OPEN ACCESS Freely available online

Journal of Information Technology & Software Engineering

Perspective

Augmenting the Web-based Security Threats and Risk Identification with Virtual Private Network

Douglas Silva*

Department of Network and Infrastructure Management, University of Murcia, Murcia, Spain

DESCRIPTION

A Virtual Private Network (VPN) is a technology that has gained immense popularity over the last few years. Originally designed to facilitate secure remote access to corporate networks, VPNs have evolved into a mainstream solution for internet users seeking to protect their data, maintain privacy, and bypass geographic restrictions. At its core, a VPN is a network that extends a private network across a public network (usually the internet), allowing users to send and receive data as if their devices were directly connected to the private network. VPNs create a secure and encrypted tunnel for data transmission, protecting it from potential threats. When we connect to a VPN server, our device encrypts the data it sends and receives. This encrypted data is then sent through a secure connection to the VPN server, which acts as an intermediary between our device and the internet. The VPN server decrypts the data, sends it to the intended destination on the internet, receives the response, encrypts it, and sends it back to our device.

This process masks our IP address and encrypts our data, making it challenging for anyone, including hackers, ISPs, and advertisers, to monitor our online activities. Online privacy has become a paramount concern in today's digital landscape. VPNs provide an effective shield, preventing unauthorized access to our online data and maintaining our anonymity. VPN technology adds a layer of security to our online interactions. Public Wi-Fi networks, like those in coffee shops, airports, or hotels, are often vulnerable to cyber-attacks. A VPN encrypts our data, rendering it useless to potential attackers, by protecting our sensitive information from theft or eavesdropping. Content restrictions are a common hindrance to accessing websites and services. Some streaming platforms, for instance, limit access based on a user's geographic location. A VPN can help us to circumvent these restrictions by connecting to a server in a location where the content is available. This way, we can enjoy global content and access websites and services that might otherwise be unavailable in our region. In an era where remote work is increasingly prevalent, VPNs play a critical role in ensuring the security of sensitive business data. Employees can use VPNs to establish a secure connection to their corporate networks, protecting sensitive information from potential threats and ensuring that confidential company data remains confidential.

By masking our IP address and encrypting our internet traffic, VPNs make it incredibly difficult for anyone to trace our online activities back to users. This is a fundamental advantage for those who value their online privacy. These also add an extra layer of security, particularly when using public Wi-Fi networks. Whether a person is browsing the web, accessing the email, or conducting online banking transactions, the encryption provided by a VPN helps them to protect their sensitive data. In regions where internet censorship is a concern, a VPN can help users bypass government-imposed restrictions. Additionally, for travellers and those interested in accessing content from different countries, VPNs are invaluable in circumventing geo-blocks.

VPNs facilitate secure remote access to business networks, which has become increasingly important in the era of remote work. They allow employees to connect to company resources, access data securely, and collaborate without compromising sensitive business information. Many users turn to VPNs for safe and anonymous tormenting. By hiding their IP addresses, users can engage in Peer-To-Peer (P2P) file sharing without the risk of copyright infringement notices or legal consequences.

Not all VPN providers are created equal. Some offer robust security and privacy features, while others may log user data or have questionable business practices. It is essential to research and choose a reputable VPN provider with a clear privacy policy and a commitment to not storing user data. Using a VPN may result in a reduction in internet speed due to the encryption and routing of data through VPN servers. The extent of this slowdown depends on various factors, including the quality and location of the VPN server. It's crucial to choose a VPN service that minimizes this impact. Even though VPNs help us to protect our privacy, but they can also be used for illicit activities. Users must ensure they use VPNs responsibly and legally. Engaging in illegal activities while using a VPN does not guarantee absolute anonymity, as authorities can still trace illegal actions through other means. Free VPN services often come with limitations and

Correspondence to: Douglas Silva, Department of Network and Infrastructure Management, University of Murcia, Murcia, Spain, E-mail: sildoug@uom.es

Received: 21-Aug-2023, Manuscript No. JITSE-23-27745; **Editor assigned:** 24-Aug-2023, PreQC No. JITSE-23-27745 (PQ); **Reviewed:** 07-Sep-2023, QC No. JITSE-23-27745; **Revised:** 14-Sep-2023, Manuscript No. JITSE-23-27745 (R); **Published:** 21-Sep-2023, DOI: 10.35248/2165-7866.23.13.352

Citation: Silva D (2023) Augmenting the Web-based Security Threats and Risk Identification with Virtual Private Network. J Inform Tech Softw Eng. 13:352.

potential privacy risks, as they may monetize their services by selling user data. Paid VPN services typically offer better performance, security, and privacy features. Users should carefully consider their needs and the trade-offs when choosing between free and paid options.