# RECENT DEVELOPMENT AND TRENDS IN VIRTUAL PRIVATE NETWORKS: SECURE REMOTE CONNECTIVITY FOR EMPLOYEES

Yin L. Loo and Young B. Choi
Regent University, USA

## ABSTRACT

Remote connectivity is necessary for businesses. Virtual Private Network provides an efficient, confidential, and cryptographically secure way to achieve remote connectivity. This paper looks at the need for remote connectivity and how it is beneficial to businesses. This paper also serves as a starting point to understanding the virtual private network and what makes it secure. Additionally, it also discusses how client-to-site VPN relates to teleworking, how it works, and the essential activities of encapsulation, encryption, and authentication. Finally, it presents some trends in remote connectivity.

*Keywords:* Diameter, IPSec, Kerberos, L2TP, OpenVPN, PPTP, RADIUS, Remote Connectivity, SSL VPN, Virtual Private Networks

## Introduction

In an increasingly connected business world, there is a compelling need for secure remote connections. Executives and employees require constant access to the organization's network, often from insecure locations such as client or customer offices, homes, cafes, fast-food joints, hotels, and airports. The Internet is the reason that these locations are insecure; it is by its nature – public, open and unregulated. Combining the growth and popularity of the Internet and the use of cryptography, Virtual Private Networks (VPN) becomes a viable solution to establish a private communication channel with an organization's internal network. This paper discusses the VPN as a secure and cryptographic form of remote connection for employees.

## The Need for Remote Connections

Modern-day businesses are competitive. Executives and employees often need to remain connected to the organization's network. The ability to respond quickly, usually at any time and space, can make or break a business. Teleworking or telecommuting is the ability to use information technology to perform work remotely (Chiru, 2017, p. 222). The ability to work remotely is done through a remote connection such as a VPN. The benefits can be seen on several fronts.

On the productivity front, such a work arrangement makes an organization more responsive and productive. For example, employees can continue working even during inclement weather conditions (Chiru, 2017, p. 223). In a randomized and controlled trial, a Chinese call center found a 13% increase in efficiency from those who worked from home (Spark, 2017, p. 1). On the human resource front, teleworking allows the organization to employ and/or retain exceptional talents who live a distance away from the office location (Chiru, 2017, p. 223). On the financial front, teleworking is a reduction of personnel and utility costs (Spark, 2017, p. 1). As a result, an organization could consider a smaller office. On the environmental front, a smaller office is a smaller pollution footprint (Chiru, 2017, p. 223). On the employees' front, flexible working hours mean lower transportation costs and less time spent on traveling (Chiru, 2017, p. 223). In the same call center trial, employee satisfaction had shown a noticeable increase (Spark, 2017, p. 1). While the notion for teleworking is favorable and positive, how can an organization maintain confidentiality and integrity of information with remote connections coming in through the Internet?

## Remote Connections and VPNs

Networks are seldom designed to be isolated. Initially, networks were connected by leased lines and data channels. Security came in the form of fixed lines and service agreements (Whitman & Mattord, 2016, p. 342). Users could connect to networks using a dial-up service and gain access with just a user id and password (Whitman & Mattord, 2016, pp. 342-343). However, dial-up connections are not secure. Using a war dialer, an attacker could easily know what the modem numbers are and use the identified modem connections to hack into the network (Whitman & Mattord, 2016, pp. 342-343).

With the explosion of the high-speed Internet, secure forms of connection and communication, such as those that use cryptography and authentication systems, are required. A VPN uses the data communication capability of an unsecured and public network, i.e., the Internet, to establish a private and secure network connection between systems (Whitman & Mattord, 2016, p. 346). As such, it fulfills the confidentiality, integrity, and availability model of information systems. The specific type of VPNs that provide remote site access is called client-to-site VPNs (Whitman, Mattord, & Green, 2012, p. 301) and it functions like cost-effective private leased lines (Whitman, Mattord, & Green, 2012, p. 295). Essentially, data are encapsulated and encrypted before transmission and authentication systems are used to ensure that only authorized users can access the network (Whitman, Mattord, & Green, 2012, p. 295).

## Encapsulation and Encryption

The process of transporting data across the Internet between the VPN client and the VPN server is known as tunneling. Encapsulation hides the original packet (that contains the original source and destination) within a packet that contains the source and destination of the gateway to the VPN. Therefore, encapsulation gives data the ability to travel across the Internet while achieving a certain level of anonymity. Encapsulation, by itself, is not enough because the Internet is a public network and is susceptible packet sniffing which is a way monitoring and capturing data traffic on a network for analysis (Varanasi & Swathi, 2016, p. 406). With the right technical skills, the data could be easily understood. Therefore, encryption is necessary to protect the confidentiality and integrity of the data.

Internet Protocol Security (IPSec) is a standard and a suite of protocols that provides security to Internet communications at the IP layer (Krishnan & Frankel, 2011, p. 4). In IPSec transport mode, the client encrypts only the data part of the packets and not the source and destination headers (Whitman, Mattord, & Green, 2012, p. 299). As such, special servers and tunneling software are not required and data can be transmitted anywhere, which makes transport mode suitable for teleworking.

## Authentication

The last essential activity of a VPN is authentication. The authentication process confirms the identity of a user by verifying one or more of the following: something known, something owned, some physical attribute, and something done. (Whitman, Mattord, & Green, 2012, p. 73). Multiple layers of security deter attackers from going all the way. Two-Factor Authentication (2FA) is a combination of something known, e.g. a set of credentials, something owned, e.g., a certificate, some physical attribute, or something done.

## Recent Trends

This section surveys the issues surrounding the adoption of telecommuting workforce, the feasibility of a multi-phase encryption algorithm to improve security, and an authentication concept known as comply-to-connect (C2C). It is said that telework does not create management problems, it merely reveals them (Spark, 2017, p. 2). There are a couple of reasons why an organization might be hesitant to adopt a teleworking culture. For one, senior management is reluctant to accept teleworking because it does not fit with their previous working experience

(Spark, 2017, p. 3). For another, managers seemed to think that employees who are not watched are not working (Spark, 2017, p. 2). Therefore, the issue of trust is called into question. However, performance can be measured by outcomes instead of effort (which is usually measured by the number of hours put in) by focusing on outputs, setting boundaries, emphasizing effective communication, embracing diversity, valuing working intelligently, and growing trust in team members (Spark, 2017, pp. 2-3). The result could be an effective business strategy that fosters creativity and productivity.

Currently, VPNs are commonly implemented with a common encryption algorithm known as Data Encryption Standards (DES) (Singh & Gupta, 2016, p. 2). Although DES is highly secure and takes years for a supercomputer to decipher a single pack, computing powers of machines are advancing (Singh & Gupta, 2016, p. 2). Forward-thinking suggests that an even more secure option be considered for the future. Multi-phase encryption algorithm provides a complex and robust mechanism to secure data inside a packet by performing encryption using different encryption algorithms on multiple levels and multiple times (Singh & Gupta, 2016, p. 2). It is a technique will not disrupt current VPN operations or tunneling process because it is applied to the user data contained in the encapsulation (Singh & Gupta, 2016, p. 2). To increase the speed of connection, administrators can opt-out of any encryption algorithm used in various stages of tunneling (Singh & Gupta, 2016, p. 4). This algorithm may see possible adoption from industries that deal with sensitive data such as e-commerce, finance, healthcare, legal, and military (Singh & Gupta, 2016, p. 2).

One of the largest threats to a network is end-points (Gillespie, 2017). Comply-to-Connect (C2C) is a concept and architecture from Cisco (Cisco, n.d.). In this architecture, before network access is granted, the system profiles the identity of the user and the device, collecting information such as who owns the device, what type of device it is (printer, smartphone, laptop, etc.), manufacturer information, and details of the operating system (Cisco, n.d.). For example, a device that does not have the latest operating system patches or does not have an updated anti-virus software installed cannot access the network (Cisco, n.d.). C2C is based on the concept of proactivity and complete visibility (Gillespie, 2017). It provides the ability to discover, classify, and perform real-time risk assessments on end-point devices (Gillespie, 2017). Some of the positive outcomes, noted by Gillespie, include an improved resilience to incidents, reduction in the probability of an outage caused by a cyber event, and an overall increased in the number of compliant-devices (2017).

## Conclusion

As businesses continue to be competitive, organization and employees are realizing the value of teleworking or telecommuting. There is a need for a solution that can support a mobile workforce in an efficient and secure manner. Virtual Private Networks (VPN) is a form of remote connection that allows employees to connect to their organization by creating an encapsulated and encrypted tunnel across the Internet at any time or location. The integrity of the data packets is protected, and their contents are hidden. VPNs could be better understood by breaking down and explaining the essential activities of encapsulation, encryption, and authentication. To achieve a greater adoption of teleworking, senior management of organizations must change their previous mindset and embrace a flexible and productive workforce that is measured on outcomes. As computing powers continue to advance, new ways to improve security, such as the multi-phase encryption algorithm, must be considered and researched. Overall, this paper serves as a good starting point to understand how the needs of modern businesses drive the need for remote connections, what a virtual private network is, what makes it secure, and what its future looks like.

## References

Chiru, C. (2017). Teleworking: Evolution and Trends in USA, EU and Romania. *Economics, Management and Financial Markets; Woodside*, *12*(2), 222–229.

Cisco. (n.d.). Understanding Comply-to-Connect (C2C) and U.S. Department of Defense Requirements. Retrieved from https://www.cisco.com/c/dam/en_us/solutions/industries/docs/fed-dod-comply2connect.pdf

Gillespie, T. (2017, March). *Comply to Connect (C2C)*. Webinar. Retrieved from https://www.csiac.org/wp-content/uploads/2017/03/comply-to-connect-agnostic-webinar.pdf

Krishnan, S., & Frankel, S. (2011, February). IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap. Retrieved February 26, 2018, from https://tools.ietf.org/html/rfc6071

Palo Alto Networks. (n.d.). Remote Access VPN with Two-Factor Authentication. Retrieved March 1, 2018, from https://www.paloaltonetworks.com/documentation/71/globalprotect/globalprotect-admin-guide/globalprotect-quick-configs/remote-access-vpn-with-two-factor-authentication

Singh, K. K. V. V., & Gupta, H. (2016). A New Approach for the Security of VPN. In *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies - ICTCS '16* (pp. 1–5). Udaipur, India: ACM Press. https://doi.org/10.1145/2905055.2905219

Spark, R. (2017). Accessibility to Work from Home for the Disabled: The Need for a Shift in Management Style. In *Proceedings of the 14th Web for All Conference on The Future of Accessible Work - W4A '17* (pp. 1–4). Perth, Western Australia, Australia: ACM Press. https://doi.org/10.1145/3058555.3058577

Varanasi, A., & Swathi, P. (2016). Comparative Study of Packet Sniffing Tools for HTTP Network Monitoring and Analyzing. *International Journal of Science, Engineering and Computer Technology; Hisar*, *6*(12), 406–409.

Whitman, M. E., & Mattord, H. J. (2016). *Principles of Information Security* (Fifth edition). Boston, MA: Cengage Learning.

Whitman, M. E., Mattord, H. J., & Green, A. (2012). *Guide to firewalls and VPNs* (3rd ed). Boston, MA: Course Technology, Cengage Learning.