

웹 보안에 최고 성능을 담다

WEBFRONT-KS

초기 설정 가이드

(주)파이오링크



개요

1. 네트워크 설정

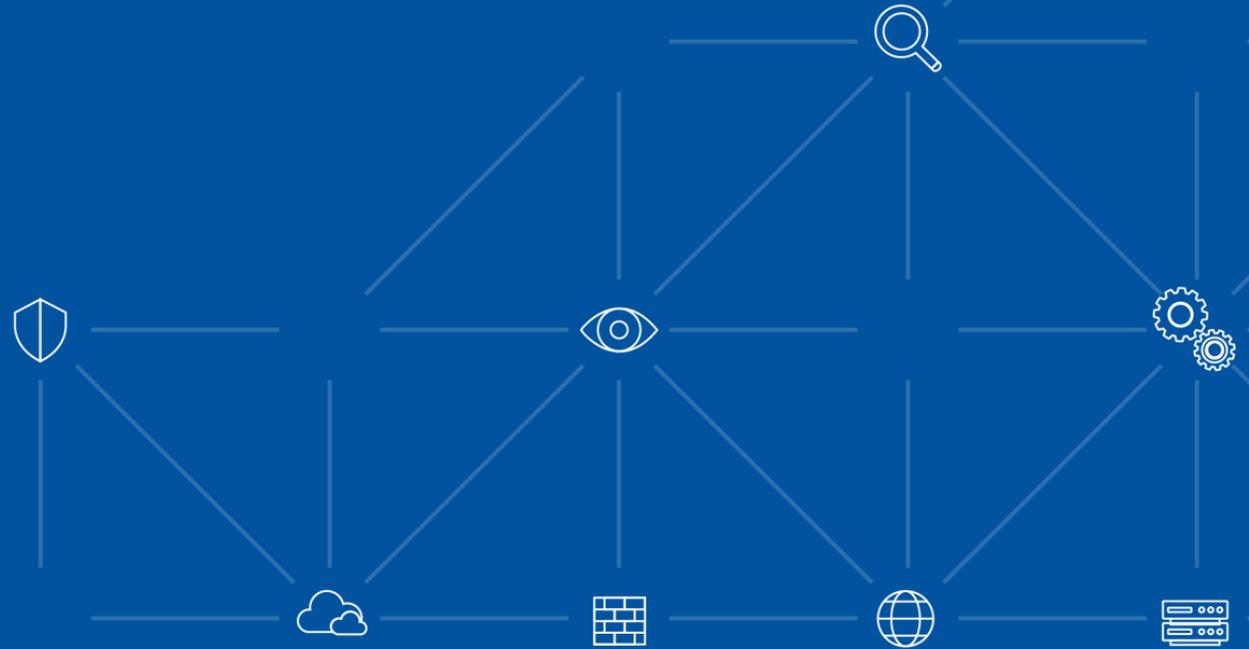
2. HTTP 서비스 설정

3. HTTPS 서비스 설정

4. 설정 체크리스트



1. 네트워크 설정



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)

네트워크 서브넷 변경

선택된 서브넷

사용 가능한 서브넷

↻ 새로 고침

Default Network (192.168.0.0/24)

network_172 (172.16.0.0/16)

serv_net (10.1.1.0/24)

sqa_sub (192.168.1.0/24)

vpc_test (192.168.2.0/24)

⇨

Vlan 설정

□ VLAN 정보

이름	아이디	Promisc	eth1	eth2	mgmt
port2	0	비활성화		U	
port1	0	비활성화	U		

(T:Tagged port, U:Untagged port)

IP주소 추가

□ IP 주소 테이블

인터페이스	IP 주소	브로드캐스트
port1	172.16.0.8/24	172.16.0.255
port2	10.1.1.8/24	10.1.1.255

추가 ➕

삭제 🗑️

추가 인터페이스 설정

Mgmt 이외의 추가 인터페이스 설정

1. 인터페이스 할당

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

★ **WAF-TEST1** ACTIVE

기본 정보 | **네트워크** | 접속 정보 | 모니터링

보안 그룹 변경

네트워크 인터페이스 ⓘ ↕	VPC ⓘ ↕	서브넷	사설 IP	
cd5ce04f-e4ef-4e24-8b73-666b4eaddc7e	Default Network (192.168.0.0/16)	Default Network (192.168.0.0/24)	192.168.0.64	mgmt
d41c28e2-2085-4673-b255-ebd67aa650ac	network_172 (172.16.0.0/16)	network_172 (172.16.0.0/16)	172.16.0.103	eth1
f1b584bf-08cf-443c-b04b-09c1adba8e11	serv_net (10.1.0.0/16)	serv_net (10.1.1.0/24)	10.1.1.46	eth2

1. 네트워크 설정

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 | WEBFRONT-K

System > 네트워크 > VLAN

eth1 eth2 mgmt

VLAN 정보

이름	아이디	Promisc	eth1	eth2	mgmt
port2	0	비활성화		U	
port1	0	비활성화	U		

추가 삭제

VLAN 추가

TYPE Tagged Untagged

VLAN 이름

VLAN 상태 UP Down

Promisc 활성화 비활성화

포트 eth1 eth2 mgmt

(T:Tagged port, U:Untagged port)

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 | WEBFRONT-K

System > 네트워크 > IP 주소

변경

□ DHCP 테이블

- DHCP 상태 : 활성화

인터페이스	IP 주소	브로드캐스트
Manage-Port	192.168.0.64	

- DHCP 라우터 : 활성화

목적지	게이트웨이	넷마스크	인터페이스
0.0.0.0	192.168.0.1	0.0.0.0	Manage-Port

□ IP 주소 테이블

인터페이스	IP 주소	브로드캐스트
port1	172.16.0.103/24	172.16.0.255
port2	10.1.1.46/24	10.1.1.255

추가

IP 추가

인터페이스: port1

IP 버전: IPv4 IPv6

IP 주소: 172.16.0.103/24 (A.B.C.D/M)

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



PIOLINK | WEBFRONT-K

V4.0.6.61.27

로그인
아이디와 비밀번호를 입력하여 주세요.

사용자 ID

패스워드

확인

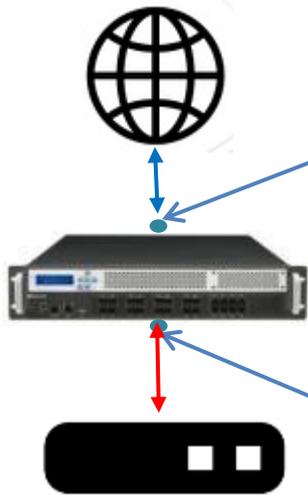
© PIOLINK WEB Application Firewall

🌐 Korean ▾

2. 애플리케이션 일반 설정

• 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)

WAF에서 처리할 도메인 및 상단
 으로부터 트래픽을 받아들이는
 IP/Port를 설정함

Application > 애플리케이션 > 일반설정

Application: 활성화

모드: 부하분산(고급)
 도메인 무시: 비활성화 로 설정

※도메인 없이 IP로만 통신:
 >> 도메인 무시 활성화로 설정

애플리케이션 일반 설정 정보

- 모드: 부하 분산(고급)
- 도메인 무시: 비활성화
- 압축 방식: 비활성화
- 클라이언트 MSS: 1414
- 서버 MSS: 1414
- CPS 제한: 비활성화
- 동시세션 제한: 비활성화
- BPS 제한: 비활성화

애플리케이션 도메인 리스트

도메인 이름	설명
test.com	

처리하고자 하는 도메인을 입력

애플리케이션 IP/포트 리스트

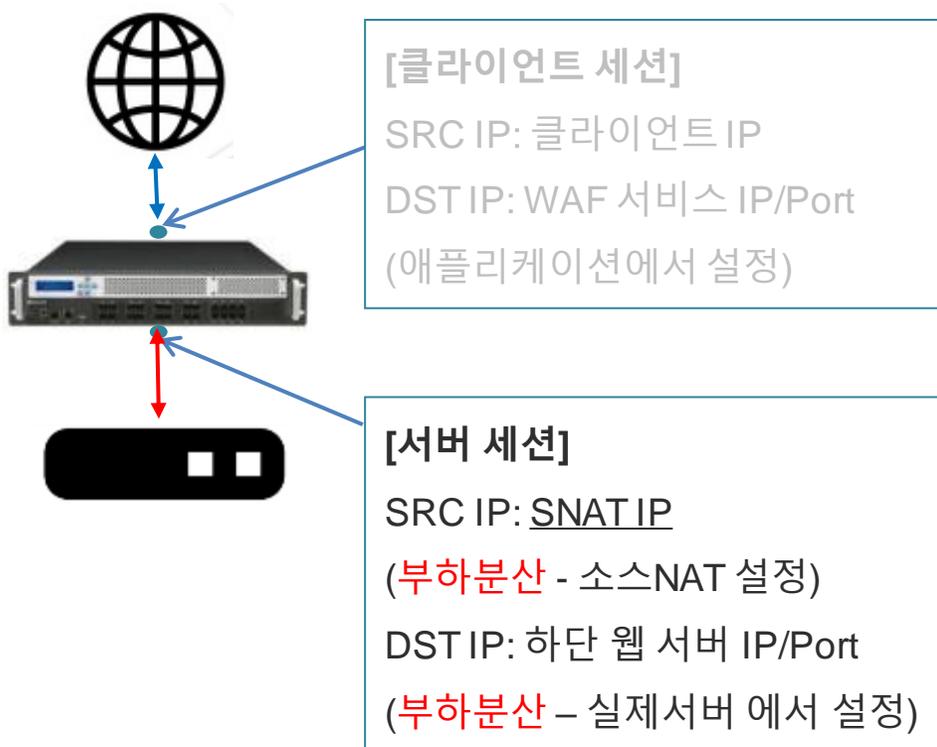
IP 버전	IP 주소	포트	IP 트랜스패런트	유형	설명
v4	192.168.0.123	80	비활성화	HTTP	

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



PIOLINK | WEBFRONT-K

System Application Application > 부하분산 > 소스NAT설정

http

모니터링
로그
요청검사
콘텐츠보호
애플리케이션
SSL
부하분산
소스NAT설정
패턴
실제서버
그룹
규칙
장애감시

소스 NAT 상태 상태: 활성화

소스 NAT IP 리스트

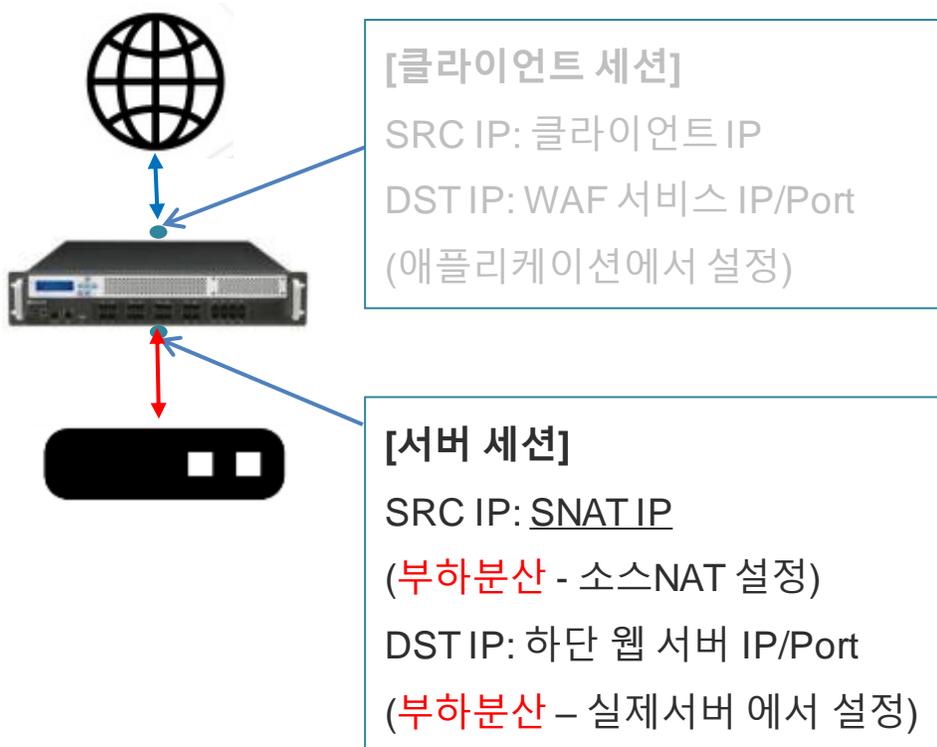
IP 주소	설명
192.168.0.123	

소스 NAT IP 리스트
- WAF의 사설 IP를 입력

4. 부하분산 – 실제 서버 설정

• WEBFRONT-KS 기본 구성

- 서버 세션 관련 설정(부하분산)
- 설정 경로: Application > 부하분산 > 실제서버



PIOLINK | WEBFRONT-K

System Application Application > 부하분산 > 실제서버

http

모니터링
로그
요청검사
컨텐츠보호
애플리케이션
SSL
부하분산
소스NAT설정
패턴
실제서버
그룹
규칙
장애감시

실제 서버 리스트

이름	IP 주소	포트	가중치	설명
web_server	192.168.0.5	80	100	Web Server

실제 서버

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

4. 부하분산 – 실제 서버 설정

• WEBFRONT-KS 기본 구성

- 서버 세션 관련 설정(부하분산)
- 설정 경로: Application > 부하분산 > 실제서버

Application > 부하분산 > 실제서버

□ 실제 서버 설정

이름	IP 주소	포트	가중치	설명
web_server	192.168.0.5	80	100	Web Server
web2	192.168.0.8	8080	100	
web3	192.168.0.9	10888	100	

Application > 부하분산 > 실제서버

□ 실제 서버 설정

이름	IP 주소	포트	가중치	설명
web_server	192.168.0.5	80	100	Web Server
web2	192.168.0.10	80	100	

실제 서버

- 실제 서버는 부하 분산을 위한 서버 리스트임

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

4. 부하분산 – 실제 서버 설정

• WEBFRONT-KS 기본 구성

- 서버 세션 관련 설정(부하분산)
- 설정 경로: Application > 부하분산 > 실제서버

Application > 부하분산 > 실제서버

이름	IP 주소	포트	가중치	설명
web_server	192.168.0.5	80	100	Web Server

① 변경

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

이름	IP 주소	포트	가중치	설명
web_server	192.168.0.5	80	100	Web Server

② 추가

실제 서버 추가

상태: 활성화 비활성화

이름: web1

IP 주소: 192.168.0.5

포트: 80

가중치: 100

설명:

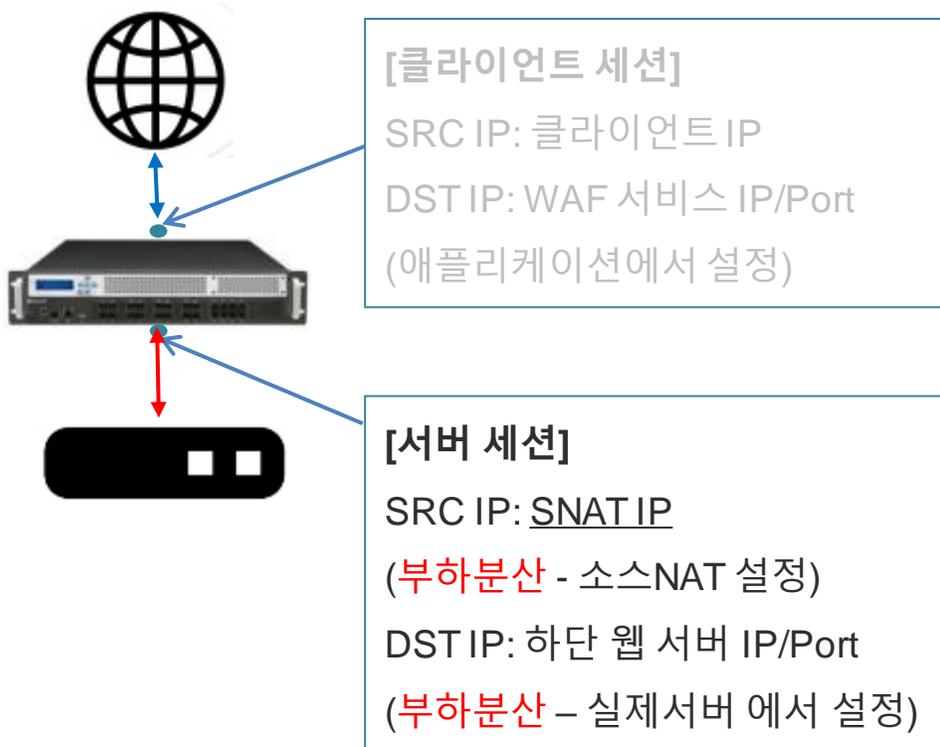
③ 확인 리셋 취소

- 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



그룹
 - 실제 서버 한 개 혹은 다수를 하나의 부하분산 그룹으로 설정함

이름	Persist	부하 분산 알고리즘	실제 서버 개수	설명	상세 보기
rr	아이피	라운드 로빈	1		상세보기

Persist 기준

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

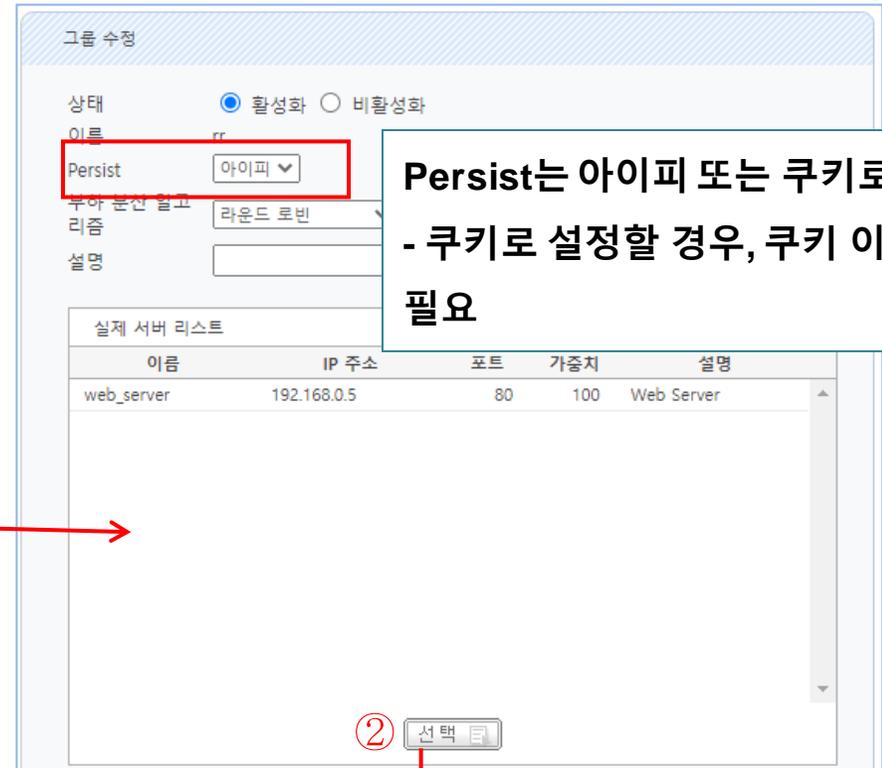
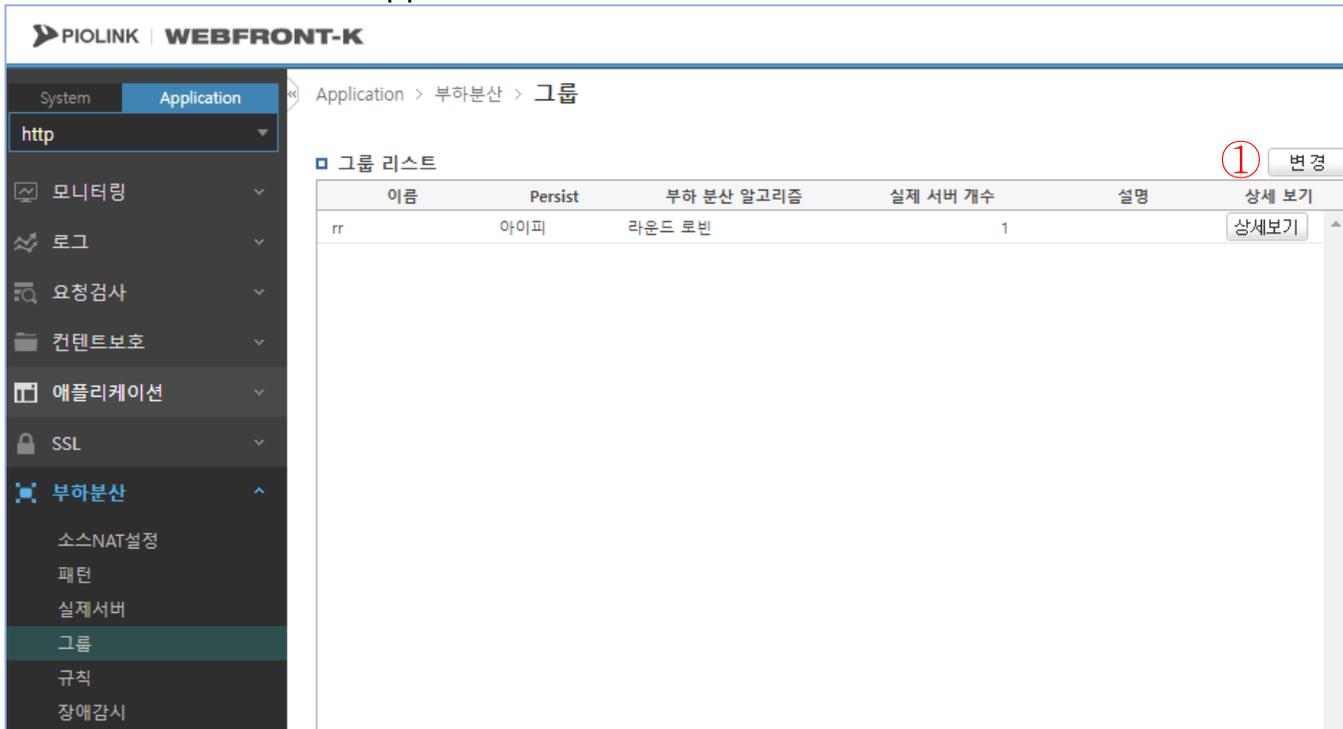
- 쿠키: 세션 맺을 때 http 쿠키 생성 후 해당 **쿠키**를 기준으로 부하분산
 (같은 **쿠키** >> 같은 웹 서버)

※ WEB서버가 다수인 경우에는 반드시 쿠키 persist 설정

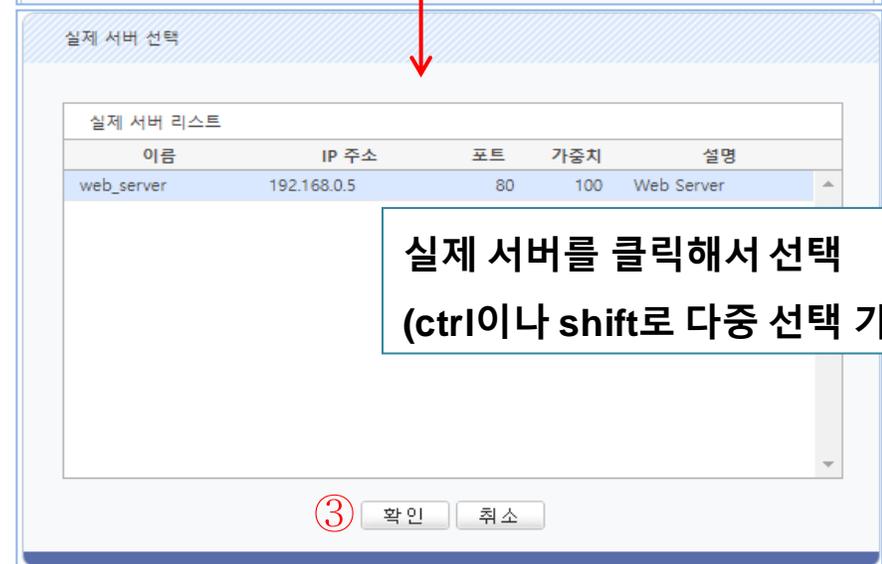
5. 부하분산 - 그룹 설정

• 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



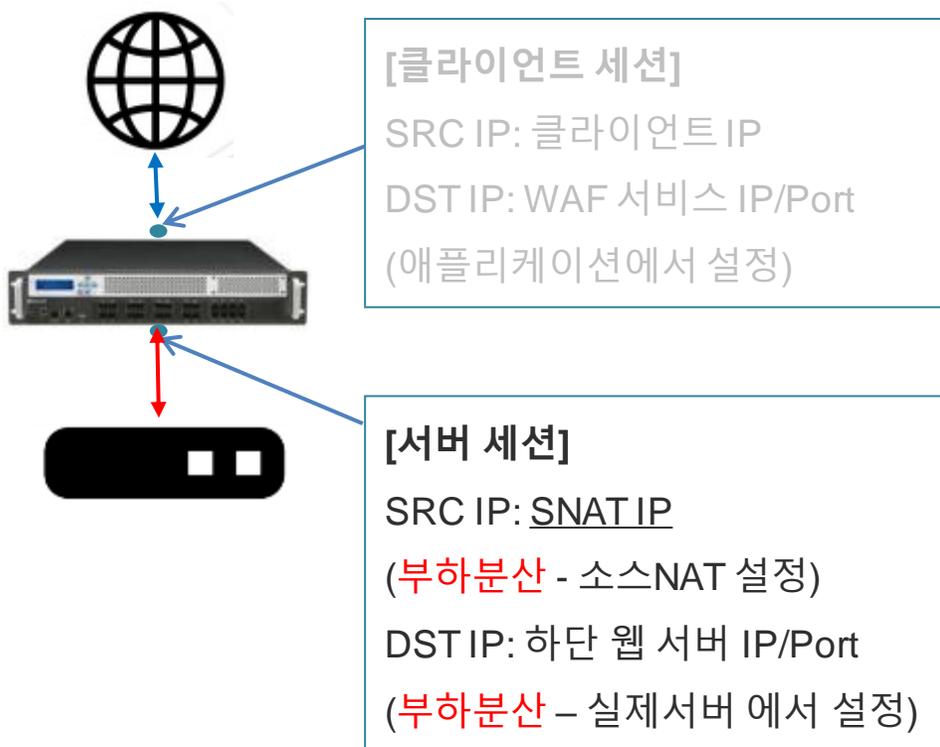
실제 서버를 클릭해서 선택
(ctrl이나 shift로 다중 선택 가능)

3 확인 취소

6. 부하분산 - 규칙 설정

• WEBFRONT-KS 기본 구성

- 서버 세션 관련 설정(부하분산)
- 설정 경로: Application > 부하분산 > 규칙



아이디	우선 순위	패턴 ID	그룹 이름	설명	상세 보기
1	100		rr		상세보기

규칙 상세 보기

- 아이디 : 1
- 상태 : 활성화
- 우선 순위 : 100
- 설명 :

아이디	유형	매치 방법	비교 문자열	설명
(Empty table content)				

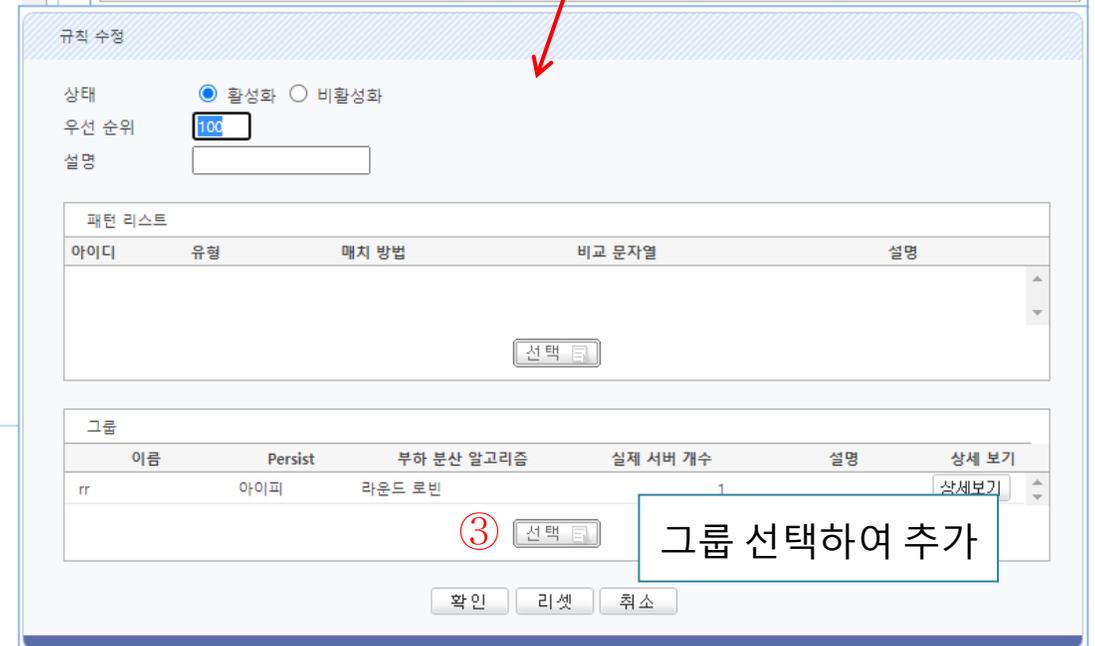
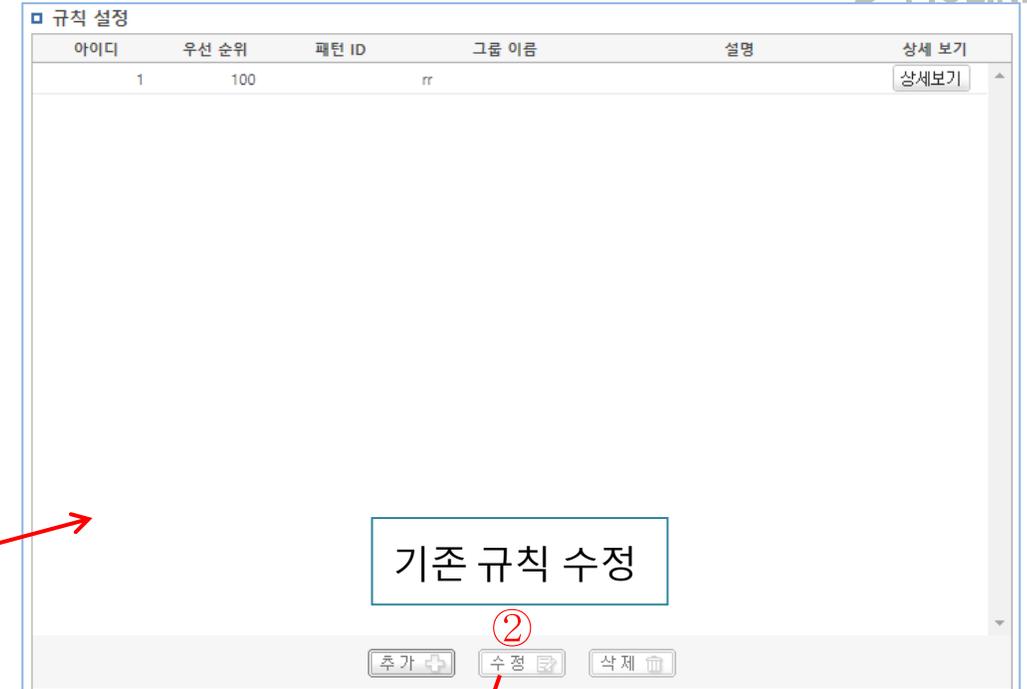
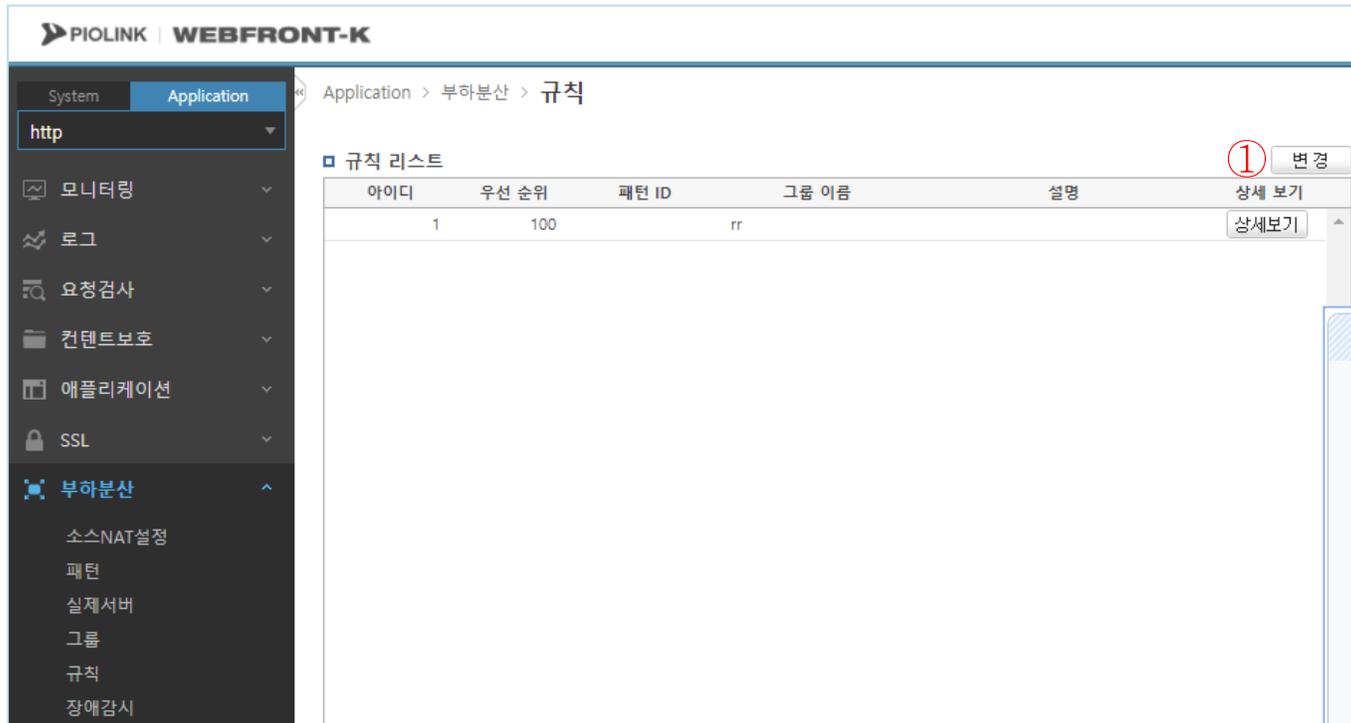
이름	Persist	부하 분산 알고리즘	실제 서버 개수	설명	상세 보기
rr	아이피	라운드 로빈	1		상세보기

규칙 = 그룹 + 패턴(패턴은 설정하지 않아도 무방함)

6. 부하분산 - 규칙 설정

• WEBFRONT-KS 기본 구성

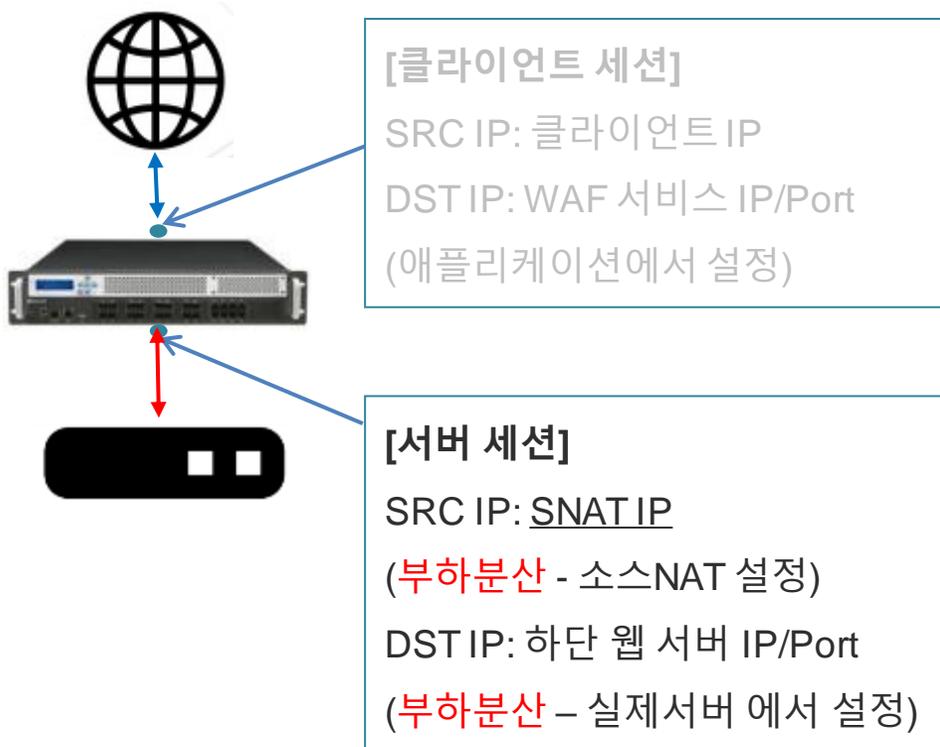
- 서버 세션 관련 설정(부하분산)
- 설정 경로: Application > 부하분산 > 규칙



7. 부하분산 - 장애 감시 설정

• WEBFRONT-KS 기본 구성

- 서버 세션 관련 설정(부하분산)
- 설정 경로: Application > 부하분산 > 장애감시



장애 감시 리스트

아이디	유형	제한 시간	간격	재시도 횟수	복구 횟수	설명	상세 보기
1	TCP	3	5	3	0		상세보기

실제 서버 장애 감시 상태

실제 서버 / 장애 감시	1
web_server	ACT ○

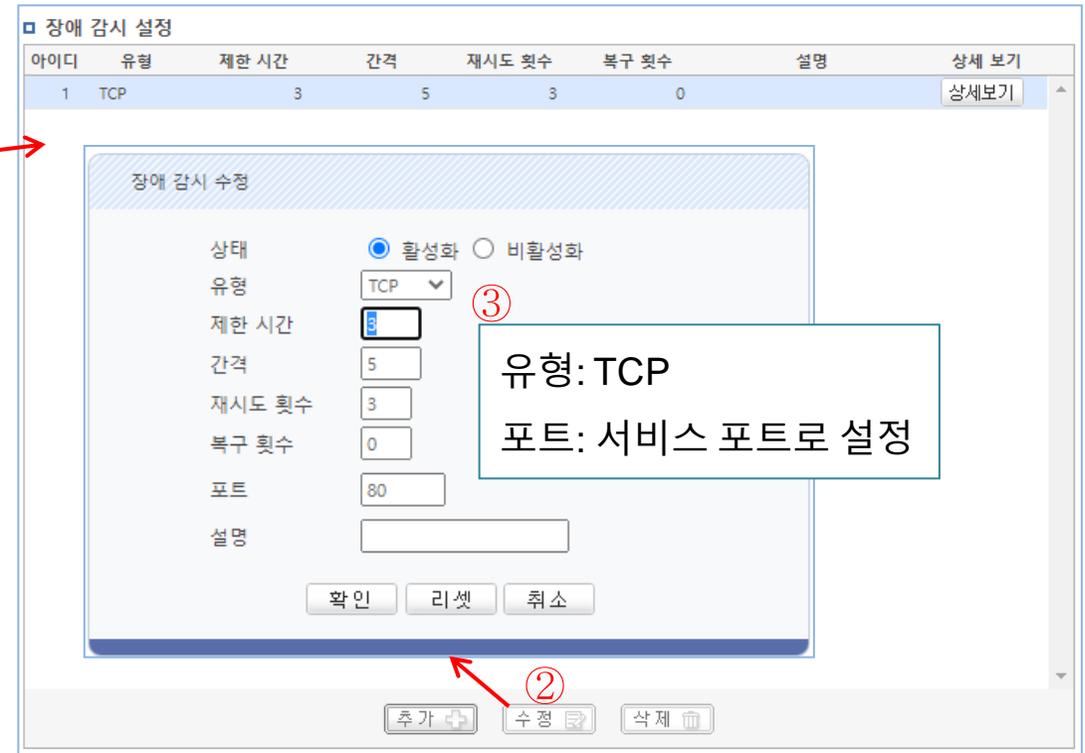
헬스체크 유형은 TCP, ICMP, HTTP, HTTPS를 제공
 ※ TCP로 설정 권고

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

PIOLINK WEBFRONT-K

System Application Application > 애플리케이션 > 일반설정

애플리케이션

- 상태: 비활성화

애플리케이션 일반 설정 정보

- 모드: 부하 분산(고급)
- 도메인 무시: 비활성화
- 압축 방지: 비활성화
- 클라이언트 MSS: 1414
- 서버 MSS: 1414
- CPS 제한: 비활성화
- 동시세션 제한: 비활성화
- BPS 제한: 비활성화

변경

애플리케이션 상태 설정

상태

활성화 비활성화

적용 리셋 취소

변경

System Application Application > 애플리케이션 > 일반설정

애플리케이션

- 상태: 활성화

애플리케이션 일반 설정 정보

- 모드: 부하 분산(고급)
- 도메인 무시: 비활성화
- 압축 방지: 비활성화
- 클라이언트 MSS: 1414
- 서버 MSS: 1414
- CPS 제한: 비활성화
- 동시세션 제한: 비활성화
- BPS 제한: 비활성화

변경

8. 애플리케이션 및 소스 NAT 활성화

• 소스NAT 활성화

- 설정 경로: Application > 부하분산 > 소스NAT설정

PIOLINK | WEBFRONT-K

System Application Application > 부하분산 > 소스NAT설정

소스 NAT 상태 ✘ 상태: 비활성화

소스 NAT IP 리스트

IP 주소	설명
192.168.0.123	

변경

소스 NAT 상태 설정

상태 ● 활성화 ○ 비활성화

③ 적용 리셋 취소

System Application Application > 부하분산 > 소스NAT설정

소스 NAT 상태 ✔ 상태: 활성화

소스 NAT IP 리스트

IP 주소	설명
192.168.0.123	

변경

9. 설정 저장

• 설정 저장

– 설정 경로: System > 일반설정 > 설정 관리

PIOLINK | WEBFRONT-K

System > 일반설정 > 설정 관리

- 현재 설정 다운로드
 시스템의 현재 설정을 다운로드하여 로컬 하드 드라이브에 저장합니다. 설정다운로드
- 설정 자동 백업 변경
 현재의 설정을 다운로드하여 자동백업합니다.
- 설정 자동 저장 변경
 상태: 비활성화
 주기: 24 시
 현재 설정을 "다음부팅시사용" 저장공간에 자동으로 저장합니다.
- 설정 저장 리스트

저장공간	상태	설명
# 1	최근 부팅에 사용되었으며 다음 부팅시에도 사용됨	2023/02/15 09:48
<div style="display: flex; justify-content: space-between;"> 전체 설정 동기화 다시저장 업로드 다운로드 다음부팅시사용 설정적용 삭제 </div>		
# 2	사용되지 않음	
<div style="display: flex; justify-content: space-between;"> 전체 설정 동기화 저장 업로드 </div>		
# 3	사용되지 않음	
<div style="display: flex; justify-content: space-between;"> 전체 설정 동기화 저장 업로드 </div>		

현재설정 저장

저장공간 설명

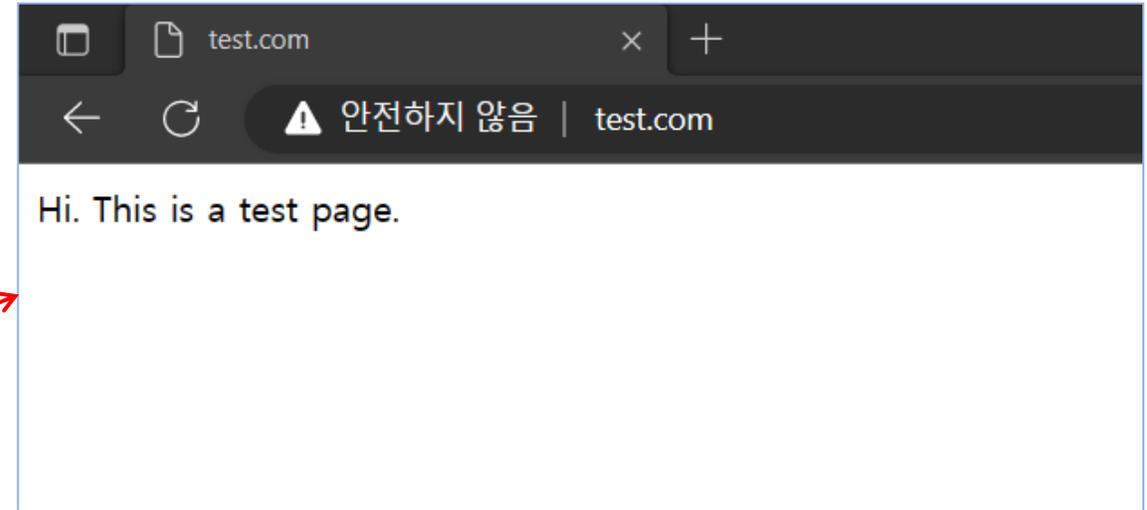
② 적용 취소

10. 웹 서비스 확인

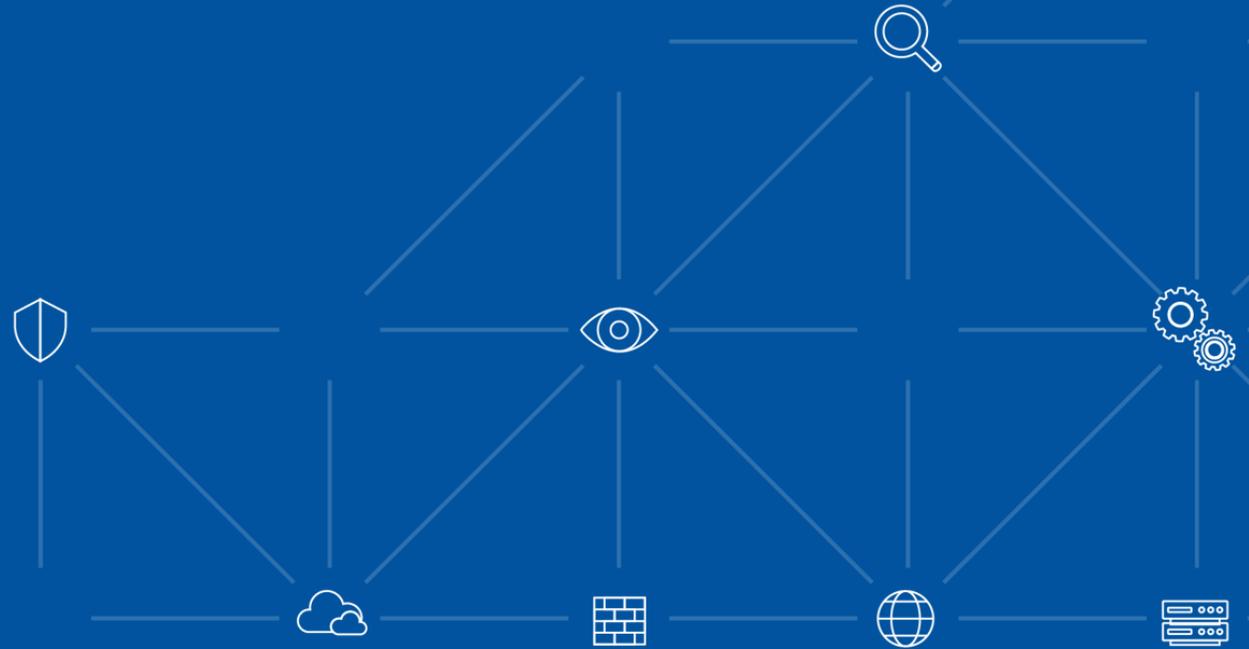
• WEBFRONT-KS 설정 완료 후 통신 가능여부 확인

- 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
```



3. HTTPS 서비스 설정



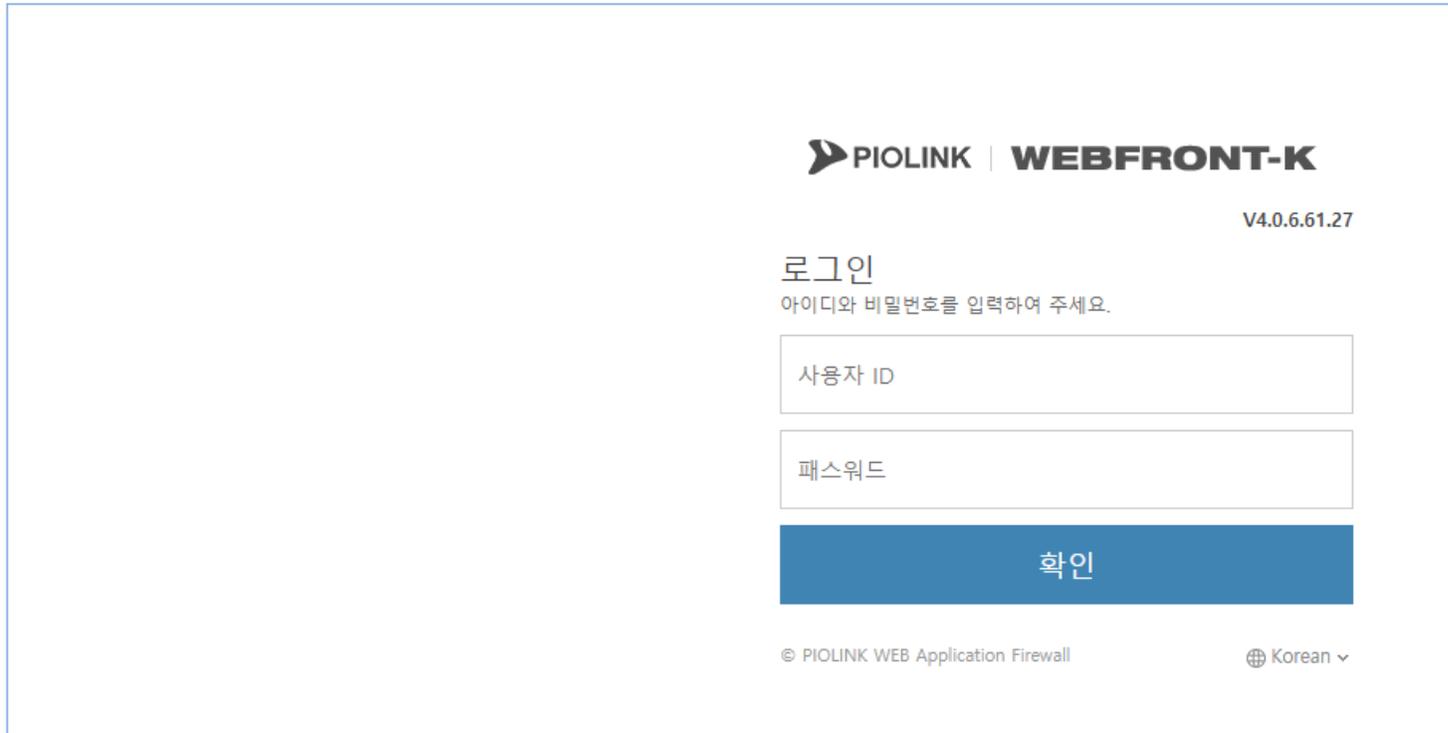
HTTPS 서비스 설정 순서

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 | WEBFRONT-K

V4.0.6.61.27

로그인
아이디와 비밀번호를 입력하여 주세요.

사용자 ID

패스워드

확인

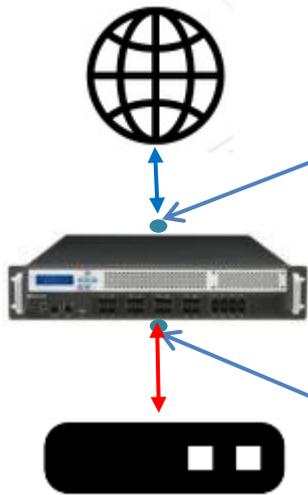
© PIOLINK WEB Application Firewall

🌐 Korean ▾

2. 애플리케이션 일반 설정

• 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)

WAF에서 처리할 도메인 및 상단
 으로부터 트래픽을 받아들이는
 IP/Port를 설정함

Application > 애플리케이션 > 일반설정

Application: 활성화

모드: 부하분산(고급)
 도메인 무시: 비활성화 로 설정

※도메인 없이 IP로만 통신:
 >> 도메인 무시 활성화로 설정

애플리케이션 일반 설정 정보

- 모드: 부하 분산(고급)
- 도메인 무시: 비활성화
- 압축 방식: 비활성화
- 클라이언트 MSS: 1414
- 서버 MSS: 1414
- CPS 제한: 비활성화
- 동시세션 제한: 비활성화
- BPS 제한: 비활성화

애플리케이션 도메인 리스트

도메인 이름	선택
test.com	<input type="checkbox"/>

처리하고자 하는 도메인을 입력

애플리케이션 IP/포트 리스트

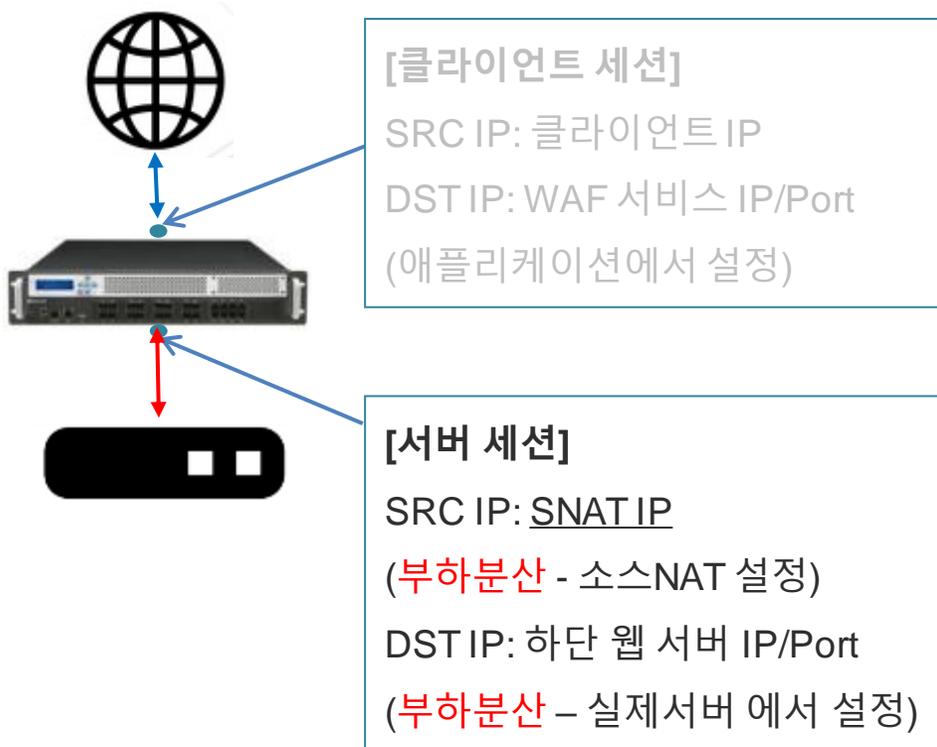
IP 버전	IP 주소	포트	IP 트랜스패런트	유형	설명
v4	192.168.0.123	443	비활성화	HTTPS	

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



PIOLINK | WEBFRONT-K

System Application Application > 부하분산 > 소스NAT설정

소스 NAT 상태 [편집]

소스 NAT 상태
 • 상태 : 활성화

소스 NAT IP 리스트 ① [편집]

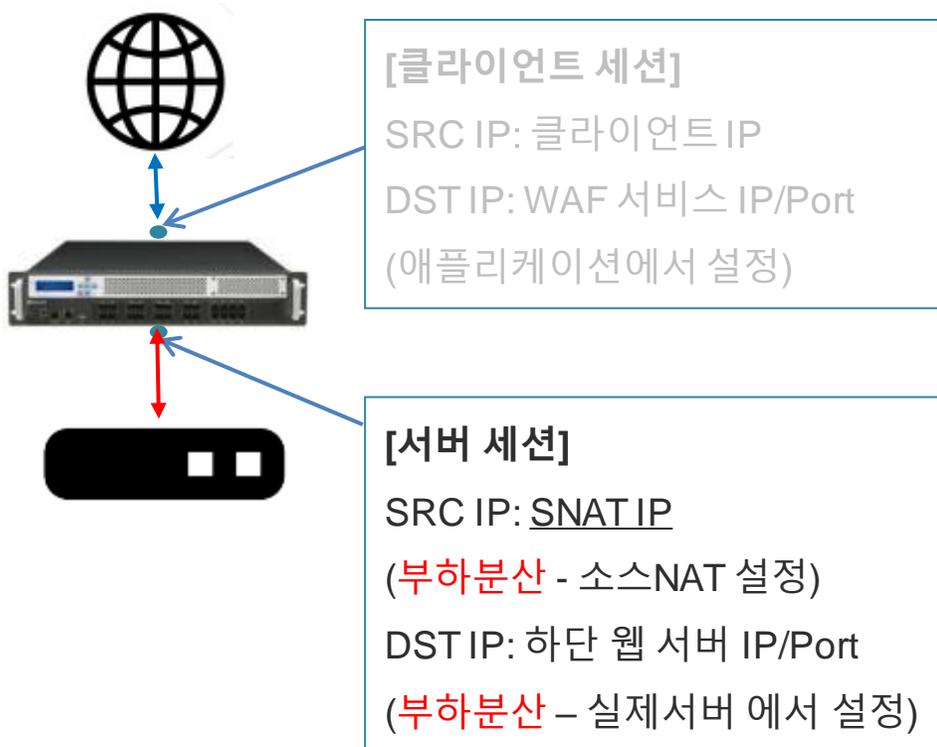
IP 주소	설명
192.168.0.123	SNAT IP

소스 NAT IP 리스트
 - WAF의 사설 IP를 입력

4. 부하분산 - 실제 서버 설정

• WEBFRONT-KS 기본 구성

- 서버 세션 관련 설정(부하분산)
- 설정 경로: Application > 부하분산 > 실제서버



PIOLINK | WEBFRONT-K

System Application Application > 부하분산 > 실제서버

이름	IP 주소	포트	가중치	설명
web_server_https	192.168.0.5	443	100	Web Server

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

4. 부하분산 – 실제 서버 설정

• WEBFRONT-KS 기본 구성

- 서버 세션 관련 설정(부하분산)
- 설정 경로: Application > 부하분산 > 실제서버

Application > 부하분산 > 실제서버

□ 실제 서버 설정

이름	IP 주소	포트	가중치	설명
web_server_https	192.168.0.5	443	100	Web Server
web2	192.168.0.8	18443	100	
web3	192.168.0.9	7443	100	

Application > 부하분산 > 실제서버

□ 실제 서버 설정

이름	IP 주소	포트	가중치	설명
web_server_https	192.168.0.5	443	100	Web Server
web2	192.168.0.10	443	100	

실제 서버

- 실제 서버는 부하 분산을 위한 서버 리스트임

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

4. 부하분산 – 실제 서버 설정

• WEBFRONT-KS 기본 구성

- 서버 세션 관련 설정(부하분산)
- 설정 경로: Application > 부하분산 > 실제서버

Application > 부하분산 > 실제서버

이름	IP 주소	포트	가중치	설명
web_server_https	192.168.0.5	443	100	Web Server

① 변경

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

이름	IP 주소	포트	가중치	설명
web_server_https	192.168.0.5	443	100	Web Server

② 추가

실제 서버 수정

상태: 활성화 비활성화

이름: web_server_https

IP 주소: 192.168.0.5

포트: 443

가중치: 100

설명: Web Server

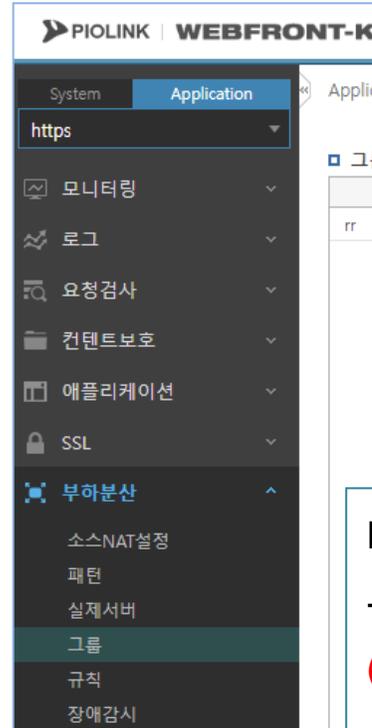
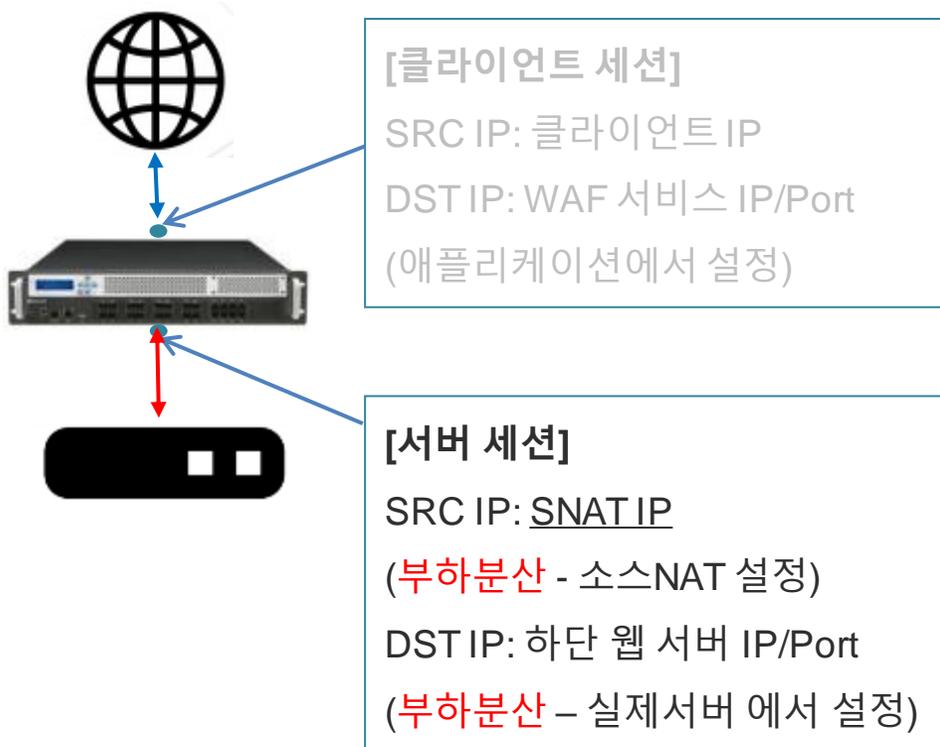
③ 확인 리셋 취소

- 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



그룹
 - 실제 서버 한 개 혹은 다수를 하나의 부하분산 그룹으로 설정함

① 변경

이름	Persist	부하 분산 알고리즘	실제 서버 개수	설명	상세 보기
rr	아이피	라운드 로빈	1		상세보기

Persist 기준

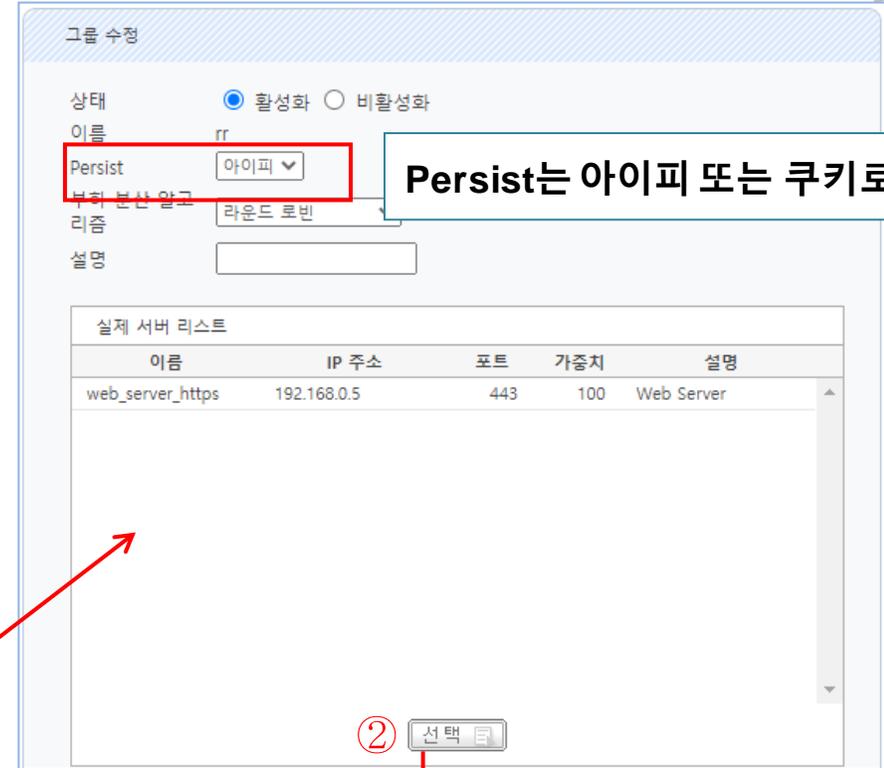
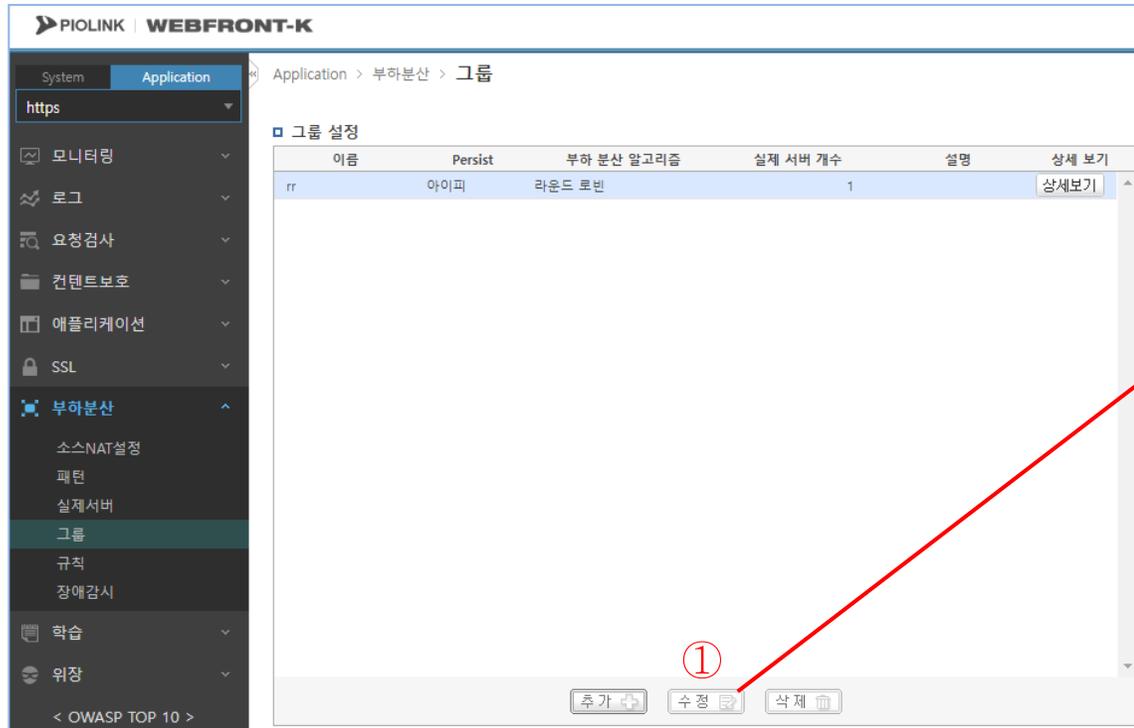
- IP: **SRC IP**를 기준으로 부하분산
 (같은 SRC IP >> 같은 웹 서버)
- 쿠키: 세션 맺을 때 http 쿠키 생성 후 해당 **쿠키**를 기준으로 부하분산
 (같은 쿠키 >> 같은 웹 서버)

※WEB서버가 다수인 경우에는 반드시 쿠키 persist 설정

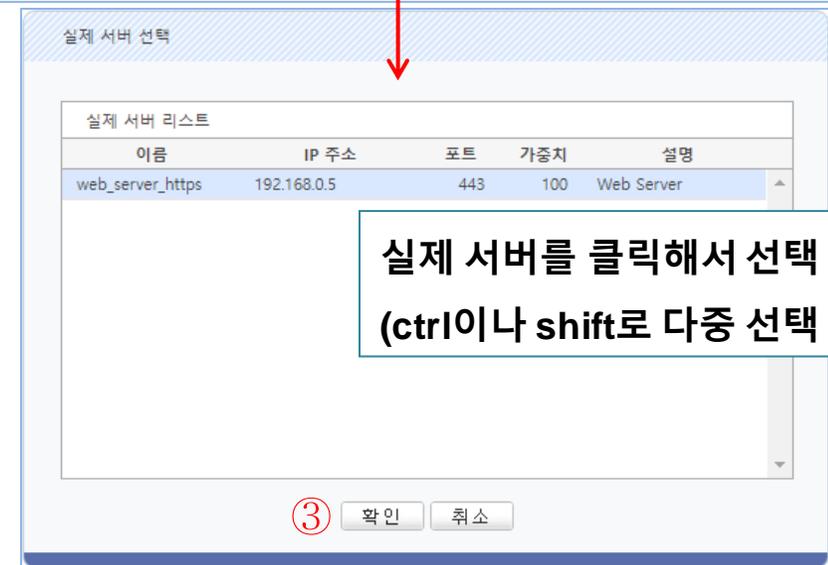
5. 부하분산 - 그룹 설정

• WEBFRONT-KS 기본 구성

- 서버 세션 관련 설정(부하분산)
- 설정 경로: Application > 부하분산 > 그룹



Persist는 아이피 또는 쿠키로 설정

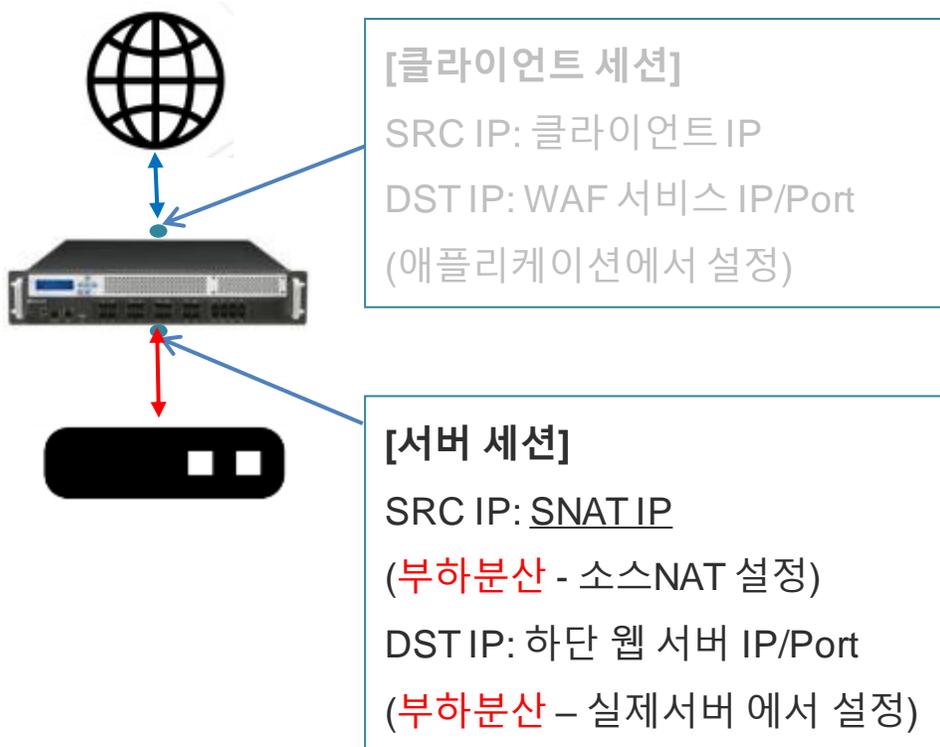


실제 서버를 클릭해서 선택 (ctrl이나 shift로 다중 선택 가능)

6. 부하분산 - 규칙 설정

• WEBFRONT-KS 기본 구성

- 서버 세션 관련 설정(부하분산)
- 설정 경로: Application > 부하분산 > 규칙



Application > 부하분산 > 규칙

규칙 상세 보기

- 아이디 : 1
- 상태 : 활성화
- 우선 순위 : 100
- 설명 :

아이디	유형	매치 방법	비교 문자열	설명
rr	아이피	라운드 로빈		

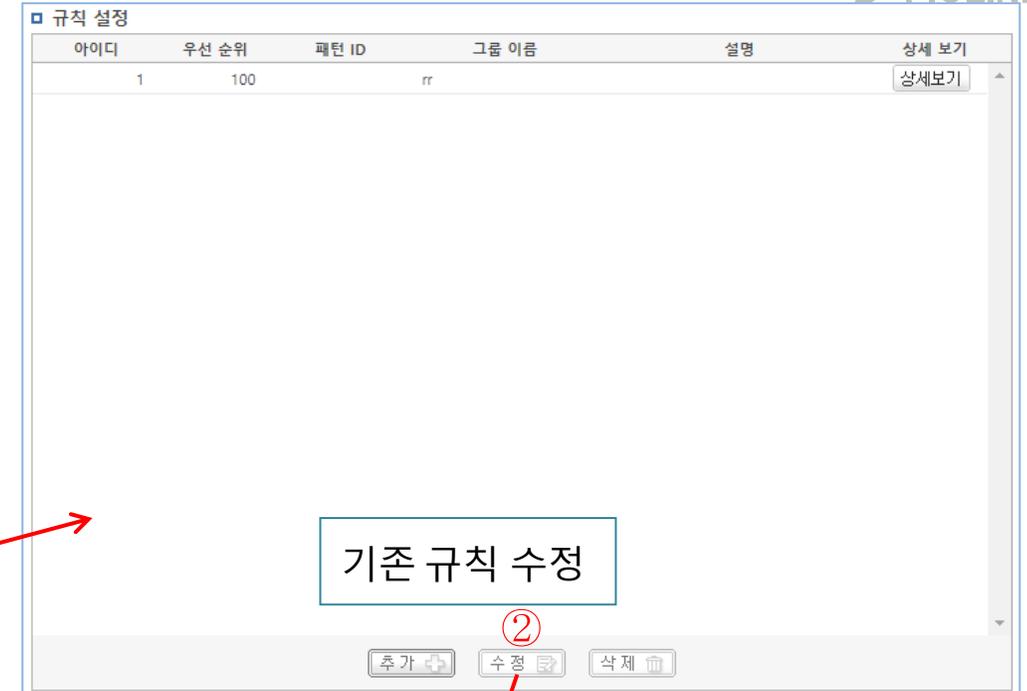
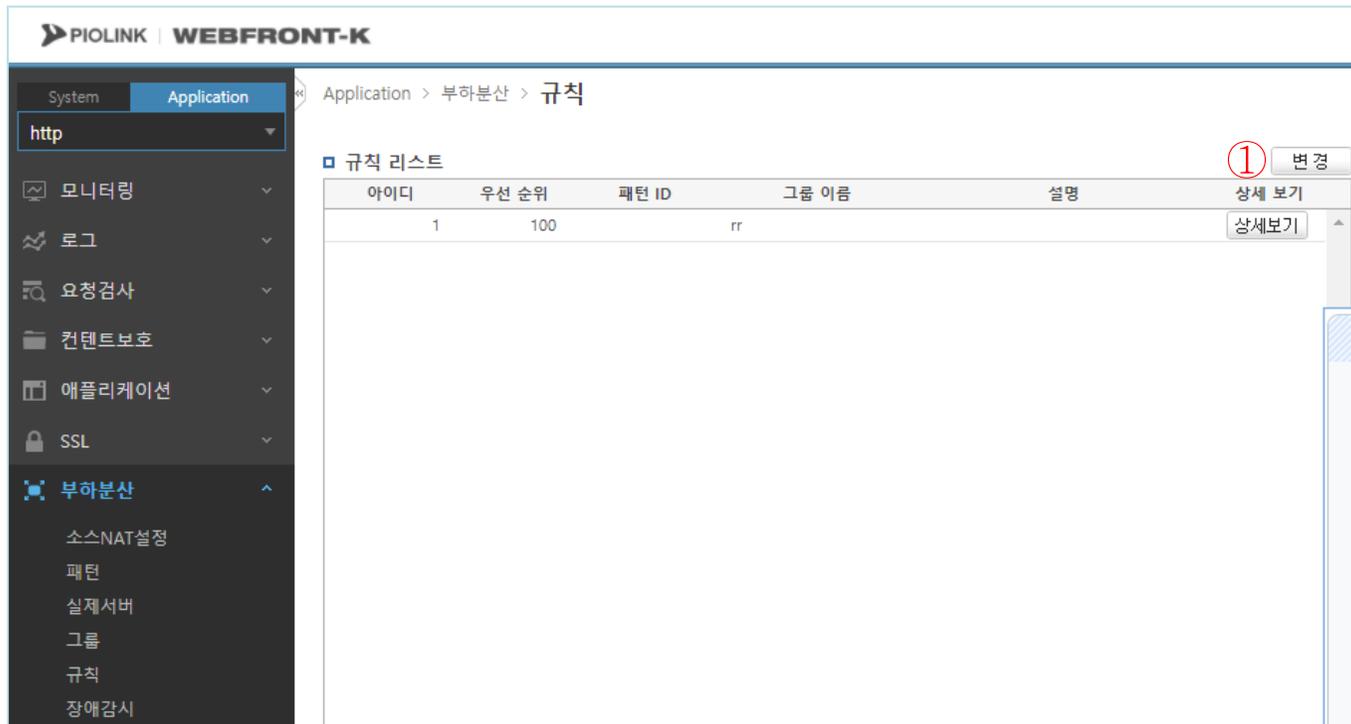
이름	Persist	부하 분산 알고리즘	실제 서버 개수	설명	상세 보기
rr	아이피	라운드 로빈	1		상세보기

규칙 = 그룹 + 패턴(패턴은 설정하지 않아도 무방함)

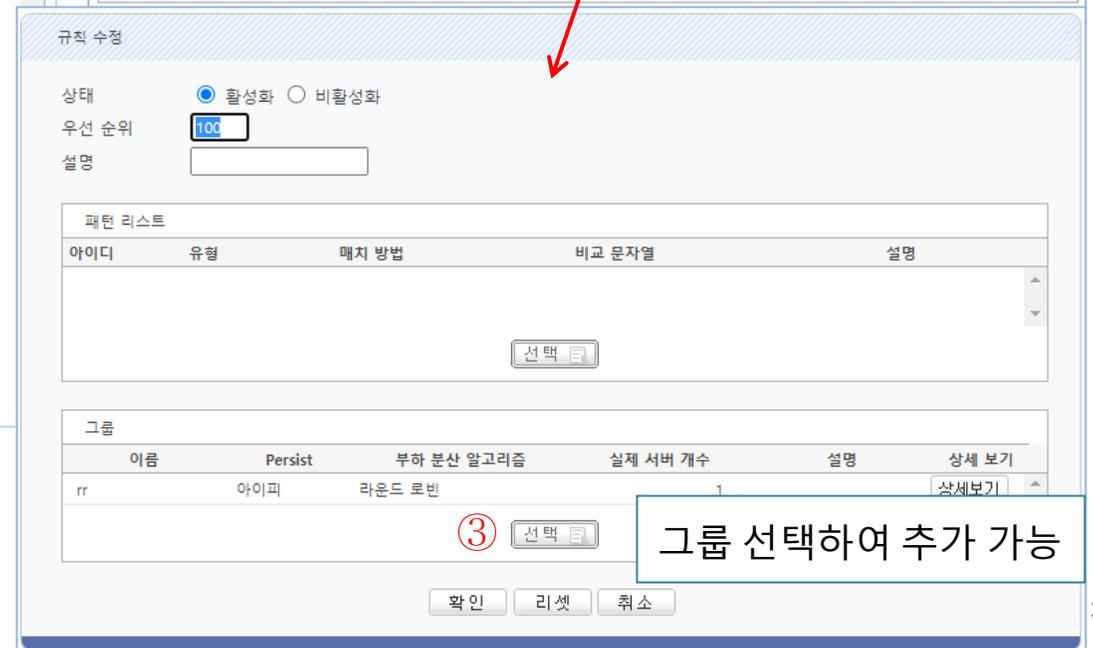
6. 부하분산 - 규칙 설정

• WEBFRONT-KS 기본 구성

- 서버 세션 관련 설정(부하분산)
- 설정 경로: Application > 부하분산 > 규칙



기존 규칙 수정

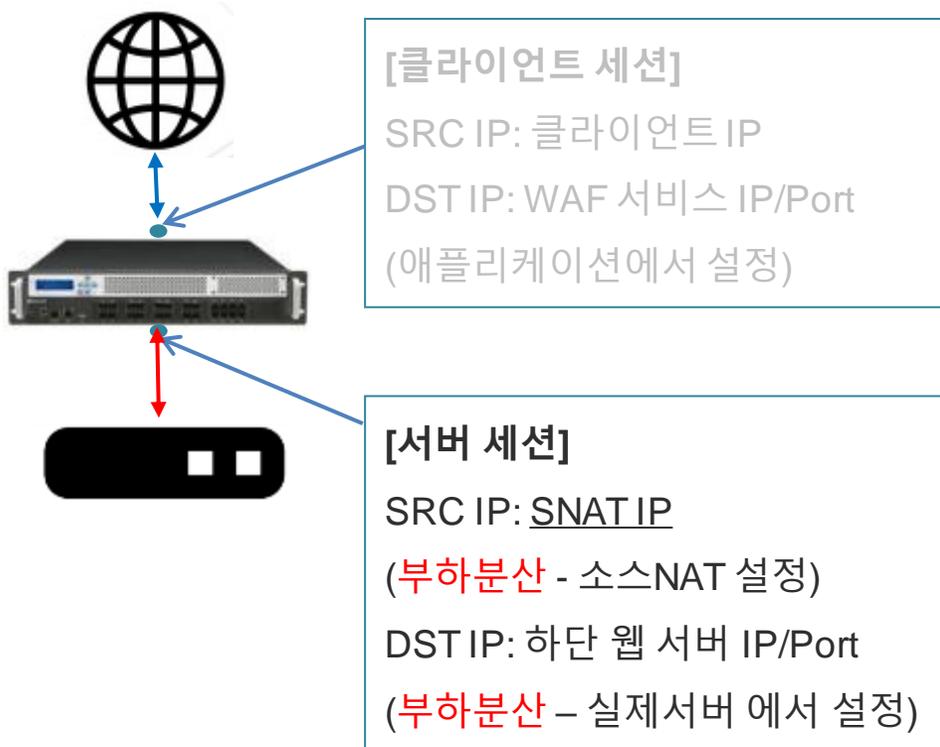


그룹 선택하여 추가 가능

7. 부하분산 - 장애 감시 설정

• WEBFRONT-KS 기본 구성

- 서버 세션 관련 설정(부하분산)
- 설정 경로: Application > 부하분산 > 장애감시



Application > 부하분산 > 장애감시

장애 감시 리스트							
아이디	유형	제한 시간	간격	재시도 횟수	복구 횟수	설명	상세 보기
1	TCP	3	5	3	0		상세보기

헬스체크 유형은 TCP, ICMP, HTTP, HTTPS를 제공
 ※ TCP로 설정 권고

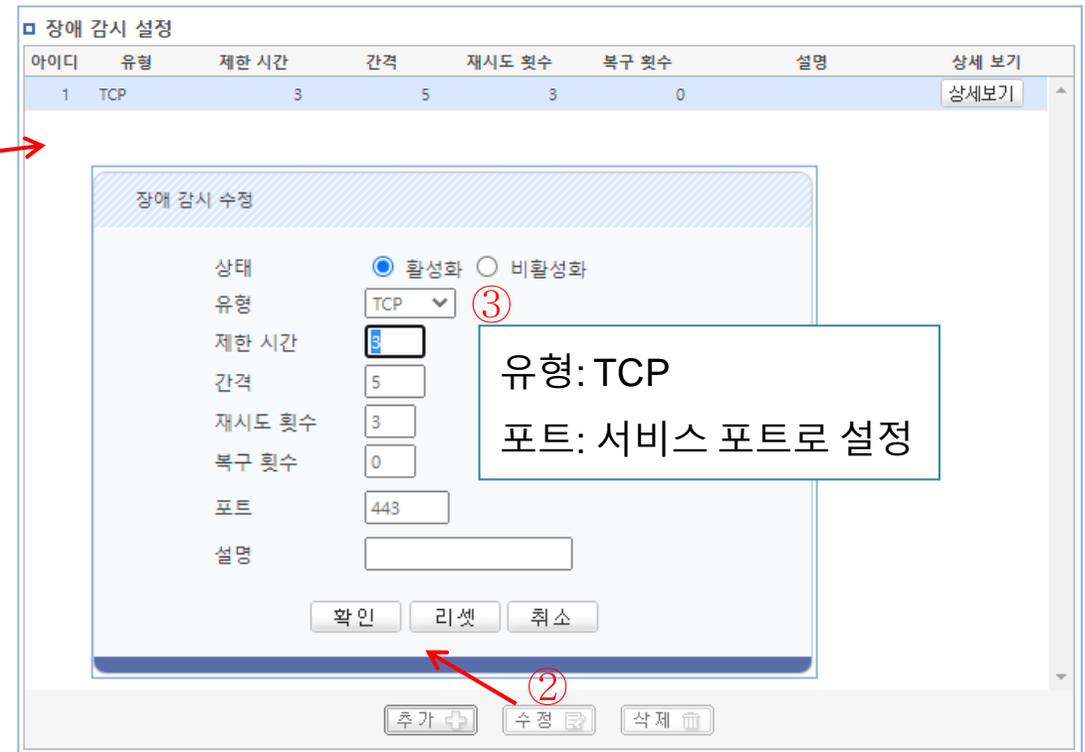
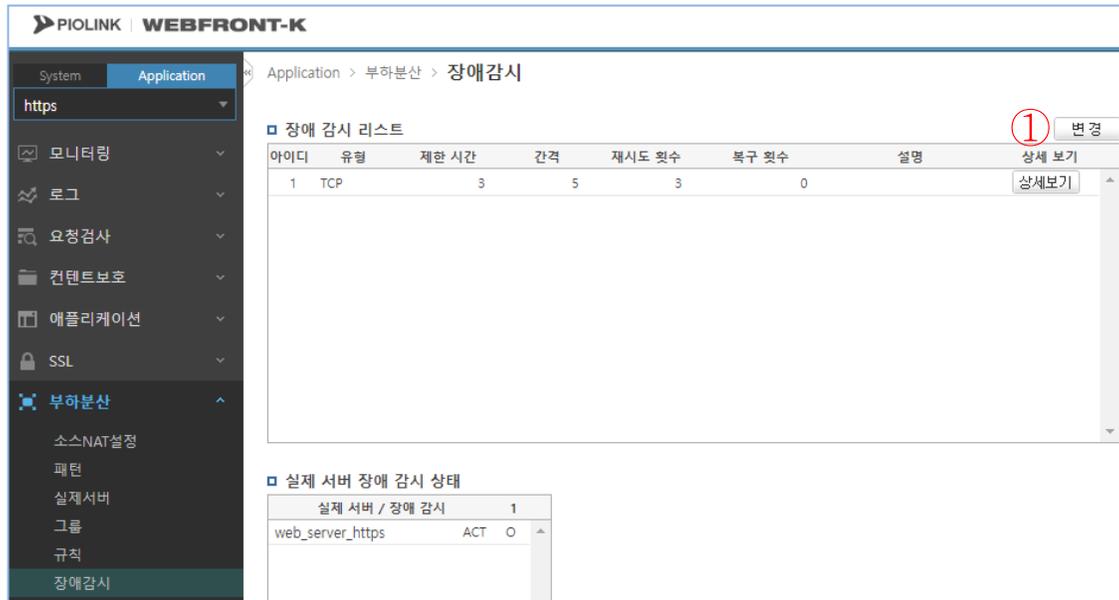
실제 서버 장애 감시 상태	
실제 서버 / 장애 감시	1
web_server_https	ACT ○

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

	상세 보기	다운로드
키	상세보기	다운로드 ↕
인증	상세보기	
인증 요청	상세보기	다운로드 ↕

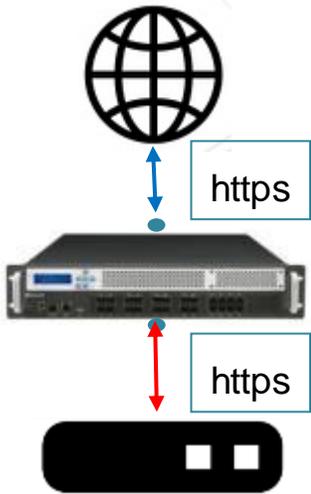
```

Certificate:
Data:
  Version: 1 (0x0)
  Serial Number:
    db:d0:8c:d4:50:14:0c:b2
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: CN=test.com
  Validity
    Not Before: Feb 15 01:52:40 2023 GMT
    Not After : Feb 15 01:52:40 2024 GMT
  Subject: CN=test.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (1024 bit)
    Modulus:
      00:b9:94:bd:cd:7d:15:c9:d5:ad:27:9f:ab:ac:38:
      4a:23:b4:77:92:6f:93:48:d8:2b:14:46:cf:83:c4:
      fb:2c:ad:5d:67:4a:31:ed:73:72:d6:bb:5a:b9:e4:
      f9:5c:78:7e:58:cd:2a:b7:4c:5e:29:44:76:11:c9:
      b3:91:f6:26:5e:31:83:6e:01:1a:33:74:54:a2:3b:
      ad:5a:93:b8:70:f0:78:f2:ed:c7:5f:d4:eb:49:88:
      e5:ae:f1:8f:32:7d:a3:a3:8f:15:50:11:1e:37:81:
      29:55:44:33:d1:ad:3f:82:01:00:03:93:b9:73:e2:
      75:b8:39:23:98:8e:49:a9:fd
    Exponent: 65537 (0x10001)
  Signature Algorithm: sha256WithRSAEncryption
    7e:86:26:37:3f:60:a6:32:a2:9b:20:fc:da:be:47:28:37:35:
    f9:7d:04:9e:a0:89:c5:64:c6:70:ab:1f:28:af:09:de:a2:37:
    24:36:c0:14:81:c5:4d:04:81:36:33:bb:da:04:d1:3b:5d:32:
    de:0f:26:81:2d:49:8d:c4:b5:09:02:ca:9f:56:83:e6:47:5f:
    
```

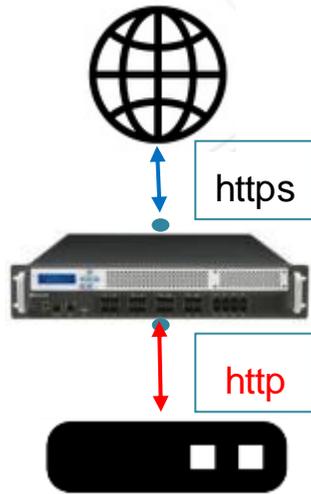
9. SSL 설정

• 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) 활성화로 설정된 경우
 - 웹 트래픽 보안 검사 후, HTTPS로 암호화하여 WEB으로 트래픽 포워딩

2) 비활성화로 설정된 경우
 - 웹 트래픽 보안 검사 후, HTTP로 복호화된 상태로 WEB에 트래픽 포워딩

주의! 로드밸런서와 WEBFRONT-K의 프록시 프로토콜 설정이 상이한 경우 서비스에 문제가 발생합니다.

9. SSL 설정

• SSL 설정

- 설정 경로: Application > SSL > 일반설정

클라이언트 구간

SSL 보안등급: 사용자 정의

SSL 보안등급: B 등급

SSL 프로토콜: A 등급

SSL 암호알고리즘: 사용자 정의

SSL 암호알고리즘: RC4-SHA:RC4-MD5:AES128-SHA:AES256-SHA:ALL:!ADH:!EXPORT

주의! SSL 보안등급에 따라 SSL 프로토콜 및 SSL 암호알고리즘의 변경으로 구형 클라이언트의 연결이 실패 할 수 있습니다.

SSL 보안등급: A등급으로 설정

- A등급으로 설정하면 안전한 cipher suite를 통해 TLSv1.2로 통신 가능

PIOLINK | WEBFRONT-K

Application > SSL > 일반설정

SSL

상태: 활성화

Server Name Indication: 활성화로 설정

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

Server Name Indication: 활성화

SSL 고급설정

클라이언트 구간

SSL 보안등급: 사용자 정의

SSL 프로토콜: SSLv3 TLSv1 TLSv1.1 TLSv1.2

SSL 암호알고리즘: RC4-SHA:RC4-MD5:AES128-SHA:AES256-SHA:ALL:!ADH:!EXPORT

SSL 취약점 진단 사이트(ssllabs.com)

주의! 로드밸런서와 WEBFRONT-K의 프록시 프로토콜 설정이 상이한 경우 서비스에 문제가 발생합니다.

9. SSL 설정

• SSL 설정

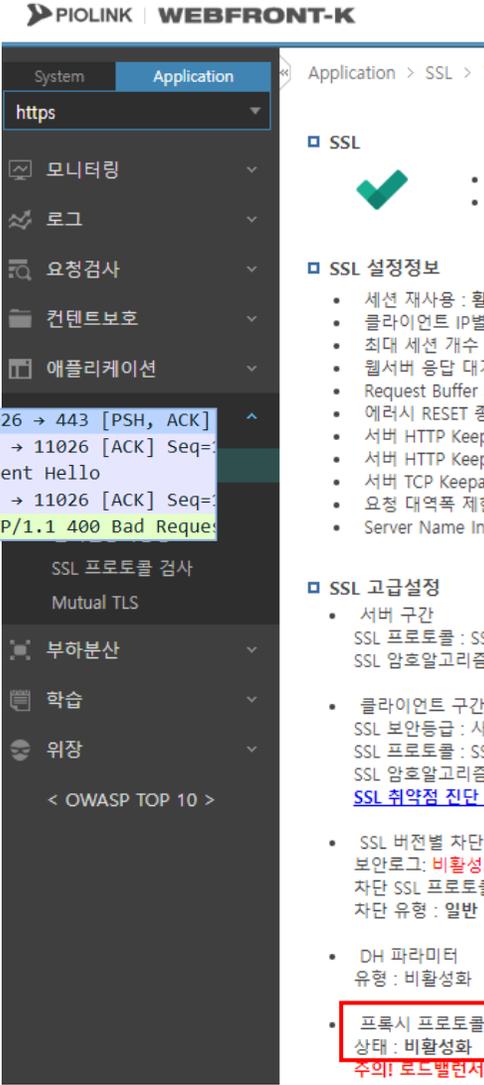
- 설정 경로: Application > SSL > 일반설정

프록시 프로토콜 활성화: WAF에서 SSL 핸드셰이크 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 Request

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:
 HTTPS트래픽 처리 시 client IP 전달 여부 설정

- 상단에 LB가 있을 경우
 >> LB와 WAF 모두 **활성화**로 설정
- 상단에 LB가 없을 경우
 >> WAF에서 **비활성화**로 설정

1-1) 상단 LB가 있을 때, 활성화로 설정된 경우
 - WAF 상단에서 SSL 핸드셰이크 이전에 proxyv1 패킷을 통해 client IP 전달

1-2) 상단 LB가 있을 때, 비활성화로 설정된 경우
 - WAF 상단에서 client IP 전달 안 함 (client IP 식별 불가)

주의! 로드밸런서와 WEBFRONT-K의 프록시 프로토콜 설정이 상이한 경우 서비스에 문제가 발생합니다.

10. SSL, 애플리케이션 및 소스 NAT 활성화

• SSL, 애플리케이션 활성화

- 설정 경로: Application > SSL > 일반설정

SSL 상태 활성화 시, 애플리케이션의 상태도 함께 활성화됨

Application > SSL > 일반설정

SSL

- 상태 : 비활성화
- 백엔드 : 비활성화

SSL 설정정보

- 세션 재사용 : 활성화
- 클라이언트 IP별 세션 재사용 : 비활성화
- 최대 세션 개수 : 30000
- 웹서버 응답 대기시간 : 600 초
- Request Buffer Size : 1M
- 에러시 RESET 종료 : 비활성화
- 서버 HTTP Keepalive 조건 : client_ip + server_ip + server_port
- 서버 HTTP Keepalive 제한 시간 : 60 초
- 서버 TCP Keepalive : 비활성화
- 요청 대역폭 제한 : 비활성화
- Server Name Indication : 활성화

변경

SSL 상태 설정

상태

백엔드

② 활성화 비활성화

② 활성화 비활성화

③ 적용 리셋 취소

Application > SSL > 일반설정

SSL

- 상태 : 활성화
- 백엔드 : 활성화

SSL 설정정보

- 세션 재사용 : 활성화
- 클라이언트 IP별 세션 재사용 : 비활성화
- 최대 세션 개수 : 30000
- 웹서버 응답 대기시간 : 600 초
- Request Buffer Size : 1M
- 에러시 RESET 종료 : 비활성화
- 서버 HTTP Keepalive 조건 : client_ip + server_ip + server_port
- 서버 HTTP Keepalive 제한 시간 : 60 초
- 서버 TCP Keepalive : 비활성화
- 요청 대역폭 제한 : 비활성화
- Server Name Indication : 활성화

변경

10. SSL, 애플리케이션 및 소스 NAT 활성화

• 소스NAT 활성화

- 설정 경로: Application > 부하분산 > 소스NAT설정

PIOLINK WEBFRONT-K

System Application Application > 부하분산 > 소스NAT설정

소스 NAT 상태 ① 변경

상태: 비활성화

소스 NAT IP 리스트 변경

IP 주소	설명
192.168.0.123	SNAT IP

소스 NAT 상태 설정

상태 ② 활성화 비활성화

③ 적용 리셋 취소

System Application Application > 부하분산 > 소스NAT설정

소스 NAT 상태 ① 변경

상태: 활성화

소스 NAT IP 리스트 변경

IP 주소	설명
192.168.0.123	SNAT IP

11. 설정 저장

• 설정 저장

– 설정 경로: System > 일반설정 > 설정 관리

PIOLINK | WEBFRONT-K

System > 일반설정 > 설정 관리

- 현재 설정 다운로드
 시스템의 현재 설정을 다운로드하여 로컬 하드 드라이브에 저장합니다.
- 설정 자동 백업
 현재의 설정을 다운로드하여 자동백업합니다.
- 설정 자동 저장
 • 상태: 비활성화
 • 주기: 24 시
 현재 설정을 "다음부팅시사용" 저장공간에 자동으로 저장합니다.
- 설정 저장 리스트

저장공간	상태	설명
# 1	최근 부팅에 사용되었으며 다음 부팅시에도 사용됨	2023/02/15 13:34
<input type="button" value="전체 설정 동기화"/> <input type="button" value="다시저장"/> <input type="button" value="업로드"/> <input type="button" value="다운로드"/> <input type="button" value="다음부팅시사용"/> <input type="button" value="설정적용"/> <input type="button" value="삭제"/>		
# 2	사용되지 않음	
<input type="button" value="전체 설정 동기화"/> <input type="button" value="저장"/> <input type="button" value="업로드"/>		
# 3	사용되지 않음	
<input type="button" value="전체 설정 동기화"/> <input type="button" value="저장"/> <input type="button" value="업로드"/>		

현재설정 저장

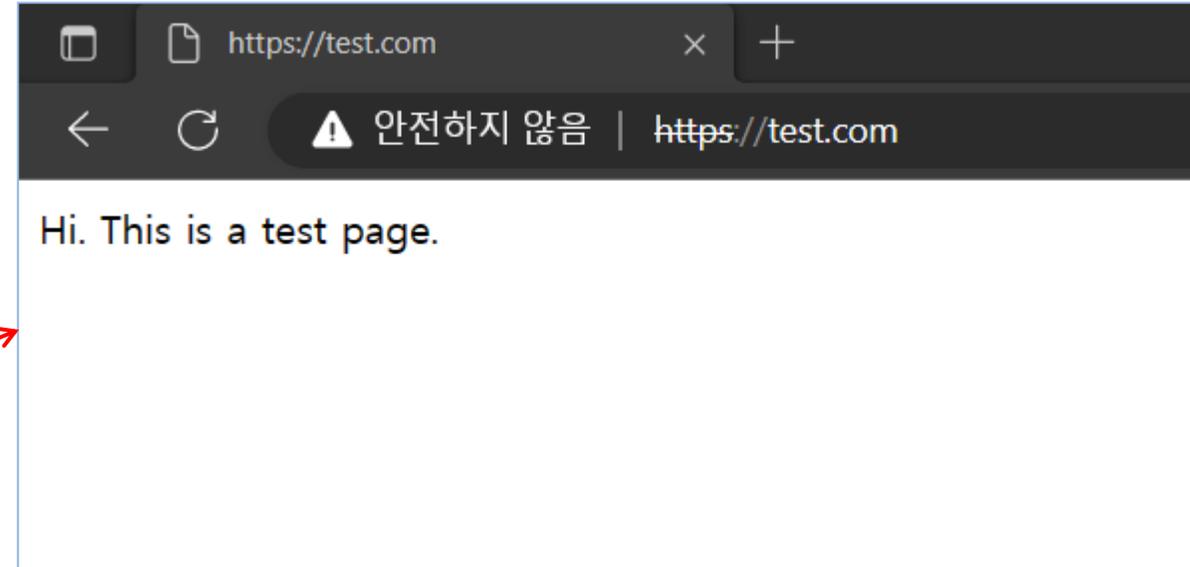
저장공간 설명

12. 웹 서비스 확인

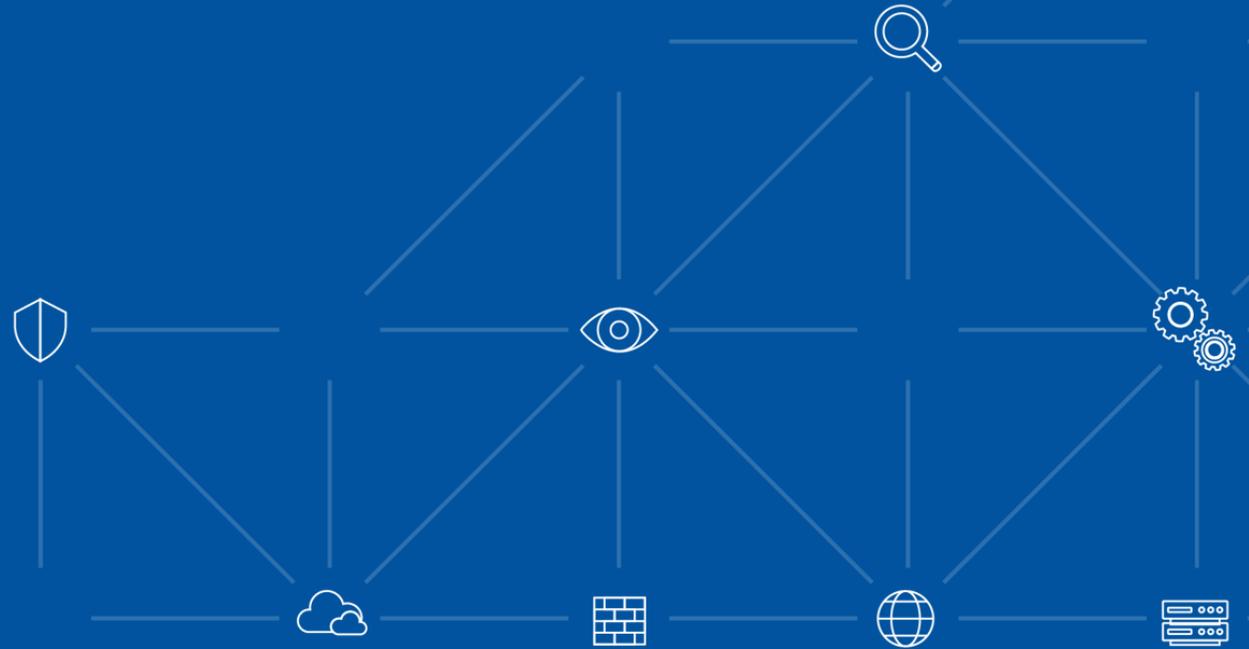
• WEBFRONT-KS 설정 완료 후 통신 가능여부 확인

- 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
```



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



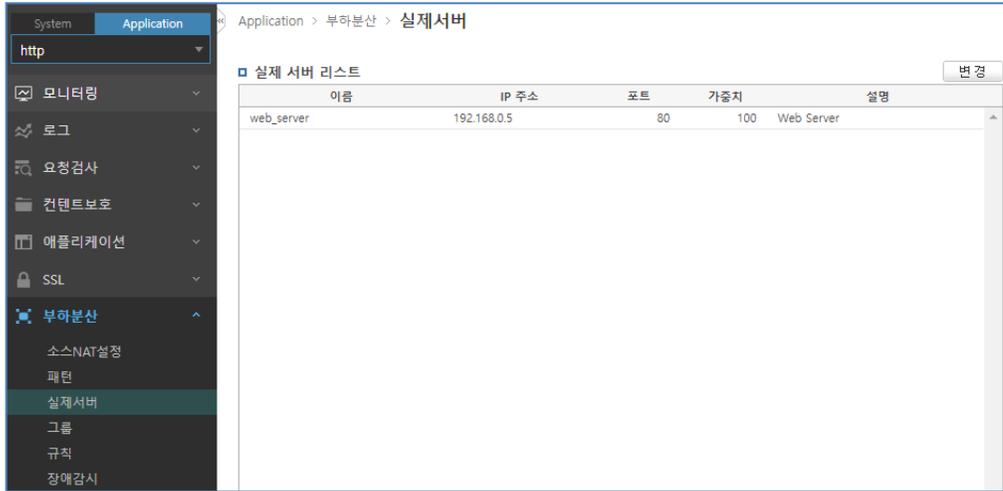
- ✓ 소스 NAT **상태 활성화** 여부
- ✓ 소스 NAT **IP 등록** 여부

1. HTTP

• WEBFRONT-KS 설정 체크

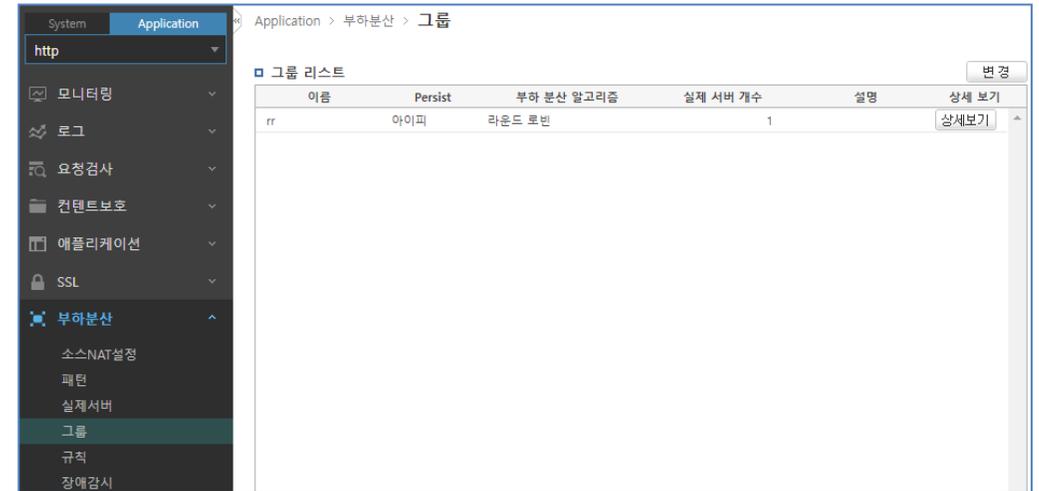
- 웹방화벽으로서 기능하기 위한 최소한의 설정 상태 체크

실제 서버 설정



- ✓ 실제서버 IP/Port 정상 등록 여부

그룹 설정



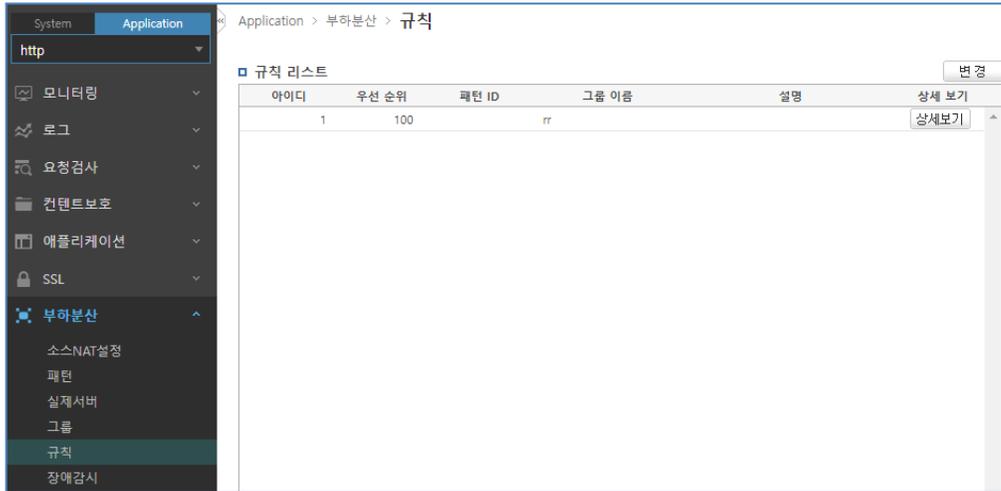
- ✓ 그룹에 등록된 실제 서버 개수 확인
- ✓ Persist 설정 확인

1. HTTP

• WEBFRONT-KS 설정 체크

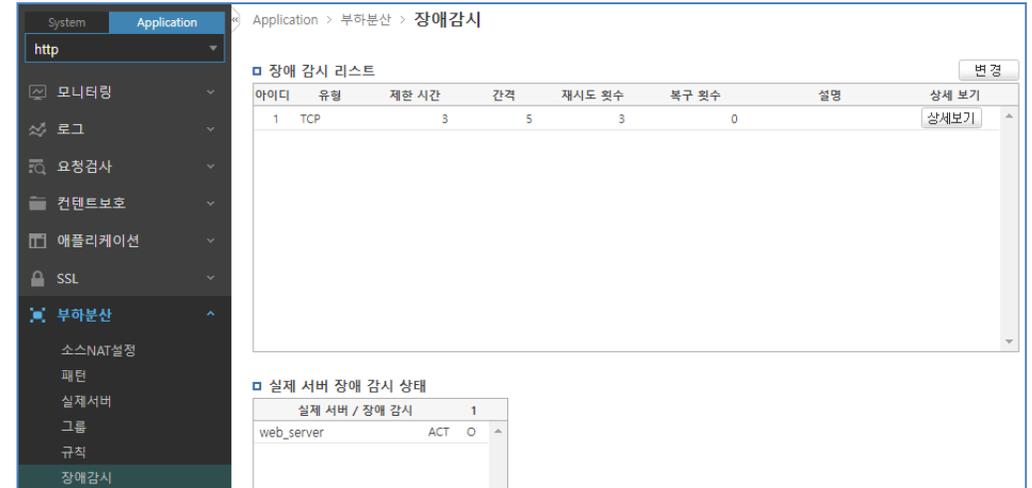
– 웹방화벽으로서 기능하기 위한 최소한의 설정 상태 체크

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

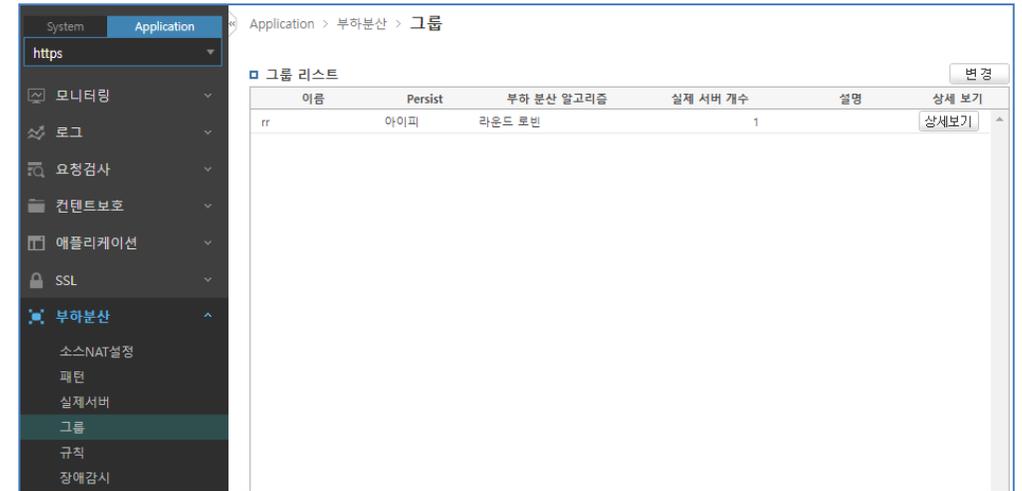
- 웹방화벽으로서 기능하기 위한 최소한의 설정 상태 체크

실제 서버 설정



- ✓ 실제서버 IP/Port 정상 등록 여부

그룹 설정



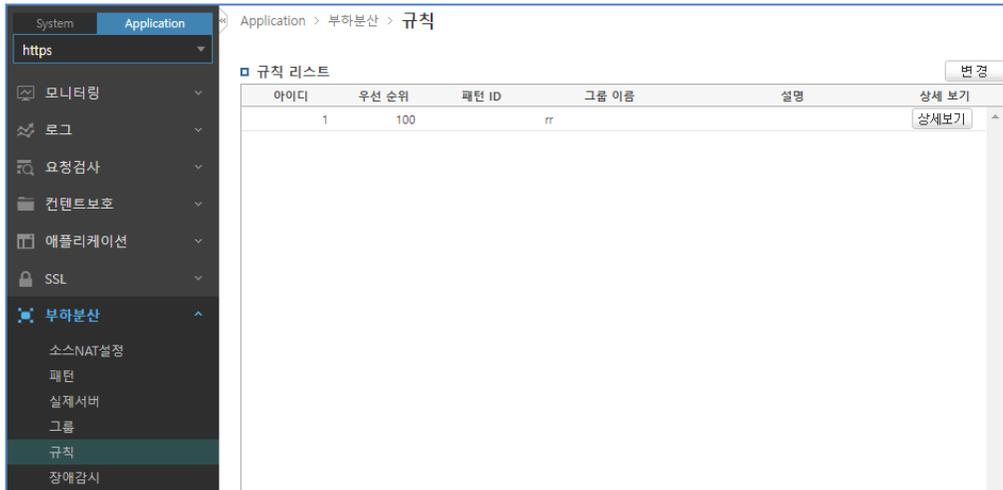
- ✓ 그룹에 등록된 실제 서버 개수 체크
- ✓ Persist 설정 확인

2. HTTPS

• WEBFRONT-KS 설정 체크

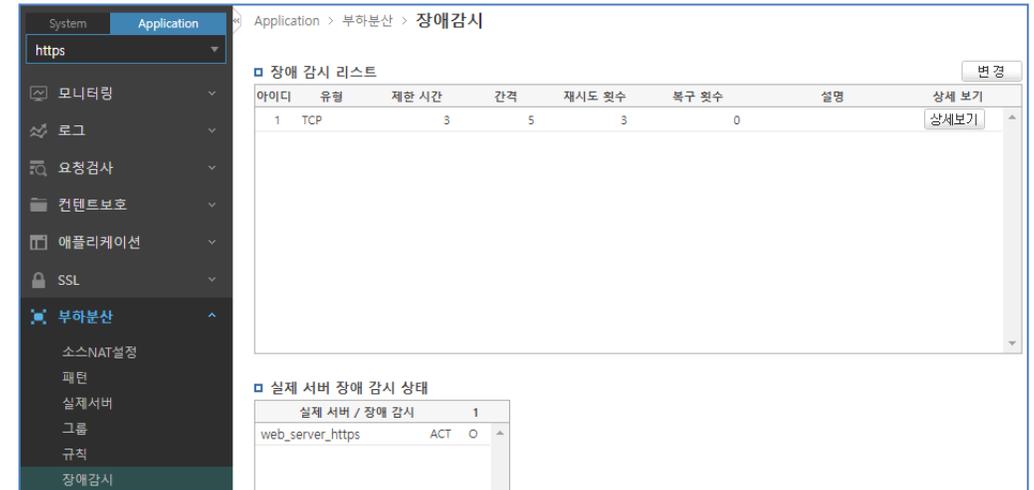
- 웹방화벽으로서 기능하기 위한 최소한의 설정 상태 체크

규칙 설정



- ✓ 규칙 내에 그룹 등록 여부

장애 감시 설정



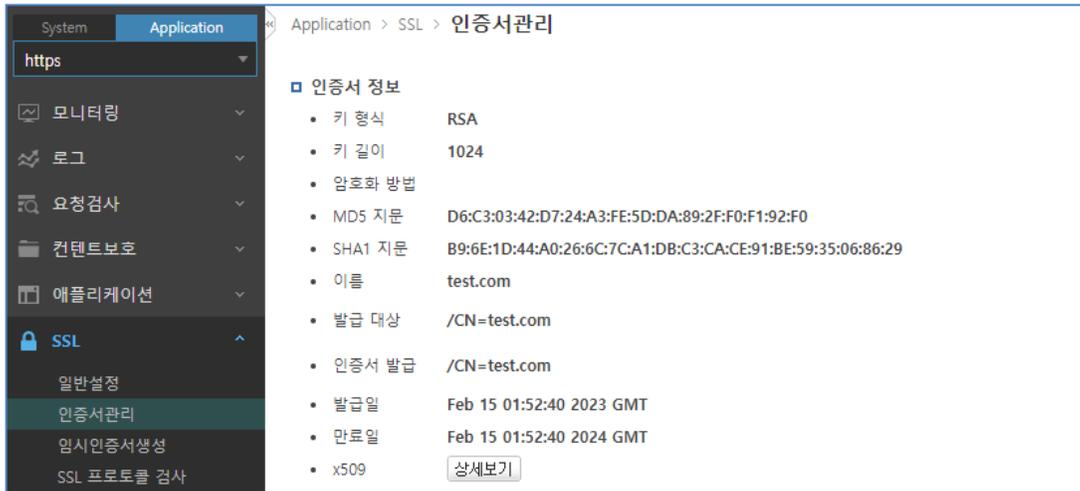
- ✓ 장애 감시 프로토콜의 tcp 설정 여부
- ✓ 장애 감시 tcp 포트 설정 확인
- ✓ 장애 감시 상태의 정상 여부

2. HTTPS

• WEBFRONT-KS 설정 체크

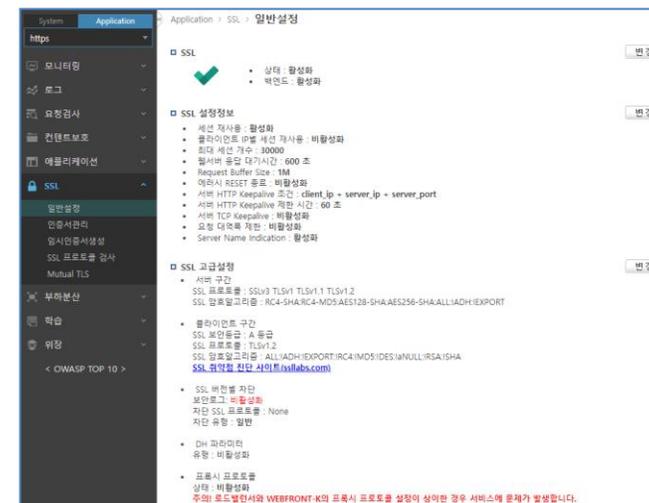
– 웹방화벽으로서 기능하기 위한 최소한의 설정 상태 체크

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



(주) 파이오링크

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