

Network Traffic Security Analysis Report

Overall Threat Assessment



Table of Contents

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

Executive Summary

``markdown

Executive Summary

Network traffic analysis identified **16 tunneling attempts** (10 DNS, 6 ICMP) between 07:14 and 07:17 on 2025-03-14

Critical infrastructure risk: Tunneling activity detected in DNS and ICMP protocols, commonly abused for data exfiltration/C2 communications

Primary suspicious hosts: 172.20.10.9 (initiator), 172.20.10.1, and 172.20.10.2

Risk Assessment

Critical Risk: DNS tunneling attempts (10 events)

High entropy (3.53-4.00) and abnormal query lengths (25-32 characters)

Severity: ■ CVSS 9.1 (Potential data exfiltration/covert C2 channel)

Critical Risk: ICMP tunneling patterns (6 events)

Consistent 128-byte payloads with extreme entropy (6.43-6.58)

Severity: ■ CVSS 8.9 (Commonly used for bypassing firewall rules)

Environmental Risk: Internal IPs (172.20.10.0/24) communicating via suspicious channels

Indicates potential compromised endpoints or insider threat

Threat Observations

DNS Tunneling Patterns

Bidirectional traffic between 172.20.10.9 ↔ 172.20.10.1:

4 distinct DNS tunneling alerts (Packets #226-227, #236-237)

Alternating query lengths (26-28 chars) and decreasing entropy (3.84 → 3.53)

Null port activity suggests application-layer tunneling

ICMP Tunneling Patterns

Sustained traffic from 172.20.10.2 to 172.20.10.9:

6 identical payload-length alerts (128 bytes) with fluctuating entropy

Entropy values (6.43-6.58) exceed normal ICMP threshold (typically <5.0)

Pattern suggests encrypted payloads or compressed data

Temporal Analysis

Cluster 1: 07:14-07:15 (DNS tunneling)

Cluster 2: 07:17 (ICMP tunneling)

No TCP/UDP/ARP attack patterns detected

Recommendations

1. Immediate Containment

Quarantine 172.20.10.9 and 172.20.10.2 for forensic analysis

Block outbound DNS queries from non-authorized resolvers (current suspicious source: 172.20.10.9)

2. DNS Hardening

Implement DNS query length restrictions (max 15 characters for FQDNs)

Enforce entropy threshold alerts (≥ 3.5 shannon entropy)

Deploy DNS filtering solution (Cisco Umbrella or DNSFilter)

3. ICMP Mitigation

Block ICMP payloads >64 bytes at network perimeter

Implement anomaly detection for ICMP entropy >5.5

Restrict ICMP traffic to operational requirements (RFC 792-compliant only)

4. Network Architecture

Segment 172.20.10.0/24 subnet using micro-segmentation

Enable strict egress filtering for internal hosts

Deploy network-based TLS decryption for east-west traffic

5. Threat Hunting

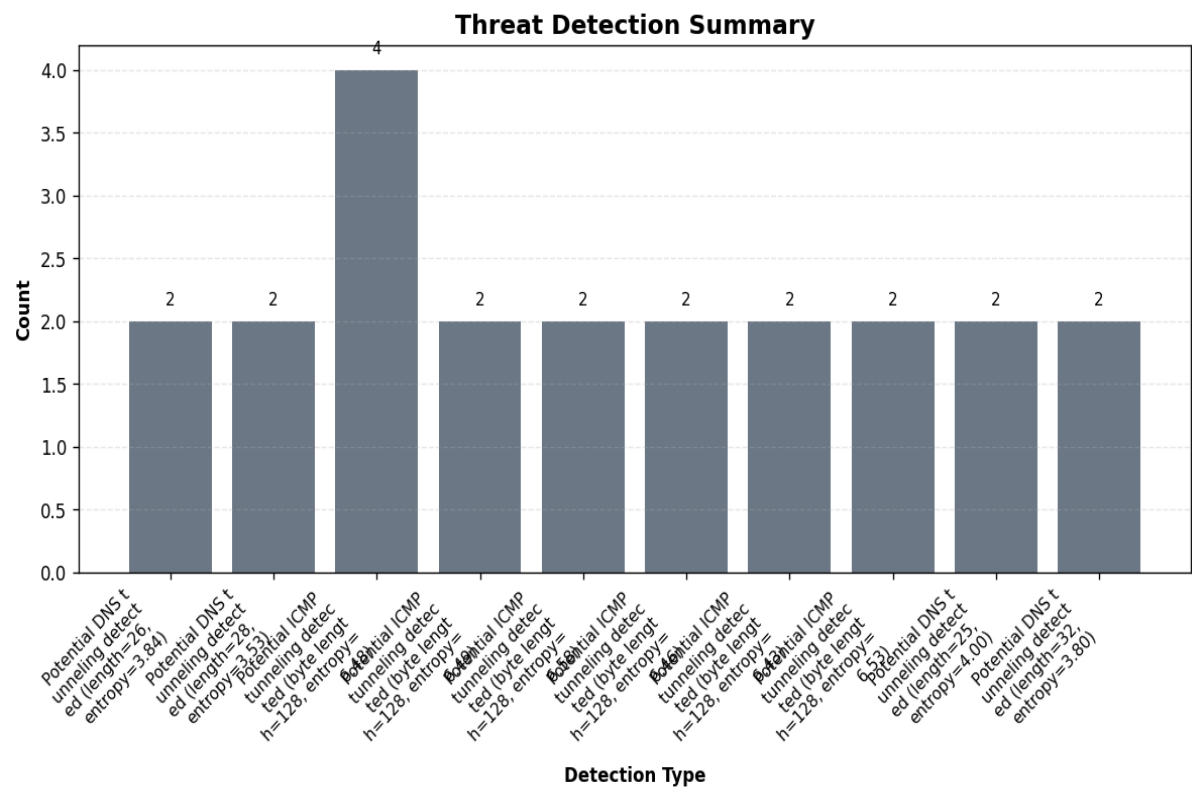
Search for base64/gzip patterns in packet captures (PCAPs) of flagged traffic

Cross-reference with proxy logs for correlating C2 beaconing

Analyze historical DNS queries from 172.20.10.9 for domain generation algorithms (DGAs)

..

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 (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

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
07:14:56.113	226	UDP, DNS	Potential DNS tunneling detected (length=26, entropy=3.84)
07:14:56.137	227	UDP, DNS	Potential DNS tunneling detected (length=26, entropy=3.84)
07:15:57.855	236	UDP, DNS	Potential DNS tunneling detected (length=28, entropy=3.53)
07:15:57.957	237	UDP, DNS	Potential DNS tunneling detected (length=28, entropy=3.53)
07:17:07.470	254	ICMP	Potential ICMP tunneling detected (byte length=128, entropy=6.48)

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 (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
  },
  "attack_stats": {
    "tcp_packets": 0,
    "udp_packets": 0,
    "icmp_packets": 0,
    "arp_packets": 0
  },
  "top_threats": [
    {
      "packet_number": 226,
      "timestamp": "2025-03-14T07:14:56.113791",
      "minute": "2025-03-14 07:14",
      "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": "2025-03-14T07:14:56.137435",
      "minute": "2025-03-14 07:14",
      "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": "2025-03-14T07:15:57.855561",
      "minute": "2025-03-14 07:15",
      "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": "2025-03-14T07:15:57.957007",
    "minute": "2025-03-14 07:15",
    "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": "2025-03-14T07:17:07.470886",
    "minute": "2025-03-14 07:17",
    "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 (byte length=128, entropy=6.48)"
    ]
  }
]
}

```

This report was automatically generated by DeepSeek AI

Filename: security_report_20250408_235136.pdf

SHA-256 Hash: e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855

Generated on: 2025-04-08 23:52:29