

SD-WAN Network Triage Report

Comprehensive Network Analysis

Generated: 2026-01-09 18:38:40 | File: TestFile.pcap

Executive Summary

0	DNS Anomalies	109	TCP Retransmissions	0	ARP Conflicts	0	Suspicious Traffic
0	Failed Handshakes	0	HTTP Errors	12	High RTT Flows	1	Devices Detected
Total Traffic:		661.9 KB		HTTP/2 Flows:		0	QUIC Flows: 0

Risk Assessment

129

Critical

Risk Score Analysis

Primary Concern: 109 TCP Retransmissions

Total Findings: 109

Recommended Actions

HIGH: Excessive TCP retransmissions indicate network congestion or hardware issues. Check links between affected hosts.

MEDIUM: Port scanning activity detected. Review source IPs and consider blocking if malicious.

LOW: High latency flows detected. Check for network congestion or routing issues.

TCP Retransmissions

Source	Destination	Source Port	Dest Port
192.168.100.203	34.36.209.34	58484	443
87.248.119.252	192.168.100.203	443	58482
188.125.72.139	192.168.100.203	443	58477
34.120.133.55	192.168.100.203	443	58495
192.168.100.203	34.120.133.55	58495	443
172.217.19.2	192.168.100.203	443	58494
192.168.100.203	172.217.19.2	58494	443
192.168.100.203	188.125.72.139	58477	443
151.101.65.44	192.168.100.203	443	58498

8.8.4.4	192.168.100.203	443	51366
---------	-----------------	-----	-------

... and 99 more

Port Scan Indicators

Source IP	Target IP	Type	Ports Scanned
192.168.100.203		Vertical	15

Top Traffic Flows

Source	Destination	Protocol	Bytes	Percentage
172.217.19.2:443	192.168.100.203:58494	TCP	42.0 KB	6.4%
2.21.74.59:443	192.168.100.203:58670	TCP	31.6 KB	4.8%
35.223.238.178:443	192.168.100.203:53663	TCP	25.8 KB	3.9%
192.168.100.203:58680	104.18.41.41:443	TCP	23.0 KB	3.5%
192.168.100.203:58477	188.125.72.139:443	TCP	22.1 KB	3.3%
35.223.238.178:443	192.168.100.203:53522	TCP	22.0 KB	3.3%
192.168.100.203:58499	151.101.193.44:443	TCP	17.5 KB	2.6%
104.18.41.41:443	192.168.100.203:58680	TCP	17.3 KB	2.6%
8.8.4.4:443	192.168.100.203:51366	TCP	17.0 KB	2.6%
192.168.100.203:53786	52.110.4.150:443	TCP	14.5 KB	2.2%