LetsDefend

Firewall Log Analysis/Details/Questions

By: Ryan Stewart

Key Log Details

- **Date:** Date
- **Time:** Time
- **Hostname:** Hostname
- **Device ID:** Device ID
- **Event Time:** Event timestamp
- **Time Zone:** Time zone
- **Log ID:** Log ID
- **Log Type:** Log Type (traffic, utm, event, etc.)
- **Sub Log Type:** Sub Log Type (forward, vpn, webfilter, virus, ips, system, etc.)
- **Log Level:** Log level
- **Source IP Address:** Source IP Address
- **Source Hostname:** Source Hostname
- **Source Port:** Source Port
- **Source Interface:** Source Interface Name
- **Source Interface Role:** Role of Source Interface
- **Destination IP Address:** Destination IP Address
- **Destination Port:** Destination Port
- **Destination Interface:** Destination Interface Name
- **Destination Interface Role:** Role of Destination Interface
- **Source Country:** Source IP information (Country)
- **Destination Country:** Destination IP information (Country)
- **Action:** Action taken (accept, deny, drop, close, client-rst, server-rst)
- **Service:** Service information
- **NAT IP:** NAT IP information (internal output of private source address)
- **NAT Port:** NAT port information
- **Duration:** Duration of communication

- **Sent Byte:** Size of sent packets (byte)
- **Received Byte:** Size of received packets (byte)
- **Sent Packet:** Number of sent packets
- **Received Packet:** Number of received packets

When analyzing firewall logs, the initial focus should be on IP and port information. Subsequently, verifying whether the traffic reaches the intended target under the "action" section is essential. The firewall log provides critical information about the source and destination of the traffic and the port on which it operates.

Action Indicators:

- **accept:** Packet passed successfully.
- **deny:** Packet transmission is blocked, and information is returned to the IP address.
- **drop:** Packet transmission is blocked without returning information.
- **close:** Communication is mutually terminated.
- **client-rst:** Communication terminated by the client.
- **server-rst:** Communication terminated by the server.

For example, examining firewall logs can reveal details such as:

- Acceptance requests from an IP address detected as an attacker and denied by the IPS in firewall logs.
- Access information to/from suspicious IPs/Domains obtained from antivirus logs' malicious content analysis.
- Detection of different systems with which an infected system communicates within the network.

Firewall logs serve as crucial resources for SOC Analysts when investigating incidents, cases, and suspicious activities. They provide valuable insights, helping analysts answer questions such as:

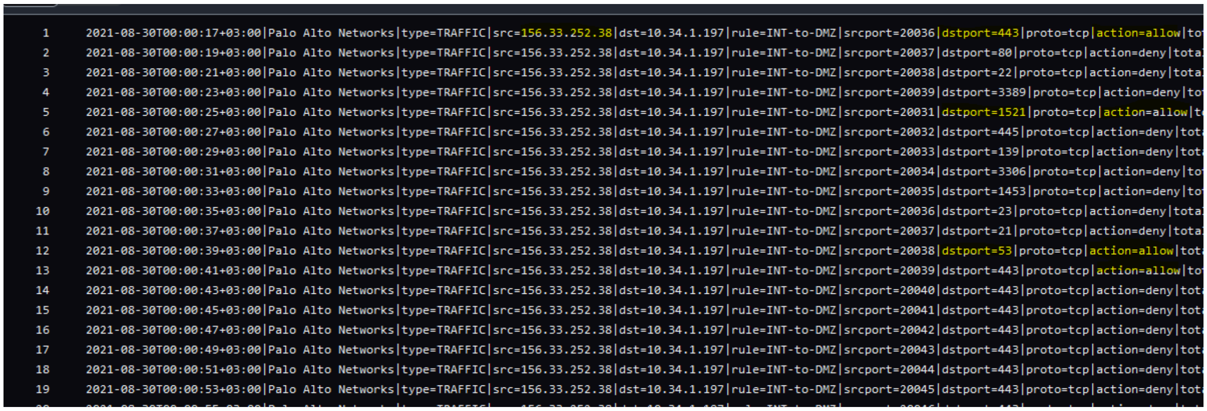
- Is there an accepted request from the IP address detected as attacking and denied by the IPS in firewall logs?
- Are there accesses to/from suspicious IPs/Domains identified through antivirus logs' malicious content analysis?
- Which different systems is an infected system communicating with in the network?

Through firewall logs, SOC Analysts can identify and respond to suspicious activities like:

- Port-Scan activities
- Communication detection with Indicators of Compromise (IoCs)
- Unauthorized access within the network, whether lateral (lan-lan) or vertical (lan-wan, wan-lan)

Firewall Logs Analysis Questions

1. **How many open ports did the attacker detect?**
    - 3



```
2021-08-30T00:00:17+03:00|Palo Alto Networks|type=TRAFFIC|src=156.33.252.38|dst=10.34.1.197|rule=INT-to-DMZ|srcport=20036|dstport=443|proto=tcp|action=allow|to
2021-08-30T00:00:19+03:00|Palo Alto Networks|type=TRAFFIC|src=156.33.252.38|dst=10.34.1.197|rule=INT-to-DMZ|srcport=20037|dstport=80|proto=tcp|action=deny|tota
2021-08-30T00:00:21+03:00|Palo Alto Networks|type=TRAFFIC|src=156.33.252.38|dst=10.34.1.197|rule=INT-to-DMZ|srcport=20038|dstport=22|proto=tcp|action=deny|tota
2021-08-30T00:00:23+03:00|Palo Alto Networks|type=TRAFFIC|src=156.33.252.38|dst=10.34.1.197|rule=INT-to-DMZ|srcport=20039|dstport=3389|proto=tcp|action=deny|to
2021-08-30T00:00:25+03:00|Palo Alto Networks|type=TRAFFIC|src=156.33.252.38|dst=10.34.1.197|rule=INT-to-DMZ|srcport=20031|dstport=1521|proto=tcp|action=allow|t
2021-08-30T00:00:27+03:00|Palo Alto Networks|type=TRAFFIC|src=156.33.252.38|dst=10.34.1.197|rule=INT-to-DMZ|srcport=20032|dstport=445|proto=tcp|action=deny|tot
2021-08-30T00:00:29+03:00|Palo Alto Networks|type=TRAFFIC|src=156.33.252.38|dst=10.34.1.197|rule=INT-to-DMZ|srcport=20033|dstport=139|proto=tcp|action=deny|tot
2021-08-30T00:00:31+03:00|Palo Alto Networks|type=TRAFFIC|src=156.33.252.38|dst=10.34.1.197|rule=INT-to-DMZ|srcport=20034|dstport=3306|proto=tcp|action=deny|to
2021-08-30T00:00:33+03:00|Palo Alto Networks|type=TRAFFIC|src=156.33.252.38|dst=10.34.1.197|rule=INT-to-DMZ|srcport=20035|dstport=1453|proto=tcp|action=deny|to
2021-08-30T00:00:35+03:00|Palo Alto Networks|type=TRAFFIC|src=156.33.252.38|dst=10.34.1.197|rule=INT-to-DMZ|srcport=20036|dstport=23|proto=tcp|action=deny|tota
2021-08-30T00:00:37+03:00|Palo Alto Networks|type=TRAFFIC|src=156.33.252.38|dst=10.34.1.197|rule=INT-to-DMZ|srcport=20037|dstport=21|proto=tcp|action=deny|tota
2021-08-30T00:00:39+03:00|Palo Alto Networks|type=TRAFFIC|src=156.33.252.38|dst=10.34.1.197|rule=INT-to-DMZ|srcport=20038|dstport=53|proto=tcp|action=allow|tot
2021-08-30T00:00:41+03:00|Palo Alto Networks|type=TRAFFIC|src=156.33.252.38|dst=10.34.1.197|rule=INT-to-DMZ|srcport=20039|dstport=443|proto=tcp|action=allow|to
2021-08-30T00:00:43+03:00|Palo Alto Networks|type=TRAFFIC|src=156.33.252.38|dst=10.34.1.197|rule=INT-to-DMZ|srcport=20040|dstport=443|proto=tcp|action=deny|tot
2021-08-30T00:00:45+03:00|Palo Alto Networks|type=TRAFFIC|src=156.33.252.38|dst=10.34.1.197|rule=INT-to-DMZ|srcport=20041|dstport=443|proto=tcp|action=deny|tot
2021-08-30T00:00:47+03:00|Palo Alto Networks|type=TRAFFIC|src=156.33.252.38|dst=10.34.1.197|rule=INT-to-DMZ|srcport=20042|dstport=443|proto=tcp|action=deny|tot
2021-08-30T00:00:49+03:00|Palo Alto Networks|type=TRAFFIC|src=156.33.252.38|dst=10.34.1.197|rule=INT-to-DMZ|srcport=20043|dstport=443|proto=tcp|action=deny|tot
2021-08-30T00:00:51+03:00|Palo Alto Networks|type=TRAFFIC|src=156.33.252.38|dst=10.34.1.197|rule=INT-to-DMZ|srcport=20044|dstport=443|proto=tcp|action=deny|tot
2021-08-30T00:00:53+03:00|Palo Alto Networks|type=TRAFFIC|src=156.33.252.38|dst=10.34.1.197|rule=INT-to-DMZ|srcport=20045|dstport=443|proto=tcp|action=deny|tot
```

2. **Will the attacker get a response from the Firewall stating that its access request was blocked?**
    - Yes

- deny: packet transmission is blocked, information is returned back to the IP address that it is blocked.

- drop: packet transmission is blocked. No information is returned back to the IP address that it is blocked.

3. **How many different ports did the attacker attempt to access?**

12

4. **What kind of attack/activity could have been made according to the logs above?**

A) Brute-Force Attack
B) Port-scan activity
C) TCP-SYN-Flood Attack
D) No suspicious activities detected

Consistent Source IP, Different Ports:

- A single source IP consistently accessing different ports within a short period suggests a scanning attempt.

Repetitive Access to Specific Ports:

- Repeated access to specific ports, especially if uncommon, can signal scanning.

Multiple Denied Connections:

- Numerous denied connections from the same source IP attempting different ports may indicate scanning.

5. **How does Firewall determine whether to forward an incoming packet to the destination or not?**

A) By analyzing behaviorally
B) According to the rule policy
C) According to the size of the traffic
D) According to the location information