Network Traffic Analysis Report

Executive Summary

Executive Summary of Network Traffic Analysis 1. Overview: - Total Packets: 140682 - Duration: 56.91 seconds - Average Packet Rate: 2471.93 packets/second 2. Traffic Distribution: - Top Source IP: 20.204.169.2 (62870 packets, 44.69% of total) - Top Destination IP: 13.126.130.109 (62745 packets, 44.60% of total) - Most Active Port: 4500 (142586 occurrences) 3. Protocol Analysis: - Primary Protocol: 17 - Protocol Distribution: 17:71308, 6:69345, 50:29 4. Packet Size Statistics: - Average: 129.34 bytes - Median: 134.00 bytes - Std Dev: 17.02 bytes 5. Security Concerns: High traffic on unusual ports: 4500, 54887, 58302, 1500, 58280, 58310, 58284, 58296 6. Key Recommendations: Review and potentially restrict traffic on identified unusual ports. Consider network capacity upgrades to handle high traffic volume. This summary provides a high-level overview of the network traffic captured in the PCAP file. For detailed analysis and visualizations, please refer to the full report.

Detailed Analysis

Protocol Distribution:

- 17: 71308 packets (50.69%)
- 6: 69345 packets (49.29%)
- 50: 29 packets (0.02%)

Top 5 Source IP Addresses:

- 20.204.169.2: 62870 packets (44.69%)
- 10.64.4.5: 55641 packets (39.55%)
- 13.126.130.109: 8449 packets (6.01%)
- 10.65.0.5: 5320 packets (3.78%)
- 10.10.10.111: 5142 packets (3.66%)

Top 5 Destination IP Addresses:

- 13.126.130.109: 62745 packets (44.60%)
- 10.10.10.111: 55811 packets (39.67%)
- 20.204.169.2: 8467 packets (6.02%)
- 10.10.3.38: 5320 packets (3.78%)
- 10.64.4.5: 5023 packets (3.57%)

Top 10 Ports:

- Port 4500: 142586 packets (101.35%)
- Port 1500: 60953 packets (43.33%)
- Port 58280: 14319 packets (10.18%)
- Port 58296: 13585 packets (9.66%)
- Port 58284: 11328 packets (8.05%)
- Port 58310: 11222 packets (7.98%)
- Port 58302: 10210 packets (7.26%)
- Port 22: 8300 packets (5.90%)
- Port 54887: 8300 packets (5.90%)
- Port 48782: 90 packets (0.06%)

Packet Size Statistics:

- Average: 129.34 bytes
- Median: 134.00 bytes
- Standard Deviation: 17.02 bytes

TCP Flags Distribution:

- A: 55624 (80.21%)
- PA: 13647 (19.68%)
- SEC: 35 (0.05%)
- S: 27 (0.04%)
- RA: 12 (0.02%)

Traffic Distribution by Hour:

- Hour 18: 140682 packets (100.00%)

Top 5 Conversations:

- 20.204.169.2 <-> 13.126.130.109: 62745 packets (44.60%)
- 10.64.4.5 <-> 10.10.10.111: 55641 packets (39.55%)
- 13.126.130.109 <-> 20.204.169.2: 8449 packets (6.01%)
- 10.65.0.5 <-> 10.10.3.38: 5320 packets (3.78%)
- 10.10.10.111 <-> 10.64.4.5: 5023 packets (3.57%)

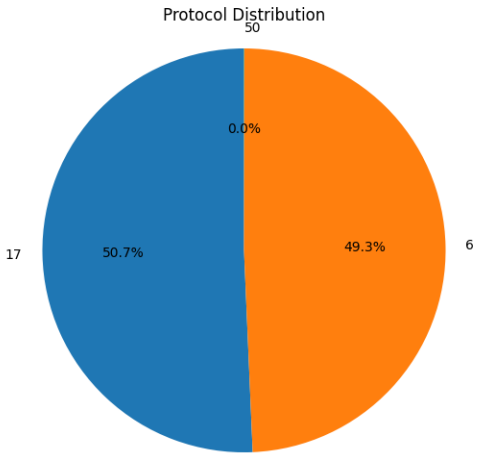
Average TTL: 168.31

Average TCP Window Size: 886.67 bytes

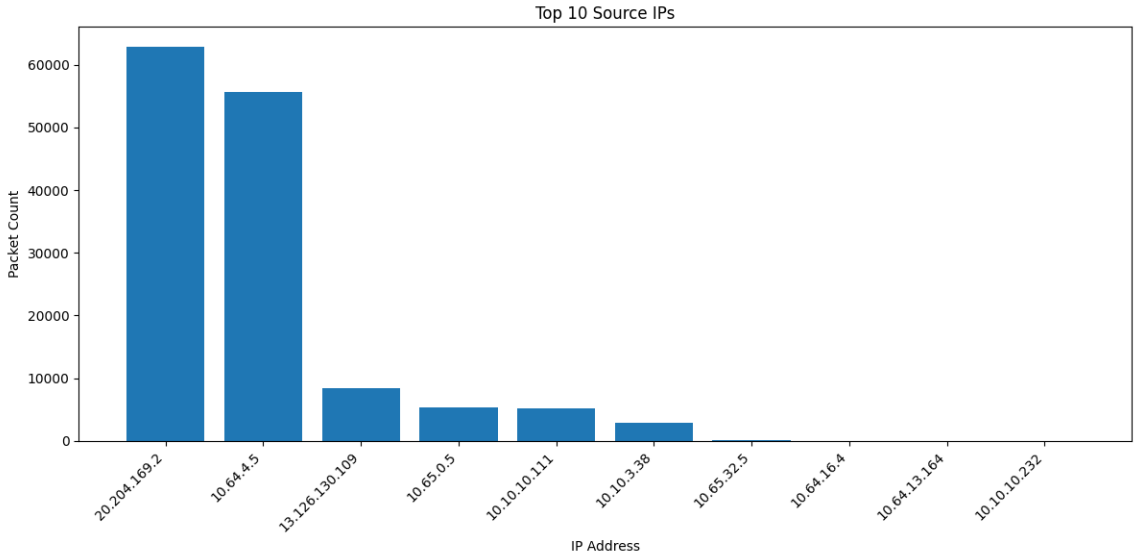
Average UDP Datagram Length: 1123.17 bytes

Visual Analysis

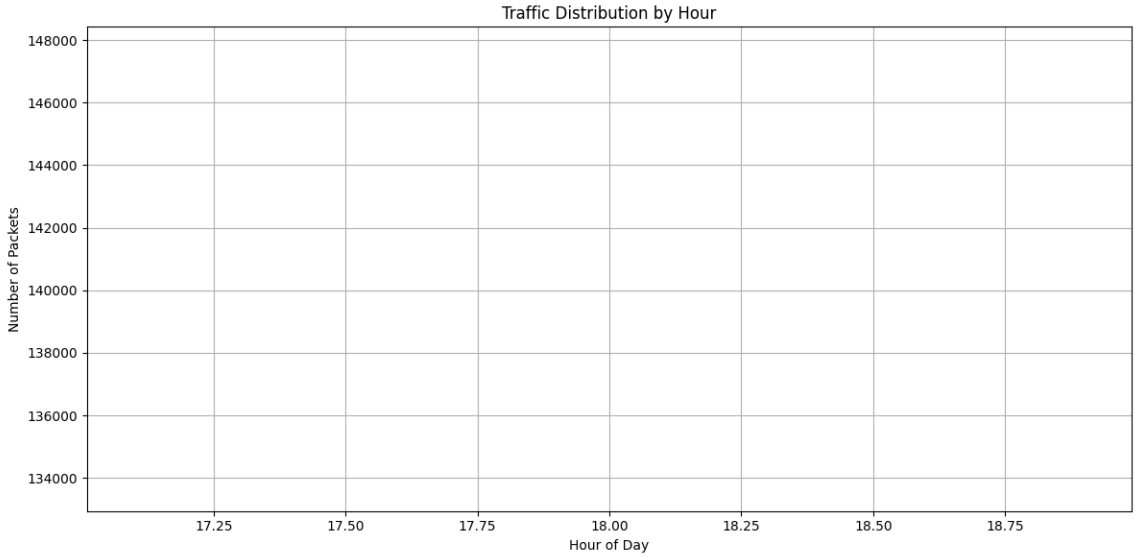
Protocol Distribution



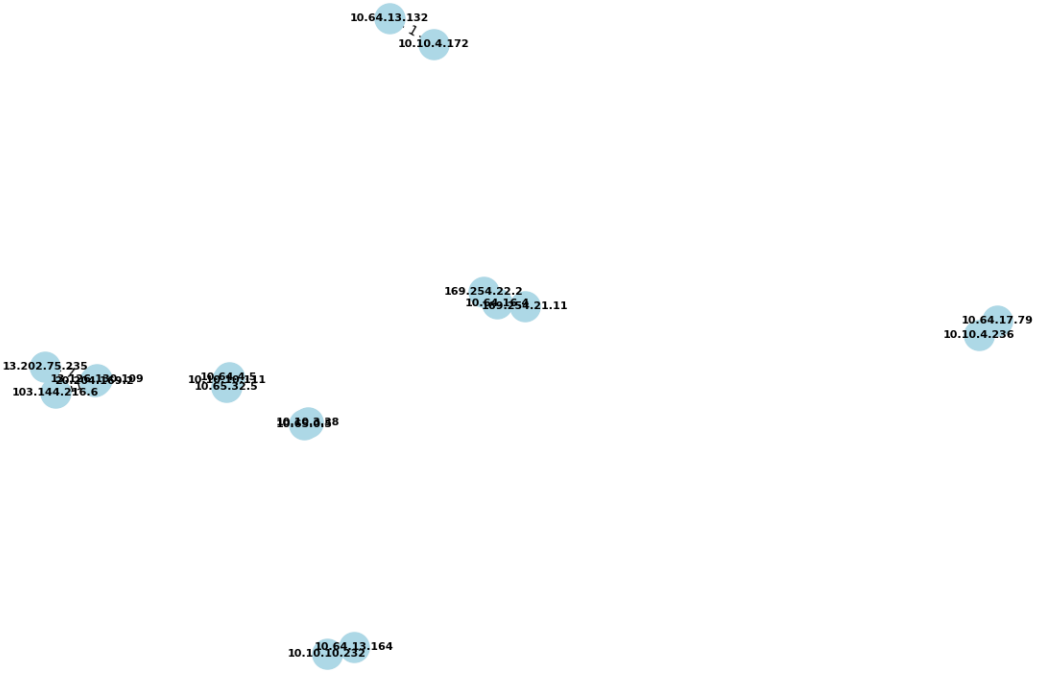
Top 10 Source IPs



Traffic Distribution by Hour



Network Communication Graph



Security Concerns

• High traffic on unusual ports: 4500, 54887, 58302, 1500, 58280, 58310, 58284, 58296

Recommendations

• Review and potentially restrict traffic on identified unusual ports.

• Consider network capacity upgrades to handle high traffic volume.