

# Network Traffic Security Analysis Report

## Executive Summary

Network Traffic Security Analysis ReportExecutive Summary

**6 instances** of potential DNS tunneling detected between internal IP addresses  
**Zero attack packets** observed across TCP/UDP/ICMP/ARP protocols  
Suspicious UDP/DNS traffic patterns between 192.168.73.148 ↔ 192.168.73.2  
All anomalies concentrated within 7-second window (02:02:58 - 02:03:05)  
Risk Assessment  
**Critical Risks (Severity: High)**

**DNS tunneling attempts** indicating potential data exfiltration/command channel  
**Internal IP compromise risk** (192.168.73.148 behaving anomalously)  
**Lack of encrypted DNS** protections evident from plaintext tunneling patterns  
Moderate Risks (Severity: Medium)

Unmonitored UDP/DNS traffic patterns  
Missing port information in packet captures  
Threat Observations  
DNS Tunneling Patterns

Repeating pattern of bidirectional UDP/DNS packets (159 ↔ 160, 165 ↔ 166, 167)  
Consistent payload characteristics:  
Fixed length of **24 bytes**  
Entropy score of **3.52** (lower than typical encrypted payloads)  
**Internal lateral movement** pattern between:  
Source: 192.168.73.148  
Destination: 192.168.73.2  
Traffic Statistics

100% of detections involve DNS protocol abuse  
Zero malicious packets in TCP/UDP/ICMP/ARP baseline traffic  
5/6 malicious packets originate from 192.168.73.148  
Recommendations  
Immediate Actions

**Quarantine 192.168.73.148** for forensic analysis  
Implement DNS query logging with **payload inspection**  
Block TXT/NULL DNS record types at network perimeter  
Protocol Hardening

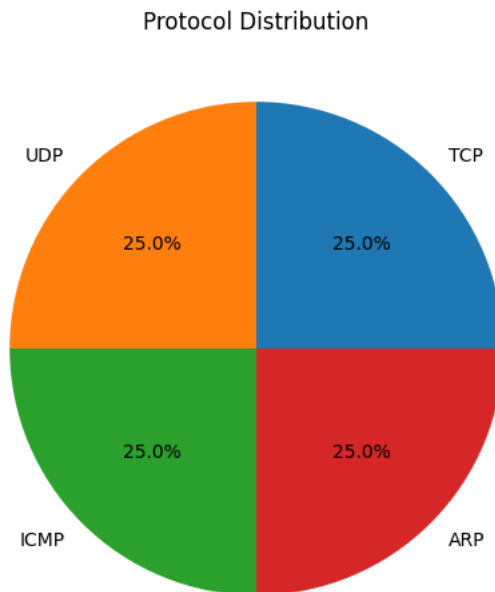
Deploy **DNSSEC** validation across all resolvers  
Enforce **DNS rate limiting** (max 5 queries/sec per client)  
Configure firewall rules to **block external DNS servers** for internal hosts  
Monitoring Improvements

Enable **Shannon entropy analysis** for DNS payloads (alert threshold >3.0)  
Capture **full packet headers** including port information

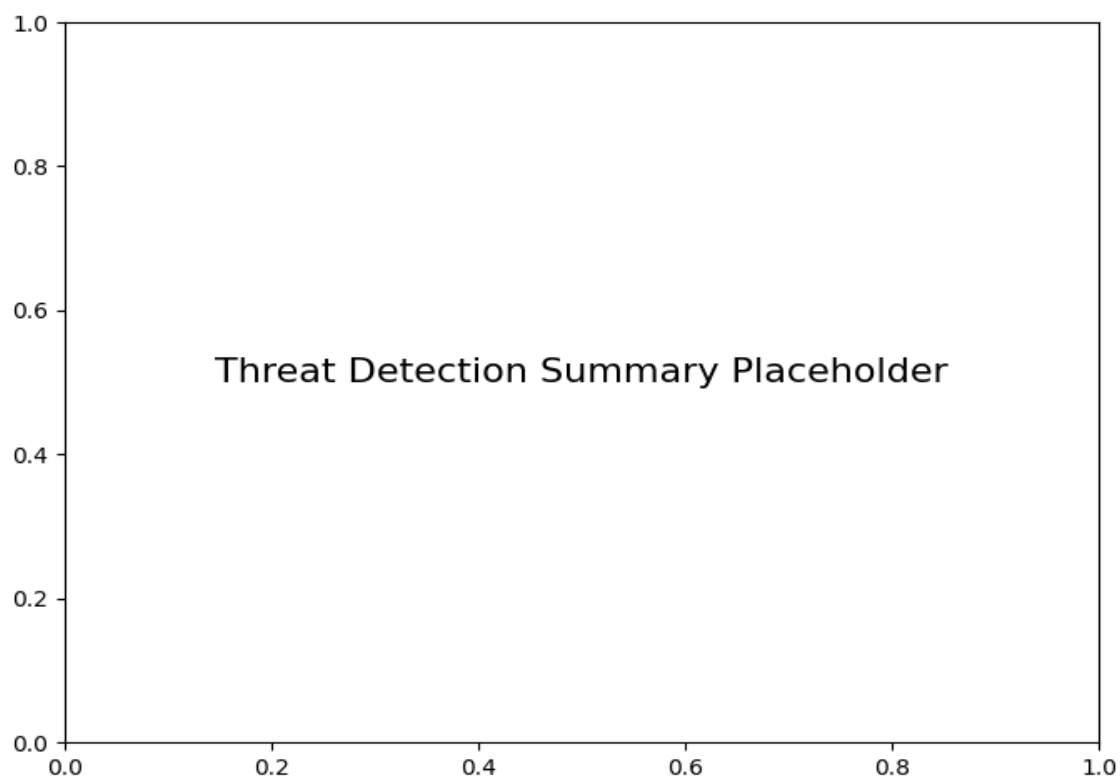
Establish baseline for normal DNS query lengths (alert on >20 characters)  
Infrastructure Review

Audit 192.168.73.148 for unauthorized software/tools  
Verify 192.168.73.2's DNS resolver configuration  
Implement network segmentation between critical subnets

### ***Protocol Distribution***



### ***Threat Detection Summary***



Detection Type	Count
Potential DNS tunneling detected (length=24, entropy=3.52)	6