CO325 - Lab01: Follow-up Questions

Group 7

E/19/163 - Jayasundara J.M.E.G.
E/19/166 - Jayathunga W.W.K. Jayathunga
E/19/167 - Jayawardena H.D.N.S.
E/19/170 - Jayawardhana K.N.N.
E/19/193 - Kaushalya N.V.K.

01.

a. **What is the default behaviour (in terms of Packet Filtering strategy) of the Cisco ASA 5510 firewall?**

   By default, the Cisco ASA 5506 firewall blocks all traffic from external computers to internal computers but allows all traffic from internal computers to external destinations.

b. **Identify the advantages and disadvantages of this default functionality.**

   <u>Advantages</u>

   Security: The default configuration follows the principle of least privilege by denying all incoming traffic, providing a higher level of security.

   Prevention of Unauthorized Access: Inbound traffic is blocked by default, reducing the risk of unauthorized access attempts, external attacks, and potential security breaches.

   Easier to Manage: Starting with a default deny stance simplifies the firewall rule management process. Administrators can then explicitly define and allow only the necessary traffic, making it easier to maintain and understand the firewall rules.

   <u>Disadvantages</u>

   Outbound Threats: While the default configuration helps protect against inbound threats, it does not explicitly prevent internal systems from initiating outbound connections to potentially malicious external destinations. This could be a concern if internal systems become compromised, as they may attempt to communicate with malicious servers.

   Application Requirements: Some applications and services may require specific inbound connections, and administrators must carefully craft rules to allow the necessary traffic. Failing to do so may lead to service disruptions.

   Complexity in Rule Management: As the network grows and more services are introduced, managing firewall rules can become complex. Administrators need to

carefully design and document rules to ensure that legitimate traffic is not inadvertently blocked.

Potential for Misconfigurations: There is a risk of misconfigurations during rule creation and maintenance. An overly permissive rule could inadvertently allow unauthorized traffic into the internal network.

02.

a. **Scenario# 1: Permit Any**

1. **What are the specific purposes of “access-list” and “access-group” commands?**

   <u>access-list command</u>
   Purpose: Creates and defines Access Control Lists (ACLs), which are sets of rules that filter network traffic based on specified criteria.
   Function: Specifies the conditions for packets to be permitted or denied, acting as a firewall.

   <u>access-group command</u>
   Purpose: Applies an existing ACL to an interface, either inbound or outbound.
   Function: Activates the ACL's filtering rules for traffic moving through that interface.

2. **What has been excluded from the filtering (i.e., permitted) by the ACEs in this scenario? Be precise!**

   All traffic is allowed to pass through without restriction. The specific rules within the ACL are configured to permit any and all traffic, regardless of source or destination IP addresses, protocols, or ports. No traffic is filtered, as all packets are unconditionally permitted.

3. **Identify the pros and cons of this approach in permitting traffic from outside to reach the internal network.**

   <u>Pros</u>

   - Simplicity: It's easy to set up and reduces the chance of mistakes. Troubleshooting is simpler since you don't have to figure out why certain traffic is being blocked.

   - Flexibility: It allows for maximum flexibility when you're not sure about specific traffic needs or if they change frequently. You can think of it as a "default-allow" approach.

   <u>Cons</u>

   - Security Risk: It's riskier because all types of traffic, even potentially harmful ones, are allowed. This increases the chances of security threats and unauthorized access.

   - Lack of Control: You don't have detailed control over the types of traffic coming into your network. This lack of specificity can result in unintended access or vulnerabilities being exploited.

   - Compliance Issues: It might not meet strict regulatory standards that require tight controls and auditing. Using a "permit any" approach may not align with these standards.

- Abuse Potential: Internal resources are more vulnerable since there are no restrictions on incoming traffic. Bad actors could take advantage of the lack of controls to compromise or disrupt services.

- Network Congestion: Allowing all types of traffic, including potentially harmful or unwanted ones, can clog up your network and slow down performance due to increased traffic load.

b. Scenario# 2a: Permit Outside Host to Inside Any

1. **What has been permitted by the ACE in this scenario? Be precise!**
   ACE enables a selected outside host to establish connections to any host within the protected network. This setup allows traffic to flow from the specified outside host to any host within the protected network.

2. **Identify the situation(s) that are best suited for such an ACE, if any. If not, explain why.**

   ➔ **Remote Management:**
   - *Scenario* - The external monitoring system must have access to different internal devices in order to conduct health checks.
   - *Example* - Allowing a specific external monitoring server to establish connections with numerous internal servers.

   ➔ **Partner Integration:**
   - *Scenario* - For collaborative projects, the server of each partner organization must connect to distinct internal servers.
   - *Example* - Allowing a specified partner server to establish connections for data exchange within the secured network.

   ➔ **External Services Access:**
   - *Scenario* - An external service or application from a specific supplier requires connectivity with many internal servers.
   - *Example* - Allowing an external API service to establish connections with several internal servers for data synchronization or integration.

c. Scenario# 2b: Permit Outside Any to Inside Host

1. **What has been permitted by the ACE in this scenario? Be precise!**
   This ACE allows any IP traffic from any source (expressed by "any") to reach a certain internal host. It enables communication from any external host to a specific internal host, allowing traffic to move from outside to within for that particular destination.

2. **Identify the situation(s) that are best suited for such an ACE, if any. If not, explain why.**

➔ **Public - Facing Servers:**
- *Scenario* - A specific internal server, such as a public-facing web server, must be accessible from any exterior source.
- *Example* - Providing unrestricted access to a website hosted on an internal server to all external users.

➔ **Temporary Access for Testing:**
- *Scenario* - Temporary access is required for testing or debugging purposes, and the specific inside host is isolated during the process.
- *Example* - Allowing any external source to connect to a specific internal server while testing new configurations.

➔ **Limited-Time Service Exposure:**
- *Scenario* - A specific internal host is purposely exposed to the internet for a limited time in order to provide a service.
- *Example* - Allowing any external source to connect to an internal server running a time-limited event or service.

d. Scenario# 3a: Permit Outside Any to Inside Any - TCP

1. **What has been permitted by the ACE in this scenario? Be precise!**
This ACE allows all TCP traffic from any source to any destination within the protected network. It enables unlimited communication of all TCP-based protocols (including HTTP, HTTPS, and FTP) from any external source to any internal host.

2. **How does this compare with Scenario# 1? What effect does this have in terms of the "cons" you identified in question 02.a.3. above.**

- **"Permit Any" Scenario:**
  - ➢ Allows all types of IP communications, such as TCP, UDP, ICMP, and others.
  - ➢ Broader in scope, potentially enabling for more applications and services.

- **"Permit Outside Any to Inside Any – TCP" Scenario:**
  - ➢ Specifically allows only TCP traffic.
  - ➢ Allows only TCP-based communication, omitting UDP, ICMP, and other non-TCP protocols.

- **Effects on Identified Cons:**

  - ➢ *Security Risk* **-** Limits access to TCP traffic solely, which reduces risk as compared to a broad "permit any" scenario. However, security

dangers remain, particularly if superfluous TCP services are exposed.

- ➢ *Lack of Control* - Allows more control than "permit any" by limiting traffic to TCP. However, it still lacks granularity for individual TCP services.
- ➢ *Compliance Issues* - It raises similar compliance difficulties as a generic "permit any" scenario because it permits unrestricted TCP traffic.
- ➢ *Abuse Potential* - The possibility for exploitation is lower than with "permit any," but it still exists, particularly if superfluous TCP services are exposed.
- ➢ *Network Congestion* - Concerns about potential network congestion caused by unlimited access are similar to those raised in a generic "permit any" scenario.

e. Scenario# 3b: Permit Outside Any to Inside Any – ICMP

1. What has been permitted by the ACE in this scenario? Be precise!

The Access Control Entry (ACE) in this scenario permits all Internet Control Message Protocol (ICMP) traffic from any source to any destination inside the protected network.

2. Identify the situation(s) that are best suited for such an ACE, if any. If not, explain why.

➔ **Wide-Scope Network Monitoring:**

- Scenario: Organizations may permit ICMP traffic from any external source to any internal host for broad network monitoring purposes.
- Example: Allowing external network monitoring tools to conduct ICMP-based checks on the entire internal network for availability and responsiveness.

➔ **Global Network Diagnostics:**

- Scenario: In environments where external entities need to perform comprehensive network diagnostics and troubleshooting across various internal hosts.
- Example: Allowing external network administrators or diagnostic tools to conduct ICMP-based tests on any internal host, facilitating a global view of network health.

➔ **Open Collaboration Environments:**

- Scenario: In collaborative environments where external entities regularly need to interact with various internal hosts for testing or collaboration purposes.

- Example: Allowing external partners or collaborators to perform ICMP-based tests on any internal host for joint development or testing initiatives.

f. Scenario# 4a: Permit Outside host to Inside Subnet – TCP/SSH

1. What has been permitted by the ACE in this scenario? Be precise!

The Access Control Entry (ACE) in this scenario permits Transmission Control Protocol (TCP) traffic using the Secure Shell (SSH) protocol from an outside host to any destination inside the specified subnet.

2. Identify the situation(s) that are best suited for such an ACE, if any. If not, explain why.

➔ **Remote Secure Shell (SSH) Access to Internal Subnet:**
- Scenario: External administrators or users need to access devices or servers within a specific subnet securely using SSH.
- Example: Allowing SSH traffic from a specific outside host to any internal device within the designated subnet for remote management and secure access.

➔ **Limited External Access to Internal Servers:**
- Scenario: Granting controlled external access to specific servers within the internal subnet for administrative purposes.
- Example: Allowing SSH connections from a designated external host to critical servers within the internal subnet while restricting access to other services.

➔ **Secure File Transfer or Remote Administration:**
- Scenario: External hosts require secure TCP/SSH access to perform file transfers or administer internal systems.
- Example: Allowing SSH connections from an authorized external host for secure file transfers or remote administration tasks.

g. Scenario# 4b: Permit Outside Any to Inside Host – TCP/HTTP

1. **What has been permitted by the ACE in this scenario? Be precise!**
   This ACE allows TCP traffic on port 80 from any source IP address to a designated inside host, and it also permits HTTP (Hypertext Transfer Protocol) traffic on port 80 from any external host to the specified internal host.

2. **Identify the situation(s) that are best suited for such an ACE, if any. If not, explain why.**

➔ **Public Web Server:**

- *Scenario:* Enabling unrestricted access from external locations to an internal web server.
- *Example:* Allowing external visitors to access a website hosted on an internal server by permitting HTTP traffic.

➔ **Web Application Access:**
- *Scenario:* Providing external users with HTTP access to a specific application or service ho*sted on an internal server.*
- *Example:* Granting external users the ability to interact with a web-based application on an internal server through HTTP.

➔ **Content Delivery Network (CDN):**
- *Scenario:* Allowing external users to retrieve content, such as images or scripts, from an internal server via HTTP.
- *Example:* Enabling external access to resources served through a CDN hosted on an internal server.

➔ **Testing and Development:**
- *Scenario:* Supporting testing or development scenarios where external hosts need HTTP access to a particular internal server.
- *Example:* Allowing external developers to test web applications hosted on an internal server by providing HTTP connectivity

h. Scenario# 5a: Deny Outside Any to Inside Host – TCP/HTTP + Permit Any

1. **What has been permitted by the ACE in this scenario? Be precise!**
   In the described situation involving two Access Control Entries (ACEs), the usual outcome is that the particular denial prevails over the general permission. Specifically, the denial ACE takes precedence, preventing the intended TCP traffic. The ACEs can be outlined as follows:

   - **Deny Outside Any to Inside Host – TCP/HTTP:**
     This ACE restricts TCP traffic from any source IP address to a designated inside host on port 80, effectively prohibiting HTTP traffic.

   - **Permit Any:**
     This ACE authorizes any IP traffic from any source to any destination. However, it does not supersede the specific denial for TCP/HTTP traffic, maintaining the restriction imposed by the first ACE.

2. **Compare this approach of traffic filtering with the approach used in scenarios 2 – 4.**

   - **Restrictiveness and Specificity:**
     - The strategy is characterized by greater restrictiveness as it explicitly disallows a specific type of traffic (TCP/HTTP), while permitting all other types of traffic. This marks a departure from previous scenarios where traffic was expressly allowed based on specific criteria.

- **Combination of "Deny" and "Permit" ACEs:**
    - The approach involves a combination of both "deny" and "permit" ACEs to create a more nuanced and controlled traffic filtering strategy.

- **Enhanced Security Layer:**
    - Through the explicit denial of TCP/HTTP traffic, an additional layer of security is introduced. This prevents access to a particular service (HTTP) while still allowing other types of traffic.

- **Increased Control:**
    - The strategy provides heightened control over the types of connections permitted, presenting a more targeted approach compared to simply allowing all traffic.

This underscores the intentional and strategic application of "deny" and "permit" ACEs to sculpt traffic filtering according to defined criteria. It signifies a security-oriented strategy by explicitly preventing access to a specific service while permitting a more extensive range of traffic. This nuanced control proves advantageous for organizations seeking to customize their security policies to specific needs and address potential risks linked to particular protocols or services.

3. Identify the situation(s) that are best suited for such an ACE, if any. If not, explain why.

➔ **Sensitive Web Application:**
- Scenario: A web application that handles confidential data and must not be directly reachable from external sources.
- Example: Prohibiting external access to the HTTP service of a financial application hosted on an internal server.

➔ **Internal Management Interface:**
- Scenario: An internal device or server possesses an HTTP-based management interface that should remain shielded from the internet.
- Example: Preventing external access to the management console of a networking device or server.

➔ **Restricted API Access:**
- Scenario: An internal API service is exclusively intended for internal usage and should not be directly accessible by external clients.
- Example: Confining external access to the HTTP-based API endpoints of an internal service.

➔ **Secure Development Environment:**

- Scenario: A development environment comprising an internal web server that houses experimental or unreleased content.
- Example: Safeguarding the development server against external HTTP access while permitting other forms of traffic for testing.

➔ **Controlled Access to Specific Services:**

- Scenario: Specific internal services, such as file servers or database servers, must not be accessed directly via HTTP from external sources.
- Example: Disallowing external HTTP access to internal services while permitting other essential traffic.

i. Scenario# 5b: Permit Any + Deny Outside Any to Inside Host – TCP/SSH

1. What has been permitted by the ACE in this scenario? Be precise!

In a scenario where the access control entries (ACEs) are configured as "Permit Any + Deny Outside Any to Inside Host – TCP/SSH", the order of these ACEs is crucial. The ACEs may be defined as follows:

- Permit Any: This ACE allows any IP traffic from any source to any destination.
- Deny Outside Any to Inside Host – TCP/SSH: This ACE denies TCP traffic from any source to a specific inside host on port 22 (SSH).

Despite the "Permit Any" ACE granting permission for any IP traffic, the subsequent "Deny" ACE takes precedence due to the order of processing in most firewall implementations. Consequently, any TCP traffic attempting to establish a connection with the designated inside host on port 22 (SSH) will be rejected. However, all other types of IP traffic that do not meet the criteria for denial will be permitted.

1. **Compare this with the scenario above (5a).**

The "permit any" ACE is utilized in both scenarios to allow all non-restricted IP traffic. However, the "deny" ACE in each scenario is focused on restricting a specific service, either SSH or HTTP. These scenarios are

suitable for situations where a particular service on an internal host needs protection from external access.

Examples:

Permit Any + Deny Outside Any to Inside Host – TCP/SSH

- Remote Server Administration: Limiting remote SSH access to a particular server.
- Secure Internal Services: Keeping other kinds of traffic open while safeguarding SSH-based services.

Deny Outside Any to Inside Host – TCP/HTTP + Permit Any

- Internal Web Application Protection: preventing direct external access to an internal web application.
- Sensitive Content Restriction:limiting outside access to a server that hosts private HTTP content.

The exact service that needs to be restricted (HTTP or SSH) in accordance with organizational security policy will determine which of these situations to use.