



# Firewall Checkpoint Questions

By: Ryan Stewart

1. What action is taken according to the provided firewall log?

```
firewall.log
1  time=07:30:52 devname="LETSDEFEND" devid="FGT60FTK19020806" eventtime=1667215851877876189 tz="-0400"
   logid="0001000014" type="traffic" subtype="local" level="notice" vd="root" srcip=192.168.68.12 srcport=58427
   srcintf="wan1" srcintfrole="wan" dstip=192.168.68.34 dstport=143 dstintf="root" dstintfrole="undefined"
   srccountry="United States" dstcountry="United States" sessionid=30340381 proto=6 action="deny" policyid=0
   policytype="local-in-policy" service="IMAP"trandisp="noop" app="IMAP" duration=0 sentbyte=0 rcvdbyte=0
   rcvdpkt=0 appcat="unscanned" crscore=5 craction=262144 crlevel="low"
```

2. What is the source IP address in the given firewall log?

```
devname="LETSDEFEND" devid="FGT60FTK19020806" eventtime=1667215851877876189 tz="-0400"
logid="0001000014" type="traffic" subtype="local" level="notice" vd="root" srcip=192.168.68.12 srcport=58427
srcintfrole="wan" dstip=192.168.68.34 dstport=143 dstintf="root" dstintfrole="undefined"
dstcountry="United States" sessionid=30340381 proto=6 action="deny" policyid=0
cal-in-policy" service="IMAP"trandisp="noop" app="IMAP" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0
at="unscanned" crscore=5 craction=262144 crlevel="low"
```

**3. According to the provided Windows Defender Firewall log, what is the IP address sending the TCP segment with a source port of 5421?**

```
pfirewall.log
1 #Version: 1.5
2 #Software: Microsoft Windows Firewall
3 #Time Format: Local
4 #Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpv
  icmpcode info path
5
6 2022-11-05 18:38:05 ALLOW TCP 127.0.0.1 127.0.0.1 3845 3844 0 - 0 0 0 - - - RECEIVE
7 2022-11-05 18:38:19 DROP UDP 192.168.1.14 192.168.1.255 137 137 78 - - - - - - RECEIVE
8 2022-11-05 18:38:20 DROP UDP 192.168.1.14 192.168.1.255 137 137 78 - - - - - - RECEIVE
9 2022-11-05 18:38:21 DROP UDP 192.168.1.14 192.168.1.255 137 137 78 - - - - - - RECEIVE
10 2022-11-05 21:18:06 ALLOW ICMP 192.168.1.9 8.8.8.8 - - 0 - - - - 8 0 - SEND
11 2022-11-05 21:18:06 DROP ICMP 8.8.8.8 192.168.1.9 - - 84 - - - - 0 0 - RECEIVE
12 2022-11-05 21:18:07 ALLOW ICMP 192.168.1.9 8.8.8.8 - - 0 - - - - 8 0 - SEND
13 2022-11-05 21:18:07 DROP ICMP 8.8.8.8 192.168.1.9 - - 84 - - - - 0 0 - RECEIVE
14 2022-11-05 21:18:08 ALLOW ICMP 192.168.1.9 8.8.8.8 - - 0 - - - - 8 0 - SEND
15 2022-11-05 21:18:08 DROP ICMP 8.8.8.8 192.168.1.9 - - 84 - - - - 0 0 - RECEIVE
16 2022-11-05 21:18:52 ALLOW TCP 192.168.1.9 34.107.221.82 5417 80 0 - 0 0 0 - - - SEND
17 2022-11-05 21:18:53 ALLOW TCP 192.168.1.9 34.160.144.191 5419 443 0 - 0 0 0 - - - SEND
18 2022-11-05 21:18:53 ALLOW UDP 192.168.1.9 192.168.1.1 59397 53 0 - - - - - - SEND
19 2022-11-05 21:18:53 ALLOW UDP 192.168.1.9 192.168.1.1 59398 53 0 - - - - - - SEND
20 2022-11-05 21:18:53 ALLOW TCP 192.168.1.9 34.102.187.140 5421 443 0 - 0 0 0 - - - SEND
21
```

**4. What is the destination port number according to the given firewall log?**

```
a:\Local\Temp\1\Temp1_firewall.log.zip\firewall.log - Notepad++
oding Language Settings Tools Macro Run Plugins Window ?
+

evname="LETSDEFEND" devid="FGT60FTK19020806" eventtime=1667215851877876189 tz="-0400"
l4" type="traffic" subtype="local" level="notice" vd="root" srcip=192.168.68.12 srcport=58427
srcintfrole="wan" dstip=192.168.68.34 dstport=143 dstintf="root" dstintfrole="undefined"
ted States" dstcountry="United States" sessionid=30340381 proto=6 action="deny" policyid=0
al-in-policy" service="IMAP" trandisp="noop" app="IMAP" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0
t="unscanned" crscore=5 craction=262144 crlevel="low"
```

## 5. According to the Windows Defender Firewall log, which network protocol do the logs associated with the IP address "8.8.8.8" belong to?

```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcppack tcpw
icmpcode info path

2022-11-05 18:38:05 ALLOW TCP 127.0.0.1 127.0.0.1 3845 3844 0 - 0 0 0 - - - RECEIVE
2022-11-05 18:38:19 DROP UDP 192.168.1.14 192.168.1.255 137 137 78 - - - - - - RECEIVE
2022-11-05 18:38:20 DROP UDP 192.168.1.14 192.168.1.255 137 137 78 - - - - - - RECEIVE
2022-11-05 18:38:21 DROP UDP 192.168.1.14 192.168.1.255 137 137 78 - - - - - - RECEIVE
2022-11-05 21:18:06 ALLOW ICMP 192.168.1.9 8.8.8.8 - - 0 - - - - 8 0 - SEND
2022-11-05 21:18:06 DROP ICMP 8.8.8.8 192.168.1.9 - - 84 - - - - 0 0 - RECEIVE
2022-11-05 21:18:07 ALLOW ICMP 192.168.1.9 8.8.8.8 - - 0 - - - - 8 0 - SEND
2022-11-05 21:18:07 DROP ICMP 8.8.8.8 192.168.1.9 - - 84 - - - - 0 0 - RECEIVE
2022-11-05 21:18:08 ALLOW ICMP 192.168.1.9 8.8.8.8 - - 0 - - - - 8 0 - SEND
2022-11-05 21:18:08 DROP ICMP 8.8.8.8 192.168.1.9 - - 84 - - - - 0 0 - RECEIVE
2022-11-05 21:18:52 ALLOW TCP 192.168.1.9 34.107.221.82 5417 80 0 - 0 0 0 - - - SEND
2022-11-05 21:18:53 ALLOW TCP 192.168.1.9 34.160.144.191 5419 443 0 - 0 0 0 - - - SEND
2022-11-05 21:18:53 ALLOW UDP 192.168.1.9 192.168.1.1 59397 53 0 - - - - - - - SEND
2022-11-05 21:18:53 ALLOW UDP 192.168.1.9 192.168.1.1 59398 53 0 - - - - - - - SEND
2022-11-05 21:18:53 ALLOW TCP 192.168.1.9 34.102.187.140 5421 443 0 - 0 0 0 - - - SEND
```