NAC EDU Chapter 4

WebUI - 정책 설정

CONTENTS

- 그룹
- 객체
- 정책

학습 전 확인 사항

Genian NAC

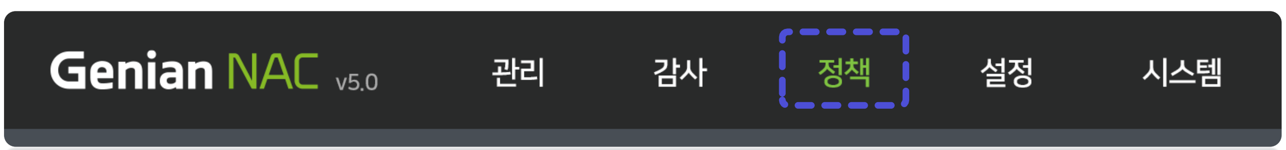
WebUI 관련 교육으로 기본적으로 WebUI 접속이 가능한지 여부 확인

Step 1. CLI Mode에서 WebUI 접속 계정 생성

Step 2. 웹브라우저에서 **접속 포트를 8443으로 변경**하여 WebUI 접속

(URL -> https://[정책서버 IP]:8443/mc2)

Step 3. 상위 메뉴화면에서 **정책** 항목 선택



그룹

그룹

노드
그룹

무선랜
그룹

사용자
그룹

그룹 - 노드 그룹

그룹 - 노드 그룹

Genian NAC

Step 1. 기본정보

카테고리	노드 그룹 포함될 카테고리를 지정하거나 생성합니다.
ID	**노드 그룹 이름을 지정합니다.**
설명	노드 그룹 설명을 입력합니다.
CWP 메시지	노드 그룹에 포함될 경우 CWP 페이지 표시 메시지를 입력합니다.
적용 모드	노드 그룹 사용 유/무를 선택합니다.
감사 로그	노드 그룹 포함 여부를 감사 로그에 남길지 여부를 선택합니다.
노드 관리 기본 뷰	노드 그룹에 포함된 노드를 표시할 때 사용할 뷰를 선택합니다.

그룹 - 노드 그룹

Genian NAC

Step 2. 노드 그룹 조건

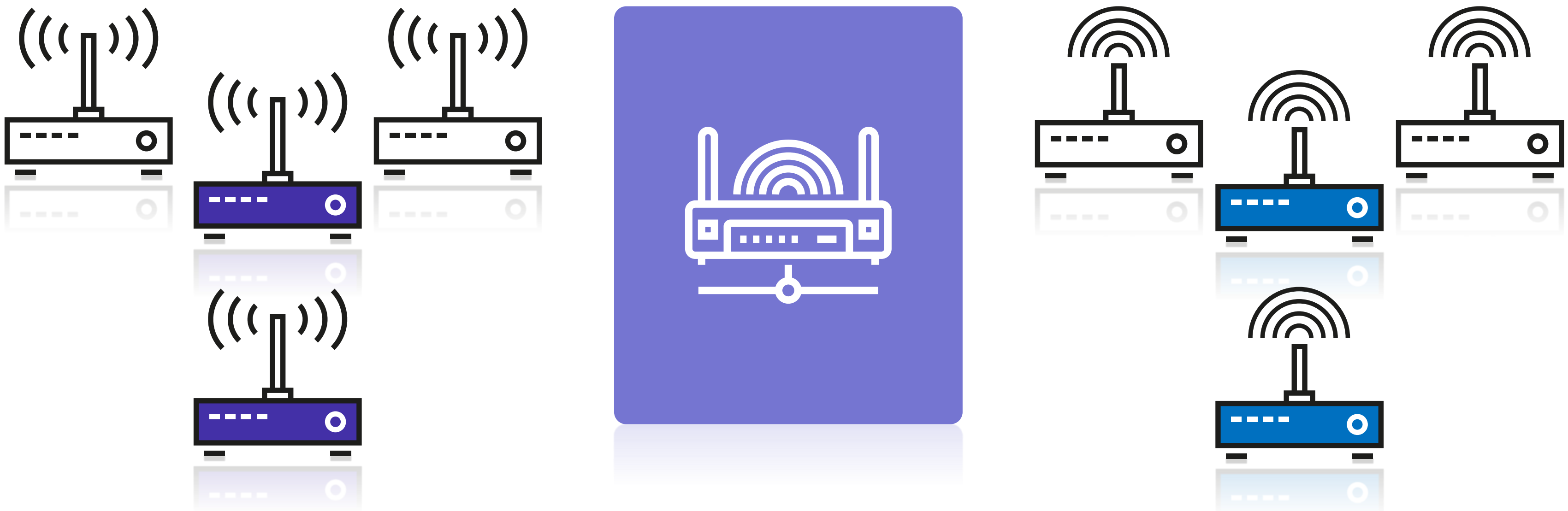
에이전트	태그	노드 타입
IPv6 주소	시간	인증 사용자
IP주소	장비소유자	센서
MAC+IP 주소	IP관리	등록일자
MAC 주소	정책그룹	

그룹 - 상태 그룹 조건

Genian NAC

에이전트	태그	노드타입	가동시간	장비설명	GPI 검사결과	운영체제 업데이트	메모
IPv6 주소	시간	인증사용자	계정 비밀번호 검증	제조일	서약동의	노드정책	플랫폼
IP주소	장비소유자	센서	네트워크	구입처	장비내 무선랜	서비스	호스트/ 도메인명
MAC+IP 주소	IP관리	등록일자	백신정보	내용연수 시작일	연결포트	이름/설명	USB 장치정보
MAC 주소	정책그룹		소프트웨어	내용연수 만료일	위험감지	호스트명제한	WMI 정보수집
NAT	접속AP	운영체제 유형	시스템	일련번호	에이전트 액션	책임자	장비명
업/다운 상태	노드그룹	트래픽	시스템 사용자 계정	구입가격	에이전트 상태	책임부서	GPI점수
플랫폼 보안취약점	열린포트						

그룹 - 무선랜 그룹



그룹 - 무선랜 그룹

Step 1. 기본정보

ID	**노드 그룹 이름을 지정합니다.**
설명	노드 그룹 설명을 입력합니다.
적용 모드	노드 그룹 사용 유/무를 선택합니다.
감사 로그	노드 그룹 포함 여부를 감사 로그에 남길지 여부를 선택합니다.

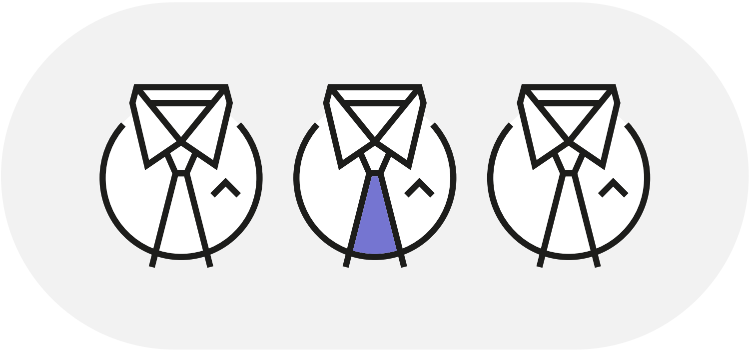
그룹 - 무선랜 그룹 조건

Genian NAC

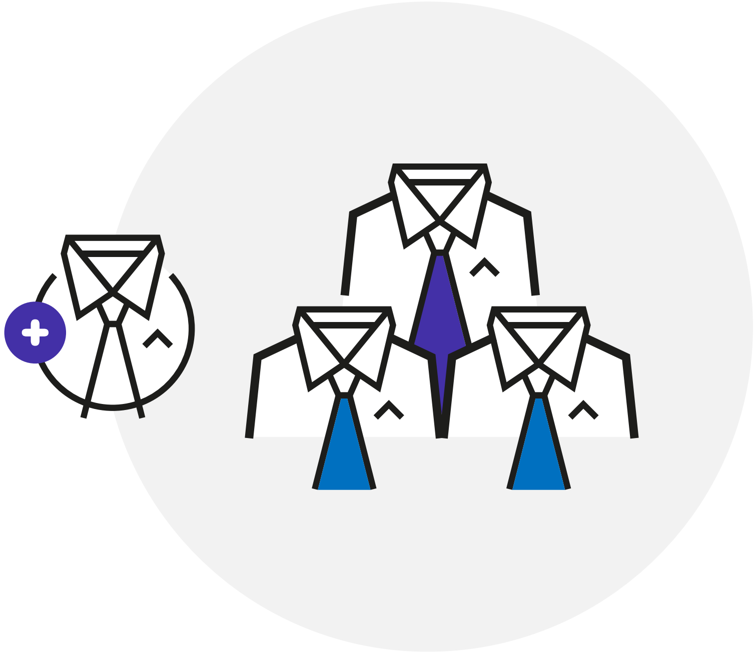
Step 2. 무선랜 그룹 조건

802.11프로토콜	MAC+SSID
MAC주소	SSID
무선랜 그룹	보안설정
상태 및 속성	인가 상태
태그	

그룹 - 사용자 그룹



NAC DB의 사용자 계정



사용자 계정의 상태, 부서, 직급 등

그룹 - 사용자 그룹

Genian NAC

Step 1. 기본정보

ID	**노드 그룹 이름을 지정합니다.**
설명	노드 그룹 설명을 입력합니다.
적용 모드	노드 그룹 사용 유/무를 선택합니다.

그룹 - 사용자 그룹 조건

Step 2. 사용자 그룹 조건

IP인증 제한	동기화 여부	사용자ID	전화번호
MAC 인증 제한	마지막 인증 시각	사용자 그룹	직급
계정 상태	만료 시각	설명	태그
계정 용도	멤버쉽	이메일 주소	회사명
계정중지사유	부서	인증 상태	휴대 전화번호
관리자권한	비밀번호	장비인증제한	

그룹 Summary

노드 그룹

노드정책 / 제어 정책 대상을
지정할 경우 사용

무선랜 그룹

노드 그룹에 ‘장비내 무선랜’,
‘접속 AP’ 조건에 사용

사용자 그룹

정책 - 노드 정책 - 인증 정책
정책 - 그룹 - 노드 그룹(조건)
설정 - 속성 관리 - IP용도

객체

객체

1. 네트워크

- IP / subnet mask
- IP Range
- FQDN
  (Fully Qualified Domain Name)

2. 서비스

- TCP
- UDP
- ICMP

3. 시간

- 기간 / 시간대 /요일

1. 네트워크 객체

2. 서비스 객체

3. 시간 객체

4. 권한

객체 - 네트워크 객체

Genian NAC

Step 1. 기본정보

ID	**네트워크 객체 이름을 지정합니다.**
설명	네트워크 객체 설명을 입력합니다.

Step 2. 포함 그룹

Step 3. 네트워크 주소

객체 - 서비스 객체

Step 1. 기본정보

ID	**서비스 객체 이름을 지정합니다.**
설명	서비스 객체 설명을 입력합니다.

Step 2. 포함 그룹

Step 3. 서비스 포트

객체 - 시간 객체

Step 1. 기본정보

ID	**시간 객체 이름을 지정합니다.**
설명	시간 객체 설명을 입력합니다.

Step 2. 포함 그룹

Step 3. 시간 객체

객체 - 권한 객체

Genian NAC

Step 1. 기본정보

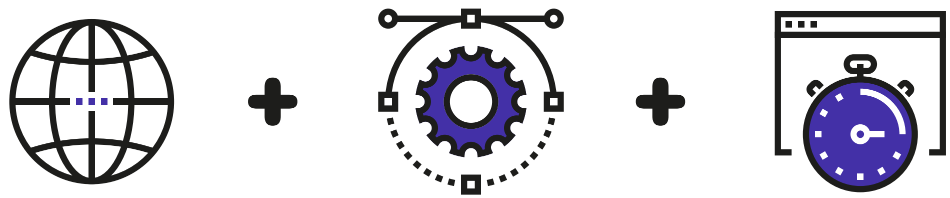
ID	**권한 객체 이름을 지정합니다.**
설명	권한 객체 설명을 입력합니다.

Step 2. 네트워크 객체

Step 3. 서비스 객체

Step 4. 시간 객체

객체 Summary



네트워크 객체　　서비스 객체　　시간 객체

권한 = 네트워크 객체 + 시간 객체 + 서비스 객체

네트워크 객체의 FQDN이란?

'전체 도메인 네임' 불리는 도메인 전체 이름을 표기하는 방식 설정

정책

정책

Genian NAC

1. 노드 정책

2. 제어 정책

3. 802.1x 정책

4. 무선랜 정책

5. Windows 업데이트 정책

6. 장치 제어 정책

Agent Action

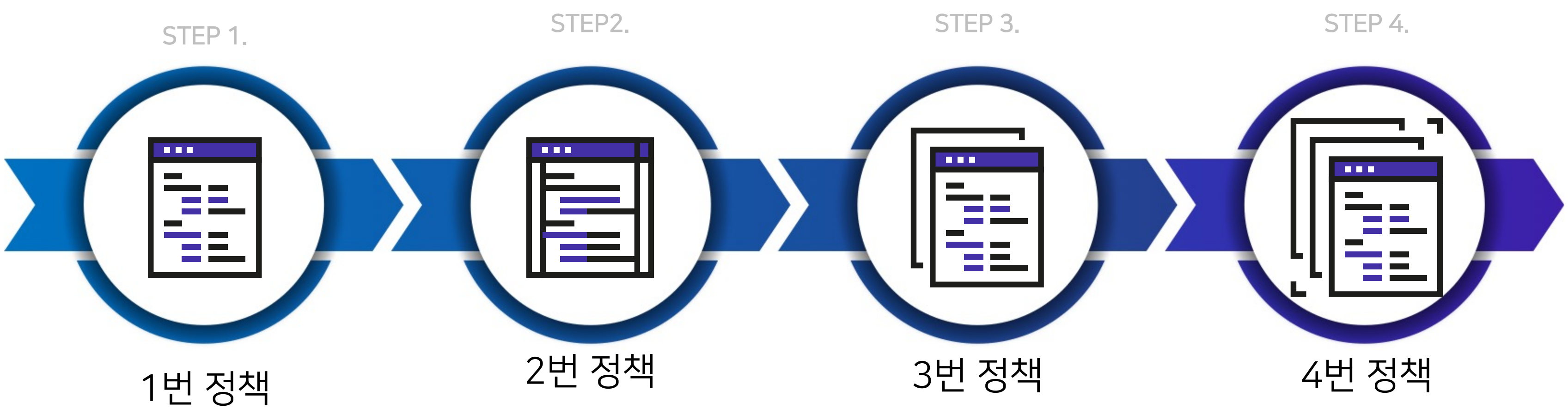
7. 컴플라이언스 정책

정책

단일 정책	복수 정책
노드 정책	무선랜 정책
제어 정책	장치 제어 정책
802.1X 정책	컴플라이언스 정책
Windows 업데이트 정책	

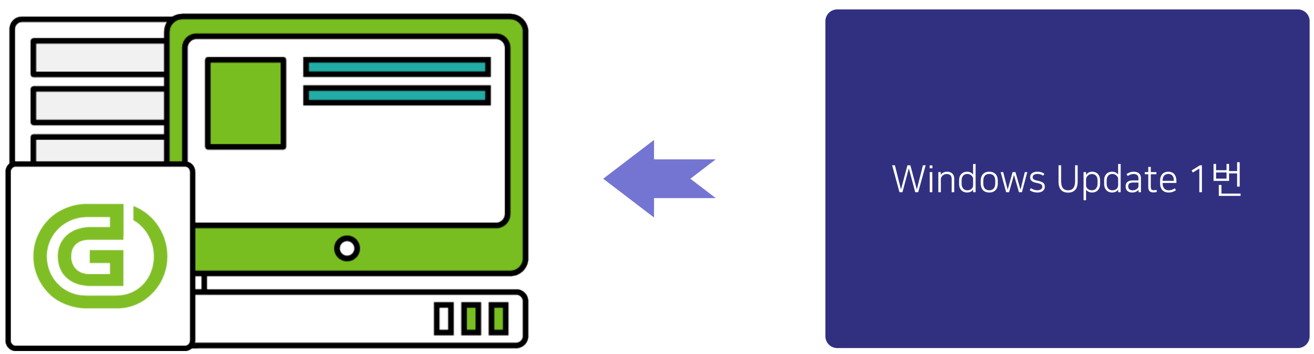
정책 – 정책 할당 방식

1. 노드정책, 제어정책, 802.1x 정책



정책 – 정책 할당 방식

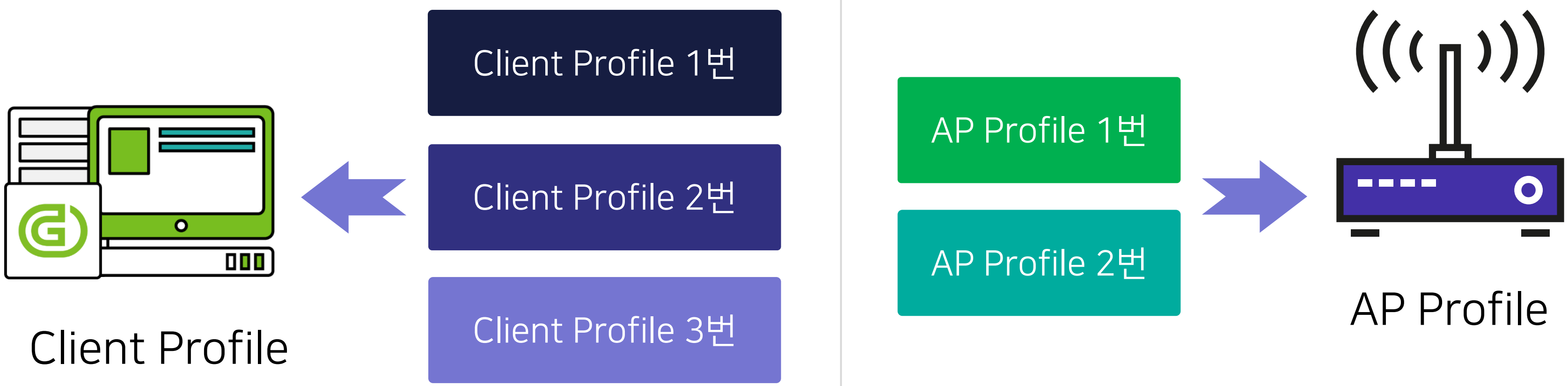
2. Windows 업데이트 정책



Windows 단말

정책 – 정책 할당 방식

3. 무선랜 정책

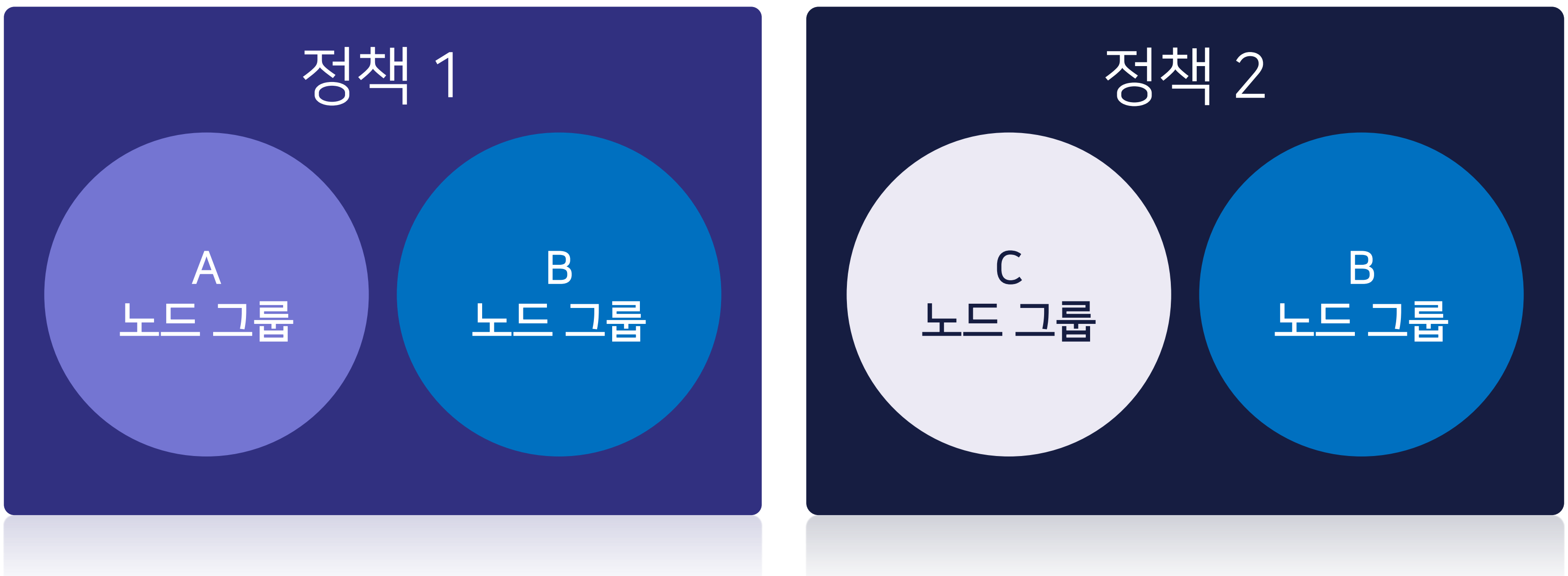


정책 – 정책 할당 방식

4. 장치 제어 정책

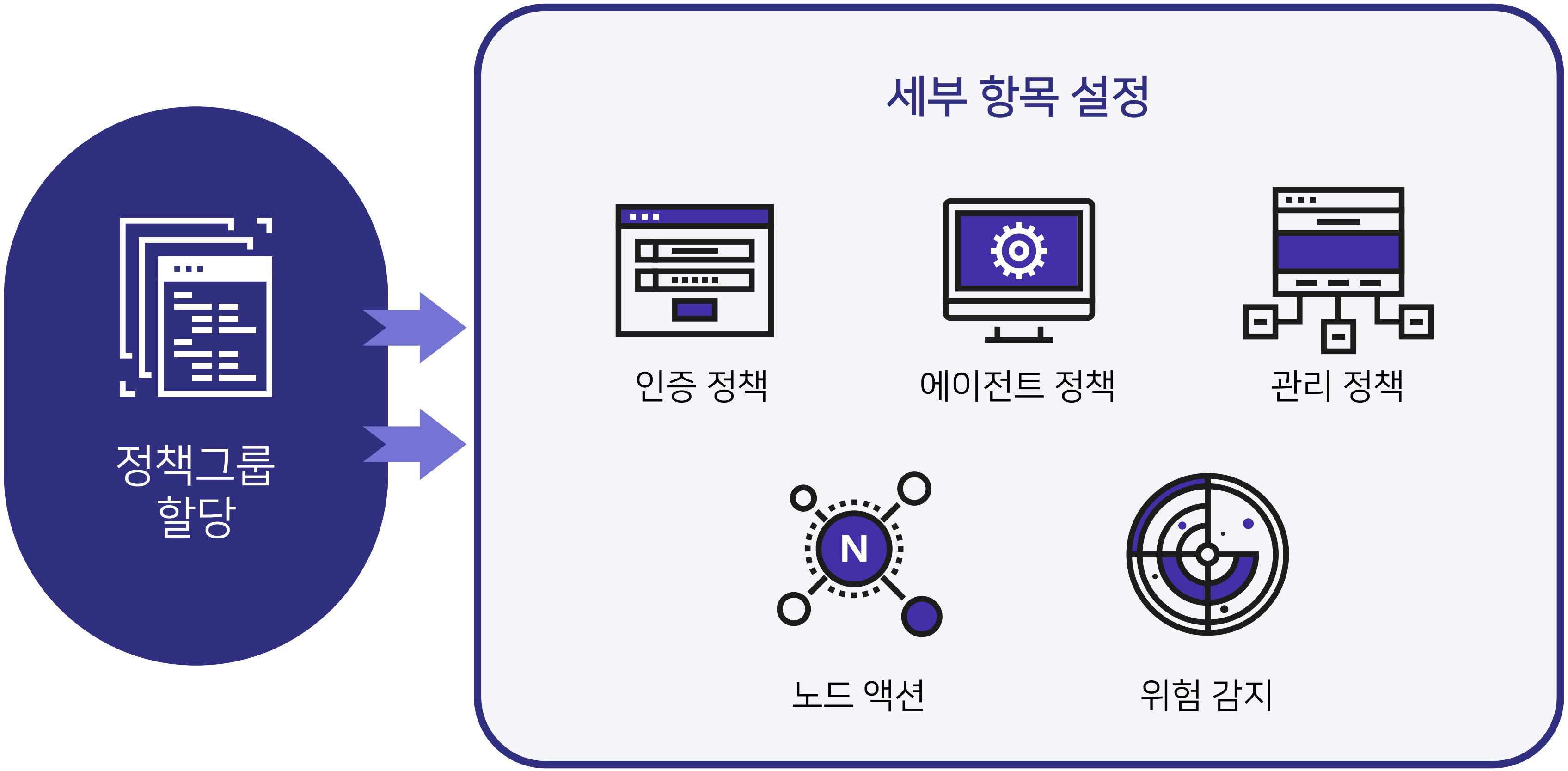
정책 – 정책 할당 방식

5. 컴플라이언스 정책



정책 - 노드 정책

- 정책 – 노드 정책 - 노드 액션
- 정책 – 노드 정책 – 위험 감지



정책 - 노드 정책 세부 설정

Genian NAC

1. **인증 정책**
   비밀번호 인증방식 : Local DB, Radius, LDAP, POP3, IMAP, SMTP, Webhook

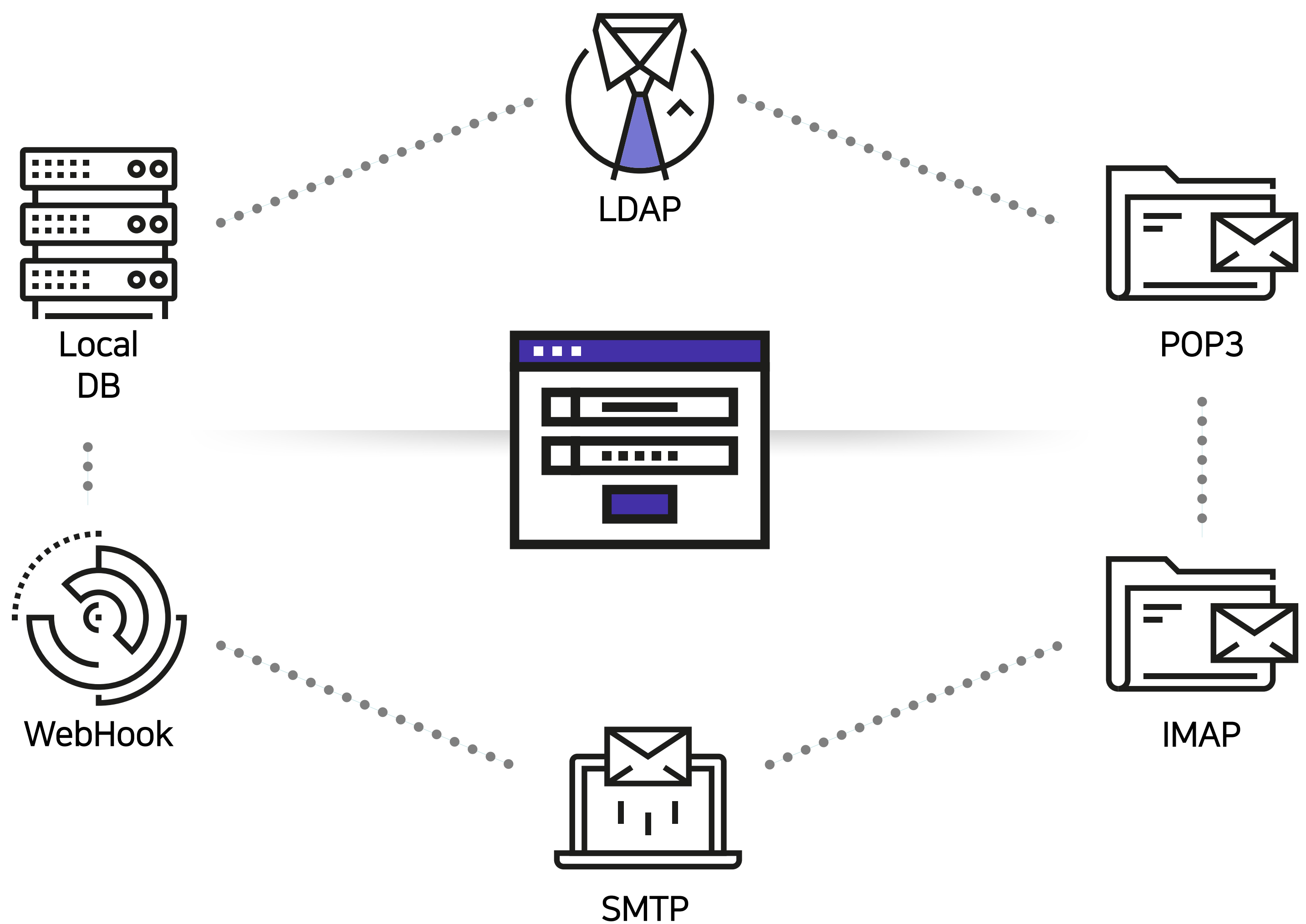
2. **에이전트 정책**
   에이전트 사용 유/무, Dissolvable Agent , 수행 계정 설정

3. **관리 정책**
   신규 노드의 호스트명 제한, 비활성 노드의 삭제 기간 설정

4. **에이전트 액션**
   정의된 에이전트 액션을 수행하도록 할당 설정

5. **위험 감지**
   위험으로 탐지할 이벤트를 할당 설정

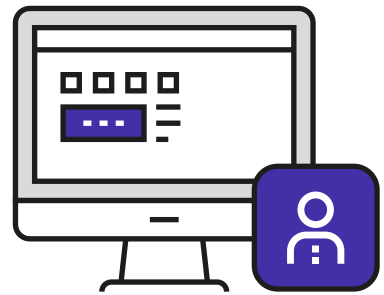
정책 - 노드 정책 > 인증 정책



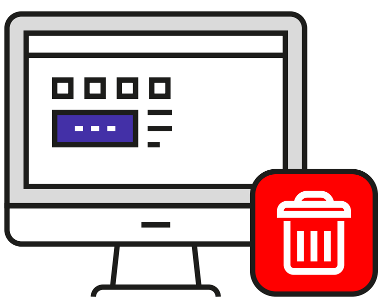
정책 - 노드 정책 > 에이전트 정책

Genian NAC

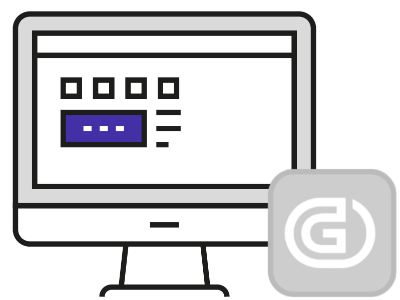
에이전트 사용 유 무



수행 계정 설정



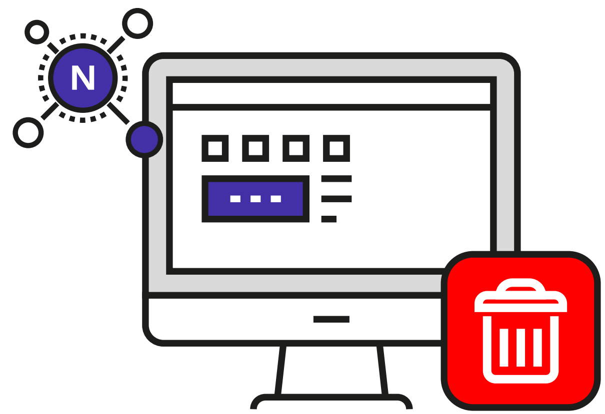
에이전트 정보 삭제



Dissolvable Agent

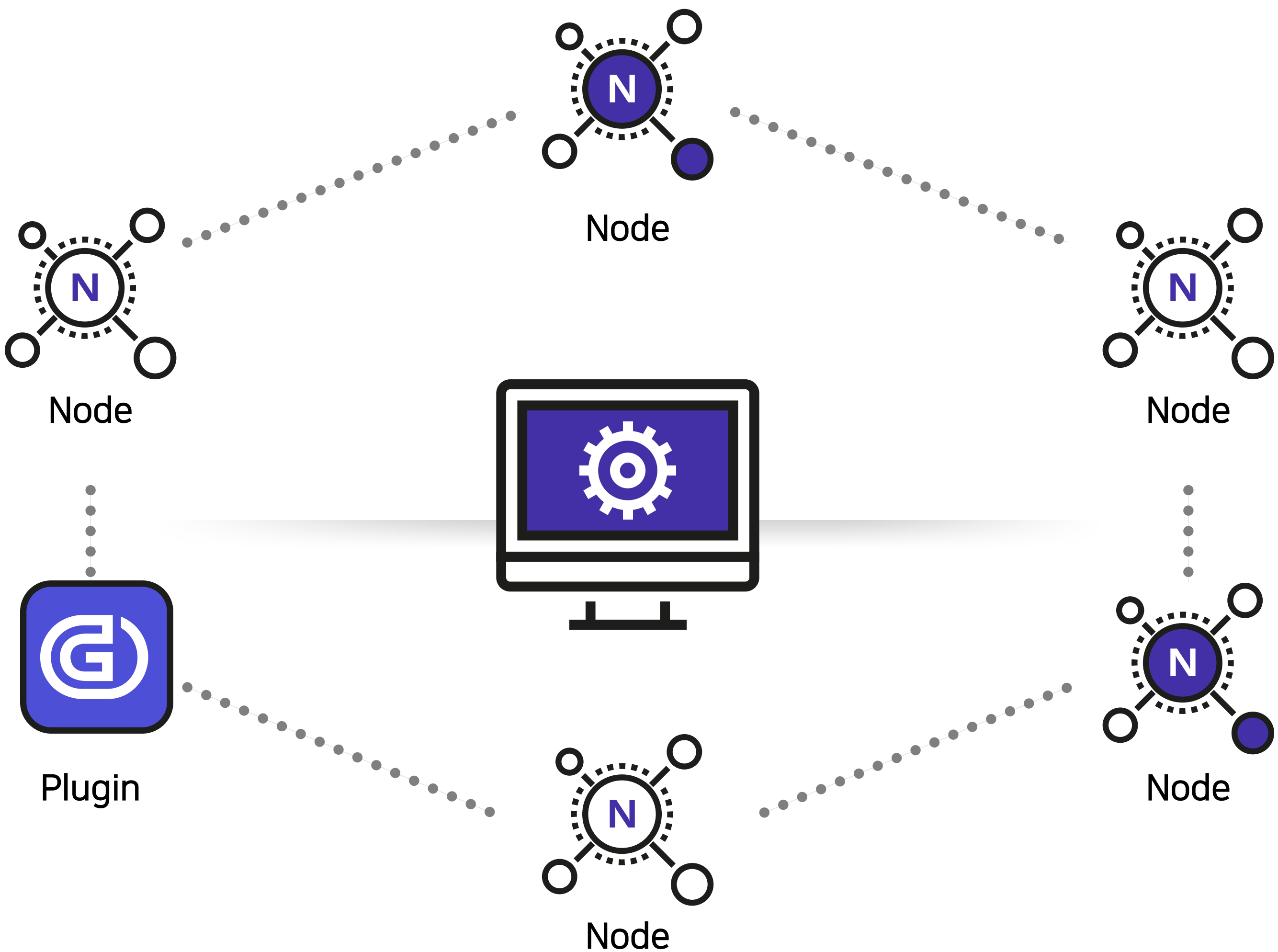
정책 - 노드 정책 > 관리 정책

Hostname
제한



비활성 노드
삭제 기능

정책 - 노드 정책 > 노드 액션 설정



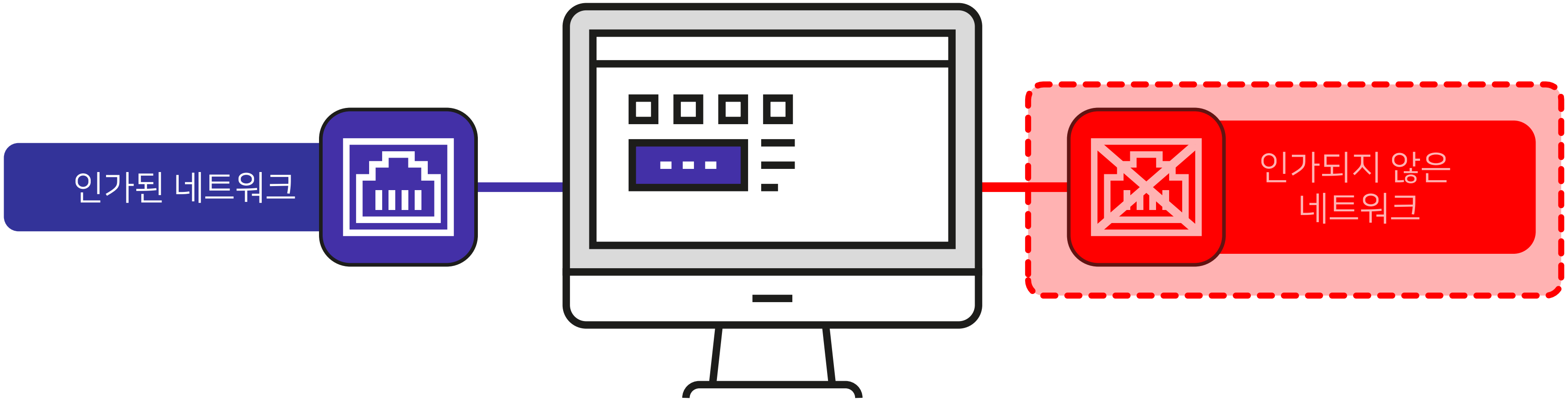
정책 - 노드 정책 > 위험 감지

NAC에서 사전에 정의한 11가지 위험 이벤트

1. AD HOC 네트워크 연결
2. ARP Bomb
3. ARP Spoofing
4. MAC/IP Clone
5. Malware Detection
6. Port Scan
7. 비 정상적인 DHCP 서버 감지
8. 센서 MAC Clone
9. 알 수 없는 서비스 요청
10. 잘못된 게이트웨이 사용
11. SNMP 차단요청

정책 - 노드 정책 > 위험 감지

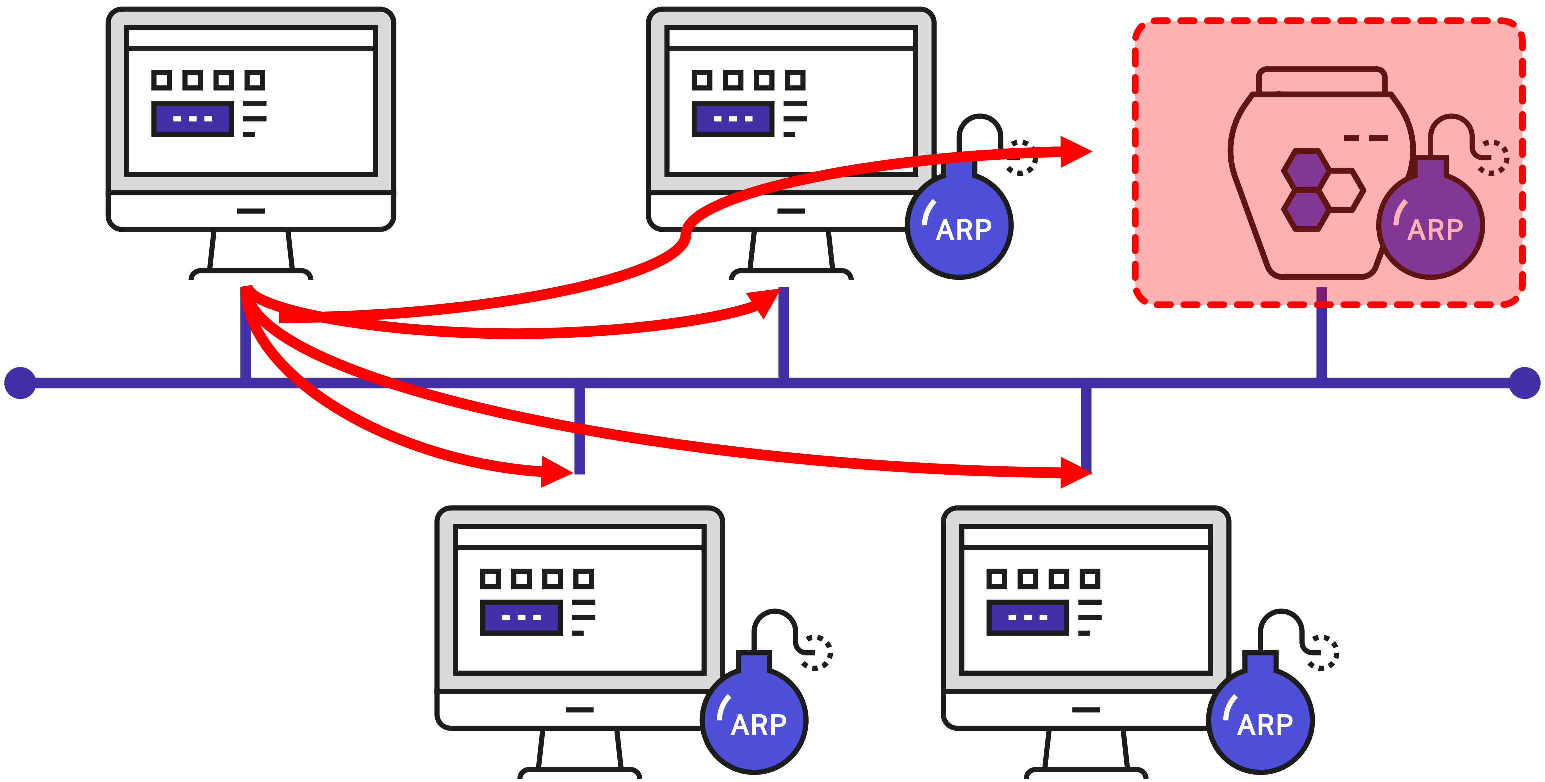
1. AD HOC 네트워크 연결



정책 - 노드 정책 > 위험 감지

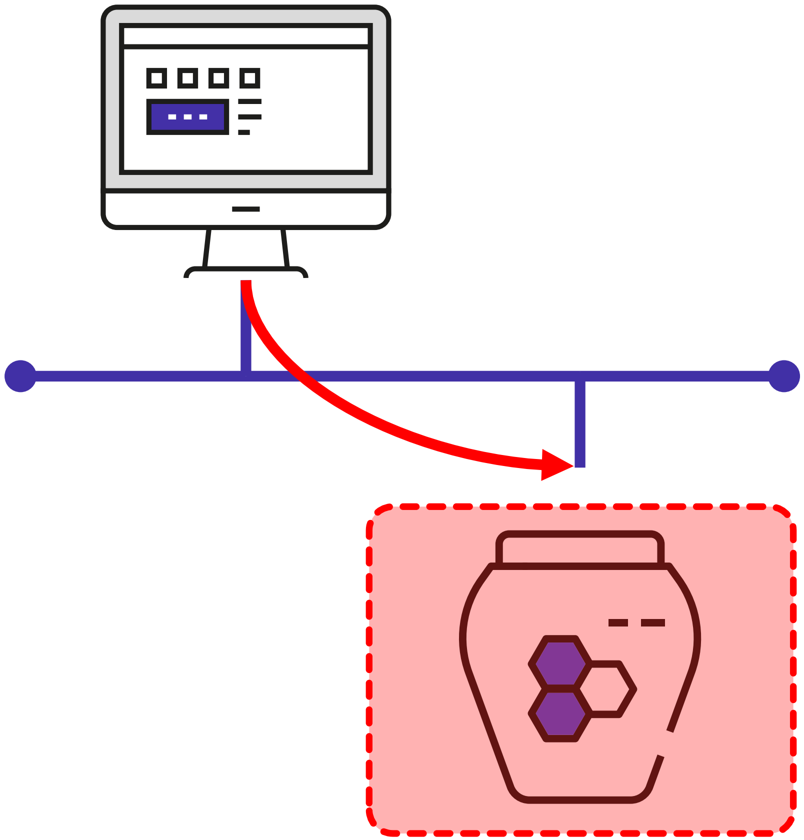
Genian NAC

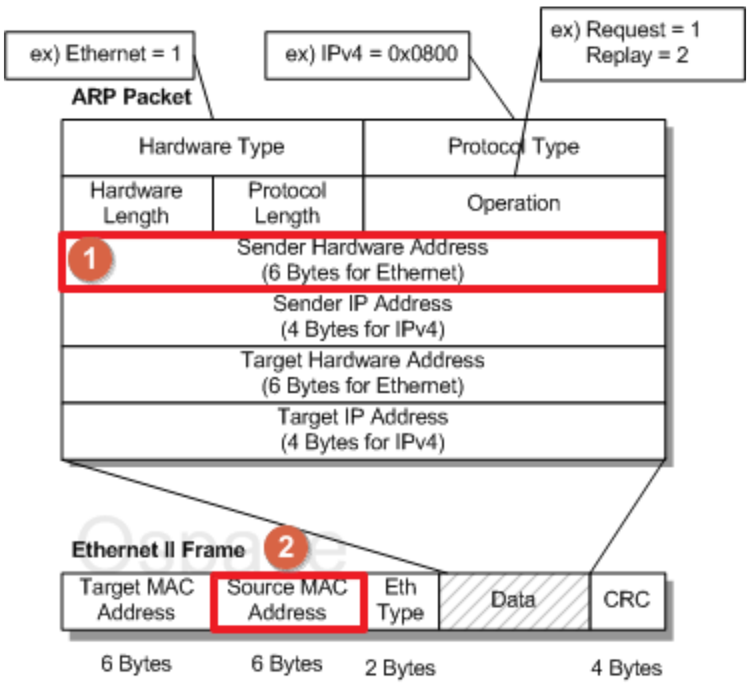
2. ARP BOMB



정책 - 노드 정책 > 위험 감지

3. ARP Spoofing

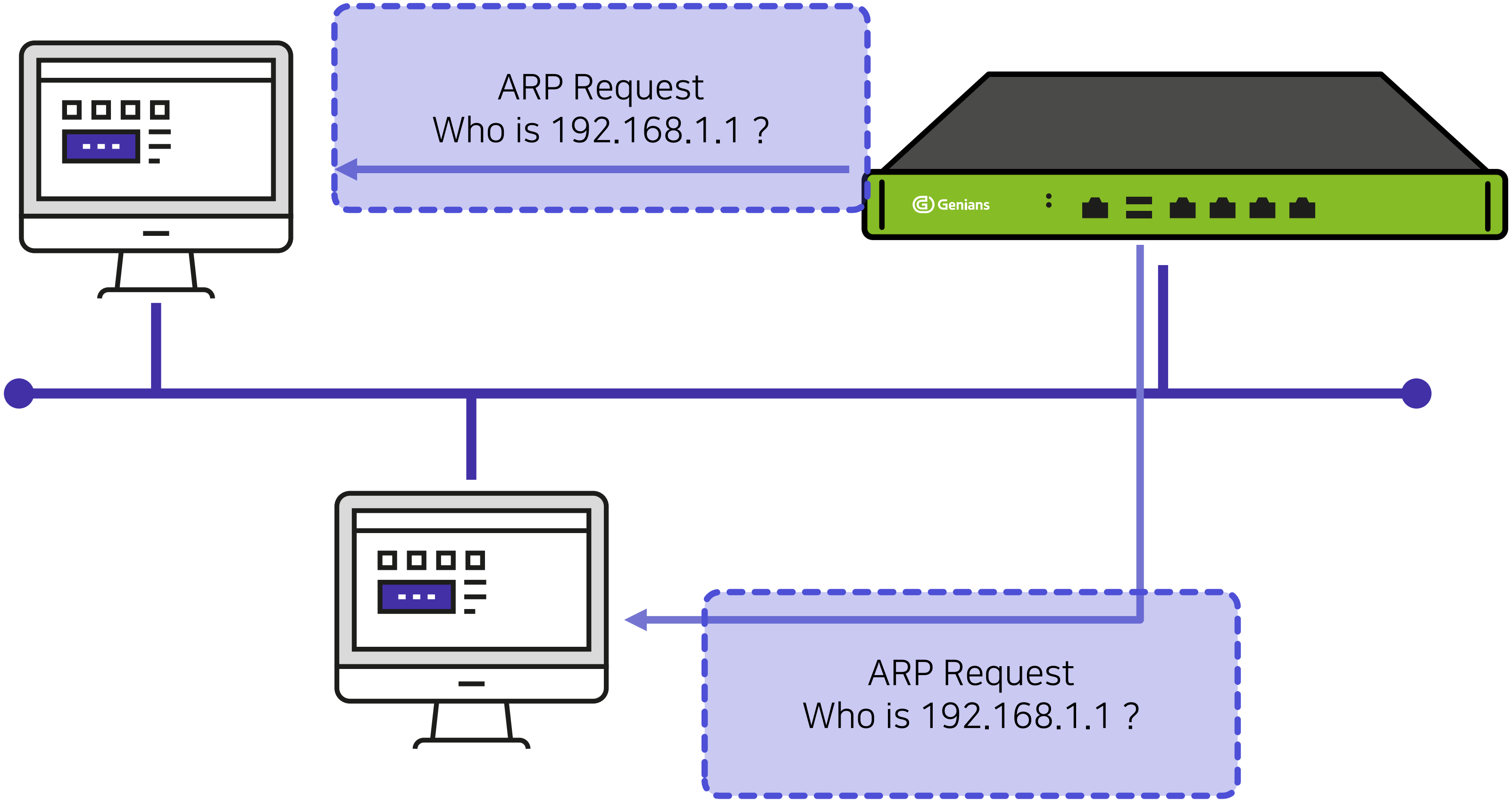




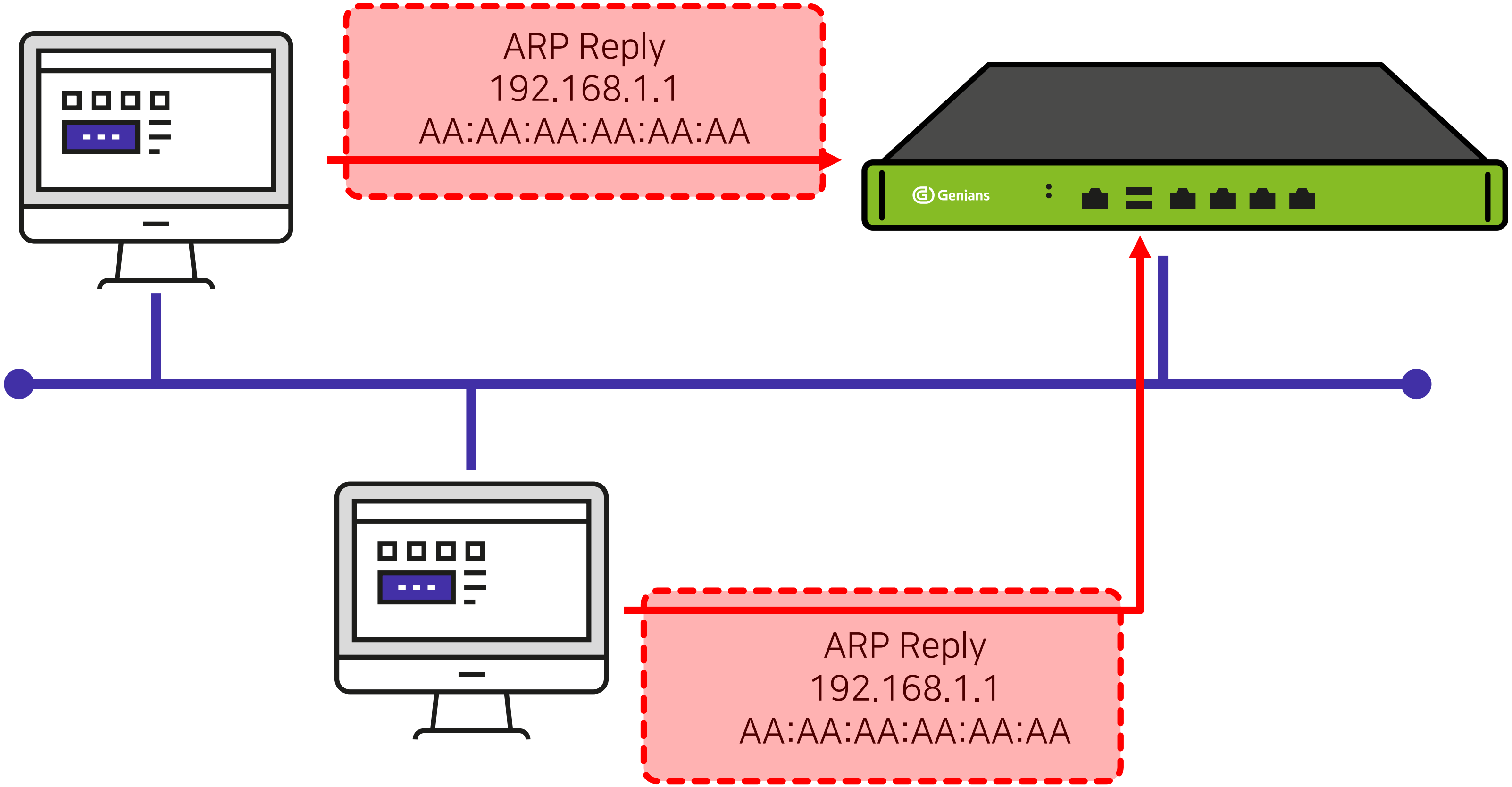
정책 - 노드 정책 > 위험 감지

Genian NAC

4. MAC / IP Clone

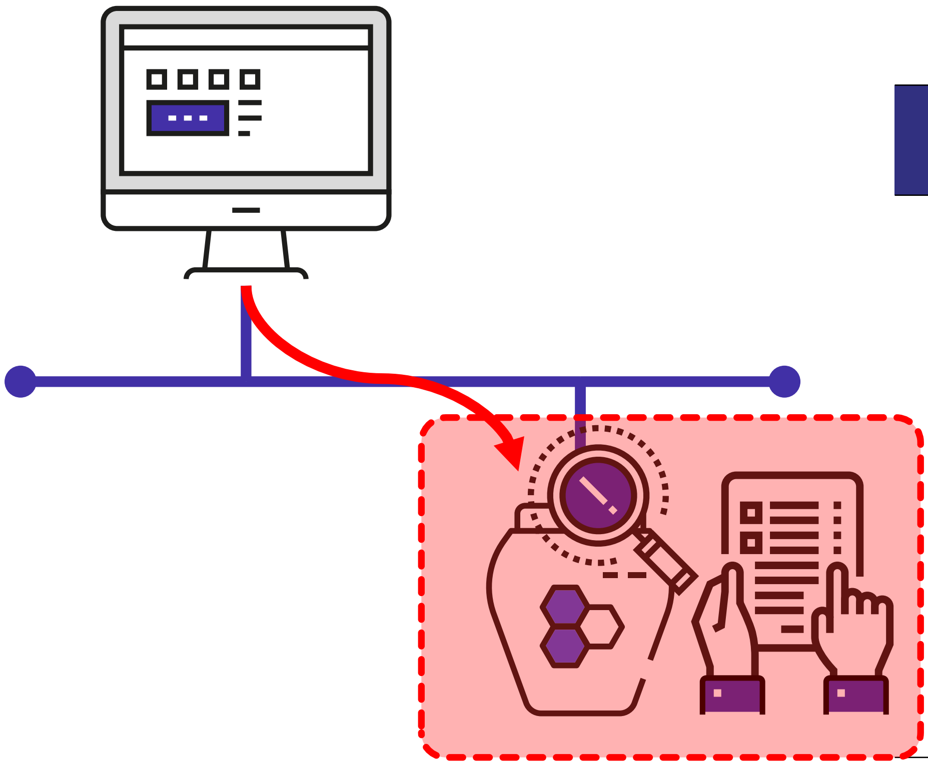


4. MAC / IP Clone



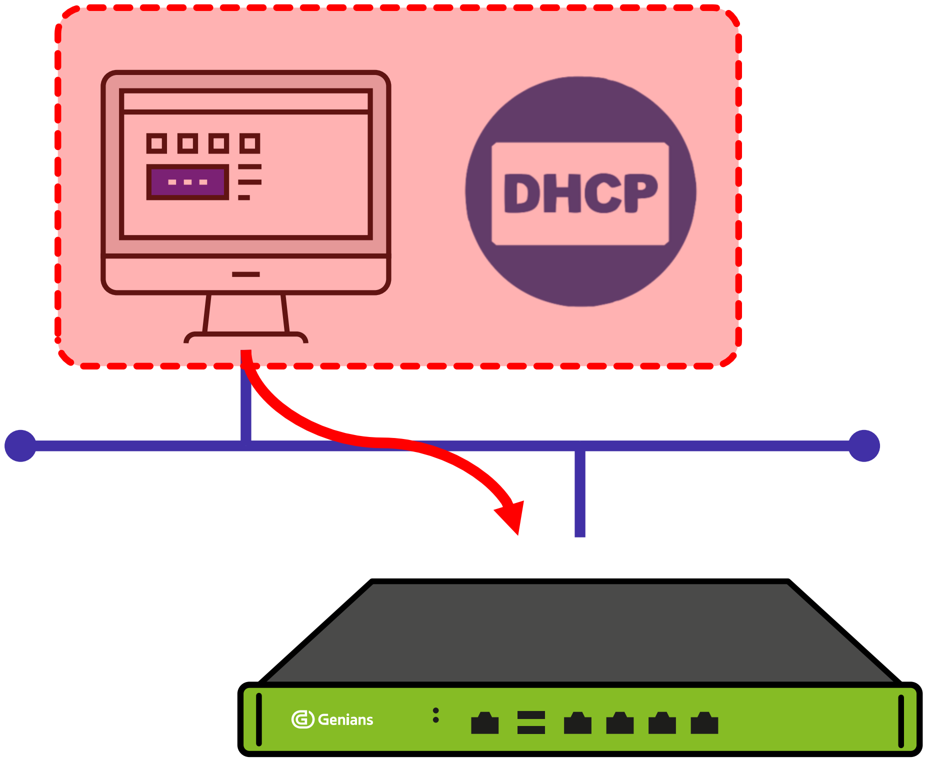
5. Malware Detection

6. Port Scan



Well-Known Port (TCP)
1/tcp TCPMUX (TCP 포트 서비스 멀티플렉서)
7/tcp ECHO 프로토콜
9/tcp DISCARD 프로토콜
13/tcp DAYTIME 프로토콜
17/tcp QOTD (Quote of the Day) 프로토콜
……

7. 비 정상적인 DHCP 서버 감지

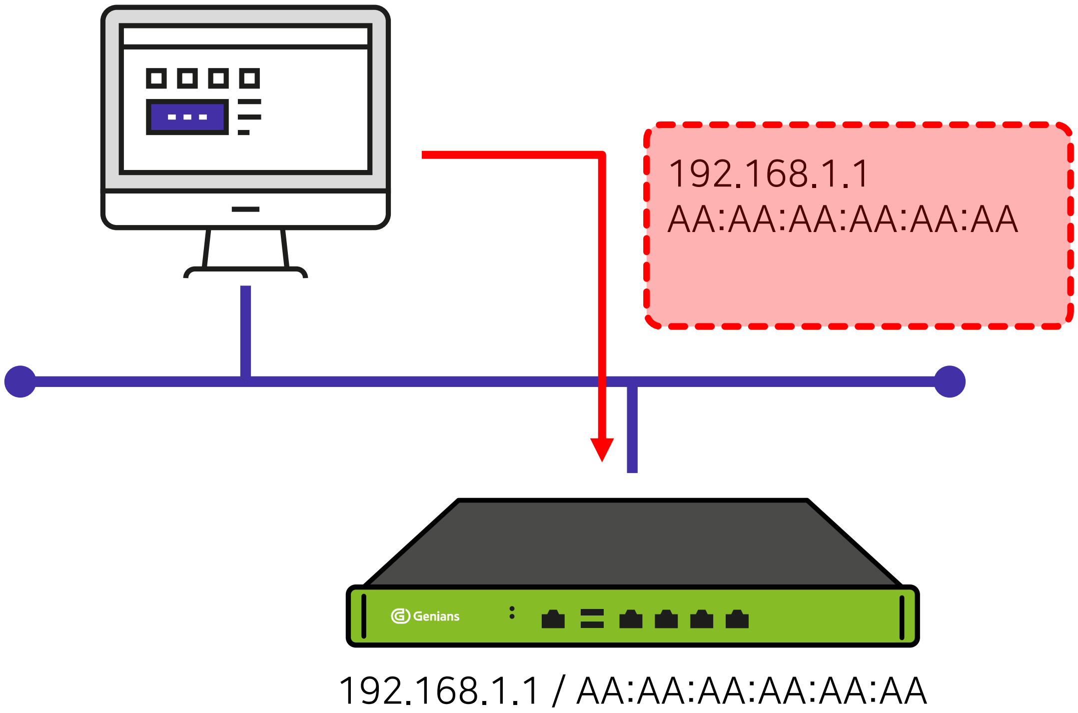


DHCP Offer
DNS 정보

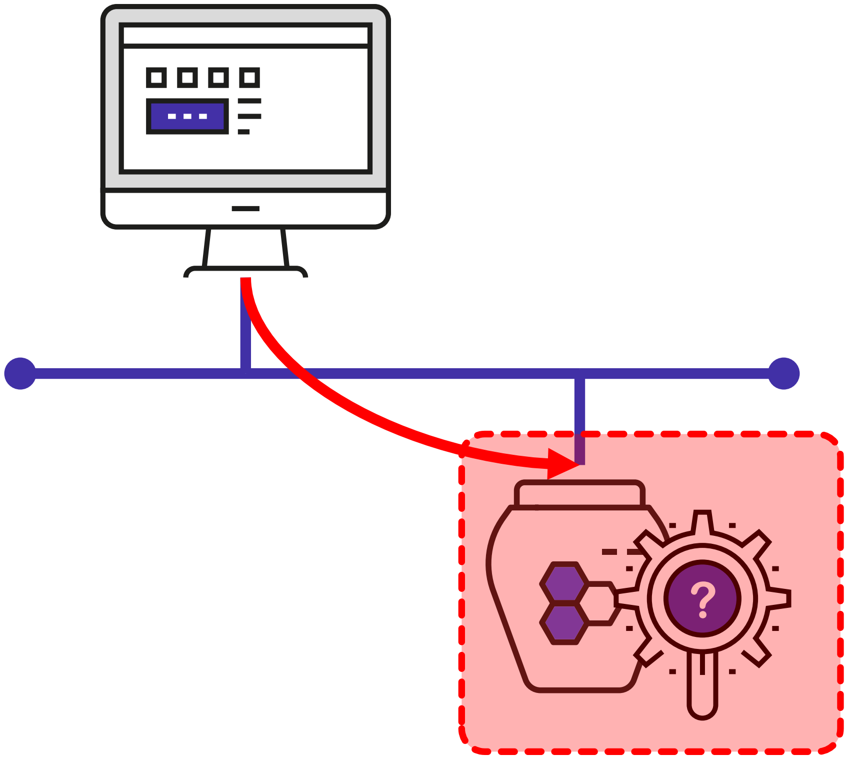
≠

네트워크 센서
DNS 정보

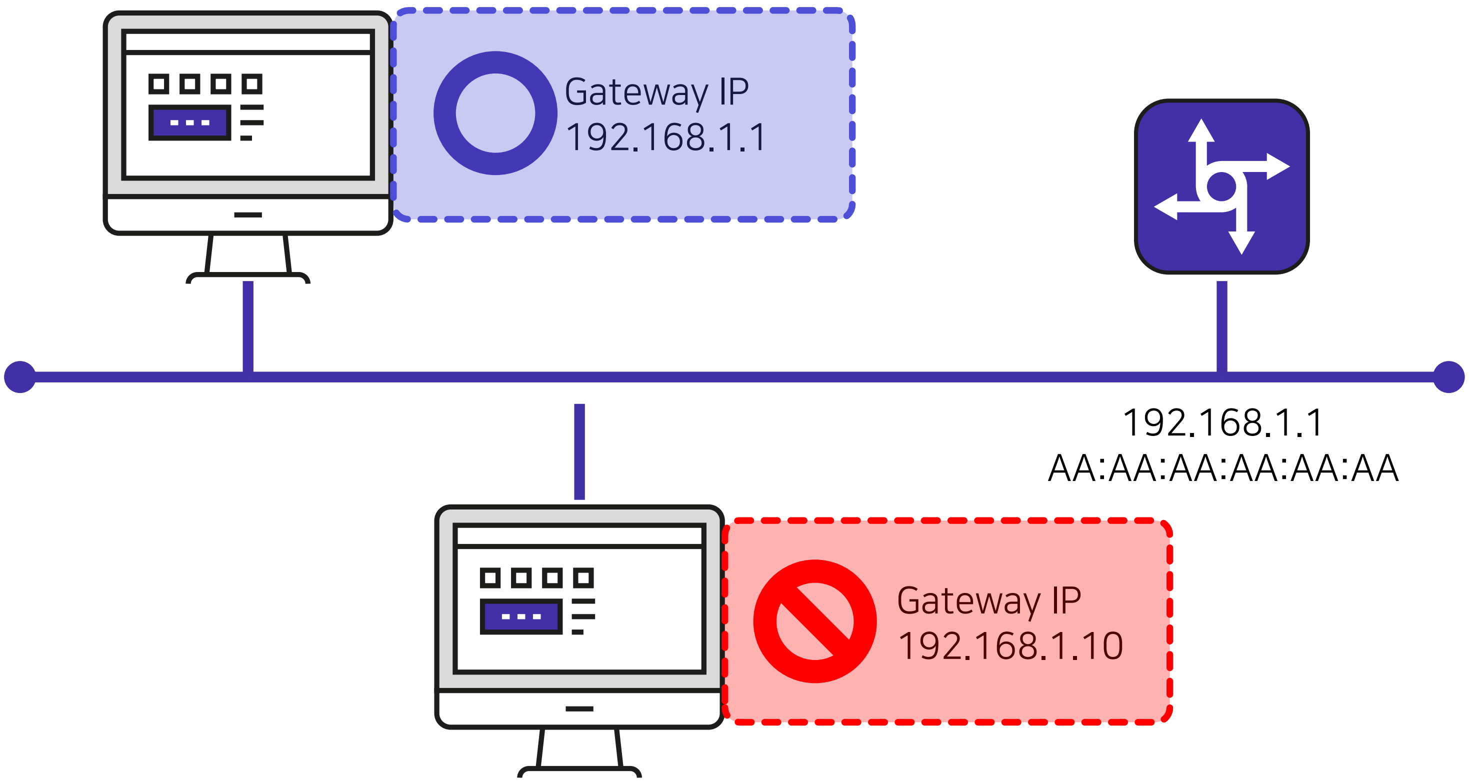
8. 센서 MAC Clone



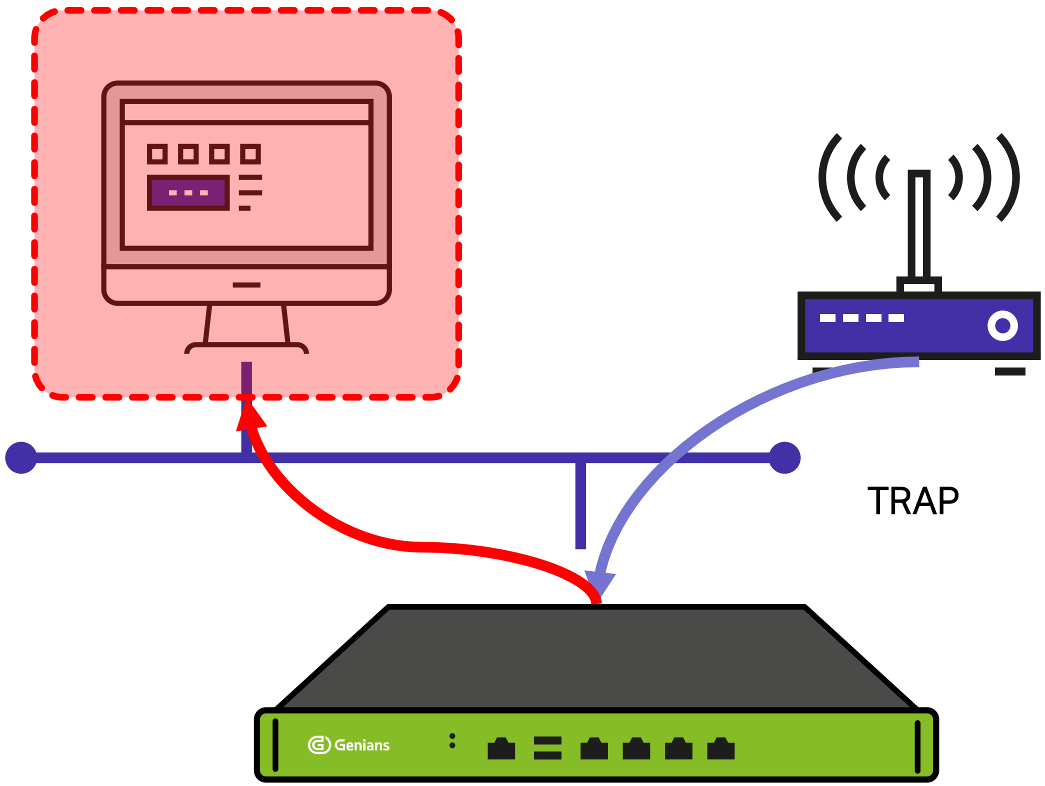
9. 알 수 없는 서비스 요청



10. 잘못된 게이트웨이 사용

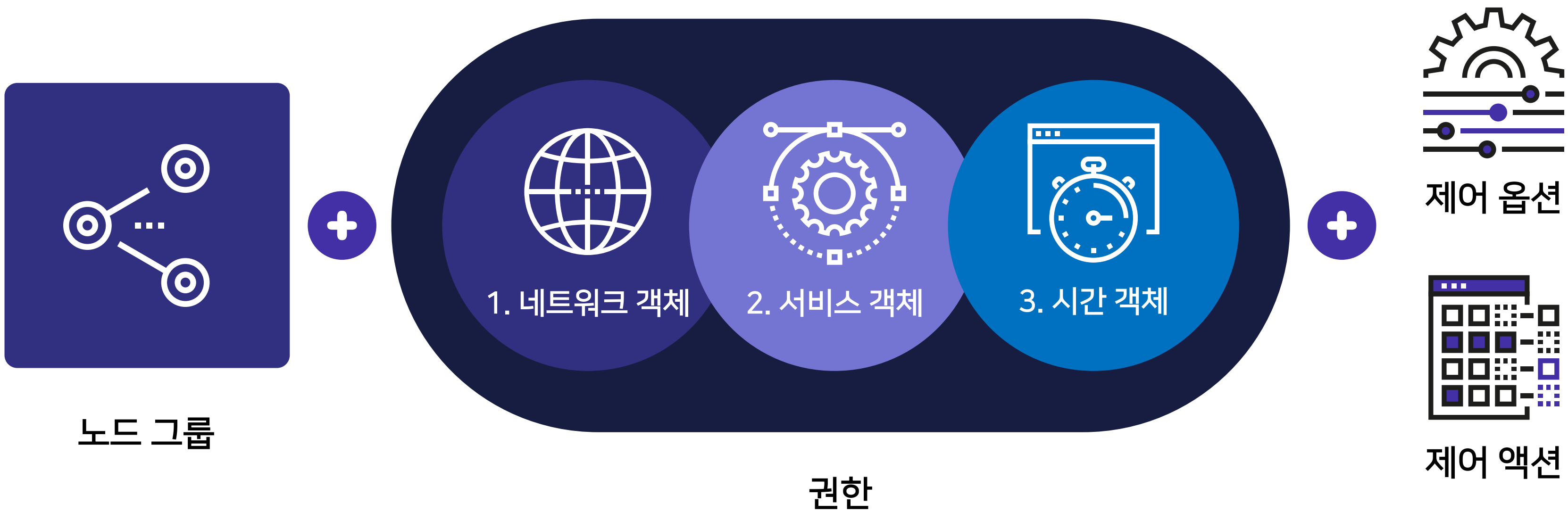


11. SNMP 차단요청



정책 – 제어 정책

- 정책 - 제어 정책 - 제어액션
- 그룹 - 노드
- 객체



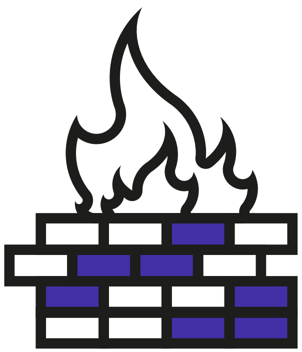
정책 – 제어 정책 > 제어 옵션

정책 별 CWP
페이지를 설정

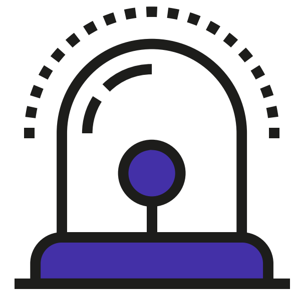
SNMP 연동 기능으로
스위치 포트를 차단

Radius Coa
사용 스위치 제어

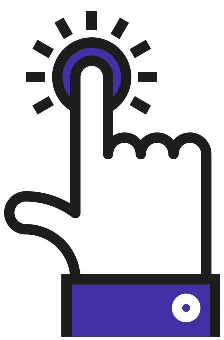
정책 – 제어 정책 > 제어 액션



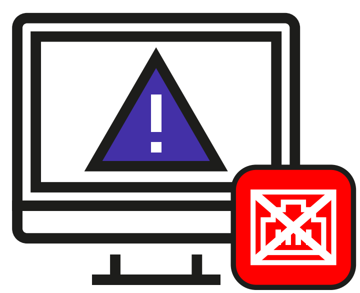
단말 방화벽
ACL 설정



차단 시 사용자
알림 메시지 발송



단말 전원
강제 종료

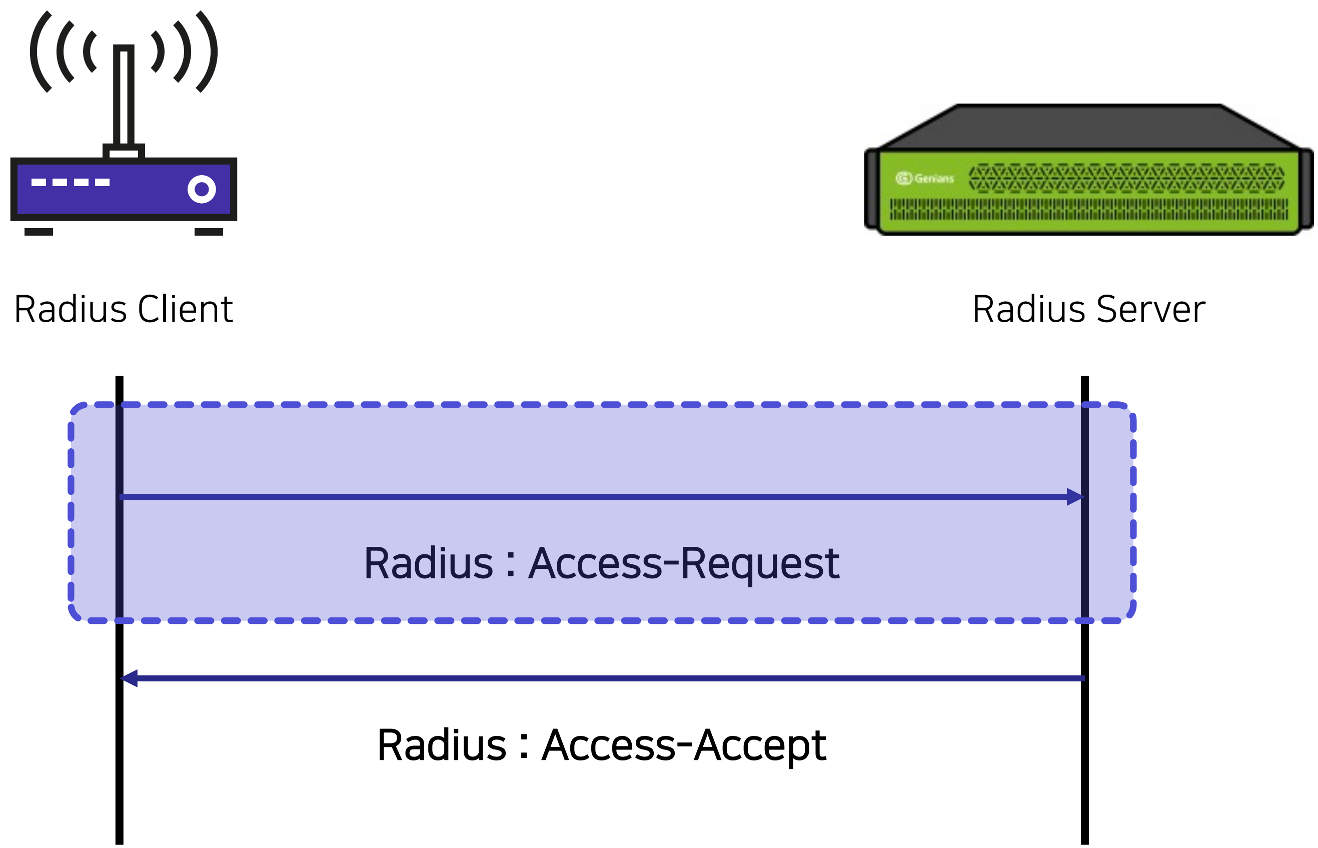


네트워크
인터페이스
사용중지

정책 - RADIUS 정책

Genian NAC

1. 그룹 조건 설정



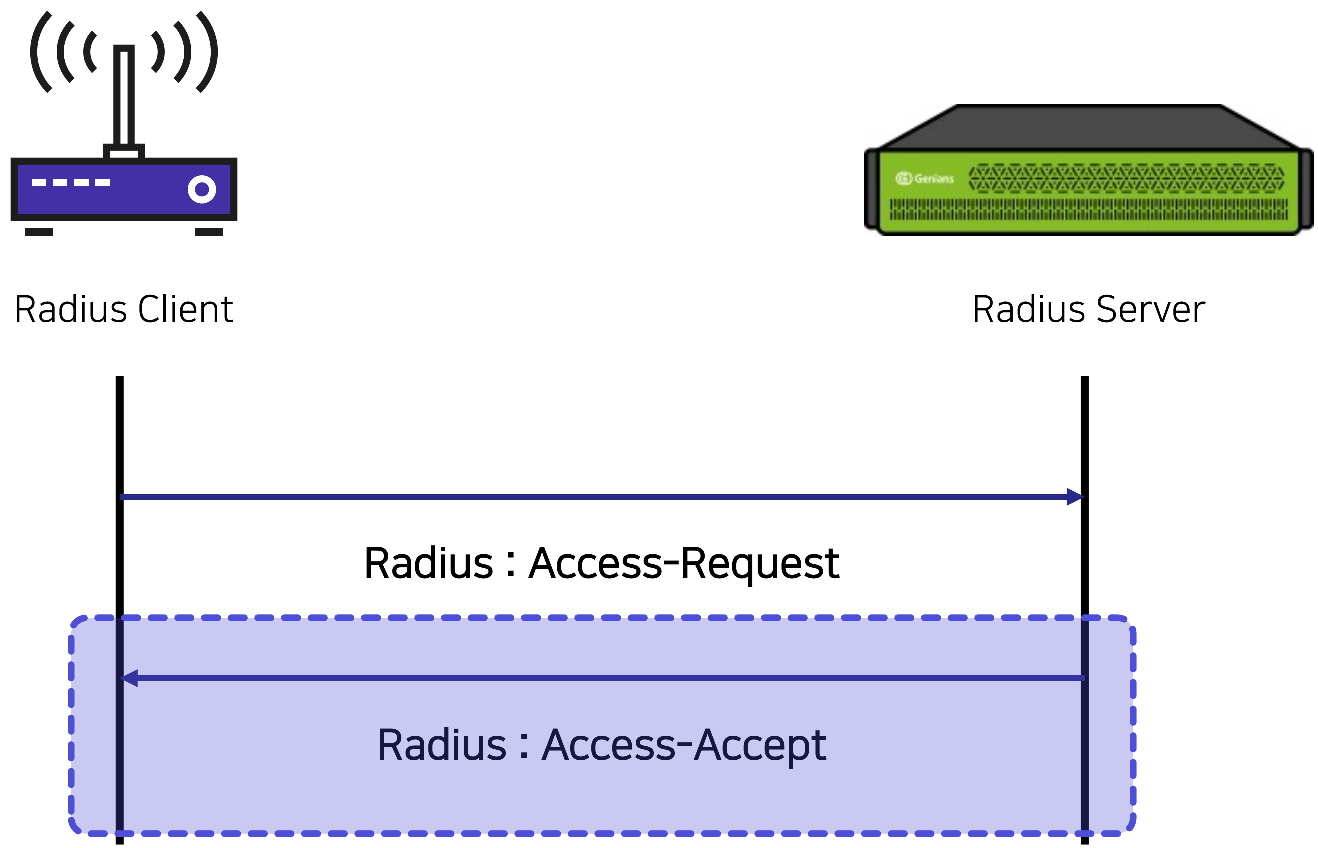
정책 - RADIUS 정책

1. 그룹 조건 설정

1	User-Name	9	Login-IP-Host
2	Calling-Station-Id	10	Class
3	Called-Station-Id	11	Vendor-Specific
4	Framed-IP-Address	12	NAS-Port-Type
5	NAS-IP-Address	13	Connect-Info
6	NAS-Port	14	NAS-Port-ID
7	Service-Type	15	Aruba-User-Role
8	Filter-Id	16	Aruba-Essid-Name

정책 - RADIUS 정책

2. 속성 할당



정책 - RADIUS 정책

Genian NAC

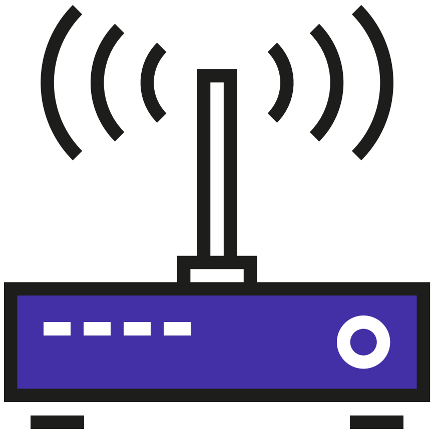
2. 속성 할당

1	VLAN 번호 / 이름
2	Cisco InBound ACL
3	Cisco OutBound ACL
4	Cisco Security Group Tag
5	Cisco Url Redirect ACL
6	Cisco Url Redirect 주소
7	Filter id
8	NAS-Filter-Rule
9	Session-Timeout
10	Termination-Action

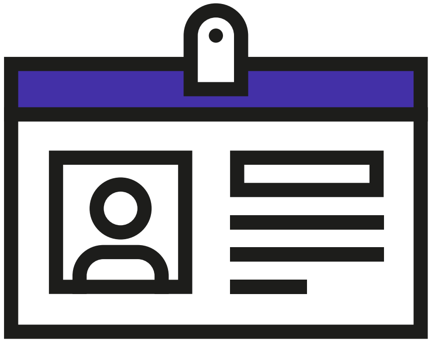
정책 - 무선랜 정책

Genian NAC

- 정책 - 노드정책
- 정책 - 노드정책 - 노드액션



AP Profile

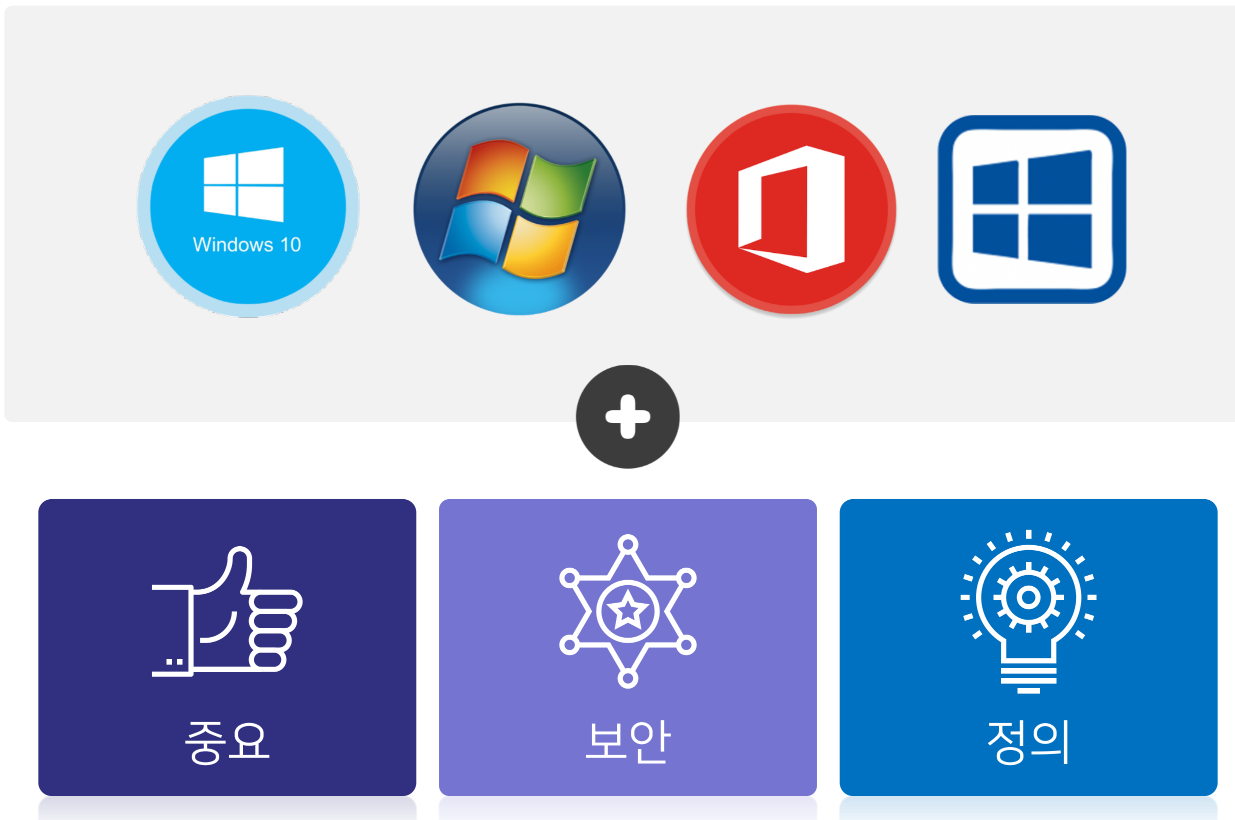


Client Profile

정책 - Windows 업데이트 정책

Genian NAC

- 정책 - 노드정책
- 정책 – 노드정책 – 노드 액션

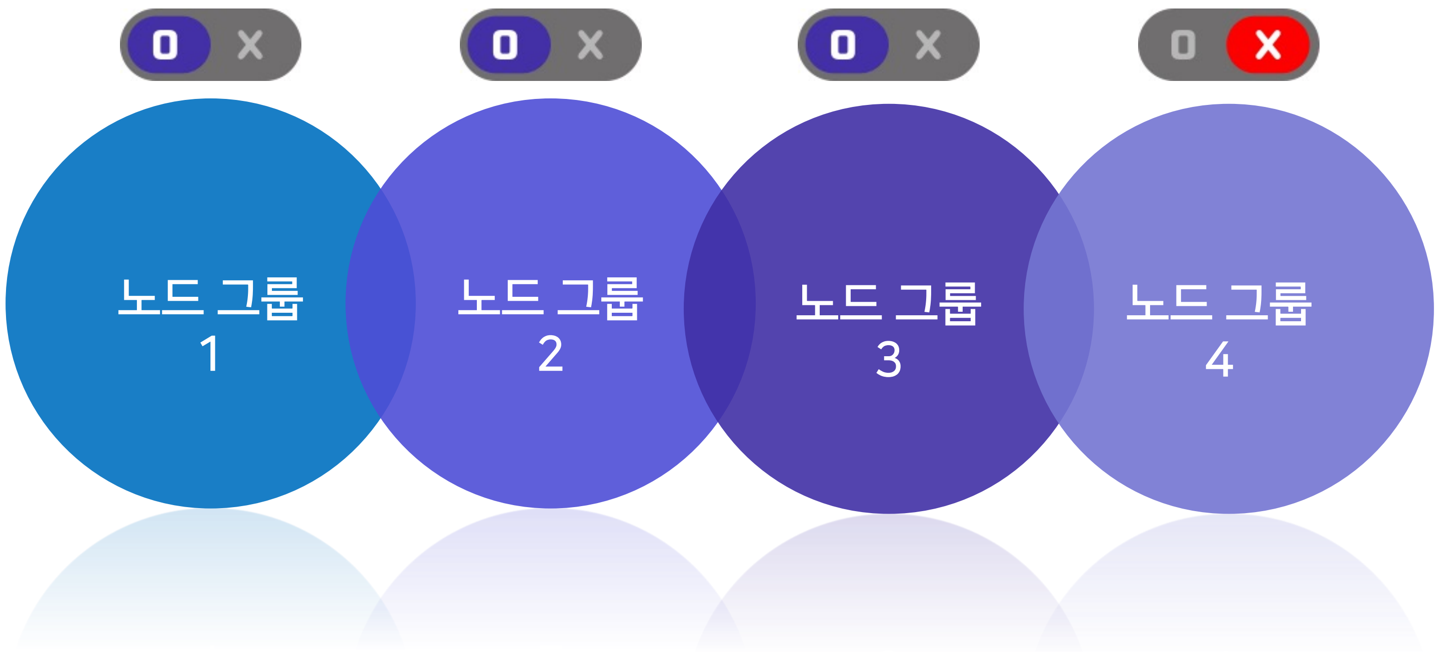


정책 - 장치 제어 정책

- 정책 - 노드정책
- 정책 – 노드정책 - 노드액션

정책 - 컴플라이언스 정책

다수의 노드 그룹을 지정하여 노드 그룹 포함 여부를 O/X 로 표시하는 기능



Summary

Genian NAC

1. 에이전트 플러그인 기능을 사용하여 정책이 적용되는 항목

- 무선랜 정책
- 장치 제어 정책
- Windows 업데이트 정책

2. 네트워크 센서를 이용하여 차단하는 정책

- 제어정책

3. 제어와 관련 없는 정책

- 컴플라이언스 정책

Genians

문의 : 지니언스 네트워크보안기술부

ca-se-nac@genians.com