Security Applications in Networking and Distributed Systems

Examination - Answers

May 2015

Remarks:

The exam is closed books and notes. You are allowed to keep a single sheet of paper with handwritten notes. The duration is 2 hours.

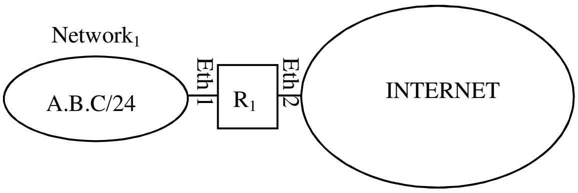
Write your name on every sheet you return. Answer in English or in French.

The answers should be concise but supported by a brief explanation.

The total number of points is 30.

Q1 (4 points)

The figure below depicts a private network connected to the Internet through an edge router R_1.



IP spoofing denotes an attack feature that consist of sending packets bearing randomly chosen source IP addresses for various malicious purposes such as denial of service at the destination.

a) Some of IP spoofing attacks targeting Network$_1$can be detected at R_1 using the information included in the routing tables of R_1. Briefly describe this detection scheme, *without* specifying any details regarding filtering rules (Hint: Reverse Path Forwarding). Are there any limitations to this technique?

b) Can some of the IP spoofing attacks be detected and prevented only by using packet filtering rules in R_1? Where would these attacks originate from? State the filtering rules designed for that purpose, by using the *iptables* notation as in the following sample ruleset. Are there any limitations to this technique?

```
iptables -F FORWARD
iptables -N FORWARD
iptables -P FORWARD DROP
iptables -A FORWARD -i Ethy -d y.y.y.y/ DD -s x.x.x.x/DD -j ACCEPT
. . . . . . . . . . .
. . . . . . . . . . .
```

Answer:

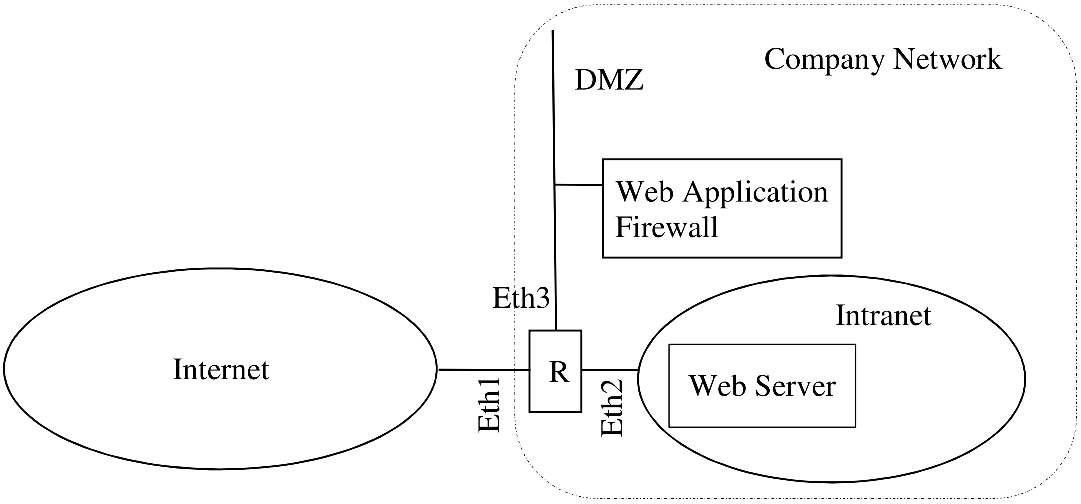
a) Based on reverse path forwarding, for every packet received from Internet, R_1 would look up in the routing table associated with the network interface from which the packet is received, for an (reverse route) entry towards the source address of the packet. Packets would only be accepted if such lookup queries return a valid entry in the table. If a destination can be reached through multiple paths and traffic to and from Network$_1$ do not follow the same path, then the RPF technique might raise a false alarm for IP spoofing.

b) Some IP spoofing attacks originating from Network$_1$ can be detected using the following ruleset:

```
iptables –F FORWARD
iptables –N FORWARD
iptables –P FORWARD DROP
iptables –A FORWARD –I Eth1 –s A.B.C/24 –j ACCEPT
iptables –A FORWARD –I Eth2 –s !A.B.C/24 –j ACCEPT
```

Limitations of this technique are: 1) a node in Network 1 that impersonates another node from the same network cannot be detected. 2) majority of IP spoofing attacks originating from the Internet, including the ones mentioned in a) cannot be detected.

Q2 (6 points)



The above figure depicts a simple network interconnection scenario whereby

- address block 192.113.4.0/24 is allocated to the Company Network
- R is a router and a packet filter based on iptables equipped with the (stateful) netfilter package and the network address translation (nat) package
- interface Eth3 of R is connected to a Demilitarized zone (DMZ)
- a Web Application Firewall (WAF) runs on host 192.113.4.10 located in the DMZ
- the port number for HTTP is 80
- a Web Server runs on a host located inside the Intranet.

The security policy governing this network is summarized by the following statements:

- Hosts located within the Intranet are authorized to initiate connections and to communicate through those connections with hosts located in the Internet using the application protocol identified by TCP port number Q.

- Hosts from the Internet are authorized to initiate connections and to communicate through those connections with the Web Server using HTTP.

- HTTP traffic between the Internet and the Web Server must be screened by the Web Application Firewall.

- All traffic across router R that is not explicitly authorized by the statements of this policy must be blocked.

Answer the following questions by keeping in mind the goal of enforcing this security policy:

a) What kind of IP addresses should be assigned to the hosts located in the Intranet? Specify the address range assigned to the Intranet and select one of this addresses as the IP address of the Web Server.

b) If Web Server is to be used as the public web server of the company, under which IP address should the company's public web server be announced in the Internet through DNS? How does the traffic from the Internet reach the Web Server using this IP address?

c) Suggest a set of filtering rules required to implement the abovementioned policy.

Answer:

a) hosts in the Intranet should be assigned private addresses, let 192.168.1.0/24 be the address block used for this purpose and 192.168.1.10 the address of the Web Server

b) WAF's public IP address 192.113.4.10. The traffic from the Internet first reaches the WAF then after screening the traffic, WAF redirects it to 192.168.1.10 on the Intranet.

c)

```
iptables –F FORWARD

iptables –N FORWARD

iptables –P FORWARD DROP

# Hosts from Intranet are authorized to initiate the application protocol identified by TCP port
number Q with hosts located in the Internet

iptables –A FORWARD -i Eth2 -o Eth1 -p tcp -s 192.168.1.0/24 --dport Q -m state

--state NEW,ESTABLISHED –j ACCEPT

iptables –A FORWARD -o Eth2 –p tcp -m state --state  ESTABLISHED –j ACCEPT

# WAF is authorized to establish web connections with Web Server.

iptables –A FORWARD -i Eth3 -o Eth2 -p tcp -s 192.113.4.10 --d 192.168.1.10 --dport 80 -m
state --state NEW,ESTABLISHED –j ACCEPT

iptables –A FORWARD -o Eth3 -i Eth2 -p tcp -s 192.168.1.10 -d 192.113.4.10 -m state

--state  ESTABLISHED –j ACCEPT
```

# Internet hosts are authorized to establish web connections with WAF.

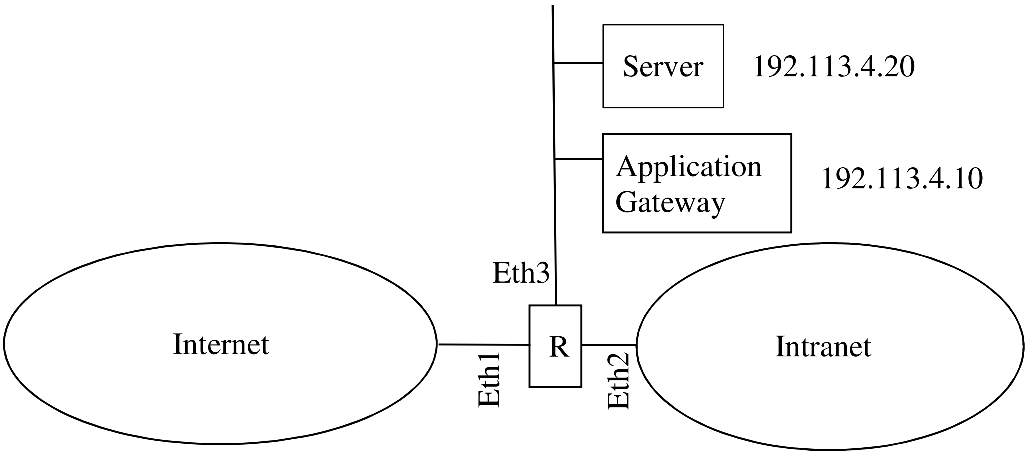
iptables –A FORWARD -i Eth1 -o Eth3 -p tcp -d 192.113.4.10 --dport 80 -m state --state NEW,ESTABLISHED –j ACCEPT

iptables –A FORWARD -i Eth3 -o Eth1 -p tcp -s 192.113.4.10 -m state --state ESTABLISHED –j ACCEPT

# NAT with port translation for internal hosts identified with a private address.

iptables -nat -A POSTROUTING -i Eth2 -o Eth1 -j SNAT --to 192.113.4.20

Q3 (3 points)



The above figure depicts a simple network interconnection scenario whereby

- R is a router and a packet filter based on iptables equipped with the (stateful) netfilter package and the network address translation (nat) package.

- an Application Gateway for the application protocol identified by port number Q runs on host 192.113.4.10.

- a Server runs on host 192.113.4.20.

Hosts from the Internet are authorized to connect to the Server using the application protocol Q and the Server's IP address (192.113.4.20) is announced to the Internet using DNS.

Specify the details of the filtering rule which assures that all traffic from the Internet to the Server gets screened by the Application Gateway for the purpose of application level security verifications such as malware filtering, data leak prevention, etc..

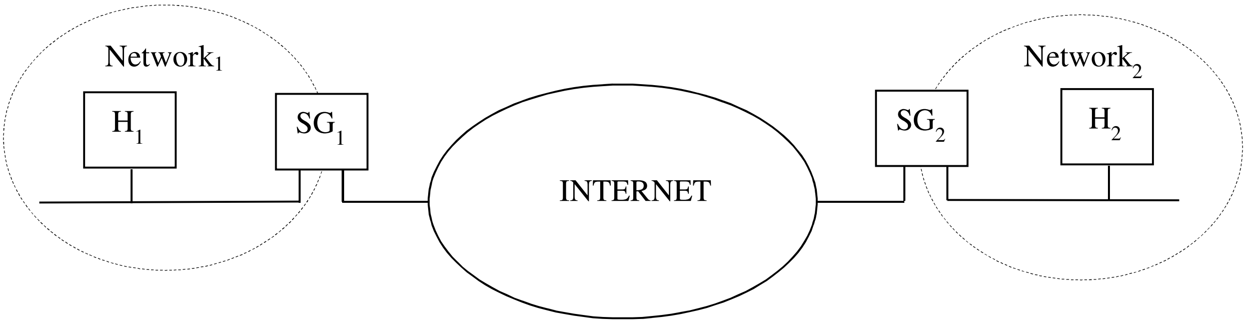
Answer:

Iptables –nat –A PREROUTING -i Eth1 -o Eth3 –p tcp -d 192.113.4.20 –j DNAT –to 192.113.4.10

Q4 (3 Points)

Network$_1$ and Network$_2$ in the below figure belong to the same organization. The goal is to interconnect the two local networks through the Internet using IPSec protocols in order to achieve a Virtual Private Network as if the nodes in both networks were part of a single private network.

We assume that H_1 and H_2 are local hosts connected to $Network_1$ and $Network_2$, respectively, and SG1 and SG2 are security gateways equipped with IPSec protocol suite and connected to both the Internet and the local networks as depicted in the figure.



a) Suggest an addressing scheme by assigning IP addresses to H_1, SG_1, H_2, and SG_2 for each of their interfaces as shown in the figure, by taking into account usual network security criteria.

b) State the security associations (SA), protocol type and mode of operation for each SA of the IPSec protocol configuration required to implement the Virtual Private Network scenario.

c) Let's assume that an IP packet carrying transport layer data is transmitted by H_1 to H_2 using the suggested IPSec solution. What is the structure of such a packet captured at the link between SG_1 and SG_2? Describe the packet structure using a simple figure whereby the following fields are positioned *without* specifying the details of the fields except where indicated otherwise:

- IP Headers
- IP Addresses in each IP header (specify using the values assigned in a))
- IPSec protocol headers
- Upper Layer Header

and indicate the fields that are protected by authentication and/or confidentiality.

Answer:

a) H_1: 192.168.1.1 (private Address)

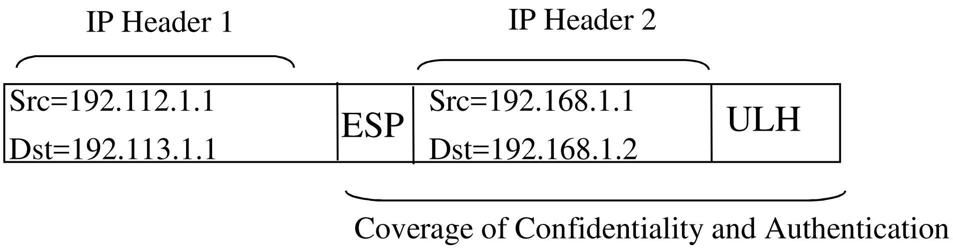
SG_1: 192.168.1.10 (private address) and 192.112.1.1 (public address)

H_2: 192.168.1.2 (private Address)

SG_2: 192.168.1.20 (private address) and 192.113.1.1 (public address)

b) At least one SA with IPSec ESP in tunnel mode between SG1 and SG2.

c)



Q5 (2 Points)

a) What is the most important security requirement with the Domain Name System (DNS)?

b) What is the solution to this problem? State either the main features of the standard designed to prevent this problem or briefly suggest the details of a basic security protocol out of your own imagination.

Answer:

a) The responses sent on behalf of a DNS server can be faked or tampered with due to the capturing of the DNS requests by some intruder and to further impersonation of the legitimate server.

b) Data origin authentication with the DNS responses or the DNS SEC standard whereby the response messages include the signature by the DNS server of the regular DNS Resource Record.

Q6 (2 Points)

a) Briefly describe the “prefix hijacking” attack with BGP.

b) Can data origin authentication be a solution that prevents this attack entirely? Briefly describe a simple scenario whereby prefix hijacking can be perpetrated despite the proper authentication of the parties.

Answer:

a) cf. course material.

b) Data origin authentication does not solve the problem in its entirety since a rogue BGP router can inject bogus route announcements and the authentication of the origin of these announcements does not help detect the fact that they propagate erroneous routing information.

Q7 (3 Points)

Let’s suppose a web-based secure electronic banking application through which each customer can access the bank’s web site and perform the following operations:

- look up his/her account to read the balance and the details of operations,

- place orders in the stock market (sell or buy shares).

a) Briefly state the security services required by this application.

b) Amid the following alternatives which one is the most suitable solution to provide the security services required by this application? Briefly discuss about the suitability of each alternative.

- a packet filtering stateful firewall

- a solution using IPSec protocols

- a client and server applications using TLS/SSL.

Answer:

a) authentication of the customer, confidentiality and integrity of all messages, optionally non-repudiation of the origin for messages sent by the customer.

b) TLS/SSL because this is the only one that would be end-to-end and be supported by clientless terminals on the user side.

Q8 (4 Points)

a) Let’s imagine simple scenario whereby

- NW is a local area network based on wireline Ethernet

- All devices connected to NW are within the premices of a company confined in a building with physical access control.

- The people who are authorized to enter the building are trusted in that they do not undertake any malicious activity.

Imagine that in the aforementioned scenario, the wireline Ethernet is replaced with wireless 802.11 (WiFi). In the resulting configuration of NW that is based on 802.11

a) what are the new security exposures regarding the access to the communication system (NW)?

b) what are the new security exposures regarding the data exchanged through NW?

c) mention a solution for each of the security requirements raised by the exposures in a) and b).

Answer:

a) Devices operated by untrusted people can get access to the wireless NW from outside the building by escaping to the physical access control.

b) Devices operated by untrusted people can eavesdrop the data exchanged by legitimate parties located within the building, impersonate those parties, and tamper with the data exchanged among those.

c) data confidentiality, integrity and data origin authentication are minimum requirements mapping to exposures in a) an network access control corresponds to the ones in b). WPA, WPA2 provide the solution to the first category of requirements whereas 802.1x can be used to assure network access control.

Q9 (3 points)

a) Briefly sketch an access control solution most suitable for each of the following scenarios, by referring to basic concepts such as access control lists, capability lists, etc.. State the rationale for your choice in each scenario. Specify if standards like SAML and XACML are suitable for the implementation of each access control solution. Briefly mention the components that would be implemented using these standards.

a) On-line access to newspapers from several servers belonging to different media providers. There are several thousands of customers, several hundreds of newspaper servers, and several hundreds of authorization centers. Each customer can request anyone of several authorization centers to get an access right for anyone of the newspapers for six months.

b) On-line professional news service. The service infrastructure consists of several thousands of customers, and a single news server. Customers get a monthly subscription to read the news.

Answer:

a) capability list (CL) technique is the most suitable because of the lack of centralization for the servers. When the population of the servers is neither small nor under the control of a single organization, management of ACL's for a dynamic user population is too complex. SAML would be very suitable to implement the CL granted to each customer.

b) access control lists (ACL) is the most suitable approach since the resource is centralized (single server) and updates are not frequent. XACML would be suitable to store the dynamic access control policy.