6G6Z1112 Information and Network Security

Assessed Coursework 1 (ACW1), Part B: Secure Network Design

Marked out of 100, worth 25% of the marks for this unit. Please direct any queries regarding this document to ……..

The specific learning outcome associated with this element of assessment is:

- ☐ LO3: Explain and critically analyse a variety of security attacks and propose appropriate security mechanisms to detect/prevent such attacks

LO3 is assessed through written and design work.

Students who complete this assessment will acquire the required skills to critically analyse real-world security situations and propose adequate and cost-effective solutions, with minimal redundancy, to face potential threats. The formative feedback provided during the lab sessions will also help students to start to manage their own professional development reflectively.

2. Introduction

This assignment will allow you to demonstrate your understanding of the security protocols and systems covered in Term 2. You will demonstrate your understanding through proposing a network design that provides secure and reliable communication for a large multi-site company. This network design will give you the opportunity to prove your understanding of advanced concepts for major security methods, such as Kerberos and IPsec, and ability to efficiently deploy physical resources such as firewalls and intrusion detection appliances. In addition, you will improve your skills in analysing companies' network configurations, identifying security vulnerabilities and potential threats, and proposing appropriate security mechanisms to prevent, detect and react to these attacks or threats.

As output for this assignment, you are asked to write a **report**, including **relevant diagrams** based on the scenario described in next section.

3. Scenario

A new multinational financial company has been recently created in Singapore (the headquarters) and its CEO (Chief Executive Officer) intends to open three new branches in Dublin, Berlin and Bordeaux to expand the company business. To this end, the company employed you as a network security expert to propose and set up a **secure network design** that ensures secure communication among the three branches and the headquarters as well as secure access to the available online applications for their customers. Currently, the company has the basic configuration proposed by the IT department technician, as shown in Figure 1.

This configuration shows that the headquarters has a data centre that hosts the ***email***, ***web*** **FTP and DNS servers** in addition to the entire hardware and software infrastructure

necessary for handling all the transactions for the whole company. Each branch including the headquarters has its own server and Avast free antivirus software installed in all local machines, and files are shared using FTP protocol through the FTP server located in the main office in Singapore. Currently, each branch has Internet access through a basic **broadband router** supplied by the company's ISP (Internet Service Provider*)*.

Your proposed secure and cost-effective design should accommodate the following requirements:

- ☐ The company is planning to bring online a few new web applications to revolutionize its business and would like to consolidate their ***authentication*** for all desktop machines across all sites (currently using a *simple password based authentication* system). In addition, the company aims to deploy an **access control** mechanism that allows its employees to access the resources available in the most efficient and secure way that minimizes the risk of any security breach.

- ☐ The CEO would like you to review how **all sites are connected together** (the current configuration shown in Figure 1) and propose a secure method to link them and permit **remote access** (e.g. from home) to desktop machines for all employees in a cost-effective way.

☐ You should propose a mechanism to ensure ***secure access*** *to the web* and *email servers* as well as incorporate into the current network design the capability of ***detecting*** and ***mitigating*** the impact of any potential security breaches.

☐ Finally, you should propose a solution to the challenging problem of **DDoS** (Distributed Denial of Service) attack that may target the company in the future.

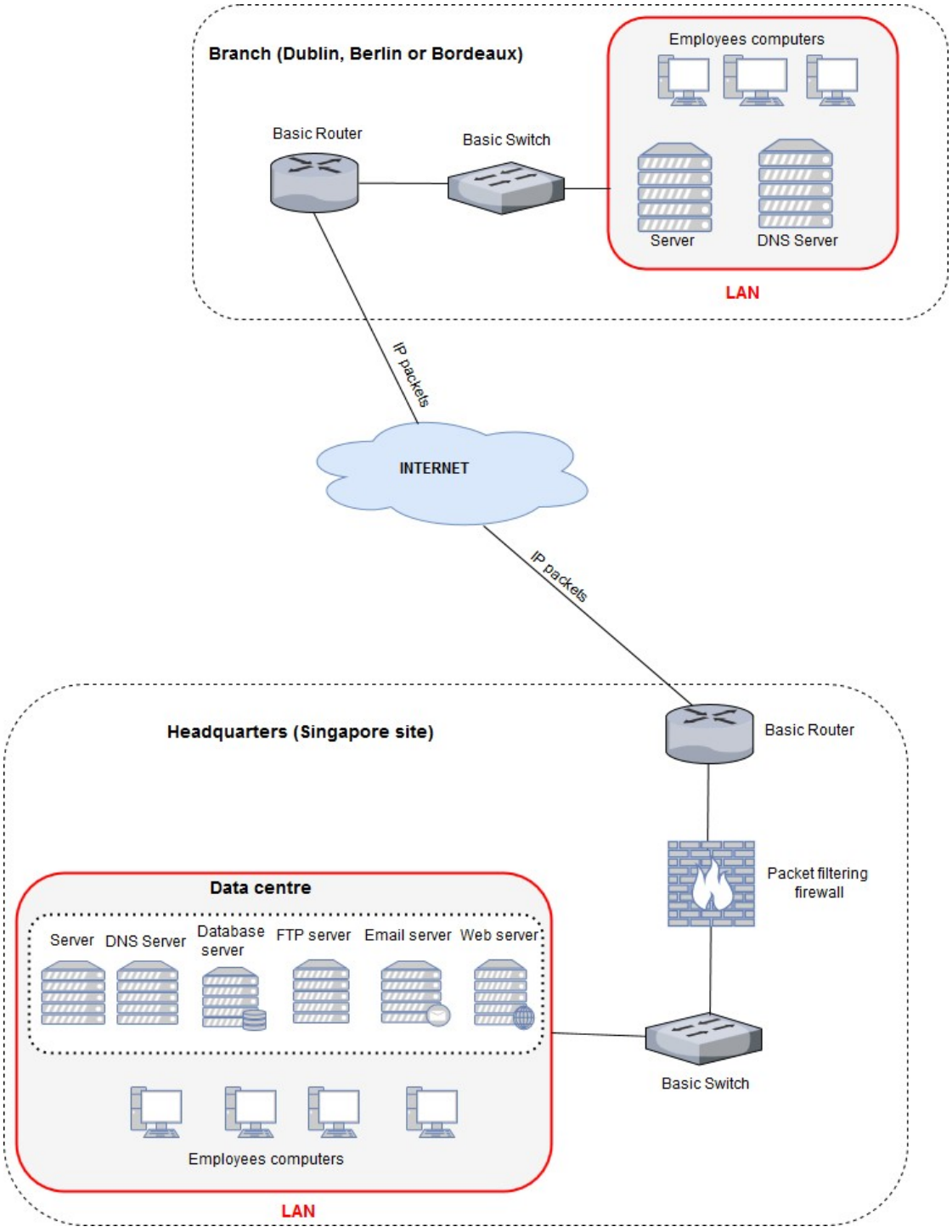

Figure 1. The company's network configuration as proposed by the IT department technician

4. **Assignment Specification**

You should submit a report of **up to 2500 words** (including references), with adequate network diagrams (e.g. the diagram shown in Figure 1) that provide a robust solution to the scenario outlined above. All reports will be run through the plagiarism checker so please do not copy and paste text from protocols technical descriptions or other resources on the web, including my lecture notes.

Report Format

1) Report Title
2) Student name, ID and affiliation
3) Abstract and keywords
4) Critical analysis of the current configuration

- ☐ Identify the vulnerabilities of the current configuration of the company's network (as described in Section 3: paragraphs 1 & 2 and shown in Figure 1) and discuss the types of security threats/attacks this company may face.

- ☐ Give one example of an attack that can exploit each identified vulnerability.

5) Secure network design proposal

- ☐ Identify and briefly discuss the security solutions (i.e., protocols and/or systems) needed to prevent the above attacks. Moreover, state which security solution(s) is deployed to defend against each identified threat(s).

- ☐ Identify and briefly discuss the security solutions needed to accommodate all the additional requirements of the company (as stated in Section 3 paragraph 3).

- ☐ Explain the implementation details of the proposed security solutions (i.e., at which level the solution is installed/deployed (networking devices, desktop machines, servers etc.), the model/type and sub-protocol you have chosen and why, etc.)

- ☐ Use a diagram(s) to support your explanation and show how those security solutions/systems are deployed within and across the different sites.

6) Conclusion
7) References – Use Harvard citation format. The Harvard Citation Reference can be downloaded from http://libguides.mmu.ac.uk/ld.php?content_id=14515784
Notes regarding the format of the report:

- ☐ Normal font should be Font 11, Times New Roman.
- ☐ Please use a cover page including the title, your name, affiliation and student ID.

PS. If you need any help in understanding this coursework you can either email s.djahel@mmu.ac.uk or come to see me during the following office hours:

Monday: 13-15
Tuesday: 11-12

5. Marking Criteria

Section	Evaluation criteria	Marks available
Abstract	- Concise abstract providing a short self-contained description of the report content, including adequately chosen keywords. - Vulnerabilities in the current company's network configuration identified and briefly explained. **15** (*5 vulnerabilities*).	**5**
Critical Analysis	- Adequate attack examples presented in a clear and concise way and supported by diagrams/figures, where appropriate. (*One example for each vulnerability*).	**15**
Secure Network Design	The proposed design should satisfy the following criteria: - Suitable security solutions proposed to face each identified vulnerability, and mapping between security solutions and attacks made correctly and in an efficient way. In addition, the choice of security protocols/systems models/types should be clearly justified. - The proposed design should accommodate all the additional requirements of the company in a **cost-effective way**: - Authentication requirement - Access control requirement - Secure connection among the different sites and secure remote access from home for employees. - Adequate attacks detection and mitigation techniques - Justification of the cost effectiveness of the proposed design - Efficient solution for DDoS (Distributed DoS) attack	**15** **30** **5 marks** **5 marks** **5 marks** **5 marks** **5 marks** **5 marks**

	- Use of adequately commented diagrams to show how the chosen security solutions are deployed across the whole company (headquarters and branches)	**10**
Conclusion	- Conclusion providing an excellent closure to the assignment by highlighting the benefits of the **5** proposed design and its potential limitations.	
Overall report	- Well written, well-structured and easy to read report - Use of adequate technical language - Appropriate citation of relevant references	**5**
	Total marks	**100**

Formative feedback: