Network Traffic Security Analysis Report

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

6 instances of Potential DNS tunneling detected between internal IPs 192.168.73.148 and 192.168.73.2
Zero observed TCP/UDP/ICMP/ARP attack packets across analyzed traffic
Activity concentrated within a 7-second window (2009-03-26 02:02:58 to 02:03:05)
All suspicious traffic utilized UDP/DNS protocols with null port identifiers
Risk Assessment

Critical Risk: DNS tunneling attempts (**Severity: High**)
Enables covert data exfiltration/command channels
Bypasses traditional firewall controls
Observed 6 bidirectional communications between internal hosts

Elevated Risk: Internal host compromise (**Severity: Medium**)
Suspicious traffic between 192.168.73.148 (source) and 192.168.73.2 (destination)
Potential lateral movement or C2 communication
Threat Observations

DNS Tunneling Patterns:
Consistent payload characteristics: length=24, entropy=3.52
Lower-than-typical entropy values suggest possible weak obfuscation
Bidirectional traffic pattern (packets 159↔160, 165↔166, 167)

Host Communication Anomalies:
UDP source/destination ports not recorded (null values)
Repeated DNS transactions within short time intervals
Unusual internal host-to-host DNS traffic volume

Temporal Patterns:
5 clustered events within 7 seconds
Consistent millisecond-level timing between request/response pairs
Recommendations

Immediate Actions:
Quarantine hosts 192.168.73.148 and 192.168.73.2 for forensic analysis
Implement DNS query filtering for non-standard record types/lengths

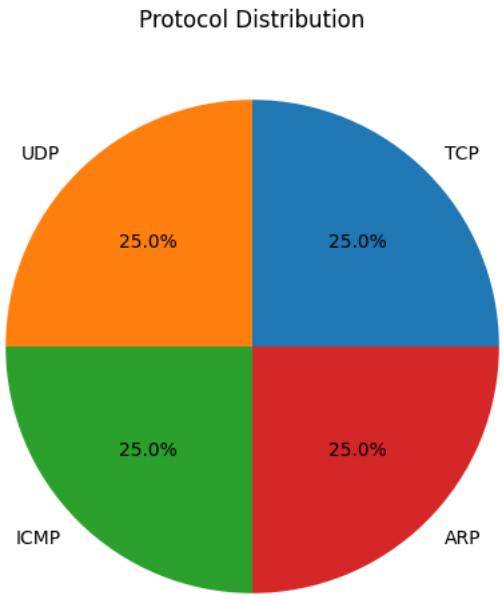
Technical Controls:
Deploy DNS monitoring solution with entropy-based detection (threshold <3.5)
Enforce port binding policies for DNS services (block null-port UDP traffic)
Configure network segmentation to limit internal DNS communication paths

Operational Improvements:
Review DNS server logs for matching transaction patterns
Conduct historical traffic analysis for previous tunneling attempts

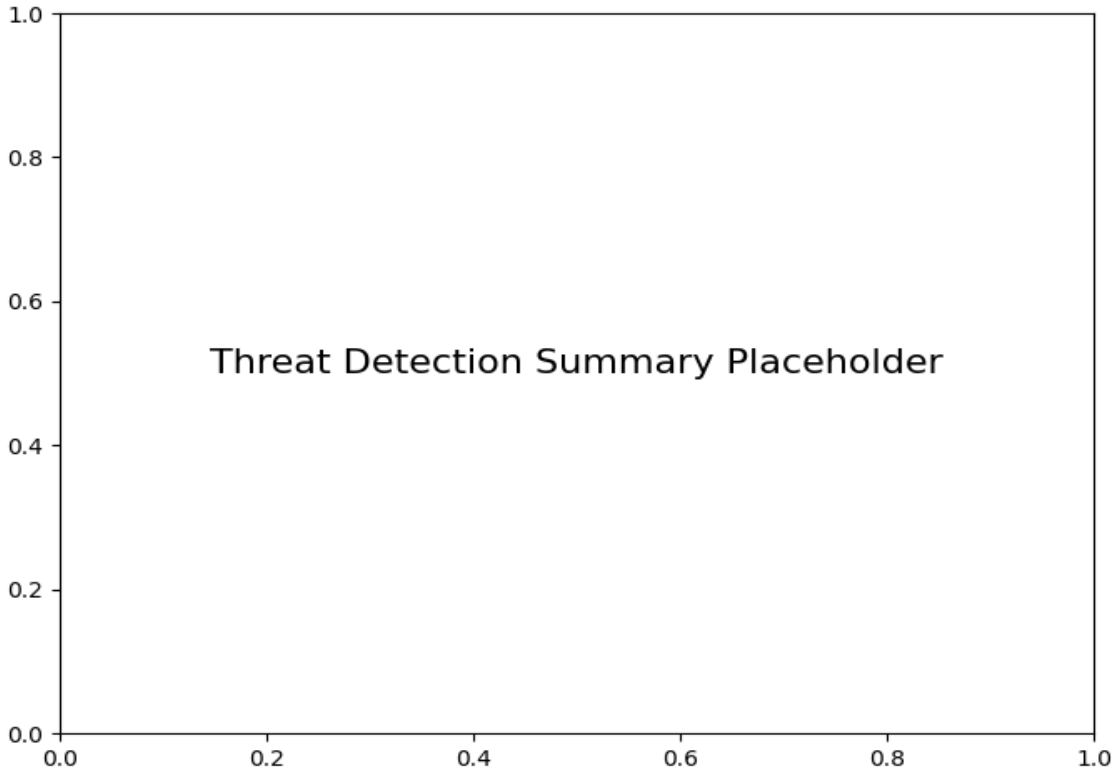
Update IDS/IPS rules to flag DNS payloads with length=24 and entropy ≥3.5

Policy Updates:
Implement strict DNS whitelisting for external resolutions
Require DNSSEC validation for all internal DNS transactions
Establish baseline for normal DNS payload characteristics per zone

Protocol Distribution



Threat Detection Summary



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