업데이트일 : 2019-2-01

IX. 보안

1. 웹방화벽 Wapples

목차

1.1 ucloud 웹방화벽 서비스 소개

1.1.1 목적/용도

웹방화벽은 웹서버 앞에 위치하여 외부로부터 들어오는 HTTP/HTTPS 트래픽을 감시하여 웹 애플리케이션에 대한 악의적인 공격이 탐지되면 해당 공격이 웹 서버에 도달하기 전에 차단하는 역할을 수행합니다.

그림이 보여주는 바와 같이 웹방화벽은 방화벽에서 걸러주지 못하는 응용계층의 위험한 유해 트래픽을 웹 서버에 도달하지 못하도록 근본적으로 차단합니다.
고도로 지능화, 다양화되고 있는 웹 공격을 효율적으로 탐지 및 차단하여 안정적이고 신뢰할 수 있는 웹 애플리케이션의 운영을 가능하게 합니다.

일반적인 방화벽은 출발지 및 목적지의 IP/Port 정보를 기반을 필터링을 하는 보안 장비로 TCP/IP 프로토콜의 헤더 정보를 이용하여 필터링을 실시하기 때문에 정상적인 IP/Port로 유입되는 해킹 공격에는 대응할 수가 없습니다. 웹방화벽은 방화벽에서 허용한 IP/Port로 유입되는 트래픽의 데이터 부분을 해석하여 유해한 트래픽이나 공격을 차단할 수 있는 장치입니다.

즉, 웹방화벽은 웹 트래픽에 대한 Payload(Data) 분석 및 패턴 기반의 필터링을 통해 악의적인 웹 애플리케이션 공격을 탐지 및 방어 합니다. 대부분의 웹 공격은 웹 어플리케이션 개발 구축 시 발생되는 취약점을 이

용하거나, HTTP 요청 메시지에 특정 공격 또는 취약점 우회 코드를 삽입해 웹 서버에 전송하게 됩니다. 웹방화벽은 웹 서버로 전송되는 HTTP 요청 메시지의 Packet을 검사하여 웹 어플리케이션에 의도하지 않은 내용의 전송을 차단하고 HTTP 응답 Packet 내용을 검사하여 특정 정보의 유출을 방지 할 수 있습니다.

▫ 웹방화벽과 방화벽의 비교

구분	방화벽(Firewall)	웹방화
동작방식	허용되지 않은 IP/Port에 대한 공격 차단	HTTP/HTTPS를 이용한 공격 차단
필터링 방법	사전 정의된 Access List에 의한 차단	사전 설정된 룰셋(패턴, 휴리스틱)기반의
인식 헤더	발신지 및 목적지의 IP/Port	헤더 정보를 포함하여 Packet의 Payload
보호 대상	대부분의 정보 자원	웹 서버
구성 형태	네트워크 경계 부분에 위치	논리적으로 웹서버 앞(Inline/Proxy 모드
특징	Access List에서 허용된 트래픽의 필터링 불가	Payload 분석에 따른 고성능의 프로세싱

▫ 웹방화벽의 주요 보안 기능

- HTTP 기반의 웹 공격 방지
- OWASP1 TOP 10 Attacks 탐지 및 차단

OWASP Top 10 2013	취약점
인젝션	전송 파라미터 기반 동적 SQL query를 처리하는 웹 모듈에 command를 삽입,
인증 및 세션 관리 취약점	허술한 계정관리나 미흡한 인증체계 구성 및 세션 처리에 의한 공격 위험 노출
크로스 사이트 스크립팅(XSS)	공격자에 의해 작성된 악성 스크립트 코드가 다른 사용자에게 전달되는 취약점
취약한 직접 객체 참조	객체(파일, 디렉터리, DB값 등)을 URL이나 HTML tag로 노출 시 이를 이용한 공
보안 설정 오류	프레임 워크/플랫폼, 서버, 웹 서버, DB 서버 등의 보안을 정의하고 최신 상태로
민감 데이터 노출	주민번호 등 민감 데이터 관리 시 평문 저장, 전송되는 취약점 이용, 불안정한
기능수준의 접근통제 누락	서비스 페이지 접근에 대한 적절한 통제 및 기술 조치 누락 시 인가되지 않은
크로스 사이트 요청 변조(CSRF)	정상 인증된 사용자의 쿠키나 세션 정보를 통해 숨겨진 스크립트, Tag 정보로
알려진 취약점이 있는 컴포넌트 사용	라이브러리, 프레임 워크 및 기타 소프트웨어 모듈과 같은 구성 요소는 전체 권격
검증되지 않은 리다이렉트 및 포워드	평문 형태로 전송되는 TCP/IP 취약점을 이용하여 전송 데이터의 정보 유출, 결

- PCI-DSS Compliance 의 요구사항 지원
- Known/Unknown Worm 탐지 및 차단 (예, Code Red, Nimda)
- 웹 보안 요소 방어
- Cookie 변조 및 도용 방지
- Hidden Field 변조 방지
- 표준 암호 알고리즘 사용(AES, SEED)

- 웹 컨텐츠 필터링
- 개인정보 포함 파일 업로드/다운로드 탐지 차단
- 주민등록번호, 신용카드번호, 이메일주소, 주소, 전화번호 탐지
- MS-Office, Open Office, PDF, MS Outlook Message, hwp 등 30 여종의 파일 검색
- 지정한 금지 단어 입력 시 자동 변환
  예) '나쁜말'(금지단어) -> '고운말'(등록된 표현)
- 해커에 의해 변조된 페이지 노출 차단 및 자동 복구

▫ 웹방화벽의 주요 특징

- 보안성
  - 웹 공격에 대한 3중 방어 구조
    Positive Security 보안모듈의 "URI 접근 제어"와, Negative Security 보안모듈의 "룰 탐지", White/Black list of IP 주소 관리 기능인 "IP Filtering" /
    "IP Block"의 웹 클라이언트 접근 제어의 3중 방어 구조를 기반으로 확실하고 안정적인 웹 공격의 탐지와 차단을 제공합니다.
  - 암호화 트래픽 지원
    SSL과 같은 암호화된 트래픽을 지원합니다. 암호화된 트래픽 내에 웹 공격이 들어있는 경우에도 이를 신속하게 복호화한 후 공격을 탐지하여 차단할 수 있습니다.

- 성능
  - 버추얼 어플라이언스
    웹 서버를 비롯한 기존 서비스 장비에 별도의 부하를 주지 않는 버추얼 어플라이언스(appliance) 형태로 구성되어 높은 성능 을 제공합니다.
  - 웹사이트/웹서버 동시 보호
    여러 웹사이트들과 하나의 웹 서버들을 동시에 보호하는 것이 가능합니다.

- 안정성
  - Watchdog 지원
    Watchdog 프로세스는 지속적이고 안정적인 웹 서비스 제공을 위해 WAF의 동작을 감시합니다. WAF에 문제가 발생하는 경우, watchdog은 문제의 증상
    을 파악하고 이에 따라 보안 및 웹 서비스 유지를 위해 대응하도록 구성되어 있습니다

- 편리성
  - 대시보드 지원
    WAF과 웹 서버의 운영 상태를 그래프와 차트를 통해 한눈에 실시간으로 파악할 수 있는 대시보드 기능을 지원합니다. WAF의 대시보드는 22가지의 다양한 그래프
    와 차트 형식을 제공하여 운영자가 원하는 형태로 데이터를 가공할 수 있도록 지원합니다

  - 설정 마법사 지원
    WAF의 모든 설정 작업은 설정 마법사를 통하여 이루어집니다. 설정 마법사는 WAF의 복잡한 설정 과정을 간단하고 편리하게 수행 할 수 있도록 도와줍니다.

  - 자유롭고 유연한 화면 구성
    로그 화면과 각종 대시보드 화면 등을 운영자가 원하는 형태로 자유롭게 배치할 수 있으며 각각의 화면 내용에 각기 다른 조건을 부여하여 다양한 정보를 동시에
    확인할 수 있습니다. 이러한 유연한 화면 구성은 운영자의 필요에 따른 적절한 정보 확인을 가능하게 해주어 관리도구 사용의 편의성을 높여줍니다.

1.1.2 구조 / 원리

▫ Reverse Proxy 구성 방식

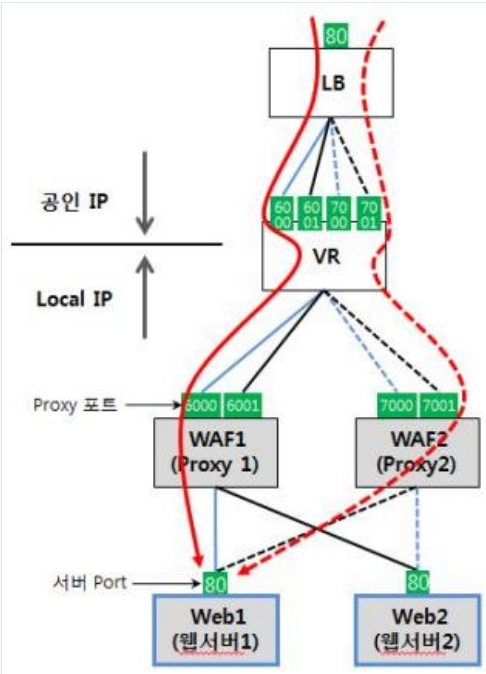
ucloud WAF의 네트워크 구성방법은 리버스 프락시 방식입니다. WAF의 리버스 프락시 구성은 일반적인 웹 프락시 서버와 유사한 구성으로 WAF의 논리적인 네트워크와 IP 등을 설정하여 구성합니다. 이러한 구성에서 특정 웹사이트를 WAF로 보호하려면 웹사이트의 DNS를 재설정하거나 L4/L7 스위치의 설정을 수정하여 웹 서버로 갈 커넥션이 WAF을 향하도록 수정해주어야 합니다. 이러한 리버스 프락시 구성에서는 WAF가 프락시로 동작하기 때문에 웹 서버의 접속 로그에는 실제 웹 브라우저 사용자의 IP 주소가 아닌 WAF의 IP 주소만이 남게 됩니다.

▫ **웹방화벽 서비스 네트워크 구조**

ucloud에서는 외부에서 공인 IP로 접속할 수 있는 VR(Virtual Router)를 제공하며, VR 내부에 사용자가 생성한 VM이 위치하게 됩니다. VM은VR을 통해 인터넷 통신이 가능하므로 Outbound Traffic은 Virtual Router를 통해서 Source NAT 가적용 됩니다. WAF와 웹서버 VM간의 통신은 내부 사설 IP(172.27.x.x)로 통신이 가능하며 사용자의 클라우드 서버는 VLAN 기술로 isolation 되어 보안성을 제공합니다.

아래그림은 로드밸런서(L4)를 이용하여 Active/Active의 WAF 이중화 구성도의 예시를 보여줍니다. LB에서는 WAF(Proxy 서버) – Web(웹서버)로 연동되는 트래픽 패스에 따라 분리 구분되는 각 서비스포트로 로드밸런싱(80 포트로 들어오는 트래픽을 60000, 6001,7000, 7001로)하고, VR에서는 WAF의 서비스 포트로 포트 포워딩(PF : Port Forwarding)이 설정되어 있어야 합니다. WAF에서는 웹서버로 트래픽을 전달하기 위한 WAF의 서비스 포트와 웹서버와 포트를 매핑 등록 구성되어야 합니다. LB, WAF, Web 서버에서의 서비스 트래픽에 포함된 TCP/IP 정보는 아래와 같이 변경됩니다

LB 에서의 TCP/IP 정보 : Source – Client IP, Destination – LB IP(공인)
WAF1,2 에서의 TCP/IP 정보 : Source – LB IP, Destination – WAF IP(공인) Proxy 포트
Web1,2 에서의 TCP/IP 정보 : Source – WAF IP(로컬), Destination – Web IP(로컬) 서버 포트



<LB 구성 정보>

서비스 Port	등록서버 Port
80	6000, 6001, 7000, 7001

<PF 설정 정보(웹서버 구성시 자동설정)>

구분	Public Port	Private Port
WAF1	6000	6000
	6001	6001
WAF2	7000	7000
	7001	7001

<WAF의 웹서버 구성 정보>

구분	Proxy 포트	(웹)서버 Port
WAF1	6000	80 (Web1)
	6001	80 (Web2)
WAF2	7000	80 (Web1)
	7001	80 (Web2)

1.1.3 유의사항/제약사항

과도한 웹 트래픽 발생시 WAF가 안정적으로 운용되기 위해서는 고객의 웹서비스 환경에 적절한 성능을 요하는 WAF 상품 선택 및 이중화 구성이 필요합니다. WAF 이중화 구성에는 로드밸런서(LB)를 이용하여 Active-Active 구성 운용이 가능합니다. (또는 WAF IP 를 별도 할당 받아 DNS, GSLB 를 이용해서도 도메인 질의시 WAF IP 를 분산하는 방법도 가능)

웹방화벽이 웹방화벽이 위치한 Zone과 다른 Zone에 위치한 웹서버를 보호할 경우의 성능은 보장하지 않습니다.

웹방화벽의 상품별 Throughput을 초과하는 Traffic 발생 시에는 과부하로 인한 웹방화벽 성능 저하 또는 서비스 중단이 발생할 수 있습니다.

웹방화벽의 업데이트 시 재부팅으로 인한 서비스 중단이 발생할 수 있으므로 자동 업데이트를 하지 않도록 초기설정 되어 있습니다. 이에 주기적으로 수동 업데이트 확인 및 업데이트를 해야 합니다.

웹방화벽은 운영체제 및 내부 데이터베이스가 안정적으로 작동하며 웹 보안 게이트웨이 애플리케이션 방화벽으로만 동작되도록 설계되고 구성된 전용 서버이므로, 내부 구성을 변경하거나 다른 목적으로 사용하는 것을 보증하지 않습니다

웹방화벽은 HTTP/HTTPS 트래픽에 대한 보안을 위하여 만들어졌습니다. 따라서 추가적으로 방화벽이나 침입탐지 시스템과 병행하여 운영되어야 합니다

웹방화벽은 네트워크 상 클라이언트와 웹서버 간 중간 지점에 위치해야 하며, 양자간의 HTTP(S) 통신은 WAF 을 통해서만 이루어져야 합니다.

네트워크 구성 변경, 웹 사이트의 증감 등으로 네트워크 환경이 변화될 때에는 반드시 변화된 환경에 맞추어 보안정책을 반영하여야 합니다.

관제시스템과 같은 외부 시스템과의 연동 시 SNMP trap, Syslog 등을 사용할 수 있으며, 이때 신뢰된 네트워크 구간 내에서 안전하게 유지되도록 관리해야 합니다.

제품 유지보수 절차를 통해 최신의 보안 패치가 적용된 상태로 운영되도록 해야 합니다.

WAF은 신뢰할 수 있는 타임스탬프를 제공합니다. 안전한 운영을 위해 관리도구용 PC 에 대해서도 OS 가 제공하는 타임스탬프 동기화 기능을 적용하여 일관성을 유지해야 합니다.

인가된 관리자에 의해 안전한 방식으로 구성, 관리, 사용되어야 합니다

관리자는 WAF 관리기능에 대해 적절히 교육 받아야 하고, 관리자 지침에 따라 정확하게 의무를 수행하여야 합니다.

WAF 관리도구는 최신의 보안 패치가 적용된 OS 가 설치된 안전한 관리자 PC 에서 사용 되어야 합니다.

관리도구는 신뢰된 네트워크 구간에서만 접속 가능하도록 하여야 합니다.

관리도구를 통해 WAF 에 접속하는 경우, SSL 로 암호화된 트래픽을 통해 정보를 전달하므로 정보의 비밀성을 유지합니다

WAF 는 정상적인 웹 트래픽의 경우에도 Payload 데이터를 분석하여 공격을 방어하는 어플리케이션 계층(L7)의 보안 장비로 L3 계층의 보안 장비에 비해 상대적으로 많은 서버 성능을 요합니다.

웹방화벽을 최신버전으로 업데이트 하려면 어떻게 해야 하나요? 업데이트 시 서비스 중단이 발생하나요?

업데이트 상세 방법은 1.8 시스템 업데이트 가이드를 참고하시기 바랍니다. 업데이트 시, 약 10분간 서비스 중단이 발생 하므로, DNS의 설정을 WAF에서 웹서버로 변경하거나, LB를 사용하는 경우, LB에서 웹서버로 트래픽이 넘어가도록 설정 후, 업데이트를 하시기 바랍니다.
시스템의 안정적 운용을 위해서, 최소 3개월에 한번씩은 최신버전으로 업데이트를 권고합니다.

웹방화벽 신청 후 팝업 및 Email로 안내 받은 패스워드로 관리도구 접속이 안 됩니다.

웹방화벽은 관리를 위해 관리도구와 SSH 터미널 두가지를 제공합니다.
신청 시, 팝업 및 Email로 안내 받은 패스워드는 SSH 터미널 패스워드이며,
관리도구의 경우, 초기 패스워드가 고정되어 있으며, 최초 로그인 후 비밀번호를 변경하시면 됩니다.
관리도구 초기 패스워드는 (M2존: penta7728 / 그외 존: penta) 입니다.

계정과 패스워드를 정확히 입력했는데도 관리도구 접속이 안됩니다.

웹방화벽 생성 시, 입력한 포트 정보를 정확히 입력해야 합니다. 클라우드 콘솔의 포트포워딩 설정 정보와 입력한 포트 정보가 일치하는지 확인이 필요합니다.
하단 우측 그림의 M2존의 경우, 접속포트에 웹방화벽 신청시 설정한 API포트를 입력해주시면 됩니다.

관리도구 패스워드 분실 시 어떻게 해야 하나요?

관리콘솔의 비밀번호를 초기화 하기 위해서는 WAF VM에 SSH 원격 접속하여 다음과 같은 절차에 따라 초기화 가능합니다.
단, CLI 명령어를 통한 WAF 관리는 충분한 기반 지식이 필요하며, 문제가 발생할 수 있으므로 다른 명령어는 사용하지 않기를 권고 드립니다.

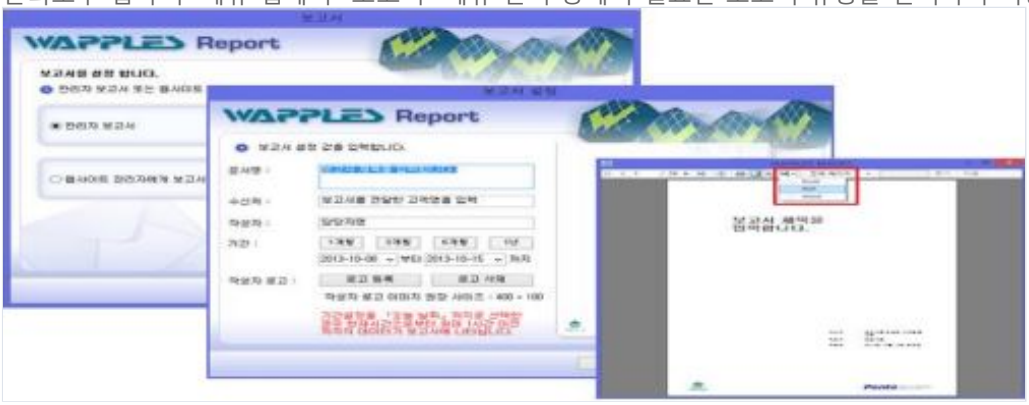
- M2 존의 경우
  1. SSH 접속
  2. CLI접속 : enable (pw:penta)
  3. 쉘접속 : st (pw:sh/wp.no1)
  4. 비밀번호 초기화 스크립트 실행 : ~# /opt/penta/wapples/scripts/db_reset_admin_passwd
  5. UI 재접속 : 초기비밀번호 (id:admin / pw:penta7728)
- 그 외 존의 경우
  1. SSH 접속
  2. CLI접속 : enable (pw:penta)
  3. 쉘접속 : st (pw:sh/wp.no1)
  4. 비밀번호 초기화 스크립트 실행 : ~# /sphere/scripts/db_reset_admin_passwd
  5. UI 재접속 : 초기비밀번호 (id:admin / pw:penta)

탐지된 웹 로그 기능 조회 기능이 제공 되나요?

기간별/출발지IP/URL/보안정책 룰/국가별에 대해 필요한 조건에 맞게 필터링 조회가 가능합니다.(WAF 관리콘솔 내 탐지로그 메뉴)

공격탐지 결과를 보고서 형태로 받을 수 있나요?

관리도구 접속 후 메뉴 탭에서 "보고서" 메뉴 선택 창에서 필요한 보고서 유형을 선택하여 이용 가능합니다.



정책설정을 백업 할 수 있나요?

M2존의 경우 정책설정과 탐지로그 백업이 가능하며, 그 외 존의 경우 정책설정 백업이 가능합니다.
정책 설정의 상세 방법은 1.8 시스템 업데이트 가이드 내, 설정 백업 항목을 참고하시기 바랍니다.
- M2 존의 경우 : 관리도구 -> 환경설정 -> 백업 설정에서 로그 DB 및 설정 DB 백업
- 그 외 존의 경우 : 관리도구 -> 정책설정 -> 모든설정 내보내기

탐지로그의 Client IP가 실제 Client IP와 달라요.

웹방화벽 상단에 LB 등 Proxy 형태의 장비가 있을 경우, Proxy 장비 특성으로 인해 TCP의 출발지 IP가 Proxy 장비의 IP로 변경됩니다. 이에 WAF에서 탐지로그 생성 시 TCP의 출발지 IP를 참조하도록 되어 있음에 따라 Proxy IP가 기록됩니다. 이런 Proxy 형태의 장비들은 Client IP를 보존하기 위해 웹의 경우 X-Forwarded-For 헤더 내에 Client IP를 저장하고 이를 Request 메시지 헤더에 포함하여 전송합니다. 웹방화벽에서도 설정을 통해, Proxy 환경일 경우 해당 헤더를 참조하여 탐지로그를 생성하도록 적용이 가능합니다.
X-Forwarded-For 헤더 참조 적용 방법
- CLI에 접근하여 아래와 같이 실행합니다. (CLI 접속 -> wapples -> logging)

```
penta-np> en
password:
penta-np# configure terminal
penta-np(config)# wapples
penta-np(config-wapples)# logging
penta-np(config-wapples-logging)# set traceSourceIP enable
Change success on TraceSourceIP
penta-np(config-wapples-logging)# apply
Apply to Logging...
Stop WAPPLES Process...
Restart wapples Process...
Start WAPPLES Process...
penta-np(config-wapples-logging)#
```

웹 서비스 페이지가 열리지 않아요.

아래와 같이 웹서비스 및 웹방화벽을 점검해 보시기 바랍니다. 상세 절차는 매뉴얼 1.7 모니터링 및 시스템 이상 시 진단 방법 항목을 참고하시기 바랍니다.
점검 후에도 문제 해소가 되지 않는 경우, 헬프데스크에 연락 주셔서 기술 지원을 받으시기 바랍니다.
step1. 웹서비스가 정상 구동 중인지 웹서버에 접근하여 웹서비스를 확인
step2. 웹방화벽이 과부하 상태인지 확인하기
step3. 웹방화벽 보호대상 추가 여부 확인하기
step4. 웹방화벽 정책 확인하기

탐지로그가 발생하지 않아요.

아래와 같이 웹방화벽 설정 및 정책, LB 설정을 점검해 보시기 바랍니다. 상세 절차는 매뉴얼 1.7 모니터링 및 시스템 이상 시 진단 방법 항목을 참고하시기 바랍니다.
점검 후에도 문제 해소가 되지 않는 경우, 헬프데스크에 연락 주셔서 기술 지원을 받으시기 바랍니다.
case1. 웹방화벽 설정 및 정책 미적용으로 인한 미탐지(웹 방화벽 정책이 탐지 없이 통과로 되어 있는지 확인합니다.)
case2. 서비스 트래픽이 웹방화벽을 경유하지 않을 경우 (LB 및 포트포워딩 설정 내역을 확인합니다.)

1.3 웹방화벽 이용방법 - M2존

ucloud 포탈에서 WAF 서비스 구성 및 환경 설정하는 방법을 설명합니다.

M2존 웹방화벽에 해당 하는 내용입니다.

그 외 존에 웹방화벽을 구성하신 경우 매뉴얼 1.4 항목을 참고하시기 바랍니다.

1.3.1 웹방화벽의 생성 및 삭제

WAF은 일반적으로 다음과 같은 설치 순서에 따라 웹 방화벽 신청 팝업 화면에서 서비스 구성을 합니다.

상품소개에서 보안 -> 웹 방화벽을 선택 -> 웹 방화벽 신청 버튼 클릭

ㅁ 1 단계 서비스 구성

(1) WAF 가 생성되기를 원하는 AZ(Availabipty zone) 선택합니다.

(2) WAF 이름을 입력합니다.

(3) WAF 이름이 다른 VM의 이름과 중복되지 않는지 확인합니다.

(4) Single 선택, WAF 의 이중화 구성하고자 하는 경우는 Single 을 2 개 생성하여 구성합니다.

(5) 사양 : 필요 트래픽에 따라 상품(Standard, Advanced, Premium)을 선택합니다. 각 상품별 Throughput은 (350 / 600 / 1000)이므로 서비스 최대 트래픽을 고려하여 상품 선택이 필요하며, 안정적 서비스를 위해 반드시 이중화 하여 구성할 것을 권고합니다.

(6) WAF이 사용하는 3개의 포트에 대한 포트포워딩 설정을 합니다. SSH 접속을 위한 22번 포트 /

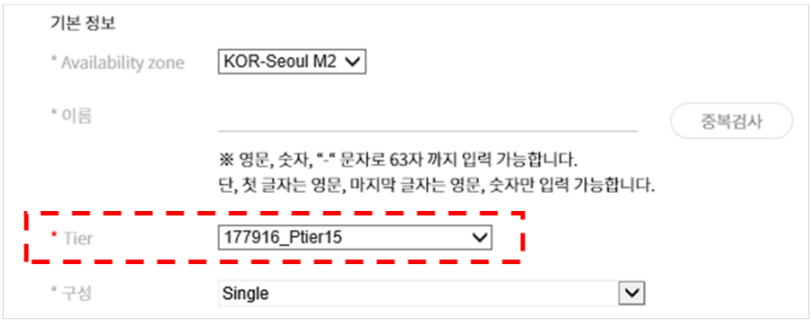
API서비스가 사용하는 5001번 포트 / 웹콘솔이 사용하는 5000번 포트 각각에 대한 공인 포트를 입력하면 됩니다.

(7) 포트포워딩 설정에 충돌이 없는지 포트 체크를 합니다.

고객의 웹서비스 환경에 따라 각 상품별 최대 throughput 은 달라질 수 있습니다.

다음 버튼을 클릭하여 신청내역 확인 단계로 넘어갑니다.

※ Enterprise security의 경우



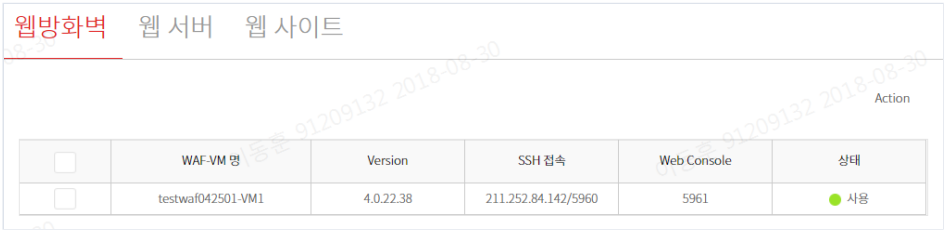
그림과 같이 Tier를 선택하는 항목이 기본정보에 추가로 표시됩니다.

해당하는 Tier를 선택하여 주시기 바랍니다.

ㅁ 2 단계 신청 내역 확인

신청 내역을 확인하고 확인 버튼을 클릭 후 웹방화벽 서버가 생성 완료될 때가지 대기합니다.

서버 생성 및 구성이 완료되면 WAF 상태가 준비 중에서 사용 상태로 변경되고 WAF 의 SSH 접속 패스워드가 팝업 됩니다. ucloud biz 포탈 email 계정의 메일을 확인하셔서, SSH 접속 패스워드를 다시 확인 할 수 있습니다.



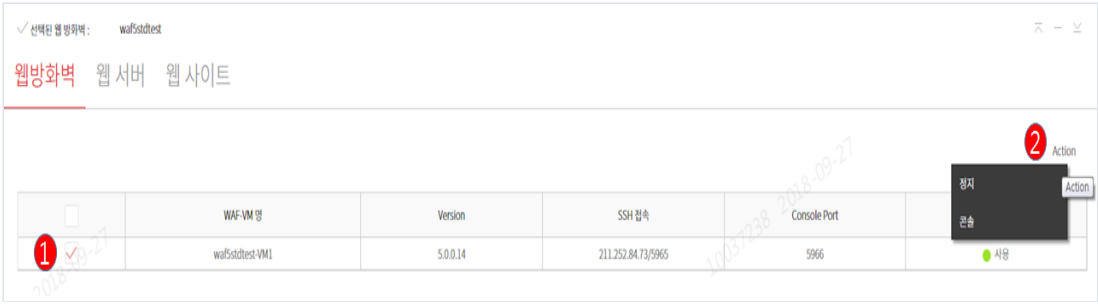
WAF VM 의 삭제는 WAF VM 이 정지된 상태에서 Action 버튼을 클릭하여 삭제 가능합니다.

엔터프라이즈 존에 WAF VM 을 생성하는 경우에는 WAF 초기화 및 업데이트 정보를 가져올 수 있도록 3 개 IP (218.145.29.166, 218.145.29.168, 218.145.29.101)에 대한 방화벽 허용 설정이 필요 합니다.

1.3.2 WAF VM의 시작/정지, SSH 접속 비밀번호 변경

ㅁ 시작 / 정지

WAF 신청 시 자동으로 시작 상태가 됩니다. 특별한 사유에 의해 WAF을 재부팅하고자 할 때 다음과 같이 정지/시작 할 수 있습니다.



(1) 웹방화벽 선택 후, 우측 상단의 Action 위치에 마우스 커서 이동합니다.

(2) 정지 클릭 후, 웹방화벽 상태가 <정지>가 될 때까지 대기합니다.

(3) 웹방화벽 상태가 <정지>가 된 후, Action 위치에 마우스 커서를 이동하고, <시작>을 클릭합니다.

◘ SSH 접속 비밀번호 변경

WAF은 주로 닷넷 기반의 관리도구 어플리케이션을 사용하여 관리하며, 상태 점검 등 특별한 경우, SSH 접속을 하여 관리할 수도 있습니다. SSH 접속 비밀번호는 다음과 같은 절차로 변경 가능합니다.

(1) 웹방화벽 선택 후, 우측 상단의 Action 위치에 마우스 커서 이동합니다.

(2) 비밀번호 변경 클릭 및 팝업 창에서 확인 클릭 시, 랜덤하게 비밀번호 변경됩니다.

1.3.3 웹서버 구성 및 웹사이트 구성

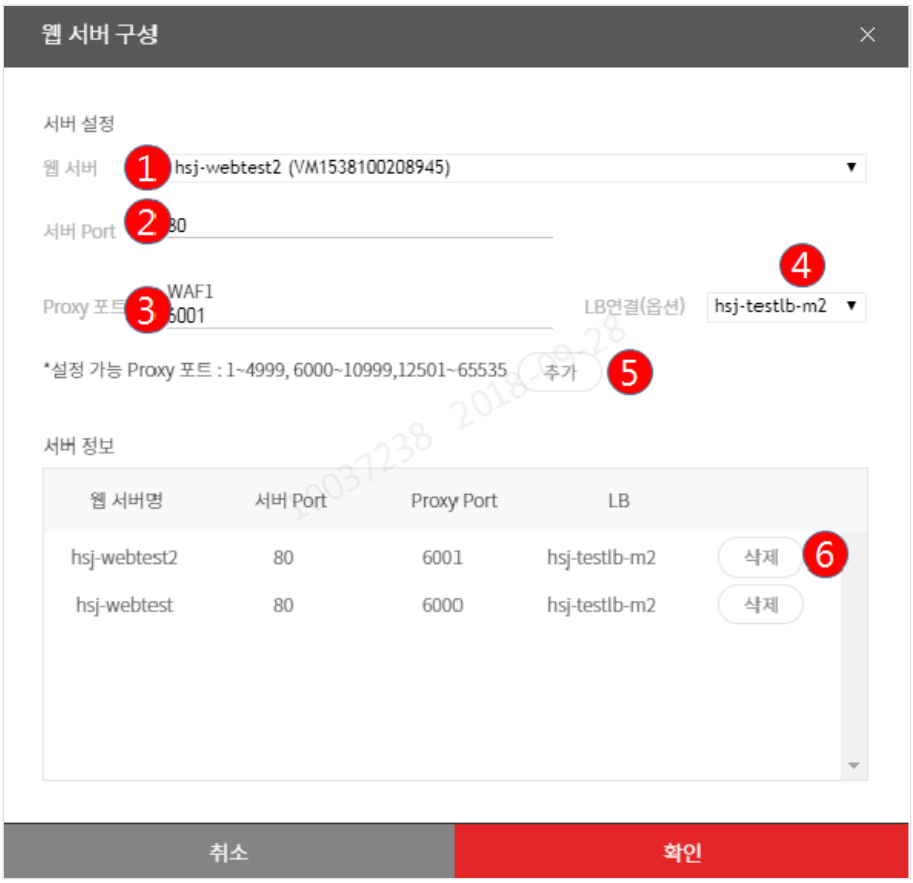
◘ 웹서버 구성

웹방화벽과 웹서버간의 서비스 구성작업을 실시 합니다.

(1) 구성하고자 하는 웹방화벽을 선택 후, 우측 상단의 Action 위치로 마우스 커서를 이동합니다.

(2) 웹서버 구성 클릭합니다.

웹방화벽이 2개의 웹서버를 보호하는 경우를 가정하여 설명합니다.



(1) 보호할 웹 서버를 선택합니다.

(2) 웹서버의 웹서비스 포트를 입력합니다.

(3) 웹방화벽의 Proxy 포트를 입력(트래픽은 웹방화벽IP:프록시포트 -> 웹서버IP:서비스포트 형태로 전달 됩니다.)

(4) 웹방화벽이 이중화 구성일 경우, 부하분산 처리할 로드밸런서를 선택해 줍니다. LB에 별도 설정 필요 없이, 여기서 입력되는 값 기준으로 LB와 WAF, 웹서버간 연결이 형성 됩니다.

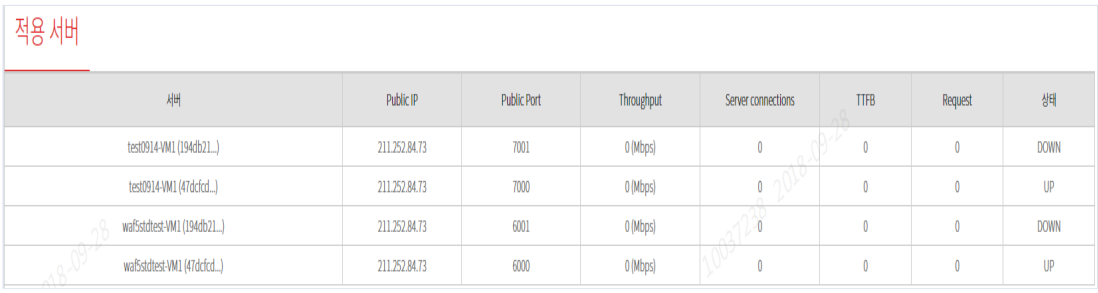
(5) 설정값 입력이 완료 되었다면, 추가를 클릭하면 하단에 입력 정보가 반영됩니다.

(6) 입력값이 잘못된 경우, 삭제 후, 다시 입력할 수 있습니다.

*참고. 이중화 구성 예제

2개의 웹방화벽으로 2개의 웹서버를 보호하는 경우 아래와 같이 설정해 줍니다. (서버 포트는 80을 가정합니다.)

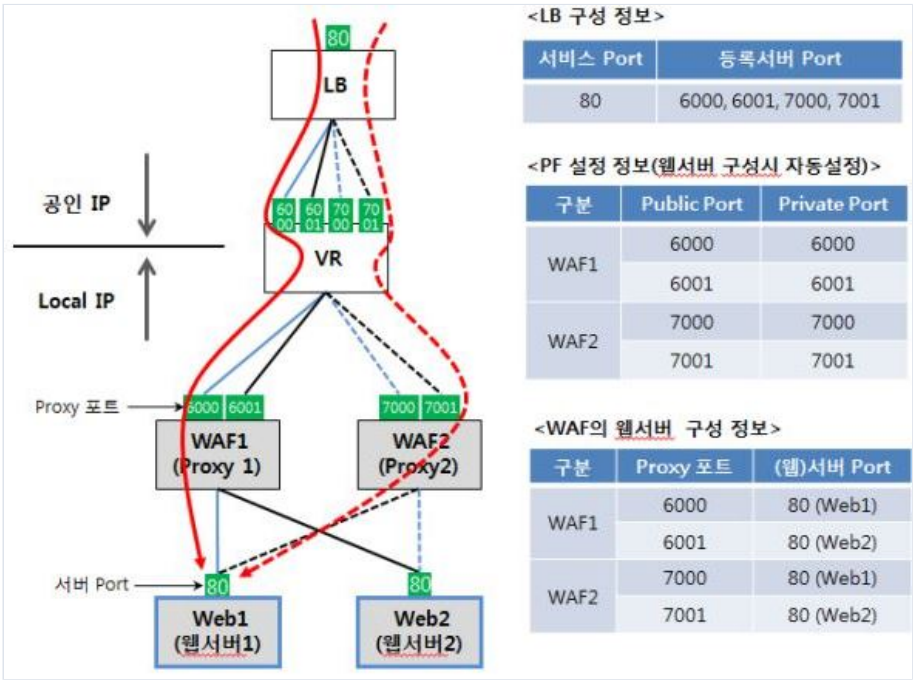
위와 같이 설정시 로드밸런서는 다음과 같이 자동으로 설정됩니다.



적용 서버

서버	Public IP	Public Port	Throughput	Server connections	TTFB	Request	상태
test0914-VM1 (194db21...)	211.252.84.73	7001	0 (Mbps)	0	0	0	DOWN
test0914-VM1 (47dcfcd...)	211.252.84.73	7000	0 (Mbps)	0	0	0	UP
waf5stdtest-VM1 (194db21...)	211.252.84.73	6001	0 (Mbps)	0	0	0	DOWN
waf5stdtest-VM1 (47dcfcd...)	211.252.84.73	6000	0 (Mbps)	0	0	0	UP

위와 같이 적용한 구성도는 아래와 같습니다.



<LB 구성 정보>

서비스 Port	등록서버 Port
80	6000, 6001, 7000, 7001

<PF 설정 정보(웹서버 구성시 자동설정)>

구분	Public Port	Private Port
WAF1	6000	6000
	6001	6001
WAF2	7000	7000
	7001	7001

<WAF의 웹서버 구성 정보>

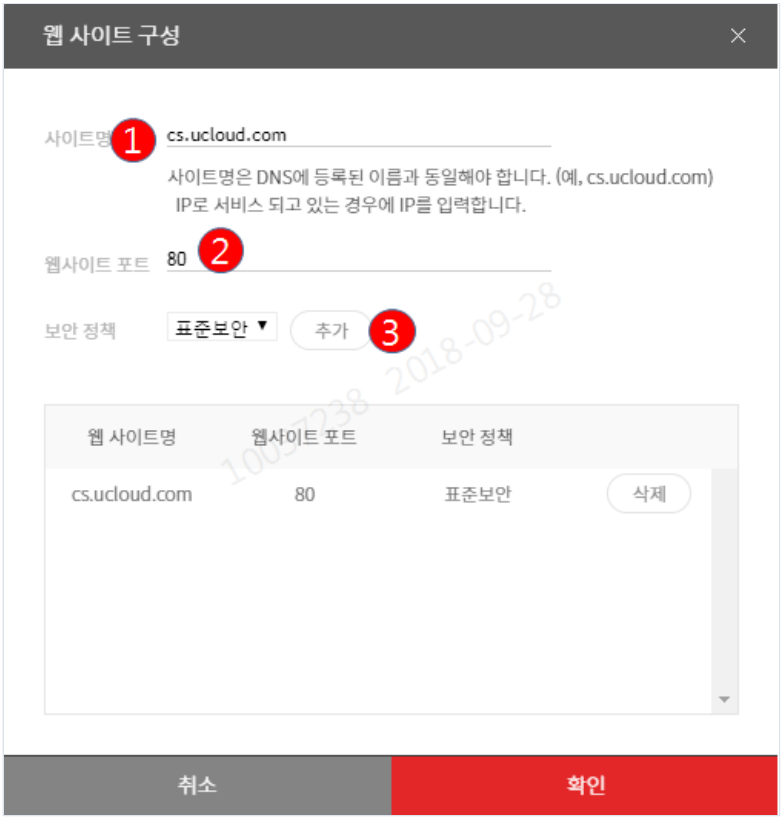
구분	Proxy 포트	(웹)서버 Port
WAF1	6000	80 (Web1)
	6001	80 (Web2)
WAF2	7000	80 (Web1)
	7001	80 (Web2)

▫ 웹사이트 구성

웹사이트 구성은 웹방화벽과 웹서버의 서비스 구성이 완료된 상태에서 웹서버를 보호하기 위해 웹서비스의 HTTP/HTTPS 메시지에서 사용되는 IP 또는 URL를 이용하여 설정 합니다. 즉, WAF에서 해당 웹서버로 연결되는 트래픽의 메시지 헤더 내용이 웹사이트 등록된 내용과 일치하여야 하여, 일치하지 않을 경우는 웹 서비스가 차단 됩니다.

(1) 웹방화벽을 선택하고, 우측 상단의 Action 위치로 마우스 커서를 이동합니다.

(2) 웹사이트구성을 클릭합니다.



(1) 웹방화벽이 보호해야 하는 URI 또는 IP를 등록합니다. 웹방화벽에서는 ;HTTP(S)의 메시지를 체크하여 외부 공격을 차단하기 때문에 HTTP(S)의 메시지의 URI에 해당하는 부분을 웹사이트로 등록하여야 한다(Client에서 입력되는 URL과 동일하게)

(2) 웹사이트 포트를 입력합니다.

(3) 사이트를 보호할 보안정책을 선택한 후, 추가를 클릭하면, 아래에 입력 내용이 반영됩니다. 확인을 클릭하여 구성을 완료합니다.

보안정책은 웹방화벽 관리콘솔에서 세부 설정이 가능합니다. 보안 정책 수준에 의한 세부적인 탐지룰에 대한 이용 방법 및 탐지로그를 확인하는 방법은 관리도구 매뉴얼을 참고하시기 바랍니다. 로

드밸런서를 같이 이용하는 경우, 탐지로그에서 Client IP를 확인 할 수 있도록 웹서버와 LB에서 X-Forward-For 옵션 이용을 권장합니다.

▫ 참고. 보안 정책

기본 정책	설명
표준 보안 정책	기본 보안 정책보다 한 단계 높은 보안 수준의 정책으로, 일반적인 웹 환경에 가장 최적화된 보안 정책
기본 보안 정책	기본적인 웹 공격을 방어하기 위한 보안 정책으로, 대중화되고 영향도가 높은 웹 공격을 방어
탐지	기본적인 탐지 부분은 [기본 보안 정책]과 동일하나 탐지된 위반 행위에 대해 차단 하지 않는 정책
탐지 없이 통과	웹 사이트에 대한 보안 위반 탐지 행위를 전혀 하지 않는 정책

보안 정책이 통과로 되어 있을 경우에는 악의적인 트래픽을 차단할 수 없습니다. 서비스 트래픽 분석 최적화된 정책 적용 및 탐지 차단 정책 이용을 권장합니다.

1.4 웹방화벽 이용방법 - M2존 외

ucloud 포탈에서 WAF 서비스 구성 및 환경 설정하는 방법을 설명합니다. M2존 외의 존에 생성한 웹방화벽에 해당 하는 내용으로, M2존에 웹방화벽을 구성하신 경우 매뉴얼 1.3 항목을 참고하시기 바랍니다.

1.4.1 웹방화벽의 생성 및 삭제

WAF은 일반적으로 다음과 같은 설치 순서에 따라 웹 방화벽 신청 팝업 화면에서 서비스 구성을 합니다.
상품소개에서 보안 -> 웹 방화벽을 선택 -> 웹 방화벽 신청 버튼 클릭

▫ 1 단계 서비스 구성

(1) WAF가 생성되기를 원하는 AZ(Availabipty zone) 선택합니다.
(2) WAF 이름을 입력합니다.
(3) WAF 이름이 다른 VM의 이름과 중복되지 않는지 확인합니다.
(4) Single 선택, WAF 의 이중화 구성하고자 하는 경우는 Single 을 2 개 생성하여 구성합니다.
(5) 사양 : 필요 트래픽에 따라 상품(Basic, Standard, Advanced, Premium)을 선택합니다. 각 상품별 Throughput은 (200 / 300 / 500 / 700)이므로 서비스 최대 트래픽을 고려하여 상품 선택이 필요하며, 안정적 서비스를 위해 반드시 이중화 하여 구성할 것을 권고합니다.
(6) WAF가 사용하는 3개의 포트에 대한 포트포워딩 설정을 합니다. SSH 접속을 위한 22번 포트 / DB가 사용하는 5433번 포트 / 관리도구&API가 사용하는 5000번 포트 각각에 대한 공인 포트를 입력하면 됩니다.
(7) 포트포워딩 설정에 충돌이 없는지 포트 체크를 합니다.
고객의 웹서비스 환경에 따라 각 상품별 최대 throughput 은 달라질 수 있습니다.
다음 버튼을 클릭하여 신청내역 확인 단계로 넘어갑니다.

▫ 2 단계 신청 내역 확인

신청 내역을 확인하고 확인 버튼을 클릭 후 웹방화벽 서버가 생성 완료될 때까지 대기합니다.

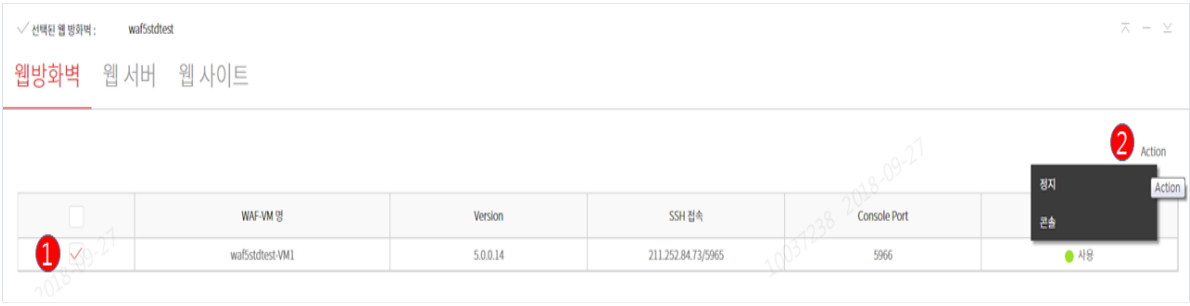
서버 생성 및 구성이 완료되면 WAF 상태가 준비 중에서 사용 상태로 변경되고 WAF 의 SSH 접속 패스워드가 팝업 됩니다. ucloud biz 포탈 email 계정의 메일을 확인하셔서, SSH 접속 패스워드를 다시 확인 할 수 있습니다.

WAF VM 의 삭제는 WAF VM 이 정지된 상태에서 Action 버튼을 클릭하여 삭제 가능합니다.
엔터프라이즈 존에 WAF VM 을 생성하는 경우에는 WAF 초기화 및 업데이트 정보를 가져올 수 있도록 3 개 IP (218.145.29.166, 218.145.29.168, 218.145.29.101)에 대한 방화벽 허용 설정이 필요 합니다.

1.4.2 WAF VM의 시작/정지, SSH 접속 비밀번호 변경

▫ 시작 / 정지

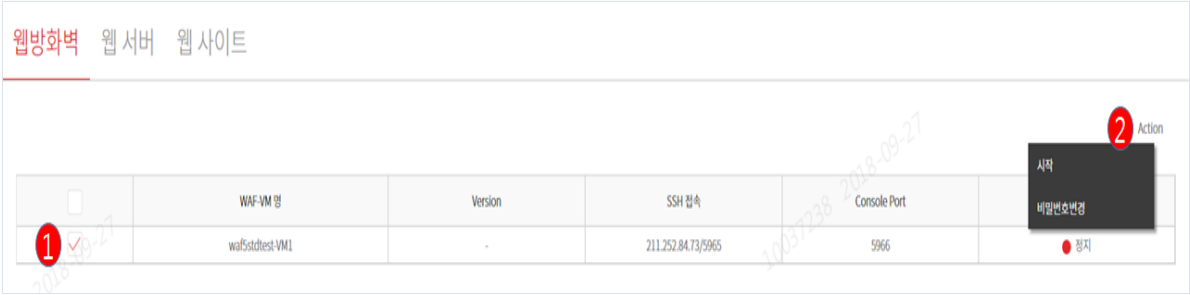
WAF 신청 시 자동으로 시작 상태가 됩니다. 특별한 사유에 의해 WAF을 재부팅하고자 할 때 다음과 같이 정지/시작 할 수 있습니다.



(1) 웹방화벽 선택 후, 우측 상단의 Action 위치에 마우스 커서 이동합니다.
(2) 정지 클릭 후, 웹방화벽 상태가 <정지>가 될 때까지 대기합니다.
웹방화벽 상태가 <정지>가 된 후, Action 위치에 마우스 커서를 이동하고, <시작> 클릭합니다.

▫ SSH 접속 비밀번호 변경

WAF은 주로 닷넷 기반의 관리도구 어플리케이션을 사용하여 관리하며, 상태 점검 등 특별한 경우, SSH 접속을 하여 관리할 수도 있습니다. SSH 접속 비밀번호는 다음과 같은 절차로 변경 가능합니다.



(1) 웹방화벽 선택 후, 우측 상단의 Action 위치에 마우스 커서 이동합니다.
(2) 비밀번호 변경 클릭 및 팝업 창에서 확인 클릭 시, 랜덤하게 비밀번호 변경됩니다.

1.3.3 웹서버 구성 및 웹사이트 구성

▫ 웹서버 구성

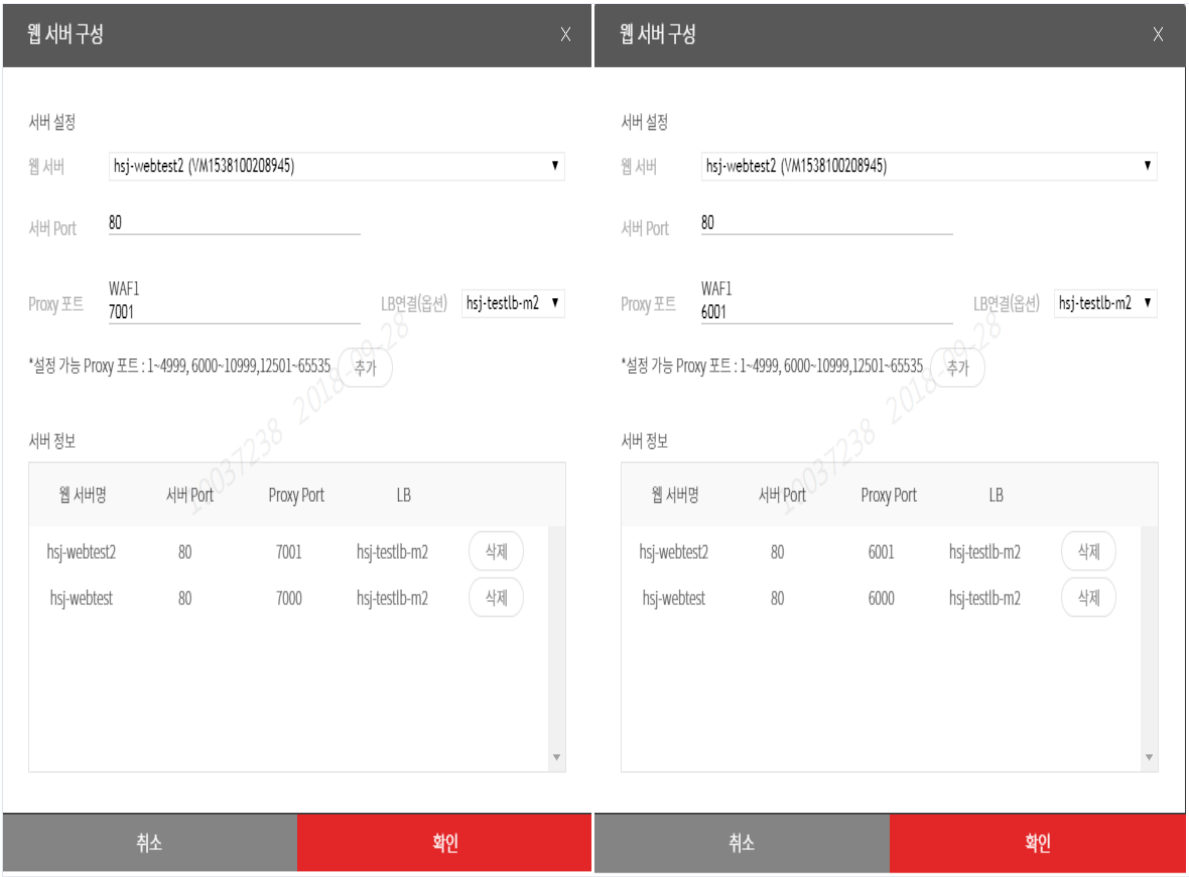
웹방화벽과 웹서버간의 서비스 구성작업을 실시 합니다.

(1) 구성하고자 하는 웹방화벽을 선택 후, 우측 상단의 Action 위치로 마우스 커서를 이동합니다.
(2) 웹서버 구성 클릭합니다.

웹방화벽이 2개의 웹서버를 보호하는 경우를 가정하여 설명합니다.

(1) 보호할 웹 서버를 선택합니다.
(2) 웹서버의 웹서비스 포트를 입력합니다.
(3) 웹방화벽의 Proxy 포트를 입력(트래픽은 웹방화벽IP:프록시포트 -> 웹서버IP:서비스포트 형태로 전달 됩니다.)
(4) 웹방화벽이 이중화 구성일 경우, 부하분산 처리할 로드밸런서를 선택해 줍니다. LB에 별도 설정 필요 없이, 여기서 입력되는 값 기준으로 LB와 WAF, 웹서버간 연결이 형성 됩니다.
(5) 설정값 입력이 완료 되었다면, 추가를 클릭하면 하단에 입력 정보가 반영됩니다.
(6) 입력값이 잘못된 경우, 삭제 후, 다시 입력할 수 있습니다.

*참고. 이중화 구성 예제
2개의 웹방화벽으로 2개의 웹서버를 보호하는 경우 아래와 같이 설정해 줍니다. (서버 포트는 80을 가정합니다.)

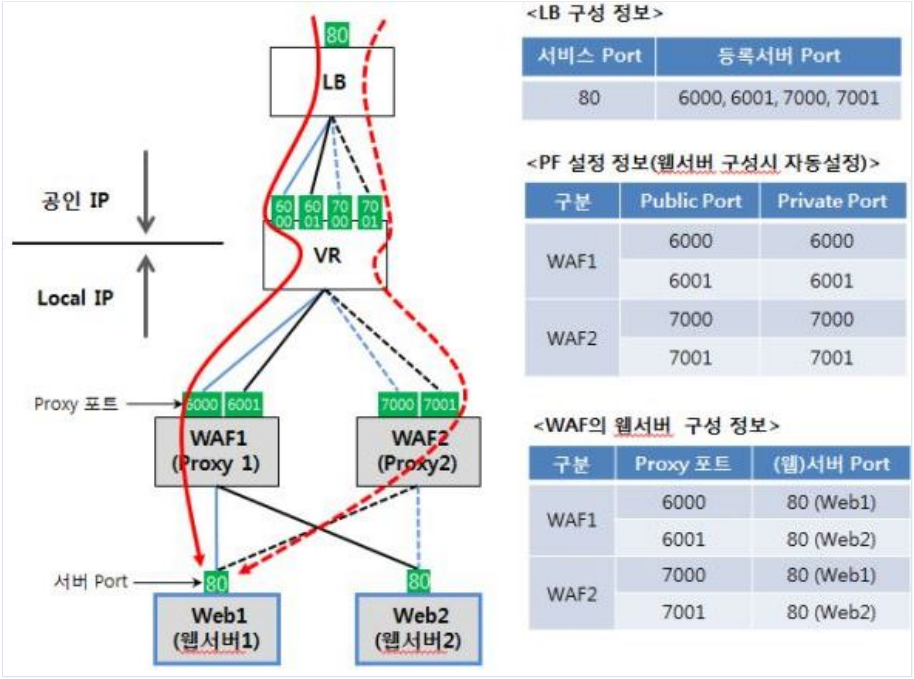


위와 같이 설정시 로드밸런서는 다음과 같이 자동으로 설정됩니다.

적용 서버

서버	Public IP	Public Port	Throughput	Server connections	TTFB	Request	상태
test0914-VM1 (194db21...)	211.252.84.73	7001	0 (Mbps)	0	0	0	DOWN
test0914-VM1 (47dcfcd...)	211.252.84.73	7000	0 (Mbps)	0	0	0	UP
waf5stdtest-VM1 (194db21...)	211.252.84.73	6001	0 (Mbps)	0	0	0	DOWN
waf5stdtest-VM1 (47dcfcd...)	211.252.84.73	6000	0 (Mbps)	0	0	0	UP

위와 같이 적용한 구성도는 아래와 같습니다.



<LB 구성 정보>

서비스 Port	등록서버 Port
80	6000, 6001, 7000, 7001

<PF 설정 정보(웹서버 구성시 자동설정)>

구분	Public Port	Private Port
WAF1	6000	6000
	6001	6001
WAF2	7000	7000
	7001	7001

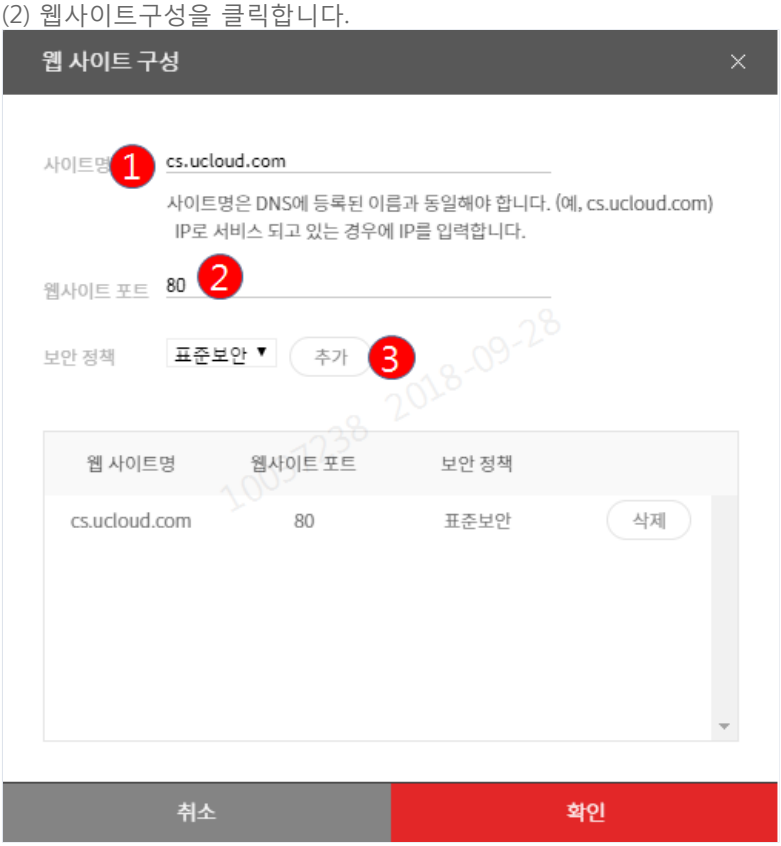
<WAF의 웹서버 구성 정보>

구분	Proxy 포트	(웹)서버 Port
WAF1	6000	80 (Web1)
	6001	80 (Web2)
WAF2	7000	80 (Web1)
	7001	80 (Web2)

▫ 웹사이트 구성

웹사이트 구성은 웹방화벽과 웹서버의 서비스 구성이 완료된 상태에서 웹서버를 보호하기 위해 웹 서비스의 HTTP/HTTPS 메시지에서 사용되는 IP 또는 URL를 이용하여 설정 합니다. 즉, WAF에서 해당 웹서버로 연결되는 트래픽의 메시지 헤더 내용이 웹사이트 등록된 내용과 일치하여야 하여, 일치하지 않을 경우는 웹서비스가 차단 됩니다.

(1) 웹방화벽을 선택하고, 우측 상단의 Action 위치로 마우스 커서를 이동합니다.
(2) 웹사이트구성을 클릭합니다.



(1) 웹방화벽이 보호해야 하는 URI 또는 IP를 등록합니다. 웹방화벽에서는 HTTP(S)의 메시지를 체크하여 외부 공격을 차단하기 때문에 HTTP(S)의 메시지의 URI에 해당하는 부분을 웹사이트로 등록하여야 한다(Client에서 입력되는 URL과 동일하게)
(2) 웹사이트 포트를 입력합니다.
(3) 사이트를 보호할 보안정책을 선택한 후, 추가를 클릭하면, 아래에 입력 내용이 반영됩니다. 확인을 클릭하여 구성을 완료합니다.
보안정책은 웹방화벽 관리콘솔에서 세부 설정이 가능합니다. 보안 정책 수준에 의한 세부적인 탐지 룰에 대한 이용 방법 및 탐지로그를 확인하는 방법은 관리도구 매뉴얼을 참고하시기 바랍니다. 로드밸런서를 같이 이용하는 경우, 탐지로그에서 Client IP를 확인 할 수 있도록 웹서버와 LB에서 X-Forward-For 옵션 이용을 권장합니다.

*참고. 보안 정책

기본 정책	설명
표준 보안 정책	기본 보안 정책보다 한 단계 높은 보안 수준의 정책으로, 일반적인 웹 환경에 가장 최적화된 보안 정책
기본 보안 정책	기본적인 웹 공격을 방어하기 위한 보안 정책으로, 대중화되고 영향도가 높은 웹 공격을 방어
탐지	기본적인 탐지 부분은 [기본 보안 정책]과 동일하나 탐지된 위반 행위에 대해 차단 하지 않는 정책

탐지 없이 통과	웹 사이트에 대한 보안 위반 탐지 행위를 전혀 하지 않는 정책

보안 정책이 통과로 되어 있을 경우에는 악의적인 트래픽을 차단할 수 없으니,서비스 트래픽 분석 최적화된 정책 적용 및 탐지 차단 정책 이용을 권장합니다.

1.5 웹방화벽 관리도구 - M2존

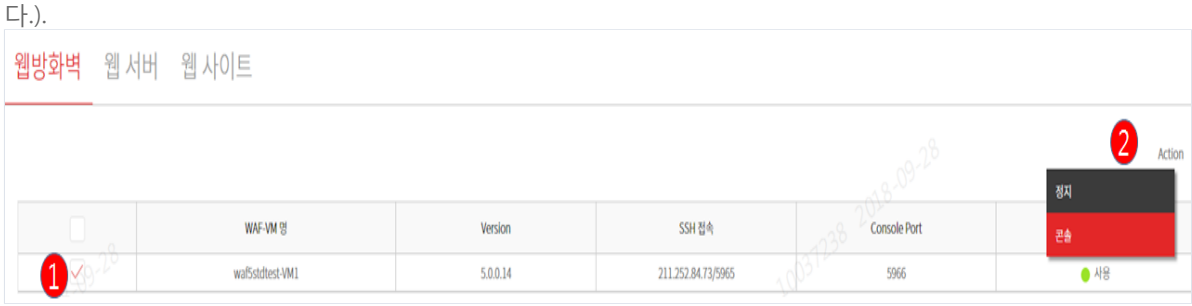
웹방화벽의 탐지 및 차단 정책 설정, 로그 확인, 환경 설정 등을 수행할 수 있는 관리도구를 제어 하는 방법을 설명합니다.
M2존 웹방화벽에 해당 하는 내용으로, 그 외 존에 웹방화벽을 구성하신 경우 매뉴얼 1.6 항목을 참고하시기 바랍니다.
*(2018년 8월 31일 이전 M2존에 생성한 웹방화벽의 경우에도 1.6 항목 참고)

본 장에서는 관리도구에 대한 간략한 사용법을 안내하며, 세부적인 관리를 위한 상세 매뉴얼은 다음 링크를 클릭하여 PDF 파일을 열람하시기 바랍니다.

***상세 매뉴얼 링크 : M2존 웹방화벽 관리콘솔 매뉴얼**

ㅁ 1 단계 관리도구 실행

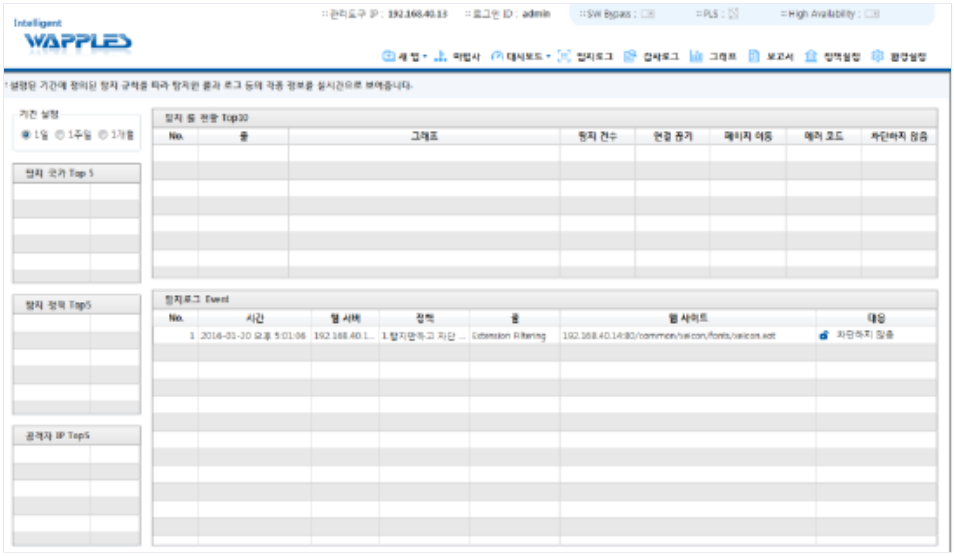
웹방화벽 관리도구는 웹서비스 구성 및 보안 탐지 룰셋을 세부적으로 설정할 때 이용할 수 있으며, 익스플로러(IE) 웹브라우저를 이용하여 접속 가능합니다.(.net을 이용하고있어 다른 브라우저는 동작 하지 않습니다.).



(1) 관리도구를 실행할 웹방화벽을 선택하고, 우측 상단의 Action 위치에 마우스 커서를 이동합니다.
(2) 콘솔을 클릭합니다. 만약 Chrome을 사용 중이라면, 콘솔 클릭 후, 브라우저의 주소를 복사하여, 인터넷 익스플로어 주소 창에 동일하게 입력해 줍니다.

상단의 화면에서 시작 버튼을 클릭하면, WAF Console GUI S/W가 설치 되는 등의 절차를 거쳐 Console 접속 초기 화면이 실행됩니다. 만일 관리자의 PC에 .Net 4.5버전이 설치 되어 있지 않은 경우, 이를 먼저 설치한 후에 관리도구 프로그램을 실행합니다.

ID는 admin을 입력합니다.
비밀번호는 <penta7728>을 입력합니다. 상단의 <로그인 후 사용자 정보 수정> 체크박스를 클릭하여 비밀번호를 변경하시기 바랍니다.
접속 포트에는 포탈에서 웹방화벽 신청 시, 입력했던 API포트(공인포트)를 입력하면 됩니다.



성공적으로 로그인 될 경우, 위와 같은 관리도구가 실행 됩니다.
초기 비밀번호 설정 이후 재 접속 시 비밀번호 5회 입력 오류 발생 시, 관리 도구가 종료되며, 10분간 로그인 계정이 잠기게 됩니다.

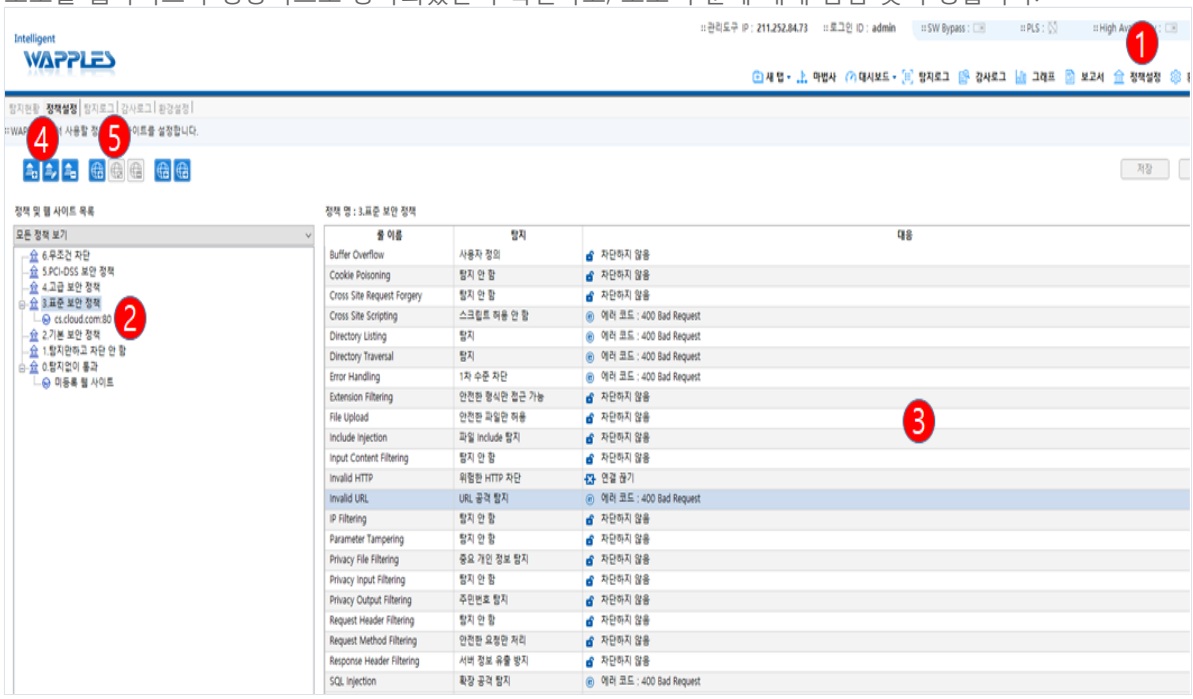
◘ 2 단계 웹서버 연결 점검

관리도구 실행 후, 웹서버와의 연결이 정상적으로 설정되었는지 확인합니다.

(1) 환결설정을 클릭합니다.
(2) 웹서버를 클릭합니다.
(3) WAF로 보호할 웹서버의 사설 IP와 서비스 포트가 정상적으로 등록되었는지 확인 합니다. 해당 화면에서 보호할 웹서버를 추가할 수도 있으나 이 경우, 클라우드 콘솔과의 정보 불일치가 발생하여 기술지원이 제약될 수 있으니, 보호할 웹서버의 등록은 클라우드 콘솔의 웹서버 구성 기능을 활용하여 주시기 바랍니다.

◘ 3 단계 웹사이트 정책 점검

보호할 웹사이트가 정상적으로 등록되었는지 확인하고, 보호 수준에 대해 점검 및 수정합니다.



(1) 정책 설정을 클릭합니다.
(2) 클라우드 콘솔에서 설정한 웹사이트가 정상적으로 등록되었는지, 원하는 정책 수준이 맞는지 확인합니다.
(3) 좌측에서 정책 리스트를 클릭하면, 해당 정책의 상세 내역을 확인할 수 있습니다. 각각의 공격 또는 정책에 대해 탐지 / 차단 / 에러메시지 발생 등 어떻게 대응할지 확인이 가능합니다.
(4) 기존 Default 정책을 기준으로 신규 정책을 생성한 후, Customizing 할 수 있습니다.
(5) 해당 화면에서 보호할 웹사이트를 추가할 수도 있으나 이 경우, 클라우드 콘솔과의 정보 불일치가 발생하여 기술지원이 제약될 수 있으니, 보호할 웹사이트의 등록은 클라우드 콘솔의 웹사이트 구성 기능을 활용하여 주시기 바랍니다.

1.5 웹방화벽 관리도구 - M2존 외

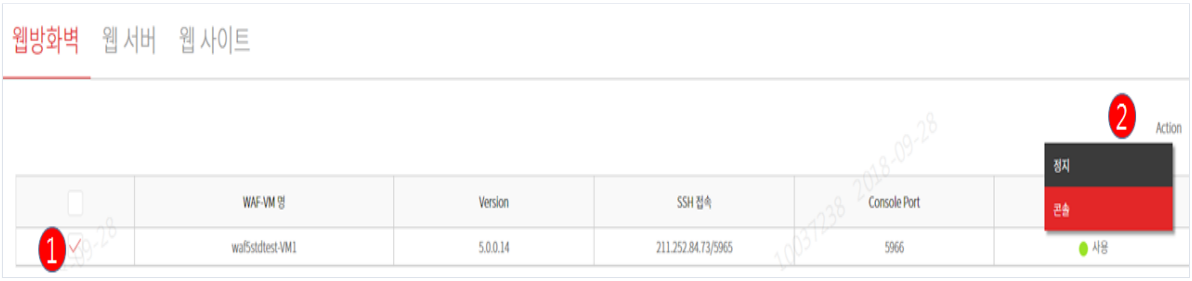
웹방화벽의 탐지 및 차단 정책 설정, 로그 확인, 환경 설정 등을 수행할 수 있는 관리도구를 제어 하는 방법을 설명합니다.
M2외의 존에 구성된 웹방화벽에 해당 하는 내용으로, M2존에 웹방화벽을 구성하신 경우 매뉴얼 1.5 항목을 참고하시기 바랍니다.
*(2018년 8월 31일 이전 M2존에 생성한 웹방화벽의 경우에는 본 장을 참고)

본 장에서는 관리도구에 대한 간략한 사용법을 안내하며, 세부적인 관리를 위한 상세 매뉴얼은 다음 링크를 클릭하여 PDF 파일을 열람하시기 바랍니다.

***상세 매뉴얼 링크 :** M2존 외 웹방화벽 관리콘솔 매뉴얼

ㅁ 1 단계 관리도구 실행

웹방화벽 관리도구는 웹서비스 구성 및 보안 탐지 룰셋을 세부적으로 설정할 때 이용할 수 있으며, 익스플로러(IE) 웹브라우저를 이용하여 접속 가능합니다.(.net을 이용하고있어 다른 브라우저는 동작 하지 않습니다.).



(1) 관리도구를 실행할 웹방화벽을 선택하고, 우측 상단의 Action 위치에 마우스 커서를 이동합니다.
(2) 콘솔을 클릭합니다. 만약 Chrome을 사용 중이라면, 콘솔 클릭 후, 브라우저의 주소를 복사하여, 인터넷 익스플로어 주소 창에 동일하게 입력해 줍니다.

상단의 화면에서 시작 버튼을 클릭하면, WAF Console GUI S/W가 설치 되는 등의 절차를 거쳐 Console 접속 초기 화면이 실행됩니다. 만일 관리자의 PC에 .Net 4.0버전이 설치 되어 있지 않은 경우, 이를 먼저 설치한 후에 관리도구 프로그램을 실행합니다.

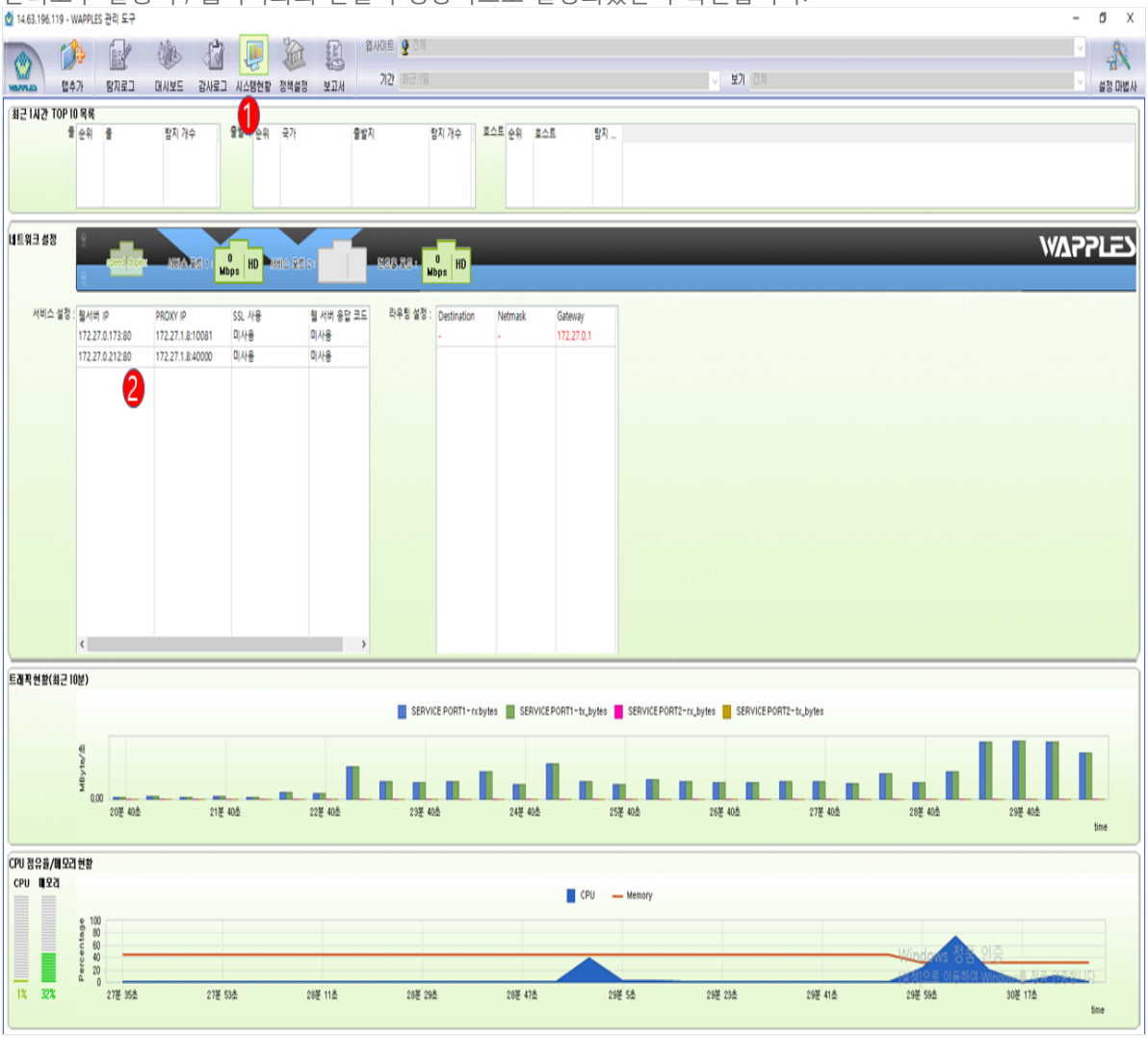
ID는 admin을 입력합니다.
비밀번호는 <penta>를 입력합니다. <로그인 후 사용자 정보 수정> 체크박스를 클릭하여 비밀번호를 변경하시기 바랍니다.
클라우드 콘솔에서 웹방화벽 신청 시, 입력했던 DB와 SSH 공인 포트를 입력한 후, 확인을 클릭하여 로그인합니다.

성공적으로 로그인 될 경우, 위와 같은 관리도구가 실행 됩니다.
초기 비밀번호 설정 이후 재 접속 시 비밀번호 3회 입력 오류 발생 시, 관리 도구가 종료되며, 10분간 로그인

계정이 잠기게 됩니다.

◘ 2 단계 웹서버 연결 점검

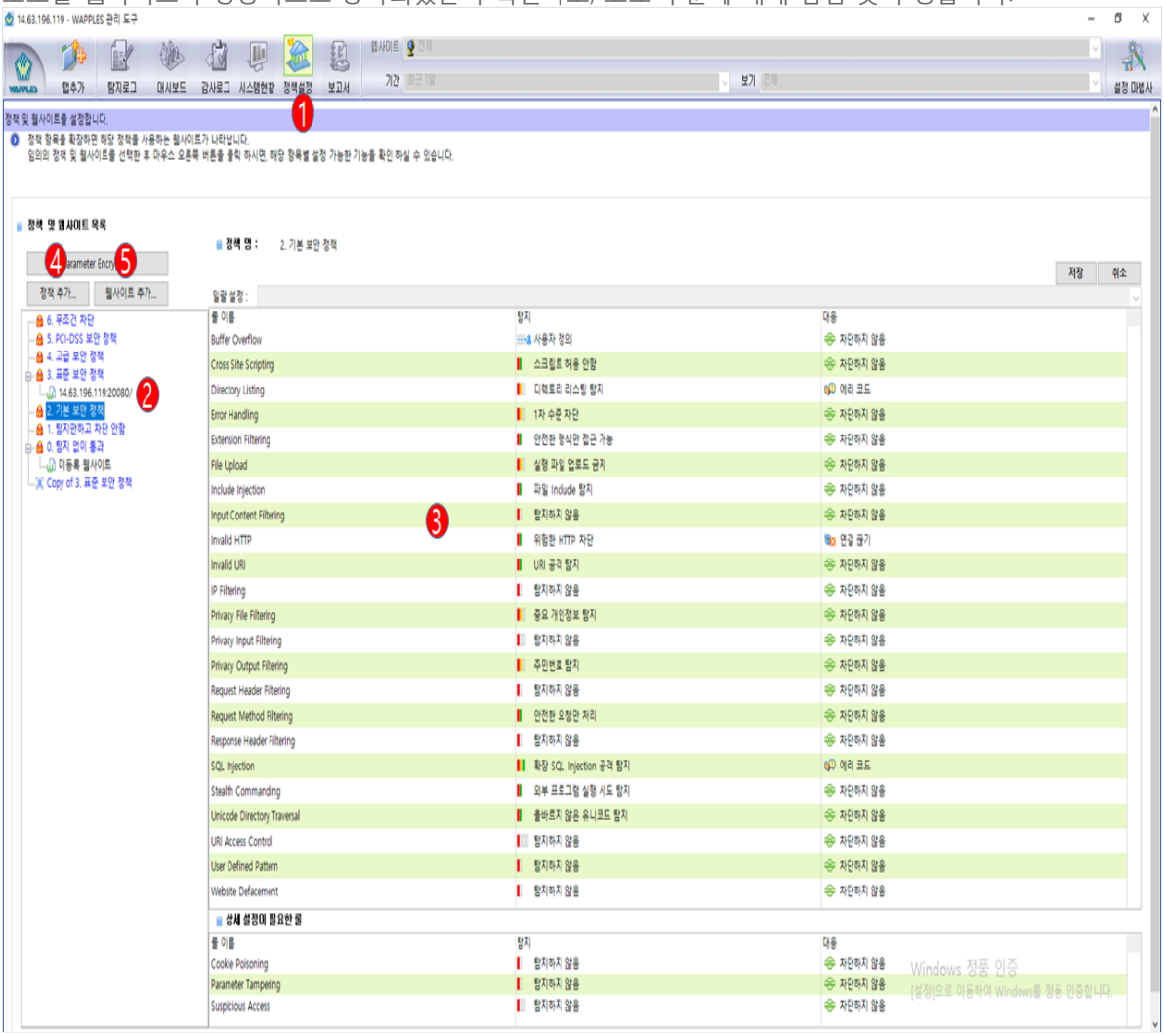
관리도구 실행 후, 웹서버와의 연결이 정상적으로 설정되었는지 확인합니다.



(1) 시스템 현황을 클릭합니다.
(2) WAF로 보호할 웹서버의 사설 IP와 서비스 포트가 정상적으로 등록되었는지 확인 합니다.

◘ 3 단계 웹사이트 정책 점검

보호할 웹사이트가 정상적으로 등록되었는지 확인하고, 보호 수준에 대해 점검 및 수정합니다.



(1) 정책 설정을 클릭합니다.
(2) 클라우드 콘솔에서 설정한 웹사이트가 정상적으로 등록되었는지, 원하는 정책 수준이 맞는지 확인합니다.
(3) 좌측에서 정책 리스트를 클릭하면, 해당 정책의 상세 내역을 확인할 수 있습니다. 각각의 공격 또는 정책에 대해 탐지 / 차단 / 에러메시지 발생 등 어떻게 대응할지 확인이 가능합니다.
(4) 기존 Default 정책을 기준으로 신규 정책을 생성한 후, Customizing 할 수 있습니다.
(5) 해당 화면에서 보호할 웹사이트를 추가할 수도 있으나 이 경우, 클라우드 콘솔과의 정보 불일치가 발생하여 기술지원이 제약될 수 있으니, 보호할 웹사이트의 등록은 클라우드 콘솔의 웹사이트 구성 기능을 활용하여 주시기 바랍니다.

1.7 모니터링 및 서비스 이상 시 진단 방법

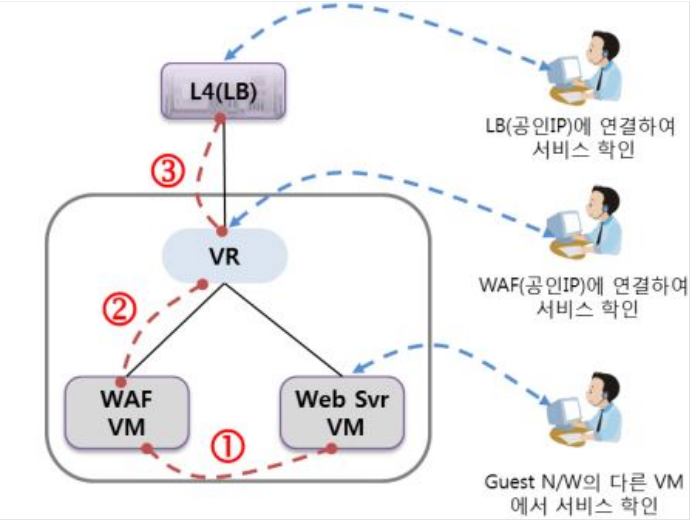
▫ WAF 서비스 구성 단계별 서비스 상태 체크

LB를 이용하는 경우는 WAF 서비스 구성이 복잡하고 서비스 접속 오류 원인을 찾기 어렵기 때문에 서비스 구성 계층별로 구분에서 확인이 가능합니다. 서비스 구성 단계별로 공인IP 또는 로컬IP(172.27.x.x)로 웹서비스 요청 테스트를 통하여 각 단계에서의 접속 오류, 응답 지연/오류 등의 구성 상태를 확인 할 수 있습니다.

공인 IP를 이용하여 확인할 때는 Client에서 LB로 접속하는 경우와 WAF로 접속하는 경우에 IP의 포트 번호가 달라질 수 있기 때문에 WAF의 웹사이트 등록(포트 부분)도 동일하게 설정되어야 합니다 (그렇지 않을 경우 연결 안됨). 또한 로컬 IP를 이용하여 확인할 때는 동일한 VR 내에 있는 다른 VM을 이용하여야 합니다 (동일한 Guest N/W 내 VM). Client에서 WAF로 연결 접속하는 경우에 오류가 발생한다면 다음과 같이 상태를 체크해 볼 수 있습니다.

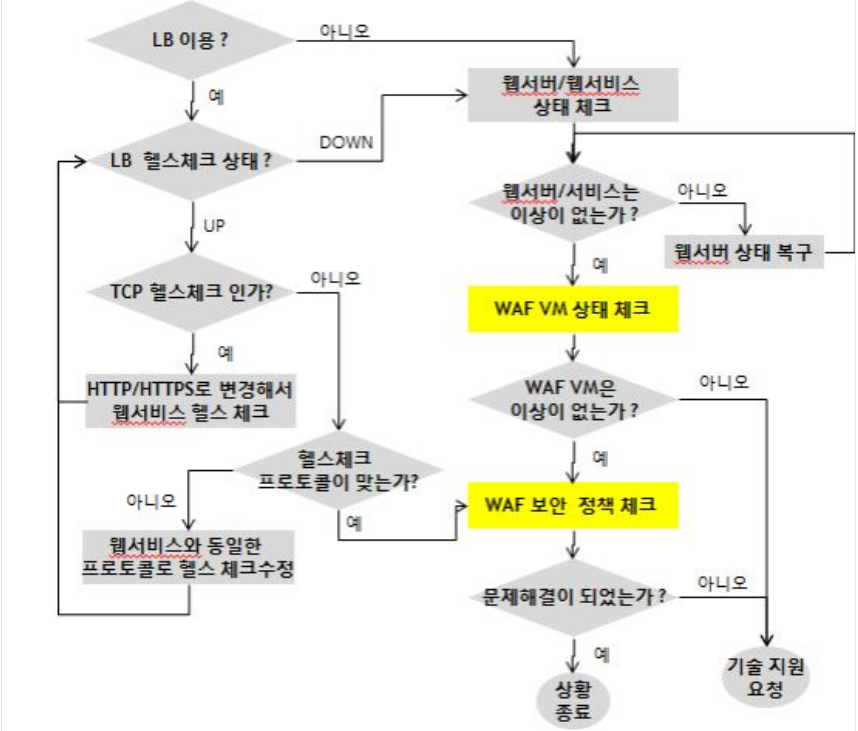
해당 URL 에 대한 웹방화벽의 정책설정 내용을 확인합니다.
관리도구 에서 해당 URL 에 대해 탐지로그에 남아 있는지 확인합니다.

관리도구 또는 WAF VM 에 접속하여 WAF 의 성능 상태를 확인해 봅니다.



구분	설정 확인 내용
WAF에서 웹서버 등록, 웹사이트 등록	웹서버 등록 (서비스 구성) - WAF 서비스 포트의 트래픽을 웹서버로 연결하는 설정 (VR에서 WAF로 포트 포워딩을 설정한 포토) 웹사이트 등록 (보호할 웹서버 등록) - 외부 공격으로부터 보호할 웹서버를 등록하는 것으로 HTTP(S)의 메시지에 이용되는 URI - 서비스에 이용되는 DNS 또는 IP 등록 - 등록되지 않은 DNS 또는 IP 서비스 도메인 트래픽은 차단됨 - 80 포트를 이용하지 않는 경우 포트까지 입력되어야 함 (ex, WAF에 연결하여 테스트하는 경우 - 80포트가 아닌 경우) - 방화벽 정책 설정에 따라 차단될 수 있는 경우는 모두 허용 정책으로 변경 후 확인
포트 포워딩 설정	공인 IP에서 접근할 수 있는 WAF 서비스 포트로의 포트 포워딩 설정 URL이 WAF IP:Port 형식으로 이용하여 접속하기 때문에 WAF의 웹사이트 등록도 WAF IP, Port를 등록하여야 함
LB 설정	LB를 이용하는 경우의 구성 - VR의 공인 IP를 이용하여 복수의 웹서버로 로드밸런싱 하기 때문에 로드밸런싱되는 각 패스를 포트로 구분 설정됨 (추가 할당된 IP를 이용할 경우는 해당 IP로 이용 가능) LB의 Health Check 기능을 이용한 상태 확인- WAF에서는 Health Check 트래픽을 Web 서버로 릴레이하는 역할 - TCP : 웹서버의 서비스 포트가 살아 있는지 상태 체크 WAF에서 웹서버가 등록 되어 있지 않거나 웹서버의 웹서버 프로세스가 동작하고 않고 있으면 Down 상태 - HTTP : WAF에 웹사이트 등록(WAF IP)이 되어 있어야 함 웹사이트가 등록되지 않으면 미등록 웹사이트 차단 정책이 적용되어 Down 상태로 표시될 수 있음 (LB에서 헬스 체크하는 URL은 "WAF IP + 입력된 Path"와 같이 만들어짐) - HTTPS : HTTP와 동일하며, WAF에 인증서가 등록되어야 함 X-Forward-For 옵션을 이용한 Client IP 확인 - WAF에서 original source IP 확인을 위해서는 LB, 웹서버에서 X-Forward-For 옵션 설정 필요 X-Forward-For 옵션 설정 시 LB에서 WAF로 가는 트래픽의 Source IP는 LB가 되기 때문에 LB에서 original Client IP를 추가해서 전송함

▫ LB 헬스체크에 의한 WAF 상태 체크



ㅇ WAF VM 상태 체크 방법

WAF VM에 접속하여 CLI(Command Line Interface) 명령어 모드로 변경한 후 CLI 명령로 WAF 프로세스 상태(sysmon)과 Disk 용량의 상태를 확인합니다.

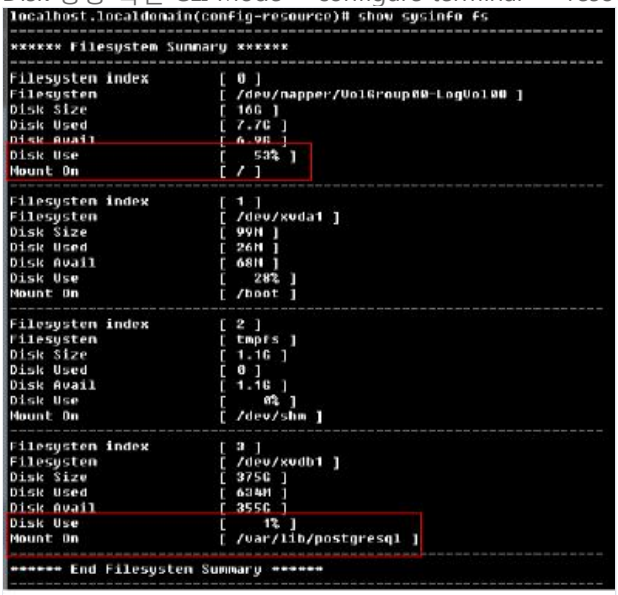
CLI 모드 변경 방법(상세 내용은 WAF 관리도구 매뉴얼 참조)
1. WAF VM에 SSH 접속
2. CLI enable mode로 진입 (초기 상태: disable)
3. enable mode 진입 시, 패스워드는 penta

```
Using username "root".
Last login: Tue Nov 11 17:00:49 2014 from 14.63.253.162

Hello, This is Network-Platform CLI tool
COPYRIGHT 2014 PENTA SECURITY SYSTEMS INC. ALL RIGHTS RESERVED

localhost.localdomain> enable
password:
localhost.localdomain#
```

Sysmon status : 실시간 WAPPLES 리소스(CPU,MEM 점유율), DB 프로세스, DB 트랜잭션, 탐지엔진 상태, HTTP 트래픽 처리 현황, 세션 현황, Throughput 을 알 수 있다.CLI Mode > configure terminal -> wapples -> show sysmon

time : 로그 기록 시간
idl : 유휴 cpu 점유율, idle이 30 미만일 경우 과부하 상태로 볼 수 있음
sy : 시스템 점유율(세션처리 등에 할당됨)
io : 디스크 사용에 의한 CPU 점유율 (파일 복사, DB백업, 탐지로그 검색 등 디스크 사용시 점유율 증가)
free : free (전체 가용 메모리), free+cache 가 300 미만일 경우 비정상적인 상태
cache : DB등 프로세스가 임시로 사용 하고 있는 메모리 (drop_cache 실행 or 시스템에서 자동으로 반환가능)
pro : DB 프로세스 개수

engine : [N] – none (서비스 구동 중, 정책 적용 중에 카운트), [G] – good(정상), 숫자가 표시되지 않고 계속 변경될 경우 비정상적인 상태 [W] – warning (CPU사용율 80%이상) [F] – Full (CPU사용율 100%), [E] – error (에러 발생, coredump 생성, 생성 위치 : /var/tmp/coredump/)
cps : 실시간 CPS(connection per sec) 수치
tps : 실시간 TPS(transaction per sec) 수치
sess : 엔진이 처리 중인 세션
traKB : 엔진이 처리 중인 웹 트랜잭션
ses : 커널(네트워크)단에서 처리중인 세션
ses : buf : 커널 앞단에 잠시 대기중인 세션(지속적으로 증가 시 서비스 지연 발생함)
ses : Throughput (KB) : 전체 트래픽 량(양방향 총합, 웹 이외의 트래픽 포함)
Disk 용량 확인 CLI Mode > configure terminal -> resource -> show sysinfo fs



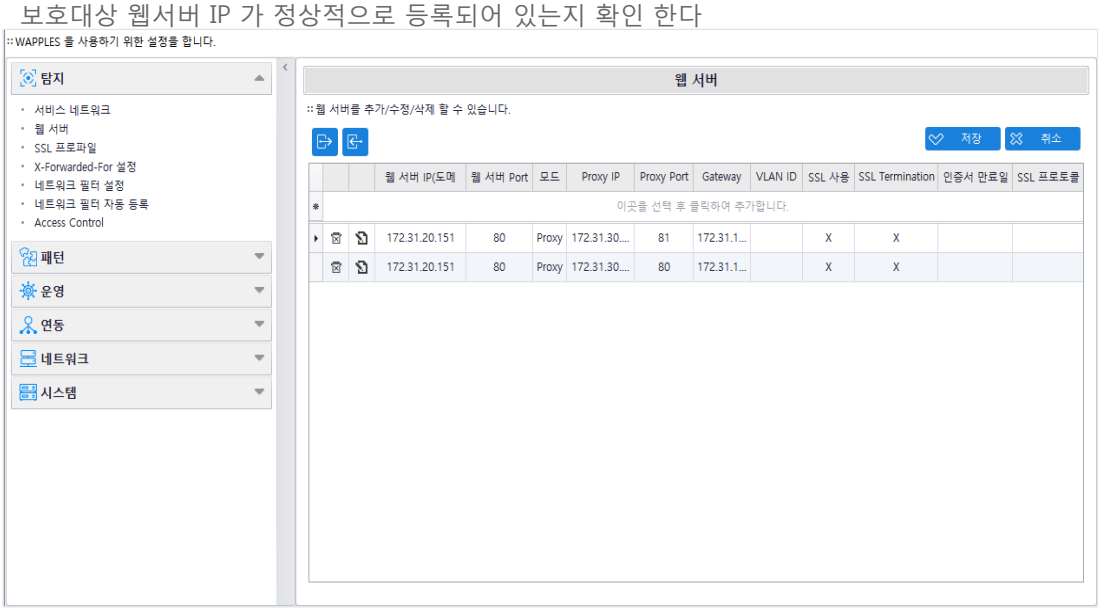
-> 빨간 박스 부분이 90% 이상 되는지 확인합니다.

ㅇ WAF 보안정책 체크 방법

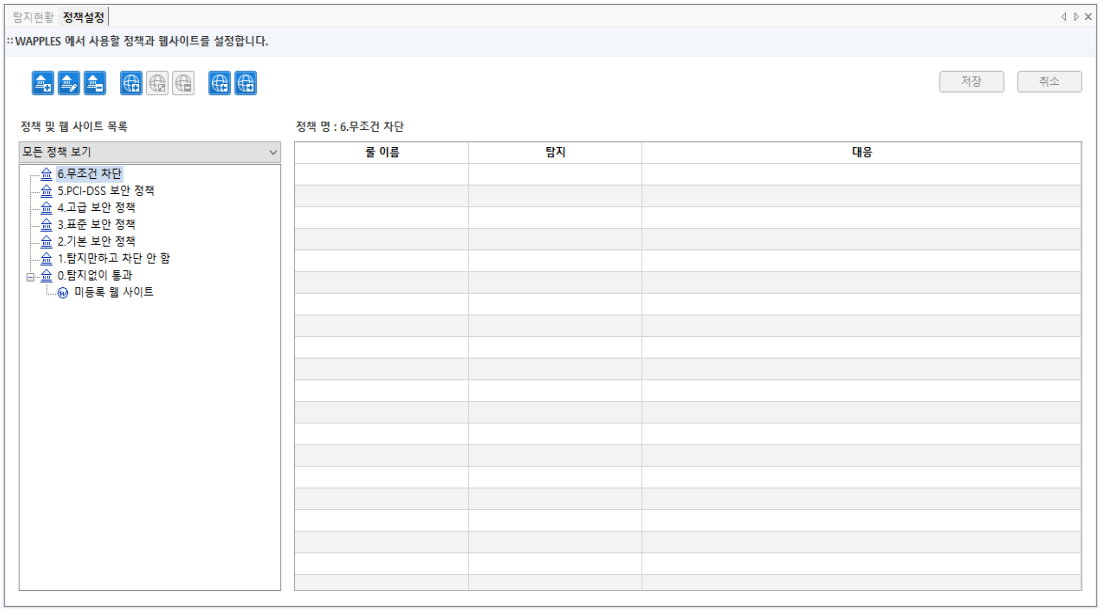
WAF 관리도구에 접속하여 WAF에 적용된 보안 정책을 체크합니다.

<M2존 WAF의 경우>

- 보호대상 서버 확인 : 관리도구 -> 환경설정 -> 웹서버
  보호대상 웹서버 IP 가 정상적으로 등록되어 있는지 확인 한다



- 보호대상 사이트 확인 : 관리도구 -> 정책설정
  보호대상 웹서버 IP 가 정상적으로 등록되어 있는지 확인합니다.

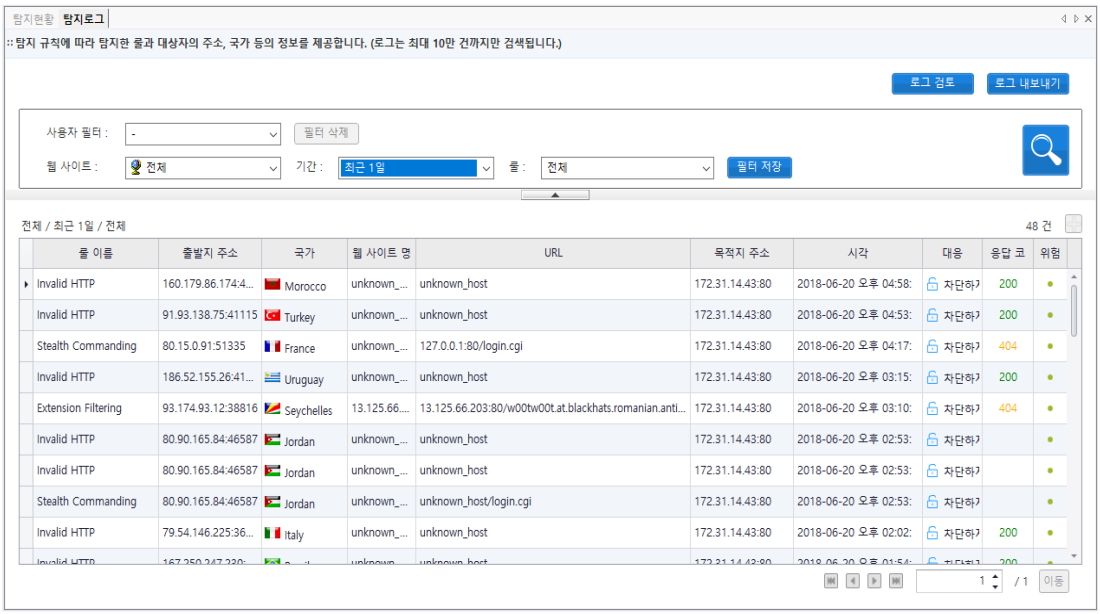


도메인이 정상적으로 입력되어져 있으며, 미등록 웹사이트의 위치를 확인합니다.

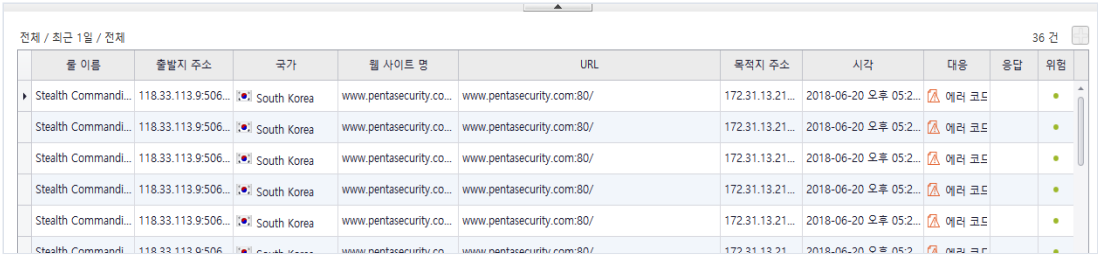
* 무조건 차단으로 설정될 경우 별도의 로그를 남기지 않고 차단됩니다. 서비스에 이용되는 웹사이트(도메인)을 추가를 하지 않을 경우 미등록 사이트로 구분됩니다 (80 포트를 이용하지 않을 경우 포트까지 입력되어야 합니다.)

* 탐지없이 통과 의 경우 탐지엔진을 거치지않고 트래픽이 웹 서버로 전달 됩니다.

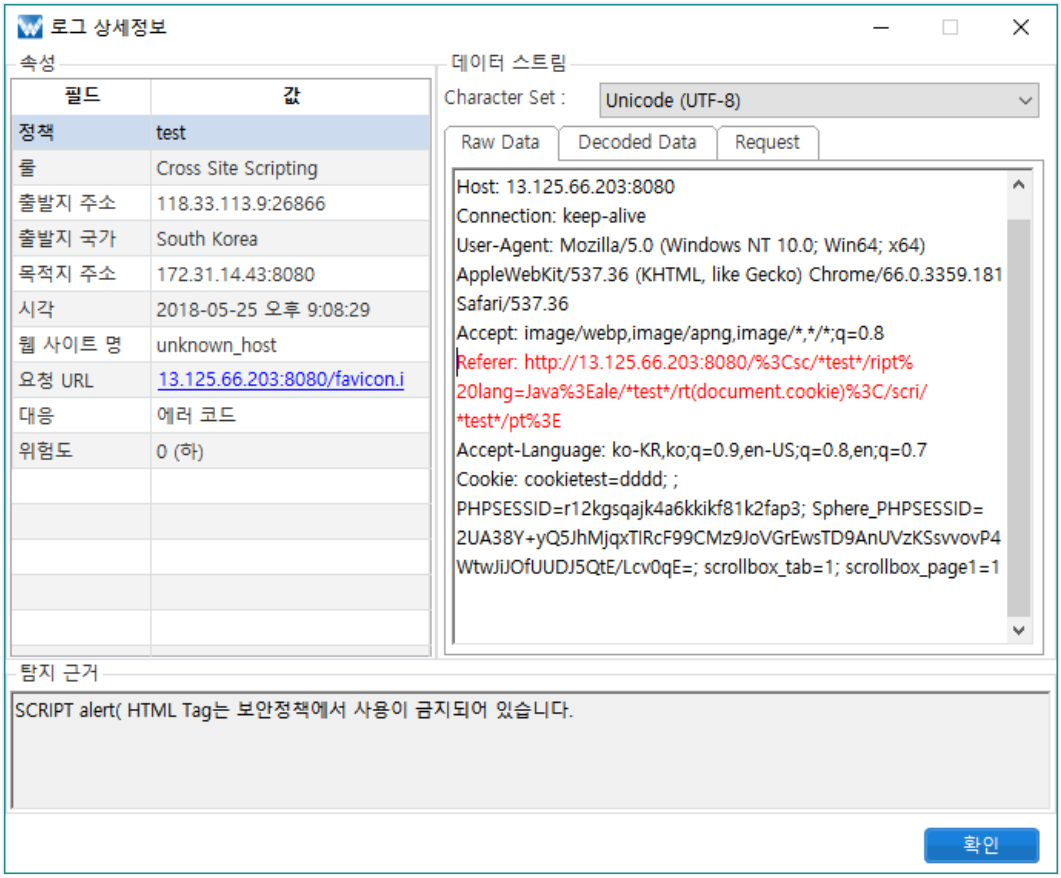
- 탐지로그 (미등록 웹사이트) 확인 관리도구 > 탐지로그



탐지로그 확인 (탐지로그 생성 여부) 관리도구 > 탐지로그



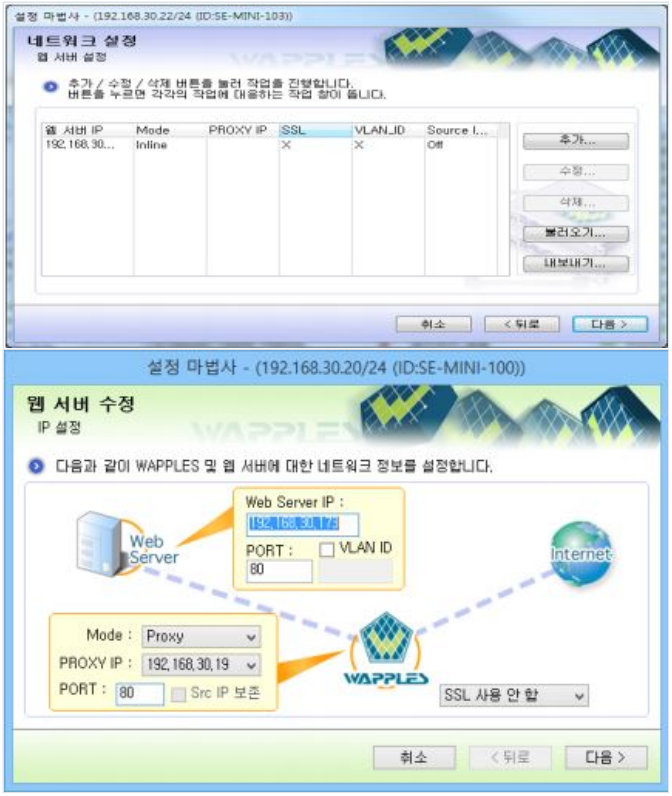
탐지상세로그에서는 탐지근거에서 대해 사용자가 손쉽게 식별이 가능하도록 붉은색으로 하이라이트 표시를 제공합니다.



Web Browser 를 이용 하여 아래와 같이 입력 후 탐지 Log 가 올라오는지 확인합니다.
http://서비스 URL/111.111 (Extension Filter)
http://서비스 URL/(script (Cross Site Script)

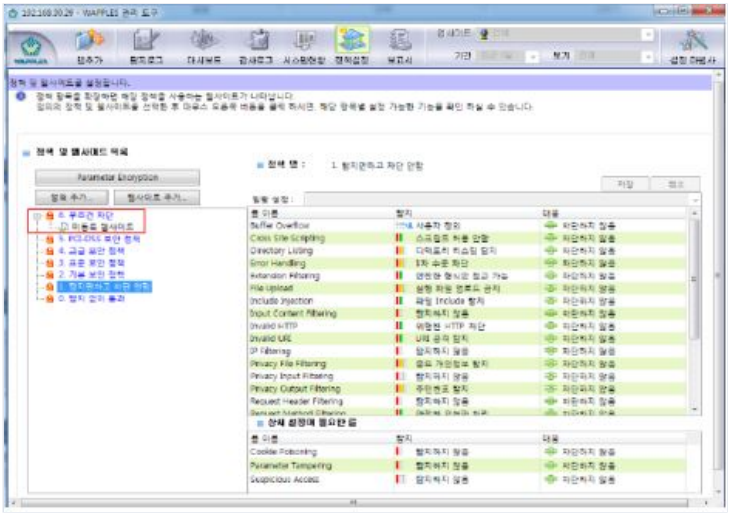
<M2존 외 WAF의 경우

- 보호 대상 서버 확인 : 관리도구 > 설정 마법사 > 네트워크 설정



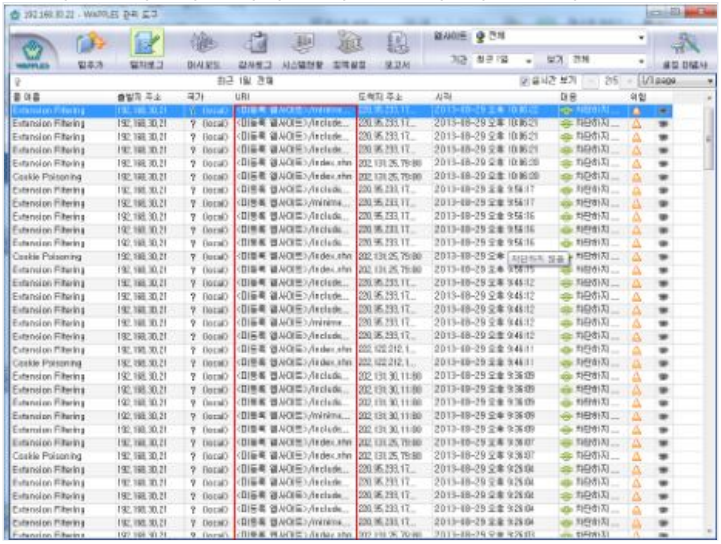
-> 보호대상 웹서버 IP 가 정상적으로 등록되어 있는지 확인합니다.

- 보호 대상 사이트 확인 : 관리도구 > 정책 설정



-> 미등록웹사이트가 차단으로 설정되어있는지 확인합니다.
* 무조건 차단으로 설정될 경우 별도의 로그를 남기지 않고 차단됩니다. 서비스에 이용되는 웹사이트(도메인)을 추가를 하지 않을 겨우 미등록 사이트로 구분됩니다(80 포트를 이용하지 않을 경우 포트까지 입력되어야 함)

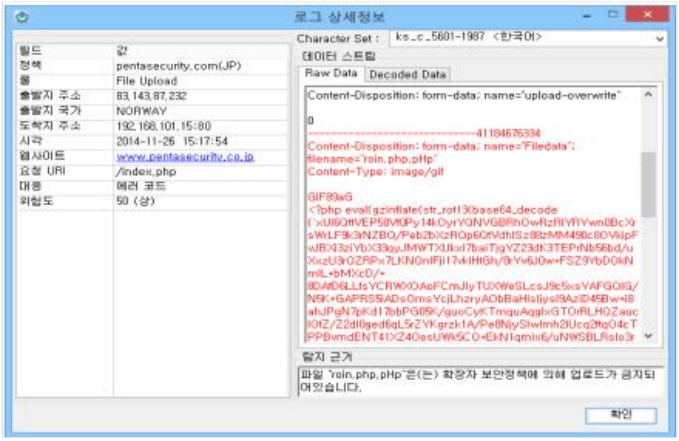
- 탐지로그(미등록 웹사이트) 확인 : 관리도구 > 탐지로그



-> 미등록웹사이트가 차단으로 설정되어있는지 확인합니다.
* 무조건 차단으로 설정될 경우 별도의 로그를 남기지 않고 차단됩니다.

- 탐지로그 확인(탐지로그 생성 여부)관리도구 > 탐지로그

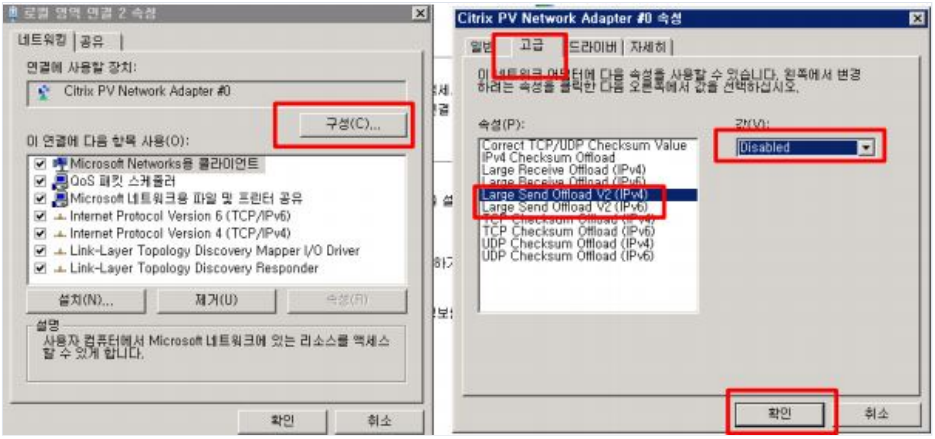
탐지상세로그에서는 탐지근거에서 대해 사용자가 손쉽게 식별이 가능하도록 붉은색으로 하이라이트 표시를 제공합니다.



-> Web Browser 를 이용 하여 아래와 같이 입력 후 탐지 Log 가 올라오는지 확인
http://서비스 URL/111.111 (Extension Filter)
http://서비스 URL/(script (Cross Site Script)

◘ 웹페이지가 느린 경우

점보 프레임 발생(WAF 4.0 이전 버전을 이용하고 있는 경우) 웹서비스에서 Large(점보) 패킷이 발생되는 경우 프레임 손상 및 흐름의 오류로 인하여 전송속도가 오히려 눈에 띄게 느려지거나 연결이 끊어지게 될 수 있습니다. WAF 버전을 최신 상태로 업데이트 할 경우, 점보 프레임 이슈는 해소 됩니다.
단, 업데이트는 서비스 중단이 필요하므로, 임시 방편으로 아래와 같이 설정하시기 바랍니다.
점보 프레임 발생을 방지하기 위하여 WAF에 연결되는 웹서의 네트워크에서 LSO(Large Send Offload) 옵션 설정을 disable로 하여야 합니다. 특히, 웹서버가 window OS인 경우 LSO 디폴트 옵션이 enable로 되어 있으므로 아래 그림과 같이 LSO를 disable로 변경하여야 한다.(네트워크 설정 -> 속성 -> 구성 -> 고급 탭 -> Large Send Offload disable-> 확인)



표준에 맞지 않도록 구현되어 있는 어플리케이션의 경우 WAF의 경우 RFC HTTP/1.1 표준 규격을 준수하도록 설계되어 있습니다. 허나, 해당 규격을 준수하지 않았을 경우 특정 페이지만 동일하게 늦게 열리는 경우가 발생합니다. 간헐적으로 느려지는 경우는 과부하로 발생되는 경우 외에는 발생할 수 없으며, 동일하게 반복적으로 계속 느려질 경우 원인 분석이 되어야 합니다.(기술지원 필요)

◘ (M2존 WAF의 경우에만 해당) 웹방화벽 Traffic을 웹서버로 bypass 처리

잘못된 정책 설정으로 인한 정상 트래픽 차단으로 인한 서비스 불가 또는, 과도한 트래픽 발생으로 인한 웹방화벽 과부하로 인한 서비스 지연 시,
웹방화벽의 탐지 및 차단 등 모든 동작을 중단하고, Traffic을 웹서버로 통과 처리하도록 하는 방법에 대해 설명 합니다.

- 웹방화벽에 SSH로 접속
- 로그인 후, enable 입력 -> password는 penta 입력
- configure terminal 입력
- bypass 입력
- sw-bypass set on 입력하여 bypass 기능 활성화
- show sw-bypass 입력하여 기능 실행 여부 확인
- bypass 설정을 끄고 정상화 할 때는 sw-bypass set off 입력

```
login as: root
root@211.252.84.73's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

Hello, This is Network-Platform CLI tool
COPYRIGHT 2018 PENTA SECURITY SYSTEMS INC. ALL RIGHTS RESERVED

VM-1233bb5c-4418-4942-8cc0-fba3a13190ea> enable
password:
VM-1233bb5c-4418-4942-8cc0-fba3a13190ea# configure terminal
VM-1233bb5c-4418-4942-8cc0-fba3a13190ea(config)# bypass
VM-1233bb5c-4418-4942-8cc0-fba3a13190ea(config-bypass)# show sw-bypass
S/W Bypass Status : Disable
VM-1233bb5c-4418-4942-8cc0-fba3a13190ea(config-bypass)# sw-bypass set on
Set OK
VM-1233bb5c-4418-4942-8cc0-fba3a13190ea(config-bypass)# show sw-bypass
S/W Bypass Status :  Enable
```

1.9 웹방화벽 시스템 업데이트 가이드

웹방화벽의 안정적 운용을 위해 주기적으로 업데이트를 확인하고, 최신 버전을 유지해 주어야 합니다.

업데이트 방식은 자동 업데이트 / 관리자 승인 후 업데이트 / 수동 업데이트의 3가지 방식이 있습니다.

대부분의 경우, 업데이트 시에 시스템 리부팅을 필요로 하기 때문에, 수동 업데이트를 권장합니다. 시스템의 초기 설정은 수동 업데이트입니다.

자동 업데이트 시, 일시적으로 웹방화벽의 서비스가 종료되어 웹서비스까지 트래픽이 넘어가지 못하기 때문에, 자동 업데이트 설정은 하지 않기를 권고합니다.

▫ 사전 작업

1. 버전 정보 확인

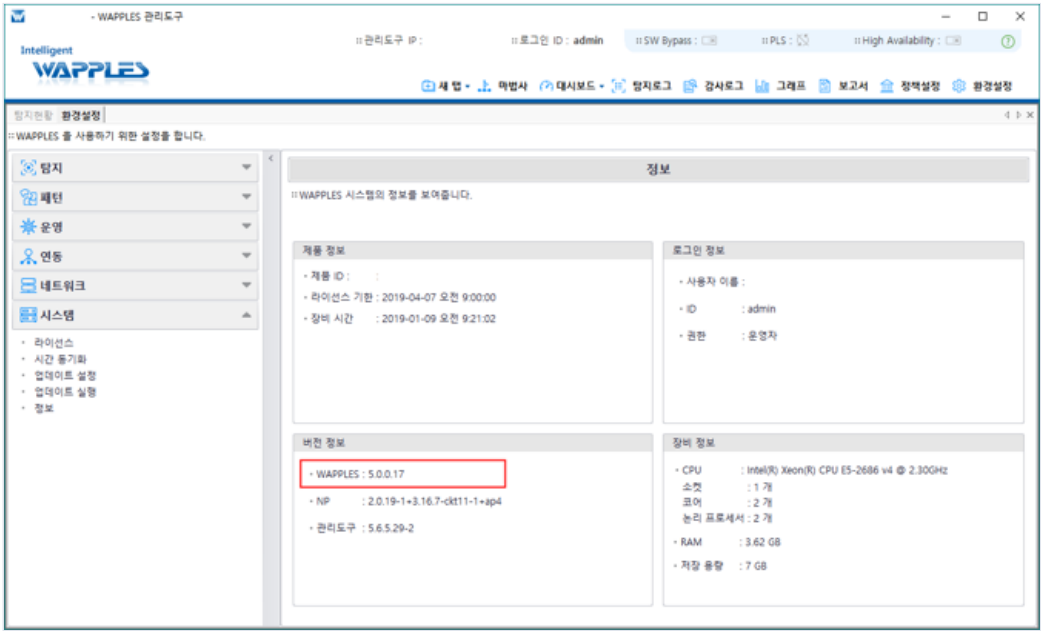
1) SSH 접속

- Enable 모드 접속(passwd : penta) -> configure terminal -> wapples -> show version

```
ip-172-31-20-136> en
password:
ip-172-31-20-136# conf t
ip-172-31-20-136(config)# wapples
ip-172-31-20-136(config-wapples)# show version

"WAPPLES Version" INFORMATION TABLE
-----------------------------------
WAPPLES:        5.0.0.17
```

2) 관리도구 접속

- [환경설정] > [시스템] > [정보] 에서 버전 정보 확인 가능



◈ 버전확인

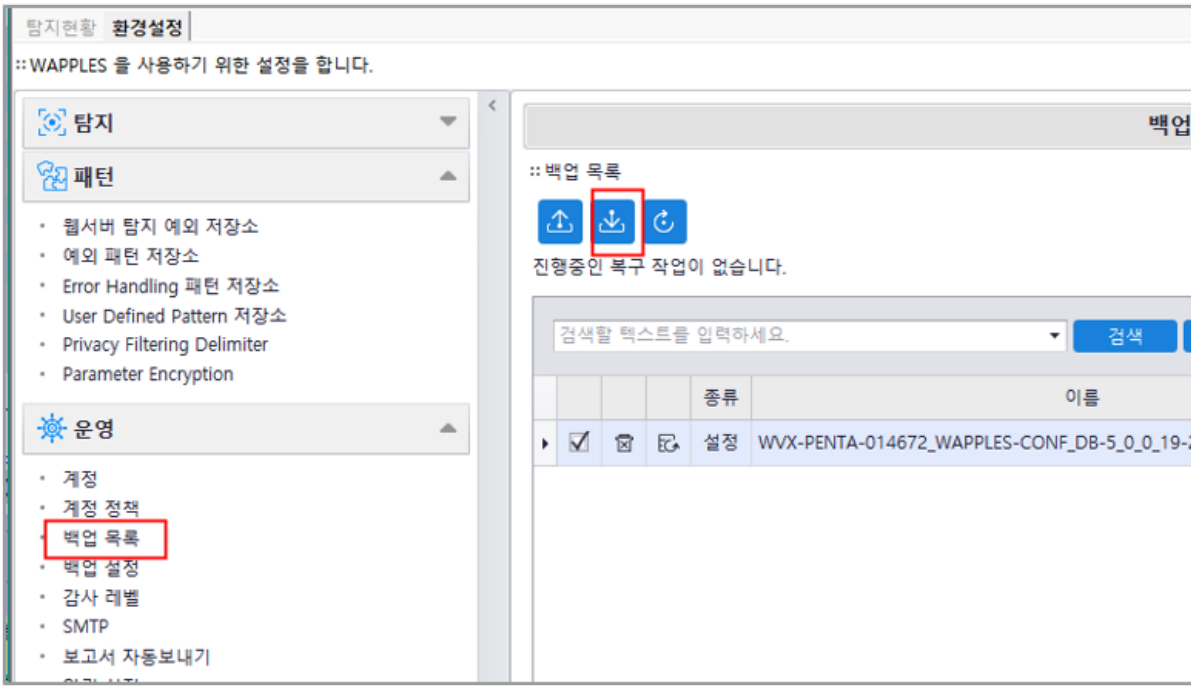
현재 최신버전은 **5.0.0.19**버전으로 5.0.0.19 미만 버전일 경우 온라인 업데이트를 이용해 주시기 바랍니다.

2. 설정 백업

- [환경설정] -> [운영] -> [백업 설정]
- [설정 DB 백업 설정] 활성화, [설정 완료 후 즉시 백업 실행]활성 후 저장 클릭

- [환경설정] -> [운영] -> [백업 목록]

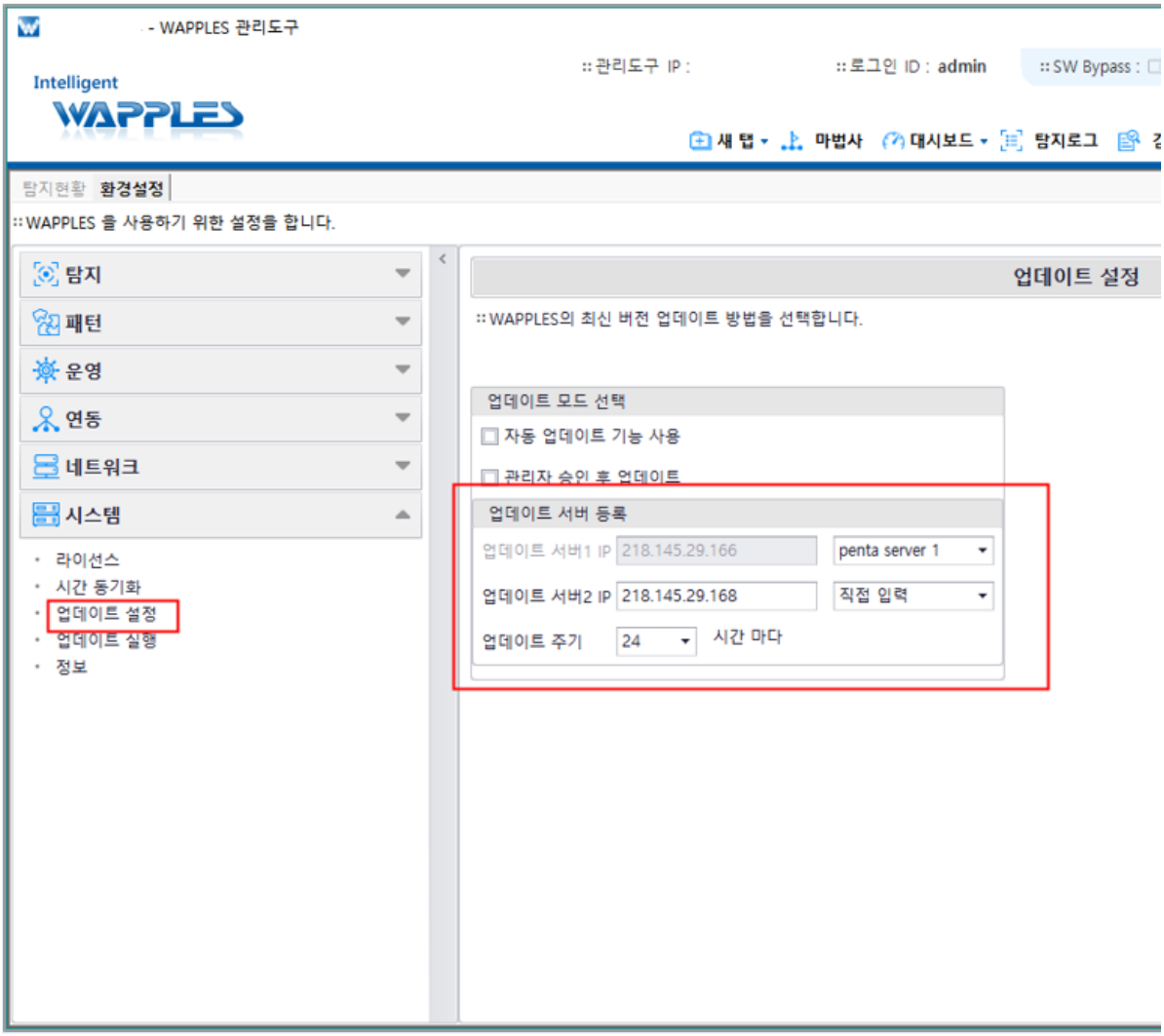
- 백업 된 파일 클릭 후 다운로드 아이콘 클릭하여 저장

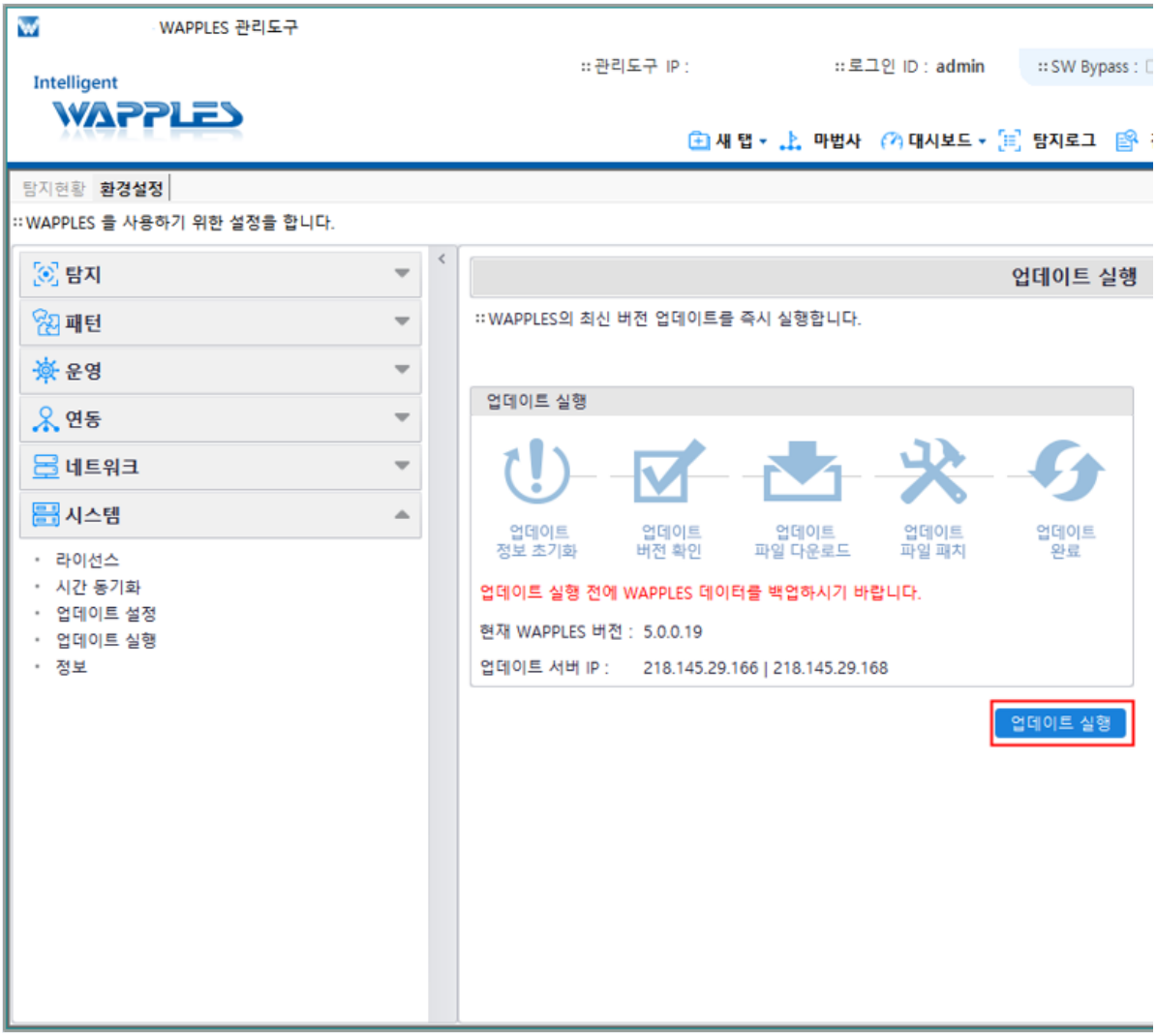


- 파일 다운로드 후 지속적인 백업이 필요 없다면 [백업 설정]에서 백업 비활성화 처리

3. 업데이트 설정

- [환경설정] -> [시스템] -> [업데이트 설정]
- 업데이트 서버(218.145.29.166 / 218.145.29.168) 지정 후 저장


- WAPPLES 관리도구
::관리도구 IP :
::로그인 ID : admin
::SW Bypass :
Intelligent
WAPPLES
새 탭
마법사
대시보드
탐지로그
탐지현황
환경설정
::WAPPLES 을 사용하기 위한 설정을 합니다.
탐지
패턴
운영
연동
네트워크
시스템
라이선스
시간 동기화
업데이트 설정
업데이트 실행
정보
업데이트 설정
::WAPPLES의 최신 버전 업데이트 방법을 선택합니다.
업데이트 모드 선택
자동 업데이트 기능 사용
관리자 승인 후 업데이트
업데이트 서버 등록
업데이트 서버1 IP
218.145.29.166
penta server 1
업데이트 서버2 IP
218.145.29.168
직접 입력
업데이트 주기
24
시간 마다



▫ 주의사항

1. 온라인업데이트 작업 시간

1) 온라인업데이트의 경우 해당 WAPPLES의 환경에 따라 소요 시간이 달라짐

2) 소요 시간은 약 5분에서 20분까지 소요 될 수 있으며 평균적으로 10분 이내 작업 완료

3) 해당 시간 동안 WAF 서비스가 다운됩니다.

✓ LB-WAF-웹서버 구조에서, LB-웹서버로 트래픽 연동 구조를 변경한 후(또는 DNS에서 직접 웹서버를 바라보도록 설정), 업데이트 하시기 바랍니다.

2. 온라인업데이트 주의사항

1)온라인업데이트 실행 시 서비스 중단 발생

① 패치 후 VM 재부팅이 발생

② 서비스에 영향을 미칠 수 있으므로 서비스 중단이 가능한 시간에 업데이트 진행 필요

2)업데이트 진행 전 관리도구 내에서 정책 및 웹서버 설정 백업 실행

① 패치 후 VM 오류 발생시 신규 VM 생성 및 설정 복원을 통해 백업 파일로 이전과 같은 설정으로 WAPPLES 사용 가능

3. 장애 시 연락 방법

1) 온라인 업그레이드가 정상적으로 안되거나 업그레이드 시 지원이 필요 한 경우 KTucloud Techcenter로 VM 정보 문의

2) 긴급 장애 시 연락처

① Email : ws3@pentasecurity.com / 메일 제목 : [고객명] Ktucloud 웹방화벽 업그레이드 문의 로 메일 전송

② 전화번호 : 펜타시큐리티 1661-4020