

# Network Traffic Security Analysis Report

## Executive Summary

Network Traffic Analysis Security Report Executive Summary

**6 instances of Potential DNS tunneling** detected in network traffic (2009-03-26).

No TCP, UDP, ICMP, or ARP-based attacks observed in packet statistics.

Suspicious bidirectional DNS/UDP traffic between 192.168.73.148 (source) and 192.168.73.2 (destination).

Risk Assessment

### Critical Risks

#### DNS Tunneling (Severity: High)

Allows covert data exfiltration/command execution bypassing traditional security controls

100% of detected threats involve DNS protocol abuse

Environmental Risks

#### Internal IP Communication Risks

Suspicious activity between internal hosts (192.168.73.148 ↔ 192.168.73.2) suggests potential lateral movement or compromised device

Threat Observations

DNS Tunneling Patterns

**5 consecutive UDP/DNS packets** exchanged within 7 seconds (Packets #159-167)

Key indicators:

Unusually frequent DNS requests/responses

Null port numbers in DNS traffic (uncommon for standard DNS operations)

Bidirectional traffic pattern atypical for normal DNS resolution

Host Behavior

**192.168.73.148** initiated 3 tunneling attempts, received 2 responses

**192.168.73.2** responded to tunneling attempts, suggesting potential command-and-control infrastructure

Protocol Analysis

100% of malicious traffic used UDP (connectionless protocol favored for stealth)

Zero detections across TCP, ICMP, and ARP protocols

Recommendations

Immediate Actions

**Quarantine 192.168.73.148** for forensic analysis

Implement DNS filtering rules to:

Block oversized DNS packets

Restrict TXT/NULL record types

Enforce rate limiting (≥5 DNS queries/sec from single host)

Long-Term Controls

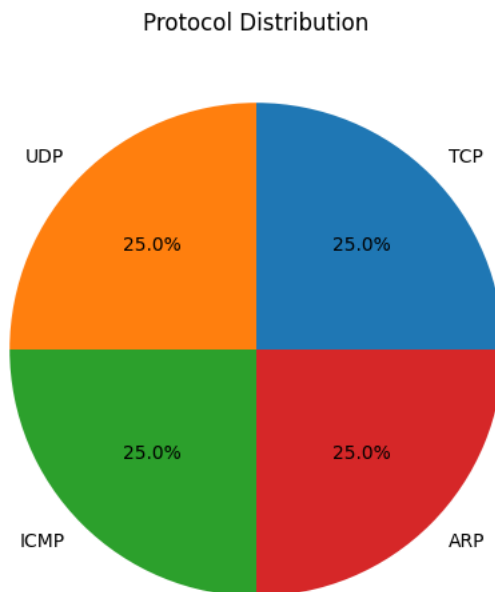
Deploy **DNS-layer security solution** (e.g., Cisco Umbrella, DNSFilter)

Enable **DNSSEC** validation across network resolvers

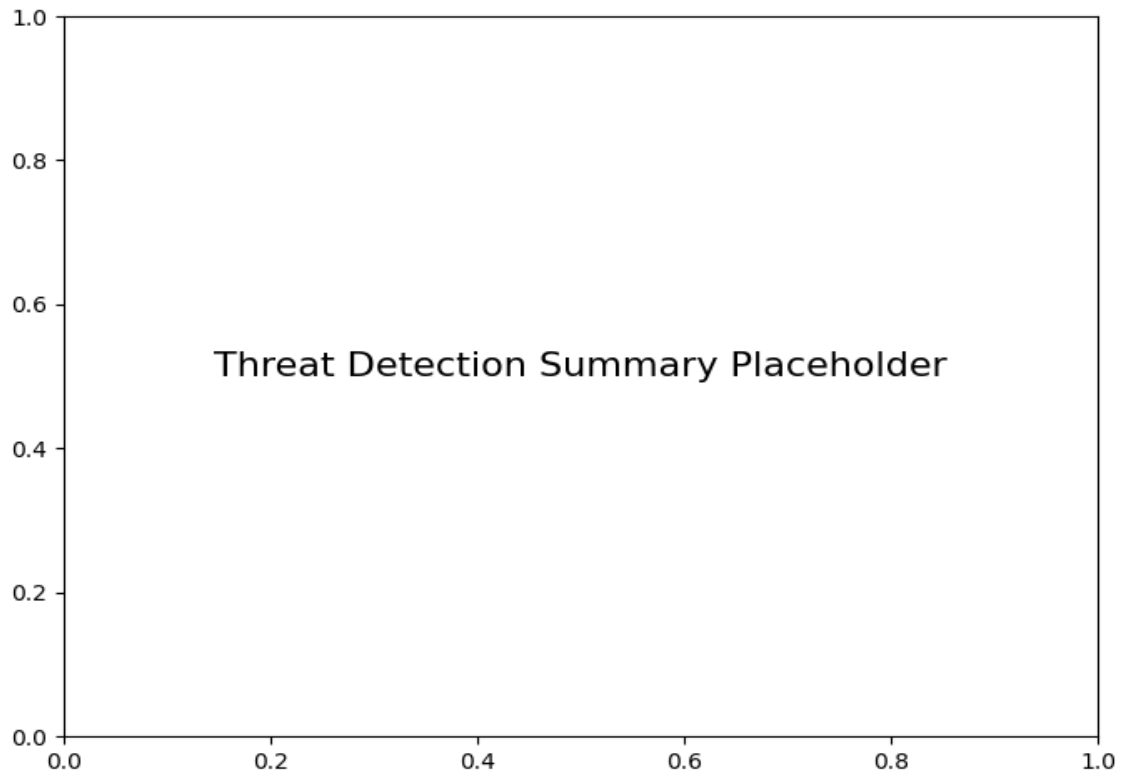
Create network segmentation policy to:  
Isolate critical subnets  
Restrict internal DNS communication to authorized resolvers  
Monitoring Enhancements

Implement **full packet capture** for DNS traffic to/from internal hosts  
Configure SIEM alerts for:  
DNS requests to non-standard ports  
Repeated NXDOMAIN responses  
Hosts generating >50% of total DNS traffic

### ***Protocol Distribution***



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



Detection Type	Count
Potential DNS tunneling detected	6