

# SD-WAN Network Triage Report

## Comprehensive Network Analysis

Generated: 2026-01-09 18:55:53 | 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 (109 total)

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
192.168.100.203	8.8.4.4	51366	443
192.168.100.203	141.226.224.32	58668	443
141.226.224.32	192.168.100.203	443	58668
142.251.141.162	192.168.100.203	443	58475
192.168.100.203	142.251.141.162	58475	443
192.168.100.203	35.223.238.178	53522	443
151.101.193.44	192.168.100.203	443	58499
192.168.100.203	151.101.193.44	58499	443
192.168.100.203	141.226.228.48	58502	443
172.64.146.215	192.168.100.203	443	58452
35.223.238.178	192.168.100.203	443	53522
192.168.100.203	8.8.8.8	58669	443
8.8.8.8	192.168.100.203	443	58669
192.168.100.203	104.16.103.112	58469	443
192.168.100.203	2.21.74.59	58670	443
2.21.74.59	192.168.100.203	443	58670
192.168.100.203	104.16.103.112	58470	443
192.168.100.203	178.250.7.136	58662	443
192.168.100.203	185.89.210.212	58664	443
192.168.100.203	35.223.238.178	53585	443
35.223.238.178	192.168.100.203	443	53585
192.168.100.203	35.223.238.178	53586	443
192.168.100.203	3.124.64.248	58665	443
35.223.238.178	192.168.100.203	443	53586
192.168.100.203	69.173.156.138	58663	443
192.168.100.203	8.8.8.8	58671	443
8.8.8.8	192.168.100.203	443	58671
192.168.100.203	142.251.38.131	58672	443
142.251.38.131	192.168.100.203	443	58672
192.168.100.203	18.97.36.68	58659	443
192.168.100.203	87.248.119.252	58482	443
151.101.1.44	192.168.100.203	443	58479
34.243.32.177	192.168.100.203	443	58488
192.168.100.203	3.124.64.248	58674	443
192.168.100.203	178.250.7.136	58673	443
192.168.100.203	185.89.210.212	58676	443

Source	Destination	Source Port	Dest Port
192.168.100.203	69.173.156.138	58675	443
185.89.210.212	192.168.100.203	443	58676
3.124.64.248	192.168.100.203	443	58674
209.38.50.75	192.168.100.203	443	58485
104.18.26.193	192.168.100.203	443	58478
185.64.189.112	192.168.100.203	443	58491
69.173.156.138	192.168.100.203	443	58675
35.186.253.211	192.168.100.203	443	58481
192.168.100.203	35.186.253.211	58481	443
34.36.209.34	192.168.100.203	443	58484
34.149.50.64	192.168.100.203	443	58492
192.168.100.203	34.149.50.64	58492	443
192.168.100.203	87.248.119.252	58493	443
192.168.100.203	151.101.65.44	58498	443
192.168.100.203	141.226.224.32	58677	443
141.226.224.32	192.168.100.203	443	58677
140.82.113.25	192.168.100.203	443	58473
192.168.100.203	140.82.113.25	58473	443
192.168.100.203	35.223.238.178	53663	443
35.223.238.178	192.168.100.203	443	53663
104.16.103.112	192.168.100.203	443	58469
104.16.103.112	192.168.100.203	443	58470
192.168.100.203	23.44.215.200	53689	443
23.44.215.200	192.168.100.203	443	53689
192.168.100.203	8.8.8.8	58678	443
8.8.8.8	192.168.100.203	443	58678
192.168.100.203	104.18.41.41	58680	443
192.168.100.203	172.217.19.10	58679	443
192.168.100.203	34.8.63.254	58681	443
104.18.41.41	192.168.100.203	443	58680
34.8.63.254	192.168.100.203	443	58681
172.217.19.10	192.168.100.203	443	58679
192.168.100.203	104.16.102.112	58682	443
104.16.102.112	192.168.100.203	443	58682
192.168.100.203	35.223.238.178	53705	443
192.168.100.203	18.97.36.68	58683	443

Source	Destination	Source Port	Dest Port
35.223.238.178	192.168.100.203	443	53705
18.97.36.68	192.168.100.203	443	58683
192.168.100.203	52.209.232.99	58654	443
192.168.100.203	104.18.26.193	58478	443
192.168.100.203	34.243.32.177	58488	443
192.168.100.203	151.101.1.44	58479	443
192.168.100.203	209.38.50.75	58485	443
192.168.100.203	185.64.189.112	58491	443
192.168.100.203	178.250.7.136	58684	443
192.168.100.203	69.173.156.138	58686	443
192.168.100.203	185.89.210.212	58685	443
185.89.210.212	192.168.100.203	443	58685
178.250.7.136	192.168.100.203	443	58684
69.173.156.138	192.168.100.203	443	58686
192.168.100.203	141.226.224.32	58687	443
141.226.224.32	192.168.100.203	443	58687
192.168.100.203	52.110.4.150	53786	443
192.168.100.203	52.110.4.150	53787	443
192.168.100.203	52.110.4.150	53789	443
192.168.100.203	52.110.4.150	53788	443
52.110.4.150	192.168.100.203	443	53789
52.110.4.150	192.168.100.203	443	53787
52.110.4.150	192.168.100.203	443	53786
192.168.100.203	52.110.4.150	53795	443
52.110.4.150	192.168.100.203	443	53795
192.168.100.203	52.110.4.150	53796	443
52.110.4.150	192.168.100.203	443	53796

## Port Scan Indicators (1 total)

Source IP	Target IP	Type	Ports Scanned
192.168.100.203		Vertical	15

## Traffic Flows (199 total)

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%
192.168.100.203:53796	52.110.4.150:443	TCP	14.5 KB	2.2%
192.168.100.203:53786	52.110.4.150:443	TCP	14.5 KB	2.2%
192.168.100.203:58494	172.217.19.2:443	TCP	12.0 KB	1.8%
192.168.100.203:58674	3.124.64.248:443	TCP	10.8 KB	1.6%
172.217.19.10:443	192.168.100.203:58679	TCP	10.4 KB	1.6%
23.44.215.200:443	192.168.100.203:53689	TCP	10.3 KB	1.6%
192.168.100.203:58681	34.8.63.254:443	TCP	10.1 KB	1.5%
192.168.100.203:58482	87.248.119.252:443	TCP	9.9 KB	1.5%
192.168.100.203:58502	141.226.228.48:443	TCP	9.9 KB	1.5%
151.101.1.44:443	192.168.100.203:58479	TCP	9.1 KB	1.4%
52.110.4.150:443	192.168.100.203:53787	TCP	8.4 KB	1.3%
192.168.100.203:58484	34.36.209.34:443	TCP	8.4 KB	1.3%
52.110.4.150:443	192.168.100.203:53795	TCP	8.3 KB	1.3%
192.168.100.203:58491	185.64.189.112:443	TCP	8.3 KB	1.3%
52.110.4.150:443	192.168.100.203:53796	TCP	8.2 KB	1.2%
52.110.4.150:443	192.168.100.203:53786	TCP	8.2 KB	1.2%
52.110.4.150:443	192.168.100.203:53788	TCP	8.1 KB	1.2%
52.110.4.150:443	192.168.100.203:53789	TCP	8.0 KB	1.2%
8.8.8.8:443	192.168.100.203:58678	TCP	7.4 KB	1.1%
104.16.102.112:443	192.168.100.203:58682	TCP	7.2 KB	1.1%
34.8.63.254:443	192.168.100.203:58681	TCP	6.9 KB	1.0%
8.8.8.8:443	192.168.100.203:58669	TCP	6.2 KB	0.9%
192.168.100.203:58679	172.217.19.10:443	TCP	5.9 KB	0.9%
18.97.36.68:443	192.168.100.203:58683	TCP	5.8 KB	0.9%
192.168.100.203:58676	185.89.210.212:443	TCP	5.7 KB	0.9%

Source	Destination	Protocol	Bytes	Percentage
192.168.100.203:58685	185.89.210.212:443	TCP	5.7 KB	0.9%
192.168.100.203:53663	35.223.238.178:443	TCP	5.7 KB	0.9%
192.168.100.203:53795	52.110.4.150:443	TCP	5.5 KB	0.8%
192.168.100.203:51366	8.8.4.4:443	TCP	5.5 KB	0.8%
192.168.100.203:58481	35.186.253.211:443	TCP	5.2 KB	0.8%
192.168.100.203:58479	151.101.1.44:443	TCP	5.2 KB	0.8%
3.124.64.248:443	192.168.100.203:58674	TCP	5.0 KB	0.8%
8.8.8.8:443	192.168.100.203:58671	TCP	5.0 KB	0.8%
192.168.100.203:58488	34.243.32.177:443	TCP	5.0 KB	0.8%
69.173.156.138:443	192.168.100.203:58675	TCP	5.0 KB	0.8%
69.173.156.138:443	192.168.100.203:58686	TCP	4.9 KB	0.7%
35.223.238.178:443	192.168.100.203:53705	TCP	4.9 KB	0.7%
192.168.100.203:53522	35.223.238.178:443	TCP	4.9 KB	0.7%
188.125.72.139:443	192.168.100.203:58477	TCP	4.8 KB	0.7%
141.226.228.48:443	192.168.100.203:58502	TCP	4.8 KB	0.7%
192.168.100.203:58478	104.18.26.193:443	TCP	4.5 KB	0.7%
192.168.100.203:53705	35.223.238.178:443	TCP	4.4 KB	0.7%
172.64.146.215:443	192.168.100.203:58452	TCP	4.4 KB	0.7%
142.251.38.131:443	192.168.100.203:58672	TCP	4.1 KB	0.6%
178.250.7.136:443	192.168.100.203:58673	TCP	4.0 KB	0.6%
178.250.7.136:443	192.168.100.203:58684	TCP	4.0 KB	0.6%
34.36.209.34:443	192.168.100.203:58484	TCP	3.9 KB	0.6%
185.89.210.212:443	192.168.100.203:58676	TCP	3.7 KB	0.6%
185.89.210.212:443	192.168.100.203:58685	TCP	3.7 KB	0.6%
192.168.100.203:58673	178.250.7.136:443	TCP	3.6 KB	0.5%
192.168.100.203:58475	142.251.141.162:443	TCP	3.6 KB	0.5%
192.168.100.203:58684	178.250.7.136:443	TCP	3.6 KB	0.5%
192.168.100.1:46616	255.255.255.255:7437	TCP	3.5 KB	0.5%
35.223.238.178:443	192.168.100.203:53585	TCP	3.5 KB	0.5%
35.223.238.178:443	192.168.100.203:53586	TCP	3.5 KB	0.5%
192.168.100.203:58675	69.173.156.138:443	TCP	3.5 KB	0.5%
192.168.100.203:58686	69.173.156.138:443	TCP	3.5 KB	0.5%
192.168.100.203:58485	209.38.50.75:443	TCP	3.4 KB	0.5%
192.168.100.203:58498	151.101.65.44:443	TCP	3.3 KB	0.5%
151.101.193.44:443	192.168.100.203:58499	TCP	3.1 KB	0.5%
192.168.100.203:58682	104.16.102.112:443	TCP	3.0 KB	0.5%

Source	Destination	Protocol	Bytes	Percentage
192.168.100.203:58492	34.149.50.64:443	TCP	2.9 KB	0.4%
141.226.224.32:443	192.168.100.203:58687	TCP	2.8 KB	0.4%
141.226.224.32:443	192.168.100.203:58677	TCP	2.8 KB	0.4%
141.226.224.32:443	192.168.100.203:58668	TCP	2.8 KB	0.4%
192.168.100.203:53787	52.110.4.150:443	TCP	2.7 KB	0.4%
192.168.100.203:53789	52.110.4.150:443	TCP	2.6 KB	0.4%
192.168.100.203:53788	52.110.4.150:443	TCP	2.6 KB	0.4%
192.168.100.203:58654	52.209.232.99:443	TCP	2.4 KB	0.4%
87.248.119.252:443	192.168.100.203:58482	TCP	2.2 KB	0.3%
192.168.100.203:58678	8.8.8.8:443	TCP	1.9 KB	0.3%
142.251.141.162:443	192.168.100.203:58475	TCP	1.9 KB	0.3%
192.168.100.203:58672	142.251.38.131:443	TCP	1.8 KB	0.3%
192.168.100.203:58669	8.8.8.8:443	TCP	1.6 KB	0.2%
fe80::969:c8be:e2b6:9e...	ff02::fb:5353	TCP	1.6 KB	0.2%
192.168.100.203:53585	35.223.238.178:443	TCP	1.5 KB	0.2%
192.168.100.203:58683	18.97.36.68:443	TCP	1.5 KB	0.2%
192.168.100.229:5353	224.0.0.251:5353	TCP	1.5 KB	0.2%
fe80::18ab:b08f:5e8c:d...	ff02::fb:5353	TCP	1.4 KB	0.2%
104.18.26.193:443	192.168.100.203:58478	TCP	1.3 KB	0.2%
192.168.100.203:58670	2.21.74.59:443	TCP	1.3 KB	0.2%
192.168.100.191:5353	224.0.0.251:5353	TCP	1.2 KB	0.2%
192.168.100.203:58671	8.8.8.8:443	TCP	1.2 KB	0.2%
192.168.100.203:58677	141.226.224.32:443	TCP	1.2 KB	0.2%
192.168.100.203:58668	141.226.224.32:443	TCP	1.2 KB	0.2%
192.168.100.203:58687	141.226.224.32:443	TCP	1.2 KB	0.2%
192.168.100.203:53586	35.223.238.178:443	TCP	1.1 KB	0.2%
34.149.50.64:443	192.168.100.203:58492	TCP	1.1 KB	0.2%
151.101.65.44:443	192.168.100.203:58498	TCP	1.1 KB	0.2%
fe80::1c69:48a7:a8e1:3...	ff02::fb:5353	TCP	1.0 KB	0.2%
192.168.100.203:5353	224.0.0.251:5353	TCP	992 B	0.1%
52.209.232.99:443	192.168.100.203:58654	TCP	934 B	0.1%
34.243.32.177:443	192.168.100.203:58488	TCP	914 B	0.1%
192.168.100.203:5353	192.168.100.191:5353	TCP	804 B	0.1%
192.168.100.203:51655	35.223.238.178:443	TCP	792 B	0.1%
8.8.8.8:53	192.168.100.203:60429	TCP	620 B	0.1%
192.168.100.220:9956	192.168.100.255:9956	TCP	592 B	0.1%

Source	Destination	Protocol	Bytes	Percentage
192.168.100.203:53689	23.44.215.200:443	TCP	484 B	0.1%
fe80::1c69:48a7:a8e1:3...	fe80::18ab:b08f:5e8c:d...	TCP	422 B	0.1%
192.168.100.203:51654	35.223.238.178:443	TCP	401 B	0.1%
35.186.253.211:443	192.168.100.203:58481	TCP	376 B	0.1%
192.168.100.1:57834	192.168.100.255:20002	TCP	356 B	0.1%
192.168.100.203:58495	34.120.133.55:443	TCP	345 B	0.1%
8.8.8.8:53	192.168.100.203:10259	TCP	269 B	0.0%
35.223.238.178:443	192.168.100.203:51655	TCP	268 B	0.0%
34.120.133.55:443	192.168.100.203:58495	TCP	255 B	0.0%
142.251.36.74:443	192.168.100.203:58451	TCP	255 B	0.0%
35.223.238.178:443	192.168.100.203:51654	TCP	253 B	0.0%
8.8.8.8:53	192.168.100.203:51241	TCP	237 B	0.0%
87.248.119.252:443	192.168.100.203:58493	TCP	213 B	0.0%
185.64.189.112:443	192.168.100.203:58491	TCP	170 B	0.0%
192.168.100.203:60429	8.8.8.8:53	TCP	168 B	0.0%
192.168.100.203:58470	104.16.103.112:443	TCP	168 B	0.0%
142.251.36.74:443	192.168.100.203:58613	TCP	168 B	0.0%
192.168.100.203:58469	104.16.103.112:443	TCP	168 B	0.0%
192.168.100.203:58493	87.248.119.252:443	TCP	165 B	0.0%
104.16.103.112:443	192.168.100.203:58469	TCP	152 B	0.0%
104.16.103.112:443	192.168.100.203:58470	TCP	152 B	0.0%
8.8.8.8:53	192.168.100.203:60011	TCP	151 B	0.0%
209.38.50.75:443	192.168.100.203:58485	TCP	124 B	0.0%
192.168.100.203:51241	8.8.8.8:53	TCP	80 B	0.0%
192.168.100.203:10259	8.8.8.8:53	TCP	80 B	0.0%
185.89.210.212:443	192.168.100.203:58664	TCP	77 B	0.0%
192.168.100.1:60336	224.0.0.251:5353	TCP	74 B	0.0%
192.168.100.1:51251	224.0.0.251:5353	TCP	74 B	0.0%
192.168.100.1:58496	224.0.0.251:5353	TCP	74 B	0.0%
192.168.100.1:56578	224.0.0.251:5353	TCP	74 B	0.0%
192.168.100.1:49765	224.0.0.251:5353	TCP	74 B	0.0%
192.168.100.1:39130	224.0.0.251:5353	TCP	74 B	0.0%
192.168.100.1:34970	224.0.0.251:5353	TCP	74 B	0.0%
192.168.100.1:47573	224.0.0.251:5353	TCP	74 B	0.0%
192.168.100.1:40611	224.0.0.251:5353	TCP	74 B	0.0%
192.168.100.1:38185	224.0.0.251:5353	TCP	74 B	0.0%



Source	Destination	Protocol	Bytes	Percentage
192.168.100.1:41363	224.0.0.251:5353	TCP	74 B	0.0%
192.168.100.1:48358	224.0.0.251:5353	TCP	74 B	0.0%
192.168.100.1:46131	224.0.0.251:5353	TCP	74 B	0.0%
192.168.100.1:46003	224.0.0.251:5353	TCP	74 B	0.0%
192.168.100.1:51234	224.0.0.251:5353	TCP	74 B	0.0%
192.168.100.1:47608	224.0.0.251:5353	TCP	74 B	0.0%
192.168.100.1:56852	224.0.0.251:5353	TCP	74 B	0.0%
192.168.100.1:50703	224.0.0.251:5353	TCP	74 B	0.0%
192.168.100.1:35812	224.0.0.251:5353	TCP	74 B	0.0%
192.168.100.1:45937	224.0.0.251:5353	TCP	74 B	0.0%
8.8.8.8:53	192.168.100.203:58484	TCP	71 B	0.0%
8.8.8.8:53	192.168.100.203:51379	TCP	71 B	0.0%
192.168.100.203:58602	108.177.15.84:443	TCP	63 B	0.0%
3.124.64.248:443	192.168.100.203:58665	TCP	63 B	0.0%
178.250.7.136:443	192.168.100.203:58662	TCP	63 B	0.0%
192.168.100.203:60011	8.8.8.8:53	TCP	55 B	0.0%
192.168.100.203:58484	8.8.8.8:53	TCP	55 B	0.0%
192.168.100.203:51379	8.8.8.8:53	TCP	55 B	0.0%
69.173.156.138:443	192.168.100.203:58663	TCP	39 B	0.0%
34.141.79.142:7500	192.168.100.203:65529	TCP	37 B	0.0%
23.44.215.194:443	192.168.100.203:52691	TCP	31 B	0.0%
192.168.100.203:52691	23.44.215.194:443	TCP	31 B	0.0%
192.168.100.203:58664	185.89.210.212:443	TCP	31 B	0.0%
192.168.100.203:58473	140.82.113.25:443	TCP	29 B	0.0%
140.82.113.25:443	192.168.100.203:58473	TCP	25 B	0.0%
192.168.100.203:58665	3.124.64.248:443	TCP	24 B	0.0%
192.168.100.203:58666	8.8.8.8:443	TCP	24 B	0.0%
192.168.100.203:58667	104.16.102.112:443	TCP	24 B	0.0%
192.168.100.203:58662	178.250.7.136:443	TCP	24 B	0.0%
18.97.36.68:443	192.168.100.203:58659	TCP	24 B	0.0%
192.168.100.203:58659	18.97.36.68:443	TCP	24 B	0.0%
192.168.100.203:58663	69.173.156.138:443	TCP	24 B	0.0%
192.168.100.203:55801	17.42.251.72:993	TCP	0 B	0.0%
192.168.100.203:65529	34.141.79.142:7500	TCP	0 B	0.0%
104.16.102.112:443	192.168.100.203:58667	TCP	0 B	0.0%
17.42.251.72:993	192.168.100.203:55801	TCP	0 B	0.0%

Source	Destination	Protocol	Bytes	Percentage
142.251.36.65:443	192.168.100.203:58572	TCP	0 B	0.0%
17.42.251.72:993	192.168.100.203:55804	TCP	0 B	0.0%
8.8.8.8:443	192.168.100.203:58666	TCP	0 B	0.0%
74.125.133.188:5228	192.168.100.203:51166	TCP	0 B	0.0%
192.168.100.203:58661	142.251.36.74:443	TCP	0 B	0.0%
192.168.100.203:58572	142.251.36.65:443	TCP	0 B	0.0%
142.251.141.161:443	192.168.100.203:58570	TCP	0 B	0.0%
192.168.100.203:58637	34.107.243.93:443	TCP	0 B	0.0%
34.107.243.93:443	192.168.100.203:58638	TCP	0 B	0.0%
34.107.243.93:443	192.168.100.203:58637	TCP	0 B	0.0%
192.168.100.203:58613	142.251.36.74:443	TCP	0 B	0.0%
142.251.36.78:443	192.168.100.203:58660	TCP	0 B	0.0%
192.168.100.203:58451	142.251.36.74:443	TCP	0 B	0.0%
192.168.100.203:51166	74.125.133.188:5228	TCP	0 B	0.0%
142.251.36.74:443	192.168.100.203:58661	TCP	0 B	0.0%
192.168.100.203:55804	17.42.251.72:993	TCP	0 B	0.0%
192.168.100.203:58660	142.251.36.78:443	TCP	0 B	0.0%
192.168.100.203:58570	142.251.141.161:443	TCP	0 B	0.0%
192.168.100.203:58638	34.107.243.93:443	TCP	0 B	0.0%
192.168.100.203:58452	172.64.146.215:443	TCP	0 B	0.0%
108.177.15.84:443	192.168.100.203:58602	TCP	0 B	0.0%