N10-008$^{\text{Q\&As}}$

CompTIA Network+

Pass CompTIA N10-008 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/n10-008.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A company wants to implement a disaster recovery site for non-critical applications, which can tolerate a short period of downtime. Which of the following types of sites should the company implement to achieve this goal?

A. Hot

B. Cold

C. warm

D. Passive

Correct Answer: C

The type of site that the company should implement for non-critical applications that can tolerate a short period of downtime is a warm site. A warm site is a disaster recovery site that has some pre-installed equipment and software, but not as much as a hot site, which is fully operational and ready to take over the primary site\\'s functions in case of a disaster. A warm site requires some time and effort to activate and synchronize with the primary site, but not as much as a cold site, which has no equipment or software installed and requires a lot of configuration and testing. A passive site is not a common term for a disaster recovery site, but it could refer to a site that only receives backups from the primary site and does not actively participate in the network operations.

QUESTION 2

A company has multiple site-to-site VPN connections using a pre-shared key. The Chief Information Security Officer (CISO) is concerned about the long-term security of the tunnels and has asked the network technicians to develop a plan to ensure the best security of the tunnels. Which of the following should the network technicians implement?

A. Purchase dedicated MPLS circuits between each of the sites.

B. Request a change of IP addresses from the ISP semiannually.

C. Perform annual key rotations on the site-to-site VPNs.

D. Terminate tunnels when they are not actively being used.

Correct Answer: C

QUESTION 3

A Network engineer is investigating issues on a Layer 2 Switch. The department typically snares a Switchport during meetings for presentations, but atter the first user Shares, no Other users can connect. Which Of the following is MOST likely related to this issue?

A. Spanning Tree Protocol is enabled on the switch.

B. VLAN trunking is enabled on the switch.

C. Port security is configured on the switch.

D. Dynamic ARP inspection is configured on the switch.

Correct Answer: C

The most likely issue related to this scenario is that port security is configured on the switch. Port security is a Layer 2 security feature that restricts access to a switch port based on the MAC address of the device that is connected to it. When a port reaches its maximum number of allowed MAC addresses, it will prevent any further connections to that port. If the department is sharing a switchport during meetings for presentations, then it is possible that the maximum number of allowed MAC addresses has already been reached by the first user, and therefore no other users can connect.

QUESTION 4

Two network technicians are installing a fiber-optic link between routers. The technicians used a light meter to verify the correct fibers. However, when they connect the fibers to the router interface, the link does not connect. Which of the following would explain the issue? (Choose two.)

A. They used the wrong type of fiber transceiver.

B. Incorrect TX/RX polarity exists on the link

C. The connection has duplexing configuration issues.

D. Halogen light fixtures are causing interference.

E. One of the technicians installed a loopback adapter.

F. The RSSI was not strong enough on the link

Correct Answer: AB

QUESTION 5

A firewall administrator observes log entries of traffic being allowed to a web server on port 80 and port 443. The policy for this server is to only allow traffic on port 443. The firewall administrator needs to investigate how this change occurred to prevent a reoccurrence. Which of the following should the firewall administrator do next?

A. Consult the firewall audit logs.

B. Change the policy to allow port 80.

C. Remove the server object from the firewall policy.

D. Check the network baseline.

Correct Answer: A

Firewall audit logs are records of the changes made to the firewall configuration, policies, and rules. They can help the firewall administrator to track who, when, and what changes were made to the firewall, and identify any unauthorized or erroneous modifications that could cause security issues or network outages. By consulting the firewall audit logs, the firewall administrator can investigate how the change that allowed traffic on port 80 to the web server occurred, and prevent it from happening again