SAFELY SCALING VIRTUAL PRIVATE NETWORK FOR A MAJOR TELECOM COMPANY DURING A PANDEMIC

Shannon Roberson, Mohammad Abdus Salam,
Mathieu Kourouma and Osman Kandara

Department of Computer Science,
Southern University and A&M College, Baton Rouge, Louisiana, USA

ABSTRACT

VPN usage across the world has increased due to the COVID-19 pandemic. With companies trying to lay the course through this unfamiliar state, corporations had to implement a Business Continuity Plan which included several elements to maintain a scalable and robust VPN connection. During this time of uncertainty, best practices need to be deployed by corporations and government entities more than ever. The purpose of this study is to highlight the necessary path SD Telecom would take to ensure a secure, reliable network during global traffic surge. Specific VPN solutions, access needs, and eligibility requirements vary based on the end user. The question being investigated is: How does a major telecom company carefully extent VPN services during a novel pandemic? It is hoped this study will inform Information Security personnel and employees about the process and procedures for scaling VPN during a major crisis.

KEYWORDS

Virtual Private Network, Network Access Server, Personal Computer, Pandemic, Virtual Worker.

1. INTRODUCTION

The implementation of Virtual Private Network (VPN) usage has been around since the existence of Virtual Circuits. Virtual Circuits (VCs) are similar to VPN in that they are cost effective and easy to implement. Since the early 1980s, the virtual circuit was created to establish a pathway from the source port to the destination port. The virtual circuit works in the same fashion as a direct link between the two sources. Hence, communication between two applications could transmit over a shared connection. This technology advanced with ad-hoc encryption tools to router systems, which decoded data involving the ports of the virtual circuit. These communication entities prevent hackers from accessing data in transit [1].

In 1996, peer-to-peer tunneling protocol, or PPTP, was developed by a Microsoft employee [2]. Originally, starting in business, VPN grew rapidly once security breaches with everyday end users became prevalent in the early 2000s. Not only does the VPN secure internet connections, but also hacking and malware prevention, digital privacy, and geo-blocking to help safeguard users from fraud and data breaches [3].

Telcom companies use VPN as main source of connecting work-from-home employees to the intranet. VPNs have been driving new remote access requirements while at the same time the availability of shared broadband access has been allowing more companies the opportunity to

explore more flexible work environments for their employees. Companies have begun seeking solutions that take advantage of lower cost shared access methods while preserving the performance and security previously only available through costly dedicated access. However, shared network access introduces a wide range of problems related to network performance and security, and support becomes more complex with difficulties to diagnose as consumers compete for bandwidth.

The paper will be organized as follows: Section 1 will include a brief history and introduction of the VPN.

Section 2 is a review of related literature. Section 3 consist of the methodology based on reliability and validity. Section 4 will include the data analysis based on the raw data collected and interpreted. Section 5 will conclude the research.

1.1. Background

VPN is currently being used to transmit data, video, and voice over secure and unsecure networks. It is designed to deliver an encrypted passageway to communicate the information between the distant user and the company network. To prevent data breaches, there are several elements put into place to secure the company's VPN and the end users network connection. This remote route is an excellent option for corporation's with remote workers with international offices to transmit data in a secluded method. Although used mainly by companies, individual users can take advantage of the security, privacy, and identity protection features as well.

1.2. How a VPN Works?

A virtual private network, or VPN, uses encryption to securely send data over an untrusted network. It acts as a transmission medium, or a pathway, connecting devices on a network. Usage of a VPN connection allows you to take advantage of an existing internet connection to securely communicate between devices.

There are multiple ways that a VPN can be configured: *host-to-host*, *site-to-site*, and *client-to-site*. VPN connectivity. A **host-to-host VPN**, as shown in Figure 1, allows for example, a host A connected to the internet to establish a VPN connection to another host B on the other end. With a host-to-host connection, both ends of the connection need to be configured to use same the VPN protocol. The sender, Host A, uses the protocol to encrypt and encapsulate packets before sending them through the internet. The receiver, Host B, on the other end must use the same protocol to de-encapsulate and decrypt the packets.

Figure 1. A host-to-host VPN

A **site-to-site VPN** establishes VPN connection between two remote network sites, let's say Site A and Site B, as shown in Figure 2. Any computer on Site A can communicate securely with any other computer on Site B. Instead of requiring VPN configuration on every single computer on the network site, a single VPN device, which acts as a gateway server, can be installed. In this

implementation, only the VPN server needs to be configured with the VPN protocol. This VPN server accepts unencrypted packets from the local network, encrypts that information, and then sends it over the internet to the destination VPN server at the other site. The destination VPN server removes the encryption information and forwards the data on to the private network at the other end.

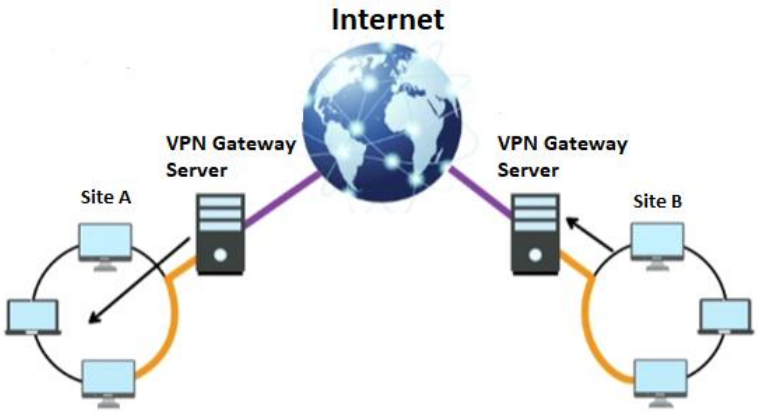

Figure 2. A site-to-site VPN

A **client-to-site VPN** provides a remote access VPN. A remote access VPN configuration replaces a dial-up remote access server. Figure 3 show a client-to-site configuration. In this configuration, individual clients (desktop, tablet, smartphone, or notebook) on a private network (home or enterprise) or travelling users establish a VPN connection through the internet to the remote site. Because of the encryption used by the VPN protocol, it's considered safe to establish remote access VPN connections from public-access Wi-Fi networks that don't use the best security, like airports and hotel networks. The client computer establishes a connection with a VPN server, often called a VPN concentrator, that sits on the edge of the private network. The VPN concentrator job is to accept multiple VPN connections through the internet. Each client is configured with the VPN protocol that allows it to encrypt and tunnel packets. The VPN concentrator is configured to allow or reject connections from users and then removes the encryption before forwarding the information to the private network [4].

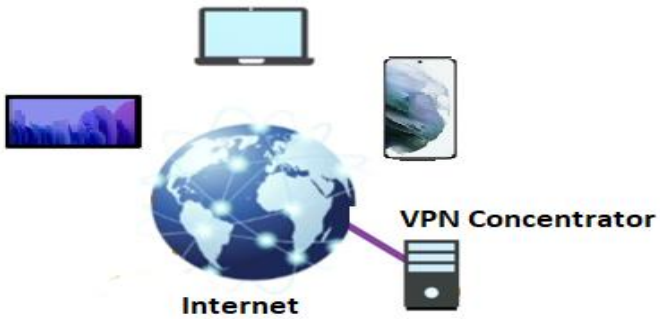

Figure 3. A host-to-Internet VPN

1.3. Significance

In 2020, we experienced a global pandemic, with the onset of COVID-19. As a result of this pandemic the way we live, and work changed almost overnight. In a small window of time, companies were forced to rethink the way they operate, with most workers having to transition to

work from home. Nowhere was the need to scale VPN more important than in the telecommunications industry; to protect proprietary information, monitor efficiency of employees and manage profitability for shareholders, all while meeting increased demand of consumers. Unfortunately, there was not a "playbook" that major telecom companies could use to safely scale VPN in a truncated period to meet demands of this new reality.

1.4. Statement of Problem

This research or paper will attempt address the following:

- What safety measures should a telecom company take to secure the VPN connection?
- What impact did the pandemic have on companies with majority of the workforce working in the office?
- What challenges did call centers within telecom companies face during the pandemic?
- What major changes/adjustments would have to be made to a telecoms company network infrastructure in order to sustain during a pandemic?

2. REVIEW OF RELATED LITERATURE

As the coronavirus persists, organizations need to assess their capability to conduct business as usual during a pandemic. This requires assessing the Business Continuity Plan accurately and often to be better prepared in the event of a disaster. This effort will help companies determine if they can support an increase number of remote workers and gauge the effects of a pandemic. For businesses without an applicable Business Continuity Plan remote working resolution, the financial impact of social distancing will be extensive. This plan will help to guide organizations to better prepare and respond to challenges, specifically COVID-19 and other global pandemics.

2.1. Playbook

The SD Telecom "Playbook" is a Business Continuity Plan that outlines the processes and procedures an organization must follow in the event of a pandemic. A great plan is supported from senior management down. In order for this "Playbook" to be successful, priority must be placed on testing and reviewing on a regular basis.

2.2. Asset Deployment Plan

Asset deployment is the most important part of the process. If there are no machines to work on, then there won't be any work getting done. Call center workers account for 30% of the business. Pre-Pandemic, these workers report to the office daily and had no access to the VPN. The Challenge: How would you request PCs/laptops, VPN access, and RSA tokens for over 30,000 employees? You first start with allowing some employees to take the equipment from the office to their home office. For those employees without that option, a bulk order for laptops, monitors, and peripherals would be placed with the PC vendor to fulfill as many orders as possible. Another option is to move employees to HVD users. This will allow them to access applications and stored data from the cloud. BYOD is an option that is not widely used due to the huge security risk involved. The training materials for setup and installation must be modified to accommodate the CCW's with no prior IT experience. Having an active helpdesk available to assist is vital in this process. RSA secure id tokens are requested in bulk to expedite the process and ensure authentication and encryption to permit employees to communicate safely over the internet.

2.3. Network Plan

The remote access server, also called “media gateway” is a server that manages network access to remote resources. The main function is to serve as a “entry way” for secure remote end users. In an enterprise setting, a network switch can act as a network access server to ensure the corporate network is accessed by authorized individuals. VPN’s are used in conjunction with the NAS to connect employees to the enterprise’s network. During a pandemic, increased internet speeds and secure flexible bandwidth are very important to sustain business. Not only will capacity be important, but redundancy is a key factor to keep the network from experiencing a loss of connectivity. Having a reliable backup source will ensure an “always on” connection so the business won’t experience any performance hits. Also, this setup will allow traffic to flow while maintenance is being performed on the backup source. Most companies have enough bandwidth and licenses (based on the number of users) to support use by 10% to 20% [5]. Having the right equipment in place, monitoring and maintaining the infrastructure regularly, and scaling remote access solutions are the key components when providing zero service disruption in the event of a pandemic.

2.4. Remote Access Plan

Internet service is essential for providing remote access to end users. Due to the surge in homebound computer users, internet speeds have decreased tremendously. Remote access can be affected by internet performance in many ways. One example, using video calls for meetings. If the service is not providing a minimum of 8 Mbps download/1.5 Mbps upload, then you may experience audio and video issues [6]. Virtual tunneling is another important element to VPN usage. Encapsulation allows the movement of data from a private network across the internet, which is considered a public network. Also, data tunneling can be helpful in hiding the identity of the user initiating the traffic. Tunneling requires three distinct protocols in order to transport the encrypted data across the internet (Passenger Protocol, Encapsulating Protocol, and Carrier Protocol) [7].

2.5. Communications Plan

Effective communication is an intricate part of progression and success of a business. Managers and executives should keep-all-employees up to date on important changes within the company daily. During a pandemic, employers must come up with a valuable communications plan to reduce anxiety and increase productivity amongst the workers. First, the organization should set up a website or hotline to provide guidance to employees who may have questions or concerns about the company’s direction. This would minimize the need for employees to email or call supervisors with questions. Messenger platforms should be readily available for more immediate assistance. Secondly, employees should be encouraged to use video conferencing platform to ease the feeling of seclusion and loneliness. Connecting with your team doesn’t seem like much but with people quarantining but seeing another individual’s face is very important to the human connection. Invite employees to lunch and learn sessions and even virtual lunch dates. Continue to celebrate milestones, anniversaries, birthdays, and small successes during this time creates a community and maintains culture within the group. Finally, review the Communications Plan to identify what worked, what didn’t work, and recognize areas of uncertainty. Recognizing these areas will reduce the impact on the business and position the company for success during the next pandemic. Be sure to elicit valuable feedback from stakeholders on a frequent basis to help streamline processes and practices. This evaluation should be an annual practice to stay up to date with domestic and international changes within and outside the company.

3. METHODOLOGY

The "Playbook" is a combination of processes and procedures used in the event of a pandemic or natural disaster. This study was made in order to minimize risk and avoid disruption of the company network and protect the customers. These steps are action items that should be taken before, during, and after a major event in order to maintain financial viability of an organization. In order to get real time information, an interview was conducted with the CSO (Chief Security Office) and the CDO (Chief Data and Security Office). These organizations were the first responders of the COVID-19 pandemic for SD Telecom. First, they ensured assets were deployed to employees so they could be able to work from home. Then, once everyone was on the network, the increased traffic caused congestion on the network servers. Circuits cards were upgraded, and concentrator subscriptions were increased in order to ramp up service capacity. As time went on, they worked around the clock to ensure zero loss of service, secure network and data, and stability of the IT infrastructure. The call center workers played a major role in gathering data as well. With 30% of the company's headcount, they were able to participate in observation interviews for IT to get insight on their job tasks, level of knowledge, and application requirements beneficial to enabling remote work.

4. DATA ANALYSIS

4.1. The Comparison

COVID-19 has augmented the trend toward telecommuting for most companies. Almost half of American workers are working from home which is twice the segment who worked remotely 3 years ago. Although remote working has had an overwhelming success rate, some companies are not on board with continuing the movement due to them struggling to contend on an innovation level, employees lack of ability to stay focus, decreased employee visibility, and lack of relationships among coworkers. The majority of the repulse is doubts regarding the accountability of whether individuals are working or not.

Southern Telecom used the "Staggering Shifts" method in order to keep their workplace safe for their staff. When using this method, employees come in and leave work at different times. For example, if you have 20 people working in a group, 10 people can work from 7am to 3pm and the rest will report from 10am to 6pm. The company felt this would ease the congestion in a crowded office space and minimize the risk of COVID-19. Figure 4 shows how companies are handling the pandemic.

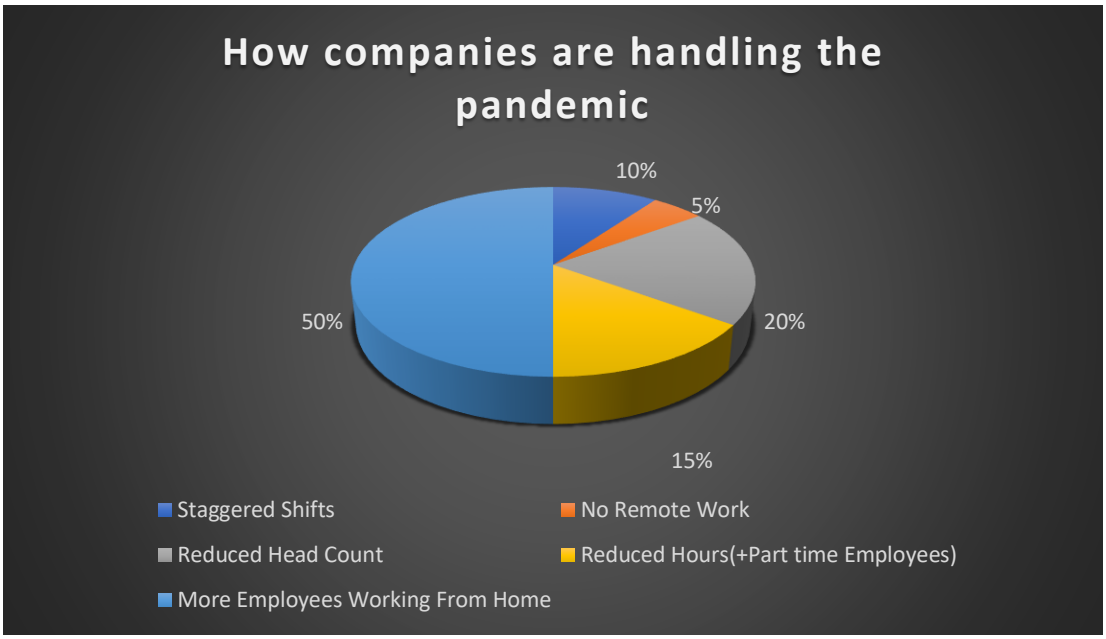

Figure 4. Pandemic Management

The downside of this method is this process does not safeguard individuals from contracting coronavirus. At some point during the day, all employees that were originally on a fixed schedule will end up in the office at the same time between the hours of 10am and 3pm. Having employees to report to the office will increase the risk of exposure and put family members in jeopardy of contracting the virus.

Companies like American Tower Telecom are out right denying employees from working remote and forcing them to come into the office at a time where the numbers are steadily increasing. As life gradually returns back to normal, the companies and their workforce maybe on a collision course because of their differences regarding the virus. At this point in time more companies are offering the flexibility the staffers need. Therefore, if you're organization isn't proposing this option some will seek employment elsewhere. Not only will the workplace environment become toxic, but the head count will start reducing, there will be a greater risk of the virus spreading in the office, and employees will be putting their families lives in danger.

Verizon wireless has implemented a "permanent work from home" program for customer service reps and telesales employees. This decision was made after COVID-19 forced the company to extend the WFH policy to employees who didn't have that option originally. Luckily there was a remote workforce training program for select employees, so the company was able to roll out the program to other organizations. This program consists of self-guided video and content training and on-the-job training. Employees outside of the support teams may not agree with this process because they will not have the option to participate in the program on a permanent basis. This will cause a shift in morale and a decrease in headcount as employees seek employment with companies with remote work options. Figure 5 displays the statistics of employees working from home.

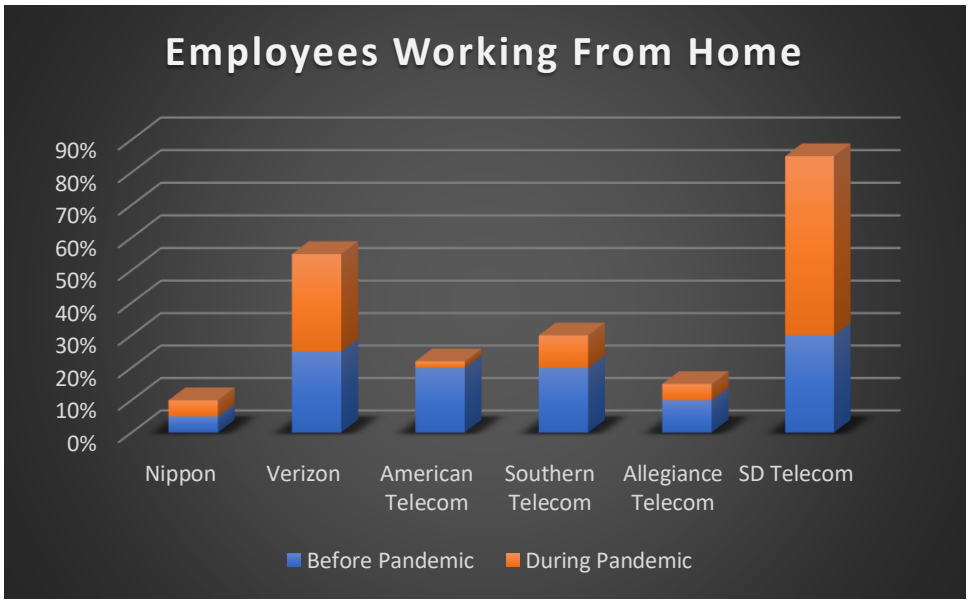

Figure 5. Percentage of Remote Work

Nippon Telegraph and Telephone Corporation has a totally different stance on working from home. Based on their Japanese culture, they value physical presence and expect employees to work long hours over efficiency and productivity. Also, they force employees to use vacation time instead of sick days when they are ill. This will pose a challenge for agencies determined to avert the spread of the virus by detaining infected individuals at home. Their belief is "work happens at the workplace" and if you're not in the office then you're said to be deceiving the company. Despite government reinforcement, companies are not outfitted or prepared to work remotely due to the unstable and unreliable IT infrastructure. Although mask is common in this society, it's still not enough to combat the rising coronavirus cases.

Allegiance Telecom more like the company that doesn't want to change despite what's going on around them. This is a very small company that doesn't require much overhead and manpower, so they feel there is no need for big changes. Their philosophy is "big changes bring on big problems". During the first 4 months of the virus, they allowed most employees to work from home using the HVD (Hosted Virtual Desktop). The HVD application that enables employees to securely access their workstation anytime, anywhere, from any device. This helps companies to save money by using utilizing user interface presented on an isolated infrastructure supported, managed, and improved by the cloud service provider. This continuity plan was already in place before the pandemic so there was no need for major changes. Many companies are making more profit due to pandemic (Figure 6).

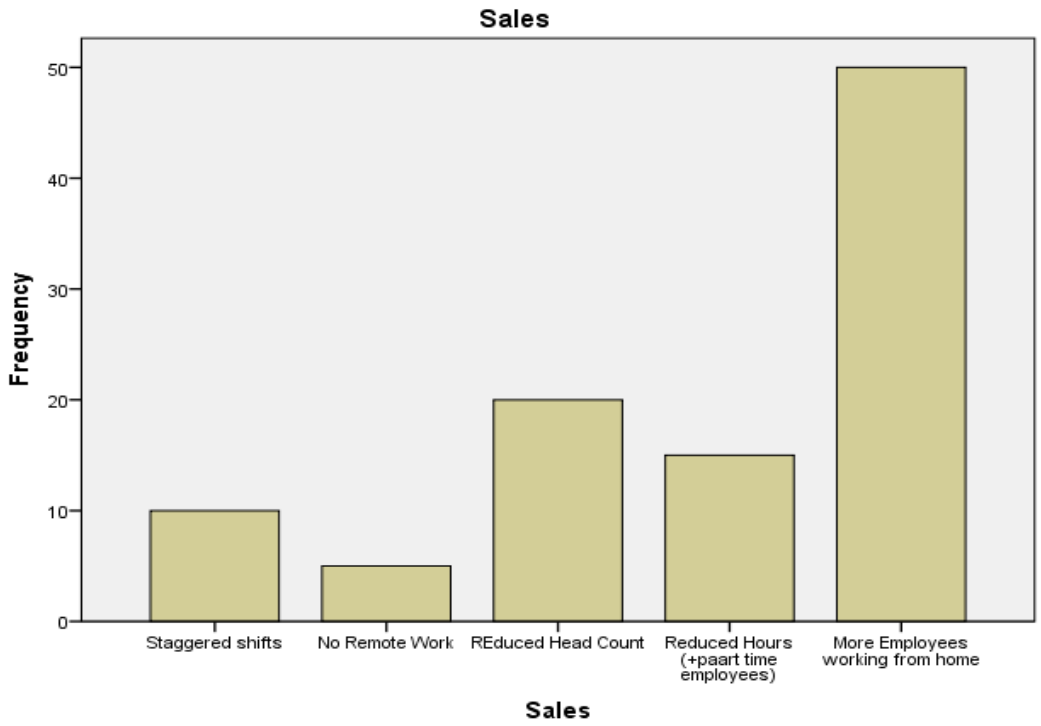

Figure 6. Bar graph showing that the frequency of sales was highest with more employees working from home (IBM SPSS).

4.2. Broadband Offerings

Broadband is the conduction of the maximum amount wide bandwidth data over a high-speed internet connection in a fixed amount of time. It delivers high speed internet access through several technologies such as wireless, DSL, cable, fiber optics, and satellite. Often mistaken for internet speediness, broadband is essentially the volume of data that can be transmitted in a quantified time frame. This calculation is known as megabits per second (Mbps). The higher the Mbps, the faster the data will download from the internet.

The best way to comprehend bandwidth is to consider a faucet and water. Envision you need to fill up a tub with water. The higher you turn on the water the faster you're fill up the tub. The same analogy can be used to describe bandwidth. An increased bandwidth will permit data from the internet to transmit quicker to the device. The more bandwidth you have the greater the experience you will have. To attain a virtually continuous experience with decreased delays, contemplate speed plans 100 Mbps and above.

Based on the bandwidth offerings above, Nippon Telegraph and Telephone Corporation offers double the amount of bandwidth than SD Telecom and Verizon. This may be due to NTT's extensive fiber infrastructure which includes Arcstar ™ Global e-VLAN and Global IP-VPN. American Telecom, Southern Telecom, and Allegiance Telecom customer base is mainly in rural areas where infrastructures are poorly maintained. The average internet speed in rural areas is 39.01 Mbps.

4.3. Remote Access VPN

A remote access VPN allows individuals who are working from home to securely access applications and data from the company network. A secure, seamless VPN tunnel is created between the company's network and a remote user. Confidentiality and reliability of confidential information is safeguarded through a multi-factor authentication, compliance scanning, and encoded data. For example, SD Telecom has remote access sites in Michigan, Georgia, Texas, and California. The individual is able to be logged into the company network from anywhere from any device that has internet access. Various remote access sites data is provided in Figure 7.

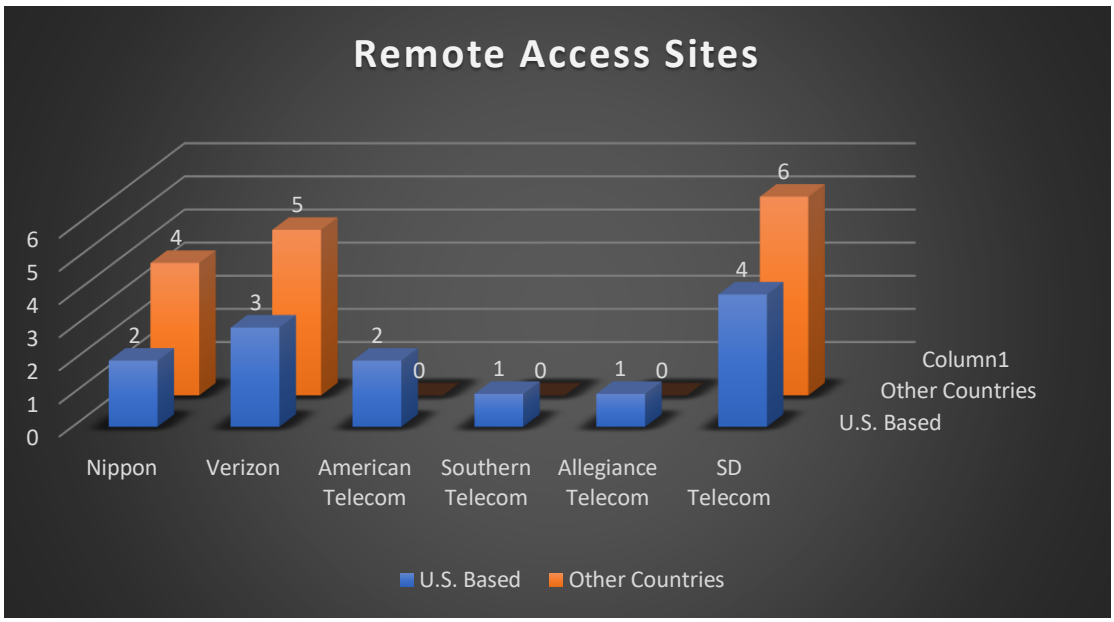

Figure 7. Remote Access Sites

The network access server (NAS) and a client software are required in a remote access VPN. A NAS, also called a remote-access server or a media gateway, may have multiple software applications functioning on a communal server or a dedicated server. A user is connected to the NAS from the internet with the purpose of using the VPN. Valid credentials are required and verified via the network access server or a different server operating on the network. The VPN software client is an application installed on the user's device that maintains and supports a secure connection to the VPN. The software client establishes the tunneled relation to a NAS specifies by its IP address. The software also controls the encryption obligated to maintain the secure connection.

Although working from home can be seen as simple, the process can be very complex behind the scenes. In the wake of the COVID-19 pandemic, companies had to "act fast" to keep the business intact. A viable network infrastructure, stable broadband connection, and remote access capabilities are vital components in the success of employees working remotely.

5. CONCLUSION

5.1. Research Outcome

SD Telecom is a state-of-the-art company that prides themselves on being ahead of the game in the field of technology and services. Based on the research, if they continue the path they are on, they will have no problem separating themselves from the average company. At the start of the pandemic, SD Telecom was able to provide a direct solution that enables in-office employees to continue to work during disruptive incidents, without obliging compromises on the network or the overall company."The Playbook" will provide processes and procedures for any organization to assist during a pandemic as well as lessen any new security risk.

5.2. Summary and Conclusion

While it is essential to have a disaster recovery plan in place to restore data and critical systems when an event hits, business continuity is your strategy to return your whole business to full functionality after a crisis. Companies should also familiarize themselves with their providers business continuity plan to get acquainted with how they will act in response to service issues. There's no such thing as being over-prepared when it comes to business continuity. Your plan must be tested regularly so any adjustments can be made in the calm outside of a crisis. Assess your business continuity plan now to review what was learned during the pandemic, what worked, what didn't work and what needs to be done moving forward. The sudden mass adoption of digital services will impact daily lives for years to come and will likely result in new business models and organizational structures.

As a future research direction, we would like to focus on more corporations and study their existing systems and proposed playbook for any possible future pandemic.

ACKNOWLEDGMENT

The authors would like to thank anonymous reviewers for their constructive suggestions that helped us improve the paper.

REFERENCES

[1] R. Younglove, "Virtual private networks - how they work," in Computing & Control Engineering Journal, vol. 11, no. 6, pp. 260-262, Dec. 2000, doi: 10.1049/cce:20000602.

[2] K. Jyothi and D. B. I. Reddy, Study on Virtual Private Network (VPN), VPN's Protocols Security, vol. 3, no. 5, 2018. [Online]. Available: http://ijsrcseit.com/CSEIT1835225.

[3] W. Rash. (2020, June 17). Your VPN May Be Your Greatest Security Risk During COVID-19 [Online]. Available: https://www.forbes.com/sites/waynerash/2020/06/17/your-vpn-may-be-your-greatest-security-risk-during-covid-19/#7b2f88db31a6.

[4] TestOut Network Pro Training, www.testout.com.

[5] R. Cohen and G. Kaempfer, "On the cost of virtual private networks," in IEEE/ACM Transactions on Networking, vol. 8, no. 6, pp. 775-784, Dec. 2000, doi: 10.1109/90.893873.

[6] G. Smith, "COVID-19 (Coronavirus) & Cybersecurity: Telecommuting and Remote Work Security FAQs," Attila, 07-Jul-2020. [Online]. Available: https://www.attilasec.com/blog/covid-19-coronavirus-cybersecurity-telecommuting-remote-work-security-faqs. [Accessed: 09-Sept-2020].

[7] L. L. Ben-Yacoub, "On managing traffic over virtual private network links," in Journal of Communications and Networks, vol. 2, no. 2, pp. 138-146, June 2000, doi: 10.1109/JCN.2000.6596734.

AUTHORS

Shannon Roberson is a Senior Consultant Systems Integration with AT&T and has over 15 years of telecommunications experience. She has worked in several organization within AT&T including Supply Chain, Network Operations, Engineering, Mobility, and Business Sales-Cybersecurity. She is currently pursuing her master's degree in Computer Science from Southern University of Baton Rouge. She loves playing tennis and spending time with her family in her downtime.

Dr. Mohammad Abdus Salam received his bachelor's degree in electrical and electronics engineering from Rajshahi University of Engineering and Technology, Bangladesh in 1991. His master's and Ph.D. degrees are from The University of Fukui, Japan in 1998, 2001, respectively. He is currently a professor of Computer Science at Southern University, Baton Rouge, Louisiana, USA. His research interest includes wireless sensor networks, wireless communication, and information theory and coding. He has taught a variety of courses from the field of computer science and engineering. He has authored and co-authored many international journals, conference proceedings, and a book chapter. He served as a guest editor for many journals. He also served on the editorial boards and panelist for NSF, NASA, and many conferences.

He is a senior member of IEEE and an executive council member of the Louisiana Academy of Sciences (LAS). He was awarded numerous awards throughout his career including the faculty outstanding achievement award from the President of the Southern University System, LAS president's award, and NASA and ONR faculty fellowship awards.

Dr. Mathieu Kourouma is full time Associate Professor in the Department of Computer Science, College of Sciences and Engineering at Southern University Baton Rouge (SUBR) since August 2006. He has a BS in Electronics from the Polytechnic Institute of the University of Conakry (Republic of Guinea), MS and PhD in Telecommunications and Computer Engineering, respectively, from the University of Louisiana at Lafayette (ULL). He is well-trained in the STEM fields and has earned a series of certifications in various industrial areas: Java, PC Pro, Network Pro, Security Pro, Desktop Pro, Client Pro, Linux Pro, Data Science with Python, Data Science with R, Data Analytics, Machine Learning, Databases, etc. from Microsoft, IBM, Oracle, TestOut, etc. His research and work areas include Cybersecurity, Robotics, Database Design, Software Development, Machine Learning, etc. He worked for the Ministry of Telecommunications in Republic of Guinea and did consulting in technology. He has trained BellSouth and AT&T employees in Telephony, Data Convergence, and Electrical. He is the Director of the Oracle Academy and directed Microsoft Academy at Southern University.

Dr. Osman Kandara received his BS in Computer Technologies Education from Marmara University in Turkey, his master's degree in systems science and his PhD in Computer Science with a minor in Educational Leadership, Research and Counseling both from Louisiana State University in the US. At present, he is an associate professor of Computer Science at Southern University and A&M College at Baton Rouge, LA. His research and teaching interests are data mining, artificial intelligence, system testing, social networking, teacherless education, and just-in-time learning.