lyit | Institiúid Teicneolaíochta Leitir Ceanainn
Letterkenny Institute of Technology

Assignment 2

Lecturer:	John O'Raw
Report Title:	Assignment 2
Submit to:	Blackboard with all files as specified in the assignment, submitted as a single ZIP folder.
Date Submitted:	14 Dec 2020

Student Name:	Mamta Mittal
Student Number:	L00161832
Programme of Study:	M.Sc. in Cloud Technology
Module:	Enterprise and Data Center Networking

Please refer to the Institute's Quality Assurance Handbook, Version 3.0, September 2018

1. Practical work, forming part of the CA of a module, will only be assessed if the student has attended the relevant practical classes.
2. CA work must be completed within the schedules and specifications (specified in the CA brief). Students who submit CA late may forfeit some or all the marks for that work.
    a. The total marks available for an assessment be reduced by 15% for work up to one week late; i.e. a grade of 50% would become (50*0.85) = 42.5%
    b. The total marks available be reduced by 30% for work up to two weeks late i.e. a grade of 60% would become (60*0.7) 42%
    c. Assessment work received more than two weeks late should receive a mark of zero.

    Work is deemed late when an unauthorized missing of a deadline has occurred.

3. CA must be the student's own work, refer to Plagiarism Policy, in section 5.7 of the QA manual.

LANs at Data Centers, Head Office and Sligo Branch Office in different cities were connected together to form a WAN so that they can communicate with each other. Leased Lines which are secured private dedicated lines were used to connect the three primary locations. AirSPeed was chosen as the Service Provider based on the availability of servicer at these locations and charges. Three Point to Point links between Data Centers and Head Office were used as below.

1. Between DCs at Malin, Donegal and Cork, 500 Mbps fibre link.
2. Between DC at Cork and Head Office in Dublin, 1000 Mbps fibre link.
3. Between Dublin Head Office and DC at Malin, Donegal,500 Mbps fibre link.

These 3 links were connected in a ring topology to provide redundancy between the links.

Separate Internet connection from AirSpeed and Eir has been provided to DC1, DC2, Head Office and Sligo branch as primary and backup links. These connections terminate on FortiGate Perimeter Firewalls which are recommended to be used in High Availability (HA) mode. The firewalls are connected to Routers which are advised to be configured in redundancy mode using HSRP. Access Switches at all the locations are designed for redundancy. Unmanaged switches along with Fortigate firewall were used to simulate the network due to simplicity but in reality, managed switches are recommended to be used.

The branch site Sligo was connected to Data Centre at Cork (DC1) using IPSec VPN tunnel, which are secured connection over internet and a good alternative to private WAN connections. Two internet connections are provided at Sligo so even if one goes down, VPN tunnel will be operational using another internet connection. Firewall by FortiGate was used at Sligo and DC1 sites to create VPN tunnel between them. Routers can also be used for Site to Site VPN. Communication between the sites was tested by doing ssh to a Server from a Ubuntu Guest client located at another site.

Firewalls were used as VPN tunnel was created which works over Internet and for security reasons firewall is required whenever connection is made to an external network. FortiGate Firewall used in the design supports routing protocols RIP, OSPF along with static routes. It also has functionality of DHCP Server, which was used to assign IP addresses to clients in Sligo LAN. Connection from the ISP was directly terminated on Firewall using its Ethernet port. Since, firewall has most routing functionality and connection from ISP could be directly connected to Firewall, a router was not used to terminate ISP connection in VPN tunnel design.

Firewalls have Security Zones to which interfaces can be assigned. Interfaces were configured in Security Zones LAN, WAN and DMZ. Multiple DMZs (Demilitarized Zones) can be configured and are generally used when we want to access an application from outside the network, i.e. internet. An access list which permits traffic only to the IP address of server/s in DMZ is configured to make sure servers are accessible from outside. A separate DMZ Zone is recommended for controllers for Solar Panel, Air Conditioning, Automation etc. so that contractors can access the equipment on site without having access to rest of the network. There are network services and business applications like File Server, Web Server, Payroll application etc. in Data Centre which needs to be accessed by Branch Office. Business Applications and Network Services are recommended to be put into two separate DMZ and access list/policy can be configured to allow access from branch to these DMZs.

Client to Site VPN or Remote User VPN was configured to allow remote access to users who are away from office, either travelling or working from home or a different location. FortiGate Firewall was configured to use FortiGate VPN Client by users for remote access. Here, a VPN tunnel gets established between the remote user and the remote device and thus access is

granted. SSL VPN was used for configuring access to remote users. It offers a portal through web browser using which applications can be accessed. SSL portal was configured on Sligo Firewall and a user “mamta” was created. This user was added to a group “Remote Staff”. VPN tunnel address range was checked to make sure it was different from internal network range. Security policies were created to allow internal network and internet access. However, the remote access test failed as FortiGate Evaluation Version was used which does not seem to support advanced encryption.

Senior Management while on the road will be able to access business applications in DC1 using FortiGate VPN Client once Client to Site VPN between Sligo and DC1 works. Access only to particular DMZ for business applications to Senior Management can be given using Access Policies in FortiGate. Customer’s Technical Staff would be able to remotely login to the devices using FortiGate VPN Client.