PIOLINK

PIOLINK

웹 보안에 최고 성능을 담다

WEBFRONT-KS 초기 설정 가이드

㈜파이오링크

PIOLINK

개요

1. 네트워크 설정
2. HTTP 서비스 설정
3. HTTPS 서비스 설정
4. 설정 체크리스트

PIOLINK

PIOLINK

1. 네트워크 설정

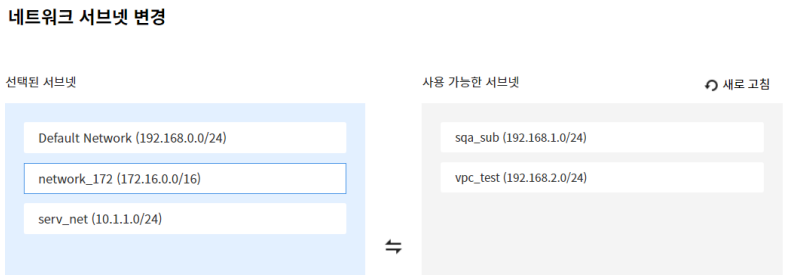
PIOLINK

추가 인터페이스 설정

Mgmt 이외의 추가 인터페이스 설정

- NHN클라우드 콘솔에서 WAF에 여러 개의 인터페이스 추가가 가능하나, mgmt 인터페이스에 대해서만 dhcp로 IP가 자동 설정됨
- Mgmt 외 추가 인터페이스에 대해서는 WAF 웹UI에서 추가 설정이 필요함

인터페이스 할당 (클라우드 콘솔)



Vlan 설정

IP주소 추가

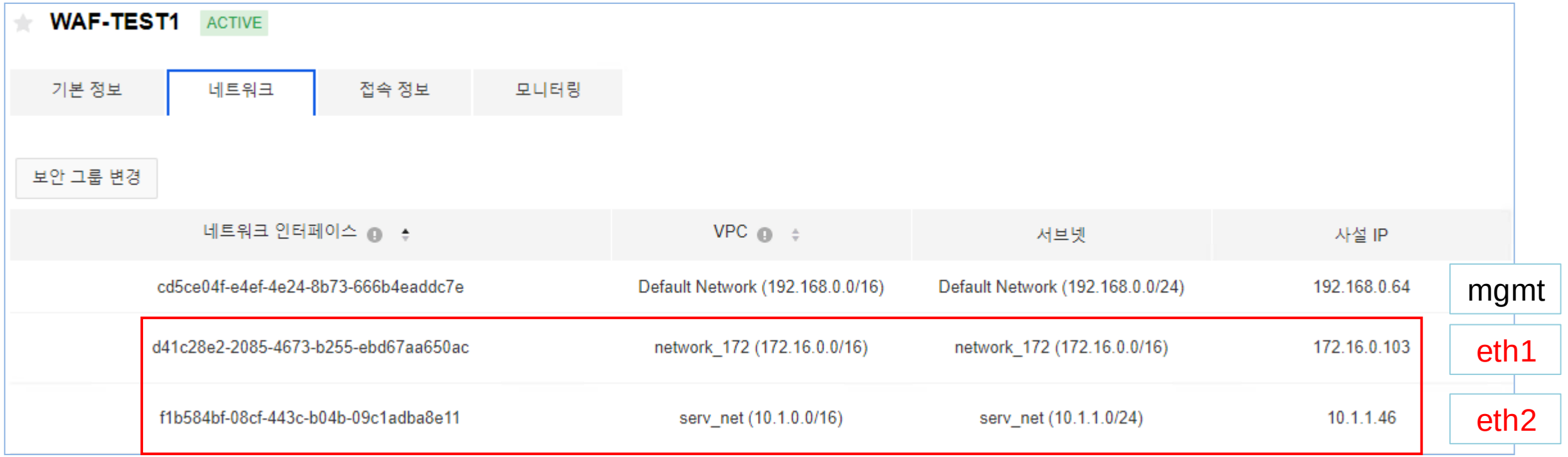
PIOLINK

추가 인터페이스 설정

Mgmt 이외의 추가 인터페이스 설정

1. 인터페이스 할당

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

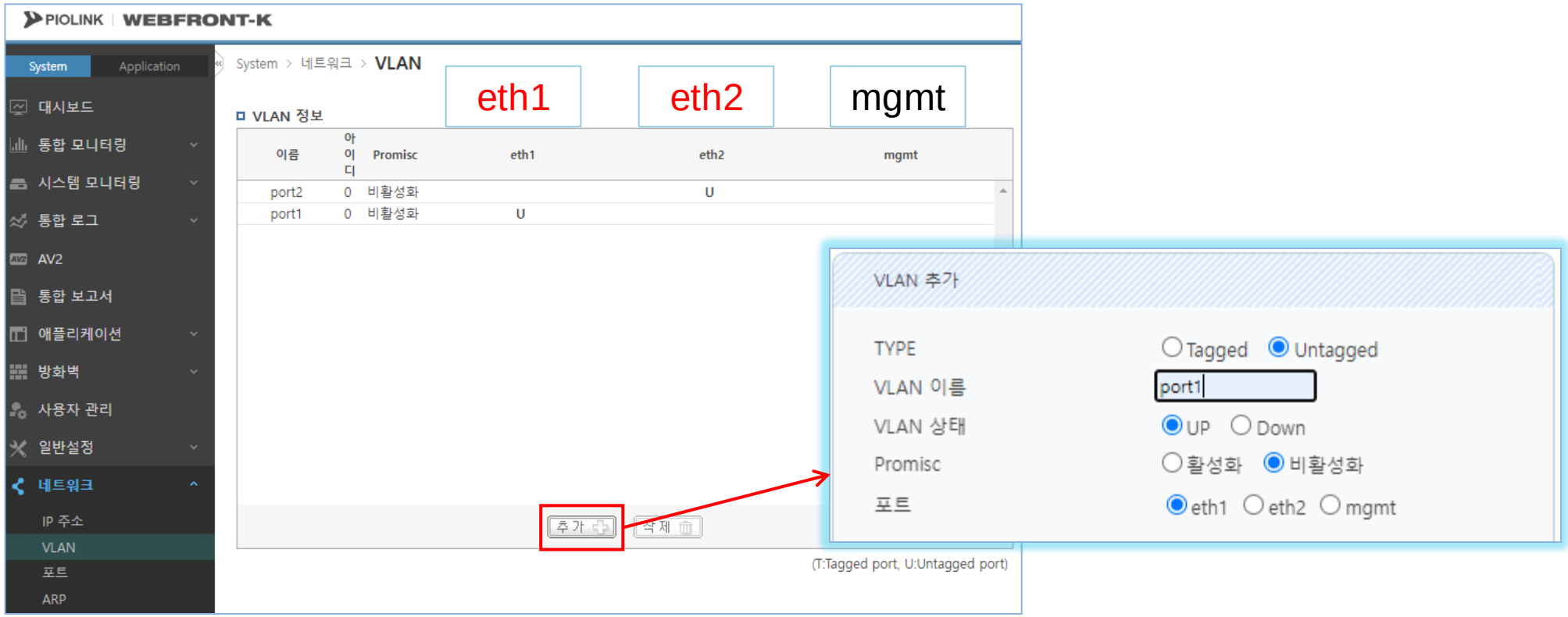


추가 인터페이스 설정

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)



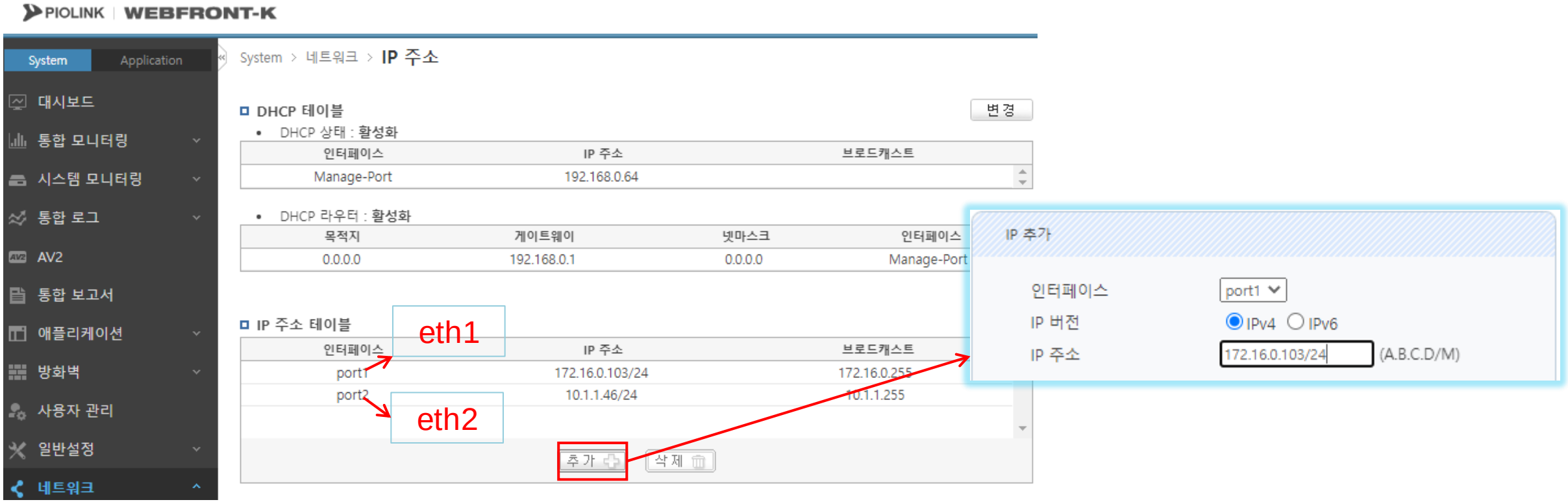
PIOLINK

추가 인터페이스 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)



PIOLINK

2. HTTP 서비스 설정

HTTP 서비스 설정 순서

1. Login
2. 애플리케이션 일반 설정
3. 부하분산 – 소스 NAT 설정
4. 부하분산 – 실제 서버 설정
5. 부하분산 – 그룹 설정
6. 부하분산 – 규칙 설정
7. 부하분산 – 장애 감시 설정
8. 애플리케이션 및 SNAT 활성화
9. 설정 저장
10. 웹 서비스 확인

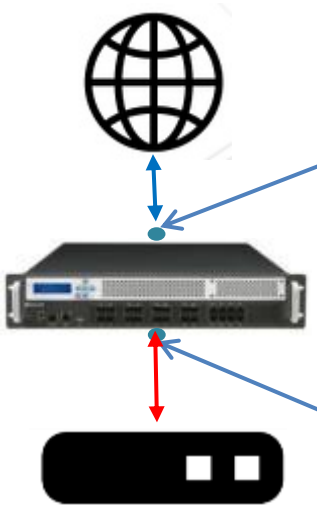
1. Login

- **WEBFRONT-KS 로그인**
  - 웹UI 접속 경로: **https://{웹방화벽 FIP}:8443**
  - 계정: wfadmin // 비밀번호: waf12!@{인스턴스 이름 첫 5글자}
    - 만약 인스턴스의 이름이 5글자 미만이라면, 인스턴스 이름 전체를 입력 (대소문자 구별 필요)
    - 인스턴스 이름에 특수문자 및 숫자가 포함되어 있더라도 그대로 입력

2. 애플리케이션 일반 설정

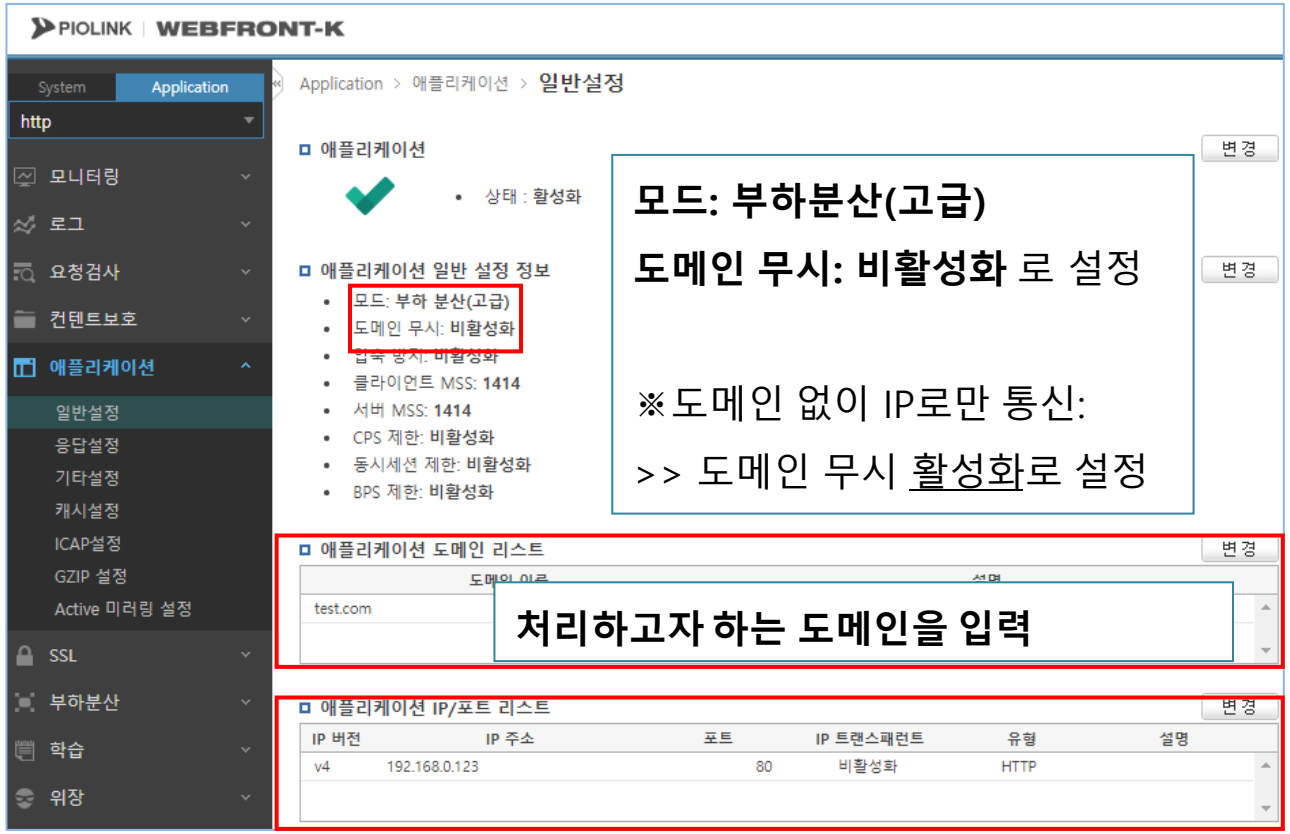
WAF에서 처리할 도메인 및 상단으로부터 트래픽을 받아들이는 IP/Port를 설정함

- **WEBFRONT-KS 기본 구성**
  - 클라이언트 세션 관련 설정(애플리케이션)
  - 설정 경로: Application > 애플리케이션 > 일반설정



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

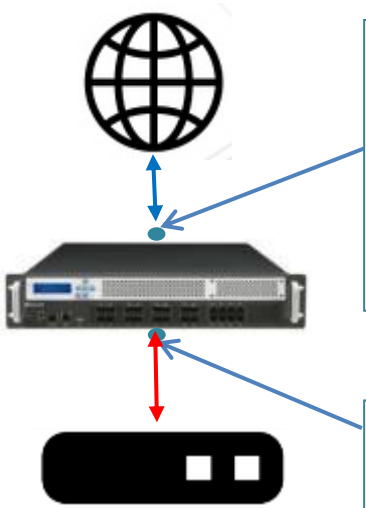
[서버 세션]
SRC IP: SNAT IP
(부하분산 - 소스NAT 설정)
DST IP: 하단 웹 서버 IP/Port
(부하분산 – 실제서버 에서 설정)



서비스용 IP/Port 입력 (웹방화벽의 사설 IP)

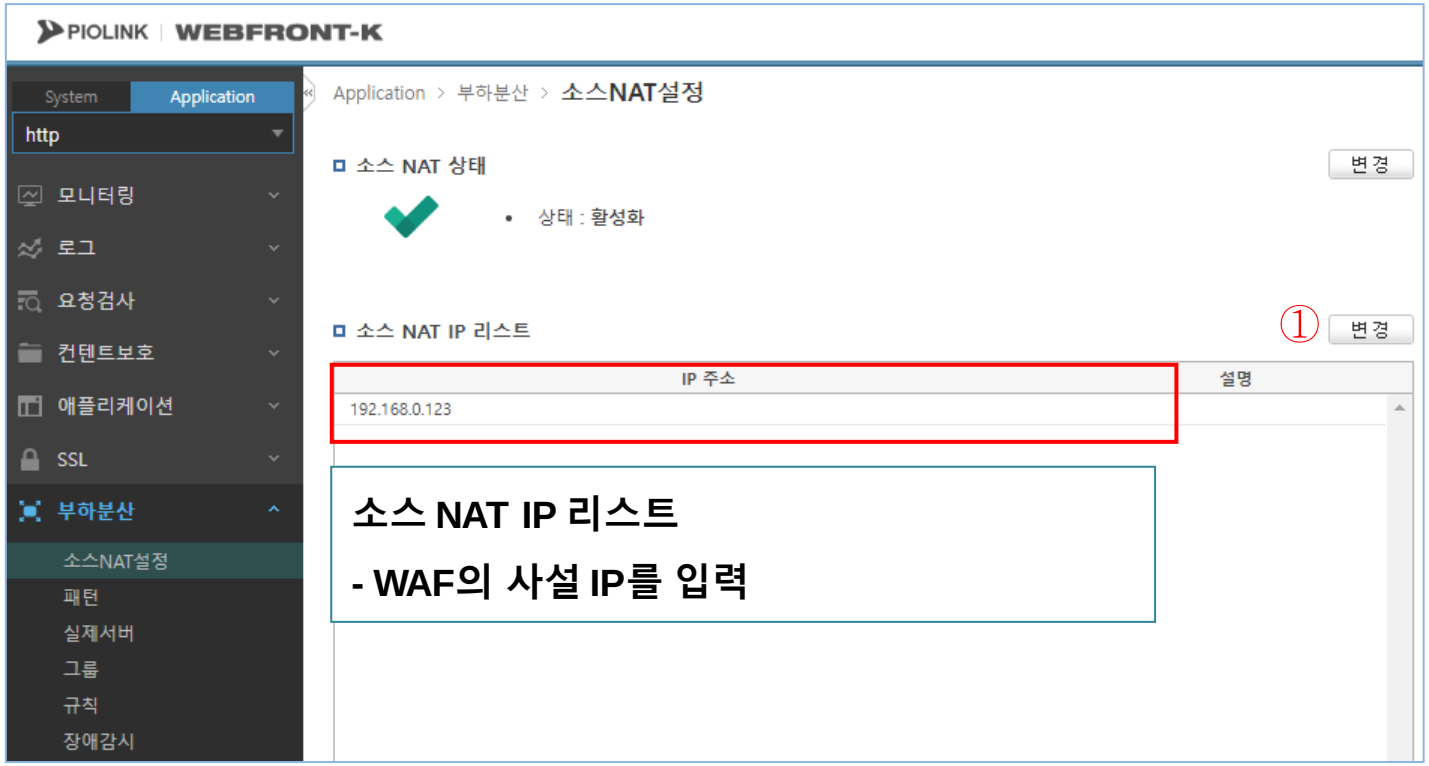
3. 부하분산 – 소스 NAT 설정

- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)
  - 설정 경로: Application > 부하분산 > 소스NAT설정



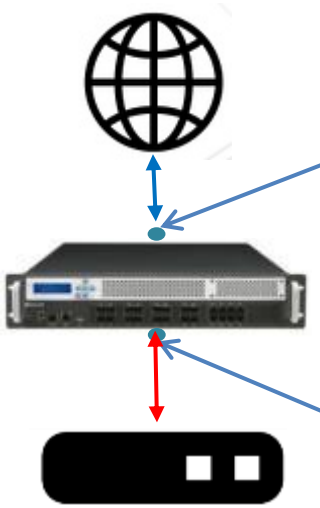
[클라이언트 세션]
SRC IP: 클라이언트 IP
DST IP: WAF 서비스 IP/Port
(애플리케이션에서 설정)

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



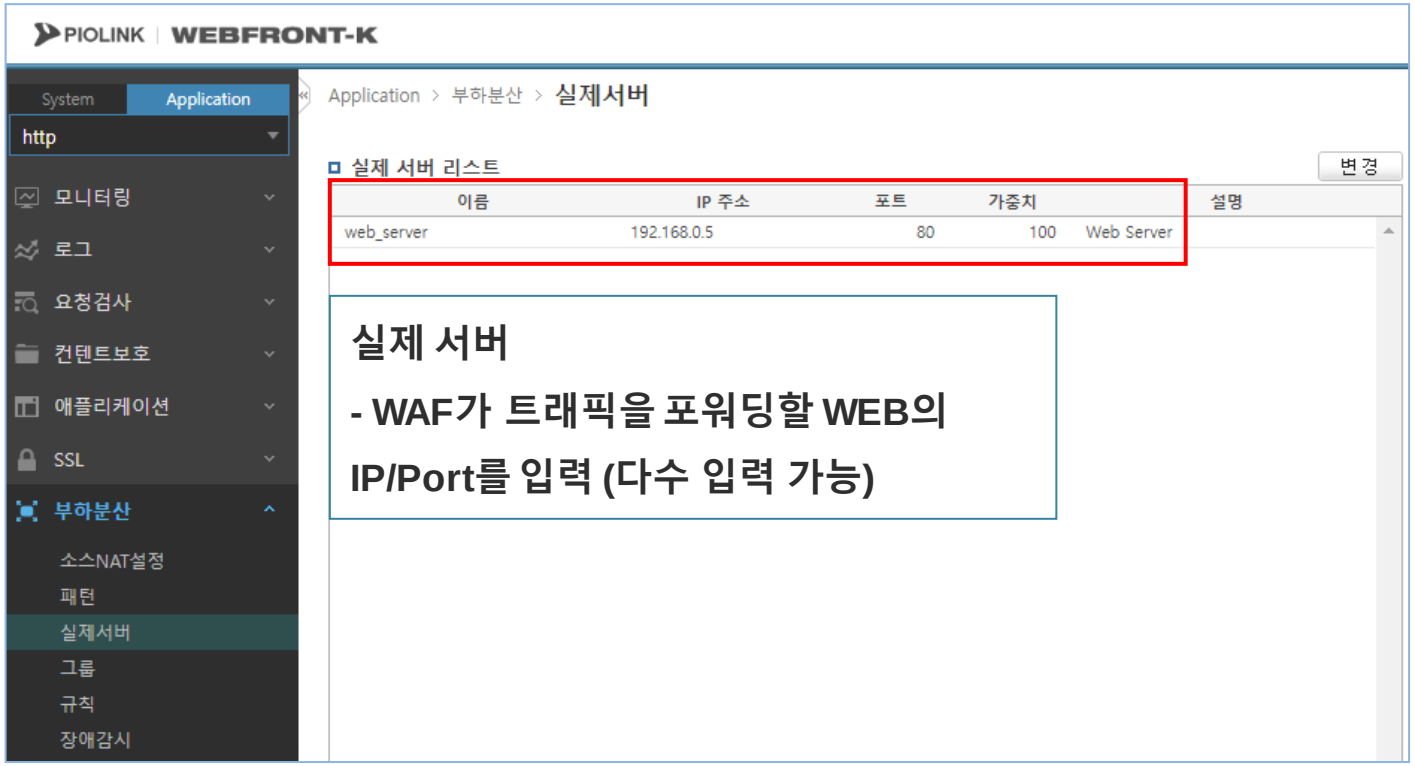
4. 부하분산 – 실제 서버 설정

- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)
  - 설정 경로: Application > 부하분산 > 실제서버



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

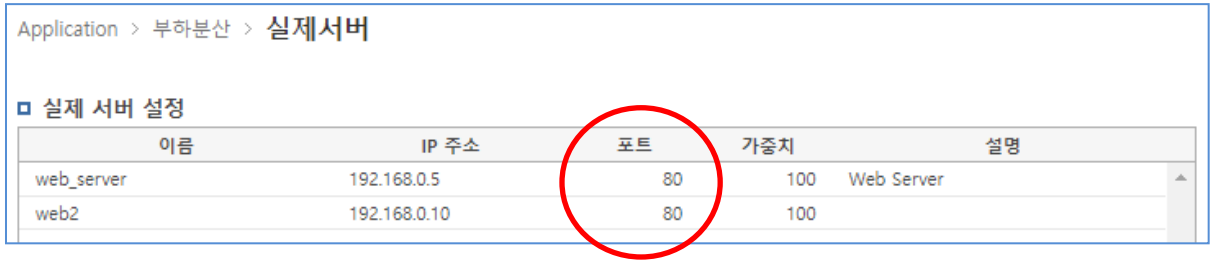
[서버 세션]
SRC IP: SNAT IP
(부하분산 - 소스NAT 설정)
DST IP: 하단 웹 서버 IP/Port
(부하분산 – 실제서버 에서 설정)



PIOLINK

4. 부하분산 – 실제 서버 설정

- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)
  - 설정 경로: Application > 부하분산 > 실제서버



실제 서버

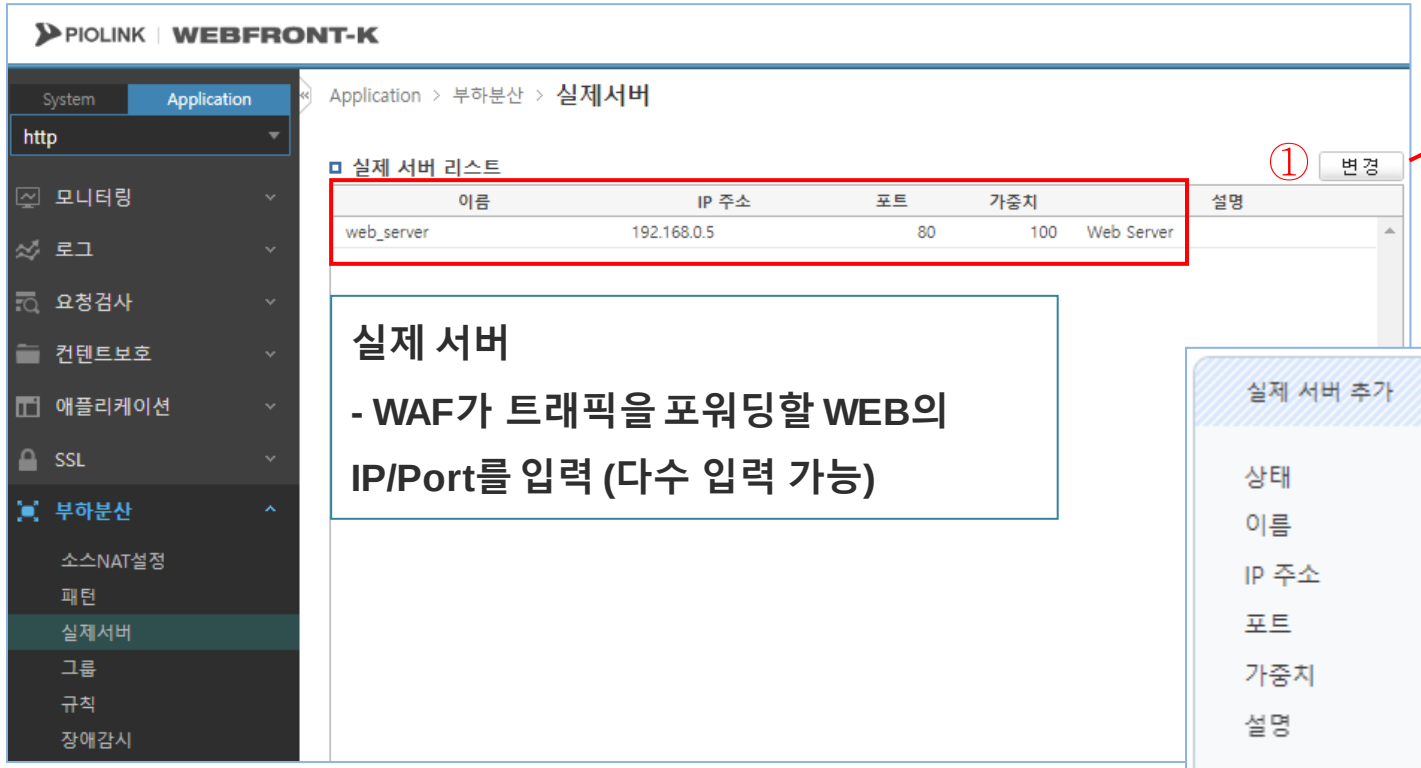
- 실제 서버는 부하 분산을 위한 서버 리스트임

>> 그러므로 다수의 WEB서버를 등록할 때에는 같은 Port를 사용하면서 같은 서비스를 수행하는 다수의 서버만 등록

PIOLINK

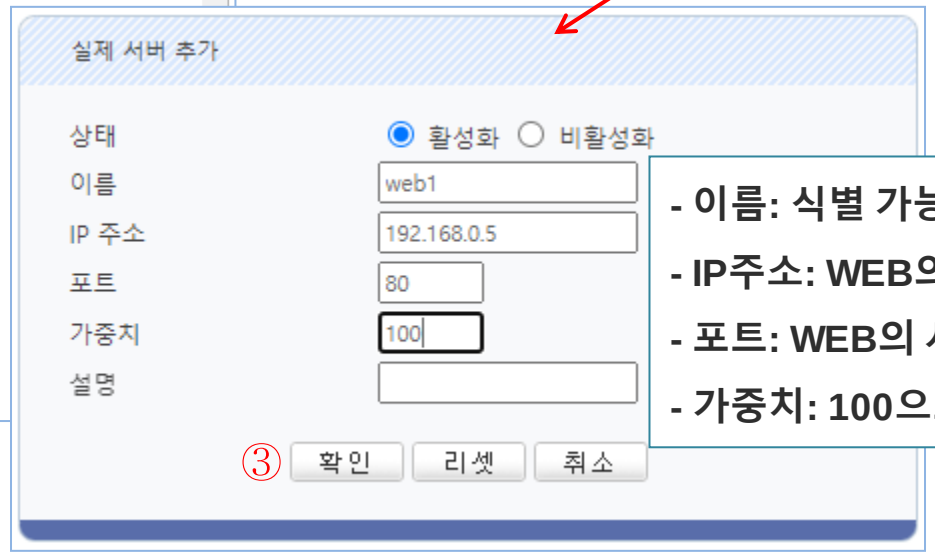
4. 부하분산 – 실제 서버 설정

- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)
  - 설정 경로: Application > 부하분산 > 실제서버



실제 서버

- WAF가 트래픽을 포워딩할 WEB의 IP/Port를 입력 (다수 입력 가능)



- 이름: 식별 가능한 임의의 이름 입력

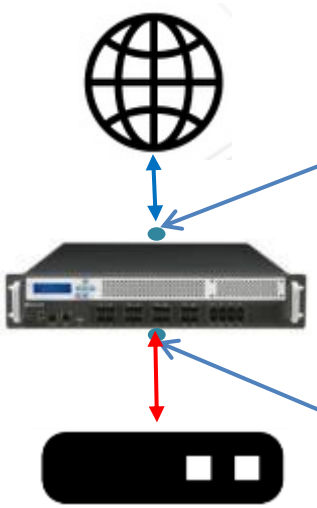
- IP주소: WEB의 사설 IP주소

- 포트: WEB의 서비스 포트

- 가중치: 100으로 입력

5. 부하분산 – 그룹 설정

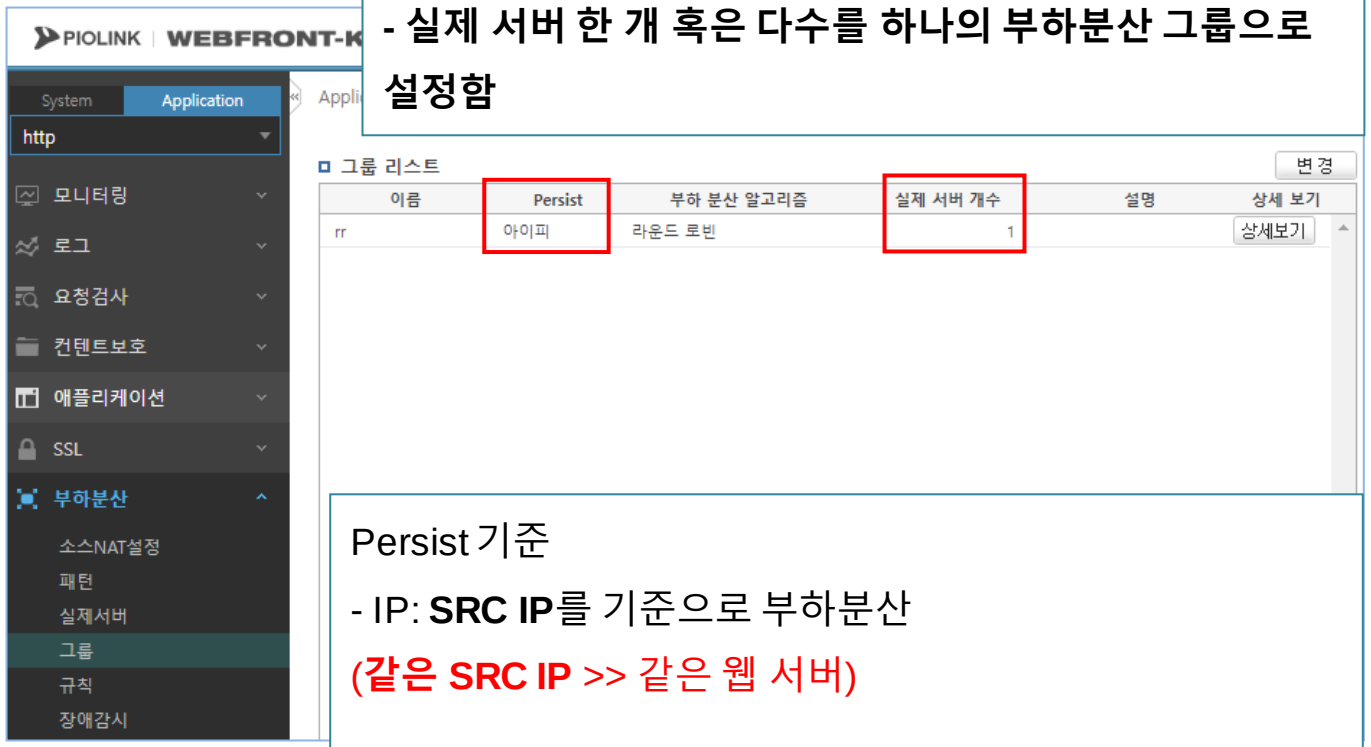
- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)
  - 설정 경로: Application > 부하분산 > 그룹



[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 다수를 하나의 부하분산 그룹으로 설정함



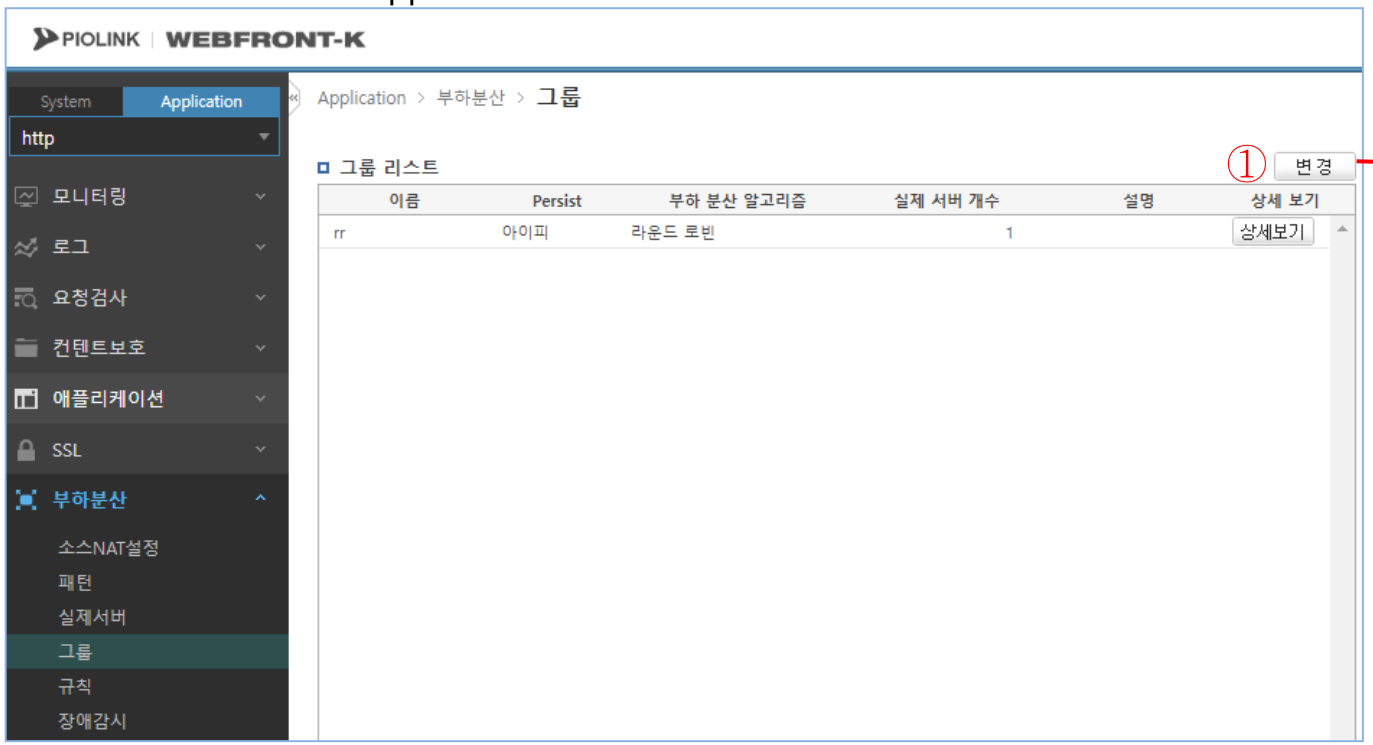
Persist 기준
- IP: **SRC IP**를 기준으로 부하분산
(**같은 SRC IP** >> 같은 웹 서버)

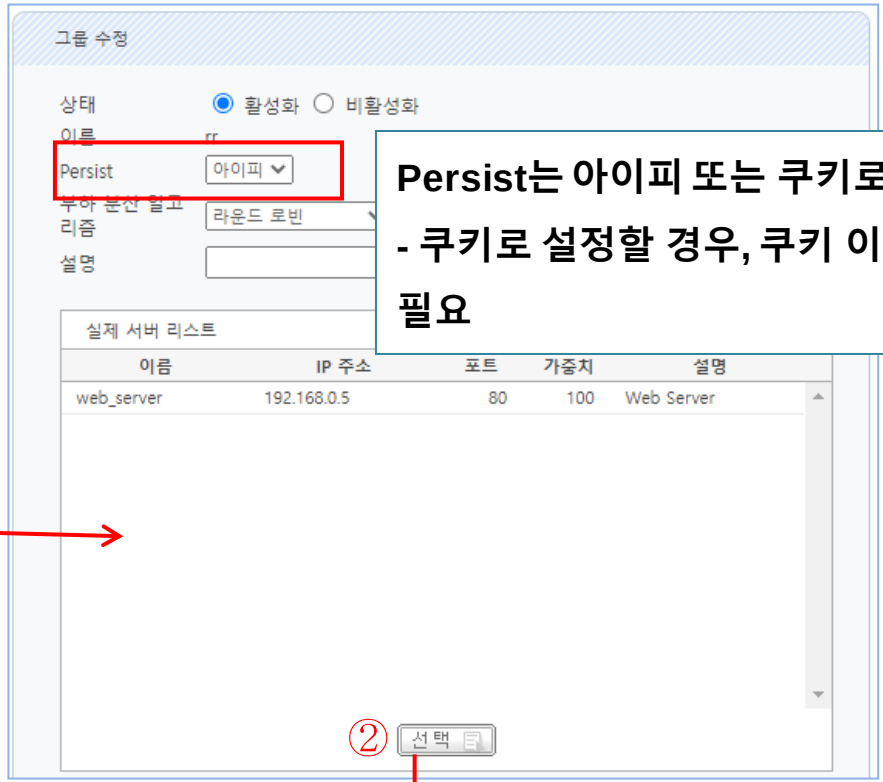
- 쿠키: 세션 맺을 때 http 쿠키 생성 후 해당 **쿠키**를 기준으로 부하분산
(**같은 쿠키** >> 같은 웹 서버)

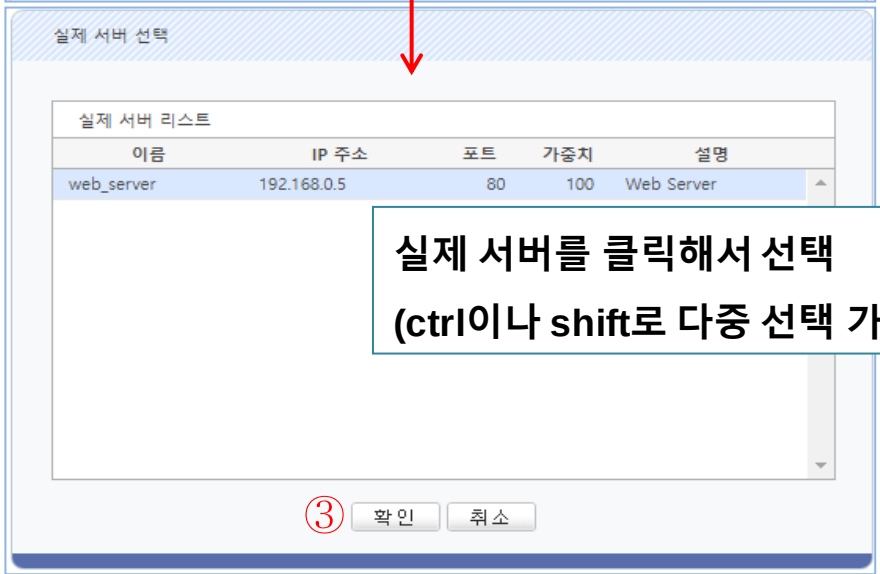
※WEB서버가 다수인 경우에는 반드시 쿠키 persist 설정

5. 부하분산 – 그룹 설정

- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)
  - 설정 경로: Application > 부하분산 > 그룹







Persist는 아이피 또는 쿠키로 설정

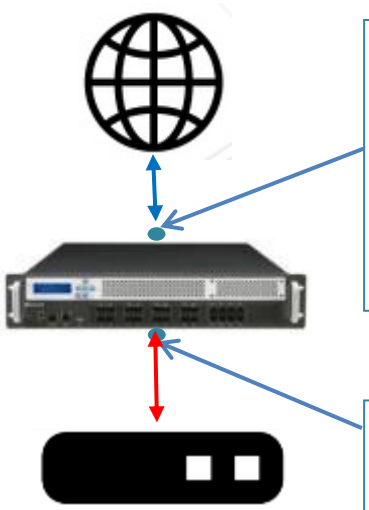
- 쿠키로 설정할 경우, 쿠키 이름 입력 필요

실제 서버를 클릭해서 선택

(ctrl이나 shift로 다중 선택 가능)

6. 부하분산 – 규칙 설정

- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)
  - 설정 경로: Application > 부하분산 > 규칙



[클라이언트 세션]

SRC IP: 클라이언트 IP

DST IP: WAF 서비스 IP/Port

(애플리케이션에서 설정)

[서버 세션]

SRC IP: SNAT IP

(부하분산 - 소스NAT 설정)

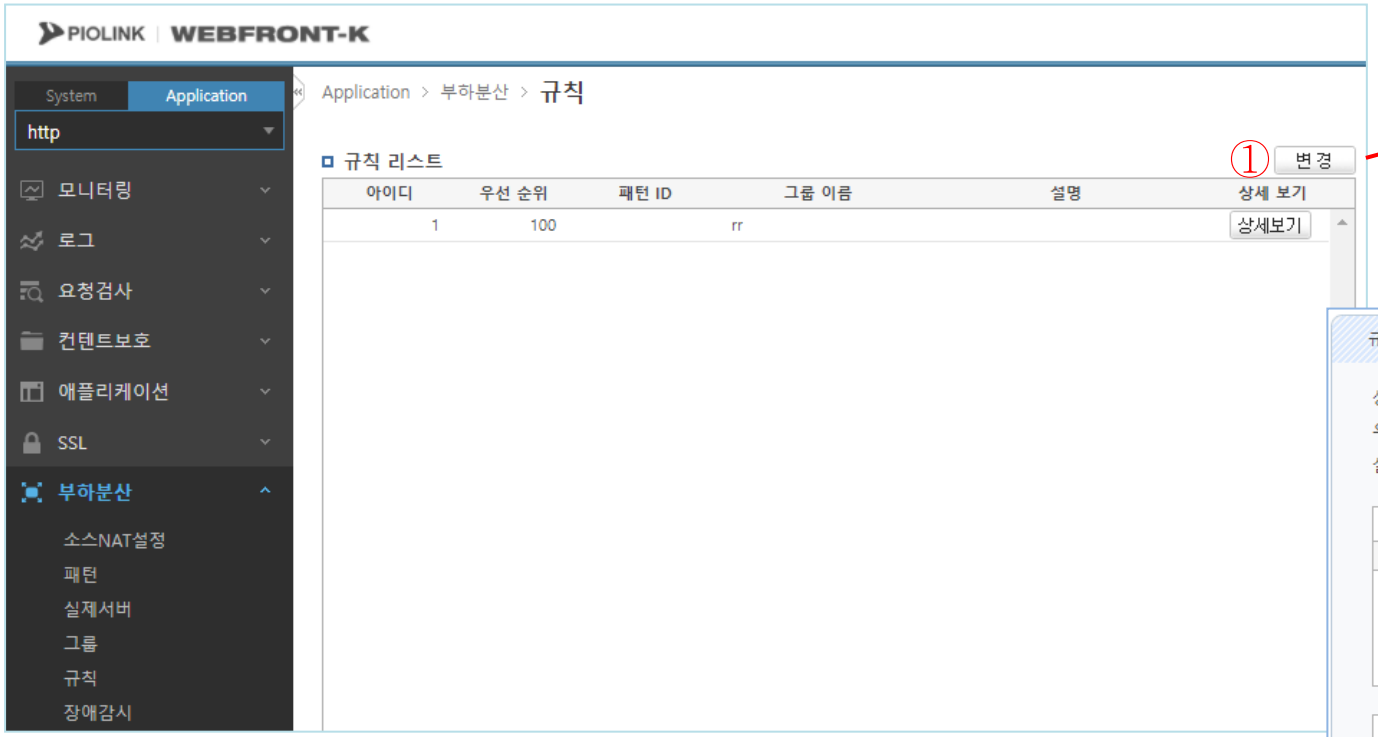
DST IP: 하단 웹 서버 IP/Port

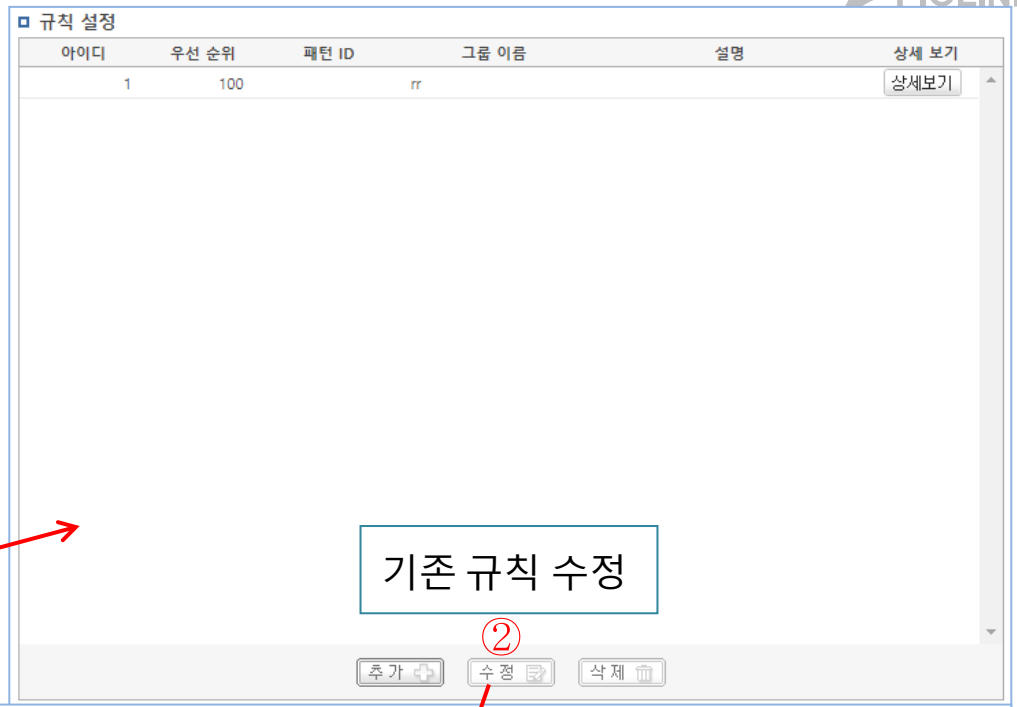
(부하분산 – 실제서버 에서 설정)

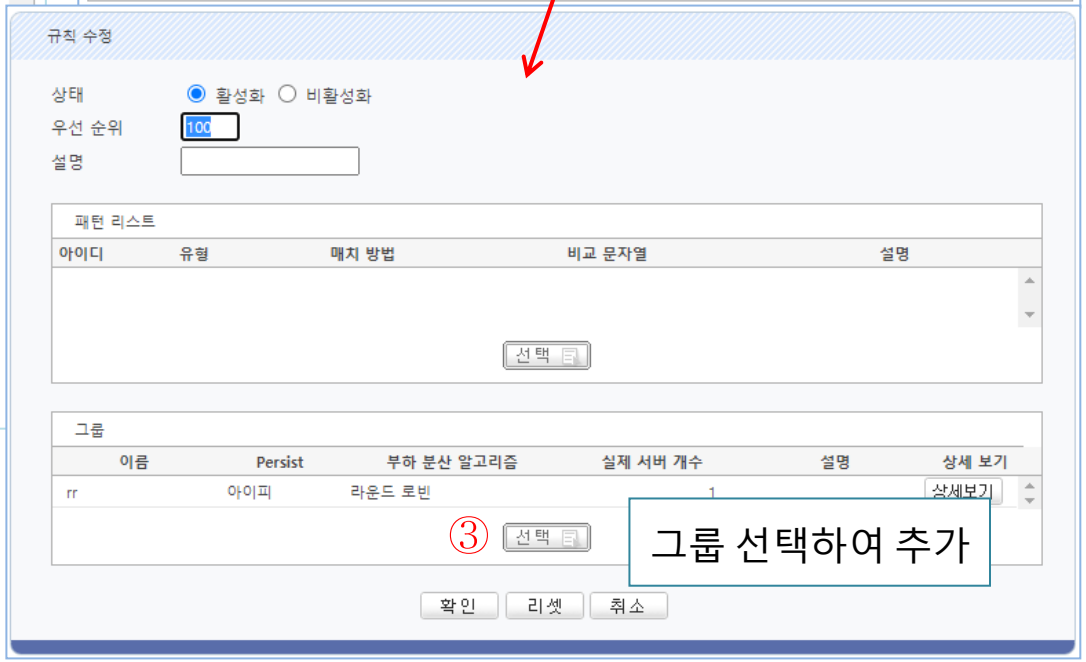
규칙 = 그룹 + 패턴(패턴은 설정하지 않아도 무방함)

6. 부하분산 – 규칙 설정

- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)
  - 설정 경로: Application > 부하분산 > 규칙

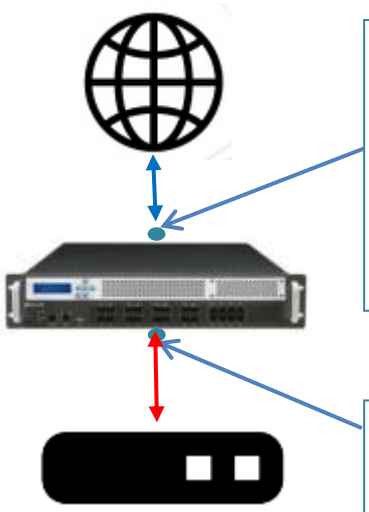






7. 부하분산 – 장애 감시 설정

- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)
  - 설정 경로: Application > 부하분산 > 장애감시



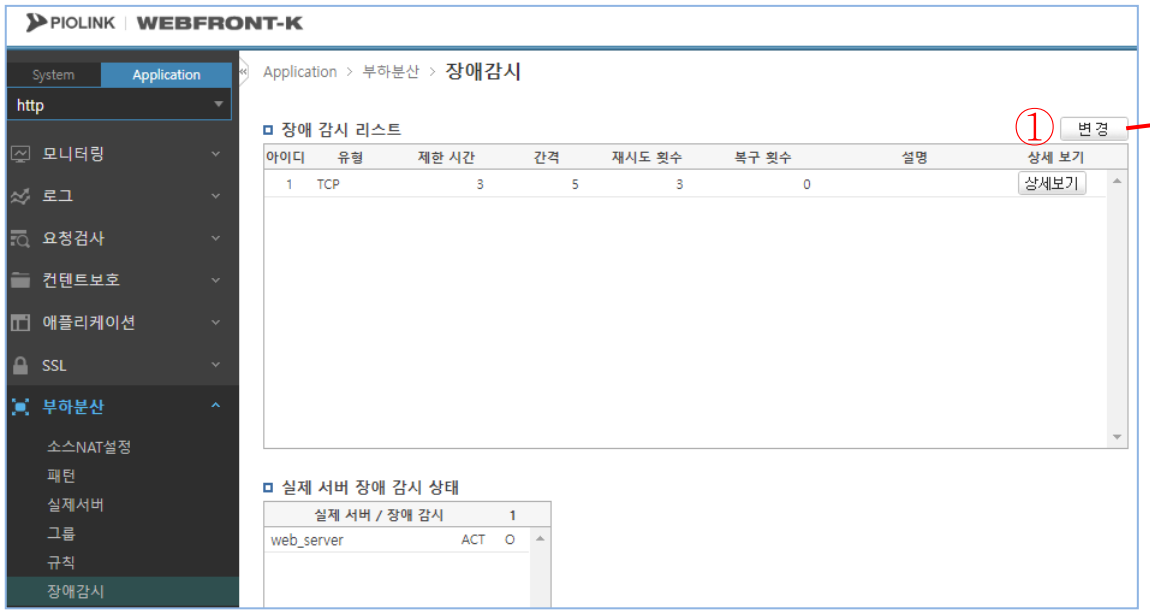
[클라이언트 세션]
SRC IP: 클라이언트 IP
DST IP: WAF 서비스 IP/Port
(애플리케이션에서 설정)

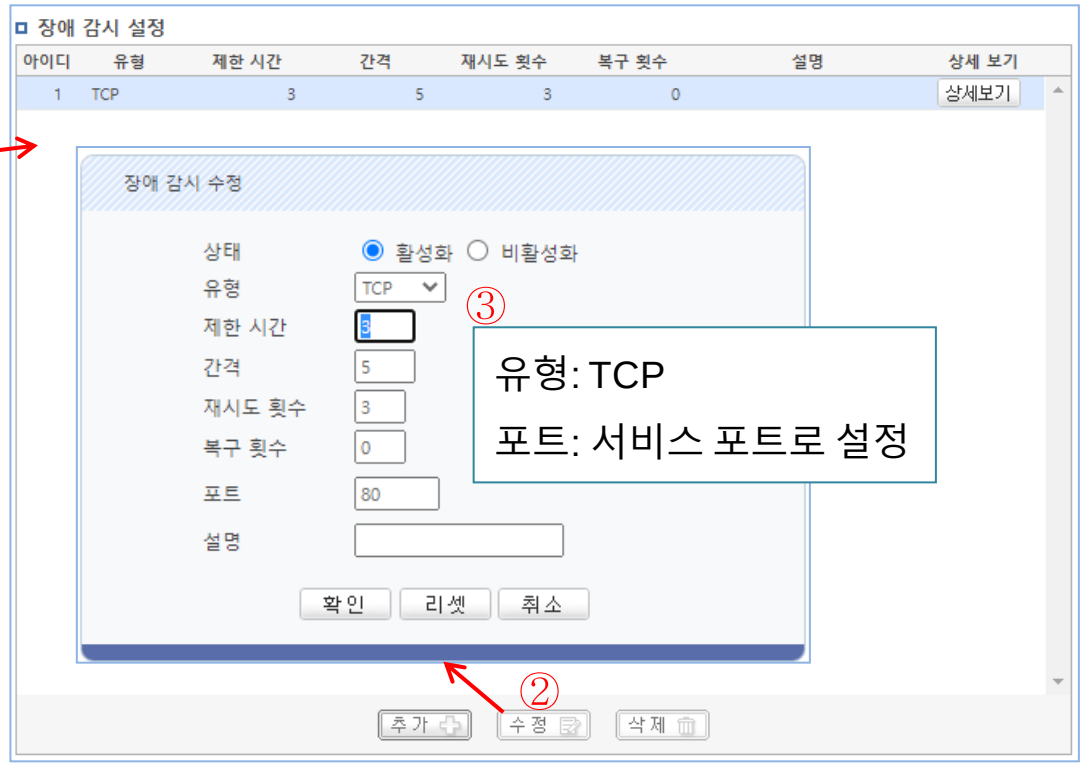
[서버 세션]
SRC IP: SNAT IP
(부하분산 - 소스NAT 설정)
DST IP: 하단 웹 서버 IP/Port
(부하분산 – 실제서버 에서 설정)

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

7. 부하분산 – 장애 감시 설정

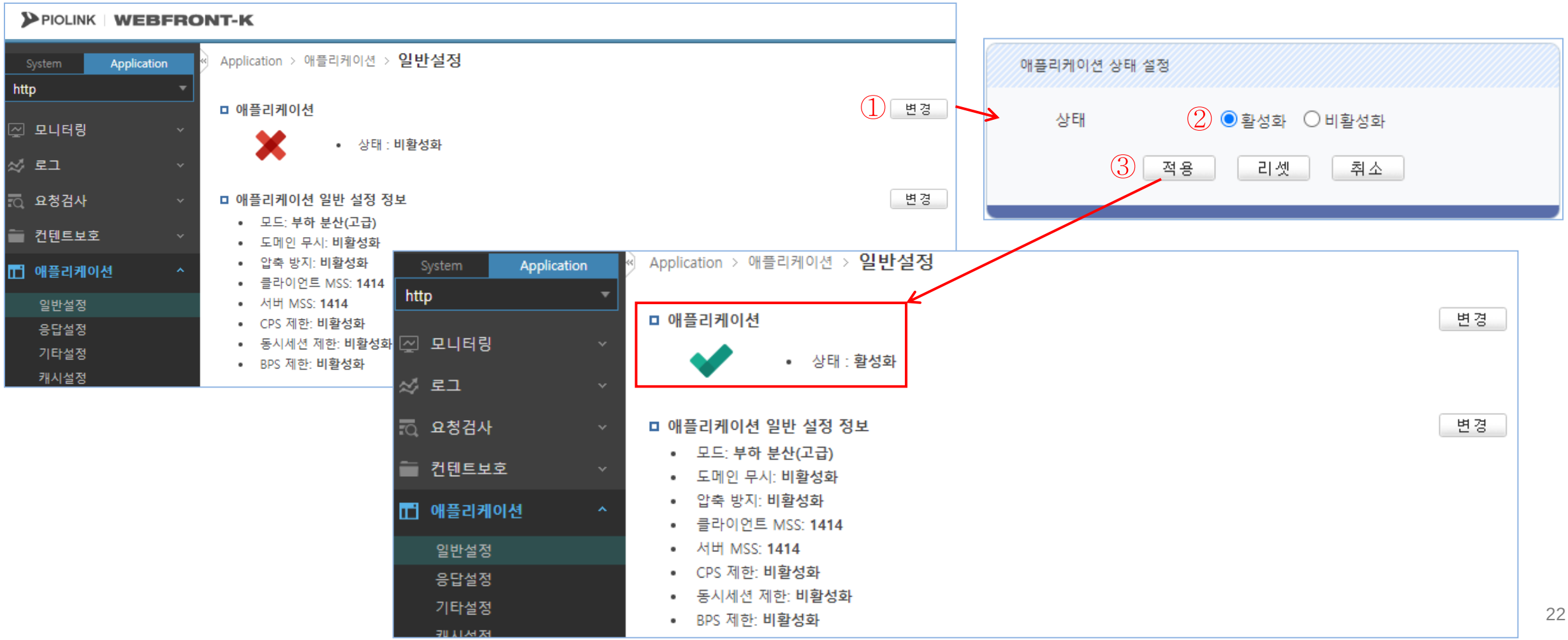
- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)
  - 설정 경로: Application > 부하분산 > 장애감시





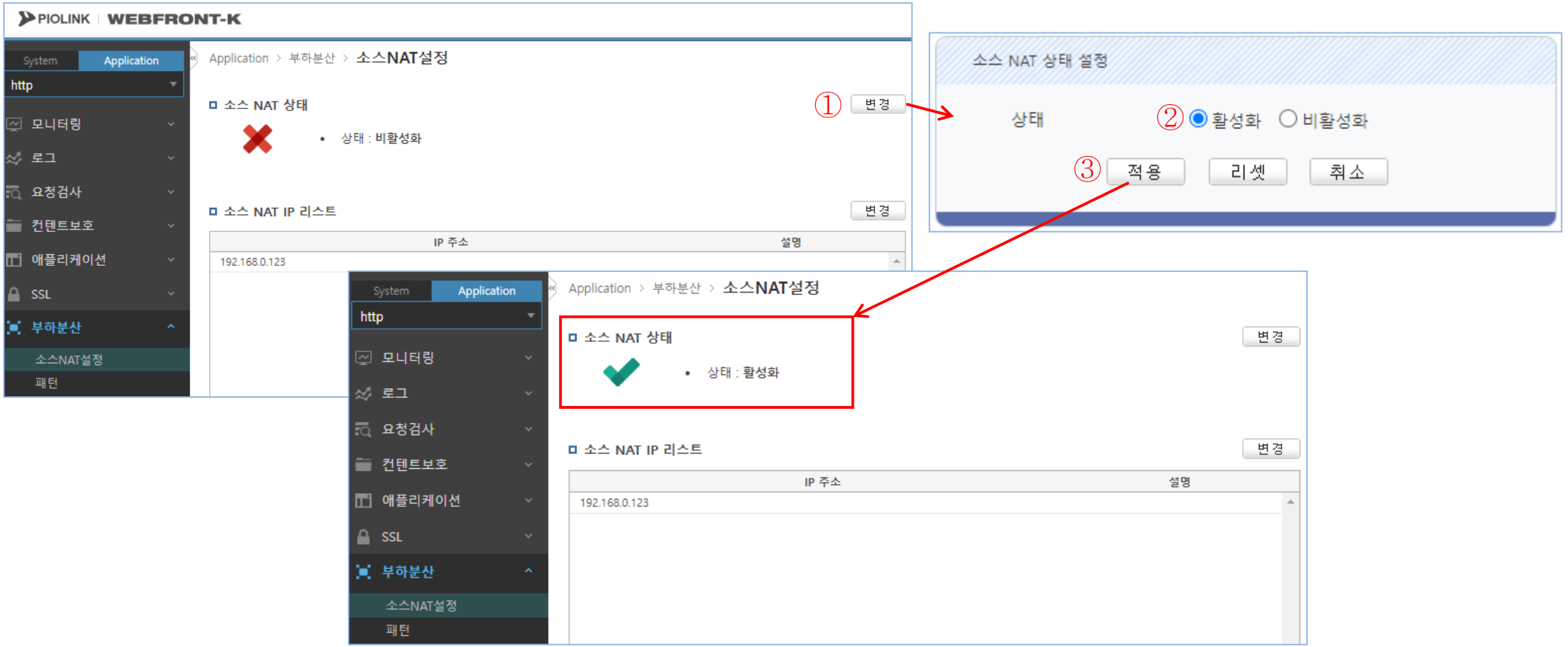
8. 애플리케이션 및 소스 NAT 활성화

- **애플리케이션 활성화**
  - 설정 경로: Application > 애플리케이션 > 일반설정



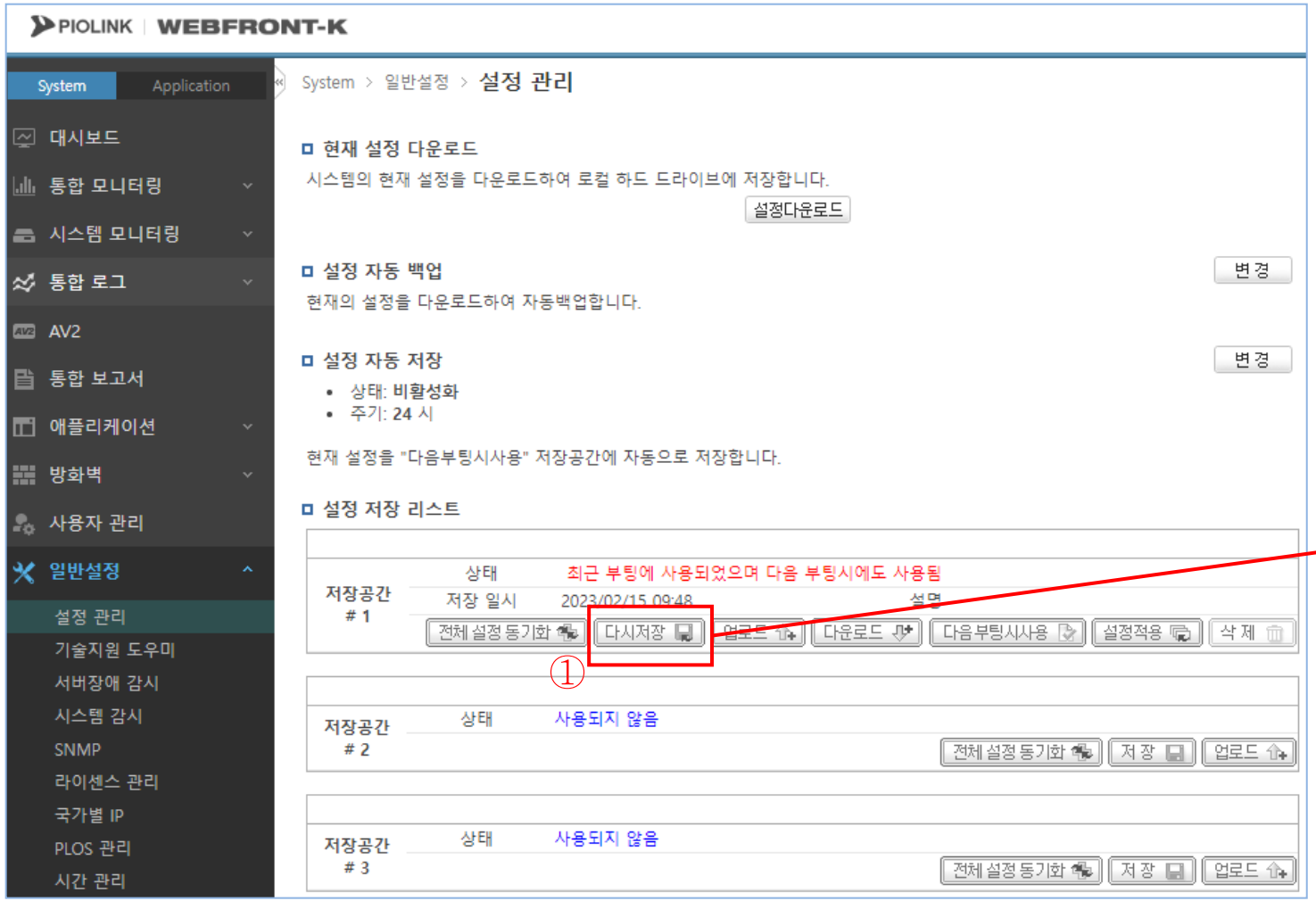
8. 애플리케이션 및 소스 NAT 활성화

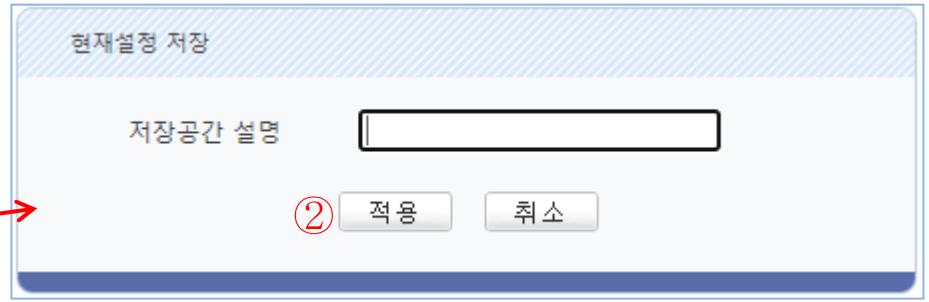
- **소스NAT 활성화**
  - 설정 경로: Application > 부하분산 > 소스NAT설정



9. 설정 저장

- **설정 저장**
  - 설정 경로: System > 일반설정 > 설정 관리





PIOLINK

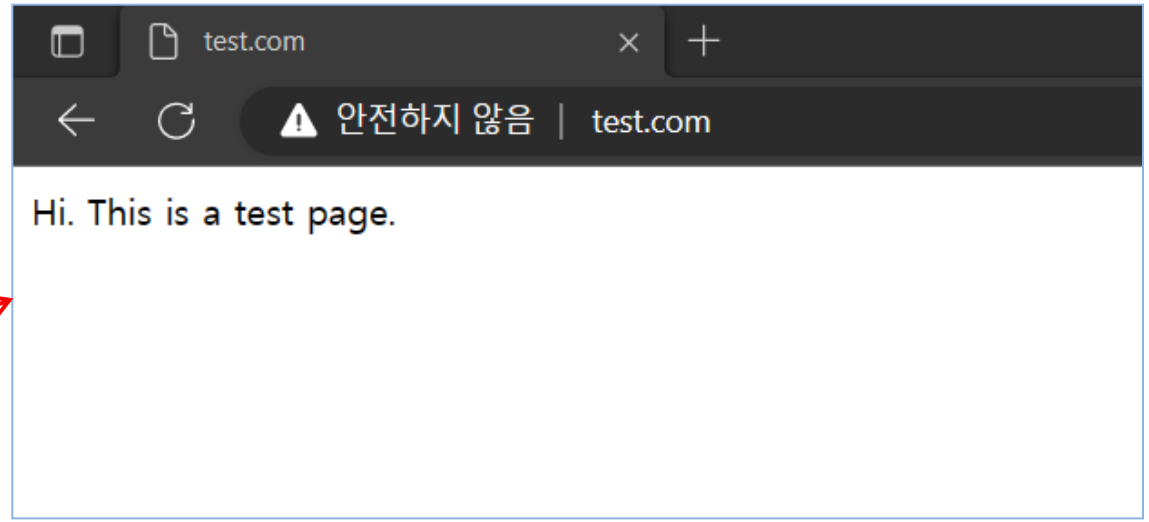
10. 웹 서비스 확인

- **WEBFRONT-KS 설정 완료 후 통신 가능여부 확인**
  - Hosts파일에 서비스 도메인에 대해 웹방화벽의 FIP를 지정해준 후, 웹 브라우저를 통해 웹방화벽을 통해 실제 통신이 가능한지 테스트 진행

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#   127.0.0.1       localhost
#   ::1             localhost

1.1.1.1 test.com
```



PIOLINK

3. HTTPS 서비스 설정

HTTPS 서비스 설정 순서

1. Login
2. 애플리케이션 일반 설정
3. 부하분산 – 소스 NAT 설정
4. 부하분산 – 실제 서버 설정
5. 부하분산 – 그룹 설정
6. 부하분산 – 규칙 설정
7. 부하분산 – 장애 감시 설정
8. SSL 인증서 등록
9. SSL 설정
10. SSL, 애플리케이션 및 SNAT 활성화
11. 설정 저장
12. 웹 서비스 확인

1. Login

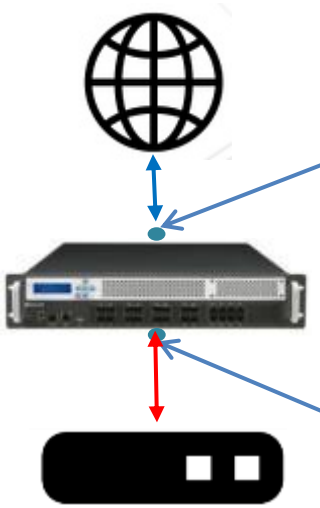
- **WEBFRONT-KS 로그인**
  - 웹UI 접속 경로: **https://{웹방화벽 FIP}:8443**
  - 계정: wfadmin // 비밀번호: waf12!@{인스턴스 이름 첫 5글자}
    - 만약 인스턴스의 이름이 5글자 미만이라면, 인스턴스 이름 전체를 입력 (대소문자 구별 필요)
    - 인스턴스 이름에 특수문자 및 숫자가 포함되어 있더라도 그대로 입력

PIOLINK

2. 애플리케이션 일반 설정

WAF에서 처리할 도메인 및 상단으로부터 트래픽을 받아들이는 IP/Port를 설정함

- **WEBFRONT-KS 기본 구성**
  - 클라이언트 세션 관련 설정(애플리케이션)
  - 설정 경로: Application > 애플리케이션 > 일반설정



[클라이언트 세션]

SRC IP: 클라이언트 IP

DST IP: WAF 서비스 IP/Port

(애플리케이션에서 설정)

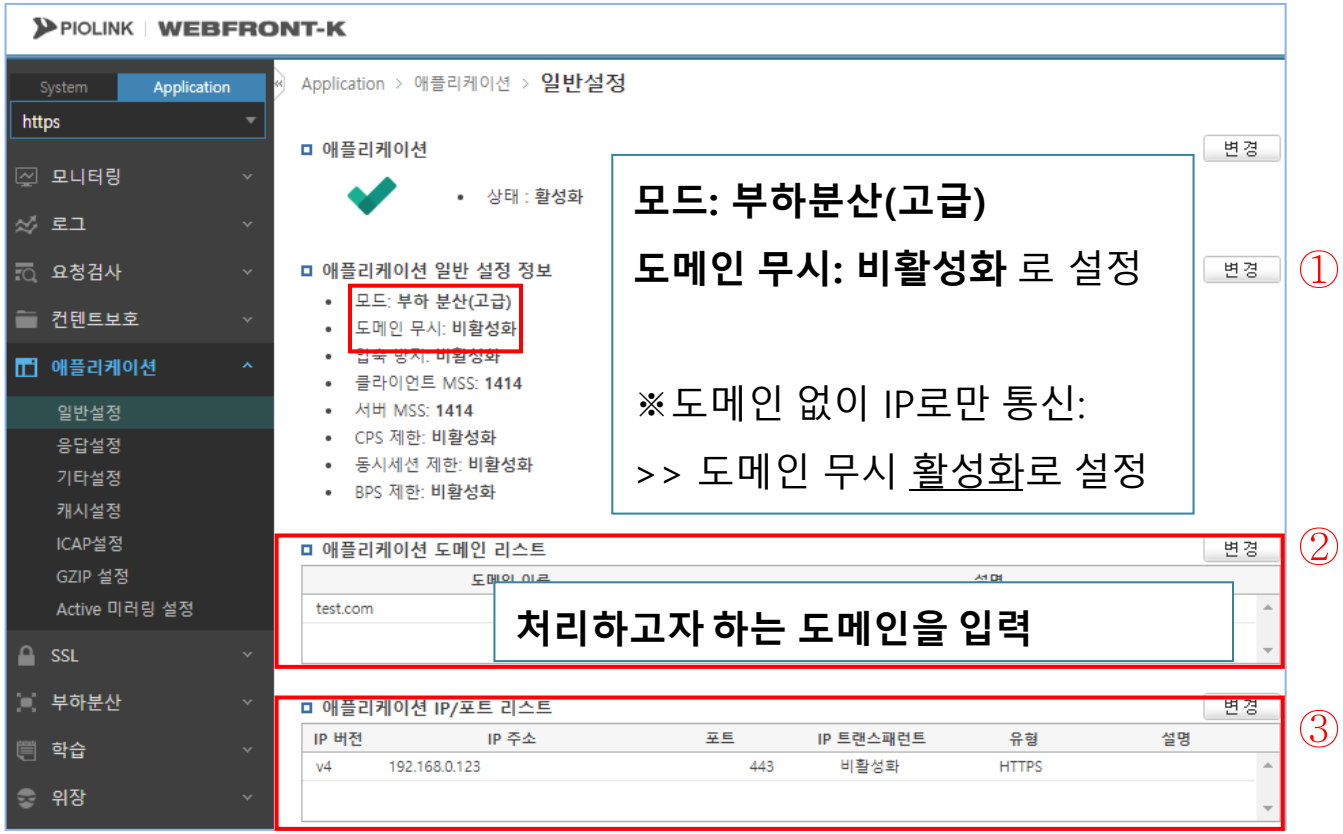
[서버 세션]

SRC IP: SNAT IP

(부하분산 - 소스NAT 설정)

DST IP: 하단 웹 서버 IP/Port

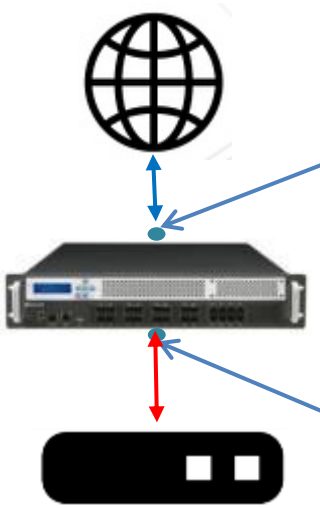
(부하분산 – 실제서버 에서 설정)



서비스용 IP/Port 입력 (웹방화벽의 사설 IP)

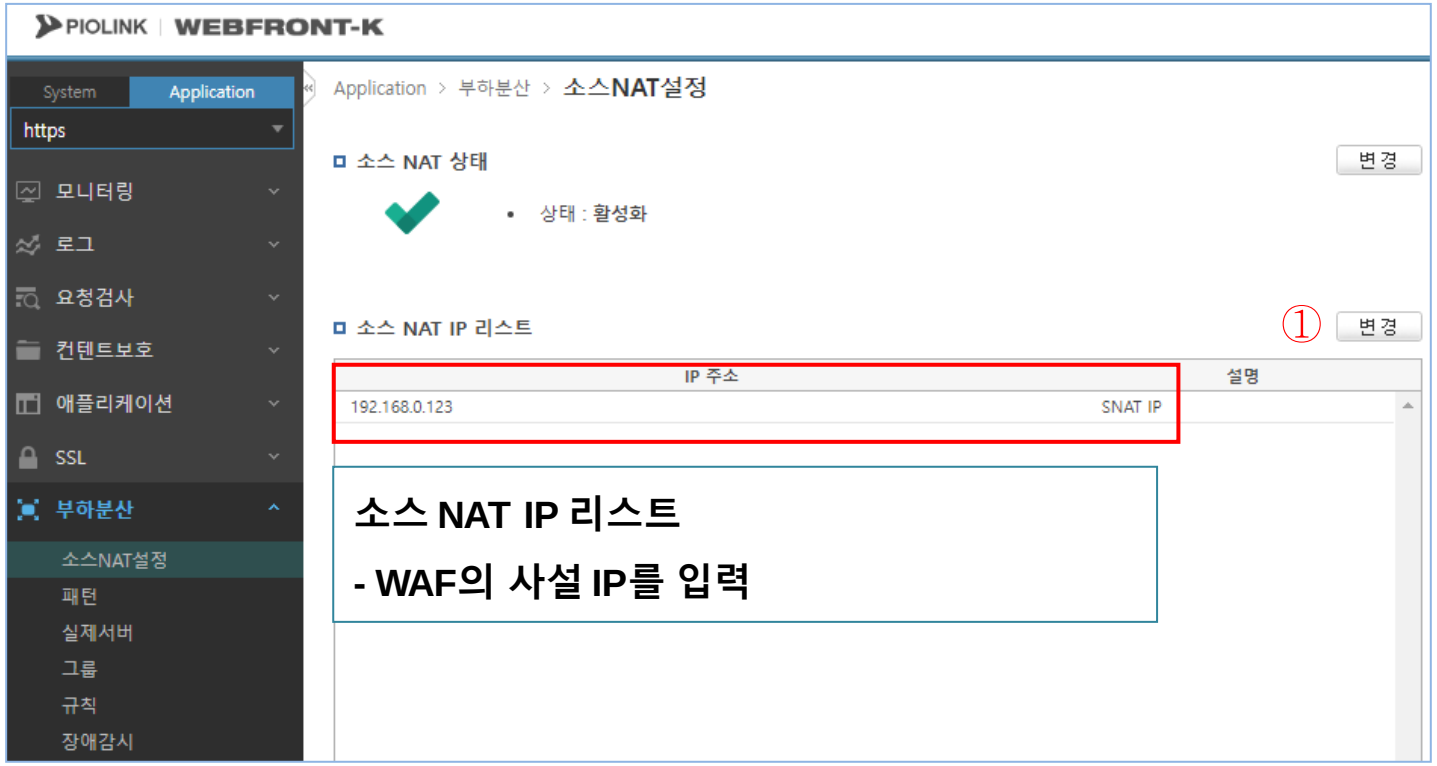
3. 부하분산 – 소스 NAT 설정

- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)
  - 설정 경로: Application > 부하분산 > 소스NAT설정



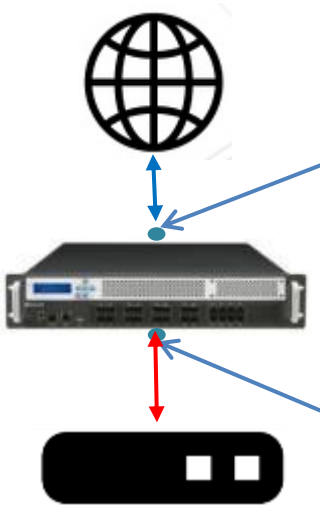
[클라이언트 세션]
SRC IP: 클라이언트 IP
DST IP: WAF 서비스 IP/Port
(애플리케이션에서 설정)

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



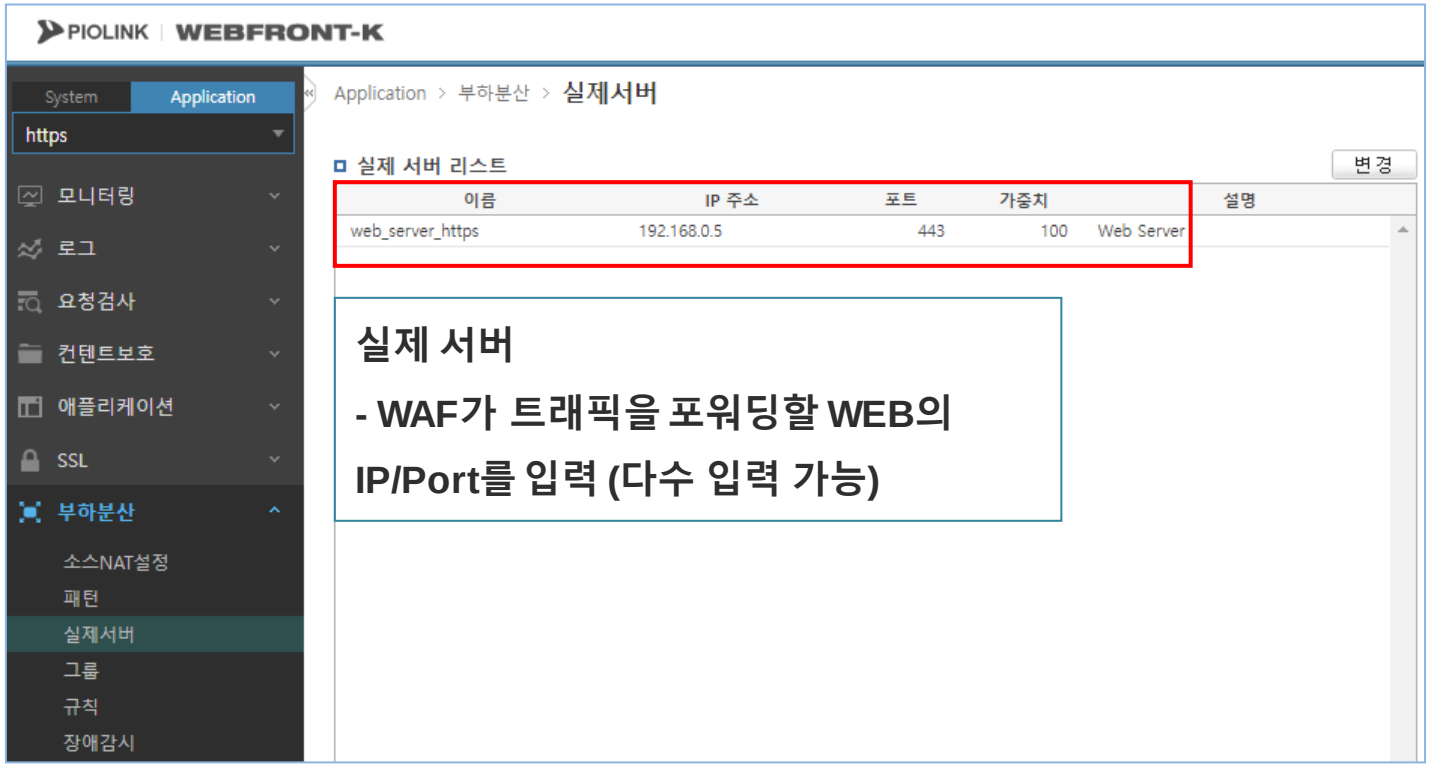
4. 부하분산 – 실제 서버 설정

- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)
  - 설정 경로: Application > 부하분산 > 실제서버



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

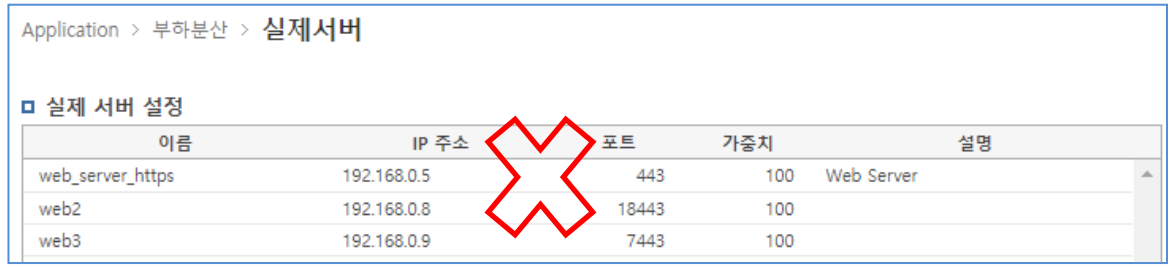
[서버 세션]
SRC IP: SNAT IP
(부하분산 - 소스NAT 설정)
DST IP: 하단 웹 서버 IP/Port
(부하분산 – 실제서버 에서 설정)



PIOLINK

4. 부하분산 – 실제 서버 설정

- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)
  - 설정 경로: Application > 부하분산 > 실제서버



실제 서버

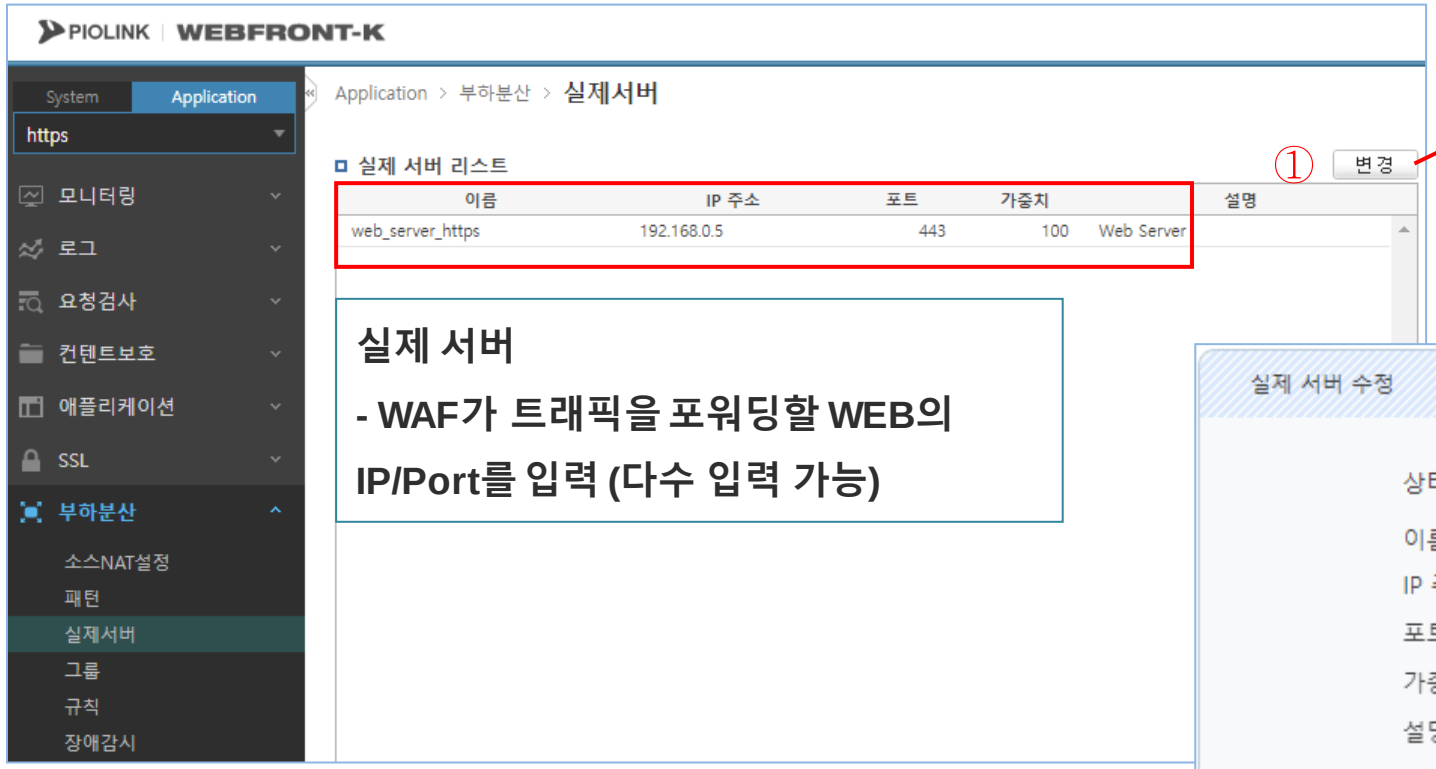
- 실제 서버는 부하 분산을 위한 서버 리스트임

>> 그러므로 다수의 WEB서버를 등록할 때에는 같은 Port를 사용하면서 같은 서비스를 수행하는 다수의 서버만 등록

PIOLINK

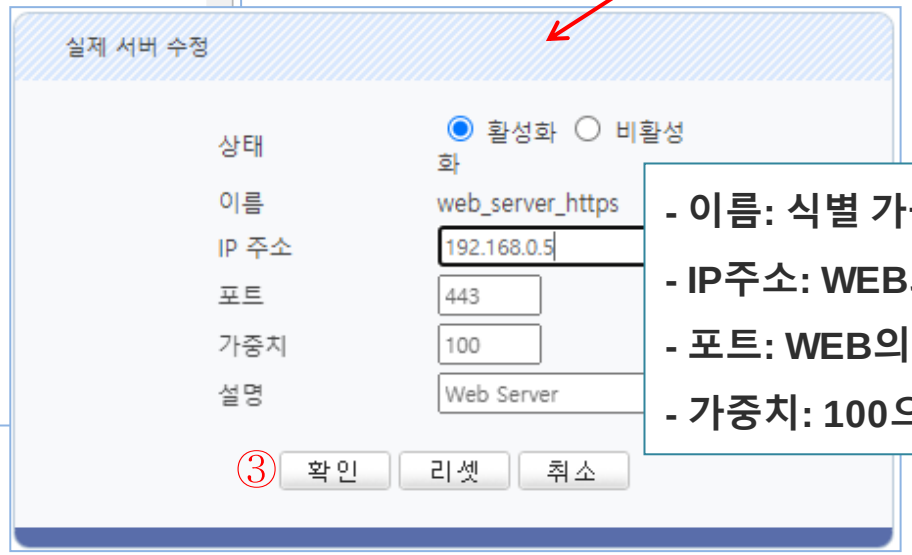
4. 부하분산 – 실제 서버 설정

- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)
  - 설정 경로: Application > 부하분산 > 실제서버



실제 서버

- WAF가 트래픽을 포워딩할 WEB의 IP/Port를 입력 (다수 입력 가능)



- 이름: 식별 가능한 임의의 이름 입력

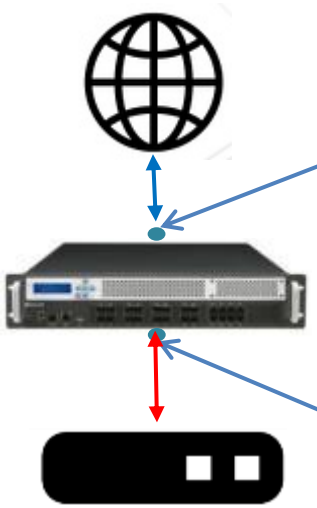
- IP주소: WEB의 사설 IP주소

- 포트: WEB의 서비스 포트

- 가중치: 100으로 입력

5. 부하분산 – 그룹 설정

- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)
  - 설정 경로: Application > 부하분산 > 그룹



[클라이언트 세션]

SRC IP: 클라이언트 IP

DST IP: WAF 서비스 IP/Port

(애플리케이션에서 설정)

[서버 세션]

SRC IP: SNAT IP

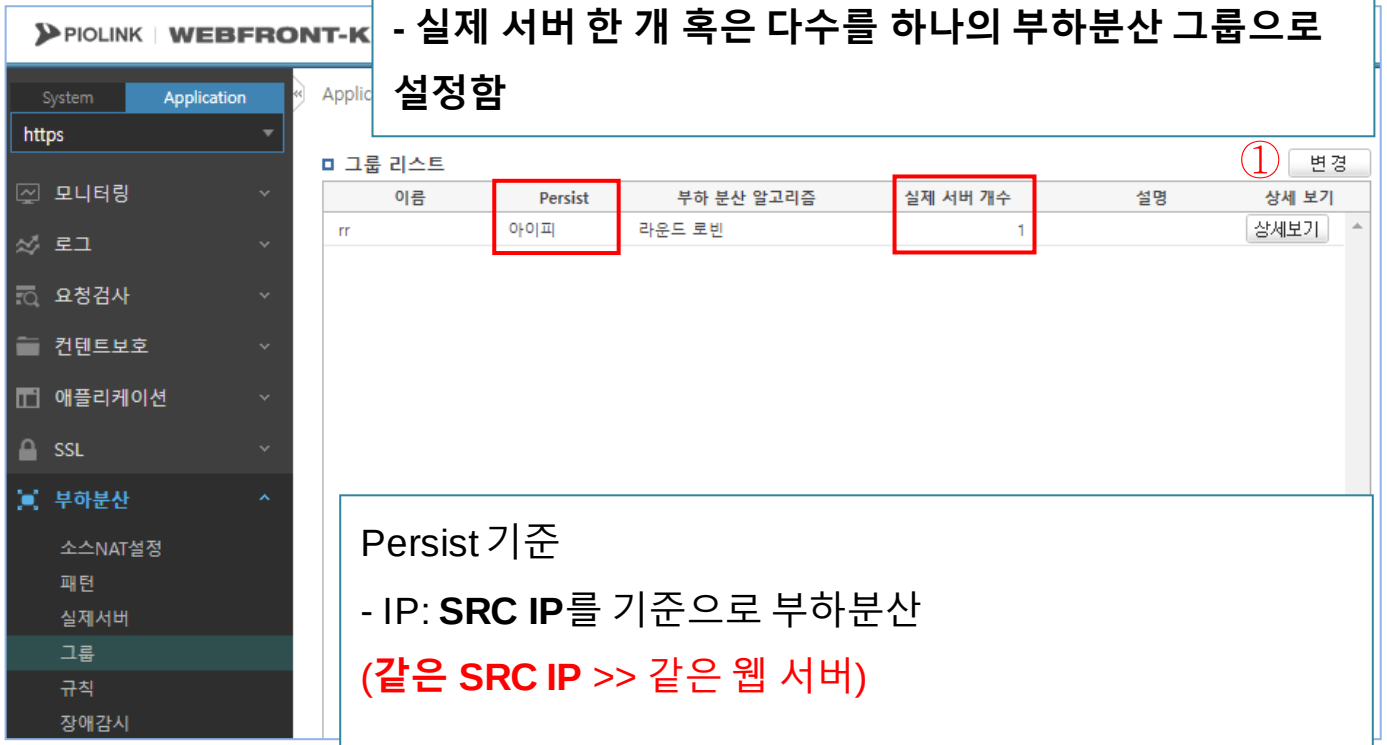
(부하분산 - 소스NAT 설정)

DST IP: 하단 웹 서버 IP/Port

(부하분산 – 실제서버 에서 설정)

그룹

- 실제 서버 한 개 혹은 다수를 하나의 부하분산 그룹으로 설정함



Persist 기준

- IP: **SRC IP**를 기준으로 부하분산

(같은 SRC IP >> 같은 웹 서버)

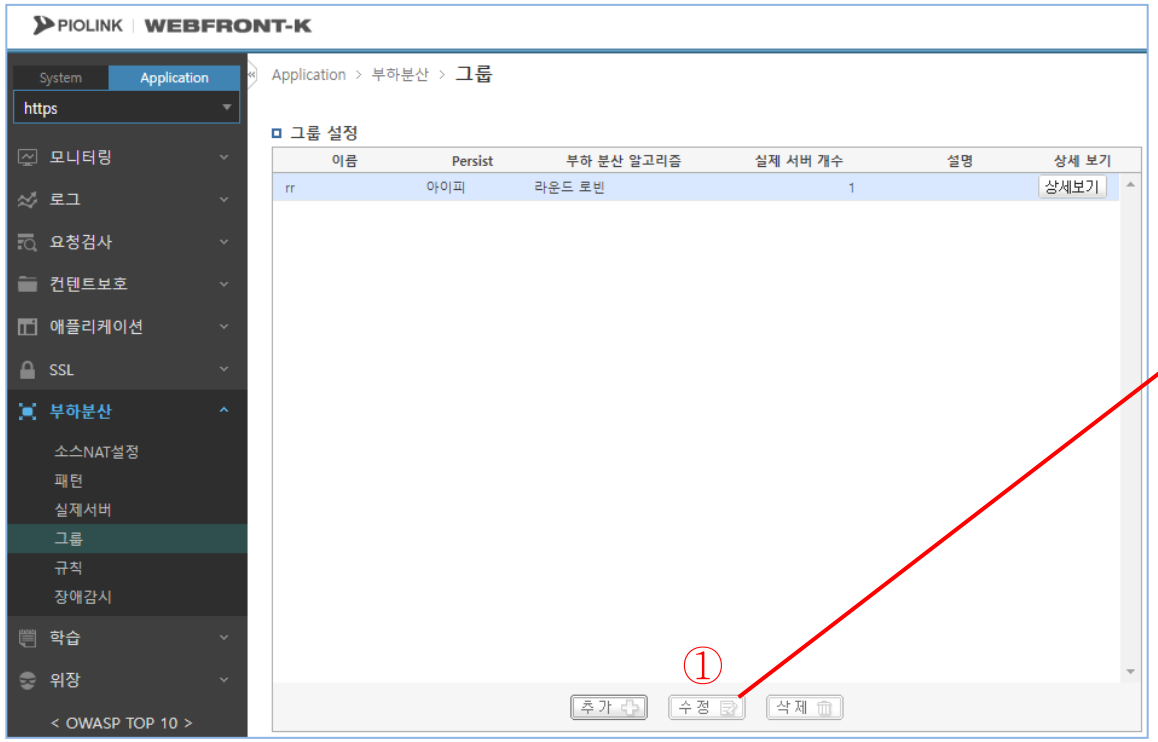
- 쿠키: 세션 맺을 때 http 쿠키 생성 후 해당 **쿠키**를 기준으로 부하분산

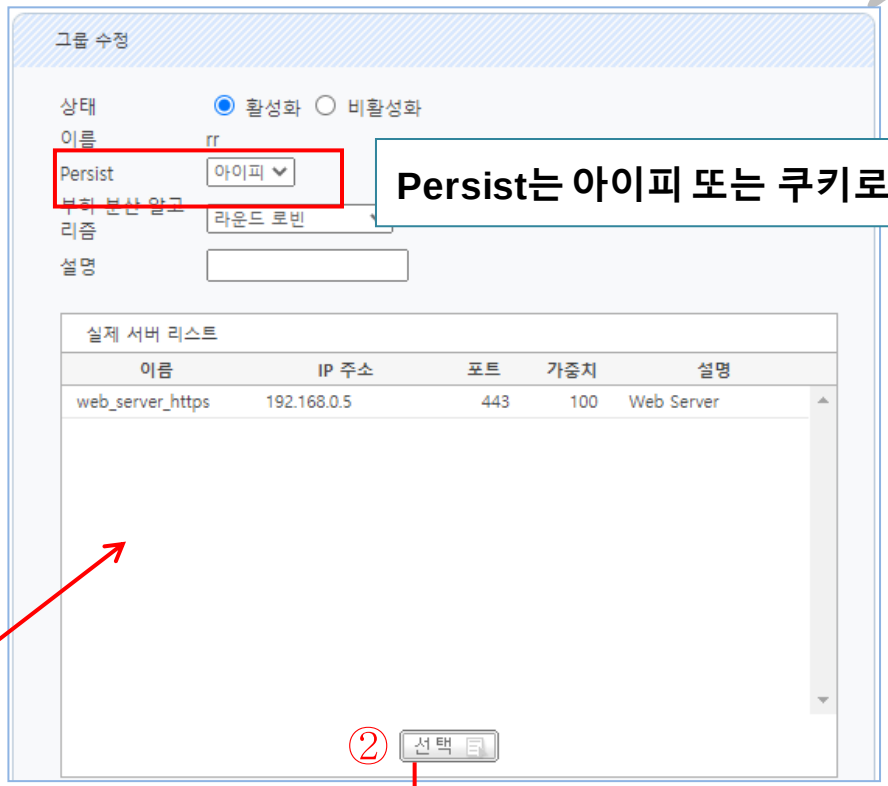
(같은 쿠키 >> 같은 웹 서버)

※WEB서버가 다수인 경우에는 반드시 쿠키 persist 설정

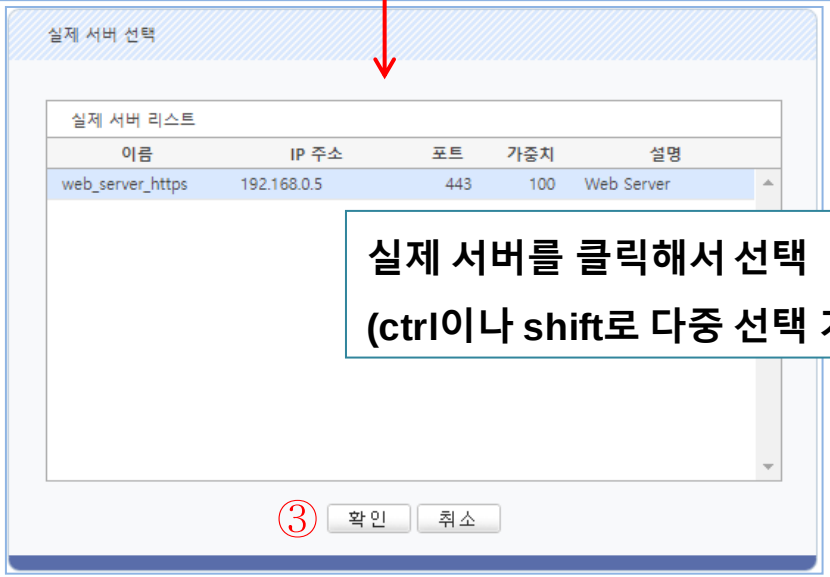
5. 부하분산 – 그룹 설정

- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)
  - 설정 경로: Application > 부하분산 > 그룹





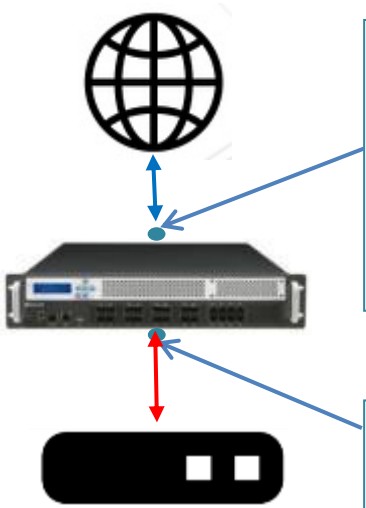
Persist는 아이피 또는 쿠키로 설정



실제 서버를 클릭해서 선택
(ctrl이나 shift로 다중 선택 가능)

6. 부하분산 – 규칙 설정

- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)
  - 설정 경로: Application > 부하분산 > 규칙



[클라이언트 세션]

SRC IP: 클라이언트 IP

DST IP: WAF 서비스 IP/Port

(애플리케이션에서 설정)

[서버 세션]

SRC IP: SNAT IP

(부하분산 - 소스NAT 설정)

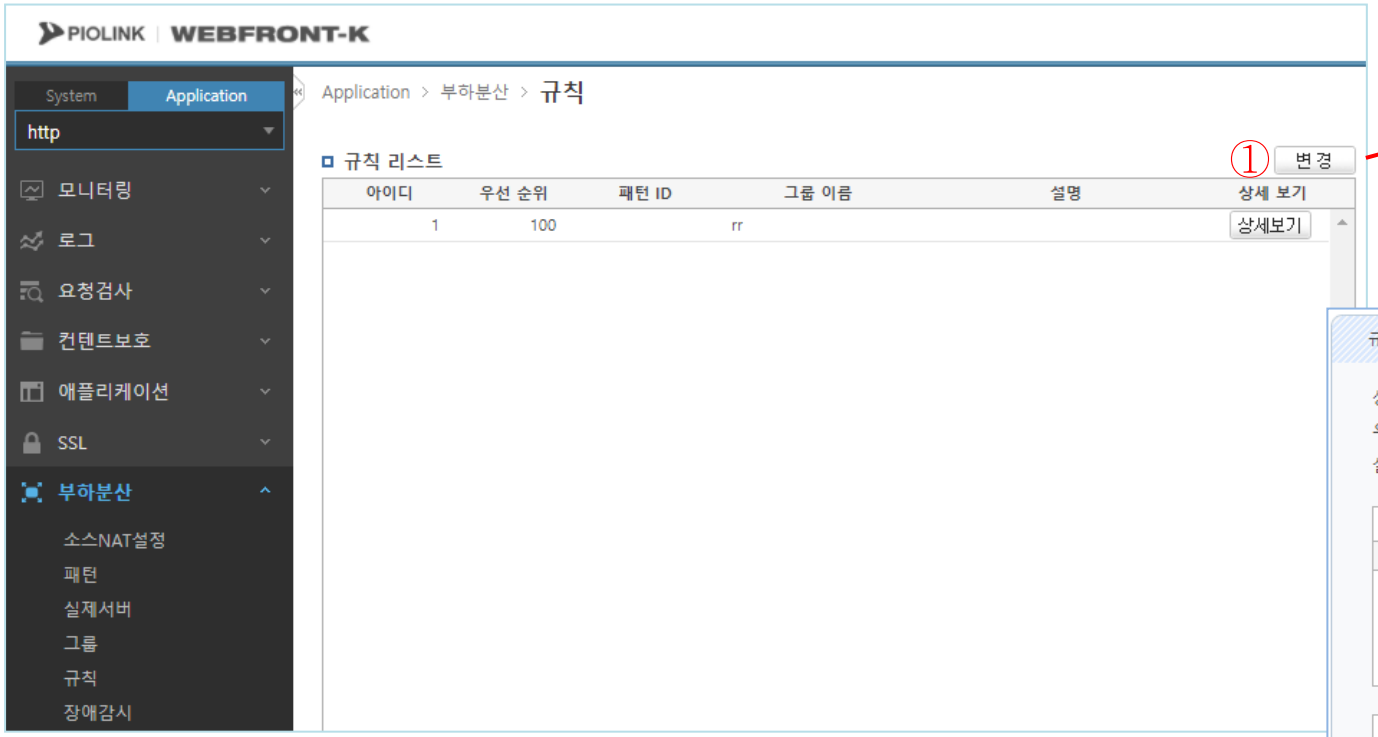
DST IP: 하단 웹 서버 IP/Port

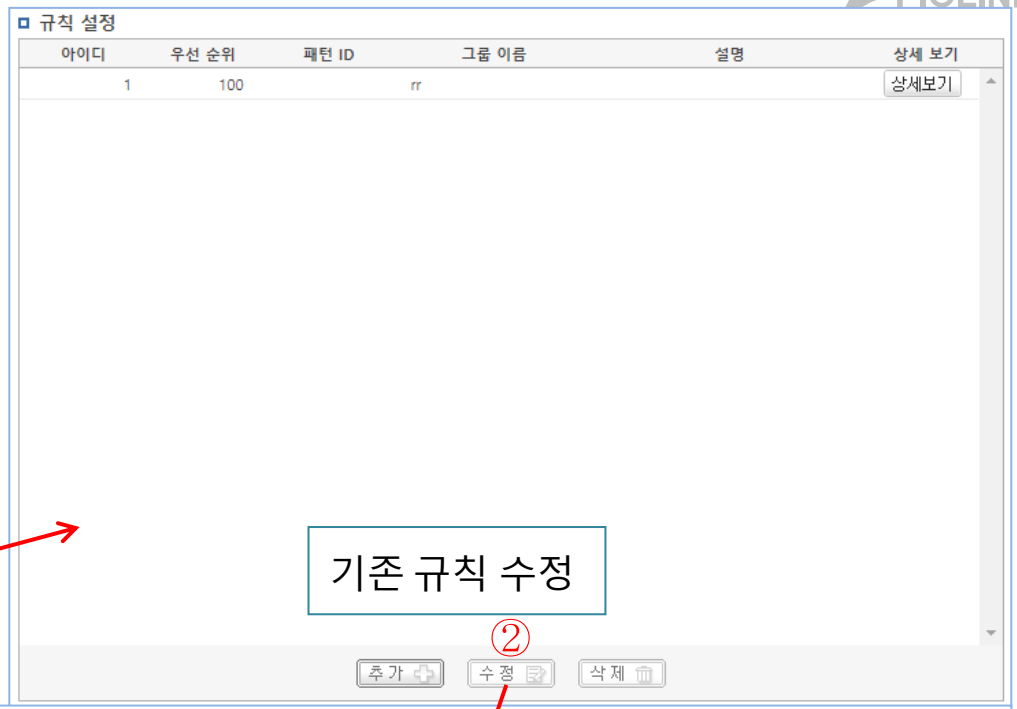
(부하분산 – 실제서버 에서 설정)

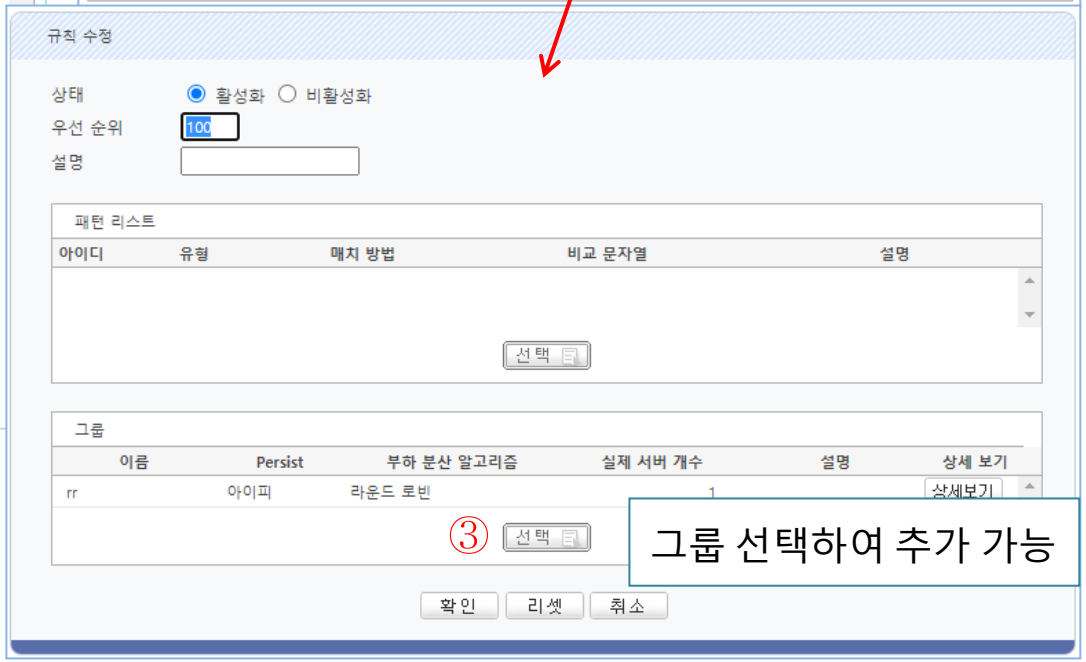
규칙 = 그룹 + 패턴(패턴은 설정하지 않아도 무방함)

6. 부하분산 – 규칙 설정

- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)
  - 설정 경로: Application > 부하분산 > 규칙

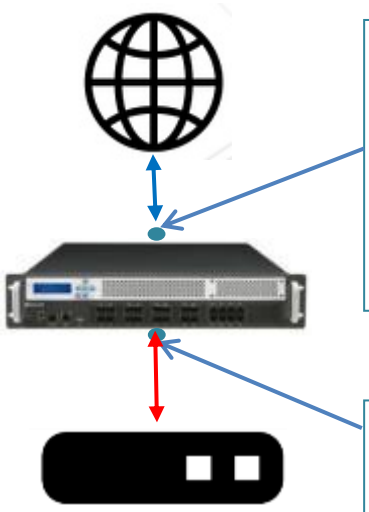






7. 부하분산 – 장애 감시 설정

- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)
  - 설정 경로: Application > 부하분산 > 장애감시



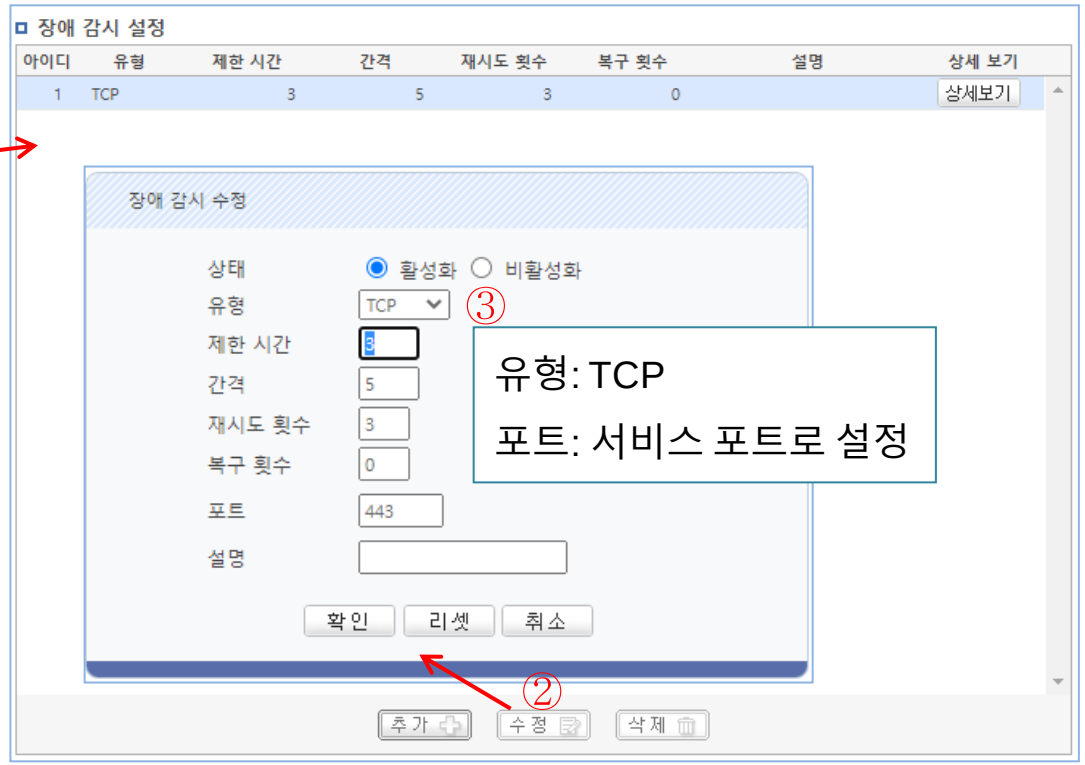
[클라이언트 세션]
SRC IP: 클라이언트 IP
DST IP: WAF 서비스 IP/Port
(애플리케이션에서 설정)

[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

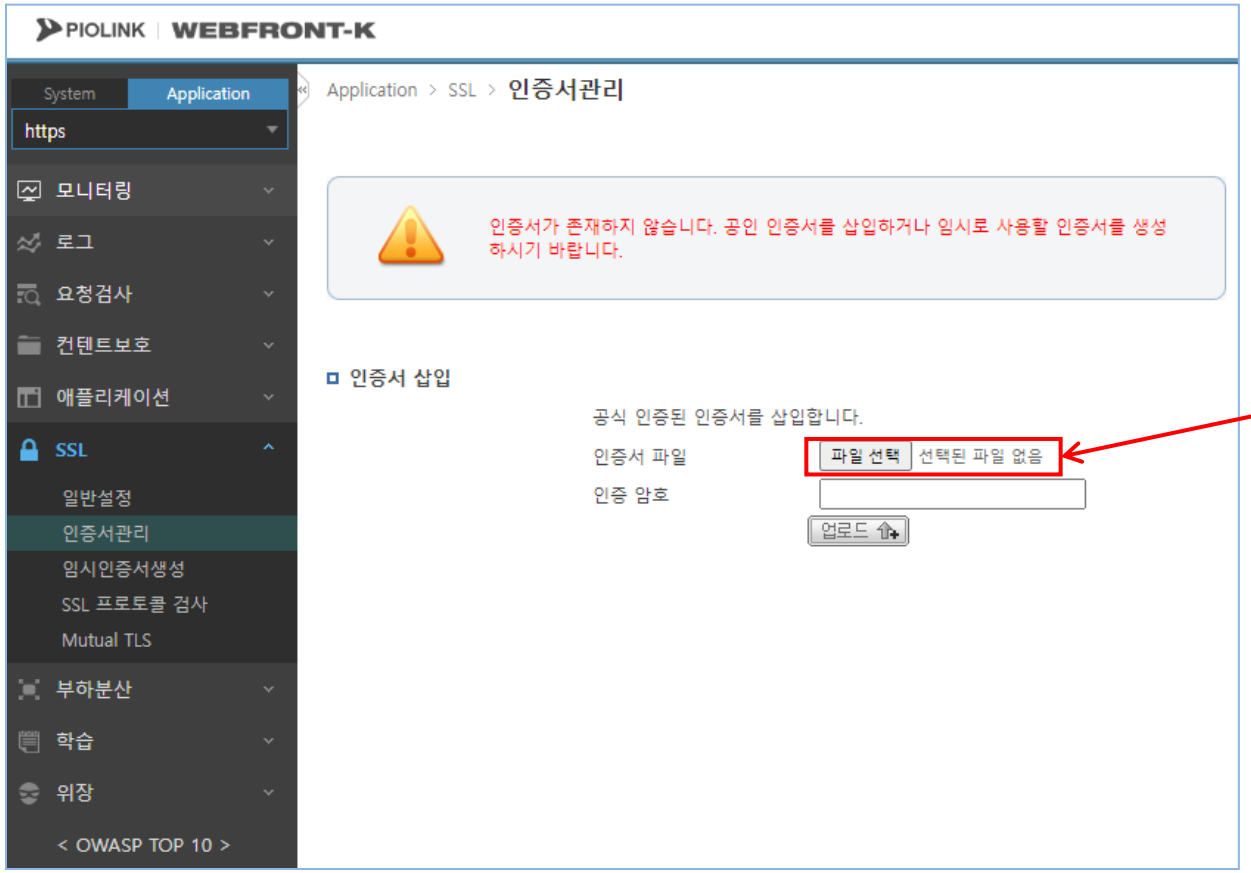
7. 부하분산 – 장애 감시 설정

- **WEBFRONT-KS 기본 구성**
  - 서버 세션 관련 설정(부하분산)
  - 설정 경로: Application > 부하분산 > 장애감시



8. SSL 인증서 등록

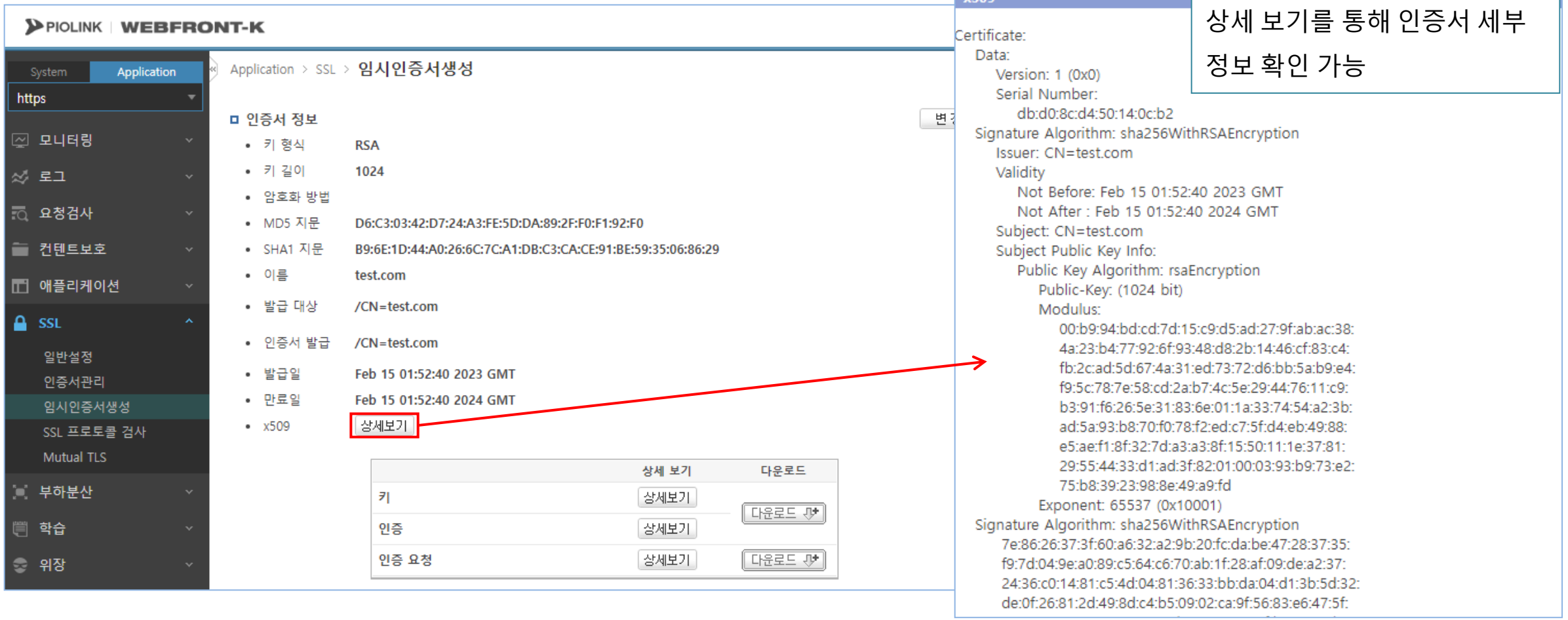
- **SSL 인증서 등록**
  - 설정 경로: Application > SSL > 인증서 관리



개인 키파일, 인증서를 복사/붙여넣기를 통해 아래의 순서대로 하나의 파일로 합친 후 업로드

8. SSL 인증서 등록

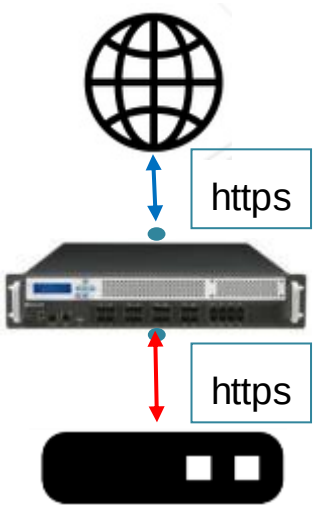
- **SSL 인증서 등록**
  - 설정 경로: Application > SSL > 인증서 관리



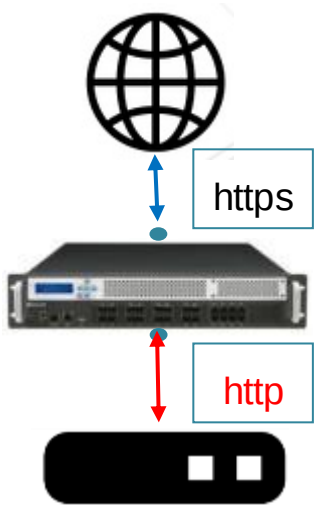
상세 보기를 통해 인증서 세부 정보 확인 가능

9. SSL 설정

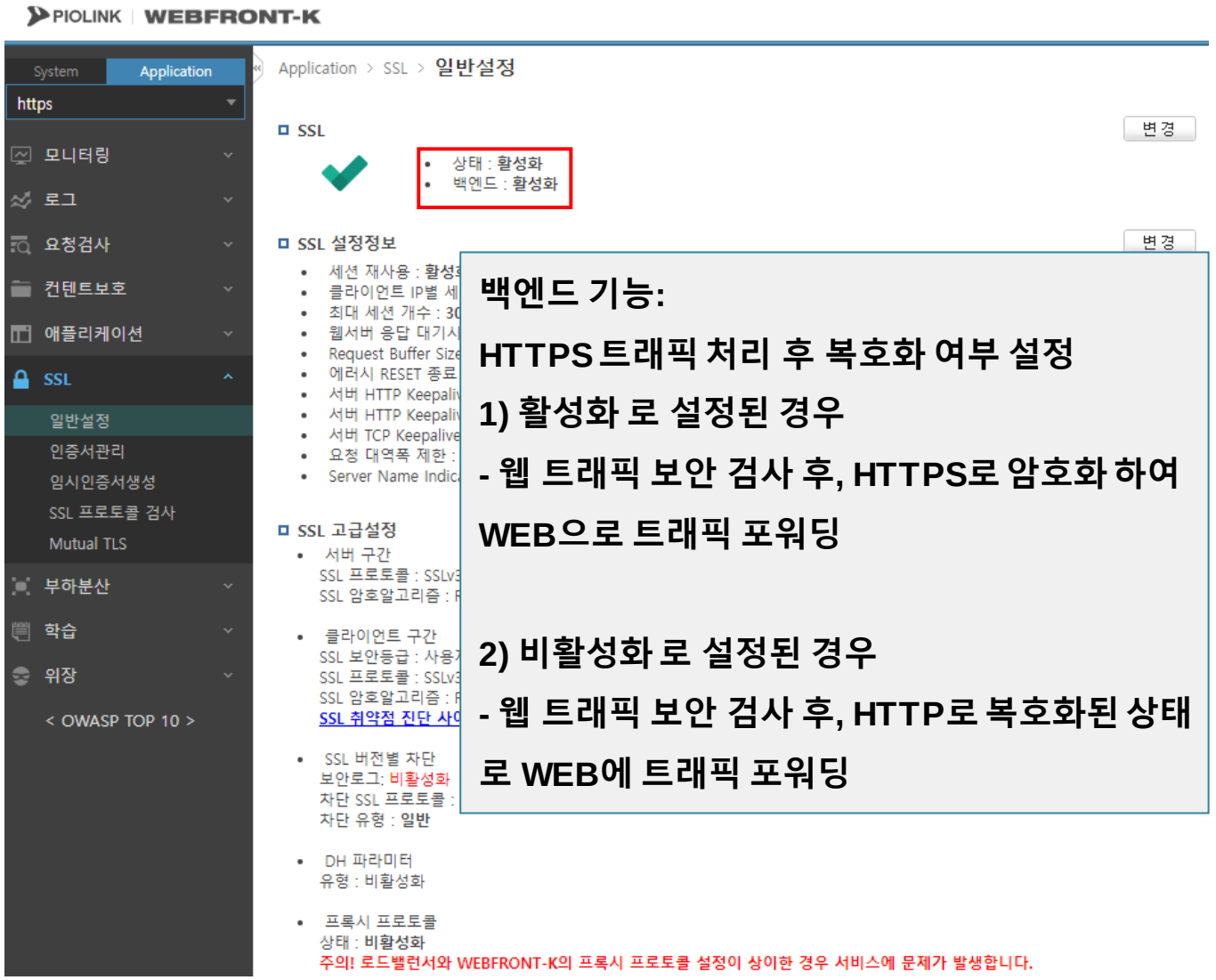
- **SSL 설정**
  - 설정 경로: Application > SSL > 일반설정



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

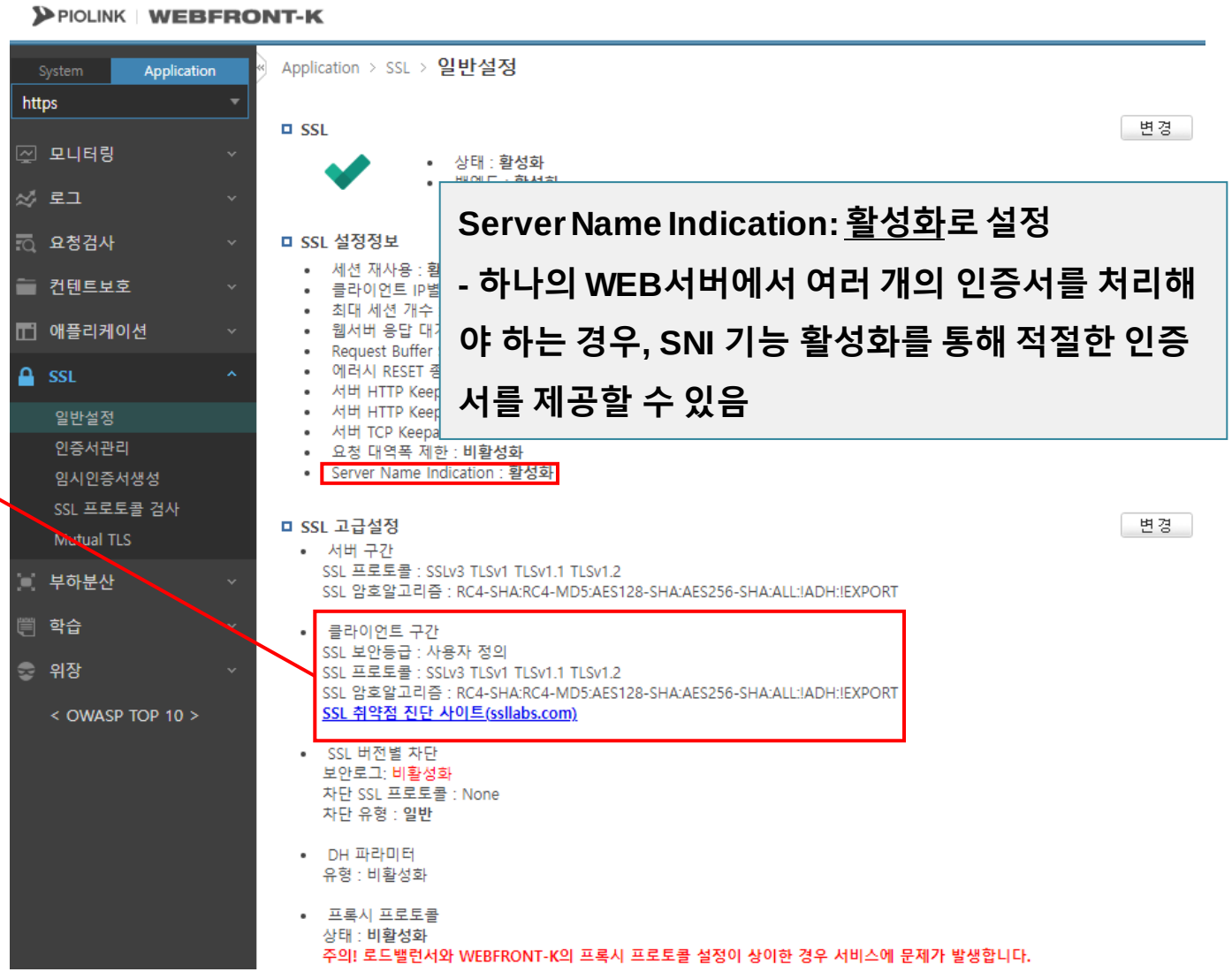
- 웹 트래픽 보안 검사 후, HTTP로 복호화된 상태로 WEB에 트래픽 포워딩

9. SSL 설정

- **SSL 설정**
  - 설정 경로: Application > SSL > 일반설정

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

9. SSL 설정

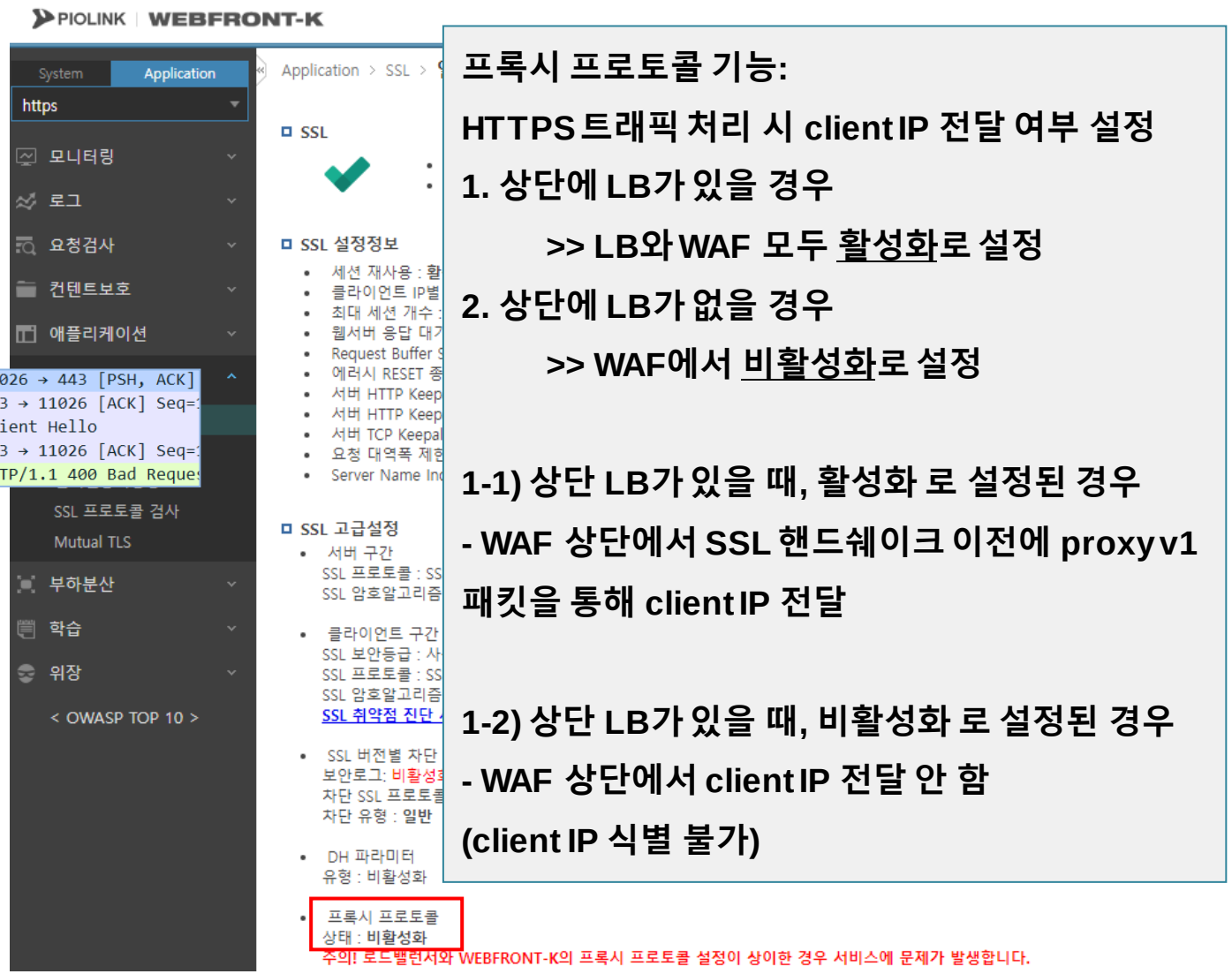
- **SSL 설정**
  - 설정 경로: Application > SSL > 일반설정

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

1-1) 상단 LB가 있을 때, 활성화 로 설정된 경우

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

1-2) 상단 LB가 있을 때, 비활성화 로 설정된 경우

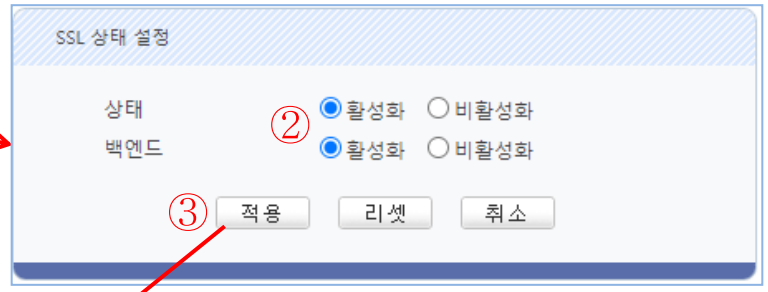
- WAF 상단에서 client IP 전달 안 함

(client IP 식별 불가)

10. SSL, 애플리케이션 및 소스 NAT 활성화

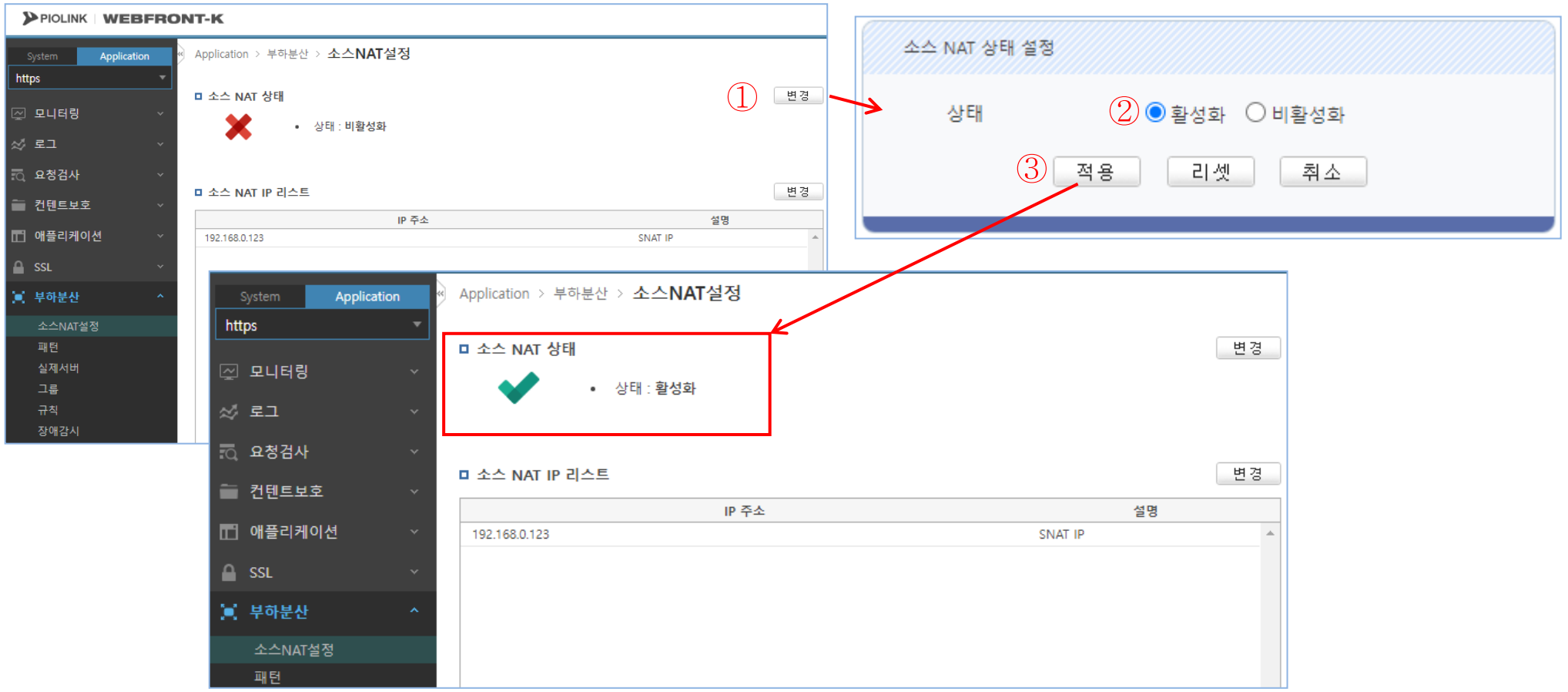
- **SSL, 애플리케이션 활성화**
  - 설정 경로: Application > SSL > 일반설정

SSL 상태 활성화 시, 애플리케이션의 상태도 함께 활성화됨



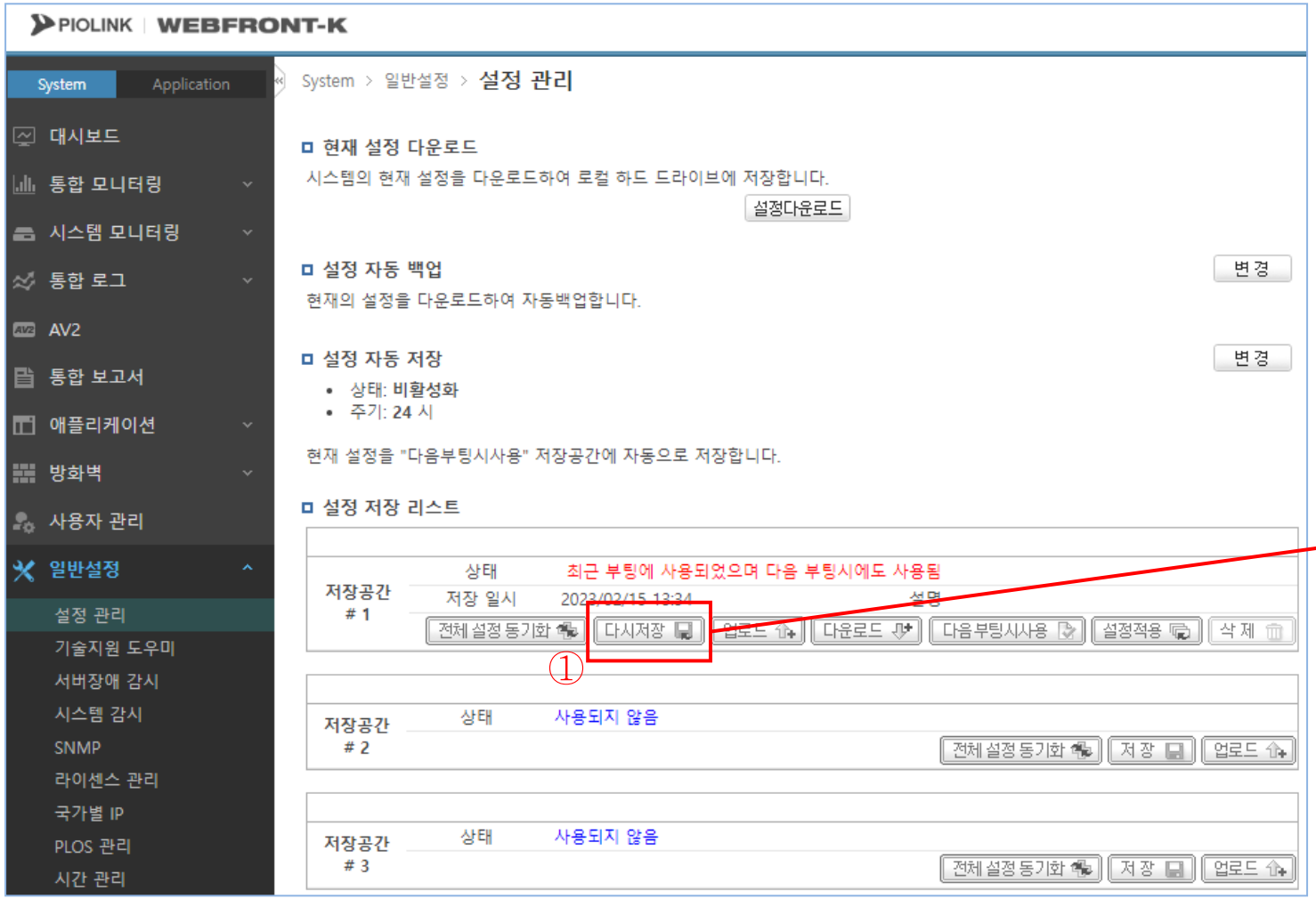
10. SSL, 애플리케이션 및 소스 NAT 활성화

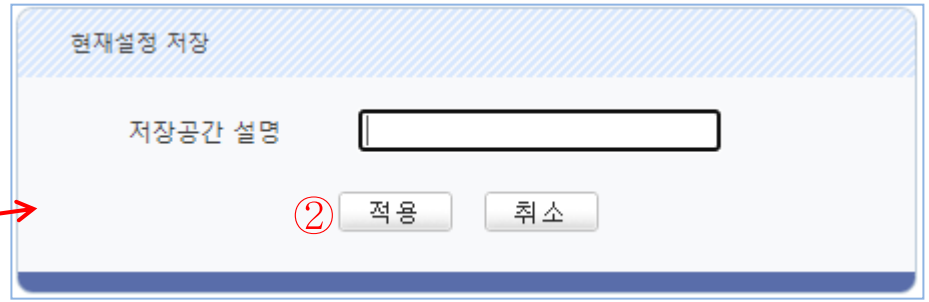
- **소스NAT 활성화**
  - 설정 경로: Application > 부하분산 > 소스NAT설정



11. 설정 저장

- **설정 저장**
  - 설정 경로: System > 일반설정 > 설정 관리





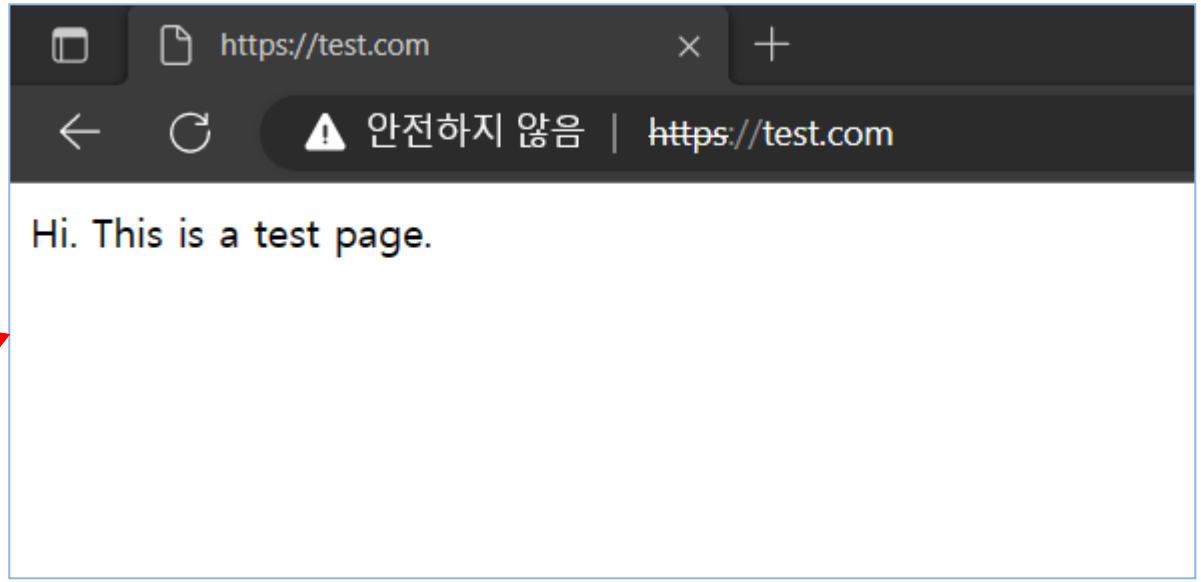
12. 웹 서비스 확인

- **WEBFRONT-KS 설정 완료 후 통신 가능여부 확인**
  - Hosts파일에 서비스 도메인에 대해 웹방화벽의 FIP를 지정해준 후, 웹 브라우저를 통해 웹방화벽을 통해 실제 통신이 가능한지 테스트 진행
    - 아래는 테스트 간 임시 인증서를 사용했기 때문에 인증서 오류가 발생하였으나, 정상적인 인증서를 사용하면 문제없이 접속됨

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#   127.0.0.1       localhost
#   ::1             localhost

1.1.1.1 test.com
```



PIOLINK

4. 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

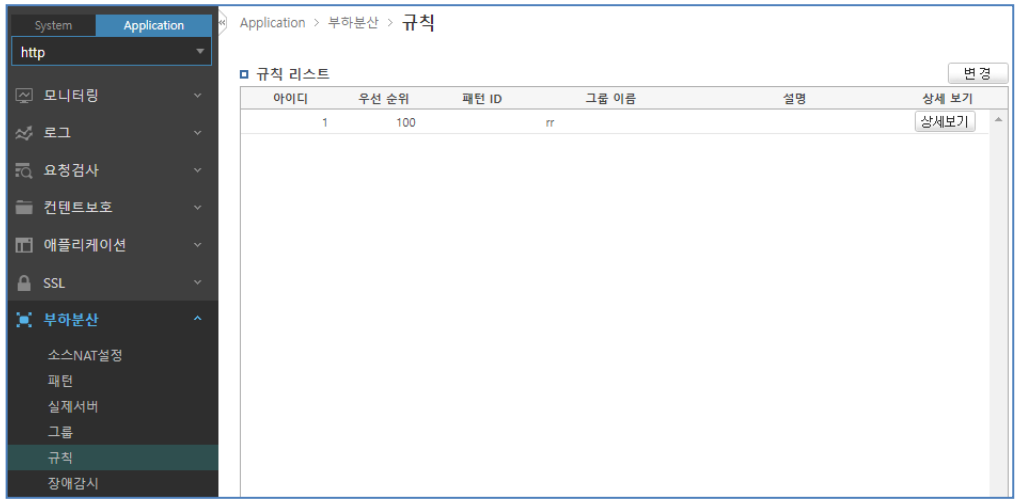
그룹 설정

✓ 그룹에 등록된 실제 서버 개수 확인
✓ Persist 설정 확인

1. HTTP

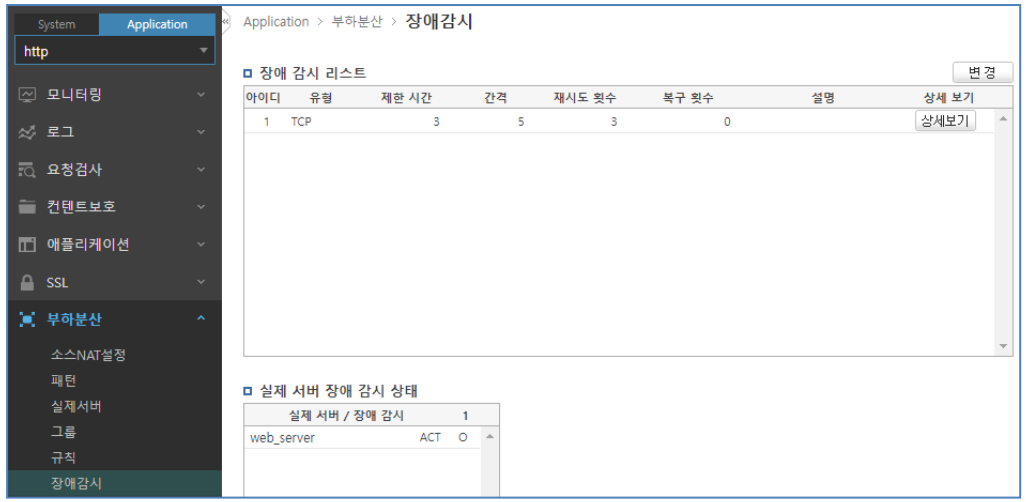
- **WEBFRONT-KS 설정 체크**
  - 웹방화벽으로서 기능하기 위한 최소한의 설정 상태 체크

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
- 인증서 관리 설정
- 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

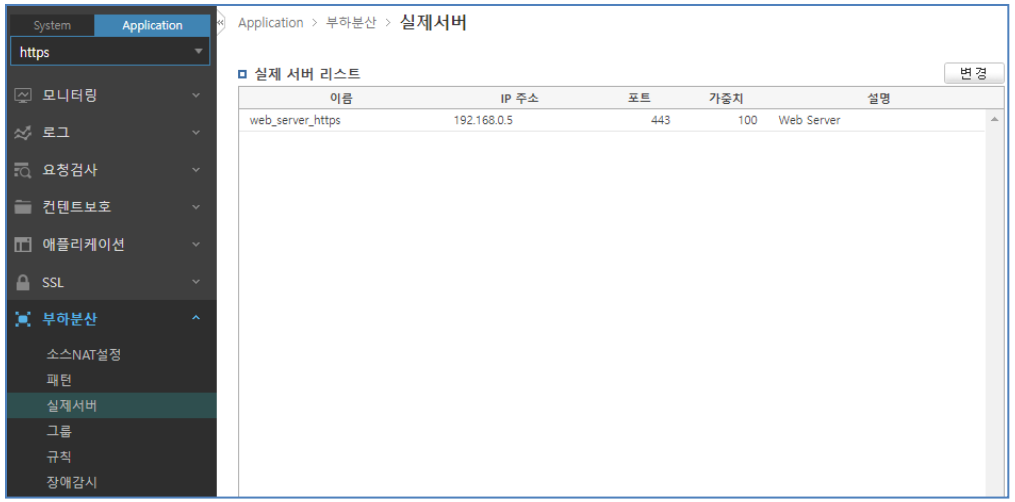
소스NAT설정

- ✓ 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

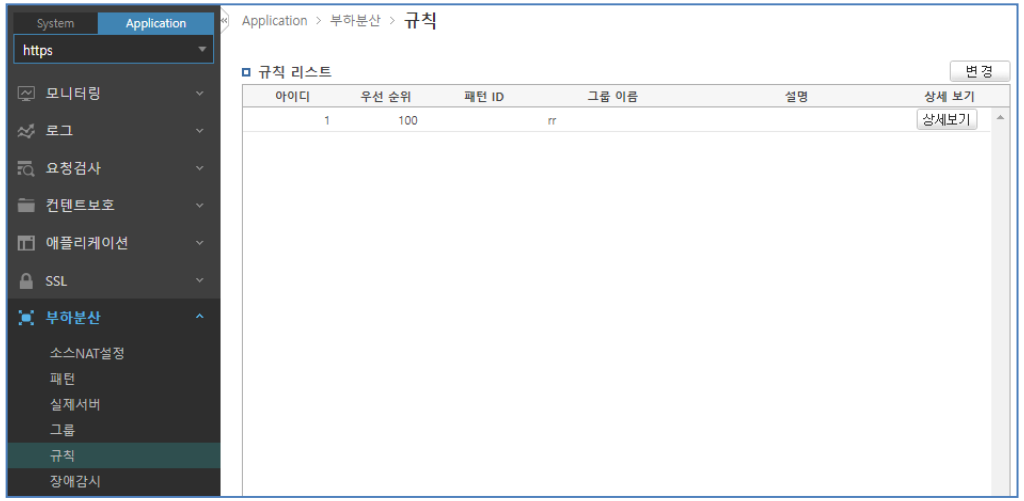
✓ 그룹에 등록된 실제 서버 개수 체크
✓ Persist 설정 확인

PIOLINK

2. HTTPS

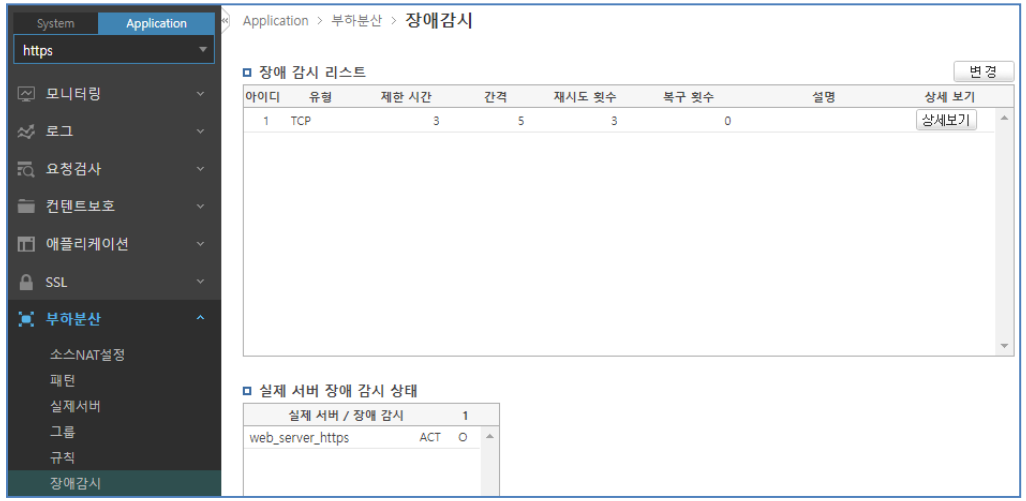
- **WEBFRONT-KS 설정 체크**
  - 웹방화벽으로서 기능하기 위한 최소한의 설정 상태 체크

규칙 설정



✓ 규칙 내에 그룹 등록 여부

장애 감시 설정



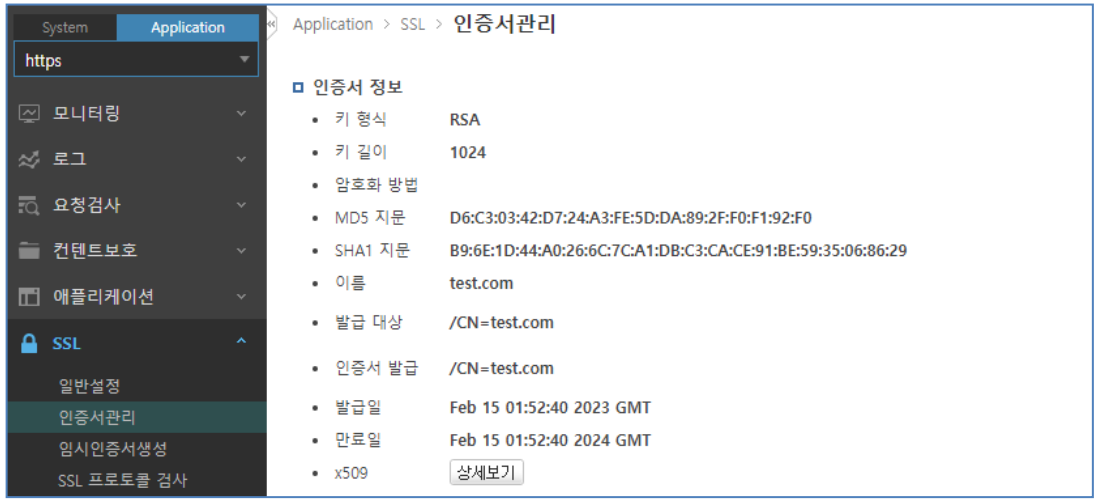
✓ 장애 감시 프로토콜의 tcp 설정 여부
✓ 장애 감시 tcp 포트 설정 확인
✓ 장애 감시 상태의 정상 여부

PIOLINK

2. HTTPS

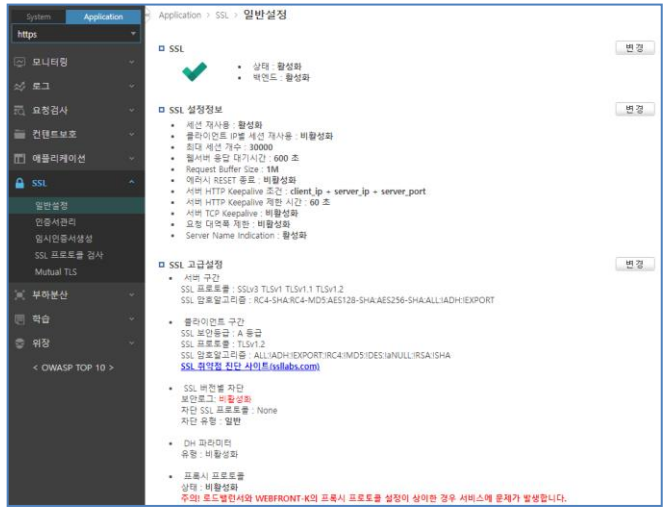
- **WEBFRONT-KS 설정 체크**
  - 웹방화벽으로서 기능하기 위한 최소한의 설정 상태 체크

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