Firewall Rules

Firewall rules are critical components in network security, **used to control incoming and outgoing traffic based on predefined security policies**. These rules can be configured to detect and block suspicious activities like brute force attacks, port scanning, large data transfers, or other indicators of compromise (IOCs). Here's how firewall rules can help with specific security concerns:

1. Brute Force Attacks (Detecting Multiple Failed Login Attempts):

- Brute force attacks involve repeated login attempts using different username-password combinations in an attempt to gain access to a system.
- Firewall Rule Example:
    - You can **set up rules to detect multiple failed login attempts within a short period**. If a certain threshold (e.g., 5 failed attempts within 1 minute) is reached, the firewall can block the IP address for a certain time to prevent further attempts.
    - Rule: If more than X failed login attempts are detected from a single IP address within Y minutes, block or throttle traffic from that IP.
        - Example:

```
Block traffic from IP 10.0.0.5 after 5 failed SSH login attempts within 2
minutes.
```

2. Detecting Port Scanning (Identifying TCP SYN Floods or Half-Open Connections):

- Port scanning is a common reconnaissance technique used by attackers to discover open ports and services on a target system. One common method of port scanning is SYN scanning, where attackers send TCP SYN packets without completing the handshake (no SYN-ACK response).
- Firewall Rule Example:
    - A rule **can be created to detect TCP SYN packets without corresponding SYN-ACK responses (half-open connections)**. This often indicates port scanning activity. Once detected, the firewall can block the source IP for a certain period or limit the connection rate from that IP.
    - Rule: If more than X half-open connections from a single IP are detected within Y seconds, block or drop further connections from that IP.
        - Example:

```
Block traffic from IP 192.168.1.20 if 50 SYN packets without SYN-ACK
responses are detected within 30 seconds.
```

3. Antivirus Software Notifications:

- Firewalls can also interact with antivirus software and block traffic from infected machines or devices that trigger malware alerts.

- Firewall Rule Example: When the antivirus software detects malware or suspicious behavior on a system, a firewall rule can be triggered to automatically isolate that machine by blocking its outgoing traffic or restricting access to certain network resources.
    - Rule: If antivirus software detects malware on host X, block outgoing traffic from that host until further inspection.
        - Example:

```
Block all outbound traffic from 192.168.1.10 after a malware detection
alert from the antivirus system.
```

4. Large Amounts of Upload Traffic:

- Unusually large upload traffic from a single device could be a sign of data exfiltration, malware activity (e.g., botnets), or a compromised device attempting to send stolen information.
- Firewall Rule Example:
    - A rule can monitor upload traffic and trigger an alert or block traffic if a device exceeds a specified threshold of outgoing data within a short time frame.
    - Rule: If more than X GB of upload traffic is detected from a single IP within Y minutes, block or throttle that device's connection.
        - Example:

```
Limit upload traffic to 500 MB per minute. Block traffic from any IP that
exceeds this limit.
```

Summary of Rules:

1. **Brute Force**: Detect excessive failed login attempts and block the attacker's IP after a threshold is reached to prevent further attempts.
2. **Port Scanning**: Monitor for half-open TCP connections (SYN packets without SYN-ACK) to detect port scanning, and block the offending IP if suspicious scanning is detected.
3. **Antivirus Notifications**: Automatically block traffic from a device that has triggered an antivirus alert to prevent the spread of malware.
4. **Large Upload Traffic**: Monitor for abnormal upload activity that could indicate data exfiltration or malware, and block or limit traffic from the offending device.

> These rules can significantly enhance the security posture of a network by preventing common attack vectors and detecting unusual behavior that could indicate an ongoing attack.