Final Project: Network Security

This assignment is due on Friday 18th January, 2019 at 11:59 pm. Late submissions will be penalised by 20% per day. If you have a conflict due to travel, etc., please plan accordingly and turn in your assignment early.

Introduction

1. This final project will introduce you to the network protocols, security techniques, and CISCO IOS configurations and commands.
2. This final project will introduce you to study the network security trends.

Objective

- Gain exposure to core network protocols and concepts

- Gain exposure to security techniques

- Practice the network configuration using the CISCO IOS configurations and commands using CISCO Packet Tracer software

- Gain more knowledge regarding the network security trends

Read this first

This assignment asks you to write the answers in ENGLISH. Plagiarism, paraphrasing and downloading large amounts of information from external sources, will not be tolerated and will be dealt with severely. Although you should make full use of any source material, which would normally be an occasional sentence and/or paragraph (referenced) followed by your own critical analysis/evaluation, you will receive no marks for work that is not your own. Your work may be subject to checks for originality which can include use of an electronic plagiarism detection service.

Important Information:

- Student is required to submit the report.

- Student is required to submit the simulation file (*.pkt).

- Student is required to compress his/her simulation file and report together and submit to the ilms system by the deadline.

Instruction:

Our insurance company, if their success continues, are planning to expand into the international arena in the reasonably near future. Having consulted you about recommendations for their national operation's network security "Inshore Insurance" would now like you to set up a demonstration network to show how their international scale version of their network could work. Therefore, using the provided network diagram, develop an access control plan and implement a set of secure tunnel connections for the provided example network. The network provided is of course much larger than the actual one that you worked on before, but it does factor in all the firm's future expansion plans.

There are four branches in four countries, including Taiwan, Thailand, South Korea and Japan.

Your goal is to ensure that...

1. Taiwan branch has 3 VLANS. They are VLAN 10(Sales), VLAN 20(Finance) and VLAN 30(Accounting). Taiwan router, which is located in Hsinchu, is configured with Passwords and Privileges Commands as 'twroc@cisco' with VTY password as 'nihao'.

2. Thailand branch has 2 VLANs. They are VLAN 100(Audit) and VLAN 200(Statistical). Thailand router, which is located in Bangkok, is configured with Passwords and Privileges Commands as 'thailand@cisco' with VTY password as 'sawasdee'.

3. South Korea branch contains Web-server and Mail-server. South Korea router, which is located in Busan, with Passwords and Privileges Commands as 'southkorea@cisco' with VTY password as 'annyeong'.

4. Japan has only the office LAN in 192.168.100.0/24 subnet and each computer is getting IP address from the DHCP Server 192.168.100.2/24. Japan router, which is located in Osaka, with Passwords and Privileges Commands as 'japan@cisco' with VTY password is ' konnichiwa'.

5. All network addressing must conform to IP version 4 addressing.

6. Users of all regions except the Factory VLAN will have access to the Web-Server and Mail-server.

7. ALL the serial interfaces on the border routers must be regarded as DTE interfaces. All network domains should use the OSPF routing protocol as Area 0

8. Inter VLAN routing has been performed and 'RIPv2' or 'OSPF' (Select one) is used as the routing protocol.

9. *Additional configurations:* Add one more router in each country including Tainan (Taiwan), Phuket (Thailand), South Korea (Daegu) and Sapporo (Japan) to contain the Server. Each router must configure with the Passwords and Privileges Commands (you can assign them by yourself). The purpose of this additional configurations is to Configure the Standard Access Control List to allow just some PCs connected to the border router of each country to connect to the Server under our new routers.

Simulation--

A. (60 pts) Use the above network configuration requirement *(1-8)* to implement the Enterprises Network Model to show the use case of Vlan and how Real Scenario works when Different Branches of Enterprises are located in Different Cities and Countries.

    a. (15 pts) Network configuration requirement number 9 is a bonus point.

Report---

B. (40 pts)

    a. Please show your assign ip address list in the table.

    b. What are the purposes of Configure the Standard Access Control List?

    c. What are the 'RIPv2' and 'OSPF?

    d. What is the VLAN hopping?

    e. What is the DHCP spoofing?

    f. Please describe the security implications of a native VLAN.

    g. Please describe the BYOD architecture framework.

    h. Please list 10 important commands you use in this assignment and describe the reason what is the main purpose to use them.

    i. Please list all the commands you use in this assignment.