

보안

ucloud 웹방화벽 관리도구 매뉴얼

목차

- 시작하기
- 서비스정보
- 설치
- 운영 전 준비
- 탐지룰의 이해
- 탐지로그
- 대시보드
- 감사로그
- 정책설정
- 설정마법사
- SSL 인증서 적용
- 기타

시작하기

매뉴얼의 목적

WAF 관리도구에 관련된 모든 정보 및 사용 방법에 대해 레퍼런스 형식으로 설명합니다.

매뉴얼의 용도

본 매뉴얼은 WAF 관리도구를 사용하는 웹사이트 관리자를 위해 제작되었습니다.

선수지식

본 매뉴얼을 이해하기 위해서는 다음과 같은 사전 지식이 필요합니다

네트워크 기본 과정

프로토콜 이해

OSI 7 Layer 이해

라우팅의 이해

웹 서비스 동작 방식

HTTP 1.1 RFC 이해

웹 서버, 웹 클라이언트 역할 이해

보안 기초 지식

OS 보안 지식

Network 보안 지식

구성 장별 간단한 요약

오류! 참조 원본을 찾을 수 없습니다.

WAF 관리도구를 설치하는 방법을 설명하고 운영에 관련한 기본적인 환경설정 방법을 설명합니다.

설치

설치에 앞서 준비해야 할 사항들을 설명하였으며, 매끄러운 설치를 위하여 본 장을 숙독해야 합니다

오류! 참조 원본을 찾을 수 없습니다.

WAF 모니터링 모드를 설정하는 방법에 대해 설명합니다.

운영 전 준비

운영에 앞서 관리도구의 기본적인 동작법에 대해 설명합니다.

탐지률의 이해

사이트에 적용한 적절한 탐지률을 결정하기 위해 각 탐지률에 대해 설명합니다.

탐지로그

보안 정책에 의해 웹사이트 공격으로 탐지된 로그를 조회하고 조회된 탐지로그를 분석하여 보안 정책을 적절히 조정하는 부분에 대해 설명합니다.

대시보드

WAF의 트래픽과 탐지로그를 분석하여 차트의 형태로 관리자에게 제공함 정보를 보는 방법에 대해 설명합니다.

감사로그

WAF 본체 및 정책 변경에 대해 감사 내용의 조회에 대한 방법을 설명합니다.

오류! 참조 원본을 찾을 수 없습니다.

WAF이 보호하는 웹 사이트와 보안 정책을 관리하는 방법에 대해 설명합니다.

설정마법사

WAF의 원활한 운영을 위한 설정과 네트워크를 설정하는방법에 대해 설명합니다.

오류! 참조 원본을 찾을 수 없습니다.

Serial 콘솔 포트를 이용하여 WAF의 관리포트 설정 및 모니터링을 위해 제공하는 WAF Command Line Interface에 대해 설명합니다.

오류! 참조 원본을 찾을 수 없습니다.

WAF 장비의 상태를 확인해 볼수 있는 방법에 대해 설명합니다.

오류! 참조 원본을 찾을 수 없습니다.

WAF 장비의 상태를 확인해 볼수 있는 방법에 대해 설명합니다.

SSL 인증서 적용

WAF이 지원하는 SSL 인증서 형식과 인증서 형식을 변환하는 방법에 대하여 설명합니다.

기타

운영 중 발생하는 장애에 대한 조치방법을 설명합니다.

용어의 정의

본 매뉴얼에서 사용되는 주요 단어들은 아래의 정의를 따릅니다.

WAF : olleh ucloud 에서 제공하는 cloud server의 부가서비스인 웹방화벽 서비스를 의미합니다.

웹사이트 관리자 : WAF 및 WAF이 설치된 환경에 접근 가능한 모든사람으로써 WAF의 설치와 운영을 담당하는 사람을 의미합니다.

서비스 정보

본 장은 WAF을 소개하는 장으로 제품의 주요기능 및 특징과 제품구성, WAF 본체의 각 부분 명칭, 제품 규격, 운영환경에 대해서 기술합니다.

개요

WAF1은 지능형 웹 애플리케이션 방화벽입니다. WAF은 웹 서버 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.



그림이 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.

주요 보안기능

WAF은 다음과 같은 보안 기능을 제공합니다.

HTTP 기반의 웹 공격 방지

OWASP2 Top 10 Attacks 탐지 및 차단

PCI-DSS Copliance의 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 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 30여종의 파일 검색

지정한 금지 단어 입력시 자동 변환 **예) "나쁜말"(금지단어) -> "고운말"(등록된 표현)**

해커에 의해 변조된 페이지 노출 차단 및 자동 복구

특징

WAF은 다음과 같은 특징을 가집니다.

보안성

웹 공격에 대한 3중 방어 구조

WAF은 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

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

성능

버추얼 어플라이언스

WAF은 웹 서버를 비롯한 기존 서비스 장비에 별도의 부하를 주지 않는 버추얼 어플라이언스(appliance) 형태로 구성되어 높은 성능 을 제공합니다.

웹사이트/웹서버 동시 보호

WAF은 여러 웹사이트들과 하나의 웹 서버들을 동시에 보호하는 것이 가능합니다.

안전성

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.

운영환경

WAF 시스템은 다음과 같은 환경에서 운영되어야 합니다.

WAF은 인가된 관리자만이 접근 가능한 물리적으로 안전한 환경에 위치하여 설치되어야 합니다.

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

WAF은 네트워크 상에 웹 클라이언트와 웹 서버 간의 물리적 또는 논리적 중간 지점에 위치해야 하며, 양자간의 HTTP(S) 통신은 WAF을 통해서만 이루어져야 합니다.

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

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

WAF은 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 OS가 설치된 안전한 관리자 PC에서 사용되어야 합니다.

관리도구는 신뢰된 네트워크 구간에서만 접속 가능하도록 하여야 합니다.

관리도구를 통해 WAF에 접속하는 경우, SSL로 암호화된 트래픽을 통해 정보를 전달하므로 정보의 비밀성을 유지합니다.

설치

이번 장은 WAF 본체와 관리도구를 설치하는 방법을 설명하고 운영에 관련한 기본적인 환경설정 방법을 설명합니다. 설치가 완료된 후 웹 사이트 보호를 위해 적절한 탐지 및 운영 정책을 설정할 수 있습니다.

WAF은 일반적으로 다음과 같은 설치 순서를 따릅니다.

1. 인가된 관리자만이 접근 가능한 물리적으로 안전한 환경에 WAF의 설치 위치를 결정합니다.
2. 물리적인 네트워크 환경과 보호하고자 하는 웹 서버의위치 중간에 WAF 를 두고 사용자의 환경에 맞도록 고려하여 네트워크를 구성합니다.
3. 네트워크 및 웹 서버 관리자와 협의하여 관련 환경 정보를 수집한 후 WAF의 네트워크 구성과 설치 위치를 결정합니다.
4. Microsoft(MS) 사의 WINDOWS계열 OS가 설치된 관리자용 PC를 최신 버전으로 업데이트 합니다.
5. Serial 콘솔 포트를 사용하여 관리포트의 IP 주소, 넷마스크, 게이트웨이를 설정합니다.
6. 관리포트에 네트워크 라인을 연결하고 관리자의 관리PC에서 웹 브라우저 MS-Intern Explorer를 사용하여 관리포트 IP에 접속합니다.
7. 웹 브라우저에서 관리도구 기동 화면이 뜨면, [시작] 버튼을 눌러 관리도구 프로그램을 수행합니다. 만일 관리자의 PC에 .Net 2.0 이 설치되어 있지 않은 경우에는 이를 먼저 설치한 후에 관리도구 프로그램을 수행합니다.
8. 설정 마법사를 기동하여 [네트워크 설정] 기능을 사용하여 WAF가 보호하고자 하는 웹 서버들의 IP 주소 정보를 설정합니다.
9. 설정 마법사의 [웹 사이트 설정] 기능을 사용하여 보호하고자 하는 웹사이트를 등록하고 이를 적절한 보안 정책에 맵핑합니다. 필요한 경우 보안 정책을 추가하거나 변경합니다.
10. 설정이 끝나면 서비스 포트에 네트워크 라인을 연결하고 정상적으로 웹 서버에 접속할 수 있는지의 여부와 WAF가 웹 트래픽을 모니터링하고 웹 공격을 탐지 및 차단하는지 확인합니다.

관리포트 설정

WAF을 TCP/IP를 이용하여 원격에서 관리합니다.원격에서 WAF을 관리 하기 위해서는 관리포트를 설정해야 하며, 이는 웹방화벽 신청 시 WAF console port 입력으로 설정할 수 있습니다.

WAF console port configuration screen showing steps 01, 02, and 03. Step 01 is highlighted. The screen includes fields for name, type, mode, and serial, and a section for port settings with tabs for Console, API, and others.

관리도구 설정

관리포트의 설정이 끝나면, 이제 관리 PC에서 WAF 관리도구를 기동할 차례입니다. WAF의 관리도구는 .NET 4.0 기반으로 Windows XP 이상에서 운용 할 수 있습니다

Net 4.0설치

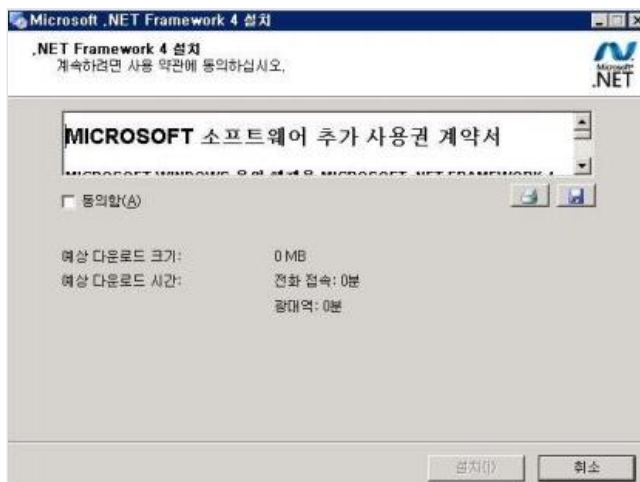
Cloud Portal의 부가서비스>웹방화벽 화면에서 해당 웹방화벽의 콘솔 버튼을 클릭하여 접속합니다. 만일 관리 PC에 .Net 4.0이 설치되어 있지 않다면 다음과 같은 설치 화면이 나타납니다. 만일 이전에 이미 이 설치 과정을 거쳤다면 본 단계는 수행하지 않고 다음 단계로 넘어 갑니다.



설치 화면 오른쪽 하단의 주황색 [설치] 버튼을 누르면 다음과 같은 경고 창이 나옵니다. 실행버튼을 클릭합니다.



설치 프로그램 실행 후에 나타나는 설명에 따라 설치를 완료하십시오.



.Net 4.0의 설치가 끝나면 웹 브라우저 설치 화면 오른쪽 하단의 [설치] 버튼 위 파란색 "시작" 링크를 클릭하여 관리도구를 실행할 수 있습니다.

관리도구 기동

.Net 4.0을 이미 설치한 상황에서 웹방화벽 메뉴의 콘솔 버튼을 클릭하여 관리포트에 접속하면 다음과 같이 기동 화면이 나타납니다.



오른쪽 하단의 주황색 [시작] 버튼을 클릭하면 WAF의 관리도구가 실행되며 아래와 같은 로그인 창이 나타납니다.

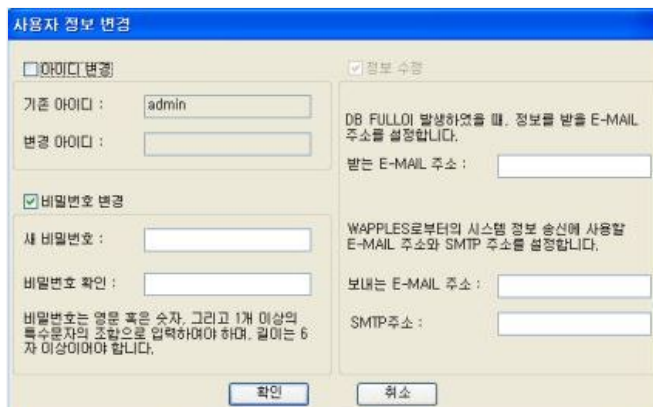


WAPPLES 로그인 화면. 화면 상단에는 WAPPLES 로고와 'Web Application Security'라는 텍스트가 보입니다. 로그인 폼에는 아이디, 비밀번호, PORT, 확인, 취소 버튼이 있습니다. 하단에는 '로그인 후 사용자 정보 수정' 체크박스도 있습니다.

olleh WAF의 관리자는 '웹 사이트 관리자' 권한으로 운용되며, 웹 사이트 관리자는 관리 권한을 받은 웹사이트에 대한 정책 수정 및 정보를 조회할 수 있습니다.

웹사이트 관리자의 아이디는 'admin' 이며 웹사이트 관리자 아이디의 초기 비밀번호는 영문자 5글자로 이루어진 'penta'입니다. 이 웹사이트 관리자 아이디와 비밀번호로 접속하면 웹사이트 관리자가 비밀번호를 보다 안전한 것으로 변경하도록 비밀번호 수정 화면이 나타납니다. 새로운 비밀번호는 1자 이상의 특수문자를 반드시 포함하며, 최소 6자 이상의 길이를 가져야만 합니다.

PORT 정보는 웹방화벽 신청 시 입력한 DB PORT 정보를 입력합니다.



사용자 정보 변경 화면 (상단). '아이디 변경' 섹션에는 기존 아이디 'admin'과 변경 아이디 입력란이 있습니다. '비밀번호 변경' 섹션에는 새 비밀번호, 비밀번호 확인, 그리고 비밀번호 규칙 설명(영문, 숫자, 1개 이상의 특수문자 조합, 길이 6 이상)이 있습니다. 오른쪽에는 '정보 수정' 섹션으로 DB FULL이 발생했을 때 정보를 받을 E-MAIL 주소와 WAPPLES로부터의 시스템 정보 송신에 사용할 E-MAIL 주소와 SMTP 주소를 설정할 수 있습니다. 확인, 취소 버튼이 있습니다.



사용자 정보 변경 화면 (하단). 이 부분은 '아이디 변경' 섹션과 '비밀번호 변경' 섹션의 상세 폼입니다. 기존 아이디 'shcho'와 변경 아이디 입력란이 있습니다. 새 비밀번호와 비밀번호 확인 입력란도 포함되어 있습니다. 비밀번호 규칙 설명도 동일합니다. 확인, 취소 버튼이 있습니다.

안전한 비밀번호로 설정한 후 관리자의 e-mail 정보를 입력합니다. 저장되는 관리자의 e-mail 주소로 DB FULL 발생 하였을시 경고 메일 및 삭제 알림 메일을 발송합니다.

송신 측 메일 주소 및 SMTP 주소 [X설정방법]->[운영 설정]-> **[오류! 참조 원본을 찾을 수 없습니다.]**에서 수정할 수 있습니다

확인 버튼을 클릭하면 관리도구 메인 화면이 실행합니다. 이로써 관리도구의 기동이 완료됩니다.

인라인 구성으로만 운영할시에는 값을 입력하지 않고 다음으로 이동할 수 있습니다.

현재 등록되어 있는 Proxy IP 주소를 사용하는 웹 서버가 등록되어 있는 경우 다음 화면과 같이 Proxy IP 는 붉은 색으로 표시됩니다. 붉은색의 Proxy IP를 삭제하기 위해서는 붉은 색의 Proxy IP를 사용하는 웹서버를 삭제한 후 삭제 할 수 있습니다.

Proxy IP 설정은 Proxy IP 와 넷마스크를 입력한 후 [추가] 버튼을 클릭하여 추가합니다.

IP 주소는 필요에 따라서 여러 개 입력이 가능합니다. 그러나 여러 개라도 동일한 서비스포트 네트워크 장치에서 사용하는 IP이므로 모두 동일 서브넷에 존재하는 IP를 입력해 주어야 합니다.

추가된 Proxy IP를 수정해야 할 경우 해당 IP를 선택하고 편집한 후 [수정] 버튼을 클릭하여 수정합니다.

추가된 Proxy IP를 삭제해야 할 경우 해당 IP를 선택하고 [삭제] 버튼을 클릭하여 삭제합니다.

미리 파일로 저장해둔 네트워크 설정 내용이 존재하면 [설정 불러오기] 버튼을 눌러 이를 입력할 수 있습니다. 네트워크 설정의 파일 저장은 나중에 설명한 [설정 내보내기] 버튼을 사용하여 가능합니다.

Proxy IP가 하나 이상 등록된 상태에서 [다음] 버튼을 누르면 아래와 같이 게이트웨이 설정 화면이 나옵니다.

게이트웨이 입력

입력한 기본 게이트웨이라도 앞서 등록한 Proxy IP의 IP 주소 및 넷마스크와 동일 서브넷에 존재하여야만 합니다.

기본 게이트웨이를 아래 화면처럼 입력한뒤 [다음] 버튼을 클릭하면 기본 게이트웨이가 설정됩니다.

만일 기본 게이트웨이 이외에 추가적으로 게이트웨이를 입력할 필요가 있으면 기본 게이트웨이 아래쪽의 입력 박스에 Destination, Netmask와 게이트웨이를 입력한 후 [추가] 버튼을 클릭하여 추가합니다.

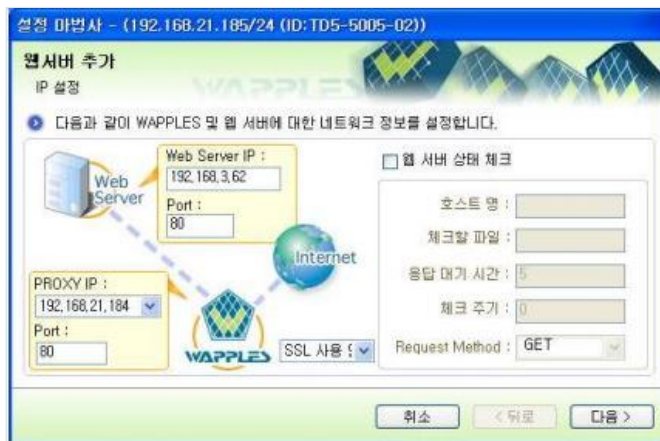
기본 게이트웨이와 달리 추가 게이트웨이는 대상이 될 네트워크를 가리키는 Destination과 Netmask 값을 입력하여야 합니다. WAF의 서비스포트 Proxy IP에서 특정 영역의 네트워크와 통신하기 위해 기본 게이트웨이 이외에 별도의 게이트웨이가 필요한 경우, 이 특정 영역의 네트워크를 가리키기 위해 Destination과 Netmask 값을 사용합니다. 192.168.1.0/24 영역의 네트워크를 대상으로 한 게이트웨이를 입력하는 경우라면 Destination은 192.168.1.0, Netmask는 255.255.255.0 이 됩니다.

웹 서버 정보 입력

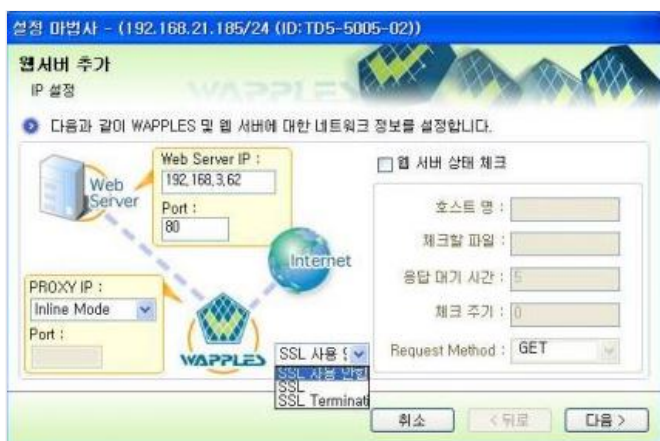
WAF의 서비스포트 Proxy IP와 게이트웨이를 입력하면 보안 서비스의 대상이 될 웹 서버 IP 주소와 port 번호를 추가/수정/삭제 할 수 있습니다.



[추가] 버튼을 클릭하여 웹 서버를 추가합니다. Proxy 구성로 운영하고자 할 시에는 입력한 웹 서버의 IP 주소 및 port 번호를 WAF Proxy IP주소 및 port와 1:1 맵핑합니다. WAF은 일종의 웹 보안 프락시 역할을 하므로 맵핑한 WAF의 Proxy IP와 port에 접속하면 이는 지정한 웹서버의 IP와 port에 연결됩니다.



인라인 구성로 운영하고자 할시에는 아래 화면처럼 Proxy IP에 Inline Mode 를 선택하면 됩니다.



입력한 웹 서버 IP와 port 번호가 SSL 통신을 사용하는 경우에는 [SSL 사용] 버튼을 클릭하여 관련 SSL 인증서와 비공개키 파일을 입력하여야 합니다. 보다 자세한 설정 방법은 Reference Manual에서 설명합니다.

WAF은 입력 받은 웹 서버 IP와 port 번호로 통신이 오면 이를 가로챍니다. 가로챈 통신 내용에서 위험한 공격들을 탐지 차단하여 웹서버를 보호합니다.



네트워크 설정 완료

이로서 WAF의 네트워크 설정이 완료됩니다. 네트워크 설정 완료 화면에서는 다음 그림과 같이 WAF의 네트워크 설정 정보를 확인할 수 있으며 [설정 내보내기...] 버튼을 눌러서 네트워크 설정 정보를 내보낼 수 있습니다.



웹사이트 추가

관리포트의 설정이 끝나면, 이제 관리 PC에서 WAF 관리도구를 기동할 차례입니다. WAF의 관리도구는 .NET 4.0 기반으로 Windows XP 이상에서 운용 할 수 있습니다

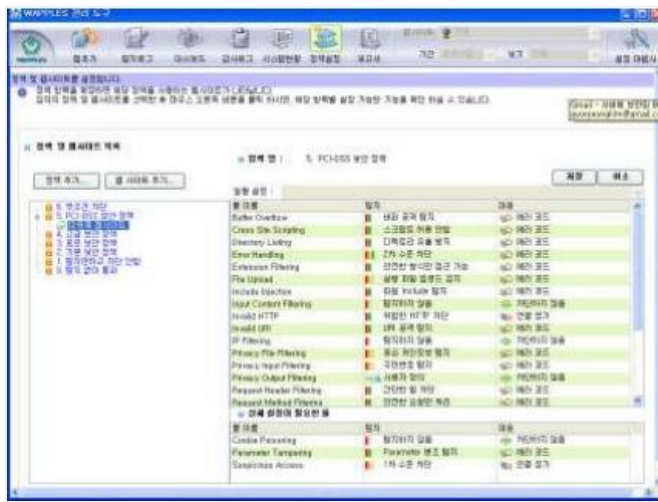
웹사이트에 맵핑할 정책 선택

네트워크 관련 설정이 모두 끝나면 보호할 웹사이트들에 적용할 정책을 결정합니다.

툴바의 [정책 설정]을 클릭합니다.



다음과 같은 웹 사이트 설정 화면을 볼 수 있습니다.



화면의 왼쪽에는 정책 리스트와 이 정책을 사용하는 웹사이트 리스트를 볼 수 있습니다. 화면의 오른쪽에는 왼쪽에서 선택한 정책의 세부정보를 볼 수 있습니다.

WAF은 기본적으로 7가지 정책을 제공합니다. 이 정책은 WAF시스템이 제공하는 정책으로 수정이나 삭제가 불가능합니다

기본 정책

| 기본 정책 | 설명 |
|---------------|--|
| 무조건차단 | 모든 트래픽을 차단하는 정책 |
| PCI-DSS 보안 정책 | PCI-DSS 인증을 준수하기 위하여 적용 가능한 정책으로, PCI-DSS에 적합한 보안 수준을 제공 |
| 고급 보안 정책 | 영향도가 낮은 공격까지 방어해주는 높은 수준의 보안 정책으로 사용자의 세부 대응이 필요한 공격 이외의 대부분의 공격을 방어 |
| 표준 보안 정책 | 기본 보안 정책보다 한단계 높은 보안수준의 정책으로, 일반적인 웹 환경에 가장 최적화된 보안 정책 |
| 기본 보안 정책 | 기본적인 웹 공격을 방어하기 위한 보안 정책으로, 대중화되고 영향도가 높은 웹 공격을 방어 |
| 탐지만하고 차단 안함 | 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 |

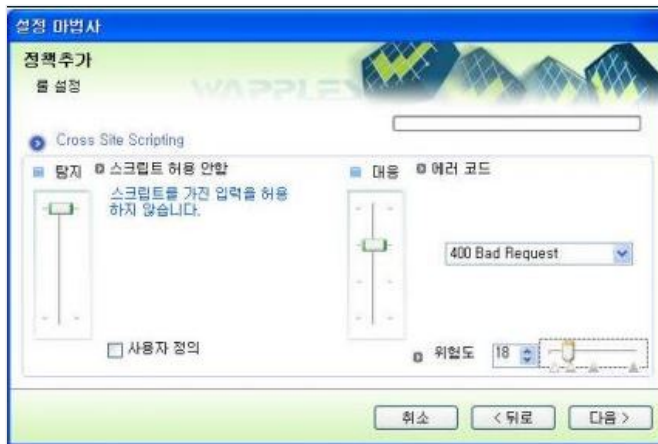
기본으로 제공되는 정책은 그 내용을 수정할 수 없으므로 관리자는 별도의 정책을 추가하여 사용하는 것이 좋습니다. 웹사이트 설정 메인 화면에서 [정책 추가] 버튼을 클릭하여 정책을 추가합니다.



기존 정책을 기반으로 하여 신규 정책을 추가하게 됩니다. 먼저 기반으로 할 정책을 선택합니다. 미리 파일로 저장할 정책이 있다면 [정책 불러오기...] 버튼을 사용하여 이를 읽어올 수 있습니다.



신규 정책의 탐지 설정 및 대응 설정 내용 중 수정하고자 하는 탐지룰을 체크하고 [다음] 버튼을 클릭합니다. 각 탐지 룰 별로 탐지 설정과 대응 설정을 원하는 내용으로 변경할 수 있습니다.



이로써 신규 정책이 추가 완료됩니다.

이 장에서는 [탐지만 하고 차단안함]을 사용하여 웹사이트 등록을 합니다. 기본으로 제공하는 정책 이외에 관리자가 직접 설정한 정책을 사용하는 방법은 Reference Manual [VIII.1정책 추가/수정]에서 설명합니다.

웹사이트 추가

신규 웹사이트 등록

[웹사이트 추가] 버튼을 누르면 신규웹 사이트를 추가할 수 있습니다.

[웹 사이트 이름]에는 실제 서비스 DNS 이름과 동일해야 하고 이미 등록되어 있거나 다른 웹 사이트의 이름과 중복하여 입력 할 수 없습니다.



[웹 사이트 설명] 부분은 특별히 지정하지 않으면 웹 사이트 이름과 동일하게 입력 됩니다.

웹 사이트의 [포트 번호]는 기본적으로 80으로 설정되어 있으나 만약 다른 포트를 사용하는 경우에는 해당하는 포트 번호를 입력합니다.

웹사이트의 이름과 포트 번호, 설명을 입력하면 [다음] 버튼을 눌러 추가적인 네트워크연결 정보를 입력합니다.

만일 입력 내용에 문제가 발생하면 빨간색 느낌표가 나타납니다. 이 느낌표에 마우스 커서를 가져가면 에러의 원인이 풍선 도움말 형태로 출력되어 원인을 확인할 수 있습니다.

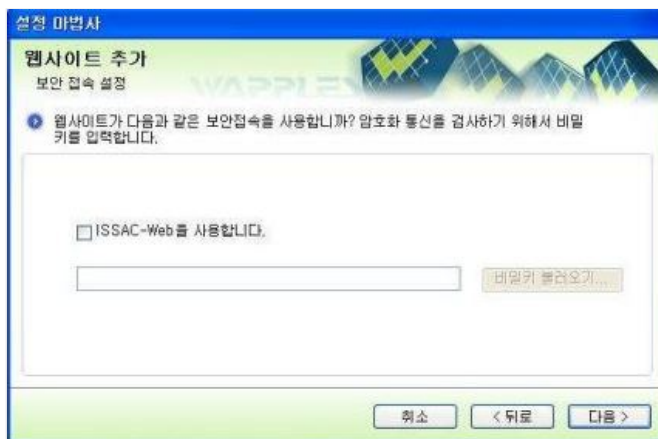
설정 마법사는 웹 사이트 이름 및 웹 사이트 설명 입력 시 관리자 입력 값에 오류가 있을 경우 다음과 같은 오류 메시지를 출력합니다.

웹 사이트 설정 오류 메시지_1

| 오류 메시지 | 출력 원인 |
|------------------|------------------------------------|
| 빈칸일 수 없습니다. | 입력된 웹사이트의 이름 및 웹사이트 설명이 없거나 빈칸일 경우 |
| 입력 가능한 범위가 아닙니다. | 입력된 웹사이트의 포트가 0보다 작거나 65535보다 클 경우 |

웹사이트 추가 정보 등록

펜타시큐리티시스템의 웹 보안 솔루션인 ISSAC-Web을 사용할 경우 "ISSAC-Web을 사용합니다."에 체크합니다. 사용을 선택할 경우, ISSAC-Web이 사용하는 웹 서버용 비밀키 파일을 [비밀키 불러오기]버튼을 이용하여 등록하고 [다음] 버튼을 클릭합니다.

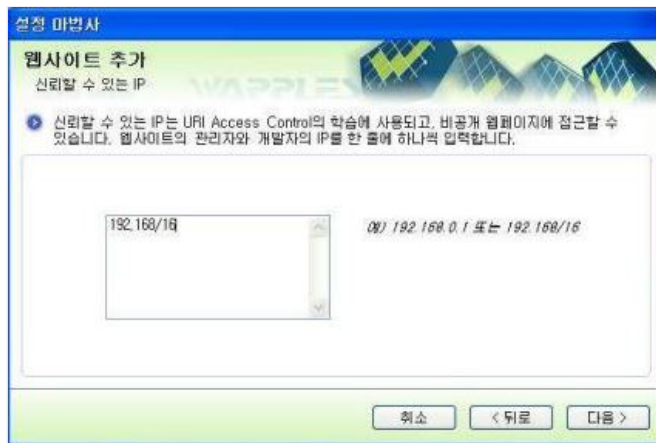


설정마법사는 ISSAC-Web 사용시 관리자 입력 값에 대하여 오류가 있을 경우 다음과 같은 오류 메시지를 출력합니다.

웹 사이트 설정 오류 메시지_2

| 오류 메시지 | 출력 원인 |
|------------------|-----------------------------------|
| 빈칸일 수 없습니다. | 비밀키를 입력하지 않았거나 입력한 비밀키의 내용이 없는 경우 |
| 입력 가능한 범위가 아닙니다. | 비밀키를 Text 형식으로 열수 없는 경우 |

위 화면에서 [다음] 버튼을 누르면 아래 화면이 나타납니다. [신뢰 IP]의 입력형식은 한줄에 하나의 IP나 IP/Netmask로 입력 합니다.



설정 마법사는 운영자가 입력한 신뢰 IP에 대하여 오류가 있을 경우 다음과 같은 오류 메시지를 출력합니다.

웹 사이트 설정 오류 메시지_3

| 오류 메시지 | 출력 원인 |
|--------------------------------------|--|
| 한 줄에 하나의 IP를 입력하십시오. 빈칸은 입력할 수 없습니다. | 입력한 IP 리스트 중 빈 행이 있을 경우 |
| 중복된 IP가 있습니다. | 입력한 IP 리스트 중 중복된 IP가 존재할 경우 |
| {입력 받은 IP}은 잘못된 IP 입니다. | 입력한 IP 리스트의 각각의 IP가 IP형식 및 넷마스크의 형식을 준수하지 않았을 경우 |

[신뢰 IP]는 URI Access Control 룰을 사용하지 않고 비공개 웹 페이지를 지정할 필요가 없는 경우라면 굳이 입력하지 않아도 됩니다. URI Access Control룰은 Reference Manual [URI Access Control]에서 자세히 설명합니다.

첫 째는 URI 접근 제어 목록을 자동으로 생성할 수 있도록 하는 기능으로 [신뢰 IP]에 등록된 IP에서 웹사이트를 접근하면 자동으로 웹사이트의 URI를 학습하여 [URI 접근 제어 목록]에 해당 URI를 등록합니다.

또 다른 기능은 요청한 웹페이지(URI)가 [URI 접근 제어 목록]에서 관리자용 비공개 지정 웹페이지로 설정되어 있는 경우 [신뢰 IP]에서 등록된 IP인 경우만 접속을 허락할 때 사용합니다. URI 접근 제어 목록에 대한 자세한 사항은 Reference Manual에서 설명합니다.

[웹사이트의 중요 정보를 암호화하는데 사용하는 보안키를 입력합니다. 관리도구가 자동으로 생성하므로 별다른 동작을 할 필요 없이 다음으로 넘어가도 무방합니다. 보안키를 변경하고자 한다면 [보안키 변경] 버튼을 클릭하면 자동으로 생성됩니다. 보안키가 생성되면, [다음]버튼을 클릭합니다.

보안키는 WAF 시스템 내부에서 사용되는 키로 충분히 복잡해야 하므로 난수 발생 알고리즘에 의해 임의의 보안키가 생성됩니다.

웹사이트 운영 중에 키의 내용이 유출되었다고 생각되거나 바꿀 필요가 있을 때 [보안키 변경]을 눌러 새로 생성하면 됩니다. 이 키는 WAF내에서 각종 암호화 및 무결성 보장을 위하여 사용됩니다.

운영 중 이 키가 변경되면 WAF 에서 쓰이는 모든 키가 같이 변경되므로 잠시 오탐(잘못된 탐지)이 발생할 수 있습니다.

설정 마법사

웹사이트 추가

웹사이트의 다른 이름

① 웹사이트 이름은 2개 이상일 수 있습니다. 예로 pentasecurity.com 은 www.pentasecurity.com 이라는 다른 이름을 가지고 있습니다. 아래에 웹사이트의 다른 이름을 한줄씩 하나씩 입력합니다. 다른 이름이 없는 경우 비워둡니다.

웹사이트의 이름:

웹사이트의 다른 이름:

마지막으로 등록된 정책들 중에서 웹사이트에서 사용할 정책을 선택합니다. 정책의 세부적인 내용을 확인하고 웹사이트의 운영 방향에 맞는 정책을 선택합니다. 여기에서는 [탐지만 하고 차단안함]을 선택합니다. 웹사이트 추가 완료 후 정책을 변경하려면 [웹사이트 수정]을 이용하여 하거나, 해당 웹사이트를 끌어다 원하는 정책으로 이동하여(Drag & Drop) 적용할 수 있습니다. 보다 자세한 정책 적용은 Reference Manual에서 설명합니다.

설정 마법사

웹사이트 추가

정책 선택

② 해당 웹사이트에서 탐지 및 대응에 사용할 정책을 선택합니다.

정책 이름: 0. 탐지 없이 통과

| 이름 | 탐지 | 대응 |
|----------------|----|-------|
| 1. 탐지만하고 차단 안함 | 탐지 | 차단 안함 |
| 2. 탐지만하고 차단 | 탐지 | 차단 |
| 3. 탐지만하고 차단 | 탐지 | 차단 |
| 4. 탐지만하고 차단 | 탐지 | 차단 |
| 5. 탐지만하고 차단 | 탐지 | 차단 |
| 6. 탐지만하고 차단 | 탐지 | 차단 |
| 7. 탐지만하고 차단 | 탐지 | 차단 |
| 8. 탐지만하고 차단 | 탐지 | 차단 |
| 9. 탐지만하고 차단 | 탐지 | 차단 |
| 10. 탐지만하고 차단 | 탐지 | 차단 |
| 11. 탐지만하고 차단 | 탐지 | 차단 |
| 12. 탐지만하고 차단 | 탐지 | 차단 |
| 13. 탐지만하고 차단 | 탐지 | 차단 |
| 14. 탐지만하고 차단 | 탐지 | 차단 |
| 15. 탐지만하고 차단 | 탐지 | 차단 |
| 16. 탐지만하고 차단 | 탐지 | 차단 |
| 17. 탐지만하고 차단 | 탐지 | 차단 |
| 18. 탐지만하고 차단 | 탐지 | 차단 |
| 19. 탐지만하고 차단 | 탐지 | 차단 |
| 20. 탐지만하고 차단 | 탐지 | 차단 |
| 21. 탐지만하고 차단 | 탐지 | 차단 |
| 22. 탐지만하고 차단 | 탐지 | 차단 |
| 23. 탐지만하고 차단 | 탐지 | 차단 |
| 24. 탐지만하고 차단 | 탐지 | 차단 |
| 25. 탐지만하고 차단 | 탐지 | 차단 |
| 26. 탐지만하고 차단 | 탐지 | 차단 |
| 27. 탐지만하고 차단 | 탐지 | 차단 |
| 28. 탐지만하고 차단 | 탐지 | 차단 |
| 29. 탐지만하고 차단 | 탐지 | 차단 |
| 30. 탐지만하고 차단 | 탐지 | 차단 |
| 31. 탐지만하고 차단 | 탐지 | 차단 |
| 32. 탐지만하고 차단 | 탐지 | 차단 |
| 33. 탐지만하고 차단 | 탐지 | 차단 |
| 34. 탐지만하고 차단 | 탐지 | 차단 |
| 35. 탐지만하고 차단 | 탐지 | 차단 |
| 36. 탐지만하고 차단 | 탐지 | 차단 |
| 37. 탐지만하고 차단 | 탐지 | 차단 |
| 38. 탐지만하고 차단 | 탐지 | 차단 |
| 39. 탐지만하고 차단 | 탐지 | 차단 |
| 40. 탐지만하고 차단 | 탐지 | 차단 |
| 41. 탐지만하고 차단 | 탐지 | 차단 |
| 42. 탐지만하고 차단 | 탐지 | 차단 |
| 43. 탐지만하고 차단 | 탐지 | 차단 |
| 44. 탐지만하고 차단 | 탐지 | 차단 |
| 45. 탐지만하고 차단 | 탐지 | 차단 |
| 46. 탐지만하고 차단 | 탐지 | 차단 |
| 47. 탐지만하고 차단 | 탐지 | 차단 |
| 48. 탐지만하고 차단 | 탐지 | 차단 |
| 49. 탐지만하고 차단 | 탐지 | 차단 |
| 50. 탐지만하고 차단 | 탐지 | 차단 |
| 51. 탐지만하고 차단 | 탐지 | 차단 |
| 52. 탐지만하고 차단 | 탐지 | 차단 |
| 53. 탐지만하고 차단 | 탐지 | 차단 |
| 54. 탐지만하고 차단 | 탐지 | 차단 |
| 55. 탐지만하고 차단 | 탐지 | 차단 |
| 56. 탐지만하고 차단 | 탐지 | 차단 |
| 57. 탐지만하고 차단 | 탐지 | 차단 |
| 58. 탐지만하고 차단 | 탐지 | 차단 |
| 59. 탐지만하고 차단 | 탐지 | 차단 |
| 60. 탐지만하고 차단 | 탐지 | 차단 |
| 61. 탐지만하고 차단 | 탐지 | 차단 |
| 62. 탐지만하고 차단 | 탐지 | 차단 |
| 63. 탐지만하고 차단 | 탐지 | 차단 |
| 64. 탐지만하고 차단 | 탐지 | 차단 |
| 65. 탐지만하고 차단 | 탐지 | 차단 |
| 66. 탐지만하고 차단 | 탐지 | 차단 |
| 67. 탐지만하고 차단 | 탐지 | 차단 |
| 68. 탐지만하고 차단 | 탐지 | 차단 |
| 69. 탐지만하고 차단 | 탐지 | 차단 |
| 70. 탐지만하고 차단 | 탐지 | 차단 |
| 71. 탐지만하고 차단 | 탐지 | 차단 |
| 72. 탐지만하고 차단 | 탐지 | 차단 |
| 73. 탐지만하고 차단 | 탐지 | 차단 |
| 74. 탐지만하고 차단 | 탐지 | 차단 |
| 75. 탐지만하고 차단 | 탐지 | 차단 |
| 76. 탐지만하고 차단 | 탐지 | 차단 |
| 77. 탐지만하고 차단 | 탐지 | 차단 |
| 78. 탐지만하고 차단 | 탐지 | 차단 |
| 79. 탐지만하고 차단 | 탐지 | 차단 |
| 80. 탐지만하고 차단 | 탐지 | 차단 |
| 81. 탐지만하고 차단 | 탐지 | 차단 |
| 82. 탐지만하고 차단 | 탐지 | 차단 |
| 83. 탐지만하고 차단 | 탐지 | 차단 |
| 84. 탐지만하고 차단 | 탐지 | 차단 |
| 85. 탐지만하고 차단 | 탐지 | 차단 |
| 86. 탐지만하고 차단 | 탐지 | 차단 |
| 87. 탐지만하고 차단 | 탐지 | 차단 |
| 88. 탐지만하고 차단 | 탐지 | 차단 |
| 89. 탐지만하고 차단 | 탐지 | 차단 |
| 90. 탐지만하고 차단 | 탐지 | 차단 |
| 91. 탐지만하고 차단 | 탐지 | 차단 |
| 92. 탐지만하고 차단 | 탐지 | 차단 |
| 93. 탐지만하고 차단 | 탐지 | 차단 |
| 94. 탐지만하고 차단 | 탐지 | 차단 |
| 95. 탐지만하고 차단 | 탐지 | 차단 |
| 96. 탐지만하고 차단 | 탐지 | 차단 |
| 97. 탐지만하고 차단 | 탐지 | 차단 |
| 98. 탐지만하고 차단 | 탐지 | 차단 |
| 99. 탐지만하고 차단 | 탐지 | 차단 |
| 100. 탐지만하고 차단 | 탐지 | 차단 |

설정된 정보를 확인한 후 [확인] 버튼을 누르면 완료됩니다

설정 마법사

웹사이트 추가

설정 확인

③ '확인'을 누르면 다음과 같은 내용으로 설정이 저장됩니다.

웹사이트 이름: www.pentasecurity.com:80

ISSAC-Web 사용 여부: 미사용

대소문자 구별 여부: 구별

신뢰할 수 있는 IP: 192.168/16

웹사이트의 다른 이름: www.pentasecurity.co.kr 외 1개

탐지 및 대응 정책: 원타 기본 정책

웹사이트는 여러 개 존재할 수 있으므로 정책적으로 관리한 모든 웹 사이트를 위와 같이 등록합니다.

서비스포트 설정

WAF의 관리도구를 사용하여 네트워크 설정 및 웹 사이트 설정을 끝내면, WAF의 보안 서비스를 이용할 준비가 완료된 것입니다. 이제 WAF의 네트워크 운영 위치에 따라 WAF의 서비스 포트에 이더넷 케이블을 연결합니다.

서비스 포트 추가, 삭제 및 확인

서비스 포트 등록은 [오류! 참조 원본을 찾을 수 없습니다.오류! 참조 원본을 찾을 수 없습니다.]을 통해 CLI에 접근하여 설정할 수 있습니다

CLI에서 [enable] 명령을 입력한 후 인증이 이뤄진후 [configure terminal] 명령어로 configure 모드로 진입합니다. configure 모드에서 [network] 명령어를 통해 network로 들어가야만 서비스 포트 설정 명령어 실행이 가능합니다.

추가

config-network 모드에서 bridge interface를 추가한 후 해당 bridge interface에 서비스 포트를 설정할 수 있습니다.

bridge interface 추가는 [bridge-int] 명령어를 입력 후 물음표(?)를 입력하면 다음에 입력한 값에 대한 정보를 볼 수 있습니다. 아래 처럼 [bridge-int add [bridge interface 명]]을 하여 bridge interface를 추가할 수 있습니다.

```
penta-np# configure terminal
penta-np(config)# network
penta-np(config-network)# bridge-int ?
add add bridge interface
del del bridge interface
penta-np(config-network)# bridge-int add br0
OK.
```

삭제

서비스 포트 삭제는 config-network 모드에서 bridge del 명령어 [bridge del [bridge interface명] [device명]]를 실행하여 설정된 서비스 포트를 삭제할 수 있습니다. 명령어를 실행하면 아래에서 보여지듯 OK를 출력하고 서비스 포트가 삭제 됩니다.

```
penta-np(config-network)# bridge del br0 tp0
OK.
```

bridge interface 삭제는 config-network 모드에서 bridge-int del 명령어 [bridge-int del [bridge interface명]]을 실행하여 설정된 bridge interface를 삭제할 수 있습니다. 명령어를 실행하면 아래에서 보여지듯 OK를 출력하고 bridge interface 삭제 됩니다. 이때 bridge interface에 설정된 서비스 포트는 모두 삭제 됩니다.

```
penta-np(config-network)# bridge-int del br0
OK.
```

확인

설정 된 서비스 포트를 확인하고자 할 시에는 아래 처럼 [show bridge] 또는 [sh bridge] 명령어로 설정된 서비스 포트를 확인할 수 있습니다.

```
penta-np(config-network)# show bridge
-----
Bridge Nic Info
br0 tp0
br0 tp1
-----
```

CLI는 관리자가 서비스포트 설정 시 관리자 입력 값에 대하여 오류가 있을 경우 다음과 같은 오류 메시지를 출력합니다.

서비스포트 연결 및 등록 오류 메시지

| 오류 메시지 | 출력 원인 |
|-----------------------|--------------------|
| % Command incomplete. | 잘못된 명령어를 실행하려 할 경우 |

% Invalid input detected at '^' marker

잘못된 입력값을 넣을 경우(잘못된 입력값 아래 "^" 표시가 보임.)

설치 점검

케이블을 모두 연결하고 정상적으로 웹 서비스와 보안 서비스가 이루어지는지 확인합니다. 환경에 따라 길게는 30초 정도 잠시 정상적인 웹 서비스가 되지 않을 수도 있습니다. 일반 사용자 PC에서 웹 브라우저를 띄운 후에 웹사이트에 이상 없이 접근이 가능한지 확인해 봅니다.

WAF의 관리도구의 위쪽 톨 바에서 "대시보드"를 선택하고, 오른쪽 위의 필터에서 "최근 5분간"과 "트래픽"을 선택하여 그래프에 정상적인 증감 변동이 있는지를 확인합니다.

만일 서비스 포트 게이트웨이의 설정이 잘못되어 있다면, 내부에서는 정상적인 웹 서비스가 이루어지나 외부 인터넷 망에서는 웹 서버가 응답이 없는 것으로 보일 수 있으므로 주의해야 합니다. 반드시 외부에서도 정상적인 웹 서비스가 이루어지는지 확인해야만 합니다.

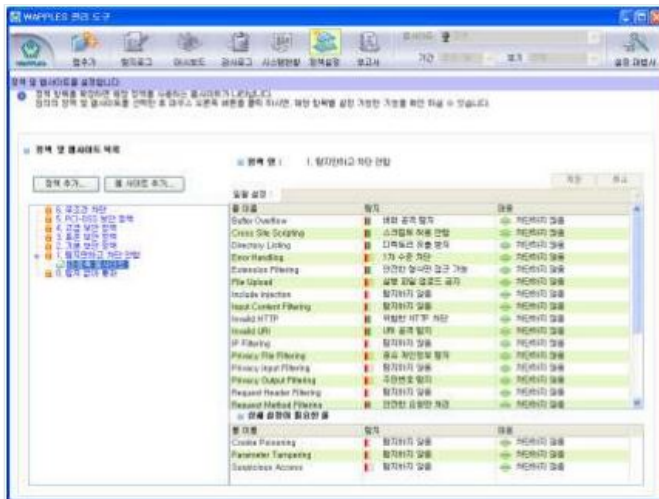
축하 드립니다. 이로써 WAF의 설치가 모두 완료되었습니다.

시험운영

WAF 설치 후, 고객의 사정으로 시험운영이 불가능한 경우또는, 보안 정책 설정에 어려움을 느끼시거나 잘못된 보안 정책 설정으로 도움이 필요할 경우, 별도의 기술지원을 요청하여 본사 또는 협력사의 기술지원 인력에게 보안 정책 설정 컨설팅을 받으실 수 있습니다.

보호하고자 하는 웹사이트의 웹 서비스 내용과 각 탐지 룰의 동작 방법을 미리 완벽하게 숙지하고 탐지 룰을 설정하는 것은 매우 어려운 일입니다. 그렇기 때문에 환경을 최대한 고려하여 설정을 하더라도 항상 원하지 않는 설정 오류가 존재하기 마련입니다. 이러한 오류를 웹 서비스 이용 장애 없이 발견하기 위해 먼저 일정 기간 침입 차단을 하지 않는 시험 운영 기간을 두는 것이 유용합니다.

시험 운영 기간 동안에는 각 침입에 대한 로그는 남기면서도 차단은 하지 않도록 설정하여 설정 문제로 인한 웹 서비스 장애가 없도록 합니다. 시험 운영 중 탐지로그를 토대로 WAF 적절한 정책을 선택한 후에 차단 대응을 커는 과정을 거치도록 하여 보다 안정적이고 믿을 수 있는 보안 서비스를 제공할 수 있습니다.



최초 설치 후 1일 ~ 1주일 간의 시험 운영 기간은 그림과 같이 보호하고자하는 웹사이트를 [탐지만 하고 차단안함] 정책을 기반으로 운영합니다.

시험 운영 기간이 끝나면 그 동안 탐지된 로그들을 분석하고 웹사이트의 상황에 따라 적용할 탐지 룰과 각 탐지 룰에 대한 대응의 활성화 여부, 예외 적용할 사항은 없는지 적절히 판단하여 사용자 정의 정책을 추가하여 정식으로 보안 서비스를 운영합니다.

정책 내의 탐지 룰 설정은 계획한 보안 강도와 서비스하는 웹 페이지의 특성에 따라 결정해야 합니다.

탐지 룰 중 Response Header Filtering, Suspicious Access, Privacy Output Filtering 등의 몇몇 룰은 '차단 안 함'으로 설정시 설정과 상관 없이 웹 페이지의 내용을 변경하거나 차단할 수 있으므로 주의하여야 합니다.

탐지 룰 예외 처리

탐지 예외 처리는 일부 특정 웹 페이지나 특정 IP 주소에 대해 탐지 룰 적용을 하고 싶지 않을 때 사용합니다.

가장 자주 예외 처리가 발생하는 예로는 Suspicious Access에 대한 예외 처리가 있을 수 있습니다. 이 룰은 웹 서비스에 접속하는 웹 브라우저가 정상인지 검사하고, 이상이 발견되면 접속을 거부하게 됩니다. 보통의 웹 페이지에서는 문제가 없으나, e-mail을 보낼 때 첨부 이미지 파일 등의 내용 일부를 웹 서버 위에 두는 경우가 있습니다. 이런 경우 e-mail 프로그램이 웹 브라우저가 아니기 때문에 WAF에 의해서 접근이 차단되어 e-mail의 내용이 제대로 보이지 않을 수 있습니다. 일반적인 경우 e-mail에 사용되는 페이지는 한정되어 있으므로 이 부분만 예외로 등록하면 정상적인 내용을 볼 수 있습니다.

탐지 예외 설정을 하려면 설정 마법사에서 다음과 같은 순서로 따라 가면 됩니다.

[정책설정] -> [설정 하고자 하는 웹 사이트 선택 후 오른쪽 클릭] -> [웹 사이트 예외 설정] -> [완료]

탐지 예외 설정은 아래와 같은 화면에서 설정합니다. 설정 열에 표시된 숫자는 각 룰에 대하여 예외 처리가 되어 있는 URL의 개수입니다.



Suspicious Access 에 대한 예외 URL를 설정하기 위해 Suspicious Access를 선택하고 다음을 누르면 아래 같은 화면이 나타납니다.



[추가] 버튼을 눌러 예외 처리할 URL과 IP 주소를 넣어 [예외 처리된 URL] 목록에 추가합니다. 이 화면에서는 "/EMAIL/"를 추가하였습니다. IP주소는 모든 IP에 대해서 전부 예외 처리할 경우 비워두어도 됩니다. [다음]을 누르고 [확인]을 누른 후 설정 마법사를 완료하면 원하는 URL과 IP에 대해서 예외 처리 됩니다.

정책 변경

시험 운영을 통하여 운영 환경에 맞는 적절한 정책 설정을 확인하고 필요한 예외 처리를 마치면 정책을 변경하여 외부의 공격을 실제 차단 할 수 있도록 해주어야 합니다. 정책 내의 차단 대응 설정을 적용하여 정식 운영을 시작합니다.

차단 대응 설정을 할 때에는 오탐의 여부와 공격의 위험성 등을 고려하여 차단을 설정 합니다. 차단 설정은 일부 룰에 대해서는 설정이 불가능합니다. Suspicious Access, Response Header Filtering은 차단을 하지 않습니다.

탐지 예외 설정을 하려면 설정 마법사에서 다음과 같은 순서로 따라 가면 됩니다.

정책의 대응 설정 변경을 하려면 설정 마법사에서 다음과 같은 순서로 따라 가면 됩니다.

[정책 설정] -> [정책 선택] -> [정책선택에서 오른쪽 마우스 클릭] -> [정책 수정] -> [확인] -> [저장]



대응 설정 변경할 룰을 체크하고 다음을 누르면 아래 화면에서 각 룰에 대한 대응 설정 변경을 할 수 있습니다. 차단 수행 여부를 선택합니다.



오른쪽 대응 설정의 바로 위로 올려 원래의 [차단하지 않습니다] 이외의 내용을 선택하면 됩니다. 모두 3가지 차단 방법 중 하나를 선택할 수 있습니다.

제일 상단의 [연결 끊기]를 선택하면 침입이 탐지되었을 때 해당 HTTP 통신을 즉시 끊습니다. 이 경우 공격자의 웹 브라우저에는 아무런 메시지도 나타나지 않습니다.

위에서 두 번째의 [에러 코드 보냄]은 HTTP 규약에 정의된 에러에서 원하는 에러를 반환합니다. 대표적으로 400 BadRequest 같은 에러가 있습니다.

세 번째의 [다른 웹 페이지로 이동]은 관리자가 별도의 에러 처리 페이지를 만든 후에 이 페이지로 자동으로 연결 되도록 합니다.

설치 제거

설치된 WAF을 네트워크에서 제거하는 작업은 먼저 WAF의 서비스 포트로 가도록 되어 있는 웹 서비스 구성을 원래대로 웹 서버로 가도록 하는 일에서 시작합니다. 이는 설치 때와 마찬가지로 운영 형태 구성에 따라 달라집니다.

리버스 프락시 구성의 경우 설치 제거 방법

WAF의 서비스 포트로 향하도록 구성된 포트포워딩 룰 혹은 VPX 설정을 원래대로 웹 서버로 향하도록 수정합니다.

운영 전 준비

본 장은 WAF을 운영하기 전 설정들을 소개하는 장으로 WAF Agent, WAF 관리도구 로그인, 비밀번호 변경, 관리도구의 초기화면 설명 등에 대한 설명을 담고 있습니다.

관리도구 사용하기

로그인

WAF 관리도구는 인가된 관리자만이 접근할 수 있습니다. 처음 웹 서버를 통하여 WAF 관리도구에 접속을 시도하면 아래화면이 나타납니다.



관리자는 3개의 모드를 사용하여 관리도구에 로그인합니다.

관리자 운영 모드

| 관리자 종류 | 설명 |
|------------|---|
| [운영자] | 관리도구의 설정마법사, 탐지로그, 대시보드, 감사로드조회 등 WAF 운영 전반에 걸친 모든 기능을 사용합니다. |
| [조회자] | 설정 마법사를 제외한 탐지로그, 대시보드, 감사로그를 조회할 수 있습니다. |
| [웹사이트 관리자] | 관리도구의 탐지로그, 대시보드, 감사로드 조회에 대해 웹사이트 관리자가 관리하고 있는 웹 사이트 정보에 한해서 확인할 수 있습니다. 설정마법사 및 웹사이트 추가 기능은 사용할 수 없습니다. |

아이디와 비밀번호를 입력하고 [확인] 버튼을 클릭하면 아이디에 따라 운영자, 웹사이트 관리자 혹은 조회자로 로그인을 하게 됩니다.

입력되는 비밀번호는 비밀번호 유출 방지를 위하여 '*'로 표시됩니다.

WAF의 인가된 관리자는 악의가 없으며, WAF의 관리기능에 대해 적절히 교육 받고, 관리자 지침에 따라 정확하게 의무를 수행해야 합니다. 운영자는 운영 전반에 걸친 관리도구의 모든 기능을 이용할 수 있으며 조회자는 설정 마법사를 제외한 탐지로그, 대시보드, 감사로그를 조회할 수 있습니다. 웹사이트 관리자는 관리도구의 탐지로그, 대시보드, 감사로드 조회에 대해 웹사이트 관리자가 관리하고 있는 웹사이트 정보에 한해서 조회할 수 있습니다. 또한 웹사이트 관리자가 관할하는 웹사이트에 대한 정책도 수정할 수 있습니다.

관리도구는 WAF시스템의 안전을 위하여 다음과 같은 보안기능을 제공합니다.

관리도구와 WAF 간에는 암호화되어 통신

관리도구와 WAF 간에는 암호화되어 통신되므로 통신 내용의 일부가 노출되더라도 안전하게 보호됩니다.

관리자 비밀번호 유추공격 차단

올바르지 못한 비밀번호로 로그인 시도 시 3회까지 재입력을 요구하며 3회 실패 시 관리도구를 종료합니다.

관리도구는 운영자 및 조회자의 아이디와 비밀번호가 일치하지 않을 경우 다음과 같은 오류 메시지를 출력합니다.

로그인 오류 메시지

| 오류 메시지 | 출력 원인 |
|--------|-------|
| | |

| | |
|------------------|--------------|
| 비밀번호가 맞지 않습니다. | 로그인 실패 |
| 비밀번호 입력 3회 오류입니다 | 로그인 연속 3회 실패 |

로그인 연속 3회 실패 로그 발생시 관리도구는 보안 경보 메시지를 출력합니다. 출력되는 보안 경보 메시지는 다음과 같습니다.

로그인 연속 3회 실패 보안 경보 메시지

| 보안 경보 메시지 | 출력 원인 |
|----------------------------|-------------------------|
| "로그인 연속 실패" 감사로그가 검색되었습니다. | 로그인 연속 3회 실패 로그가 기록된 경우 |

보안 경보 메시지는 로그인 3 회 연속 실패, IP 차단, DB 용량 위험 감사로그, DB 용량 초과 감사로그가 기록된 경우 출력되며 가장 최근에 기록된 해당 로그 1 개에 대해서만 보안 경보 메시지를 출력합니다.

관리자 정보 변경

위 그림에서 [로그인 후 사용자 정보 변경]을 체크하고 로그인하면 관리자 정보를 다시 설정할 수 있습니다. 모든 아이디에 대해 제공되는 WAF 관리도구의 접속에 필요한 비밀번호는 기본적으로 "penta" 이며 이 비밀번호로 접속하면 "로그인 후 사용자 정보 변경"을 체크 했을 때와 같이 사용자 정보를 변경할 수 있는 화면이 나타납니다.

사용자 정보 변경을 선택하거나 최초의 로그인인 경우 아래화면에서 변경할 수 있습니다. 운영자와 조희자, 웹사이트 관리자의 비밀번호는 각각의 아이디에 대해 독립적으로 관리되어 서로 다른 비밀번호로 변경 할 수 있습니다.

비밀번호는 6자 이상이어야 하며 특수문자를 1개 이상 포함 하여야 합니다. 이와 같은 규칙에 어긋날 경우 재입력을 요구합니다.

입력되는 비밀번호는 비밀번호 유출방지를 위하여 '*'로 표시됩니다.

새로 입력되는 비밀번호를 2회 입력 받아 입력 받은 비밀번호가 동일하지 않으면 재입력을 요구하여 사용자의 실수를 미연에 방지합니다.

관리도구는 비밀번호 변경에 실패할 경우 다음과 같은 오류메시지를 출력합니다.

사용자 정보 변경 오류 메시지

| 오류 메시지 | 출력 원인 |
|--------------------------------|--|
| 비밀번호는 6자리 이상이어야 합니다. | 변경할 비밀번호가 6자리 미만일 경우 |
| 비밀번호는 1개 이상의 특수문자를 포함 하여야 합니다. | 변경할 비밀번호가 특수문자를 포함하지 않을 경우 |
| 신규비밀번호와 재입력 비밀번호 값이 일치하지 않습니다. | 변경할 비밀번호를 2회 입력받아 입력 받은 비밀번호가 동일하지 않을 경우 |

안전한 비밀번호로 설정한 후 관리자의 e-mail 정보를 입력합니다. 저장되는 관리자의 e-mail 주소로 DB FULL 발생 하였을시 경고 메일 및 삭제 알림 메일을 발송합니다.

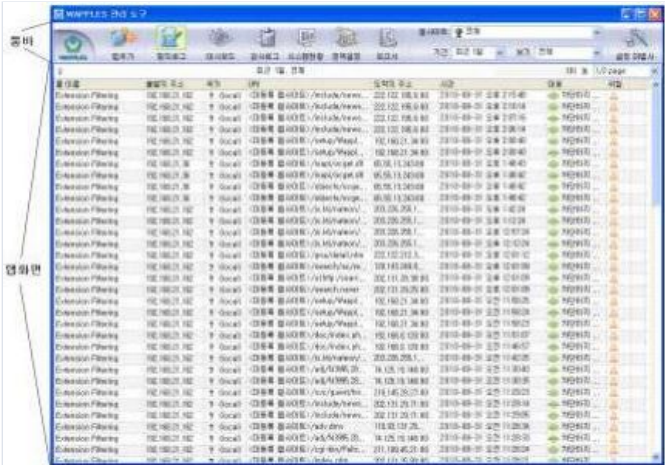
송신 측 메일 주소 및 SMTP 주소 [X설정방법사]->[운영 설정]-> [오류! 참조 원본을 찾을 수 없습니다.]에서 수정할수 있습니다

관리자 E-MAIL 주소 설정 오류 메시지

| 오류 메시지 | 출력 원인 |
|---------------|---|
| 이메일 형식이 아닙니다. | 보내는 E-MAIL 주소와 받는 E-MAIL 주소가 E-MAIL 형식이 아닐 경우 |
| 잘못된 IP입니다. | 입력한 SMTP 주소가 잘못된 경우. |

관리도구 초기화면

로그인에 성공하면 다음과 같은 화면을 볼 수 있습니다. 초기 화면은 상단의 툴 바와 하단의 탭 화면으로 나누어 집니다.



툴 바는 다음과 같은 컨트롤로 구성되어 있습니다.

- 최대 10개의 탭을 추가할 수 있는 [탭추가] 버튼
- 탭화면 [탐지로그], [대시보드], [감사로그], [시스템 현황]을 전환하는 전환버튼

- 탭화면에서 표시되는 여러 가지 내용을 필터링할 수 있는 필터그룹
- [설정 마법사]

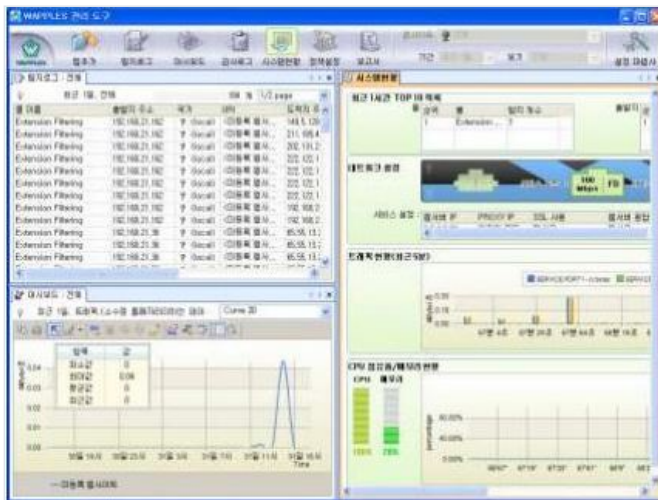


툴 바의 설정 마법사 버튼은 운영자로서 로그인에 성공할 경우 화면에 출력됩니다. 조회자로서 로그인에 성공할 경우 툴 바의 설정 마법사 버튼은 화면에 출력되지 않습니다

탭 화면

탭 추가

[탭추가] 버튼을 클릭하면 탭 화면이 추가됩니다. 추가된 화면은 보는 대상(정책설정, 탐지로그, 시스템현황,)이나 필터를 따로 설정 할 수 있으며 화면을 분할하여 동시에 여러 탭을 볼 수도 있습니다. 최대 10개의 탭을 추가할 수 있습니다.



탐지로그, 대시보드, 감사로그, 시스템 현황 전환 버튼

[탐지로그], [대시보드], [감사로그], [시스템현황] 버튼은 활성화된 탭 화면의 내용을 전환하는 역할을 합니다.

[탐지로그] 버튼은 탭 화면에 탐지 로그를 보여주고, [대시보드] 버튼은 웹 서버의 트래픽 데이터나 탐지 데이터에 대한 그래프를 보여주고, [감사로그] 버튼은 관리자의 로그인이나 설정 변경 등의 행위에 대한 감사 데이터를 보여주는 화면으로 전환 됩니다. [시스템현황] 버튼은 WAF의 시스템 상황을 화면에 보여주는 화면으로 전환됩니다.

추가된 탭은 각각을 한꺼번에 보거나 또는 일부만을 선택하여 보는 것이 가능합니다.

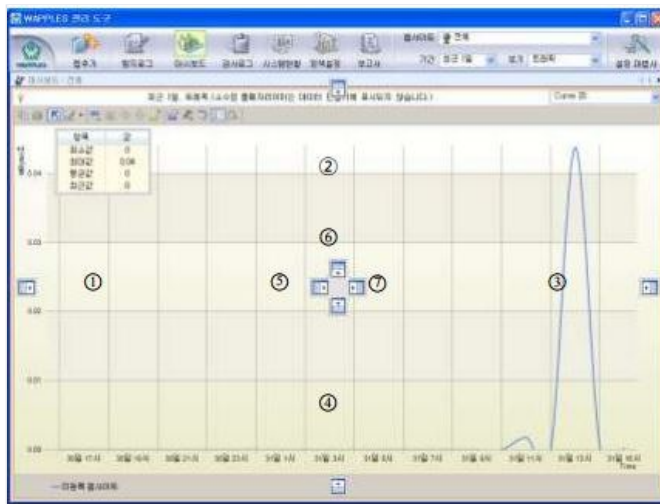
[탭추가] 버튼과 전환 버튼을 이용하여 첫 번째 탭 화면에서는 탐지로그를, 두 번째 화면에서는 대시보드를 보도록 설정한 화면은 다음과 같습니다.

그림 44. 탭 추가 후 대시보드 선택

탭 화면 분할



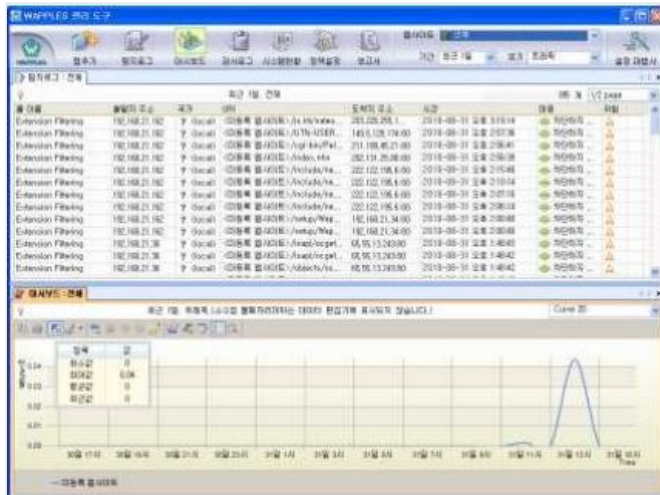
그림과 같이 탭화면의 이름 [대시보드:전체]를 선택하고 마우스 왼쪽 버튼을 클릭한 상태로 끌기를 하면 아래 화면과 같은 화면이 나타나면서 탭을 분할할 수 있습니다.



탭 화면의 상하좌우에 조그마한 아이콘이 생기는데 이곳으로 끌어다놓기를 하면 아이콘 방향으로 탭이 분리됩니다.

바깥쪽 아이콘인 ①,②,③,④은 전체 화면에서의 상하좌우 위치이고 ⑤⑥⑦⑧과 같은 안쪽 아이콘은 지금 해당되는 화면의 상하좌우 위치 입니다.(현재의 화면에서는 화면이 1개 이므로 의미가 같게 됩니다.)

그림에서 ④번 위치로 끌어다 놓기를 하면 아래와 같이 화면이 상하로 분할 됩니다.



이러한 방식으로 하나의 WAF 관리도구에서 한번에 여러 화면을 조회하여 볼 수 있습니다. 또 각 탭 화면 간의 경계에서 끌어다 놓기를 하면 각각의 화면 크기를 조절할 수 있습니다. 또 관리자의 필요에 부합하는 유연하고 자유로운 화면 구성이 가능합니다. 이 화면 구성 내용은 자동으로 저장되기 때문에 관리도구를 재기동 하여도 그대로 유지됩니다.

웹사이트, 기간, 보기 필터

필터 부분은 웹사이트 필터, 기간 필터, 보기 필터가 있습니다. 각각의 필터 내용은 해당되는 탭 화면의 내용에 따라 달라질 수 있습니다.

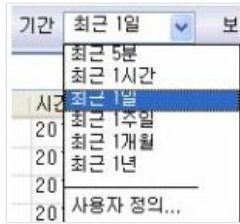
웹사이트 필터

웹사이트 필터는 조회한 웹사이트를 선택하여 볼 수 있도록 합니다. 어느 웹사이트 하나만을 선택하거나 전체를 선택할 수 있습니다. 단, 감사로그를 볼 때에는 감사로그 자체가 각 웹사이트의 개별 로그가 아니기 때문에 선택할 수 없습니다.

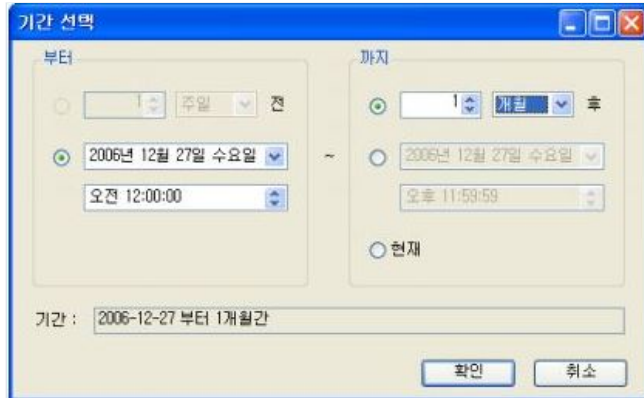


기간 필터

기간 필터는 조회할 데이터의 기간을 선택하여 볼 수 있는 필터 입니다. 간단하게 현재부터 5분, 1시간, 1일, 1주일, 1개월, 1년 등을 선택할 수 있으며, [사용자 정의..]를 선택하면 기간을 자유롭게 지정할 수 있습니다.



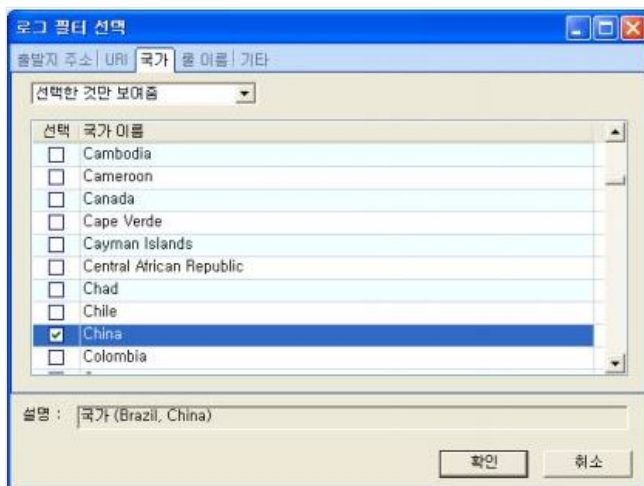
그림에서 사용자 정의를 선택하면 아래와 같은 화면에서 자유롭게 기간을 선택할 수 있습니다. 아래화면은 2006년 12월 27일부터 1개월간의 내용을 보고 싶을 때의 설정 예 입니다.



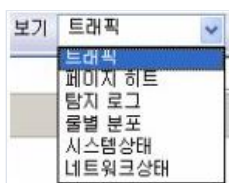
보기 필터

보기 필터는 탐지로그, 대시보드, 감사로그 화면에 따라 완전히 다른 기능을 하게 됩니다.

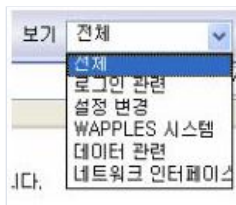
탐지로그의 경우 간단히 각 룰 별로 선택하여 보여주거나, [사용자 정의..] 메뉴를 사용하여 IP, URI, 국가, 룰 별 등의 여러 필터를 자유롭게 조합하여 볼 수 있습니다. 탐지로그의 보기 필터에 대한 자세한 설명은 [V 탐지로그]에서 볼 수 있습니다.



대시보드는 다음과 같은 범주로 나누어 볼 수 있습니다. 대시보드의 보기 필터에 대한 자세한 설명은 [VI 대시보드]에서 볼 수 있습니다.



감사로그에서 보기 필터는 전체를 보거나 범주 별로 나누어 볼 수 있습니다. 감사로그의 보기 필터에 대한 자세한 설명은 [VII 감사로그]에서 볼 수 있습니다.



설정 마법사

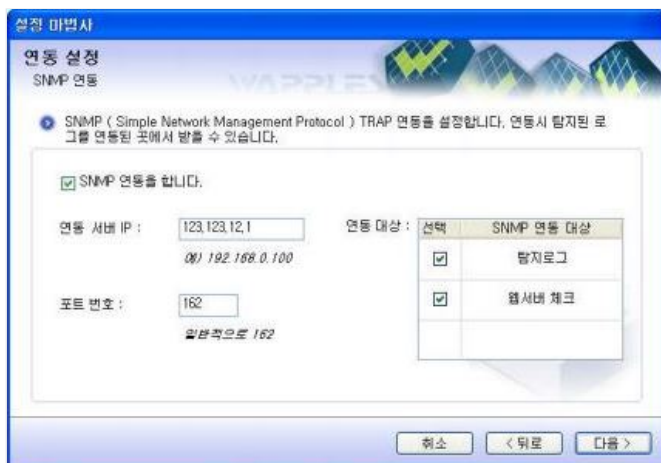
[설정 마법사] 버튼을 클릭하면 아래화면이 나오고 WAF의 관리포트 IP와 관련된 항목을 제외한 모든 항목의 설정을 변경을 할 수 있습니다.



WAF의 설정 변경은 설정 마법사를 따라 가면서 손쉽게 할 수 있습니다. 자세한 내용은 [IX 설정마법사]장에서 볼 수 있습니다.

모든 설정들은 설정 마법사의 가장 마지막에 있는 [완료] 버튼을 클릭 해야 WAF 시스템에 설정 내용이 저장되고 적용됩니다. 만약 설정을 진행하다가 잘못 설정한 부분이 있거나 원래의 설정으로 되돌리고 싶으면 [취소] 버튼을 클릭하여 설정을 취소 할 수 있습니다.

WAF 관리도구의 설정 마법사는 사용자의 실수를 최대한 방지하기 위하여 많은 부분이 설정 가능한 내용을 보여주고 이를 선택하는 방식으로 구성되어 있습니다. 그러나 일부 설정 내용은 사용자가 직접 입력하여야 합니다. 예를 들어 IP 주소를 입력해야 할 때, 각각의 숫자는 0~255 사이로 넣어야 합니다. 이러한 부분을 잘못 입력하였을 때 아래화면에서 보이는 바와 같이 빨간색 느낌표 (!)마크가 잘못된 곳의 오른쪽에 표시되고 이 표시 위에 마우스 커서를 놓으면 잘못된 이유가 나타납니다. !마크가 표시되면 설정 마법사에서 다음으로 진행 할 수가 없습니다. 반드시 잘못된 사항을 수정하고 진행하여야 합니다.



설정 마법사는 운영자로 로그인한 경우에만 접근이 가능합니다.

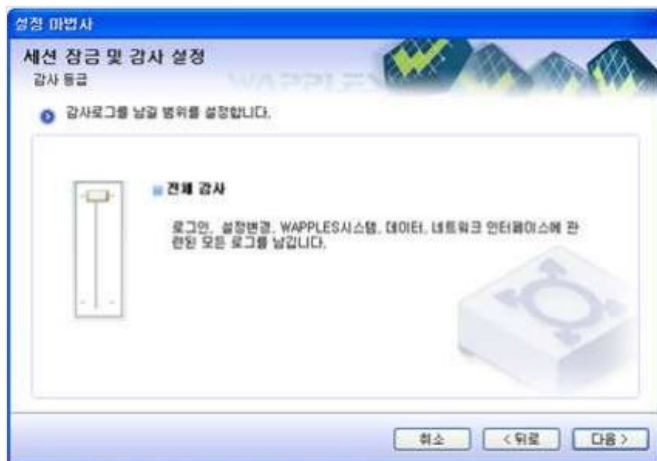
세션 잠금 및 감사 설정

[감사 설정]은 감사 수준별 감사로그를 기록하기 위해 인가된 관리자에게 보여지는 감사 기록의 수준을 선택할 수 있는 기능입니다.

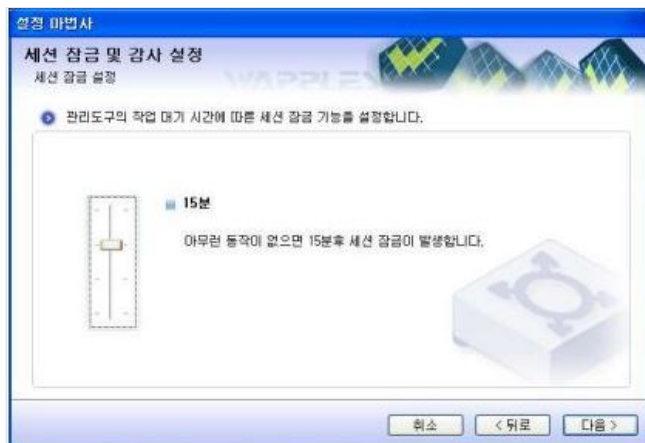
감사 등급은 [기본감사]와 [전체감사]가 있으며 각각의 의미와 감사 항목은 아래 표에서 설명합니다.

감사 수준별 감사 항목

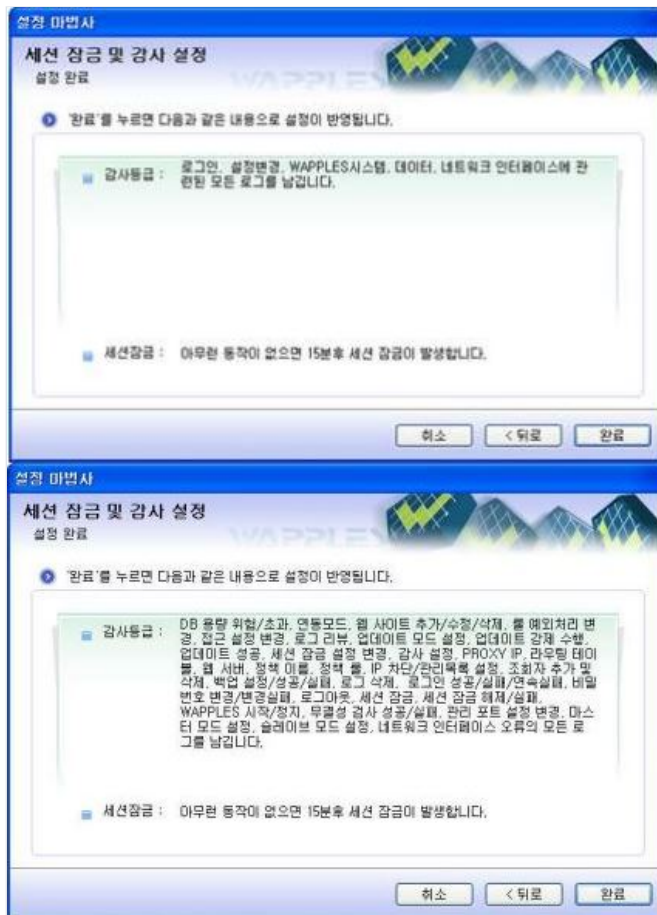
| 감사 수준 | 설명 | 감사 항목 |
|-------|--|--|
| 기본감사 | WAF 시스템의 중대한 사건이나 변경사항에 대한 감사 자료를 기록합니다. | DB용량 위험/초과, 연동모드, 웹 사이트 추가/수정/삭제, 룰 예외처리 변경, 접근설정 변경, 로그 리뷰, 업데이트 설정, 업데이트 성공, 세션 잠금 설정 변경, 감사설정, WAF IP, 라우팅 테이블, 웹 서버, 정책 이름, 정책 룰, 백업 설정/성공/실패, 로그 삭제, 로그인 실패/연속실패, 비밀번호 변경/실패, 세션 잠금 실패, WAF 시작/정지, 무결성 검사 실패, 관리포트설정 변경, 백업 설정, 네트워크 인터페이스 오류, 보안 경고, 조회자 아이디 추가/삭제, 시간동기화 설정 변경, 시간동기화 성공/실패, 표준 시간대 변경/실패,패턴저장소 설정 변경, 정책/로그 동기화 설정/결과, 보고서 메일 보내기 성공/실패, 기능별 라이선스 등록 성공/실패 |
| 전체감사 | 기본 감사 항목 외에 일반적인 정보 및 주기적인 점검 사항의 정상 작동에 관한 내용까지 감사 자료로 기록합니다. | 기본 감사 수준의 감사 항목 및 업데이트 강제 수행, IP 차단/관리목록 설정, 조회자 추가 및 삭제, 로그아웃, 세션 잠금, 세션 잠금 해제, WAF 시작/정지, 무결성 검사 성공, 관리포트 설정 변경, |



[감사 등급 설정]화면에서 슬라이드 바를 상하로 끌어서 기본 혹은 전체 감사상태로 바꾼 후 [다음] 버튼을 클릭합니다



[세션 잠금 설정]은 관리자가 WPPLES 관리도구에 로그인 한 상태로 장시간 자리를 비웠을 때 보안을 위하여 일정 시간 이후 자동으로 관리 도구에 접근을 차단하는 기능입니다. [세션 잠금 설정] 화면에서는 세션 잠금이 발생하는 시간을 5분/15분/30분/사용안함 으로 조절 할 수 있습니다.



[세션 잠금 설정] 화면에서 [다음] 버튼을 클릭하면 **[오류! 참조 원본을 찾을 수 없습니다.오류! 참조 원본을 찾을 수 없습니다.]**화면이 나타납니다. [완료] 버튼을 클릭하면 세션 잠금 및 감사 설정이 저장 되어 WAF에 반영됩니다.

세션 잠금 기간 설정을 하면 설정된 시간 동안 WAPPLES 관리도구 프로그램에 키보드 입력이나 마우스 클릭이 없을 경우 WAF 관리도구와 WAF간의 연결이 끊어지고 **[오류! 참조 원본을 찾을 수 없습니다.]**화면이 나타납니다.

[오류! 참조 원본을 찾을 수 없습니다.]화면에서 세션 잠금을 해제하거나 관리도구를 종료할 수 있습니다. 관리도구를 다시 사용하려면 암호를 재 입력하고 [세션 잠금 해제]버튼을 클릭합니다.

[오류! 참조 원본을 찾을 수 없습니다.]화면은 아이디는 입력할 수 없으며 비밀번호 입력만을 허용합니다. 로그인 방법은 아이디와 비밀번호 변경 체크박스를 입력할 수 없을 뿐 [III.1.1 로그인] 과 동일합니다.



백업 설정

WAF에 기록된 설정 정보, 탐지 로그 및 감사로그를 WAF 시스템 혹은 외부의 FTP서버로 백업 데이터를 저장하기 위해 [백업 설정] 기능을 사용합니다.



백업단위는 매일, 매주, 매월, 사용 안 함을 설정할 수 있습니다.

매일 백업을 원할 경우 백업시간을 입력하고 매주 백업을 원할 경우 원하는 요일과 백업 시간을 입력합니다. 매월 백업을 원할 경우 백업 날짜와 시간을 입력합니다.

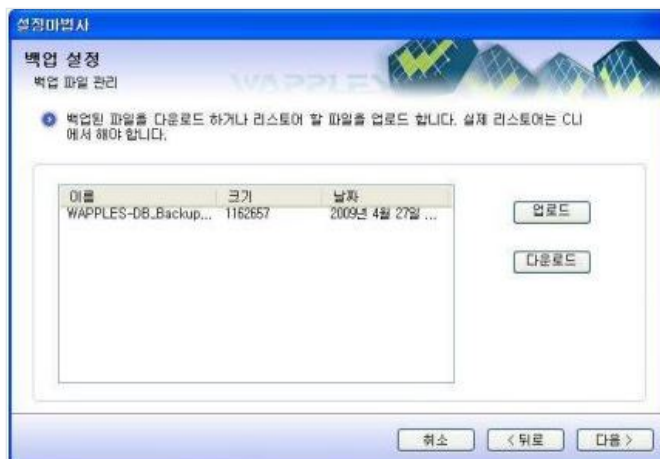
백업은 FTP를 사용하여 백업 데이터를 전송합니다. FTP 사용에 필요한 정보인 FTP 서버 IP, FTP 서버 경로, FTP 아이디, FTP 비밀번호를 입력합니다.

백업 설정 오류 메시지

| 오류 메시지 | 출력 원인 |
|-------------------|---|
| 하나 이상의 요일을 선택합니다. | 백업단위를 [매주]로 선택 시 하나 이상의 요일에 체크하지 않았을 경우 |
| 빈칸일 수 없습니다. | Remote 백업 선택 시 FTP 서버 IP, FTP 서버 경로, FTP 아이디, FTP 비밀번호 입력 값이 빈칸일 경우 |
| 잘못된 IP 입니다. | FTP 서버 IP 가 올바른 IP형식이 아닐 경우 |

[오류! 참조 원본을 찾을 수 없습니다.] 화면에서 [다음] 버튼을 클릭하면 **[오류! 참조 원본을 찾을 수 없습니다.]** 화면이 나타납니다.

다운로드 받을 백업파일을 선택 후, [다운로드]버튼을 누르면 백업파일을 다운로드합니다. [업로드] 버튼을 누르고 백업파일을 선택한 후 열기 버튼을 누르면 백업파일을 시스템에 업로드 합니다.



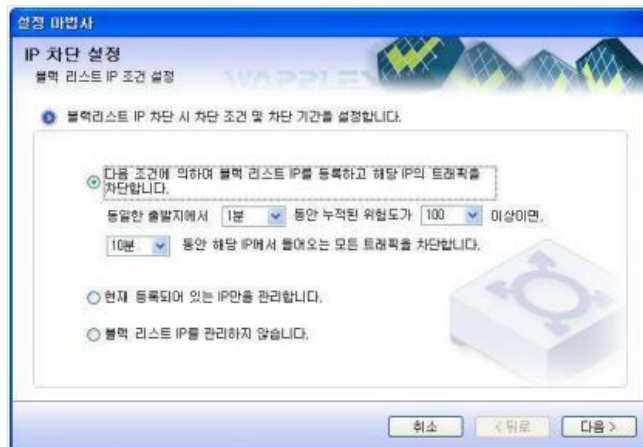
[오류! 참조 원본을 찾을 수 없습니다.] 화면에서 다음 버튼을 클릭하면 **[오류! 참조 원본을 찾을 수 없습니다.]**과 같은 [설정 완료] 화면이 나타납니다. 이 화면에서 설정 내용을 확인하고 [완료] 버튼을 클릭합니다.



IP 차단 설정

IP차단은 하나의 출발지에서 계속하여 공격을 시도하는 것을 막기 위해 사용됩니다. WAF은 같은 출발지에서 발생한 공격을 탐지하여 차단한 사건에 대하여 시간당 위험도를 점수로 기록하고 누적 점수가 설정치 이상이 되었을 때 일정시간 그 출발지에서 발생하는 모든 트래픽을 차단 하도록 합니다.

이 화면에서 IP 차단 관리목록에 대한 IP 관리 기능을 활성화 할지 여부를 선택하고, 활성화 한다면 어떠한 조건으로 IP 차단 관리목록을 등록하고 얼마나 오랫동안 관리한지 혹은 현재 등록되어 있는 IP막을 관리 할지를 설정할 수 있습니다.



[다음] 버튼을 클릭하면 [오류! 참조 원본을 찾을 수 없습니다.]화면이 나타납니다. 다음과 같은 항목을 설정할 수 있습니다.

- 연결 차단 IP/연결 차단 시간
- 연결 허용 IP /연결 허용 시간

[특정 IP 혹은 IP 대역에 대해 일정 시간 동안 연결을 차단하거나 허용 할 수 있습니다. 설정을 원하는 IP와 연결 차단 혹은 연결 허용할 시간을 입력하고 [해당 IP 연결 허용] 체크 박스에 허용 유무를 체크한 뒤 추가 버튼을 사용하여 관리 IP를 관리 IP 목록에 추가합니다.



설정된 IP의 수정/삭제는 IP 리스트에서 삭제할 IP를 선택하고 [수정]/[삭제] 버튼을 누른 후 [다음]을 클릭하면, 설정 요약 화면이 나타납니다. 설정한 내용을 다시 한번 확인하고 [완료] 버튼을 클릭하면 IP차단 설정 내용이 WAF에 적용됩니다.

설정 마법사는 IP 차단 설정 시 사용자 입력 값에 오류가 있을 경우 다음과 같은 오류 메시지를 출력합니다.

로그인 오류 메시지

| 오류 메시지 | 출력 원인 |
|-----------------------------|-------------------------------------|
| 잘못된 IP입니다. | 관리 IP 추가/수정 시 입력된 IP가 IP형식이 아닐 경우 |
| 현재 시간부터 5분 이상을 설정 할 수 있습니다. | 설정된 시간이 현재 시간부터 5분 이상의 미래 시간이 아닐 경우 |

IP 관리 종료 예정 시간은 현재의 시간보다 5 분 이상의 미래의 시간을 입력해야 합니다.



IP차단을 위한 위험도 설정은 정책설정의 모든 룰에서 설정이 가능합니다. 다음은 Buffer Over Flow 룰의 위험도 설정 화면입니다. 대응 하단의 위험도를 각 룰의 점수를 설정합니다.



룰의 위험도 설정은 탐지 프로세스에 적용되기 때문에 '탐지'와 '사용자정의' 설정에서만 수정이 가능하고, '탐지안함' 상태에서는 위험도 수치를 설정할 수 없습니다.

E-MAIL 설정

[오류! 참조 원본을 찾을 수 없습니다. 오류! 참조 원본을 찾을 수 없습니다.]과 [IX 설정마법사 오류! 참조 원본을 찾을 수 없습니다. 오류! 참조 원본을 찾을 수 없습니다.]의 [탐지로그 연동] 기능에서 사용하는 EMAIL 관련 정보를 설정할 수 있습니다.

[운영 설정]에서 [E-MAIL 설정]을 클릭하면 다음과 같은 화면이 나타납니다.



보내는 주소는 E-MAIL 발신자의 E-MAIL 주소를 의미하며, SMTP 주소는 SMTP 서버의 IP 주소를 의미합니다.

설정이 끝난 후, 화면 우측 하단의 [다음>]버튼을 클릭합니다. [오류!참조 원본을 찾을 수 없습니다.]이 나타나면 설정된 내용을 확인한 후 화면 우측 하단의 [완료] 버튼을 클릭합니다.



계정 관리 참조

탐지룰의 이해

이번 장에서는 WAF 운영 기본 지식인 탐지 룰에 대한 설명을 합니다.

탐지룰의 정의

탐지룰이란 WAF이 웹 트래픽을 검사하여 웹 공격을 탐지하고 차단하는 기준 요소입니다. WAF은 정상적인 웹 트래픽과 웹 공격을 이들 탐지룰의 근거로 검사하고 탐지 근거를 기록합니다.

WAF의 탐지룰은 단순한 패턴 형식으로 구성된 일대일 대응 기재가 아니라, 웹 트래픽에 대한 논리적 분석을 바탕으로 웹 공격을 찾아내는 방식입니다. 따라서, 새로운 형태의 웹 공격이나 기존 공격의 일부분을 변형시켜 만들어진 변칙 공격에 대해서도 추가적인 패턴 업데이트 없이 탐지가 가능한 장점이 있습니다. WAF은 이러한 탐지룰을 웹 공격의 형식에 따라 24가지로 분류하여 활용하고 있습니다. 그리고, 각 탐지룰의 활성화 여부의 조합을 탐지 정책으로 설정하여 웹 서버를 보호합니다.

WAF이 제공하는 기본 제공 탐지 정책은 안정적인 운영을 위하여 일부 탐지 룰을 사용하지 않도록 되어 있습니다. 기본정책에 대한 세부내용은 [오류! 참조 원본을 찾을 수 없습니다.]에서 볼 수 있습니다. 관리자는 웹사이트 별로 특수한 요구 사항이 있거나, 보안강도를 높이거나 낮추기 위하여 정책의 룰 별 탐지 및 대응 설정을 변경할 수 있습니다.

탐지 룰에 대한 이해를 돕기 위해 탐지 룰들을 탐지 위치, 탐지 방식, 공격 방식에 따라 다음과 같이 분류하였습니다.

탐지 위치에 따른 탐지를 분류

웹 서비스는 기본적으로 HTTP Request Message와 HTTP Response Message로 이루어져 있습니다. WAF은 각각의 보안 위협 종류와 그 내용에 따라 Request Message 또는 Response Message에서 위협이 되는 부분을 탐지합니다. 만약 Request Message에서 탐지가 가능한 위협에 대해 차단 설정을 하면, 보호 대상이 되는 웹 서버에 Request Message가 전달되지 않습니다. 반면 Response Message에서 탐지되는 위협에 대한 차단 설정은 침입을 시도한 결과가 침입자에게 전달되지 못하게 합니다.

탐지 위치에 따라 분류해보면 다음 표와 같습니다.

탐지 위치에 따른 분류

| | |
|-----------------------|---|
| HTTP Request Message | Buffer Overflow, Cookie Poisoning, Cross Site Script, Extension Filtering, File Upload, Input Content Filtering, Include Injection, Invalid Http, Invalid URI, IP Filtering, Parameter Tampering, Privacy File Filtering, Request Header Filtering, Request Method Filtering, SQL Injection, Stealth Commanding, Suspicious Access, Unicode Directory |
| HTTP Response Message | Directory Listing, Error Handling, Invalid Http, Privacy Output Filtering, Response Header Filtering, Website Defacement |

탐지 방식에 따른 탐지를 분류

WAF의 탐지률은 탐지 방식에 따라 [일반 탐지], [상호 작용], [정보 감춤/변조]로 분류할 수 있습니다

일반적인 탐지는 Request/Response Message의 통신 내용을 검사하는 것으로 보안 위협을 판별할 수 있는 방식입니다.

상호 작용 탐지는 WAF이 마치 질문/응답을 하는 것처럼 의심되는 공격자에게 특수한 상황을 만들어주고 이에 대한 응답을 분석하여 탐지하는 방식입니다.

정보 감춤/변조는 웹 서버와 클라이언트 간의 통신 상에서 실제 서비스 이용에는 별로 필요가 없으나 공격에는 의미 있는 부분을 감추거나,정책상 노출되지 말아야 할 정보 등을 자동으로 변조해 주는 방식입니다.

탐지 방식에 따른 분류

| | |
|----------|--|
| 일반 탐지 | Buffer Overflow, Cross Site Script, Directory Listing, Error Handling, Extension Filtering, File Upload, Include Injection, Invalid Http, Invalid URI, IP Filtering, Privacy File Filtering, Privacy Input Filtering, Request Header Filtering, Request Method Filtering, SQL Injection, Stealth Commanding, Unicode Directory traversal, URI Access Control, User Defined Pattern, Website Defacement |
| 상호 작용 | Cookie Poisoning, Parameter Tampering, Suspicious Access |
| 정보 감춤/변조 | Input Content Filtering, Privacy Output Filtering, Response Header Filtering, Cross Site Script |

공격자 의도에 따른 탐지를 분류

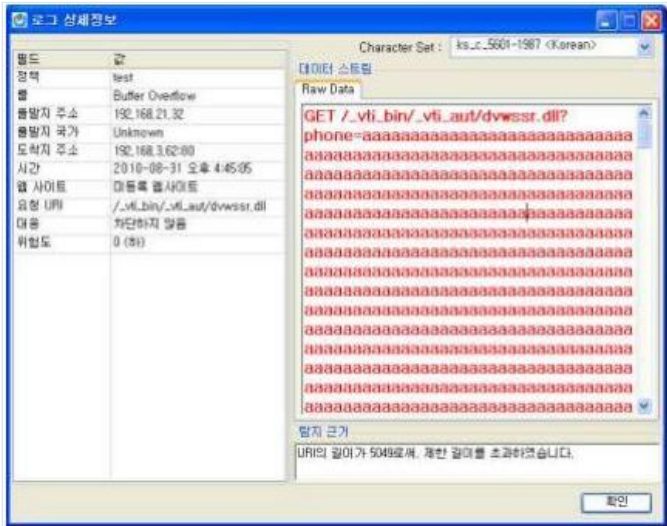
탐지률은 공격자의 의도에 따라 공격 방식을 분리해 볼 수 있습니다. 공격자가 직접 공격을 가해 올 수도 있고, 공격을 위한 준비작업이나, 정보 수집 작업을 할 수도 있습니다.

공격 방식에 따른 분류

| | |
|---------|--|
| 직접 공격 | Buffer Overflow, Extension Filtering, Include Injection, Invalid Http, Invalid URI, Parameter Tampering, Request Header Filtering, Request Method Filtering, SQL Injection, Stealth Commanding, Suspicious Access, Unicode Directory traversal, User Defined Pattern |
| 정보 수집작업 | Cookie Poisoning, Cross Site Script, Directory Listing, Error Handling, File Upload, IP Filtering, Response Header Filtering, URI Access Control |

WAF 룰의 상세

못한 결과를 유도하는 공격이며, 아무런 결과가 나타나지 않는다 하더라도 위의 공격 시 아무런 오류 상황이 나타나지 않았다면 공격자는 웹 서버가 Buffer Overflow에 노출 되어있다는 것을 예상할 수 있습니다.



대응 방안

웹 서버와 웹 애플리케이션에 대한 최신의 버그 리포트를 지속적으로 참고하여 최신 패치를 적용해야 합니다.

웹 애플리케이션 개발 시에는 Perl, Python, Java와 같이 자동화된 바운드 체크 기능을 제공하는 언어를 사용하도록 합니다. 표준 C 라이브러리의 경우 get(), strcpy(), strcmp() 함수 등과 인자에 대해 한계 체크를 수행하지 않는 취약점이 존재하는 라이브러리 함수의 사용을 자제합니다. 애플리케이션이 실행될 시스템에 무엇이 존재하고 누가 그것을 실행시킬 권한을 갖는지 파악해야 합니다. SUID가 root로 설정되었거나 root 소유의 world writable 파일들과 디렉터리들은 공격의 대상이 될 수 있으므로 변경하도록 합니다.

WAF에서는 위의 Buffer Overflow 공격에 대한 대응 방안으로 아래 표와 같이 3개의 탐지 모드를 제공합니다.

감사 수준별 감사 항목

| 모드 | 설명 |
|-----------|--|
| [일반 설정] | [키 길이] 64바이트, [URI 길이] 352바이트, [헤더길이] 512바이트를 초과하는 요청을 허용하지 않습니다. |
| [사용자 정의] | [URI 길이]는 요청되는 URI에 포함될 수 있는 최대 문자의 개수를 지정할 수 있으며 최대 값은 2047입니다. 기본 설정값은 352입니다.[키 길이]는 HTTP Request문 헤더의 키 길이에 포함될 수 있는 최대 문자의 개수를 지정할 수 있으며 최대 값은 128입니다. 기본 설정값은 64입니다. [헤더 길이]는 요청되는 HTTP의 헤더의 최대 길이를 지정할 수 있으며 최대 값은 4096 입니다.기본 설정값은 512입니다. |
| [탐지하지 않음] | 해당 룰을 탐지하지 않습니다. |

설정 마법사는 Buffer Overflow 탐지 모드를 [사용자 정의]로 설정 시 사용자 입력 값에 오류가 있을 경우 다음과 같은 오류 메시지를 출력합니다.

Buffer Overflow 사용자 정의 오류 메시지

| 오류 메시지 | 출력 원인 |
|-----------------|---------------------------------|
| 입력 값에 오류가 있습니다. | 입력 값이 URI 길이가 음수 혹은2048 이상일 경우 |
| | 입력 값이 키의 길이가 음수 혹은129 이상일 경우 |
| | 입력 값이 헤더의 길이가 음수 혹은 4097 이상일 경우 |
| 속성 값이 잘못되었습니다. | 입력 값이 숫자가 아닐 경우 |

위 탐지 모드에 의해 Buffer Overflow 공격의 탐지가 일어났을 때 아래 표의 4가지 대응 방법 중 하나를 선택하여 대응 할 수 있습니다.

대응 설정 항목

| 모드 | 설명 |
|--------------|--|
| 연결 끊기 | HTTP 연결을 강제 종료 합니다. |
| 에러 코드 보냄 | HTTP의 상태 코드를 응답합니다. 일반적으로 요구 메시지가 잘못된 형식으로 구성 되어 있거나 제대로 처리할수 없는 경우 등의 코드를 보냅니다. |
| 다른 웹 페이지로 이동 | 준비된 에러 처리 웹 페이지로 이동합니다. |
| 차단하지 않음 | 탐지로그에 기록은 남으나 웹 서버로 전달하는 것은 허용합니다. 차단을 원치 않는 경우에 사용합니다. |

대응 모드 중 [에러 코드 보냄]설정 시 선택 가능한 HTTP 상태 코드 및 의미는 [XI.4 에러처리 상태코드]의 [표 HTTP 상태코드와 의미] 와 같습니다.

예외 처리

운영자는 웹사이트의 환경에 따라 Buffer Overflow의 탐지가 해당 웹페이지에 적합하지 않다고 판단될 경우 해당 웹페이지에 대하여 BufferOverflow 탐지를 예외 처리 할 수 있습니다. 탐지 예외 설정 방법은 [VIII.7탐지 예외 설정 변경] 에서 볼 수 있습니다.

Cookie Poisoning

탐지률은 공격자의 의도에 따라 공격 방식을 분리해 볼 수 있습니다. 공격자가 직접 공격을 가해 올 수도 있고, 공격을 위한 준비작업이나, 정보 수집 작업을 할 수도 있습니다.

개요

쿠키(Cookies)란 서버와 통신하는데 필요한 지속적인 정보를 저장하는 곳을 지칭합니다. 쿠키는 웹 서버가 웹 브라우저에게 보내어 저장되었다가 서버의 부가적인 요청이 있을 때 다시 서버로 보내집니다.

예를 들어, 어떤 사용자가 특정 웹사이트에 접속한 후 그 사이트 내에서 어떤 정보를 보았는지 등에 관련된 기록을 남겨 놓았다가 다음에 접속하였을 때 그것을 인어 이전의 상태를 유지하면서 검색할 수 있게 구현하는데 활용됩니다.

많은 웹 애플리케이션은 중요 정보(사용자 ID, 타임스탬프 등)를 쿠키에 저장하여 사용합니다. 쿠키값은 HTTP 헤더의 일부분에 포함되어 전송됩니다. 쿠키는 항상 그 내용이 안전하지 않을 수 있기 때문에 공격자는 쿠키를 획득, 변조할 수 있고, 이를 통해 웹 애플리케이션을 속일수 있습니다. 쿠키를 변조함으로써 특정 계정에 대한 접근 권한을 얻거나, 또한 사용자의 쿠키를 훔쳐서 ID, 암호 없이 또는 어떤 인증도 없이 사용자 계정을 얻을 수 있습니다.

요즘은 중요한 정보를 Cookie를 통해 제공하는 일이 드물어 그다지 많이 사용되는 공격 기법은 아니지만, 사용자 정보를 유지할 수 없는 HTTP의 한계를 극복할 수 있다는 장점 때문에 아직도 많은 곳에서 쿠키를 사용하고 있으며 이를 이용한 악의적인 공격이 이루어지고 있습니다.

공격 예

웹사이트 접속 후 공격자 콘솔에 저장된 쿠키를 간단한 텍스트도구를 이용하여 변경 후 재접속합니다. 재접속시 기존에 서버에서 전송한 쿠키값에 대한 검증절차가 없다면 변경된 쿠키가 그대로 적용될 수 있습니다. 아래의 그림은 쿠키값 중 "ud2"라는 쿠키값이 변조되었음을 나타내고 있습니다.

다음 모드 중 [에러 코드 보냄] 설정 시 선택 가능한 HTTP 상태 코드 및 의미는 [XI.4 에러처리 상태코드]의 [표 HTTP 상태코드와 의미]와 같습니다.

예외 처리

운영자는 웹사이트의 환경에 따라 Cookie Poisoning의 탐지가 해당 웹 페이지에 적합하지 않다고 판단될 경우 해당 웹페이지에 대하여 Cookie Poisoning 탐지를 예외 처리 할 수 있습니다. 탐지 예외 설정 방법은 [VIII.7탐지 예외 설정 변경]에서 볼 수 있습니다.

Cross Site Scripting

개요

JavaScript, VBScript, Flash, ActiveX, XML/XSL, DHTML 등과 같이 클라이언트 측에서 실행되는 언어로 작성된 코드를 사용자 입력으로 주게되면 이 코드가 그대로 클라이언트 측 브라우저에서 수행됩니다. 이러한 특성을 이용하여 악성 스크립트 코드를 웹 페이지, 웹 게시판 또는 이메일에 포함시켜 사용자에게 전송하는 것이 Cross Site Scripting(XSS) 공격 기법입니다.

웹 사용자가 취약한 웹 서버에 접속 중일 때 공격자는 악성 스크립트를 업로드 한 후 웹 사용자에게 이메일이나 웹 페이지를 전송하여 악성스크립트가 있는 링크를 클릭하도록 유도합니다. 웹 사용자가 해당링크를 클릭하게 되면 자신의 쿠키 등의 정보가 공격자에게 전송되고, 공격자는 수집된 정보를 이용하여 피해자의 권한으로 웹 서버에 접속할 수 있습니다.

또한 다른 방법으로는, 악의적인 사용자가 만든, 동적으로 생성되는 웹 페이지에서 악의적인 HTML 태그나 스크립트를 포함시키는 방법이 있습니다. 이렇게 받아들여진 데이터는 다른 클라이언트가 그 페이지에 접근할 경우에 전달 되게 되고, 이 클라이언트는 정상적인 데이터로 인식하고 그 내용을 인터프리트 (interpret)하게 됩니다. 즉, 웹 애플리케이션을 매개로 하여 다른 사용자의 브라우저에서 스크립트 실행이 가능해지는 것입니다. 결과적으로 DOM (Document Object Model) security restrictions을 건너뛰어 명령 실행이 가능해집니다. 이러한 태그나 스크립트는 웹 서버가 입력이나 출력을 제대로 필터링하지 못할 경우에 의도하지 않은 스크립트를 실행하도록 할 수 있습니다. 대부분의 웹브라우저들은 웹 페이지에 삽입된 스크립트를 해석하고 실행할 수 있습니다. 이러한 스크립트는 자바스크립트나 VB스크립트로 만들어진 경우가 대부분 입니다.

예상되는 피해는 다른 사용자의 정보 취득 및 이를 통한 계정 도용과 트로이 목마 같은 프로그램 실행 등 이 있습니다. 이는 위에서도 언급했듯이 대부분의 경우 사용자가 웹 서버에 데이터를 입력할 수 있는 수단이 있는 곳에 주로 이용되고 있습니다

기본적으로 XSS는 다음과 같은 공격들이 가능합니다.

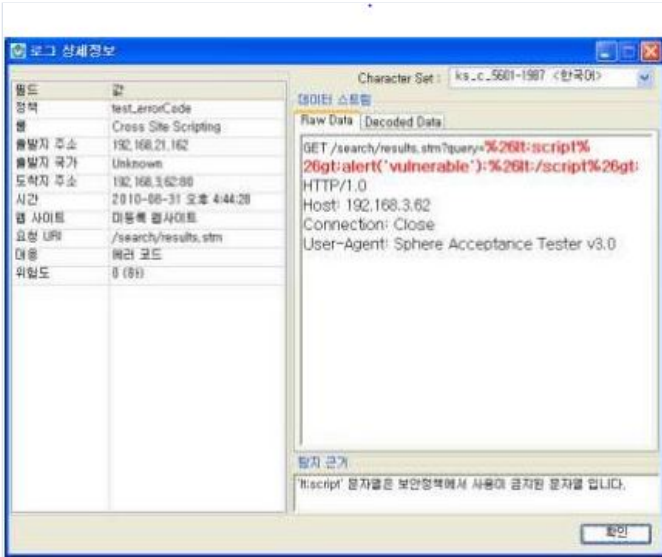
- 페이지의 모양 바꾸기
- SSL 암호화 커넥션 노출
- 쿠키 변형시키기를 통한 지속적인 공격
- 제한된 웹 사이트 접근
- DOM 기반 보안 정책 위반
- 잘 사용하지 않는 문자 셋을 사용하면 문제 확대
- 폼의 행동 방식을 변경
- 쿠키 훔치기

공격 예

WAF에 미리 설정된 태그나 스크립트 명령에 의해 탐지된 예입니다. 사용자가 웹 서버에 데이터를 입력할 수 있는 게시판 등의 공간에서 아래와 같이 금지된 (script) 사용하여 게시판 내용을 등록합니다.

The screenshot shows a web form titled "사내게시판" (Intranet Bulletin Board). The form has fields for "작성자" (Author), "Email", "제목" (Subject), and "내용" (Content). The "Email" field contains "cracklen@ncc.com". The "제목" field contains "XSS test". The "내용" field contains the JavaScript payload: `<script> alert(document.cookie) </script>`. This payload is highlighted with a red box. At the bottom of the form, there are buttons for "등록" (Register) and "취소" (Cancel).

WAF은 HTTP Request문에서 금지 스크립트 문을 발견하고 탐지한 예입니다.



대응 방안

웹페이지에서 사용하는 사용자 ID, 암호, 검색어 등 모든 입력부분을 필터링 하도록 해야 합니다. 클라이언트가 입력한 데이터에서 특수문자를 표준적인 HTML 표현 문자로 변경하는 것도 유용한 방법입니다.

WAF에서는 위의 Cross Site Scripting 공격에 대한 대응 방안으로 아래 표와 같이 3개의 탐지 모드를 제공합니다.

Cross Site Scripting 탐지 모드

| 모드 | 설명 |
|---------------|---|
| [스크립트 허용 안 함] | Cross Site Scripting 공격을 야기할 수 있는 모든 스크립트의 입력을 허용하지 않습니다. |
| [사용자 정의] | 허용하지 않을 HTML의 태그, 허용하지 않을 스크립트 패턴, 태그 자동 변환 여부, 이미지 태그 탐지 여부를 사용자 정의 합니다. |
| [탐지하지 않음] | 해당 룰을 탐지하지 않습니다. |

위 탐지 모드에 의해 Cross Site Scripting 공격의 탐지가 일어났을 때 아래 표의 4가지 대응방법 중 하나를 선택 하여 대응 할 수 있습니다.

대응 설정 항목

| 모드 | 설명 |
|--------------|---|
| 연결 끊기 | HTTP 연결을 강제 종료 합니다. |
| 에러 코드 보냄 | HTTP의 상태 코드를 응답합니다. 일반적으로 요구 메시지가 잘못된 형식으로 구성 되어 있거나 제대로 처리할 수 없는 경우 등의 코드를 보냅니다. |
| 다른 웹 페이지로 이동 | 준비된 에러처리 웹 페이지로 이동합니다. |
| 차단하지 않음 | 탐지로그에 기록은 남으나 웹 서버로 전달하는 것은 허용합니다. 차단을 원치 않는 경우에 사용합니다. |

대응 모드 중 [에러 코드 보냄]설정 시 선택 가능한 HTTP 상태 코드 및 의미는 [XI.4 에러처리 상태코드]의 [표 HTTP 상태코드와 의미]와 같습니다.

사용자 정의의 태그 자동 변환 기능은 허용하지 않을 HTML 태그 및 허용하지 않을 스크립트 패턴을 스크립트가 동작하지 않도록 변조하며 이와 같은 변조 기능을 이용하려면 대응 설정이 [차단하지 않음]으로 설정되어야 함

웹 서버의 설정에서 웹 서버의 DirectoryIndex에 대한 표기를 하지 못하도록 모든 디렉토리 리스팅 방지에 대한 설정을 변경해야 합니다

WAF에서는 위의 Directory Listing 공격에 대한 대응 방안으로 아래 표와 같이 2개의 탐지 모드를 제공합니다.

Directory Listing 탐지 모드

| 모드 | 설명 |
|--------------|------------------------------------|
| [디렉터리 유출 방지] | 웹 사이트의 디렉터리 내용이 그대로 보여지는 것을 탐지합니다. |
| [탐지하지 않음] | 해당 룰을 탐지하지 않습니다. |

위 탐지 모드에 의해 Directory Listing 공격의 탐지가 일어났을 때 아래 표의 4가지 대응방법 중 하나를 선택하여 대응 할 수 있습니다.

대응 설정 항목

| 모드 | 설명 |
|--------------|---|
| 연결 끊기 | HTTP 연결을 강제 종료 합니다. |
| 에러 코드 보냄 | HTTP의 상태 코드를 응답합니다. 일반적으로 요구 메시지가 잘못된 형식으로 구성 되어 있거나 제대로 처리할 수 없는 경우 등의 코드를 보냅니다. |
| 다른 웹 페이지로 이동 | 준비된 에러처리 웹 페이지로 이동합니다. |
| 차단하지 않음 | 탐지로그에 기록은 남으나 웹 서버로 전달하는 것은 허용합니다. 차단을 원치 않는 경우에 사용합니다. |

대응 모드 중 [에러 코드 보냄]설정 시 선택 가능한 HTTP 상태 코드 및 의미는 [XI.4 에러처리 상태코드]의 [표 HTTP 상태코드와 의미]와 같습니다.

예외 처리

운영자는 웹사이트의 환경에 따라 Directory Listing의 탐지가 해당 웹페이지에 적합하지 않다고 판단될 경우 해당 웹페이지에 대하여 Directory Listing 탐지를 예외 처리 할 수 있습니다. 탐지 예외 설정 방법은[VIII.7탐지 예외 설정 변경]에서 볼 수 있습니다.

Error Handling

개요

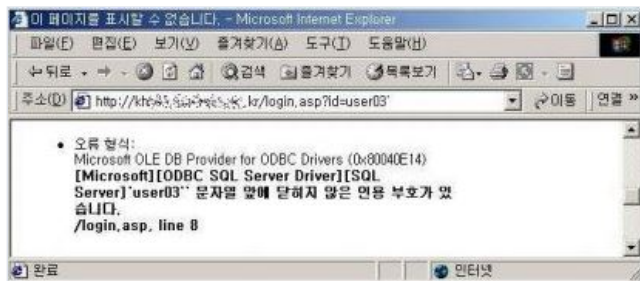
웹 애플리케이션 사용 시 메모리 부족, Null Pointer Exception, 시스템 콜 실패, 데이터베이스 접속 에러, 네트워크 타임 아웃 등 다양한 에러가 발생하는데, 이러한 에러의 부적절한 처리는 악의적인 사용자들에게 해당 사이트가 가진 잠재적 취약점에 대한 힌트를 제공하는 등 다양한 보안 문제를 야기할 수 있습니다.

예상되는 피해는 웹 서버, 웹 애플리케이션의 DB 관련 정보 유출 및 웹 서버의 오류 문구나 DB의 오류 문구 등을 통해 연동된 웹 서버 및 애플리케이션의 버전, 종류 등의 정보 노출입니다.

공격 예

의도적으로 잘못된 요청을 전송하여 웹 서버나 웹 애플리케이션의 오류 발생을 유도하는 공격 방법입니다. 중복된 문자열, 주석, 다른 ID 삽입 등을 통해 오류 발생을 유도하며 다음과 같은 에러 화면을 발생시킵니다.

위와 같은 오류 메시지를 통해 위의 웹 서버가 현재 연동하고 있는 웹 서버의 종류를 알 수 있으며 후속 공격으로 이러한 정보를 바탕으로 SQL Injection등의 공격이 일어날 수 있습니다.



WAF은 위와 같은 오류 메시지를 사전에 탐지합니다.



대응 방안

웹 애플리케이션 개발자는 발생할 수 있는 모든 경우의 에러에 대해 대응할 수 있도록 설계해야 하고, 모든 상황에 대해 발생 가능한 에러를 검토하여 그에 대한 조치를 문서화해야 합니다.

실제로 에러가 발생할 경우에는 필요한 경우 시스템에 대한 최소한의 정보만을 표시하도록 하고 발생한 에러의 정도나 횟수에 따라 악의적인 공격을 탐지할 수 있도록 설계합니다.

애플리케이션이 오류로 인해 제 기능을 다하지 못할 경우에는 서비스 거부 상태가 되도록 설계합니다.

WAF에서는 위의 Error Handling 공격에 대한 대응 방안으로 아래 표와 같이 4개의 탐지 모드를 제공합니다

Error Handling 탐지 모드

| 모드 | 설명 |
|------------|--|
| [2차 수준 차단] | 웹 서버나 웹 애플리케이션의 오류발생으로 인한 중요한 정보의 유출을 탐지합니다. |
| [1차 수준 차단] | 500 Internal Server Error를 제외한 웹 서버나 웹 애플리케이션의 오류발생으로 인한 중요한 정보의 유출을 탐지합니다. |
| [사용자 정의] | [status code] 항목에 [HTTP 상태코드]를 입력 합니다 입력 가능한 [status code]는 [표 HTTP 상태코드와 의미]를 참고합니다 |
| [탐지하지 않음] | 해당 룰을 탐지하지 않습니다. |

설정 마법사는 Error Handling 탐지 모드를 [사용자 정의]로 설정할 시 사용자 입력 값에 대하여 오류가 있을 경우 다음과 같이 오류 메시지를 출력합니다.

Error Handling 사용자 정의 오류 메시지

| 오류 메시지 | 출력 원인 |
|------------------------------------|---|
| {해당 status code}은 상태코드 범위를 벗어났습니다. | 입력된 status code의 범위가 100 ~ 101, 200 ~ 206, 300 ~ 307, 400 ~ 417, 500 ~ 505의 범위에 속하지 않을 경우 |

위 탐지 모드에 의해 Error Handling 공격의 탐지가 일어났을 때 아래 표의 4가지 대응방법 중 하나를 선택하여 대응 할 수 있습니다.

대응 설정 항목

| 모드 | 설명 |
|--------------|---|
| 연결 끊기 | HTTP 연결을 강제 종료 합니다. |
| 에러 코드 보냄 | HTTP의 상태 코드를 응답합니다. 일반적으로 요구 메시지가 잘못된 형식으로 구성 되어 있거나 제대로 처리할 수 없는 경우 등의 코드를 보냅니다. |
| 다른 웹 페이지로 이동 | 준비된 에러처리 웹 페이지로 이동합니다. |
| 차단하지 않음 | 탐지로그에 기록은 남으나 웹 서버로 전달하는 것은 허용합니다. 차단을 원치 않는 경우에 사용합니다. |

대응 모드 중 [에러 코드 보냄]설정 시 선택 가능한 HTTP 상태 코드 및 의미는 [XI.4 에러처리 상태코드]의 [표 HTTP 상태코드와 의미]와 같습니다.

예외 처리

운영자는 웹사이트의 환경에 따라 Error Handling의 탐지가 해당 웹페이지에 적합하지 않다고 판단될 경우 해당 웹페이지에 대하여 Error Handling 탐지를 예외 처리 할 수 있습니다. 탐지 예외 설정 방법은 [VIII.7탐지 예외 설정 변경]에서 볼 수 있습니다.

Extension Filtering

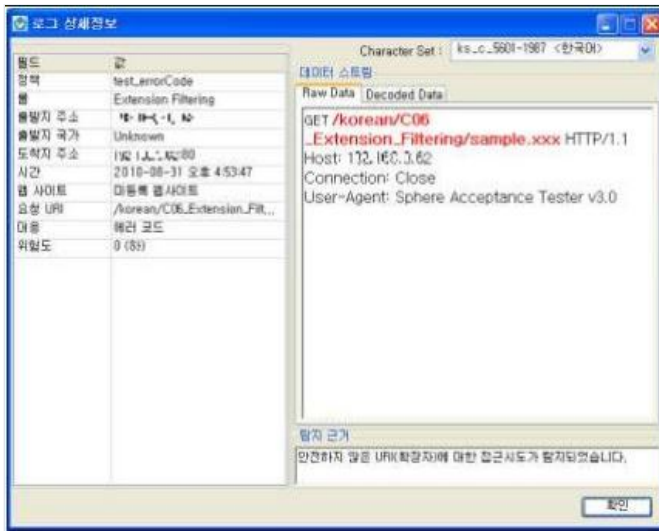
개요

웹 서버의 내부 파일에 대해 접근 권한이 허술하게 설정되어 있을 경우 악의적인 사용자의 공격 대상이 될 수 있습니다. 이를 막기 위해서는 사전에 웹 브라우저를 통해 사용자가 입력한 URL의 확장자를 검사하여 접근 가능하도록 설정된 확장자 이외의 접근은 차단해야 합니다.

대부분의 접근 가능한 웹 서버에서 외부공개를 위한 파일 및 디렉토리에 대한 접근 권한이 익명의 사용자에게도 허용되어 있다면 시스템에 중요한 파일들(시스템 파일, 라이브러리, 패스워드 파일 등)의 접근 가능은 악의적인 공격의 대상이 될 수 있습니다.

공격 예

아래 탐지로그는 /_vti_bin/owssvr.dll에 대한 접근이 탐지된 예입니다. 이는 과거 Nimda와 같은 웜이나 트로이 목마 프로그램에서 스캐닝 용도로 사용되었습니다. 현재 대부분 IE 브라우저의 툴 바에서 [토론]을 선택했을 경우 생성되는 요청으로 피해를 끼치지 않습니다.



대응 방안

외부 공개를 위한 파일 및 디렉터리를 제외한 모든 파일 및 디렉터리에 대한 접근 권한을 변경하여 허가 받지 않은 사용자로부터의 접근을 차단하여야 합니다.

웹 브라우저를 통해 사용자가 입력한 URL의 웹 콘텐츠 확장자를 파싱하여 접근 가능하도록 설정된 확장자 이외의 접근은 차단하도록 합니다.

WAF에서는 위의 Extension Filtering 공격에 대한 대응 방안으로 아래표와 같이 3개의 탐지 모드를 제공합니다.

Extension Filtering 탐지 모드

| 모드 | 설명 |
|-----------------|---|
| [안전한 형식만 접근 가능] | 다음과 같은 확장자의 접근을 허용합니다.(html, htm, shtml, cgi, pl, py, php, php4, php3, phtml, asp, aspx, jsp, css, inc, js, txt, jar, java, class, cab, vcs, vbs, exe, xml, xpi, xhtml, xss, rdf, bmp, gif, jpg, jpeg, png, swf, ico, avi, mov, asf, wmv, wma, mp3, mp2, wav, gz, tar, tgz, bz2, zip, arc, ace, arj, lzh, alz, rar, doc, ppt, rtf, xls, hwp, ps, pdf) |
| [사용자 정의] | 사용자가 임의의 확장자를 정의합니다. |
| [탐지하지 않음] | 해당 룰을 탐지하지 않습니다. |

Extension Filtering 탐지 룰 설정 시 주의 할 점은 먼저 웹 서버마다 사용되는 파일 형식이 달라지므로 상황에 맞게 설정 하여야 합니다. 따라서 웹 서버의 OS 종류(Windows, Linux, Unix), HTTP 서버 종류(Apache, IIS), Active Page 언어(PHP, Perl, ASP, JSP)등에 따라 적절하게 설정을 하여야 합니다.

위 탐지 모드에 의해 Extension Filtering 공격의 탐지가 일어났을 때 아래 표의 4가지 대응방법 중 하나를 선택 하여 대응 할 수 있습니다.

대응 설정 항목

| 모드 | 설명 |
|--------------|---|
| 연결 끊기 | HTTP 연결을 강제 종료 합니다. |
| 에러 코드 보냄 | HTTP의 상태 코드를 응답합니다. 일반적으로 요구 메시지가 잘못된 형식으로 구성 되어 있거나 제대로 처리할 수 없는 경우 등의 코드를 보냅니다. |
| 다른 웹 페이지로 이동 | 준비된 에러처리 웹 페이지로 이동합니다. |
| 차단하지 않음 | 탐지로그에 기록은 남으나 웹 서버로 전달하는 것은 허용합니다. 차단을 원치 않는 |

대응 모드 중 [에러 코드 보냄] 설정 시 선택 가능한 HTTP 상태 코드 및 의미는 [XI.4 에러처리 상태코드]의 [표 HTTP 상태코드와 의미]와 같습니다.

예외 처리

운영자는 웹사이트의 환경에 따라 Extension Filtering의 탐지가 해당 웹페이지에 적합하지 않다고 판단될 경우 해당 웹 페이지에 대하여 Extension Filtering 탐지를 예외 처리 할 수 있습니다. 탐지 예외 설정 방법은 [VIII.7 탐지 예외 설정 변경]에서 볼 수 있습니다.

File Upload

개요

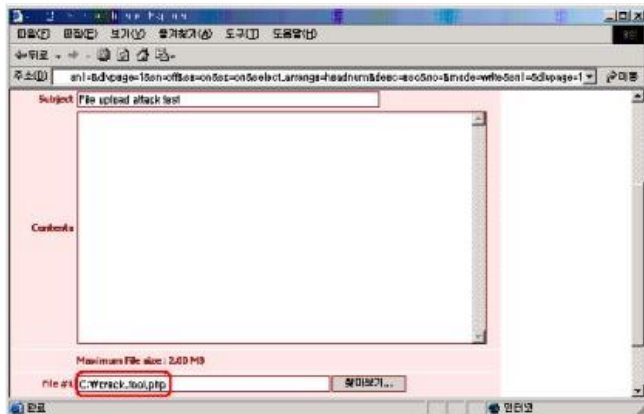
공격자가 공격에 사용되는 도구를 웹 서버에 업로드 하는 것을 적절히 막지 못하는 문제점이 있는 경우 공격자는 PHP나 ASP, JSP 등으로 작성된 공격 도구를 서버에 업로드 하여, 웹 서버를 장악할 수 있습니다.

홈페이지 게시판 등에 php, asp, css 등의 확장자를 가진 파일을 업로드한 후 업로드 된 위치를 알아내어 해당 파일을 실행시켜 공격이 가능합니다. 이는 웹 서버가 파일 업로드 시 필터링을 하지 않거나, 웹 서버의 권한이 root(Admin)의 계정으로 동작할 경우 이러한 공격을 받을 수 있습니다. 이 공격은 성공하였을 시 가장 위험한 공격이 될 수 있습니다. 웹 서버의 모든 제어 권한 탈취가 가능합니다. 또한 공격을 위해 필요한 기술적 난이도가 매우 낮기 때문에 쉽게 공격이 가능합니다.

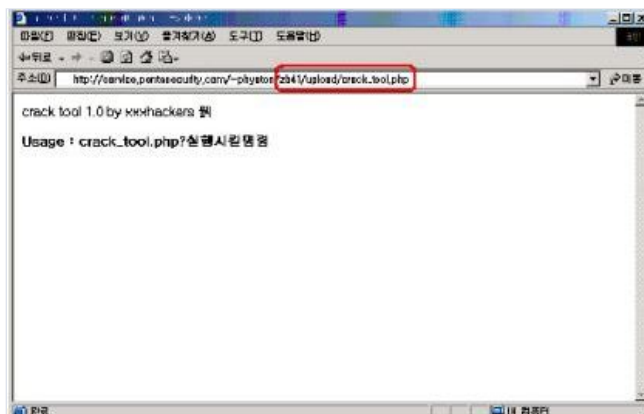
가장 흔히 시도되는 공격은 미리 작성된 백도어 파일을 웹 서버에 업로드 하는 것입니다. 이러한 공격은 공개 게시판의 파일 업로드가 가능한 곳이면 어디든 공격 대상이 되고 있습니다. 이 공격을 당한 웹 서버는 다른 곳을 공격하기 위한 경우지로 사용되는 경향이 있습니다. 대부분 업로드 된 백도어 파일을 다른 이름으로 숨겨두기 때문에 상당 기간 동안 침탈 사실을 관리자가 인지하지 못할 수 있습니다. (알려진 이름을 가진 프로세스 형태의 백도어 프로그램을 하나 더 숨겨두기도 합니다.

공격 예

웹페이지 게시판에서 "crack_tool.php"를 업로드 합니다.



파일이 업로드된 위치를 알아내어 이를 아래와 같이 실행하면 공격자가 원하는 공격이 가능하게 됩니다.



대응 방안

웹 서버나 웹 애플리케이션에서 업로드 되는 파일에 대한 필터링을 수행하도록 합니다. 특히 실행 가능한 확장자를 가진 파일에 대한 업로드를 금지합니다. 만약 UNIX시스템의 웹 서버가 root 권한으로 실행된다면 반드시 이를 변경하도록 합니다.

WAF에서는 위의 File Upload공격에 대한 대응 방안으로 아래 표와 같이 4개의 탐지 모드를 제공합니다.

File Upload 탐지 모드

| 모드 | 설명 |
|---------------|---|
| [안전한 파일만 허용] | 일반적으로 안전하다고 알려진 그림 파일(jpg, bmp, gif, png, jpeg), 압축 파일(zip, tar, gz, bz2, rar, alz, ace)과 텍스트 파일(txt)의 업로드만을 허용합니다. |
| [실행파일 업로드 금지] | 실행 가능한 파일(cgi, php, exe, asp, jsp, dll, pl)을 제외한 다른 파일의 업로드만을 허용합니다. |
| [사용자 정의] | 사용자의 임의로 확장자를 정의합니다. 기본 설정은 안전한 파일(jpg, bmp, gif, png, jpeg, zip, tar, gz, bz2, rar, alz, ace, txt)만 허용하도록 되어 있습니다. |
| [탐지하지 않음] | 해당 룰을 탐지하지 않습니다. |

File Upload 룰은 일반 보안도의 "실행파일 업로드 금지" 설정으로 위험한 파일을 업로드하는 것을 항상 탐지하는 것이 좋습니다. 또한 게시판 성격에 따라 높은 보안도의 "안전한 파일만 허용" 설정으로 업로드 가능 파일 종류를 소수로 제한하는 것이 안전합니다. 또한 URI Access Control 룰과 함께 사용하여 WAF 설치 이전에 미리 숨겨진 백도어 파일 접근을 차단하도록 합니다.

설정 마법사는 File Upload 탐지 모드를 [사용자 정의]로 지정 시 사용자 입력 값에 대하여 오류가 있을 경우 다음과 같은 오류 메시지를 출력합니다.

File Upload 사용자 정의 오류 메시지

| 오류 메시지 | 출력 원인 |
|-----------------------------|-----------------------------|
| 파일의 크기는 음수일 수 없습니다 | 입력된 파일 확장자 크기가 음수 일 경우 |
| 파일의 최대 크기는 100M를 넘을 수 없습니다. | 파일 확장자 크기가 100 MB 를 초과 할 경우 |
| 속성 값이 잘못되었습니다. | 파일 확장자 크기의 형식이 숫자가 아닐 경우 |

위 탐지 모드에 의해 File Upload 공격의 탐지가 일어났을 때 아래 표의 4가지 대응방법 중 하나를 선택하여 대응 할 수 있습니다.

대응 설정 항목

| 모드 | 설명 |
|--------------|--|
| 연결 끊기 | HTTP 연결을 강제 종료 합니다. |
| 에러 코드 보냄 | HTTP의 상태 코드를 응답합니다. 일반적으로 요구 메시지가 잘못된 형식으로 구성되어 있거나 제대로 처리할 수 없는 경우 등의 코드를 보냅니다. |
| 다른 웹 페이지로 이동 | 준비된 에러처리 웹 페이지로 이동합니다. |
| 차단하지 않음 | 탐지로그에 기록은 남으나 웹 서버로 전달하는 것은 허용합니다. 차단을 원치 않는 경우에 사용합니다. |

대응 모드 중 [에러 코드 보냄]설정 시 선택 가능한 HTTP 상태 코드 및 의미는 [XI.4 에러처리 상태코드]의 [표 HTTP 상태코드와 의미]와 같습니다.

예외 처리

운영자는 웹사이트의 환경에 따라 File Upload의 탐지가 해당 웹페이지에 적합하지 않다고 판단될 경우 해당 웹 페이지에 대하여 File Upload 탐지를 예외 처리 할 수 있습니다. 탐지 예외 설정 방법은 [VIII.7탐지 예외 설정 변경] 에서 볼 수 있습니다.

Include Injection

개요

파일명을 변수로 사용하여 include 하는 취약성을 가진 웹페이지를 대상으로 변수를 조작하여 악의적인 파일을 include 하도록 유도합니다.

공격 예

악의적인 목적을 가진 사용자가 자신의 서버의 웹 디렉토리에 악의적인 파일을 만들고 Include Injection에 취약한 웹페이지의 파일명 변수를 조작하여 악의적인 파일을 include 하도록 합니다.

대응 방안

웹 애플리케이션에서 include 될 소지가 있는 파일명 변수에 "http", "ftp" 와 파일의 경로를 표시해주는 "..", "/" 와 같은 문자열을 쓰지 못하도록 해야 하고 또한 파일의 확장자를 나타내는 문자열을 함께 사용하지 못하도록 웹 애플리케이션을 수정하여야 합니다.

WAF에서는 위의 Include Injection공격에 대한 대응 방안으로 아래 표와 같이 2개의 탐지 모드를 제공합니다.

Include Injection 탐지 모드

| 모드 | 설명 |
|-----------|--|
| [일반 설정] | 악의적인 파일의 Include 를 탐지합니다. |
| [사용자 정의] | 입력한 호스트 목록의 include를 허용할지 거부할지를 설정할수 있습니다. |
| [탐지하지 않음] | 해당 룰을 탐지하지 않습니다. |

위 탐지 모드에 의해 Include Injection 공격의 탐지가 일어났을 때 아래 표의 4가지 대응방법 중 하나를 선택하여 대응 할 수 있습니다.

대응 설정 항목

| 모드 | 설명 |
|--------------|---|
| 연결 끊기 | HTTP 연결을 강제 종료 합니다. |
| 에러 코드 보냄 | HTTP의 상태 코드를 응답합니다. 일반적으로 요구 메시지가 잘못된 형식으로 구성 되어 있거나 제대로 처리할 수 없는 경우 등의 코드를 보냅니다. |
| 다른 웹 페이지로 이동 | 준비된 에러처리 웹 페이지로 이동합니다. |
| 차단하지 않음 | 탐지로그에 기록은 남으나 웹 서버로 전달하는 것은 허용합니다. 차단을 원치 않는 경우에 사용합니다. |

대응 모드 중 [에러 코드 보냄]설정 시 선택 가능한 HTTP 상태 코드 및 의미는 [XI.4 에러처리 상태코드]의 [표 HTTP 상태코드와 의미] 와 같습니다

예외 처리

운영자는 웹사이트의 환경에 따라 Include Injection의 탐지가 해당 웹 페이지에 적합하지 않다고 판단될 경우 해당 웹페이지에 대하여 Include Injection 탐지를 예외 처리 할 수 있습니다. 탐지 예외 설정 방법은[VIII.7탐지 예외 설정 변경]에서 볼 수 있습니다.

Input Content Filtering

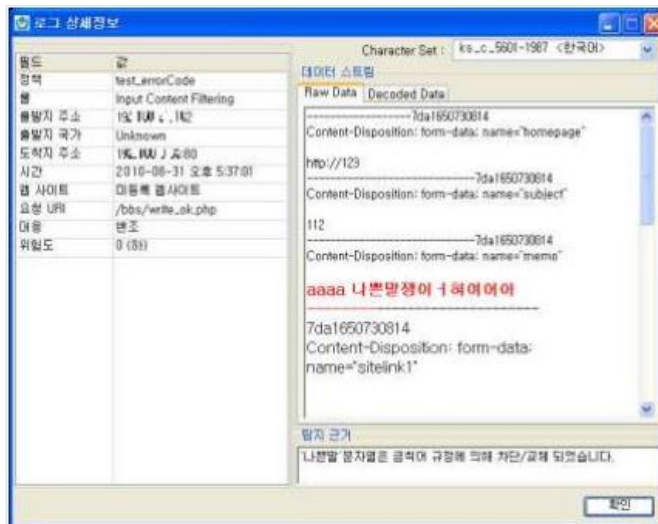
개요

사용자가 입력하는 문자열 가운데 다른 사람에게 불쾌감을 줄 수 있는 내용이 있을 수 있습니다. 이러한 경우 이러한 문자열을 등록하여 웹 사이트를 사용자에게 불쾌감을 주는 공격입니다.

모든 웹 서버와 웹 애플리케이션 서버, 웹 애플리케이션 환경에 InputContent Filtering을 적용할 수 있습니다. 특히 게시판 운영을 하는 사이트에 유용합니다.

공격 예

아래 그림은 웹 애플리케이션에서 사용자 입력 값 중 운영자가 탐지하고자 하는 문자열 "나쁜말" 이 포함되어 WAF이 탐지한 예입니다.



대응 방안

웹 서버나 웹 애플리케이션에서 사용자 입력 내용에 대해 필터링을 수행할 수 있습니다.

웹 서버 혹은 웹 서버와 연동된 웹 애플리케이션에 피해를 주는 행동은 아니지만 웹 서버가 운영하는 웹사이트를 이용하는 다수의 고객들에게 불쾌감을 주거나 문제의 소지가 될 수 있는 부분을 사전 탐지/차단하도록 합니다.

WAF에서는 위의 Input Content Filtering공격에 대한 대응 방안으로 아래 표와 같이 2개의 탐지 모드를 제공합니다.

Input Content Filtering 탐지 모드

| 모드 | 설명 |
|-----------|-----------------------------|
| [사용자 정의] | 탐지하고자 하는 문자열과 변경문자열을 정의합니다. |
| [탐지하지 않음] | 해당 룰을 탐지하지 않습니다 |

설정 마법사는 Input Content Filtering 탐지 모드를 [사용자 정의]로 설정 시 사용자 입력 값에 대하여 오류가 있을 경우 다음과 같은 오류메시지를 출력합니다.

Input Content Filtering 사용자 정의 오류 메시지

| | |
|--|--|
| | |
|--|--|

| 오류 메시지 | 출력 원인 |
|-----------------------|--|
| 변경 문자열이 없는 항목은 삭제합니다. | 입력된 변경 전 문자열이 빈칸일 경우 |
| 20개 이상 설정할 수 없습니다. | 입력된 변경 전 문자열과 변경 후 문자열의 쌍으로 이루어진 항목이 20개를 초과할 경우 |
| 문자열 선택 메시지를 출력 | 입력된 변경 전 문자열 다른 문자열 쌍에 중복되어 있을 경우 |

위 탐지 모드에 의해 관리자가 설정한 문자열 탐지가 일어났을 때 아래 표의 4가지 대응방법 중 하나를 선택하여 대응 할 수 있습니다.

대응 설정 항목

| 오류 메시지 | 출력 원인 |
|--------------|--|
| 연결 끊기 | HTTP 연결을 강제 종료 합니다. |
| 에러 코드 보냄 | HTTP의 상태 코드를 응답합니다. 일반적으로 요구 메시지가 잘못된 형식으로 구성 되어 있거나 제대로 처리할 수 없는 경우 등의 코드를 보냅니다. |
| 다른 웹 페이지로 이동 | 준비된 에러처리 웹 페이지로 이동합니다. |
| 차단하지 않음 | 탐지로그에 기록은 남으나 웹 서버로 전달하는 것은 허용합니다. 차단을 원치 않는 경우에 사용합니다. Input Content Filtering 룰의 경우에는 사용자 정의에서 설정한 항목별 출력 방식에 따라 탐지 항목이 출력됩니다.예) Pattern : 나쁜말 Replace Value : 좋은말 실제 입력: "나쁜말은 못된행동" 실제 출력: "좋은말은 못된행동" |

대응 모드 중 [에러 코드 보냄]설정 시 선택 가능한 HTTP 상태 코드 및 의미는 [XI.4 에러처리 상태코드]의 [표 HTTP 상태코드와 의미] 와 같습니다.

Input Content Filtering 은 탐지하고자 하는 문자열을 변경문자열로 정의하고자 할 경우 대응방법을 [차단하지 않음]으로 설정하여야 합니다. 입력된 변경 전 문자열과 변경 후 문자열이 같을 경우 실제 메시지는 변경되지 않습니다.

예외 처리

운영자는 웹사이트의 환경에 따라 Input Content Filtering의 탐지가 해당 웹페이지에 적합하지 않다고 판단될 경우 해당 웹페이지에 대하여 Input Content Filtering 탐지를 예외 처리 할 수 있습니다. 탐지 예외 설정 방법은 [VIII.7탐지 예외 설정 변경]에서 볼 수 있습니다.

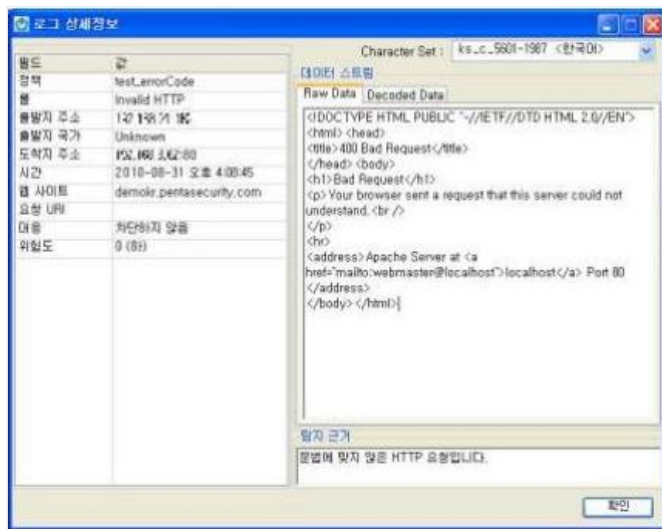
Invalid HTTP

개요

HTTP의 규격에서 벗어난 요청이나 응답, 존재하지 않는 웹사이트에 대한 요청은 비정상적인 트래픽으로, 일반적으로 웜을 비롯한 각종 공격 도구들로부터 생성됩니다. 이러한 트래픽은 정상적인 웹 브라우저에서는 생성되지 않는 것이므로 이상징후로 간주할 수 있습니다.

공격 예

HTTP규격에서 요구하는 헤더 정보가 충분하지 않아 Invalid HTTP공격으로 탐지된 로그입니다.



대응 방안

해당 트래픽을 발생시킨 프로그램이 무엇인지 확인하여 대응할 수 있습니다. 원을 비롯한 공격 도구가 의심될 경우 웹 서버나 웹 애플리케이션에서 필터링을 수행할 수 있습니다. WAF에서는 HTTP의 규격에서 벗어난 요청이나 응답, 존재하지 않는 웹사이트에 대한 요청은 비정상적인 트래픽으로 간주합니다.

WAF에서는 HTTP규격에 벗어난 트래픽에 대한 대응 방안으로 아래 표와 같이 2개의 탐지 모드를 제공합니다.

Invalid URI 탐지 모드

| 모드 | 설명 |
|--------------|--|
| [위험한 HTTP차단] | HTTP 규격을 지키지만 위험한 요청은 탐지합니다. |
| [탐지하지 않음] | HTTP 규격에 벗어난 트래픽에 대해 탐지 하지않습니다. |
| 사용자 정의 | Request Header에 Host필드가 없는 경우 , 보호 웹 서버를 Forward Proxy로 사용하려는 시도에 대해 사용자 설정으로 탐지 유무를 결정할 수 있습니다. |

위 탐지 모드에 의해 Invalid URI 공격의 탐지가 일어났을 때 아래 표의 4가지 대응방법 중 하나를 선택하여 대응 할 수 있습니다.

대응 설정 항목

| 모드 | 설명 |
|--------------|---|
| 연결 끊기 | HTTP 연결을 강제 종료 합니다. |
| 에러 코드 보냄 | HTTP의 상태 코드를 응답합니다. 일반적으로 요구 메시지가 잘못된 형식으로 구성 되어 있거나 제대로 처리할 수 없는 경우 등의 코드를 보냅니다. |
| 다른 웹 페이지로 이동 | 준비된 에러처리 웹 페이지로 이동합니다. |
| 차단하지 않음 | 탐지로그에 기록은 남으나 웹 서버로 전달하는 것은 허용합니다. 차단을 원치 않는 경우에 사용합니다. |

대응 모드 중 [에러 코드 보냄]설정 시 선택 가능한 HTTP 상태 코드 및 의미는 [XI.4 에러처리 상태코드]의 [표 HTTP 상태코드와 의미]와 같습니다.

Invalid HTTP 사용자 정의에 Host 필드 없는 경우에 대한 허용 설정은 Host 필드를 알수 없는 트래픽에 대한 탐지 정책을 '미등록 웹사이트'에 속한 정책으로 적용하겠다는 의미 입니다.

Invalid URI

개요

RFC에 정의된 형식을 벗어난 URI는 웹 서버나 웹 애플리케이션의 오동작을 야기할 수 있습니다.

공격 예

URI 에 문법에 맞지 않거나 알 수 없는 이상한 문자를 넣어 시스템의 오동작을 유발 시키는 공격입니다.



대응 방안

웹 서버나 웹 애플리케이션에서 입력 URI에 대해 필터링을 수행해야합니다.

WAF에서는 위의 Invalid URI 공격에 대한 대응 방안으로 아래 표와 같이 2개의 탐지 모드를 제공합니다.

Invalid URI 탐지 모드

| 모드 | 설명 |
|-----------|--|
| [일반 설정] | URI에서 사용할 수 없는 문자를 사용하거나 잘못된 방식으로 인코딩하는 등의 부적절한 형식의 URI를 탐지합니다 |
| [탐지하지 않음] | 해당 룰을 탐지하지 않습니다. |

위 탐지 모드에 의해 Invalid URI 공격의 탐지가 일어났을 때 아래 표의 4가지 대응방법 중 하나를 선택하여 대응 할 수 있습니다.

대응 설정 항목

| 모드 | 설명 |
|--------------|---|
| 연결 끊기 | HTTP 연결을 강제 종료 합니다. |
| 에러 코드 보냄 | HTTP의 상태 코드를 응답합니다. 일반적으로 요구 메시지가 잘못된 형식으로 구성 되어 있거나 제대로 처리할 수 없는 경우 등의 코드를 보냅니다. |
| 다른 웹 페이지로 이동 | 준비된 에러처리 웹 페이지로 이동합니다. |
| 차단하지 않음 | 탐지로그에 기록은 남으나 웹 서버로 전달하는 것은 허용합니다. 차단을 원치 않는 경우에 사용합니다. |

대응 모드 중 [에러 코드 보냄]설정 시 선택 가능한 HTTP 상태 코드 및 의미는 [XI.4 에러처리 상태코드]의 [표 HTTP 상태코드와 의미]와 같습니다.

예외 처리

운영자는 웹사이트의 환경에 따라 Invalid URI의 탐지가 해당 웹페이지에 적합하지 않다고 판단될 경우 해당 웹 페이지에 대하여 Invalid URI 탐지를 예외 처리 할 수 있습니다. 탐지 예외 설정 방법은 [VIII.7탐지 예외 설정 변경]에서 볼 수 있습니다.

IP Filtering

개요

웹 서버로 접속하는 클라이언트 IP에 대하여 필터링 합니다. 일반적인 IP 또는 IP와 netmask조합, 국가별로 할당 된 IP에 따른 필터링이 가능합니다.

공격 예

공격이라고 단정할 수는 없으나 필요에 따라 접속IP를 탐지하고 차단할 수 있습니다.

등록된 IP 및 국가에 포함되지 않는 IP에서 접속한 경우 탐지된 예입니다.



대응 방안

사용자에 의해 추가된 IP나 국가에 대하여 필터링을 설정 할 수 있습니다. 필터링을 할 때에는 추가한 IP나 특정 국가인 경우 필터링 하는 옵션과 추가한 IP나 특정국가만 허용하는 옵션을 선택할 수 있습니다.

국가의 IP 는 InterNIC 등에 등록된 국가별 IP 할당 현황을 기준으로 반영되며 정기적인 WAF Online Update 를 통하여 갱신되므로 시간차에 따른 오차가 발생할 수 있습니다.

IP Block 과 IP Filtering 은 다음과 같은 차이점이 있습니다.

IP Block과 IP Filtering의 차이점

| IP Block | IP Filtering |
|--|---|
| 다른 룰에 대한 누적 탐지/대응에 따라 자동으로 IP가 추가됩니다. | 자동으로 추가되는 IP는 없으나 국가별로 추가할 수 있습니다. |
| 차단 IP로 등록된 경우 무조건차단합니다. (연결 허용의 경우 자동 차단을 금지하는 의미입니다.) | 등록된 목록을 차단할지 등록된 목록만 허용할지를 선택 할 수 있습니다. |
| 차단 목록에서 삭제되는 시간이 있어 해당 시간이 되면 자동으로 목록에서 삭제 됩니다. | 자동으로 삭제되지 않습니다. |
| 차단 목록에 있는 경우 호스트나 정책에 상관없이 차단합니다. | 정책 별로 차단 목록을 작성할수 있습니다. |

| | |
|---------------------------------------|------------------------------|
| 차단 목록에 있는 경우 WAF을 통과하는 모든 트래픽을 차단합니다. | 등록된 호스트에 따라 웹 트래픽만 영향을 받습니다. |
|---------------------------------------|------------------------------|

위 탐지 모드에 의해 IP Filtering에 해당 했을 때 아래 표의 4가지 대응방법 중 하나를 선택하여 대응 할 수 있습니다.

대응 설정 항목

| 모드 | 설명 |
|--------------|--|
| 연결 끊기 | HTTP 연결을 강제 종료 합니다. |
| 에러 코드 보냄 | HTTP의 상태 코드를 응답합니다. 일반적으로 요구 메시지가 잘못된 형식으로 구성되어 있거나 제대로 처리할 수 없는 경우 등의 코드를 보냅니다. |
| 다른 웹 페이지로 이동 | 준비된 에러처리 웹 페이지로 이동합니다. |
| 차단하지 않음 | 탐지로그에 기록은 남으나 웹 서버로 전달하는 것은 허용합니다. 차단을 원치 않는 경우에 사용합니다. |

대응 모드 중 [에러 코드 보냄]설정 시 선택 가능한 HTTP 상태 코드 및 의미는 [XI.4 에러처리 상태코드]의 [표 HTTP 상태코드와 의미]와 같습니다.

설정 방법

IP Filtering룰의 사용자 정의 설정 화면은 2가지 목록과 1가지의 선택사항이 있습니다.

IP 목록의 설정은 아래 입력 창에 IP 또는 IP/netmask bit를 넣고 [추가]버튼으로 등록하고, 삭제할 사항을 선택한 후 [삭제]버튼을 클릭하여 삭제할 수 있습니다.

국가 목록은 해당 국가 앞의 체크박스에 체크를 하면 됩니다.

선택 사항은 작성된 목록의 IP를 탐지할지 목록에 없는 IP를 탐지 할지 선택합니다

IP Filtering의 사용자 정의 설정의 예입니다.



예외 처리

운영자는 웹사이트의 환경에 따라 Invalid URI의 탐지가 해당 웹페이지에 적합하지 않다고 판단될 경우 해당 웹 페이지에 대하여 Invalid URI 탐지를 예외 처리 할 수 있습니다. 탐지 예외 설정 방법은 [VIII.7탐지 예외 설정 변경]에서 볼 수 있습니다.

Parameter Tampering

개요

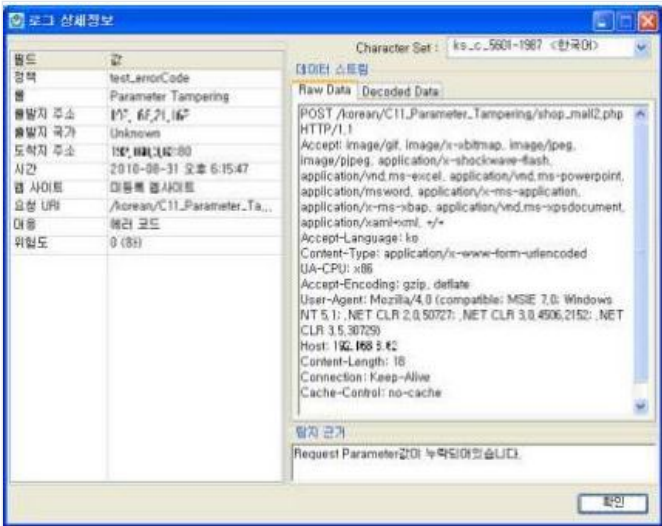
웹 애플리케이션의 URL이나 인자를 프로그래머가 원하지 않는 다른 값으로 변조하여 공격하는 기법입니다. 웹 애플리케이션이 사용자의 입력값을 적절히 검증하지 않는 경우 예기치 못한 오동작을 유발하거나, 웹애플리케이션의 보안 메커니즘을 우회할 수 있습니다.

URI에 포함된 인자를 변경하여 SQL 문을 조작하거나, HTML 문서 내의 Hidden field 값을 변경하여 전송하는 Hidden Field Manipulation등을 포함합니다.

공격 예

WAF에서 Parameter Tampering이 활성화되면 보호하고자 하는 웹 서버로 접근시도 시 무결성을 보장하기 위한 부가 정보를 보내오지 않으면 정상적인 접속으로 판단하지 않게 됩니다.

무결성을 보장하기 위한 부가 정보를 보내오지 않았기 때문에 탐지된 예입니다.



대응 방안

웹 서버나 웹 애플리케이션에서 입력 값에 대한 필터링을 수행해야 합니다. 단, 특정한 인자나 패턴만을 필터링 하는 Negative 방식은 유지보수에 있어 비효율적이므로, 허용된 값만을 받아들이는 Positive 방식을 사용하여 인자를 검증하여야 합니다.

WAF에서는 위의 Parameter Tampering 공격에 대한 대응 방안으로 아래 표와 같이 2개의 탐지 모드를 제공합니다.

Parameter Tampering 탐지 모드

| 모드 | 설명 |
|-----------|---|
| [일반 설정] | 웹 사이트에서 요구하지 않은 입력 Parameter값을 보내거나 웹사이트에서 전송한 Parameter를 조작하는 공격을 탐지합니다. |
| [탐지하지 않음] | 해당 룰을 탐지하지 않습니다. |

Parameter Tampering 은 웹 페이지 내에서 JavaScript 를 사용하여 parameter 를 조작하는 경우 탐지될 수 있으며 JavaScript 사용이 빈번한 웹사이트에 적용 시 오탐 발생률이 높을 수 있습니다.

위 탐지 모드에 의해 Parameter Tampering 공격의 탐지가 일어났을 때 아래 표의 4가지 대응방법 중 하나를 선택하여 대응 할 수 있습니다.

대응 설정 항목

| 모드 | 설명 |
|-------|---------------------|
| 연결 끊기 | HTTP 연결을 강제 종료 합니다. |

| | |
|--------------|--|
| 에러 코드 보냄 | HTTP의 상태 코드를 응답합니다. 일반적으로 요구 메시지가 잘못된 형식으로 구성되어 있거나 제대로 처리할 수 없는 경우 등의 코드를 보냅니다. |
| 다른 웹 페이지로 이동 | 준비된 에러처리 웹 페이지로 이동합니다. |
| 차단하지 않음 | 탐지로그에 기록은 남으나 웹 서버로 전달하는 것은 허용합니다. 차단을 원치 않는 경우에 사용합니다. |

대응 모드 중 [에러 코드 보냄]설정 시 선택 가능한 HTTP 상태 코드 및 의미는 [XI.4 에러처리 상태코드]의 [표 HTTP 상태코드와 의미]와 같습니다.

예외 처리

운영자는 웹사이트의 환경에 따라 Invalid URI의 탐지가 해당 웹페이지에 적합하지 않다고 판단될 경우 해당 웹 페이지에 대하여 Invalid URI 탐지를 예외 처리 할 수 있습니다. 탐지 예외 설정 방법은 [VIII.7탐지 예외 설정 변경]에서 볼 수 있습니다.

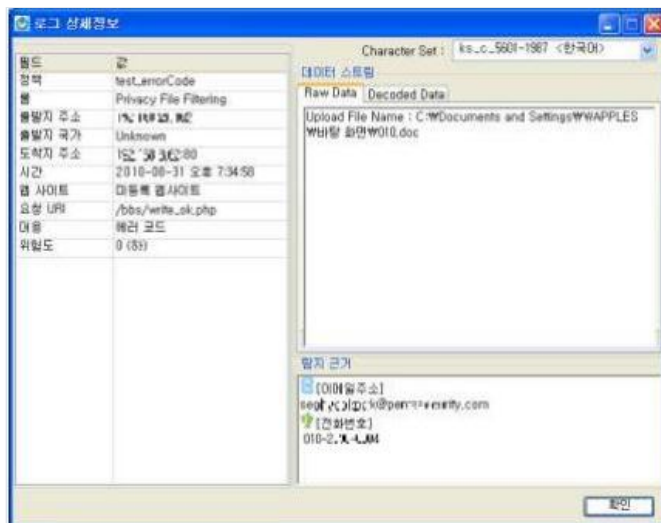
Privacy File Filtering

개요

웹사이트에는 문서 종류의 파일을 게시할 수 있습니다. 이 경우 개인정보가 포함된 문서가 웹사이트로 게시되는 경우 개인정보 누출이라는 위험이 발생합니다.

공격 예

개인 정보가 포함된 ms-word 문서를 업로드 시 탐지된 예입니다.



대응 방안

게시판 및 자료실에 민감한 개인 정보가 포함된 문서 파일을 업로드시 파일의 내용을 분석하여 내부에 기록된 개인정보(주민등록번호, 신용카드번호, 전화번호, 이메일 주소, 거주지 주소)를 탐지 합니다.

지원 하는 문서 파일은 다음과 같습니다.

Microsoft Word

Microsoft Excel

Microsoft PowerPoint

한글과 컴퓨터 HWP

Adobe PDF

삼성 소프트 훈민정음 gul

압축 파일 zip, tar, gz

plain text

WAF에서는 위의 Privacy File Filtering 위협에 대한 대응 방안으로 아래 표와 같이 4개의 탐지 모드를 제공합니다.

Privacy File Filtering 탐지 모드

| 모드 | 설명 |
|--------------|---|
| [모든 개인정보 차단] | 웹사이트로 업로드 되는 문서파일에 주민등록번호, 카드번호, 이메일, 주소, 전화번호가 포함되어 있는지 검사합니다. |
| [중요 개인정보 차단] | 웹사이트로 업로드 되는 문서파일에 개인정보인 주민등록번호, 카드번호가 포함되어 있는지 검사합니다. |
| [사용자 정의] | 파일의 업로드와 다운로드시의 탐지 여부와 법인등록번호, 사업자등록번호, 은행계좌번호양식, 이메일, 전화번호, 주민등록번호, 외국인등록번호, 주소, 카드번호 포함 여부 등을 사용자가 정의합니다. |
| [탐지하지 않음] | 해당 룰을 탐지하지 않습니다 |

위 탐지 모드에 의해 Privacy File Filtering이 일어났을 때 아래 표의 4가지 대응방법 중 하나를 선택하여 대응 할 수 있습니다.

대응 설정 항목

| 모드 | 설명 |
|--------------|--|
| 연결 끊기 | HTTP 연결을 강제 종료 합니다. |
| 에러 코드 보냄 | HTTP의 상태 코드를 응답합니다. 일반적으로 요구 메시지가 잘못된 형식으로 구성되어 있거나 제대로 처리할 수 없는 경우 등의 코드를 보냅니다. |
| 다른 웹 페이지로 이동 | 준비된 에러처리 웹 페이지로 이동합니다. |
| 차단하지 않음 | 탐지로그에 기록은 남으나 웹 서버로 전달하는 것은 허용합니다. 차단을 원치 않는 경우에 사용합니다. |

대응 모드 중 [에러 코드 보냄]설정 시 선택 가능한 HTTP 상태 코드 및 의미는 [XI.4 에러처리 상태코드]의 [표 HTTP 상태코드와 의미]와 같습니다.

예외 처리

운영자는 웹사이트의 환경에 따라 Invalid URI의 탐지가 해당 웹페이지에 적합하지 않다고 판단될 경우 해당 웹 페이지에 대하여 Invalid URI 탐지를 예외 처리 할 수 있습니다. 탐지 예외 설정 방법은 [VIII.7탐지 예외 설정 변경]에서 볼 수 있습니다.

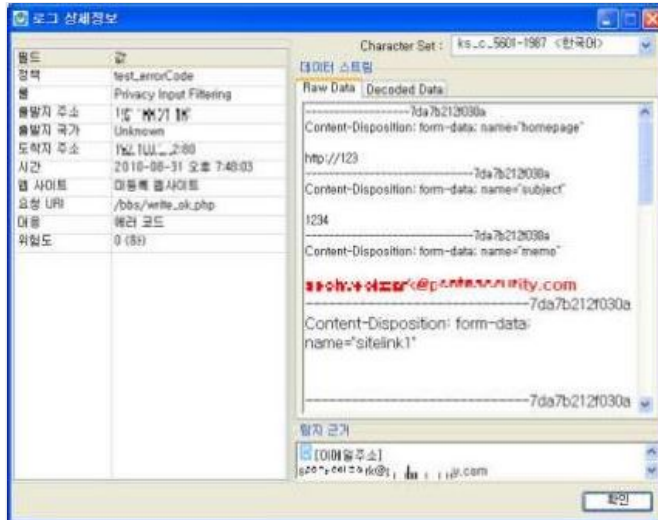
Privacy Input Filtering

개요

게시판 등을 통하여 웹 서버로 전송된 Request Message의 내용을 분석하여 내부에 기록된 개인정보(주민등록번호, 외국인등록번호, 신용카드번호, 전화번호, 이메일 주소, 거주지 주소, 법인 등록번호, 사업자등록번호, 은행계좌번호양식)를 탐지 합니다. 개인정보가 포함된 Request Message가 웹 서버로 전송될 경우 개인정보의 유입을 사전에 차단할 수 있습니다. Request Message의 내용은 변경하지 않고 Request Message에 개인정보가 포함되어 있을 경우에만 탐지 및 차단하므로 게시판의 특성에 맞게 탐지 룰을 적용시킬 필요가 있습니다.

공격 예

RequestMessage에 포함된 이메일이 탐지된 예입니다.



대응 방안

게시판 등을 통하여 웹 서버로 전송된 Request Message의 내용을 검사하여 개인정보의 포함 여부를 확인합니다. 개인정보가 포함된 Request Message 인 경우 이를 사용자 및 관리자에게 통보하고 상황에 따라 아예 차단하거나 또는 경고를 표시할 수 있습니다.

WAF에서는 위의 Privacy Input Filtering 위협에 대한 대응 방안으로 아래 표와 같이 3개의 탐지 모드를 제공합니다.

Privacy Input Filtering 탐지 모드

| 모드 | 설명 |
|--------------|--|
| [모든 개인정보 차단] | HTTP Request Message에 주민등록번호, 카드번호가 포함되어 있는지 검사합니다. |
| [중요 개인정보 차단] | HTTP Request Message에 주민등록번호가 포함되어 있는지 검사합니다. |
| [사용자 정의] | HTTP Request Message에 법인등록번호, 사업자등록번호, 은행계좌번호양식, 이메일, 전화번호, 주민등록번호, 외국인등록번호, 주소, 카드번호 포함 여부 등을 검사하도록 사용자가 정의합니다. |
| [탐지하지 않음] | 해당 룰을 탐지하지 않습니다 |

위 탐지 모드에 의해 Privacy Input Filtering이 일어났을 때 아래 표의 4가지 대응방법 중 하나를 선택하여 대응할 수 있습니다.

대응 설정 항목

| 모드 | 설명 |
|--------------|--|
| 연결 끊기 | HTTP 연결을 강제 종료 합니다. |
| 에러 코드 보냄 | HTTP의 상태 코드를 응답합니다. 일반적으로 요구 메시지가 잘못된 형식으로 구성되어 있거나 제대로 처리할 수 없는 경우 등의 코드를 보냅니다. |
| 다른 웹 페이지로 이동 | 준비된 에러처리 웹 페이지로 이동합니다. |
| 차단하지 않음 | 탐지로그에 기록은 남으나 웹 서버로 전달하는 것은 허용합니다. 차단을 원치 않는 경우에 사용합니다. |

대응 모드 중 [에러 코드 보냄]설정 시 선택 가능한 HTTP 상태 코드 및 의미는 [XI.4 에러처리 상태코드]의 [표 HTTP 상태코드와 의미]와 같습니다.

예외 처리

운영자는 웹사이트의 환경에 따라 Invalid URI의 탐지가 해당 웹페이지에 적합하지 않다고 판단될 경우 해당 웹 페이지에 대하여 Invalid URI 탐지를 예외 처리 할 수 있습니다. 탐지 예외 설정 방법은 [VIII.7탐지 예외 설정 변경]에서 볼 수 있습니다.

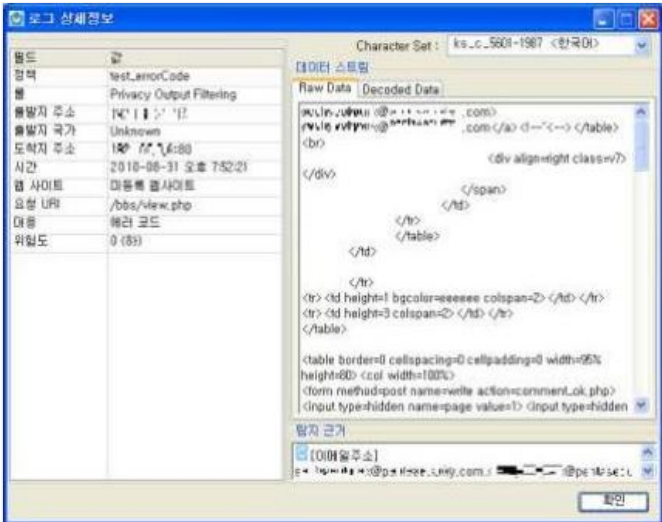
Privacy Output Filtering

개요

웹 서비스를 통하여 유출될 수 있는 정보를 차단합니다. 기본적으로 신용카드번호와 같은 개인정보의 유출을 차단하는 목적으로 사용됩니다.

공격 예

HTTP Response Message에 이메일주소가 존재하여 탐지된 예입니다.



대응 방안

신용카드번호가 유출되는 것을 발견하면 페이지 전체를 차단하거나, 신용카드번호 부분의 일부만 가려서 출력할 수 있습니다.

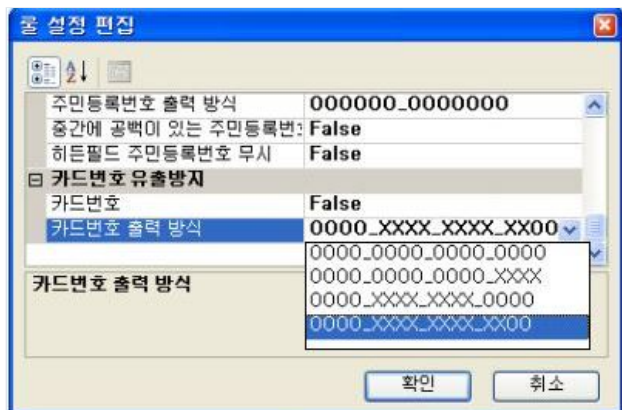
WAF에서는 위의 Privacy Output Filtering공격에 대한 대응 방안으로 아래 표와 같이 4개의 탐지 모드를 제공합니다.

Privacy Output Filtering 탐지 모드

| 모드 | 설명 |
|-----------------|---|
| [모든 개인정보 유출 방지] | HTTP Response Message에 주민등록번호, 카드번호가 포함되어 있는지 검사합니다. |
| [주민등록번호 유출 방지] | HTTP Response Message에 주민등록번호가 포함되어 있는지 검사합니다. |
| [사용자 정의] | |
| | [주민등록번호] |
| | 주민등록번호 유출 방지의 활성화 여부를 True/False값으로 설정합니다. [출력방식] 항목은 주민등록번호의 각 자리 별로 표시 여부를 선택하는 것으로 X부분은 "*"로 변조되어 웹사이트 사용자에게 전달됩니다. [히든 필드 주민등록번호 무시]항목은 주민등록번호의 HTML Tag 데이터 속성이 hidden인 경우 변조 여부를 True/False로 설정합니다. |
| | [카드번호] |
| | 카드번호 유출 방지의 활성화할지 여부를 True/False값으로 설정합니다. [출력방식] 항목은 카드번호의 각 자리 별로 표시 여부를 선택하는 것으로 X부분은 "*"로 변조되어 웹사이트 사용자에게 전달됩니다. |

| | | |
|-----------|-----------|--|
| | | |
| | [주소] | Http Response Message에 포함된 주소의 탐지여부를 설정합니다. [주소유출방지]항목은 주소 유출 방지기능의 활성화 여부를 True/False 값으로 설정합니다. |
| | [계좌번호] | 계좌번호 유출방지 기능의 활성화 여부를 True/False 값으로 설정합니다. [은행 계좌번호 양식]항목은 은행 계좌번호의 숫자 구성을 입력합니다. 연속된 숫자의 개수를 나열합니다. 입력된 계좌번호 양식이 없을 경우 계좌번호는 탐지하지 않습니다.예)000-0000-00-000 -> 3423 |
| | [이메일] | Http Response Message에 포함된 이메일의 탐지여부를 설정합니다. [이메일 정보 유출방지]항목은 이메일 정보 유출방지 기능의 활성화 여부를 True/False 값으로 설정합니다. |
| | [전화번호] | Http Response Message에 포함된 전화번호의 탐지여부를 설정합니다. [전화번호 유출방지]항목은 전화번호 유출방지 기능의 활성화 여부를 True/False 값으로 설정합니다. |
| | [법인등록번호] | 법인등록번호 유출방지 기능의 활성화 여부를 True/False 값으로 설정합니다. [법인등록번호 출력방식]항목은 법인등록번호의 각 자리 별로 표시 여부를 선택하는 것으로 X부분은 "*"로 변조되어 웹사이트 사용자에게 전달됩니다. |
| | [사업자등록번호] | 사업자등록번호 유출방지 기능의 활성화 여부를 True/False 값으로 설정합니다. [사업자등록번호 출력방식]항목은 사업자등록번호의 각 자리 별로 표시 여부를 선택하는 것으로 X부분은 "*"로 변조되어 웹사이트 사용자에게 전달됩니다. |
| [탐지하지 않음] | | 해당 룰을 탐지하지 않습니다 |

주민등록번호, 계좌번호, 법인등록번호, 사업자등록번호의 탐지는 한국내에서 사용되는 형식만 탐지 가능합니다.



위 탐지 모드에 의해 Privacy Input Filtering이 일어났을 때 아래 표의 4가지 대응방법 중 하나를 선택하여 대응할 수 있습니다.

대응 설정 항목

| 모드 | 설명 |
|--------------|--|
| 연결 끊기 | HTTP 연결을 강제 종료 합니다. |
| 에러 코드 보냄 | HTTP의 상태 코드를 응답합니다. 일반적으로 요구 메시지가 잘못된 형식으로 구성되어 있거나 제대로 처리할 수 없는 경우 등의 코드를 보냅니다. |
| 다른 웹 페이지로 이동 | 준비된 에러처리 웹 페이지로 이동합니다. |
| 차단하지 않음 | 탐지로그에 기록은 남으나 웹 서버로 전달하는 것은 허용합니다. 차단을 원치 않는 |

경우에 사용합니다. Privacy Output Filtering의 경우에는 사용자 정의에서 설정한 항목별 출력 방식에 따라 탐지 항목이 출력됩니다.예) 카드번호 출력 방식 설정:OOOO_XXXX_XXXX_OOOO 실제 출력 내용:1234_****_****_5678

대응 모드 중 [에러 코드 보냄]설정 시 선택 가능한 HTTP 상태 코드 및 의미는 [XI.4 에러처리 상태코드]의 [표 HTTP 상태코드와 의미]와 같습니다.

Privacy Output Filtering 은 탐지하고자 하는 문자열을 변경문자열로 정의하고자 할 경우 대응방법을 [차단하지 않음]으로 설정 하여야 합니다.

예외 처리

운영자는 웹사이트의 환경에 따라 Privacy Output Filtering의 탐지가 해당 웹페이지에 적합하지 않다고 판단될 경우 해당 웹페이지에 대하여 Privacy Output Filtering 탐지를 예외 처리 할 수 있습니다. 탐지 예외 설정 방법은 [VIII.7탐지 예외 설정 변경]에서 볼 수 있습니다.

Request Header Filtering

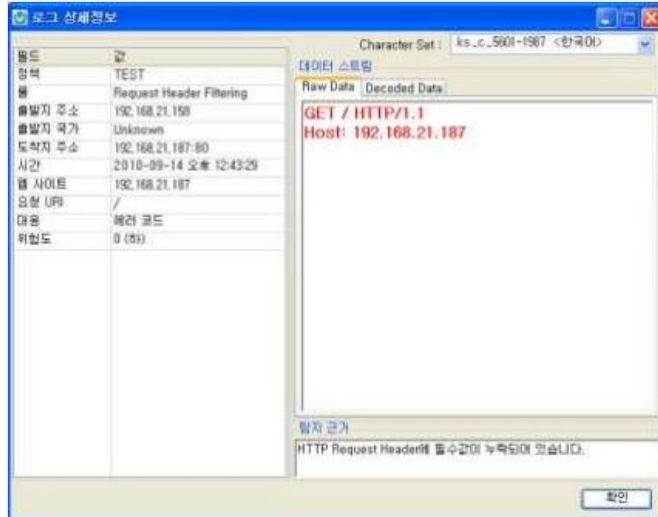
개요

HTTP Request Header 부분의 정보를 검사하여, 설정된 Field와 Value의 존재 여부에 따라 Filtering합니다.

사용자의 설정에 따라 HTTP Request Header Field의 내용을 한정 지어, Browser를 제약할 수도 있으며, 원치 않는 클라이언트의 접속을 차단하거나 접근을 제한할 수 있습니다

공격 예

HTTP Request Header Data 중 User-Agent Field의 Value값이 존재 하지 않아 탐지한 예 입니다.



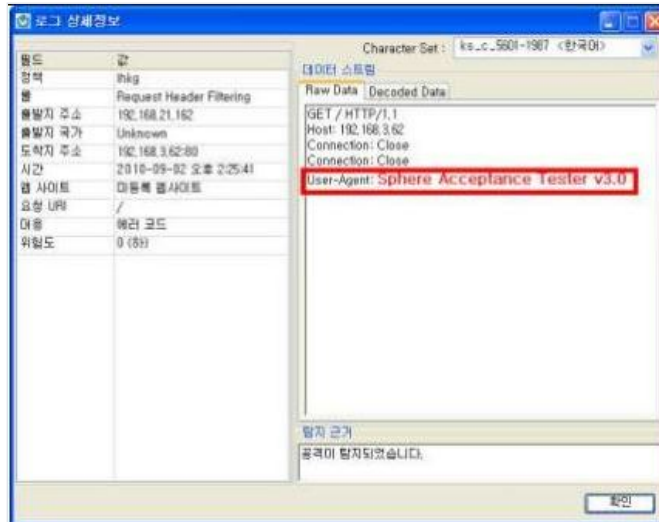
Request Header Filtering은 사용자 정의 기능을 통하여 [리스트 포함] 기능과 [리스트 차단] 기능을 제공합니다. [리스트 포함] 기능은 리스트에 추가한 Key와 Value가 포함되어 있는 트래픽 만을 통과 시키는 방식이며, 리스트 차단 기능은 리스트에 추가한 Key 또는 Value가 포함되어 있는 트래픽을 차단시키는 기능입니다.

아래 그림 은 [사용자정의]의 리스트 포함 기능 설정을 다음과 같이 설정한 예입니다.

User-Agent의 Value값에 Mozilla 라는 정보가 포함 되어 있는 트래픽만 허용합니다.

Request Header 이름 중 Accept Key가 있는 트래픽만 허용합니다.

이와 같이 설정된 탐지 룰이 적용 되어 있을 경우 아래그림 에서 보여지는 HTTP 요청 메시지는 User-Agent Value값(Sphere acceptance Tester v2.1)에 Mozilla 문자열이 포함되지 않아 탐지 대상이 됩니다.



아래그림은 [사용자 정의]의 리스트 차단 기능에 cache-control Key를 설정한 예입니다.



Cache-control이라는 헤더 키를 가지고 있는 트래픽에 대해 차단하기에 아래그림과 같은 탐지 결과를 볼 수 있습니다.



대응 방안

WAF에서는 Request Header Filtering에 대한 대응 방안으로 아래 표와 같이 3개의 탐지 모드를 제공합니다.

탐지 모드중 사용자 설정에서는 HTTP 요청 메시지의 Field값과 Value 값에 제한을 주어 사용자 환경에 적절한 유동적인 탐지를 가능하게 합니다. [표 53 사용자 정의 필드 리스트]에서는 HTTP 요청 Field각각에 대한 간단한 설명과 Value값 예시가 있습니다

Request Header Filtering 탐지 모드

| 모드 | 설명 |
|------------|--|
| [간단한 원 차단] | HTTP Request Header Field중 User-Agent가 없으면 탐지합니다. 각 field의 Value 값은 유무만 판별하여 NULL일 경우 탐지 합니다. |
| [사용자 정의] | HTTP Request Header Field와 Value 값을 사용자가 정의합니다. Field와 Value값은 리스트 포함 기능과 리스트 차단 기능에 따라 구분하여 설정 하여야 합니다. 설정된 Field에 대한 각 Value 값은 일치와 포함(부분 일치)으로 나뉠 수 있으며, Value값은 검사하지 않고 Field값만 검사할 수도 있습니다. 설정된 사용자 정의 값에 따라 들어오는 트래픽에 대한 차단여부에 대해서는 [표 사용자 정의에 따른 탐지 여부] 를 참조합니다.탐지는 모든 설정에 대해 OR 연산으로 탐지 여부를 가리므로 설정된 조건 중 하나라도 해당되는 트래픽은 모두 탐지됩니다. |
| [탐지하지 않음] | 해당 룰을 탐지하지 않습니다. |

사용자 정의에 따른 탐지 여부

| 사용자 설정 환경 | | key 유무 | value 유무 | 탐지 결과 |
|-----------|----------|--------|----------|-------|
| 리스트 차단 | value 일치 | O | O(일치) | 탐지 |
| | | | O(포함) | 탐지 안됨 |
| | | | X | 탐지 안됨 |
| | value 포함 | O | O | 탐지 |
| | | | X | 탐지 안됨 |
| | | X | 무관 | 탐지 안됨 |
| | | | 무관 | 탐지 안됨 |
| | Key 검사 | O | 무관 | 탐지 |
| | | X | 무관 | 탐지 안됨 |
| 리스트 차단 | value 일치 | O | O(일치) | 탐지 안됨 |
| | | | O(포함) | 탐지 |
| | | | X | 탐지 |
| | | X | 무관 | 탐지 |
| | Value 포함 | O | O | 탐지 안됨 |
| | | | X | 탐지 |

| | | | | |
|--|--------|---|----|-------|
| | | X | 무관 | 탐지 |
| | Key 검사 | O | 무관 | 탐지 안됨 |
| | | X | 무관 | 탐지 |

Request Header Filtering의 탐지 모드중 [사용자 정의]를 선택하였을 경우 아래 표의 [Field]를 탐지 조건으로 설정할 수 있습니다.

사용자 정의 필드 리스트

| Field | 설명 |
|------------------|---|
| Accept | 허용하는 특정 미디어 유형을 지정하는데 사용할 수 있습니다. 예) Accept: text/plain; q=0.5, text/html, text/x-dvi; q=0.8, text/x-c |
| AcceptCharset | 허용하는 문자 집합을 나타내기 위해 사용합니다. 예)Accept-Charset: iso-8859-5, unicode-1-1;q=0.8 |
| AcceptEncoding | Accept와 유사하지만, 응답으로 사용할 수 있는 Content-codings 값에 제한이 있습니다.예) Accept-Encoding: compress;q=0.5, gzip;q=1.0 |
| AcceptLanguage | Accept와 유사. 요청에 대한 응답으로 선호되는 자연어의 집합을 제한할 수 있습니다. 예) 덴마크어를 선호하지만, 영국식 영어나 다른 타입의 영어도 허용합니다 Accept-Language: da, en-gb;q=0.8, en;q=0.7 |
| Allow | 리소스와 연관된 타당한 메소드의 수용을 명시할 수 있습니다., 클라이언트가 다른 methods를 사용하고자 시도하는 것을 방지할 수는 없으나, Allow 헤더 필드가 표시하는 내용은 준수해야만 합니다. 예) Allow: GET, HEAD, PUT |
| Authorization | 서버에서 자신을 인증하고자 하는 사용자 에이전트는 (꼭 그런 것은 아니지만 대개의 경우 401 응답을 수신한 후) 요구에 Authorization requestheader 필드를 포함하여 자신의 인증 획득을 시도할 수 있습니다. |
| Connection | 발송 측이 특정 연결이 원하는 선택 사항을 명시하는데 사용하며 추가적인 연결 시 프락시를 통하여 통신 해서는 절대 안 됩니다.예) Connection: close |
| Content-Encoding | 주로 문서를 기저의 media type의 identity를 상실하지 않고도 압축할 수 있도록 하는 데 사용됩니다. 예) Content-Encoding: gzip |
| Content-Language | 사용자가 사용자 자신이 선호하는 언어에 따라 엔티티를 식별하거나 구별할 수 있도록 하는 것입니다 예) 본문 내용은 덴마크어 이해할수 있는 사람을 위한것입니다. Content-Language: da |
| Content-Length | 엔터티의 media type에 관계 없이 이 필드를 전송하는 message-body의 크기를 표시하는 데 사용됩니다 예) Content-Length: 3495 |
| Content-Type | 수신 측에 발송한 entity-body의 media type을 표시하는데 사용합니다.예) Content-Type: text/html; charset=ISO-8859-4 |
| ETag | 관련된 엔터티의 엔터티 태그를 정의합니다. 또한 동일한 자원의 다른 엔터티와 비교하는 데도 사용할 수 있습니다.예) ETag: W/"xyzyzy" |
| Host | 사용자나 참조하고자 하는 자원이 할당한 원래의 목적지 URL을 기준으로 인터넷 호스트와 포트 숫자를 명시합니다 예) Host: www.w3.org. |
| If-Match | method와 함께 사용하여 method를 조건적으로 만듭니다. 이전에 자원에서 획득한 하나 또는 그 이상의 엔터티를 가진 클라이언트는 연관된 엔터티 태그의 목록을 If-Match 헤더 필드에 포함하여 이러한 엔터티 중의 하나가 현재의 것임을 증명할 수 있습니다. 이 기능의 목적은 트랜잭션 오버헤드를 최소화하면서 캐시 된 정보를 효과적으로 갱신할 수 있도록 하는 것입니다. 또한 요구 |

| | |
|-------------------|--|
| | 를 갱신할 때 자원의 잘못된 버전에 대한 부주의한 변경을 방지하는 데 사용할 수 있습니다.예) If-Match: "xyzyz", "r2d2xxxx", "c3piozzzz" |
| If-ModifiedSince | GET method와 함께 사용하여 GET method를 조건적으로 만듭니다. 요구된 변형자가 이 필드에 명시된 시간 이후에 변경되지 않았으면 엔터티는 서버로부터 리턴 되지 않습니다.예)If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT |
| If-NoneMatch | method와 함께 사용하여 method를 조건적으로 만듭니다. 이전에 자원에서 획득한 하나 또는 그 이상의 엔터티를 가진 클라이언트는 연관된 엔터티 태그의 목록을 If-None-Match 헤더 필드에 포함하여 이러한 엔터티 중의 하나가 현재의 것임을 증명할 수 있습니다. |
| If-Range | 클라이언트가 자신의 캐시에 엔터티의 부분적 사본을 가지고 있고 전체 엔터티의 최신 갱신 사본을 가지고 싶다면 조건적인 GET의 Range request-header를 사용할 수 있습니다. |
| IfUnmodifiedSince | method와 함께 사용하여 method를 조건적으로 만듭니다. 요구된 자원이 이 필드에 명시된 시간 이후 변경되지 않았으면 서버는 If-Unmodified-Since 헤더가 존재하지 않는 것처럼 요구 받은 작업을 수행해야 합니다. |
| LastModified | 원 서버가 변형자가 마지막으로 변경되었다고 믿는 날짜와 시간을 표시합니다.예) Last-Modified: Tue, 15 Nov 1994 12:45:26 GMT |
| MaxForwards | TRACE method와 함께 사용하여 다음의 들어오는 방향의 서버에 요구를 전달할 수 있는 프락시나 게이트웨이의 숫자를 제한합니다. |
| Referer | 클라이언트가 서버를 위해 Request-URI를 얻은 자원의 주소를 명시하기 위하여 사용합니다.예)Referer:http://www.w3.org/hypertext/DataSources/Overview.html |
| User-Agent | Request를 만들어 낸 사용자 에이전트에 관한 정보를 포함하고 있습니다. 이것은 통계 목적, 규약 위반의 추적, 특정 사용자 에이전트 한계를 피하기 위해 Response를 고칠 목적으로하는 사용자 에이전트를 탐지할 때 사용합니다.예)User-Agent: CERN-LineMode/2.15 libwww/2.17b3 |

위 탐지 모드에 의해 Request Header Filtering이 일어났을 때 아래 표의 4가지 대응방법 중 하나를 선택하여 대응 할 수 있습니다.

대응 설정 항목

| 모드 | 설명 |
|--------------|--|
| 연결 끊기 | HTTP 연결을 강제 종료 합니다. |
| 에러 코드 보냄 | HTTP의 상태 코드를 응답합니다. 일반적으로 요구 메시지가 잘못된 형식으로 구성되어 있거나 제대로 처리할 수 없는 경우 등의 코드를 보냅니다. |
| 다른 웹 페이지로 이동 | 준비된 에러처리 웹 페이지로 이동합니다. |
| 차단하지 않음 | 탐지로그에 기록은 남으나 웹 서버로 전달하는 것은 허용합니다. 차단을 원치 않는 경우에 사용합니다. |

대응 모드 중 [에러 코드 보냄]설정 시 선택 가능한 HTTP 상태 코드 및 의미는 **[오류! 참조 원본을 찾을 수 없습니다.오류! 참조 원본을 찾을 수 없습니다.]의 [오류! 참조 원본을 찾을 수 없습니다.]와 같습니다**

예외 처리

운영자는 웹사이트의 환경에 따라 Request Header Filtering룰의 탐지가 해당 웹 페이지에 적합하지 않다고 판단될 경우 해당 웹 페이지에 대하여 Request Header Filtering 탐지를 예외 처리 할 수 있습니다. 탐지 예외 설정 방법은 **[오류! 참조 원본을 찾을 수 없습니다. 오류! 참조 원본을 찾을 수 없습니다.]**을 참조하시기 바랍니다.

Request Method Filtering

개요

HTTP 요청 가운데 불필요하거나 공격에 악용될 수 있는 HTTP Method를 필터링합니다.

공격 예

"PROPFIND"메소드를 이용한 WebDAV 취약점을 이용한 시도로 보여 탐지된 예입니다.



대응 방안

웹 서버에서 불필요한 HTTP method에 대해 필터링을 수행해야 합니다.

WAF에서는 위의 Request Method Filtering 공격에 대한 대응 방안으로 아래 표와 같이 3개의 탐지 모드를 제공합니다.

Request Method Filtering 탐지 모드

| 모드 | 설명 |
|--------------|--|
| [안전한 요청만 처리] | 일반적으로 사용되는 요청 메소드 GET, POST, HEAD, OPTIONS 4개만을 허용합니다. |
| [사용자 정의] | 요청 메소드를 정의하고 해당 메소드를 금지하거나 허용하는 설정을 합니다. |
| [탐지하지 않음] | 해당 룰을 탐지하지 않습니다 |

위 탐지 모드에 의해 Request Method Filtering이 일어났을 때 아래 표의 4가지 대응방법 중 하나를 선택하여 대응 할 수 있습니다.

대응 설정 항목

| 모드 | 설명 |
|--------------|---|
| 연결 끊기 | HTTP 연결을 강제 종료 합니다. |
| 에러 코드 보냄 | HTTP의 상태 코드를 응답합니다. 일반적으로 요구 메시지가 잘못된 형식으로 구성 되어 있거나 제대로 처리할 수 없는 경우 등의 코드를 보냅니다. |
| 다른 웹 페이지로 이동 | 준비된 에러처리 웹 페이지로 이동합니다. |
| 차단하지 않음 | 탐지로그에 기록은 남으나 웹 서버로 전달하는 것은 허용합니다. 차단을 원치 않는 경우에 사용합니다. |

대응 모드 중 [에러 코드 보냄]설정 시 선택 가능한 HTTP 상태 코드 및 의미는 [XI.4 에러처리 상태코드]의 [표 HTTP 상태코드와 의미]와 같습니다.

예외 처리

운영자는 웹사이트의 환경에 따라 Invalid URI의 탐지가 해당 웹페이지에 적합하지 않다고 판단될 경우 해당 웹 페이지에 대하여 Invalid URI 탐지를 예외 처리 할 수 있습니다. 탐지 예외 설정 방법은 [VIII.7탐지 예외 설정 변경]에서 볼 수 있습니다.

Response Header Filtering

개요

웹 서버의 헤더 응답들 중 사용자에게 필요 이상의 정보를 주는 경우 사이트가 가진 잠재적 취약점에 대한 힌트를 제공하는 등 다양한 보안 문제를 야기할 수 있습니다.

대응 방안

웹 서버나 웹 애플리케이션에서 필터링을 수행해야 합니다.

웹 서버에서 기본적으로 발생시키는 서버 정보(웹 서버의 OS, 서버 종류, Active 페이지 언어)등을 얻어 해킹에 사용될 수 있습니다. 일부 사이트에서 특정 헤더를 필요로 하거나 추가적인 정보가 발생하여 이를 가려야 할 때에는 수정이 필요할 수 있습니다.

WAF에서는 위의 Response Header Filtering 공격에 대한 대응 방안으로 아래 표와 같이 3개의 탐지 모드를 제공합니다.

Response Header Filtering 탐지 모드

| 모드 | 설명 |
|---------------|--|
| [서버 정보 유출 방지] | 서버 정보가 유출될 수 있는 Server, XPowered-By 항목을 필터링하여 제거합니다. |
| [사용자 정의] | [출력 허용] 여부, [헤더 문자열]을 관리자가 직접 입력할 수 있습니다. |
| [탐지하지 않음] | 해당 룰을 탐지하지 않습니다 |

해당 룰에 대한 대응은 운영자가 결정하지 않습니다. WAF에서 HTTP Response Message에 금지 헤더가 포함되어 있으면 이를 모두 제거한 후 응답합니다.

예외 처리

운영자는 웹사이트의 환경에 따라 Response Header Filtering의 탐지가 해당 웹페이지에 적합하지 않다고 판단될 경우 해당 웹페이지에 대하여 Response Header Filtering 탐지를 예외 처리 할 수 있습니다. 탐지 예외 설정 방법은 [VIII.7탐지 예외 설정 변경]에서 볼 수 있습니다.

SQL Injection

개요

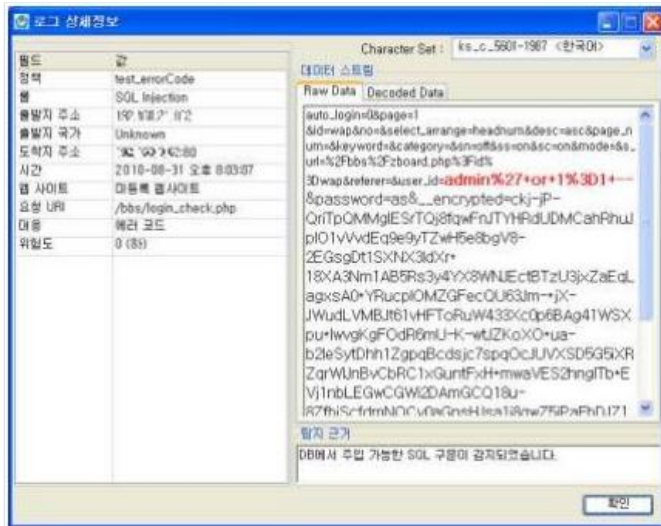
웹 애플리케이션에 강제로 SQL 구문을 삽입하여 내부 데이터베이스의 데이터를 유출, 변조 가능하며, 관리자 인증을 우회할 수도 있습니다. 먼저 공격자는 웹 애플리케이션이 데이터베이스로 전달하는 인자를 찾아냅니다. 악의적인 SQL 명령어를 주의 깊게 인자로 삽입하여, 공격자는 웹 애플리케이션이 악의적인 질의를 데이터베이스로 전달하도록 조작할 수 있습니다. 이 공격 기법은 수행하기 어렵지 않으며 해당 취약점을 찾아주는 다양한 툴들이 지속적으로 발전해나가고 있습니다.

공격 예

"SELECT userid FROM logins WHERE name='admin' OR 1=1;-- AND password= "와 같은 SQL구문을 입력하여 로그인을 시도하고 있습니다.



위와 같은 시도는 WAF에서도 Login 페이지의 ID, Password 창에 SQL Injection 공격 탐지한 예입니다.



대응 방안

웹 서버나 웹 애플리케이션에서 입력 값 검증을 수행하여 악의적인 구문 삽입을 방지할 수 있습니다. 웹 애플리케이션이 해당 기능을 수행하는데 필요한 권한 이상으로 권한을 갖지 않도록 설정합니다.

WAF에서는 위의 SQL Injection 공격에 대한 대응 방안으로 아래 표와 같이 4개의 탐지 모드를 제공합니다.

SQL Injection 탐지 모드

| 모드 | 설명 |
|--------------------------|---|
| [사용자 정의] | SQL Injection으로 사용될 수 있는 SQL 키워드를 기준으로 SQL공격 의심 키워드가 포함된 모든 요청을 탐지합니다. |
| [확장 SQL Injection 공격 탐지] | Cookie 및 Request Parameter를 통해 강제로 SQL 구문을 삽입하여 내부 데이터베이스의 데이터를 유출, 변조하거나 인증을 우회하는 공격을 탐지합니다. |
| [기본 SQL Injection 공격 탐지] | Request Parameter를 통해 강제로 SQL 구문을 삽입하여 내부 데이터베이스의 데이터를 유출, 변조 하거나 인증을 우회하는 공격을 탐지합니다. |
| [탐지하지 않음] | 해당 룰을 탐지하지 않습니다 |

위 탐지 모드에 의해 SQL Injection 공격의 탐지가 일어났을 때 아래 표의 4가지 대응방법 중 하나를 선택하여 대응 할 수 있습니다.

대응 설정 항목

| 모드 | 설명 |
|-------|---------------------|
| 연결 끊기 | HTTP 연결을 강제 종료 합니다. |

| | |
|--------------|--|
| 에러 코드 보냄 | HTTP의 상태 코드를 응답합니다. 일반적으로 요구 메시지가 잘못된 형식으로 구성되어 있거나 제대로 처리할 수 없는 경우 등의 코드를 보냅니다. |
| 다른 웹 페이지로 이동 | 준비된 에러처리 웹 페이지로 이동합니다. |
| 차단하지 않음 | 탐지로그에 기록은 남으나 웹 서버로 전달하는 것은 허용합니다. 차단을 원치 않는 경우에 사용합니다. |

대응 모드 중 [에러 코드 보냄]설정 시 선택 가능한 HTTP 상태 코드 및 의미는 [XI.4 에러처리 상태코드]의 [표 HTTP 상태코드와 의미]와 같습니다.

[SQL Injection 의심 요청 탐지] 모드는 공격 가능성이 있는 대부분의 SQL query 및 keyword 를 탐지하므로, 예상치 못한 오탐이 발생할 수 있습니다.

예외 설정

운영자는 웹사이트의 환경에 따라 SQL Injection의 탐지가 해당 웹페이지에 적합하지 않다고 판단될 경우 해당 웹페이지에 대하여 SQL Injection 탐지를 예외 처리 할 수 있습니다. 탐지 예외 설정 방법은 [VIII.7 탐지 예외 설정 변경]에서 볼 수 있습니다.

Stealth Commanding

개요

많은 웹 애플리케이션이 OS나 외부 프로그램을 사용하여 기능을 수행하고 있습니다. 웹 애플리케이션이 HTTP 요청을 받아 이 정보를 외부로 전달할 때, 공격자가 악의적인 명령어를 정보로 삽입할 수 있고, 웹 애플리케이션은 이 정보를 그대로 외부 프로그램에 전달하여 실행하게 합니다. 공격자는 이를 이용하여 트로이 목마를 심거나 악의적인 코드를 실행할 수 있습니다.

웹 사이트 고유 애플리케이션을 대상으로 하는 경우는 상대적으로 적으며 잘 알려진 웹 애플리케이션의 버그를 주로 이용하고 있습니다. 이는 먼저 스캐너를 사용하여 존재 여부 탐색하고 악의적인 명령을 실행합니다.

공격 예

/etc/passwd 등의 보안 관련 시스템 파일 접근 시도하기 위해 세미콜론(%3b), 파이프문자(%7c), 스페이스(%20)를 이용하여 명령(/bin/l;/bin/lsgrep main)을 실행하는 예입니다.



대응 방안

SQL Injection과 마찬가지로, 웹 서버나 웹 애플리케이션에서 입력 값 검증을 수행하여 악의적인 명령 삽입을 방지 할 수 있습니다. 웹 애플리케이션이 해당 기능을 수행하는데 필요한 권한 이상으로 권한을 갖지 않도록 설정 합니다.

WAF에서는 위의 Stealth Commanding 공격에 대한 대응 방안으로 아래 표와 같이 3개의 탐지 모드를 제공합니다.

Stealth Commanding 탐지 모드

| 모드 | 설명 |
|-----------|--|
| [일반설정] | 웹 애플리케이션은 HTTP 요청을 받아 해당 정보를 외부로 전달하며 이곳에 외부프로그램을 실행할 수 있는 악의적인 명령어가 공격자에 의해 삽입되었는지 탐지합니다. |
| [사용자 정의] | 상대 경로를 통한 접근 시도 탐지 여부를 선택하여 탐지 할수 있습니다. |
| [탐지하지 않음] | 해당 룰을 탐지하지 않습니다 |

위 탐지 모드에 의해 Stealth Commanding 공격의 탐지가 일어났을 때 아래 표의 4가지 대응방법 중 하나를 선택하여 대응 할 수 있습니다.

대응 설정 항목

| 모드 | 설명 |
|--------------|--|
| 연결 끊기 | HTTP 연결을 강제 종료 합니다. |
| 에러 코드 보냄 | HTTP의 상태 코드를 응답합니다. 일반적으로 요구 메시지가 잘못된 형식으로 구성되어 있거나 제대로 처리할 수 없는 경우 등의 코드를 보냅니다. |
| 다른 웹 페이지로 이동 | 준비된 에러처리 웹 페이지로 이동합니다. |
| 차단하지 않음 | 탐지로그에 기록은 남으나 웹 서버로 전달하는 것은 허용합니다. 차단을 원치 않는 경우에 사용합니다. |

대응 모드 중 [에러 코드 보냄]설정 시 선택 가능한 HTTP 상태 코드 및 의미는 [XI.4 에러처리 상태코드]의 [표 HTTP 상태코드와 의미]와 같습니다.

예외 처리

운영자는 웹사이트의 환경에 따라 Stealth Commanding의 탐지가 해당 웹페이지에 적합하지 않다고 판단될 경우 해당 웹페이지에 대하여 Stealth Commanding의 탐지를 예외 처리 할 수 있습니다. 탐지 예외 설정 방법은 [VIII.7탐지 예외 설정 변경]에서 볼 수 있습니다.

Suspicious Access

개요

웜이나 해킹 스크립트, 보안 스캔 툴과 같은 자동화된 공격 도구는 웹 브라우저와는 달리 HTTP 규약의 모든 내용을 다 제대로 처리하지 못합니다. 또한 웜의 경우에는 확산 시 단시간 내에 대량의 접속 시도가 발생합니다. Suspicious Access 규칙은 이와 같은 자동화된 공격 도구의 특성을 판단하여 정상적인 웹 브라우저가 아닌 클라이언트의 접속을 차단하거나 접근을 제한할 수 있습니다.

웜이나 자동화 된 도구 사용 공격을 탐지하기 위한 수단입니다.

대응 방안

같이 4개의 탐지 모드를 제공합니다.

Suspicious Access 탐지 모드

| 모드 | 설명 |
|-----------|---|
| [1차 수준] | User-Agent 필드가 없는 경우 탐지합니다. User-Agent 필드의 내용이 search bot 이름이면 통과 Accept 필드가 있을 경우 다음을 검사하여 맞으면 통과합니다. From 필드가 있을 경우 그 내용이 "msn(at)microsoft.com", "googlebot(at)googlebot.com", "nhnbot@naver.com"이면 통과 Client IP가 Search Bot Ip일 경우 통과 요청 URI의 확장자가 이미지일 경우 통과 Gif, jpg, jpeg, bmp, png등 요청 URI의 확장자가 동영상일 경우 통과 Avi, mpg, mpeg, mpe, wmv, asf, flv, rm, mov Request의 Parameter가 없으면 통과 |
| [2차 수준] | User-Agent 필드가 없는 경우 탐지합니다 User-Agent 필드의 내용이 search bot 이름이면 통과 Client IP가 Search Bot Ip일 경우 통과 |
| [사용자 정의] | 다음과 같은 통과 조건을 on/off 함으로써 통과조건을 변경이 가능합니다. User-Agent 필드가 없는 경우 탐지합니다. User-Agent 필드의 내용이 search bot 이름이면 통과 Accept 필드가 있을 경우 다음을 검사하여 맞으면 통과합니다. From 필드가 있을 경우 그 내용이 ["msn(at)microsoft.com", "googlebot(at)googlebot.com", "nhnbot@naver.com"]이면 통과 Client IP가 Search Bot Ip일 경우 통과 요청 URI의 확장자가 이미지일 경우 통과 Gif, jpg, jpeg, bmp, png등 요청 URI의 확장자가 동영상일 경우 통과 Avi, mpg, mpeg, mpe, wmv, asf, flv, rm, mov Request의 Parameter가 없으면 통과 Request의 Referer 필드가 존재할 경우 통과(대부분의 웹 브라우저는 히스토리로 Referer을 사용) Request의 Cookie가 존재만 해도 통과 |
| [탐지하지 않음] | 해당 룰을 탐지하지 않습니다. |

웹 서버나 웹 애플리케이션에서 필터링을 해야 합니다.

해당 룰에 대한 대응은 운영자가 결정하지 않고 WAF에서 이상 징후가 발견되면 자동으로 차단합니다.

Suspicious Access 탐지 룰은 일반적인 웹 브라우저 대신 특수 웹 클라이언트를 사용하는 경우도 탐지할 가능성이 있습니다. 또한 웹 검색 사이트에서 페이지 정보를 모으기 위하여 사용하는 로봇도 탐지/차단될 수 있습니다.

예외 처리

운영자는 웹사이트의 환경에 따라 Suspicious Access의 탐지가 해당 웹페이지에 적합하지 않다고 판단될 경우 해당 웹페이지에 대하여 Suspicious Access의 탐지를 예외 처리 할 수 있습니다. 탐지 예외 설정 방법은 [VIII.7 탐지 예외 설정 변경]에서 볼 수 있습니다.

Unicode Directory Traversal

개요

웹 애플리케이션의 특정 인자로 개발자가 예상치 못한 디렉터리나 파일을 지정하여, 해당 파일이나 디렉터리의 내용을 살펴볼 수 있는 공격 기법입니다. 관리자의 ID와 패스워드, DBMS 서버 접속에 사용되는 정보, 소스 파일 등 서버의 주요 정보가 노출될 수 있습니다.

공격 예

IIS의 버그를 사용하여 시스템 디렉터리에 접근하는 공격입니다. 이는 /를 UTF-8의 확장 영역으로 억지로 할당하여 사용하고 있습니다. 아래의 탐지된 예는 시스템의 cmd 명령을 수행 하려 하고 있습니다.



대응 방안

웹 서버나 웹 애플리케이션에서 필터링을 수행해야 합니다.

WAF에서는 위의 Unicode Directory Traversal 공격에 대한 대응 방안으로 아래 표와 같이 2개의 탐지 모드를 제 공합니다.

Unicode Directory Traversal 탐지 모드

| 모드 | 설명 |
|-----------|--|
| [일반설정] | 유니코드 인코딩 특성을 이용하여 불법적으로 디렉토리를 이동하려는 행위를 탐지합니다. |
| [탐지하지 않음] | 해당 룰을 탐지하지 않습니다 |

위 탐지 모드에 의해 Unicode Directory Traversal 공격의 탐지가 일어났을 때 아래 표의 4가지 대응방법 중 하나를 선택하여 대응할 수 있습니다.

대응 설정 항목

| 모드 | 설명 |
|--------------|---|
| 연결 끊기 | HTTP 연결을 강제 종료 합니다. |
| 에러 코드 보냄 | HTTP의 상태 코드를 응답합니다. 일반적으로 요구 메시지가 잘못된 형식으로 구성 되어 있거나 제대로 처리할 수 없는 경우 등의 코드를 보냅니다. |
| 다른 웹 페이지로 이동 | 준비된 에러처리 웹 페이지로 이동합니다. |
| 차단하지 않음 | 탐지로그에 기록은 남으나 웹 서버로 전달하는 것은 허용합니다. 차단을 원치 않는 경우에 사용합니다. |

대응 모드 중 [에러 코드 보냄] 설정 시 선택 가능한 HTTP 상태 코드 및 의미는 [XI.4 에러처리 상태코드]의 [표 HTTP 상태코드와 의미]와 같습니다.

예외 처리

운영자는 웹사이트의 환경에 따라 Unicode Directory Traversal의 탐지가 해당 웹페이지에 적합하지 않다고 판단될 경우 해당 웹페이지에 대하여 Unicode Directory Traversal의 탐지를 예외 처리 할 수 있습니다. 탐지 예외 설정 방법은 [VIII.7탐지 예외 설정 변경]에서 볼 수 있습니다.

URI Access Control

개요

강제 접근(Forceful Browsing)은, 관리자 페이지 등 중요한 페이지에 인증이 설정되어 있는 경우, 관리자 게시물 쓰기 URL 이나 관리자 게시물 지우기 URL 등 관리자 페이지의 다른 메뉴로 강제 접속하여 인증을 우회하고 관리자 권한을 획득하는 공격 기법입니다.

대응 방안

WAF에서는 이와 같은 강제 접근 공격을 막을 뿐만 아니라, 허용된 접근만을 허용하는 Positive Security Model 을 제공함으로써 각종 웜의 확산이나 정보 수집 시도 등을 사전에 차단할 수 있습니다.

URI Access Control를 사용하기 전에 웹사이트가 가지고 있는 모든 페이지를 URI 접근 제어 목록에 등록 해야 합니다. 만약 URI 목록에 등록하지 않고 URI Access Control의 보안도를 탐지함으로 선택했다면, 웹사이트자의 모든 요청이 불법으로 간주되어 탐지됩니다.

URI 접근 제어 목록에 URI를 추가하기 위해 수동으로 등록하는 방법과 자동으로 등록하는 방법이 있습니다. 수동 등록 방법은 [URI 접근제어 목록 관리]기능에서 URI를 입력하고 추가하는 방법과, 관리자 편의를 제공하기 위해 등록된 신뢰 IP를 통한 웹페이지 요청인 경우와 탐지로그의 [로그 검토]를 통하여 URI 접근 제어 목록에 자동으로 추가하는 URI 학습기능을 제공합니다. 수동 등록방법은 [VIII.8 URI 접근 제어 목록 편집]을 [신뢰 IP]등록은 [VIII.4 웹사이트 추가 및 수정]에서 볼 수 있고, 탐지로그의 [로그 검토]기능은 [V.4 검색된 로그를 검토하기]에서 볼 수 있습니다.

WAF에서는 위의 URI Access Control 공격에 대한 대응 방안으로 아래 표와 같이 5개의 탐지 모드를 제공합니다.

URI Access Control 탐지 모드

| 모드 | | 설명 |
|-------------|------|---|
| [탐지함, 학습안함] | | URI 접근 제어 목록의 학습이 완료 된 후 웹 사이트에 페이지가 추가되거나 삭제되지 않을 때 사용합니다. |
| [탐지함, 학습함] | | URI 접근 제어 목록을 생성하기 위해 학습하면서 탐지도 할 때 사용합니다. 웹사이트에 등록된 신뢰 IP에서 요청된 웹페이지만을 학습합니다. |
| [탐지안함, 학습함] | | URI 접근 제어 목록을 생성하기 위해 학습만 할 때 사용합니다. 웹사이트에 등록된 신뢰 IP에서 요청된 웹 페이지만을 학습합니다. |
| 사용자정의 | 학습조건 | [학습] 항목은 학습을 수행 할지 여부를 True/False 값으로 설정합니다. [학습] 기능이 True로 되어 있을 때만, [레퍼러], [신뢰IP], [올바른 브라우저] 항목의 설정 값이 의미가 있습니다. [레퍼러] 항목은 접근 허용된 URI를 통해 연결된 경우 학습할지 여부를 True/False 값으로 설정합니다. [신뢰 IP] 항목은 신뢰 IP에서 요청된 페이지인 경우 학습할지 여부를 True/ False 값으로 설정합니다. [올바른 브라우저] 항목은 브라우저를 통하여 접속된 페이지인 경우만 학습할지 여부를 True/False 값으로 설정합니다. |
| | 탐지여부 | 학습되지 않은 페이지로 접속을 시도할 때 탐지 여부를 True/False 값으로 설정합니다. |
| [탐지하지 않음] | | 해당 룰을 탐지하지 않습니다. |

WAF에서는 접근 허용할 URI를 미리 등록하고 이외의 모든 접근을 탐지 차단합니다. 이는 학습 기간을 거쳐 접근 허용할 URI를 등록한 후에 탐지 정책을 적용하기 때문에 웹 페이지의 변경이나 추가가 있을 때에도 학습이 필요합니다. 학습된 URI 이외에는 모두 탐지 차단하기 때문에 업로드 디렉토리와 같이 수시로 바뀌는 페이지는 미리 예외 처리를 하는 것이 좋습니다.

위 탐지 모드에 의해 URI Access Control이 일어났을 때 아래 표의 4가지 대응방법 중 하나를 선택하여 대응할 수 있습니다.

대응 설정 항목

| | |
|--|--|
| | |
|--|--|

| 모드 | 설명 |
|--------------|---|
| 연결 끊기 | HTTP 연결을 강제 종료 합니다. |
| 에러 코드 보냄 | HTTP의 상태 코드를 응답합니다. 일반적으로 요구 메시지가 잘못된 형식으로 구성 되어 있거나 제대로 처리할 수 없는 경우 등의 코드를 보냅니다. |
| 다른 웹 페이지로 이동 | 준비된 에러처리 웹 페이지로 이동합니다. |
| 차단하지 않음 | 탐지로그에 기록은 남으나 웹 서버로 전달하는 것은 허용합니다. 차단을 원치 않는 경우에 사용합니다. |

대응 모드 중 [에러 코드 보냄]설정 시 선택 가능한 HTTP 상태 코드 및 의미는 [XI.4 에러처리 상태코드]의 [표 HTTP 상태코드와 의미]와 같습니다.

예외 처리

운영자는 웹사이트의 환경에 따라 URI Access Control의 탐지가 해당 웹페이지에 적합하지 않다고 판단될 경우 해당 웹페이지에 대하여 URI Access Control의 탐지를 예외 처리 할 수 있습니다. 탐지 예외 설정 방법은 [VIII.7 탐지 예외 설정 변경]에서 볼 수 있습니다.

User Defined Pattern

개요

User defined Pattern 은 사용자의 특수한 상황에 알맞은 조건을 임의로 추가 할 수 있는 패턴 기반의 룰입니다.

운영설정의 패턴 저장소에 저장된 패턴에 한해서 적용할수 있으며, Black List 방식으로 설정된 패턴과 일치하는 값이 해당 탐지 위치에서 발견되면 탐지합니다.

대응 방안

탐지 모드는 사용자 정의만 제공합니다. [사용자 정의 편집하기] 에 들어가면, 아래그림처럼 패턴 저장소에 저장되어 있는 패턴들을 확인할 수 있습니다.

각 패턴을 더블 클릭하면 패턴의 탐지 위치, 탐지 Key, 탐지 문자열(패턴)등의 상세 정보를 알 수 있습니다.

패턴의 상세 정보에서 보여지는 탐지 위치, Key, 탐지 패턴에 대한 간략한 정보는 [표 패턴 정보]를 통해 알수 있으며, 필요시에는 HTTP RFC를 참조하여 자세한 정보를 얻을수 있습니다.

User defined Pattern에서는 패턴 저장소에 저장된 패턴에 한해서 적용할 수 있으며, [표 탐지 위치에 따른 분류]에서 명시하였듯 HTTP Request Message의 위치에서 탐지합니다.



User Defined Pattern

User Defined Pattern Rule :

패턴

| 탐지위치 | 탐지 패턴 | Key |
|-------|----------|-----------|
| URI | hello | 모든 key 검사 |
| PARAM | variable | Cookie |
| | | |

Regex

Regex

Regex Key

화면전환

URI Access Control 탐지 모드

| 패턴 | 설명 |
|-------|--|
| 탐지위치 | URI 아래그림의 4번 부분 자원의 절대 경로입니다.예시) /pub/WWW/TheProject.html |
| | REQLINE 아래그림의 1번 부분 Request-Line = Method URI HTTP-Version으로 구성 예시) GET /pub/WWW/TheProject.html HTTP/1.1 |
| | PARAM 아래그림의 6번 파랑박스 부분 Parameter 는 다른 페이지로 값을 전달할 때 사용하는 변수로 "=" 수식 우측에 오는 부분입니다. |
| | REQHEADER 아래그림의 2번 부분 HTTP Request Header 부분 요구 및 클라이언트 자신에 관한 추가 정보를 클라이언트가 서버에게 전달할 수 있도록 합니다. |
| 탐지 패턴 | 탐지 하고자 하는 임의의 문자열 입니다. REQHEADER, REQCONTENT의 Value 부분 이거나 파라미터 등의 탐지위치에서 찾습니다.예시)아래그림의 6번 부분 |
| Key | Key는 "=" 수식 좌측에 오는 부분의 문자열입니다. 설정 하지 않으면, 모든 키에 대해 패턴 탐지됨.예시)아래그림의 5번 주황박스 부분 |



User defined Pattern는 탐지된 HTTP 요청 메시지를 아래 표의 4가지 대응방법 중 하나를 선택하여 대응 할 수 있습니다.

대응 설정 항목

| 모드 | 설명 |
|--------------|---|
| 연결 끊기 | HTTP 연결을 강제 종료 합니다. |
| 에러 코드 보냄 | HTTP의 상태 코드를 응답합니다. 일반적으로 요구 메시지가 잘못된 형식으로 구성 되어 있거나 제대로 처리할 수 없는 경우 등의 코드를 보냅니다. |
| 다른 웹 페이지로 이동 | 준비된 에러처리 웹 페이지로 이동합니다. |
| 차단하지 않음 | 탐지로그에 기록은 남으나 웹 서버로 전달하는 것은 허용합니다. 차단을 원치 않는 |

대응 모드 중 [에러 코드 보냄]설정 시 선택 가능한 HTTP 상태 코드 및 의미는 [XI.4 에러처리 상태코드]의 [표 HTTP 상태코드와 의미]와 같습니다.

예외 처리

운영자는 웹사이트의 환경에 따라 User defined Pattern의 탐지가 해당 웹페이지에 적합하지 않다고 판단될 경우 해당 웹페이지에 대하여 User defined Pattern의 탐지를 예외 처리 할 수 있습니다. 탐지 예외 설정 방법은 [VIII.7탐지 예외 설정 변경]에서 볼 수 있습니다.

Website Defacement

개요

많은 웹 공격자들은 웹사이트의 초기 페이지를 변조하여 자식의 주의, 주장을 알리는데 중점을 두고 있습니다. 이러한 웹 페이지의 변경을 탐지하여 변조된 페이지가 무수의 고객에게 노출되지 않도록 하거나 정상적 페이지로 복구하여 서비스할 수 있습니다.

대응 방안

Web Site Defacement 룰은 각 페이지에 포함된 특정 문자열로 변조여부를 검사하거나 페이지 전체를 등록하여 변조여부를 검사합니다. 변조된 웹 페이지로 판단된 웹 페이지는 미리 등록한 복구 페이지를 표시하여 서비스를 보완할 수도 있습니다.

Web Site Defacement 탐지 룰의 로그가 남았다면 정상적으로 페이지가 갱신되었는지 확인해 보아야 합니다. 만약 정상적인 페이지 변경으로 Web Site Defacement 탐지 로그가 남았다면 변경된 사항을 Web Site Defacement를 설정에 반영하여야 합니다.

정상적인 페이지 변경이 아니라면 이미 해킹을 당했다고 판단될 수 있습니다. 이러한 경우 웹 서버에 해당 페이지를 복구하고 웹 서버 및 주변 서버 등에 대한 보안 점검을 실시하여야 합니다.

변조 여부를 탐지할 페이지가 고정된 내용이 아닌 액티브페이지 (매 요청 시마다 다른 내용을 표시하는 페이지)인 경우 페이지 전체를 등록할 수 없습니다. 이러한 경우 모든 내용에 포함될 특정 문자열을 정하여 이를 등록해 주시기 바랍니다.

설정 방법

Web Site Defacement의 사용자 정의 설정에서 각 페이지의 변조여부 검사를 다음 그림과 같이 설정 할 수 있습니다.

웹 사이트/URI를 입력하고 탐지 방식을 패턴(특정 문자열)과 해쉬(페이지 전체)를 선택합니다. 해쉬를 선택한 경우 등록한 URI의 페이지를 파일로 저장하였다가 [비교 페이지] 버튼을 클릭하여 파일을 등록합니다. 만약 변조가 탐지된 경우 복구를 원하면 [복구]체크박스를 선택하고, [복구 페이지]버튼을 클릭하여 복구 페이지 파일을 등록합니다. 내용을 다 입력한 후 왼쪽 하단의 [추가]버튼을 클릭 하여 페이지가 등록합니다

위의 설정된 탐지 방법에 의해 Web Site Defacement가 일어났을 때 아래 표의 4가지 대응방법 중 하나를 선택하여 대응 할 수 있습니다.

대응 설정 항목

| 모드 | 설명 |
|--------------|---|
| 연결 끊기 | HTTP 연결을 강제 종료 합니다. |
| 에러 코드 보냄 | HTTP의 상태 코드를 응답합니다. 일반적으로 요구 메시지가 잘못된 형식으로 구성 되어 있거나 제대로 처리할 수 없는 경우 등의 코드를 보냅니다. |
| 다른 웹 페이지로 이동 | 준비된 에러처리 웹 페이지로 이동합니다. |
| 차단하지 않음 | 탐지로그에 기록은 남으나 웹 서버로 전달하는 것은 허용합니다. 차단을 원치 않는 경우에 사용합니다. |

대응 모드 중 [에러 코드 보냄]설정 시 선택 가능한 HTTP 상태 코드 및 의미는 [XI.4 에러처리 상태코드]의 [표 HTTP 상태코드와 의미]와 같습니다.

예외 처리

운영자는 웹사이트의 환경에 따라 Web Site Defacement 의 탐지가 해당 웹페이지에 적합하지 않다고 판단될 경우 해당 웹페이지에 대하여 Web Site Defacement 의 탐지를 예외 처리 할 수 있습니다. 탐지 예외 설정 방법은 [VIII.7탐지 예외 설정 변경]에서 볼 수 있습니다.

IP Block

개요

웹 환경에서는 무수히 많은 공격들이 시도되고 있으며 이러한 공격들은 대부분 자동화된 툴에 의해서 공격되는 것이 대부분 입니다.

이러한 악의적인 방법에는 특정 서버의 취약점을 찾아 접근을 시도하기도 하지만 반복적으로 접속을 시도할 수 있는 자동화된 툴을 이용하여 정상적인 접속방식으로 짧은 시간 안에 다수의 접속시도를 통해 웹 서버의 과부하를 유도하기도 합니다.

같은 공격이 자동으로 계속 발생하는 공격에 대한 탐지 룰입니다

공격 예

IP Block 설정은 탐지 룰이 아니라 탐지 결과를 바탕으로하는 운영 기능이기 때문에 [정책 설정 마법사]를 이용하여 설정하지 않고 [운영 설정 마법사]를 이용하여 설정합니다.

IP Block 은 동일한 출발지에서 지속적인 공격이 들어오는 것을 차단하기 위하여 정책설정에서 각 룰 마다 고유의 위험도를 미리 설정합니다.

동일한 출발지에서의 악의적인 접근에 대해 설정한 위험도 수치의 합이 관리자가 **[오류! 참조 원본을 찾을 수 없습니다. 오류! 참조 원본을 찾을 수 없습니다.]**에서 설정한 시간내에 위험도 최대값 이상이 되면 공격이 탐지되어 이 출발지로부터 웹서버로의 접근을 차단합니다.

[오류! 참조 원본을 찾을 수 없습니다. 오류! 참조 원본을 찾을 수 없습니다.]에서 설정한 사항이 **[오류! 참조 원본을 찾을 수 없습니다.]**과 같으며 그림처럼 SQL Injection 룰의 위험도를 60으로 설정한 경우, 동일한 IP에서 SQL Injection 공격이 두번 이상 시도되면 그합이 120으로 100을 초과하므로, 해당 IP를 차단하며 그림 같은 로그 정보를 확인할 수 있습니다.



IP Block 보안 경고 메시지

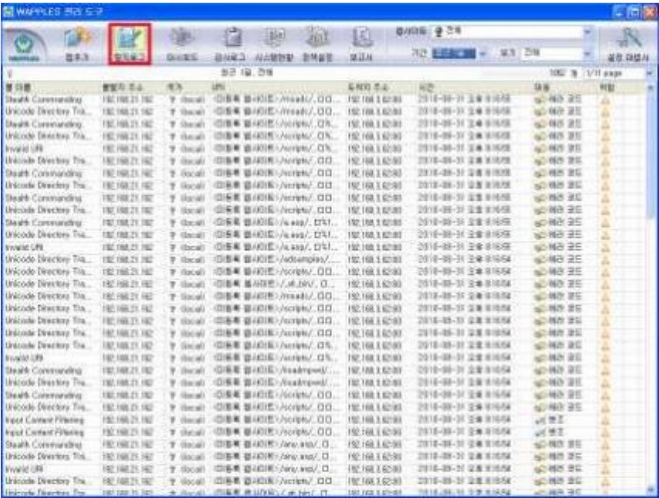
| 보안 경보 메시지 | 출력 원인 |
|-------------------------|---------------------|
| "IP BLOCK" 로그가 검색되었습니다. | IP Block 로그가 기록된 경우 |

대응 방안

IP Block 차단에 대한 규칙 설정 및 차단된 IP 관리에 대한 자세한 설명은 **[오류! 참조 원본을 찾을 수 없습니다. 오류! 참조 원본을 찾을 수 없습니다.]**절을 참고합니다.

탐지로그

탐지로그는 [IV탐지물의 이해]에서 정의한 탐지규칙에 따라 탐지한 룰과 위험한 행동을 한 대상자의 주소, 국가, 대상이 된 URL, 발생한 시각 등의 정보를 제공합니다. WAF 관리도구 툴 바에서 [탐지로그]를 클릭하면 탐지로그를 볼 수 있습니다.



탐지로그 화면은 크게 상단의 툴 바와 그 아래 대부분을 차지하고 있는 로그 목록 부분으로 나눌 수 있습니다. 툴 바의 [웹사이트], [기간] 및 [보기]는 로그의 목록을 검색할 때 사용됩니다. 로그 목록에서 직접 로그를 확인하거나 로그 관리를 위한 컨텍스트 메뉴를 호출 할 수 있습니다.

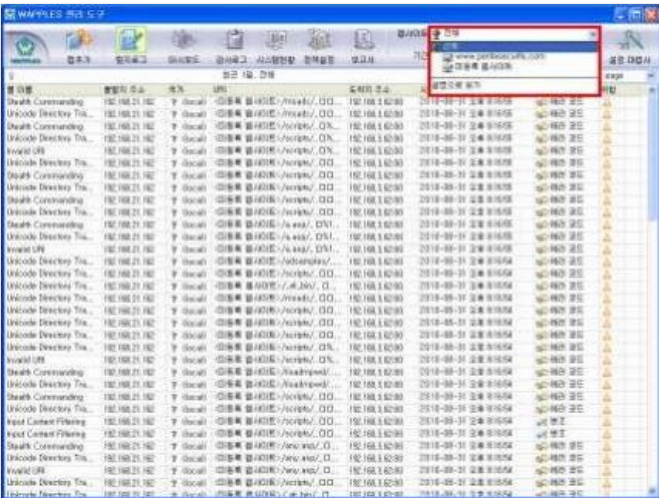
탐지로그는 한꺼번에 최대 10,000개까지 볼 수 있습니다

조회하기

탐지로그 툴은 조회할 로그 목록의 [웹사이트], [기간], [보기(필터)]를 자유롭게 선택하여 원하는 로그를 조회할 수 있는 기능을 제공합니다.

웹사이트 별 조회

웹사이트의 드롭다운 목록에서 검색을 원하는 웹사이트를 선택합니다. [전체]를 선택하면 등록되어 있는 모든 웹사이트가 검색 대상이 됩니다. 리스트 목록에서 [설명으로 보기], [이름으로 보기]항목을 선택하면 웹 사이트의 리스트를 이름과 설명으로 교차 하여 볼 수 있습니다. 웹사이트 이름과 설명의 등록은 [IX.2.2 웹 서버 추가/수정]에서 볼 수 있습니다.



기간 별로 조회

로그 목록을 기간으로 조회할 수 있습니다. 기간 선택 메뉴는 기본적으로 제공되는 시간과 사용자가 정의할 수 있는 시간으로 나누어집니다. 기본적으로 [최근 5분 간], [최근 1시간 간], [최근 1일간], [최근 1주일 간], [1개월 간]부터 현재까지 기간을 선택할 수 있고, [사용자 정의...]를 선택하면 더 자세한 설정이 가능합니다.

[illegible]

시작 시간과 종료 시간의 첫 번째 라디오 버튼의 사용자 입력은 숫자 이외의 문자는 입력이 불가능하고 숫자는 최대 1000이며 입력 값이 1000 이 넘으면 1000으로 간주하게 됩니다.

기간 선택

부터

☐ 일 전

☒ 2010년 8월 31일 화요일

오전 12:00:00

~

까지

☒ 1 시간 후

☐ 2010년 8월 31일 화요일

오후 11:59:59

☐ 현재

기간 : 2010-08-31 부터 1시간간

확인 취소

기간 선택 오류 메시지

| 오류 메시지 | 출력 원인 |
|-----------------|---|
| 입력 값에 오류가 있습니다. | 시간 입력 시 검색 시작 시간이 검색 종료 시간보다 미래의 시간을 설정하였을 경우 |

숨긴 로그 포함여부

위 필터 항목 중 자주 사용하는 필터 조건 중 전체, 전체(숨긴 로그포함), 각 룰별 로그보기는 기본 필터로 제공하고 그 이외에 관리자가 [사용자정의...] 항목을 이용하여 조건을 구성할 수 있습니다.

[illegible]

로그 필터에서는 [출발지 주소], [URI], [국가], [롤 이름], [기타]의 항목이 있으며, 각각의 설정을 AND 조합하여 모두 반영할 수 있습니다. [출발지 주소], [URI], [국가], [롤 이름] 태그에서는 [필터링 하지 않음], [입력(선택)한 것만 보여줌], [입력(선택) 이외의 것만 보여줌]으로 선택 할 수 있습니다. [필터링 하지 않음]을 선택하면 해당 항목은 필터링 되지 않습니다.

로그 필터 선택

출발지 주소: URI | 국가 | 콜 이름 | 기타

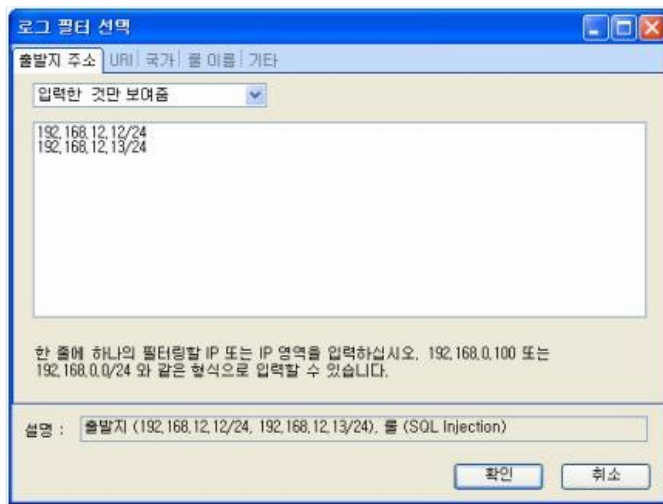
필터링 하지 않음

한 줄에 하나의 필터링할 IP 또는 IP 영역을 입력하십시오. 192.168.0.100 또는 192.168.0.0/24 와 같은 형식으로 입력할 수 있습니다.

내용: (SQL Injection)

확인 취소

잘못된 IP형식일 경우 오류 상황을 설명 부분에 표시하고 [확인]을 클릭했을 때 오류 메시지를 출력하게 됩니다. 정해진 형식과 다른 형식으로 입력한 경우에는 아래쪽 [설명] 영역에 오류 메시지가 출력됩니다. 또한 이때 [확인] 버튼을 클릭하면 입력 값 오류에 대한 상세 메시지 창이 나타납니다.

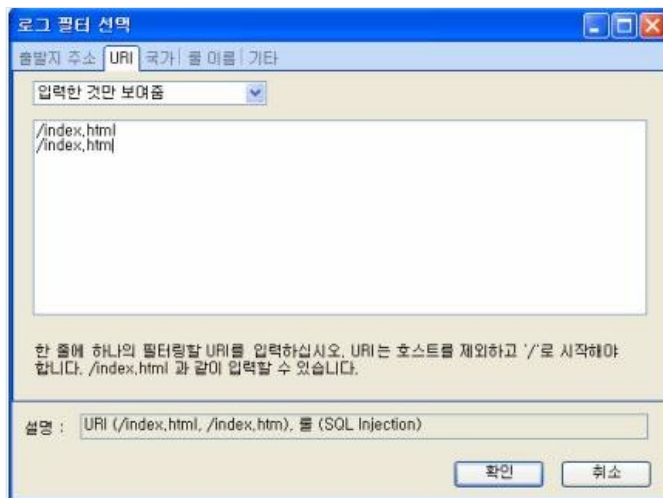


로그 필터 선택 화면에서는 출발지 주소와 URI 설정 시 사용자 입력 값에 대하여 오류가 있을 경우 다음과 같은 오류 메시지를 출력합니다

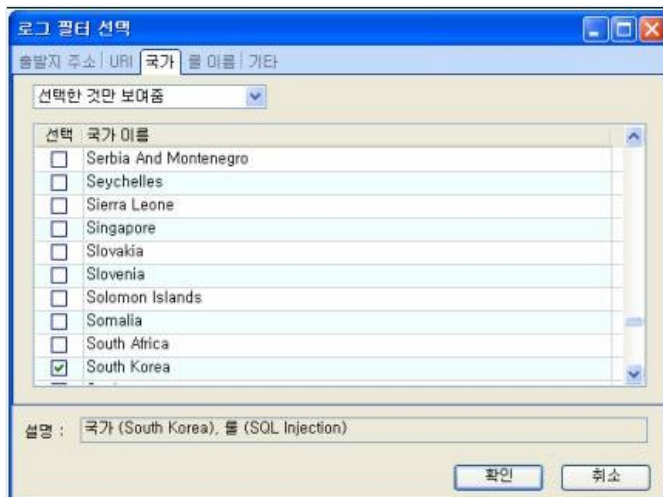
로그 필터 선택 화면 오류 메시지

| 오류 메시지 | 출력 원인 |
|-----------------|--------------------------|
| 입력 값에 오류가 있습니다. | 입력된 출발지 주소가 IP 형식이 아닐 경우 |
| 입력 값에 오류가 있습니다. | 입력된 URI가 "/"로 시작하지 않을 경우 |

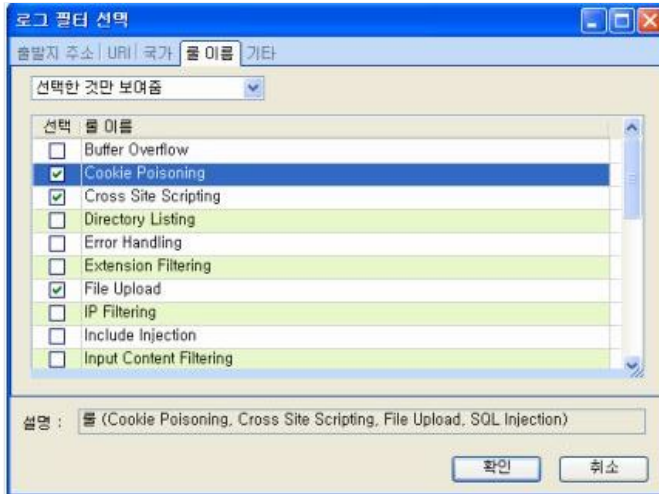
[URI]로 필터링 방법도 [출발지 주소]와 같은 방식으로 입력합니다.



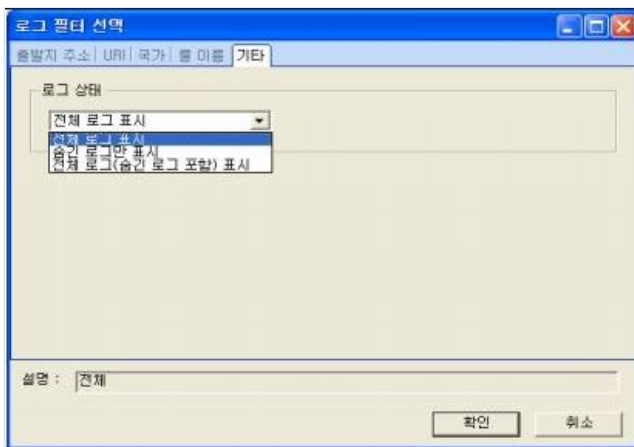
[국가] 필터도 [출발지 주소]와 같은 방식으로 입력합니다.



[룰 이름] 필터도 [출발지 주소]와 같은 방식으로 입력합니다.

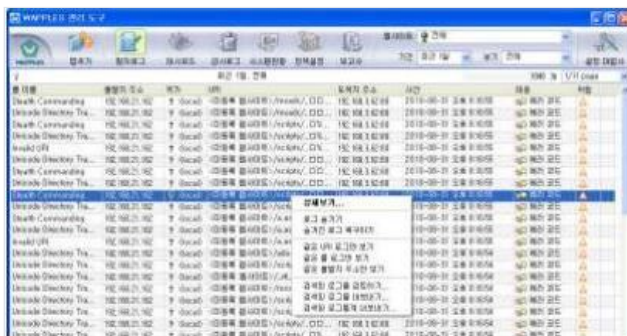


[기타]에서 전체 로그와 숨긴 로그만 표시 여부를 선택 할 수 있습니다



빠른 조회 기능

탐지로그의 조회는 필터를 이용하는 방식 이외에 검색된 로그에서 마우스 오른쪽 버튼을 클릭하여 [같은 URI 로 그만 보기], [같은 룰 로그만 보기], [같은 출발지 주소 만 보기] 기능을 제공합니다. 이를 사용하여 연관이 있는 탐지로그들을 한번에 모아볼 수 있습니다.



조회 결과 확인

로그 조회 조건에 따라 조회된 결과인 탐지 로그의 룰 이름, 주소, 국가, URL, 시간 정보를 WAF 메인 화면에 표시합니다. 조회된 목록의 개수는 우측 상단에 표시되며 한 페이지에 100개의 목록이 표시되고 우측 상단의 페이지 목록으로 조회 할 수 있습니다.

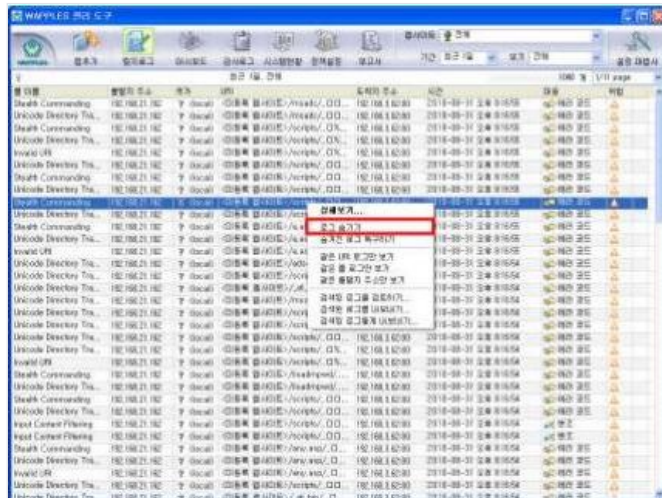
페이지 목록은 100페이지 단위로 표시되고 페이지 목록 최 하단의 [다음 페이지], [이전 페이지] 항목을 클릭하면 100페이지 단위로 페이지 목록이 갱신됩니다.

탐지로그는 10초 단위로 재 검색하여 결과 화면을 갱신합니다.

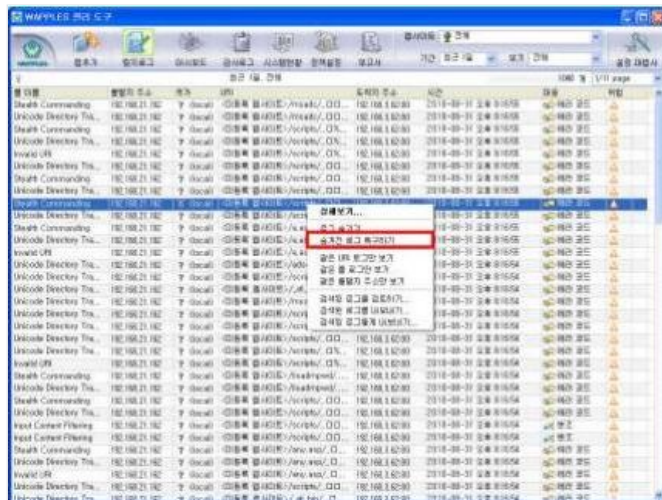
로그 숨기기/복구하기

로그 숨기기 기능은 탐지된 로그에서 사용자가 화면에서 배제하고 싶은 로그를 필터링하고 싶을 때 유용하게 쓰일 수 있습니다.

검색된 로그에서 마우스 오른쪽 버튼을 클릭하여 컨텍스트 메뉴를 호출한 후 [로그 숨기기]를 클릭하면 선택된 로그가 화면에서 숨겨집니다. 이는 로그가 완전히 삭제되는 것을 의미하지 않습니다.



[로그 숨기기]로 숨겨진 로그는 톨 바의 [보기]에서 "전체(숨긴 로그 포함)"필터의 설정으로 다시 보는 것이 가능하며 숨겨진 로그는 휴지통 아이콘이 나타나게 됩니다. 숨겨진 로그를 선택한 후 마우스 오른쪽 버튼을 클릭하여 [숨겨진 로그 복구하기]를 클릭하면 숨겨진 로그를 복구 할 수 있습니다.



검색된 로그를 검토하기

[검색된 로그를 검토하기]기능은 검색된 로그를 이용하여 [탐지 예외 설정 목록]에 URI를 등록하고 등록된 URI는 탐지로그에서 검색되지 않게 [로그 숨기기]의 기능을 순차적으로 진행하는 마법사입니다. URI Access Control에 의해 탐지된 URI는 [URI 접근 제어 목록]에 URI를 등록하는 절차가 하나 추가됩니다. 로그를 검토하여 룰 별로 관리자가 안전하다고 판단 되는 URI를 선택하여 [탐지예외설정] 및 [URI 접근 제어 목록]추가를 합니다.

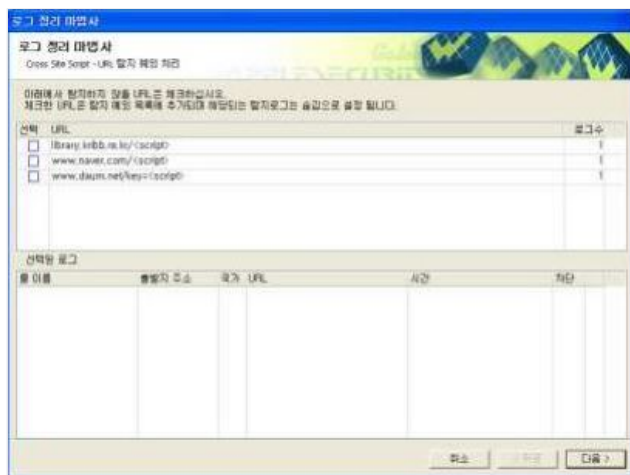
검색된 로그에서 오른쪽 마우스 버튼을 클릭 후 [검색된 로그를 검토하기...]를 선택하면 아래와 같은 창이 나타납니다.

아래그림은 Cross Site Script룰에 의해 탐지된 URI를 [탐지 예외 설정 목록]에 추가할지 여부를 관리자에게 물어보는 화면입니다.

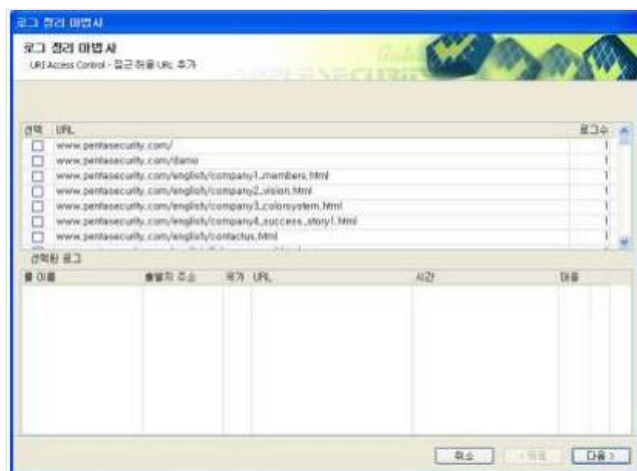
화면의 위쪽에 있는 리스트는 탐지된 로그의 중복된 URI를 제거하고 유일한 URI목록을 표시합니다. 화면 하단의 리스트는 위쪽의 유일한 URI목록에서 하나를 선택하면 해당 URI를 갖는 모든 탐지로그가 표시됩니다.

탐지예외 처리하고자 하는 URI의 체크박스를 체크한 후 [다음]버튼을 클릭합니다.

검색된 탐지로그에 다른 룰이 있으면 이를 반복합니다.



URI Access Control를 [탐지 예외 설정]과 추가로 [URI 접근 제어 목록]에 대상 URI의 추가 여부를 관리자에게 물어봅니다.



모든 설정이 완료된 선택된 URI의 탐지 로그들은 숨긴 로그로 처리됩니다.

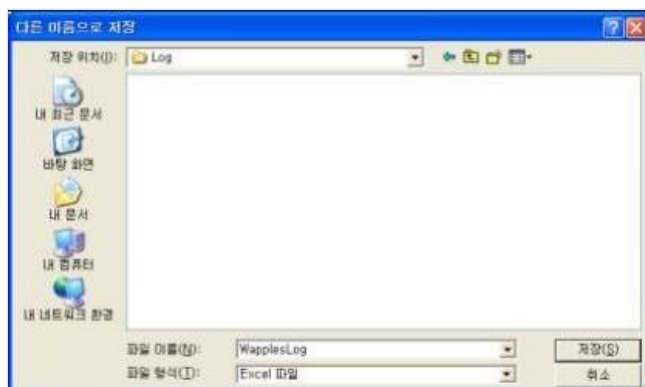
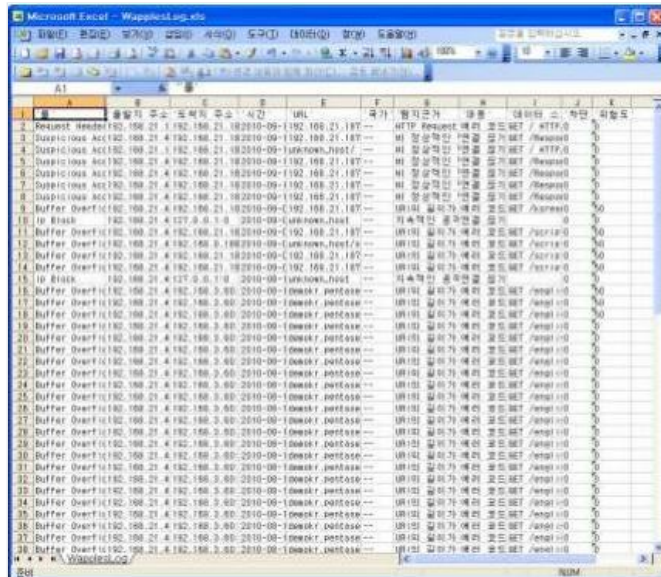


검색된 로그를 내보내기

로그 내보내기 기능은 검색된 로그를 MS-Excel 파일로 저장하여 WAF 외부에서 조회를 가능하게 합니다.

검색된 로그에서 마우스 오른쪽 버튼을 클릭하여 [검색된 로그를 내보내기...]를 클릭하면 아래와 같이 저장할 파일 이름 선택 창이 나타납니다.

저장하려는 파일명과 같은 파일이 이미 존재하는 경우 파일을 덮어쓸지 물어보며 저장하려는 파일명으로 폴더에 저장할 수 없는 경우 오류 메시지를 출력하고 다시 입력하게 합니다.



Microsoft Excel - WappesLogStat.xls

요약 보고서

모든 웹사이트: 총 3778개의 탐지로그

종별 TOP 10

| 순위 | 종 | 탐지 횟수 |
|----|--------------------------|-------|
| 1 | Cross Site Scripting | 1594 |
| 2 | Extension Filtering | 959 |
| 3 | SQL Injection | 561 |
| 4 | Stealth Commanding | 478 |
| 5 | Privacy Output Filtering | 125 |
| 6 | Request Method Filtering | 32 |
| 7 | Buffer Overflow | 21 |
| 8 | Error Handling | 4 |
| 9 | Invalid HTTP | 2 |
| 10 | Parameter Tampering | 2 |

국가별 TOP 10

| 순위 | 국가 | 탐지 횟수 |
|----|---------|-------|
| 1 | Unknown | 3778 |

출발지 IP별 TOP 10

| 순위 | 출발지 주소 | 탐지 횟수 |
|----|---------------|-------|
| 1 | 192.168.1.202 | 3725 |
| 2 | 192.168.0.45 | 53 |

URI별 TOP 10

| 순위 | URI | 탐지 횟수 |
|----|---|-------|
| 1 | demokr.pentasecurity.com/board/zero/zboard.php | 175 |
| 2 | demokr.pentasecurity.com/board/zero/write.php | 46 |
| 3 | demokr.pentasecurity.com/board/login_chk.php | 39 |
| 4 | demokr.pentasecurity.com/index.php | 35 |
| 5 | demokr.pentasecurity.com/board/zero/write_ok.php | 25 |
| 6 | demokr.pentasecurity.com/board/zero/login.php | 23 |
| 7 | demokr.pentasecurity.com/board/zero/login_check.php | 19 |
| 8 | demokr.pentasecurity.com/board/zero/comment_ok.php | 18 |

대시보드

WAF의 대시보드는 트래픽 및 탐지된 로그에 관련한 정보를 차트 형태로 보여줍니다. 대시보드는 10초 단위로 탐지로그 정보를 재 분석하여 결과 화면을 갱신합니다.

대시보드에서 보여주는 데이터의 종류는 다음과 같습니다.

대시보드 종류

| | |
|--------|--|
| 트래픽 | WAF를 통하여 전송된 데이터의 시간당 분포를 보여줍니다. (Mbytes/초) |
| 페이지 히트 | WAF에 요청된 HTTP Request Message의 시간당 분포를 보여줍니다. (Page hit/초) |

대시보드에서는 데이터를 조회하고자 하는 대상 웹사이트, 기간, 보기 항목으로 이용하여 데이터의 종류와 차트의 타입을 선택할 수 있습니다.

관리도구 툴 바에서 [대시보드]를 클릭하면 대시보드를 볼 수 있습니다.



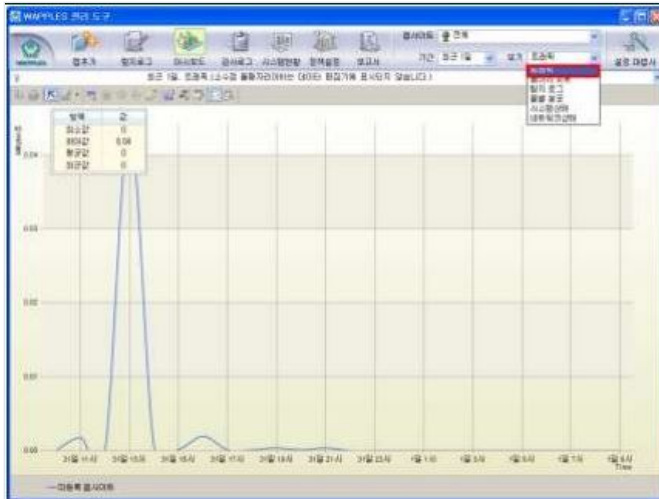
웹사이트 및 기간별 조회하기

웹사이트 및 기간별 조회하기는 탐지로그의 조회 기능과 동일합니다. 자세한 설명은 [V.1.1웹사이트 별 조회], [V.1.2기간 별로 조회]에서 볼 수 있습니다.

데이터 종류별 조회

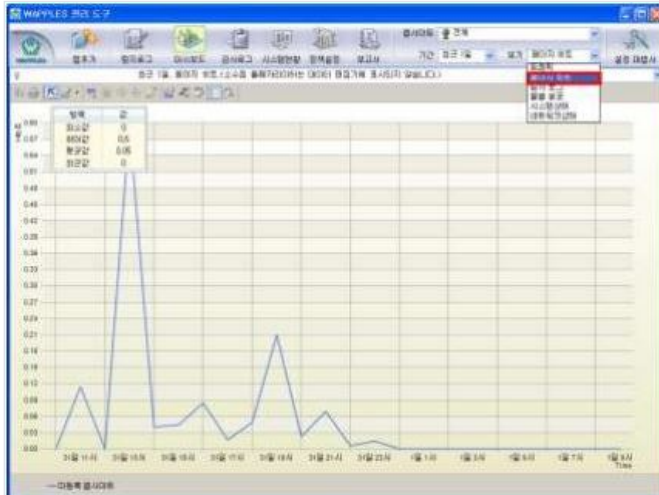
트래픽

트래픽 보기는 WAF을 통하여 전송된 데이터의 시간당 분포(MBytes/초)를 가로의 시간 축과 세로축의 트래픽으로 변화 추이를 보여줍니다. 툴 바의 [보기] 메뉴에서 [트래픽]을 선택합니다.



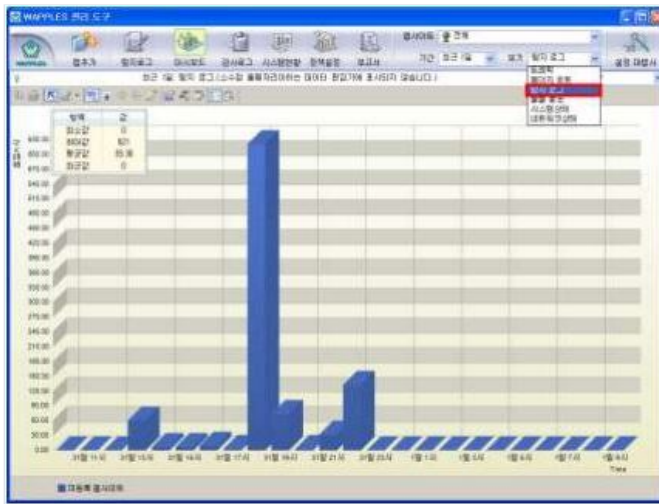
페이지 히트

WAF에 요청된 HTTP Request Message의 시간당 분포를 가로축에는 시간(가로축)을 세로축에는 히트 수(세로축)로 변화 추이를 보여줍니다. 툴 바의 [보기] 메뉴에서 [페이지 히트]를 선택합니다.



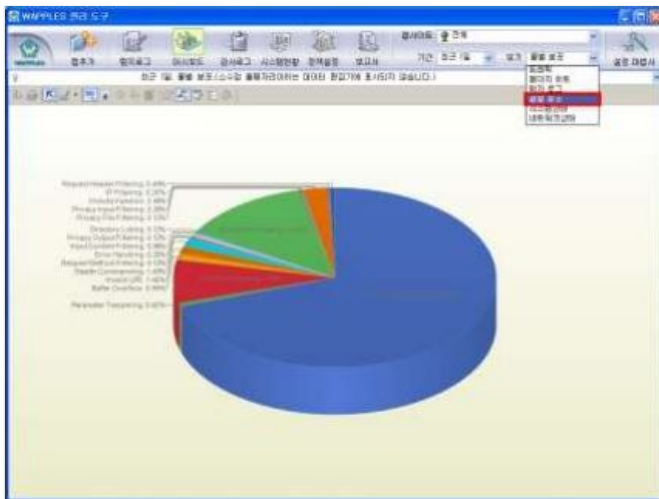
탐지 로그

탐지된 로그의 시간당 분포(로그개수/초)를 가로축에는 시간을 세로축에는 탐지(침입) 횟수의 변화 추이를 보여줍니다. 툴 바의 [보기] 메뉴에서 [탐지 로그]를 선택합니다.



로별 분포

선택한 기간 내의 탐지된 공격의 비율을 차트로 보여줍니다. 툴 바의 [보기]메뉴에서 [로 별 분포]를 선택합니다.



시스템 상태

선택한 기간 내의 기록된 CPU 및 RAM 사용률을 차트로 보여줍니다. 툴 바의 [보기]메뉴에서 [시스템상태]를 선택합니다.

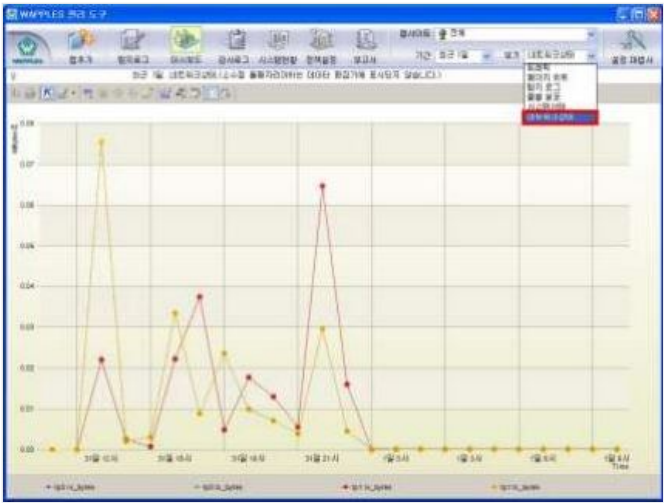
시스템 상태는 과거 2주간의 데이터에 한하여 조회 가능하며 2주 이상의 기간 조회는 지원하지 않습니다.



네트워크 상태

선택한 기간 내의 기록된 서비스 포트의 네트워크 상태(rx_bytes, rx_packets, rx_errors, rx_dropped, rx_fifo_errors, rx_frame_errors, rx_compressed, rx_multicast, tx_bytes, tx_packets, tx_errors, tx_dropped, tx_fifo_errors, tx_carrier_errors, tx_compressed, collisions)를 차트로 보여줍니다. 톨 바의 [보기]메뉴에서 [네트워크상태]를 선택합니다.

네트워크 상태는 과거 2주간의 데이터에 한하여 조회 가능하며 2주 이상의 기간 조회는 지원하지 않습니다.



대시보드 부가 기능

대시보드는 탐지로그를 관리자가 이해하기 쉽게 그래픽으로 분석하여 보여주는 기능으로 그래픽 속성을 관리자가 자유 자제로 변경할 수 있도록 여러 가지 부가 기능을 제공합니다

차트 모양 선택

대시보드에서 제공하는 분석 자료는 다양한 형태의 차트 모양으로 선택하여 볼 수 있습니다.

데이터 종류별 가능한 차트 모양은 다음과 같습니다.

데이터 종류별 제공하는 차트 모양

| | |
|------------------|---|
| 트래픽 페이지 히트 탐지 로그 | Bar 2D Stack, Bar 2dSideBySide, Bar 3D Stack, Bar 3D SideBySide, Bar 3D Cluster, Step Line 2D, Step Line 3D Cluster, Line 2D, Line 3D Cluster, Curve 3D Cluster, Area 2D Stack, Area 3D Stack, Area 3D Cluster (Mbytes/초) |
| 로열 분포 | Pie 2D, Pie 2D Legend, Pie 3D, Pie 3D Legend, Doughnut 3D. Doughnut 3D. Radar r |

이 절에서는 각 차트 모양 별 예제 화면을 설명합니다.

Bar 2D Stack

등록되어 있는 웹사이트 별로 다른 색으로 쌓이기 때문에 전체 높이는 전체 트래픽과 같습니다.



Bar 2D SideBySide

웹사이트 별로 하나의 바가 그려집니다.



Bar 3D Stack

Bar 2D Stack 차트와 같은 모양에서 3D로 표현됩니다.



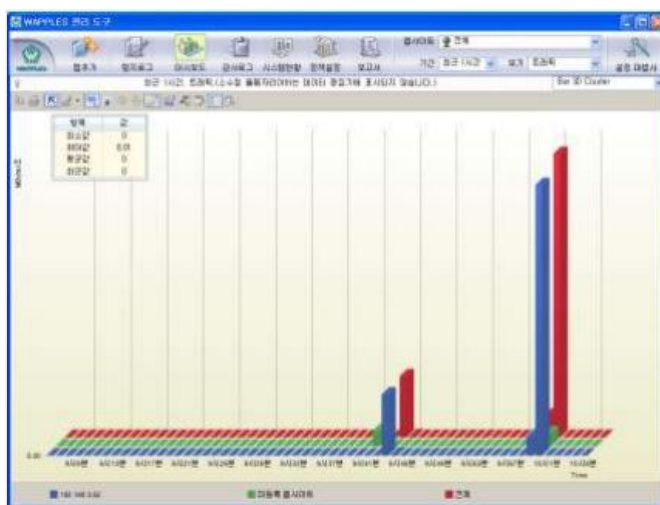
Bar 3D SideBySide

Bar 2D SideBySide 차트와 같은 모양에서 3D로 표현됩니다.



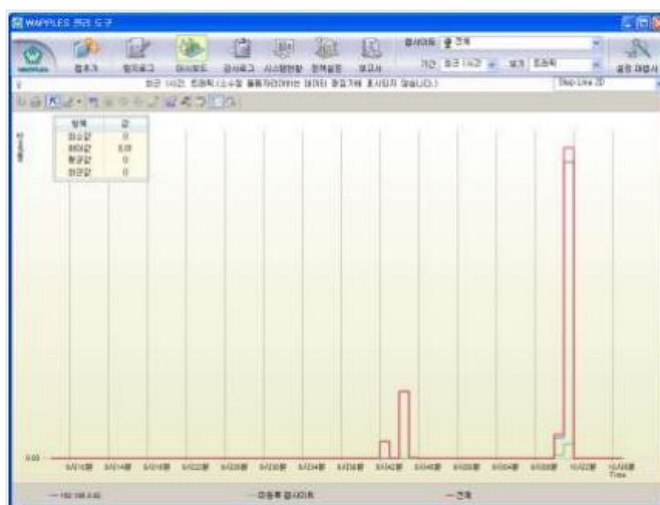
Bar 3D Cluster

웹사이트별로 앞뒤로 배치된 입체적인 바 차트입니다.



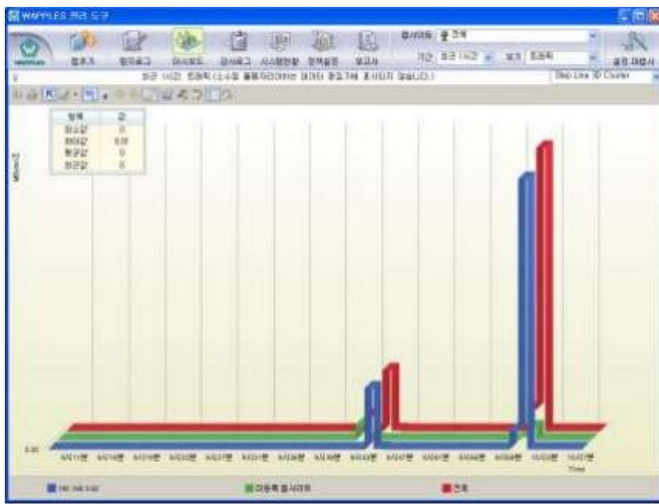
Step Line 2D

스텝 라인의 선 그래프입니다.



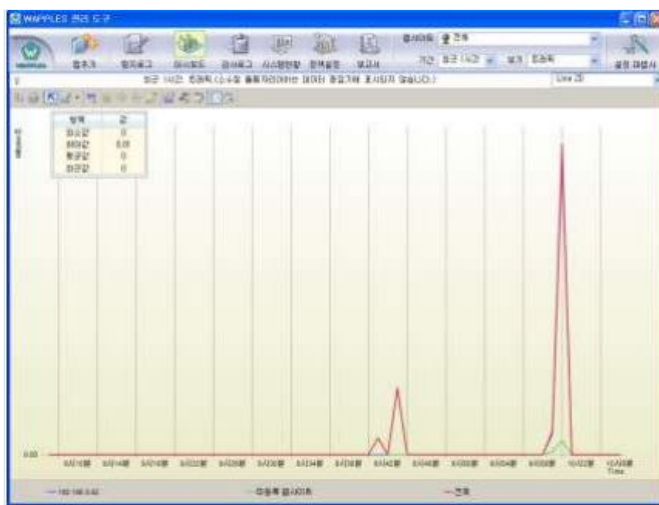
Step Line 3D Cluster

스텝 라인의 선 그래프를 웹사이트 별로 앞뒤로 배치된 입체적인 형태의 차트입니다.



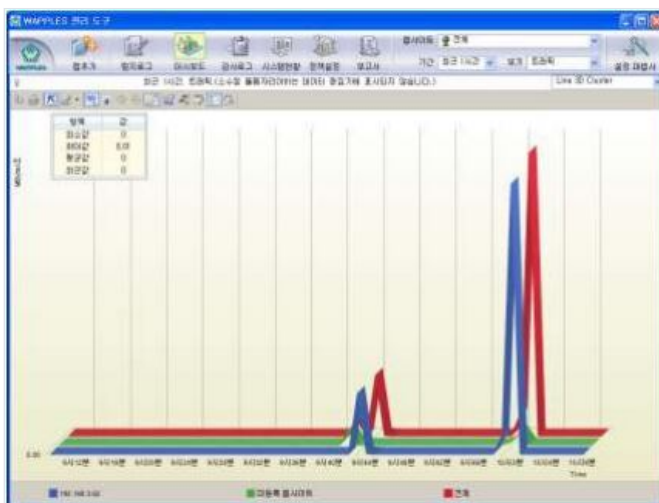
Line 2D

꺾은선 그래프로 구현된 차트입니다



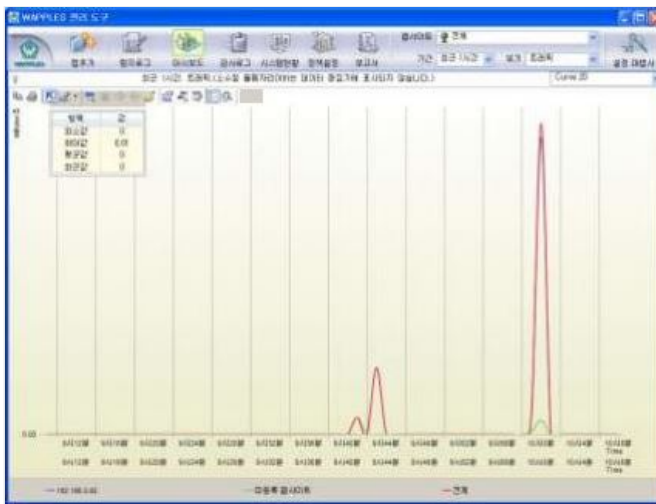
Line 3D Cluster

꺾은선 그래프를 웹사이트 별로 앞뒤로 배치한 입체적인 형태의 차트 입니다



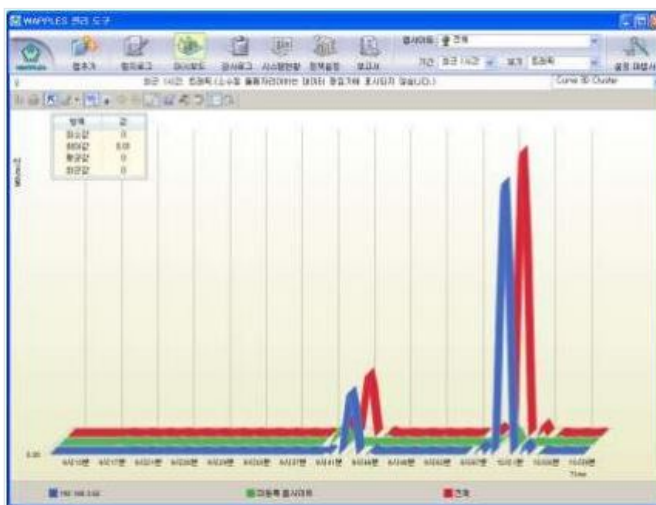
Curve 2D

꺾은선 그래프의 날카로운 부분을 둥글게 처리한 차트입니다.



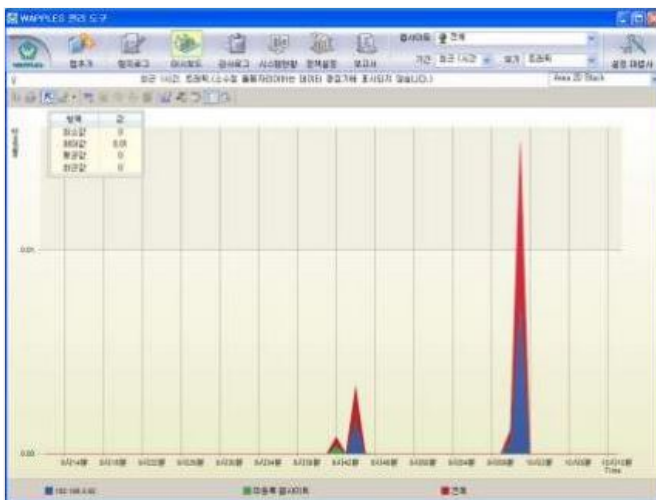
Curve 3D Cluster

Curve 2D 차트를 웹사이트 별로 앞뒤로 배치한 입체적인 형태의 차트입니다.



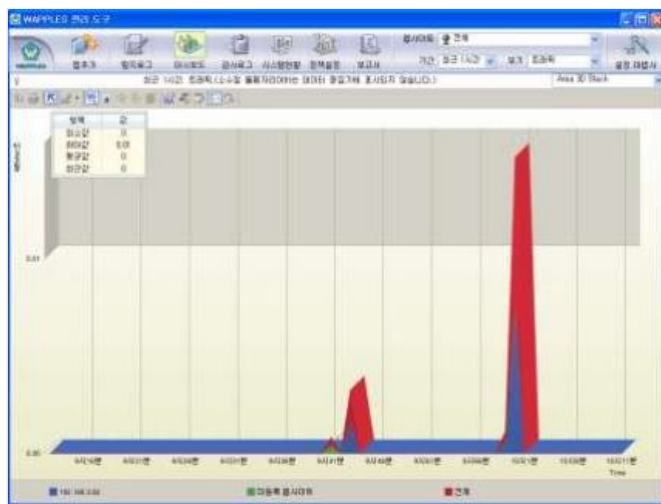
Area 2D Stack

썬은선 그래프의 내부를 채운 형태입니다. 등록되어 있는 웹사이트 별로 다른 색으로 쌓이기 때문에 전체 높이는 전체 트래픽과 같습니다.



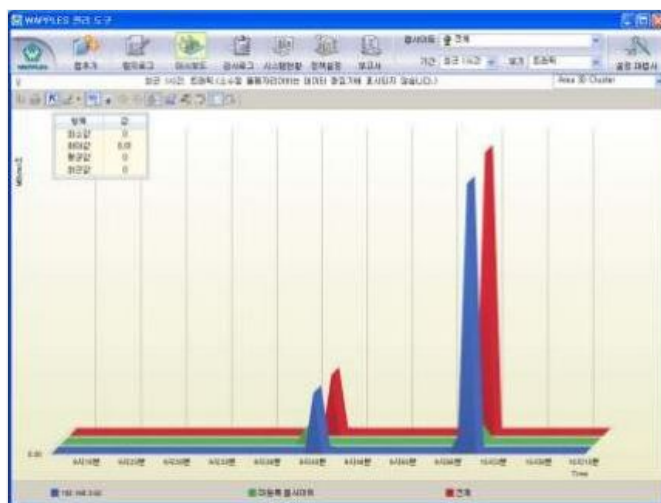
Area 3D Stack

Area 2D Stack 차트의 입체적인 형태입니다.



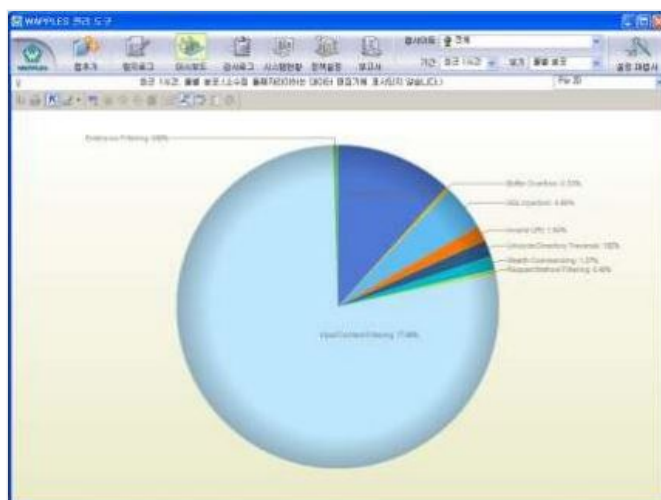
Area 3D Cluster

Area 3D Stack 차트에서 웹사이트 별로 앞뒤로 배치한 형태입니다.



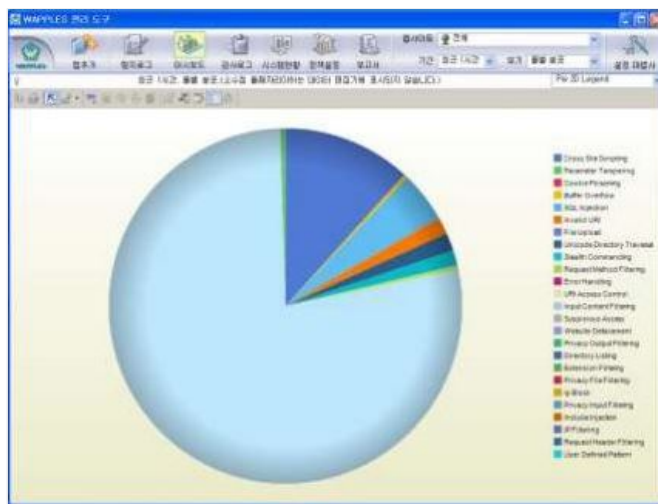
Pie 2D

탐지된 공격의 비율을 파이 차트로 보여줍니다.



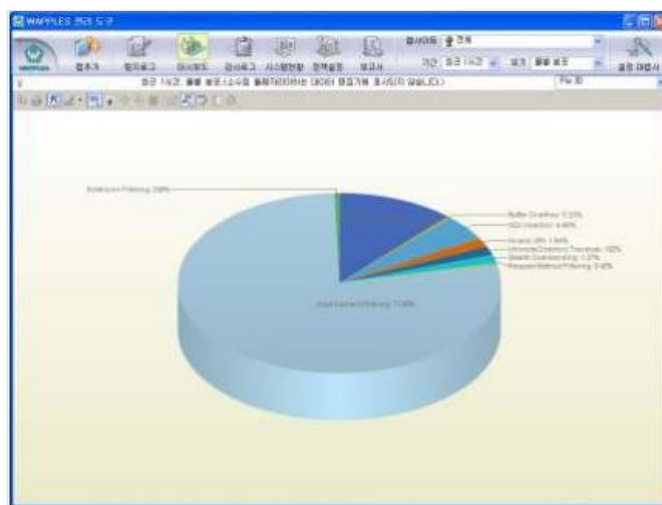
Pie 2D Legend

파이 차트와 범례를 표시합니다.



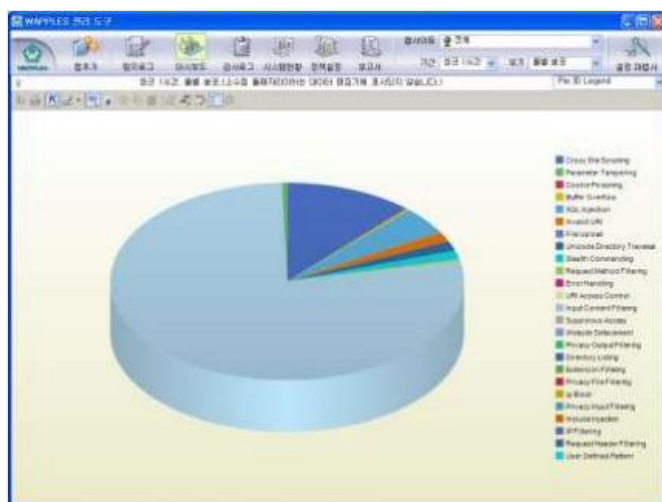
Pie 3D

파이 차트를 입체적으로 보여줍니다.



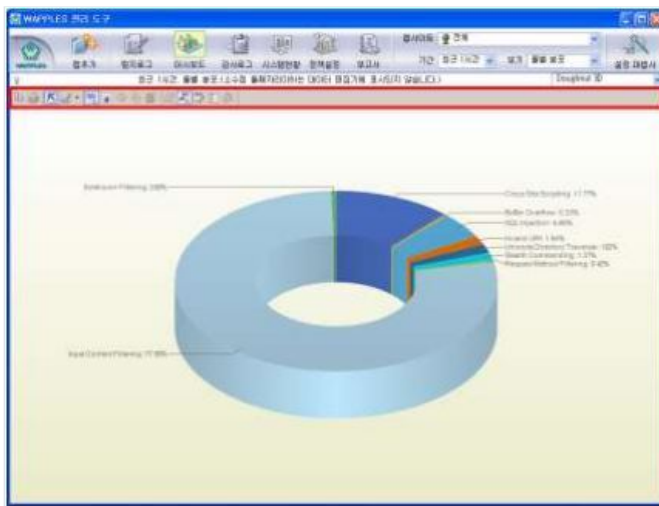
Pie 3D Legend

입체적인 파이 차트와 범례를 보여줍니다.



Doughnut 3D

변형된 파이 차트로 도넛 모양의 차트입니다.



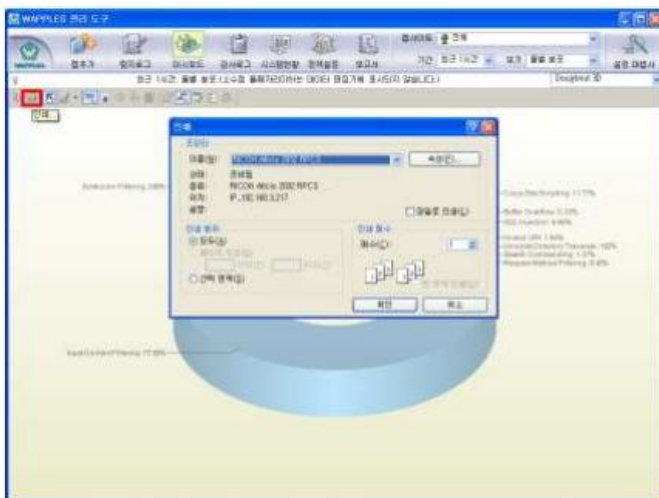
클립보드에 복사

도구 바의 [클립보드에 복사]를 클릭하여 그래프를 복사하면 Microsoft사의 Office 제품과 같은 프로그램에 현재 보고 있는 그래프를 붙여넣기하여 문서작업을 할 수 있습니다.



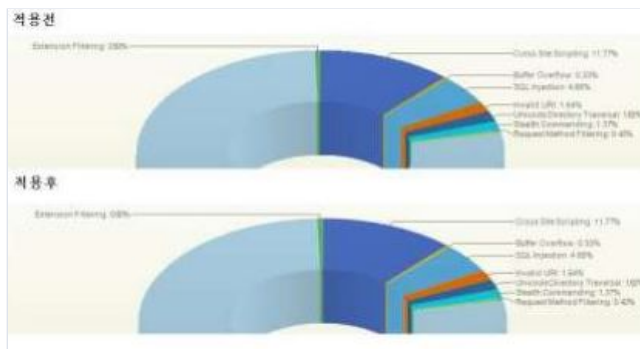
인쇄

도구 바의 [인쇄]를 클릭하면 현재 보고 있는 그래프를 인쇄물로 출력하여 확인할 수 있습니다.



안티앨리어싱

도구 바의 [안티앨리어싱]을 클릭하여 활성화 시키면 그래프를 좀 더 매끄러운 형태로 변경할 수 있습니다.



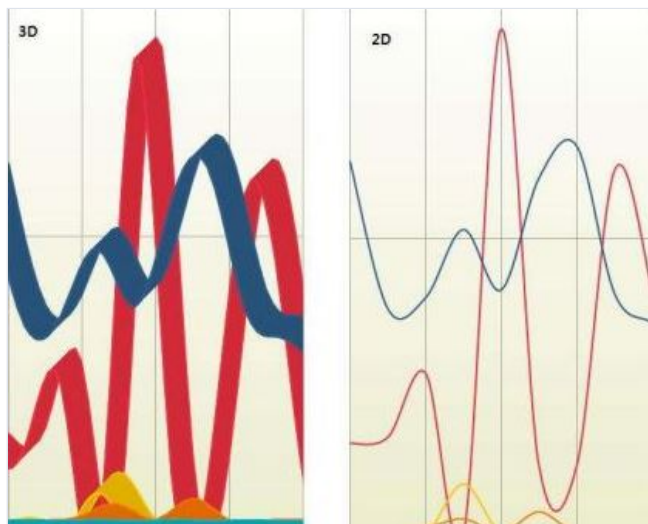
팔레트 구분자

도구 바의 [팔레트 구분자]를 클릭하면 현재 그래프를 구성하고 있는 각 요소의 색을 도구 바가 제공하는 다른 색 조합으로 변경하여 그래프를 관찰할 수 있습니다



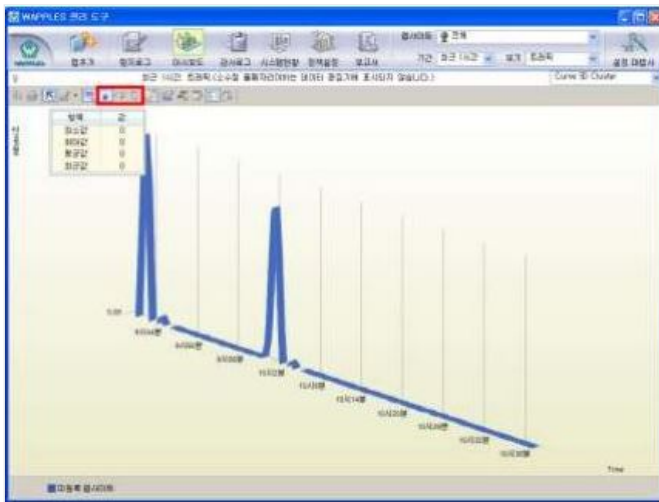
3D/2D

도구 바의 [3D/2D]를 클릭하면 2D 상태의 그래프를 3D로 변형시키거나, 3D 상태의 그래프를 2D로 변형시킬 수 있습니다.



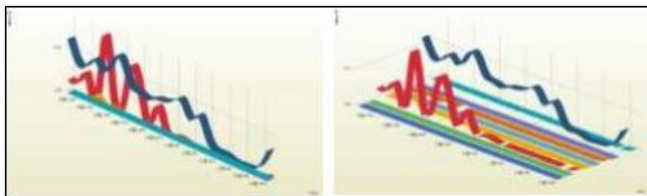
회전시켜보기

3D 형태의 그래프의 경우 도구 바의 [회전시켜보기]를 이용하면 그래프를 다양한 시각에서 확인할 수 있습니다. 도구 바의 [회전시켜보기]를 클릭하여 [X-축 주위 회전]과 [Y-축 주위 회전]을 활성화 시킨 후 [X-축 주위 회전]과 [Y-축 주위 회전]를 클릭하여 X축과 Y축을 중심으로 그래프를 회전시킬 수 있습니다.



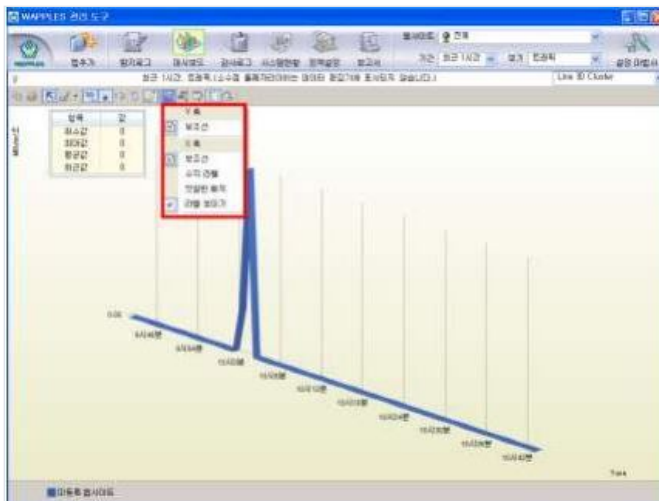
무리짓기 (Z-축)

2D 형태의 그래프를 [3D/2D]를 클릭하여 3D형태의 그래프로 변형시킨경우 1개 이상의 기준데이터가 그래프로 표현되는 경우라면, 기준데이터가 하나의 X축에 겹쳐서 보이게 됩니다. 이를 분리하여 기준데이터별로 구별하여 보고자 할 때, [무리짓기] 기능을 클릭하면 Z축이 생성되어 기준데이터를 구분하여 볼 수 있습니다



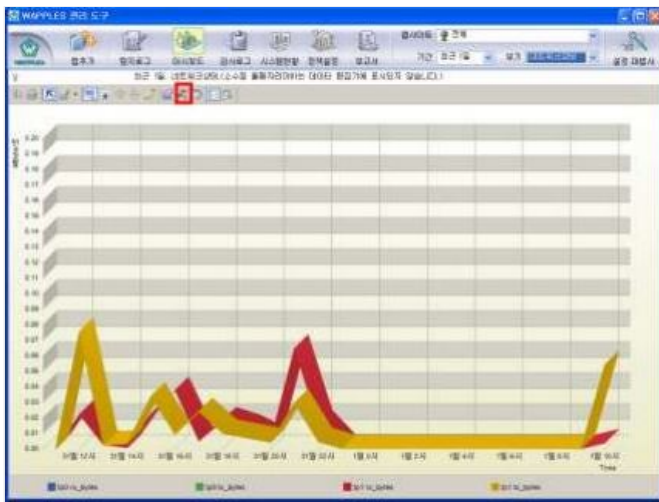
축 설정

그래프의 X축과 Y축의 레이블 정보 구분을 시각적으로 표현하고자 할 때 도구 바의 [축설정]을 클릭하여 그래프 표현 형태를 다양하게 변형시킬 수 있습니다.



포인트 라벨

도구 바의 [포인트 라벨]을 클릭하면 차트에 데이터의 수치가 표시됩니다.



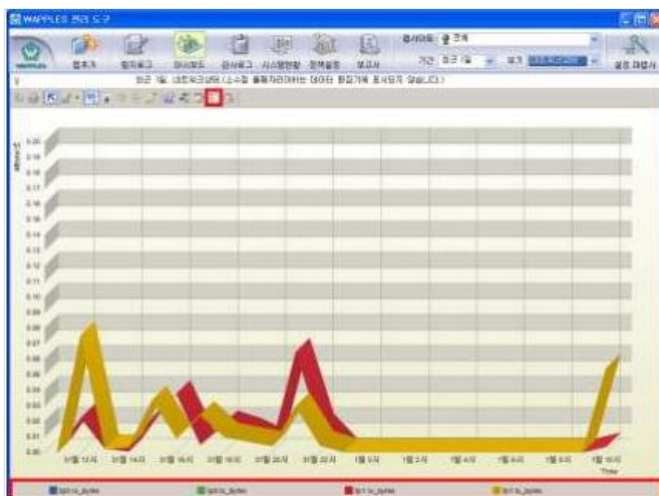
데이터 편집기

도구 바의 [데이터 편집기]를 클릭하면 다음과 같이 데이터 편집기가 표시되며 데이터 편집기를 이용하여 시간에 따른 데이터를 확인할 수 있습니다.



레전드 박스

도구 바의 [레전드 박스]를 클릭하면 다음과 같이 범례가 표시됩니다.



줌(Zoom)

도구 바의 [줌]을 클릭한 후, 그래프에서 자세히 보고 싶은 부분을 마우스로 드래그하여 선택하면 해당 부분이 확대되어 표시됩니다

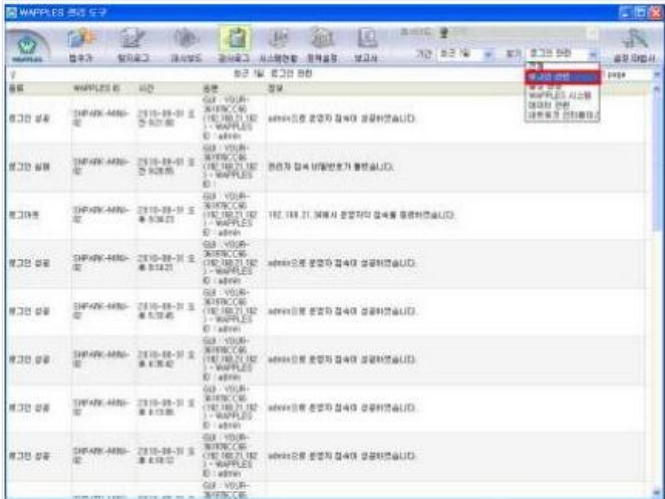
기간별 조회 하기

감사로그의 기간 선택 부분은 탐지로그나 대시보드에서의 기간 선택과 같습니다. [기간 별로 조회]에서 볼 수 있습니다.

감사로그 종류

로그인

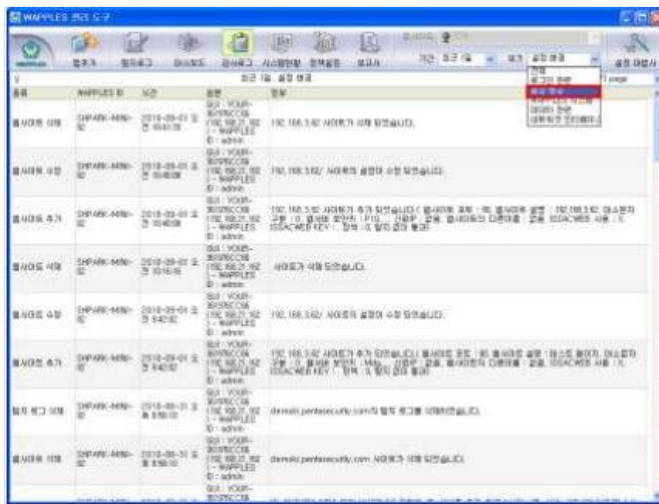
툴 바의 [보기] 메뉴에서 [로그인 관련]을 선택합니다.



로그인 관련 로그 종류

| | |
|-------------|--|
| 로그인 성공 | 운영자 또는 조회자가 관리도구 로그인 창으로 WAF에 접속이 성공한 경우 운영자가 CLI를 통해 WAF에 접속이 성공한 경우 |
| 로그인 실패 | 관리도구 로그인 창에서 아이디와 비밀번호가 틀려 WAF 접속이 실패한 경우 CLI 로그인 기능에서 아이디와 비밀번호가 틀려 WAF에 접속이 실패한 경우 |
| WAF 시스템 | WAF의 시작 및 종료에 대한 감사로그를 보여줍니다. |
| 로그인 연속 실패 | 관리도구에서 비밀번호가 연속 3회 틀렸을 경우 |
| 비밀번호 변경 | 운영자 또는 조회자가 비밀번호를 변경했을 경우 |
| 비밀번호 변경 실패 | 운영자 또는 조회자가 비밀번호 변경에 실패한 경우 |
| 로그아웃 | 관리도구를 종료했을 경우 |
| 세션 잠금 | 운영자 관리도구에 접속이 성공한 후 운영자가 세션 잠금이 발생하도록 설정한 시간 동안 아무런 동작이 없을 경우 |
| 세션 잠금 해제 | 세션 잠금이 발생한 후 비밀번호를 입력하여 인증에 성공한 경우 |
| 세션 잠금 해제 실패 | 세션 잠금이 발생하고 세션 잠금 해제 시도시 비밀번호가 틀렸거나 세션 잠금을 연속 3회 해제하지 못하여 WAF 관리도구가 종료된 경우 |

설정 변경



[설정 변경] 필터에서 보여주는 감사로그의 종류는 다음과 같습니다.

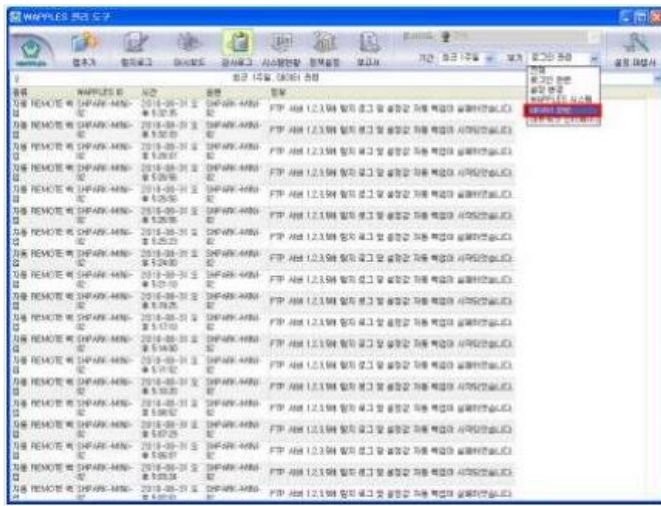
설정 변경 관련 로그 종류

| | |
|---------------|--|
| WAF IP | [설정 마법사]의 [네트워크 설정]에서 Proxy IP 설정을 변경했을 경우 |
| 웹 서버 | 웹 사이트가 설치된 웹 서버를 추가, 수정, 삭제하였을 경우 |
| 웹사이트 추가 | WAF에서 보호할 웹사이트를 추가한 경우 |
| 웹사이트 수정 | WAF에서 보호할 웹사이트 정보를 수정한 경우 |
| 웹사이트 삭제 | WAF에서 보호하는 웹사이트를 삭제한 경우 |
| 정책 이름 | 정책이름이 추가/수정/삭제된 경우 |
| 정책 룰 | 정책 추가/수정을 통하여 정책에 대한 룰의 탐지 설정이나 대응방법이 변경된 경우 |
| 룰 예외처리 변경 | 룰의 예외설정을 변경했을 경우 |
| 접근 설정 변경 | 웹사이트의 특정 경로에 대한 접근 설정을 변경했을 경우 |
| 로그 리뷰 | 로그 검토하기를 수행한 경우 |
| 감사 설정 | 감사 설정이 변경된 경우 |
| 세션 잠금 설정 변경 | 세션 잠금 설정이 변경된 경우 |
| 라우팅 테이블 | 게이트웨이 정보가 추가, 수정, 삭제된 경우 |
| 연동모드 | [설정 마법사]의 [운영 설정]->[연동 설정]에서 설정이 변경된 경우 |
| IP 차단 설정 | [설정 마법사]의 [운영 설정]->[IP 차단 설정]에서 조건 설정이 변경된 경우 |
| IP 차단 관리목록 설정 | [설정 마법사]의 [운영 설정]->[IP 차단 설정]에서 관리하고 있는 IP목록이 변경된 경우 |
| 관리 포트 설정 | Serial 콘솔 포트 (시리얼(serial) 케이블)를 사용하여 관리 포트를 변경한 경우 |
| S/W BYPASS | S/W BYPASS의 설정이 변경된 경우 |

| | |
|-----------------------|--|
| WAF 시작 | WAF 시작 |
| WAF 정지 | WAF 정지 |
| WAF 시스템 | WAF의 시작 및 종료에 대한 감사로그를 보여줍니다. |
| 무결성 검사 성공 | 무결성 검사 성공 |
| 무결성 검사 실패 | 무결성 검사 실패 |
| 보안 경보 확인 | IP BLOCK, 로그인 3회 실패, DB 용량 위험 및 DB 용량 초과 관련 로그 발생시 출력되는 경고 창을 확인한 경우 |
| 업데이트 성공 | WAF 업데이트에 성공한 경우 |
| 업데이트 실패 | WAF 업데이트에 실패한 경우 |
| 업데이트 강제 수행 | WAF 업데이트가 자동으로 실행되지 않고 운영자에 의해 강제로 수행된 경우 |
| 정책/로그 동기화 설정(PLS) | 정책/로그 동기화 설정(PLS)을 했을 경우 |
| 정책/로그 동기화(PLS) – 통신성공 | 정책/로그 동기화(PLS) 통신이 성공했을 경우 |
| 정책/로그 동기화(PLS) – 통신실패 | 정책/로그 동기화(PLS) 통신이 실패했을 경우 |
| 보고서 메일 보내기성공 | 보고서 메일 보내기가 성공했을 경우 |
| 보고서 메일 보내기 실패 | 보고서 메일 보내기가 실패했을 경우 |
| 라이선스 등록 | 기능별 라이선스 등록이 성공했을 경우 |
| 라이선스 등록 실패 | 기능별 라이선스 등록이 실패했을 경우 |
| 라이선스 기능제한 | 기능별 라이선스의 기능 제한이 성공했을 경우 |
| 라이선스 체크섬 확인 실패 | 기능별 라이선스 체크섬 확인이 실패했을 경우 |
| 라이선스 체크섬 복구 성공 | 기능별 라이선스 체크섬을 복구했을 경우 |
| 라이선스 체크섬 복구 실패 | 기능별 라이선스 체크섬 복구에 실패했을 경우 |

데이터 관련

툴 바의 [보기] 메뉴에서 [데이터 관련]을 선택합니다.



[데이터 관련] 필터에서 보여주는 감사로그의 종류는 다음과 같습니다.

데이터 관련 로그 종류

| | |
|-----------------|---|
| DB 용량 위험 | 침입로그의 최대 저장 용량은 100GB입니다. 상태로그의 최대 저장 용량은 40GB입니다. 감사로그의 최대 저장 용량은 1GB입니다. 최대 저장 용량의 95%를 초과한 경우 표시됩니다 |
| DB 용량 초과 | 침입로그의 최대 저장 용량은 100GB입니다. 상태로그의 최대 저장 용량은 40GB입니다. 감사로그의 최대 저장 용량은 1GB입니다. 최대 저장 용량을 초과한 경우 기존 데이터의 가장 오래된10%분량을 삭제하고 이를 표시합니다. |
| 자동 백업 | DB의 탐지로그 및 설정값에 대해 설정된 기간에 따라서 자동 백업을 수행한 경우 |
| 자동 REMOTE 백업 | DB의 탐지로그 및 설정값에 대해 설정된 기간에 따라서 자동 REMOTE 백업을 수행한 경우 |
| 자동 백업 실패 | DB의 탐지로그 및 설정값에 대하여 자동 백업에 실패한 경우 |
| 자동 REMOTE 백업 실패 | DB의 탐지로그 및 설정값에 대하여 자동 REMOTE 백업에 실패한 경우 |

데이터 관련 로그 발생시 관리도구는 보안 경보 메시지를 출력합니다. 출력되는 보안 경보 메시지는 다음과 같습니다.

데이터 관련 로그 보안 경보 메시지

| | |
|--------------------------|--|
| 보안 경보 메시지 | 출력 원인 |
| "DB 용량 위험"감사로그가 검색되었습니다 | [데이터 관련 로그 종류] 에서와 같이 DB 용량 위험 로그가 기록된 경우 |
| "DB 용량 초과"감사로그가 검색되었습니다. | [데이터 관련 로그 종류] 에서와 같이 DB 용량 초과 감사로그가 기록된 경우 |

보안 경보 메시지는 로그인 3 회 연속 실패, IP 차단, DB 용량 위험 감사로그, DB 용량 초과 감사로그가 기록된 경우 출력되며 가장 최근에 기록된 해당 로그 1 개에 대해서만 보안 경보 메시지를 출력합니다

네트워크 인터페이스

[보기] 메뉴에서 [네트워크 인터페이스]을 선택합니다.

| ID | Name | Time | Action |
|----|-------------------|---------------------|--------|
| 1 | Network Interface | 2013-09-11 10:00:00 | Filter |
| 2 | Network Interface | 2013-09-11 10:00:00 | Filter |
| 3 | Network Interface | 2013-09-11 10:00:00 | Filter |
| 4 | Network Interface | 2013-09-11 10:00:00 | Filter |
| 5 | Network Interface | 2013-09-11 10:00:00 | Filter |
| 6 | Network Interface | 2013-09-11 10:00:00 | Filter |
| 7 | Network Interface | 2013-09-11 10:00:00 | Filter |
| 8 | Network Interface | 2013-09-11 10:00:00 | Filter |
| 9 | Network Interface | 2013-09-11 10:00:00 | Filter |
| 10 | Network Interface | 2013-09-11 10:00:00 | Filter |
| 11 | Network Interface | 2013-09-11 10:00:00 | Filter |
| 12 | Network Interface | 2013-09-11 10:00:00 | Filter |
| 13 | Network Interface | 2013-09-11 10:00:00 | Filter |
| 14 | Network Interface | 2013-09-11 10:00:00 | Filter |
| 15 | Network Interface | 2013-09-11 10:00:00 | Filter |
| 16 | Network Interface | 2013-09-11 10:00:00 | Filter |
| 17 | Network Interface | 2013-09-11 10:00:00 | Filter |
| 18 | Network Interface | 2013-09-11 10:00:00 | Filter |
| 19 | Network Interface | 2013-09-11 10:00:00 | Filter |
| 20 | Network Interface | 2013-09-11 10:00:00 | Filter |

[네트워크 인터페이스] 필터에서 보여주는 감사로그의 종류는 다음과 같습니다

네트워크 인터페이스 관련 로그 종류

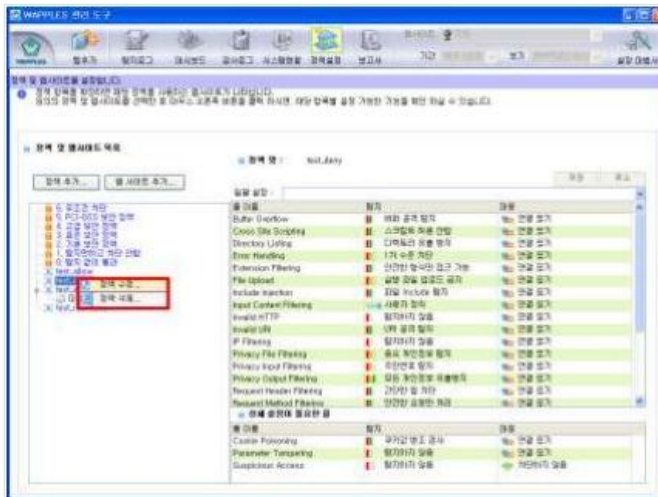
| | |
|---------------|-----------------|
| 네트워크 인터페이스 | NIC의 상태가 변경된 경우 |
| 네트워크 인터페이스 오류 | 에러 패킷이 발생된 경우 |

정책 설정

WAF은 아래화면 정책 설정에서 WAF의 탐지 보안 정책과 웹 서버의 웹사이트정보를 설정할 수 있습니다.

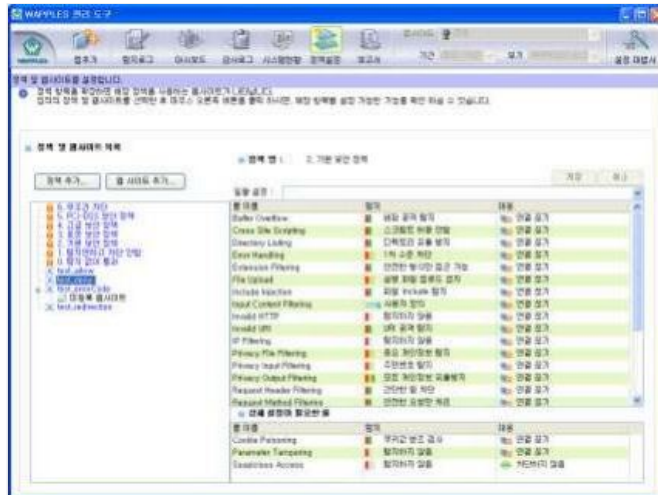


정책 설정 뷰에서 정책이 변경될 경우 아래 와 같이 [저장][취소] 버튼이 활성화 됩니다. [취소]버튼을 누를 경우 정책은 저장되지 않으며 [저장]버튼을 눌러야만 변경된 정책이 반영됩니다.



아래화면은 왼쪽의 [정책 및 웹사이트 목록]과 오른쪽의 [정책 세부 정보 목록]이 있습니다.

[정책 및 웹사이트 목록]은 윈도우의 탐색기에서 폴더형태의 트리뷰와 같습니다. 첫 번째 레벨은 정책의 목록을 보여주고 정책 중 (+) 기호가 있는 부분을 클릭하면 확장되어 해당 정책에 속해있는 웹 사이트 목록을 볼 수 있습니다.



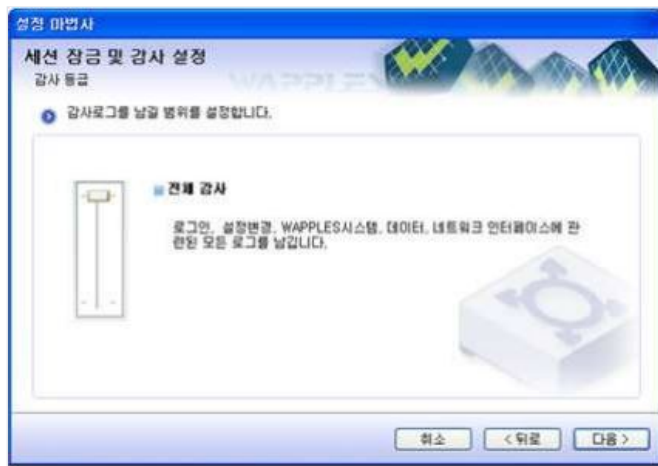
WAF는 웹사이트 별 관리자를 지정할 수 있습니다. [정책 및 웹사이트 목록] 에 표시되는 정책과 웹사이트는 이름 앞에 관리자명을 표시합니다. [IX.1.1세션 잠금 및 감사 설정]

[감사 설정]은 감사 수준별 감사로그를 기록하기 위해 인가된 관리자에게 보여지는 감사 기록의 수준을 선택할 수 있는 기능입니다.

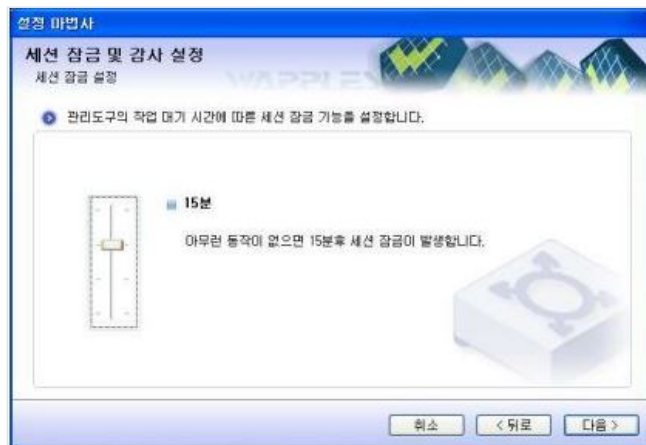
감사 등급은 [기본감사]와 [전체감사]가 있으며 각각의 의미와 감사 항목은 아래 표에서 설명합니다

감사 수준별 감사 항목

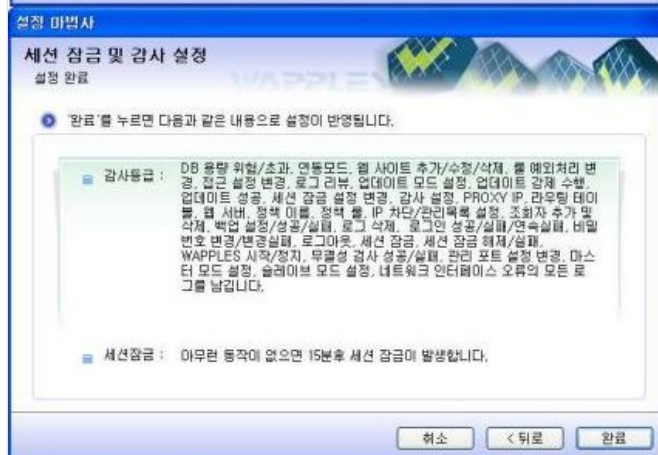
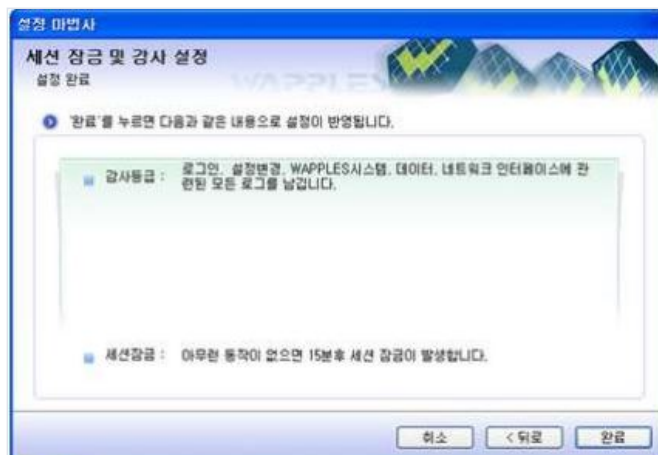
| 감사 수준 | 설명 | 감사 항목 |
|-------|--|--|
| 기본감사 | WAF 시스템의 중대한 사건이나 변경사항에 대한 감사 자료를 기록합니다. | DB용량 위험/초과, 연동모드, 웹 사이트 추가/수정/삭제, 룰 예외처리 변경, 접근설정 변경, 로그 리뷰, 업데이트 설정, 업데이트 성공, 세션 잠금 설정 변경, 감사설정, WAF IP, 라우팅 테이블, 웹 서버, 정책 이름, 정책을, 백업 설정/성공/실패, 로그 삭제, 로그인 실패/연속실패, 비밀번호 변경/실패, 세션 잠금 실패, WAF 시작/정지, 무결성 검사 실패, 관리포트설정 변경, 백업 설정, 네트워크 인터페이스 오류, 보안 경보, 조회자 아이디 추가/삭제, 시간동기화 설정 변경, 시간동기화 성공/실패, 표준시간대 변경/실패,패턴저장소 설정 변경, 정책/로그 동기화 설정/결과, 보고서 메일 보내기 성공/실패, 기능별 라이선스 등록 성공/실패 |
| 전체감사 | 기본 감사 항목 외에 일반적인 정보 및 주기적인 점검 사항의 정상 작동에 관한내용까지의 감사 자료로 기록합니다. | 기본 감사 수준의 감사 항목 및 업데이트 강제 수행, IP 차단/관리목록 설정, 조회자 추가 및 삭제, 로그아웃, 세션 잠금, 세션 잠금 해제, WAF 시작/정지, 무결성 검사 성공, 관리포트 설정 변경 |



[감사 등급 설정]화면에서 슬라이드 바를 상하로 끌어서 기본 혹은 전체 감사상태로 바꾼 후 [다음] 버튼을 클릭 합니다



[세션 잠금 설정]은 관리자가 WPPLES 관리도구에 로그인 한 상태로 장시간 자리를 비웠을 때 보안을 위하여 일정 시간 이후 자동으로 관리 도구에 접근을 차단하는 기능입니다. [세션 잠금 설정] 화면에서는 세션 잠금이 발생하는 시간을 5분/15분/30분/사용안함 으로 조절 할 수 있습니다.



[세션 잠금 설정] 화면에서 [다음] 버튼을 클릭하면 **[오류! 참조 원본을 찾을 수 없습니다.오류! 참조 원본을 찾을 수 없습니다.]**화면이 나타납니다. [완료] 버튼을 클릭하면 세션 잠금 및 감사 설정이 저장 되어 WAF에 반영됩니다.

세션 잠금 기간 설정을 하면 설정된 시간 동안 WAPPLES 관리도구 프로그램에 키보드 입력이나 마우스 클릭이 없을 경우 WAF 관리도구와 WAF간의 연결이 끊어지고 **[오류! 참조 원본을 찾을 수 없습니다.]**화면이 나타납니다.

[오류! 참조 원본을 찾을 수 없습니다.]화면에서 세션 잠금을 해제하거나 관리도구를 종료할 수 있습니다. 관리도구를 다시 사용하려면 암호를 재 입력하고 [세션 잠금 해제]버튼을 클릭합니다.

[오류! 참조 원본을 찾을 수 없습니다.]화면은 아이디는 입력할 수 없으며 비밀번호 입력만을 허용합니다. 로그인 방법은 아이디와 비밀번호 변경 체크박스를 입력할 수 없을 뿐 [Ⅲ.1.1 로그인] 과 동일합니다.



백업 설정

WAF에 기록된 설정 정보, 탐지 로그 및 감사로그를 WAF 시스템 혹은 외부의 FTP서버로 백업 데이터를 저장하기 위해 [백업 설정] 기능을 사용합니다.



백업단위는 매일, 매주, 매월, 사용 안 함을 설정할 수 있습니다.

매일 백업을 원할 경우 백업시간을 입력하고 매주 백업을 원할 경우 원하는 요일과 백업 시간을 입력합니다. 매월 백업을 원할 경우 백업 날짜와 시간을 입력합니다.

백업은 FTP를 사용하여 백업 데이터를 전송합니다. FTP 사용에 필요한 정보인 FTP 서버 IP, FTP 서버 경로, FTP 아이디, FTP 비밀번호를 입력합니다.

백업 설정 오류 메시지

| 오류 메시지 | 출력 원인 |
|-------------------|--|
| 하나 이상의 요일을 선택합니다. | 백업단위를 [매주]로 선택 시 하나 이상의 요일에 체크하지 않았을 경우 |
| 빈칸일 수 없습니다. | Remote 백업 선택 시 FTP 서버 IP, FTP 서버 경로, FTP 아이디, FTP 비밀번호 입력 값이 |

| | |
|-------------|-----------------------------|
| | 빈칸일 경우 |
| 잘못된 IP 입니다. | FTP 서버 IP 가 올바른 IP형식이 아닐 경우 |

[오류! 참조 원본을 찾을 수 없습니다.] 화면에서 [다음] 버튼을 클릭하면 [오류! 참조 원본을 찾을 수 없습니다.] 화면이 나타납니다.

다운로드 받을 백업파일을 선택 후, [다운로드]버튼을 누르면 백업파일을 다운로드합니다. [업로드] 버튼을 누르고 백업파일을 선택한 후 열기 버튼을 누르면 백업파일을 시스템에 업로드 합니다.



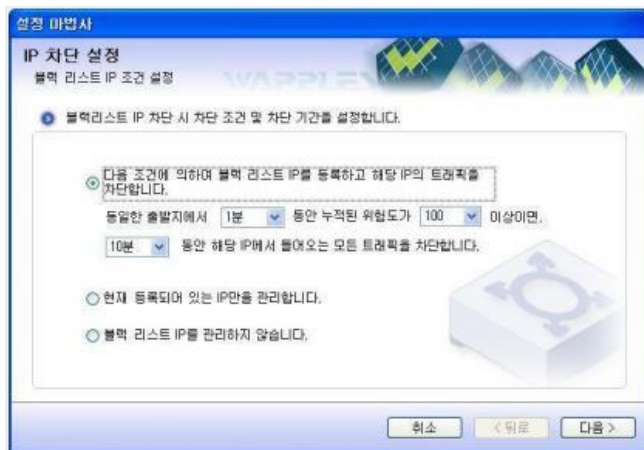
[오류! 참조 원본을 찾을 수 없습니다.] 화면에서 다음 버튼을 클릭하면 [오류! 참조 원본을 찾을 수 없습니다.]과 같은 [설정 완료] 화면이 나타납니다. 이 화면에서 설정 내용을 확인하고 [완료] 버튼을 클릭합니다.



IP 차단 설정

IP차단은 하나의 출발지에서 계속하여 공격을 시도하는 것을 막기 위해 사용합니다. WAF은 같은 출발지에서 발생한 공격을 탐지하여 차단한 사건에 대하여 시간당 위험도를 점수로 기록하고 누적 점수가 설정치 이상이 되었을 때 일정시간 그 출발지에서 발생하는 모든 트래픽을 차단 하도록 합니다.

이 화면에서 IP 차단 관리목록에 대한 IP 관리 기능을 활성화 할지 여부를 선택하고, 활성화 한다면 어떠한 조건으로 IP 차단 관리목록을 등록하고 얼마나 오랫동안 관리한지 혹은 현재 등록되어 있는 IP만을 관리 할지를 설정할 수 있습니다.



[다음] 버튼을 클릭하면 **[오류! 참조 원본을 찾을 수 없습니다.]**화면이 나타납니다. 다음과 같은 항목을 설정할 수 있습니다.

- 연결 차단 IP/연결 차단 시간
- 연결 허용 IP /연결 허용 시간

[특정 IP 혹은 IP 대역에 대해 일정 시간 동안 연결을 차단하거나 허용 할 수 있습니다. 설정을 원하는 IP와 연결 차단 혹은 연결 허용할 시간을 입력하고 [해당 IP 연결 허용] 체크 박스에 허용 유무를 체크한 뒤 추가 버튼을 사용하여 관리 IP를 관리 IP 목록에 추가합니다.



설정된 IP의 수정/삭제는 IP 리스트에서 삭제할 IP를 선택하고 [수정]/[삭제] 버튼을 누른 후 [다음]을 클릭하면, 설정 요약 화면이 나타납니다. 설정한 내용을 다시 한번 확인하고 [완료] 버튼을 클릭하면 IP차단 설정 내용이 WAF에 적용됩니다.

설정 마법사는 IP 차단 설정 시 사용자 입력 값에 오류가 있을 경우 다음과 같은 오류 메시지를 출력합니다.

로그인 오류 메시지

| 오류 메시지 | 출력 원인 |
|-----------------------------|-------------------------------------|
| 잘못된 IP입니다. | 관리 IP 추가/수정 시 입력된 IP가 IP형식이 아닐 경우 |
| 현재 시간부터 5분 이상을 설정 할 수 있습니다. | 설정된 시간이 현재 시간부터 5분 이상의 미래 시간이 아닐 경우 |

IP 관리 종료 예정 시간은 현재의 시간보다 5 분 이상의 미래의 시간을 입력해야 합니다.



IP차단을 위한 위험도 설정은 정책설정의 모든 룰에서 설정이 가능합니다. 다음은 Buffer Over Flow 룰의 위험도 설정 화면입니다. 대응 하단의 위험도를 각 룰의 점수를 설정합니다.



룰의 위험도 설정은 탐지 프로세스에 적용되기 때문에 '탐지'와 '사용자정의' 설정에서만 수정이 가능하고, '탐지안함' 상태에서는 위험도 수치를 설정할 수 없습니다.

E-MAIL 설정

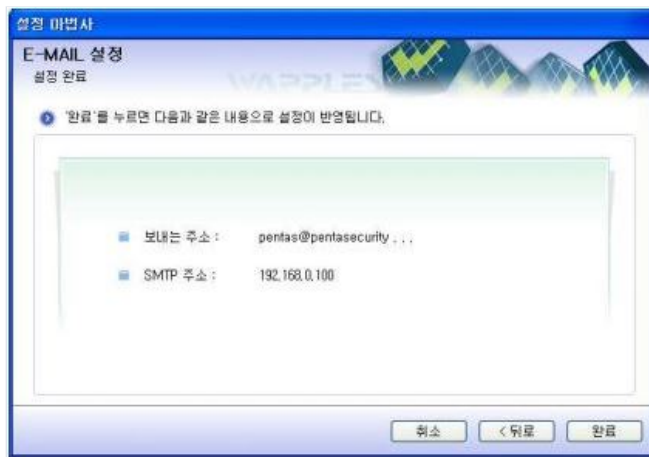
[오류! 참조 원본을 찾을 수 없습니다. 오류! 참조 원본을 찾을 수 없습니다.]과 [IX 설정마법사 오류! 참조 원본을 찾을 수 없습니다. 오류! 참조 원본을 찾을 수 없습니다.]의 [탐지로그 연동] 기능에서 사용하는 EMAIL 관련 정보를 설정할 수 있습니다.

[운영 설정]에서 [E-MAIL 설정]을 클릭하면 다음과 같은 화면이 나타납니다.



보내는 주소는 E-MAIL 발신자의 E-MAIL 주소를 의미하며, SMTP 주소는 SMTP 서버의 IP 주소를 의미합니다.

설정이 끝난 후, 화면 우측 하단의 [다음>]버튼을 클릭합니다. [오류!참조 원본을 찾을 수 없습니다.]이 나타나면 설정된 내용을 확인한 후 화면 우측 하단의 [완료] 버튼을 클릭합니다.



계정 관리 참조

WAF은 사용자가 따로 설정하지 않아도 사용할 수 있는 7가지 기본 정책이 마련되어 있습니다. 기본 정책에 대한 설명은 다음 표와 같습니다

기본 정책 목록

| 기본 정책 | 설명 |
|---------------|--|
| 무조건차단 | 모든 트래픽을 차단하는 정책 |
| PCI-DSS 보안 정책 | PCI-DSS 인증을 준수하기 위하여 적용 가능한 정책으로, PCI-DSS에 적합한 보안 수준을 제공 |
| 고급 보안 정책 | 영향도가 낮은 공격까지 방어해주는 높은 수준의 보안 정책으로 사용자의 세부 대응이 필요한 공격 이외의 대부분의 공격을 방어 |
| 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 |
| 탐지만하고 차단 안함 | 기본적인 탐지 부분은 [기본 보안 정책]과 동일하나 탐지된 위반 행위에 대해 차단하지 않는 정책 |
| 탐지 없이 통과 | 웹 사이트에 대한 보안 위반 탐지 행위를 전혀 하지 않는 정책 |

각 기본 정책에 대한 룰별 보안도 설정 및 대응설정 내용은 다음 표와 같습니다. 각 탐지 규칙에 대한 자세한 설명은 [탐지룰의 이해]에서 볼 수 있습니다

기본 정책 내용

== 탐지 없이 통과 ==

| 룰 이름 | 탐지 | 대응 |
|----------------------|---------|---------|
| Buffer Overflow | 탐지하지 않음 | 차단하지 않음 |
| Cross Site Scripting | 탐지하지 않음 | 차단하지 않음 |
| Directory Listening | 탐지하지 않음 | 차단하지 않음 |
| Error Handling | 탐지하지 않음 | 차단하지 않음 |

| | | |
|-----------------------------|---------|---------|
| Extension Filtering | 탐지하지 않음 | 차단하지 않음 |
| File Upload | 탐지하지 않음 | 차단하지 않음 |
| Include Injection | 탐지하지 않음 | 차단하지 않음 |
| Input Content Filtering | 탐지하지 않음 | 차단하지 않음 |
| Invalid HTTP | 탐지하지 않음 | 차단하지 않음 |
| Invalid URI | 탐지하지 않음 | 차단하지 않음 |
| IP Filtering | 탐지하지 않음 | 차단하지 않음 |
| Privacy File Filtering | 탐지하지 않음 | 차단하지 않음 |
| Privacy Input Filtering | 탐지하지 않음 | 차단하지 않음 |
| Privacy Output Filtering | 탐지하지 않음 | 차단하지 않음 |
| Request Header Filtering | 탐지하지 않음 | 차단하지 않음 |
| Request Method Filtering | 탐지하지 않음 | 차단하지 않음 |
| Response Header Filtering | 탐지하지 않음 | 차단하지 않음 |
| SQL Injection | 탐지하지 않음 | 차단하지 않음 |
| Stealth Commanding | 탐지하지 않음 | 차단하지 않음 |
| Unicode Directory Traversal | 탐지하지 않음 | 차단하지 않음 |
| URI Access Control | 탐지하지 않음 | 차단하지 않음 |
| User Defined Pattern | 탐지하지 않음 | 차단하지 않음 |
| Website Defacement | 탐지하지 않음 | 차단하지 않음 |
| 상세 설정이 필요한 룰 | | |
| Cookie Poisoning | 탐지하지 않음 | 차단하지 않음 |
| Parameter Tampering | 탐지하지 않음 | 차단하지 않음 |
| Suspicious Access | 탐지하지 않음 | 차단하지 않음 |

== 탐지만 차단 안함 ==

| 룰 이름 | 탐지 | 대응 |
|-----------------|--------|---------|
| Buffer Overflow | 사용자 정의 | 차단하지 않음 |
| | | |

| | | |
|-----------------------------|------------------------|---------|
| Cross Site Scripting | 사용자 정의 | 차단하지 않음 |
| Directory Listing | 디렉토리 유출 방지 | 차단하지 않음 |
| Error Handling | 1차 수준 차단 | 차단하지 않음 |
| Extension Filtering | 안전한 형식만 접근 가능 | 차단하지 않음 |
| File Upload | 실행 파일 업로드 금지 | 차단하지 않음 |
| Include Injection | 탐지하지 않음 | 차단하지 않음 |
| Input Content Filtering | 탐지하지 않음 | 차단하지 않음 |
| Invalid HTTP | 위험한 HTTP 차단 | 차단하지 않음 |
| Invalid URI | URI 공격 탐지 | 차단하지 않음 |
| IP Filtering | 탐지하지 않음 | 차단하지 않음 |
| Privacy File Filtering | 중요 개인정보 탐지 | 차단하지 않음 |
| Privacy Input Filtering | 탐지하지 않음 | 차단하지 않음 |
| Privacy Output Filtering | 주민번호 탐지 | 차단하지 않음 |
| Request Header Filtering | 탐지하지 않음 | 차단하지 않음 |
| Request Method Filtering | 안전한 요청만 처리 | 차단하지 않음 |
| Response Header Filtering | 서버 정보 유출 방지 | 차단하지 않음 |
| SQL Injection | 기본 SQL Injection 공격 탐지 | 차단하지 않음 |
| Stealth Commanding | 외부 프로그램 실행 시도 탐지 | 차단하지 않음 |
| Unicode Directory Traversal | 일반 설정 | 차단하지 않음 |
| URI Access Control | 탐지하지 않음 | 차단하지 않음 |
| User Defined Pattern | 탐지하지 않음 | 차단하지 않음 |
| Website Defacement | 탐지하지 않음 | 차단하지 않음 |
| 상세 설정이 필요한 룰 | | |
| Cookie Poisoning | 탐지하지 않음 | 차단하지 않음 |
| Parameter Tampering | 탐지하지 않음 | 차단하지 않음 |
| Suspicious Access | 탐지하지 않음 | 차단하지 않음 |

== 기본 보안 정책 ==

| 룰 이름 | 탐지 | 대응 |
|-----------------------------|------------------------|---------|
| Buffer Overflow | 사용자 정의 | 차단하지 않음 |
| Cross Site Scripting | 사용자 정의 | 차단하지 않음 |
| Directory Listing | 디렉토리 유출 방지 | 에러 코드 |
| Error Handling | 1차 수준 차단 | 차단하지 않음 |
| Extension Filtering | 안전한 형식만 접근 가능 | 차단하지 않음 |
| File Upload | 실행 파일 업로드 금지 | 차단하지 않음 |
| Include Injection | 탐지하지 않음 | 차단하지 않음 |
| Input Content Filtering | 탐지하지 않음 | 차단하지 않음 |
| Invalid HTTP | 위험한 HTTP 차단 | 연결 끊기 |
| Invalid URI | URI 공격 탐지 | 차단하지 않음 |
| IP Filtering | 탐지하지 않음 | 차단하지 않음 |
| Privacy File Filtering | 중요 개인정보 탐지 | 차단하지 않음 |
| Privacy Input Filtering | 탐지하지 않음 | 차단하지 않음 |
| Privacy Output Filtering | 주민번호 탐지 | 차단하지 않음 |
| Request Header Filtering | 탐지하지 않음 | 차단하지 않음 |
| Request Method Filtering | 안전한 요청만 처리 | 차단하지 않음 |
| Response Header Filtering | 서버 정보 유출 방지 | 차단하지 않음 |
| SQL Injection | 기본 SQL Injection 공격 탐지 | 에러 코드 |
| Stealth Commanding | 외부 프로그램 실행 시도 탐지 | 차단하지 않음 |
| Unicode Directory Traversal | 일반 설정 | 차단하지 않음 |
| URI Access Control | 탐지하지 않음 | 차단하지 않음 |
| User Defined Pattern | 탐지하지 않음 | 차단하지 않음 |
| Website Defacement | 탐지하지 않음 | 차단하지 않음 |
| 상세 설정이 필요한 룰 | | |
| Cookie Poisoning | 탐지하지 않음 | 차단하지 않음 |
| Parameter Tampering | 탐지하지 않음 | 차단하지 않음 |

| | | |
|-------------------|---------|---------|
| Suspicious Access | 탐지하지 않음 | 차단하지 않음 |
|-------------------|---------|---------|

== 표준 보안 정책 ==

| 룰 이름 | 탐지 | 대응 |
|-----------------------------|------------------------|---------|
| Buffer Overflow | 버퍼 공격 탐지 | 차단하지 않음 |
| Cross Site Scripting | 사용자 정의 | 에러 코드 |
| Directory Listening | 디렉토리 유출 방지 | 에러 코드 |
| Error Handling | 1차 수준 차단 | 에러 코드 |
| Extension Filtering | 안전한 형식만 접근 가능 | 차단하지 않음 |
| File Upload | 실행 파일 업로드 금지 | 차단하지 않음 |
| Include Injection | 파일 Include 탐지 | 차단하지 않음 |
| Input Content Filtering | 탐지하지 않음 | 차단하지 않음 |
| Invalid HTTP | 위험한 HTTP 차단 | 연결 끊기 |
| Invalid URI | URI 공격 탐지 | 에러 코드 |
| IP Filtering | 탐지하지 않음 | 차단하지 않음 |
| Privacy File Filtering | 중요 개인정보 탐지 | 차단하지 않음 |
| Privacy Input Filtering | 탐지하지 않음 | 차단하지 않음 |
| Privacy Output Filtering | 주민번호 탐지 | 차단하지 않음 |
| Request Header Filtering | 탐지하지 않음 | 차단하지 않음 |
| Request Method Filtering | 안전한 요청만 처리 | 차단하지 않음 |
| Response Header Filtering | 서버 정보 유출 방지 | 차단하지 않음 |
| SQL Injection | 확장 SQL Injection 공격 탐지 | 에러 코드 |
| Stealth Commanding | 외부 프로그램 실행 시도 탐지 | 차단하지 않음 |
| Unicode Directory Traversal | 일반 설정 | 에러 코드 |
| URI Access Control | 탐지하지 않음 | 차단하지 않음 |
| User Defined Pattern | 탐지하지 않음 | 차단하지 않음 |
| Website Defacement | 탐지하지 않음 | 차단하지 않음 |

| 상세 설정이 필요한 룰 | | |
|---------------------|---------|---------|
| Cookie Poisoning | 탐지하지 않음 | 차단하지 않음 |
| Parameter Tampering | 탐지하지 않음 | 차단하지 않음 |
| Suspicious Access | 탐지하지 않음 | 차단하지 않음 |

== 고급 보안 정책 ==

| 룰 이름 | 탐지 | 대응 |
|-----------------------------|------------------------|---------|
| Buffer Overflow | 버퍼 공격 탐지 | 에러 코드 |
| Cross Site Scripting | 스크립트 허용 안함 | 에러 코드 |
| Directory Listing | 디렉토리 유출 방지 | 에러 코드 |
| Error Handling | 1차 수준 차단 | 에러 코드 |
| Extension Filtering | 안전한 형식만 접근 가능 | 에러 코드 |
| File Upload | 실행 파일 업로드 금지 | 에러 코드 |
| Include Injection | 파일 Include 탐지 | 에러 코드 |
| Input Content Filtering | 탐지하지 않음 | 차단하지 않음 |
| Invalid HTTP | 위험한 HTTP 차단 | 연결 끊기 |
| Invalid URI | URI 공격 탐지 | 에러 코드 |
| IP Filtering | 탐지하지 않음 | 차단하지 않음 |
| Privacy File Filtering | 중요 개인정보 탐지 | 에러 코드 |
| Privacy Input Filtering | 탐지하지 않음 | 차단하지 않음 |
| Privacy Output Filtering | 주민번호 탐지 | 차단하지 않음 |
| Request Header Filtering | 간단한 원 차단 | 에러 코드 |
| Request Method Filtering | 안전한 요청만 처리 | 에러 코드 |
| Response Header Filtering | 서버 정보 유출 방지 | 차단하지 않음 |
| SQL Injection | 확장 SQL Injection 공격 탐지 | 에러 코드 |
| Stealth Commanding | 외부 프로그램 실행 시도 탐지 | 에러 코드 |
| Unicode Directory Traversal | 일반 설정 | 에러 코드 |
| URI Access Control | 탐지하지 않음 | 차단하지 않음 |

| | | |
|----------------------|-----------------|---------|
| User Defined Pattern | 탐지하지 않음 | 차단하지 않음 |
| Website Defacement | 탐지하지 않음 | 차단하지 않음 |
| 상세 설정이 필요한 룰 | | |
| Cookie Poisoning | 탐지하지 않음 | 차단하지 않음 |
| Parameter Tampering | Parameter 변조 탐지 | 차단하지 않음 |
| Suspicious Access | 탐지하지 않음 | 차단하지 않음 |

== PSI-DSS 보안 정책 ==

| 룰 이름 | 탐지 | 대응 |
|---------------------------|------------------------|---------|
| Buffer Overflow | 버퍼 공격 탐지 | 에러 코드 |
| Cross Site Scripting | 스크립트 허용 안함 | 에러 코드 |
| Directory Listing | 디렉토리 유출 방지 | 에러 코드 |
| Error Handling | 2차 수준 차단 | 에러 코드 |
| Extension Filtering | 안전한 형식만 접근 가능 | 에러 코드 |
| File Upload | 실행 파일 업로드 금지 | 에러 코드 |
| Include Injection | 파일 Include 탐지 | 에러 코드 |
| Input Content Filtering | 탐지하지 않음 | 차단하지 않음 |
| Invalid HTTP | 위험한 HTTP 차단 | 연결 끊기 |
| Invalid URI | URI 공격 탐지 | 에러 코드 |
| IP Filtering | 탐지하지 않음 | 차단하지 않음 |
| Privacy File Filtering | 중요 개인정보 탐지 | 에러 코드 |
| Privacy Input Filtering | 주민번호 탐지 | 에러 코드 |
| Privacy Output Filtering | 사용자 정의 | 차단하지 않음 |
| Request Header Filtering | 간단한 원 차단 | 에러 코드 |
| Request Method Filtering | 안전한 요청만 처리 | 에러 코드 |
| Response Header Filtering | 서버 정보 유출 방지 | 차단하지 않음 |
| SQL Injection | 확장 SQL Injection 공격 탐지 | 에러 코드 |
| Stealth Commanding | 외부 프로그램 실행 시도 탐지 | 에러 코드 |

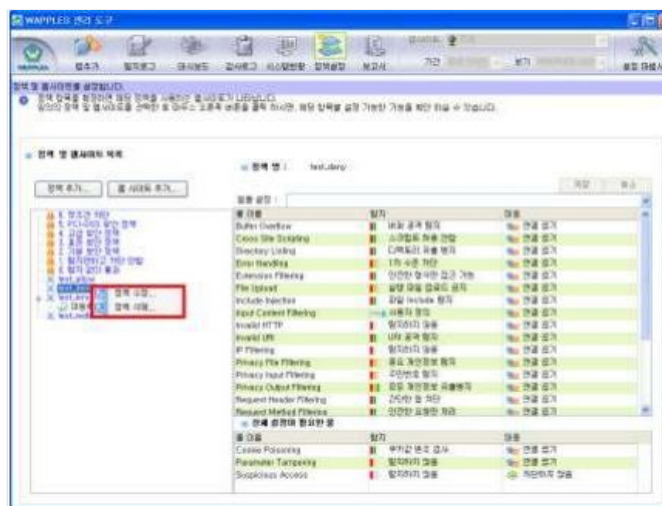
| | | |
|-----------------------------|-----------------|---------|
| Unicode Directory Traversal | 일반 설정 | 에러 코드 |
| URI Access Control | 탐지안함, 학습함 | 에러 코드 |
| User Defined Pattern | 탐지하지 않음 | 차단하지 않음 |
| Website Defacement | 탐지하지 않음 | 차단하지 않음 |
| 상세 설정이 필요한 룰 | | |
| Cookie Poisoning | 탐지하지 않음 | 차단하지 않음 |
| Parameter Tampering | Parameter 변조 탐지 | 에러 코드 |
| Suspicious Access | 1차 수준 차단 | 연결 끊기 |

또한 기본적으로 등록되어 있는 특수 웹 사이트로 [미등록 웹사이트] 가 있습니다. 이 [미등록 웹사이트]는 WAF의 네트워크 구성에서 통과하게 되지만 정책 설정 화면에서 등록되지 않은 웹 사이트를 통칭 하는 것으로 기본적으로 [무조건 차단]정책에 설정 되어 있습니다.

정책 목록 트리뷰에서 정책이나 웹 사이트를 선택 하면 해당하는 정책의 룰 설정 내용을 오른쪽 세부 정보 목록에서 확인 할 수 있습니다.

정책 추가/수정

위의 그림에서 [정책 추가...] 버튼을 클릭하면 새로운 정책을 추가 할 수 있고, 만약 이미 추가된 정책이 있을 경우 [정책 및 웹사이트 목록] 트리뷰에서 사용자가 추가한 정책을 선택하고 마우스의 오른쪽 버튼을 클릭하여 컨텍스트 메뉴의 [정책 수정...]을 선택하면 정책 수정을 할 수 있습니다.



[정책추가...] 버튼을 클릭하면 아래화면이 나타납니다.

정책을 추가할 때 WAF의 기본 정책이나 사용자가 이미 만들어놓은 정책을 사용하려면 기반 정책 선택 콤보 박스에서 기반이 될 정책을 선택하고, 파일에서 인어 오려면 [정책 불러오기...] 버튼을 클릭하면 파일 시스템 내에 저장되었던 정책을 복사해 올 수 있습니다. 불러올 파일형식은 wpc 이며 WAF 웹 사이트 보안 정책 설정 형식의 파일이어야 합니다.

를 설정 화면은 크게 왼쪽의 탐지 설정 부분과 오른쪽의 차단 대응 설정 부분으로 나눌 수 있습니다. WAF의 보안 위반 탐지는 각 룰에 따라 탐지 방법이 다르기 때문에 탐지 설정 부분도 서로 다를 수 밖에 없으며 이를 보다 간단하게 하기 위하여 대부분의 필요한 설정은 슬라이드를 통하여 설정 할 수 있도록 되어 있습니다. 다만 몇 가지 각 사이트의 특성에 맞는 값을 요구하는 룰에 대해서는 슬라이드에서 설정을 선택 할 수 없고 사용자정의로 선택 하여야 합니다. 탐지 대응 설정은 대응과 위험도로 나누어 집니다. 대응은 [차단하지 않음], [페이지 이동], [에러 코드], [연결 끊기]의 4가지 중에 선택 할 수 있고 [페이지 이동]은 이동할 페이지를 [에러 코드]는 에러코드 번호가 필요합니다. 위험도는 점수에 따라 상(50이상)/중(20이상)/하(20이하)의 3단계로 나뉘어지며 해당 룰로 탐지되었을 경우 로그를 분류하기 쉽게 해줍니다. 또한 위험도 점수를 IP별로 누적하여 IP차단 기능에 블랙리스트로 자동 등록 하는데 활용됩니다.

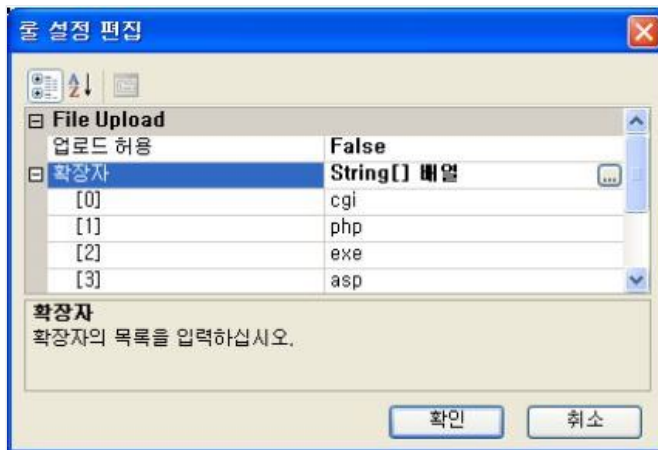


아래화면은 사용자 정의 체크박스에 체크를 하였을 때의 화면입니다. 슬라이드가 없어지고 [사용자 정의 편집하기] 버튼이 나타납니다.



[사용자 정의 편집하기] 버튼을 클릭하면 선택한 룰에 따라 다른 세부 편집화면이 아래와 같이 나타납니다. WAF의 룰에는 사용자 정의 설정이 필요 없어 사용자 정의 체크박스가 나타나지 않는 경우도 있습니다.

각 룰별 사용자 정의 항목에 대한 자세한 설명은 [IV탐지룰의 이해]절 을 참고합니다.



아래화면은 룰 설정을 모두 마치면 나타나는 정책 설정 완료 화면입니다. 설정한 정책의 내용을 보고 정책 내용을 따로 파일로 저장하거나 [확인] 버튼을 클릭하여 정책 추가/변경한 내용을 마칠 수 있습니다. [정책 내보내기...] 버튼을 클릭하면 설정한 정책을 파일로 내보낼 수 있습니다.



화면에서 [확인]버튼을 클릭하면 웹사이트 정책 추가/수정 마법사가 닫히고 화면으로 돌아갑니다.

정책 삭제

등록한 웹 사이트 보안 정책이 잘못 설정되었거나 더 이상 필요가 없을 경우 등록된 웹 사이트 보안 정책을 삭제할 수 있습니다. [정책 삭제...]를 선택하면 사용자가 추가한 정책을 삭제할 수 있습니다. 정책의 삭제는 기호로 표시되는 사용자 추가 정책을 삭제할 수 있으며, 해당 정책을 사용하는 웹 사이트가 없어야 합니다.

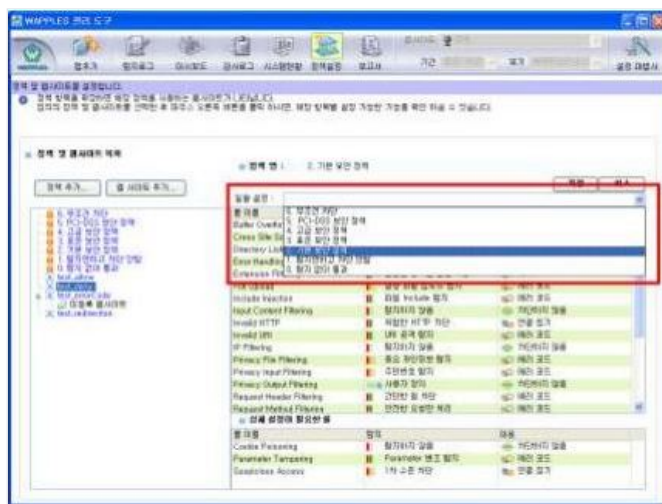
화면에서 삭제할 정책의 내용을 다시 한번 확인하고 하단의 정책 삭제 동의에 체크를 하면 확인 버튼을 누를 수 있습니다.



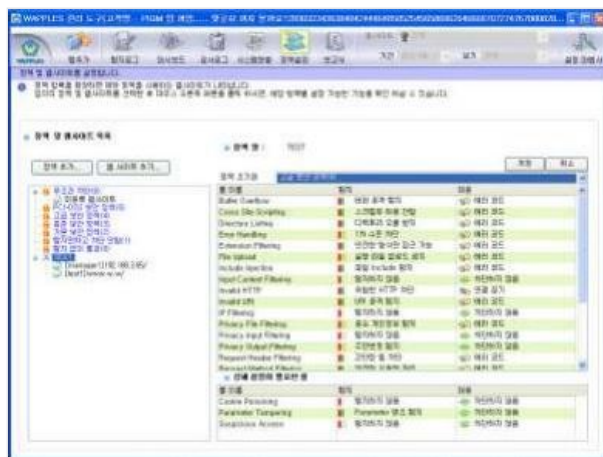
정책을 삭제하면 해당 정책은 복구가 불가능합니다. 해당 정책의 재 사용 및 유지 및 관리를 위해 정책을 삭제하기 전에 [정책내 보내기...] 버튼으로 해당 정책의 내용을 파일로 내보낼 것을 권장합니다.

정책 일괄 설정

일괄 설정기능은 정책을 수정할 경우에 룰을 하나하나 수정하지 않고, 기본 정책으로 일괄 수정하는 기능입니다.



화면에서 초기화할 정책을 선택후 일괄 설정 콤보버튼을 클릭하면 기본 정책들이 표시됩니다. 이중 초기화할 기본 정책을 선택하면 아래 처럼 정책이 수정됩니다.

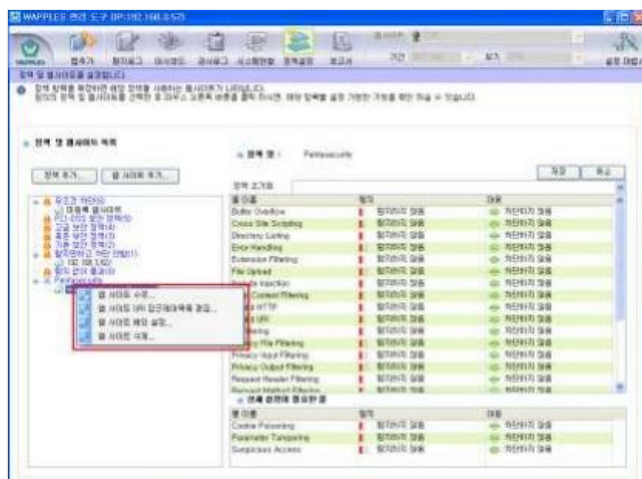


웹사이트 추가 및 수정

[웹 사이트 추가...] 버튼을 사용하고 수정은 수정할 웹사이트를 선택한 다음 컨텍스트 메뉴를 호출하여 [웹 사이트 수정...]을 선택 하면 됩니다.]

WAF 에 추가 가능한 웹 사이트 수는 웹 서비스의 전체 트래픽양에 비례합니다. 따라서, 다량의 트래픽을 발생시키는 웹사이트를 여러 대 추가할 경우 WAF 이 임의로 bypass 될 수 있습니다.

아래 화면은 웹사이트 수정을 위하여 정책 목록에서 정책 부분을 확장하여 웹 사이트가 보이도록 한 다음 웹 사이트에서 마우스의 오른쪽 버튼을 클릭하여 컨텍스트 메뉴를 호출한 모양입니다.



컨텍스트 메뉴는 기본으로 등록되어 있는 웹 사이트나 정책에서는 표시 되지 않습니다. (기본으로 등록 된 '미등록 웹 사이트'의 수정 및 삭제는 불가능 합니다.)

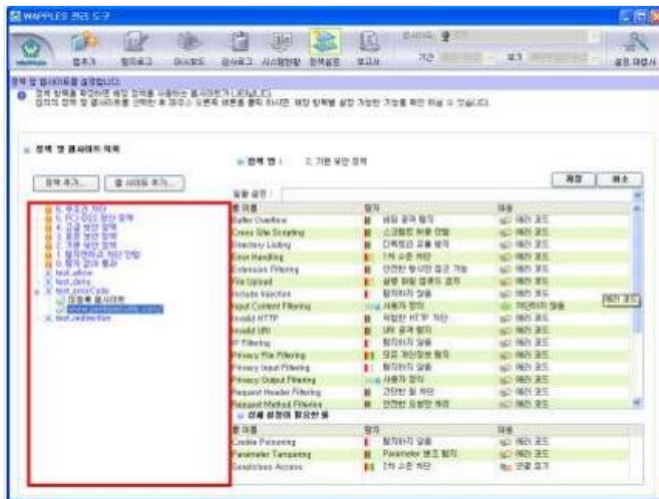
웹 사이트를 추가할 때 경우에 따라 디렉토리를 포함한 가상 웹 사이트가 사용될 수 있습니다. 아래 화면에서 [웹사이트의 Sub Directory 등록]을 체크하면 등록된 웹 사이트를 선택하고 서브디렉토리를 추가하여 가상 웹 사이트를 등록할 수 있습니다.

웹 사이트의 추가와 수정의 방법은 기본적으로 동일 합니다. 다만 추가의 경우 새로운 내용이 추가 되어야 하므로 빈 칸이나 기본 값으로 나오고 수정은 기존에 설정 되었던 값으로 나온다는 점이 다릅니다.

웹사이트 추가/수정 시 입력 방법은 본 매뉴얼의 [III.5.2 웹사이트 추가]절에서 설명합니다.

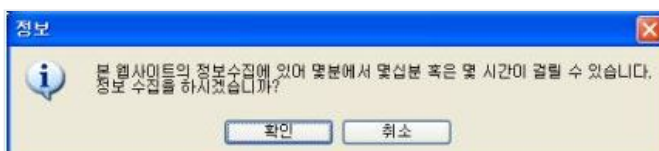
웹사이트의 보안 정책 이동

아래화면에서 "Pentasecurity" 정책에 포함 되어 있던 "www.pentasecurity.com"웹사이트를 "고급 보안 정책"으로 바꾸려고 한다면 단지 "www.pentasecurity.com"을 마우스 왼쪽버튼을 클릭하고 "고급 보안 정책"으로 끌고 와서 놓으면 됩니다. (drag & drop) 이러한 작업은 [저장] 버튼을 클릭하여 변경 사항을 종료하여야 시스템에 적용됩니다



웹사이트 삭제

정책 목록에서 정책 부분을 확장하여 웹 사이트가 보이도록 하고 삭제할 웹 사이트를 선택한 다음 컨텍스트 메뉴를 호출하여 [웹 사이트 삭제...]를 선택합니다.



[확인]을 선택할 경우 삭제를 선택한 웹 사이트의 정보를 아래 같이 수집합니다. 취소를 선택하면 별도의 정보 수집 없이 웹 사이트 삭제를 시작할 수 있습니다.

설정 마법사 - (www.pentasecurity.com)

웹사이트 삭제

설정 확인

다음의 웹사이트를 삭제합니다. 웹사이트를 삭제하면 해당 사이트의 모든 정보 및 탐지로그가 와콤시스템에서 제거됩니다. 삭제가 확실한 경우 아래의 체크박스를 체크합니다.

대상 : www.pentasecurity.com [www.pentasecurity.com]

정보 수집 중

진행률 : [Progress Bar]

취소 < 뒤로 확인

수집이 완료되면 아래화면과 같이 수집된 정보를 화면을 출력합니다. 삭제하고자 하는 웹사이트인지 다시 한번 확인합니다. [네, 웹사이트의 모든 정보와 함께 탐지로그를 삭제합니다.]에 체크를 할 경우 웹사이트의 모든 정보와 함께 탐지로그를 모두 WAF에서 삭제하며 체크하지 않을 경우 탐지로그는 그대로 유지하고 웹사이트의 정보만을 삭제합니다.

설정 마법사 - (demokr.pentasecurity.com)

웹사이트 삭제

설정 확인

웹사이트를 삭제하면 해당 사이트의 모든 설정 정보가 와콤시스템에서 제거되며, 해당 웹사이트의 설정정보와 함께 탐지로그를 삭제할 경우 아래의 체크박스를 체크합니다.

대상 : demokr.pentasecurity.com [demokr.pentasecurity.com]

- + 탐지 로그 261개
- + 웹 사이트의 다른이름 0개
- + 예외처리 URI 0개
- + 접근관리 URI 0개

☒ 네, 웹사이트의 모든 정보와 함께 탐지로그를 삭제합니다.

취소 < 뒤로 확인

웹사이트를 삭제하면 해당 웹사이트와 대시보드를 위한 관련 자료가 모두 소실되므로, 미리 백업을 받은 후 삭제하는 것을 권장합니다.

웹사이트의 정보만을 삭제한 경우 삭제된 웹사이트에 해당하는 로그는 미등록 웹사이트로 관리됩니다.

/br>

[미등록 웹사이트]를 선택하고 오른쪽 마우스 버튼을 클릭하여 [웹사이트 삭제]를 선택하면 삭제하고자 하는 로 그를 선택하여 삭제할 수 있습니다.

설정 마법사 - (unknown_host)

웹사이트 삭제

설정 확인

선택된 미등록 웹사이트의 로그를 삭제합니다.

대상 : Unknown Host [unknown_host]

호스트명 : [모든 웹사이트] (Dropdown menu showing: 모든 웹사이트, demokr.pentasecurity.com, unknown_host)

- + 탐지 로그 5945개
- + 웹 사이트의 다른이름 0개
- + 예외처리 URI 0개
- + 접근관리 URI 0개

취소 < 뒤로 확인

탐지 예외 설정 변경

WAF은 보호 대상 웹 서버의 독립적인 특성에 따라 탐지 하지 말아야 할 [탐지 예외 설정 기능]을 제공합니다. [탐지 예외 설정 기능]을 사용하여 인가된 운영자는 보호 대상 웹 서버의 특성에 맞게 웹 사이트 보호 정책을 구성 할 수 있습니다.

정책 목록에서 정책 부분을 확장하여 웹 사이트가 보이도록 하고 변경할 웹 사이트를 선택한 다음 컨텍스트 메뉴를 호출하여 [웹사이트 예외 설정...]을 선택합니다.

탐지 예외 설정은 아래와 같은 화면에서 설정 합니다. 설정란의 숫자는 각 룰에 대하여 예외처리가 되어 있는 URL의 개수입니다.



하나의 룰을 선택하고 [다음] 버튼을 클릭하면 아래 같은 화면이 나타납니다.

URI 입력란에 예외로 처리할 URI와 IP입력란에 예외 IP대역을 입력한 다음 [추가]버튼을 클릭하여 예외를 추가 할 수 있습니다. 예외 설정은 URI와 IP의 조합으로 설정 됩니다. IP는 IP/Netmask 로도 쓸 수 있습니다. 예외 처리할 URL의 마지막 글자가 "/" 인 경우에는 주어진 URL의 모든 하부 URL 들이 동시에 예외 처리가 됩니다. 이외의 글자가 마지막인 경우에는 오로지 주어진 URL에 대해서만 예외 처리가 이루어집니다

예외 목록에서 예외 항목을 선택하면 URI/IP 입력란에 선택한 예외 항목이 표시되고, 목록을 선택한 후[수정]버튼을 클릭하여 내용을 수정하거나 [삭제]버튼을 클릭하여 삭제할 수 있습니다.



예외 목록을 작성하고 [다음]을 클릭하면 아래와 같은 설정 확인 화면이 나타나고 [확인]버튼을 클릭하면 탐지 예외설정이 완료됩니다.



URI Access Control룰과 밀접한 관련이 있습니다. URI Access Control 룰에 보안도가 탐지함으로 되어 있다면, URI 접근 제어 목록에 등록되어 있지 않는 URI를 웹 사용자가 요청한 경우 모두 불법으로 간주하여 탐지하게 됩니다.

URI 접근 제어 목록에 등록된 URI는 공개, 또는 비공개 속성을 가집니다. URI가 [공개] 속성을 가질 때는 모든 사용자에게 해당 URI에 대한 접근을 허용하고, [비공개]로 설정되면, [웹사이트 추사 및 수정]에서 등록한 [신뢰 IP]에서의 접근만 허용합니다.

URI 접근 제어 목록 편집기능은 다음과 같이 사용합니다. 정책 목록에서 정책 부분을 확장하여 웹 사이트가 보이도록 하고 삭제할 웹 사이트를 선택한 다음 컨텍스트 메뉴를 호출하여 [웹사이트 URI 접근 제어 목록 편집...]을 선택하면 아래 같은 URI 접근 제어 목록 관리 화면이 나타납니다.

URI 접근 제어 목록 관리 화면은 상단의 검색 및 추가부분과 하단의 목록 부분으로 나눌 수 있습니다. URI 입력 창과 [공개], [비공개], [Broken 연결] 체크박스 검색할 내용을 넣고 [검색]버튼으로 필요한 부분의 URI를 검색할 수 있습니다.

URI 목록의 [제한] 컬럼은 해당 URI가 공개 페이지, 공개 디렉토리 페이지, 비공개 페이지, 비공개 디렉토리 페이지인지를 표시하는 컬럼입니다. 컬럼의 아이콘 위에 마우스를 올려놓으면 해당 URI의 공개 페이지, 공개 디렉토리 페이지, 비공개 페이지, 비공개 디렉토리 페이지 정보가 표시됩니다.

[Broken연결]은 웹 서버 운영 중, 페이지가 없어지거나, 이름이 변경되어, URI 접근 제어목록과 웹사이트의 URI가 일치하지 않는 것을 의미하며,[Broken 연결]컬럼에 아이콘이 표시됩니다. 실제로 웹 서버에서 더 이상 관리하는 페이지가 아닌 경우, 컨텍스트 메뉴의 삭제 기능을 이용하여 [Broken 연결]된 URI를 제거할 수 있습니다.

URI를 접근 제어 목록에 URI를 등록하는 방법은 두 가지가 있습니다. URI 입력 창에 등록할 URI를 입력한 후, [추가] 버튼을 클릭하는 방법과 [URI 파일 불러오기...] 버튼을 클릭하면 웹 서버에서 직접 조회한 URI의 목록을 파일로 만들어 바로 일괄등록 할 수 있습니다.

URI등록 시 입력된 URI의 맨 오른쪽 끝자리가 "/"로 끝날 경우 기본적으로 공개 디렉토리 페이지로 등록되며 입력된 URI의 맨 오른쪽 끝자리가 "/"로 끝나지 않을 경우 공개 페이지로 등록됩니다. 추가된 URI는 URI목록에서 마우스의 오른쪽 버튼을 클릭하여 컨텍스트 메뉴를 실행하여 전환할 수 있습니다.

입력된 URI의 맨 오른쪽 끝자리가 "/"는 해당 URI의 하위URI를 모두 포함하는 의미로써 공개 디렉토리 페이지로 등록됩니다. URI 등록 시 "*"는 등록되지 않습니다.

설정 마법사는 운영자가 입력한 접근 가능 URI에 대하여 오류가 있을 경우 다음과 같은 오류 메시지를 출력합니다.

URI 접근 제어 오류 메시지

| 오류 메시지 | 출력 원인 |
|---------------|--|
| 중복된 이름이 있습니다. | URI 접근 제어 목록 추가 시 추가 할 URI와 동일한 URI가 URI 접근 제어 목록에 존재 할 경우 |

또한 등록된 URI를 검색하고 싶을 때에는 URI 입력 창에 검색할 URI를 입력한 후 검색 버튼을 클릭하면 목록 화면에 검색 결과가 출력됩니다.



아래에서 보는 바와 같이 조회한 URI의 목록에서 마우스의 오른쪽 버튼을 클릭하여 컨텍스트 메뉴를 실행한 후 [공개 페이지]/[비공개 페이지]/[공개 디렉토리 페이지]/[비공개 디렉토리 페이지]로 전환 또는 [목록에서 삭제]

기능을 수행 할 수 있습니다.



웹사이트에서 학습되거나 추가된 URI의 리스트에서 접근을 제한하고자 하는 URI를 선택하고 마우스의 오른쪽 버튼을 클릭하여 컨텍스트 메뉴를 실행한 후 [비공개 페이지로 설정]을 선택합니다.

해당 URI 맨 오른쪽 끝자리가 [/] 끝나고 하위 URI 모두 접근을 제한하고자 할 경우 [비공개 디렉토리 페이지로 설정]을 선택합니다.

공개/비공개/공개 디렉토리/비공개 디렉토리 페이지는 아이콘으로 표기되며 해당 아이콘에 마우스를 올려 놓을 경우 설명이 표시됩니다.



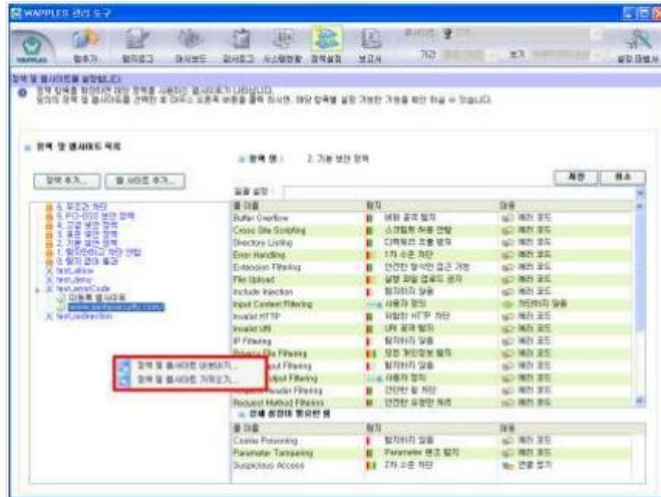
화면에서 [다음] 버튼을 클릭하면 아래와 같은 설정한 내용을 확인하고 학습된 URI목록을 파일로 내보낼 수 있습니다. [확인]을 클릭하면 URI 접근제어 목록 편집이 완료됩니다.



정책 및 웹사이트 가져오기/내보내기

WAF의 정책 및 웹사이트 가져오기/내보내기 기능은 도구바의 정책설정 뷰에서 관리하는 보안 정책과 웹사이트에 대한 정보를 일괄적으로 저장하거나 불러오기 하여 적용할 수 있는 기능입니다. 본 기능은 아래화면의 [정책 트리] 레이아웃 중 빈 공간에서 마우스 우측 클릭을 하여 [정책 및 웹 사이트 내보내기] 와 [정책 및 웹사이트 가져오기] 툴팁 창을 보이게 한 다음 아래 기능을 수행합니다.

- 정책 및 웹사이트 내보내기 [정책 및 웹사이트 내보내기] 버튼을 누르면 파일을 저장할 수 있는 마법사가 나타나며, 파일이름을 정한 후, 저장 버튼을 클릭하면 현재 [정책 및 웹사이트]가 파일로 저장됩니다.
- 정책 및 웹사이트 가져오기 [정책 및 웹사이트 가져오기] 버튼을 누르면 환경 설정 내용 파일을 가져올 수 있는 마법사가 나타나며, 파일을 선택하면 Export된 정책 파일의 정책 및 웹사이트가 적용됩니다.



설정마법사

WAF 관리도구에서 설정 사항의 대부분은 마법사 형태로 되어 있습니다. 일반적으로 복잡해지기 쉬운 정보보호 관련 제품을 보다 쉽게 설정 할 수 있도록 고안되었습니다. 설정 마법사를 통하여 설정 하고자 하는 방향으로 선택해 가면 쉽게 WAF의 관리포트 IP와 관련된 항목을 제외한 모든 항목에 대한 설정할 수 있습니다.

설정 마법사의 구성은 다음과 같습니다.

| 대분류 | 소분류 |
|---------|--------------------|
| 운영설정 | 계정 관리 |
| | 백업 설정 |
| | 세션 잠금 및 감사 설정 |
| | 연동 설정 |
| | IP 차단 설정 |
| | 정책/로그 동기화 |
| | 라이선스 설정 |
| | 패턴 저장소 |
| | 시간 동기화 |
| | IP/PORT 접근제어 |
| 네트워크 설정 | E-MAIL 설정 |
| | WAF 서비스 포트 설정 |
| | WAF의 보호 대상 웹 서버 관리 |

설정 마법사는 WAF 관리도구에 로그인 후 WAF 메인 화면에의 우측 상단의 [설정마법사] 버튼을 클릭하여 기동할 수 있습니다. 기동된 설정 마법사는 화면과 같이 표시되고 [운영 설정] / [네트워크 설정] 중 하나를 선택하고 다음을 클릭하면 해당 소분류로 이동할 수 있습니다.



운영 설정

화면에서 운영 설정 아이콘을 선택하고 다음을 클릭하면 다음과 같이 운영 설정 소분류 화면을 확인할 수 있습니다.

[계정 관리]

조회자의 ID 및 웹사이트 관리자 ID를 관리 하기 위해 사용합니다. 인가된 운영자는 조회자의 ID, 웹사이트 관리자 ID를 추가 및 삭제 할 수 있습니다.

[백업 설정]

탐지로그 및 감사로그와 설정 마법사를 이용하여 설정한 모든 자료를 원하는 시기에 자동으로 백업할 수 있습니다.

[세션 잠금 및 감사 설정]

관리자가 WPPLES 관리도구에 로그인 한 상태로 장시간 자리를 비웠을 때 보안을 위하여 일정 시간 이후 자동 관리도구를 사용하지 하도록 설정하는 기능과 감사 기록의 수준을 설정할 수 있습니다.

[연동 설정]

WAF과 SNMP (Simple Network Management Protocol) TRAP과의 연동을 설정할 수 있습니다.

[업데이트 설정 및 실행]

WAF의 최신 보안 패치를 자동으로 또는 수동으로 업데이트 할지 를 설정할 수 있습니다.

[IP 차단 설정]

IP차단은 하나의 출발지에서 계속하여 공격을 시도하는 것을 막기 위해 사용합니다.

[패턴 저장소]

탐지를 위한 패턴의 저장소로, User Define Pattern Rule의 패턴 탐지를 위해 사용될 패턴을 등록 및 삭제 수정할 수 있습니다.

[시간 동기화 설정]

WAF의 시스템 시간을 동기화하기 위하여 시간 서버를 등록하고, 표준 시간대를 설정할 수 있습니다.

[IP/PORT 접근 제어]

IP/PORT 접근 제어는 설정한 출발지에서 설정한 도착지로 가는 트래픽에 대한 접근을 허용 또는 거부할 수 있습니다.

[라이선스 설정]

라이선스 설정은 WAF 3.0R5이후 버전에 대해 반드시 설정해야 하는 항목으로 입력된 라이선스에 따라 WAF는 기능을 제한할 수 있습니다.

[E-MAIL 설정]

WAF에서 E-MAIL 전송으로 서비스하고 있는 기능의 송신측 EMAIL주소 및 SMTP 주소를 설정합니다.

[정책/로그 동기화]

정책 및 로그 동기화 설정과 동기화할 WAF의 접속 정보를 설정할 수 있습니다.



세션 잠금 및 감사 설정

[감사 설정]은 감사 수준별 감사로그를 기록하기 위해 인가된 관리자에게 보여지는 감사 기록의 수준을 선택할 수 있는 기능입니다.

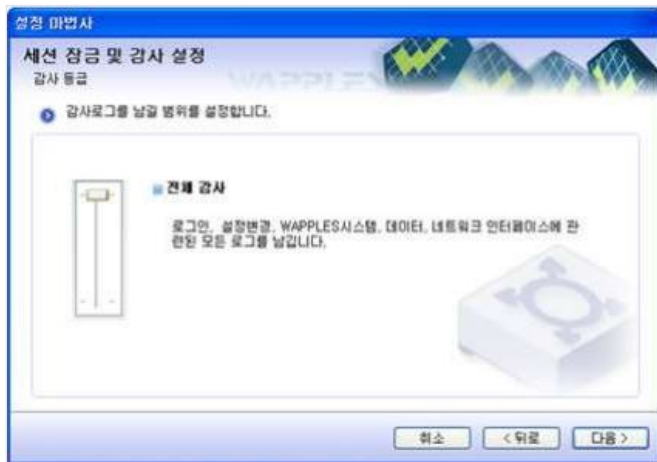
감사 등급은 [기본감사]와 [전체감사]가 있으며 각각의 의미와 감사 항목은 아래 표에서 설명합니다.

감사 수준별 감사 항목

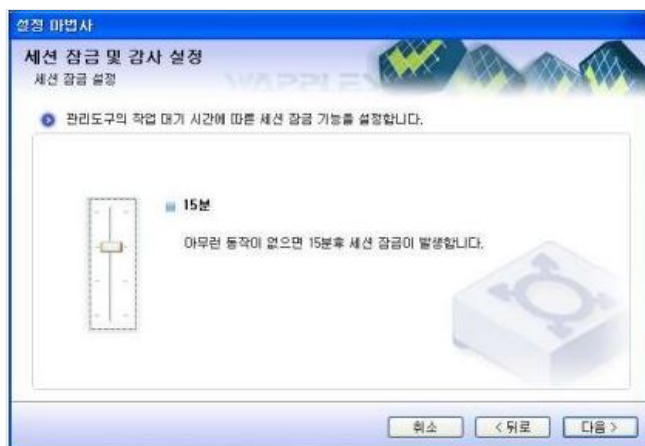
| 감사 수준 | 설명 | 감사 항목 |
|-------|--|---|
| 기본감사 | WAF 시스템의 중대한 사건이나 변경사항에 대한 감사 자료를 기록합니다. | DB용량 위험/초과, 연동모드, 웹 사이트 추가/수정/삭제, 룰 예외처리 변경, 접근설정 변경, 로그 리뷰, 업데이트 설정, 업데이트 성공, 세션 잠금 설정 변경, 감사설정, WAF IP, 라우팅 테이블, 웹 서버, 정책 이름, 정책 룰, 백업 설정/성공/실패, 로그 삭제, 로그인 실패/연속실패, 비밀번호 변경/실패, 세션 잠금 실패, WAF 시작/정지, 무결성 검사 실패, 관리포트설정 변경, 백업 설정, 네트워크 인터페이스 오류, 보안 경보, 조회자 아이디 추가/삭제, 시간동기화 설정 변경, 시간동기화 성공/실패, 표준 시간대 변경/실패, 패턴저장소 설정 변경, 정책/로그 동기화 설정/결과, 보고서 메일 보내기 성공/실패, 기능별 라이선스 등록 성공/실패 |
| | | |

| | | |
|------|--|--|
| 전체감사 | 기본 감사 항목 외에 일반적인 정보 및 주기적인 점검 사항의 정상 작동에 관한 내용까지 감사 자료로 기록합니다. | 기본 감사 수준의 감사 항목 및 업데이트 강제 수행, IP 차단/관리목록 설정, 조회자 추가 및 삭제, 로그아웃, 세션 잠금, 세션 잠금 해제, WAF 시작/정지, 무결성 검사 성공, 관리포트 설정 변경, |
|------|--|--|

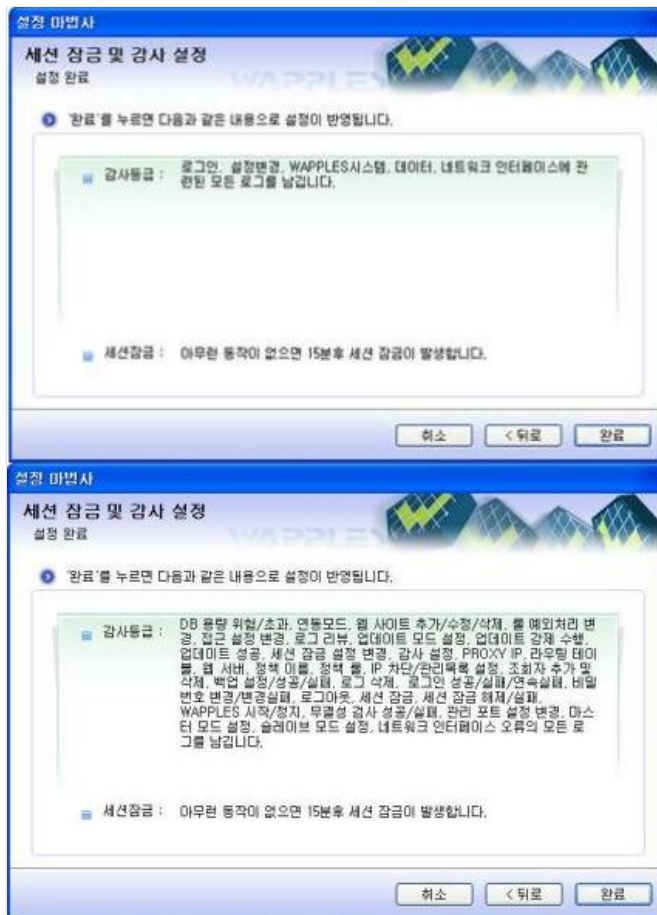
화면에서 [세션 잠금 및 감사 설정]을 선택하고 [계속]버튼을 클릭하면[오류! 참조 원본을 찾을 수 없습니다.]화면이 나타납니다.



[감사 등급 설정]화면에서 슬라이드 바를 상하로 끌어서 기본 혹은 전체 감사상태로 바꾼 후 [다음] 버튼을 클릭합니다



[세션 잠금 설정]은 관리자가 WPPLES 관리도구에 로그인 한 상태로 장시간 자리를 비웠을 때 보안을 위하여 일정 시간 이후 자동으로 관리 도구에 접근을 차단하는 기능입니다. [세션 잠금 설정] 화면에서는 세션 잠금이 발생하는 시간을 5분/15분/30분/사용안함 으로 조절 할 수 있습니다.



[세션 잠금 설정] 화면에서 [다음] 버튼을 클릭하면 **[오류! 참조 원본을 찾을 수 없습니다.오류! 참조 원본을 찾을 수 없습니다.]**화면이 나타납니다. [완료] 버튼을 클릭하면 세션 잠금 및 감사 설정이 저장 되어 WAF에 반영됩니다.

세션 잠금 기간 설정을 하면 설정된 시간 동안 WAPPLES 관리도구 프로그램에 키보드 입력이나 마우스 클릭이 없을 경우 WAF 관리도구와 WAF간의 연결이 끊어지고 **[오류! 참조 원본을 찾을 수 없습니다.]**화면이 나타납니다.

[오류! 참조 원본을 찾을 수 없습니다.]화면에서 세션 잠금을 해제하거나 관리도구를 종료할 수 있습니다. 관리도구를 다시 사용하려면 암호를 재 입력하고 [세션 잠금 해제]버튼을 클릭합니다.

[오류! 참조 원본을 찾을 수 없습니다.]화면은 아이디는 입력할 수 없으며 비밀번호 입력만을 허용합니다. 로그인 방법은 아이디와 비밀번호 변경 체크박스를 입력할 수 없을 뿐 [III.1.1 로그인] 과 동일합니다.



백업 설정

WAF에 기록된 설정 정보, 탐지 로그 및 감사로그를 WAF 시스템 혹은 외부의 FTP서버로 백업 데이터를 저장하기 위해 [백업 설정] 기능을 사용합니다.

백업단위는 매일, 매주, 매월, 사용 안 함을 설정할 수 있습니다.

매일 백업을 원할 경우 백업시간을 입력하고 매주 백업을 원할 경우 원하는 요일과 백업 시간을 입력합니다. 매월 백업을 원할 경우 백업 날짜와 시간을 입력합니다.

백업은 FTP를 사용하여 백업 데이터를 전송합니다. FTP 사용에 필요한 정보인 FTP 서버 IP, FTP 서버 경로, FTP 아이디, FTP 비밀번호를 입력합니다.

백업 설정 오류 메시지

| 오류 메시지 | 출력 원인 |
|-------------------|---|
| 하나 이상의 요일을 선택합니다. | 백업단위를 [매주]로 선택 시 하나 이상의 요일에 체크하지 않았을 경우 |
| 빈칸일 수 없습니다. | Remote 백업 선택 시 FTP 서버 IP, FTP 서버 경로, FTP 아이디, FTP 비밀번호 입력 값이 빈칸일 경우 |
| 잘못된 IP 입니다. | FTP 서버 IP 가 올바른 IP형식이 아닐 경우 |

[오류! 참조 원본을 찾을 수 없습니다.] 화면에서 [다음] 버튼을 클릭하면 **[오류! 참조 원본을 찾을 수 없습니다.]** 화면이 나타납니다.

다운로드 받을 백업파일을 선택 후, [다운로드]버튼을 누르면 백업파일을 다운로드합니다. [업로드] 버튼을 누르고 백업파일을 선택한 후 열기 버튼을 누르면 백업파일을 시스템에 업로드 합니다.

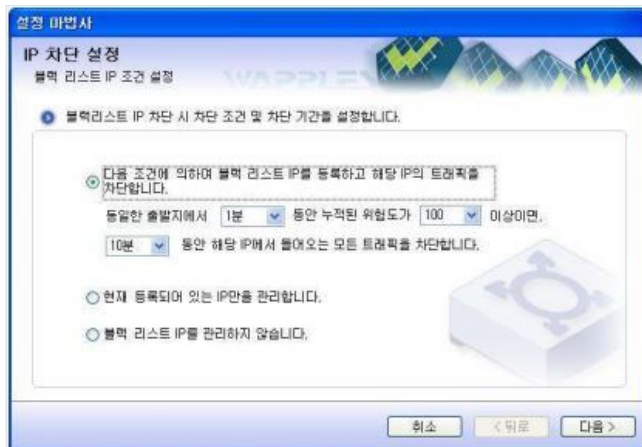
[오류! 참조 원본을 찾을 수 없습니다.] 화면에서 다음 버튼을 클릭하면 **[오류! 참조 원본을 찾을 수 없습니다.]**과 같은 [설정 완료] 화면이 나타납니다. 이 화면에서 설정 내용을 확인하고 [완료] 버튼을 클릭합니다.



IP 차단 설정

IP차단은 하나의 출발지에서 계속하여 공격을 시도하는 것을 막기 위해 사용됩니다. WAF은 같은 출발지에서 발생한 공격을 탐지하여 차단한 사건에 대하여 시간당 위험도를 점수로 기록하고 누적 점수가 설정치 이상이 되었을 때 일정시간 그 출발지에서 발생하는 모든 트래픽을 차단 하도록 합니다.

이 화면에서 IP 차단 관리목록에 대한 IP 관리 기능을 활성화 할지 여부를 선택하고, 활성화 한다면 어떠한 조건으로 IP 차단 관리목록을 등록하고 얼마나 오랫동안 관리한지 혹은 현재 등록되어 있는 IP만을 관리 할지를 설정할 수 있습니다.



[다음] 버튼을 클릭하면 [오류! 참조 원본을 찾을 수 없습니다.]화면이 나타납니다. 다음과 같은 항목을 설정할 수 있습니다.

- 연결 차단 IP/연결 차단 시간
- 연결 허용 IP /연결 허용 시간

[특정 IP 혹은 IP 대역에 대해 일정 시간 동안 연결을 차단하거나 허용 할 수 있습니다. 설정을 원하는 IP와 연결 차단 혹은 연결 허용할 시간을 입력하고 [해당 IP 연결 허용] 체크 박스에 허용 유무를 체크한 뒤 추가 버튼을 사용하여 관리 IP를 관리 IP 목록에 추가합니다.



설정된 IP의 수정/삭제는 IP 리스트에서 삭제할 IP를 선택하고 [수정]/[삭제] 버튼을 누른 후 [다음]을 클릭하면, 설정 요약 화면이 나타납니다. 설정한 내용을 다시 한번 확인하고 [완료] 버튼을 클릭하면 IP차단 설정 내용이 WAF에 적용됩니다.

설정 마법사는 IP 차단 설정 시 사용자 입력 값에 오류가 있을 경우 다음과 같은 오류 메시지를 출력합니다.

로그인 오류 메시지

| 오류 메시지 | 출력 원인 |
|-----------------------------|-------------------------------------|
| 잘못된 IP입니다. | 관리 IP 추가/수정 시 입력된 IP가 IP형식이 아닐 경우 |
| 현재 시간부터 5분 이상을 설정 할 수 있습니다. | 설정된 시간이 현재 시간부터 5분 이상의 미래 시간이 아닐 경우 |

IP 관리 종료 예정 시간은 현재의 시간보다 5 분 이상의 미래의 시간을 입력해야 합니다.



IP차단을 위한 위험도 설정은 정책설정의 모든 룰에서 설정이 가능합니다. 다음은 Buffer Over Flow 룰의 위험도 설정 화면입니다. 대응 하단의 위험도를 각 룰의 점수를 설정합니다.



룰의 위험도 설정은 탐지 프로세스에 적용되기 때문에 '탐지'와 '사용자정의' 설정에서만 수정이 가능하고, '탐지안함' 상태에서는 위험도 수치를 설정할 수 없습니다.

E-MAIL 설정

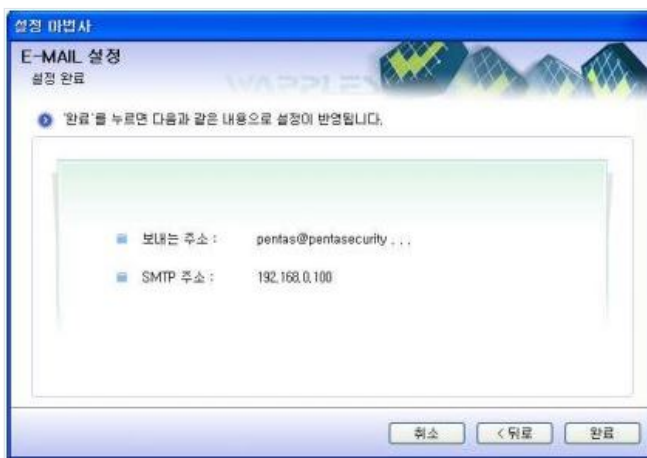
[오류! 참조 원본을 찾을 수 없습니다. 오류! 참조 원본을 찾을 수 없습니다.]과 [IX 설정마법사 오류! 참조 원본을 찾을 수 없습니다. 오류! 참조 원본을 찾을 수 없습니다.]의 [탐지로그 연동] 기능에서 사용하는 EMAIL 관련 정보를 설정할 수 있습니다.

[운영 설정]에서 [E-MAIL 설정]을 클릭하면 다음과 같은 화면이 나타납니다.



보내는 주소는 E-MAIL 발신자의 E-MAIL 주소를 의미하며, SMTP 주소는 SMTP 서버의 IP 주소를 의미합니다.

설정이 끝난 후, 화면 우측 하단의 [다음>]버튼을 클릭합니다. [오류!참조 원본을 찾을 수 없습니다.]이 나타나면 설정된 내용을 확인한 후 화면 우측 하단의 [완료] 버튼을 클릭합니다.



계정 관리

WAF은 시스템 감사 항목 및 보안 위반 발생 항목을 조회 할 수 있는 조회자와 웹사이트를 관리 할 수 있는 [웹사이트 관리자] 기능을 제공합니다.

조회자 관리

[계정 관리]를 선택하면 아래화면이 나타납니다.



관리하고자 하는 계정이 조회자인 경우 [조회자 관리]를 선택하고 다음을 클릭하면 아래 화면이 출력됩니다.

추가하고자 할 아이디를 입력하고 [+] 버튼을 클릭하면 등록된 조회자 아이디 목록에 조회자 아이디가 추가되며 추가된 아이디의 비밀번호는 기본적으로 "penta"로 추가됩니다. 이 비밀번호로 인하여 조회자는 최초 로그인 시 도 시 비밀번호를 변경하여야 하며 비밀번호 변경 취소 시 관리도구는 종료됩니다.

아이디는 영문과 숫자만을 사용할 수 있으며 반드시 알파벳으로 시작해야 합니다. 알파벳은 소문자만 가능하며 대문자로 입력 시 자동으로 소문자로 입력됩니다. ID에는 특수문자가 들어갈 수 없으며 4자 이상 10자 이하로 입력해주셔야 합니다.

조회자 아이디는 이미 존재하고 있는 동일한 아이디를 추가할 수 없으며 조회자 아이디는 다음과 같이 추가됩니다.

삭제하고자 한 아이디를 등록된 조회자 아이디 목록에서 선택한 후 [-] 버튼을 클릭합니다.

설정 마법사는 조회자 ID 관리 설정 시 사용자 입력 값의 오류에 대하여 다음의 메시지를 출력합니다.

조회자 ID 관리 오류 메시지

조회자는 탐지로그, 감사로그, 대시보드 메뉴만 사용할 수 있습니다.

웹사이트 관리자 설정

관리하고자 하는 계정이 보안 웹사이트별 관리자인 경우 화면에서 [웹사이트 관리자 설정]을 선택하고 [다음]버튼을 클릭하면 아래화면이 나타납니다.

화면에서는 웹사이트 관리자에 대하여 추가/수정/삭제를 할 수 있습니다.

[추가] 버튼을 클릭하면 아래화면이 출력됩니다.

추가하고자 할 관리자의 필수 입력 사항인 이름, 아이디, 비밀번호, 소속, 이메일, 유효기간을 입력합니다.

필수 입력 사항은 입력하지 않으면 다음 설정을 진행할 수 없습니다.

유효기간이 만료된 웹사이트 관리자는 더 이상 WAF 관리도구에 로그인 할 수 없습니다.

[로그인시 비밀번호를 변경하도록 지시합니다.] 체크박스에 체크를 할 경우 해당 웹사이트 관리자는 로그인시 비밀번호 변경화면이 나타나며 변경할 때까지 로그인 시마다 비밀번호 변경 화면이 출력됩니다.

추가입력 사항은 필요사항에 대해서만 입력하고 반드시 입력할 필요는 없습니다.

속성의 [인기 전용] 항목을 체크할 경우 추가하고자 하는 웹사이트 관리자는 WAF 시스템의 설정사항을 변경할 수 없는 조회자 모드로 동작하게 됩니다.

보안 정책별 관리자 ID 관리 오류 메시지

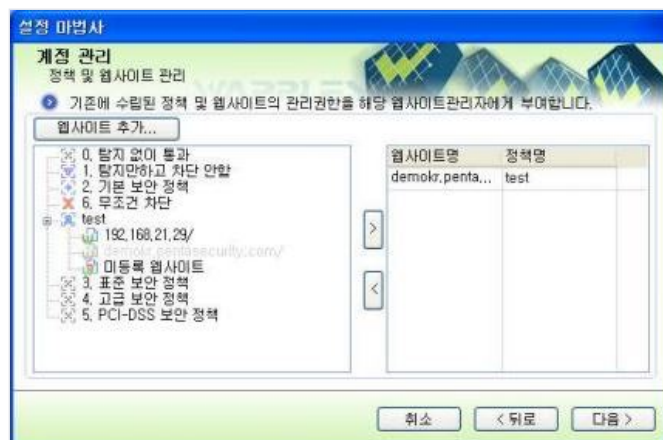
| 오류 메시지 | 출력 원인 |
|-------------------------------|--|
| 더 이상 추가하실 수 없습니다. | 아이디를 추가할 때 이미 조회자 아이디가 5개 이상 존재할 경우 |
| 빈칸일 수 없습니다. | 입력한 조회자 아이디가 빈칸일 경우 |
| {추가할 아이디} 는 현재 접속하고 있는 ID입니다. | 입력한 조회자 아이디가 관리도구에 접속해 있는 운영자 아이디와 같을 경우 |

| | |
|--------------------------|--|
| 조회자로 추가된 아이디입니다. | 입력한 조회자 아이디가 이미 조회자 아이디로 등록되어 있는 경우 |
| 보안 정책별 관리자로 추가 된 아이디입니다. | 입력한 조회자 아이디가 이미 보안 정책별 관리자 아이디로 등록되어 있는 경우 |
| ERROR | 네트워크 문제상 조회자 아이디를 추가 할 수 없는 경우 |

| 오류 메시지 | 출력 원인 |
|--|--|
| 빈칸일 수 없습니다. | 입력한 조회자 아이디가 빈칸일 경우 |
| 아이디는 영문과 숫자만을 사용할 수 있으며 반드시 알파벳으로 시작해야 합니다 | 아이디에 특수문자 또는 아이디 규칙에 맞지 않을 경우 |
| 아이디는 4자 이상 10자 이하를 입력하여야 합니다 | 4자 이하 또는 10자 이상으로 아이디 규칙에 맞지 않을 경우 |
| {추가할 아이디} 는 이미 존재하는 아이디 입니다. | 이미 추가된 조회자 아이디 또는 운영자 아이디 일 경우 |
| {추가할 아이디} 는 현재 접속하고 있는 ID입니다. | 입력한 조회자 아이디가 관리도구에 접속해 있는 운영자 아이디와 같을 경우 |
| 조회자로 추가된 아이디입니다 | 입력한 조회자 아이디가 이미 조회자 아이디로 등록되어 있는 경우 |
| 웹사이트 관리자로 추가된 아이디입니다. | 입력한 조회자 아이디가 이미 보안 정책별 관리자 아이디로 등록되어 있는 경우 |
| ERROR | 네트워크 문제상 조회자 아이디를 추가 할 수 없는 경우 |

[다음] 버튼을 클릭하면 아래화면이 출력됩니다. 왼쪽의 [정책 및 웹사이트 트리 뷰]에서는 인가된 운영자의 정책과 할당되지 않은 웹사이트 목록이 표시됩니다. 웹사이트 관리자에게 할당하고자 할 웹사이트를 선택하고 [>] 버튼을 클릭하면 해당 웹사이트를 해당 웹사이트 관리자에게 할당할 수 있습니다.

왼쪽의 [정책 및 웹사이트 트리 뷰]에서 할당된 웹사이트는 비활성화로 표시되며 오른쪽 [웹사이트 리스트 뷰]에서 할당된 웹사이트를 확인 할 수 있습니다.



할당하고자 하는 웹사이트를 모두 할당하고 [다음]버튼을 클릭하면 아래화면이 출력됩니다.

설정 사항을 확인하고 [완료] 버튼을 누르면 웹사이트 관리자가 추가됩니다.

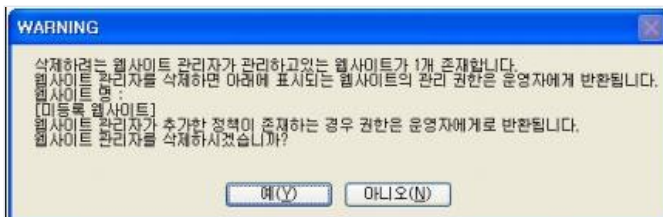


화면에서 [수정] 버튼을 클릭할 경우 해당 웹사이트 관리자에게 설정된 사항을 변경 수정할 수 있습니다. 기본적인 입력하상으로는 웹사이트 관리자 추가할 때와 같으며 아래 화면과 같이 아이디만 변경 불가능합니다.

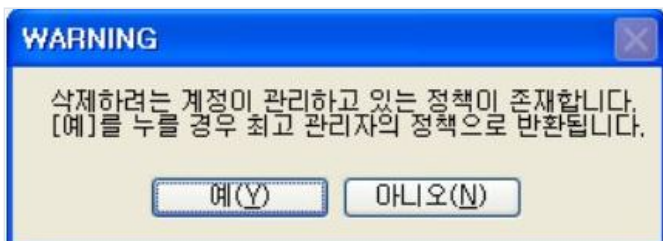


화면에서 삭제하고자 하는 관리자를 선택하고 [삭제] 버튼을 클릭할 경우 해당 웹사이트 관리자를 삭제 할 수 있습니다.

삭제할 웹사이트 관리자에게 할당된 웹사이트가 존재하면 다음과 같은 경고 메시지가 출력됩니다.



삭제할 웹사이트 관리자가 추가한 정책이 존재하면 다음과 같은 경고 메시지가 출력됩니다.



웹사이트 관리자는 다음과 같은 주요 특징을 가지고 있습니다.

- 웹사이트 관리자는 할당된 웹사이트 개수 * 2 만큼의 정책을 추가하여 사용할 수 있습니다.
- 웹사이트 관리자는 자신이 추가한 정책에 대해서만 수정 권한을 가집니다.
- 웹사이트 관리자는 다른 웹사이트 관리자가 생성한 정책을 보지 못합니다.
- 웹사이트 관리자는 운영자의 정책을 사용할 수 있지만 수정할 수 없습니다.
- 웹사이트 관리자는 탐지로그, 대시보드, 감사로그, 보고서 작성 메뉴를 이용할 수 있습니다.

운영자 관리

관리하고자 하는 계정이 조회와 설정이 모두 가능한 운영자 권한을 가진다면 화면에서 [운영자 설정]을 선택하고 [다음] 버튼을 클릭하면 아래화면이 나타 납니다. 운영관리자는 탐지로그, 대시보드, 감사로그, 보고서 작성 메뉴를 이용할 수 있습니다.

추가하고자 할 아이디를 입력하고 [+] 버튼을 클릭하면 등록된 운영자 아이디 목록에 운영자 아이디가 추가되며 추가된 아이디의 비밀번호는 기본적으로 "penta"로 추가됩니다. 이 비밀번호로 인하여 운영자는 최초 로그인 시 도 시 비밀번호를 변경하여야 하며 비밀번호 변경 취소 시 관리도구는 종료됩니다.

아이디는 특수문자를 제외한 대소문자 구분 없는 영문 또는 숫자만 허용되며 4 자 이상 10 자 이하를 입력하여야 합니다

운영자 아이디는 이미 존재하고 있는 동일한 아이디를 추가할 수 없으며 운영자 아이디는 위 조회자 아이디 추가 방법과 동일합니다.

삭제하고자 할 아이디를 등록된 운영자 아이디 목록에서 선택한 후 [-] 버튼을 클릭합니다.

설정 마법사는 운영자 ID 관리 설정 시 사용자 입력 값의 오류에 대하여 다음의 메시지를 출력합니다.

운영자 ID 관리 오류 메시지

연동 설정

[연동 설정]에서는 WAF과 SNMP (Simple Network Management Protocol) TRAP, SIMS(Security Information Management System), E-MAIL, SYSLOG 연동을 설정합니다.

SNMP연동

[오류! 참조 원본을 찾을 수 없습니다.]화면에서 [SNMP 연동을 합니다] 라고 되어 있는 체크박스에 연동 여부에 대한 설정을 합니다. 이 체크박스에 체크 하지 않으면 연동 설정을 해제하게 되며 연동 서버의 IP 주소와 포트번호를 넣을 필요가 없게 됩니다.

SNMP 연동을 설정 하려면 SNMP 연동 체크박스에 체크를 한 후 연동서버의 IP주소와 포트번호를 입력하고 연동 대상에 체크하면 됩니다.

WAF에서 탐지가 되면 SNMP TRAP을 통하여, WAF은 [오류! 참조 원본을 찾을 수 없습니다.]의 정보를 설정한 연동서버 IP에게 전송합니다.

SNMP 연동 탐지 전송 정보

| 오류 메시지 | 출력 원인 |
|--|--|
| 더 이상 추가하실 수 없습니다. | 아이디를 추가할 때 이미 조회자 아이디가 5개 이상 존재할 경우 |
| 아이디는 영문과 숫자만을 사용할 수 있으며 반드시 알파벳으로 시작해야 합니다 | 아이디에 특수문자 또는 아이디 규칙에 맞지 않을 경우. |
| 아이디는 4자 이상 10자 이하를 입력하여야 합니다. | 4자 이하 또는 10자 이상으로 아이디 규칙에 맞지 않을 경우. |
| 빈칸일 수 없습니다. | 입력한 조회자 아이디가 빈칸일 경우 |
| {추가할 아이디} 는 현재 접속하고 있는 ID입니다. | 입력한 조회자 아이디가 관리도구에 접속해 있는 운영자 아이디와 같을 경우 |
| 조회자로 추가된 아이디입니다. | 입력한 조회자 아이디가 이미 조회자 아이디로 등록되어 있는 경우 |
| 웹 사이트 관리자로 추가된 아이디입니다. | 입력한 조회자 아이디가 이미 보안 정책별 관리자 아이디로 등록되어 있는 경우 |
| ERROR | 네트워크 문제상 조회자 아이디를 추가 할 수 없는 경우 |

| 종류 | 설명 |
|-------------|----------------|
| 탐지 시간 | 탐지된 시간 |
| 출발지 IP | 공격을 시작한 출발지 IP |
| 공격 URI | 탐지된 URI의 정보 |
| 탐지 RULE | 탐지된 RULE의 이름 |
| 탐지 Raw Data | 패킷 데이터 |
| Response | HTTP 응답 |
| | |

| | |
|-------------|-------------|
| 웹사이트 호스트 이름 | 웹사이트 호스트 이름 |
| 도착지 IP | 설정된 서버 IP |

[다음] 버튼을 클릭하면 [오류! 참조 원본을 찾을 수 없습니다.]와 같은 [SIMS연동 설정] 화면이 나타납니다.

SIMS 연동

SIMS 연동 설정을 하려면 SIMS 연동 체크박스에 체크를 한 후 SIMS ID, SIMS 서버 IP, SIMS Port, WAF IP, 인증 코드, sleep Time을 입력하면 됩니다. 이때, sleep Time은 분 단위로 입력이 가능합니다.

E-MAIL & SysLog 연동

[다음] 버튼을 클릭하면 [오류! 참조 원본을 찾을 수 없습니다.]과 같은 [E-mail 및 SysLog 연동 설정] 화면이 나타납니다.

E-mail 연동 설정을 하려면 E-mail 연동 체크박스에 체크하고 E-mail을 보낼 시간 간격과 보내는 E-mail 주소, 받는 E-mail 주소를 주소, SM TP주소를 입력합니다. E-mail 연동은 E-mail에서 SMTP주소 및 보내는 E-mail주소가 미리 설정 되어 있어야 합니다.

([IX.오류! 참조 원본을 찾을 수 없습니다. 오류! 참조 원본을 찾을 수 없습니다.]에서 E-MAIL 관련 설정을 미리 하지 않았다면, E-MAIL 설정 화면이 체크 후에 나타납니다) E-MAIL을 보낼 [시간 간격]과 E-MAIL을 [받는 주소]를 입력합니다.

SYSLOG 연동 설정을 하려면 SYSLOG 연동 체크박스에 체크하고 [SYSLOG 전송 서버]의 IP 주소를 입력합니다

[다음] 버튼을 클릭하면 [오류! 참조 원본을 찾을 수 없습니다.]와 같은 [연동 설정 완료] 화면이 나타납니다. 이 화면에서 설정 내용을 확인하고 [완료] 버튼을 클릭하면 WAF에 설정내용이 반영 됩니다.

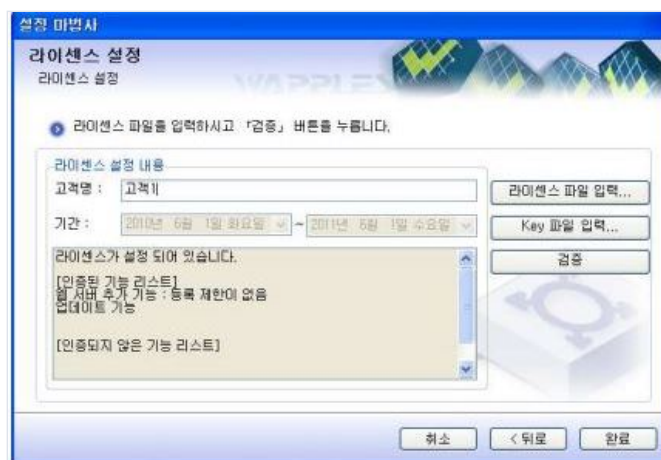
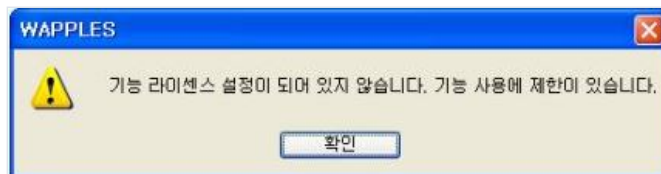


라이선스 설정

라이선스 설정은 WAF 3.0R5 이후 버전에 대해 반드시 설정해야 하는 항목입니다. 라이선스를 설정하지 않는다면, WAF의 기능사용에 제한을 받습니다.

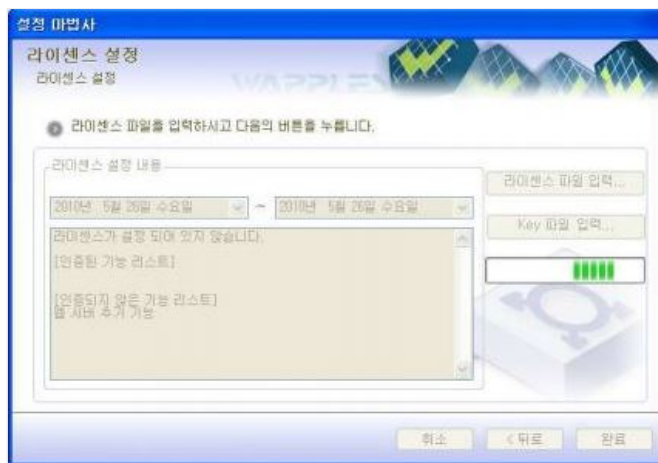
입력된 라이선스에 따라 WAF는 기능 제한을 할 수 있습니다.

WAF 관리자 Console를 실행하여 접속 하였을 시 라이선스가 설정되지 않았다면 **[오류! 참조 원본을 찾을 수 없습니다.]** 을 확인할 수 있습니다.

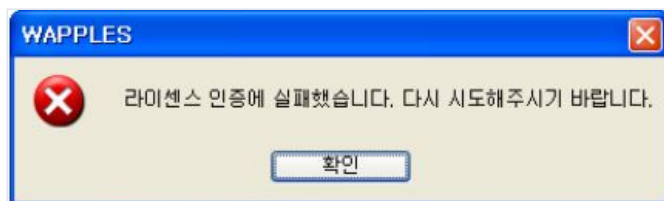


[오류! 참조 원본을 찾을 수 없습니다.] 화면에서 라이선스를 설정할 수 있습니다.

[오류! 참조 원본을 찾을 수 없습니다.] 화면에서 [라이선스 파일 입력] 버튼으로 라이선스 (*.cer)를 import합니다. [key 파일 입력] 버튼으로 key 파일을 (*.key)을 import합니다. [검증]버튼을 클릭하면 인증서를 검증하는 화면**[오류! 참조 원본을 찾을 수 없습니다.]**에서 몇 초간 기다립니다.



실패 인증에 실패 했을 경우 **[오류! 참조 원본을 찾을 수 없습니다.]**창을 확 인할수 있습니다.



성공 설정이 성공하면 [라이선스 설정 내용]에서 유지보수 기간과 서비스 제 한 관련 사항을 확인할 수 있습니다.

라이선스 설정 오류 메세지

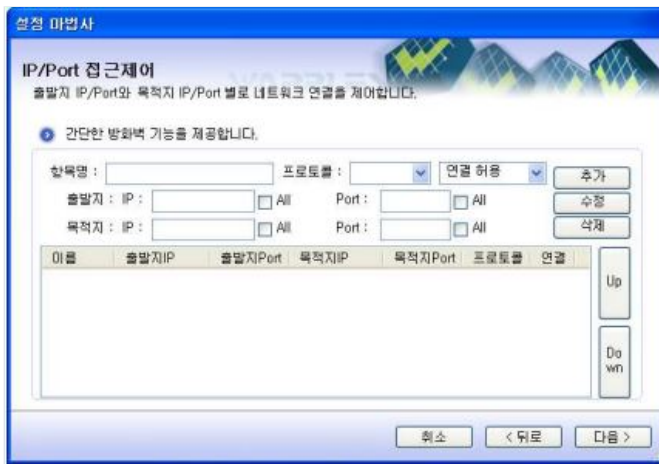
| 오류 메시지 | 출력 원인 |
|------------------|---|
| 중복된 이름이 있습니다 | IP/Port 접근제어 목록을 구분 짓는 이름 중복 되었을 경우 |
| 잘못된 IP입니다 | 입력된 IP가 IP형식이 아닐 경우 |
| 입력 가능한 범위가 아닙니다. | Port입력박스가 빈칸일 경우. 또는 포트 범위가 0~65535범위를 벗 어난 값을 입력한 경 우. |
| 숫자만 입력 가능합니다. | Port의 범위 설정할 때 [:] 또는 [-]외의 다른 문자를 넣었을 경우 |

IP/Port 접근 제어

IP/Port 접근제어는 설정한 Source IP/Port 에서 출발하여 Destination IP/Port 로 향하는 트래픽에 대한 접근제 어 기능을 제공합니다. IP/Port 접근제어로 설정한 IP와 PORT 는, WAF의 탐지와 무관하게, 그 설정에 따라 허용 또는 차단만 가능합니다. 또한 설정된 순서에 따라서 IP/Port 제어처리에 대한 우선순위를 갖습니다. 우선순위는 **[오류! 참조 원본을 찾을 수 없습니다.]**에서 보이는 Up, Down 버튼으로 설정할 수 있으며 리스트의 상단으로 갈 수록 우선순위는 높습니다.

IP/Port 접근제어 설정은 인라인 구성일 때만 설정 가능합니다.

IP/Port 접근 제어 설정은 [설정 마법사] -> [운영설정]화면에서 [IP/PORT 접근제어]를 클릭하여**[오류! 참조 원본 을 찾을 수 없습니다.]**화면에서 설정합니다.



[오류! 참조 원본을 찾을 수 없습니다.] 화면에서 IP/Port 접근에 관하여 추가, 수정, 삭제를 할 수 있습니다.

추가

[오류! 참조 원본을 찾을 수 없습니다.]화면에서 중복되지 않는 이름과, 프로토콜, 출발지 IP/Port 및 도착지 IP/Port, 그리고 연결 허용 또는 연결 거부를 체크하여 설정 합니다.

- 이름 각 접근제어 설정을 구분 짓는 고유 이름을 입력합니다
- 프로토콜 접근제어 선택 가능한 프로토콜은 TCP, UDP, ICMP가 있으며 이 중 ICMP는 포트 설정을 할 수 없습니다.
- 출발지 및 목적지 IP 출발지와 목적지의 IP와 Netmask를 받으며, IP만 입력 시 Netmask 는 기본 값인 32로 설정됩니다.
- 출발지 및 목적지 Port Port 입력 박스는 하나의 Port값을 입력할 수도 있으며, [:]또는 [-] 의 기호를 써서 Port의 범위를 입력할 수 있습니다. 예를 들면 [80-100]으로 입력한 경우 80번에서 100번 사이의 Port를 접근제 어로 설정합니다.

IP/Port 설정까지 모든 입력이 끝난 뒤 [추가] 버튼을 누르면, 리스트에 설정한 값이 나타나는 것을 확인할 수 있습니다. 그 값을 클릭한 후 Up & Down 버튼으로 우선 순위를 결정합니다.

모든 설정을 다 추가한 뒤 [다음]을 누르면 설정 사항에 대한 내용을 확인 할 수 있으며 그 후 완료를 누르면 IP/Port접근 제어 설정이 완료됩니다.

수정 및 삭제

- 수정 IP/Port 접근제어 리스트에서 수정할 내용을 클릭한 뒤 수정하고자 하는 설정을 변경한 뒤 수정 버튼을 누르면, 수정된 설정이 리스트에 나타납니다. [다음]을 누르면 설정 사항에 대한 내용을 확인 할 수 있으며 그 후 완료를 누르면 수정이 완료됩니다.
- 삭제 IP/Port 접근제어 리스트에서 삭제할 내용을 클릭하고 삭제 버튼을 누르면, 해당 내용이 삭제됩니다. [다음]을 누르면 설정 사항에 대한 내용을 확인 할 수 있으며 그 후 완료를 누르면 삭제가 완료됩니다.

IP/Port 접근제어 오류 메시지

| 오류 메시지 | 출력 원인 |
|------------------|--|
| 중복된 이름이 있습니다 | IP/Port 접근제어 목록을 구분 짓는 이름 중복 되었을 경우 |
| 잘못된 IP입니다 | 입력된 IP가 IP형식이 아닐 경우 |
| 입력 가능한 범위가 아닙니다. | Port입력박스가 빈칸일 경우. 또는 포트 범위가 0~65535범위를 벗 어난 값을 입력한 경우. |
| 숫자만 입력 가능합니다. | Port의 범위 설정할 때 [:] 또는 [-] 외의 다른 문자를 넣었을 경우 |

패턴 저장소

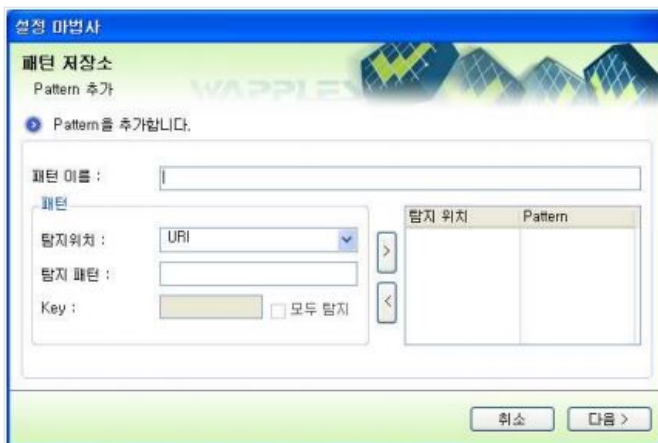
WAF에서는 패턴 저장소에 다양한 패턴을 등록할 수 있으며, 등록된 패턴을 종합관리하는 저장소 기능을 제공합니다.

정책의 User Defined Pattern 사용자 정의 설정화면에서 패턴저장소에 등록된 패턴들을 이용하여 공격을 탐지할 수 있습니다.

[오류! 참조 원본을 찾을 수 없습니다.] 에서 레벨이란 등록된 주체를 의미합니다. Management System에서 패턴 저장소를 설정하여 줄 수 있기 때문에 레벨을 통하여 누가 등록을 했는지 알 수 있습니다. W1이란 WAF를 의미하며, M2는 Management System을 의미합니다.



- 패턴 추가 탐지 패턴 추가를 위한 [오류! 참조 원본을 찾을 수 없습니다.] 화면이 나타나며, 패턴을 추가 할 수 있습니다.
- 패턴 수정 탐지 패턴 리스트에서 수정할 내용을 클릭하고 수정 버튼을 누르면, 패턴의 수정화면이 나타납니다. 내용을 수정하고, 완료버튼을 누르면 수정된 내용이 패턴 스트에 표시 됩니다.
- 패턴 삭제 탐지 패턴 리스트에서 삭제할 내용을 클릭하고 수정 버튼을 누르 면, 탐지 패턴 리스트에서 해당 내용이 삭제됩니다



[패턴 이름]에 패턴을 대표하는 이름을 작성한 후, [탐지위치]를 선택하고 [탐지패턴]에 탐지해야 할 패턴을 작성한 후에 [>] 버튼을 클릭하여 패턴을 등록합니다. [<]을 누르면 패턴을 삭제할 수 있습니다.

탐지 위치

| 종류 | 설명 |
|-----------|-------------------|
| URI | URI |
| REQLINE | Request Line |
| PARAM | Request Parameter |
| REQHEADER | Request Header |

오류 메시지

| 오류 메시지 | 출력 원인 |
|-------------|------------------------------------|
| 빈칸일 수 없습니다. | 패턴의 이름 과 탐지 패턴 및 탐지 패턴 리스트가 빈칸일 경우 |

[오류! 참조 원본을 찾을 수 없습니다.] 화면에서 [다음] 버튼을 누르면 [오류! 참조 원본을 찾을 수 없습니다.] 화면이 나타납니다.



Regular Expression을 사용하려면 체크박스를 클릭 한 후, 탐지 위치를 선택하고 탐지 패턴을 정규식으로 입력합니다.

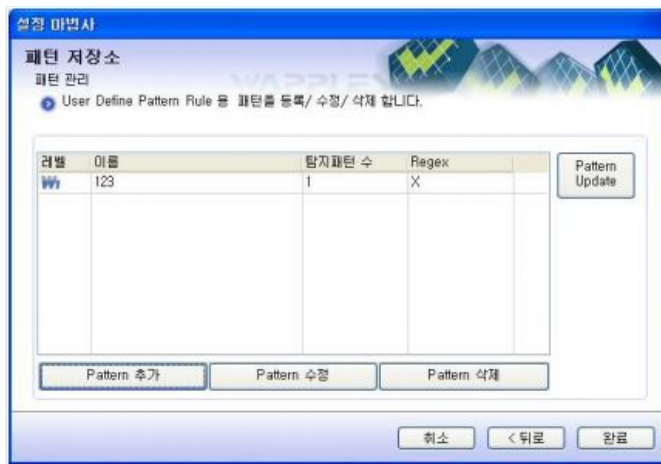
오류 메시지

| 오류 메시지 | 출력 원인 |
|-------------|---|
| 빈칸일 수 없습니다. | Regular expression을 사용하며, 탐지패턴과 키가 빈칸일 경우 |

입력을 마친 후에 [다음]버튼을 누르면 [오류! 참조 원본을 찾을 수 없습니다.] 화면이 나타납니다.

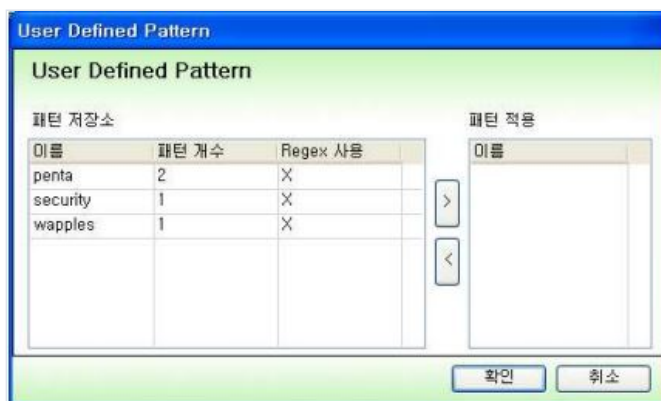


[오류! 참조 원본을 찾을 수 없습니다.] 화면에서 설정의 내용을 확인하고 [완료] 버튼을 누르면 패턴이 저장됩니다.



[오류! 참조 원본을 찾을 수 없습니다.] 화면에서 [완료]버튼을 누르면 패턴 등록을 완료합니다.

등록된 패턴은 탐지 정책의 User Defined Pattern의 사용자 정의 설정에서 등록된 패턴을 확인 할 수 있으며 탐지 패턴으로 사용할 수 있습니다.



정책/로그 동기화

정책/로그 동기화(PLS) 기능은 서로 다른 두 대의 WAF간에 정책 및 탐지로그를 동기화하기 위해 사용됩니다.

본 기능을 실행할 경우 다음과 같은 유의사항을 숙지하여야 합니다.

- 웹사이트 관리자 권한 제한 본 기능이 실행되면 웹사이트 관리자가 설정한 정책은 동기화되지 않습니다 .
- 운영설정, 네트워크 설정 본 기능은 정책설정과 로그만을 동기화하는 기능이므로, 운영설정 과 네트워크 설정은 각각의 WAF 관리도구를 이용하여 설정합니다.
- 웹 서버 IP 등록 네트워크 설정에서 등록 가능한 웹 서버 IP 역시, 각각의 WAF 관리도구의 네트워크 설정을 이용하여 등록해주어야 합니다
- 관리자 비밀번호 변경 관리자의 비밀번호를 변경할 경우, 본 기능의 설정환경의 비밀번호 역시 동일하게 변경해주어야 합니다.

[오류! 참조 원본을 찾을 수 없습니다.]화면 에서 [정책/로그 동기화]라고 되어 있는 체크박스에 동기화 여부를 설정 합니다. 이 체크박스에 체크하지 않으면 정책/로그 동기화 설정이 해제 됩니다.

정책/로그 동기화 설정을 하려면 [정책/로그 동기화] 체크박스에 체크를 한 후 동기화할 WAF IP, 관리도구 접속 ID, 관리도구 접속 비밀번호를 입력하면 됩니다.

또한 [로그 동기화] 체크박스에 체크하지 않으면 정책만 동기화 되고 [로그 동기화] 체크박스에 체크하면 정책과 탐지로그가 동기화 됩니다.

정책/로그 동기화 오류 메시지

| 오류 메시지 | 출력 원인 |
|-------------|---|
| 빈칸일 수 없습니다. | WAF IP가 빈칸일 경우 관리도구 접속ID가 빈칸일 경우 관리도구 접속 비밀번호가 빈칸일 경우 |
| 잘못된 IP입니다. | 관리 IP 추가/수정 시 입력된 IP가 IP 형식이 아닐 경우 |

동기화하고자 하는 WAF 에 대해서 각각 본 기능(정책/로그 동기화(PLS))이 활성화 되어야 정상적으로 동작합니다.

시간 동기화 설정

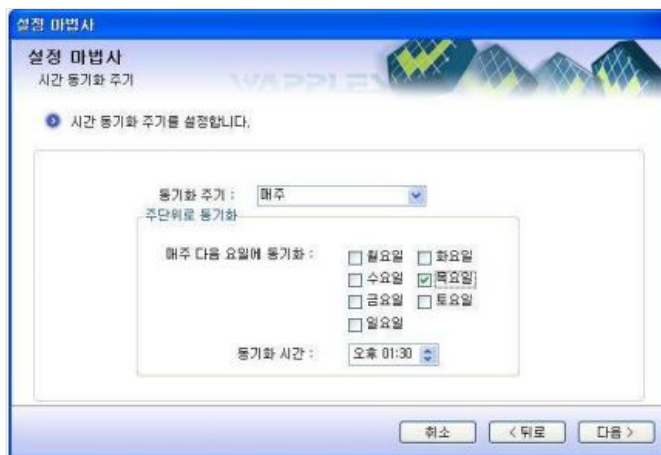
WAF은 사용자가 등록한 타임 서버의 시간과 WAF의 시스템의 시간을 동기화하며, 사용자가 선택한 표준 시간을 설정하기 위하여, [시간 동기화 설정] 기능을 사용합니다.

시간 동기화 설정 오류 메시지

| | |
|--|--|
| | |
|--|--|

| 오류 메시지 | 출력 원인 |
|------------------|---|
| 빈칸일 수 없습니다. | 시간 서버 IP와 포트 번호가 빈 칸일 경우 |
| 잘못된 IP입니다. | 시간 서버 IP 추가/수정 시 입력된 IP가 IP형식이 아닐 경우 |
| 입력 가능한 범위가 아닙니다. | 포트 번호 입력 창에 입력된 P 포트 번호가 0보다 작고 65535 보다 클 경우 |
| 숫자만 입력 가능합니다. | 입력된 포트 번호가 정수가 아닐 경우 |

[오류! 참조 원본을 찾을 수 없습니다.]에서 동기화 실행 체크박스를 클릭을 합니다. [시간 동기화 설정]은 시간 서버의 IP와 포트를 통하여 동기화를 시도하기 때문에, IP와 포트 정보가 필요 합니다. 시간 서버 IP와 포트 번호 및 시스템에 적용 할 표준시간대를 설정을 한 후, [다음] 버튼을 누르면, [오류! 참조 원본을 찾을 수 없습니다.] 화면이 나타납니다.



시간 동기화 주기 단위는 매시, 매일, 매주, 매월을 설정할 수 있습니다

매일 시간 동기화를 원할 경우 백업시간을 입력하고 매주 시간 동기화를 원할 경우 원하는 요일과 백업 시간을 입력합니다. 매월 시간 동기화를 원할 경우 백업 날짜와 시간을 입력합니다.



업데이트 설정 및 실행

WAF은 최신 보안위반 사건목록을 업데이트 하기 위해 [업데이트 설정 및 실행]기능을 사용합니다.

업데이트 서버는 WAF 서비스 IP를 통해 원격지 WAF과 통신하며, 안전한 채널 형성을 위하여 SSL 프로토콜을 이용합니다. 따라서 관리자는 업데이트 서버의 443 포트와 WAF 간의 통신이 가능하도록 내부 네트워크의 포트를 개방하는 등의 조치를 취해야 하며, 업데이트 서버와 WAF간 네트워크의 안정성을 보장해야 합니다.

업데이트 설정을 한번도 설정하지 않았다면 아래의 첫번째 화면이 나옵니다. 업데이트 서버 IP 설정되어 있지 않기에, 업데이트 즉시 실행을 할수 없습니다. 업데이트 서버 설정이 되어 있다면 두번째 화면처럼 업데이트 즉시 실행을 선택할수 있습니다.

[업데이트 설정]화면에서 외부에 있는 업데이트 서버와 연동하는 업데이트 여부를 확인하고 자동으로 업데이트를 설정할지를 결정하는 [업데이트 모드설정]과 외부에 있는 업데이트 서버를 지금 연결하여 업데이트 여부를 확인하는 [업데이트 즉시 실행]을 선택할 수 있습니다.



[업데이트 버전 업데이트]화면에서 [업데이트 모드 설정]을 선택하고 [다음] 버튼을 클릭하면 아래화면이 나타납니다.

업데이트 모드는 아래 표와 같이 3개의 모드를 선택할 수 있습니다.

업데이트 모드 설정

| 모드 | 설명 |
|-----------------|---|
| [자동 업데이트] | 매일 새벽 4시에 업데이트 서버에서 신규 업데이트 사항이 있는지 확인하고 신규 업데이트 사항이 있으면 자동으로 업데이트합니다 |
| [관리자 승인 후 업데이트] | 매일 새벽 4시에 업데이트 서버에서 신규 업데이트 사항이 있는지 확인하고 신규 업데이트 사항이 있으면 관리자가 WAF 관리도구에 접속 할 때 화면이 표시되고 업데이트 여부를 관리자가 결정하는 화면이 수행됩니다. ([업데이트 즉시 실행]화면과 같습니다.) |
| [수동 업데이트] | 자동 업데이트를 진행하지 않습니다. |



화면에서 [관리자 승인 후 업데이트]를 선택하고 [다음]버튼을 클릭하고 보조 업데이트 서버 주소와 업데이트 기준 시간과 업데이트 주기를 입력합니다. WAF는 업데이트 기준 시간에 입력된 시간을 기준으로 업데이트 주기에 입력된 시간마다 업데이트를 확인하게 됩니다.

선택 마법사
업데이트 설정 및 실행
보조 업데이트 서버 등록

업데이트 서버의 IP를 입력합니다. 입력하지 않으면 기본 업데이트 서버로 설정됩니다.

업데이트 서버 1 IP : 118.33.113.96 [직접입력]
업데이트 서버 2 IP : 118.33.113.97 [직접입력]
업데이트 기준 시간 : 오후 2:00
업데이트 주기 : 24 시간 마다

[취소] [뒤로] [다음]

업데이트 서버 IP에 입력된 IP가 없을 경우 WAF의 기본 업데이트 서버인 펜타시큐리티 시스템에서 관리하는 서버 주소를 사용하게 됩니다.

업데이트 서버에 입력되는 IP는 WAF 시스템이 특별히 외부 네트워크와 단절 되어 있거나, 다수의 WAF 시스템을 운영하고 있어 업데이트 서버로 접속하는 트래픽이 증가될 우려가 있다고 판단되는 경우 따로 펜타시큐리티 시스템에 요청하여 할당 받을 수 있습니다.

업데이트 서버를 운영하지 않는 경우에는 업데이트 서버 IP를 입력하지 않습니다.

백업 설정 오류 메시지

| 오류 메시지 | 출력 원인 |
|-------------|---------------------------------|
| 잘못된 IP 입니다. | 입력된 업데이트 서버IP가 올바른 IP 형식이 아닐 경우 |

[업데이트 서버 등록] 화면에서 다음 버튼을 클릭하면 아래화면이 나타납니다. 이 화면에서 설정 내용을 확인하고 [완료] 버튼을 클릭하면 업데이트 설정을 저장하고 설정 내용이 WAPPLSES에 반영 됩니다.

선택 마법사
업데이트 설정 및 실행
설정 완료

변경된 내용이 없습니다.

업데이트 모드 : 자동 업데이트
업데이트 서버 IP : Default
업데이트 시간 : 오전 2:00 부터 매 24시간 마다

[취소] [뒤로] [완료]

[즉시 업데이트 실행]을 선택하고 [다음] 버튼을 클릭하면 아래화면이 나타납니다. 이 화면에서 현재 WAF의 서버 버전과 업데이트할 사항이 있는지 확인한 후 [다음]버튼을 클릭합니다.

업데이트 설정 및 실행
업데이트 설정 및 실행
업데이트 실행

'완료'를 누르시면 업데이트가 시작됩니다.

업데이트 실행 전에 다음 데이터를 백업 하셔야 합니다.

현재 외플 버전 : 3.0R5, 10186, K1, 2, 7-1, U1, 2, 7-2, x86_64
업데이트 서버 IP : 218.145.29.163 | 118.33.113.90

[취소] [뒤로] [다음] [완료]

화면에서 [완료] 버튼을 클릭하면 아래 화면이 나타납니다. 만약 업데이트를 원하지 않으면 [취소] 버튼을 클릭하여 업데이트 마법사를 종료합니다.



업데이트 실행은 다음과 같은 5가지 절차를 따라 진행됩니다.

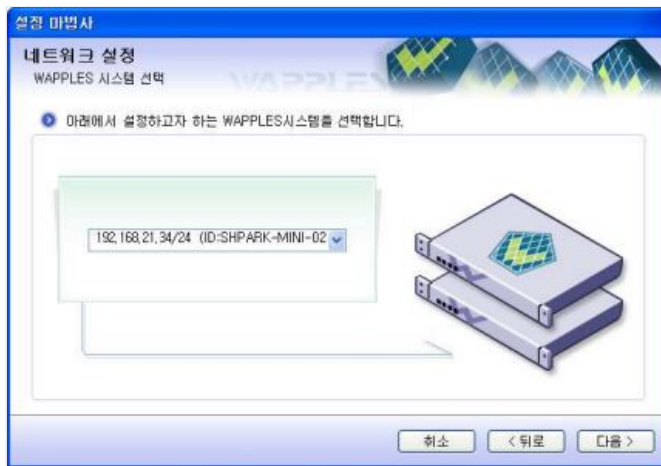
- 업데이트 정보 초기화: 업데이트 정보를 초기화하는 단계입니다
- 업데이트 버전 확인: 현재 업데이트 서버에 업데이트 가능 버전이 있는지 확인합니다
- 업데이트 파일 다운로드: 업데이트 서버로부터 업데이트 할 파일을 다운로드 받습니다.
- 업데이트 파일 패치: 다운로드 받은 파일을 현 장비에 패치합니다
- 업데이트 완료: 업데이트 완료 단계입니다. 업데이트를 완료 하면 업데이트 결과 창이 나타나게 되고 [확인] 버튼을 클릭하면 관리도구는 재시작 됩니다.

업데이트를 하기 전에 반드시 WAF 데이터를 백업하여 주시기 바랍니다. 데이터 백업 방법은 [WAF 백업 방법은 여기를 클릭해주세요]를 클릭하면 나타나는 아래화면을 참조하여 주십시오.



네트워크 설정

WAF은 보호 대상 웹 서버의 앞 단에 위치하여 보안 위반 HTTP/HTTPS 트래픽을 감시하기 위해 Proxy와 같은 역할을 수행해야 합니다. WAF을 서비스하기 위해서는 WAF의 네트워크를 설정해야 합니다. 설정마법사를 통해서 WAF의 네트워크를 설정합니다.



Proxy IP 추가/수정/삭제

화면에서 설정할 WAF을 선택한 후 [계속]버튼을 클릭하면 WAF의 Proxy IP 설정하는 화면이 나타납니다. 와플의 네트워크 구성에 따라서 인라인 구성으로만 운영할시에는 값을 입력하지 않고 다음으로 이동할수 있습니다

리버스 프락시 구성으로 할 경우에는 WAF의 서비스 포트에서 사용할 Proxy IP 주소와 기본 게이트웨이를 입력합니다. Proxy IP 주소는 필요에 따라서 여러 개 입력이 가능합니다. 그러나 여러 개라도 동일한 서비스포트 네트워크 장치에서 사용하는 IP이므로 모두 동일 서버넷에 존재하는 IP를 입력해 주어야 합니다 각 Proxy IP는 IP와 넷마스크를 설정하여야 합니다. 현재 설정되어 있는 Proxy IP는 오른쪽 표에 Proxy IP/넷마스크 리스트에서 볼 수 있으며 왼쪽의 추가/수정/삭제 버튼과 IP/넷마스크 입력 창을 통하여 추가/수정/삭제할 수 있습니다. [설정 불러오기...]버튼으로 이전에 설정된 정보를 [불러오기]하여 쉽게 Proxy IP 설정을 할 수 있습니다.

[설정 불러오기...] 버튼은 이전에 설정하여 저장해 놓은 파일을 다시 불러올 수 있는 기능으로 이 버튼을 사용하여 설정을 가져오면 기존의 설정은 모두 사라지므로 주의하여야 합니다.

Proxy IP의 추가/수정/삭제는 IP/넷마스크 입력 창, 추가/수정/삭제 버튼의 조작을 통하여 이루어집니다. 추가/수정/삭제 방법은 다음과 같습니다.

- 추가 IP/넷마스크 입력 창에 IP와 넷마스크를 넣고, [추가] 버튼을 클릭하 면 WAF IP/넷마스크 리스트에 입력한 내용이 추가됩니다.
- 수정 WAF IP/넷마스크 리스트에서 수정할 내용을 클릭하면, IP/넷마스크 입력 창에 해당 내용이 표시됩니다. IP/넷마스크 입력 창에서 내용을 수정하고 [수정]버튼을 클릭하면 수정된 내용이 WAF IP/넷마스크 리스트에 표시됩니다.
- 삭제 WAF IP/넷마스크 리스트에서 삭제할 내용을 클릭하고, [삭제]버튼 을 클릭하면 WAF IP/넷마스크 리스트에서 해당 내용이 삭제 됩니다.

설정 마법사는 Proxy IP 설정 시 사용자 입력 값에 오류가 있을 경우 다음과 같은 오류 메시지를 출력합니다.

Proxy IP 설정 오류 메시지

| 오류 메시지 | 출력 원인 |
|------------------|--|
| 빈칸일 수 없습니다. | Proxy IP 입력 창이 빈칸인 상태에서 추가 및 수정을 시도한 경우 |
| 잘못된 IP입니다. | Proxy IP 입력 창에 입력된 IP가 IP형식이 아님에도 불구하고 추가 및 수정을 시도한 경우 |
| 잘못된 netmask 입니다. | 넷마스크 입력 창이 빈칸이거나 입력 된 넷마스크가 IP 형식이 아닌 상태에서 추가 및 수정을 시도한 경우 |

WAF IP/넷마스크 리스트에 목록을 보면 빨간색으로 표시된 내용이 보일 수 있습니다. 빨간색으로 표시된 부분은 해당 IP 에 종속된 웹 서버가 존재한다는 뜻입니다. 이러한 경우 해당 IP 를 바로 삭제 할 수 없습니다. 해당 IP 에 종속된 웹 서버를 모두 삭제하여야 WAF IP/넷마스크 리스트에서 삭제 할 수 있습니다



우선 웹 서버 설정에 대해서 살펴보겠습니다. 여러 웹사이트를 하나의 물리적 웹 서버에서 운영할 경우, 각각의 웹사이트를 독립된 웹 서버로 간주하고 WAF를 설정해야 합니다. 예를 들어, IP가 192.168.0.10인 웹 서버에서 80 Port에 대표 웹 사이트(HTTP 서비스)를 운영하고, 로그인 또는 개인정보용으로 443 Port를 SSL 웹 사이트(HTTPS)로 사용하며, 또한 특수 용도로 8080번 Port를 사용한다고 가정하겠습니다. 이 경우에는 3개의 웹사이트를 3개의 웹 서버로 간주되어 등록해야 합니다. 즉, 웹 서버의 IP 및 Port를 기준으로 웹사이트를 등록하는 것입니다.

웹 서버 구성을 Proxy 모드로 설정하려면, 오른쪽 WAF의 Proxy IP 주소는 이전 단계에서 등록된 Proxy IP 주소 중에서 하나를 선택하고, Port는 직접 입력합니다.

웹 서버 구성을 Inline 모드로 하고자 하면, 아래 그림처럼 오른쪽 Proxy IP 입력란에 Inline 모드를 선택합니다. Inline Mode를 선택했을 때는 Port는 입력하지 않습니다.

아래그림에서 볼 수 있듯이, WAF의 보호를 받는 웹 서버의 주소를 왼쪽 웹 서버 입력란에 입력합니다. 일반적인 HTTP 서비스를 제공하는 웹 서버 설정의 경우에는 웹 서버 수정 화면 가운데의 콤보박스에서 [SSL 사용 안함]을 선택합니다. 설정한 웹 서버가 HTTPS 서비스를 위한 SSL Port(일반적으로 443)일 경우, 웹 서버 수정 화면 가운데 있는 콤보박스에서 [SSL]을 선택합니다. 설정한 웹 서버가 HTTP 서비스를 하지만, Client 와 WAF 사이는 SSL 통신을 하고자 할시에는 웹 서버 수정 화면 가운데 있는 콤보박스에서 [SSL Termination]을 선택합니다.

아래그림 우측 우측 상단에 있는 웹 서버 상태 체크 체크박스를 체크하면 웹 서버 상태 체크 기능이 활성화 됩니다. 이 경우 [표 웹 서버 상태 체크 입력값]과 같이 웹 서버 상태 체크 속성을 설정할 수 있습니다. 입력값은 [표 웹 서버 상태 체크 입력값]과 같습니다.

웹 서버 상태 체크 입력값

| 항목 | 설명 |
|----------------|-------------------------------|
| 호스트 명 | 웹 서버에 설치되어 있는 웹사이트의 호스트 명 |
| 체크할 파일 | 체크 주기마다 요청할 파일의 경로를 설정 |
| 응답대기 시간 | 웹 서버가 응답하는데 걸리는 최대 시간(초) |
| 체크주기 | 웹 서버 체크 주기 (초) |
| Request Method | 체크할 때 사용할 Method (HEAD/GET) |

웹 서버 상태 체크 결과는 **[오류! 참조 원본을 찾을 수 없습니다.]**이나, SNMP Trap을 통하여 웹 서버가 정상적인 상태인지 확인할 수 있습니다. SNMP 웹서버 체크 연동 설정을 확인하고자 하면 **[오류! 참조 원본을 찾을 수 없습니다.]**를 참조 하시길 바랍니다. 웹 서버가 보내는 200, 400, 404, 505등과 같은 상태 코드(Status Code)를 출력합니다. 만약 웹 서버에 소켓 연결이 안될 경우에는 "연결 실패"를 표시하고, 소켓 연결은 성공했으나 적절한 웹 서버 응답이 없을 경우 "응답 없음"으로 표시합니다.

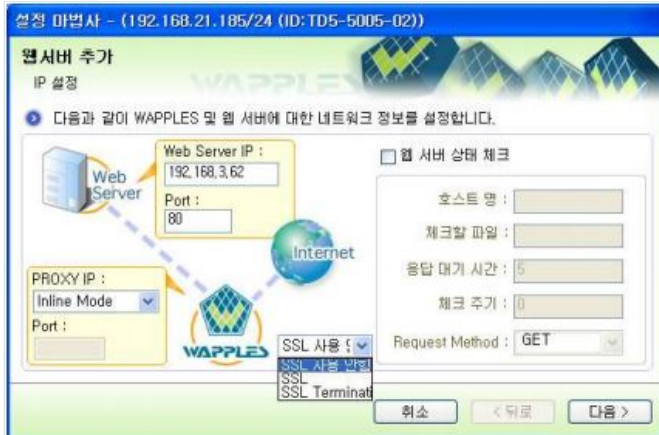
웹 서버 상태 체크 설정 오류 메시지

| 오류 메시지 | 출력 원인 |
|------------|----------------------------|
| 빈칸일 수 없습니다 | 호스트 명이나 체크할 파일이 입력되지 않았을 때 |

숫자만 입력 가능합니다.

응답 대기 시간이나 체크 주기가 숫자(정수)로 입력되지 않았거나 비어 있을 때

입력란에 알맞은 사항을 입력하고 [다음] 버튼을 클릭하면 SSL 사용 여부에 따라 SSL 인증서 등록이나 설정 확인 페이지로 이동합니다



설치 마법사 - (192.168.21.185/24 (ID:TD5-5005-02))

웹 서버 추가
IP 설정

다음과 같이 WAPPLES 및 웹 서버에 대한 네트워크 정보를 설정합니다.

Web Server IP : 192.168.3.62
Port : 80

PROXY IP :
Port :
Mode : Inline Mode

SSL 사용 ()
SSL 사용 안함
SSL Termination

웹 서버 상태 체크

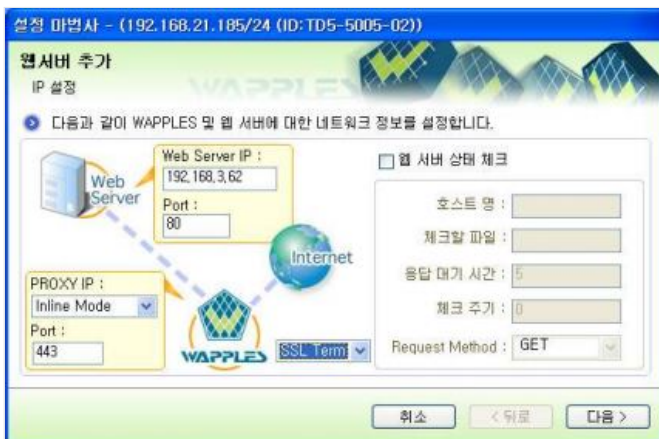
호스트 명 :
체크할 파일 :
응답 대기 시간 : 5
체크 주기 : 0
Request Method : GET

취소 < 뒤로 다음 >

WAF의 SSL 기능성은, WAF가 웹클라이언트의 암호화된 Request 패킷을 복호화(Decryption)하고 검열한 후, 다시 암호화(Encryption)하여 웹 서버로 전달합니다. 또한 WAF는 웹 서버의 암호화된 Response 패킷을 복호화(Decryption)하고 검열한 후, 다시 암호화(Encryption)하여 웹클라이언트로 전달합니다. 이러한 방식은 안전하게 SSL 트래픽을 검사할 수 있는 방식이지만, 암호화 및 복호화 작업이 중복 발생되어 SSL 트래픽 처리가 지연되는 단점이 있습니다. 이러한 성능 저하 문제를 해결하기 위해서 WAF에서는 SSL Termination 기능성을 제공하고 있습니다.

SSL Termination 기능성이 동작할 경우, WAF는 웹클라이언트의 암호화 된 Request 패킷을 복호화하여 검열한 후, 암호화 없이 바로 웹 서버에게 Request 패킷을 전달합니다. WAF는 웹 서버의 암호화되지 않은 Response 패킷을 받아 검열한 후, Response 패킷을 암호화하여 웹클라이언트에게 전달합니다. 즉, WAF가 SSL Termination 상태일 때는 웹클라이언트는 WAF를 SSL 웹 서버로 각주하고 HTTPS로 통신하며, 한편으로 WAPPLES는 웹클라이언트 패킷을 복호화하고 검사한 후, 웹 서버를 대상으로 HTTP로 통신을 합니다. 이로 인해서 암호화 및 복호화를 1/2로 줄일 수 있게되어 성능을 향상시킬 수 있습니다. 단, SSL Termination을 이용할 경우, 웹 서버는 WAF만 접근할 수 있도록 하거나 WAPPLES 같은 네트워크에 설치되고, 외부 네트워크에서 접근이 불가능하도록 설정해야 합니다.

SSL Termination 기능성을 Inline 모드에서 설정할 경우, 아래그림 같이 화면 좌측의 웹 서버의 Port를 일반 HTTP 서비스를 제공하는 Port (일반적으로 80 또는 8080)으로 설정해야 합니다. 화면 우측의 WAF Port도 변경할 수 있으나 일반적으로 HTTPS를 위해 사용되는 443 Port를 사용합니다.



설치 마법사 - (192.168.21.185/24 (ID:TD5-5005-02))

웹 서버 추가
IP 설정

다음과 같이 WAPPLES 및 웹 서버에 대한 네트워크 정보를 설정합니다.

Web Server IP : 192.168.3.62
Port : 80

PROXY IP :
Port : 443
Mode : Inline Mode

SSL 사용 ()
SSL 사용 안함
SSL Termination

웹 서버 상태 체크

호스트 명 :
체크할 파일 :
응답 대기 시간 : 5
체크 주기 : 0
Request Method : GET

취소 < 뒤로 다음 >

SSL Termination 기능성을 Proxy 모드에서 설정할 경우에도, 아래그림 같이 화면 좌측의 웹 서버의 Port를 일반 HTTP 서비스를 제공하는 Port (일반적으로 80 또는 8080)으로 설정해야 합니다. 화면 우측의 WAF IP는 설정했던 IP를 콤보박스에서 선택할 수 있습니다. WAF Port도 변경할 수 있지만 Inline 모드의 경우와 마찬가지로 HTTPS를 위해 사용되는 443 Port를 사용합니다.

설정 마법사는 웹 서버 설정 시 사용자 입력 값에 오류가 있을 경우 다음과 같은 오류 메시지를 출력합니다.

웹 서버 추가/수정 오류 메시지

| 오류 메시지 | 출력 원인 |
|------------------|--|
| 빈칸일 수 없습니다 | 웹 서버 IP 입력 창에 입력된 웹 서버 IP가 빈칸일 경우 |
| 잘못된 IP입니다. | 입력된 웹 서버 IP가 IP형식이 아닐 경우 |
| 입력 가능한 범위가 아닙니다. | Port 입력 창에 입력된 Port 번호가 0보다 작고 65535 보다 클 경우 |
| 숫자만 입력 가능합니다. | 입력된 Port 번호가 정수가 아닐 경우 |

WAF의 Proxy Port를 자동으로 설정하려면 Port란에 빈 문자를 입력하면 WAF 내부에서 자동으로 Port번호를 할당하여 사용하게 됩니다.

WAF Proxy IP의 Port를 수정으로 할당하는 경우는 이전 등록된 Proxy IP와 겹치지 않도록 설정합니다.

입력란에 알맞은 사항을 입력하고 [다음] 버튼을 클릭하면 SSL 사용 여부에 따라 SSL 인증서 등록이나 설정 확인 페이지로 이동합니다.

아래화면은 앞 단계 중앙 하단부의 콤보 박스에서 [SSL] 또는 [SSL Termination]을 선택 했을때 나오는 SSL 인증서 등록 페이지입니다.

[SSL 사용]을 활성화할 경우, 웹 서버의 port 와 WAF의 proxy port 는 SSL 통신을 위해 웹 서버에 설정된 port 를 적어야 합니다.

SSL을 사용하는 웹 페이지를 WAF이 보호하기 위해서는 WAF 에 웹사이트가 사용하는 인증서와 비공개키를 등록하여야 합니다.

이를 위하여 [찾아보기] 버튼을 클릭하여 인증서를 가져옵니다. 사용할 수 있는 인증서의 종류는 인증서와 개인 키가 합쳐져 있는 PKCS #12 형식과 인증서 단독으로 구성된 파일 입니다. 인증서의 종류에 따라 인증서와 개인 키 파일을 순차적으로 가져오거나, 암호를 요구합니다.

인증서와 개인 키 파일을 전부 인으면 인증서와 개인 키의 일치 여부를 조사하여 일치하여야 정상적으로 가져올 수 있습니다.

만약 웹 사이트의 인증서가 중개인증서를 필요로 할 때에는 [중개 인증서 등록]을 체크한 다음 중개 인증서 파일을 가져옵니다.

정상적으로 인증서와 개인 키를 가져오면 아래화면에서 인증서의 정보를 볼 수 있습니다.

만약 웹 서버가 이미 SSL로 설정되어있고, 이를 수정 중이라면 화면 없이 아래화면이 바로 나타나게 되며 인증서 부분을 수정하려면 [다시 가져오기] 버튼을 클릭하여 다시 설정 할 수 있습니다.

설정 마법사는 웹 서버 SSL 인증서 및 비공개키 값 설정 시 사용자 입력 값에 오류가 있을 경우 각 화면에 따라 다음과 같은 오류 메시지를 출력합니다

SSL 추가/수정 오류 메시지

| 화면 | 오류 메시지 | 출력 원인 |
|---------------|---------------------|--|
| 인증서/개인 키 가져오기 | 빈칸일 수 없습니다. | 입력된 인증서 및 개인 키 파일 경로가 비어있는 경우 |
| | 파일을 읽을 수 없습니다. | 입력된 인증서 및 비공개 키의 파일 형식을 알 수 없을 경우 |
| | 파일을 찾을 수 없습니다. | 가져올 파일을 찾을 수 없는 경우 |
| 암호입력 | 비밀번호가 맞지 않습니다. | PKCS #12 형식의 파일에서 설정된 암호가 입력된 암호와 일치되지 않는 경우 |
| 기타 | 인증서와 키가 일치 하지 않습니다. | 입력된 인증서와 개인 키가 일치 하지 않는 경우 |

SSL 사용 안함을 클릭하거나 위의 그림에서 [다음]을 클릭하면 아래화면이 나타납니다.

설정한 내용을 다시 한번 확인하고 [완료] 버튼을 클릭하면 웹 서버의 추가나 변경이 완료되고 화면으로 돌아갑니다.

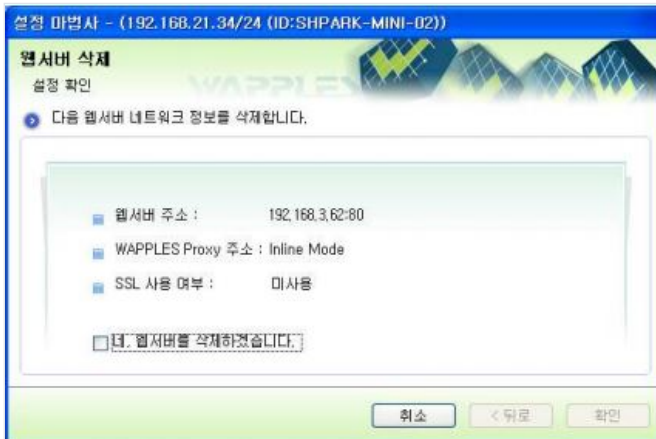


웹 서버 삭제

등록한 웹 서버가 잘못 설정되었거나 더 이상 보호 대상이 아닐 경우 등록된 웹 서버를 삭제 할 수 있습니다.

삭제할 웹 서버를 리스트에서 선택한 후 [삭제] 버튼을 클릭하면 아래화면이 나타납니다. 하단의 [네, 웹 서버를 삭제하겠습니다]에 체크를 하고 확인 버튼을 클릭하면 등록된 웹 서버가 삭제됩니다.

삭제가 완료되면 [웹 서버 삭제]화면이 닫히고 화면으로 돌아갑니다



[설정 내보내기...] 버튼을 클릭하면 네트워크 설정 내용을 파일로 저장 할 수 있습니다.

[완료] 버튼을 클릭하면 설정한 내용이 WAF에 적용됩니다. 현재 WAF에 적용되어 있는 네트워크 환경이 관리도구에 올바르게 입력되었다면 웹 서버와의 통신이 가능하게 됩니다.



네트워크 설정 내용에 SSL 설정 사항이 있다면, 이를 WAF 에 적용될 때 WAF 를 통과하는 웹 트래픽이 잠시 멈출 수 있습니다.

SSL 인증서 적용

이번 장은 SSL 통신을 이용하는 웹 서비스에 적용된 WAF에서 사용 가능한 SSL 인증서 종류와 SSL 인증서 변환 작업에 대해 기술합니다. 기본적인 운영은 [VII.2.2 웹서버 추가/수정]에서 설명합니다

SSL 인증서 지원

WAF은 기본적으로 PEM형식의 SSL 인증서를 지원합니다. 그러나, PEM 형식이 아닌 다른 형식의 SSL 인증서 역시 SSL 인증서 형식을 변환하여 지원할 수 있습니다.

SSL 이란?

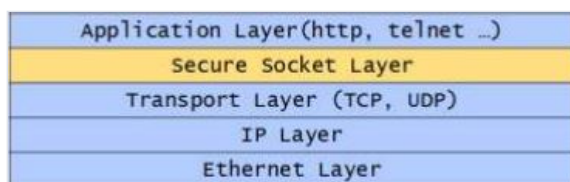
HTTP는 TCP통신을 기반으한 프로토콜로써 양단간의 통신 신뢰성을 보장하나 보안에 취약한 단점을 갖고 있습니다.

따라서 개인정보 및 기밀정보를 평문으로 전달하는 HTTP는 해커에 의해 통신 내용이 유출되거나 변조될 가능성이 존재합니다.

SSL(Secure Socket Layer)는 TCP/IP 4계층중 Transport Layer와 Applicaton Layer의 중간에서 TCP/IP의 보안 취약성을 보완합니다

SSL은 상호 인증, 무결성, 암호화 등을 통한 클라이언트와 서버간의 통신 보안을 유지할 수 있습니다.

데이터 종류별 제공하는 차트 모양



데이터 암호화 방식

비밀키(대칭키) 암호화

통신양단에서 동일한 키를 가지고 데이터 암/복호화를 하는 방식으로 암/복호화에 사용되는 키가 사전 협의시 유출 가능성이 있습니다.



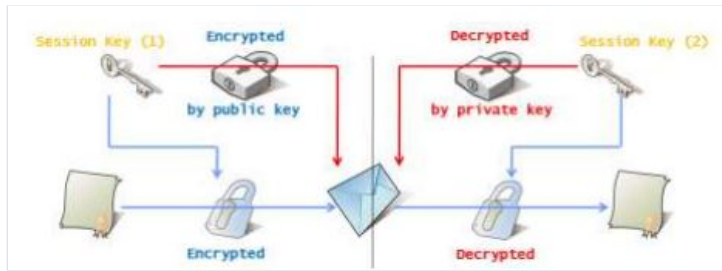
공개키 암호화

암호화를 위해 공개키(Public Key)를 사용, 복호화를 위해 개인키(Private Key)를 사용하는 방식으로 비밀키(대칭키) 암호화 방식의 암/복호화 시 에 동일키를 사용하는 문제점을 해결합니다.



하이브리드 암호화(SSL)

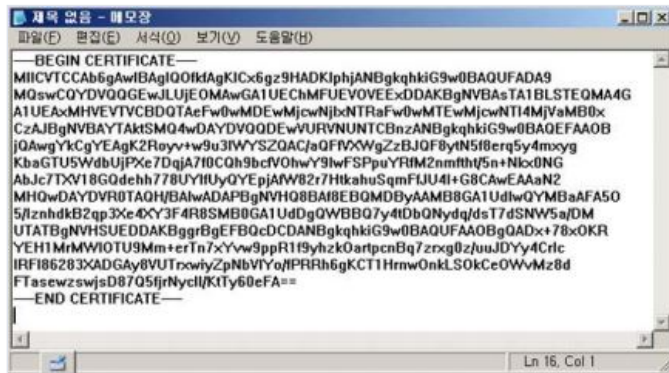
데이터 암호화를 위해 세션키(세션키의 Key, 비밀키)를 사용하는 방식이며, 암호화에 사용된 세션키를 상대방의 공개키를 사용하여 암호화, 수신자는 자신의 공개키로 암호화된 송신자의 세션키값을 구하기 위해 자신의 세션키를 사용하여 복호화, 복호화된 송신자의 세션키를 이용하여 암호화된 데이터를 최종적으로 복호화하는 방식입니다.



PEM 형식의 SSL 인증서

PEM 형식의 SSL 인증서는 텍스트 파일로서 텍스트 편집기(ex. notepad.exe, vi)를 사용하여 내용을 확인할 수 있습니다.

PEM 형식의 SSL 인증서는 아래와 같은 구조를 갖습니다.



인증서는 크게 2개의 구분자와 1개의 내용으로 구성되며 화면의 인증서 내용은 다음 표와 같이 설명할 수 있습니다

PEM형식의 인증서 구성

| 구분 | 설명 |
|---------------------|---|
| -BEGIN CERTIFICATE- | 인증서 내용의 시작을 알리는 Header로서 항상 파일의 첫 라인에 위치합니다. |
| 인증서 내용 | 인증서로 기능하는 내용으로써 DER(Distinguished Encoding Rule)로 처리된 바이너리 값으로 표현하도록 되어 있는데, 이를 text로 표현할 수 있도록 Base64 인코딩한 ASCII 값입니다. |
| -END MESSAGE- | 인증서 내용의 끝을 알리는 Tailer로서 인증서의 마지막에 삽입됩니다. |

상기 인증서를 PEM 형식이라고 부르는 이유는 다음과 같습니다. Privacy-enhanced Electronic Mail (PEM)은 RFC1421에 정의되어 있으며, 안전한 이메일 전송을 위한 표준으로 보안 데이터에 대한 표현 양식을 정의하고 있습니다. 이것이 e-mail 이외의 영역에서도 널리 사용되면서, "-----BEGIN MESSAGE-----"로 시작되고, "-----END MESSAGE-----"로 끝나며, Base64 인코딩된 데이터를 PEM 형식이라고 부르게 되었습니다.

PEM형식의 SSL인증서의 파일 확장자는 cer, crt, der, pem 등 다양한 값을 가질 수 있습니다. 그러나 WAF에 PEM형식의 SSL인증서를 등록하기 위해서 파일의 확장자 자체는 의미 없는 정보이며, 파일의 내용이 위와 같은 PEM 구조라면 WAF에서 인식 가능합니다.

단, WAF 콘솔에서는 cer 과 crt 만을 인식하도록 되어 있으므로, 파일의 확장자를 변경한 후에 입력하시면 됩니다.

정상적인 인증서는 WAF 콘솔을 통하여, [인증서 불러오기 ...]를 수행했을 때, [[Subject] CN= ...]와 같은 형식으로 인증서 발급 대상에 대한 이름이 표시됩니다.

DER 형식의 SSL 인증서

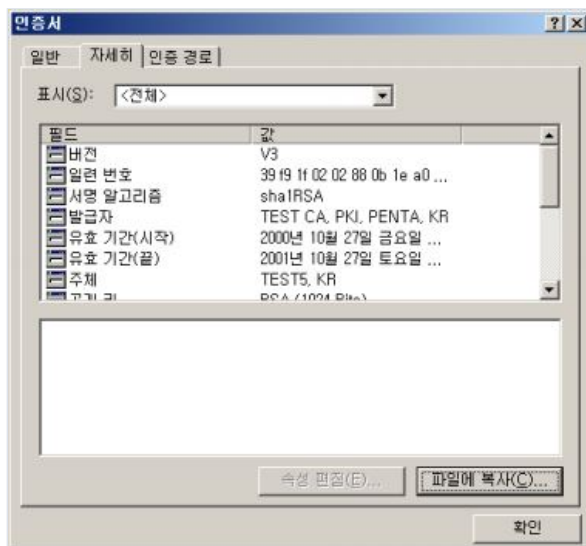
SSL 인증서의 내부 구조가 위 그림과 같은 ASCII 데이터가 아닌 Binary 데이터인 경우 DER형식의 인증서입니다. DER 형식의 인증서인 경우 PEM형식으로 다음과 같이 변환하여 WAF에 등록해야 합니다.

Windows OS가 설치된 PC의 경우

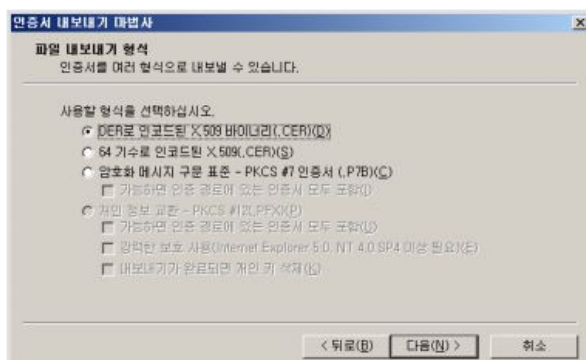
SSL인증서 파일은 Double-Click 만으로 인증서 여부를 확인할 수 있습니다. Windows OS의 경우 cer, der, crt의 확장자를 가진 파일은 Double-Click으로 인증서로 인식하고 해석하여 보여줍니다.

확장자가 cer, der, crt 가 아닌 경우, 파일의 확장자를 cer, der, crt 중 하나로 변경하여 확인합니다.

올바른 인증서 내용을 담고 있는 파일인 경우, 아래와 같이 표시됩니다



DER 형식의 인증서를 PEM 형식의 SSL 인증서로 변환하기 위하여 화면의 [파일에 복사(C)...]를 클릭하여 [인증서 내보내기 마법사]를 실행합니다



인증서 내보내기 마법사가 실행되면 그림과 같이 [DER로 인코딩된 X.509 바이너리(.CER)(D)]를 선택하고 다음을 눌러 PEM형식의 SSL 인증서 파일로 변환합니다.

Open SSL을 사용하는 경우

본 매뉴얼은 Open SSL 0.9.8h 를 기준으로 설명하오니 타 버전의 Open SSL 의 경우 본 매뉴얼에서 사용하는 명령어를 해당 버전의 명령어 형식으로 변환하여 사용하십시오.

DER형식의 Open SSL 인증서의 경우 x509명령어를 이용하여 PEM형식의 SSL 인증서로 변환할 수 있습니다.

```
> openssl x509 -in input.cer -inform DER -out output.cer
```

-outform PEM

Windows 환경에서 인식되지 않는 인증서이거나, Openssl 과 같은 Utility 설치가 불가한 경우 제조사 Penta Security Systems, Inc. 로 문의하시기 바랍니다.

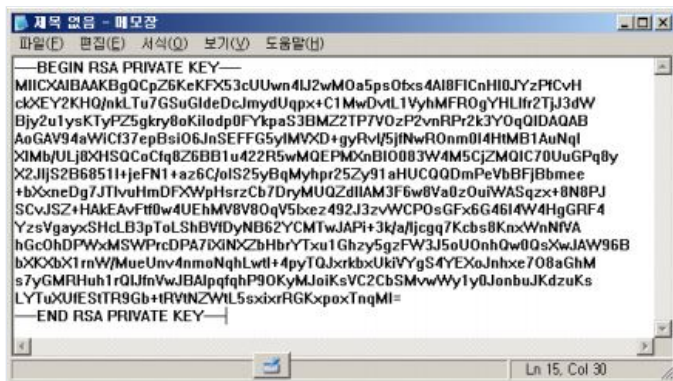
RSA 비공개키 지원

WAF의 설치 위치는 인가된 관리자만이 접근 가능한 물리적으로 안전한 환경에 위치해야 합니다. 이 후 관리자는 WAF을 어떠한 네트워크 구성으로 운영할 것인지를 물리적인 네트워크 환경과 보호하고자 하는 웹 서버의 위치를 고려하여 구성해야 합니다.

PEM 형식의 RSA 비공개키

PEM 형식의 RSA 비공개키는 텍스트 파일로서 텍스트 편집기(ex. notepad.exe, vi)를 사용하여 내용을 확인할 수 있습니다.

PEM 형식의 RSA 비공개키는 아래와 같은 구조를 가집니다.



비공개키는 인증서와 동일하게 2개의 구분자와 1개의 내용으로 구성되어 있으며, 각 구성은 다음과 같은 의미를 가집니다.

RSA형식의 비공개키 구성

| 구분 | 설명 |
|-------------------------|--|
| -BEGIN RSA PRIVATE KEY- | 비공개키 내용의 시작을 알리는 Header로서 항상 파일의 첫 라인에 위치합니다. |
| 비공개키 내용 | 비공개키로 기능하는 내용으로써 DER(Distinguished Encoding Rule)로 처리된 바이너리 값으로 표현하도록 되어 있는데, 이를 text로 표현할 수 있도록 Base64 인코딩한 ASCII 값입니다. |
| -END RSA PRIVATE KEY- | 비공개키 내용의 끝을 알리는 Tailer로써 비공개키의 마지막에 삽입됩니다. |

비공개키 파일의 확장자는 key, pem 등 다양한 값을 가질 수 있지만, 확장자 자체는 의미 없는 정보이고, 파일의 내용이 위와 같은 PEM 구조이어야만 WAF에 등록하여 사용할 수 있습니다.

WAF 콘솔에서는 key 만을 인식하도록 되어 있으므로, 다른 확장자 이름을 갖는 비공개키 파일의 경우 확장자를 [key]로 변경한 후에 입력하시면 됩니다.

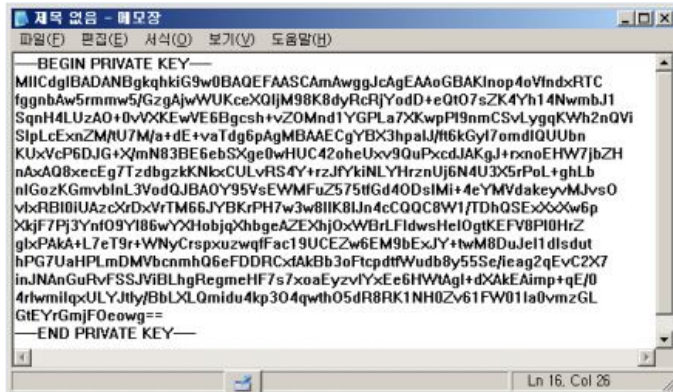
정상적인 RSA 비공개키는 WAF 콘솔을 통하여, [비공개 키 불러오기...]를 수행했을 때, Header와 파일의 내용 앞부분이 표시됩니다

Private Key 파일의 적용

PRIVATE KEY 파일은 알고리즘에 대한 독립성을 갖도록 저장하는 데이터 형식(PKCS#8)입니다.

PKCS: RSA Security사에서 기술학 기술 Specification으로 PKCS#1에서는 RSA 알고리즘과 키 정보 표현 방식에 대해서 기술합니다. PKCS#8에서는 RSA 알고리즘 이외의 다른 공개키 암호 알고리즘에 대해서도 키 정보를 표현할 수 있도록 확장하여 기술합니다.

WAF에서는 RSA 알고리즘 비공개키(PKCS#1) 형식뿐만 아니라 PKCS#8 형식의 비공개키도 등록 가능 합니다.

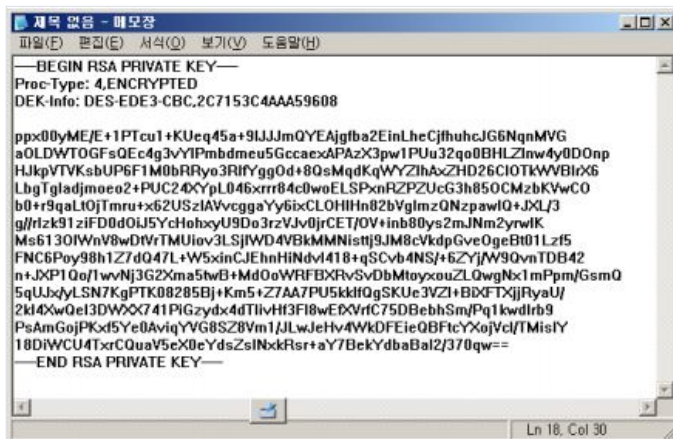


암호화 옵션이 사용된 RSA 비공개키

암호화 옵션이 사용된 PEM 형식의 RSA 비공개키는 복호화 과정을 거쳐야 합니다. RSA PRIVATE KEY에 대한 PEM 형식 파일이지만, Proc-Type 옵션 'ENCRYPTED'가 사용되어 암호화된 비공개키에 대해서는 복호화 과정을 거쳐서 Proc-Type 옵션을 제거해야 합니다.

Proc-Type은 [Privacy-enhanced Electronic Mail(PEM)] 형식으로 표현된 데이터를 인식하기 위해서 처리해 주어야 하는 절차를 정의하는 Header를 의미합니다. Proc-Type에 [ENCRYPTED]가 사용될 경우, [DEK-Info]를 통하여 사용된 알고리즘과 파라미터 정보 등이 전달되어야 합니다.

암호화 옵션이 사용된 RSA 비공개키는 다음과 같은 구조를 가집니다.



기본적으로 PEM형식의 RSA 비공개키와 구조가 동일하나, 그림과 같이 header에 암호화 형식이 표현됩니다.

이를 복호화하기 위해서는 비공개키 생성과정에서 사용한 Passphrase를 기억하고 있어야 합니다. 비공개키 암호화/복호화 절차는 비공개키가 사용되는 웹 서버 환경에 의존적입니다. 따라서, 복호화는 암호화 절차에 사용된 툴을 이용하여 복호화할 것을 권장합니다.

일반적으로는 openssl의 Utility와 호환이 가능하기 때문에 openssl의 'rsa' 명령어를 이용하여 복호화가 가능합니다.

```
> openssl rsa -in enc.key -out dec.key -outform PEM
```

암호화된 데이터가 바이너리 형태인 경우, 일반적으로 웹 서버의 비공개키 생성 매뉴얼을 참고해야만 복호화 방식을 알 수 있습니다.

Openssl 과 호환되는 비공개키 생성기를 사용하는 경우(ex. 명령어 'req'), 생성 과정에서 '-nodes' 옵션을 사용하면 비공개키는 암호화 되지 않습니다.

SSL과 WAF

SSL이 적용된 웹 서버에 WAF를 적용할 경우 SSL termination과 SSL non-termination 두 가지 종류의 선택사항이 있습니다.

두 가지 경우 모두 서버에 사용된 것과 동일한 SSL 인증서를 WAF에 등록해 주어야 합니다.

SSL non-Termination

설정 마법사 - (192.168.21.185/24 (ID:TD5-5005-02))

웹서버 추가

IP 설정

다음과 같이 WAPPLES 및 웹 서버에 대한 네트워크 정보를 설정합니다.

Web Server IP : 192.168.3.62
Port : 80

PROXY IP : Inline Mode
Port :

SSL 사용 :
SSL 사용 안함
SSL Termination

호스트명 :
체크할 파일 :
응답 대기 시간 : 5
체크 주기 : 0
Request Method : GET

취소 < 뒤로 다음 >

SSL(SSL non-termination)방식은 WAF와 Web-server간에도 SSL통신이 그대로 유지되는 방식입니다.



설정 마법사 - (192.168.3.59/24 (ID:WHD-0003059))

웹서버 추가

인증서 가져오기

가져올 파일을 지정하십시오

인증서 파일 이름 :
찾아보기...

중개 인증서 등록
중개 인증서 파일 이름 :
찾아보기...

다음과 같은 형식의 인증서를 가져올 수 있습니다.

- PKCS #12 형식의 인증서 (.PFX, .P12)
- 단일 X.509 인증서 (.CER, .CRT) 있습니다.

취소 < 뒤로 다음 >

SSL, SSL termination 두 방식 모두 SSL 인증서와 중개인증서(해당 사항이 있을 경우)를 WAF에 등록해 주어야 합니다.



SSL Termination의 경우 Client와 WAF 사이의 통신은 기존 구성 환경과 동일한 SSL통신을 합니다. 하지만 WAF에서 Web Server의 통신은 HTTP 평문으로 통신을 하게 됩니다.

기타

WAF의 내부 Architecture, Port 운영정보, 보안 경보, 운영 장애 대응,에러처리 상태 코드 등과 같이 운영상의 발생할 수 있는 주의 사항을 소개 합니다.

WAF 사용 중 고객이 임의로 제품의 고유 기능을 변경할 경우 펜타시큐리티시스템㈜에서는 제품의 장애에 대해서 책임을 지지 않습니다.

WAF의 Port 운영 정보

WAF은 관리 도구 접속 및 다른 네트워크 장비와의 연동 등 다양한 서비스 운영을 위하여 [표 WAF이 사용하는 port]와 같은 네트워크 port를 사용합니다. WAF이 설치되어있는 네트워크 환경에서 방화벽등에 의해 해당 port의 통신이 차단되어 있는 경우 정상적인 운영이 불가능하므로, 시스템 담당자에게 해당 port의 통신을 가능하도록 조치해야 합니다.

WAF이 사용하는 port

| 서비스 | NIC 포트 | 포트 번호 |
|-----------|--------|----------|
| ICS 접속 | 관리포트 | 443, 444 |
| Syslog 연동 | 관리포트 | 514 |
| SNMP 연동 | 관리포트 | 161 |
| SMTP 연동 | 관리포트 | 25 |
| WAF MS 연동 | 관리포트 | 5432 |
| PLS 연동 | 관리포트 | 5433 |

보안 경보

보안 경보는 IP 차단, 로그인 연속 3회 실패, 데이터 관련(VII.2.4 데이터 관련 참조) 로그 발생시 메시지를 출력하여 관리자가 즉시 인지할 수 있도록 합니다.

보안 경보는 관리도구의 실행 이후에 IP 차단, 로그인 연속 3회 실패,데이터 관련 로그발생 시 메시지가 출력되며 항상 최근에 검색된 사건 1개 만을 메시지 창으로 출력합니다.

관리자는 보안 경보 메시지가 출력되면 운영자는 해당 보안 경보 메시지를 인지하고 다음과 같은 행동을 취할 수 있습니다

보안 경보

| 보안 경보 종류 | 해결 방법 |
|-----------------|---|
| IP 차단(IP Block) | [설정 마법사]->[운영 설정]->[IP 차단 설정] 에서 차단된 IP를 확인하고 운영자의 판단에 따라 해당 IP 설정 사항을 변경합니다 |
| 로그인 연속 실패 | 로그인 연속 실패가 일어난 IP를 감사로그에서 확인하고 운영자의 판단에 따라 CLI를 통해 접근 허용 IP를 수정합니다. |
| 데이터 관련 | 데이터 관련 보안 경보는 DB 용량 위험 및 DB 용량 초과로 인해 발생되며 가장 오래된 로그 순으로 [로그 내보내기] 기능을 통해 엑셀 파일로 저장합니다. |

운영 장애 대응

운영 시 발생 할 수 있는 장애에 대한 예와 해결 방법을 소개 합니다

운영 장애 대응

| 오류 메시지 | 해결 방법 |
|--|--|
| 내부 사용자는 문제가 없는 데 외부에서는 접속이 안됩니다. | 원인 게이트웨이 설정이 잘못 되었을 수 있습니다. |
| | 해결책 설정 마법사 -> 네트워크 설정 -> 게이트웨이 IP 주소 설정을 확인해 주시고 네트워크 관리자와 협조하여 정확한 게이트웨이 IP를 넣어 주십시오. |
| 웹 서비스 접속은 이상 없으나 아무런 보안 기능도 안 되는 것 같습니다. | 원인 네트워크 설정에서 웹 서버의 IP주소 설정이 잘못되었습니다. |
| | 해결책 설정 마법사 -> 네트워크 설정 -> 웹 서버 설정에서 설정된 웹 서버 목록 중 수정할 웹 서버 IP를 선택하여 수정 버튼을 눌러 정확한 IP를 입력하십시오. |
| 웹사이트에 연결 시 초기 페이지에서 "404 Not Found" 에러가 발생합니다. | 원인 웹사이트 이름 등록이 잘못 되었습니다 |
| | 해결책 설정 마법사 -> 웹사이트 설정 -> 웹사이트를 선택하여 오른쪽 마우스 버튼을 눌러 웹사이트 수정 선택 -> 정확한 웹사이트 이름으로 수정하여 주십시오. |
| | 원인 웹사이트가 등록되지 않았습니다. |
| | 해결책 설정 마법사 -> 웹사이트 설정 -> 웹사이트 추가에서 해당 웹사이트를 등록하여 주십시오. |

에러처리 상태코드

WAF 에서 공격에 대한 에러처리를 나타낼 때 사용하는 http에러코드 별 메시지와 의미는 아래와 같습니다.

HTTP 상태코드와 의미

| 상태코드 | 메시지 | 의미 |
|------|-------------------------------|------------------|
| 400 | Bad Request | 잘못된 요청 |
| 401 | Unauthorized | 인증되지 않았음 |
| 402 | Payment Required | 요금 지불 요청 |
| 403 | Forbidden | 금지되었음 |
| 404 | Not Found | 찾을 수 없음 |
| 405 | Method Not Allowed | method를 사용할 수 없음 |
| 406 | Not Acceptable | 허용할 수 없음 |
| 407 | Proxy Authentication Required | 프락시 인증 필요 |
| 408 | Request Time-out | 요구 시간 초과 |
| 409 | Conflict | 리소스간 충돌 |
| 410 | Gone | 내용물이 사라졌음 |
| 411 | Length Required | 길이가 필요함 |

| | | |
|-----|---------------------------------|-------------------|
| 412 | Precondition Failed | 사전 조건 충족 실패 |
| 413 | Request Entity Too Large | 요구 엔터티가 너무 큼 |
| 414 | Request-URI Too Large | Request-URI가 너무 김 |
| 415 | Unsupported Media Type | 지원되지 않는 미디어 유형 |
| 416 | Requested range not satisfiable | 요청 범위가 불 충분함 |
| 417 | Expectation Failed | 요청이 기대와 다름 |