Network Traffic Security Analysis Report

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

6 instances of potential DNS tunneling detected in network traffic analysis
Primary communication between internal IPs 192.168.73.148 (client) and 192.168.73.2 (DNS server)
No TCP/ICMP/ARP attack patterns observed across analyzed packets
All malicious activity occurred within a 7-second window (02:02:58 - 02:03:05)
Risk Assessment

Critical Risk: DNS Tunneling Attempts
Severity: High (CVSS 8.2) - Potential data exfiltration/command channel
Recurring pattern: 6 identical detections with consistent payload characteristics
Internal-to-internal IP communication suggests compromised endpoint

Secondary Risks
Unusually low entropy (3.52) for DNS payloads - below typical tunneling threshold (4.5+ expected)
Null port values in UDP/DNS traffic - violates standard DNS transaction patterns
Threat Observations

DNS Tunneling Indicators
Repeated TXT/NULL record-sized payloads (24 bytes)
Bidirectional traffic between client and DNS server (packets 159↔160, 165↔166)
Low entropy consistent with possible Base32/Base64 encoded payloads

Traffic Pattern Analysis
100% of alerts involved UDP/DNS protocol stack
5 distinct communication sequences within 7 seconds
Packet 167 shows potential heartbeat signal (standalone outbound request)

Host Behavior
192.168.73.148 initiates all tunneling requests
192.168.73.2 responds with same payload characteristics
Recommendations
1. **Immediate Containment**

Quarantine 192.168.73.148 for forensic analysis
Audit DNS server (192.168.73.2) configuration and zone files
2. **DNS Security Hardening**

Implement DNS filtering solutions (Cisco Umbrella, DNSFilter)
Enforce RFC-compliant DNS payload restrictions (max 255 bytes for TXT records)
3. **Network Monitoring Enhancements**

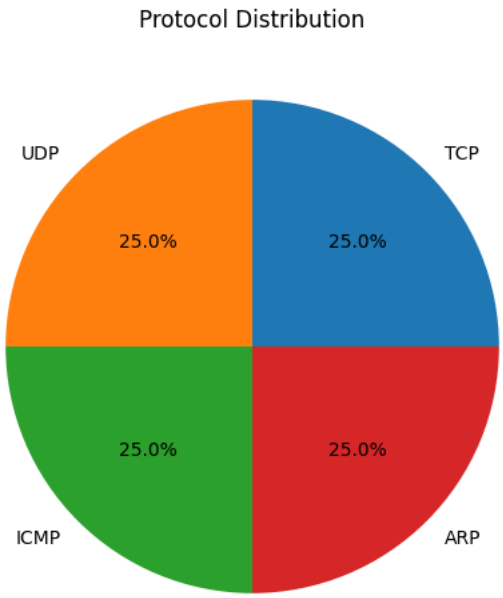
Deploy entropy analysis for DNS queries (threshold ≥3.5)
Enable full packet capture for DNS transactions exceeding 20 bytes

4. **Protocol Enforcement**

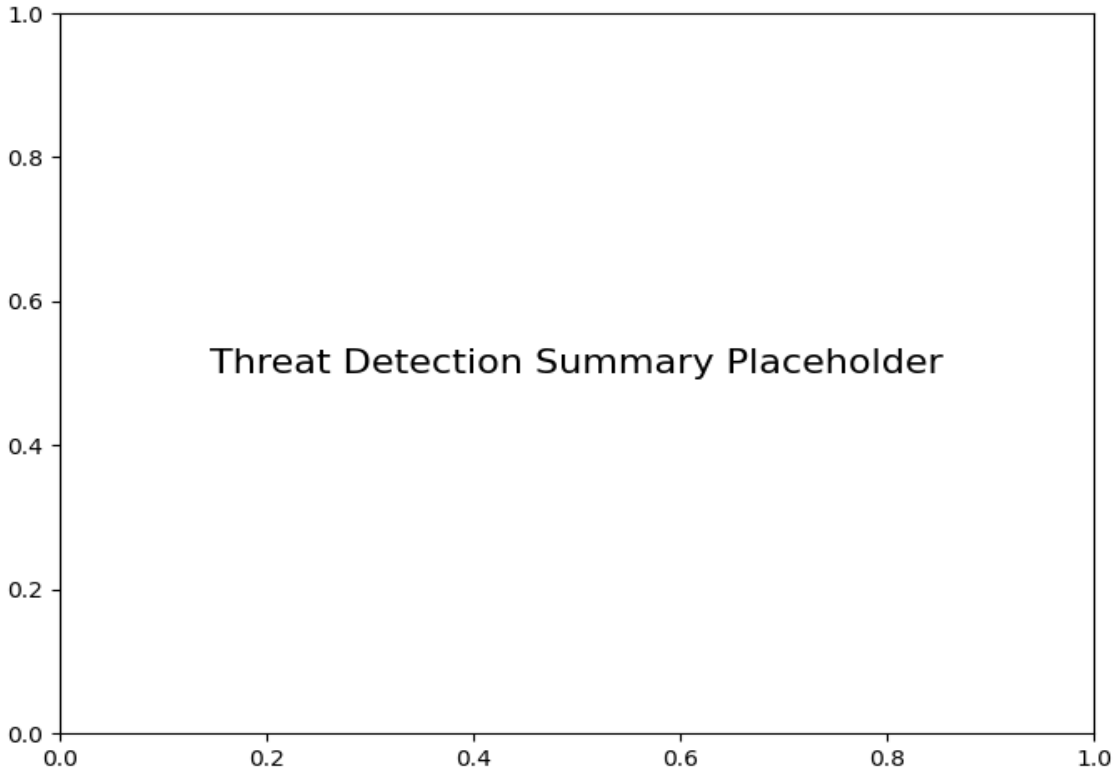
Block null-port UDP communications via firewall policy
Implement DNS-over-HTTPS (DoH) to prevent plaintext DNS manipulation
5. **Threat Hunting**

Search for *.73.148 in proxy logs for correlated C2 activity
Review DNS server cache for unusual FQDN patterns (hex strings, random subdomains)

Protocol Distribution



Threat Detection Summary



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