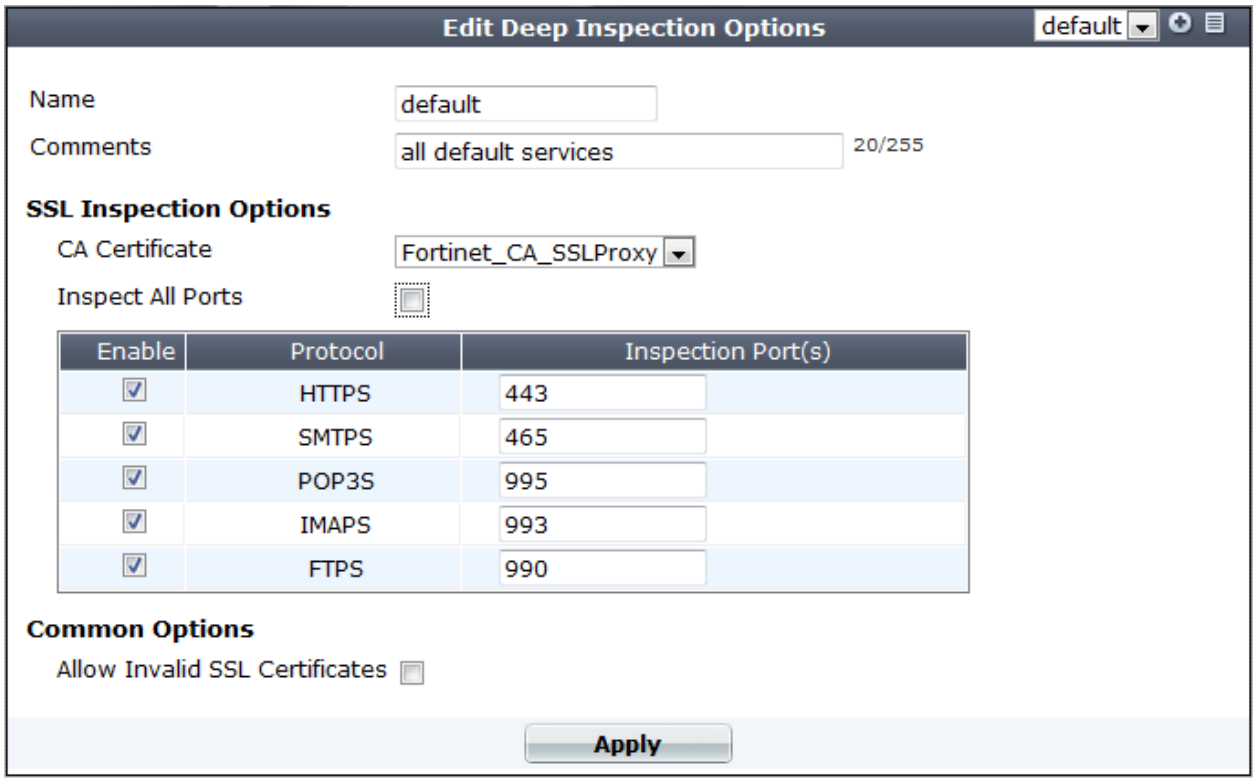
깨진 메일이나 조각난 메일을 허용할 경우 메일 사이에 악성코드가 첨부되어 보안상 위험합니다. 그래도 메일 보기를 원하는 경우 Allow Fragmented Messages를 사용하여 깨진 메일과 조각난 메일을 재 조합하여 다른 쪽 메일서버에서 읽을 수 있도록 허용합니다.

Append Signature(SMTP)

이메일에 서명을 추가 합니다.

4. SSL Inspection

암호화 되어 있는 SSL 트래픽 검사에 사용할 인증서 및 포트를 설정 합니다.

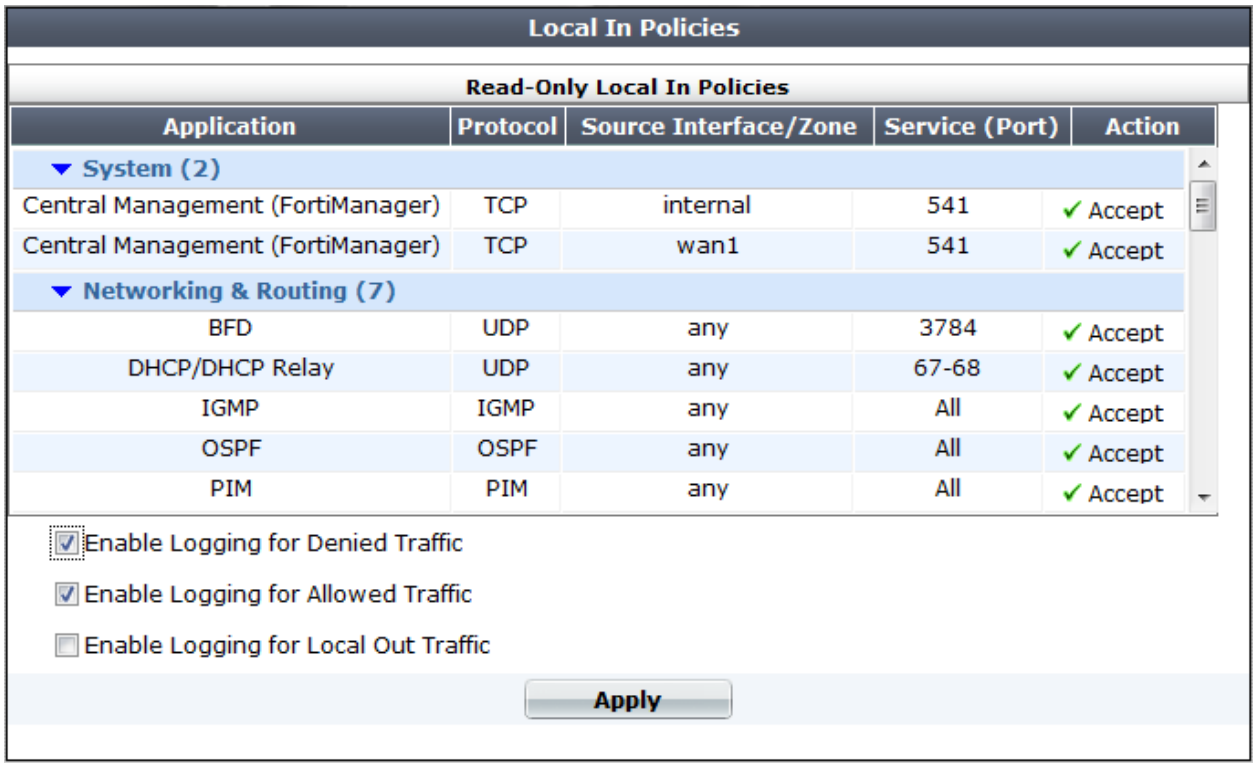


- SSL Inspection 프로파일 화면 -

CA Certificate — SSL 트래픽을 검사하기 위해 사용되는 인증서 입니다.
Allow Invalid SSL Certificates — 유효하지 않은 인증서의 허용 여부를 설정합니다.

5. 로컬 정책 (Local In Policy)

SNMP, VPN, Dynamic라우팅 등 Fortigate시스템이 직접 통신을 하는 트래픽에 대한 정책입니다. 정책의 수정은 불가능하고 로그의 수집 여부만 설정 가능 합니다.



– 로컬 정책 화면 –

6. 멀티캐스트 정책(Multicast Policy)

멀티캐스트가 통신하기 위한 정책을 설정합니다. VRRP와 같이 멀티캐스트를 이용하는 트래픽이 Fortigate를 지나가야 할 경우 설정을 합니다.

7. 정책 모니터(Policy Monitor)

Active Sessions, Bytes, Packets 별 사용량이 많은 정책의 정보를 보여줍니다.

4. 방화벽 객체(Firewall Objects)

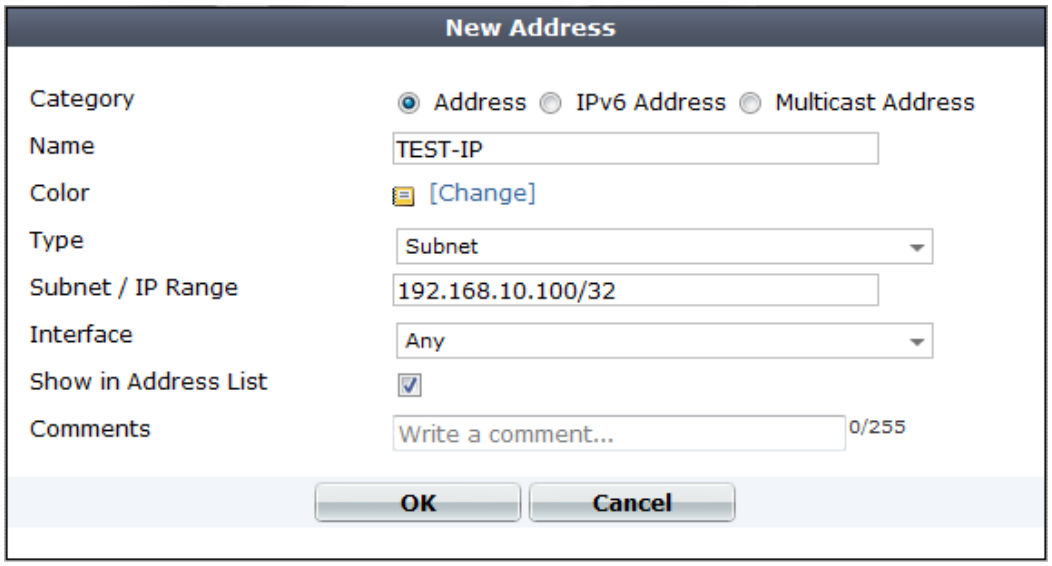
방화벽 정책을 생성하기 위해서는 IP주소, 서비스포트, 스케줄 등 많은 방화벽 객체가 필요합니다.
이러한 객체들을 생성, 편집, 삭제하는 방법을 알아봅니다.

1. 주소(Address)

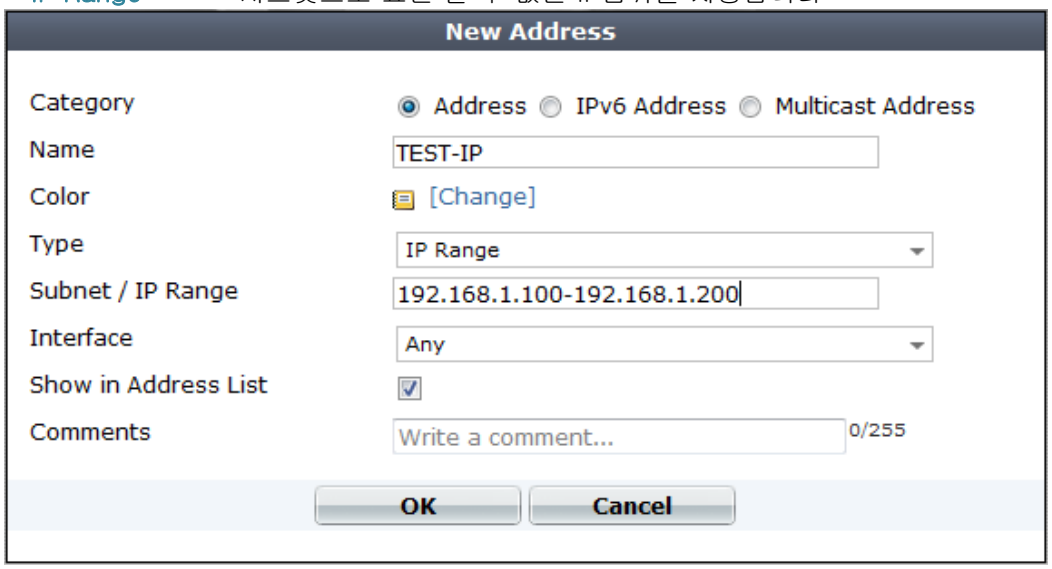
방화벽 정책에서 사용할 IP주소를 관리 합니다. 주소는 다음 형식을 지원합니다.

1-1. 주소(Address)

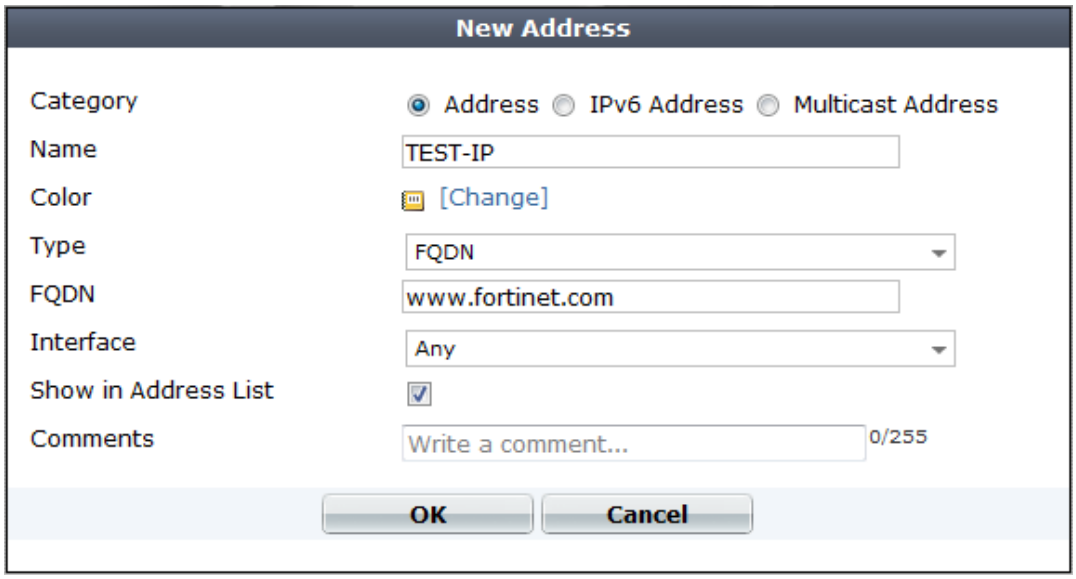
- Subnet 서브넷으로 표현되는 일반적인 IP주소 형식을 나타냅니다.



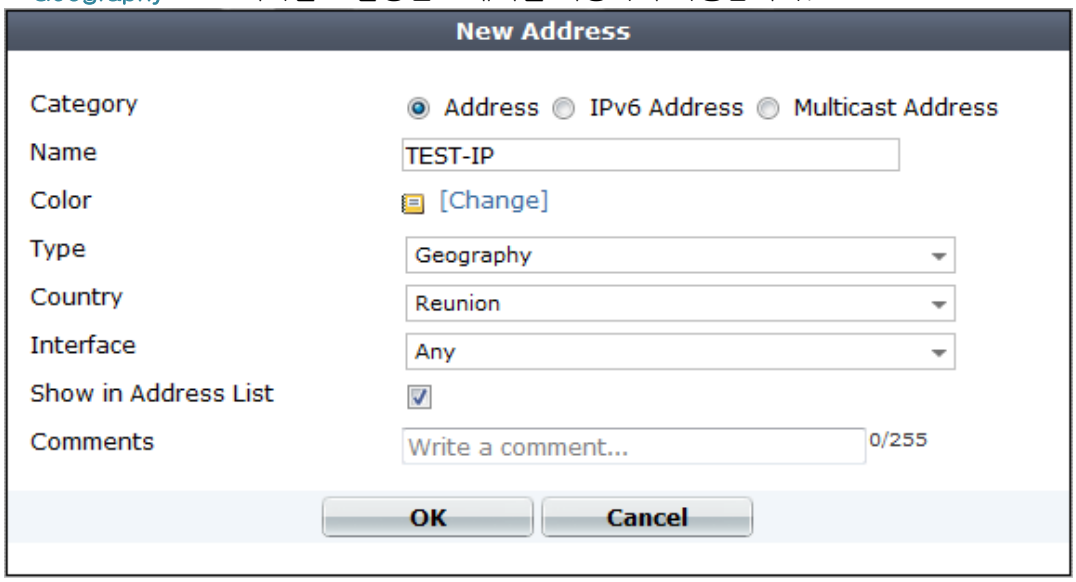
- IP Range 서브넷으로 표현 할 수 없는 IP범위를 지정합니다



- FQDN 도메인 이름을 주소로 사용하는 방식입니다. 해당 도메인의 실제 IP주소가 변경되어도 지속적으로 정책이 적용되는 장점이 있습니다.

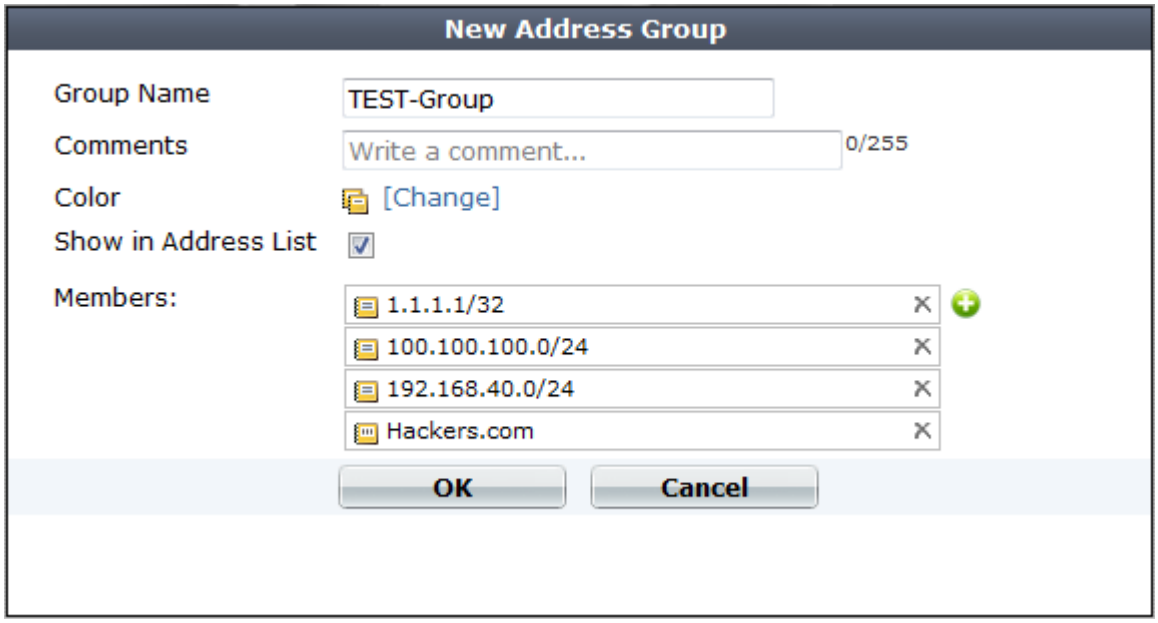


- Geography 국가별로 할당된 IP대역을 지정하여 사용합니다.



1-2. 그룹(Group)

생성된 주소들을 Group으로 묶어서 사용 할 수 있습니다.

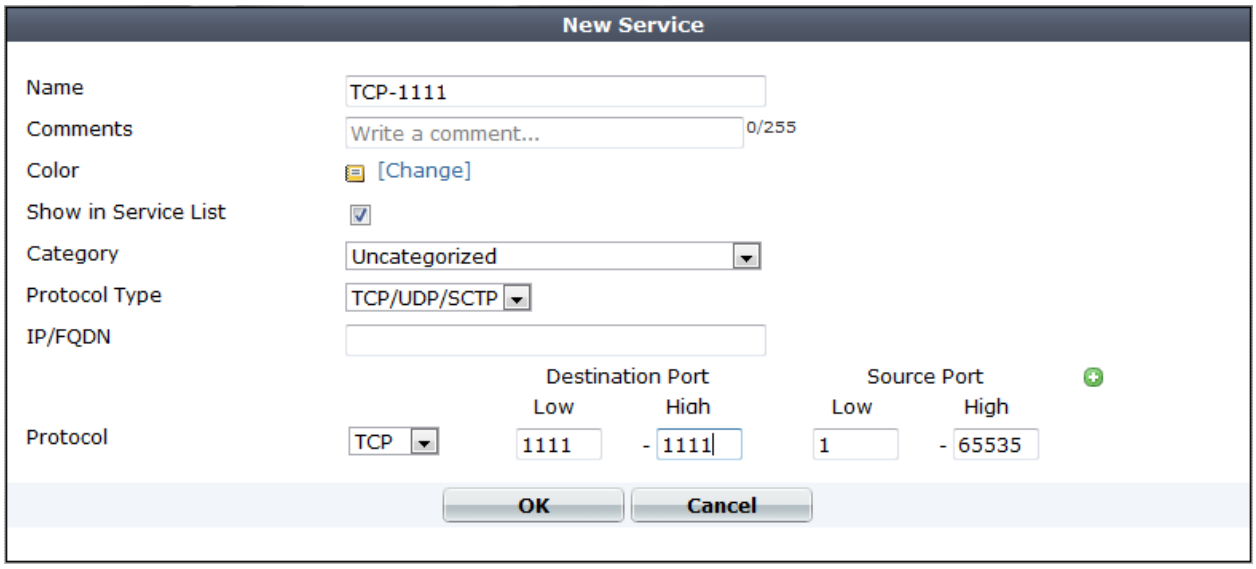


2. 서비스(Service)

2-1 서비스(Service)

방화벽 정책에서 사용할 서비스포트를 관리 합니다. 많이 사용되는 포트들은 미리 정의가 되어 있고, 추가적으로 사용자가 생성 할 수 있습니다.

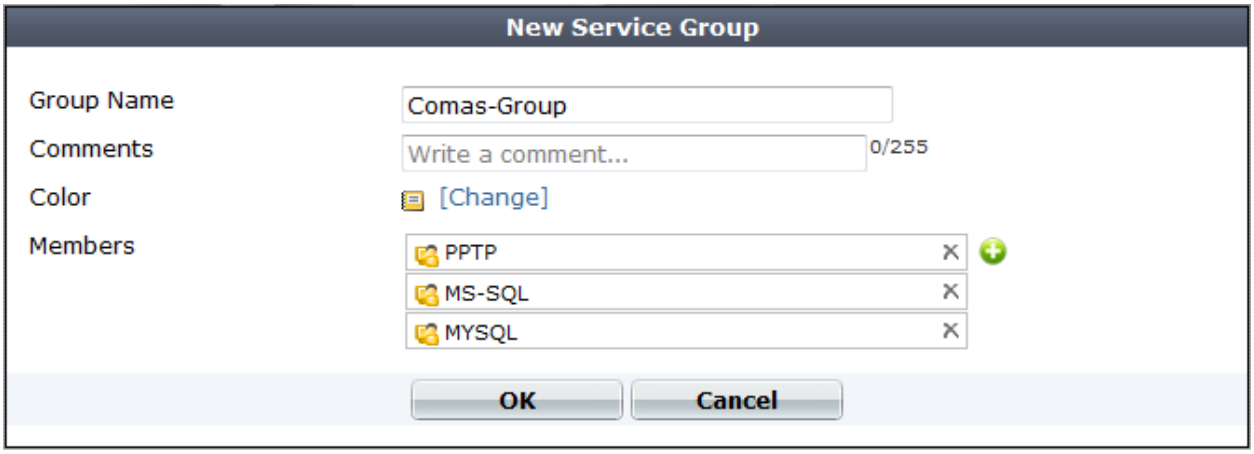
하나의 객체에 여러개의 포트 범위를 넣을 수 있습니다. 보통 Source Port는 랜덤하기 때문에 범위를 1~65535로 설정하고 Destination Port만 특정범위로 설정을 합니다.



- 서비스 설정 화면 -

2-2. 그룹(Group)

생성된 Service들을 그룹으로 묶어 사용 할 수 있습니다.



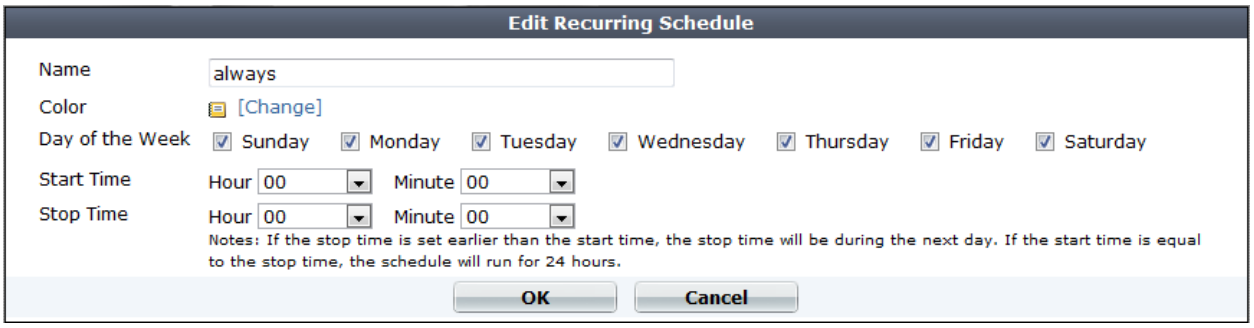
- 그룹 설정 화면 -

3. 일정(Schedule)

방화벽에 정책을 적용할 시간을 설정합니다. 반복, 일회성 객체를 생성 할 수 있습니다.

3-1. 반복(Recurring)

요일 단위로 반복 되는 시간을 설정 합니다.

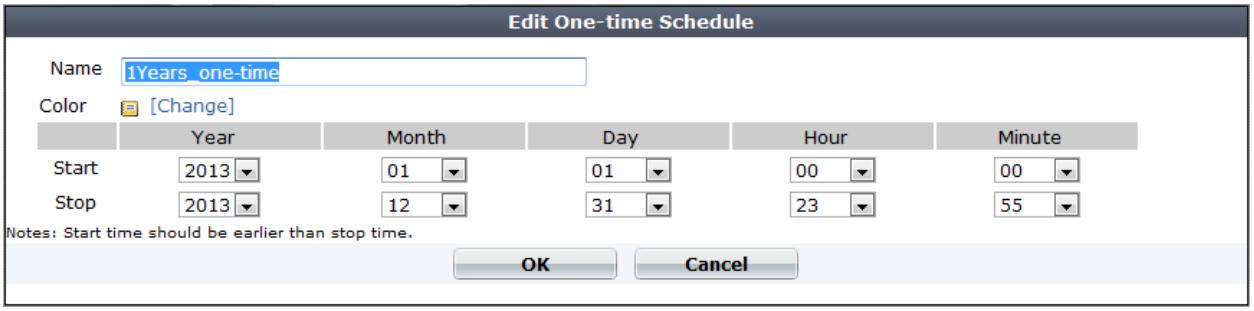


– 반복 스케줄 설정 화면 –

요일, 시작시간, 끝시간 을 지정하여 스케줄을 설정 합니다.

3-2. 일회(One-Time)

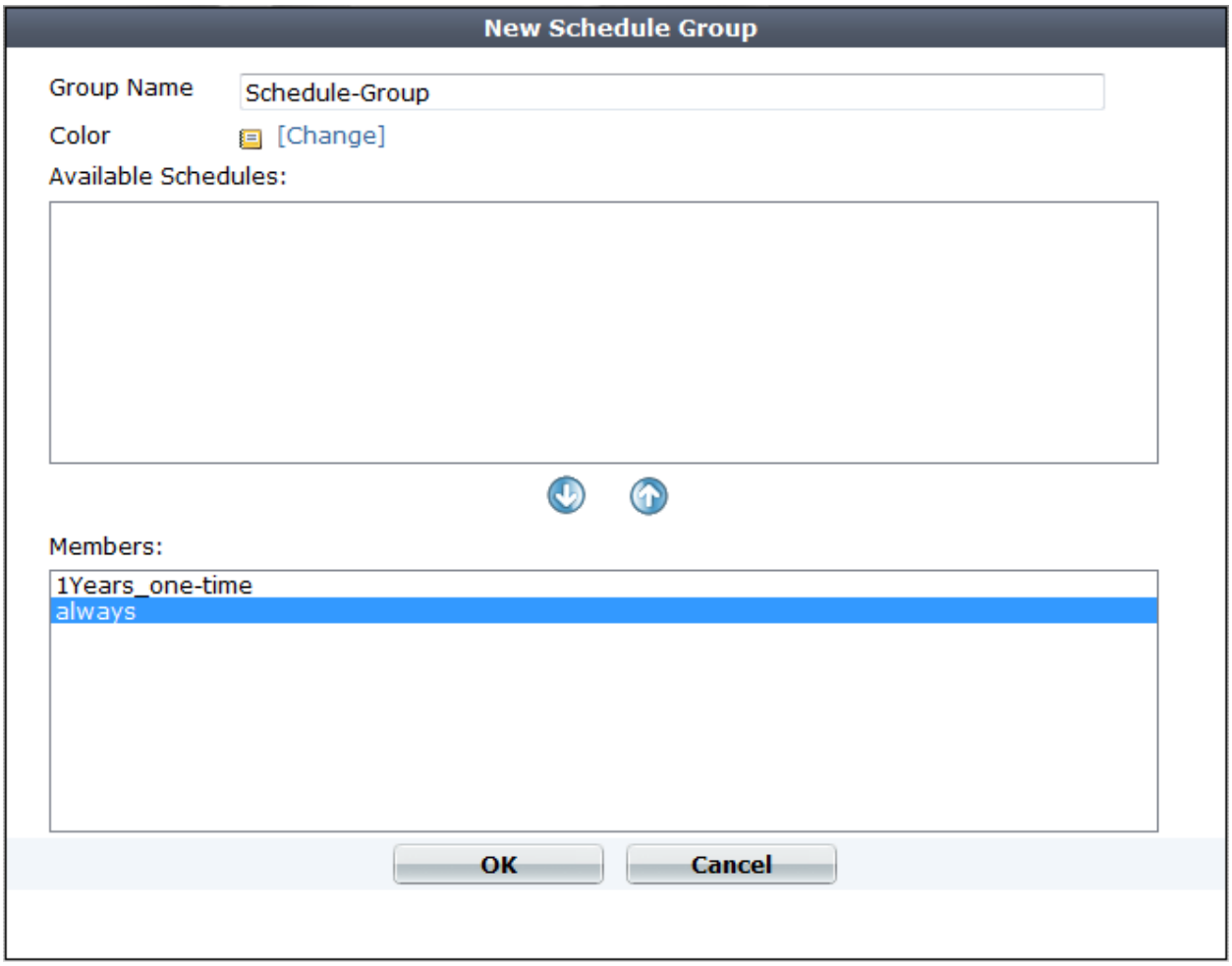
정해진 날짜나 시간, 기간을 정해 한 번만 적용을 합니다.



– 일회 스케줄 설정 화면 –

3-3. 그룹(Group)

생성된 스케줄 객체들을 그룹으로 묶어서 사용 할 수 있습니다.



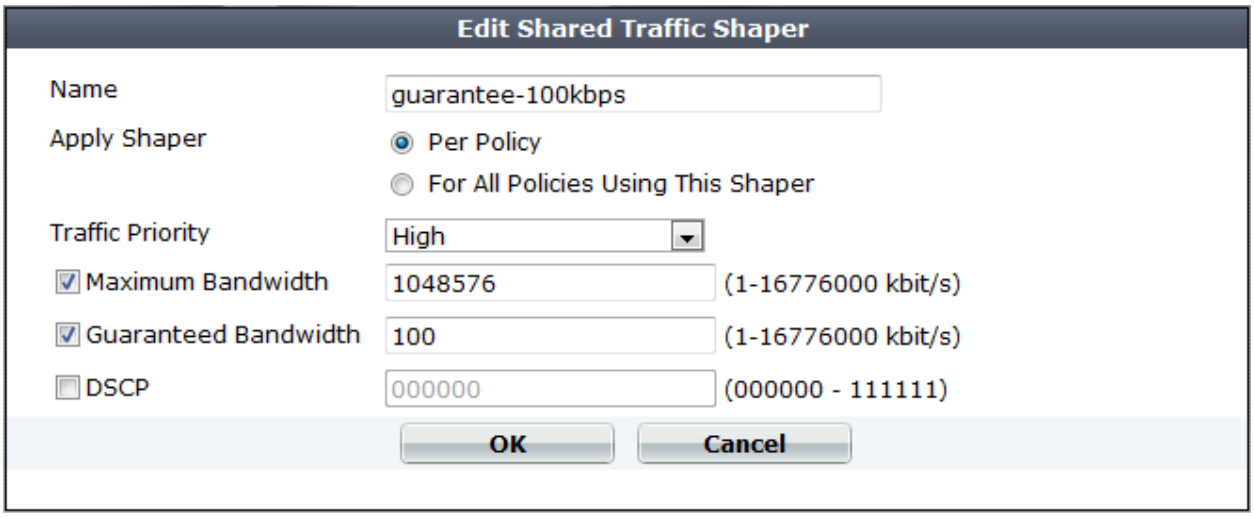
- 스케줄 그룹 설정 화면 -

4. 트래픽 쉐이퍼(Traffic Shaper)

Fortigate시스템은 정책을 기반으로 트래픽의 대역폭 조절이 가능합니다. 정책을 기준으로 일정 사용량을 쓰지 못하게 하거나 IP별로 트래픽을 할당 할 수 있습니다. 트래픽 쉐이퍼에서 생성된 프로파일은 방화벽 정책에 적용을 하여야 동작을 합니다.

4-1. 공유 (Shared)

설정된 임계값을 정책적으로 또는 전체적으로 공유를 합니다.



- Shared 프로파일 설정 화면 -

Apply Shaper 쉐이퍼의 적용형태를 설정합니다.

Per Policy 적용된 정책 하나에서만 임계값이 공유 됩니다.

For All Polices Using This Shaper 적용된 정책들 모두가 임계값을 공유을 공유합니다.

Traffic Priority 프로파일의 우선순위를 설정합니다.

Maximum Bandwidth 최대 트래픽 값을 설정합니다. 임계값 이상의 트래픽이 흐르지 못합니다.

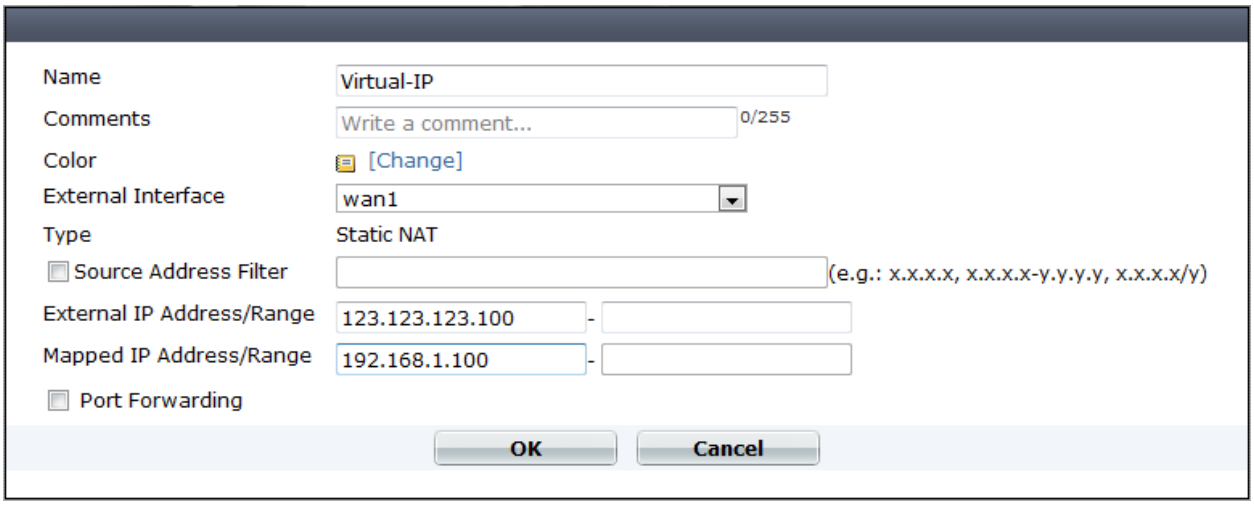
Guaranteed Bandwidth 최소 보장대역을 설정합니다.

5. 가상 IP(Virtual IP)

외부 공인IP와 내부 사설IP를 1:1로 매핑하거나 포트포워딩 설정을 하여 외부에서 내부 서버로 접속을 가능하게 합니다.

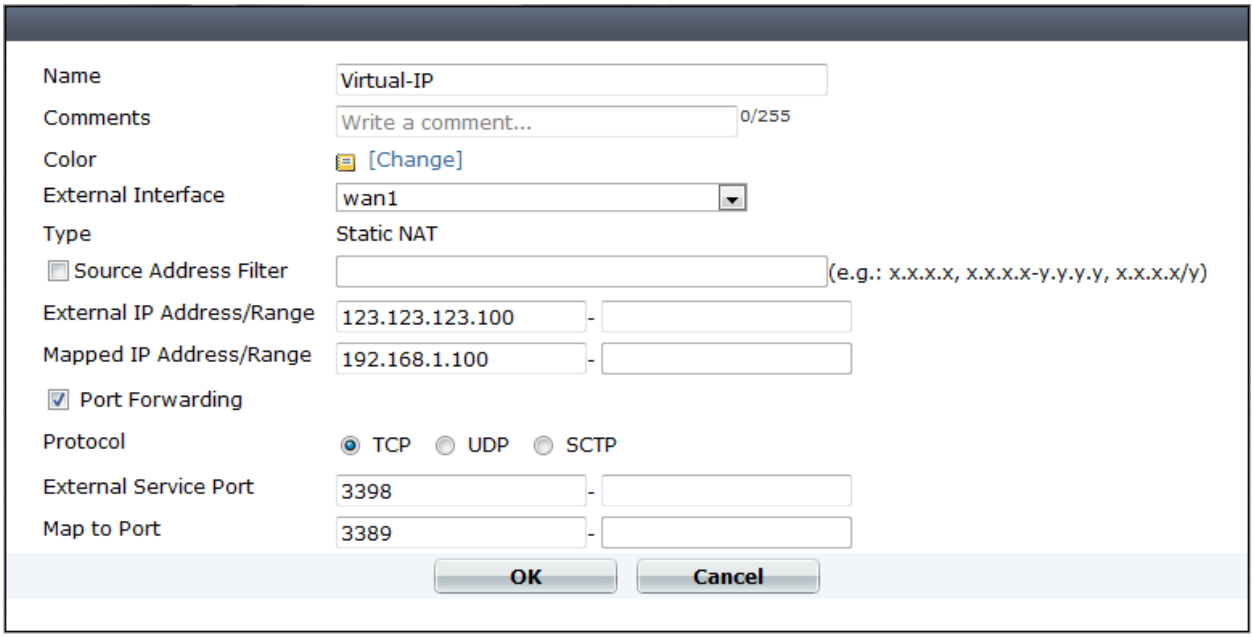
5-1. 가상IP(Virtual IP)

- 1:1 NAT 외부 공인IP와 내부 사설IP를 1:1로 매핑을 하여 모든 포트를 포워딩 합니다.



External Interface 외부 공인IP가 할당 된 인터페이스 입니다.
Source Address Filter 특정 출발지 IP에 대해서 NAT처리를 합니다.
External IP Address/Range 매핑할 외부 공인IP를 설정합니다.
Mapped IP Address/Range 매핑할 내부 사설IP를 설정합니다

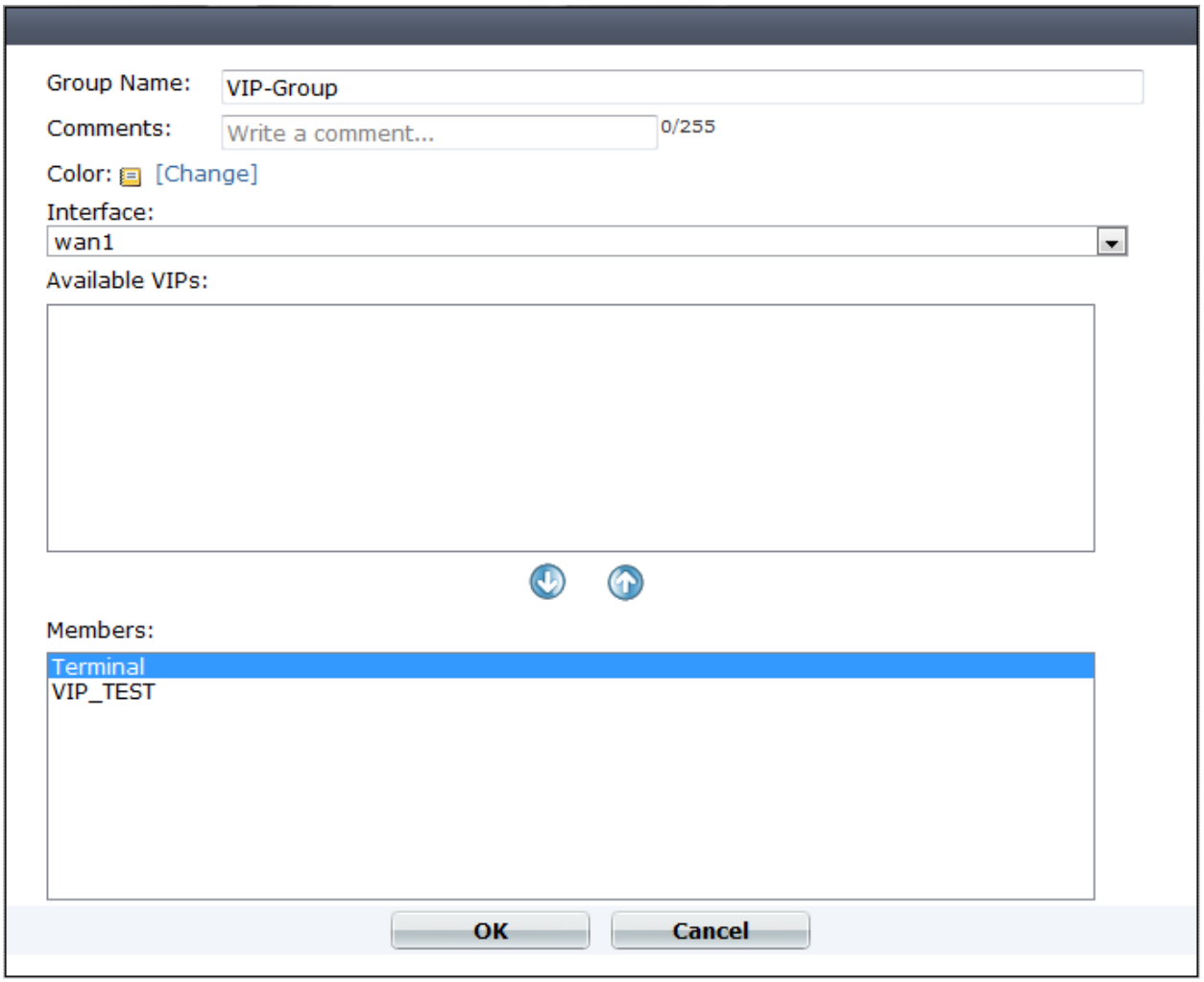
- 포트포워딩 외부 공인IP와 내부 사설IP를 매핑하고 설정된 포트만 포워딩 합니다. 하나의 공인IP에 대하여 다수의 포트포워딩 객체 생성이 가능합니다.



External Service Port 매핑할 외부 포트를 설정합니다.
Map to Port 매핑할 내부 포트를 설정합니다.

5-2. VIP 그룹(VIP Group)

생성된 VIP객체들을 그룹으로 묶어서 사용 할 수 있습니다.

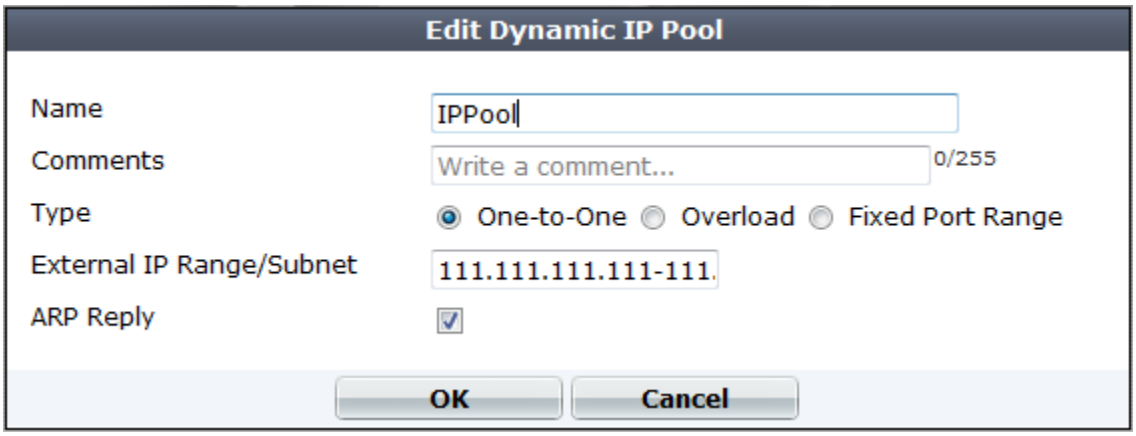


– VIP 그룹 설정 화면 –

5-3. IP 풀(IP Pool)

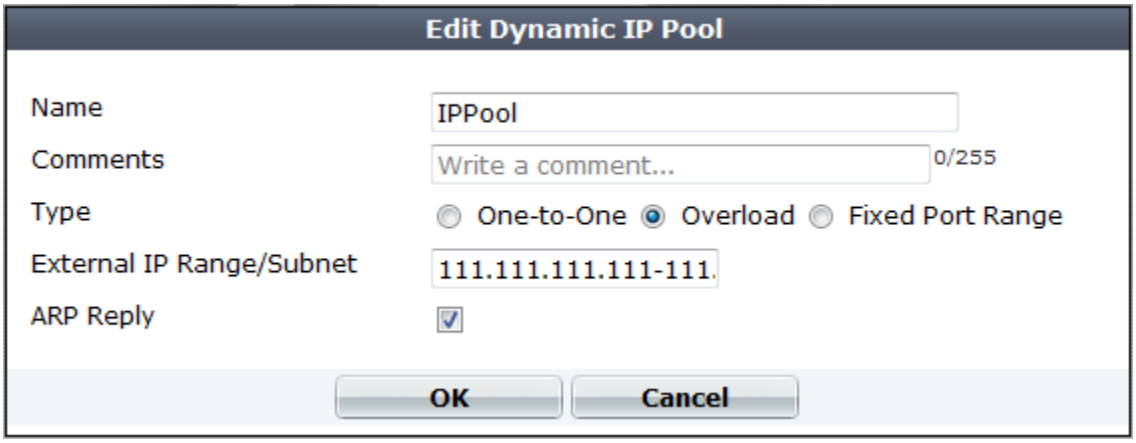
트래픽이 NAT되어 나갈 때 변경 되는 IP의 값을 설정 할 수 있습니다.

- One-to-One



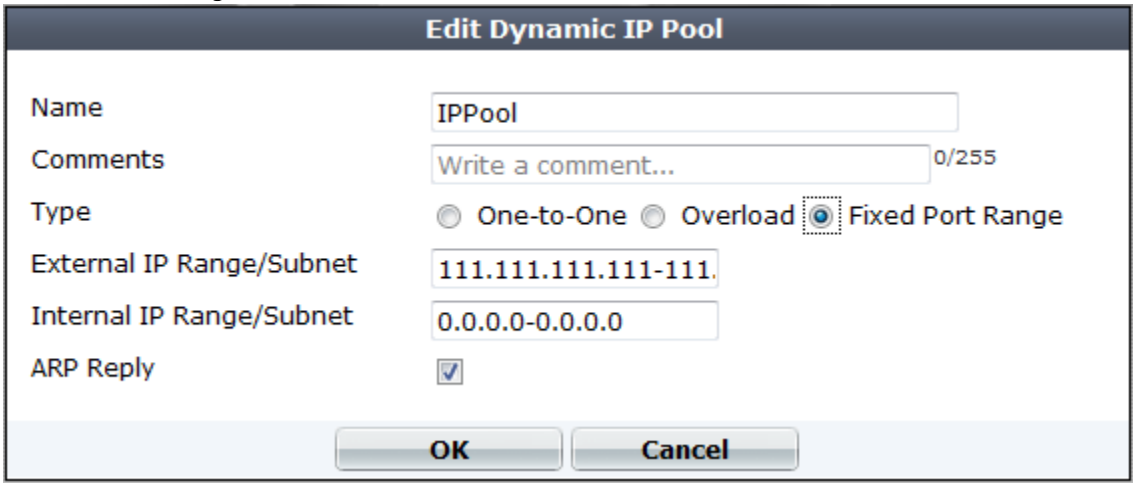
VIP의 NAT테이블을 참고하여 해당 IP만

- Overload



기본적인 IP_Pool 방법입니다. 출발지주소가 설정된 대역의 IP로 랜덤하게 IP를 변경합니다.

- Fixed Port Range



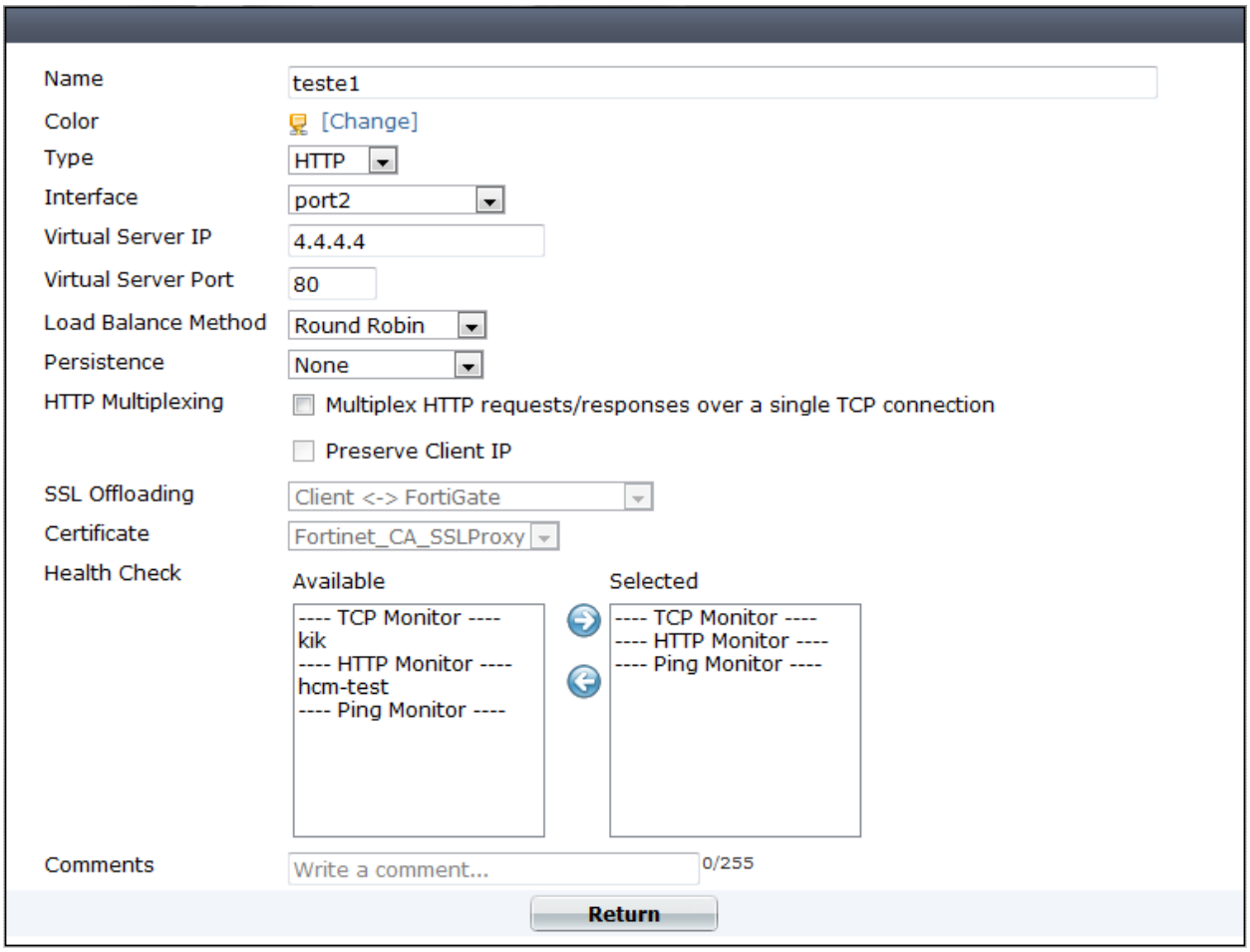
설정된 내부 주소 범위의 출발지주소만 설정된 대역으로 IP가 랜덤하게 변경됩니다. 내부 주소범위 외의 주소는 Deny 처리 됩니다.

6. 부하분산(Load Balance)

Fortigate시스템은 Layer 4스위치의 기능인 SLB(Server Load Balancing)를 구현 할 수 있습니다.

6-1. 가상 서버(Virtual Server)

사용자에게 서비스 할 가상 서버를 설정 합니다. 실제 사용자들은 가상서버의 IP로 접속을 시도 합니다.



- 가상 서버 설정 화면 -

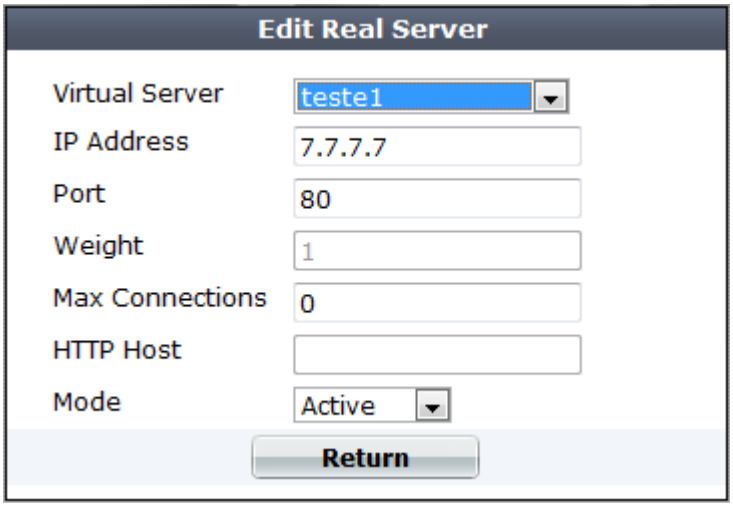
Interface 가상 서버의IP가 할당 된 인터페이스를 설정 합니다.
Virtual Server IP 가상 서버의IP를 설정 합니다.
Virtual Server Port 사용자에게 서비스 할 포트를 설정합니다.
Load Balance Method 로드밸런싱 방식을 설정합니다.

- Sourece IP Hash 출발지 주소를 기준으로 해시함수를 돌려 밸런싱 합니다.
- Round Robin 라운드 로빈(한번씩 번갈아 가면서 리얼서버로 트래픽을 던짐) 방식으로 밸런싱 합니다.
- Weighted 리얼서버에 할당된 Weight를 기준으로 밸런싱 합니다.
- First Alive 리얼서버 리스트 중 첫번째로 가동 중인 서버로 트래픽을 전송 합니다.
- Least RTT 리얼서버까지의 패킷 왕복 시간이 가장 작은 순서대로 밸런싱 합니다 .
- Lease Session 세션이 가장 적은 리얼서버의 순서대로 밸런싱 합니다.
- HTTP Host 호스트가 HTTP 접속을 했던 정확한 리얼서버로 다시 접속을 할 수 있도록 HTTP 헤더를 참조 하여 밸런싱 합니다.

Persistence 호스트와 리얼서버와의 연결을 지속시키기 위한 설정을 합니다.
Health Check Fortigate시스템이 리얼서버의 상태를 확인 하기 위한 방법을 설정합니다.

6-2. 리얼 서버(Real Server)

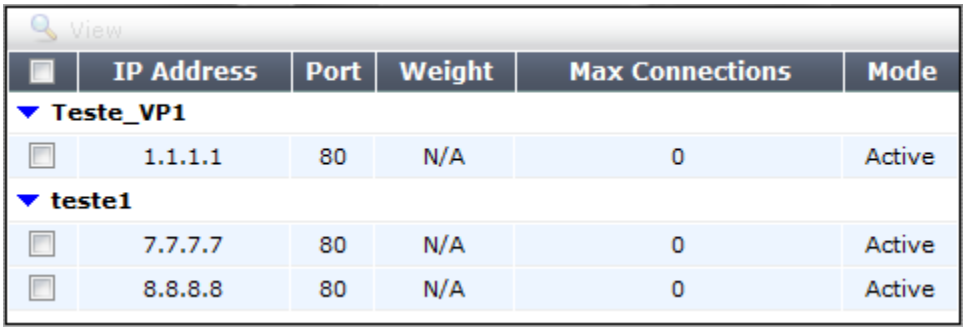
실제 서비스를 할 리얼서버를 설정 합니다.



- 리얼 서버 설정 화면 -

Virtual Server 연동할 가상 서버를 설정합니다.
IP Address 리얼서버의 IP주소를 설정합니다.
Port 리얼서버가 서비스 할 포트를 설정 합니다.
Weight 리얼서버의 가중치를 설정합니다.
Mode 리얼서버의 운용상태를 설정합니다

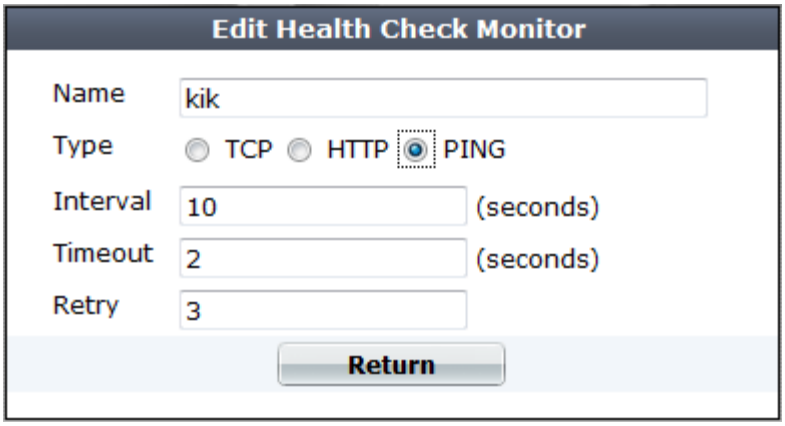
.



- 가상 서버와 리얼 서버가 연동 설정 된 리스트 화면 -

6-3. 핫빗상태 모니터(Health Check)

Fortigate시스템이 리얼서버의 상태를 확인하기 위한 방법을 설정합니다.



위의 예는 리얼서버로 10초에 한번씩 ping체크를 하고 2초 동안 응답을 기다립니다. 이 과정을 세 번 반복을 하고 계속 응답이 없으면 리얼서버가 서비스 불능 상태로 판단을 하여 밸런싱을 하지 않습니다.

7. 모니터(Monitor)

Traffic Shaper Monitor

트래픽 쉐이퍼가 적용되는 트래픽에 대한 모니터링 화면입니다. 트래픽 조절 기능으로 Drop되는 패킷의 통계도 확인이 가능합니다.

5. UTM 보안 프로파일(UTM Security Profiles)

UTM 보안 프로파일은 Fortigate시스템이 제공하는 여러 UTM기능의 사용 여부와 적용DB를 설정합니다. 각각의 방화벽 정책별로 다르게 프로파일을 적용 할 수 있습니다.

1. 바이러스 탐지(Antivirus)

Antivirus 는 viruses, worms, trojans, 그리고 malware 에 대해 파일을 검사 합니다.
Antivirus Scan 엔진은 감염을 식별하기 위한 signature DB를 가지고 있고 DB 사이즈에 따라 아래와 같이 나누어 집니다.

Normal DB	현재 FortiGuard 에서 확인한 세계적으로 위험도가 큰 Virus를 포함 합니다. 이 Database는 Fortigate 에서 지원하는 기본 Database 입니다.
Extended DB	현재는 사용빈도가 낮은 Virus 뿐만 아니라 Normal DB도 포함합 니다.
Extreme DB	위 두 DB 및 Zoo Virus까지 추가로 확장한 DB가 포함합니다. Zoo Virus는 이미 오래 전부터 알려져 있던 Virus이기 때문에 사용빈도가 매우 낮습니다.

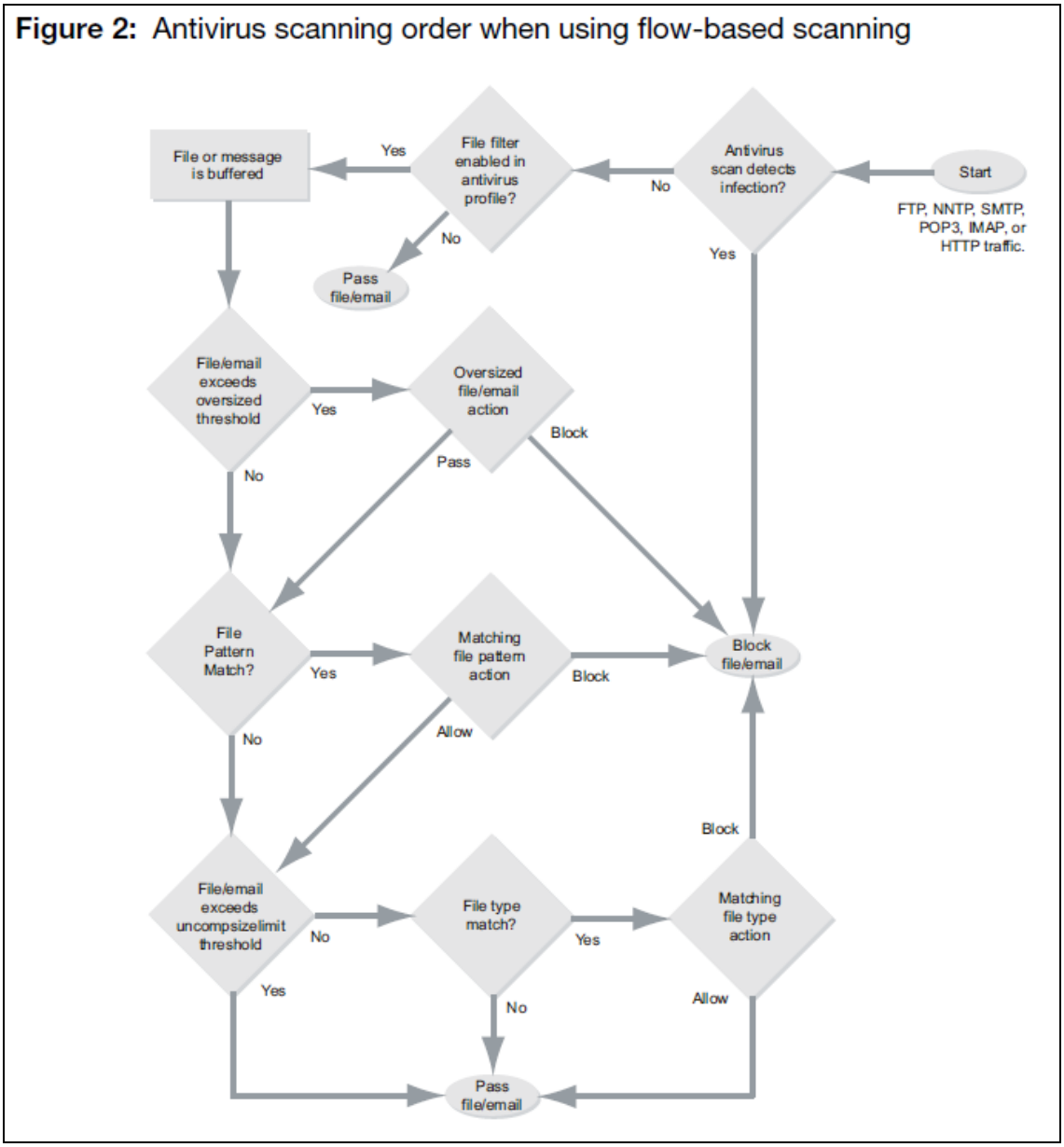
- Fortigate에 적용하는 AV 시그니처 DB는 모델에 따라 적용 DB가 달라 질 수 있습니다.

1-1. 탐지 방법(Scanning Method)

안티바이러스 엔진은 검사파일에서 signature가 확인되면 감염으로 판단하고 이에 대한 조치를 하게 됩니다. Fortigate시스템은 아래의 두 가지 방법으로 바이러스를 탐지 할 수 있습니다 .

1-1-1. Flow-based antivirus scanning

Flow-based antivirus scanning 은 검사할 파일을 버퍼에 할당하지 않고 viruses, worms, trojans, 그리고 malware 에 대해 네트워크 트래픽을 검사 할 수 있는 Fortigate의 IPS 엔진을 사용 합니다. Flow-based antivirus scanning 의 장점은 파일의 크기와 관계 없이 빠른 스캔이 가능 합니다. 단점은 짧은 순간에 파일의 작은 부분을 검사 하기 때문에 감염에 대한 탐지율이 낮아집니다. 또한 ZIP 과 GZIP 형식의 파일은 탐지를 하지 못합니다.



- Flow-based antivirus scanning 의 순서도 -

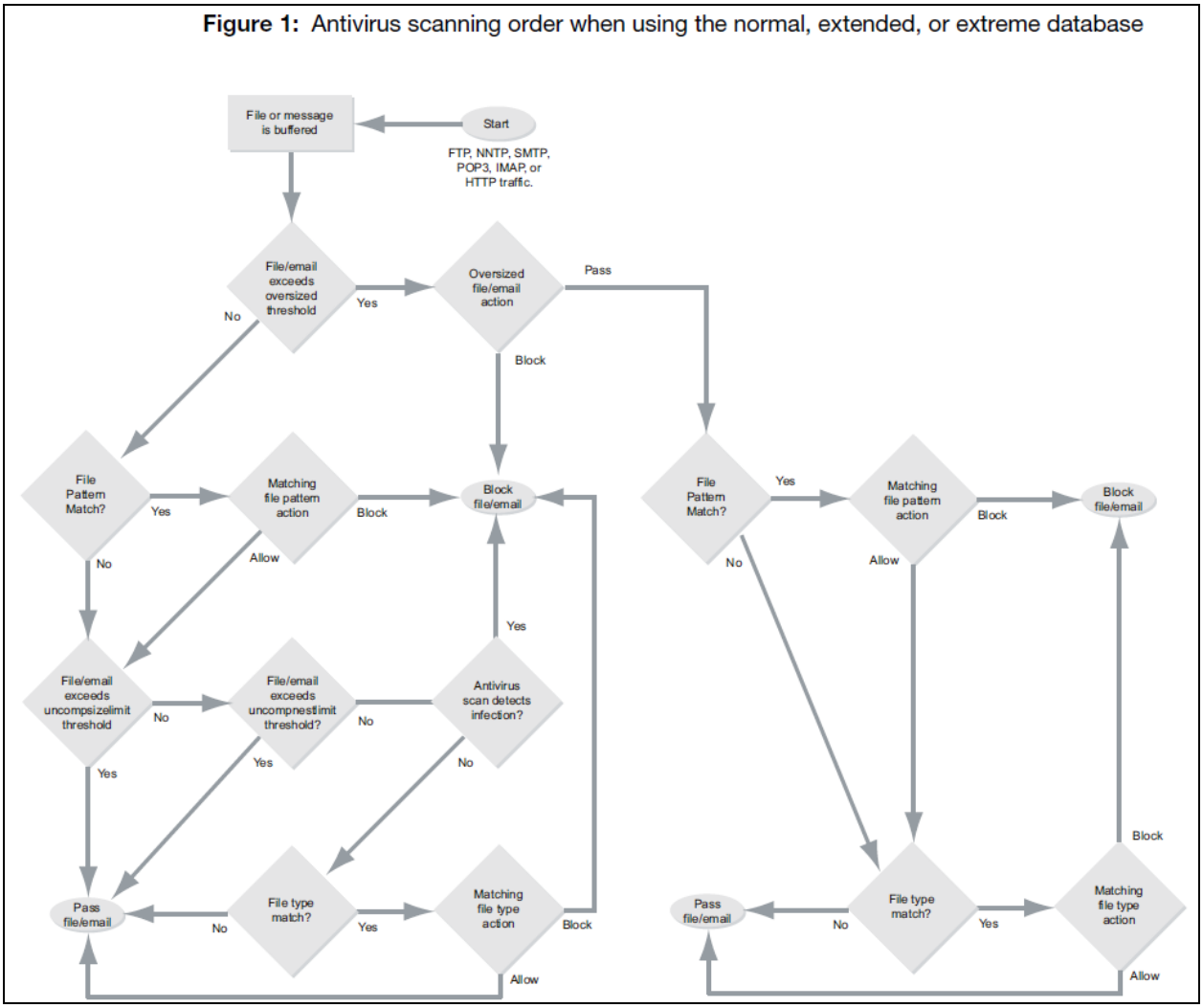
1-1-2. Proxy-based antivirus scanning order

Proxy-based antivirus scanning 은 첫 번째 검사로 대형파일/이메일에 대해 파일 임계 값을 초과 여부를 확인 합니다. 이후 임계 값이 초과 할 경우 해당 파일은 antivirus scanning 을 하지 않고 통과 합니다. 임계 값 미만의 경우 아래 그림과 같이 Scanning 기준에 따라 패킷을 처리하게 됩니다. 만약 파일이 바이러스 스캔 작업을 실패 하는 경우 더 이상 스캔이 수행 되지 않습니다.

아래 파일 처리 순서 참조.

만약 fakefile.exe라는 파일을 차단 패턴으로 인식하는 경우 사용자에게 대체 메시지를 보내고 파일을 삭제하거나 격리 시킵니다. 이전 검사가 이미 파일이 위험하다고 처리 하였기 때문에 이후 의 스캔 순서인 virus scan, grayware, heuristics, and file type scans 의 유형을 수행 하지 않습니다.

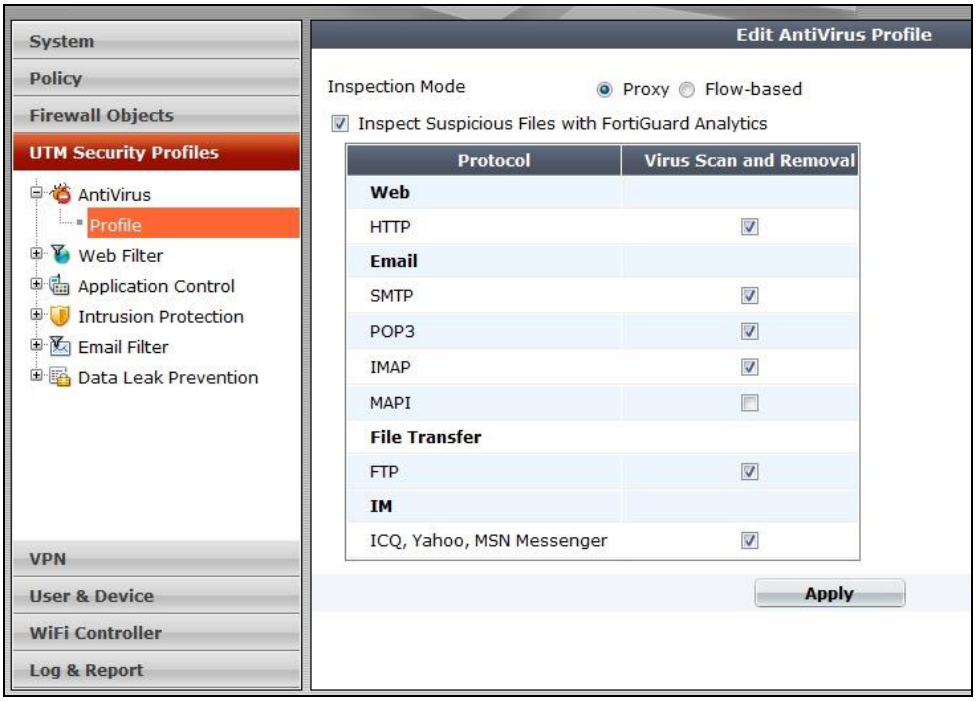
Figure 1: Antivirus scanning order when using the normal, extended, or extreme database



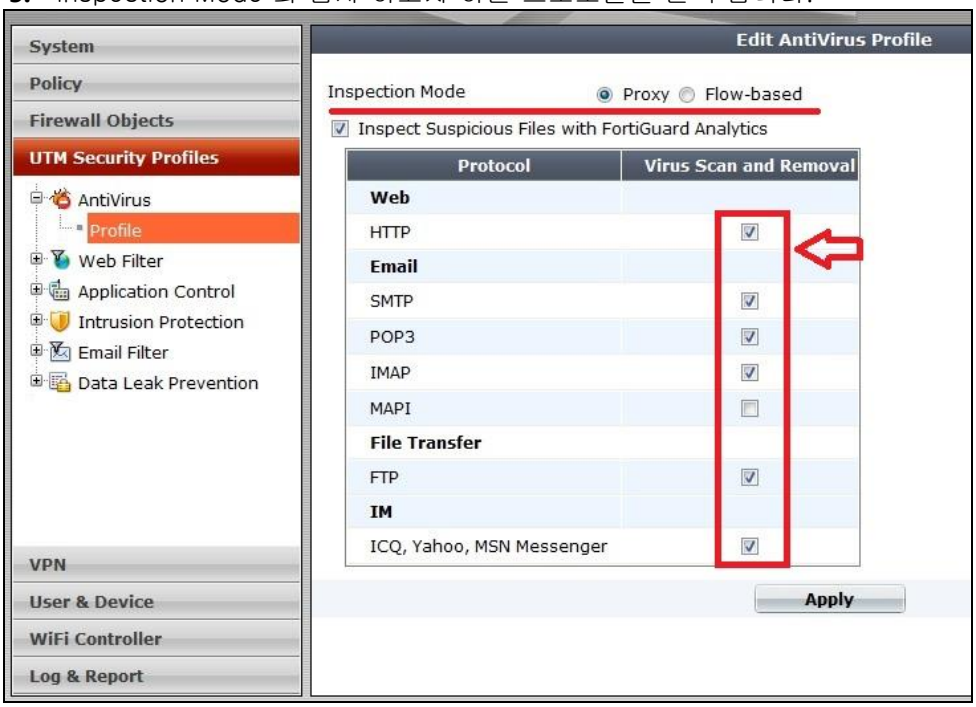
1-2. 바이러스 탐지 활성화(Enable antivirus scanning)

Fortigate시스템의 바이러스 탐지 기능을 사용하기 위해서는 다음과 같이 설정 합니다.

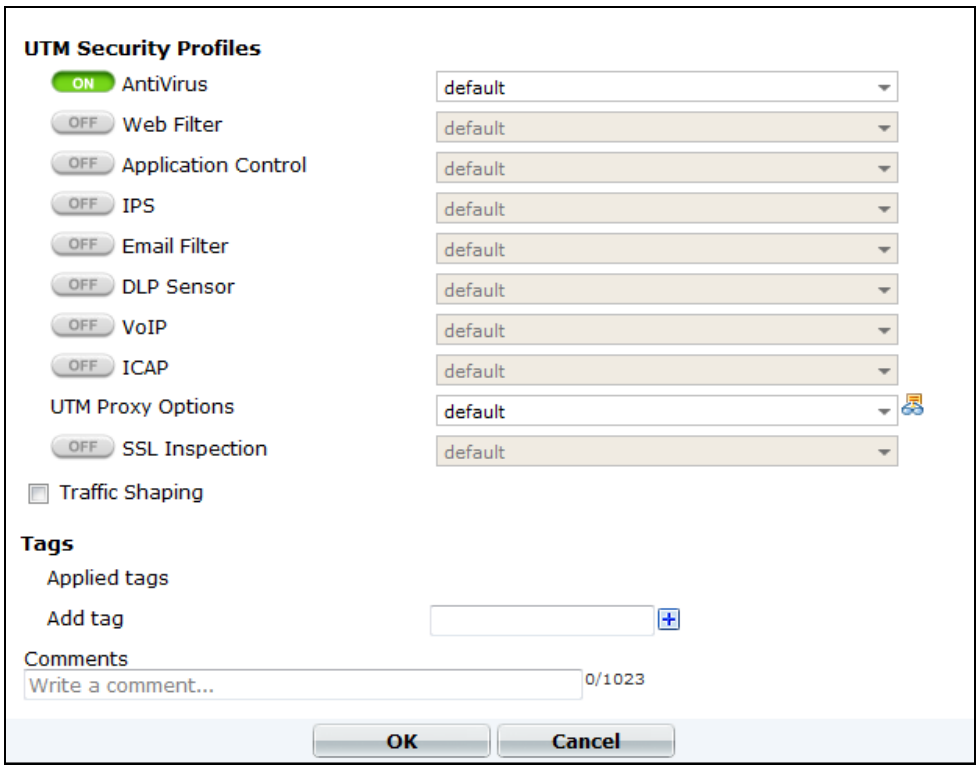
1. *UTM Security Profiles > AntiVirus > Profile*. 로 이동합니다.



2. 기본 선택은 Default Profile 입니다.
   새로운 Virus Profile 을 만들거나 기존 Anti Virus Profile을 편집 할 수 있습니다.
3. Inspection Mode 와 검사 하고자 하는 프로토콜을 선택 합니다.

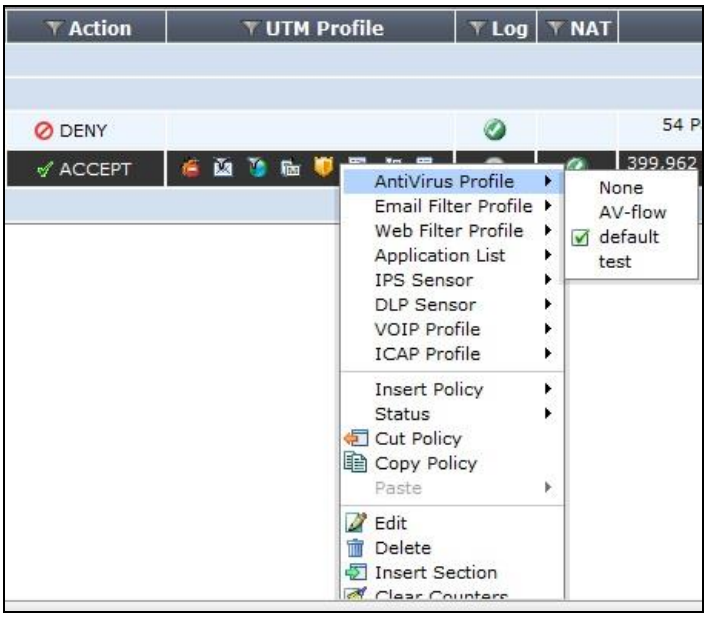


4. *OK* 를 선택 합니다.
5. *Policy > Policy > Policy* 에서 Anti Virus를 적용 할 보안정책을 생성 또는 편집 합니다.
6. UTM Security Profiles 기능에서 AntiVirus 기능을 활성화하고 프로파일을 적용합니다.



7. *OK* 를 선택 합니다.

- 현재 5.0 GA Patch 1 (Build 0147) 버전에서는 Display Options on GUI > Multiple UTM Profiles 기능을 활성화를 해야 신규 생성이 가능합니다. CLI는 바로 생성 가능. 새로 생성한 Profile은 보안정책 우 클릭 에서 변경이 가능합니다.



1-2-1. 기본 바이러스 DB 설정과 탐지 버퍼 사이즈 설정

관리자는 장비의 성능과 해당 고객사에 상황에 맞게 AntiVirus의 DB 타입과 탐지 Buffer Size를 조절 할 수 있습니다.

버퍼사이즈의 최대값은 Fortigate의 모델마다 다릅니다.

- 기본 바이러스 DB 변경 및 버퍼 사이즈 설정 예

바이러스 DB 변경 예

```
config antivirus settings
  set default-db extended
end
```

버퍼사이즈 변경 예

```
config antivirus service http
  set uncompsizelimit 20
end
```

1-3. 파일 격리 활성화

Fortigate시스템이 Local hard disk 또는 FortiAnalyzer 와 연동이 되어 있다면 감염파일을 격리 시킬 수 있습니다.

- HTTP traffic에 대해 바이러스 감염파일을 격리 방법. (web site로부터 다운로드 한 파일)

1. 격리하려는 위치와 용량 설정합니다.

```
config antivirus quarantine
  set destination disk          <- disk or FortiAnalyzer
  set quarantine-quota 500   <- 할당량 설정
end
```

2. 검역 설정을 적용하고자 하는 Profile 과 traffic 설정합니다.

```
config antivirus profile
  edit default
    config http
      set options scan quarantine
    end
end
```

3. 보안정책에 해당 AntiVirus Profiles 적용합니다.

1-4. 그레이웨어 탐지(Grayware scanning)

Grayware 프로그램은 사용자의 동의 없이 컴퓨터에 원치 않는 소프트웨어를 설치 합니다.
이는 시스템의 성능문제를 일으킬 수 있고 악의적인 목적으로도 사용이 가능합니다.
Fortigate 에서 Grayware프로그램을 검색할 수 있도록 하려면 antivirus scanning 과 grayware detection 기능을 활성화 해야 합니다.

- Grayware 탐지 활성화 방법.

```
config antivirus settings
```

```
    set grayware enable
end
```

1-5. 지능형 지속 공격 차단(APT protection)

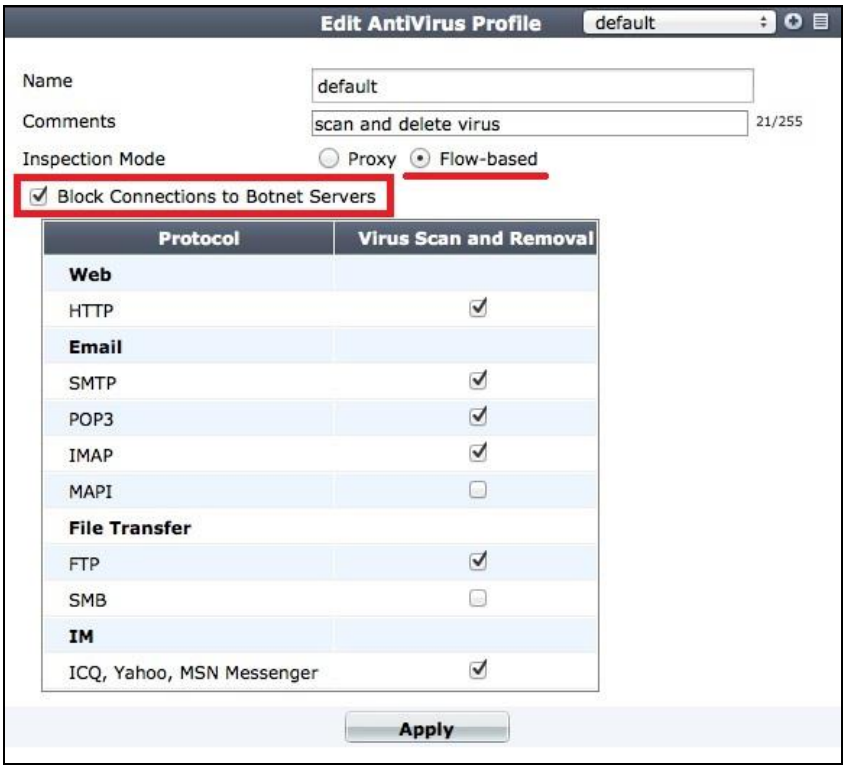
FortiOS 5.0 에서는 Advanced Persistent Threat (APT) 보호를 위해 sandbox 상에서 FortiGuard 로그 분석을 합니다. 이를 통하여 botnet 보호, phishing 보호 그리고 zero-day 공격에 대해 보호 합니다.

Botnet 과 phishing 보호

Virus Profile 에는 Botnet에 대해 추가 설정이 가능합니다.

Fortigate는 Botnet을 감지하고 연결 시도를 차단 합니다. 이 기능은 Phishing URL에 대한 접근도 차단 합니다.

AntiVirus의 DataBase 는 잘 알려진 C&C 사이트 및 Phishing URL에 대해서 지속 적인 업데이트를 합니다.



2.웹 필터(Web Filter)

웹필터는 인터넷 사용자가 악성코드를 배포 하는 웹 사이트 또는 업무와 무관한 웹 사이트 등을 제어 합니다.

웹 응용 프로그램의 사용이 증가하면서 웹 접근에 대한 모니터링과 제어가 필요하게 되었습니다. 웹 필터링이 필요한 이유는 다음과 같습니다.

- 업무와 관련이 없는 웹사이트 접근으로 인해 생산성이 낮아짐
- 불필요한 대역폭 소비로 인한 정상적인 업무까지 지장이 생김.
- 채팅 사이트, 허가되지 않은 웹메일 시스템, IM 및 P2P 사이트의 파일공유로 인한 내부 기밀 유출.
- 업무와 관련되지 않은 웹서핑을 통한 웹 기반 공격에 노출
- 내부 사용자가 부적절한 자료에 대해 접근 또는 다운로드를 통한 저작권 등의 침해

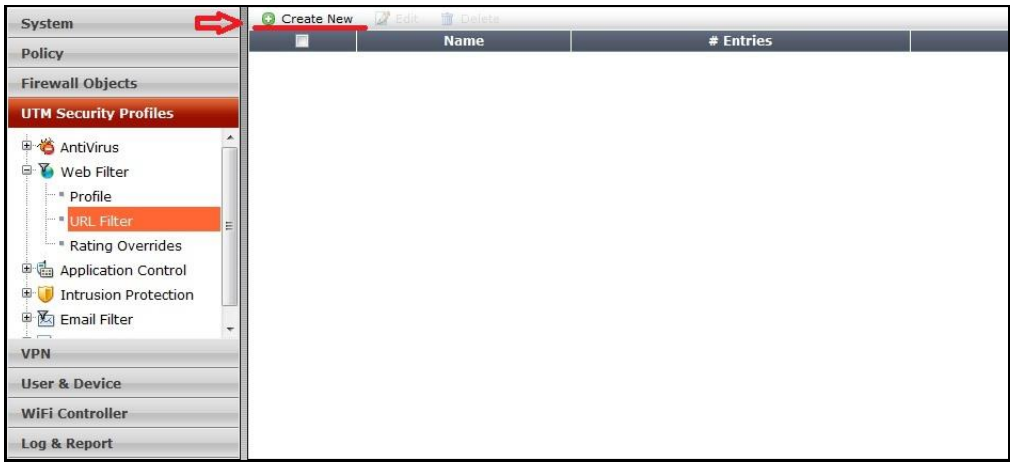
위와 같은 문제를 해결할 수 있는 방법으로 웹 필터를 사용할 수 있습니다.

2-1. URL filter

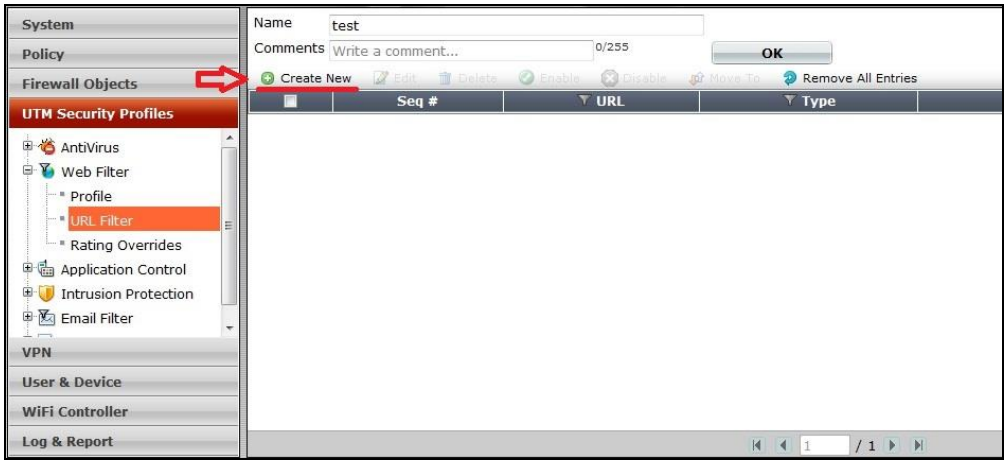
관리자는 URL필터 목록에 특정 URL을 추가하여 접근 허용을 하거나 차단을 할 수 있습니다.

2-1-1.URL 필터 리스트 생성

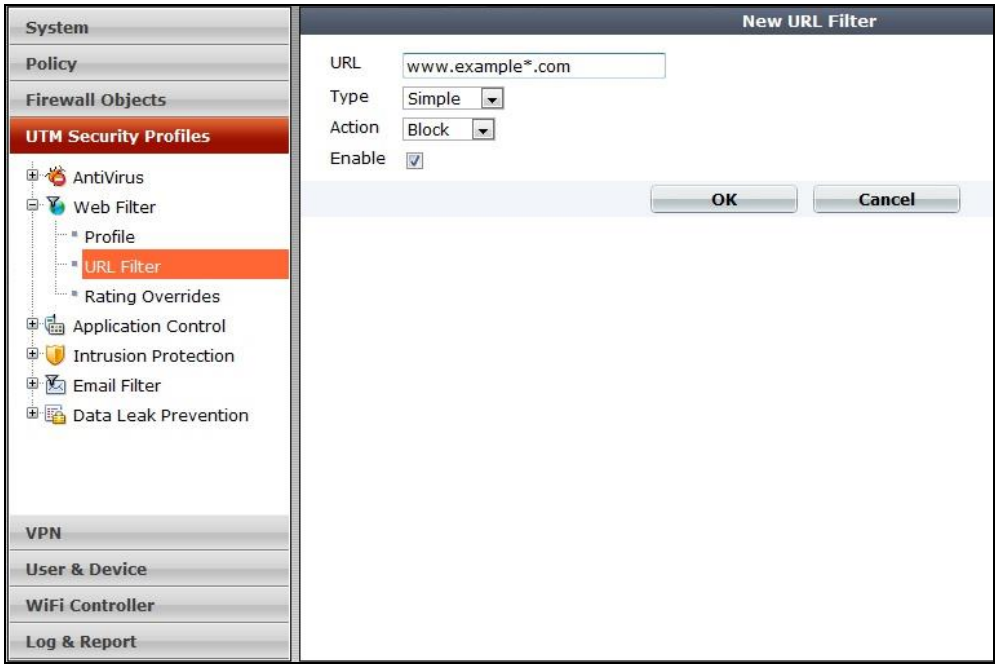
1. *UTM Security Profiles* > *Web Filter* > *URL Filter* 로 이동합니다
2. *Create New* 선택합니다.



3. URL filter list를 추가 합니다.
4. *Create New* 선택합니다.



5. example: www.example*.com. 라는 URL 등록 후 *OK* 선택합니다.

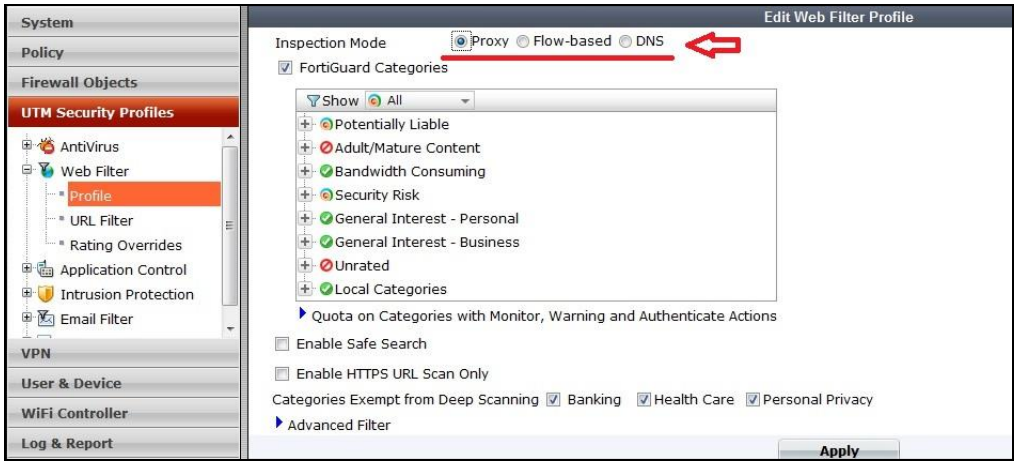


2-1-2. FortiGuard Web Filter

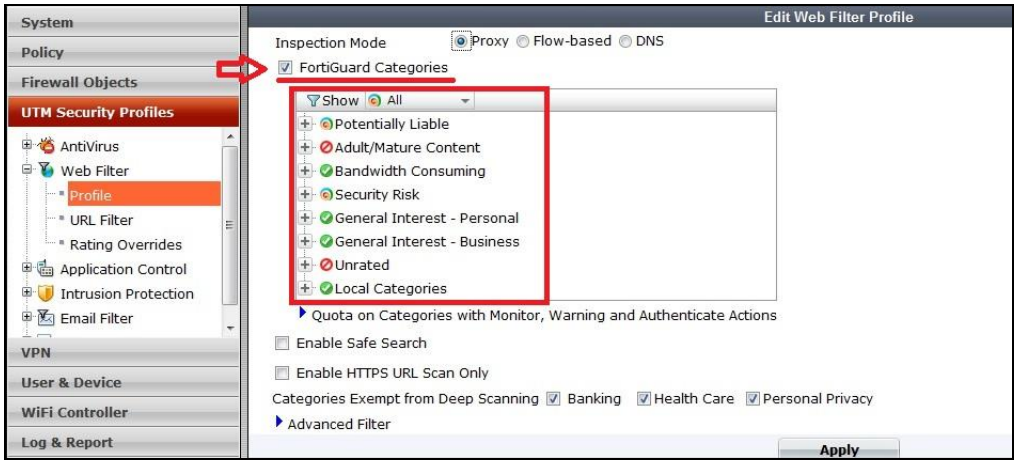
FortiGuard Web 필터를 사용하여 웹사이트에 대해 접근을 허용하거나 차단할 수 있습니다. FortiGuard Web 필터는 수십억개의 WebPage에 대해 카테고리별로 분류하고 있습니다. 이 기능은 별도의 라이선스가 필요 합니다.

▪ FortiGuard 웹 필터링 설정

1. *UTM Security Profiles* > *Web Filter* > *Profile* 로 이동합니다.
2. Inspection mode 선택합니다.



3. FortiGuard Categories 체크박스 체크 후 카테고리별 동작을 설정합니다.



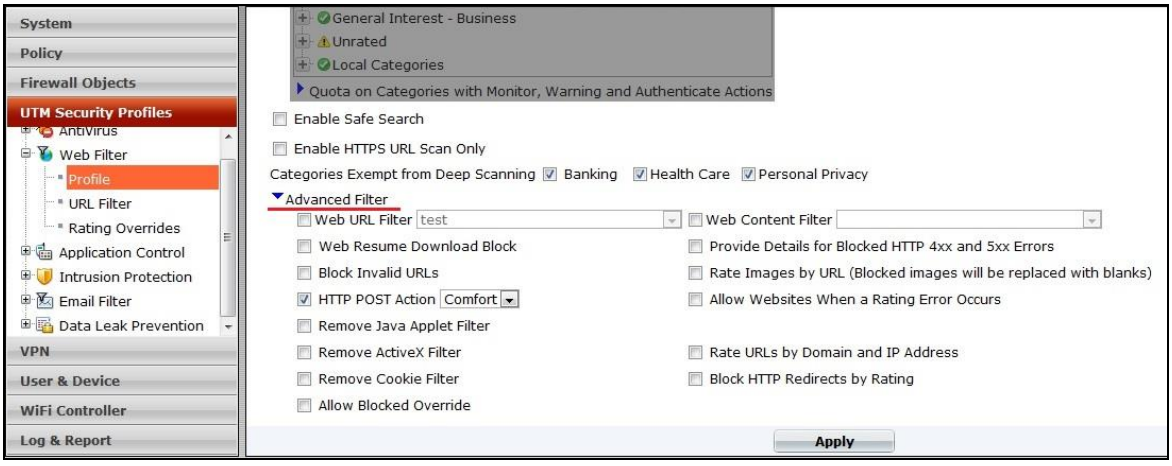
2-1-3. 웹 콘텐츠 필터(Web Content Filter)

관리자는 특정 단어나 패턴을 포함하는 웹페이지를 제어할 수 있습니다.

- **웹 콘터츠 필터 리스트 생성 예제**

```
config webfilter content
  edit 3
    set name "inappropriate language"
      config entries
      edit offensive
      set action block
      set lang western
      set pattern-type wildcard
      set score 15
      set status enable
    next
    edit rude
      set action block
      set lang western
      set pattern-type wildcard
      set score 5
      set status enable
    end
  end
end
```

위의 필터 항목들을 생성 한 후 정책에 사용하고자 하는 프로파일에 각 필터 들을 설정 합니다.



Advanced Filter를 클릭하여 Web URL Filter, Web Conetnt Filter 등을 활성화 한 후 앞서 만든 Filter 들을 지정 합니다.

※ 주의사항 ※

해당 Web Filter 의 프로파일만 생성 한다고 하여 Cilent 에 적용이 되는 것이 아니므로 다시 정책에 설정을 해 주도록 합니다.

3. 어플리케이션 제어(Application Contro)l

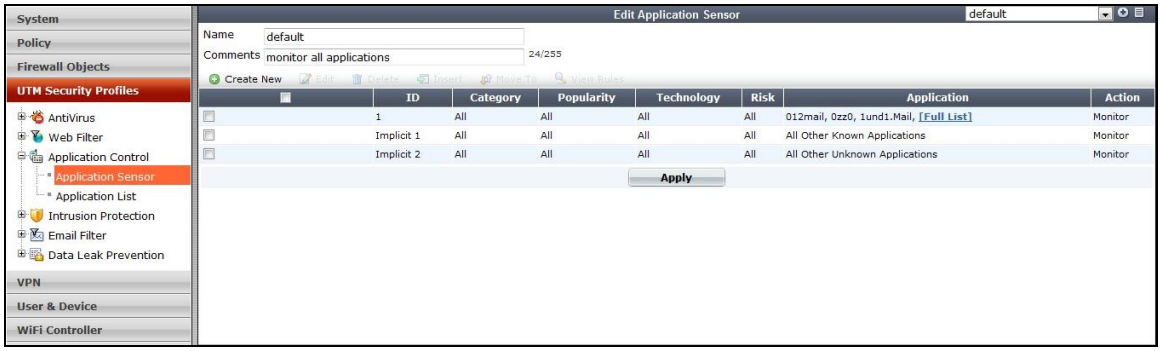
일반적으로 방화벽은 IP주소, 포트 등의 객체를 이용하여 네트워크 트래픽을 제어 합니다. 하지만 특정 응용프로그램의 트래픽을 제어 하려면 주소 또는 포트로만 제어하기에는 부족할 수 있습니다.

FortiGate 는 2000개 이상의 응용프로그램, 포트 및 프로토콜에 대한 Signature가 포함 되어 있습니다.

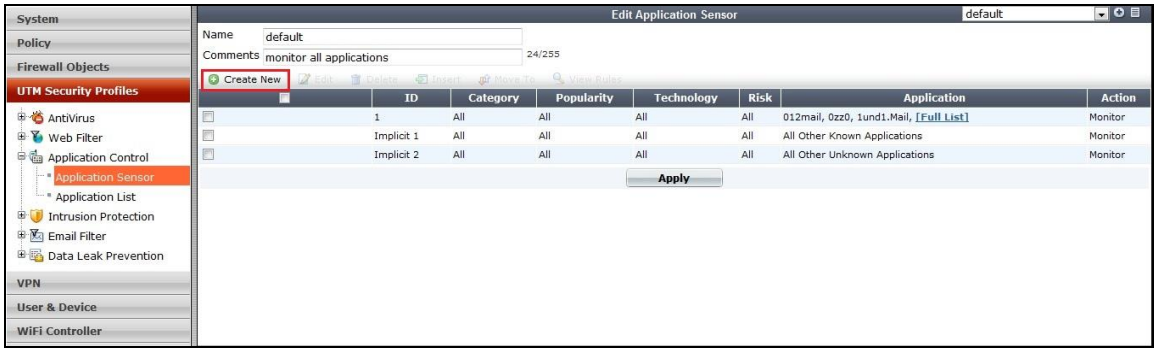
3-1. 어플리케이션 제어 활성화

- **어플리케이션 센서 생성 방법**

1. *UTM Security Profiles > Application Control > Application Sensor* 로 이동.

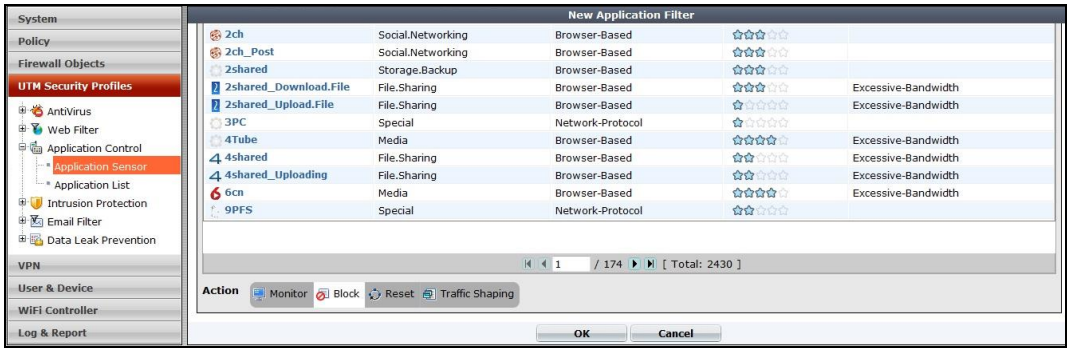


2. *Create New* 클릭.



3. 카테고리 별 분류가 가능하며 특정 응용프로그램 별로 선택이 가능 함.

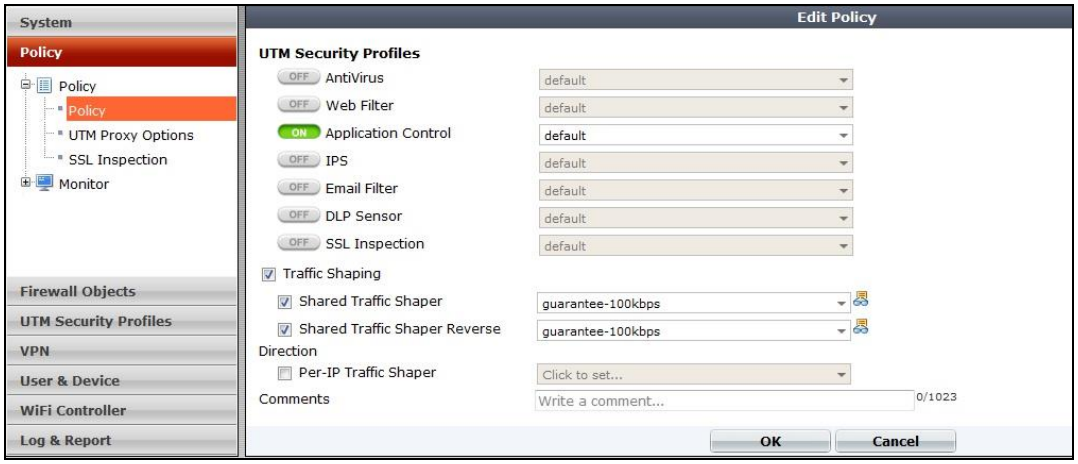
4. 선택한 응용프로그램에 대한 동작을 정의 합니다.



5. *OK* 선택합니다.

- **적용방법**

보안정책에서 해당 Application Sensor 를 정의 합니다.

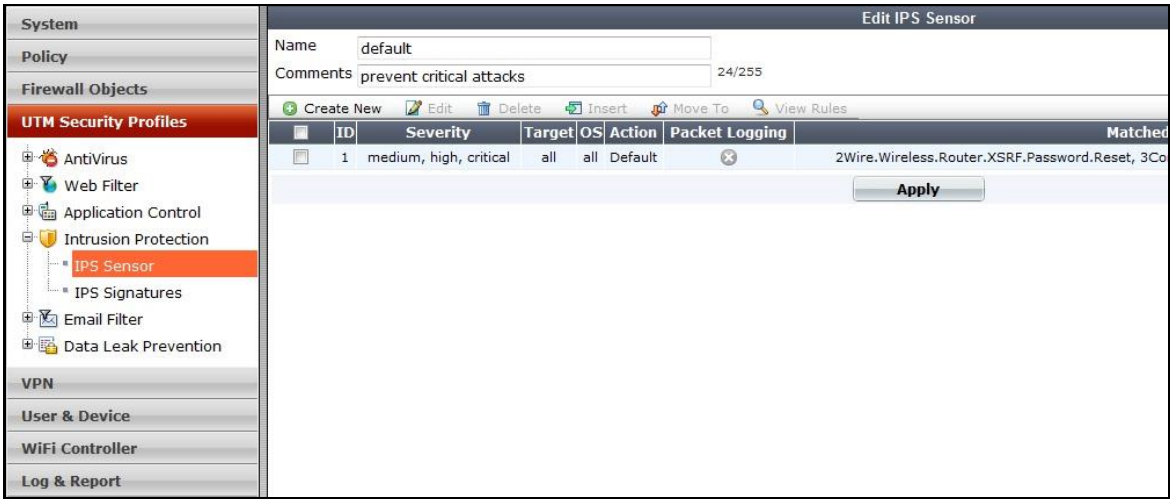


4.침입 방지(Intrusion Protection)

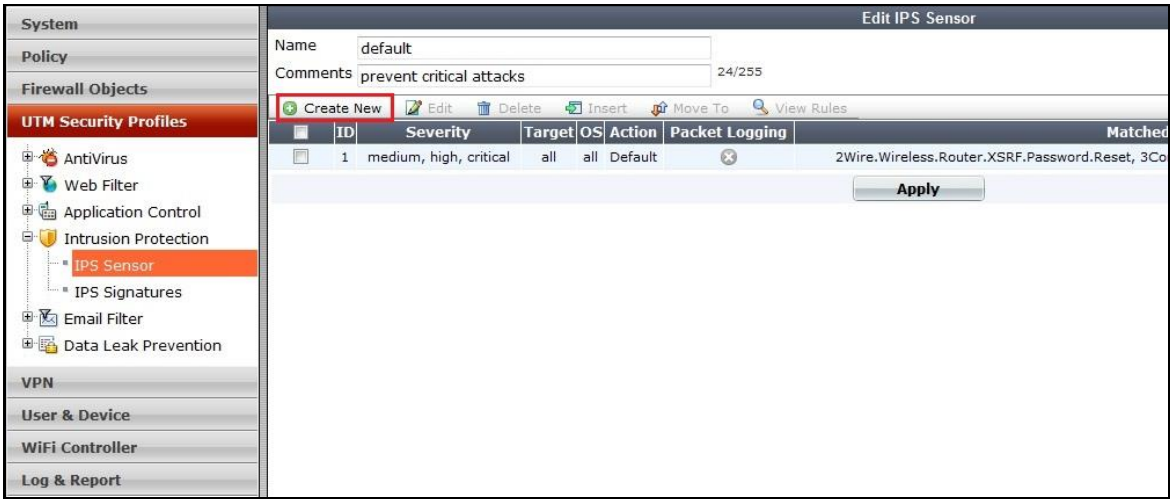
Fortigate시스템 의 Intrusion Protection 은 signature 와 anomaly detection을 지원하며, 낮은 지연시간 및 우수한 안정성을 가지고 있습니다.

▪ IPS 센서 생성 방법

1. *UTM Security Profiles > Intrusion Protection > IPS Sensor* 로 이동.

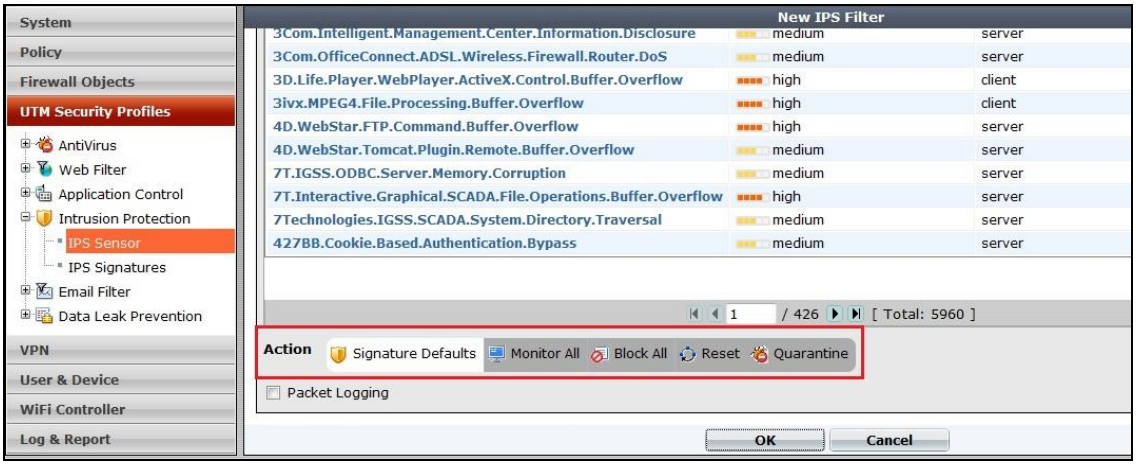


2. *Create New* 선택 합니다.



3. Filter option 에서 위험도수준, 타겟, OS 별 설정 가능 합니다.

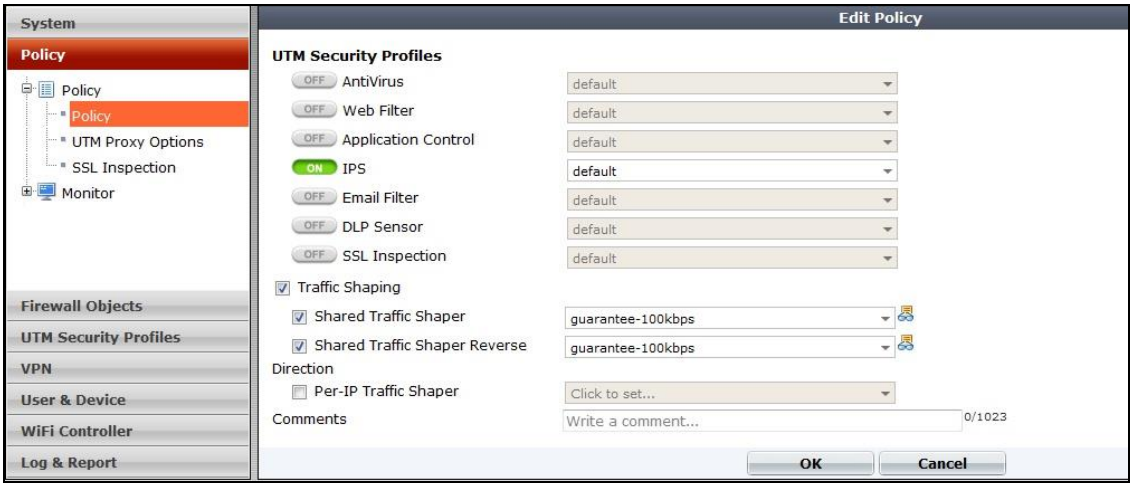
4. Filter option 정의 후 동작 방식 선택.



5. *OK* 선택 합니다.

- 적용방법

보안정책에서 해당 IPS Sensor 를 정의 합니다.

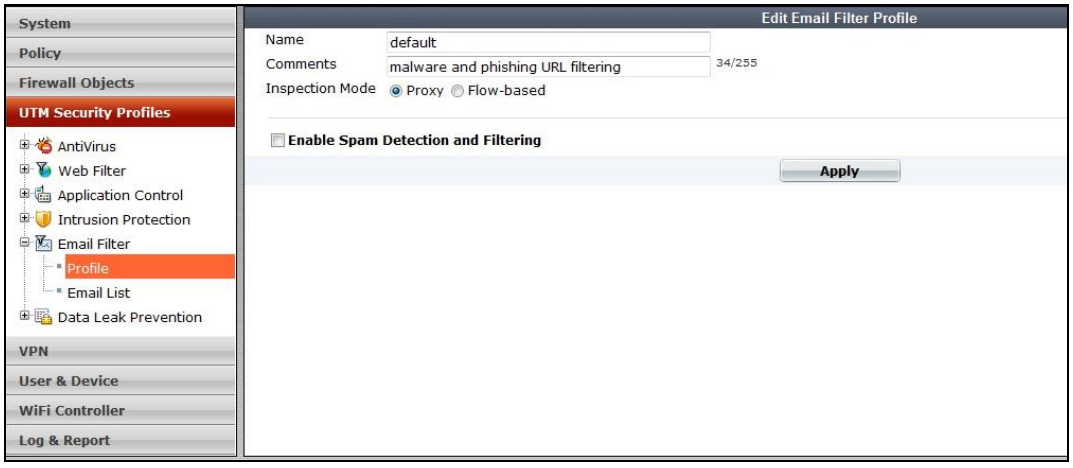


5. 이메일 필터(Email Filter)

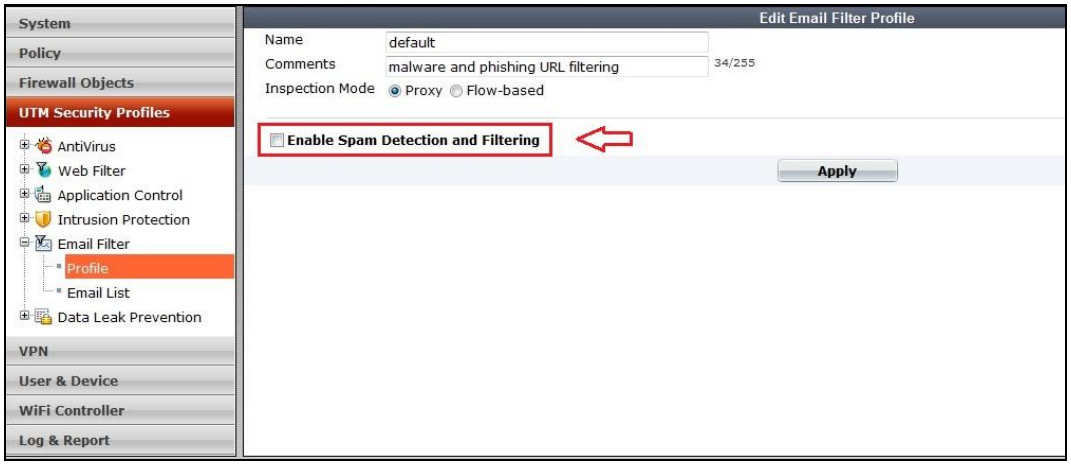
관리자는 Email Filter 를 사용하여 Email의 메시지에 단어 또는 파일 등에 대한 필터링을 할 수 있습니다.

▪ 이메일 필터 프로파일 생성 방법

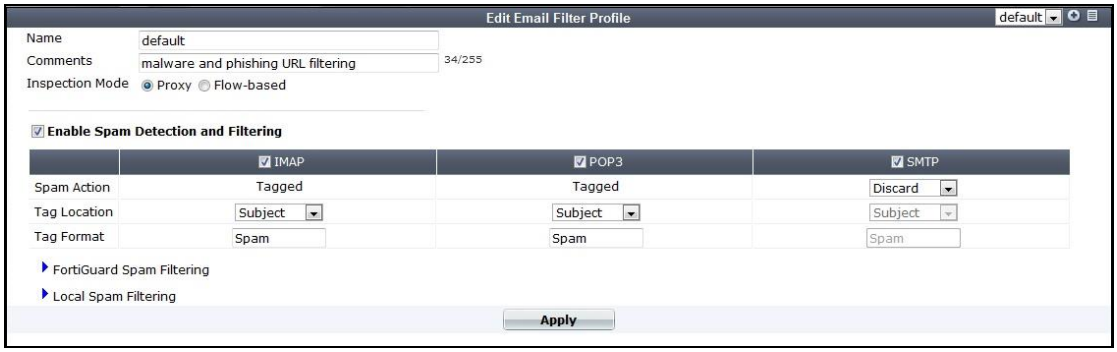
1. *UTM Security Profiles > Email Filter > Profile* 로 이동.



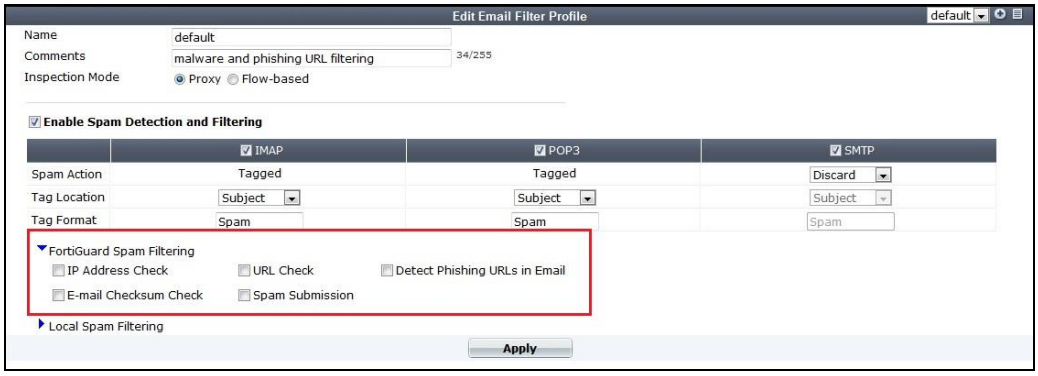
2. Enable Spam Detection and Filtering 활성



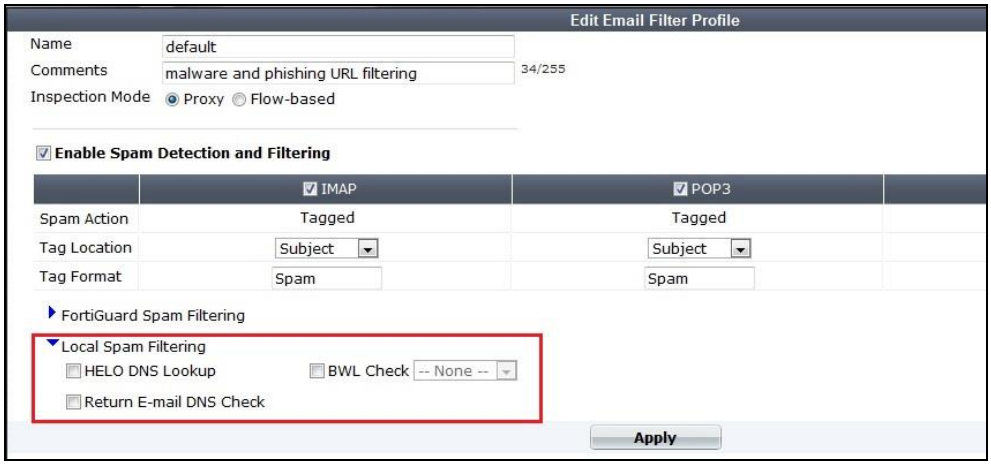
3. Spam Filter 기능을 적용하고자 하는 Protocol 에 대해 활성화 합니다..



4. FortiGuard Spam 라이선스가 있을경우 FortiGuard Spam Filtering 체크 후 Filtering 하고자 하는 option을 체크 합니다.

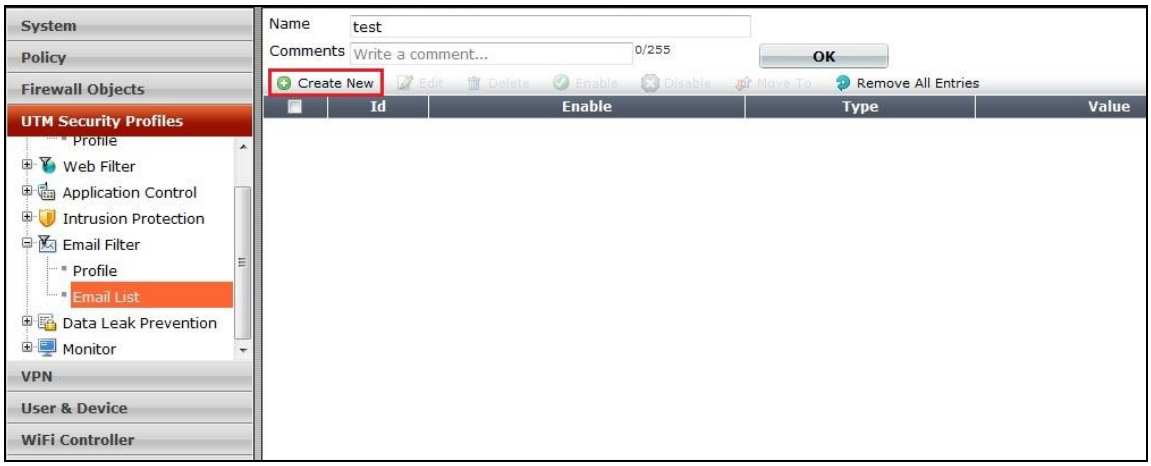


5. 별도의 라이선스가 없다면 Local Spam 기능으로 사용이 가능합니다.

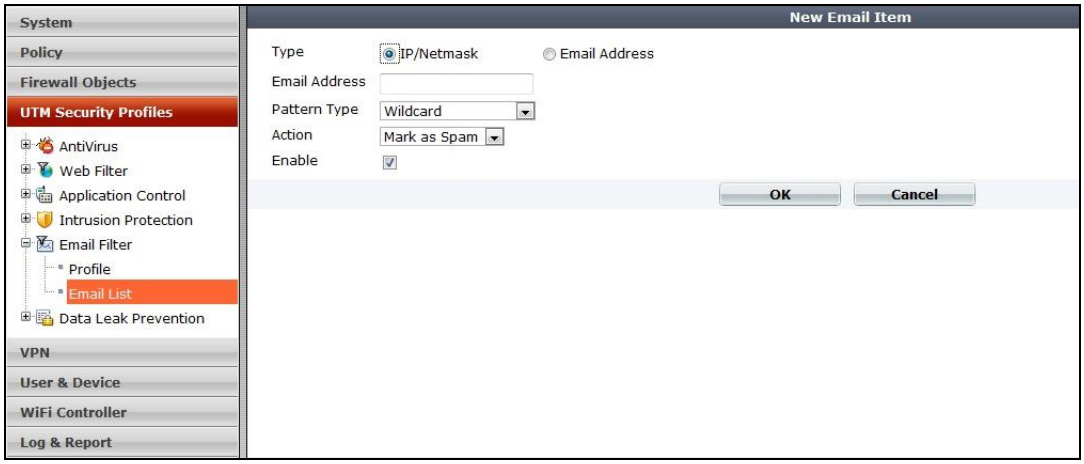


6. FortiGate Local 기능으로 이용 시 Email, IP 주소는 GUI 상으로 설정이 가능 하지만 Bword 를 설정 하기 위해서는 CLI로 가능합니다.

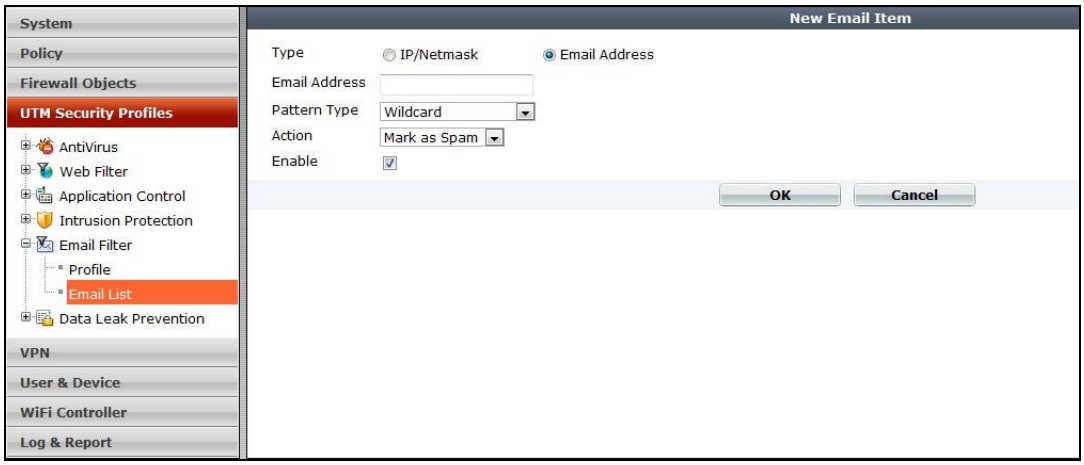
7. *UTM Security Profiles > Email Filter > Email list* 로 이동 후 Create New 선택.



8. Local DB IP 정의



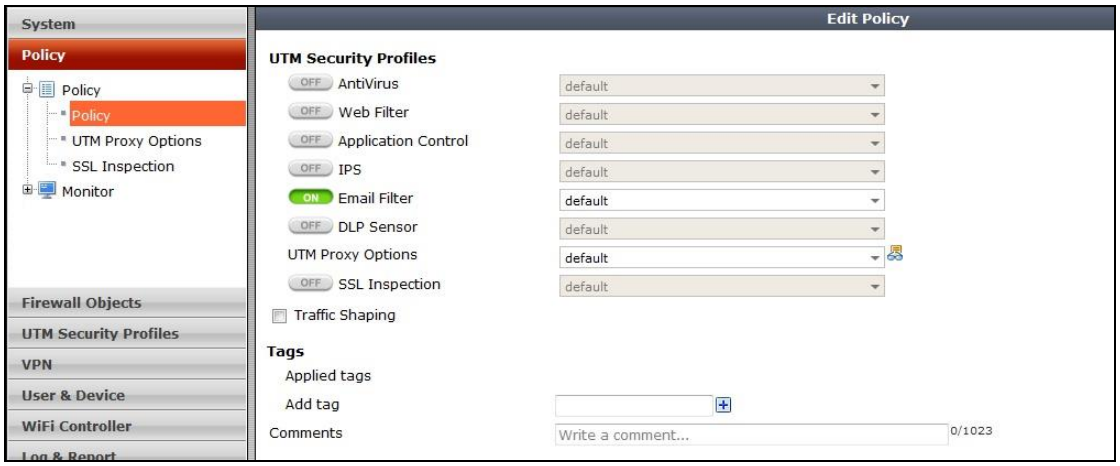
9. Local DB Email 정의



9. *OK* 선택.

- 적용방법

보안정책에서 해당 Email Filter 를 정의 합니다.

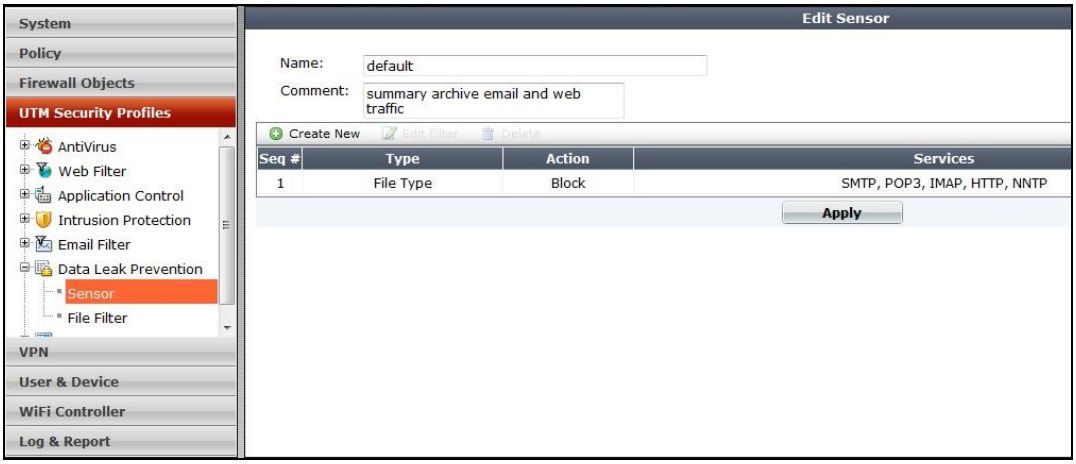


6.정보유출방지(Data Leak Prevention)

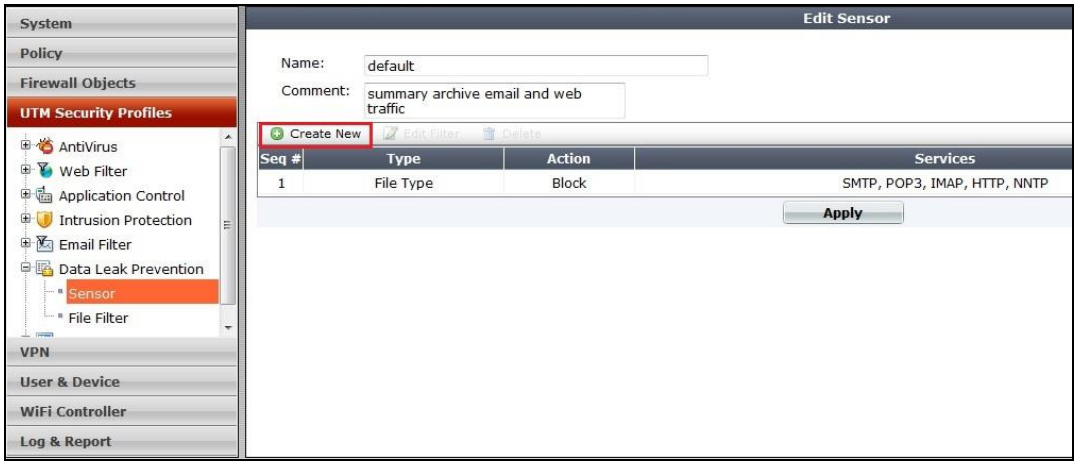
Data Leak Prevention 은 네트워크 내에서 민감한 데이터에 대한 유출을 방지 합니다.
관리자는 Foritgate에 파일형식, 파일크기, 정규표현, 고급규칙등을 통해 필터를 생성하고 보안정책에 해당 센서를 적용할 수 있습니다.

- DLP 센서 생성 방법

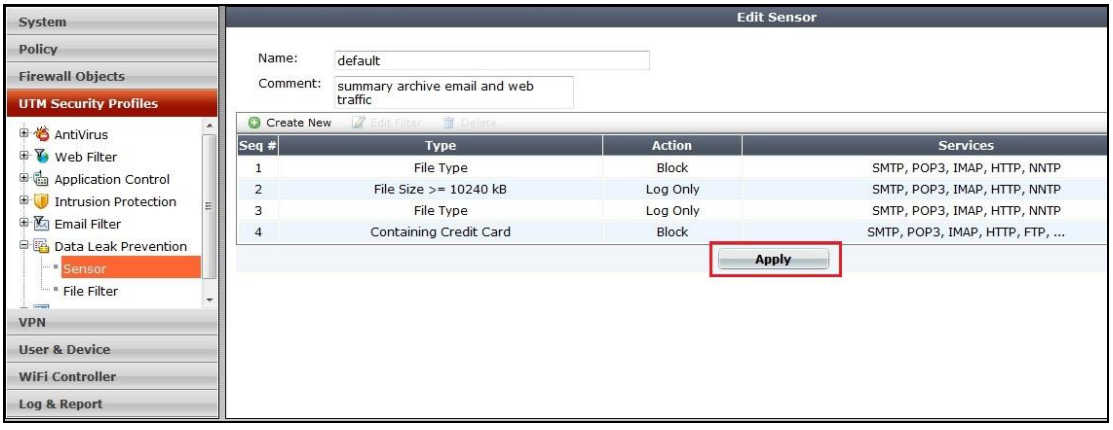
1. *UTM Security Profiles > Data Leak Prevention > Sensor* 로 이동.



2. *Create New* 를 선택하여 File에 대해 정의 합니다.



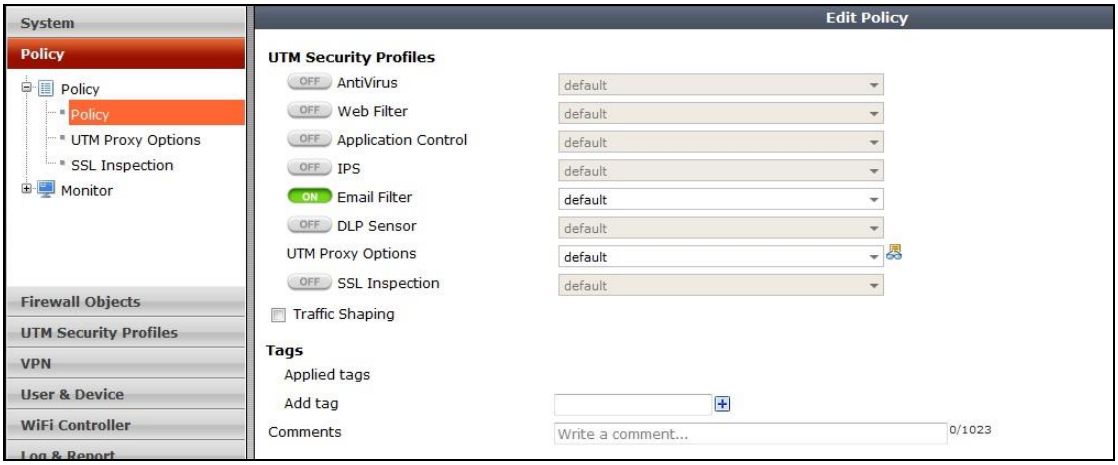
3. File에 대한 정의 후 Apply 를 클릭 합니다.



6. OK 선택.

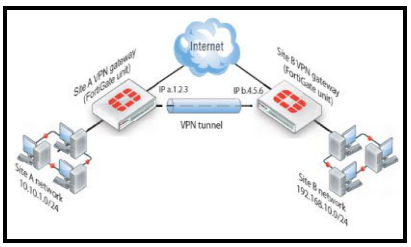
- 적용방법

보안정책에서 해당 Email Filter 를 정의 합니다.

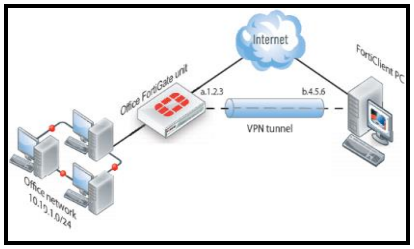


6.가상사설망(VPN)

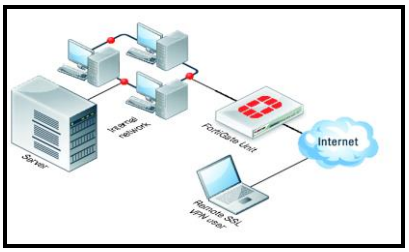
Fortigate시스템은 VPN기능을 지원합니다. VPN기능은 공중망을 이용하여 원격에 위치한 사설 네트워크 간의 통신을 가능하게 합니다. 공중망을 이용하기 때문에 트래픽에 대한 암호화와 인증을 통하여 보안위협으로 부터 보호를 합니다. Fortigate시스템에서 지원하는 VPN방식은 IPsec 과 SSL 방식을 지원합니다.



<IPsec VPN>



<Client IPsec>



<SSL VPN>

1. IPsec

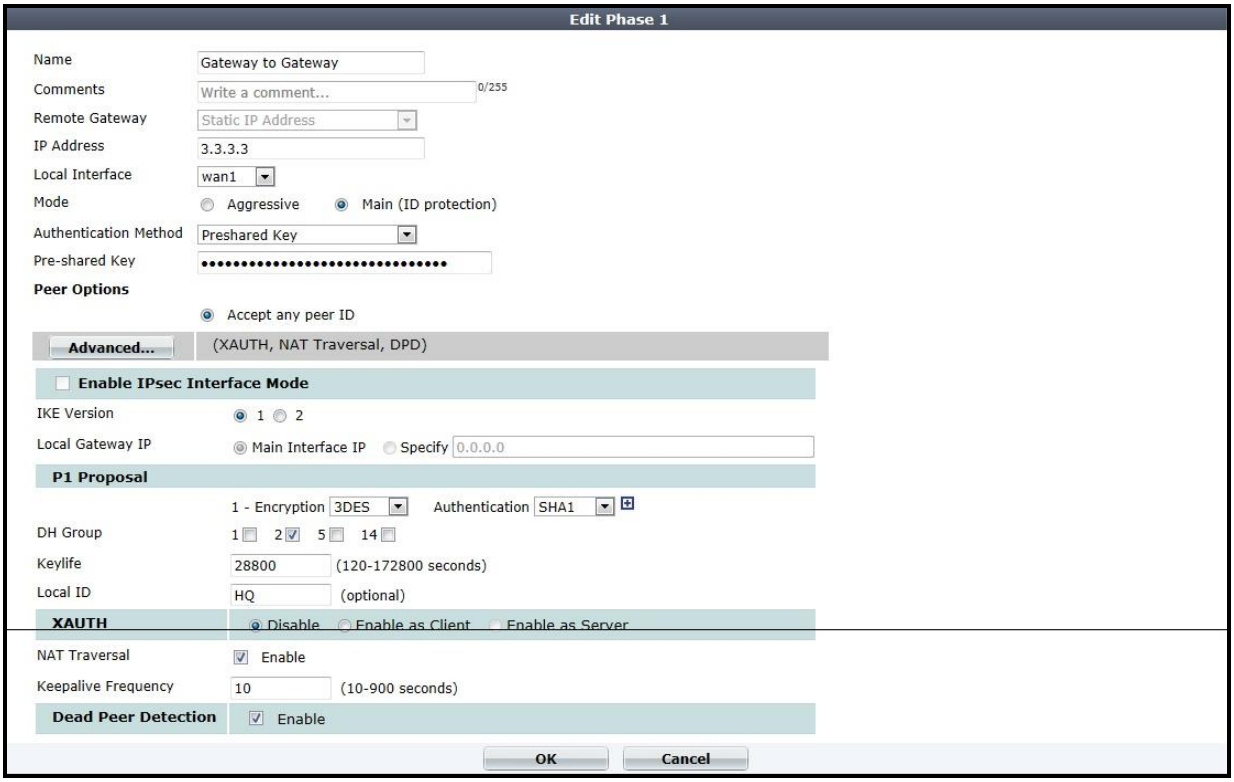
가장 많이 사용되는 VPN 방식으로 IP Security Protocol을 이용하여 VPN을 구현합니다. 장비 대 장비, 장비 대 클라이언트 간의 트래픽에 대하여 암호화,무결성,상대방 인증이 가능합니다. Fortigate는 Policy Base mode 와 Interface mode 방식으로 VPN을 구성할 수 있습니다.

1-1. Policy base mode

- Phase1 설정

IKE Phase2에서 SA관련 설정들을 안전하게 협상할 수 있도록 보안 채널을 생성합니다. 실질적인 데이터를 보호하는 것이 아니라 IKE Phase2에서 사용할 메시지들을 어떤 방식으로 보호할 것인지를 설정합니다. 이 단계에서 생성된 SA를 IKE SA라고 합니다.

Main Mode	다음 3쌍의 메시지를 교환해서 구현 합니다.
1st Pair	어떤 IKE SA 설정들을 사용할 것인지 협상을 합니다. 한 쪽이 자기가 지원하는 알고리즘을 상대방에게 알리면 이를 수신한 상대방이 그 중에서 자기가 지원하는 알고리즘으로 골라서 서로 협상을 합니다.
2dn Pair	첫 번째 메시지에서 결정된 사항을 바탕으로 Diffie-Helman 키 교환 방식에 의해 공개키 값을 교환함으로써 마스터 키를 설정하고 Phase2에서 사용할 메시지의 암호화에 사용할 키를 안전하게 교환합니다.
3rd Pair	두 번째 메시지에서 결정된 사항을 바탕으로 Diffie-Helman 키 교환 방식에 의해 인증서를 서로 교환함으로써 서로 간의 인증을 합니다.
Aggressive Mode	Main Mode보다 빠른 방식이라고 생각하면 됩니다. 3쌍의 메시지가 아닌 3개의 메시지를 교환하여 구현 합니다. 이 모드는 빠르게 협상을 할 수 있으나 Session ID가 노출 되어 보안성은 낮아집니다. 따라서 일반적으로 Main Mode를 권장합니다.



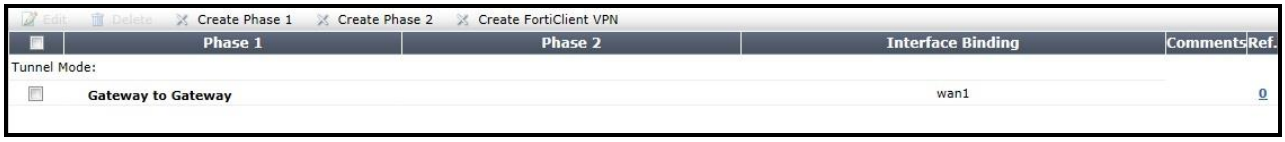
- IPsec Phase1 설정 화면 -

1. *VPN > IPsec > Auto Key (IKE) >* 우측화면 Create Phase1 클릭합니다.
2. Name에 Phase1의 이름을 넣습니다.
3. Remote Gateway에서 원격지 장비에 대한 접속 주소 타입을 설정합니다.
   - Stiatic IP Address : Remote 장비의 IP를 알고 있을 경우
   - Dialup User : 지사가 많거나 Remote 장비의 IP가 유동인 경우
   - Dynamic DNS : Remote 장비에 DDNS 설정이 되어있을 경우 주소 입력
4. IP Address : 터널을 맺을 상대방 장비의 IP를 넣어줍니다.
5. Local Interface : 원격지 장비로 나가는 인터페이스를 선택합니다.
6. Mode : Main, Aggressive 모드 중 선택을 합니다.
7. Authentication Method : Preshared Key , RSA Signature 중 선택
   - Preshared Key - Remote 장비와 동일하게 Key값 입력
   - RSA Signature - RSA 인증서을 사용하여 인증
8. Advanced 클릭 후 계속 입력
9. Enable IPsec Interface Mode는 선택하지 않습니다.
10. P1 Proposal : 암호화 DES,3DES,AES128,AES192,AES256 중 택1
    인증 MD5,SHA1,SHA256,SHA384,SHA512,Null 중 택1
11. DH Group : 1,2,5,14 중 선택
12. Keylife : 최소 120 ~ 최대 172800 Seconds 까지 입력
13. Local ID : Remote 장비에 어느 장비인지 알려주는 이름.
    예) 현재 세팅하는 장비가 HQ라고 하면 Local ID에 HQ입력. Remote 장비의 터널 모니터링에 HQ라고 표시되어 진다.

14. XAUTH : 추가 사용자 인증정보를 요구하여 보안을 향상시킨다. SecurID 사용자 그룹을 사용하는 경우 코드를 입력
15. Nat Traversal : Packet은 NAT장치를 통과 할 때 헤더의 원본 또는 주소가 수정된다. ESP Tunnel의 IPsec packet에서는 NAT를 수행 할 수 없다. 따라서 NAT장치가 존재할 때는 이 옵션을 사용하여 IPsec packet에 캡슐화의 레이어를 추가한다. Fortigate와 FortiClient는 Packet을 복호화 하기 전 캡슐화의 레이어를 제거한다.
16. Keepalive Frequency : Nat Traversal 을 사용 시 Keepalive Frequency 입력
17. Dead Peer Detection : Remote 장비가 VPN Tunnel 을 맺었다가 Tunnel이 떨어졌을 경우 감지한다.

18. Phase1의 설정값을 입력하고 OK를 클릭한다

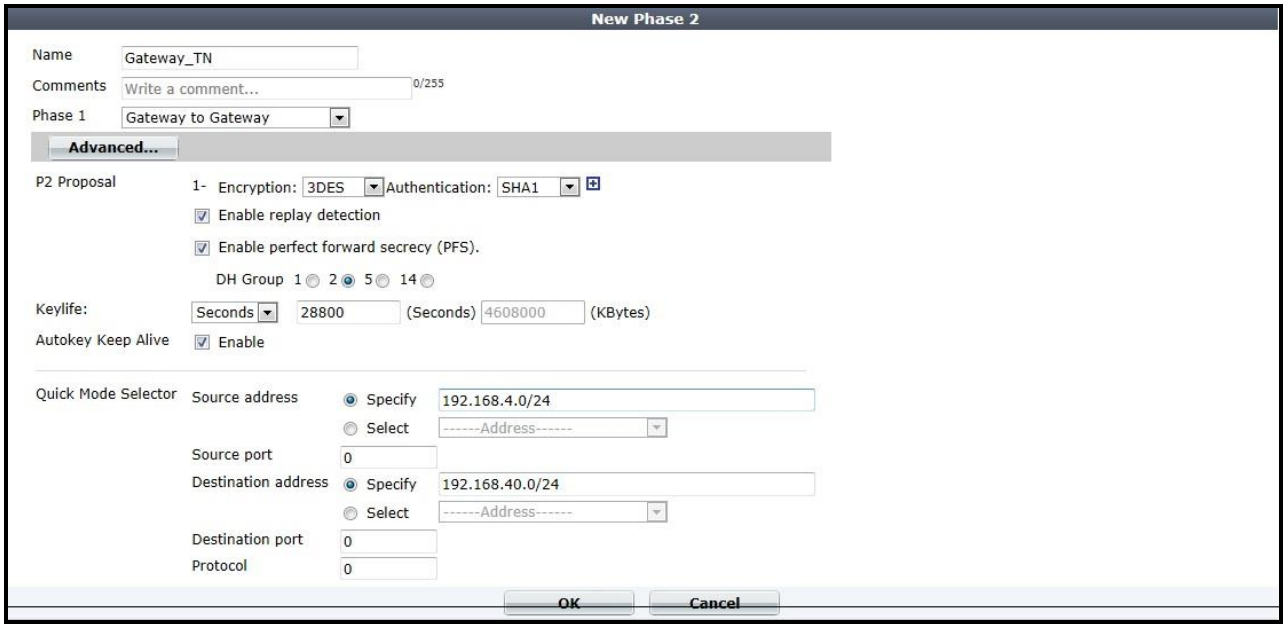
참고 > 위의 설정 값은 Remote 장비의 IP Address, Local ID를 제외한 설정이 모두 동일해야 합니다



- Phase1을 생성 한 후 화면 -

- Phase2 설정

Phase1 단계가 IPSec VPN을 구현하기 위한 준비 단계였다면 Phase2는 실질적인 IPSec 연결을 하는 단계입니다. 즉, 실질적인 데이터를 어떤 방식으로 보호할 것인지를 협상합니다. 이 단계를 통해 생성된 SA를 IPSec SA라고 하고 이 과정을 거치면 IPSec용 세션 키가 생성이 됩니다. 이러한 세션키를 이용하여 각 세션마다 세션 키가 달리 설정 되고 암호화 통신을 하게 됩니다.



1. *VPN > IPsec > Auto Key (IKE) >* 우측 화면 Create Phase2 클릭

2. Name : Phase2의 이름을 입력 , 주로 Phase1과 연관되도록 입력
3. Phase1 : 생성 해 놓은 Phase1을 선택
4. Advanced 클릭 후 계속 입력
5. P2 Proposal : Phase1과 같이 암호화, 인증 알고리즘을 선택

   Enable replay detection : 인증되지 않은 사용자의 IPSec패킷 도청으로 인한 재생 공격을 탐지 합니다.

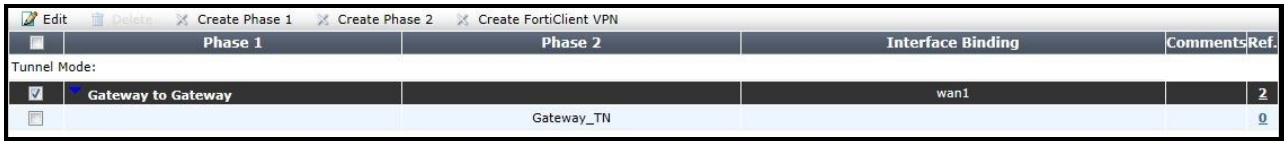
   Enable perfect forward secrecy (PFS) : Keylife 유효기간이 만료 될 때 마다 새로운 Diffie-Helman 교환을 강요하여 보안을 향상 시킵니다.

   DH Group : Diffie-Helman 그룹을 선택합니다. 이 설정은 원격지 장비 또는 클라이언트 사용자의 DH그룹과 일치해야 합니다.

   Keylife : Phase2의 키가 만료되는 시점을 설정합니다.

   Autokey Keep Alive : VPN터널로 데이터가 흐르지 않아도 터널을 활성 상태로 유지 시킵니다.
6. Quick Mode Selector : IKE 협상에 사용할 출발지 주소와 목적지 주소를 설정합니다.
7. Phase2의 설정 값을 입력하고 OK 클릭한다

참고 > 위의 설정 값은 Remote 장비와 모두 같아야 한다



- Phase2을 생성 한 후 화면 -

위와 같이 IPsec에 대한 세팅은 모두 끝났으며, 다시 정책으로 돌아가 정책을 생성합니다.

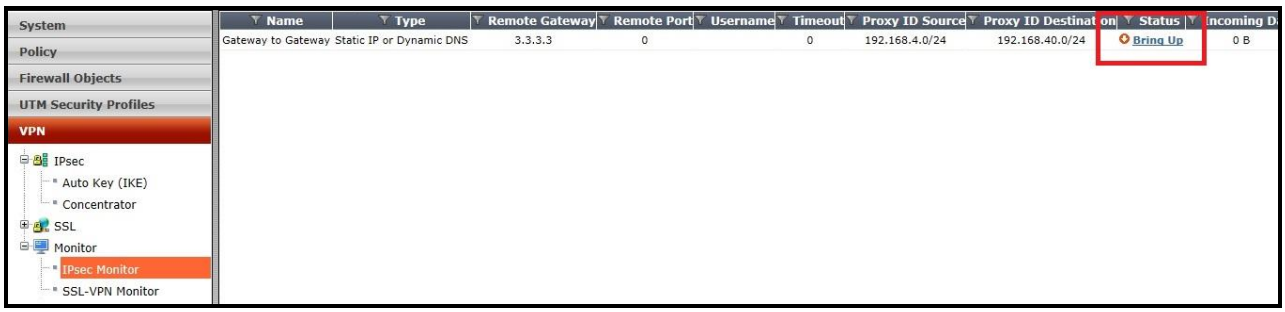
▪ IPsec 정책 설정

1.Policy Type : VPN을 선택

2. Policy Subtype : IPsec 선택
3. Local Interface : VPN 통신을 할 출발지 인터페이스를 선택합니다.
4. Local Protected Subnet : VPN 통신을 할 출발지 주소를 선택합니다.
5. Outgoing VPN Interface : 원격지 VPN 장비로 나가기 위한 인터페이스를 선택합니다.
6. Remote Protected Subnet : VPN 통신을 할 목적지 주소를 선택합니다.
7. Schedule, Service : 일정과 Port 설정
8. VPN Tunnel : Create New – 현재 정책을 생성하면서 터널을 같이 생성할 수 있습니다.
   Use Existing – 미리 정의 해놓은 터널을 사용합니다. VPN Tunnel – 생성된 Auto Key (IKE) 선택
   Allow traffic to be initiated from the remote site – 체크

9. 위의 세팅이 완료되면 OK 클릭합니다.

– IPsec VPN 정책 생성 완료 화면–

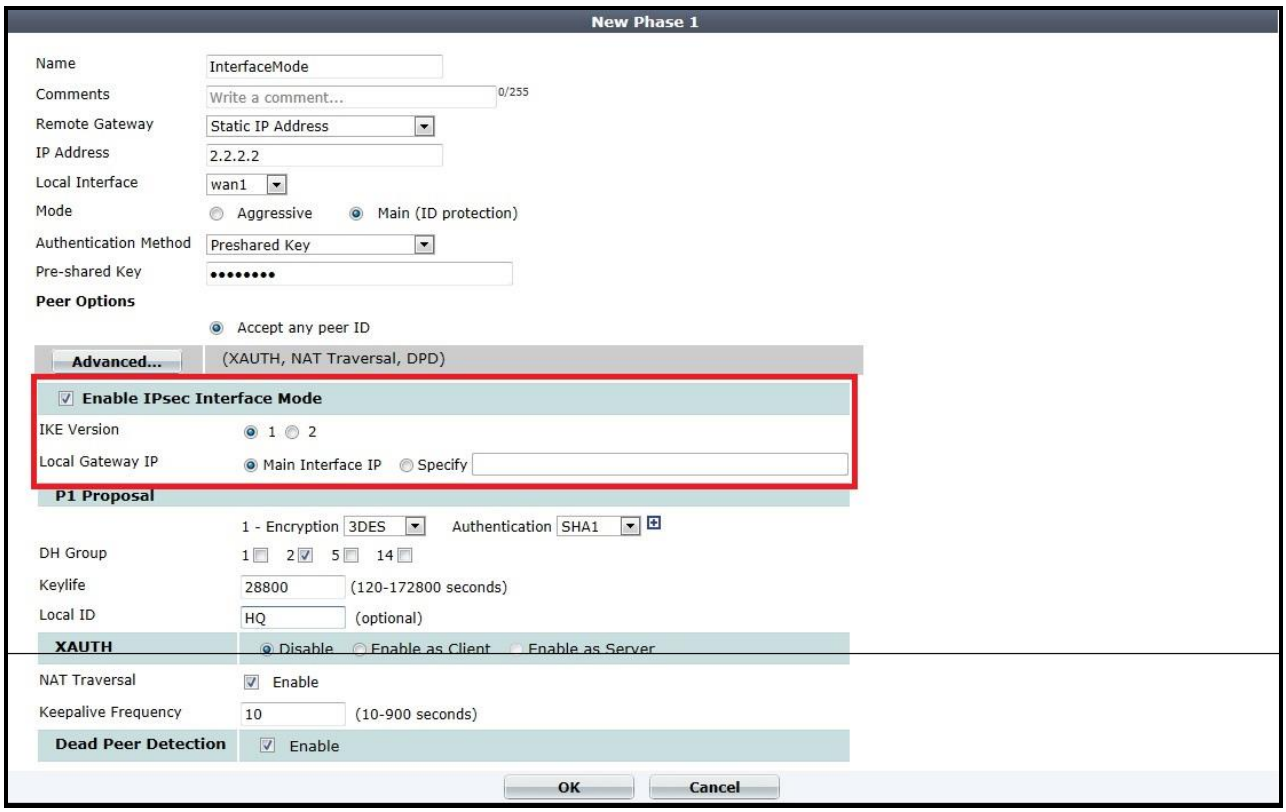


VPN > Monitor > IPsec Monitor 에서 터널 모니터링을 할 수 있습니다. Bring UP을 클릭하게 되면 Bring Down으로 바뀌면서 Tunnel이 업이 됩니다.

1-2. Interface mode

Route-based VPN이라고도 하며 VPN터널을 생성하면 가상의 인터페이스가 생성이 되고 이 인터페이스를 이용하여 정책을 설정합니다. 가상의 인터페이스가 생기기 때문에 VPN 트래픽에 관련된 트러블 슈팅이 용이한 장점이 있습니다. NAT모드에서만 지원합니다.

- Phase1 설정



Interface Mode의 설정 방법은 Policy Base Phase1방법과 동일하며 추가로 Enable IPsec Interface Mode에 체크합니다.

- Phase1을 생성 한 후 화면 -

▪ Phase2 설정

Policy Base mode Phase2와 동일하게 설정 하면 됩니다. (Policy Base Phase2 설정 방법 참조)

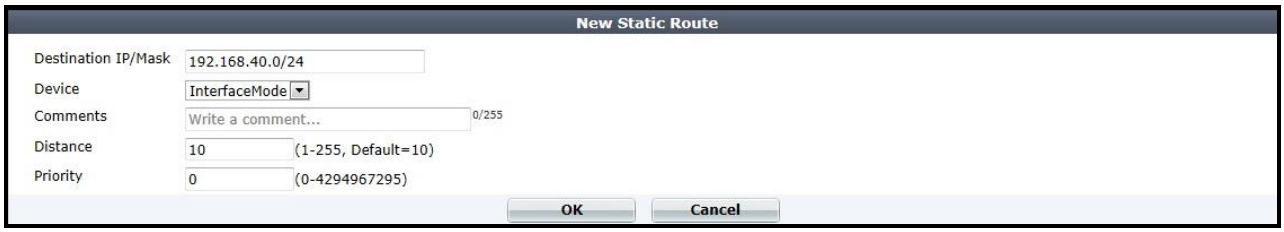
- Phase2을 생성 한 후 화면-

Interface mode로 터널을 생성하면 *System > Network > Interface* 의 wan1 인터페이스에 VPN터널 이름의 가상 인터페이스가 생성된 것을 볼 수 있다. 이 인터페이스를 통하여 목적지와 통신을 하기 때문에 목적지에 대한 라우팅 설정을 해야 합니다.

- Type이 Tunnel 이라는 가상 인터페이스가 생성된 것을 볼 수 있다 -

▪ Route 추가

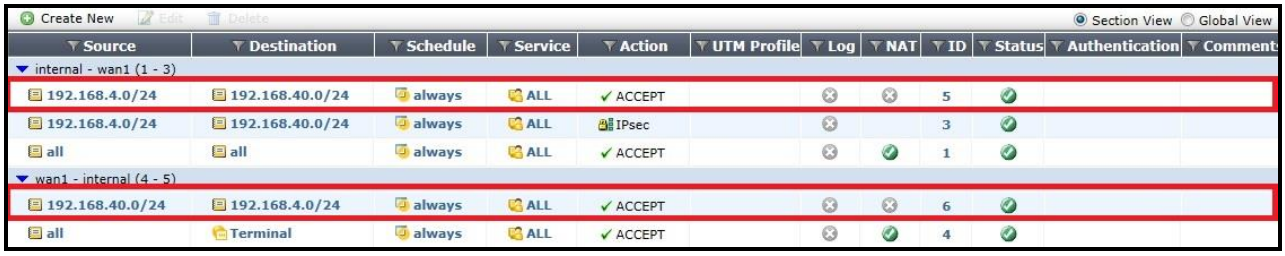
원격지 네트워크를 Destination IP/Mask에 설정하고 Device를 가상 인터페이스로 선택합니다.



- 가상 인터페이스로 라우팅을 추가한 모습 -

▪ 정책추가

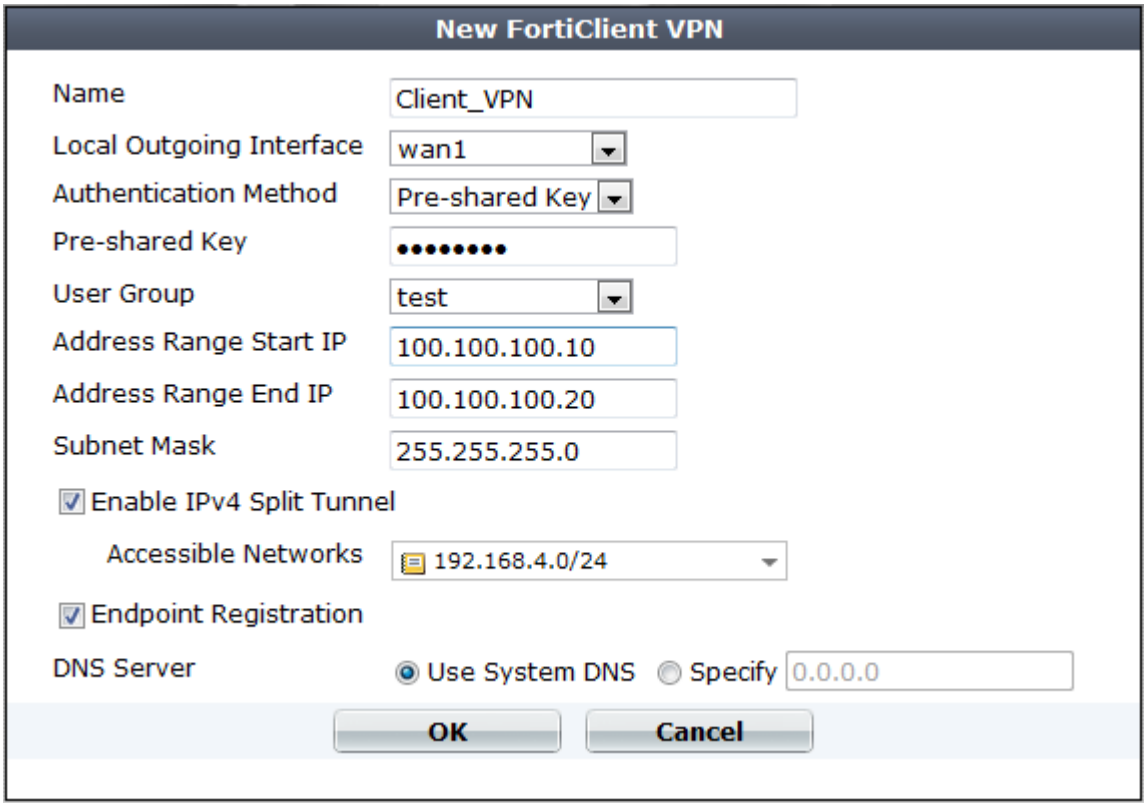
생성된 가상 인터페이스를 이용하여 통신 정책을 생성합니다. Policy Base와 다르게 VPN정책으로 설정하지 않고 일반 방화벽 정책으로 설정하며 양방향 생성 하여야 서로 통신이 가능합니다.



Bring UP을 클릭하게 되면 Bring Down으로 바뀌면서 Tunnel이 업이 된다.

1-3. Client VPN

Fortigate시스템은 사용자가 Client 프로그램을 이용하여 IPSec VPN을 구성할 수 있도록 합니다.
이러한 클라이언트 VPN에 대한 터널생성을 간단하게 할 수 있습니다.

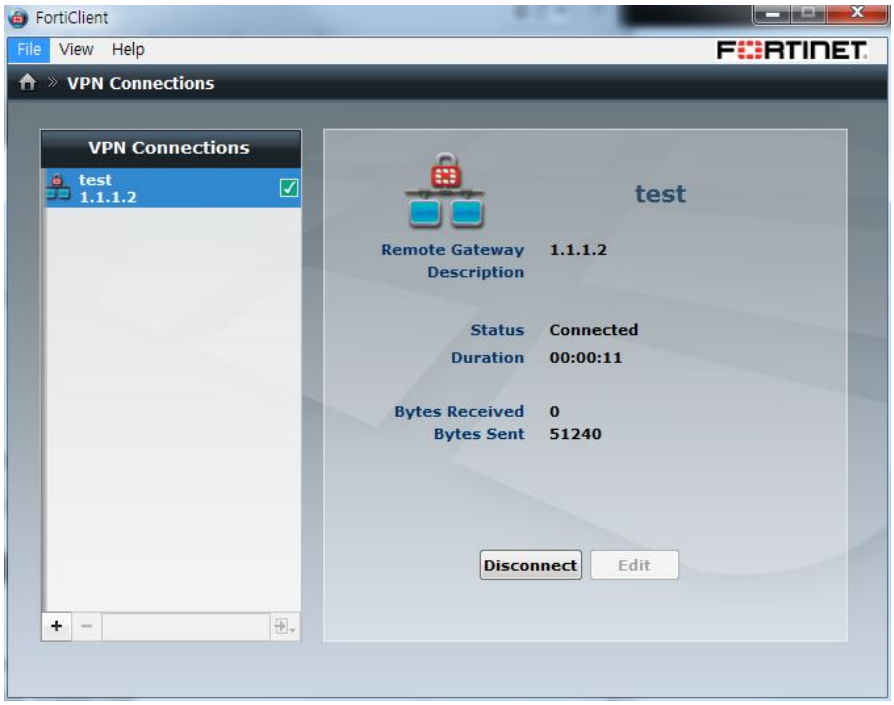


- Client VPN 설정 화면 -

Name	VPN터널 이름을 설정합니다. 터널 생성이 완료되면 설정이름으로 된 가상 인터페이스가 생성 됩니다.
Local Outgoing Interface	VPN사용자와 통신 할 인터페이스를 설정합니다.
Authentication Method	인증 방법을 설정합니다.
Pre-shared Key	공유키를 설정합니다.
User Group	인증 할 사용자를 선택합니다.
Address Range Start IP	사용자에게 할당 할 IP대역의 시작을 설정 합니다.
Address Range End IP	사용자에게 할당 할 IP대역의 끝을 설정합니다.
Enable IPv4 Split Tunnel	통신대역에 대한 분산 처리를 설정합니다.
Accessible Networks	사용자가 접속 할 목적지주소를 설정합니다.
Endpoint Registration	VPN연결이 설정 되기 전에 FortiClient로 등록키를 요구합니다. 등록키는 *System > Config > Advanced* 에서 설정합니다.
DNS Server	사용자에게 할당할 DNS를 설정합니다.

- Client VPN 생성이 완료되면 해당 이름의 가상 인터페이스가 생성됩니다. Interface Mode VPN설정과 마찬가지로 사용자에게 할당 할 대역을 생성된 인터페이스로 라우팅을 설정하고 가상인터페이스에서 내부인터페이스로의 접근허용 정책을 생성하면 설정이 완료 됩니다.

– FortiClient VPN 설정 화면 –



– Client VPN으로 연결 된 화면 –

1-4. Concentrator

본사와 지사가 IPSec VPN을 연결 되어 있을 때 본사는 고정IP 회선을 사용하고 지사는 유동IP회선을 사용하는 경우가 있습니다. 이러한 구성에서 Concentrator 기능은 유동IP 회선을 사용하는 지사 간의 VPN 통신을 가능하게 합니다. 본사 장비와의 터널을 통하여 지사 간의 통신이 이루어 집니다.

1. *VPN > IPsec > Concentrator* 로 이동합니다.
2. 서로 통신을 하기 위해 생성된 Tunnel들을 Members로 추가시킵니다.
3. 본사 장비의 정책은 출발지주소는 본사 대역을 포함한 서로 통신할 지사 대역을 모두 설정 합니다. 목적지주소는 서로 통신할 지사 대역 모두 설정합니다.
4. 지사 장비의 정책은 출발지 주소는 해당 지사 대역을 설정합니다. 목적지는 본사 대역을 포함한 서로 통신할 지사 대역을 모두 설정 합니다.

2. SSL VPN

SSL(Secure Socket Layer) 프로토콜을 이용하여 VPN을 구현 합니다. 사용자는 별도의 프로그램이 필요 없고 웹 브라우저만 있으면 VPN접속을 할 수 있기 때문에 사용에 많은 편의를 제공합니다. Fortigate시스템은 다음의 세가지 모드를 지원합니다.

Web-access mode	Fortigate가 Proxy 역할을 수행합니다. 사용자는 Fortigate에 요청을 하고 Fortigate는 서버와 통신 한 결과를 사용자에게 돌려줍니다. 접속 할 수 있는 서비스가 제한 됩니다.
Tunnel-access mode	IPSec과 같이 터널을 연결하여 사용자가 직접 서버와 통신합니다. 모든 서비스포트로 통신이 가능합니다.
Full-access mode	Web-access와 Tunnel-access 모드를 같이 지원합니다.

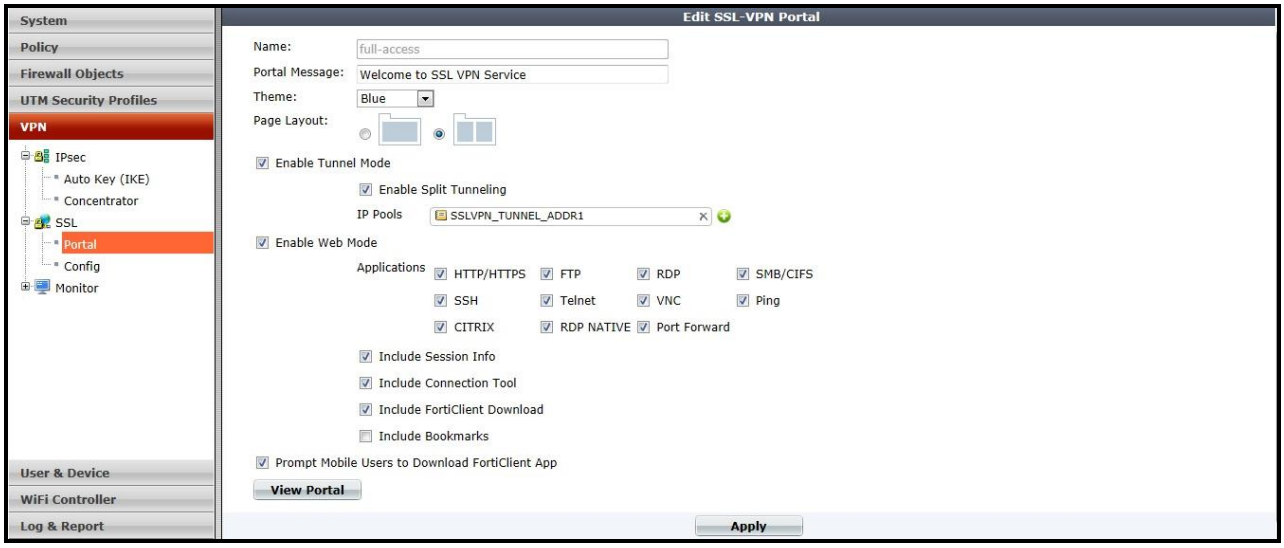
사용자 ID/PW는 Fortigate시스템에 직접 생성하여 사용하거나 원격 인증 서버와 연동하여 사용합니다.

IOS, Android모바일에서도 SSL-VPN Client 를 지원합니다.

2-1. SSL-VPN 설정

2-1-1. 포탈(Portal)

사용자가 SSL-VPN으로 연결되어 보여질 웹페이지의 레이아웃과 사용자에게 할당 될 IP대역을 설정합니다.



1. *VPN > SSL > Portal* 로 이동합니다.
2. Enable Tunnel Mode : Tunnel Mode를 사용할 경우 Enable

   Enable Split Tunneling : 활성화 할 경우 Client들은 SSL-VPN을 통하여 모든 트래픽을 내보냅니다.

   비활성화 할 경우 각 Client가 속한 회선을 통하여 인터넷을 합니다.

   IP Pools : Client들은 내부 망과 통신하기 위해 VIP를 할당 받습니다.
3. Enable Web Mode : Web Mode를 사용할 경우 Enable

   Applications : VPN portal 을 통해 연결되면 사용자가 Access 할 수 있는 응용프로그램을 선택합니다.

   Include Session Info : Portal 페이지에 세션정보 위젯을 표시하려면 선택한다

   사용자의 로그인 ID,로그인한 시간, 트래픽 통계를 나타낸다

   Include Connection Tool : Portal 페이지에 연결도구 위젯을 표시하려면 선택한다

   유형을 선택하고 Host의 URL 또는 IP주소를 지정한다

   Include Bookmarks : Web Portal에서 북마크를 포함하려면 선택한다

   내부 망의 리소스에 대한 즐겨찾기 링크로 사용된다

   즐겨찾기 목록에서 선택하면 팝업 창에 웹페이지가 표시된다

   Telnet,VNC,RDP 플러그인이 필요하며, FTP와 삼바는 파일브라우저를 HTML로 북마크 페이지를 대체한다
4. Prompt Mobile Users to Download FortiClient App

   : 원격사용자가 웹 브라우저를 사용할 경우 FortiClient를 다운로드 할 것인지 묻는 메시지가 나타난다

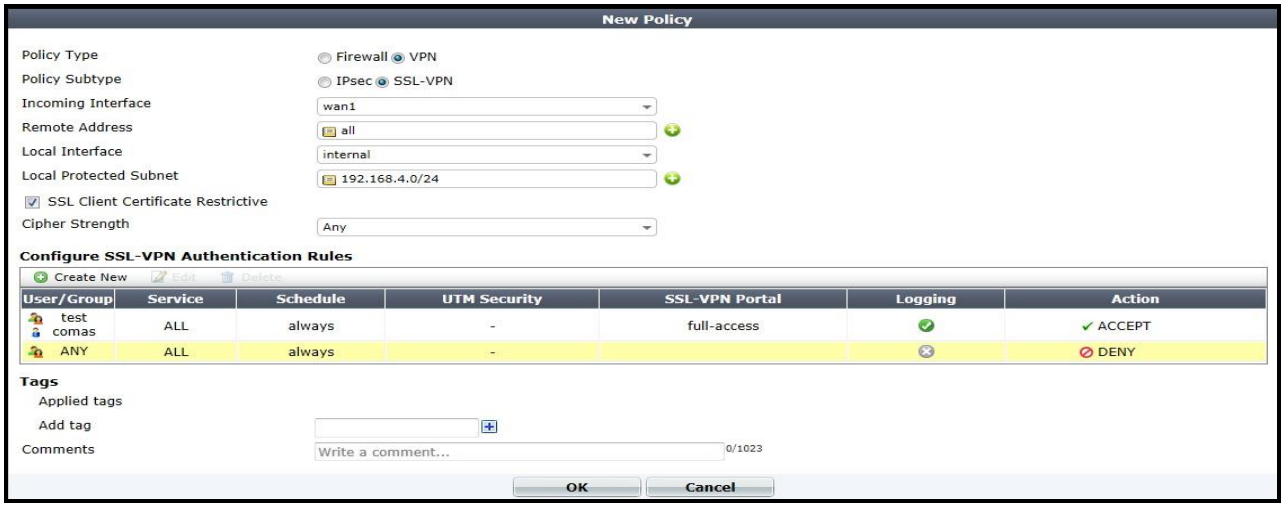
   사용자는 알림을 수락하거나 거부할 수 있다. 만약 수락하면 FortiClient 웹사이트로 리다이렉션 된다

2-1-2. 설정(Config)

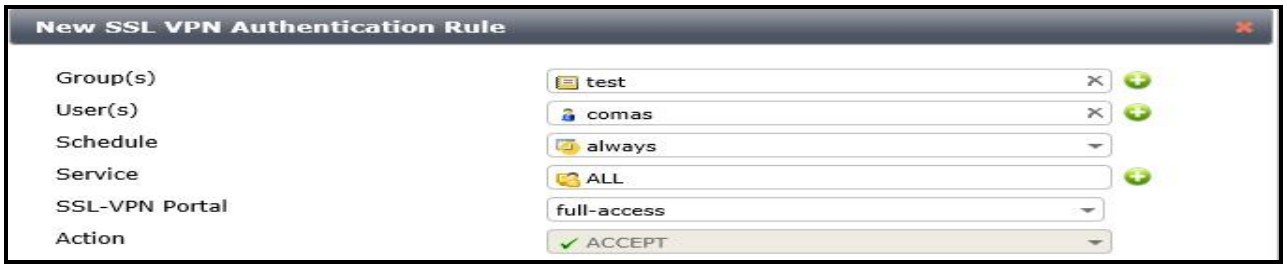
1. IP Pools : Tunnel Mode에서 Client들이 받아가는 IP Address 선택
2. Server Certificate : 인증에 사용할 서명된 서버 인증서를 선택한다
   Self-Signed(default)로 선택하면 Fortigate의 기본 인증서를 제공한다
3. Require Client Certificate : Client를 인증하는 인증서를 사용하려면 선택
   Client가 Tunnel 연결을 시작하면 Fortigate는 인증 프로세스의 일환으로 Client의 인증서를 확인하는 메시지가 나타난다
4. Encryption Key Algorithm : Client와 Fortigate 사이의 보안 SSL연결을 만들기 위해 알고리즘을 선택
5. Idle Timeout : SSL VPN 연결을 유지 할 수 있는 시간을 입력한다 (SSL session에 적용된다)
   범위는 10~28800 초 이며, 값을 0 으로 설정하면 Idle Timeout는 비활성화된다
6. Login Port : HTTPS access를 위한 port number를 입력한다
7. Enable Endpoint Registration (Tunnel Mode Only) : FortiClient가 Fortigate에 등록되도록 선택
   (단, Tunnel Mode에서 사용)
8. Advanced를 클릭하여 DNS 및 WINS Server 정보를 입력한 후 Apply 클릭

2-1-3. 정책 및 라우팅 세팅

1. 외부 -> 내부 : 외부에서 내부로 SSL VPN 정책 설정

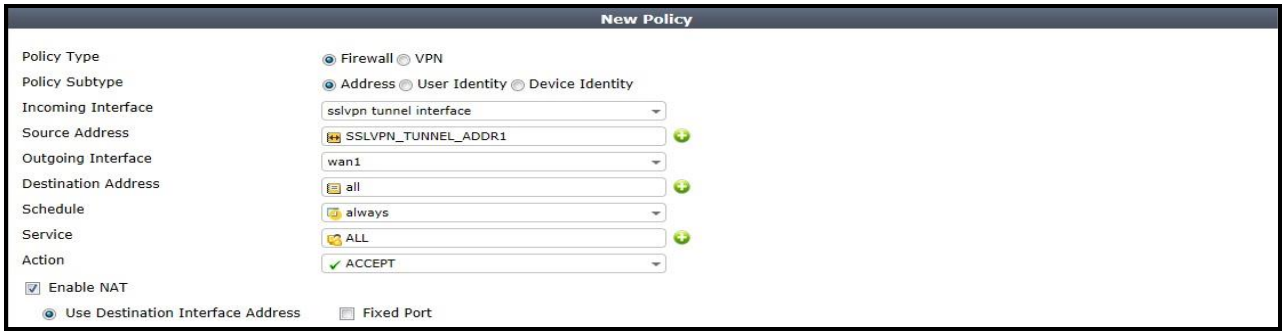


Configure SSL-VPN Authentication Rules : Creat New를 클릭하여 접근할 User/Group 및 Portal설정



2.SSL_interface -> 내부 : SSL.root 가상 interface에서 내부 Local interface로 정책 활성화

3. SSL_interface -> 외부 : 이 정책은 split tunneling 비활성화 할 경우 Client의 인터넷이 Fortigate를 통하여 나가기 때문에 설정한다(활성화 할 경우 설정할 필요 없다)



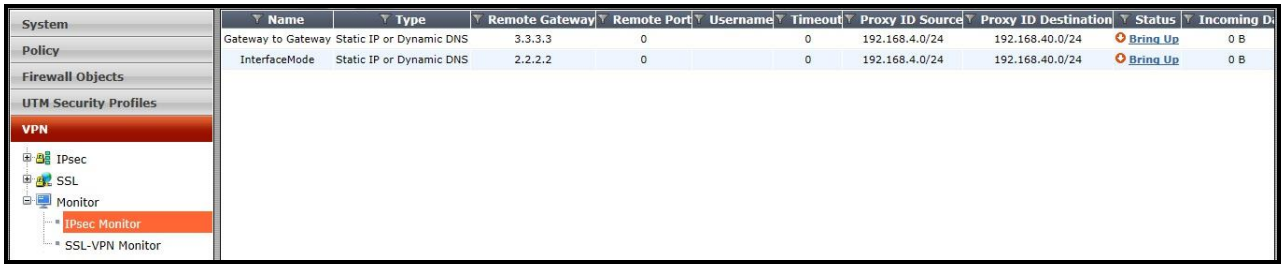
4. route 설정 : SSL 대역을 SSL 가상 interface로 라우팅을 설정한다

2-1-4. 모니터(Monitor)

IPsec , SSL VPN 을 모니터링 할 수 있다

- IPsec Monitor

IPsec Tunnel에 대해서 Tunnel Name, Type , Remote Gateway, port , Timeout 등 모니터링 한다



- SSL-VPN Monitor

SSL VPN을 사용하고 있는 User ID, Remote IP , 시작시간, User VIP 를 모니터링 한다


Delete

	No.	사용자	출발지 IP	시작 시간	설명
	1	Eun		Fri Mar 15 09:05:31 2013	
			서브세션		터널 IP:192.168.2.1
	2	Seo		Fri Mar 15 15:47:04 2013	
			서브세션		터널 IP:192.168.2.3
	3	Jang		Fri Mar 15 16:16:09 2013	
			서브세션		터널 IP:192.168.2.2
	4	Son	203.	Fri Mar 15 10:26:56 2013	
			서브세션		터널 IP:192.168.2.4
	5	Lee Hoseob	175. .19	Fri Mar 15 16:16:34 2013	
			서브세션		터널 IP:192.168.2.6
	6	Cha	183.	Fri Mar 15 10:41:58 2013	
			서브세션		터널 IP:192.168.2.5

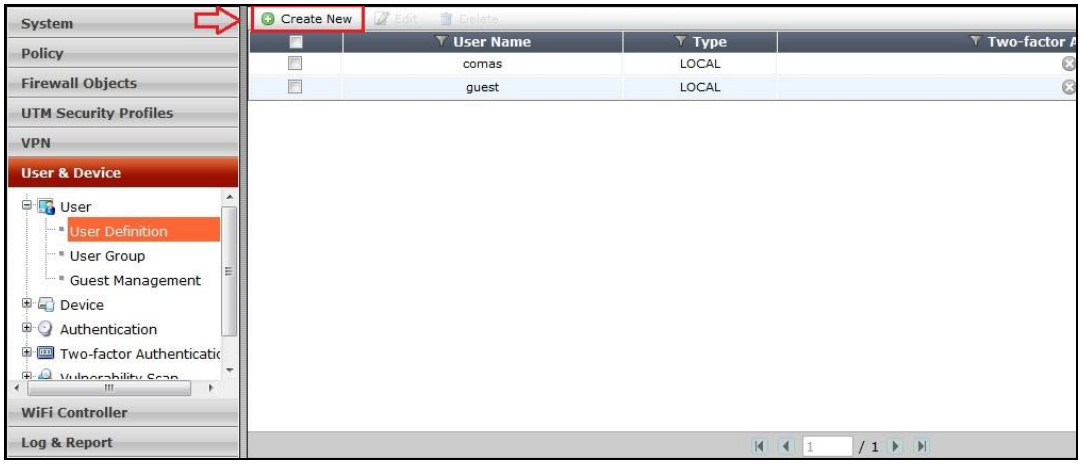
7. 사용자 & 장치(User & Device)

FortiOS 5.0 에서는 사용자에 대해서 Fortigate 에 정의된 IP로만 분류 하는 것이 아니라 User ID, Device, 원격 인증, Forti-Token 등을 이용, 다양한 인증 방법을 통해 분류가 가능합니다.

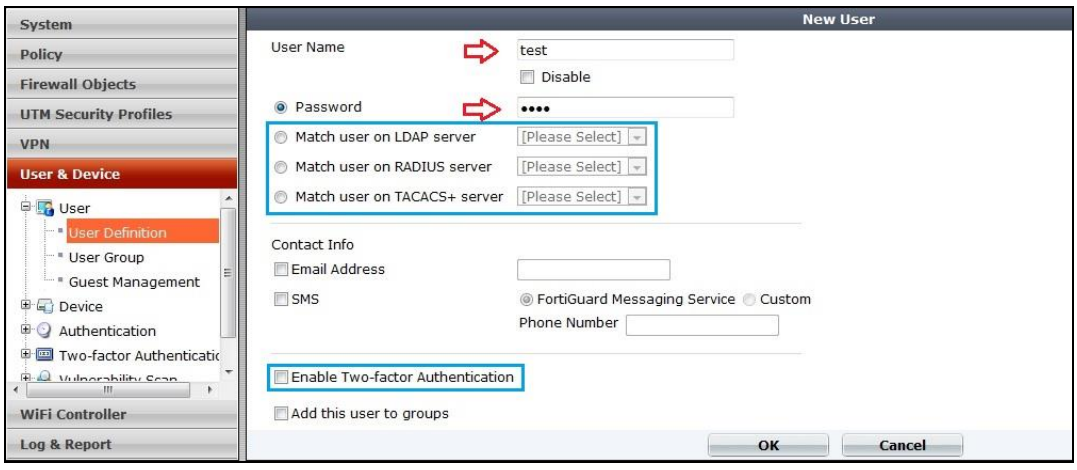
1. 사용자(User)

기본적인 인증방법으로써 Fortigate 자체에 ID/PW 를 통한 사용자 인증을 제공합니다.

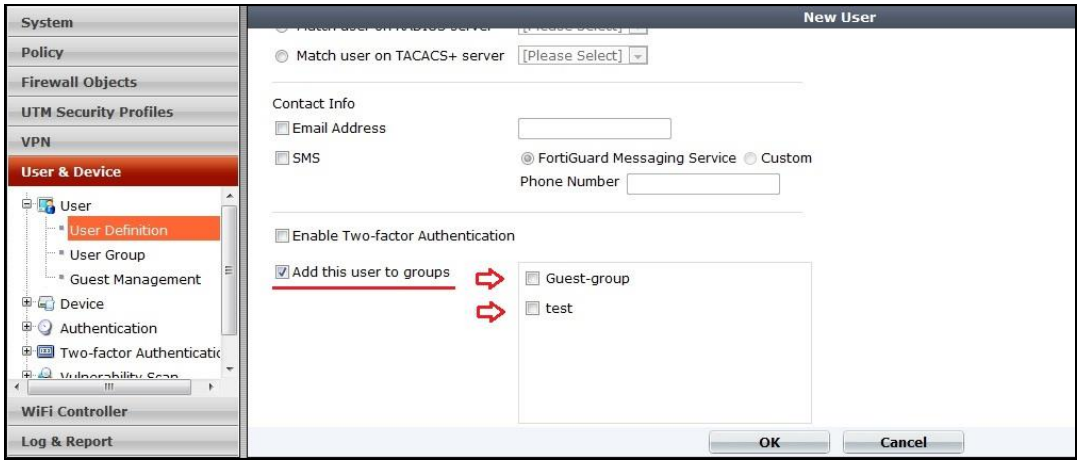
1. *User & Device > User > User Definition* 로 이동 후 *Create New* 선택.



2. User Name 및 Password 를 입력 후 OK 선택.

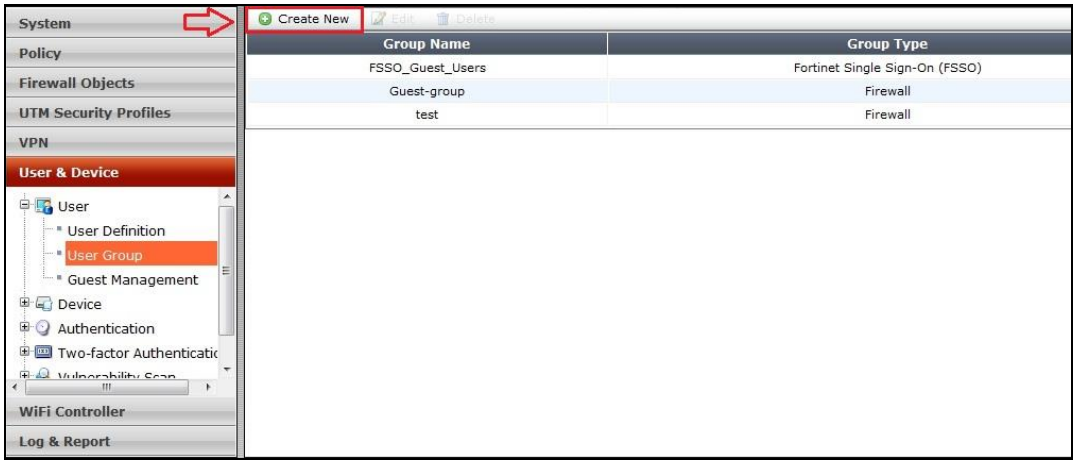


위의 그림에서 파란색으로 표시된 부분은 아래의 Authentication, Two-factor Authentication 이 사전에 구성되어 있어야 설정이 가능합니다.

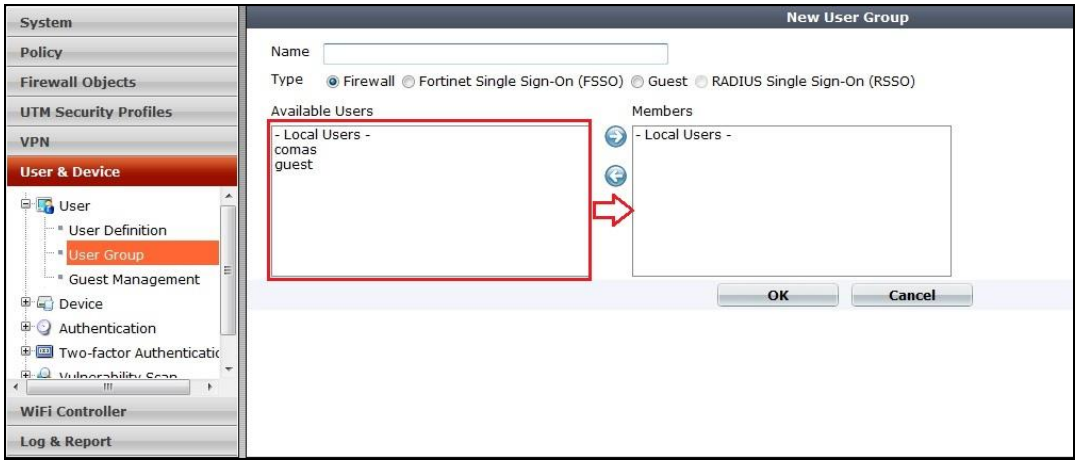


User 생성 시 Add this user to groups 를 통하여 기존에 만들어진 User Group 에 빠르게 포함 할 수 있습니다.

3. *User & Device > User > User Group* 로 이동 후 *Create New* 선택.

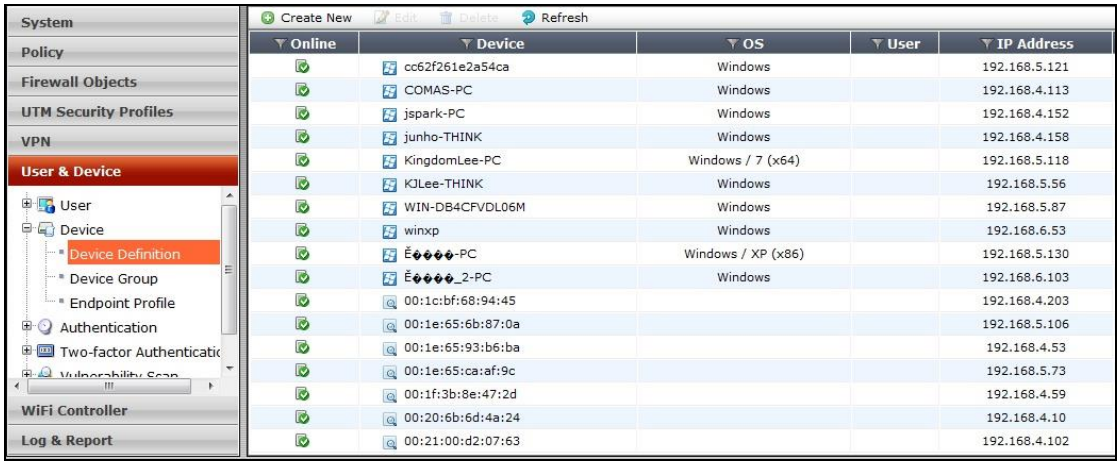


4. User Entry 에서 우측으로 이동시켜 만들고자 하는 그룹에 포함시켜 줍니다.

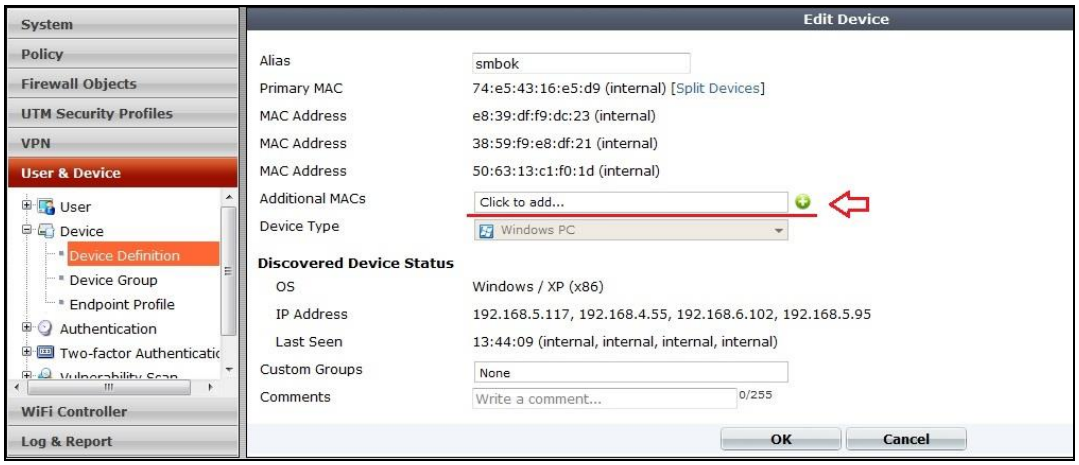


2. 장치(Device)

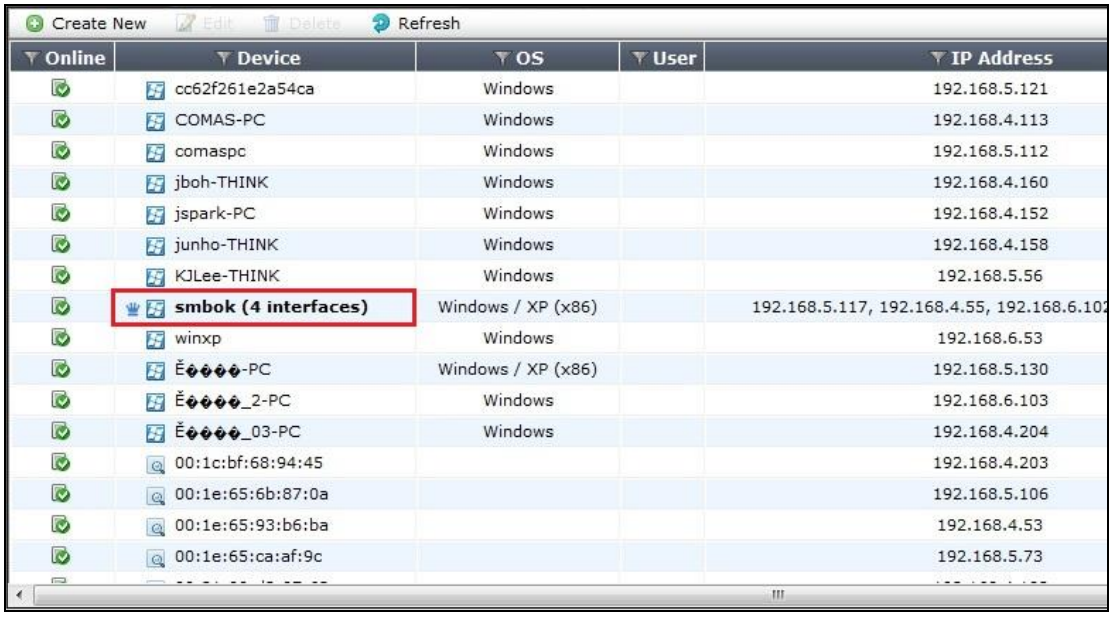
FortiOS 5.0 에서는 Network에 연결 된 Device를 확인 할 수 있습니다.
Device의 OS, IP, Mac 주소등을 확인 할 수 있기 때문에 관리자 측면에서 내부 사용자들을 한눈에 볼 수 있습니다.



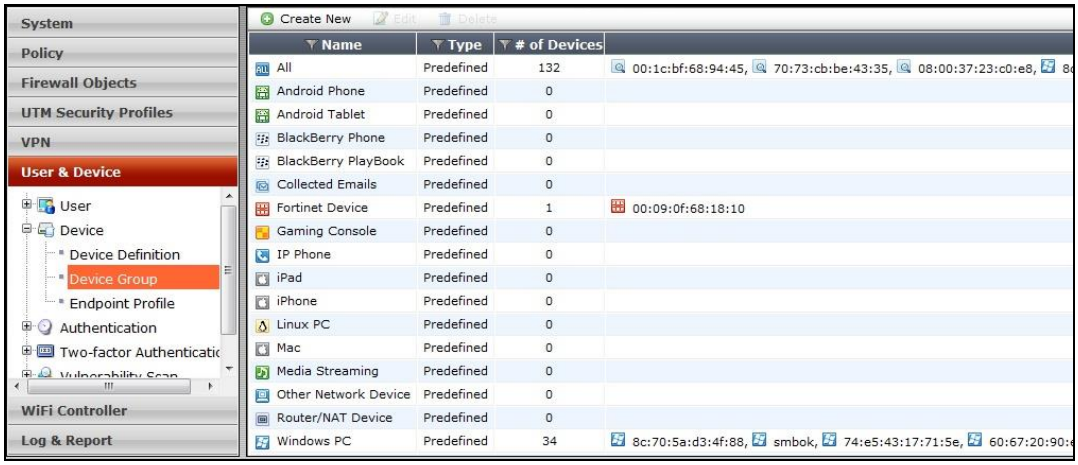
한 명의 사용자가 태블릿 또는 핸드폰등 여러 개의 device를 이용 할 경우 Alias를 입력하여 대표 Device 이름으로 묶을 수 있습니다.



Alias를 입력 한 경우 Device 명 앞에  이 표시 됩니다.

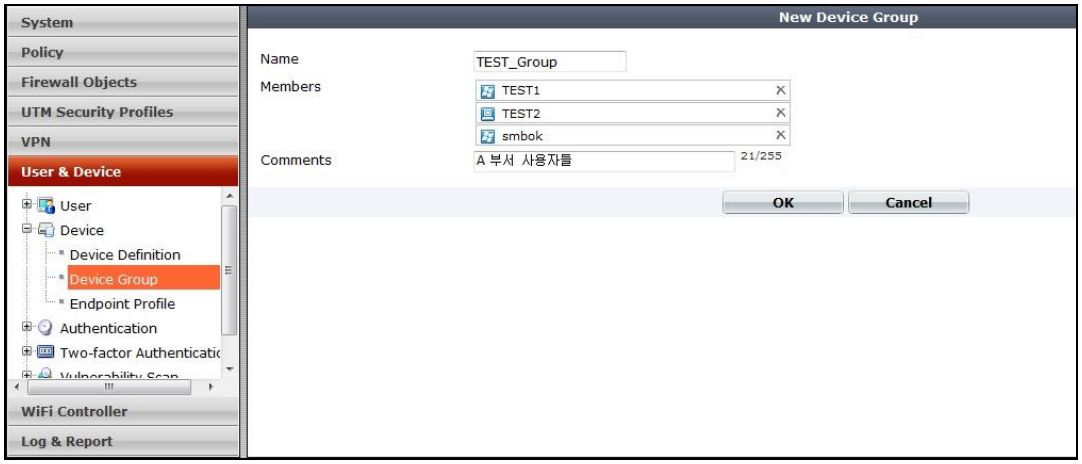


Device Group 에서는 Default 로 19개 의 제품이 등록 되어 있습니다.

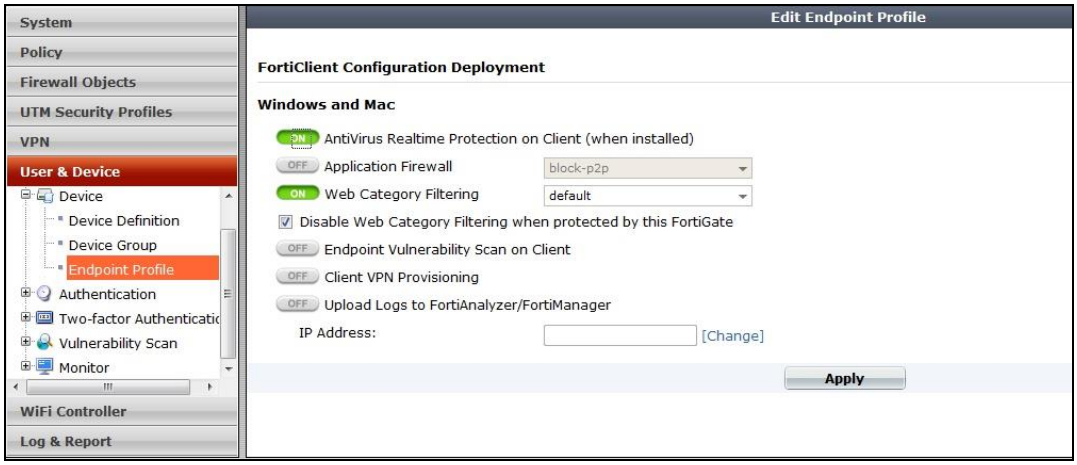


Fortigate는 Network Scan 시 동일 Device 끼리 그룹화 시키기 때문에 다른 Device를 그룹으로 생성 하기 위해서는 그룹을 신규로 생성해야 합니다.

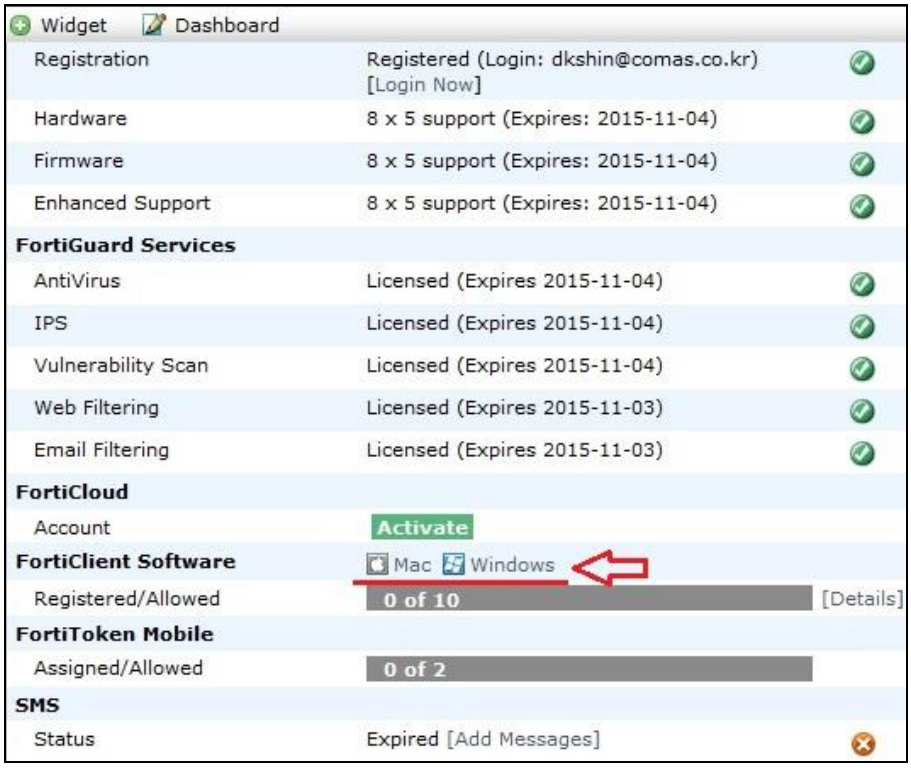
이때, 신규 그룹에 포함 시키려면 먼저 Device에 대한 Alias가 설정 되어야 합니다.



Endpoint Profile 은 사용자가 Fortigate 를 통해 FortiClient를 Download 시 사용 할 수 있는 기능에 대해 정의 합니다.



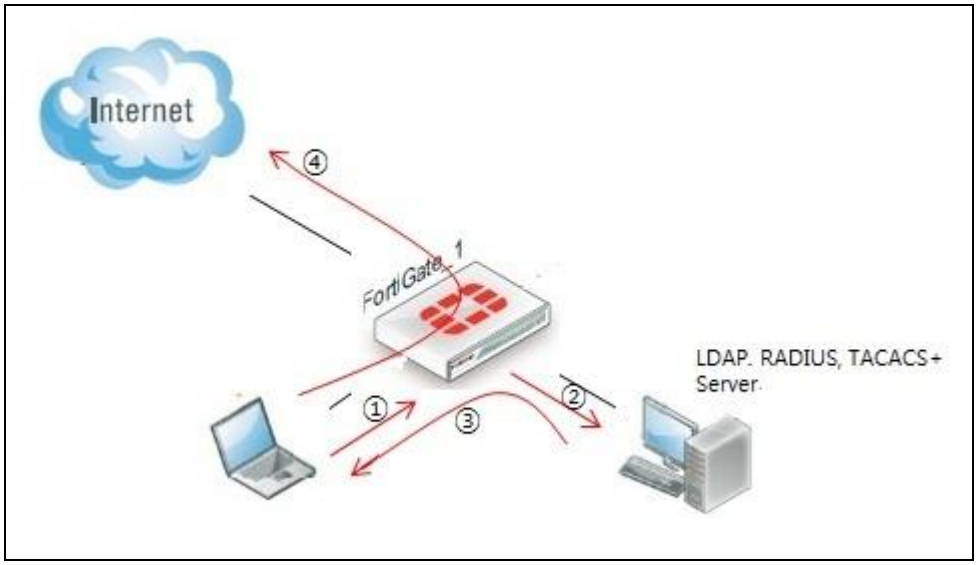
Dashboard 의 License Information Widget 에서 아래 그림과 같이 Mac 이나 Windows OS 대해 FortiClient Software Down 가능합니다.



기본적으로 Client 10 EA, FortiToken Mobile 2 EA 에 대해 지원 합니다.

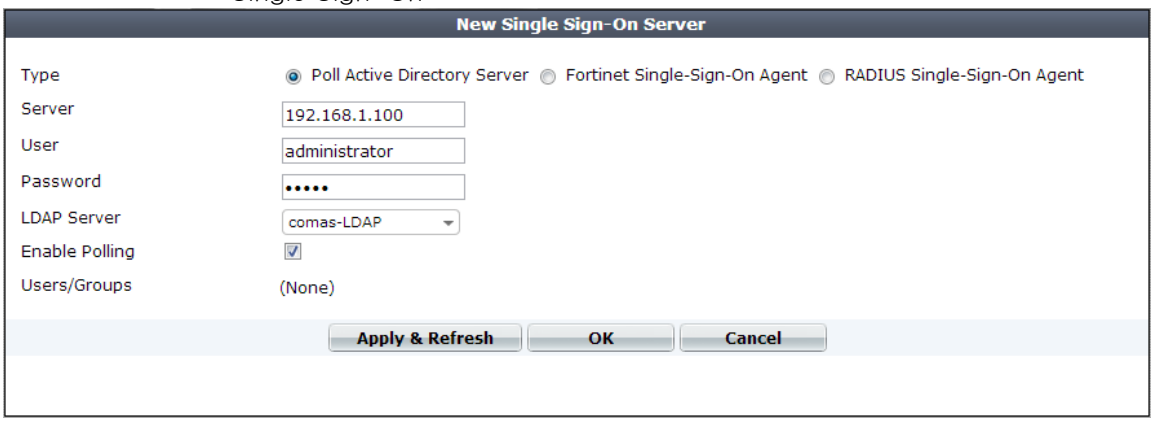
3. 인증(Authentication)

방화벽으로 인증요청이 들어왔을 때 원격 인증 설정이 되어 있으면 자체 Local 인증이 아닌 해당 식별자에 대해 인증서버로 질의를 할 수 있습니다.

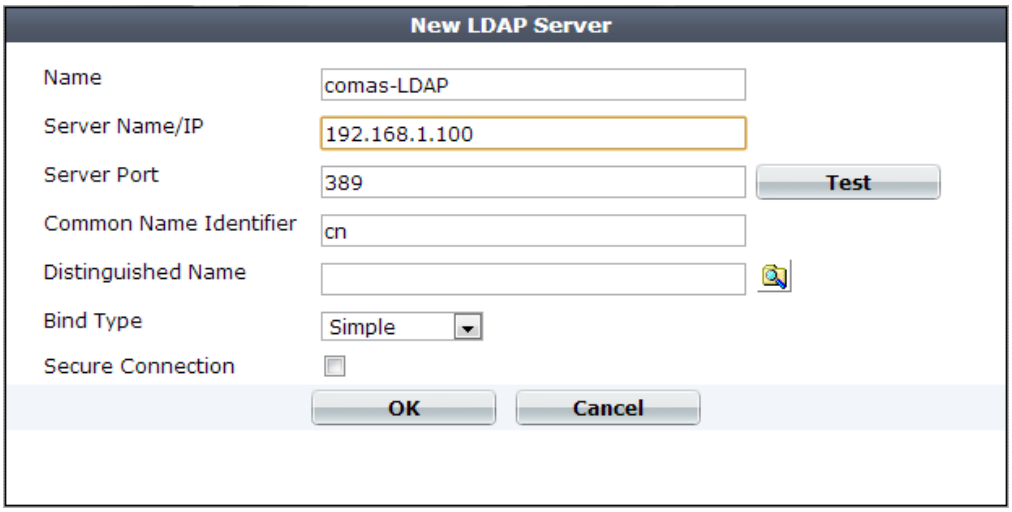


- 원격 인증 개념도 -

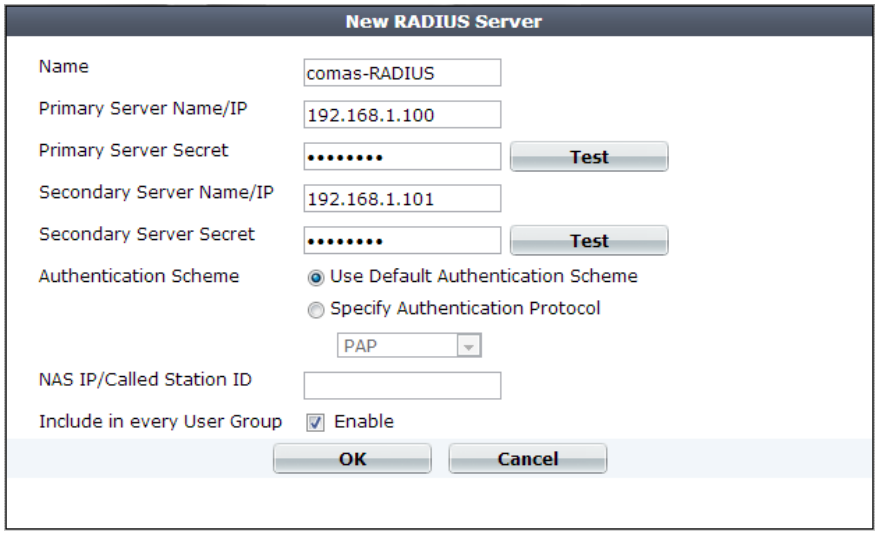
■ Single Sign-On



■ LDAP Server



■ RADIUS Server

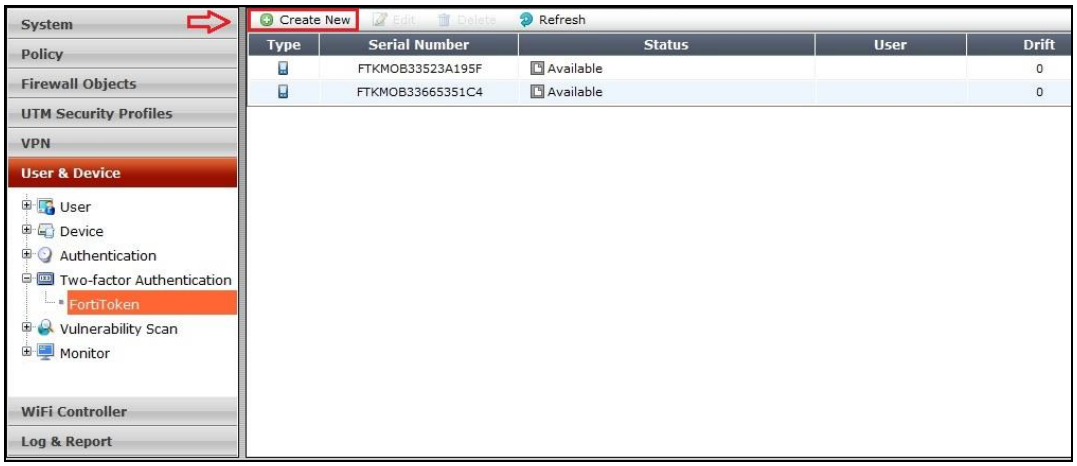


원격 인증을 연동할 서버의 설정을 확인하여 위의 그림과 같은 정보를 입력하면 됩니다.
(자세한 설정 및 동작은 docs.fortinet.com을 참조하세요)

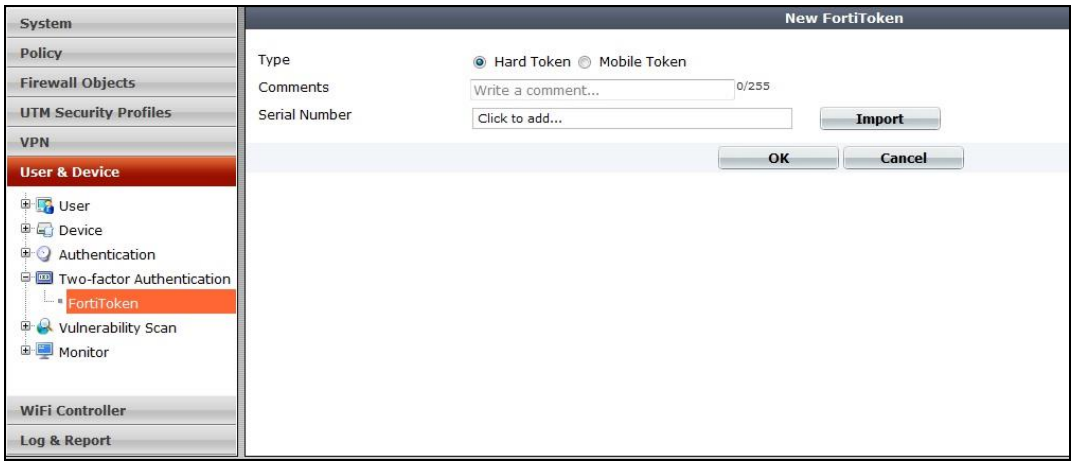
4. Two-factor 인증(Authentication)

Two-factor Authentication 인증은 Local 인증이나 원격인증을 통해 바로 서비스 연결을 허용하는 것이 아닌 FortiToken 이라는 OTP 발생기를 이용하여 한 단계 더 인증 하는 것 입니다.

1. *User & Device > Two-factor authentication* 로 이동 후 *Create New* 선택.

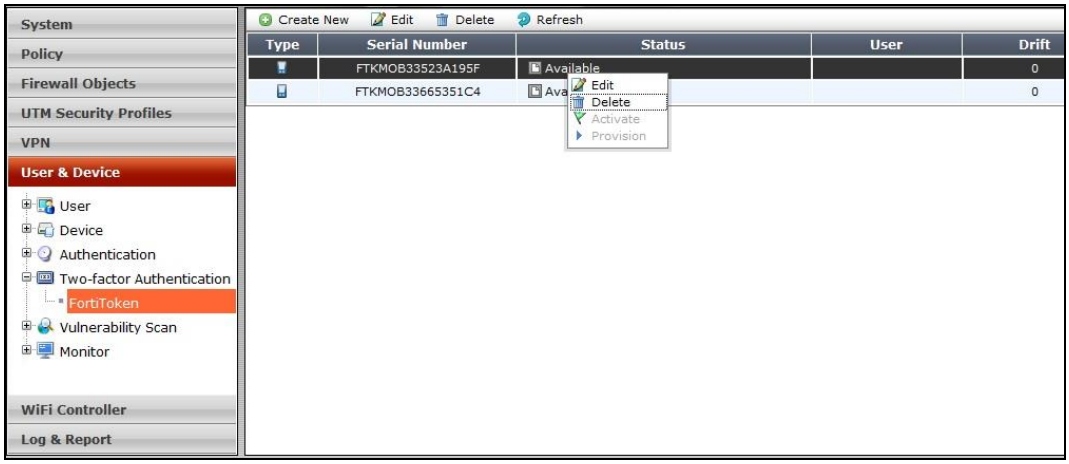


2. Type 선택 Serial Number 입력.



3. OK 선택.

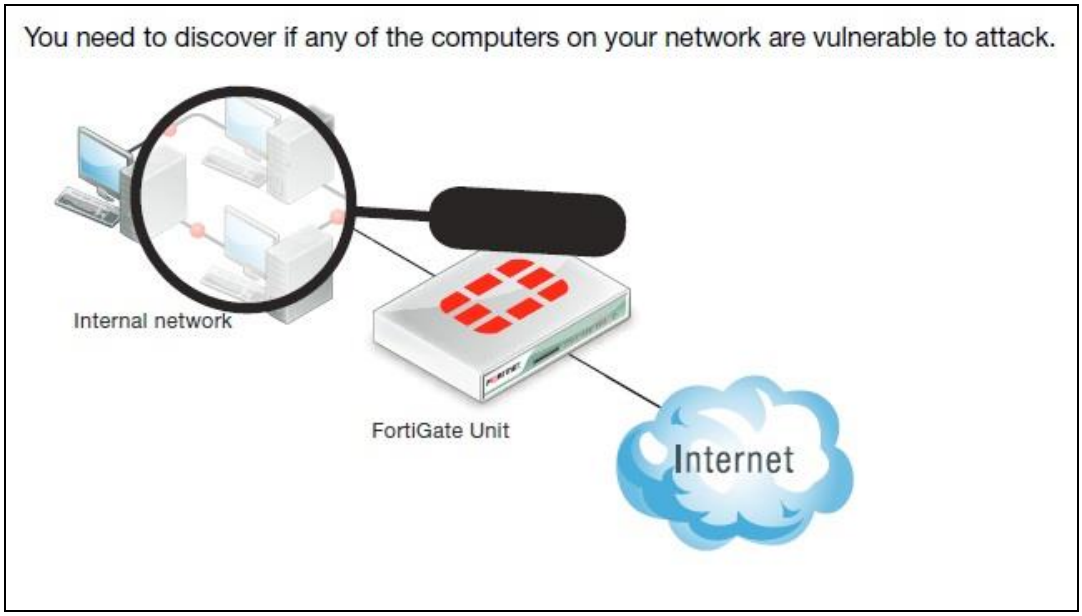
4. 해당 Token 우클릭 후 Activate 해야지만 실질적인 사용이 가능합니다.



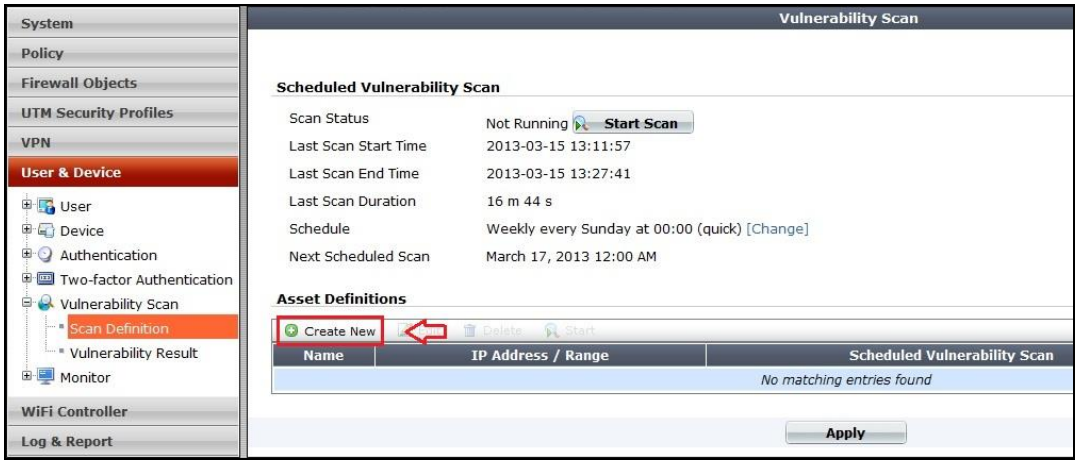
FortiGaurd 센터와 연동이 되어 있어야 FortiToken 활성이 됩니다.

5. 취약점 스캔(Vulnerability Scan)

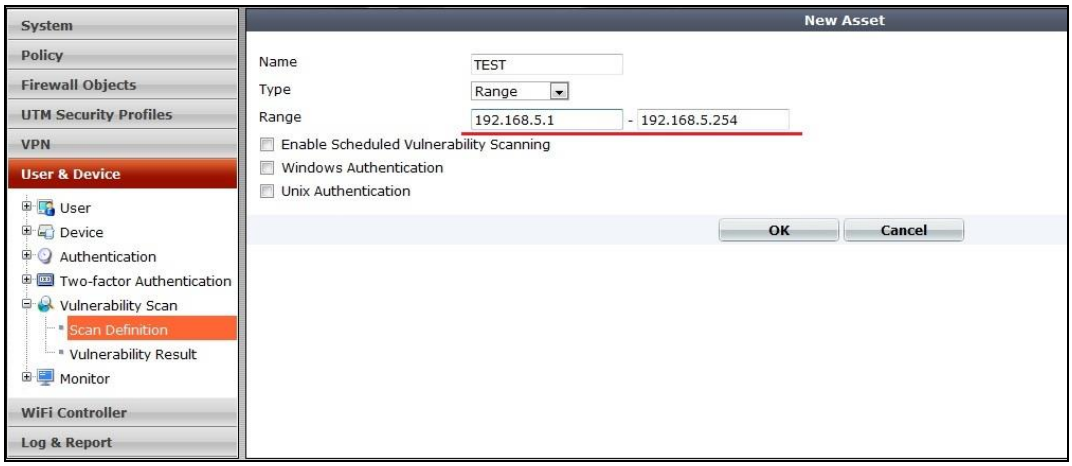
관리자는 Fortigate를 통해 내부 네트워크의 취약한 host 에 대해 검색 할 수 있습니다.



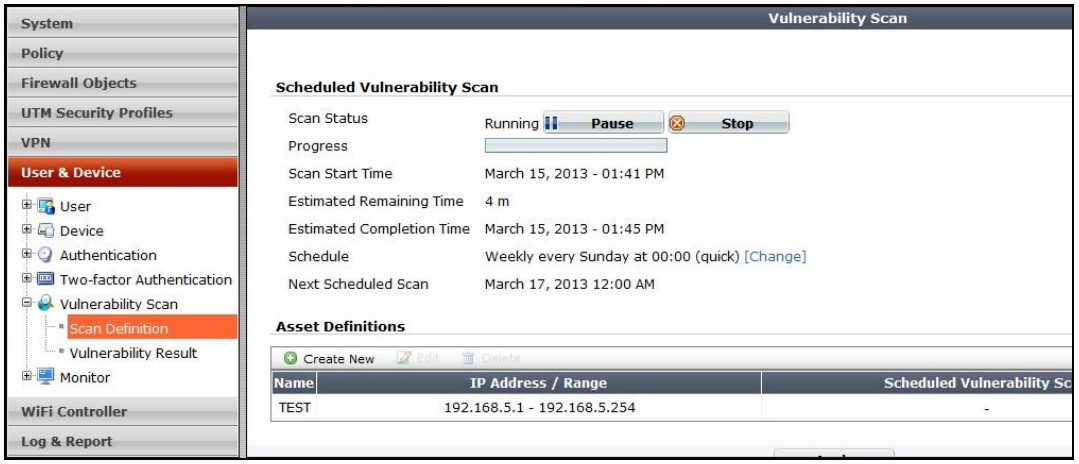
1. *User & Device > Vulnerability Scan* 로 이동 후 *Create New* 선택.



2. Name을 입력하고 Type으로 단일 IP 또는 범위를 지정 할 수 있습니다.



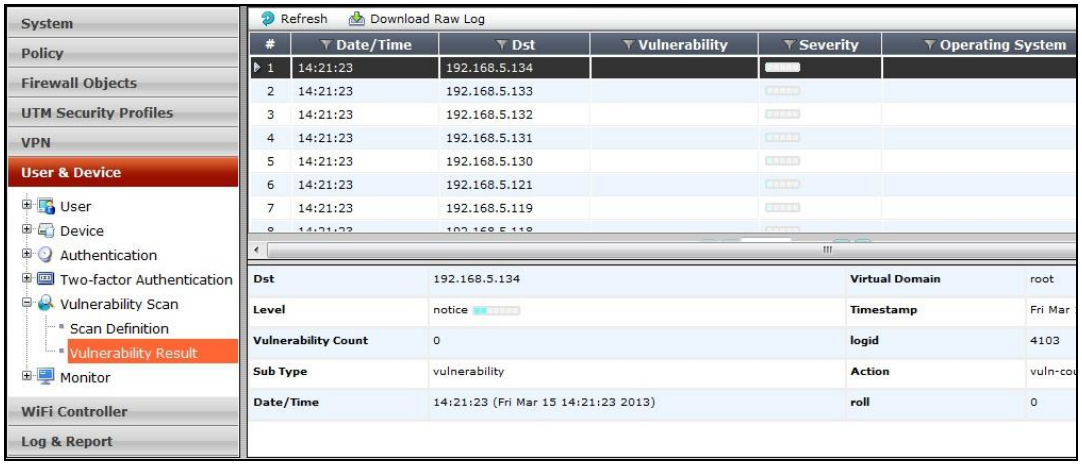
3. Start Scan 을 통해 Scan을 시작합니다.
Schedule 기능으로 주기적인 취약점 분석이 가능합니다.



4. Vulnerability Scan Mode 는 아래 그림과 같습니다.

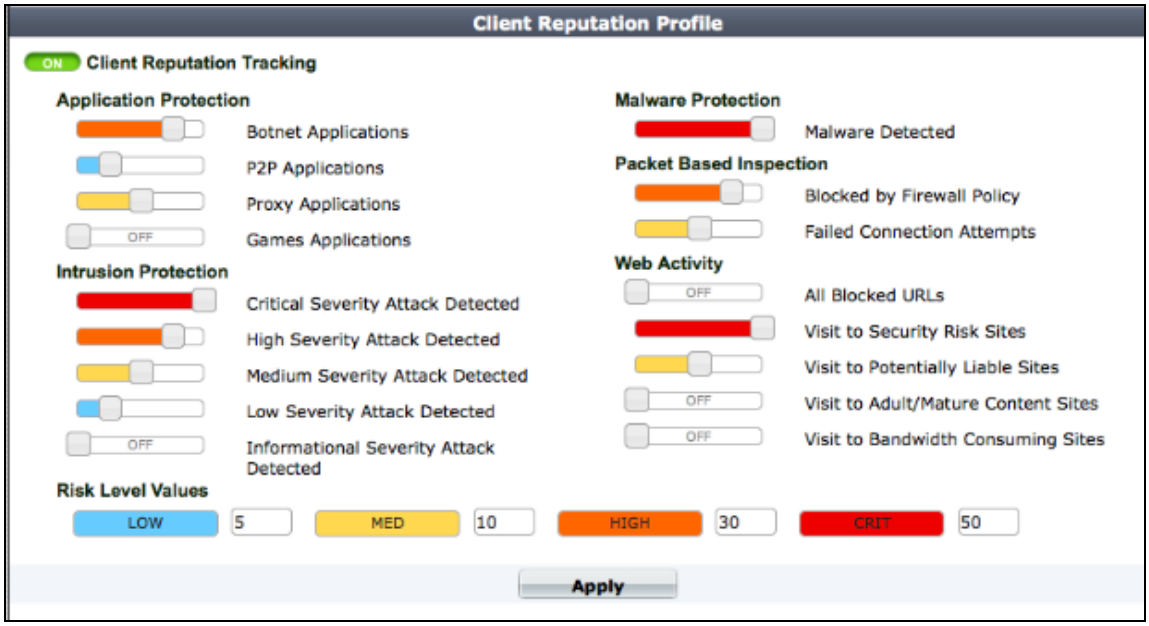
Vulnerability Scan Mode	**Quick** — check only the most commonly used ports **Standard** — check the ports used by most known applications **Full** — check all TCP and UDP ports

4. Scan이 완료 되면 *User & Device* > *Vulnerability Result* Tap 에서 결과를 확인 할 수 있습니다.



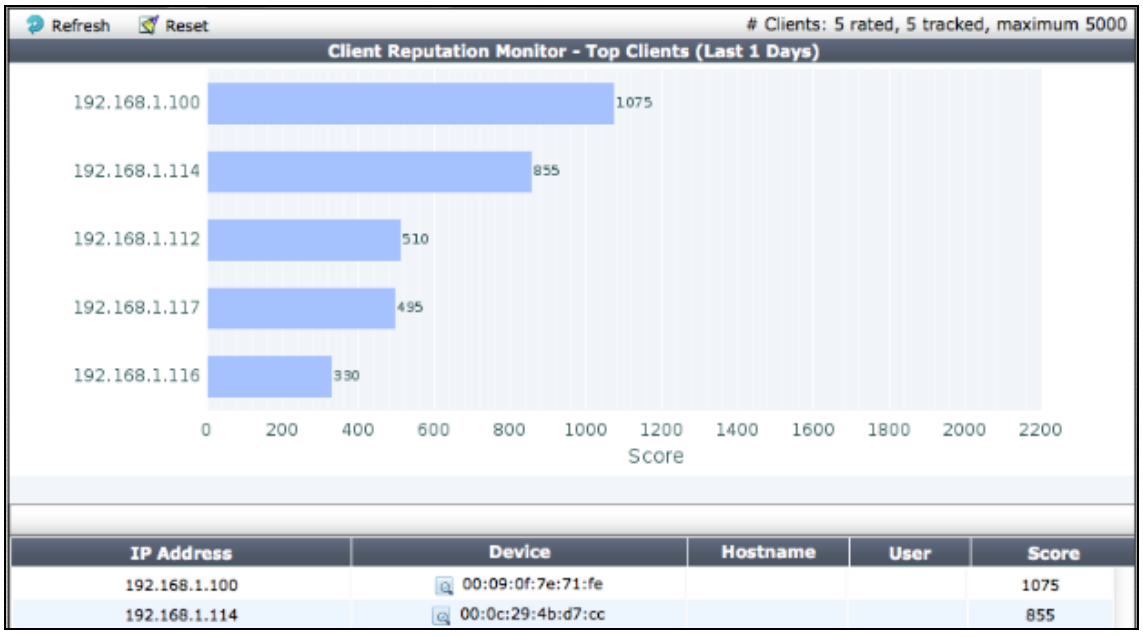
6. 클라이언트 평판(Client Reputation)

Fortigate시스템의 UTM기능은 다양한 보안적 위협을 감지합니다. 종종 공격이나 감염에 노출된 하나의 사용자가 내부 전체를 감염시키기도 합니다. 이러한 사용자는 네트워크에서 분리를 시켜 보안적 위협을 제거 해야 합니다. Fortigate의 Client Reputation기능은 보안적 위협 성향을 가진 사용자를 예측하여 찾을 수 있도록 도와 줍니다.



- Client Reputation 프로파일 설정 화면 -

Client Reputation 프로파일에서 여러 위협 요소에 대해서 점수를 설정 합니다. 이 프로파일을 참고로 사용자들의 행동을 감시하고 사용자에 대해 평가 점수를 측정하게 됩니다.



- Client Reputation 결과 화면 -

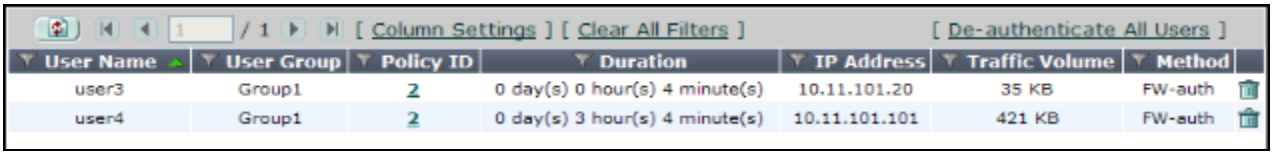
Client Reputation 기능이 설정 되면 Client Reputation 결과 화면을 확인 할 수 있습니다.

7. 모니터(Monitor)

사용자 & 장치 객체에 대한 사용자 인증 정보를 모니터링 합니다.

▪ 방화벽(Firewall)

방화벽 사용자 인증 정보를 보여줍니다.



– 방화벽 사용자 인증 정보 화면 –

깔때기 아이콘을 눌러 항목 별로 원하는 정보를 필터링 할 수 있습니다.

▪ 차단 사용자(Banned User)

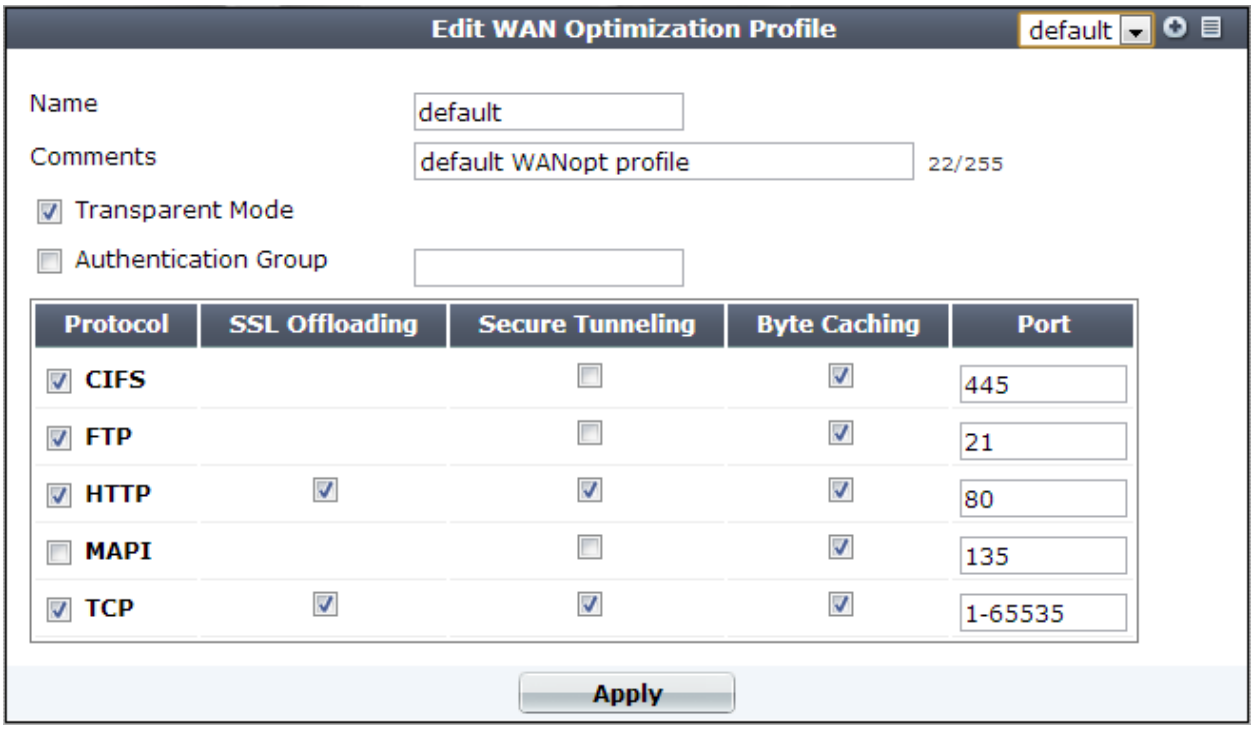
NAC기능에 의해 차단 된 IP주소와 인터페이스 정보 등을 보여줍니다.

8. Wan 최적화 & 캐시(WAN Opt & Cache)

Fortiate 시스템은 Wan 최적화 와 캐싱 기능을 지원 합니다. 이 기능으로 내부 네트워크와 인터넷 사이의 트래픽 전달 성능과 보안을 향상 시킬 수 있습니다

1. WAN Opt. Profile

Wan 최적화에 적용할 프로파일을 설정 합니다.



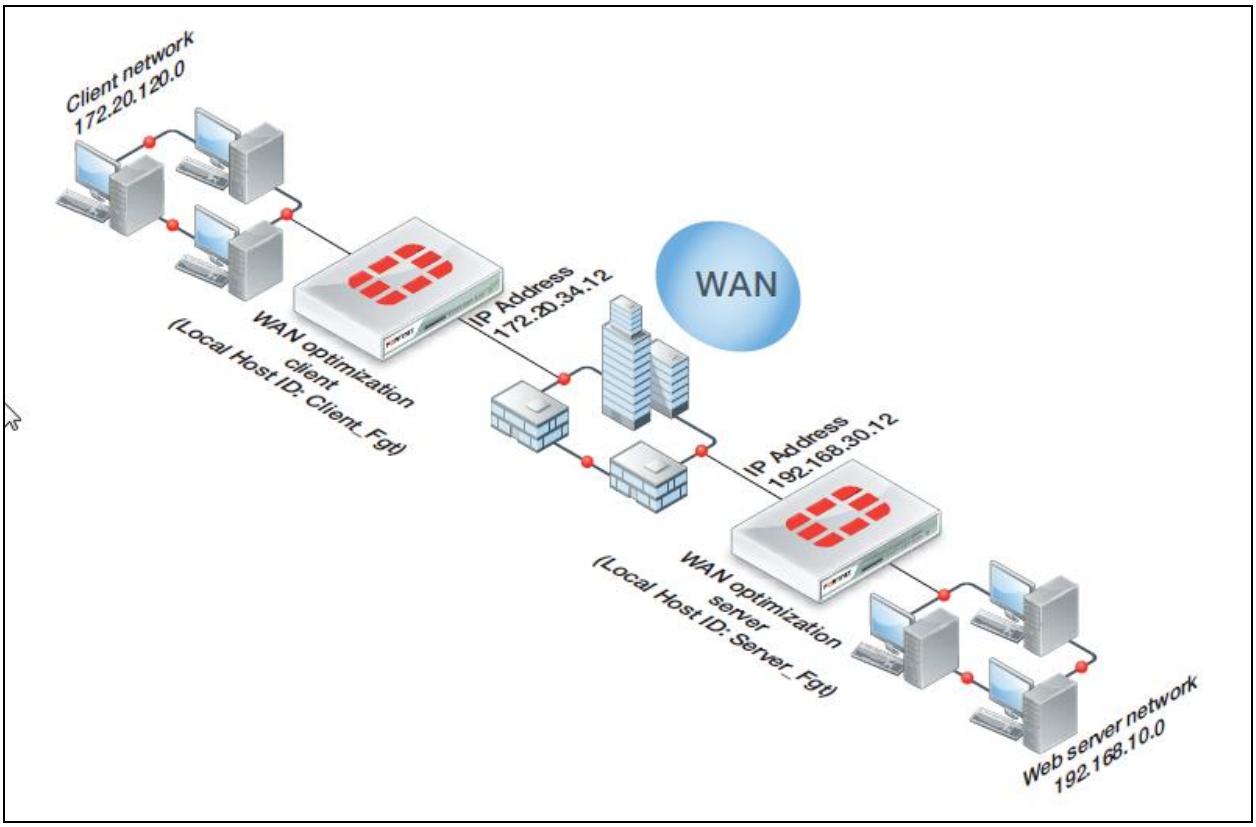
– WAN Optimization Profile 설정 화면 –

Transparent Mode	사용자와 서버간 통신에서 원본 주소를 유지하게 끔 합니다.
Authentication Group	Wan 최적화 터널을 시작하기 전에 서로 인증을 수행 합니다.
Protocol	최적화 시킬 프로토콜을 선택합니다. CIFS, FTP, HTTP, MAPI프로토콜을 선택하지 않고 하나 이상의 프로토콜을 선택하려면 TCP를 체크 합니다.
SSL Offloading	보안 프로토콜에 대한 가속 설정을 합니다.
Secure Tunneling	해당 프로토콜에 대해 SSL 암호화를 이용하여 암호화합니다.
Byte Caching	커다란 application 데이터를 chunk로 쪼개고, 해시와 저장된 chunk를 이용하여 각 chunk에 라벨링을 합니다. 그 후 실제 데이터를 보내지 않고 chunk별 해시를 보내어 이를 Byte Cache 데이터베이스와 비교한 후 해시가 일치하면 터널을 통해

	데이터를 전송하지 않습니다.
Port	해당 프로토콜의 포트 또는 포트 범위를 지정합니다.

2. WAN Opt. Peer

Peer-to-Peer 구성에서 트래픽 전달 성능을 향상 시킵니다.



- Peer to Peer 구성 예제 -

위 구성처럼 Client 네트워크에서 Web서버 네트워크로의 트래픽 전달 성능을 향상 시키고자 한다면 다음과 같이 설정을 합니다.

- 사용자 단 Fortigate설정

1. WAN Opt. & Cache > WAN Opt. Peer > Peer 로 이동하여 Local Host ID를 Client로 입력한다.
2. Apply를 누른다.
3. Create New를 누르고 Peer Host ID를 Server로 입력하고 IP Address를 192.168.30.12로 설정한다.
4. OK를 누른다.
5. Firewall Objects > Address > Address에서 Create New로 사용자 네트워크와 서버 네트워크 객체를 생성한다.
6. WAN Opt. & Cache > WAN Opt. Profile > Profile에서 Transparent 모드를 선택하고 Apply를

누른다.

7. Policy > Policy > Policy 에서 내부->외부(all -> all) 정책을 만들고 WAN Optimization을 active로 설정 하고 프로파일을 default로 설정한다.

8. CLI에서 해당 정책의 wanopt-detection을 off설정한다.

```
config firewall policy
  edit 5
    set wanopt-detection off
    set wanopt-peer Server(피어 호스트 ID)
    set wanopt-profile default
  end
end
```

- 서버 단 Fortigate설정

1. WAN Opt. & Cache > WAN Opt. Peer > Peer 로 이동하여 Local Host ID를 Client로 입력한다.

2. Apply를 누른다.

3. Create New를 누르고 Peer Host ID를 Server로 입력하고 IP Address를 192.168.30.12로 설정한다.

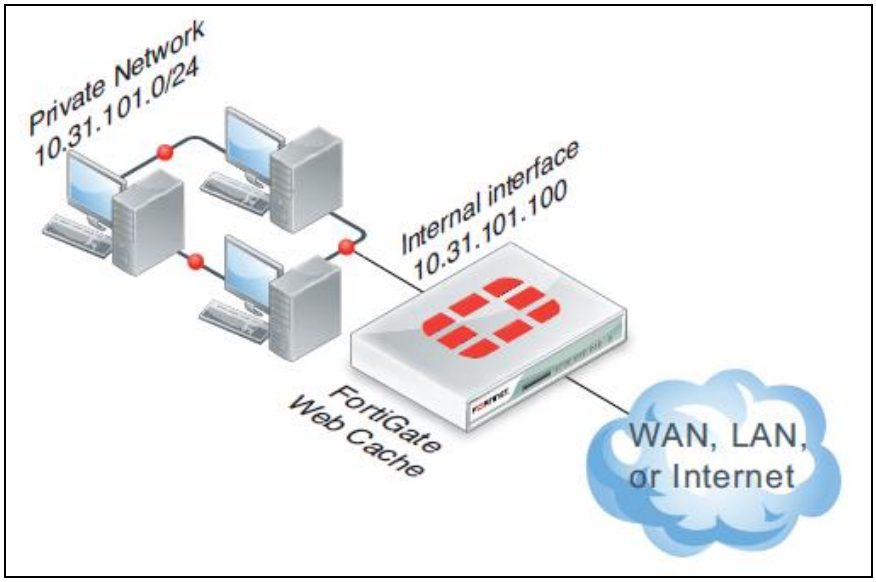
4. OK를 누른다.

5. Policy > Policy > Policy 에서 wanopt ->내부(all -> all) 정책을 만든다.

3. 캐시(Cache)

Web Caching

웹 캐싱은 트래픽 전달능력을 높이기 위해 HTML페이지, 이미지, 서블릿 응답 및 웹 기반 객체를 저장하며, *System > Config > Advanced > Disk Management* 에서 저장용량을 확인 할 수 있다.



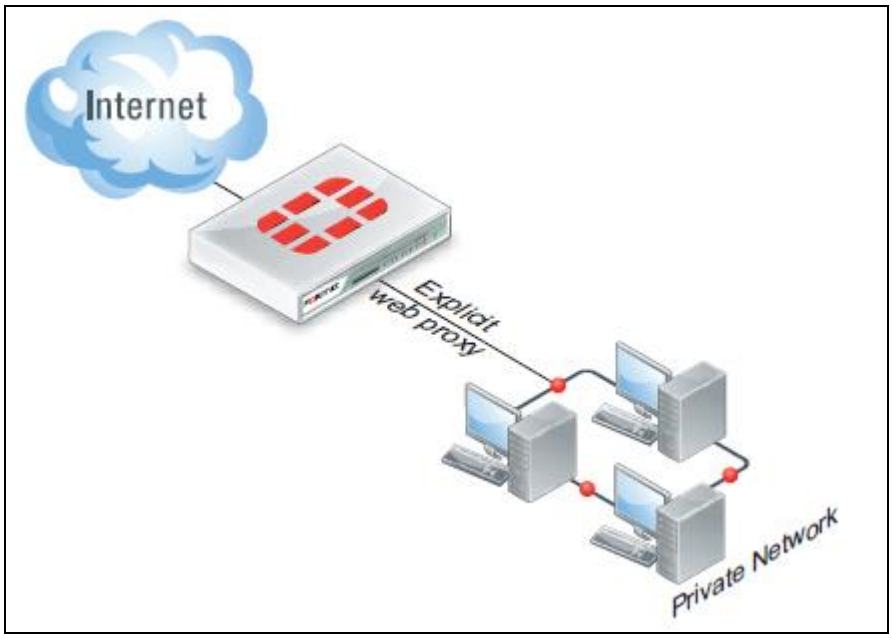
- 기본 적인 웹 캐싱 구성도 -

▪ 웹캐싱 정책 설정

1. *Policy* > *Policy* > *Policy* 에서 내부사용자가 외부 인터넷으로 접속하는 정책을 생성합니다.
2. NAT를 설정하고 *Use Destination Interface Address*를 선택합니다.
3. Enable Web cache를 선택합니다.
4. OK를 선택합니다.

4. Explicit Web Proxy

전통적인 Proxy 서버의 구성형태로 사용자의 브라우저에 PAC파일을 이용하거나 Proxy서버를 지정하여 운영 될 수 있습니다.



– Explicit 웹 프록시 구성 –

▪ Explicit Web Proxy 설정

1. *System* > *Network* > *Explicit Proxy* 에서 Enable Explicit Web Proxy(HTTP, HTTPS)를 선택합니다.
2. Apply를 누릅니다.
3. *System* > *Network* > *Interface* 에서 explicit web proxy를 설정할 인터페이스를 선택한 후 Edit를 누른다
4. Enable Explicit Web Proxy를 선택한다.
5. *Firewall Objects* > *Address* > *Address* 에서 explicit proxy를 적용할 출발지 주소를 생성한다.(인터페이스는 Any로 설정해야 함)
6. *Policy* > *Policy* > *Policy* 에서 출발지 인터페이스가 web-proxy이고 목적지 인터페이스가 외부인터페이스인 정책을 생성한다

9. 무선 콘트롤러(WiFi Controller)

Fortigate시스템은 FortiAP와 연동을 하여 무선 콘트롤러의 기능을 수행하며, Fortigate의 다양한 UTM기능을 무선네트워크에 적용을 할 수 있습니다. 또한 WIDS기능과 로밍 기능을 통하여 안전하고 안정적인 무선 네트워크를 구축 할 수 있습니다.

- 지역설정

  국가별로 Wi-Fi 네트워크에 대한 최대 송신기 출력과 허용 Radio 채널이 다릅니다. 기본 설정은 US이고, 만약 US와 차이가 나는 국가에 FortiAP를 설치 할 경우 지역설정을 변경하여야 합니다. 설정변경은 CLI에서만 가능합니다.

  예) Korea

  ```
  config wireless-controller setting
      set country KR
  end
  ```

  국가 코드는 set countory 이후 "?"를 입력하면 확인 가능합니다.

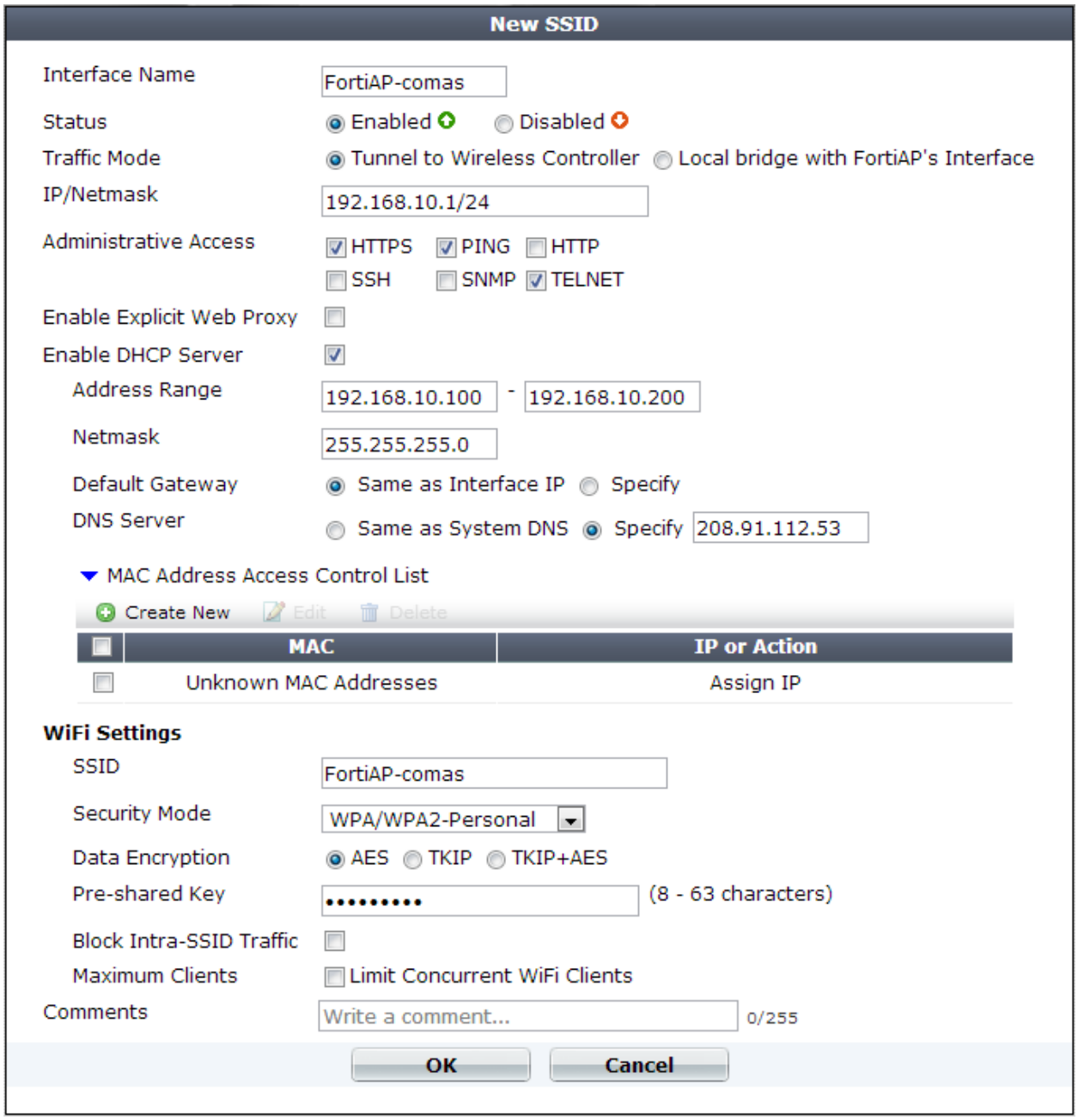
  지역설정 변경 전에 반드시 모든 사용자AP 프로 파일(Custom AP Profile)을 삭제 하여야 합니다. AP프로파일이 있는 경우 지역설정 변경이 안됩니다.

1. 무선 네트워크 (WiFi Network)

무선 사용자가 접근 할 SSID를 설정하고, 불법AP(Rouge AP)와 WIDS에 관한 설정을 합니다.

1-1. SSID(Service Set Identifierd)

SSID란, 무선사용자가 접속하고자 하는 무선네트워크의 고유 식별자로 SSID 이름, 네트워크 설정 및 보안 관련 설정을 할 수 있습니다.



*WiFi Controller > WiFi Network > SSID > Creat e New*를 눌러 SSID를 생성합니다.

Interface Name　　무선네트워크의 이름을 설정합니다. Fortigate시스템에서는 SSID를 생성하면 새로운 인터페이스가 생성이 되고 이 인터페이스를 이용하여 정책을 설정합니다.

Status　　해당 SSID의 사용여부를 정합니다.

Traffic Mode　　별도의 무선네트워크를 구성할 지 Bridge형태로 구성할 지를 설정합니다

- Tunnel to Wireless Controller　　생성한 무선네트워크가 새로운 네트워크

세그먼트를 만듭니다. NAT/Route 형태로 이해할 수 있습니다.

- Local bridge with FortiAP's Interface 무선네트워크가 Bridge(TP)형태로 구성됩니다. Tunnerl 모드에서 생성된 무선네트워크는 기존에 Fortigate에 없던 새로운 세그먼트가 생성이 됩니다. 이 경우 무선 사용자가 기존 유선네트워크와 다른 IP대역을 가지게 됩니다. Bridge모드의 경우 기존 유선네트워크와 Transparent한 구성이 되어 동일한 IP대역을 가질 수 있기 때문에 네트워크의 구성변경 없이 무선네트워크를 구성 할 수 있습니다.

IP/Netmask 생성할 무선네트워크에 IP와 서브넷을 설정합니다. (Tunnel모드만 해당)

WiFi Settings SSID이름 및 보안 설정을 합니다.

- SSID 무선사용자가 접속할 SSID 이름을 설정합니다.
- Security Mode 무선접속시의 보안설정을 합니다. WEP, WPA, Captive-Potal, Open모드를 지원합니다. (WEP는 CLI에서 설정합니다.)
- Data Encryption 데이터 암호화 방식을 설정합니다.
- Pre-shared Key 무선네트워크 접속 시 입력할 암호(공유키)를 설정합니다.
- Block Intra-SSID Traffic
- Maximum Clients 최대 접속 사용자 수를 설정합니다.

1-2. 불법AP 설정(Rouge AP Settings)

Fortigate시스템은 불법AP에 대하여 탐지가 가능합니다.

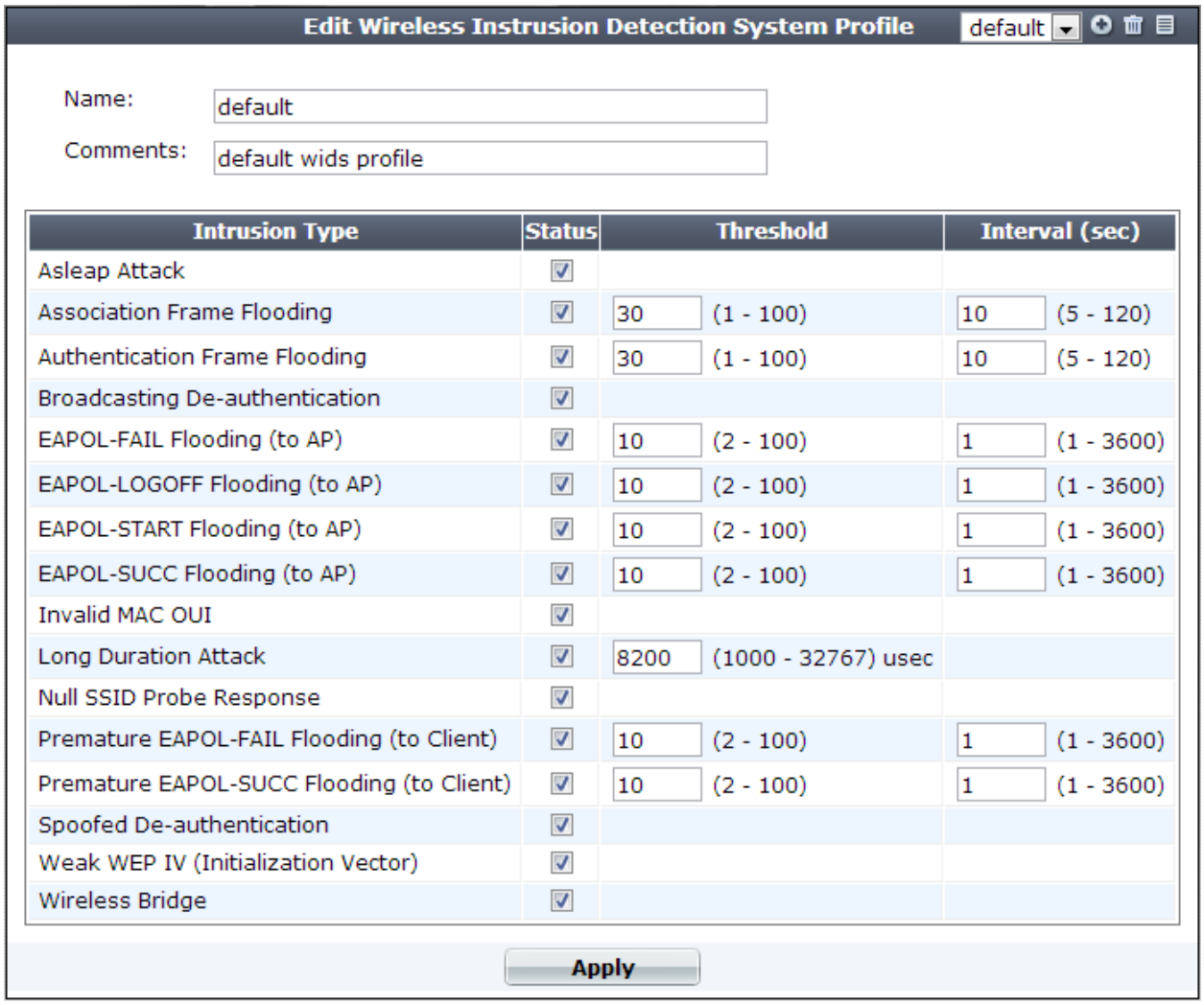
- Enable Rogue AP Detection 불범AP 탐지 기능을 활성화 합니다.
- Enable On-Wire Rogue AP Detection Technique 유선네트워크에 연결 되어 있는 불법AP를 탐지 합니다.

유선네트워크 상의 불법AP 탐지 기술

동일한 MAC주소가 유선네트워크와 무선네트워크에서 보인다면, 이것은 무선사용자가 유선네트워크에 연결이 되어있다는 것을 의미하고, Non-NAT 불법AP가 유선네트워크에 연결되어 있는 것을 의미합니다. 불법AP가 NAT 역할을 할 경우 불법AP에 대한 탐지가 더 어렵습니다. 하지만, AP의 WiFi 인터페이스의 MAC주소와 유선 인터페이스의 MAC주소가 일반적으로 같은 범위를 갖습니다. MAC주소의 일정범위가 동일하다면 불법AP의 연결을 의심 할 수 있습니다. ₩

1-3. WIDS(Wireless IDS) 프로파일

Fortigate시스템은 무선네트워크 상의 불법, 공격적인 트래픽을 탐지 차단 할 수 있습니다.



- WIDS 프로파일 화면 -

2. 액세스 포인트 관리(Managed Access Points)

Fortigate와 연동 할 FortiAP장비의 설정을 합니다. 물리적인 AP에 SSID, 채널, 신호세기 등을 설정 합니다.

2-1. FortiAP 설정

Fortigate에서 FortiAP를 검색하고 등록하기 위해서는 FortiAP에 아래의 설정을 합니다.

cfg -a AP_IPADDR=xxx.xxx.xxx.xx	AP의 IP를 설정합니다.
cfg -a AP_NETMASK=255.255.255.0	AP의 서브넷을 설정합니다.
cfg -a IPGW=yyy.yyy.yyy.yyy	AP의 게이트웨이를 설정합니다.
cfg -a AC_IPADDR_1=zzz.zzz.zzz.zzz	WiFi-Contorllor의 IP를 설정합니다.
cfg -a ADDR_MODE:=STATIC	AP의 IP를 정적으로 설정합니다. (유동은 DHCP)

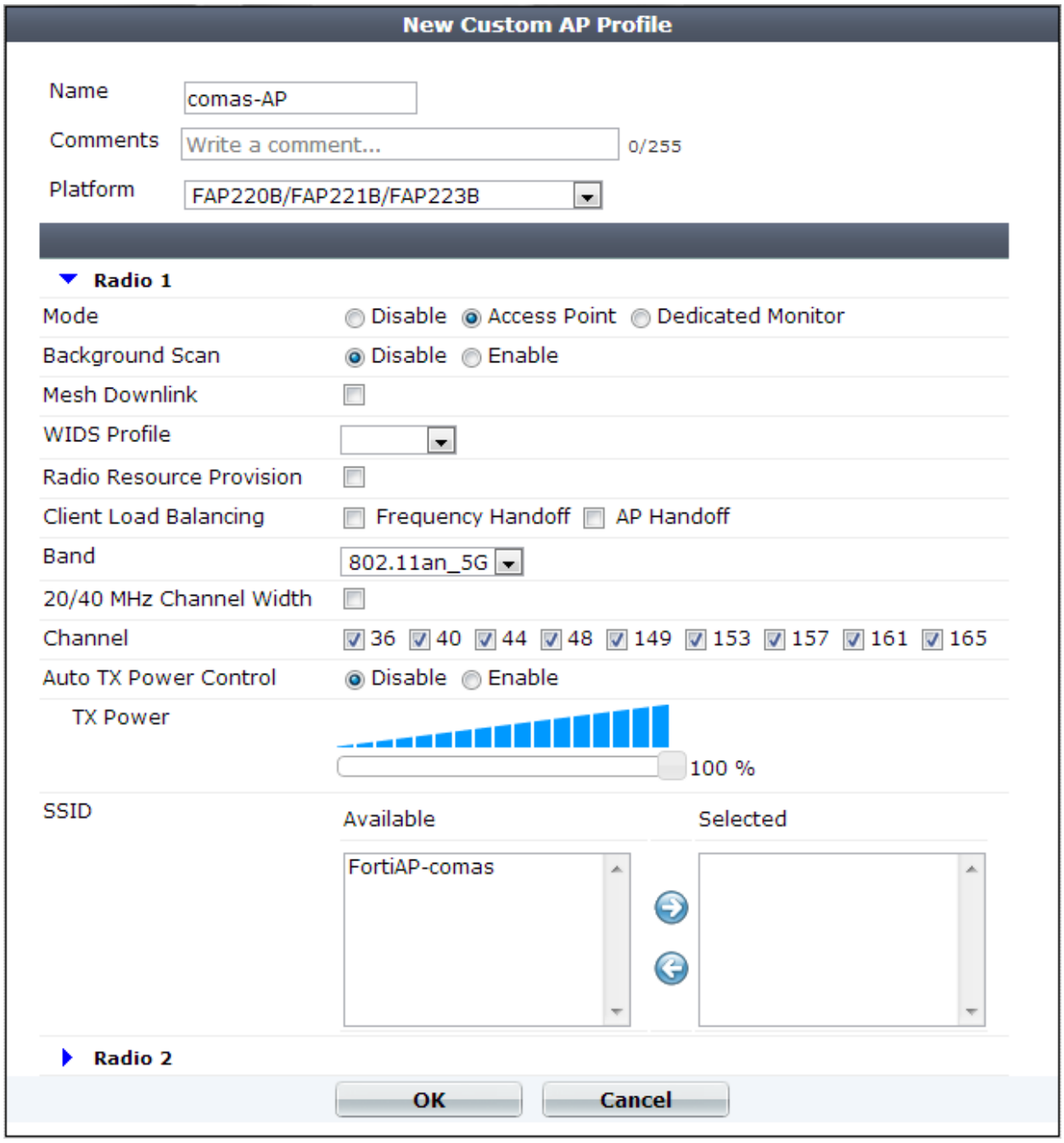
cfg -c 설정을 저장합니다.

cfg -s 설정을 확인합니다.

FortiAP-221B와 같이 Zero Configuration(설정이 필요 없는)만을 지원하는 장비는 Static 설정이 불가능 하기 때문에 Fortigate와 같은 네트워크에 설치가 되어야 합니다.

2-2. 사용자 AP프로파일 (Custom AP Profile)

Radio의 Band, 채널, 송신 출력 등을 설정합니다.



Name AP프로파일의 이름입니다.

Platform 프로파일을 적용 할 수 있는 FortiAP 플랫폼을 설정합니다.

Radio 무선 관련 설정을 합니다.

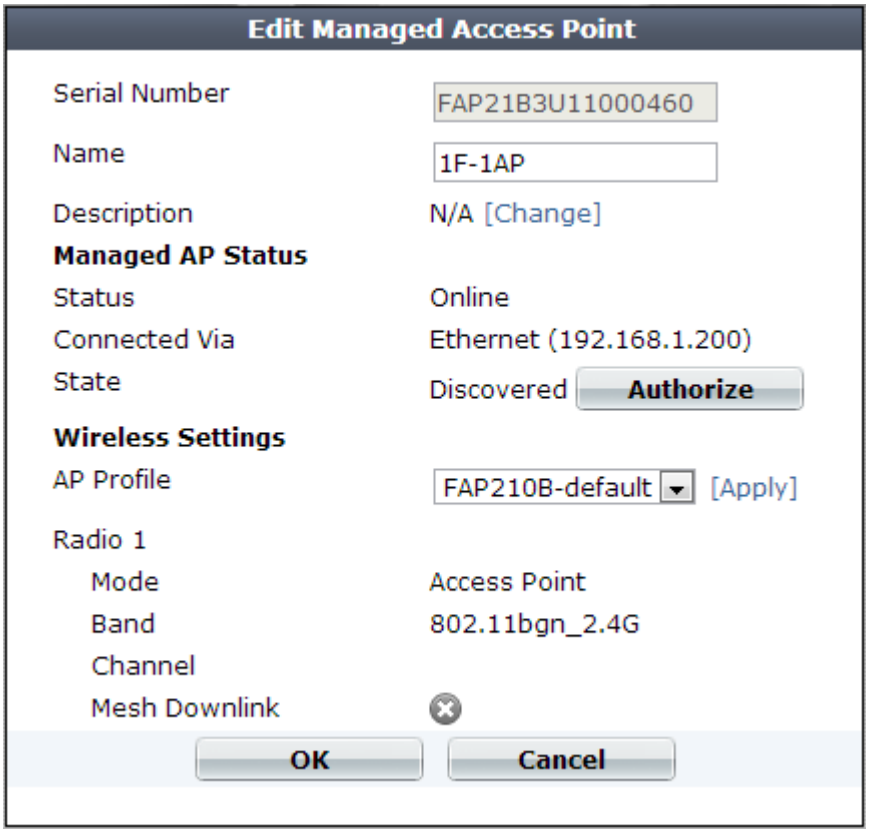
- Mode 해당 Radio를 어떤 형태로 사용할 지를 설정 합니다.
  - Disable 해당 Radio를 사용하지 않습니다.
  - Access Point 해당 Radio를 AP형태로 사용합니다.
  - Dedicated Monitor 해당 Radio를 무선 모니터링 전용으로 사용합니다.
- Background Scan AP역할을 하는 동안 Radio는 동일 무선대역 내의 채널을 모니터링 할 수 있습니다. 기본적으로 탐지 주기는 매 300초마다 시작되고, 모든 채널이 확인 될 때 까지 매초 다른 채널을 20ms 동안 모니터링 합니다. 하지만, Radio가 모니터링으로 전환 될 때 패킷 손실이 발생 할 수 있기 때문에 트래픽이 많은 경우 사용을 안 하는 것이 좋습니다.
- Mesh Downlink 무선을 이용하여 FortiAP가 WiFi Controller에 연결되도록 합니다.
- WIDS Profile Wireless IDS 보안 프로파일을 설정 합니다.
- Radio Resource Provision 큰 무선 네트워크 구조에서 무선 네트워크가 서로 간섭하지 않도록 FortiAP가 채널을 선택할 수 있도록 합니다.
- Client Load Balancing 무선네트워크의 트래픽을 효율적으로 분산 처리 합니다.
  - Frequency Handoff FortiAP는 2.4GHz와 5GHz 대역의 사용량을 모니터링하고 사용량이 적을 주파수 대역으로 사용자를 전환 시킵니다. (듀얼밴드 사용자만 해당)
  - AP Handoff FortiAP에 임계값을 초과하여 과부하가 걸리면(예를 들어 30사용자이상 접속) 신호가 가장 약한 사용자를 다른 AP쪽으로 연결 시킵니다.
- Band 무선 주파수 대역을 설정 합니다.
- 20/40 MHz Channel Width 802.11n-5G대역에서 채널폭을 20/40으로 설정합니다.
- Channel 사용할 무선 채널을 설정합니다.
- Auto TX Power Control 송신 신호의 강도를 설정 합니다.
  - Disable 신호강도를 수동 설정합니다.
  - Enable 신호강도를 자동 설정합니다.
- SSID 해당 AP프로파일을 적용할 SSID를 선택합니다.

2-3. 관리 FortiAP(Managed FortiAP)

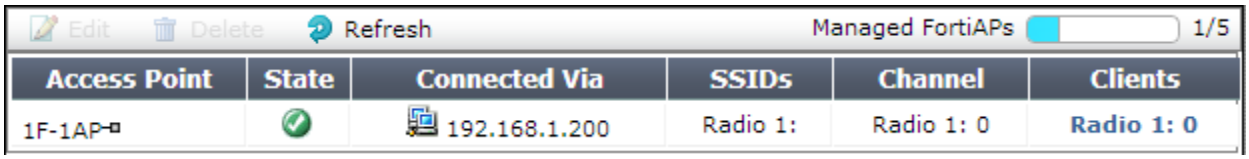
검색된 FortiAP의 리스트를 확인 하고, FortiAP 장비를 수정, 삭제, AP기능을 활성화 합니다.

– 검색된 FortiAP 리스트 –

Fortigate로 접속을 시도하는 FortiAP는 2분 이내에 *WiFi Controller* > *Managed Access Points* > *Managed FortiAP* 페이지에 리스트가 보여야 합니다. 검색된 FortiAP의 설정 화면에서 AP프로파일을 설정하고 Authorize 버튼을 눌러 사용인증을 하면 FortiAP가 활성화 됩니다.



– FortiAP 설정 화면 –



– 활성화 된 FortiAP –

■무선네트워크 설정 요약

1. SSID를 생성합니다.
2. AP프로파일을 생성하고, SSID를 할당 합니다.
3. FortiAP를 설정합니다.
4. 검색리스트에서 FortiAP를 확인하고 해당AP에 AP프로파일을 할당 후 사용인증을

합니다.

3. 모니터(Monitor)

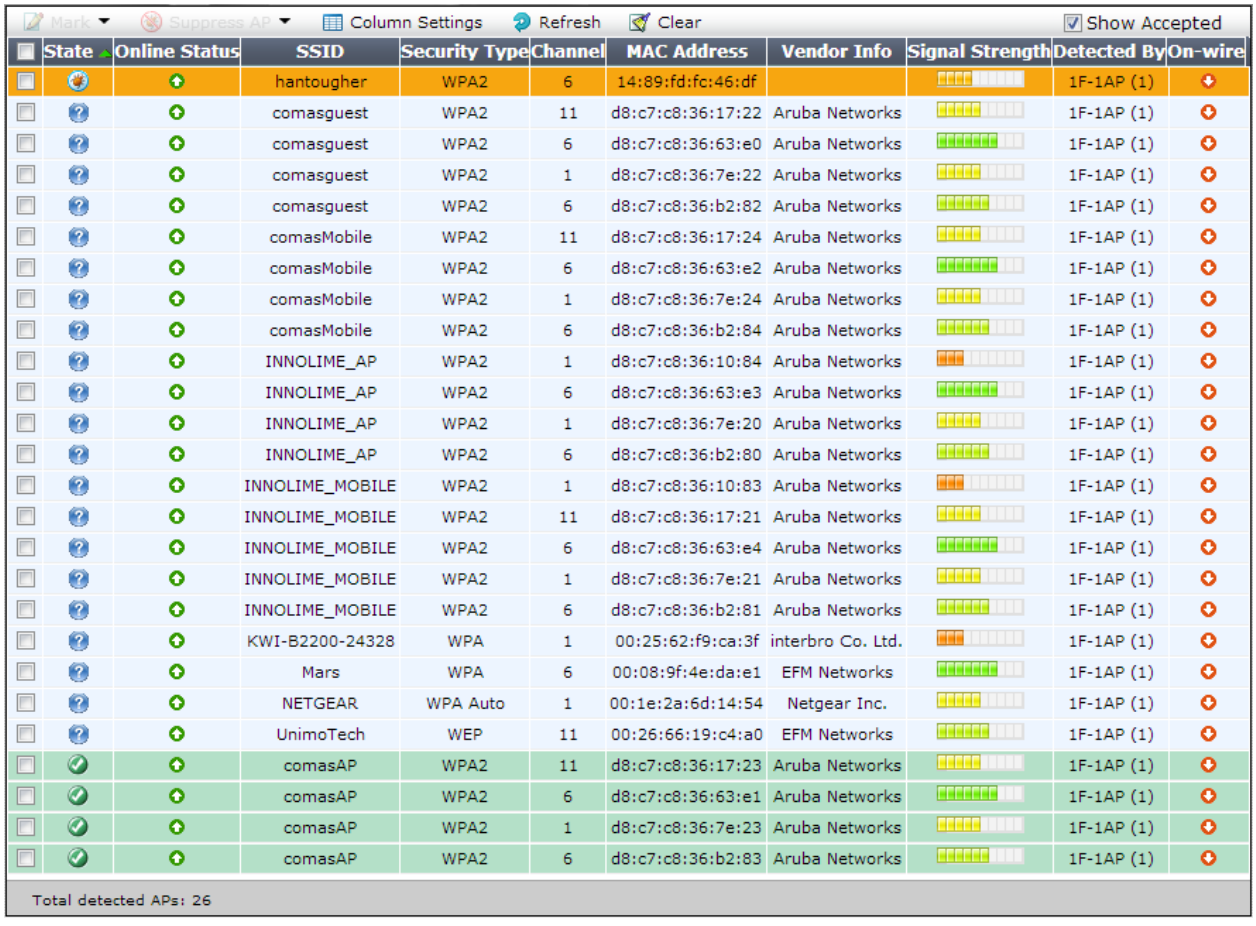
FortiAP 사용자에 대한 모니터링이 가능합니다.

3-1. 사용자 모니터 (Client Monitor)

- 무선 사용자 모니터링 화면 -

사용자 모니터에서는 무선 사용자의 IP, MAC주소, 무선사용대역, 신호세기 등을 확인 할 수 있습니다.

3-2. 불법AP 모니터 (Rogue AP Monitor)



- 불법AP 모니터링 화면 -

불법AP 모니터에서는 FortiAP로 수신 되는 다른 액세스포인트 리스트를 확인 할 수 있습니다.

Mark 메뉴를 이용하여 해당 AP의 상태표시를 변경 할 수 있습니다.

 Rogue AP 네트워크에 인증되지 않은 AP를 나타냅니다.

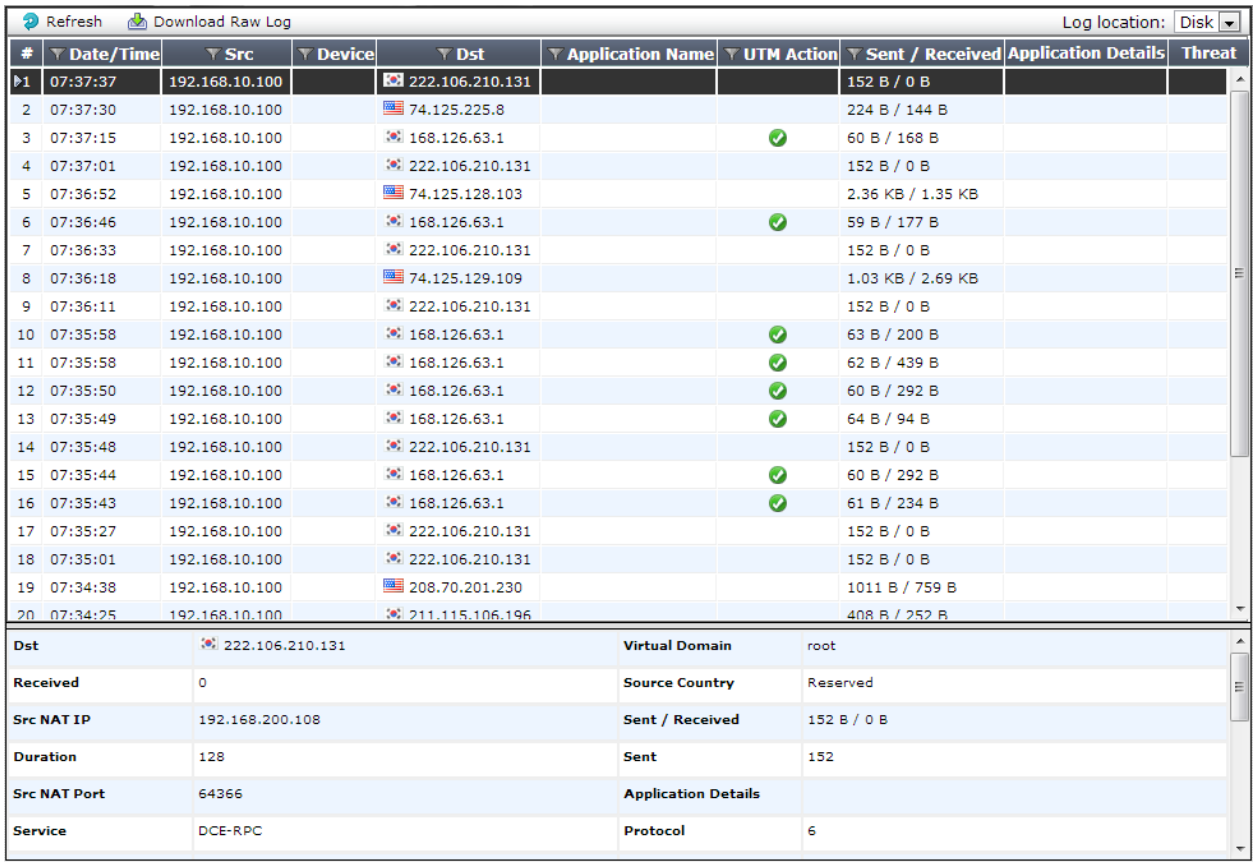
 Accepted AP 네트워크에 인증된 AP나 보안적 위협이 없는 AP를 나타냅니다.

 Unclassified AP AP가 검색된 초기 상태입니다.

- 불법AP 차단 *WiFi Controller > Monitor > Rogue AP Monitor*에서 차단 할 AP를 *Mark Rogue*로 선택하고 *Suppress AP*를 선택합니다.

10. 로그& 보고서(Log & Report)

Fortigate시스템에서 발생하는 각종 로그와 레포트를 확인 할 수 있고, 로그설정 관련 메뉴가 있습니다.



– 트래픽 로그 화면–

로그화면의 위쪽은 로그 리스트를 나타내고 로그를 클릭하면 하단에 해당 로그의 상세 내역을 확인 할 수 있습니다.

1. 트래픽(Traffic) 로그

Forward Traffic 정책에 의해 Fortigate 장비를 통과하는 트래픽 로그를 나타냅니다.

Local Traffic Fortigate 시스템의 트래픽 로그를 나타냅니다. 예를들어 SNMP, Syslog, 관리접속 등을 확인 할 수 있습니다.

Multicast Traffic 멀티캐스트 정책에 의해 Fortigate 장비를 통과하는 멀티캐스트 트래픽 로그를 나타냅니다

Invalid Packets Fortigate가 유효하지 않은 패킷을 받았을 때 로그를 기록합니다.

2. 이벤트(Event) 로그

System 관리적 접근, 정책의 변경 등 Fortigate의 시스템 이벤트에 대한 로그를

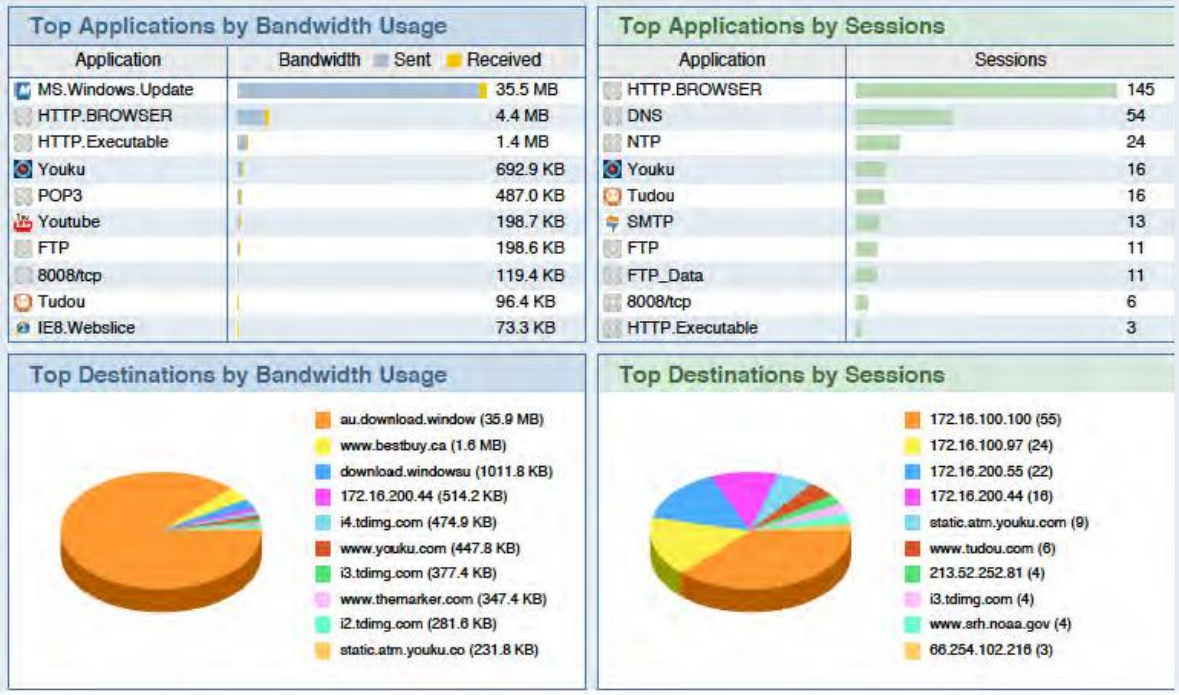
	나타냅니다.
Router	
VPN	IPSec, SSL VPN 관련한 이벤트에 대한 로그를 나타냅니다.
User	사용자 인증 관련한 이벤트에 대한 로그를 나타냅니다.
WAN Opt. & Cache	
WiFi	무선 관련 이벤트에 대한 로그를 나타냅니다.

3. UTM 보안(Security) 로그

AntiVirus	바이러스 탐지, 차단 등 안티바이러스 관련 로그를 나타냅니다.
WebFilter	유해사이트 차단의 웹필터 관련 로그를 나타냅니다.
Intrusion Protection	공격 탐지, 방어의 IPS 관련 로그를 나타냅니다.
Email Filter	스팸 탐지, 차단의 이메일 필터 로그를 나타냅니다.
Data Leak Prevention	정보유출 탐지, 차단의 DLP 관련 로그를 나타냅니다.

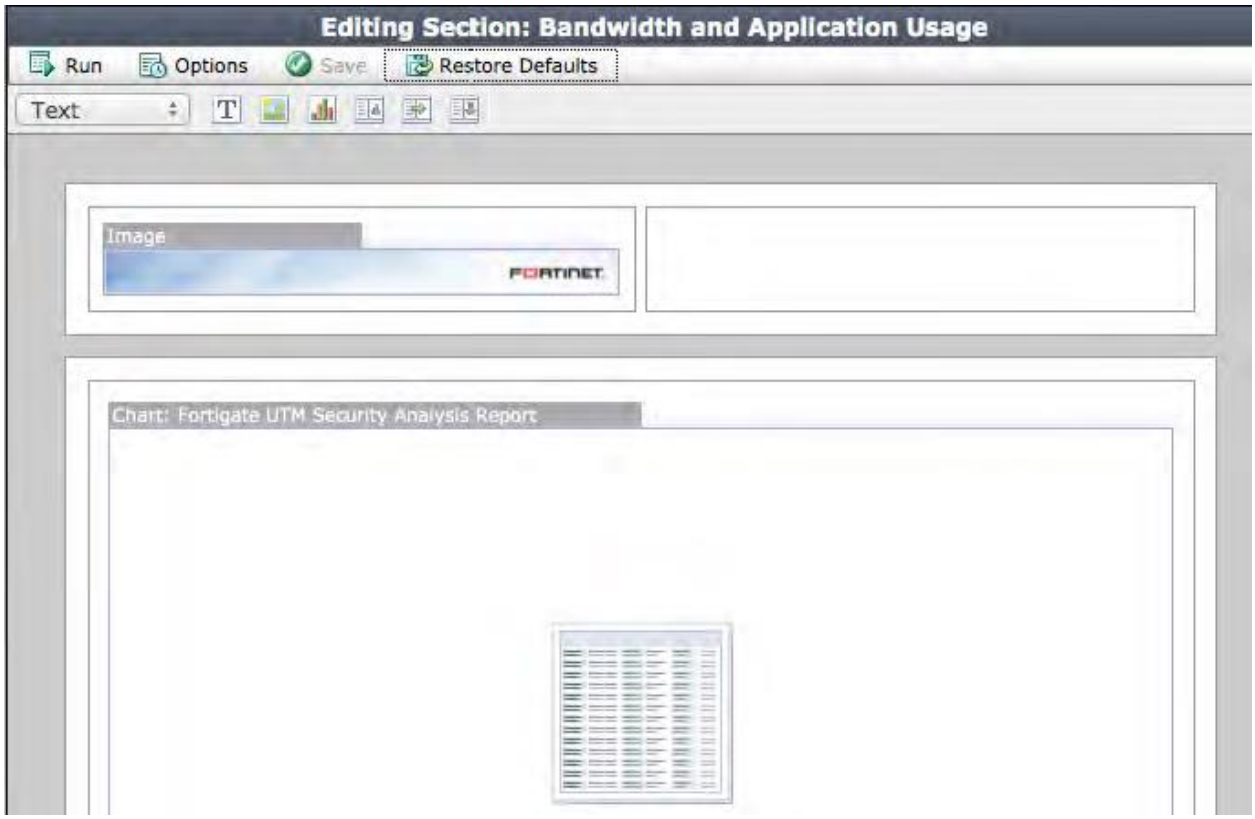
4. 보고서(Report)

보고서에서는 대역폭, Application 사용, 사용자, 목적지, 스트리밍 사용, 이메일 트래픽 등을 확인 할 수 있습니다.



- 보고서 화면 -

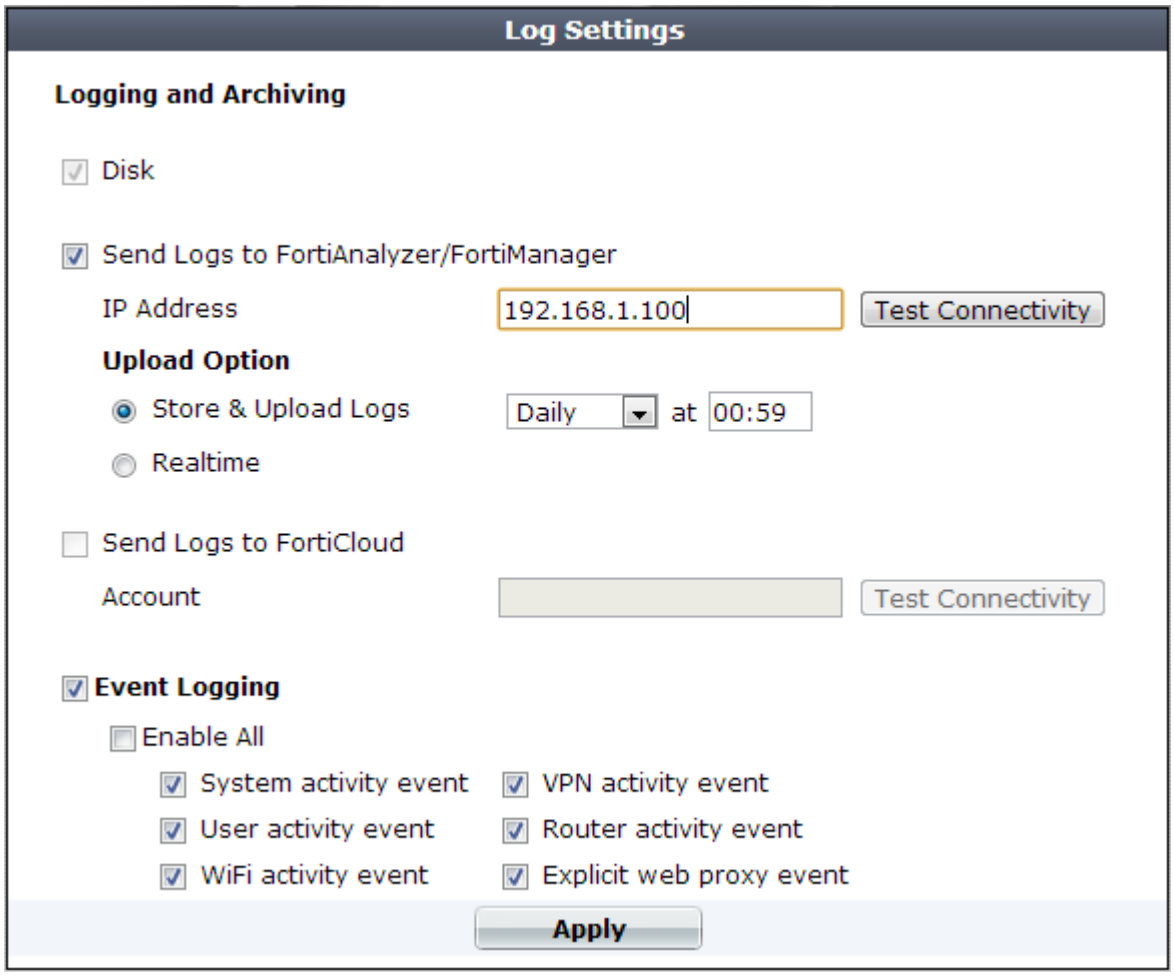
Lastest	가장 최근의 보고서를 보여줍니다. 새로 생성된 보고서는 24시간 후에 Historical로 이동 합니다.
Historical	과거에 생성된 보고서를 보여줍니다.
Config	보고서의 양식과 내용을 설정하고 생성(Run을 누르면 바로 생성됩니다.)합니다. 또한 보고서 생성 스케줄 을 설정 합니다



- 보고서 설정 화면 -

5. 로그 설정(Log Config)

로그 저장 장비의 설정 및 로그 발생 항목을 설정하고 관리자에게 이메일 통보를 하기 위한 설정을 합니다.



- 로그 설정 화면 -

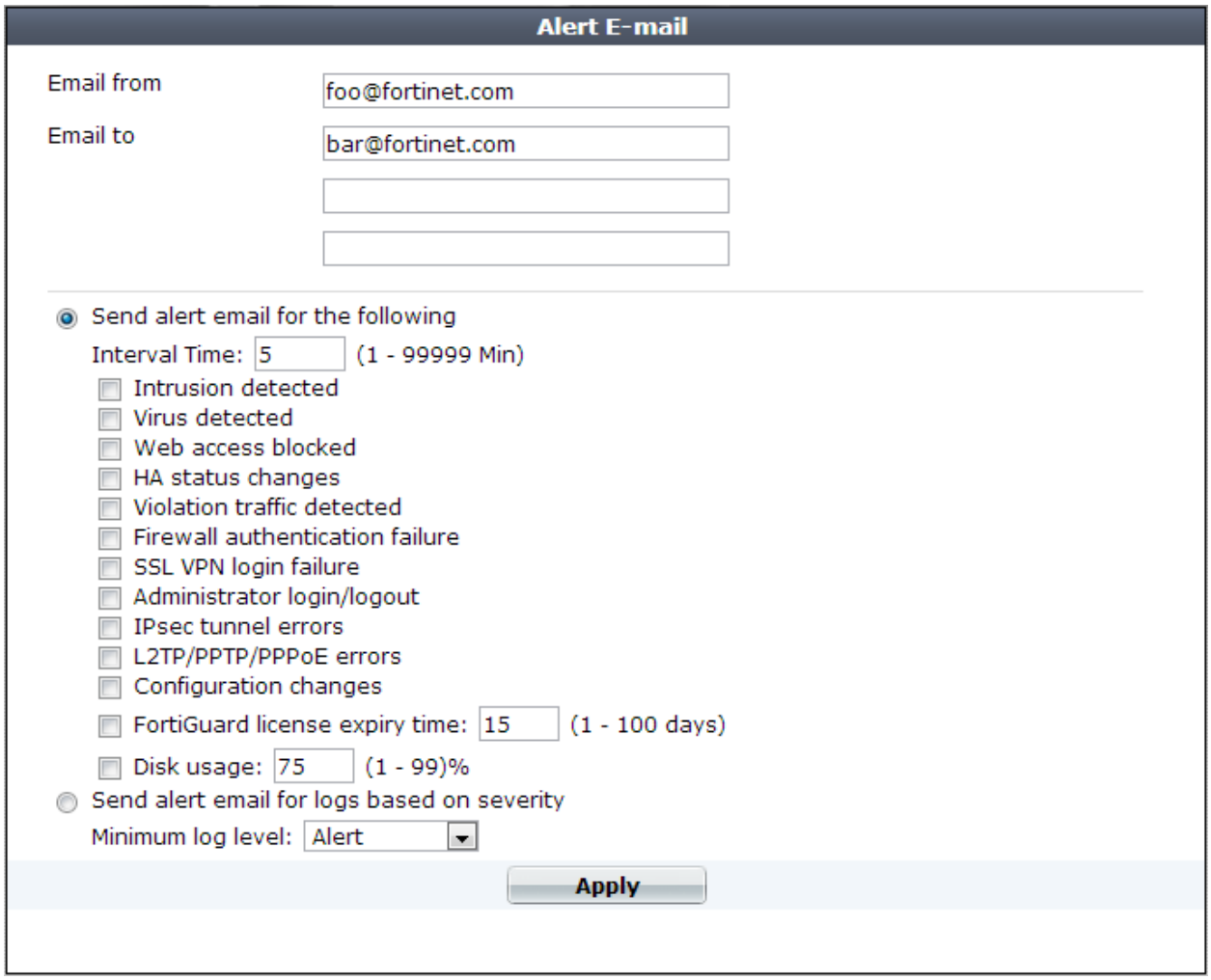
Log Setting 로그을 쌓기 위한 설정과 이벤트 로그 발생 항목을 설정합니다.

Disk 디스크를 내장하고 있는 모델은 로그를 로컬 디스크에 저장 합니다.

Send Log to FortiAnalyzer/FortiManager FortiAnalyzer또는 FortiManager와 연동하여 로그를 수집합니다. Upload Option의 Store&Upload Logs는 로그를 수집했다가 지정한 시간에 연동장비로 로그를 보내고, Realtime은 실시간으로 로그를 보냅니다.

Send Logs to FortiCloud FortiCloud로 로그를 보내어 수집합니다.

Event Logging 이벤트 발생 로그 항목을 설정 합니다.

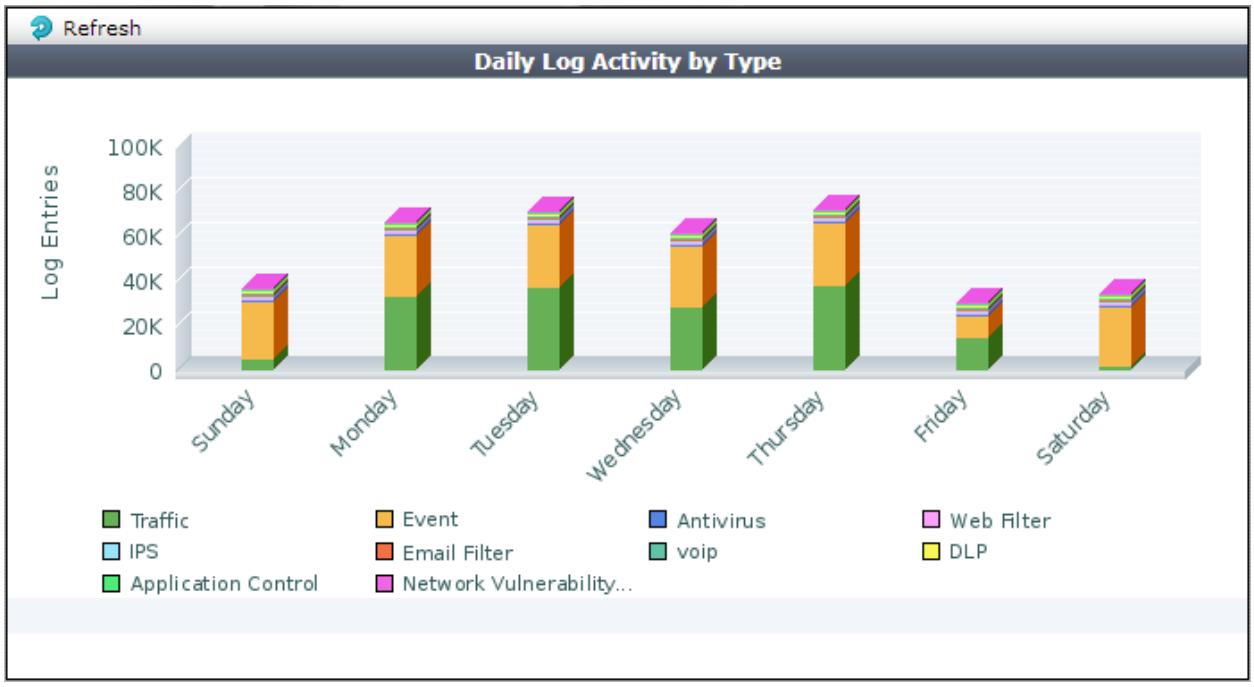


– 이메일 통보 설정 화면 –

Alert E-mail　　이메일 통보 기능을 통해 특정 이벤트가 발생했을 때 담당자는 실시간으로 메일로 로그를 받을 수 있습니다.

6. 모니터(Monitor)

Logging Monitor　　일별 로그 발생 현황을 그래프로 확인 할 수 있습니다.



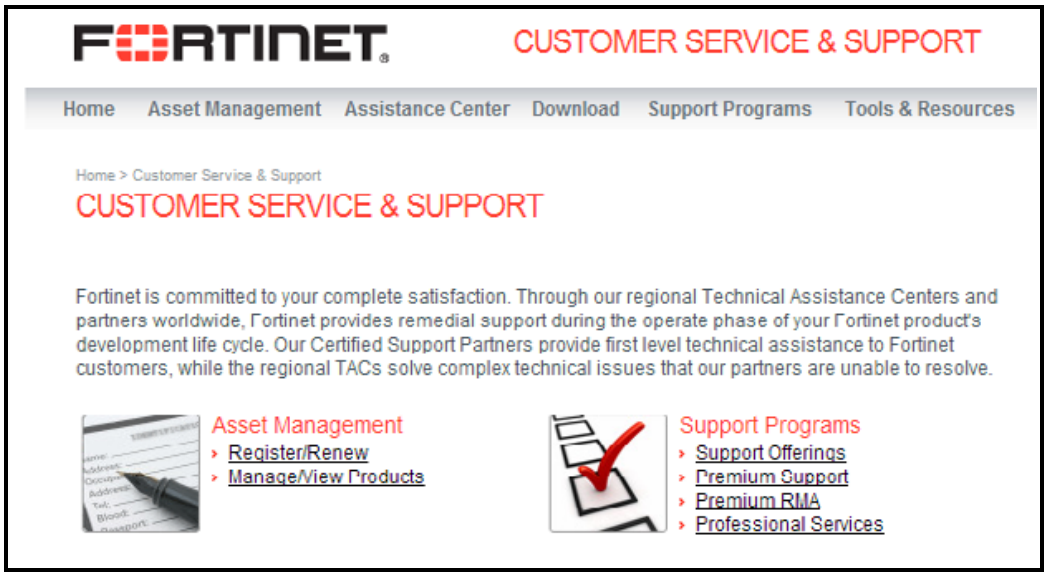
- 로깅 모니터 화면 -

7. FortiCloud 서비스

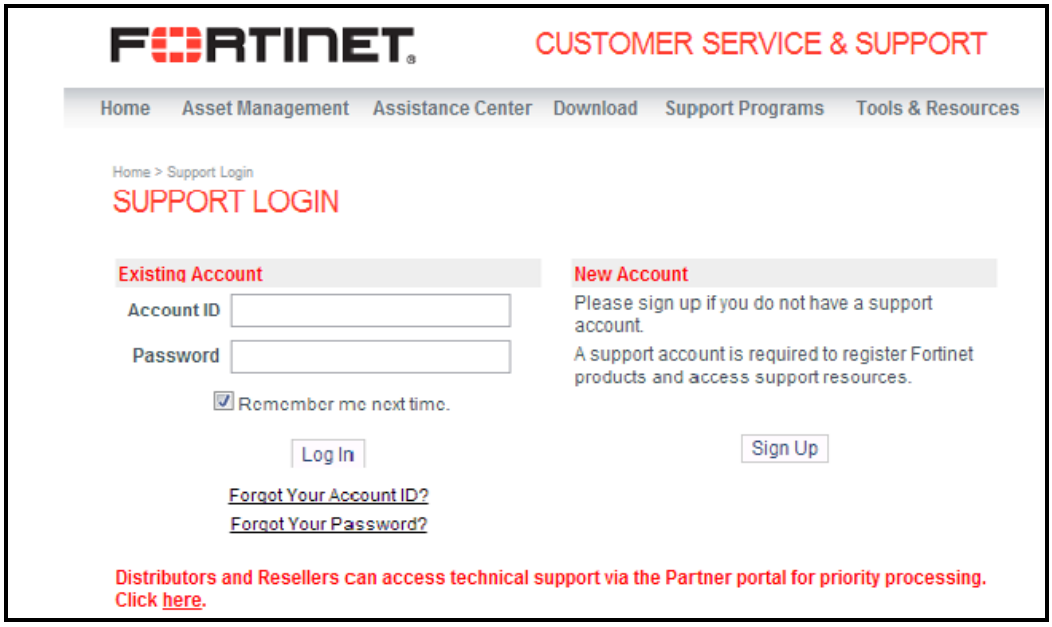
포티클라우드란 Fortigate 및 FortiWiFi 시스템에 대한 보안 관리 와 로그보관 서비스를 제공합니다. 하드웨어, 소프트웨어의 추가 없이 트래픽 분석, 구성 및 로그보관 도구를 제공하여 중앙집중적인 시스템 관리를 할 수 있습니다.

7-1. FortiCloud 계정생성

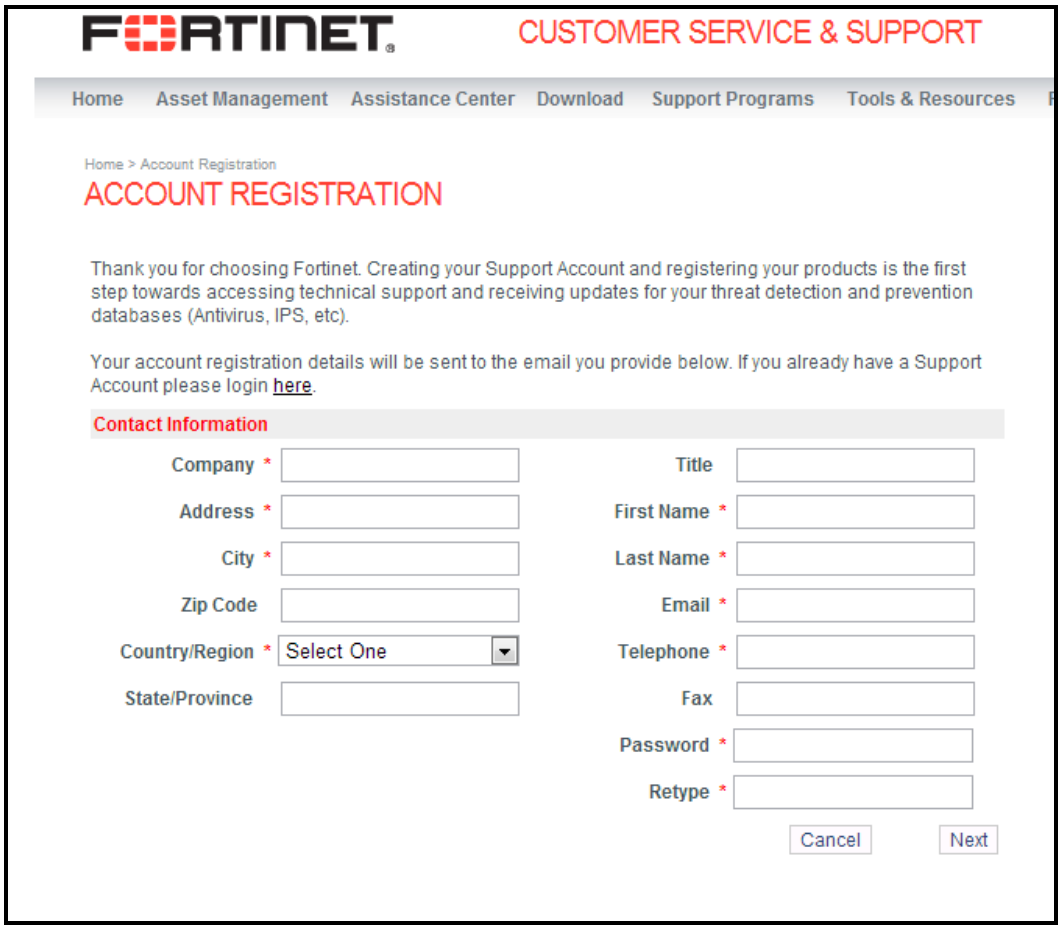
1. https://support.fortinet.com 으로 접속 합니다.



2. Register/Renew를 선택합니다.

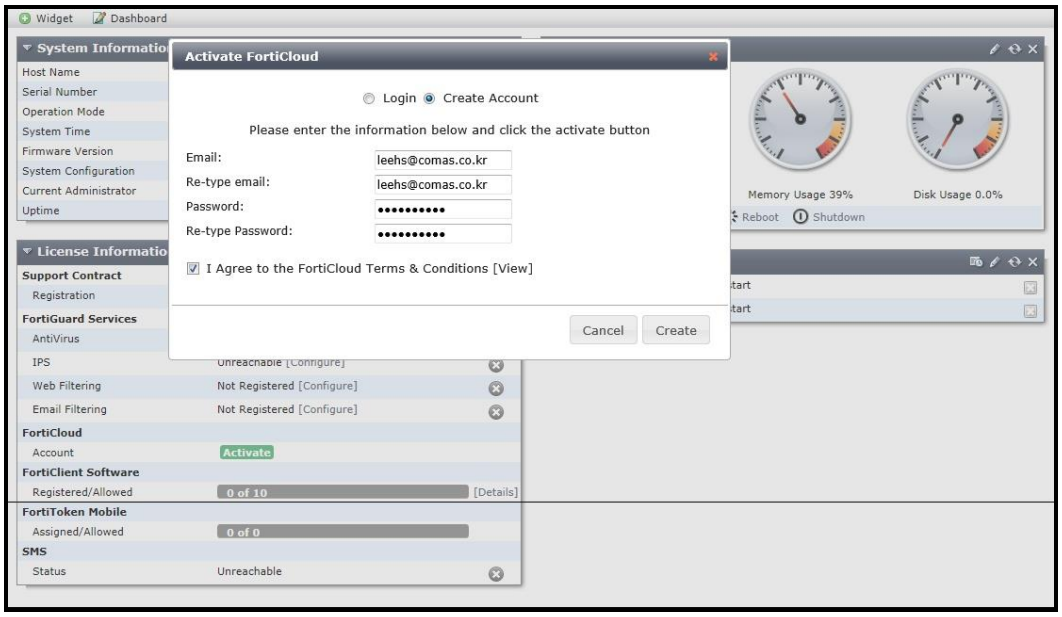


3. 로그인을 합니다. (계정이 없을 경우 Sign Up버튼을 눌러 계정을 생성합니다.)



4. Fortigate의 시리얼넘버로 장비를 등록합니다.
5. Fortigate시스템에 접속 후 *Dashboard > License Information > FortiCloud > Account >*에서 Activate 클릭합니다.

6. Create Account 선택 후 Email, Password 입력 후 이용약관에 동의 체크 후 Create 클릭합니다.



위와 같이 설정을 하면 Dashboard 창에 ''Please view confirmation email'이라는 메시지가 보입니다.

확인 메일을 열고 확인 link 를 클릭하면, FortiCloud 페이지가 열리고 귀하의 계정이 확인되었다는 메시지가 나타납니다.

이 후 Fortigate 시스템의 Dashboard에서 '1GB 무료 또는 200GB 가입' 메시지가 확인되고 하나를 선택하면 FortiCloud 포털에 대한 링크가 제공됩니다.

7-2. FortiCloud Portal

포티클라우드 서비스를 활성화 하면 Fortigate의 대시보드 화면에 FortiCloud 포털 링크가 활성화 되고 이것을 클릭하면 FortiCloud 포털사이트로 이동 할 수 있습니다.

FortiCloud 포털사이트에서는 아래의 다섯 가지 메인 탭을 제공합니다.

- Dashboards
- Logs & Archives
- Drilldown
- Reports
- Management

1. 대시보드(Dashboards)

전반적인 장비의 배경 정보를 제공합니다. 여러 차트와 위젯을 제공하여 현재 상황을 알려줍니다.

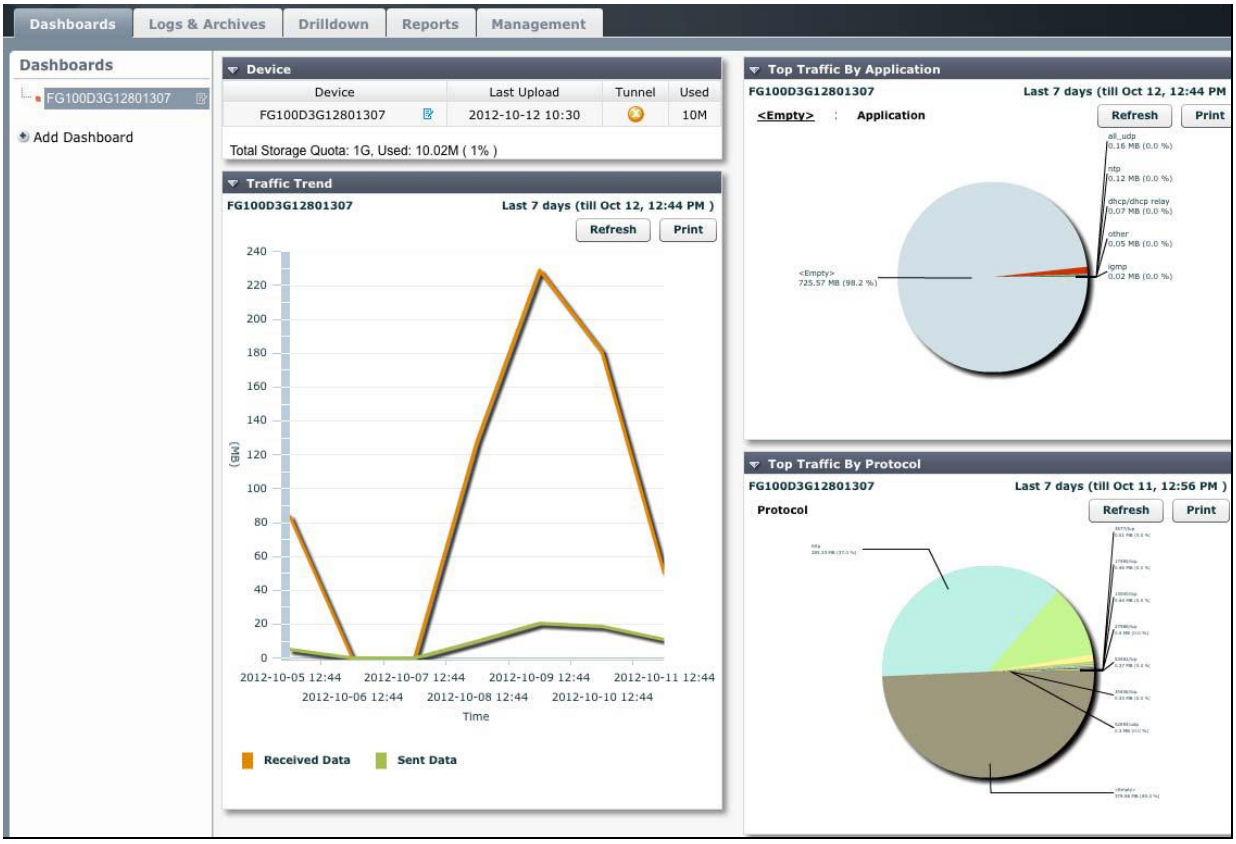
Device : 등록된 장비 S/N , 마지막 업로드시간, Tunnel(Cloud활성화 상태)
Quota(License) , 사용량이 표시됩니다

Traffic Trend : Sent Data, Received Data 가 표시됩니다.

Top Traffic By Application : 어플리케이션 중 가장 많이 트래픽을 사용한 것이 표시됩니다

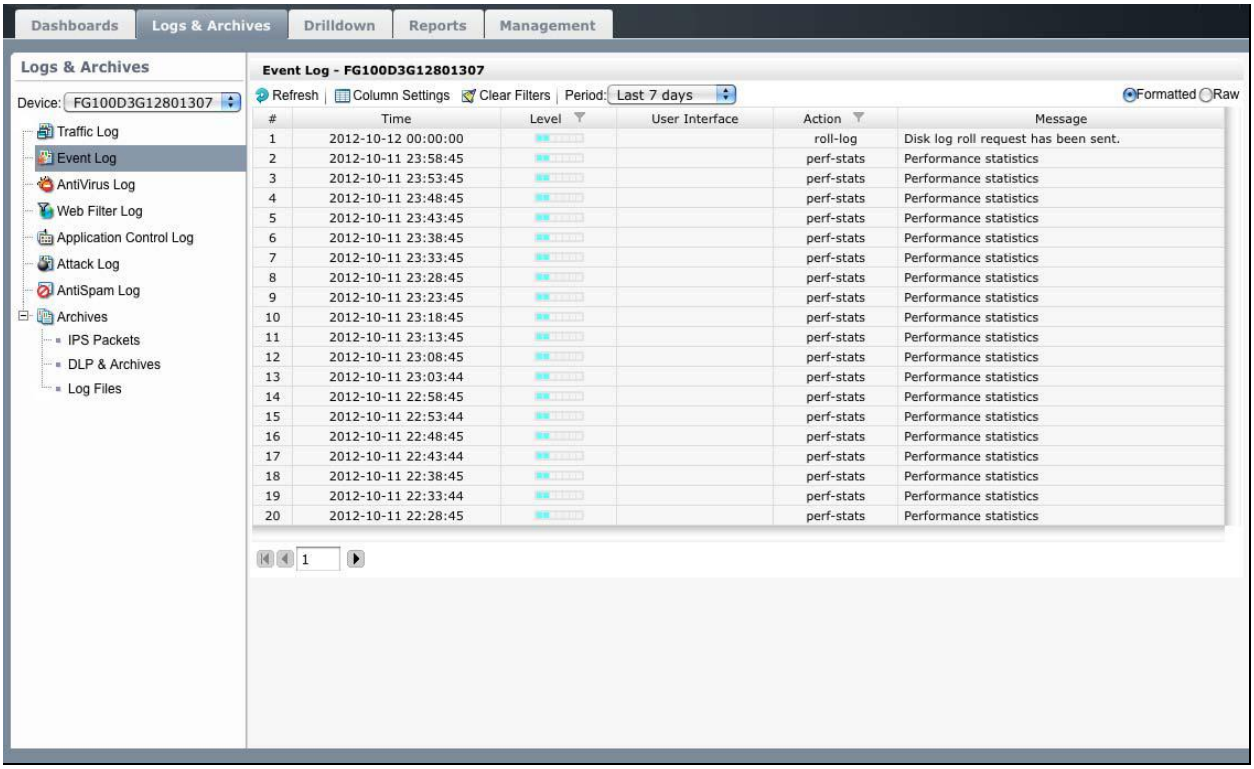
Top Traffic By Protocol : 프로토콜 중 가장 많이 트래픽을 사용한 것이 표시됩니다.

Top Application Category : 어플리케이션 카테고리 별로 표기됩니다.



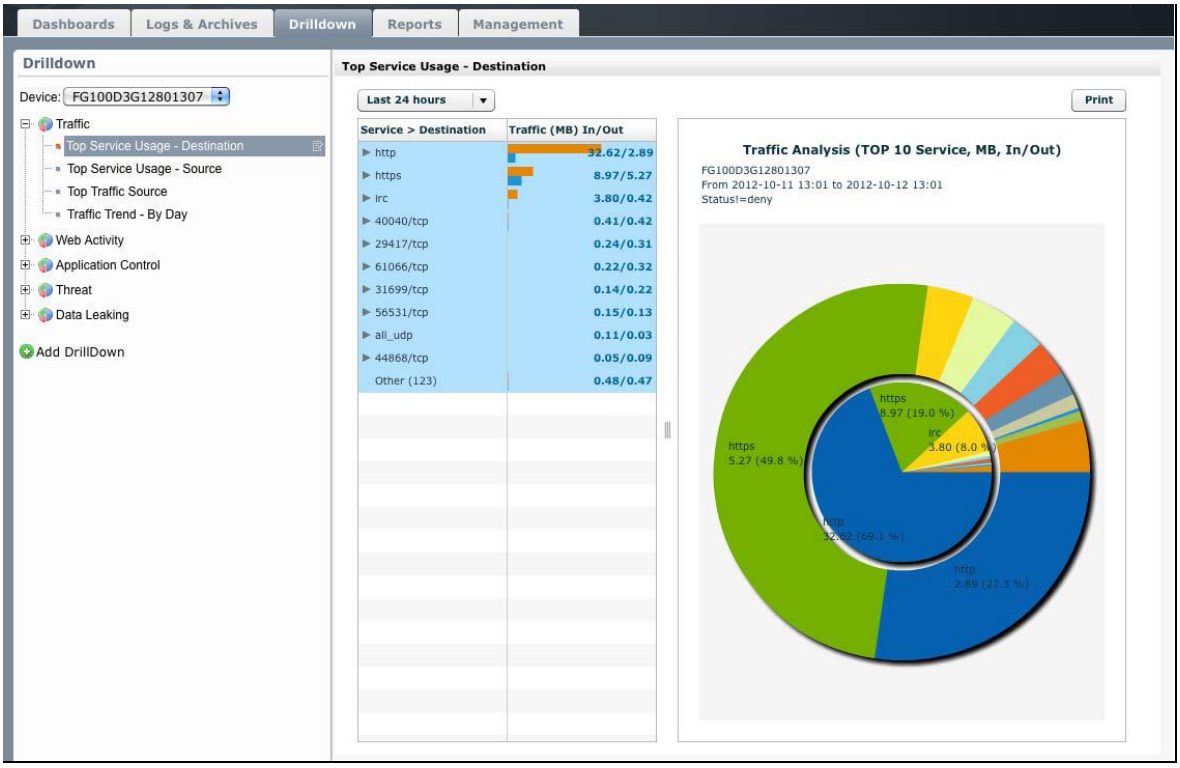
2. 로그와 기록(Log & Archives)

각각의 로그 메시지를 카테고리 별로 보여줍니다. Traffic , Event , AntiVirus , Web Filter , Application Control , Attack , AntiSpam Log 및 Archives 를 볼 수 있습니다.



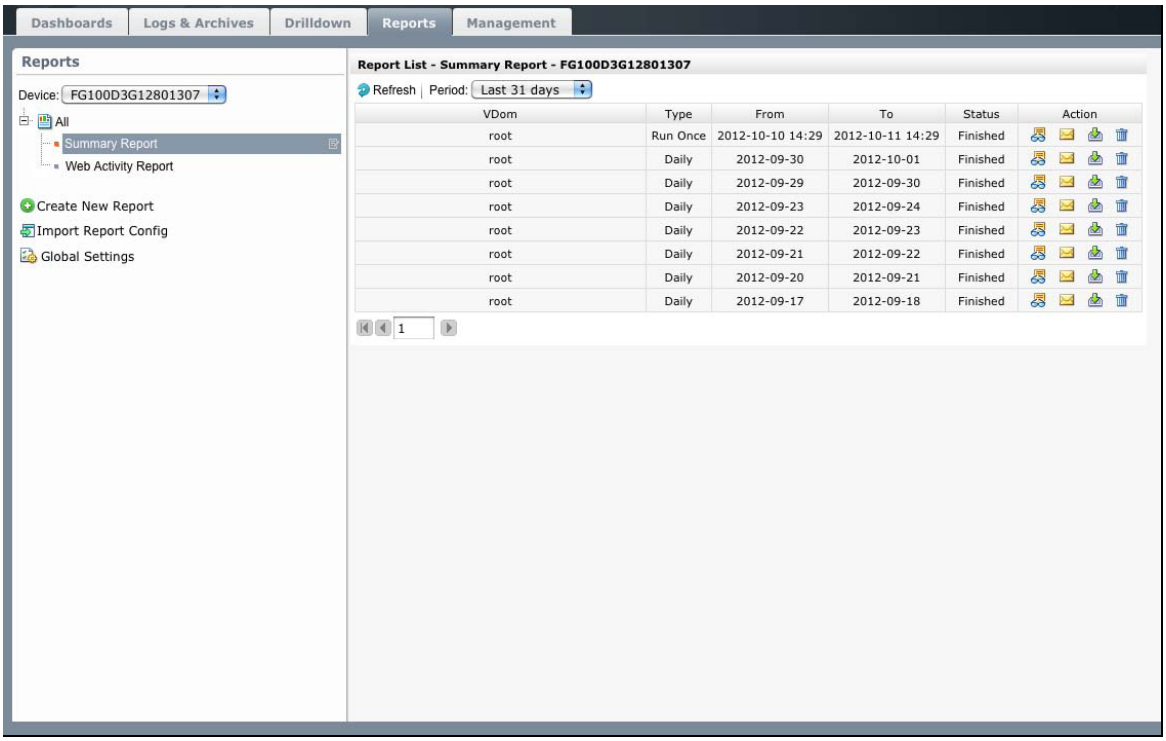
3. **Drilldown**

Drilldown 탭은 특정 항목에 대한 자세한 정보를 찾을 수 있습니다. 이 정보는 Fortigate에서 업로드한 로그에서 자동으로 추출되고 도표화 됩니다.



4. 보고서(Reports)

보고서 탭은 생성된 보고서를 확인, 발송, 삭제 할 수 있고, 새로운 보고서를 생성 할 수 있습니다. 또한, 보고서의 형식을 편집 할 수 있습니다.



5. 관리(Management)

관리 탭은 FortiCloud의 또 다른기능을 제어하기 위한 설정을 할 수 있습니다. 이 탭은 장비의 정보를 추적하고 원격장비로 스크립트를 실행 할 수 있습니다. 또한 다양한 문제에 대하여 관리자에게 경고메일을 설정합니다.