aruba
a Hewlett Packard Enterprise company

TỔNG QUAN GIẢI PHÁP

Aruba ESP với Zero Trust Security

Bảo mật cho môi trường Biên (Edge)

Những thách thức về an ninh mạng đã gia tăng đáng kể trong những năm gần đây khi người dùng ngày càng bị phân quyền và các cuộc tấn công trở nên tinh vi và dai dẳng hơn. Bên cạnh đó, các phương pháp bảo mật truyền thống, chỉ chủ yếu tập trung xung quanh của hệ thống mạng, không còn hiệu quả dưới dạng là các chiến lược bảo mật độc lập. Vì vậy, an ninh mạng hiện đại phải phù hợp với đa dạng nhóm người dùng chuyên nghiệp và thiết bị luôn thay đổi, cũng như việc nhiều mối đe dọa phổ biến đang nhắm vào các phần "đáng tin cậy" trước đây của cơ sở hạ tầng mạng.

Giải pháp Zero Trust nổi lên như một mô hình hiệu quả để giải quyết tốt các yêu cầu bảo mật đang thay đổi cho doanh nghiệp hiện đại, có khả năng giả định để nghi ngờ tất cả người dùng, thiết bị, máy chủ và các phân đoạn mạng (network segment) không an toàn. Bằng cách này, Aruba ESP với Zero Trust Security có thể cải thiện tình hình an ninh mạng tổng thể bằng cách áp dụng một tập hợp các biện pháp kiểm soát và thực tiễn tốt nhất, mang đến khả năng bảo mật nghiêm ngặt hơn cho các tài nguyên mạng quan trọng trước đây.

ARUBA ESP: NGUYÊN TẮC KHÔNG TIN TƯỞNG CỐT LÕI

Giải pháp bảo mật Zero Trust mang đến sự thay đổi đáng kể cho hệ thống mạng, tuỳ thuộc vào miền (domain) bảo mật đang được xem xét. Mặc dù kiểm soát cấp ứng dụng là trọng tâm trong Zero Trust, nhưng một chiến lược toàn diện cũng cần phải bao quát hệ thống an ninh mạng và số lượng thiết bị kết nối ngày càng tăng, bao gồm môi trường làm việc tại nhà. Do đó, Giải pháp Aruba ESP với Zero Trust Security sẽ kết hợp chặt chẽ khả năng hiển thị toàn diện, kiểm soát và phân đoạn vi mô (Micro Segmentation) quyền truy cập tối thiểu, cũng như giám sát và thực thi liên tục, mang đến giải pháp bảo mật đáng tin cậy nhất. Ngay cả các giải pháp VPN truyền thống cũng được cải tiến bằng cách đảm bảo rằng các điều khiển tương tự, được áp dụng cho hệ thống mạng tại toà nhà (campus), các chi nhánh, hoặc được mở rộng cho nhân viên làm việc tại nhà hoặc từ xa.

Trong thời đại IoT, nguyên tắc cơ bản của an ninh mạng được đánh giá tốt, thường khó có thể thực hiện. Khi có thể, tất cả các thiết bị và người dùng phải được hệ thống nhận dạng và xác thực đúng cách trước khi cấp cho họ quyền truy cập mạng. Ngoài việc xác thực, người dùng và thiết bị cũng cần được cung cấp tối thiểu các quyền truy cập cần thiết, để thực hiện các hoạt động quan trọng đối với doanh nghiệp khi họ trực tuyến. Điều này có nghĩa là cấp phép tài nguyên mạng và ứng dụng mà bất kỳ người dùng hoặc thiết bị nhất định nào cũng có thể truy cập. Cuối cùng, tất cả mọi phương tiện liên lạc giữa người dùng cuối và ứng dụng phải được mã hóa.

SỰ CẦN THIẾT CỦA KHẢ NĂNG HIỂN THỊ TOÀN DIỆN

Việc IoT ngày càng được chấp thuận và thông qua IoT dẫn đến khả năng hiển thị toàn diện tất cả thiết bị và người dùng trên hệ thống mạng trở thành một nhiệm vụ đầy thách thức. Nếu không có khả năng hiển thị toàn diện, các biện pháp kiểm soát bảo mật quan trọng hỗ trợ cho mô hình Zero Trust rất khó áp dụng. Khi đó, tự động hóa, học máy (machine learning) dựa trên trí tuệ nhân tạo AI, cũng như khả năng xác định nhanh các loại thiết bị là các tính năng rất quan trọng.

Giải pháp Aruba ClearPass Device Insight vận dụng sự kết hợp giữa kỹ thuật khám phá và lập hồ sơ chủ động lẫn thụ động nhằm phát hiện toàn bộ các thiết bị được kết nối hoặc cố gắng kết nối vào hệ thống mạng. Giải pháp này có thể áp dụng với các thiết bị phổ biến trong người dùng như máy tính xách tay hay máy tính bảng. Điểm khác biệt của Aruba ClearPass Device Insight so với công cụ truyền thống là khả năng nhìn thấy được nhiều bộ thiết bị IoT đa dạng khác nhau đang thâm nhập khắp các hệ thống mạng hiện nay.

LỰA CHỌN "TRUY CẬP TỐI THIỂU" VÀ PHÂN ĐOẠN VI MÔ

Một khi đã có khả năng hiển thị, việc áp dụng các phương pháp tốt nhất của Zero Trust liên quan đến "Truy cập tối thiểu" (Least Access) và phân đoạn vi mô (Micro Segmentation) được xem là các bước quan trọng tiếp theo. Điều này có nghĩa là sử dụng phương pháp xác thực tốt nhất có thể cho mỗi điểm cuối trên mạng (tức là xác thực đầy đủ 802.1X và đa yếu tố cho thiết bị của người dùng) và áp dụng chính sách kiểm soát truy cập chỉ cho quyền duy nhất truy cập vào các tài nguyên thực sự cần thiết cho thiết bị hoặc người dùng đó.

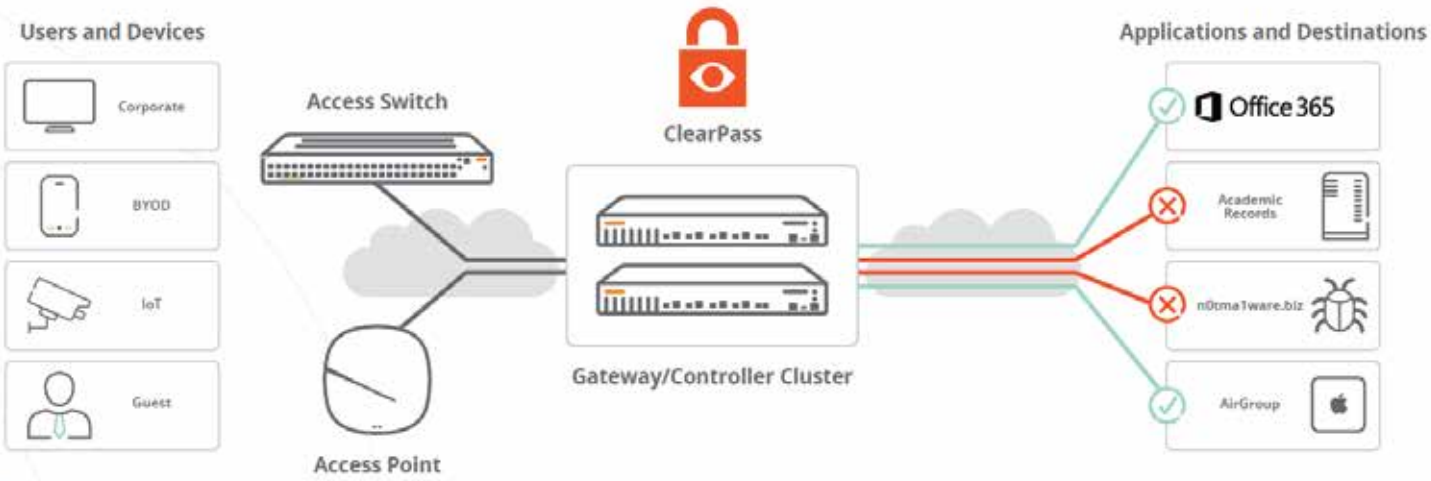
Aruba ClearPass Policy Manager cho phép tạo các chính sách truy cập dựa trên vai trò cho phép của các nhóm CNTT và bảo mật để vận hành các phương pháp tốt nhất này thông qua việc sử dụng một vai trò duy nhất và các đặc quyền truy cập liên quan - có thể được áp dụng tại mọi nơi trên hệ thống mạng, từ cơ sở hạ tầng có dây hoặc không dây, trong chi nhánh hay trong khuôn viên toà nhà (campus). Sau khi được lập hồ sơ, các thiết bị sẽ tự động được chỉ định chính sách kiểm soát truy cập thích hợp, đồng thời được phân đoạn khỏi các thiết bị khác thông qua tính năng Aruba Dynamic Segmentation. Khả năng thực thi được cung cấp bởi Aruba's Policy Enforcement Firewall (PEF), một tường lửa ứng dụng đầy đủ được nhúng trong cơ sở hạ tầng mạng Aruba. Cơ sở hạ tầng Aruba cũng tận dụng các giao thức mã hóa an toàn nhất như tiêu chuẩn WPA3 trên các kết nối mạng không dây.

ClearPass Policy Manager cũng tích hợp nhiều giải pháp xác thực, cho phép sử dụng xác thực đa yếu tố và khả năng buộc xác thực lại tại các điểm chính trong toàn hệ thống mạng. Thông qua hệ sinh thái ClearPass, khách hàng cũng có thể dễ dàng kết hợp với các giải pháp khác để đáp ứng các yêu cầu của Zero Trust liên quan đến thông tin theo ngữ cảnh và khả năng đo từ xa bảo mật khác.

Điều này đồng nghĩa việc ClearPass có thể tích hợp với cả nhiều giải pháp khác nhau, chẳng hạn như công cụ Bảo mật điểm cuối (Endpoint Security) nhằm đưa ra các quyết định kiểm soát truy cập thông minh hơn dựa trên tình trạng của thiết bị. Chính sách kiểm soát truy cập cũng có thể được thay đổi dựa trên loại thiết bị đang được sử dụng, vị trí của người dùng đang kết nối và các tiêu chí dựa trên ngữ cảnh khác.

THEO DÕI VÀ THỰC THI LIÊN TỤC

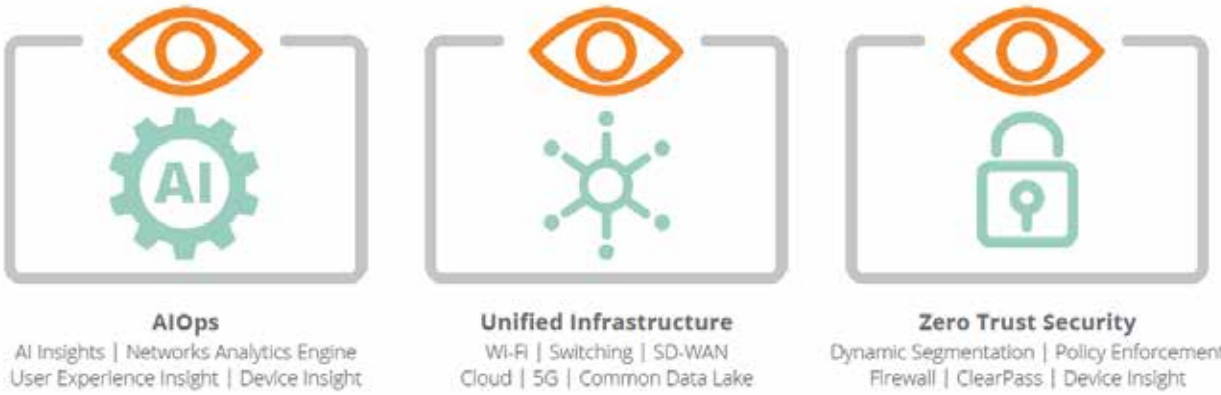
Với tính năng kiểm soát truy cập dựa trên vai trò để thực thi phân đoạn chi tiết, việc giám sát liên tục người dùng và thiết bị trên hệ thống mạng tạo nên một phương pháp tốt nhất khác của Zero Trust. Điều này giúp giải quyết rủi ro liên quan đến các mối đe dọa nội gián, phần mềm độc hại nâng cao hoặc các mối đe dọa dai dẳng đã phá vỡ các biện pháp phòng thủ truyền thống.



Hình 1: Aruba ClearPass tự động chỉ định các chính sách kiểm soát truy cập dựa trên vai trò được thực thi bằng cách sử dụng Dynamic Segmentation

NỀN TẢNG ARUBA ESP (EDGE SERVICES PLATFORM)

Nền tảng đầu tiên trong ngành dùng giác quan thứ 6 hỗ trợ bởi AI để tự động hóa và bảo vệ



Hình 2: Giải pháp Zero Trust Security là một trụ cột chính của Aruba ESP

Phòng thủ trước các mối nguy hại với IDS/IPS

Khả năng phòng thủ của Aruba có thể chống lại vô số mối đe dọa, bao gồm tấn công lừa đảo (Phishing), từ chối dịch vụ (DoS) và các cuộc tấn công ransomware khác đang ngày càng lan rộng. Cụ thể, giải pháp Aruba 9000 SD-WAN Gateway có khả năng phát hiện và ngăn chặn xâm nhập trái phép dựa trên nhận dạng (IDS/IPS), hỗ trợ hoạt động cùng Aruba Central, ClearPass Policy Manager và Policy Enforcement Firewall. Nhận dạng IDS/IPS sẽ thực hiện kiểm tra lưu lượng dựa trên thông tin xác thực và mẫu thiết bị trên lưu lượng mạng LAN (east-west) của văn phòng chi nhánh, cũng như lưu lượng SD-WAN (north-south) đi qua cổng (gateway) để cung cấp bảo mật mạng chi nhánh dạng nhúng. Bảng điều khiển bảo mật nâng cao trong Aruba Central cung cấp cho các nhóm CNTT khả năng hiển thị trên toàn mạng, số liệu mối đe dọa đa chiều, dữ liệu tình báo về mối đe dọa, cũng như quản lý tương quan và sự cố. Các sự kiện đe dọa được gửi đến hệ thống SIEM và ClearPass để khắc phục.

Trao đổi bảo mật 360 độ

Với hơn 150 mô-đun tích hợp được tạo thành từ các giải pháp bảo mật tốt nhất, bao gồm cả bộ công cụ Security Operations and Response (SOAR), ClearPass Policy Manager có thể tự động thực thi quyền truy cập dựa trên phép đo từ xa mối đe dọa theo thời gian thực đến từ nhiều nguồn. Các chính sách có thể được tạo nhằm đưa ra quyết định kiểm soát truy cập theo thời gian thực, dựa trên các cảnh báo đến từ các công cụ Next-Gen Firewalls (NGFW), Security Information and Event Management (SIEM) và nhiều nguồn khác. Các hành động ClearPass hoàn toàn có thể được định cấu hình, từ việc giới hạn quyền truy cập (tức là chỉ Internet) cho đến việc xóa hoàn toàn thiết bị khỏi mạng để khắc phục sự cố.

NỀN TẢNG ARUBA ESP (EDGE SERVICES PLATFORM)

Để giúp khách hàng tận dụng các cơ hội tại môi trường Biên (Edge), chúng tôi đã phát triển Aruba ESP, nền tảng hỗ trợ AI đầu tiên trong ngành, được thiết kế để hợp nhất, tự động hóa và bảo mật cho môi trường Biên (Edge). Giải pháp Zero Trust Security là một yếu tố then chốt của Aruba ESP, và khi được kết hợp với AIOps và Cơ sở hạ tầng hợp nhất, cho phép các tổ chức giảm chi phí, đơn giản hóa hoạt động vận hành và giữ an toàn.

TÓM LƯỢC

Môi trường mạng và bối cảnh mối đe dọa ngày nay đã và đang đòi hỏi một cách tiếp cận mới. An ninh mạng tập trung trong phạm vi khuôn viên trước đây không còn phù hợp cho lực lượng nhân sự di động hiện nay hoặc các thiết bị IoT thế hệ mới. Giải pháp Aruba ESP với Zero Trust Security cung cấp một tập hợp toàn diện, mở rộng khả năng hiển thị, kiểm soát và thực thi để giải quyết các yêu cầu của cơ sở hạ tầng mạng phi tập trung, định hướng IoT.