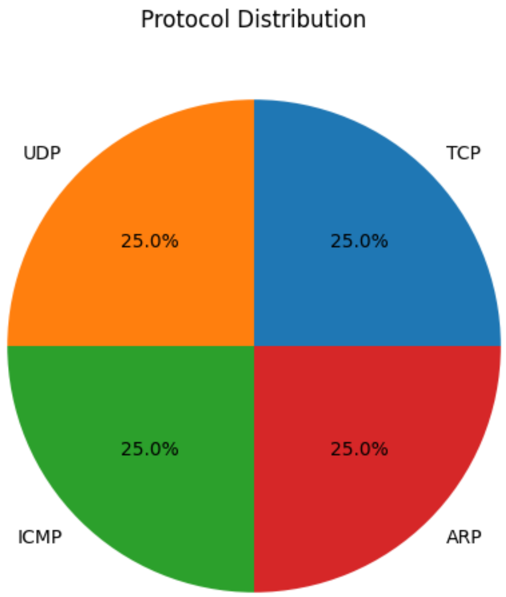
Network Security Analysis Report

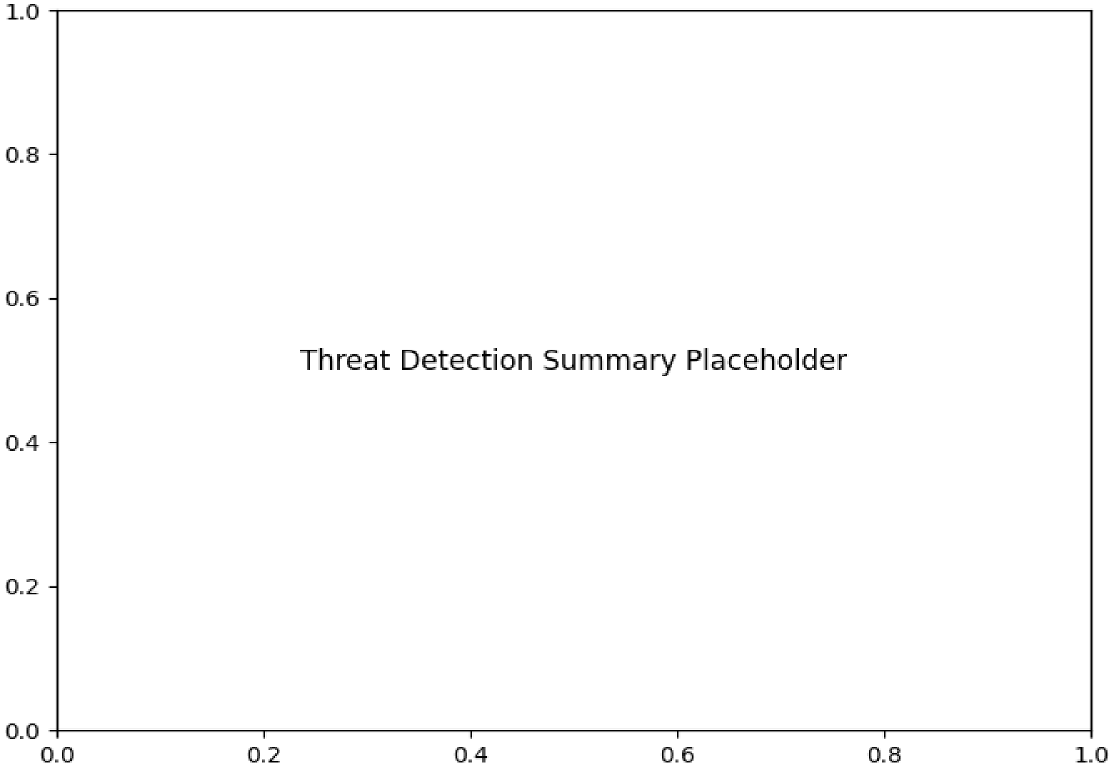
AI-Powered Security Insights

# Network Traffic Analysis Security Report ## Executive Summary - **Critical threats detected**: DNS tunneling attempts, ARP poisoning incidents, and anomalous traffic spikes from internal/external IPs. - **Primary offender**: IP `192.168.1.104` linked to **4674 anomalous traffic events** and repeated DNS tunneling attempts. - **External IPs of concern**: `151.101.129.140` (4,886 events), `151.101.193.140` (4,924 events), and `216.58.203.98` (17 events) showing high traffic volumes. - **Network integrity risks**: ARP poisoning involving gateway IP `192.168.1.1` (34 instances) and endpoint `192.168.1.104`. ## Risk Assessment ### **Critical Severity** - **DNS tunneling via 192.168.1.104**: 215 detections paired with 4,674 traffic anomalies. - **ARP poisoning at gateway (192.168.1.1)**: 34 instances of MAC address spoofing. - **Sustained volumetric traffic from external IPs**: Three `151.101.*.140` IPs collectively triggered **9,871 anomalies**. ### **High Severity** - **Endpoint ARP spoofing (192.168.1.104)**: 1 instance of MAC address conflict. - **UDP scan activity**: 1 detection of sub-8-byte packets (potential reconnaissance). ### **Moderate Severity** - Low-volume anomalies from `104.74.36.68` (5 events) and `151.101.65.140` (1 event). ## Threat Observations - **DNS tunneling pattern**: - Top 5 threats (packets #556, 557, 600, 602, 604) show UDP/DNS traffic from `192.168.1.104` to gateway `192.168.1.1`. - **Payload analysis recommended**: Tunneling often uses long DNS queries or non-standard record types. - **ARP cache poisoning**: - Gateway IP `192.168.1.1` mapped to multiple MACs, suggesting **man-in-the-middle attacks**. - Endpoint `192.168.1.104` also flagged for MAC spoofing. - **Traffic volume outliers**: - Internal IP `192.168.1.104` generated **4674 anomalies** (likely exfiltration/C2 activity). - External IPs `151.101.129.140` and `151.101.193.140` exceed 4,800 events each (potential DDoS/data harvesting). ## Recommendations ### **Immediate Actions** - **Quarantine 192.168.1.104**: Investigate for malware/unauthorized tools (e.g., dnscat2, Iodine). - **Block malicious external IPs**: Add `151.101.129.140`, `151.101.193.140`, and `216.58.203.98` to firewall denylist. - **Enable ARP inspection**: Configure switches to validate MAC-IP bindings and log ARP changes. ### **Network Hardening** - **Deploy DNS filtering**: Block non-standard DNS query types (TXT, NULL) and limit query length. - **Implement traffic baselining**: Use ML-driven tools to flag volumetric deviations (>1,000 packets/IP/5min). - **Enforce UDP restrictions**: Rate-limit UDP packets ≤8 bytes to mitigate scans. ### **Forensic Follow-Up** - **Analyze DNS logs**: Extract payloads from `192.168.1.104`’s UDP/DNS sessions for encoded data. - **Review gateway traffic**: Inspect `192.168.1.1` for asymmetric routing or unexpected outbound flows. - **Update IDS/IPS signatures**: Prioritize DNS tunneling and ARP spoofing detection rules.

Protocol Distribution



Threat Detection Summary



Detection Type	Count
Potential DNS tunneling detected	215
ARP poisoning detected: IP 192.168.1.1 has multiple MAC addresses.	34
Anomalous traffic volume detected from IP 192.168.1.104	4674
Anomalous traffic volume detected from IP 151.101.129.140	4886
Anomalous traffic volume detected from IP 151.101.1.140	61
UDP scan detected: Packet length <= 8	1
Anomalous traffic volume detected from IP 192.168.1.1	180
ARP poisoning detected: IP 192.168.1.104 has multiple MAC addresses.	1
Anomalous traffic volume detected from IP 151.101.193.140	4924
Anomalous traffic volume detected from IP 104.74.36.68	5
Anomalous traffic volume detected from IP 151.101.65.140	1
Anomalous traffic volume detected from IP 216.58.203.98	17