International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 5, ISSN No. 2455-2143, Pages 152-157
Published Online September 2020 in IJEAST (http://www.ijeast.com)

IMPACT OF VPN TECHNOLOGY ON IT INDUSTRY DURING COVID-19 PANDEMIC

Abhijith M S
ME Computer Science and Engineering
Department of Computer Science and Engineering
Erode Sengunthar Engineering College
Erode, Tamilnadu

K.Senthilvadivu
Assistant Professor
Department of Computer Science and Engineering
Erode Sengunthar Engineering College
Erode, Tamilnadu

Abstract - **COVID-19 or Coronavirus is the virus which is now being affected globally. Since the end of 2019, it has been spreading rapidly across the world. Since then, most of the countries around the world were went into lockdown and proper measures like social distancing have been taken in an attempt to reduce the spread of the disease. The disease has been also declared as a global pandemic by the world health organization. COVID-19 has a huge impact on every industry. To overcome the effects of COVID-19 and to ensure employee safety and also to ensure business continuity, most of the IT companies have been moved to remote working. Virtual Private Network (VPN) is one of the main tools which is being used by companies to permit secure access to corporate resources while employees are working from home. This paper talks about various VPN technologies, VPN providers and how IT companies used them effectively during the pandemic.**

Keywords - COVID-19, Coronavirus, working from home, remote working, IT industry, VPN technologies, Impact

I. COVID-19

Coronaviruses are a family of viruses which cause illness in both animals and humans. Coronaviruses cause respiratory infections from common cold to severe diseases such as Severe Acute Respiratory Syndrome (SARS) and Middle East Respiratory Syndrome (MERS). COVID-19 disease is caused by the most recently discovered Coronavirus. The virus outbreak started in Wuhan, China, in December 2019. Before that this new virus was unknown. COVID-19 is now a global pandemic affecting many countries throughout the world.

The common symptoms of COVID-19 disease are dry cough, fever and tiredness. Other symptoms like headache, conjunctivitis, pains, nasal congestion, sore throat, diarrhea, loss of taste, loss of smell, rashes on skin, discoloration of fingers, discoloration of toes, etc. are less common. These symptoms are mild and begin gradually. Some infected people only have very mild symptoms.

80% of infected people recover from the disease without any hospital treatment. Around 20% of people who are affected with COVID-19 becomes seriously ill and may develop difficulty in breathing. Usually people with underlying medical problems like high blood pressure, heart and lung problems, diabetes, or cancer, and also older people are at higher risk of developing serious illness. However, anyone may catch COVID-19 and its possible to become seriously ill.

People can catch COVID-19 disease from others who are already infected. It spreads primarily from person to person through small droplets from the mouth or nose which are expelled when an infected person coughs, sneezes, or speaks. These droplets are comparatively heavy and do not travel far and quickly reach to the ground. People can catch the disease if they breathe in these droplets from a person infected with COVID-19. It is also possible that these droplets land on objects and surfaces around the infected person such as tables, doorknobs and handrails. So, people can also become infected by coming in contact with these objects or surfaces, and then touching their face. Most of the people with COVID-19 experience only mild symptoms. This is particularly true in the early stages of COVID-19 disease. However, it is possible to catch the disease from someone who has just a mild cough and does not feel ill. Certain reports have indicated that people with no symptoms at all can also transmit the virus. It is not yet fully known how often it happens.

II. COVID-19 & WORKPLACE

COVID-19 mainly spreads through respiratory droplets or contact with contaminated surfaces. Virus exposure can occur at the workplace, while travelling to work, during work related travel to a location with community transmission. The risk of exposure to the virus in the workplace depends on the likelihood of coming within close proximity of others, in having frequent physical contact with people who may be infected with the virus, and through contact with contaminated surfaces and objects. Jobs without close contact with the general public can be regarded as of low exposure risk. Workers in low exposure risk group have only minimal occupational contact with the public and co-workers. Examples of such jobs may include remote workers and workers providing teleservices. Jobs with close contact with the general public are of medium exposure risk. This risk level may apply to workers who have frequent and close contact with a lot of people (fruit/vegetable markets, bus stands, railway station, etc.), or tasks that require close contact between colleagues. This may also include contact with people returning from areas with local community transmission. Examples of such jobs may include workers in retail, home deliveries, construction, police force and public transport. Jobs with close contact with people who may be more likely to have the virus are of high exposure risk. Examples include transporting people known/suspected to have the virus without separation between the driver and the passenger, providing domestic services for people with the virus, and having contact with the deceased who were known/suspected of having the virus at the time of their death. Jobs that come under this category include domestic workers, social workers, personal transport and home delivery providers and home repair technicians who have to provide services in the homes of people with COVID-19.

III. IMPACAT ON IT SECTOR

IT and IT enabled services have been one of the key driving forces fueling economic growth of the world. The IT sector includes IT services, software, engineering services, hardware and business process management. The coronavirus crisis has taken the Industry by surprise and it is probably one of the biggest ever challenge faced by IT sector. The speed with which this crisis has hit the information technology industry is definitely unprecedented and it has fatally tested disaster recovery strategies and business continuity plans.

In the information technology and software industries, employees usually have to share the same office space with multiple employees and teams. Usually, they interact physically in internal meetings and even attend client meetings as and when required. If an employee is diagnosed with coronavirus, he/she can affect others when they cough and sneeze. The widespread nature of the virus is causing challenges for IT companies, and many of them have started evaluating its impact on the business operations. But, as their customers scrambled for contingency plans, IT companies have done a wonderful job by quickly enabling work from home for most of their employees. This timely action not only ensured business continuity for majority of customers but also ensured safety for employees.

While parts shortage and unpredictability of supply chains were dragging down the technology industry as a whole, software is definitely a growth catalyst. Companies who already enabled remote working technologies are now seeing increased demand as businesses are on the way to increase their remote working capabilities. Security softwares' are witnessing huge benefits from a growing remote workforce. Spending on security software is going to increase as companies race to secure their endpoints, VPNs, cloud hosted tools, etc. Increase in the use of teleconferencing software as more technology companies encourage employees to telecommute will have benefits for companies that have such technologies already in place. For example, Zoom meetings, Cisco WebEx, Microsoft Teams, etc. Also, the need for faster access to data will increase the focus on communications and network, leading to speeding up 5G network deployments and adoption of 5G equipment.

IV. REMOTE WORKING

As coronavirus cases are increasing around the world, many leading tech giants are taking precautionary measures to ensure the safety of their employees. To control the spread of COVID-19, tech companies are allowing their employees to work from home and also revamping their remote working policies. Irrespective of the size and services, remote working is a growing trend in the IT industry. Also, it is poised to be the best solution to drive more productivity and ensure safety in the current scenario. The COVID-19 pandemic will definitely create a permanent increase in remote working even after the crisis. Most people currently working remotely believe that doing so does not affect their productivity. Even before the pandemic, there was a gradual increase in the number of people who choose to work from home, and so many enterprises have already moved to more flexible workplace models. However, the current situation is serving as some sort of remote working experiment, which demonstrates what works and what does not. COVID-19 pandemic accelerated the trend towards more flexible workplace models, and it has a positive effect on society as a whole, since it is giving people more flexibility in terms of location and time management. It is also lowering the burden on our roads and even rail infrastructure. It is possible that for some people working remotely can be more productive than working in an office. Depending on the job, some people can get things done more efficiently when they are not in a noisy office.

Millions of employees are currently working from home across the world. businesses are trying to keep up with their commitments to customers, as employees work remotely. But not every organization has been ready enough with their existing IT infrastructure to support a scenario like this. While hackers are taking advantage of the COVID-19 pandemic and given the rise of cyberattacks, an immediate need to protect data has already erupted.

Most of it is due to the fact that employees usually access enterprise data through insecure and unsafe networks and endpoints as they work remotely. Some employees may also be ignorant towards enterprise policies when it comes to information security. This in turn creates an ideal environment for hackers. Cybercriminals have been exploiting various ways of stealing sensitive and valuable data from organizations globally. Few incidents have been reported where large number of domain names related to Covid-19 being registered and also large-scale spam campaigns using Covid-19 as a handle in order to spread ransomware and steal data or even install banking malware.

Information security continues to be a major requirement of every organizations, particularly in the current situation. Organizations have a great responsibility to ensure that proper authentication and access policies are in place to protect their internal networks and sensitive data. Organizations have to ensure that both efficiency of work and protection of sensitive data go hand in hand. This requirement will not just hold importance in the current situation but will set the trend for the upcoming future too. This is because enterprises are taking this as an opportunity for assessment of the scalability and robustness of their existing data security measures.

The main solution proposed for all remote working related security concerns is Virtual Private network or VPN. VPN enables secure and safe remote work; not only for IT sector but also for everyone else.

V. VIRTUAL PRIVATE NETWORK (VPN)

A virtual private network can be regarded as a way to simulate a private network over a public network like internet. It is called a virtual network because it actually depends temporary connections which does not have any physical presence. They consist of packets routed over various servers and routers on the Internet on an ad hoc basis. VPN connections are created between two endpoints, an endpoint and a network, or two networks.

There are a number of technologies that VPNs use in order to protect data travelling across the internet. The most important ones are firewalls, authentication, encryption, and tunneling.

Firewalls uses techniques such as examining IP on packets or ports on incoming connections requested to decide which traffic is allowed into a network. Most VPN packages don’t implement firewalls directly themselves, still they are an integral part of a VPN product. The idea is to use the firewall to keep unwanted visitors from entering an enterprise network, while allowing genuine VPN users though. A VPN without a firewall is absolutely useless since it is exposing the corporate assets to considerable amount of risk. The most common firewall is a packet filtering firewall, which will block specified IP services from crossing the gateway router.

Authentication techniques are compulsory to VPNs since they ensure both of the communicating parties that they are exchanging data with the correct host or user. VPNs use strict authentication systems to verify identities. Most of the VPN authentication methods use a shared key system. A hashing algorithm will generate a hash value for the keys. And the other party holding the keys will generate their own hash value. The hash values which is sent across the internet is meaningless to a third-party who is observing the transmission. So even if someone try to sniff the network, they wouldn’t be able to get any passwords.

All VPNs should support some type of encryption method which actually packages the data to be transmitted through the VPN into a secure envelope. Encryption is in fact essential as authentication. Because encryption protects the transported data from packet sniffing. Mainly there are two encryption techniques used in VPNs. Private key encryption and public key encryption. In private key encryption, there is a passphrase known to all parties that need access to the encrypted information, which is known as the shared secret. This single passphrase is used for both encryption and decryption of information. Data Encryption standard (DES) is an example of a private key encryption technique. In contrast to private key encryption, public key encryption involves two keys - a public key and a private key. The public key will be known to everyone but not the private key. While sending the sensitive data, it will be encrypted with a combination of the senders’ private key and the receivers’ public key. Upon reception, it can be decrypted with receivers’ private key and senders’ public key. RSA is an example of this scheme. However, public key encryption is slower and time consuming when compared to private key encryption. Since VPN’s need to encrypt data in real time, they usually use private key encryption for streaming session. But the session secret will be encrypted using public key encryption and the same will be sent over the link.

VPN solution providers use tunneling in order to create a virtual private network. For example, point to point tunneling protocol (PPTP), IPSec tunnel, SSL tunnel, etc. Tunneling allows VPN providers to encapsulate a packet within a packet such as to accommodate incompatible protocols. The packet within the packet can be of the same protocol or a different protocol. It is also possible to encapsulate an IP packet within another IP packet. The practical aspect of this is, we can use private IP address space but still access the hosts across internet, which makes the internal corporate resources available through the internet to the employees who are working from home.

VI. Enterprise VPN Providers

Virtual private networks have become an imperative part of today's enterprise networks, since they provide a cost effective and secure means of assuring private internal and external communications over the shared Internet infrastructure.

One of the main VPN service providers in the industry is Cisco and their VPN solution is aptly named as AnyConnect. Cisco AnyConnect is a unified security endpoint agent which delivers multiple security services to protect the endpoint and the enterprise. It also provides the visibility and the control to identify who and which devices are accessing the enterprise resources. AnyConnect has wide range of security features including functions such remote access, posture enforcement, web security features, and even roaming protection. It is in fact a modular software product. AnyConnect provides VPN access through IPsec IKEv2 and Secure Sockets Layer (SSL). It also implements enterprise compliance check through the VPN with Cisco's ASA firewall or through wired, wireless, and VPN with Cisco Identity Services Engine (ISE) as headend. AnyConnect can implement web security with Cisco Cloud Web Security. It also offers network visibility into endpoint flows within Cisco's Stealthwatch. Off-network roaming protection with Cisco Umbrella (OpenDNS) is also present. AnyConnect client software are available for most of the platforms including Windows, macOS, Linux, iOS, Android, etc.

Pulse Connect Secure is the VPN offering from Pulse Secure, which was initially Junos Pulse owned by Juniper networks. It provides a seamless and cost-effective VPN solution for remote users from any device to internal corporate resources. Pulse Connect Secure claims they are the most widely deployed SSL VPN for organizations across every major industry. Pulse Connect Secure includes both Pulse Secure Clients and AppConnect SDK for customizing the VPN solution. They offer dynamic and multiservice network clients for mobile and personal devices. The software can be deployed simply, enabling users to quickly connect from any devices. The SDK provides per application SSL VPN connectivity for both iOS and Android phones, thereby allowing customers to create a secure and safe mobile app experience.

FortiClient VPN is offered by Fortinet. FortiClient included both IPSec and SSL VPN. They also support multiple devices and platforms like Windows, Mac, Linux, iOS and Android. Unlike other VPN providers, Fortinet provides antimalware protection as a main feature. FortiClient also simplifies remote user experience with built-in auto-connect and always-up VPN features. Multi factor authentication can also be used to provide an additional layer of security.

GlobalProtect is a part of the security ecosystem provided by Palo Alto. This requires the Palo Alto's hardware-based firewall solution to work. So, scaling up the capacity needs a significant investment in the infrastructure. It supports all existing authentication methods and also provides the next generation firewall with a user to IP mapping to ensure secure access control for all VPN users. GlobalProtect also supports RADIUS and SAML integrations in order to accommodate a range of third-party multi factor authentication methods. Which includes one-time passwords, certificates, and even smart cards. GlobalProtect helps to eliminate blind spots in the remote workforce traffic by offering full visibility across all network traffic, applications, ports, and protocols.

Check Point VPN provides secure access to an enterprise resources to both individual hosts or clients like telecommuters, mobile users, and even extranet consumers. Each host will have a VPN client software installed or they can also use a web-based client. Security and privacy of information is guaranteed by incorporating techniques like multi factor authentication, encryption of all transmitted data and also compliance verification of endpoints.

Microsoft DirectAccess allows connectivity for remote employees to the enterprise network resources without requiring traditional VPN connections Remote endpoints are always connected to the organization by using DirectAccess connections. There is no need to start and stop connections for the remote users, like traditional VPN. DirectAccess provides support only for endpoints who joined a domain. Also, the endpoint should include operating system support for DirectAccess. So, it essentially supports Windows operating system. The DirectAccess connections are initiated and established by the endpoint, not by the user. DirectAccess connections are secure and authenticated and established automatically whenever the DirectAccess client has an active Internet connection. The connections are also bidirectional in nature, which is an important distinction when compared to traditional VPN.

Few cloud-hosted VPNs are also there. It’s a low-cost method of adopting VPN protections which is more suitable for small companies that are in the growth phase but not yet ready to manage their own servers or firewalls yet. These cloud solutions usually tie directly into other cloud service providers such as AWS, Azure, and Google Cloud.

VII. VPN DURING COVID-19

VPNs cannot handle the entire workforce traffic that is operating from their homes in the current scenario. An enterprise shifting from about 300 employees using a VPN to 1,000 is definitely a major challenge. So, it needs the addition of extra remote access servers, firewalls, RADIUS servers and load balancers which takes weeks to order, deliver and install.

Under these circumstances, most of the companies are looking for an active-passive VPN setup. It helps in shifting the load between two headend devices. Enterprises should also go through the Service Level Agreement they had with their VPN providers. It is better to talk to the hardware provider and ask for an extra device. Backup hardware is always a part of every SLA.

VPNs are currently in the middle of a vast surge in use all around the globe since enterprises are adopting remote work and work from home policies quickly to stay active during COVID-19 lockdowns and social distancing measures which are implemented during the pandemic. This is surely a great test for modern VPN providers and how well they can scale up with the sudden demand. But, it’s also difficult for businesses who are practicing such remote work setups for the first time. Since the security needs are different and complex. A VPN is the ideal option for encrypting corporate data from home computers to enterprise networks, but many businesses haven’t even considered using a VPN before the pandemic.

This is the reason why we’re witnessing a lot more research and experimentation with implementing VPNs in enterprise scenarios to protect data from remote work. A traditional method which was being followed is to set up a VPN server hosted on a private network and instructing remote workers to use client apps on their devices. This offers end to end encryption with some flexibility for businesses which handles a lot of data. However, enterprises that are not yet ready to scale up to such setups can use free VPN setups that still provide benefits and can be implemented very quickly when remote work is a sudden change.

Large enterprises were already using commercial and proprietary VPN solutions. The demand for remote access VPN has been particularly pronounced among such large enterprises. Some were expanding its employee remote access from around 8,000 daily users to 80,000 daily users, while another was scaling up to 130,000 concurrent users relying on the VPN every day. Some of the remote access VPN expansions have driven additional business for VPN solution providers, while others have been accommodated by increased access to licenses the customer already owns. In some instances, enterprises even took equipment that was planned for other projects and used it for the VPN extension.

The transition to remote work has expedited the planning process with companies going from having a pipeline of projects set out a year in advance to needing things done in days or hours. In fact, the need for remote access VPN was so great that VPN providers were actually shipping the equipment to customers before even receiving the order so they could get set up more quickly.

Popular VPN provider Cisco offered customers with free licenses for up to 13 weeks so that they can scale up and function effortlessly meanwhile they get enough time to proceed with purchasing the product license eventually. Meanwhile Pulse Secure offered customers with expedited and flexible licensing to facilitate rapid implementation. This allowed organizations to readily deploy and gain the advantages of Pulse Virtual Traffic Manager with Optimal Gateway Selection. It offered purpose-built virtual and cloud software-based load balancing.

VIII. CONCLUSION

Most of the companies in the IT industry were already equipped with some amount of infrastructure to support those employees who work from home. So, the main challenge which organizations faced with VPN, during the pandemic is scaling up to accommodate more VPN users. Major percentage of the VPN solutions rely on the hardware provided by the same vendor. Reliance on physical appliances also means challenges when scaling a VPN across an organization. If fluctuations in workers requiring VPNs are expected, firms should instead look to software-based VPNs, which can be installed on any physical server or even in the cloud, such as in Azure or AWS, allowing for significantly more flexibility.

The main factors which companies were looking for in a VPN solution were performance, user experience, scalability and security. A VPN solution should be able to achieve latency and throughput performance and improve the end-user experience thus protecting end-user productivity. Also, it should be able to scale to a large number of concurrent users on a single hardware platform without performance degradation. It should provide not only encryption but also deep packet inspection and application-level filtering without adversely affecting overall system performance.

Companies can get a lot more use from VPNs than just basic data encryption. By taking a look at business-facing VPN vendors, we could see a host of security services, including better encryption for customer/partner data, more robust firewalls, whitelist management for important employee tools, and a lot more.

This can provide a big boost in security for businesses that deal with digital data — but most companies in these industries were already aware of this. What we're seeing now is a broader realization among many different companies that VPNservices can lower their security risks as a whole.

In many respects, COVID-19 pushed many industries into remote work solutions when they were balking at the change before. It was often overdue. When threats from the pandemic fade, a lot of organizations are going to find that their structure now incorporates remote work permanently. It just won't be as feasible to return to the old situations. That means VPNs are becoming an integral part of more business's networks, and faster than expected.

IT industry is built on strong foundations and it surely has all the required resilience to absorb the shocks of corona crisis. So, any setbacks due to current scenario is going to be just temporary and the IT industry will be able to come back on track rather quickly.

IX. REFERENCES

[1] Tom Rowan (2007), VPN technology: IPSEC vs SSL, Network Security, Volume 2007, Issue 12, December 2007, pp. 13-17

[2] R. Maria del Rio-Chanona, Penny Mealy, Anton Pichler, Francois Lafond, Doyne Farmer (2020), Supply and demand shocks in the COVID-19 pandemic: An industry and occupation perspective, COVID ECONOMICS, VETTED AND REAL-TIME PAPERS, ISSUE 6, 17 APRIL 2020, pp. 65

[3] Erik Brynjolfsson, John J. Horton, Adam Ozimek, Daniel Rock, Garima Sharma, Hong-Yi TuYe (2020), COVID-19 and Remote Work: An Early Look at US Data, NBER Working Paper No. 27344, Issue June 2020

[4] Bick, Alexander and Blandin, Adam and Mertens, Karel(2020), Work from Home after the Covid-19 Outbreak (June, 2020). FRB of Dallas Working Paper No. 2017

[5] Guillermo Gallacher, Iqbal Hossain (2020), Remote Work and Employment Dynamics under COVID-19: Evidence from Canada, DOI 10.3138/cpp.2020- 026

[6] Elizabeth S. Veinott, Judith Olson, Gary M. Olson, Xiaolan Fu (2020), Video helps remote work: speakers who need to negotiate common ground benefit from seeing each other, DOI 10.1145/302979.303067

[7] Adam Ozimek (2020), The Future of Remote Work, SSRN 3638597

[8] Irene Hardill, Anne Green (2003), Remote working—altering the spatial contours of work and home in the new economy, DOI/10.1111/1468-005X.00122

[9] M. Bishr Omary, Jeetendra Eswaraka, S. David Kimball, Prabhas V. Moghe, Reynold A. Panettieri Jr., Kathleen W. Scotto (2020), The COVID-19 pandemic and research shutdown: staying safe and productive, DOI 10.1172/JCI138646

[10] Dimitris Papanikolaou, Lawrence D.W. Schmidt (2020), Working Remotely and the Supply-side Impact of Covid-19, DOI 10.3386/w27330

[11] Crowley Frank, Daly Hannah, Doran Justin, Ryan Geraldine (2020), COVID-19, social distancing, remote work and transport choice, DOI 10419/221739