INSTITUTE OF TECHNOLOGY

BLANCHARDSTOWN

Academic Term	2014-15
Year of Study	4
Semester	Semester One
Date of Examination	Mon 12th Jan 2015
Time of Examination	12.30pm – 2.30pm

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) *Intrusion Detection Systems (IDS)* form an integral part of network security solutions. Outline the **four** types of Signature Alarms.

(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, in brief, the operation of a *Keyed Hash Message Authentication Code (HMAC).*

(8 marks)

Total: 40 marks

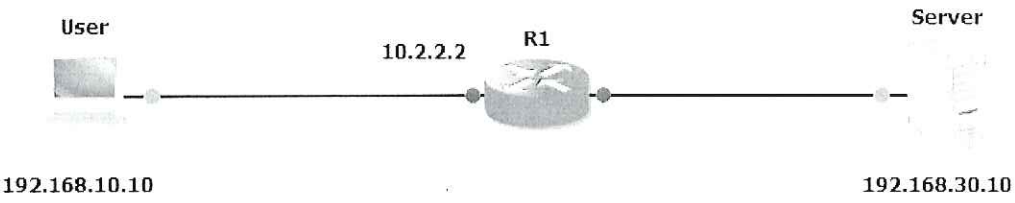
Answer any two questions from Questions 2, 3 and 4.

Question 2

(a) *Access Control Lists (ACLs)* can use the *Established* option in their configuration. How does this option work and what is the advantage of using it.

(6 marks)

(b)



The diagram above shows a User that needs to access resources on the Server. You decide that the best solution is to allow temporary access for a period of 10 minutes after the user has authenticated with the router first.

(i) What configuration needs to be configured on R1 to make this happen?

(8 marks)

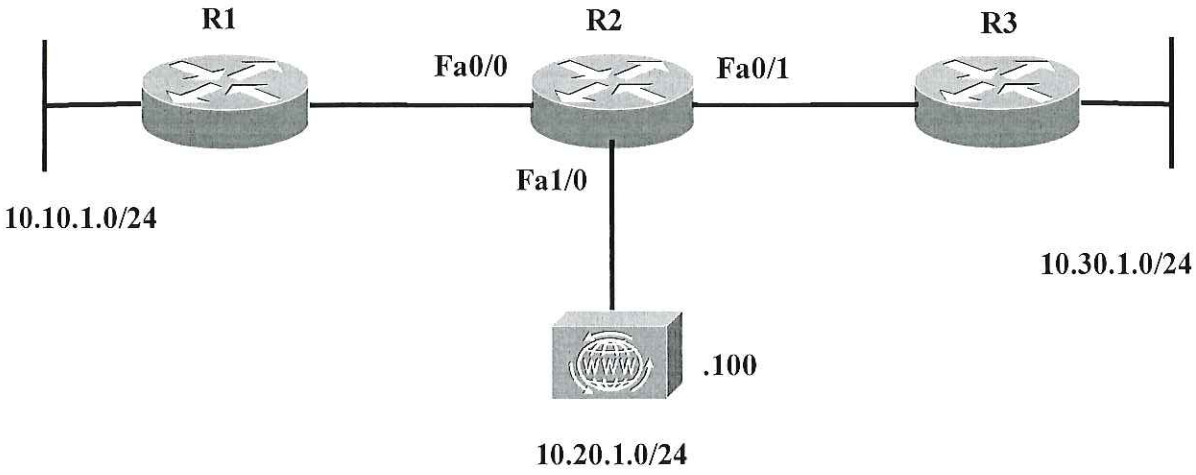
(ii) Outline the security **benefits** of your approach over using standard and static extended *Access Control Lists (ACLs).*

(4 marks)

Question 2 (Contd. on next page)

Question 2 (Contd.)

(c)



Using the diagram above, implement *Access Control Lists* on R2 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) All other traffic from the 10.10.1.0/24 subnet should be denied to the server 10.20.1.100 on R2.

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

(12 marks)

Total: 30 marks

Question 3

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

(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.

(10 marks)

(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.

(10 marks)

Total: 30 marks

Question 4

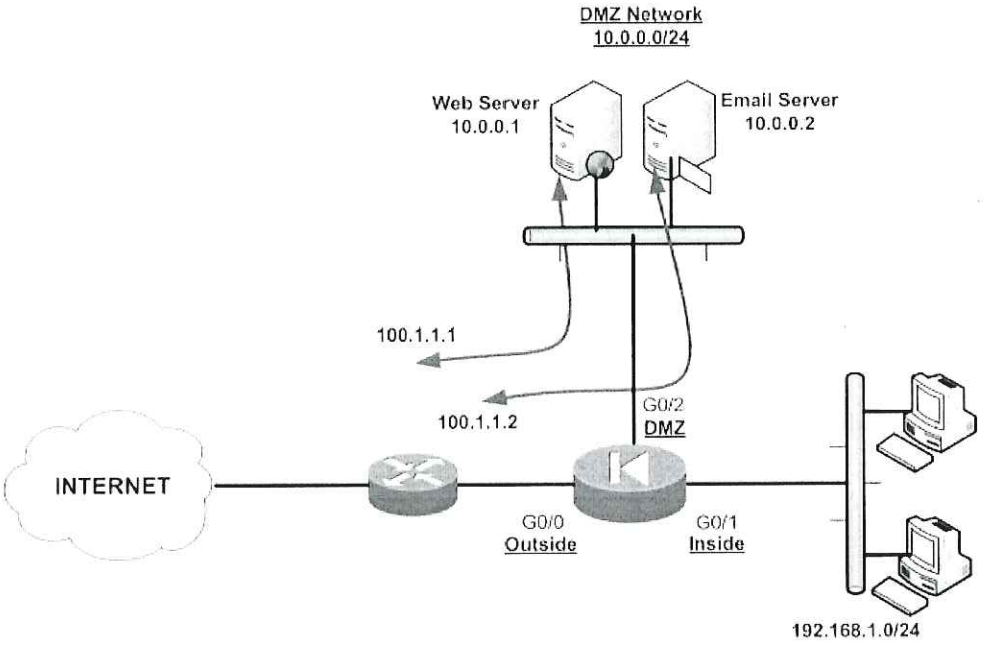
(a) Outline the main **limitations** in using a Firewall to protect a network.

(8 marks)

(b) Give an overview of **four** advanced features to be found in an *Adaptive Security Appliance (ASA).*

(12 marks)

(c)



Configure the ASA in the topology above so that both the Web Server and the Email Server can be accessed from the Internet.

(10 marks)

Total: 30 marks