

NORTH-SOUTH AND EAST-WEST TRAFFIC

It's a simple question without an easy answer: What encryption technologies are organizations seeing in their networks, not just for North-South internet traffic, but also East-West intra-organization communications? There are many surveys and research reports for public internet use of SSL/TLS. This research is unique in studying trends in the use of encryption for internal network and applications.

PRODUCTION TRAFFIC DATA



654,498,305,927

North-South Flows



706,535,646,582

East-West Flows

ENCRYPTED VS. NOT ENCRYPTED



81%

81% of North-South Traffic is encrypted. Overwhelming amount of encrypted traffic underscores the importance of decrypting and inspecting this blind spot.

19%

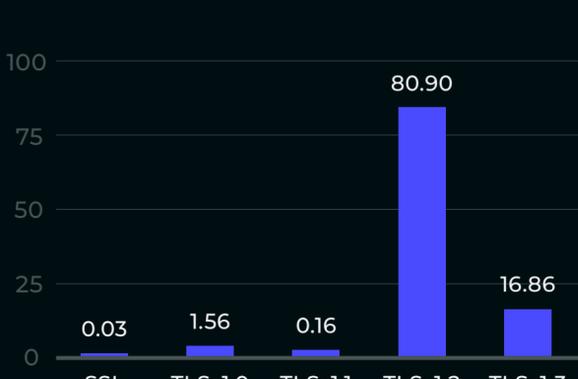
35% of East-West Traffic is not encrypted. Encrypting all feasible East-West Traffic is an opportunity for organizations to improve security posture.

65%



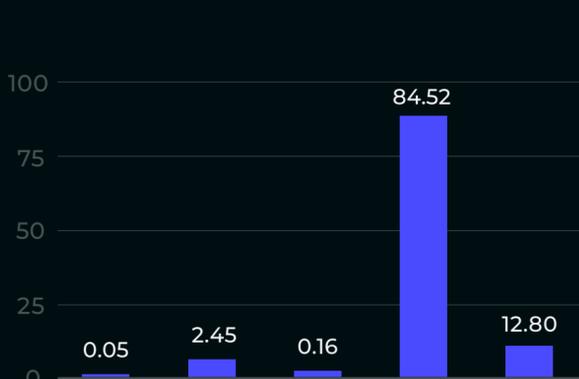
35%

VERSION BREAKDOWN



TLS 1.3 is off to a strong start in North-South Traffic. TLS 1.3 may require some reworking of tool deployment architecture, but allowing this traffic through uninspected poses an increasingly greater risk.

TLS 1.2 dominates East-West Traffic. Use of outdated protocols poses an unacceptable risk and must be addressed.



THE CONTINUED USE OF SSL



0.03%

SSL encrypted traffic

42,424,651

Total flows across data set



0.13%

SSL encrypted traffic

219,286,189

Total flows across data set

RECOMMENDATIONS

- Know your traffic's volume and composition
- Know what traffic needs to be decrypted
- Determine your solution's limitations
- Have an inspection plan
- Understand the impact of decryption on network devices
- Plan for traffic growth
- Research potential decryption platforms
- Eliminate the possibility of outages

Gigamon offers a deep observability pipeline that harnesses actionable network-level intelligence to amplify the power of observability tools. This powerful combination enables IT organizations to assure security and compliance, speed root-cause associated with performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures.

Read the report for more findings and actionable TLS inspection recommendations.