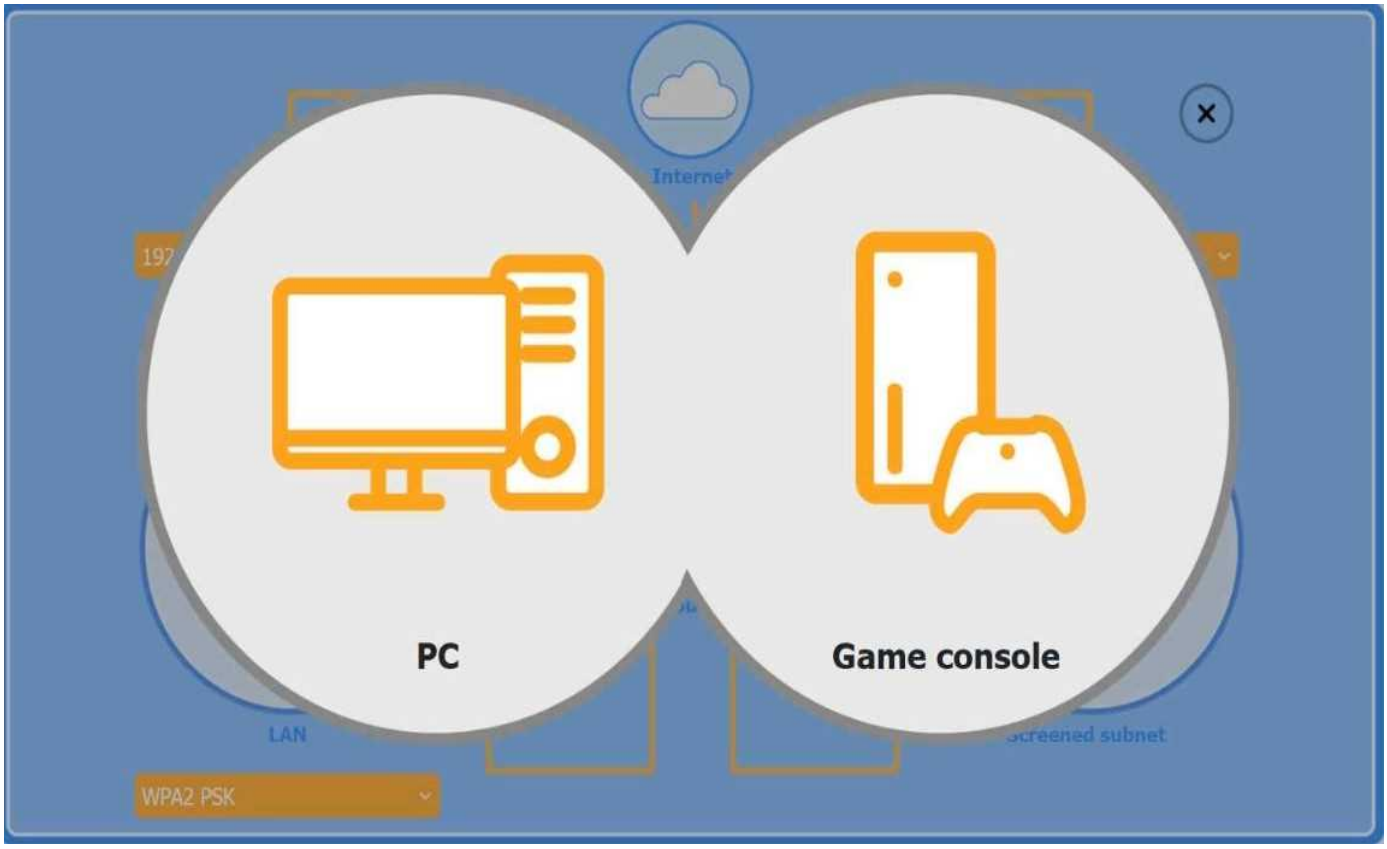
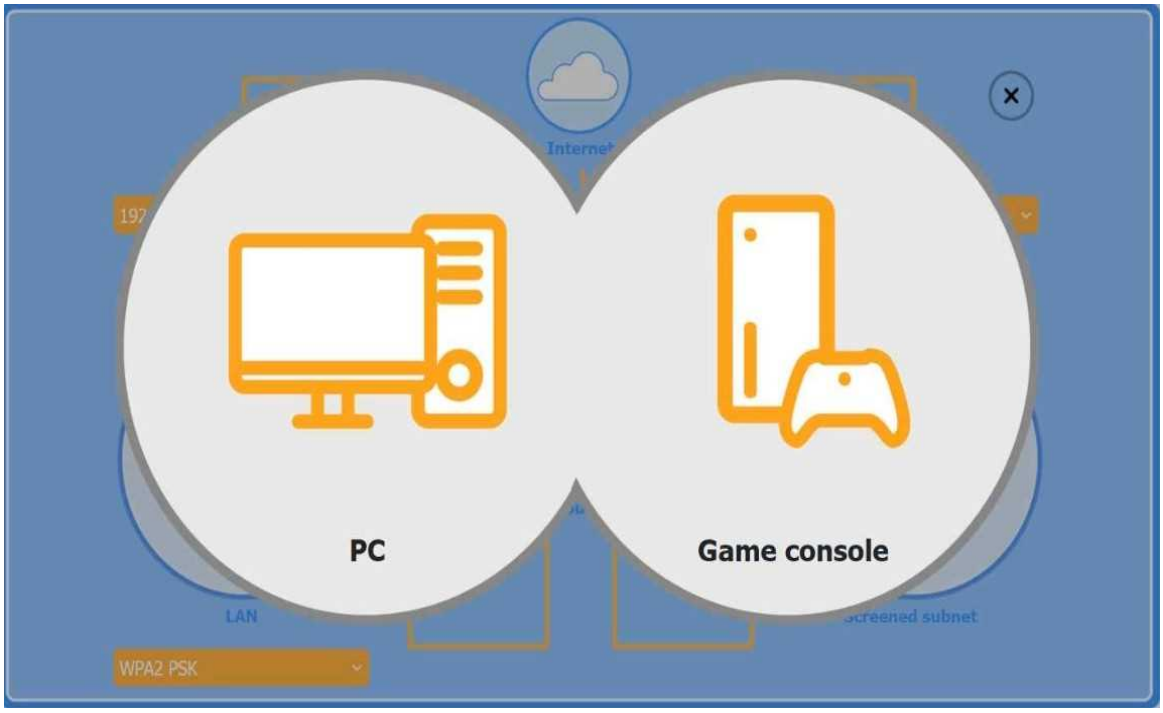
Product Questions: 75
Version: 4.0

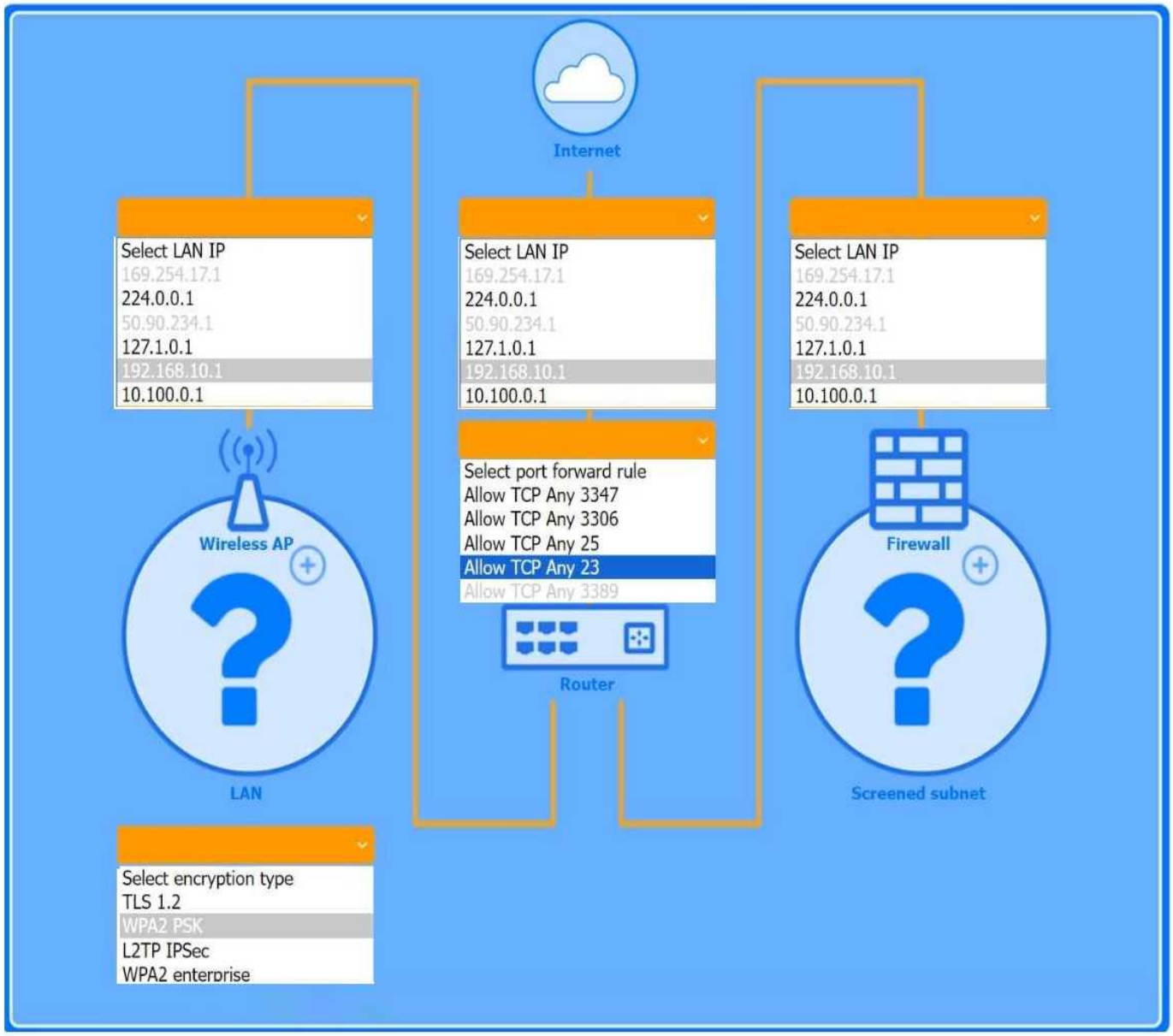
Question: 1

SIMULATION
You are configuring a home network for a customer. The customer has requested the ability to access a Windows PC remotely, and needs all chat and optional functions to work in their game console.
INSTRUCTIONS
Use the drop-down menus to complete the network configuration for the customer. Each option may only be used once, and not all options will be used.
Then, click the + sign to place each device in its appropriate location.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.
Wireless AP LAN



Firewall Screened Subnet


Internet
PC
Game console
LAN
Screened subnet
WPA2 PSK



Answer: See explanation below.

Explanation:

The completed configuration:

1. Wireless AP (LAN side)
   1. LAN IP: 192.168.10.1
   2. Encryption: WPA2 PSK
2. Router (port-forward rule)
   1. Allow TCP Any 3389

This forwards inbound RDP traffic (TCP/3389) from the Internet to the Windows PC, enabling Remote Desktop access.

3. Firewall (screened subnet side)
   1. LAN IP: 10.100.0.1
4. Device placement

1. PC: place behind the router (where the port-forward rule points).
2. Game console: place on the Wireless AP (so it can use chat and extra services over WPA2 PSK).
3. Firewall: place in front of the screened subnet (with its 10.100.0.1 IP facing that subnet).

Question: 2

A technician needs to provide remote support for a legacy Linux-based operating system from their Windows laptop. The solution needs to allow the technician to see what the user is doing and provide the ability to interact with the user's session. Which of the following remote access technologies would support the use case?

A. VPN
B. VNC
C. SSH
D. RDP

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The correct answer is VNC (Virtual Network Computing). VNC is a graphical desktop-sharing system that uses the Remote Frame Buffer protocol (RFB) to remotely control another computer. It is platform-independent and widely supported on Linux, which makes it ideal for providing interactive remote support for a Linux-based operating system. It allows the technician not only to view the remote desktop session but also to control it, fulfilling the need to see and interact with the user's session.
A . VPN (Virtual Private Network) creates a secure tunnel to a network but does not provide desktop sharing or session control by itself.
C . SSH (Secure Shell) provides secure command-line access to Unix/Linux systems but does not offer graphical desktop interaction, which is a requirement in this case.
D . RDP (Remote Desktop Protocol) is primarily a Microsoft protocol, and although it can be made to work on Linux, it is not natively supported on legacy Linux systems, and thus less suitable than VNC in this scenario.
✅ CompTIA A+ 220-1102 Core 2 Objective Reference:
Objective 1.8 – Given a scenario, use features and tools of the operating system.
Under this objective, candidates are expected to be familiar with remote access technologies, including RDP, SSH, and VNC, and understand their appropriate uses and limitations on different platforms such as Windows and Linux.

Question: 3

A technician is attempting to join a workstation to a domain but is receiving an error message stating the domain cannot be found. However, the technician is able to ping the server and access the internet. Given the following information:
IP Address – 192.168.1.210
Subnet Mask – 255.255.255.0
Gateway – 192.168.1.1
DNS1 – 8.8.8.8
DNS2 – 1.1.1.1
Server – 192.168.1.10
Which of the following should the technician do to fix the issue?

A. Change the DNS settings.
B. Assign a static IP address.
C. Configure a subnet mask.
D. Update the default gateway.

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The issue described—"domain cannot be found" despite the ability to ping the server and access the internet—indicates a DNS resolution problem, not a network connectivity issue. The workstation is currently using public DNS servers (8.8.8.8 and 1.1.1.1) which cannot resolve internal domain names, such as the ones used in Active Directory environments. To resolve this, the technician needs to change the DNS settings to point to the internal DNS server, which in most domain setups is the domain controller itself (likely 192.168.1.10 in this case).
Here's the breakdown of the incorrect options:
B . Assign a static IP address: The IP is already assigned and functioning; the device can ping and reach the network and internet.
C . Configure a subnet mask: The subnet mask is appropriate for the network range (Class C /24).
D . Update the default gateway: The gateway is valid and allows internet access; this is not the issue.
✅ CompTIA A+ 220-1102 Core 2 Objective Reference:
Objective 1.8 – Given a scenario, use features and tools of the operating system.
Under this objective, candidates must know how to troubleshoot OS-based network configurations, including proper DNS settings in domain environments.

Question: 4

A network technician notices that most of the company's network switches are now end-of-life and need to be upgraded. Which of the following should the technician do first?

A Implement the change
B. Approve the change.
C. Propose the change.
D. Schedule the change.

Answer: C

Explanation:

In a structured change-management process, the very first step is to propose (or formally request) the change via a Request for Change (RFC). This ensures stakeholders review the need, assess risks, and determine the priority before any approvals, scheduling, or implementation occur.

Question: 5

MFA for a custom web application on a user's smartphone is no longer working. The last time the user remembered it working was before taking a vacation to another country. Which of the following should the technician do first?

A. Verify the date and time settings.
B. Apply mobile OS patches.
C. Uninstall and reinstall the application.
D. Escalate to the website developer.

Answer: A

Explanation:

Time-based one-time password (TOTP) MFA apps rely on accurate clock synchronization. Traveling can desynchronize the device’s clock, causing generated codes to be invalid. Ensuring the smartphone’s date/time (and time zone) are correct will typically restore MFA functionality immediately.

Question: 6

Which of the following is found in an MSDS sheet for a battery backup?

A. Installation instructions
B. Emergency procedures
C. Configuration steps
D. Voltage specifications

Answer: B

Explanation:

A Material Safety Data Sheet (MSDS) provides critical safety and handling information for hazardous

materials - in this case, the battery's chemicals. It includes emergency procedures (first-aid measures, fire-fighting steps, spill containment), ensuring responders know how to act safely in an incident.

Question: 7

The screen of a previously working computer repeatedly displays an OS Not Found error message when the computer is started. Only a USB drive, a keyboard, and a mouse are plugged into the computer. Which of the following should a technician do first?

A. Run data recovery tools on the disk.
B. Partition the disk using the GPT format.
C. Check boot options.
D. Switch from UEFI to BIOS.

Answer: C

Explanation:

An "OS Not Found" error most commonly indicates the system isn't booting from the correct device. Verifying and correcting the boot order (ensuring the internal hard drive is prioritized over USB or other entries) is the quickest first step before making any changes to the disk or firmware settings.

Question: 8

A security administrator teaches all of an organization's staff members to use BitLocker To Go. Which of the following best describes the reason for this training?

A. To ensure that all removable media is password protected in case of loss or theft
B. To enable Secure Boot and a BIOS-level password to prevent configuration changes
C. To enforce VPN connectivity to be encrypted by hardware modules
D. To configure all laptops to use the TPM as an encryption factor for hard drives

Answer: A

Explanation:

BitLocker To Go is specifically designed to encrypt removable drives (USB flash drives, external HDDs). Training staff on its use guarantees that any data stored on such media requires a password (or recovery key) to access, protecting sensitive information if the device is lost or stolen.

Question: 9

Which of the following is used to detect and record access to restricted areas?

A. Bollards
B. Video surveillance
C. Badge readers
D. Fence

Answer: C

Explanation:

Badge readers authenticate and log each entry attempt - recording who accessed (or tried to access) a secured area and when. This audit trail is essential for monitoring and reviewing access to restricted zones.

Question: 10

An administrator received an email stating that the OS they are currently supporting will no longer be issued security updates and patches. Which of the following is most likely the reason the administrator received this message?

A. Support from the computer's manufacturer is expiring.
B. The OS will be considered end of life.
C. The built-in security software is being removed from the next OS version.
D. A new version of the OS will be released soon.

Answer: B

Explanation:

When an operating system reaches end of life (EOL), the vendor ceases issuing security updates and patches. Administrators are notified so they can plan upgrades or migrations before support ends.

Question: 11

Which of the following is the best way to distribute custom images to 800 devices that include four device vendor classes with two types of user groups?

A. Use xcopy to clone the hard drives from one to another.
B. Use robocopy to move the files to each device.
C. Use a local image deployment tool for each device.
D. Use a network-based remote installation tool.

Answer: D

Explanation:

A network-based remote installation tool (such as Windows Deployment Services, MDT, or a similar solution) scales efficiently across hundreds of devices with varying hardware and user configurations. It allows you to segment deployments by vendor classes and user groups, automate imaging processes, and manage version control centrally - far more effectively than one-to-one cloning or file-copy methods.

Question: 12

Which of the following types of social engineering attacks sends an unsolicited text message to a user's mobile device?

A. Impersonation
B. Vishing
C. Spear phishing
D. Smishing

Answer: D

Explanation:

Smishing is the act of sending fraudulent messages via SMS or other texting platforms to trick users into revealing sensitive information or clicking malicious links. This distinguishes it from phishing over email (spear phishing), voice calls (vishing), or in-person deception (impersonation).

Question: 13

A user reports some single sign-on errors to a help desk technician. Currently, the user is able to sign in to the company's application portal but cannot access a specific SaaS-based tool. Which of the following would the technician most likely suggest as a next step?

A. Reenroll the user's mobile device to be used as an MFA token.
B. Use a private browsing window to avoid local session conflicts.
C. Bypass single sign-on by directly authenticating to the application.
D. Reset the device being used to factory defaults.

Answer: B

Explanation: