Comprehensive and Secure Networking Solution

Liam Bergerson

CSU - Global

ITS315-1

J. Leaston

11/7/21

Table of Contents

Abstract

Rocky Mountain Corporation requires an upgrade to their existing networking infrastructure. This proposal will contain the recommended network topology, the network devices to be used on the network, the encryption methods, and the network protocols used. Internet Protocol (IP) infrastructure will be discussed to ensure proper IP class assignment and deciding which portions of the network will be using Dynamic Host Configuration Protocol (DHCP) and which require static IP addresses. Lastly, the security aspect will be discussed to ensure the proper policies are implemented and the proper countermeasures are in place should any malware or viruses infect the system in order to prevent or decrease the exposure from compromised information.

Introduction

Your company currently has a 50 user client-server based network using the WPA security standard and with no additional security outside of the defaults that were put in place. In its current state, company information is vulnerable and easily compromised. In this proposal, I will illustrate the measures that need to be implemented in order for your company to have the highest levels of security required to protect valuable company information. This proposal will also allow for expandability up to 500 users in 12 months. This proposal will talk about what network topology will be used, the network devices used, encryption methods, IP infrastructure, policies used, and countermeasures for malware and viruses.

Section 1: Topology (type of network) and network devices

The type of network topology that will be used is the star topology. The star topology consists of a central host or server that all of the desktops and laptops can connect to. The star topology will be chosen because it is a balance between cost and resources, security, and user experience. The two other topologies that were considered were the bus and mesh. A bus topology is severely outdated and hardly used because all of the devices are connected to a single bus. If there is a break in the bus, all of the devices will be disconnected. In the full mesh topology, it is far too expensive and exhausts resources because a cable connection will be required to connect every single device together on the network. A star topology is a nice balance because only a single connection is needed to connect the device to the central server and any problems or breaks in the connection will only disable that device and not every single device connected to the network. However, if there are any problems with the central server, all of the devices will lose connection to the network and staff will need to troubleshoot the network as soon as possible to bring systems back on online.

Internal and external networking components

The internal networking components will be what's inside of the desktops and laptops. For the desktop, the internal networking components will be a wired network interface card with a 1 Gigabit per second connection speed. Some motherboards do not include ethernet connectability so having that wired network interface card will guarantee ethernet support for the desktops. The 1 Gigabit connection speed will be an adequate speed for the operations that are being run at this company. This will require

that the network topology must be able to support a 1 Gigabit per second connection speed. The internal components that will be in the laptops will be a wireless network interface card. The laptops are more portable than their desktop counterparts so a wireless network interface card will be required for easy connection to the network wherever the laptop is. Again, a 1 Gigabit connection speed is the goal for fast and easy operations.

The external networking components will be what's outside of the desktops and laptops that run the network. The first component that will be required is a modem(s). Modems are what receive the internet connection from the internet service provider. A connection to the internet is not possible without a modem. The next networking component required are routers. Routers are crucial to the topology because they perform a wide array of functions. Routers manage and assign IP addresses, act as the local domain name service, send requests over the internet on behalf of your device and return results, etc. (Peters, 2021). The next networking component required are switches. Switches extend the number of desktops that can be plugged into the router via ethernet cable. Since routers only have a few ethernet ports, multiple switches are required for up to 500 connections. In fact, a switchboard will be required to accommodate the high number of desktop connections. The last external networking component that will be required are wireless access points. Since there are laptops that need to be connected to the network, wireless access points are required to accommodate those laptop connections. Wireless access points can be plugged into the switch that's connected to the router and will serve as the Wi-fi connection that the laptops need for network connectivity and retain their portability.

Cryptography method

The cryptography method that will be used on all data at rest storage devices is symmetric encryption with the advanced encryption standard. Symmetric encryption uses the same key for encrypting and decrypting a packet (uCertify, n.d, pp. 96). Symmetric encryption is faster than its counterpart, asymmetric encryption, which uses two different keys for encryption and decryption of packets (uCertify, n.d, pp. 96). The advanced encryption standard will be used because it uses 128-bit, 192-bit, and 256-bit version keys compared to the data encryption standard which only uses a 56-bit key (uCertify, n.d, pp. 96). Transport layer security is another encryption that could be considered. Transport layer security is used to secure the data that travels between a web browser and website via hypertext transfer protocol secure (Lake, 2021).

Network protocols

A variety of network protocols will be used on this network topology. The first protocol that will be used is Dynamic Host Configuration Protocol (DHCP). DHCP assigns IP address information including IP address, subnet mask, Domain Name System (DNS) IP address, and default gateway address to devices connected to the network (uCertify, n.d, pp. 21). DHCP will be preferred over static assignment because DHCP automatically assigns IP address information to each device that connects to the network. If a static protocol is used, IP address assignment will have to be assigned manually to each device. For a 500 user network, DHCP is crucial. A DNS server will be another protocol used on the network. A DNS server converts the domain name (www.ciscopress.com) into an IP address that the router can read and vice versa

(uCertify, n.d, pp. 21). There are two mailing protocols that will be used on the network. The first protocol is Internet Message Access Protocol (IMAP). IMAP is used to access received emails from multiple clients. Post Office Protocol 3 (POP3) is the other mail receiving protocol that can only receive emails from one application. IMAP will be preferred over POP3 if email needs to be accessed from multiple locations. The other mail protocol that will be used is Simple Mail Transfer Protocol (SMTP). SMTP is how emails are going to be sent to other employees on the network. The next protocol that will be used on the network is Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP will be used because it is a connection based protocol. TCP/IP is reliable and ensures end-to-end delivery. TCP/IP uses a 3-way handshake to ensure that the data arrives at its destination unharmed. User Datagram Protocol (UDP) is another protocol that can be used instead of TCP/IP but it is far less reliable than TCP/IP. UDP is a connectionless protocol meaning that there is no guarantee that the information will arrive at its destination unharmed. UDP does not offer any 3-way handshake or acknowledgements that the data has arrived at its destination making it unreliable and does not ensure end-to-end delivery. Another protocol that will be used that is related to the TCP/IP protocol is Internet Control Message Protocol (ICMP). ICMP is in charge of error reporting in the event that a file has not arrived at its destination (Cooper, 2020). For example, if a packet is too large for transfer the router will drop that packet and send an ICMP error report notifying the source that the packet was dropped.

Network capabilities

The network needs to be capable of doing a variety of operations including printer and scanner connectability, file sharing options, managing resources in a central location, and allowing internal users to connect to the internet and external users to connect to the Local Area Network (LAN). All of the desktops and laptops will be connected to the printers and scanners via ethernet or Wi-fi. The printers and scanners will be connected to a switch on the network via ethernet cable. For file sharing options, each branch of the company will be on different subnets. Each branch can share files to other devices on the subnet and other devices that aren't on that subnet cannot see the files being shared. All of the desktops and laptops will all be connected on one subnet for only printer and scanner access as well as internet access. All of the modems and routers will be in a central server room of the company building. All of the switches and wireless access points will be on each floor. The switches will be on a switchboard on each floor. The wireless access points will also be on each floor for optimal wireless signal. All internal users will be connected to the internet via either ethernet or Wi-fi. The external users will have access to the LAN through a Virtual Private Network (VPN) connection to ensure information is accessed and transferred in a safe and secure way.

Network budget

The budget for this chosen topology will be estimated at $20,000. That will include the networking devices needed to accommodate for 500 users: Modems, routers, switches, wireless access points, Network Interface Cards (NICs), etc. That will

also include the server room needed for the star topology, encryption methods, printers, scanners, and network protocols used.

Section 2: IP Infrastructure

The network will be based on a DHCP structure for IP addresses. Since the company needs around 500 users to connect to the network, DHCP will make it easier for IP address assignment since it assigns IP addresses automatically. Static IP addresses have to be configured manually for each device and doing that for 500 devices will take longer than assigning IP addresses automatically like with DHCP. However, the printers and scanners can have a static IP address because there are limited printers and scanners that are used. I would recommend assigning a class B IP address because the company is, even after the growth to 500 employees, still a medium sized company and class B IP addresses are the best for medium sized companies.

Remote access plan

A remote access plan is required for safe and secure connections to the network from off-site. With a good remote access plan, the company can take on employees from anywhere in the country or even in the world. Multi-Factor Authentication (MFA) will be the first thing that's included in the remote access plan. MFA may be a bother to do every time information needs to be accessed but it is crucial that the information stays safe and protected from breaches that could result in stolen information. Access control will be required as well. Each user will only be given access for their certain

duties and nothing more. If all users were given access to everything, an account breach will result in the hacker having access to everything. Lastly, the remote access plan must support zero trust based technology. Zero trust based technology will ensure that every single user is authenticated using multi-factor authentication regardless of their position in the company and regardless of whether the connection is internal or remote (Gondoly, 2021).

Section 3: Security

Secure access control

Secure access starts with a good password policy. A good password needs to be easily remembered but complex enough so that it doesn't get cracked. A good password needs to be short enough so that it doesn't need to be written on a piece of paper which will then have a chance at being lost and needing a password reset. I recommend having a password that is 8+ characters with lowercase and uppercase letters, numbers, and special characters. A remote access policy is necessary for secure access, especially for remote users. There are a couple of goals of a remote access policy. The goal is to provide appropriate access for remote workers to maximise productivity and protect information assets from loss or damage (Simon, 2017). Some guidelines that Simon (2017) provides are what should be included in a remote access policy. Hardware and software should be configured for remote access, including firewalls, antivirus, and antimalware. Encryption policies should be in place for secure file transfer. Security, confidentiality, and email policies should be in place. Policy compliance and enforcement should be required. If policies are not followed and

enforced, there isn't a point to implementing them. The remote access policy should also include role based access so that employee accounts have the access only for their duties and nothing more. The last policy that's needed is an Acceptable Use Policy (AUP). Sheil (2020) highlights what should be included in an acceptable use policy. The AUP should define systems covered in the policy. For example, internet devices, email, and browsing. The AUP should clearly illustrate that all devices in the workplace are strictly used for business purposes only. The AUP should outline the consequences for non-compliance. The AUP should not interfere with their work and establish what websites are allowed and which are prohibited. Finally, the AUP should require users to lock their computer when they step away and never leave unlocked devices unattended.

Protecting the network from malware

In the event that an employee accidentally downloads a virus or a piece of malware that should compromise the information of the company, proper antimalware and antivirus software should be used. Antimalware and antivirus software must be installed and run on every device and be documented when it is updated. User training should be required for every employee to ensure that phishing is prevented and that they are able to have some resistance to social engineering. Users should also be trained to identify unsecured and fraudulent websites and not to be interacted with in any way. Lastly, hardware firewalls must be installed in the routers to block any unauthorized files attempting to be transferred in and out of the network.

Conclusion

The recommendations I have made for your company will provide expandability for 500 users in 12 months and provide the highest security required to keep your information confidential, available, and have integrity. The network topology used is the star topology in order to accommodate for 500 users in 12 months. The network has the proper encryption methods used to maximize security. The network protocols used on the network will allow proper business operations over the network. Each device will be configured with DHCP to ensure easy IP address assignment for new devices on the network. The printers and scanners will be given a static IP address because there are minimal printers and scanners in the office. The policies discussed will ensure that employees are browsing correctly to mitigate the chances of security breaches.

References

Cooper, S. (2020, August 30). *What is ICMP? The Internet Control Message Protocol Explained*. Comparitech. Retrieved October 27, 2021, from https://www.comparitech.com/net-admin/what-is-icmp/

Gondoly, K. (2021, May 13). *Designing a secure remote access plan*. ITProPortal. Retrieved October 27, 2021, from https://www.itproportal.com/features/designing-a-secure-remote-access-plan/

Lake, J. (2021, March 18). *What is TLS and how does it work?* Comparitech. Retrieved October 27, 2021, from https://www.comparitech.com/blog/information-security/tls-encryption/

Peters, A. (2021, January 12). *Do You Need a Modem and a Router?* Lifewire. Retrieved October 27, 2021, from https://www.lifewire.com/do-i-need-a-modem-and-router-4686028

Sheil, J. (2021, May 13). *Electric AI, Inc.* Electric. Retrieved October 29, 2021, from https://www.electric.ai/blog/what-is-an-acceptable-use-policy

Simon, B. (2017, August 15). *Increase Productivity While Maintaining Organizational Security with an Effective Remote Access Policy*. Smartsheet. Retrieved October 27, 2021, from https://www.smartsheet.com/effective-remote-access-policy

uCertify. (n.d.). CompTIA Pearson-N10-007-Complete. *uCertify.com.* (pp. 21, 96)