Exam Report: 13.10.7 Practice Questions

Date: 4/15/2020 5:24:58 pm
Time Spent: 0:52

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 29%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

A user can't make an RDP connection from outside the network to a server inside the network.

Which network device will a network administrator MOST likely configure to allow this connection?

- Hub
- Firewall
- Switch
- Access point

Explanation

A firewall filters network traffic based on a set of rules. The network administrator will most likely configure the firewall to allow RDP traffic.

A switch maintains a table of MAC addresses by port and forwards network frames to only the port that matches the MAC address. An access point gives Wi-Fi access to a network. A hub transmits a data frame to every port except the port that received the data frame.

References

TestOut PC Pro - 13.10 Firewalls
[e_firewall_pp6.exam.xml Q_NET_FIREW_01]

Question 2: Correct

A technician is tasked with installing a network-enabled camera that runs on power that is supplied through its network connection. The network device that connects to the camera does not have the capability to supply this power. There is a power outlet close to the camera.

Which of the following devices can be used to supply power?

- A repeater
- A Power over Ethernet injector

- ◯ A modem

Explanation

A Power over Ethernet (PoE) injector acts as an intermediary device between a non-PoE switch and a PoE device to inject power over the Ethernet cable.

An Ethernet over Power adapter uses the existing electrical wiring to transmit network traffic. A modem modulates an analog signal to encode digital information for transmission and demodulates the signals to decode the transmitted information. A repeater is a simple network device that receives and transmits a signal to extend a network's reach.

References

TestOut PC Pro - 13.10 Firewalls
[e_firewall_pp6.exam.xml Q_NET_FIREW_02]

Question 3: Incorrect

You want to be able to access your home computer using Remote Desktop while traveling. You enable Remote Desktop, but you find that you cannot access your computer outside of your home network.

Which of the following is the BEST solution to your problem?

- ◯ Configure a VPN connection to your computer.
- ◉ ~~Open the Telnet and SSH ports in your firewall.~~
- ➡ ◯ Open the firewall port for the Remote Desktop protocol.
- ◯ Move your home computer outside of the firewall.

Explanation

You need to open the firewall port for the Remote Desktop program. Firewalls prevent all traffic except authorized traffic. To allow a specific program, open the port that corresponds to the port used by that application.

Placing your computer outside of the firewall leaves it open to attack. A VPN encrypts communications between two computers through the internet. However, the VPN will not allow a Remote Desktop connection. The Telnet and SSH ports do not apply to this scenario.

References

TestOut PC Pro - 13.10 Firewalls
[e_firewall_pp6.exam.xml Q_NET_FIREW_03]

Question 4: Incorrect

You are configuring a network firewall to allow SMTP outbound email traffic and POP3 inbound email traffic. Which of the following IP ports should you open on the firewall? (Select TWO).

- ☐ 143
- ➡ ☐ 25
- ➡ ☐ 110

- [x] ~~21~~
- [x] ~~443~~

Explanation

The Simple Mail Transfer Protocol (SMTP) uses IP port 25. The Post Office Protocol version 3 (POP3) uses IP port 110.

The File Transfer Protocol (FTP) uses IP Ports 20 and 21. The Internet Message Access Protocol (IMAP) uses IP port 143. IP port 443 is used by the Secure Sockets Layer (SSL) protocol.

References

TestOut PC Pro - 13.10 Firewalls
[e_firewall_pp6.exam.xml Q_NET_FIREW_04]

Question 5: Incorrect

To increase security on your company's internal network, the administrator has disabled as many ports as possible. Now, however, you can browse the internet, but you are unable to perform secure credit card transactions when making purchases from e-commerce websites.

Which port needs to be enabled to allow secure transactions?

- 443
- 21
- 80
- 69
- ~~23~~

Explanation

To perform secure transactions, SSL on port 443 needs to be enabled. HTTPS uses port 443 by default.

References

TestOut PC Pro - 13.10 Firewalls
[e_firewall_pp6.exam.xml Q_NET_FIREW_05]

Question 6: Incorrect

Which of the following is the BEST device to deploy to protect your private network from a public, untrusted network?

- ~~Router~~
- Gateway
- Firewall
- Hub

A firewall is the best device to deploy to protect your private network from a public, untrusted network. Firewalls are used to control traffic entering and leaving your trusted network environment. Firewalls can manage traffic based on source or destination IP address, port number, service protocol, application or service type, user account, and even traffic content.

Routers offer some packet-based access control, but not as extensively as a firewall. Hubs and gateways are not sufficient for managing the interface between a trusted network and an untrusted network.

References

TestOut PC Pro - 13.10 Firewalls
[e_firewall_pp6.exam.xml Q_NET_FIREW_06]

Question 7: Incorrect

Which of the following is a firewall function?

- Encrypting
- Protocol converting
- ~~Packet rearranging~~
- FTP hosting
- Packet filtering

Explanation

Firewalls often filter packets by checking each packet against a set of administrator-defined criteria. If the packet is not accepted, it is simply dropped.

References

TestOut PC Pro - 13.10 Firewalls
[e_firewall_pp6.exam.xml Q_NET_FIREW_07]

Question 8: Incorrect

In which of the following situations should you install a firewall?

- You want internet users to see a single IP address when accessing your company network.
- ~~You want to improve internet performance by saving popular websites locally.~~
- You want to implement a password system for internet users who access your private website.
- You want to restrict internet users from accessing private data on your network.

Explanation

Firewalls limit traffic by blocking connections that are initiated from an untrusted network, such as the internet, unless the traffic matches rules you configure in the firewall's access control list (ACL).

TestOut PC Pro - 13.10 Firewalls
[e_firewall_pp6.exam.xml Q_NET_FIREW_08]

Question 9: Correct

For some time now, you have been using an application on your Windows 10 computer at home and while in the office. This application communicates with the internet. Today, your team lead decided to have a special team meeting at a local hotel. During this meeting, you obtained access to the internet using the hotel's network, but when you tried to run your application, it could not communicate with the internet.

Which of the following Control Panel settings is MOST likely causing this behavior?

- Firewall settings
- Security settings
- Programs settings
- Privacy settings

Explanation

Microsoft's Windows Defender Firewall lets you configure which applications have access in and out of your computer by means of the internet. This helps you to protect your computer, your data, and even your identity, and the program runs in the background. Since the application had access at home (a private network) and at the office (a domain network), but not in the hotel (a guest or public network), the most likely scenario is that this application is being blocked by the firewall's Guest and Public Networks settings.

The Privacy settings control the level of access cookies have to your machine.

Security settings is where you maintain the settings for each of your four internet zones. The zones can have their security set from medium to high. Security Settings is where you can enable or disable Protected Mode. Since the only change in your program access was moving to the hotel, it is not likely that Protected Mode is blocking access.

Programs settings let you define your default web browser and allow or block add-ons or plug-ins used to accelerate multimedia performance, including Active X features.

References

TestOut PC Pro - 13.10 Firewalls
[e_firewall_pp6.exam.xml Q_NET_FIREW_09]

Question 10: Incorrect

A company has chosen a UTM instead of an IDS or IPS appliance to protect their network.

Which of the following UTM security features is not available with an IDS or IPS?

- Email and antispam filtering
- Anomaly logs and alerts

- ◯ Intrusion prevention

Explanation

A unified threat management (UTM) appliance offers the best network protection in a single device. It has all the features of an intrusion detection system (IDS) or intrusion prevention system (IPS). One of the features of a UTM that is not found in an IDS or IPS is email and antispam filtering.

UTMs, IDSs, and IPSs all provide intrusion detection functions. Both UTMs and IPSs provide intrusion prevention functions. UTMs, IDSs, and IPSs all log anomalies and send alerts.

References

TestOut PC Pro - 13.10 Firewalls
[e_firewall_pp6.exam.xml Q_NET_UTM_01]

Question 11: Correct

Employees complain to the company IT division that they are spending considerable time and effort discarding unwanted junk email.

Which of the following should be implemented?

- ➡ ◉ Email filtering
- ◯ Antivirus
- ◯ Multifactor authentication
- ◯ Firewall

Explanation

While email filtering can be implemented by each user, it can also be enabled in incoming mail services to reduce spam and other unwanted email by blocking email based on the sender address or by content.

Antivirus software can protect computers from viruses found in emails, but is not used to filter email content. Firewalls are placed between the company network and the internet to filter network traffic at the IP level. Normally, they do not filter email based on content. Multifactor authentication combines a strong password with at least one other form of authentication before granting access. It does not filter email.

References

TestOut PC Pro - 13.10 Firewalls
[e_firewall_pp6.exam.xml Q_NET_UTM_02]

Question 12: Incorrect

You are configuring a firewall to allow access to a server hosted in the demilitarized zone of your network. You open IP ports 80, 25, 110, and 143. Assuming that no other ports on the firewall need to be configured to provide access, which applications are most likely to be hosted on the server?

- ◯ Web server, DNS server, or email server
- ◯ Web server, DNS server, or DHCP server

Web server and email server

~~Email server, Newsgroup server, or DNS server~~

Explanation

TCP/IP port 80 is associated with accessing webpages from a web server using the Hypertext Transfer Protocol (HTTP). Email can be accessed using a number of protocols, including the Simple Mail Transfer Protocol (SMTP), the Post Office Protocol version 3 (POP3), and the Internet Message Access Protocol version 4 (IMAP4). SMTP uses TCP/IP port 25, while POP3 uses TCP/IP port 110, and IMAP4 uses TCP/IP port 143.

Domain Name Service (DNS) traffic uses TCP/IP port 53. Newsgroup servers are accessed using the Network News Transfer (NNTP) protocol on TCP/IP port 119. Dynamic Host Configuration Protocol (DHCP) traffic uses the BOOTP protocol on TCP/IP ports 67 and 68.

References

TestOut PC Pro - 13.10 Firewalls
[e_firewall_pp6.exam.xml Q_NET_UTM_03]

Question 13: Incorrect

To access your company's internal network from home, you use Secure Shell (SSH). The administrator has recently implemented a new firewall at the network perimeter and disabled as many ports as possible.

Which port needs to remain open so you can still work from home?

23

~~443~~

21

80

22

Explanation

SSH uses port 22. This port would need to remain open for you to access your company's internal network from home.

SSL uses port 443, FTP uses port 21, and HTTP uses port 80. Telnet uses port 23.

References

TestOut PC Pro - 13.10 Firewalls
[e_firewall_pp6.exam.xml Q_NET_UTM_04]

Question 14: Incorrect

A local dentist has contracted with you to implement a network in her new office. Because of security concerns related to patient privacy laws, she has asked that the new network meet the following criteria:

- No one from the internet should be able to access her internal network.
- Email messages should be scanned for spam, phishing attacks, and malware

• Employees access to non-work-related websites, especially sites that contain inappropriate content, should be blocked.
• A system should be put in place to detect and prevent external attacks on her network.

Which of the following would BEST meet your client's criteria?

- ~~Implement an email security appliance.~~
- Implement an all-in-one security appliance.
- Implement a content filter.
- Implement an intrusion prevention system (IPS).
- Implement a firewall.

Explanation

You should implement an all-in-one security appliance. The network criteria specified by your client requires several different network devices to be implemented, including a firewall, an email scanner, a content filter, and an intrusion prevention system.

While you could purchase each device separately, the cost of doing so would probably be quite high. Because you are working with a small business, an all-in-one security appliance that includes all of these functions in a single device would be more cost-effective and easier for you to manage.

References

TestOut PC Pro - 13.10 Firewalls
[e_firewall_pp6.exam.xml Q_NET_UTM_05]