

9.

연동 설정 안내서(SL3)

9.1 시작하기 전에

9.1.1 개요

본 안내서는 WAPPLES 5.0.12 버전을 기준으로 작성되었다.

여기에서는 WAPPLES과 SNMP, SYSLOG를 연동하는 설정 방법에 대해 설명한다.

9.2 SNMP 연동 설정

SNMP¹란, 네트워크에 접속되어 있는 기기를 관리하는 간이 통신망 관리 규약을 의미한다.

SNMP 연동 설정에는 v1, v2, v3가 있으며, 외부 연동 서버에서 SNMP 툴을 이용하여 설정한 연동 정보를 확인할 수 있다.

1. SNMP(Simple Network Management Protocol): 간이 통신망 관리 규약

9.2.1 SNMP Trap 연동 설정하기

WAPPLES에서 발생하는 로그를 외부 서버에 기록하기 위한 연동 서비스로, SNMP Manager가 별도 메시지를 요청하지 않더라도 자체적으로 생성하여 전송한다.

1. 관리도구의 [환경설정] - [연동] - [SNMP Trap]에서 SNMP 연동을 'ON'으로 설정한다.
2. [연동] 설정 된 목록에서  버튼 선택 후, [SNMP 등록] 창에서 SNMP 서버 정보를 입력한다.
3. 입력할 서버 정보는 다음과 같다.
 - IP
 - 포트(default: UDP 161)
 - 버전
 - 커뮤니티(SNMP 연동 톨과 동일하게 설정)
4. 신규 추가한 항목은 테이블 목록에 추가되어 표시된다.
5. 좌측  **설정 항목** 을 선택하고, 연동시킬 항목을 테이블 목록에서 선택한 후 [저장] 한다.

그림 9-1 SNMP 연동 서버 등록 화면

SNMP 등록

×

IP

포트

버전

V1

V2

V3

사용자

보안 레벨

AUTH_PRIV

AUTH_NOPRIV

NOAUTH_NOPRIV

사용자 인증

인증 비밀번호

인증 프로토콜

SHA

MD5

Private 인증

Private 비밀번호

적용

취소

SNMP Trap 탐지로그 전송 포맷

생성된 탐지 로그는 SNMP 서버로 전송되며, 전송 시 탐지 로그의 포맷은 아래와 같다.

그림 9-2 SNMP 서버로 전송되는 탐지로그 포맷

DETECTION TIME	SOURCE IP	URL	RULE NAME	RAW DATA	RESPONSE TYPE	HOST NAME	DESTINATION IP	SOURCE PORT	DESTINATION PORT	DESTINATION IPv6	POLICY NAME	VHOST	HTTP REQUEST HEADER	HTTP RESPONSE HEADER	DETECTION REASON	APPLICATION NAME
----------------	-----------	-----	-----------	----------	---------------	-----------	----------------	-------------	------------------	------------------	-------------	-------	---------------------	----------------------	------------------	------------------

- **DETECTION TIME:** 탐지된 시각
- **SOURCE IP:** 공격자 IP
- **URL:** 탐지 URL
- **RULE NAME:** 탐지된 룰
- **RAW DATA:** 탐지로그의 Raw Data
- **RESPONSE TYPE:** 대응 방법
- **HOST NAME:** 접속을 시도한 웹 사이트
- **DESTINATION IP:** 공격 받은 웹 서버 IP
- **SOURCE PORT:** 공격자 포트
- **DESTINATION PORT:** 공격 받은 웹 서버 포트
- **DESTINATION IPv6:** 공격 받은 IPv6 웹 서버
 - IPv4일 경우에는 출력되지 않는다.
- **POLICY NAME:** 탐지된 정책의 이름
- **VHOST:** 가상 호스트
 - 존재하지 않을 경우에는 출력되지 않는다.
- **HTTP REQUEST HEADER:** HTTP REQUEST에 대한 헤더
- **HTTP RESPONSE HEADER:** HTTP RESPONSE에 대한 헤더
- **DETECTION REASON:** 탐지 근거
- **APPLICATION NAME:** Application Name (사용자 입력: Sender 구분)

감사로그 SNMP 전송 포맷

감사로그가 생성되면 SNMP 서버로 전송한다.

그림 9-3 SNMP 서버로 전송되는 감사로그 포맷

AUDIT SOURCE	AUDIT TIME	AUDIT INFO	AUDIT TYPE	AUDIT MSG TYPE	AUDIT MSG	APPLICATION NAME
--------------	------------	------------	------------	----------------	-----------	------------------

- **AUDIT SOURCE:** 감사로그 원본
- **AUDIT TIME:** 감사로그 기록 시간
- **AUDIT INFO:** 감사로그 종류
- **AUDIT TYPE:** 감사로그 타입
 - GUI: 202
 - H/W 바이패스: 704

- S/W 바이패스: 703
- **AUDIT MSG TYPE:** 바이패스 설정 여부에 대한 메시지
- **AUDIT MSG:** 감사로그 메시지
- **APPLICATION NAME:** Application Name (사용자 입력: Sender 구분)

시스템 모니터 SNMP 전송 포맷

설정된 전송 주기에 따라 SNMP 서버로 시스템 리소스를 전송한다.

그림 9-4 SNMP 서버로 전송되는 시스템 모니터 포맷

CHECK TIME	CPU USED	MEM USED	CPU IDLE	CPU SYS	CPU IO	MEM TOTAL	MEM FREE	MEM CACHE	MEM BUFFER	SW BYPASS	DE TOTAL	DE STATUS	CPS	TPS	DE SESSION	DE TRAFFIC	NP SESSION	NP KERNEL BUFFER	THROUGH PUT	APPLICATION NAME
------------	----------	----------	----------	---------	--------	-----------	----------	-----------	------------	-----------	----------	-----------	-----	-----	------------	------------	------------	------------------	-------------	------------------

- **CHECK TIME:** WAPPLES 체크 시간
- **CPU USED:** WAPPLES CPU 사용률
- **MEM USED:** WAPPLES 메모리 사용률
- **CPU IDLE:** WAPPLES CPU IDLE 사용률
- **CPU USER:** WAPPLES CPU USER 사용률
- **CPU SYS:** WAPPLES CPU SYS 사용률
- **CPU IO:** WAPPLES CPU의 입출력 사용률
- **MEM TOTAL:** 전체 메모리
- **MEM FREE:** 미사용 메모리
- **MEM CACHE:** 캐시 메모리
- **MEM BUFFER:** 버퍼 메모리
- **SW BYPASS:** S/W 바이패스의 상태
- **DE TOTAL:** 탐지 엔진 수
- **DE STATUS:** 탐지 엔진 상태
- **CPS:** 초(sec) 당 커넥션 수
- **TPS:** 초(sec) 당 트랜잭션 수
- **DE SESSION:** 탐지 엔진의 동시 세션 수
- **DE TRAFFIC:** 탐지 엔진의 트래픽
- **NP SESSION:** NP 동시 세션 수
- **NP KERNEL BUFFER:** NP 커널 버퍼 수
- **THROUGHPUT:** 초(sec) 당 처리량
- **APPLICATION NAME:** Application Name (사용자 입력: Sender 구분)

차단된 IP SNMP 전송 포맷

차단된 IP가 발생한 경우 SNMP 서버로 전송한다.

그림 9-5 SNMP 서버로 전송되는 '차단된 IP' 전송 포맷

CLIENT ADDRESS	BLOCK DURATION	CLIENT IPv6 ADDRESS	REASON	APPLICATION NAME
----------------	----------------	---------------------	--------	------------------

- **CLIENT ADDRESS:** 차단된 클라이언트 IP
- **BLOCK DURATION:** 차단 지속 시간
- **CLIENT IPv6 ADDRESS:** 차단된 클라이언트 IPv6
 - IPv4일 경우에는 출력되지 않는다.
- **REASON:** IP 차단 근거
- **APPLICATION NAME:** Application Name (사용자 입력: Sender 구분)

웹 사이트 상태 SNMP 전송 포맷

웹 사이트의 '부가 정보'에 설정된 상태 주기에 따라, SNMP 서버로 웹 사이트 상태를 전송한다.

그림 9-6 웹 사이트 상태 SNMP 전송 포맷

START TIME	END TIME	STATUS CODE	TIMEOUT OCCURRENCE	HOST NAME	URL	APPLICATION NAME
------------	----------	-------------	--------------------	-----------	-----	------------------

- **START TIME:** 웹 서버 체크 시작 시간
- **END TIME:** 웹 서버 체크 종료 시간
- **STATUS CODE:** 웹 서버 체크 결과 코드
- **TIMEOUT OCCURRENCE:** 웹 서버 체크 시 발생한 타임 아웃 정보
- **HOST NAME:** 접속을 시도한 웹 사이트
- **URL:** 탐지 URL
- **APPLICATION NAME:** Application Name (사용자 입력: Sender 구분)

9.2.2 SNMP Agent 연동 설정하기

SNMP Agent는 SNMP Manager가 OID 형식의 쿼리문으로 요청할 경우, WAPPLES에서 요청한 OID 쿼리문에 매칭되는 정보를 제공한다.

WAPPLES SNMP OID 관련된 내용은 <[6. WAPPLES SNMP OID 정보](#)>를 참조한다.

SNMP v2, v3는 Agent를 사용하며, SNMP Agent를 이용한 연동 설정 방법은 다음과 같다.

1. [환경설정] - [연동] - [SNMP Agent] 화면으로 이동한다.
2. SNMP Agent에서 SNMP 툴의 포트와 SNMP 접근 제어 설정 정보를 동일하게 설정한다.



단, SNMP v2는 암호화를 하지 않으므로, 별도 SNMP 접근 제어에 대해 설정하지 않는다.

3. 연동 서버에서 SNMP 툴을 이용하여, 등록된 Agent에 OID 형식의 쿼리문을 전송한다.
4. WAPPLES에서 SNMP 툴을 이용하여 OID 형식에 맞는 정보를 전송한다.

그림 9-7 SNMP Agent 설정 화면

서비스 포트

161

SNMP 접근 제어 설정

ON

커뮤니티

SNMP v3 접근 제어 설정

ON

사용자

보안 레벨

AUTH_PRIV

AUTH_NOPRIV

NOAUTH_NOPRIV

인증 비밀번호

인증 프로토콜

SHA

MD5

Private 비밀번호

Private 프로토콜

AES

DES

저장

취소

9.3 SYSLOG 연동 설정

SYSLOG 연동을 통해, 원격으로 SYSLOG 서버에 '감사로그/탐지로그/시스템 정보' 등을 전송한다.

1. [환경설정] - [연동] - [SYSLOG] 에서 SYSLOG 연동 기능을 'ON'으로 설정한다.
2. SYSLOG 서버의 IP, 포트, 프로토콜에 대해 각각 설정한다.
3. 좌측의 **설정 항목** 을 선택한 후 [저장] 한다.

그림 9-8 SYSLOG 연동 설정 화면

SYSLOG 연동 ON

설정 항목

탐지 로그

- Access Control
- Buffer Overflow
- Content Spoofing
- Cookie Poisoning
- Cross Site Request Forg...
- Cross Site Scripting
- Directory Listing
- Directory Traversal
- Error Handling
- Extension Filtering

감사 로그

- WAPPLES 설정
- CLI 설정
- 로그인
- 네트워크
- 리소스 알림
- 보고서 전송
- DB (MariaDB)
- PLS
- 시간 동기화

시스템 모니터

전송 주기: 10초

	IP	포트	프로토콜
☐	Q	Q	(All)

IP: * 포트: *

프로토콜: *

적용 **취소**

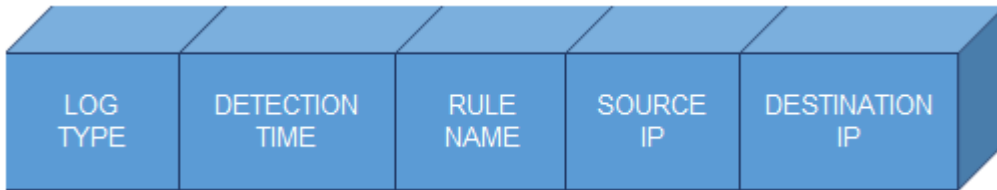
	수정	1.1.1.0	133	TCP
☐				

탐지로그 SYSLOG 전송 포맷

탐지로그(기본)

WAPPLES에서 탐지로그가 발생할 경우, SYSLOG 서버로 탐지로그를 전송한다.

그림 9-9 SYSLOG 서버로 전송되는 탐지로그(기본) 포맷



- **LOG TYPE:** 로그 유형
- **DETECTION TIME:** 탐지된 시각
- **RULE NAME:** 탐지된 룰
- **SOURCE IP:** 공격자 IP
- **DESTINATION IP:** 공격 받은 웹 서버 IP

탐지로그(자세히)

탐지로그의 연동 설정 시, 전송 포맷을 '자세히'로 설정한 경우, 아래와 같이 보다 자세한 정보를 확인할 수 있다.

그림 9-10 SYSLOG 서버로 전송되는 탐지로그(자세히) 전송 포맷

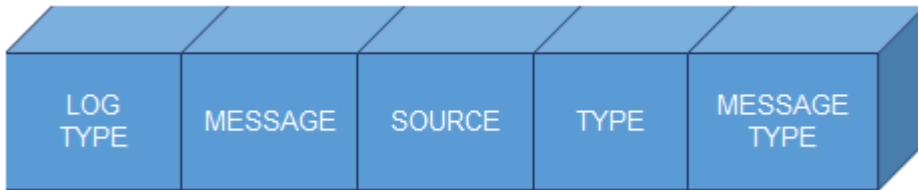


- **LOG TYPE:** 로그 유형
- **DETECTION TIME:** 탐지된 시각
- **SOURCE IP:** 공격자 IP
- **URL:** 탐지 URL
- **RULE NAME:** 탐지된 룰
- **HOST NAME:** 접속을 시도한 웹 사이트
- **DESTINATION IP:** 공격 받은 웹 서버 IP
- **RESPONSE TYPE:** 대응 설정
- **RISK:** 위험도
- **POLICY NAME:** 정책명
- **VHOST NAME:** 가상 호스트
- **STATUS CODE:** 응답 코드
- **REASON:** 탐지 근거
- **HTTP REQUEST HEADER:** HTTP Request에 대한 헤더
- **HTTP RESPONSE HEADER:** HTTP Response에 대한 헤더
- **RAW DATA:** 탐지로그에 대한 Raw Data

감사로그 SYSLOG 전송 포맷

WAPPLES에서 감사로그가 발생할 경우, SYSLOG 서버로 감사로그를 전송한다.

그림 9-11 SYSLOG 서버로 전송되는 감사로그 전송 포맷

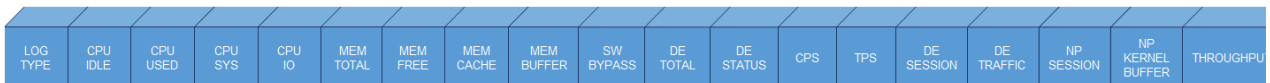


- **LOG TYPE:** 로그 유형
- **MESSAGE:** 감사로그의 상세 내용
- **SOURCE:** 감사로그의 원본
- **TYPE:** 연동 설정한 감사로그 유형
- **MESSAGE TYPE:** 감사로그의 메시지 유형

시스템 모니터 SYSLOG 전송 포맷

설정된 시간 간격에 따라, 시스템 정보를 SYSLOG 서버로 전송한다.

그림 9-12 SYSLOG 서버로 전송되는 시스템 리소스 전송 포맷

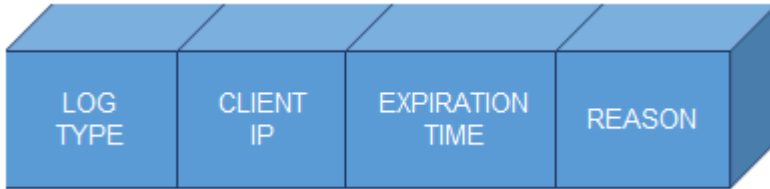


- **LOG TYPE:** 로그 유형
- **CPU IDLE:** WAPPLES CPU IDLE사용률
- **CPU USER:** WAPPLES CPU USER 사용률
- **CPU SYS:** WAPPLES CPU SYS 사용률
- **CPU IO:** WAPPLES CPU 입출력 사용률
- **MEM TOTAL:** 전체 메모리
- **MEM FREE:** 미사용 메모리
- **MEM CACHE:** 캐시 메모리
- **MEM BUFFER:** 버퍼 메모리
- **SW BYPASS:** S/W 바이패스의 상태
- **DE TOTAL:** 탐진 엔진 수
- **DE STATUS:** 탐지 엔진 상태
- **CPS:** CPS
- **DE SESSION:** 탐지 엔진의 동시 세션 수
- **DE TRAFFIC:** 탐지 엔진의 트래픽
- **NP SESSION:** NP 동시 세션 수
- **NP KERNEL BUFFER:** NP 커널 버퍼 수
- **THROUGHPUT:** 초(sec) 당 처리량

차단된 IP SYSLOG 전송 포맷

WAPPLES IP가 차단된 경우, 차단된 IP 정보를 SYSLOG 서버로 전송한다.

그림 9-13 SYSLOG 서버로 전송되는 차단된 IP 전송 포맷

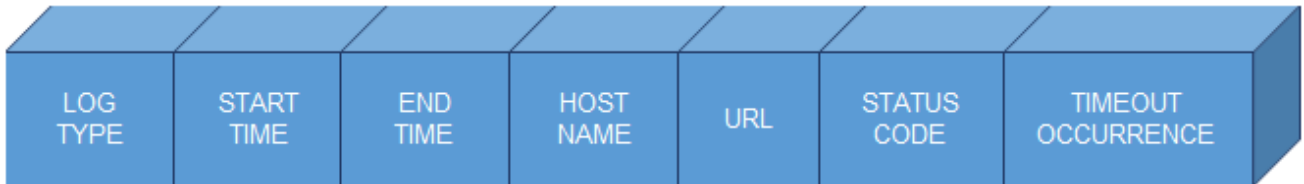


- LOG TYPE: 로그 유형
- CLIENT IP: 차단된 클라이언트 IP
- EXPIRATION TIME: 차단 종료 시간
- REASON: IP 차단 근거

웹 사이트 상태 SYSLOG 전송 포맷

웹 사이트의 [부가 정보]에 설정된 상태 주기에 따라, 웹 사이트의 체크 정보를 SNMP 서버로 전송한다.

그림 9-14 SYSLOG 서버로 전송되는 웹 사이트 상태 전송 포맷



- LOG TYPE: 로그 유형
- START TIME: 웹 서버 체크 시작 시간
- END TIME: 웹 서버 체크 종료 시간
- HOST NAME: 접속을 시도한 웹 사이트
- TIMEOUT OCCURRENCE: 웹 서버 체크 시 발생한 타임 아웃 정보