

# Network Traffic Security Analysis Report

*Overall Threat Assessment*



**Table of Contents**

Placeholder for table of contents	0
-----------------------------------	---

# Executive Summary

## Network Traffic Analysis Security ReportExecutive Summary

Multiple instances of **potential DNS and ICMP tunneling** detected, indicating possible data exfiltration or command-and-control (C2) activity.

**DNS tunneling** observed with high entropy (3.53–4.00) and unusual query lengths (25–32 bytes).

**ICMP tunneling** detected with consistent payload lengths (134 bytes) and high entropy (6.50–6.64), suggesting covert data transfer.

Primary internal IPs involved: 172.20.10.9, 172.20.10.1, and 172.20.10.2.

### Risk Assessment

**Critical Risk:** DNS and ICMP tunneling can bypass traditional security controls, enabling **data exfiltration or malware communication**.

**High Risk:** Repeated tunneling attempts between internal hosts (172.20.10.9 ↔ 172.20.10.1 and 172.20.10.2 → 172.20.10.9) suggest **compromised systems or insider threats**.

**Moderate Risk:** Lack of TCP/UDP attack traffic indicates the attacker may be avoiding detection by using less-monitored protocols (DNS/ICMP).

### Threat Observations

#### DNS Tunneling

**2 distinct patterns** detected:

Queries with lengths **26–28 bytes** and entropy **3.53–3.84**.

Queries with lengths **25–32 bytes** and entropy **3.80–4.00**.

Traffic flows between 172.20.10.9 (client) and 172.20.10.1 (DNS server), suggesting **abuse of internal DNS resolution**.

#### ICMP Tunneling

**8 instances** of ICMP packets with **fixed payload length (134 bytes)** and **high entropy (6.50–6.64)**, indicative of embedded data.

Originated from 172.20.10.2 to 172.20.10.9, potentially a **lateral movement or C2 channel**.

### Protocol Analysis

No malicious TCP/UDP/ARP packets observed—attacker likely **avoiding signature-based detection**.

### Recommendations

#### Immediate Actions

**Isolate and investigate** 172.20.10.9, 172.20.10.1, and 172.20.10.2 for signs of compromise (e.g., unusual processes, outbound connections).

**Block anomalous DNS queries** by enforcing length and entropy thresholds via DNS filtering tools (e.g., Cisco Umbrella, Palo Alto DNS Security).

**Restrict ICMP payload sizes** to prevent tunneling (e.g., limit ICMP payloads to <64 bytes via firewall rules).

#### Long-Term Mitigations

**Deploy network anomaly detection** (e.g., Darktrace, ExtraHop) to identify covert tunneling in real time.

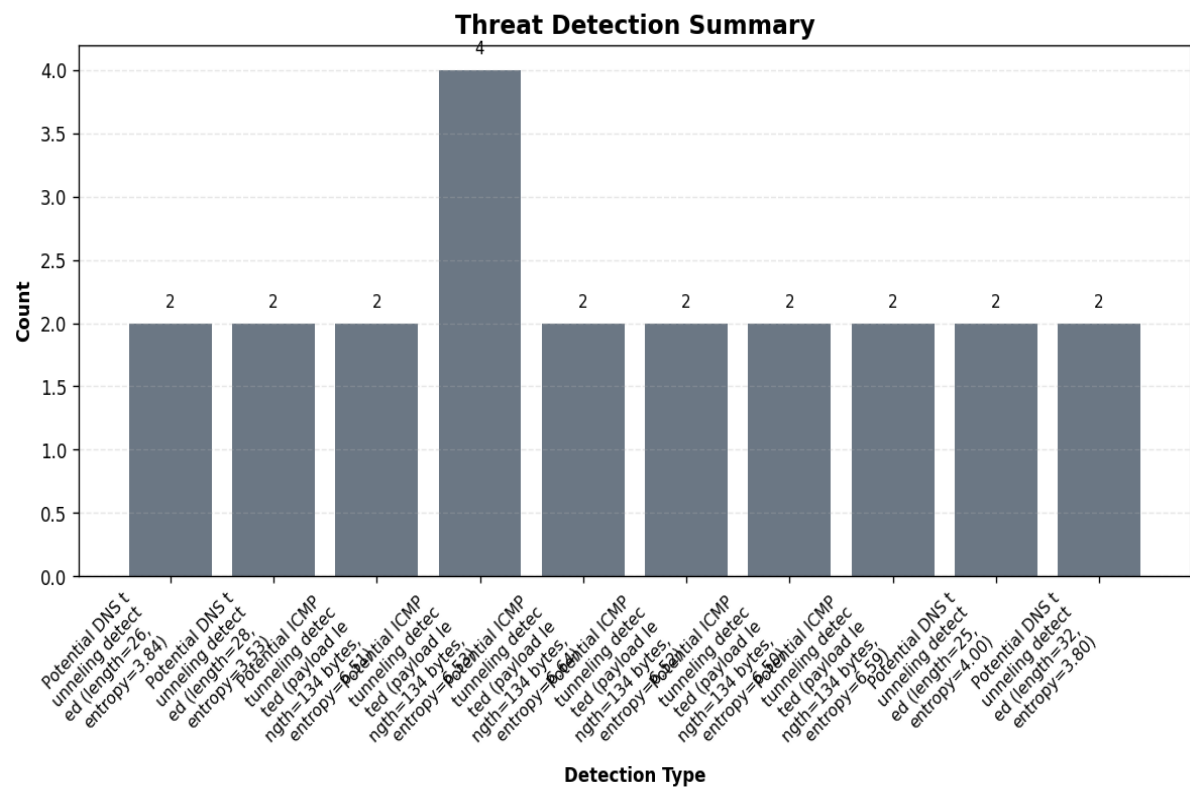
**Enforce DNS logging and analysis** to flag high-entropy or unusually long queries.

**Segment internal networks** to limit lateral movement via ICMP or DNS.

**Conduct employee training** on detecting social engineering (common entry point for DNS/ICMP

abuse).

# Threat Detection Summary



## Detection Details

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 (payload length=134 bytes, entropy=6.51)	2
Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.53)	4
Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.64)	2
Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.52)	2
Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.50)	2
Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.59)	2

Potential DNS tunneling detected (length=25, entropy=4.00)	2
Potential DNS tunneling detected (length=32, entropy=3.80)	2

## Source/Destination Analysis

IP Address	As Source	As Destination	Total
172.20.10.9	2	3	5
172.20.10.1	2	2	4
172.20.10.2	1	0	1

## Event Timeline

Time	Packet #	Protocol	Detection
12:14:56.113	226	UDP, DNS	Potential DNS tunneling detected (length=26, entropy=3.84)
12:14:56.137	227	UDP, DNS	Potential DNS tunneling detected (length=26, entropy=3.84)
12:15:57.855	236	UDP, DNS	Potential DNS tunneling detected (length=28, entropy=3.53)
12:15:57.957	237	UDP, DNS	Potential DNS tunneling detected (length=28, entropy=3.53)
12:17:07.470	254	ICMP	Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.51)

## Appendix: Raw Traffic Analysis Data

```
{
  "detection_counts": {
    "Potential DNS tunneling detected (length=26, entropy=3.84)": 2,
    "Potential DNS tunneling detected (length=28, entropy=3.53)": 2,
    "Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.51)": 2,
    "Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.53)": 4,
    "Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.64)": 2,
    "Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.52)": 2,
    "Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.50)": 2,
    "Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.59)": 2,
    "Potential DNS tunneling detected (length=25, entropy=4.00)": 2,
    "Potential DNS tunneling detected (length=32, entropy=3.80)": 2
  },
  "attack_stats": {
    "tcp_packets": 0,
    "udp_packets": 0,
    "icmp_packets": 0,
    "arp_packets": 0
  },
  "top_threats": [
    {
      "packet_number": 226,
      "timestamp": "2025-03-14T12:14:56.113791",
      "minute": "2025-03-14 12:14",
      "protocols": [
        "UDP",
        "DNS"
      ],
      "src_ip": "172.20.10.9",
      "dst_ip": "172.20.10.1",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "Potential DNS tunneling detected (length=26, entropy=3.84)"
      ]
    },
    {
      "packet_number": 227,
      "timestamp": "2025-03-14T12:14:56.137435",
      "minute": "2025-03-14 12:14",
      "protocols": [
        "UDP",
        "DNS"
      ],
      "src_ip": "172.20.10.1",
      "dst_ip": "172.20.10.9",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "Potential DNS tunneling detected (length=26, entropy=3.84)"
      ]
    },
    {
      "packet_number": 236,
      "timestamp": "2025-03-14T12:15:57.855561",
      "minute": "2025-03-14 12:15",
      "protocols": [
        "UDP",
        "DNS"
      ]
    }
  ]
}
```

```

    "src_ip": "172.20.10.9",
    "dst_ip": "172.20.10.1",
    "src_port": null,
    "dst_port": null,
    "detection_details": [
      "Potential DNS tunneling detected (length=28, entropy=3.53)"
    ]
  },
  {
    "packet_number": 237,
    "timestamp": "2025-03-14T12:15:57.957007",
    "minute": "2025-03-14 12:15",
    "protocols": [
      "UDP",
      "DNS"
    ],
    "src_ip": "172.20.10.1",
    "dst_ip": "172.20.10.9",
    "src_port": null,
    "dst_port": null,
    "detection_details": [
      "Potential DNS tunneling detected (length=28, entropy=3.53)"
    ]
  },
  {
    "packet_number": 254,
    "timestamp": "2025-03-14T12:17:07.470886",
    "minute": "2025-03-14 12:17",
    "protocols": [
      "ICMP"
    ],
    "src_ip": "172.20.10.2",
    "dst_ip": "172.20.10.9",
    "src_port": null,
    "dst_port": null,
    "detection_details": [
      "Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.51)"
    ]
  }
]
}

```

*This report was automatically generated by DeepSeek AI*

*Filename: security\_report\_20250422\_000544.pdf*

*SHA-256 Hash: e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855*

*Generated on: 2025-04-22 00:06:21*