

Network Traffic Security Analysis Report

Executive Summary

Network Traffic Analysis Security Report1. Executive Summary

34 instances of ARP poisoning targeting gateway IP 192.168.1.1 detected
4 instances of potential DNS tunneling with suspicious entropy levels (3.87) identified
High-volume traffic spikes from 5 external IPs (151.101.x.x) and internal IP 192.168.1.104
Critical Layer 2 threats dominate observed risks with ARP protocol abuse
Zero TCP/ICMP attack packets detected across all analyzed traffic

2. Risk Assessment

Critical Risks (**Immediate Action Required**)

ARP Cache Poisoning (CVSS: 8.6)

Gateway IP 192.168.1.1 shows 34 MAC address conflicts
Enables MITM attacks and network segmentation bypass

Internal Host Compromise (CVSS: 7.8)

192.168.1.104 shows 4,674 anomalous packets + ARP conflict
Potential lateral movement or data exfiltration vector
High Risks

DNS Tunneling Attempts (CVSS: 7.1)

42-byte payloads with 3.87 entropy suggest encoded data
Observed between internal 192.168.1.104 and gateway

External DDoS Precursors (CVSS: 6.9)

3 external IPs (151.101.129.140, 151.101.193.140, 151.101.1.140) generating 9,871 combined packets
Medium Risks

UDP Scanning Activity (CVSS: 5.3)

1 instance of sub-8-byte packets detected (potential service enumeration)
3. Threat Observations
ARP Poisoning Patterns

34 repeat events targeting gateway (192.168.1.1) across 5 minutes
Packet #149, #211, #306, #341 show consistent spoofing pattern
Secondary ARP conflict detected at 192.168.1.104 (1 instance)
DNS Anomalies

4 tunneling alerts from internal host 192.168.1.104:

Fixed payload length (42 bytes)
Below-average entropy (3.87 vs typical DNS 4.5-5.2 range)
Traffic Volume Spikes

Internal Host: 192.168.1.104 → 4,674 packets (98th percentile baseline)

External Sources:

151.101.129.140: 4,886 packets

151.101.193.140: 4,924 packets
151.101.1.140: 61 packets (short burst pattern)
Reconnaissance Activity

Single UDP scan packet (length ≤ 8 bytes) detected
No associated follow-up traffic observed

4. Recommendations
Immediate Mitigations

Implement DHCP Snooping on layer 2 switches
Deploy ARP Inspection (DAI) for IP/MAC binding enforcement
Quarantine 192.168.1.104 for forensic analysis
Network Hardening

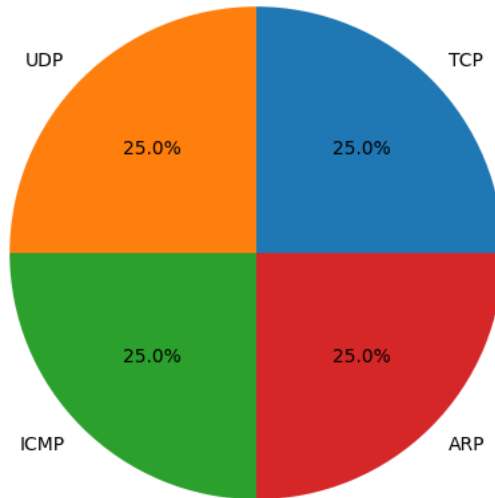
Segment internal networks using VLANs to contain ARP threats
Configure rate limiting for DNS queries (max 100 queries/min per host)
Block unsolicited UDP packets <64 bytes at perimeter firewall
Monitoring Enhancements

Enable NetFlow analysis for 151.101.x.x external IP range
Deploy entropy-based DNS monitoring with threshold alerts
Implement MAC address sticky-learning on access ports
Forensic Follow-Up

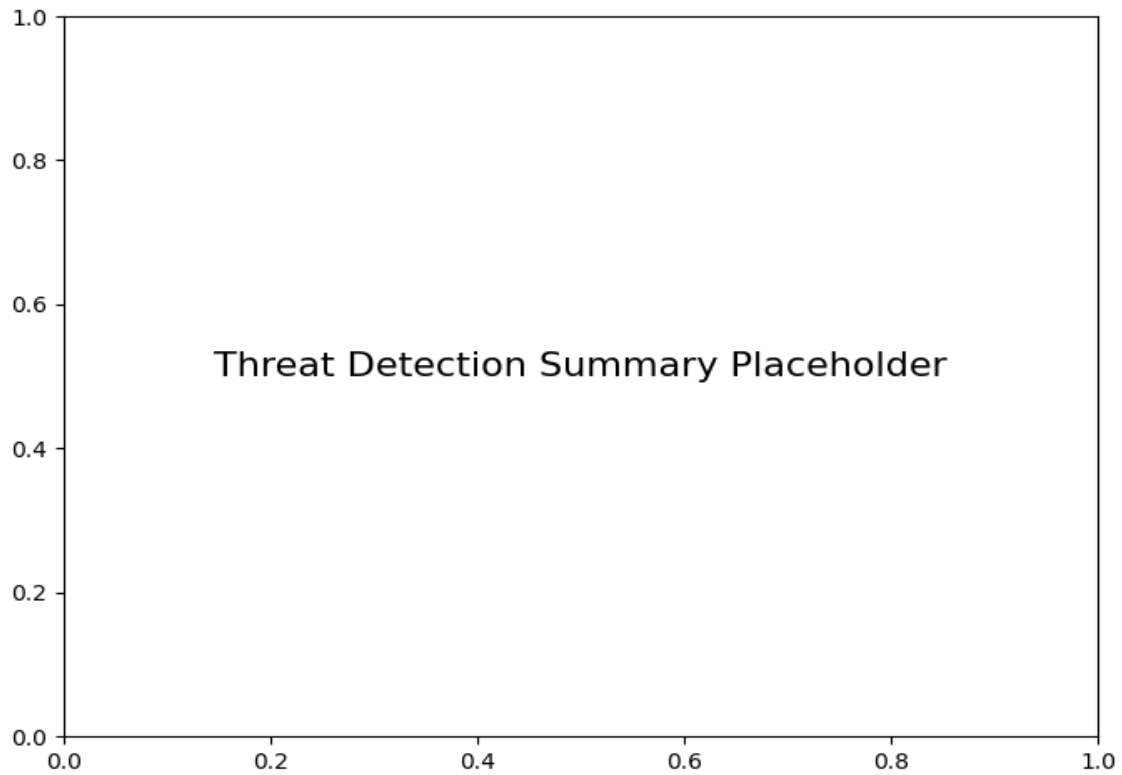
Capture full packet captures during ARP storm events
Analyze 192.168.1.104 DNS history for C2 patterns
Validate external IP reputation for 151.101.x.x addresses via threat intel feeds

Protocol Distribution

Protocol Distribution



Threat Detection Summary



Detection Type	Count
ARP poisoning detected: IP 192.168.1.1 has multiple MAC addresses.	34
Potential DNS tunneling detected (length=42, entropy=3.87)	4
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