Network Traffic Security Analysis Report

Executive Summary

Network Traffic Analysis Security Report1. Executive Summary

Critical anomalies detected: DNS tunneling, ARP poisoning, and sustained traffic spikes from internal/external IPs.
Primary threat actor: Internal IP 192.168.1.104 linked to **4674 anomalous traffic events** and **215 DNS tunneling alerts**.
External risks: High-volume traffic from external IPs (e.g., 151.101.129.140, 151.101.193.140) exceeding 4800 events each.
Active attacks: ARP spoofing involving gateway IP 192.168.1.1 (34 alerts) and endpoint 192.168.1.104.
2. Risk Assessment
Critical Vulnerabilities

DNS tunneling via 192.168.1.104 (Severity: Critical)
215 detections indicating potential data exfiltration/C2 communication.
ARP poisoning at gateway (192.168.1.1) (Severity: Critical)
34 alerts: MAC address conflicts suggest man-in-the-middle (MitM) attacks.
Anomalous traffic from internal IP 192.168.1.104 (Severity: High)
4674 events: Likely indicative of malware propagation or DDoS participation.
Secondary Risks

High-volume external traffic (Severity: Medium)
IPs 151.101.129.140 (4886 events) and 151.101.193.140 (4924 events): Potential DDoS sources or data exfiltration.
Single UDP scan event (Severity: Low)
Packet length ≤8 bytes: Reconnaissance activity but limited scope.
3. Threat Observations
DNS Tunneling

Source IP 192.168.1.104 generated 215 DNS tunneling alerts (e.g., packets 556, 557, 600, 602, 604).
Traffic patterns: Repeated UDP/DNS requests to gateway (192.168.1.1) with no resolved ports.
ARP Poisoning

Gateway IP 192.168.1.1: 34 MAC address conflicts.
Endpoint IP 192.168.1.104: 1 MAC conflict, suggesting bidirectional spoofing.
Traffic Anomalies

Internal IPs:
192.168.1.104: 4674 events (highest internal volume).
192.168.1.1: 180 events (unusual for gateway devices).
External IPs:
151.101.129.140 (4886) and 151.101.193.140 (4924): Traffic spikes likely non-legitimate.
Reconnaissance

UDP scan: 1 event with minimal packet length (≤8 bytes), possibly testing network responsiveness.

4. Recommendations

Immediate Actions

Isolate 192.168.1.104: Conduct forensic analysis for malware, DNS tunneling tools, or C2 artifacts.

Mitigate ARP spoofing:

Enable DHCP snooping and dynamic ARP inspection on network switches.

Audit MAC address tables for rogue devices.

Block malicious external IPs: Temporarily restrict traffic from 151.101.129.140 and 151.101.193.140 pending investigation.

Long-Term Controls

Implement DNS monitoring: Deploy anomaly-based DNS filtering (e.g., block oversized/obfuscated DNS queries).

Enforce rate limiting: Throttle UDP/DNS traffic volumes per device to disrupt tunneling.

Update IDS/IPS signatures: Prioritize rules for DNS tunneling (e.g., TXT/NULL record abuse) and ARP anomalies.

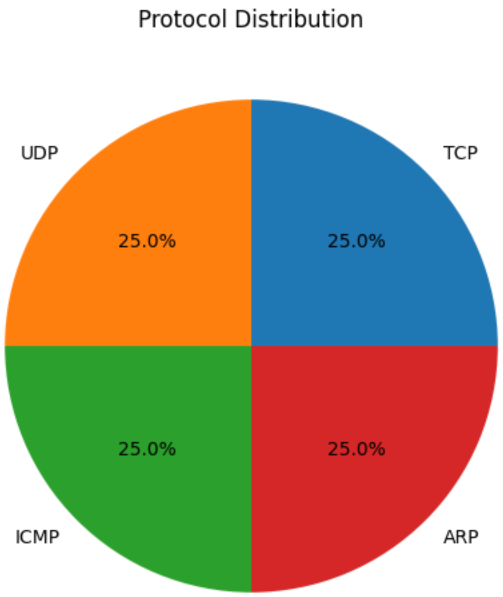
Network Hardening

Segment critical infrastructure: Separate gateway (192.168.1.1) from user devices.

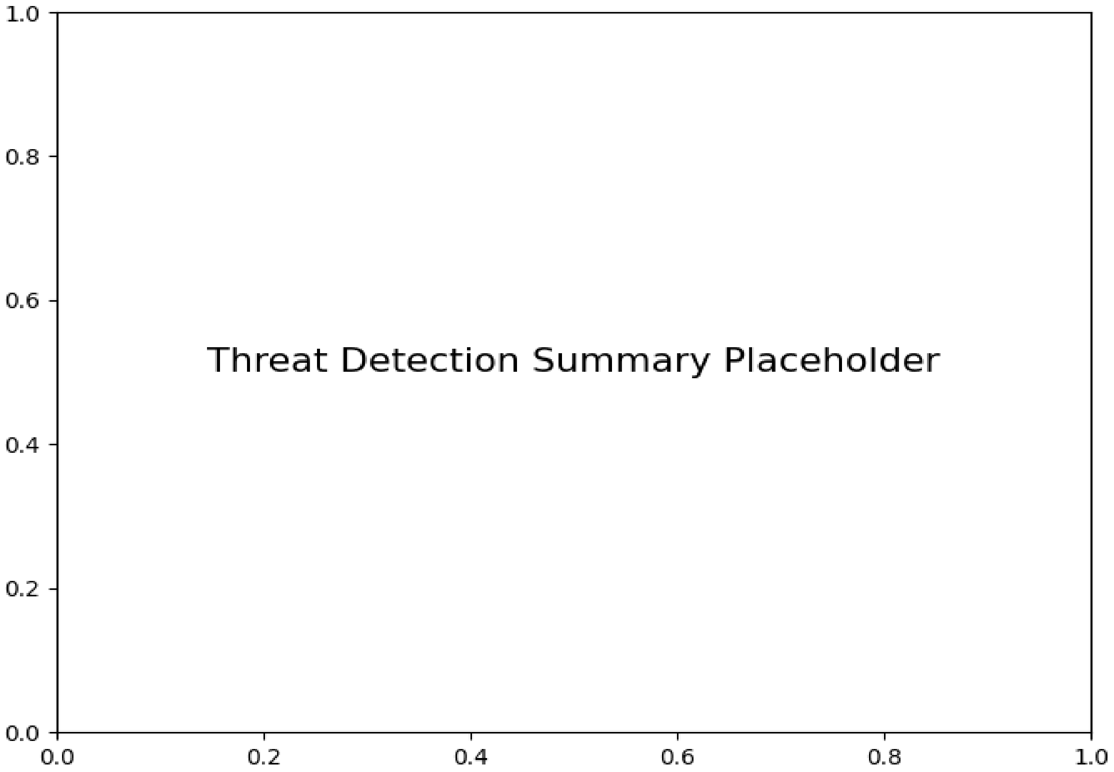
Deploy endpoint protection: Mandate host-based firewalls and ARP spoofing detection tools on all devices.

Review firewall rules: Block unsolicited UDP traffic and enforce strict egress filtering.

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