PIOLINK

PIOLINK

웹 보안에 최고 성능을 담다

WEBFRONT-KS

㈜파이오링크

PIOLINK

개요

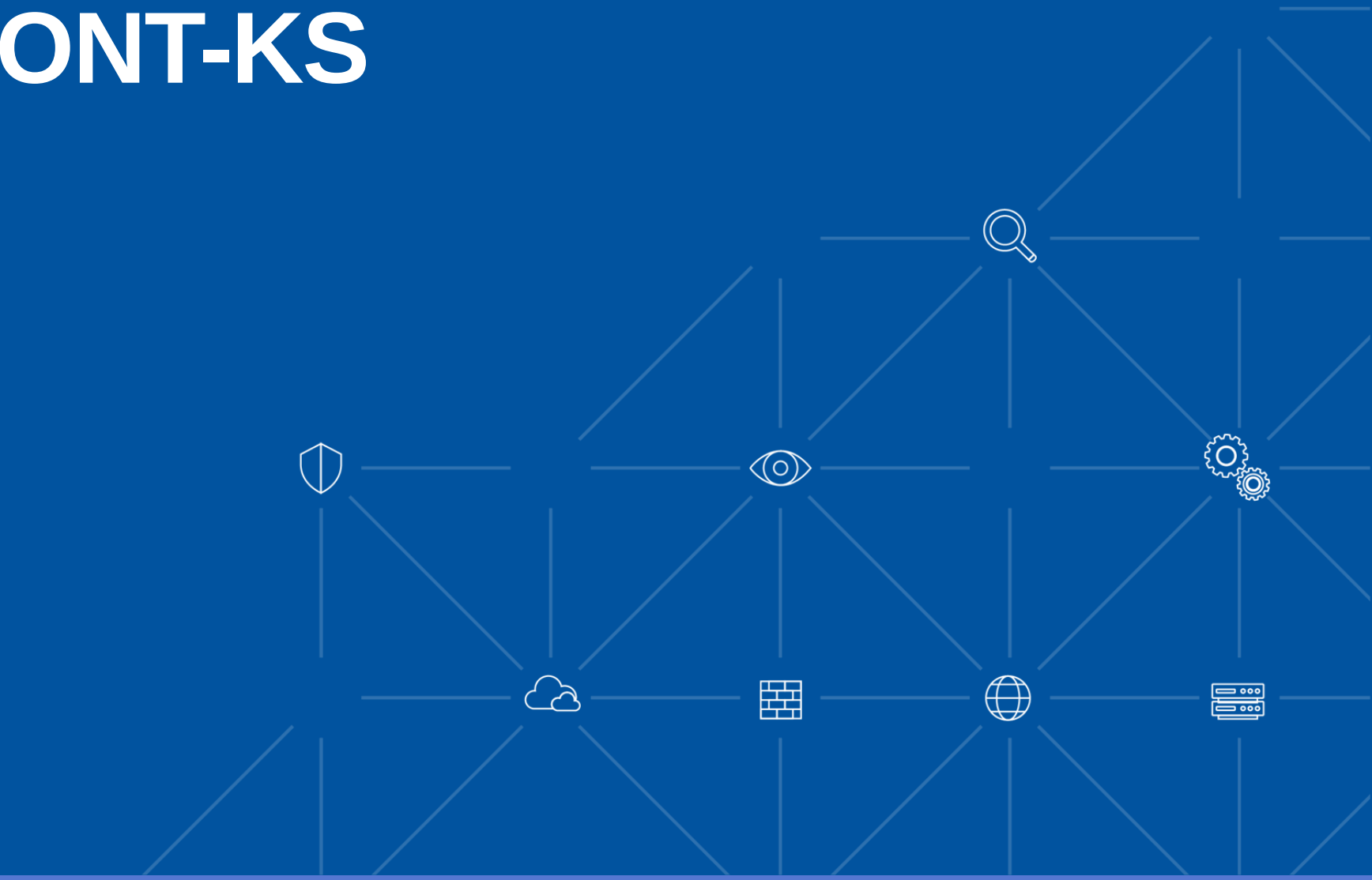
1. WEBFRONT-KS
2. 메뉴 설명
3. 기본 사용 방법
4. 기본 설정
5. 설정 체크리스트

PIOLINK

PIOLINK

PIOLINK

1. WEBFRONT-KS



PIOLINK

웹방화벽이란?

웹방화벽

- 웹 애플리케이션과 인터넷 간의 웹 트래픽을 모니터링/필터링하여 웹 애플리케이션 및 웹 서버를 보호하는 솔루션

- XSS, CSRF, SQL injection 등의 공격을 방어

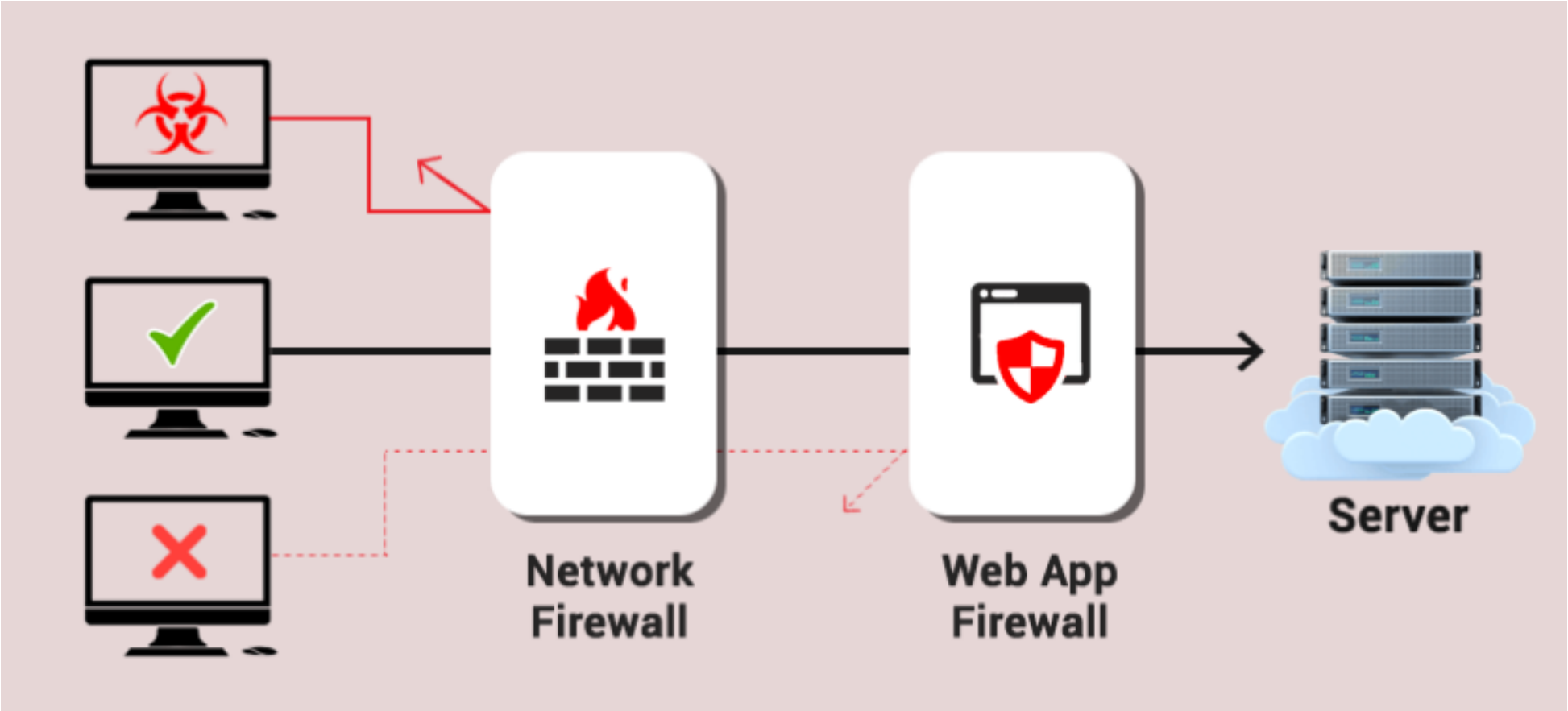
- L7 계층에서 동작

- 리버스 프록시로 주로 동작

항목	방화벽	웹방화벽
역할	허용되지 않은 접근을 차단	웹 공격을 차단
검사대상	네트워크 트래픽	웹트래픽 (HTTP/HTTPS)
방어대상	내부 네트워크 및 자산	웹애플리케이션, 웹서버
차단대상	비정상/비인가 접근	XSS, SQL인젝션, 쿠키 조작 등
OSI 계층	3 / 4	7

PIOLINK

웹방화벽이란?



PIOLINK

WEBFRONT-KS

WEBFRONT-KS 장점

- 국내 유일 네트워크스위치 Base의 WAF
  - 네트워크 스위치 Base이므로 구축에 용이

- L7 SLB (Server Load Balance) 가능
  - **별도 L7 없이 SLB 지원**

- 사용자 정의 필터 기능
  - 다양한 조건 값 (항목, 변수, 값, 조건 등) 의 사용자 정의 필터 가능

- 업데이트
  - 시그니처 월 1회 (자동 업데이트 X)
  - PLOS 분기별 1회

PIOLINK

WEBFRONT-KS

WEBFRONT-KS

- 클라우드 전용 웹방화벽

- private 클라우드 + public 클라우드(AWS, NHN Cloud, Azure)

- 자체 부하분산 지원 (별도의 스위치나 LB 없이 구성 가능)

- 인스턴스 간편 생성, 기본설정 자동 적용 > 간단한 웹방화벽 구성

PIOLINK

WEBFRONT-KS

WEBFRONT-KS 보안 검사

1-1) 요청검사

- 웹 보안의 가장 중요한 기능으로 클라이언트가 웹 서비스에 대한 **요청**을 보냈을 때 악의적인 요청 및 침입을 검사하여 차단

1-2) 시그니처 기반 탐지

- 보안기능과 별개로 시그니처를 기반으로 탐지/차단 수행

(기본정책: 탐지)

2) 응답검사

- 클라이언트 요청에 대한 웹 서비스의 **응답**을 확인하여 차단 또는 마스킹(Masking)
- 신용 카드나 주민등록번호 등의 개인 정보 및 서버 정보 유출 차단

PIOLINK

2. 메뉴 설명

WEBFRONT-KS 메뉴

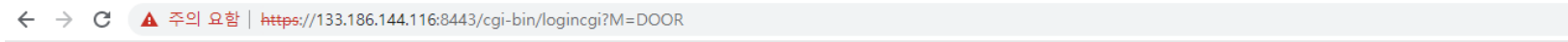
WEBFRONT-KS 메뉴

웹UI 접속 경로

https://{mgmt IP}:8443

계정: wfadmin // 비밀번호: waf12!@{인스턴스 이름 첫 5글자}

- 만약 인스턴스의 이름이 5글자가 되지 않는다면, 인스턴스 이름 전체를 입력
- 특수문자 및 숫자도 그대로 입력

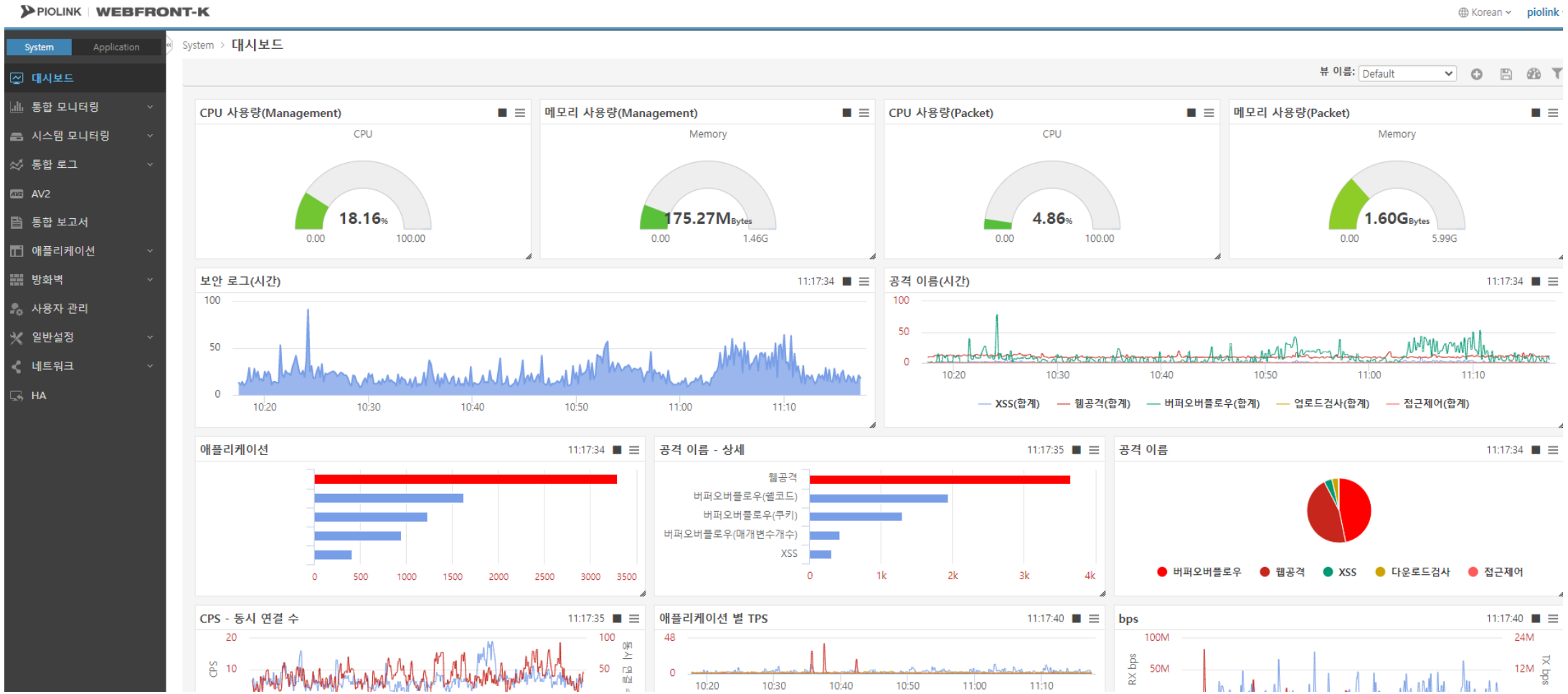


WEBFRONT-KS 메뉴

WEBFRONT-KS 메뉴

대시보드

장비의 전반적인 하드웨어 상태 및 보안 현황을 시각화 하여 표기함



PIOLINK

WEBFRONT-KS 메뉴

WEBFRONT-KS 메뉴

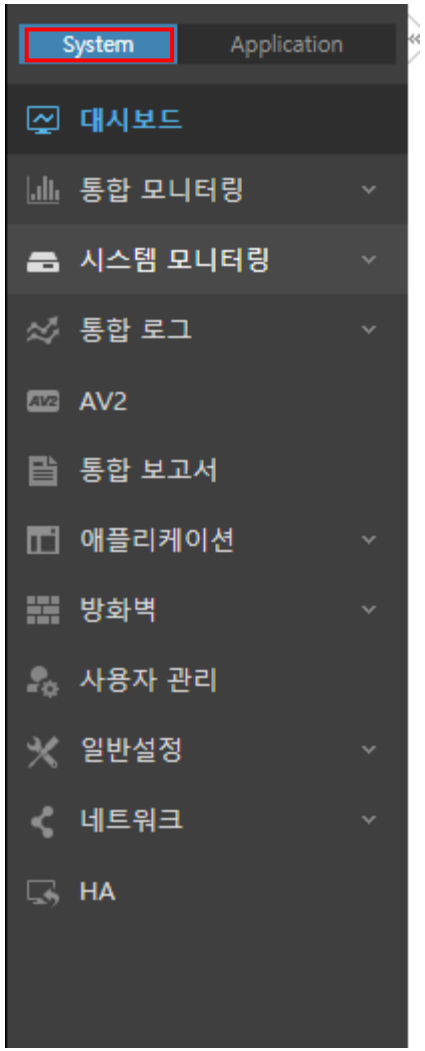
기본 메뉴

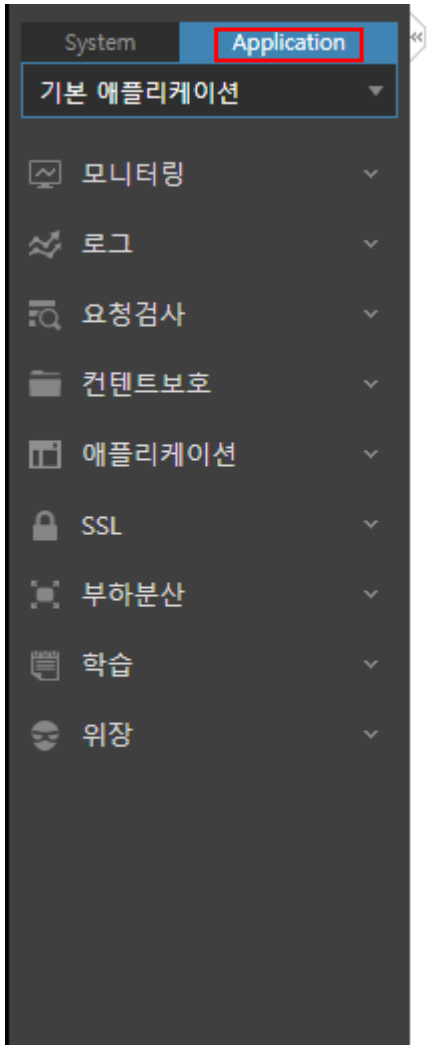
1) System

- 웹방화벽 내 전반적인 설정 가능
- 네트워크, 사용자 관리, 모니터링 등

2) Application

- 애플리케이션: WEBFRONT-KS에서 웹 보안 기능을 적용하는 단위
- 특정 애플리케이션에 대한 보안 기능 설정 가능
- 애플리케이션의 요청검사 설정 등

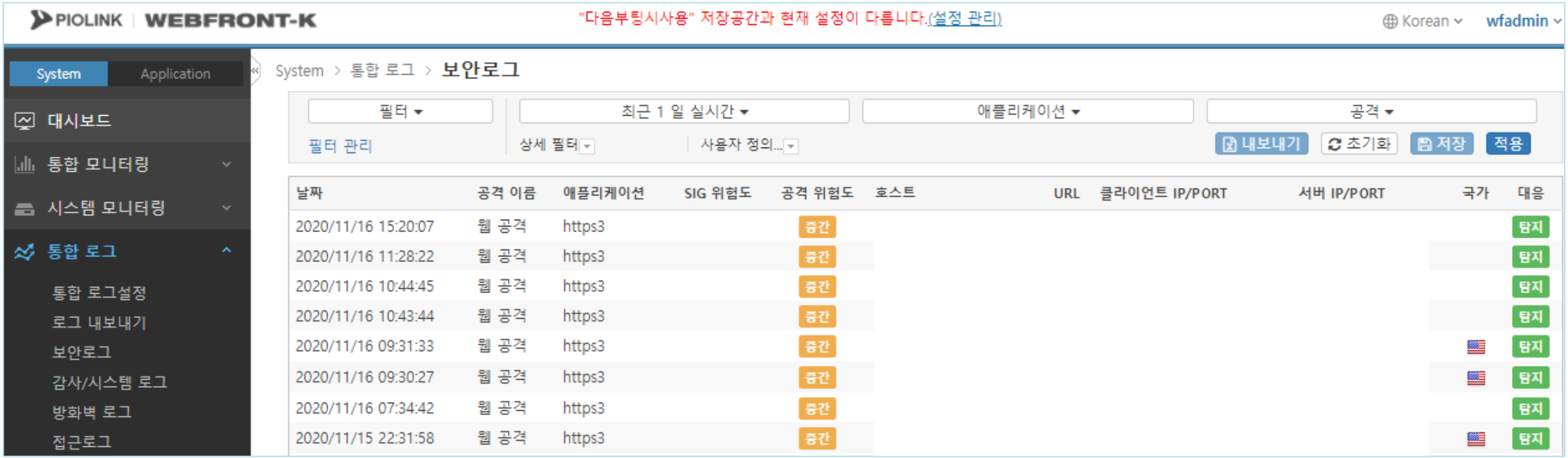




WEBFRONT-KS 메뉴

WEBFRONT-KS 메뉴

보안 로그 (이벤트 로그) 확인 (System > 통합로그 > 보안로그)



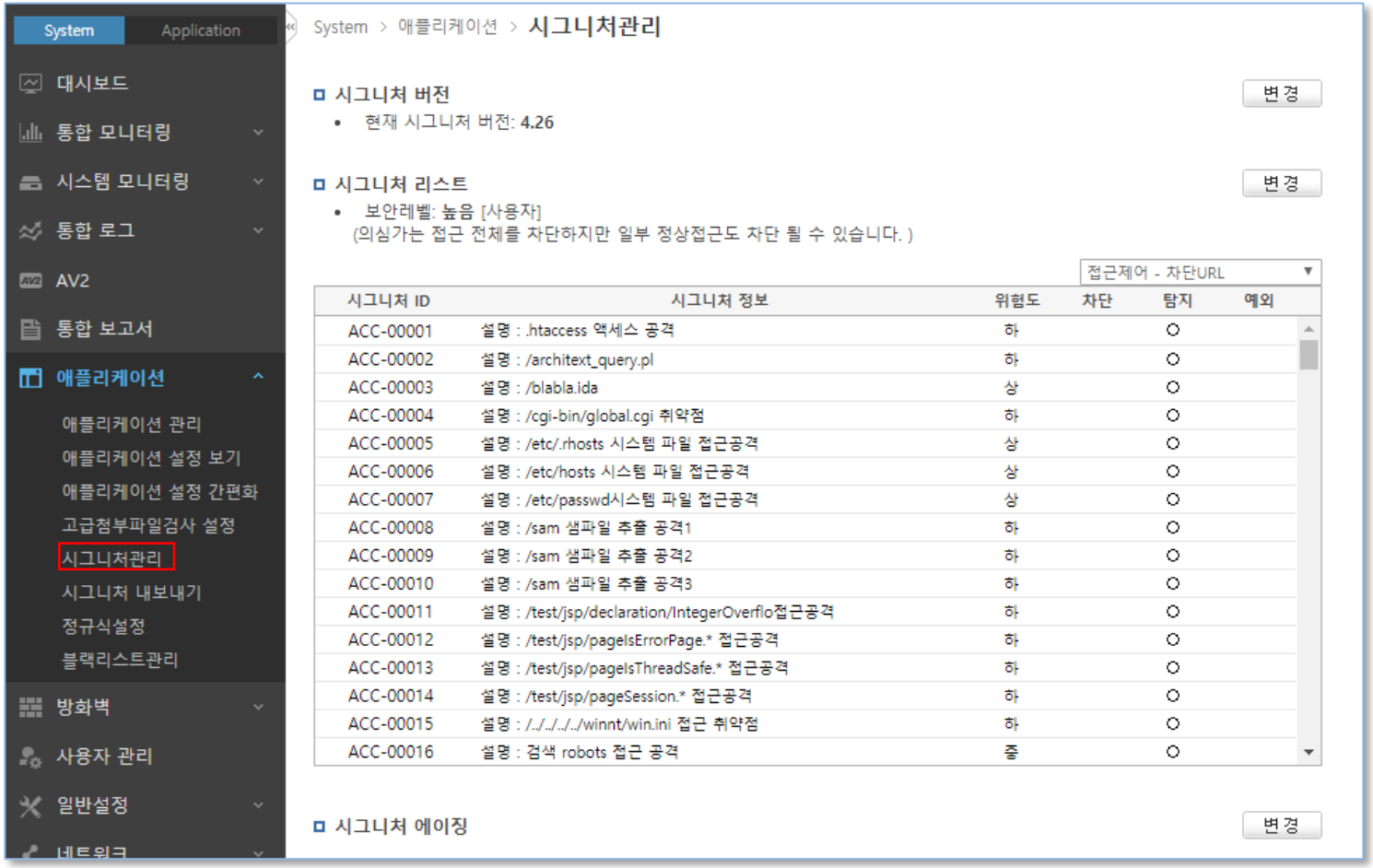
WEBFRONT-KS 메뉴

WEBFRONT-KS 메뉴

시그니처관리 (System > 애플리케이션 > 시그니처관리)

웹 공격에 사용되는 패턴을 정의한 후 각 패턴에 대해 차단/탐지/예외 정책을 애플리케이션 별로 설정하여 관리

- 시그니처 버전 관리
- 시그니처 리스트 관리
- 사용자 시그니처
- 시그니처 에이징



WEBFRONT-KS 메뉴

WEBFRONT-KS 메뉴

사용자 관리 (System > 사용자관리)

WEBFRONT-KS에 접속하는 사용자 관리

사용자 권한

통합관리자 : 모든 메뉴 사용 가능

사이트 관리자 : 사용자 관리를 제외한 모든 메뉴 사용 가능

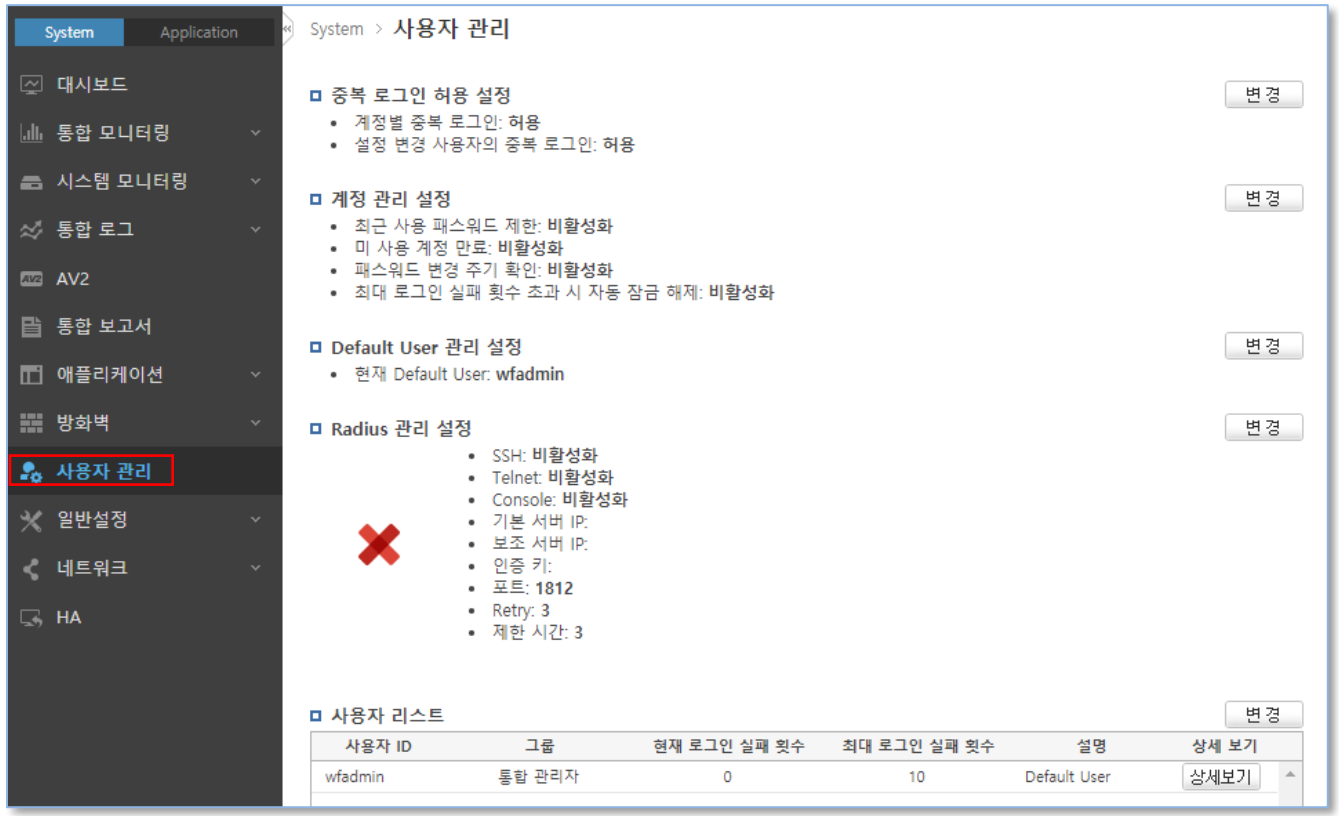
애플리케이션 관리자 : 지정한 애플리케이션만 관리 가능 (복수 애플리케이션 지정 가능)

모니터 관리자 : 시스템 정보만 볼 수 있음 시스템 메뉴 중 대시보드, 시스템 정보, 포트 모니터링 메뉴만 사용 가능

최대 로그인 실패 횟수

정해진 횟수 만큼 연속 로그인이 실패 할 경우 해당 계정으로 로그인 불가

통합 관리자만 해제 가능

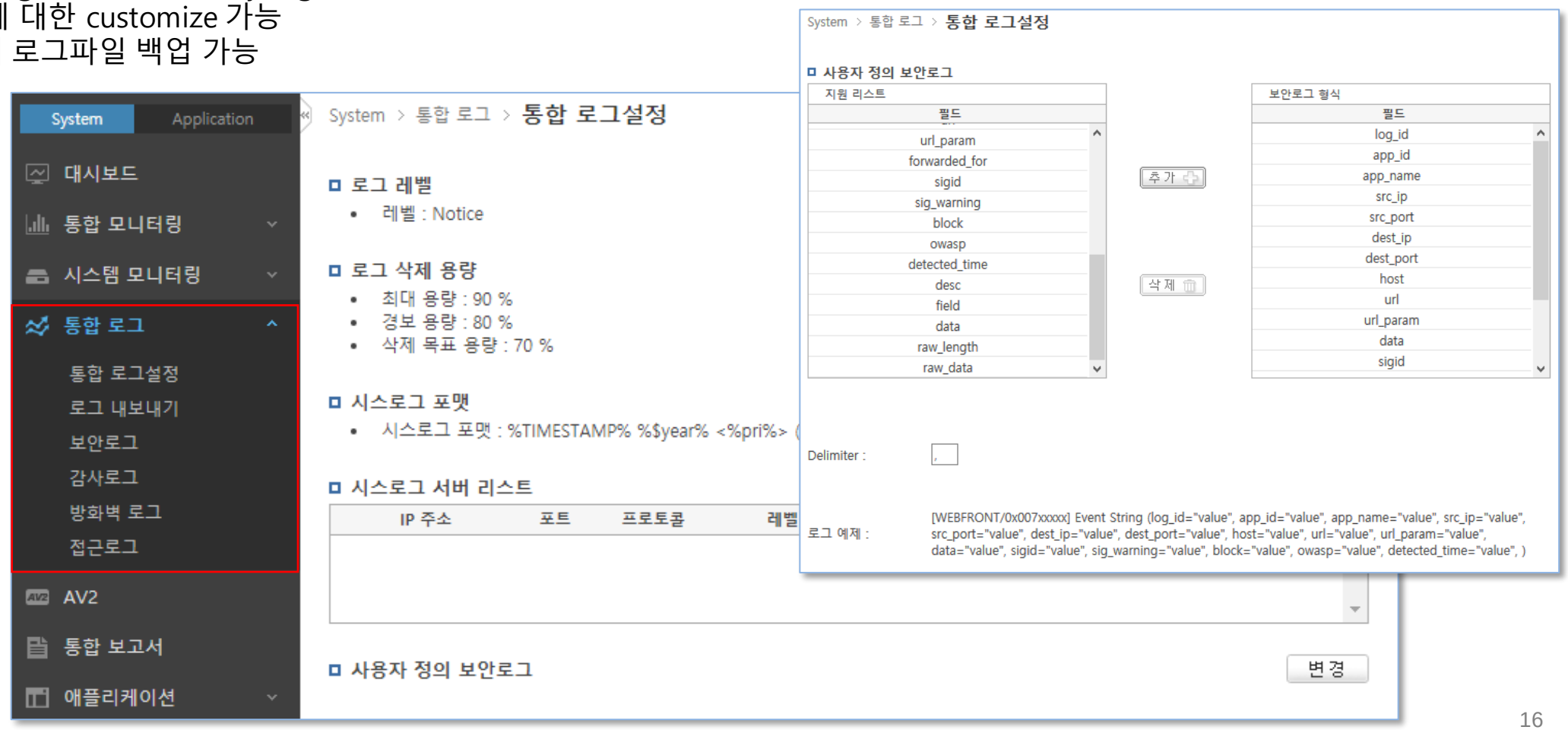


WEBFRONT-KS 메뉴

WEBFRONT-KS 메뉴

통합 로그설정 (System > 통합로그 > 통합 로그설정)

외부 syslog 서버로 다수의 syslog 전송 설정 가능
Syslog 에 대한 customize 가능
외부로의 로그파일 백업 가능

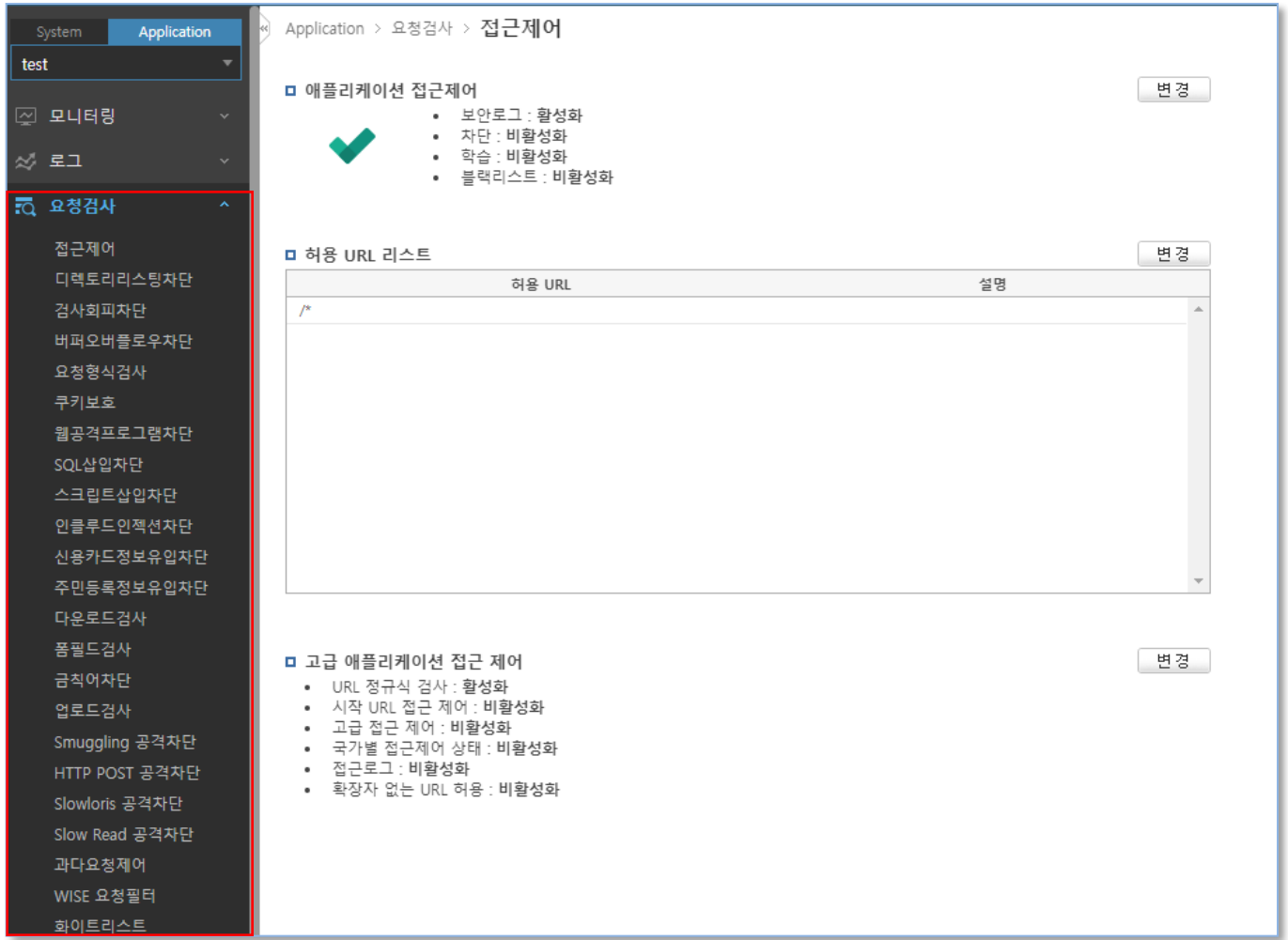


PIOLINK

WEBFRONT-KS 메뉴

WEBFRONT-KS 메뉴

애플리케이션 요청검사(Application > 요청검사)
웹 요청 관련 보안기능 설정



PIOLINK

WEBFRONT-KS 메뉴

WEBFRONT-KS 메뉴

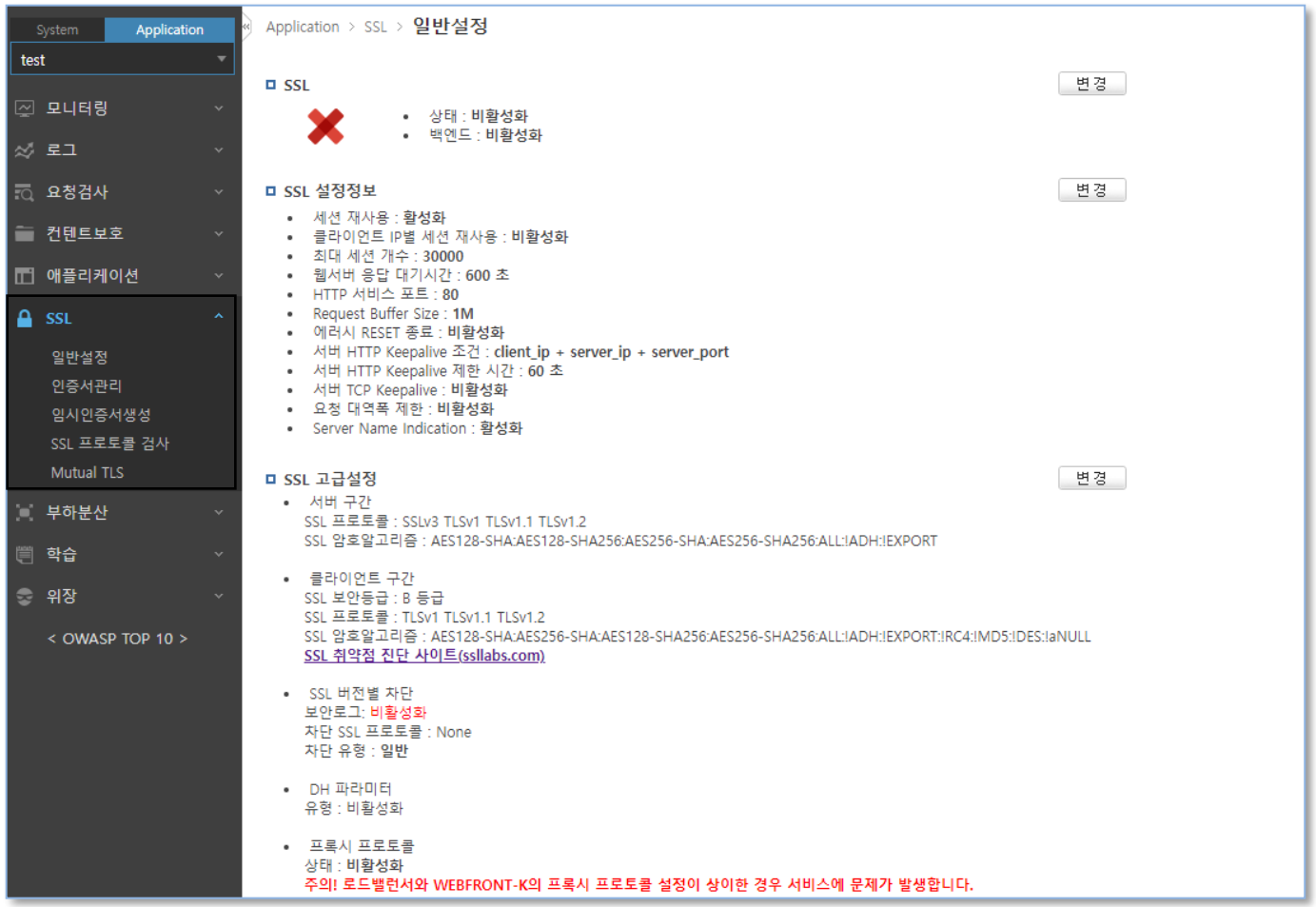
애플리케이션 일반 설정(Application > 애플리케이션 > 일반 설정)
웹 서비스 관련 설정

PIOLINK

WEBFRONT-KS 메뉴

WEBFRONT-KS 메뉴

SSL 관련 설정(Application > SSL > 일반설정, 인증서 관리
SSL 처리 관련 설정



PIOLINK

3. 기본 사용 방법

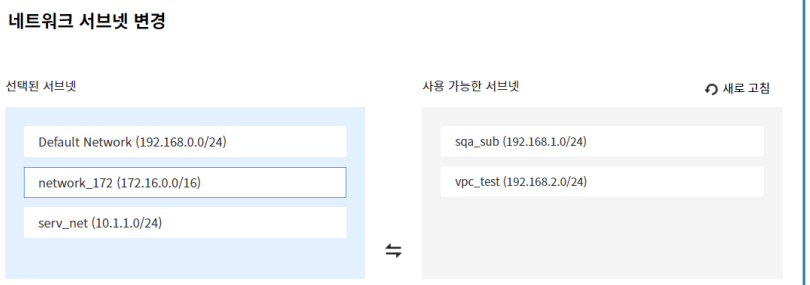
PIOLINK

인터페이스 추가 설정

Mgmt 이외의 추가 인터페이스 설정

- NHN클라우드 콘솔에서 여러 개의 서브넷에 인터페이스 추가 및 정보 확인이 가능하나, mgmt 인터페이스에 대해서만 dhcp로 자동 설정됨
- Mgmt 외 추가 인터페이스에 대해서는 WAF 웹UI에서 추가 설정이 필요함

인터페이스 할당 (클라우드 콘솔)



Vlan 설정

IP주소 추가

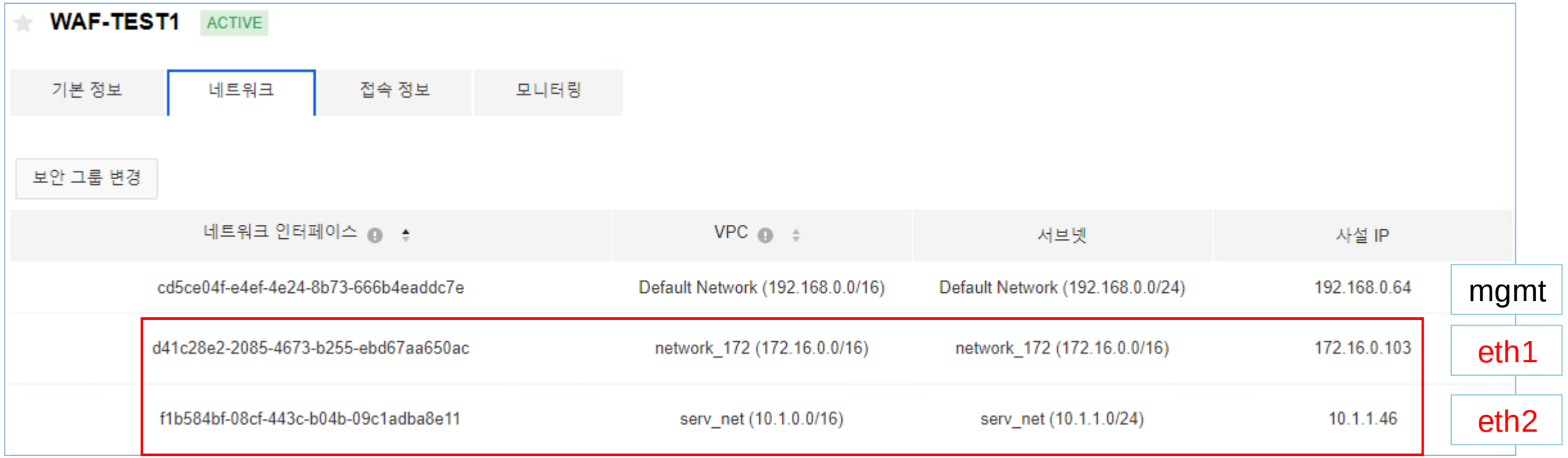
PIOLINK

인터페이스 추가 설정

Mgmt 이외의 추가 인터페이스 설정

1. 인터페이스 할당

- 클라우드 콘솔에서 서브넷 할당 시 자동으로 인터페이스가 추가 및 IP가 부여됨

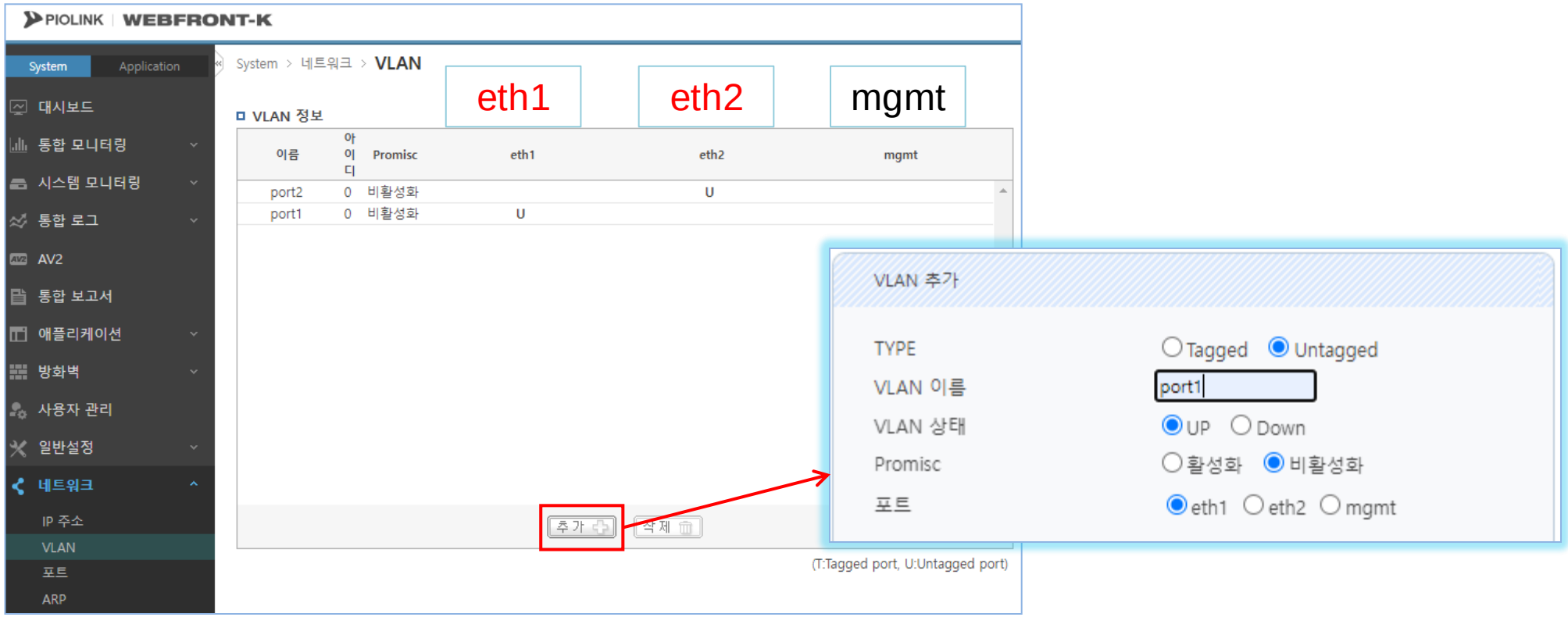


인터페이스 추가 설정

Mgmt 이외의 추가 인터페이스 설정

2. Vlan 설정

- 설정 경로: System – 네트워크 – vlan 설정
- 추가 인터페이스 별로 vlan을 1개씩 생성해야 함 (untagged, promisc 비활성화로 설정)

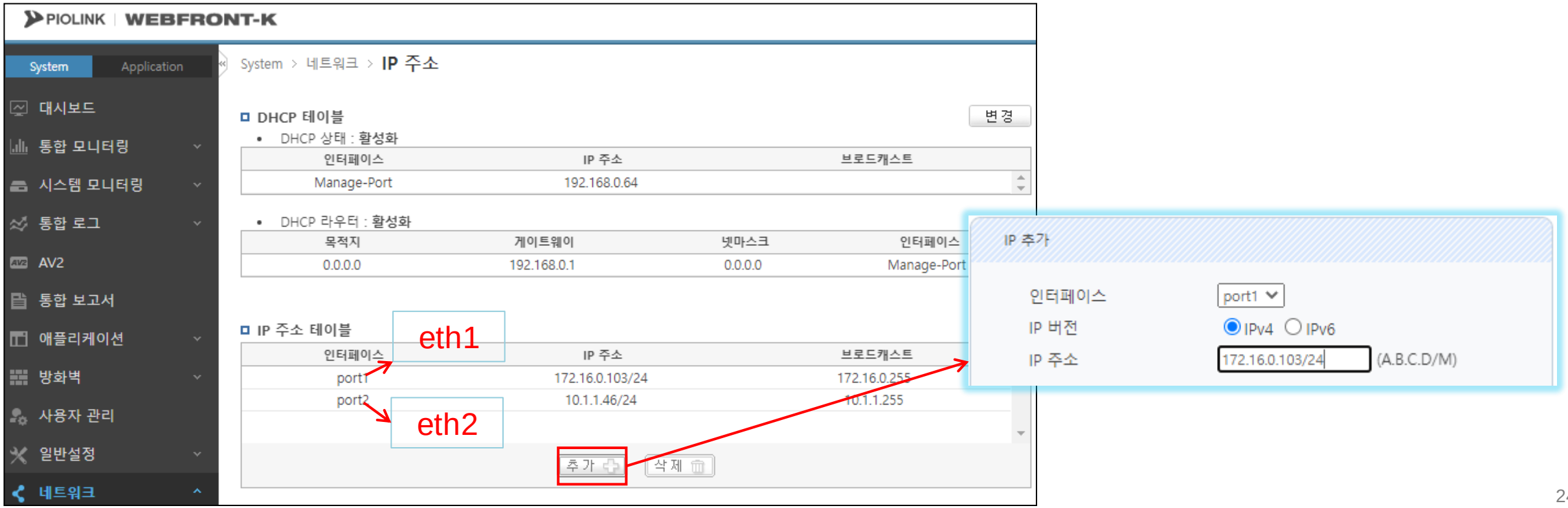


인터페이스 추가 설정

Mgmt 이외의 추가 인터페이스 설정

3. IP주소 추가

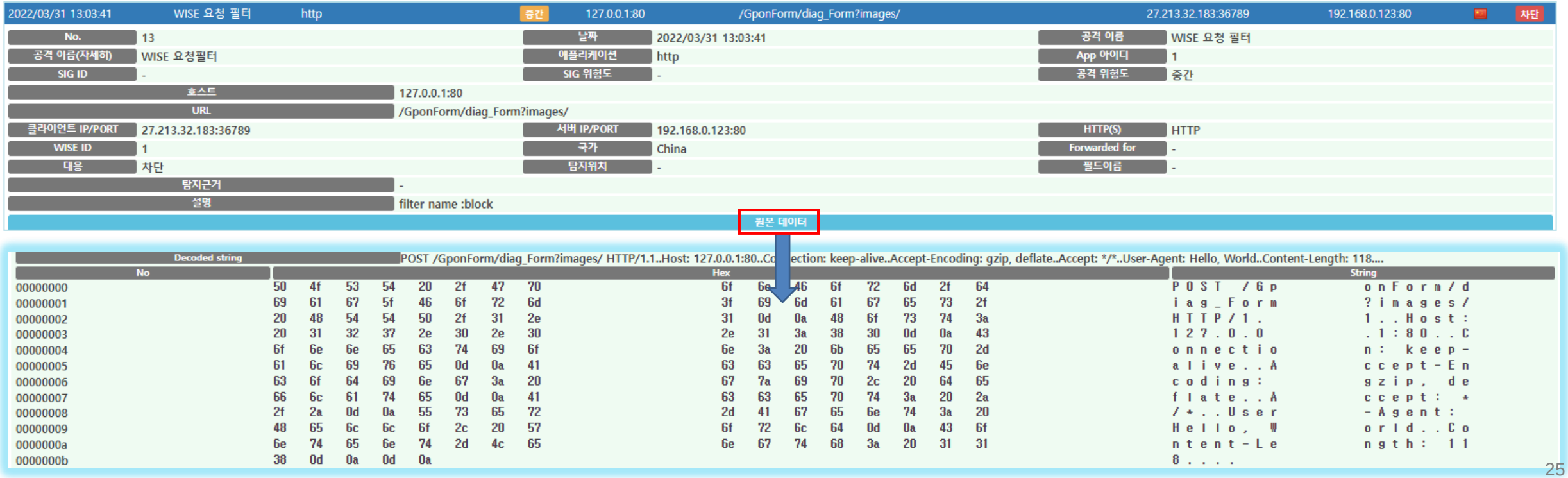
- 설정 경로: System – 네트워크 – IP주소 설정
- WAF 내 각 인터페이스에 클라우드 콘솔에서 확인되는 IP를 입력 (서브넷 마스크는 /24로 입력 필요)



로그 확인

로그 상세내용 확인

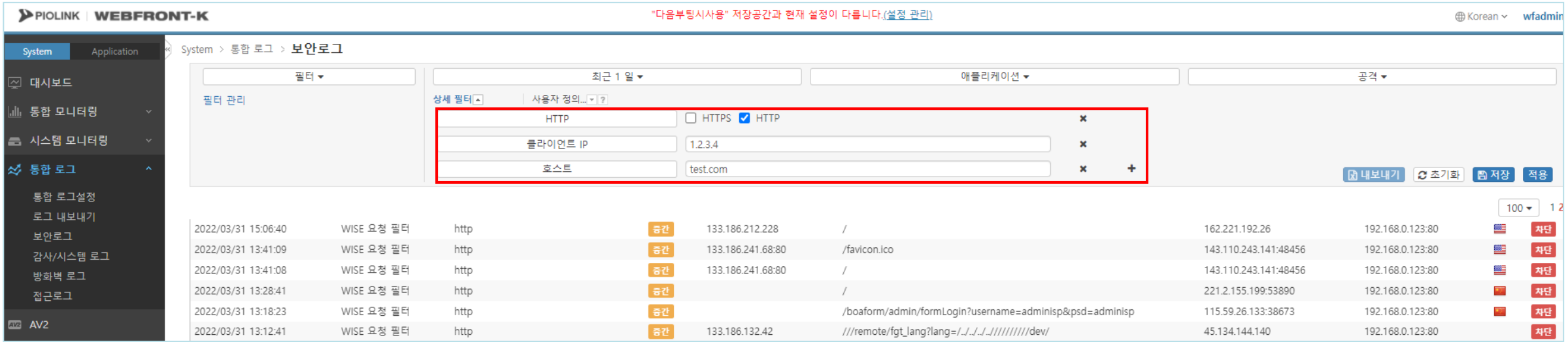
- System탭 – 통합로그 – 보안로그 에서 모든 서비스에 대한 보안로그 확인 가능
- 시그니처 매칭으로 인해 발생한 이벤트의 경우, 매칭된 스트링이 탐지근거에 표기되며, 패킷 내용 중 매칭된 스트링은 빨간색으로 하이라이트 됨
- 원본 데이터 클릭 시 패킷 내용 확인 가능



로그 확인

로그 상세내용 확인

- 상세필터 내 조건 설정을 통해 특정 조건에 부합하는 로그만 조회가 가능

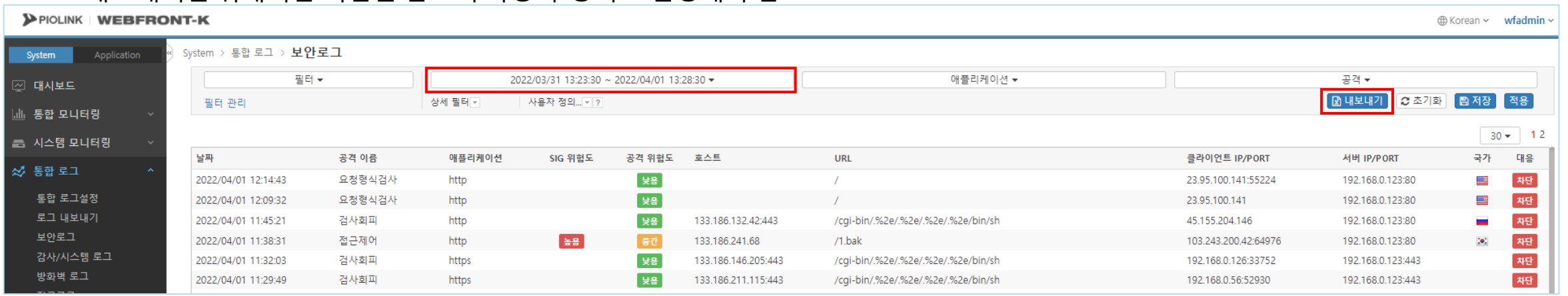


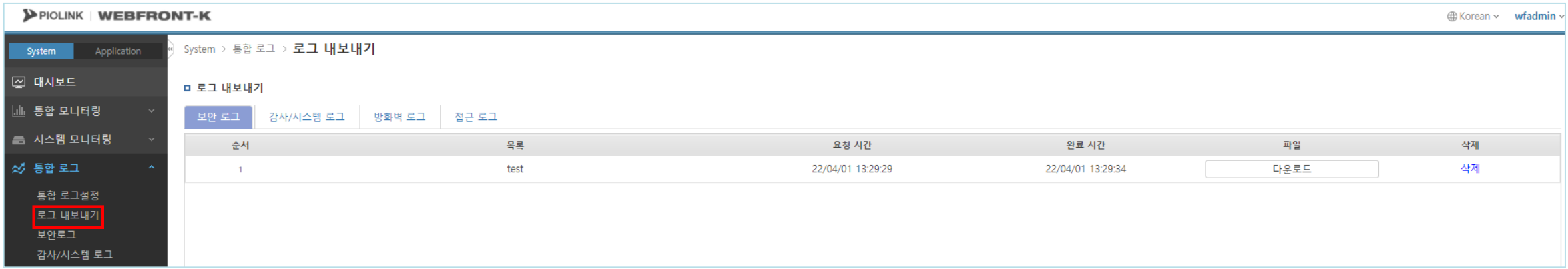
- 상세필터의 조건은 아래와 같음

로그 확인

로그 내보내기

- 로그 내보내기 기능을 통해 엑셀 파일로 추출 가능 (내보내기 후 System탭 – 통합로그 – 로그 내보내기 에서 다운로드 가능)
- 로그 내보내기를 위해서는 기간을 반드시 사용자 정의로 설정해야 함

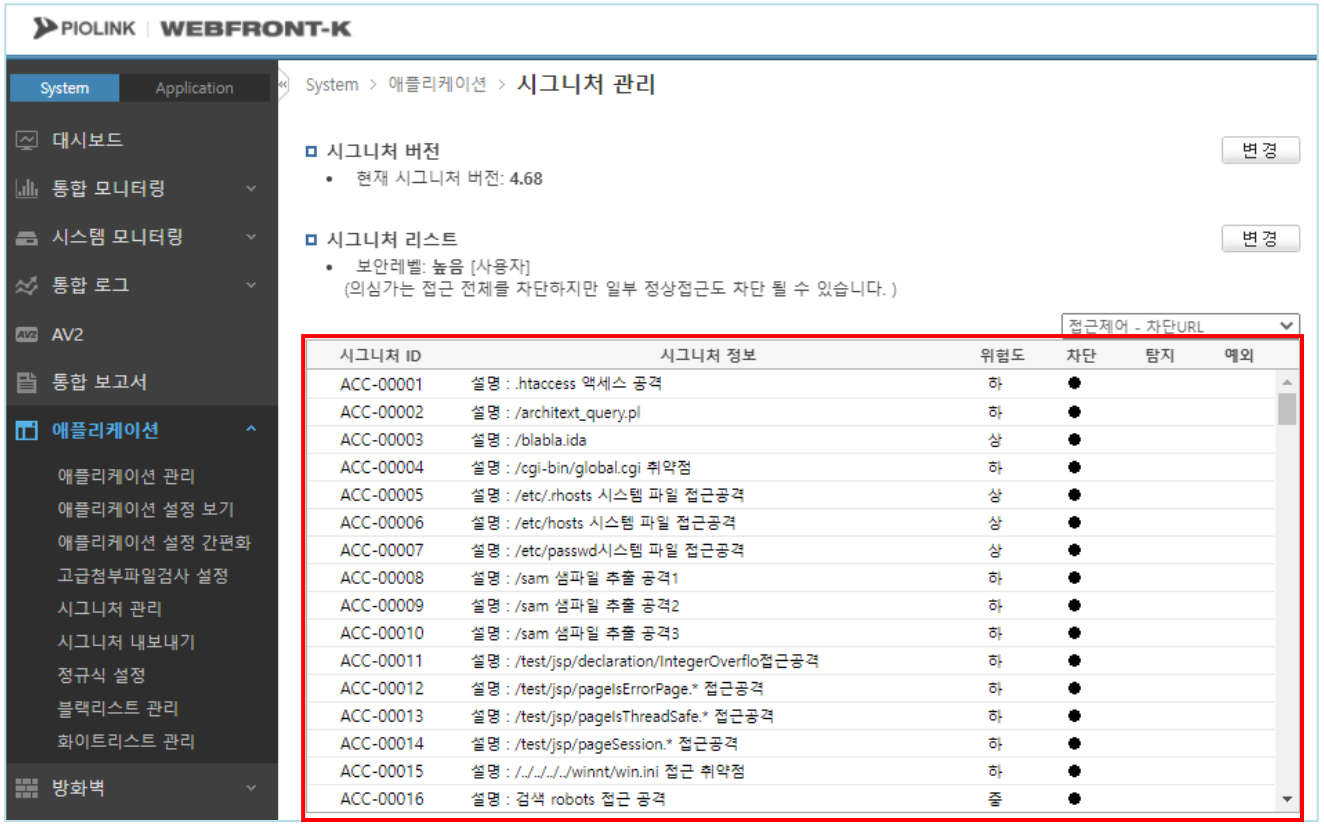




차단 정책

시그니처 확인

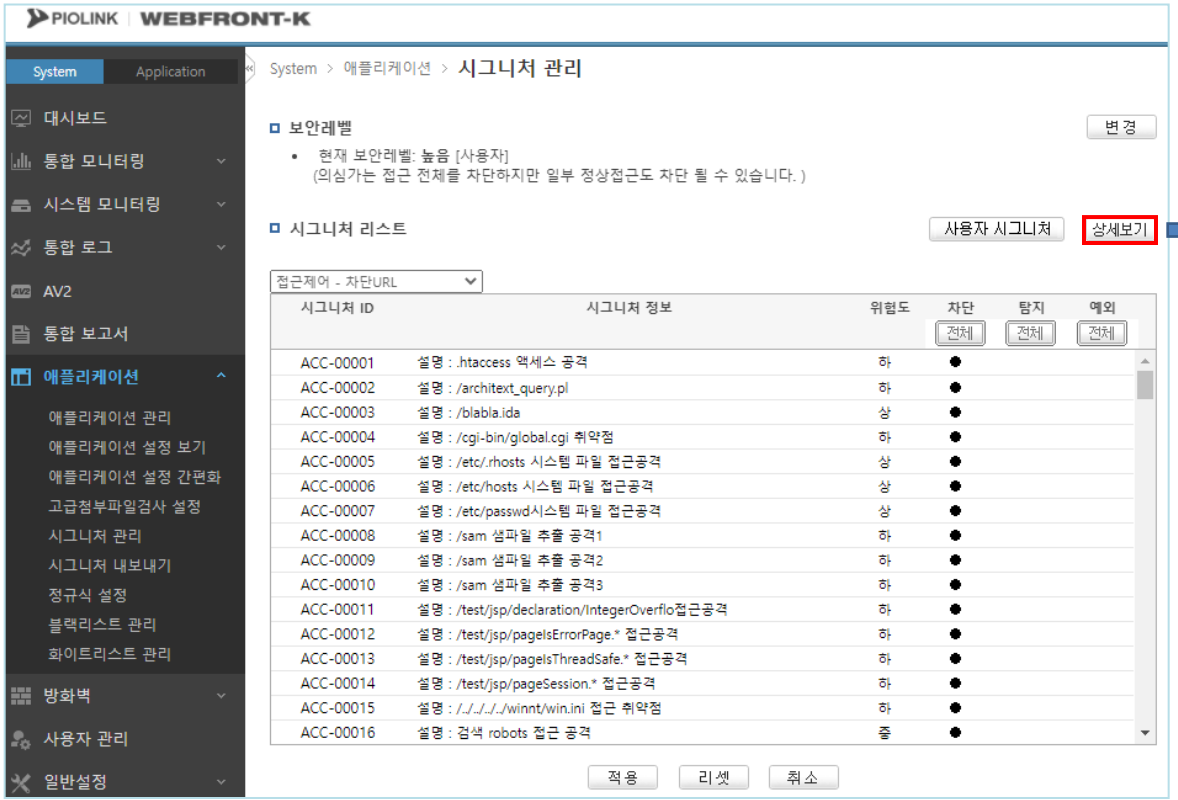
- System탭 – 애플리케이션 – 시그니처 관리 에서 시그니처 리스트와 정책 확인 가능
- 시그니처 정책은 **차단**(매칭 시 차단 및 로그 발생), **탐지**(매칭 시 통과 및 로그 발생), **예외**(매칭 시 통과 및 로그 미 발생) 중 하나로 설정

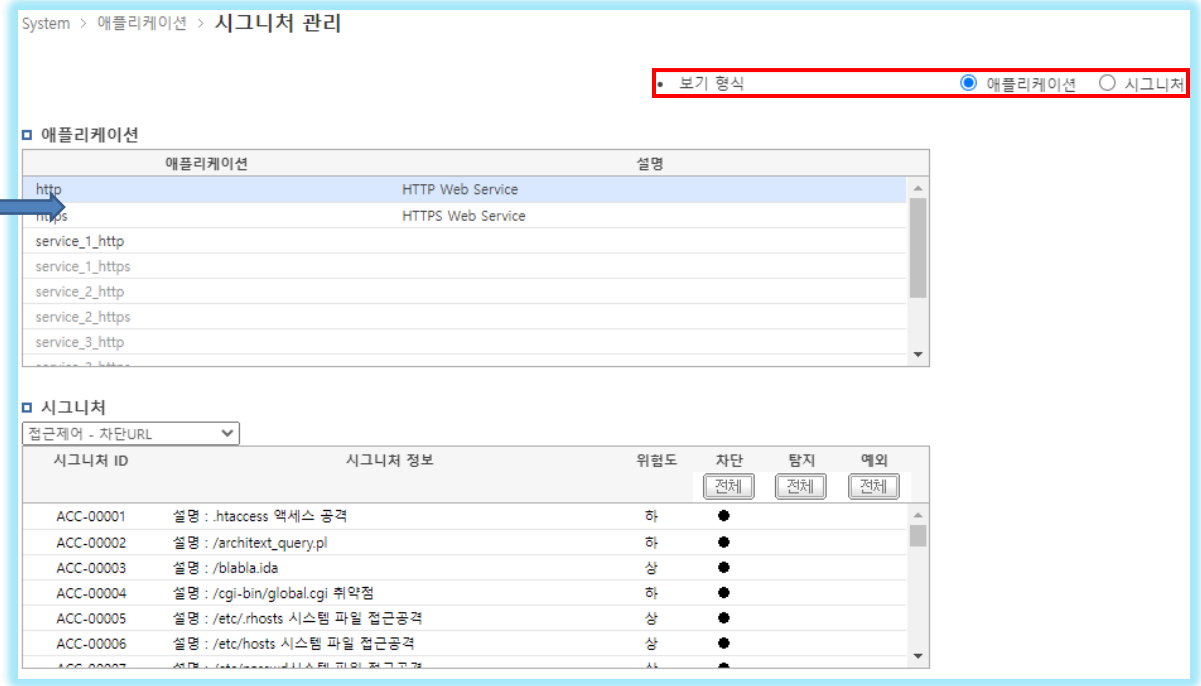


차단 정책

시그니처 변경

- 시그니처 리스트의 변경 버튼 클릭 후 시그니처 별 정책 설정이 가능
- 시그니처 별, 애플리케이션 별로 시그니처 확인 및 정책 설정이 가능 (특정 서비스에서만 시그니처 정책을 별도로 설정할 수 있음)

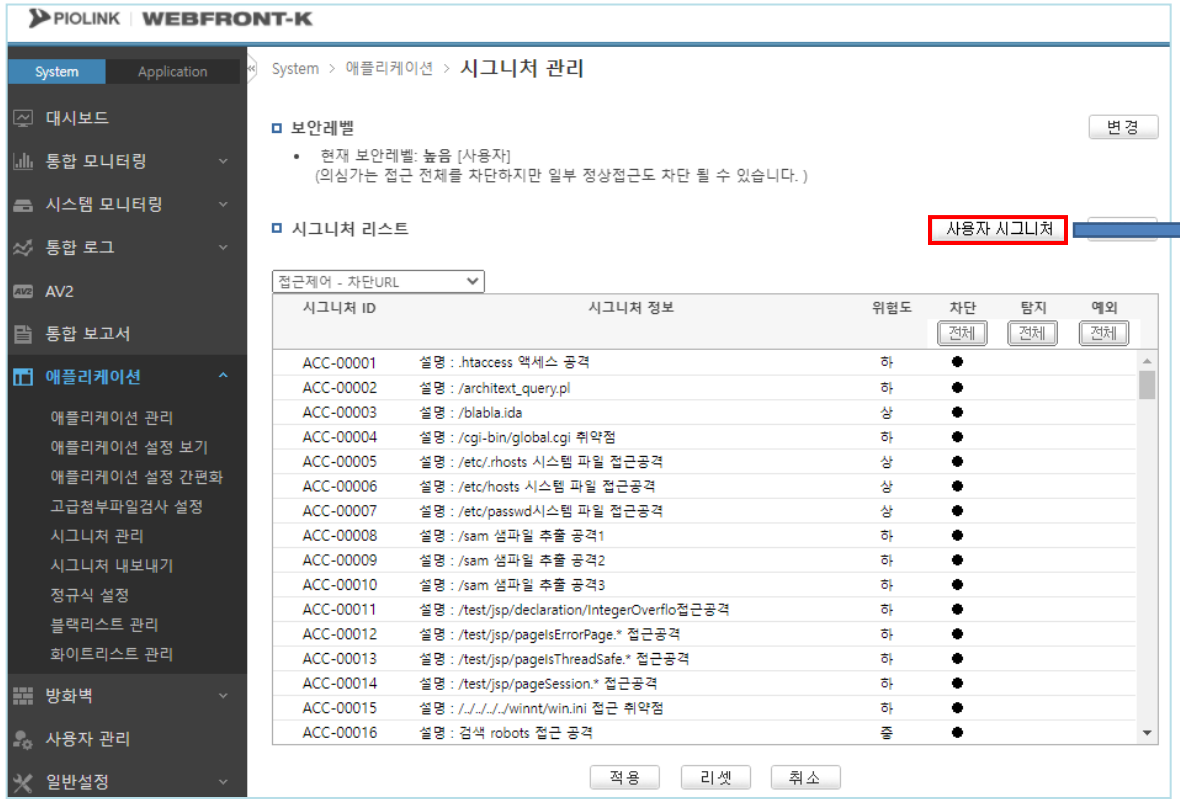


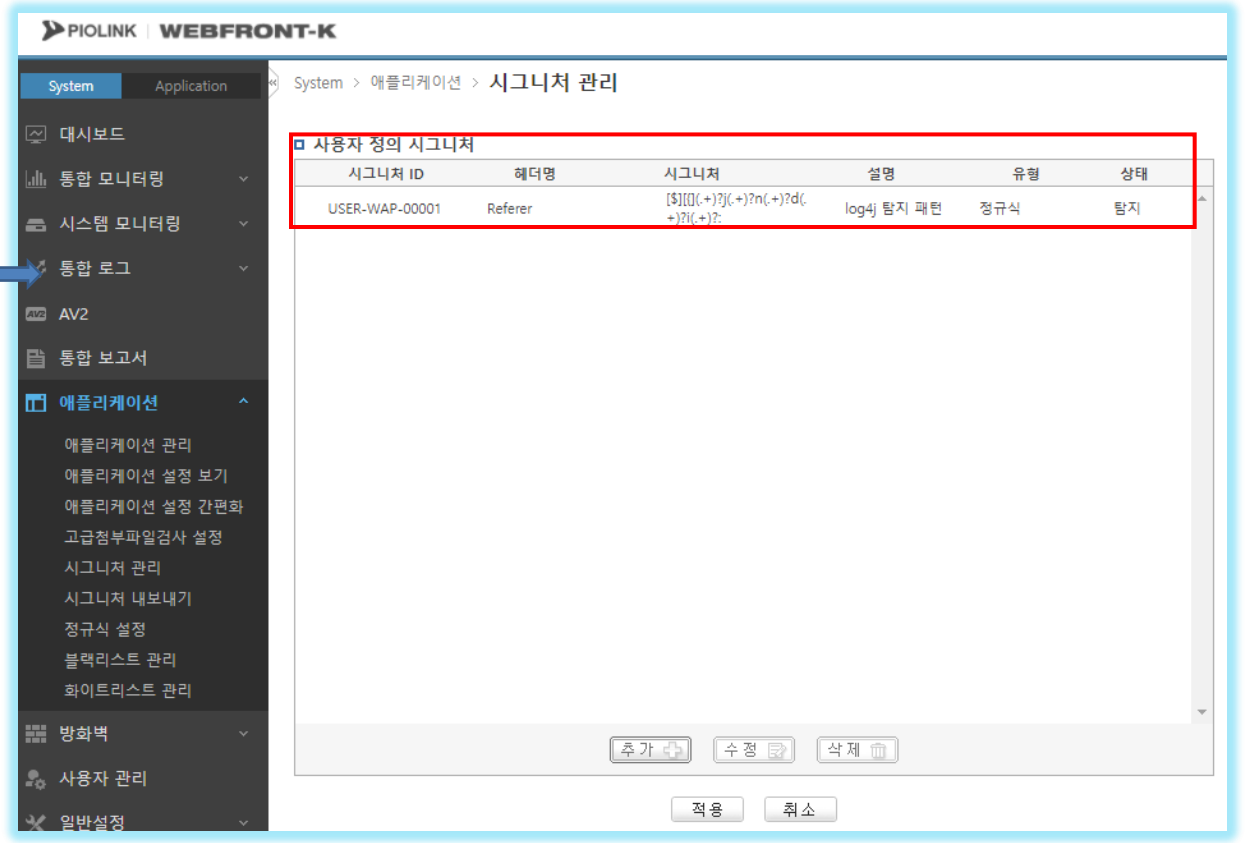


차단 정책

사용자 시그니처 추가

- 시그니처 리스트의 변경 버튼 클릭 후 시그니처 별 정책 설정이 가능
- 사용자 시그니처 추가 가능 (공격 종류에 따라 문자열, 정규식, PCRE 패턴으로 추가 가능)





예외 처리

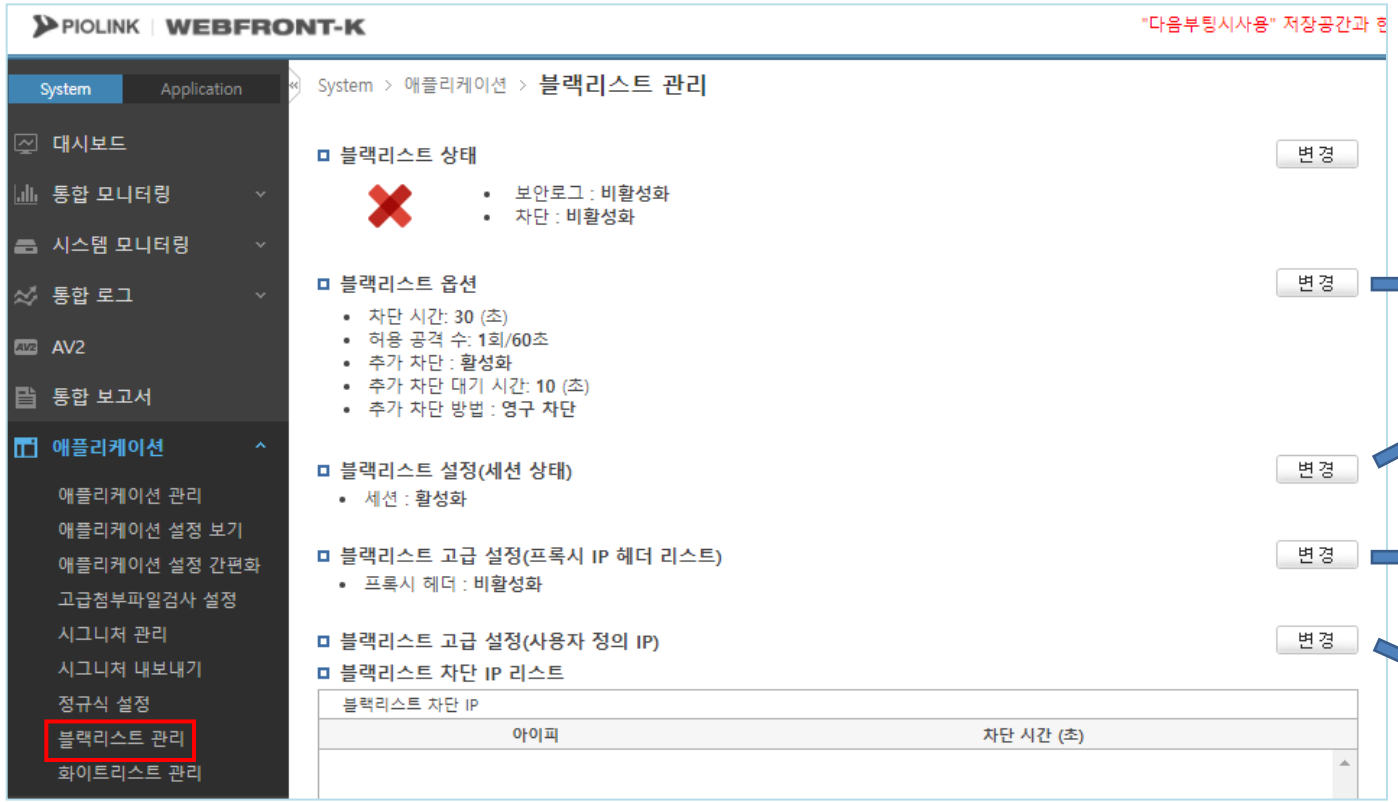
화이트리스트

- System탭 – 애플리케이션 – 화이트리스트 관리 에서 IP/Port 기반의 화이트리스트 기능 제공 (IP 대역으로 설정 가능)
  - WAF 전체에 대해 통합적으로 적용됨 (개별 도메인 등에 대해서 설정 안 됨)
- 네트워크 구성에 따라 적용하기 힘들 수 있음 (상단에 LB 위치할 경우)

예외 처리

블랙리스트

- System탭 – 애플리케이션 – 블랙리스트 관리 에서 IP 기반의 블랙리스트 기능 제공 (IP 대역으로 설정 가능)
- WAF 전체에 대해 통합적으로 적용됨 (개별 도메인 등에 대해서 설정 안 됨)



조건에 따른 자동 차단 설정

클라이언트IP 기반 블랙리스트 설정

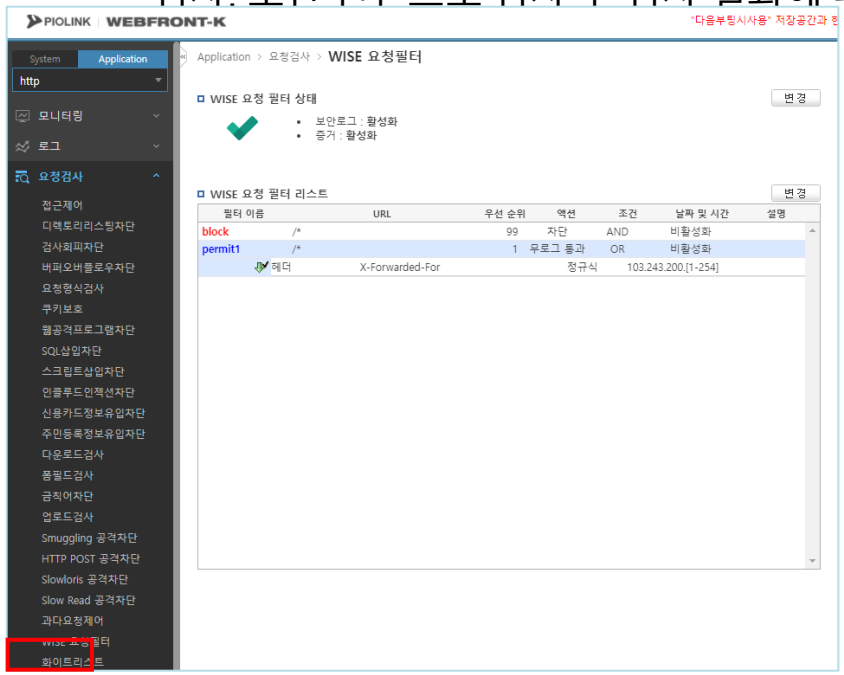
프록시 헤더 IP 기반 블랙리스트 설정(XFF헤더 등)

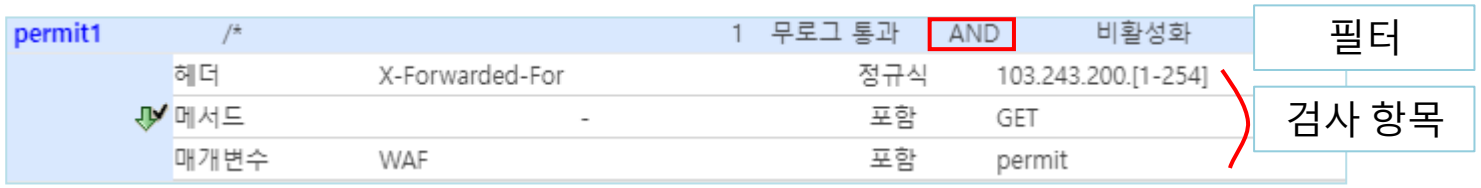
수동으로 특정 IP를 추가

예외 처리

WISE 요청필터

- Application탭 – {특정 애플리케이션} – 요청검사 – WISE 요청필터에서 다양한 조건의 검사 항목 따른 필터 설정 가능
- 각 필터 별로 통과, 무로그 통과, 차단, 무로그 차단, 검사, 무로그 검사 등의 액션 설정 가능 (AND / OR 조건 설정)
    - 통과: 무조건 통과
    - 차단: 무조건 차단
    - 검사: 보안 엔진으로 검사 후 검사 결과에 따라 통과 또는 차단

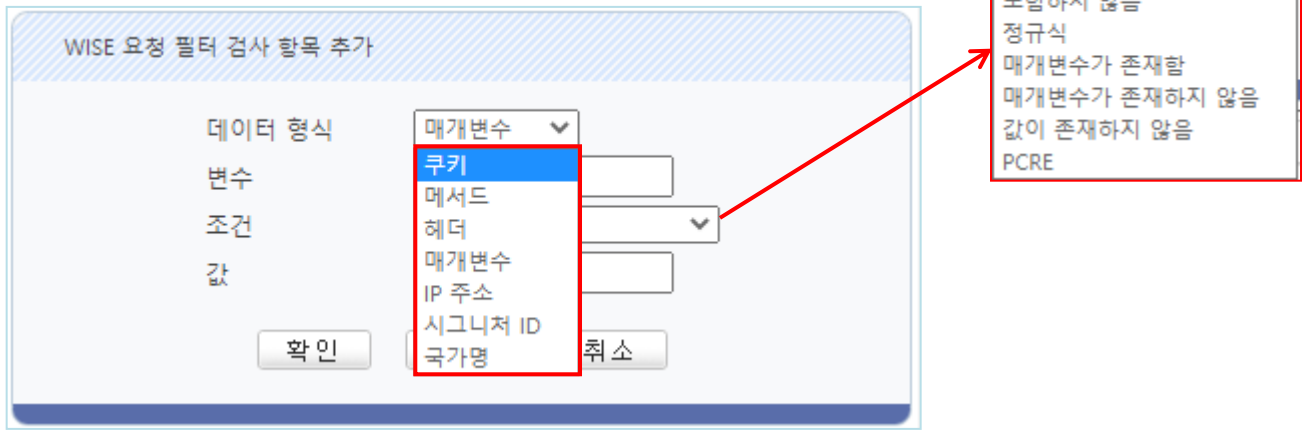




예외 처리

WISE 요청필터

- 필터에 등록된 검사 항목이 없을 시 조건 없이 동작함
- 검사 항목에는 아래의 7가지 조건을 통한 설정이 가능

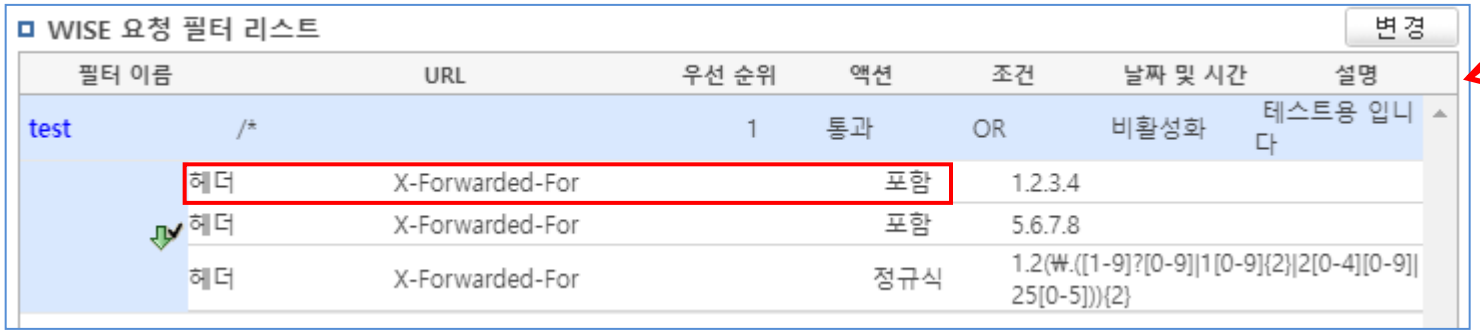


예외 처리

WISE 요청필터

- IP를 기준으로 검사 항목을 추가할 경우, 네트워크 구성에 따라 다른 방법으로 추가해야 함

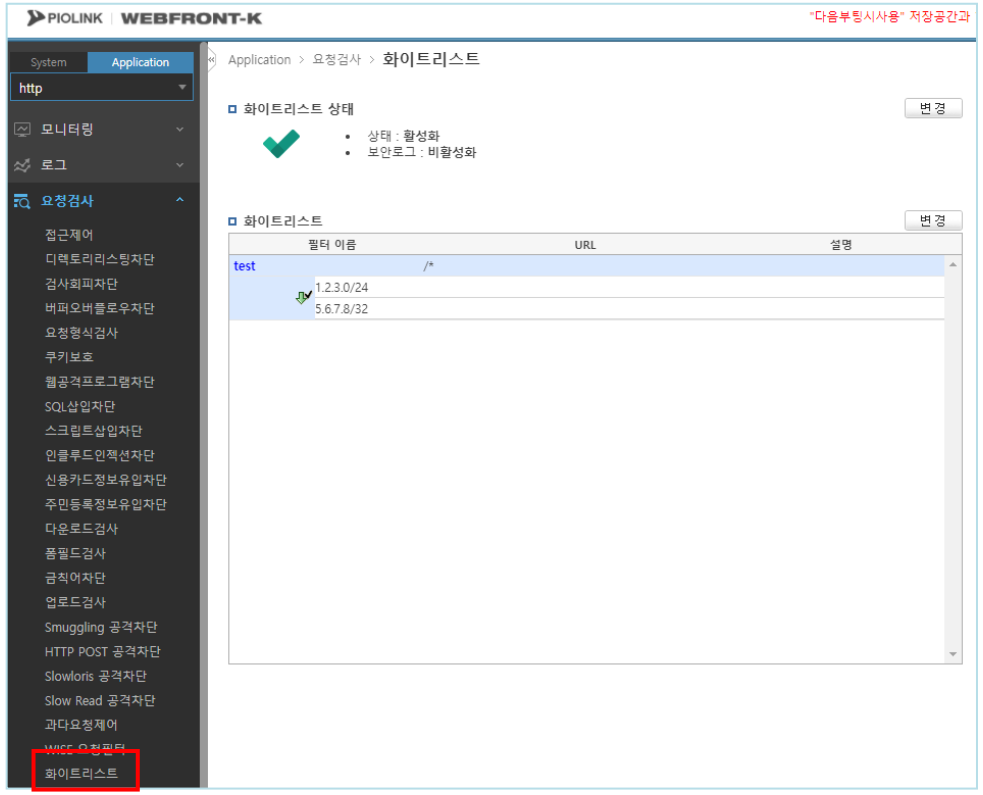
1. WAF가 최상단일 경우 >> IP주소로 대응 (IP 대역으로 추가 가능)
2. [HTTP 통신 or HTTPS 통신] + WAF 상단에 LB가 존재 + (LB에서 인증서 처리) >> 헤더 (X-Forwarded-For)로 대응
3. HTTPS 통신 + WAF 상단에 LB가 존재 + LB에서 인증서 처리가 되지 않을 경우 >> WISE 요청필터로 IP기반 대응 불가능



예외 처리

화이트리스트(요청검사)

- Application탭 – {특정 애플리케이션} – 요청검사 – 화이트리스트 에서 특정 URL에 대해 특정 IP(대역)로부터의 접근을 허용할 수 있음
- 해당 애플리케이션에 설정되어 있는 도메인에 대해서만 접근 허용
- 네트워크 구성에 따라 적용하기 힘들 수 있음 (상단에 LB 위치할 경우)

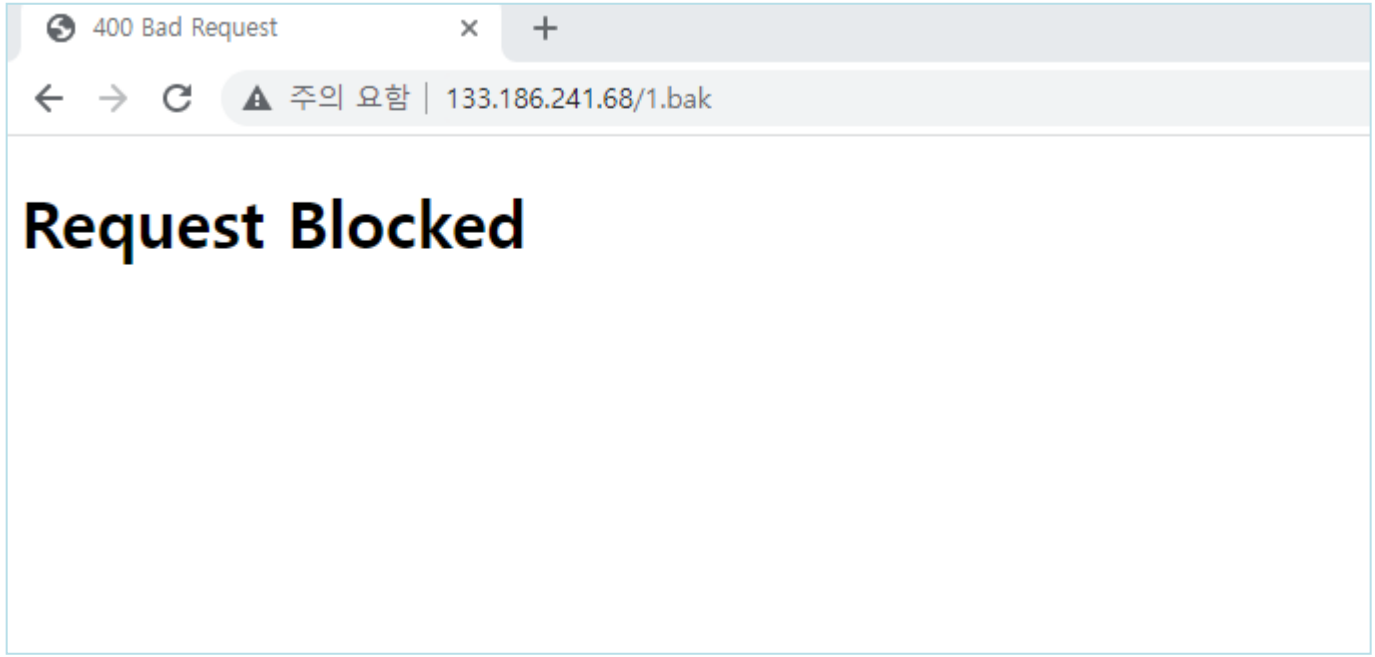


PIOLINK

장애 조치

차단으로 인한 이슈

- System탭 – 통합로그 – 보안로그 에서 차단 내역 확인 후 정책 변경 / 예외 처리를 통해 대응
- 실제 WAF가 차단하는 것인지 식별이 우선적으로 필요
- WAF 차단으로 인한 경우, 기본적으로는 아래의 페이지가 출력되면서 http 400 응답 코드가 리턴됨 (설정에 따라 별도 메시지 리턴 가능)

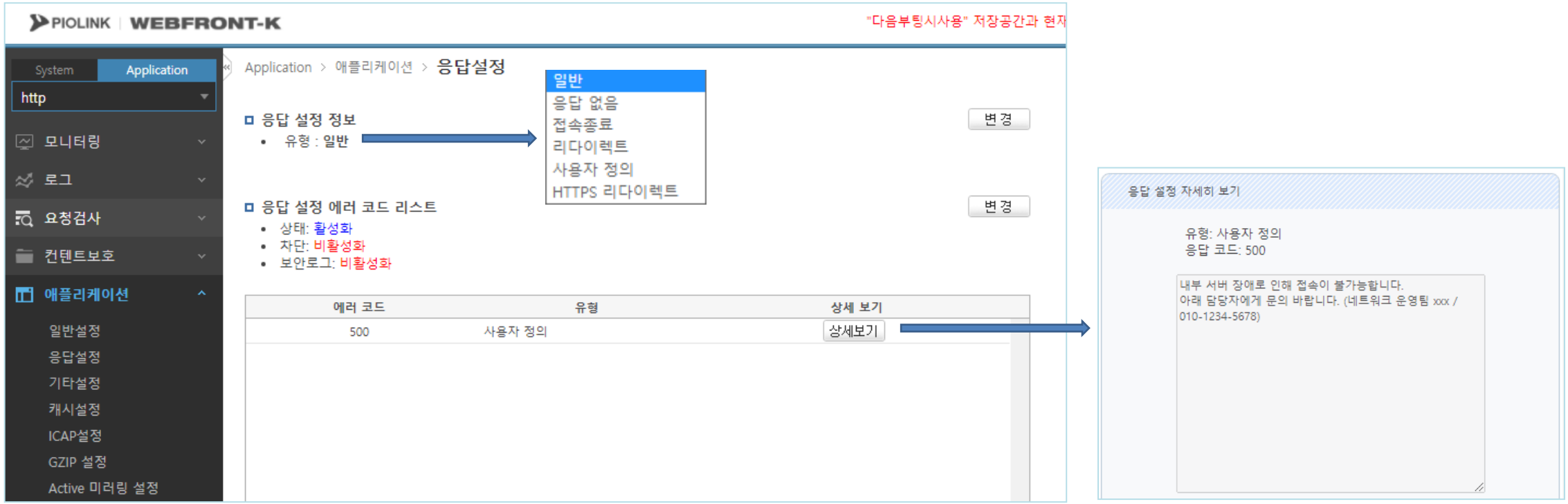


장애 조치

차단으로 인한 이슈

- WAF 차단 시 출력되는 메시지나 동작은 별도 설정 가능 (Application탭 – {특정 애플리케이션} – 애플리케이션 – 응답설정)

- 접속 종료: reset 전송
- 리다이렉트: 지정한 URL로 리다이렉트
- 사용자 정의: 작성된 메시지 전송
- https 리다이렉트: 차단된 도메인에 대해 http가 아닌 https로 리다이렉트 (http 응답코드 중 307 Temporary Redirect를 이용함 / 301, 302 리다이렉트 아님)



PIOLINK

장애 조치

통신 불량으로 인한 이슈

- 클라이언트가 받는 응답코드 확인이 필요 (WAF 기준)
- WAF 상단에 다른 네트워크 장비가 있을 경우에는 응답 코드가 달라질 수 있음

1. http 4xx (WAF 차단 메시지 확인 안 될 경우) : 하단 서버에서 확인 및 조치 필요
2. http 500 (Internal server error) : WAF에서 하단 서버로 헬스 체크가 되지 않음 > 헬스 체크 확인
3. http 502 (Bad gateway) : 하단 서버로부터 비정상적인 응답을 받을 경우 or WAF가 요청/응답을 제대로 처리하지 못할 경우
4. http 504 (Gateway Timeout) : 하단 서버에서 특정 시간 안에 응답을 주지 않을 경우 (시간 제한 기본값: 600초)

장애 조치

통신 불량으로 인한 이슈

- WAF 내부 shell에 접속 후 nginx 에러로그의 확인이 필요

** NHN클라우드 내 WAF에는 ID/PW가 아닌 개인키 인증을 통해서만 접속 가능

SSH를 통해 CLI 접속

```
WF-KS# conf
WF-KS(config)# st
piolink's password:                    (해당 계정의 비밀번호 입력 시 linux shell로 변경됨)
root@WF-KS:~# cd /opt/k2/hdd/log/nginx/
root@WF-KS:~/log/nginx# ls             (해당 경로에서 에러로그 확인)
error.log    error.log.2  error.log.4  piolink
error.log.1  error.log.3  error.log.5
```

장애 조치

통신 불량으로 인한 이슈

http 500 (Internal server error) : WAF에서 하단 서버로 헬스 체크가 되지 않음 > 헬스 체크 확인

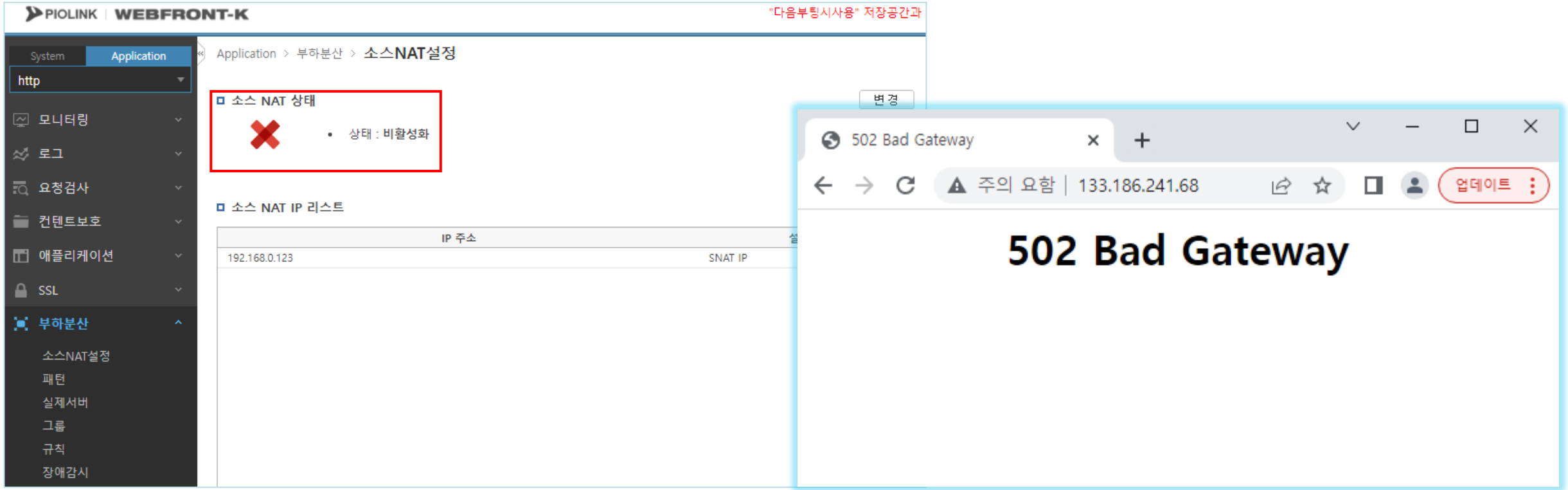
- 경로: Application탭 – {특정 애플리케이션}– 부하분산 – 장애감시
- 조치: 헬스체크 여부 확인 후 통신 복구 조치 (방화벽 차단 / 특정 통신구간 장애 / 서버 다운 등)

장애 조치

통신 불량으로 인한 이슈

http 502 (Bad gateway) : 하단 서버로부터 비정상적인 응답을 받을 경우 or WAF가 요청/응답을 제대로 처리하지 못할 경우

- WAF내 Nginx 에러로그 및 설정, 통신 구간 별 이상여부 체크 등을 통한 복합적인 원인 분석이 필요
- 간혹 WAF 내 소스NAT가 비활성화 되어있을 경우 502 응답 코드를 리턴하므로 확인 필요



장애 조치

통신 불량으로 인한 이슈

http 502 (Bad gateway) : 하단 서버로부터 비정상적인 응답을 받을 경우 or WAF가 요청/응답을 제대로 처리하지 못할 경우

- 분석에 필요한 파일을 자동으로 수집/반출하는 기술지원 도우미 파일 제공 시 분석에 용이함 (Application탭 – 일반설정 – 기술지원 도우미)

장애 조치

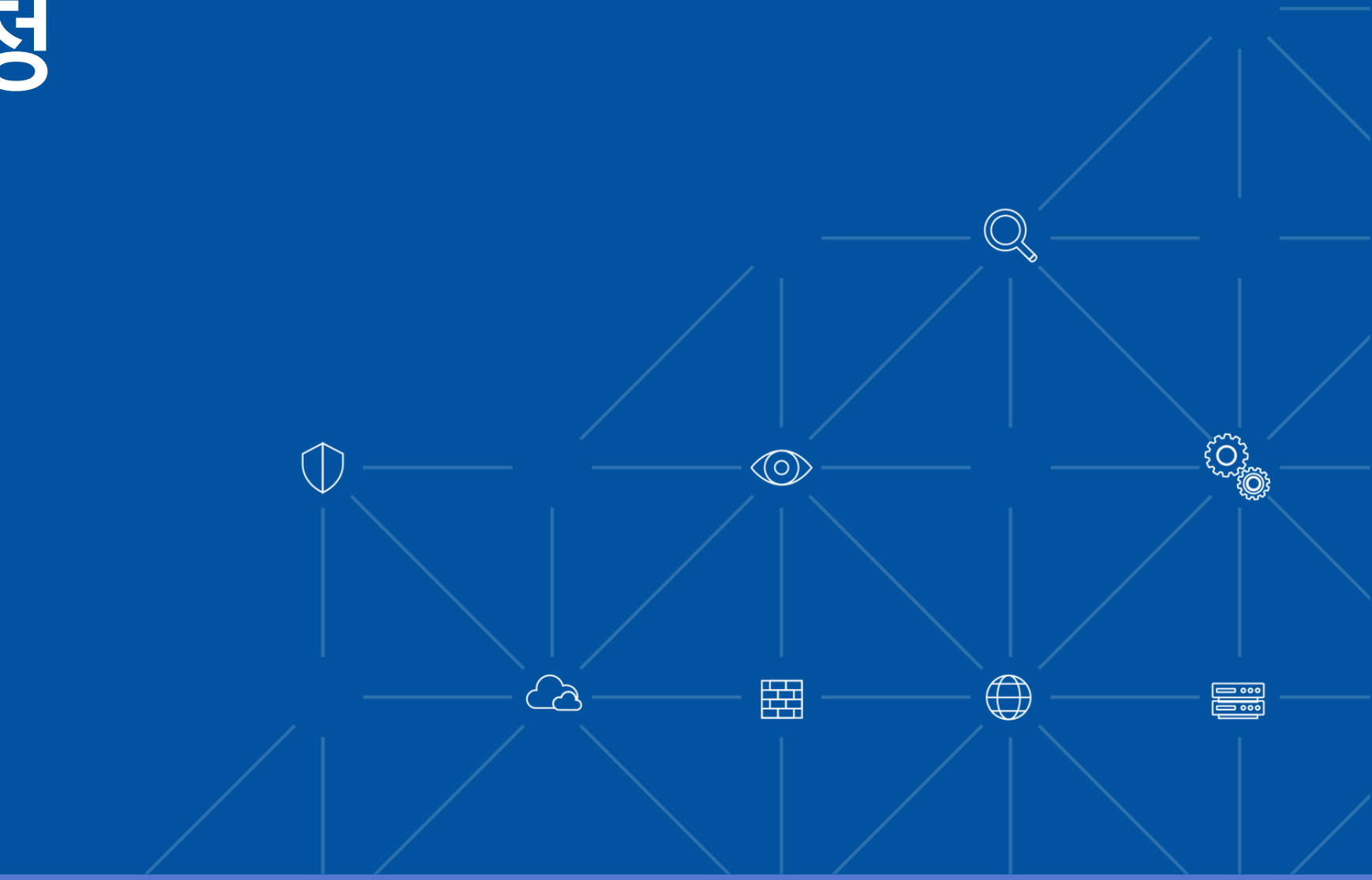
통신 불량으로 인한 이슈

http 504 (Gateway Timeout) : 하단 서버에서 특정 시간 안에 응답을 주지 않을 경우 (시간 제한 기본값: 600초)

- 경로: Application탭 – {특정 애플리케이션} – SSL – 일반설정 (SSL 설정이지만 http 통신에도 전역적으로 적용됨)
- 조치: SSL 설정정보 내 웹서버 응답 대기시간을 더 큰 값으로 변경

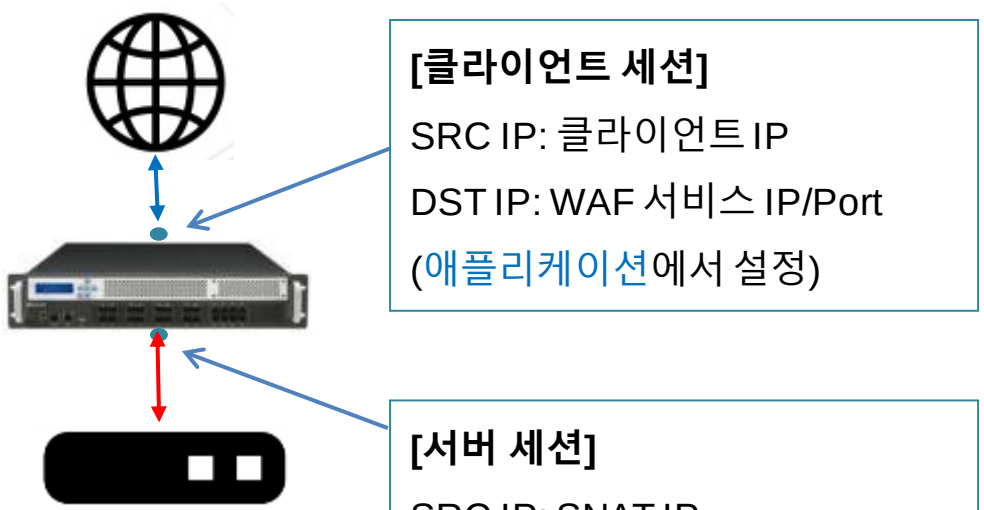
PIOLINK

4. 기본 설정



어플리케이션 설정

- **WEBFRONT-KS 기본 구성**
  - 클라이언트, 내부 서버와 각각 세션을 맺어 프록시로서 동작함
  - 클라이언트, 서버 각 세션은 독립적으로 동작하는 서로 다른 세션임



[클라이언트 세션]

SRC IP: 클라이언트 IP

DST IP: WAF 서비스 IP/Port

(애플리케이션에서 설정)

[서버 세션]

SRC IP: SNAT IP

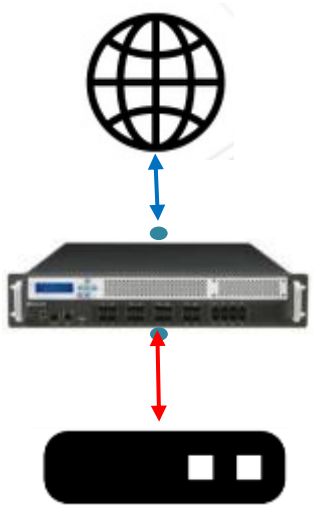
(부하분산 - 소스NAT 설정)

DST IP: 하단 웹 서버 IP/Port

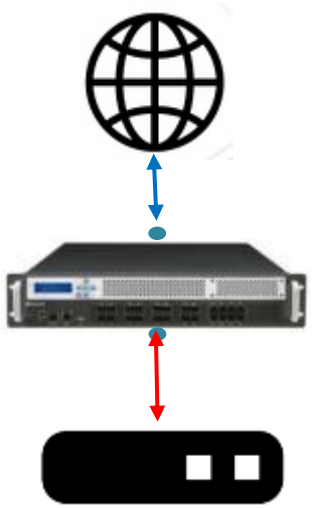
(부하분산 – 실제서버 에서 설정)

어플리케이션 설정

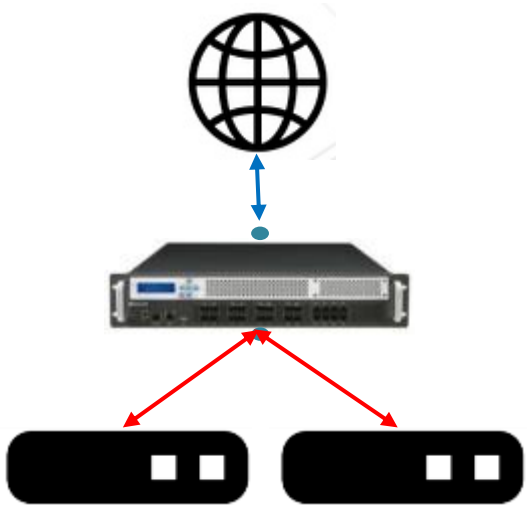
- **WEBFRONT-KS 기본 구성**
  - 웹방화벽 구축 시, 크게 3가지 케이스로 구분 가능



도메인: 1개
WEB: 1개



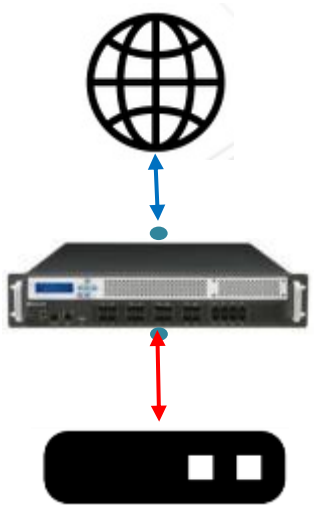
도메인: 2개 이상
WEB: 1개



도메인: 1개
WEB: 2개 이상

어플리케이션 설정

- **WEBFRONT-KS 기본 구성**
  - 아래와 같은 환경으로 구축한다고 가정



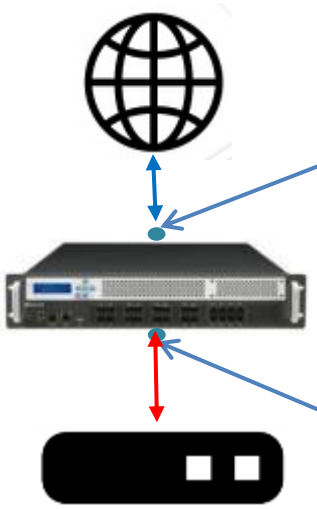
도메인: 1개 (test.com)

WEB: 1개 (192.168.0.5)

프로토콜: http

어플리케이션 설정

- **WEBFRONT-KS 기본 구성**
  - 클라이언트 세션 관련 설정(애플리케이션)



[클라이언트 세션]

SRC IP: 클라이언트 IP

DST IP: WAF 서비스 IP/Port

(애플리케이션에서 설정)

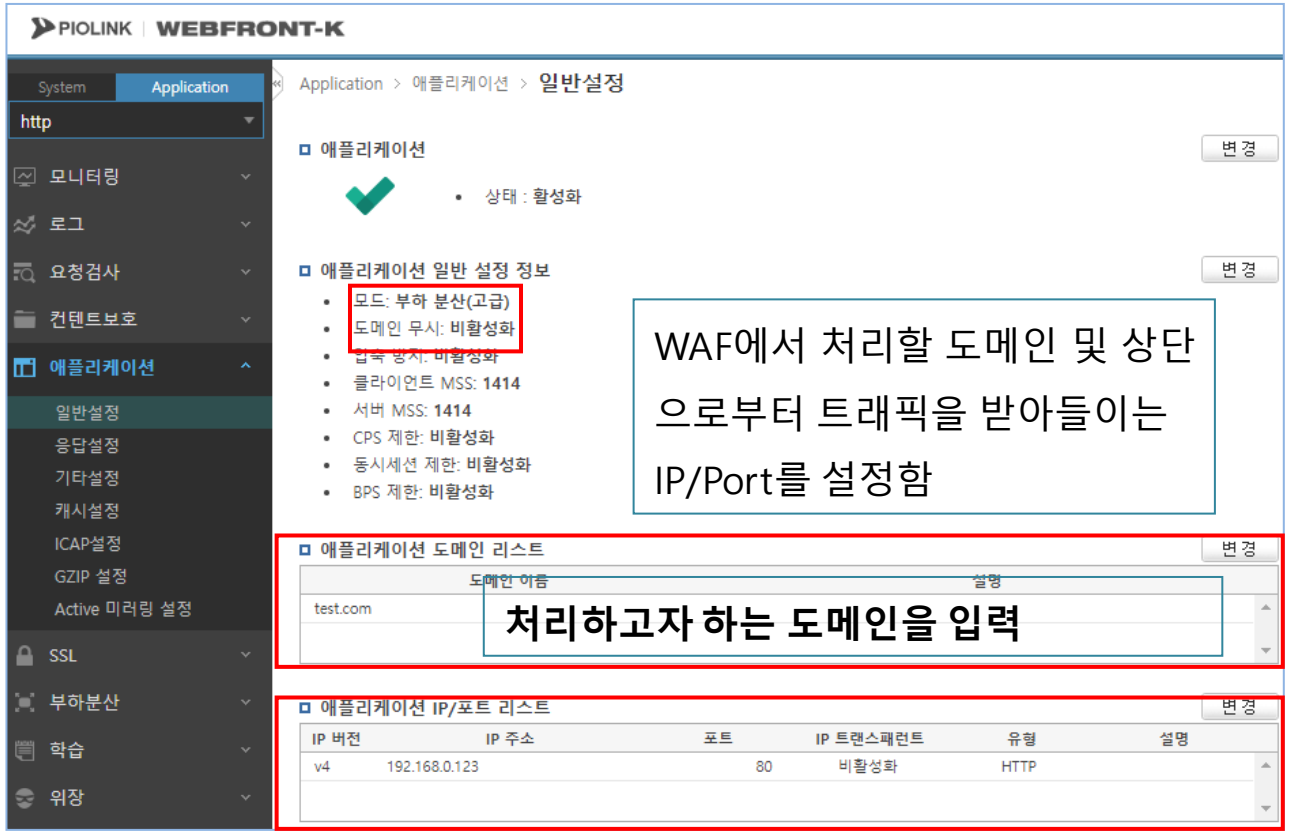
[서버 세션]

SRC IP: SNAT IP

(부하분산 - 소스NAT 설정)

DST IP: 하단 웹 서버 IP/Port

(부하분산 – 실제서버 에서 설정)



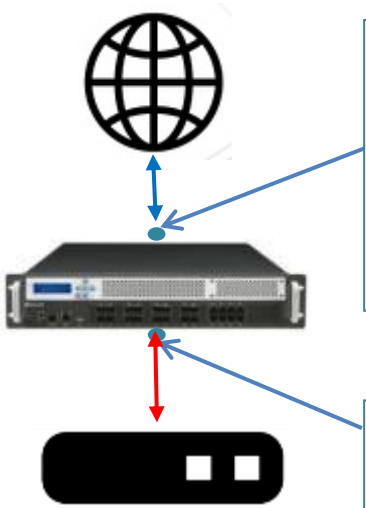
WAF에서 처리할 도메인 및 상단으로부터 트래픽을 받아들이는 IP/Port를 설정함

처리하고자 하는 도메인을 입력

서비스용 IP/Port 입력 (웹방화벽의 사설 IP)

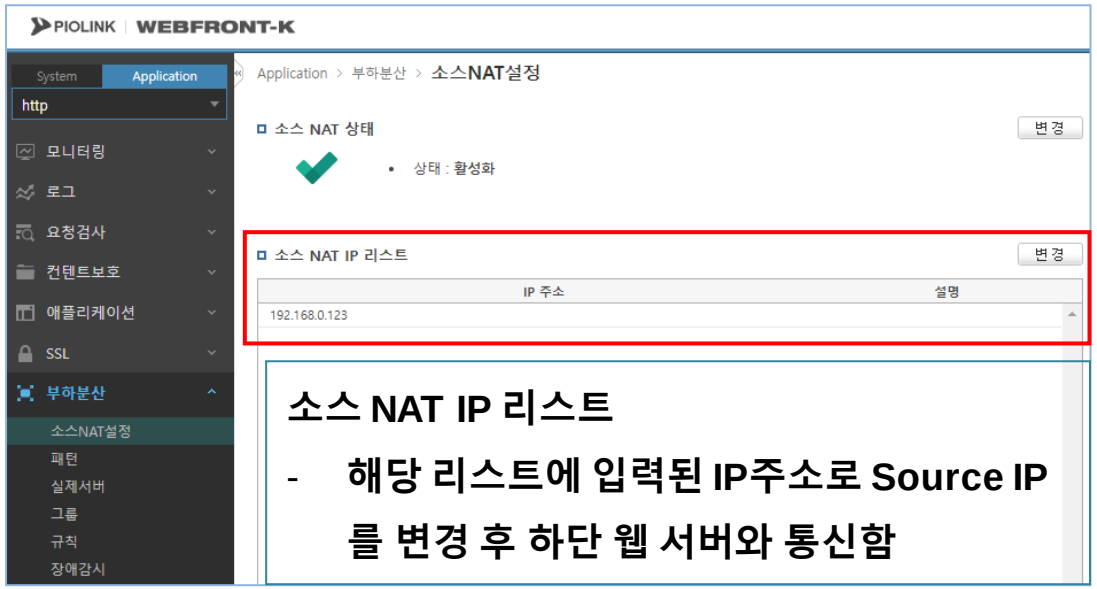
어플리케이션 설정

- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)



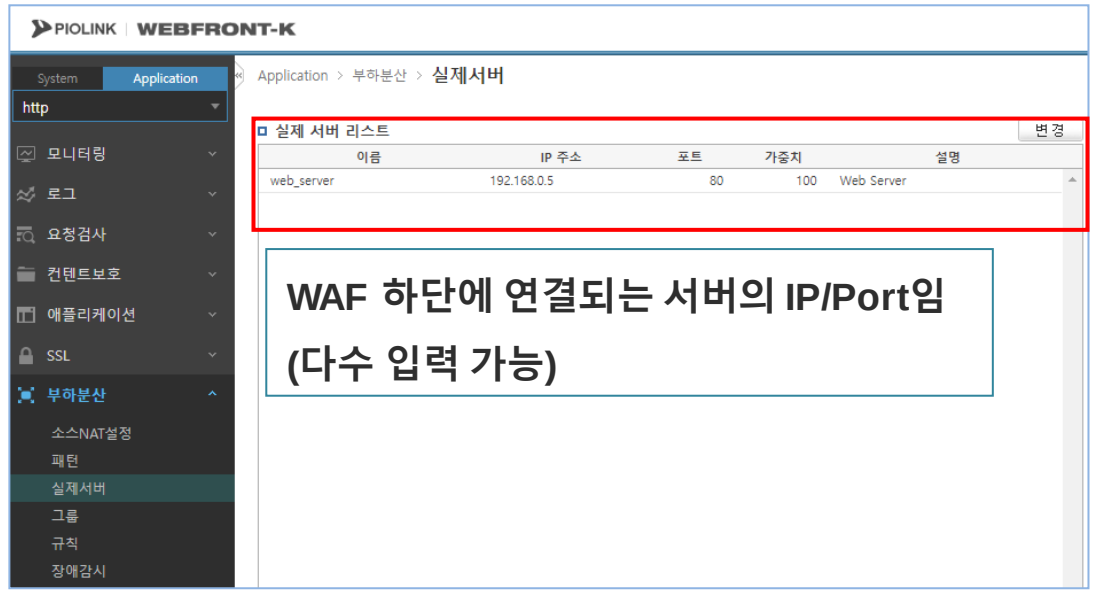
[클라이언트 세션]
SRC IP: 클라이언트 IP
DST IP: WAF 서비스 IP/Port
(애플리케이션에서 설정)

[서버 세션]
SRC IP: SNAT IP
(부하분산 - 소스NAT 설정)
DST IP: 하단 웹 서버 IP/Port
(부하분산 – 실제서버 에서 설정)



소스 NAT IP 리스트

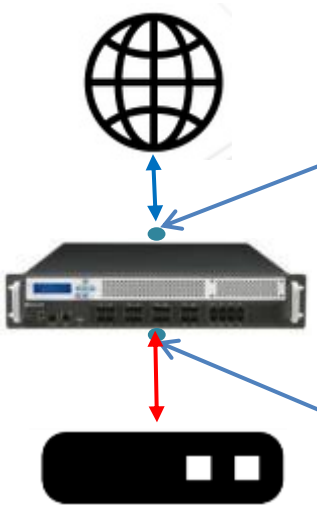
- 해당 리스트에 입력된 IP주소로 Source IP 를 변경 후 하단 웹 서버와 통신함



WAF 하단에 연결되는 서버의 IP/Port임 (다수 입력 가능)

어플리케이션 설정

- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)



[클라이언트 세션]

SRC IP: 클라이언트 IP

DST IP: WAF 서비스 IP/Port

(애플리케이션에서 설정)

[서버 세션]

SRC IP: SNAT IP

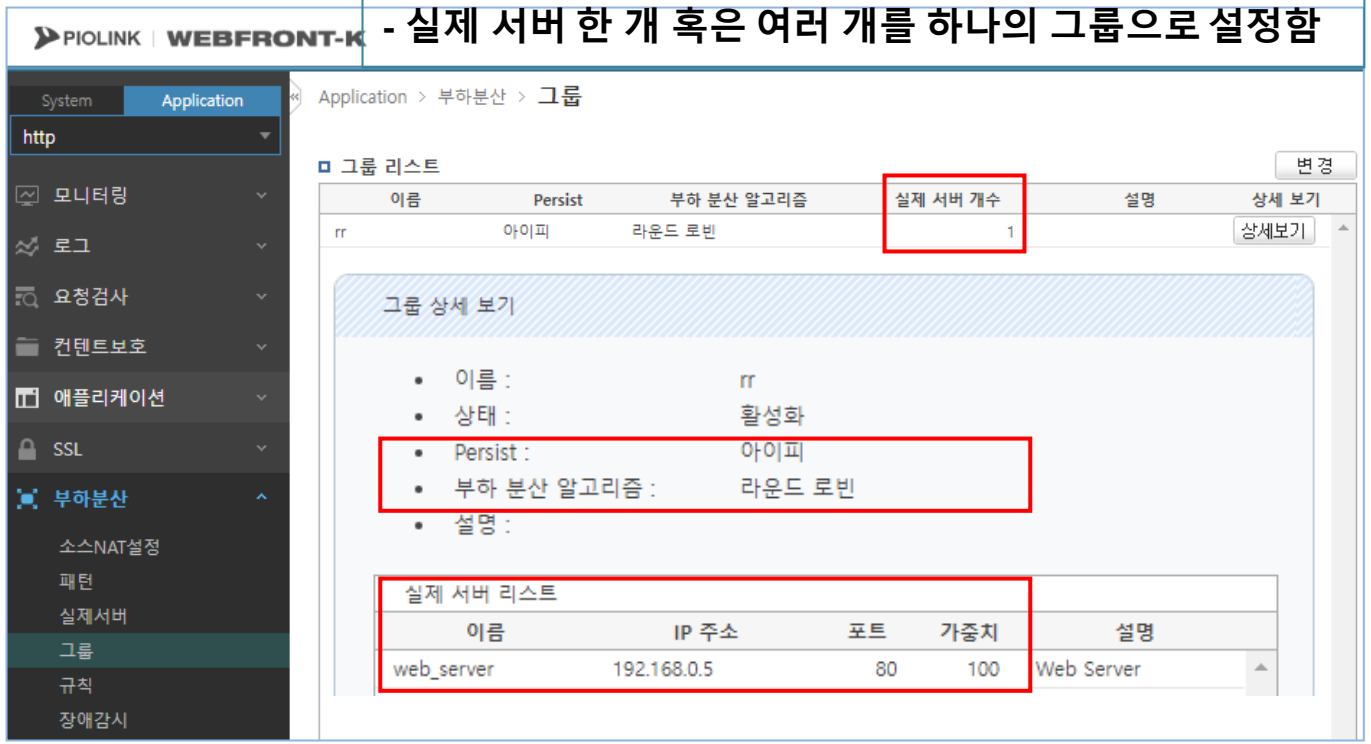
(부하분산 - 소스NAT 설정)

DST IP: 하단 웹 서버 IP/Port

(부하분산 – 실제서버 에서 설정)

그룹

- 실제 서버 한 개 혹은 여러 개를 하나의 그룹으로 설정함



Persist 기준

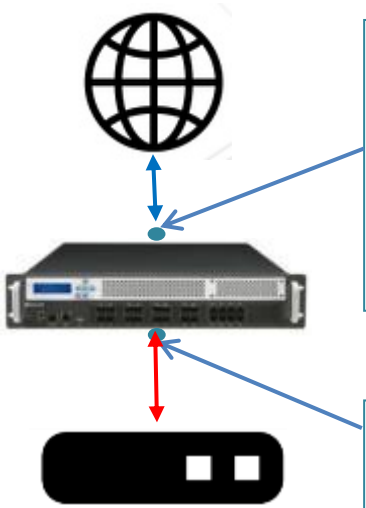
- IP: **SRC IP**를 기준으로 부하분산

(**같은 SRC IP** >> 같은 웹 서버)

- 쿠키: 세션 맺을 때 쿠키 생성 후 해당 **쿠키**를 기준으로 부하분산 (**같은 쿠키** >> 같은 웹 서버)

어플리케이션 설정

- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)



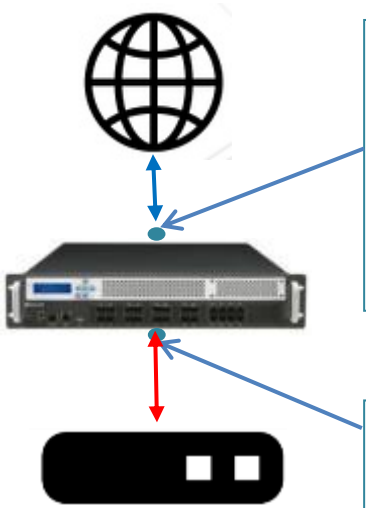
[클라이언트 세션]
SRC IP: 클라이언트 IP
DST IP: WAF 서비스 IP/Port
(애플리케이션에서 설정)

[서버 세션]
SRC IP: SNAT IP
(부하분산 - 소스NAT 설정)
DST IP: 하단 웹 서버 IP/Port
(부하분산 – 실제서버 에서 설정)

규칙 = 그룹 + 패턴(패턴은 설정하지 않아도 무방함)

어플리케이션 설정

- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)



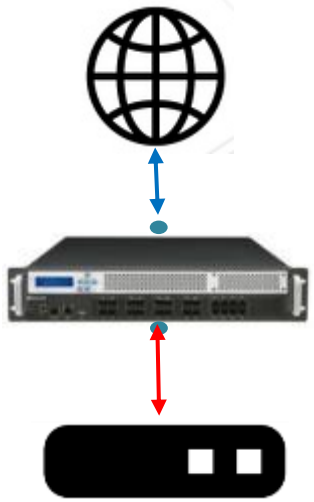
[클라이언트 세션]
SRC IP: 클라이언트 IP
DST IP: WAF 서비스 IP/Port
(애플리케이션에서 설정)

[서버 세션]
SRC IP: SNAT IP
(부하분산 - 소스NAT 설정)
DST IP: 하단 웹 서버 IP/Port
(부하분산 – 실제서버 에서 설정)

장애감시: 웹 서버에 대한 헬스체크 상태 확인
◆ 헬스체크가 되지 않는 웹 서버로는 트래픽 전송 X

어플리케이션 설정

- **WEBFRONT-KS 기본 구성**
  - 아래와 같은 환경으로 구축한다고 가정
  - 기본적인 애플리케이션 및 부하분산 설정은 http를 설정할 경우와 동일하나, 일부 추가/변경이 필요한 설정이 존재함



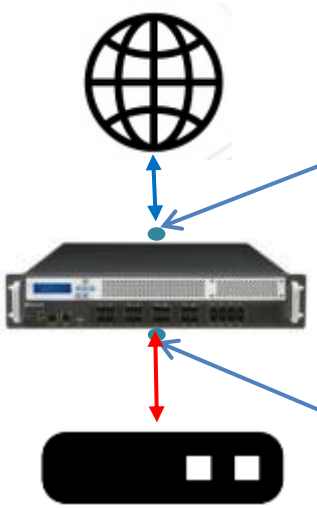
도메인: 1개 (test.com)

WEB: 1개 (192.168.0.5)

프로토콜: **https**

어플리케이션 설정

- **WEBFRONT-KS 기본 구성**
  - 클라이언트 세션 관련 설정(애플리케이션/https)



[클라이언트 세션]

SRC IP: 클라이언트 IP

DST IP: WAF 서비스 IP/Port

(애플리케이션에서 설정)

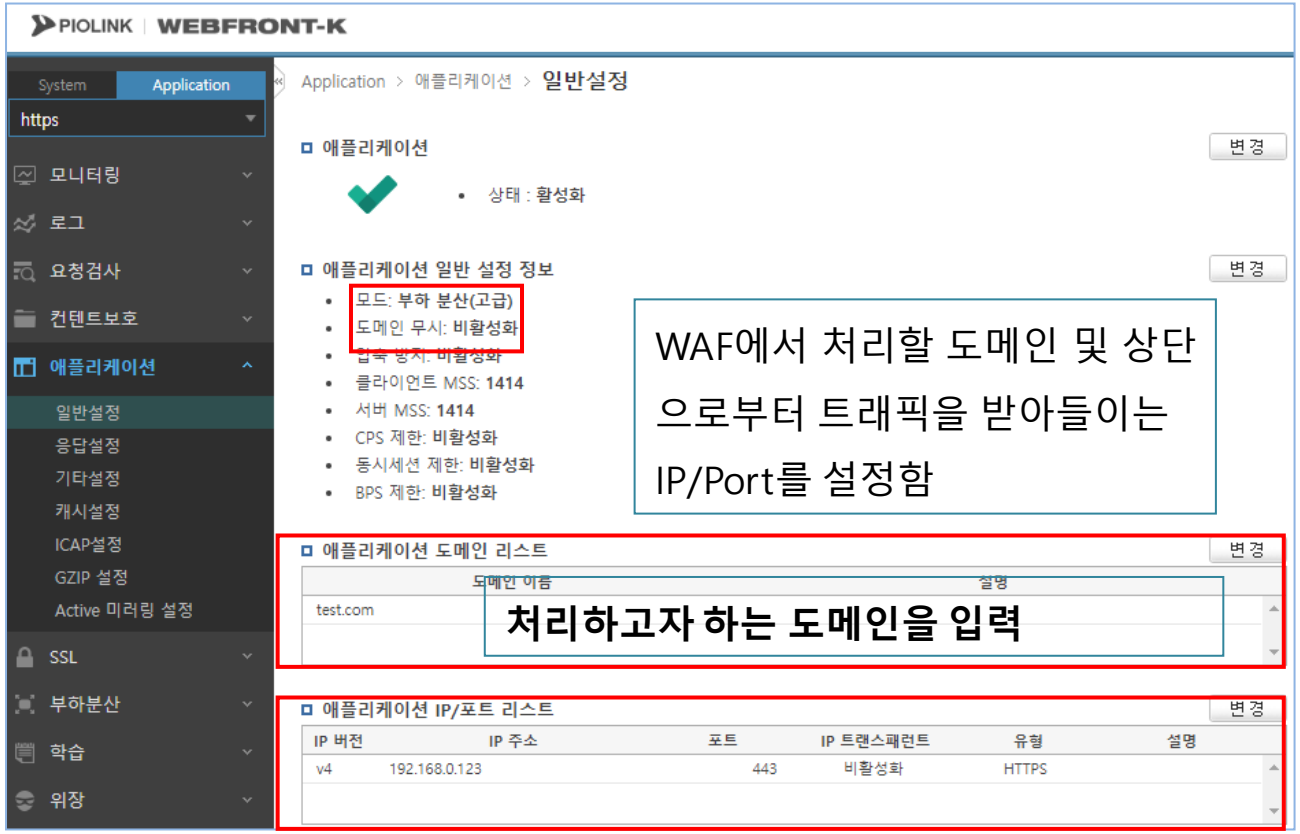
[서버 세션]

SRC IP: SNAT IP

(부하분산 - 소스NAT 설정)

DST IP: 하단 웹 서버 IP/Port

(부하분산 – 실제서버 에서 설정)



WAF에서 처리할 도메인 및 상단으로부터 트래픽을 받아들이는 IP/Port를 설정함

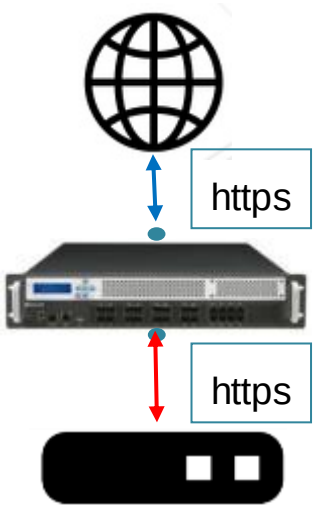
처리하고자 하는 도메인을 입력

서비스용 IP/Port 입력 (웹방화벽의 사설 IP)

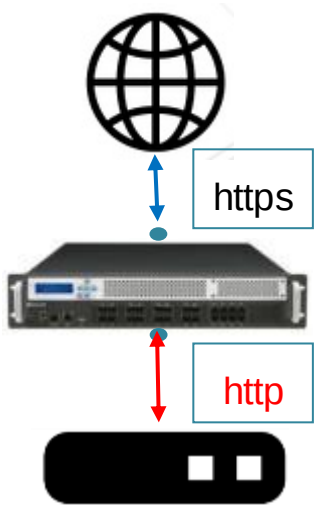
유형을 HTTPS로 설정

어플리케이션 설정

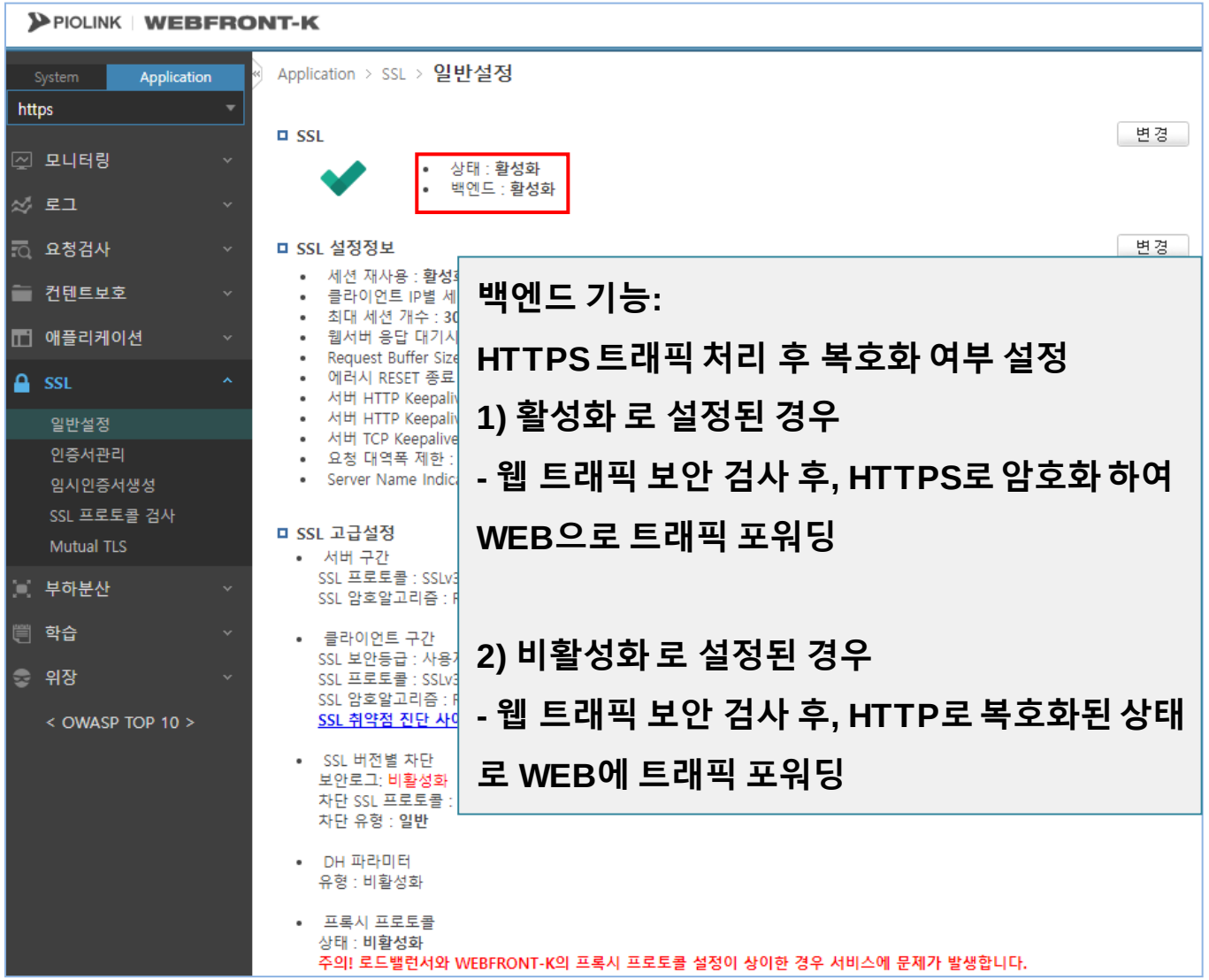
- **WEBFRONT-KS 기본 구성**
  - 클라이언트+서버 세션 관련 설정(SSL)



백엔드 활성화 한 경우



백엔드 비 활성화 한 경우



백엔드 기능:

HTTPS 트래픽 처리 후 복호화 여부 설정

1) 활성화 로 설정된 경우

- 웹 트래픽 보안 검사 후, HTTPS로 암호화 하여 WEB으로 트래픽 포워딩

2) 비활성화 로 설정된 경우

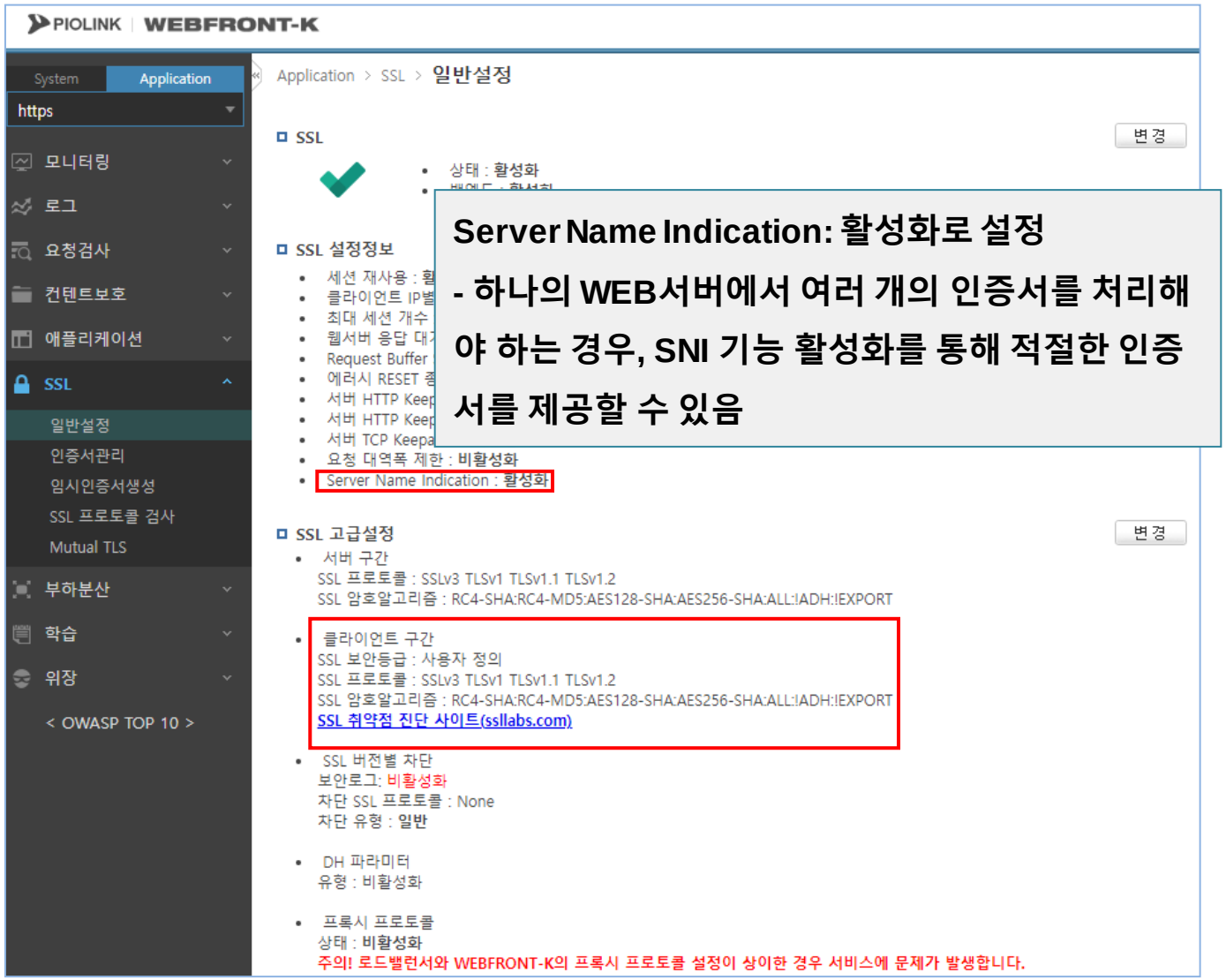
- 웹 트래픽 보안 검사 후, HTTP로 복호화된 상태로 WEB에 트래픽 포워딩

어플리케이션 설정

- **WEBFRONT-KS 기본 구성**
  - 클라이언트+서버 세션 관련 설정(SSL)

SSL 보안등급: A등급으로 설정

- A등급으로 설정하면 안전한 cipher suite를 통해 TLS v1.2로 통신 가능



Server Name Indication: 활성화로 설정

- 하나의 WEB서버에서 여러 개의 인증서를 처리해야 하는 경우, SNI 기능 활성화를 통해 적절한 인증서를 제공할 수 있음

어플리케이션 설정

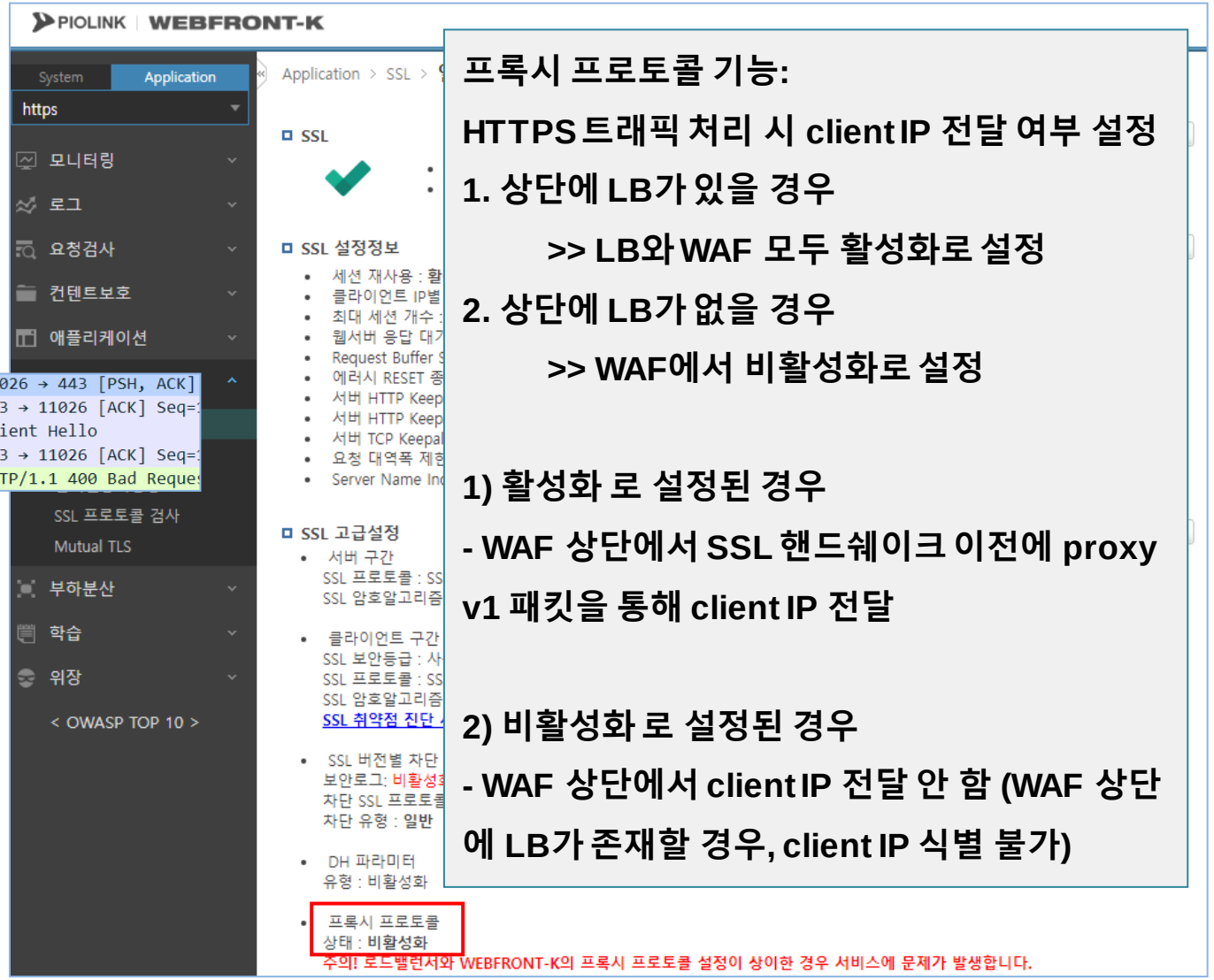
- **WEBFRONT-KS 기본 구성**
  - 클라이언트+서버 세션 관련 설정(SSL)

프록시 프로토콜 활성화: WAF에서 SSL 핸드쉐이크 이전에 proxy v1패킷 수신 대기 (proxy v1 이외의 패킷 수신 시 rst 발송)

192.168.0.12	192.168.0.123	PROXYv1	103	0.000041000	0.000041000	11026 → 443 [PSH, ACK]
192.168.0.123	192.168.0.12	TCP	54	0.000009000	0.000009000	443 → 11026 [ACK] Seq=
192.168.0.12	192.168.0.123	TLSv1	571	0.000091000	0.000091000	Client Hello
192.168.0.123	192.168.0.12	TCP	54	0.000008000	0.000008000	443 → 11026 [ACK] Seq=
192.168.0.123	192.168.0.12	HTTP	322	0.000057000	0.000057000	HTTP/1.1 400 Bad Reque

```
PROXY Protocol
  PROXY v1 magic
  Protocol: TCP4
  Source Address:
  Destination Address: 192.168.0.12
  Source Port: 49937
  Destination Port: 443
```

Proxy v1 패킷 내 client IP 정보 포함



프록시 프로토콜 기능:

HTTPS 트래픽 처리 시 client IP 전달 여부 설정

1. 상단에 LB가 있을 경우

>> LB와 WAF 모두 활성화로 설정

2. 상단에 LB가 없을 경우

>> WAF에서 비활성화로 설정

1) 활성화 로 설정된 경우

- WAF 상단에서 SSL 핸드쉐이크 이전에 proxy v1 패킷을 통해 client IP 전달

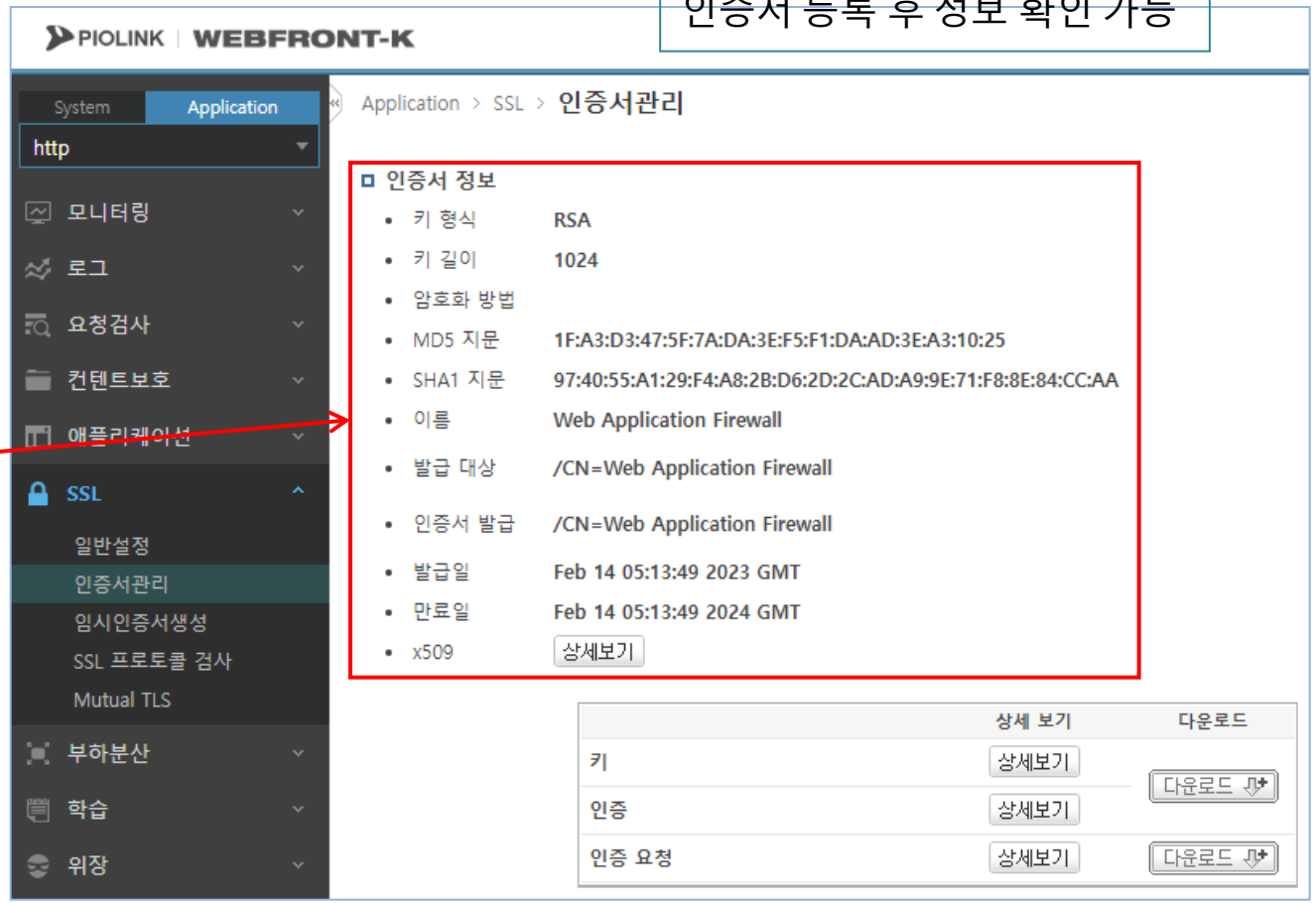
2) 비활성화 로 설정된 경우

- WAF 상단에서 client IP 전달 안 함 (WAF 상단에 LB가 존재할 경우, client IP 식별 불가)

어플리케이션 설정

- **WEBFRONT-KS 기본 구성**
  - 클라이언트+서버 세션 관련 설정(인증서 관리)
  - 아래 순서대로 인증서+개인키를 하나의 파일로 합친 후 등록

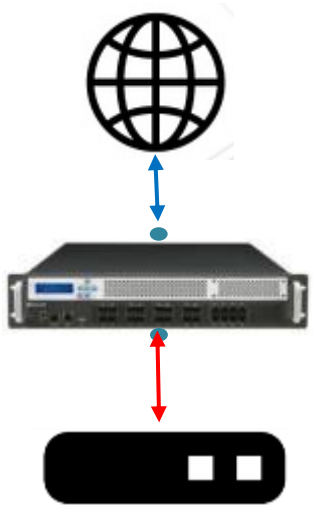
인증서 등록 후 정보 확인 가능



PIOLINK

어플리케이션 설정

- **WEBFRONT-KS 기본 구성**
  - 아래와 같은 환경으로 구축한다고 가정
  - 기본적인 애플리케이션 및 부하분산 설정은 http를 설정할 경우와 동일하나, 일부 변경이 필요한 설정이 존재함 (애플리케이션 도메인 리스트)
  - 만약 도메인 별로 처리하는 WEB의 IP가 다르다면, 각각의 도메인 별로 다수의 애플리케이션을 생성해야 함



도메인: 2개

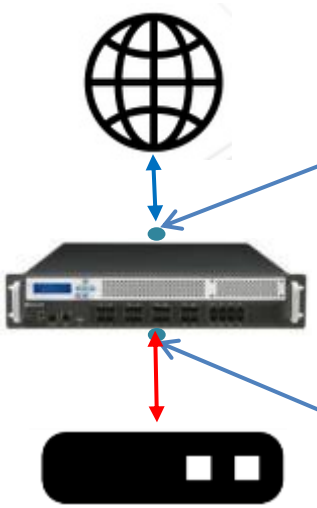
(test1.com, test2.com)

WEB: 1개 (192.168.0.5)

프로토콜: http

어플리케이션 설정

- **WEBFRONT-KS 기본 구성**
  - 클라이언트 세션 관련 설정(애플리케이션)



[클라이언트 세션]

SRC IP: 클라이언트 IP

DST IP: WAF 서비스 IP/Port

(애플리케이션에서 설정)

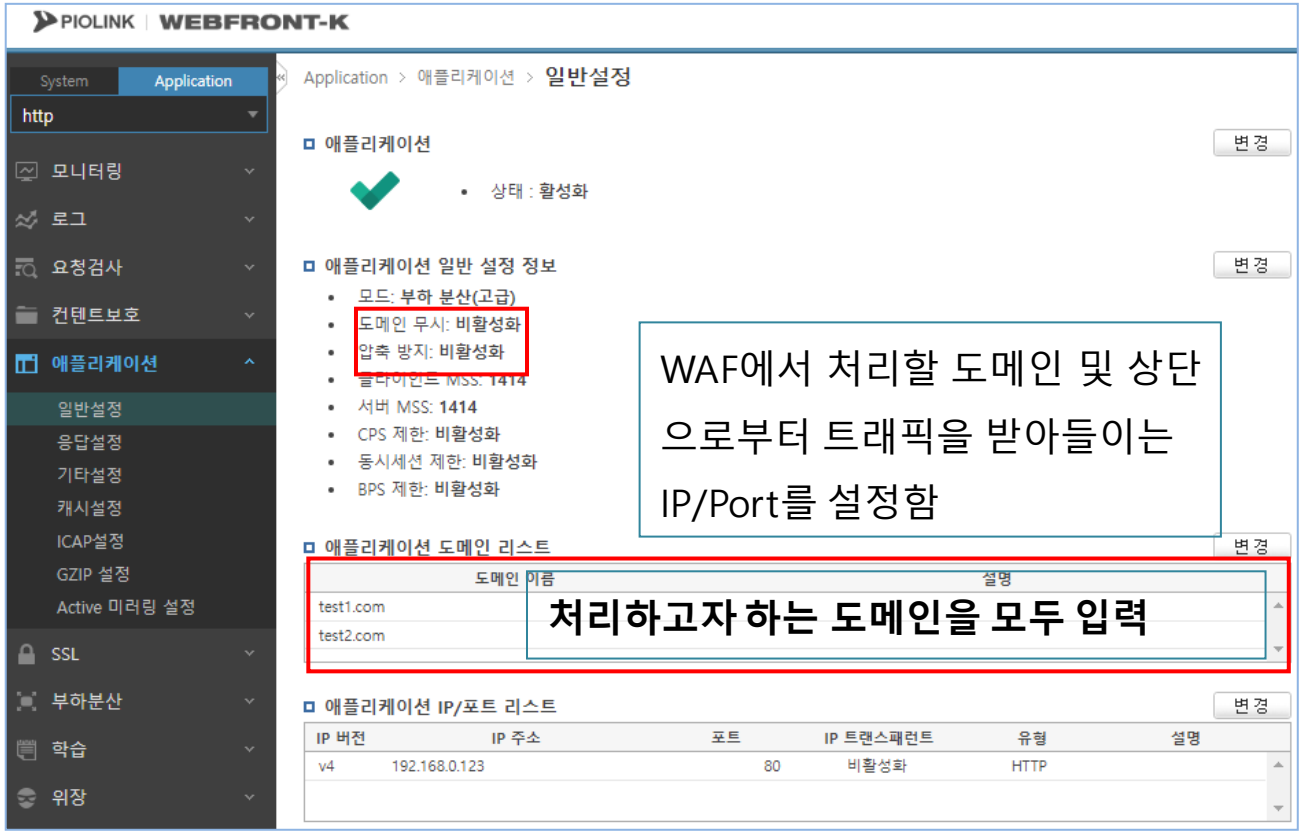
[서버 세션]

SRC IP: SNAT IP

(부하분산 - 소스NAT 설정)

DST IP: 하단 웹 서버 IP/Port

(부하분산 – 실제서버 에서 설정)



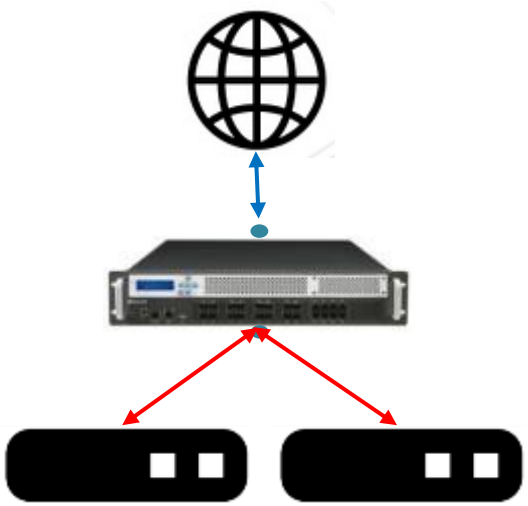
WAF에서 처리할 도메인 및 상단으로부터 트래픽을 받아들이는 IP/Port를 설정함

처리하고자 하는 도메인을 모두 입력

PIOLINK

어플리케이션 설정

- **WEBFRONT-KS 기본 구성**
  - 아래와 같은 환경으로 구축한다고 가정
  - 기본적인 애플리케이션 및 부하분산 설정은 http를 설정할 경우와 동일하나, 일부 변경이 필요한 설정이 존재함 (부하분산 내 실제서버 및 그룹)



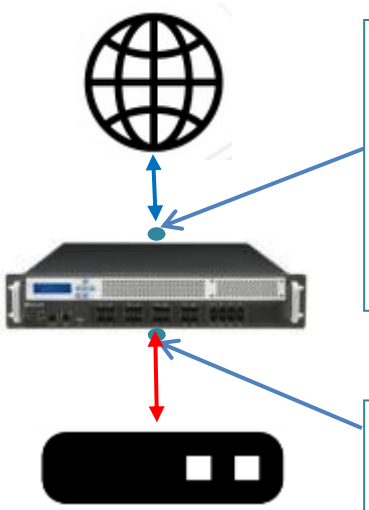
도메인: 1개 (test.com)

WEB: 2개 (192.168.0.5, 192.168.0.6)

프로토콜: http

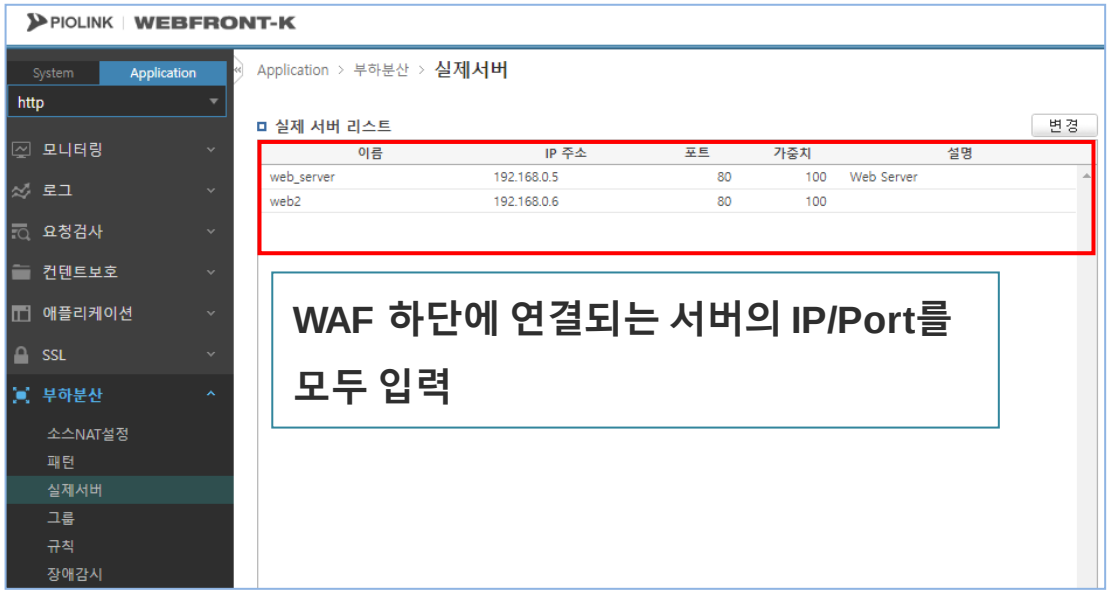
어플리케이션 설정

- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)

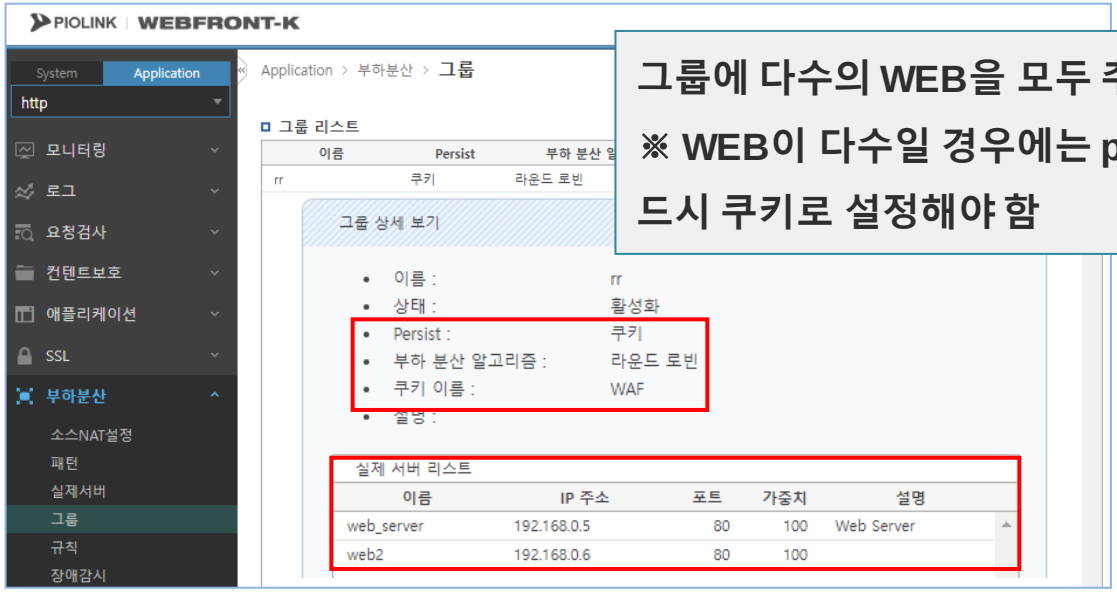


[클라이언트 세션]
SRC IP: 클라이언트 IP
DST IP: WAF 서비스 IP/Port
(애플리케이션에서 설정)

[서버 세션]
SRC IP: SNAT IP
(부하분산 - 소스NAT 설정)
DST IP: 하단 웹 서버 IP/Port
(부하분산 – 실제서버 에서 설정)



WAF 하단에 연결되는 서버의 IP/Port를 모두 입력



그룹에 다수의 WEB을 모두 추가
※ WEB이 다수일 경우에는 persist를 반드시 쿠키로 설정해야 함

PIOLINK

5. 설정 체크리스트

HTTP 설정 체크

- 애플리케이션 일반 설정
- 부하분산 – 소스 NAT 설정
- 부하분산 – 실제 서버 설정
- 부하분산 – 그룹 설정
- 부하분산 – 규칙 설정
- 부하분산 – 장애 감시 설정

1. HTTP

- **WEBFRONT-KS 설정 체크**
  - 웹방화벽으로서 기능하기 위한 최소한의 설정 상태 체크

애플리케이션 일반 설정

✓ 애플리케이션 상태 활성화 여부
✓ 애플리케이션 도메인 등록 여부
✓ 애플리케이션 IP/Port 등록 여부

소스NAT설정

✓ 소스 NAT 상태 활성화 여부
✓ 소스 NAT IP 등록 여부

1. HTTP

- **WEBFRONT-KS 설정 체크**
  - 웹방화벽으로서 기능하기 위한 최소한의 설정 상태 체크

실제 서버 설정

✓ 실제서버 IP/Port 정상 등록 여부

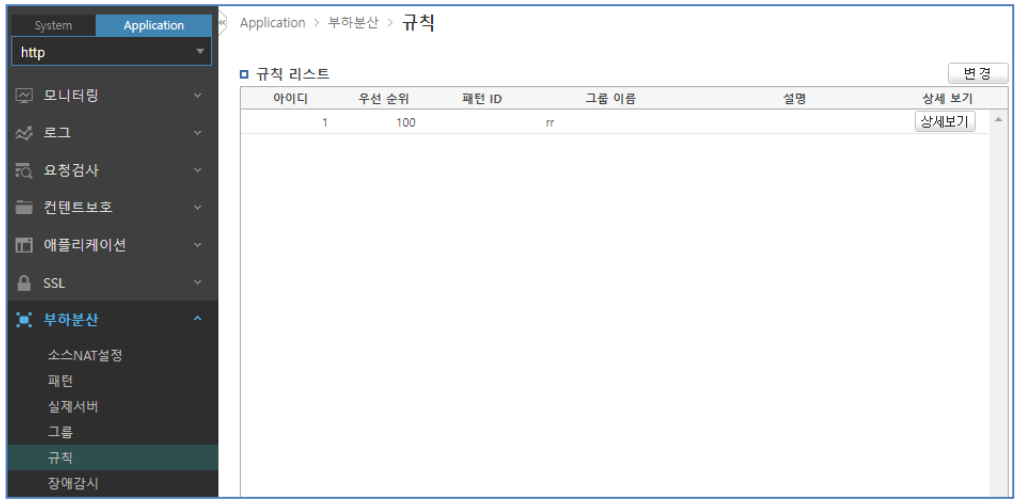
그룹 설정

✓ 그룹에 등록된 실제 서버 개수 확인
✓ Persist 설정 여부

1. HTTP

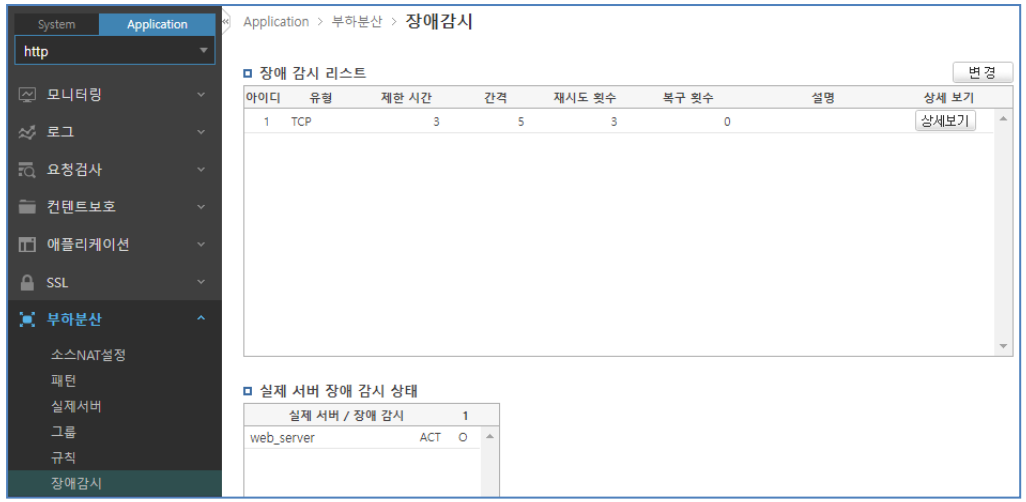
- **WEBFRONT-KS 설정 체크**
  - 웹방화벽으로서 기능하기 위한 최소한의 설정 상태 체크

규칙 설정



✓ 규칙 내에 그룹 등록 여부

장애 감시 설정



✓ 장애 감시 프로토콜의 tcp 설정 여부
✓ 장애 감시 tcp 포트 설정 확인
✓ 장애 감시 상태의 정상 여부

HTTPS 설정 체크

- 애플리케이션 일반 설정
- 부하분산 – 소스 NAT 설정
- 부하분산 – 실제 서버 설정
- 부하분산 – 그룹 설정
- 부하분산 – 규칙 설정
- 부하분산 – 장애 감시 설정
- SSL 인증서 등록
- SSL 일반 설정

2. HTTPS

- **WEBFRONT-KS 설정 체크**
  - 웹방화벽으로서 기능하기 위한 최소한의 설정 상태 체크

애플리케이션 일반 설정

- ✓ 애플리케이션 상태 활성화 여부
- ✓ 애플리케이션 도메인 등록 여부
- ✓ 애플리케이션 IP/Port 등록 + 유형의 HTTPS 설정 여부

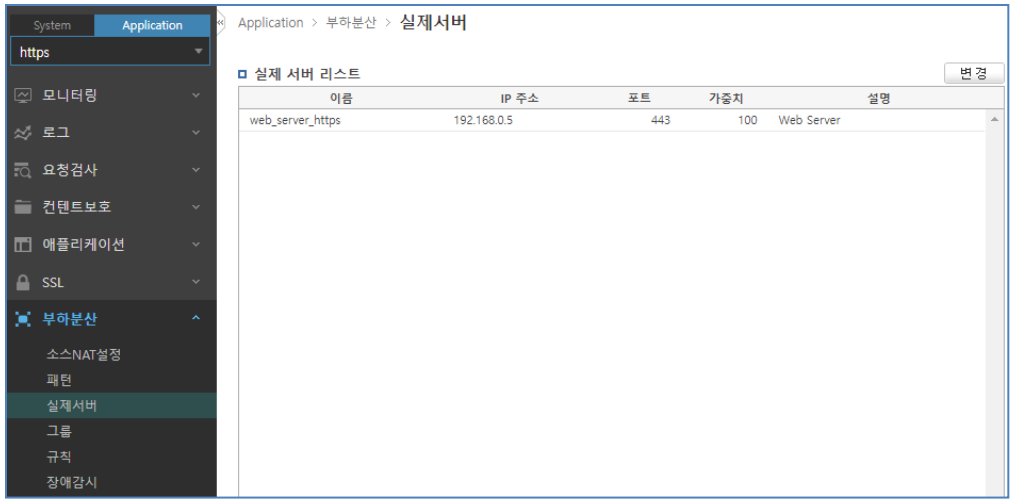
소스NAT설정

- ✓ 소스 NAT 상태 활성화 여부
- ✓ 소스 NAT IP 등록 여부

2. HTTPS

- **WEBFRONT-KS 설정 체크**
  - 웹방화벽으로서 기능하기 위한 최소한의 설정 상태 체크

실제 서버 설정



✓ 실제서버 IP/Port 정상 등록 여부

그룹 설정

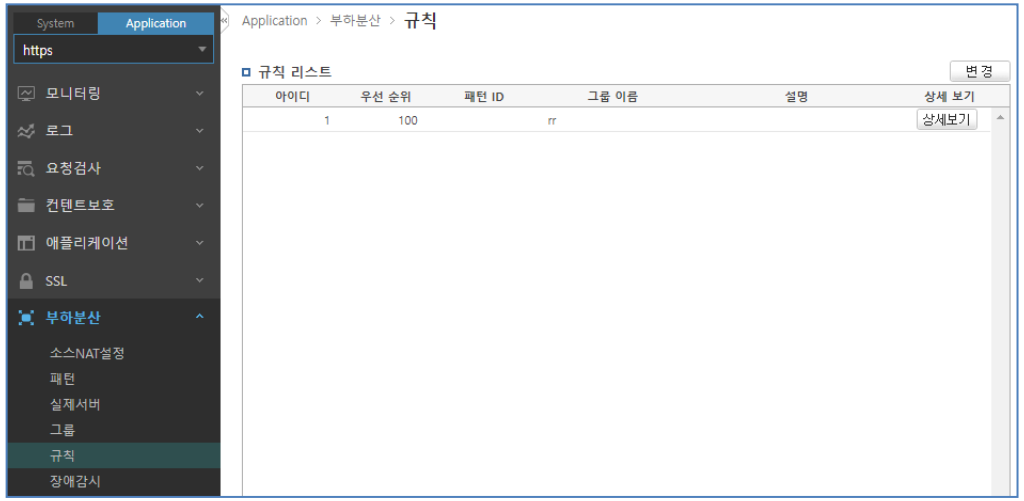
✓ 그룹에 등록된 실제 서버 개수 체크
✓ Persist 설정 여부

PIOLINK

2. HTTPS

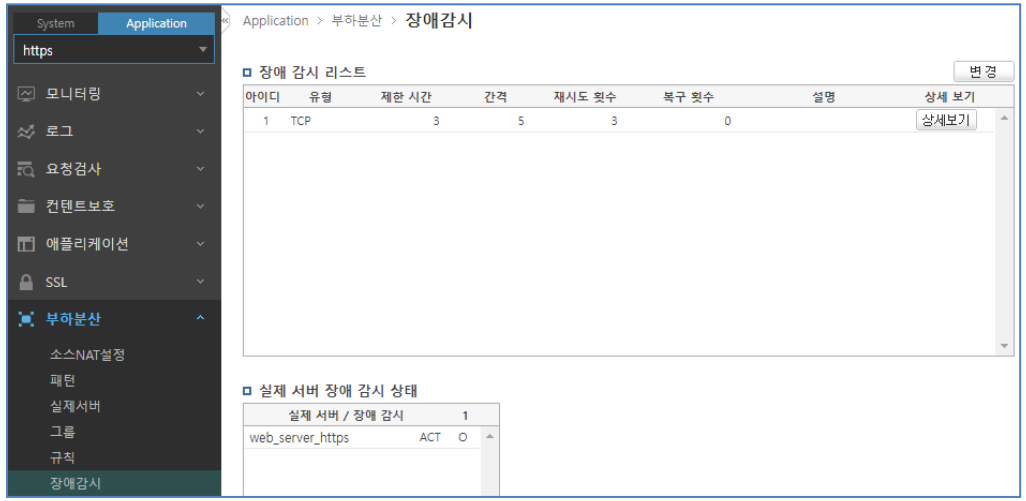
- **WEBFRONT-KS 설정 체크**
  - 웹방화벽으로서 기능하기 위한 최소한의 설정 상태 체크

규칙 설정



✓ 규칙 내에 그룹 등록 여부

장애 감시 설정



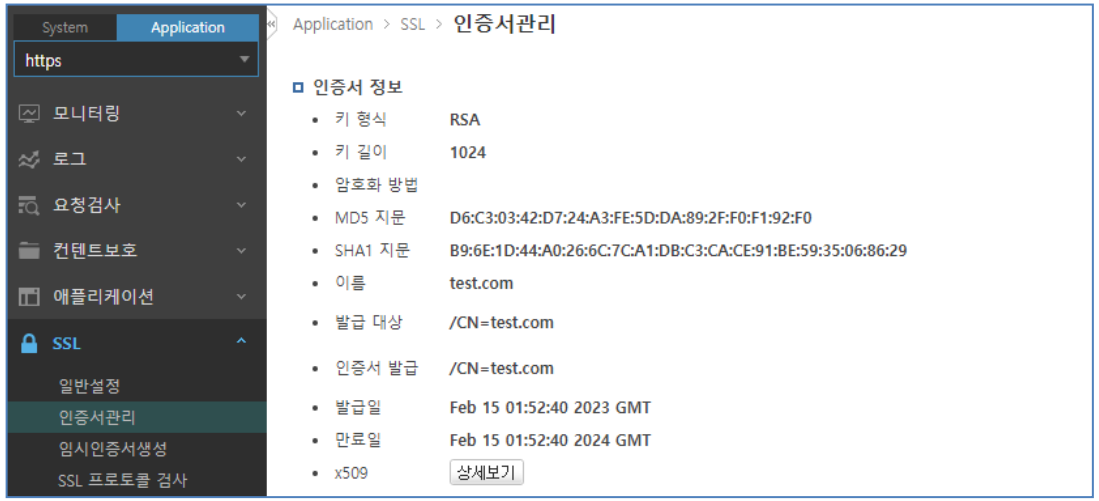
✓ 장애 감시 프로토콜의 tcp 설정 여부
✓ 장애 감시 tcp 포트 설정 확인
✓ 장애 감시 상태의 정상 여부

PIOLINK

2. HTTPS

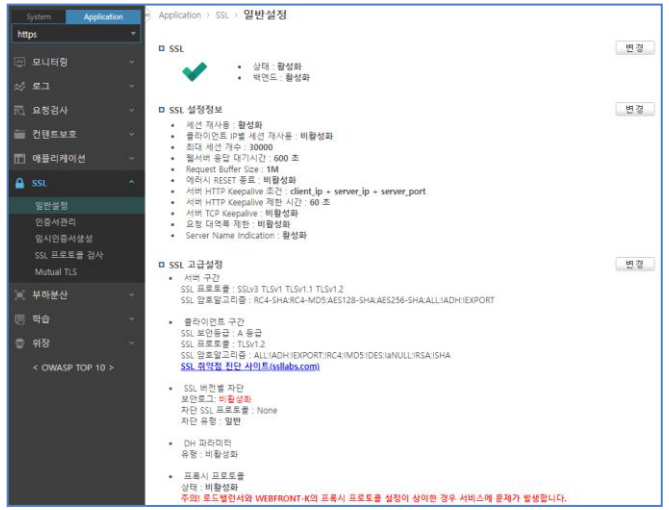
- **WEBFRONT-KS 설정 체크**
  - 웹방화벽으로서 기능하기 위한 최소한의 설정 상태 체크

인증서 관리 설정



✓ 인증서 정상 등록 여부
✓ 인증서 내 유효 도메인 및 유효 날짜 확인

SSL 일반 설정



✓ SSL 상태 활성화 여부 확인
✓ 백엔드 설정 확인
✓ 프록시 프로토콜 설정 확인

PIOLINK

(주) 파이오링크

(본사) 서울시 금천구 가산디지털2로 98, IT캐슬 1동 401호
대표전화 02 2025 6900 | www.PIOLINK.com