기술 요약

다이나믹 세그멘테이션을 위한 POLICY ENFORCEMENT FIREWALL

엔터프라이즈 네트워크가 디지털 혁신의 촉매 역할을 하고 연결성이 보편화됨에 따라 기존 네트워크 및 보안 접근 방식의 당면 과제를 해결할 수 있는 새로운 정책 시행 및 사이버 보안 솔루션이 요구되고 있습니다. IoT 디바이스를 통해 기업 유무선 네트워크상에서 직원, 고객, 방문자가 모여들고 있으며 그 결집 범위는 끊임없이 변화하고 있습니다. IP 주소에 기반을 둔 규칙과 물리적 네트워크 구성을 사용하는 방화벽과 같은 표준 방어 체계로는 이제 충분하지 않습니다.

POLICY ENFORCEMENT FIREWALL (PEF)

내부에서 이루어지는 새로운 공격은 기존 보안 방어 체계를 회피하고 이용하도록 고안되고 있습니다. 이러한 공격은 몇 주 또는 몇 개월 동안 네트워크에 머무르다가 전혀 예기치 않은 시점에 데이터를 추출하여 치명적으로 암호화하거나 IT 리소스를 침해합니다. 이와 동시에 IT는 애플리케이션 레이어에 대한 가시성이 부족합니다. 이로 인해 네트워크 성능 및 최종 사용자 경험이 부정적인 영향을 받습니다.

유무선 네트워킹 분야 선도업체인 아루바 휴렛팩커드 엔터프라이즈 컴퍼니(Aruba, a Hewlett Packard Enterprise company)는 군사 등급 암호화와 Policy Enforcement Firewall(PEF)이라는 특수 ID 기반 액세스 솔루션이 포함된 종합적인 에지 기반 사이버 보호 기능을 처음으로 개발하였습니다. PEF는 ArubaOS 및 InstantOS에서 실행되며, **전 세계적으로 400만 건 이상 설치**되어 운영 중인 입증된 기술입니다. PEF는 액세스 포인트에서 "제로 트러스트" 경계를 제공하는 유일한 사용자 및 디바이스 대상 방화벽입니다.

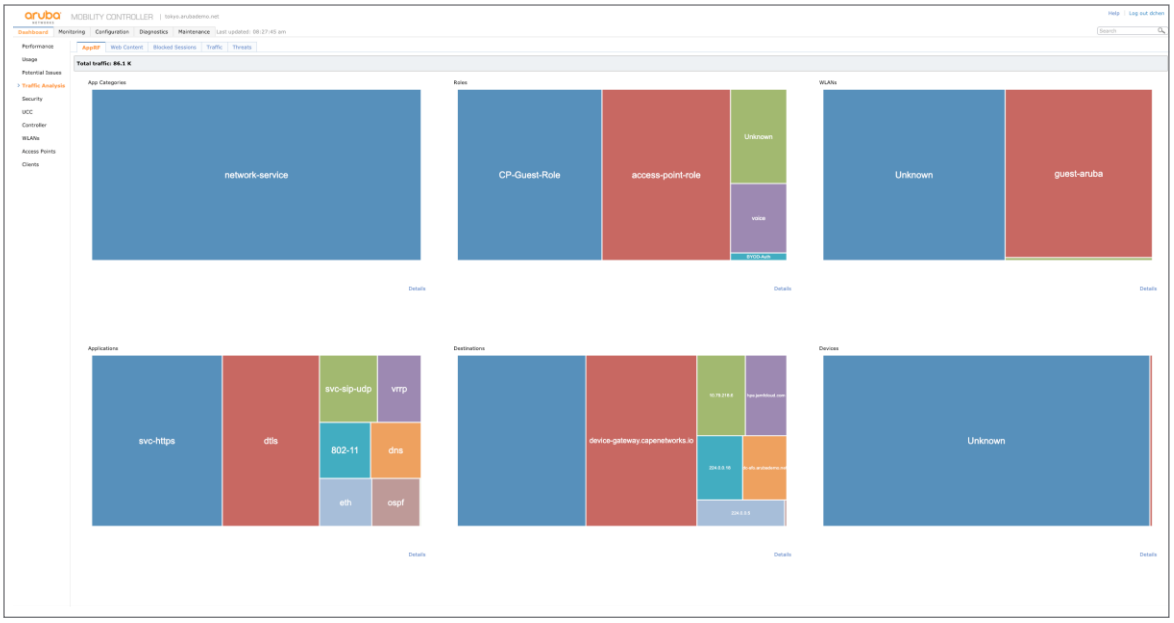
제어를 위해 IP 기반 VLAN을 활용하고 사용자 또는 디바이스가 네트워크의 승인을 받은 후에만 활성화되는 기존 방화벽은 고급공격에 대한유혹의 여지를 를 남깁니다. PEF를 이용한 아루바의 사용자 및 애플리케이션 방화벽 접근 방식에서는 ID, 트래픽 속성, 기타 보안 컨텍스트를 사용하여 초기 연결 시점에 중앙에서 액세스 권한을 제어함으로써 이러한 취약점을 보완합니다. 공격자가 네트워크에 접속하는 순간마다 수천 개의 악성 프로그램 패킷이 방출될 수 있으므로 이러한 공백을 메우는 것이 필수적입니다.

주요 이점

- **중앙집중식 제로 트러스트 액세스:** 초기 네트워크 연결 및 기존 방화벽 시행 간의 차이 감소
- **Marsh가 Cyber Catalyst℠로 지정:** 위험을 줄일 수 있는 PEF의 능력에 근거하여 선별된 보험사의 강화된 사이버 보험 정책 약관에 대한 자격을 갖추도록 지원
- **사용자 및 애플리케이션 방화벽:** 역할 기반 액세스 제어를 통해 구성 오류 최소화
- **추가 하드웨어 불필요:** 기존 아루바 네트워크 인프라에서 PEF 실행
- **작업 수행 간소화:** 하드웨어 가속 트래픽 처리 포함
- **자동화된 자기 학습:** 통찰력 있는 네트워크 및 애플리케이션 사용량 데이터 제공
- **재사용할 수 있는 정책 라이브러리:** 관리자가 유용하고 일관성 있는 정책을 손쉽게 생성
- **연결 독립성:** 역할은 유무선 및 원격 연결 전반에 걸쳐 사용자 및 디바이스를 따름
- **보안 인증:** 정부에서 후원하는 전방위 검증

CYBER CATALYST℠로 지정된 솔루션

아루바의 PEF(Policy Enforcement Firewall) 기술을 사용하는 조직은 ID, 트래픽 속성, 기타 컨텍스트를 사용하는 제로 트러스트 액세스 모델을 구현하여 초기 연결 시점에 중앙에서 액세스 권한을 시행할 수 있습니다. 안전한 역할 기반 정책을 동적으로 시행할 수 있는 기술 및 능력을 갖춘 Aruba Policy Enforcement Firewall은 위험을 효과적으로 줄일 수 있는 능력에 근거하여 “Cyber Catalyst℠”로 지정되었습니다.



ArubaOS 대시보드 보기: 3000개 이상의 애플리케이션에 대한 가시성

단순하고 안전한 네트워크 액세스

PEF는 유무선 네트워크를 단순화하고 보호하는 아루바의 Experience Edge 내 핵심 기술 솔루션인 다이나믹 세그멘테이션 (Dynamic Segmentation) 을 활성화하는 기본 기술이기도 합니다. 사용자 및 애플리케이션 제어로 인해 IT가 VLAN, SSID 또는 ACL을 추가할 필요가 없어지므로 복잡성이 획기적으로 감소합니다.

네트워크 관리자는 PEF의 애플리케이션 가시성 기능을 사용해 네트워크에서 실행 중인 애플리케이션과 애플리케이션 사용자에 대한 풍부한 통찰을 얻을 수 있습니다. WebCC는 URL 필터링, IP Reputation 및 지리적 위치 필터링을 포함함으로써 PEF를 강화하는 구독 기반 애드온 기능입니다.

제로 트러스트 보호를 위한 강력한 인증 및 역할 기반 제어

먼저 네트워크 사인온 프로세스 중에 각 사용자 또는 디바이스의 ID를 Active Directory(AD), RADIUS, LDAP, SQL 데이터베이스, LDAP 기반 ID 저장소 또는 게스트 데이터베이스와의 통합을 통해 확인합니다. ID를 구성하면 역할이 할당됩니다. 역할은 애플리케이션 액세스 권한을 포함하는 권한과 사용자 또는 디바이스 간 커뮤니케이션의 논리적 그룹화입니다.

사용자를 역할에 연결하면 사용자의 보안 컨텍스트가 변경되었을 때(예; 디바이스가 침해를 받은 경우) 네트워크를 재구성할 필요 없이 새롭고 더 제한적인 역할을 할당하는 것만으로도 액세스 권한을 즉시 변경할 수 있다는 이점이 있습니다.

사용자 또는 디바이스의 역할이 할당되면 조직의 보호 우선순위에 따라 정책이 적용됩니다. 이러한 정책은 네트워크 전반에 걸쳐 사용자를 따르며 유무선 및 VPN 연결 전반에 걸쳐 획일적으로 적용됩니다. 디바이스가 디렉터리에 등록되면 지문이 등록된 디바이스유형에 따라 기본 정책을 적용할 수 있습니다(예: "모든 텔레비전 화면에 DNS, DHCP, 인터넷 기반 HTTPS 서비스에 대한 액세스 권한이 부여되지만 내부 리소스에 대한 권한은 부여되지 않음").

PEF에서 제어하는 액세스 네트워크에 접속하는 승인된 사용자는 처음에 역할 (예: "병원 인사 관리자") 을 할당받으며 이 역할과 함께 일련의 IT 권한이 주어집니다. 이 경우 관리자는 이메일, Microsoft Office, 직원 기록과 같이 자신의 작업에 필요한 도구 및 네트워크 서비스에만 액세스할 수 있고 환자의 의료 정보에는 액세스할 수 없습니다. 사용자가 침해를 당한 경우 새 역할("잠재적 침해, 검역소로 보냄")이 자동으로 적용되고 시행됩니다.

결과적으로 PEF는 VLAN 구성을 결정하고 변경하는고된 수동 작업과 오류가 발생하기 쉬운 작업을 제거하고 동시에 정확한 시행을 실시간으로 제공합니다.

또한 PEF는 심층 패킷 검사를 이용하므로 **레이어 7 애플리케이션 인식 기능이 있으며 3,000개 이상의 애플리케이션을 승인**합니다. 결과적으로 트래픽 분리를 하나의 특정 애플리케이션에 대해 하나의 사용자 또는 디바이스만큼이나 세밀하게 수행할 수 있습니다. 이는 VLAN 기반 접근 방식에서는 불가능한 기술입니다.

풍부한 애플리케이션 가시성

심층 패킷 검사(DPI)를 통한 풍부한 애플리케이션 가시성을 이용해 애플리케이션 성능 관련 문제를 실시간으로 해결하고 전역 정책을 설정하고 향후 성장을 계획할 수 있습니다.

내장형 대시보드를 통해 IT는 사용자 역할, 애플리케이션, 네트워크, 기타 기준에 따라 정렬할 수 있는 모바일 애플리케이션 사용량 및 성능을 탁월하게 시각화하여 간편하게 볼 수 있습니다.

- **모바일 애플리케이션:** Apple FaceTime과 같은 개인 애플리케이션의 Box와 같은 기업 애플리케이션을 구별합니다(이 애플리케이션이 동일 모바일 디바이스에서 실행 중일 때도 가능).
- **Apple AirPrint 및 AirPlay와 같은 네트워크 서비스:** Aruba는 IP 멀티캐스트 비디오 트래픽을 최적화하고 서비스의 우선순위를 자동으로 정하고 정책 제어를 추가합니다.
- **웹 기반 애플리케이션:** 다수의 웹 기반 애플리케이션에서는 동일한 포트를 사용하여 클라이언트와 커뮤니케이션하며 HTTP 트래픽으로 표시됩니다. Aruba의 기술은 대상 주소를 분석하여 Facebook, Twitter, Box, WebEx 등 고유한 수백 가지 애플리케이션을 식별합니다.
- **암호화된 애플리케이션:** 암호화된 트래픽의 경우 Aruba는 휴리스틱을 사용해 트래픽 패턴을 검색하고 고유한 지문을 구성하여 이러한 애플리케이션을 식별합니다.

정책 기반 트래픽 관리 및 제어

PEF는 트래픽 활용도를 최적화하는 제어 기능이 특징입니다. 역할 기반 정책을 통해 특정 사용자 또는 사용자 클래스의 대역폭 최대 소비량을 제한하고 고급 사용자가 네트워크 리소스를 독점하는 것을 방지할 수 있습니다.

이와 동시에 트래픽 관리 정책은 사용자가 생산성을 유지할 수 있도록 디바이스의 최소 대역폭을 보장할 수 있습니다. PEF는 성능을 저하시키는 브로드캐스트 및 멀티캐스트 트래픽을 최적화하여 애플리케이션 성능을 향상시킵니다.

mDNS, ARP 및 NetBIOS 브로드캐스트와 같이 대역폭을 많이 소비하는 기타 프로토콜은 완전히 필터링하여 네트워크의 특정 부분에만 국한시킬 수 있습니다.

이외에도 PEF는 포괄적인 온라인 위협 인텔리전스를 제공하여 사용자 및 네트워크를 악성 파일 및 URL에서 실시간으로 보호합니다. 사용자 역할 또는 디바이스 컨텍스트뿐 아니라 URL 필터링, IP Reputation 및 지리적 위치(WebCC 구독)에 따라 정책이 시행될 수 있습니다.

QUALITY OF SERVICE (QoS)

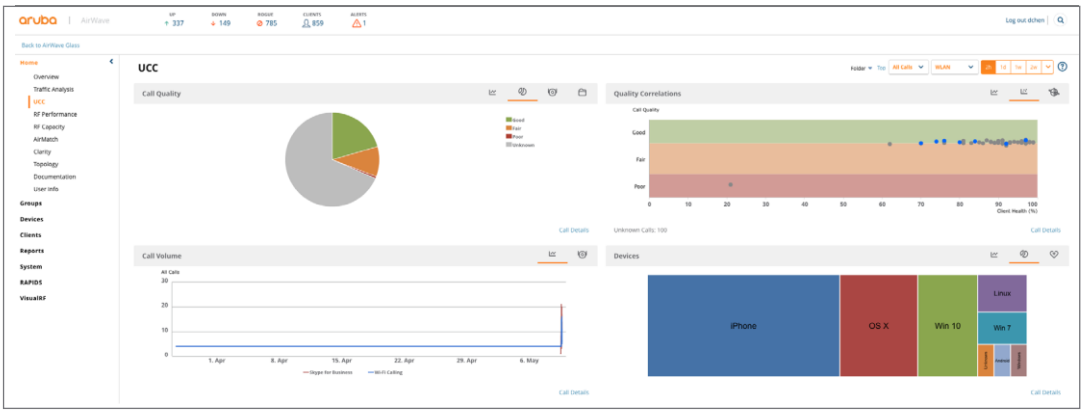
모바일 앱을 파악하여 시각화한 후에는 액세스 제어 및 정책을 적용하여 엔터프라이즈 애플리케이션이 개인 애플리케이션보다 우선적으로 실행되게 할 수 있습니다. 모바일 디바이스가 Wi-Fi 대역폭을 두고 다툴 때 PEF는 사용자가 가장 염려하는 앱을 보호합니다.

Apple AirPrint, AirPlay 같은 네트워크 서비스는 최적화되고, IP 멀티캐스트 비디오 트래픽은 우선순위가 자동으로 지정되며, 독점적인 Apple FaceTime 트래픽과 Microsoft Teams나 Skype for Business와 같은 암호화된 음성 및 비디오 세션은 자동으로 식별되고 우선순위가 지정됩니다.

이외에도 Pandora, Netflix, Google Drive, Citrix GoToMeeting, Salesforce.com, Dropbox와 같은 일반 웹 서비스는 사용자, 디바이스, 위치에 따라 네트워크보다 높은 우선순위가 지정될 수 있습니다.

PEF는 트래픽에 허용, 삭제, 로그, 거부 등 다수의 방화벽 보안 작업을 적용할 수 있습니다. 패킷은 802.1p 또는 DSCP 표시로 태그가 지정되고 여러 대기열로 우선순위가 지정되며 프로토콜에 따라 여러 대상으로 리디렉션될 수도 있습니다.

음성 및 비디오 프로토콜에 대한 첨단 인식을 통해 적절한 QoS가 제어 프로토콜 및 통화 세션 모두에 자동으로 적용됩니다.



Aruba UCC 대시보드 보기

PEF는 적절한 우선순위 레벨이 관련 프로토콜에 매핑되도록 보장합니다. 예를 들어 사용자가 수신 또는 발신하는 트래픽이 음성에 대한 관련 QoS 설정과 일치하지 않는다면 이 트래픽은 적절한 우선순위로 재분류됩니다.

중요 통합 커뮤니케이션(UCC) 서비스의 경우 통화 상태 및 품질에 관한 지식에 근거하여 더 스마트한 VoIP 관리가 가능합니다. 아루바의 AirMatch 및 ClientMatch RF 최적화 기술이 탑재된 AI 기반 스마트는 활성 세션 중단을 완화합니다.

UCC에 최적화된 환경

통합 UCC 대시보드를 통해 아루바는 Microsoft Teams, Microsoft Skype for Business, Apple FaceTime, Wi-Fi 통화, Jabber/Spark 및 SIP 등 다양한 UCC 애플리케이션에 대한 핵심 통화 품질 메트릭스를 단순하게 시각화합니다.

대시보드에 커서를 갖다 대거나 직접 클릭하여 전화 번호 연결, 통화 품질 추적, 상세 통화 기록(CDR), CAC (Call Admission Control)와 같은 자세한 보고 및 문제해결 정보를 얻을 수 있습니다.

대시보드에 포함된 항목은 다음과 같습니다.

- 통화 품질 및 상관관계 – 이 그래프는 AP-클라이언트 간 통화 품질이 WLAN 탭에, 통화 유무선 레그를 포함한 엔드 투 엔드 품질이 엔드 투 엔드 탭에 표시됩니다.
- 통화 볼륨 – 이 그래프에는 시도된 통화의 총 횟수가 UCC 애플리케이션 유형별로 표시됩니다. 예: SIP, Lync, SCCP, H.323, NOE, SVP, VOCERA, FaceTime.
- 디바이스 – 이 그래프에는 음성 세션 분석 정보가 디바이스 유형별로 표시됩니다. 예: iPhone, OS X, Win 10 등

고성능 트래픽 처리

PEF를 사용하면 정책 시행 시 성능이 저하되지 않고 추가 외부 하드웨어도 필요 없습니다.

Aruba Mobility Controllers는 제어 처리, 네트워크 트래픽 처리 및 암호화를 위한 전용 하드웨어를 이용해 네트워크 트래픽을 고속으로 처리하기 위한 목적으로 고안되었습니다.

이를 통해 최대 수천 명의 사용자와 수십만 건의 활성 세션으로 확장되는, 지연 시간이 짧은 고속 정책 시행이 가능합니다.

외부 인증 및 권한부여 인터페이스

PEF는 권한부여 및 인증 서버에서부터 사용자에 대한 세밀한 제어를 확장합니다. 네트워크로부터의 자동 연결 해제, 역할 재할당, 방화벽 정책 동적 업데이트와 같은 제어 기능을 활성화할 수 있습니다.

이러한 기능은 두 가지 애플리케이션 프로그래밍 인터페이스(API)인 IETF 표준 RFC 3576과 단순하지만 유연한 XML 기반 API로 활성화됩니다. 이 두 API를 통해 외부 시스템은 Mobility Controllers에 대한 사용자 및 정책 제어권을 행사할 수 있습니다.

세 번째 통합 인터페이스인 syslog 프로세서는 외부 시스템에서 syslog 메시지를 받아들여 정규식 규칙 언어에 따라 처리한 후 사용자 역할 변경, 블랙리스트에 사용자 배치 등 구성 가능 조치를 제공합니다.

공격 대응 평균 시간 단축

VLAN 기반 네트워크 구성을 피하여 제어를 시행하면 IT 액세스 정책 구현에 필요한 리소스가 획기적으로 줄고 공격 대응을 자동화할 수 있습니다.

PEF의 세밀한 제어를 사용하면 합법적 자격증명을 공동 채택하고 네트워크 전체에 끈질기게 확산하는 내부 공격을 효과적으로 제압할 수 있습니다. 일련의 협소한 액세스 권한이 포함된 역할이 사용자 또는 디바이스에 있다면 공격자도 그럴 것입니다. 수평적 확산은 봉쇄됩니다.

데이터 반출 또는 랜섬웨어와 같은 공격이 감지되면 PEF는 역할을 변경하여 사용자 또는 디바이스와 연결된 권한을 자동으로 변경할 수 있습니다. 공격 대응에는 대역폭 축소, 검역, 전면 차단 등 다양한 조치가 포함될 수 있습니다. 공격에 대한 경고는 단순 API 통합에 따라 조직의 보안 생태계 내 어느 보안 제품에서도 발신될 수 있습니다.

CLEARPASS POLICY MANAGER와의 통합

Policy Enforcement Firewall은 자족적인 액세스 제어 솔루션으로서 선택적으로 아루바의 ClearPass Policy Manager와 통합할 수 있습니다. ClearPass는 규모에 따라 중앙집중형 시행을 위해 PEF에 제공되는 인증 및 정책 정의 서비스를 간소화할 수 있는 기능을 제공합니다. ClearPass의 주요 이점은 개별 사무실에서 글로벌 기업에 이르기까지 인증 및 권한부여 액세스 제어 기능을 통합할 수 있다는 것입니다.

또한 ClearPass는 모바일 디바이스 관리에서 ServiceNow와 같은 헬프 데스크 솔루션에 이르는 140개 이상의 Aruba 기술 파트너 솔루션을 통해 정책 통합, 역할 시행 및 공격 대응을 지원합니다.

최고 수준의 보안 인증

아루바의 Policy Enforcement Firewall(PEF)은 공통 평가 기준(CC) 및 DoDIN-APL에 따라 NIAP 공인을 받은 기술입니다. 또한 PEF는 NATO 승인 제품 목록에 포함되어 있습니다.

구현 편의성

IT가 자체 환경을 쉽게 구현하고 보호할 수 있도록 PEF는 컨트롤러 기반 인프라를 위한 Aruba 운영 체제 (AOS) 에서 개별적으로 라이선스가 부여된 소프트웨어 옵션으로 제공되며 컨트롤러 없는 액세스 포인트의 라이선싱에 포함되어 있습니다. 또한 다이나믹 세크멘테이션을 통해 아루바 네트워크 스위치에도 제공됩니다. 추가 하드웨어는 필요 없습니다.

요약

기존 방화벽은 액세스 달성 후 VLAN 기반 정책 시행을 사용하므로 IT 팀은 네트워크 연결 시점에 시작하는 공격에 맞춰 이를 무효화하느라 애를 먹습니다. 아루바의 PEF를 통한 사용자 방화벽 접근 방식은 위치, 연결 방법 또는 디바이스 유형에 상관없이 사용자 또는 디바이스의 ID 및 역할에 따라 네트워크 연결 시점에 제로 트러스트 경계를 제공하기 위해 설계된 유일한 액세스 제어 솔루션입니다.

PEF가 적용하는 세분화된 액세스 권한을 통해 조직은 손상된 사용자와 디바이스가 정밀 격리를 통해 공격에 참여하지 못하도록하고 공격이 탐지 될 때 엔드 포인트를 자동으로 차단하거나 격리 할 수 있습니다.

PEF는 기존 아루바 네트워크 인프라에서 소프트웨어 솔루션으로 구현되므로 식별되고 인증된 사용자 디바이스만 네트워크에 연결하도록 보장하기 위해 추가 하드웨어를 설치할 필요가 없습니다.

기능 요약	
기능	**이점**
완전 스테이트풀 레이어 4-7 애플리케이션 가시성	데이터 흐름을 양방향으로 제어하여 네크워크 에지에서 고유한 가시성 및 보안 제공
성능에 영향을 주지 않음	컨트롤러에서 트래픽 처리 속도가 저하되지 않음
사용자 방화벽	AllAllows 역할 기반 정책을 사용자, 디바이스 유형, 애플리케이션 또는 대상에 설정
UCC 대시보드	MOS와 같은 통화 품질과 Teams 및 SIP와 같은 UCC 서비스의 상태 확인
애플리케이션 인식 QoS	관리자가 애플리케이션 트래픽의 우선순위를 정하고 RF 레이어 동작을 제어할 수 있음
실시간 애플리케이션 대시보드	네트워크 모니터링 또는 문제해결을 위해 최상위 애플리케이션, 디바이스 및 대상을 실시간으로 추적
재사용할 수 있는 정책 라이브러리	관리자가 유용하고 일관성 있는 정책을 손쉽게 생성
과거 데이터 수집	애플리케이션 사용 및 용량 계획에 대한 장기 가시성을 위해 AirWave 사용
ClearPass 및 외부 RADIUS 통합	사용자를 인증하고, 제3자 장비 또는 ClearPass가 세부적인 디바이스 식별 및 동적 정책 업데이트를 할 수 있게 허용

Cyber Catalyst℠ 프로그램에서 선도적인 사이버 보험사는 사이버 위험을 줄이는 데 효과적이라고 생각하는 솔루션을 평가하고 식별합니다. 참여 보험사는 Allianz, AXIS, AXA XL(AXA의 사업 부문), Beazley, CFC, Munich Re, Sompo International, Zurich North America입니다. Microsoft는 이 프로그램의 기술 자문입니다.

a Hewlett Packard Enterprise company

© Copyright 2019 Hewlett Packard Enterprise Development LP. 이 문서에 수록된 내용은 통보 없이 변경될 수 있습니다. Hewlett Packard Enterprise 제품 및 서비스에 대한 유일한 보증은 해당 제품 및 서비스와 함께 동봉된 보증서에 명시되어 있습니다. 이 문서에 설명된 내용 중 어느 것도 추가적인 보증을 구성하는 내용으로 해석되어선 안 됩니다. Hewlett Packard Enterprise는 이 문서에 포함된 기술상 또는 편집상의 오류나 누락에 대해 책임지지 않습니다.

TB_PEF_090419 a00073442enw