Network Security Analysis Report

AI-Powered Security Insights

Network Traffic Analysis Security Report

Executive Summary

6 instances of Potential DNS tunneling detected between internal IPs `192.168.73.148` (source) and `192.168.73.2` (destination).
All malicious activity involved **UDP/DNS protocols**, with bidirectional communication observed.
No TCP, ICMP, or ARP-based attacks detected during the analysis period.

Risk Assessment

Critical Risks
DNS Tunneling (Severity: Critical): 6 occurrences indicate potential data exfiltration or command-and-control (C2) activity.
Unusual UDP/DNS Traffic Patterns: Sustained UDP/DNS traffic between internal hosts suggests compromised systems or misconfigured services.

Operational Risks
Lack of port metadata (null src/dst ports) in threat logs limits granular analysis of DNS query patterns.

Threat Observations

DNS Tunneling Activity
Source IP `192.168.73.148` initiated 3 DNS requests, with responses from **`192.168.73.2`** (2 replies).
Traffic clustered within **6 seconds** (02:02:58 to 02:03:05), indicating rapid, automated communication.
All malicious packets lacked port identifiers, deviating from standard DNS (port 53) conventions.

Protocol Analysis
100% of detected threats used **UDP/DNS**, bypassing TCP-based security controls.
Zero malicious TCP/ICMP/ARP packets observed, suggesting attacker focus on stealthy DNS abuse.

Recommendations

Immediate Actions

Block UDP/DNS traffic between `192.168.73.148` and `192.168.73.2` at the firewall.

Isolate both hosts for forensic analysis to identify data leakage or malware.

Long-Term Mitigations

Implement DNS filtering to flag/block non-standard query lengths, unusual subdomains, or TXT record abuse.

Enable DNS logging with port visibility to correlate suspicious activity with process-level data.

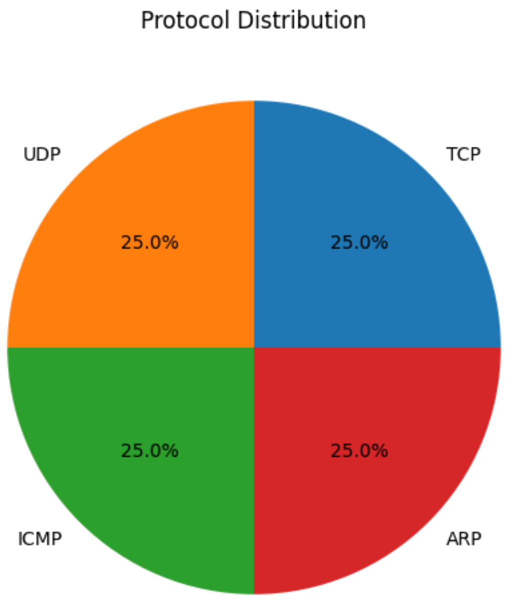
Deploy anomaly detection for UDP traffic patterns, focusing on request/response timing and volume deviations.

Configuration Updates

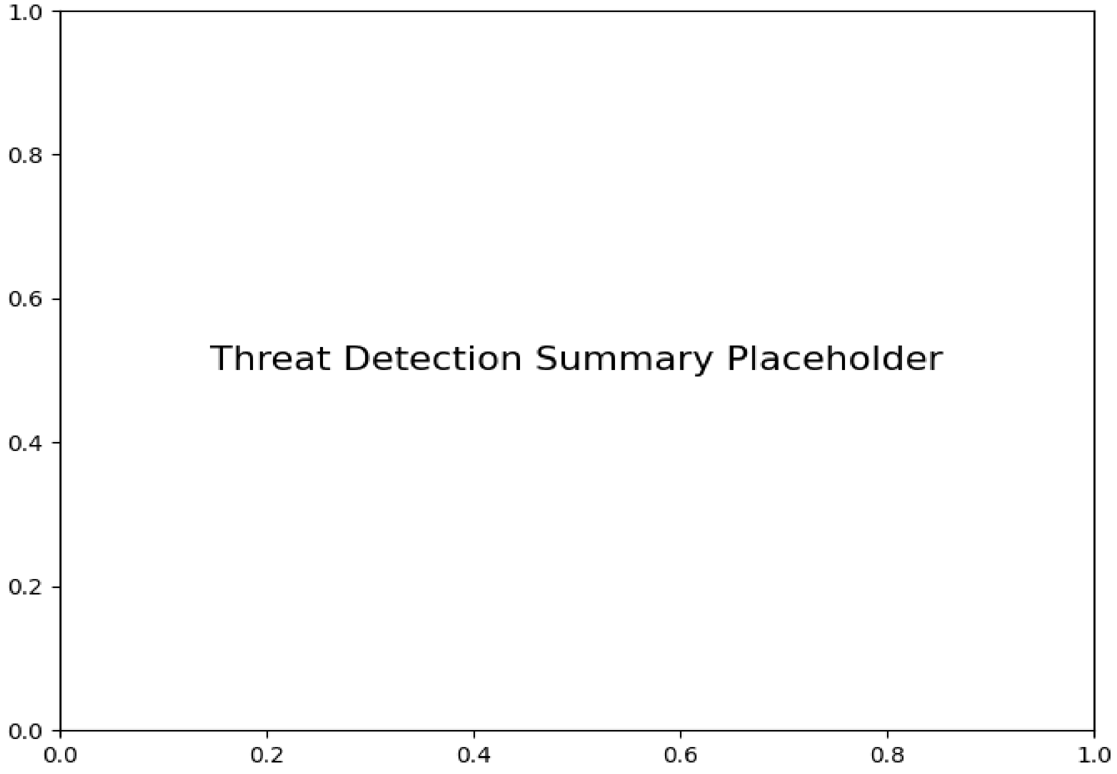
Restrict internal DNS servers from resolving external zones unless explicitly required.

Enforce DNSSEC to prevent DNS cache poisoning and tampering attacks.

Protocol Distribution



Threat Detection Summary



Detection Type	Count
Potential DNS tunneling detected	6