100% Pass N10-009 - CompTIA Network+ Certification Exam Latest Latest Dumps Ppt

DOWNLOAD the newest DumpsTorrent N10-009 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1qB8Tz7tHHm9KgkUzAr-iL7eAQpQZgYfb

The DumpsTorrent is a leading platform that is committed to making the N10-009 exam dumps preparation simple, quick, and successful. To achieve this objective DumpsTorrent is offering real, valid, and updated CompTIA N10-009 practice questions in three different formats. These formats are DumpsTorrent CompTIA N10-009 PDF Dumps Files, desktop practice test software, and web-based practice test software. All these DumpsTorrent CompTIA Network+ Certification Exam exam questions formats are easy to use and compatible with all web browsers, operating systems, and devices.

Our N10-009 training materials are the latest, valid and accurate study material for candidates who are eager to clear N10-009 exams. You can actually grasp the shortest time to do as much interesting and effective things you like as possible. N10-009 real questions are high value & high pass rate with competitive price products. And our pass rate of N10-009 Study Guide is as high as 99% to 100%. As long as you study with our N10-009 exam questions, you will pass the N10-009 exam easily.

>> Latest N10-009 Dumps Ppt <<

CompTIA N10-009 Web-Based Practice Exam Questions Software

New developments in the tech sector always bring new job opportunities. These new jobs have to be filled with the N10-009

certification holders. So to fill the space, you need to pass the N10-009 Exam. Earning the N10-009 certification helps you clear the obstacles you face while working in the CompTIA field.

CompTIA N10-009 Exam Syllabus Topics:

Topic	Details
Topic 1	• Selection and configuration of wireless devices.
Topic 2	• Cloud concepts and connectivity options, and Common networking ports.
Topic 3	• Network Operations: For IT operations staff and network operations center (NOC) technicians, this part of the exam covers the purpose of organizational processes and procedures and use of network monitoring technologies.
Topic 4	• Networking Concepts: For network administrators and IT support professionals, this domain covers
Topic 5	• Network Security: This section of the exam for cybersecurity specialists and network security administrators covers the importance of basic network security concepts, Various types of attacks and their impact on the network, application of network security features, defense techniques, and solutions.| Network Troubleshooting: For help desk technicians and network support specialists, this section covers troubleshooting methodology, troubleshooting common cabling and physical interface issues, troubleshooting common issues with network services, and use of appropriate tools or protocols to solve networking issues.

CompTIA Network+ Certification Exam Sample Questions (Q453-Q458):

NEW QUESTION # 453
Which of the following network cables involves bouncing light off of protective cladding?

- A. Single-mode
- B. Coaxial
- C. Multimode
- D. Twinaxial

Answer: C

Explanation:
Comprehensive and Detailed Explanation (aligned to N10-009):
Multimode fiber uses multiple paths (modes) of light that bounce off the cladding to travel through the fiber. This is effective for shorter distances but more prone to dispersion.
A . Twinaxial is copper, not fiber.
B . Coaxial carries electrical signals, not light.
C . Single-mode fiber uses a single light path directly through the core without bouncing.
Reference (CompTIA Network+ N10-009):
Domain: Networking Concepts - Fiber optics: single-mode vs. multimode.

NEW QUESTION # 454
Which of the following allows for interactive, secure remote management of a network infrastructure device?

- A. RDP
- B. SNMP
- C. VNC
- D. SSH

Answer: D

Explanation:

SSH (Secure Shell) is a cryptographic network protocol that enables secure remote management and operation of network devices, including routers and switches. SSH encrypts traffic, making it more secure than alternatives like Telnet, which sends data in plaintext. The document states:
"SSH (Secure Shell) is the recommended protocol for secure, interactive remote management of network devices. It provides a secure channel over an unsecured network by encrypting the traffic between the administrator's workstation and the managed device."

NEW QUESTION # 455
SIMULATION
A network technician needs to resolve some issues with a customer's SOHO network.
The customer reports that some of the devices are not connecting to the network, while others appear to work as intended.
INSTRUCTIONS
Troubleshoot all the network components and review the cable test results by Clicking on each device and cable.
Diagnose the appropriate component(s) by identifying any components with a problem and recommend a solution to correct each problem.

Cable Test Results:
Cable 1:
Cable 2:
Cable 3:
Cable 4:

Answer:

Explanation:
See the Explanation for detailed information on this simulation
Explanation:
(Note: Ips will be change on each simulation task, so we have given example answer for the understanding) To troubleshoot all the network components and review the cable test results, you can use the following steps:
Click on each device and cable to open its information window.
Review the information and identify any problems or errors that may affect the network connectivity or performance.
Diagnose the appropriate component(s) by identifying any components with a problem and recommend a solution to correct each problem.
Fill in the remediation form using the drop-down menus provided.
Here is an example of how to fill in the remediation form for PC1:
The component with a problem is PC1.
The problem is Incorrect IP address.
The solution is Change the IP address to 192.168.1.10.
You can use the same steps to fill in the remediation form for other components.
To enter commands in each device, you can use the following steps:
Click on the device to open its terminal window.
Enter the command ipconfig /all to display the IP configuration of the device, including its IP address, subnet mask, default gateway, and DNS servers.
Enter the command ping <IP address> to test the connectivity and reachability to another device on the network by sending and receiving echo packets. Replace <IP address> with the IP address of the destination device, such as 192.168.1.1 for Core Switch 1.
Enter the command tracert <IP address> to trace the route and measure the latency of packets from the device to another device on the network by sending and receiving packets with increasing TTL values. Replace <IP address> with the IP address of the destination device, such as 192.168.1.1 for Core Switch 1.
Here is an example of how to enter commands in PC1:
Click on PC1 to open its terminal window.
Enter the command ipconfig /all to display the IP configuration of PC1. You should see that PC1 has an incorrect IP address of 192.168.2.10, which belongs to VLAN 2 instead of VLAN 1.
Enter the command ping 192.168.1.1 to test the connectivity to Core Switch 1. You should see that PC1 is unable to ping Core Switch 1 because they are on different subnets.
Enter the command tracert 192.168.1.1 to trace the route to Core Switch 1. You should see that PC1 is unable to reach Core Switch 1 because there is no route between them.
You can use the same steps to enter commands in other devices, such as PC3, PC4, PC5, and Server 1.

NEW QUESTION # 456
A network administrator is implementing security zones for each department. Which of the following should the administrator use to accomplish this task?

- A. ACLs
- B. NAC
- C. Content filtering
- D. Port security

Answer: A

Explanation:
Understanding ACLs:
Access Control Lists (ACLs): A set of rules used to control network traffic and restrict access to network resources by filtering packets based on IP addresses, protocols, or ports.
Implementing Security Zones:
Defining Zones: ACLs can be used to create security zones by applying specific rules to different departments, ensuring that only authorized traffic is allowed between these zones.
Control Traffic: ACLs control inbound and outbound traffic at network boundaries, enforcing security policies and preventing unauthorized access.
Comparison with Other Options:
Port Security: Limits the number of devices that can connect to a switch port, preventing MAC address flooding attacks, but not used for defining security zones.
Content Filtering: Blocks or allows access to specific content based on predefined policies, typically used for web filtering rather than network segmentation.
NAC (Network Access Control): Controls access to the network based on the security posture of devices but does not define security zones.
Implementation Steps:
Define ACL rules based on the requirements of each department.
Apply these rules to the appropriate network interfaces or firewall policies to segment the network into security zones.
Reference:
CompTIA Network+ study materials on network security and access control methods.

NEW QUESTION # 457
SIMULATION
A network administrator has been tasked with configuring a network for a new corporate office. The office consists of two buildings, separated by 50 feet with no physical connectivity. The configuration must meet the following requirements:
. Devices in both buildings should be
able to access the Internet.
. Security insists that all Internet traffic
be inspected before entering the
network.
. Desktops should not see traffic
destined for other devices.
INSTRUCTIONS
Select the appropriate network device for each location. If applicable, click on the magnifying glass next to any device which may require configuration updates and make any necessary changes.
Not all devices will be used, but all locations should be filled.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Answer:

Explanation:
See the step by step complete solution below
Explanation:
Devices in both buildings should be able to access the Internet.
Security insists that all Internet traffic be inspected before entering the network.
Desktops should not see traffic destined for other devices.

Here is the corrected layout with explanation:
Building A:
Switch: Correctly placed to connect all desktops.
Firewall: Correctly placed to inspect all incoming and outgoing traffic.
Building B:
Switch: Not needed. Instead, place a Wireless Access Point (WAP) to provide wireless connectivity for laptops and mobile devices.
Between Buildings:
Wireless Range Extender: Correctly placed to provide connectivity between the buildings wirelessly.
Connection to the Internet:
Router: Correctly placed to connect to the Internet and route traffic between the buildings and the Internet.
Firewall: The firewall should be placed between the router and the internal network to inspect all traffic before it enters the network.
Corrected Setup:
Top-left (Building A): Switch
Bottom-left (Building A): Firewall (inspect traffic before it enters the network) Top-middle (Internet connection): Router Bottom-middle (between buildings): Wireless Range Extender Top-right (Building B): Wireless Access Point (WAP) In this corrected setup, the WAP in Building B will connect wirelessly to the Wireless Range Extender, which is connected to the Router. The Router is connected to the Firewall to ensure all traffic is inspected before it enters the network.
Configuration for Wireless Range Extender:
SSID: CORP
Security Settings: WPA2 or WPA2 - Enterprise
Key or Passphrase: [Enter a strong passphrase]
Mode: [Set based on your network plan]
Channel: [Set based on your network plan]
Speed: Auto
Duplex: Auto
With these settings, both buildings will have secure access to the Internet, and all traffic will be inspected by the firewall before entering the network. Desktops and other devices will not see traffic intended for others, maintaining the required security and privacy.

To configure the wireless range extender for security, follow these steps:
SSID (Service Set Identifier):
Ensure the SSID is set to "CORP" as shown in the exhibit.
Security Settings:
WPA2 or WPA2 - Enterprise: Choose one of these options for stronger security. WPA2-Enterprise provides more robust security with centralized authentication, which is ideal for a corporate environment.
Key or Passphrase:
If you select WPA2, enter a strong passphrase in the "Key or Passphrase" field.
If you select WPA2 - Enterprise, you will need to configure additional settings for authentication servers, such as RADIUS, which is not shown in the exhibit.
Wireless Mode and Channel:
Set the appropriate mode and channel based on your network design and the environment to avoid interference. These settings are not specified in the exhibit, so set them according to your network plan.
Wired Speed and Duplex:
Set the speed to "Auto" unless you have specific requirements for 100 or 1000 Mbps.
Set the duplex to "Auto" unless you need to specify half or full duplex based on your network equipment.
Save Configuration:
After making the necessary changes, click the "Save" button to apply the settings.
Here is how the configuration should look after adjustments:
SSID: CORP
Security Settings: WPA2 or WPA2 - Enterprise
Key or Passphrase: [Enter a strong passphrase]
Mode: [Set based on your network plan]
Channel: [Set based on your network plan]
Speed: Auto
Duplex: Auto
Once these settings are configured, your wireless range extender will provide secure connectivity for devices in both buildings.
Firewall setting to to ensure complete compliance with the requirements and best security practices, consider the following adjustments and additions:
DNS Rule: This rule allows DNS traffic from the internal network to any destination, which is fine.
HTTPS Outbound: This rule allows HTTPS traffic from the internal network (assuming 192.169.0.1/24 is a typo and should be

192.168.0.1/24) to any destination, which is also good for secure web browsing.
Management: This rule allows SSH access to the firewall for management purposes, which is necessary for administrative tasks.
HTTPS Inbound: This rule denies inbound HTTPS traffic to the internal network, which is good unless you have a web server that needs to be accessible from the internet.
HTTP Inbound: This rule denies inbound HTTP traffic to the internal network, which is correct for security purposes.
Suggested Additional Settings:
Permit General Outbound Traffic: Allow general outbound traffic for web access, email, etc.
Block All Other Traffic: Ensure that all other traffic is blocked to prevent unauthorized access.
Firewall Configuration Adjustments:
Correct the Network Typo:
Ensure that the subnet 192.169.0.1/24 is corrected to 192.168.0.1/24.
Permit General Outbound Traffic:
Rule Name: General Outbound
Source: 192.168.0.1/24
Destination: ANY
Service: ANY
Action: PERMIT
Deny All Other Traffic:
Rule Name: Block All
Source: ANY
Destination: ANY
Service: ANY
Action: DENY
Here is how your updated firewall settings should look:
Rule Name
Source
Destination
Service
Action
DNS Rule
192.168.0.1/24
ANY
DNS
PERMIT
HTTPS Outbound
192.168.0.1/24
ANY
HTTPS
PERMIT
Management
ANY
192.168.0.1/24
SSH
PERMIT
HTTPS Inbound
ANY
192.168.0.1/24
HTTPS
DENY
HTTP Inbound
ANY
192.168.0.1/24
HTTP
DENY
General Outbound
192.168.0.1/24
ANY
ANY
PERMIT
Block All
ANY

ANY
ANY
DENY
These settings ensure that:
Internal devices can access DNS and HTTPS services externally.
Management access via SSH is permitted.
Inbound HTTP and HTTPS traffic is denied unless otherwise specified.
General outbound traffic is allowed.
All other traffic is blocked by default, ensuring a secure environment.
Make sure to save the settings after making these adjustments.

NEW QUESTION # 458
.....

The CompTIA N10-009 certification exam is one of the valuable credentials designed to demonstrate a candidate's technical expertise in information technology. They can remain current and competitive in the highly competitive market with the N10-009 certificate. For novices as well as seasoned professionals, the CompTIA Network+ Certification Exam Questions provide an excellent opportunity to not only validate their skills but also advance their careers.