문서분류	공개문서
문서취급	사외유출가능

SMILE-WAF
웹페이지 메뉴얼

(방화벽 + 웹방화벽 버전)

문 서 버 전	Ver 1.0
최초작성일	2011년 7월 13일
최근개정일	2011년 7월 13일
작 성 자	김 성 태
감 수 자	조 현 성
부 서	보안관제팀

목차

1. 메뉴구성

(1) Smile-waf 웹페이지 접속후 초기 발급된 아이디/암호로 로그인

(2) 초기화면

(3) 메뉴구성

: 로그인 아이디 관리메뉴

: 방화벽관련 메뉴

: 웹방화벽 관련 메뉴

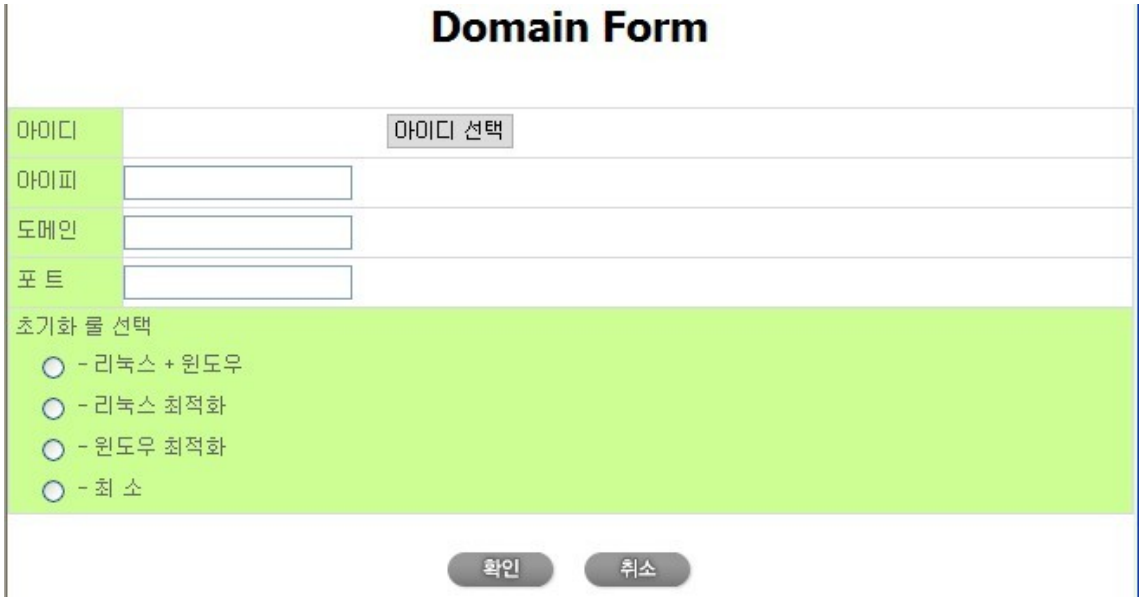
: 모니터링 관련 메뉴

등록: 도메인 등록
삭제: 도메인 삭제
룰체크: 룰의 오류등을 체크하여 이상유무를 가려냅니다
재시작: 아파치 웹데몬을 재시작합니다

2. 도메인 등록,수정,삭제 하기

(가) 등록

(1) 초기화면에서 “등록” 버튼을 누릅니다
(2) 아래와 같은 폼이 나오면 모두 입력하고 확인을 누릅니다

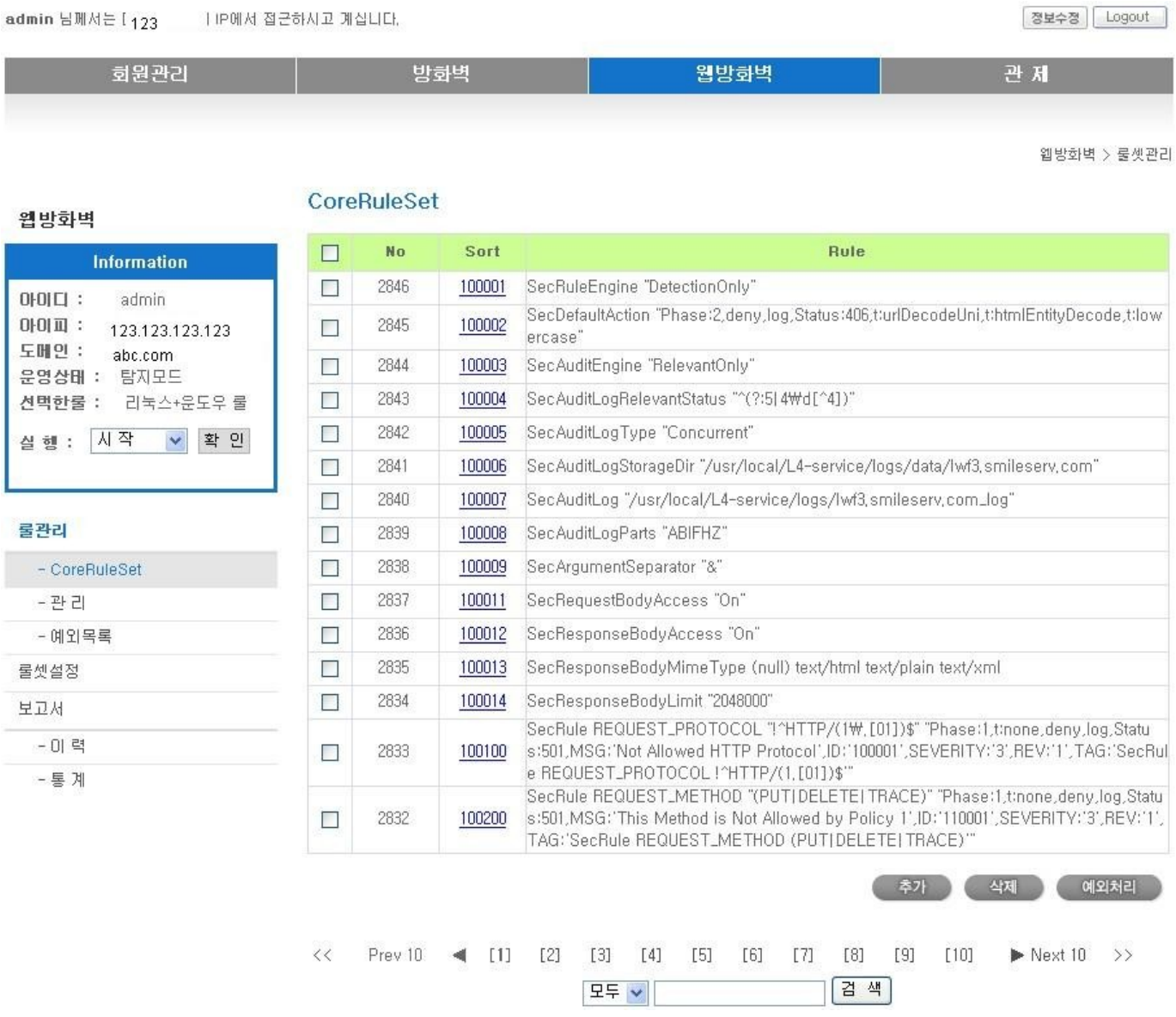


(3) 그럼 아래와 같이 등록된것을 볼수 있습니다

(나) 삭제

(1) 초기화면에서 좌측 체크박스에 체크후 하단에 “삭제” 를 눌러 삭제합니다
(주의: 웹사이트를 완전히 삭제하므로 동작을 하지 않으며 복구할수 없습니다 [재등록가능])

3. 웹방화벽 룰작업 (초기화면: 변경버튼)



- 웹방화벽 “설정” 초기화면

(가) 개요

(1) SMILE-WAF는 기본적으로 시작,중지,탐지모드 의 3가지 모드로 운영됩니다

- 시작 (운영중) : 웹방화벽의 룰셋으로 웹크래킹을 방비하고 있는중을 뜻합니다
- 중지 (중지중) : 모든 룰셋을 중지하고 있는 상태이며, 방어하지 않습니다
- 탐지 (탐지중) : 공격이 있을경우 로그에 기록만 하며, 모든 웹서비스 요청을 받아들입니다

(2) SMILE-WAF는 기본 4가지의 룰이 있습니다

- 리눅스 + 윈도우 : 모든 방어에 대해 룰을 동작시킵니다 (권장)
- 리눅스 최적화 : 리눅스 관련된 룰만 동작합니다
- 윈도우 최적화 : 윈도우 관련된 룰을 동작합니다
- 최소룰 : 웹방화벽서버의 부하가 심할경우 선택합니다

(3) SMILE-WAF의 모든 룰을 수정후에는 “완료” 버튼을 눌러 아파치의 데몬을 재시작합니다

(나) 메뉴구성

(1) CoreRuleSet : 룰셋의 리스트입니다 오탐을 주석처리하거나 추가 삭제 수정이 가능합니다
(2) 관 리 : 현재 룰셋의 초기화및 기본룰변경과 백업,복구등을 할수 있습니다
(3) 예외목록 : 오탐 주석을 처리한 결과가 이곳에 보여집니다
(4) 룰셋설정 : 공격분류에 따른 룰을 이곳에서 쉽게 On / Off 시킬수 있습니다
(5) 보고서 : 이력과 통계로 나뉘어 집니다
- 이력 : 공격을 막았을경우 그에 대한 상세한 정보를 보여줍니다
- 통계 : 일간 주간 월간 년간 으로 나누어 공격횟수(count) 의 그래프를 작성합니다

4. 웹방화벽 룰작업

(가) CoreRuleSet

CoreRuleSet

	No	Sort	Rule
☐	2846	100001	SecRuleEngine "DetectionOnly"
☐	2845	100002	SecDefaultAction "Phase:2,deny,log,Status:406,t:urlDecodeUni,t:htmlEntityDecode,t:lowercase"
☐	2844	100003	SecAuditEngine "RelevantOnly"
☐	2843	100004	SecAuditLogRelevantStatus "^(?:5|4₩d[^4])"
☐	2842	100005	SecAuditLogType "Concurrent"
☐	2841	100006	SecAuditLogStorageDir "/usr/local/L4-service/logs/data/lwf3,smileserv,com"
☐	2840	100007	SecAuditLog "/usr/local/L4-service/logs/lwf3,smileserv,com_log"
☐	2839	100008	SecAuditLogParts "ABIFHZ"
☐	2838	100009	SecArgumentSeparator "&"
☐	2837	100011	SecRequestBodyAccess "On"
☐	2836	100012	SecResponseBodyAccess "On"
☐	2835	100013	SecResponseBodyMimeType (null) text/html text/plain text/xml
☐	2834	100014	SecResponseBodyLimit "2048000"
☐	2833	100100	SecRule REQUEST_PROTOCOL "!^HTTP/(1₩,[01])$" "Phase:1,t:none,deny,log,Status:501,MSG:'Not Allowed HTTP Protocol',ID:'100001',SEVERITY:'3',REV:'1',TAG:'SecRule REQUEST_PROTOCOL !^HTTP/(1,[01])$'"
☐	2832	100200	SecRule REQUEST_METHOD "(PUT|DELETE|TRACE)" "Phase:1,t:none,deny,log,Status:501,MSG:'This Method is Not Allowed by Policy 1',ID:'110001',SEVERITY:'3',REV:'1',TAG:'SecRule REQUEST_METHOD (PUT|DELETE|TRACE)'"

추가 삭제 예외처리

<< Prev 10 ◀ [1] [2] [3] [4] [5] [6] [7] [8] [9] [10] ▶ Next 10 >>

모두 검 색

(1) 추가 : 룰셋을 추가합니다
(2) 삭제 : 체크한 룰셋을 삭제합니다
(3) 예외처리 : 특정 룰셋문제로 인해 발생한 룰셋을 주석(예외)처리합니다
(4) 수정 : 각룰셋의 Sort 번호를 클릭하여 수정합니다

(나) 관 리

룰초기화(INIT)	○ 초기화 [INIT] (최초 설치시 룰로 초기화)	룰초기화
룰 생성(CONF)	○ [Current DB -> CoreRuleSet]	생 성
룰 복구	○ [Current CoreRuleSet -> DB]	DB업데이트
룰업데이트	○ 현재룰을 업데이된 룰로 변경	룰업데이트
기본 룰 변경	◉ - 리눅스 + 윈도우 ○ - 리눅스 최적화 ○ - 윈도우 최적화 ○ - 최 소	기본룰변경

SERVER to SERVER	백 업	DB -> SQL	○ SLOT [1] : ○ SLOT [2] : ○ SLOT [3] : ○ SLOT [4] : ○ SLOT [5] :	백 업
	복 구	SQL -> DB		복 구

SERVER to PC	백 업	SQL -> PC	○ CoreRuleSet 텍스트 파일로 저장	백 업

PC to SERVER	저 장	SQL -> SQL	찾아보기... ○ SLOT [1] : ○ SLOT [2] : ○ SLOT [3] : ○ SLOT [4] : ○ SLOT [5] :	저 장
	복 구	CRS -> DB	찾아보기...	복 구

(1) 룰초기화 : 처음 생성했던 룰로 초기화 시킵니다 (오류 발생시 등에 사용)
(2) 룰생성 : 편집이 완료된 룰을 conf 파일로 복사전환 시킵니다
(3) 룰복구 : 편집중 실수한 룰을 현재 사용중인 conf 파일로부터 복구합니다
(4) 룰업데이트 : Update 서버로 부터 현재의 룰을 최신의 룰로 업데이트 합니다
(5) 기본룰변경 : 용도에 따라 기본룰을 변경합니다
(6) Server to Server 백업/복구 : 현재 룰(db)을 백업/복구합니다 (로컬백업/복구)
(7) Server to PC : 현재 룰(db)을 text 형식으로 백업합니다
(8) PC to Server : pc에 저장된 룰로 부터 복구 합니다

(다) 예외목록

☐	No	Sort	Rule
☐	4	200200	#SecRule REQUEST_URI "@pmFromFile /usr/local/L4-service/global/php_injection.txt" "chain,MSG:'PHP Injection Attack From File',ID:'200002',SEVERITY:'3',REV:'1',TAG:'SecRule REQUEST_URI @pmFromFile php_injection.txt chain (../|(http|https|ftp):/)'"
☐	3	200201	#SecRule REQUEST_URI "(₩.₩./|(http|https|ftp):/)"
☐	2	610059	#SecRule REQUEST_URI_RAW|QUERY_STRING|ARGS_NAMES|FILES|FILES_NAMES|XML:/* "(?:₩.₩s*₩w+₩₩*=)|(?:₩₩₩s*(?:location|document)₩s*₩₩[^({[;]+[({[;])|(?:₩(₩w+₩?[:₩w]+₩))|(?:₩w{30,}₩s*=₩s*₩d+[^&₩w]₩w+)|(?:₩]₩s*₩(₩s*₩w+)" "capture,multiMatch,t:none,t:urlDecodeUni,t:replaceComments,t:compressWhiteSpace,t:lowercase,ctl:auditLogParts=+E,block,auditlog,MSG:'Detects JavaScript location/document property access and window access obfuscation',ID:'615023',SEVERITY:'3',REV:'1',TAG:'WEB_ATTACK',logdata:'%{TX.0}',setvar:'tx.msg=%{rule.msg}',setvar:tx.anomaly_score=+20,setvar:tx.%{rule.id}-WEB_ATTACK-%{matched_var_name}=%{matched_var}"
☐	1	810151	#SecRule TX:/^PM_BADCODE_DATA_*/ "(₩<.*iframe src=(₩'|₩")http://.*(₩'|₩").*width=(₩'|₩")[0-9](₩'|₩").*height=(₩'|₩")[0-9](₩'|₩"))|(₩<.*iframe src=(₩'|₩")http://.*(₩'|₩").*height=(₩'|₩")[0-9](₩'|₩"))|(₩<.*iframe src=(₩'|₩")http://.*(₩'|₩").*frameborder=(₩'|₩")[0-9](₩'|₩").*height=(₩'|₩")[0-9](₩'|₩"))" "Phase:2,Phase:4,MSG:'WebShell Load Attempt enable',ID:'810149',SEVERITY:'2',REV:'1',TAG:'TX:/^PM_BADCODE_DATA_*/ iframe src=http.*width=[0-9].*height=[0-9]'"

예외해제

<< Prev 10 ◀ [1] ▶ Next 10 >>

모두 검색

- 예외해제 : 주석(예외) 처리했던 룰을 다시 룰셋으로 복구합니다

(라) 룰셋설정

- 공격형식에 따라 On/Off 합니다