Bibliography

Alcock, S. and Nelson, R., "Libprotoident: Traffic classification using lightweight packet inspection," *WAND Network Research Group, Tech. Rep.*, 2012.

Alcock, S. and Nelson, R., "Measuring the accuracy of open-source payload-based traffic classifiers using popular Internet applications," in "38th Annual IEEE Conference on Local Computer Networks - Workshops," pp. 956–963, 2013.

Almubayed, A., Ali, H., and Atoum, J., "A Model for Detecting Tor Encrypted Traffic using Supervised Machine Learning," *International Journal of Computer Network and Information Security*, volume 7(7) pp. 10–23, 2015.

Antonello, R., Fernandes, S., Kamienski, C., Sadok, D., Kelner, J., Gdor, I., Szab, G., and Westholm, T., "Deep packet inspection tools and techniques in commodity platforms: Challenges and trends," *Journal of Network and Computer Applications*, volume 35(6) pp. 1863 – 1878, 2012.

Appsruntheworld, "Top 10 Enterprise Software Vendors, 2016 Market Overview and Forecast," , 2016, URL `https://www.appsruntheworld.com/top-10-enterprise-software-vendors-2016-market-overview-and-forecast/`, [Online] Accessed: 2017-04-10.

Barker, J., Hannay, P., and Szewczyk, P., "Using Traffic Analysis to Identify the Second Generation Onion Router," in "2011 IFIP 9th International Conference on Embedded and Ubiquitous Computing," pp. 72–78, 2011.

Bendrath, R. and Mueller, M., "The end of the net as we know it? Deep packet inspection and internet governance," *New Media & Society*, volume 13(7) pp. 1142–1160, 2011.

Bujlow, T., Carela-Espaol, V., and Barlet-Ros, P., "Independent comparison of popular {DPI} tools for traffic classification," *Computer Networks*, volume 76 pp. 75 – 89, 2015.

Callado, A., Kamienski, C., Szabo, G., Gero, B. P., Kelner, J., Fernandes, S., and Sadok, D., “A Survey on Internet Traffic Identification,” *IEEE Communications Surveys Tutorials*, volume 11(3) pp. 37–52, 2009.

Camarillo, G. and IAB, “Peer-to-Peer (P2P) Architecture: Definition, Taxonomies, Examples, and Applicability,” RFC 5694 (Informational), 2009.

Cho, Y. H. and Mangione-Smith, W. H., “Deep packet filter with dedicated logic and read only memories,” in “12th Annual IEEE Symposium on Field-Programmable Custom Computing Machines,” pp. 125–134, 2004.

Cui, W., Kannan, J., and Wang, H. J., “Discoverer: Automatic Protocol Reverse Engineering from Network Traces.” in “Usenix Security,” volume 158, 2007.

Deri, L., Martinelli, M., Bujlow, T., and Cardigliano, A., “nDPI: Open-source high-speed deep packet inspection,” in “2014 International Wireless Communications and Mobile Computing Conference (IWCMC),” pp. 617–622, 2014.

Dubrawsky, I., “Firewall Evolution - Deep Packet Inspection,” , 2003, URL `https://www.symantec.com/connect/articles/firewall-evolution-deep-packet-inspection`, [Online] Accessed: 2017-06-15.

Dyer, K. P., Coull, S. E., Ristenpart, T., and Shrimpton, T., “Protocol Misidentification Made Easy with Format-transforming Encryption,” in “Proceedings of the 2013 ACM SIGSAC Conference on Computer &#38; Communications Security,” CCS ’13, pp. 61–72, New York, NY, USA: ACM, 2013.

Ferguson, R., “The history of the next-generation firewall,” , 2012, URL `http://www.computerweekly.com/news/2240159432/The-history-of-the-Next-Generation-Firewall`, [Online] Accessed: 2017-06-15.

Freed, N., “Behavior of and Requirements for Internet Firewalls,” RFC 2979 (Informational), 2000.

helium, “Web Testing and Automation — Helium,” , 2017, URL `http://heliumhq.com/`, [Online] Accessed: 2017-04-10.

Ingham, K. and Forrest, S., “A history and survey of network firewalls,” *University of New Mexico, Tech. Rep*, 2002.

Mogul, J., Rashid, R., and Accetta, M., “The Packer Filter: An Efficient Mechanism for User-level Network Code,” in “Proceedings of the Eleventh ACM Symposium on Operating Systems Principles,” SOSP ’87, pp. 39–51, New York, NY, USA: ACM, 1987.

Mohajeri Moghaddam, H., Li, B., Derakhshani, M., and Goldberg, I., “SkypeMorph: Protocol Obfuscation for Tor Bridges,” in “Proceedings of the 2012 ACM Conference on Computer and Communications Security,” CCS ’12, pp. 97–108, New York, NY, USA: ACM, 2012.

ntop, “ntop - High Performance Network Monitoring Solutions based on Open Source and Commodity Hardware.” http://www.ntop.org/, 2017, [Online] Accessed: 2017-03-30.

Pescatore, J. and Young, G., “Defining the next-generation firewall,” *Gartner RAS Core Research Note*, 2009.

Renals, P. and Jacoby, G. A., “Blocking Skype through Deep Packet Inspection,” in “2009 42nd Hawaii International Conference on System Sciences,” pp. 1–5, 2009.

Rohde&Schwarz, “DPI Engine - RS PACE 2 — Deep Packet Inspection from RS Cybersecurity ipoque GmbH,” , 2017, URL https://www.ipoque.com/products/dpi-engine-rsrpace-2, [Online] Accessed: 2017-03-30.

Saputra, F. A., Nadhori, I. U., and Barry, B. F., “Detecting and blocking onion router traffic using deep packet inspection,” in “2016 International Electronics Symposium (IES),” pp. 283–288, 2016.

Skyhighnetworks, “The Most Popular Cloud Services Rankings 2016,” , 2017, URL https://www.skyhighnetworks.com/cloud-security-blog/the-20-totally-most-popular-cloud-services-in-todays-enterprise/, [Online] Accessed: 2017-04-10.

Stallings, W., *Network security essentials: applications and standards*, Pearson Education, 2011.

Tan, L. and Sherwood, T., “A High Throughput String Matching Architecture for Intrusion Detection and Prevention,” in “Proceedings of the 32Nd Annual International Symposium on Computer Architecture,” ISCA ’05, pp. 112–122, Washington, DC, USA: IEEE Computer Society, 2005.

UltraTools, “Whois IP Lookup Tool,” , 2017, URL `https://www.ultratools.com/tools/ipWhoisLookup`, [Online] Accessed: 2017-04-23.

Velan, P., ermk, M., eleda, P., and Draar, M., “A survey of methods for encrypted traffic classification and analysis,” *International Journal of Network Management*, volume 25(5) pp. 355–374, 2015, nem.1901.

WAND, “WAND Network Research Group: libprotoident,” , 2017, URL `https://research.wand.net.nz/software/libprotoident.php`, [Online] Accessed: 2017-03-30.