NAC EDU Chapter 2

구성요소

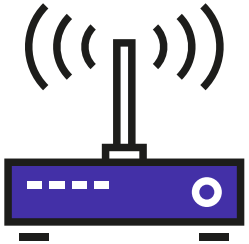
CONTENTS

구성요소

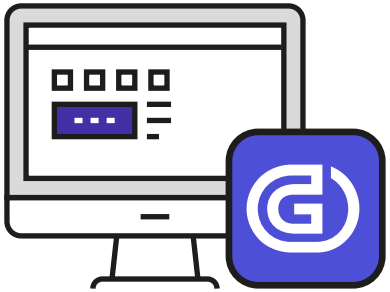
구성 요소

정책 서버

네트워크 센서



무선 센서



에이전트

구성 별 기능

Genian NAC

정책서버

- NAC 정책 설정 기능 제공
- 다수의 네트워크 센서 & 에이전트 관리
- 정책 및 노드의 실시간 상태 값 저장
- 발생되는 감사 로그 기록(저장)
- AAA : 인증(Authentication), 권한 부여(Authorization) 계정관리(Accounting)

네트워크 센서

- 네트워크 차단/허용 기능 수행사용자 역할 기반의 네트워크
  - 통제 기능 수행
- 이상 트래픽 발생 단말 탐지

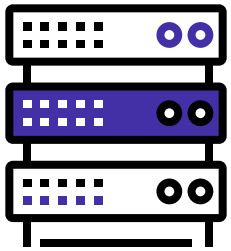
무선 센서

- Wireless 환경(Wifi)에서 발생되는 정보 수집
  - 접속 리스트 기반으로 접속 AP 제어

에이전트

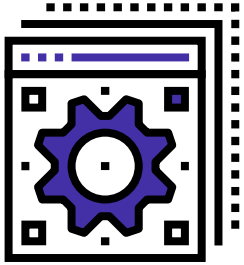
- 사용자 PC의 무결성 검증
  - OS패치(Windows), 백신, 필수 S/W 설치 검증
- 단말 정보 수집
  - Hardware, Software 정보 및 운영체제 정보 수집

정책 서버 구성 요소

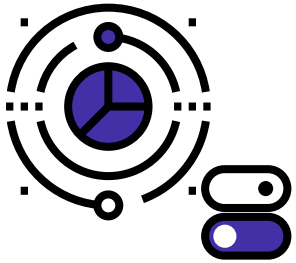


Web Server

Database Server



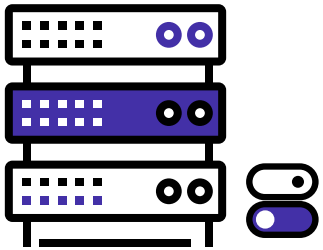
Log Server



Radius

네트워크 센서 구성 요소

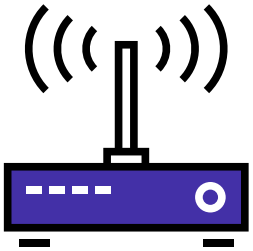
Genian NAC



Web Server

Enforce

무선 센서 구성 요소

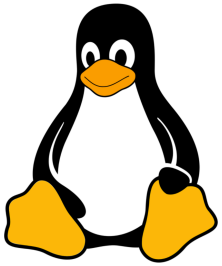


Access Point

Enforce

에이전트 구성 요소_지원 OS

Genian NAC



Windows

windows 7 이상

MAC

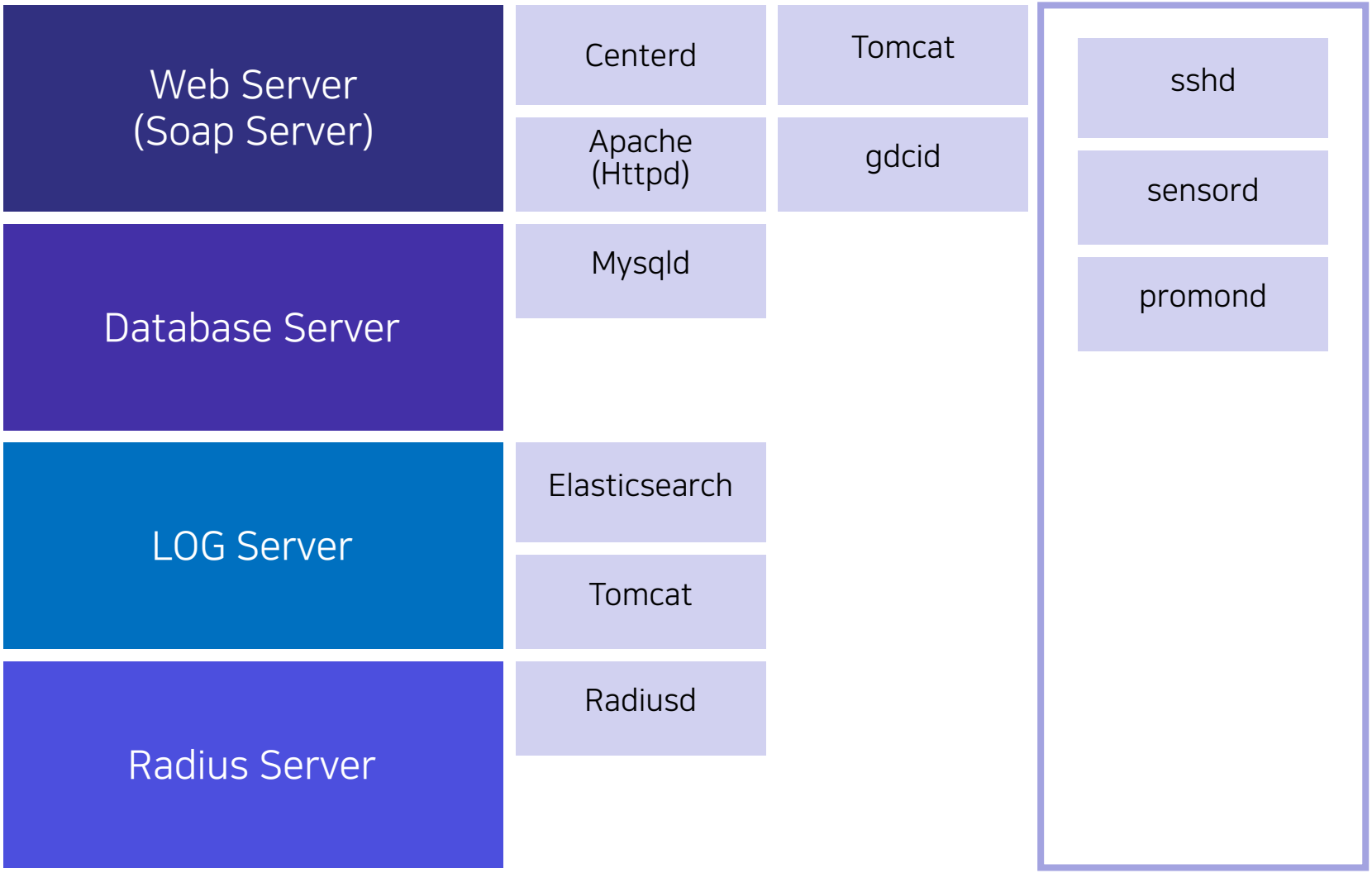
OS X Mavericks 이상

Linux

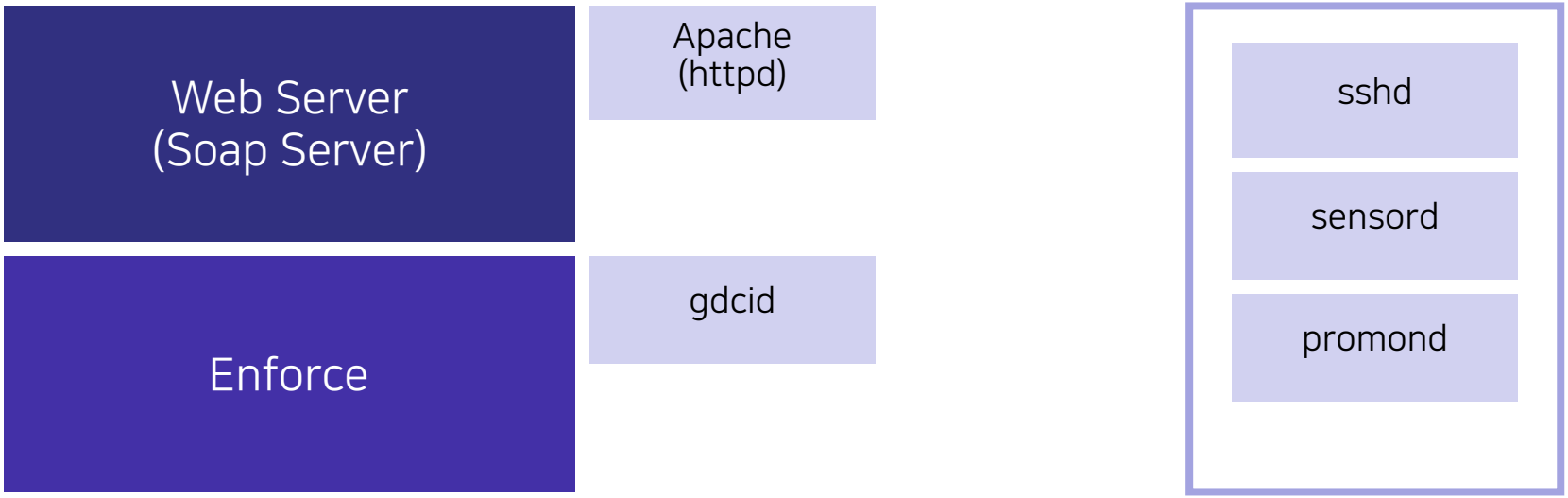
CentOS, Debian, Red Hat, Ubuntu ..

정책 서버 구성 별 동작 데몬

Genian NAC

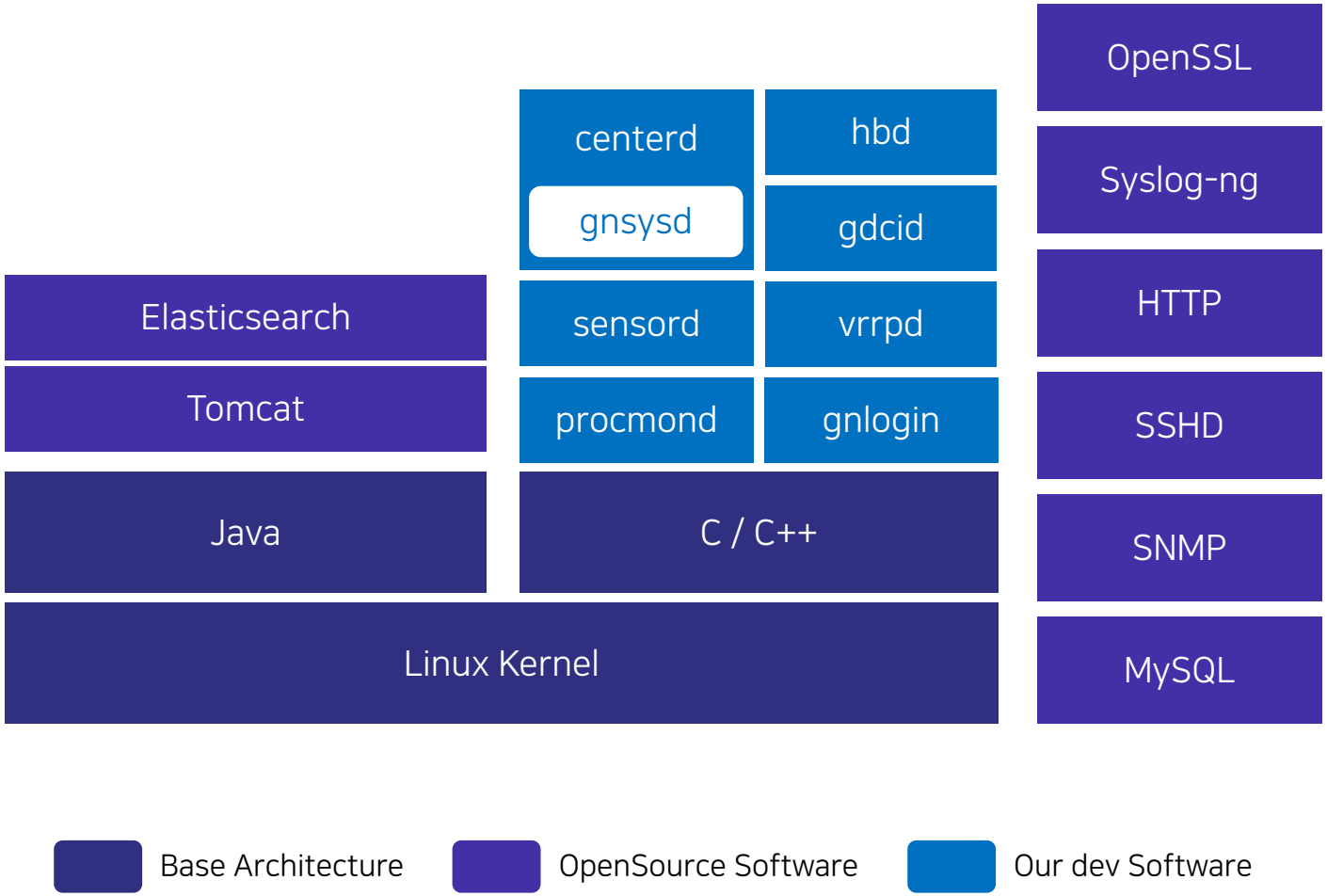


네트워크 센서 구성 별 동작 데몬

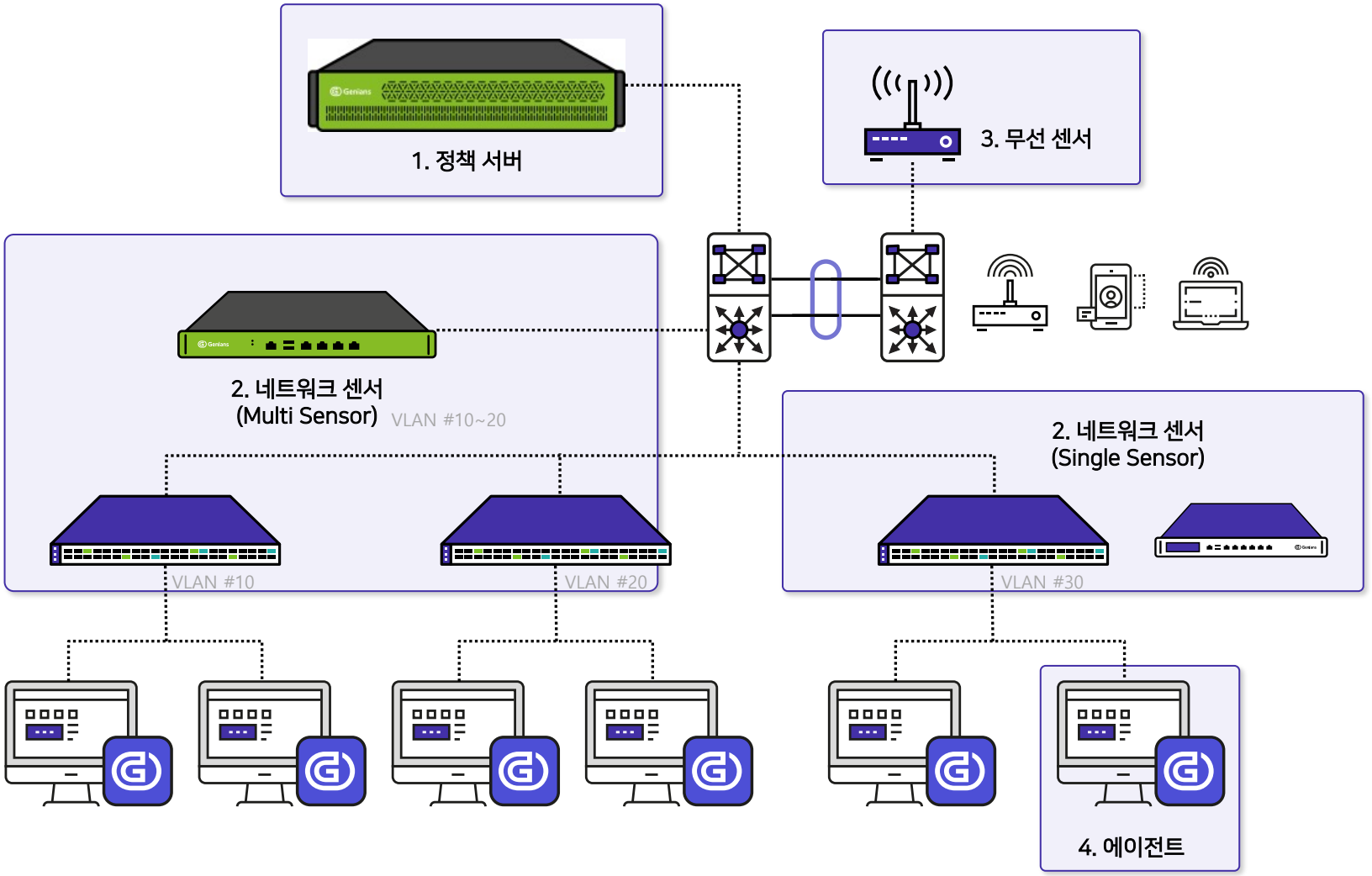


시스템 아키텍처

Genian NAC

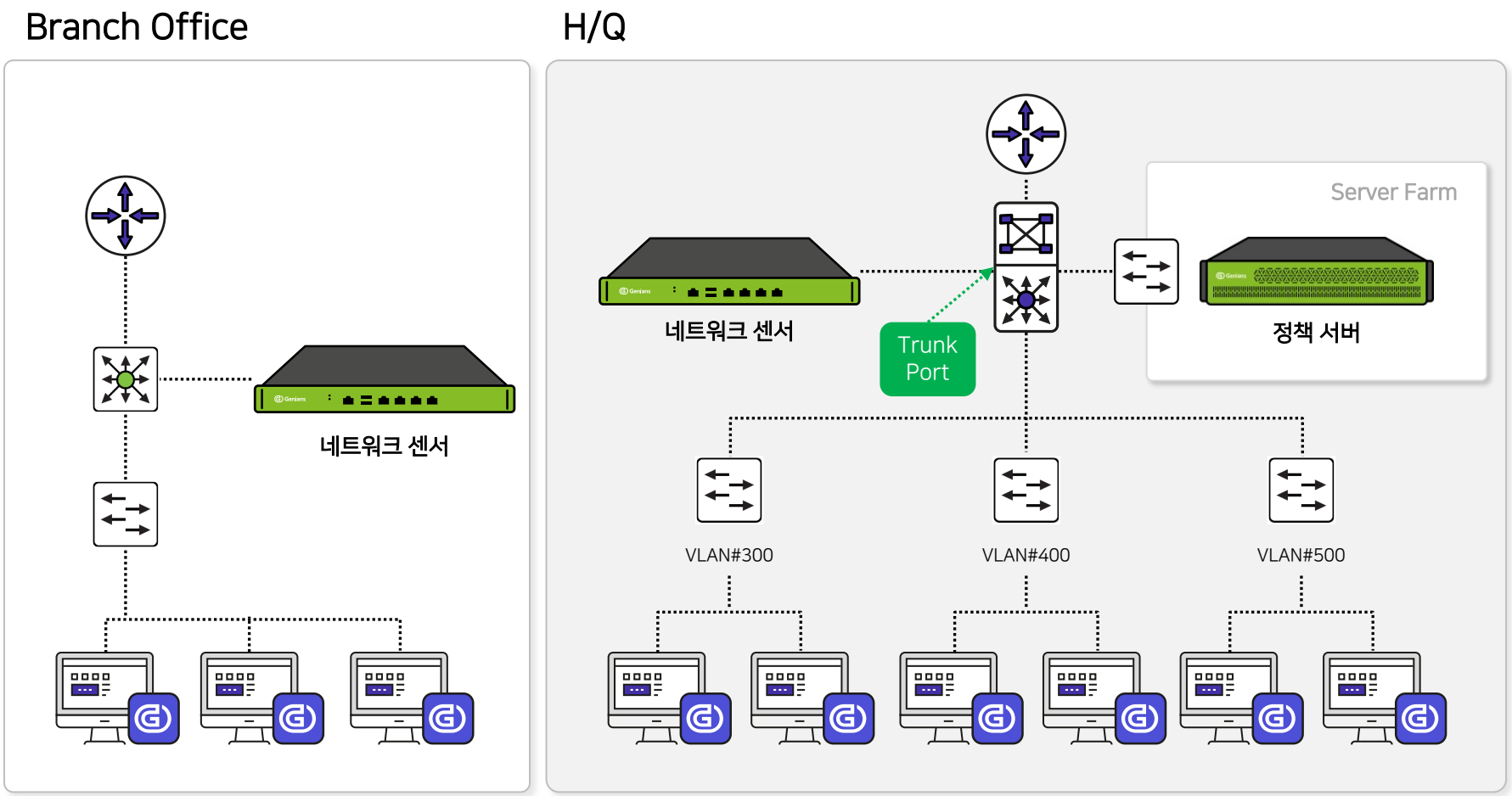


네트워크 구성도


1. 정책 서버
3. 무선 센서
2. 네트워크 센서
(Multi Sensor) VLAN #10~20
2. 네트워크 센서
(Single Sensor)
VLAN #10
VLAN #20
VLAN #30
4. 에이전트

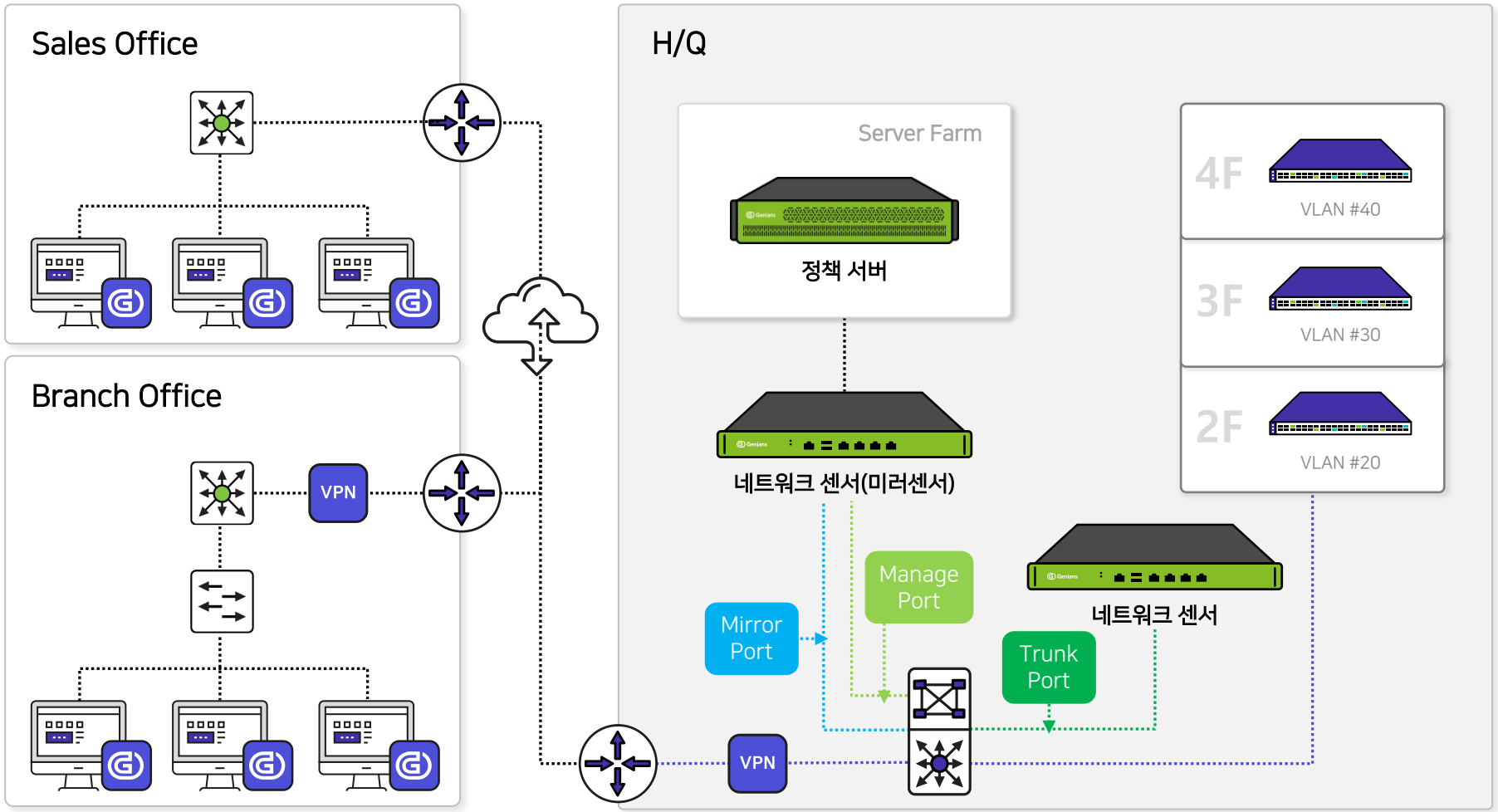
네트워크 구성도_멀티, 싱글 센서 구성

Genian NAC



네트워크 구성도_멀티, 미러 센서 구성

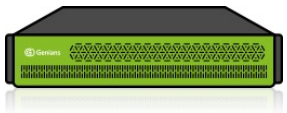
Genian NAC



Summary

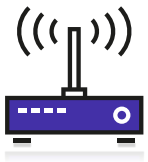
Genian NAC

1. Genian NAC 구성 요소



정책 서버

네트워크 센서



무선 센서

에이전트

2. Genian NAC 구성 별 세부 구성 요소

항목	내용
정책 서버	Web Server
	Database
	Log
	Radius

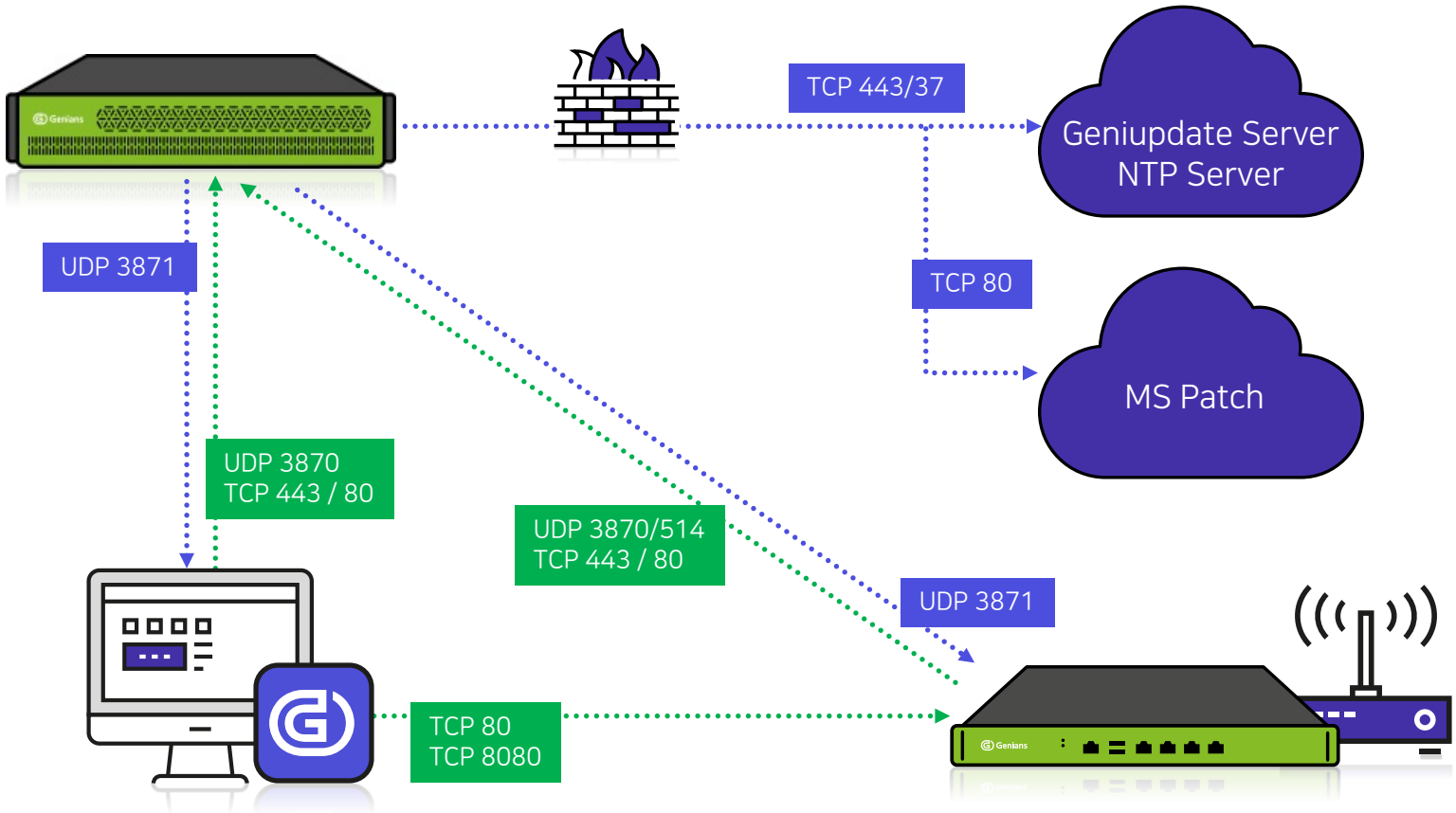
항목	내용
네트워크 센서	Web Server
	Enforce
무선 센서	Access Point
	Enforce

항목	내용
에이전트	윈도우
	리눅스
	맥

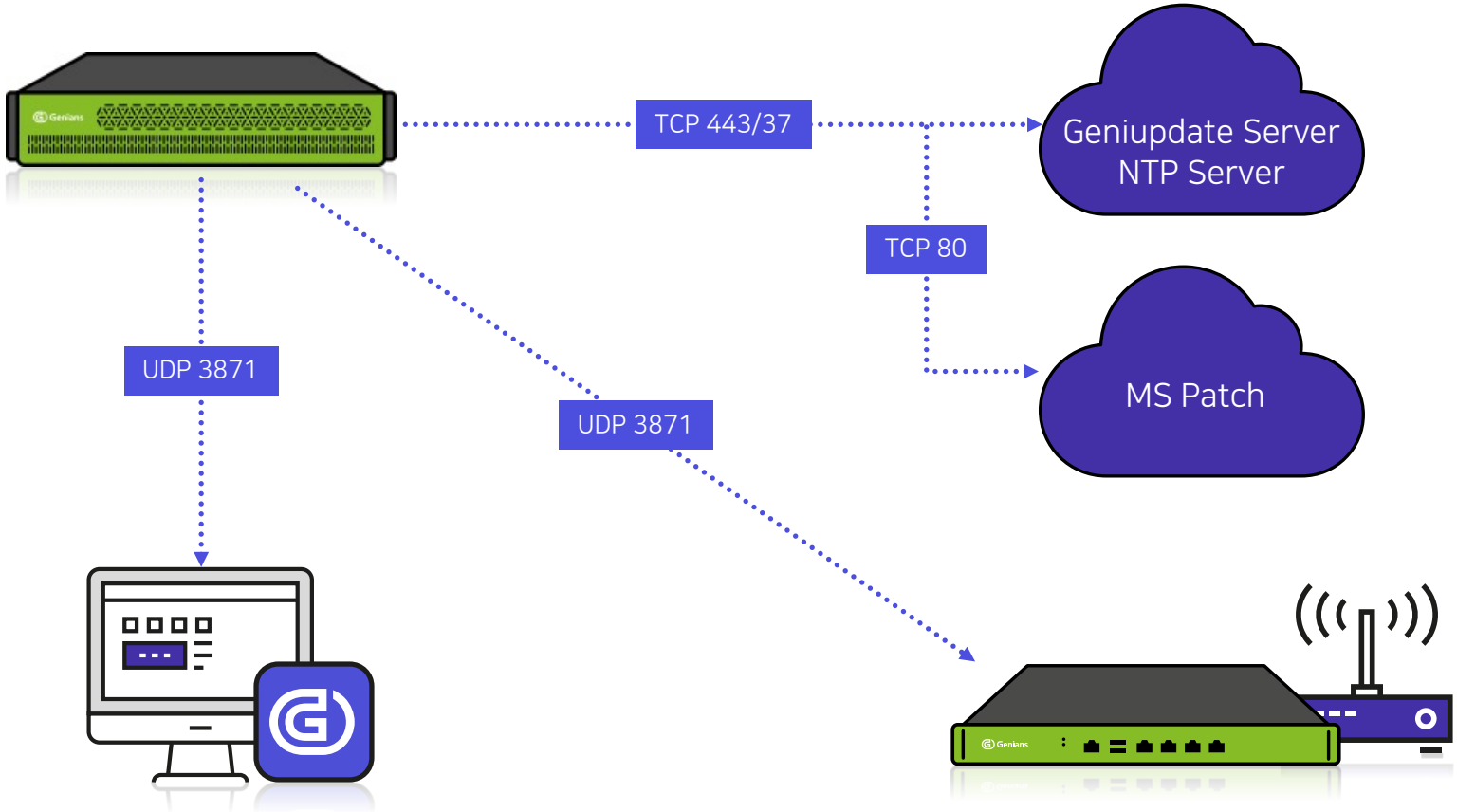
구성 간 네트워크 통신

구성 간 네트워크 통신

Genian NAC



구성 간 네트워크 통신_정책 서버



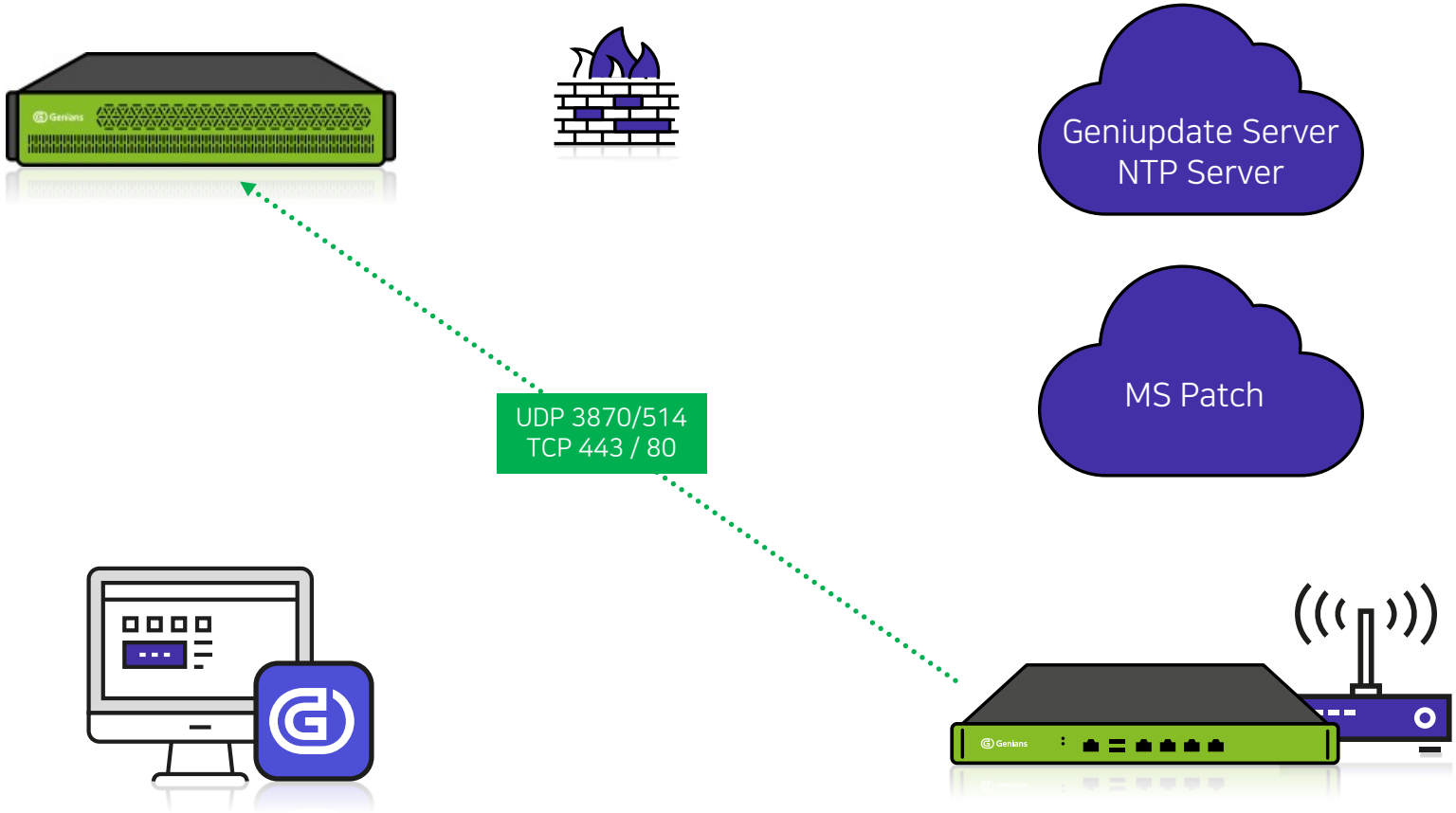
구성 간 네트워크 통신_정책 서버

Genian NAC

출발지	서비스	용도	목적지
정책 서버	TCP/443	Genian Data Sync SMS 전송	geniupdate. geninetworks.com
	TCP/37	NTP Server Sync	pool.ntp.org
	UDP/3871	이벤트 송신 Keep Alive	네트워크 센서 (무선 센서)
			에이전트

구성 간 네트워크 통신_네트워크 센서

Genian NAC



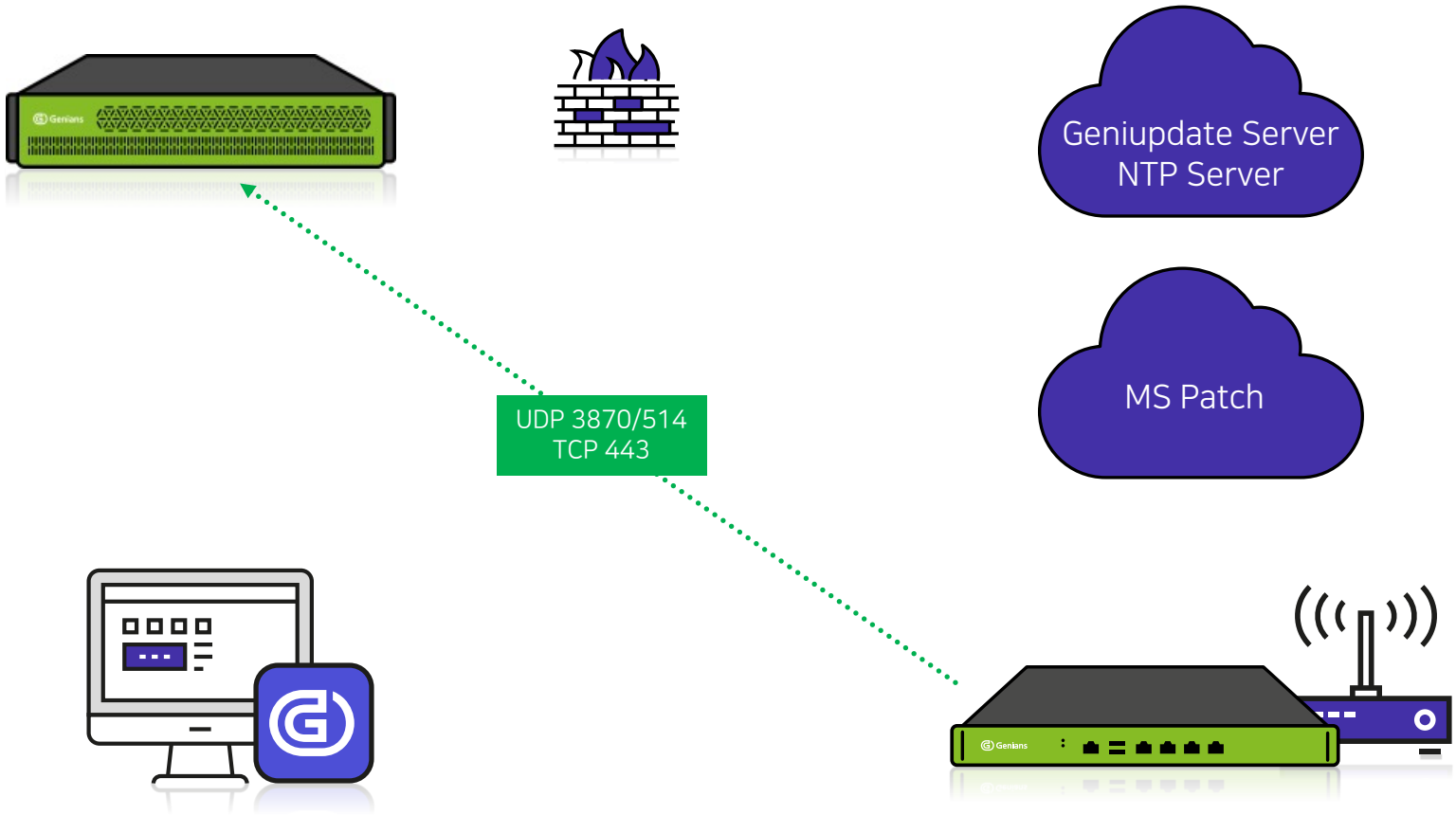
구성 간 네트워크 통신_네트워크 센서

Genian NAC

출발지	서비스	용도	목적지
네트워크 센서	UDP/3870	Keep Alive	정책 서버
	TCP/443	정책 수신	
	UDP/514	SYSLOG 전송	
	TCP/80	파일 다운로드	

구성 간 네트워크 통신 _무선 센서

Genian NAC

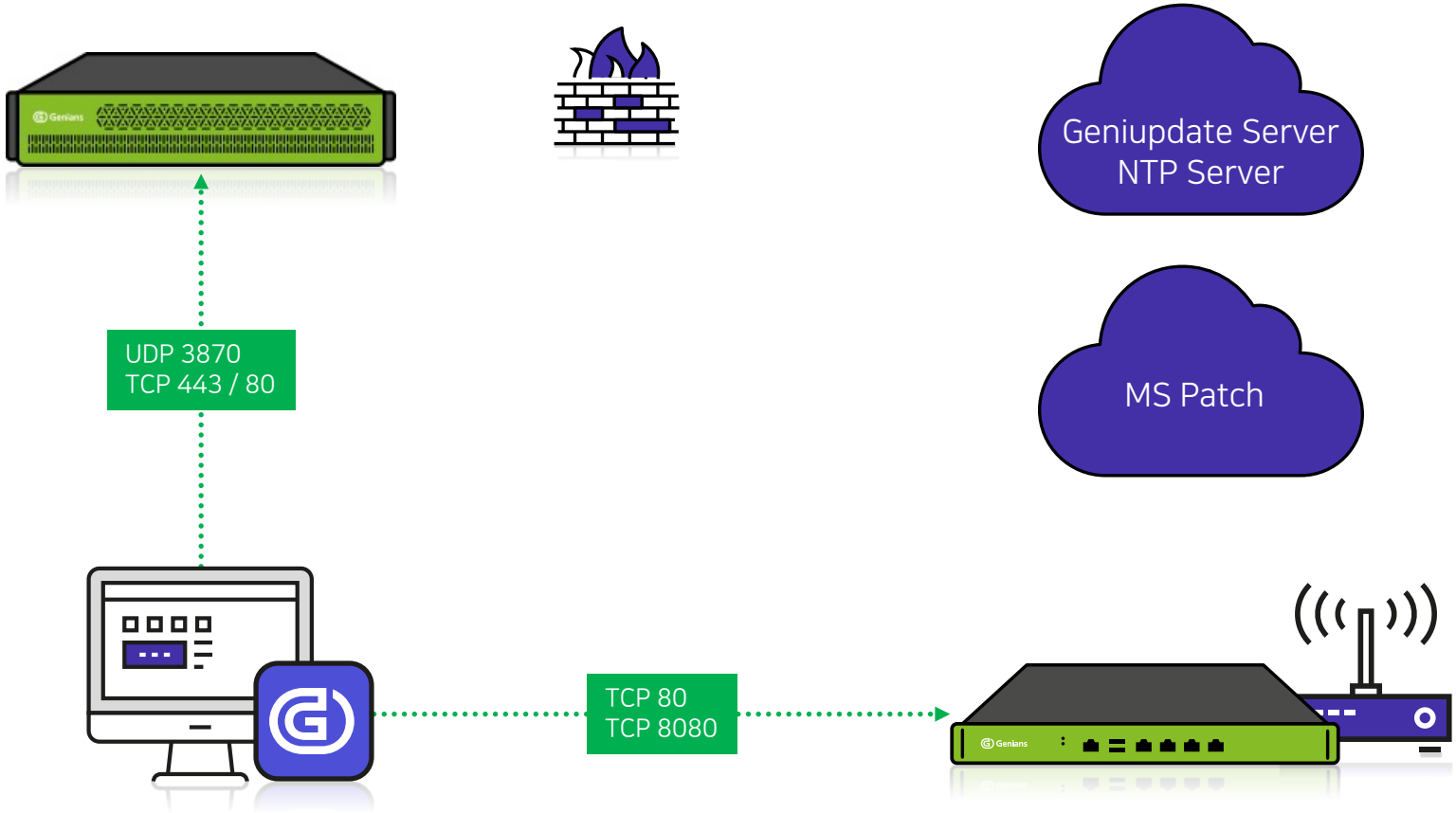


구성 간 네트워크 통신 _무선 센서

Genian NAC

출발지	서비스	용도	목적지
무선센서	UDP/3870	Keep Alive	정책서버
	TCP/443	정책 수신	
	UDP/514	SYSLOG 전송	

구성 간 네트워크 통신 _에이전트



구성 간 네트워크 통신 _에이전트

Genian NAC

출발지	서비스	용도	목적지
에이전트	UDP/3870	Keep Alive	정책 서버
	TCP/443	SOAP 통신 파일 다운로드	
	TCP / 80	SOAP 통신 파일 다운로드	
	TCP/ 8080	PMS	네트워크 센서 (운영체제 업데이트 Proxy 서비스 설정)

Summary

Genian NAC

1. 정책 서버 외부 통신

항목	내용	목적
정책 서버	geniupdate.geninetworks.com	Genian Data Sync, PMS Patch list
	pool.ntp.org	Time Sync

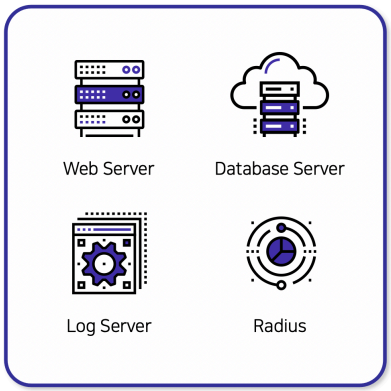
2. Keep Alive 확인

대상	포트	대상	포트
네트워크 센서 무선 센서 에이전트	3871	정책 서버	3870

구성 방안

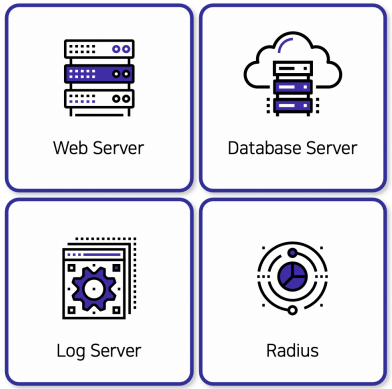
정책 서버 구성 방안

Genian NAC



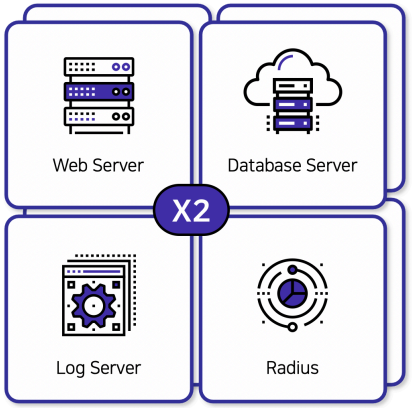
1. 단일 구성

하나의 장비에
정책 서버를 구성하는 방식



2. 분리 구성

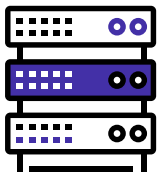
정책 서버 구성 요소를
다수의 장비로 분리하여
구성하는 방식



3. HA 구성

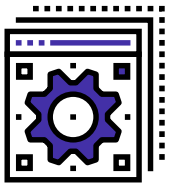
정책 서버 구성 요소를
이중화 구성하는 방식

정책 서버_단일 구성

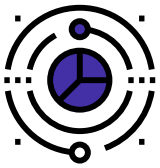


Web Server

Database Server



Log Server



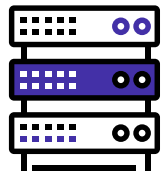
Radius

비용절감 효과

Single Point
of Failure

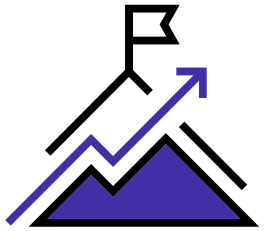
정책 서버_분리 구성

Genian NAC

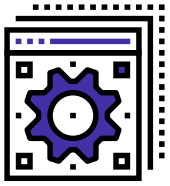


Web Server

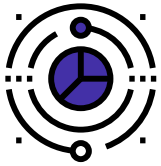
Database Server



성능 향상



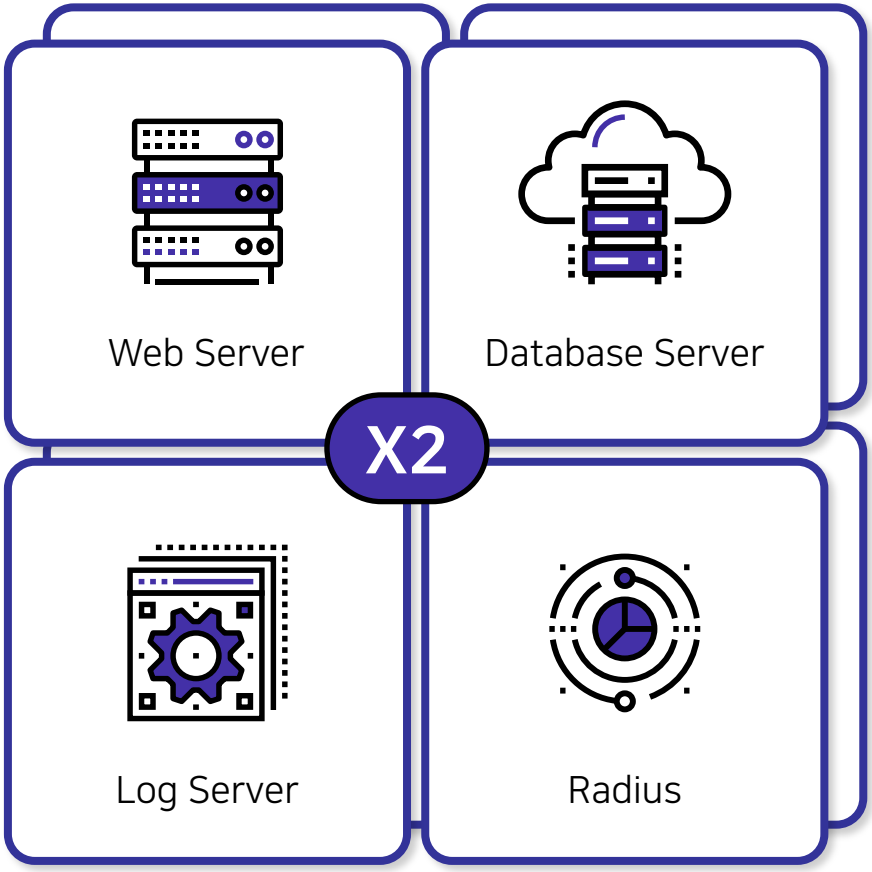
Log Server

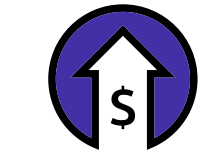


Radius

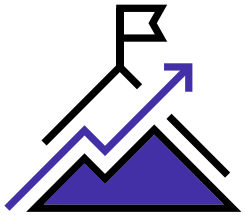
Single Point
of Failure

정책 서버_HA 구성

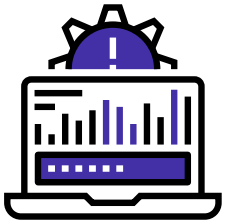




비용 상승



성능 향상



Fault tolerant

네트워크 센서 구성 방안

Genian NAC

1. 단일 구성

2. 멀티 구성 (802.1q)

3. HA 구성

4. Mirror 구성

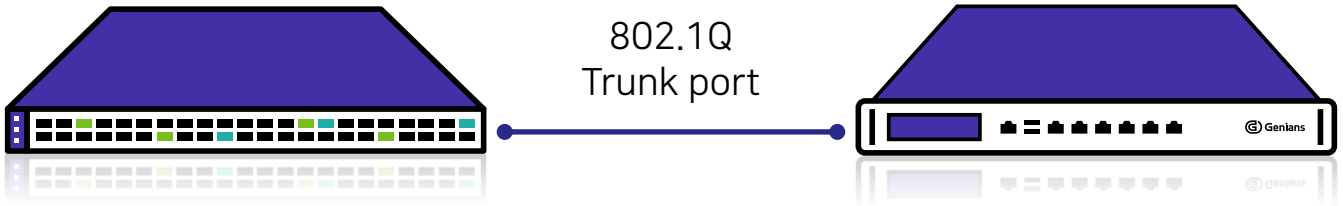
5. Bonding 구성

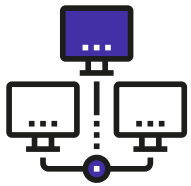
네트워크 센서_단일 구성

네트워크 대역 수량 < = 설정 포트수

네트워크 센서_멀티 구성

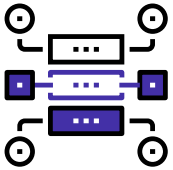
Genian NAC





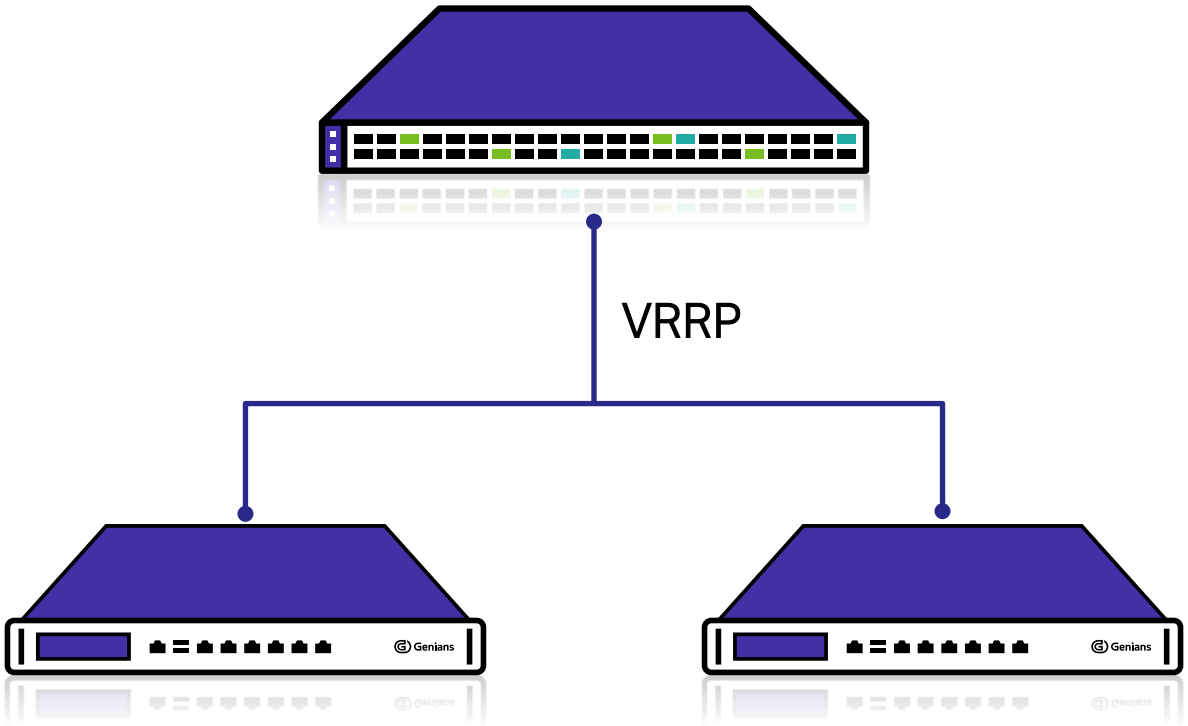
네트워크 대역 수량

>

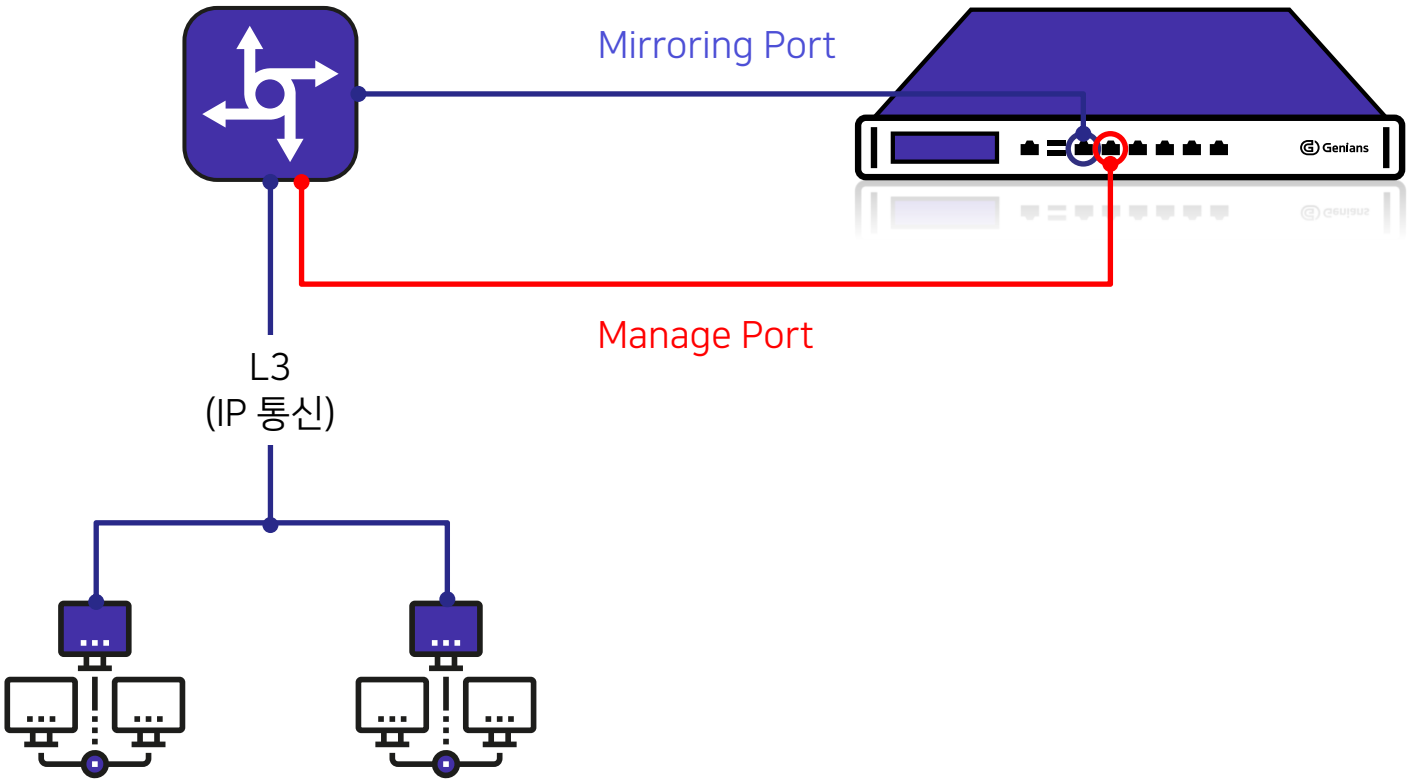


설정 포트

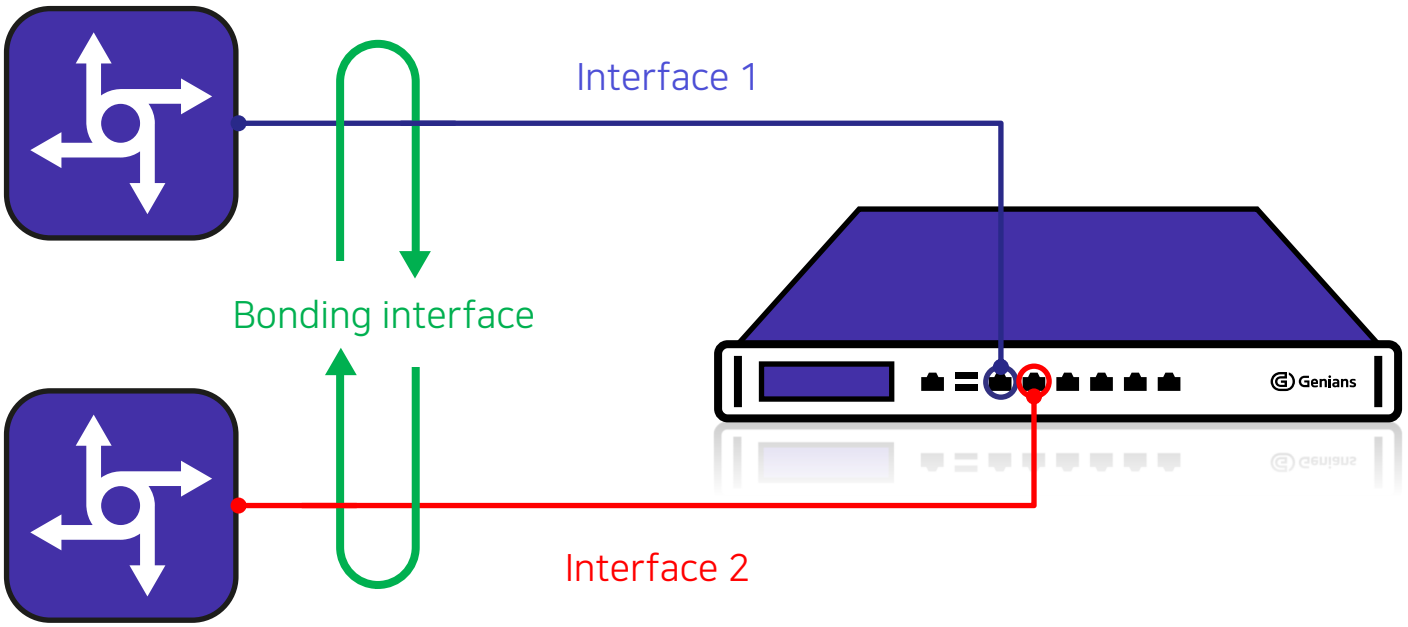
네트워크 센서_HA 구성



네트워크 센서_Mirror 구성



네트워크 센서_Bonding 구성



Summary

1. 정책 서버

항목	내용
단일 구성	모든 모듈을 하나에 장비에 구성
분리 구성	모듈별 별도의 장비에 구성
HA 구성	고가용성을 위해 Slave 장비 추가 구성

2. 네트워크 센서

항목	내용
단일 구성	물리적인 인터페이스로 구성
멀티 구성	VLAN 논리적인 인터페이스로 구성
HA 구성	고가용성을 위해 Slave 장비 추가 구성
Mirror 구성	L3 기반 IP제어를 위해 구성
Bonding 구성	스위치 고가용성을 위해 구성

Genians

문의 : 지니언스 네트워크보안기술부

ca-se-nac@genians.com