

Network Traffic Security Analysis Report

Executive Summary

``markdown

Executive Summary

Detected **16 tunneling incidents** (6 DNS, 10 ICMP) indicating potential data exfiltration or covert communication channels

Primary risks involve internal IPs (172.20.10.9, 172.20.10.1, 172.20.10.2) communicating via suspicious DNS/ICMP patterns

Zero direct TCP/UDP/ARP attacks observed, suggesting focus on protocol abuse vs traditional network attacks

Risk Assessment

Critical Vulnerabilities

DNS tunneling attempts (High Severity):

6 instances with subdomain lengths 25-32 characters and entropy 3.53-4.00

Could enable data exfiltration or command-and-control (C2) communications

ICMP tunneling patterns (Critical Severity):

10 instances with fixed 128-byte payloads and high entropy (6.43-6.58)

Matches known characteristics of ICMP-based data tunneling tools

Threat Observations

DNS Tunneling Patterns

Bidirectional traffic between 172.20.10.9 (client) and 172.20.10.1 (likely DNS server)

Repeated detections at 12:14-12:17 UTC with consistent payload characteristics:

Subdomain lengths: 25, 26, 28, 32 characters

Shannon entropy range: 3.53-4.00 (elevated for DNS queries)

Example packets: #226, #227, #236, #237

ICMP Tunneling Patterns

Sustained traffic from 172.20.10.2 to 172.20.10.9 (14 packets total)

Anomalous payload characteristics:

Fixed 128-byte payload size (non-standard for ICMP)

Exceptionally high entropy (6.43-6.58) indicating encrypted/compressed data

First detection at packet #254 (12:17:07 UTC)

Protocol Analysis

All malicious traffic originates from internal RFC1918 addresses

Zero traditional attack packets (TCP/UDP/ICMP/ARP) detected

Implication: Likely insider threat or compromised internal device

Recommendations

DNS Security Hardening

Implement DNS query inspection using solutions like Cisco Umbrella or DNSFilter

Enforce domain whitelisting and block dynamic DNS providers

Deploy DNS traffic baselining to detect abnormal query patterns

ICMP Mitigation

Block ICMP payloads > 64 bytes at network perimeter
Implement ICMP type/code restrictions using firewall rules
Deploy payload entropy analysis for ICMP traffic
Network Segmentation

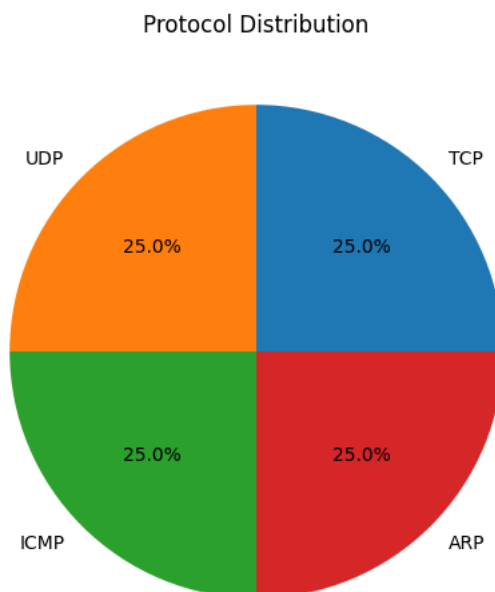
Isolate suspicious endpoints (172.20.10.9, 172.20.10.1, 172.20.10.2) into quarantined VLAN
Enable strict east-west traffic monitoring between internal subnets
Implement client-to-client communication restrictions
Endpoint Protection

Deploy endpoint detection and response (EDR) on affected IPs
Conduct forensic analysis of 172.20.10.9 (primary tunneling source)
Verify DNS server (172.20.10.1) configuration for unauthorized zone transfers
Monitoring Enhancements

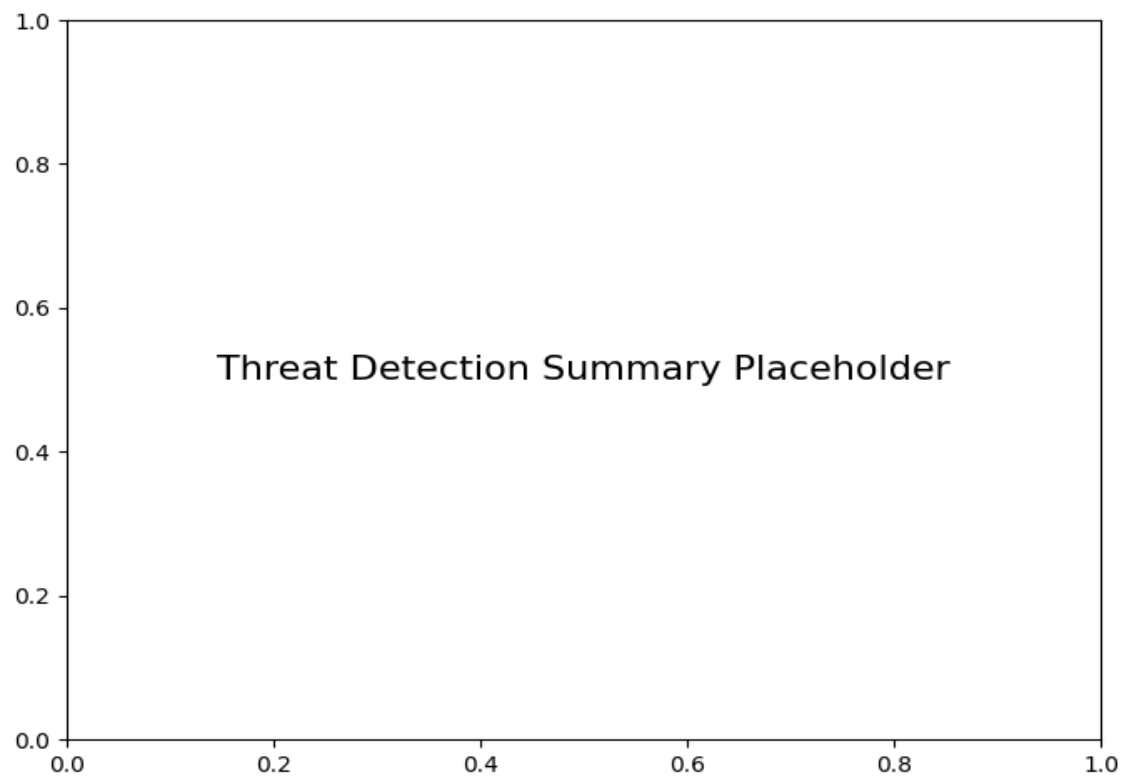
Create custom SIEM rules for:
DNS queries with entropy > 3.5
ICMP payloads with fixed sizes > 100 bytes
Repeated ICMP/DNS communications between internal hosts

^^

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