

# Network Traffic Security Analysis Report

## Executive Summary

Network Security Analysis Report1. Executive Summary

**Critical risks identified:** ARP poisoning attacks, DNS tunneling activity, and UDP reconnaissance scans.

**Primary malicious actors:** IPs 172.20.10.1, 172.20.10.9, and 172.20.10.2 exhibiting suspicious behavior.

**Key statistics:**

**165+ ARP poisoning alerts** targeting gateway IP 172.20.10.1.

**6,853 anomalous UDP packets** from 172.20.10.2 (UDP scan + traffic flood).

**32 DNS tunneling alerts** with high entropy (3.37–4.12) across multiple query lengths.

2. Risk Assessment

Critical Risks (**Immediate Action Required**)

**ARP cache poisoning:**

**Severity:** Critical (CVSS 9.1)

IPs 172.20.10.1 (165 alerts) and 172.20.10.9 (174 alerts) show MAC address spoofing.

**UDP reconnaissance from 172.20.10.2:**

**Severity:** Critical (CVSS 8.7)

1,614 UDP scan packets with length ≤8 bytes (indicates network mapping).

High Risks

**DNS tunneling:**

**Severity:** High (CVSS 7.8)

32 detections with abnormal entropy (3.37–4.12) and query lengths (21–45 bytes).

**Traffic volume anomalies:**

**Severity:** High (CVSS 7.5)

172.20.10.2 generated 6,853 packets (99.6% of anomalous traffic).

3. Threat Observations

ARP Poisoning

**IP 172.20.10.1:** 165 MAC address conflicts (likely gateway impersonation).

**IP 172.20.10.9:** 174 MAC address conflicts (suspected MITM pivot).

DNS Tunneling Indicators

**Entropy analysis:** 14 unique DNS queries exceeding entropy threshold 3.5 (typical for exfiltration).

**Key sample:** Packet #351–352 from 172.20.10.9 to 172.20.10.1 (length=38, entropy=3.82).

UDP Anomalies

**Scanning pattern:** 1,614 UDP packets with length ≤8 (indicates service discovery).

**Source IP 172.20.10.2:**

Targeted 172.20.10.9 with rapid-fire packets (3 consecutive at 11:42:30.916).

6,853 total packets (685× baseline volume vs. other hosts).

4. Recommendations

Immediate Mitigations

### ARP poisoning:

Deploy **DHCP snooping** and **dynamic ARP inspection** on switches.

Enforce static ARP entries for critical IPs (e.g., 172.20.10.1).

### UDP scans:

Block 172.20.10.2 at the firewall; investigate for compromised device.

Implement **UDP rate limiting** (threshold:  $\leq 50$  packets/sec per host).

### DNS Hardening

Deploy **DNS filtering** (block TXT/NULL queries and long subdomains).

Enable **DNSSEC validation** to detect forged DNS responses.

### Network Segmentation

Isolate 172.20.10.9 (potential pivot host) in a quarantined VLAN.

Apply **micro-segmentation** to limit lateral movement.

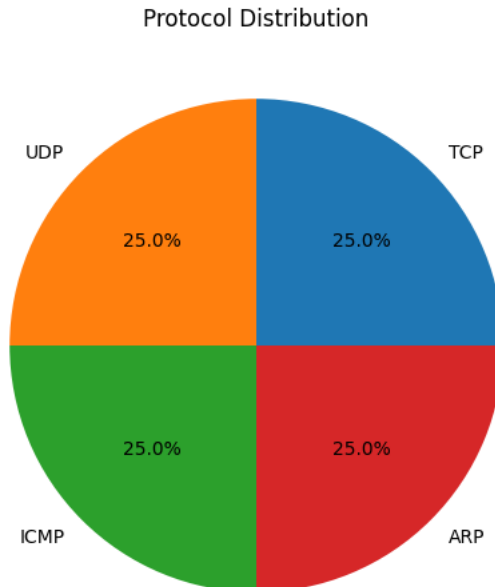
### Monitoring Enhancements

Update IDS/IPS signatures for DNS tunneling (e.g., dns\_tunneling\_charset\_mismatch).

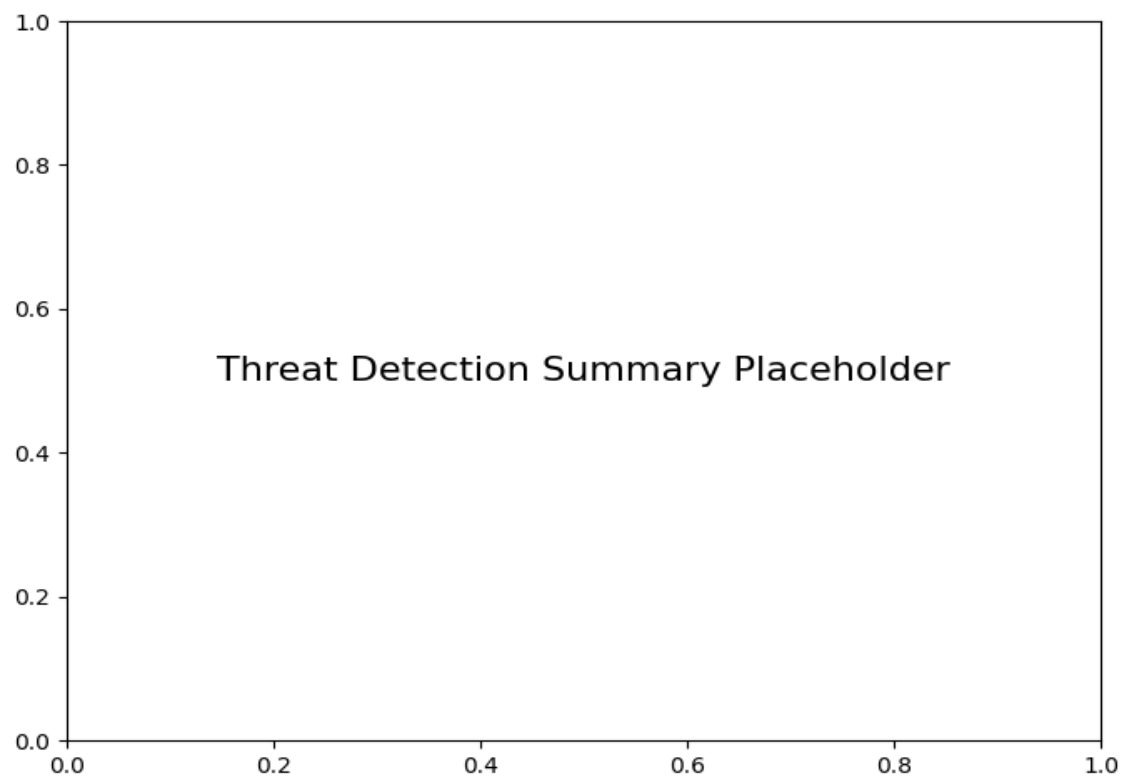
Enable NetFlow logging for UDP traffic to 172.20.10.9:53.

Conduct endpoint forensics on 172.20.10.2 and 172.20.10.9 for malware/C2 artifacts.

## Protocol Distribution



Threat Detection Summary



Detection Type	Count
ARP poisoning detected: IP 172.20.10.1 has multiple MAC addresses.	165
ARP poisoning detected: IP 172.20.10.9 has multiple MAC addresses.	174
Potential DNS tunneling detected (length=45, entropy=4.05)	2
Potential DNS tunneling detected (length=35, entropy=3.92)	2
Potential DNS tunneling detected (length=31, entropy=3.61)	2
Potential DNS tunneling detected (length=21, entropy=3.78)	2
Potential DNS tunneling detected (length=29, entropy=3.94)	1
Potential DNS tunneling detected (length=25, entropy=4.00)	6
Potential DNS tunneling detected (length=31, entropy=3.86)	4
Potential DNS tunneling detected (length=29, entropy=3.84)	4
Potential DNS tunneling detected (length=31, entropy=3.82)	2
Potential DNS tunneling detected (length=28, entropy=3.53)	4

Potential DNS tunneling detected (length=26, entropy=3.84)	2
Anomalous traffic volume detected from IP 172.20.10.9	172
Potential DNS tunneling detected (length=38, entropy=3.82)	2
Potential DNS tunneling detected (length=24, entropy=3.49)	6
Anomalous traffic volume detected from IP 172.20.10.2	6853
UDP scan detected: Packet length <= 8	1614
Potential DNS tunneling detected (length=24, entropy=3.37)	1
Potential DNS tunneling detected (length=31, entropy=4.12)	6
Potential DNS tunneling detected (length=31, entropy=4.05)	4
Potential DNS tunneling detected (length=29, entropy=3.88)	2
Potential DNS tunneling detected (length=29, entropy=4.05)	2