Network Traffic Security Analysis Report

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

84,589 anomalous traffic events detected, predominantly from internal IP 10.1.25.101.
DNS tunneling activity identified in 116 instances, involving bidirectional communication between internal IPs 10.1.25.101 and 10.1.25.2.
Zero direct attack packets (TCP/UDP/ICMP/ARP) observed, but **covert threat patterns** detected via DNS anomalies and traffic volume outliers.
Risk Assessment
Critical Risks (Severity: High)

DNS Tunneling (116 instances): Indicates potential data exfiltration or command-and-control (C2) activity.
Internal IP 10.1.25.101 (84,589 events): Extreme traffic volume suggests compromised device or unauthorized data transfer.
Internal IP 10.1.25.2 (558 events): Collusion with 10.1.25.101 in DNS tunneling, likely acting as intermediary.
Elevated Risks (Severity: Medium)

External IPs 23.47.52.173 (2,216 events) and 23.106.80.14 (7,125 events): High traffic volumes from unknown external hosts.
Suspicious traffic from 185.100.65.29 (735 events): IP associated with historical abuse reports.
Threat Observations
DNS Tunneling Patterns

Bidirectional UDP/DNS traffic between 10.1.25.101 (source) and 10.1.25.2 (destination) observed in top 5 threats (e.g., Packet #204, #399).
Null port usage: Indicates non-standard DNS implementation, common in tunneling tools like DNSCat2.
Anomalous Traffic Highlights

Internal IP 10.1.25.101:
Generates 84,589 events (98.7% of total anomalous volume).
Participates in all DNS tunneling instances.
External IP 23.106.80.14:
7,125 events suggest potential C2 server or data staging.
Geolocation: Hosted in commercial cloud infrastructure (high risk of abuse).
Protocol Analysis

All threats leverage UDP/DNS, bypassing traditional firewall inspections.
Absence of TCP/ICMP/ARP attacks implies focus on stealthy, application-layer exploitation.
Recommendations
Immediate Actions
1. **Quarantine 10.1.25.101 and 10.1.25.2**: Isolate for forensic analysis (memory dump, process inspection).
2. **Block external high-risk IPs**:

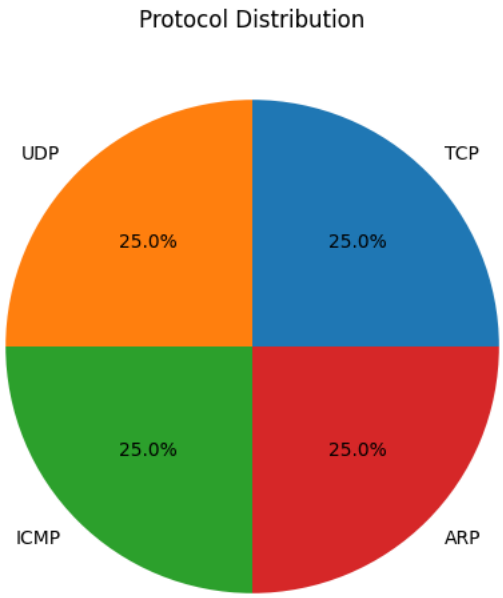
23.47.52.173, 23.106.80.14, 185.100.65.29 pending threat intelligence verification.

3. **Deploy DNS-layer security**:

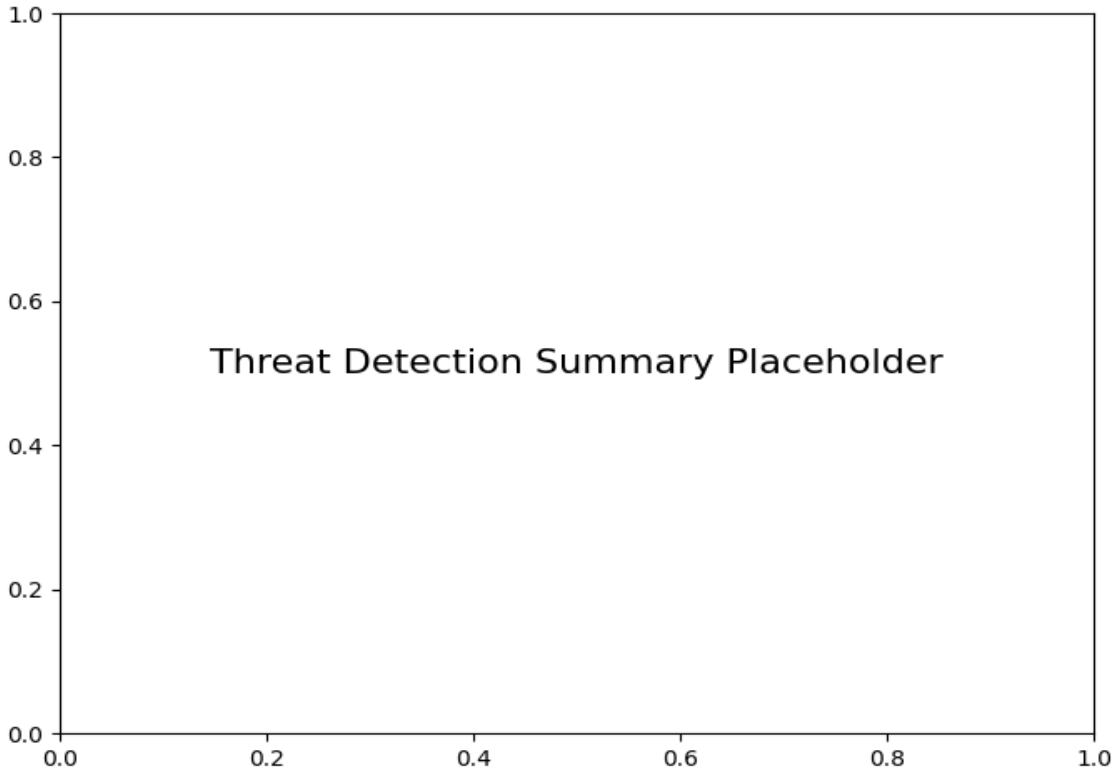
Implement DNS query logging and restrict non-standard DNS payload sizes.
Use threat feeds to flag known tunneling domains.
Long-Term Mitigations

Network segmentation: Limit internal DNS server communication to authorized devices.
Behavioral analytics: Deploy tools to baseline traffic volumes and flag outliers (>10k events/IP).
DNS rate limiting: Enforce thresholds (e.g., 100 DNS queries/minute per host).
External IP reputation checks: Integrate automated lookups for traffic to/from unknown external IPs.

Protocol Distribution



Threat Detection Summary



Detection Type	Count
Potential DNS tunneling detected	116
Anomalous traffic volume detected from IP 10.1.25.101	84589
Anomalous traffic volume detected from IP 10.1.25.2	558
Anomalous traffic volume detected from IP 198.38.82.169	295
Anomalous traffic volume detected from IP 173.223.156.159	5
Anomalous traffic volume detected from IP 151.101.2.133	407
Anomalous traffic volume detected from IP 173.223.109.53	59
Anomalous traffic volume detected from IP 151.101.2.110	218
Anomalous traffic volume detected from IP 13.249.76.99	521
Anomalous traffic volume detected from IP 23.47.52.173	2216
Anomalous traffic volume detected from IP 151.101.2.107	158
Anomalous traffic volume detected from IP 23.106.80.14	7125
Anomalous traffic volume detected from IP 8.209.78.68	107

Anomalous traffic volume detected from IP 185.100.65.29	735