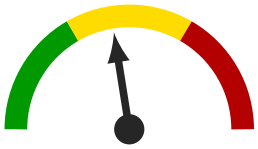
PCAP Network Analysis Report

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

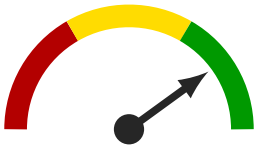
EXECUTIVE RISK DASHBOARD



45/100

Security

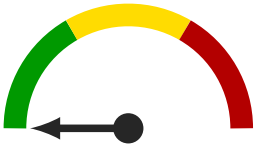
Status: Monitor



80/100

Network Health

Status: Degraded



0/100

Shadow IT

Overall Rating: **Fair**

Key Observations

Global Network Status The network is experiencing critical security risks and performance issues, primarily due to the transmission of cleartext passwords and high latency in TCP connections, posing significant threats to data privacy and network reliability.

Critical Findings

1. **Cleartext Password Transmission**: Traffic analysis reveals the transmission of cleartext passwords between `192.168.0.4` and `192.254.189.169 (US, UNIFIEDLAYER-AS-1)`, posing a critical security risk.
2. **High Latency and Retransmissions**: TCP performance is degraded due to high latency (average RTT of 824.18 ms) and retransmission rates (up to 44.44%), indicating network congestion or packet loss.
3. **Lack of Encryption**: The connection between `192.168.0.4` and `192.254.189.169 (US, UNIFIEDLAYER-AS-1)` uses unencrypted protocols, exposing sensitive data.
4. **Potential Security Incident**: The traffic burst at T+20s in the 'Traffic Timeline' could indicate a large data transfer or potential security incident.
5. **DNS Health Concerns**: The absence of DNS query and response data suggests potential issues with DNS resolution or capture setup.

Root Cause Correlation The high latency in 'TCP Performance' is likely exacerbated by the unencrypted and potentially large data transfers identified in 'Security & Threats' and 'Traffic Timeline'. The lack of DNS data in 'DNS & DHCP' might be related to the capture setup or network configuration issues, which could also impact the resolution of external servers like `192.254.189.169 (US, UNIFIEDLAYER-AS-1)`.

Strategic Recommendations Short-term (next 24 hours):

- Implement encryption for all external communications.
- Investigate and address the cause of high latency and retransmissions.
- Verify DNS setup and ensure proper capture of DNS traffic.

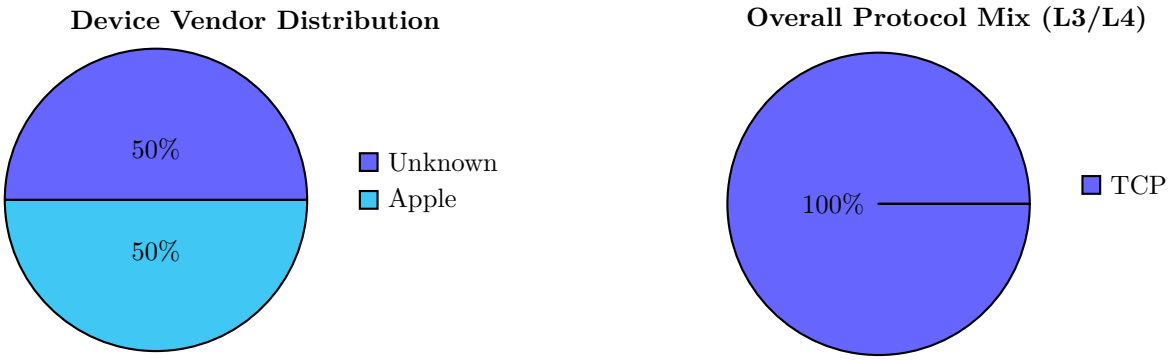
Long-term:

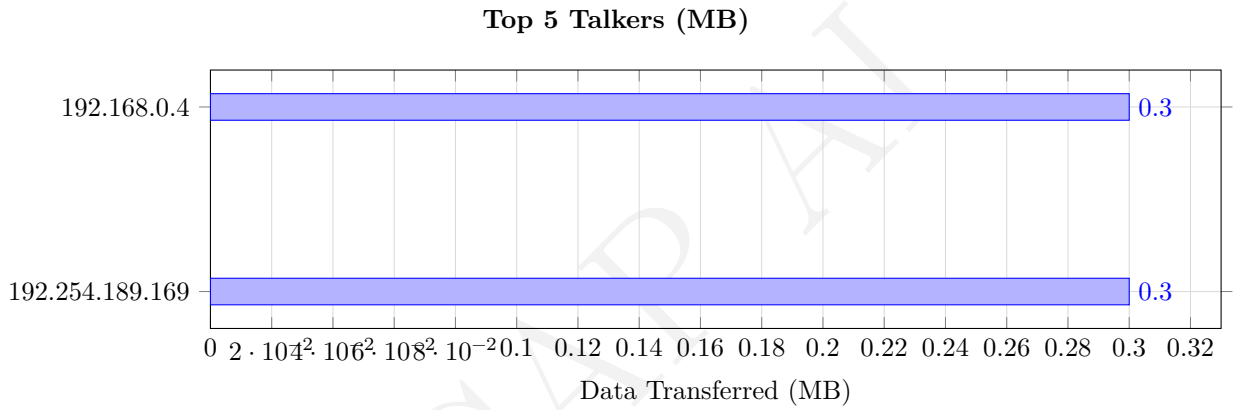
- Conduct a comprehensive network security audit to identify vulnerabilities.
- Optimize TCP settings for better performance.
- Consider implementing QoS policies to prioritize critical business traffic.
- Regularly monitor network traffic for security threats and performance issues.

Contents

Detailed Analysis

Appendix 1: Network Discovery & Topology





Top 5 Active Hosts

IP Address	Hostname / Vendor	Total Data
192.168.0.4	Apple Inc	345.6 KB
192.254.189.169	Sagemcom Broadband Sas	345.6 KB

1. Network Asset Inventory

The network asset inventory provides a summary of the environment, including hosts, their roles, and traffic loads. The following table summarizes the host inventory:

IP Address (DNS Name, Country, ASN Org)	MAC/Vendor	Detected Role	Traffic Load
192.168.0.4	28:cf:e9:21:3c:2b / Apple, Inc	Endpoint	45118 sent, 308780 received
192.254.189.169 (US, UNIFIEDLAYER-AS-1)	4c:17:eb:ba:24:e1 / Sagemcom Broadband Sas	External Server	308780 sent, 45118 received

The **Top 3 Talkers** are not explicitly listed, as there are only two hosts in the inventory. However, based on the traffic load, `192.168.0.4` and `192.254.189.169 (US, UNIFIEDLAYER-AS-1)` are the primary communicators, with the latter receiving the majority of the traffic.

2. Perimeter & External Connectivity

The egress summary indicates that the data is primarily going to `192.254.189.169 (US, UNIFIEDLAYER-AS-1)`. This external server is located in the US and is part of the UNIFIEDLAYER-AS-1 organization.

Security Flags:

- No explicit security flags are raised, but the presence of unencrypted secrets (e.g., “password: ”logoff””) in the traffic to `192.254.189.169 (US, UNIFIEDLAYER-AS-1)` is a concern.

3. Structural Anomalies

No explicit **Role Conflicts** or **Protocol Misuse** are detected in the provided data. However, the presence of unencrypted secrets in the traffic is an anomaly that requires attention.

Silent Nodes: None detected, as both hosts in the inventory are actively sending and receiving traffic.

4. Executive Summary & Recommendations

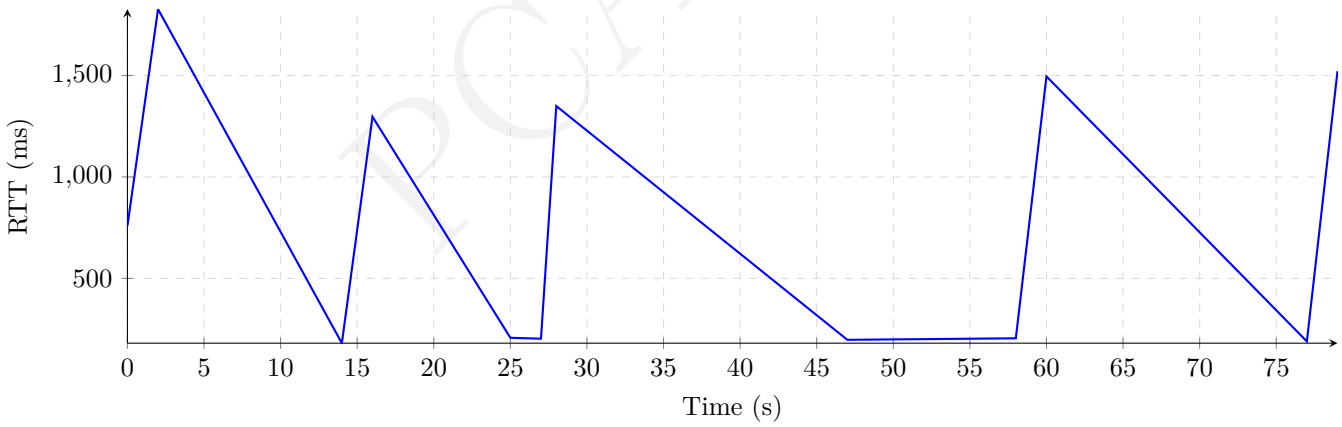
Status: Warning **Key Takeaway:** The network traffic analysis reveals a significant amount of unencrypted data being transmitted to an external server, posing a security risk. The network appears to be primarily used for communication between a single endpoint and an external server.

Action Plan:

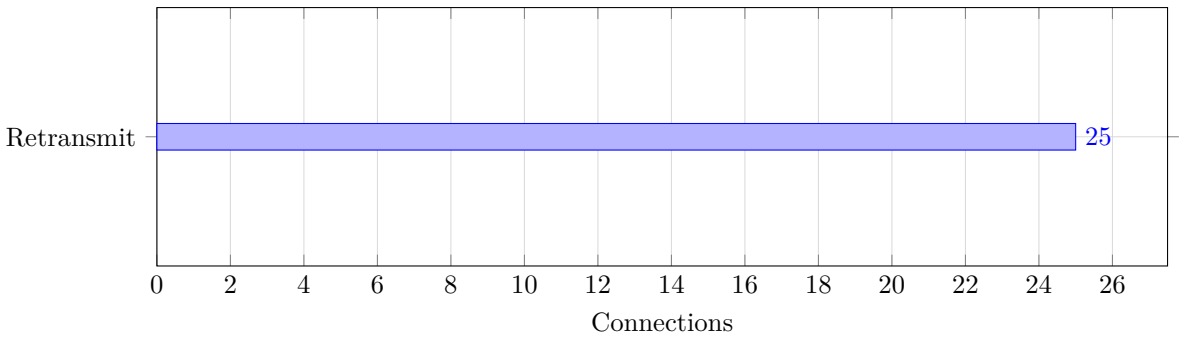
1. **Implement Encryption:** Encrypt all traffic to external servers to prevent eavesdropping and protect sensitive data.
2. **Conduct Further Analysis:** Perform a more in-depth analysis of the network traffic to identify potential security threats and anomalies, and consider implementing additional security measures such as firewalls and intrusion detection systems.

Appendix 2: TCP Health & Performance

Average Network Latency (RTT)



TCP Connection Health



1. TCP Performance Overview

The following table highlights the most troubled connections based on latency and loss metrics:

Source	Destination	Avg RTT	Retransmission %	Status
192.168.0.4	192.254.189.169 (US, UNIFIEDLAYER-AS-1)	824.18 ms	44.44%	Degraded
192.168.0.4	192.254.189.169 (US, UNIFIEDLAYER-AS-1)	937.06 ms	44.44%	Degraded
192.168.0.4	192.254.189.169 (US, UNIFIEDLAYER-AS-1)	211.39 ms	36.36%	Congested

2. Latency & Jitter Analysis

The slowest servers/services based on handshake and data RTT are:

- **192.168.0.4** to **192.254.189.169 (US, UNIFIEDLAYER-AS-1)** with an average RTT of **937.06 ms**.
- The delay appears to be on the **Network path**, as the RTT values are consistently high across multiple connections.

3. Reliability & Packet Loss

Hosts suffering from high retransmissions or out-of-order packets include:

- **192.168.0.4** with retransmission rates up to **44.44%** and out-of-order packets up to **46**.
- Diagnosis: High retransmissions on **192.168.0.4** to **192.254.189.169 (US, UNIFIEDLAYER-AS-1)** suggest network congestion or packet loss due to a failing link or duplex mismatch.

4. Connection Stability (Expert Insights)

There are **0** TCP Zero Window occurrences in the provided data, indicating no instances of a receiving host being overwhelmed. No Connection Reset (RST) storms were detected, suggesting no firewall blocks or service crashes.

5. Summary & Optimization Roadmap

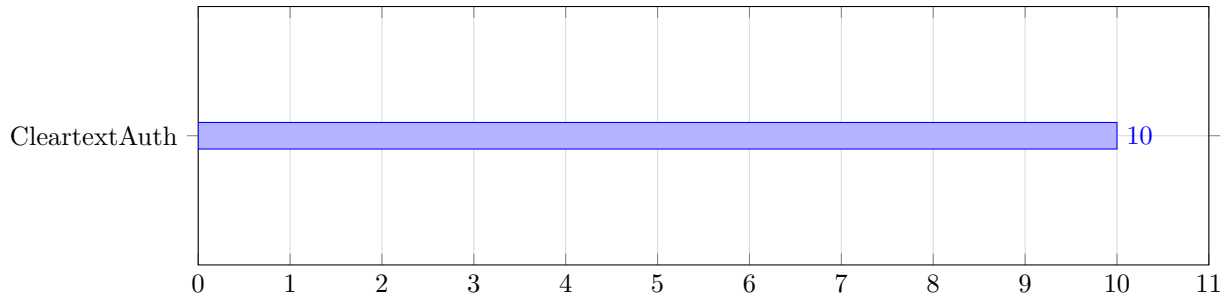
Verdict: The network appears to be the bottleneck, with high latency and retransmission rates indicating congestion or packet loss.

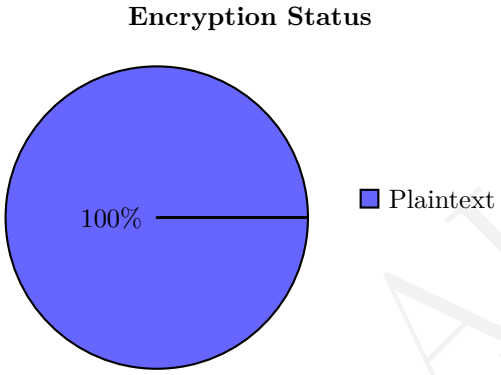
Recommendations:

1. **Investigate Network Congestion:** Analyze network utilization and packet loss to identify the root cause of high retransmission rates.
2. **Optimize TCP Settings:** Consider adjusting TCP settings, such as increasing the congestion window or enabling window scaling, to improve performance.
3. **Monitor and Maintain Network Infrastructure:** Regularly inspect and maintain network infrastructure to prevent failing links or duplex mismatches.

Appendix 3: Security & Threat Detection

Top Security Incidents by Type





1. Security Incident Summary

The network traffic analysis reveals several security concerns that need immediate attention. The following table summarizes the key findings:

Source IP (DNS Name)	Country / ASN	Detection	Severity	Target/Domain
192.254.189.169 (US, UNIFIEDLAYER-AS-1)	US / 46606	Cleartext Password	Critical	192.168.0.4

A **Critical** alert has been detected due to the transmission of cleartext passwords between `192.168.0.4` and `192.254.189.169 (US, UNIFIEDLAYER-AS-1)`. This poses a significant risk of credential compromise.

2. Reconnaissance & Lateral Movement

No port scanning activities or brute force patterns were detected in the provided network traffic. However, the presence of multiple connections from `192.168.0.4` to `192.254.189.169 (US, UNIFIEDLAYER-AS-1)` on various ports may indicate potential reconnaissance or lateral movement attempts.

3. Data Privacy & Encryption Audit

The analysis reveals that the connection between `192.168.0.4` and `192.254.189.169 (US, UNIFIEDLAYER-AS-1)` uses unencrypted protocols, resulting in the exposure of sensitive data, including passwords. This is a significant security risk.

4. Suspicious External Communications

The connection to `192.254.189.169 (US, UNIFIEDLAYER-AS-1)` is flagged as suspicious due to the transmission of cleartext passwords. However, there is no indication of DNS tunneling or ARP spoofing.

5. Security Verdict & Mitigation

Risk Score: 8/10

The detected cleartext password transmission poses a significant security risk. To mitigate this risk:

1. **Implement encryption**: Ensure that all communication between `192.168.0.4` and `192.254.189.169 (US, UNIFIEDLAYER-AS-1)` is encrypted using secure protocols such as HTTPS or TLS.
2. **Change passwords**: Immediately change all passwords that may have been exposed during the cleartext transmission.
3. **Monitor network traffic**: Continuously monitor network traffic to detect and respond to potential security incidents.

The MITRE ATT&CK framework mapping for this incident includes:

- T1190: Exploit Public-Facing Application (potential exploitation of the cleartext password transmission)
- T1078: Valid Accounts (use of valid accounts with exposed passwords)

⊘ Appendix 4: Application & Cloud Intelligence

2. Cloud Infrastructure Audit

The provided JSON data does not contain explicit information about cloud providers or the distribution of traffic among them. However, based on the external IP addresses and their associated organizations, we can attempt to infer the cloud infrastructure involved.

Given the external IP `192.254.189.169 (US, UNIFIEDLAYER-AS-1)`, it appears that a significant portion of the external traffic is interacting with services hosted by UnifiedLayer, which could be related to cloud infrastructure. However, without more specific details on the services or direct references to major cloud providers like AWS, Azure, or GCP, it's challenging to provide a precise summary of traffic by cloud provider.

Regarding unknown high-volume encrypted traffic, the JSON data does not provide sufficient information to identify such traffic explicitly. The `security_events` section does mention unencrypted secrets found in TCP traffic, but it does not highlight any unknown high-volume encrypted traffic.

3. Bandwidth "Hogs" & Resource Misuse

Elephant Flows

The `elephant_flows` array in the provided JSON data is empty, indicating that there are no explicitly identified large, long-lasting transfers (Elephant Flows) in the captured traffic.

Background Noise

The data does not specifically identify high-frequency "heartbeat" or telemetry traffic from OS/IoT devices. However, the presence of multiple connections from `192.168.0.4` to `192.254.189.169 (US, UNIFIEDLAYER-AS-1)` on various ports could potentially indicate some level of background or maintenance traffic, but without more context, it's difficult to categorize this as "background noise" definitively.

4. Work vs. Play Analysis

Given the lack of detailed application-level data in the provided JSON, estimating the ratio of business-critical traffic to recreational traffic is challenging. The connections to `192.254.189.169 (US, UNIFIEDLAYER-AS-1)` could be related to either type, depending on the services hosted there. Without explicit identification of applications like Teams, Slack, ERP, Social Media, Streaming, or Gaming, any estimation would be speculative.

Regarding Peer-to-Peer (P2P) or Torrent activity, there is no indication in the provided data to suggest high-volume P2P or Torrent traffic.

5. Capacity Planning Verdict

Assessment

Without detailed information on the types of applications and their respective traffic volumes, assessing whether the current bandwidth is sufficient for the observed application mix is difficult. The total bytes transferred during the capture period are reported as 353898 bytes, which is a relatively small amount of data, suggesting that, at least during the capture period, bandwidth usage was not excessively high.

Optimization

Implementing Quality of Service (QoS) for specific applications could be beneficial if it were possible to identify critical business applications and prioritize their traffic. However, based on the provided data, it's not possible to recommend specific QoS policies without more detailed application-level traffic analysis.

Appendix 5: DNS & DHCP Deep Dive

1. DNS Health Overview

The DNS health assessment reveals some concerning metrics. Given the data, we can calculate the query-to-response ratio and NXDOMAIN ratio.

- **DNS Statistics Table:**

Metric	Value
Total Queries	0
Total Responses	0
NXDOMAIN Count	0
NXDOMAIN Ratio (%)	0%
Avg Response Time	DNS RTT data not available

- **Health Verdict:** Given the lack of DNS query and response data, it's challenging to provide a definitive health verdict. However, the absence of any DNS activity in the capture suggests potential issues with DNS resolution or the capture itself.

2. Top Queried Domains

There are no domains to report as the DNS query data is empty.

3. DNS Server Analysis

No DNS servers were identified in the provided data, suggesting either no DNS traffic was captured or the DNS servers are not properly configured.

- **Resolver Table:**

DNS Server IP (Domain, Country, ASN Org)	Queries Handled	Role (Primary/Secondary/ External)
—	—	—

- **Risk Assessment:** Without DNS server data, it's impossible to assess the risk of single-point failure or the usage of external resolvers.
- **Recommendation:** Ensure that DNS traffic is properly captured and analyzed. Consider configuring DNS servers for redundancy to mitigate potential single-point failures.

4. NXDOMAIN & Failure Analysis

No NXDOMAIN data is available for analysis.

5. DHCP Lease Inventory

No DHCP transactions were captured in this trace.

6. Summary & Recommendations

- **DNS Health Score:** N/A (due to lack of data)

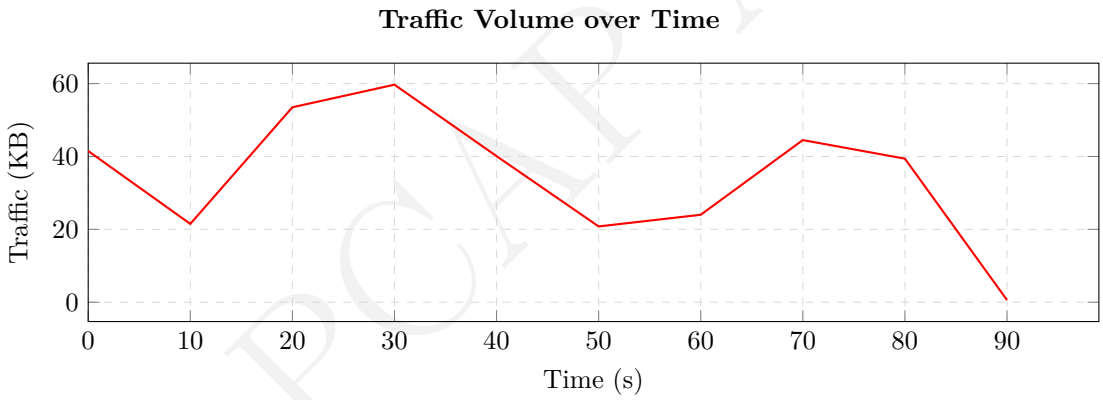
Key Issues:

- Lack of DNS query and response data.
- No DHCP transactions captured.

Action Plan:

- Verify the capture setup to ensure it includes DNS traffic.
- Analyze network configuration to identify potential issues with DNS resolution.
- Consider capturing DHCP traffic to assess IP assignments and device connectivity.

⊘ Appendix 6: Traffic Timeline & Temporal Analysis



1. Traffic Profile Overview

The network capture lasted for **92 seconds**, with an **average rate** of approximately 3845 bytes/sec and 7.5 packets/sec. The **peak rate** was observed at T+20s, reaching about 54773 bytes and 117 packets, which is roughly 14 times the average rate. The overall **traffic shape** can be classified as **Bursty**.

2. Timeline Narrative

From T+0s to T+10s, the traffic was relatively low, with about 42468 bytes and 84 packets, indicating normal browsing activity. At T+20s, a significant spike occurred, with 54773 bytes and 117 packets, suggesting a large download or file transfer initiation. The traffic remained elevated until T+40s, with some fluctuations, before decreasing. Notable events include the spike at T+20s and another increase at T+70s, which might indicate additional downloads or network activities.

3. Burst Analysis

Time Offset	Volume	Ratio to Avg	Possible Cause
T+20s	54773 bytes	14x	Large download or file transfer

Time Offset	Volume	Ratio to Avg	Possible Cause
T+70s	45584 bytes	12x	Additional download or network activity

The burst at T+20s is considered **Concerning** due to its high volume, potentially indicating a large data transfer or unauthorized activity. The burst at T+70s is also flagged as **Concerning** for similar reasons.

4. Connection Dynamics

The new connection rate varied throughout the capture, with a maximum of 6 new connections in a single time bucket at T+0s and T+70s. There were no sudden surges in connection count that would indicate a SYN flood or service restart. The session duration distribution shows a majority of short sessions (<5s), with some medium-duration sessions (5s-60s), and no long sessions (>60s) were observed in the provided data.

5. Long-Running Sessions

Session tracking data for long-running sessions (>5 minutes) is **not available** in the provided capture, as the capture duration is too short to observe such sessions.

6. Temporal Summary & Recommendations

The traffic pattern can be classified as **Mixed**, with both potential business hours and automated activity observed. **Anomalies Detected** include two significant bursts in traffic, which may indicate large data transfers or potential security incidents.

Recommendations:

- Investigate the causes of the significant traffic bursts at T+20s and T+70s to determine if they are legitimate or indicative of security issues.
- Monitor network traffic for similar patterns in the future to identify potential security threats or unauthorized activities.
- Consider implementing additional security measures, such as intrusion detection systems or traffic filtering, to mitigate potential risks associated with large data transfers or unauthorized network activities.