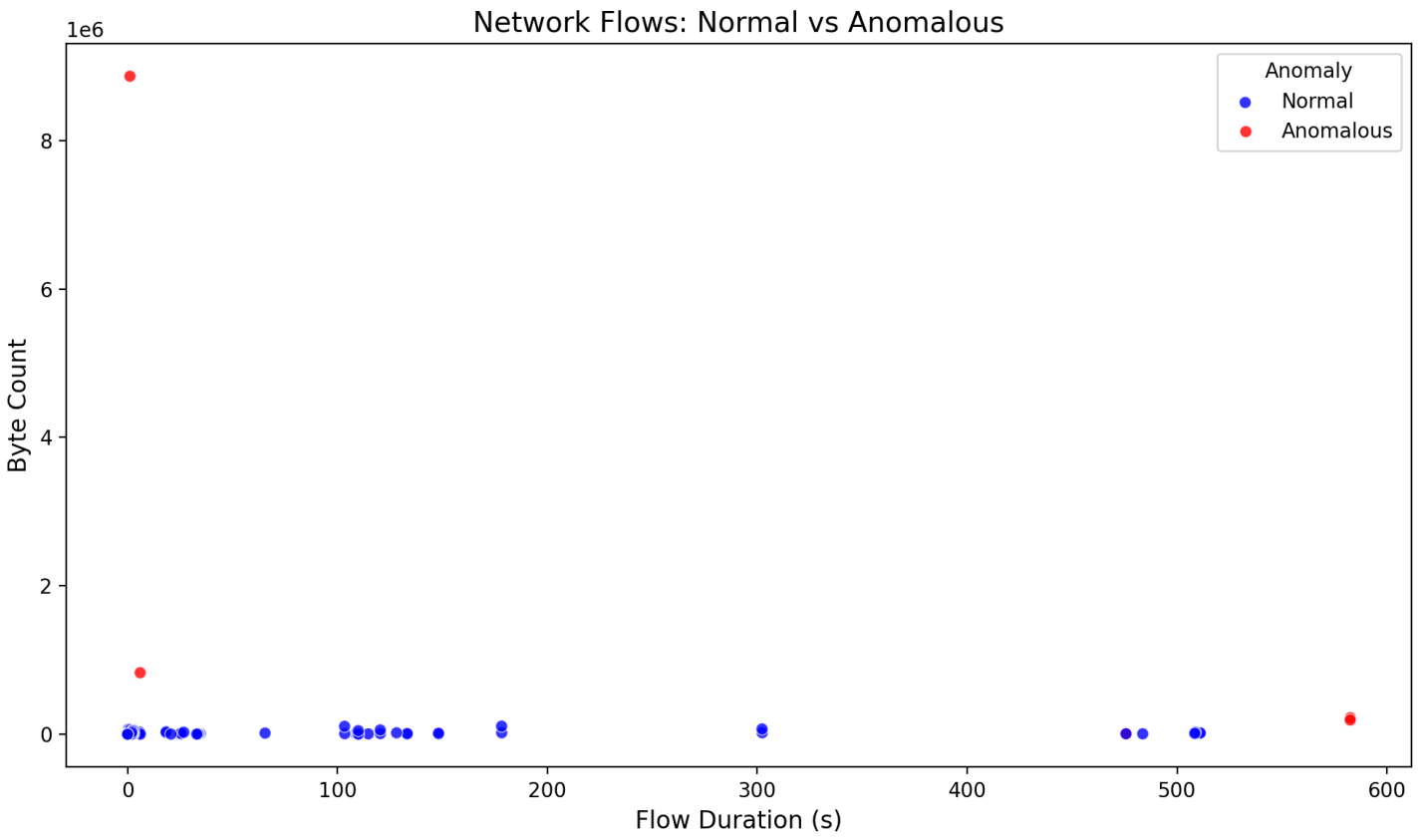
Network Anomaly Report

Generated on 2025-05-26 22:19



Detected Anomalies

Flow #6

Source IP : 172.16.1.66
Destination IP : 172.16.1.4
Protocol : 6
Duration : 582.57 sec
Packets : 797
Bytes : 222643
Bytes/sec : 382.18

MITRE ATT&CK Mappings:

- T1021 | Remote Services
- T1570 | Serverless Execution
- T1071 | Application Layer Protocol
- T1105 | Remote File Copy

Flow #7

Source IP : 172.16.1.4

Destination IP : 172.16.1.66
Protocol : 6
Duration : 582.52 sec
Packets : 715
Bytes : 191613
Bytes/sec : 328.94

MITRE ATT&CK Mappings:
- T1021 | Remote Services
- T1570 | Serverless Execution
- T1071 | Application Layer Protocol
- T1105 | Remote File Copy

Flow #30

Source IP : 172.16.1.66
Destination IP : 20.7.2.167
Protocol : 6
Duration : 475.79 sec
Packets : 17
Bytes : 3677
Bytes/sec : 7.73

MITRE ATT&CK Mappings:
- T1071 | Application Layer Protocol
- T1105 | Remote File Copy

Flow #39

Source IP : 185.199.110.133
Destination IP : 172.16.1.66
Protocol : 6
Duration : 5.99 sec
Packets : 582
Bytes : 828901
Bytes/sec : 138303.91

MITRE ATT&CK Mappings:
- T1021 | Remote Services
- T1570 | Serverless Execution

Flow #41

Source IP : 199.232.196.209
Destination IP : 172.16.1.66
Protocol : 6
Duration : 1.13 sec
Packets : 6085
Bytes : 8868103
Bytes/sec : 7817204.88

MITRE ATT&CK Mappings:
- T1048 | Exfiltration Over Alternative Protocol
- T1029 | Scheduled Transfer
- T1021 | Remote Services

- T1570 | Serverless Execution