CompTIA

Exam Questions 220-1202

CompTIA A+ Certification Exam: Core 2

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
Recently, the number of users sharing smartphone passcodes has increased. The management team wants a technician to deploy a more secure screen lock method. Which of the following technologies should the technician use?

A. Pattern lock
B. Facial recognition
C. Device encryption
D. Multifactor authentication

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Facial recognition is a biometric authentication method that ties access to a unique physical feature of the user. Unlike passcodes or pattern locks—which can be easily shared—facial recognition provides a more secure and non-transferable form of access. It also enhances user convenience and is widely supported by modern smartphones.
* A. Pattern locks can still be shared and are less secure.
* C. Device encryption protects data but does not prevent screen access if a passcode is shared.
* D. Multifactor authentication typically applies to app or account access, not basic phone unlocking.
Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast common security measures and authentication technologies.
Study Guide Section: Biometric screen lock technologies (e.g., facial recognition, fingerprint)
===========================

NEW QUESTION 2
A technician uses AI to draft a proposal about the benefits of new software. When reading the draft, the technician notices that the draft contains factually incorrect information. Which of the following best describes this scenario?

A. Data privacy
B. Hallucinations
C. Appropriate use
D. Plagiarism

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
In the context of artificial intelligence, "hallucinations" refer to instances where an AI system generates information that is plausible-sounding but factually incorrect or entirely fabricated. This is a known limitation of large language models, including generative AI tools.
* A. Data privacy refers to the protection of personal or sensitive data, not content accuracy.
* C. Appropriate use relates to ethical and policy-based concerns, not factual correctness.
* D. Plagiarism involves presenting someone else's work as your own — this situation is about accuracy, not ownership.
Reference:
CompTIA A+ 220-1102 Objective 4.4: Identify basic concepts of scripting and automation. Study Guide Section: AI tools and responsible usage — hallucinations and fact-checking outputs
===========================

NEW QUESTION 3
A company would like to deploy baseline images to new computers as they are started up on the network. Which of the following boot processes should the company use for this task?

A. ISO
B. Secure
C. USB
D. PXE

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
PXE (Preboot Execution Environment) allows workstations to boot over the network and download an OS image from a server. It is ideal for automating mass deployments using
baseline images across many machines without the need for physical media.
* A. An ISO is a disk image file but requires mounting or physical media.
* B. Secure Boot is a security feature, not a method of deploying OS images.
* C. USB requires manual installation and is not suitable for automated deployment at scale. Reference:
CompTIA A+ 220-1102 Objective 1.4: Given a scenario, use appropriate Microsoft operating system installation methods.
Study Guide Section: Remote installation methods — PXE boot deployment
===========================

NEW QUESTION 4
Which of the following methods involves requesting a user's approval via a push notification to verify the user's identity?

A. Call
B. Authenticator
C. Hardware token
D. SMS

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Authenticator apps (e.g., Microsoft Authenticator, Google Authenticator, Duo) often support push notifications. When the user logs in, the app sends a push to their mobile device, prompting the user to approve or deny the authentication request — a common and user- friendly form of multi-factor authentication (MFA).
* A. Phone call verification is a separate method involving voice-based confirmation.
* C. Hardware tokens generate one-time codes but do not send push notifications.
* D. SMS sends a text message with a code — again, no push mechanism. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast multi-factor authentication methods.
Study Guide Section: Authentication apps and push notification verification
==========================

NEW QUESTION 5
Which of the following describes a vulnerability that has been exploited before a patch or remediation is available?

A. Spoofing
B. Brute-force
C. DoS
D. Zero-day

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
A Zero-day vulnerability refers to a security flaw in software or hardware that is unknown to the vendor or has not yet been patched. If this vulnerability is exploited before the vendor has issued a fix or patch, it becomes a Zero-day exploit. These attacks are highly dangerous because they take advantage of the absence of defenses due to the lack of awareness or mitigation options.
* A. Spoofing is a form of impersonation, not necessarily tied to unpatched vulnerabilities.
* B. Brute-force attacks rely on repeatedly guessing credentials and are not related to software flaws.
* C. DoS (Denial of Service) attacks are meant to overwhelm systems and don't necessarily exploit unknown vulnerabilities.
Reference:
CompTIA A+ 220-1102 Objective 2.3: Compare and contrast common social engineering, threats, and vulnerabilities.
Study Guide Section: Threat types — Zero-day attacks, definitions, and implications

NEW QUESTION 6
A technician is using a credential manager to safeguard a large number of credentials. Which of the following is important for using this application?

A. Restricted log-in times
B. Secure master password
C. TPM module
D. Windows lock screen

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Credential managers or password vaults (e.g., Windows Credential Manager, KeePass, or LastPass) store passwords securely. The integrity of such tools heavily depends on the strength of the master password protecting the vault. If compromised, all saved credentials could be exposed. Therefore, setting a secure master password is crucial.
* A. Login time restrictions are general user account settings, not specific to credential managers.
* C. TPM is used more commonly for full disk encryption, not specifically required for password managers.
* D. The lock screen protects general access but does not protect stored credentials alone. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast authentication technologies and secure credential storage.
Study Guide Section: Password management and protection best practices
==========================

NEW QUESTION 7
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:
Comprehensive and Detailed Explanation From Exact Extract:
BitLocker To Go is a Microsoft encryption feature specifically designed for removable drives such as USB flash drives and external hard drives. It allows users to protect the data on these devices by requiring a password to decrypt the contents, thereby preventing unauthorized access in the event the device is lost or stolen.
A is correct because BitLocker To Go is directly tied to password-protecting removable media.
B and C are unrelated to BitLocker To Go; Secure Boot and VPN encryption are entirely
different security layers.
D applies to BitLocker (not BitLocker To Go) and full disk encryption on internal drives using TPM.
Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast common security measures and tools.
Study Guide Section: Encryption technologies (BitLocker, BitLocker To Go)
==========================

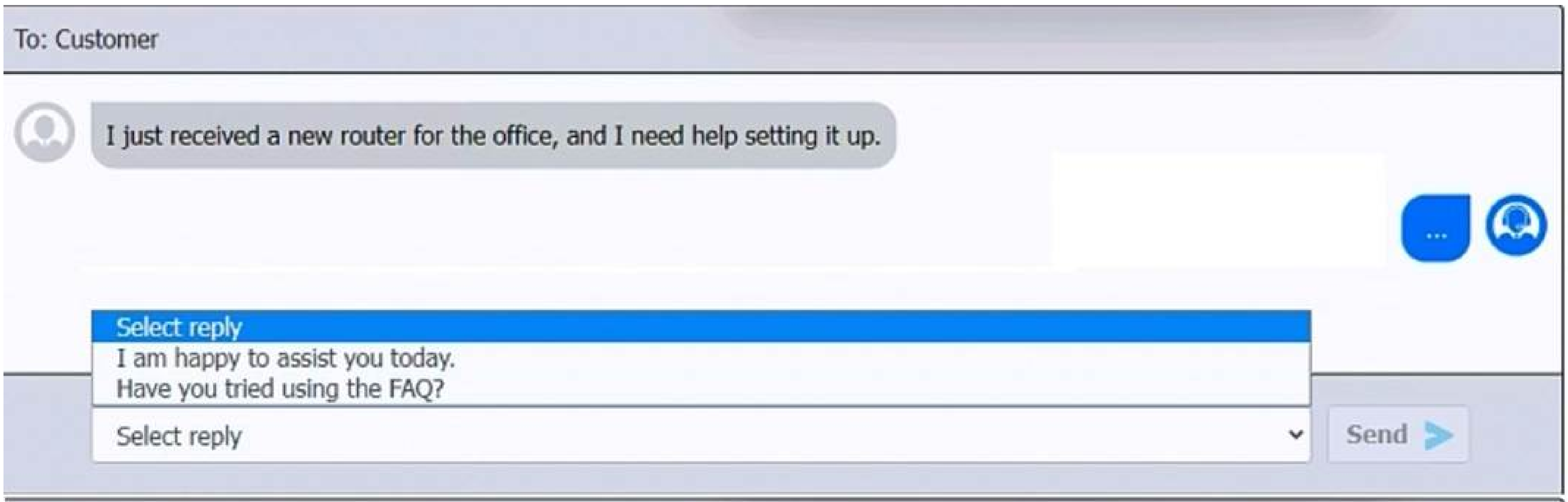
NEW QUESTION 8
A company recently transitioned to a cloud-based productivity suite and wants to secure the environment from external threat actors. Which of the following is the most effective method?

A. Multifactor authentication
B. Encryption
C. Backups
D. Strong passwords

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Multifactor authentication (MFA) is considered one of the most effective security measures for cloud environments. It requires users to verify their identity using two or more factors (e.g., password + phone app code), making it significantly harder for external attackers to gain access, even if the primary password is compromised.
* B. Encryption is important for data protection but doesn??t prevent unauthorized logins.
* C. Backups protect against data loss but don??t stop breaches.
* D. Strong passwords are helpful but can still be phished or cracked — MFA adds a critical
extra layer. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast authentication technologies. Study Guide Section: Cloud security best practices — MFA and access control

NEW QUESTION 9
SIMULATION
You have been contacted through the help desk chat application. A user is setting up a replacement SOHO router. Assist the user with setting up the router.
INSTRUCTIONS
Select the most appropriate statement for each response. Click the send button after each response to continue the chat.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

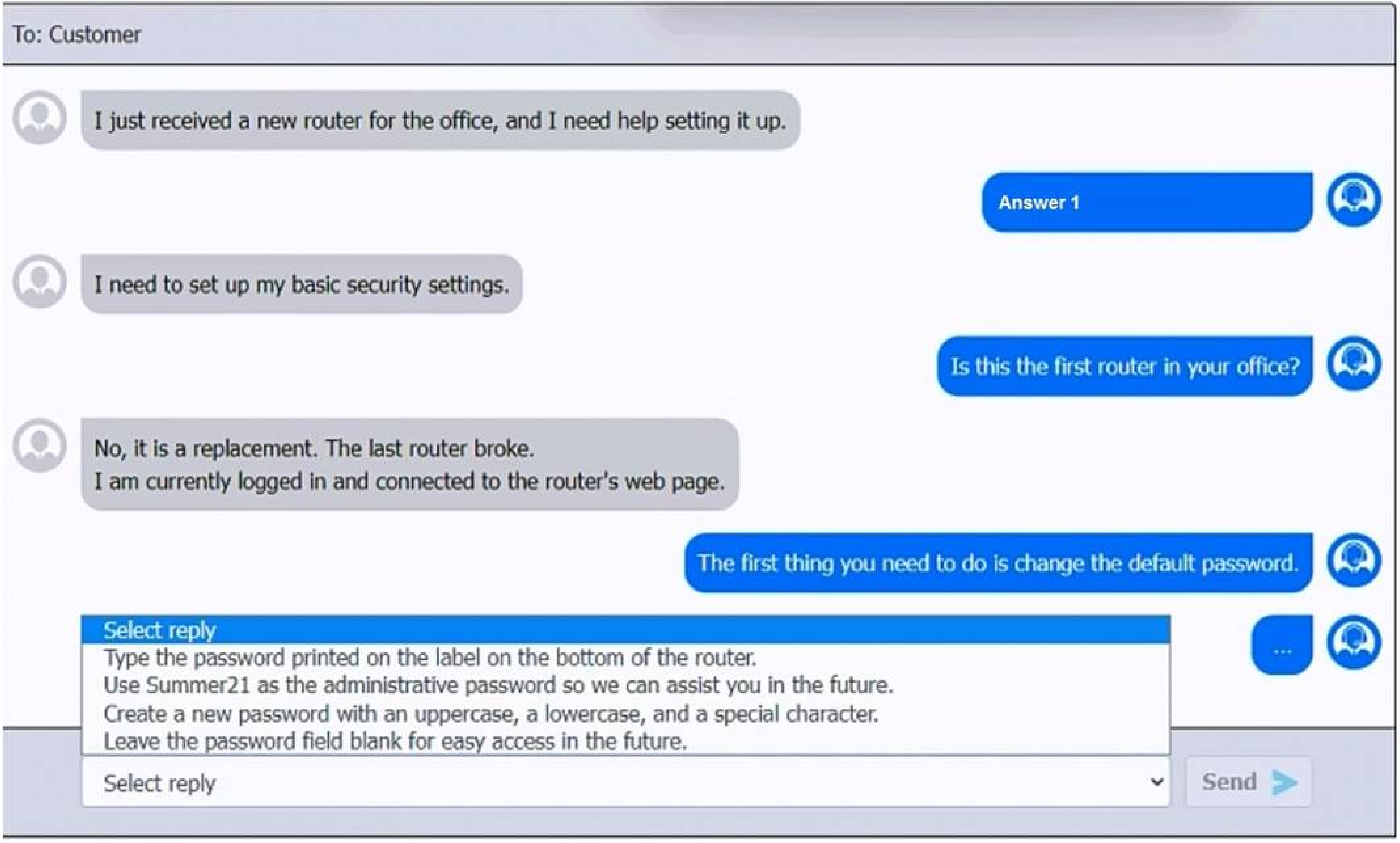


To: Customer

I just received a new router for the office, and I need help setting it up.

Select reply
I am happy to assist you today.
Have you tried using the FAQ?

Select reply



To: Customer

I just received a new router for the office, and I need help setting it up.

Answer 1

I need to set up my basic security settings.

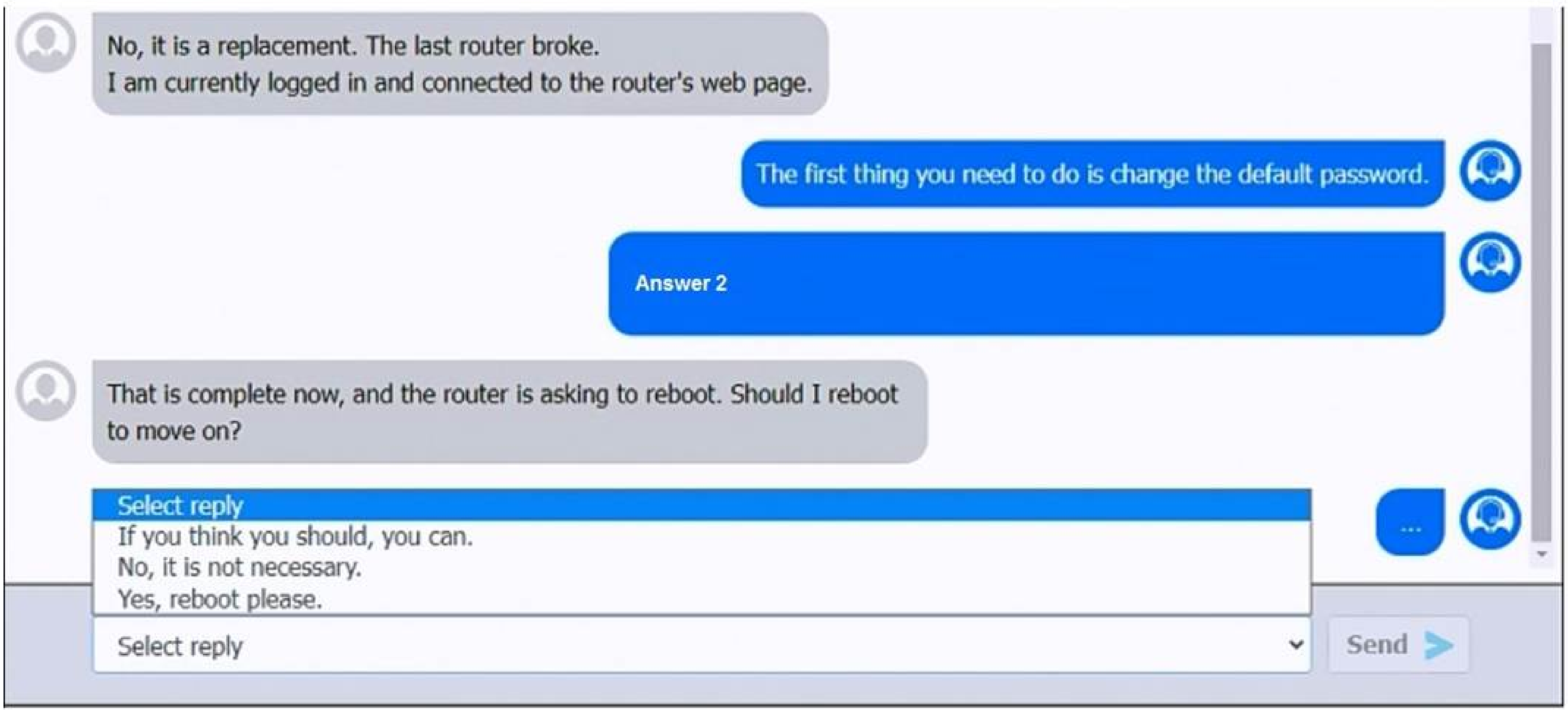
Is this the first router in your office?

No, it is a replacement. The last router broke.
I am currently logged in and connected to the router's web page.

The first thing you need to do is change the default password.

Select reply
Type the password printed on the label on the bottom of the router.
Use Summer21 as the administrative password so we can assist you in the future.
Create a new password with an uppercase, a lowercase, and a special character.
Leave the password field blank for easy access in the future.

Select reply



No, it is a replacement. The last router broke.
I am currently logged in and connected to the router's web page.

The first thing you need to do is change the default password.

Answer 2

That is complete now, and the router is asking to reboot. Should I reboot to move on?

Select reply
If you think you should, you can.
No, it is not necessary.
Yes, reboot please.

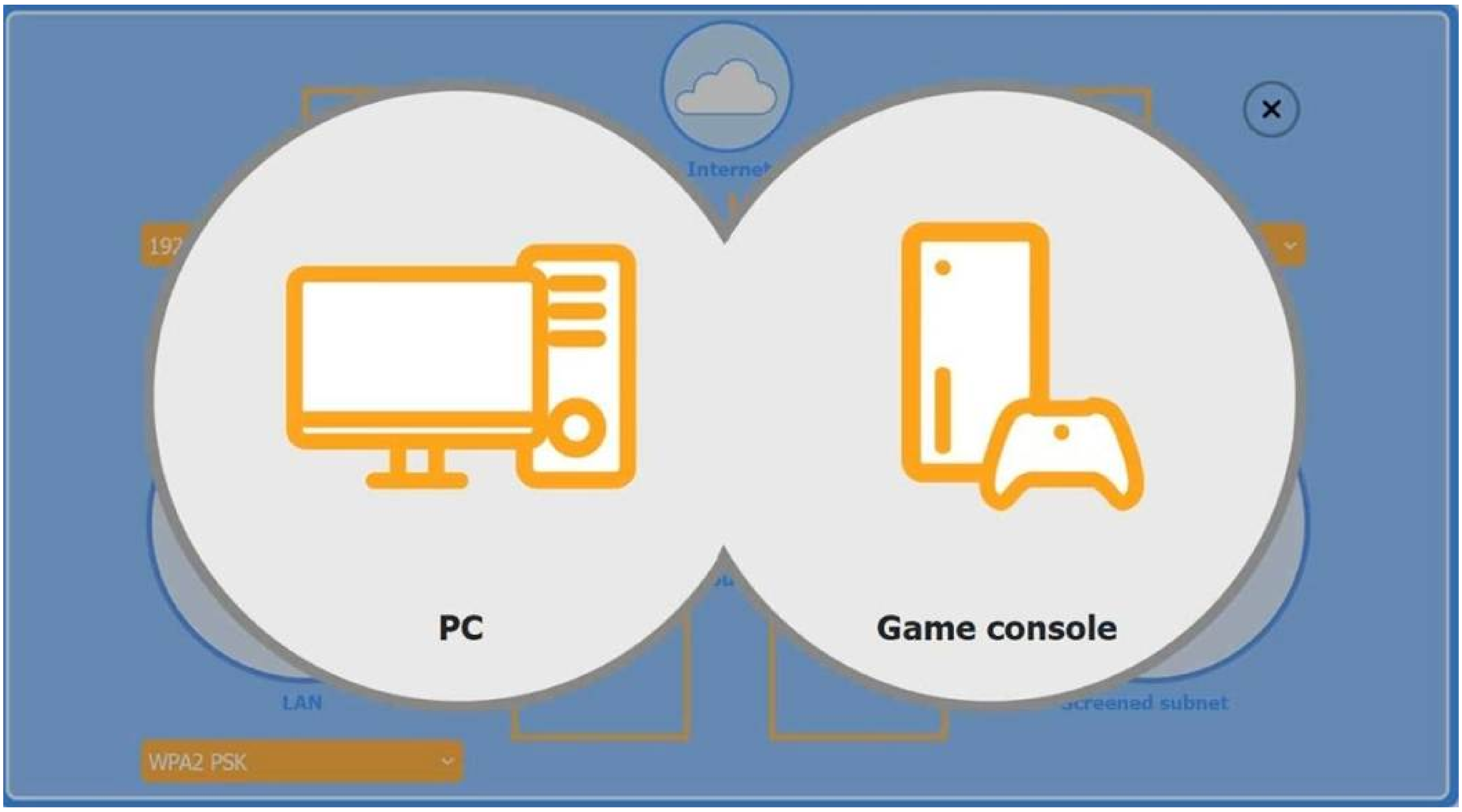
Select reply

A. Mastered
B. Not Mastered

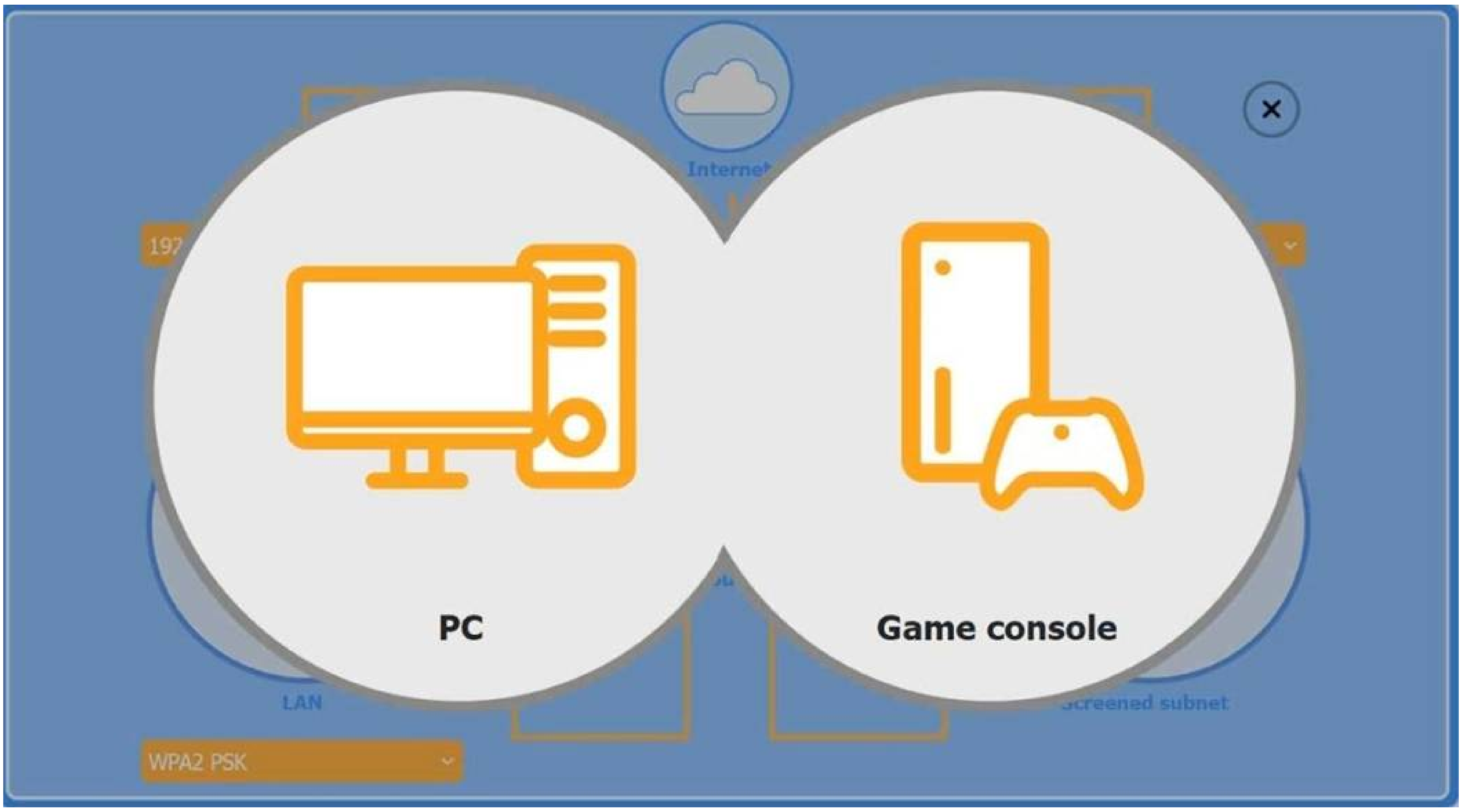
Answer: A

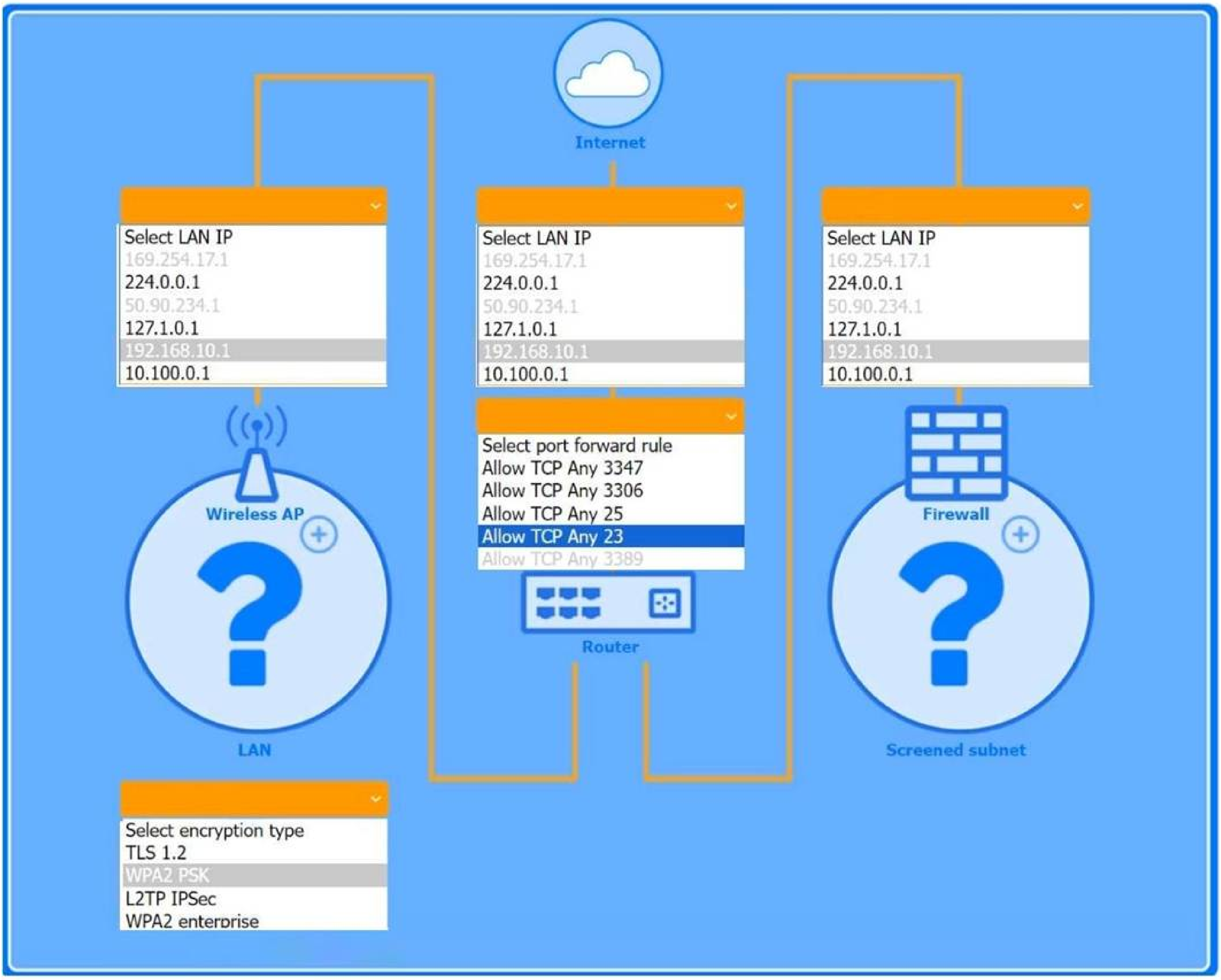
Explanation:
First Chat Response:When the user mentions setting up a new router, the best initial response to maintain a helpful and professional tone is:
>Select reply:"I am happy to assist you today."
Second Chat Response:When the user states that they need to set up basic security settings:
>Select reply:"Is this the first router in your office?"
Third Chat Response:After learning it's a replacement router and the user is logged into the router's web page:
>Select reply:"The first thing you need to do is change the default password."
Fourth Chat Response:For the response about password settings:
>Select reply:"Create a new password with an uppercase, a lowercase, and a special character."
Fifth Chat Response:When the router prompts to reboot:
>Select reply:"Yes, reboot please."
Study Guide Reference: The CompTIA A+ Core 2 guide highlights the importance of changing default credentials and using strong password policies, particularly in SOHO environments where routers are often targeted.

NEW QUESTION 10
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





A. Mastered
B. Not Mastered

Answer: A

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).
? The Windows PC is placed in the screened subnet (behind the firewall) for enhanced security. Remote access to this PC requires port forwarding of TCP port 3389 (RDP), which is correctly configured through the router.
? The Game Console is placed on the Wireless AP LAN, using WPA2 PSK for a secure wireless connection. Game consoles typically use peer-to-peer chat and online services that require open access without firewall restrictions, which is why the console is not placed behind the firewall.
CompTIA A+ 220-1102 Reference Points:
? Objective 3.4: Given a scenario, implement best practices associated with data and device security.
? Objective 2.4: Given a scenario, use appropriate tools to support and configure network settings.
? Study Guide Reference: CompTIA A+ Core 2 guides recommend using screened subnets (a type of DMZ) for systems needing controlled external access, such as remote desktops, while placing gaming and media devices on less restricted networks for full functionality.

NEW QUESTION 10
A technician is troubleshooting an issue in which a service runs momentarily and stops at certain points in the process. The technician needs to determine the root cause of this issue. Which of the following tools should the technician use?

A. Event Viewer
B. Task Manager
C. Internet Options
D. Process Explorer

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Event Viewer is the best tool to analyze the root cause of service failures in Windows. It provides detailed logs from system processes, including errors, warnings, and crash reports related to services and applications. When a service starts and stops unexpectedly, Event Viewer will often record the cause, such as dependency failures or access violations.
* B. Task Manager shows active processes but doesn't retain logs or causes of failure.
* C. Internet Options is used for configuring browser settings, not troubleshooting services.
* D. Process Explorer is powerful but more suited for live monitoring and detailed process trees, not post-failure log analysis.
Reference:
CompTIA A+ 220-1102 Objective 3.1: Given a scenario, troubleshoot common Windows OS problems.
Study Guide Section: Log file analysis using Event Viewer
==========================

NEW QUESTION 12
An end user's laptop is having network drive connectivity issues in the office. The end user submits a help desk ticket, and a support technician is able to establish a remote connection and fix the issue. The following day, however, the network drive is disconnected again. Which of the following should the technician do next?

A. Connect remotely to the user's computer to see whether the network drive is still connected.
B. Send documentation about how to fix the issue in case it reoccurs.
C. Escalate the ticket to the next level.
D. Keep the ticket open until next day, then close the ticket.

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Since the issue has recurred after a temporary fix, it is likely a deeper or persistent configuration or server issue. Escalating the ticket to the next tier of support (e.g., network or system administrator) ensures further investigation and permanent resolution. Escalation is part of the standard support protocol when issues reoccur despite initial troubleshooting.
* A. Rechecking remotely may confirm the issue, but doesn??t resolve it long term.
* B. Providing documentation helps the user but doesn??t solve the root cause.
* D. Keeping the ticket open is passive and doesn??t address the recurring issue. Reference:
CompTIA A+ 220-1102 Objective 4.1: Given a scenario, implement best practices associated with documentation and support systems information.
Study Guide Section: Escalation procedures and ticket management
==========================

NEW QUESTION 17
Which of the following filesystem types does the Linux OS use?

A. exFAT
B. APFS
C. ext4
D. NTFS

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The ext4 (Fourth Extended Filesystem) is the most widely used default filesystem in modern Linux distributions. It is designed for high performance, scalability, and reliability, and is supported by all mainstream Linux kernels.
* A. exFAT is used for cross-platform external drives, not native Linux systems.
* B. APFS is Apple's proprietary filesystem for macOS and iOS.
* D. NTFS is the default filesystem for Windows, not Linux. Reference:
CompTIA A+ 220-1102 Objective 1.9: Identify common features and tools of the Linux client/desktop OS.
Study Guide Section: Filesystem types in Linux — ext3, ext4, and their characteristics

NEW QUESTION 19
An employee is using a photo editing program. Certain features are disabled and require a log-in, which the employee does not have. Which of the following is a way to resolve this issue?

A. License assignment
B. VPN connection
C. Application repair
D. Program reinstallation

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Many modern commercial software applications (including photo editors like Adobe Photoshop) offer tiered features based on user subscriptions or license levels. If certain features are locked and prompt for a login, the issue is likely due to a missing or unassigned software license. Assigning the correct license through a centralized license management system (such as Adobe Admin Console or Microsoft 365 portal) will enable those features.
* B. VPN connection does not affect local software licensing.
* C. Repairing the application does not resolve license entitlement.
* D. Reinstalling the software won??t help unless the license is assigned. Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common software and application issues.
Study Guide Section: Troubleshooting licensing and access control for applications
==========================

NEW QUESTION 24
Which of the following provides information to employees, such as permitted activities when using the organization's resources?

A. AUP
B. MNDA
C. DRM
D. EULA

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
An Acceptable Use Policy (AUP) outlines the rules and guidelines for employees or users regarding the appropriate use of company systems, resources, and internet access. It defines permitted and prohibited activities, helping to mitigate security risks and establish clear behavioral expectations.
* B. MNDA (Mutual Non-Disclosure Agreement) deals with confidentiality, not usage guidelines.
* C. DRM (Digital Rights Management) controls access to copyrighted content.
* D. EULA (End User License Agreement) pertains to software licensing, not internal policies.
Reference:
CompTIA A+ 220-1102 Objective 4.3: Explain common safety and environmental impacts and procedures.
Study Guide Section: Organizational policies — AUP, security best practices
==========================

NEW QUESTION 27
A user is working from home and is unable to access work files on a company laptop. Which of the following should a technician configure to fix the network access issue?

A. Wide-area network
B. Wireless network
C. Proxy network settings
D. Virtual private network

Answer: D

Explanation:
A VPN creates a secure tunnel from the user??s home network into the corporate network, providing the necessary routing and access controls for the laptop to reach internal file servers. Without a VPN, the device remains outside the corporate LAN and cannot directly reach protected resources.
A VPN creates a secure tunnel from the user??s home network into the corporate network, providing the necessary routing and access controls for the laptop to reach internal file servers. Without a VPN, the device remains outside the corporate LAN and cannot directly reach protected resources.

NEW QUESTION 31
A computer technician is implementing a solution to support a new internet browsing policy for a customer's business. The policy prohibits users from accessing unauthorized websites based on categorization. Which of the following should the technician configure on the SOHO router?

A. Secure management access
B. Group Policy Editor
C. Content filtering

D. Firewall

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Content filtering allows administrators to block or allow access to websites based on categories (e.g., social media, adult content, streaming). On a SOHO (Small Office/Home Office) router, this is often built-in or available via DNS-level filtering, and is the most appropriate method for enforcing browsing policies without needing to touch each individual device.
* A. Secure management access protects router admin interfaces but doesn??t control user browsing.
* B. Group Policy Editor is a Windows tool, not used on routers.
* D. A firewall can block specific IPs or ports, but it doesn't categorize web content. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast security measures and tools. Study Guide Section: SOHO router security features — content filtering, parental controls

NEW QUESTION 35
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:
Comprehensive and Detailed Explanation From Exact Extract:
Operating systems periodically reach a status known as "end of life" (EOL), at which point the developer (e.g., Microsoft, Apple) ceases to provide security updates, patches, or technical support. When this happens, the OS becomes vulnerable and non-compliant with security best practices, which is why organizations typically receive advance notifications from vendors or support teams.
* A. Manufacturer support expiration only applies to hardware, not OS patching.
* C. Security software may be upgraded or removed, but that does not affect patching the OS itself.
* D. The release of a new version doesn??t automatically stop updates for the current version. Reference:
CompTIA A+ 220-1102 Objective 1.3: Given a scenario, use appropriate Microsoft operating system features and tools.
Study Guide Section: OS lifecycle management and vendor support phases (e.g., EOL)
==========================

NEW QUESTION 38
A user reports getting a BSOD (Blue Screen of Death) error on their computer at least twice a day. Which of the following should the technician use to determine the cause?

A. Event Viewer
B. Performance Monitor
C. System Information
D. Device Manager

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Event Viewer is the primary tool used to investigate system-level errors and logs, including BSODs. When a BSOD occurs, Windows logs the error codes and associated system behavior under ??System?? logs in Event Viewer. This allows the technician to review crash events, identify error codes (e.g., STOP codes), and pinpoint hardware or driver issues.
* B. Performance Monitor is used for real-time performance tracking and trend analysis, not crash logs.
* C. System Information displays system specs but not crash logs or events.
* D. Device Manager shows device status and driver issues but doesn??t retain error logs related to BSODs.
Reference:
CompTIA A+ 220-1102 Objective 3.1: Given a scenario, troubleshoot common Windows OS problems.
Study Guide Section: Troubleshooting BSODs using Event Viewer and system logs
==========================

NEW QUESTION 40
A user reports some single sign-on errors to a help desk technician. Currently, the user is able tosign 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:
Comprehensive and Detailed Explanation From Exact Extract:
SSO issues are often related to cached session data, cookies, or browser artifacts. The fact that the user can access the company portal but not one specific SaaS tool suggests a session or token problem. Using a private/incognito browsing window allows a clean session to be initiated, which often resolves SSO conflicts.
* A. Reenrolling MFA is not related unless access issues stem from failed multifactor authentication.
* C. Bypassing SSO may not be possible depending on the SaaS tool and company policies.
* D. Factory resetting a device is a last resort and unnecessary in this case. Reference:

CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common software, application, and OS security issues.
Study Guide Section: Troubleshooting login and authentication issues, especially with SSO services.
==========================

NEW QUESTION 43

......

Relate Links

100% Pass Your 220-1202 Exam with Exambible Prep Materials

https://www.exambible.com/220-1202-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/