## Network Security Implementation Report

This report details the configuration of network security mechanisms, including one firewall rule, one IDS configuration, and one IPS configuration, along with examples of detected events. These mechanisms were implemented to secure network traffic and detect or prevent malicious activity in the network.

### 1. Firewall Rule Implementation (Proxy Firewall)

**Objective:**

To secure the network by blocking unauthorized access attempts and mitigating the risk of attacks, particularly through vulnerable services like SSH.

**Firewall Configuration:**

- **Firewall Type:** Proxy Firewall
- **Location:** Building #1, Bottom-right side of the network.
- **Rule Implemented:** Disable inbound and outbound access to port 22 (SSH).
    - **Justification for Blocking Port 22:**
      Port 22 (SSH) is commonly exploited in attacks, particularly brute-force attempts to gain unauthorized remote access. Disabling this port at the perimeter reduces the attack surface for potential attackers attempting to use SSH for unauthorized access.

**Firewall Rule Example (pseudo-config):**

bash
Copy

```
block incoming tcp any any eq 22
block outgoing tcp any any eq 22
```

- **Effect:** This rule blocks any incoming or outgoing traffic destined for port 22 (SSH), effectively preventing any remote SSH login attempts.

**Example Detected Event:**

- **Event:** An external IP attempts to initiate an SSH connection to a server inside Building #1's network.
- **Detection:** The Proxy Firewall intercepts the connection attempt and denies access based on the rule blocking port 22.
- **Response:** The attacker receives no response, and the connection is silently dropped without further interaction, preventing any unauthorized login attempt.

### 2. Intrusion Detection System (IDS) Configuration

**Objective:**

To monitor and alert on potentially malicious activity within the network without taking automatic action.

**IDS Configuration:**

- **IDS Type:** Passive Network IDS
- **Location:** Japan’s network.

- **Action:** The IDS is configured to passively monitor the network for any signs of intrusion or suspicious activities. It is set to alert system administrators when certain events or behaviors are detected, such as abnormal login attempts or potential exploitation of vulnerabilities.

**IDS Configuration Details:**

- **Event Detection Criteria:**
  The IDS is configured to monitor for suspicious login attempts, such as failed login attempts from multiple external IPs, or unusual login times.
- **Alert Thresholds:**
  An alert is triggered if more than 3 failed login attempts occur within 5 minutes, or if login attempts are made from an unrecognized or foreign IP address.

**Example of IDS Configuration (simplified):**

bash
Copy

```
alert tcp any any -> 192.168.1.0/24 (msg:"Suspicious Login Attempt"; flags:S; threshold: type both, track by_src, count 3, seconds 300; sid:10001;)
```

- **Effect:** The IDS sends a notification to the administrator upon detecting multiple failed login attempts from an external source to any internal system. It does not block the traffic but informs the administrator to investigate further.

**Example Detected Event:**

- **Event:** A series of failed login attempts to a critical server inside Japan's network.
- **Detection:** The IDS identifies that more than 3 login attempts from an unfamiliar external IP address have occurred within a 5-minute window.
- **Response:** The IDS generates an alert and sends an email to the network administrator for further investigation. The administrator can decide whether to block the IP or investigate further.

**3. Intrusion Prevention System (IPS) Configuration**

**Objective:**

To actively block malicious traffic and protect against known vulnerabilities in real-time.

**IPS Configuration:**

- **IPS Type:** Inline IPS
- **Location:** Building #1, protecting the network from attacks that bypass the router or firewall.

**IPS Configuration Details:**

- **Inspection Rules:**
  The IPS is configured to detect and block common exploits, such as attempts to modify file extensions or send malicious payloads through

the network. The IPS will inspect the contents of packets and block any file that has suspicious or unauthorized extensions.

- **Action:**
  The IPS is set to automatically block and drop any packets that contain certain types of malicious payloads or file extensions that could be used in exploits (e.g., ".exe", ".bat", ".vbs").

**Example of IPS Rule (simplified):**

bash
Copy

```
alert ip any any -> any any (msg:"Suspicious File Extension Detected";
content:"exe"; nocase; pcre:"/\.exe$/"; action:block;)
```

- **Effect:** Any file with a suspicious extension (like ".exe" or ".bat") detected in the network traffic will be blocked by the IPS before it reaches its destination.

**Example Detected Event:**

- **Event:** A user inside Building #1 sends a file that was altered to have a ".exe" extension, attempting to bypass the network security.
- **Detection:** The IPS detects that the file passing through the firewall has been renamed with a potentially dangerous file extension (".exe").
- **Response:** The IPS immediately blocks the file transfer, preventing any executable from entering the network. A log entry is generated, and the administrator is notified of the event.

## Summary of Detected Events

1. **Proxy Firewall Event (Port 22 Blocked):**
   - **Event:** An external IP attempts an SSH connection to a device inside Building #1's network.
   - **Response:** The connection is blocked, and no further interaction occurs.
2. **IDS Event (Failed Login Attempts):**
   - **Event:** Multiple failed login attempts from an unknown IP address to a server in Japan.
   - **Response:** The IDS generates an alert notifying the network administrator of potential malicious activity.
3. **IPS Event (Suspicious File Extension Detected):**
   - **Event:** A file with a ".exe" extension is detected in the network traffic.
   - **Response:** The IPS blocks the file from entering the network, preventing a potential malware infection.