WAF User Guide

강력한 클라우드 서비스, 엔클라우드24

목 차

1. 제품 정보

본 장은 WAF을 소개하는 장으로 제품의 주요기능 및 특징과 운영환경에 대해서 기술합니다

1.1 개요

WAF은 지능형 웹 애플리케이션 방화벽입니다. WAF은 웹서버 앞 단에 위치하여 외부로부터 들어오는 HTTP/HTTPS 프로토콜 트래픽을 감시합니다. 이때 웹 애플리케이션에 대한 악의적인 공격이 탐지되면 해당 공격이 웹 서버에 도달하기 전에 차단하는 역할을 수행합니다.

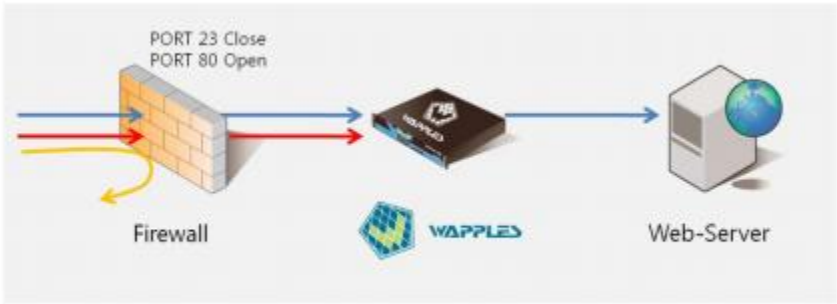


그림 1 WAF의 역할

[그림 1 WAF의 역할]이 보여주는 바와 같이 WAF은 방화벽(Firewall)에서 걸러주지 못하는 위험한 유해 트래픽을 웹 서버에 도달하지 못하도록 근본적으로 차단합니다. WAF은 고도로 지능화, 다양화되고 있는 웹 공격을 효율적으로 탐지 및 차단하여 안정적이고 신뢰할 수 있는 웹 애플리케이션의 운영을 가능하게 합니다

1.2 주요 보안기능

WAF은 다음과 같은 보안 기능을 제공합니다.

- HTTP 기반의 웹 공격 방지
- OWASP1 Top 10 Attacks 탐지 및 차단
- PCI-DSS Copliance 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

- Hidden Field 변조 방지
- 표준 암호 알고리즘 사용(AES, SEED)
- 웹 콘텐츠 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 입력시 자동 변환
  예) '나쁜말'(금지단어) -> '고운말'(등록된 표현)
- 해커에 의해 변조된 페이지 노출 차단 및 자동 복구

1.3 특징

WAF은 다음과 같은 특징을 가집니다.

보안성

- 웹 공격에 대한 3 중 방어 구조

WAF은 Positive Security 보안모듈의 "URI 접근 제어"와, Negative Security 보안 모듈의 "룰 탐지", White/Black list of IP 주소 관리기능인 "IP Filtering" / "IP Block"의 웹 클라이언트 접근 제어의 3중 방어 구조를 기반으로 확실하고 안정적인 웹 공격의 탐지와 차단을 제공합니다.

- 암호화 트래픽 지원

WAF은 SSL과 같은 암호화된 트래픽을 지원합니다. 암호화된 트래픽 내에 웹 공격이 들어있는 경우에도 이를 신속하게 복호화한 후에 공격을 탐지하여 차단할 수 있습니다.

성능

-다수 웹사이트/웹서버 동시 보호

WAF은 여러 웹사이트들과 다수의 웹 서버들을 동시에 보호하는 것이 가능합니다.

안정성

-Watchdog 지원

Watchdog 프로세스는 지속적이고 안정적인 웹 서비스 제공을 위해 WAF의 동작을 감시합니다. WAF에 문제가 발생하는 경우, watchdog 프로세스는 문제의 증상을 파악하고 이에 따라 보안 및 웹 서비스 유지를 위해 대응하도록 구성되어 있습니다.

편리성

- 대시보드 (Dashboard) 지원

WAF은 WAF과 웹 서버의 운영 상태를 그래프와 차트를 통해 한눈에 실시간으로 파악할 수 있는 대시보드 기능을 지원합니다. WAF의 대시보드는 22가지의 다양한 그래프와 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 수행할 수 있도록 도와줍니다. 자유롭고 유연한 화면 구성 WAF은 로그 화면과 각종 대시보드 화면 등을 메인 화면 상에 운영자가 원하는 형태로 자유롭게 배치할 수 있습니다. 또한 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.

2. 운영환경

WAF 시스템은 다음과 같은 환경에서 운영되어야 합니다.

- WAF 은 하드웨어, 운영체제 및 내부 데이터베이스가 안정적으로 작동하며 웹 보안 게이트웨이애플리케이션 방화벽으로만 동작되도록 설계되고 구성된 전용 서버이므로, 내부 구성을 변경하거나 다른 목적으로 사용하는 것을 보증하지 않습니다.
- WAF 은 인가된 관리자만이 접근 하여야 합니다.
- WAF 은 HTTP/HTTPS 트래픽에 대한 보안을 위하여 만들어졌습니다. 따라서 추가적으로 방화벽이나 침입탐지 시스템과 병행하여 운영되어야 합니다.
- WAF 은 네트워크 상에 웹 클라이언트와 웹 서버 간의 물리적 또는 논리적 중간 지점에 위치해야 하며, 양자간의 HTTP(S) 통신은 WAF 을 통해서만 이루어져야 합니다.
- 네트워크 구성 변경, 웹 사이트의 증감 등으로 WAF 이 설치된 내부 네트워크 환경이 변화될 때에는 반드시 변화된 환경에 맞추어 보안정책을 반영하여야 합니다.
- WAF 은 관제시스템과 같은 외부 시스템과의 연동 시 SNMP trap, Syslog 등을 사용할 수 있으며, 이때 신뢰된 네트워크 구간 내에서 안전하게 유지되도록 관리해야 합니다.
- WAF 시스템은 ISSAC-Web 으로 암호화된 트래픽에 대해서도 안전한 키 관리를 통해 패킷을 복호화하여, 공격을 탐지하고 차단합니다.
- WAF 은 제품 유지보수 절차를 통해 최신의 보안 패치가 적용된 상태로 운영되도록 해야 합니다.
- WAF 은 신뢰할 수 있는 타임스탬프를 제공합니다. 안전한 운영을 위해 관리도구용 PC 에 대해서도 OS 가 제공하는 타임스탬프 동기화 기능을 적용하여 일관성을 유지해야 합니다.
- WAF 은 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

3. 설치 전 준비

이번 장은 WAF을 설치하기 전에 준비할 것들과 결정해야 할 것들에 대해 기술합니다. WAF을 정상적으로 설치하기 위하여 "설치 전 준비" 장을 숙독합니다.

3.1 특징

WAF의 설치 위치는 인가된 관리자만이 접근 가능한 안전한 환경에 위치해야 합니다. 이 후 관리자는 운영 형태에 맞춰 WAF의 network를 구성합니다. KT WAF의 네트워크 구성방법은 리버스 프락시방식입니다.

3.2 리버스 프락시(reverse proxy) 구성 방식

리버스 프락시 구성은 WAF을 일반적인 웹 프락시 서버와 동일한 구성으로 위치시킵니다. WAF의 물리적인 네트워크와 IP의 설정 등은 일반적인 웹 프락시와 동일하게 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 WAF이 프락시로 동작하기 때문에 웹 서버의 접속 로그에는 실제 웹 브라우저 사용자의 IP 주소가 아닌 WAF의IP 주소만이 남게 됩니다.

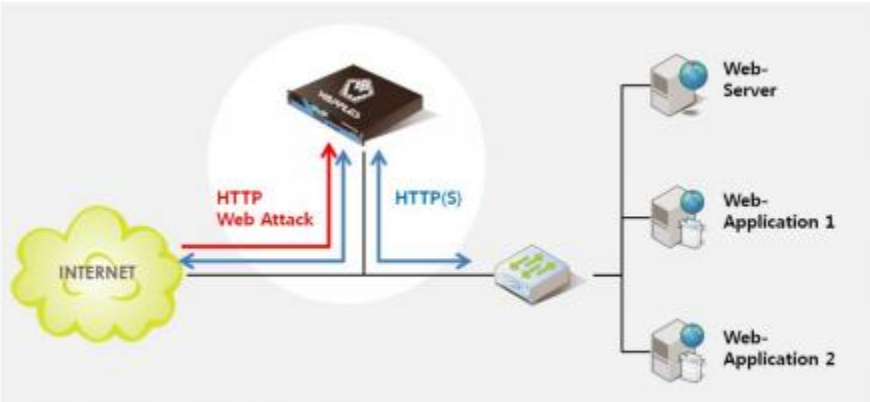


그림 2 리버스 프락시 구성 방식

3.3 운영 네트워크 구성에 따른 설치 예시

운영 네트워크 구성과 함께 WAF의 설치 위치를 정합니다. 상황에 따라 여러 변수가 있을 수 있으나, 대부분의 환경에서는 다음과 같은 위치에 설치하는 것이 일반적입니다.

- 단일 웹 서버 머신 1 대만을 보호할 때 (Single 상품)

Routter-VM 하단 단일 웹서버 사이에 Proxy 방식으로 구성 설치합니다.

- VPX 를 사용하여 2 대 이상의 웹 서버를 로드밸런싱하여 사용할 때 (Dual 상품)

VPX SW L4로 로드밸런싱한 서비스를 Router_VM에서 포트포워딩 한후 Router_VM과 웹서버 사이에 Proxy 방식으로 구성 설치 합니다.

3.4 기본 네트워크 자원 확보

기존에 서비스되는 포트 포워딩 룰을 확인 합니다.

- Single WAF 상품: Router VM 및 Web 서버로 구성된 1:1 구성 입니다. 기존에 서비스 되고 있는 포트포워딩 룰이 있다면 해당 포트포워딩 룰을 삭제 합니다.
- Dual WAF 상품: Dual WAF 상품은 VPX 로드밸런서 부가서비스와 2 개의 WAF, N 개의 Web 서버로 구성된 상품입니다.

Network 구성을 위해서 기존에 서비스 되고 있는 포트포워딩 룰이 있다면 해당 포트포워딩 룰을 삭제 합니다.

WAF의 서비스 구성을 위해서 public ip에 매핑된 4개의 public port가 필요합니다

5950 ~ 5999 Port 대역중 4개를 선택하여 설정 해야 하니 아래 설정하여야 할 포트 대역이 중복이 되지 않는지 확인 합니다.

- Console: WAF 를 원격에서 TCP/IP 를 통해서 관리 할수 있는 관리 포트 입니다.
- API: WAF 에 대한 Network 구성을 자동으로 처리 해 주기 위한 API 연결 포트 입니다.
- SSH: WAF VM 에 원격으로 접속 하기 위한 연결 포트 입니다.
- DB: WAF 관리도구에서 사용하는 PostgreSQL DB 에 Network 을 설정하기 위한 포트 입니다.

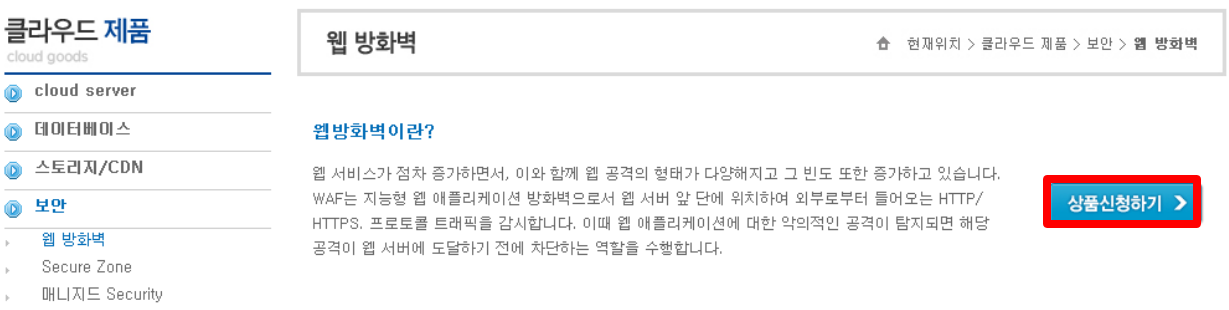
4. 신청 및 구성

이번 장은 WAF를 신청하고 운영에 관련한 기본적인 환경설정 방법을 설명합니다. 설치가 완료된 후 웹 사이트 보호를 위해 적절한 탐지 및 운영 정책을 설정할 수 있습니다

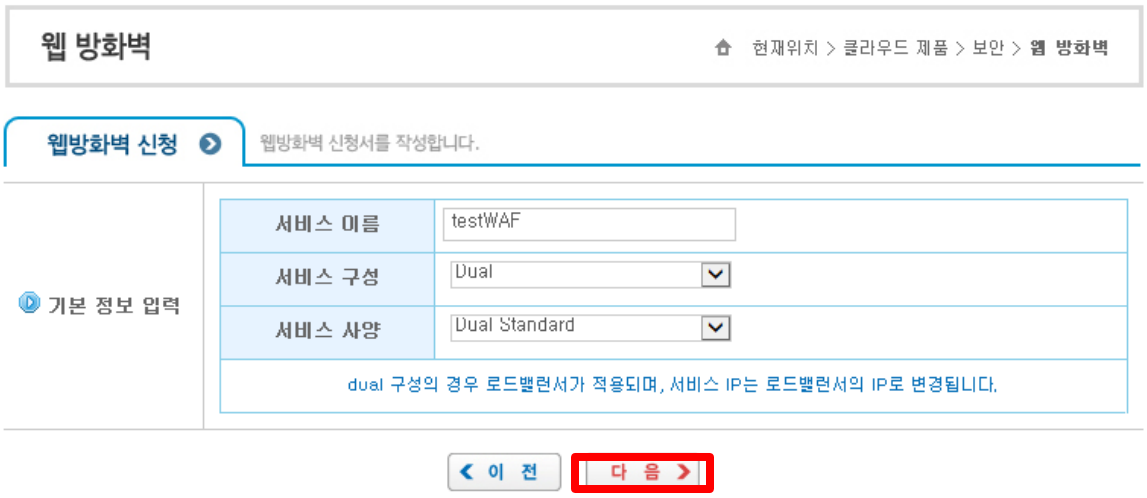
4.1 신청

WAF은 일반적으로 다음과 같은 설치 순서를 따릅니다.

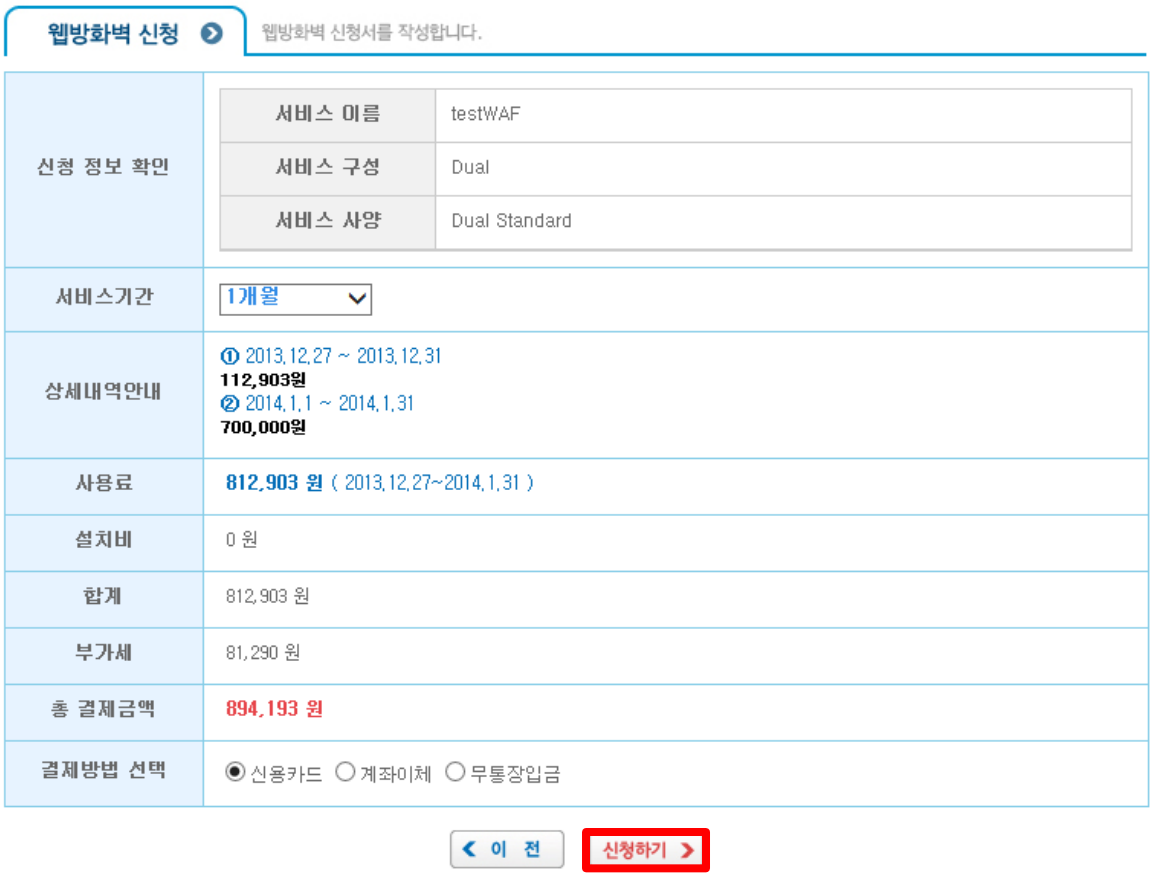
클라우드 제품 > 보안 > 웹 방화벽을 선택합니다. 상품 신청을 선택합니다.



WAF명을 입력한 뒤 구성 및 사용을 선택합니다.

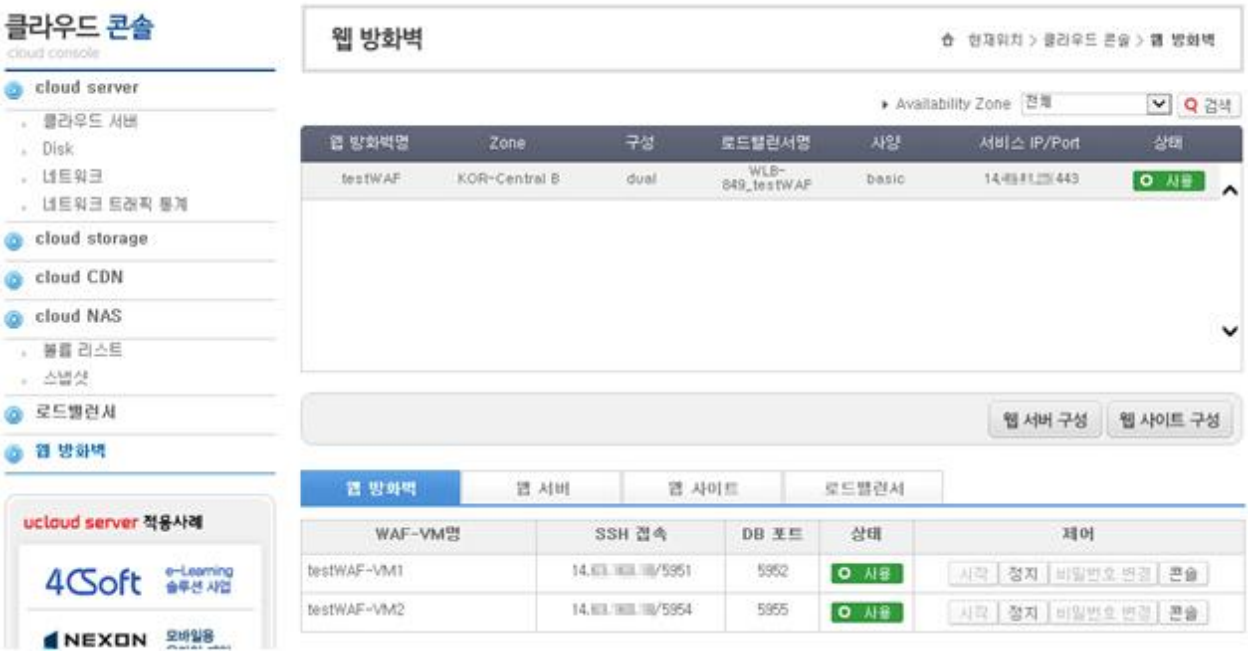


원하시는 정보 입력 후 신청을 하시면 입금 확인 및 WAF-VM 생성 후 고객님의 메일로 정보를 보내드리고 연락을 드립니다.

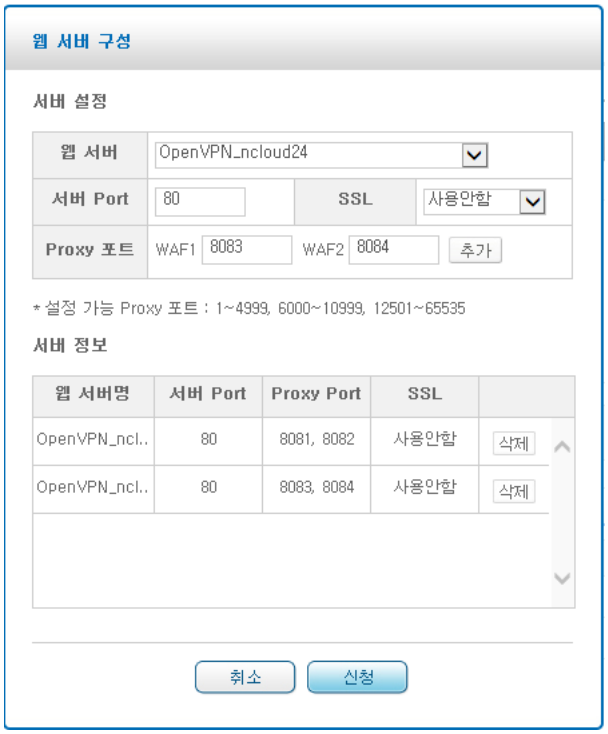


4.2 웹 서버 등록 및 서비스 등록

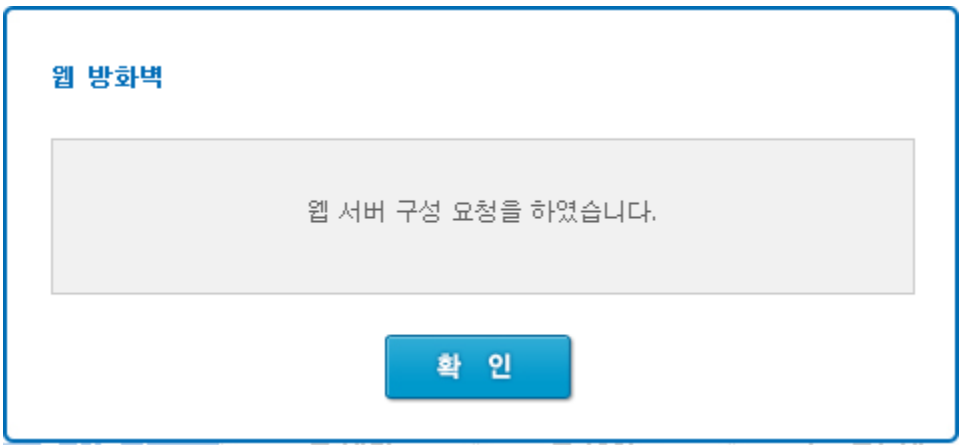
이후 클라우드콘솔 > 웹 방화벽으로 이동 후 WAF와 WEB 서버간의 서비스 구성작업을 진행합니다.



웹 서버 구성을 위해서 웹 서버 구성 버튼을 클릭 합니다



- WAF 가 보호해야 하는 웹 서버를 선택 합니다.
-서비스 Port 입력: 웹 서버가 서비스 하고 있는 서비스 포트를 선택 합니다. (80, 8080, 443)
- SSL 사용 여부를 체크 합니다. 기본은 SSL 사용하지 않음 입니다. SSL 을 사용하는 경우 사용으로 체크 하시고 세부 설정은 관리도구에서 설정 가능 합니다.
- Router-VM 및 WAF 간의 Proxy 포트를 입력합니다. Single 의 경우 (80, 8080, 443)
- 모든 사항이 입력되었으면 추가 버튼을 클릭하고 확인 버튼을 선택 합니다.



최종 내역은 웹방화벽 리스트에서 확인 할 수 있습니다.

웹 방화벽 | 웹 서버 | 웹 사이트 | 로드밸런서

웹 서버명	IP	서버 Port	Proxy Port	SSL
OpenVPN_ncloud24	172.	80	8083, 8084	사용안함
OpenVPN_ncloud24	172.	80	8081, 8082	사용안함

WAF가 보호 해야 하는 URI 또는 IP를 등록을 위해 웹사이트 구성을 클릭 합니다.

- 서비스 사이트의 사이트명을 등록 합니다. DNS 서비스에 등록되어 있는 URI 와 동일하게 등록 합니다.
- URI 가 없는 경우 IP 를 입력합니다.
- ncloud24.com 또는 1.1.1.1
- 사이트를 보호하는 보안 정책 수준을 설정 합니다.

표준 보안 정책 : 기본 보안 정책보다 한단계 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

확인 버튼을 클릭하여 서비스 등록을 완료 합니다.

웹 사이트	웹사이트 포트	보안 정책
ncloud24.com	8080	표준 보안
entscale.com	8081	탐지

서비스 타입이 Dual인 경우는 로드밸런서 설정을 할 수 있습니다.

5. Console 관리도구 직접 사용

① 인가된 관리자만이 접근 가능하도록 합니다.
② Microsoft(MS) 사의 WINDOWS계열 OS가 설치된 관리자용 PC를 최신 버전으로 업데이트 합니다.
③ 웹 브라우저에서 관리도구 기동 화면이 뜨면, [시작] 버튼을 눌러 관리도구 프로그램을 수행합니다. 만일 관리자의 PC에 .Net 4.0 이 설치되어 있지 않은 경우에는 이를 먼저 설치한 후에 관리도구 프로그램을 수행합니다.
④ 설정 마법사를 기동하여 [네트워크 설정] 기능을 사용하여 WAF가 보호하고자 하는 웹 서버들의 IP 주소 정보를 설정합니다.
⑤ 설정 마법사의 [웹 사이트 설정] 기능을 사용하여 보호하고자 하는 웹사이트를 등록하고 이를 적절한 보안 정책에 맵핑합니다. 필요한 경우 보안 정책을 추가하거나 변경합니다.
⑥ 설정이 끝나면 서비스 포트에 네트워크 라인을 연결하고 정상적으로 웹 서버에 접속할 수 있는지의 여부와 WAF가 웹 트래픽을 모니터링하고 웹 공격을 탐지 및 차단하는지 확인합니다.

6. 서비스 상담 및 문의

엔클라우드24 상품의 모든 상담 및 장애 신고 방법은 전화상담과 게시판 상담을 통해 이루어집니다.

6.1 FAQ 및 매뉴얼

각종 사용 매뉴얼 및 FAQ는 엔클라우드24 고객센터의 FAQ 게시판(자주하는 질문) 및 자료실을 통하여 확인하실 수 있습니다.

6.2 전화 상담

상품 문의는 엔클라우드24 고객센터 (070-7422-0541~2)를 통하여 상담 받으실 수 있습니다.

6.3 게시판 상담

엔클라우드24 로그인 후, 고객센터 – 1:1 문의하기 게시판에 문의사항 및 장애 상황을 작성 후 답변을 확인하시면 됩니다. 클라우드 기술 전문가가 해당 내용에 대해 기술적 문의사항에 대해 지원을 해줍니다.