솔루션 개요

다이내믹 세그멘테이션

글로벌 스케일의 Edge-to-Cloud 제로 트러스트 및 SASE 보안을 위한 ID 기반 액세스 제어

IoT 디바이스의 확산과 하이브리드 업무 형태의 도입으로 네트워크가 공간적으로 분산되고 있으며, 이로 인해 새로운 가시성 및 보안 과제가 생겨나고 있습니다.

또한 조직들이 비즈니스 효율을 높이기 위한 디지털 트랜스포메이션을 가속화하면서 IT 부서는 Edge-to-Cloud로부터 제로 트러스트 및 SASE 보안 프레임워크를 구현해야 하는 과제를 마주하고 있습니다.

아루바 다이내믹 세그멘테이션(Aruba Dynamic Segmentation)은 Aruba ESP(Edge Services Platform)에 구축된 Edge-to-Cloud 보안의 핵심 요소이며, ID와 관련 액세스 권한에 따라 트래픽을 세분화하여 IT 자원에 대한 최소 권한 액세스를 구축하는 것을 근간으로 합니다. 이는 제로 트러스트와 SASE 프레임워크의 기본 개념으로써, 사용자 또는 IoT 기기와 같은 엔드포인트 클라이언트의 연결 위치나 연결 방식이 아니라 역할과 정책을 기반으로 신뢰 여부를 결정합니다.

다이내믹 세그멘테이션은 중앙화된 정책 정의를 통해 유선, 무선 및 WAN 네트워크 모두에 대한 역할 기반 액세스 및 정책 실행을 통합함으로써 사용자와 디바이스가 각각의 역할과 관련이 있는 대상과만 통신하도록 하여 트래픽을 보호하고 분리시켜 줍니다..

ID 기반 세그멘테이션은 제로 트러스트 및 SASE의 핵심

사용자 또는 디바이스의 연결 방식과 위치에 따라 액세스 제어를 결정할 경우 네트워크를 일일이 직접 구성해야 하고 이에 따른 오류 위험도 높아져서 보안에 큰 갭이 발생한다는 점은 잘 알려진 사실입니다. 제로 트러스트가 처음 소개된 것은 이미 10년 전입니다. 사용자 또는 클라이언트의 ID와 역할에 따라 정의된 자원에 대한 제한된 액세스를 바탕으로 IT 액세스 정책을 정의하고 실행할 수 있는 보안 아키텍처를 조직에 제공함으로써 이러한 문제를 해결하도록 지원하는 것이 목적이었습니다. 예컨대, 프린터는 직원들의 급여 정보가 저장된 서버에 접속하도록 허용되면 안 됩니다.

주요 이점

- **네트워크 운영 간소화 –** SSID, ACL, 서브넷, 유선 포트 구성의 번거로움을 줄여서 시간을 절약하고 VLAN 스프롤을 제거합니다.
- **보안 및 가시성 향상 –** 중앙화된 정책 정의 및 역할 기반 액세스를 통해 사용자와 디바이스가 각자의 역할과 관련된 대상과만 통신하도록 합니다.
- **클라우드 기반 관리 및 자동화 –** 정책 정의 및 네트워크 구성을 위한 인텐트 기반의 사용하기 쉬운 워크플로우를 활용합니다.
- **글로벌 스케일 및 상호운용성 –** 타사 인프라와의 상호운용성을 보장하여 글로벌 스케일을 지원합니다.
- **성능 및 효율성 –** 자동으로 업데이트되고 지속적으로 실행되는 정책으로 IT 오버헤드를 제거합니다.

제로 트러스트 네트워크는 연결 방법과 관계 없이 액세스 제어 정책에 따라 트래픽을 분할합니다.

이미 오래전부터 SASE(Secure Access Service Edge)는 클라우드 기반 워크로드의 중요성을 확인하고 제로 트러스트를 SD-WAN과 클라우드 제공 보안 서비스를 포함하도록 확장했습니다. 제로 트러스트와 SASE 프레임워크는 조직을 보호하기 위해 네트워크에 내장되는 ID 기반 세그멘테이션을 이용하는 안전한 네트워크 기초를 위한 청사진을 제공합니다.

다이내믹 세그멘테이션의 원리

아루바는 제로 트러스트 및 **SASE**에 의해 정의된 액세스 제어 방식을 지원하는 네트워크 분야의 리더입니다. 아루바의 다이내믹 세그멘테이션은 **ID**, 정책 및 네트워크 인프라를 활용하여 **IT** 부서의 중요 자산 보호를 간소화하고 자동화하며, 다음과 같은 기능으로 구성됩니다.

디바이스 검색 및 프로파일링

네트워크로 유입되는 **IoT** 디바이스 또는 클라이언트의 수가 지속적으로 증가함에 따라, **IT** 부서가 네트워크에 접속하는 모든 대상을 관찰하고 추적하기는 어렵습니다. 그 결과 조직 전체를 위험에 빠뜨릴 수도 있는 운영 및 보안 상의 사각지대가 발생할 수 있습니다. 아루바의 다이내믹 세그멘테이션의 핵심 요소는 아루바 센트럴**(Aruba Central)**의 **AI** 기반 클라이언트 인사이트**(Client Insights)**입니다. 이 솔루션은 아루바 네트워크 인프라의 텔레메트리와 머신러닝을 이용하여 네트워크에 접속하는 모든 유형의 클라이언트를 자동으로 프로파일링하며, 그 유효성은 95%가 넘습니다.

아루바는 타사 네트워크 구축에서 사용할 수 있는 자동화된 AI 기반 클라이언트 프로파일링도 옵션으로 제공합니다. 자세히 보기.

ID 및 인증

802.1x 또는 기타 기술을 통해 사용자 또는 디바이스의 **ID** 인증이 완료되고 나면 이제 **IT** 부서는 적합한 역할 및 액세스 권한을 정의할 수 있으며, 이러한 권한은 자동으로 적용됩니다. 이를 통해 사용자 또는 디바이스의 네트워크 상태 또는 위치와 관계 없이 해당 **ID**에 액세스 권한이 부여됩니다.

역할 기반 정책

역할이란 사용자 또는 클라이언트의 **ID**가 확인된 후에 할당되는 권한으로 구성된 논리적 그룹을 말합니다. 권한에는 액세스 가능한 애플리케이션들의 목록, 접근 가능한 서비스 및 기타 클라이언트, 심지어 특정 사용자가 네트워크에 접속할 수 있는 주당 일수까지도 포함될 수 있습니다. 역할과 실행은 제로 트러스트와 **SASE**에 대한 조직의 전반적 관점과 **GDPR**과 같은 컴플라이언스 요구사항에 의해 결정됩니다.

자동화된 실행

역할이 정의되고 나면 실행은 네트워크 인프라에 의해 액세스 권한을 이용한 트래픽의 적합한 라우팅 및 세분화를 통해 진행됩니다. 아래 설명된 것처럼 아루바 다이내믹 세그멘테이션은 개별적으로 또는 함께 사용 가능한 여러 가지 실행 모델을 선택할 수 있습니다.

다이내믹 세그멘테이션 모델

아루바는 조직의 전반적인 네트워크 아키텍처에 따라 두 가지 다이내믹 세그멘테이션 수행 방식을 지원합니다.

분산된 다이내믹 세그멘테이션

조직이 자사의 네트워크를 현대화하기 위해 오버레이 및 **EVPN/VXLAN** 등의 널리 이용되는 프로토콜을 채택하면서 이러한 오버레이를 활용하여 다이내믹 세그멘테이션을 통해 보안 및 스케일을 향상시킬 수 있는 기회가 생겼습니다. 아루바 센트럴 넷컨덕터(Aruba Central NetConductor)를 도입하면 클라우드를 통해 다이내믹 세그멘테이션을 관리할 수 있으며, 중앙에서 액세스 정책을 정의 및 적용하고 아루바 스위치와 게이트웨이를 통해 분산된 방식으로 정책을 인라인으로 실행할 수 있습니다(그림 1 참조).

비즈니스 인텐트 기반 워크플로우

Central NetConductor를 통해 **IT** 부서는 fabric wizard를 이용하여 기반 네트워크의 복잡성을 추상화하고 정책 정의를 단순화하며 동시에 네트워크 정의 및 구성을 자동화할 수 있습니다. 푸시버튼 자동화와 결합된 직관적이고 시각적인 워크플로우는 **CLI** 기반 프로그래밍, 테이블 스프레드시트 라우팅, **ACL** 수동 구성의 번거로움을 없애줍니다.

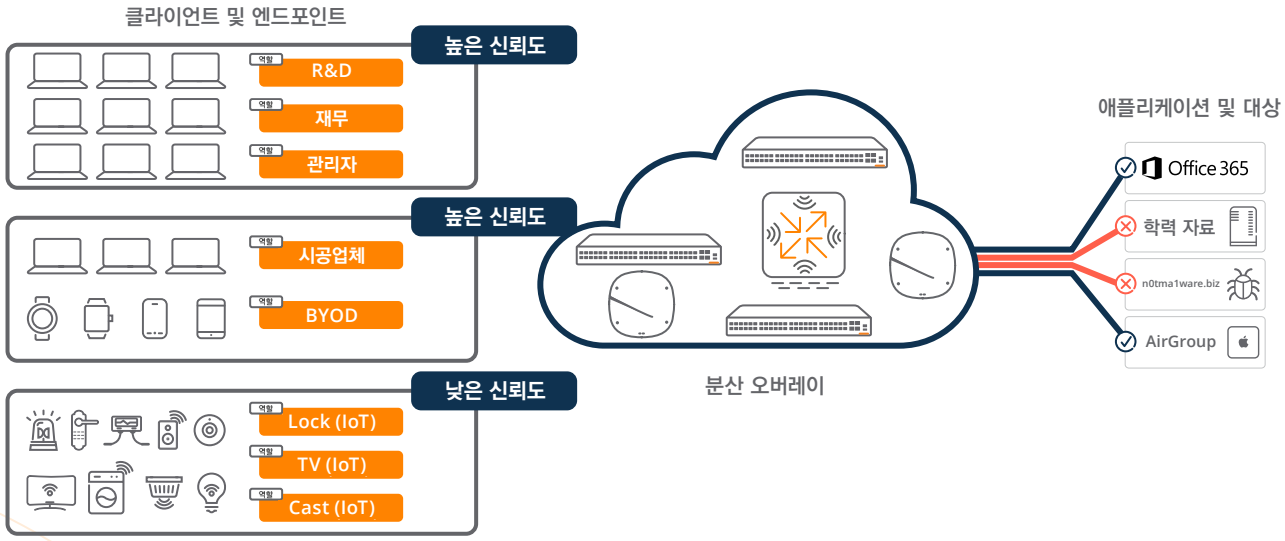

그림 1: 분산 오버레이 패브릭을 지원하는 다이내믹 세그멘테이션

인라인 정책 실행을 위한 그룹 정책 식별자(GPID)

Central NetConductor의 정책 관리자는 역할과 관련 액세스 정책을 정의합니다. 이 정책들은 그룹 정책 식별자**(Group Policy Identifier)**로 표현되어 사용자 또는 클라이언트의 역할과 액세스 권한을 반영하며 네트워크가 트래픽 자체를 통해 액세스 제어 정보를 전달할 수 있게 합니다. 그룹 정책 식별자는 패킷 헤더에 내장되고 아루바 **CX** 스위치 및 게이트웨이를 통해 인라인으로 분석됩니다(그림 2 참조). 클라이언트의 보안 상태가 변경되는 경우 해당 클라이언트의 역할은 액세스를 제한하도록 자동으로 변경되며, 이후 이러한 역할 변경은 전체 네트워크에 적용됩니다.

그룹 정책 식별자를 통해 분산된 다이내믹 세그멘테이션은 정책 실행 규모를 크게 개선할 수 있으며, 동시에 지연시간과 트래픽 오버헤드는 줄일 수 있습니다. 그룹 정책 식별자는 업계 표준을 기반으로 하며 타사 네트워크와의 양방향 통합을 지원합니다.

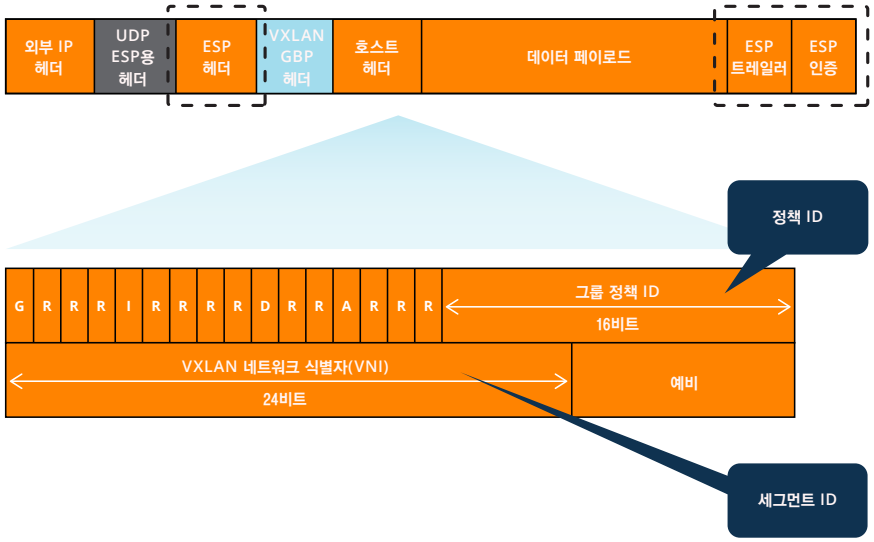

그림 2: 네트워크 트래픽을 통해 액세스 제어 정보를 전달하여 인라인 정책을 실행하는 그룹 정책 식별자

CENTRAL NETCONDUCTOR – 솔루션 구성 요소

그림 **3**에서처럼 **Central NetConductor**를 구성하는 요소들은 분산된 다이내믹 세그멘테이션을 구현하여 확장성과 성능을 높입니다.

그림 3: 분산된 다이내믹 세그멘테이션을 위한 Central Netconductor 의 솔루션 구성 요소

- **클라이언트 인사이트(Client Insights)** – 최초로 클라우드 네이티브 관리 플랫폼에 내장된 에이전트리스 방식의 클라이언트 가시성 및 핑거프린팅 기술로서 네트워크의 사각지대를 제거해줍니다. **AI**를 기반으로 하는 클라이언트 인사이트는 인프라 텔레메트리와 머신러닝 기반 분류 모델을 활용하여 유무선 인프라 전체에서 다양한 클라이언트를 추적하고 식별하고 정확하게 프로파일링합니다.
- **클라우드 인증(Cloud Auth)** – MAC 어드레스 기반 인증 또는 Google Workspace나 Azure Active Directory와 같은 공동 클라우드 ID 스토어를 통해 적합한 네트워크 액세스 레벨을 자동으로 할당함으로써 최종 사용자와 클라이언트 디바이스의 원활한 온보딩을 지원합니다.
- **정책 관리자** – 사용자 및 디바이스 그룹을 정의하고 해당 물리 네트워크에 대한 관련 액세스 실행 규칙을 생성합니다(그림 4 참조).

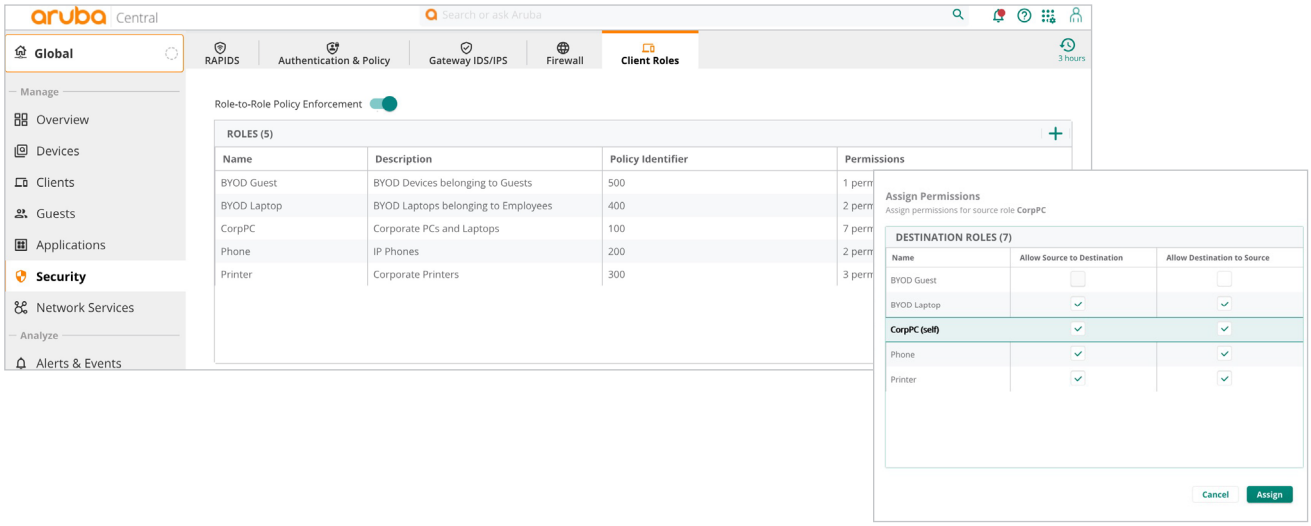

그림 4: 글로벌 정책 정의를 위한 직관적이고 시각적인 인터페이스

- **Fabric Wizard** – 직관적이고 시각적인 사용자 인터페이스를 통해 오버레이 생성을 단순화함으로써 가상 컴포넌트를 정의하고 구성 인스트럭션을 생성하여 스위치 및 게이트웨이에 푸시하는 작업을 훨씬 수월하게 해줍니다(그림 5 참조).

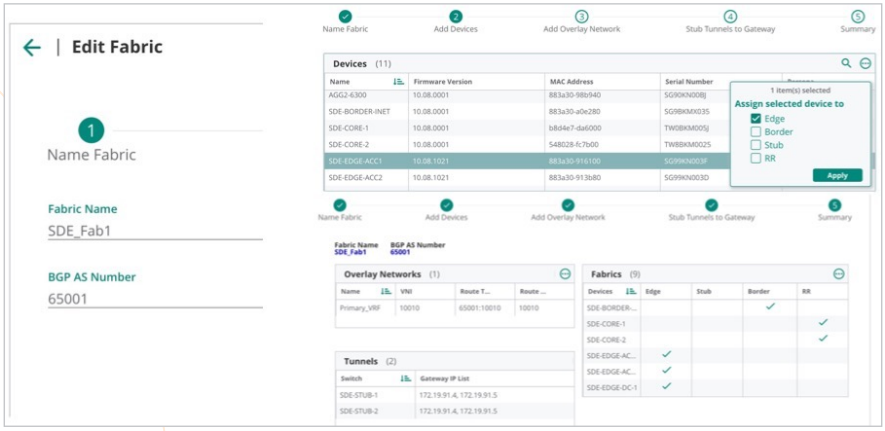

그림 5: 구성 간소화 및 패브릭 오버레이 구축 자동화를 위한 사용하기 쉽고 시각적인 워크플로우

- **그룹 정책 식별자(GPID)** – 트래픽을 통해 클라이언트 정책 정보를 전달하고 인라인 정책을 실행하여 구성 및 보안 오버헤드를 줄이고 이동성과 확장성을 개선합니다.
- **패브릭 지원 아루바 스위치 및 게이트웨이** – 그룹 정책 식별자에 정의된 라우팅 인스트럭션 및 액세스 권한에 따라 구성 및 실행을 지원합니다.

참고: 정책 오케스트레이션을 위해 **Central NetConductor**의 정책 관리자를 이용하는 네트워크는 클라우드 인증**(Cloud Auth)** 또는 클리어패스**(ClearPass)**를 통해 인증 및 역할 할당을 수행할 수 있습니다.

중앙화된 다이내믹 세그멘테이션

중앙화된 다이내믹 세그멘테이션은 여러 세대에 걸쳐 가장 널리 사용된 **IT** 액세스 제어 방식이었습니다. 이 모델은 액세스 포인트와 아루바 게이트웨이(또는 컨트롤러 기반 환경의 모빌리티 컨트롤러)를 연결하는 **GRE** 터널들로 구성된 중앙화된 오버레이를 이용하여 트래픽을 지속적으로 보호하고 분리합니다. 게이트웨이는 소스나 대상 클라이언트 또는 애플리케이션의 역할에 관한 정보를 보유하는 인그레이스 정책 실행 포인트의 역할을 합니다(그림 6 참조).

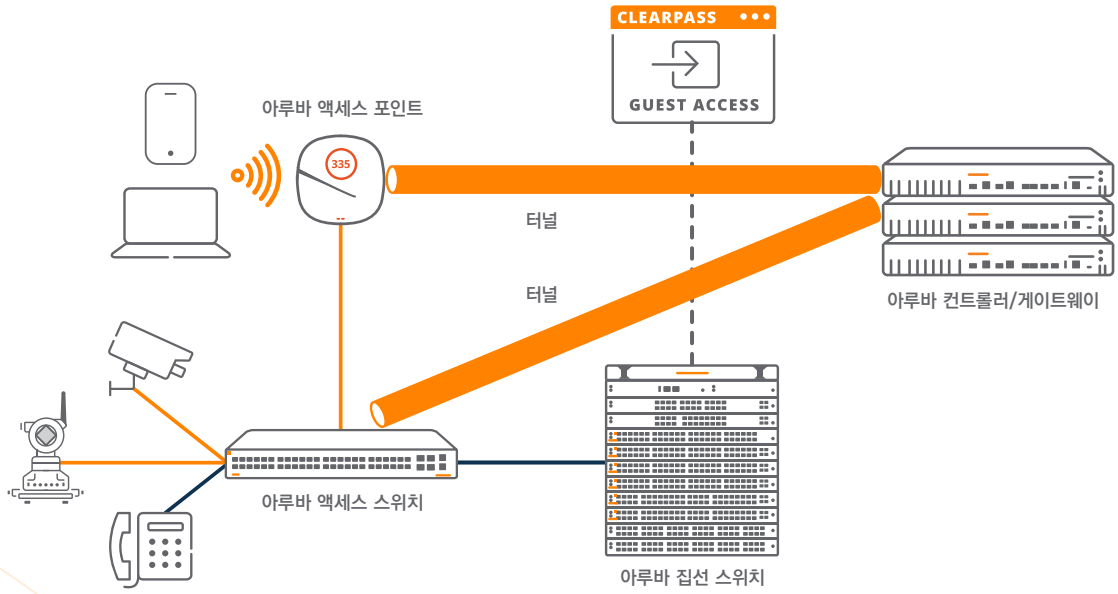

그림 6: 중앙화된 다이내믹 세그멘테이션

정책 정의

중앙화된 정책 정의는 중앙화된 실행 모델을 위한 **ClearPass** 또는 **NetConductor** 정책 관리자를 통해 얻을 수 있습니다.

ClearPass는 네트워크 전체에서 사용자를 추적하고 유무선 및 **VPN** 접속에 일률적으로 적용되는 인증, 권한 부여 및 중앙화된 정책 정의를 제공합니다. 사용자가 알려지지 않은 디바이스로 변경되거나 보호되지 않는 네트워크 상에 있는 경우 해당 정책이 부여된 권한을 자동으로 변경합니다.

ClearPass는 표준 기반 **802.1X** 실행 및 기타 보안 인증 방식을 지원합니다. ClearPass는 다양한 인증 솔루션과 통합하여 멀티팩터 인증을 지원하고 전체 네트워크의 주요 포인트에서 재인증을 강제할 수 있게 해줍니다.

또한, **ClearPass**는 방화벽, **UEM** 및 기타 솔루션을 이용한 통합 보안 커버리지 및 대응을 위해 **150**개 이상 파트너와 통합된 **Aruba 360 Security Exchange Program**을 지원합니다.

자세히 보기.

정책 실행 방화벽(PEF)

IP 기반 **VLAN**을 활용하여 통제하는 기존의 방화벽은 사용자나 디바이스가 네트워크에 입장한 다음에야 비로소 활성화됩니다. 이는 진화한 공격에 당할 여지를 남깁니다. 아루바의 스테이트풀 **(stateful)** 레이어 **7** 방화벽 **PEF**는 **ID**, 트래픽 속성 및 기타 컨텍스트를 이용하여 최초 접속 시 액세스 권한을 중앙화된 방식으로 실행합니다. **PEF**를 통한 트래픽 검사는 사용자, 디바이스, 애플리케이션 및 위치에 관한 세분화된 컨텍스트를 제공합니다. **PEF**는 아루바 게이트웨이(또는 컨트롤러 기반 환경의 모빌리티 컨트롤러)에서 정책 실행을 지원하는 기반 네트워크 기술의 역할을 수행합니다.

다이내믹 세그멘테이션 모델 선택

EVPN/VXLAN을 기반으로 하는 지능형 오버레이 패브릭을 통해 **VLAN** 기반 아키텍처를 확장함으로써, 사일로화된 구성 및 보안 이슈를 해결하여 복잡한 글로벌 분산 네트워크에 대한 정책을 수월하게 실행할 수 있습니다(그림 7 참조). 널리 채택된 프로토콜을 이용할 경우 기존 인프라를 전부 대체하지 않고도 타사 네트워크와의 통합을 위한 멀티벤더 상호운용성을 구현할 수 있습니다.

중앙화된 오버레이 패브릭과 분산된 오버레이 패브릭의 두 실행 모델은 단일 환경에서 공존할 수 있기 때문에 고객은 이 중 하나를 사용할 수도 있고 둘 다 사용할 수도 있습니다. 중앙화된 방식을 이용 중인 조직들은 액세스 디바이스에 의해 실행이 이루어지는 분산 방식을 자사가 원하는 속도로 유연하게 채택할 수 있습니다.

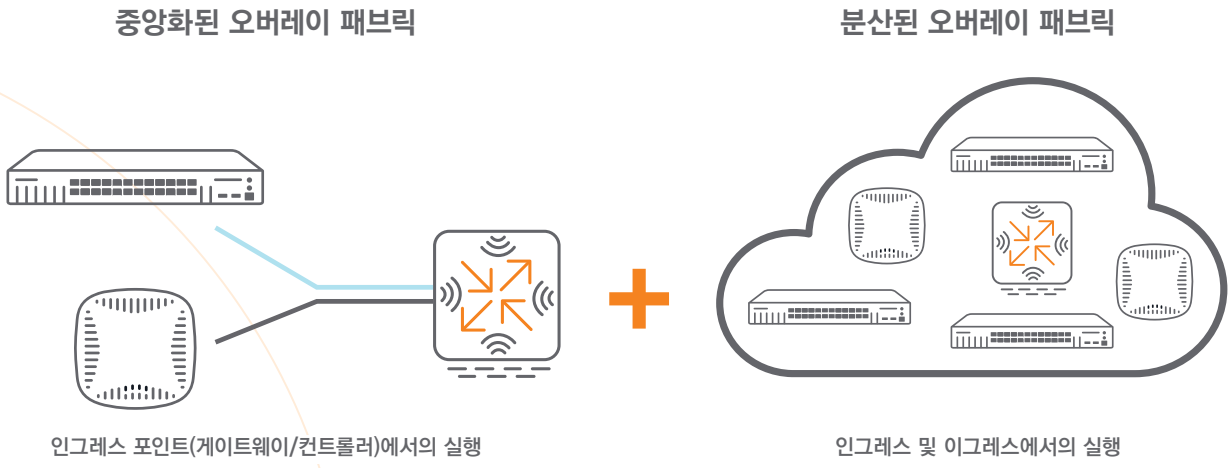

그림 7: 인그레스 및 이그레스 포인트 모두에서 정책 실행을 위한 분산된 오버레이 패브릭을 활용하여 향상된 스케일과 성능을 지원하는 분산된 다이내믹 세그멘테이션

요약

조직들이 자사 네트워크에 대한 강력한 보안을 모색함에 따라 **IoT, BYOD** 클라이언트 및 사용자 트래픽에 대한 세그먼트화의 중요성이 더욱 커지고 있습니다. 아루바의 혁신적인 다이내믹 세그멘테이션 솔루션은 **Edge-to-Cloud**를 위한 통합 정책 및 실행 기능을 동적으로 적용함으로써 **IT** 부서가 자사 환경의 보안을 강화하기 위한 이상적인 모델을 선택할 수 있도록 지원합니다. 다이내믹 세그멘테이션이 실행하는 세분화된 역할 기반 액세스 권한을 통해 공격이 탐지되었을 때 엔드포인트 클라이언트를 자동으로 차단 또는 격리함으로써 침해된 사용자와 클라이언트가 공격에 이용되는 것을 손쉽게 막을 수 있습니다.

또한 클라우드 또는 온프레미스로 사용 가능한 중앙화된 모델과 분산된 모델 중에서 선택할 수 있도록 하여 전체 네트워크 토폴로지에 걸쳐 적합한 액세스 및 보안 정책이 자동으로 업데이트되고 지속적으로 실행될 수 있도록 보장합니다. 아루바 다이내믹 세그멘테이션은 네트워크의 규모 및 복잡성과 관계 없이 글로벌 스케일의 제로 트러스트 및 **SASE** 보안 채택을 간소화하는 독보적 솔루션입니다.

SO_DynamicSegmentation_030322 a00058593enw