Module 3 Assessment (Advanced Networking 3rd)

Due Oct 8 at 11:59pm **Points** 20 **Questions** 17
Available Sep 25 at 12am - Oct 9 at 11:59pm **Time Limit** 45 Minutes
Allowed Attempts 2

Instructions

You have two attempts to take this assessment with the highest score being retained. The assessment has a time limit of 45 minutes.

Suggestion: take the assessment in the beginning of the module and then after the reading and assignments are done. You can then use the results of both to gauge your learning and retention.

Take the Quiz Again

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	42 minutes	13 out of 20 *

* Some questions not yet graded

Answers will be shown after your last attempt

Score for this attempt: **13** out of 20 *
Submitted Oct 3 at 10:38am
This attempt took 42 minutes.

Question 1 — 1 / 1 pts

A firewall is monitoring traffic going into or out of a network. It allows only traffic that is part of an active connection or initiating a new connection. What kind of firewall is this?

- A stateful inspection firewall

- An application firewall
- A host-based firewall
- A proxy server

A is correct. A stateful inspection firewall identifies active connections as they are created and monitors the status of these connections in a state table within the firewall. B, C, and D are incorrect. An application firewall includes multiple elements and monitors traffic for different protocols. A host-based firewall monitors traffic for a specific host. A proxy server is not a firewall.

Question 2

1 / 1 pts

How can you provide defense diversity when implementing a DMZ?

- Ensure that you use at least two firewalls.
- Ensure that you use at least two firewalls from different vendors.
- Ensure that you use at least two firewalls from the same vendor.
- Ensure that you use at least two packet-filtering firewalls.

B is correct. A demilitarized zone (DMZ) is typically created with two firewalls. Using firewalls from two separate vendors provides defense diversity for the DMZ. It requires the attacker to have more skills and knowledge to exploit both firewalls. A, C, and D are incorrect. Just having two firewalls (of any kind) doesn't provide defense diversity; instead, the two firewalls must be from different vendors.

Question 3

1 / 1 pts

Of the following choices, which is NOT a step that an organization will take to harden a private branch exchange?

- Implement physical security
- Block all calls
- Control call forwarding
- Control long distance calling

B is correct. Because the purpose of a private branch exchange (PBX) is to support the use of phones, the organization would not block all phone calls. A, C, and D are incorrect. Implementing physical security, controlling call forwarding, and controlling long distance calling are all valid security steps to protect the phone system.

Question 4

1 / 1 pts

Of the following choices, which is NOT used as a VPN tunneling protocol?

- L2TP
- PPTP
- IPSec
- SRTP

D is correct. Secure Real-time Transport Protocol (SRTP) provides confidentiality, message authentication, and replay protection for audio and video traffic, including VoIP. It is not used as a virtual private network (VPN) tunneling protocol. A, B, and C are incorrect. Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol, and Internet Protocol Security (IPSec) can all be used as VPN tunneling protocols.

Question 5

1 / 1 pts

Of the following choices, which is NOT valid method that a client can use to create a remote access connection?

- Dial-up
- VPN
- ISDN
- RADIUS

D is correct. The Remote Authentication Dial-In Service (RADIUS) is a service that provides centralized authentication, authorization, and accounting (AAA) for remote clients. It does not create a connection. A, B, and C are incorrect. Virtual Private Network (VPN) connections can be created using phone connections (both dial-up and ISDN lines will work) or a VPN.

Question 6

1 / 1 pts

An organization has a DMZ using two firewalls of the same brand and model. A security professional is strongly recommending that the DMZ be

upgraded using firewalls from different vendors. What is the goal?

- (●) To provide defense diversity
- ( ) To increase administrative tasks
- ( ) To reduce administrative tasks
- ( ) To reduce costs

A is correct. A demilitarized zone (DMZ) is typically created with two firewalls. Using firewalls from two separate vendors provides defense diversity for the DMZ. It requires the attacker to have more skills and knowledge to exploit both firewalls. B, C, and D are incorrect. Although having firewalls from separate vendors will likely increase administrative tasks, that isn't the goal. It's doubtful that adding a firewall from a different vendor will reduce administrative tasks or reduce costs, but it will increase security.

Question 7

1 / 1 pts

Many firewalls require the placement of a "deny any" rule in the firewal to block all traffic that is not explicitly allowed. However, many firewalls use this rule even if it isn't defined. What is this called?

- ( ) Defense diversity
- (●) Implicit deny
- ( ) Explicit deny
- ( ) Defense in depth

B is correct. A packet filtering firewall often uses an implicit deny policy. All traffic is blocked (implicitly denied) unless there is a rule in the access control list (ACL) that explicitly allows traffic. A, C, and D are incorrect. Defense diversity uses more than one brand of firewall in a demilitarized zone (DMZ). Explicit deny includes the rule. Defense in depth includes multiple layers of security.

Question 8

1 / 1 pts

Which of the following provides the best definition of a network-based firewall?

- It provides protection for systems by blocking malicious traffic from reaching individual hosts.
- It uses both packet filtering and application filtering.
- It provides only packet filtering.
- It provides protection for a network by filtering and blocking malicious traffic coming from the Internet.

D is correct. A network-based firewall provides protection for a network by filtering and blocking malicious traffic coming from the Internet. A, B, and C are incorrect. A how-based firewall provides protection for systems by blocking malicious traffic from reaching individual hosts. Network-based firewalls can use a variety of different filtering methods and are not limited to only packet filtering or application filtering.

Question 9

1 / 1 pts

Which of the following is used for central authentication for VPNs?

- L2TP
- PPTP
- RADIUS
- Kerberos

C is correct. The Remote Authentication Dial-In Service (RADIUS) is a service that provides centralized authentication, authorization, and accounting (AAA) for virtual private network (VPN) clients. A, B, and D are incorrect. Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP) are tunneling protocols used with remote access. Kerberos si used for network authentication.

Question 10

1 / 1 pts

A packet-filtering fireweall can filter traffic going into or out of a network. What does a packet-filtering firewall use to identify what traffic is filtered?

- SSL
- TLS
- SSH
- ACL

D is correct. Access Control List (ACL) is a list of rules to filter traffic based on source or destination IP addresses, subnet addresses, entire domains, ports, and or protocols. A, B, and C are incorrect. Secure Socket Layter (SSL), Transport Lay Security (TLS), and Secure Shell (SSH) are all protocols used to secure traffic, not filter it.

Question 11

1 / 1 pts

A packet-filtering firewall includes a “deny any” rule. Where should this rule be placed?

- At the beginning of the ACL
- At the end of the ACL
- Before any Allow rules
- The placement of this rule does njot matter

B is correct. If a previous rule doesn’t explicity allow the traffic, this rule will block it, so the rule should be palced last in the ACL. A, C, and D are incorrect. If you place this rule anywhere but at the end of the list, it will ignore any other rules in the ACL and deny all traffic. The placement does matter.

Question 12

1 / 1 pts

A firewall administrator wants to block ICMP traffic using a packet-filtering firewall. What should the ACL use to identify the ICMP traffic.

- Protocol number 1

Protocol number 6

Port 1

Port 6

A is correct. The protocol number for Internet Control Message Protocol (ICMP) is 1 and a packet-filtering firewall can filter traffic based on the protocol number by using an access control list (ACL). B, C, and D are incorrect. The protocol number for Transmission Contrl Protocol (TCP) is 6. ICMP is identified by a port. Although not included in this question, the protocol number for Internet Group Message Protocol (IGMP) is 2, User Datagram Protocol (UDP) is 17, Internet PRotocol Security (IPSec) AH is 51, and IPSec Encapsulating Security Protocol (ESP) is 50.

Question 13

1 / 1 pts

A firewall administrator wants to ensure that all traffic going through a packet-filtering firewall is using IPSec ESP. What should the administtrator use in the ACL to identify the IPSec traffic?

Protocol 1

Protocol 6

Protocol 50

Protocol 51

C is correct.The protocol number for Internet Protocol Security (IPSec) Encapsulating Security Protocol (ESP) is 50, and a packet-filtering firewall can filter traffic based on the protocol number. A, B, and C are incorrect.

Incorrect

Question 14

0 / 1 pts

An application firewall is also known as an _____ and an _____.

application layer firewall, application proxy firewall

Question 15

Not yet graded / 1 pts

In your own words, describe the purpose of Network Address Translation, or NAT.

Your Answer:

NAT allows for the preservation of IPv4 addresses through translating private IP addresses to public ones. NAT also adds a little bit of security to the network by masking the internal IP addresses from the outside making it harder for a bad actor to access internal resources from the internet

Question 16

Not yet graded / 2 pts

Describe the purpose of each A in AAA.

Your Answer:

Authentication: This is the step that verifies the identity of the system users or the identity of the device trying to access network resources.

Authorization: This is the step where the level or permissions authenticated users or devices are allowed to perform on the network, through checking the user or device's credentials against permission lists, roles and policies.

Accounting: This step tracks or records the activities of an authenticated and authorized user or device while logged into the network

Question 17

Not yet graded / 3 pts

As the Information Assurance specialist in your company, you are asked whether the company should move their operations to the cloud. What would be your pros and cons of doing this transition?

Your Answer:

There are many Pros and Cons to moving operations to the cloud.

From an information assurance stand point the pros would be :

Accessibility: data and network resources would be available from pretty much anywhere which would allow for remote work increased continuity across large distances.

Updates and maintenance: cloud providers usually handle all of the updates, patches and other maintenance.

Disaster recovery: cloud providers also usually provide detailed disaster recovery and redundancy options

The Cons would be:

Compliance Challenges: meeting industry compliance requirements might be a bit challenging

Reliability: Service outages could be an issue

Data Security and privacy: There might be concerns about how secure and private the data is when it is stored on third party servers.

Quiz Score: **13** out of 20