Juniper Networks | Driven by Experience™

AI 기반 캠퍼스

향후 10년의 캠퍼스 네트워크를 위한 인공지능(AI) 활용

백서

목차

개요

앞으로 10년간 네트워크는 최고의 사용자 경험을 제공하고 IT 운영을 간소화하는 데 초점이 맞추어질 것입니다. 기존의 유무선 LAN 솔루션은 오늘날의 다양한 엔터프라이즈 요구 사항을 해결하는 데 필요한 확장성, 안정성, 민첩성이 부족합니다.

클라우드, 모바일, IoT 시대에 AI 기반 캠퍼스는 인공지능(AI)을 활용합니다. 주니퍼의 캠퍼스 솔루션은 강력한 하드웨어 포트폴리오에 Mist AI™를 결합하여 네트워크 운영을 간소화하고, 사용자 경험을 개선하고, IT 팀이 전략적 이니셔티브에 집중할 수 있는 환경을 제공합니다. 이 백서에서는 Mist AI로 지원하는 엔드투엔드 AI 기반 캠퍼스 네트워크 구성요소를 설명합니다.

소개

엔터프라이즈 네트워크는 점점 증가하는 클라우드 지원 네트워크의 필요성과 다양한 모바일 및 IoT 디바이스를 지원하는 방향으로 대대적인 전환기를 겪고 있습니다. 하지만 디바이스 개수가 증가하면 그만큼 복잡성도 심해집니다. 클라우드 기반 애플리케이션은 새로운 비즈니스 모델을 구현하며 비즈니스 민첩성을 향상시키고 UC(unified communications), 비디오, 기타 지연에 민감한 애플리케이션 등 핵심 기술의 사용을 지원합니다. 또한 기술이 발전하고 머신러닝(ML) 및 AI가 광범위하게 도입됨에 따라 IT 팀과 최종 사용자의 운영과 경험을 크게 개선할 수 있습니다.

오늘날 네트워크 설계자는 개방형 표준과 소프트웨어 기반 관리 플랫폼을 사용하여 데이터, 음성, 비디오를 위한 클라우드 애플리케이션을 배포하고 운영 비용 절감하고자 하는 기업 요구를 충족하기 위해 네트워크를 재설계하고 있습니다. 궁극적인 목표는 더욱 간소화된 자동화, 텔레메트리, AI 기능을 활용하여 향후 10년을 위한 네트워크를 구축하는 일입니다.

주니퍼 AI 기반 캠퍼스 네트워크

주니퍼 네트웍스의 클라우드 서비스, 소프트웨어, 하드웨어 제품 포트폴리오는 WAN, LAN, Wi-Fi, 보안 영역 전반으로 확장되는 엔드투엔드 캠퍼스 네트워크 솔루션을 제공하며 EVPN-VXLAN(Ethernet VPN-Virtual Extensible LAN)과 같은 개방형 표준 지원으로 아키텍처 단순성, 확장성, 성능을 향상시킵니다.

주니퍼의 AI 기반 캠퍼스는 다음과 같이 구성됩니다.

- 현대적인 마이크로서비스 클라우드 AIOps 플랫폼
- AI 기반 Wi-Fi 및 유선 스위칭
- EVPN-VXLAN을 실행하는 캠퍼스 패브릭
- 클라우드 레디 캠퍼스 이더넷 스위치
- Wi-Fi, Bluetooth LE 및 IoT를 위한 엔터프라이즈급 액세스 포인트
- 주니퍼 커넥티드 시큐리티(Connected Security) 및 네트워크 세그먼테이션
- Junos® 운영 체제
- Junos Telemetry

현대적인 마이크로서비스 클라우드 AIOps 플랫폼

Juniper® Mist 클라우드 아키텍처는 마이크로서비스로 구축되어 탁월한 민첩성, 확장성, 복원력을 발휘합니다. 필요에 따라 클라우드 서비스를 탄력적으로 확장하거나 축소함으로써 모놀리식(Monolithic) 하드웨어의 비용과 복잡성에서 탈피할 수 있습니다. 또한 네트워크 중단 없이 거의 매주 최신 기능과 버그 수정이 제공될 수 있습니다. 플랫폼은 개방형 API를 사용하여 100% 프로그래밍 가능하며, 이에 따라 완전한 자동화를 달성했으며 여러 보완 제품과 원활하게 통합됩니다. 주니퍼 Mist 클라우드 아키텍처는 AI, ML, 데이터 서비스를 최신 마이크로서비스 기술과 조합하는 혁신적인 엔터프라이즈 네트워크 접근 방식을 통해 완전히 새로운 솔루션을 제공합니다.

AI 기반 Wi-Fi와 유선 스위칭

주니퍼는 Mist AI를 캠퍼스 네트워크에 적용하여 통합된 유무선 솔루션 전체에서 사용자 경험을 최적화하고 IT 운영을 간소화합니다. 기존 솔루션은 이미 15년이 넘었으며 확장하기에 너무 많은 비용이 들고, 버그가 쉽게 발생하며, 관리하기 어려운 모놀리식 코드 기반을 사용합니다. 사용자 경험은 새로운 업타임이나 마찬가지이며, 성공적인 IT 인프라를 평가하기 위해 가장 중요한 단일 측정 항목입니다. 주니퍼는 이를 어떻게 달성할까요?

주니퍼 Mist Wi-Fi Assurance 서비스는 더 이상 수작업으로 문제를 해결할 필요가 없는 자동화된 무선 운영을 통해 예측 가능하고 신뢰할 수 있으며 측정 가능한 Wi-Fi를 구현합니다. 이상 징후를 탐지하면 자동으로 패킷 캡처가 트리거되어 이벤트를 상관분석하고 클라이언트 레벨에서 네트워크 인텔리전스 구축과 RRM(Radio Resource Management)이 이루어집니다. 그 결과 무선 네트워크 사용자 경험을 이전보다 훨씬 명확하게 파악할 수 있는 가시성을 확보합니다.

주니퍼 Mist Wired Assurance(그림 1)는 유선 디바이스를 AI 기반으로 자동화합니다. 주니퍼 네트웍스 EX 시리즈 이더넷 스위치의 Junos 텔레메트리를 활용하여 운영이 더욱 간편해지고 평균 복구 소요 시간(MTTR)이 단축되며 IoT 디바이스, 서버, 프린터 등의 사용자 경험에 대한 가시성도 높아집니다. 주니퍼 Mist Wired Assurance로 주니퍼 Mist 클라우드 아키텍처에서 수행하는 온보딩, 프로비저닝, 관리 작업 등 모든 EX 시리즈 스위칭이 간소화됩니다.

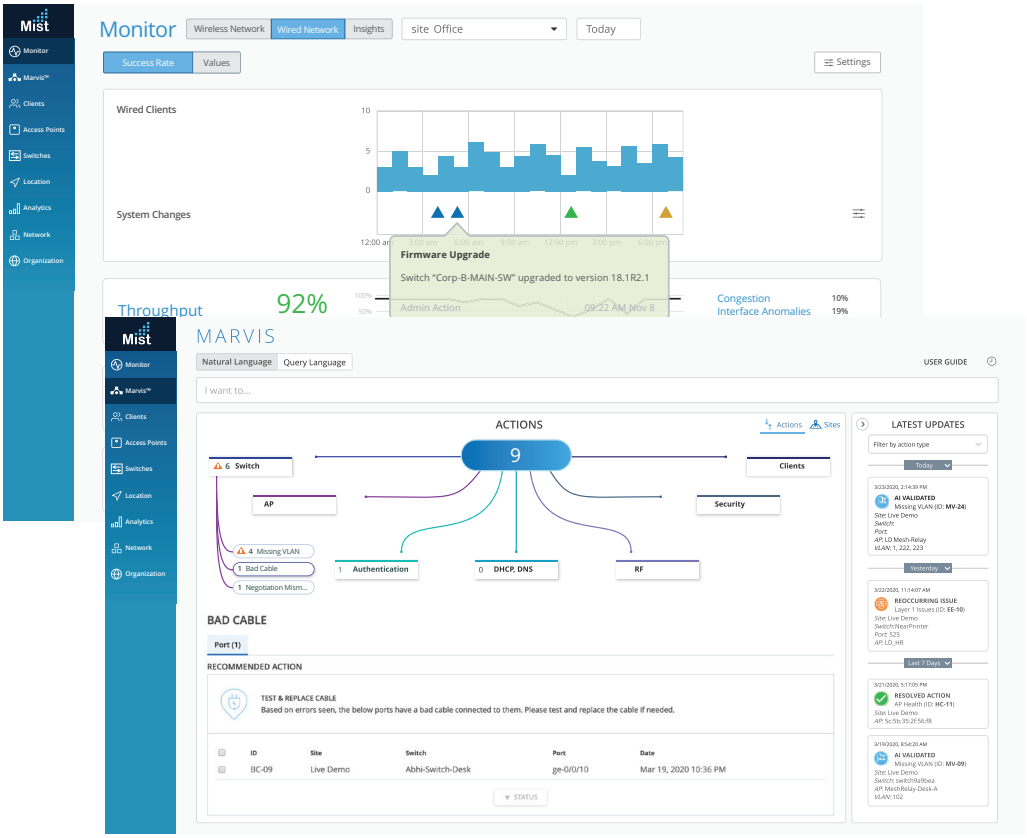

그림 1: Wired Assurance 및 Marvis Virtual Network Assistant

Marvis Virtual Network Assistant(그림 1)는 Mist AI를 통해 엔터프라이즈 WLAN, LAN, WAN 네트워크를 운영하고 관리합니다. 사용자는 자연어를 사용하여 Mist AI 엔진과 직접 상호작용할 수 있습니다. 따라서 네트워크 운영 방식이 사후대응식의 문제 해결에서 셀프 드라이빙 액션을 통한 선제적 수정 방식으로 발전합니다. Marvis는 IT 효율성을 높이고 지원 요청 티켓을 최소화하며 해결에 소요되는 시간을 줄입니다. AIOps(AI for IT Operations) 도입이 가속화됨에 따라 Marvis는 조직이 대규모 IT 운영을 정확하고 효율적으로 관리할 수 있도록 지원합니다.

캠퍼스 패브릭

캠퍼스에서 IoT 디바이스의 사용이 증가함에 따라 네트워크는 복잡성을 추가하지 않고 빠르게 확장해야 합니다. 이러한 IoT 디바이스 중 상당수는 네트워킹 기능이 제한적이며 건물이나 캠퍼스에서 L2 인접성(L2 Adjacency)을 필요로 합니다. 하지만 L2 네트워크는 루프를 유발하고 장애에 대한 컨버전스 속도가 느리며 데이터 플레인 플러딩(Data Plane Flooding)으로 인한 보안 우려가 있습니다. 이전까지는 독점적인 프라이빗 VLAN을 통해 보안 문제가 해결되었지만, L2에는 루프와 느린 컨버전스 문제가 여전히 존재합니다. 하지만 이러한 접근 방식은 비효율적이고 관리하기가 어렵습니다. 네트워크 대역폭을 과도하게 소모하기 때문에 비효율적이며, 새로운 네트워크 포트로 VLAN을 확장해야 하기 때문에 관리하기 어렵습니다.

EVPN-VXLAN

AI 기반 캠퍼스 아키텍처는 EVPN(Ethernet VPN)과 VXLAN(Virtual Extensible LAN) 등의 공개 표준 기술을 활용하여 언더레이 네트워크에서 오버레이 네트워크를 분리합니다. 이로써 루프가 없고 컨버전스 속도가 더욱 빠른 네트워크를 제공할 수 있으며 네트워크 관리자가 여러 L3 네트워크에서 논리적 L2 네트워크를 생성할 수 있게 되어 현대적인 엔터프라이즈 네트워크에 대한 요구를 충족합니다. 또한 EVPN-VXLAN은 IoT 디바이스 사이에서 트래픽을 분리하여 마이크로 세그먼테이션을 지원함으로써 보안을 더욱 강화합니다. 주니퍼는 다음과 같은 검증된 EVPN-VXLAN 캠페인 패브릭을 지원합니다.

- **EVPN 멀티호밍(collapsed core 또는 distribution)**: 네트워크 분산 시 EVPN 멀티호밍을 통해 디바이스 한 쌍에서 LAG에 대한 액세스 스위치가 가능해집니다. 액세스 레이어에서 분산 레이어에 대한 멀티호밍 기능이 제공되므로 캠퍼스 네트워크 전체에서 STP(Spanning Tree Protocol)를 사용할 필요가 없습니다. 또한 디스트리뷰션 및 코어 레이어가 통합될 수 있습니다.
- **캠퍼스 패브릭 코어 디스트리뷰션**: 상호 연결된 EX 시리즈 코어 또는 디스트리뷰션 스위치 한 쌍이 EVPN L2 및 L3 VXLAN 게이트웨이에 대한 지원을 제공할 수 있습니다. 디스트리뷰션 및 코어 레이어 간의 IP Clos 네트워크는 두 가지 모드의 코어 레이어로 중앙식 또는 에지 라우팅 브리지 오버레이를 제공합니다.
- **캠퍼스 패브릭 IP Clos:** 캠퍼스 패브릭 IP Clos 아키텍처는 VXLAN L2 게이트웨이 기능을 액세스 레이어로 푸시하며, 이에 따라 마이크로 표준 기반, 그룹 기반 정책에 따른 세그먼트 분할이 가능해집니다.

엔드투엔드 EVPN-VXLAN 아키텍처를 사용하면 주니퍼에서 제공하는 OTT(Over-the-Top) 정책 및 제어를 통해 캠퍼스와 데이터센터를 단일 IP 패브릭으로 관리할 수 있습니다. 또한 네트워크 전체에서 그룹 기반 정책을 사용한 정책 적용이 간편해집니다. Clos 네트워크 또는 IP 패브릭에서 원하는 개수의 스위치를 연결할 수 있습니다. EVPN-VLAN이 패브릭을 확장하고 여러 엔터프라이즈 건물을 연결하며, VXLAN이 네트워크 전체로 L2를 확장합니다.

자세한 내용은 www.주니퍼.net/assets/us/en/local/pdf/solutionbriefs/3510643-en.pdf를 참조하십시오.

주니퍼는 EVPN-VXLAN 기반 아키텍처뿐만 아니라 Virtual Chassis 기술을 지원하여 최대 10개의 상호 연결된 스위치가 단 하나의 IP 주소를 사용하는 단일, 논리적 디바이스로 작동할 수 있습니다. Virtual Chassis 기술을 통해 엔터프라이즈는 엔드포인트를 논리적 그룹으로 그룹화하여 물리적 토폴로지를 분리함으로써 리소스를 효율적으로 활용할 수 있습니다.

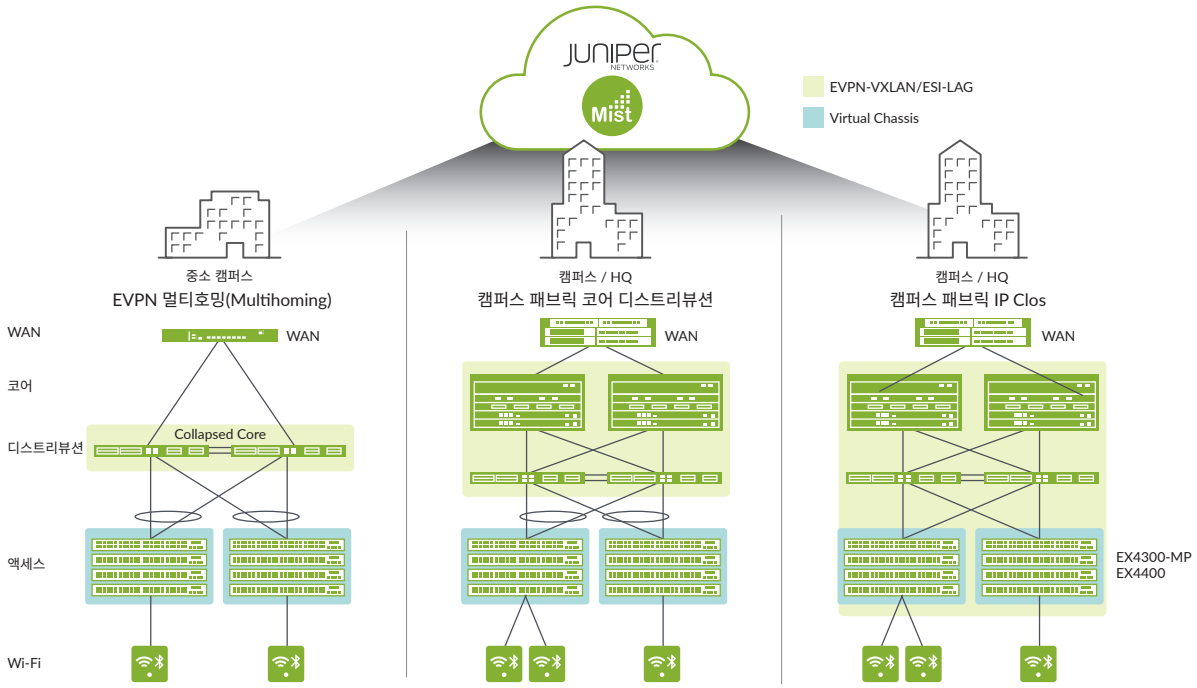

그림 2: Virtual Chassis 와 EVPN-VXLAN 기반 아키텍처를 보여주는 캠퍼스 패브릭

클라우드 레디 캠퍼스 이더넷 스위치

주니퍼는 엔터프라이즈 캠퍼스 네트워크를 위해 AI 기반의 프로그래밍 가능한 오픈 액세스 및 코어/디스트리뷰션 스위치 포트폴리오를 제공합니다. 액세스 스위치는 클라우드에 사용할 수 있고 주니퍼 Mist Wired Assurance를 지원하므로 AIOps가 레이어 스위칭에 액세스할 수 있습니다. 스위치는 다음과 같은 여러 가지 캠퍼스 요구 사항을 충족합니다.

- 클라우드 레디 및 주니퍼 Mist 클라우드 아키텍처 기반 관리
- 멀티기가비트 지원
- MACsec(Media Access Control Security) AES256
- Power over Ethernet(PoE/PoE+/PoE++)
- Virtual Chassis 및 EVPN-VXLAN를 통해 확장 가능한 패브릭 아키텍처
- 멀티벤더 지원
- 그룹 기반 정책(GBP)을 사용한 표준 기반 마이크로 세그먼테이션
- 플로우 기반 텔레메트리

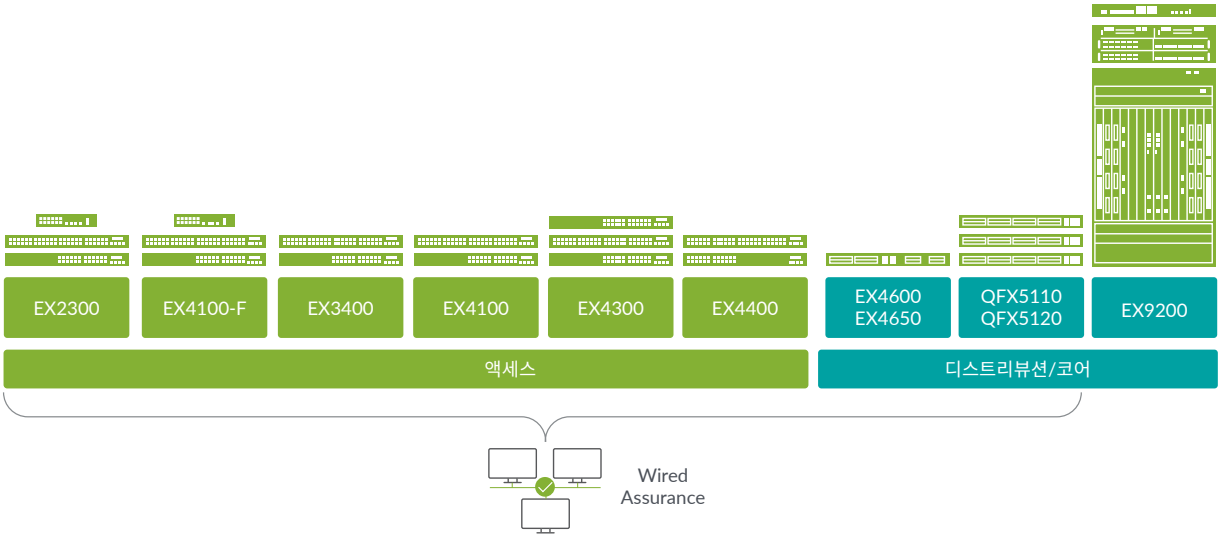

그림 3: EX 시리즈 및 QFX 시리즈 스위치의 캠퍼스 포트폴리오

AI 기반 캠퍼스 패브릭 구축

캠퍼스 패브릭을 수작업으로 구성하면 구축 시 일관성이 떨어지며, 작업자에 의한 오류가 발생할 수 있습니다. 주니퍼는 EVPN-VXLAN 캠퍼스 패브릭의 수월한 구축과 관리를 지원하는 주니퍼 Mist 클라우드를 통해 이러한 운영 부담을 해결합니다. 구체적으로 설명하면, 관리자가 토폴로지(EVPN 멀티호밍, 디스트리뷰션-코어, 또는 IP CLOS)를 선택하기만 하면 소프트웨어가 나머지 작업을 처리합니다(그림 4 참조). 이러한 AI 기반 접근 방식은 캠퍼스와 브랜치의 LAN, WLAN, WAN 환경 전체에 대한 관리를 통합하며, 동시에 유무선 캠퍼스 네트워크가 뛰어난 사용자 경험을 제공하도록 보장합니다.

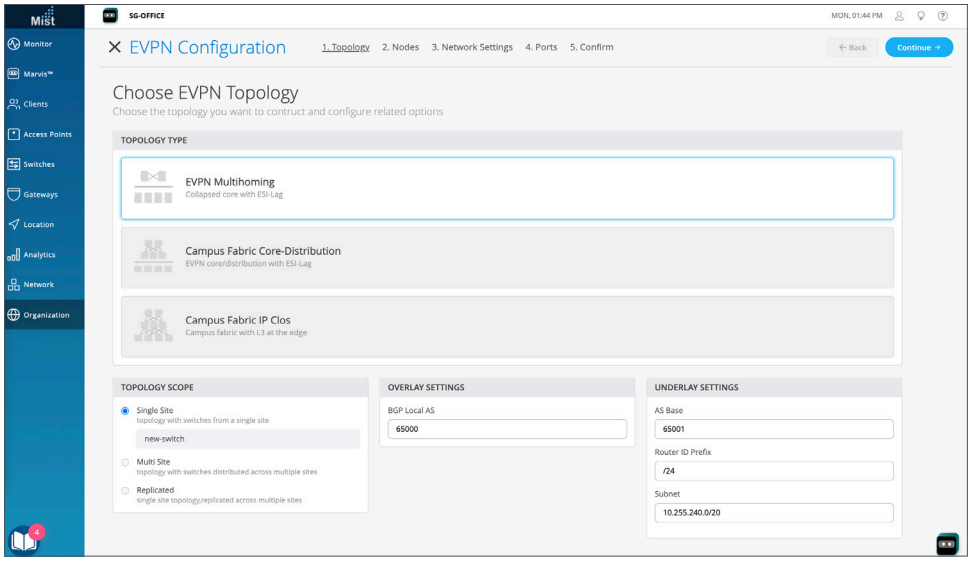

그림 4: 주니퍼 Mist Wired Assurance 캠퍼스 패브릭 설계

*처음에는 EVPN 멀티호밍이 지원되며, 향후 릴리스에서 다른 아키텍처가 추가로 지원됩니다.

AI 기반 캠퍼스 패브릭 운영

주니퍼 Mist™ Wired Assurance는 클라우드에서 관리하는 EX 시리즈 이더넷 스위치를 클레임, 구성, 관리하고 문제를 해결합니다. 클라우드 기반 서비스는 연결된 디바이스에 더욱 우수한 경험을 제공하기 위해 AI 지원 자동화와 서비스 레벨을 제공합니다. 주니퍼 Mist Wired Assurance는 풍부한 Junos® 운영 체제 스위치 텔레메트리 데이터를 활용하여 운영을 간소화하고, 평균 복구 소요 시간(MTTR)을 줄이고, 가시성을 높입니다. Day 0부터 Day 2 운영까지 핵심적인 특성은 다음과 같습니다.

- **Day 0 운영**—단일 활성화 코드를 사용하여 그린필드 스위치를 클레임하거나 브라운필드 스위치를 채택하여 온보드가 원활하게 전환되고 플러그 앤 플레이의 간편함을 확실히 누릴 수 있습니다.
- **Day 1 운영**—기존 및 캠퍼스 패브릭 구축의 대량 롤아웃을 위해 템플릿 기반 구성 모델을 구현하며, 동시에 맞춤형 사이트 또는 스위치별 속성을 적용하는 데 필요한 유연성과 제어 능력을 유지합니다. 다이나믹 포트 프로필(Dynamic Port Profiles)을 통해 포트 프로비저닝을 자동화합니다.
- **Day 2 운영**—주니퍼 Mist Wired Assurance의 AI를 활용하여 핵심적인 사전 또는 사후 연결 메트릭으로 처리량, 성공적인 연결, 스위치 상태와 같은 서비스 레벨의 기대를 충족합니다(그림 5 참조). 여기에 루프를 감지하고, 누락된 VLAN을 추가하고, 잘못 구성된 포트를 수정하고, 문제 있는 케이블을 파악하고, 플래핑하는 포트를 격리하고, 계속 문제가 발생하는 클라이언트를 찾는 Marvis Actions의 셀프 드라이빙 기능까지 더해졌습니다(그림 6 참조). 또한 주니퍼 Mist 클라우드를 통해 소프트웨어 업그레이드를 손쉽게 수행합니다.

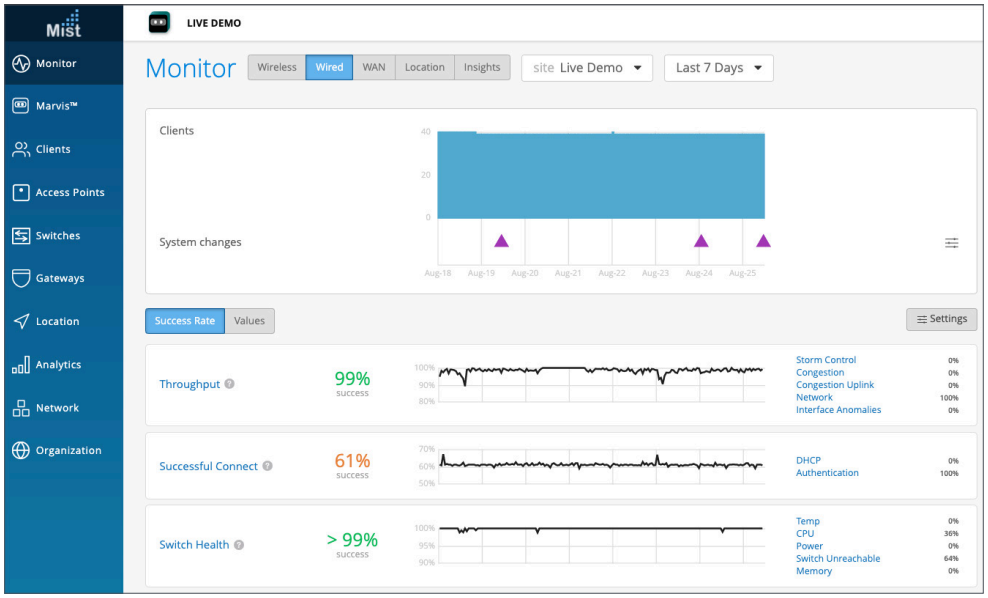

그림 5: 주니퍼 Mist Wired Assurance SLE(Service-Level Expectations)

그림 6: 유선 스위치를 위한 Marvis Actions

주니퍼 Mist™ Wired Assurance에 대해 자세한 정보를 확인하십시오.

엔터프라이즈급 Wi-Fi 액세스 포인트

주니퍼는 엔터프라이즈급 액세스 포인트를 사용해 Wi-Fi, Bluetooth LE(Low Energy), IoT의 컨버전스를 가속화합니다. 이러한 제품들은 머신 러닝과 이벤트 상관관계를 활용하여 데이터 수집, 분석, 정책 시행 기능을 제공합니다. 주니퍼 고성능 액세스 포인트 AP 43 및 AP 45 시리즈에는 특허 출원된 동적 vBLE 기반 16 요소 안테나 어레이가 탑재되어 업계에서 가장 정확하고 확장성이 뛰어난 위치 서비스를 제공합니다. 주니퍼 액세스 포인트는 150개 이상의 상태에 대한 메타데이터를 수집하여 Mist AI 엔진으로 유입하도록 특별히 설계되었습니다.

특징	AP45	AP34	AP43	AP63	AP33	AP32	AP12
Wi-Fi 표준	Wi-Fi 6E 802.11ax (Wi-Fi 6) 4x4: 4SS	Wi-Fi 6E 802.11ax (Wi-Fi 6) 2x2: 2SS	802.11ax (Wi-Fi 6) 4x4: 4SS	802.11ax (Wi-Fi 6) 4x4: 4SS	802.11ax (Wi-Fi 6) 5GHz: 4x4 : 4SS 2.4GHz: 2x2: 2SS	802.11ax (Wi-Fi 6) 5GHz: 4x4 : 4SS 2.4GHz: 2x2 : 2SS	802.11ax (Wi-Fi 6) 2x2 : 2SS
안테나 옵션	내부/외부	내장	내부/외부	내부/외부	내장	내부/외부	내장
Virtual BLE	✓	—	✓	✓	✓	—	—

주니퍼 커넥티드 시큐리티(Connected Security)

ZDNet은 2020년 FBI에 알려진 보안 공격에 대한 불만이 매년 69% 증가했다고 보고했습니다. 지금은 그 어느 때보다도 규모에 상관없이 모든 조직에서 유효한 보안 전략을 갖추는 것이 매우 중요합니다. 조직은 지속적으로 네트워크를 보호하기 위해 전체적인 그림을 바라봐야 합니다. 보호할 대상과 방어할 대상 모두에 관해 가시성의 큰 허점이 존재하면 안 됩니다. 지난 10년 동안 수많은 네트워크 보안 혁신이 이루어졌지만, 업계는 공격 성공 횟수를 줄이지 못했습니다. 이러한 상황은 전체 캠퍼스의 모든 연결 지점에 보안이 필요하다는 역설입니다. 이 방법을 통해 네트워크는 AI를 활용한 방어 조치를 성공적으로 구축하고 네트워크를 보다 성공적으로 신속하게 방어할 수 있습니다.

Juniper® 커넥티드 시큐리티(Connected Security)는 가시성, 인텔리전스, 정책 적용을 클라이언트부터 워크로드에 이르는 네트워크상의 모든 연결 지점으로 확장합니다. 조직은 캠퍼스의 네트워크에 존재하는 데이터와 사용자에 대한 인사이트를 얻기 위해 모든 연결 지점을 활용하고 해당 순간의 위험을 판별하기 위해 AI를 활용하며 위험을 완화하고 캠퍼스 보안의 균형을 맞추는 동시에 캠퍼스 리소스에 대한 액세스를 보장합니다.

데이터. 보안이 보호하는 두 가지 대상은, 데이터센터의 데이터와 에지에 있는 데이터에 대한 액세스입니다. 제로 트러스트의 다른 모든 요소는 데이터와 데이터 액세스를 보호하도록 설계되었지만, 데이터를 보호하려면 전송 중 암호화, 저장 중 암호화, 보안 연결이 필요합니다.

- Secure Vector Routing에서는 라우팅 벡터에 기반한 세그먼테이션을 지원하므로, 공격자가 전송 중인 데이터를 가로채기 훨씬 더 어렵습니다.
- Secure Connect는 어떤 소스에서든 네트워크에 연결할 때 제로 트러스트 네트워크 액세스(Zero Trust Network Access, ZTNA)를 제공하며, 프라이빗 터널에서 캡슐화합니다.
- 인텐트 기반 보안 제어는 Junos 자동화를 통해 퍼블릭 클라우드 환경에서 데이터 보안 정책 시행을 자동화합니다. 예를 들어, 새로 생성된 Amazon S3 버킷 내의 모든 데이터는 저장 중에 암호화되며, 규칙을 수동으로 구성하지 않고도 권한 부여된 데이터 액세스가 적용됩니다.

네트워크

네트워크에서 지점 사이를 이동하는 패킷은 합법적이어야 하고, 악성 프로그램이나 맬웨어를 포함하지 않아야 하며, 지점 A에서 지점 B로 이동할 권한이 있어야 합니다. 트래픽은 악의적 컨텐츠를 포함하는지 검사하거나 프로파일링해야 합니다.

차세대 방화벽(Next-Generation Firewall, NGFW)은 트래픽 검사에 적합한 솔루션으로 계속 진화해왔습니다. 서명은 일반적으로 패킷 헤더와 본문, 그리고 패킷 그룹에 적용되어 트래픽이 악의적인 컨텐츠인지를 판별하는 반면, AI는 알려지지 않은 파일, 시스템 동작, 트래픽 패턴을 빠르게 평가하여 공격 시도 중인지를 확인할 수 있습니다.

주니퍼 네트웍스 SRX 시리즈 서비스 게이트웨이는 네트워크 트래픽에 대한 가시성과 제어를 제공하고 AI 기반 보안 서비스, 새로운 맬웨어에 대한 위협 방지와 같은 서비스를 통해 알려진 위협과 알려지지 않은 위협을 저지할

- 추가적 보안 기능을 제공합니다. 주니퍼 ATP 클라우드는 머신러닝을 사용하여 알려지지 않은 파일을 빠르게 평가하고 런타임으로 파일 동작을 파악해 맬웨어 또는 그레이웨어인지를 판별합니다.
- 암호 해독 없이 가시성 및 제어 지원. ATP 클라우드는 트래픽 동작 및 사용된 인증서의 중요 구성 요소를 파악하여 IoT를 비롯한 연결 디바이스 및 암호화된 네트워크 트래픽에서의 위험도 평가합니다.

사람/사용자

캠퍼스의 모든 사용자가 내부 리소스와 인터넷에 연결된 리소스에 액세스합니다. 사용자는 잠재적 공격 벡터이며, 위험을 제한하려면 사용자 액세스를 제어하고 인증해야 합니다.

SRX 시리즈에서 사용자 기반 정책은 내부 또는 외부 리소스에 대한 세분화된 액세스 제어를 지원합니다. SRX 시리즈는 모든 종류의 아이덴티티 프로바이더와 통합 가능하며, 사용자가 어디를 가든 사용자를 따라 보안 액세스와 보안 정책을 적용합니다. 또한, ATP 클라우드는 사용자 계정이 위협을 받는지를 평가하고 적절한 보안 정책 및/또는 VLAN으로 동적으로 조정하며 필요한 경우 추가 인증 계층을 적용합니다.

워크로드

워크로드는 애플리케이션을 구성하는 구성 요소이며, 때로는 지속 시간이 상당히 짧기도 합니다. 데이터센터에서 핵심 자산의 최종 방어선을 구축하려면 애플리케이션에서 워크로드가 악용되지 않게 보호하고 다른 워크로드와 애플리케이션에서 해당 워크로드를 세그먼테이션하지 않도록 조치하는 것이 가장 바람직합니다.

- 클라우드 워크로드 보호는 제로데이 공격 발생 시 클라우드 또는 온프레미스 환경의 애플리케이션 워크로드를 자동으로 보호합니다. 이를 통해 생산 애플리케이션을 취약점 공격으로부터 항상 안전하게 보호하여 비즈니스 크리티컬 서비스의 연결 상태와 복원력을 유지할 수 있습니다. 수동 개입 없이도 마이크로세그먼테이션을 활용하여 개별 데이터베이스, 데이터 수집기, 모든 개별 리소스(예: 런타임 애플리케이션 보호)를 보호합니다.
- 주니퍼 네트웍스 cSRX 컨테이너 방화벽은 개별 애플리케이션을 오가는 트래픽을 세그먼테이션하고 제어하여 중앙 방화벽을 통해 애플리케이션을 보호합니다.

디바이스

캠퍼스에서 네트워크로 연결되는 디바이스는 사용자 디바이스, 임시 서버, IoT 디바이스를 포함하기 때문에 이러한 디바이스에 대한 가시성을 확보하기 어렵습니다. IoT 디바이스는 커넥티드 자판기에서 커피포트, 프린터에 이르기까지 캠퍼스 곳곳에 존재합니다. 사용자 기반 디바이스와 달리, IoT 디바이스는 엔드포인트 에이전트가 장착되지 않기 때문에 네트워크 액세스 및 현재 디바이스 상태에 대한 적절한 수준을 식별하기가 어렵습니다.

- ATP 클라우드는 주니퍼의 네트워크용 위협 인텔리전스 허브이며, 연결 디바이스에서 위험을 평가하고, IoT를 포함한 여러 디바이스 유형을 식별하고, 디바이스가 위협을 받을 때 적절한 조치를 오케스트레이션합니다.

ATP 클라우드에서 다음 기능은 제로 트러스트 네트워크 내에서 디바이스를 보호할 수 있습니다.

Mist AI 기반 위험 프로파일링

이 기능은 분산 액세스 네트워크 에지에 네트워크 보안 기능을 구현합니다. 이 기능을 통해 IT 팀은 심층적인 네트워크 가시성을 제공하고 네트워크 전체의 모든 연결 지점에서 정책 적용을 수행하여 인프라를 방어할 수 있습니다. 위협 인식 네트워크에 해당되는 캠퍼스 네트워크는 방어 체계에 능동적으로 참가하는 주체입니다.

Mist 보안 인텔리전스

ATP 클라우드 및 SRX 시리즈에서 감지하는 위협 경고는 사용자와 디바이스가 무선 네트워크에 연결할 때 보안 위험을 신속하게 평가하고 격리 또는 정책 적용과 같은 적절한 조치를 취합니다.

EX 시리즈의 SecIntel

ATP 클라우드는 EX 스위치로 디바이스 위협 정보를 전송합니다. 이를 통해 EX 스위치는 엔드포인트 에이전트가 없어도 감염된 디바이스를 차단하거나 격리하여 디바이스 제어를 제공할 수 있습니다.

분석 및 자동화

네트워크에서 발생하는 상황에 대한 가시성만이 보안의 전부가 아닙니다. 가시성을 확보하고 인텔리전스를 수집한 다음 이를 활용해 제로 트러스트 정책을 시행해야 네트워크 및 보안 팀 내에서 확장성을 보장하면서 추가적으로 위험을 줄일 수 있습니다. 조직은 다음을 통해 가시성을 확보할 수 있습니다.

- Security Director 클라우드. 하나의 사용자 인터페이스에서 온프레미스, 클라우드 기반 보안 제어, 클라우드에서 제공하는 보안 제어를 관리합니다. Security Director 클라우드를 사용하여 사용자, 디바이스, 애플리케이션이 위치를 변경할 때 가시성 또는 위협 방지 보호 조치를 위반하지 않도록 보안 정책이 이들을 따라 적용됩니다. 보안 정책을 한 번 작성한 후에는 위치가 변경되어도 모든 사용자, 디바이스, 애플리케이션으로 확대할 수 있습니다.
- Security Director 인사이트. 모든 타사 보안 도구에서 인텔리전스 및 감지 정보를 수집하는 Security Director의 이 기능을 통해 진행 중인 공격을 표시하고 Mitre ATT&CK 프레임워크에 감지 정보를 매핑합니다. 그러면 Security Director는 Ansible 자동화를 통해 또는 직접 적절한 조치를 정의하여 네트워크의 다른 도구에 오케스트레이션을 제공할 수 있습니다.
- Junos 자동화. 강력한 API 세트와 기타 네이티브 자동화 요소를 갖춘 주니퍼의 Junos 운영체제를 통해 자동화 기능을 강화합니다. 조직은 주니퍼 플랫폼 전반에서 거의 모든 프로세스/기능의 성능을 제어 및 구성하고 감사하는 기능을 확보합니다. Junos의 탁월한 성능에 프로그래밍 방식으로 액세스하는 이 기능을 활용하면 전체 아키텍처의 전반적인 상태를 보장하면서 고객의 변경 요청과 프로세스 티켓을 자동화하여 CapEx 및 OpEx 모두를 절감하는 작업을 간편하게 진행할 수 있습니다.

캠퍼스 네트워크 세그먼테이션

네트워크 아키텍트는 데이터와 자산을 보호하기 위해 마이크로 및 매크로 세그먼테이션과 같은 기술의 조합을 채택할 수 있습니다. 유니버설 EVPN-VXLAN 아키텍처는 캠퍼스와 데이터센터 전체로 확장하여 엔드포인트와 애플리케이션의 일관된 엔드투엔드 세그먼테이션을 수행할 수 있습니다. 또한 Layer 2 플러딩을 최소화하여 보안 위협을 줄이고 네트워크를 간소화합니다.

- 매크로 세그먼테이션은 공유 네트워크 디바이스와 공유된 링크 전체 내에서 네트워크에 대한 논리적 세그먼트 분할입니다. Layer 2에서 VLAN을 사용하고 Layer 3에서 가상 라우팅 및 포워딩(VRF)을 사용하여 이를 행할 수 있습니다. VRF는 서로 격리된 두 VRF 디바이스 간의 IP 트래픽을 유지하여 격리를 제공합니다.
- 마이크로 세그먼테이션은 위험을 줄이고 보안 요구 사항에 적응하여 중대한 네트워크 보호 문제를 해결합니다. 주니퍼는 내부 가상 네트워크 제어를 위한 액세스 제어 리스트(ACL) 또는 방화벽 필터를 기반으로 한 마이크로 세그먼테이션의 구현을 돕습니다.

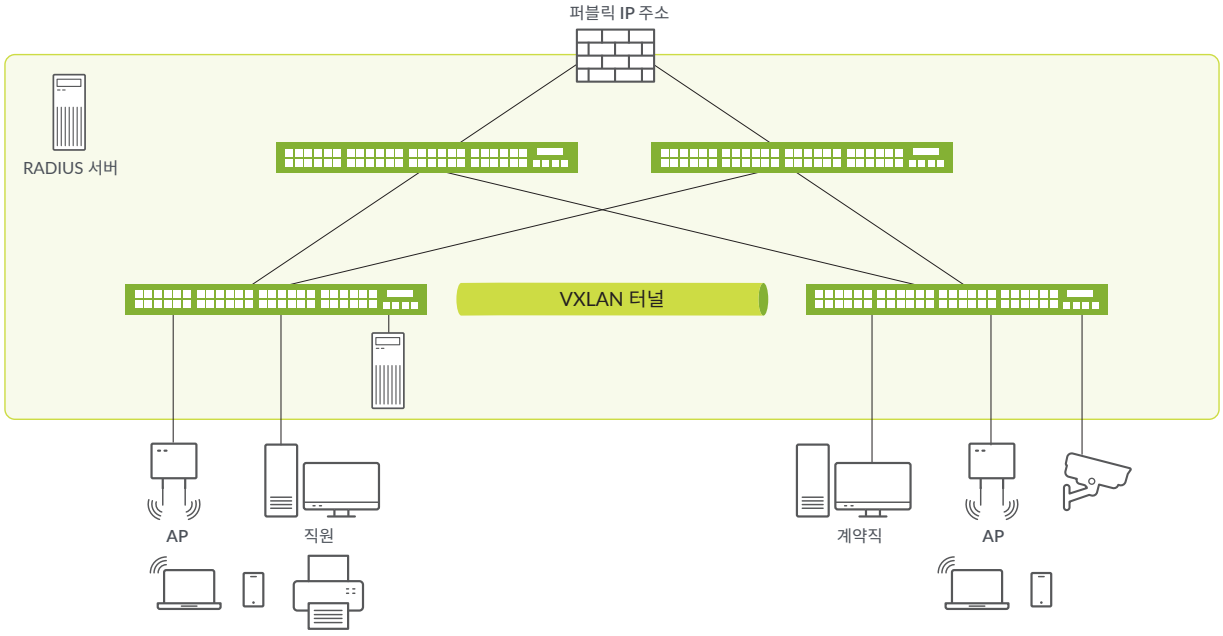

그림 7: 직원 또는 IoT 디바이스를 기반으로 한 네트워크 세그먼테이션

Junos OS: 하이 퍼포먼스 네트워크의 기반

Junos® 운영 체제는 주니퍼의 라우팅, 스위칭, 보안 디바이스 전체를 위한 공통의 언어를 제공합니다. 단일 Junos OS의 강력한 성능으로 고성능 네트워크의 복잡성을 줄임으로써 가용성이 증가하며 서비스를 더욱 빠르게 구축할 수 있으며 TCO가 낮아집니다. Junos OS의 일관적인 사용자 경험과 자동화된 툴세트로 계획 수립과 교육이 더욱 쉬워지고, 일상 운영 업무 효율성이 높아지며, 네트워크 전체에서 변경 사항을 더욱 빠르게 구현할 수 있습니다.

Junos OS가 다른 네트워크 운영 시스템과 다른 점이 있다면, 바로 구축된 방식입니다. Junos OS는 단일 소프트웨어 릴리스 트랙과 단일 모듈식 아키텍처로 제공되는 단일 운영 시스템입니다. 대표적인 장점은 다음과 같습니다.

- 모든 유형 및 크기의 플랫폼을 위한 단일 운영 체제라 네트워크 및 보안 인프라를 계획, 구축, 운영하는 데 드는 시간과 노력이 줄어듭니다.
- 단일 릴리스 트랙은 오랜 시간에 걸쳐 검증된 일관된 릴리스를 통해 새로운 기능을 안정적으로 제공하여 소프트웨어에 대한 변화하는 요구 사항을 충족합니다.
- 단일 모듈형 아키텍처가 자동화와 파트너 혁신을 위한 매우 가용성이 높고, 안전하며, 확장성이 뛰어난 오픈 소프트웨어를 제공합니다.

Junos Telemetry

운영 상태 통계를 수집하는 기존 데이터 모델은 네트워크 확장 및 효율의 한계에 도달했습니다. Junos Telemetry Interface는 푸시 모델을 통해 데이터를 비동기적으로 제공하여 폴링(polling) 현상을 제거함으로써 이러한 한계를 극복합니다. 결과적으로 Junos Telemetry Interface는 확장성이 매우 뛰어나며 네트워크에서 수천 개의 개체를 모니터링할 수 있습니다.

Junos Telemetry Interface를 통해 물리적 인터페이스 및 방화벽 필터와 같은 다양한 시스템 리소스에 대한 데이터를 수집하고 내보내기 위한 센서를 프로비저닝할 수 있습니다. 다음과 같은 두 가지 데이터 모델이 지원됩니다.

- 주니퍼 네트웍스에서 정의한 확장 가능한 오픈 데이터 모델이 지원됩니다. 이 모델은 분산형 아키텍처를 지원하므로 쉽게 확장됩니다.
- OpenConfig 데이터 모델이 데이터를 유니버설 키/값 형식의 Google 프로토콜 버퍼(gpb) 구조화 메시지로 생성합니다. gRPC 원격 프로시저 호출은 TCP를 기반으로 하고 SSL 암호화를 지원하므로 안전하고 신뢰할 수 있는 것으로 간주됩니다.

결론

주니퍼의 AI 기반 캠퍼스는 미래의 클라우드 환경에 대비하여 유연하고 표준을 기반으로 하는 현대적인 아키텍처를 제공하도록 설계되었습니다. 오늘날의 까다로운 요구사항을 충족하면서도 신뢰성, 보안, 민첩성을 유지합니다. 공통 빌딩 블록, 사전 패키지 방식의 자동화 워크플로우, 맞춤형 자동화 툴킷으로 데이터센터를 넘어 캠퍼스 환경까지 예측적 분석의 장점을 확장할 수 있습니다.

추가 리소스

- 캠퍼스 디자인 센터
- EX 시리즈 제품군 웹페이지
- 주니퍼 Mist 클라우드 서비스
- 주니퍼 커넥티드 시큐리티(Connected Security)
- 라이브 데모: Wired and Wireless Wednesday
- 라이브 데모: AI 기반의 엔터프라이즈
- 주니퍼 커넥티드 시큐리티(Connected Security)

주니퍼 네트웍스에 대하여

주니퍼 네트웍스는 네트워크 운영을 대폭 간소화하고 최종 사용자에게 탁월한 경험을 제공하는 데 주력합니다. 주니퍼 솔루션은 업계 최고 수준의 인사이트, 자동화, 보안, AI를 통해 실질적인 비즈니스 성과를 도출합니다. 주니퍼는 전 세계 고객이 견고한 연결을 통해 협력을 강화하고 웰빙, 지속 가능성, 평등에 대한 가장 어려운 도전 과제를 해결하도록 지원합니다.

JUNIPER NETWORKS | Driven by Experience™

한국주니퍼네트웍스
서울 강남구 테헤란로 142
아크플레이스 19층
우편번호 06236
www.kr.juniper.net
전화: 02-3483-3400
팩스: 02-3483-3488

본사
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
전화: 888.JUNIPER (888.586.4737)
또는 +1.408.745.2000 +1.408.745.2100
www.juniper.net

2000752-006-KO 2022년 7월