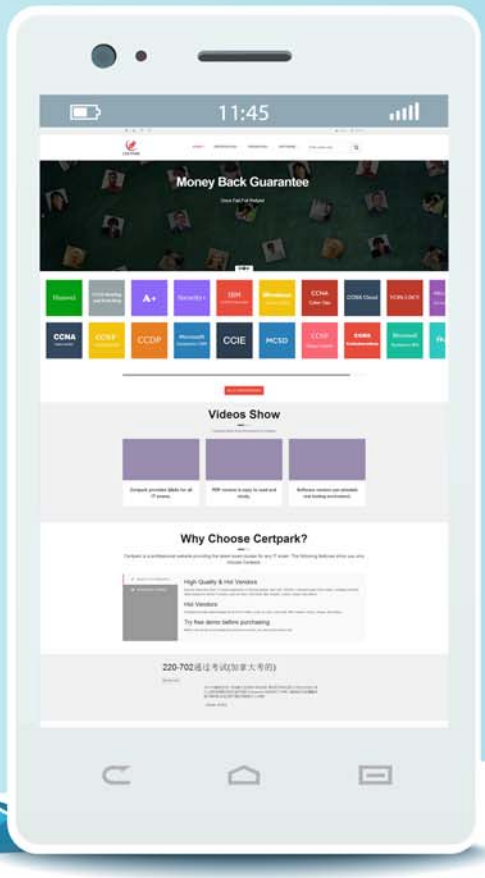
CERTPARK

QUESTION & ANSWER

CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



https://www.certpark.com

Exam : **NSE7_NST-7.2**

Title : Fortinet NSE 7 - Network Security 7.2 Support Engineer

Version : DEMO

1.Refer to the exhibit, which shows the omitted output of a real-time OSPF debug

```
OSPF: RECV[Hello]: From 0.0.0.112 via port2:192.168.37.114 (192.168.37.115 -> 224.0.0.5)
OSPF: ----------------------------------------------------
OSPF: Header
OSPF:   Version 2
OSPF:   Type 1 (Hello)
OSPF:   Packet Len 48
OSPF:   Router ID 0.0.0.112
OSPF:   Area ID 0.0.0.0
OSPF:   Checksum 0x2f85
OSPF:   AuType 0
OSPF: Hello
OSPF:   NetworkMask 255.255.255.0
OSPF:   HelloInterval 10
OSPF:   Options 0x2 (*|-|-|-|-|-|E|-)
OSPF:   RtrPriority 1
OSPF:   RtrDeadInterval 40
OSPF:   DRouter 192.168.37.114
OSPF:   BDRouter 192.168.37.115
OSPF:   # Neighbors 1
OSPF:     Neighbor 0.0.0.111
OSPF: ----------------------------------------------------
OSPF: RECV[Hello]: From 0.0.0.112 via port2:192.168.37.114: Authentication type mismatch
```

Which statement is false?

A. A password has been configured on the local OSPF router but is not shown in the output

B. The Hello packet is being sent from an OSPF router with ID 0.0.0.112.

C. The two FortiGate devices attempting adjacency are in area 0.0.0.0.

D. One FortiGate device is configured to require authentication, while the other is not

Answer: A

Explanation:

Examine the OSPF debug output:

The OSPF Hello packet debug output shows the Router ID as 0.0.0.112.

It shows that the OSPF packet is being sent from 0.0.0.112 via port2:192.168.37.114.

The OSPF Hello packet contains information such as the network mask (255.255.255.0), hello interval (10), router priority (1), dead interval (40), and designated router (192.168.37.114) and backup designated router (192.168.37.115).

Check the area configuration:

The area ID is shown as 0.0.0.0, indicating that the two devices attempting adjacency are in area 0.0.0.0.

Authentication mismatch:

The debug output indicates an "Authentication type mismatch". This means one device is configured to require authentication while the other is not.

Password configuration:

The statement claiming that "A password has been configured on the local OSPF router but is not shown in the output" is false because the output indicates an authentication mismatch, not the presence or absence of a password. The other statements are true based on the provided debug output.

Reference: Fortinet Network Security 7.2 Support Engineer Documentation OSPF Configuration Guides

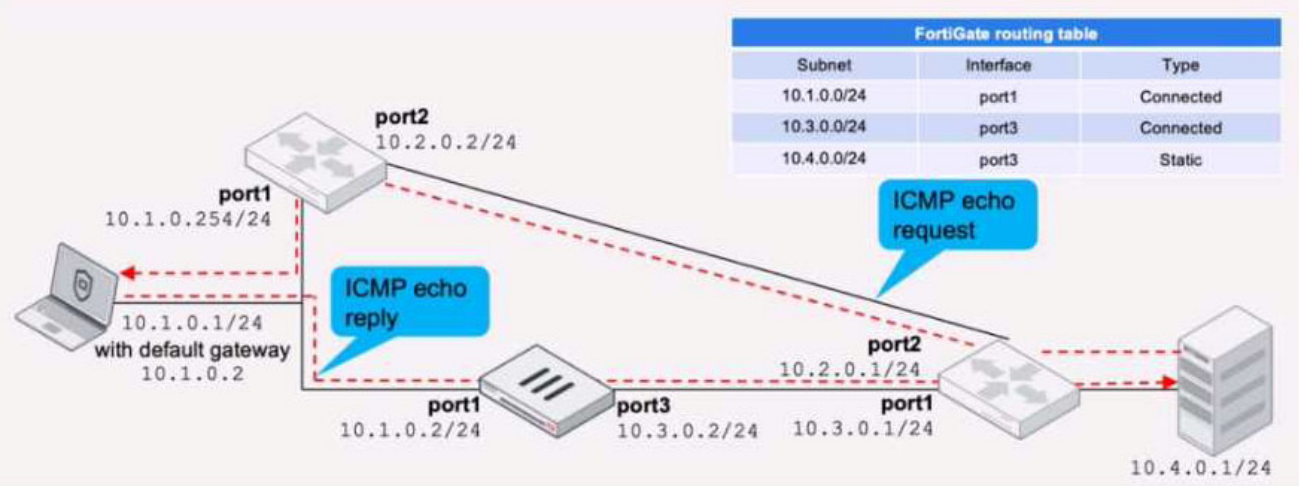
2.Which of the following regarding protocol states is true?

A. proto_state=00 indicates that UDP traffic flows in both directions.

B. proto_state-01 indicates an established TCP session.
C. proto_state=10 indicates an established TCP session.
D. proto state=01 indicates one-way ICMP traffic.
Answer: C
Explanation:
Understanding protocol states:
proto_state=00: Indicates no traffic or a closed session.
proto_state=01: Typically indicates one-way ICMP traffic or a partially established TCP session.
proto_state=10: Indicates an established TCP session, where the session has completed the three-way handshake and both sides can send and receive data.
proto_state=11: Often indicates a fully established and active bidirectional session.
Explanation of correct answer
proto_state=10 is the correct indication for an established TCP session as it signifies that the session is fully established and active.
Reference: Fortinet Network Security 7.2 Support Engineer Documentation Fortinet Firewall Protocol State Documentation

3.Which statement is correct regarding LDAP authentication using the regular bind type?
A. The regular bind type goes through four steps to successfully authenticate a user.
B. The regular bind type cannot be used if users are authenticated using sAMAccountName.
C. The regular bind type is the easiest bind type to configure on FortiOS.
D. The regular bind type requires a FortiGate super_admin account.
Answer: A
Explanation:
LDAP Authentication Process:
The regular bind type for LDAP authentication involves multiple steps to verify user credentials.
Step 1: The client sends a bind request with the username to the LDAP server.
Step 2: The LDAP server responds to the bind request.
Step 3: The client sends a bind request with the password.
Step 4: The LDAP server responds, confirming or denying the authentication.
Explanation of Answer.
The regular bind type follows these four steps to authenticate a user, making it a comprehensive method but not necessarily the easiest to configure.
The statement regarding sAMAccountName and super_admin account requirements are not accurate in the context of regular bind type LDAP authentication on FortiOS.
Reference: Fortinet Network Security 7.2 Support Engineer Documentation FortiOS LDAP Authentication Configuration Guides

4.Refer to the exhibit.



FortiGate has already been configured with a firewall policy that allows all ICMP traffic to flow from port1 to port3.

Which changes must the administrator perform to ensure the server at 10.4.0.1/24 receives the echo reply from the laptop at 10.1.0.1/24?

A. Enable asymmetric routing under config system settings.

B. Modify the default gateway on the laptop from 10.1.0.2 to 10.2.0.2

C. A firewall policy that allows all ICMP traffic from port3 to port1.

D. Change the configuration from strict RPF check mode to feasible RPF check mode

Answer: C

Explanation:

Current Configuration Analysis:

The firewall policy currently allows ICMP traffic from port1 to port3, enabling the ICMP echo request to reach the server.

However, for the server to send an ICMP echo reply back to the laptop, the traffic must be allowed from port3 to port1.

Required Configuration:

To ensure the server at 10.4.0.1/24 can send the ICMP echo reply back to the laptop at 10.1.0.1/24, the administrator needs to configure a new firewall policy.

The policy must explicitly allow ICMP traffic from port3 to port1.

Steps to Configure:

Access the FortiGate configuration interface.

Navigate to the Firewall Policy section.

Create a new policy allowing ICMP traffic from port3 to port1.

Save and apply the new policy to ensure bidirectional ICMP traffic is permitted.

Reference: Fortinet Network Security 7.2 Support Engineer Documentation FortiGate Firewall Policy Configuration Guides

5.Which two conditions would prevent a static route from being added to the routing table? (Choose two.)

A. The next-hop IP address is unreachable.

B. The interface specified in the route configuration is down

C. The route has a lower priority value than another route to the same destination.

D. There is another other route to the same destination, with a lower distance.

Answer: AB

Explanation:

Next-hop IP address:

For a static route to be added to the routing table, the next-hop IP address must be reachable. If it is not reachable, the route cannot be considered valid and will not be added.

Interface status:

If the interface specified in the static route configuration is down, the route will not be added to the routing table. The interface must be up and operational for the route to be valid.

Priority and Distance:

While priority and administrative distance affect route selection, they do not prevent a route from being added to the routing table. Instead, they influence which route is preferred when multiple routes to the same destination exist.

Reference: Fortinet Network Security 7.2 Support Engineer Documentation Routing Configuration and Troubleshooting Guides