Fortinet.Premium.NSE4_FGT-6.0.by.VCEplus.70q

Number: NSE4_FGT-6.0 VCEplus
Passing Score: 800
Time Limit: 120 min
File Version: 1.3

Exam Code: NSE4_FGT-6.0
Exam Name: Fortinet NSE4 - FortiOS 6.0
Certification Provider: Fortinet
Corresponding Certification: NSE4
Website: www.vceplus.com
Free Exam: https://vceplus.com/exam-nse4-fgt-6-0/
Questions & Answers Exam Engine is rigorously checked before being put up for sale. We make sure there is nothing irrelevant in NSE4_FGT-6.0 exam products and you get latest questions. We strive to deliver the best NSE4_FGT-6.0 exam product for top grades in your first attempt.

Website: https://vceplus.com
VCE to PDF Converter: https://vceplus.com/vce-to-pdf/
Facebook: https://www.facebook.com/VCE.For.All.VN/
Twitter : https://twitter.com/VCE_Plus

QUESTION 1
What files are sent to FortiSandbox for inspection in flow-based inspection mode?

A. All suspicious files that do not have their hash value in the FortiGuard antivirus signature database.
B. All suspicious files that are above the defined oversize limit value in the protocol options.
C. All suspicious files that match patterns defined in the antivirus profile.
D. All suspicious files that are allowed to be submitted to FortiSandbox in the antivirus profile.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which statements about a One-to-One IP pool are true? (Choose two.)

A. It is used for destination NAT.
B. It allows the fixed mapping of an internal address range to an external address range.
C. It does not use port address translation.
D. It allows the configuration of ARP replies.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which of the following FortiGate configuration tasks will create a route in the policy route table? (Choose two.)

A. Static route created with a Named Address object
B. Static route created with an Internet Services object
C. SD-WAN route created for individual member interfaces

D. SD-WAN rule created to route traffic based on link latency

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
A company needs to provide SSL VPN access to two user groups. The company also needs to display different welcome messages on the SSL VPN login screen for both user groups.
What is required in the SSL VPN configuration to meet these requirements?

A. Different SSL VPN realms for each group.
B. Two separate SSL VPNs in different interfaces mapping the same ssl.root.
C. Two firewall policies with different captive portals.
D. Different virtual SSL VPN IP addresses for each group.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
An administrator is investigating a report of users having intermittent issues with browsing the web. The administrator ran diagnostics and received the output shown in the exhibit.

```
# diagnose sys session stat
misc info: session_count=16 setup_rate=0 exp_count=0 clash=889
memory_tension_drop=0 ephemeral=1/16384 removeable=3
delete=0, flush=0, dev_down=16/69
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=0005e722
ids_recv=000fdc94
url_recv=00000000
av_recv=001fee47
fqdn_count=00000000
tcp reset stat: syncqf=119 acceptqf=0 no-listener=3995 data=0 ses=2 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0
```

Examine the diagnostic output shown exhibit. Which of the following options is the most likely cause of this issue?

A. NAT port exhaustion
B. High CPU usage
C. High memory usage
D. High session timeout value

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
An administrator has configured central DNAT and virtual IPs. Which of the following can be selected in the firewall policy Destination field?

A. A VIP group

B. The mapped IP address object of the VIP object
C. A VIP object
D. An IP pool

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
An administrator needs to strengthen the security for SSL VPN access. Which of the following statements are best practices to do so? (Choose three.)

A. Configure split tunneling for content inspection.
B. Configure host restrictions by IP or MAC address.
C. Configure two-factor authentication using security certificates.
D. Configure SSL offloading to a content processor (FortiASIC).
E. Configure a client integrity check (host-check).

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Which statement about FortiGuard services for FortiGate is true?

A. The web filtering database is downloaded locally on FortiGate.
B. Antivirus signatures are downloaded locally on FortiGate.
C. FortiGate downloads IPS updates using UDP port 53 or 8888.
D. FortiAnalyzer can be configured as a local FDN to provide antivirus and IPS updates.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which of the following route attributes must be equal for static routes to be eligible for equal cost multipath (ECMP) routing? (Choose two.)

A. Priority
B. Metric
C. Distance
D. Cost

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
View the exhibit.

```
Local-FortiGate # diagnose sys ha checksum cluster

================== FGVM010000058290 ==================

is_manage_master()=1, is_root_master()=1
debugzone
global: 85 26 52 f2 f9 6e 3c c9 f5 21 1a 78 69 b6 20 bd
root: 30 51 63 1b 2d ef 77 aa f7 50 00 25 4d 42 a9 7d
all: 38 28 3d e4 24 8f 5b 10 8a 64 30 f2 34 13 c1 35

checksum
global: 85 26 52 f2 f9 6e 3c c9 f5 21 1a 78 69 b6 20 bd
root: 30 51 63 1b 2d ef 77 aa f7 50 00 25 4d 42 a9 7d
all: 38 28 3d e4 24 8f 5b 10 8a 64 30 f2 34 13 c1 35

================== FGVM010000058289 ==================

is_manage_master()=0, is_root_master()=0
debugzone
global: 85 26 52 f2 f9 6e 3c c9 f5 21 1a 78 69 b6 20 bd
root: 30 51 63 1b 2d ef 77 aa f7 50 00 25 4d 8a 55 8b
all: 38 28 3d e4 24 8f 5b 10 8a 64 30 f2 34 dc 9a 43

checksum
global: 85 26 52 f2 f9 6e 3c c9 f5 21 1a 78 69 b6 20 bd
root: 30 51 63 1b 2d ef 77 aa f7 50 00 25 4d 8a 55 8b
all: 38 28 3d e4 24 8f 5b 10 8a 64 30 f2 34 dc 9a 43
```

Based on this output, which statements are correct? (Choose two.)

A. The all VDOM is not synchronized between the primary and secondary FortiGate devices.
B. The root VDOM is not synchronized between the primary and secondary FortiGate devices.
C. The global configuration is synchronized between the primary and secondary FortiGate devices.
D. The FortiGate devices have three VDOMs.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

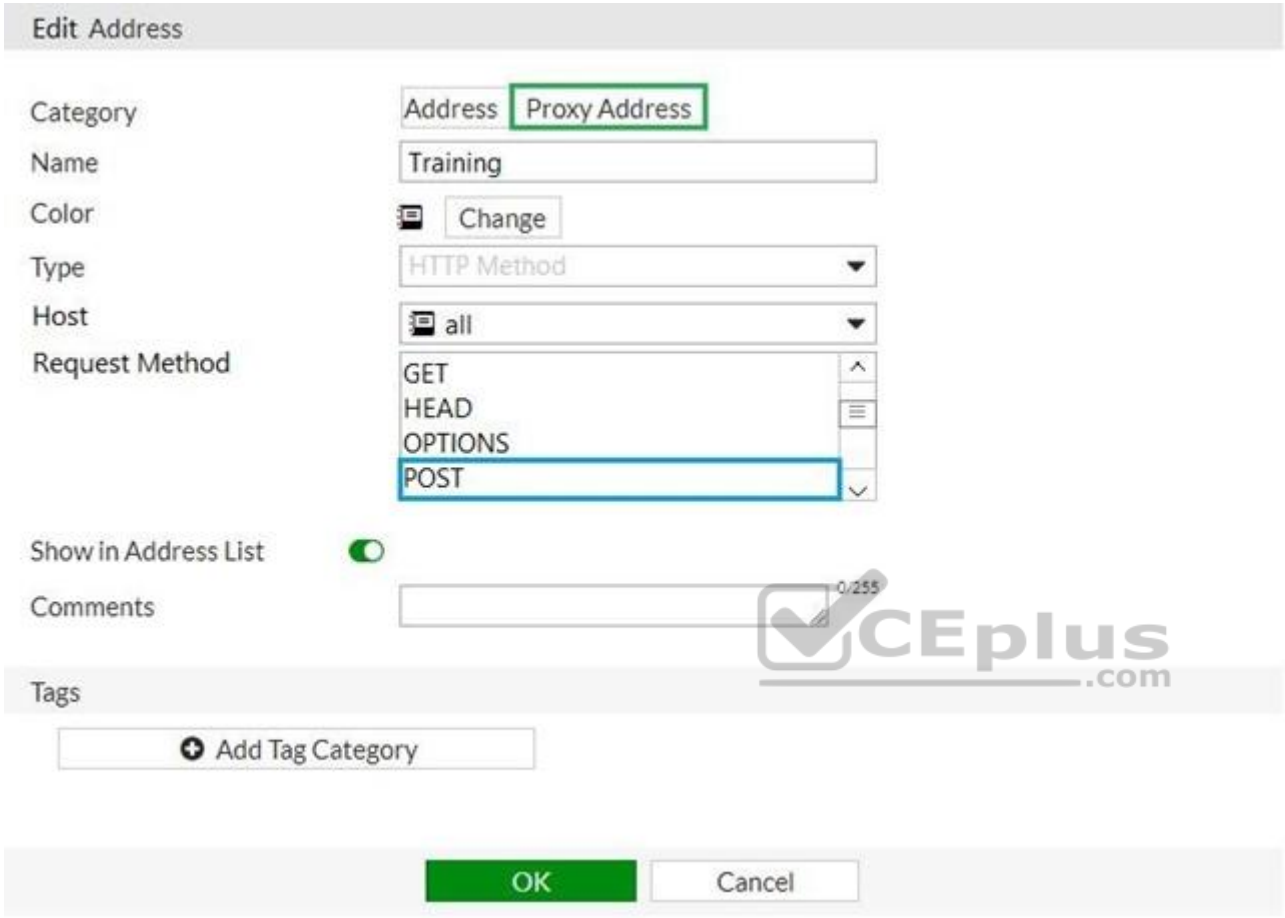
QUESTION 11
Which statement is true regarding the policy ID number of a firewall policy?

A. Defines the order in which rules are processed.
B. Represents the number of objects used in the firewall policy.
C. Required to modify a firewall policy using the CLI.
D. Changes when firewall policies are reordered.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
An administrator wants to block HTTP uploads. Examine the exhibit, which contains the proxy address created for that purpose.



Where must the proxy address be used?

A. As the source in a firewall policy.
B. As the source in a proxy policy.
C. As the destination in a firewall policy.
D. As the destination in a proxy policy.

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 13
Which statement is true regarding SSL VPN timers? (Choose two.)

A. Allow to mitigate DoS attacks from partial HTTP requests.
B. SSL VPN settings do not have customizable timers.
C. Disconnect idle SSL VPN users when a firewall policy authentication timeout occurs.
D. Prevent SSL VPN users from being logged out because of high network latency.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Which of the following conditions must be met in order for a web browser to trust a web server certificate signed by a third-party CA?

A. The public key of the web server certificate must be installed on the browser.
B. The web-server certificate must be installed on the browser.
C. The CA certificate that signed the web-server certificate must be installed on the browser.
D. The private key of the CA certificate that signed the browser certificate must be installed on the browser.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
When using SD-WAN, how do you configure the next-hop gateway address for a member interface so that FortiGate can forward Internet traffic?

A. It must be configured in a static route using the sdwan virtual interface.
B. It must be provided in the SD-WAN member interface configuration.
C. It must be configured in a policy-route using the sdwan virtual interface.
D. It must be learned automatically through a dynamic routing protocol.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which of the following services can be inspected by the DLP profile? (Choose three.)

A. NFS
B. FTP
C. IMAP
D. CIFS
E. HTTP-POST

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which of the following statements describe WMI polling mode for the FSSO collector agent? (Choose two.)

A. The NetSessionEnum function is used to track user logoffs.
B. WMI polling can increase bandwidth usage in large networks.
C. The collector agent uses a Windows API to query DCs for user logins.
D. The collector agent do not need to search any security event logs.

Correct Answer: BC

Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Which statements about DNS filter profiles are true? (Choose two.)

A. They can inspect HTTP traffic.
B. They can redirect blocked requests to a specific portal.
C. They can block DNS requests to known botnet command and control servers.
D. They must be applied in firewall policies with SSL inspection enabled.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
An administrator has configured a dialup IPsec VPN with XAuth. Which statement best describes what occurs during this scenario?

A. Phase 1 negotiations will skip preshared key exchange.
B. Only digital certificates will be accepted as an authentication method in phase 1.C
C. Dialup clients must provide a username and password for authentication.
D. Dialup clients must provide their local ID during phase 2 negotiations.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
An administrator has configured two VLAN interfaces:

```
config system interface
  edit "VLAN10"
        set vdom "VDOM1"
        set forward-domain 100
        set role lan
        set interface "port9"
        set vlanid 10
    next
    edit "VLAN5"
        set vdom "VDOM1"
        set forward-domain 50
        set role lan
        set interface "port10"
        set vlanid 5
    next
end
```

A DHCP server is connected to the VLAN10 interface. A DHCP client is connected to the VLAN5 interface. However, the DHCP client cannot get a dynamic IP address from the DHCP server. What is the cause of the problem?

A. Both interfaces must belong to the same forward domain.
B. The role of the VLAN10 interface must be set to server.
C. Both interfaces must have the same VLAN ID.
D. Both interfaces must be in different VDOMs.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Which of the following statements about virtual domains (VDOMs) are true? (Choose two.)

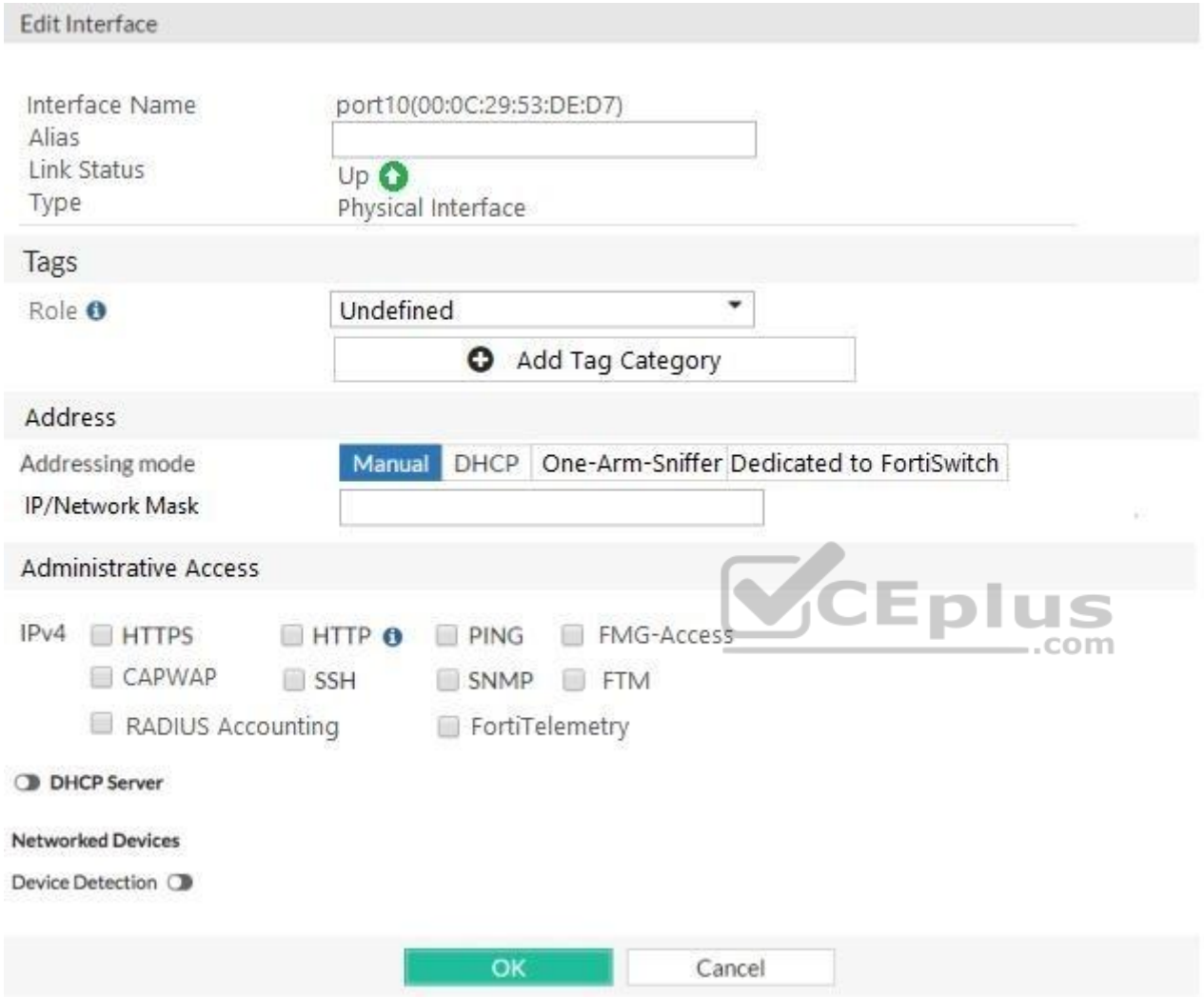
A. The root VDOM is the management VDOM by default.
B. A FortiGate device has 64 VDOMs, created by default.

C. Each VDOM maintains its own system time.
D. Each VDOM maintains its own routing table.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
You are configuring the root FortiGate to implement the security fabric. You are configuring port10 to communicate with a downstream FortiGate. View the default Edit Interface in the exhibit below:



When configuring the root FortiGate to communicate with a downstream FortiGate, which settings are required to be configured? (Choose two.)

A. Device detection enabled.
B. Administrative Access: FortiTelemetry.
C. IP/Network Mask.
D. Role: Security Fabric.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
What FortiGate components are tested during the hardware test? (Choose three.)

A. Administrative access
B. HA heartbeat
C. CPU
D. Hard disk
E. Network interfaces

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

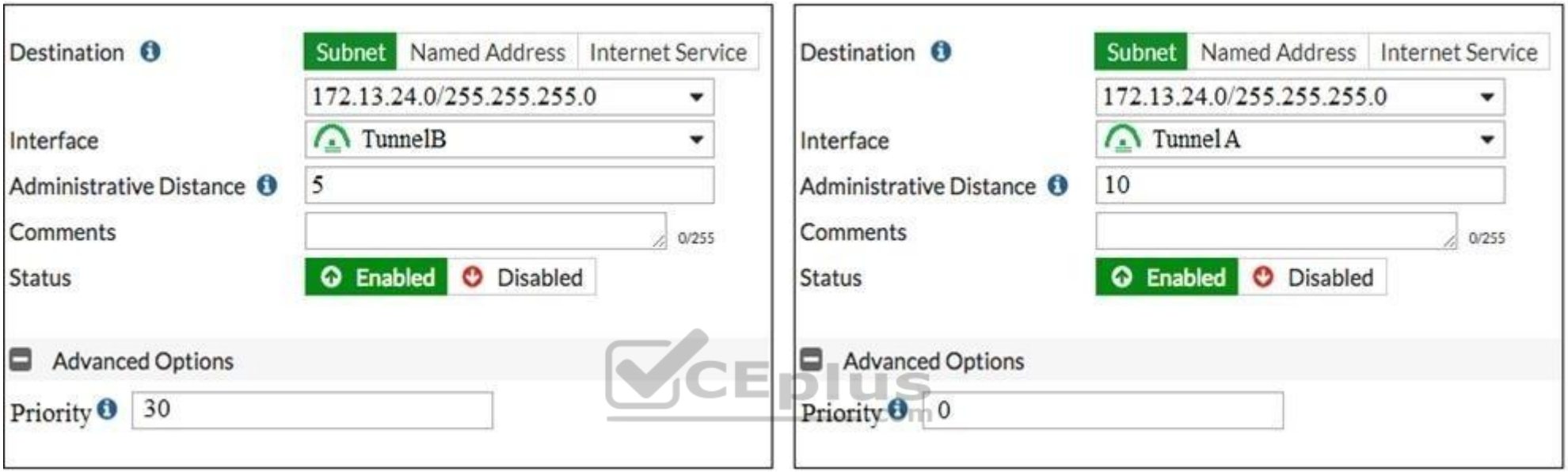
QUESTION 24
Which statements correctly describe transparent mode operation? (Choose three.)

A. All interfaces of the transparent mode FortiGate device must be on different IP subnets.
B. Ethernet packets are forwarded based on destination MAC addresses, not IP addresses.
C. The transparent FortiGate is visible to network hosts in an IP traceroute.
D. It permits inline traffic inspection and firewalling without changing the IP scheme of the network.
E. FortiGate acts as transparent bridge and forwards traffic at Layer 2.

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
View the exhibit.



Which of the following statements are correct? (Choose two.)

A. This setup requires at least two firewall policies with the action set to IPsec.
B. Dead peer detection must be disabled to support this type of IPsec setup.
C. The TunnelB route is the primary route for reaching the remote site. The TunnelA route is used only if the TunnelB VPN is down.
D. This is a redundant IPsec setup.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26

Which one of the following processes is involved in updating IPS from FortiGuard?

A. FortiGate IPS update requests are sent using UDP port 443.
B. Protocol decoder update requests are sent to service.fortiguard.net.
C. IPS signature update requests are sent to update.fortiguard.net.
D. IPS engine updates can only be obtained using push updates.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
How does FortiGate select the central SNAT policy that is applied to a TCP session?

A. It selects the SNAT policy specified in the configuration of the outgoing interface.
B. It selects the first matching central SNAT policy, reviewing from top to bottom.
C. It selects the central SNAT policy with the lowest priority.
D. It selects the SNAT policy specified in the configuration of the firewall policy that matches the traffic.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Which of the following conditions are required for establishing an IPSec VPN between two FortiGate devices? (Choose two.)

A. If XAuth is enabled as a server in one peer, it must be enabled as a client in the other peer.
B. If the VPN is configured as route-based, there must be at least one firewall policy with the action set to IPSec.
C. If the VPN is configured as DialUp User in one peer, it must be configured as either Static IP Address or Dynamic DNS in the other peer.
D. If the VPN is configured as a policy-based in one peer, it must also be configured as policy-based in the other peer.

Correct Answer: BC

Section: (none)
Explanation

Explanation/Reference:

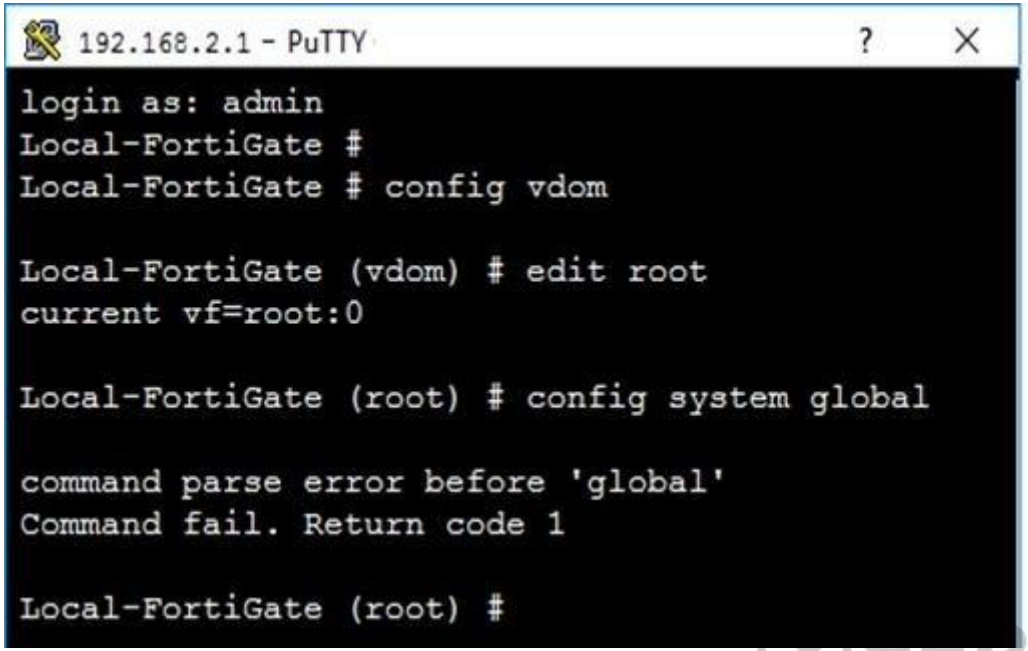
QUESTION 29
Which of the following statements about converse mode are true? (Choose two.)

A. FortiGate stops sending files to FortiSandbox for inspection.
B. FortiGate stops doing RPF checks over incoming packets.
C. Administrators cannot change the configuration.
D. Administrators can access the FortiGate only through the console port.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
View the exhibit.



Why is the administrator getting the error shown in the exhibit?

A. The administrator must first enter the command edit global.
B. The administrator admin does not have the privileges required to configure global settings.
C. The global settings cannot be configured from the root VDOM context.
D. The command config system global does not exist in FortiGate.

Correct Answer: A
Section: (none)
Explanation

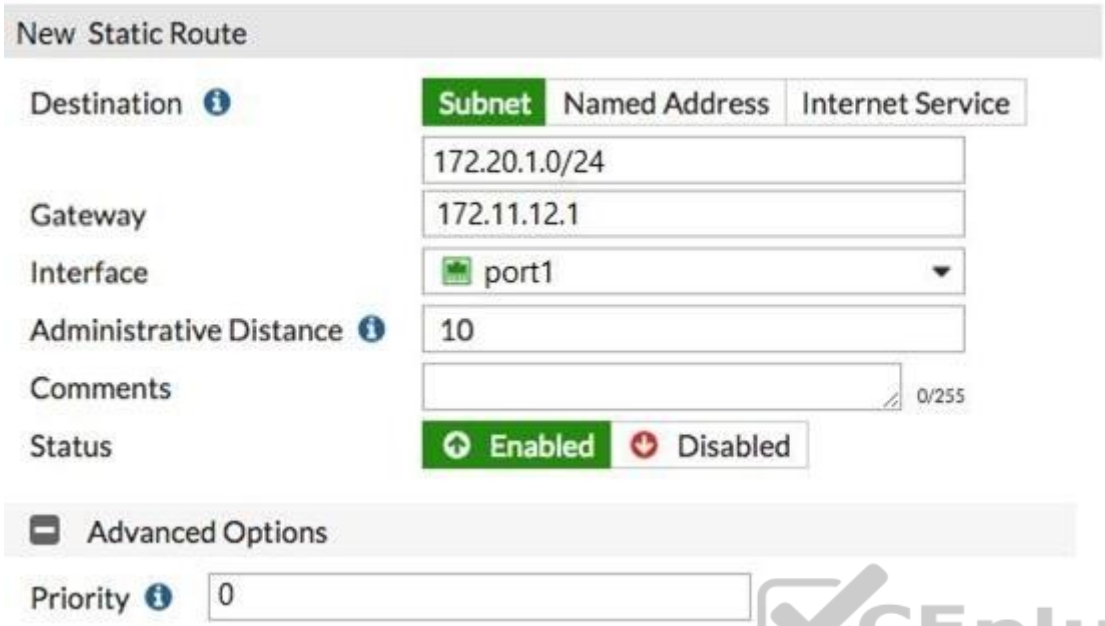
Explanation/Reference:

QUESTION 31
Examine the network diagram and the existing FGTI routing table shown in the exhibit, and then answer the following question:


```
FGT1 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1,  N2 - OSPF external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default;

S      172.20.0.0/16 [10/0] via 172.21.1.2, port2
C      172.21.0.0/16 is directly connected, port2
C      172.11.11.0/24 is directly connected, port1
```

An administrator has added the following static route on FGTI.



Since the change, the new static route is not showing up in the routing table. Given the information provided, which of the following describes the cause of this problem?

A. The new route's destination subnet overlaps an existing route.
B. The new route's Distance value should be higher than 10.
C. The Gateway IP address is not in the same subnet as port1.
D. The Priority is 0, which means that this route will remain inactive.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which configuration objects can be selected for the Source field of a firewall policy? (Choose two.)

A. Firewall service

B. User or user group
C. IP Pool
D. FQDN address

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
View the exhibit.

Which users and user groups are allowed access to the network through captive portal?

A. Users and groups defined in the firewall policy.
B. Only individual users - not groups - defined in the captive portal configuration
C. Groups defined in the captive portal configuration
D. All users

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
NGFW mode allows policy-based configuration for most inspection rules. Which security profile's configuration does not change when you enable policy-based inspection?

A. Web filtering
B. Antivirus
C. Web proxy
D. Application control

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
During the digital verification process, comparing the original and fresh hash results satisfies which security requirement?

A. Authentication.
B. Data integrity.
C. Non-repudiation.
D. Signature verification.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
An administration wants to throttle the total volume of SMTP sessions to their email server. Which of the following DoS sensors can be used to achieve this?

A. tcp_port_scan
B. ip_dst_session
C. udp_flood
D. ip_src_session

Correct Answer: A
Section: (none)
Explanation