Introduction:

Network Security and Cryptography is important for every organization to protect network resources from unauthorized access and malicious attacks. iSee clinic is an independent hospital which suffered ransomeware attack recently. As a network consultant the CEO of iSee clinic asked me to ensure that any future ransomeware attacks are unsuccessful and also identify the key security challenges faced by the company and recommend solution.

Task-1

a) Five important electronically held information assets relating to iSee Clinic are given below,

1. Patient personal record
2. Employee data
3. Financial or Transaction data
4. Order processing
5. Email data

b)

Assets	Threat	CIA	Likelihood	Impact	Risk
Patient personal data	Server failure	A	Low	Medium	Low
	Employee theft	C	Low	High	Medium
	Phishing Emails	C	Low	Medium	Low
	Viruses	A	Low	Medium	Low
Employee Data	Spyware	C	Low	Medium	Low
	Employee theft	C	Low	Medium	Low
	Phishing Emails	C	Low	Medium	Low
Financial Data	Spyware	C	Medium	High	High
	SQL injections	I	Low	High	Medium
	Phishing	C	High	High	Very High
	Malware	A	Medium	High	High
	Ransom ware	A	High	High	High

	Attack				
Email data	Server failure	A	Low	High	Medium
	Accidental	A	Low	High	Medium
	Ransom ware Attack	A	High	High	Very high
Order Processing or Transaction	SQL injection	A	Low	Medium	Medium
	Phishing	C	Medium	High	High
	Ransom ware Attack	A	Medium	High	High
	Malware	A	High	Low	Medium

Task-2

a) Security Threats:

After observed from the scenario of iSee Clinic Hospital I have identified the highest security risks, threats and possible solutions are given below to reduce these risks,

1. Data at Rest (Server):

From scenario we can see that iSee clinic's financial system, order processing, patient's record data, email data, human resources data and special equipment for photographing eyes are linked to the Domain controller running Windows Server 2012R2 so we can understand server is in the highest risk. Some phishing email has been found on email server and also they suffered ransomware attack recently. In future they may again faced these type or similar types of logical attack like malware, DDoS, SQL injection because it's still have some vulnerabilities and also physical attacks may occurred like natural disaster, fire, hardware failure and theft.

Solutions:

1. Sever will be placed into DMZ (Demilitarized zone) so that a secure zone will be created through dual firewall which will provide additional layer of security from internal and external attack to the LAN (Searchsecurity.techtarget.com, 2016). Resources of LAN will be accessible through DMZ but internal local area network will not be reachable to hackers.

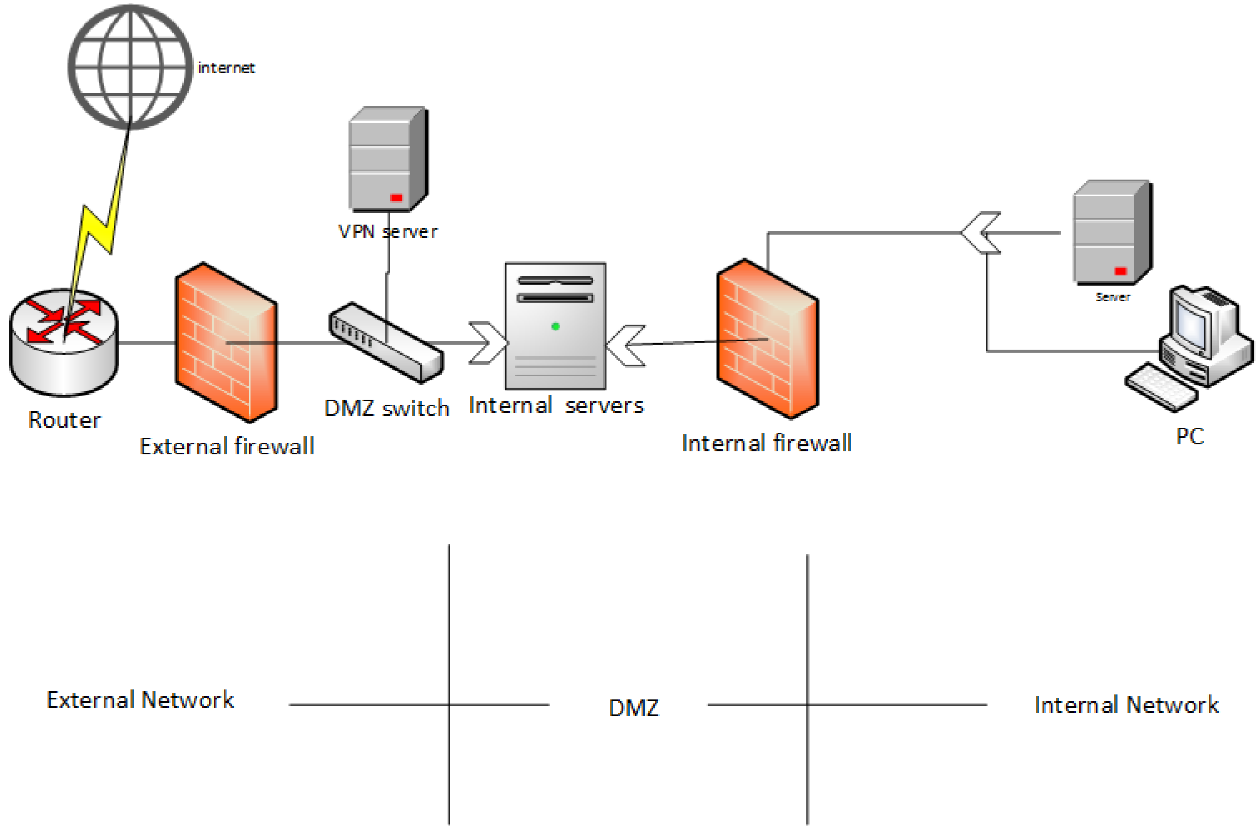

Figure-1: DMZ protecting servers from external and internal attack

2. Standard security configuration need to be applied
3. Regular auditing is important to all network controlled devices.
4. Unnecessary service port should not be opened
5. Update latest patches
6. Proper authentication should followed

Data at Transmission (Order Processing transaction):

After analyzing the scenario we can see that Manchester and Glasgow clinic connect London headquarters to store and share every information through the internet and also access London headquarters data.. So we can say the data transmission of iSee Clinic is at risk like eavesdropping, DDoS, malware, phishing, Trojans etc.

Solutions:

1. Virtual Private Network will be used to protect data through tunneling from external data theft and attacks at the time of data transmission over the internet (Mils.com, 2016). Data will be automatically encrypted at the time of transmission and secure connection will be creating between London headquarters with Manchester and Glasgow branches.

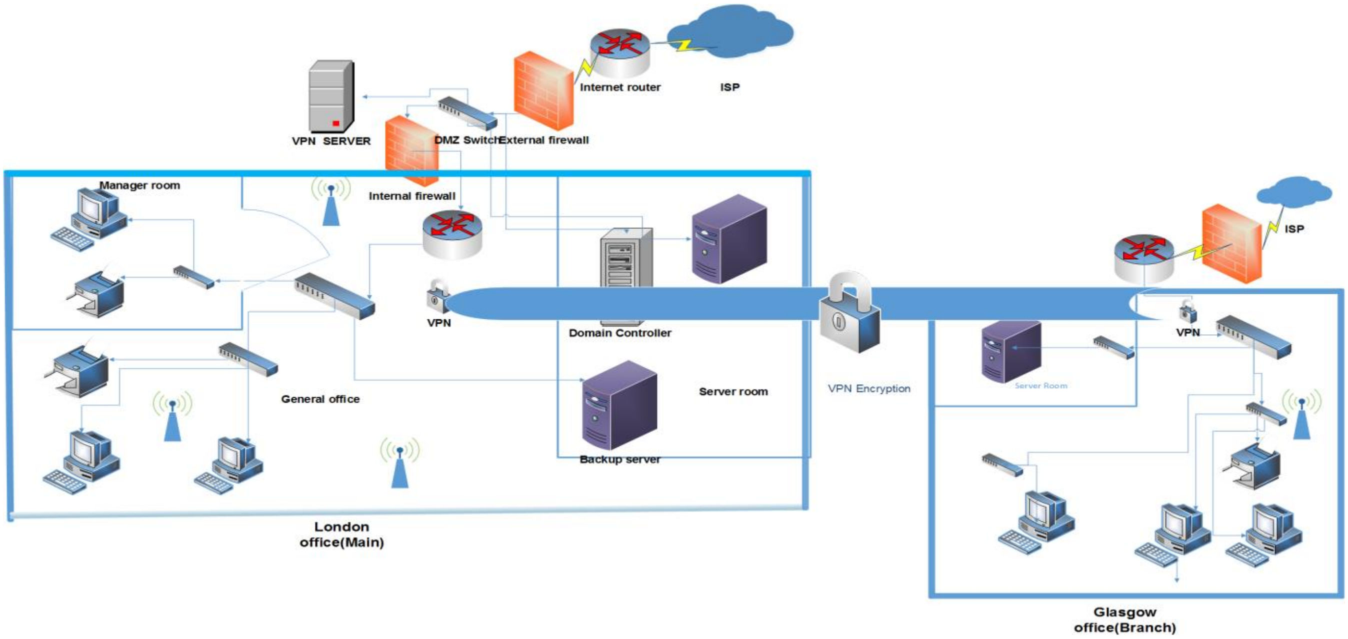

Figure-2: Data transmission through VPN

2. Content management System website data transmission security will be given using Secure Socket Layers (SSL) (Apgar, 2016).

3. IPSec will provide confidentiality, integrity and authentication during data transmission and IPSec headers will ensure that data has not changed at the time of transmission.

4. Using encryption mechanism and digital signature security will be given at the time of transmission.

Data Security:

iSee Clinic has many important patient record data, human resources data and order processing data which needs to be stored securely because there might be internal threat like employee theft, prank or hardware failure and external threat could be phishing attack and malware attack.

Solutions:

1. EFS certificate will be used to encrypt file so that only authorized user can access the document.
2. To give document protection the full disk encryption will be used including Master Boot Record (MBR).
3. Level of access will be fixed so that different user can access different level of data.
4. Metadata (file names, file sizes, time stamps, directory structures) will be also encrypted for document security.

Remote Access Control:

From scenario we can see that marketing staff remotely access site via web portal and update the news and blog. Regional office Glasgow and Manchester connect to the London headquarters through internet. Remote access control also needs to be secure because data access might be in threat like DNS poisoning, DOS attack, Port scanning, Internet Control Message Protocol attack and TCP Desynchronization (Techopedia.com, 2016).

Solution:

1. Using SSL VPN technology external access will be restricted for user and only authorized user will be allowed to access (Gamby, 2016).
2. Turning of split tunneling prevent man-in-the-middle attack while user connected to the remote desktop (Gamby, 2016).
3. Remote access server will be configured to invoke policies
4. Data will be encrypted at the time of transmission to protect confidentiality and integrity

Network Hardware security:

Hardware like equipment for photographing eyes, router, firewalls, access points, printers, switches and PC's are at many types of physical risks such as natural disasters, fire, flood, power loss, electronic threats and maintenance.

Solutions:

1. Secure configuration for network devices
2. Room temperature should be controlled and using heat sensors also smoke detectors to avoid accident
3. Controlled level of access, lock and biometric access control system for network devices must be maintained properly (Rouse, 2017).
4. Performances of network hardware need to be monitored continuously twenty-four hours and also the physical location through surveillance cameras (Rouse, 2017).

b) 10 steps to cyber security: Cyber essentials are government- backed cyber security certification that helps to focus on business objectives and protected from common cyber attacks. Following 10 steps to cyber security published on 2012 and using these steps means protecting organization from cyber attacks.

1. Information risk management regime & Secure configuration
2. Network security Managing with user privileges
3. User education and awareness with Incident Response management
4. Malware prevention & detection with Monitoring
5. Removable media controls from Home and mobile networking.

ISO 27001:

ISO 27001 is a specification of information security management system and provides a framework which will help iSee Clinic to protect and manage their valuable information assets and data. Steps of ISO 27001is given below,

1. Decision
2. ISO Management Representative
3. Gap Analysis and Risk Management
4. Scope and Implementation Plan
5. Employee Introduction
6. Documentation
7. Realization
8. Internal ISO 27001 Audits
9. ISO 27001 Certification
10. Maintaining the ISO 27001 Certification

c) Encryption:

Data transmission and storage need to be encrypted because iSee clinic's recently suffered ransomware attack which encrypted their most of the data and was unable to operate for a week. Financial system, order processing system and email are all sensitive data, they need to give protection at the time of transmission and also when they are at rest.

To protect data at the time of transmission VPN encryption with AES algorithm will be used and the protocols of VPN encryption are PPTP, L2TP/IPSec, SSTP and IKEv2/IPSec. For remote communication openVPN and AES will use.

To give data security in the storage 3DES algorithm will be used to encrypt the data and Encrypted File System will use.

Task-3

a)

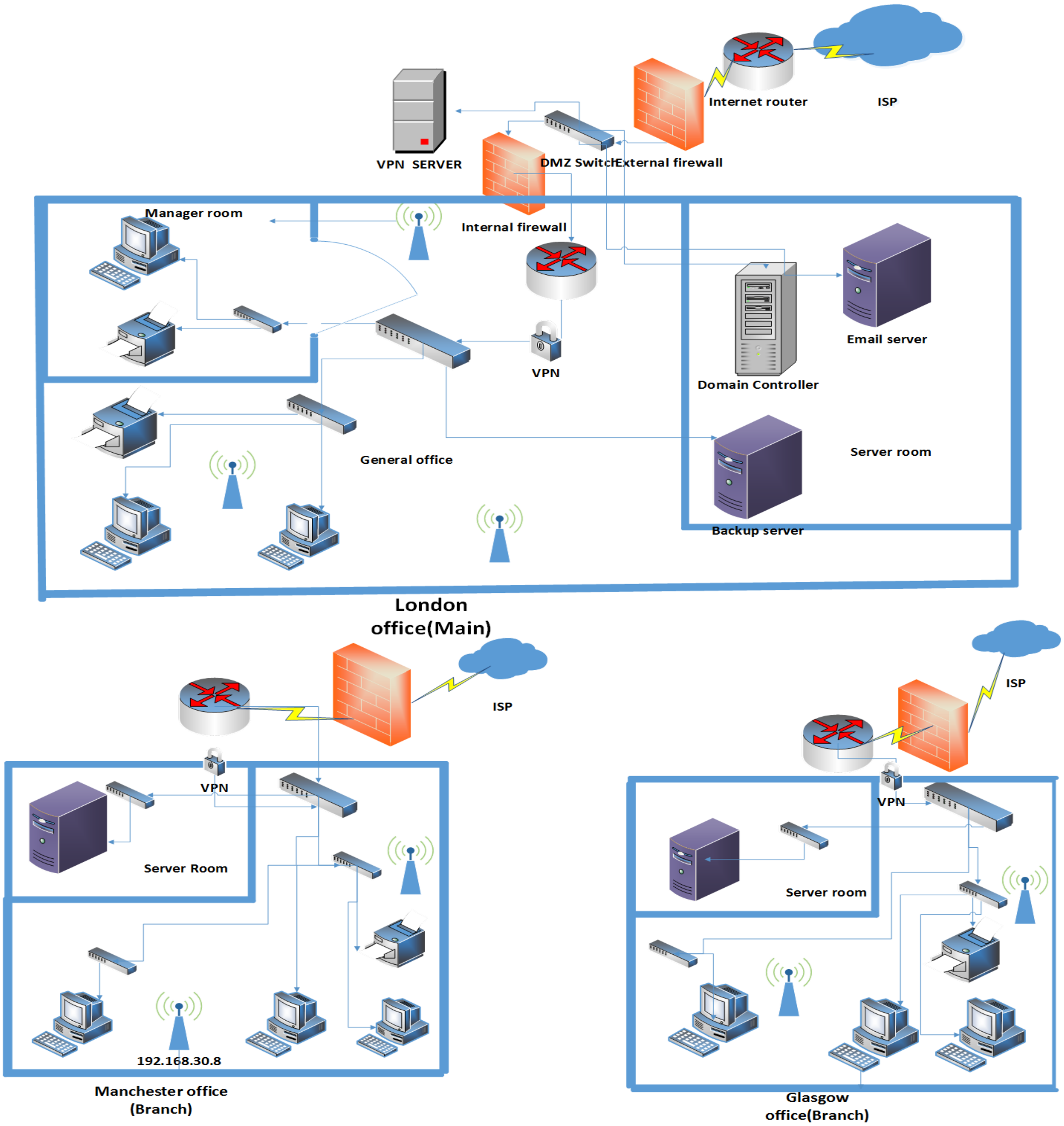

Figure- 3: Proposed network diagram of iSee Clinic

b)

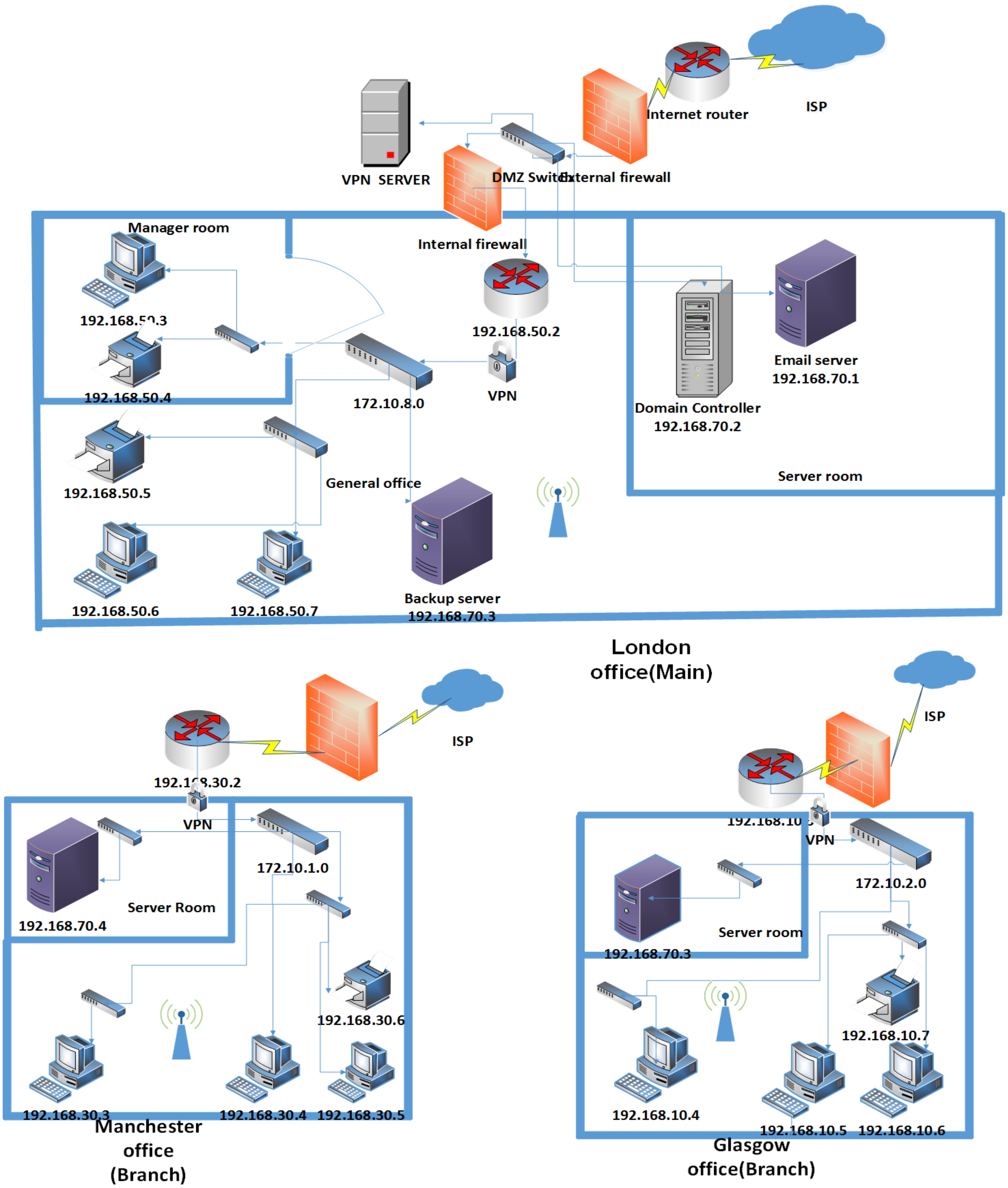

Figure-4: Proposed network diagram of iSee Clinic with realistic IP address

c)

Network of iSee Clinic has been designed considering the risks, issues and security vulnerabilities. If we observe the above network diagram, we can clearly see that DMZ has been placed in the London headquarters for server security in the proposed network diagram. To ensure secure data transmission from London headquarters to Glasgow and Manchester branch Virtual Private Network (VPN) has been provided. In addition to for data and document security we have implement file and folder encryption. I tried to overcome iSee Clinic security issues and vulnerabilities and believe that proposed network will fulfill the security requirements.

TASK-4

Vulnerability of iSee Clinic network has been identified, after proper analysis their network security and to ensure security we already give protection server using DMZ, document, file and folder through encryption and transmission using VPN. To maintain future security of iSee clinic the following step should be maintained.

1. Standard security policies have to be developed and deployed to ensure iSee clinic security.
2. Technical training have to be arranged periodically for the staffs
3. Security audit and vulnerabilities need to be performed frequently to identify threats and weakness of the system
4. Network devices like hardware and software should monitored regularly
5. Access control policies have to be maintained for hardware resources as well as for software

TASK-5

Reflective commentary:

a) Difficult part was analyzing and designing the security network for iSee Clinic because a proper and well-designed network can prevent many types of malicious attack from various sources. I have analysis the security of iSee Clinic and tried to identify and provide the best solution such as many data protection law like cyber essentials, cryptography, encryption algorithm, VPN, DMZ, authentication method and techniques are configured to secure the networks.

b) If I could start it again, I would like to research more about data protection, security methods and network technologies because these subject knowledge are important before designing a secure network. For better understanding of iSee network I would like to draw more visualized detailed diagram.

Conclusion:

After analyzing the iSee Clinic overall scenario, to ensure security DMZ has been placed in the server, VPN has been provided for secure data transmission and related solution has given for associated risk. To ensure security regular vulnerability assessment, monitoring and auditing is recommended.

Bibliography and References

Apgar, C. (2016) *Searchsecurity.techtarget.com*, 3 June, [Online], Available: http://searchsecurity.techtarget.com/tip/Secure-data-transmission-methods [2 January 2017].

Gamby, R. (2016) *Searchsecurity.techtarget.com*, 10 March, [Online], Available: http://searchsecurity.techtarget.com/answer/Secure-remote-access-best-practices-Guidelines-for-the-enterprise [3 January 2017].

Mils.com (2016), 5 May, [Online], Available: http://www.mils.com/products/secure-connections/ [2 January 2017].

Nordvpn.com (2016), 10 May, [Online], Available: https://nordvpn.com/blog/security-protocols/ [10 January 2017].

Nordvpn.com (2016), 10 May, [Online], Available: https://nordvpn.com/blog/security-protocols/ [11 January 2017].

Rouse, M. (2017) *Searchsecurity.techtarget.com*, 1 January, [Online], Available: http://searchsecurity.techtarget.com/definition/physical-security [3 January 2017].

Searchsecurity.techtarget.com (2016), 5 June, [Online], Available: http://searchsecurity.techtarget.com/definition/DMZ [1 January 2017].

Technet.microsoft.com (2009), 13 February, [Online], Available: https://technet.microsoft.com/en-us/library/dd469817(v=ws.10).aspx [4 January 2017].

Technet.microsoft.com (2009), 13 February, [Online], Available: https://technet.microsoft.com/en-us/library/dd469817(v=ws.10).aspx [10 January 2017].

Techopedia.com (2016), 23 October, [Online], Available: https://www.techopedia.com/definition/4078/remote-attack [4 January 2017].