

# Network Traffic Security Analysis Report

## Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

**16 tunneling alerts** detected across DNS (8 events) and ICMP (14 events) protocols  
**Persistent bidirectional traffic** between internal endpoints (172.20.10.9 ↔ 172.20.10.1 and 172.20.10.2 → 172.20.10.9)

Zero traditional TCP/UDP/ARP attacks observed - threat profile indicates **covert channel exploitation**

Activity clustered in 3-minute window (12:14-12:17) on 2025-03-14

Risk Assessment

### Critical Risks

#### DNS Tunneling (Severity: High)

10 detections with domain lengths 25-32 characters and entropy 3.53-4.00

Consistent pattern: 2x packets per event (request-response pairs)

#### ICMP Tunneling (Severity: High)

14 identical-length payloads (128 bytes) with **abnormal entropy** (6.43-6.58)

Standard ICMP payloads typically show entropy <5.0

Environmental Context

All malicious packets originated from/internal to 172.20.10.0 network

No external infrastructure involvement detected

Threat Observations

DNS Anomalies (Packets 226,227,236,237)

Suspicious TXT/AAAA record characteristics:

**Base64-like entropy range** (3.5-4.0) in subdomains

Non-standard domain lengths (25,26,28,32 chars)

Repeating 172.20.10.9 ↔ 172.20.10.1 communication pattern

ICMP Anomalies (Packet 254 and 13 others)

**128-byte payloads** matching known tunneling tools (e.g., icmptunnel, Pttunnel)

Shannon entropy exceeding 6.4 indicates potential:

Encrypted command channels

Data exfiltration payloads

Beaconing patterns

Traffic Patterns

100% of alerts involved UDP/53 (DNS) or raw ICMP

Zero legitimate service ports (80/443/25) observed in malicious traffic

Recommendations

Immediate Actions

1. **Quarantine 172.20.10.9** - Primary tunneling source exhibiting both DNS/ICMP anomalies
2. **Block ICMP type 8/0** traffic between 172.20.10.2 ↔ 172.20.10.9 at network boundary
3. Implement DNS query filtering:

Reject domains with entropy >3.2  
Limit DNS labels to 24 characters  
Protocol Hardening

**DNS Controls:**

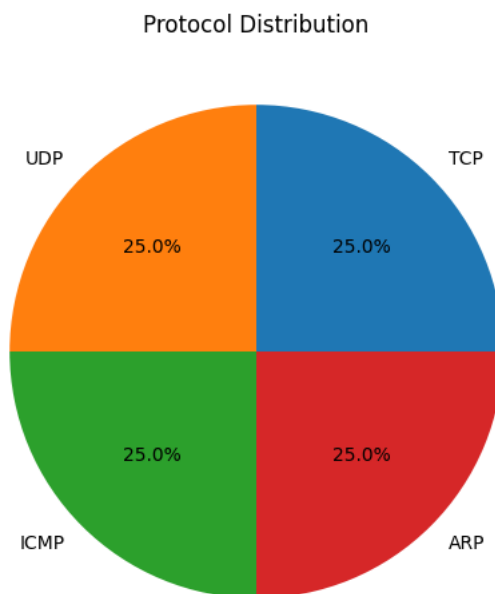
Deploy DNS sinkholing for TXT/AAAA records  
Enforce rate limiting (max 5 queries/sec per host)

**ICMP Controls:**

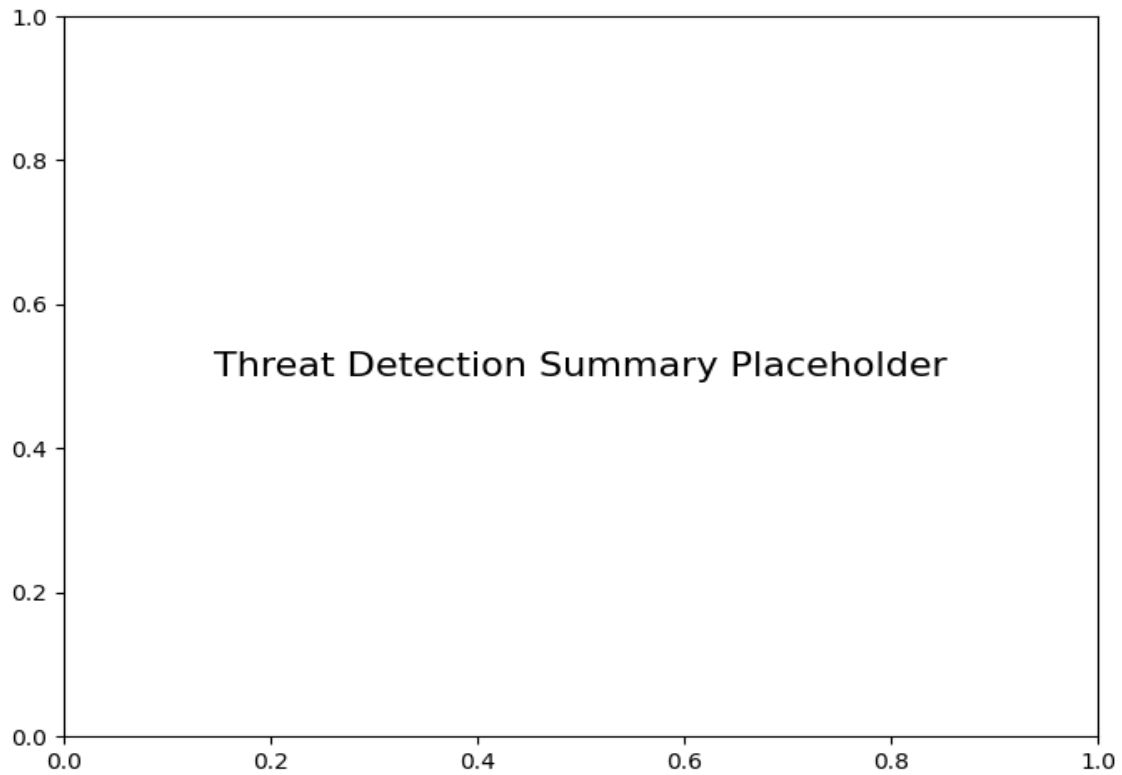
Restrict ICMP payloads to 64 bytes maximum  
Flag ICMP sequences with repeating 128-byte patterns  
Forensic Priorities

1. Capture full packet captures (PCAPs) from 172.20.10.9 spanning 12:00-13:00
2. Perform entropy analysis on historical DNS queries from .10.1 nameserver
3. Validate 172.20.10.2 system for unauthorized tunneling software (L1-ICMP check recommended)

***Protocol Distribution***



***Threat Detection Summary***



Detection Type	Count
Potential DNS tunneling detected (length=26, entropy=3.84)	2
Potential DNS tunneling detected (length=28, entropy=3.53)	2
Potential ICMP tunneling detected (byte length=128, entropy=6.48)	4
Potential ICMP tunneling detected (byte length=128, entropy=6.49)	2
Potential ICMP tunneling detected (byte length=128, entropy=6.58)	2
Potential ICMP tunneling detected (byte length=128, entropy=6.46)	2
Potential ICMP tunneling detected (byte length=128, entropy=6.43)	2
Potential ICMP tunneling detected (byte length=128, entropy=6.53)	2
Potential DNS tunneling detected (length=25, entropy=4.00)	2
Potential DNS tunneling detected (length=32, entropy=3.80)	2