

WAPPLES SA 접속 및 보호대상 설정 가이드

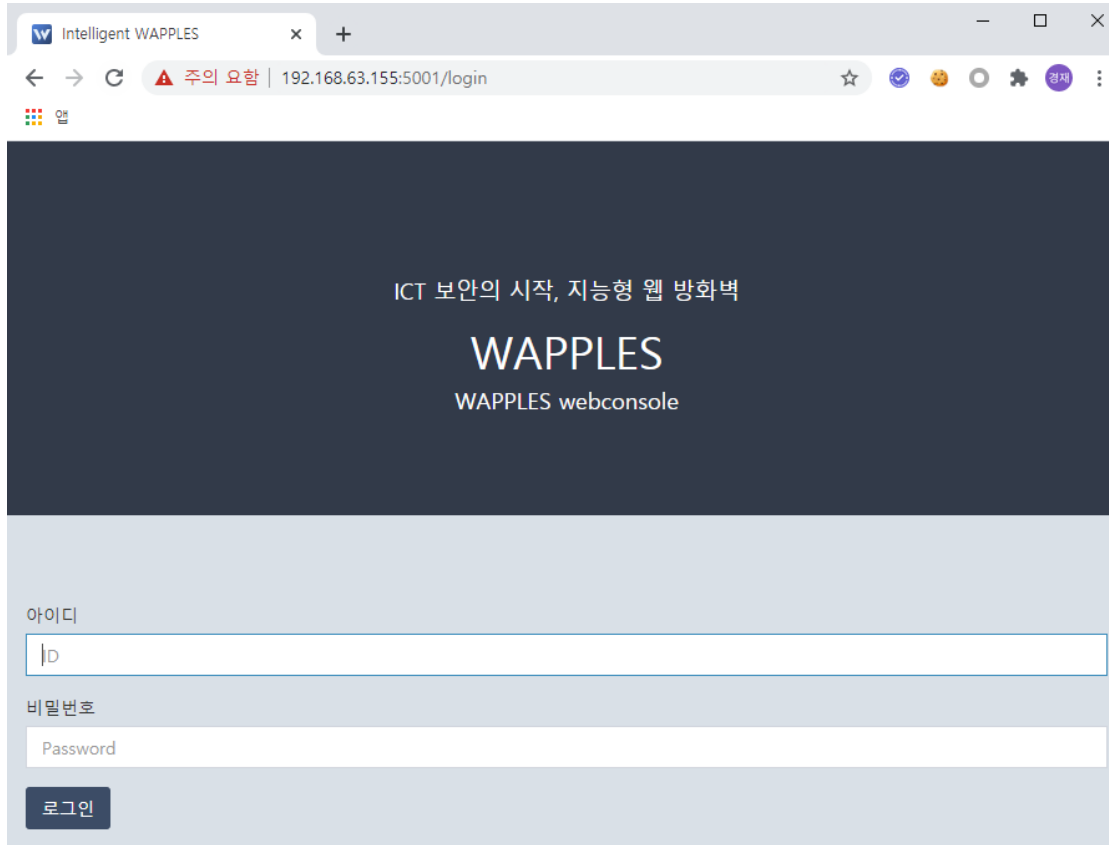
목차

- I. 웹방화벽 접속 방법
- II. 보호 대상 정보 설정
- III. 정책 설정
- IV. X-forwarded-for 설정

웹방화벽 접속 방법

웹방화벽 접속 방법

■ 관리도구

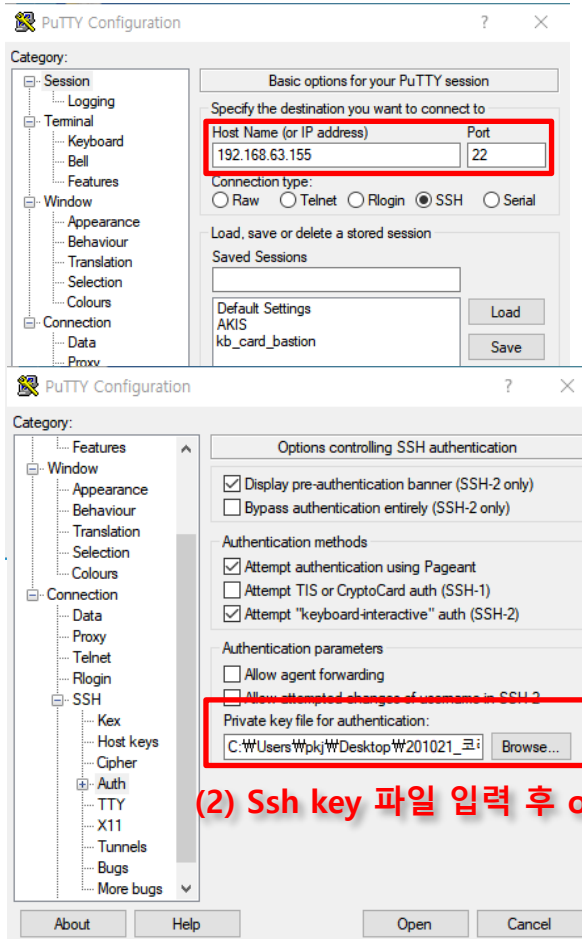


(1) 브라우저(크롬 권장)에서 웹방화벽 GUI 접속

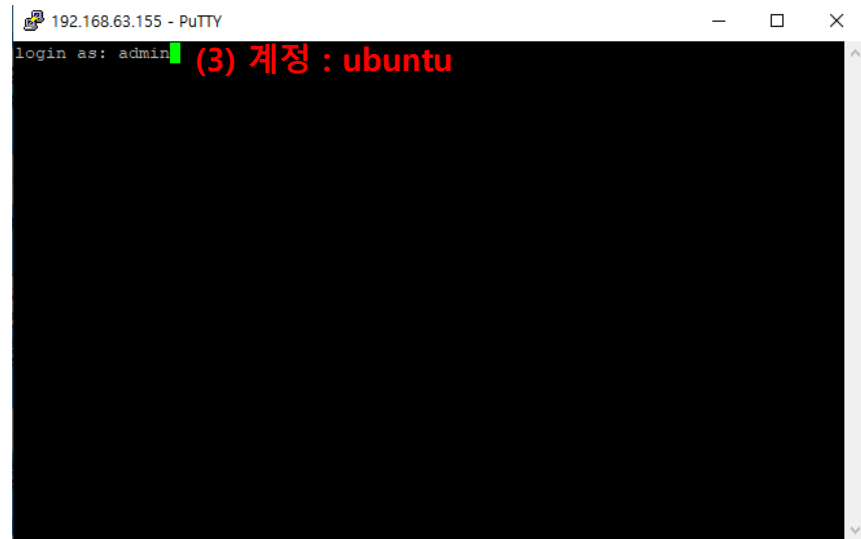
- <https://WAF IP:5001>
- ID : admin
- PW : penta7728.

웹방화벽 접속 방법

■ SSH



(1) Ssh프로그램 이용, 웹방화벽 IP 및 port 입력



(2) Ssh key 파일 입력 후 open

보호 대상 정보 설정

초기 설정

■ 프록시 IP 설정

```
pentasec@ip-172-31-31-132:(network) # show if
br0
  LINK - address: 0a:fc:89:9e:b4:60, broadcast ff:ff:ff:ff:ff:ff
  INET - address: 172.31.31.132/20
ens5
  LINK - address: 0a:fc:89:9e:b4:60, broadcast ff:ff:ff:ff:ff:ff
pentasec@ip-172-31-31-132:(network) # show rt
DESTINATION: default, GATEWAY: 172.31.16.1, IFACE: br0
DESTINATION: 172.31.16.0/20, GATEWAY: 0.0.0.0, IFACE: br0
DESTINATION: 172.31.16.1/32, GATEWAY: 0.0.0.0, IFACE: br0
pentasec@ip-172-31-31-132:(network) #
```

웹방화벽 IP 정보 확인

- (1) SSH enable 모드 접속
 - enable 모드 명령어 : enable
 - enable PW : Penta@1997

(2) network 이동

(3) show if 와 show rt 수행

보안 설정 > 네트워크 설정 > 프록시 IP (서비스 네트워크를 설정합니다.)

(4) '+' 클릭 후 SSH 에서 확인한 정보 입력

프록시 IP	네트mask	게이트웨이
172.31.31.132	255.255.240.0	172.31.16.1

(5) '적용' 클릭

(6) '저장' 클릭

보호대상 정보 등록

■ 보호 대상 서버 등록(단일 방식)

WAPPLES

대시보드 < 통계 분석 < 로그 조회 < 보안 설정 > 네트워크 설정 > 보호 대상 서버 (웹 서버를 추가/수정/삭제할 수 있습니다.)

(1) '+' 클릭 후 보호 대상 서버 추가

(2) 서버 모드 Proxy 선택

(3) 웹방화벽 프록시 IP 선택 및 Port 입력 (프록시 IP는 사전에 입력한 프록시 IP가 자동 선택 되어짐)

(4) 보호대상 서버 IP(또는 인스턴스 DNS 주소) 및 Port 정보 입력

(5) '적용' 클릭 후 저장

보호대상 정보 등록

■ 보호 대상 서버 등록(다중 방식)

보호 대상 서버 수정

서버 모드

Inline

Proxy

T.Proxy

단일 호스트 LB

다중 호스트 LB

프록시 IP

172.31.31.132

프록시 포트

80

단일

다중

+

호스트 기준으로 보호대상 서버 IP 입력

검색....

	호스트명	대상 웹 서버	포트	헬스 체크	적... ↑
수정 삭제	www.abc.com	172.31.29.15	80	사용 안 함	1

SSL 설정

SSL 사용 안 함

SSL 사용

SSL Termination

VLAN 아이디

인증서 파일

인증서 상세 정보

적용

취소

정책 설정

초기 설정

■ 탐지 정책 설정

The screenshot shows the WAPPLES interface with the '탐지 정책 설정' (Detection Policy Setting) menu item highlighted in the left sidebar. The main area displays the '정책 목록' (Policy List) table. A red box highlights the '+' button in the top-left corner of the table, with a red arrow pointing to it. A red box also highlights the '정책' (Policy) tab in the '정책/웹 사이트 추가' (Add Policy/Website) dialog box. The dialog box shows the '정책명' (Policy Name) field with the value 'test' and the '사용할 기반 정책을 선택해 주세요.' (Please select the base policy to use.) dropdown menu with the value '1. 탐지만 하고 차단 안 함' (Detect only, do not block).

(1) '+' 클릭 후 탐지 정책 생성

정책/웹 사이트 추가

정책명: test

사용할 기반 정책을 선택해 주세요.
1. 탐지만 하고 차단 안 함

(2) 기반 정책 선택 후 '적용' 클릭

(2) 기반 정책 선택 후 '적용' 클릭
- 일반적으로 최초 구축 후 탐지 수행할 경우
'탐지만 하고 차단 안 함' 선택

The screenshot shows the WAPPLES interface with the '정책 목록' (Policy List) table. A red box highlights the '미등록 웹 사이트' (Unregistered Website) button in the top-right corner of the table, with a red arrow pointing to it. A red box also highlights the '미등록 웹 사이트' (Unregistered Website) button in the '웹 사이트 이동' (Move Website) dialog box. The dialog box shows the '선택한 웹 사이트' (Selected Website) field with the value '미등록 웹 사이트' and the '이동할 정책을 선택해 주세요.' (Please select the policy to move to.) dropdown menu with the value 'test'. The '적용' (Apply) button is highlighted in a red box.

(3) '미등록 웹 사이트' 선택 후 'G' 버튼 클릭하여 적용 정책 변경

웹 사이트 이동

선택한 웹 사이트: 미등록 웹 사이트

이동할 정책을 선택해 주세요.
test

(4) 정책 선택 후 '적용' 클릭

(5) '저장' 클릭

(5) '저장' 클릭

보호대상 정보 등록

■ 보호 대상 도메인 등록

보안 설정 > 정책 (WAPPLES에서 사용할 정책과 웹 사이트를 설정합니다.)

정책 목록

(1) '+' 클릭 후 웹사이트 추가

+  검색....

☒ 정책/웹 사이트

☐ 6.무조건 차단

☐ 5.PCI-DSS 보안 정책

☐ 4.고급 보안 정책

☐ 3.표준 보안 정책

☐ 2.기본 보안 정책

☐ 1.탐지만 하고 차단 안 함

☐ 0.탐지없이 통과

☒ test01

▶ ☐ test10

정책/웹 사이트 추가

정책 **웹 사이트** (2) 웹사이트 선택

웹 사이트 이름 포트

www.test.com 80 (3) 보호대상 도메인 및 포트 정보 입력

서브 디렉터리 -option

웹 사이트를 저장할 정책을 선택해 주세요.

test01 (4) 기존에 생성한 정책 선택

적용 x 취소 (5) '적용' 클릭 후 저장

X-forwarded-for 설정

초기 설정

■ X-Forwarded-For 설정(WAF 가 최상단이 아닌 경우 설정)

X-forwarded-for 헤더에 있는 IP로 탐지 및 / 차단이 필요한 환경에서 사용

The screenshot displays the WAPPLES WAF configuration interface. On the left is a dark sidebar with a menu. The main content area is titled '보안 설정 > 정책 부가 설정 > X-Forwarded-For (X-Forwarded-For를 설정합니다.)'. It contains two sections: 'Block X-Forwarded-For IP:' and 'Detect by X-Forwarded-For IP:'. Both sections have a toggle switch set to 'ON' and a text description. At the bottom right, there are '저장' (Save) and '취소' (Cancel) buttons.

WAPPLES

대시보드 < | 통계 분석 < | 로그 조회 < | **보안 설정** > | 네트워크 설정 < | 정책 설정 < | **정책 부가 설정** > | **◎ X-Forwarded-For** > | Access Control < | 자동 차단 필터 < | 탐지 예외 < | 패턴 저장소 < | S/W 바이패스 < | 보고서 < | 환경 설정 < |

보안 설정 > 정책 부가 설정 > X-Forwarded-For (X-Forwarded-For를 설정합니다.)

Block X-Forwarded-For IP: ☒ ON **(1) 옵션 ON 설정**

설명: 헤더의 X-Forwarded-For에 있는 IP를 차단합니다.
X-Forwarded-For 헤더가 없는 경우, 네트워크 출발지 IP를 차단합니다.

Detect by X-Forwarded-For IP: ☒ ON

설명: 헤더의 X-Forwarded-For에 있는 IP로 탐지합니다.
X-Forwarded-For 헤더가 없는 경우, 네트워크 출발지 IP로 탐지합니다.

저장 **취소**

(2) 옵션 선택 후 '저장' 클릭

t h a n k y o u



KOREA Yeouido, Seoul www.pentasecurity.com (HQ)
U.S.A. Houston, Texas www.pentasecurity.com/en
JAPAN Shinjuku-Ku, Tokyo www.pentasecurity.co.jp