INSTITUTE OF TECHNOLOGY BLANCHARDSTOWN

Year	Year 4
Semester	January, Semester 1
Date of Examination	Friday 13 January 2012
Time of Examination	3.30pm – 5.30pm

Programme Title	Bachelor of Science (Honours) in Computing
Programme Code	BN402
Module Title	**Network Security**
Banner Module Code	COMP H4014

Programme Title	Bachelor of Science (Honours) in Computing
Programme Code	BN104
Module Title	**Network Security**
Banner Module Code	COMP H4014

Internal Examiner(s): **Mr. Michael O'Donnell**

External Examiner(s): **Dr. Richard Studdert**

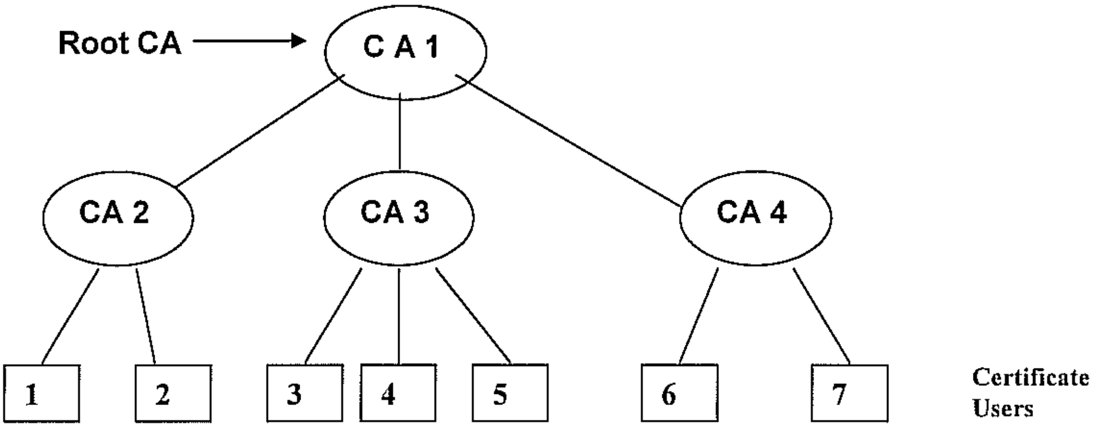
Instructions to candidates:

1) To ensure that you take the correct examination, please check that the module and programme which you are following is listed in the tables above.
2) This paper consists of <u>four</u> questions. You <u>must</u> do Question 1 and any other <u>two</u> questions.
3) This paper is worth 100 marks. Question 1 is worth 40 marks and each of the other questions is worth 30 marks.

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

Question 1 (Compulsory Question)

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



(8 marks)

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

(8 marks)

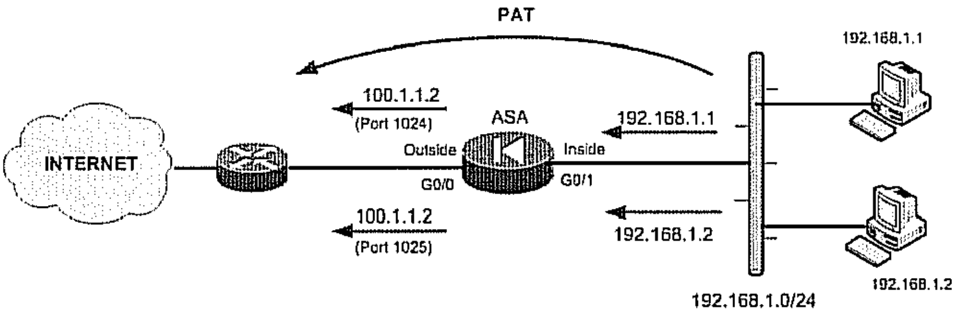
(c) Describe the **four** types of Signature Alarms found in *Intrusion Detection Systems (IDS)*.

(8 marks)

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

(8 marks)

(e)



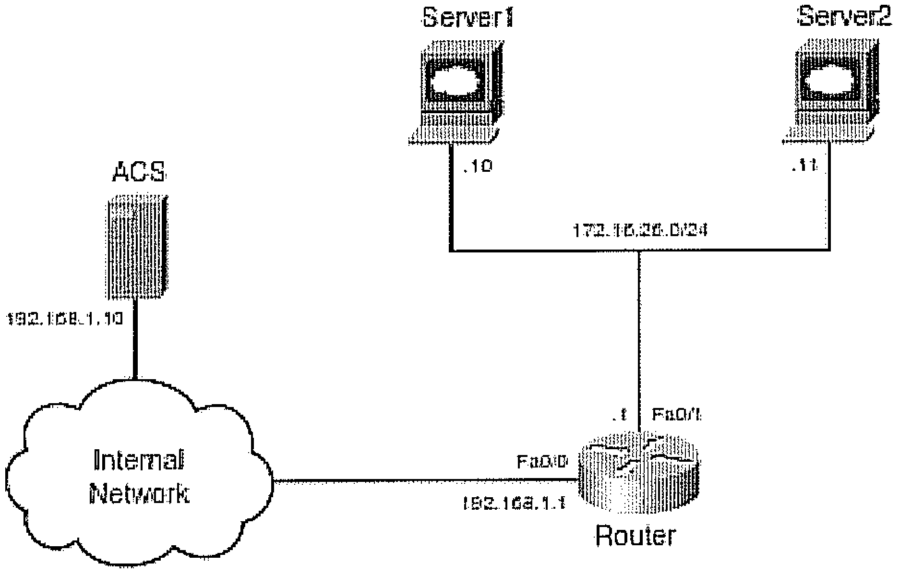
Configure *Port Address Translation* for the topolgy in the diagram above.

(8 marks)

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

Question 2

(a) Case Study – Authentication Proxy



ABC Inc. has two web servers in a network separated from their internal network by a router. These servers contain sensitive data. The company wants access to these servers to be restricted and monitored. The employees who need access to Server1 are members of the Research group on ACS. The employees who need access to Server2 are members of the Engineering group on ACS.

The ACS server is in the internal network. The inbound ACL on the ingress interface of the router denies all traffic to the servers. The company wants the router to authenticate all HTTP sessions and then download ACL from ACS to permit traffic as needed. The router is added in ACS as a TACACS+ client with a shared key of *secret*.

Assuming the configuration of the ACS has already been done, what configuration needs to be implemented on the router to effect the requirements of the Case Study above.

(10 marks)

Question 2 (Contd. on next page)

Question 2 (contd)

(b) Case Study – AAA Authentication & Authorization

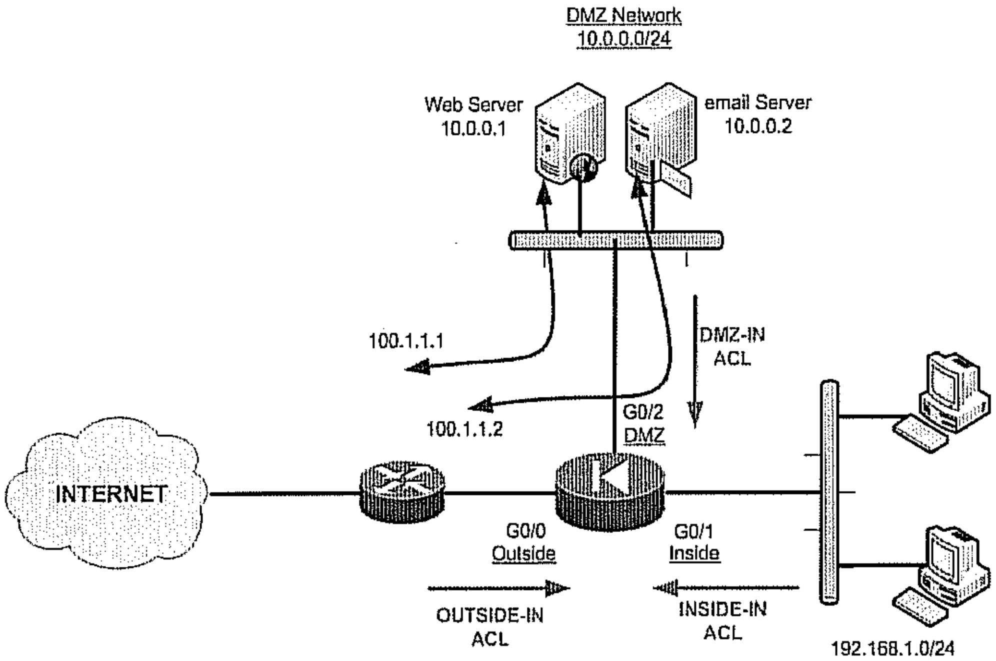
XYZ Inc. has purchased an ACS and they want to use TACACS+ to authenticate all administrative session on their ASA. In addition to that, they want to ensure that users belonging to the Admins can execute all commands except *shutdown*.

The IP address of the ASA is 192.168.1.1 and the IP address of ACS is 192.168.1.10 and the secret key is *secret* between the ACS and the ASA.

Assuming the configuration of the ACS has already been done, what configuration needs to be implemented on the router to effect the requirements of the Case Study above.

(10 marks)

(c)



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

What configuration on the ASA needs to be implemented to allow Internet access to both servers in the DMZ network.

(10 marks)

Question 3

(a) Describe the operation of Context-Based Access Control (CBAC) as an example of providing security up to the application layer on an IOS Firewall router.

(8 marks)

(b) Describe the **five** steps involved in the manual configuration of a *Zone-Based Firewall.*

(10 marks)

(c) Outline the primary features of a *Stateful Packet-filtering Firewall.* Include in your answer reference to its limitations.

(12 marks)

Question 4

(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.

(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)