

Network Security Automation

v1.1

JS Lab

2021년 11월 일
안종석
james@jslab.kr

1

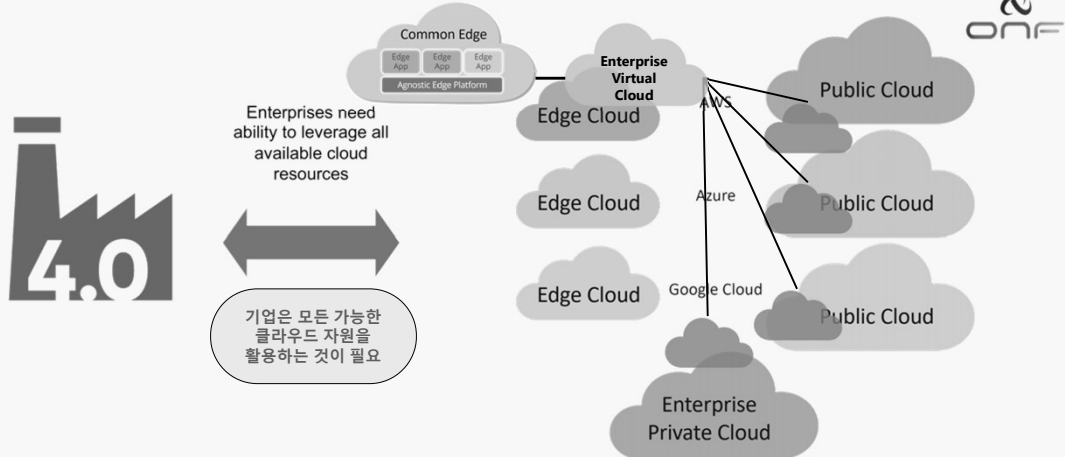
I. 개요	3
II. 제조사 솔루션	19
III. 네트워크 보안 자동화	28
IV. 요약	33

2

1. 개요

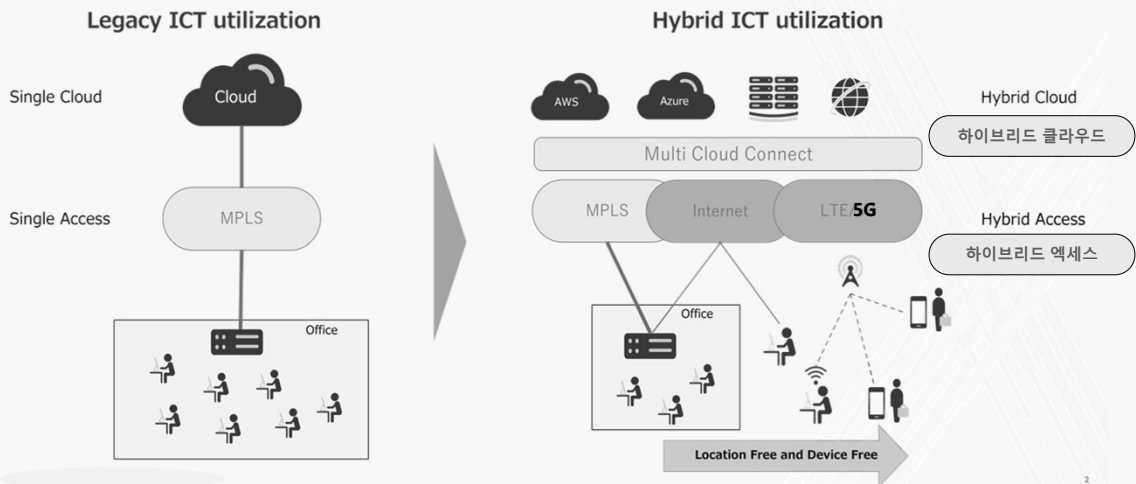
□ 엔터프라이즈 멀티클라우드는 뉴노멀 (ONF: Enterprise Multi-Cloud is the New Normal)

▪ Can't afford to be tied to just a single hyperscaler – 하나의 'Virtual Cloud' 필요



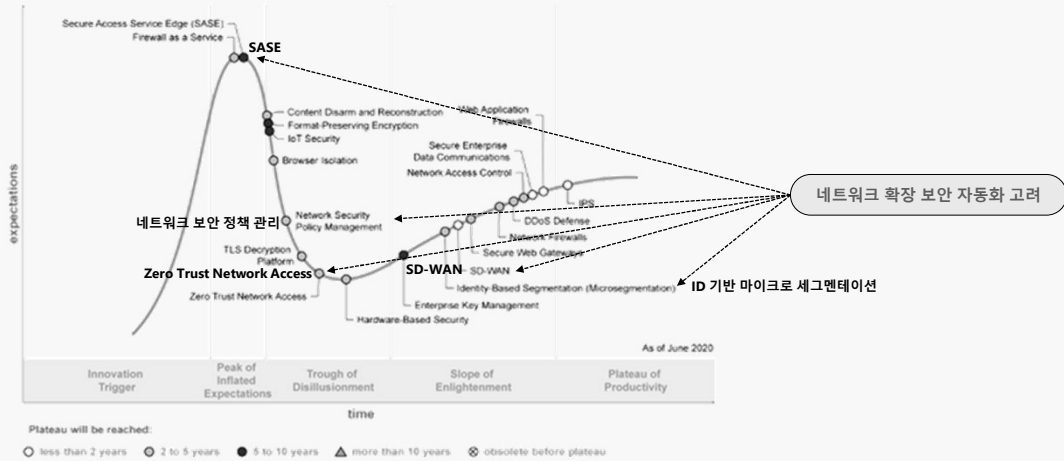
1. 개요

□ Enterprise Network Transitions (예: NTT Communications Corporation)



1. 개요

□ Hype Cycle for Network Security (Gartner 2020)



<https://www.criticalstart.com/2020-updates-gartner-endpoint-security-hype-cycle-insights/>

5

1. 개요

□ 6 trends in corporate campus networks

1. Network automation
2. IT security and work from anywhere with any device
3. Wireless
4. IoT and edge computing
5. More cloud, less on-premises data center
6. Machine learning and AI

Networks are evolving, and that evolution includes enterprise campus networks. Trends like network automation, 5G and machine learning are modernizing campus networks.



By **Terry Slattery**, NetCraftsmen

<https://www.techtarget.com/searchnetworking/answer/6-trends-in-corporate-campus-networks>

6 corporate campus network trends

1. Network automation	네트워크 자동화
2. IT security and work from anywhere	보안과 이동성
3. Wireless	무선
4. IoT and edge computing	IoT와 엣지
5. Cloud	클라우드
6. Machine learning and AI	머신러닝과 AI

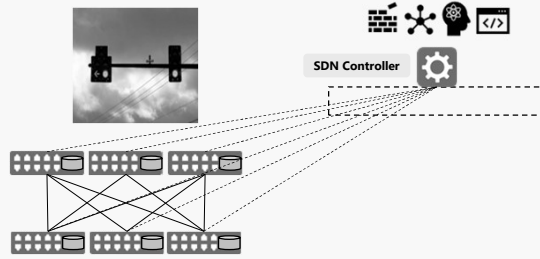
SOURCE: TERRY SLATTERY, ILLUSTRATION: ALDREDD, ADONE STOCK / PEXELS, TECHTARGET. ALL RIGHTS RESERVED.

6

1. 개요

□ 소프트웨어 정의 네트워크(SDN)

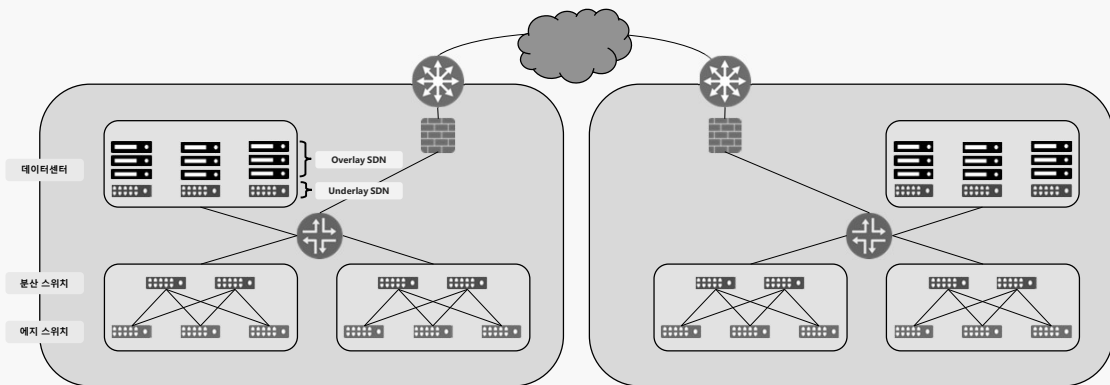
- 네트워크 정보 집중화
- SDN 제어기의 API(Application Programming Interface) 제공
- 네트워크 상황 전지화(全知化) 기반 서비스 제공



1. 개요

□ 자동화를 위한 소프트웨어 정의 네트워크(SDN) 기술 확장 (데이터센터→캠퍼스)

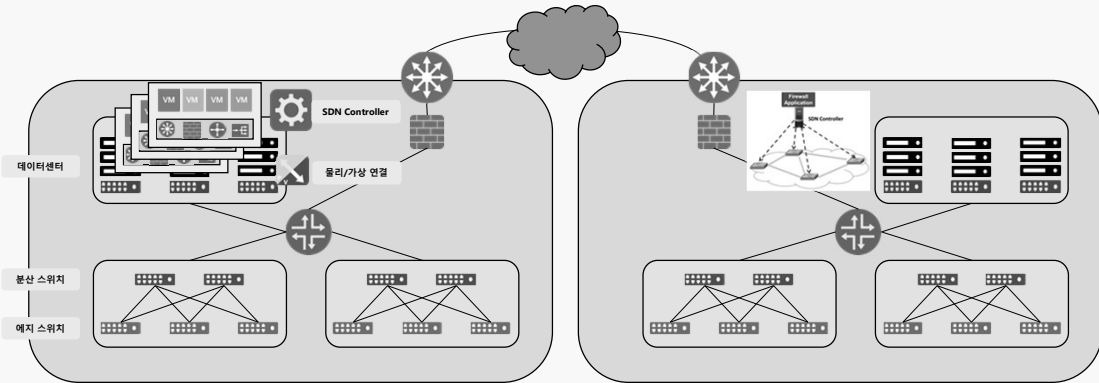
- 언더레이(Underlay) SDN
- 오버레이(Overlay) SDN



1. 개요

□ 데이터센터의 오버레이 SDN (가상 네트워크)

- 오버레이 SDN의 분산처리: dSwitch, dRouter, dFW, dLB (VM 이동시 보안 정책 유지)
- 전용 제어기(SDN Controller) 사용
- Overlay/Underlay (물리/가상) 연결: VxLAN 프로토콜 사용 (VLAN, Multicast, VxLAN 헤더)



9

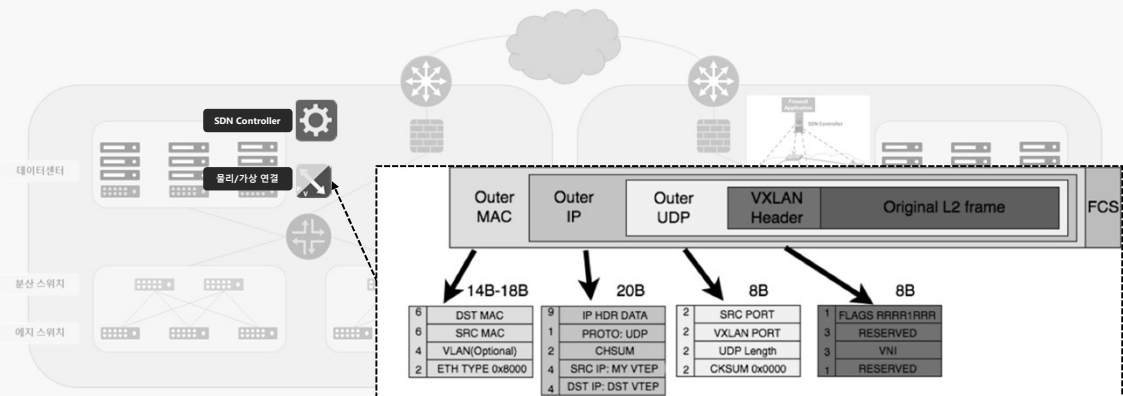
JS Lab

9

1. 개요

□ 오버레이 SDN을 위한 VxLAN

- VXLAN tunnel endpoint (VTEP)
- VLAN
- Multicast



10

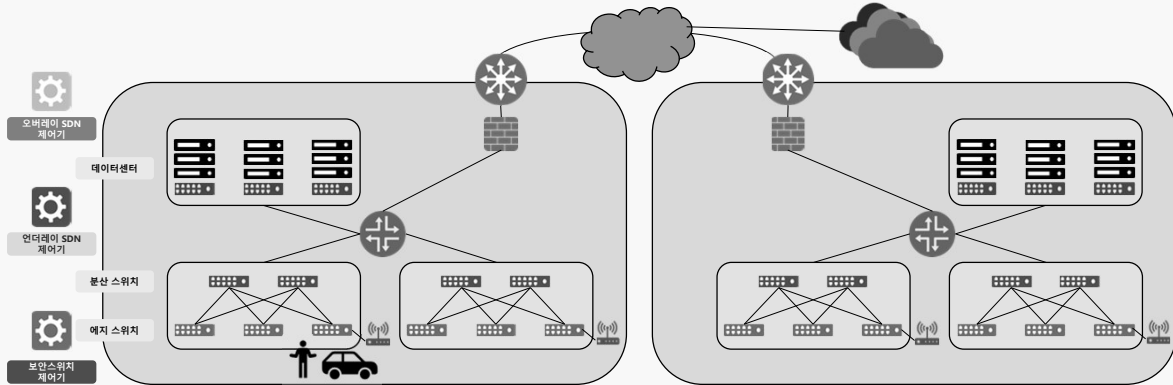
JS Lab

10

1. 개요

□ SDN 기술의 캠퍼스 네트워크 확장

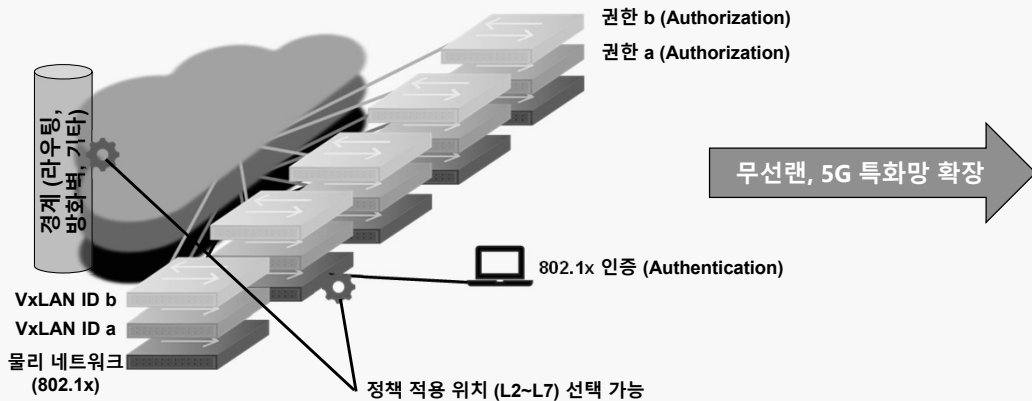
- 기대 서비스: 사용자 이동시 보안 정책 유지
- 보안 연동 기술 필요: VxLAN, 802.1x, 인증서버, 인사 DB 연계 등
- 제조사 기술: SD-WAN, 보안스위치, 일반 스위치, 무선랜 확장, 5G 특화망 연계 등



1. 개요

□ VxLAN 기반 SDN의 사용자 물리적 멀티 사이트 이동 (예)

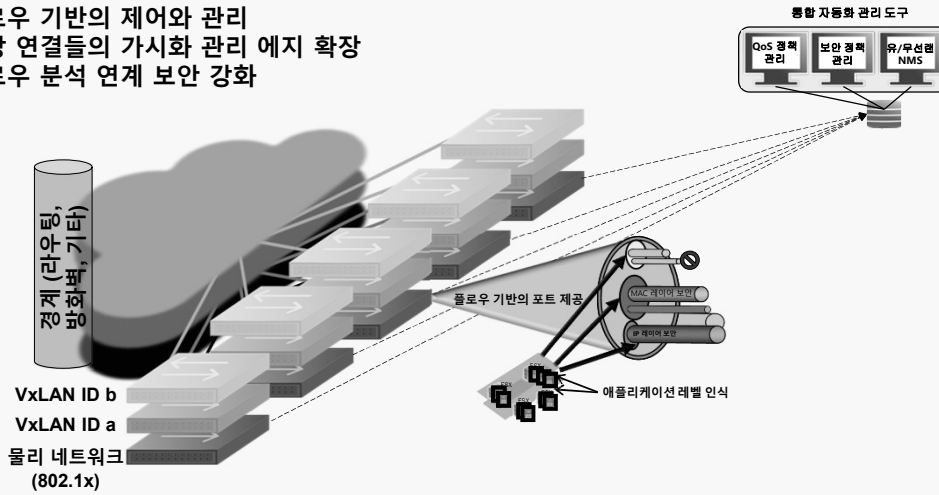
- 인증(Authentication) 기반 권한(Authorization)
- L2~L7 정책 기반 권한
- 정책(권한) 적용 위치 에지에 가까울수록 강화



1. 개요

□ 캠퍼스 제어 관리 경계 구성 (예)

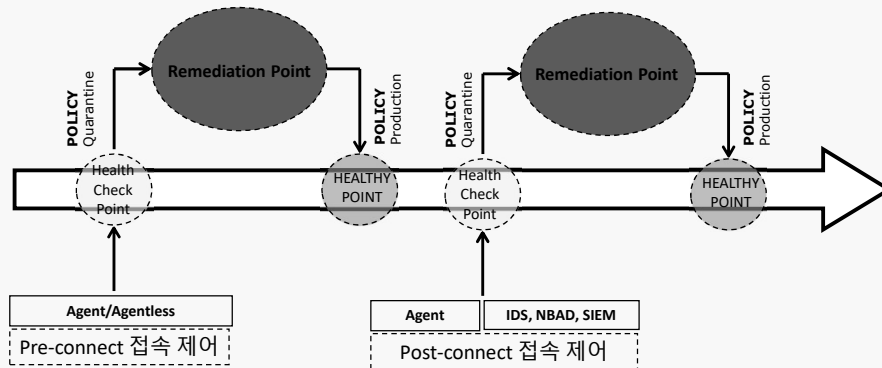
- 플로우 기반의 제어와 관리
- 가상 연결들의 가시화 관리 에지 확장
- 플로우 분석 연계 보안 강화



1. 개요

□ 네트워크 접속제어 (NAC)

- Pre-connect 접속 제어
- Post-connect 접속 제어



1. 개요

□ 네트워크 접속제어 (NAC) 부가 기능

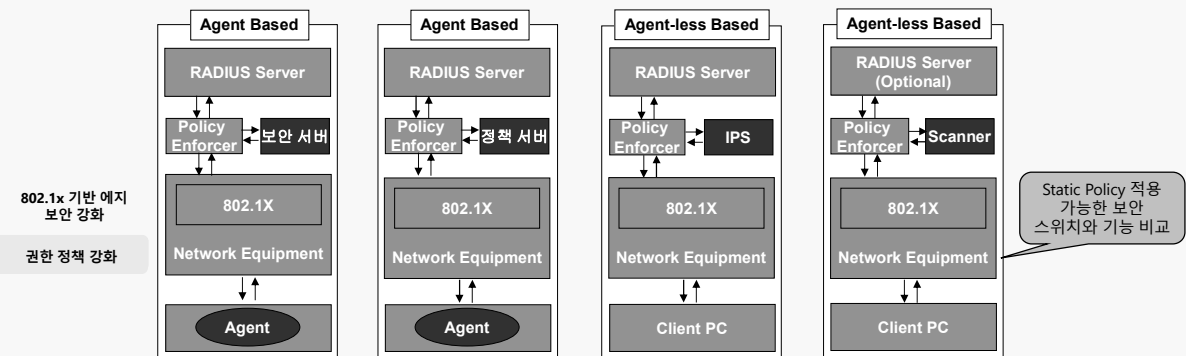
- 위치 기반 (Location)
- 시간 (Time)
- 기기/사용자 결합 (Matching of device to user identity Bonding)



1. 개요

□ 802.1x 사용 예지 보안 강화 유형 (Pre/Post-Connect NAC)

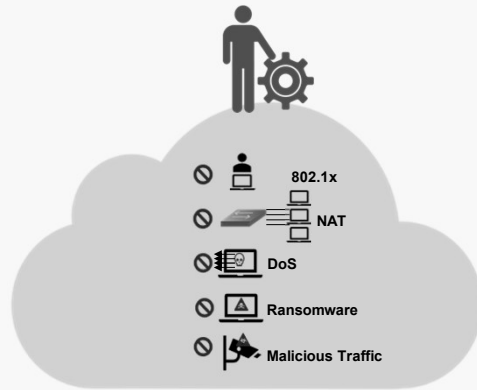
- 네트워크에 보안기능 추가: 보안 장비 추가/연계
- 네트워크 장비에 보안기능 추가: 보안스위치, 일반 스위치의 보안 기능
- 기존 보안장비의 네트워크 통합: ESM 연계, SIEM 연계
- 기존의 보안 기능을 네트워크로 연동: NAC (인증서버 연동, 인사 정보 연동)



1. 개요

□ SDN 제어기(Controller) 기반 에지 스위치의 자동화/Static Policy 보안 강화 (예)

- 802.1x 지원
- 보안 강화 사전 차단
 - 스푸핑 공격,
 - 랜섬웨어 확장
 - IP 전화 도청/IP 카메라 유출/PC 화면 유출
 - 비인가 단말 접근
 - NAT 장비 내부망 접근 제어
 - 유해사이트 / 비인가 사이트
- 네트워크 안정성 설정
 - STP 루프차단
 - QoS 지원 (성능 유지)
- SDN 제어기 기반 중앙 원격 관리
 - 설정
 - 케이블 불량 감지
 - Zero Touch Installation (통신망, USB 매체 등 사용)
- 자동 설정 Backup/Recovery

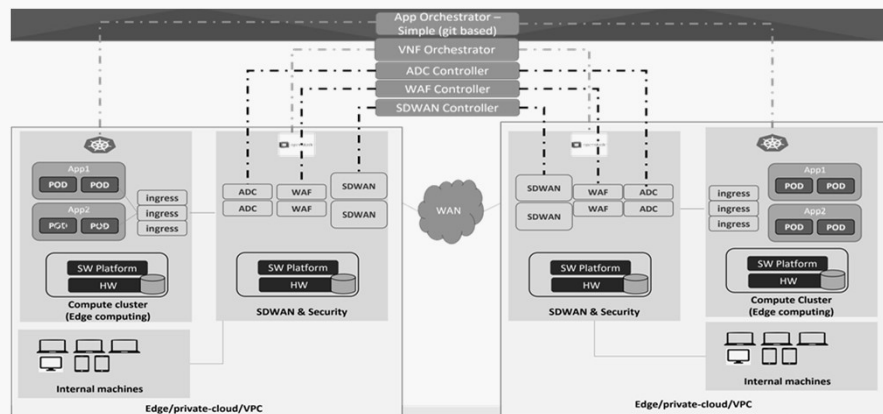


1. 개요

□ 인프라의 보안 종단(End-to-End)간 중앙 제어의 Technical Gap Issues

- Current traffic management and security does not follow application life cycle

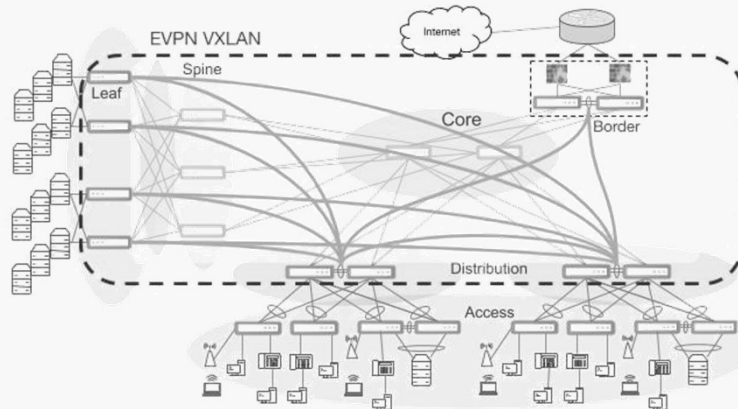
(예) No automation. Any security configuration change takes weeks → No support for dynamic and ephemeral applications, No support for apps that need to scale-out across edges Does not support new kinds of applications



2. 제조사 솔루션

□ 802.1x 멀티 캠퍼스 확장 (큐물러스)

- 컨트롤 플레인: EVPN (Ethernet Virtual Private Network)
- 데이터 플레인: VxLAN (Virtual Extensible LAN)



<https://docs.cumulusnetworks.com/guides/campus-architecture-guide/>

19

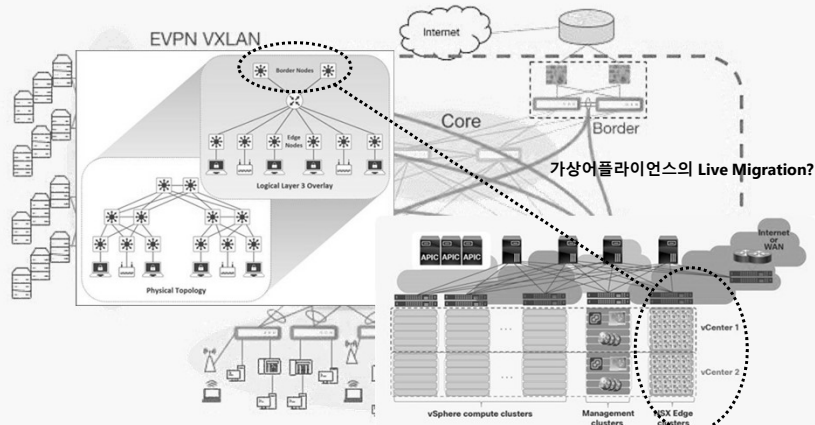
JS Lab

19

2. 제조사 솔루션

□ 802.1x 멀티 캠퍼스 확장 (시스코/VMware)

- 오버레이의 Border node는 물리적으로 1개의 Rack 구성 권장
- 오버레이간 보안 기능 필요 (가상 보안 어플라이언스의 가용성, 성능?)



<https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html>

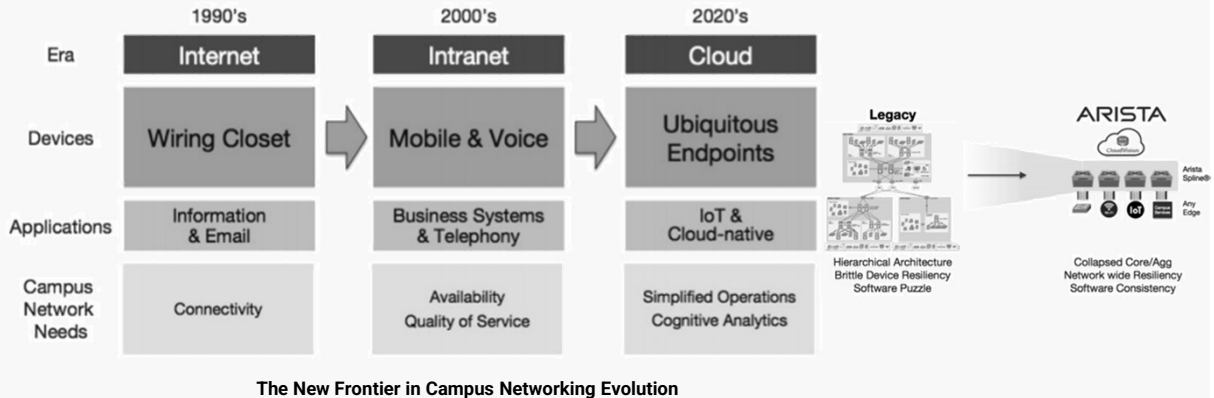
20

JS Lab

20

2. 제조사 솔루션

□ Extending Cloud Grade Principles to the Campus (아리스타)



<https://www.arista.com/en/solutions/cognitive-campus-network>

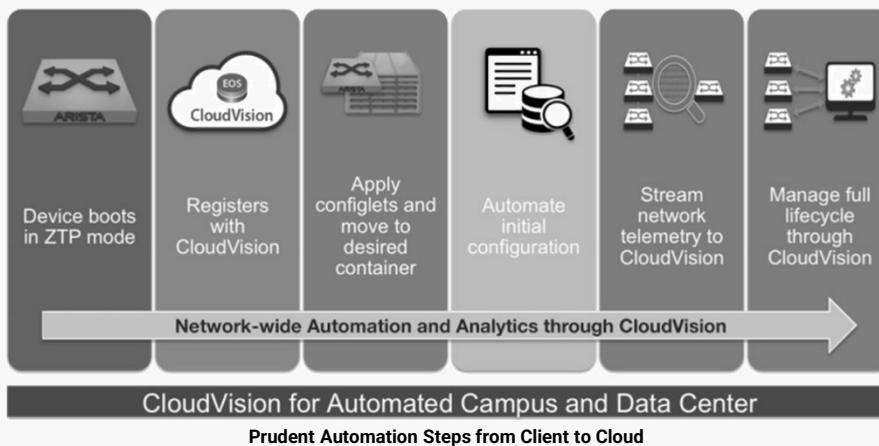
21

JS Lab

21

2. 제조사 솔루션

□ Extending Cloud Grade Principles to the Campus (아리스타)



<https://www.arista.com/en/solutions/cognitive-campus-network>

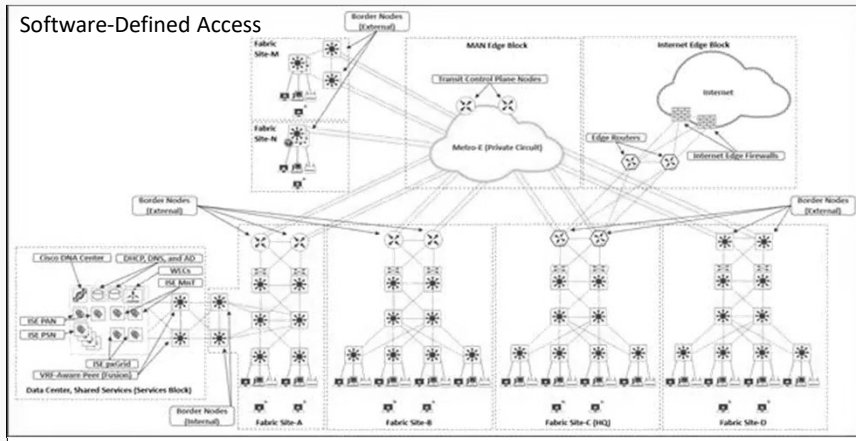
22

JS Lab

22

2. 제조사 솔루션

- SD-Access for Distributed Campus Reference Design (시스코)
- 소프트웨어 정의 접속 (SD-Access)



Design Zone for Campus - Cisco SD-Access Solution Design Guide (CVD) - Cisco

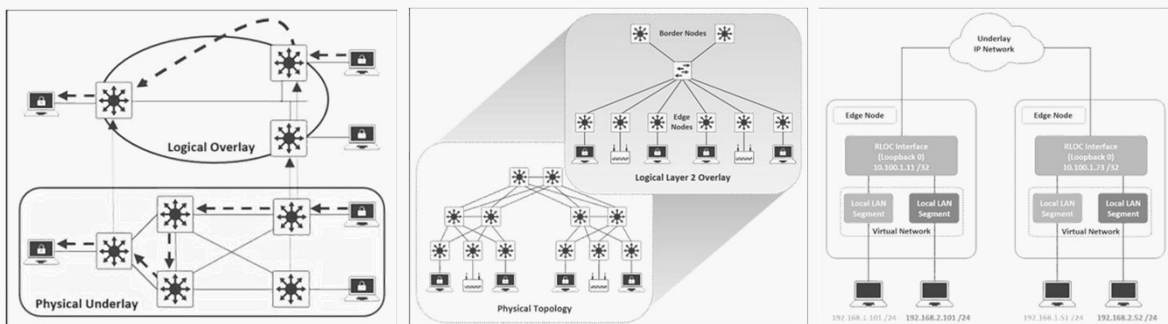
23

JS Lab

23

2. 제조사 솔루션

- SD-Access Architecture (시스코)
 - Overlay and Underlay
 - Subnet Stretching



<https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html#EvolutionofCampusNetworkDesignsforDigitalReadyOrganizations>

24

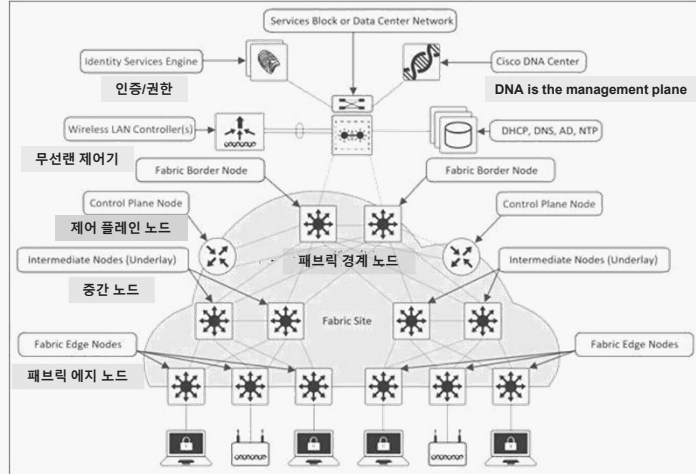
JS Lab

24

2. 제조사 솔루션

□ SD-Access Architecture (시스코)

▪ SD-Access Fabric Roles



<https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html#EvolutionofCampusNetworkDesignsforDigitalReadyOrganizations>

2. 제조사 솔루션

□ 802.1x 지원 국내 스위치 (파이오링크, 핸드림넷)

The screenshot shows the PIOLINK website for the Cloud-Security-Switch. The page features a header with the PIOLINK logo and navigation links. The main content area includes a product image and a list of features:

- 직관적인 인터페이스, 모바일 앱 제공
- 다수의 사이트, 스위치 및 연결 장비의 통합 뷰
- 제스, OAS, DSM, MAC 기능 통합
- 관리자 권한을 설정할 수 있음
- 규모와 상관없이 한 개터 관리시스템

 Below the features, there is a section titled '한눈에 보고, 바로 파악.' (See at a glance, understand immediately.) with sub-points:

- 모바일, IoT 등으로 내부 네트워크가 확대되면서 알 수 없거나 관리되지 않는 장비가 늘어났습니다. 가시성 문제는 보안과 연결됩니다. 클라우드 보안스위치는 분산 구축된 스위치, 연결 단말, 트래픽 현황 등을 세밀하게 모니터링하고 한눈에 파악할 수 있습니다.

 At the bottom, there are three icons representing:

- 지도와 토폴로지 맵으로 스위치 위치 및 연결구성 관리
- 스위치/포트/클라이언트별 트래픽 분석 및 필터링
- 사용자 단말 정보 수집 및 분류, IP 관리 및 저지관리

 The URL at the bottom is <http://www.piolink.com/kr/product/Cloud-Security-Switch.php>

<http://www.piolink.com/kr/product/Cloud-Security-Switch.php>

The screenshot shows the HANDREAM website for the subgate_security_switch. The page features a header with the HANDREAM logo and navigation links. The main content area includes a product image and a list of features:

- 클라우드 매니지드 환경에 최적화, 지능형 네트워크 보안 적용
- 모놀리식 내트 워크에서 멀티-클라우드 환경으로 넘어가면서 Config 자동 설치, Config 자동 백업 및 장애 시 설정 복구 기능 통해 보안 사고 예방 네트워크 운영환경 제공이 가능합니다.
- 차세대 MDS 보안 엔진 적용
- 차세대 MDS 엔진 탑재로 랜섬웨어 확산 방지, IP공유기 방지 차단이 가능하며, Full Wire Speed의 성능을 제공하여 보안 가능 수량 시에도 속도 저하 없이 안정적인 운영이 가능합니다.
- 지능형 보안 네트워크 전용 네트워크 플로우 분석 엔진(NFA Engine) 탑재
- 네트워크 플로우 분석, 알람 플로우 분석, 제3자 플로우 분석, 대용량 세션 관리 기술, 하이브리드 스위칭 기술 등 Network Flow Analytics로 악의적 보안 위협 행위에 대해 지능형 공격 탐지(Intelligent Security Network)를 제공합니다.
- 향상된 하드웨어 설계
- 안정적인 네트워크 서비스 제공을 위해 최대 56포트로 지원하고, 고밀도/모놀리식 임플리 10G 지원, 향상된 용량과 대용량 메모리 탑재 등 고밀도 기술 적용 및 최적의 성능을 제공합니다.

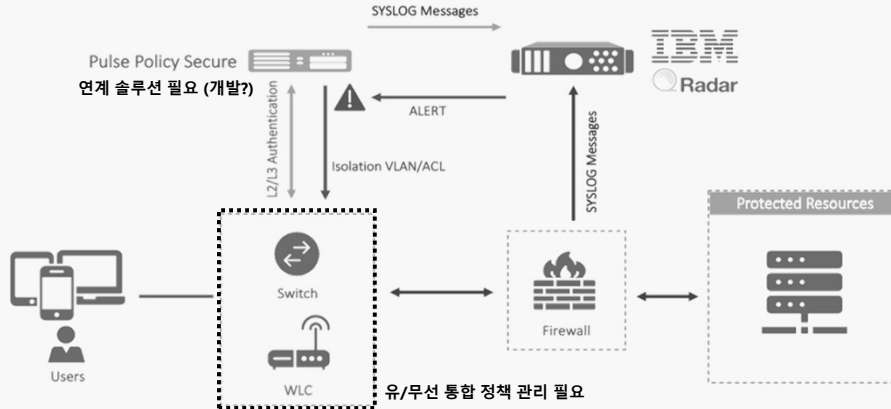
 The URL at the bottom is https://www.handream.net/product/subgate_security_switch/cloud_security_switch/

https://www.handream.net/product/subgate_security_switch/cloud_security_switch/

2. 제조사 솔루션

□ Threat Management Integration (IBM, Pulse Secure)

- 스위치 연계 L7 보안 영역 자동화 확장 (Isolation VLAN/ACL)



https://www.google.com/url?sa=i&url=https://3A%2F%2Fjp.pulsesecure.net%2Fresource%2Fibm-radar%2Fdownload%2F&sig=AOvAw1uuQ7pqjYf91y09f87Jk0ust=16154446674480008&source=images&cd=vfe&ved=2ahUKEwjud29jqXvAHUnQUHUU_gDJ4Q4kDeqUIARCIAQ

27

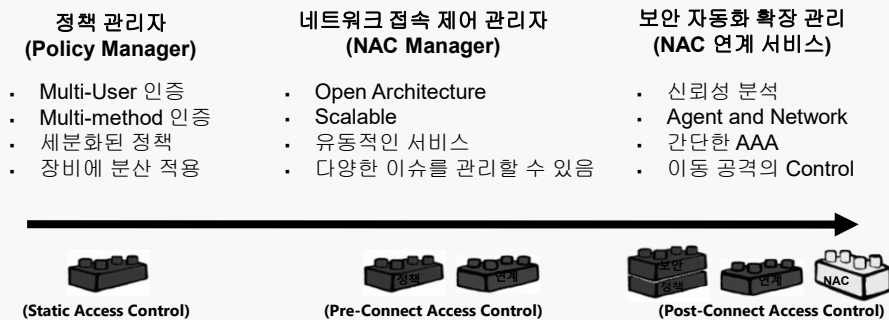
JS Lab

27

III. 네트워크 보안 자동화

□ Threat Management Levels for Access Control

- Static Access Control (예: Policy Manager 사용)
- Pre-Connected Access Control (예: NAC Manager, AAA 인증/권한/측정)
- Post-Connect Access Control (예: 보안의 NAC Manager 연계 서비스)



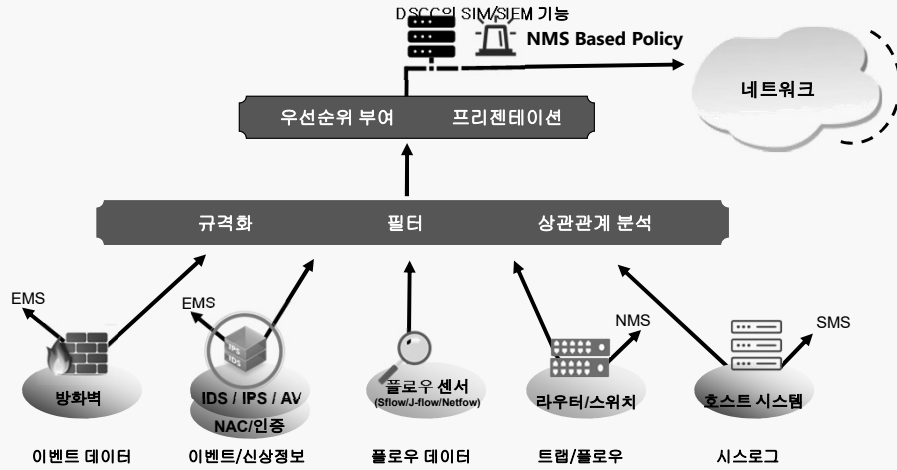
28

JS Lab

28

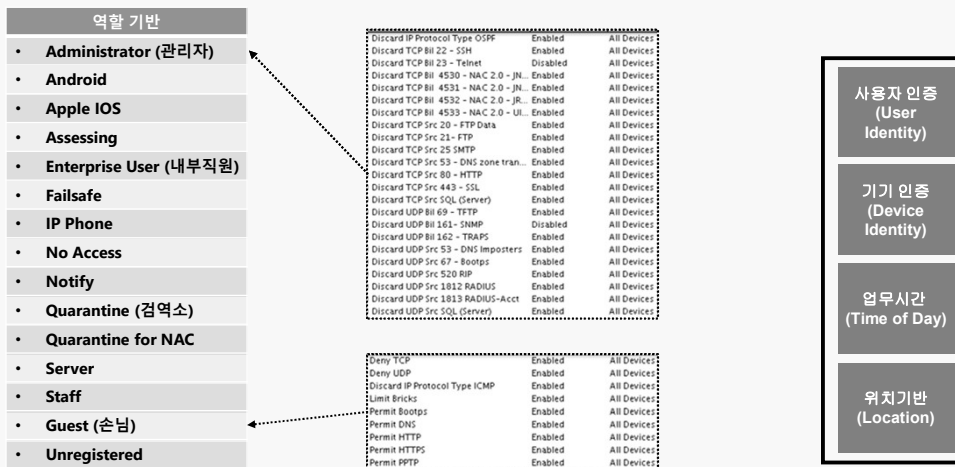
III. 네트워크 보안 자동화

□ Security Event and Incident Management (SEIM)의 상호연관 분석 확장



III. 네트워크 보안 자동화

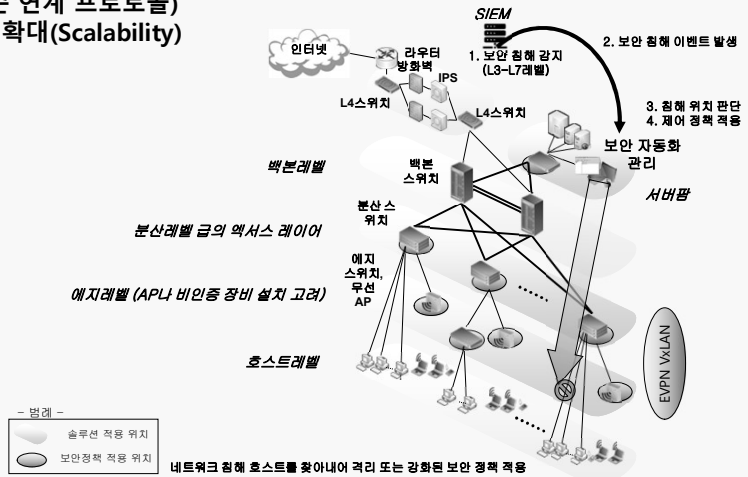
□ 역할 기반 관리(예): Static and/or Dynamic ACL



III. 네트워크 보안 자동화

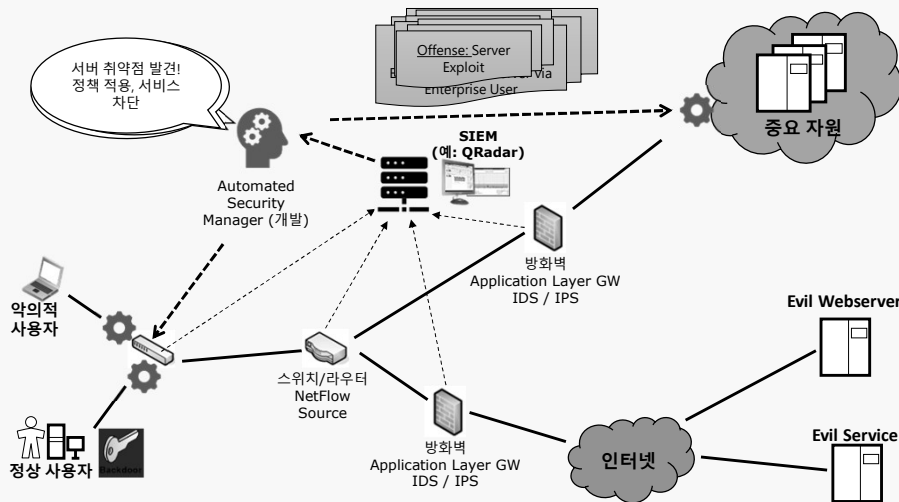
□ Post-Connect Access Control with Automated Security (App/Service)

- SIEM 연계 Open Architecture(표준 연계 프로토콜)
- 보안/네트워크 장비들의 적용 범위 확대(Scalability)
- 유동적인 서비스



III. 네트워크 보안 자동화

□ 보안 자동화 관리 (Automated Security Manager)



IV. 요약

□ 단말 보안 고려 요소: 중앙관리, 운영체제 다양화, 클라우드나 IoT 등의 트렌드 수용



33

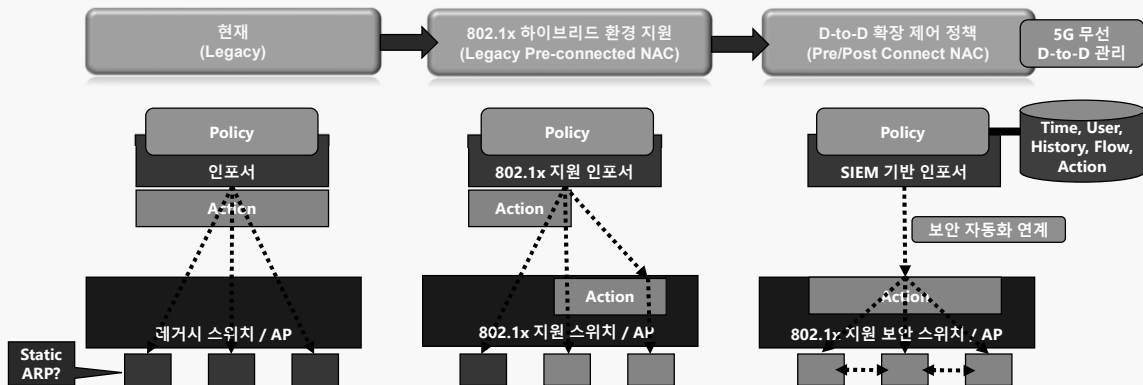
JS Lab

33

IV. 요약

□ 제어기 사용 SDN 기반 인포서를 사용하는 Migration:

- 레거시 NAC / 802.1x 적용 하이브리드 / 802.1x 보안 스위치 지원
- 제어기 기반 정책/제어 강화: Device 접속 위치에서 Action
- 분산 정책 인포서 (Distributed Policy Enforcer)



34

JS Lab

34

감사합니다.

