CONTENTS

LIST OF USED ABBREVIATIONS

VPN - Virtual Private Network

INTRODUCTION

In an age when digital communications plays an vital role in modern socienty, ensuring the confidentiality and integrity of network communications has become crucial. The emergence of virtual private networks (VPNs) as a method of securing and privatizing digital communications on the public Internet has been a significant development in this direction. Because of the growing popularity of virtual private networks (VPNs), governmental agencies and corporate network administrators have increased their efforts to identify and block these encrypted connections. The result has been an arms race between organizations seeking to monitor, control, or censor Internet traffic and VPN service providers competing for the privacy of their users. The implementation of VPN obfuscation, a progressive collection of technologies capable of disguising VPN traffic as routine Internet operations, is central to this dispute. This obfuscation allows unrestricted access to the global digital environment.

VPNs were initially implemented as a simple way to establish secure network connections across the insecure infrastructure of the public Internet. However, the use of VPN technology eventually surpassed the scope of corporate applications. Private users are increasingly adopting virtual private networks (VPNs) for their own benefit, owing to the potential for enhanced privacy, circumvention of surveillance, circumvention of content geo-restrictions, and protection against cyber threats. In response, efforts to undermine the effectiveness of virtual private networks (VPNs) have increased. These initiatives include corporate firewall policies, government censorship initiatives such as China's Great Firewall, and anti-VPN measures implemented by content providers (El-Maghraby et al. 2017).

The proliferation of anti-VPN initiatives has sparked the emergence of a complex area of cybersecurity that uses data packet signatures to distinguish VPN connections. In response, the VPN obfuscation movement has developed a number of countermeasures. 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 & Ahsan 2003). The effectiveness and subtlety of this method are assessed, offering insights into its limitations and useful applications in different network environments.

Another way of obfuscating VPN traffic is through the application of port switching. To avoid detection, a VPN server is configured to use non-standard ports, which can assist in getting around simple DPI systems that keep an eye on popular VPN ports.

Another way of providing VPN obfuscation is the integration of encrypted proxy tunneling software like Shadowsocks and Stunnel. It can be used to make VPN traffic look like HTTPS traffic (Clowwindy et al. n.d.).

All of these methods, excluding port switching, bring with them a trade-off of in connection speed and throughput, though of varying degrees.

The thesis begins with a comprehensive overview of VPN technology and then describes the various use cases for VPNs as well as the fundamental principles underlying their operation. It then describes the techniques used to detect VPN traffic. The following is a comprehensive examination of various obfuscation methods and their adaptation to evolving VPN traffic detection strategies. The goal of this analysis is to provide insight into VPN detection methodologies and obfuscation techniques through experimentation, qualitative assessment, and technical proficiency in the process developing a methodology by which one can consider selecting an obfuscation method in real-life scenarios.

1. BACKGROUND

1.1. Deep packet inspection

1.2. OpenVPN identification

1.3. Packet manipulation

1.4. Protocol obfuscation

CONCLUSION

REFERENCES

1. Bock, K., Hughey, G., Qiang, X. & Levin, D. (2019), Geneva: Evolving censorship evasion strategies, pp. 2199–2214.

2. Clowwindy, Madeye & Max, L. (n.d.), 'Shadowsocks'.
   URL: *http://www.shadowsocks.org/*

3. El-Maghraby, R. T., Abd Elazim, N. M. & Bahaa-Eldin, A. M. (2017), A survey on deep packet inspection, *in* '2017 12th International Conference on Computer Engineering and Systems (ICCES)', pp. 188–197.

4. Kundur, D. & Ahsan, K. (2003), 'Practical internet steganography: Data hiding in ip'.