INSTITUTE OF TECHNOLOGY

BLANCHARDSTOWN

Academic Term	2013-14
Year of Study	4
Semester	Semester One
Date of Examination	Monday 20th January 2014
Time of Examination	3.30pm – 5.30pm

Programme Code	Programme Title	Module Code
BN402	Bachelor of Science (Honours) in Computing	COMP H4014
BN104	Bachelor of Science (Honours) in Computing	COMP H4014

Module Title	**Network Security**

Internal Examiner(s)	Michael O'Donnell
External Examiner(s)	Dr. Tom Lunney, Mr. Michael Barrett

Instructions to candidates:

1.	**To ensure that you take the correct examination, please check the module and programme which you are following is listed in the table above.**
2.	**Attempt ALL PARTS of Question 1 and any TWO other questions**
3.	**Question 1 is worth 40 marks and all other questions are worth 30 marks each.**

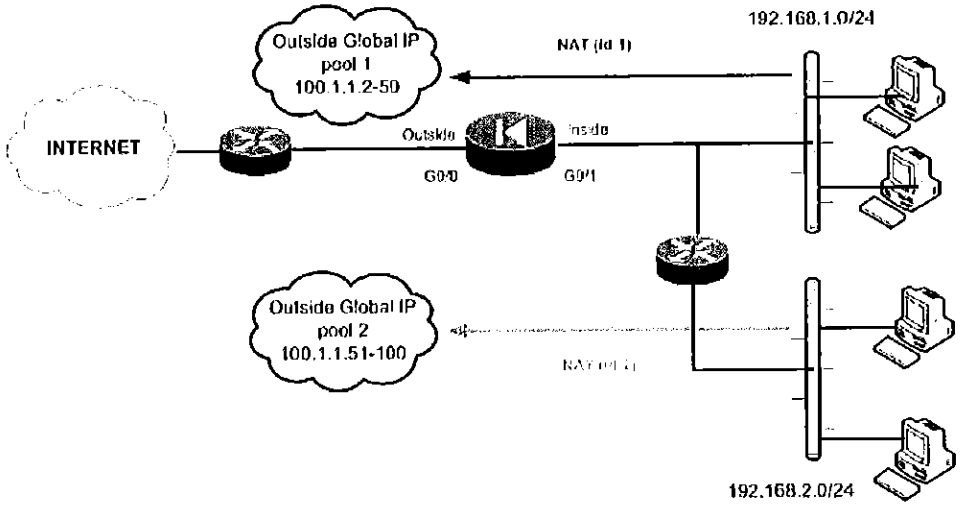
DO NOT TURN OVER THIS PAGE UNTIL YOU ARE TOLD TO DO SO

Question 1 (Compulsory)

(a) Tabulate the primary differences between the *RADIUS* and *TACACS+* protocols.

(8 marks)

(b)



Shown in the diagram above are two internal networks accessing the Internet through an ASA firewall. Configure *Dynamic NAT Translation* for these two internal networks.

(8 marks)

(c) Outline the primary features of a *Stateful Packet-filtering Firewall.*

(8 marks)

(d) Briefly outline the **three** functional components of the *AAA* architecture.

(8 marks)

(e) Describe, with the aid of a diagram, how a *Digital Signature* functions.

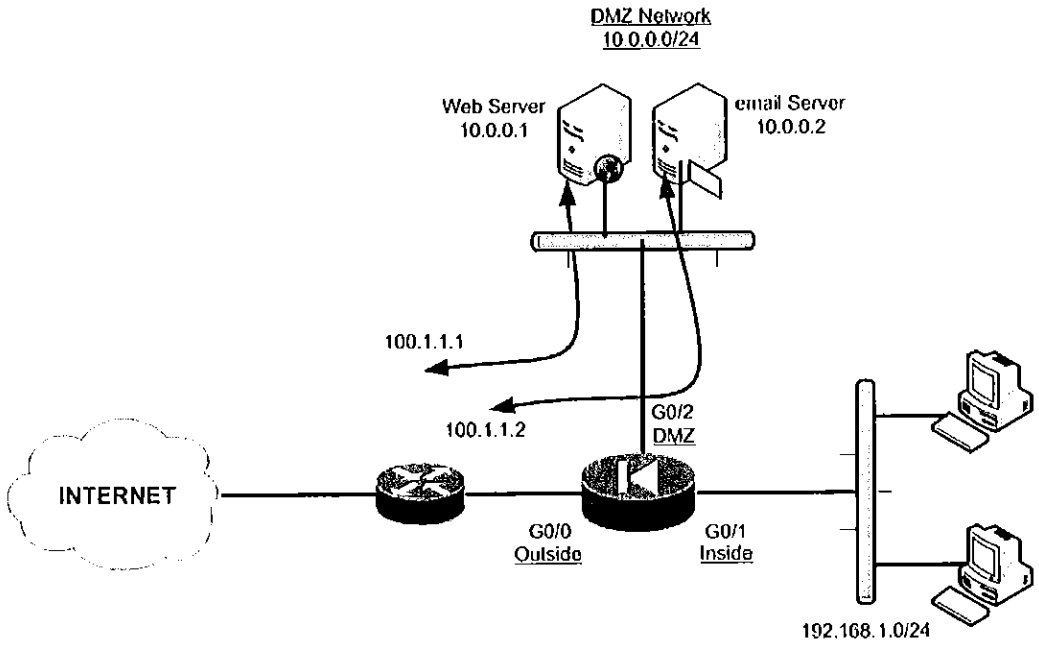
(8 marks)

Total: 40 marks

Answer any two questions from Questions 2, 3 and 4.

Question 2

(a)



The diagram above shows a Web Server and Email Server that needs to be accessible from the Internet through an ASA. Assume you have a whole Class C public address range of 100.1.1.0/24 available.

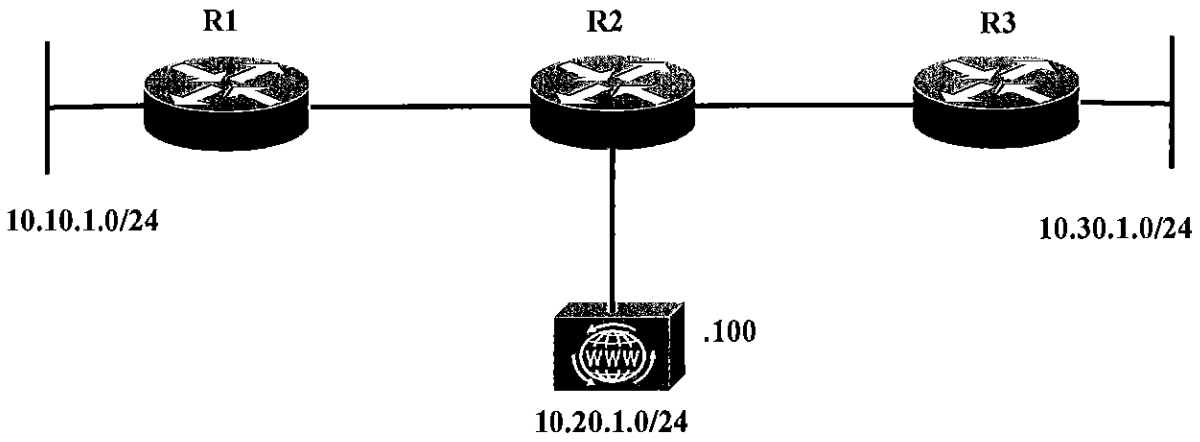
What configuration is needed to allow Internet access to both servers in the DMZ network.

(4 marks)

Question 2 (Contd. on next page)

Question 2 (Contd.)

(b)



Using the diagram above, implement *Access Control Lists* that accomplish the following:

(i) Allow only HTTP and FTP traffic to the server on R2 from the 10.10.1.0/24 subnet.

(ii) Allow all other traffic from the 10.10.1.0/24 subnet should be denied to the server on R2.

(iii) Traffic from any other source to any other destination should be allowed.

(12 marks)

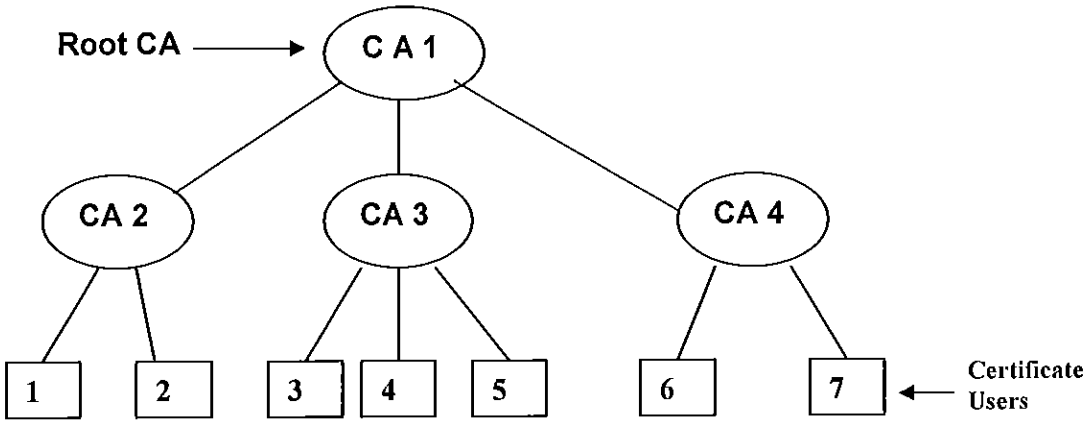
(c) Describe the operation of *Zone-Based Firewalls* regarding zone membership rules.

(14 marks)

Total: 30 marks

Question 3

(a) Outline the process of **User 2** getting and verifying the Digital Certificate of **User 6**.



(10 marks)

(b) A *Public Key Infrastructure (PKI)* provides a framework upon which you can base security services, such as encryption, authentication, and nonrepudiation.

Describe the operation of *PKI* under the following headings:

(i) The role of Certificate Authorities. Include in your answer reference to how an end user retrieves a CA certificate and how a certificate request for a Digital Certificate is made to the Certificate Authority.

(ii) How an end user Alice ensures Data Integrity and Confidentiality in the exchange of data with another end user Bob.

Illustrate your answers with diagrams.

(20 marks)

Total: 30 marks

Question 4

Intrusion Detection Systems (IDS) form an integral part of network security solutions. Describe in detail their operation under the following headings:

(a) Types of IDS Sensors

(8 marks)

(b) Host-based IPS compared with Network-based IDS

(8 marks)

(c) Types of Signature Alarms

(8 marks)

(d) IDS Best Practices

(6 marks)

Total: 30 marks