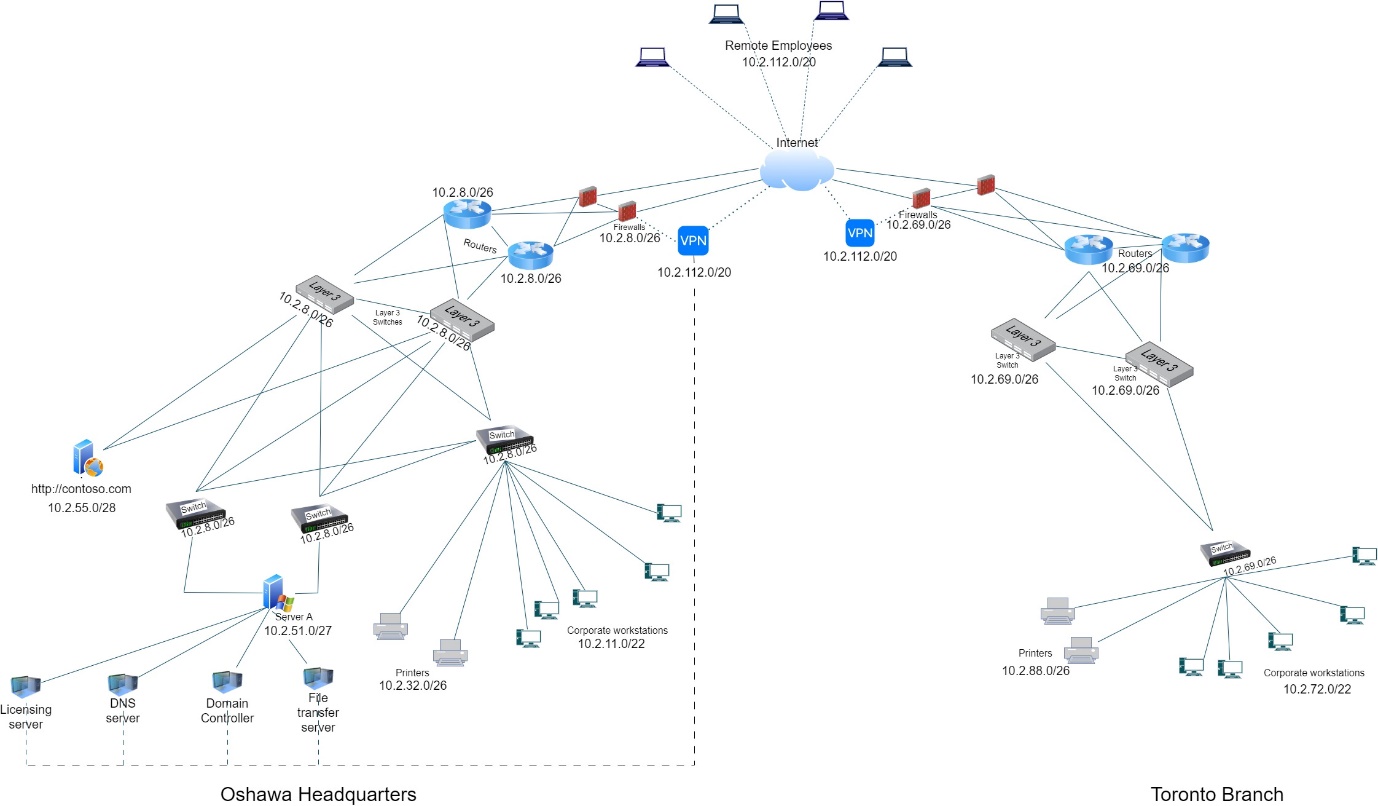


**Deliverable – Network Design**

**Bhargav Gosai**

**(**

1. **Provide a diagram of your recommended network topology for the Contoso Company. The diagram includes the devices in the network, connection types between devices, the IP addressing scheme, and additional network devices you are proposing.**

****

**[Network Design]**

1. **Provide reasoning for the network topology. Categorize the design into the four basic characteristics of a network (reliability, scalability, quality of service, and security).**

To design a network, we need to understand the requirements of the organization first, Contoso is an online store which makes it necessary to reduce all the single point of failures to virtually none in order to keep the store online and prevent network failures. We tried our level best to live up to those expectations and developed a network that compliments the organization needs. The network is developed layer by layer and making a mesh of all the layers together which gives it a unique redundant structure where there are no single point of failures and no single device is responsible for handling the flow of traffic at any certain layer.

We believe a network stands on four pillars of reliability, scalability, quality of service, and security. below is a short description on how we focused on each aspect while designing the network.

**Reliability:** We designed the network in such way that in case of a device failure, the flow of traffic stays uninterrupted. This is achieved this by adding redundant links between devices and adding backup devices where necessary (Placeholder1) (Ashtari, 2022). Each layer is a mesh network in its own and all the layers are meshed together making it a mesh network of mesh networks which pretty much makes sure that network failure does not bother the organization.

**Scalability:** The organization is growing rapidly as they are planning to welcome around 700 new employees in next 16 months. Keeping that in mind, we added additional switches, routers and firewalls so they don’t have to compromise in performance or the functionality. The additional devices are blended in topology in such manner that the redundancy is maximized making these additional devices best of both worlds.

**Quality of Service**: Contoso is a digital artwork on their online store which makes it critical to have their web server up and running all the time, we use dynamic bandwidth allocation to keep the traffic flow in its peak state as slow response time is the last thing an online store would want. Bandwidth allocation helps to manage the traffic flow and dynamic allocation helps us to adjust the available bandwidth according to real time requirements and conditions making the full use of bandwidth and maximizing the network potential.

**Security:** The most important aspect of the network design is to secure the network. And as per the organization they have only one lock room and they don’t have any other security policies. So, to secure the network we provided firewalls and VPNs to protect the network from malicious traffic and DDOS attack they will block the traffic that is not verified or suspicious.We also implemented access control policies so only authorized users can have access to the network and to restrict the unauthorized users. We also created an Access Control List to determine thatwhich user is allowed to access network and which is not. We used Transport Layer Security and Secure Socket Layer for the encryption of data to send the data on network in an encrypted form to protect data from cybercriminals. We used intrusion prevention and detection system to monitor the network traffic and malicious infections. So, they can take some necessary steps to mitigate the risk. They don’t have facility to work from home. So, we added VPNs for remote employees, allowing them to work from home effectively and securely.

1. **Provide the IPv4 addressing details for the table below. Provide a brief explanation for why you chose these subnet sizes.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Location**  **(HQ = Headquarters BR = Branch)** | **End Devices** | **Network ID (CIDR)** | **First Host** | **Last Host** | **Broadcast Address** |
| HQ – Subnet 1 - Management Devices | 15 | /26 | 10.2.8.1 | 10.2.8.62 | 10.2.8.63 |
| HQ - Subnet 2 - Corporate Workstations | 240 | /22 | 10.2.11.1 | 10.2.14.254 | 10.2.14.255 |
| HQ - Subnet 3 - Printers | 22 | /26 | 10.2.32.1 | 10.2.32.62 | 10.2.32.63 |
| HQ - Subnet 4 – Windows Server | 22 | /27 | 10.2.51.1 | 10.2.51.30 | 10.2.51.31 |
| HQ-subnet 5- Web Server | 1 | /28 | 10.2.55.1 | 10.2.55.14 | 10.2.55.15 |
| BR - Subnet 1 - Management Devices | 30 | /26 | 10.2.69.1 | 10.2.69.62 | 10.2.69.63 |
| BR - Subnet 2 - Corporate Workstations | 460 | /22 | 10.2.72.1 | 10.2.75.254 | 10.2.75.255 |
| BR Subnet 3 - Printers | 55 | /26 | 10.2.88.1 | 10.2.88.62 | 10.2.88.63 |
| HQ + BR - VPN workstations | 200 | /20 | 10.2.112.1 | 10.2.127.254 | 10.2.127.255 |

The size of subnet is defined according to the number of end devices on a subnet.

* For HQ subnet-1 we have 15 end devices so we assign 0/26 subnet with 64 IP addresses keeping future expansion possibilities in mind.
* Same situation for all the other subnets, for HQ subnet-2 we allocated 0/24 subnet for 240 devices.
* HQ subnet-3 with 22 devices gets 0/26 subnet. We could give assign 0/27 subnet but that might cause trouble in future if the limit exceeds.
* HQ Subnet-4 gets the size of 32 IP addresses as this subnet is dedicated to windows server and it is less likely to witness a huge jump in number of servers rapidly in near future.
* Finally, there is a DMZ server entirely dedicated for web server since it is public facing.
* Similar to HQ subnets, Toronto branch subnets are also assigned according to number of end devices in a particular subnet. BR subnet-1 is given the size of 64 IP addresses since that subnet has 30 end devices leaving 34 more addresses for future additions.
* BR subnet-2 is for employees and it has 460 end devices listed so we assigned the 0/23 subnet with 510 IP addressed leaving space for 50 more devices if needed in future.
* BR subnet-3 is for printers and has 55 end devices so we assigned 0/26 subnet with 64 IP addresses.
* Lastly, we have VPNs with 200 end devices, keeping that in mind we allocated it the 0/24 subnet with 255 IP addresses.

1. **Vulnerabilities and threats**

Network Vulnerability 1:

**Segmentation of servers:**

One major problem in current network is that web server and data server are on same subnet which makes entire network vulnerable if an attacker manages to hack into web server. Not only attacker can travel across the network pretty easily but can misconfigure the network and steal the sensitive information. Attacks that can occur due to lack of segmentation of server are listed below.

* Privilege escalation
* Data theft
* Insider attacks

1. Privilege escalation: If the attacker gains access of web server, they can use that access to escalate their privilege to gain access of data server and steal or alter information or can compromise entire system.
2. Data theft: If web server is compromised, all other servers would be at risk too as travelling through same subnet will be easy for the attacker and the attacker can easily steal any data available on our servers.
3. Insider attacks: segregation pf duties might prove to be useless if segmentation of network is not done correctly, in this case an employee with web server access can also access data server easily if they want to which is not a good practice for an organization.

Security standards to follow: The solution for this situation is to follow ISO 27001 A 13.1 Network Security Management standard which states that all and any public accessible domains should be inside a De-Militarized zone (DMZ) and the internal LAN should be behind a firewall protection. The idea behind this is that assuming attacker compromises and breaks into our web server, he or she still might not be able to break into our LAN since it is separated from public servers and that way damage can be minimum.

Network Vulnerability 2:

**Open Ports:**

Open ports may not be that big of an issue but considering the situation of our servers we need to make sure that firewalls and ports are not misconfigured. If an attacker gains access to the network, open ports may provide him an easy way to navigate around the network or allow malicious traffic to pass through.

Poorly configured ports may lead to attacks such as:

* Port 20 and 21: Can be targeted to brute force passwords and cross site scripting
* Port 23: Can be used for sniffing and spoofing
* Port 25: Can be targeted for spamming and spoofing
* Port 53: Can be targeted for DDoS attack
* Port 80, 443, 8080, 8443: Can be targeted for SQL injections, Cross site scripting and DDoS attacks.

Security standards to follow: To mitigate the risk related to open ports we should follow the ISO 27001 A 8.20 Network Security Control standard which indicates that network and network devices should be secured, managed and controlled to protect the information in network and other facilities from compromise via network. As ports cannot be closed all the time, it makes firewalls even more important for the network since firewalls monitor and filter traffic flowing through these ports.

1. **Configuration commands  
    a. Password and lockout configuration**

i. Actual CLI commands to configure

* Switch Configuration

S1(config)# line console 0

S1(config-line)# password Contoso@123

S1(config-line)# login

S1(config-line)# exit

S1(config)# enable password Cisco@123

S1(config)# exit

S1# config t

S1(config)# enable secret Contoso@245

S1(config)# exit

S1# conf t

S1(config)# service password-encryption

S1(config)# login block-for 60 attempts 3 within 60

S1(config)# exit

* Router Configuration

R1(config)# line console 0

R1(config-line)# password Contoso@123

R1(config-line)# login

R1(config-line)# exit

R1(config)# enable password Cisco@123

R1(config)# exit

R1# config t

R1(config)# enable secret Contoso@245

R1(config)# exit

R1# conf t

R1(config)# service password-encryption

#### R1(config)# banner motd "Unauthorized Access Prohiited!"

R1(config)# login block-for 60 attempts 3 within 60

R1(config)# exit

**Explanation:**

In order to secure the Contoso network, we'll start by enabling the password on the console so that whenever a user wants to log in to the system, they must input the password to confirm whether they are a verified user or not. Next, in order to improve security, we will enable the password for privileged mode, which details the unique privileges granted to particular users, such as administrators or other senior level users. After enabling this, we will now encrypt the password using enable secret, which will replace the original text with a new encrypted password. You can verify this by executing the show run command. The enable and console passwords are still in plain text even if the password for access privilege mode has been encrypted. To encrypt both passwords, use the service encryption command. And we will add the message of the day for unauthorized users, so whenever any unauthorized person tries to access to the network, they will get the warning message "Unauthorized Access Prohibited. Additionally, we will block logins by suspending the network for 60 seconds and denying access to anyone who makes more than three unsuccessful attempts by using login block command. This will help us to protect from brute-force attack.

**b. Port Security**  
 i. Access Port Workstations

S1# conf t

S1(config)# interface GigabitEthernet0/1

S1(config-if-range)# switchport mode access

S1(config-if-range)# switchport port-security

S1(config-if-range)# switchport port-security maximum 1

S1(config-if-range)# switchport port-security mac-address sticky

S1(config-if-range)# switchport port-security violation restrict

S1(config-if-range)# spanning-tree portfast

S1(config-if-range)# end

ii. Access Port Servers

S1# conf t

S1(config)# interface GigabitEthernet0/2

S1(config-if-range)# switchport mode access

S1(config-if-range)# switchport port-security

S1(config-if-range)# switchport port-security maximum 1

S1(config-if-range)# switchport port-security mac-address sticky

S1(config-if-range)# switchport port-security violation restrict

S1(config-if-range)# spanning-tree portfast

S1(config-if-range)# end

iii. Access Port Not used

S1# conf t

S1(config)# interface GigabitEthernet0/3

S1(config-if-range)# switchport mode access

S1(config-if-range)# switchport port-security

S1(config-if-range)# switchport port-security maximum 1

S1(config-if-range)# switchport port-security violation shutdown

S1(config-if-range)# end

**Explanation:**

We will now enable security on the ports after enabling security on the switch and router. We will thus use switchport mode for that, which switches the port into an access port to connect to workstations and other endpoints. The port security will then be enabled, limiting the number of MAC addresses to prevent DDOS attacks and unauthorized access. We will also set the maximum number of MAC addresses that can connect to the port in order to restrict the MAC address. In addition, we will add the sticky MAC address to safeguard the network. By doing this, the switch will be able to discover the MAC address, and if it is secure, it will store it in memory as a secure MAC address. Also, we will provide the Violation Restrict command, which will close the port whenever a violation occurs, to limit the breach. In order to quickly recover the port after shutdown, we use the portfast command. This will enable the ports to enter a forwarding state without waiting for STP or get stuck in loops. By doing this, the connection time to the port will be reduced.

**c. Router Hardening**

R1(config)# router ospf 2

R1(config-router)# router-id 1.1.1.1

R1(config-router)# network 10.2.8.0 0.0.0.63 area 0

R1(config-router)# passive-interface g0/0/0

**Explanation:**

We will use OSPF (Open Shortest Path First) to harden the router, therefore first, we will set the process id. Now to prevent other devices from joining the OSPF network, we will now configure OSPF to only advertise the necessary networks. Additionally, to increase security, we will use passive interfaces, which will only update OSPF on the designated interfaces, ensuring that it is only shared with trusted devices. This reduces the risk of rouge attempting.

**d. Route to the internet**

**i.** ACL for network

R1(config) #access-list 1 permit 10.2.8.0 0.0.0.63

R1(config) #access-list 1 deny any

R1(config-if) #interface GigabitEthernet0/0

R1(config-if) #ip address 192.168.2.1 255.255.255.0

R1(config-if) #ip access-group 2 in

**Explanation:**

We'll implement the access control list to lessen network traffic. We will then apply this traffic to one interface of the router that is configured with the IP address, define the subnet mask, grant the permit to route the traffic, and refuse all other traffic on the network. This will help us in preventing unauthorized traffic and network access. Moreover, it can be used to filter traffic and block particular ports or protocols, which will reduce attacks performed by malicious sources.

**ii.** Primary and backup default route to the internet

R1(config) #ip route 0.0.0.0 0.0.0.0 192.168.2.57

R1(config) # ip route 0.0.0.0 0.0.0.0 192.168.2.75

R1(config) # router ospf 2

R1(config-router)# default-information originate

**Explanation:**

To avoid network failures, we will use primary and backup default route. So, in case the primary route fails the backup route will help us to ensure the continuous internet connectivity. This can help to assure continuity of operations and prevent network service disruptions.

1. **Purchase recommendations**

**Purchase recommendation 1: VPN service**

In the post-Covid era, where remote work and working from home have become an essential part of arguably every corporation, the importance of VPN servers has increased drastically in order to provide secure and reliable connections for remote workers. Just like any other organization, Contoso also provides the facility to work remotely after the COVID era, and we have kept that factor in mind while designing the network. But just providing remote access may lead to many security issues, such as unauthorized access and data breaches, as intruders might try to break into the network and act as a remote worker, which might not only result in financial loss but may also damage the company’s reputation. Which is why we have decided to implement a trustworthy VPN provider to filter and monitor traffic coming from remote workers.

* **Software recommendation:**

We did some research on which products would be a perfect fit for the company and narrowed down our list to two that might be a good fit for the company network.

1. **Cisco AnyConnect**

Cisco AnyConnect is a VPN solution developed by Cisco that allows secure network connections to remote workers. It offers numerous features such as multifactor authentication, split tunnelling, network access control, threat protection, web security, and endpoint security.

1. **Fortinet FortiClient**

FortiClient is a free endpoint security service that offers VPN connections, web filtering, antivirus, and a firewall. FortiClient’s VPN offers multiple features, such as multifactor authentication, split tunnelling, and endpoint compliance checking.

While both of the software packages seemed to be a perfect match for the company infrastructure, we had to pick only one of them as, despite having enough budget to implement both software in the network, it might not be ideal to have two VPNs in a single network as it might lead to confusion among employees, which can lead to many more complications in the company.

After comparing both software side by side, we came to the conclusion that Cisco AnyConnect would in fact be the most suitable choice for the company due to the various reasons listed below.

* **Compatibility:** Cisco AnyConnect supports a wider range of operating systems compared to Fortinet FortiClient. While FortiClient does support all the commonly used operating systems, it does not offer as many operating system compatibilities as AnyConnect. For example, AnyConnect supports Blackberry, Solaris, Chrome OS, and Windows Phone, whereas FortiClient does not.
* **User-Friendliness:** Both the competitors are user-friendly, but while testing them, our team found the AnyConnect interface to be cleaner and easier to understand. But as user experience is a subjective thing, we cannot judge on the basis of the experience an individual user had. So, we also focused on different factors such as customization options, user guides, and tutorials, which give AnyConnect a slight edge over FortiClient.
* **Security:** Both software offers similar standards of security, which makes it harder to pick one over the other. To come to a conclusion, our team considered the implementation of this software as a factor of security, as almost all the security features are similar, but the functions of these features may vary according to how they are put to use. Having a lot of security features but not having a compatible way to put them to use might make them less effective. which brought us to our previous point of user friendliness. As the features are almost identical, the functions and implementation of these features are comparatively easier to understand and use in AnyConnect due to its user-friendly environment.
* **Additional features**: While there are a lot of similarities in both VPNs, there are some additional features that makes Cisco AnyConnect slightly superior to FortiClient. One biggest additional feature being allowing third party VPNs, AnyConnect allows third party VPNs which can allow the company to have multiple VPN providers at the same time.
* **Changes Required:**

Certain changes will be required in the company environment and network.

1. **Traffic flow:** VPN tends to increase the traffic flow in the network; we will have to make sure that the network can sustain this increase in traffic. If not, changes in the network will be required.
2. **Training and awareness:** The company will be required to provide training programs to employees to make sure the software is utilized correctly.
3. **Management: The** company should provide a dedicated management team to manage and monitor the VPN traffic and troubleshoot.

* **Negative Impact:**

There are a lot of benefits of using VPN for remote workers and it is ideal to use it so, but the one major downside of using VPN is increased traffic flow which might slow down the network’s performance and negatively impacts employee’s productivity and efficiency. as Contoso is expected to grow rapidly in next 16 months, the traffic flow will only increase rapidly and VPN will add more to it, this might slow down the network.

**Purchase Recommendation 2: Firewall Upgradation**

In the current period, businesses are experiencing more stress to strengthen their level of security due to the growing number of cyber threats, including malware, ransomware, and phishing attacks. Each and every type of safety architecture must have firewalls, and upgrading these firewalls can improve security from threats. In addition to secure confidential data and restricting cyber-attack, firewalls provide support in blocking unauthorized access to a company's system by filtering the traffic on the network. Sometimes it is impossible to identify the breach, which results in loss of sensitive data, financial loss, and damage to the company’s reputation. Thus, we made some improvements to the firewall by including certain advanced technologies like an intrusion prevention system and an intrusion detection system. This will help the company identify the threat, block the unnecessary traffic on the network, and secure it from malicious attack.

**Software recommendation:**

We conducted some research to see which product would be the ideal fit for the business and reduced our choice to two programs that would be suitable for the company network.

1. **CISCO ASA Firewall**

The Cisco ASA firewall is a network security device that provides firewall functionality with various security features such as intrusion prevention using signature-based and behaviour-based analysis, inspection of traffic flowing through the network, and access control.

1. **PF Sense Firewall**

PF Sense is an open-source firewall software. One advantage of the PF Sense firewall is that it can be modified to fit the organization according to its needs. It identifies and blocks or allows traffic based on IP addresses, protocols, and applications.

After analysing both Cisco ASA and PF Sense and having a deep discussion with the staff, we came to the conclusion that Cisco ASA would be ideal for the business. Though it is very expensive, Contoso is a large organization. It needs high-level support and advanced features. As with Cisco ASA, it would be beneficial for Contoso to have a tested and popular intrusion prevention system in their organization to get rid of future cybercrimes and malware attacks. The reason for selecting Cisco ASA is mentioned below:

* + **Security Features:** As we all know that CISCO ASA give more features like advanced threat detection, advanced access control policies, next generation firewall. This all features protects network from phishing, malware attacks, etc. whereas on the other side PF sense also provides advanced security features like threat detection but it is not as strong as CISCO ASA because installing new security features using CISCO ASA needs additional hardware or software license but PF sense is opensource and free to everyone.
  + **Scalability:** CISCO ASA is highly customizable and used for large organization as it provides multiple interfaces and higher bandwidth because it works on command line interface and it needs high level of understanding to operate it. On the other hand, PF sense is also scalable but it will not be able to handle the larger traffic because it is user-friendly and it is a web interface it can be easily configured and that will give advantage to the attacker to attack the system. For instance, Contoso is a large organization and is planning to expand and adding new 700 employees and also planning to open new branch so CISCO ASA is the best option rather than PF Sense.
  + **Integration:** CISCO ASA can easily integrate with other cisco products such as routers, switches and other security devices while it would be quite difficult for PF sense to integrate with the CISCO products. CISCO products can work easily with each other and are easy to maintain.
  + **Cost:** PF sense is free and open source used by anyone while CISCO ASA is expensive and needs license but benefit of CISCO ASA is it provides advanced security features, scalability, support and easy integration with other CISCO products.
* **Changes Required:**

Certain changes will be required in the company environment and network.

1. **The implementation of additional security technologies Upgrading the** firewall affects the data loss prevention techniques. So, we will have to plan for the changes that need to be made, and they should be compatible with the new firewall and enable new functions.
2. **Impact on Customers:** Upgrades to the firewall may have an effect on customers depending on the business's operations. The company should provide clients with alternate access methods and let them know in advance about any expected difficulties.
3. **Training Employees:** We should provide proper training to the IT staff and end users to make sure that they get completely used to the new functionalities and features of the upgraded firewall and also get used to the new policies and procedures.
4. **Network Topology:** When we upgrade the firewall, we have to change the configurations of the routers or add or remove network segments.

* **Negative impact:**

Even though firewall upgrades are beneficial for systems, upgrading a firewall might require additional education for IT personnel or end users in order to understand its new functions and features. These alteration procedures may take longer and cost more as a result. Company operations may be disrupted if a firewall upgrade requires leaving the system offline for a while.