Summary Report

Overview

The Firewall Log Analysis was conducted on the logs generated by ABC Inc.'s firewall. The analysis aimed to provide insights into the network traffic, identify potential threats, and make recommendations for improving the network's security posture.

Key Metrics

- Total Logs: 13
- Allowed Logs: 7
- Blocked Logs: 6

Insights

Top Source IP

- **192.168.1.105:** 6 logs
    - This source IP has the highest number of logs, indicating frequent network activity.
- Various other source IPs had minimal logs, suggesting sporadic interactions.

Top Destination IP

- There were various destination IPs in this log with no repetitions, signifying diverse communication in the network.

Top Protocols

1. **TCP:** 8 logs
    - Most logs use the TCP protocol, indicating predominant usage for network traffic.
2. **UDP:** 3 logs
    - Fewer logs with UDP, suggesting less frequent use for perhaps for specific purposes.
3. **ICMP:** 2 logs
    - ICMP logs, indicating network diagnostics or communication issues within the network.

Port Usage

1. **Source ports**
    - **Ports 44345, 44346, 44347, 44348, 44349, 44350, 44351, 44352, 44353 (TCP):** An ephemeral port used dynamically by the client for communication.
    - **138 (UDP):** Traditionally associated with the NetBIOS Datagram Service, which is part of the NetBIOS over TCP/IP suite used for communication between computers on a local network.
    - **Port 53 (UDP):** Associated with the DNS (Domain Name System) service. UDP is commonly used for DNS queries.

2. **Destination ports**
    - **Port 80 (TCP):** Default port for HTTP (Hypertext Transfer Protocol), the protocol used for transmitting web pages.
    - **Port 22 (TCP):** Default port for SSH (Secure Shell), a cryptographic network protocol used for secure remote login and command execution.
    - **Port 138 (UDP):** Traditionally associated with the NetBIOS Datagram Service, which is part of the NetBIOS over TCP/IP suite used for communication between computers on a local network.
    - **Port 443 (TCP):** Default port for HTTPS (Hypertext Transfer Protocol Secure), the secure version of HTTP. It is commonly used for secure web communication.

- **Port 53 (UDP):** Associated with the DNS (Domain Name System) service. UDP is commonly used for DNS queries.
- **Port 445 (TCP):** Used by Microsoft-DS (Microsoft Directory Services), including SMB (Server Message Block) over TCP and is commonly associated with file and printer sharing in Windows environments.
- **Port 1433 (TCP):** Default port for Microsoft SQL Server. It is used for communication with SQL databases.
- **Port 3306 (TCP):** Default port for MySQL, relational database management system (RDBMS).
- **Port 161 (UDP):** Associated with the SNMP (Simple Network Management Protocol) service, used for monitoring and managing network devices.

Traffic Types

1. **Internal Traffic:** Refers to the communication and data exchange that occurs between devices or systems within the same local network or organization. In this log file internal network can be likely identified as Class C with the ip range 192.168.0.0 to 192.168.255.255.

2. **External Inbound Traffic:** Refers to the data and communication that is incoming from external sources into the internal network.

3. **External Outbound Traffic:** Refers to the data and communication that is outgoing from the internal network to external destinations.

Allowed Traffic

In a firewall log file, "allowed" traffic refers to network activity that the firewall permits to pass through. When a firewall receives a network packet, it evaluates the packet based on a set of predefined rules. If the packet matches one of the rules and is considered safe and authorized, the firewall allows it to pass through and reach its destination.
The following should be highlighted even though they have been allowed through the firewall,

1. **Client Hello (TCP) - 192.168.1.105 to 93.184.216.34**

   This is an External Outbound Traffic, a TCP connection initiated by the internal device with IP address 192.168.1.105 going to the external server at 93.184.216.34. The "Client Hello" likely indicates the beginning of a secure communication session, often associated with the establishment of a TLS/SSL connection, such as during the initial steps of an HTTPS connection.

2. **Echo request (ICMP) - 192.168.1.105 to 8.8.8.8**

   This is an External Outbound Traffic, a ICMP Echo Request sent by the device with the internal IP address 192.168.1.105 to the external server at 8.8.8.8. ICMP Echo Requests are commonly used for network diagnostics, and in this case, the device is likely checking if it can reach the external server and receive a response.

3. **DNS request (UDP) - 192.168.1.105 to 8.8.4.4**

   This is an External Outbound Traffic, a DNS request sent by the device with the internal IP address 192.168.1.105 to the external DNS server at 8.8.4.4. The device is asking the DNS server to resolve a domain name to an IP address. DNS requests are common when a device needs to translate human-readable domain names into IP addresses to locate resources on the internet.

Blocked Traffic

In a firewall log file, "blocked" traffic refers to network activity that the firewall does not permit to pass through. When a firewall receives a network packet, it evaluates the packet based on a set of predefined rules. If the packet does not match one of the rules and is considered unsafe and unauthorized, the firewall then allows drops the packet and block the connection.

1. **Local Broadcast (UDP) - 192.168.1.105 to 192.168.1.255:**

   This Internal UDP traffic is a local broadcast from the device with IP address 192.168.1.105 to all devices in the same local network (broadcast address

192.168.1.255). Local broadcasts are used for communication within the same network segment. The blocking might be due to a security policy that restricts or monitors such broadcast traffic.

2. **SSH Attempt (TCP) - 192.168.1.105 to 203.0.113.5:**

   This Outbound External TCP traffic represents an attempt from the device with IP address 192.168.1.105 to establish an SSH (Secure Shell) connection with the external server at 203.0.113.5. The firewall blocked this attempt, possibly because SSH traffic might be restricted for security reasons.

3. **Client Hello (TCP) - 192.168.1.106 to 198.51.100.24:**

   This Outbound External TCP traffic is a "Client Hello" message initiated by the device with IP address 192.168.1.106, attempting to communicate with the external server at 198.51.100.24. The firewall blocked this communication, and the "Client Hello" suggests an attempt to establish a secure connection, possibly for HTTPS.

4. **SQL Server Access Attempt (TCP) - 192.168.1.108 to 203.0.113.10:**

   This Outbound External TCP traffic represents an attempt from the device with IP address 192.168.1.108 to access a SQL Server on the external server at 203.0.113.10. The firewall blocked this access, which might be a security measure to protect against unauthorized attempts to connect to SQL servers..

5. **Destination Unreachable (ICMP) - 192.168.1.110 to 10.10.10.10:**

   This Outbound External ICMP traffic is a "Destination Unreachable" message sent by the device with IP address 192.168.1.110 to the external server at 10.10.10.10. The firewall blocked this ICMP message, indicating that the destination (10.10.10.10) is unreachable.

6. **SNMP Access Attempt (UDP) - 192.168.1.112 to 192.168.1.230:**

   This Internal UDP traffic represents an attempt from the device with IP address 192.168.1.112 to access an SNMP service on the device with IP address 192.168.1.230 within the same local network. The firewall blocked this SNMP access attempt, possibly due to security policies.

Recommendations

1. **Local Broadcasts Blocking:**
    - Blocking local broadcasts is a common practice for security. Ensure that local broadcast traffic is limited to necessary communication within the local network.
    - If local broadcasts are frequently expected behavior, consider adjusting firewall rules accordingly.
2. **DNS Request Security:**
    - Validate that DNS requests from internal hosts to external servers are legitimate.
    - Consider using internal DNS servers for local queries and restrict direct external DNS requests if not required.
3. **Enhance SSH Security:**
    - Investigate the reason for unexpected SSH attempts and from blocked ports.
    - Ensure that SSH access is properly restricted and monitor for any unauthorized attempts.
    - Adjust firewall rules accordingly.
4. **Monitor External Communications:**
    - Ensure that secure communication (possibly HTTPS) initiated by internal host to external servers/hosts.
    - Regularly monitor and validate such secure connections.
5. **Review SQL Server Access:**
    - Validate the necessity of SQL Server access attempts from internal hosts to external servers and if not required, block such traffic.
    - Ensure that only authorized devices can access SQL servers externally.
6. **Investigate ICMP requests:**

- ICMP Echo requests are commonly used for network diagnostics. Ensure that devices in your network are authorized to perform such requests.
- Monitor and set appropriate restrictions on ICMP traffic to prevent misuse.

7. **Review SNMP Security:**

    - Review the necessity of SNMP access attempts between internal hosts.
    - Ensure that SNMP is configured securely, and access is restricted to authorized devices.