Network Security Analysis Report

AI-Powered Security Insights

Network Traffic Analysis Security Report
Executive Summary

6 instances of Potential DNS tunneling detected in analyzed traffic patterns
Suspicious activity concentrated between two internal IP addresses (192.168.73.148 ↔ 192.168.73.2)
No traditional attack packets (TCP/UDP/ICMP/ARP) observed in attack statistics
Repeated DNS-over-UDP transactions suggest covert channel activity

Risk Assessment

Critical Risk: DNS Tunneling Attempts

Severity: High - Potential data exfiltration/command channel hidden in DNS traffic
Internal Compromise Risk

Severity: Medium - Suspicious communication between internal endpoints (192.168.73.148 and 192.168.73.2)
Protocol Anomaly

Severity: Medium - Null port values in DNS traffic contradict standard implementations (DNS typically uses port 53)

Threat Observations

Pattern Analysis
5 consecutive DNS tunneling events within 6-second window (Packets #159-167)
Bidirectional communication pattern between endpoints

Consistent UDP/DNS protocol stack usage

Key Artifacts

Packet #159: Initial tunneling attempt from 192.168.73.148 to 192.168.73.2
Packet #160: Response from 192.168.73.2 to originator

Repeating pattern observed in Packets #165-167

Technical Indicators

Absence of standard DNS port identifiers (null port values)
High-frequency DNS transactions (5 events in 6 seconds)
Lack of legitimate service discovery preceding events

Recommendations

Immediate Actions
Quarantine endpoint 192.168.73.148 for forensic analysis

Inspect DNS server (192.168.73.2) logs for:

Unusually large TXT/Null records
Non-standard query types (AXFR, ANY)
Base64/Hex encoded subdomains

Network Hardening

Implement DNS filtering policies to:
Block non-standard DNS record types
Enforce maximum query length (≤ 100 characters)
Require explicit port 53 usage

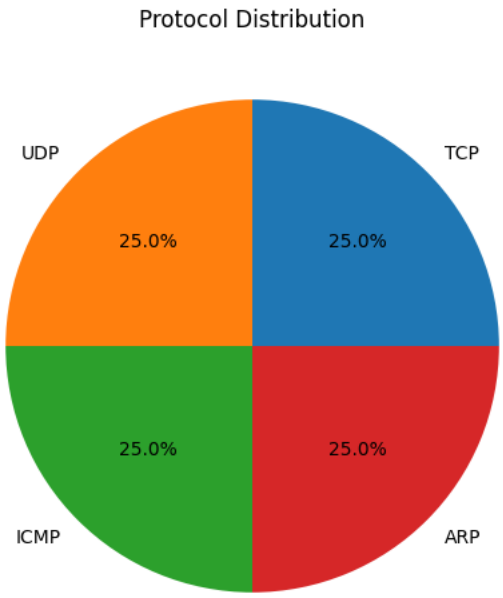
Deploy protocol anomaly detection for:

DNS traffic without port identifiers
Rapid DNS query patterns (>1 query/sec from single host)

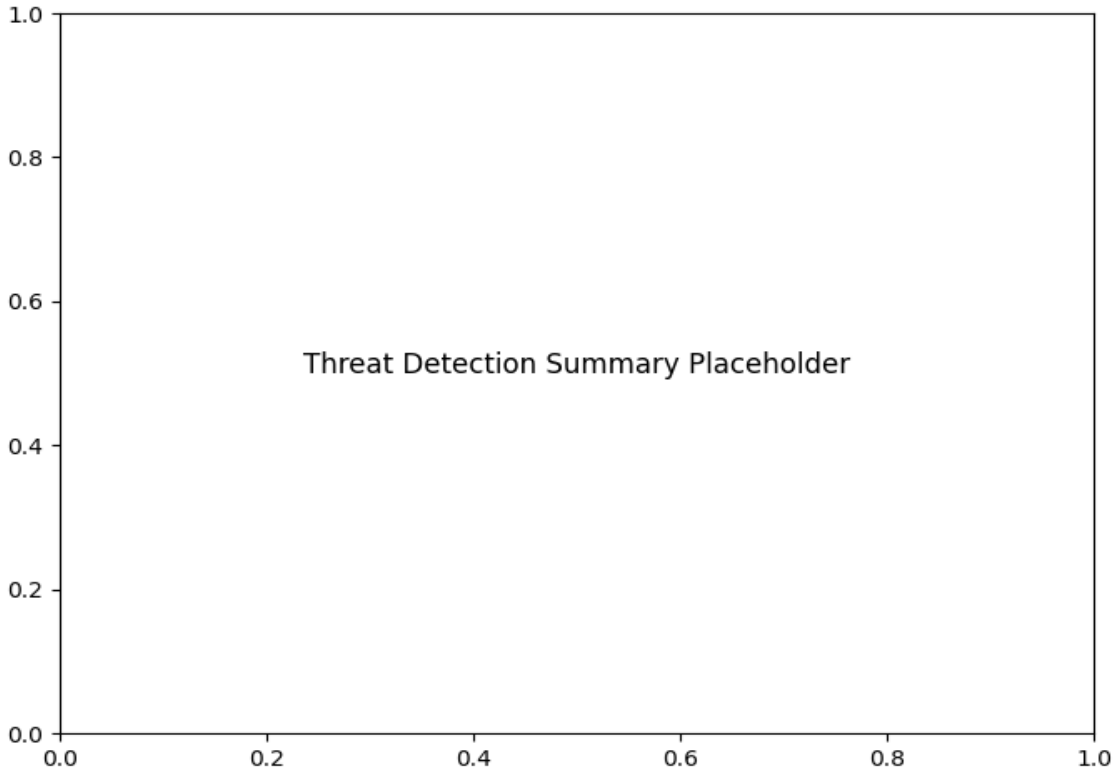
Long-Term Controls

Establish baseline DNS behavior metrics
Implement DNSSEC validation
Configure network segmentation to restrict DNS server communication
Conduct user training on DNS tunneling indicators

Protocol Distribution



Threat Detection Summary



Detection Type	Count
Potential DNS tunneling detected	6