TestpassportQ&A

Higher Quality Better Service!

We offer free update service for one year

Http://www.testpassport.com

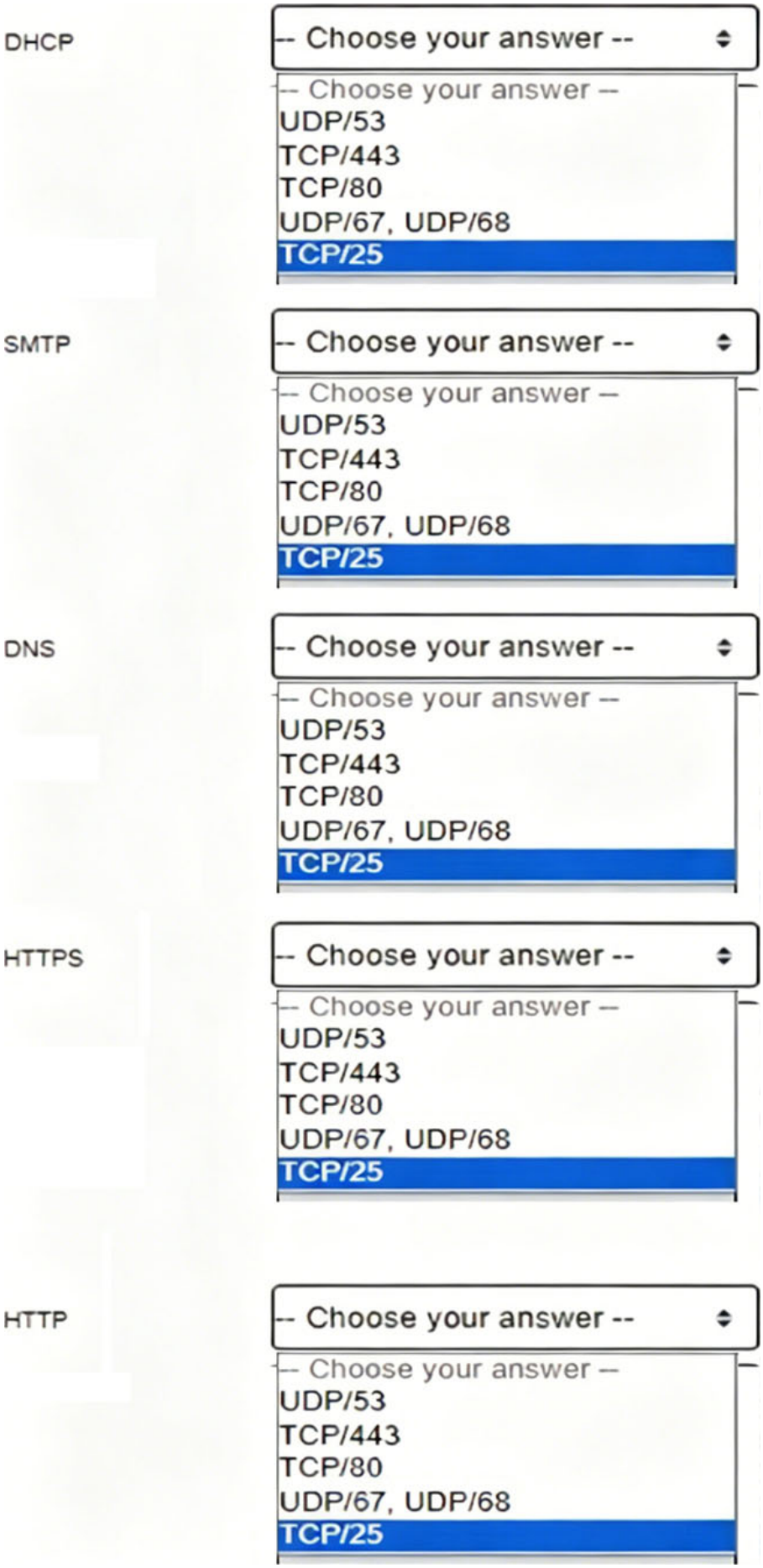
Exam : **Network Security Essentials**

Title : Network Security Essentials for Locally-Managed Fireboxes

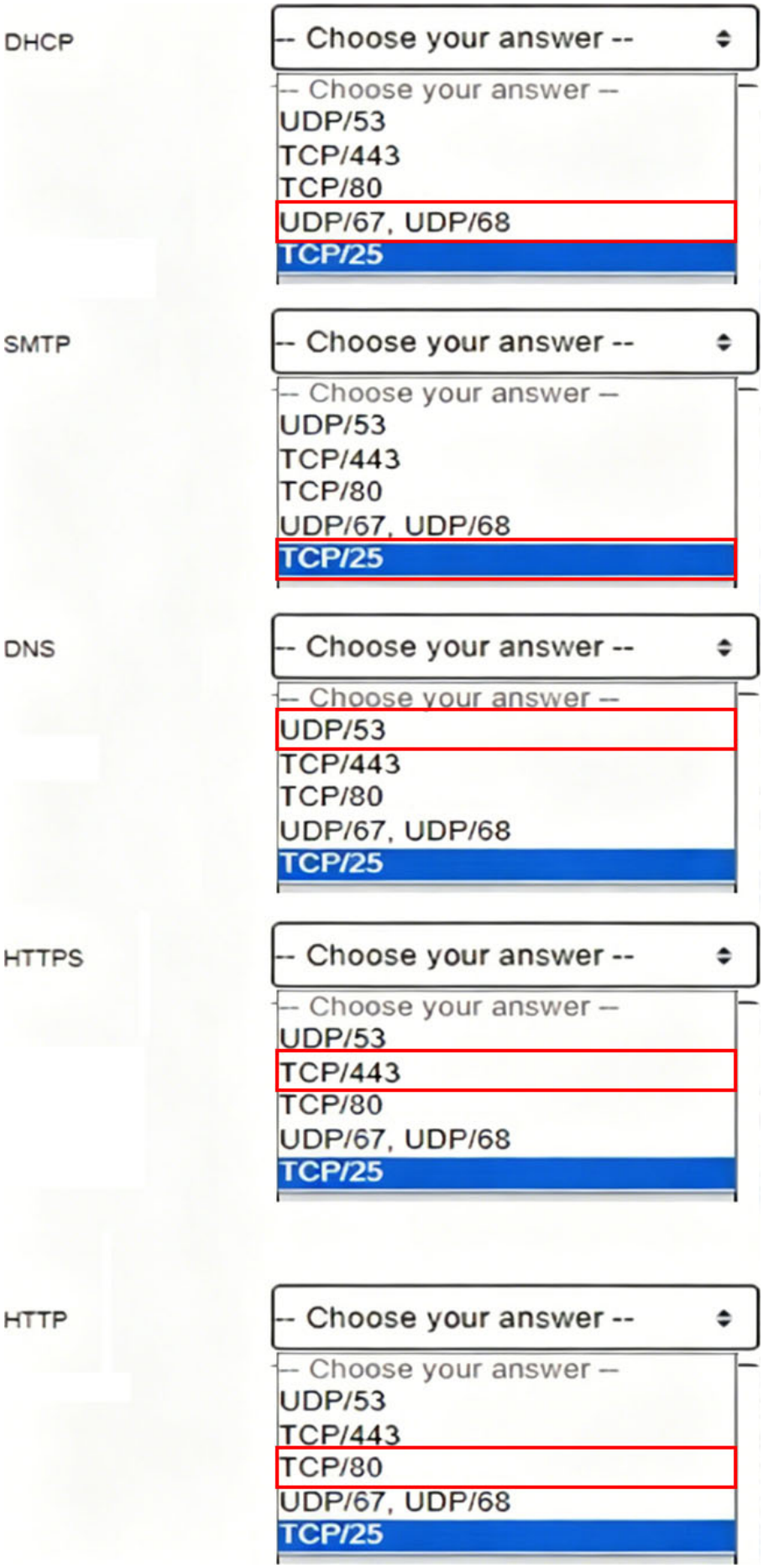
Version : DEMO

1.HOTSPOT

Match the "network server to the protocol and port it uses."


DHCP
-- Choose your answer --
-- Choose your answer --
UDP/53
TCP/443
TCP/80
UDP/67, UDP/68
TCP/25
SMTP
-- Choose your answer --
-- Choose your answer --
UDP/53
TCP/443
TCP/80
UDP/67, UDP/68
TCP/25
DNS
-- Choose your answer --
-- Choose your answer --
UDP/53
TCP/443
TCP/80
UDP/67, UDP/68
TCP/25
HTTPS
-- Choose your answer --
-- Choose your answer --
UDP/53
TCP/443
TCP/80
UDP/67, UDP/68
TCP/25
HTTP
-- Choose your answer --
-- Choose your answer --
UDP/53
TCP/443
TCP/80
UDP/67, UDP/68
TCP/25

Answer:


DHCP
-- Choose your answer --
-- Choose your answer --
UDP/53
TCP/443
TCP/80
UDP/67, UDP/68
TCP/25
SMTP
-- Choose your answer --
-- Choose your answer --
UDP/53
TCP/443
TCP/80
UDP/67, UDP/68
TCP/25
DNS
-- Choose your answer --
-- Choose your answer --
UDP/53
TCP/443
TCP/80
UDP/67, UDP/68
TCP/25
HTTPS
-- Choose your answer --
-- Choose your answer --
UDP/53
TCP/443
TCP/80
UDP/67, UDP/68
TCP/25
HTTP
-- Choose your answer --
-- Choose your answer --
UDP/53
TCP/443
TCP/80
UDP/67, UDP/68
TCP/25

Explanation:
DHCP (Dynamic Host Configuration Protocol): DHCP operates over UDP ports 67 and 68. Port 67 is used by the DHCP server to listen for client requests, and port 68 is used by the DHCP client. This allows devices to automatically receive IP addresses and other network configuration details on a network, essential for automating IP management. [Referenced from multiple sources on network fundamentals]
SMTP (Simple Mail Transfer Protocol): SMTP uses TCP port 25 for sending emails from client to server or between mail servers. SMTP is integral for email transmission, allowing efficient communication across mail servers within and outside organizational networks. [Referenced in standard protocols documentation in network management guides]
DNS (Domain Name System): DNS typically runs on UDP port 53 for standard queries, with TCP/53 used for zone transfers and other larger requests. DNS is critical for resolving human-readable domain names into IP addresses, which allows users to connect to websites using easily remembered names rather than numerical IP addresses. [Foundational knowledge as detailed in network security and management resources]
HTTPS (Hypertext Transfer Protocol Secure): HTTPS, an encrypted version of HTTP, operates on TCP port 443. It provides secure communication over the internet by encrypting data between the client and server using SSL/TLS, protecting data integrity and privacy. [Security essentials for network communications as found in secure web traffic documentation]
HTTP (Hypertext Transfer Protocol): HTTP operates on TCP port 80 and is used for unencrypted web traffic. HTTP is the foundation of data exchange on the World Wide Web, supporting basic client-server interactions for retrieving resources from the web. [Basic networking knowledge referenced across multiple network essentials texts]

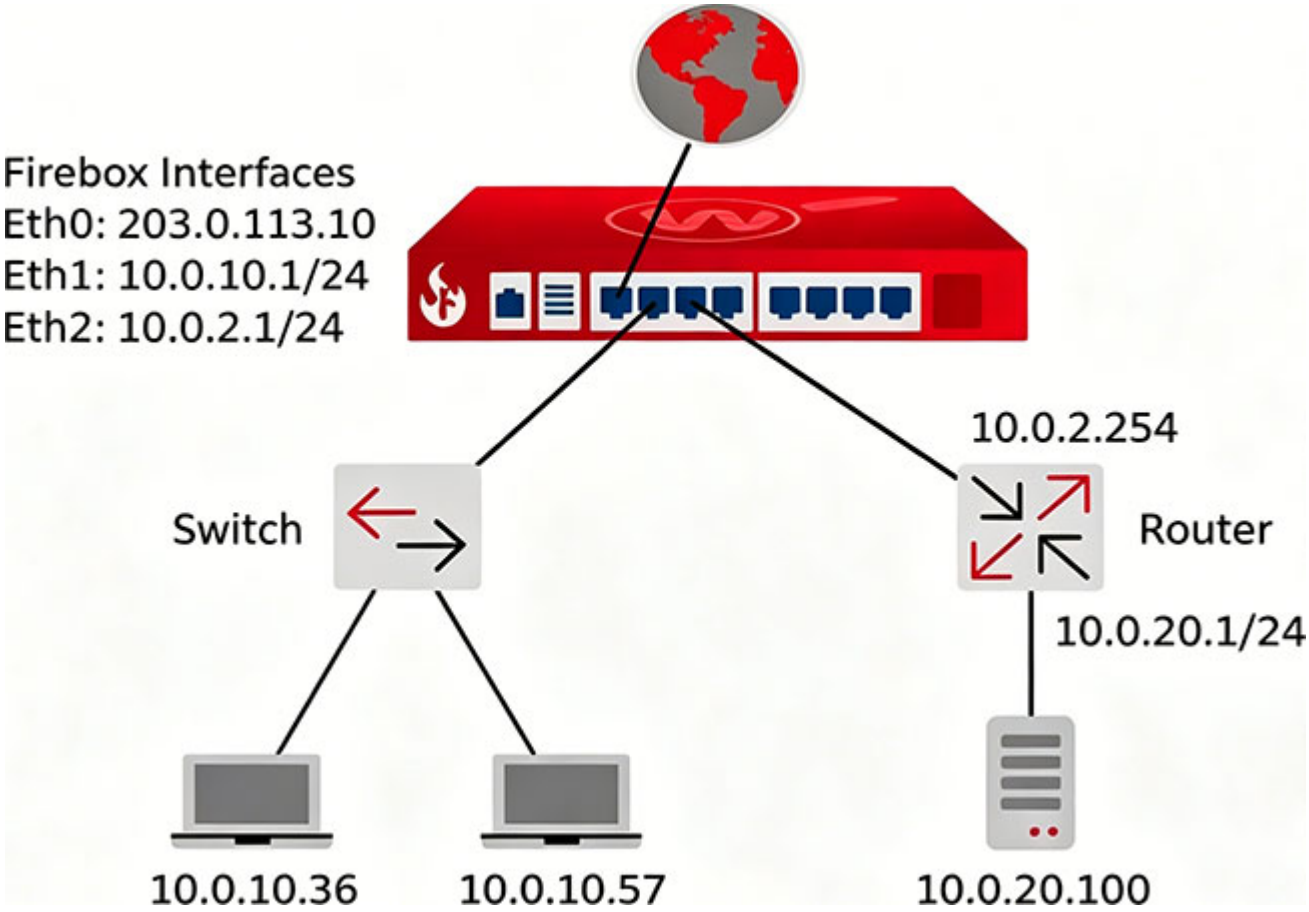
2.Which of these is a network IP address? (Select one.)
A. 1G2 153 10 0 1
B. 1Q2 158.10 0-24
C. 172 16 100 1/12
D. 10 0.1 255 8
E. 10 10 10 255/24
Answer: E
Explanation:
In this question, we need to identify the correctly formatted network IP address. IPv4 addresses are represented in a dotted decimal format, typically in the form of x.x.x.x/n, where x represents decimal values from 0 to 255, and /n is the CIDR notation indicating the subnet mask. Among the options:

3.When does a network host make an ARP request? (Select one.)
A. To find the IP address associated with a hostname
B. To find the IP address of the default gateway
C. To find the hostname associated with an IP address
D. To find the MAC address associated with an IP address
E. To find the IP address associated with a MAC address
Answer: D
Explanation:

The Address Resolution Protocol (ARP) is used to map an IP address to a physical machine (MAC) address on a local network. When a device wants to communicate with another device on the same local network, it uses an ARP request to discover the MAC address associated with a known IP address. The ARP process is essential for IP-based communication within the same network segment.

4.Which of these is a valid host IP address in the subnet 10.0.1.0/24? (Select one.)
A. 10.0.10.24/24
B. 10.0.1.255/24
C. 10.0.1.100/24
D. 10.0.0.1/24
E. 10.0.1.0/24
Answer: C
Explanation:
The subnet 10.0.1.0/24 has an IP range from10.0.1.1 to 10.0.1.254. In a /24 subnet:
Option C (10.0.1.100/24) falls within the valid range for host addresses in the 10.0.1.0/24 subnet, making it the correct answer.

5.You added a route on the Firebox for the 10.0.20.0/24 network. The server has 10.0.2.1 configured as its default gateway. The clients have 10.0.10.1 configured as their default gateway. The client computers on the 10.0.10.0/24 network cannot route traffic to the server at 10.0.20.100.
What could cause this problem? (Select one.)



A. The router at 10.0.2.254 does not have a route to reach the server

B. The default gateway of the clients is misconfigured
C. The default gateway of the server is misconfigured
D. The router at 10.0.2.254 needs an IP address in the 10.0.10.0/24 network
E. The server does not have a route for the 10.0.10.0/24 network
Answer: C
Explanation:
In this scenario:
The issue arises because the server is in the 10.0.20.0/24 network and should have a gateway that directs traffic through the appropriate path. However, since 10.0.2.1 is configured as the server's gateway, the server likely doesn’t have a correct return path to the clients on 10.0.10.0/24. This misconfiguration prevents the server from properly routing responses back to clients.