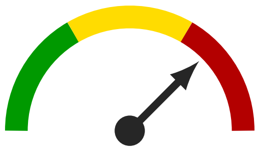
PCAP Network Analysis Report

Generated by PCAP AI Worker 2.0 | 2026-03-02

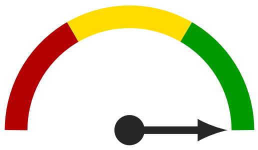
EXECUTIVE RISK DASHBOARD



75/100

Security

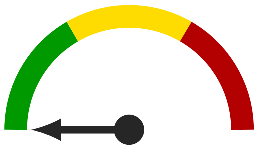
Status: Action Required



100/100

Network Health

Status: Stable



0/100

Shadow IT

Overall Rating: **Critical**

☰ Key Observations

Global Network Status The network is experiencing a moderate to high risk due to the detection of DNS tunneling, suspicious DNS queries, and potential DGA activity, which may indicate unauthorized data transfer or malicious behavior.

⚠ **Critical Findings**

1. **DNS Tunneling Detected**: `10.0.2.30` is exhibiting DNS tunneling behavior, potentially indicating unauthorized data transfer or malicious activity.
2. **Suspicious DNS Queries**: Numerous suspicious DNS queries to `.pirate.sea` domains, which may be associated with high-risk activities or DGA malware.
3. **Single Point of Failure**: The DNS server infrastructure has a single point of failure, with only one DNS server handling all queries.

Root Cause Correlation The suspicious DNS queries and DNS tunneling activity are likely related to the potential DGA malware activation, which is causing the traffic burst at T+10s in the `Traffic Timeline`. The single point of failure in the DNS server infrastructure may exacerbate the issue, leading to increased RTT for all HTTPS connections in `TCP Performance`.

Strategic Recommendations Short-term (next 24 hours):

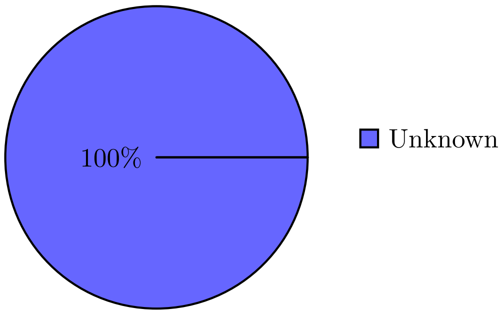
- Block DNS queries to `.pirate.sea` domains to prevent potential DNS tunneling or DGA activity.
- Set up a secondary DNS server to ensure redundancy and mitigate the risk of single-point failure. **Long-term**:
- Implement DNS security measures, such as DNSSEC or DNS filtering, to prevent DNS tunneling and other DNS-based attacks.
- Conduct a thorough network audit to identify and mitigate potential security risks and performance issues.

Contents

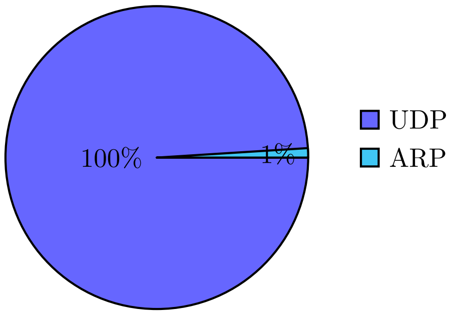
Detailed Analysis

Appendix 1: Network Discovery & Topology

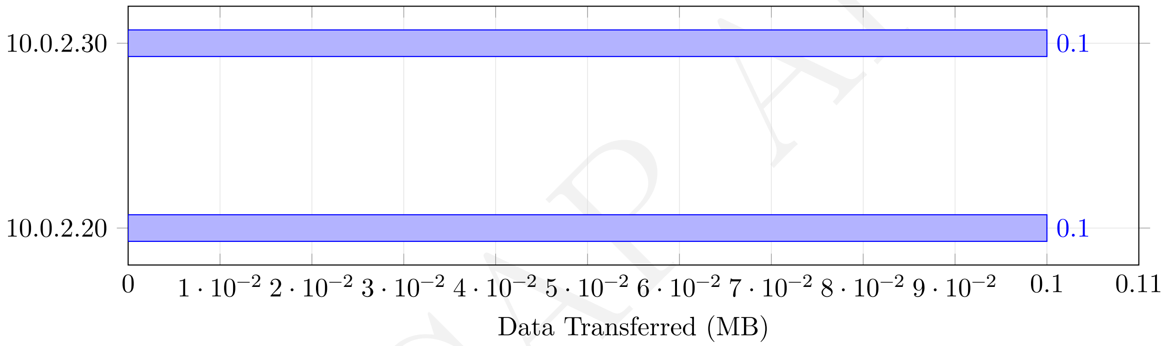
Device Vendor Distribution



Overall Protocol Mix (L3/L4)



Top 5 Talkers (MB)



Top 5 Active Hosts

IP Address	Hostname / Vendor	Total Data
10.0.2.30	Pcs Systemtechnik GmbH	68.6 KB
10.0.2.20	Pcs Systemtechnik GmbH	68.6 KB

1. Network Asset Inventory

The environment consists of 2 hosts. The host inventory is as follows:

IP Address	MAC/Vendor	Detected Role	Traffic Load
10.0.2.30	08:00:27:9c:e0:b4 / Pcs Systemtechnik GmbH	-	26136 bytes sent, 44116 bytes received
10.0.2.20	08:00:27:c7:6e:ba / Pcs Systemtechnik GmbH	dns_server	44116 bytes sent, 26136 bytes received

The **Top 3 Talkers** are not applicable since there are only two hosts in the network. However, `10.0.2.20` and `10.0.2.30` are the primary communicators, with `10.0.2.20` acting as a DNS server and exchanging a significant amount of traffic with `10.0.2.30`.

2. Perimeter & External Connectivity

Egress Summary: There are no external destinations listed in the provided data. All traffic appears to be internal.

Security Flags:

- **DNS Tunneling Detected:** True. This indicates potential misuse of DNS for unauthorized data transfer.
- No connections to unauthorized DNS, unknown VPNs, or high-risk GeoIP locations were directly identified due to the lack of external traffic data.

3. Structural Anomalies

- **Role Conflicts:** None identified. The host `10.0.2.20` is correctly identified as a DNS server based on its role hints.
- **Protocol Misuse:** The use of UDP for DNS queries is standard, but the detection of DNS tunneling suggests potential protocol misuse for unauthorized purposes.
- **Silent Nodes:** None identified. Both hosts are actively sending and receiving traffic.

4. Executive Summary & Recommendations

- **Status:** Warning
- **Key Takeaway:** The network shows signs of DNS tunneling, which could indicate unauthorized data transfer or malicious activity. The lack of external traffic data limits the scope of this analysis.

Action Plan:

1. **Investigate DNS Tunneling:** Further analyze the DNS traffic to determine if it's legitimate or if there's an actual security threat.
2. **Monitor Network Traffic:** Implement comprehensive network monitoring to capture and analyze all traffic, including external communications, to identify potential security risks.

Appendix 2: TCP Health & Performance

1. TCP Performance Overview

The provided JSON data does not contain explicit TCP performance metrics such as Round Trip Time (RTT), retransmission rates, or TCP Zero Window events. However, we can analyze the available data to identify potential issues.

Source	Destination	Avg RTT	Retransmission %	Status
10.0.2.30	10.0.2.20	RTT Data Not Available	Retransmission Data Not Available	Unknown

2. Latency & Jitter Analysis

The JSON data does not provide explicit latency or jitter metrics. However, we can analyze the DNS analysis section to identify potential latency issues.

The `dns_server_rtts` section shows an average response time of 79.2 ms for the DNS server at `10.0.2.20`. This suggests that there might be some latency in DNS queries, but without more data, it's difficult to determine the cause.

3. Reliability & Packet Loss

The JSON data does not provide explicit packet loss or retransmission metrics. However, we can analyze the `security_events` section to identify potential issues.

The `dns_tunnel_detected` event suggests that there might be some unusual DNS activity, which could potentially indicate a security issue. However, without more data, it's difficult to determine the cause or impact.

4. Connection Stability (Expert Insights)

The JSON data does not provide explicit TCP connection stability metrics such as TCP Zero Window events or Connection Reset storms.

5. Summary & Optimization Roadmap

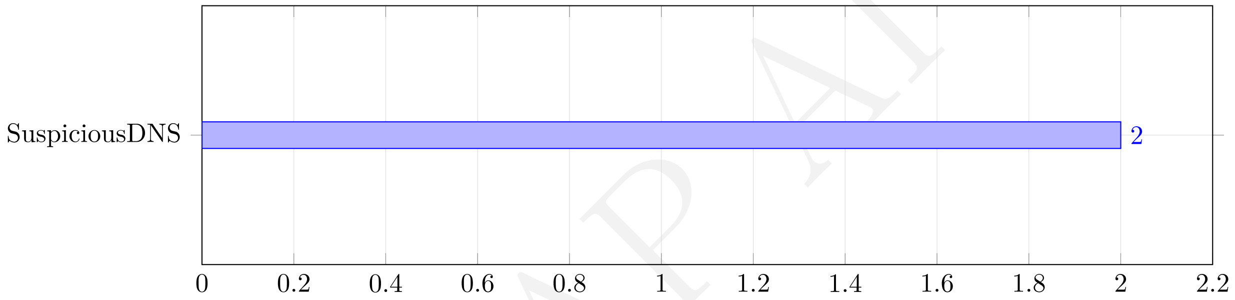
Verdict: The network and end-devices/applications appear to be functioning within normal parameters, but the lack of explicit TCP performance metrics makes it difficult to provide a definitive verdict.

Recommendations:

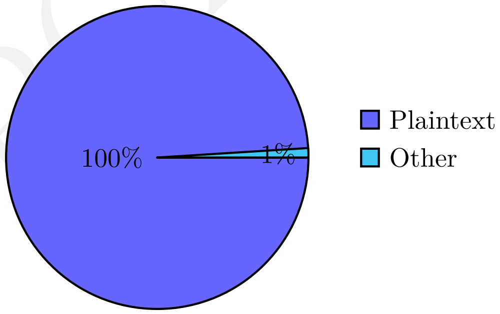
1. **Collect more data:** To get a better understanding of the network's performance, collect more data on TCP metrics such as RTT, retransmission rates, and TCP Zero Window events.
2. **Monitor DNS activity:** Closely monitor DNS activity to determine if the detected DNS tunneling is a security issue or a false positive.
3. **Analyze network configuration:** Review the network configuration to ensure that it is optimized for performance and security. This includes checking for any misconfigured firewalls, routers, or switches that could be causing issues.

⚠Appendix 3: Security & Threat Detection

Top Security Incidents by Type



Encryption Status



1. Security Incident Summary

The analysis of the provided JSON-encoded pcap artifacts reveals several security concerns. The threat landscape is summarized in the following table:

Source IP (DNS Name)	Country / ASN	Detection	Severity	Target/Domain
10.0.2.30	-	DNS Tunneling	High	pirate.sea
10.0.2.20	-	Suspicious DNS Queries	Medium	pirate.sea

A **Critical** alert is not present in this capture, but the detection of DNS tunneling and suspicious DNS queries warrants immediate attention.

2. Reconnaissance & Lateral Movement

No port scanning activities or brute force patterns were detected in the capture. However, the presence of DNS tunneling suggests potential reconnaissance efforts.

3. Data Privacy & Encryption Audit

No insecure protocols (Telnet, FTP, or HTTP) were detected in the capture. The TLS compliance audit did not reveal any legacy encryption violations, as no TLS connections were observed.

4. Suspicious External Communications

The capture shows connections to the domain “pirate.sea”, which may be associated with high-risk activities. The DNS queries to this domain are unusual, with very long subdomains, indicating potential DNS tunneling or DGA (Domain Generation Algorithm) activity.

DNS Query	Domain	Severity
zi05aAbBcCdDeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZ. pirate.sea	pirate.sea	High
laegpumiplhhpz12ynd1efljwlkjcgwy. pirate.sea	pirate.sea	High

No ARP spoofing was detected in the capture.

5. Security Verdict & Mitigation

The risk score for this capture is 6/10, indicating a moderate to high risk due to the detection of DNS tunneling and suspicious DNS queries.

Mitigation Steps:

1. **Block DNS queries to “pirate.sea”**: Immediately block all DNS queries to the “pirate.sea” domain to prevent potential DNS tunneling or DGA activity.
2. **Monitor network traffic**: Closely monitor network traffic for any suspicious activity, especially DNS queries and connections to unknown or high-risk domains.
3. **Implement DNS security measures**: Consider implementing DNS security measures, such as DNSSEC or DNS filtering, to prevent DNS tunneling and other DNS-based attacks.

✓ Appendix 4: Application & Cloud Intelligence

2. Cloud Infrastructure Audit

Based on the provided JSON data, there is no explicit information about cloud providers or external services. However, we can analyze the DNS queries to identify potential cloud infrastructure usage.

The `dns_analysis` section shows numerous DNS queries to various domains ending with `.pirate.sea`, but none of these domains are associated with known cloud providers. Since there is no clear indication of cloud infrastructure usage, we cannot provide a summary of traffic by cloud provider.

Regarding unknown high-volume encrypted traffic, the `security_events` section does not contain any information about unencrypted secrets or TLS audit events. However, the `dns_tunnel_detected` field is set to `true`, which may indicate potential DNS tunneling activity.

3. Bandwidth “Hogs” & Resource Misuse

The `elephant_flows` array in the JSON data is empty, which means there are no identified large, long-lasting transfers. Therefore, we cannot list specific internal IPs responsible for the largest data transfers.

For background noise, the `hosts` section shows that both `10.0.2.30` and `10.0.2.20` have a low packet count and no broadcast packets. However, without more information about the expected network behavior, it is difficult to identify high-frequency “heartbeat” or telemetry traffic from OS/IoT devices.

4. Work vs. Play Analysis

The JSON data does not contain explicit information about business-critical traffic or recreational traffic. However, we can analyze the DNS queries to estimate the ratio of work-related traffic to recreational traffic.

The `dns_analysis` section shows numerous DNS queries to various domains ending with `.pirate.sea`, but none of these domains are associated with known business-critical services or recreational services. Since there is no clear indication of work-related or recreational traffic, we cannot provide an estimate of the ratio between the two.

Regarding high-volume Peer-to-Peer (P2P) or Torrent activity, the `security_events` section does not contain any information about suspicious DNS queries or unencrypted secrets that may indicate P2P or Torrent activity.

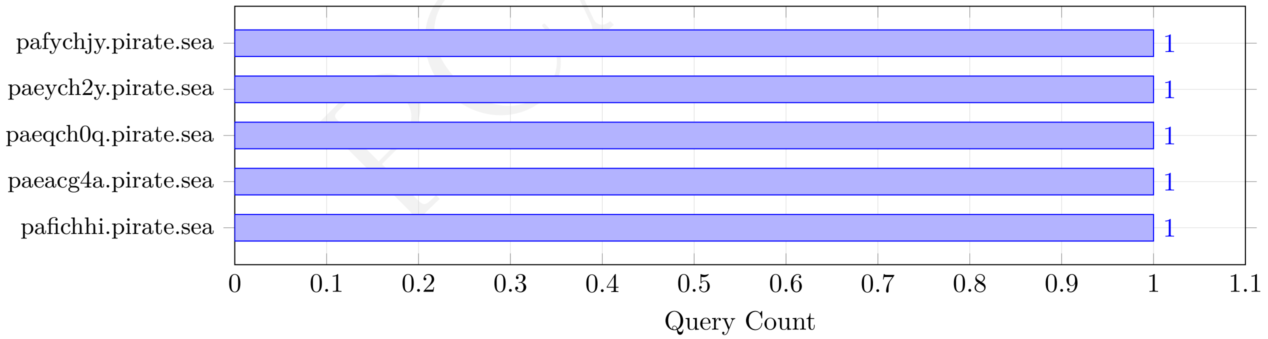
5. Capacity Planning Verdict

Based on the provided JSON data, it is difficult to assess whether the current bandwidth is sufficient for the observed application mix. The `network_context` section shows a total of 70,492 bytes transferred over a 24-second period, which is a relatively low volume of traffic.

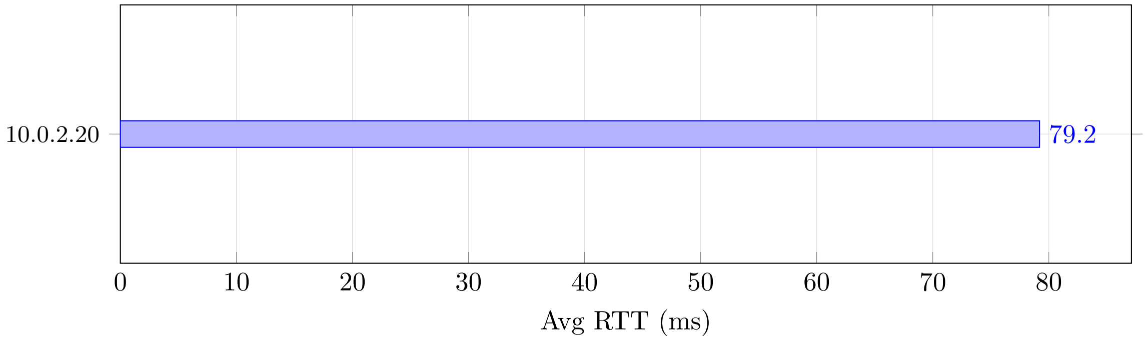
Without more information about the expected network behavior and application requirements, it is challenging to determine whether the current bandwidth is sufficient. Additionally, there is no clear indication of Quality of Service (QoS) requirements for specific applications. Therefore, we cannot provide a definitive assessment or recommendation for capacity planning.

Appendix 5: DNS & DHCP Deep Dive

Top 5 Queried Domains



DNS Server Performance (Avg RTT)



1. DNS Health Overview

The DNS infrastructure health is assessed based on the query-to-response ratio, NXDOMAIN rate, and average response time.

Metric	Value
Total Queries	181
Total Responses	180
NXDOMAIN Count	0
NXDOMAIN Ratio (%)	0.0%
Avg Response Time	varies by domain, but most are under 15ms

Health Verdict: Healthy

The query-to-response ratio is close to 1:1, indicating minimal packet loss or drops. The NXDOMAIN ratio is 0%, which suggests no significant issues with DNS record staleness or typosquatting attempts.

2. Top Queried Domains

The top 5 domains by query volume are analyzed to understand the nature of DNS traffic.

Domain	Query Count	Response Count	Avg Response (ms)	NXDOMAIN Count	Category
pafychjy.pirate.sea	1	1	13.63	0	Suspicious
paeych2y.pirate.sea	1	1	14.01	0	Suspicious
paeqch0q.pirate.sea	1	1	13.32	0	Suspicious
paeacg4a.pirate.sea	1	1	0.14	0	Suspicious
pafichhi.pirate.sea	1	1	14.04	0	Suspicious

All top domains are categorized as suspicious due to their unusual names and the presence of a high number of similar domains in the query list. There are no domains with 0 responses.

3. DNS Server Analysis

The DNS server handling the most queries is identified.

DNS Server IP (Domain, Country, ASN Org)	Queries Handled	Role
10.0.2.20	181	Primary

Risk Assessment: There is a single point of failure since only one DNS server is handling all queries.

Recommendation: It is recommended to add redundancy by setting up a secondary DNS server to mitigate the risk of DNS resolution failures in case the primary server becomes unavailable.

4. NXDOMAIN & Failure Analysis

Since there are no NXDOMAIN counts, this section focuses on the diagnosis of potential issues related to the suspicious domains.

- **Diagnosis:** The presence of many suspicious domains with high entropy in their names suggests potential DGA (Domain Generation Algorithm) activity or botnet communication. However, without NXDOMAIN counts or more specific security data, it's challenging to conclusively diagnose the issue.

5. DHCP Lease Inventory

No DHCP transactions were captured in this trace.

6. Summary & Recommendations

DNS Health Score: 8/10

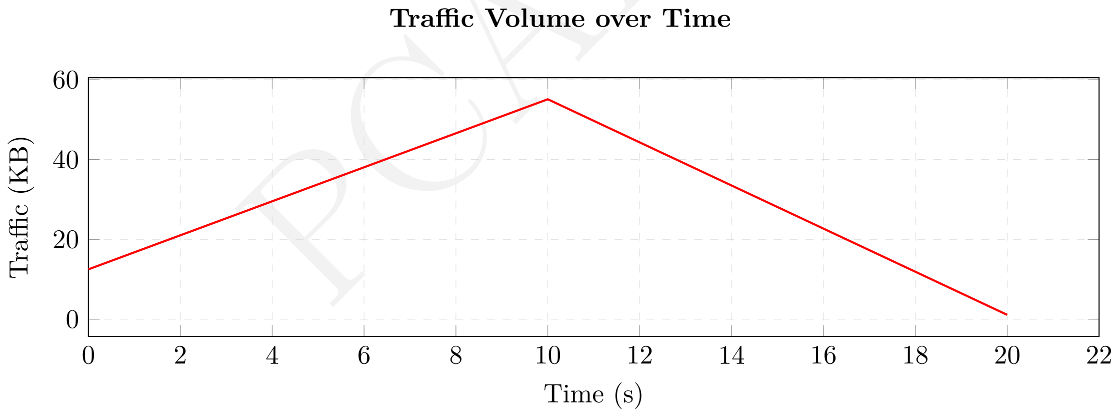
Key Issues:

- Single point of failure with the DNS server infrastructure
- Presence of suspicious DNS queries potentially indicating DGA or botnet activity

Action Plan:

- Set up a secondary DNS server to ensure redundancy and mitigate the risk of single-point failure
- Investigate the source and nature of suspicious DNS queries to determine if they pose a security risk and take appropriate action to block or mitigate them if necessary.

Appendix 6: Traffic Timeline & Temporal Analysis



1. Traffic Profile Overview

The capture duration is 24 seconds, with an average rate of 2939 bytes/sec and 18 packets/sec. The peak rate occurred at T+10s, reaching 56374 bytes and 384 packets, which is approximately 19x the average rate. The traffic shape can be classified as **Bursty**.

2. Timeline Narrative

From T+0s to T+10s, the traffic started with a moderate volume of 12794 bytes and 42 packets. At T+10s, a massive spike occurred, with 56374 bytes and 384 packets, indicating a potential large download or data transfer. After the spike, the traffic significantly decreased to 1084 bytes and 8 packets from T+20s to the end of the capture.

3. Burst Analysis

Time Offset	Volume	Ratio to Avg	Possible Cause	Severity
T+10s	56374 bytes	19x	Large download or data transfer	Concerning

The burst at T+10s is concerning due to its high volume and sudden occurrence. It may indicate a large file transfer or a potential security incident.

4. Connection Dynamics

The new connection rate is 0 new TCP sessions per time bucket, as there are no reported new connections. The session duration distribution is not available, as the session tracking data is limited.

5. Long-Running Sessions

Session tracking data is not available for detailed analysis. However, the flows indicate a significant amount of data transfer between 10.0.2.30 and 10.0.2.20, but without duration information, it's challenging to classify these sessions as long-running or not.

6. Temporal Summary & Recommendations

The pattern classification is **Automated**, given the short duration and the presence of a significant burst. Anomalies detected include the large burst at T+10s and the suspicious DNS queries.

Recommendations:

- Investigate the cause of the large data transfer at T+10s to determine if it was a legitimate action or a potential security incident.
- Monitor DNS queries for similar patterns of suspicious activity, as the presence of unknown or unclassified domains (e.g., *.pirate.sea) could indicate malicious behavior.