Network Analysis and Architecture Evaluation

SNHUEnergy Inc.

Name

IT 640 Final Project

Instructor Name

September 13, 2018

SNHUEnergy Inc.

Network Analysis and Architecture Evaluation

Executive Summary

SNHUEnergy Inc is a mid-size company that deals with the exploration, discovery, and drilling of oil-based products. The next big thing for SNHUEnergy Inc is to provide transportation and refinement of its investigations. The company is at a critical stage of growth and expansion, and the company relies on its network infrastructure to support the process. There is a concern with the current network architecture of SNHUEnergy Inc as the company has faced serious problems with its routers. The loss of connectivity between its Memphis and Dallas routers impact the business as well as communication between users. The loss of connectivity affects accounting processes, emailing, payroll and video conferencing, this means that users experience delays as they wait for their network to keep up with the speed at which they are working. Therefore, SNHUEnergy Inc needs to extend its service networks across the Wide Area Network (WAN) and using TCP communication processes to connect the sites. Although WAN connections differ in bandwidth depending on users' needs. WAN connections can also be set up through a direct connection via the internet (Achetson, 2014). In any of the cases, a good connection between your locations enables secure and better communication within the corporation

This report will look into the infrastructure and architectural capabilities of the current network, as well as performance and security issues that may arise if the system is not changed after the expansion. It comprehensively looks into the existing network OSI model, the physical network devices in use as well as the current traffic flow and its challenges. An overview of a Wireshark is used to identify the everyday problems of the network and also identify a pattern

across the infrastructure of the company. Besides, performance and security issues are defined for the current system and the existing vulnerabilities and risks designated.

The report then proposes a future network architecture for the company that addresses all the identified communication needs, security concerns, as well as increased data traffic. In the new network, the report introduces a network redesign that adds a hierarchical Network design with three primary layers; core, distribution, and access and improves its capabilities. It then expounds on the details of the network on each layer and the protocols to be administered on the sheets. The report concludes with planning and security recommendations that could guide the organization during implementation and the potential benefits of the new network. Further, the report identifies a network management tool and proposes a solution to risks and vulnerabilities.

Current Network Architecture

Network Applications

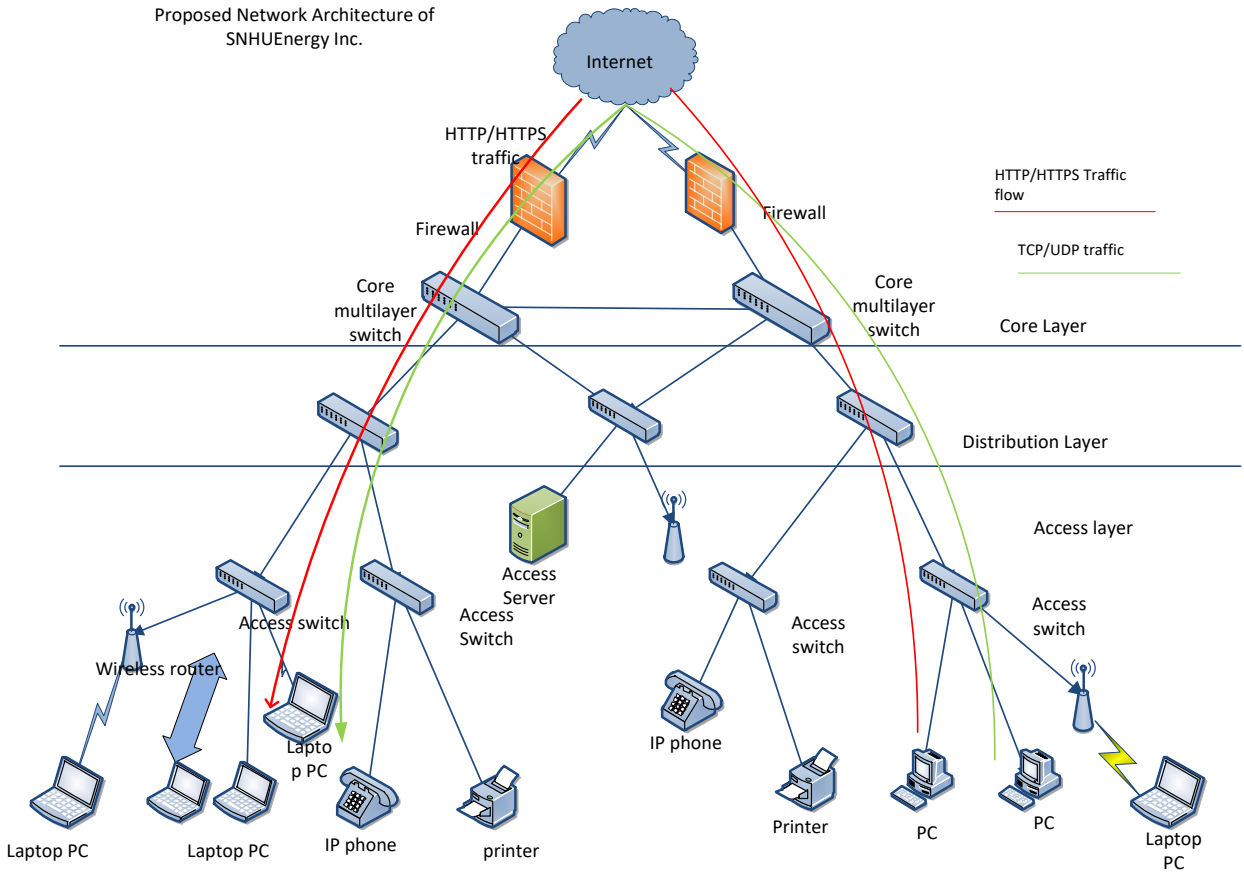
Presently, SNHUEnegry Inc uses four applications, i.e., Accounting and HR, payroll and email. This network architecture plays a critical role in application performance management in the corporation. According to Harrell, depending on server locations and network geography, traffic networks can vary in different areas of the network (n.d). In such a case it needs a wide view of the network in regards to capturing of applications flows. It is important to understand and control traffic patterns. Additionally, it is critical to centralize computing facilities to provide greater visibilities.

OSI Model

The OSI transport layer model includes servers, PC workstations, applications, router and switch (The OSI Model: applications, devices, and protocols related to the OSI model Layers. The router is used as the network layer. The OSI model router (the network layer) allows an all

through logical addressing system. The firewall device is the transport layer of the OSI model. The device provides an all through communication between the end devices in the network. The company currently uses the internet layer as the source address and the destination address to enable data movement between the Transport layer and the network access layer.

VISIO DIAGRAM



Physical Network Devices

SNHUEnergy Inc. uses a variety of physical network devices such as routers, switches, physical servers, firewall equipment, and PCs to connect internet users internally and externally.

1. Routers are network layer devices that function by forwarding IP packets from one network to another and can connect dissimilar LANs on the same protocols. The router

restricts broadcasts to the system and acts as a default gateway. The router also performs protocol translation, for instance from wired Ethernet to a wireless network

2. Switches are linkage ports of an Ethernet network that work at the level of LAN (Local Area Network). Devices such as computers and laptops are connected to them through twisted pair cabling. Switches operate in full duplex mode where can send and receive data from the switch simultaneously. Switches enable the connection of office PCs and other hardware such as printers to the network.
3. SNHUEnergy Inc. also uses hardware firewall the router and the internet connection, and hence all devices connected to the router will be protected by the firewall. The firewall performs the functionality of controlling the access of network to trusted sites. The device plays a vital role in the enforcement of a security policy for communication between systems.
4. Physical servers- this is a piece of equipment that provides a mainframe for communications, data storage and processing big ranges of information. Servers facilitate the operation of different applications such as accounting and operations at SNHUEnergy Inc.
5. PCs- these are the access points for end-users through which data is accessed, and applications are executed. SNHUEnergy Inc. has PCs on every employees' workstation as they facilitate most of the organizational operations.

Critical Traffic Patterns

SNHUEnergy Inc. serves an extensive clientele and also conducts a lot of work simultaneously. Hence the company relies heavily on the efficiency of its network. However, the performance of a system is often affected by a variety of variables. Reviewing the critical traffic

patterns of the network could help in understanding the interface better and hence provide opportunities to improve efficiency and reliability.

Service (Voice over Internet Protocol [VoIP])

The Wireshark highlights the interactions between IP address 67.16.104.172 and a private network 10.0.6.73 through a Real Time Protocol (RTP). RTP specify the way programs manage the real-time broadcast of multimedia information over unicast or multicast network services. Hence, these IP patterns signal the use of Voice over Internet Protocol [VoIP] which may include audio or video real-time transmission. The Wireshark interaction has a defined source and destination and only shows where one IP is located. This could be communication between a client and a customer (Source) to the company (target).

Application (Structured Query Language [SQL])

Drawing from the Wireshark capture, a pattern of sending data and receiving can be observed on Private Networks 10.0.8.73 and 10.0.8.42 over Transport Control Protocol (TCP). This interactions also have a protocol labeled MySQL between these two IP addresses. The MySQL protocol is a relational database management system that uses SQL and is suitable for adding, accessing and managing content in a database. Therefore, these IP interactions show that the database is in use and data is sent and received in both ways. Ideally, this can be interpreted as one IP address, let’s say 10.0.8.73, an employee is editing data on payrolls and sending it to a supervisor on 10.0.8.42, which reviews and sends it back to the employee. This is the most prominent pattern in the Wireshark signaling that most interactions in the organization take this format.

Network Management

The capture also shows a device with an IP address 127.0.01 registered as a source and a destination connected through TCP. Given the fact that SNHUEnergy Inc.'s network is switch based, the network device is a switch. Also, the fact that the source and destination are the same during these interactions signals the presence of performance issues. This probably happens because there is more than one layer of two paths between two endpoints (Bailis & Kingsbury, 2014). The effect is unreachability of the destination, and every user loses the ability to communicate on the network until the issue is solved. To address such issues, SNHUEnergy Inc. needs to ensure constant maintenance that assures proper connection of network devices.

Other Interactions

Also, private use network 10.1.0.73 communicates back with address 10.1.0.248 through a Secure Shell (SSH) which is a method of secure remote login from one PC to another. The use of SSH indicates remote login from that occurs from a known IP address. The reciprocal action is an interaction between IPv4 10.1.0.248 and 10.1.0.73 over through a TCP. This could signal access encrypted data and transmission through TCP assures data integrity persists.

Patterns across the Infrastructure

SNHUEnergy Inc. has offices in Dallas and small facilities in the central United States. The Dallas office performs most if the activities which include facilitating communication with the smaller facilities. In this office, the server enables the use of applications such as email, accounting packages, payroll, human resource, and IT infrastructure management. This information is conveyed through a switch-based network, through the router to a client PC within the Dallas network or the other facilities in the central United States. Communication over the phone or video for the offices require related equipment's and applications which are compatible

with VoIP. The information in the VoIP system, data is transmitted over the switch which conveys it to the router which in turn communicates the information through the LAN to the other end.

Performance Issues

SNHUEnergy Inc. plans to expand by adding three regional offices in Kansas City and Houston. Also, the company plans to increase the number of employees by 50% annually for the next two years. This translates to increased traffic on existing infrastructure as more devices will be connected to the network to facilitate communication and run critical applications. The consequences of having more traffic on the current network include network congestion which may result in outages, slow connections, and potential data loss. For instance, VoIP applications require high-level traffic, and in any case, multiple VoIP actions run concurrently on the four offices with other critical applications such as MySQL, the network will be slow and have outages. Ideally, network congestion occurs when there are too many packets present in the network causing a delay on the route (Bhatele et al., 2015).

Also, more employees mean more physical devices such as PCs. In any case, the current network devices such as switches are not updated and increased in number; communication will be regularly interrupted. Broadcasts storms occur due to connections of many devices to one subnet. Outages, interruptions, and slow connections hinder the efficiency of employees thereby affecting the ability of the organization to operate and deliver its mandate (Franklin et al., 2014).

Security Issues

Security protocols are mandatory for SNHUEnergy Inc. These will help the company avert threats, protect organizational data and address risks and vulnerabilities. With the increase in employees, devices, and traffic, security should be managed keenly. If the network

architecture isn't improved, increased traffic and devices will increase endpoints vulnerabilities presented on the PCs end. Data on emails, billing, payrolls, HR, and accounting may be susceptible in any case of an attack. For instance, if a new employee connects an unauthorized device on the network, the whole network may be at risk of an attack. Also, without updating servers, backups may take long to load and hence present risks of data loss.

Addressing these security issues can be done by updating and expanding the network architecture to suit the increased traffic. This could include increasing the number of switches and introducing redundancy and aggregate links. After upgrading the system, it is imperative to train all the existing and new employees on the usage of the new policies and strategies to ensure the safety of the network (Sinkovics et al., 2018). Also, the devices will require authorization from the network administrator before being allowed to access the network (Sandberg et al., 2015). Furthermore, with increased traffic and employees, SNHUEnergy Inc. needs to update its organizational security policy to limit access to different organizational data.

Future Network Architecture

Future Communication needs

The future communication needs of SNHUEnergy Inc. include;

I. Increased network capacity and stability to cater for the new task force and increased operations.

II. Efficient network infrastructure that allows a stable flow of data between the headquarters in Dallas, to the three new offices in Kansas and Houston as well as the smaller offices in the central of United States.

III. Reliable access to the critical applications that allow HR, IT, billing, payroll, accounting, and operations departments to perform their tasks efficiently

IV. Extension of the company's services across a Wide Area Network (WAN) by using TCP/IP communication processes.

V. More computing density and capabilities. The increased number of workers will lead to improved data traffic. Hence, there will be a need for more processing capacity.

VI. Proper configuration of network security to safeguard the organization against malicious attacks and ensure that organizational data is appropriately handled and secured.

VII. Network performance in terms of bandwidth and speed. Speed and higher bandwidth will ensure efficiency and productivity regardless of the increased workforce and operations.

Future Network Architecture

SNHUEnergy Inc. needs a future-proof network architecture that will help the company meet its communication needs, security concerns, and increased data traffic. The redesign of the network will take into consideration several critical variables such as security, cost, efficiency and performance of the system. Ideally, the new design will allow SNHUEnergy Inc. to move from a small network covering up to 200 devices to a medium size network that provides services for 200 to 1000 devices. It will entail upgrading of existing network infrastructure and the addition of new systems that will improve the capabilities of the network. Besides, additions will include new designs and layouts of network infrastructure in the new branches, integrating new security measures, and adding new network applications for database management or content networking. Changes to existing infrastructure will include improving the efficiency of network addressing as the system uses TCP/IP and enhancing the quality of existing network services.

The redesign will introduce the hierarchical Network design with three primary layers; core, distribution, and access and improve its capabilities. In any network hierarchical model, the core layer is tasked with transporting large chunks of data quickly and reliably (Taft & Engineer, 2016). In the case of SNHUEnergy Inc., routers and switches will facilitate high-speed connectivity as the core layer connects offices branches and a server farm to be located at the headquarters in Dallas.

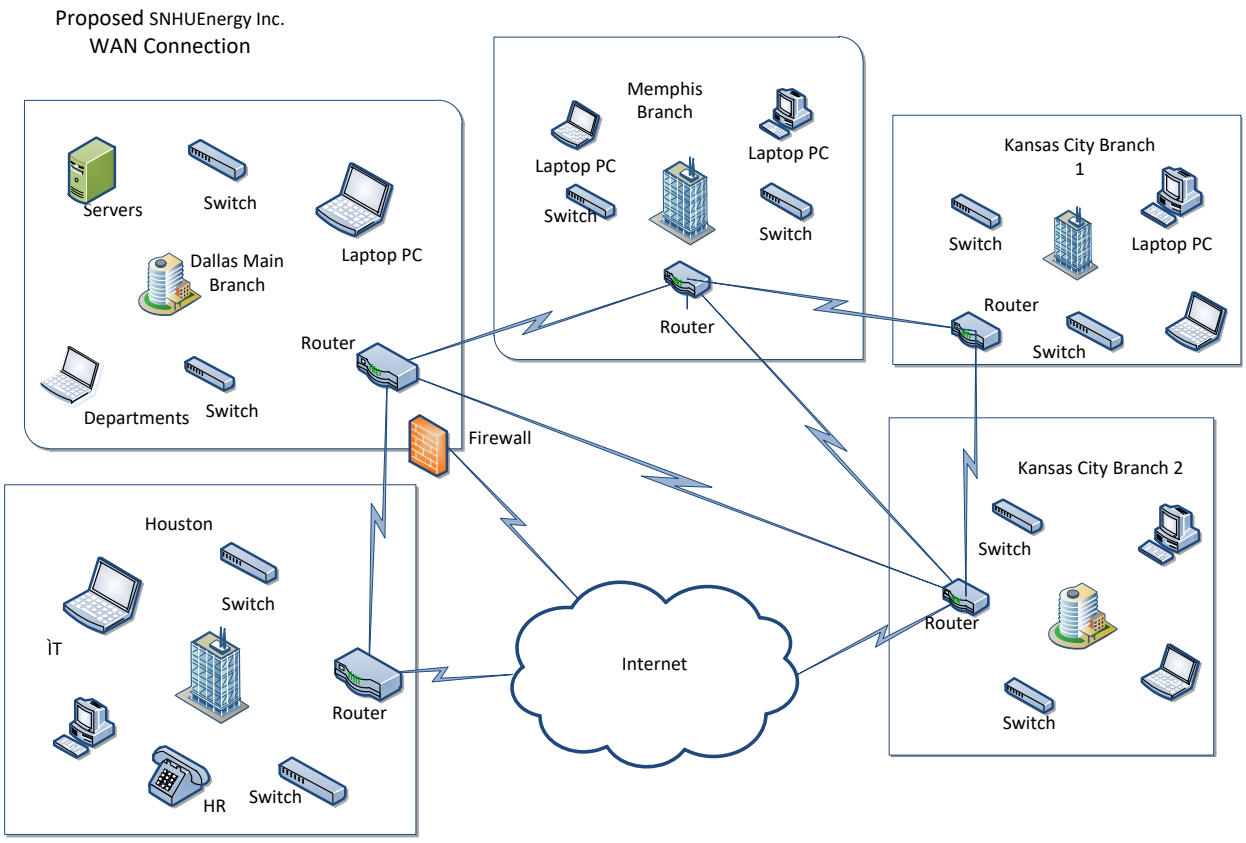
The new network will entail Aggregate WAN links and redundancy and load balancing connections to the devices to enable the internet, extranet and WAN access. These introductions into the system will guarantee that devices have alternative pathways to direct data in the instance of failure. Further, this layer will also serve as the point for installation of Access control Lists (ACL) which will restrict access and thwart unwanted traffic from inflowing to the system (Zhang et al., 2015). Placing ACLs is a necessary security measure that will safeguard SNHUEnergy Inc. organizational data and minimize vulnerabilities of the network. Additional measures with the aim of assuring security, reliability, and efficiency of the network will ensure that core routers and switches have dual power supplies and fans as well as management and maintenance routines (Owais & Osman, 2018).

On the distribution layer, the goal will be to filter and manage traffic streams, enforce access control policies, and separate the core from the access layer. Redundant paths will be used to ensure that the system can survive a link or failure. This layer will be used to institute the policy of the network. The policy will ensure routing updates, routing summaries, address aggregation as well as VLAN traffic, and have a primary mandate of securing the network and preserving resources by preventing unnecessary traffic.

The access layer of the network will cover all the end devices connecting to the network in the organization. Due to the scale of this layer, it will succinctly define the services and devices that are in every branch and at the edge of the network. This layer will help in controlling user access to internet resources and also ensure that the network meets the capacity needs of the organization (Al-Fares et al., 2008). Due to the increased demands of the SNHUEnergy Inc., the network will have a wired infrastructure as well as wireless access points. Each floor of the Dallas office and the other offices will have a wiring closet that will facilitate cabling within the different departmental offices.

At the endpoints, application classification will be conducted to prioritize and mark traffic. Devices on the endpoints will have to be authenticated to limit the entry of intruders into the network (Shan & Liao, 2016). The new network will retain the existing Secure Shell (SSH) and also update the security policy of SNHUEnergy Inc. on setting a password, installation of unauthorized applications and training on the usage of the network. Addressing vulnerabilities and implementing the network though phasing will ensure that SNHUEnergy Inc. has an efficient, stable and reliable network apparatus that fulfills the communication needs of the company, while also ensuring success and providing more space for growth.

Proposed Network at SNHUEnergy Inc.



Planning and security

Performance

The expected performance issues at SNHUEnergy Inc. are due to an increase in the number of employees and the expansion of the network. Traffic flow is based on TCP/IP which has a blunt flow algorithm and therefore if the receiver or interface can't handle the speed that the sender is working, showed by packet loss timeouts, or an excess of out-of-order packets, network flow drops to half the rate. When the speed ramps up again, it becomes slower than the first time. These recurrent performance issues can be solved through TCP optimization which aid in avoiding network drops and out-of-order delivery or triggering TCP flows directly.

TCP optimization can be done through network prioritizing. This will ensure that SNHUEnergy Inc. has control over how bandwidth is consumed. Traffic shaping will ensure that even though the number of users has increased, specific vital applications, devices, or users get bandwidth. Also, it can be used to limit bandwidth to specific users, devices, or applications. This approach will ensure that the performance of critical applications receives priority and runs undisrupted. For instance, the accounting and operations can be prioritized due to the applications used in the department. Additional policy measures include the creation of policies that can eliminate traffic. For instance, setting policy on the websites to be avoided. Social media sites such as Facebook and streaming sites should be avoided. This can be done through the establishment of firewall rules, and content filtering packages. The goal of these policies will be to reduce traffic in the organizational network

Network Management Tools

Network management tools will be used to facilitate fault management, configuration management, performance management, security management, and accounting management. A Simple Network Management Protocol (SNMP) tool will be used to detect, isolate, notify and correct faults in the system. SNMP will also be also be widely applied to manage operations, network devices, and networks. The platform has been preferred due to the ease of integrating solutions that support the increasing number of solutions. With the increased number of network components and application to the network, the Solstice Enterprise Agent (SEA) is recommended to ensure flexibility and dynamic management of multiple devices. SEA allows the integration and use of SNMP-based legacy agents but has master and Sub-agents that facilitate the management of different components and aligned explicitly with for applications.

This technology also has a software development kit that will allow the creation, release, and installation of sub-agents within the network.

The main parts of the SEA package include SNMP and Desktop Management Interface (DMI) which mediates between management applications and components residing in a system. The potential benefits of using SNMP include an ease in management as the protocol will allow network administrators to monitor key parameters of network devices constantly and the uniform GUI based reporting facilitates easier monitoring. On the other hand, DMI assures the management of network elements such as PCS, routers, and workstations. This comprehensive management protocol will ensure that the company installs all ACLs and firewalls and components and application used within the network are well managed and monitored. Generally, the potential benefits of the Sun Solstice tool will be a reduced downtime of network devices, higher performance of networks, and faster and more predictable response times.

Changes to existing devices

The new network will also require changes and upgrades of the existing devices. The new network will have a wide variety of new end-user devices. The active devices to be added include firewalls and content filtering devices that will enable the company to monitor the flow of packets in the network. Content filtering will entail web filtering, screening, email filtering, screening of e-mail and other unauthorized access. Further, Intrusion Detection systems will be used to monitor malicious activities in a network, log information about activities and take steps to stop them. They facilitate an alarm on detection of an intrusion, drop the packet and reset the connection. In this network, intrusion detection systems can prevent TCP sequencing and correct Cyclic Redundancy Check errors. Additional measures can include the use of penetration testing

devices which are preventative devices that could guide upgrades and changes on the system in the future.

Challenges

Security is one of the key challenges that will need to be addressed adequately. Threats are ever changing, and the organization has to stay ahead by ensuring that they are up to date with new systems and identified threats. Further, the organization is growing, and this has facilitated a continuous increase in capacity. The company has to ensure that current users (employees) are well versed with the security protocols enacted by the new infrastructure. Endpoints have been recognized as the biggest challenge and have to be addressed before implementation of the new system. Further, the future network will introduce wireless networks. The wireless network will introduce mobile devices that need strategic coverage.

Even though users can be unpredictable, it is imperative to train and educate all end users on new security protocols and the ACLs. This can also be used to create awareness on the organization and call for more vigilance in operations. Besides, it is a step towards mitigating endpoint vulnerabilities. Also, before the implementation of wireless security networks, it is imperative to define the wireless security policies such as the activating 802.11 encryption that makes data unintelligible to unauthorized users. Also, the wireless network will be on a separate VLAN to ensure that breaches on the wireless network do not reach corporate servers. Besides, the deployment of wireless LANs has to be coordinated with the employees who will be informed of the authorized access points and approved vendor products. Since the current state does not have wireless LANs, this implementation has to be done correctly.

Overall Risks

One of the core principles of cybersecurity is ensuring that the network is above standard and up to date. This principle provides that the company is well prepared to address the ever advancing threats. The combinative risks of attacks, and intrusions increases if the company fails to keep the network on the standard. Standards include continuously maintaining and monitoring fortified network defenses, having up to date security protocols for devices, applications and components of the network, and having industry recommended systems that could help secure the network. Also, endpoint users have to be aware of the potential risks and the practices that ascertain the safety of the network. Failure to achieve this will increase end session management weakness and poorly defined gaps. Therefore, SNHUEnergy Inc. has to ensure its network services have been kept above standard.

References

Achetson, K. (2014). The Seven Layers of Networking. Retrieved August 19, 2017, from http://blog.boson.com/bid/102913/The-Seven-Layers-of-Networking-Part-III

Al-Fares, M., Loukissas, A., & Vahdat, A. (2008). A scalable, commodity data center network architecture. In *ACM SIGCOMM Computer Communication Review* (Vol. 38, No. 4, pp. 63-74). ACM.

Architecture evolution for automation and network programmability. (2014). Retrieved August 6, 2017, from https://www.ericsson.com/en/publications/ericsson-technology-review/archive/2014/architecture-evolution-for-automation-and-network-programmability?fromDate=2014-01-01&categoryFilter=ericsson_review_1270673222_c&toDate=2014-12-31

Bailis, P., & Kingsbury, K. (2014). The network is reliable. *Queue*, *12*(7), 20.

Bhatele, A., Titus, A. R., Thiagarajan, J. J., Jain, N., Gamblin, T., Bremer, P. T., ... & Kale, L. V. (2015). Identifying the culprits behind network congestion. In *Parallel and Distributed Processing Symposium (IPDPS), 2015 IEEE International* (pp. 113-122). IEEE.

Franklin, M. J., Ghodsi, A., Hellerstein, J. M., & Stoica, I. (2014). Coordination avoidance in database systems. *Proceedings of the VLDB Endowment*, *8*(3), 185-196.

Harrell, R. (n.d). Understanding the network application environment. Retrieved August 19, 2017, from http://searchenterprisewan.techtarget.com/tip/Understanding-the-network-application-environment

Harrell, R. (n.d.). Understanding the network application environment. Retrieved August 19, 2017, from http://searchenterprisewan.techtarget.com/tip/Understanding-the-network-application-environment

Henderson, R. (2013). Network Architecture of The Future: It's now. Retrieved August 6, 2017, from http://blog.mavtechglobal.com/blog/2013/10/01/network-architecture-of-the-future-its-now

Owais, M., & Osman, M. K. (2018). Complete hierarchical multi-objective genetic algorithm for transit network design problem. *Expert Systems with Applications*, *114*, 143-154.

Ranbe, R. (n.d.). What Happens if a Firewall Is Disabled? Retrieved July 9, 2017, from http://smallbusiness.chron.com/happens-firewall-disabled-62134.html

Sandberg, H., Amin, S., & Johansson, K. H. (2015). Cyberphysical security in networked control systems: An introduction to the issue. *IEEE Control Systems*, *35*(1), 20-23.

Shan, Z., & Liao, B. (2016). Design and Implementation of A Network Security Management System. *arXiv preprint arXiv:1609.00099*.

Sinkovics, N., Hoque, S. F., & Sinkovics, R. R. (2018). Supplier Strategies and Routines for Capability Development: Implications for Upgrading. *Journal of International Management*.

Taft, J. D., & Engineer, C. D. (2016). *Distributed intelligence for physical networks: Sensing, data and analytics, control, and platforms. part 2: Data and analytics*. Technical report, Cisco Systems.

The OSI Model: applications, devices, and protocols related to the OSI model Layers. (n.d.). Retrieved July 9, 2017, from https://www.examcollection.com/certification-training/network-plus-osi-model-application-devices-and-protocols.html

Zhang, R., Wang, J., Wang, Z., Xu, Z., Zhao, C., & Hanzo, L. (2015). Visible light communications in heterogeneous networks: Paving the way for user-centric design. *IEEE Wireless Communications*, *22*(2), 8-16.