IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 8, June 2022
Impact Factor: 6.252

Traffic Filtering (QoS) Dataset for SD-WAN

Mr. Vinayak Singh[1], Ms. Megha Dhar[2], Mr. Shivanshu Shrivastav[3], Prof. Asharani Chadchankar[4]
Student, Computer Engineering, NBNSSOE, Pune, India [1,2,3]
Assistant Professor, Computer Engineering, NBNSSOE, Pune, India[4]

Abstract: *The demand for reliable and efficient Wide Area Networks (WANs) from business customers is continuously in- creasing. Companies and enterprises use WANs to exchange critical data between headquarters, far-off business branches and cloud data centers. Today, the emerging technology for WAN is Software-Defined Wide Area Networking (SD-WAN) that introduces the Software-Defined Networking (SDN) paradigm into the enterprise-network market. SD-WAN can support differentiated services over public WAN by dynamically reconfiguring in real-time network devices at the edge of the network according to network measurements and service requirements. On the one hand, SD-WAN reduces the high costs of guaranteed QoS WAN solutions (as MPLS), without giving away reliability in practical scenarios. On the other, it brings numerous technical challenges, such as the implementation of Traffic Engineering (TE) methods.*

Keywords: Intrusion, Dataset, Network Traffic, Network Security, Software Defined Networking (SDN), Software- Defined Wide Area Network (SD-WAN), etc.

REFERENCES

[1] M. S. Elsayed, N. -A. Le-Khac and A. D. Jurcut, "This: A Novel SD-WAN QoS Dataset," in IEEE Access, vol. 8, pp. 165263165284,2020, doi:10.1109/ACCESS.2020.3022633, doi:10.1126/science.1065467.
[2] O. Salman, I. H. Elhajj, A. Chehab and A. Kayssi, "QoS guarantee over hybrid SD-WAN/non-SD-WAN networks," 2017 8th International Conference on the Network of the Future (NOF), London, 2017, pp. 141-143, doi:10.1109/NOF.2017.8251237
[3] R. Amin, M. Reisslein and N. Shah, "Hybrid SD-WAN Networks: A Survey of Existing Approaches," in IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3259-3306, Fourth quarter 2018, doi: 10.1109/COMST.2018.2837161.
[4] A. Prakash and R. Priyadarshini, "An intelligent software defined network controller for preventing distributed denial of service attack", Proc. 2nd Int. Conf. Inventive Commun. Comput. Technol. (ICICCT), pp. 585-589, Apr. 2018.
[5] D. Li, C. Yu, Q. Zhou and J. Yu, "Using SVM to detect DDoS attack in SD-WAN network", IOP Conf. Ser. Mater. Sci. Eng., vol. 466, Dec. 2018.
[6] M. Banton, N. Shone, W. Hurst and Q. Shi, "Intrusion Detection Using Extremely Limited Data Based on SD-WAN," 2020 IEEE 10th International Conference on Intelligent Systems (IS), Varna, Bulgaria, 2020, pp. 304309, doi: 10.1109/IS48319.2020.9199950.
[7] Habibi Lashkari, Arash. (2018). CICFlowmeter-V4.0 (formerly known as ISCXFlowMeter) is a network traffic Bi-flow generator and analyser for anomaly detection. https://github.com/ISCX/CICFlowMeter. 10.13140/RG.2.2.13827.20003.
[8] S. P. Bendale and J. Rajesh Prasad, "Security Threats and Challenges in Future Mobile Wireless Networks," 2018 IEEE.
[9] Global Conference on Wireless Computing and Networking (GCWCN), Lonavala, India, 2018, pp. 146-150, doi: 10.1109/GCWCN.2018.8668635.
[10] Shailesh Pramod Bendale, Jayashree Rajesh Prasad. (2020). Security Challenges to provide Intelligence in SD-WAN with the help of Machine Learning or Deep Learning. International Journal of Advanced Science and Technology, 29(05), 356 – 363, http://sersc.org/journals/index.php/IJAST/article/view/8983

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 8, June 2022
Impact Factor: 6.252

[11] Chinmay Dharmadhikari, Salil Kulkarni, Swarali Temkar, Shailesh Bendale, Comparative Analysis of DDoS Mitigation Algorithms in SD-WAN, International Journal of Future Generation Communication and NetworkingVol.13, No.2s, (2020), pp.17001707http://www.sersc.org/journals/index.php/IJFGCN/article/view/29228/16286.