aruba
a Hewlett Packard Enterprise company

TỔNG QUAN VỀ GIẢI PHÁP

CÁC ACCESS POINT LÀM NỀN TẢNG IOT

Kết nối các mạng IT và OT

SỰ PHÁT TRIỂN CỦA NỀN TẢNG

Sự ra đời của Wi-Fi 6 (802.11ax) đã mở rộng vai trò của Access Point (AP) để không chỉ đảm bảo khả năng kết nối Wi-Fi mà còn nâng cao khả năng hỗ trợ IoT mở rộng Wi-Fi 6, Bluetooth 5 , 802.15.4 (Zigbee) và tính năng của bên thứ ba qua cổng USB. Kết hợp lại, các ứng dụng mới như tìm đường, xác định địa lý, thông báo đẩy và theo dõi tài sản sẽ chuyển đổi các AP của Aruba thành các trung tâm giao tiếp đa chức năng, bảo mật, vừa là nền tảng Internet Vạn vật (IoT) truy cập mạng Internet chính thức.

ƯU ĐIỂM CỦA ARUBA

- Nhiều radio IoT và cổng USB linh hoạt hỗ trợ đa dạng ứng dụng IoT
- Khả năng định vị và phủ sóng lý tưởng cho các thiết bị IoT RF và IR
- Tối đa hóa tuổi thọ pin của các thiết bị IoT
- Các lựa chọn trong nhà, ngoài trời và ATEX Vùng 1
- Giảm sự phụ thuộc vào các cổng IoT đơn lẻ
- Giảm thiểu hoặc loại bỏ sự phức tạp của mạng meshi
- Hỗ trợ truyền đa giao thức, phân luồng linh hoạt, quản lý chính sách và phân tích bất thường tăng cường bảo mật IoT

Các Radio Wi-Fi 802.11ax

Truy cập mạng 802.11ax
Thẻ theo dõi tài sản
Biểu tượng định vị cá nhân
Băng đeo tay thông minh có cảm biến từ xa
Mũ bảo hiểm thông minh an toàn cho người lao động
Cảm biến, thiết bị truyền động và hệ thống chiếu sáng thông minh
Máy quét mã vạch và máy in di động

Sóng ZigBee 802.15.4

Cảm biến an toàn thực phẩm
Cảm biến nấu ăn và làm lạnh
Cảm biến hệ thống sưởi ấm, chất lượng không khí, hiện diện, an ninh, khẩn cấp, cuộc gọi, nút bấm, ánh sáng, rò rỉ
Bộ điều khiển tải và bộ truyền động
Hệ thống khóa cửa và ra vào

Sóng Bluetooth 5

Tính năng tìm đường và xác định địa lý
Các cảm biến: tiêu hao năng lượng cho hệ thống sưởi, chất lượng không khí, hiện diện, an ninh, hoảng loạn, cuộc gọi, nút bấm, ánh sáng, rò rỉ
Bộ điều khiển tải và thiết bị truyền động
Hệ thống khóa cửa và truy cập
Thẻ vị trí tài sản Ex và nhân sự chính xác cao

Cổng USB

Giao diện di động
Nhãn kệ điện tử
Máy dò súng
Trang bị thêm giao diện ZigBee cho các triển khai hiện có
Giao diện tùy chỉnh

Hình 1: Access Point Aruba Wi-Fi 6 làm nền tảng IoT

Tất cả các ứng dụng hệ thống tòa nhà sử dụng điện áp thấp - bao gồm các tính năng tiện ích, phát hiện xâm nhập, quản lý năng lượng, kiểm soát truy cập, theo dõi nhân sự và tài sản, nút gọi, phát hiện rò rỉ và thậm chí cả hệ thống giám sát súng - giờ đây có thể thực hiện một cách tin cậy và bảo mật thông qua các Access Point chuẩn Wi-Fi 6 của Aruba.

LỢI THẾ LÝ TƯỞNG

Với tính năng độc đáo có thể gắn trên trần nhà, tường và thậm chí dưới ghế ngồi, các AP có độ phủ bao quát, không bị cản trở tới tất cả các thiết bị lân cận, rất lý tưởng cho khả năng truyền sóng không dây.

Tốc độ bit giảm tương ứng với khoảng cách, do đó, để mang lại trải nghiệm tốc độ cao cho người dùng, các AP Wi-Fi 6 thường được đặt cách nhau 12-15 mét trong các khu vực mở và mỗi phòng sẽ có một điểm truy cập.

Khoảng cách này là phạm vi phủ sóng tối ưu cho các thiết bị RF IoT thu năng lượng và hoạt động bằng pin năng lượng thấp.

Nhiều thiết bị IoT gắn trên trần nhà cần một nguồn điện cục bộ, lý tưởng nhất là có pin dự phòng, khi các ổ cắm điện và thiết bị UPS rất ít khi xuất hiện trên trần của căn hộ.

Các AP của Aruba cung cấp một giải pháp đơn giản cho vấn đề nguồn điện IoT: cổng USB là một nguồn cung tiện lợi cho dữ liệu tốc độ cao cũng như điện năng mà không cần chạy cáp hoặc thiết bị mới.

Đối với các thiết bị sử dụng pin hoạt động trên nền tảng Wi-Fi, các AP Wi-Fi 6 của Aruba hỗ trợ cả Target Wake Time (TWT) và các thiết bị IoT kênh 20MHz. TWT tối đa hóa thời gian nghỉ của các thiết bị IoT lên đến vài ngày trước khi hoạt động, tăng thời lượng pin gấp 10 lần so với các công nghệ Wi-Fi trước đây. Với wake-up time được cân đối giữa thiết bị và điểm truy cập, TWT mang lại chế độ hoạt động chắc chắn, hiệu quả hơn. Hoạt động trên kênh 20MHz cho phép hoạt động ở chế độ năng lượng thấp hơn, từ đó kéo dài tuổi thọ pin. Và với khả năng hỗ trợ 1.000 thiết bị IoT trên mỗi điểm phát, các AP có thể mở rộng triển khai IoT ở mọi quy mô.

Các AP hỗ trợ IP-66/67 ứng dụng cho dải nhiệt độ rộng và vỏ bọc polycarbonate ATEX Zone 1 do đối tác cung cấp cho môi trường ngoài trời và vị trí nguy hiểm (hazloc). Vì vậy, bất kể chế độ triển khai IoT - trong nhà, ngoài trời hay vị trí nguy hiểm - Aruba đều hỗ trợ bạn.

Hình 2: Vỏ ngoài Bartec Polycarbonate ATEX Zone 1 cho môi trường IoT nguy hiểm

ĐƠN GIẢN VÀ ĐÁNG TIN CẬY

Các Access Point Wi-Fi 6 loại bỏ nhu cầu về Gateway bằng cách liên kết trực tiếp với các thiết bị IoT và truyền dữ liệu hai chiều đến các ứng dụng mục tiêu. Việc loại bỏ các thiết bị trung gian giúp giảm độ phức tạp và chi phí của hệ thống, tăng độ tin cậy của toàn hệ thống và loại bỏ yếu tố bề mặt nhạy cảm, dễ bị tấn công.

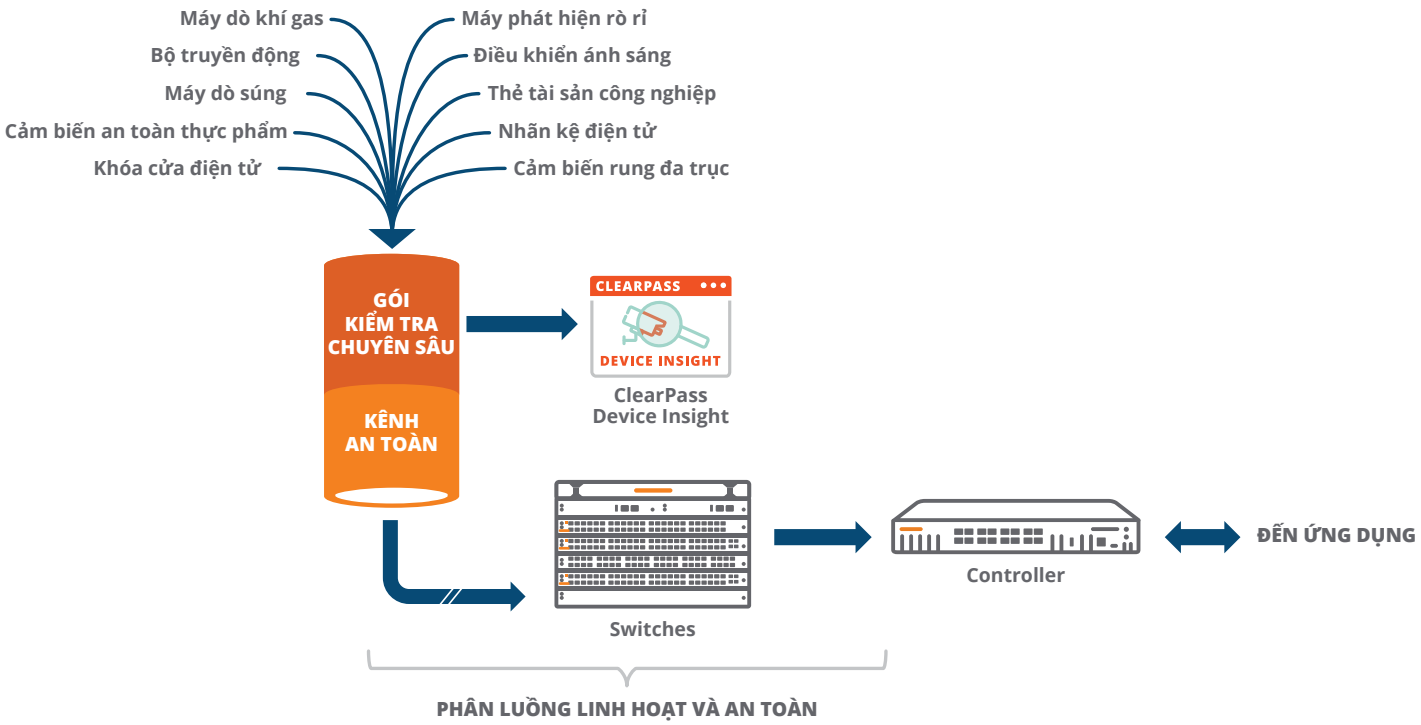
Bằng cách liên kết trực tiếp với các thiết bị IoT, các AP cũng có thể giảm kích thước cụm của mạng lưới IoT, nếu không muốn nói là loại bỏ chúng hoàn toàn. Mạng lưới backhaul tăng cấp số nhân băng thông sử dụng trong việc truyền IoT - hiệu ứng là tác nhân lớn trong các băng tần ISM 900MHz và 2.4GHz bị tắc nghẽn. Việc loại bỏ các mạng lưới RF hoặc cho phép chúng hoạt động trong các cụm nhỏ hơn, bảo toàn băng thông và giảm thiểu ảnh hưởng đến các thiết bị IoT khác hoạt động trên cùng tần số. Điều này có lợi ích bổ sung là tăng tuổi thọ pin của các thiết bị IoT, các thiết bị này không cần phải truyền lại các gói xử lý ngược thường xuyên, nếu có.

GIẢI QUYẾT CÁC THỬ THÁCH BẢO MẬT CHO IOT

Các thiết bị IoT là mục tiêu tấn công vì chúng hiếm khi được tích hợp khả năng bảo mật cao, xác thực mạnh, tính năng lưu trữ mật khẩu rõ ràng do những hạn chế trong nỗ lực tiết kiệm chi phí sản xuất, khả năng tính toán hạn chế hoặc sự cẩu thả trong các thiết kế. Các thiết bị IoT thường được đặt ở các khu vực công cộng và dễ bị thăm dò, thao túng và xâm nhập. Do đó, ưu tiên hàng đầu của các doanh nghiệp là thận trọng đánh giá sự tin cậy an ninh thiết bị IOT cũng như đưa ra các phương án an toàn để giảm thiểu tối đa các vụ tấn công vào các thiết bị này

Kết nối lưu lượng IoT thông qua các AP và switches của Aruba cho phép nhiều cơ chế bảo mật chủ động và thụ động để bảo vệ các thiết bị IoT và lưu lượng của chúng. Các Modules Trusted Platform tích hợp trong AP lưu trữ thông tin truy cập nên việc thăm dò một AP sẽ không thể tìm kiếm được các chi tiết xác thực, ủy quyền hay mã hóa. Dữ liệu từ thiết bị ITO sẽ được truyền một cách an toàn từ AP đến các thiết bị quản trị Aruba tại chỗ, virutal hay đám mây mà không cần có sự điều khiển trực tiếp.

Các quyết định được đưa ra dựa trên chính sách phân quyền theo vai trò và quyền truy cập sẽ giúp phân khúc lưu lượng từ AP tới các thiết bị mục tiêu một cách đơn giản, không cần cấu hình mạng phức tạp hay VLAN. Cơchế Policy Enforcement Firewall được tích hợp sẵn của Aruba sẽ tự động thực hiện kiểm tra chuyên sâu đối với các lưu lượng truy cập bị đánh giá chứa nhiều rủi ro. Ví dụ, một camera an ninh có thể bị giới hạn chỉ giao tiếp với các tài nguyên mạng thực sự cần thiết để thực hiện chức năng chụp và lưu trữ video



Hình 3: Kênh bảo mật thiết bị IoT

Tính năng ClearPass Device Insight của Aruba ghi dấu các thiết bị để phần mềm ClearPass Policy Manager của Aruba có thể tự động chỉ định các chính sách phù hợp với các thiết bị. Trong trường hợp thiết bị có các Chỉ số Thỏa hiệp (IoC), quyền truy cập có thể bị hạn chế đáng kể hoặc thiết bị có thể bị cách ly hoàn toàn khỏi mạng.

Các nhà cung cấp IoT bỏ qua kênh bảo mật bằng cách sử dụng mạng LoRa, khiến doanh nghiệp gặp rủi ro do định tuyến lưu lượng truy cập xung quanh các cơ chế bảo vệ tốt nhất. Do đó, các thiết bị bị nhiễm hoặc bị xâm nhập có thể không được chú ý.

NỀN TẢNG CỦA TƯƠNG LAI

Gartner ước tính rằng vào khoảng năm 2022 sẽ không có sự khác biệt đáng chú ý giữa các thiết bị CNTT và IoT do sự phổ biến rộng rãi của các thiết bị IoT trên cơ sở hạ tầng CNTT. Để các hoạt động chính xác và đáng tin cậy hơn, với các chính sách bảo mật đồng nhất và khả năng hiển thị trên cả thiết bị CNTT và IoT, ta cần có một cách tiếp cận mới về việc triển khai hệ thống. Các thiết bị AP chuẩn Wi-Fi 6 giàu tính năng của Aruba là nền tảng được lựa chọn cho sự chuyển đổi đó.

Tìm hiểu thêm về Aruba Access Points .

a Hewlett Packard Enterprise company

SO_APasIOTPlatforms_SK_061720 a00097094enw