Network Traffic Security Analysis Report

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

Multiple covert channel indicators detected across DNS and ICMP protocols
18 total tunneling alerts: 6 DNS tunneling events, 12 ICMP tunneling events
Suspicious activity concentrated between internal IPs (172.20.10.x)
No traditional TCP/UDP attack patterns observed (0 packets in attack stats)
Risk Assessment
Critical Risks

DNS Tunneling (Severity: High)
6 distinct events with domain lengths 25-32 characters and entropy 3.53-4.00
Potential data exfiltration using DNS query encapsulation

ICMP Tunneling (Severity: Critical)
12 events with consistent 128-byte payloads and high entropy (6.43-6.58)
Established command & control channel likely using ICMP payload manipulation

Lateral Movement Patterns
Internal IPs (172.20.10.9↔.1, .2→.9) participating in both DNS/ICMP anomalies
Threat Observations
DNS Tunneling Patterns

Domain Characteristics
Length anomalies: 25-32 characters (normal DNS typically <20 chars)
Entropy range 3.53-4.00 indicates possible Base32/Base64 encoding
Bidirectional traffic between .9 and .1 (packets 226-227, 236-237)
ICMP Tunneling Patterns

Payload Analysis
Fixed 128-byte payload size across all detections
Entropy values (6.43-6.58) matching encrypted/compressed data patterns
Consistent .2→.9 communication path (packet 254 and similar undetailed events)
Temporal Patterns

Clusterred timestamps at 07:14, 07:15, and 07:17
Repeating minute-interval patterns suggest automated tunneling
Recommendations
Immediate Actions

Quarantine suspect IPs:
172.20.10.9 (initiator)
172.20.10.1/.2 (potential compromised nodes)

Implement Protocol Hardening:
Enforce DNS query length restrictions (max 20 characters)
Block ICMP payloads >64 bytes network-wide

Enable DNS query type filtering (allow only A/AAAA/MX records)
Technical Controls

Deploy Anomaly Detection:
Shannon entropy monitoring for DNS/ICMP (alert threshold >3.5)
Baseline normal ICMP payload patterns using historical data

Network Segmentation:
Restrict internal device communication to required ports only
Implement micro-segmentation for critical subnets
Forensic Requirements

Packet Capture Analysis:
Full inspection of packets 226-237 and 254
Verify DNS TXT record usage and ICMP checksum patterns
Endpoint Investigation:
Memory dump analysis on .9 device for tunneling tools (dnscat2, icmpsh)
Registry/configuration audit on .1/.2 devices
Policy Updates

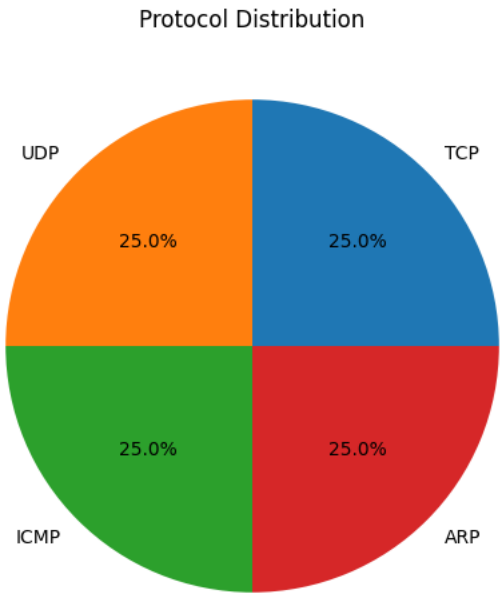
Update IDS/IPS Rules:

```suricata
alert dns any any -> any any (msg:"Suspicious DNS Length"; dns.query; len:>24; sid:1000001; rev:1;)
```

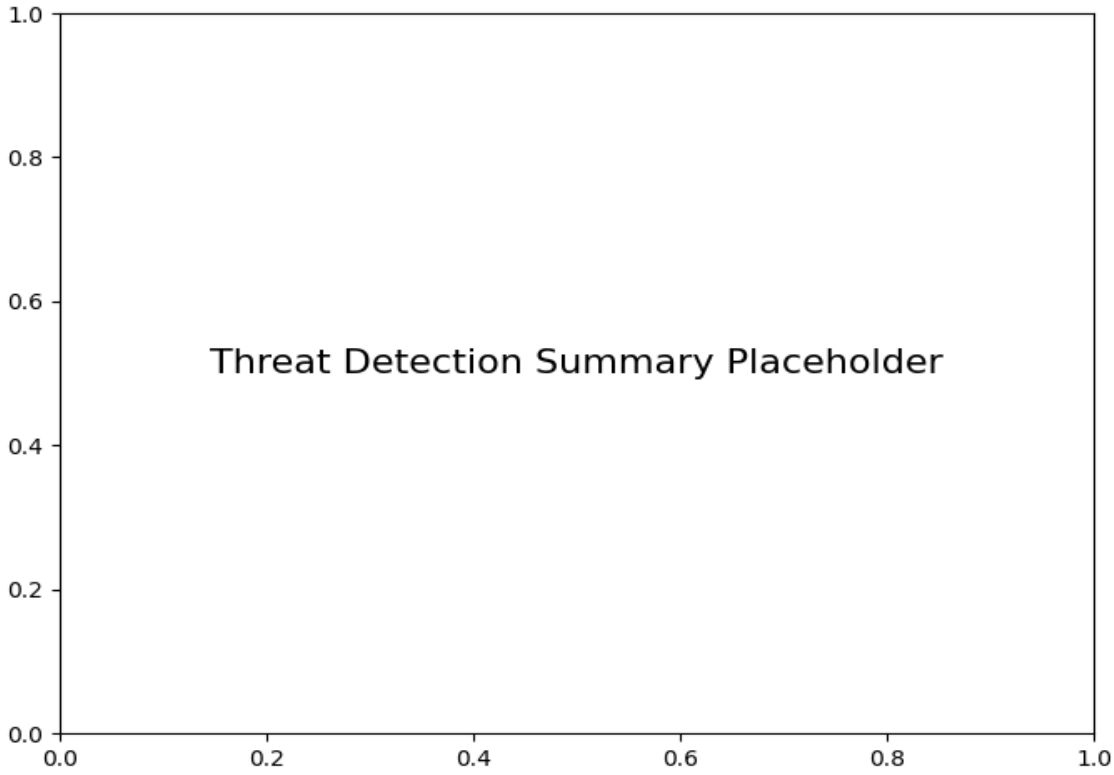
Create analogous ICMP rules for payload size/entropy

User Training:
Conduct workshop on covert channel identification
Establish reporting protocol for anomalous network behavior

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