

# 소프트웨어 정의 네트워킹 환경에서 제로 트러스트 보안 모델을 위한 사용자 인증 절차

(User Authentication Procedure for Zero-Trust Security Model in Software Defined Networking Environment)

전남대학교 대학원  
정보보안협동과정  
김영현

연구의 배경 및 목표

01

기존 연구들의  
수준 및 문제

02

# TABLE OF CONTENTS

03

SDN 환경에서  
제로 트러스트 보안 모델을  
위한 사용자 인증 절차

04

현재까지의 연구 내용

05

결론 및 향후 연구 계획



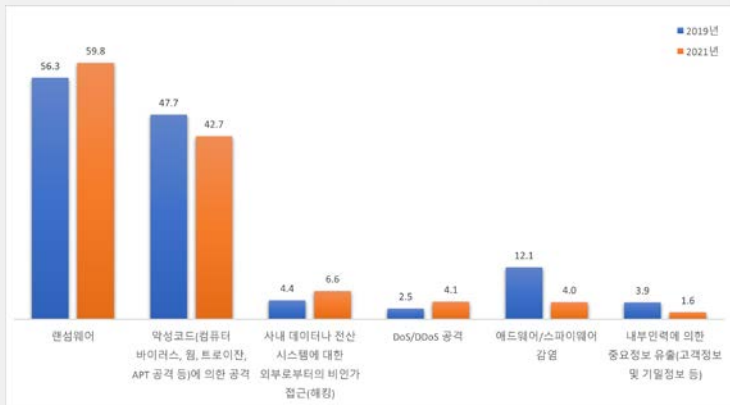
# 01

## 연구의 배경 및 목표

# 01. 연구의 배경 및 목표 [ 1 / 2 ]

## 연구 배경 및 목적 [ 1 / 2 ]

- IoT, 빅데이터, 인공지능, 클라우드 등 차세대 신기술에 대한 관심과 노력이 높아지면서 비교적 단순했던 기업 인프라의 규모와 복잡성 증가
  - 차세대 신기술에서 확장성, 유연성 등을 요구
  - 새로운 형태의 네트워크 구조 필요
- 최근 발생하는 사이버 보안 위협의 증가와 고도화함에 따라 사전 예방적인 보안 방법의 필요



< 2019년과 2021년의 침해사고 경험 유형 >

# 01. 연구의 배경 및 목표 [ 1 / 2 ]

## 연구 배경 및 목적 [ 2 / 2 ]

- 새로운 형태의 네트워크 구조의 SDN(Software Defined Networking)
  - SDN은 네트워크 성능 향상에 초점을 맞춘 설계
  - 차세대 신기술의 요구 사항 충족 - 확장성, 유연성 등
  - 그러나, 기본적으로 보안 기능을 갖지 않아 취약
- 사전 예방적인 방법의 사이버 보안 패러다임인 제로 트러스트(Zero-Trust) 보안 모델
  - 누구도, 무엇도 신뢰하지 않으며, 인증을 통해 접근해야 한다는 개념
  - 미국의 사이버 보안 강화 행정명령에 포함
- 네트워크 액세스를 위한 인증 표준인 IEEE 802.1X
  - 제로 트러스트 보안 모델의 기본 원칙인 인증 후 연결에 부합
  - 그러나, 기존 네트워크에 대한 설계로 SDN 환경에서 제한적
  - 인증 기능의 잘못된 배치로 인한 네트워크 성능 저해

# 01. 연구의 배경 및 목표 [ 2 / 2 ]

## 연구 목표

1. 전체 아키텍처는 SDN, IEEE 802.1X, 제로 트러스트 보안 모델을 통합
  - 전체 구성 및 특성에 맞게 최적화
2. 제안하는 사용자 인증 절차는 인증 후 연결을 기본 원칙으로 액세스에 대한 최소한의 권한 제공
3. 제안하는 사용자 인증 절차는 네트워크 뿐만 아니라 사용자도 보호



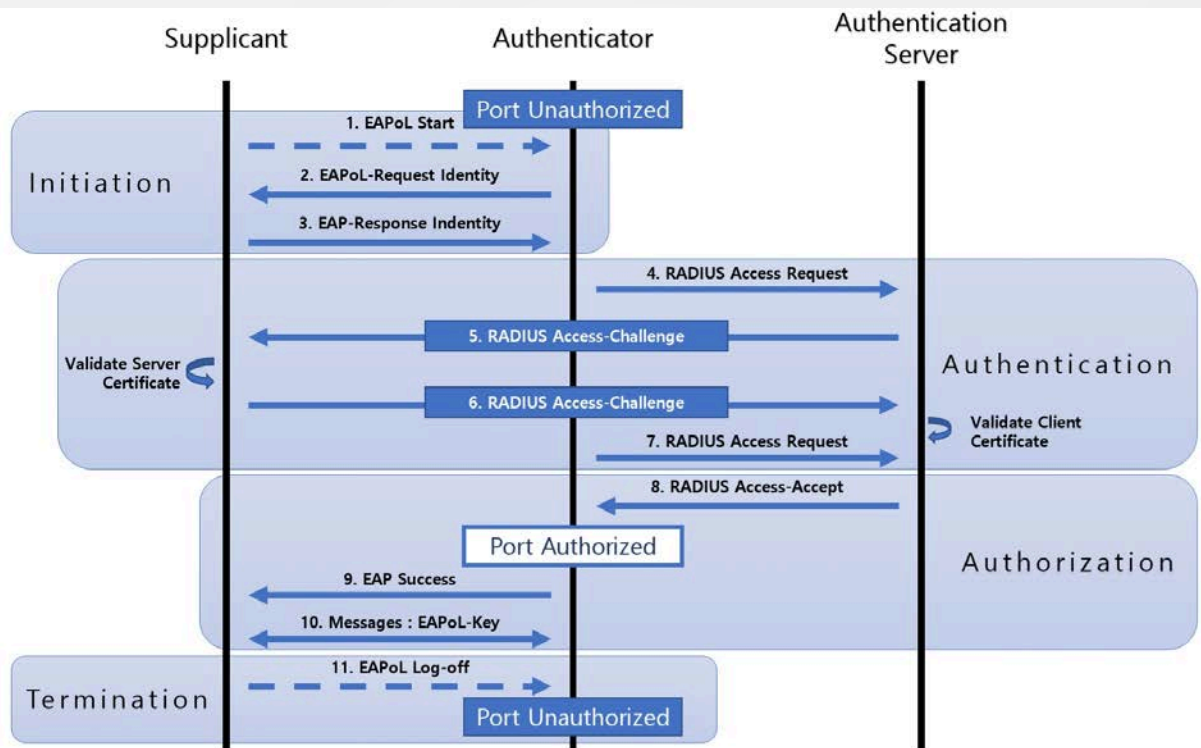
# 02

## 기존 연구들의 수준 및 문제

---

## 02. 기존 연구들의 수준 및 한계 [ 1 / 4 ]

### IEEE 802.1X





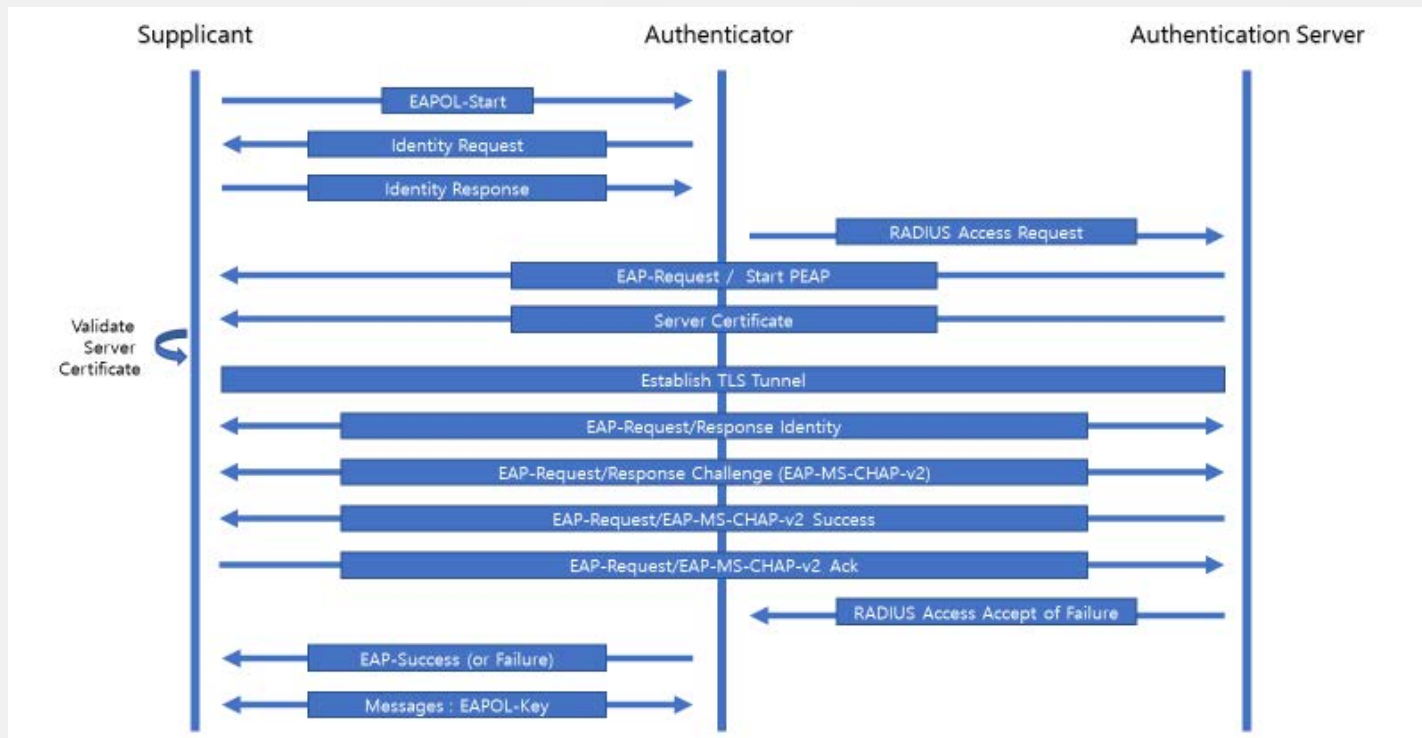
## 02. 기존 연구들의 수준 및 한계 [ 2 / 4 ]

### IEEE 802.1X의 인증 알고리즘 비교

<div> <div>EAP의 인증 알고리즘</div> <div>항목</div> </div>	EAP-TLS	EAP-TTLS	EAP-MD5	EAP-PEAP	EAP-LEAP
클라이언트 인증서	필요	불필요	불필요	불필요	불필요
서버 인증서	필요	필요	불필요	필요	불필요
인증 방식	인증서	아이디/패스워드	아이디/패스워드	아이디/패스워드	패스워드
인증 방향	양방향	양방향	일방	양방향	양방향
보안 등급	최상	상	하	상	상
구현 난이도	최상	중	하	중	중

## 02. 기존 연구들의 수준 및 한계 [ 3 / 4 ]

### IEEE 802.1X의 EAP-PEAP-MSCHAPv2

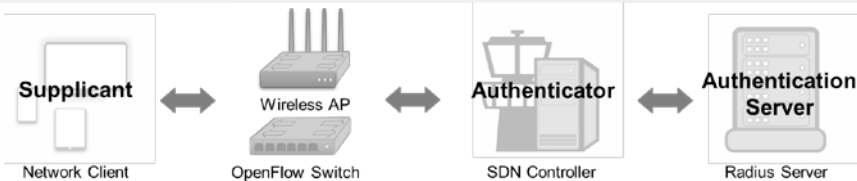


## 02. 기존 연구들의 수준 및 한계 [ 3 / 3 ]

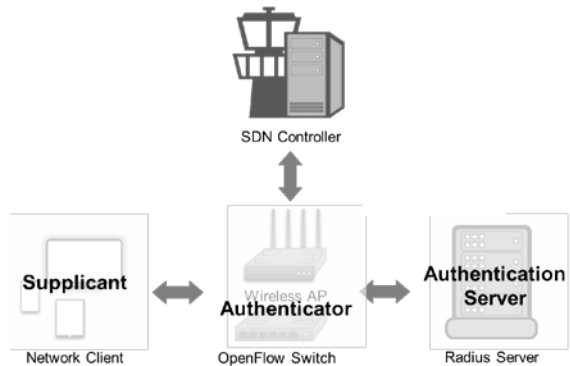
### 기존 SDN 환경에서 IEEE 802.1X를 통한 사용자 인증에 관한 연구 [ 1 / 2 ]



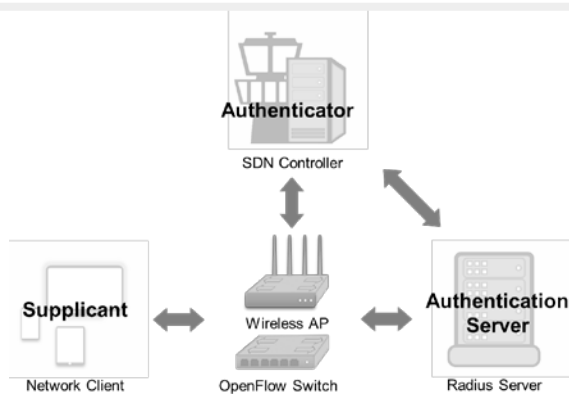
◀ 전통적인 네트워크 ▶



◀ 컨트롤러에 집중된 인증 ▶



◀ OF 스위치 인증 ▶



◀ 컨트롤러 인증 ▶

## 02. 기존 연구들의 수준 및 한계 [ 4 / 4 ]

### 기존 SDN 환경에서 IEEE 802.1X를 통한 사용자 인증에 관한 연구 [ 2 / 2 ]

기존 연구 구성	OpenFlow 기반 접근 관리 시스템 [YIY11]	무선 LAN 로밍에 대한 액세스 제어 시스템 [KAS12]	FlowNAC [JNM14]	AuthFlow [DMF16]	사용자와 단말 간의 관 계를 고려한 인증 프레 임워크 [PNR20]
인증	컨트롤러	인증자/컨트롤러	인증자	인증자	인증자
허가	컨트롤러	컨트롤러	컨트롤러	컨트롤러	컨트롤러
정책 설정	정적	정적	정적	정적	정적
컨트롤러 부하	매우 높음	높음	높음	높음	중간
사용자 정보 보호	매우 취약	취약	보통	보통	취약
보안 등급	매우 취약	취약	취약	보통	취약

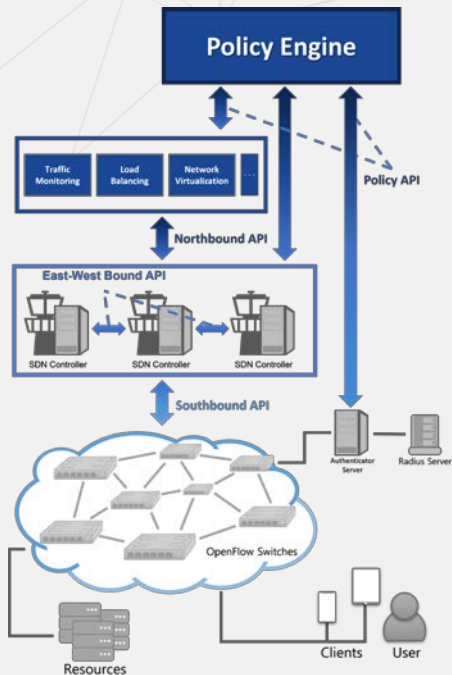


# 03

## SDN 환경에서 제로 트러스트 보안 모델을 위한 사용자 인증 절차

### 03. SDN 환경에서 제로 트러스트 보안 모델을 위한 사용자 인증 절차 [ 1 / 2 ]

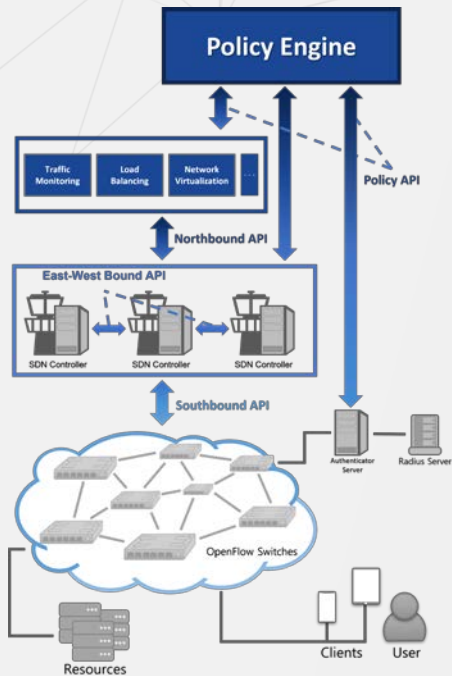
#### 제안된 사용자 인증의 통합 환경 구성 [ 1 / 2 ]



- Policy Engine
  - ✓ 사용자 클라이언트의 인증 및 허가를 최종적으로 결정
- SDN Controller
  - ✓ OpenFlow 스위치에 액세스 권한에 대한 정책 실행 수행
- OpenFlow Switch
  - ✓ 컨트롤러를 통해 전달 받은 사용자의 액세스 권한에 해당하는 플로우를 플로우 테이블에 추가하는 정책 집행 수행
- Authenticator Server
  - ✓ 사용자 크리덴셜을 통한 인증 정보 및 클라이언트의 정보를 정책 엔진에 전달

### 03. SDN 환경에서 제로 트러스트 보안 모델을 위한 사용자 인증 절차 [ 1 / 2 ]

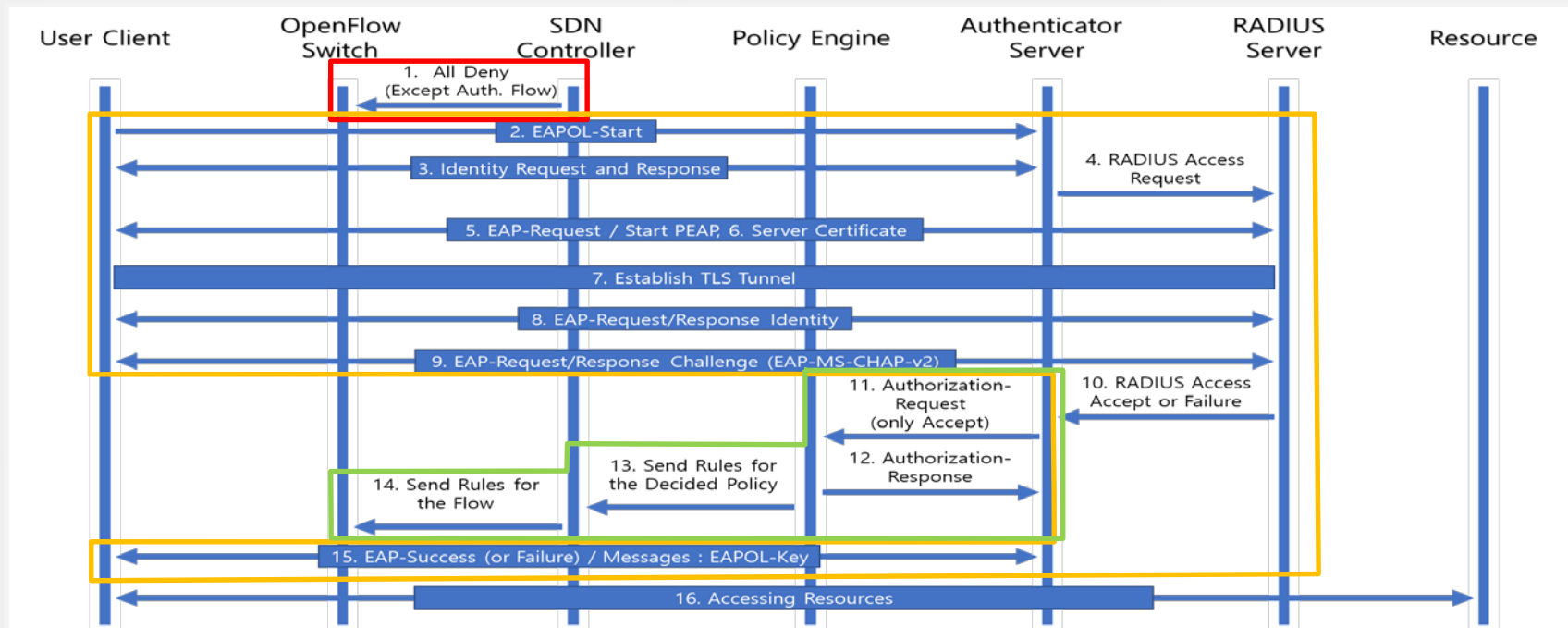
#### 제안된 사용자 인증의 통합 환경 구성 [ 2 / 2 ]



- **RADIUS Sever**
  - ✓ Root CA로부터 서명 받은 RADIUS 서버 인증서를 통해 TLS 터널링을 생성 후 사용자 크리덴셜을 통한 사용자를 인증
- **User Clients**
  - ✓ 사용자 정보 및 클라이언트 정보를 통해 액세스 인증을 시도
  - ✓ Root CA 인증서를 통해 Root CA에서 서명한 RADIUS 인증서로 사용자 보호
- **Resources**
  - ✓ 사용자의 액세스 권한에 따라 접근할 수 있는 데이터 및 서비스

# 03. SDN 환경에서 제로 트러스트 보안 모델을 위한 사용자 인증 절차 [ 2 / 2 ]

## 제안된 사용자 인증 절차





# 04

## 현재까지의 연구 내용

## 04. 현재까지의 연구 내용 [ 1 / 3 ]

### 실험 환경

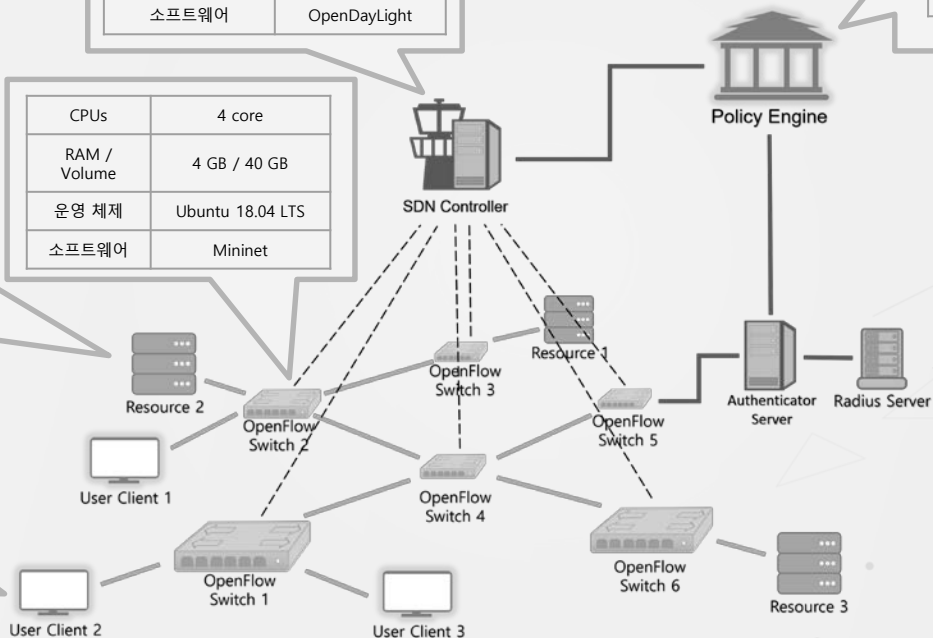
CPU	4 core
RAM / Volume	4 GB / 40 GB
운영 체제	Ubuntu 18.04 LTS
소프트웨어	OpenDayLight

CPU	4 core
RAM / Volume	4 GB / 40 GB
운영 체제	Ubuntu 18.04 LTS
개발 언어	Golang

CPU	4 core
RAM / Volume	4 GB / 40 GB
운영 체제	Ubuntu 18.04 LTS
소프트웨어	Mininet

CPU	2 core
RAM / Volume	2 GB / 20 GB
운영 체제	Ubuntu 18.04 LTS
소프트웨어	NodeJS

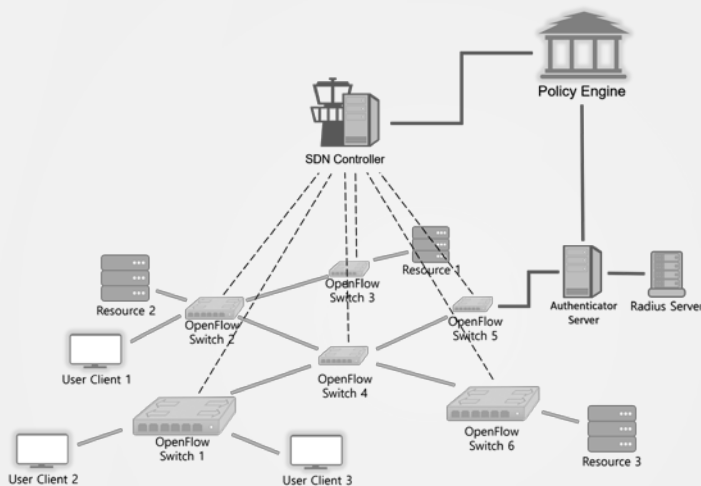
CPU	2 core
RAM / Volume	4 GB / 32 GB
운영 체제	Android 10
소프트웨어	Android App.



CPU	4 core
RAM / Volume	4 GB / 40 GB
운영 체제	Ubuntu 18.04 LTS
소프트웨어	freeRADIUS

## 04. 현재까지의 연구 내용 [ 2 / 3 ]

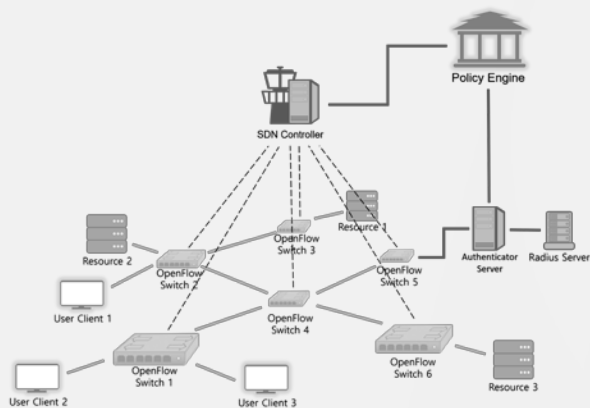
### 실험 시나리오 및 평가 항목



- 제안하는 통합 환경 및 사용자 인증 절차가 제로 트러스트 보안 모델의 기본 원리
- 제안하는 통합 환경이 제로 트러스트 보안 모델의 네트워크 구성에 맞는 설계

## 04. 현재까지의 연구 내용 [ 3 / 3 ]

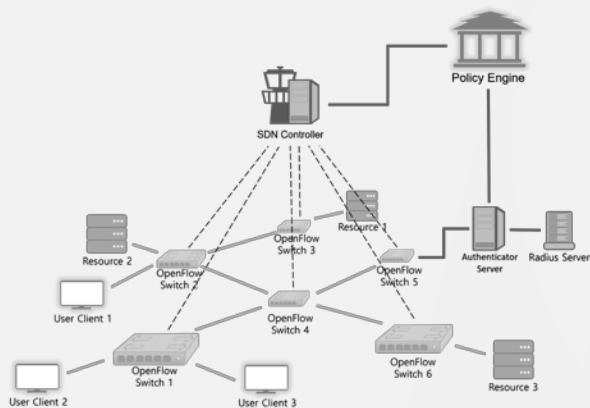
### 평가 결과 [ 1 / 2 ]



제로 트러스트 보안 모델의 기본 원리	결과
1. 모든 데이터 및 서비스를 리소스로 간주	○
2. 네트워크 위치에 관계없이 모든 통신을 보호	○
3. 리소스에 대한 액세스를 세션 단위로 허가	○
4. 동적 정책으로 리소스에 대한 액세스를 결정	○
5. 모든 리소스의 무결성/보안 상태를 감시하고 조치	△
6. 모든 리소스의 인증/인가를 동적으로 강력하게 실시한 후 접근 허용	○
7. 현 상태에 대해 가능한 한 많은 정보를 수집 및 개선	△

## 04. 현재까지의 연구 내용 [ 3 / 3 ]

### 평가 결과 [ 2 / 2 ]



제로 트러스트 보안 모델의 네트워크 구성	결과
1. 내부 네트워크 전체를 암묵적 트러스트 존으로 간주하지 않는다.	△
2. 연결된 단말은 기업 소유가 아닐 수도, 기업이 설정할 수 없을 수도 있다.	○
3. 신뢰할 수 있는 리소스는 없다.	○
4. 모든 리소스가 내부 인프라에 위치하고 있는 것은 아니다.	△
5. 자산은 네트워크 연결을 완전히 신뢰할 수 없다.	○
6. 자산 및 워크플로우의 보안 정책 및 보안 상태는 일괄적이고 유지되어야 한다.	△

# 05

## 결론 및 향후 연구 계획



## 05. 결론 및 향후 연구 계획

- 인프라의 규모와 복잡성으로 인한 보안 위협으로 SDN 환경에서 사용자 인증 절차 제안
  - 차세대 신기술에 대한 확장성 및 유연성 등 요구사항 충족
  - SDN의 보안 기능 제공
- SDN, IEEE 802.1X, 제로 트러스트 보안 모델의 구성 및 특성을 고려하여 액세스를 위한 사용자 인증 절차 제공
  - 네트워크 액세스에 대한 보안 위협 방지
  - 인증 및 허가에 관한 구성을 분리 및 재배포 하면서 컨트롤러에 대한 부하 완화
  - 인증서를 통해 연결하는 네트워크를 인증하여 사용자 정보를 보호
- 향후, 멀티 도메인 환경에서 여러 연결점에 대한 액세스 정책의 연구 진행



# THANKS