Available online www.unicrossjournals.com

JOURNAL OF CONTEMPORARY RESEARCH (JOCRES)

RESEARCH ARTICLE VOL. 2 (1) ISSN:2814-2241

Date Accepted: 30th June, 2023

Pages 231 - 239

RETROSPECTION ON THE KEY CONCEPTS AND SHORTCOMINGS OF VIRTUAL PRIVATE NETWORKS

Fidelis I. Onah
ikonah80@yahoo.com
Department of Computer Science
Cross River University of Technology, Calabar, Nigeria

Abstract

With the globalization of businesses nowadays, many companies deploy Virtual Private Networks (VPNs), not only to maintain fast, secure and reliable communications throughout their branches, but also to reach out to the outside world. The dependence on VPNs for work-from-home, especially during the COVID-19 global pandemic, heightened the need for remote employees to stay "plugged in" to their organization's VPNs irrespective of the location of their offices. In this present study, some information about key concepts of VPNs is described. The definition, types, reasons for the use, and the operation of VPNs are highlighted. Then the most popular VPN solutions are presented. Finally, common vulnerabilities in VPN are mentioned. This section reveals that a growing number of network problems still threaten the continuity of mission-critical activities in organizations deploying VPNs. If compromised systems allow third parties to be harmed, a business may be subjected to criminal or legal proceeding. This could result to widespread, irreparable financial loss and damage to its reputation. IT admin awareness is very important for timely auditing, incident handling and risk mitigations. The need to strengthen the security of VPNs in today's heterogeneous environment is therefore recommended as an important area for future research.

Keywords: Virtual Private Network, security, vulnerability.

1.0 Background

In the world of today; many businesses think about global markets and logistics rather than dealing with local or regional concerns. Many companies have facilities spread out nationally across the country, or even around the world. To reach out to the outside world, company employees first used intranets, which are specialized "secure dial-up" services or a leased line separate from the Internet because of the need for security and reliability in connecting their remote offices. But leased lines do not support mobile workers well because the lines fail to extend to people's homes or their travel destinations. To log in to a dial-up intranet, a remote worker must call into a company's remote access server using either a toll-free number or a local number. The overhead of maintaining such a system internally is alarming. And if offices are very far apart, the cost can be prohibitively high. Thus, virtual private networks (VPNS) were created by many businesses or organizations to enable users to exchange private data in a fast, secure and reliable manner across all branches of the network. The goal of a VPN is to provide the organization with the same secure access to network resources as a dedicated, real-world connection, like leased line, but at a much lower cost.

Recently, VPN which was seen originally as invisible and impenetrable has been found to actually be the weakest link in an otherwise secure system (Roy Hills, 2005). While performing VPN security tests, NTA Monitor Ltd, based in Rochester, England alerted the IT world that "VPNs have remotely exploitable vulnerabilities". According to the test reports, "VPNs are far from being the impenetrable systems that many people believe them to be", because they "carry sensitive information over an insecure network". Attackers can, therefore, gain unauthorized access to the VPN, view or alter VPN traffic, or disrupt the VPN server for personal uses; causing financial and emotional damage to organizations that thought they were secure.

It is important to understand these common VPN technology issues to enable you make informed decision to implement a VPN connection, or even mount multiple convenient and secure solutions that minimizes the associated risks.

2.0 What is a Virtual Private Network?

A Virtual Private Network (VPN) is a private network that uses a public network (usually the Internet) to connect remote sites (offices) or individual users together in a secure and reliable manner (Nadir F. Mir, 2005; IBM Corporation, 2010).

Fig. 1 below shows one type of VPN called Virtual Private Dial-up Network (VPDN), or host-to-network VPN or remote-access VPN. It is a user-to-LAN (Local Area Network) connection that an organization uses to connect its users to a private network from various remote locations.

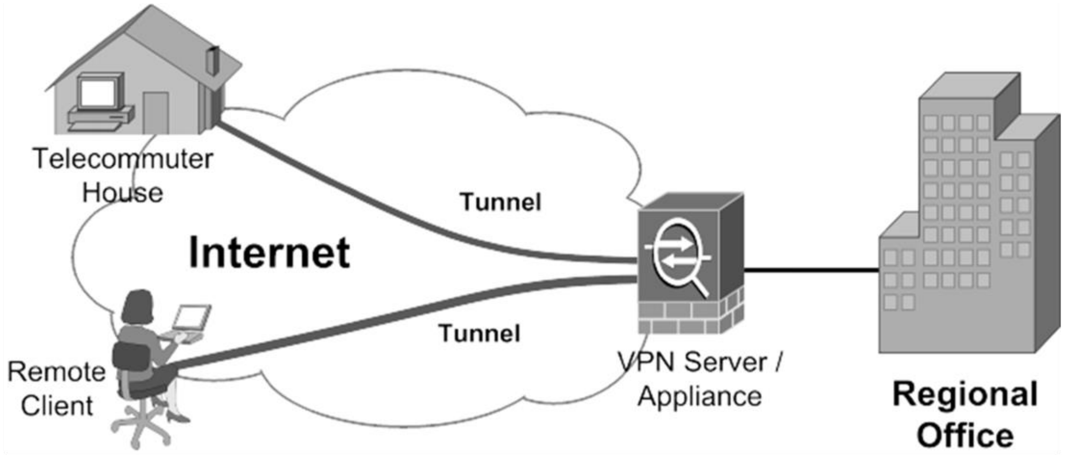


Fig. 1: Remote-access VPN (*Source: ResearchGate, 2013*)

Fig. 2 shows a VPN site-to-site network used to connect multiple fixed sites over a public network. Site-to-site VPN can further be classified as either intranets or extranets. A site-to-site VPN built between offices of the same company is said to be an intranet VPN, while a VPN built to connect the company to its partner, supplier or customer is referred to as an extranet VPN.

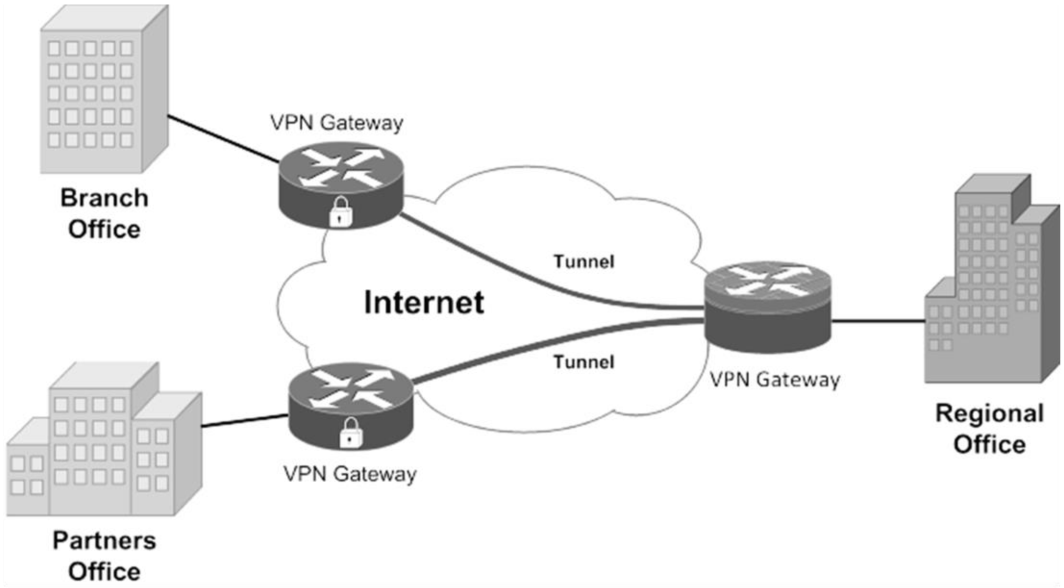


Fig. 2: Site-to-Site VPN (*Source: ResearchGate, 2013*)

A VPN works by using an encrypted virtual tunnel to send private data between a computer and the Internet. The tunnel encapsulates packets and moves them from one protocol to another at the same or higher layer over the public network (Fig, 3). Tunneling ensures that such sensitive data transported between the two end points of its connection (called tunnel interfaces) reach their intended destination safely (ResearchGate, 2013; CISCO, 2008).

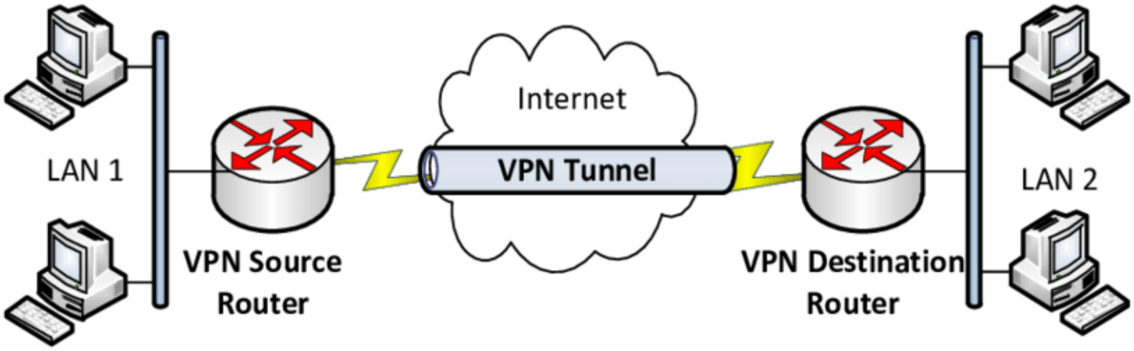


Fig. 3: VPN Tunneling structure (CISCO, 2008)

To protect the confidentiality, integrity and authentication of network traffic, VPNs use tunneling as well as a number of cryptographic algorithms and protocols. If someone intercepts encrypted packets sent in the VPN tunnel, he would only see encrypted data that is unreadable (Rick Lehtimen, 2006).

When a remote node (client) logs into the company VPN services, then the client authenticates with the VPN server and applies an encrypted protocol to the entire Internet data. Once the connection has been established, the remote client can communicate with the company network just as securely over the public network as if it resided on the internal LAN itself (CISCO, 2008; Paul Ferguson and Geoff Huston, 1998).

Tunneling has amazing implications for VPNs. For example, you can place a packet that uses a protocol not supported on the Internet (such as NetBeui) inside an IP packet and send it safely over the Internet. Alternatively, you could put a packet that uses a private (non-routable) IP address inside a packet that uses a globally unique IP address to extend a private network over the Internet.

Appropriate networking software and hardware are required on the client's local network and computers to use a VPN. Examples include: desktop software client for each remote user, dedicated hardware such as a VPN concentrator, or secure PIX (Private Internet Exchange) firewall, dedicated VPN server for dial-up services, NAS (Network access server) used by service providers for remote-user VPN access, VPN network and policy-management center, user authentication, Address Management, data encryption, key management and multi-protocol support.

It is important to note that the physical distance between the client and server as well as the extra storage space for the heavier encryption algorithms may reduce performance of the network. This leaves less computational resources (CPU power) for the network (Sanel Habibovic, 2019).

In Remote-Access VPN, client software is used on the user's device and the user needs to initiate the VPN tunnel setup. But in Site-to-Site VPN, no client software is needed on the user's device and the user does not need to initiate the VPN tunnel setup in. Another key difference is that the user's device communicates with the VPN gateway using a VPN tunnel in Remote-Access VPN. But the VPN gateway from one LAN communicates with the VPN gateway of another LAN and creates secure VPN tunnel in Site-to-Site VPN (Amrita Mitra, 2020).

3.0 Benefits and Drawbacks of VPNS

3.1 Benefits

The benefits of creating a VPN to an organization include:

1. Providing extended geographical communication – in leased lines, the cost increases in proportion to the distances involved. In VPN, the geographical locations of each office matter little.
2. Cost savings – A VPN saves operational cost by eliminating expensive long-distance leased lines, thereby reducing long-distance telephone charges. Organizations outsource the cost of maintaining servers from professional third-party service providers.
3. Internet VPN offers superior reach, quality of service and ease of use.
4. Providing enhanced network management with simplified local area networks – Network tunneling and Remote Authentication Dial-in Service (RADIUS) technologies greatly reduce problems with security and user account management.
5. Network scalability – The main benefit of using a VPN is scalability (high availability) with a reasonable cost. A VPN can grow to accommodate more users and different locations much easier than a leased line.
6. Providing improved productivity and globalization – With a VPN service, employees can work remotely; focusing on the task and not on their security. Non-members are excluded from the network; so employees are protected from curios eyes and threats. Hence, resources are conserved, and costly, time-consuming

paper works are eliminated (Fortinet, Inc, 2023).

3.2 Drawbacks

Despite their popularity, VPNs are not perfect, and organizations should consider the following deficiencies when deploying and using VPNs in their operations:

1. VPNs require detailed understanding of network security issues and careful installation/configuration procedures to ensure sufficient protection on a public network like the Internet.
2. The reliability and performance of an Internet-based VPN is not under an organization's direct control. Instead, the solution relies on an ISP and their quality of service.
3. Historically, VPN products and solutions from different vendors have not always been compatible due to issues with VPN technology standards. Attempting to mix and match equipment may cause technical problems, and using equipment from one provider may not give the much needed low-cost (Gavin Philips, 2020; Rama Bansode and Anup Girdhar, 2021).

4.0 Different VPN Solutions

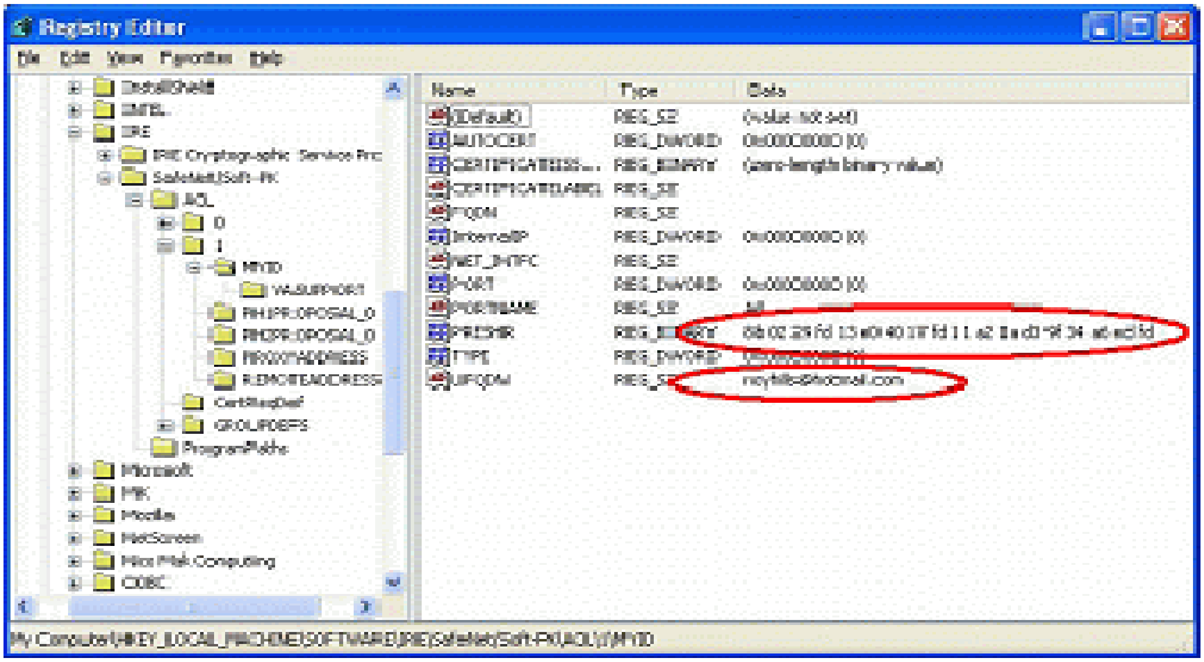
There are many VPN solutions on the market. The most supported one is Open VPN followed by IPSec. A new solution named WireGuard was released in 2018 to replace these two VPN solutions. The key features of 6 main VPN protocols are summarized as follows:

1. **OpenVPN:** This is an open source VPN protocol accessible to anyone who wishes to review the code. It offers the strongest encryption with no major vulnerabilities. It supports both TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) but defaults at UDP, which is faster but does not perform error correction as TCP. OpenVPN is fully functional on Windows, MacOS and Linux.
2. **IPSec with L2TP:** Internet Security Protocol (IPSec) is a protocol suite with good speeds. Tunneling for VPN process is done by Layer 2 Tunneling Protocol (L2TP). However, it is easily blocked due to its reliance on a single port. It is also complex and very process heavy due to the encryption and decryption involved. It is available on windows, MacOS and Linux as well.
3. **SSTP (Secure Socket Tunneling Protocol):** This is solely owned by Microsoft. It is difficult to block and detect; hence offers good security.
4. **IKEv2 (Internet Key Exchange version 2):** This is a fast and mobile-friendly protocol with several open-source implementations. Both IKEv2 and L2TP are built into IPSec.
5. **PPTP (Point-to-Point Tunneling Protocol):** This is a fast and widely supported protocol, but full of security holes which makes it not secure enough today. It is only used for streaming and basic web browsing.
6. **WireGuard:** This is the newest VPN protocol which claims to be faster, simpler and less complex than other VPN solutions. It is open-source with growing support among VPN providers (Gavin Philips, 2020).

5.0 Security Vulnerabilities in VPNs and Mitigations

VPN was originally intended to be unbreakable and thus expected to keep information secure without any form of exploitation by hackers. This should allow users to transfer sensitive data without using additional encryption, and to use protocols that transmit authentication credentials in the clear. This trust was massively broken during COVID-19 global pandemic. During this lock-down period, enterprises were more dependent on the VPN for Work-from-Home, where remote employees can connect as a VPN client to the corporate infrastructure and access internal network services (Rama Bansode and Anup Girdhar, 2021). Exploitation of weak protocols and non-secure Internet connections by malicious hackers was on the increase; causing data breaches at major companies.

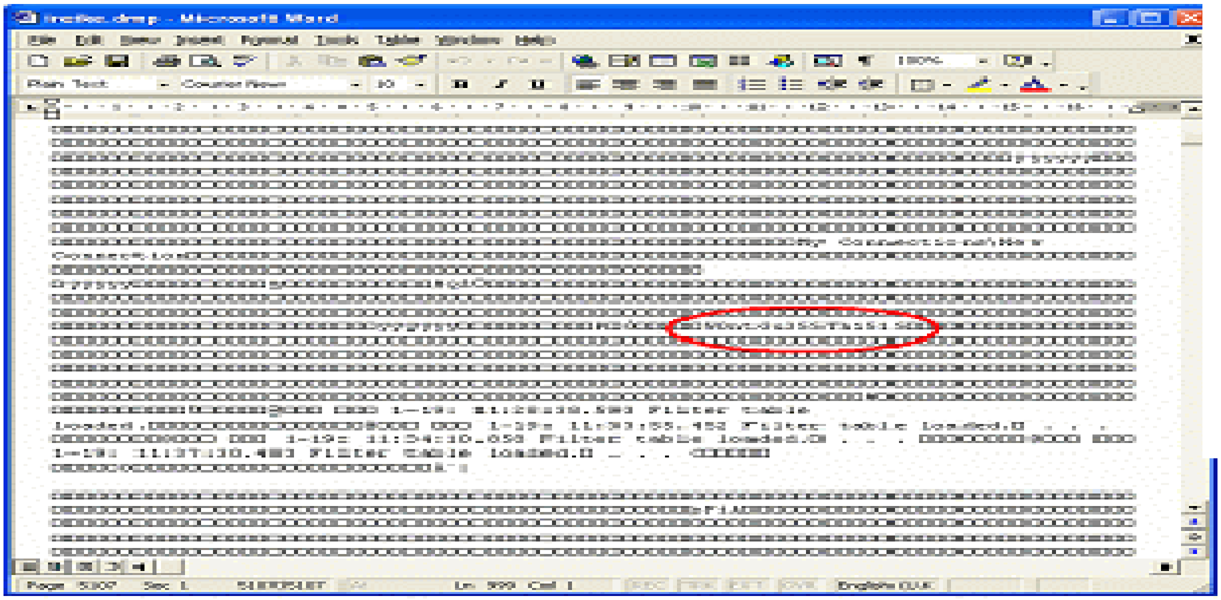
Username and password cracking are new forms of threats and attack being discovered. Easy-to-guess VPN username and password combination expose your systems and data to cyber criminals. It could be used to obtain a hash from the VPN server and this can be exploited to mount an off-line attack to crack the associated passwords (NTA Monitor Ltd, 2022).



Name	Type	Data
(Default)	REG_SZ	(value not set)
AUTOCERT	REG_DWORD	0x00000000 (0)
CERTIFICATEISS...	REG_BINARY	(zero-length binary value)
CERTIFICATELABEL	REG_SZ	
FQDN	REG_SZ	
InternalIP	REG_DWORD	0x00000000 (0)
NET_IHTFC	REG_SZ	
PORT	REG_DWORD	0x00000000 (0)
PORTNAME	REG_SZ	All
PRESHR	REG_BINARY	0b 02 29 fd 13 a0 40 1f fd 11 a2 8a d3 9f 34 ab ac fd
TYPE	REG_DWORD	[illegible]
UFQDN	REG_SZ	[illegible]@hotmail.com

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\IRE\SafeNet\Soft-PK\ACL\1\MYID

Fig.4: VPN Client Process Memory Dump showing Plain Text Password (*Source: NTA Monitor Ltd*)


[illegible].dmp - Microsoft Word
File Edit View Insert Format Tools Table Window Help
Plain Text
Courier New
10
100%
Page 5307 Sec 1
Ln 599 Col 1
REC TRK EXT OVR
English (U.K)

```
1-19: 11:28:38.580 Filter table
loaded.  1-19: 11:32:55.452 Filter table loaded.
 1-19: 11:34:10.050 Filter table loaded.
1-19: 11:37:30.480 Filter table loaded.
```

Fig.5: Username and Obfuscated Password stored in Registry (*Source: NTA Monitor Ltd*)

Other common threats and attacks on weak VPNs include: repeated login attempts (brute-force attacks), cyber-attacks on internal/external web sites, injecting virus or malicious code into the application, Domain Name Server (DNS) hijacking, spoofing attacks, etc. Once the attacker has breached the network through a compromised device, the entire network can be brought down.

One easy way hackers enter a network is through a third-party connection. Sometimes, third-party vendors follow a number of VPN practices that create opportunities for hackers to entire the network e.g. sharing credentials with co-workers, or re-using weak passwords from personal accounts that are easily exploited. The more servers, applications, and network equipment vendors can access, the more a business is exposed to risks. So, if your business has many third-party vendors, and each of them has full access to your network, a hacker now has multiple potential routes to break into and exploit your network using VPN traffic. Unfortunately, VPNs typically provide little or no audit records; no centralized remote management and no partial access to required resources. So, you cannot monitor and record the actions of every third-party vendor using the VPN.

Another important flaw in VPNs is the exposure of protocols due to poor configuration. Default configurations are often chosen for ease-of-use rather than security. Even though attention is often focused on the cryptographic algorithms, real-World VPN security problems are generally caused by poor configuration or bad implementation. VPN implementations have not taken account of not leaking valid usernames, and locking out accounts after a number of failed attempts as is the case with operating system login authentication for decades. End-users, on their own part, do not even understand potentially insecure configuration options. For instance, most implementations will not warn you of the know problems inherent in choosing pre-shared key authentication with IKE (Internet Key Exchange) Aggressive Mode (Roy Hills, 2005; Fortinet Inc., 2023; Matthew Schwartz, 2005).

For the purpose of mitigations, admin can enforce clear, written policy about what constitutes acceptable Internet usage while connected to the VPN; e.g. using the strongest possible authentication, encryption and password policies; limiting VPN access to those with a valid business reason when necessary; using antivirus, antispam and personal firewall protection to prevent the spread of infection throughout the network; etc. But in addition to this, there is urgent need for advanced security solutions in an ever-evolving battle against fraud and malicious intent. This is required in order to deploy, monitor and manage all of your connections from a single place. Without easy, centralized access to all the historical information on a connection (user, applications accessed, connection time, the reason for access, etc), it is impossible to prove who or what created an issue when a breach or mistake occur due to a third-party vendor. The probability of an attack can be reduced by using a checklist to assess risks and the vulnerabilities of third-parties' remote access points (Joes Burleson-David, 2022; Softchoice, 2018; Martin Heller, 2006).

A well-designed VPN uses several methods for keeping your connection and data secure, such as firewalls, encryption systems, Internet protocol security (IPSec) and AA (Authentication, Authorization and Accounting) servers.

The implementation of these security technologies is an important goal for modern security solutions. However, maintaining network security requires constant vigilance, and maintaining VPN security even more vigilance.

6.0 Concluding remarks

This research paper was aimed at reviewing the key concepts and shortcomings of VPNs. VPN technology is designed to address issues surrounding the current business trend toward increased telecommuting and widely distributed global operations. VPNs allow users or corporations to connect to remote servers, branch offices, or to other companies over a public network. An organization using a VPN uses a service provider's IP network, builds a private network and runs its own traffic.

This paper has also looked into the benefits and draw backs of VPNs. The most popular VPN solutions and common security vulnerabilities in VPNs are also presented. Finally, the paper noted that today's VPNs are at high risk. The need to strengthen the security of VPNs in today's heterogeneous environment is, therefore, highlighted as an important area for future research. This should provide multiple convenient and secure ways to authenticate all of your users, analyze their behaviour and context, and manage which systems and resources they are authorized to access. Vendors may, for example, be given access only to the resources they require to get their job done and not to your entire network.

In today's rapidly growing business environment, this research is a good eye-opener for employees, contractors, vendors, customers, audit teams, partners, and indeed all stakeholders in the VPN enterprise.

References

Amrita Mitra (Jul 1, 2020). *Remote-Access VPN vs. Site-to-Site VPN*. Accessed from https://www.Fortinet.com on 28/05/2023.

CISCO (October 13, 2008). *How Virtual Private Networks Work*. Cisco Systems, Inc.

Fortinet, Inc (2023). *Benefits of a VPN: What are the advantages of using a VPN?* Accessed from http://www.fortinet.com.

Fortinet Inc (2023). *VPN Security: How Secure Is It & Do you Need One?* Accessed from https://www.fortinet.com/resources/cyberglossary/are-vpns-safe on 22/06/2022.

Gavin Philips (Sep. 03, 2020). *The 6 Major VPN Protocols Explained*. Retrieved from https://www.makeuseof.com on 21//06/2022.

IBM Corporation (2010). *Virtual Private Networking*. North Castle Drive, Armonk, NY 10504-1758, U.S.A.

Joes Burleson-David (June 02, 2022). *Common VPN Security Risks: The Not-So-Good, The Bad, and the Ugly*. Retrieved from https://www.securelink.com on 21/06/2022.

Matthew Schwartz (02/23/2005). *Unraveling common VPN Flaws*. ESJ Enterprise Systems Journal. Retrieved from https://esj.com on 23/06/2022.

Martin Heller (Oct, 2006). *10 Tips to secure client VPNs*. IDG Communications, Inc. Retrieved from https://www.computerworld.com o 29/06/2022.

Nader F. Mir (2005), *Computer and Communication Networks.* Second Edition. Pearson Education Inc. retrieved from http://ptgmedia.pearsoncmg.com 0n 22/06/2022

NTA Monitor Ltd (2022). *VPNs are attractive targets to hackers*. Rochester, England. Retrieved from https://www.nta-monitor.com/ on 22/06/2022.

Paul Ferguson and Geoff Huston (1998). *What is a VPN?* Retrieved from https://www.semanticscholar.org on 22/06/2022.

Rama Bansode and Anup Girdhar (2021). *Common Vulnerabilities Exposed in VPN – A Survey*. J. Phys. Conf. Ser 1714 012045, Retrieved from https://www.copscience.iop.org on 22/06/2022.

ResearchGate (2013). *Research Gate Remote-Access VPN-fig2*. Accessed from: https://www.researchgate.net/figure/Remote-access-VPN-1_fig2_256843676

ResearchGate (2013). *Site-to-Site VPN-fig1*. Accessed from: https://www.researchgate.net/figure/Site-to-Site-VPN-1_fig1_256843676

ResearchGate (2013). *VPN Tunneling structure*. Retrieved from https://www.researchgate.net/figure/VPN-Tunneling-structure_fig1_320536838c on 28/05/2023.

Rick Lehtinen (June 2006), *Computer Security Basic*, O'reilly, 2nd Edition.

Roy Hills (January 2005). *Common VPN Security Flaws*, NTA Monitor Ltd; Rochester, England. Retrieved from https://www.doc.lagout.org on 22/06/2022.

Sanel Habibovic (2019). *An Analysis of the Performance in State-of-the-Art Virtual Private Network Solutions in Unreliable Network Conditions*. Bachelor Degree Project in Information Technology, University of Skovde.

Softchoice (12 Mar 2018). *4 Tips for Strengthening the Security of Your VPN Access*. Retrieved from https://www.m.softchoice.com on 22/06/2022.