University of Sunderland

Faculty of Technology

CET236 – Network Security

Assessment 2

This assessment is worth **60%** of your **overall** module mark. It equates to roughly 36 hours of work time.

This assesses your ability to:

- Select and implement a range of Management Plane security protocols that meet the needs of a client
- Select and implement edge security and data privacy protocols that meets the needs of a client
- Robustly test your security implementation
- Create and maintain a network engineer's journal.

You would be expected to spend 30 hours on this assessment.

You must also submit your **Engineering Journal** for the module. This is worth **10%** of your module grade.

The Scenario

Build the network shown below in your choice of either Packet Tracer or CML2.4 then deploy the security services requested in this assessment. You will need to submit your simulation file along with your supporting documentation in a single .zip file via Canvas by **the date given on Canvas**.

Your Tasks:

Network Deployment (11 marks)

- Single area OSPF should be used to manage routing within the HQ Site. **(3 marks)**
- Secure all OSPF communication **(2 marks)**
- Deploy suitable static and default routes on the ISP router and the two permitter routers (**R1** and **R4**) routers to enable connectivity between the HQ site and the Secondary Site. **(3 marks)**
- Assign the switches their IP address, subnet mask and default gateway. **(3 marks)**

AAA Services for the Management Plane (20 marks)

- Implement an AAA Server running TACACS+ **(6 marks)**
- Create two user accounts on the AAA server for network management purposes. **(4 marks)**
- Configure routers **R1, R2** and **R3** along with switches **S1, S2** and **S3** to communicate with the AAA Server. Make sure that **R1, R2, R3, S1, S2** and **S3** use the AAA server for all network management authentication requests. **(5 marks)**
- Configure **SSHv2** as the only remote access management protocol recognised by all routers and switches within the HQ site. **(5 marks)**

Site to Site Security (30 marks)

- Create a site-to-site VPN between **R1** and **R4**. All traffic travelling between the internal networks of both sites should be sent over the VPN. All Internet traffic should remain unencrypted. Choose suitable authentication, data integrity and data privacy protocols for the VPN.

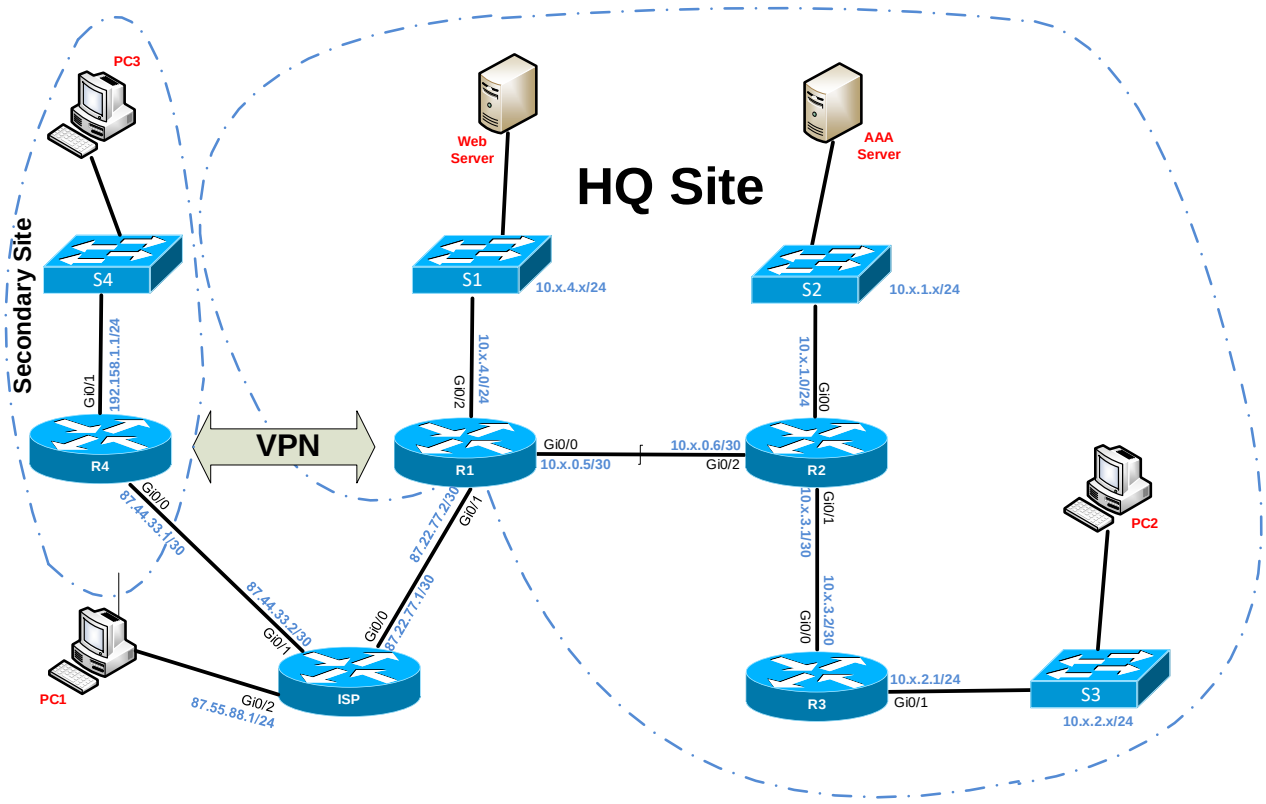
Firewall Services (19 marks)

- Deploy a stateful firewall on **R1**. All conversations that are initiated by an end device internal to the HQ Site (reachable via **Gi0/0** of **R1**) and destined for a device on the Internet (represented by **PC1**) should be allowed through the firewall. All responses should be allowed back through the firewall. **(8 marks)**

- If a device connected to the Internet (**ISP**) attempts to start a conversation with one of the internal devices within the **HQ** site, then that conversation should be blocked by the firewall. **(4 marks)**

- Make sure that Internet devices and internal devices do have access to the Web Server. Make sure that only web traffic is permitted through the firewall to the web server. The web server should not be allowed to initiate any conversation with any internal or Internet device but it must respond to all Web requests. **(7 marks)**

Network Topology



Replace the **x** within the IP addresses shown in the diagram with your birth date. For example, if you were born on the **29th of February 2001** then your **x** would be **29**.

The IP addresses of all PCs should be chosen from spare addresses from their local network address block.

Required Documentation (20 marks)

Contents Page

Introduction

VPN Protocols Recommended (3 marks)

Identify the encryption, data integrity and authentication protocols you used for your VPN. Justify your choices where appropriate

Security Configuration (5 marks)

Command listing for each network device you configured. Only show the commands you added to the base configurations

Testing Strategy (5 marks)

Create a test plan that identifies the tests you performed to verify the following:

- Your two user accounts could be used to login to any network device within the HQ Site
- Your management traffic was secured using SSH within the HQ Site.
- Your firewall was fully operational
- Your site-to-site VPN was operational and was protecting user traffic travelling between the HQ Site and the Secondary Site.

Conclusion

Review the level of success achieved. Suggest one recommendation that may enhance the security requested by the company.

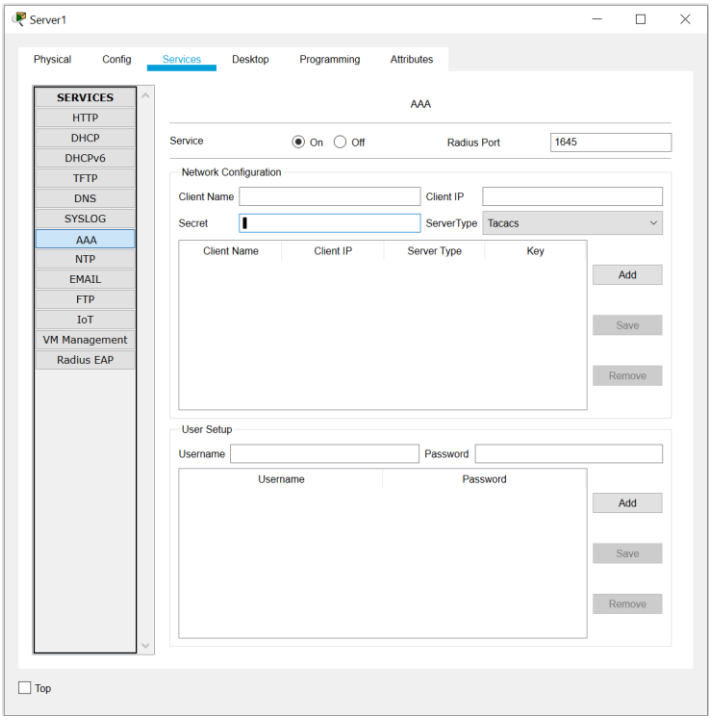
Appendix

- Table of Test Results **(4 marks)**

Note: **3 marks** are reserved for structure and conclusion.

Additional Information:

For those using Packet Tracer – this actually supports AAA servers. The interface is fairly straightforward (see diagram below).



You will need to:

- Select TACACS+ as the communication protocol
- Make sure the service is set to ON
- The clients are the routers and switches within the network
- The user accounts are the usernames and passwords of your users.