\*Cloud Security witch ACCESS Point control list(ACL) & Security tool(ST)

ACL->network, infracstructure

ST->Apps

PACKET

IP HEADER TCP/UDP PACKET LOAD

DEST IP / SOURCE IP DEST PORT SOURCR PORT

Chặn Chặn

ACL -> danh sách truy cập dùng để lọc gói tin lớp 3 và phân loại dữ liệu áp dụng cho các dịch vụ: NAT, Distribute-list, VPN

Lọc gói tin lớp 3. Đóng vai trò là 1 chốt canh khi gán vào 1 cổng của Router, chốt canh sẽ cho phép dữ liệu đi qua hay bị chặn

In the table, the ACL permits all hosts with source addresses in the 192.168.10.0/24 network and destination addresses in the 192.168.200.0/24 network.

**1. Wildcard mask match 1 host**

Vd: Tính wildcard mask match host 192.168.1.1

Theo nguyên tắc: bit 0 kiểm tra – bit 1 bỏ qua

-> Địa chỉ IP: 192.168.1.1 0.0.0.0 hoặc từ khóa “host”

**2. Wildcard mask match tất cả địa chỉ IP**

Vd: Tính wildcard mask match tất cả địa chỉ IP

Theo nguyên tắc: bit 0 kiểm tra – bit 1 bỏ qua

-> Địa chỉ IP: 192.168.1.1 255.255.255.255 hoặc từ khóa “any”

**3. Wildcard mask match 1 subnet**

Vd: Tính wildcard mask match subnet 192.168.1.0/24

Cách tính: Lấy 255.255.255.255 trừ đi subnet mask của subnet

-> Địa chỉ IP: 192.168.1.1 0.0.0.255

**. Tính Wildcard mask match range địa chỉ IP liên tục**

Vd: Tính wildcard mask match range từ 192.168.2.0 đến 192.168.4.255

Cách tính: Lấy địa chỉ cuối trừ địa chỉ đầu

-> Địa chỉ IP: 192.168.2.0 0.0.2.255

**5. Tính widcard mask match 1 số IP add đầu tiên**

Vd: Cho địa chỉ IP 192.168.1.0, tính wildcard mask match X host đầu tiên

-> Dải địa chỉ cần match: 192.168.1.0 – > 192.168.1.X

-> wildcard mask: 0.0.0.X (lấy địa chỉ cuối trừ địa chỉ đầu)

-> Địa chỉ IP: 192.168.1.0 0.0.0.X

**6. Tính wildcard mask của nửa trên (upper half) hoặc nửa dưới (lower half) 1 dải mạng:**

Vd: Cho địa chỉ IP 192.168.1.0, tính wildcard mask match nửa dải IP phía trên và dưới:

-> Dải địa chỉ nửa trên: 192.168.1.0 – > 192.168.1.127

-> wildcard mask: 0.0.0.127 (lấy địa chỉ cuối trừ địa chỉ đầu)

-> Địa chỉ IP: 192.168.1.0 0.0.0.127

-> Dải địa chỉ nửa dưới: 192.168.1.128 – > 192.168.1.255

-> wildcard mask: 0.0.0.127 (lấy địa chỉ cuối trừ địa chỉ đầu)

-> Địa chỉ IP: 192.168.1.128 0.0.0.127

\*\*\*

Từ khóa "established" trong danh sách kiểm soát truy cập (ACL) được sử dụng để cho phép lưu lượng đi vào dựa trên trạng thái kết nối đã thiết lập. Điều này liên quan đến cách các giao thức TCP hoạt động.

Khi hai máy tính (máy gửi và máy nhận) thiết lập kết nối TCP, có một quá trình ba bước:

1. **Máy tính gửi gửi một gói tin SYN (Synchronize) đến máy tính nhận.**
2. \*\*Máy tính nhận gửi lại một gói tin SYN-ACK (Synchronize-Acknowledgment) để xác nhận và thiết lập kết nối.
3. **Máy tính gửi lại một gói tin ACK (Acknowledgment) để hoàn tất quá trình kết nối.**

Khi quá trình này hoàn tất, kết nối TCP được coi là "đã thiết lập" (established). Từ khóa "established" trong ACL cho phép lưu lượng đi vào chỉ khi nó thuộc về một kết nối TCP đã thiết lập.

Trong trường hợp của danh sách kiểm soát truy cập 102 và 110 trong cấu hình bạn đã cung cấp, việc sử dụng "established" đảm bảo rằng lưu lượng truy cập FTP (File Transfer Protocol) và dữ liệu FTP chỉ được phép đi vào hoặc đi ra nếu nó là một phần của một kết nối đã thiết lập. Điều này giúp đảm bảo rằng lưu lượng FTP hoạt động một cách đúng đắn và an toàn, vì FTP sử dụng cả các kết nối điều khiển và dữ liệu để hoàn thành truyền tải tệp.

FTP Traffic:

+ Active mode: Control port 21, data port:20

+Passive mode:Control port 21, dynamic port greater than 1024 for data.

A computer screen shot of a computer code

Description automatically generated

Permit FTP Control (Port 21) from NetB to FTP Server (192.168.1.100)

Permit Passive Mode FTP Data Connections (Ports >= 1024) from NetB to FTP Server (192.168.1.100):

Allow Established Connections (to permit FTP data responses)::