Use CaseSystems/System boundary: IDS (Done)

[Link](https://lucid.app/lucidchart/1bb4faa9-76a2-4f4f-9e92-be6a694a19f4/edit?viewport_loc=-109%2C-30%2C1304%2C586%2C0_0&invitationId=inv_b288620f-a74d-416b-a117-495d2a032043)

Look at textbook for systems engineering

Sequence Diagram  
Actors (users of system for specific role):

* + Primary (initiates the use case)
  + Secondary (reactionary):
* Use cases (describes function of system and must yield value):

Sequence: Firewall (Done)

[Link](https://lucid.app/lucidchart/d269b336-2017-4004-9cea-d1e6e6debd32/edit?view_items=XS5jqnQsODTo%2CXS5j7lz1CdoN%2CXS5jKKwQYVbe%2CXS5jHVw4l~aS%2CXS5j8lB2ZHP_%2CXS5jD.rkf.US%2CXS5jsurTPxcB%2CXS5jHymPj4WB%2CXS5jphTXfaZV%2CXS5j06oC2oxJ%2CXS5j0pC_lPRb%2CXS5jppn-CQVs%2CXS5jQzIyWizb%2CXS5jpVXK0kKc%2CXS5jCl7CBdBO%2CXS5jVEBZ0Y2-%2CXS5jvR7439x.%2CXS5j38PnA2~z%2CXS5jjjd2jquv%2CXS5jq97-xl.3%2CXS5jRTrI-7ha%2CXS5jfcgSy6TZ&invitationId=inv_eebaf479-c9c9-45c8-ab5f-b02119cc4ef1)

* Actors
* Objects
* Sequence
* Alternative frames
  + If file was suspicious, one sequence
  + If file was not, another sequence
  + Valid vs invalid login requests

Activity: Authentication

[Link](https://lucid.app/lucidchart/9aee4a5e-6a3b-4bf2-8e1f-6adb6653e9c2/edit?viewport_loc=-2397%2C-1234%2C4080%2C2064%2C0_0&invitationId=inv_aeb68ecb-075d-4a15-b712-e6328d800789)

* start/end points
* actions/action state
* Control flow
* Decisions
* Fork nodes
* Time events
* splits/merges
* Swimlanes for different actors

Creating an activity diagram for a firewall system involves outlining the processes and decision points involved in monitoring and filtering network traffic. Here are the key components to include:

### 1. \*\*Actors\*\*

- \*\*User/Administrator:\*\* Initiates configurations and monitoring of the firewall.

- \*\*Firewall System:\*\* Monitors traffic, applies rules, and takes action based on configurations.

### 2. \*\*Activities\*\*

- \*\*Monitor Incoming Traffic:\*\* The firewall continuously observes traffic attempting to enter the network.

- \*\*Check Rules:\*\* The firewall examines the traffic against its predefined security rules.

- \*\*Log Traffic Data:\*\* Record details about the traffic for auditing and analysis.

- \*\*Alert Administrator:\*\* Notify if suspicious activity or rule violations are detected.

- \*\*Apply Security Policies:\*\* Execute rules to either allow or block traffic based on configurations.

### 3. \*\*Decision Points\*\*

- \*\*Traffic Matches Rules?\*\* Determines if the incoming traffic meets any of the defined security rules.

- \*\*Allow Traffic:\*\* If it matches an allow rule.

- \*\*Block Traffic:\*\* If it matches a block rule.

- \*\*Threat Detected?\*\* Checks if the traffic appears to be malicious or a security threat (e.g., intrusion detection).

- \*\*Log and Alert:\*\* If a threat is detected, log the incident and alert the administrator.

- \*\*Policy Update Required?\*\* Evaluates if any security policies need adjustments based on monitoring results.

### 4. \*\*Flows\*\*

- \*\*Allowed Traffic Flow:\*\* If traffic is allowed, it proceeds to the destination network or system.

- \*\*Blocked Traffic Flow:\*\* If traffic is blocked, it is dropped and the event is logged.

- \*\*Suspicious Activity Flow:\*\* If suspicious traffic is detected, it triggers alerts and logging for further analysis.

### 5. \*\*Actions and System Responses\*\*

- \*\*Log Details:\*\* Capture details of allowed, blocked, or suspicious traffic.

- \*\*Send Alerts:\*\* Notify the administrator about security incidents or policy violations.

- \*\*Update Rules:\*\* Allow administrators to modify firewall rules based on findings and network behavior.

- \*\*Generate Reports:\*\* Create periodic reports for traffic analysis and security audits.

Including these components will create a comprehensive activity diagram that illustrates the processes and decision-making involved in a firewall system's operation.

### **Flow for Incoming Traffic in a Firewall System**

1. **Start**: The firewall system is active and monitoring incoming network traffic.
2. **Monitor Incoming Traffic**: The system observes each data packet attempting to enter the network.
3. **Check Rules**:
   * **Decision Point**: Does the incoming traffic match a rule?
     + If **Yes**, proceed to step 4.
     + If **No**, default action may be to block or allow, based on firewall policy.
4. **Apply Security Policy**:
   * **Decision Point**: Is it an “Allow” rule?
     + **If Yes**:
       - **Allow Traffic**: The traffic is permitted to continue to its destination.
       - **Log Details**: Record information about the allowed traffic for future auditing and analysis.
     + **If No** (traffic matches a “Block” rule):
       - **Block Traffic**: The traffic is dropped and prevented from entering the network.
       - **Log Details**: Record information about the blocked traffic.
5. **Threat Detection (if enabled)**:
   * **Decision Point**: Does the traffic appear suspicious (e.g., flagged by intrusion detection)?
     + **If Yes**:
       - **Log and Alert Administrator**: Log details of the suspicious activity and notify the administrator.
       - **Generate Alert Report**: Prepare a report for the administrator on the suspicious event.
     + **If No**, proceed without additional logging or alerts.
6. **Periodic Policy Update (as needed)**:
   * **Decision Point**: Is a policy update required based on recent logs or detected threats?
     + **If Yes**:
       - **Update Rules**: Administrator modifies or adds firewall rules based on security needs.
       - **Apply New Rules**: The updated rules are applied to the firewall for future traffic checks.
7. **End**: The cycle repeats with continuous monitoring of incoming traffic.

In the firewall system activity flow, the tasks can be divided between the **user (administrator)** and the **system** as follows:

### **User (Administrator) Tasks**

1. **Periodic Policy Update (as needed)**:
   * **Decision Point: Is a policy update required?**
     + The administrator decides if security policies need updating based on the logs or detected threats.
   * **Update Rules**:
     + The administrator creates, modifies, or deletes firewall rules based on recent activity or identified threats.
2. **Receive Alerts**:
   * If the system detects suspicious activity or a potential threat, the administrator receives an alert and may decide on further action.

### **System Tasks**

1. **Monitor Incoming Traffic**:
   * The firewall continuously observes each data packet attempting to enter the network.
2. **Check Rules**:
   * **Decision Point: Does the incoming traffic match a rule?**
     + The system compares incoming traffic against predefined rules.
3. **Apply Security Policy**:
   * **Decision Point: Is it an “Allow” rule?**
     + The system decides whether to allow or block traffic based on matched rules.
   * **Allow Traffic**:
     + The system forwards allowed traffic to the destination network or system.
   * **Block Traffic**:
     + The system drops traffic that matches a “Block” rule, preventing it from entering the network.
4. **Log Details**:
   * The system records information about allowed, blocked, or suspicious traffic for audit purposes.
5. **Threat Detection**:
   * **Decision Point: Does the traffic appear suspicious?**
     + If enabled, the system checks if traffic is malicious or a potential threat.
   * **Log and Alert Administrator**:
     + If suspicious traffic is detected, the system logs the event and sends an alert to the administrator.
6. **Generate Alert Report**:
   * When suspicious activity is detected, the system prepares a report for the administrator detailing the event.