

웹 보안에 최고 성능을 담다

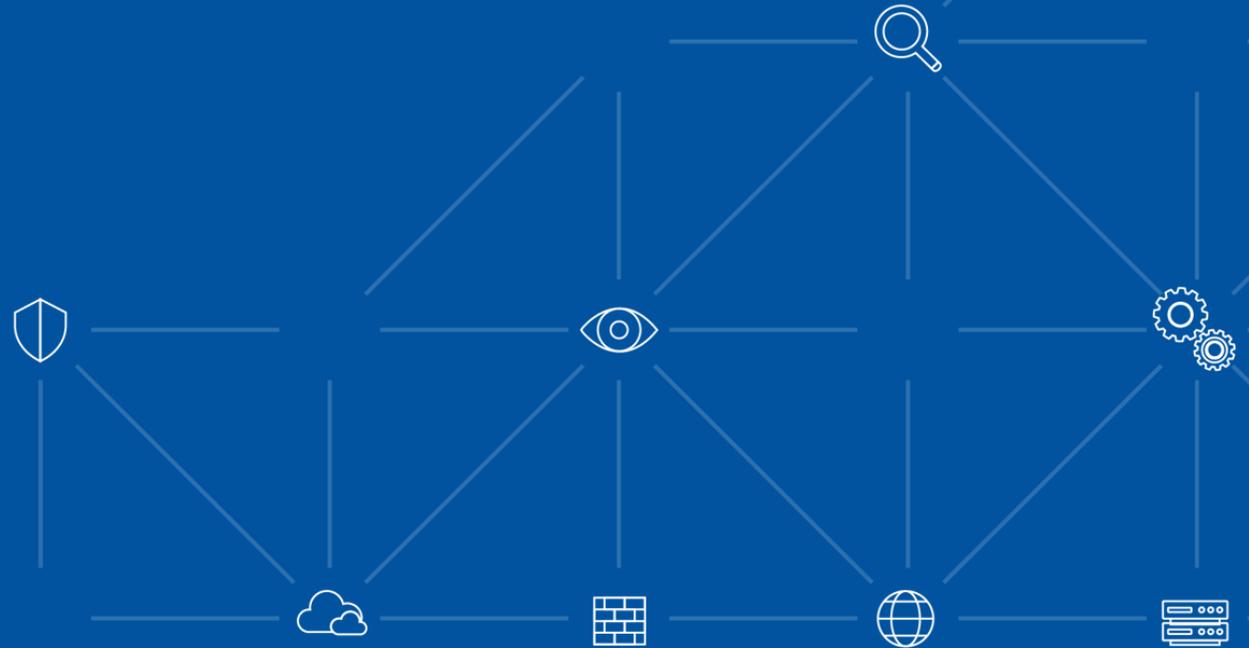
WEBFRONT-KS

(주)파이오링크



개요

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



1. WEBFRONT-KS



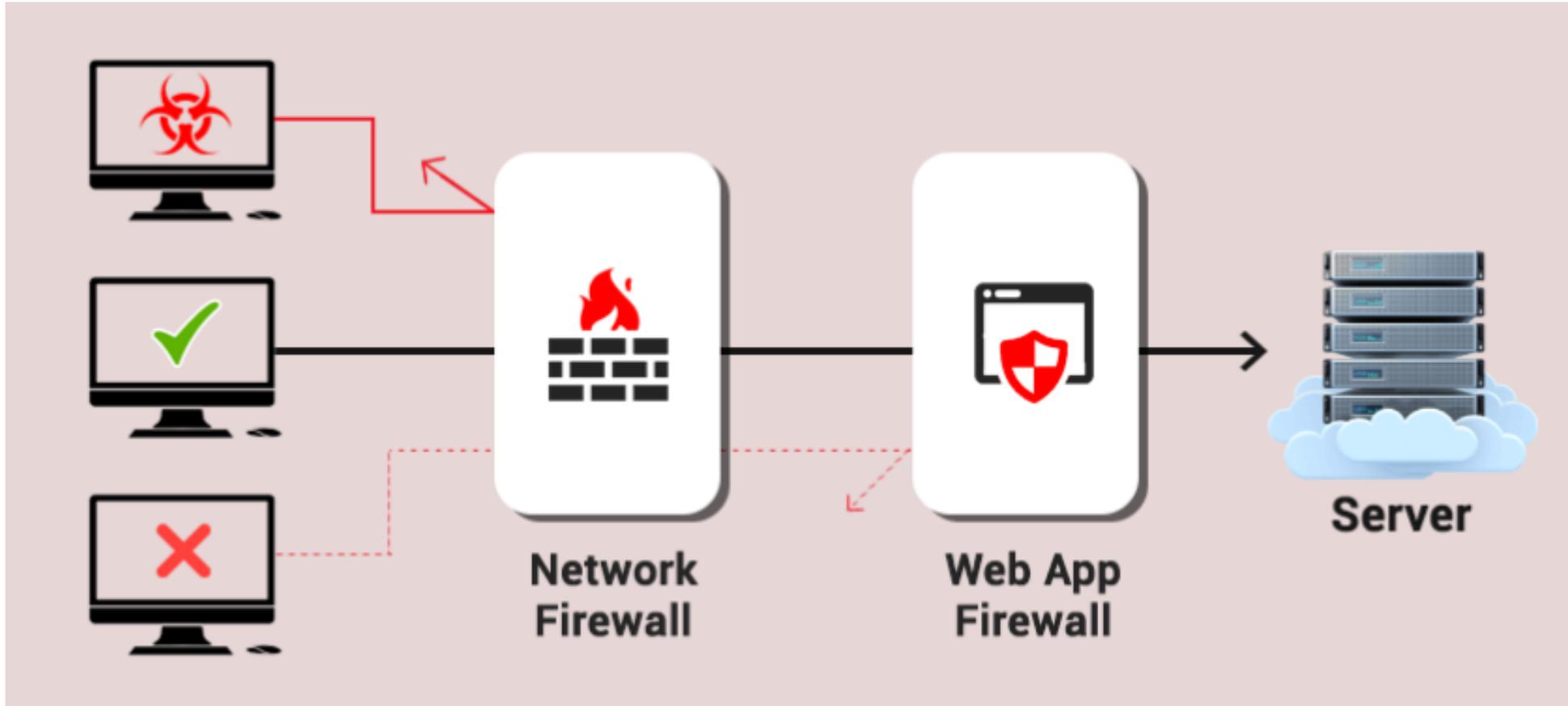
웹방화벽이란?

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

웹방화벽이란?



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

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



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)

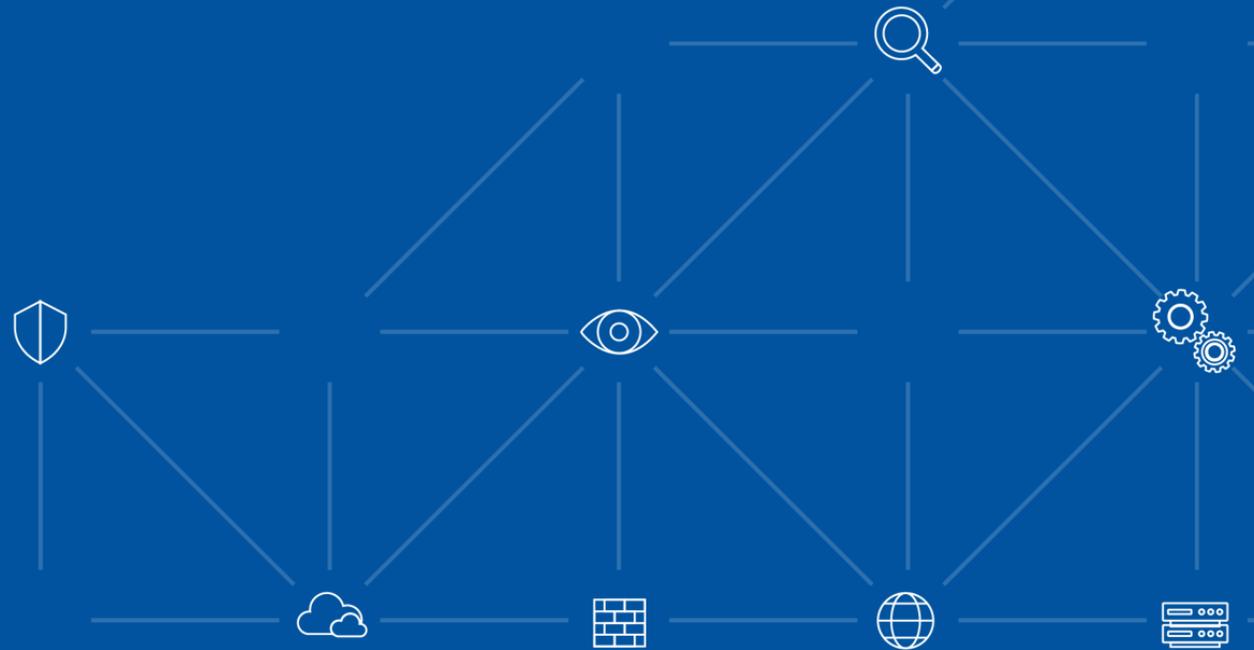


2) 응답검사

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



2. 메뉴 설명



WEBFRONT-KS 메뉴

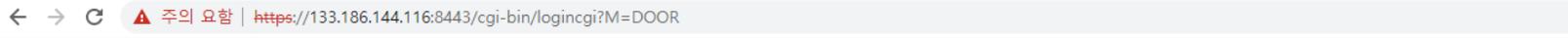
WEBFRONT-KS 메뉴

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



v2.0.61.0.23

로그인

아이디와 비밀번호를 입력하여 주세요.

확인

© PIOLINK WEB Application Firewall

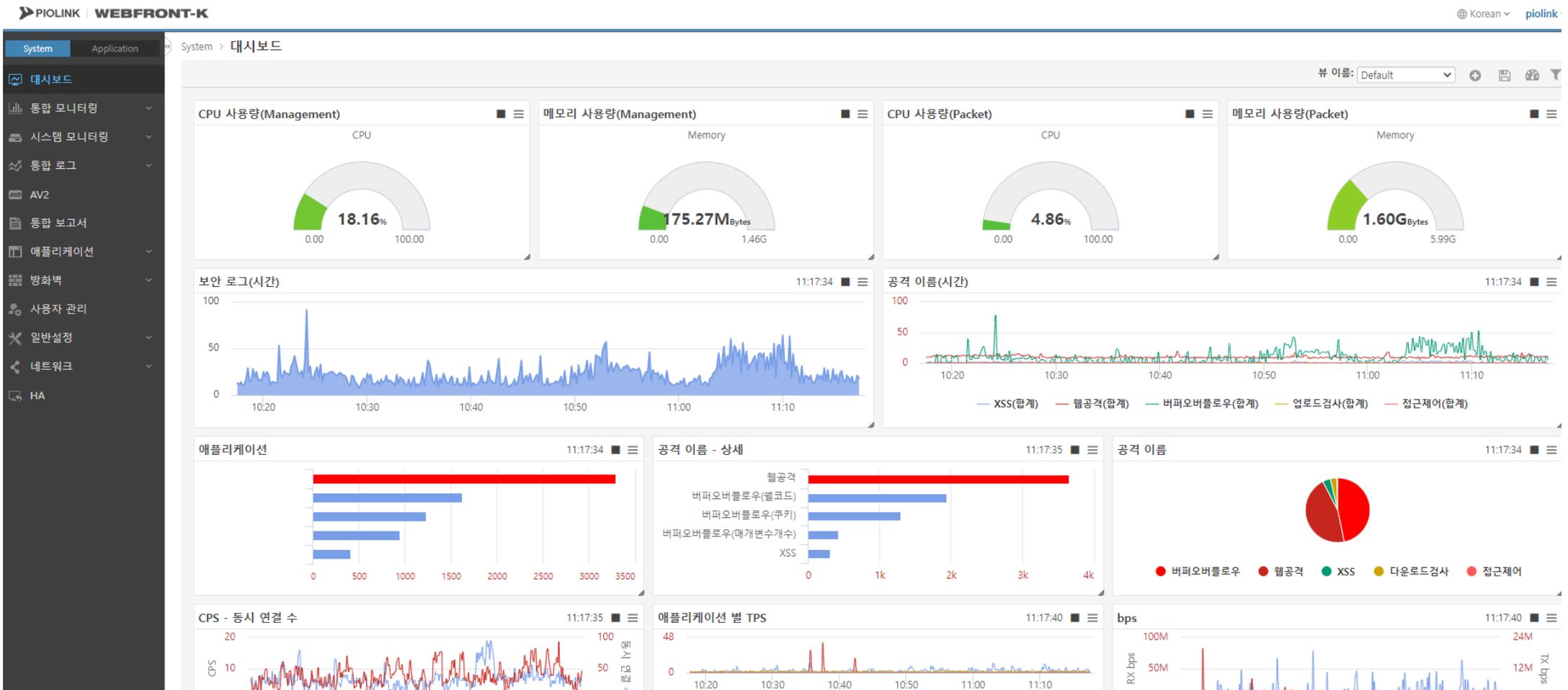
🌐 Korean ▾

WEBFRONT-KS 메뉴

WEBFRONT-KS 메뉴

대시보드

장비의 전반적인 하드웨어 상태 및 보안 현황을 시각화 하여 표기함



WEBFRONT-KS 메뉴

WEBFRONT-KS 메뉴

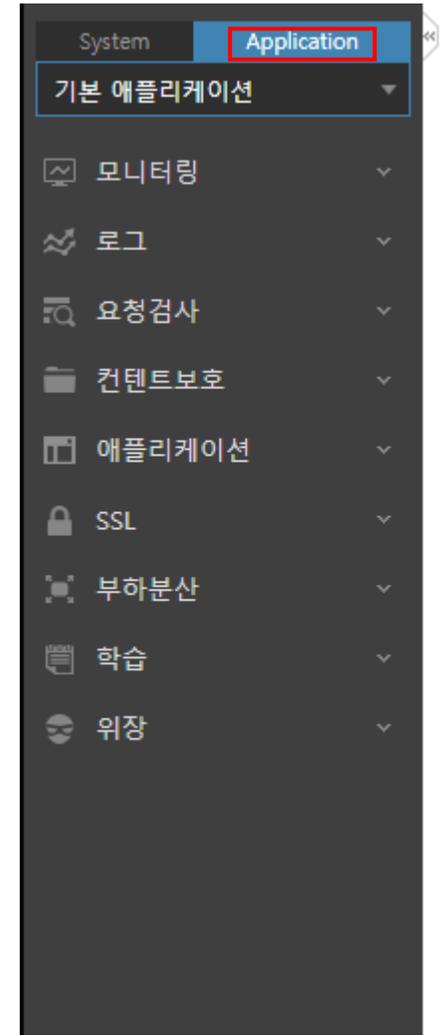
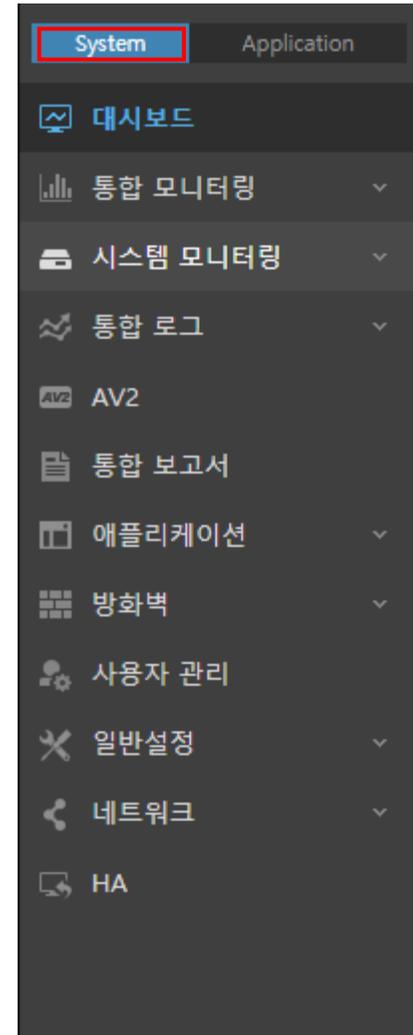
기본 메뉴

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)

PIOLINK | WEBFRONT-K "다음부팅시사용" 저장공간과 현재 설정이 다릅니다.(설정 관리) Korean wfadmin

System > 통합 로그 > 보안로그

필터 > 최근 1 일 실시간 > 애플리케이션 > 공격 > 내보내기 > 초기화 > 저장 > 적용

날짜	공격 이름	애플리케이션	SIG 위험도	공격 위험도	호스트	URL	클라이언트 IP/PORT	서버 IP/PORT	국가	대응
2020/11/16 15:20:07	웹 공격	https3		중간						탐지
2020/11/16 11:28:22	웹 공격	https3		중간						탐지
2020/11/16 10:44:45	웹 공격	https3		중간						탐지
2020/11/16 10:43:44	웹 공격	https3		중간						탐지
2020/11/16 09:31:33	웹 공격	https3		중간					USA	탐지
2020/11/16 09:30:27	웹 공격	https3		중간					USA	탐지
2020/11/16 07:34:42	웹 공격	https3		중간						탐지
2020/11/15 22:31:58	웹 공격	https3		중간					USA	탐지

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

System > 애플리케이션 > 시그니처관리

■ 시그니처 버전

- 현재 시그니처 버전: 4.26

■ 시그니처 리스트

- 보안레벨: 높음 [사용자]
(의심가는 접근 전체를 차단하지만 일부 정상접근도 차단 될 수 있습니다.)

접근제어 - 차단URL

시그니처 ID	시그니처 정보	위험도	차단	탐지	예외
ACC-00001	설명 : .htaccess 액세스 공격	하	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACC-00002	설명 : /architext_query.pl	하	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACC-00003	설명 : /blabla.ida	상	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACC-00004	설명 : /cgi-bin/global.cgi 취약점	하	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACC-00005	설명 : /etc/.rhosts 시스템 파일 접근공격	상	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACC-00006	설명 : /etc/hosts 시스템 파일 접근공격	상	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACC-00007	설명 : /etc/passwd시스템 파일 접근공격	상	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACC-00008	설명 : /sam 샘플일 추출 공격1	하	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACC-00009	설명 : /sam 샘플일 추출 공격2	하	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACC-00010	설명 : /sam 샘플일 추출 공격3	하	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACC-00011	설명 : /test/jsp/declaration/IntegerOverflo접근공격	하	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACC-00012	설명 : /test/jsp/pagelsErrorPage.* 접근공격	하	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACC-00013	설명 : /test/jsp/pagelsThreadSafe.* 접근공격	하	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACC-00014	설명 : /test/jsp/pageSession.* 접근공격	하	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACC-00015	설명 : /././././winnt/win.ini 접근 취약점	하	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACC-00016	설명 : 검색 robots 접근 공격	중	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

■ 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 실패할 경우 해당 계정으로 로그인 불가
통합 관리자만 해제 가능

System > 사용자 관리

- 중복 로그인 허용 설정
 - 계정별 중복 로그인: 허용
 - 설정 변경 사용자의 중복 로그인: 허용
- 계정 관리 설정
 - 최근 사용 패스워드 제한: 비활성화
 - 미 사용 계정 만료: 비활성화
 - 패스워드 변경 주기 확인: 비활성화
 - 최대 로그인 실패 횟수 초과 시 자동 잠금 해제: 비활성화
- Default User 관리 설정
 - 현재 Default User: wfadmin
- Radius 관리 설정
 - SSH: 비활성화
 - Telnet: 비활성화
 - Console: 비활성화
 - 기본 서버 IP:
 - 보조 서버 IP:
 - 인증 키:
 - 포트: 1812
 - Retry: 3
 - 제한 시간: 3

사용자 리스트

사용자 ID	그룹	현재 로그인 실패 횟수	최대 로그인 실패 횟수	설명	상세 보기
wfadmin	통합 관리자	0	10	Default User	상세보기

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

System > 통합 로그 > 통합 로그설정

로그 레벨

- 레벨 : Notice

로그 삭제 용량

- 최대 용량 : 90 %
- 경보 용량 : 80 %
- 삭제 목표 용량 : 70 %

시스로그 포맷

- 시스로그 포맷 : %TIMESTAMP% %\$year% <%pri%>

시스로그 서버 리스트

IP 주소	포트	프로토콜	레벨

사용자 정의 보안로그

System > 통합 로그 > 통합 로그설정

사용자 정의 보안로그

지원 리스트

필드
url_param
forwarded_for
sigid
sig_warning
block
owasp
detected_time
desc
field
data
raw_length
raw_data

추가 ➔

삭제 🗑

Delimiter :

로그 예제 : [WEBFRONT/0x007xxxx] Event String (log_id="value", app_id="value", app_name="value", src_ip="value", src_port="value", dest_ip="value", dest_port="value", host="value", url="value", url_param="value", data="value", sigid="value", sig_warning="value", block="value", owasp="value", detected_time="value",)

변경

보안로그 형식

필드
log_id
app_id
app_name
src_ip
src_port
dest_ip
dest_port
host
url
url_param
data
sigid

WEBFRONT-KS 메뉴

WEBFRONT-KS 메뉴

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

System Application

test

- 모니터링
- 로그
- 요청검사**
 - 접근제어
 - 디렉토리 리스팅 차단
 - 검사회피 차단
 - 버퍼오버플로우 차단
 - 요청형식 검사
 - 쿠키 보호
 - 웹 공격 프로그램 차단
 - SQL 삽입 차단
 - 스크립트 삽입 차단
 - 인클루드 인젝션 차단
 - 신용카드 정보 유입 차단
 - 주민등록 정보 유입 차단
 - 다운로드 검사
 - 폼 필드 검사
 - 금칙어 차단
 - 업로드 검사
 - Smuggling 공격 차단
 - HTTP POST 공격 차단
 - Slowloris 공격 차단
 - Slow Read 공격 차단
 - 과다 요청 제어
 - WISE 요청 필터
 - 화이트리스트

Application > 요청검사 > 접근제어

□ 애플리케이션 접근제어 변경

- 보안로그 : 활성화
- 차단 : 비활성화
- 학습 : 비활성화
- 블랙리스트 : 비활성화

□ 허용 URL 리스트 변경

허용 URL	설명
/*	

□ 고급 애플리케이션 접근 제어 변경

- URL 정규식 검사 : 활성화
- 시작 URL 접근 제어 : 비활성화
- 고급 접근 제어 : 비활성화
- 국가별 접근 제어 상태 : 비활성화
- 접근로그 : 비활성화
- 확장자 없는 URL 허용 : 비활성화

WEBFRONT-KS 메뉴

WEBFRONT-KS 메뉴

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

Application > 애플리케이션 > 일반설정

test

모니터링
로그
요청검사
콘텐츠보호
애플리케이션
일반설정
응답설정
기타설정
캐시설정
ICAP설정
GZIP 설정
Active 미러링 설정
SSL
부하분산
학습
위장
< OWASP TOP 10 >

애플리케이션

애플리케이션

상태 : 비활성화

애플리케이션 일반 설정 정보

- 모드: 일반(고속)
- 도메인 무시: 비활성화
- 압축 방지: 비활성화
- 클라이언트 MSS: 1460
- 서버 MSS: 0
- CPS 제한: 비활성화
- 동시세션 제한: 비활성화
- BPS 제한: 비활성화

애플리케이션 도메인 리스트

도메인 이름	설명

애플리케이션 IP/포트 리스트

IP 버전	IP 주소	포트	IP 트랜스패런트	유형	설명

예외 IP/포트 정보

클라이언트 IP 주소	클라이언트 포트	서버 IP 주소	서버 포트	설명

2. 메뉴 설명

WEBFRONT-KS 메뉴

WEBFRONT-KS 메뉴

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

System Application Application > SSL > 일반설정

test

- 모니터링
- 로그
- 요청검사
- 컨텐츠보호
- 애플리케이션
- SSL**
 - 일반설정
 - 인증서관리
 - 임시인증서생성
 - SSL 프로토콜 검사
 - Mutual TLS
- 부하분산
- 학습
- 위장
- < OWASP TOP 10 >

SSL

- 상태 : 비활성화
- 백엔드 : 비활성화

SSL 설정정보

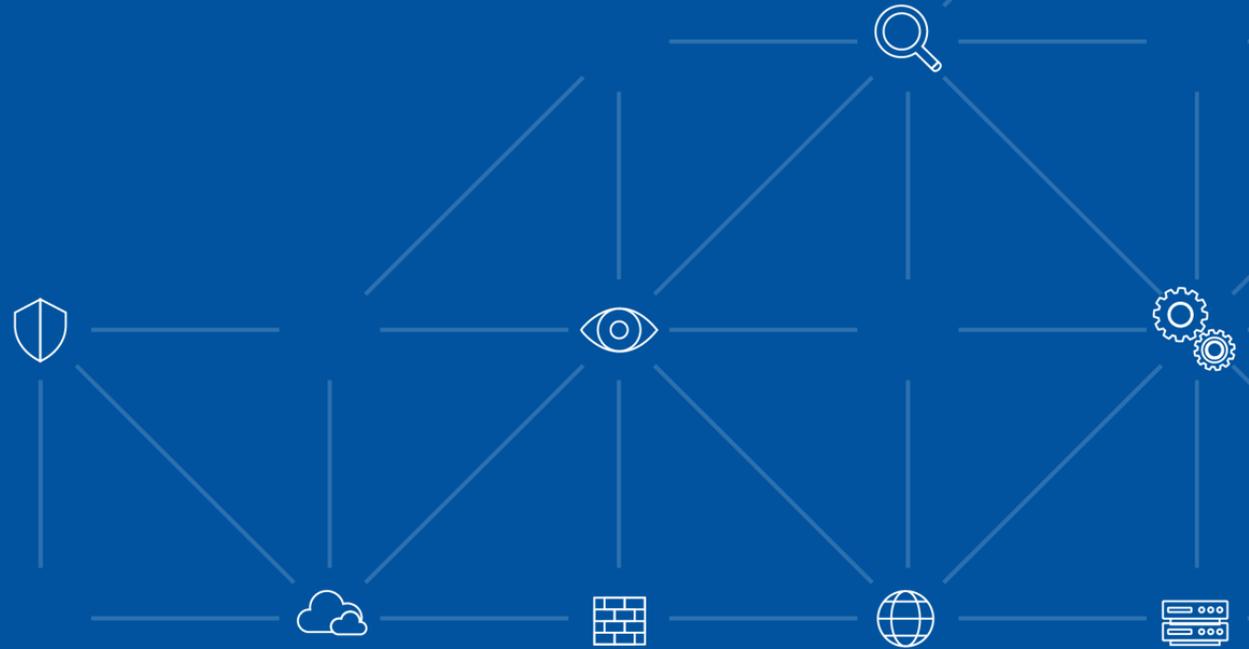
- 세션 재사용 : 활성화
- 클라이언트 IP별 세션 재사용 : 비활성화
- 최대 세션 개수 : 30000
- 웹서버 응답 대기시간 : 600 초
- HTTP 서비스 포트 : 80
- Request Buffer Size : 1M
- 에러시 RESET 종료 : 비활성화
- 서버 HTTP Keepalive 조건 : client_ip + server_ip + server_port
- 서버 HTTP Keepalive 제한 시간 : 60 초
- 서버 TCP Keepalive : 비활성화
- 요청 대역폭 제한 : 비활성화
- Server Name Indication : 활성화

SSL 고급설정

- 서버 구간
 - SSL 프로토콜 : SSLv3 TLSv1 TLSv1.1 TLSv1.2
 - SSL 암호알고리즘 : AES128-SHA:AES128-SHA256:AES256-SHA:AES256-SHA256-ALL:ADH:EXPORT
- 클라이언트 구간
 - SSL 보안등급 : B 등급
 - SSL 프로토콜 : TLSv1 TLSv1.1 TLSv1.2
 - SSL 암호알고리즘 : AES128-SHA:AES256-SHA:AES128-SHA256:AES256-SHA256-ALL:ADH:EXPORT:RC4:MD5:DES:jaNULL
 - [SSL 취약점 진단 사이트\(ssllabs.com\)](https://www.ssllabs.com)
- SSL 버전별 차단
 - 보안로그 : 비활성화
 - 차단 SSL 프로토콜 : None
 - 차단 유형 : 일반
- DH 파라미터
 - 유형 : 비활성화
- 프록시 프로토콜
 - 상태 : 비활성화

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

3. 기본 사용 방법



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)

네트워크 서브넷 변경

선택된 서브넷

- Default Network (192.168.0.0/24)
- network_172 (172.16.0.0/16)
- serv_net (10.1.1.0/24)

⇨

사용 가능한 서브넷

- sqa_sub (192.168.1.0/24)
- vpc_test (192.168.2.0/24)

↻ 새로 고침

Vlan 설정

□ VLAN 정보

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

추가 ↗ 삭제 🗑️

(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 🗑️

인터페이스 추가 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

3. 기본 사용 방법

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)

System > 네트워크 > VLAN

eth1 **eth2** **mgmt**

□ VLAN 정보

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

추가 삭제

(T:Tagged port, U:Untagged port)

VLAN 추가

TYPE Tagged Untagged

VLAN 이름

VLAN 상태 UP Down

Promisc 활성화 비활성화

포트 eth1 eth2 mgmt

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)

System > 네트워크 > IP 주소

IP 주소 테이블

인터페이스	IP 주소	브로드캐스트
port1	172.16.0.103/24	172.16.0.255
port2	10.1.1.146/24	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)

3. 기본 사용 방법

로그 확인

로그 상세내용 확인

- System 탭 – 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

2022/03/31 13:03:41	WISE 요청 필터	http	응답	127.0.0.1:80	/GponForm/diag_Form?images/	27.213.32.183:36789	192.168.0.123:80	차단
No.	13	날짜	2022/03/31 13:03:41	공격 이름	WISE 요청 필터			
공격 이름(자세히)	WISE 요청 필터	애플리케이션	http	App 아이디	1			
SIG ID	-	SIG 위험도	-	공격 위험도	중간			
호스트	127.0.0.1:80	클라이언트 IP/PORT	27.213.32.183:36789	서버 IP/PORT	192.168.0.123:80			
URL	/GponForm/diag_Form?images/	WISE ID	1	국가	China			
대응	차단	탐지위치	-	HTTP(S)	HTTP			
탐지근거	-	설명	filter name :block	Forwarded for	-			
필드이름	-							

원본 데이터

No	Decoded string														Hex														String
00000000	POST /GponForm/diag_Form?images/ HTTP/1.1..Host: 127.0.0.1:80..Co														nnection: keep-alive..Accept-Encoding: gzip, deflate..Accept: */*..User-Agent: Hello, World..Content-Length: 118....														POST /Gp
00000001	50	4f	53	54	20	2f	47	70	6f	6e	46	6f	72	6d	2f	64	3f	69	6d	61	67	65	73	2f	onForm/d				
00000002	69	61	67	5f	46	6f	72	6d	31	69	6d	61	67	65	73	2f	31	0d	0a	48	6f	73	74	3a	diag_Form				
00000003	20	48	54	54	50	2f	31	2e	2e	31	3a	38	30	0d	0a	43	20	31	3a	38	30	0d	0a	43	?images/				
00000004	20	31	32	37	2e	30	2e	30	6e	3a	20	6b	65	65	70	2d	127.0.0	6e	3a	20	6b	65	65	70	2d	.1:80..C			
00000005	6f	6e	6e	65	63	74	69	6f	63	63	65	70	74	2d	45	6e	connectio	63	63	65	70	74	2d	45	6e	n: keep-			
00000006	61	6c	69	76	65	0d	0a	41	67	7a	69	70	2c	20	64	65	alive..A	67	7a	69	70	2c	20	64	65	cccept-En			
00000007	63	6f	64	69	6e	67	3a	20	63	63	65	70	74	3a	20	2a	coding:	63	63	65	70	74	3a	20	2a	gzip, de			
00000008	66	6c	61	74	65	0d	0a	41	2d	41	67	65	6e	74	3a	20	flate..A	2d	41	67	65	6e	74	3a	20	cccept: *			
00000009	2f	2a	0d	0a	55	73	65	72	6f	72	6c	64	0d	0a	43	6f	/*..User	6f	72	6c	64	0d	0a	43	6f	-Agent:			
0000000a	48	65	6c	6c	6f	2c	20	57	6e	67	74	68	3a	20	31	31	Hello, W	6e	67	74	68	3a	20	31	31	orld..Co			
0000000b	6e	74	65	6e	74	2d	4c	65	38	0d	0a	0d	0a	ntent-Le	38	0d	0a	0d	0a	ngth: 11	38	0d	0a	0d	0a	8....			

3. 기본 사용 방법

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

날짜	공격 이름	애플리케이션	SIG 위험도	공격 위험도	호스트	URL	클라이언트 IP/PORT	서버 IP/PORT	국가	대응
2022/04/01 12:14:43	요청형식검사	http		낮음		/	23.95.100.141:55224	192.168.0.123:80	USA	차단
2022/04/01 12:09:32	요청형식검사	http		낮음		/	23.95.100.141	192.168.0.123:80	USA	차단
2022/04/01 11:45:21	검사회피	http		낮음	133.186.132.42:443	/cgi-bin/%2e/%2e/%2e/%2e/bin/sh	45.155.204.146	192.168.0.123:80	Russia	차단
2022/04/01 11:38:31	접근제어	http	높음	중간	133.186.241.68	/1.bak	103.243.200.42:64976	192.168.0.123:80	China	차단
2022/04/01 11:32:03	검사회피	https		낮음	133.186.146.205:443	/cgi-bin/%2e/%2e/%2e/%2e/bin/sh	192.168.0.126:33752	192.168.0.123:443		차단
2022/04/01 11:29:49	검사회피	https		낮음	133.186.211.115:443	/cgi-bin/%2e/%2e/%2e/%2e/bin/sh	192.168.0.56:52930	192.168.0.123:443		차단

순서	목록	요청 시간	완료 시간	파일	삭제
1	test	22/04/01 13:29:29	22/04/01 13:29:34	다운로드	삭제

3. 기본 사용 방법

차단 정책

시그니처 확인

- System 탭 – 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

System > 애플리케이션 > 시그니처 관리

시그니처 버전

- 현재 시그니처 버전: 4.68

시그니처 리스트

- 보안레벨: 높음 [사용자]
(의심가는 접근 전체를 차단하지만 일부 정상접근도 차단 될 수 있습니다.)

시그니처 ID	시그니처 정보	위험도	차단	탐지	예외
ACC-00001	설명 : .htaccess 액세스 공격	하	●		
ACC-00002	설명 : /architext_query.pl	하	●		
ACC-00003	설명 : /blabla.ida	상	●		
ACC-00004	설명 : /cgi-bin/global.cgi 취약점	하	●		
ACC-00005	설명 : /etc/hosts 시스템 파일 접근공격	상	●		
ACC-00006	설명 : /etc/hosts 시스템 파일 접근공격	상	●		
ACC-00007	설명 : /etc/passwd 시스템 파일 접근공격	상	●		
ACC-00008	설명 : /sam 샘플일 추출 공격1	하	●		
ACC-00009	설명 : /sam 샘플일 추출 공격2	하	●		
ACC-00010	설명 : /sam 샘플일 추출 공격3	하	●		
ACC-00011	설명 : /test/jsp/declaration/IntegerOverflo접근공격	하	●		
ACC-00012	설명 : /test/jsp/pageIsErrorPage.* 접근공격	하	●		
ACC-00013	설명 : /test/jsp/pageIsThreadSafe.* 접근공격	하	●		
ACC-00014	설명 : /test/jsp/pageSession.* 접근공격	하	●		
ACC-00015	설명 : /././././winnt/win.ini 접근 취약점	하	●		
ACC-00016	설명 : 검색 robots 접근 공격	중	●		

3. 기본 사용 방법

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)

The interface shows the 'System > Application > 시그니처 관리' (System > Application > Signature Management) page. The left sidebar contains navigation options like '대시보드', '통합 모니터링', '시스템 모니터링', '통합 로그', 'AV2', '통합 보고서', '애플리케이션', '방화벽', and '사용자 관리'. The main content area is divided into '보안레벨' (Security Level) and '시그니처 리스트' (Signature List). A red box highlights the '사용자 시그니처' (User Signature) button in the '시그니처 리스트' section. The right screenshot shows the '사용자 정의 시그니처' (User Defined Signature) dialog box, which contains a table of existing signatures.

시그니처 ID	헤더명	시그니처	설명	유형	상태
USER-WAP-00001	Referer	[\${}][+]?n(+)?d(+)?n(+)?	log4j 탐지 패턴	정규식	탐지

예외 처리

화이트리스트

- System 탭 – 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)

PIOLINK | WEBFRONT-K "다음부팅시사용" 저장공간과

System > 애플리케이션 > 화이트리스트 관리

화이트리스트 상태 [전체]

- 상태 : 활성화
- 보안로그 : 비활성화

화이트리스트 목록 [전체]

화이트리스트 IP/PORT	클라이언트 IP 주소	클라이언트 포트	서버 IP 주소	서버 포트	설명
	1.2.3.4/32	전체	전체	80	

Left Sidebar: **화이트리스트 관리**

예외 처리

블랙리스트

- System 탭 – 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)

PIOLINK | WEBFRONT-K

System > 애플리케이션 > 블랙리스트 관리

블랙리스트 상태

- 보안로그 : 비활성화
- 차단 : 비활성화

블랙리스트 옵션

- 차단 시간: 30 (초)
- 허용 공격 수: 1회/60초
- 추가 차단 : 활성화
- 추가 차단 대기 시간: 10 (초)
- 추가 차단 방법 : 영구 차단

블랙리스트 설정(세션 상태)

- 세션 : 활성화

블랙리스트 고급 설정(프록시 IP 헤더 리스트)

- 프록시 헤더 : 비활성화

블랙리스트 고급 설정(사용자 정의 IP)

블랙리스트 차단 IP 리스트

아이피	차단 시간 (초)

조건에 따른 자동 차단 설정

클라이언트 IP 기반 블랙리스트 설정

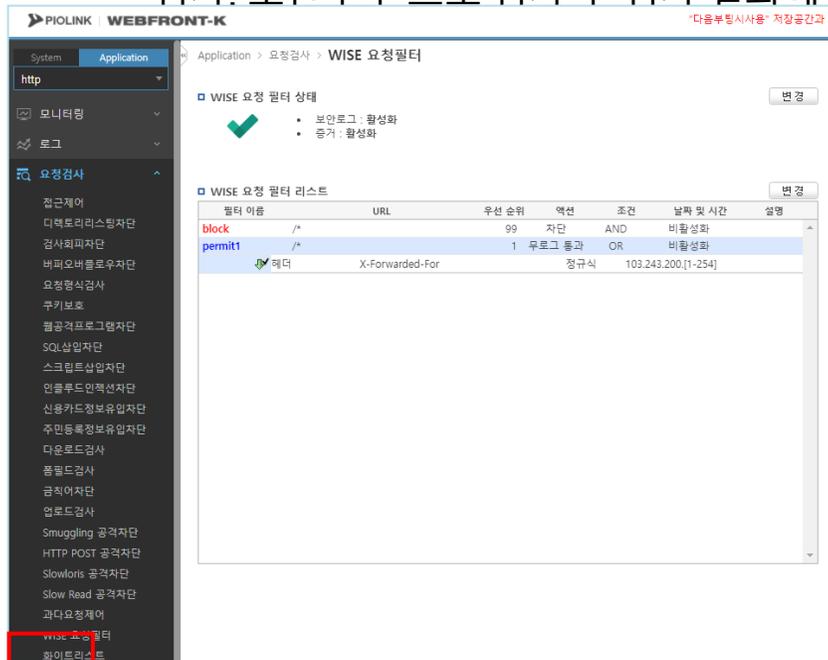
프록시 헤더 IP 기반 블랙리스트 설정(XFF헤더 등)

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



필터	URL	우선 순위	액션	조건	발행 및 시간	설명
permit1	/*	1	무로그 통과	AND	비활성화	
	헤더			X-Forwarded-For	정규식	103.243.200.[1-254]
	메서드			-	포함	GET
	매개변수			WAF	포함	permit

예외 처리

WISE 요청필터

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

WISE 요청 필터 검사 항목 추가

데이터 형식	매개변수 ▼		
변수	<div style="border: 1px solid #ccc; padding: 2px;"> 쿠키 메서드 헤더 매개변수 IP 주소 시그니처 ID 국가명 </div>	<input type="text"/>	<input type="text"/>
조건		▼	
값		<input type="text"/>	<input type="text"/>

- 같은

 - 포함
 - 포함하지 않음
 - 정규식
 - 매개변수가 존재함
 - 매개변수가 존재하지 않음
 - 값이 존재하지 않음
 - PCRE

예외 처리

WISE 요청필터

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

1. WAF가 최상단일 경우
2. [HTTP 통신 or HTTPS 통신] + WAF 상단에 LB가 존재 + (LB에서 인증서 처리)
3. HTTPS 통신 + WAF 상단에 LB가 존재 + LB에서 인증서 처리가 되지 않을 경우

>> IP주소로 대응 (IP 대역으로 추가 가능)

>> 헤더 (X-Forwarded-For)로 대응

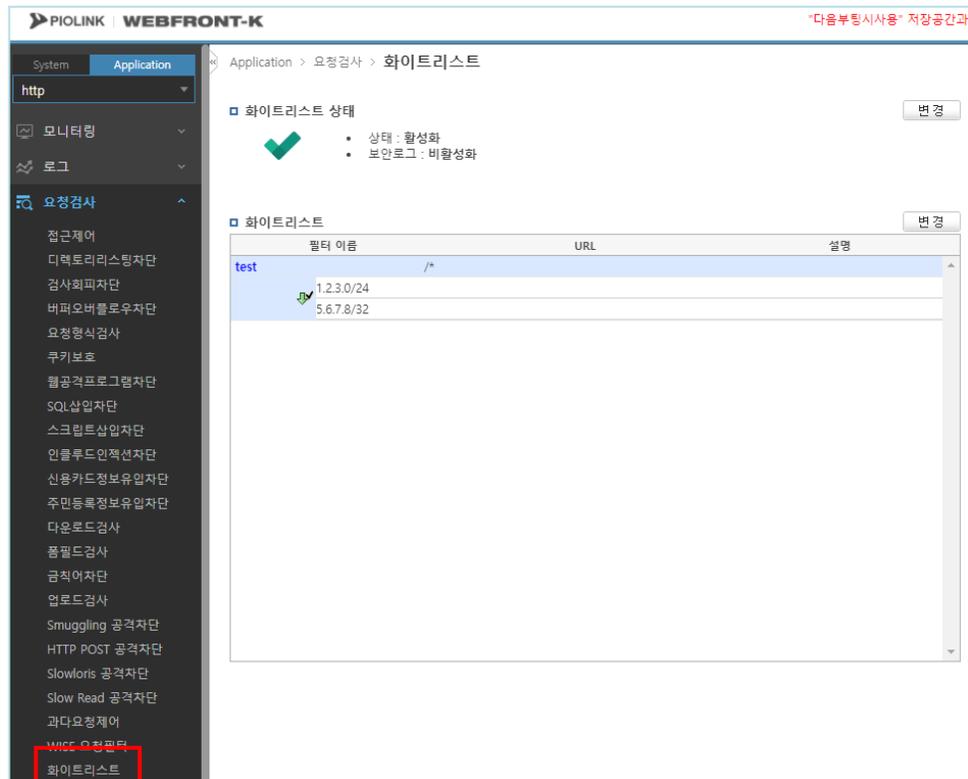
>> WISE 요청필터로 IP기반 대응 불가능

필터 이름	URL	우선 순위	액션	조건	날짜 및 시간	설명
test	/*	1	통과	OR	비활성화	테스트용 입니 다
헤더	X-Forwarded-For		포함	1.2.3.4		
헤더	X-Forwarded-For		포함	5.6.7.8		
헤더	X-Forwarded-For		정규식	1.2(\w{1}[0-9]?[0-9]{1}[0-9]{2} 2[0-4][0-9] 25[0-5]){2}		

예외 처리

화이트리스트(요청검사)

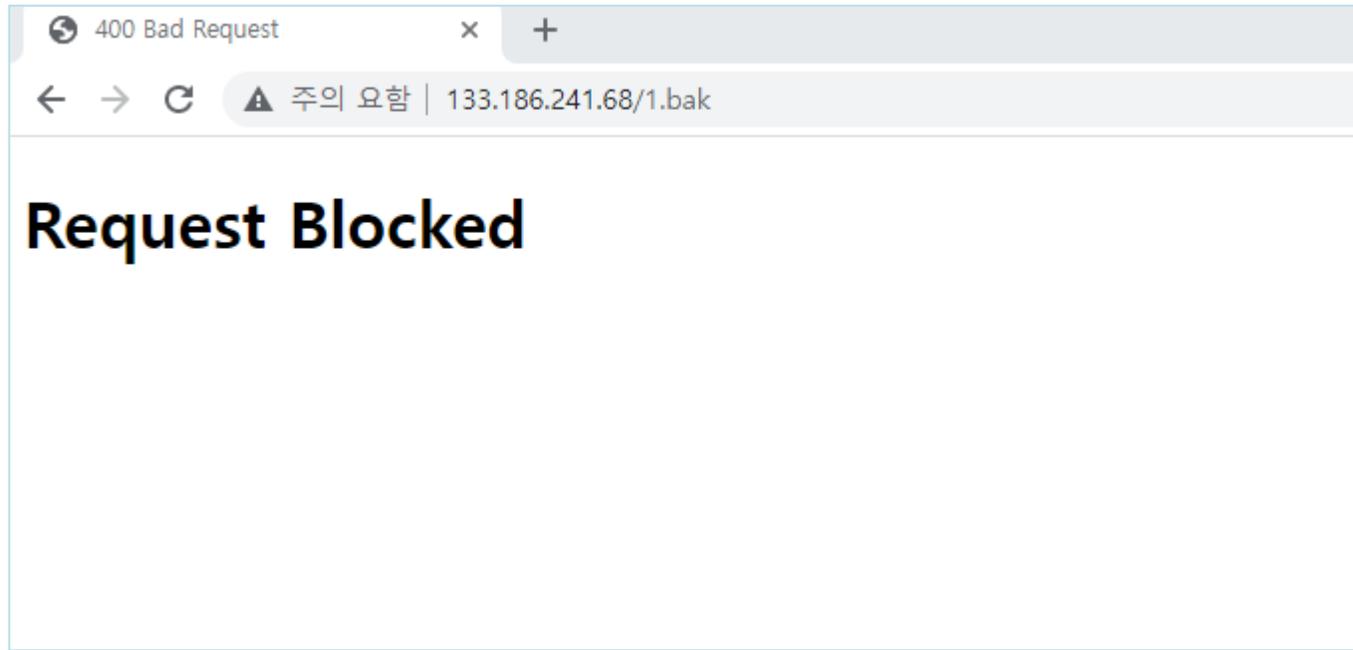
- Application탭 - {특정 애플리케이션} - 요청검사 - 화이트리스트 에서 특정 URL에 대해 특정 IP(대역)로부터의 접근을 허용할 수 있음
- 해당 애플리케이션에 설정되어 있는 도메인에 대해서만 접근 허용
- 네트워크 구성에 따라 적용하기 힘들 수 있음 (상단에 LB 위치할 경우)



장애 조치

차단으로 인한 이슈

- System 탭 – 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)



3. 기본 사용 방법

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)

Application > 애플리케이션 > 응답설정

응답 설정 정보

- 유형: 일반

응답 설정 에러 코드 리스트

- 상태: 활성화
- 차단: 비활성화
- 보안로그: 비활성화

에러 코드	유형	상세 보기
500	사용자 정의	상세보기

응답 설정 자세히 보기

유형: 사용자 정의
응답 코드: 500

내부 서버 장애로 인해 접속이 불가능합니다.
아래 담당자에게 문의 바랍니다. (네트워크 운영팀 xxx / 010-1234-5678)

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)

PIOLINK | WEBFRONT-K "다음부팅시사용" 저장공간과

System Application Application > 부하분산 > 장애감시

service_1_http

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

장애 감시 리스트 변경

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
web1	INACT	X	
web2	INACT	X	

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

The image shows two overlapping screenshots. The background screenshot is the PIOLINK WEBFRONT-K management console. It displays the '소스NAT설정' (Source NAT Settings) page. A red box highlights the '소스 NAT 상태' (Source NAT Status) section, which shows a red 'X' icon and the text '상태 : 비활성화' (Status : Deactivated). Below this, there is a table for '소스 NAT IP 리스트' (Source NAT IP List) with columns for 'IP 주소' (IP Address) and 'SNAT IP' (SNAT IP). One entry is visible with IP '192.168.0.123' and SNAT IP '192.168.0.123'. The foreground screenshot is a web browser window showing a '502 Bad Gateway' error page. The browser's address bar shows the URL '133.186.241.68' and a warning icon. The main content of the browser window is the text '502 Bad Gateway'.

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 | WEBFRONT-K "다음부팅시사용" 저장공간과

System Application Application > SSL > 일반설정

https

- 모니터링
- 로그
- 요청검사
- 컨텐츠보호
- 애플리케이션
- SSL
 - 일반설정
 - 인증서관리
 - 임시인증서생성

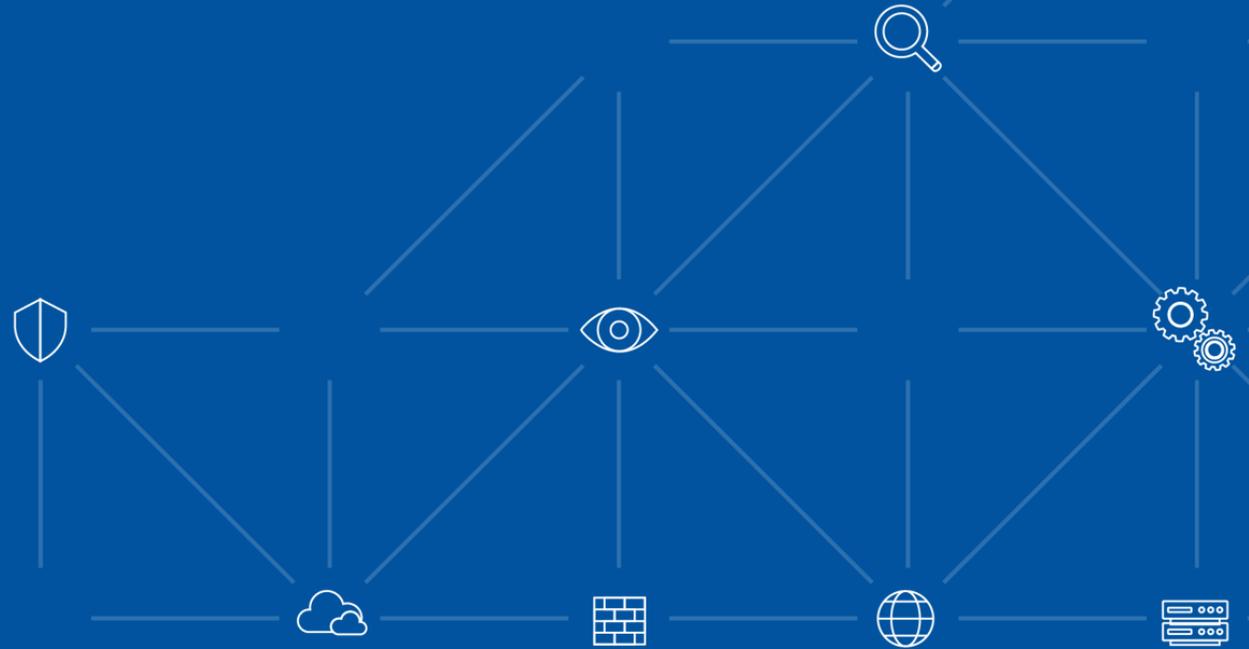
SSL 변경

- 상태 : 활성화
- 백엔드 : 활성화

SSL 설정정보 변경

- 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 : 비활성화

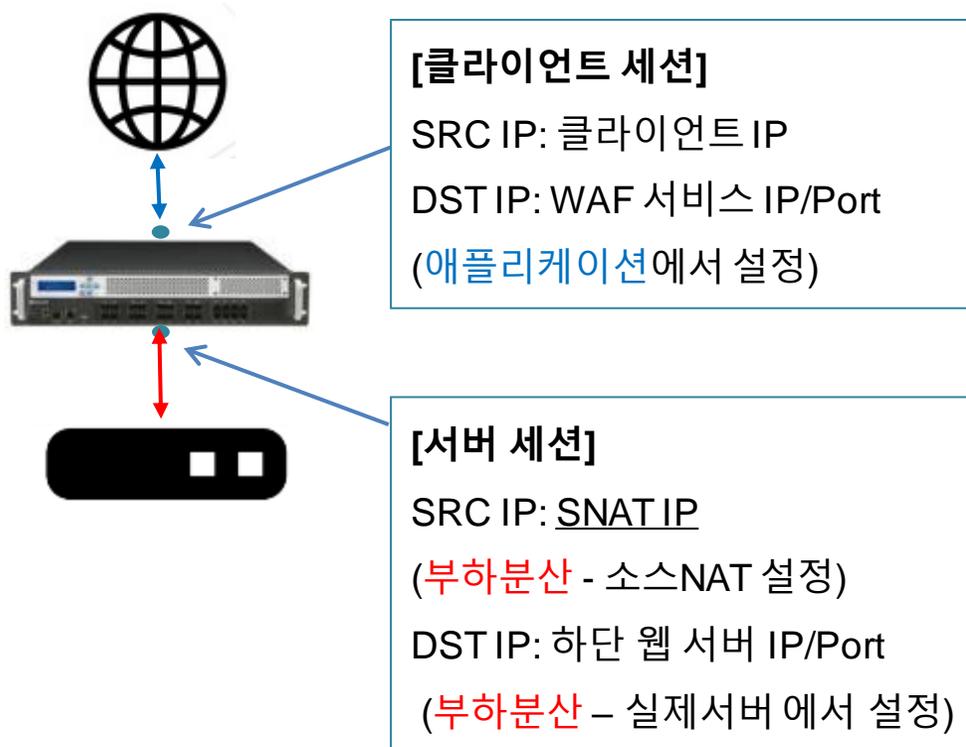
4. 기본 설정



어플리케이션 설정

• WEBFRONT-KS 기본 구성

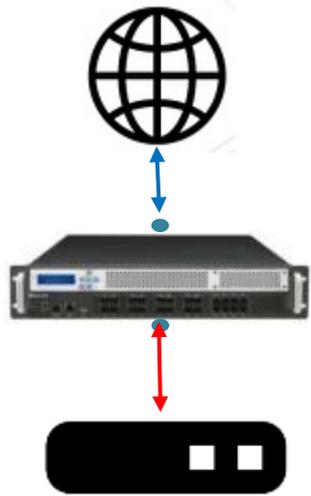
- 클라이언트, 내부 서버와 각각 세션을 맺어 프록시로서 동작함
- 클라이언트, 서버 각 세션은 독립적으로 동작하는 서로 다른 세션임



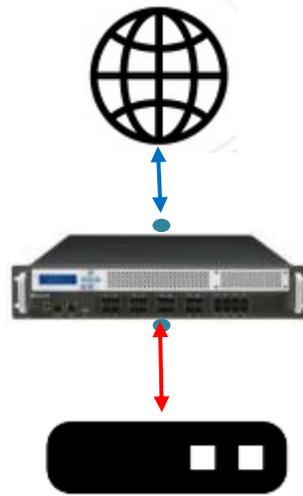
어플리케이션 설정

• WEBFRONT-KS 기본 구성

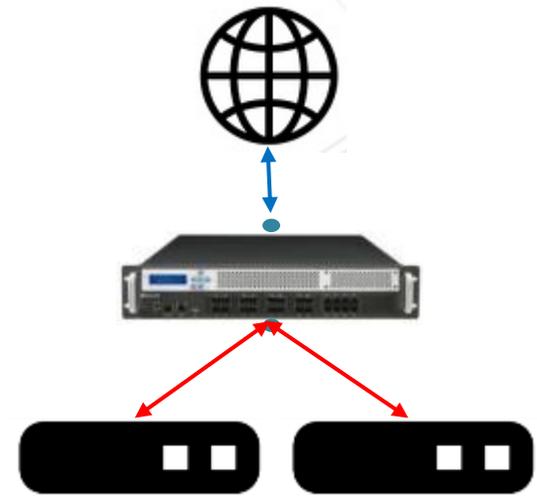
- 웹방화벽 구축 시, 크게 3가지 케이스로 구분 가능



도메인: 1개
WEB: 1개



도메인: 2개 이상
WEB: 1개

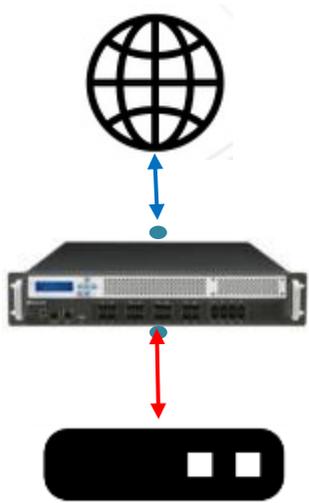


도메인: 1개
WEB: 2개 이상

어플리케이션 설정

- WEBFRONT-KS 기본 구성

- 아래와 같은 환경으로 구축한다고 가정



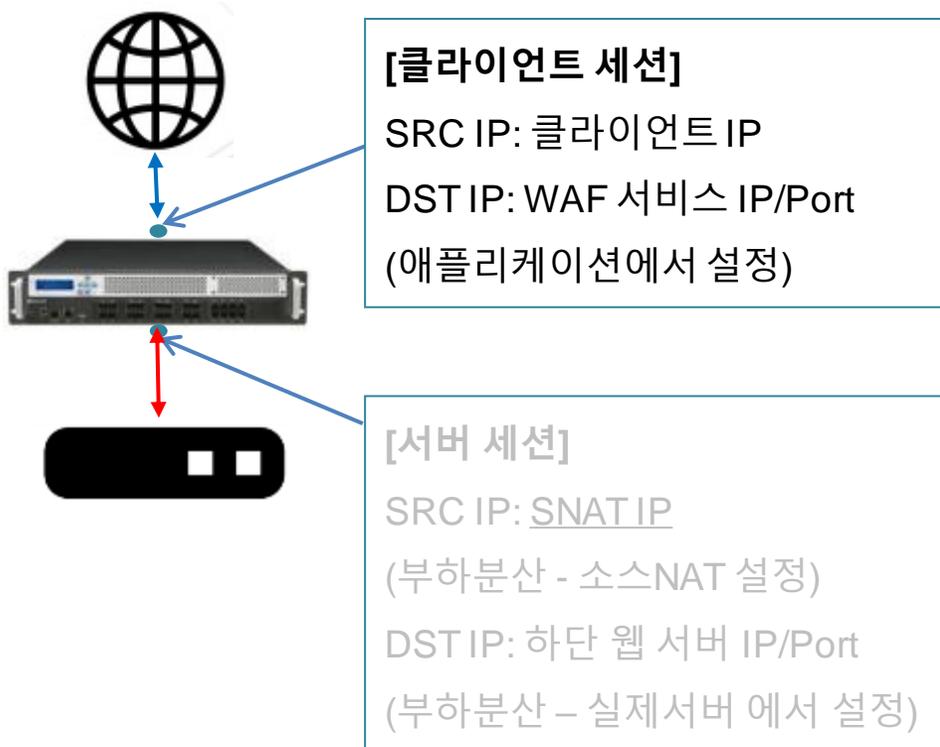
도메인: 1개 (test.com)
WEB: 1개 (192.168.0.5)
프로토콜: http

4. 기본 설정

어플리케이션 설정

• WEBFRONT-KS 기본 구성

- 클라이언트 세션 관련 설정(어플리케이션)



Application > 애플리케이션 > 일반설정

애플리케이션 상태 : 활성화

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

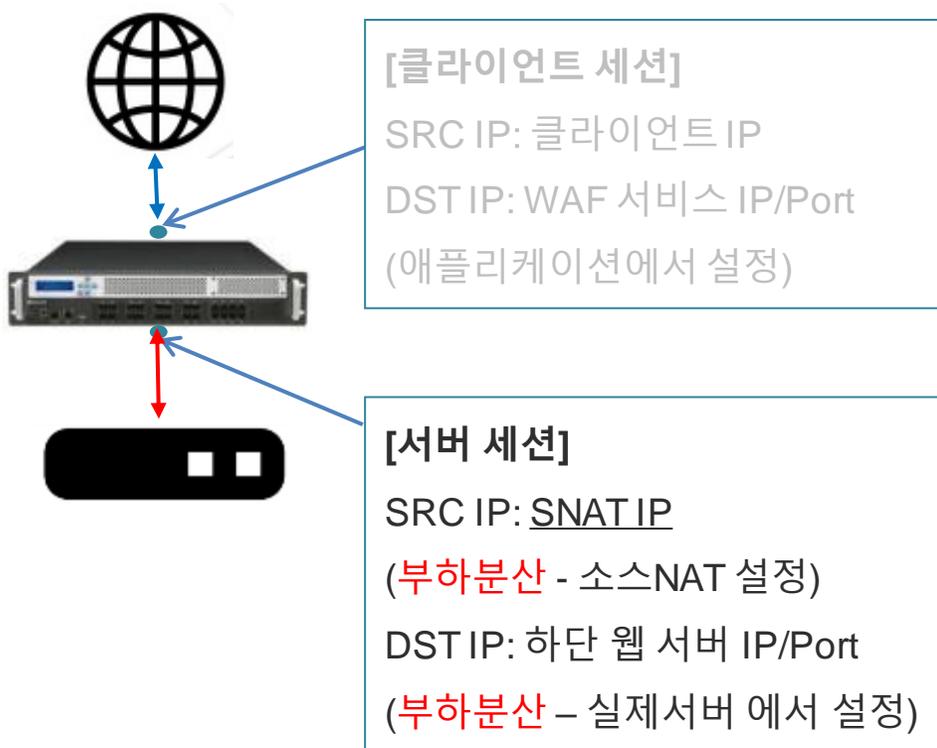
IP 버전	IP 주소	포트	IP 트랜스패런트	유형	설명
v4	192.168.0.123	80	비활성화	HTTP	

서비스용 IP/Port 입력 (웹방화벽의 사설 IP)

4. 기본 설정

어플리케이션 설정

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



PIOLINK | WEBFRONT-K

Application > 부하분산 > 소스NAT설정

소스 NAT 상태 변경

✓ 상태 : 활성화

소스 NAT IP 리스트 변경

IP 주소	설명
192.168.0.123	

소스 NAT IP 리스트

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

PIOLINK | WEBFRONT-K

Application > 부하분산 > 실제서버

실제 서버 리스트 변경

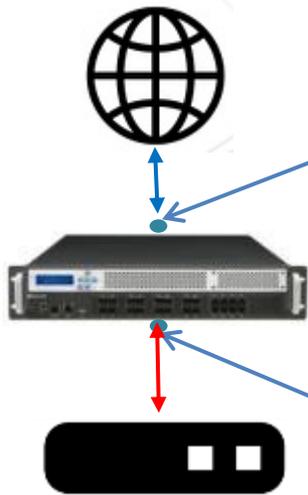
이름	IP 주소	포트	가중치	설명
web_server	192.168.0.5	80	100	Web Server

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
 (어플리케이션에서 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

The screenshot shows the 'Application > 부하분산 > 그룹' configuration page. The left sidebar has '부하분산' expanded. The main area shows a table of groups and a detailed view of the 'rr' group.

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

그룹 상세 보기

- 이름 : rr
- 상태 : 활성화
- Persist : 아이피
- 부하 분산 알고리즘 : 라운드 로빈
- 설명 :

실제 서버 리스트

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

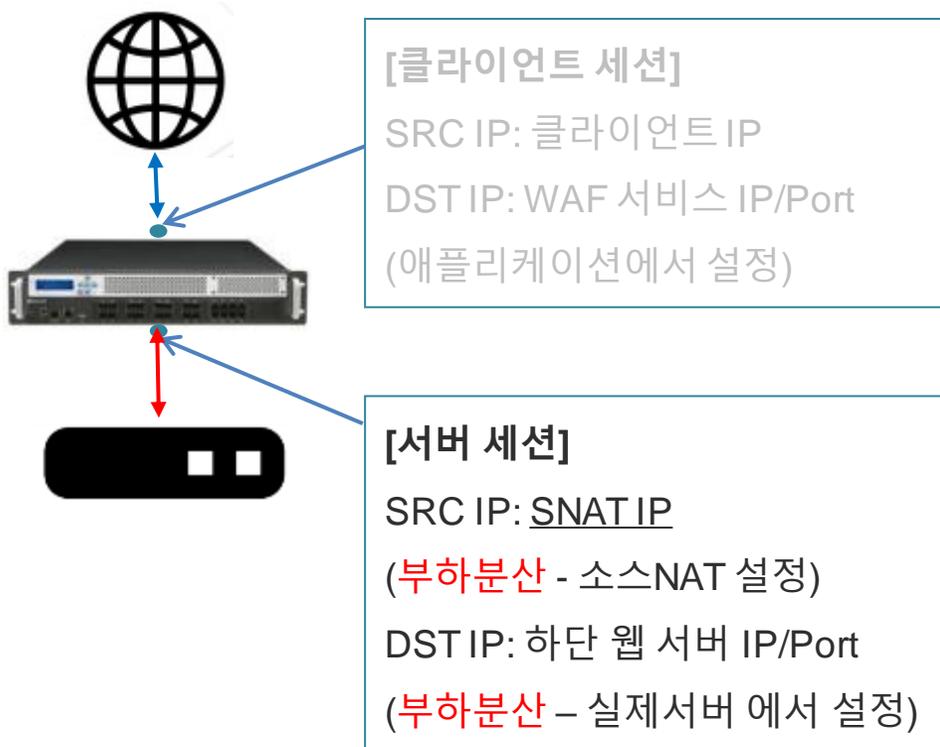
Persist 기준

- 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)



Application > 부하분산 > 규칙

규칙 리스트

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 :

패턴 리스트

아이디	유형	매치 방법	비교 문자열	설명

그룹

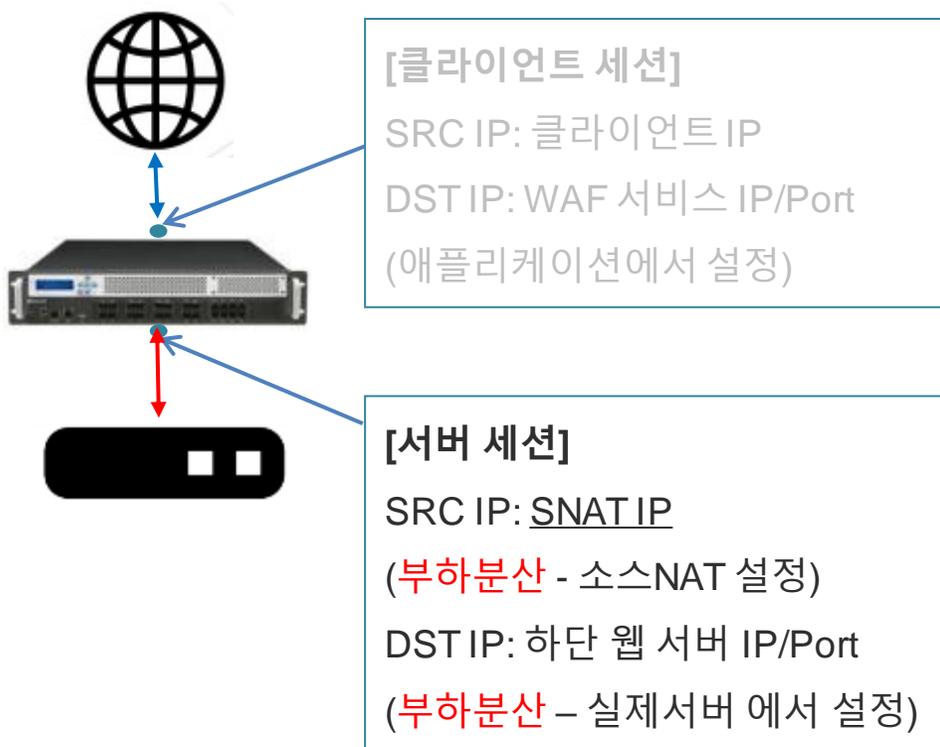
이름	Persist	부하 분산 알고리즘	실제 서버 개수	설명	상세 보기
rr	아이피	라운드 로빈	1		상세보기

규칙 = 그룹 + 패턴(패턴은 설정하지 않아도 무방함)

어플리케이션 설정

• WEBFRONT-KS 기본 구성

- 서버 세션 관련 설정(부하분산)



PIOLINK | WEBFRONT-K

System Application Application > 부하분산 > 장애감시

□ 장애 감시 리스트 변경

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

□ 실제 서버 장애 감시 상태

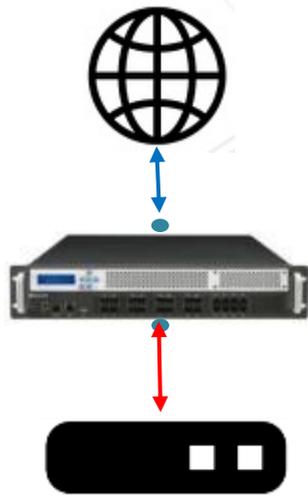
실제 서버 / 장애 감시	1
web_server	ACT ○

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



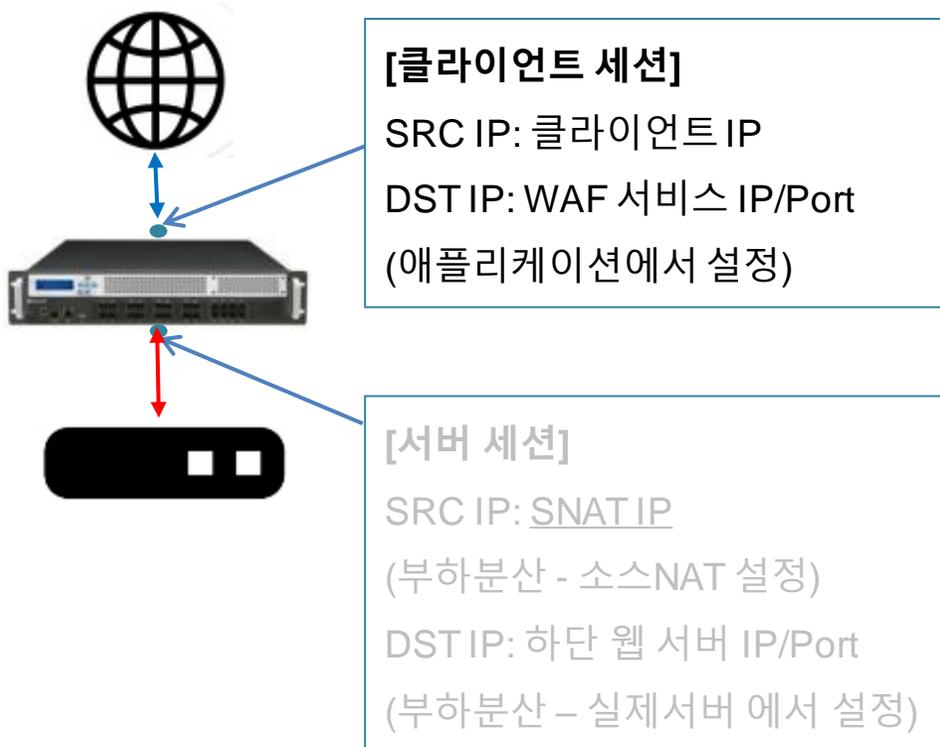
도메인: 1개 (test.com)
WEB: 1개 (192.168.0.5)
프로토콜: **https**

4. 기본 설정

어플리케이션 설정

• WEBFRONT-KS 기본 구성

- 클라이언트 세션 관련 설정(어플리케이션/https)



Application > 애플리케이션 > 일반설정

애플리케이션 상태: 활성화

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 트랜스퍼런트	유형	설명
v4	192.168.0.123	443	비활성화	HTTPS	

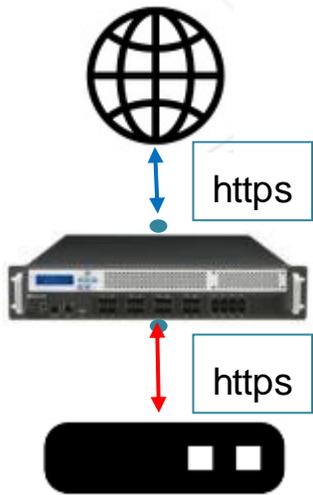
서비스용 IP/Port 입력 (웹방화벽의 사설 IP)
 유형을 HTTPS로 설정

4. 기본 설정

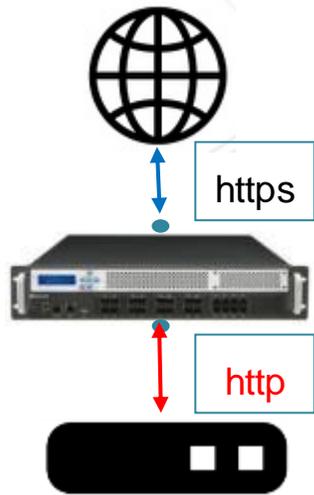
어플리케이션 설정

• WEBFRONT-KS 기본 구성

- 클라이언트+서버 세션 관련 설정(SSL)



백엔드 활성화 한 경우



백엔드 비 활성화 한 경우

PIOLINK | WEBFRONT-K
Application > SSL > 일반설정

System Application

https

- 모니터링
- 로그
- 요청검사
- 컨텐츠보호
- 애플리케이션
- SSL
- 일반설정
- 인증서관리
- 임시인증서생성
- SSL 프로토콜 검사
- Mutual TLS
- 부하분산
- 학습
- 위장

< OWASP TOP 10 >

변경

SSL

- 상태 : 활성화
- 백엔드 : 활성화

SSL 설정정보

- 세션 재사용 : 활성화
- 클라이언트 IP별 세션
- 최대 세션 개수 : 30
- 웹서버 응답 대기시간
- Request Buffer Size
- 에러시 RESET 종료
- 서버 HTTP Keepalive
- 서버 HTTP Keepalive
- 서버 TCP Keepalive
- 요청 대역폭 제한 :
- Server Name Indication

SSL 고급설정

- 서버 구간
 - SSL 프로토콜 : SSLv3
 - SSL 암호알고리즘 : F
- 클라이언트 구간
 - SSL 보안등급 : 사용자
 - SSL 프로토콜 : SSLv3
 - SSL 암호알고리즘 : F
 - [SSL 취약점 진단 사이트](#)
- SSL 버전별 차단
 - 보안로그 : 비활성화
 - 차단 SSL 프로토콜 :
 - 차단 유형 : 일반
- DH 파라미터
 - 유형 : 비활성화
- 프록시 프로토콜
 - 상태 : 비활성화

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.

4. 기본 설정

어플리케이션 설정

• WEBFRONT-KS 기본 구성

- 클라이언트+서버 세션 관련 설정(SSL)

클라이언트 구간

SSL 보안등급: 사용자 정의

SSL 보안등급: B 등급

SSL 프로토콜: A 등급

SSL 암호알고리즘: 사용자 정의

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

상세보기

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
- 백엔드: 활성화

SSL 설정정보

- 세션 재사용: 활성화
- 클라이언트 IP별: 비활성화
- 최대 세션 개수: 1000
- 웹서버 응답 대기: 비활성화
- Request Buffer: 비활성화
- 에러시 RESET: 비활성화
- 서버 HTTP Keep: 비활성화
- 서버 HTTP Keep: 비활성화
- 서버 TCP Keep: 비활성화
- 요청 대역폭 제한: 비활성화
- Server Name Indication: **활성화**

SSL 고급설정

- 서버 구간: SSLv3 TLSv1 TLSv1.1 TLSv1.2
- SSL 프로토콜: SSLv3 TLSv1 TLSv1.1 TLSv1.2
- SSL 암호알고리즘: RC4-SHA:RC4-MD5:AES128-SHA:AES256-SHA:ALL:!ADH:!EXPORT
- 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)
- SSL 버전별 차단:
 - 보안로그: 비활성화
 - 차단 SSL 프로토콜: None
 - 차단 유형: 일반
- DH 파라미터:
 - 유형: 비활성화
- 프록시 프로토콜:
 - 상태: 비활성화

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

Server Name Indication: 활성화로 설정

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

4. 기본 설정

어플리케이션 설정

• WEBFRONT-KS 기본 구성

- 클라이언트+서버 세션 관련 설정(SSL)

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:

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) 활성화로 설정된 경우

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

2) 비활성화로 설정된 경우

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

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

4. 기본 설정

어플리케이션 설정

• WEBFRONT-KS 기본 구성

- 클라이언트+서버 세션 관련 설정(인증서 관리)
- 아래 순서대로 인증서+개인키를 하나의 파일로 합친 후 등록

개인키 파일

도메인 인증서

루트 인증서

체인 인증서 1,2...

인증서 등록 후 정보 확인 가능

Application > SSL > 인증서관리

인증서 정보

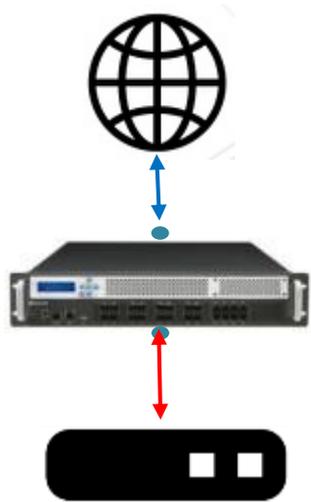
- 키 형식 RSA
- 키 길이 1024
- 암호화 방법
- MD5 지문 1F:A3:D3:47:5F:7A:DA:3E:F5:F1:DA:AD:3E:A3:10:25
- SHA1 지문 97:40:55:A1:29:F4:A8:2B:D6:2D:2C:AD:A9:9E:71:F8:8E:84:CC:AA
- 이름 Web Application Firewall
- 발급 대상 /CN=Web Application Firewall
- 인증서 발급 /CN=Web Application Firewall
- 발급일 Feb 14 05:13:49 2023 GMT
- 만료일 Feb 14 05:13:49 2024 GMT
- x509 상세보기

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

어플리케이션 설정

• WEBFRONT-KS 기본 구성

- 아래와 같은 환경으로 구축한다고 가정
- 기본적인 어플리케이션 및 부하분산 설정은 http를 설정할 경우와 동일하나, 일부 변경이 필요한 설정이 존재함 (어플리케이션 도메인 리스트)
- 만약 도메인 별로 처리하는 WEB의 IP가 다르다면, 각각의 도메인 별로 다수의 어플리케이션을 생성해야 함



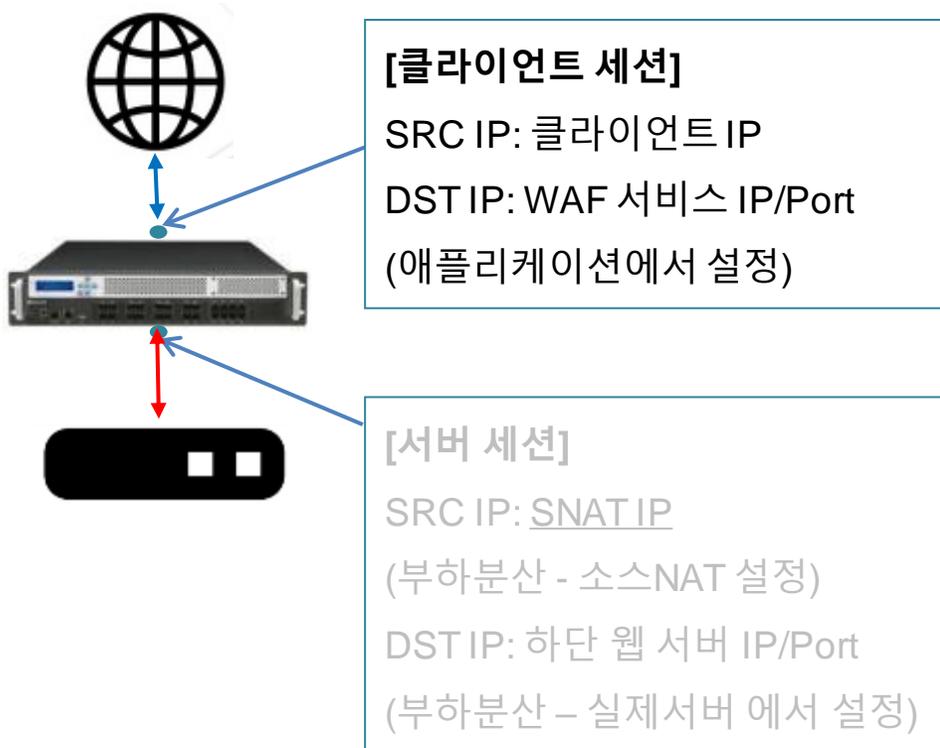
도메인: 2개
(test1.com, test2.com)
WEB: 1개 (192.168.0.5)
프로토콜: http

4. 기본 설정

어플리케이션 설정

• WEBFRONT-KS 기본 구성

- 클라이언트 세션 관련 설정(어플리케이션)



The screenshot shows the 'Application' configuration page in the WEBFRONT-KS interface. The left sidebar lists various settings like Monitoring, Logs, and Application. The main area is titled 'Application > 애플리케이션 > 일반설정'.

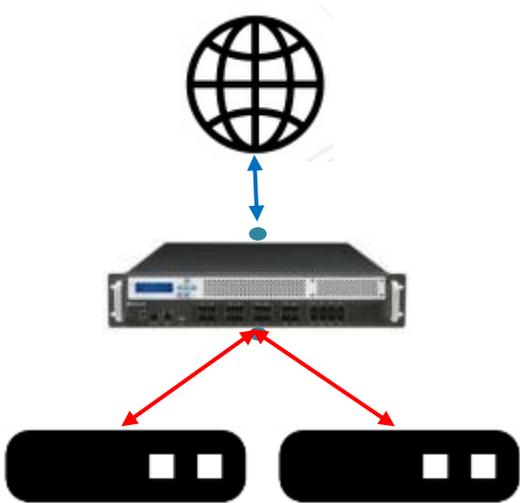
- 애플리케이션** (Application): Status is '활성화' (Activated).
- 애플리케이션 일반 설정 정보** (Application General Settings):
 - 모드: 부하 분산(고급)
 - 도메인 무시: 비활성화
 - 압축 방지: 비활성화
 - 클라이언트 MSS: 1414
 - 서버 MSS: 1414
 - CPS 제한: 비활성화
 - 동시세션 제한: 비활성화
 - BPS 제한: 비활성화
- 애플리케이션 도메인 리스트** (Application Domain List): A table with columns '도메인' (Domain) and '이름' (Name). It lists 'test1.com' and 'test2.com'. A red box highlights this table with the text '처리하고자 하는 도메인을 모두 입력' (Enter all domains to be processed).
- 애플리케이션 IP/포트 리스트** (Application IP/Port List): A table with columns 'IP 버전' (IP Version), 'IP 주소' (IP Address), '포트' (Port), 'IP 트랜스퍼트' (IP Transport), '유형' (Type), and '설명' (Description). It lists 'v4' with IP '192.168.0.123', port '80', and type 'HTTP'.

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

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)

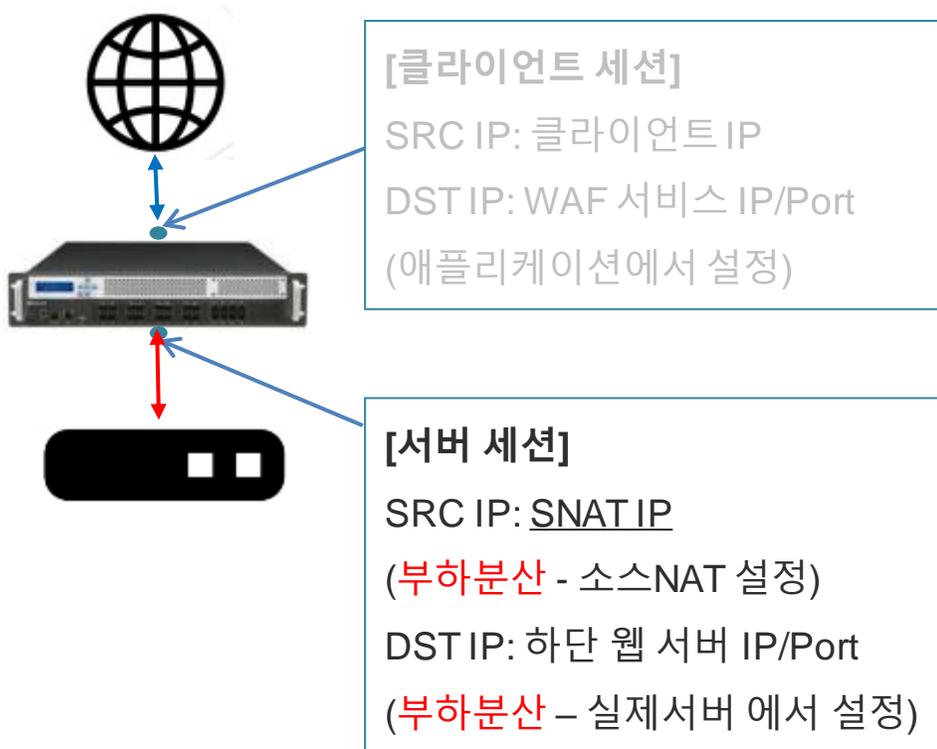


도메인: 1개 (test.com)
WEB: 2개 (192.168.0.5, 192.168.0.6)
프로토콜: http

4. 기본 설정

어플리케이션 설정

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



PIOLINK | WEBFRONT-K

Application > 부하분산 > 실제서버

이름	IP 주소	포트	가중치	설명
web_server	192.168.0.5	80	100	Web Server
web2	192.168.0.6	80	100	

WAF 하단에 연결되는 서버의 IP/Port를 모두 입력

PIOLINK | WEBFRONT-K

Application > 부하분산 > 그룹

이름	Persist	부하 분산 알고리즘
rr	쿠키	라운드 로빈

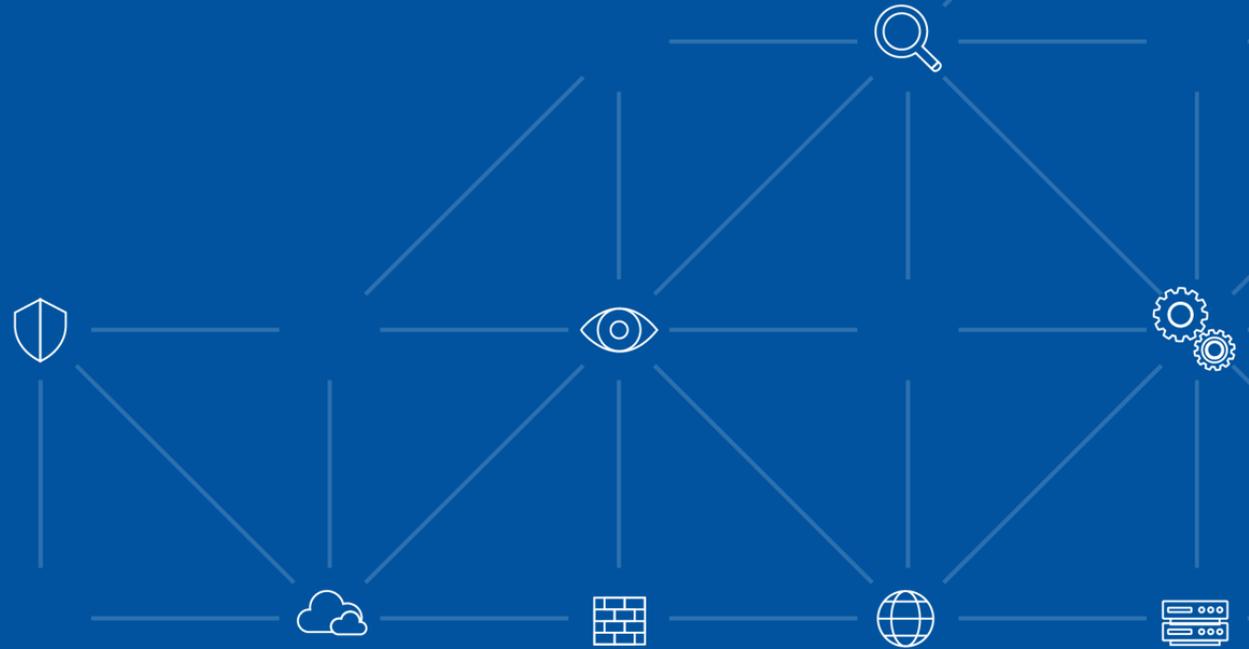
그룹 상세 보기

- 이름 : rr
- 상태 : 활성화
- Persist : 쿠키
- 부하 분산 알고리즘 : 라운드 로빈
- 쿠키 이름 : WAF

이름	IP 주소	포트	가중치	설명
web_server	192.168.0.5	80	100	Web Server
web2	192.168.0.6	80	100	

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

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



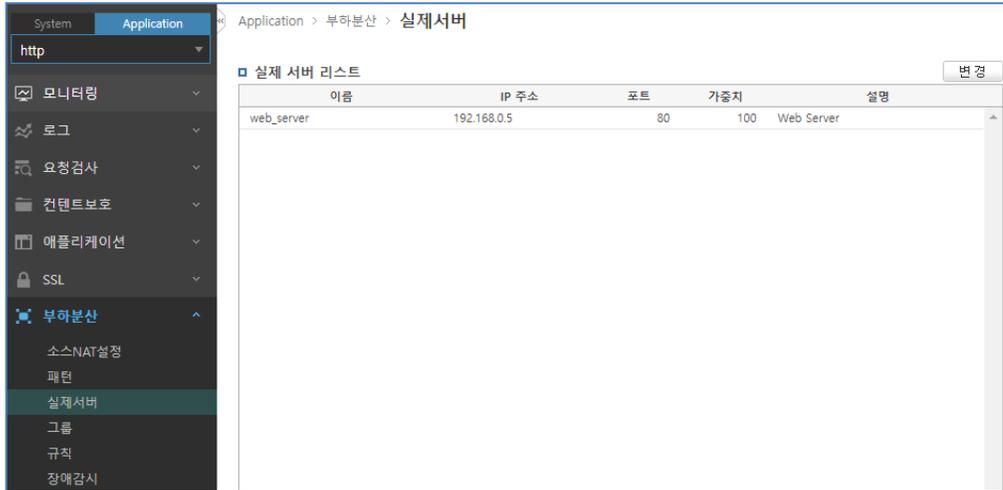
- ✓ 소스 NAT **상태 활성화** 여부
- ✓ 소스 NAT **IP 등록** 여부

1. HTTP

• WEBFRONT-KS 설정 체크

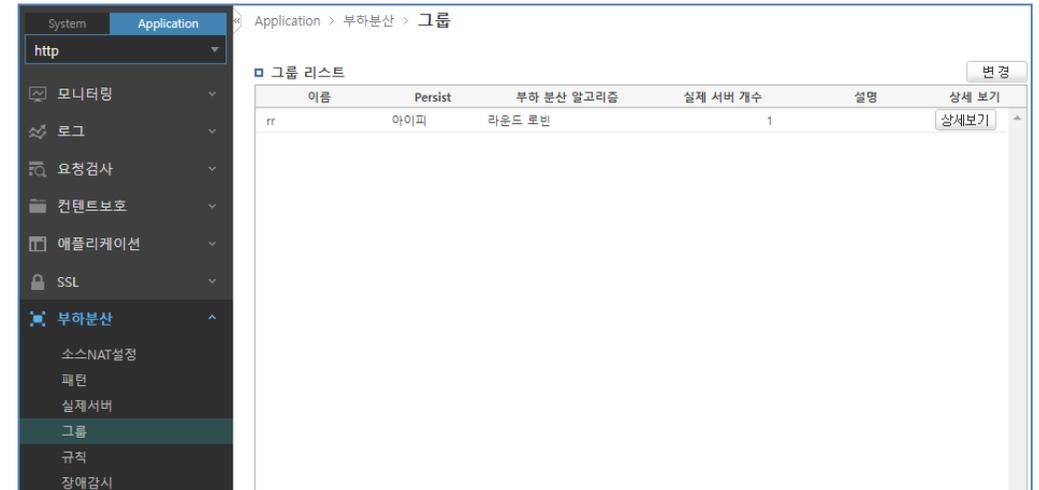
– 웹방화벽으로서 기능하기 위한 최소한의 설정 상태 체크

실제 서버 설정



✓ 실제서버 IP/Port 정상 등록 여부

그룹 설정



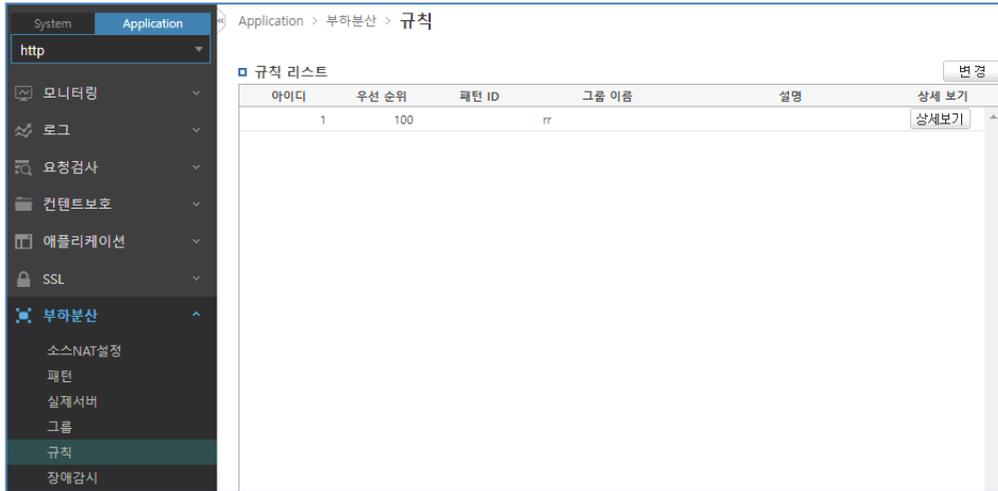
✓ 그룹에 등록된 실제 서버 개수 확인
✓ Persist 설정 여부

1. HTTP

• WEBFRONT-KS 설정 체크

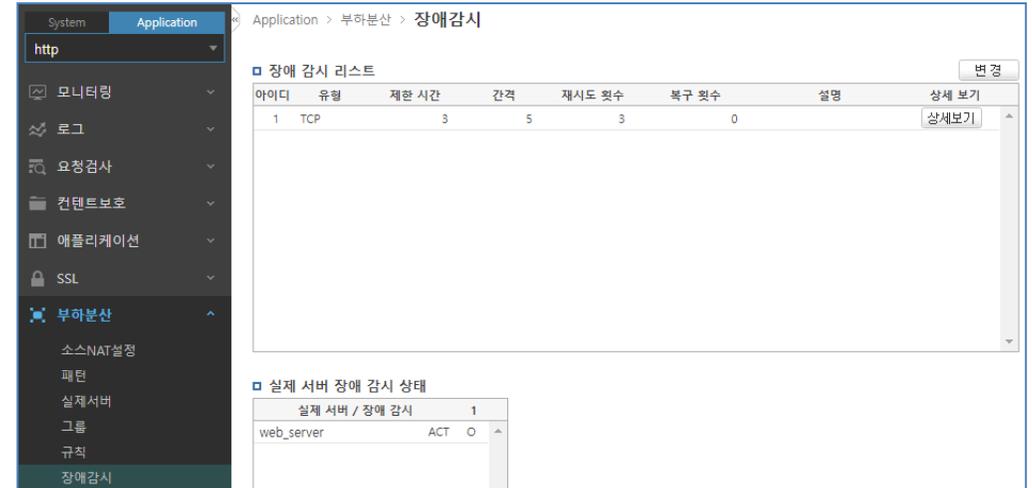
– 웹방화벽으로서 기능하기 위한 최소한의 설정 상태 체크

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

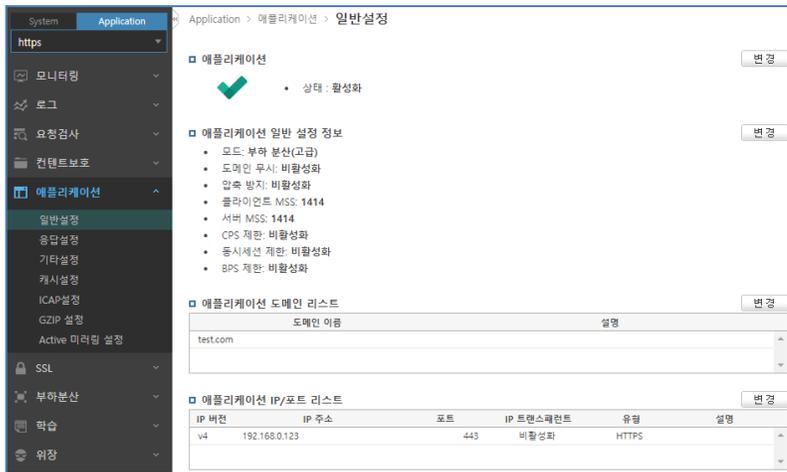
● SSL 일반 설정

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



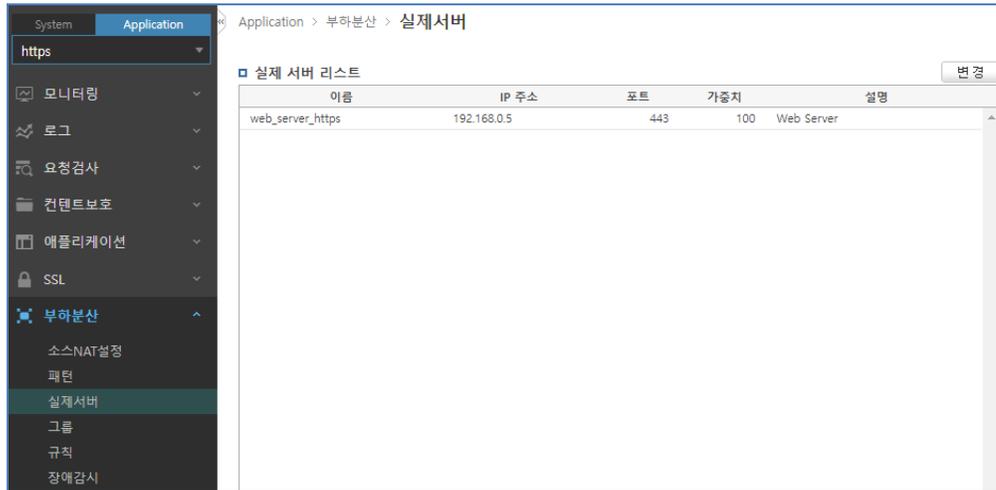
- ✓ 소스 NAT 상태 활성화 여부
- ✓ 소스 NAT IP 등록 여부

2. HTTPS

• WEBFRONT-KS 설정 체크

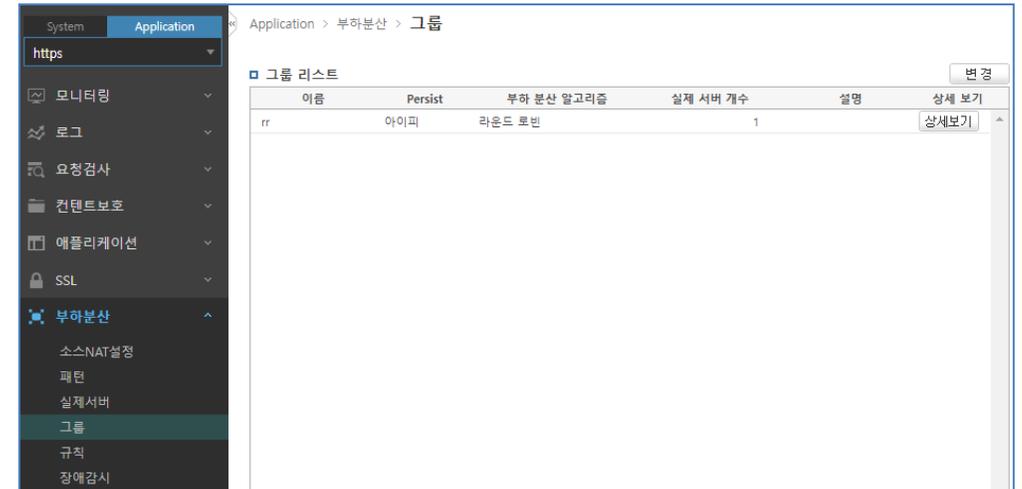
- 웹방화벽으로서 기능하기 위한 최소한의 설정 상태 체크

실제 서버 설정



- ✓ 실제서버 IP/Port 정상 등록 여부

그룹 설정



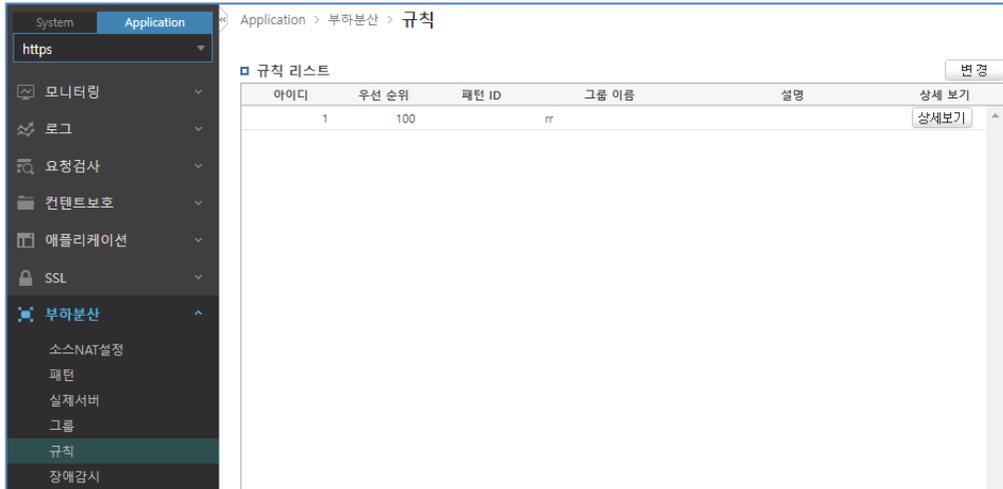
- ✓ 그룹에 등록된 실제 서버 개수 체크
- ✓ Persist 설정 여부

2. HTTPS

• WEBFRONT-KS 설정 체크

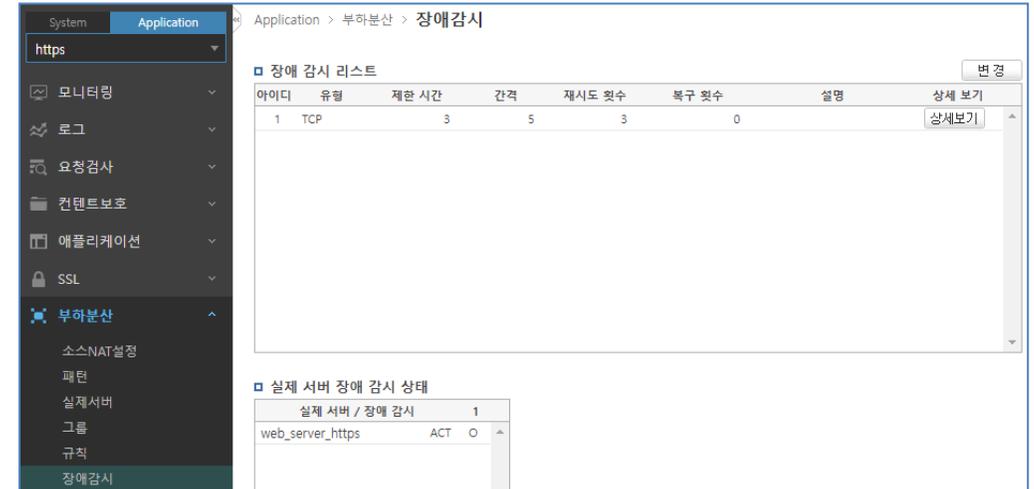
- 웹방화벽으로서 기능하기 위한 최소한의 설정 상태 체크

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



(주) 파이오링크

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