ANALYSIS OF VPN OBFUSCATION METHODS

Andris Začs

Transport and Telecommunication Institute
Lomonosova 1, Riga, LV-1019, Latvia
andriszacs0@gmail.com

Keywords: VPN Obfuscation, deep packet inspection, steganography, traffic morphing

The need for various VPN obfuscation techniques came about due to the rapid advancement of Deep Packet Inspection (DPI) technologies, which bought with it concerns regarding online privacy and unrestricted internet access (El-Maghraby, 2017). This paper offers an analysis of VPN obfuscation's present situation and potential future developments, emphasizing novel approaches to foil DPI strategies that are becoming increasingly complex. As a recent example, we have the Geneva algorithm which employs genetic algorithms to generate dynamic, packet- manipulation-based evasion strategies, providing a new take on DPI evasion (Bock *et al*., 2019).

Steganography can also be utilized in VPN obfuscation. This method provides a way around DPI systems by embedding VPN traffic inside regular data streams. Steganography enables regular web traffic, like audio or video streams, to conceal VPN packets, making it difficult for DPI tools to discern between encrypted and regular traffic (Kundur, 2003). The effectiveness and subtlety of this method are assessed, offering insights into its limitations and useful applications in different network environments.

The investigation of traffic morphing is another essential component of VPN obfuscation. By altering the properties of VPN traffic to resemble regular HTTP or HTTPS traffic, this method avoids detection by DPI systems. Traffic Morphing obfuscates by modifying packet sizes, timing, and other traffic attributes (Wright, 2009). The efficacy of this approach is evaluated, considering variables such as network performance and adaptability to various DPI technologies.

Another way of obfuscating VPN traffic is through the application of port and multi- protocol obfuscation. To avoid detection, Multi-Protocol Obfuscation involves switching between several VPN protocols and adjusting their settings. On the other hand, port obfuscation concentrates on using non-standard ports for VPN traffic, which can assist in getting around simple DPI systems that keep an eye on popular VPN ports. The usability of these techniques, along with their effects on security and network performance, is carefully examined.

More novel obfuscation techniques are also analysed like Randomized Packet Padding, Shadowsocks usage, and Tor integration with VPNs. By adding variance to VPN packets, randomized packet padding makes it more difficult for DPI systems to recognize patterns. An encrypted proxy called Shadowsocks is used to make VPN traffic look like HTTPS traffic (Clowwindy). Tor and VPNs work together to add an extra layer of encryption and obfuscation, though there may be a trade-off in connection speed. This thorough examination attempts to give readers a basic understanding of different VPN obfuscation methods while assessing their efficacy in a world where internet censorship and monitoring are becoming more commonplace.

The research is supervised by Mg.sc.comp. Jeļena Revzina.

References

1. El-Maghraby, R.T., Abd Elazim, N.M. and Bahaa-Eldin, A.M. (2017) A survey on deep packet inspection. *12th International Conference on Computer Engineering and Systems (ICCES).* IEEE. Available at: https://doi.org/10.1109/icces.2017.8275301.
2. Bock, K., Hughey, G., Qiang, X., Levin, D. (2019) Geneva. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*.

3. Kundur, Deepa & Ahsan, Kamran. (2003) *Practical internet steganography: data hiding in IP*.
4. Wright, C.V., Coull, S.E., & Monrose, F. (2009) Traffic Morphing: An efficient defense against statistical traffic analysis. *Network and Distributed System Security Symposium*.
5. Clowwindy, Madeye, and L. Max. Shadowsocks. [Online]. Available: http://www.shadowsocks.org/