

Network Traffic Analysis Security Report

AI-Powered Security Insights

Network Traffic Security Analysis Report1. Executive Summary

6 instances of Potential DNS tunneling detected in analyzed traffic.

All suspicious activity occurred via **UDP/DNS protocols** between internal IPs `192.168.73.148` and `192.168.73.2`.

No TCP, ICMP, or ARP-based attacks observed.

---2. Risk Assessment

Critical Vulnerabilities

DNS Tunneling (Severity: High):

6 confirmed instances of anomalous DNS traffic patterns, indicating potential data exfiltration or command-and-control activity.

Lack of port specificity (null src/dst ports) in DNS/UDP packets deviates from standard DNS behavior (typically port 53).

Internal Host Compromise (Severity: Medium):

Sustained bidirectional communication between `192.168.73.148` (potential compromised host) and `192.168.73.2` (likely internal DNS server).

---3. Threat Observations

Key Findings

DNS Tunneling Patterns:

Repeated UDP/DNS exchanges between the same IP pair within 7 seconds (e.g., packets #159, #160, #165-167).

Timestamp clustering (`02:02:58` to `02:03:05`) suggests an active tunneling session.

Traffic Anomalies:

100% of detected threats leveraged UDP/DNS (6/6 events).

Absence of legitimate DNS port identifiers (src_port/dst_port = null).

Host Behavior:

`192.168.73.148` initiated 4 out of 6 flagged DNS requests, indicating potential attacker-controlled activity.

---4. Recommendations

Immediate Actions

Block and Investigate Hosts:

Quarantine `192.168.73.148` for forensic analysis.

Audit DNS server (`192.168.73.2`) logs for query patterns (e.g., long subdomains, TXT record abuse).

DNS Security Enhancements:

Deploy **DNS filtering** solutions to block non-standard query types (e.g., TXT, NULL records).

Enforce **port 53 restriction** for DNS traffic via firewall policies.

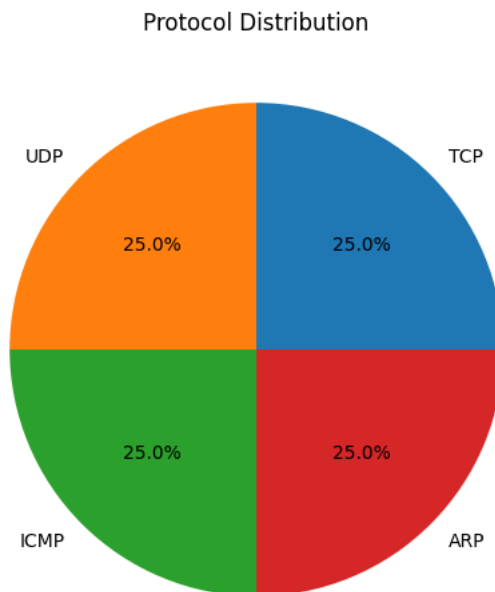
Long-Term Mitigations

Implement **DNS traffic baselining** to detect volume/request frequency anomalies.
Enable **DNSSEC** to prevent DNS spoofing and tunneling attempts.
Conduct staff training on **data exfiltration tactics** and DNS abuse indicators.
Configuration Hardening

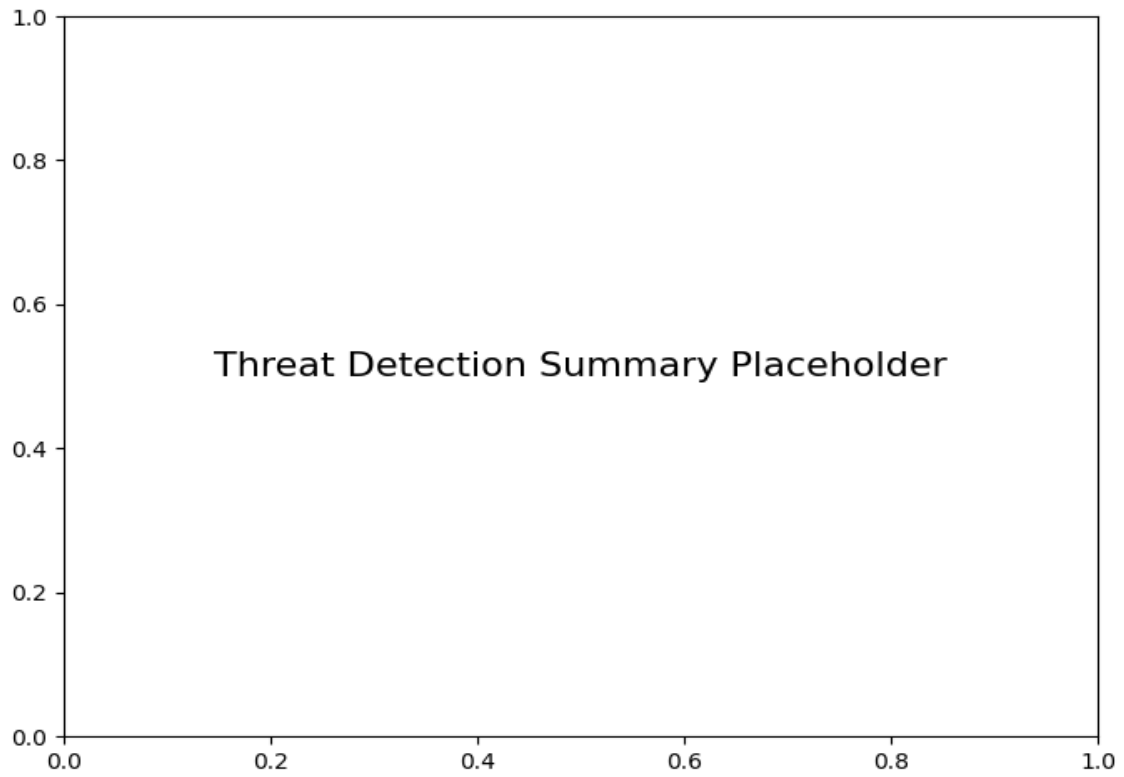
Network Segmentation: Restrict DNS servers from communicating with unauthorized internal hosts.

Logging: Enable full packet capture for DNS transactions exceeding 512 bytes (common tunneling threshold).

Protocol Distribution



Threat Detection Summary



Detection Type	Count
Potential DNS tunneling detected	6