"Đánh giá thiết bị" (Device Posture) là gì?

Khi một thiết bị (laptop, điện thoại, máy tính bảng...) kết nối vào mạng công ty, không phải cứ có mật khẩu là được truy cập. Thiết bị đó còn phải được đánh giá xem có an toàn không — điều này gọi là posture assessment.

👉 Ví dụ: Công ty yêu cầu thiết bị phải có antivirus được bật, tường lửa đang chạy, Windows phải được cập nhật bản vá mới nhất... Nếu thiết bị không đạt, thì dù bạn có đúng username/password, bạn vẫn bị từ chối truy cập.

Hai thành phần chính trong Posture:

1. Posture (Thu thập thông tin)
- Có bật antivirus không?
- Có cài bản vá bảo mật mới nhất không?
- Có đang chia sẻ file trái phép không?
- Có chạy phần mềm quản lý thiết bị (MDM) không?

Posture có thể được thu thập qua:
- Option 1: Device Manager – hệ thống quản lý thiết bị đầu cuối (như Intune, Jamf, hoặc phần mềm bảo mật nội bộ).
- Option 2: Cisco AnyConnect + ISE Posture module – một agent trên thiết bị, tự động gửi posture về cho Cisco ISE đánh giá.

2. Assessment (Đánh giá và xử lý)

Cisco ISE (Identity Services Engine) hoặc hệ thống NAC sẽ đánh giá dữ liệu posture đó:

- ✅ Nếu đạt chuẩn → cấp quyền truy cập bình thường theo chính sách Access Policy.
- ❌ Nếu không đạt → đưa vào VLAN cách ly, yêu cầu remediation (ví dụ: cài bản vá, bật antivirus…).

Lợi ích của Posture Assessment

- Bảo vệ mạng nội bộ khỏi thiết bị không an toàn.
- Hạn chế lây lan malware, ransomware.
- Tự động hóa kiểm tra và phản hồi.
- Kết hợp mạnh mẽ với mô hình Zero Trust — “Never Trust, Always Verify”.

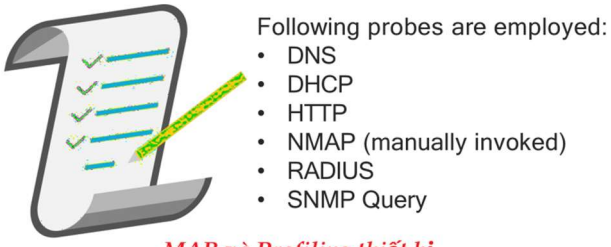
Ví dụ thực tế

Một nhân viên từ xa kết nối VPN về công ty. AnyConnect trên máy họ sẽ tự động thực hiện kiểm tra posture:
→ Nếu máy tính bị tắt Windows Update hoặc hết hạn antivirus, họ sẽ không vào được các tài nguyên nội bộ cho đến khi khắc phục.

MAB Authentication, Profiling & Trusted Devices – Bạn đã làm đúng cách?

MAB Authentication & Profiling: Không chỉ là MAC

Khi triển khai kiểm soát truy cập mạng (NAC), rất nhiều hệ thống trong doanh nghiệp vẫn còn phụ thuộc vào các thiết bị không hỗ trợ 802.1X – ví dụ: máy in, camera, điện thoại IP hoặc thiết bị IoT. Lúc này, ta cần đến một kỹ thuật gọi là MAB (MAC Authentication Bypass) – tức xác thực theo địa chỉ MAC. Tuy nhiên, nếu chỉ dựa vào MAC thì cực kỳ rủi ro. Vì vậy, Cisco cung cấp cơ chế Device Profiling để tăng mức độ tin cậy.



MAB và Profiling thiết bị

✅ Trường hợp ngoại lệ: Nếu MAC được gán tĩnh cho một endpoint group (ví dụ: bạn đã phân loại MAC đó là máy in cố định), thì không cần profile động.

Yêu cầu tối thiểu khi profiling:

- Phải có ít nhất một thuộc tính "đáng tin cậy" (trusted attribute).

- Và thêm một hoặc nhiều thuộc tính có mức độ tin cậy cao (high confidence).

Ví dụ thực tế: Với thiết bị họp trực tuyến Cisco TP, CDP có thể chỉ ra loại thiết bị và Cisco OUI giúp xác định nhà sản xuất – được xem là “trusted attributes”.

Các probe được sử dụng để thu thập dữ liệu profiling:

- DNS
- DHCP
- HTTP
- NMAP (phải chạy thủ công)

- RADIUS
- SNMP Query

Profiling – Giải quyết bài toán TCAM khi áp ACL

Khi triển khai dACL (downloadable ACLs) hoặc redirect ACLs để kiểm soát lưu lượng theo người dùng, chúng ta gặp giới hạn nghiêm ngặt về kích thước:
- Giống như ACL gán theo người dùng (per-user ACL)
- Giới hạn chỉ 4000 ký tự ASCII

Nếu ta áp cùng một ACL cho tất cả loại thiết bị, dung lượng ACL sẽ "nổ tung" vì phải chứa đủ luật phù hợp cho mọi loại thiết bị khác nhau. Đây là nguyên nhân gây "cháy TCAM" – vùng bộ nhớ phần cứng trên switch để xử lý ACLs.

📌 Giải pháp: Sử dụng profiling để phân loại thiết bị, từ đó áp ACL riêng cho từng loại endpoint:

- ACL riêng cho thiết bị Windows
- ACL riêng cho thiết bị Linux
- ACL riêng cho thiết bị Cisco
- ACL riêng cho thiết bị lạ hoặc IoT

Cách này giúp:
- Tối ưu hóa dung lượng TCAM
- Áp đúng chính sách phù hợp với từng loại thiết bị
- Tăng bảo mật và hiệu quả kiểm soát truy cập

☑ Posture & Trusted Device: Thế nào là thiết bị đáng tin?

Không chỉ xác định thiết bị là gì, hệ thống NAC còn đánh giá posture – trạng thái bảo mật của thiết bị. Đây là tiêu chí rất quan trọng để xác định xem thiết bị có nên được cấp quyền truy cập mạng không.

Một thiết bị "trusted" cần đạt các tiêu chí:

1. Đã đăng ký (Device Registration)
2. Có phần mềm chống mã độc (Anti-Malware)
3. Mã hóa dữ liệu (Encryption) theo chính sách Cisco
4. Đang chạy OS tối thiểu (Minimum OS)
5. Đã cập nhật bản vá (Patching) mới nhất
6. Hỗ trợ xóa dữ liệu từ xa (Remote Wipe) – với thiết bị di động
7. Có thiết lập khóa màn hình hoặc mật khẩu

8. Hiển thị thông tin phần cứng/phần mềm (Inventory)
9. Không bị root (với thiết bị di động)

💡 Khi bạn bật tính năng Posture trên Cisco ISE (kết hợp với AnyConnect Secure Client), hệ thống sẽ quét và đánh giá thiết bị theo các tiêu chí trên. Chỉ khi thiết bị được đánh giá "trusted", hệ thống mới cấp full access – nếu không thì chuyển vào VLAN cách ly hoặc Portal Remediation.

📌 Tổng kết

- MAC không phải là tất cả: Dùng MAB thì phải profile!
- Đừng lãng phí TCAM: Dùng profiling để phân loại và áp ACL riêng.
- Posture mới là bảo mật thực sự: Không "trusted" thì không nên được vào mạng nội bộ.

Nếu bạn đang triển khai Cisco ISE hoặc đang vận hành mạng LAN bảo mật, hãy đảm bảo bạn hiểu rõ vai trò của MAB + Profiling + Posture. Đây là ba trụ cột trong Zero Trust Network Access (ZTNA) dành cho hạ tầng truyền thống.