**\* FIREWALL**

I. Khái niệm

+ Là phần cứng hoặc phần mềm được thiết kế để bảo vệ sự xâm nhập trái phép từ mạng các nhân (private network)

+ Đặt tại giao điểm (junction) hoặc cổng giữa hai mạng thường là một mạng riêng và một mạng chung (Internet)

+ Tường lửa kiểm tra tất cả các tin nhắn vào hoặc ra khỏi mạng nội bộ và chặn những tin nhắn không đáp ứng các tiêu chí bảo mật đã được chỉ định

+ Tưởng lửa có thể quan tâm đến loại lưu lượng truy cập hoặc đến địa chỉ và cổng nguồn hoặc đích

+ Mô hình:

A computer screen shot of a firewall

Description automatically generated

II. Kiến trúc

+ Bastion Host:

* Là một hệ thống máy tính được thiết kế và cấu hình nhằm bảo vệ các tài nguyên mạng khỏi các cuộc tấn công
* Lưu lượng ra vào mạng qua firewall có 2 giao diện:

+ Giao diện công cộng (public interface) được kết nối trực tiếp với Internet

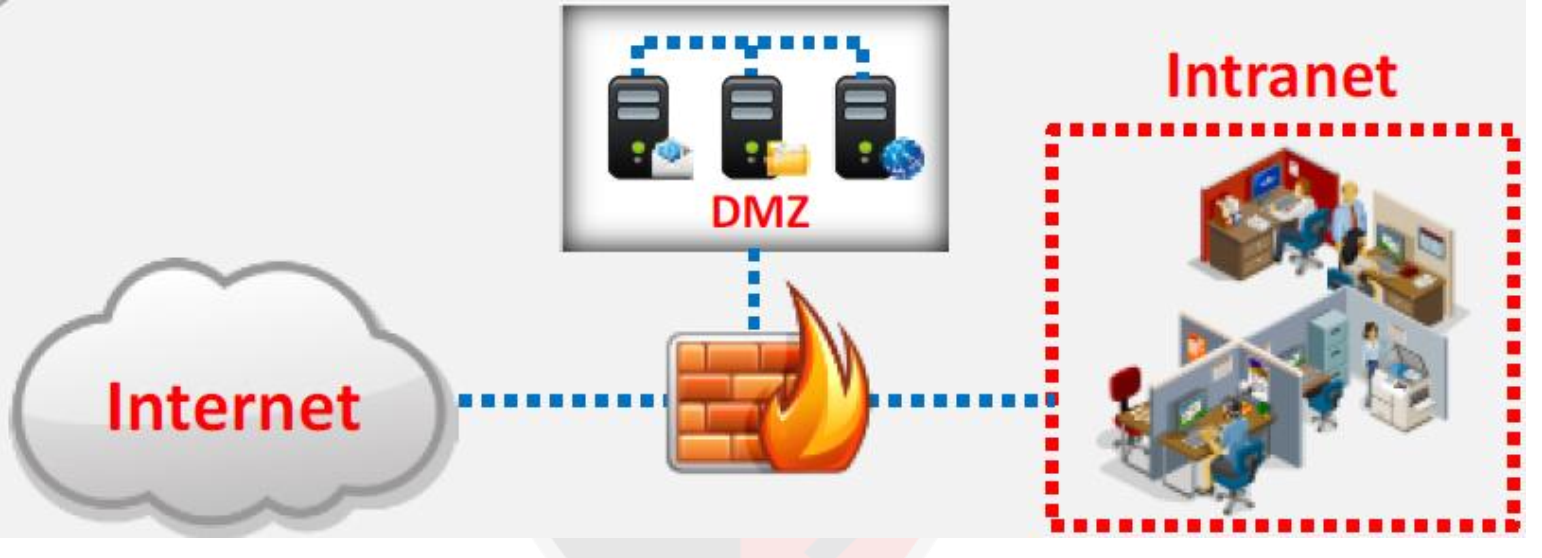
+ Giao diện riêng tư (private interface) kết nối đến Intranet

A computer server and firewall

Description automatically generated

+ Screened Subnet or DeMilitarized Zone:

* The screened Subnet or DMZ (additional zone) bao gồm các máy chủ (hosts) cung cấp dịch vụ công cộng (public service)
* Cổng DMZ phản hồi các public request và không có máy chủ nào được truy cập mạng riêng
* Cổng Private không thể kết nổi bởi người dùng Internet



+ DeMilitarized Zone:

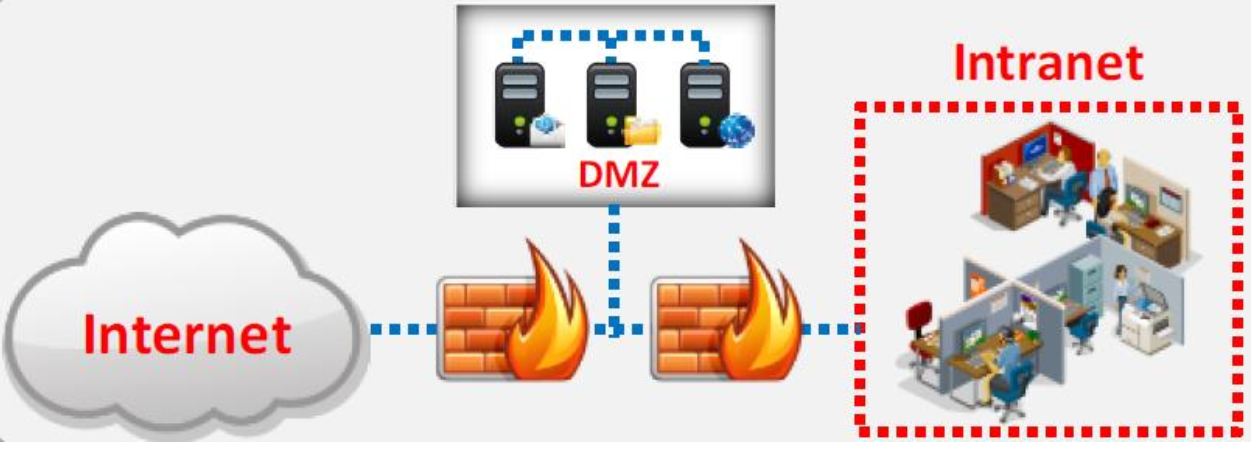
- DMZ phơi bày các dịch vụ hướng ra bên ngoài của 1 tổ chức đến 1 mạng không đáng tin cậy, trong khi phần còn lại của mạng của mạng tổ chức được bảo vệ bởi tường lửa

- DMZ là một mạng lưới hoạt động như một vùng đệm giữa mạng nội bộ an toàn và Internet không an toàn

- Nó có thể được tạo bằng cách sử dụng tường lửa với 3 hoặc nhiều giao diện mạng được gán các vai trò cụ thể như mạng nội bộ đáng tin cậy, mạng DMZ và mạng bên ngoài đáng tin cậy (như hình trên)

+ Multi-homed Firewall:

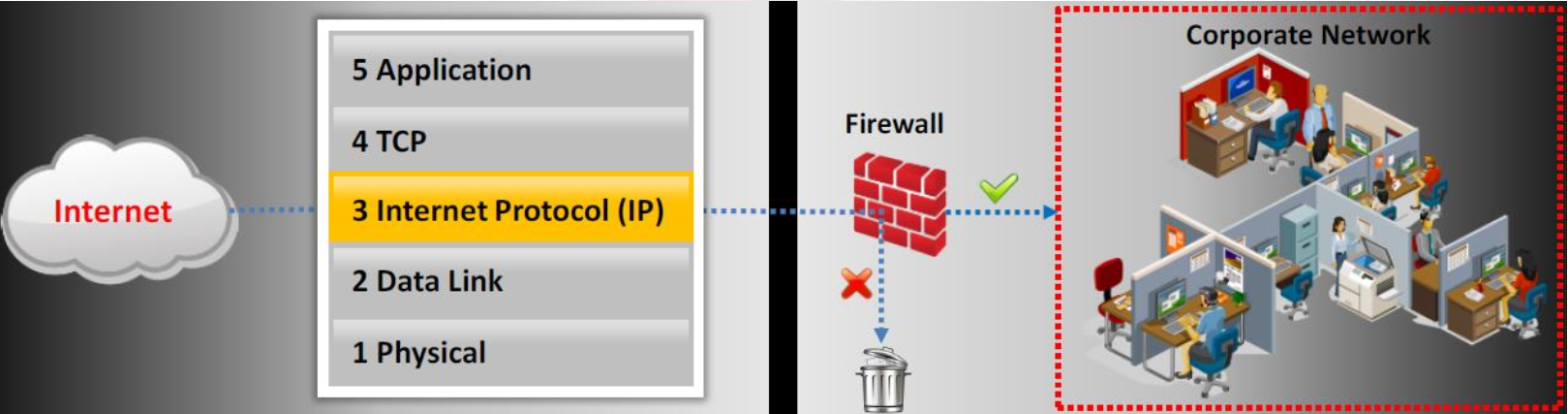
- Trong trường hợp này, một tường lửa với 2 hoặc nhiều giao diện xuất hiện cho phép phân chia thêm mạng dựa trên mục tiêu bảo bảo mật của tổ chức



=> Kiến trúc của tường lửa bao gồm 3 loại: Bastion Host, DMZ zone, Multi-Homed

III. Các loại Firewall

+ Packet Filtering Firewall:



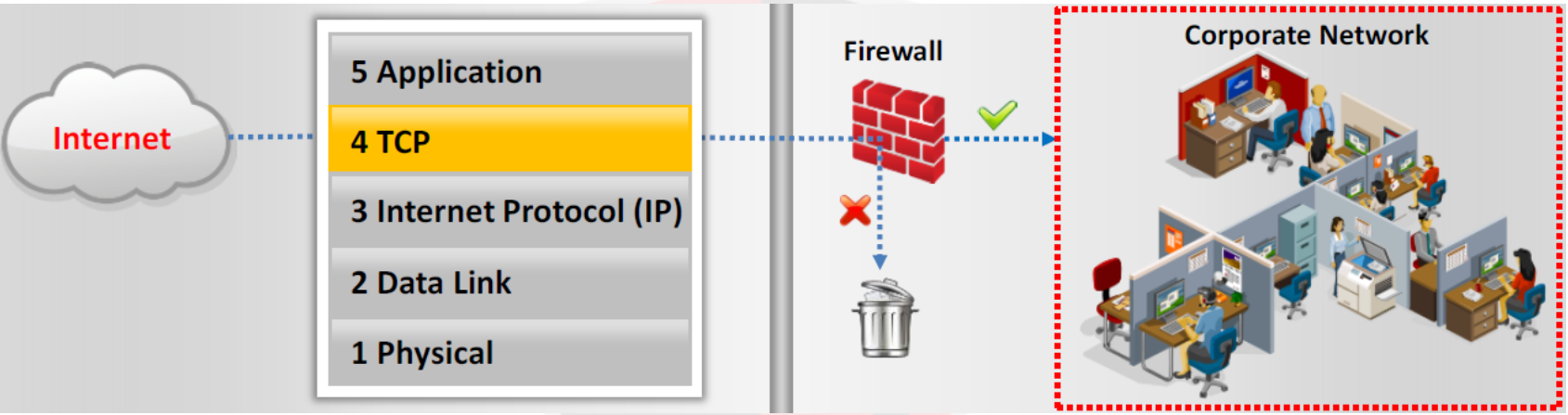
- Hoạt động tại Network layer trong OSI model (hoặc IP layer trong TCP/IP), là một phần của router

- Trong packet filtering firewall, mỗi packet được so sánh với một tập các tiêu chí trước khi được chuyển tiếp

- Phụ thuộc vào packet và tiêu chí, firewall có thể loại bỏ packet và chuyển chúng hoặc gửi thông báo cho người gửi

- Quy tắc có thể bao gồm địa chỉ IP nguồn/đích, số cổng nguồn/đích và giao thức được sử dụng

+ Gateway mức mạng:



- Hoạt động tại session layer trong OSI model (hoặc tầng TCP của TCP/IP)

- Thông tin được truyền đến một máy tính từ xa thông qua cổng cấp mạch (circuit-level gateway) dường như có nguồn gốc từ chính cổng đó.

(Có nghĩa là khi dữ liệu được truyền qua cổng cấp độ mạch đến một máy tính từ xa, cổng sẽ che dấu thông tin nguồn gốc của dữ liệu ⬄ máy tính từ xa sẽ thấy dữ liệu được bắt nguồn từ cổng đó chứ không phải máy nguồn)

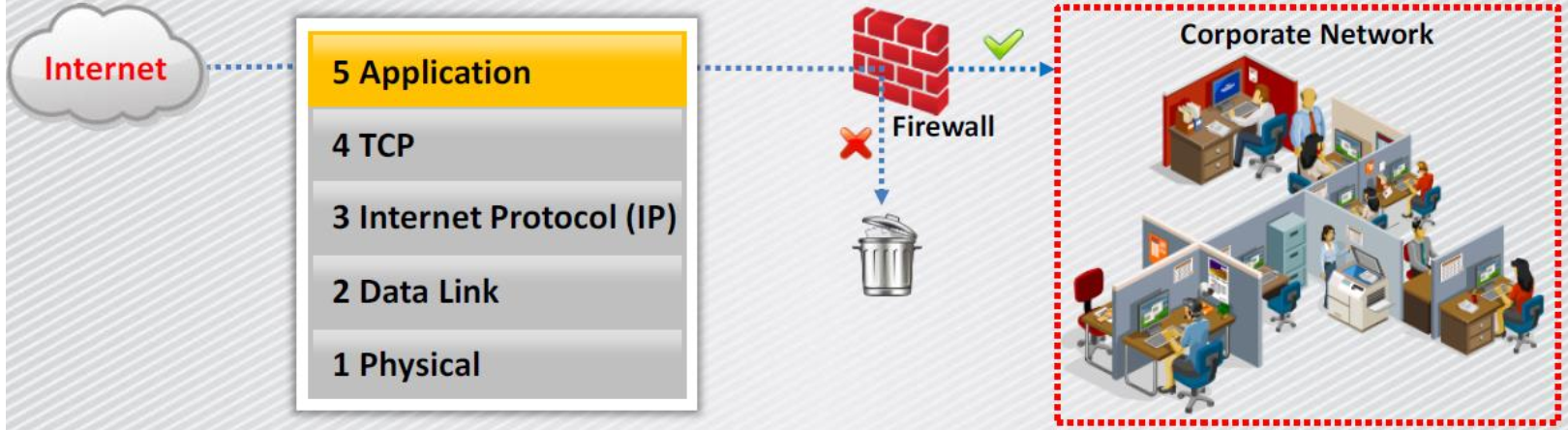
- Chúng quản lý yêu cầu tạo phiên (sessions) và xác định rằng phiên này sẽ được cho phép

- Circuit proxy firewalls cho phép hoặc ngăn chặn các luồng dữ liệu (data streams), nhưng không lọc các gói tin riêng lẻ (filter individual packet)

(Có nghĩa là: firewall này chỉ quan tâm đến phiên kết nối có hợp lệ hay không, việc nội dung từng gói tin như thế nào sẽ không được kiểm tra)

\*\* Cơ chế của cổng này có phần giống NAT là đều ẩn thông tin về mạng nội bộ nhưng NAT tập trung vào chuyển đổi IP, trong khi các cổng mạch tập trung theo dõi và xác minh gói tin trên mạch ảo

+ Application-Level Firewall:



* Application-Level gateways (proxies) có thể lọc các gói tin ngay tại tầng Application của OSI model (hoặc tầng application trong TCP/IP model)
* Lưu lượng truy cập ra vào đều bị hạn chế chỉ dành cho các dịch vụ được hỗ trợ bởi proxy; tất cả các yêu cầu dịch vụ khác đều bị từ chối
* Application-level gateways được cấu hình giống như web proxy cấm lưu lượng truy cập FTP, gopher, telnet hoặc một số lưu lượng khác

(Cấu hình giống web proxy nghĩa là cho phép lưu lượng web đi qua như: HTTP/HTTPS)

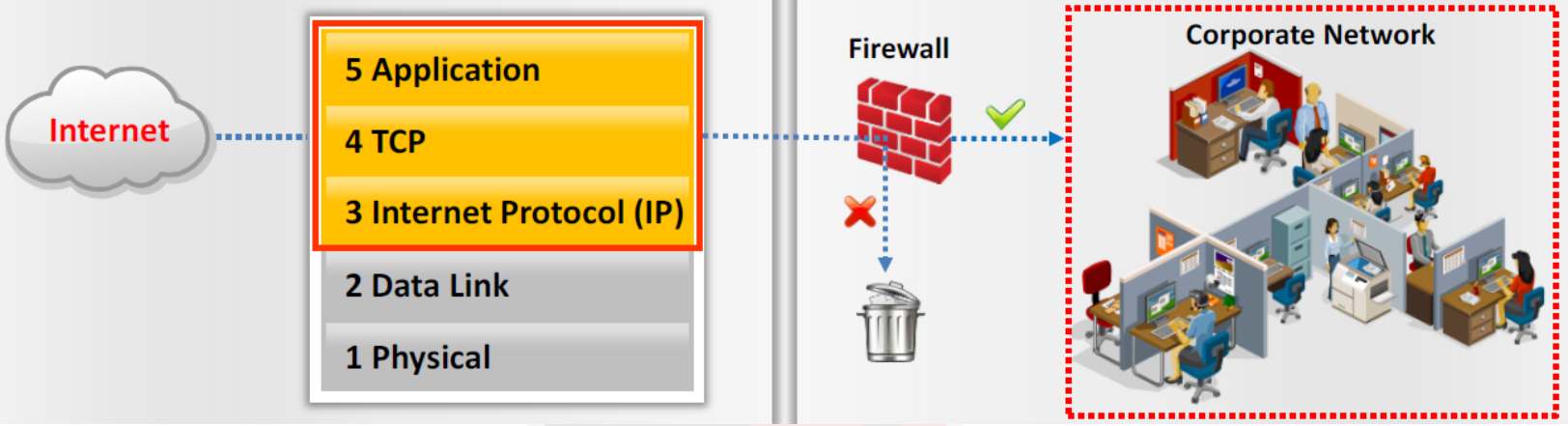
* Application-level gateways kiểm tra lưu lượng mạng và lọc dựa trên các lệnh cụ thể của ứng dụng như http:post và get

\* Application-Level Firewall có thể hoạt động ở một trong hai chế độ sau:

+ Active application-level firewall: chúng kiểm tra các request vào bao gồm cả các thông điệp thực sự được trao đổi, so sánh chúng với các lỗ hổng đã biết như: SQLi, làm giả parameter và cookie, và XSS (cross-site scripting). Request sẽ được thông qua nếu hợp lệ.

+ Passive application-level firewall: Hoạt động giống với IDS, chúng kiểm tra toàn bộ các yêu cầu vào (incoming request), so sánh chúng với các lỗ hổng đã biết nhưng không chủ động loại bỏ yêu cầu nếu chúng bị phát hiện là có tiềm năng tấn công

+ Stateful Multilayer Inspection Firewall (?)



* Bao gồm nhiều khía cạnh của 3 loại firewall trên
* Chúng lọc các packet tại tầng Network trong OSI model (tầng IP trong TCP/IP model), xác định các phiên packet nào là hợp lệ (legitimate) và đánh giá nội dung của các packet tại tầng application
* SPI (Stateful Multilayer Inspection Firewall) đưa ra quyết định dựa trên thông tin về SYN.ACK, số thứ tự và một số data chứa trong TCP header

(Nghĩa là tường lửa này không chỉ kiểm tra các quy tắc thông thường như IP, cổng, mà còn theo dõi trạng thái của kết nối – các thông tin như SYN/ACK, TCP header,… đều dùng để xác minh điều đó )

* SPI firewalls theo dõi trạng thái của từng phiên và có thể mở đóng một cổng linh hoạt theo yêu cầu của các phiên cụ thể

\*\* Vậy mỗi loại tường lửa được triển khai như thế nào (Tại sao lại sử dụng từng loại tường lửa trên trong khi có một loại chứa 3 khía cạnh của 3 loại tưởng lửa trên ⬄Mỗi loại dùng trong trường hợp như thế nào)

+ Packet-filtering Firewall: Triển khai ở tầng 3 (Network Layer) trong TCP/IP model, nhiệm vụ là lọc gói tin dựa trên: IP nguồn/đích, cổng nguồn/đích, giao thức. Firewall này kiểm tra header của mỗi gói tin nhưng không theo dõi trạng thái của các kết nối

* Nhược điểm: Dễ bị tấn công IP Spoofing

+ Circuit-Level Firewall: Triển khai ở tầng 4 (Transport or TCP) trong TCP/IP và ở tầng 5 (Session Layer) trong OSI model. Nhiệm vụ: Xác lập kết nối TCP hoặc UDP giữa các máy, không kiểm tra nội dung gói tin thiết lập

* Nhược điểm: Không ngăn chặn được các cuộc tấn công dựa trên nội dung

+ Application-Level Firewall: Hoạt động ở tầng 7 (OSI) tầng 5 trong TCP/IP. Nhiệm vụ là kiểm tra và lọc lưu lượng dựa trên nội dung cụ thể của ứng dụng (HTTP, HTTPS, FTP, telnet, … request)

* Nhược điểm: Tốn tài nguyên do yêu cầu phân tích nội dung sâu => chậm hiệu suất

+ Stateful Multilayer Inspection Firewall: Triển khai ở tầng 3,4,5 trong TCP/IP và theo dõi trạng thái của các kết nối (stateful inspection). Tường lửa này kết hợp các khía cạnh của 3 tường lửa trên để cung cấp bảo mật

* Nhược điểm: Phức tạp trong triển khai và cấu hình, tốn tài nguyên

\*\* Trong mạng thực tế, nên triển khai bao nhiêu loại thì phù hợp (có thể lấy kịch bản cụ thể)

+ Số lượng sử dụng phụ thuộc vào nhiều yếu tố: yêu cầu bảo mật, cơ sở hạ tầng mạng, các mối đe dọa

+ Kịch bản triển khai: như triển khai ở trên

\*\* Còn những loại tường lửa hoạt động ở tầng khác không? Nếu có thì sao không được đề cập đến? Có phải do chức năng của chúng nên dẫn đến không cần tường lửa? Như vậy hacker có thể tấn công được từ những điểm đó vào hệ thống hay không

+ Còn một số loại khác, được phân theo mục đích sử dụng, mức độ hoạt động trong OSI, công nghệ sử dụng

1. Phân theo công nghệ hoạt động

+ Packet-filtering firewall

+ Stateful Inspection Firewall

+ Proxy Firewall (Application-Level Gateway)

+ Next Generation Firewall (NGFW): Kết hợp nhiều công nghệ của các tường lửa trên; có thêm một số chức năng: IPS, lọc URL, chống mã độc

1. Phân theo vị trí triển khai:

+ Network Firewall (triển khai giữa mạng nội bộ và mạng ngoài – LAN/Internet)

+ Host-Based Firewall (Cài đặt trực tiếp trên thiết bị đầu cuối – máy tính, máy chủ)

+ Cloud-Based Firewall (cung cấp dưới dạng dịch vụ trong môi trường đám mây)

1. Phân theo mục đích sử dụng:

+ Personal Firewall: cá nhân, văn phòng

+ Enterprise Firewall: tổ chức

\*\* Thế nào là một tường lửa yếu? Kỹ thuật để bypass tường lửa

\*\* Các kiểu tấn công có thể có với 4 loại tường lửa trên:

+ Do chức năng của chúng mỗi tường lửa gắn với việc hoạt động của từng tầng mạng (trong mô hình OSI hoặc TCP/IP) => Các kiểu tấn công với từng tầng mạng có thể triển khai với các loại tường lửa trên:

* Packet Filtering Firewall

+ IP spoofing: kẻ tấn công thay đổi địa chỉ IP nguồn trong gói tin, giả mạo chúng giống nguồn đáng tin cậy

+ Fragmentation Attack: kẻ tấn công chia gói tin thành các mảnh nhỏ để vượt qua rules

+ Tiny Fragment Attack: kẻ tấn công chia gói tin nhỏ hơn bình thường để che giấu phần header

* Circuit-Level Firewall

+ Session Hijacking: kẻ tấn công chiếm quyền điều khiển một phiên kết nối hợp lệ giữa hai thiết bị mà tường lửa thiết lập trước đó

+ Connection Hijacking: giống session hijack, nhưng xảy ra ở mức kết nối TCP, nơi kẻ tấn công tiếp quản kết nối hợp lệ sau khi nó đã được thiết lập

+ Man-in-the-middle: kẻ tấn công đặt mình giữa 2 bên giao tiếp, chuyển tiếp và thay đổi thông tin mà không bị phát hiện

* Application Firewall

+ Application Layer Attacks: SQLi, XSS, buffer overflow

+ Bypassing Proxy Restrictions: sử dụng Tunnling, VPN vượt qua proxy firewall

+ HTTP flood Attack: DDoS

* Stateful Multilayer Inspection Firewall

+ SYN Flood Attack

+ ACK Flood Attack

+ TCP Sequence Prediction Attack: dự đoán số thứ tự TCP của gói tin tiếp theo trong 1 kết nối, chèn gói tin giả mạo vào kết nối hợp lệ

\* IDS/IPS SYSTEM

1. IDS

+ Hệ thống phát hiện xâm nhập (IDS) kiểm tra tất cả lưu lượng mạng vào ra để tìm kiếm các mẫu nghi ngờ có thể chỉ ra sự vi phạm an ninh mạng hoặc hệ thống

+ IDS kiểm tra lưu lượng truy cập, đối chiếu kết quả với các mẫu xâm nhập đã biết và phát cảnh báo nếu tìm thấy sự trùng khớp

+ Nó được thiết lập đúng cách để nhận diện được lưu lượng truy cập bình thường trên mạng so với hoạt động độc hại, nhằm tránh cảnh báo giả

A diagram of a network connection

Description automatically generated

2. Cách phát hiện xâm nhập

A diagram of a computer system

Description automatically generated with medium confidence

+ Signature based Recognition:

- Signature-based IDS phát hiện tấn công dựa trên các mẫu cụ thể như số byte hoặc số lượng bit 1 hoặc bit 0 trong lưu lượng mạng

- Nó cũng phát hiện dựa trên chuỗi lệnh độc hại đã được biết đến mà phần mềm độc hại sử dụng. Nó sử dụng database gồm hàng ngàn chữ ký (mẫu) được định nghĩa trước

=> Ưu điểm: Tốc độ xử lý cao và phản hồi nhanh

=> Nhược điểm: Chỉ phát hiện những mẫu đã biết, thất bại đối với zero-day exploits

+ Anomaly based Recognition:

- Thường sử dụng để phát hiện các cuộc tấn công chưa biết. Nó sử dụng machine learning để tạo ra 1 mô hình hoạt động tin cậy, và bất kỳ điều gì đến sau sẽ được so sánh với mô hình này. Nếu không tìm thấy trong mô hình, sẽ bị coi là đáng ngờ

=> Khắc phục được điểm yếu của phần trên: zero-day exploit

- Việc phân loại dựa trên các quy tắc, phương pháp (thay vì các mẫu) và cố gắng phát hiện các lạm dụng nằm ngoài hoạt động bình thường

=> Ưu điểm: Phát hiện zero-day attacks

=> Nhược điểm: Dương tính giả, tốn thời gian và tài nguyên

+ Stateful Protocol based Recognition:

- Xác định các sai lệch của trạng thái giao thức tương tự như phương pháp anomaly-based nhưng sử dụng các hồ sơ toàn cầu đã được xác định trước dựa trên “các định đã được chấp nhận về hoạt động vô hại” do các nhà cung cấp và lãnh đạo trong ngành phát triển

- Theo dõi các yêu cầu cùng với phản hồi tương ứng; nếu nằm ngoài mong đợi sẽ được đánh dấu và phân tích thêm

=> Ưu điểm: Nhận diện các chuỗi lệnh không mong đợi

=> Nhược điểm: Tốn tài nguyên – nhiều chi phí phụ, không thể phát hiện các cuộc tấn công không vi phạm các đặc điểm của hành vi giao thức chấp nhận được.

3. Dấu hiệu chung của xâm nhập

4. IDS/IPS/Firewall

5. Honeypots

\* SNORT

1. Khái niệm

2. Cách hoạt động

3. Quy tắc của Snort

\* Evading IDS

1. Che dấu Payload

2. Insertion Attacks

3. Denial of Service

4. Session Splicing

\* Evading Firewall

1. SSH Tunneling

2. IP Spoofing

3. Source Routing

4. ICMP Tunneling

5. HTTP Tunneling