NSE7_EFW-7.2 Q&As

Fortinet NSE 7 - Enterprise Firewall 7.2

Pass Fortinet NSE7_EFW-7.2 Exam with 100% Guarantee

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

https://www.leads4pass.com/nse7_efw-7-2.html

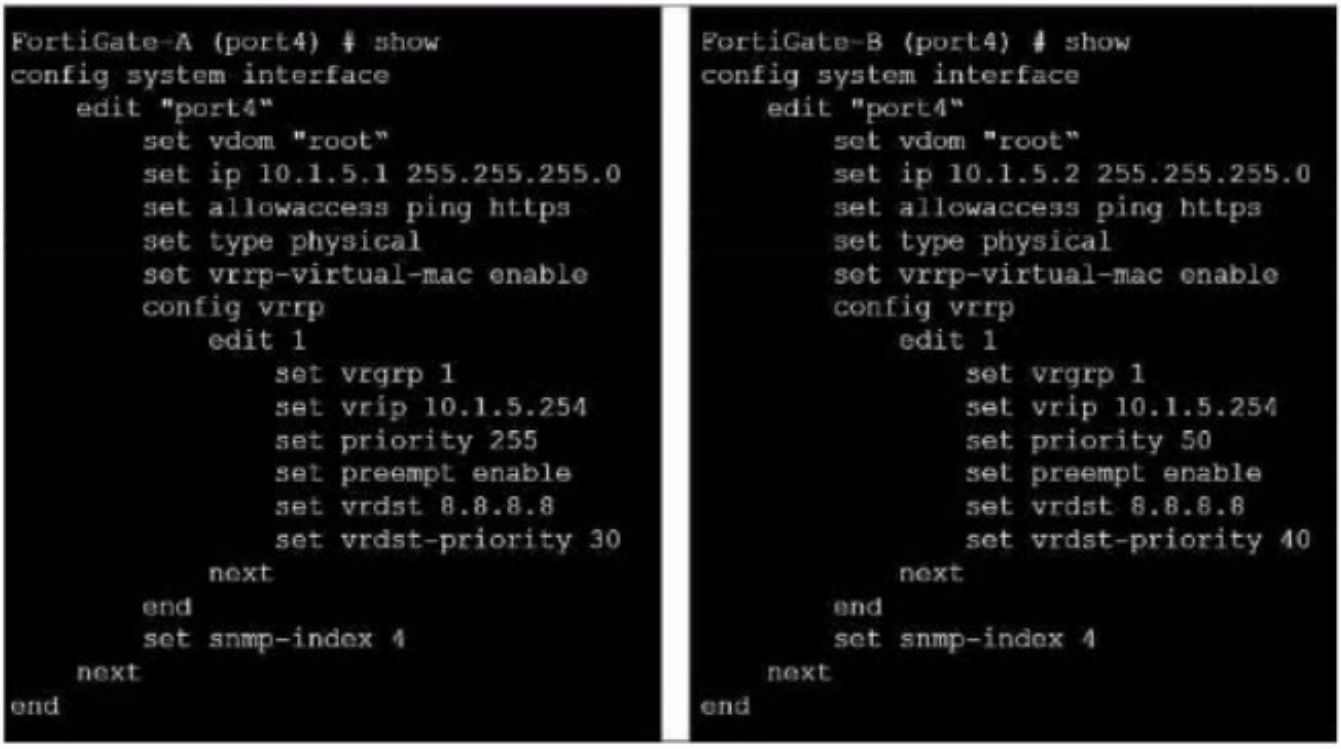
100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Exhibit.



```
FortiGate-A (port4) # show
config system interface
    edit "port4"
        set vdom "root"
        set ip 10.1.5.1 255.255.255.0
        set allowaccess ping https
        set type physical
        set vrrp-virtual-mac enable
        config vrrp
            edit 1
                set vrgrp 1
                set vrip 10.1.5.254
                set priority 255
                set preempt enable
                set vrdst 8.8.8.8
                set vrdst-priority 30
            next
        end
        set snmp-index 4
    next
end
```

```
FortiGate-B (port4) # show
config system interface
    edit "port4"
        set vdom "root"
        set ip 10.1.5.2 255.255.255.0
        set allowaccess ping https
        set type physical
        set vrrp-virtual-mac enable
        config vrrp
            edit 1
                set vrgrp 1
                set vrip 10.1.5.254
                set priority 50
                set preempt enable
                set vrdst 8.8.8.8
                set vrdst-priority 40
            next
        end
        set snmp-index 4
    next
end
```

Refer to the exhibit, which contains the partial interface configuration of two FortiGate devices.

Which two conclusions can you draw from this con figuration? (Choose two)

A. 10.1.5.254 is the default gateway of the internal network

B. On failover new primary device uses the same MAC address as the old primary

C. The VRRP domain uses the physical MAC address of the primary FortiGate

D. By default FortiGate B is the primary virtual router

Correct Answer: AB

The Virtual Router Redundancy Protocol (VRRP) configuration in the exhibit indicates that 10.1.5.254 is set as the virtual IP (VRIP), commonly serving as the default gateway for the internal network (A). Withvrrp-virtual-macenabled, both FortiGates would use the same virtual MAC address, ensuring a seamless transition during failover (B). The VRRP domain does not use the physical MAC address (C), and the priority settings indicate that FortiGate-A would be the primary router by default due to its higher priority (D).

QUESTION 2

Winch two statements about ADVPN are true? (Choose two)

A. auto-discovery receiver must be set to enable on the Spokes.

B. Spoke to-spoke traffic never goes through the hub

C. It supports NAI for on-demand tunnels

D. Routing is configured by enabling add-advpn-route

Correct Answer: AC

ADVPN (Auto Discovery VPN) is a feature that allows to dynamically establish direct tunnels (called shortcuts) between the spokes of a traditional Hub and Spoke architecture. The auto-discovery receiver must be set to enable on the spokes to allow them to receive NHRP messages from the hub and other spokes. NHRP (Next Hop Resolution Protocol) is used for on-demand tunnels, which are established when there is traffic between spokes. Routing is configured by enabling add-nhrp-route, not add-advpn- route. References := ADVPN | FortiGate / FortiOS 7.2.0 | Fortinet Document Library, Technical Tip: Fortinet Auto Discovery VPN (ADVPN)

QUESTION 3

Which two statements about metadata variables are true? (Choose two.)

A. You create them on FortiGate

B. They apply only to non-firewall objects.

C. The metadata format is $.

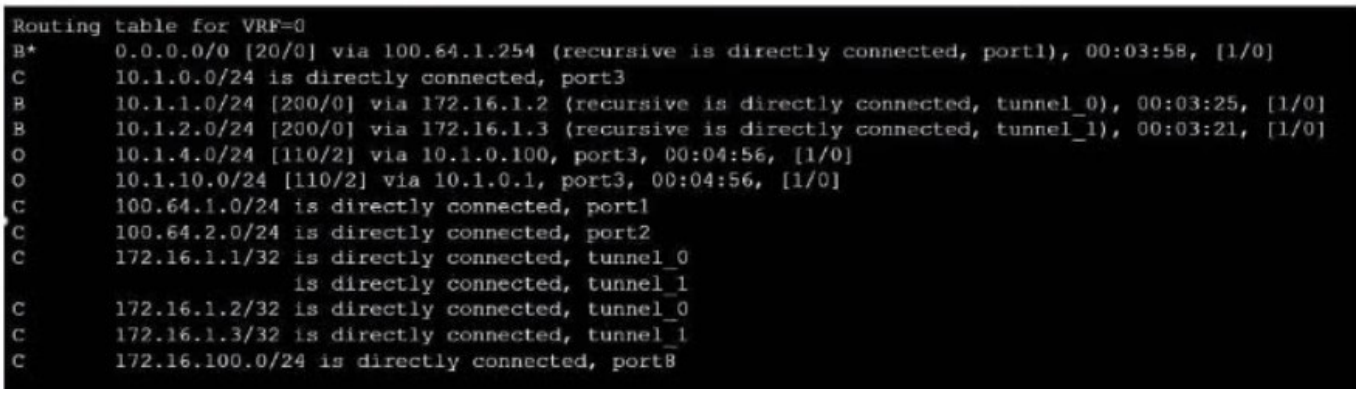
D. They can be used as variables in scripts

Correct Answer: AD

Metadata variables in FortiGate are created to store metadata associated with different FortiGate features. These variables can be used in various configurations and scripts to dynamically replace the variable with its actual value during processing. A: You create metadata variables on FortiGate. They are used to store metadata for FortiGate features and can be called upon in different configurations. D: They can be used as variables in scripts. Metadata variables are utilized within the scripts to dynamically insert values as per the context when the script runs. Fortinet FortiOS Handbook: CLI Reference

QUESTION 4

Exhibit.



```
Routing table for VRF=0
B*      0.0.0.0/0 [20/0] via 100.64.1.254 (recursive is directly connected, port1), 00:03:58, [1/0]
C       10.1.0.0/24 is directly connected, port3
B       10.1.1.0/24 [200/0] via 172.16.1.2 (recursive is directly connected, tunnel_0), 00:03:25, [1/0]
B       10.1.2.0/24 [200/0] via 172.16.1.3 (recursive is directly connected, tunnel_1), 00:03:21, [1/0]
O       10.1.4.0/24 [110/2] via 10.1.0.100, port3, 00:04:56, [1/0]
O       10.1.10.0/24 [110/2] via 10.1.0.1, port3, 00:04:56, [1/0]
C       100.64.1.0/24 is directly connected, port1
C       100.64.2.0/24 is directly connected, port2
C       172.16.1.1/32 is directly connected, tunnel_0
                      is directly connected, tunnel_1
C       172.16.1.2/32 is directly connected, tunnel_0
C       172.16.1.3/32 is directly connected, tunnel_1
C       172.16.100.0/24 is directly connected, port8
```

Refer to the exhibit, which shows a partial touting table

What two concisions can you draw from the corresponding FortiGate configuration? (Choose two.)

A. IPSec Tunnel aggregation is configured

B. net-device is enabled in the tunnel IPSec phase 1 configuration

C. OSPI is configured to run over IPSec.

D. add-route is disabled in the tunnel IPSec phase 1 configuration.

Correct Answer: BD

Option B is correct because the routing table shows that the tunnel interfaces have a netmask of 255.255.255.255, which indicates that net-device is enabled in the phase 1 configuration. This option allows the FortiGate to use the tunnel interface as a next-hop for routing, without adding a route to the phase 2 destination1. Option D is correct because the routing table does not show any routes to the phase 2 destination networks, which indicates that add-route is disabled in the phase 1 configuration. This option controls whether the FortiGate adds a static route to the phase 2 destination network using the tunnel interface as the gateway2. Option A is incorrect because IPSec tunnel aggregation is a feature that allows multiple phase 2 selectors to share a single phase 1 tunnel, reducing the number of tunnels and improving performance3. This feature is not related to the routing table or the phase 1 configuration. Option C is incorrect because OSPF is a dynamic routing protocol that can run over IPSec tunnels, but it requires additional configuration on the FortiGate and the peer device4. This option is not related to the routing table or the phase 1 configuration. References: =

1: Technical Tip: `set net-device\\' new route-based IPsec logic2

2: Adding a static route5

3: IPSec VPN concepts6

4: Dynamic routing over IPsec VPN7

QUESTION 5

Which two statements about ADVPN are true? (Choose two.)

A. You must disable add-route in the hub.

B. AllFortiGate devices must be in the same autonomous system (AS).

C. The hub adds routes based on IKE negotiations.

D. You must configure phase 2 quick mode selectors to 0.0.0.0 0.0.0.0.

Correct Answer: CD

C. The hub adds routes based on IKE negotiations: This is part of the ADVPN functionality where the hub learns about the networks behind the spokes and can add routes dynamically based on the IKE negotiations with the spokes. D. You must configure phase 2 quick mode selectors to 0.0.0.0 0.0.0.0: This wildcard setting in the phase 2 selectors allows any-to-any tunnel establishment, which is necessary for the dynamic creation of spoke-to-spoke tunnels. These configurations are outlined in Fortinet\\'s documentation for setting up ADVPN, where the hub\\'s role in route control and the use of wildcard selectors for phase 2 are emphasized to enable dynamic tunneling between spokes.