Report on Security Implementation

1. Firewall Rule Implementation

A firewall protects the network by controlling traffic based on rules.

Example Rule: Allow HTTPS traffic (port 443) from the internal network (`192.168.1.0/24`) to the internet, and block all other outbound traffic.

Configuration:

```
ALLOW TCP 192.168.1.0/24 ANY 443
DENY ALL
```

- **Purpose**: Ensures secure web traffic is allowed, while blocking unauthorized communication.

2. IDS (Intrusion Detection System) Configuration

An IDS monitors traffic for suspicious activity and alerts administrators.

Example Configuration: Snort IDS to detect port scans.

```
alert tcp any any -> any any (msg:"Port scan detected"; flags:S;
threshold:type both, track by_src, count 5, seconds 10;)
```

- **Purpose**: Triggers an alert if more than 5 connection attempts from a single source are detected within 10 seconds, signaling a possible port scan.

3. IPS (Intrusion Prevention System) Configuration

An IPS not only detects threats but also blocks them in real-time.

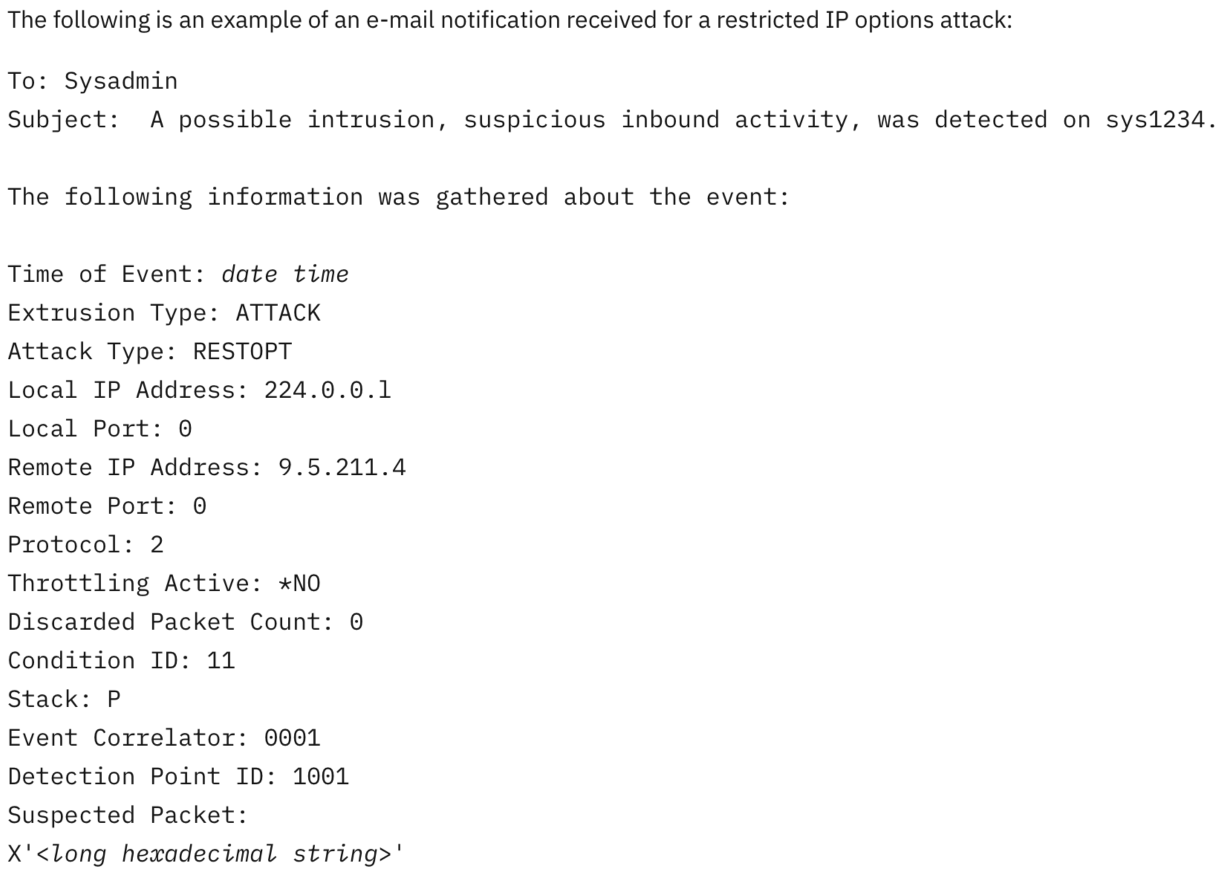
Example Configuration: Blocking SQL injection attempts using an IPS:

```
drop tcp any any -> any 80 (msg:"SQL Injection attempt blocked";
content:"' OR '1'='1"; nocase; sid:1000001;)
```

- **Purpose**: Prevents malicious SQL commands from reaching a server by recognizing patterns commonly used in attacks.

4. Example of Detected Event

- The following example is from IBM documentation
- In this example, IDS detected an intrusion on the local system and sent an e-mail notification to the systems administrator.



The following is an example of an e-mail notification received for a restricted IP options attack:

```
To: Sysadmin
Subject:  A possible intrusion, suspicious inbound activity, was detected on sys1234.

The following information was gathered about the event:

Time of Event: date time
Extrusion Type: ATTACK
Attack Type: RESTOPT
Local IP Address: 224.0.0.l
Local Port: 0
Remote IP Address: 9.5.211.4
Remote Port: 0
Protocol: 2
Throttling Active: *NO
Discarded Packet Count: 0
Condition ID: 11
Stack: P
Event Correlator: 0001
Detection Point ID: 1001
Suspected Packet:
X'<long hexadecimal string>'
```