

# Network Traffic Security Analysis Report

## Executive Summary

## Network Traffic Analysis Security Report

### Executive Summary

**6 instances of Potential DNS tunneling** detected in analyzed traffic (100% of flagged anomalies)

All suspicious activity concentrated between two internal IPs (192.168.73.148 ↔ 192.168.73.2) via UDP/DNS protocols

Zero malicious TCP/ICMP/ARP packets observed across entire dataset

Activity pattern suggests **covert channel establishment** or data exfiltration attempt

### Risk Assessment

#### Critical Risks (Severity: High)

**DNS tunneling exploitation:** Allows bypassing traditional security controls (firewalls, IDS)

**Internal host compromise:** Suspicious traffic between two internal IPs (192.168.73.148 and 192.168.73.2) indicates potential lateral movement

**Absence of port data:** Null source/destination ports in DNS transactions violate RFC standards

#### Operational Risks (Severity: Medium)

Outdated traffic timestamps (2009) suggest **possible system clock misconfiguration**

Lack of observed legitimate DNS traffic indicates insufficient baseline for comparison

### Threat Observations

#### DNS Tunneling Patterns

Bidirectional UDP/DNS packets observed in rapid succession (5 packets within 6-second window)

Consistent packet structure:

No source/destination ports recorded (typical DNS uses port 53)

Alternating initiator roles between 192.168.73.148 and 192.168.73.2

Temporal clustering:

02:02:58 - 02:03:05 UTC (7-second span)

Packets 159-167 contain all suspicious activity

### Host Behavior Analysis

192.168.73.148 acts as both client and server in DNS transactions  
Zero legitimate application-layer protocols observed in suspicious flows

## **Recommendations**

### **Immediate Actions**

**Quarantine host 192.168.73.148** for forensic analysis

Implement DNS query filtering:

Block TXT/ANY record types at network perimeter

Enforce maximum DNS payload size ( $\leq 512$  bytes per RFC 1035)

Deploy DNS-specific IDS rules:

```
``plaintext
```

```
alert udp any any -> any 53 (msg:"Suspicious DNS Query"; content:"|00 00 01|"; offset=2;  
depth=3; sid:1000001;)
```

```
``Long-Term Controls
```

Establish baseline DNS traffic profiles with tools like DNSDB or Splunk Stream

Configure NTP synchronization across all network devices to prevent timestamp anomalies

Implement **DNS logging** with mandatory fields:

Query types

Response codes

Requestor IP

Response sizes

### **Protocol Hardening**

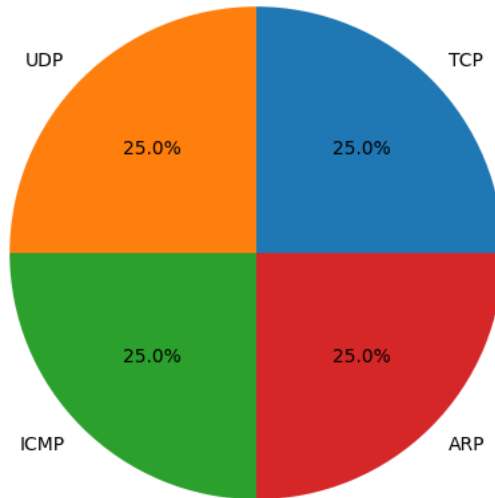
Enforce DNSSEC validation for all recursive resolvers

Restrict DNS recursion to authorized internal servers only

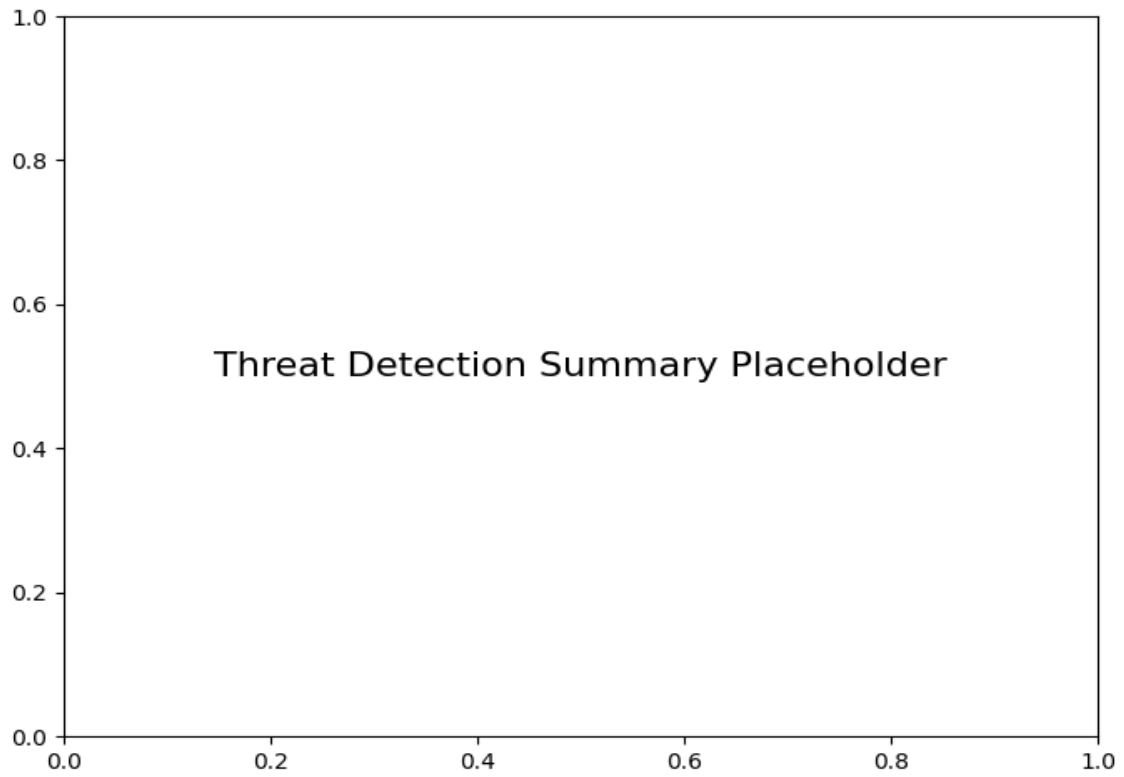
Deploy protocol anomaly detection using tools like Zeek or Suricata

### **Protocol Distribution**

Protocol Distribution



***Threat Detection Summary***



Detection Type	Count
Potential DNS tunneling detected	6