



# HPE Aruba Networking Dynamic Segmentation

글로벌 규모의 엣지 투 클라우드에서 제로 트러스트 보안과  
SASE 를 실현하는 ID 기반 접근제어



IoT( 사물 인터넷 ) 장치가 급증하고 업무 환경이 하이브리드화되면서 전체 상태를 파악하고 보안 유지가 어려운 복잡하고 지리적으로 분산된 네트워크가 등장했습니다. 또한 비즈니스를 효율적으로 운영하기 위해 조직에서 신속하게 디지털 트랜스포메이션을 진행하게 되자 IT 팀은 엣지 투 클라우드에서 제로 트러스트 보안과 SASE( 보안 액세스 서비스 엣지 ) 프레임워크를 구현하기 더 어려워지게 되었습니다.

HPE Aruba Networking Dynamic Segmentation 은 HPE Aruba Networking 의 AI 기반 보안 우선 네트워킹에 내장된 엣지 투 클라우드 보안의 중요한 요소입니다. 그 기반은 ID 와 그에 따른 액세스 권한에 따라 트래픽을 세분화하여 IT 리소스에 대한 액세스 권한을 최소한으로 설정하는 것입니다. 이는 사용자의 장치가 연결되는 위치와 방법이 아니라 역할과 정책을 기반으로 신뢰하는 제로 트러스트와 SASE 프레임워크 모두의 기본 개념입니다.

HPE Aruba Networking Dynamic Segmentation 은 중앙 집중식 정책 정의를 통해 유무선과 WAN 네트워크 전반에 걸쳐 역할 기반 액세스와 정책 시행을 통합하여 사용자와 장치가 그 역할과 일치하는 대상과만 통신하게 하여 트래픽을 안전하고 분리된 상태로 유지합니다.

#### 주요 이점

- 네트워크 작동 간소화 - SSID, ACL, 서브넷, 유선 포트에 필요한 구성을 줄여 시간을 절약하고 VLAN 스프롤 제거
- 보안 강화 및 전체 상황 파악 용이 - 중앙 집중식 정책 정의와 역할 기반 액세스를 통해 사용자와 장치가 그 임무와 관련된 대상과만 통신하도록 허용
- 클라우드 기반 관리 및 자동화 - 정책 정의와 네트워크 구성에 인텐트 기반의 사용하기 쉬운 워크플로 활용
- 글로벌 규모 및 상호 운용성 - 타사 인프라와의 상호 운용성을 활용하여 글로벌 규모 지원
- 성능 및 효율 - 정책을 자동으로 업데이트하고 지속적으로 적용하여 IT 오버헤드 완화

## ID 기반 세분화가 제로 트러스트와 SASE 의 열쇠

사용자 또는 장치가 연결되는 방식과 위치에 따라 접근제어가 결정되면 수작업이 많아지고 오류가 발생하기 쉬운 네트워크가 구성되는 것에 더해 보안 격차 또한 커진다는 점은 오래 전부터 알려진 사실입니다. 제로 트러스트는 조직이 사용자 또는 클라이언트의 ID 와 역할에 따라 리소스에 대한 액세스를 제한하는 IT 액세스 정책을 정의하고 시행할 수 있는 보안 아키텍처를 제공하여 이 문제를 해결할 수 있도록 10 년 전에 도입되었습니다. 예를 들어, 프린터는 급여 정보가 있는 서버에 액세스할 수 없어야 합니다.

제로 트러스트 네트워크는 연결 방법에 관계없이 접근제어 정책에 기반하여 트래픽을 세분화합니다. 몇 년 전 SASE 아키텍처에서 클라우드 기반 워크로드가 중요하다는 점을 인식하여 제로 트러스트를 확장하여 SD-WAN 과 클라우드 제공 보안 서비스를 포함시켰습니다. 제로 트러스트와 SASE 프레임워크는 네트워크에 내장된 ID 기반 세분화를 활용하여 조직을 보호하는 보안 네트워크 기반의 청사진을 제시합니다.

# HPE Aruba Networking Dynamic Segmentation 의 원칙

Hewlett Packard Enterprise 는 제로 트러스트와 SASE 로 정의되는 접근제어 메커니즘을 지원하는 네트워크 제공 시장의 리더입니다 . HPE Aruba Networking Dynamic Segmentation 은 ID, 정책, 네트워크 인프라를 활용하여 IT 팀이 중요 자산을 보호하는 방법을 간소화하고 자동화하며 다음과 같은 기능으로 구성됩니다 .

## 장치 검색 및 프로파일링

점점 더 많은 IoT 장치가 네트워크에 연결됨에 따라 IT 부서가 이러한 모든 장치와 그 핑거프린트를 확인하는 데는 한계가 있습니다 . 그에 따라 작동과 보안 양면에서 사각지대가 생기며 이로 인해 조직 전반에서 문제가 발생할 수 있습니다 . HPE Aruba Networking Dynamic Segmentation 의 핵심 요소는 HPE Aruba Networking Central 의 일부인 AI 기반 HPE Aruba Networking Client Insights 입니다 . 이 솔루션은 HPE Aruba Networking 네트워크 인프라와 기계 학습의 원격 측정을 사용하여 IoT 장치 등 네트워크에 연결되는 다양한 클라이언트를 자동으로 프로파일링합니다 .

또한 HPE 는 타사 네트워크에서 작동하는 자동화된 AI 기반 클라이언트 프로파일링 옵션을 제공합니다 . 오늘날의 IoT 기반 네트워크 전체 상태를 파악하는 방법과 인사이트를 더 자세히 알아보시기 바랍니다 .

## ID 및 인증

사용자 또는 장치가 802.1X 또는 기타 기술이 활용되는 인증 과정을 통해 확인되면 IT 팀은 적합한 역할과 액세스 권한을 정의할 수 있고 , 이는 자동으로 적용됩니다 . 네트워크 연결 또는 사용자나 장치의 위치와 관계없이 ID 에 액세스 권한을 연결합니다 .

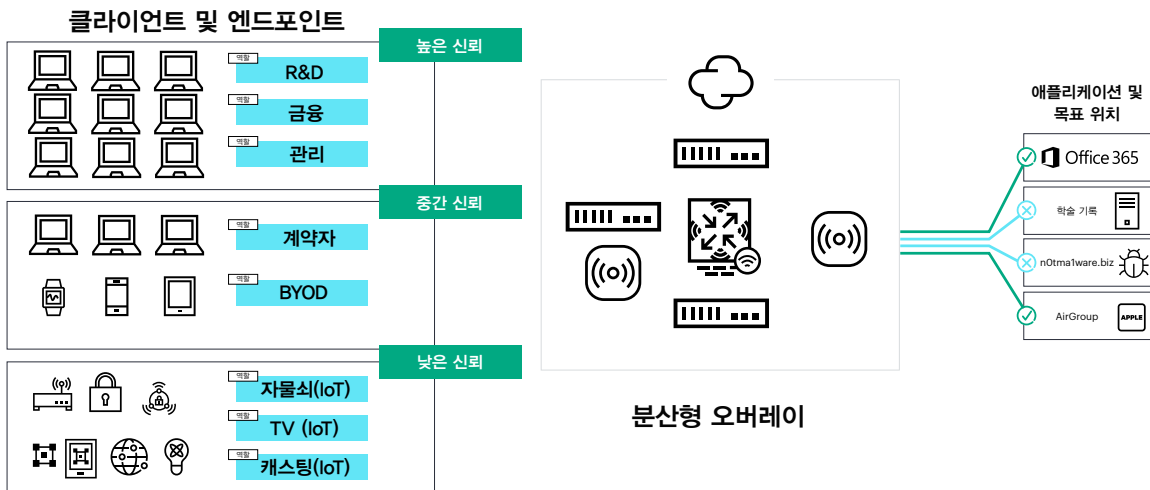


그림 1. HPE Aruba Networking Dynamic Segmentation 과 분산 오버레이 패브릭

## 역할 기반 정책

역할은 사용자 또는 클라이언트의 ID 가 설정될 때 한 번 할당되는 권한의 논리적 그룹입니다 . 권한에는 액세스 가능한 애플리케이션 목록, 접근 가능한 서비스와 기타 클라이언트 , 특정 사용자가 네트워크에 연결 가능한 요일 등이 포함될 수 있습니다 . 역할과 시행은 제로 트러스트와 SASE 에 대한 조직의 전체적인 접근 방식과 GDPR 과 같이 준수해야 하는 규제 요건에 의해 결정됩니다 .

## 시행 자동화

역할이 정의되면 네트워크 인프라가 액세스 권리를 사용하여 적절한 트래픽을 경로 설정하고 세분화하여 시행합니다 . HPE Aruba Networking Dynamic Segmentation 에서 개별적으로 또는 함께 사용할 수 있는 시행 모델을 선택할 수 있습니다 .

# HPE Aruba Networking Dynamic Segmentation 모델

HPE Aruba Networking 은 조직의 전체적인 네트워크 아키텍처에 따라 2 가지 방법으로 동적 세분화를 지원합니다 .

## 분산형 동적 세분화

조직이 오버레이와 EVPN/VXLAN 과 같이 널리 사용되는 프로토콜을 도입하여 네트워크를 고도화하게 되면 HPE Aruba Networking Dynamic Segmentation 을 통해 보호를 확대하고 규모를 확장하기 위해 오버레이를 활용할 기회가 열립니다 . HPE Aruba Networking Central NetConductor 를 도입하면 액세스 정책을 중앙에서 정의하고 전파하며 HPE Aruba Networking 스위치와 게이트웨이로 이러한 정책을 인라인의 분산된 방식으로 시행하는 기능으로 동적 세분화를 클라우드를 통해 관리할 수 있습니다 ( 그림 1).

## 비즈니스 인텐트 기반 워크플로

IT 팀은 HPE Aruba Networking Central NetConductor 를 통해 패브릭 마법사를 사용하여 기본 네트워크의 복잡성을 줄이고 정책 정의를 간소화하는 동시에 네트워크 정의와 구성을 자동화할 수 있습니다. 직관적인 그래픽 워크플로와 버튼만 누르면 되는 자동화가 합쳐져 CLI 기반 프로그래밍, 경로 테이블 스프레드시트, ACL 수작업 구성이 필요치 않게 됩니다.

## 인라인 정책 시행을 위한 그룹 정책 식별자

HPE Aruba Networking Central NetConductor 정책 관리자는 역할과 관련 액세스 정책을 정의합니다. 이 정책은 GPID(그룹 정책 식별자)로 표현되며 네트워크가 접근제어

정보를 트래픽 자체를 통해 전달할 수 있게 하고 사용자 또는 클라이언트의 역할과 액세스 권한을 반영합니다. 식별자는 패킷 헤더에 내장되며 HPE Aruba Networking CX 스위치와 게이트웨이를 통해 인라인으로 해석됩니다 (그림 2). 클라이언트의 보안 상태가 변경되면 역할을 자동으로 수정하여 액세스를 제한하고, 수정된 역할은 네트워크에 전파됩니다.

분산형 동적 세분화는 GPID 를 통해 정책을 시행할 규모를 크게 늘리면서 대기 시간과 트래픽 오버헤드를 줄일 수 있습니다. 식별자는 업계 표준에 따라 타사 네트워크와의 양방향 통합을 지원합니다.

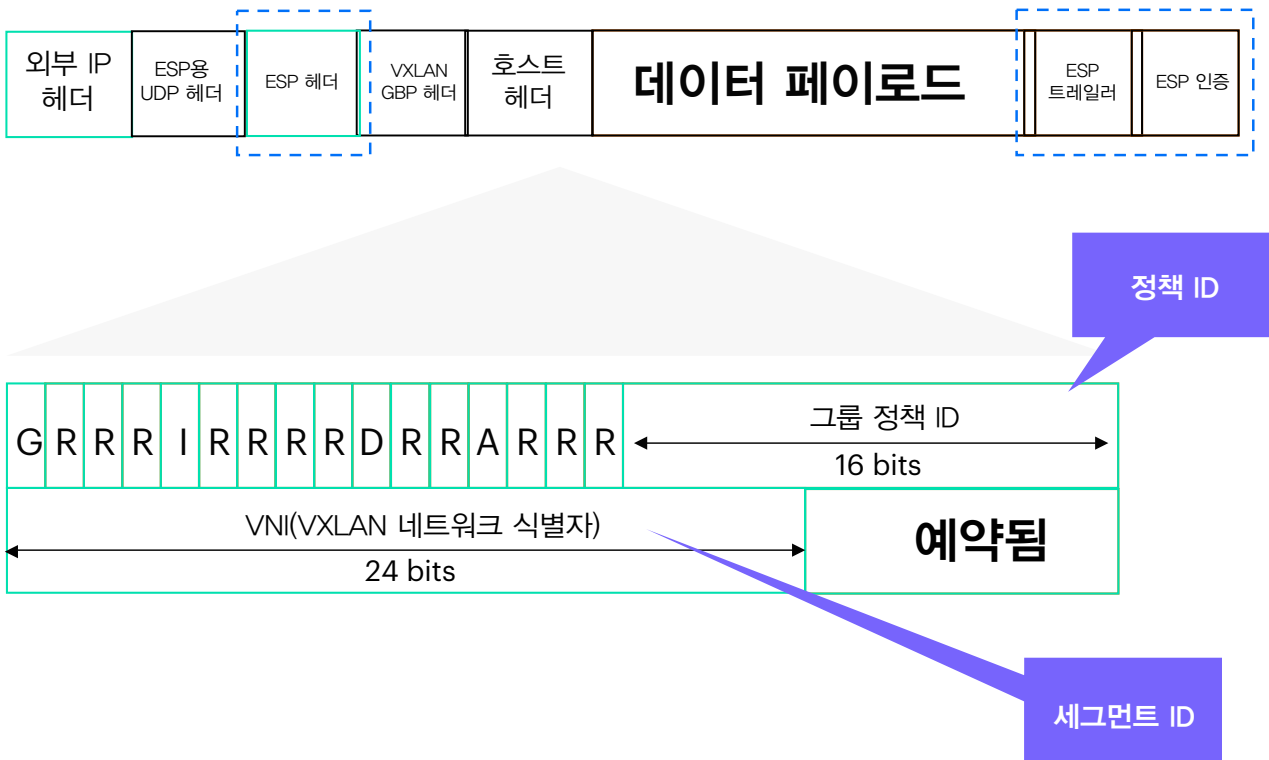


그림 2. GPID 가 인라인 정책 시행을 위해 접근제어 정보를 네트워크 트래픽을 통해 전달

## HPE Aruba Networking Client Insights

AI 기반 가시성 및 프로파일링

### GPID

패브릭 지원 HPE Aruba Net-working 스위치 및 게이트웨이를 통한 인라인 액세스 시행



### 정책 관리자

정책 개발

### 클라우드 인증(또는) HPE Aruba Networking ClearPass

인증, 역할 할당

그림 3. HPE Aruba Networking Central NetConductor 를 통한 분산형 동적 세분화를 위한 솔루션 구성요소

## HPE Aruba Networking Central NetConductor - 솔루션 구성요소

HPE Aruba Networking Central NetConductor 의 구성요소는 확장과 성능을 위해 분산형 동적 세분화를 지원하며, 이는 그림 3 을 통해 확인할 수 있습니다.

- **HPE Aruba Networking Client Insights** — 최초이자 유일한 에이전트리스 클라이언트의 전체 상태 파악 기능과 핑거프린팅 기능이 클라우드 네이티브 관리 플랫폼에 내장되어 있어 네트워크의 사각지대를 없앱니다. AI 기반 HPE Aruba Networking Client Insights 는 유무선 인프라 전체에 걸쳐 IoT 장치를 포함하여 다양한 클라이언트의 핑거프린팅, 식별, 정확한 프로파일링을 위해 인프라 원격 측정과 기계 학습 기반 분류 모델을 활용합니다.
- **Cloud Auth** — MAC 주소 기반 인증을 통해 또는 일반 클라우드 ID 저장소 ( 예 : Google Workspace™ 또는 Azure Active Directory) 와의 통합을 통해 최종 사용자와 클라이언트 장치의 원활한 온보딩을 지원하여 올바른 수준의 네트워크 액세스 권한을 자동으로 할당합니다.
- **정책 관리자** — 사용자와 장치 그룹을 정의하고 물리적 네트워크에 대한 액세스 시행 규칙을 생성합니다 ( 그림 4).

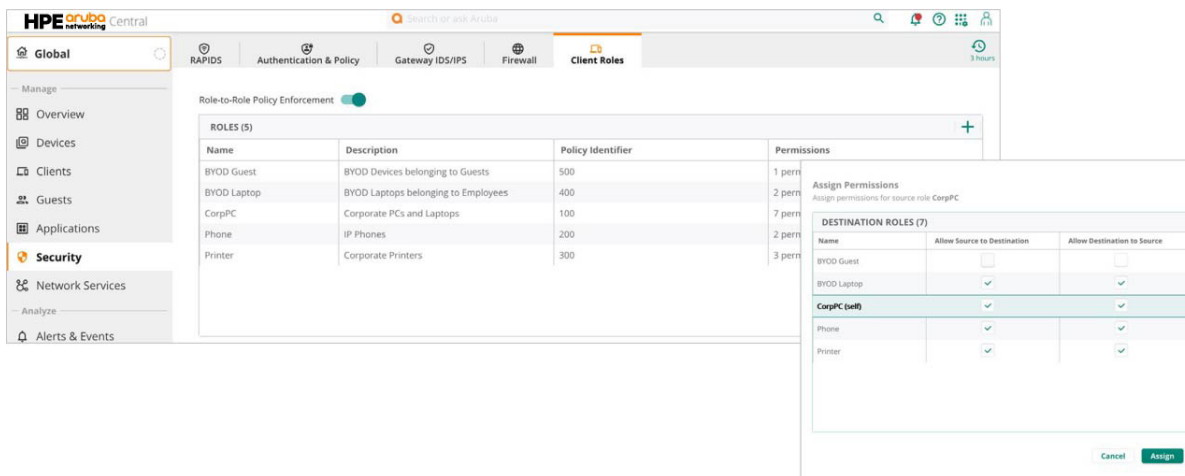


그림 4. 글로벌 정책 정의를 위한 직관적인 그래픽 인터페이스

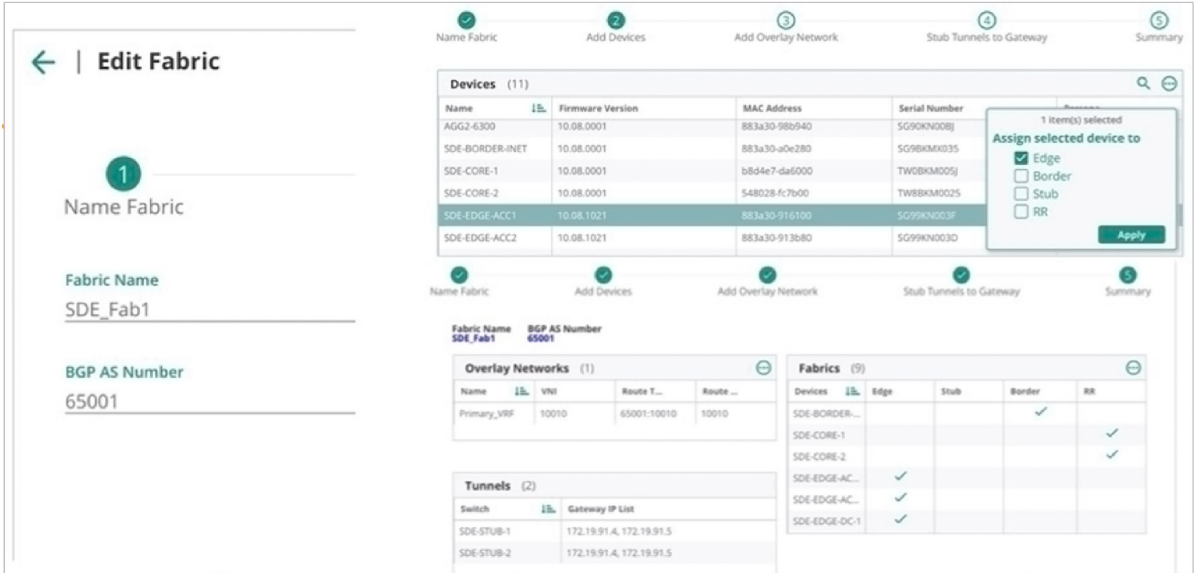


그림 5. 패브릭 오버레이의 구성 간소화와 배포 자동화를 위한 사용하기 쉬운 그래픽 워크플로

- **패브릭 마법사** — 직관적인 그래픽 사용자 인터페이스로 오버레이 생성을 간소화하여 가상 구성요소를 정의하고 구성 지침을 생성하며 스위치와 게이트웨이로 푸시하는 방법을 매우 손쉽게 만듭니다 (그림 5).
- **GPID** — 인라인으로 정책을 시행하기 위해 트래픽에 클라이언트 정책 정보를 전달하여 구성과 보안 오버헤드를 줄이고 이동성과 확장성을 높입니다.
- **패브릭 기반 HPE Aruba Networking 스위치 및 게이트웨이** — GPID 에 정의된 라우팅 지침과 액세스 권한을 기반으로 구성과 시행을 지원합니다.

**참고 :** 정책 오케스트레이션을 위해 HPE Aruba Networking Central NetConductor 정책 관리자를 사용하는 네트워크는 인증 및 역할 할당에 HPE Aruba Networking Central

클라우드 또는 HPE Aruba Networking ClearPass 를 사용할 수 있습니다.

## 중앙 집중식 동적 세분화

중앙 집중식 동적 세분화는 여러 세대의 네트워크 기술에 걸쳐 접근제어를 실현하는 주요 방식이었습니다. 이 모델의 경우 트래픽은 액세스 포인트와 HPE Aruba Networking 게이트웨이 ( 또는 컨트롤러 기반 환경의 경우 HPE Aruba Networking 모빌리티 컨트롤러 ) 간의 GRE 터널로 구성된 중앙 집중식 오버레이를 사용하여 안전하게 분리됩니다. 게이트웨이는 소스와 대상 클라이언트 또는 애플리케이션의 역할에 대한 지식을 가졌으며 정책 시행을 전달하는 포인트로 기능합니다 (그림 6).

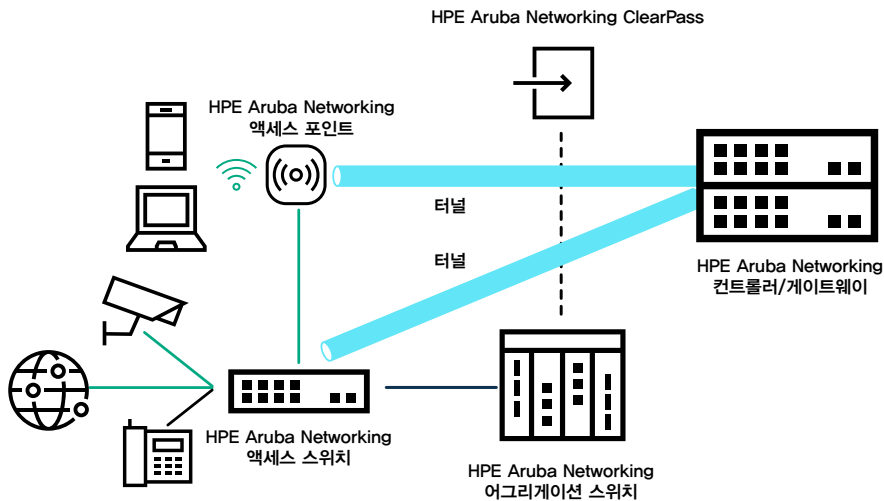


그림 6. HPE Aruba Networking 의 중앙 집중식 동적 세분화

## 정책 정의

중앙 집중식 적용 모델을 위한 HPE Aruba Networking ClearPass 또는 HPE Aruba Networking Central NetConductor 정책 관리자를 통해 중앙 집중식으로 정책을 정의할 수 있습니다.

HPE Aruba Networking ClearPass 는 네트워크 전반에 걸쳐 사용자를 따라가고 유무선, WAN, VPN 연결에 균일하게 적용되는 인증, 권한 부여, 중앙 집중식 정책 정의를 가능케 합니다. 사용자가 장치를 알 수 없는 것으로 바꾸거나 보호되지 않는 네트워크에 있는 경우 정책이 자동으로 인증 권한을 변경합니다.

HPE Aruba Networking ClearPass 는 보안 인증을 위해 표준 기반 802.1X 시행과 기타 기술을 지원합니다. 이는 다단계 인증을 사용하고 네트워크 전체의 주요 지점에서 재인증을 실현하는 다양한 인증 솔루션과 통합됩니다.

HPE Aruba Networking ClearPass 는 또한 포괄적인 통합 보안 커버리지와 응답을 위해 150 여 개의 파트너 통합과 함께 HPE Aruba Networking 360 Security Exchange Program 을 지원합니다.

HPE Aruba Networking ClearPass Policy Manager 를 자세히 알아보십시오.

## Policy Enforcement Firewall

제어에 IP 기반 VLAN 을 활용하는 전통적인 방화벽은 사용자 또는 장치가 네트워크에 들어섰을 때만 활성화되며

이는 고도화된 공격의 진입로가 되기도 합니다. HPE Aruba Networking 의 스테이트풀 레이어 7 PEF( 정책 시행 방화벽 ) 는 초기 연결 시에 ID, 트래픽 속성 그리고 기타 컨텍스트를 사용하여 중앙 집중식으로 액세스 권한을 적용합니다. PEF 를 통한 트래픽 감사로 사용자, 장치, 애플리케이션, 위치에 대한 세분화된 컨텍스트를 제공합니다. PEF 는 HPE Aruba Networking 게이트웨이 ( 또는 컨트롤러 기반 환경의 경우 모빌리티 컨트롤러 ) 에서 정책 시행을 지원하는 기본 네트워크 기술로 작동합니다.

## HPE Aruba Networking Dynamic Segmentation 모델 선택 가능

VLAN 기반 아키텍처를 EVPN/VXLAN 기반 인텔리전트 오버레이 패브릭으로 확장하면 사일로화된 구성과 보안 문제를 해결하여 넓게 분산된 복잡한 네트워크에서 정책 시행을 촉진할 수 있습니다 ( 그림 7 ). 널리 도입된 프로토콜을 사용하면 기존 인프라를 완전히 교체하지 않고도 다양한 벤더와의 상호 운용성을 통해 타사 네트워크와 통합할 수 있습니다.

고객은 중앙 집중식 또는 분산형 오버레이 패브릭 중 하나를 선택하거나 둘 다 사용할 수 있습니다. 두 모델이 한 환경에서 공존할 수 있기 때문입니다. 현재 중앙 집중식 접근 방식을 사용 중인 조직도 자신들의 상황에 맞춰 유연하게 액세스 장치를 통해 시행되는 분산형 방식을 도입할 수 있습니다.

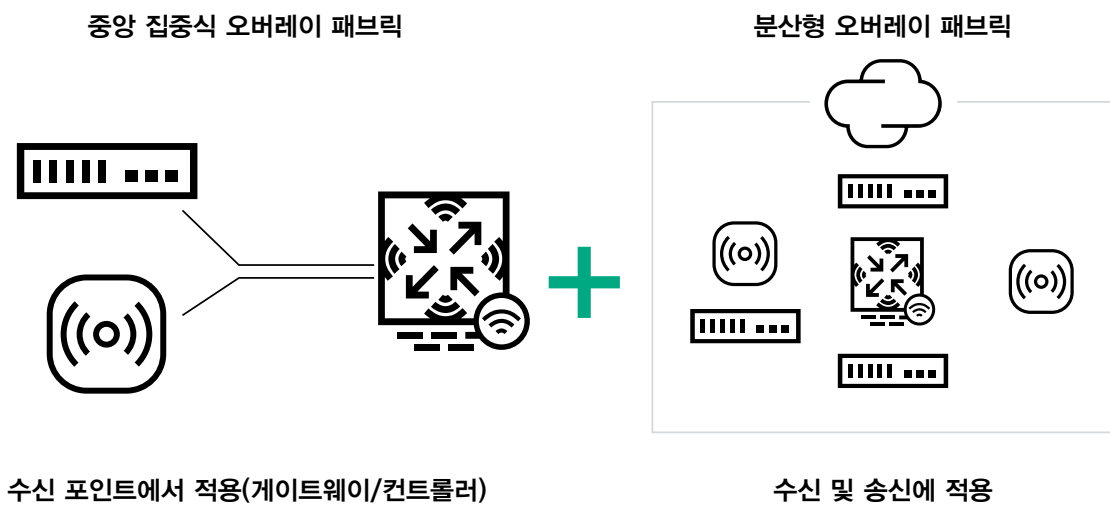


그림 7. 분산형 동적 세분화가 송수신 양쪽 지점에서 정책을 시행하기 위해 분산형 오버레이 패브릭을 활용하여 더 큰 규모와 성능 지원

## 요약

조직에서 네트워크를 더 강하게 보호하려면 IoT, BYOD 클라이언트, 사용자 트래픽의 세분화가 매우 중요합니다. IT 팀은 HPE Aruba Networking의 혁신적인 동적 세분화를 통해 환경에 가장 잘 맞는 모델을 선택하여 엣지 투 클라우드에 통합 정책과 시행 기능을 동적으로 적용하여 보안을 강화할 수 있습니다. HPE Aruba Networking Dynamic Segmentation이 적용하는 세밀한 역할 기반 액세스 권한으로, 공격이 감지될 경우 엔드포인트 클라이언트를 자동으로 차단하거나 격리하여 손상된 사용자와 클라이언트가 공격에 이용되는 것을 쉽게 방지할 수 있습니다.

클라우드 또는 온프레미스를 통해 구현 가능한 중앙 집중식 또는 분산형 모델을 선택하여 어떤 네트워크 토폴로지에서도 액세스를 적절하게 제어하고 보안 정책을 자동으로 업데이트하며 지속적으로 시행할 수 있습니다. HPE Aruba Networking Dynamic Segmentation을 통해 글로벌 규모로 네트워크의 크기와 복잡성에 관계없이 제로 트러스트 보안과 SASE 프레임워크 도입을 간소화할 수 있습니다.

HPE.com 방문하기

## 자세히 알아보기

[HPE.com/ww/  
network-security](https://www.hpe.com/network-security)



## 채팅 상담하기

© Copyright 2025 Hewlett Packard Enterprise Development LP. 본 문서의 내용은 사전 통지 없이 변경될 수 있습니다. Hewlett Packard Enterprise 제품 및 서비스에 대한 보증의 경우, 해당 제품 및 서비스와 함께 제공된 보증서에 명시된 내용만이 적용됩니다. 본 문서에는 어떠한 추가 보증 내용도 들어 있지 않습니다. Hewlett Packard Enterprise는 본 문서의 기술상 또는 편집상의 오류나 누락에 대해 책임지지 않습니다.

Google Workspace는 Google Inc.의 상표입니다. Active Directory와 Azure는 미국 및 / 또는 기타 국가에서 Microsoft Corporation의 등록 상표 또는 상표입니다. 모든 타사 마크는 해당 소유자의 재산입니다.

a00058593KOP, 제 1 차 개정판

HEWLETT PACKARD ENTERPRISE

hpe.com

