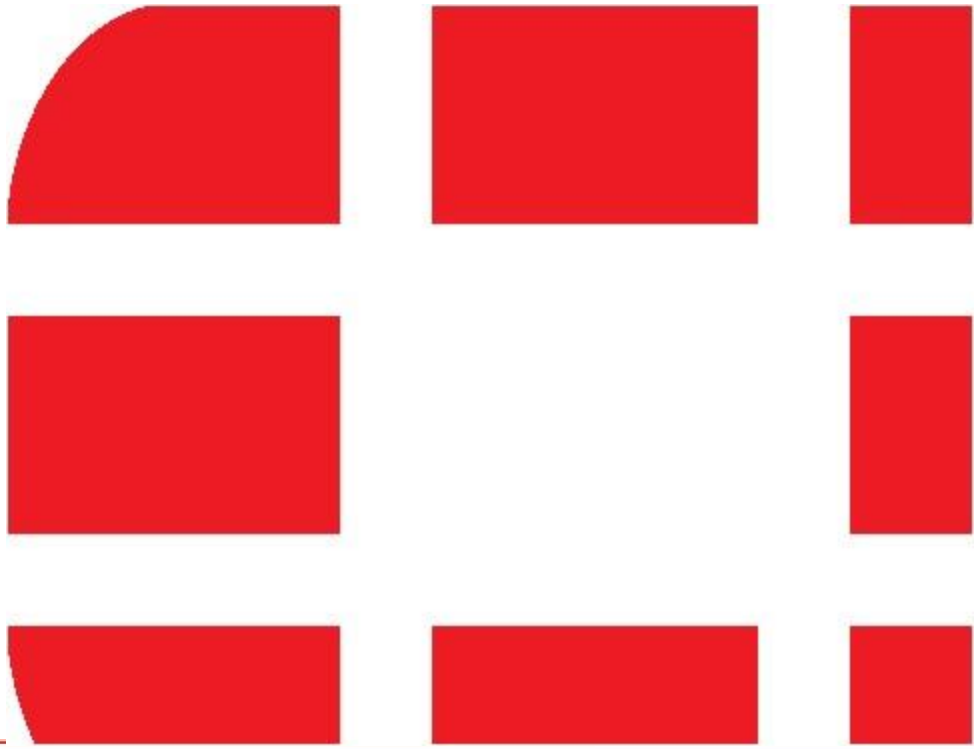
Fortigate Q&A

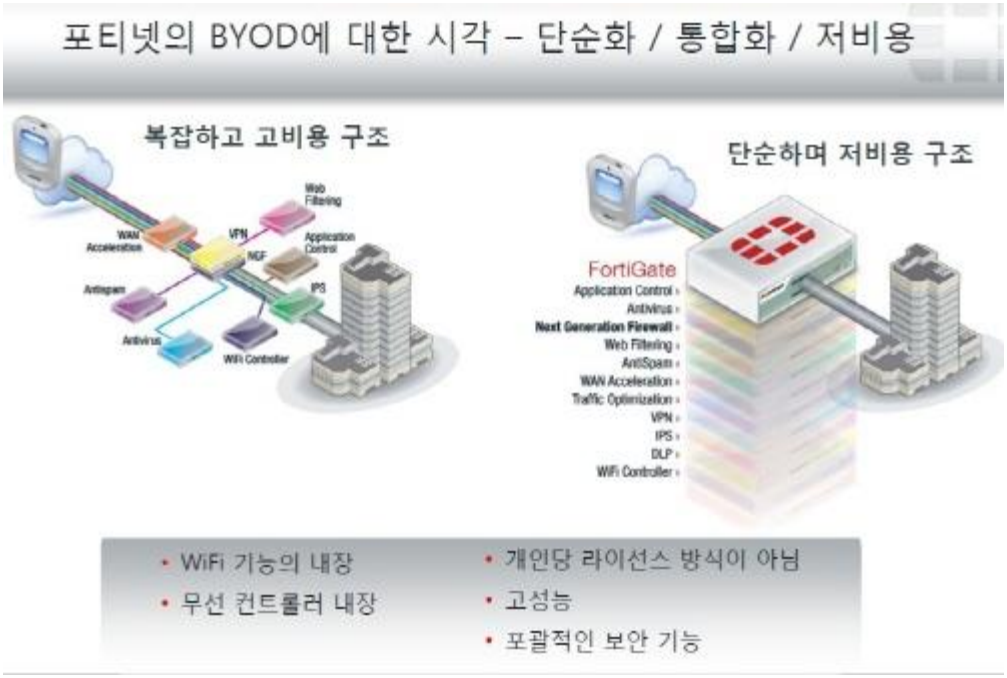


1. 차세대 UTM 이란 무엇인가요?

UTM (Unified Threat Management)이란 하나의 장비에서 여러 보안 기능을 통합적으로 제공하는 것을 말한다. 예전과 같이 독립적으로 보안 기능을 수행하던 방화벽, IPS, VPN, Anti Virus 등의 기능을 한 장비에서 제공함으로써 관리 편의성과 비용절감의 이점을 얻을 수 있다.

보안위협의 진화(다양한 공격 및 혼합 위협)에 따라 전통적인 단일 보안 장비로는 충분치 않게 되었고, 이에 대한 대응책으로 UTM은 새로운 흐름이 되었다.

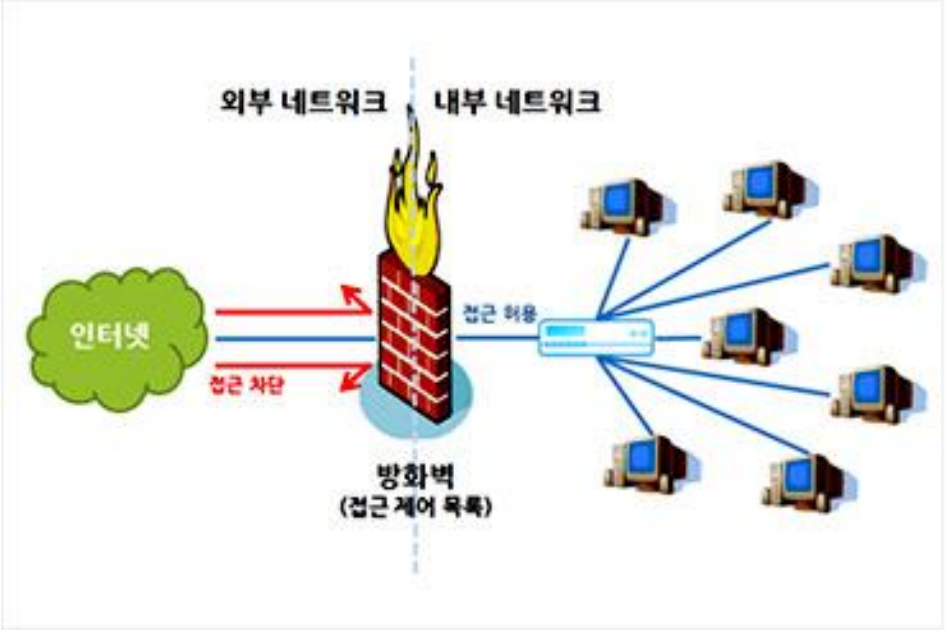
또한, UTM도 계속 진화를 하여 차세대에서 중요시 되는 기능 및 성능에서도 괄목할 만한 성장을 보여주고있다. 전통적인 보안 기능 뿐만 아니라 Wireless-Control, Application Control, DLP등 폭넓은 보안기능이 추가 되고 있는 추세이다.



2. 방화벽(Firewall)이란 무엇인가요?

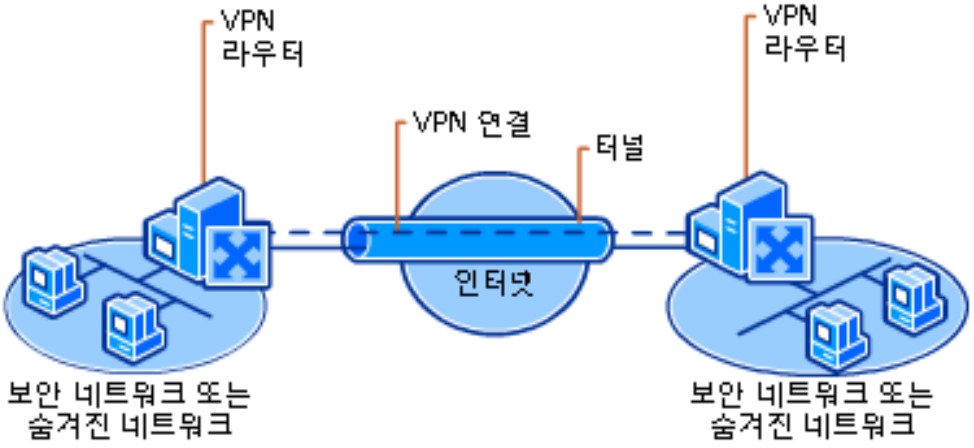
네트워크 단계의 인터넷 보안 시스템 가운데 가장 널리 쓰이는 방법으로, 외부로부터의 침입을 불에 비유해 그것을 막는 벽으로 표현한 것이다.

방화벽은 물리적으로 네트워크를 연결하고 절단시키는 구조를 갖고 있기 때문에 응용 프로그램을 고칠 필요 없이 쉽게 사용할 수 있고, 네트워크에 흘러다니는 모든 패킷을 검사하므로 해킹과 같은 외부 침해를 근본적으로 막을 수 있다는 장점이 있다. 또한 관리자가 규칙을 정하기만 하면 그에 따라 탄력적으로 운용되므로 온라인 상황에서 내·외부의 접속상황을 감시할 수 있어 병목현상을 파악하는 데에도 활용할 수 있다.



3. VPN 이란 무엇인가요?

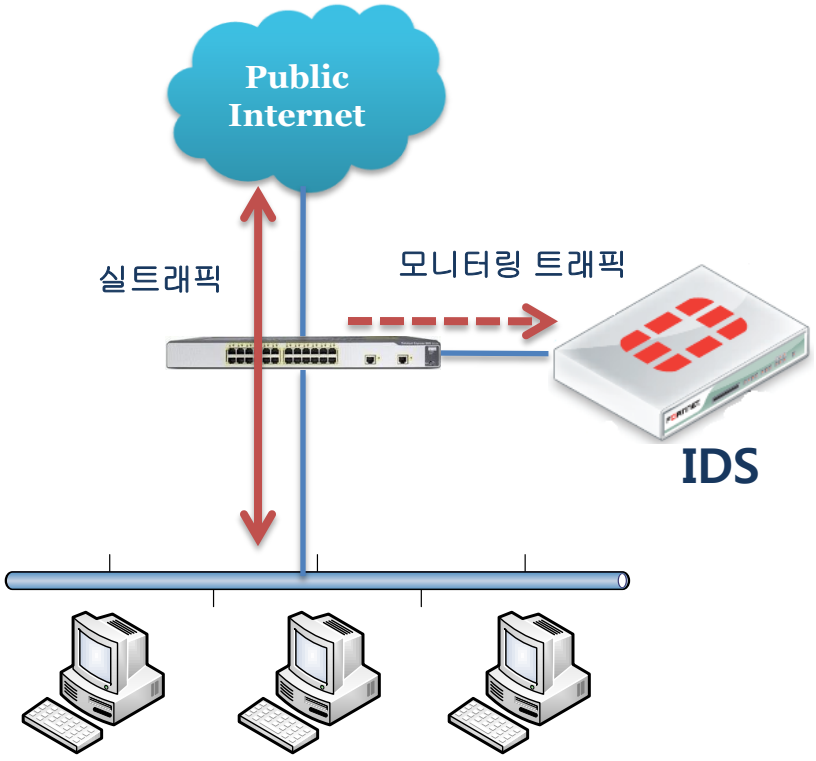
공중 또는 공용 IP(Internet protocol) 인프라 내에 구축된 사설망으로 인트라넷(intranet) 외부에서 가상의 선로(터널)를 만들어 인트라넷에 접속하는 것을 의미하며, 인트라넷을 외부에 개방하지 않고도 필요한 사용자에게 인트라넷에 접근할 수 있도록 허용하는 것이다. VPN의 원래 개념은 자체 정보 통신망을 보유하지 않은 사용자라도 공중 데이터 통신망을 이용하여 마치 개인이 구축한 통신망과 같이 이를 직접 운영·관리할 수 있는 것을 말한다. 공중망을 이용하기 때문에 보안적으로 취약한 부분이 있지만 트래픽에 대한 인증과 암호화로 취약점을 해결 한다.
Fortigate에서는 IPSec, SSL 등의 VPN을 제공한다.



4. IDS란 무엇인가요?

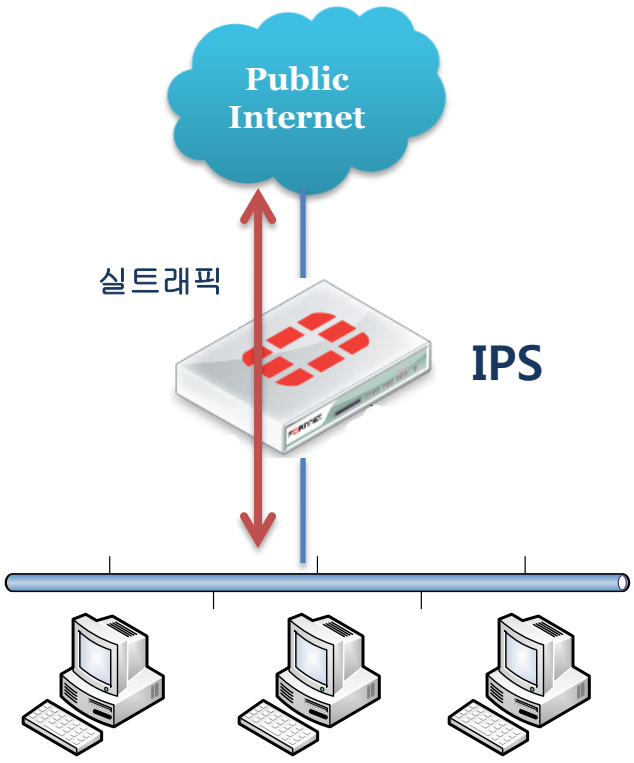
침입탐지시스템(Intrusion Detection System)으로 정보시스템의 보안을 위협하는 침입행위가 발생할 경우 이를 탐지하고, 적극 대응하기 위한 시스템이다. 특히 침입차단을 목적으로 하는 방화벽과는 달리 각종 해킹 수법의 패턴을 자체에 내장하고 있어 침입행동을 실시간으로 감지,추적할 수 있다.

보통 One-Armed 형태로 설치 되기 때문에 실 서비스에 영향을 주지 않고 운영이 가능하다.



5. IPS란 무엇인가요?

- IPS(Intrusion Prevention System)는 공격 피해를 최소화 할 수 있는 능동적 보안 시스템으로, IDS는 탐지하는 역할을 하지만 IPS는 실제 차단 기능 까지 수행을 한다. IDS와 마찬가지로 네트워크 트래픽을 감시하고, 검사하여 그것이 부당한 패킷 이라고 판단되면 주어진 정책에 따라 차단을 하고, 정상적인 트래픽에 대해서는 서비스 지연 없이 수신 측에 전달 한다.

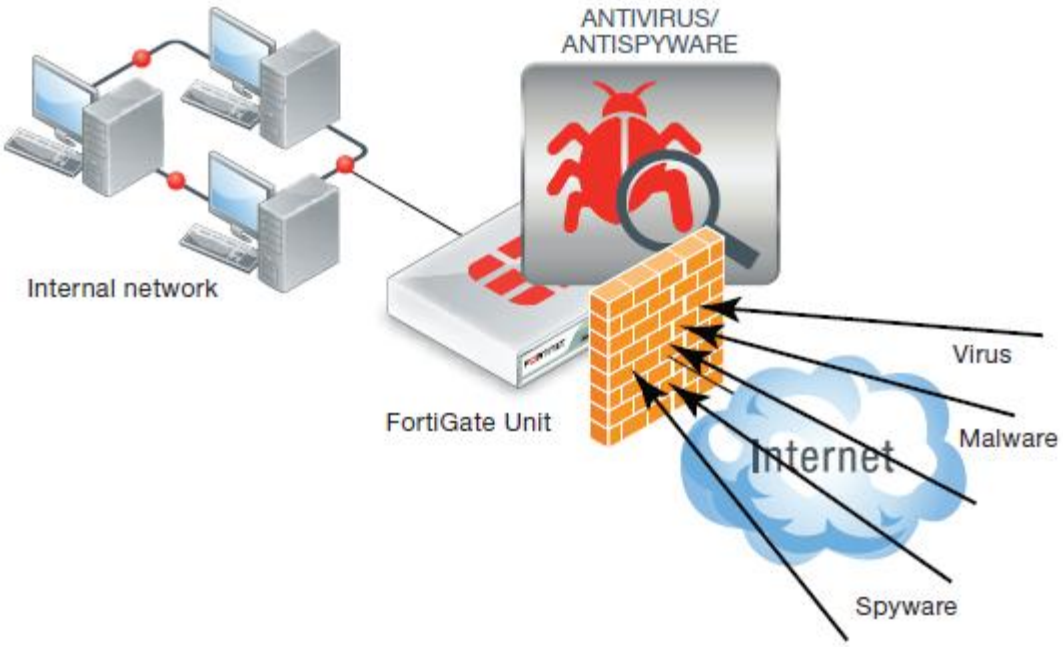


6. Anti Virus 란 무엇인가요?

보통 AntiVirus는 바이러스나 malware를 진단 및 치료 하는 컴퓨터 백신을 가리키나 Fortigate와 같은 UTM장비에서 AntiVirus는 그 개념이 다르다.

UTM의 특성이 네트워크 트래픽에 대한 검사이기 때문에 AntiVirus 또한 유입되는 바이러스나 malware를 네트워크 레벨에서 차단 하는 것을 말한다. 치료가 아닌 차단이 임무이다.

AntiVirus는 신규 바이러스에 대한 대응이 중요하기 때문에 항상 최신의 패턴으로 동작을 하여야 한다. Fortinet은 항상 FortiGuard Center(패턴업데이트 센터)에서 최신의 패턴을 Fortigate로 업데이트 하고 있다.



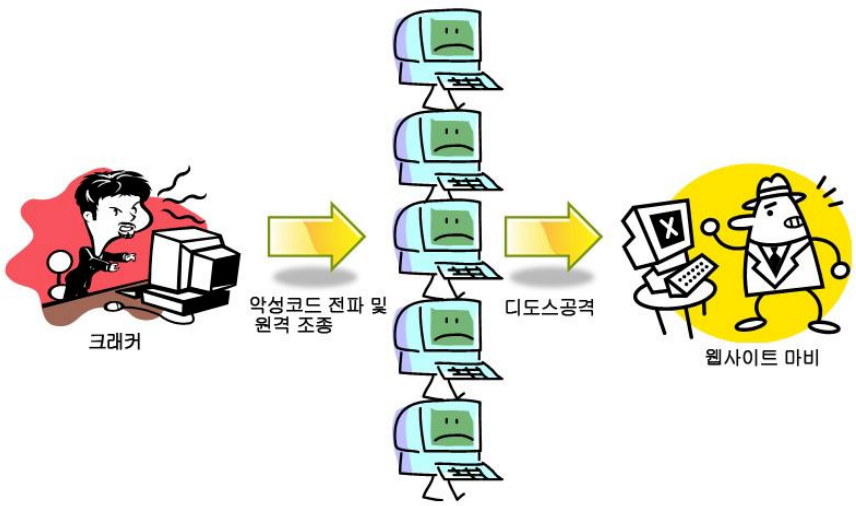
7. Anti Spam 이란 무엇인가요?

- 네트워크를 통해 불특정 다수에게 유포되는 광고 성 메일을 가리켜 Spam Mail이라고 한다. Spam Mail은 여러가지 해킹 기술과 접목하여 개인 및 기업 정보보안을 위협하는 요소가 되었다. 이러한 Spam Mail을 차단하는 솔루션을 AntiSpam이라 한다.
  Fortigate 또한 AntiSpam 기능을 지원을 하고, Banned Word, IP address, FortiGuard 등 여러 가지 차단 방법을 지원하고 있다.

8. (D)DoS란 무엇인가요?

DoS(Denial of Service)공격이란 시스템을 악의 적으로 공격해 해당 시스템에 부하를 주어 정상적인 서비스를 하지 못하게 하는 공격을 말한다. 보통 공격 서버에 수 많은 접속 시도를 하여 서버가 서비스 할 수 있는 한계치를 넘게 되면 더 이상의 정상적인 접속이 불가능 해진다. 하지만 DoS공격은 공격자가 하나의 IP를 이용하기 때문에 방화벽 만으로도 공격자의 IP를 막아 해결 할 수 있다.

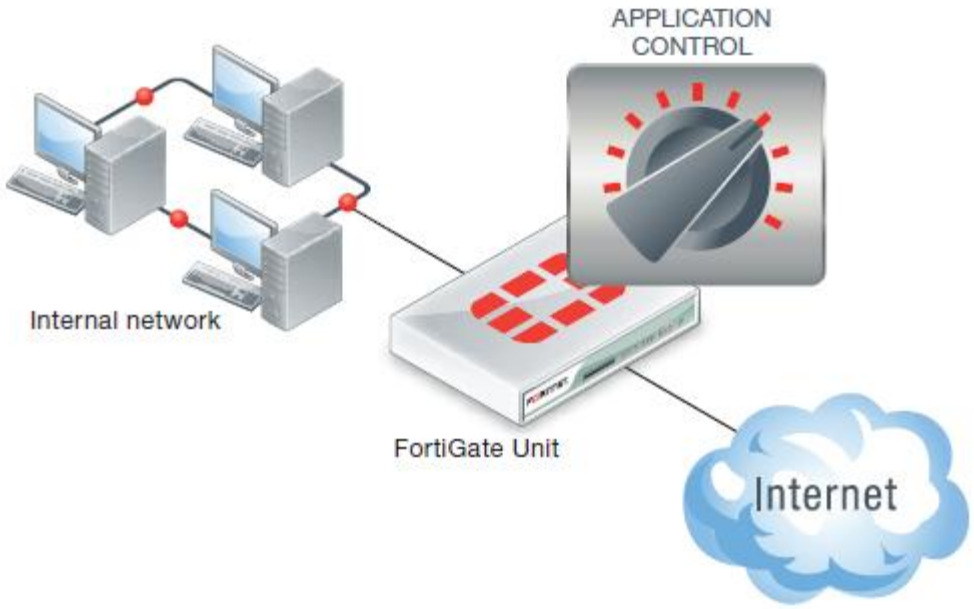
DDoS(Distributed DoS)란 DoS의 발전형으로 공격자는 악성코드를 이용하여 수 많은 좀비PC를 만들고, 실제 이 좀비PC를 이용하여 대상을 공격한다. 이 경우 다양한 IP에서 대량의 접속이 발생하기 때문에 서버 입장에서는 정상적인 접속과 공격을 분간해내기 힘들고, 실 공격자의 수도 많기 때문에 그 파급력이 크다.



9. Application Control 이란 무엇인가요?

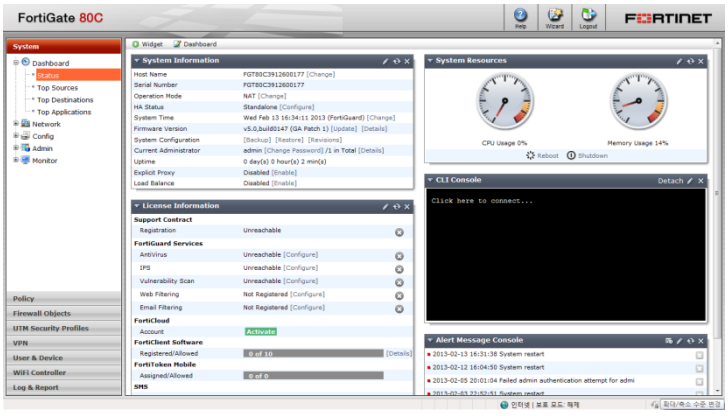
현 시대는 네트워크를 이용하여 수 많은 정보를 공유하고 수 많은 사람들과 커뮤니케이션을 한다. 하지만, 이러한 행동들이 기업 업무나 정보보안에 위협이 될 수 있다. 예를 들어 사내에서 P2P를 이용하여 네트워크가 마비 된다던가, SNS나 메신저를 이용해 기업 정보가 유출 되는 경우가 종종 있다. 이러한 Application 들은 실제 좋은 용도로 개발 되었으나, 부득이 차단하거나 제어해야 할 경우가 생기게 된다.

Fortigate는 다양한 Application패턴을 제공하여 내부에서 발생 할 수 있는 보안 위협에 능동적으로 대처 할 수 있도록 한다.

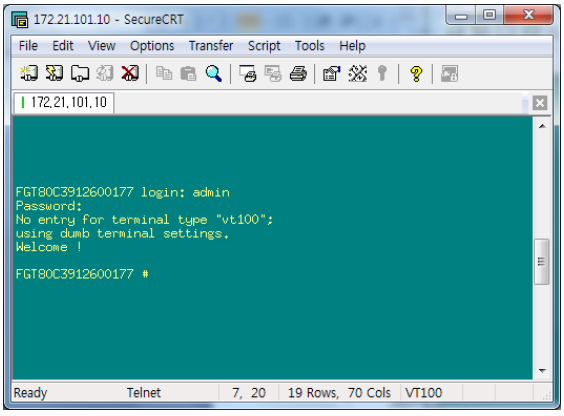


10. 차세대UTM장비를 접속할 때 https, http, telnet , ssh로 접속한다고 하는데, 이것들은 무엇이며, 어떻게 접속한다는 것인가요?

관리자가 정책을 설정하기 위해 Fortigate에 접속하는 방법은 크게 GUI(Graphic User Interface), CLI(Command Line Interface) 두 가지로 나누어진다. GUI에는 http와 https가 있는데 둘 다 인터넷 브라우저를 이용하여 접속을 한다. 두 접속의 차이점은 접속 자체가 보안 접속인지 아닌지의 차이라고 보면 된다. http의 경우 보안 접속이 아니고, https는 보안 접속이다. 마찬 가지로 CLI는 전용 접속 프로그램을 이용하여 접속을 하고, telnet은 보안 접속이 아니지만, ssh는 보안 접속이다.



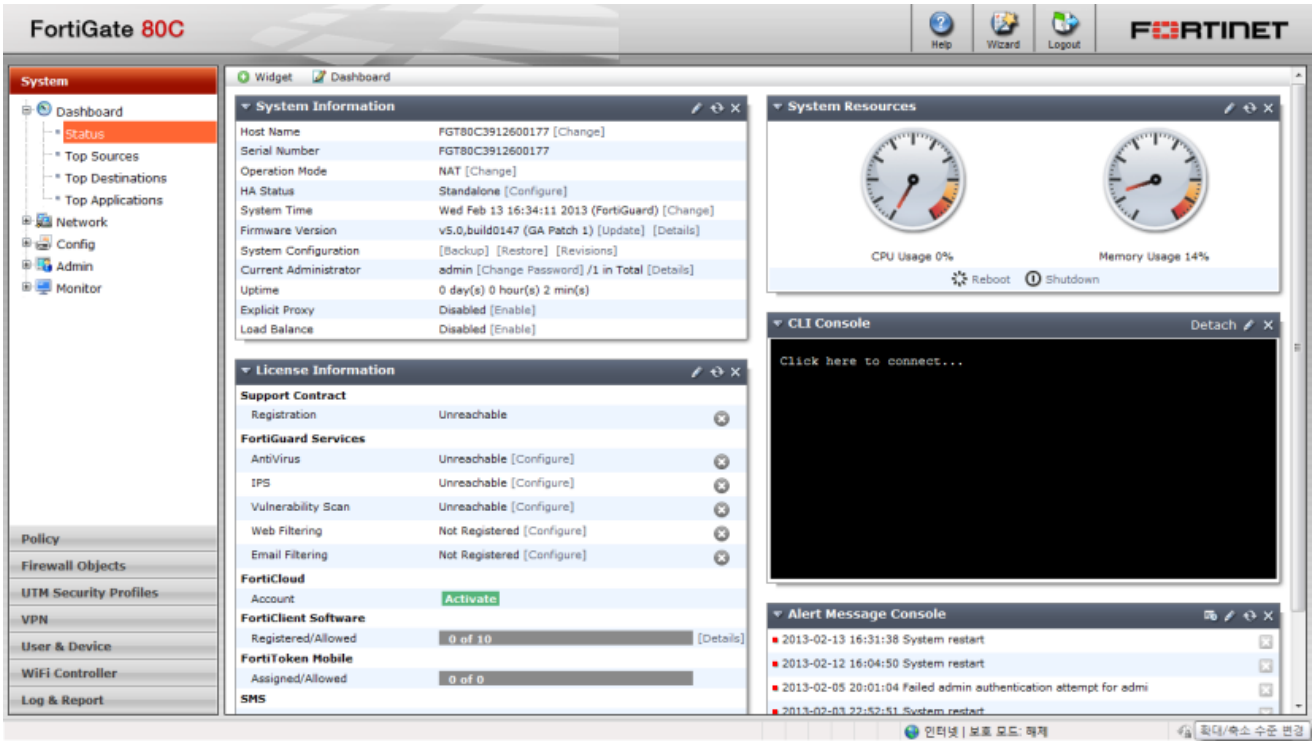
- GUI 접속화면 -



- CLI 접속화면 -

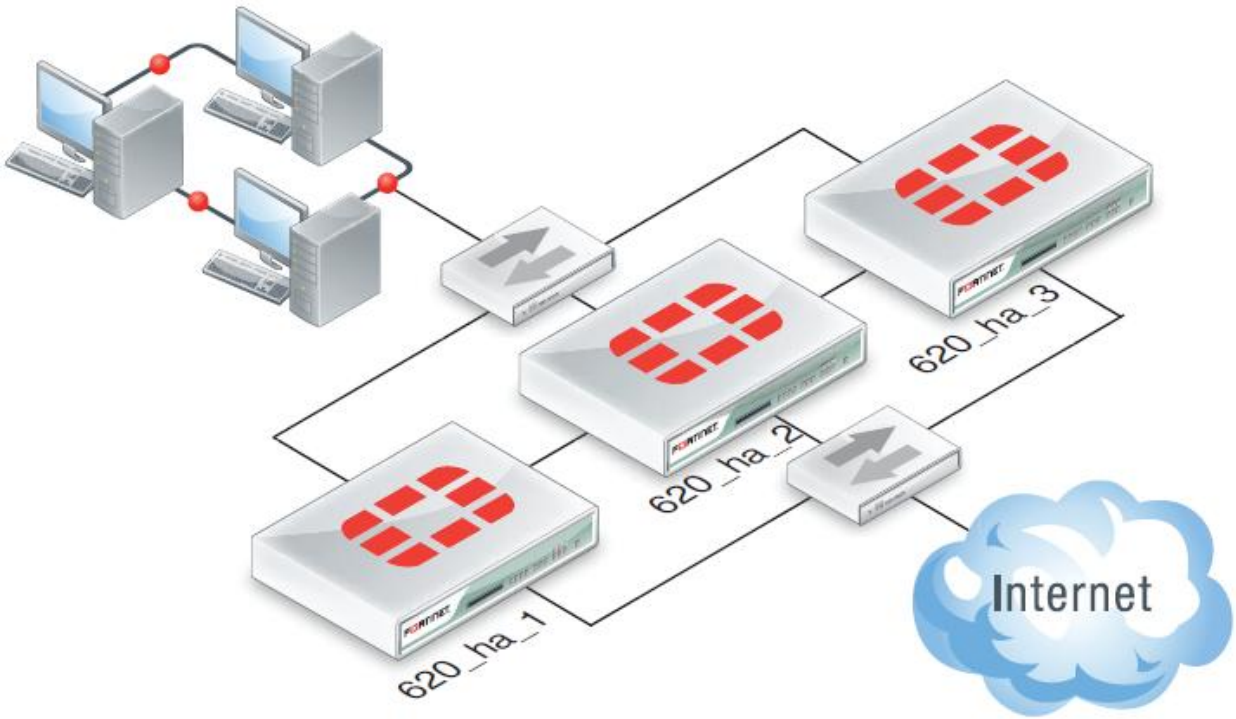
11. 시스템상태에서 DashBoard란 무엇이며, 어떤 기능을 하나요?

- GUI에서, 한 화면에서 다양한 정보를 중앙 집중적으로 관리하고 찾을 수 있도록 하는 사용자 인터페이스를 말한다. Fortigate의 경우 시스템정보, 라이선스 정보, CPU Memory현황, 트래픽 히스토리, 경고메시지 등 다양한 정보를 제공하고 있어, 관리자가 네트워크 현황이나 보안 위협에 대한 정보를 확인하기 쉽도록 되어 있다.



12. HA 이중화 구성설정이라는 것이 무엇이죠?

- HA(High Availability, 고 가용성)이란 하드웨어나 소프트웨어 장애에도 불구하고 사용자가 특정한 애플리케이션을 지속적으로 사용할 수 있도록 고안된 시스템을 넓은 개념으로 나타낸 것이다. HA를 구현하는 방법 중의 하나가 이중화 인데 Fortigate는 전용 프로토콜인 FGCP와 표준인 VRRP를 모두 지원하고 있어 다양한 장비 이중화로 고 가용성을 구현 할 수 있다.

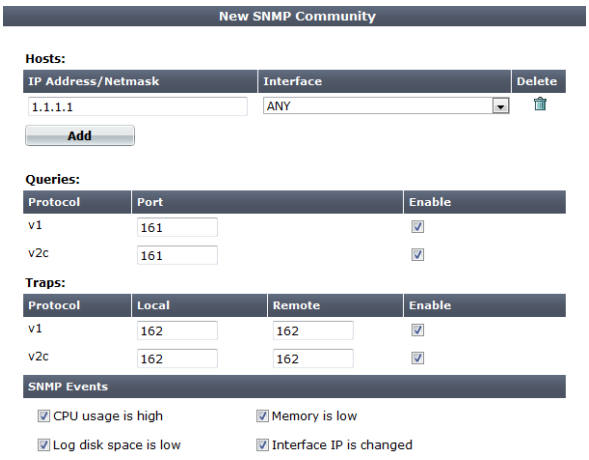


13. SNMP Agent 설정은 어떻게 하는 건가요?

1) 인터페이스 설정
System > *Network* > *Interface* 에서 SNMP Manger와 통신할 인터페이스에 snmp접속을 허용한다.

2) SNMP agent 설정
1 *System* > *Config* > *SNMP*로 이동한다.
2 *SNMP Agent* 활성화를 선택한다.
3 Enter a description, location, contact를 써 넣는다. (선택사항)
4 *Apply*를 선택한다.

3) SNMP community 설정
1 *System* > *Config* > *SNMP* 로 이동한다.
2 *SNMP v1/v2c* 에서 *Create New*를 선택한다.
3 *Community Name*을 설정한다 .
4 SNMP manager의 IP를 설정한다.
5 SNMP manager가 Fortigate와 같은 서브넷에 있지 않다면 interface를 설정한다.
6 SNMP manager과 쿼리, 트랩 및 프로토콜과 통신할 *Port number*를 설정한다.
7 *OK*를 선택한다.



14. 인증부분에서 Fortigate인증, Remote인증, CA인증이 있는데 각각 어떻게 틀린가요?

System -> Certificates (인증서) 메뉴는 인증방법을 설정하는 것이 아니라 사용자 인증에 사용할 인증서를 등록하는 메뉴다. 인증서는 https를 이용하여 네트워크 서비스에 접속하려는 사용자 인증의 중요한 역할을 한다.

1. Local Certificates
   로컬인증서는 사설 인증서로 분류되며, 내부 기업 네트워크에 사용된다. 인증파일에 개인키 파일이나 PEM(전자인증메일)을 포함한다.

2. Remote Certificates
   원격인증서는 개인키가 없는 공개인증서로 OCSP서버를 사용하여 인증을 받는다.

3. CA Certificates
   CA 인증서는 로컬 인증서와 유사하지만 인증서가 폭넓은 주소 범위나 회사 전체에 대해 적용된다.

15. 라우팅 설정에서 정적 라우팅이 있고 다이나믹 라우팅이 있는데 어떻게 다른가요?

- 라우팅이란 패킷의 경로를 설정하는 것을 말한다. 크게 Static(정적) 라우팅과, Dynamic(유동)라우팅으로 나누어 지는데 Static은 말그대로 미리 정해져 있는 경로테이블 대로 패킷을 전송 시킨다. 반면 Dynamic은 목적지로 갈 수 있는 여러 경로 중 최적의 경로를 찾아서 패킷을 전송 시킨다. Dynamic의 경우 라우팅을 하는 장비들이 서로 정보를 공유하여 경로를 산출하기 때문에 각 장비들이 Dynamic 라우팅 프로토콜을 지원해야 구현이 가능 하다. Fortigate는 BGP, RIP, OSPF의 Dynamic 라우팅 프로토콜을 지원한다.

16. Access control 같은 Policy Routing을 제공한다고 하는데 이건 어떤 기능인가요?

PBR(Policy Based Routing)이란 ACL(Access Control List)과는 다른 개념이다. Routing이라는 단어가 보이듯이 패킷의 경로를 설정해 주는 기능이다. 위 에서 설명했듯이 라우팅에는 크게 Static와 Dynamic나누어 진다. 하지만 두 라우팅 방식 모두 목적지 주소(Destination IP)를 조건으로 경로를 설정한다. PBR이란 이런 라우팅 조건의 확장이라고 할 수 있다. 경로 설정의 조건을 목적지 주소 뿐만 아니라 출발지 주소, Source 포트, Destination 포트 등 여러 가지로 주어 더욱 다양한 라우팅 설정을 가능하게 한다.

17. 인바운드 무엇이고, 아웃바운드는 무엇인가요?

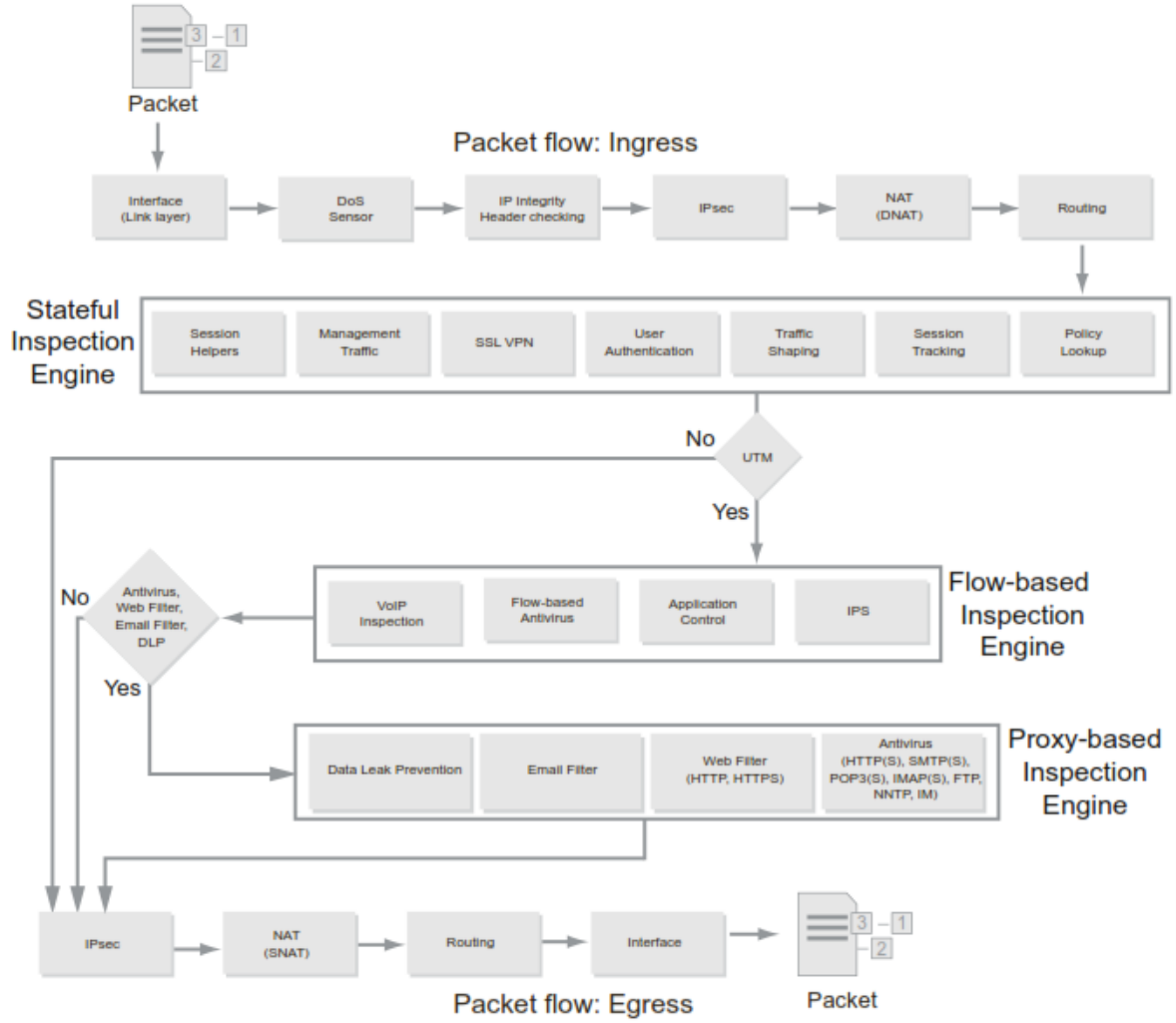
보통 방화벽은 외부 네트워크와 내부 네트워크를 나누는 구간에 위치를 한다. 그래서 외부 네트워크를 External, Untrust 내부 네트워크를 Internal, Trust라고 표현을 하고, 이 두 구간에 대한 방화벽 정책을 인바운드, 아웃바운드 정책이라고 표현한다.

인바운드(Inbound)는 외부에서 내부로 접근하는 정책을 말하며 아웃바운드(Outbound)는 내부에서 외부로 접근하는 정책을 말한다.

18. 보안정책의 우선순위는 어떤 정책부터 적용되나요?

- 기본적인 방화벽 정책은 상위 정책부터 우선순위가 적용된다. 여러 보안 기능에 대한 처리 순서는 아래 Packet Flow를 참고한다.

Figure 9: Packet flow



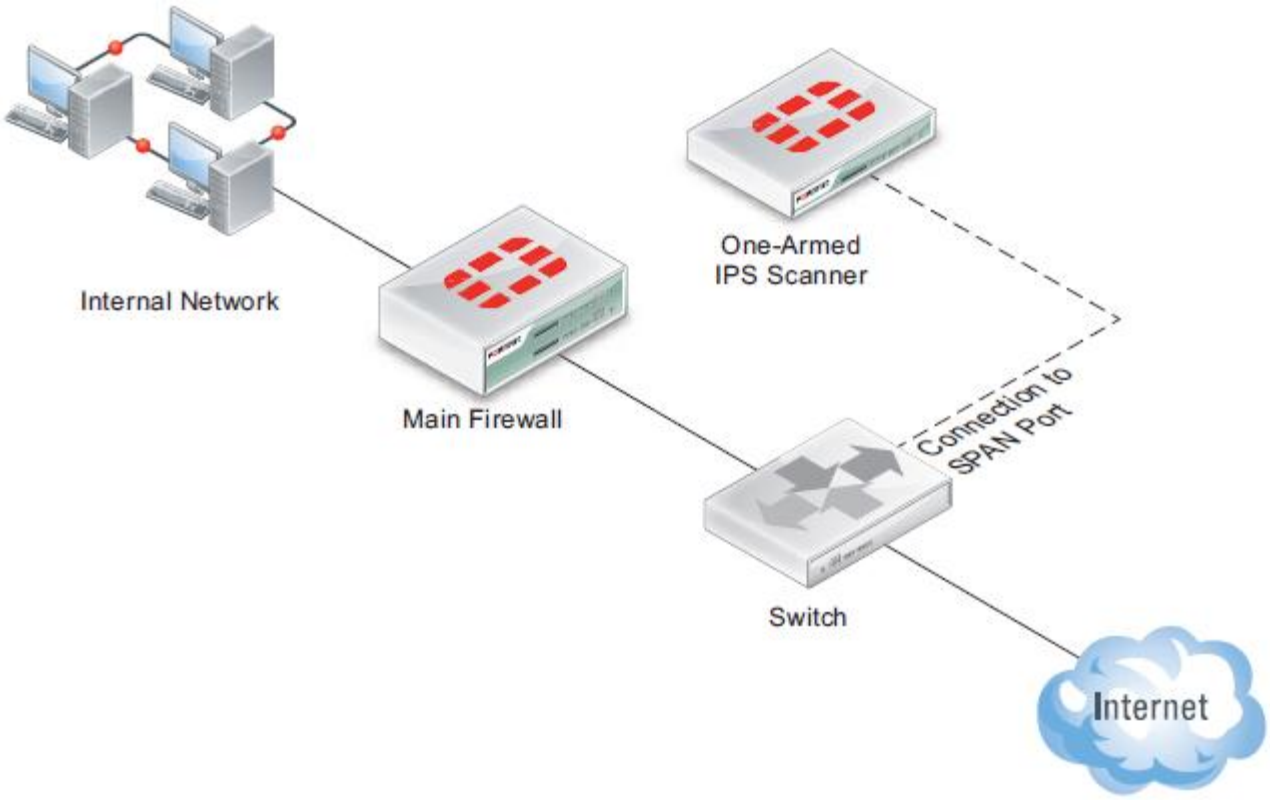
19. Sniffer Policy란 무엇이며 어떤 경우 쓰이나요?

위에서 IDS를 설명할 때 One-Armed 형태라는 것을 말하였다. One-Armed는 실제 서비스에 영향없이 구성이 가능하다.

Sniffer Policy란 이런 One-Armed형태의 IDS를 구성하기 위한 기능으로 Fortigate의 특정 인터페이스를 one-armed 모드로 변경하고 해당 인터페이스에 Sniffer Policy를 설정하게 되면 Fortigate가 가지고 있는 UTM기능을 이용하여 IDS를 구현 할 수 있다.

20. One Arm 구성이란 무엇이며 어떤 경우 쓰이나요?

- One-Armed 구성이란 아래 그림과 같이 Inline 구성이 아닌 한 쪽 라인으로 연결되는 구성을 말한다. 일반적으로 IDS, Proxy서버 등을 구현 할 때 사용하고, 실트래픽을 Redirection 시키거나 미러링하여 해당 장비로 트래픽을 흘리도록 한다.
  Fortigate의 경우 스위치의 port 미러링 이나 mirror TAP을 이용하여 IDS를 구현 할 때 사용한다.



21. 프로토콜 옵션에서 각각의 프로토콜에 대한 설명을 해주세요

HTTP : 웹서버와 클라이언트가 상호 통신하기 위해 사용하는 하이퍼텍스트 전송 규약(일반적으로 80port 사용)
HTTPS : 암호화된 HTTP, SSL이라 불리며 443port 사용
FTP : 인터넷상에서 컴퓨터 사이의 파일을 전달하는 데 사용되는 프로토콜, 21port사용
FTPS : FTP over SSL/TLS'를 가리키며 FTP 패킷을 SSL/TLS로 암호화된 패킷 통신을 하는 프로토콜, 990port사용
IMAP : 인터넷 메일 서버에서, 메일을 읽기 위한 인터넷 표준 통신 프로토콜. POP3보다도 유연하고 뛰어난 성능을 가진다. 143port 사용
POP3 : 메일 클라이언트가 메일을 사용자 자신의 PC로 다운로드할 수 있도록 해주는 프로토콜 ,110port 사용
SMTP : 인터넷에서 전자우편(E-mail)을 보낼 때 이용하게 되는 표준 통신 프로토콜, 25port 사용
NMTP : 인터넷 상의 뉴스 서버 간에 뉴스를 주고받기 위한 역할을 하는 프로토콜. 119port 사용
IMAPS : 암호화된 IMAP , 993port 사용
POP3S : 암호화된 POP3 , 995port 사용
SMTPS : 암호화된 SMTP , 465port 사용
IM : 인터넷을 통해 쪽지, 파일, 자료들을 실시간 전송할 수 있는 서비스로 채팅이나 전화와 마찬가지로 실시간으로 의사소통이 가능하다.

22. 세션은 어떻게 생성되나요?

- 데이터 통신에서 세션이란, 데이터 송신측과 수신측과의 논리적인 연결을 가리킨다. 보통 TCP 통신을 말하지만, Stateful Inspection 방식의 방화벽 처럼 세션을 관리하는 장비에서는 UDP나 ICMP까지 세션테이블에 나타낸다.
  Fortigate는 처음 패킷이 지나갈 때 세션테이블을 생성하고 각 프로토콜(TCP, UDP, ICMP)의 현재 상태를 모니터링 한다.

23. 주소에서 FQDN, Geography(지리) 방식이 지원된다고 하는데 이것은 어떤 건가요?

- Fortigate에서 주소 객체를 생성하는 방법은 IP Address, FQDN, Geography 세가지 이다.
  IP Address 는 대부분의 방화벽에서 주소를 정의하는 방법으로 실제 IP 주소를 정의 하는 방식이다.
  FQDN(Fully Qualified Domain Name)은 주소 정의를 도메인으로 등록하여 Fortigate에 정의된 DNS로부터 해당 URL의 IP정보를 가져오는 방식으로 URL의 IP가 유동적인 경우 사용한다.
  Geography 방식은 Fortinet사에서 국가별로 할당 되어진 IP 대역들을 미리 정의하여 사용하는 방식으로 특정 국가에 대한 정책을 설정할 경우 사용한다.

24. 서비스 기본정의, 사용자정의, 그룹 설정 서비스는 어떻게 다른가요?

- 서비스 기본정의 : 방화벽 정책 설정 시 많이 쓰이는 Port 들로 미리 정의 된 Service 객체 이다.
  사용자 정의 : 기본정의에서 없는 Service 객체의 경우 사용자가 직접 만들어 객체를 만들 수 있는데, 이렇게 사용자에 의해 정의된 Service 객체를 말한다.
  그룹 설정 : 서비스 기본정의 및 사용자 정의 에서 만들어 놓은 Service 객체들을 그룹으로 묶어서 사용할 수 있도록 하는 집합 객체 이다.

서비스 기본정의

이름	내용
AFS3	TCP/7000-7009 UDP/7000-7009
AH	IP/51
ANY	ALL
AOL	TCP/5190-5194
BGP	TCP/179
CVSPSERVER	TCP/2401 UDP/2401

서비스 사용자정의

Create New 편집 Delete

	서비스 이름	내용
☐	4Team_NAS	TCP/1-65535:80,1-65535:9090,1-65535:20-21
☐	6660	TCP/1-65535:6660,1-65535:6610,1-65535:6620,1-65535:6630,1-65535:6640,1-65535:6650
☐	9105	TCP/1-65535:9105

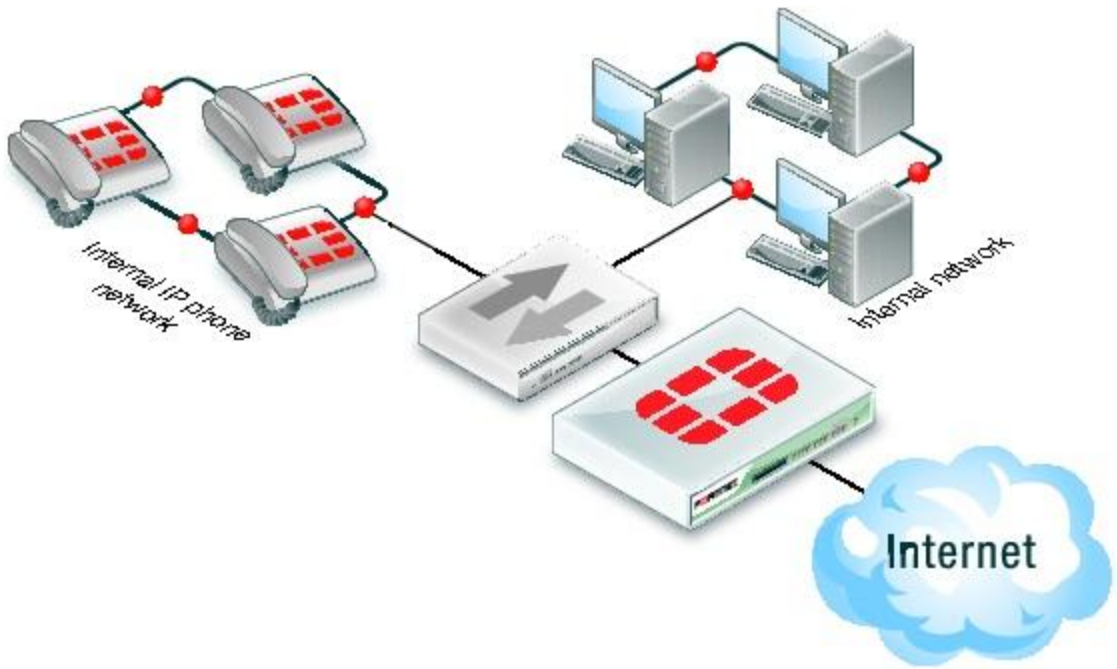
서비스 그룹

Create New 편집 Delete

	그룹 이름	멤버
☐	Helpdesk	HTTP, MS_SQL
☐	Mail_Service	DNS, HTTPS, POP3, SMTP
☐	SpamOut	DNS, HTTP, HTTPS, NNTP, POP3, SMTP, Watcher_Service

25. 트래픽 쉐이퍼란 무엇인가요?

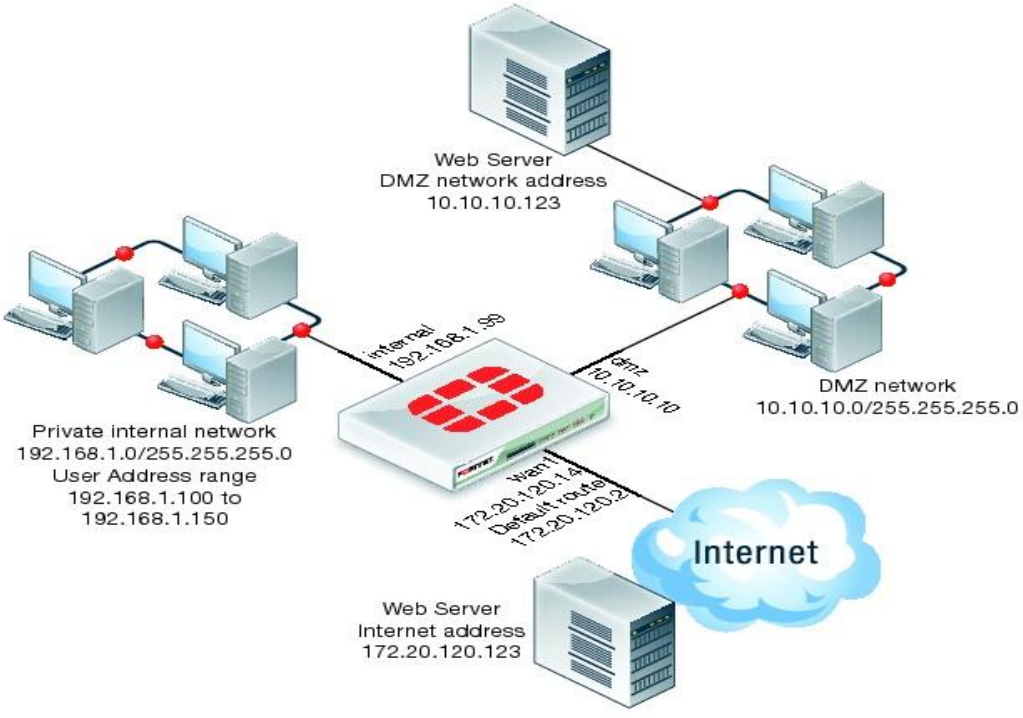
- QoS(Quality of Service)와 동일한 뜻으로 보면 된다. Fortigate의 Traffic Shaper 기능은 정책을 기반으로 해당 정책의 트래픽 Bandwidth의 보장(Guarantee) 대역 및 최대(Maximum) 대역을 정의 할 수 있고, 이러한 대역폭 보장을 통하여 중요한 서비스에 대한 품질을 보장 할 수 있다.



26. 가상주소란 무엇인가요?

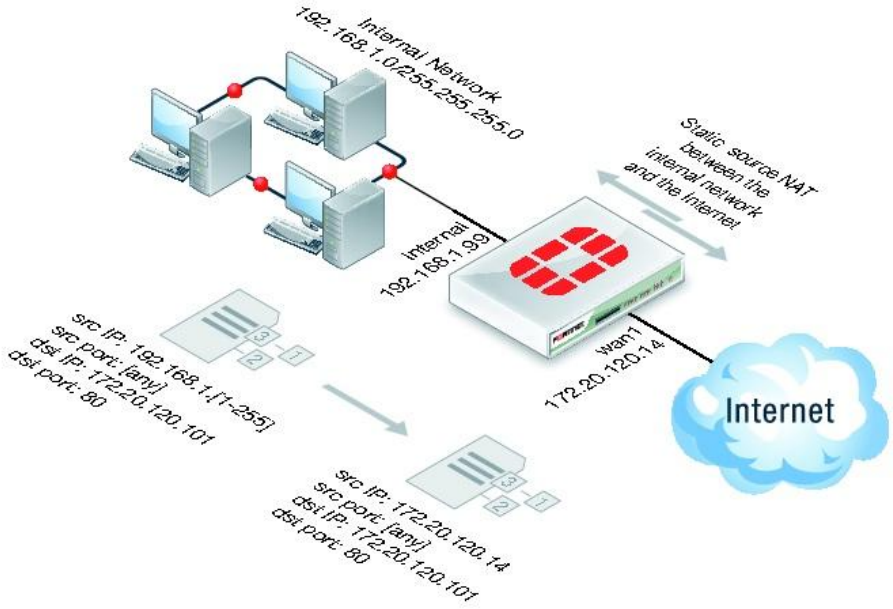
- Fortigate에서 가상주소(Virtual IP)란 사설 IP로 구성되어 있는 내부 시스템을 외부 네트워크에서 접속이 가능하도록 내부 사설 IP와 외부 공인 IP를 1:1로 맵핑되거나, 포트포워딩 되어진 주소 객체 이다.

Protecting a web server on a DMZ network



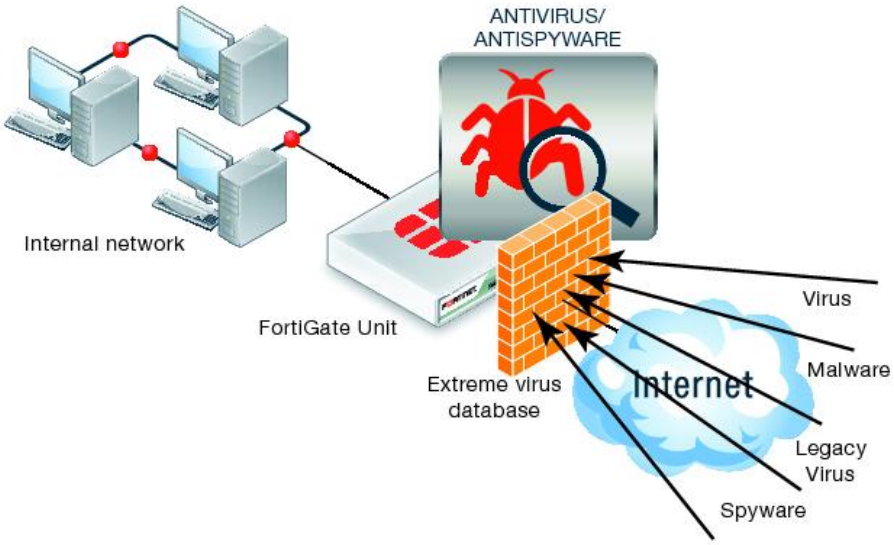
27. NAT란 무엇인가요?

- NAT (Network Address Translation)란 사설 IP주소를 공인 IP 주소로 바꿔주는데 사용하는 통신망의 주소 변환방식으로 Static(1:1) NAT, PAT(1:N), Dynamic(N:M) NAT로 구분 된다.
  - 1:1 NAT : port변환이 일어나지 않고 사설IP와 공인IP를 1:1로 매핑한다.
  - 1:N NAT : 공유기나 방화벽에서 일반적으로 사용되며 내부의 사설IP 다수를 공인IP 하나로 변환한다.
  - N:M NAT - IP Pool을 사용하여 내부사설IP 다수가 여러 개의 공인IP로 변환되어 나간다. 단, 내부사설IP별로 밸런싱됨.



28. 바이러스 탐지는 어떻게 하나요?

- Fortigate의 AntiVirus Scanning은 바이러스, 웜, 트로이목마 및 악성코트에 대한 파일을 검사한다. AntiVirus Scan 엔진은 바이러스 패턴 DB를 사용하여 감염 여부를 식별하는데, 정밀한 검사를 하기 위해서는 검사 대상의 전체 파일이 필요하다. 그래서 AntiVirus Proxy는 패킷이 도착하는대로 버퍼로 전송하고 전송이 완료되면, Virus Scanner가 파일을 검사한다. 감염되지 않은 파일이면 목적지로 전송되고, 감염이 된 파일이면 대체 메시지를 사용자에게 보낸다.

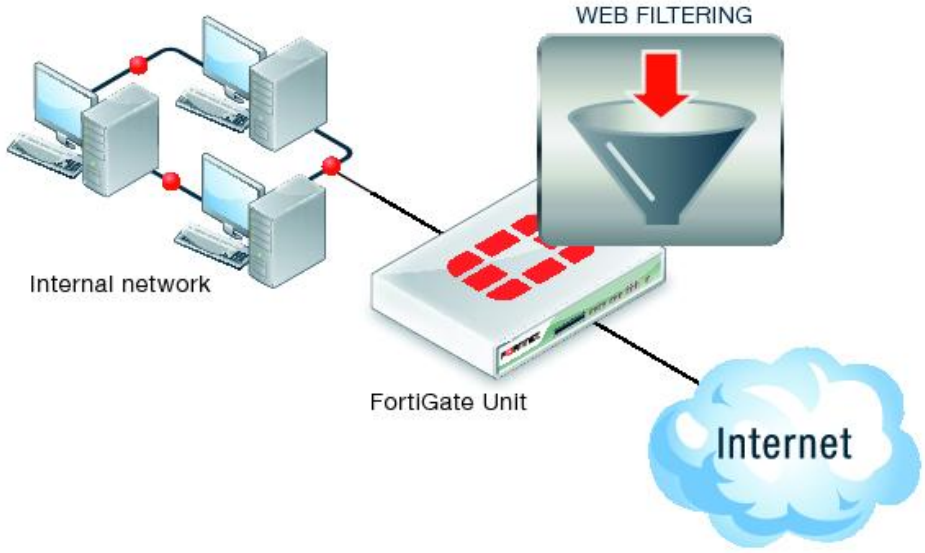


29. 웹 필터란 무엇인가요?

웹 필터란 인터넷 사용자가 접속 가능한 웹 페이지를 제어하는 방법으로 웹 응용프로그램이 확산되면서 보안 관리 시스템의 핵심 구성 요소가 되고 있다.

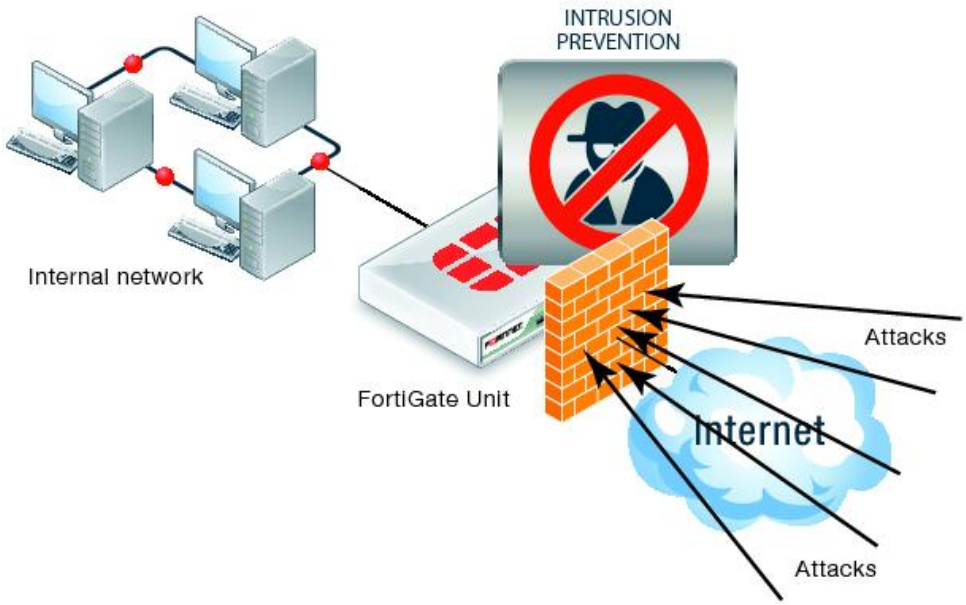
Fortigate의 웹 필터 방식은 다음과 같다.

1. URL Filter : 제어할 URL 리스트를 직접 등록하여 웹페이지를 차단 또는 예외처리 한다.
2. FortiGuard Web Filter : Fortiguard (분류된 웹사이트 DB)서비스(유료)를 이용하여 사이트의 목적 및 등급 별로 자동 차단이 가능하다.
3. Web Content Filter : 특정 단어나 패턴을 등록하여 이것을 포함하는 웹페이지를 차단한다.



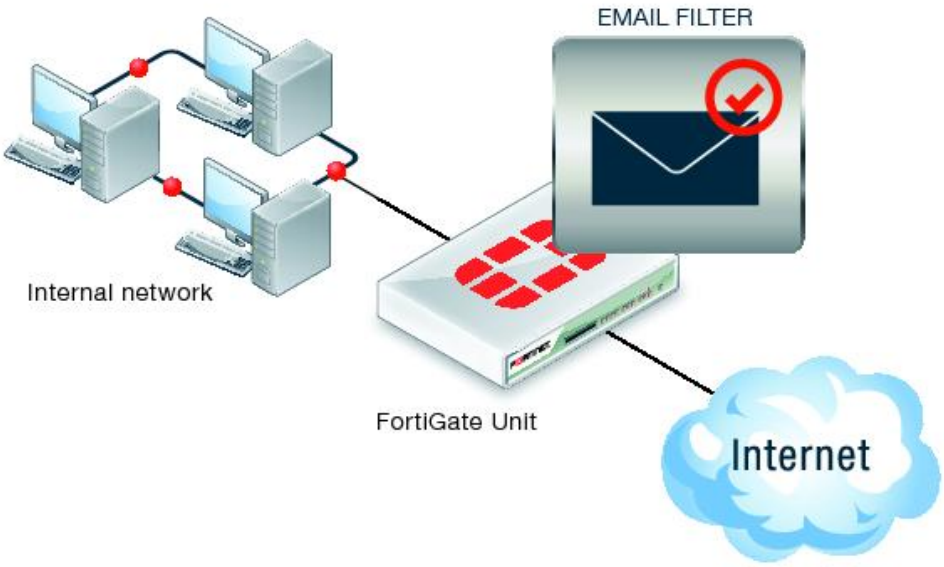
30. 침입탐지는 어떻게 하나요?

Fortigate에서 침입 탐지를 하는 방법은 Anomaly-based defense와 Signature-based defense 두 가지를 가지고 있다.
Anomaly-based 방식은 DoS 공격과 같이 네트워크 트래픽 자체가 위협이 되는 경우에 사용되고 특정 임계값을 설정 하여 차단 한다.
Signature-based 방식은 알려진 공격 또는 취약점에 대해 사용된다. 이런 경우 공격자는 특정 명령, 변수, 시퀀스 등을 이용하여 특정 호스트와 통신을 하고 원하는 목적을 달성하기 위해 노력한다. Fortigate는 이러한 패턴들을 정의해 놓고 패턴이 감지가 되면 공격을 차단 한다.



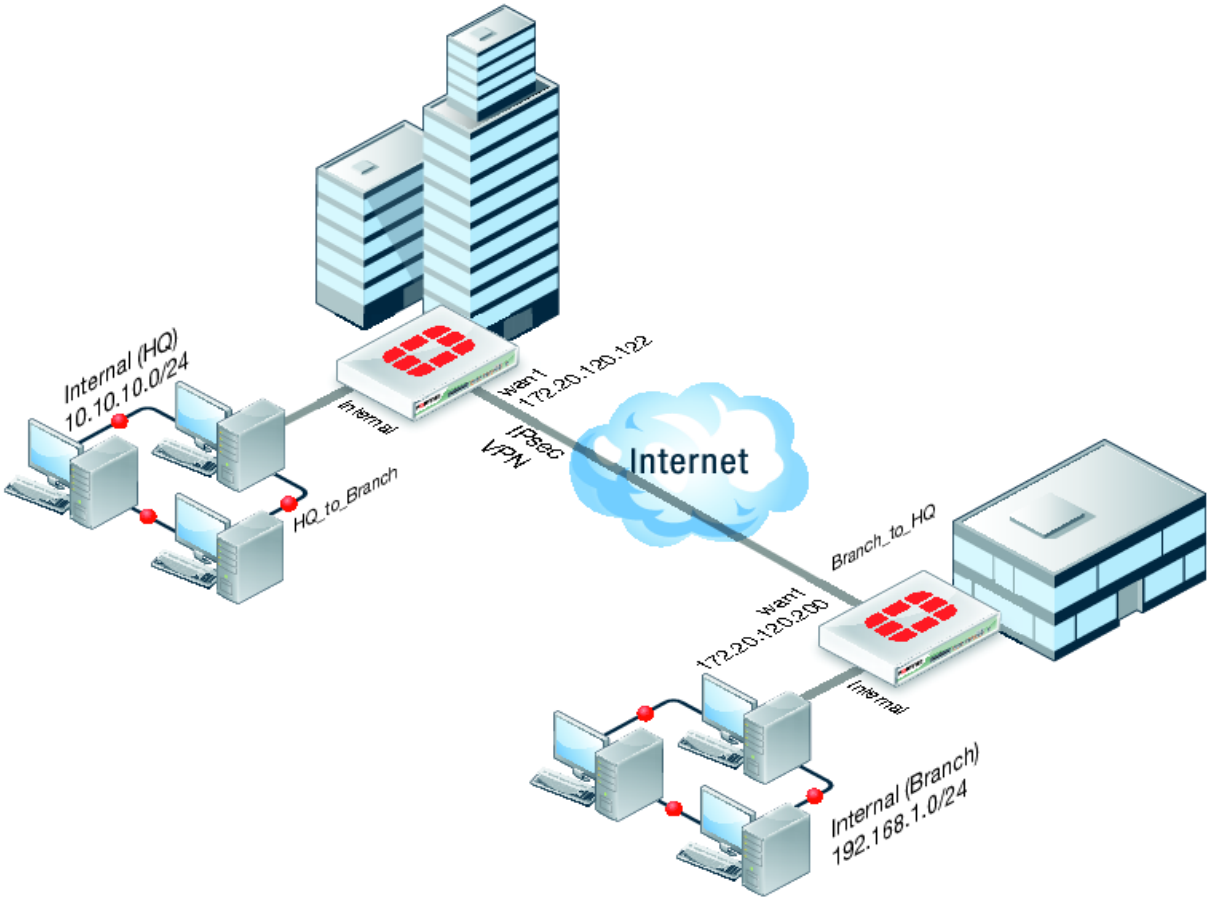
31. 이메일 필터는 어떻게 하나요?

- Fortigate는 다양한 방법의 이메일 필터링 기능을 제공한다. 메일 제목이나 본문의 특정단어를 검사하는 Banned Word 방식, 스팸 메일을 보내는 IP주소나 이메일 주소를 등록하여 차단 할 수 도 있고, Fortiguard의 AntiSpam 서비스(유료)를 이용하여 차단을 할 수 도 있다.



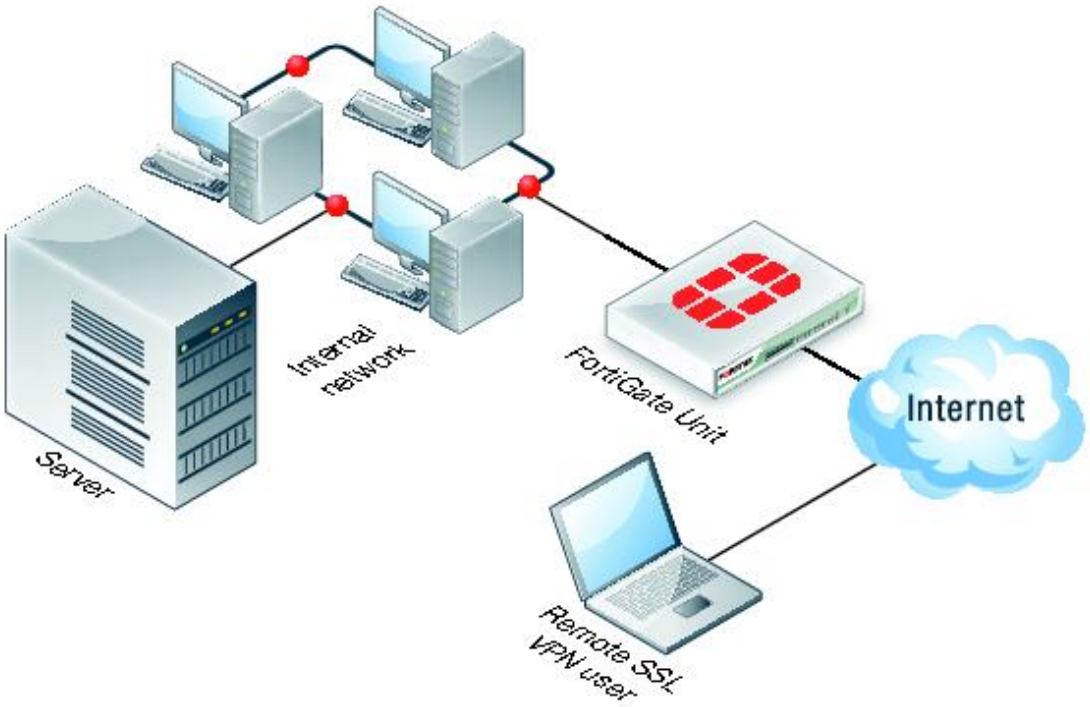
32. VPN에서 IPSec이란 무엇인가요?

IPSec(Internet Protocol Security)이란 단순한 데이터 전송만을 하기 위한 IP(Internet Protocol)의 보안 문제점을 해결하기 위해 만들어 졌다. 네트워크 계층인 인터넷 프로토콜에서 보안성을 제공해 주는 표준화된 기술로 데이터 송신자의 인증을 허용하는 인증 헤더(AH)와 송신자의 인증 및 데이터 암호화를 함께 지원하는 ESP(Encapsulating Security Payload) 등을 사용한다.
이를 기반으로 VPN을 구현 한 것을 IPSec VPN이라고 한다.



33. VPN에서 SSL이란 무엇인가요?

SSL(Secure Sockets Layer)이란 웹브라우저와 서버 간의 통신에서 정보를 암호화함으로써 도중에 해킹을 통해 정보가 유출되더라도 정보의 내용을 보호할 수 있는 기능을 갖춘 보안 프로토콜이다. 이를 기반으로 한 SSL-VPN은 원격지에서 인터넷으로 내부 시스템 자원을 안전하게 사용할 수 있도록 해준다. 또한 웹브라우저 만 있으면 VPN연결이 가능하기 때문에 사용자들에게 큰 편의성을 제공한다.



34. 현재 설정된 정보를 백업 받을 수 있나요?

Fortigate는 설정(Configuration)정보를 백업하는 기능을 제공한다. 백업은 로컬 PC, USB 메모리, FTP나 TFTP 등을 이용하여 저장 할 수 있다. (FTP, TFTP의 경우는 CLI로만 가능)
GUI에서 백업을 받을 때 password를 입력하면 추후 복원 시 password를 재 입력하여야 한다.

35. TCP와 UDP는 무엇인가요?

TCP (Transmission Control Protocol)

TCP[티씨피]는 인터넷상의 컴퓨터들 사이에서 데이터를 메시지의 형태로 보내기 위해 IP와 함께 사용되는 프로토콜이다. IP가 실제로 데이터의 배달처리를 관장하는 동안, TCP는 데이터 패킷을 추적 관리한다 (메시지는 인터넷 내에서 효율적인 라우팅을 하기 위해 여러 개의 작은 조각으로 나뉘어지는데, 이것을 패킷이라고 부른다).
예를 들면, HTML 파일이 웹 서버로부터 사용자에게 보내질 때, 서버 내에 있는 TCP 프로그램 계층은 파일을 여러 개의 패킷들로 나누고, 패킷 번호를 붙인 다음, IP 프로그램 계층으로 보낸다. 각 패킷이 동일한 수신지 주소(IP주소)를 가지고 있더라도, 패킷들은 네트웍의 서로 다른 경로를 통해 전송될 수 있다. 다른 한쪽 편(사용자 컴퓨터 내의 클라이언트 프로그램)에 있는 TCP는, 각 패킷들을 재조립하고, 사용자에게 하나의 완전한 파일로 보낼 수 있을 때까지 기다린다.
TCP는 연결지향 프로토콜이라고 알려져 있는데, 이것은 메시지들이 각단의 응용 프로그램들에 의해 교환되는 시간동안 연결이 확립되고 유지되는 것을 의미한다. TCP는 IP가 처리할 수 있도록 메시지를 여러 개의 패킷들로 확실히 나누고, 반대편에서는 완전한 메시지로 패킷들을 재조립할 책임이 있다. OSI 통신모델에서, TCP는 4계층인 트랜스포트 계층에 속한다.

35. TCP와 UDP는 무엇인가요?

UDP (User Datagram Protocol)

UDP[유디피]는 IP를 사용하는 네트웍 내에서 컴퓨터들 간에 메시지들이 교환될 때 제한된 서비스만을 제공하는 통신 프로토콜이다. UDP는 TCP의 대안이며, IP와 함께 쓰일 때에는 UDP/IP라고 표현하기도 한다. TCP와 마찬가지로 UDP도 한 컴퓨터에서 다른 컴퓨터로 데이터그램 이라고 불리는 실제 데이터 단위를 받기 위해 IP를 사용한다. 그러나 UDP는 TCP와는 달리, 메시지를 패킷(데이터그램)으로 나누고, 반대편에서 재조립하는 등의 서비스는 제공하지 않으며, 특히 도착하는 데이터 패킷들의 순서를 제공하지 않는다. 이 말은 UDP를 사용하는 응용프로그램은, 전체 메시지가 올바른 순서로 도착했는지에 대해 확인할 수 있어야 한다는 것을 의미한다. 교환 해야 할 데이터가 매우 적은(그러므로 재 조립 해야 할 메시지도 매우 적은) 네트워크 응용프로그램들은 처리시간 단축을 위해 TCP 보다 UDP를 더 좋아할 수 있다. 일례로 TFTP는 TCP 대신에 UDP를 사용한다.

UDP는 IP 계층에서 제공되지 않는 두 개의 서비스를 제공하는데, 하나는 다른 사용자 요청을 구분하기 위한 포트 번호와, 도착한 데이터의 손상여부를 확인하기 위한 체크섬 기능이다.

OSI 통신 모델에서, UDP는 TCP와 마찬가지로 4계층인 트랜스포트 계층에 속한다.

36. 포트 통신이란 무엇인가요?

포트통신이란?

OSI 7Layer 중 4계층에서 이루어 지는 통신을 말한다.
전송 계층(Transport Layer)
- 통신 양단간에 정확한 데이터 전송을 제공
- OSI 7계층의 하위 3계층과 상위 3계층의 인터페이스 역할
- 시스템 간의 에러 제어와 흐름 제어 등의 종단간 신뢰성을 제어
- **TCP**, UDP 프로토콜 등
- 대표적인 4Layer 장비로는 L4 Switch 가 있다.

37. 포트는 몇 번까지 있나요?

인터넷의 전송 제어 프로토콜(TCP)이나 사용자 데이터그램 프로토콜(UDP)에서 애플리케이션이 상호 통신을 위해 사용하는 번호, 각 포트는 번호로 구별되며 이 번호를 포트 번호라고 한다. 포트번호는 0번 부터 65535번 내에서 정의되며 크게 세 종류로 분류 가능하다.

Well-Known Port Numbers	0~1023	기정 포트 번호 (일반적으로 사용하는)
Registered Port Numbers	1024~49151	회사용으로 등록된 포트 번호
Dynamic Port Numbers	49152~65535	동적 포트 번호 (자유롭게 사용 가능)

38. Well Known 포트란 무엇이며, 어떤 것들이 있나요?

- Well Known Ports

TCP/IP 네트웍에서 포트 번호는, 들어오는 트래픽을 컴퓨터 내에서 실행되고 있는 적절한 프로그램에 분배시키기 위해 할당되는 숫자를 말한다. 이것은 물리적인 플러그나 소켓이 아니며, 다만 논리적인 할당일 뿐이다. 포트번호는 Well Known Port와, Registered Port 그리고, Dynamic and/or Private Port 등 3가지 범주로 나뉘는데, Well Known Port에는 0~1023까지의 숫자가, Registered Port에는 1024~49151까지의 숫자가, 그리고 Dynamic and/or Private Port에는 49152~65535까지의 숫자가 각각 사용된다. 예를 들어, 월드와이드웹 트래픽, 즉 HTTP 패킷들에는 대체로 80번 포트가, FTP 전송에는 20번 포트가, 그리고 Kerberos 인증에는 88번 포트가 각각 할당된다.

39. NAT모드와 TP모드는 무엇이며, 서로 어떻게 다른가요?

NAT [Network Address Translation]

NAT Mode : NAT를 사용하는 목적에는 2가지가 있는데, 첫째는 인터넷의 공인 IP주소를 절약할 수 있다는 점이고 둘째는 인터넷이란 공공망과 연결되는 사용자들의 고유한 사설망을 침입자들로부터 보호할 수 있다는 점이다.
인터넷의 공인 IP주소는 한정되어 있기 때문에 가급적 이를 공유할 수 있도록 하는 것이 필요한데 NAT를 이용하면 사설 IP주소를 사용하면서 이를 공인 IP주소와 상호 변환 할 수 있도록 하여 공인 IP주소를 다수가 함께 사용할 수 있도록 함으로써 이를 절약할 수 있는 것이다.
공개된 인터넷과 사설망 사이에 방화벽(Firewall)을 설치하여 외부 공격으로부터 사용자의 통신망을 보호하는 기본적인 수단으로 활용할 수 있다. 이때 외부 통신망 즉 인터넷망과 연결하는 장비인 라우터에 NAT를 설정할 경우 라우터는 자신에게 할당된 공인 IP주소만 외부로 알려지게 하고, 내부에서는 사설 IP주소만 사용하도록 하여 필요시에 이를 서로 변환시켜 준다. 따라서 외부 침입자가 공격하기 위해서는 사설망의 내부 사설 IP주소를 알아야 하기 때문에 공격이 불가능해지므로 내부 네트워크를 보호할 수 있다.

TP [Transparent]

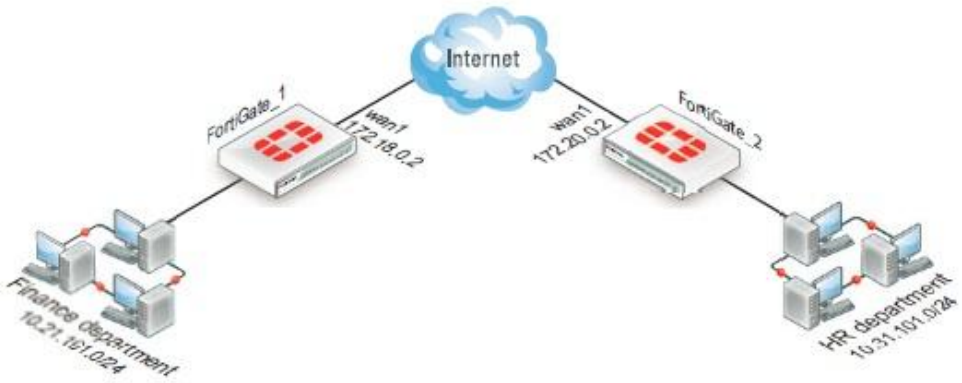
Transparent mode : 스위치나 브릿지같은 Layer2 장비처럼 목적지 MAC을 가지고 Ethernet Frame를 포워딩한다.Routed Mode와는 틀리게 방화벽의 인터페이스에 연결된 네트워크주소는 틀린다. 정확히 말하면 방화벽에 입력하는 주소는 단지 관리를 위한것이지 Ethernet Frame의 흐름과는 관련이 없다.

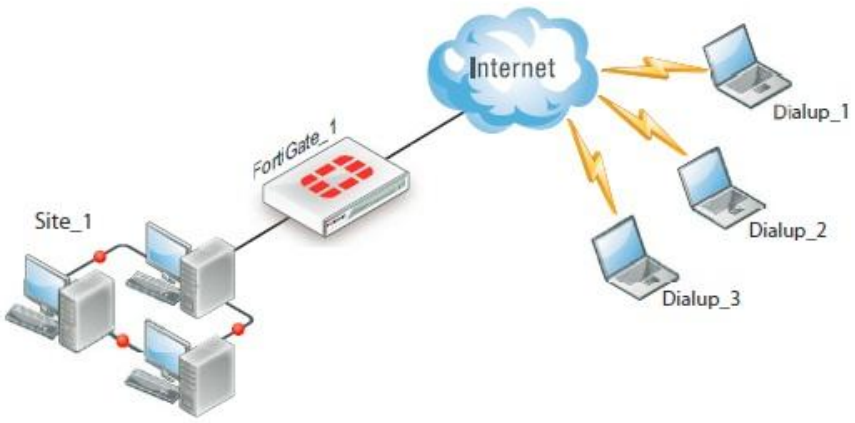
두가지 Mode 는 L2 layer 기반으로 한 운용방식인지 L3 layer 기반으로 한 운용방식인지의 차이점을 가진다.

40. VPN Tunnel 연결 시 공인 고정IP가 꼭 필요한가요?

VPN을 구성하려면 상대쪽 VPN 게이트웨이의 IP주소를 알아야 해당 IP로 터널을 맺기 위한 협상을 시도할 수 있다. 양쪽이 모두 유동IP일 경우 두 곳의 IP가 모두 변경이 되면 서로 협상을 시도 할 수 없기 때문에 어느 한 쪽은 고정 IP를 사용하기를 권장한다.

양쪽이 유동 회선이라도 DDNS를 이용하여 구성이 가능하나 많이 사용이 되고 있지는 않다.





41. PFS(Perfect Forward Secrecy)란 무엇인가요?

- 암호화 용어로써 하나의 세션키가 공개되어진 경우에도 다른 세션키는 여전히 안전할 수 있는 성질을 말한다.

42. DH그룹이란 무엇인가요?

- 키 교환 프로토콜로 알려진 Diffie-Hellman은 이산대수의 어려움에 기반으로 하는 알고리즘이다. 공개키 암호에 대한 시초로 광범위하게 인정되고 있으며 1979년경에 발표되었다.

43. Quick 모드 기능이란 무엇인가요?

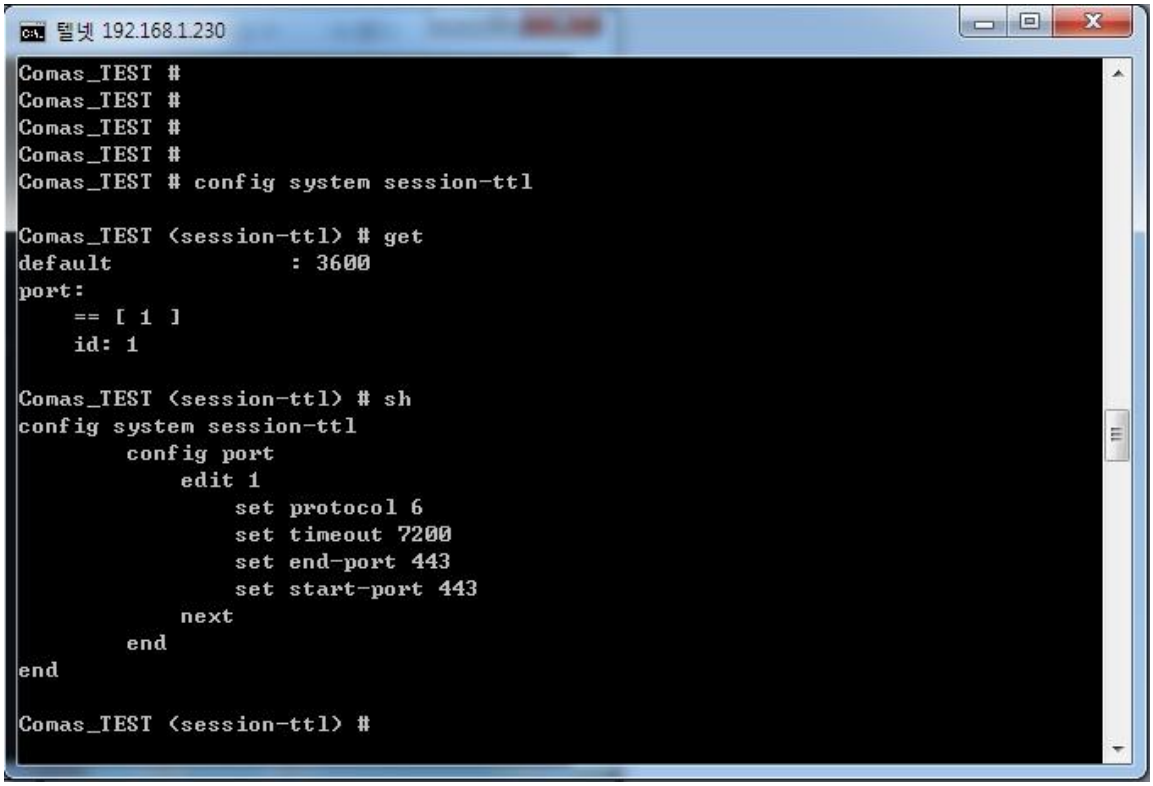
- Quick Mode(Phase 2)는 IPSec Packet(AH, ESP등)에 적용될 암호화 방식과 세션 키를 결정하는 절차로서 IPSec SA 설정 절차라고 한다. 이 과정은 Phase 1과 달리 3쌍이 아닌 3개의 메시지를 통해서 구현이 되고 송수신 되는 모든 IKE 패킷들은 Phase 1에서 설정한 IKE용 SA에 의해 보호된다.

44. Dial UP IPSEC이란 무엇인가요?

- 고정IP회선으로 운영되는 센터 장비에서 유동 회선 사용자에 대한 VPN터널을 구현하기 위한 방법이다. 상대쪽의 VPN 게이트웨이의 IP주소가 유동적으로 변경이 되는 경우에 사용한다. 센터 장비에서는 상대의 IP 주소를 알 수 없기 때문에 VPN터널을 맺기 위한 요청도 Branch 장비 또는 VPN 클라이언트 사용자 쪽에서 먼저 요청을 하게 된다.

45. 세션유지시간은 얼마나 되나요?

- Fortigate 의 Default 세션 유지시간 값은 3600초 이다.
  Default 및 특정 포트에 대한 유지시간 변경 가능하다.



46. SSL VPN의 기본 인증 유휴 초과 시간은 얼마나 되나요?

- Fortigate 의 Default SSL-VPN 세션유지시간 값은 300초 이다.
  해당 값은 변경이 가능 하다.

47. Web Mode와 Tunnel Mode는 무엇이며 각 Mode는 어떻게 다른가요?

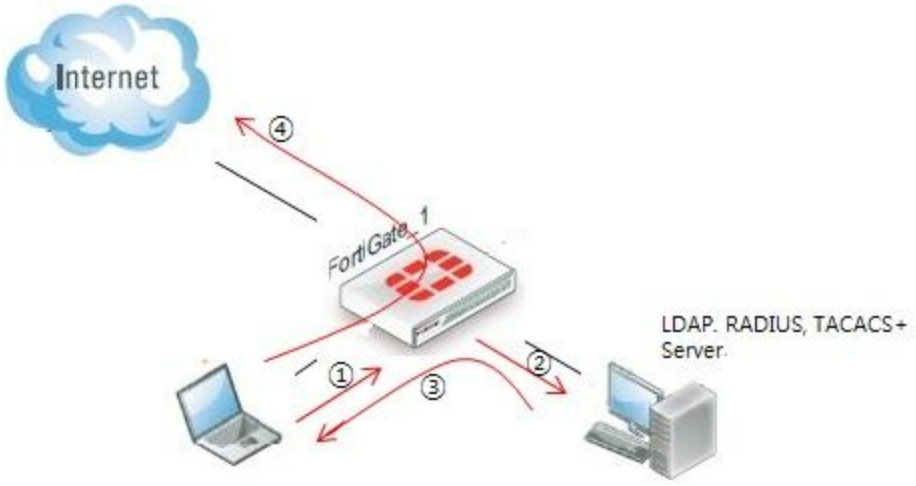
- Fortigate에서 SSL-VPN 접속 방법으로 Web Mode와 Tunnel Mode를 지원 한다.
  Web Mode는 Fortigate를 Proxy로 이용하여 내부 서버에 접근하는 방식이다. SSL-VPN 접속 페이지에 즐겨찾기 형식으로 내부 서버에 접속하는 메뉴를 제공하고 이를 통하여 내부 서버에 접속을 한다. Proxy로 동작을 하기 때문에 서비스 접근에 많은 제약이 있다.
  반면 Tunnel Mode는 VPN사용자와 Fortigate간에 VPN 터널을 생성하고 실제 사용자가 직접 내부 서버로 접근을 하는 방식이다. 실제 사용자가 접속을 하기 때문에 서비스 접근에 대한 제약이 없다.

48. Split 터널 기능은 무엇인가요?

- SSL-VPN이 연결된 사용자는 VPN Tunnel 을 통해서 이동하는 암호화 된 트래픽과 그 외의 일반적인 Traffic 이 움직이는 경로가 다르다. 실제 SSL-VPN이 연결된 PC의 라우팅 테이블을 확인하면 SSL-VPN 접속 대역만 VPN 쪽으로 전송하도록 라우팅 처리 되어있다. 이런 경우 인터넷과 VPN이 동시에 사용이 가능하게 되는데, 사용자 PC를 통한 보안 취약점이 발생한다. 이러한 문제점을 해결하기 위해 모든 traffic이 연결된 Tunnel 을 통해 움직이게 하는 기능이 Split 터널 기능이다.

49. 사용자 계정의 패스워드를 Local 인증을 하지 않고 LDAP, RADIUS, TACACS+등의 인증서버와 연동 설정이 가능하다고 하는데, 여기서 LDAP, RADIUS, TACACS+란 무엇이며 어떻게 연동을 하나요?

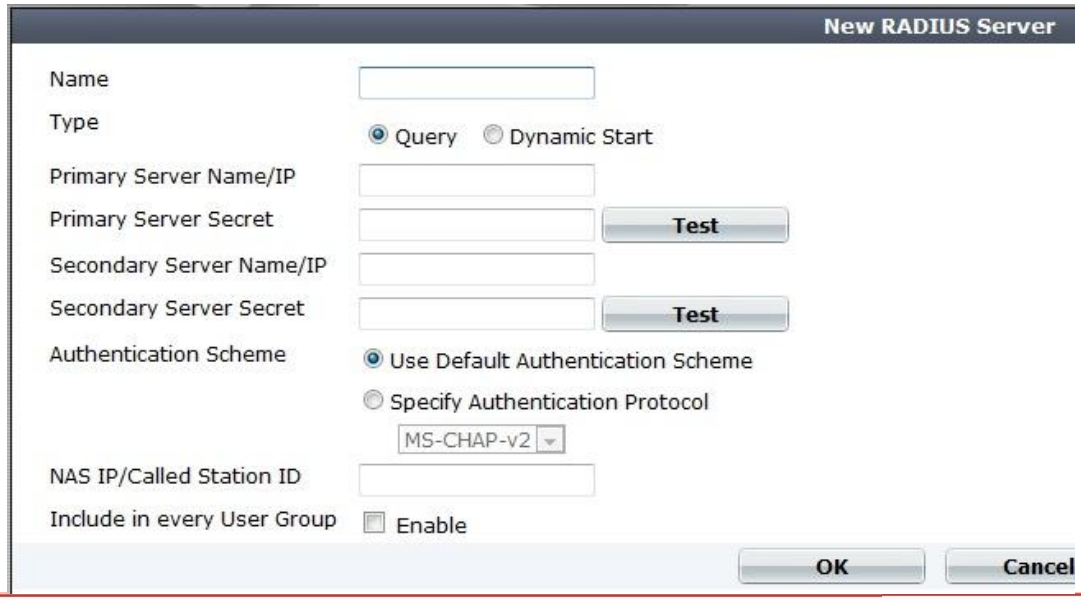
- LDAP, RADIUS, TACACS+ 사용자의 식별과 인증을 수행하는 서버이다.
  Fortigate에 Remote 인증 서버를 등록하면 User 객체로 사용이 가능하고, Local User 객체와 마찬가지로 사용자 인증 정책에 적용이 가능하다. Fortigate로 인증요청이 들어오면 해당 식별자를 원격 인증 서버로 보내어 인증을 수행하게 된다.



49. 사용자 계정의 패스워드를 Local 인증을 하지 않고 LDAP, RADIUS, TACACS+등의 인증서버와 연동 설정이 가능하다고 하는데, 여기서 LDAP, RADIUS, TACACS+란 무엇이며 어떻게 연동을 하나요?

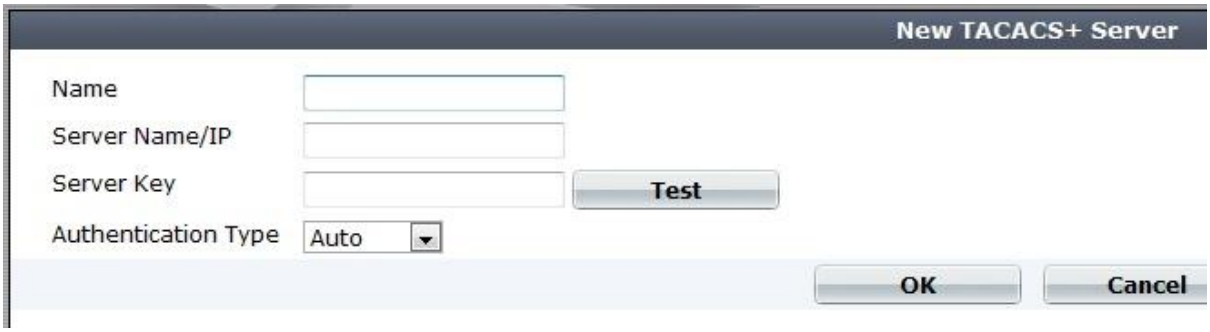
LDAP 서버

RADIUS 서버



49. 사용자 계정의 패스워드를 Local 인증을 하지 않고 LDAP, RADIUS, TACACS+등의 인증서버와 연동 설정이 가능하다고 하는데, 여기서 LDAP, RADIUS, TACACS+란 무엇이며 어떻게 연동을 하나요?

- TACACS+ 서버



- 연동할 서버의 설정을 확인하여 위의 그림과 같은 정보를 입력하면 된다.

50. 포티넷 장비가 가지고 있는 Virus Database에서 Regular Virus Database와 Extended Virus Database는 어떻게 다른가요?

- Fortinet Virus Database는 4.0 MR3 이상에서 다음 세가지로 분류하여 지원한다.

Normal(Regular)

현재 FortiGuard 에서 확인한 세계적으로 위험도가 큰 Virus를 포함 한다. 이 Database는 Fortigate 에서 지원하는 기본 Database 이다.

Extended

현재는 출현 빈도가 낮은 Virus 뿐만 아니라 Normal DB도 포함한다.

Extreme

위 두 DB 및 Zoo Virus까지 추가로 확장한 DB가 포함한다. Zoo Virus는 이미 오래 전부터 알려져 있던 Virus이기 때문에 출현 빈도가 매우 낮다.

51. Grayware 사용 유무 활성화를 적용할 수 있는데, Grayware란 무엇이며 활성화 유무에 따라 어떻게 달라지나요?

그레이웨어(Grayware)

그레이웨어(Grayware)란 사용자의 허가 또는 인지 없이 컴퓨터에 몰래 설치되어 특정 정보를 추적해서 외부로 보고하는 스파이웨어뿐 아니라 애드웨어, 또 인터넷 뱅킹 사고의 주범인 키로거(Keylogger), 백도어, 루트킷, BHO(Browser Help Object), 봇 등을 모두 포괄하는 단어이다. 그레이웨어는 대부분 설치에 앞서 사용자 동의를 구하여 합법적인 프로그램으로 위장하고 있다.
예를 들어 인터넷 사이트에서 PC 유틸리티나 게임 등 무료로 다운로드하여 설치할 때 자동으로 악성 프로그램이 함께 다운로드된다고 가정해도 된다. 결국 악성 코드인지 정상 코드인지 분간이 되지 않는 중간이기에 그레이웨어라고 한다.

Fortigate 그레이웨어 활성화를 하게 되면 그레이웨어로 분류된 프로그램은 차단된다.

52. URL 필터란 무엇인가요?

URL 필터란 Web Filter 방식의 하나로 URL 리스트를 정의 하여 웹페이지에 대한 사용자의 접속을 제어한다.

URL 필터의 Action 은 다음 세가지 이다.

- Block

사용자가 접근하려는 모든 URL에 패턴이 일치하면 접근거부 된다.

- Allow

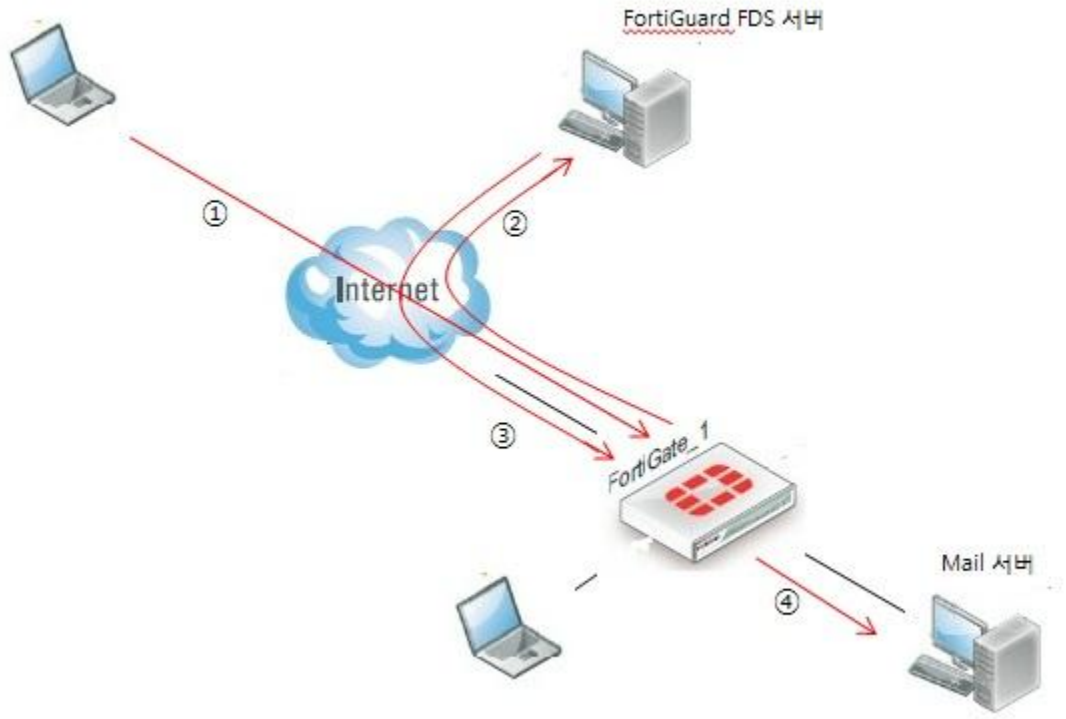
사용자가 접근하려는 URL에 패턴이 허용되어 있으면 접근허용 되지만 다음사항을 참조한다.
FortiGuard 웹필터, 웹 콘텐츠 필터, 웹 스크립트 필터 및 Virus 백신 검색 등을 참조 후에 정상적일 경우 접근이 허용된다.

- Exempt

사용자가 접근하려는 URL에 대해 모든 참조사항을 확인하지 않고 접근을 허용한다.

53. 안티스팸은 어떻게 동작하나요?

- 안티스팸은 Mail 서버 앞단에 구성되며 외부에서 Mail이 들어오게 되면 ①으로 패킷이 흐른다. 포티에서 패킷을 받아 ②번 FDS 서버로 질의하게 된다. Spam이 아닌 정상 Mail 이라면 포티자체 DB를 참조 후에 정상 Mail은 서버로 넘겨주고 Spam 이라면 설정값에 따라 처리 된다.



54. E-Mail 전송 프로토콜에 IMAP, SMTP, POP3가 있는데 각각은 어떻게 다른가요?

- IMAP [internet messaging access protocol]

클라이언트가 메일 서버에서 메일을 읽기 위한 인터넷 표준 프로토콜의 한 가지로서, TCP/IP의 상위 프로토콜이며 최신 버전인 IMAP4는 RFC2060으로 규정되어 있다. POP3보다도 유연하고 뛰어나다고 할 수 있다.

서버측에 메일 박스를 둘 수 있다는 것과 메일의 헤드만을 읽을 수 있는 것이 특징이다. 클라이언트는 서버의 메일 박스에서 메일을 삭제하지 않고 필요한 메일만 복사할 수 있다. 또 저속 다이얼-업 접속 시에는 헤드만 읽고 판단하여 크기가 큰 메일이나 우선도가 낮은 메일을 나중에 읽거나 삭제할 수 있다. 이러한 특징 때문에 이동 기기 액세스에 적합한 프로토콜이라고 할 수 있다.

- POP3 [Post Office Protocol 3]

메일 클라이언트가 메일을 사용자 자신의 PC로 다운로드할 수 있도록 해주는 프로토콜을 말한다.현재 대부분의 메일서버에서는 POP3을 사용하고 있으며 사용자는 넷스케이프나 아웃룩 익스프레스로 서버에 있는 자신의 메일 수신함을 체크하여 메일을 자신의 컴퓨터로 수신한다. 메일을 수신하는 프로토콜에는 POP3와 IMAP(Internet Message Access Protocol)가 있는데, IMAP은 서버에 직접 접속해 메일을 관리하는데 비해 POP3은 메일서버에 있는 메일을 자신의 컴퓨터로 가져와 관리한다는 차이가 있다.

54. E-Mail 전송 프로토콜에 IMAP, SMTP, POP3가 있는데 각각은 어떻게 다른가요?

SMTP [simple mail transfer protocol]

인터넷에서 전자우편(E-mail)을 보낼 때 이용하게 되는 표준 통신 규약을 말한다.SMTP와 관련된 프로토콜의 표준은 STD와 RFC에서 정해진 것이다. 서버에서 서버로의 프로토콜이며 이외의 다른 여러 프로토콜은 메시지를 접속하기 위해서 사용한다. 이와 관련된 프로토콜을 살펴보면 다음과 같다.

① STD 10/RFC 821:두 컴퓨터 사이의 메일 교환 표준을 정의하며 SMTP 자체에 관한 표준으로 TCP/IP 호스트 사이에서 메일을 전달하는데 사용된다.

② STD 11/RFC 822, RFC1049:RFC 822와 RFC 1049에 포함된 메일 메시지의 형식에 관한 표준을 정의하며 공식적인 프로토콜명은 MAIL이다. RFC822는 메일 헤더 필드의 의미를 기술하고 헤더 필드 집합과 그에 대한 해석을 정의한다. RFC 1049는 평문 아스키 이외의 문서 형식들이 메일 본문에서 어떻게 사용될 수 있는지에 대해 기술하고 있다.

③ RFC 974:DNS(domain name system)을 이용한 메일 경로 배정에 관한 표준을 정의하고 있으며 공식 프로토콜명은 DNS-MX이다.

STD 10/RFC 821에서는 SMTP를 통해 전달되는 데이터는 상위 비트가 0으로 설정된 7비트 아스키 데이터라고 기술하고 있다. 이는 영문텍스트 메시지를 전송하는데는 적합하지만, 비영어권 데이터 또는 비 텍스트 데이터에 대해서는 부적합하다. 이러한 제약을 극복하기 위해 다음과 같은 접근 방식이 사용된다.

① MIME(multipurpose internet mail extension):RFC 2045부터 RFC 2049에서는 텍스트와 2진 데이터를 RFC 822에서 정의한 7비트 아스키로 코드화하는 메카니즘을 명시한다.

② SMTP Service Extensions:RFC 821에서 정의한 SMTP의 기능을 확장하는 메커니즘을 RFC 1869, RFC 1652, 1870에서 각각 정의하고 있다.

55. Data Leak Prevention이란 무엇이며 어떠한 동작을 하나요?

- 데이터 유출 방지 [Data Loss Prevention , Data Leakage/Loss Prevention]

기업 내부자의 고의나 실수로 인한 외부로의 정보 유출을 방지하는 솔루션. 사내에서 주고받는 데이터를 내용이나 형식 등을 기준으로 탐지해 중요 정보 유출을 차단할 뿐만 아니라 데이터 보호 규제에 적극 대응할 수 있다.

56. File Filter란 무엇이며 어떠한 기능을 하나요?

- File Filter 란?

DLP 기능중 하나로써 파일 이름이나 파일 형식을 사전에 정의 후 Network traffic에서 해당 파일이름, 형식에 대해 검사를 하는 것이다.

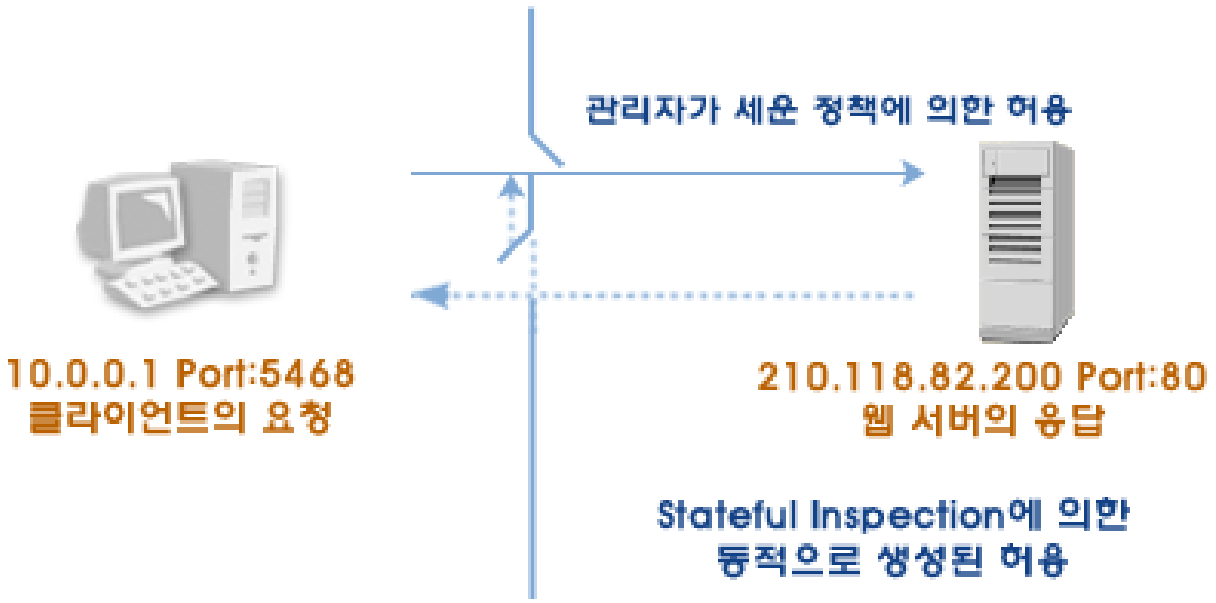
예를 들어, secret.* 이름에 JPEG라는 파일형식을 필터로 정의 한다면 Network traffic에서 위의 필터 항목에 해당하는 Traffic을 control 할 수 있다.

57. Endpoint Control이란 무엇이며 어떤 기능을 하나요?

- Endpoint Control 이란 Fortigate가 사용자 PC의 네트워크 접근을 제어방법이다. 사용자가 네트워크를 사용하기 위해서는 Fortigate에서 설정한 보안 요구사항(특정 Application 설치, 패턴 업데이트 등)을 만족하여야 한다. 만족하지 못하면 네트워크 사용을 차단 한다. 사용자 PC에 설치된 FortiClient는 PC의 Application 상태를 감시한다.

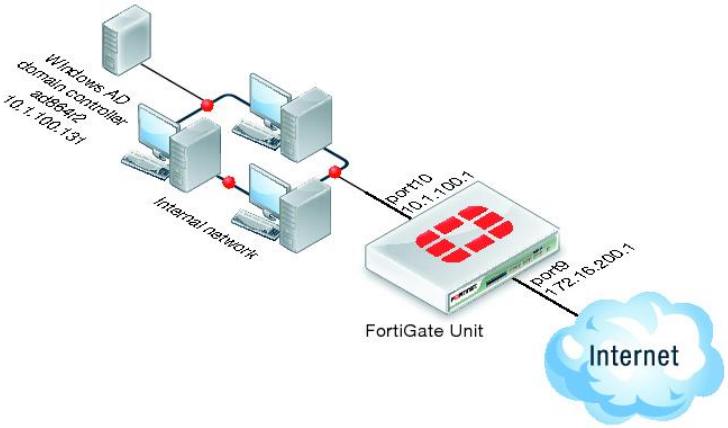
58. Stateful Inspection이란 무엇인가요?

- 라우터의 ACL과 같이 패킷 자체만을 보고 미리 설정된 정책에 따라 허용 또는 차단을 결정하는 초창기 방화벽을 1세대 방화벽이라고 한다. 이러한 패킷 필터 방화벽은 나갔다 돌아오는 패킷을 허용하는 정책이 있어야 하기 때문에 보안적으로 취약해 질 수 있고, FTP와 같이 파생 세션을 만드는 일부 프로토콜을 지원하기 위해서는 모든 포트를 다 오픈해야 하는 경우가 생기기도 한다. 이러한 문제점을 해결하기 위해 고안된 것이 세션 단위의 검사를 하는 Stateful Inspection 이다. 이 방식은 서비스에 대한 특성 및 통신상태(session)를 관리하기 때문에 접근규칙(Access Rule)을 생성할 때에 되돌아오는Flow에 대한 또 다른 접근규칙을 설정할 필요가 없다. 즉, 나갔다 들어오는 패킷에 대해 보안 정책을 정의하지 않아도 통신이 가능하다.



59. 인증기반 Policy 적용과 보안프로파일 기반 Policy 적용은 어떻게 다른가요?

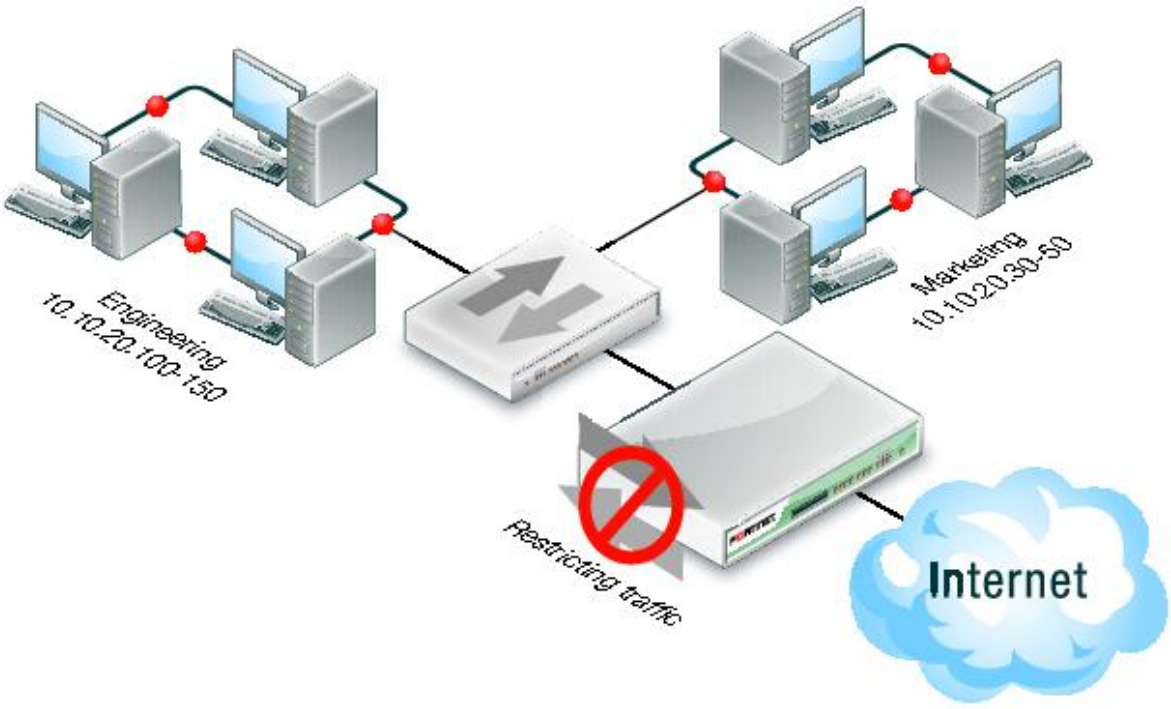
- 사용자 인증기반(Identity Based) policy와 보호 프로파일 정책은 별개의 개념으로 이해를 해야 한다.
  사용자 인증은 사용자의 ID/PW를 통해 인증을 거친 사용자 별로 상이한 보안정책을 적용할 수 있는 기능으로 전통적인 IP주소를 통한 제어가 아닌 실 사용자에 따른 제어를 구현 한다.
  보호프로파일이란 UTM기능의 사용여부 및 적용 룰을 정의해놓은 것으로 방화벽 정책에 UTM정책을 적용하기 위해 사용한다.



보호프로파일

60. Time Based 방화벽 정책을 사용하면 어떤 것들을 기대할 수 있나요?

- 방화벽 정책에 스케줄을 적용하면 정책을 탄력적으로 운영을 할 수 있다. 예를 들어 업무시간에는 업무사이트만 허용하고, 점심시간 또는 업무 외 시간에는 모든 사이트를 허용한다면 업무에 대한 집중도를 높일 수 있고, 인터넷을 사용하고 싶은 근무자들의 개인적인 불만도 어느 정도 해소 될 수 있을 것이다.
  이렇듯 스케줄을 이용하면 정책 설정에 있어 요구 되는 여러 가지 Needs를 해소 할 수 있다.



61. P2P란 무엇인가요?

P2P(Peer to Peer)란 인터넷으로 다른 사용자의 컴퓨터에 접속하여 각종 정보나 파일을 교환, 공유할 수 있게 해 주는 서비스를 말한다. 기존의 서버와 클라이언트로 이루어졌던 데이터 업로드, 다운로드 방식을 사용자끼리 직접 하게 함으로써 수 많은 정보와 파일이 공유되고, 빠른 다운로드 속도 구현한다.

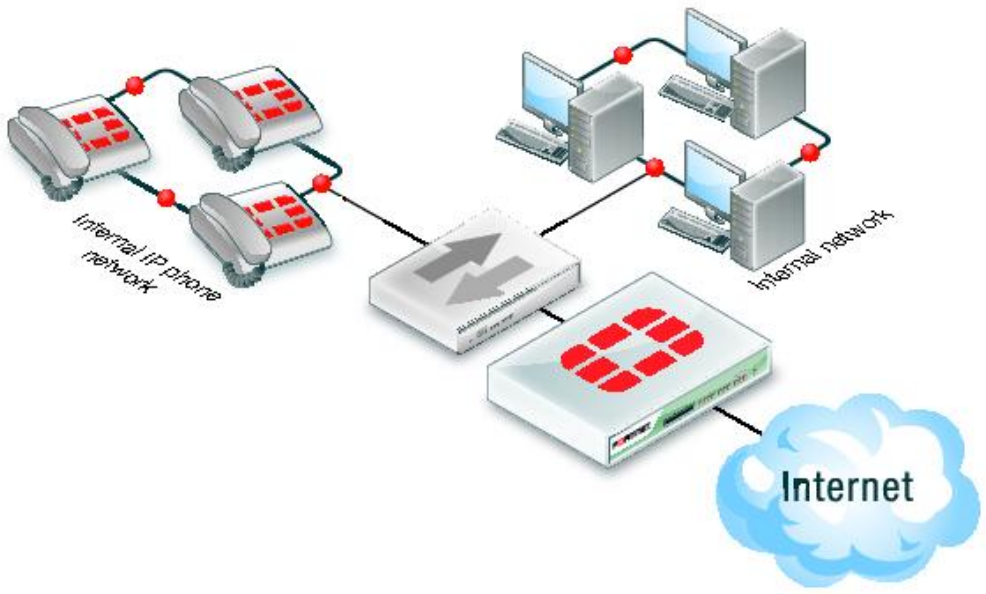
하지만, 기업 네트워크의 리소스를 차지하여 업무를 방해하거나 해커들의 악성코드 배포의 수단으로 사용되어 보안에 위협요소 가 되고 있다.

FOBOX WeDISK pruna

Application Name	Category	Popularity	Risk
9PTV	P2P	low	medium
100Bao	P2P	low	high
ABC	P2P	medium	high
AllMusic	P2P	high	low
Anatomic	P2P	medium	high
Apollon	P2P	low	high
Applejuice	P2P	medium	high
Arctic.Torrent	P2P	medium	high
Ares	P2P	high	high
Ares_Chat.Join	P2P	medium	high
Azureus	P2P	high	high
BTJunki	P2P	medium	high
Baidu.Xiaba	P2P	low	high
Bbcp	P2P	low	medium
Bearshare	P2P	medium	high
BitLord	P2P	low	high
BitTorrent	P2P	high	high
BitTorrent.Download	P2P	high	medium

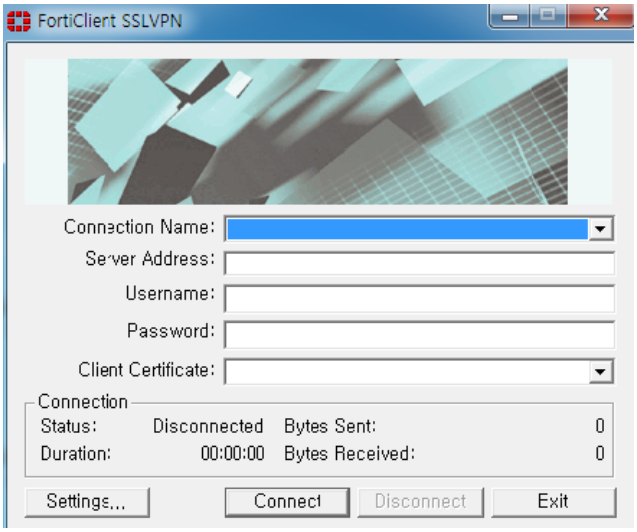
62. VoIP란 무엇인가요?

VoIP(Voice over Internet Protocol)란 흔히 말하는 인터넷 전화로인터넷 망을 이용하여, 음성 데이터를 인터넷 프로토콜 데이터로 변환해 일반 전화망에서의 통화를 가능케 해주는 통신 서비스 기술이다.
예전에는 H.323을 많이 사용되었으나 현재는 SIP 프로토콜의 사용이 빠르게 확산 되는 추세이고, 이와 더불어 음성데이터 보안의 중요성도 커지고 있다.

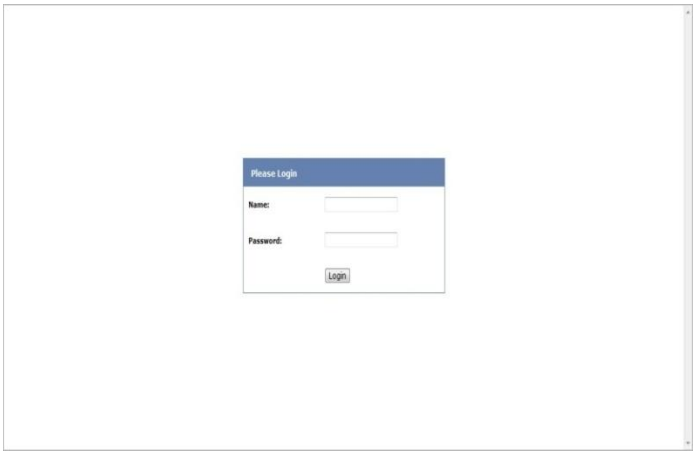


63. SSL VPN에서 Application 모드와 Tunnel 모두 2가지가 있는데, 각각 어떻게 다른가요?

- SSL-VPN을 구성하는 방법은 Web Mode와 Tunnel모드로 나눈다. Web Mode는 클라이언트와 서버 사이에서 Fortigate가 Proxy역할을 하는 방식이고, Tunnel모드는 실제 클라이언트가 터널을 열어 서버로 접속하는 방식을 말한다.
  SSL-VPN을 접속하는 방법은 인터넷 브라우저를 이용하여 접속하는 방식과 SSL-VPN Application 을 이용하여 접속 하는 방법이 있다.



SSL-VPN Application을
이용한 접속



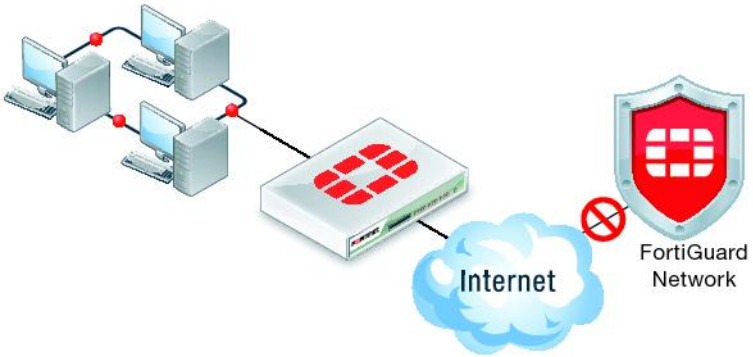
인터넷 브라우저를
이용한 접속

64. IPS 시그니처 패턴은 어떻게 업데이트 되나요?

Fortigate에서 사용되는 IPS 시그니처 패턴 및 AntiVirus 패턴은 FDS(FortiGuard Distribution Servers)를 통하여 업데이트 된다. Fortinet은 FDS를 전 세계적으로 구축을 하였고, 이러한 시스템을 FDN(FortiGuard Distribution Network)라고 한다.

Fortigate가 업데이트를 위해 FDN에 연결하면, 가장 가까운 FDS로 연결되어 업데이트를 수행하게 된다. (가장 가까운 FDS를 찾는 것은 Fortigate에 설정된 TimeZone을 기준으로 한다.)

이렇게 업데이트를 받기 전에 해당 Fortigate는 Fortinet 웹사이트에 유효한 라이선스를 가진 장비로 등록이 되어 있어야 한다.

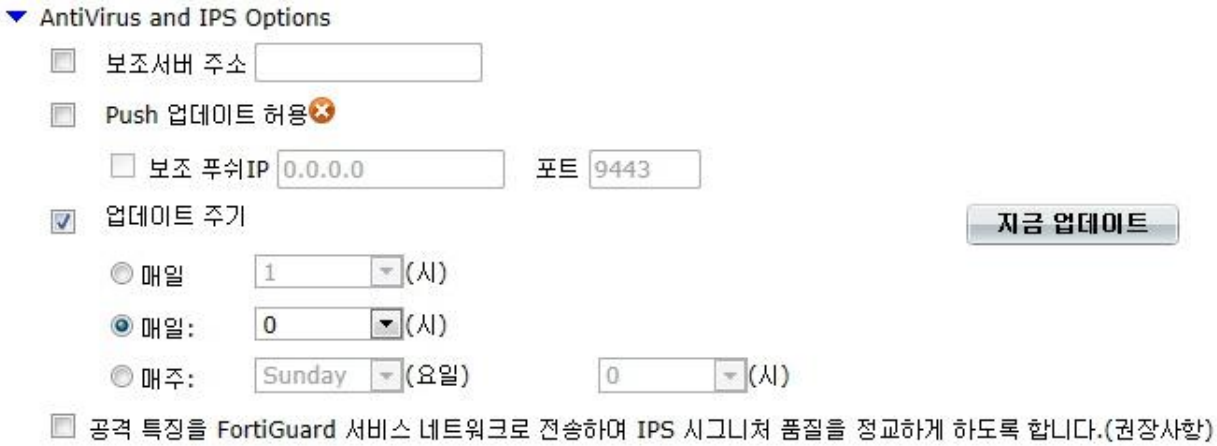


License Information

Support Contract		
Registration	Registered (Login ID: [redacted]) [Login Now]	✓
Hardware	8 x 5 support (Expires: 2011-07-25)	✓
Firmware	8 x 5 support (Expires: 2011-07-25)	✓
Enhanced Support	8 x 5 support (Expires: 2011-07-25)	✓
Comprehensive Support	8 x 5 support (Expired: 2009-07-25) [Renew]	✗
FortiGuard Services		
AntiVirus	Licensed (Expires 2011-07-25)	✓
AV Definitions	12.00520 (Updated 2010-11-02) [Update]	
Extended set	12.00520 (Updated 2010-11-02)	
Intrusion Protection	Licensed (Expires 2011-07-25)	✓
IPS Definitions	2.00888 (Updated 2010-11-01) [Update]	
Web Filtering	Licensed (Expires 2011-07-24)	✓
Email Filtering	Licensed (Expires 2011-07-24)	✓
Analysis & Management Service	Expired [Renew]	✗
Services Account ID		
Virtual Domain		
VDOMs Allowed	10	
Endpoint Security		
FortiClient Software		
Windows Installer	4.1.3 (Updated 2010-11-02) [Download]	
Application Signature Package	1.331 (Updated 2010-11-02)	

65. 패턴 업데이트 시에는 과부하가 안 걸리나요?

- 패턴 업데이트 시 Fortigate는 CPU와 Memory 리소스 사용량이 증가하지만, 서비스에 영향을 줄 정도의 수준은 아니며 업데이트 종료 후 다시 이전 사용량으로 복구 되기 때문에 크게 문제 되지는 않는다. 그러나 장비 리소스에 부하는 주는 작업이기 때문에 트래픽이 많지 않은 시간에 업데이트 하기를 권장한다.



66. IPS기능에서 8가지 Action설정을 할 수 있는데 각각 어떻게 동작을 하나요?

Action	Description
Pass	패턴이 탐지 되어도 추가 액션 없이 통과 시킨다.
Drop	패턴이 탐지 되면 해당 패킷을 버린다. 방화벽 세션에는 영향을 주지 않기 때문에 TCP 세션 기반의 공격은 다른 액션을 사용하는 것을 권장한다.
Reset	패턴이 탐지되면 해당 패킷을 버리고, 서버와 클라이언트 양쪽에 reset 패킷을 보낸다. 세션 테이블에서 해당 세션을 삭제한다.
Reset Client	패턴이 탐지되면 해당 패킷을 버리고, 클라이언트 쪽으로 reset 패킷을 보낸다. 세션 테이블에서 해당 세션을 삭제한다.
Reset Server	패턴이 탐지되면 해당 패킷을 버리고, 서버 쪽으로 reset 패킷을 보낸다. 세션 테이블에서 해당 세션을 삭제한다.
Drop Session	패턴이 탐지되면 해당 패킷을 버리고, 해당 세션으로 따라 들어오는 모든 패킷을 버린다.
Pass Session	패턴이 탐지되어도 차단하지 않고 통과 되며, 해당 세션을 따라 들어오는 모든 패킷도 IPS기능이 Bypass된다.
Clear Session	패턴이 탐지되면 해당 세션을 세션 테이블에서 바로 삭제한다. reset 패킷은 보내지 않는다.

67. Buffer Overflow Attack이란 무엇이며 어떻게 방어하나요?

- 버퍼오버플로우란 이름에서 알 수 있듯이 버퍼를 넘치게 하여 시스템에 장애를 일으키는 공격이다. 메모리에 할당되는 버퍼의 양을 초과하는 데이터를 입력하여 프로그램의 복귀 주소를 조작, 궁극적으로 해커가 원하는 공격을 수행한다.
  Fortigate는 이러한 취약점에 대한 패턴을 가지고 있고 패턴이 감지 되면 차단을 하게 된다.

68. SCAN은 어떻게 방어를 하나요?

- 스캐닝은 공격을 위한 사전작업으로 대상 시스템에 접속 가능한 Port를 파악해 내는 기법이다.
  Fortigate는 Anormaly 트래픽에 대한 차단 기능이 단위 시간당 임계치 이상의 스캐닝 공격이 탐지 되면 차단 한다.

69. Anti Virus에서 File base와 Flow base는 어떻게 다른가요?

Fortigate의 AntiVirus 기능은 Proxy와 Flow-based의 두 가지 scan 방식을 제공한다.

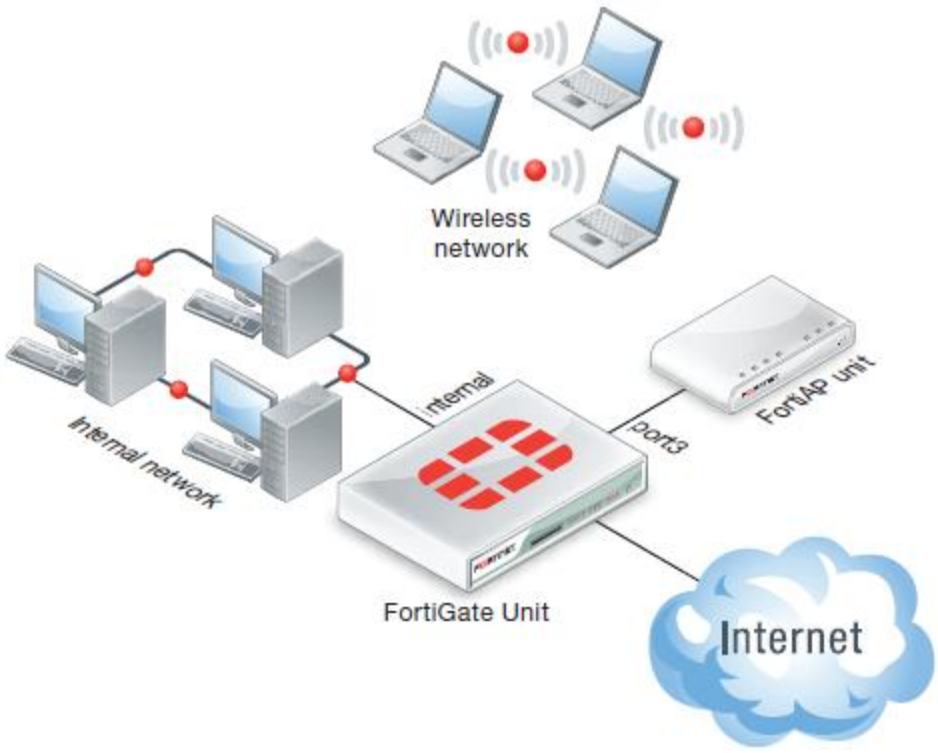
Proxy 방식은 전통적인 scan방식으로 메모리버퍼에 해당 패킷을 캐싱하여 AntiVirus 엔진으로 검사를 하는 방식이다. 정밀한 검사가 가능하지만 장비에 부하를 주기 때문에 고사양의 장비가 요구 된다.

Flow-based 방식은 Proxy방식의 캐싱으로 인한 장비 부하를 완화 할 수 있는 이상적인 솔루션으로 패킷 상태에서 검사를 하는 방식이다.

70. Wireless Control이란 무엇이며 어떤 기능을 담당하나요?

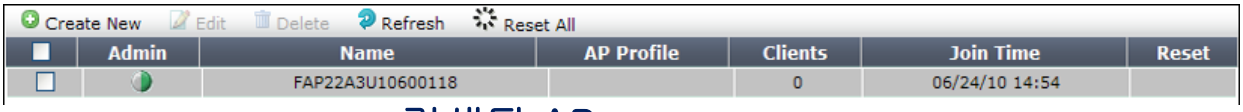
Wireless Controller란 중앙 집중식 무선랜 구조를 구현하기 위한 장비로 이전의 무선랜이 AP에 인증, 보안, 로밍과 같은 모든 기능을 집어넣는 분산형 구조였다. 그래서 높아지는 AP가격과 트래픽 처리 기능의 한계를 해결하고자 생겨났다.

중앙집중식 무선랜에서는 강력한 성능과 지능을 가진 콘트롤러가 모든 트래픽을 처리하고 보안, 인증 같은 기능도 담당함으로써 무선랜의 안정성을 높여주며, AP에 많은 기능을 담지 않아도 되기 때문에 가격 부담이 적어 무선랜을 쉽게 확장할 수 있다는 장점이 있다.

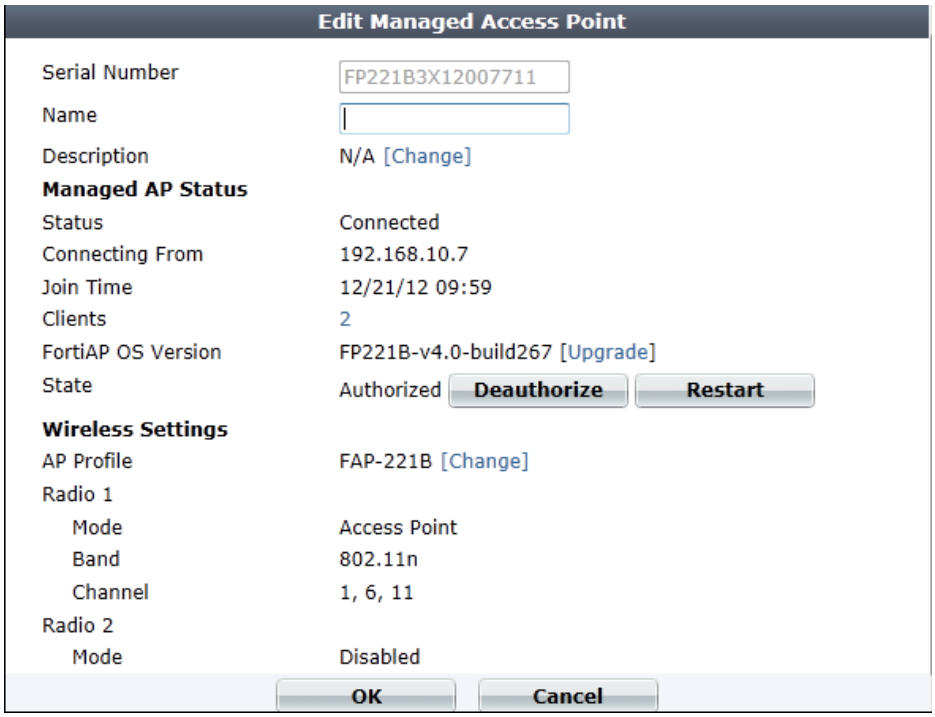


71. 어떻게 AP의 WIFI Radio를 통합 관리하죠?

Fortigate의 WiFi Controller 기능은 Fortigate와 연동된 FortiAP 들을 중앙 집권적인 형태로 관리를 하게 된다. 실제 FortiAP자체에는 무선 설정에 관한 관리 기능이 전혀 없고, *WiFi Controller > Managed Access Points > Managed* 에 등록된 FortiAP에 AP프로파일을 적용 함으로써 Radio 할당, 보안설정 등을 관리구성을 하게 된다.



– 검색된 AP–



– AP 설정 화면–

72. 다른 제조사의 AP도 관리할 수 있나요?

- Fortigate의 WiFi-Controller 기능은 타 벤더의 AP와 연동이 불가하다.

73. 인증방식에 WPA와 Captive Portal이 있는데 각각이 어떤 내용이며, 어떤 경우에 사용이 되나요?

WPA란 무선 랜 보안 표준의 하나로 기존 WEP방식의 취약점을 보완한 방식이다. WPA는 무선 접속에 대한 암호화와 인증을 통해 무선 보안을 구현한다. 보통 무선 접속을 할 때 인증 키를 입력하여 인증 받는 방식이라고 생각 하면 된다.

Captive Portal이란 무선망에 최초로 접속 시에 URL에 접근하면 자동으로 나타나는 웹 페이지를 말하며, 무선망을 사용하기 전에 반드시 로그인 정보를 입력하거나 망 이용 목적 제한 방침에 동의 해야 한다. 일반적으로 공항, 호텔로비, 커피숍 등 Wi-Fi 핫 스팟을 인터넷 사용자에게 무료로 제공하는 곳에서 사용한다.