Acknowledgement

Complete this assignment successfully I am expressing my thanks to almighty for his special kindness to give me this opportunity. So, I would like to thank our course instructor for his continuous support, supervisor, suggestion and providing me valuable information that was very needed and valuable for the completion of this assignment successfully.

Introduction:

Mary Lane Cosmetics is high quality beauty products Manufacturer Company. This company runs LAN technology with windows server 2012 R2 besides office staff PCs running windows 10 professional OS. Now this company business update purpose they want to run E-commerce infrastructure business policies with ISP based LAN Network besides they don't want to use Wi-Fi network technology. So, LAN network technology with ISP connected network this company query from me how much additional risks with cyber Attack can get when they develop this network Architecture and suggested better solution for safe and secure network for their.

Task 1

a) Five most important electronically held assets information for risk assessment assumption in hare:

a. Organization's crucial data.
b. Customer record data.
c. Employee's information data.
d. Financial and product records data.
e. Transactions and orders Records data.

b), c), d):

Asset list with the main security threats and where impacts on the company explained on a table based:

Asset	Threat	CIA?	Likelihood	Impact	Risk
Organization's crucial data.	Server failure	A	low	medium	Low
	Employee theft	C	low	high	Medium
	Phishing	C	medium	high	High
	Malware	I	medium	medium	Medium
	DDoS attack	A	Medium	High	Medium
Customer record data.	SQL injection	I	medium	high	High
	Buffer overflow	A	low	high	Medium
	Trojan horse	I	high	high	High
	Eaves dropping	C	medium	high	High

	Spyware	C	Medium	Medium	Very High
Employee's information data.	Phishing	C	medium	medium	Medium
	Financial malware	I	high	low	Medium
	Malicious spyware	C	medium	medium	Medium
	SQL injection	I	medium	high	High
	Employee theft	C	Low	High	Medium
Financial and product records data.	Theft	C	low	high	Medium
	Server failure	A	low	medium	Low
	Eaves dropping	C	low	medium	Low
	Spyware	A	medium	medium	Medium
	Ransomware attack	A	High	High	Very High
Transactions and orders Record data.	Spyware	C	high	High	High
	Server failure	A	low	medium	Low
	Phishing	C	medium	high	High
	Malware	C	Medium	Medium	Medium
	Ransomware attack	A	High	High	Very High

Task 2

A) Security solutions with controlling risks:

After analysis and observed the whole scenario, Identified the highest security threats for Mary Lane Cosmetics system. Now, these stages discuss about the all possible solutions in order to control or reduce that risks. If the company system faced ransom ware attack or another cyber-attack it can stopped all business services. So, on this case build a secure network infrastructure with the suitable recommended solutions are also give in there.

Risk 1: Server

Mary Lane Cosmetics business data are stored and used for e-commerce business development. For this reason many internal and external attack like Ransomware, Brute force, DDos attack are create problem also (Symantec, 2017). There are many popular threats and attack like ransomware and spyware attack is very dangerous attack which can be occurred in a server any situation. So, if server is not protected properly data can be lost or hacked by hacker (UKessays, 2003).

Solution:

- Avoid default configuration and apply manual secure configuration.
- Unnecessary service port must be closed and install latest security patches.
- Must be applying regular security auditing with preventing theft as much as possible.
- Data must be update and back up in regularly.

- Demilitarized zone (DMZ) can be protecting the server if it placed for internal and external threatens because it creates a secured zone on each side of firewall. Internet connected to firewall via router. Then workstations and other servers are connected to DMZ on opposite side. So, it is a secure zone now it will be protected by external and internal threats.

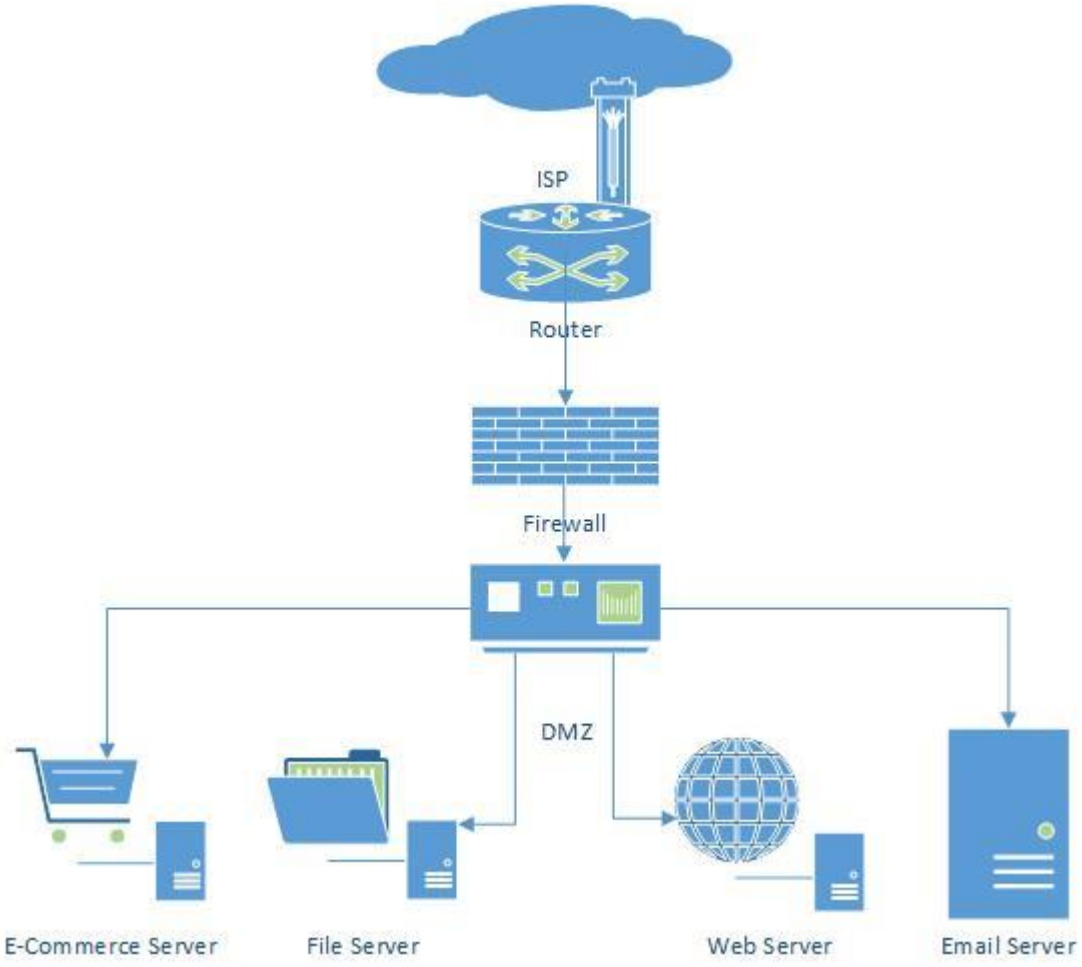


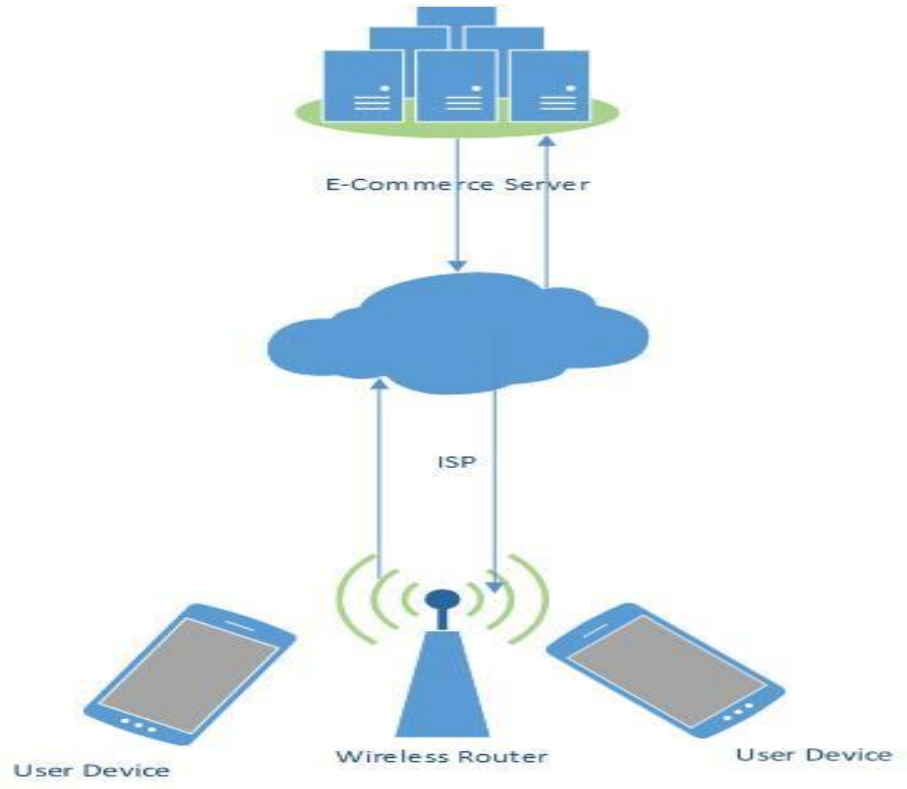
Figure 1: E-commerce, file, web and Email server are deployed in DMZ zone.

Risk 2: Data transmission

Mary Lane Cosmetics data transmission processes when user access data from server that's time server have a risk of phishing, Trojan, spyware, malware attack while it is transmitting (Quickbooks.intuit, 2005). So, transmission of data must be built in secure process. They transmit important data like customer, transaction details employee information through online.

Solution:

- SSLVPN must be used for encrypt data and storage in backup server when data transmitting.
- Must be deployed Anti-phishing and anti-malware protection application.
- Can be used Digital signatures for secure Authentication in application processes via smartphone (Krollontrack, 2006).



Risk 3: Hardware

Mary Lane Cosmetics network things hardware can be damage by physical or natural process such as heating, flood, theft of equipment, tempering and maintenance, any type of physical force, power voltage surges etc. So, router, switch, PCs, firewall, DMZ hardware and cable must be protected properly as much as possible (Synaxiom, 2011).

Solution:

- Voltage stabilizer IPS and UPS must be used properly.
- Must be strict control form of temperature, humidity and water detection.
- Installing networking devices with video and audio recording system.
- Sensor and alarm should be attached for equipment accidently displaced.

Risk 4: Data security

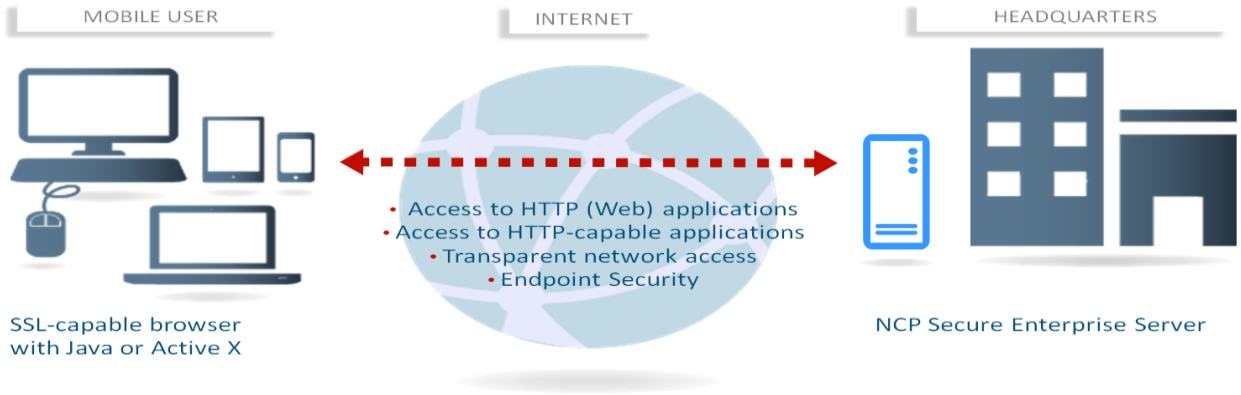
Mary Lane Cosmetics have data risk of confidentiality, integrity and availability. Many Internal and external threats can be happened there, such as phishing, malware, DDoS, SQL injection and ransomware attack, employee theft and hardware failure etc. (Tripwire, 2008). So, it is very important to keep or store data securely.

Solution:

- Set permissions for whole disk full data, folders and individual files access control must be encrypted with authentication process.
- Metadata file system must be used Cryptographic file format. So, data and file must be back up in encryption processes.
- Individual documents installed processes allow user for password authentication.

Risk 5: Remote access

Incoming threat reasons Mary Lane Cosmetics network will be accessed remotely by the users, security issues of this network must be strong. So, this tunnel must be secure of allowing the remote access. Without permission one or more authentication can't allow for VPN access.



(Remoteaccess, 2010)

Solution:

- Restrict access to remote can be using RDP gateway when desktop ports supporting remote access connections.
- Secure connection in remote access openVPN must be used.
- Secure dial up remote access connection must be use encryption with secure application authentication processes.

B) Recommended protocol and encryption algorithm:

Mary Lane Cosmetics network protocols and encryption algorithms. Where encryption is used:

- **Authentication:** AES and RSA algorithm are used to provide authentication. Also hashing algorithm can be used for password protection.
- **VPN:** IPsec, 3DES, Diffie-Hellman key exchange algorithm with some Encryption and Authentication algorithm can use.
- **Data storage:** Symmetric encryption is used to encrypt data at rest and AES algorithm is used for file folder encryption.

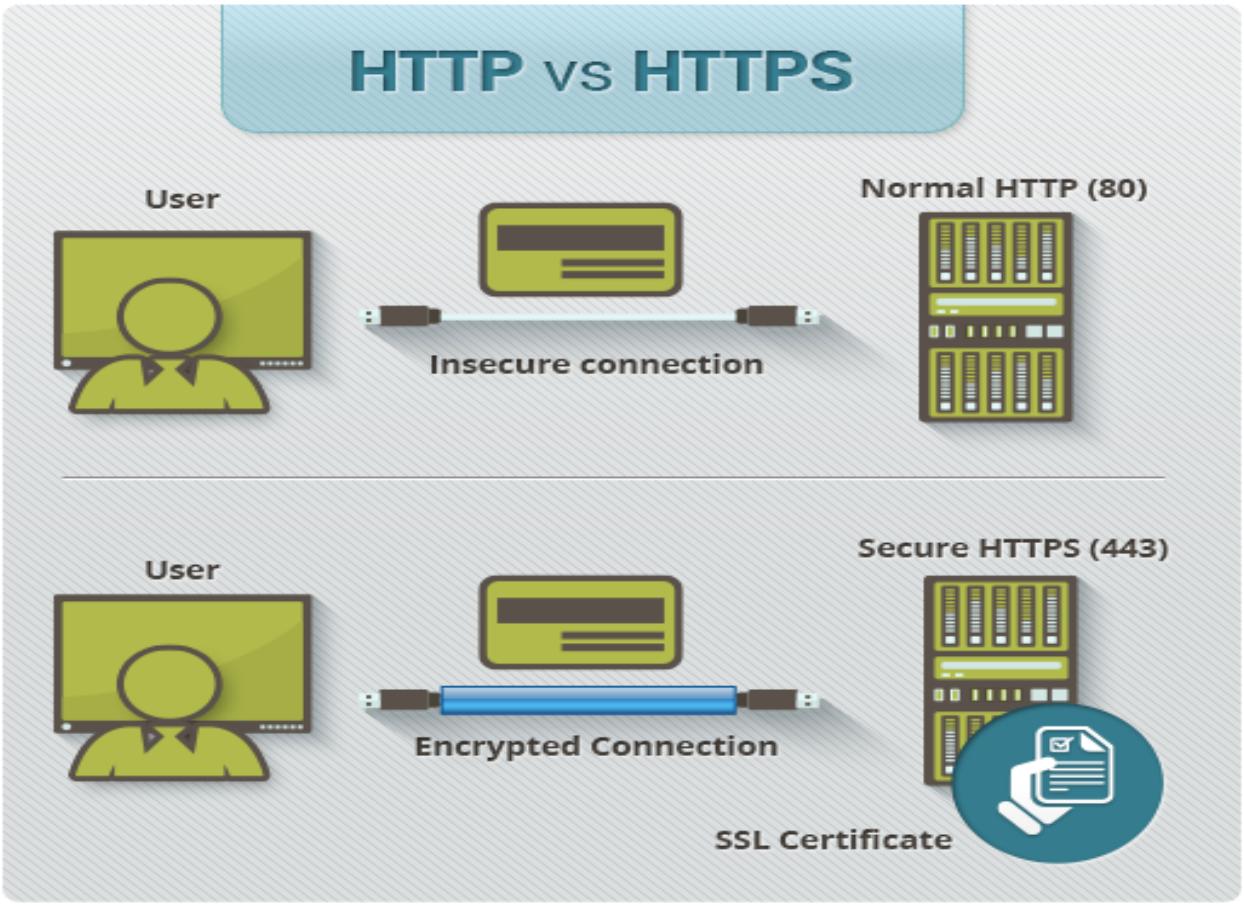
Recommended protocol and encryption algorithm

DES Algorithm four model (ECB, CBC, CFB), IPsec (IP security), PPTP, L2TP (layer 2 tunnel protocol) create a VPN tunnel. Public key encryption techniques and AES, 3DES and IDEA algorithm can used to encrypt data from Brute-force or another critical attack.

SSL and Encryption:

Security Socket Layer (SSL) is a cryptographic protocol. This protocol provide security in networking layer OSI model transport layer stage. SSL provide security between machine and devices operating over the internet (Info.ssl, 2007). This technology establishing encrypted link between web server and browser. So, SSL web server creates two cryptographic key these are private and public key (Digicert, 2017). ECC, RSA and DSA encryption option also contribution with TLS certificate. When SSL is

used to create secure communication between web browser and server the website address turn in HTTP to HTTPS. (Digicert, 2017) So, this ‘S’ is meaning of Secure. For this project TLS, AES, RSA, 3DES algorithm can be used now days for e-commerce site SSL certification (Globalsign, 2012).



(Instantssl, 2011)

Example of website secure with SSL Layer which is show in browser URL.

Task 3

a) Network diagram excluding IP Address:

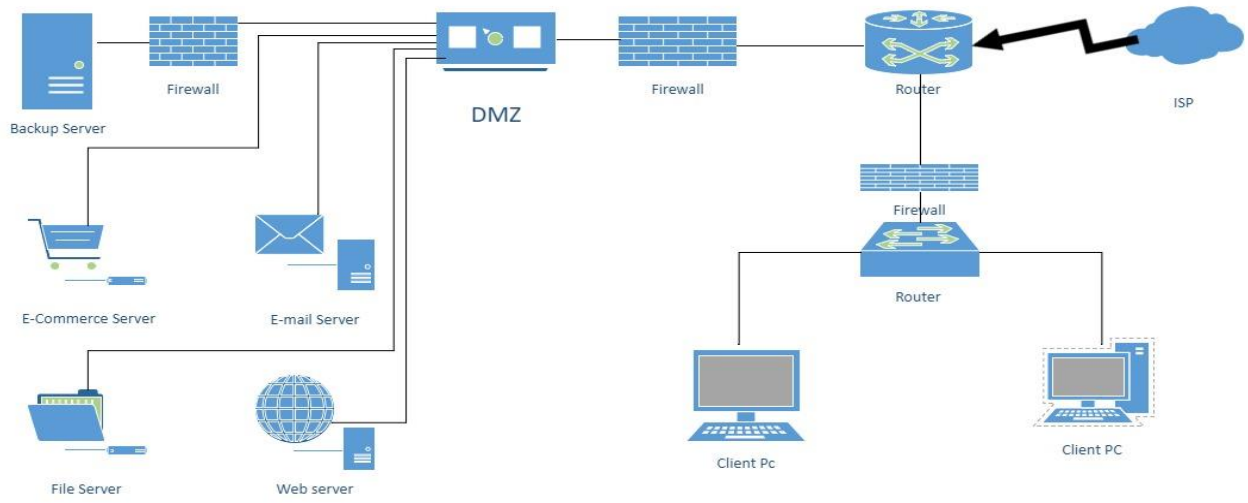


Figure 2: Proposed Network diagram for Mary Lane Cosmetics without IP.

b) Network diagram including IP addresses:

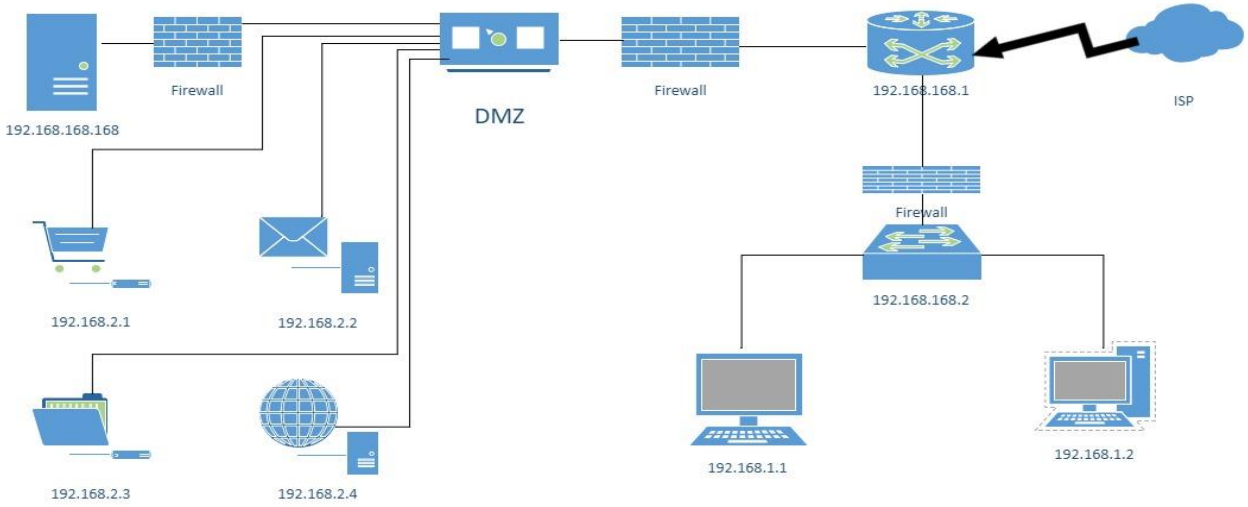


Figure 3: Proposed Network diagram for Mary Lane Cosmetics with IP.

c) How the network design meet Security requirements:

Observe the whole network diagram it can be say that DMZ has been placed for server security in the proposed network diagram. So, Mary Lane Cosmetics important electronically held information assets relating highest risks of this system and also their protection explained in there:

- E-commerce, e-mail, file and web server where most important data like customer, employee and financial transaction data are recorded. So, it is placed in DMZ zone the stored data can be protected from external and internal threats which is show in figure 2.
- Extra backup server are placed in another security places where connection with extra firewall which is connected with DMZ zone. So, that it will create a secure tunnel and transmitted data in securely besides DMZ provide an additional layer of security which is restricted for hackers to directly access internal server.
- Data which are stored as file or folder in a system are encrypted using file encryption system besides firewall used properly in this network with proper security configuration. This is the first stage security of a network. The firewalls are password protected. So, data can be secured from unauthorized access and malwares attack.

Alternative solutions:

- Proxy server which acts as an intermediary between client and server it provides anonymous browsing and filters request from external site and server.

- Data can be back up in cloud and another external devices. So, if necessary it can be found quickly.
- VPN can be used to create secure end to end communication in remote access besides it provides encryption facility using Open SSL. Now it is more secured comparing to other VPN technologies.

Data and document security I tried to fulfill security issues, vulnerabilities and believe that proposed network will fulfill the security requirements. So, all the security system should be maintained properly to keep the network system information safely.

Task 4

Mary Lane Cosmetics network is analyzed properly and vulnerabilities of the network which is identified. Now, how these security solutions will be maintained in the future are explained here.

- Regular vulnerability assessment and security audit must be done the system.
- Backup, restriction, disk removable and downloading policy must be established in standard security way.
- DMZ, firewall, router, VPN and EFS technology must be deployed strictly.
- Regular monitoring of server and hardware should be done to identify threats and prevent theft.
- Training must be provided new and previous employee for use the network in authentication way.
- Identify the threat and security bug in IT audit which is mandatory recommended.
- Unnecessary service port must be shut down when computer or server connect to the network and important and essential port open with two step authentication way.
- File encryption and backup must be done in a regular basis.

Task 5

a) Complete this assignment I faced limitation of time which is challenge for me, analyze the whole scenario properly and also visualize some diagrams to explain the security terms more perfectly. Difficult part was analyzing and designing the secure network diagram for Mary Lane Cosmetics. A proper and well-designed network can prevent many types of cyber-attack from known and unknown sources. I have analysis the current network structure of Mary Lane Cosmetics and tried to identify and provide the best solution. Data protection law like cyber essential tool, cryptography, encryption and decryption algorithm, VPN, DMZ, authentication method and techniques are configured for secure the network.

b) Start the assignment at very beginning, I must produce more time to analyze the scenario. Then analyzing and measurement the threats and possible attack for particular days. So, all the security measurement and tool would be explained perfectly. At last I try to explain and visualize main network security architecture for Mary Lane Cosmetics LAN Network.

Conclusion:

After analyzing the whole scenario Mary Lane Cosmetics network design try to provide all possible security solution with important components which is very essential. To ensure the security label DMZ placed on the server, user and external communication devise in middle stage. So, at last it can be said that try to fulfill all the requirements for Mary Lane Cosmetics network most effective and dynamic way.

References

Digicert (2017) *https://www.digicert.com*, 10 September, [Online], Available: https://www.digicert.com/ssl/ [28 January 2018].

Digicert (2017) *https://www.digicert.com*, 10 September, [Online], Available: https://www.digicert.com/ssl-cryptography.htm [28 January 2018].

Globalsign (2012) *https://www.globalsign.com*, 15 January, [Online], Available: https://www.globalsign.com/en/ssl-information-center/what-is-an-ssl-certificate/ [28 January 2018].

Info.ssl (2007) *http://info.ssl.com*, 06 September, [Online], Available: http://info.ssl.com/article.aspx?id=10241 [28 January 2018].

Instantssl (2011) *https://www.instantssl.com*, 15 September, [Online], Available: https://www.instantssl.com/ssl-certificate-products/https.html [28 January 2018].

Instantssl (2011) *https://www.instantssl.com*, 1 September, [Online], Available: https://www.instantssl.com/ssl-certificate-products/https.html [28 January 2018].

Krollontrack (2006) *https://www.krollontrack.com*, 01 Jauary, [Online], Available: https://www.krollontrack.com/blog/2015/09/15/data-breach-cyber-attacks/ [28 January 2018].

Quickbooks.intuit (2005) *quickbooks.intuit.com*, 07 December, [Online], Available: https://quickbooks.intuit.com/r/technology-and-security/8-types-of-cyber-attacks-your-business-needs-to-avoid/ [28 January 2018].

Remoteaccess (2010) *http://www.remoteaccess.org*, 01 January, [Online], Available: http://www.remoteaccess.org [28 January 2018].

Symantec (2017) *www.symantec.com*, 08 August, [Online], Available: https://www.symantec.com/connect/articles/common-security-vulnerabilities-e-commerce-systems [28 January 2018].

Synaxiom (2011) *http://www.synaxiom.com*, 15 March, [Online], Available: http://www.synaxiom.com/impact-of-ecommerce-in-todays-business-world/ [28 January 2018].

Tripwire (2008) *https://www.tripwire.com*, 20 June, [Online], Available: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/protect-e-commerce-business-cyber-attacks/ [28 January 2018].

UKessays (2003) *www.ukessays.com*, 01 January, [Online], Available: https://www.ukessays.com/essays/computer-science/study-of-attacks-on-e-commerce-systems-computer-science-essay.php [28 January 2018].