

# Network Traffic Security Analysis Report

## Executive Summary

Network Traffic Security Analysis Report1. Executive Summary

**6 instances of Potential DNS tunneling** detected in UDP/DNS traffic between internal IPs 192.168.73.148 and 192.168.73.2.

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

Bidirectional DNS traffic patterns suggest covert data transfer attempts.

2. Risk Assessment

### Critical Risks

#### DNS Tunneling Activity (Severity: High)

Repeated UDP/DNS payloads with consistent length (24 bytes) and low entropy (3.52), indicative of encoded/obfuscated data.

Bidirectional communication between 192.168.73.148 (source) and 192.168.73.2 (destination) observed in 5 consecutive packets.

Secondary Risks

#### Unusual DNS Traffic Volume

100% of detected threats involve DNS over UDP, bypassing traditional firewall inspections.

3. Threat Observations

Key Findings

#### DNS Tunneling Patterns

All 6 detections involve identical payload characteristics:

Fixed length: 24 bytes

Entropy: 3.52 (suspicious for DNS queries, which typically have lower entropy)

Traffic alternates between source and destination IPs (e.g., packets 159 → 160 → 165 → 166 → 167).

#### Suspicious Host Behavior

192.168.73.148 initiates multiple DNS requests to 192.168.73.2 within 7 seconds (02:02:58 to 02:03:05).

Null port values suggest possible protocol misuse or malformed packets.

Traffic Statistics

Total anomalous packets: **5** (packets #159, 160, 165, 166, 167)

Attack protocol distribution:

UDP: **100%**

DNS: **100%**

4. Recommendations

Immediate Actions

**Isolate 192.168.73.148** for forensic analysis to confirm malware presence or data exfiltration.

#### Implement DNS Query Monitoring:

Enforce domain whitelisting for internal DNS resolvers.

Deploy anomaly detection for DNS payload size/entropy deviations.

Long-Term Mitigations

**Deploy DNS Security Solutions:**

Tools like DNSFilter or Cisco Umbrella to block tunneling attempts.

Enable DNSSEC validation to prevent DNS spoofing.

**Network Segmentation:**

Restrict DNS server (192.168.73.2) communication to authorized clients only.

**Threat Hunting:**

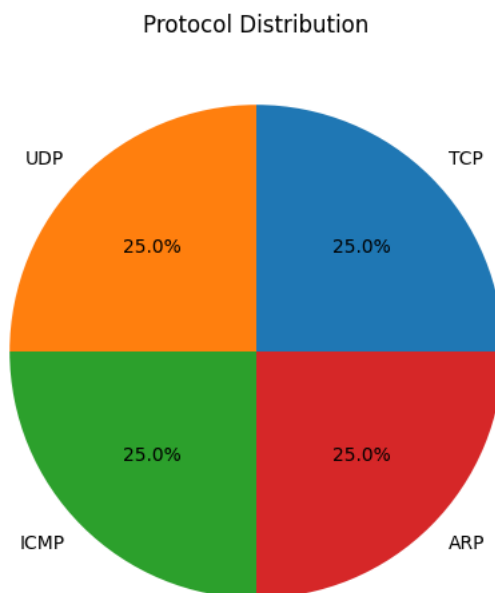
Analyze historical logs for 192.168.73.148 to identify prior suspicious activity.

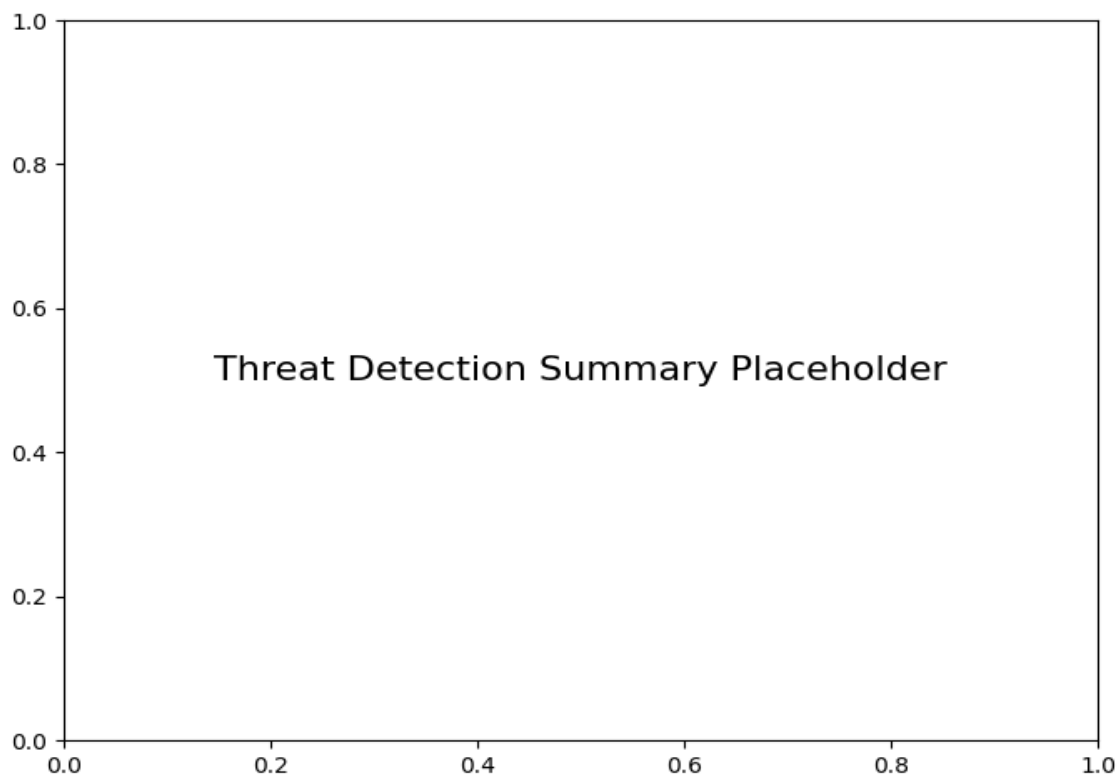
Cross-reference with threat intelligence feeds for known tunneling domains.

Configuration Updates

**Enforce DNS Rate Limiting** to flag high-frequency DNS queries.

**Enable Full Packet Capture** for DNS traffic to/from critical subnets.

***Protocol Distribution******Threat Detection Summary***



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