aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

DYNAMIC SEGMENTATION

간단하고 안전한 유무선 네트워크 통합 액세스

증가하는 IoT 디바이스와 비즈니스 모빌리티, 클라우드 서비스 사용이 디지털 업무환경의 혁신을 주도하고 있습니다. 기존 네트워크 에지는 모든 유형의 기기와 사용자를 안전하게 연결할 수 있을만큼 스마트할까요? 레거시 유무선 네트워크는 비즈니스에 필수적인 모빌리티, IoT 액세스, 보안을 염두에 두지 않고 설계되었습니다. 캠퍼스와 브랜치 네트워크 전반에 연결된 모바일 기기와 IoT 기기에 수작업 중심의 정적 구성을 사용하는 현재의 방식은 새로운 보안 위험을 불러옵니다. 또한 IT 팀에 날마다 번거로운 작업으로 인한 부담을 가중시킵니다.

아루바 다이나믹 세그멘테이션(Dynamic Segmentation)은 네트워크를 간소화하고 보호하기 위해 유무선 네트워크 전반에 대한 정책 실행을 통합하고 트래픽을 안전하게 분리합니다. 따라서 IoT 디바이스와 IT 팀이 관리하는 클라이언트 디바이스가 공존하는 기업 네트워크의 운영을 간소화하고 엔드 투 엔드 네트워크 경험과 IT 작업을 최적화할 수 있습니다.

다이나믹 세그멘테이션(Dynamic Segmentation)은 아루바의 역할 기반 정책 기능, 사용자 방화벽, 풍부한 Layer 7 애플리케이션 가시성 및 웹 컨텐츠 필터링을 통해 수집된 인텔리전스를 활용합니다

주요 비즈니스 및 기술 동인

정책 관리 간소화

IoT 디바이스와 클라이언트 디바이스를 온보딩에는 일반적으로 다수의 터치포인트가 필요하고, 네트워크의 모든 홉마다 새로운 VLAN, ACL 또는 서브넷을 수동으로 구성해야 했습니다. 또한 대규모 분산 네트워크에서 끊임없는 이동, 추가, 변경을 실행하는 데에는 시간이 많이 걸리고 오류도 빈번할 수 있습니다. 이 때문에 강력한 보안을 갖춘 네트워크를 설계하면서 복잡성을 줄인다는 것은 거의 불가능한 일이었습니다.

사용자 경험 향상

사용자들은 사무실 내에서 또는 다른 사이트로 이동하더라도 연결 위치나 유선 또는 무선에 관계없이 동일한 네트워크 환경을 기대합니다. 또한 사용자에게 VPN 사용을 요구하기도 어렵습니다. 사용자에게 IT 팀의 지원이 필요한 모든 네트워크 경험은 부정적으로 인식됩니다.

주요 이점

일관되고 향상된 사용자 경험

- 사용자 역할, 애플리케이션 DPI(deep packet inspection), 디바이스 프로파일링 기능을 무선 네트워크에서 유선 네트워크로 확대

네트워크 운영 간소화

- SSID, ACL, 서브넷, 유선 포트 구성의 필요성을 줄여서 시간을 절약하고 VLAN 스프롤을 제거

보안 및 디바이스 가시성 향상

- 클리어패스(ClearPass)와 PEF(Policy Enforcement Firewalls)가 향상된 가시성과 정책 실행 제공

직원, 게스트, 쇼핑객, 학생 등 모든 사용자들의 경험이 조직의 성공에 영향을 미칩니다. 스마트폰, 프린터, 화상회의 장비와 같은 새로운 유형의 디바이스 연결은 대개 IT 지식이나 지원없이 수행됩니다. 사용자들은 IT 팀이 안전한 네트워크에서 모든 것의 가시성과 관리를 유지하면서 완벽한 경험을 제공하기를 기대합니다.

스마트 조명에서 보안 카메라, 배지 리더에 이르기까지 IoT 기기가 모든 규모의 네트워크에 빠르게 배포되고 있습니다. 이 새로운 네트워크 연결은 많은 매력적인 이점을 제공하지만 동시에 네트워크를 위험에 노출시킵니다. 이러한 기기들이 민감한 금융, 의료, 비즈니스 크리티컬 데이터와 동일한 경로를 사용하기 때문입니다. 이러한 기기들에는 강력한 보안 기능이 거의 없으며 강력한 인증 기능도 없습니다. 암호는 일반 텍스트로 저장되고 보안 요청자(Supplicant)가 없으며, 안전하지 않은 공공 장소에 위치하여 네트워크 보안 침해의 입구로 악용되는 경우도 빈번합니다.

2020년 엔터프라이즈 네트워크에 연결된 IoT/헤드리스 디바이스 수가 2백억대를 넘어설 것으로 예상되며 이로 인한 네트워크 취약성이 노출될 것이다.

출처 : Gartner (2017년 1월)

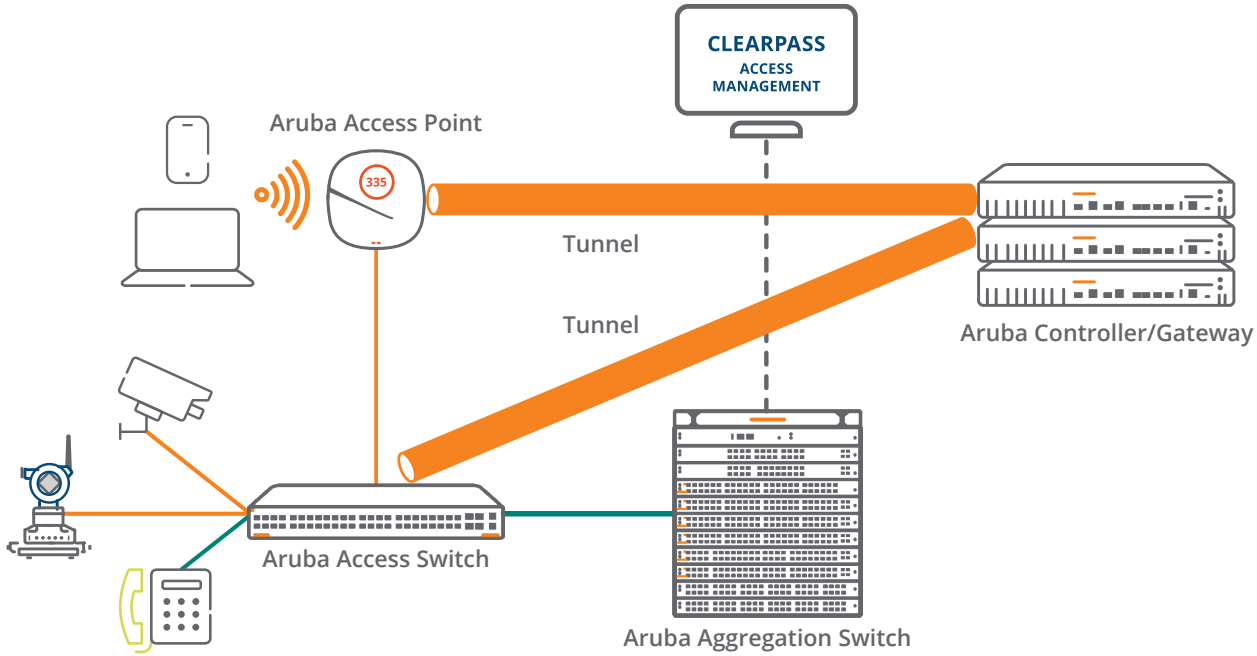
WLAN 혁신을 스위칭으로 확대

다이나믹 세그멘테이션(Dynamic Segmentation)은 아루바의 보안 정책 관리와 WLAN 정책 실행 기능을 확장하여 유선 네트워크 액세스 보안을 강화하고 간소화합니다. 이 기능을 통해 유선 클라이언트 디바이스에 포트 또는 사용자 역할에 따라 동적으로 정책을 할당할 수 있습니다. IoT 디바이스 수가 2020년 2백억 대를 넘어설 것으로 전망되는 상황에서 이상적인 기술이라 할 수 있습니다. 정책 관리를 수행하는 클리어패스(ClearPass)와 정책 실행을 담당하는 모빌리티 컨트롤러(Mobility Controller)로 지원되는 아루바 네트웍스 스위치는 네트워크 액세스를 통합하는 데 핵심적인 역할을 합니다.

역할 기반 정책

다이나믹 세그멘테이션(Dynamic Segmentation)을 구현하면 디바이스 유형, 사용 애플리케이션, 사용자/디바이스 위치에 따라 역할 기반 정책 결정과 액세스 권한이 정해집니다.

원래 무선 보안을 처리하는 데 사용되었던 역할 기반 정책은 직원, 게스트, 계약 업체와 같은 사용자 유형별로 네트워크 트래픽을 세분화하고 복잡한 정적 네트워크 구성을 없애 네트워크 관리를 대폭 간소화합니다. 이 강력한 기능은 액세스 관리, BYOD 정책 등의 IT 워크플로우를 간소화하고 애플리케이션 성능을 향상시킵니다.



다이나믹 세그멘테이션(Dynamic Segmentation) 및 Experience Edge

무선 AP와 유선 스위치 전반으로 동적인 역할 기반 정책 관리를 확장하면 단순하고 안전하면서도 각기 다른 방식으로 모빌리티, IoT, 클라우드에 대한 정책을 관리하고 실행할 수 있습니다. 이제 클리어패스(ClearPass) 정책 정의를 실행하는 아루바의 모빌리티 컨트롤러/게이트웨이는 역할을 동적으로 식별하고 활용할 수 있습니다. 이 기능은 정책을 동적으로 할당함으로써 많은 시간과 잦은 오류가 수반되는 복잡하고 정적인 VLAN, ACL, 서브넷 관리 작업을 없애줍니다.

Layer 4-7 세그멘테이션

아루바 스위치가 활용하는 두 번째 기본 기능은 세그멘테이션 (segmentation)입니다. 아루바 WLAN 아키텍처는 액세스 포인트와 컨트롤러 또는 게이트웨이 사이에 터널을 사용하여 트래픽을 안전하게 보호하고 분리합니다. 이 터널 기반 세그멘테이션은 아루바의 빌트인 PEF(Policy Enforcement Firewall)를 사용하여 고위험 트래픽의 방화벽 검사와 같은 보안을 제공합니다. PEF가 세부적인 컨텍스트 (사용자, 디바이스, 앱, 위치)를 제공하므로 1차 조사와 방어를 위한 고가의 방화벽이 필요 없게 됩니다. ID, 디바이스 유형, 위치를 기반으로 한 컨텍스트 정책을 통해 트래픽 플로우가 할당된 역할에 맞게 적용됩니다. 따라서 단일 네트워크 구성으로 다양한 사용자 그룹의 요구를 만족시킬 수 있습니다.

이 WLAN 터널링 아키텍처를 사용함으로써 아루바 스위치는 수작업 방식의 기존 로컬 VLAN 대신에 역할 기반 세그멘테이션을 제공할 수 있습니다. 아루바 스위치는 액세스 포인트와 마찬가지로 DPI(Deep Packet Inspection)와 디바이스 인증을 위해 특정 트래픽을 컨트롤러로 동적으로 터널링할 수 있습니다. 따라서 신뢰할 수 없는 IoT 디바이스나 애플리케이션 가시성을 제공하는 데 이상적입니다. 예를 들어 보안 카메라에는 트래픽을 지정된 서버로만 전송할 수 있는 권한과 역할이 할당되므로 네트워크의 다른 부분에 악의적으로 액세스할 수 있는 기회가 차단됩니다.

이 새로운 세그멘테이션 기능은 모든 인증이 컨트롤러에서 이루어지는 PBT(Port- Based Tunnelling) 또는 스위치에서 이루어지는 UBT (User-Based-Tunnelling)로 셋업할 수 있는 터널링을 통해 보안 태세를 강화합니다. 이러한 세그멘테이션은 오버레이로 작동하기 때문에 전체 스위칭 인프라를 교체하지 않고도 지정된 영역에서 보안 터널을 활용하여 VLAN과 공존할 수 있습니다.

다이나믹 세그멘테이션(Dynamic Segmentation)은 모빌리티 컨트롤러(Mobility Controller)를 통합 PEE(Policy Enforcement Engine)로 사용하여 유무선 네트워크를 단순화하고 보호합니다. AP 또는 스위치의 트래픽은 PEF (Policy Enforcement FIrewall)에서 검사하기 위해 GRE 터널에 캡슐화됩니다.

솔루션 구성요소

아루바 무선 액세스 포인트

다양한 환경의 요구를 맞는 802.11ac 및 802.11ax Wi-Fi 성능을 제공합니다. 빌트인된 AI 인텔리전스와 로케이션 서비스를 통해 사용자와 IoT 디바이스에 최적의 환경을 제공하는 데 필요한 자동화와 가시성을 제공합니다.

.아루바 네트워크 스위치

캠퍼스와 브랜치 네트워크를 위한 확장성, 보안, 고성능을 제공하는 유무선 통합 기반을 구현합니다. 다이나믹 세그멘테이션(Dynamic Segmentation)은 IT 팀이 간단한 방식으로 정책 적용, 고급 서비스 활용, 유선 사용자와 IoT 트래픽의 안전한 분리를 수행할 수 있도록 해줍니다. 유선 사용자와 IoT 트래픽을 안전하게 분리하기 위해 컨트롤러에서 인증을 수행하는 PBT(Port-Based Tunnel) 또는 아루바 스위치에서 인증을 실행하는 UBT(User-Based Tunnel)를 사용합니다.

아루바 게이트웨이와 모빌리티 컨트롤러

컨트롤러나 게이트웨이는 솔루션의 핵심 요소로서 유선 트래픽과 무선 트래픽 모두를 위한 폴리시 인포서(Policy Enforcer) 역할을 합니다. AOS 8.1 이상이 탑재된 아루바 모빌리티 컨트롤러(Mobility Controller)는 IT 팀이 정책 실행, 대역폭 계약(Bandwidth Contract), 트래픽 제한을 수행하도록 해줍니다. 브랜치 환경에서는 아루바 센트럴(Central)로 관리되는 브랜치 게이트웨이가 이러한 역할을 담당합니다. PEF(Policy Enforcement Firewall)는 이 두 환경을 지원하는 기본 네트워크 기술 역할을 합니다.

아루바 클리어패스 폴리시 매니저(ClearPass Policy Manager) 및 프로파일링 기능

유무선 접근제어를 위한 네트워크 액세스 정책을 중앙에서 관리하고 실행합니다. 아루바 클리어패스 폴리시 매니저(ClearPass Policy Manager)의 주요 기능은 디바이스 프로파일링, 인증, 권한 부여, 정책 실행입니다. 클리어패스(ClearPass)를 사용하여 역할과 권한을 정의해 놓으면 그 내용이 유무선 액세스 전반에서 해당 사용자 또는 디바이스를 따라다닙니다.

따라서 사용자가 언노운 디바이스로 기기를 변경하거나 보안되지 않은 네트워크로 연결할 경우에는 정책이 자동으로 액세스 권한을 변경하게 됩니다. 클리어패스(ClearPass)에서 DUR(Downloadable User Roles)을 구성할 수 있기 때문에 스위치에서 따로 역할(Role)이나 정책을 정의할 필요가 없습니다.

요약

비즈니스 모빌리티와 증가하는 IoT 연결 요구를 효과적으로 처리하기 위해 아루바의 혁신적인 다이나믹 세그멘테이션(Dynamic Segmentation) 솔루션은 네트워크 어디서나 동적으로 일관된 정책을 적용하고 고급 서비스를 실행함으로써 IT 작업을 간소화하고 보안을 향상시킵니다. 이를 통해 적절한 액세스와 보안 정책을 효율적으로 배포하고 자동 적용하여 모든 유무선 사용자와 디바이스에 대해 개별적으로 실행되도록 보장합니다.

aruba
a Hewlett Packard Enterprise company

www.arubanetworks.co.kr

아루바 휴렛팩커드 엔터프라이즈 컴퍼니
서울특별시 영등포구 국제금융로 8길 31번지
제품정보 및 구입안내: www.arubanetworks.com/ko/company/contact-us/contact-us-form/

M10/2019

SO_DynamicSegmentation_SK_092419
a00058593enw