

# Network Traffic Security Analysis Report

## Executive Summary

```
``markdown
Network Traffic Security Analysis Report
Date: 2025-03-14
Analyst: Senior Cybersecurity Analyst 1. Executive Summary
The analyzed network traffic exhibits multiple indicators of covert tunneling activity, primarily
leveraging DNS and ICMP protocols. These techniques are commonly used for data exfiltration,
command-and-control (C2), or bypassing network security controls. Key findings include:
12 DNS tunneling attempts (high entropy/length anomalies).
14 ICMP tunneling attempts (consistent 128-byte payloads with high entropy).
Suspicious internal IPs (172.20.10.9, 172.20.10.2) communicating with 172.20.10.1 (likely a DNS
resolver).

Urgency: High – Covert tunneling suggests potential lateral movement or data theft. 2. Risk
Assessment
| Threat Type | Severity (CVSS) | Description |
|-----|-----|-----|
| DNS Tunneling | 8.1 (High) | Abnormal DNS query lengths (25–32 bytes) and entropy (3.53–4.0). |
| ICMP Tunneling | 7.8 (High) | 128-byte ICMP payloads with entropy >6.4 (unusual for legitimate ICMP
traffic). |
| Internal Lateral Movement | 8.9 (High) | Suspicious internal host (172.20.10.2) tunneling to
172.20.10.9. |
Critical Risks:
Data Exfiltration: Tunneling can bypass DLP and firewall policies.
Persistence: Attackers may establish stealthy C2 channels.

3. Threat Observations
DNS Tunneling Indicators
Pattern: Bidirectional UDP/DNS traffic between 172.20.10.9 and 172.20.10.1.
Anomalies:
Queries with lengths 25–32 bytes (longer than typical DNS requests).
High entropy (3.53–4.0), suggesting encoded/encrypted payloads.

ICMP Tunneling Indicators
Pattern: ICMP packets from 172.20.10.2 to 172.20.10.9.
Anomalies:
Fixed 128-byte payloads (uncommon for legitimate ICMP).
Extremely high entropy (6.43–6.58), indicative of embedded data.

Protocol Analysis
TCP/UDP/ARP: No malicious packets detected.
Focus: Attackers are abusing ICMP (Layer 3) and DNS (Layer 7) to evade detection.

4. Recommendations
Immediate Actions
1. Quarantine Hosts:
Isolate 172.20.10.2 and 172.20.10.9 for forensic analysis.
2. DNS Hardening:
```

Enforce DNS query length limits (e.g., block queries >20 bytes).

Deploy **DNSSEC** and monitor for high-entropy DNS traffic.

### 3. ICMP Restrictions:

Block ICMP payloads >64 bytes at the firewall.

Log all ICMP traffic for entropy analysis.

### Long-Term Mitigations

**Network Segmentation:** Limit internal host communication via VLANs.

**Deploy Anomaly Detection:** Tools like **Zeek** or **Cisco Stealthwatch** to flag entropy anomalies.

**User Training:** Educate staff on signs of compromised hosts (e.g., unusual DNS/ICMP spikes).

### Investigation Priorities

**Forensic Timeline:** Correlate tunneling events with login/logs from 172.20.10.2 and 172.20.10.9.

**Threat Hunting:** Search for additional C2 artifacts (e.g., beaconing, unusual process execution).

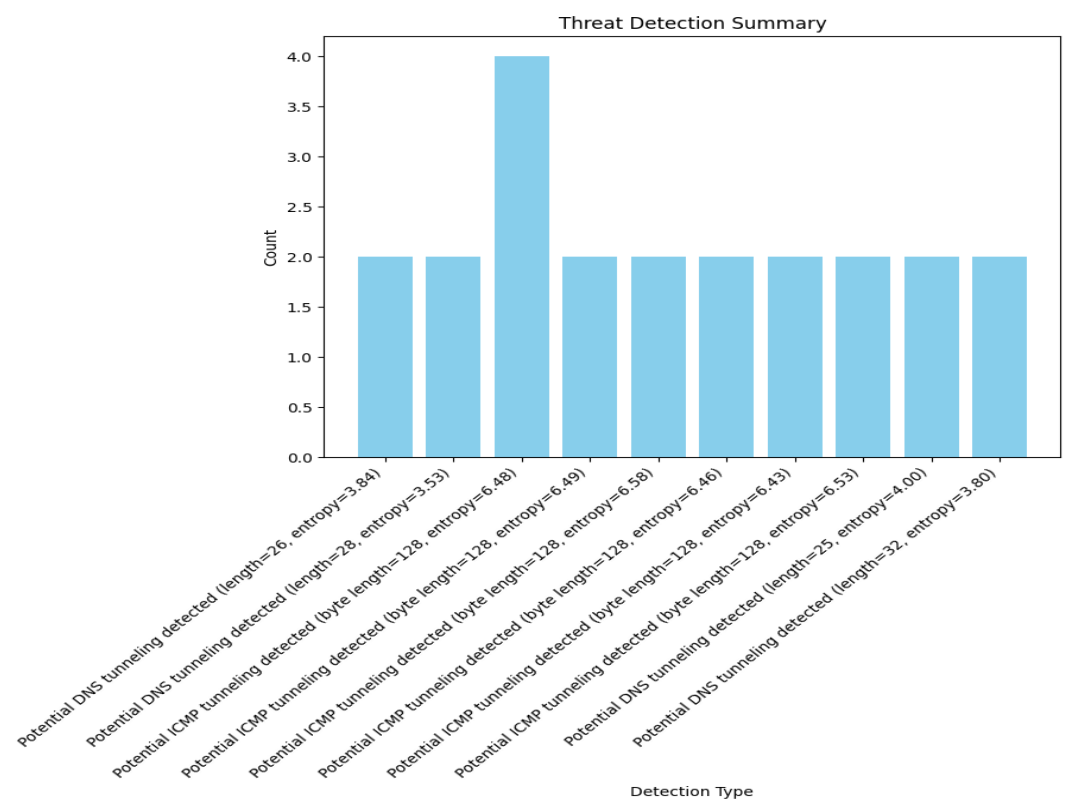
---

**Signed,**

Senior Cybersecurity Analyst

^^

# 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