Network Segmentation

**I. Khái niệm:**

+ Là một thiết kế kiến trúc mạng chia mạng thành nhiều phân đoạn (mạng con- subnet) với mỗi phân đoạn hoạt động như một mạng riêng lẻ nhỏ hơn.

+ Phân đoạn (Segmentation) hoạt động bằng cách kiểm soát luồng lưu lượng trong mạng.

**II. Cách hoạt động**

- Phân đoạn mạng chia mạng thành nhiều vùng và quản lý từng vùng hoặc phân đoạn riêng lẻ. Điều này nghĩa là áp dụng các giao thức lưu lượng để quản lý lưu lượng được và không được đi qua.

- Các phân đoạn mạng được chỉ định bằng phần cứng chuyên dụng riêng để ngăn cách với nhau. Sẽ chỉ truy cập được khi người dùng được xác thực. Các quy tắc sẽ được tích hợp vào cấu hình mạng để xác định cách người dùng, dịch vụ và thiết bị trên mạng được kết nối với nhau

**III. Các loại Network Segment:**

- Physical Segment:

+ Sử dụng các phần cứng chuyên dụng để xây dựng các phân đoạn mạng (firewall, router, switch)

+ Còn được gọi là phân đoạn dựa trên chu vi (perimeter-based segmentation) do mỗi phân đoạn đều cần kết nối Internet, hệ thống dây điện vật lý và tường lửa riêng

+ Phân đoạn này làm việc dựa trên sự tin cậy: Mọi thứ bên trong đều đáng tin cậy, những thứ bên ngoài thì không

+ Không an toàn (nếu thiết bị phần cứng dùng để phân đoạn bị vượt qua, tin tặc có thể tự do di chuyển bên trong ), khó quản lý

- Virtual Segment:

+ Phân đoạn mạng ảo bao trùm toàn bộ mạng. Switch quản lý môi trường mạng cục bộ ảo và tường lửa được chia sẻ, giảm phần cứng cần thiết. Phân đoạn dựa trên chu vi hiện đã được ảo hóa và phân phối, đồng thời các chính sách bảo mật cụ thể và chi tiết hơn

**IV. Mô hình Network Segment:**

A diagram of a network segmentation

Description automatically generated

**V. Cách triển khai:**

1. Thực hiện kiểm kê:

+ Có những hệ thống gì, ai là người có quyền truy cập, …

2. Nhận diện người cần sử dụng dữ liệu:

+ Giúp triển khai hệ thống bằng cách chỉ cấp quyền truy cập cho những người cần nó

3. Xem xét những thứ chiếm dụng băng thông:

+ Xem xét nhằm tránh những ứng dụng lớn chiếm nhiều dung lượng làm chậm dung lượng khác

4. Thiết kế một mạng phân đoạn:

+ Các phân đoạn có thể được thiết kế sau khi khám phá những người dùng nào cần quyền truy cập vào dữ liệu và hệ thống cụ thể.

5. Bắt đầu với những phân đoạn nhỏ và dễ nhất:

+ Quản trị viên có thể thực hành và tìm hiểu trên các phân đoạn ít phức tạp hoặc ít phụ thuộc hơn

6. Quy tắc từ chối mặc định:

+ Tuân theo cơ sở cấu hình tường lửa này, từ chối quyền truy cập vào mọi thứ chưa được cho phép rõ ràng.

7. Xem các thay đổi thường xuyên:

+ Đảm bảo rằng các thay đổi không vi phạm cấu hình phân đoạn

8. Giám sát chặt chẽ:

+ Chú ý đến mọi thứ, từ các ứng dụng hoạt động kém đến lưu lượng truy cập mạng bất thường. Quản trị viên nên xem lại nhật ký hàng ngày và phân tích chúng để phát hiện hành vi đáng ngờ hoặc bất thường.

VI. Một số kiểu phân đoạn khác

* Firewall Segment:A diagram of a computer process

  Description automatically generated

+ Sử dụng tường lửa để Segment

+ Tường lửa sẽ triển khai bên trong mạng hoặc cơ sở dữ liệu nhằm tạo các khu vực nội bộ riêng biệt. Ở từng khu vực nội bộ sẽ có chức năng và nhiệm vụ khác nhau

* Segment with SDN:

A diagram of a computer network

Description automatically generated

* Micro-Segment:

A diagram of a computer application

Description automatically generated

+ là kỹ thuật mạng giúp các kỹ sư bảo mật chia trung tâm dữ liệu thành những Segment nhỏ tách biệt với nhau. Sau đó các kỹ sư có thể tạo lập các biện pháp kiểm soát bảo mật riêng biệt và cung cấp dịch vụ riêng biệt cho từng Segment một

+ Hình thức phổ biến: iptables (Linux), Windows Filtering Platform (Windows)

+ Micro-Segment chia nhỏ hơn so với Network Segment, các tác vụ như web, application, database,… đều được phân đoạn

\*\* (Thắc mắc thêm)

1. Cách dữ liệu di chuyển trong Network Segment:

+ Truyền từ thiết bị nguồn đến switch:

\* Khi một thiết bị (máy tính) trong segment gửi dữ liệu, dữ liệu này sẽ đi qua switch

\* Switch hoạt động ở layer 2 của mô hình OSI, nơi nó đọc địa chỉ MAC của thiết bị đích để quyết định gửi dữ liệu đến đúng cổng

\* Switch cũng có thể sử dụng VLAN để phân tách các mạng logic, đảm bảo dữ liệu chỉ di chuyển trong phân đoạn nó thuộc về trừ khi có yêu cầu ra khỏi phân đoạn

+ Chuyển dữ liệu giữa các Segment:

\* Nếu dữ liệu cần di chuyển giữa các segment khác nhau (ví dụ, từ một VLAN này sang một VLAN khác), nó sẽ đi qua một router hoặc Layer 3 switch

\* Router đọc địa chỉ IP đích trong gói tin và quyết định tuyến đường tối ưu để gửi dữ liệu đến đúng segment đích.

+ kiểm tra, lọc bởi Firewall

\* Dữ liệu cũng có thể đi qua firewall trước khi rời khỏi hoặc đi vào một segment khác

\* Firewall kiểm tra dữ liệu dựa trên các quy tắc bảo mật, quyết định chặn hoặc cho phép dữ liệu đi qua.

\* Firewall có thể làm việc ở tầng 3 (kiểm tra địa chỉ IP) hoặc tầng 4 (kiểm tra số cổng), và một số firewall nâng cao cũng làm việc ở tầng ứng dụng (tầng 7).

+ Truyền qua các thiết bị bảo mật khác

\* Nếu hệ thống có các thiết bị bảo mật khác như IDS/IPS, dữ liệu có thể được kiểm tra thêm để phát hiện các hành vi bất thường hoặc các mối đe dọa tiềm ẩn.

\* IDS/IPS sẽ phân tích các gói tin để tìm kiếm các dấu hiệu tấn công và có thể ngăn chặn dữ liệu nếu phát hiện thấy mối đe dọa.

+ Di chuyển đến đích

\* Sau khi qua các bước trên, dữ liệu sẽ đến đúng thiết bị đích trong segment khác, hoặc trở lại trong cùng một segment nếu là dữ liệu nội bộ.